

Cloudpath Protected Extensible Authentication Protocol (PEAP) Configuration Guide

Supporting 5.2

Copyright Notice and Proprietary Information

© 2018 ARRIS Enterprises, LLC. All rights reserved.

No part of this documentation may be used, reproduced, transmitted, or translated, in any form or by any means, electronic, mechanical, manual, optical, or otherwise, without prior written permission of or as expressly provided by under license from ARRIS.

Destination Control Statement

Technical data contained in this publication may be subject to the export control laws of the United States of America. Disclosure to nationals of other countries contrary to United States law is prohibited. It is the reader's responsibility to determine the applicable regulations and to comply with them.

Disclaimer

THIS DOCUMENTATION AND ALL INFORMATION CONTAINED HEREIN ("MATERIAL") IS PROVIDED FOR GENERAL INFORMATION PURPOSES ONLY. ARRIS and RUCKUS WIRELESS, INC. AND THEIR LICENSORS MAKE NO WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, WITH REGARD TO THE MATERIAL, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT AND FITNESS FOR A PARTICULAR PURPOSE, OR THAT THE MATERIAL IS ERROR-FREE, ACCURATE OR RELIABLE. ARRIS and RUCKUS RESERVE THE RIGHT TO MAKE CHANGES OR UPDATES TO THE MATERIAL AT ANY TIME.

Limitation of Liability

IN NO EVENT SHALL ARRIS or RUCKUS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL OR CONSEQUENTIAL DAMAGES, OR DAMAGES FOR LOSS OF PROFITS, REVENUE, DATA OR USE, INCURRED BY YOU OR ANY THIRD PARTY, WHETHER IN AN ACTION IN CONTRACT OR TORT, ARISING FROM YOUR ACCESS TO, OR USE OF, THE MATERIAL.

Trademarks

Ruckus Wireless, Ruckus, the bark logo, BeamFlex, ChannelFly, Dynamic PSK, FlexMaster, ICX, Simply Better Wireless, SmartCell, SmartMesh, SmartZone, Unleashed, ZoneDirector and ZoneFlex are trademarks of Ruckus Wireless, Inc. in the United States and in other countries. Other trademarks may belong to third parties.

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	8
Configuring a PEAP WLAN on a Ruckus ZoneDirector Controller	9
Configuring a PEAP WLAN on a Ruckus SmartZone Controller	13
Configuring PEAP on Cloudpath to Integrate with the Ruckus Controller	19
Adding a PEAP Branch to Your Workflow.....	19
Adding a PEAP Device Configuration to Your Workflow.....	22
Configuring Cloudpath to Communicate with the External RADIUS server.....	24
Testing the PEAP User Experience.....	26
Troubleshooting Tips.....	28

Preface

Document Conventions

The following tables list the text and notice 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.



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

bold text

italic text

[]

{ x | y | z }

x | y

< >

...

Description

Identifies command names, keywords, and command options.

Identifies a variable.

Syntax components displayed within square brackets are optional.

Default responses to system prompts are enclosed in square brackets.

A choice of required parameters is enclosed in curly brackets separated by vertical bars. You must select one of the options.

A vertical bar separates mutually exclusive elements.

Nonprinting characters, for example, passwords, are enclosed in angle brackets.

Repeat the previous element, for example, *member*[*member*...].

Convention

Description

\

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: docs@ruckuswireless.com

When contacting us, please include the following information:

- Document title and release number
- Document part number (on the cover page)
- Page number (if appropriate)
- For example:
 - Ruckus Small Cell Alarms Guide SC Release 1.3
 - Part number: 800-71306-001
 - Page 88

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 documentation by product or perform a text search. Access to Release Notes requires an active support contract and Ruckus Support Portal user account. Other technical documentation content is available without logging into 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 Networks products, and customers and partners with active support contracts.

For product support information and details on contacting the Support Team, go directly to the 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.

Overview of PEAP Configuration

- 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. Request 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, and Asia Pacific, toll-free numbers are available at <https://support.ruckuswireless.com/contact-us> and Live Chat is also available.

Self-Service Resources

The Support Portal at <https://support.ruckuswireless.com/contact-us> 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)—<https://support.ruckuswireless.com/documents>
- [Community Forums](https://forums.ruckuswireless.com/ruckuswireless/categories)—<https://forums.ruckuswireless.com/ruckuswireless/categories>
- [Knowledge Base Articles](https://support.ruckuswireless.com/answers)—<https://support.ruckuswireless.com/answers>
- [Software Downloads and Release Notes](https://support.ruckuswireless.com/software)—<https://support.ruckuswireless.com/software>
- [Security Bulletins](https://support.ruckuswireless.com/security)—<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 9
3. [Configuring PEAP on Cloudpath to Integrate with the Ruckus Controller](#) on page 19

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 8
2. [Configuring a PEAP WLAN on a Ruckus SmartZone Controller](#) on page 13
3. [Configuring PEAP on Cloudpath to Integrate with the Ruckus Controller](#) on page 19

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	<input type="text" value="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*	<input type="text" value="10.176.209.54"/>
Port*	<input type="text" value="1812"/>
Shared Secret*	<input type="password" value="••••••••"/>
Confirm Secret*	<input type="password" value="••••••••"/>
Retry Policy	
Request Timeout*	<input type="text" value="3"/> seconds
Max Number of Retries*	<input type="text" value="2"/> times

Enter the following values for the authentication server:

- Name = Any descriptive name you wish.
- Type = RADIUS
- Encryption: Leave the TLS box unchecked.

Set up the AAA Authentication Server on the Ruckus SmartZone Controller

- 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 9.

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 displays the 'Edit AAA Server: [Jeff AAA Auth vSZ]' configuration window. The window is titled 'Edit AAA Server: [Jeff AAA Auth vSZ]' and has a close button in the top right corner. The main content area is divided into sections. At the top is a 'General Options' section with a dropdown arrow. Below this are several fields: 'Name' (Jeff AAA Auth vSZ), 'Description' (empty), and 'Type' (RADIUS selected, Active Directory and LDAP unselected). There is also a 'Backup RADIUS' checkbox labeled 'Enable Secondary Server' which is currently unchecked. Below these is a 'Primary Server' section with a white background, containing fields for 'IP Address' (10.176.209.54), 'Port' (1812), 'Shared Secret' (masked with dots), and 'Confirm Secret' (masked with dots). At the bottom of the window are two buttons: 'OK' and 'Cancel'.

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 13.

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**.

Configuring a PEAP WLAN on a Ruckus ZoneDirector Controller

- 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. The page 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' and a note: '(Recommended to enable 802.11k Neighbor-list Report for assistant.)'
- 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 and dropdown menus:
 - 'Web Authentication': 'Enable captive portal/Web authentication' (checkbox), with a note: '(Users will be redirected to a Web portal for authentication before they can access the WLAN.)'
 - 'Authentication Server': A dropdown menu set to 'Local Database' and a 'Create New' button.
 - 'Wireless Client Isolation': Two checkboxes for isolating traffic, and a dropdown menu set to 'No WhiteList' with a 'Create New' button. A note below reads: '(Requires whitelist for gateway and other allowed hosts.)'
 - 'Zero-IT Activation™': 'Enable Zero-IT Activation' (checkbox), with a note: '(WLAN users are provided with wireless configuration installer after they log in.)'
 - 'Priority': Radio buttons for 'High' (selected) and 'Low'.

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

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*	eng-PEAP ESSID eng-PEAP
Description	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 (Recommended to enable 802.11k Neighbor-list Report for assistant.)

- 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 ▼ 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 ▼ 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

WLAN List						
This table lists your current WLANs and provides basic details about them. Click Create New to add another WLAN, or click Edit to make changes to an existing WLAN.						
<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 19.

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.

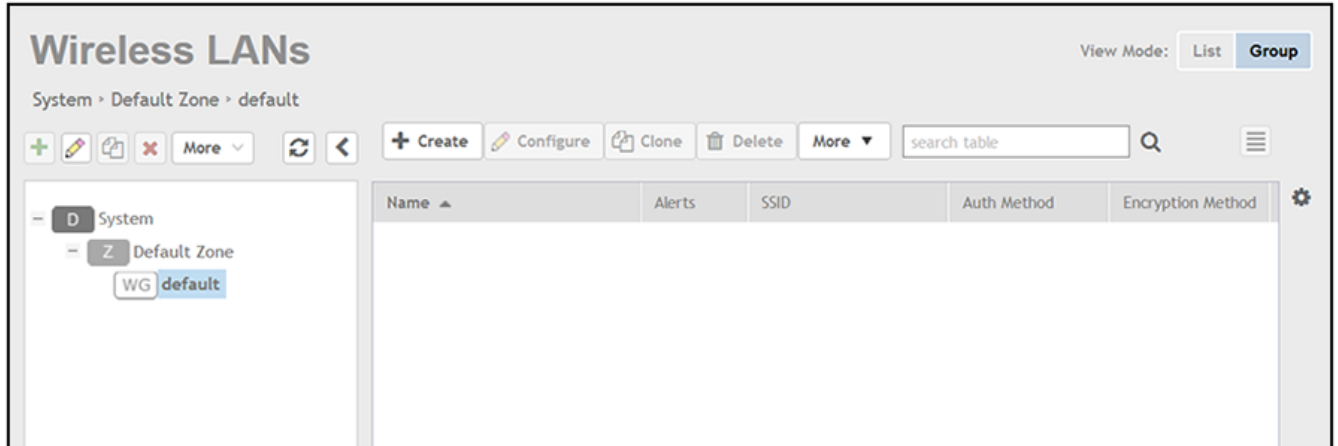
1. Log in to your Ruckus SmartZone controller.

Configuring a PEAP WLAN on a Ruckus SmartZone Controller

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

The following screen appears:

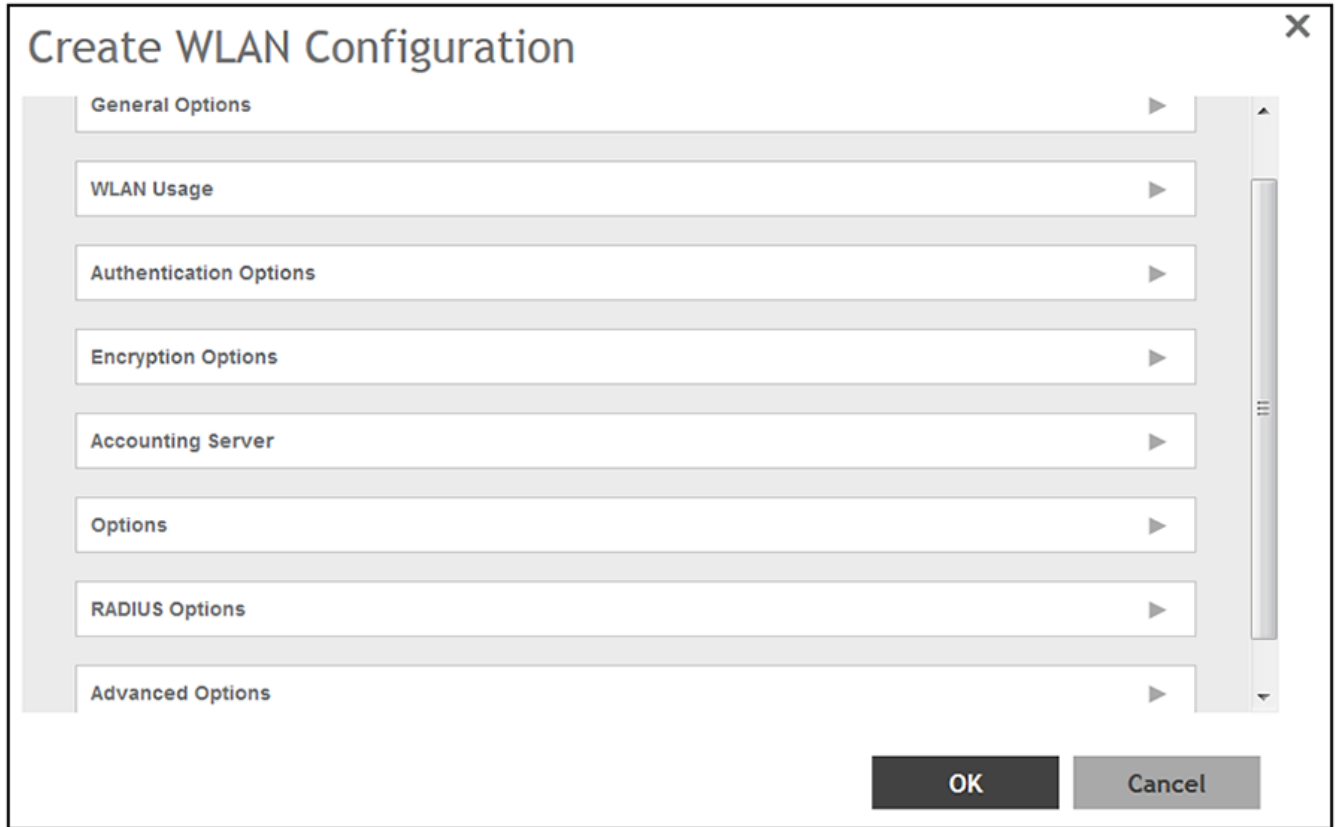
FIGURE 10 Wireless LANs Screen



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

General Options

* Name:

* SSID:

Description:

* Zone:

* WLAN Group:

- 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

WLAN Usage

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

Authentication 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 8 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
(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:

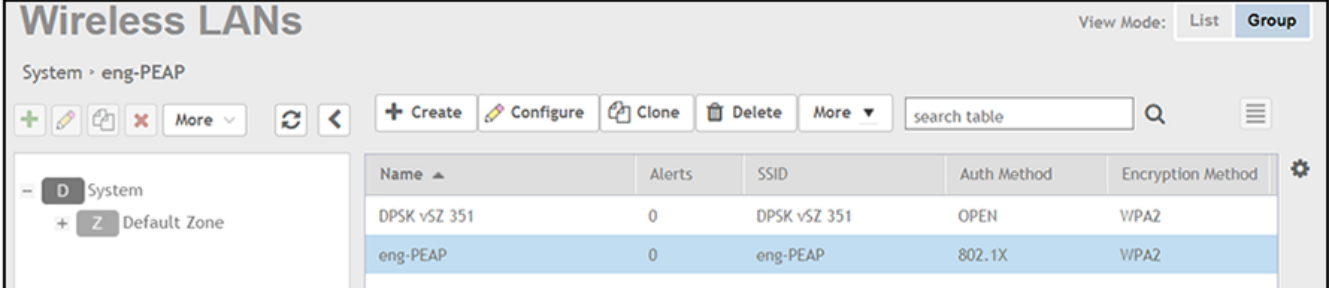
- NAS ID: WLAN BSSID AP MAC User-defined: [text box]
- Delimiter: Dash Colon
- NAS Request Timeout: [3] Seconds
- NAS Max Number of Retries: [2] Times
- NAS Reconnect Primary: [5] Minute (1-60)
- Called STA ID: WLAN BSSID AP MAC None AP GROUP
- NAS IP: Disabled SZ Control IP User-defined: [text box]

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



Name	Alerts	SSID	Auth Method	Encryption Method
DPSK vSZ 351	0	DPSK vSZ 351	OPEN	WPA2
eng-PEAP	0	eng-PEAP	802.1X	WPA2

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 19.

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 22
- [Configuring Cloudpath to Communicate with the External RADIUS server](#) on page 24
- [Testing the PEAP User Experience](#) on page 26
- [Troubleshooting Tips](#) on page 28

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

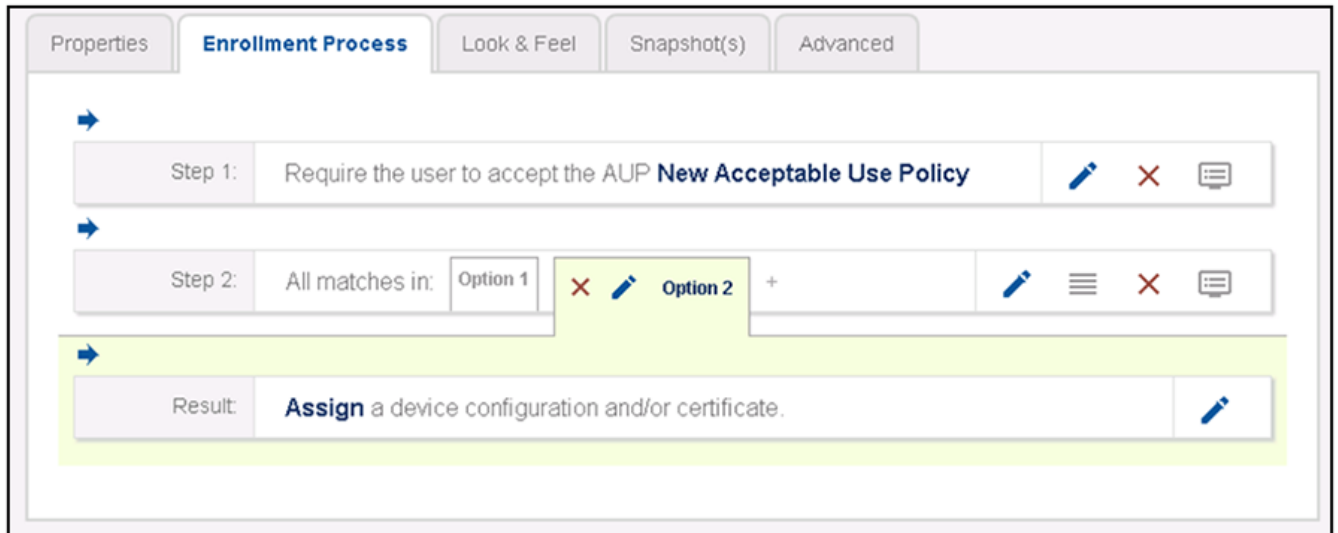
1. Log in to the Cloudpath user interface.
2. Go to **Configuration > Workflows**.

Configuring PEAP on Cloudpath to Integrate with the Ruckus Controller

Adding a PEAP Branch to Your Workflow

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

Display Title
This is the Display Text field, which may contain multiple lines of text to describe this option.

Short Name: PEAP

Display Title: PEAP

Display Text:

Enabled:

Icon File: Default: Using default file. [↓](#)

Upload: No file chosen

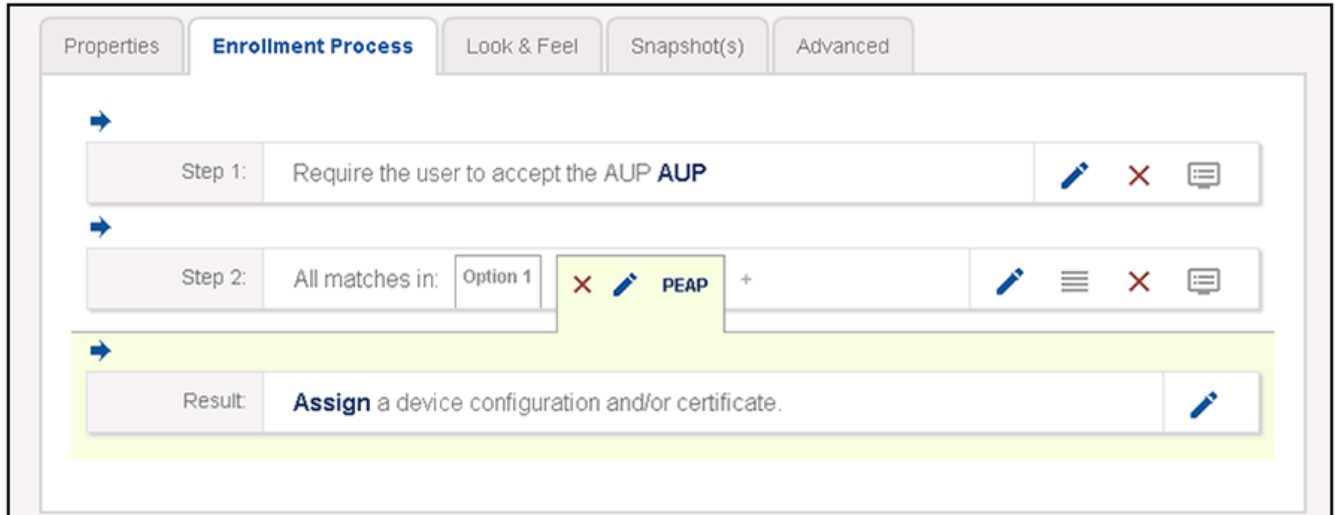
Enter a Short Name and Display Title, and, optionally, Display Text, then click **Save**.

Configuring PEAP on Cloudpath to Integrate with the Ruckus Controller

Adding a PEAP Device Configuration to Your Workflow

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

Which device configuration should be used?

- An existing device configuration.**
Configure the user using an existing configuration.
- A new device configuration.**
Configure the user using a new configuration.
- None.**
Do not configure the user.

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

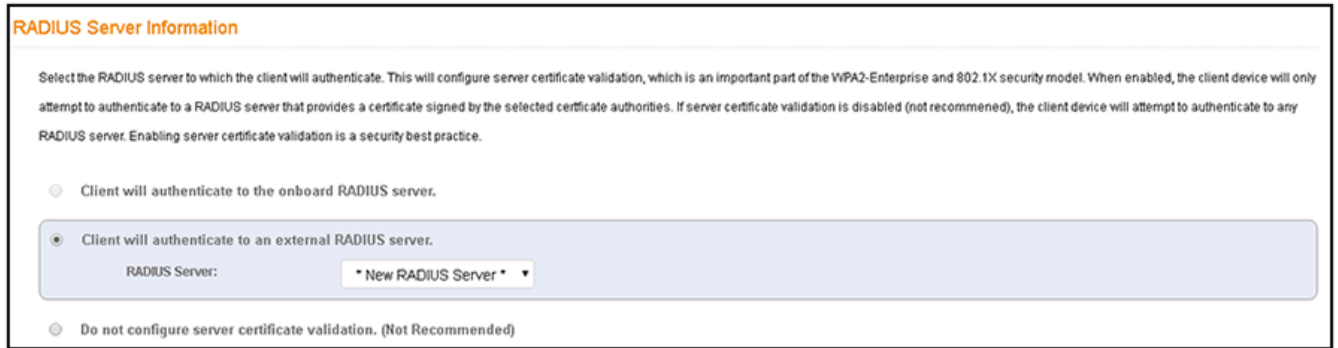
- The Wireless Connections button must be selected.
- SSID: This name must match the PEAP SSID exactly as you configured it on the controller:
 - For a Ruckus ZoneDirector controller, it is the name configured in [Figure 4](#) on page 11.
 - For a Ruckus SmartZone controller, it is the name configured in [Figure 12](#) on page 16.
- 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:

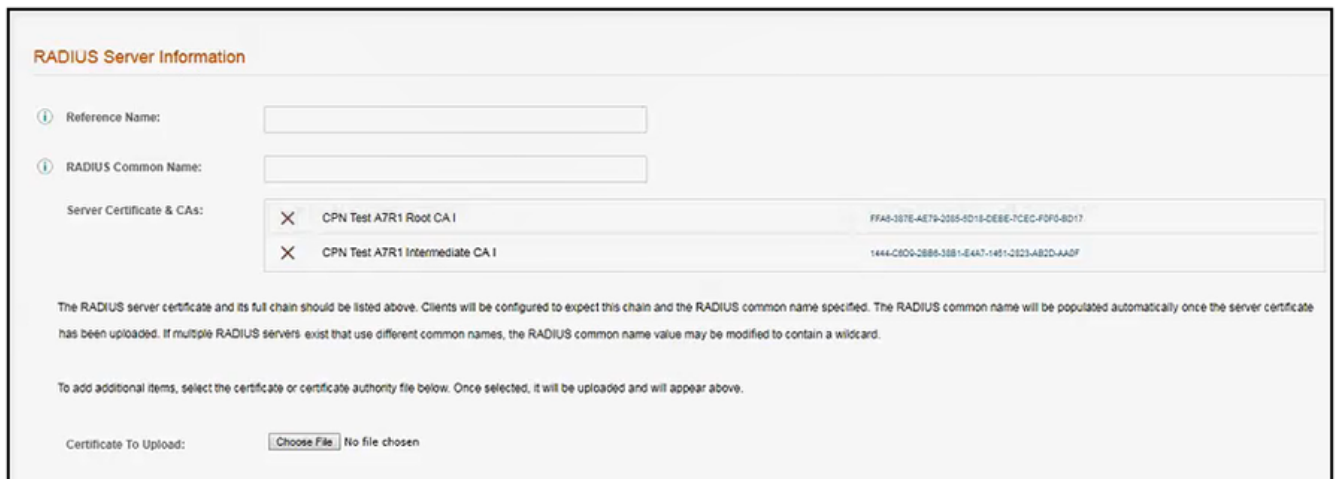
FIGURE 26 RADIUS Server Information



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

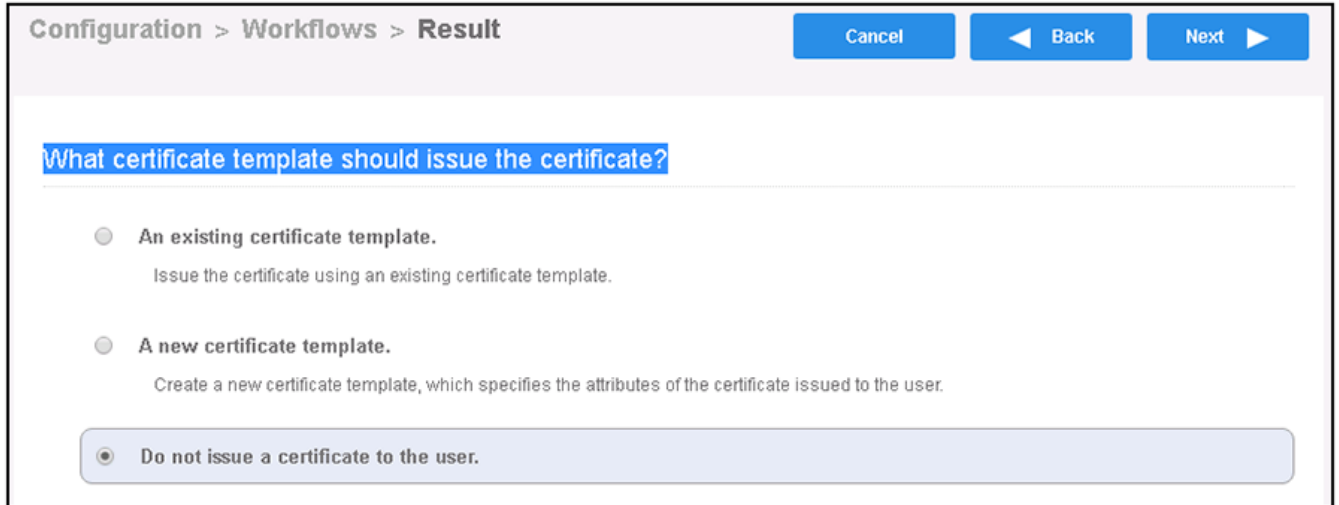


The Reference Name is an internal name (typically a name for the external RADIUS server) and is not obtained from the certificate, but the RADIUS Common Name is obtained from the certificate. Both these fields can be left blank if you wish. Click **Next**.

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

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

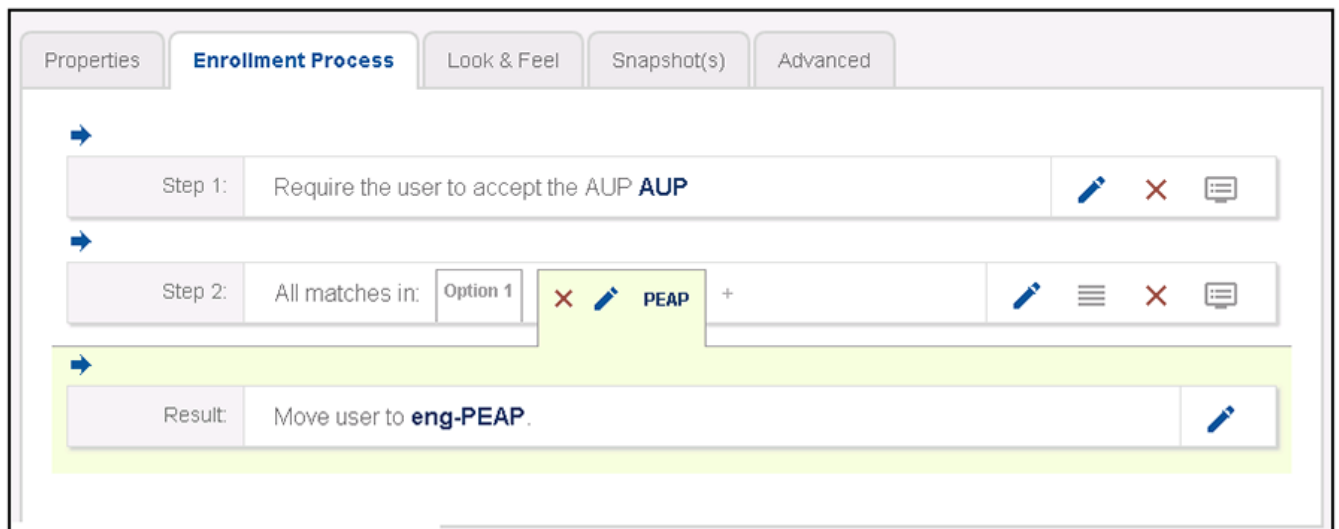
FIGURE 28 What certificate template should issue the certificate?



Click **Next**.

- 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:

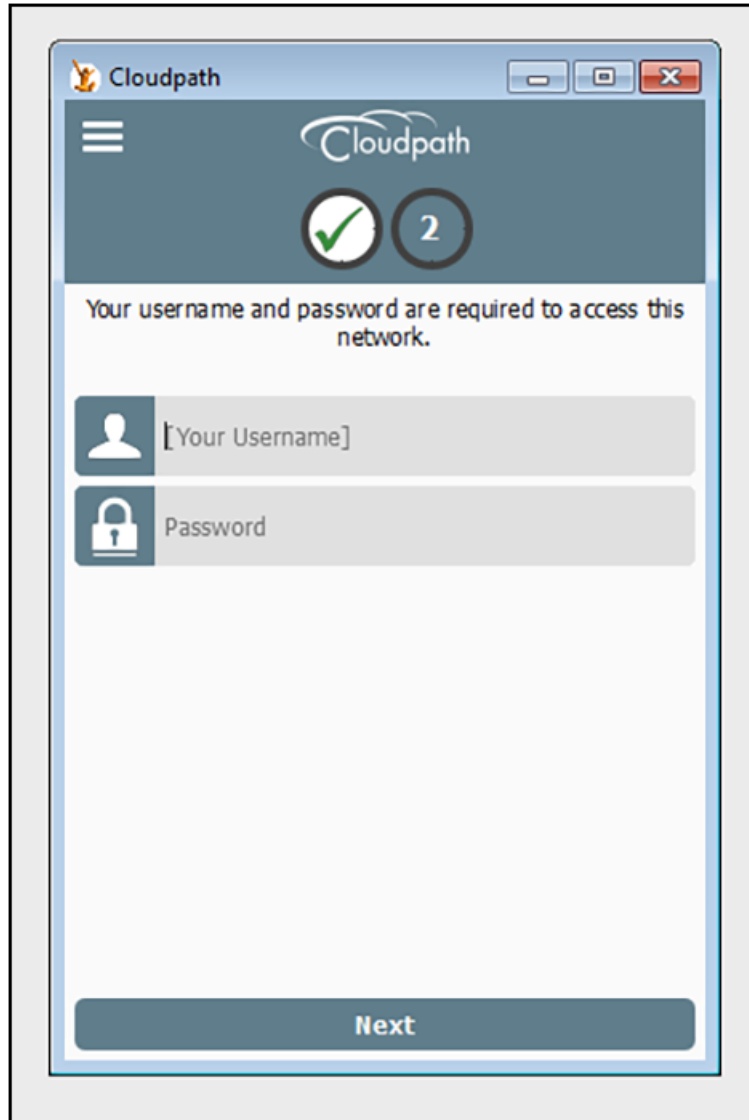
FIGURE 30 Testing the Workflow - PEAP Branch



4. Follow any prompts to continue.

5. The user is presented with the following screen 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.



© 2018 ARRIS Enterprises, LLC. All rights reserved.
350 West Java Dr. Sunnyvale, CA 94089. USA
www.ruckuswireless.com