

Ruckus ICX Flexible Authentication with Cloudpath ES 5.2 Deployment Guide

Supporting FastIron 08.0.80

Copyright, Trademark and Proprietary Rights Information

© 2019 ARRIS Enterprises LLC. 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 ARRIS International plc and/or its affiliates ("ARRIS"). ARRIS reserves the right to revise or change this content from time to time without obligation on the part of ARRIS 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, ARRIS 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. ARRIS 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. ARRIS 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 ARRIS 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 ARRIS, ARRIS 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 ARRIS 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, Ruckus, Ruckus Wireless, Ruckus Networks, Ruckus logo, the Big Dog design, BeamFlex, ChannelFly, Edgellon, FastIron, HyperEdge, ICX, IronPoint, OPENG, SmartCell, Unleashed, Xclaim, ZoneFlex are trademarks of ARRIS International plc and/or its affiliates. Wi-Fi Alliance, Wi-Fi, the Wi-Fi logo, the Wi-Fi CERTIFIED logo, Wi-Fi Protected Access (WPA), the Wi-Fi Protected Setup logo, and WMM are registered trademarks of Wi-Fi Alliance. Wi-Fi Protected Setup™, Wi-Fi Multimedia™, and WPA2™ are trademarks of Wi-Fi Alliance. All other trademarks are the property of their respective owners.

Contents

Preface	5
Introduction.....	5
Purpose of This Document.....	5
Audience.....	6
Related Documents.....	6
Document History.....	6
Overview	7
802.1X Authentication.....	7
Message Exchange During Authentication.....	7
MAC Authentication.....	9
Flexible Authentication.....	9
How Flexible Authentication Works.....	9
Platform Support for Flexible Authentication.....	10
Web Authentication Configuration Considerations.....	11
Configuring Cloudpath for RADIUS, HTTP, and Clients.....	12
Use Case 1: Basic MAC Authentication of Headless and Unknown Devices	17
Cloudpath Configuration.....	19
Switch Configuration	26
Switch Show Commands and Syslog Information.....	27
Cloudpath Information.....	28
Use Case 2: Onboarding an 802.1X Wired Client Using Certificate-based Authentication	31
Cloudpath Configuration.....	33
Switch Configuration	35
Switch Show Commands and Syslog Information.....	36
Cloudpath Information.....	37
Use Case 3: Guest Internet Access Using External Captive Portal	43
Cloudpath Configuration.....	45
Switch Configuration	48
Switch Show Commands and Syslog Information.....	48
Cloudpath Information.....	49
Use Case 4: Authentication of an IP Phone and a PC on the Same Port Using Flexible Authentication	51
Cloudpath Configuration.....	52
Switch Configuration	57
Switch Show Commands and Syslog Information.....	58
Cloudpath Information.....	60
Summary	67
Troubleshooting	69
Cloudpath RADIUS Server.....	69
ICX Debugging.....	70
Commonly Used Show Commands.....	71
Commonly Used Debug Commands.....	71

Preface

- Introduction.....5
- Purpose of This Document.....5
- Audience.....6
- Related Documents.....6
- Document History.....6

Introduction

Ruckus ICX switches running FastIron software support Network Access Control features, including IEEE 802.1X, MAC authentication, and Web authentication. These authentication methods can be used to address various use cases in granting network access to users and devices.

The Flexible Authentication feature, or Flex Auth, provides the flexibility to use authentication methods such as 802.1X and MAC authentication. Both mechanisms can be used in a configurable sequence for additional flexibility, depending on the use case of authenticating a user or a device or a combination of both. This flexibility also helps to provide a common configuration set that can be used across all ports on a switch regardless of the clients connecting to it.

Flexible Authentication allows the network administrator to set the sequence of authentication methods to be attempted on a switch port. The Ruckus Flexible Authentication implementation allows each client connected to the same switch port to have a different network policy (such as a dynamic VLAN or ingress IPv4 ACL). This implementation is achieved by using MAC-based VLANs that allow the creation of VLANs based on MAC addresses instead of the traditional method of port membership.

Web authentication is a sought-after authentication method opted for by various market segments, such as hospitality, enterprises, higher education, and so on. Web authentication can be used in conjunction with Flexible Authentication (a combination of IEEE 802.1X authentication and MAC authentication) or as a standalone authentication mechanism. When a guest user attempts to access a web page for the first time, the user is redirected to a web login page to enter credentials and confirm identity. Upon successful authentication, the user is directed to the requested web page.

With the growing market trend toward Bring Your Own Devices (BYOD) such as mobile devices, laptops, and so on, it is essential for companies to address client onboarding in as seamless a way as possible. Ruckus Cloudpath provides best-in-class service for client onboarding in conjunction with Ruckus ICX switches.

Purpose of This Document

The purpose of this deployment guide is to provide an understanding of Flexible Authentication and the steps required to successfully configure and deploy a strong set of authentication schemes suitable for your network. This guide describes the following use cases:

- Basic MAC authentication of headless and unknown devices
- Onboarding an 802.1X wired client using certificate-based authentication
- Guest Internet access using the external captive portal
- Authentication of an IP phone and a PC on the same port using Flexible Authentication

Audience

This document can be used by technical marketing engineers, system engineers, technical assistance center engineers, and customers to deploy a Flexible Authentication scheme for a network.

Related Documents

- *Ruckus FastIron Security Configuration Guide, 08.0.80*
<https://support.ruckuswireless.com/documents/2368-fastiron-08-0-80-ga-security-configuration-guide>
- Cloudpath
<https://www.ruckuswireless.com/products/smart-wireless-services/cloudpath>
- *Cloudpath Deployment Guide (Supporting Software Release 5.2)*
https://support.ruckuswireless.com/documents/2006-cp_es-5-2-ga-deployment-guide
- Cloudpath Administrative Console
<https://xpc.cloudpath.net/login.php>
- Cloudpath OVA Download
https://xpc.cloudpath.net/view_ova_download.php
- *Cloudpath Quick Start Guide*
https://xpc.cloudpath.net/documents/ES_QuickStartGuide.pdf
- IEEE 802.1X-2004
<http://www.ieee802.org/1/pages/802.1x-2004.html>
- PPP Extensible Authentication Protocol (EAP)
<https://tools.ietf.org/html/rfc2284>
- Remote Authentication Dial In User Service (RADIUS)
<https://tools.ietf.org/html/rfc2865>
- RADIUS Extensions
<https://tools.ietf.org/html/rfc2869>
- Dynamic Authorization Extensions to RADIUS
<https://tools.ietf.org/html/rfc3576>

Document History

Date	Part Number	Description
June 8, 2017	53-1005026-01	Initial release.
June 15, 2017	53-1005026-02	Corrections to command examples.
October 10, 2018	53-1005026-03	Updates to reflect changes to Cloudpath ES 5.2.
February 5, 2019	53-1005026-04	Addition of Web authentication configuration considerations and corrections to command examples. Addition of troubleshooting and ICX debugging information.

Overview

- 802.1X Authentication..... 7
- MAC Authentication..... 9
- Flexible Authentication..... 9
- How Flexible Authentication Works..... 9
- Platform Support for Flexible Authentication..... 10
- Configuring Cloudpath for RADIUS, HTTP, and Clients..... 12

802.1X Authentication

The 802.1X-based authentication is a standards-based implementation, and it defines three types of device roles in a network:

- Client/Supplicant
- Authenticator
- Authentication Server

Client/Supplicant: The devices (for example, desktop, laptop, and IP phone) that seek to gain access to the network. Clients must be running software that supports the 802.1X standard. Clients can be directly connected to a port on the authenticator, or they can be connected by way of a hub.

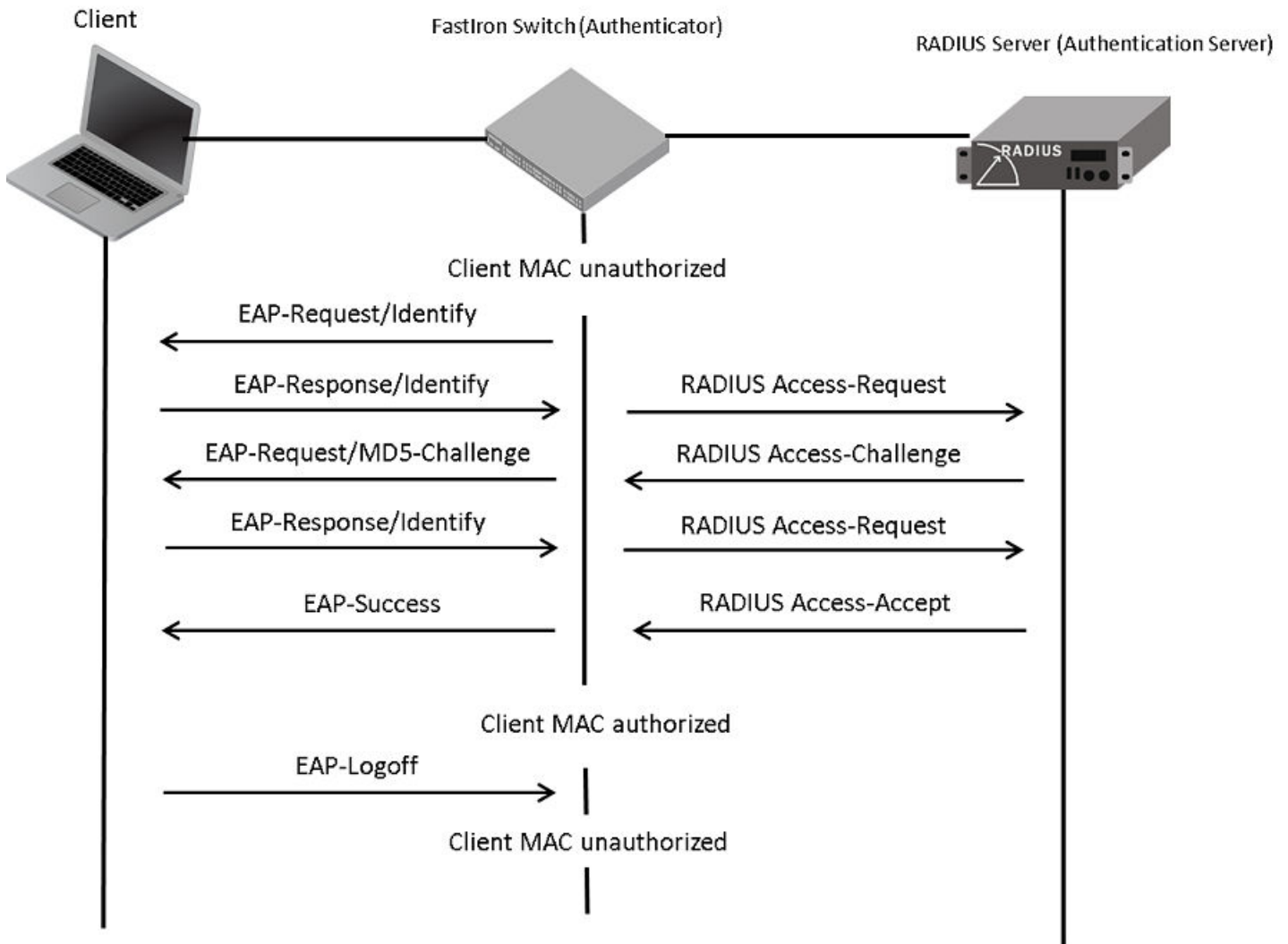
Authenticator: The device that controls access to the network. In an 802.1X configuration, the Ruckus device serves as the authenticator. The authenticator passes messages between the client and the authentication server. Based on the identity information supplied by the client and the authentication information supplied by the authentication server, the authenticator either grants or restricts network access to the client.

Authentication Server: The device that validates the client and specifies whether the client may access services on the device. Ruckus supports authentication servers that run RADIUS.

Message Exchange During Authentication

For communication between devices, 802.1X port security uses the Extensible Authentication Protocol (EAP), defined in RFC 2284. The 802.1X standard specifies a method for encapsulating EAP messages so that they can be carried over a LAN. This encapsulated form of EAP is known as EAP over LAN (EAPOL). During authentication, EAPOL messages are exchanged between the client/supplicant and the authenticator, and RADIUS messages are exchanged between the authenticator and the authentication server.

FIGURE 1 Message Exchange Between the Client, Authenticator, and Authentication Server



In this example, the authenticator (the ICX switch) initiates communication with an 802.1X-enabled client. When the client responds, it is prompted for a username (255 characters maximum) and a password. The authenticator passes this information to the authentication server, which determines whether the client can access services provided by the authenticator. If authentication succeeds, the MAC address of the client is authorized. In addition, the RADIUS server may include a network access policy, such as a dynamic VLAN or an ingress IPv4 ACL, in the Access-Accept message for this client. When the client logs off, the MAC address of the client becomes unauthorized again.

A client may fail to be authenticated in various scenarios. The following scenarios and options are available to place the client in various VLANs due to authentication failure:

- Guest VLAN
- Critical VLAN
- Restricted VLAN

Guest VLAN: The client is moved to a guest VLAN when it does not respond to the 802.1X requests for authentication. It is possible that the client does not have the 802.1X authenticator loaded and thus needs some way to access the network to

download the authenticator. The administrator can configure the guest VLAN with such access and other access methods, as required.

Critical VLAN: There may be scenarios in which the RADIUS server is not available and authentication fails. This can happen the first time the client is authenticating or when the client re-authenticates. In this situation, the administrator can decide to grant some or the same access as the original instead of blocking the access. This VLAN should be configured with the desired access levels.

Restricted VLAN: When authentication fails, the client can be moved into a restricted VLAN instead of failing completely. The administrator may decide to grant some access in this scenario instead of blocking the access. This VLAN should be configured with the desired access levels.

For more information about 802.1X authentication, refer to the *Ruckus FastIron Security Configuration Guide*.

MAC Authentication

MAC authentication is a mechanism by which incoming traffic originating from a specific MAC address is forwarded by the Ruckus switch only if a RADIUS server successfully authenticates the source MAC address. The MAC address itself is used as the username and password for RADIUS authentication; the user does not provide a specific username and password to gain access to the network. If RADIUS authentication for that MAC address succeeds, traffic from that MAC address is forwarded.

If the RADIUS server cannot validate the device's MAC address, it is considered an authentication failure, and a specified authentication-failure action can be taken. The format of the MAC address sent to the RADIUS server is configurable by way of the CLI. MAC authentication supports the use of a critical VLAN and a restricted VLAN, as described in [802.1X Authentication](#) on page 7.

For more information about MAC authentication, refer to the *Ruckus FastIron Security Configuration Guide*.

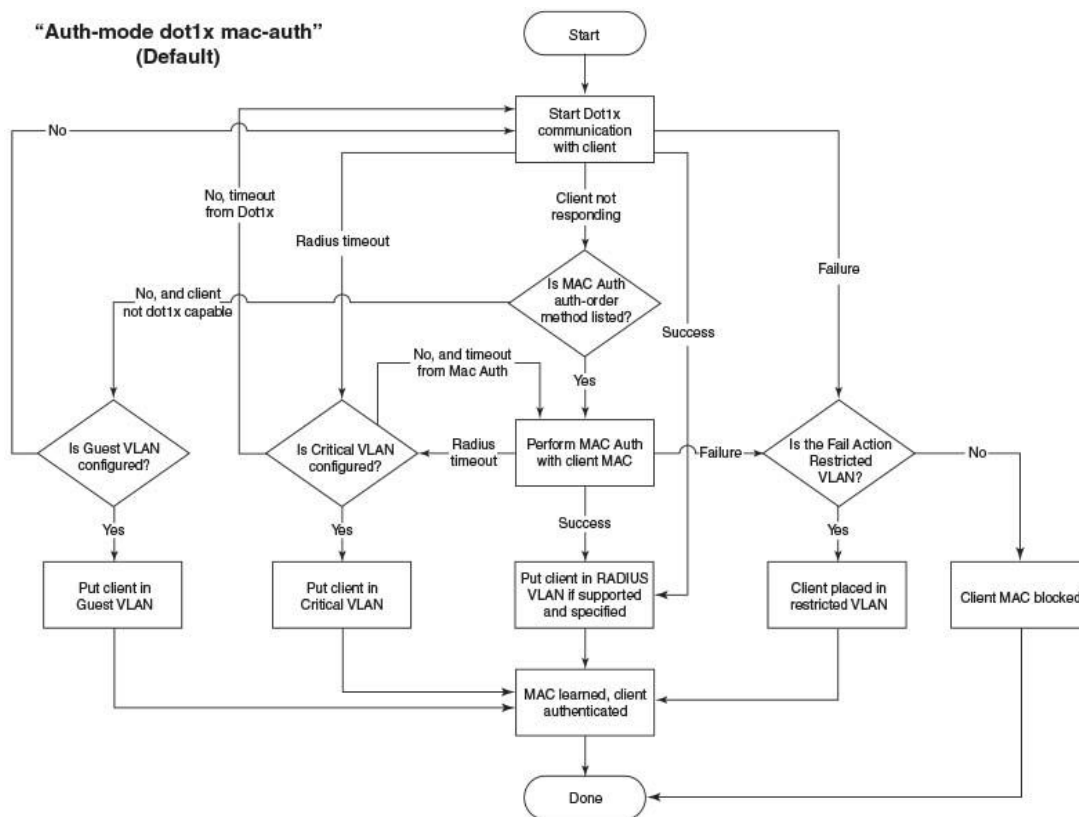
Flexible Authentication

Flexible Authentication allows the network administrator to set the sequence of the authentication methods to be attempted on a switch port. Flexible Authentication supports two methods: 802.1X authentication and MAC authentication. By default the sequence is set to 802.1X followed by MAC authentication.

How Flexible Authentication Works

The following flowchart explains how Flexible Authentication is implemented in FastIron. 802.1X is attempted first. If the client is not 802.1X-capable, MAC authentication is attempted.

FIGURE 2 Default Sequence: 802.1X Followed by MAC Authentication



Platform Support for Flexible Authentication

FastIron 08.0.80 supports Cloudpath with the following platforms:

- ICX 7150
- ICX 7250
- ICX 7450
- ICX 7650
- ICX 7750

ATTENTION

This guide is written based on the Layer 2 switch image. It is the responsibility of the network administrator to ensure the Layer 3 uplink port connectivity to reach the Cloudpath server. Administrators using the Layer 3 router image for their deployments must configure the respective "interface ve" configuration and IP address.

Web Authentication Configuration Considerations

Web authentication is modeled after other RADIUS-based authentication methods currently available on Ruckus edge switches. However, Web authentication requires a Layer 3 protocol (TCP/IP) between the host and the authenticator. Therefore, to implement Web authentication, you must consider the following configuration and topology configuration requirements:

- Web authentication works only when both the HTTP and HTTPS servers are enabled on the device.
- Web authentication works only on the default HTTP or HTTPS port.
- The host must have an IP address prior to Web authentication. This IP address can be configured statically on the host; however, DHCP addressing is also supported.
- If you are using DHCP addressing, a DHCP server must be in the same broadcast domain as the host. This DHCP server does not have to be physically connected to the switch. Also, DHCP assist from a router may be used.
- Web authentication is not supported on a reserved VLAN.

The following consideration applies to Web authentication in the Layer 2 switch image:

- If the management VLAN and the Web authentication VLAN are in different IP networks, make sure there is at least one routing element in the network topology that can route between these IP networks.

The following considerations are required for Web authentication in the base Layer 3 and full Layer 3 images:

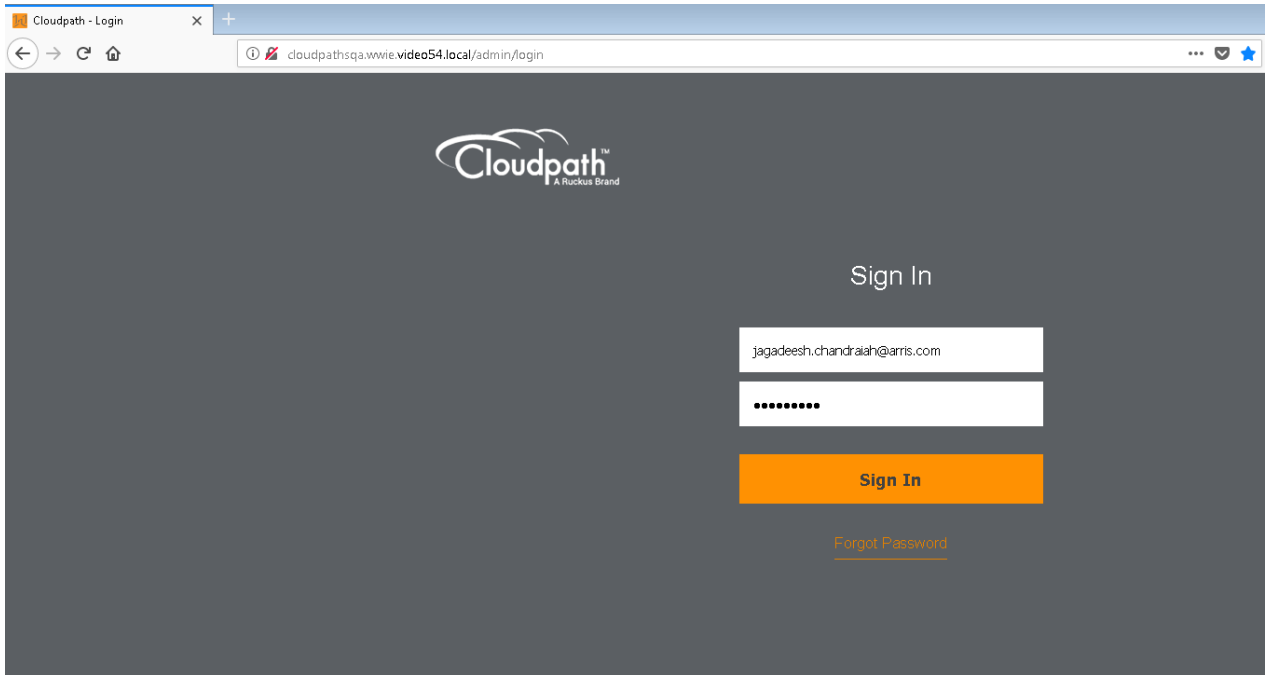
- Each Web authentication VLAN must have a virtual interface (VE).
- The VE must have at least one assigned IPv4 address.

When Web authentication is enabled on a VLAN, that VLAN becomes a Web authentication VLAN that acts in the following ways:

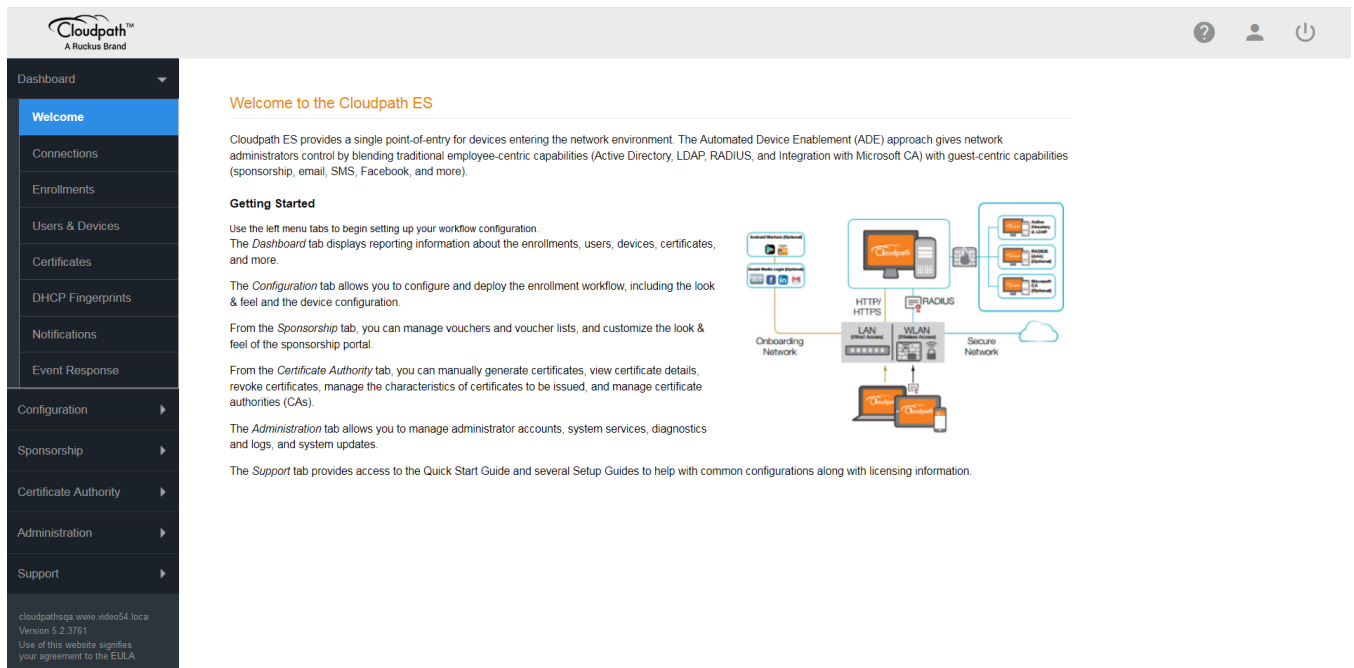
- Forwards traffic from authenticated hosts, just like a regular VLAN.
- Blocks traffic from unauthenticated hosts except from ARP, DHCP, DNS, HTTP, and HTTPS that are required to perform Web authentication.

Configuring Cloudpath for RADIUS, HTTP, and Clients

1. Log in to the Cloudpath server.



After login, the welcome page is displayed.



2. Navigate to **System Services** and check for the web server configuration. In this deployment guide, for testing purposes, HTTP is used. It is recommended to use HTTPS in a production environment.

The screenshot displays the Cloudpath Administration interface. On the left is a dark sidebar with a navigation menu. The main content area is titled "Administration > System Services" and shows the configuration for the "Web Server" service. The service status is "Running (19224)". The URL is "cloudpathsqa.wwie.video54.local:80". The "Using HTTPS" option is currently set to "No" with an "Enable" button. The port is "80" and the version is "5.2.3761". There are "Restart WWW" and "Restart App" buttons. Below this, the "Web Server Certificate" section shows "Public Key: Missing", "Private Key: Missing", and "Chain: Missing", with an "Upload WWW Certificate" button. The "Code Signing Certificate" section has a note and an "Upload" button. Other settings include "Restrict Admin UI To: [Unrestricted]", "Enroll Session Timeout: 1800 seconds", "SSL Cipher: HIGH:!aNULL:@STRENGTH:+DH", "SSL Protocol: all -SSLv2 -SSLv3", and "Strict Transport Security: Disabled".

Cloudpath™
A Ruckus Brand

Dashboard ▶
Configuration ▶
Sponsorship ▶
Certificate Authority ▶
Administration ▼
Administrators
Company Information
System Services
System Updates
Replication
Data Cleanup
Firewall Requirements
Support ▶

Administration > System Services

Service: Web Server

Web Server Status: ● Running (19224)

URL: cloudpathsqa.wwie.video54.local:80

Using HTTPS: No [Enable](#)

Ports: 80

Version: 5.2.3761

Actions: [Restart WWW](#) [Restart App](#)

Web Server Certificate

Public Key: Missing

Private Key: Missing

Chain: Missing

Actions: [Upload WWW Certificate](#)

Code Signing Certificate: The web server certificate will be used. Alternately, a code signing certificate may be uploaded. [Upload](#)

Restrict Admin UI To: [Unrestricted]

Enroll Session Timeout: 1800 seconds.

SSL Cipher: HIGH:!aNULL:@STRENGTH:+DH

SSL Protocol: all -SSLv2 -SSLv3

Strict Transport Security: Disabled

Overview

Configuring Cloudpath for RADIUS, HTTP, and Clients

3. Navigate to **Configuration > RADIUS Server > Status** and note the configuration of IP Address: cloudpathsqa.wwie.video54.local (Domain/IP address defined), Authentication Port 1812, Accounting Port 1813, and Shared Secret "Foundry1" (viewable by clicking the magnifying glass symbol) because these will be used in the switch configuration. The user should confirm that **Connection Tracking** and **COA** are enabled.

The screenshot shows the Cloudpath web interface. On the left is a navigation menu with the following items: Dashboard, Configuration, Workflows, Device Configurations, **RADIUS Server** (highlighted), Passpoint OSU, Authentication Servers, Firewalls & Web Filters, MAC Registrations, API Keys, Sponsorship, Certificate Authority, and Administration. The main content area is titled "Configuration > RADIUS Server" and has a sub-tab "Status" selected. Below the sub-tabs are sections for "RADIUS Server Status" and "RADIUS Server Settings".

RADIUS Server Status

The built-in RADIUS server is designed to handle RADIUS authentication for certificate-based (EAP-TLS) and MAC-based authentication (CHAP).

Status: ● Running (18294) [Restart](#) [Stop](#)

Connection Tracking: ● Active [Disable](#)

COA: ● Active [Disable](#)

RADIUS Server Settings

This system will need to be configured, using the IP, ports, and shared secret below, as the RADIUS server within your WLAN infrastructure or wired switches.

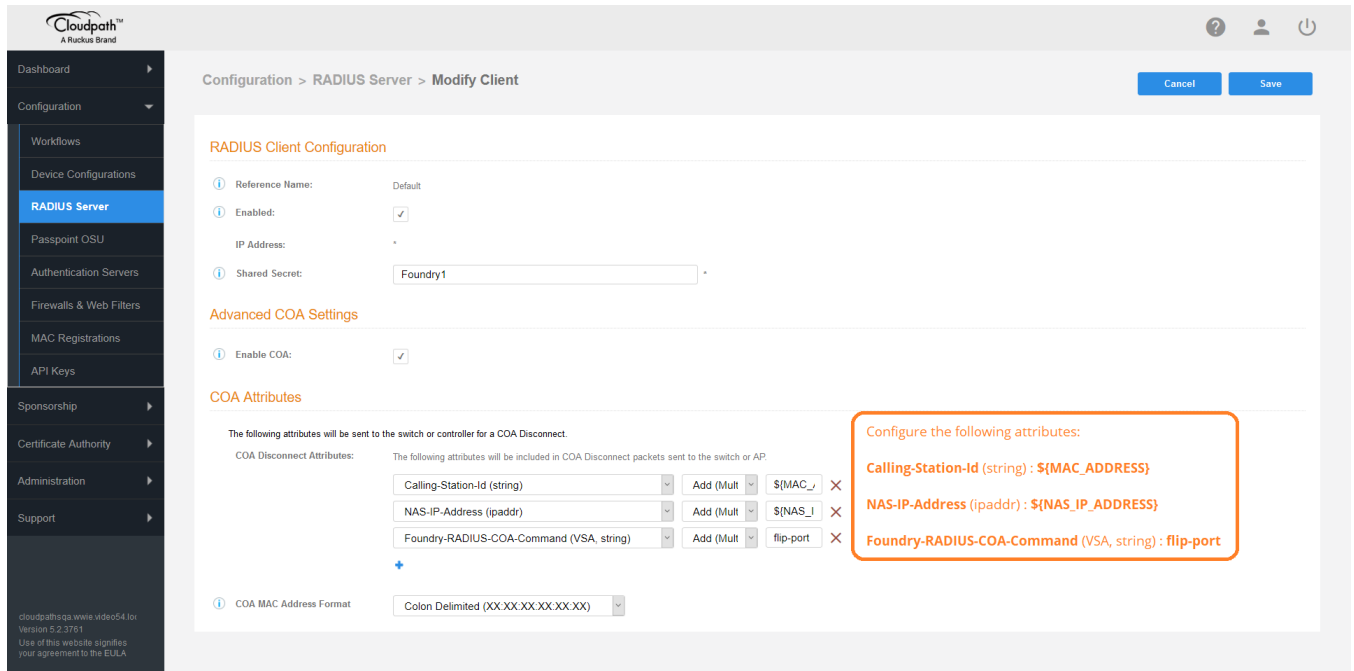
IP Address: cloudpathsqa.wwie.video54.local

Authentication Port: 1812

Accounting Port: 1813

Shared Secret: ***** [New Random](#) [Set](#)

4. Navigate to **Configuration > RADIUS Server > Clients** and edit the default client, add a secret key, and enable the COA option "flip-port" if required with the necessary attributes.



Refer to "Creating a Workflow From a Blank Slate" in the *Cloudpath Deployment Guide (Supporting Software Release 5.2)* at https://support.ruckuswireless.com/documents/2006-cp_es-5-2-ga-deployment-guide.

Use Case 1: Basic MAC Authentication of Headless and Unknown Devices

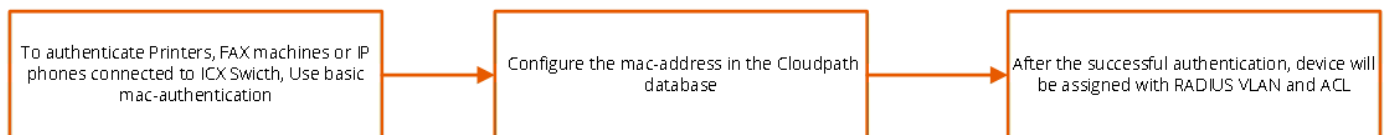
- Cloudpath Configuration..... 19
- Switch Configuration 26
- Switch Show Commands and Syslog Information..... 27
- Cloudpath Information..... 28

MAC authentication can be used to authenticate “headless” devices such as printers, wireless access points, and IP phones. This is achieved by manually adding the MAC addresses of the headless devices into the Cloudpath database. After successful authentication, the client is assigned to the predefined VLAN for the device type and any relevant ACLs are applied.

MAC authentication can also be used to authenticate user devices such as PCs, but for this application Ruckus Networks recommends the use of 802.1X as described in [Use Case 2: Onboarding an 802.1X Wired Client Using Certificate-based Authentication](#) on page 31.

The following example uses MAC authentication to authenticate an IP phone, but the same process can be used for any device.

FIGURE 3 Use Case 1 Workflow



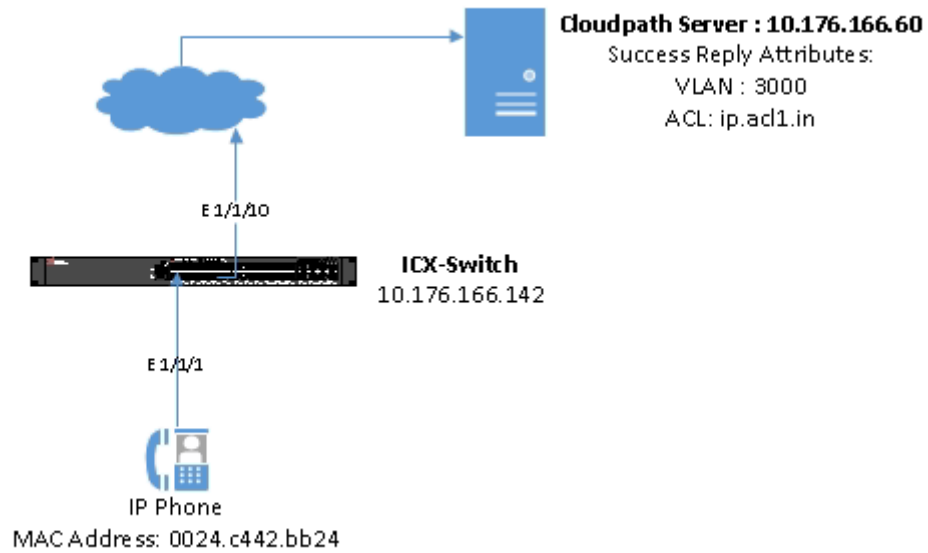
IP Phone

- The MAC address is 0024.c442.bb24.
- After authentication:
 - The IP phone should be placed in VLAN 3000.
 - Incoming traffic from the client should be filtered by ACL "acl1".

NOTE

The administrator can apply a policy such as a VLAN, an ACL, or both from the RADIUS server depending on the network design and its implementation.

FIGURE 4 Example of Assigning a Dynamic VLAN and ACL with MAC Authentication



The basic topology shows the basic components of a network topology. You will need:

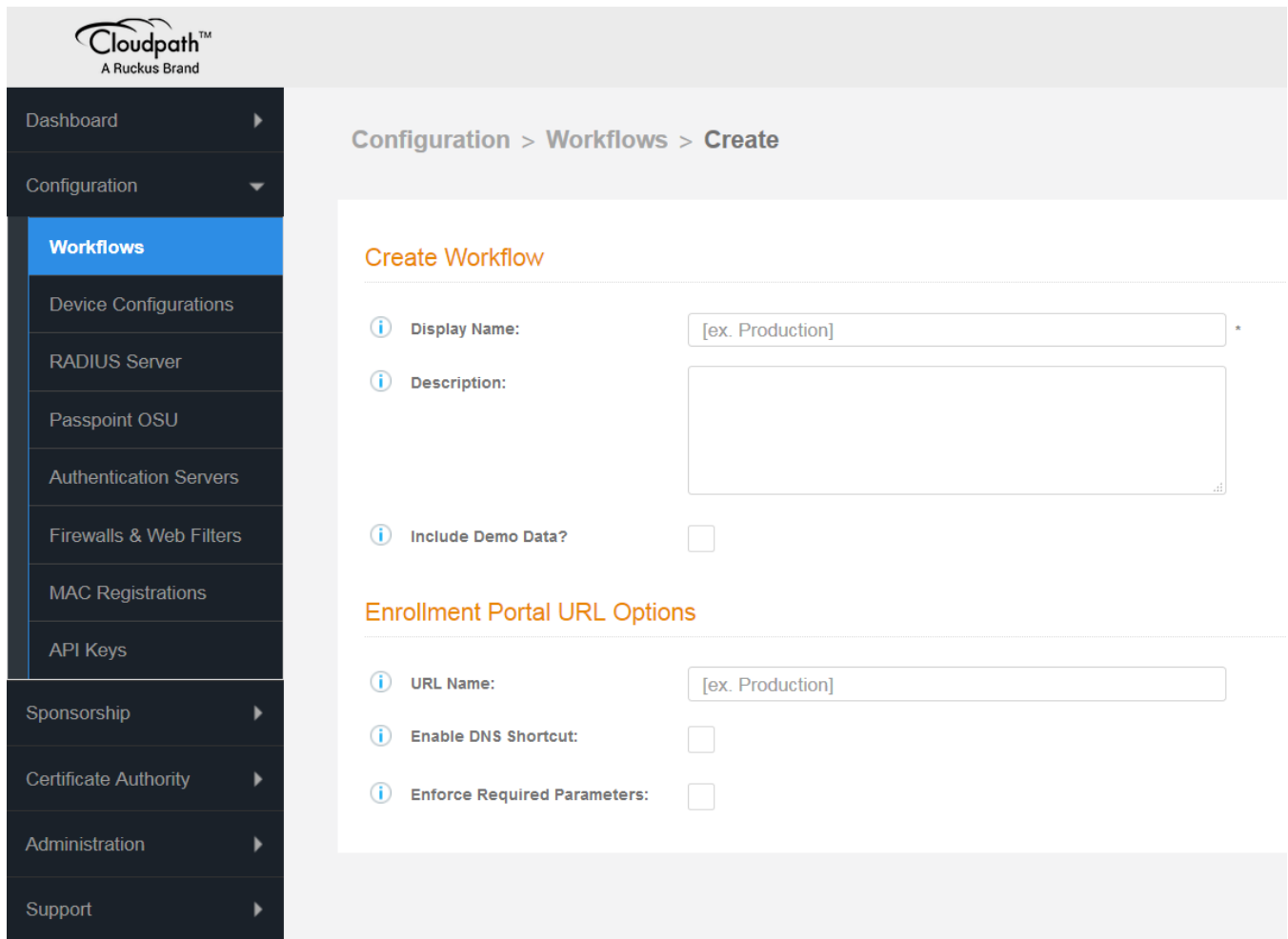
- A Ruckus FastIron switch
- A DHCP server, if dynamic IP addressing is to be used
- An IP phone, printer, or FAX machine
- A RADIUS server with some Trusted Source such as LDAP or Active Directory

NOTE

The Web server, RADIUS server, and DHCP server can all be the same server.

Cloudpath Configuration

1. Navigate to **Configuration > Workflows**. On the right side of the **Workflows** page, select **Add New Workflow**.
 - On the **Create Workflow** page, enter a name and description. Leave the **Include Demo Data?** check box unselected, and click **Save**.
 - On the blank workflow page, click **Get Started** to add your first workflow step.



Use Case 1: Basic MAC Authentication of Headless and Unknown Devices Cloudpath Configuration

A selection page opens that allows you to choose which type of step (workflow plug-in) to add to the enrollment workflow. Every time you add a step, the **Step Selection** page appears.

Configuration > Workflows > Insert Step

Cancel Next

Which Type Of Step Should Be Added?

- Display an Acceptable Use Policy (AUP).**
Displays a message to the user and requires that they signal their acceptance. This is normally used for an acceptable use policy (AUP) or end-user license agreement (EULA).
- Authenticate to a traditional authentication server.**
Prompts the user to authenticate to an Active Directory server, and LDAP server, RADIUS or a SAML server.
- Ask the user to name their device.**
Prompts the user to provide a name for the device, with the option to reuse or delete previously enrolled devices. This may suggest that old devices be removed or may limit the maximum number of concurrent devices.
- Ask the user about concurrent certificates.**
Prompts the user with information about previously issued certificates that are still valid. This may suggest that old certificates be removed or may limit the maximum number of concurrent certificates.
- Split users into different branches.**
Creates a branch or fork in the enrollment process. This can occur (1) visually by having the user make a selection or (2) it can occur automatically based on criteria associated with each option. For example, a user that selects "Guest" may be sent through a different process than a user that selects to enroll as an "Employee". Likewise, an Android device may be presented a different enrollment sequence than a Windows device.
- Authenticate to a third party.**
Prompts the user to authenticate via a variety of third-party sources. This includes internal OAuth servers as well as public OAuth servers, such as Facebook, LinkedIn, and Google.
- Authenticate using a voucher from a sponsor.**
Prompts the user to enter a voucher previously received from a sponsor. The sponsor generates the voucher via the Sponsor Portal, typically before the user arrives onsite.
- Perform out-of-band verification**
Sends the user a code via email or SMS to validate their identity.
- Request access from a sponsor.**
Prompts the user for a sponsor's email address and then notifies the sponsor. The sponsor can accept or reject the request via the Sponsor Portal.
- Register device for MAC-based authentication.**
Registers the MAC address of the device for MAC authentication by RADIUS. This is used for two primary use cases: (1) to authenticate the device on the current SSID via the WLAN captive portal or (2) to register a device, such as a gaming device, for a PSK-based SSID. In both cases, the MAC address will be captured and the device will be permitted access for a configurable period of time.
- Display a message.**
Displays a message to the user along with a single button to continue.
- Redirect the user.**
Redirects the user to a specified external URL. This may be used to authenticate the user to the captive portal of the onboarding SSID.
- Prompt the user for information.**
Displays a prompt screen with customizable data entry fields.
- Authenticate via a shared passphrase.**
Prompts the user for a passphrase and verifies it is correct. A shared passphrase is useful for controlling access to an enrollment process separate from, or in addition to, user credentials.
- Generate a Ruckus DPSK.**
Generates a DPSK via a Ruckus WLAN controller.
- Send a notification**
Generates a notification about the enrollment. Notification types include email, SMS, REST API, syslog and more. This step is invisible to the end-user.

2. After creating the new workflow, click the **Get Started** button to select the steps for the workflow.

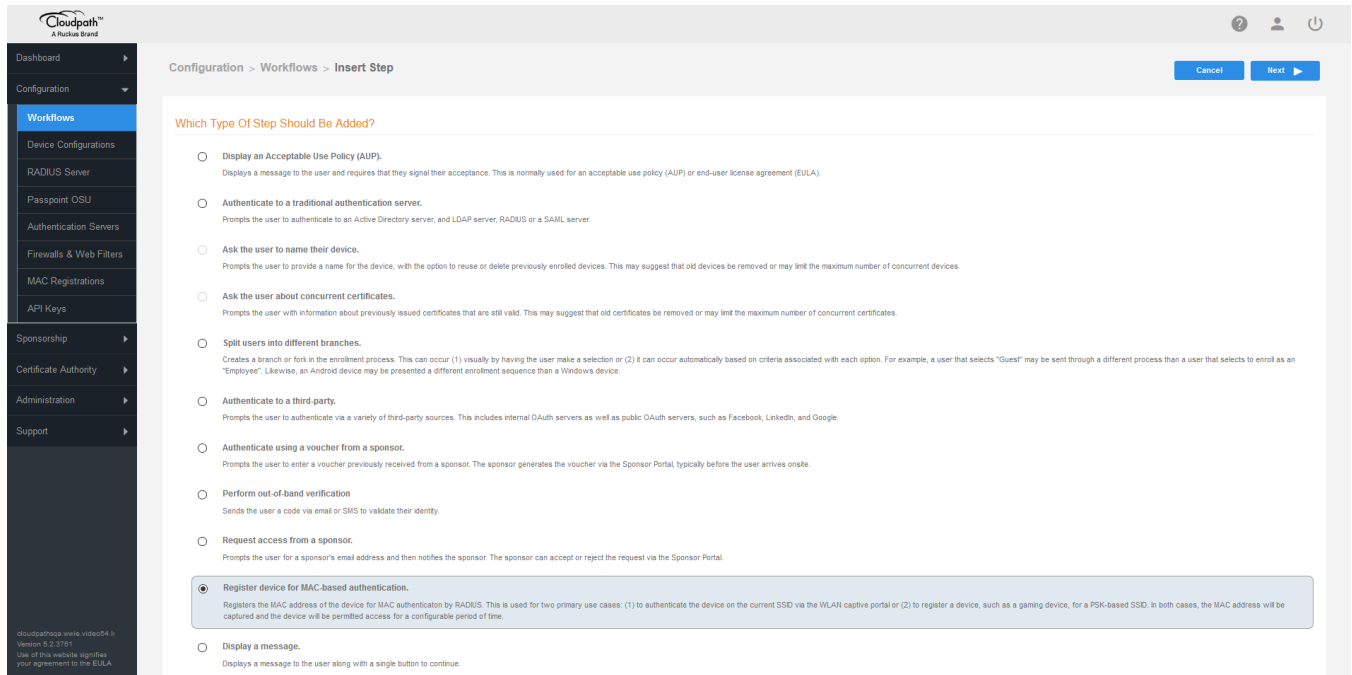
Properties Enrollment Process Look & Feel Snapshot(s) Advanced

Enrollment Process

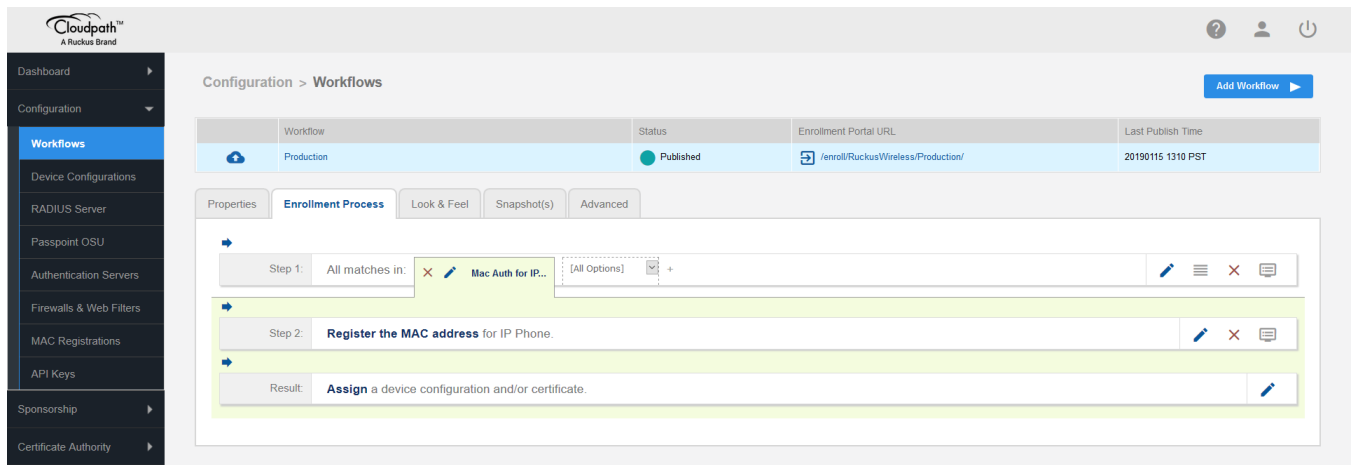
This is where we define the workflow the user goes through to get on the network. Typically, the first step is to add an Acceptable Use Policy, followed by an authentication to Active Directory, LDAP, or AAA. The last step is normally to configure and connect the user to the secure network.

Get Started

3. Select the appropriate steps required to configure the workflow.



The workflow for registering the MAC address is displayed.



Use Case 1: Basic MAC Authentication of Headless and Unknown Devices

Cloudpath Configuration

4. Modify the MAC registration by configuring the authentication success and failure reply attributes.

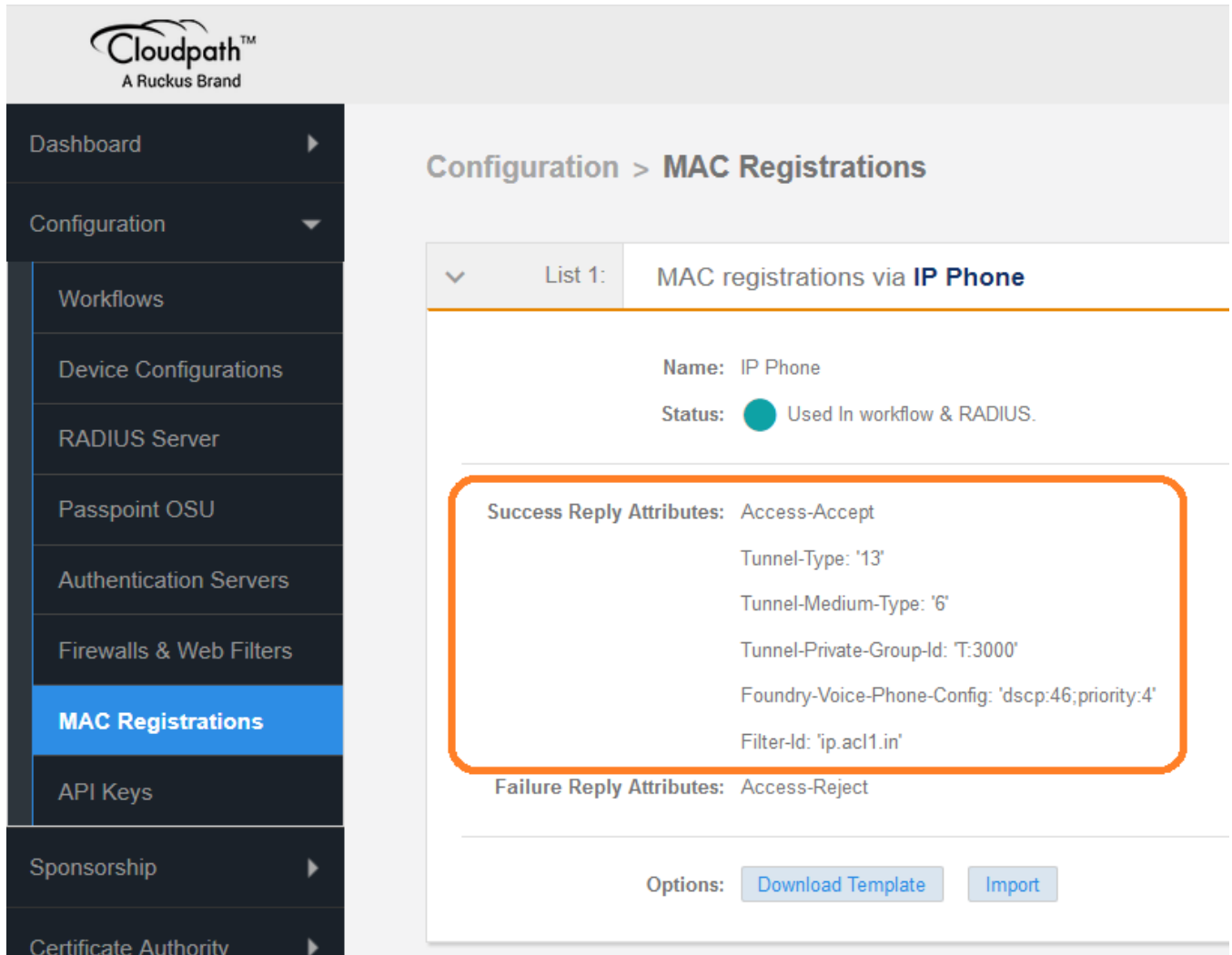
The screenshot shows the Cloudpath configuration interface for 'Modify MAC Registration'. The interface is divided into several sections:

- Modify MAC Registration:** Includes fields for 'Display Name' (IP Phone) and 'Description'.
- Registration Information:** Includes fields for 'SSID Regex' (*), 'Expiration Date Basis' (Years After), 'Offset' (1), and 'Behavior' (Prompt user when MAC is undetermined).
- Web Page Information:** Includes fields for 'Title' (Enter the MAC address of your device below), 'Prompt Text' (The MAC address must be in one of the following formats: AA:BB:CC:DD:EE:FF, AA-BB-CC-DD-EE-FF, or AABBCCDDEEFF), 'MAC Address Label' (MAC Address), 'Help Link Caption' ([ex. How Do I Find This?]), 'Help Link URL' ([ex. http://help.company.com/findMac]), 'Continue Button Label' (Continue >), and 'Invalid MAC Error' (MAC address specified is invalid. The MAC address must be).
- Authentication Attributes:** Includes 'Success Reply Attributes' and 'Failure Reply Attributes'. The 'Success Reply Attributes' section is highlighted with a red box and contains a table of attributes:

Attribute Name	Type	Add (Mult)	Value	Action
Tunnel-Type	(integer)	13	X	
Tunnel-Medium-Type	(integer)	6	X	
Tunnel-Private-Group-Id	(string)	T.3000	X	
Foundry-Voice-Phone-Config	(VSA, string)	dscp 46	X	
Filter-Id	(string)	ip.ac1.ir	X	

The 'Failure Reply Attributes' section is currently empty, with a note: 'No additional attributes currently exist.'

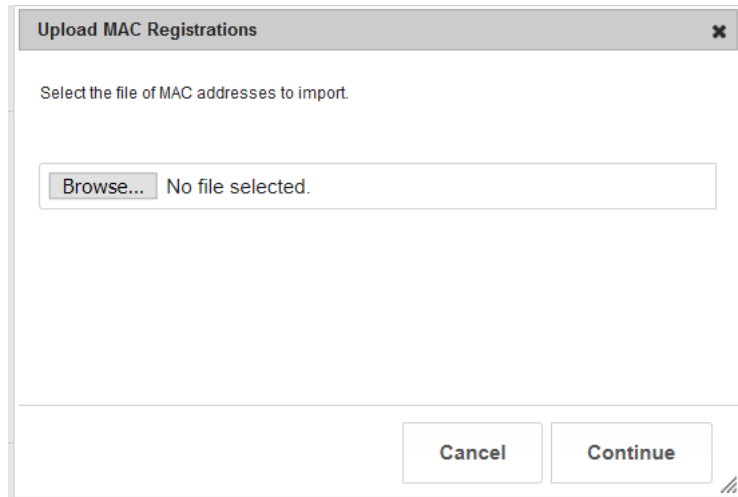
- Navigate to **Configuration > MAC Registrations** to view the configured success and failure attributes.



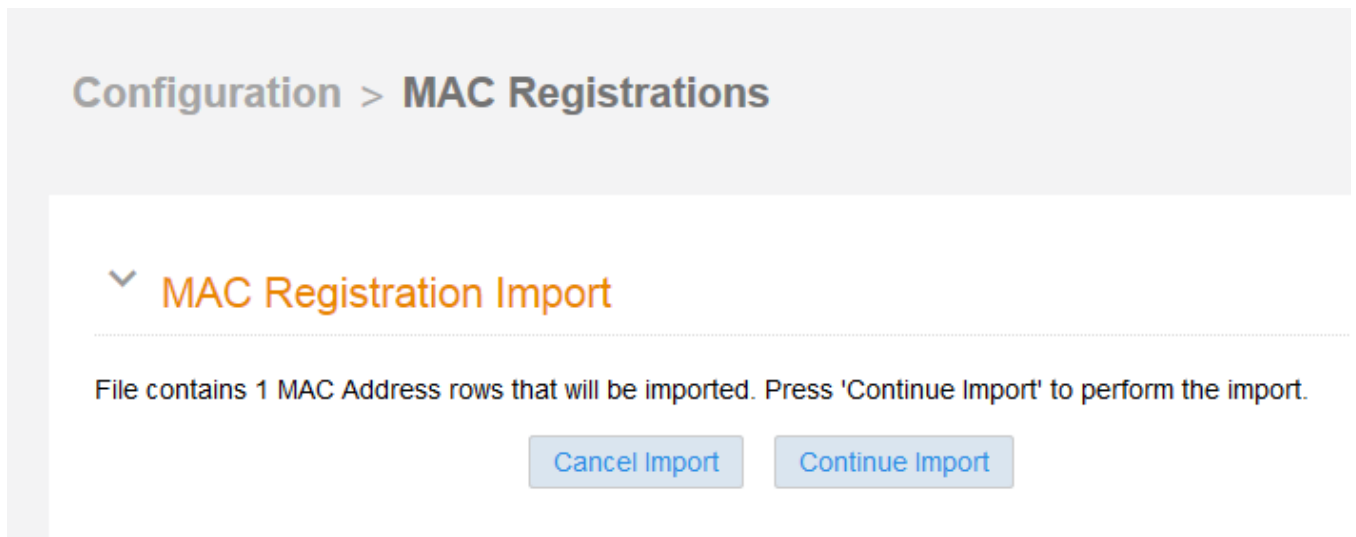
- For printers, FAX machines, and IP phones, register the MAC address manually. Navigate to **Configuration > MAC Registrations > Options**, click **Download Template**, and add the MAC addresses of the clients and the expiration dates for those clients.

A	B	C	D	E	F
MAC Address	Expiration Date	Username	Email	Device Name	Location
0024c442bb24	4/4/2020	0024c442bb24	jagadeesh.chandraiah@arris.com	IP-Phone-G06	Sunnyvale

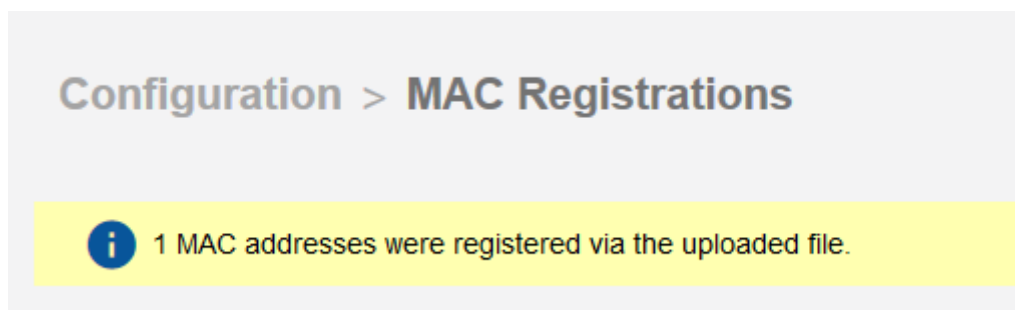
7. Import the updated template.



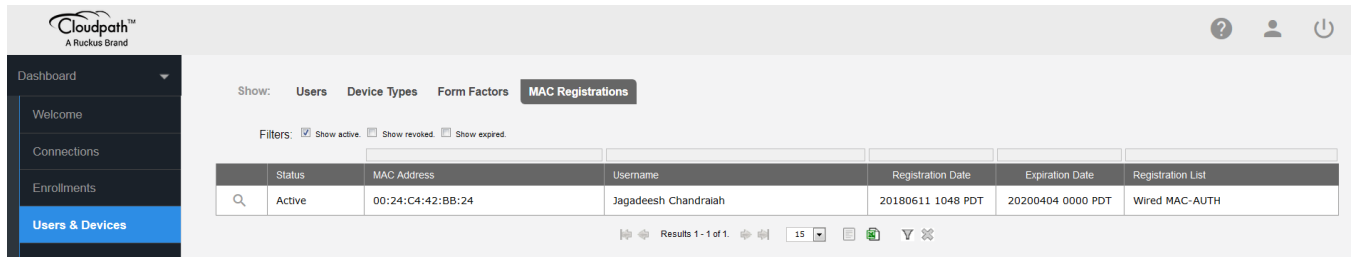
8. Click **Continue Import** to perform the import.



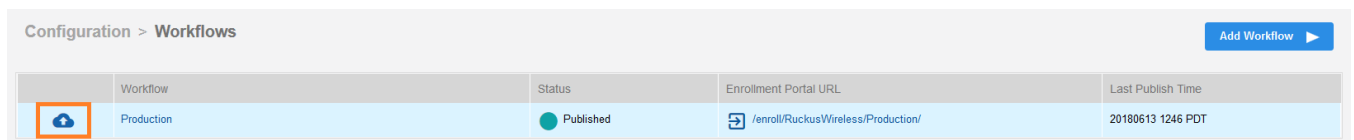
After uploading the imported template, the MAC addresses are registered.



9. Navigate to **Dashboard > Users & Devices > MAC Registrations** to verify the manually registered MAC address.



10. After allowing any changes in Cloudpath to take effect, navigate to **Configuration > Workflows** and click the cloud symbol to publish.



11. Create a new snapshot.

Create New Snapshot? ✕

⚠ Are you sure that you want to create and activate a new snapshot?

Wizard Version: ▼

The URL below will be used by end-users during enrollment. It is important that this URL is correct for communication from the end-user to the system. Also, if HTTPS, it is important that the web server certificate and DNS are properly configured. Incorrect setup of this URL may lead to 404 NOT FOUND errors during enrollment. If the end-user is accessing the system through a load balancer, this most likely should be the DNS handled by the load balancer.

URL: `http://cloudpathsqa.wwie.video54.local/enroll/RuckusWireless/Production/`

Remove oldest inactive snapshot if 5 exist.

Switch Configuration

```
!  
vlan 2 name AUTH-DEFAULT by port  
  tagged ethe 1/1/10  
  spanning-tree  
!  
vlan 100 name Management-NW by port  
  tagged ethe 1/1/10  
  untagged ethe 1/1/20  
  spanning-tree  
  management-vlan  
  default-gateway 10.176.166.1 1  
!  
vlan 3000 by port  
  tagged ethe 1/1/10  
!  
authentication  
  auth-default-vlan 2  
  mac-authentication enable
```

```

mac-authentication enable ethe 1/1/1
!
aaa authentication dot1x default radius
aaa authorization coa enable
aaa accounting dot1x default start-stop radius
aaa accounting mac-auth default start-stop radius
!
ip address 10.176.166.142/24
ip dns domain-list wwie.video54.local
ip dns server-address 10.176.4.10 10.176.4.11
!
radius-client coa host 10.176.166.60 key Foundryl
radius-server host 10.176.166.60 auth-port 1812 acct-port 1813 default key Foundryl dot1x mac-auth web-auth
radius-server accounting interim-updates
radius-server accounting interim-interval 5
!
web-management https
!
ip access-list extended acl1
 permit ip any any
!

```

Switch Show Commands and Syslog Information

```

ICX-Switch#
SYSLOG: <14> Jan 16 16:43:01 ICX-Switch System: Interface ethernet 1/1/1, state up
SYSLOG: <14> Jan 16 16:43:01 ICX-Switch STP: VLAN 4094 Port 1/1/1 STP State -> BLOCKING (DOT1wTransition)
SYSLOG: <14> Jan 16 16:43:05 ICX-Switch STP: VLAN 4094 Port 1/1/1 STP State -> LEARNING (DOT1wTransition)
SYSLOG: <14> Jan 16 16:43:05 ICX-Switch STP: VLAN 4094 Port 1/1/1 STP State -> FORWARDING (DOT1wTransition)
SYSLOG: <13> Jan 16 16:43:06 ICX-Switch MACAUTH: port 1/1/1 mac 0024.c442.bb24 vlan 2: Session is created
Warning: port 1/1/1 does not belong to vlan 3000
SYSLOG: <10> Jan 16 16:43:06 ICX-Switch MACAUTH: RADIUS server 10.176.166.60 Accepted for 0024.c442.bb24 with
(ST:3020399 V4I:ac11 V4O: V6I:V6O: T:3000 )
SYSLOG: <13> Jan 16 16:43:06 ICX-Switch MACAUTH: Port 1/1/1 Mac 0024.c442.bb24 - received AAA-ACCEPT
SYSLOG: <13> Jan 16 16:43:06 ICX-Switch FLEXAUTH: Port 1/1/1 is added into Dynamic Vlan 3000 as tagged member
SYSLOG: <13> Jan 16 16:43:06 ICX-Switch MACAUTH: port 1/1/1 mac 0024.c442.bb24 vlan 3000: Session is created

```

```

ICX-Switch#
ICX-Switch# show authentication sessions all
-----

```

Port	MAC Addr	IP (v4/v6) Addr	User Name	VLAN	Auth Method	Auth State	ACL	Session Time	Age	PAE State
1/1/1	0024.c442.bb24	10.176.167.237	Jagadeesh Chandra	3000	MAUTH	Permit	Yes	32	Ena	N/A

```

ICX-Switch#
ICX-Switch# show vlan 3000
Total PORT-VLAN entries: 12
Maximum PORT-VLAN entries: 1024

```

```

Legend: [Stk=Stack-Id, S=Slot]

PORT-VLAN 3000, Name VOICE_VLAN, Priority level0, in single spanning tree domain
  Untagged Ports: None
  Tagged Ports: (U1/M1) 1 10
  Mac-Vlan Ports: None
  Monitoring: Disabled

```

```

ICX-Switch#
ICX-Switch# show authentication acls all
-----

```

Port	MAC Address	V4 Ingress	V4 Egress	V6 Ingress	V6 Egress
1/1/1	0024.c442.bb24	ac11	-	-	-

```

ICX-Switch#
ICX-Switch# show lldp neighbors detail ports e 1/1/1
Local port: 1/1/1
Neighbor: 0024.c442.bb24, TTL 174 seconds
+ Chassis ID (network address): 10.176.167.237
+ Port ID (locally assigned): 808464948
+ Time to live: 180 seconds

```

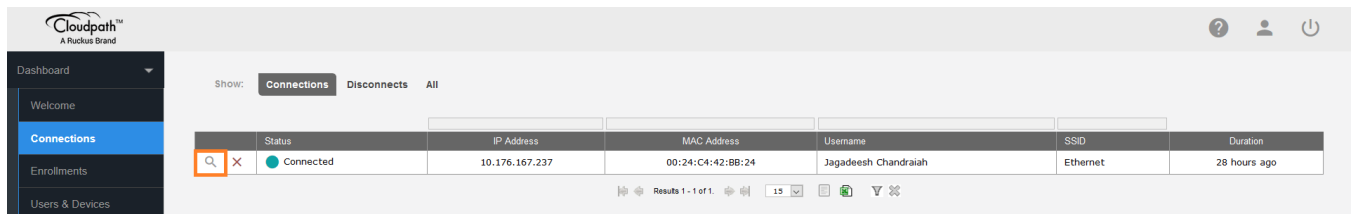
Use Case 1: Basic MAC Authentication of Headless and Unknown Devices

Cloudpath Information

```
+ Port description      : "SW PORT"
+ System name          : "SEP0024C442BB24.wwie.video54.local"
+ System description   : "Cisco IP Phone 7965G,V5, SCCP45.9-1-1SR1S"
+ System capabilities  : bridge, telephone
  Enabled capabilities: bridge, telephone
+ Management address (IPv4): 10.176.167.237
+ 802.3 MAC/PHY       : auto-negotiation enabled
  Advertised capabilities: fdxSPause, fdxBPause, 1000BaseX-FD, 1000BaseT-HD
  Operational MAU type  : 1000BaseT-FD
+ MED capabilities: capabilities, networkPolicy, extendedPD, inventory
  MED device type : Endpoint Class III
+ MED Network Policy
  Application Type : Voice
  Policy Flags     : Known Policy, Tagged
  VLAN ID         : 3000
  L2 Priority      : 5
  DSCP Value      : 46
+ MED Network Policy
  Application Type : Voice Signaling
  Policy Flags     : Known Policy, Tagged
  VLAN ID         : 3000
  L2 Priority      : 4
  DSCP Value      : 32
+ MED Extended Power via MDI
  Power Type      : PD device
  Power Source    : Unknown Power Source
  Power Priority   : Unknown
  Power Value     : 12.0 watts (PSE equivalent: 13190 mWatts)
+ MED Hardware revision : "5"
+ MED Firmware revision : "tnp65.8-3-1-21a.bin"
+ MED Software revision : "SCCP45.9-1-1SR1S"
+ MED Serial number     : "FCH13078LY5"
+ MED Manufacturer     : "Cisco Systems, Inc."
+ MED Model name       : "CP-7965G"
+ MED Asset ID         : ""
```

Cloudpath Information

1. Navigate to **Dashboard** and click **Connections** to verify the MAC authentication.






The screenshot shows the Cloudpath dashboard interface. On the left is a navigation sidebar with 'Connections' selected. The main area displays a table of connections. A search icon is visible in the top left of the table area. The table contains one entry with the following details:

Status	IP Address	MAC Address	Username	SSID	Duration
Connected	10.176.167.237	00:24:C4:42:BB:24	Jagadeesh Chandraiah	Ethernet	28 hours ago

At the bottom of the table, it shows 'Results 1 - 1 of 1' and a page size of '15'.

2. Click the magnifying glass symbol to get more information about the connection.

Connection Information

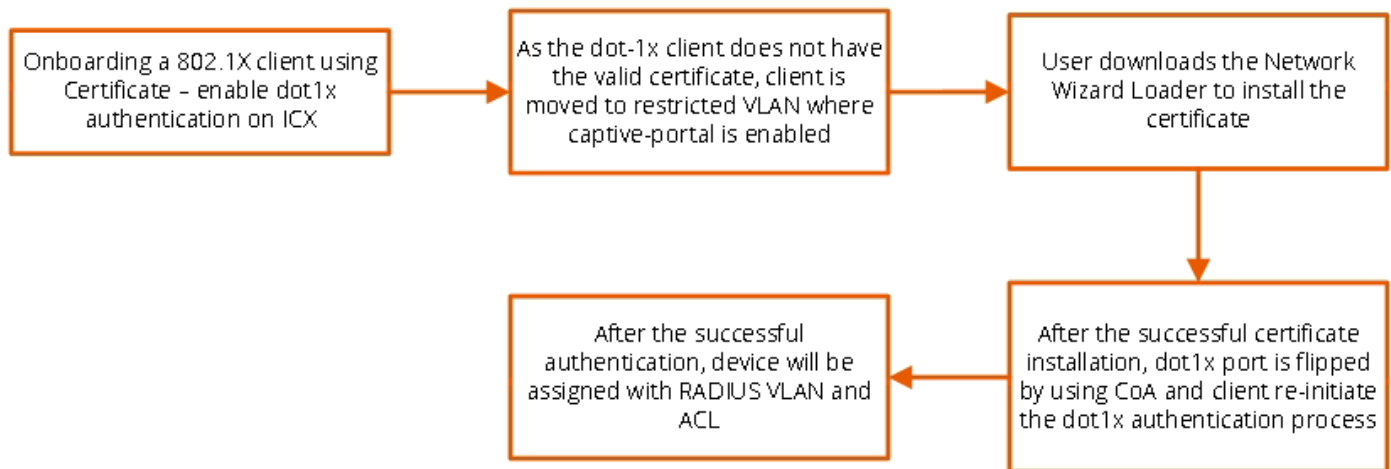
 Status:	 Connected
Username:	Jagadeesh Chandraiah
 IP Address:	10.176.167.237
MAC Address:	00:24:C4:42:BB:24
SSID:	Ethernet
Session Start Time:	27 minutes ago
NAS Identifier:	ICX-Switch
NAS IP:	10.176.166.142
NAS Port ID:	1/1/1
NAS Port:	1
NAS Port Type:	Ethernet
Session ID:	17
Last Accounting Update:	19189 millis
Input Traffic:	30 MB (148071 packets)
Output Traffic:	76 MB (665022 packets)
Accumulated Session Time:	1489 seconds
Additional Information:	Enrollment Record

Use Case 2: Onboarding an 802.1X Wired Client Using Certificate-based Authentication

- Cloudpath Configuration..... 33
- Switch Configuration 35
- Switch Show Commands and Syslog Information..... 36
- Cloudpath Information..... 37

The following example uses 802.1X authentication for authenticating a client using a certificate. When the device is connected to a switch, authentication fails because the valid device certificate does not exist. The client is moved to a restricted VLAN where captive portal is enabled. The user must download the certificate and install it. After the successful authentication, the client is assigned a RADIUS VLAN and an ACL.

FIGURE 5 Use Case 2 Workflow



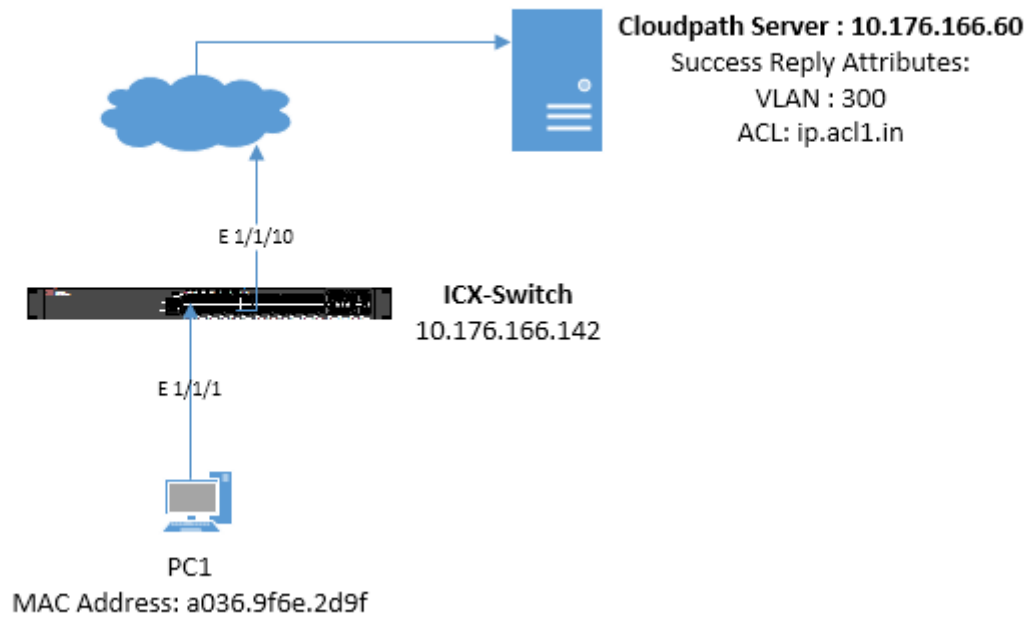
Client PC1

- Username: jagadeesh.chandraiah@arris.com
- Password: Foundry1#
- After authentication:
 - The client should be placed in VLAN 300.
 - Incoming traffic from client should be filtered by ACL "acl1".

NOTE

The administrator can apply a policy such as a VLAN, an ACL, or both from the RADIUS server depending on the network design and its implementation. It is recommended to use "virtual-port 443" for captive portal and "secure-login" under a Web authentication configuration in a production environment.

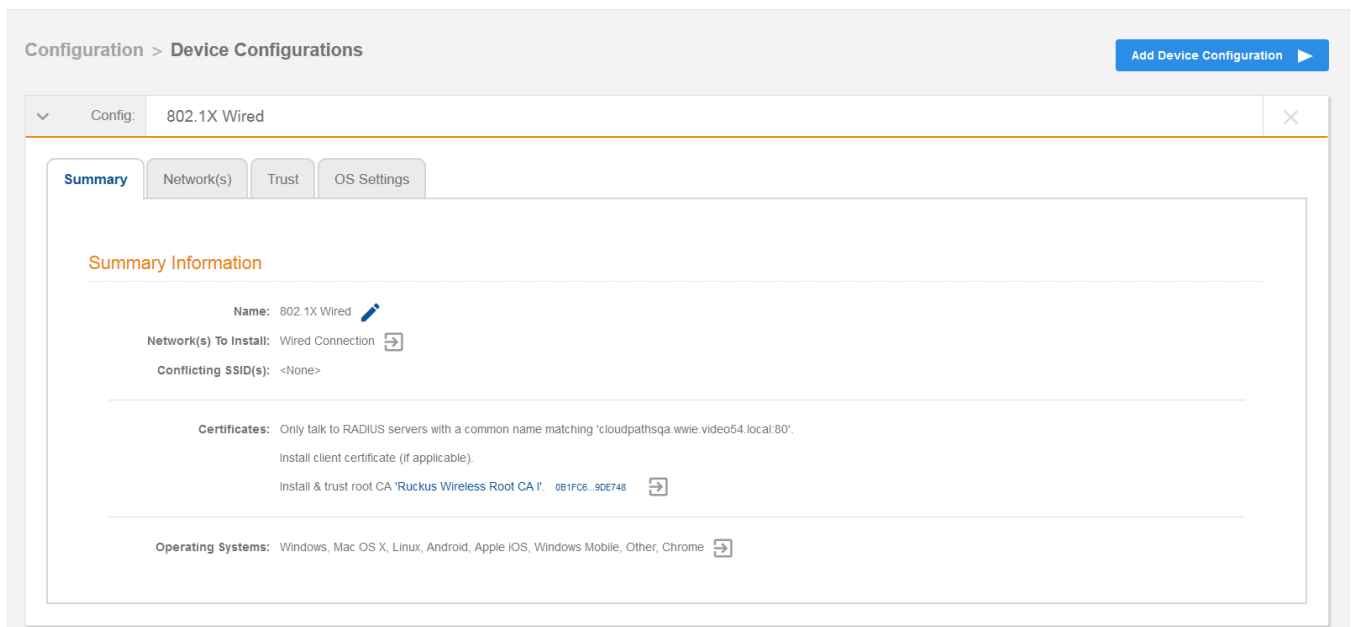
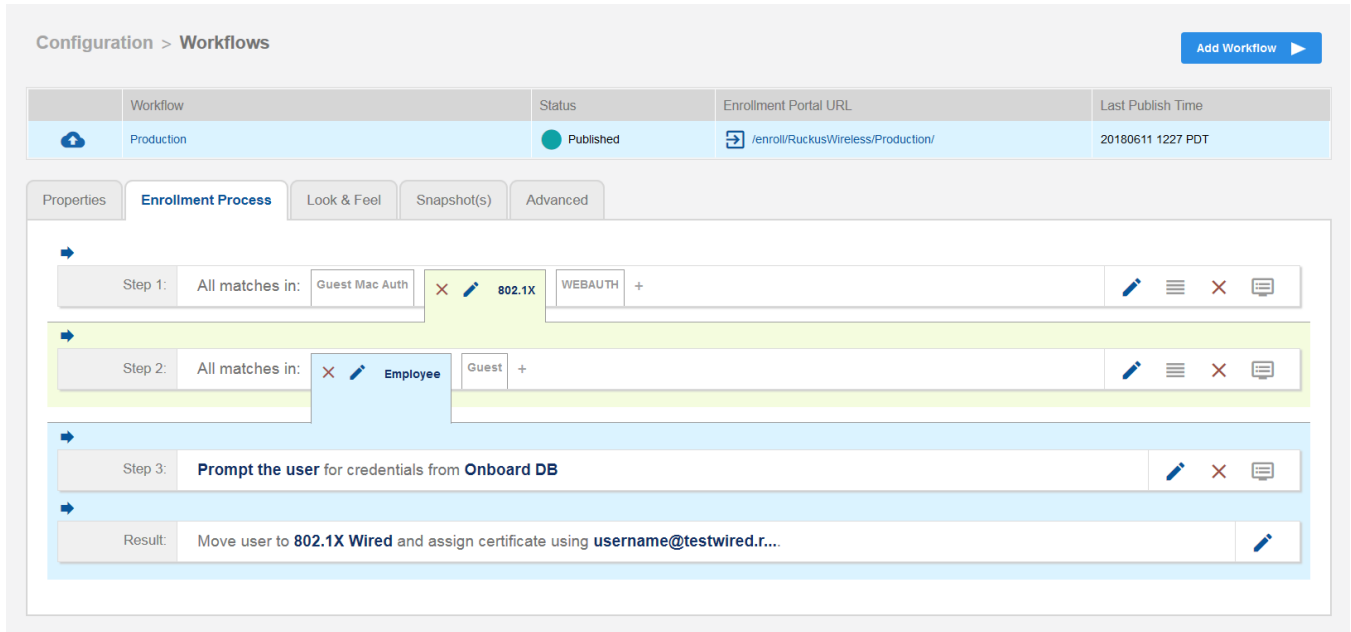
FIGURE 6 Example of Assigning a Dynamic VLAN and ACL with 802.1X Authentication



Cloudpath Configuration

1. Configure the following steps to authenticate the client using 802.1X certificate-based authentication.

The following screenshots demonstrate steps for configuring the 802.1X authentication workflow.



Use Case 2: Onboarding an 802.1X Wired Client Using Certificate-based Authentication Cloudpath Configuration

Configuration > Device Configurations Add Device Configuration ▶

Config: 802.1X Wired

Summary **Network(s)** Trust OS Settings

WLAN & Wired Network Information

Network(s) To Install:

Network	Protocol	Roaming	Behavior
Wired Connection	802.1X Certificate-based		Configure and move to network. (Onsite)

Add ✖ ^ v

Conflicting SSID(s): <None> ✎
 Post-Transition URL: <None> ✎

Configuration > Device Configurations Add Device Configuration ▶

Config: 802.1X Wired

Summary Network(s) **Trust** OS Settings

Wi-Fi Trust

Trusted RADIUS Server(s): Onboard RADIUS Server Change

When connecting to the network, the end-user's device will compare the server certificate presented by the RADIUS server to the information specified here, including both the common name of the RADIUS server certificate and the chain of the issuing CA. On some operating systems, including Mac OS X, this value is case-sensitive.

Trusted Common Name: cloudpathsqa.wwie.video54.local:80

Trusted RADIUS Chain:

Root CA:	Ruckus Wireless Root CA 1	0B1FC8...9DE748	20380208	
Server Certificate:	cloudpathsqa.wwie.video54.local:80	33F32E...8433FF	20210328	Ruckus Wireless Root CA 1

Web Browser Trust

Install Additional CAs: No additional CAs have been specified. Upload

- Navigate to **Certificate Authority > Manage Templates** to edit the certificates.

Certificate Authority > Manage Templates Add Template ▶

> Template:	Onboard template Server Template				
> Template:	Onboard template username@defaultcert.ruckuswireless.com				
> Template:	Onboard template username@guest.ruckuswireless.com				
▼ Template:	Onboard template username@employee.ruckuswireless.com				

Common Name: \${USERNAME}@employee.ruckuswireless.com

CA Type: Onboard

CA Reference Name: Ruckus Wireless Intermediate CA I

CA Common Name: Ruckus Wireless Intermediate CA I

Chain:

Name	Notes	Expires
Ruckus Wireless Intermediate CA I		20380208
Ruckus Wireless Root CA I		20380208

Notifications: No notifications currently exist. Add

RADIUS Policies: VLAN: '300'
Filter ID: 'ip.acl1.in'

SCEP Keys: No SCEP keys currently exist. Add

- Create a snapshot to save the changes.

Configuration > Workflows Add Workflow ▶

	Workflow	Status	Enrollment Portal URL	Last Publish Time
	Production	Published	/enroll/RuckusWireless/Production/	20180611 1240 PDT

Switch Configuration

```
!
captive-portal cp-sqa
virtual-ip cloudpathsqa.wwie.video54.local
virtual-port 80
login-page /enroll/RuckusWireless/Production/
!
vlan 2 name AUTH-DEFAULT by port
tagged ethe 1/1/10
spanning-tree
!
vlan 3 name RESTRICTED/GUEST by port
tagged ethe 1/1/10
spanning-tree
webauth
captive-portal profile cp-sqa
auth-mode captive-portal
no secure-login
trust-port ethernet 1/1/10
```

Use Case 2: Onboarding an 802.1X Wired Client Using Certificate-based Authentication Switch Show Commands and Syslog Information

```
enable
!
vlan 100 name Management-NW by port
  tagged ethe 1/1/10
  untagged ethe 1/1/20
  spanning-tree
  management-vlan
  default-gateway 10.176.166.1 1
!
vlan 300 by port
  tagged ethe 1/1/10
!!
authentication
  auth-default-vlan 2
  restricted-vlan 3
  auth-fail-action restricted-vlan
  dot1x enable
  dot1x enable ethe 1/1/1
  dot1x port-control auto ethe 1/1/1
  dot1x guest-vlan 3
  dot1x timeout tx-period 5
!
!
aaa authentication dot1x default radius
aaa authorization coa enable
aaa accounting dot1x default start-stop radius
aaa accounting mac-auth default start-stop radius
!
ip address 10.176.166.142/24
ip dns domain-list wwie.video54.local
ip dns server-address 10.176.4.10 10.176.4.11
!
radius-client coa host 10.176.166.60 key Foundry1
radius-server host 10.176.166.60 auth-port 1812 acct-port 1813 default key Foundry1 dot1x mac-auth web-auth
radius-server accounting interim-updates
radius-server accounting interim-interval 5
!
web-management https
!
ip access-list extended acl1
  permit ip any any
!
```

Switch Show Commands and Syslog Information

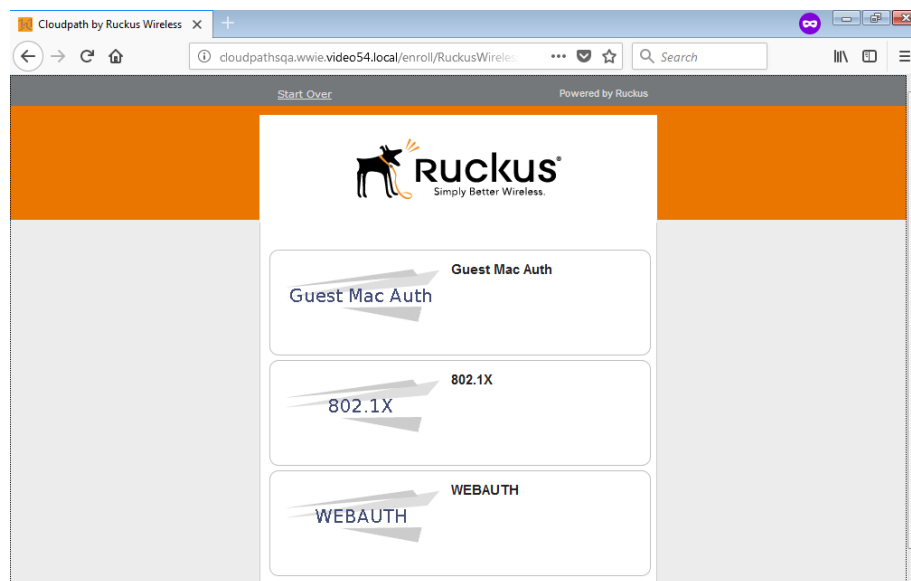
```
ICX-Switch#
SYSLOG: <14> Jun 12 13:46:19 ICX-Switch System: Interface ethernet 1/1/1, state up
SYSLOG: <14> Jun 12 13:46:19 ICX-Switch STP: VLAN 4094 Port 1/1/1 STP State -> BLOCKING (DOT1wTransition)
SYSLOG: <14> Jun 12 13:46:20 ICX-Switch System: PoE: Power disabled on port 1/1/1 because of detection of non-
PD. PD detection will be disabled on port.
SYSLOG: <14> Jun 12 13:46:24 ICX-Switch STP: VLAN 4094 Port 1/1/1 STP State -> LEARNING (DOT1wTransition)
SYSLOG: <14> Jun 12 13:46:24 ICX-Switch STP: VLAN 4094 Port 1/1/1 STP State -> FORWARDING (DOT1wTransition)
SYSLOG: <14> Jun 12 13:46:24 ICX-Switch DOT1X: Port 1/1/1 - mac a036.9f6e.2d9f AuthControlledPortStatus change:
unauthorized
SYSLOG: <13> Jun 12 13:46:42 ICX-Switch FLEXAUTH: Port 1/1/1 is added into Limited-Access Vlan 3 as mac-vlan
member
SYSLOG: <13> Jun 12 13:46:42 ICX-Switch FLEXAUTH: Port 1/1/1 is deleted from Auth-Default Vlan 2 as mac-vlan
member
SYSLOG: <13> Jun 12 13:46:42 ICX-Switch DOT1X: Port 1/1/1 Mac a036.9f6e.2d9f Vlan 3 - AuthControlledPortStatus
change: guest
SYSLOG: <13> Jun 12 13:52:10 ICX-Switch DOT1X: Port 1/1/1 mac a036.9f6e.2d9f vlan 3: Session is cleared
[Termination-cause: Recv-802.1x-BPDU]
SYSLOG: <13> Jun 12 13:52:10 ICX-Switch FLEXAUTH: Port 1/1/1 is added into Auth-Default Vlan 2 as mac-vlan
member
SYSLOG: <13> Jun 12 13:52:10 ICX-Switch FLEXAUTH: Port 1/1/1 is deleted from Limited-Access Vlan 3 as mac-vlan
member
SYSLOG: <14> Jun 12 13:52:12 ICX-Switch DOT1X: Port 1/1/1 - mac a036.9f6e.2d9f AuthControlledPortStatus change:
unauthorized
```

```

SYSLOG: <10> Jun 12 13:52:12 ICX-Switch DOT1X: RADIUS server 10.176.166.60 Accepted for a036.9f6e.2d9f with
(V4I:ac11 V4O: V6I:V6O: U:300 )
SYSLOG: <13> Jun 12 13:52:12 ICX-Switch DOT1X: Port 1/1/1 Mac a036.9f6e.2d9f - received AAA-ACCEPT
SYSLOG: <13> Jun 12 13:52:12 ICX-Switch FLEXAUTH: Port 1/1/1 is added into Dynamic Vlan 300 as mac-vlan member
SYSLOG: <13> Jun 12 13:52:12 ICX-Switch FLEXAUTH: Port 1/1/1 is deleted from Auth-Default Vlan 2 as mac-vlan
member
SYSLOG: <14> Jun 12 13:52:12 ICX-Switch DOT1X: Port 1/1/1 - mac a036.9f6e.2d9f, AuthControlledPortStatus
change: authorized
ICX-Switch#
ICX-Switch# show authentication sessions all
-----
Port      MAC          IP (v4/v6)   User          VLAN  Auth  Auth  ACL  Session  Age  PAE
  Addr                    Addr          Name           State  Method State  Time     State
-----
1/1/1    a036.9f6e.2d9f  10.176.167.171 jagadeesh.chandra 300   802.1X Permit Yes     52     Ena
AUTHENTICATED
ICX-Switch#
ICX-Switch# show authentication acls all
-----
Port      MAC Address    V4 Ingress    V4 Egress     V6 Ingress    V6 Egress
-----
1/1/1    a036.9f6e.2d9f  ac11          -             -             -
ICX-Switch#
ICX-Switch# show vlan 300
Total PORT-VLAN entries: 10
Maximum PORT-VLAN entries: 1024
Legend: [Stk=Stack-Id, S=Slot]
PORT-VLAN 300, Name [None], Priority level0, in single spanning tree domain
Untagged Ports: None
Tagged Ports: (U1/M1) 10
Mac-Vlan Ports: (U1/M1) 1
Monitoring: Disabled
    
```

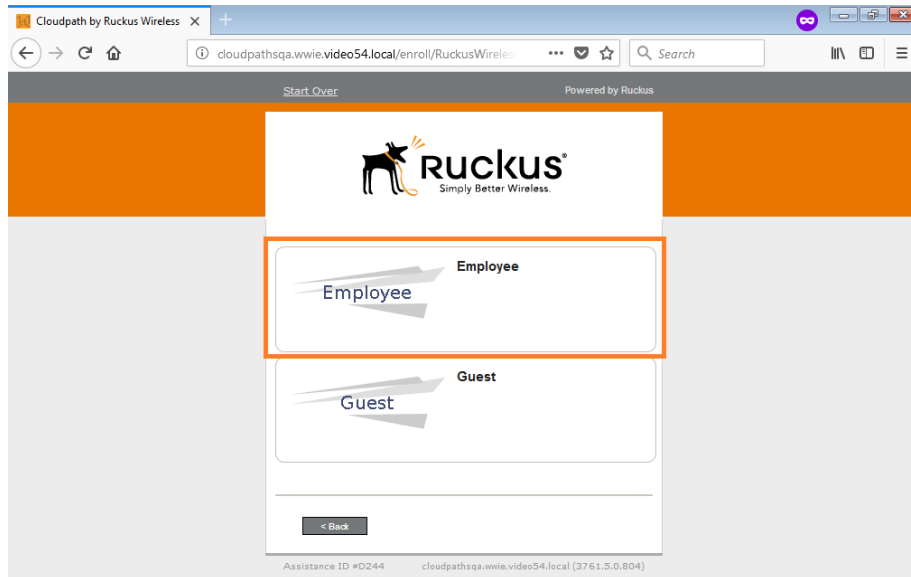
Cloudpath Information

1. On the client PC, open a browser and enter any website. You will be redirected to the captive-portal page. Click the **802.1X** tab.

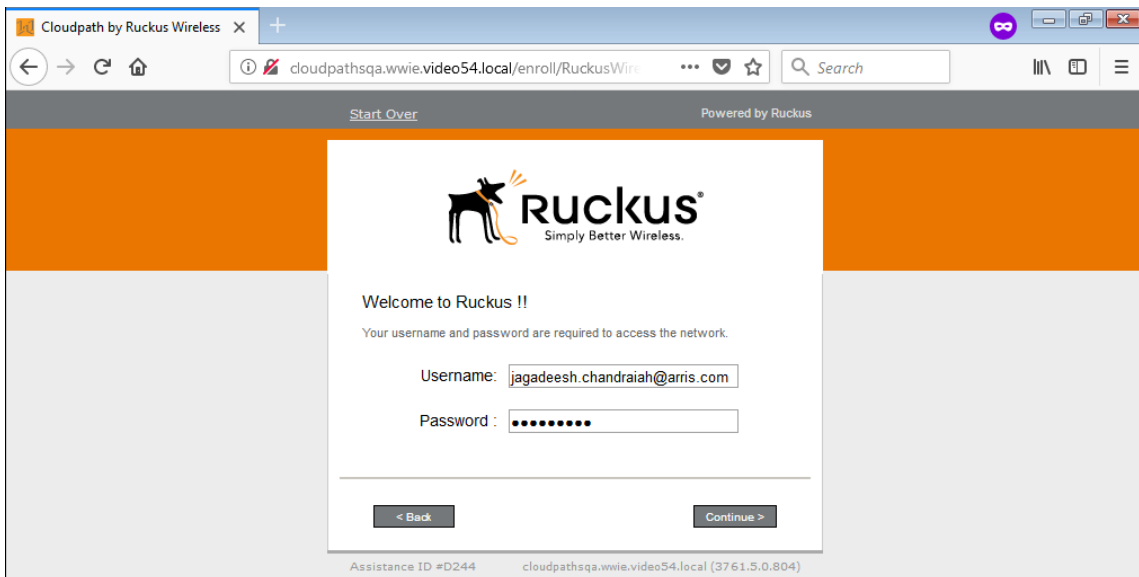


Use Case 2: Onboarding an 802.1X Wired Client Using Certificate-based Authentication
Cloudpath Information

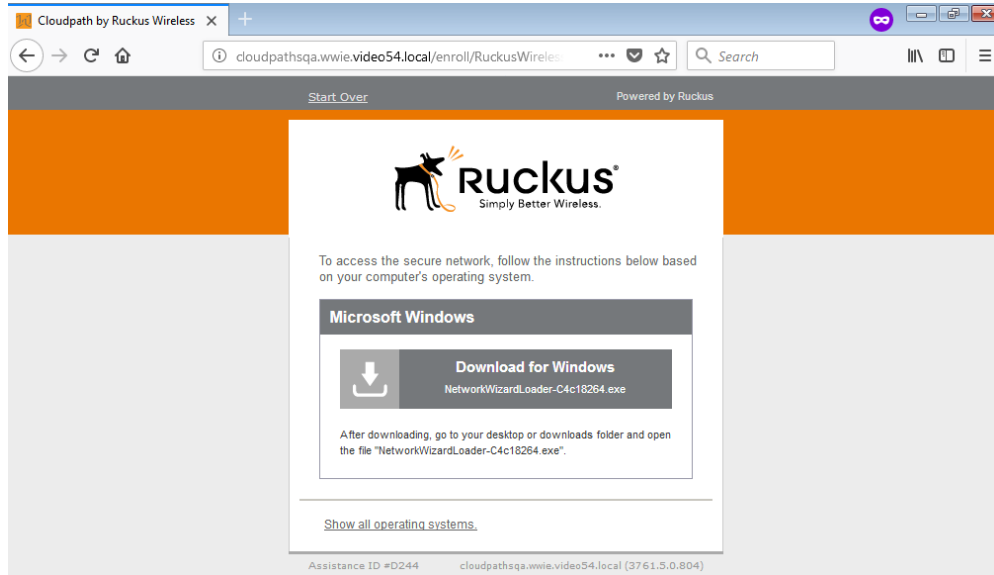
- 2. Click the **Employee** tab.



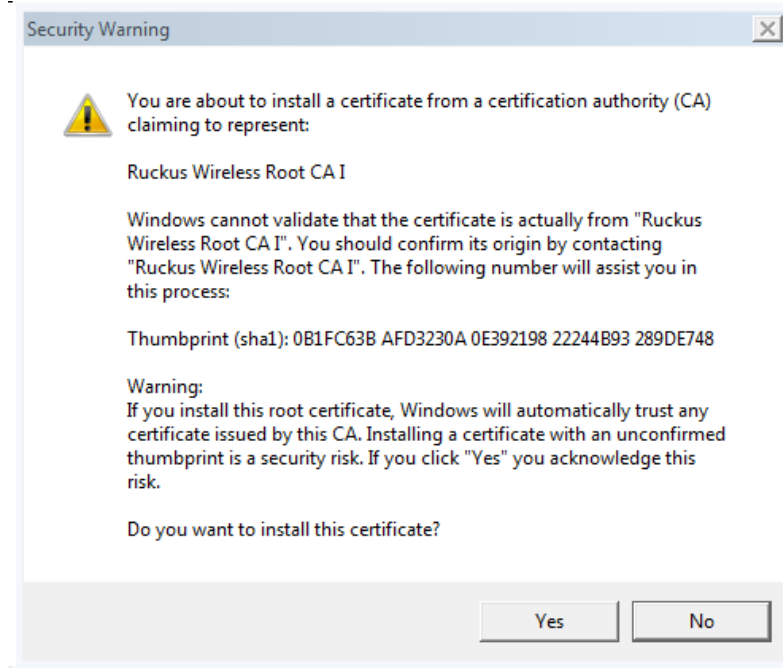
- 3. Enter the login credentials to access the network.



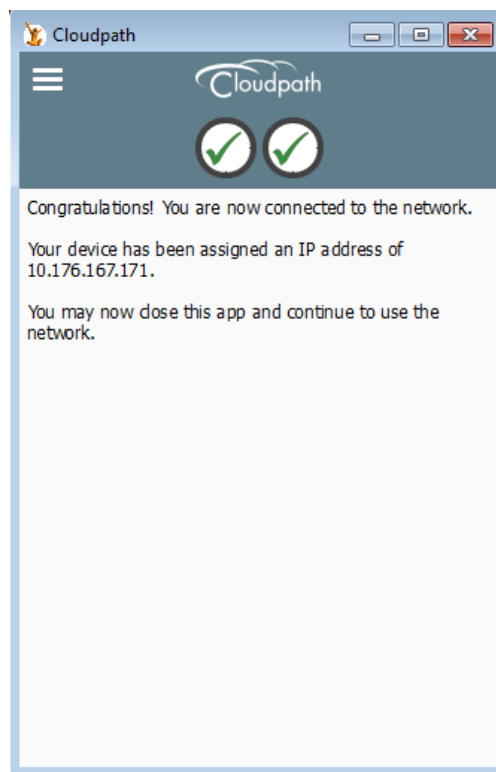
4. Download the network loader and follow the instructions based on your operating system.



5. When prompted, install the root certificate.



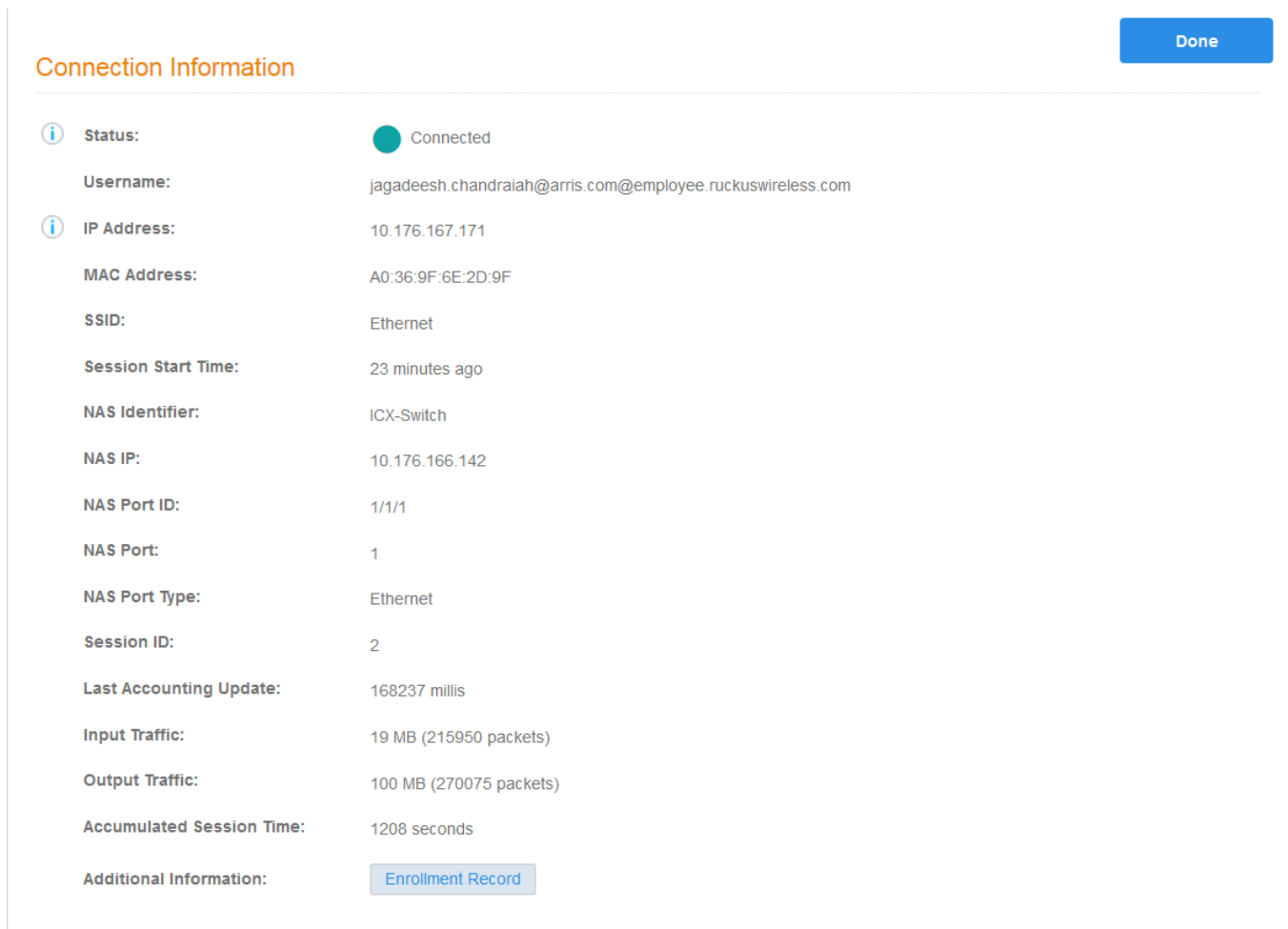
The network loader configures the device and attempts to connect to the network. After the successful connection, the client PC is connected to the network.



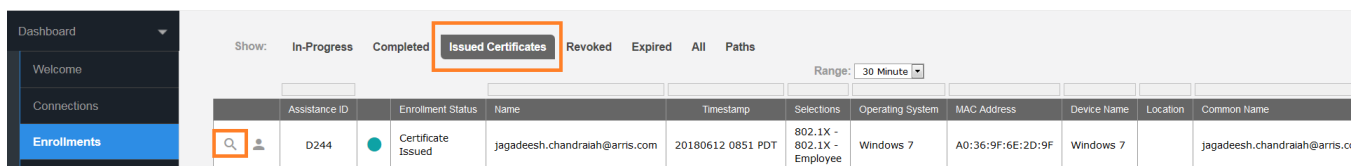
- On the Cloudpath server, navigate to **Dashboard > Connections** to verify the username of the certificate issued to the user.



- Click the magnifying glass symbol to get more information about the connection.



- Navigate to **Dashboard > Enrollments** and click **Issued Certificates** to view the enrollment status details.



9. Click the magnifying glass symbol for the issued certificate to view more information about the enrollment.

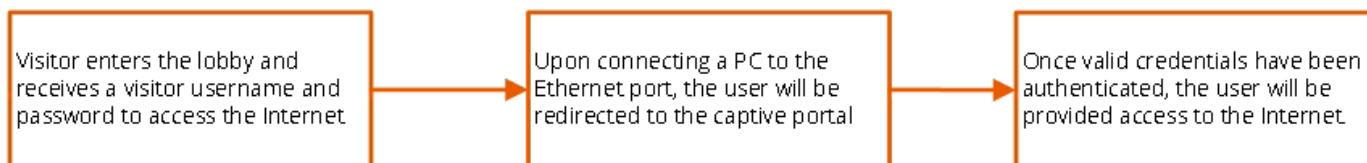
The screenshot displays the Cloudpath user interface. On the left is a dark sidebar menu with options: Dashboard, Welcome, Connections, **Enrollments** (highlighted), Users & Devices, Certificates, DHCP Fingerprints, Notifications, Event Response, Configuration, Sponsorship, Certificate Authority, Administration, and Support. The main content area shows the breadcrumb 'Dashboard > Enrollments > View'. Below this is a section titled 'Enrollment Information' with a dropdown arrow. It lists the following details: Enrollment Status: Certificate Issued (with a 'Block' button); Name: Jagadeesh Chandraiah; Email Address: jagadeesh.chandraiah@arris.com; Selections: 802.1X - 802.1X - Employee; Operating System: Windows 7; Browser: Firefox; Form Factor: Computer; MAC Address: A0:36:9F:6E:2D:9F; Language: en-US,en;q=0.5; Notes: (with a magnifying glass icon). Below this is a section titled 'Connection Information' with a dropdown arrow, listing: Connection State: **Connected**; Session Start Time: 18 minutes ago; Session Last Update: 149 seconds ago; WLAN Username: jagadeesh.chandraiah@arris.com@employee.ruckuswireless.com; Session ID: 2; IP Address: 10.176.167.171. At the bottom of the sidebar, it shows 'cloudpathsqa.wwie.video54.local Version 5.2.3761' and a notice: 'Use of this website signifies your agreement to the EULA'.

Use Case 3: Guest Internet Access Using External Captive Portal

- Cloudpath Configuration..... 45
- Switch Configuration 48
- Switch Show Commands and Syslog Information..... 48
- Cloudpath Information..... 49

The following example uses the captive portal (Web authentication) for authenticating a client and then dynamically assigns an ACL after a successful authentication. In a typical scenario, a visitor enters the lobby and receives a visitor username and password to access the Internet. In the following use case, VLAN 3 is an Internet-only-enabled VLAN. Upon connecting a PC to the Ethernet port, the user will be redirected to the captive portal. Once valid credentials have been authenticated, the user will be provided access to the Internet.

FIGURE 7 Use Case 3 Workflow



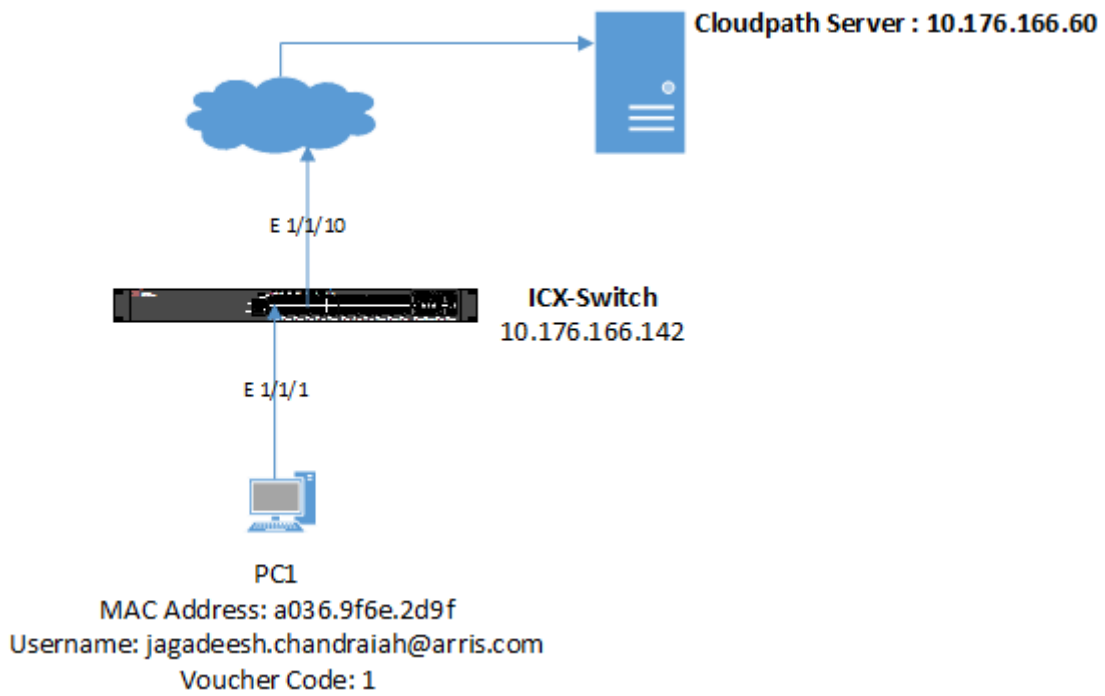
Client PC1

- The MAC address is a036.9f6e.2d9f.
- After authentication, incoming traffic from client should be filtered by ACL "acl1".

NOTE

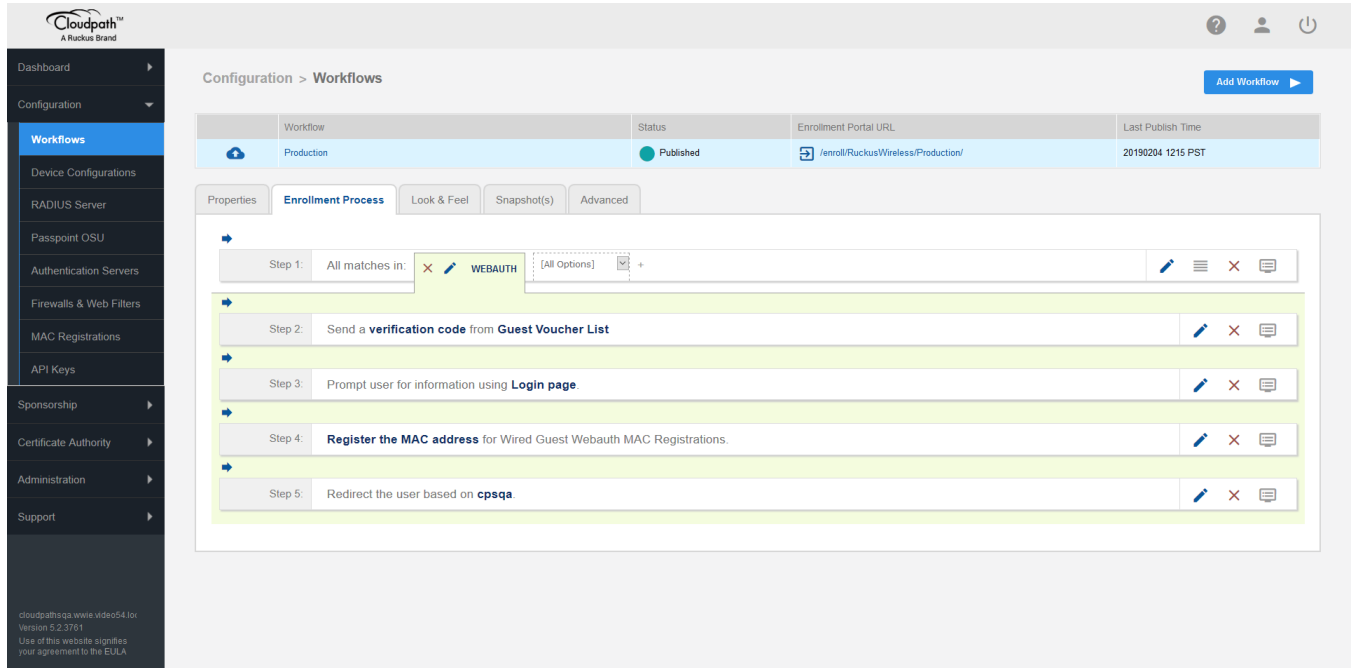
The administrator can apply a policy such as an ACL from the RADIUS server depending on the network design and its implementation. It is recommended to use "virtual-port 443" for captive portal and "secure-login" under a Web authentication configuration in a production environment.

FIGURE 8 Example of Web Authentication (Captive Portal) with a Guest VLAN



Cloudpath Configuration

1. Navigate to **Configuration > Workflows** and create steps for Web authentication.



2. Modify the data prompt by clicking "Login page" for input field 1.

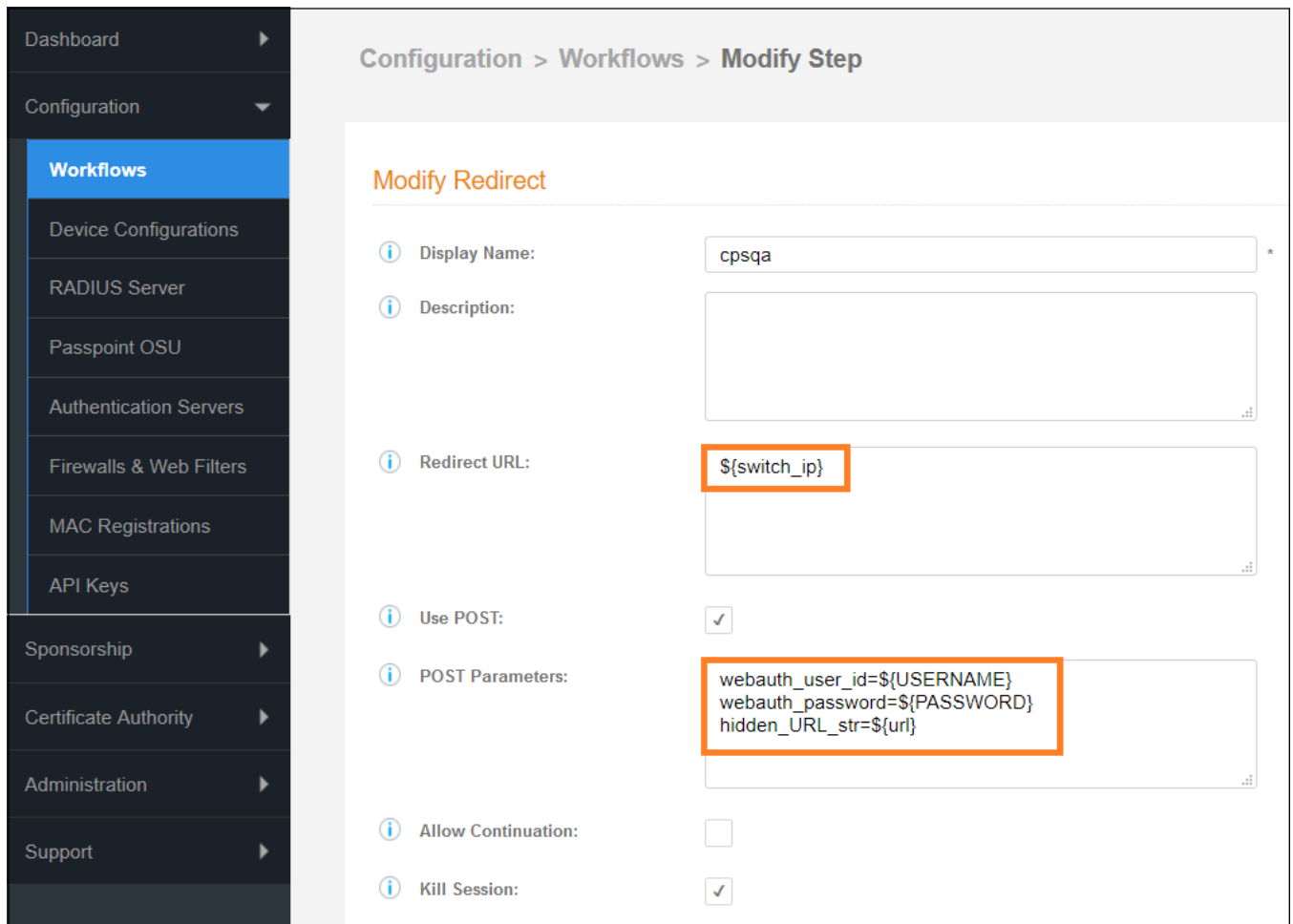
The screenshot shows the Ruckus Cloudpath configuration interface. On the left is a dark sidebar with navigation options: Dashboard, Configuration, Workflows (highlighted), Device Configurations, RADIUS Server, Passpoint OSU, Authentication Servers, Firewalls & Web Filters, MAC Registrations, API Keys, Sponsorship, Certificate Authority, Administration, and Support. The main content area is titled 'Configuration > Workflows > Modify Step'. It contains three sections:

- Modify Data Prompt:** Includes 'Display Name' (Login page) and 'Description' (empty text area).
- Webpage Display Information:** Includes 'Title' (Welcome to Ruckus !!), 'Message HTML' (empty text area), 'Bottom Label' (empty text field), and 'Continue Button Label' (Continue >).
- Input Field 1:** (Highlighted with an orange border) Includes 'Label' (username), 'Regex' (empty text field), and 'Variable Name' (USERNAME).

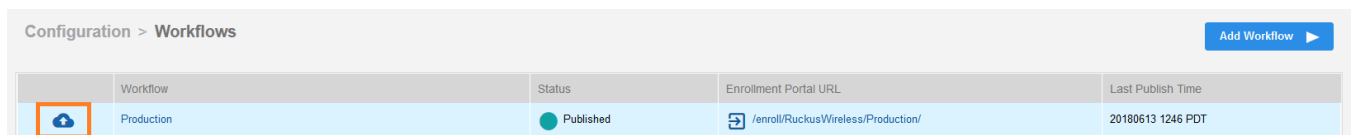
At the bottom left of the sidebar, there is a footer: cloudpathsqa.wwie.video54.loc, Version 5.2.3761, Use of this website signifies your agreement to the EULA.

3. Create the Redirect URL `${switch_ip}` and enter the following POST parameters:
 - `webauth_user_id=${USERNAME}`
 - `webauth_password=${PASSWORD}`
 - `hidden_URL_str=${url}`

Based on administrator preference, the "hidden_URL_str" parameter can be configured, which will be used to redirect to the specific website after authentication.



4. Create a snapshot to save the changes.



Switch Configuration

```
!  
captive-portal cp-sqa  
  virtual-ip cloudpathsqa.wwie.video54.local  
  virtual-port 80  
  login-page /enroll/RuckusWireless/Production/  
!  
vlan 3 name INTERNET by port  
  tagged ethe 1/1/10  
  untagged ethe 1/1/1  
  spanning-tree  
  webauth  
    captive-portal profile cp-sqa  
    auth-mode captive-portal  
    no secure-login  
    trust-port ethernet 1/1/10  
    enable  
!  
vlan 100 name Management-NW by port  
  tagged ethe 1/1/10  
  untagged ethe 1/1/20  
  spanning-tree  
  management-vlan  
  default-gateway 10.176.166.1 1  
!  
aaa authentication dot1x default radius  
aaa authorization coa enable  
aaa accounting dot1x default start-stop radius  
aaa accounting mac-auth default start-stop radius  
!  
ip address 10.176.166.142/24  
ip dns domain-list wwie.video54.local  
ip dns server-address 10.176.4.10 10.176.4.11  
!  
radius-client coa host 10.176.166.60 key Foundry1  
radius-server host 10.176.166.60 auth-port 1812 acct-port 1813 default key Foundry1 dot1x mac-auth web-auth  
radius-server accounting interim-updates  
radius-server accounting interim-interval 5  
!  
web-management https  
!
```

Switch Show Commands and Syslog Information

```
ICX-Switch#  
SYSLOG: <14> Jun 12 17:09:09 ICX-Switch System: Interface ethernet 1/1/1, state up  
SYSLOG: <14> Jun 12 17:09:09 ICX-Switch STP: VLAN 4094 Port 1/1/1 STP State -> BLOCKING (DOT1wTransition)  
SYSLOG: <14> Jun 12 17:09:10 ICX-Switch System: PoE: Power disabled on port 1/1/1 because of detection of non-  
PD. PD detection will be disabled on port.  
SYSLOG: <14> Jun 12 17:09:13 ICX-Switch STP: VLAN 4094 Port 1/1/1 STP State -> LEARNING (DOT1wTransition)  
SYSLOG: <14> Jun 12 17:09:13 ICX-Switch STP: VLAN 4094 Port 1/1/1 STP State -> FORWARDING (DOT1wTransition)  
SYSLOG: <10> Jun 12 17:10:32 ICX-Switch WEBAUTH: RADIUS server 10.176.166.60 Accepted for a036.9f6e.2d9f with  
(ST:86400 )  
SYSLOG: <14> Jun 12 17:10:32 ICX-Switch Web Auth in Vlan 3: Authentication succeeded for user :  
jagadeesh.chandraiah@arris.com using mac: a036.9f6e.2d9f on port 1/1/1 for a duration 86400 seconds  
ICX-Switch#  
ICX-Switch# show webauth allowed-list  
=====
```

VLAN 3: Web Authentication, Mode: I = Internal E = External						

Web Authenticated List			Configuration	Auth Duration	Dynamic	
Port	MAC Address	User Name	Mode	Static/Dynamic	HH:MM:SS	ACL

1/1/1	a036.9f6e.2d9f	jagadeesh.chandraiah@a	E	D	23:59:52	No

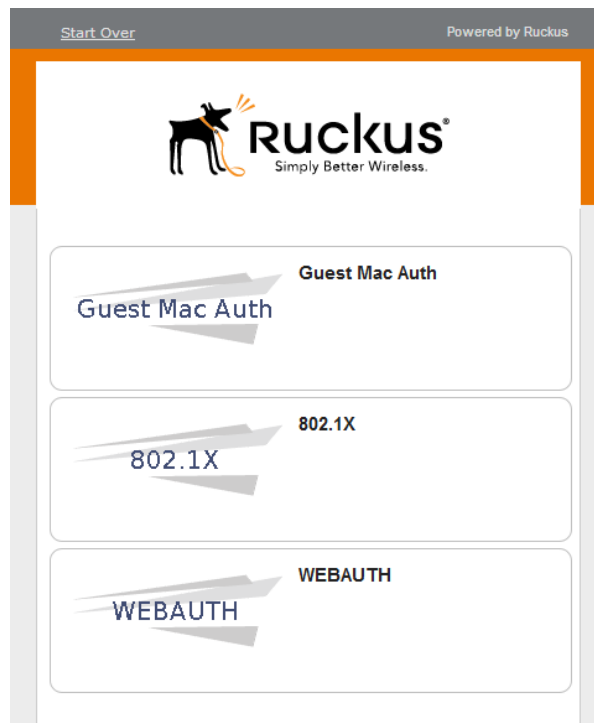
```
ICX-Switch#
```



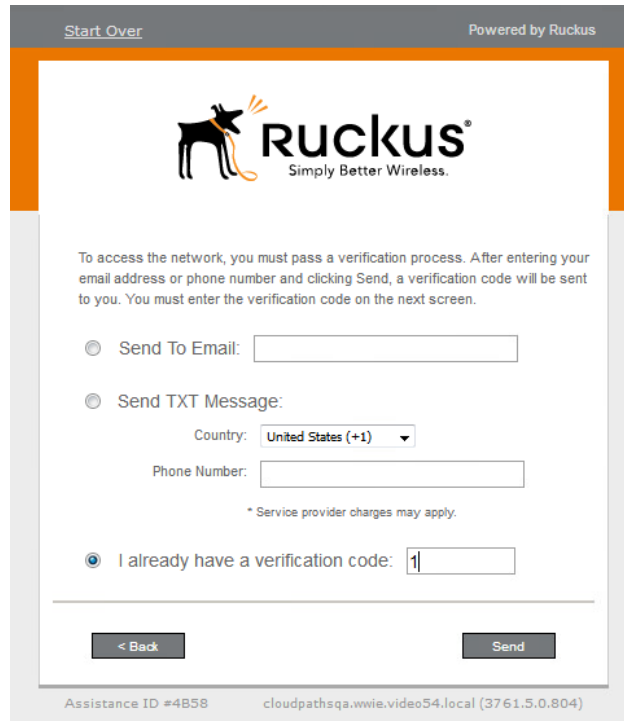
```
ICX-Switch# show vlan 3
Total PORT-VLAN entries: 10
Maximum PORT-VLAN entries: 1024
Legend: [Stk=Stack-Id, S=Slot]
PORT-VLAN 3, Name INTERNET, Priority level0, in single spanning tree domain
Untagged Ports: (U1/M1) 1
Tagged Ports: (U1/M1) 10
Mac-Vlan Ports: None
Monitoring: Disabled
```

Cloudpath Information

1. Open a web browser on the client PC and enter any website address or <https://www.ruckuswireless.com/>.
Because captive-portal authentication is configured on Webauth VLAN 3 and the captive-portal profile points to "cp-sqa", the browser will redirect to <http://cloudpathsqa.wwie.video54.local/enroll/RuckusWireless/Production/process>.
2. Click **WEBAUTH**.

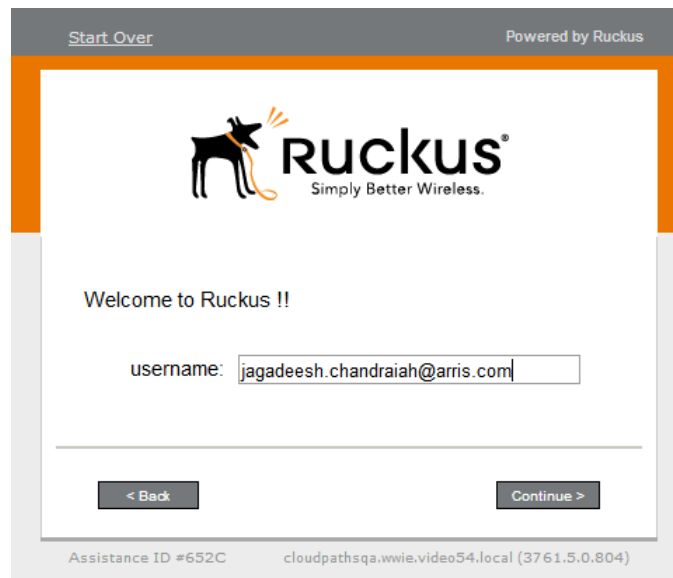


3. Enter the verification code.



The screenshot shows a Ruckus captive portal verification screen. At the top, it says "Start Over" and "Powered by Ruckus". The Ruckus logo is prominently displayed. Below the logo, there is a paragraph explaining the verification process: "To access the network, you must pass a verification process. After entering your email address or phone number and clicking Send, a verification code will be sent to you. You must enter the verification code on the next screen." There are three radio button options: "Send To Email:" with an empty text box, "Send TXT Message:" with a "Country:" dropdown menu set to "United States (+1)" and a "Phone Number:" text box, and "I already have a verification code:" with a text box containing the number "1". At the bottom, there are two buttons: "< Back" and "Send". The footer contains "Assistance ID #4858" and "cloudpathsqa.wwie.video54.local (3761.5.0.804)".

4. Enter the username and click **Continue**.



The screenshot shows a Ruckus captive portal login screen. At the top, it says "Start Over" and "Powered by Ruckus". The Ruckus logo is prominently displayed. Below the logo, it says "Welcome to Ruckus !!". There is a "username:" label followed by a text box containing the email address "jagadeesh.chandraiah@arris.com". At the bottom, there are two buttons: "< Back" and "Continue >". The footer contains "Assistance ID #652C" and "cloudpathsqa.wwie.video54.local (3761.5.0.804)".

You will be redirected to <https://www.ruckuswireless.com/>.

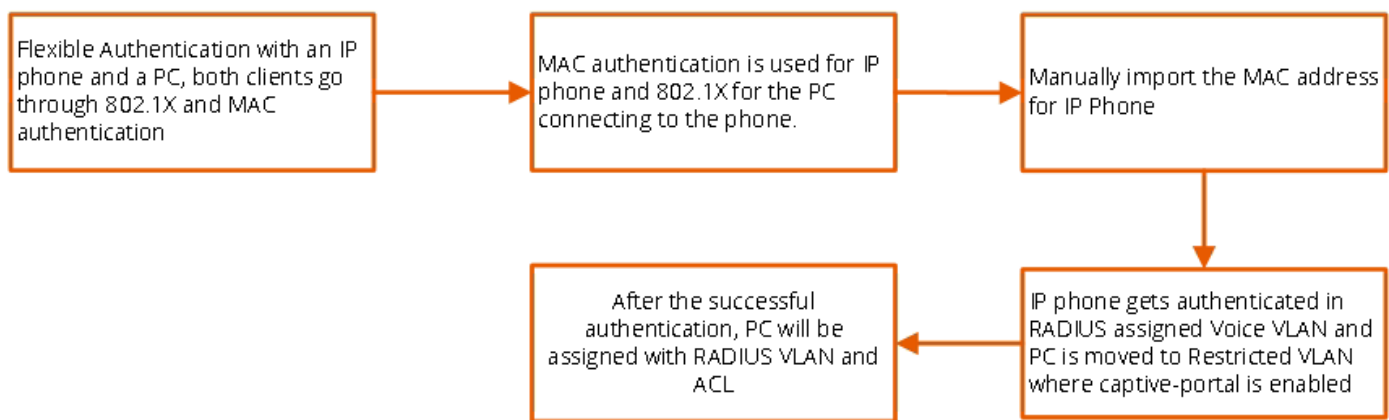
Use Case 4: Authentication of an IP Phone and a PC on the Same Port Using Flexible Authentication

- Cloudpath Configuration..... 52
- Switch Configuration 57
- Switch Show Commands and Syslog Information..... 58
- Cloudpath Information..... 60

The following example demonstrates the use for Flexible Authentication in a setup where a PC is daisy-chained to an IP phone connected to a switch port. When Flexible Authentication is enabled on a port with an IP phone and a PC, both clients go through 802.1X and MAC authentication. A typical scenario uses MAC authentication for the IP phone and 802.1X for the PC connecting to the phone.

Note that if the IP phone is not capable of participating in the 802.1X process, it will time out, and then MAC authentication will be tried. If the IP phone is capable of 802.1X, 802.1X authentication is used first by default. If 802.1X succeeds, MAC authentication is not performed.

FIGURE 9 Use Case 4 Workflow



If LLDP is not configured by way of the RADIUS server, the following LLDP configuration must be added to enable LLDP MED on the port connecting to the IP phone:

```
lldp med network-policy application voice tagged vlan 3000 priority 4 dscp 46 ports ethernet 1/1/2
```

IP Phone: The IP phone MAC address is 0024.c442.bb24.

Client PC2

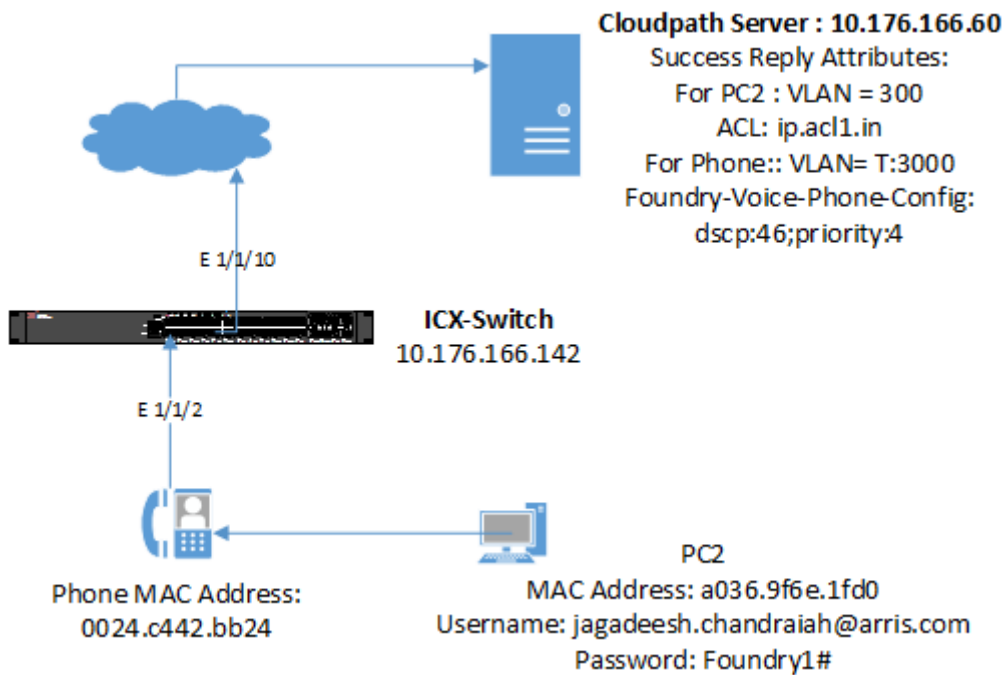
- 802.1X username: jagadeesh.chandraiah@arris.com
- Password: Foundry1#
- Before authentication:
 - On the Client PC2, 802.1X authentication is not enabled.

- After authentication:
 - The client should be placed in VLAN 300.
 - Incoming traffic from the client should be filtered by ACL "acl1".

NOTE

The administrator can apply a policy such as a VLAN, an ACL, or both from the RADIUS server depending on the network design and its implementation. It is recommended to use "virtual-port 443" for captive portal and "secure-login" under a Web authentication configuration in a production environment.

FIGURE 10 Example of Authenticating an IP Phone and a PC on the Same Port Using Flexible Authentication



Cloudpath Configuration

Configure the workflow for 802.1X authentication for PC2 and MAC authentication for an IP phone.

Refer to [Use Case 2: Onboarding an 802.1X Wired Client Using Certificate-based Authentication](#) on page 31 for configuring the 802.1X workflow.

The screenshot displays the 'Configuration > Workflows' interface. At the top right, there is an 'Add Workflow' button. Below it is a table with the following data:

Workflow	Status	Enrollment Portal URL	Last Publish Time
Production	Published	/enroll/RuckusWireless/Production/	20180613 1246 PDT

Below the table are tabs for 'Properties', 'Enrollment Process', 'Look & Feel', 'Snapshot(s)', and 'Advanced'. The 'Enrollment Process' tab is active, showing a workflow with four steps:

- Step 1:** All matches in: Guest Mac Auth, 802.1X, WEBAUTH, Mac Auth for IP... +
- Step 2:** All matches in: Employee, Guest +
- Step 3:** Prompt the user for credentials from Onboard DB
- Result:** Move user to 802.1X Wired and assign certificate using username@employee.ru...

Use Case 4: Authentication of an IP Phone and a PC on the Same Port Using Flexible Authentication Cloudpath Configuration

The following screenshots demonstrate steps for configuring the workflow for MAC authentication for an IP phone.

The screenshot displays the 'Configuration > Workflows' page in the Ruckus Cloudpath interface. At the top right, there is an 'Add Workflow' button. Below this is a table listing workflows:

Workflow	Status	Enrollment Portal URL	Last Publish Time
Production	Published	/enroll/RuckusWireless/Production/	20180613 1246 PDT

Below the table, the 'Enrollment Process' tab is selected, showing a workflow with three steps:

- Step 1:** All matches in: Guest Mac Auth, 802.1X, WEBAUTH, Mac Auth for IP... (with a plus sign for adding more)
- Step 2:** Register the MAC address for IP Phone.
- Result:** Assign a device configuration and/or certificate.

Configuration > MAC Registrations

> List 1: MAC registrations via **Wired MAC-AUTH**

> List 2: MAC registrations via **Wired Guest Webauth MAC Registrations**

▼ List 3: MAC registrations via **IP Phone**

Name: IP Phone

Status: ● Used In workflow & RADIUS.

Success Reply Attributes: Access-Accept
 Tunnel-Type: '13'
 Tunnel-Medium-Type: '6'
 Tunnel-Private-Group-Id: 'T:3000'
 Foundry-Voice-Phone-Config: 'dscp:46;priority:4'

Failure Reply Attributes: Access-Reject

Options: [Download Template](#) [Import](#)

A	B	C	D	E	F
MAC Address	Expiration Date	Username	Email	Device Name	Location
0024c442bb24	4/4/2020	0024c442bb24	jagadeesh.chandraiah@arris.com	IP-Phone-G06	Sunnyvale

Upload MAC Registrations ✕

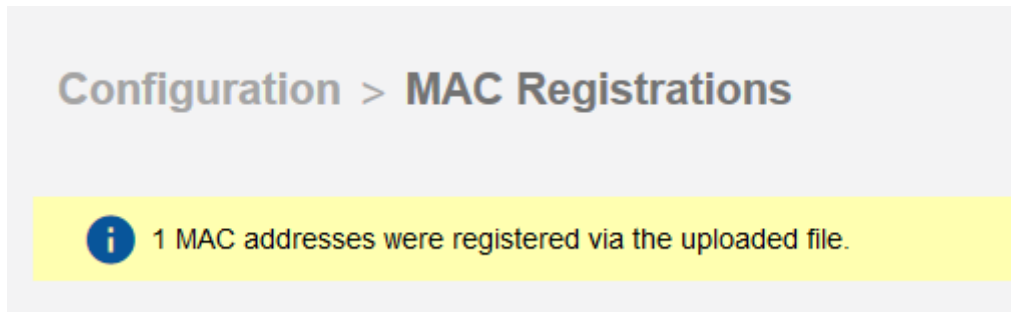
Select the file of MAC addresses to import.

mac_template.xlsx

Configuration > MAC Registrations

▼ **MAC Registration Import**

File contains 1 MAC Address rows that will be imported. Press 'Continue Import' to perform the import.



Show: **Users** Device Types Form Factors **MAC Registrations**

Filters: Show active Show revoked Show expired.

Status	MAC Address	Username	Registration Date	Expiration Date	Registration List
Active	00:24:C4:42:BB:24	Jagadeesh Chandraiah	20180613 1209 PDT	20200404 0000 PDT	IP Phone

Results 1 - 1 of 1.

Configuration > Workflows Add Workflow ▶

Workflow	Status	Enrollment Portal URL	Last Publish Time
Production	Published	/enroll/RuckusWireless/Production/	20180613 1246 PDT

Switch Configuration

```
!  
captive-portal cp-sqa  
  virtual-ip cloudpathsqa.wwie.video54.local  
  virtual-port 80  
  login-page /enroll/RuckusWireless/Production/  
!  
vlan 2 name AUTH-DEFAULT by port  
  tagged ethe 1/1/10  
  spanning-tree  
!  
vlan 3 name RESTRICTED/GUEST by port  
  tagged ethe 1/1/10  
  spanning-tree  
  webauth  
  captive-portal profile cp-sqa  
  auth-mode captive-portal  
  no secure-login  
  trust-port ethernet 1/1/10  
  enable  
!  
vlan 100 name Management-NW by port  
  tagged ethe 1/1/10  
  untagged ethe 1/1/20  
  spanning-tree  
  management-vlan  
  default-gateway 10.176.166.1 1  
!  
vlan 300 by port  
  tagged ethe 1/1/10  
!  
vlan 3000 name VOICE_VLAN by port
```

Use Case 4: Authentication of an IP Phone and a PC on the Same Port Using Flexible Authentication Switch Show Commands and Syslog Information

```

tagged ethe 1/1/10
spanning-tree
!
authentication
auth-mode multiple-untagged
auth-default-vlan 2
restricted-vlan 3
auth-fail-action restricted-vlan
dot1x enable
dot1x enable ethe 1/1/2
dot1x port-control auto ethe 1/1/2
dot1x guest-vlan 3
dot1x timeout tx-period 5
mac-authentication enable
mac-authentication enable ethe 1/1/2
!
!
aaa authentication dot1x default radius
aaa authorization coa enable
aaa accounting dot1x default start-stop radius
aaa accounting mac-auth default start-stop radius
!
ip address 10.176.166.142/24
ip dns domain-list wwie.video54.local
ip dns server-address 10.176.4.10 10.176.4.11
!
radius-client coa host 10.176.166.60 key Foundryl
radius-server host 10.176.166.60 auth-port 1812 acct-port 1813 default key Foundryl dot1x mac-auth web-auth
radius-server accounting interim-updates
radius-server accounting interim-interval 5
!
web-management https
!
ip access-list extended acl1
permit ip any any
!
!lldp run
!

```

Switch Show Commands and Syslog Information

```

ICX-Switch#
SYSLOG: <14> Jun 15 14:02:58 ICX-Switch System: Interface ethernet 1/1/2, state up
SYSLOG: <14> Jun 15 14:02:58 ICX-Switch STP: VLAN 4094 Port 1/1/2 STP State -> BLOCKING (DOT1wTransition)
SYSLOG: <14> Jun 15 14:03:02 ICX-Switch STP: VLAN 4094 Port 1/1/2 STP State -> LEARNING (DOT1wTransition)
SYSLOG: <14> Jun 15 14:03:02 ICX-Switch STP: VLAN 4094 Port 1/1/2 STP State -> FORWARDING (DOT1wTransition)
SYSLOG: <14> Jun 15 14:03:03 ICX-Switch DOT1X: Port 1/1/2 - mac a036.9f6e.1fd0 AuthControlledPortStatus change:
unauthorized
SYSLOG: <14> Jun 15 14:03:03 ICX-Switch DOT1X: Port 1/1/2 - mac 0024.c442.bb24 AuthControlledPortStatus change:
unauthorized
SYSLOG: <13> Jun 15 14:03:21 ICX-Switch MACAUTH: port 1/1/2 mac 0024.c442.bb24 vlan 2: Session is created
SYSLOG: <13> Jun 15 14:03:21 ICX-Switch MACAUTH: port 1/1/2 mac a036.9f6e.1fd0 vlan 2: Session is created
SYSLOG: <10> Jun 15 14:03:21 ICX-Switch MACAUTH: RADIUS server 10.176.166.60 Rejected for a036.9f6e.1fd0
SYSLOG: <13> Jun 15 14:03:21 ICX-Switch MACAUTH: Port 1/1/2 Mac a036.9f6e.1fd0 - received AAA-REJECT
SYSLOG: <13> Jun 15 14:03:21 ICX-Switch FLEXAUTH: Port 1/1/2 is added into Limited-Access Vlan 3 as mac-vlan
memberWarning: port 1/1/2 does not belong to vlan 3000
SYSLOG: <10> Jun 15 14:03:21 ICX-Switch MACAUTH: RADIUS server 10.176.166.60 Accepted for 0024.c442.bb24 with
(ST:3020399 T:3000 )
SYSLOG: <13> Jun 15 14:03:21 ICX-Switch MACAUTH: Port 1/1/2 Mac 0024.c442.bb24 - received AAA-ACCEPT
SYSLOG: <13> Jun 15 14:03:21 ICX-Switch FLEXAUTH: Port 1/1/2 is added into Dynamic Vlan 3000 as tagged member
SYSLOG: <13> Jun 15 14:03:23 ICX-Switch MACAUTH: port 1/1/2 mac 0024.c442.bb24 vlan 3000: Session is created
ICX-Switch#
ICX-Switch# show authentication sessions all

```

Port	MAC Addr	IP (v4/v6) Addr	User Name	VLAN	Auth Method	Auth State	ACL	Session Time	Age	PAE State
1/1/2	0024.c442.bb24	N/A	Jagadeesh Chandra	3000	MAUTH	Permit	None	36	Ena	N/A

Use Case 4: Authentication of an IP Phone and a PC on the Same Port Using Flexible Authentication

Switch Show Commands and Syslog Information

```

1/1/2 a036.9f6e.1fd0 N/A a0369f6e1fd0 3 MAUTH Restrict None 38 S2 N/A
ICX-Switch#
SYSLOG: <13> Jun 15 14:06:18 ICX-Switch DOT1X: Port 1/1/2 mac a036.9f6e.1fd0 vlan 4092: Session is cleared
[Termination-cause: Recv-802.1x-BPDU]
SYSLOG: <13> Jun 15 14:06:18 ICX-Switch MACAUTH: port 1/1/2 mac a036.9f6e.1fd0 vlan 3: restricted Session is
Cleared[Termination-Cause: Recv-802.1x-BPDU]
SYSLOG: <13> Jun 15 14:06:18 ICX-Switch FLEXAUTH: Port 1/1/2 is deleted from Limited-Access Vlan 3 as mac-vlan
member
SYSLOG: <14> Jun 15 14:06:19 ICX-Switch DOT1X: Port 1/1/2 - mac a036.9f6e.1fd0 AuthControlledPortStatus change:
unauthorized
SYSLOG: <10> Jun 15 14:06:35 ICX-Switch DOT1X: RADIUS server 10.176.166.60 Accepted for a036.9f6e.1fd0 with
(V4I:ac11 V4O: V6I:V6O: U:300 )
SYSLOG: <13> Jun 15 14:06:35 ICX-Switch DOT1X: Port 1/1/2 Mac a036.9f6e.1fd0 - received AAA-ACCEPT
SYSLOG: <13> Jun 15 14:06:35 ICX-Switch FLEXAUTH: Port 1/1/2 is added into Dynamic Vlan 300 as mac-vlan member
SYSLOG: <14> Jun 15 14:06:35 ICX-Switch DOT1X: Port 1/1/2 - mac a036.9f6e.1fd0, AuthControlledPortStatus
change: authorized
ICX-Switch#
ICX-Switch# show authentication sessions all
-----
Port      MAC              IP (v4/v6)      User              VLAN  Auth  Auth  ACL  Session  Age  PAE
  Addr                Addr              Name                Method  State  Time  Time  State
-----
1/1/2    0024.c442.bb24  10.176.167.235  Jagadeesh Chandra 3000  MAUTH Permit None   243     Ena  N/A
1/1/2    a036.9f6e.1fd0  10.176.167.171  jagadeesh.chandra 300   802.1X Permit Yes    67     Ena
AUTHENTICATED
ICX-Switch#
ICX-Switch# show authentication acls all
-----
Port      MAC Address      V4 Ingress      V4 Egress        V6 Ingress      V6 Egress
-----
1/1/2    0024.c442.bb24  -                -                 -                -
1/1/2    a036.9f6e.1fd0  ac11            -                 -                -
ICX-Switch#
ICX-Switch# show vlan 300
Total PORT-VLAN entries: 10
Maximum PORT-VLAN entries: 1024
Legend: [Stk=Stack-Id, S=Slot]
PORT-VLAN 300, Name [None], Priority level0, in single spanning tree domain
Untagged Ports: None
Tagged Ports: (U1/M1) 10
Mac-Vlan Ports: (U1/M1) 2
Monitoring: Disabled
ICX-Switch#
ICX-Switch# show vlan 3000
Total PORT-VLAN entries: 10
Maximum PORT-VLAN entries: 1024
Legend: [Stk=Stack-Id, S=Slot]
PORT-VLAN 3000, Name VOICE_VLAN, Priority level0, in single spanning tree domain
Untagged Ports: None
Tagged Ports: (U1/M1) 2 10
Mac-Vlan Ports: None
Monitoring: Disabled
ICX-Switch#
ICX-Switch# show lldp neighbors detail ports e 1/1/2
Local port: 1/1/2
Neighbor: 0024.c442.bb24, TTL 156 seconds
+ Chassis ID (network address): 10.176.167.235
+ Port ID (locally assigned): 808464948
+ Time to live: 180 seconds
+ Port description : "SW PORT"
+ System name : "SEP0024C442BB24.wwie.video54.local"
+ System description : "Cisco IP Phone 7965G,V5, SCCP45.9-1-1SR1S"
+ System capabilities : bridge, telephone
Enabled capabilities: bridge, telephone
+ Management address (IPv4): 10.176.167.235
+ 802.3 MAC/PHY : auto-negotiation enabled
Advertised capabilities: fdxSPause, fdxBPause, 1000BaseX-FD, 1000BaseT-HD
Operational MAU type : 1000BaseT-FD
+ MED capabilities: capabilities, networkPolicy, extendedPD, inventory
MED device type : Endpoint Class III
+ MED Network Policy
Application Type : Voice

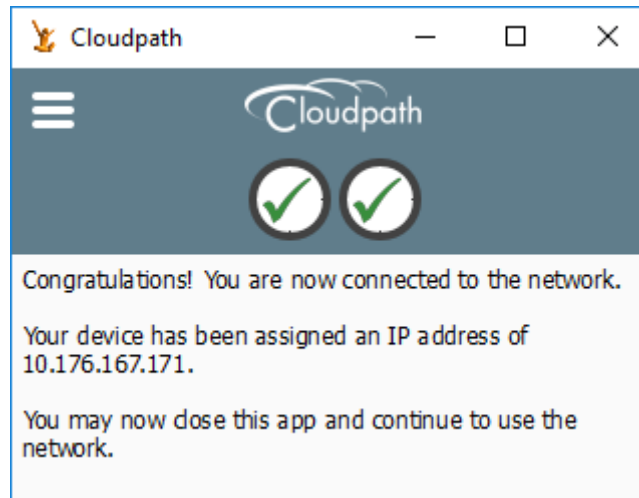
```

Use Case 4: Authentication of an IP Phone and a PC on the Same Port Using Flexible Authentication Cloudpath Information

```
Policy Flags      : Known Policy, Tagged
VLAN ID          : 3000
L2 Priority       : 5
DSCP Value       : 46
+ MED Network Policy
Application Type  : Voice Signaling
Policy Flags     : Known Policy, Tagged
VLAN ID         : 3000
L2 Priority      : 4
DSCP Value      : 32
+ MED Extended Power via MDI
Power Type       : PD device
Power Source     : Unknown Power Source
Power Priority    : Unknown
Power Value      : 12.0 watts (PSE equivalent: 13190 mWatts)
+ MED Hardware revision : "5"
+ MED Firmware revision : "tnp65.8-3-1-21a.bin"
+ MED Software revision : "SCCP45.9-1-1SR1S"
+ MED Serial number     : "FCH13078LY5"
+ MED Manufacturer     : "Cisco Systems, Inc."
+ MED Model name       : "CP-7965G"
+ MED Asset ID         : ""
```

Cloudpath Information

After the successful connection, the client PC is connected to the network.



1. On the Cloudpath server, navigate to **Dashboard > Connections** and click the magnifying glass symbol to view the connection details for both 802.1X authentication for the PC and MAC authentication for an IP phone.

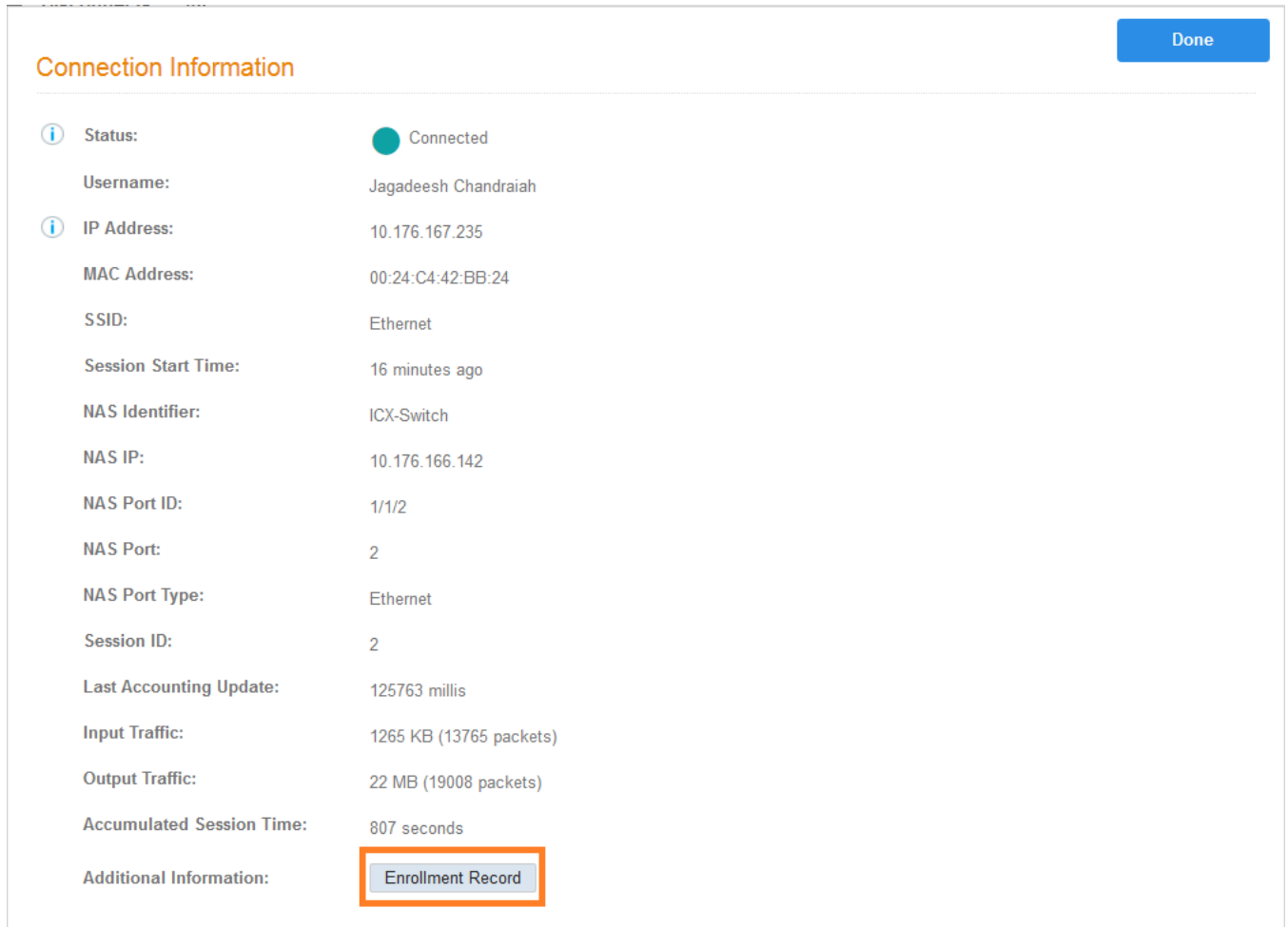
Dashboard

Show: **Connections** Disconnects All

Status	IP Address	MAC Address	Username	SSID	Duration
Connected	10.176.167.171	A0:36:9F:6E:1F:D0	jagadeesh.chandraiah@arris.com@employee.ruckuswireless.com	Ethernet	9 minutes ago
Connected	10.176.167.235	00:24:C4:42:BB:24	Jagadeesh Chandraiah	Ethernet	16 minutes ago

Results 1 - 2 of 2

FIGURE 11 Connection Information for an IP Phone



The screenshot displays a 'Connection Information' window with a 'Done' button in the top right corner. The window lists various session parameters for an IP phone. The 'Additional Information' field contains a button labeled 'Enrollment Record', which is highlighted with an orange border.

Field	Value
Status:	Connected
Username:	Jagadeesh Chandraiah
IP Address:	10.176.167.235
MAC Address:	00:24:C4:42:BB:24
SSID:	Ethernet
Session Start Time:	16 minutes ago
NAS Identifier:	ICX-Switch
NAS IP:	10.176.166.142
NAS Port ID:	1/1/2
NAS Port:	2
NAS Port Type:	Ethernet
Session ID:	2
Last Accounting Update:	125763 millis
Input Traffic:	1265 KB (13765 packets)
Output Traffic:	22 MB (19008 packets)
Accumulated Session Time:	807 seconds
Additional Information:	Enrollment Record

2. Click the enrollment record button to view more information.

The screenshot displays the Cloudpath Information web interface. On the left is a dark sidebar menu with the following items: Dashboard (dropdown), Welcome, Connections, **Enrollments** (highlighted in blue), Users & Devices, Certificates, DHCP Fingerprints, Notifications, Event Response, Configuration (dropdown), Sponsorship (dropdown), Certificate Authority (dropdown), Administration (dropdown), and Support (dropdown). At the bottom of the sidebar, it shows 'cloudpathsqa.wwie.video54.loc', 'Version 5.2.3761', and a notice about EULA agreement.

The main content area is titled 'Dashboard > Enrollments > View'. It features two sections:

- Enrollment Information:** A list of details for a specific enrollment record:
 - Enrollment Status: Completed
 - Name: Jagadeesh Chandraiah (with a user icon)
 - Email Address: jagadeesh.chandraiah@arris.com
 - Location: Sunnyvale
 - MAC Address: 00:24:C4:42:BB:24
 - Last Seen by MAC Auth: 20180508 0809 PDT
 - Notes: (with a pencil icon for editing)
- Connection Information:** A list of details for the current connection:
 - Connection State: **Connected**
 - Session Start Time: 17 minutes ago
 - Session Last Update: 145 seconds ago
 - WLAN Username: Jagadeesh Chandraiah
 - Session ID: 2
 - IP Address: 10.176.167.235
 - SSID: Ethernet
 - NAS Identifier: ICX-Switch (10.176.166.142)
 - NAS Port ID: 1/1/2
 - NAS Port Type: Ethernet
 - Input Traffic: 1265 KB (13765 packets)
 - Output Traffic: 22 MB (19008 packets)

FIGURE 12 Connection Information for the Client PC

Connection Information Done

Status:	● Connected
Username:	jagadeesh.chandraiah@arris.com@employee.ruckuswireless.com
IP Address:	10.176.167.171
MAC Address:	A0:36:9F:6E:1F:D0
SSID:	Ethernet
Session Start Time:	10 minutes ago
NAS Identifier:	ICX-Switch
NAS IP:	10.176.166.142
NAS Port ID:	1/1/2
NAS Port:	2
NAS Port Type:	Ethernet
Session ID:	1
Last Accounting Update:	295569 millis
Input Traffic:	1140 KB (12942 packets)
Output Traffic:	22 MB (18061 packets)
Accumulated Session Time:	315 seconds
Additional Information:	Enrollment Record

3. Click the enrollment record button to view more information.

Dashboard > Enrollments > View

Enrollment Information

Enrollment Status:	Certificate Issued	Block
Name:	jchandra@brocade.com	
Email Address:	jchandra@brocade.com	
Selections:	Employee - Employee	
Operating System:	Windows 10	
Browser:	Firefox	
Form Factor:	Computer	
MAC Address:	A0:36:9F:6E:1F:D0	
Language:	en-US,en;q=0.5	
Notes:		

Connection Information

Connection State:	Connected
Session Start Time:	25 minutes ago
Session Last Update:	5 minutes ago
WLAN Username:	jagadeesh.chandraiah@arris.com@employee.ruckuswireless.com
Session ID:	1
IP Address:	10.176.167.171
SSID:	Ethernet
NAS Identifier:	ICX-Switch (10.176.166.142)
NAS Port ID:	1/1/2
NAS Port Type:	Ethernet
Input Traffic:	1335 KB (15113 packets)

cloudpathsqa.wwie.video54.loc
Version 5.2.3764
Use of this website signifies your agreement to the EULA

Summary

The use cases can be implemented based on the network configuration and implementation designed by the administrator using Ruckus ICX devices and the Ruckus Cloudpath Enrollment System (ES).

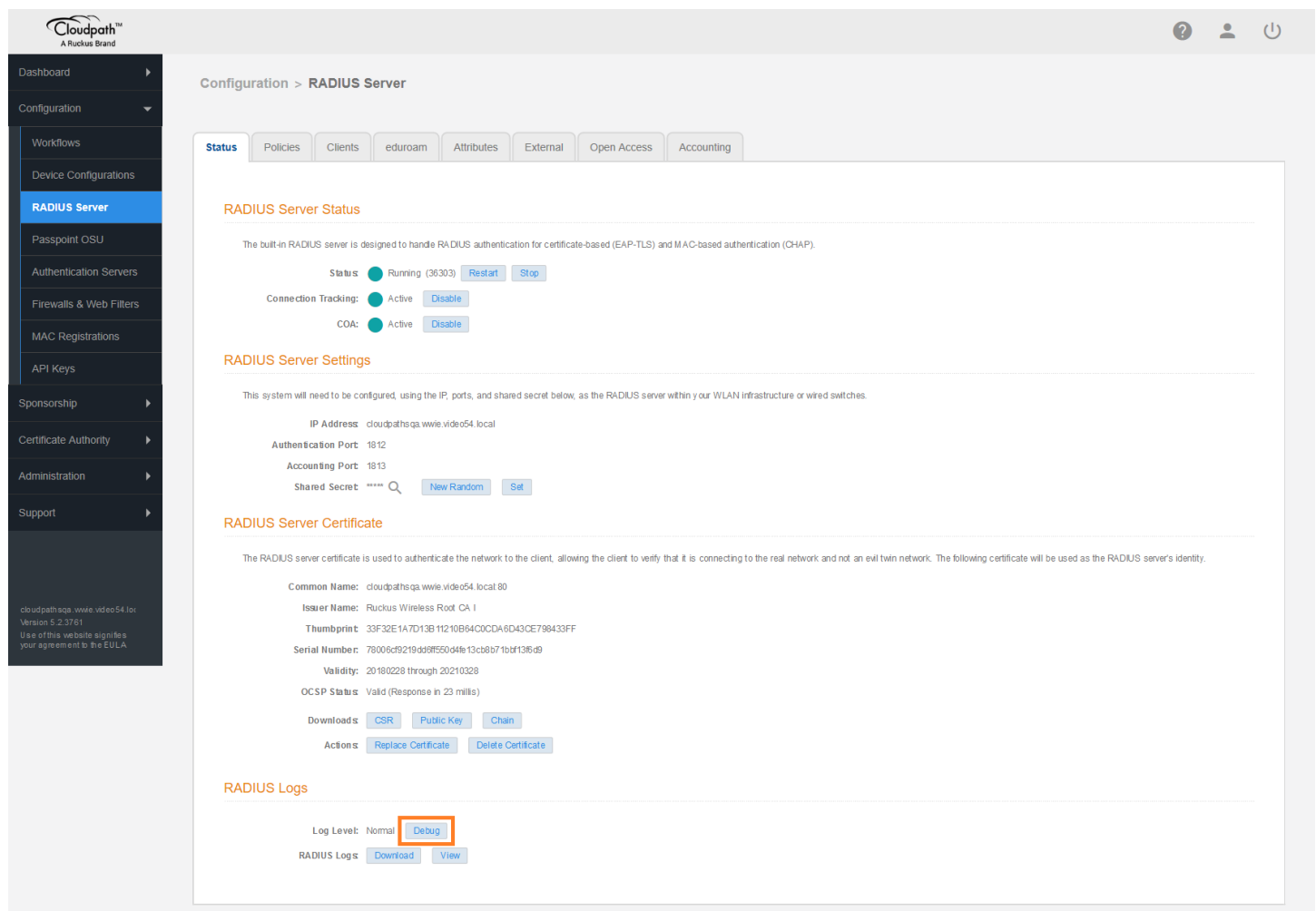
Troubleshooting

- Cloudpath RADIUS Server..... 69
- ICX Debugging..... 70

Cloudpath RADIUS Server

On the Cloudpath server, navigate to **Configuration > RADIUS Server** and click **Debug**.

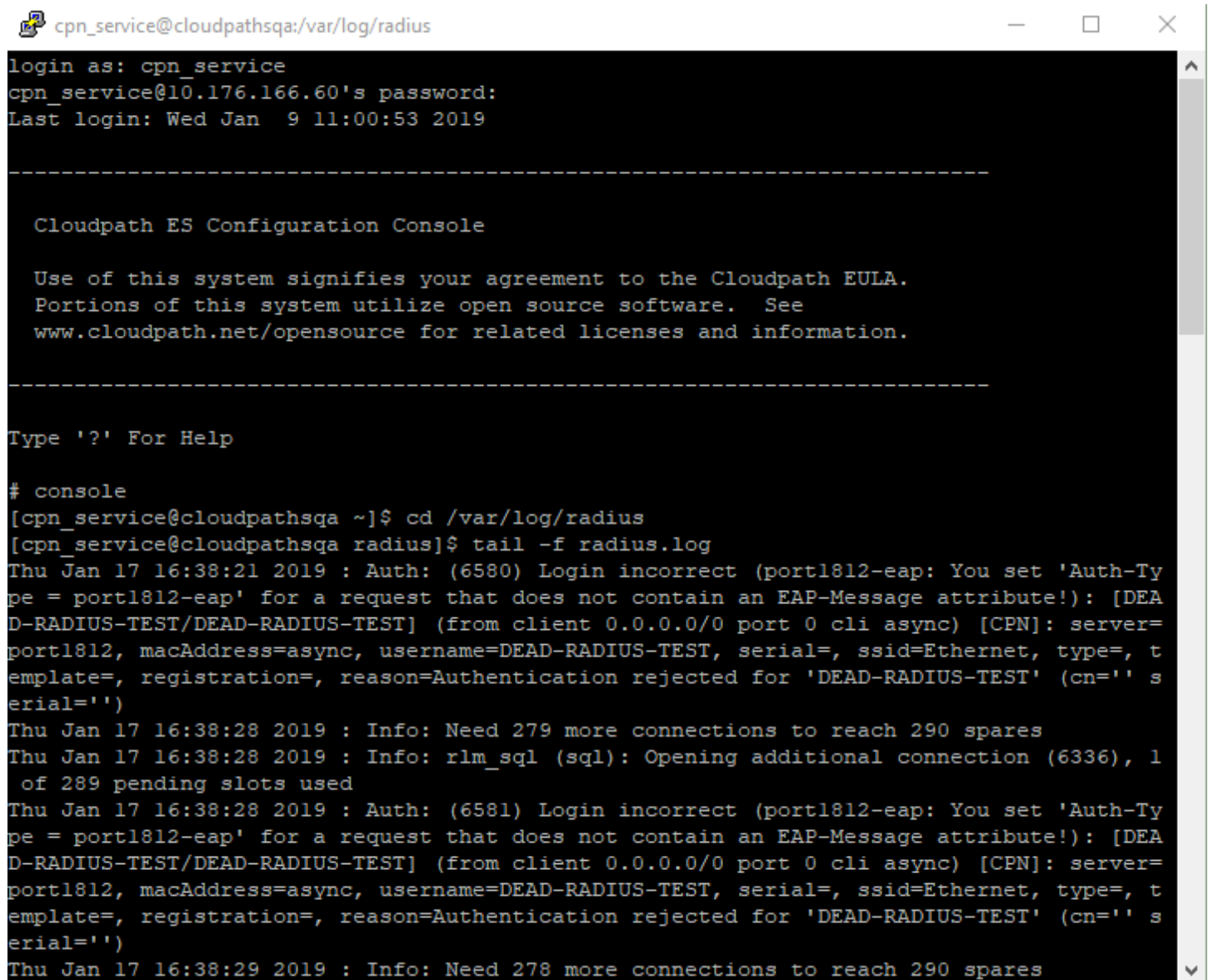
FIGURE 13 Debugging the Cloudpath RADIUS Server



Use SSH to connect to the Cloudpath server and enter the following commands for debugging.

```
# console
[cpn_service@cloudpathsqa ~]$ cd /var/log/radius
[cpn_service@cloudpathsqa radius]$ tail -f radius.log
```

FIGURE 14 Cloudpath ES Configuration Console



```
cpn_service@cloudpathsqa:/var/log/radius
login as: cpn_service
cpn_service@10.176.166.60's password:
Last login: Wed Jan  9 11:00:53 2019

-----

Cloudpath ES Configuration Console

Use of this system signifies your agreement to the Cloudpath EULA.
Portions of this system utilize open source software.  See
www.cloudpath.net/opensource for related licenses and information.

-----

Type '?' For Help

# console
[cpn_service@cloudpathsqa ~]$ cd /var/log/radius
[cpn_service@cloudpathsqa radius]$ tail -f radius.log
Thu Jan 17 16:38:21 2019 : Auth: (6580) Login incorrect (port1812-eap: You set 'Auth-Type = port1812-eap' for a request that does not contain an EAP-Message attribute!): [DEAD-RADIUS-TEST/DEAD-RADIUS-TEST] (from client 0.0.0.0/0 port 0 cli async) [CPN]: server=port1812, macAddress=async, username=DEAD-RADIUS-TEST, serial=, ssid=Ethernet, type=, template=, registration=, reason=Authentication rejected for 'DEAD-RADIUS-TEST' (cn=' serial='')
Thu Jan 17 16:38:28 2019 : Info: Need 279 more connections to reach 290 spares
Thu Jan 17 16:38:28 2019 : Info: rlm_sql (sql): Opening additional connection (6336), 1 of 289 pending slots used
Thu Jan 17 16:38:28 2019 : Auth: (6581) Login incorrect (port1812-eap: You set 'Auth-Type = port1812-eap' for a request that does not contain an EAP-Message attribute!): [DEAD-RADIUS-TEST/DEAD-RADIUS-TEST] (from client 0.0.0.0/0 port 0 cli async) [CPN]: server=port1812, macAddress=async, username=DEAD-RADIUS-TEST, serial=, ssid=Ethernet, type=, template=, registration=, reason=Authentication rejected for 'DEAD-RADIUS-TEST' (cn=' serial='')
Thu Jan 17 16:38:29 2019 : Info: Need 278 more connections to reach 290 spares
```

ICX Debugging

Configure the following commands for dead RADIUS server detection.

```
ICX-Switch# configure terminal
ICX-Switch(config)# radius-server test DEAD-RADIUS-TEST
ICX-Switch(config)# radius-server dead-time 1
ICX-Switch(config)# end
```

Commonly Used Show Commands

Use the **show radius servers** command to verify the current status of the linked RADIUS servers.

```
ICX-Switch# show radius servers
-----
Server                               Type      Opens    Closes   Timeouts  Status
-----
10.176.166.60                        any       6146     6148     13        active
Auth Servers: available
Acct Servers: available
```

Use the **show authentication sessions detail** command to verify the detailed description of authentication sessions.

```
ICX-Switch# show authentication sessions detail e 1/1/1
Auth Session Info (Port 1/1/1, MAC 0024.c442.bb24) :
  State           : Permitted
  Auth Method     : MAC-Auth
  VLAN Type      : Auth-Default-VLAN
  Voice VLAN     : 3000
  Tagged VLANs   : 3000
  User Name      : Jagadeesh Chandraiah
  Session Time   : 606
  Idle Timeout   : 120
  Acct session ID : 19
  PAE State      : N/A
  Qos Priority    : 0
  Auth Filter Applied : No
  VLAN Add Req State : Init
  Filter Add Req State : Complete
  Stale          : No
  802.1X Enabled : No
  V4 ACL Applied : Yes
  V4 IN ACL (Session) : acl1
  V6 IN ACL (Session) : -
  Client Voice Phone : Yes
  802.1X Capable  : Yes
  IP Addresses   : 10.176.167.237

  V4-IN ACL (Dynamic) : 3933
  V6-IN ACL (Dynamic) : 0
  V4-IN ACL RefCnt   : 1
  V6-IN ACL RefCnt   : 0
  V4 ACL Trap Rule   : Yes
  Addr Change Count  : 0
  Radius VLAN RefCnt : 0

  V4-OUT ACL (Dynamic) : 0
  V6-OUT ACL (Dynamic) : 0
  V4-OUT ACL RefCnt   : 0
  V6-OUT ACL RefCnt   : 0
  V6 ACL Trap Rule    : No
  MBV Usage Count     : 1

  Auth Order         : dot1x, mac-auth
  Auth Timeout Action : Failure
  SG Protection      : Disabled
  Reauthentication   : Disabled
  Reauth Timeout     : 300

  Auth Mode         : Single Untagged
  VLAN             : 2
  PVID             : 2
  Reauth Time      : 3019791
  Session Timeout  : 3020399
  PCE Index        : 1
  Age              : Enabled
  Failure Reason    :
  Tagged           : Yes
  VLAN Del Req State : Init
  Filter Del Req State : Init
  Delete Pending    : No
  Session Control   : Self
  V6 ACL Applied    : No
  V4 OUT ACL (Session) : -
  V6 OUT ACL (Session) : -
  Client Wireless AP : No

  Auth Fail Action   : Restricted VLAN (3)
  Aging              : Enabled
  DOS Protection     : Disabled (limit = 512)
  Reauth Period      : 15
  Max Ssessions      : 2
```

Commonly Used Debug Commands

ptrace aaa

Use the same command **ptrace aaa** to disable this functionality.

```
ICX-Switch# ptrace aaa
specified trace was turned ON
ICX-Switch# configure terminal
ICX-Switch(config)# int e 1/1/1
ICX-Switch(config-if-e1000-1/1/1)# enable
ICX-Switch(config-if-e1000-1/1/1)# end
ICX-Switch#Debug: Jan 17 17:26:53 Tracing the outgoing Radius Authentication packet..
Debug: Jan 17 17:26:53 UDP packet source IP=10.176.166.142, port=1406, destination IP=10.176.166.60, port=1812
Debug: Jan 17 17:26:53 Radius Header : ACCESS-REQ Identifier =21 Length = 120
```

Troubleshooting ICX Debugging

```
Authenticator (HEX):7A8126F7249CE1F76EBE21DA50942C0F
Attribute Type (Length) = User-Name ( 14) Value(ASCII) = 0024c442bb24
Attribute Type (Length) = User-Password ( 18) Value(HEX) = 360F3831B87534EBEED6650B4FCE1F2
Attribute Type (Length) = Service-Type ( 6) Value(ASCII) = Callcheck (MacAuth)
Attribute Type (Length) = Framed-MTU ( 6) Value(ASCII) = 1500
Attribute Type (Length) = NAS-IP-Address ( 6) Value(ASCII) = 10.176.166.142
Attribute Type (Length) = NAS-Port-Type ( 6) Value(ASCII) = Ethernet (FlexAuth)
Attribute Type (Length) = NAS-Port ( 6) Value(ASCII) = 1/1/1
Attribute Type (Length) = NAS-Port-Id ( 7) Value(ASCII) = 1/1/1
Attribute Type (Length) = NAS-Identifier ( 12) Value(ASCII) = ICX-Switch
Attribute Type (Length) = Calling-Station-Id ( 19) Value(ASCII) = 00-24-C4-42-BB-24
```

Debug: Jan 17 17:26:53 Tracing the received Radius packet..

Debug: Jan 17 17:26:53 Radius Header : ACCESS-ACPT Identifier =21 Length = 237

```
Authenticator (HEX):6E96874D0FCAD19920AAE43D1017EFBA
Attribute Type (Length) = Session-Timeout ( 6) Value(ASCII) = 3020399
Attribute Type (Length) = Reply-Message (131) Value(ASCII) = type=MacRegistration, mac=00:24:C4:42:BB:
24, registrationDb=IP Phone, registrationPk=361, enrollmentPk=986, registrationDbIndex=0
Attribute Type (Length) = User-Name ( 22) Value(ASCII) = Jagadeesh Chandraiah
Attribute Type (Length) = Tunnel-Type ( 6) Value(ASCII) = 13
Attribute Type (Length) = Tunnel-Medium-Type ( 6) Value(ASCII) = 6
Attribute Type (Length) = Tunnel-group-ID ( 8) Value(ASCII) = T:3000
Attribute Type (Length) = Fdry-Voice-Phone-Cfg ( 20) Value(ASCII) = dscp:46;priority:4
Attribute Type (Length) = Filter-ID ( 12) Value(ASCII) = ip.ac11.in
```

Warning: port 1/1/1 does not belong to vlan 3000

Debug: Jan 17 17:26:53 Tracing the outgoing Radius Accounting packet..

Debug: Jan 17 17:26:53 UDP packet source IP=10.176.166.142, port=1407, destination IP=10.176.166.60, port=1813

Debug: Jan 17 17:26:53 Radius Header : ACCT-REQ Identifier =22 Length = 132

```
Authenticator (HEX):5AE63FAB2914D15EA4E2BC3234F294D0
Attribute Type (Length) = User-Name ( 22) Value(ASCII) = Jagadeesh Chandraiah
Attribute Type (Length) = NAS-IP-Address ( 6) Value(ASCII) = 10.176.166.142
Attribute Type (Length) = NAS-Port-Type ( 6) Value(ASCII) = Ethernet (FlexAuth)
Attribute Type (Length) = NAS-Port ( 6) Value(ASCII) = 1/1/1
Attribute Type (Length) = NAS-Port-Id ( 7) Value(ASCII) = 1/1/1
Attribute Type (Length) = NAS-Identifier ( 12) Value(ASCII) = ICX-Switch
Attribute Type (Length) = Calling-Station-Id ( 19) Value(ASCII) = 00-24-C4-42-BB-24
Attribute Type (Length) = Acct-Status-Type ( 6) Value(ASCII) = Start
Attribute Type (Length) = Acct-Authentic ( 6) Value(ASCII) = RADIUS
Attribute Type (Length) = Service-Type ( 6) Value(ASCII) = Callcheck (MacAuth)
Attribute Type (Length) = Framed-MTU ( 6) Value(ASCII) = 1500
Attribute Type (Length) = Acct-Session-Id ( 4) Value(ASCII) = 20
Attribute Type (Length) = Acct-Delay-Time ( 6) Value(ASCII) = 0
```

Debug: Jan 17 17:26:53 Tracing the received Radius packet..

Debug: Jan 17 17:26:53 Radius Header : ACCT-RESP Identifier =22 Length = 20

```
Authenticator (HEX):6E690D221ABBAB235FF646635E228E30
```

Debug: Jan 17 17:27:01 Tracing the outgoing Radius Accounting packet..

Debug: Jan 17 17:27:01 UDP packet source IP=10.176.166.142, port=1408, destination IP=10.176.166.60, port=1813

Debug: Jan 17 17:27:01 Radius Header : ACCT-REQ Identifier =23 Length = 186

```
Authenticator (HEX):83920849054A433420DF15445557FA84
Attribute Type (Length) = User-Name ( 22) Value(ASCII) = Jagadeesh Chandraiah
Attribute Type (Length) = NAS-IP-Address ( 6) Value(ASCII) = 10.176.166.142
Attribute Type (Length) = NAS-Port-Type ( 6) Value(ASCII) = Ethernet (FlexAuth)
Attribute Type (Length) = NAS-Port ( 6) Value(ASCII) = 1/1/1
Attribute Type (Length) = NAS-Port-Id ( 7) Value(ASCII) = 1/1/1
Attribute Type (Length) = NAS-Identifier ( 12) Value(ASCII) = ICX-Switch
Attribute Type (Length) = Calling-Station-Id ( 19) Value(ASCII) = 00-24-C4-42-BB-24
Attribute Type (Length) = Acct-Status-Type ( 6) Value(ASCII) = Interim-Update
Attribute Type (Length) = Acct-Authentic ( 6) Value(ASCII) = RADIUS
Attribute Type (Length) = Acct-Input-Octets ( 6) Value(ASCII) = 8277332
Attribute Type (Length) = Acct-output-Octets ( 6) Value(ASCII) = 21429442
Attribute Type (Length) = Acct-Input-Packets ( 6) Value(ASCII) = 41886
Attribute Type (Length) = Acct-output-Packets ( 6) Value(ASCII) = 173068
Attribute Type (Length) = Tunnel-Type ( 6) Value(ASCII) = 13
Attribute Type (Length) = Tunnel-Medium-Type ( 6) Value(ASCII) = 6
Attribute Type (Length) = Tunnel-group-ID ( 6) Value(ASCII) = 3000
Attribute Type (Length) = Acct-Session-Time ( 6) Value(ASCII) = 7
Attribute Type (Length) = Framed-IP-Address ( 6) Value(ASCII) = 10.176.167.237
Attribute Type (Length) = Service-Type ( 6) Value(ASCII) = Callcheck (MacAuth)
Attribute Type (Length) = Framed-MTU ( 6) Value(ASCII) = 1500
```



```
Attribute Type (Length) = Acct-Session-Id      ( 4)  Value(ASCII) = 20
Attribute Type (Length) = Acct-Delay-Time     ( 6)  Value(ASCII) = 0
```

```
Debug: Jan 17 17:27:01 Tracing the received Radius packet..
Debug: Jan 17 17:27:01 Radius Header : ACCT-RESP Identifier =23 Length = 20
Authenticator (HEX):00959424FF55028321FC55E8AE0CDB36
```

```
ICX-Switch# ptrace aaa
specified trace was turned OFF
```

debug ip aaa

Use the **no** form of this command to disable this functionality.

```
ICX-Switch# debug ip aaa
IP: aaa debugging is on
ICX-Switch#Debug: Jan 17 17:28:27 AAA-FlexAuth:GET: AUTH session with portid=1/1/1 and
sessionid=[24c442,ffcb24] is not found
Debug: Jan 17 17:28:27 Extracted username=0024c442bb24 from EAP buffer.
Debug: Jan 17 17:28:27 AAA-FlexAuth (MAC-AUTH): Created a new session for MAC Authentication
Debug: Jan 17 17:28:27 AAA-FlexAuth:ADD: AUTH session with mac 0024.c442.bb24 portid=1/1/1 is added
Debug: Jan 17 17:28:27 Resetting RADIUS Client structure
Debug: Jan 17 17:28:27 RADIUS: Reset client 0, Session type 2, Total number of active clients=1
Debug: Jan 17 17:28:27 AAA: Open RADIUS UDP port
Debug: Jan 17 17:28:27 AAA-FlexAuth:CHECK: AUTH session with portid=1/1/1 and sessionid=[0,0] is found
Debug: Jan 17 17:28:27 AAA-FlexAuth:CHECK: AUTH session with portid=1/1/1 and sessionid=[0,0] is found
Debug: Jan 17 17:28:27 RADIUS message received from server of len 237.
Debug: Jan 17 17:28:27 Radius secret len 8, total len 237
Debug: Jan 17 17:28:27 BROCADE VSA - Voice Phone Field
Debug: Jan 17 17:28:27 RADIUS Timer cancelled for client 0.
Debug: Jan 17 17:28:27 RADIUS server ACCEPTed request
Debug: Jan 17 17:28:27 AAA-FlexAuth:CHECK: AUTH session with portid=1/1/1 and sessionid=[0,0] is found
Debug: Jan 17 17:28:27 AAA-FlexAuth: (MAC-AUTH) - Authentication successful for port 1/1/1 session
[24c442,ffcb24]. RADIUS 0/26
Debug: Jan 17 17:28:27 AAA-FlexAuth: Send response to port 1/1/1 VLAN 4092 sessId [24c442,ffcb24]
Debug: Jan 17 17:28:27 AAA-FlexAuth:DEL: AUTH session with portid=1/1/1 and sessionid=[24c442,ffcb24] client-
id 0 is deleted
Debug: Jan 17 17:28:27 Closing RADIUS UDP port
Debug: Jan 17 17:28:27 RADIUS: radius_authenticate_stop for client Idx 0. Actv Clients left 0
Debug: Jan 17 17:28:27 Resetting RADIUS Client structure
Warning: port 1/1/1 does not belong to vlan 3000
Debug: Jan 17 17:28:27 AAA-FlexAuth:GET: ACCT session with portid=1/1/1 and sessionid=[24c442,2bb24] is not
found
Debug: Jan 17 17:28:27 AAA-FlexAuth (MAC-AUTH): Created a new session for MAC Authentication
Debug: Jan 17 17:28:27 AAA-FlexAuth:ADD: ACCT session with mac 0024.c442.bb24 portid=1/1/1 is added
Debug: Jan 17 17:28:27 AAA-FlexAuth: DOT1X Accounting Starts...
Debug: Jan 17 17:28:27 Resetting RADIUS Client structure
Debug: Jan 17 17:28:27 RADIUS: Reset client 0, Session type 2, Total number of active clients=1
Debug: Jan 17 17:28:27 AAA: Open RADIUS UDP port
Debug: Jan 17 17:28:27 RADIUS message received from server of len 20.
Debug: Jan 17 17:28:27 Radius secret len 8, total len 20
Debug: Jan 17 17:28:27 RADIUS Timer cancelled for client 0.
Debug: Jan 17 17:28:27 RADIUS server ACCEPTed request
Debug: Jan 17 17:28:27 AAA-FlexAuth:CHECK: ACCT session with portid=1/1/1 and sessionid=[0,0] is found
Debug: Jan 17 17:28:27 AAA-FlexAuth: login Accounting status - accept.
Debug: Jan 17 17:28:27 AAA-FlexAuth: Send response to port 1/1/1 VLAN 2 sessId [24c442,2bb24]
Debug: Jan 17 17:28:27 Closing RADIUS UDP port
Debug: Jan 17 17:28:27 RADIUS: radius_authenticate_stop for client Idx 0. Actv Clients left 0
Debug: Jan 17 17:28:27 Resetting RADIUS Client structure
Debug: Jan 17 17:28:27 AAA-FlexAuth:DEL: ACCT session with portid=1/1/1 and sessionid=[24c442,2bb24] client-id
65535 is deleted
Debug: Jan 17 17:28:27 RADIUS: radius_authenticate_stop for client Idx 0 which is not in use
Debug: Jan 17 17:28:29 Resetting RADIUS Client structure
Debug: Jan 17 17:28:29 RADIUS: Reset client 240, Session type 5, Total number of active clients=1
Debug: Jan 17 17:28:29 Server Status: Send server probe for server with index 0, Client index 240
Debug: Jan 17 17:28:29 AAA: Open RADIUS UDP port
Debug: Jan 17 17:28:29 RADIUS message received from server of len 93.
Debug: Jan 17 17:28:29 Radius secret len 8, total len 93
Debug: Jan 17 17:28:29 RADIUS Timer cancelled for client 240.
Debug: Jan 17 17:28:29 RADIUS server REJECTed request
Debug: Jan 17 17:28:29 Closing RADIUS UDP port
```

Troubleshooting

ICX Debugging

```
Debug: Jan 17 17:28:29 RADIUS: radius_authenticate_stop for client Idx 240. Actv Clients left 0
Debug: Jan 17 17:28:29 Reseting RADIUS Client structure
Debug: Jan 17 17:28:35 AAA-FlexAuth:GET: ACCT session with portid=1/1/1 and sessionid=[24c442,bb8bb24] is not
found
Debug: Jan 17 17:28:35 AAA-FlexAuth:ADD: ACCT session with mac 0000.0000.0000 portid=1/1/1 is added
Debug: Jan 17 17:28:35 Reseting RADIUS Client structure
Debug: Jan 17 17:28:35 RADIUS: Reset client 0, Session type 2, Total number of active clients=1
Debug: Jan 17 17:28:35 AAA: Open RADIUS UDP port
Debug: Jan 17 17:28:35 RADIUS message received from server of len 20.
Debug: Jan 17 17:28:35 Radius secret len 8, total len 20
Debug: Jan 17 17:28:35 RADIUS Timer cancelled for client 0.
Debug: Jan 17 17:28:35 RADIUS server ACCEPTed request
Debug: Jan 17 17:28:35 AAA-FlexAuth:CHECK: ACCT session with portid=1/1/1 and sessionid=[0,0] is found
Debug: Jan 17 17:28:35 AAA-FlexAuth: logoff or Interim Accounting status - accept.
Debug: Jan 17 17:28:35 AAA-FlexAuth: Send response to port 1/1/1 VLAN 3000 sessId [24c442,bb8bb24]
Debug: Jan 17 17:28:35 AAA-FlexAuth:DEL: ACCT session with portid=1/1/1 and sessionid=[24c442,bb8bb24] client-
id 0 is deleted
Debug: Jan 17 17:28:35 Closing RADIUS UDP port
Debug: Jan 17 17:28:35 RADIUS: radius_authenticate_stop for client Idx 0. Actv Clients left 0
Debug: Jan 17 17:28:35 Reseting RADIUS Client structure
```

```
ICX-Switch# no debug ip aaa
IP: aaa debugging is off
```

debug coa

Use the **no** form of this command to disable this functionality.

```
ICX-Switch# debug coa
CoA message debug is enabled
ICX-Switch#Debug: Jan 17 17:30:21 RADIUS message received from DAC of len 62.Debug: Jan 17 17:30:21 Tracing the
packet
Code : 43 Identifier : 4 Length: 62
Authenticator Request :8B1F62BAC52A2AA95E4926D39D950857
Attribute: Type = 31 Length = 19 Value = 30 30 3A 32 34 3A 43 34 3A 34 32 3A 42 42 3A 32 34
Attribute: Type = 4 Length = 6 Value = 0A B0 A6 8E
Attribute: Type = 26 Length = 17 Value = 00 00 07 C7 0A 0B 66 6C 69 70 2D 70 6F 72 74

Debug: Jan 17 17:30:21 radius_coa_update_req_list : 4AA0B 4
Debug: Jan 17 17:30:21 radius_coa_update_req_list: Session 4AA0B not found operation: 4
Debug: Jan 17 17:30:21 Extract NAS identifier and session identifier
Debug: Jan 17 17:30:21 radius_coa_extract attributes returned with 0
Debug: Jan 17 17:30:21 radius_coa_update_req_list : 4AA0B 6
Debug: Jan 17 17:30:21 C5C8DF8 0 4 AA0B 0 0
Debug: Jan 17 17:30:21 -----NAS_Identifier-----
NAS IP Address: 10.176.166.142
NAS identifier:
NAS Ipv6 Address : ::
Debug: Jan 17 17:30:21 Session MAC-address: 0024.c442.bb24
Session Age : 0
ITC req. sent count : 0
ITC req. sending failed count :0
ITC res. received count :0
Num. of times reply resent :0
Response (1- ACK 0- NACK): 0
Session error (in case of NACK) : 0
Session- Id : 4AA0B
Identifier : 4
Code type : 43
Rem. Socket address: 10.176.166.60
Rem. Socket port : 43531
ACCT Session id : 0
Calling Station ID: 0024.c442.bb24
Username :
Cmd Type : 16
IPV4 ACL IN :
IPV4 ACL OUT :
IPV6 ACL IN :
IPV6 ACL OUT :
Debug: Jan 17 17:30:21 aaa_radius_find_next_session_based_on_mac : Found session for 0024.c442.bb24
Debug: Jan 17 17:30:21 aaa_radius_send_itc_msg: type = 0 mac = 0024.c442.bb24 port = 1/1/1
```

```
Debug: Jan 17 17:30:21 aaa_radius_find_next_session_based_on_mac : Found session for 0024.c442.bb24
Debug: Jan 17 17:30:21 aaa_radius_send_itc_msg: type = 0 mac = 0024.c442.bb24 port = 1/1/1
Debug: Jan 17 17:30:21 aaa_radius_find_next_session_based_on_mac : Not found session for 0024.c442.bb24
Debug: Jan 17 17:30:21 macauth_coa_msg_callback : Received CoA Req with cmd_type 16
Debug: Jan 17 17:30:21 radius_coa_update_req_list : 4AA0B 4
Debug: Jan 17 17:30:21 Found the session id 4AA0B
Debug: Jan 17 17:30:21 flexauth_coa_req_flip_port - 1/1/1
Debug: Jan 17 17:30:21 macauth_coa_msg_callback : Received CoA Req with cmd_type 16
Debug: Jan 17 17:30:21 radius_coa_update_req_list : 4AA0B 4
Debug: Jan 17 17:30:21 Found the session id 4AA0B
Debug: Jan 17 17:30:21 flexauth_coa_req_flip_port - 1/1/1
Debug: Jan 17 17:30:21 radius_coa_update_req_list : 4AA0B 4
Debug: Jan 17 17:30:21 Found the session id 4AA0B
Debug: Jan 17 17:30:21 radius_coa_update_req_list : 4AA0B 4
Debug: Jan 17 17:30:21 Found the session id 4AA0B
Debug: Jan 17 17:30:21 Sending ACK for code_type 43
Debug: Jan 17 17:30:21 radius_coa_update_req_list : 4AA0B 4
Debug: Jan 17 17:30:21 Found the session id 4AA0B
Debug: Jan 17 17:30:21 radius_coa_send_response:Sending IPv4 packet
Debug: Jan 17 17:30:21 radius_coa_send_response:Tracing the outgoing Radius Authentication packet..Debug: Jan
17 17:30:21 Tracing the packet
Code : 44 Identifier : 4 Length: 20
Authenticator Request :B3DAAB1CA0DA066E557A24EE1D5E7789
```

```
ICX-Switch# no debug coa
CoA message debug is disabled
```



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