

# Ruckus ICX Flexible Authentication with Cloudpath ES 5.0 Deployment Guide

Supporting FastIron 08.0.60

© 2017, Brocade Communications Systems, Inc. All Rights Reserved.

Brocade, the B-wing symbol, and MyBrocade are registered trademarks of Brocade Communications Systems, Inc., in the United States and in other countries. Other brands, product names, or service names mentioned of Brocade Communications Systems, Inc. are listed at [www.brocade.com/en/legal/brocade-Legal-intellectual-property/brocade-legal-trademarks.html](http://www.brocade.com/en/legal/brocade-Legal-intellectual-property/brocade-legal-trademarks.html). Other marks may belong to third parties.

Notice: This document is for informational purposes only and does not set forth any warranty, expressed or implied, concerning any equipment, equipment feature, or service offered or to be offered by Brocade. Brocade reserves the right to make changes to this document at any time, without notice, and assumes no responsibility for its use. This informational document describes features that may not be currently available. Contact a Brocade sales office for information on feature and product availability. Export of technical data contained in this document may require an export license from the United States government.

The authors and Brocade Communications Systems, Inc. assume no liability or responsibility to any person or entity with respect to the accuracy of this document or any loss, cost, liability, or damages arising from the information contained herein or the computer programs that accompany it.

The product described by this document may contain open source software covered by the GNU General Public License or other open source license agreements. To find out which open source software is included in Brocade products, view the licensing terms applicable to the open source software, and obtain a copy of the programming source code, please visit <http://www.brocade.com/support/oscd>.

# Contents

---

<b>Preface</b> .....	<b>5</b>
Introduction.....	5
Purpose of This Document.....	5
Audience.....	6
Related Documents.....	6
Document History.....	6
<b>Overview</b> .....	<b>7</b>
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.....	11
Configuring Cloudpath for RADIUS, HTTP, and Clients.....	12
<b>Use Case 1: Dynamic VLAN and ACL Assignment with MAC Authentication</b> .....	<b>17</b>
Cloudpath Configuration.....	18
Switch Configuration .....	24
Switch Show Commands and Syslog Information.....	25
Cloudpath Information.....	26
<b>Use Case 2: Dynamic VLAN and ACL Assignment with 802.1X Authentication</b> .....	<b>29</b>
Cloudpath Configuration.....	30
Switch Configuration .....	34
Switch Show Commands and Syslog Information.....	34
Cloudpath Information.....	35
<b>Use Case 3: Guest VLAN with External Captive Portal (Web Authentication)</b> .....	<b>39</b>
Cloudpath Configuration.....	40
Switch Configuration .....	41
Switch Show Commands and Syslog Information.....	42
Cloudpath Information.....	43
<b>Use Case 4: Authentication of an IP Phone and a PC on the Same Port Using Flexible Authentication</b> .....	<b>47</b>
Cloudpath Configuration.....	49
Switch Configuration .....	52
Switch Show Commands and Syslog Information.....	53
Cloudpath Information.....	55
MAC Authentication for an IP Phone.....	59
<b>Use Case 5: Authentication of a Phone, PC, and Guest User Using Flexible Authentication</b> .....	<b>61</b>
Cloudpath Configuration.....	63
Switch Configuration .....	64
Switch Show Commands and Syslog Information.....	66
Combined Output for Both Ports e 1/1/1 (PC1) and e 1/1/2 (PC2 Behind the IP Phone).....	67
Cloudpath Information.....	70
<b>Summary</b> .....	<b>83</b>



# 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 reduce authentication traffic, and provides 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 Brocade 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:

- Dynamic VLAN and ACL assignment with MAC authentication
- Dynamic VLAN and ACL assignment with 802.1X authentication
- Guest VLAN with external captive portal
- Authentication of a phone and a PC on the same port using Flexible Authentication
- Authentication of a phone, PC, and guest user 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

- *Brocade FastIron Security Configuration Guide, 08.0.60*  
<http://www.brocade.com/content/html/en/fastiron-os/08-0-60/fastiron-08060-securityguide/GUID-CA45229B-F8EE-4074-9175-046A1E3B1830-homepage.html>
- Cloudpath  
<https://www.ruckuswireless.com/products/smart-wireless-services/cloudpath>
- *Cloudpath ES 5.0 Deployment Guide*  
<https://support.ruckuswireless.com/documents/1279-cloudpath-es-5-0-ga-deployment-guide>
- Cloudpath Administrative Console  
<https://xpc.cloudpath.net/login.php>
- Cloudpath OVA Download  
[https://xpc.cloudpath.net/view\\_ova\\_download.php](https://xpc.cloudpath.net/view_ova_download.php)
- *Cloudpath Quick Start Guide*  
[https://xpc.cloudpath.net/documents/ES\\_QuickStartGuide.pdf](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>

## Document History

Date	Part Number	Description
June 8, 2017	53-1005026-01	Initial release.
June 15, 2017	53-1005026-02	Corrections to command examples.

# Overview

---

- 802.1X Authentication..... 7
- MAC Authentication..... 9
- Flexible Authentication..... 9
- How Flexible Authentication Works..... 9
- Platform Support for Flexible Authentication..... 11
- 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.

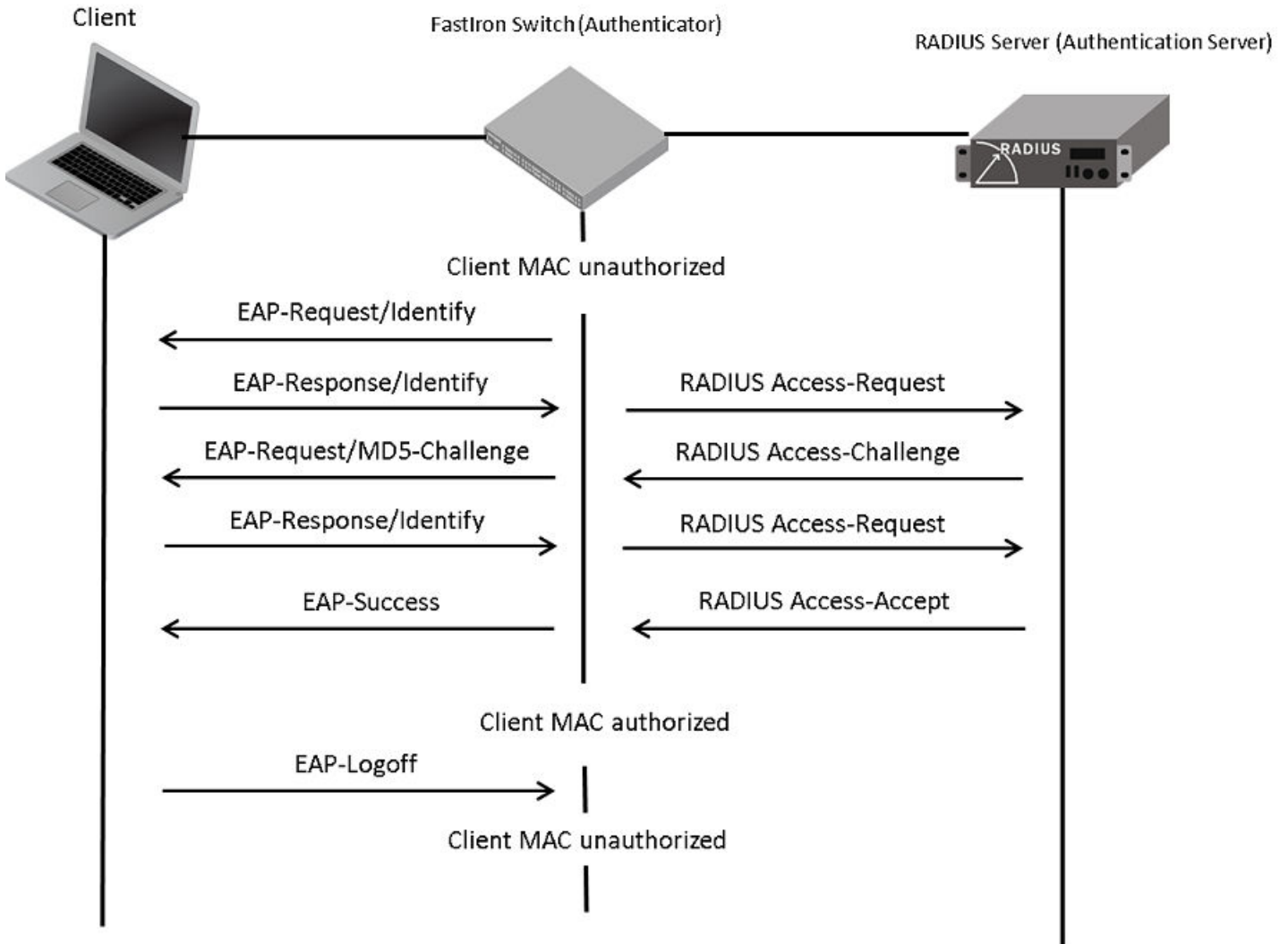
**Authenticator**—The device that controls access to the network. In an 802.1X configuration, the Brocade device serves as the authenticator. The authenticator passes messages between the client and the authentication server. Based on the identity information supplied by the client and the authentication 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. Brocade 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 *Brocade 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 Brocade 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 user'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 *Brocade FastIron Security Configuration Guide*.

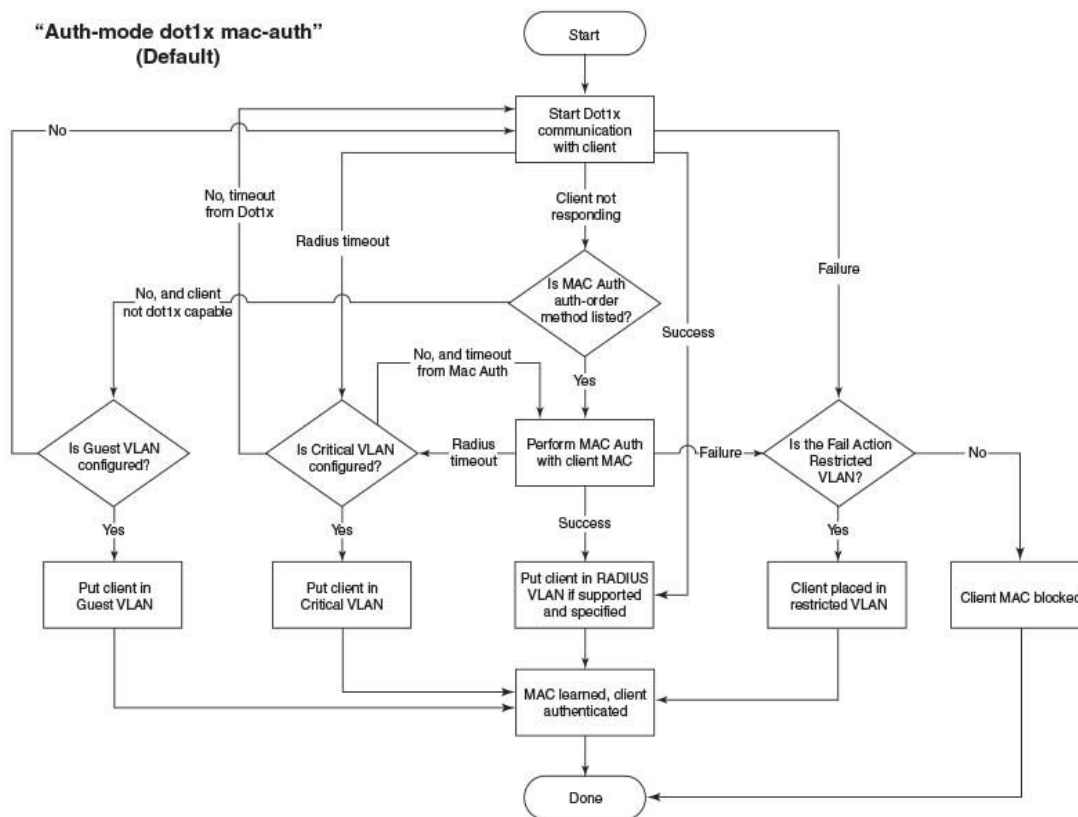
## Flexible Authentication

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 flow chart 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.

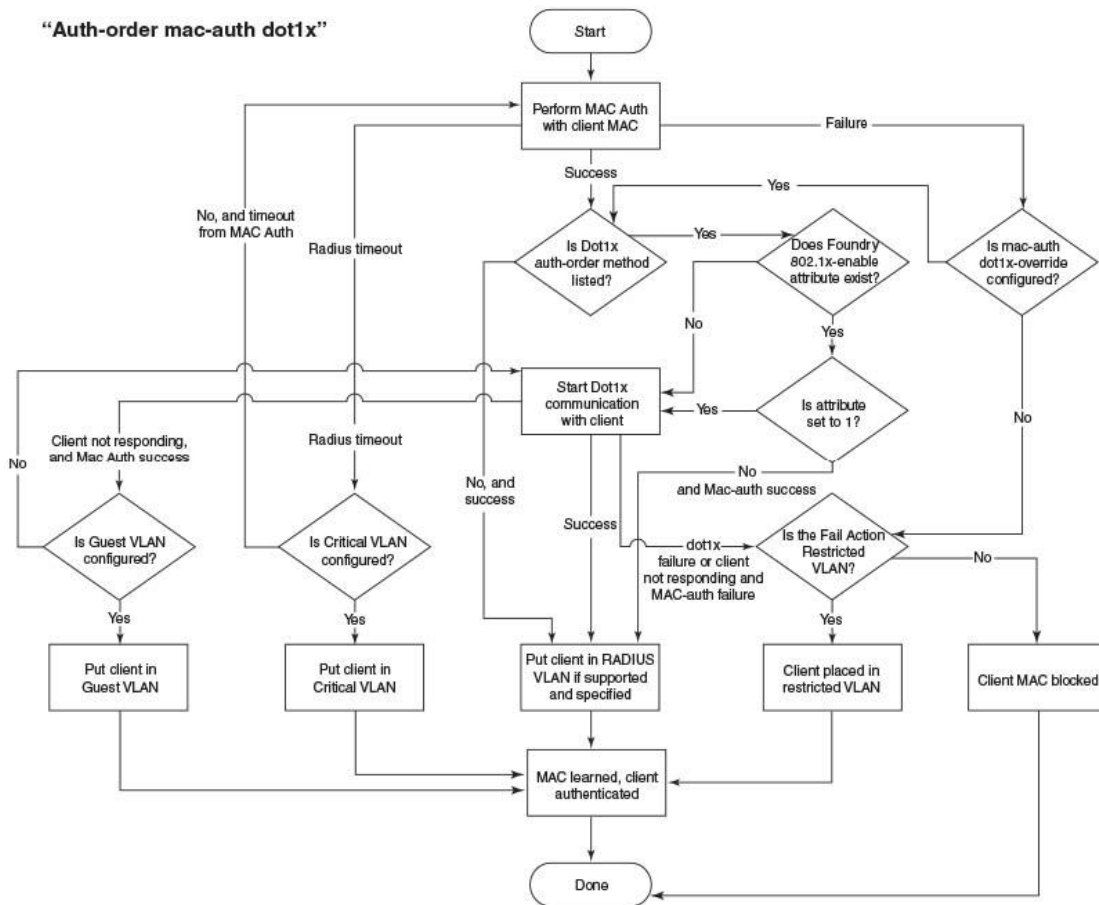
FIGURE 2 Default Sequence: 802.1X Followed by MAC Authentication



When the sequence is set to MAC authentication followed by 802.1X:

- MAC authentication is attempted first. If it succeeds, the 802.1X method is also attempted.
- If MAC authentication succeeds, the 802.1X process can be skipped by using a RADIUS vendor-specific attribute (VSA) called "Foundry-802\_1x-enable" for the MAC authentication process. If this attribute is present in the RADIUS Access-Accept message during MAC authentication and the value of this attribute is set to 1, 802.1X is not attempted for the client.
- If MAC authentication fails, 802.1X is not attempted and the configured failure action is taken. However, the administrator can configure the **dot1x-override** command to allow the clients that failed MAC authentication to authenticate by way of the 802.1X method.

FIGURE 3 MAC Authentication Followed by 802.1X



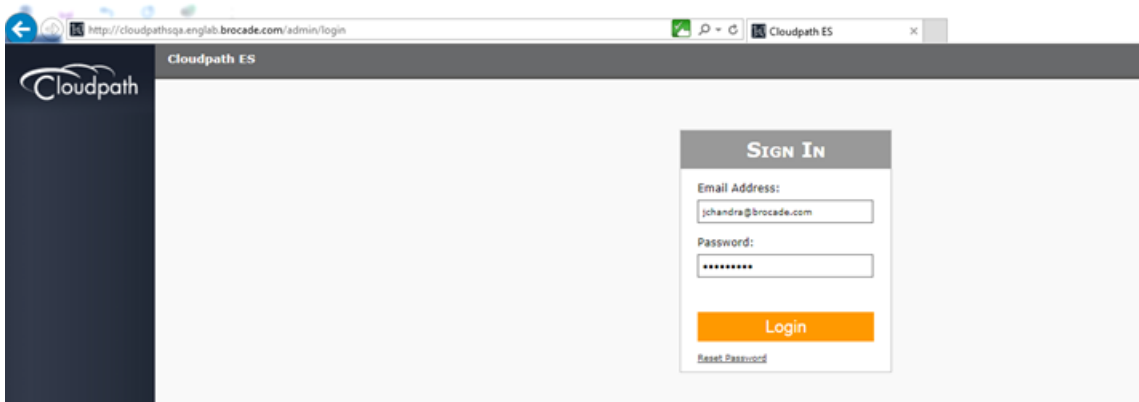
## Platform Support for Flexible Authentication

FastIron 08.0.60 supports Cloudpath with the following platforms:

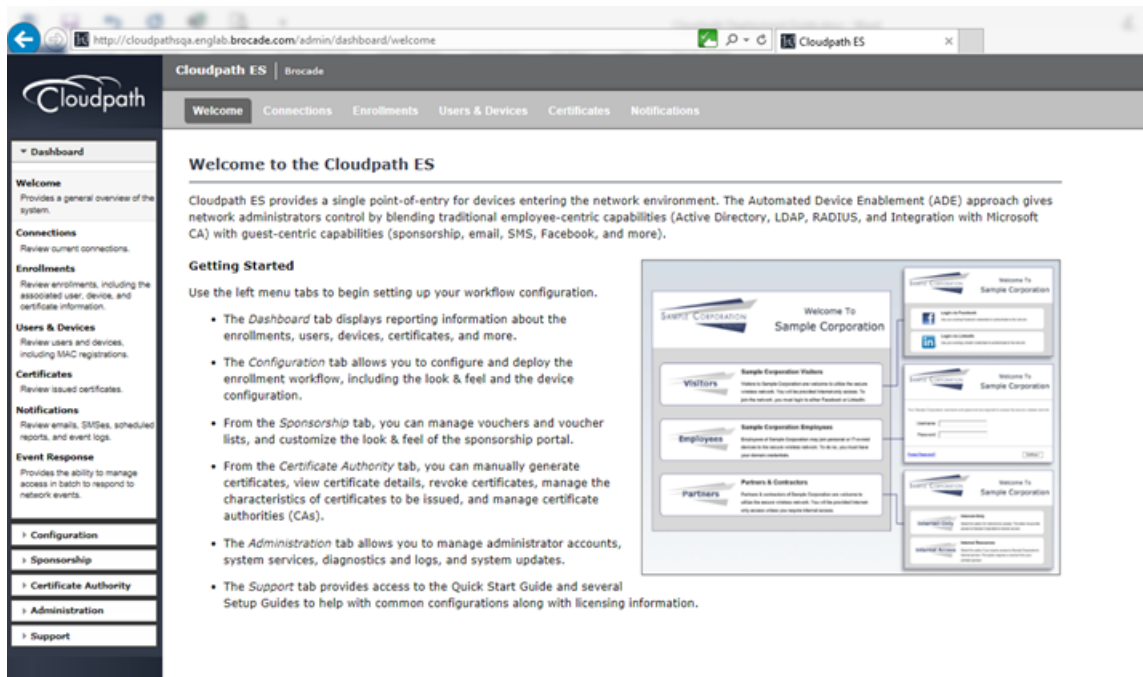
- ICX 7150
- ICX 7250
- ICX 7450
- ICX 7750

# Configuring Cloudpath for RADIUS, HTTP, and Clients

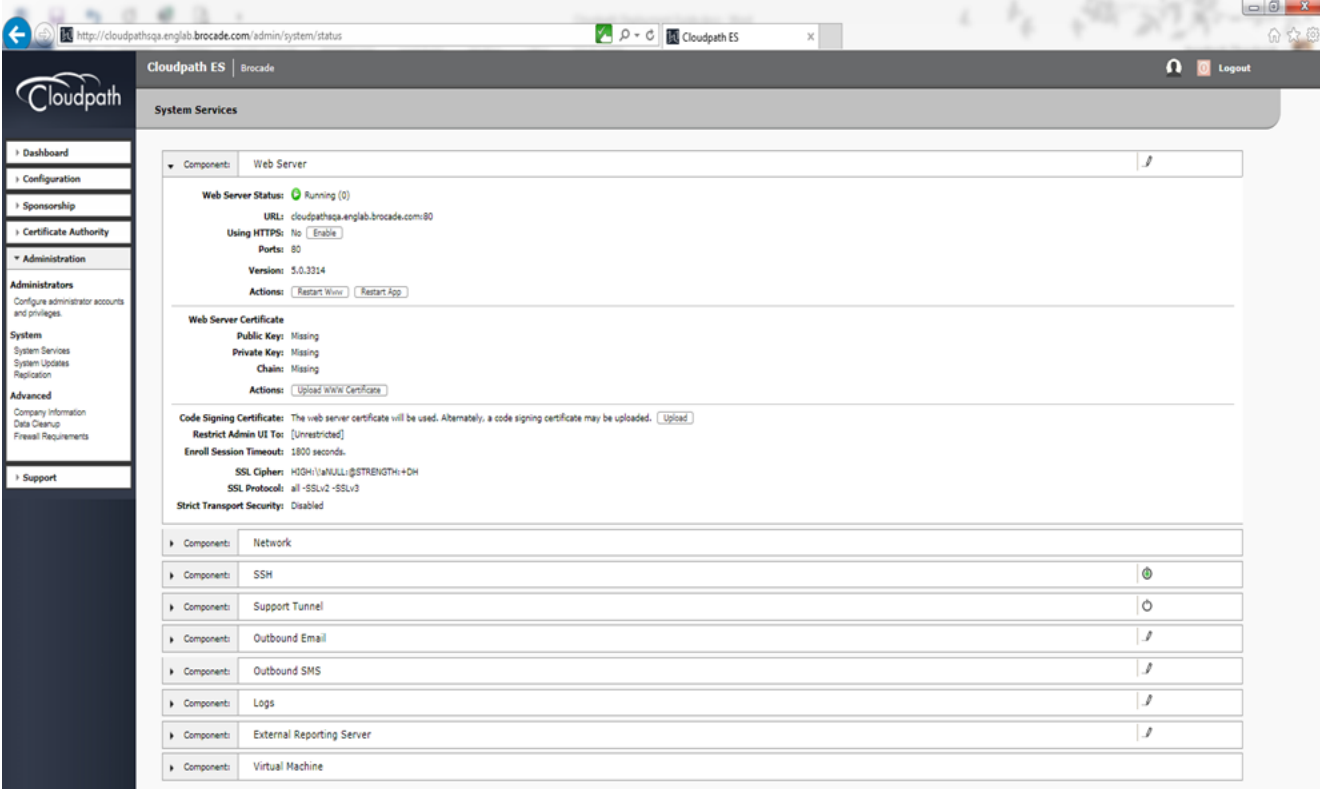
1. Log in to the Cloudpath server.



After login, the welcome page is displayed.



- 2. Navigate to **System Services** and check for the web server configuration. In this deployment guide, HTTP is used.



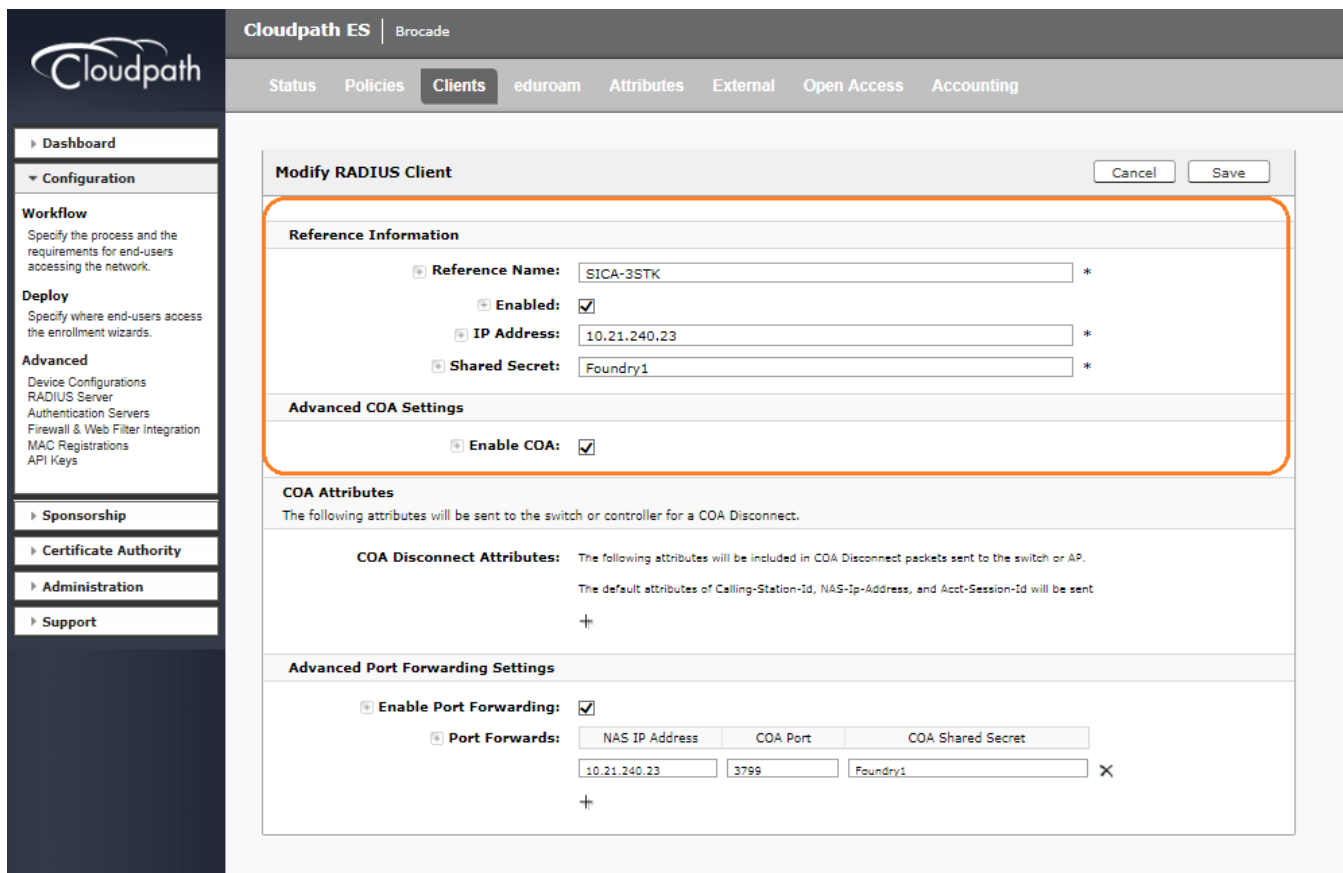
- Navigate to **Configuration > RADIUS Server > Status** and check for IP Address: cloudpathsqa.englab.brocade.com (Domain/IP address defined), Authentication Port 1812, Accounting Port 1813, and Shared Secret "Foundry1".

The screenshot displays the Cloudpath ES administration interface. The browser address bar shows the URL: `http://cloudpathsqa.englab.brocade.com/admin/aaa/status/`. The page title is "Cloudpath ES | Brocade". The navigation menu includes "Status", "Policies", "Clients", "eduroam", "Attributes", "External", "Open Access", and "Accounting". The left sidebar contains a "Configuration" menu with options like "Workflow", "Deploy", and "Advanced".

The main content area is titled "Onboard RADIUS Server" and is divided into four sections:

- RADIUS Server Status:** The built-in RADIUS server is designed to handle RADIUS authentication for certificate-based (EAP-TLS) and MAC-based authentication (CHAP). The status is "Running (29638)". Other settings include "Connection Tracking: Active" and "COA: Active".
- 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. The settings are:
  - IP Address: cloudpathsqa.englab.brocade.com
  - Authentication Port: 1812
  - Accounting Port: 1813
  - Shared Secret: \*\*\*\*\* (with a "New Random" button)
- RADIUS Server Certificate:** The RADIUS server certificate is used to authenticate the network to the client, allowing the client to verify that it is connecting to the real network and not an evil twin network. The following certificate will be used as the RADIUS server's identity.
  - Common Name: cloudpathsqa.englab.brocade.com
  - Issuer Name: Brocade Root CA I
  - Thumbprint: 5B7842A8F9B392D1103722ED1E4762F2E51418A9
  - Serial Number: 0503d59efa22ade58b16e8f4ce66c6ed9354c50a
  - Validity: 20161023 through 20211123
  - OCSP Status: Valid (Response in 10 millis)
  - Downloads: CSR, Public Key, Chain
  - Actions: Replace Certificate, Delete Certificate
- RADIUS Logs:** Log Level: Normal (with a "Debug" button). RADIUS Logs: Download, View

- Navigate to **Configuration > RADIUS Server > Clients** and add the NAS IP Address of the switch, the COA shared secret key, and enable the COA option if required.







# Use Case 1: Dynamic VLAN and ACL Assignment with MAC Authentication

- Cloudpath Configuration.....18
- Switch Configuration .....24
- Switch Show Commands and Syslog Information.....25
- Cloudpath Information.....26

The following example uses MAC authentication for authenticating a client and then dynamically assigns a VLAN and ACL after a successful authentication.

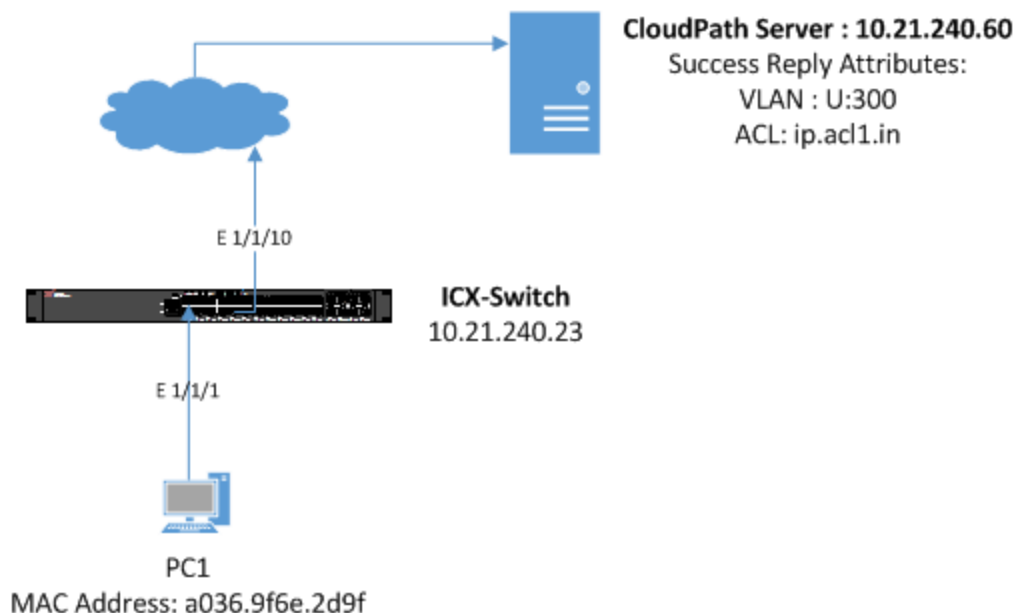
## Client PC1

- The MAC address is a036.9f6e.2d9f.
- After authentication:
  - The client should be placed in VLAN 300.
  - Incoming traffic from the client should be filtered by ACL "acl1".

## NOTE

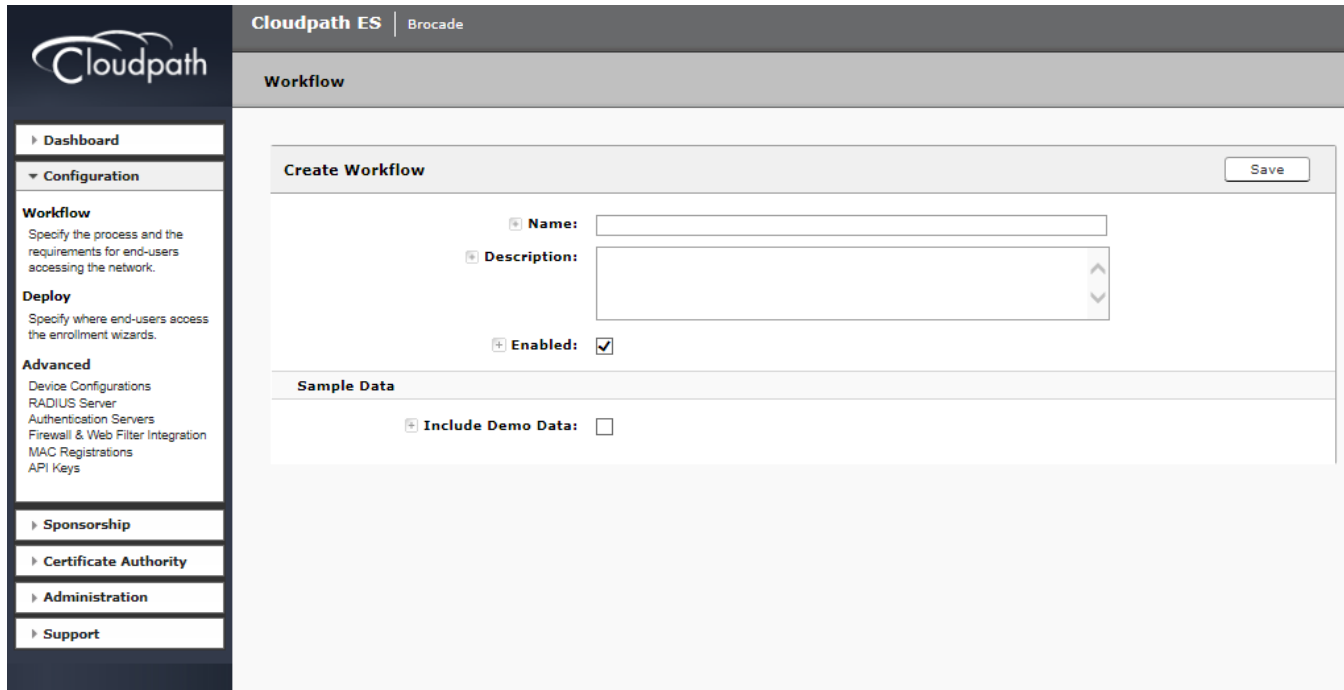
The administrator can apply a policy such as a VLAN, an ACL, or both from the RADIUS server depending on the network design and its implementation.

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

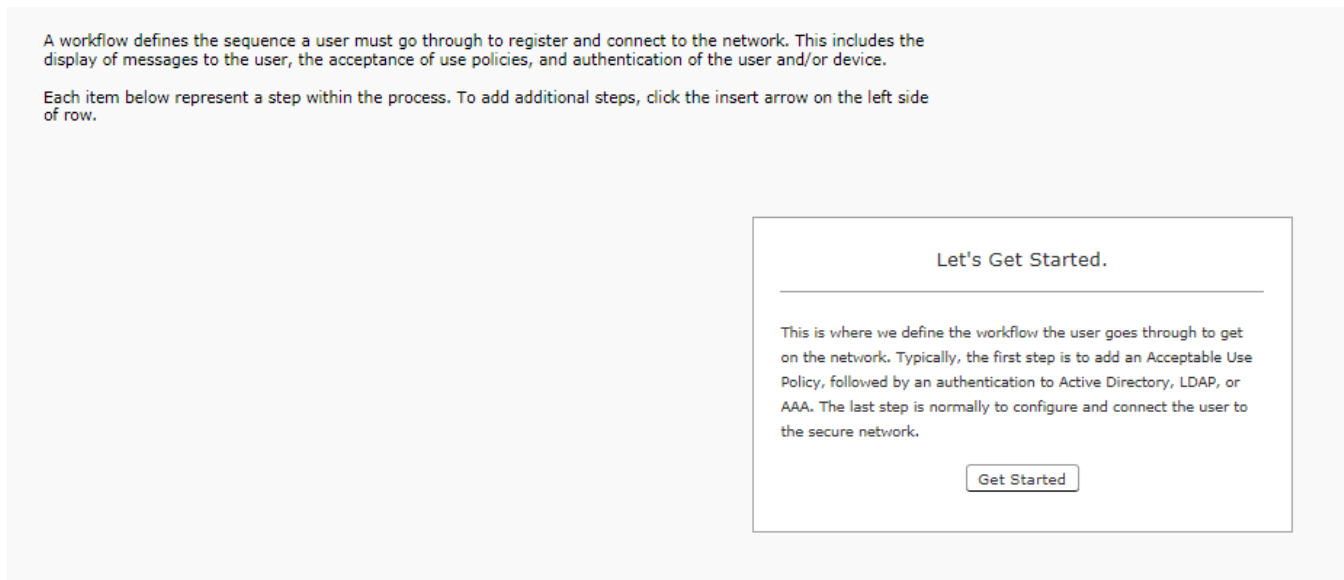


# Cloudpath Configuration

1. Navigate to **Configuration > Workflow**, and select + Add new workflow.



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



- Select the appropriate steps required to configure the workflow.

Cloudpath ES | Brocade

Workflow: Primary Workflow

Cloudpath

- ▶ Dashboard
- ▼ Configuration
- Workflow**  
Specify the process and the requirements for end-users accessing the network.
- Deploy**  
Specify where end-users access the enrollment wizards.
- Advanced**  
Device Configurations  
RADIUS Server  
Authentication Servers  
Firewall & Web Filter Integration  
MAC Registrations  
API Keys
- ▶ Sponsorship
- ▶ Certificate Authority
- ▶ Administration
- ▶ Support

cloudpath@englab.brocade.com  
jchandra@brocade.com  
Version 5.0.3314  
Use of this website signifies your agreement to the [EULA](#)

Cancel Next >

**What type of step should be added to the workflow?**

- 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, or a RADIUS server.
- 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.**

The workflow for registering the MAC address is displayed.

The screenshot shows the Cloudpath ES administration interface. The main content area displays a workflow configuration with the following steps:

- Step 1:** Require the user to accept the AUP Acceptable Use Policy
- Step 2:** All matches in: 802.1X, Mac-Auth, Webauth
- Step 3:** Prompt the user for credentials from Brocade DB
- Step 4:** Register the MAC address for Wired Mac Auth 1.
- Result:** Move user to Wired 3 Device Conf... and assign certificate using username@defaultcert....

The interface includes a left-hand navigation menu with sections like Dashboard, Configuration, Workflow, Deploy, and Advanced. The main area also contains a brief description of a workflow and instructions on how to add or modify steps.

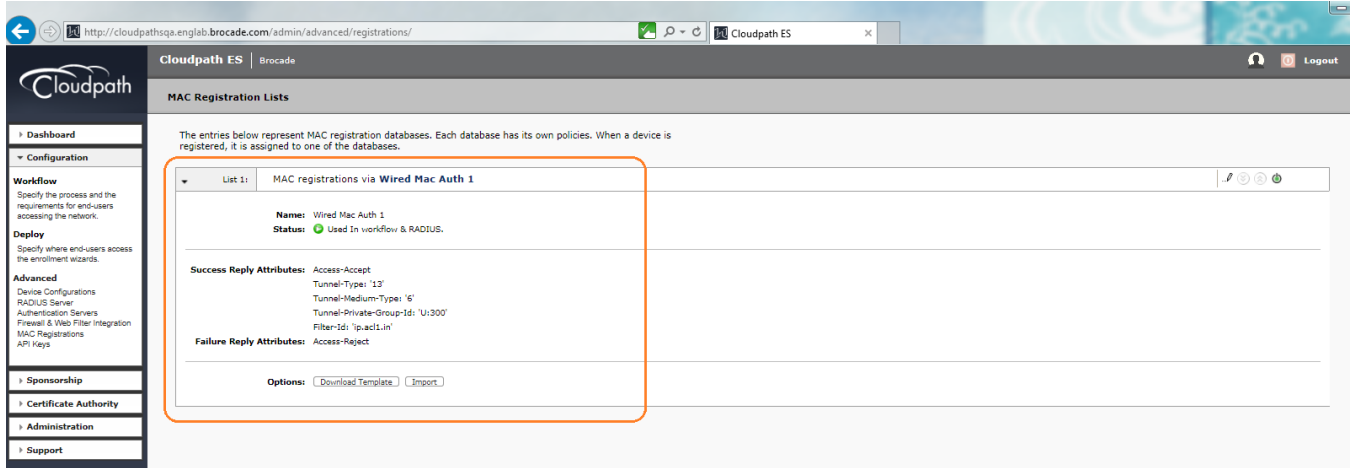
4. Modify the MAC registration by configuring the authentication success and failure reply attributes.

The screenshot displays the 'Modify MAC Registration' configuration page in the Cloudpath ES admin interface. The page is organized into three main sections:

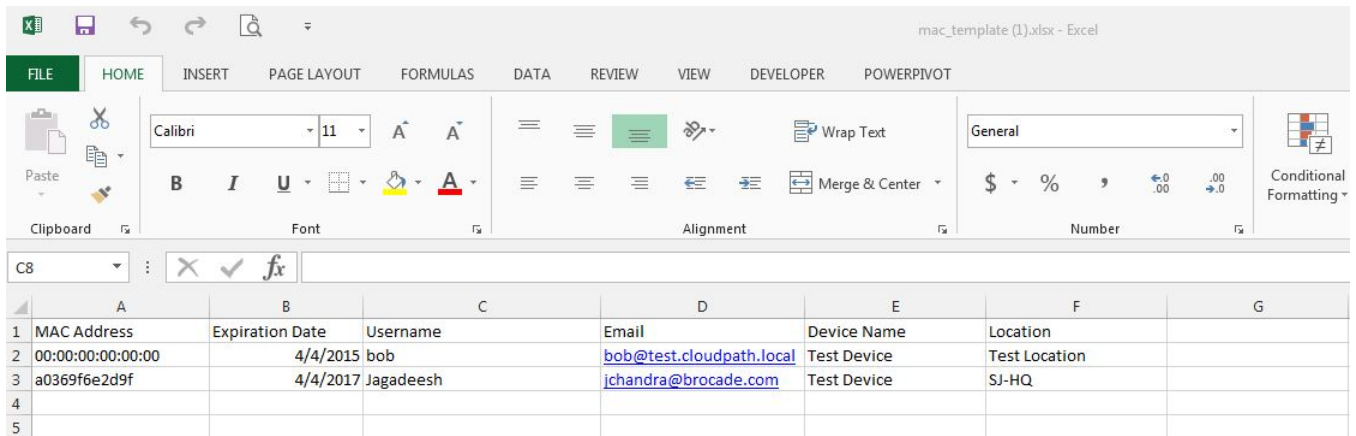
- Reference Information:** Contains a 'Name' field set to 'Wired Mac Auth 1' and an empty 'Description' text area.
- Registration Information:** Contains several configuration options:
  - SSID Regex:** Set to '\*'
  - Expiration Date Basis:** Set to 'Days After' with a dropdown arrow.
  - Offset:** Set to '1'
  - Behavior:** Set to 'Always redirect to authenticate user.' with a dropdown arrow.
  - Config Shortcuts:** A row of buttons for 'Ruckus SZ HTTP', 'Ruckus ZD HTTP', 'Cisco HTTP', 'Aruba HTTP', and 'Aerohive HTTP', followed by another row for 'Ruckus SZ HTTPS', 'Ruckus ZD HTTPS', 'Cisco HTTPS', 'Aruba HTTPS', and 'Aerohive HTTPS'.
  - Redirect URL:** A text area containing '[ex. https://wlan.company.com]'.
  - Use POST:** An unchecked checkbox.
  - POST Parameters:** A text area containing '[ex. username=bob]'.
  - Allow Continuation:** A checked checkbox.
  - Kill Session:** A checked checkbox.
- Authentication Attributes:**
  - Success Reply Attributes:** A descriptive text followed by a list of attribute-value pairs: 'Tunnel-Type (integer): 13', 'Tunnel-Medium-Type (integer): 6', 'Tunnel-Private-Group-Id (string): U:300', and 'Filter-Id (string): ip.acl1.in'. Each entry has a dropdown menu, an 'Add Or Repl' button, and a delete 'X' icon.
  - Failure Reply Attributes:** A descriptive text.

At the bottom left of the interface, there is contact information for Cloudpath ES: cloudpathsqa.englab.brocade.com, jchandra@brocade.com, Version 5.0.3314, and a note about the site's use and agreement to the SLA.

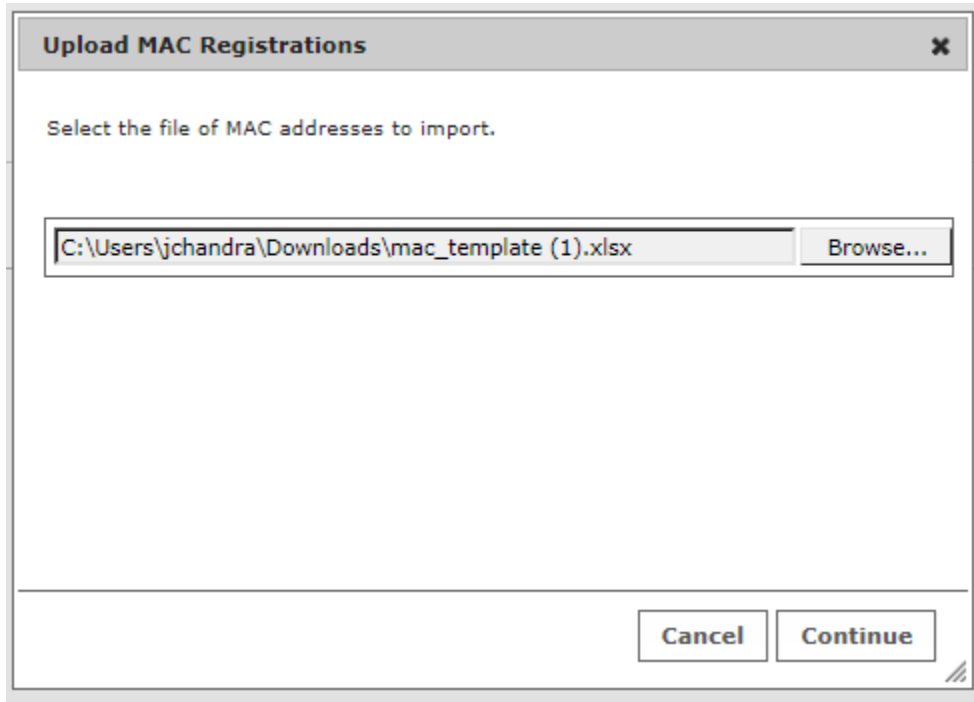
- Navigate to **Configuration > MAC Registrations** to view the configured success and failure attributes.



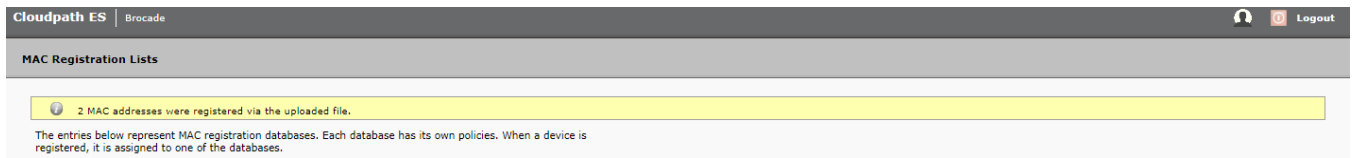
- Navigate to **Configuration > MAC Registrations > Options**, click **Download Template**, and add the MAC addresses of the clients and the expiration dates for those clients.



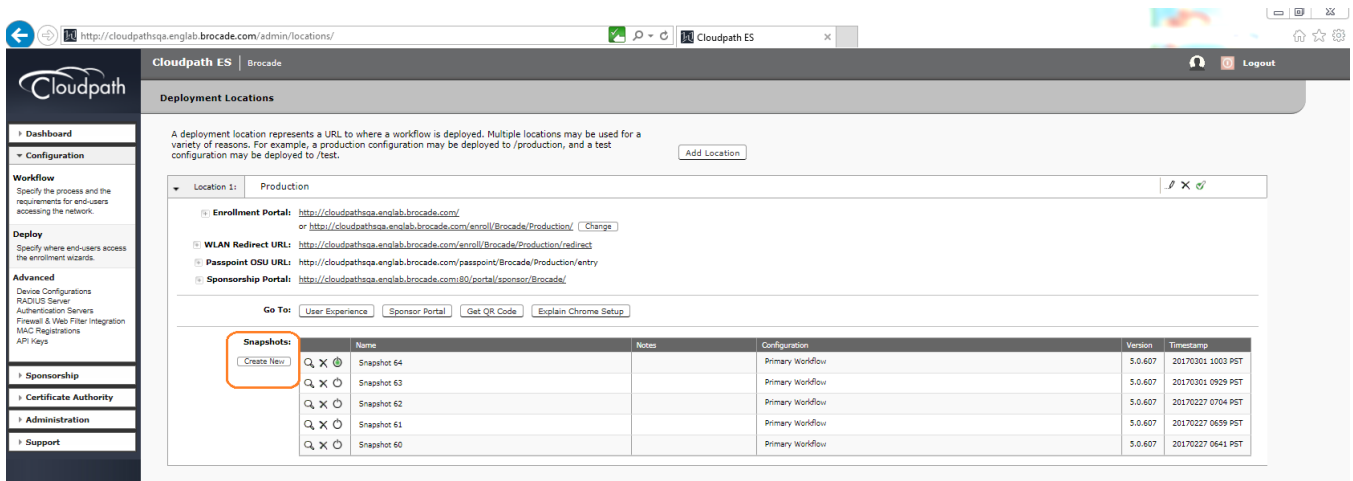
7. Import the updated template.



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



8. After allowing any changes in Cloudpath to take effect, navigate to **Configuration > Deploy > Create**.



## 9. Create a new snapshot.

**Create New Snapshot?** ✕

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

**Workflow:** Primary Workflow ▼

**Wizard Version:** 5.0.607 (Newest) ▼

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.englab.brocade.com/enroll/Brocade/Production/>

Remove oldest inactive snapshot if 5 exist.

Cancel
Create

## Switch Configuration

```

!
vlan 2 name AUTH-DEFAULT by port
!
vlan 300 name MAC-AUTH 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
radius-server host 10.21.240.60 auth-port 1812 acct-port 1813 default key Foundry1 dot1x mac-auth web-auth
!
ip access-list extended acl1
  permit ip any any
!

```



# Switch Show Commands and Syslog Information

```
ICX-Switch#
SYSLOG: <14> Mar  1 17:36:25 ICX-Switch System: Interface ethernet 1/1/1, state up
SYSLOG: <13> Mar  1 17:36:26 ICX-Switch MAC Authentication succeeded for [a036.9f6e.2d9f ] on port 1/1/1
SYSLOG: <13> Mar  1 17:36:26 ICX-Switch FLEXAUTH: Port ethe 1/1/1  is added into VLAN 300 as MAC-VLAN member
SYSLOG: <13> Mar  1 17:36:26 ICX-Switch FLEXAUTH: Port ethe 1/1/1  is deleted from VLAN 2 as MAC-VLAN member
```

```
ICX-Switch#show mac-auth sessions all
```

Port	MAC Addr	IP (v4/v6) Addr	VLAN	Auth State	ACL	Session Time	Age
1/1/1	a036.9f6e.2d9f	10.21.80.226	300	Yes	Yes	6	Ena

```
ICX-Switch#show vlan 300
Total PORT-VLAN entries: 7
Maximum PORT-VLAN entries: 64
```

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

```
PORT-VLAN 300, Name MAC-AUTH, Priority level0, Spanning tree Off
Untagged Ports: None
Tagged Ports: (U1/M1)  10
Uplink Ports: None
DualMode Ports: None
Mac-Vlan Ports: (U1/M1)  1
Monitoring: Disabled
```

```
ICX-Switch#show mac-authentication ip-acl all
```

Port	MAC Address	V4 Ingress	V4 Egress	V6 Ingress	V6 Egress
1/1/1	a036.9f6e.2d9f	acl1	-	-	-

# Cloudpath Information

1. Navigate to **Dashboard > Users & Devices** and click **MAC Registrations** to verify the MAC authentication.

The screenshot shows the Cloudpath ES admin interface. The main content area is titled "MAC Registrations" and contains a table with the following data:

	Status	MAC Address	Username	Registration Date	Expiration Date	Registration List
Q	Active	A0:36:9F:6E:2D:9F	jchandra@brocade.com	20170301 1232 PST	20170404 0000 PDT	Wired Mac Auth 1
Q	Active	00:24:C4:42:8B:24	0024c4428b24	20170213 2036 PST	20200405 0700 PDT	Wired Mac Auth 1
Q	Active	A0:36:9F:6E:2D:9F	a0369f6e2d9f	20170213 2022 PST	20200405 0700 PDT	Wired Mac Auth 1
Q	Active	00:24:C4:42:8B:24	0024c4428b24	20170213 2022 PST	20200405 0700 PDT	Wired Mac Auth 1
Q	Active	00:24:C4:42:8B:24	0024c4428b24	20170213 2018 PST	20200405 0700 PDT	Wired Mac Auth 1
Q	Active	A0:36:9F:6E:2A:58	a0369f6e2a58	20161228 2011 PST	20200405 0700 PDT	Wired Mac Auth 1
Q	Active	A0:36:9F:6E:1F:DD	a0369f6e1fdd	20161228 2011 PST	20200405 0700 PDT	Wired Mac Auth 1
Q	Active	A0:36:9F:6E:2D:9F	a0369f6e2d9f	20161228 2011 PST	20200405 0700 PDT	Wired Mac Auth 1
Q	Active	A0:36:9F:6E:1F:DD	a0369f6e1fdd	20161220 2311 PST	20200405 0700 PDT	Wired Mac Auth 1
Q	Active	A0:36:9F:6E:2D:9F	a0369f6e2d9f	20161220 2311 PST	20200405 0700 PDT	Wired Mac Auth 1
Q	Active	A0:36:9F:6E:1F:DD	a0369f6e1fdd	20161217 0121 PST	20200405 0700 PDT	Wired Mac Auth 1
Q	Active	A0:36:9F:6E:2D:9F	a0369f6e2d9f	20161217 0121 PST	20200405 0700 PDT	Wired Mac Auth 1
Q	Active	A0:36:9F:6E:1F:DD	jchandra@brocade.com	20161217 0120 PST	20200405 0700 PDT	Wired Mac Auth 1
Q	Active	A0:36:9F:6E:2D:9F	jchandra@brocade.com	20161217 0120 PST	20200405 0700 PDT	Wired Mac Auth 1
Q	Active	A0:36:9F:6E:1F:DD	jchandra@brocade.com	20161217 0115 PST	20200405 0700 PDT	Wired Mac Auth 1

At the bottom of the table, it says "Results 1 - 15 of 16." The sidebar on the left includes sections for Dashboard, Welcome, Connections, Enrollments, Users & Devices, Certificates, Notifications, Event Response, Configuration, Sponsorship, Certificate Authority, Administration, and Support.

2. Click the search button of the MAC address to view MAC registration details.

The screenshot shows the Cloudpath ES administration console. The main content area displays the details for a specific MAC registration. The interface is organized into several sections:

- MAC Registration Information:**
  - Status: Valid through 20170404 0000 PDT (Revoked)
  - MAC Address: A0:36:9F:6E:2D:9F
  - Username: jchandra@brocade.com
  - Location: SJ-HQ
  - SSID(s):
  - Registration Date: 20170301 1232
  - Expiration Date: 20170404 0000
  - Last Seen Timestamp: 20170301 1237
- Identity Information:**
  - Username: jchandra@brocade.com
  - Email: jchandra@brocade.com
  - Blocked Status: No (Block)
  - Distinguished Name: type=admin, cn=jchandra@brocade.com
  - Authentication Server: Brocade DB
- Device Information:**
  - Device Name: Test Device
- All Registrations By MAC Address:** A table listing various registration records.

Status	Registration List	MAC Address	Username	Creation Date	Expiration Date	Last Seen	Permitted SSID(s)
Valid through 20170404 0000 PDT	Wired Mac Auth 1	A0:36:9F:6E:2D:9F	jchandra@brocade.com	20170301 1232 PST	20170404 0000 PDT	20170301 1237 PST	
Valid through 20200405 0700 PDT	Wired Mac Auth 1	A0:36:9F:6E:2D:9F	a0369fa289f	20170213 2022 PST	20200405 0700 PDT	20170227 0634 PST	
Valid through 20200405 0700 PDT	Wired Mac Auth 1	A0:36:9F:6E:2D:9F	a0369fa289f	20161228 2011 PST	20200405 0700 PDT	20170213 2019 PST	
Expired on 20161221 2334 PST	Wired Mac Auth 1	A0:36:9F:6E:2D:9F	jchandra@brocade.com	20161220 2334 PST	20161221 2334 PST	20161220 2337 PST	
Expired on 20161221 2313 PST	Wired Mac Auth 1	A0:36:9F:6E:2D:9F	jchandra@brocade.com	20161220 2313 PST	20161221 2313 PST	20161220 2337 PST	
Valid through 20200405 0700 PDT	Wired Mac Auth 1	A0:36:9F:6E:2D:9F	a0369fa289f	20161220 2311 PST	20200405 0700 PDT	20161228 2000 PST	
Valid through 20200405 0700 PDT	Wired Mac Auth 1	A0:36:9F:6E:2D:9F	a0369fa289f	20161217 0121 PST	20200405 0700 PDT	20161228 2308 PST	
Valid through 20200405 0700 PDT	Wired Mac Auth 1	A0:36:9F:6E:2D:9F	jchandra@brocade.com	20161217 0120 PST	20200405 0700 PDT	20161217 0120 PST	
Valid through 20200405 0700 PDT	Wired Mac Auth 1	A0:36:9F:6E:2D:9F	jchandra@brocade.com	20161217 0115 PST	20200405 0700 PDT	20161217 0119 PST	



# Use Case 2: Dynamic VLAN and ACL Assignment with 802.1X Authentication

- Cloudpath Configuration.....30
- Switch Configuration ..... 34
- Switch Show Commands and Syslog Information..... 34
- Cloudpath Information.....35

The following example uses 802.1X authentication for authenticating a client and then dynamically assigns a VLAN and ACL after a successful authentication.

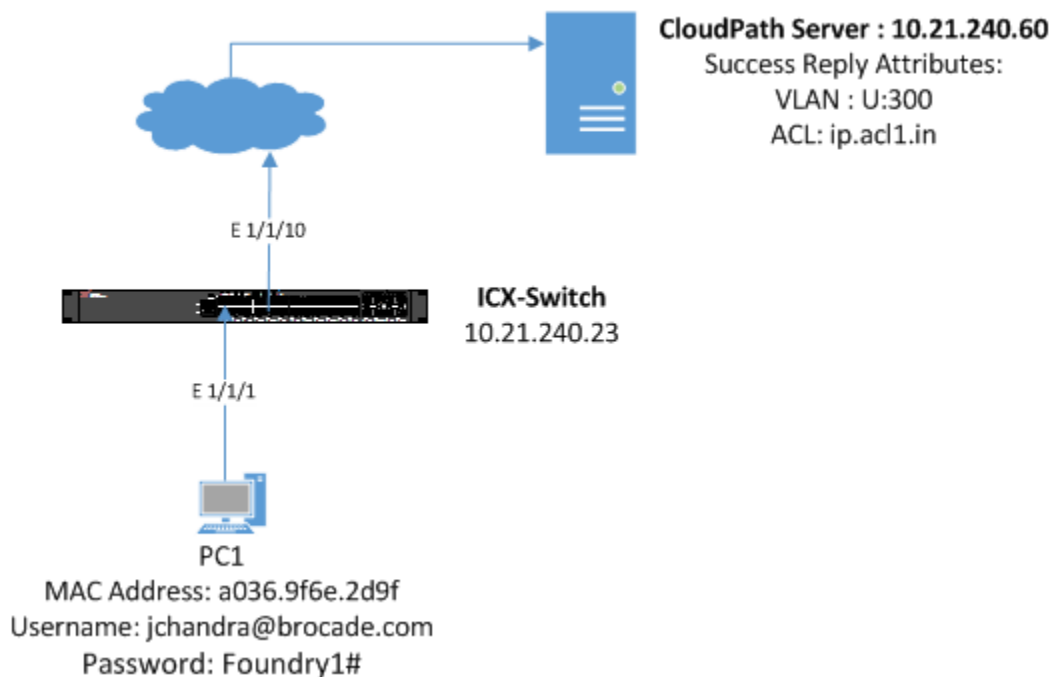
## Client PC1

- Username: jchandra@brocade.com
- Password: Foundry1#
- After authentication:
  - The client should be placed in VLAN 300.
  - Incoming traffic from client A 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 5 Example of Assigning a Dynamic VLAN and ACL with 802.1X Authentication

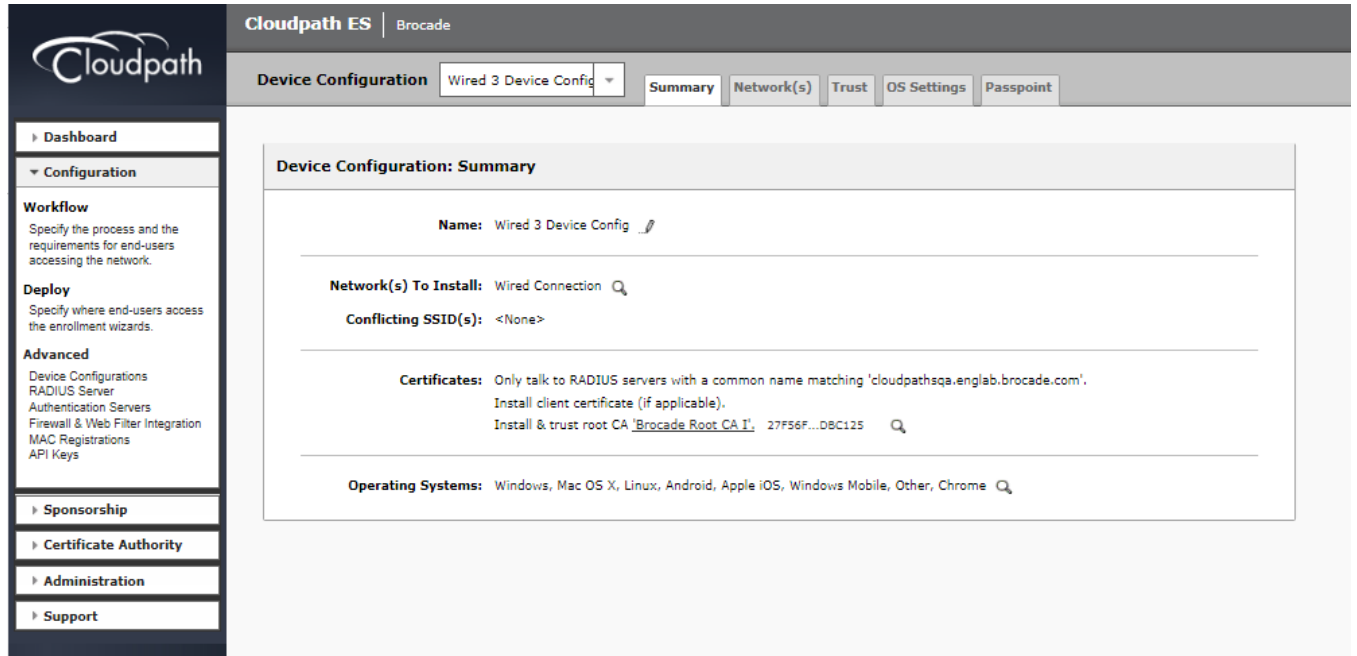
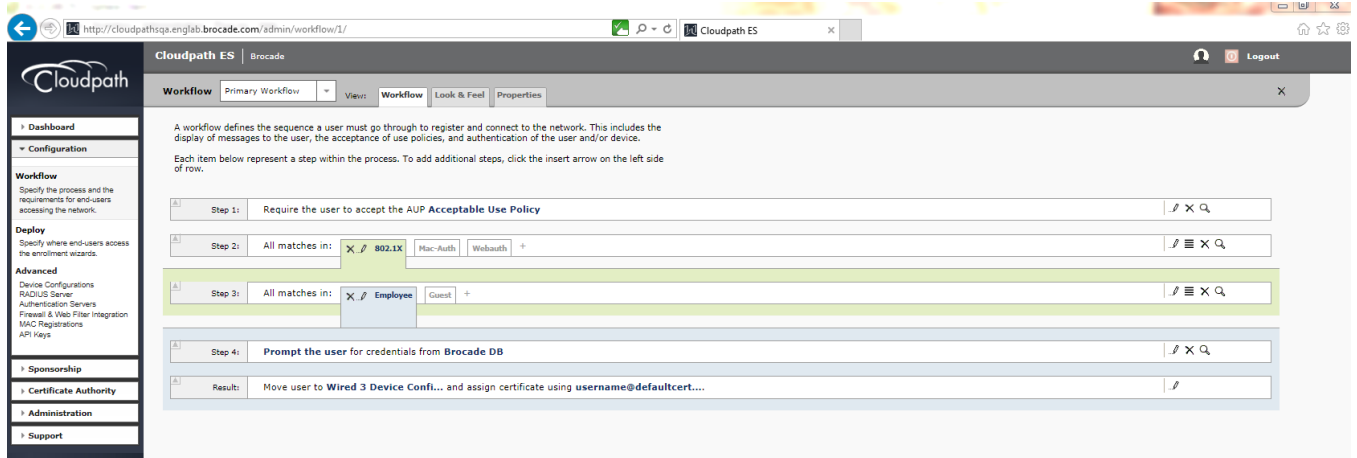


# Cloudpath Configuration

The following configuration assumes that the administrator has already installed the certificates to the users, such as Employees.

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.



Cloudpath ES | Brocade

Device Configuration | Wired 3 Device Config | Summary | **Network(s)** | Trust | OS Settings | Passpoint

**Device Configuration: Network(s)**

**WLAN & Wired Network Information**

**Network(s) To Install:**

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

**Conflicting SSID(s):** <None>

**Post-Transition URL:** <None>

Cloudpath ES | Brocade

Device Configuration | Wired 3 Device Config | Summary | Network(s) | **Trust** | OS Settings | Passpoint

**Device Configuration: Trust 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:** cloudpathsq.english.brocade.com

**Trusted RADIUS Chain:**


	Root CA:	27956F...D8C125	20361123
Server Certificate:	cloudpathsq.english.brocade.com	587842...141849	20211123 Brocade Root CA 1

**Web Browser Trust**

**Install Additional CAs:** No additional CAs have been specified. [Upload](#)



Cloudpath ES Brocade

 Logout

**Device Configuration** Wired 3 Device Config

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

### Device Configuration: OS-Specific Settings

**Windows:**

Setting	XP	Vista	7	8	8.1	10	Future
<input type="button" value="Add Setting"/> <input type="checkbox"/> User experience options							
<input type="checkbox"/> Settings from the <a href="#">lastupdate(s)</a> tab will be applied to these versions:	⬆	⬆	⬆	⬆	⬆	⬆	⬆

**Mac OS X:**

Setting	10.7	10.8	10.9	10.10	10.11	10.12	Future
<input type="button" value="Add Setting"/> <input type="checkbox"/> User experience options							
<input type="checkbox"/> Settings from the <a href="#">lastupdate(s)</a> tab will be applied to these versions:	⬆	⬆	⬆	⬆	⬆	⬆	⬆

**iOS:**

Setting	6	7	8	9	10	Future
<input type="button" value="Add Setting"/> <input type="checkbox"/> User experience options						
<input type="checkbox"/> Settings from the <a href="#">lastupdate(s)</a> tab will be applied to these versions:						

**Android:**

Setting	4.0.2	4.1	4.2	4.3	4.4	5.0	5.1	6.0	7.0	Future
<input type="button" value="Add Setting"/> <input type="checkbox"/> User experience options										
<input type="checkbox"/> Settings from the <a href="#">lastupdate(s)</a> tab will be applied to these versions:										

**Chrome:**

Setting	Chrome
<input type="button" value="Add Setting"/> <input type="checkbox"/> User experience options	
<input type="checkbox"/> Settings from the <a href="#">lastupdate(s)</a> tab will be applied to these versions:	

**Linux:**

Setting	12.04	12.10	13.04	13.10	14.04	14.10	15.04	15.10	16.04	16.10	18	19	20	21	22	23	24	25	Future	
<input type="button" value="Add Setting"/> <input type="checkbox"/> User experience options																				
<input type="checkbox"/> Settings from the <a href="#">lastupdate(s)</a> tab will be applied to these versions:	⬆	⬆	⬆	⬆	⬆	⬆	⬆	⬆	⬆	⬆	⬆	⬆	⬆	⬆	⬆	⬆	⬆	⬆	⬆	

**Win Mobile:**

Setting	5.0	6.0
<input type="checkbox"/> Settings from the <a href="#">lastupdate(s)</a> tab will be applied to these versions:		
* Windows Mobile support is limited to specific devices. Contact support for supported devices.		

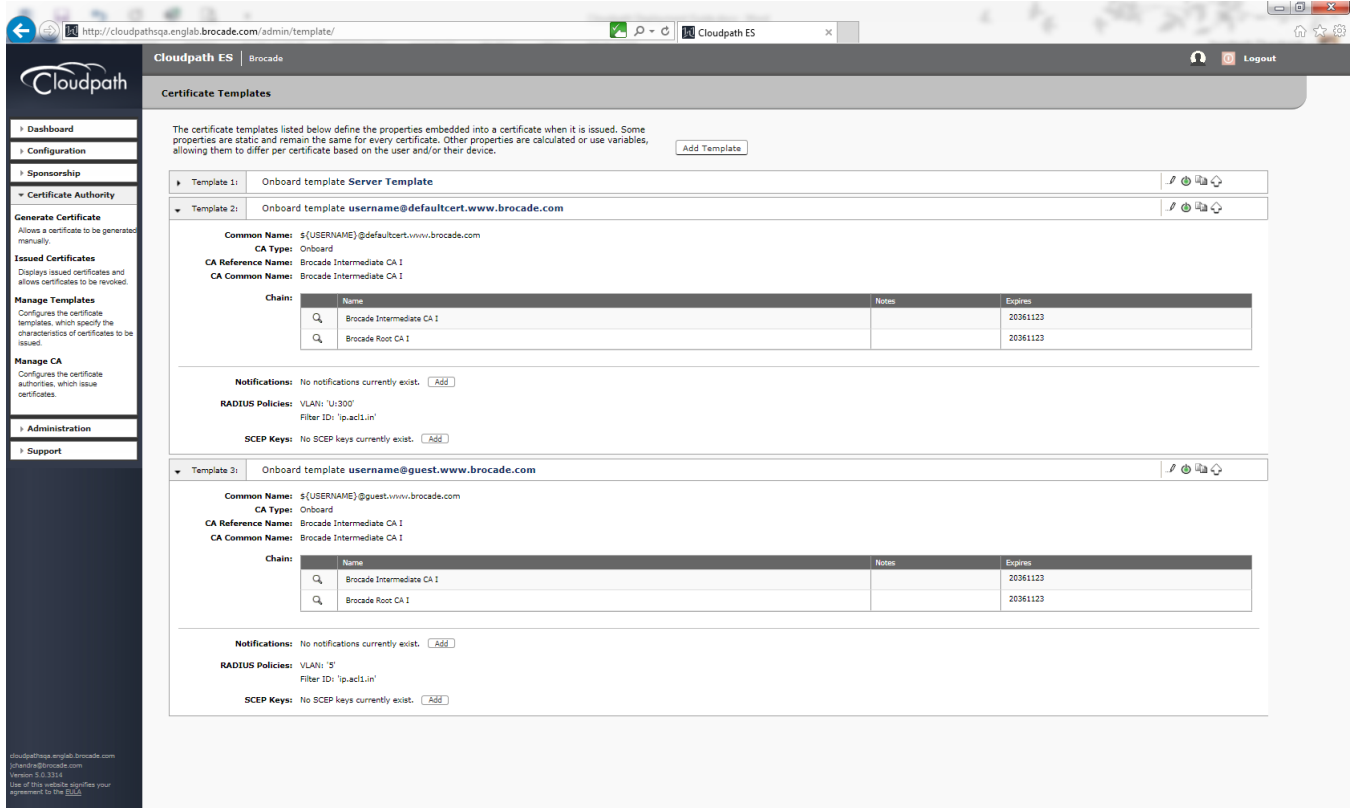
**Other OSes:**

Setting	Generic	WinRT	BlackBerry	Windows Phone
<input type="checkbox"/> User experience options				
<input type="checkbox"/> Settings from the <a href="#">lastupdate(s)</a> tab will be applied to these versions:				

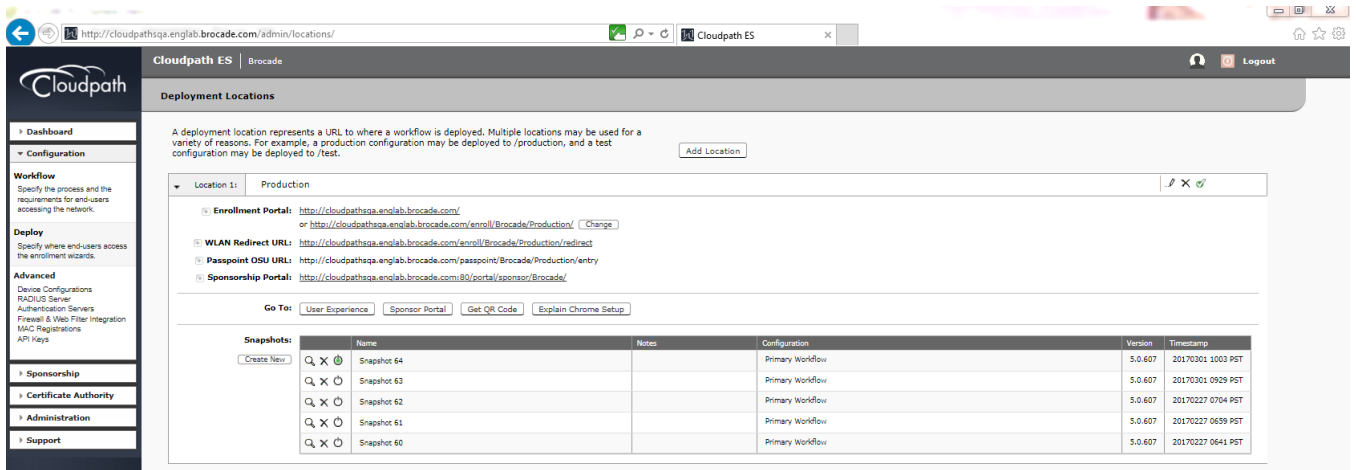
cloudpathes@brocade.com | brocade.com | Version 5.0.2214 | Use of this website signifies your agreement to the EULA



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



- Create a snapshot to save the changes.



## Switch Configuration

```

!
vlan 2 name AUTH-DEFAULT by port
!
vlan 300 name 802.1X by port
  tagged ethe 1/1/10
!
authentication
  auth-default-vlan 2
  dot1x enable
  dot1x enable ethe 1/1/1
!
interface ethernet 1/1/1
  dot1x port-control auto
!
aaa authentication dot1x default radius
radius-server host 10.21.240.60 auth-port 1812 acct-port 1813 default key Foundry1 dot1x mac-auth web-auth
!
ip access-list extended acl1
  permit ip any any
!

```

## Switch Show Commands and Syslog Information

```

!
ICX-Switch#
SYSLOG: <14> Mar  1 16:25:02 ICX-Switch DOT1X: Port 1/1/1 - mac a036.9f6e.2d9f AuthControlledPortStatus change:
unauthorized

SYSLOG: <14> Mar  1 16:25:02 ICX-Switch System: Interface ethernet 1/1/1, state up

SYSLOG: <14> Mar  1 16:25:03 ICX-Switch DOT1X: Port 1/1/1 - mac a036.9f6e.2d9f, AuthControlledPortStatus
change: authorized

SYSLOG: <13> Mar  1 16:25:03 ICX-Switch FLEXAUTH: Port ethe 1/1/1  is added into VLAN 300 as MAC-VLAN member

SYSLOG: <13> Mar  1 16:25:03 ICX-Switch FLEXAUTH: Port ethe 1/1/1  is deleted from VLAN 2 as MAC-VLAN member

ICX-Switch#show dot1x sessions all
-----
Port      MAC                IP (v4/v6)          User                VLAN  Auth    ACL    Session  Age    PAE
  Addr                    Addr                Name                  State              State
-----
1/1/1    a036.9f6e.2d9f    10.21.80.226        jchandra@broc 300  permit  Yes     25      Ena
AUTHENTICATED
ICX-Switch#
SYSLOG: <14> Mar  1 16:25:28 ICX-Switch CLI CMD: "show dot1x sessions all" by un-authenticated user from
console

ICX-Switch#show vlan 300
Total PORT-VLAN entries: 7
Maximum PORT-VLAN entries: 64

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

PORT-VLAN 300, Name 802.1X, Priority level0, Spanning tree Off
  Untagged Ports: None
    Tagged Ports: (U1/M1)  10
    Uplink Ports: None
  DualMode Ports: None
  Mac-Vlan Ports: (U1/M1)  1
    Monitoring: Disabled
ICX-Switch#show dot1x ip-acl all
-----

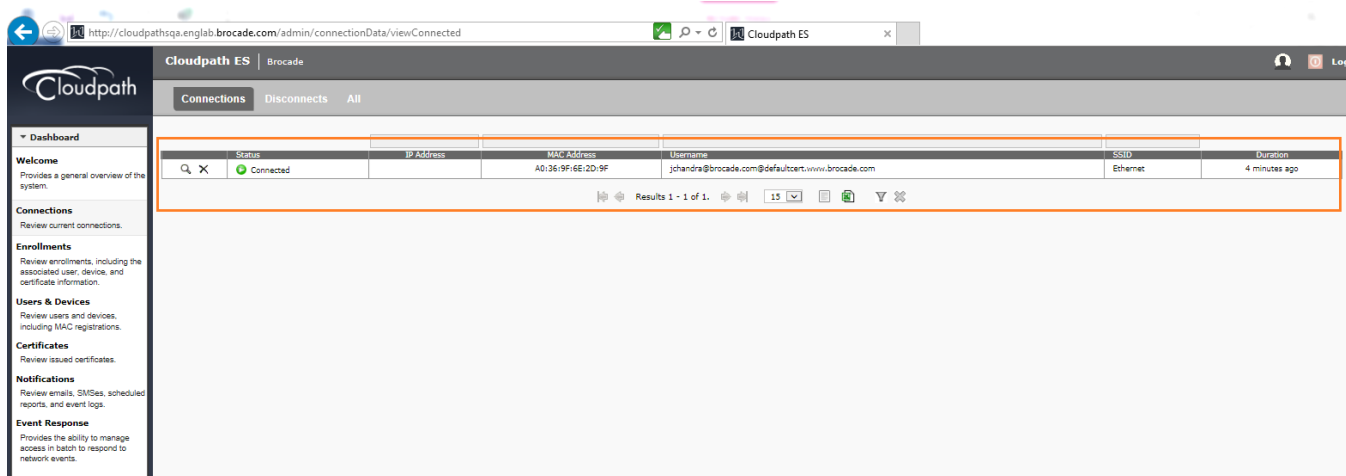
```

```

Port          MAC Address      V4 Ingress  V4 Egress  V6 Ingress  V6 Egress
-----
1/1/1        a036.9f6e.2d9f  ac11
Refer following show command to check status of radius server.
ICX-Switch#show radius server
-----
Server        Tyoe           Opens        Closes     Timeouts    Status
-----
10.21.240.60  any            0            0          0           active
    
```

# Cloudpath Information

1. Navigate to **Dashboard > Connections** to verify the username of the certificate issued to the user.



2. Click the search button of the connection to view the connection details.

**View Connection** Done

**Status:** ● Connected

**Username:** jchandra@brocade.com@defaultcert.www.brocade.com

**IP Address:**

**MAC Address:** A0:36:9F:6E:2D:9F

**SSID:** Ethernet

**Session Start Time:** 83 seconds ago

**NAS Identifier:** ICX-Switch

**NAS IP:**

**NAS Port:**

**NAS Port Type:**

**Session ID:**

**Last Accounting Update:** 83488 millis

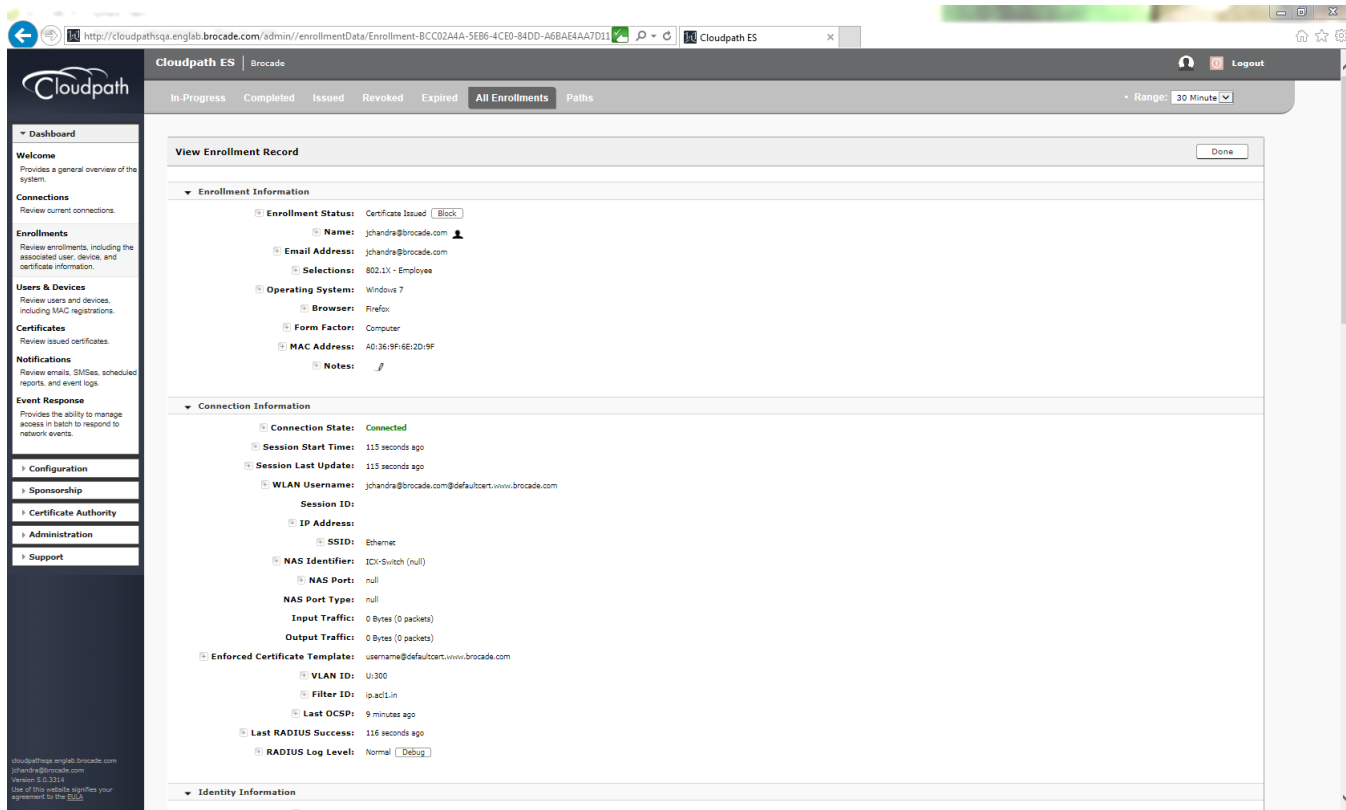
**Input Traffic:** 0 Bytes (0 packets)

**Output Traffic:** 0 Bytes (0 packets)

**Accumulated Session Time:** 0 seconds

**Additional Information:** [Enrollment Record](#)

3. Click the **Enrollment Record** button to view the additional details for the connection.





# Use Case 3: Guest VLAN with External Captive Portal (Web Authentication)

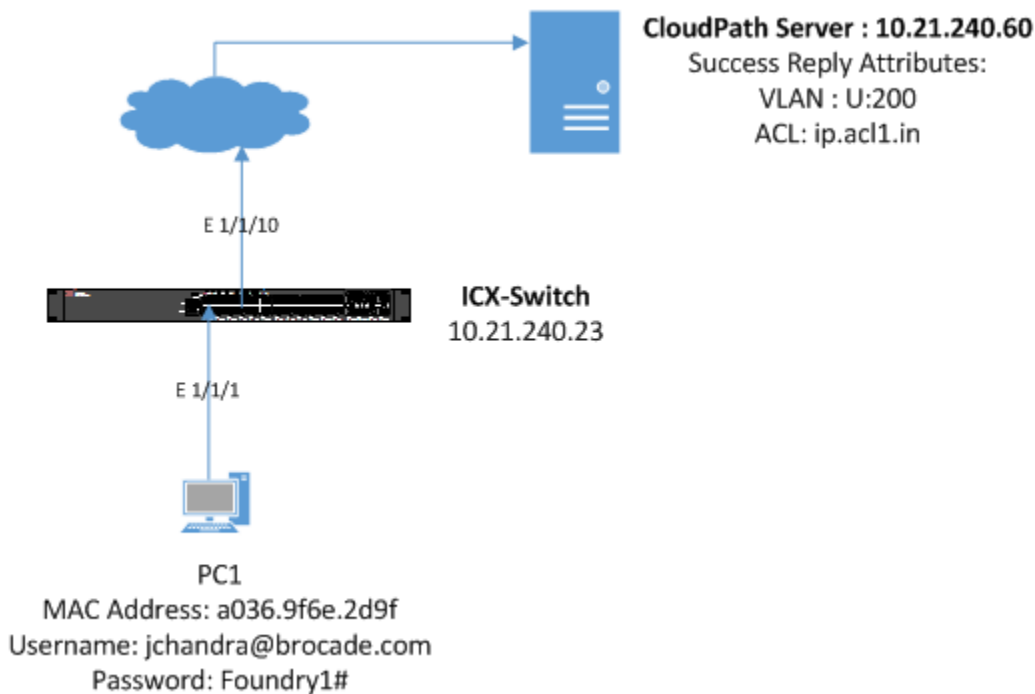
- Cloudpath Configuration.....40
- Switch Configuration .....41
- Switch Show Commands and Syslog Information.....42
- Cloudpath Information.....43

The following example uses 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 200 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.

## Client PC1

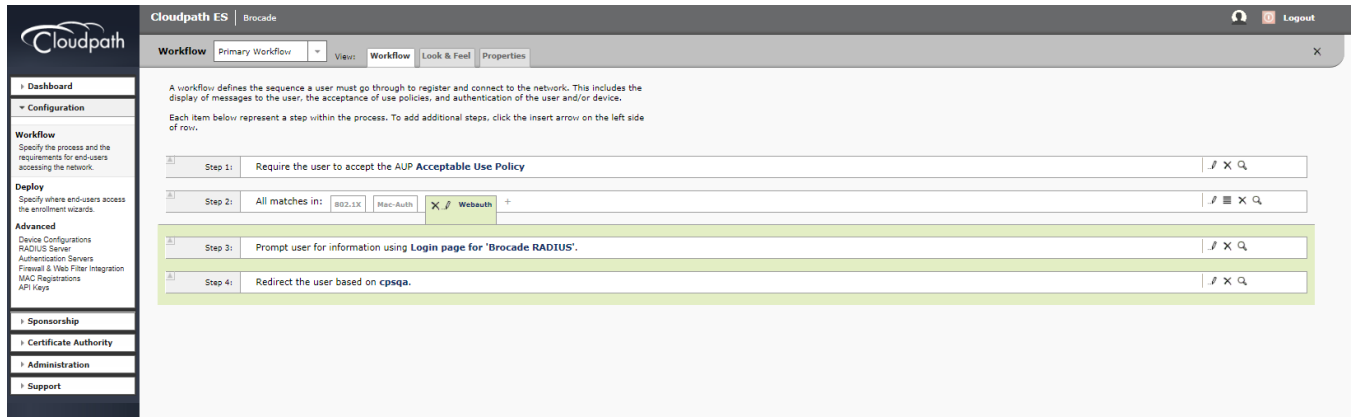
- The MAC address is a036.9f6e.2d9f.
- After authentication, incoming traffic from client A should be filtered by ACL "acl1".

FIGURE 6 Example of Web Authentication (Captive Portal) with a Guest VLAN

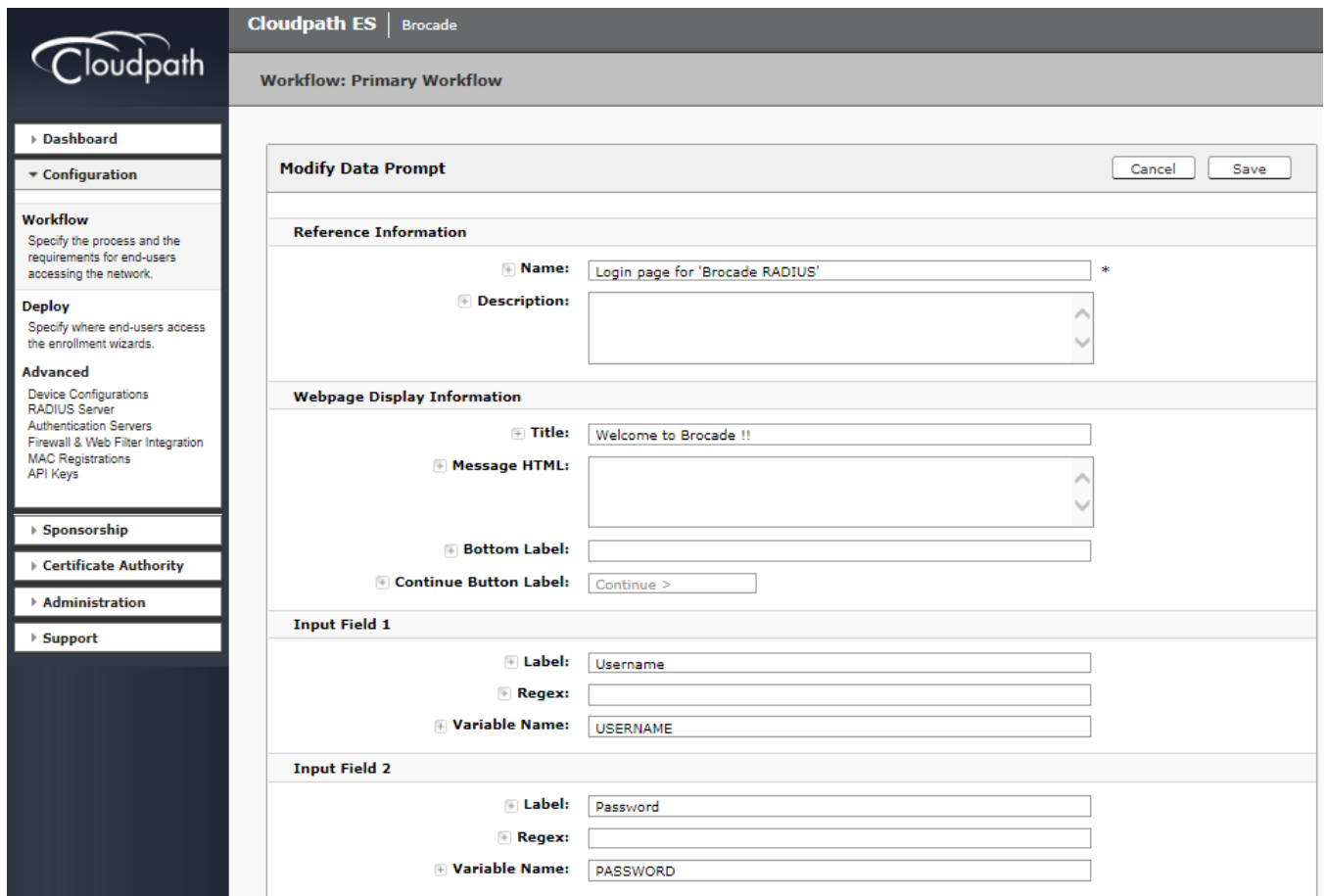


# Cloudpath Configuration

1. Navigate to **Configuration > Workflow** and create steps for web authentication.



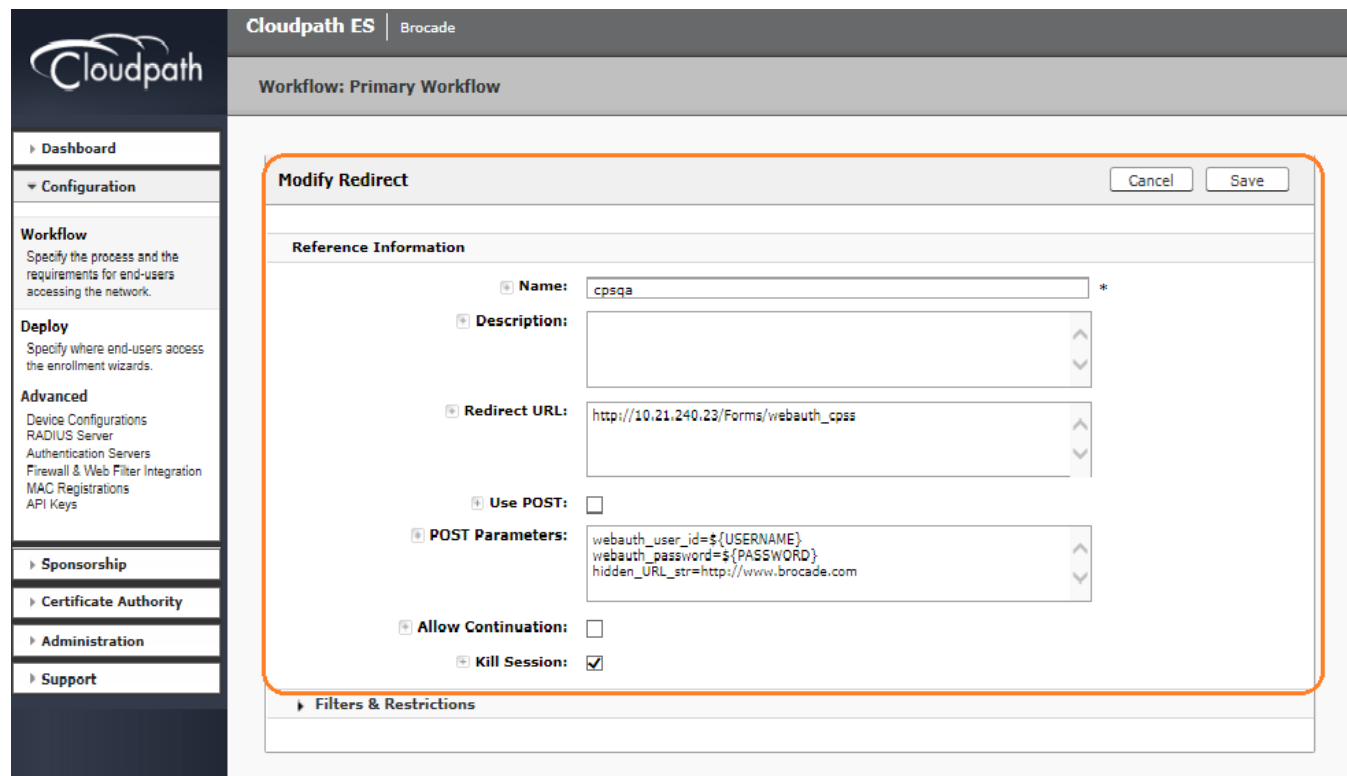
2. Modify the data prompt by clicking "Login page for 'Brocade RADIUS'" for input fields 1 and 2.





3. Create the Redirect URL `http://10.21.240.23/Forms/webauth_cpss`, where 10.21.240.23 is the NAS IP address of the switch, and enter the following POST parameters:
  - `webauth_user_id=${USERNAME}`
  - `webauth_password=${PASSWORD}`
  - `hidden_URL_str=http://www.brocade.com`

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



## Switch Configuration

```

!
captive-portal cp-sqa
  virtual-ip 10.21.240.60
  virtual-port 80
  login-page /enroll/Brocade/Production/
!
captive-portal cp-sqa1
  virtual-ip Cloudpathsqa.englab.brocade.com
  virtual-port 80
  login-page /enroll/Brocade/Production/
!
vlan 2 name AUTH-DEFAULT by port
!
vlan 200 name GUEST by port
  tagged ethe 1/1/10
  untagged ethe 1/1/1
  router-interface ve 200
  webauth

```

```

captive-portal profile cp-sqa1
auth-mode captive-portal
no secure-login
trust-port ethernet 1/1/10
enable
!
aaa authentication dot1x default radius
radius-server host 10.21.240.60 auth-port 1812 acct-port 1813 default key Foundry1 dot1x mac-auth web-auth
!
ip dns server-address 10.37.2.1 10.37.2.2 10.31.2.10 10.31.2.11
!
web-management https
!
interface ve 200
ip address 10.21.80.130/27
!
ip access-list extended acl1
permit ip any any
!

```

## Switch Show Commands and Syslog Information

```

ICX-Switch#
SYSLOG: <14> Mar 1 21:40:41 ICX-Switch System: Interface ethernet 1/1/1, state up

SYSLOG: <14> Mar 1 21:41:00 ICX-Switch Web Auth in Vlan 200: Authentication succeeded for user :
jchandra@brocade.com using mac: a036.9f6e.2d9f on port 1/1/1 for a duration 28800 seconds

```

```
ICX-Switch#show webauth allowed-list
```

```
=====
VLAN 200: Web Authentication, Mode: I = Internal E = External
-----
```

Web Authenticated List			Configuration	Auth Duration	Dynamic
Port	MAC Address	User Name	Static/Dynamic	HH:MM:SS	ACL
1/1/1	a036.9f6e.2d9f	jchandra@brocade.com	E D	07:59:57	Yes

```
ICX-Switch#show webauth ip-acl
```

VLAN	Port	MAC Address	V4 Ingress ACL	V4 Egress ACL
200	1/1/1	a036.9f6e.2d9f	acl1	-

```

ICX-Switch#show vlan e 1/1/1
Total PORT-VLAN entries: 7
Maximum PORT-VLAN entries: 64

```

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

```
PORT-VLAN 200, Name GUEST, Priority level0, Spanning tree Off
```

```

Untagged Ports: (U1/M1) 1
Tagged Ports: (U1/M1) 10
Uplink Ports: None
DualMode Ports: None
Mac-Vlan Ports: None
Monitoring: Disabled

```

```
Refer following show command to check status of radius server.
```

```
ICX-Switch#show radius server
```

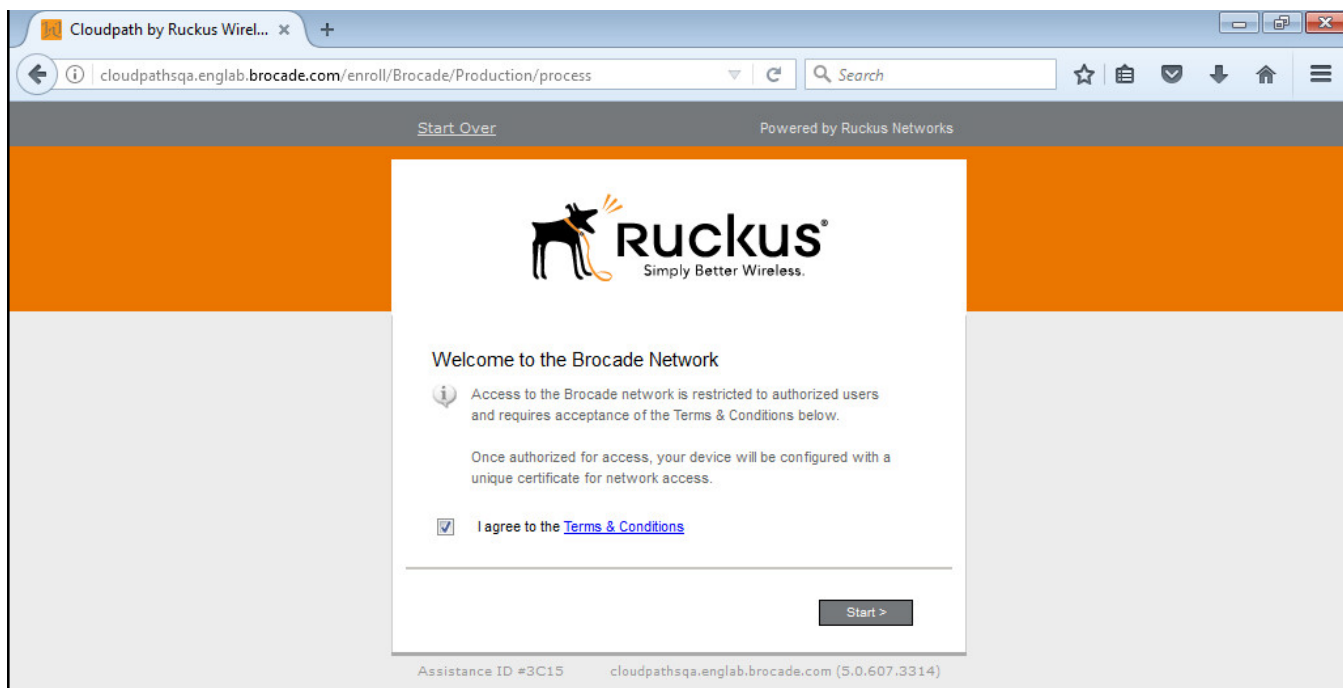
Server	Type	Opens	Closes	Timeouts	Status
10.21.240.60	any	0	0	0	active

# Cloudpath Information

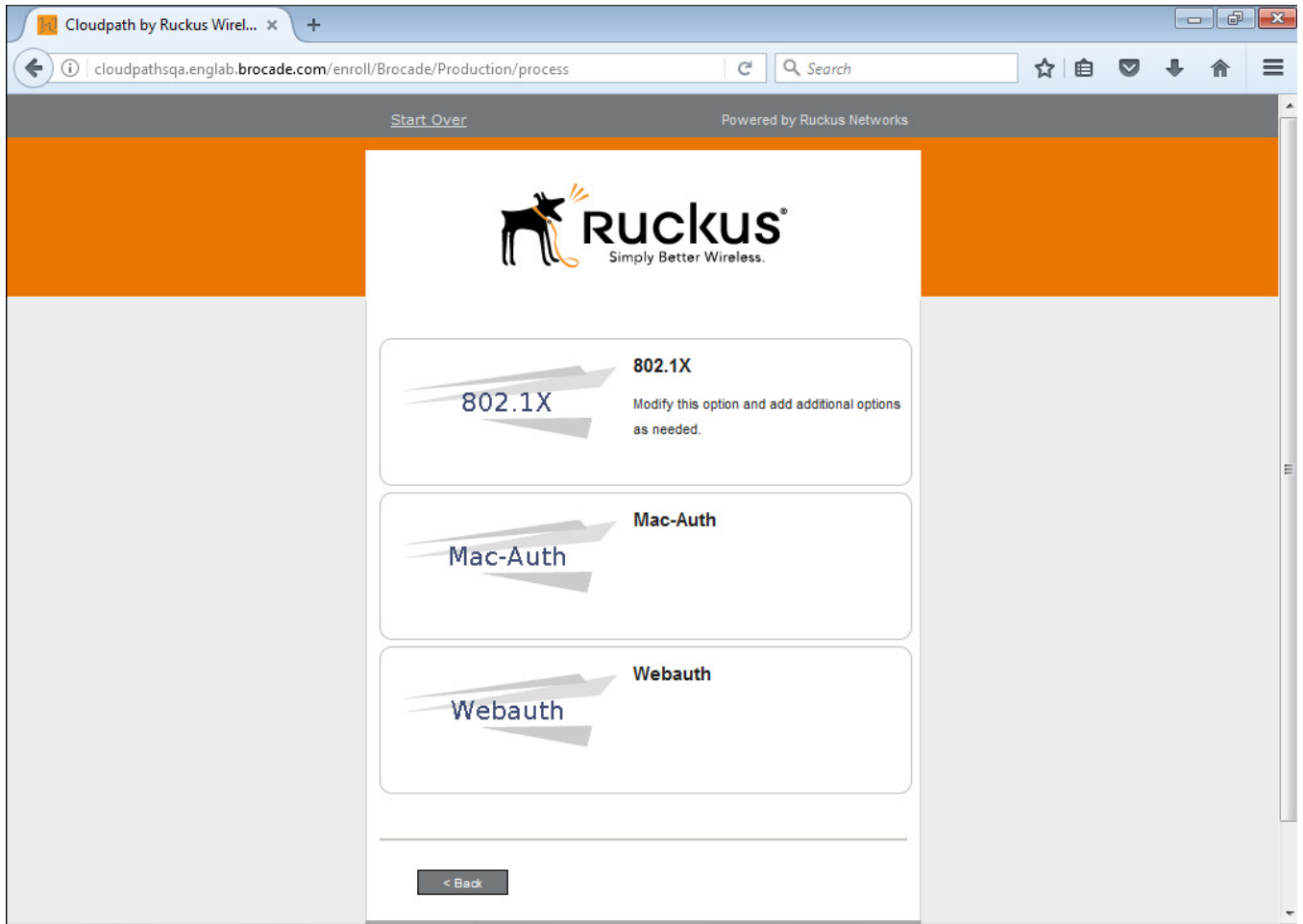
1. Open a web browser on the client PC and enter any website address or <http://www.brocade.com/>.

Because captive-portal authentication is configured on Webauth VLAN 200 and the captive-portal profile points to "cp-sqa1", the browser will redirect to <http://Cloudpathsqa.englab.brocade.com/enroll/Brocade/Production/redirect>.

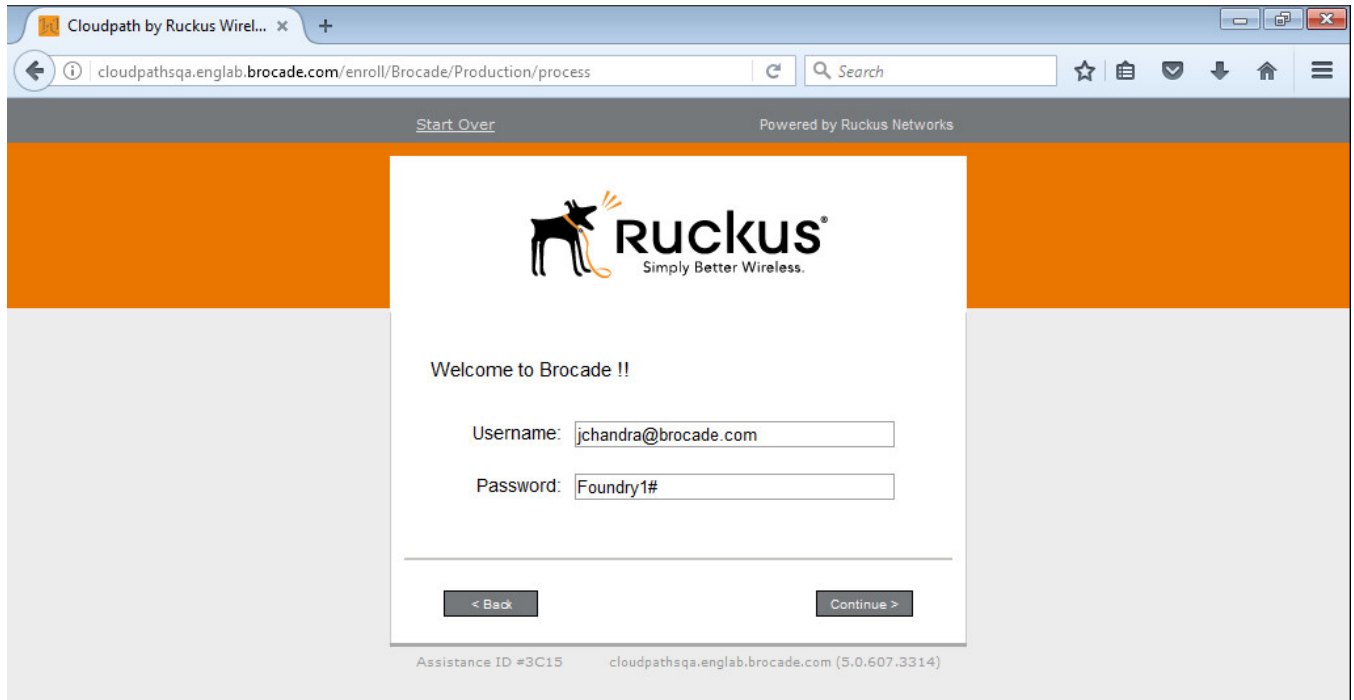
2. Accept the user policy and click **Start**.



3. Click **Webauth**.



4. Enter the user credentials and click **Continue**.



The screenshot shows a web browser window with the address bar displaying `cloudpathsqa.englab.brocade.com/enroll/Brocade/Production/process`. The page features the Ruckus logo (a dog) and the tagline "Simply Better Wireless." Below the logo, it says "Welcome to Brocade !!". There are two input fields: "Username:" with the value `jchandra@brocade.com` and "Password:" with the value `Foundry1#`. At the bottom of the form are two buttons: "< Back" and "Continue >". The footer of the page includes "Assistance ID #3C15" and "cloudpathsqa.englab.brocade.com (5.0.607.3314)".

You will be redirected to <http://www.brocade.com/>.



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

---

- Cloudpath Configuration.....49
- Switch Configuration ..... 52
- Switch Show Commands and Syslog Information..... 53
- Cloudpath Information..... 55
- MAC Authentication for an IP Phone..... 59

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.

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:

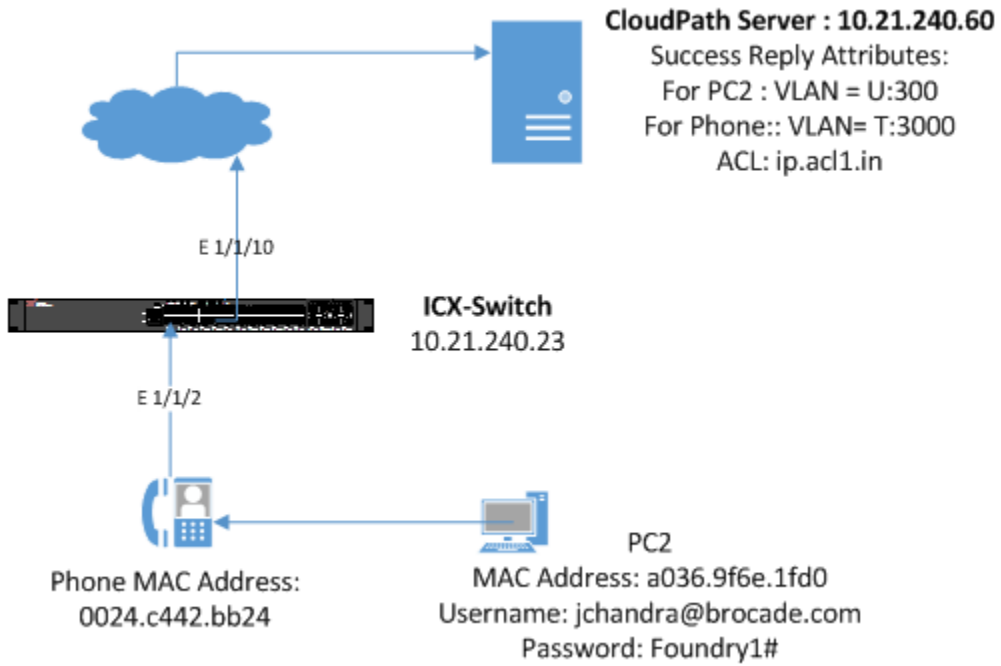
```
lldp med network-policy application voice tagged vlan 3000 priority 4 dscp 46 ports ethernet 1/1/2
```

**IP Phone:** The IP phone MAC address is 0024.c442.bb24, and the IP phone is in tagged VLAN 3000.

## Client PC2

- 802.1X username: jchandra@brocade.com
- Password: Foundry1#
- After authentication:
  - The client should be placed in VLAN 300.
  - Incoming traffic from client A should be filtered by ACL "acl1".

FIGURE 7 Example of Authenticating an IP Phone and a PC on the Same Port Using Flexible Authentication

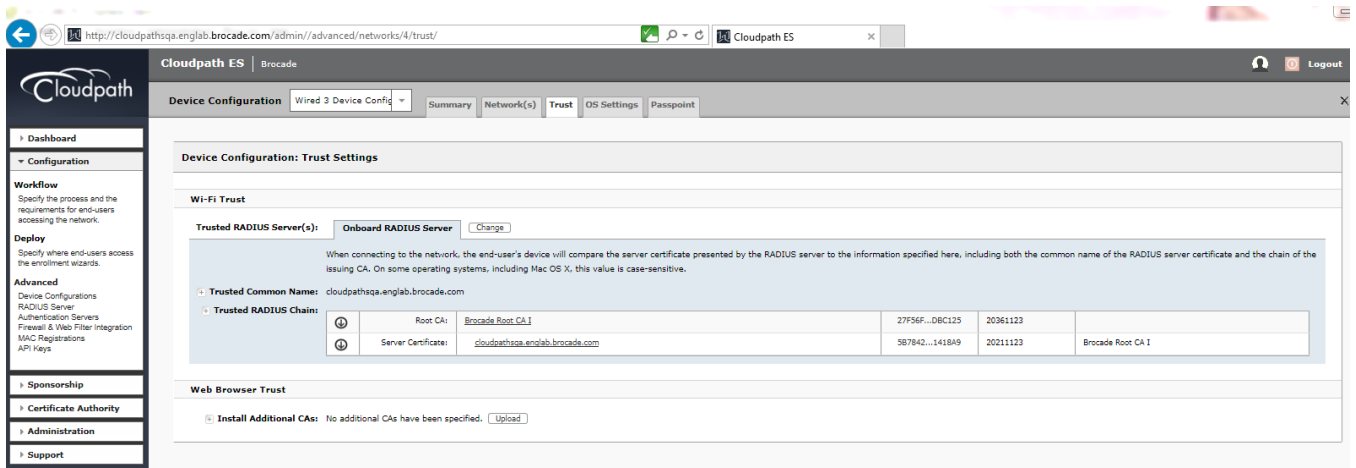
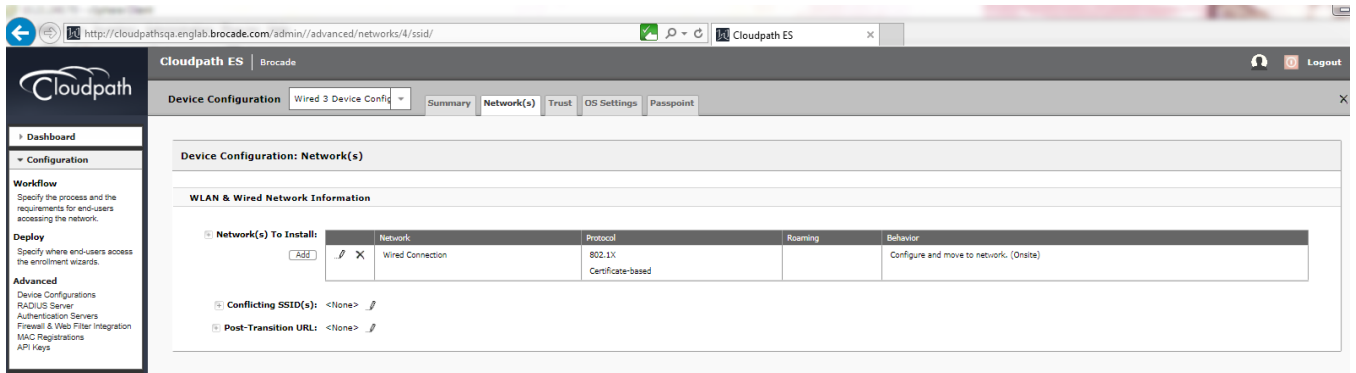
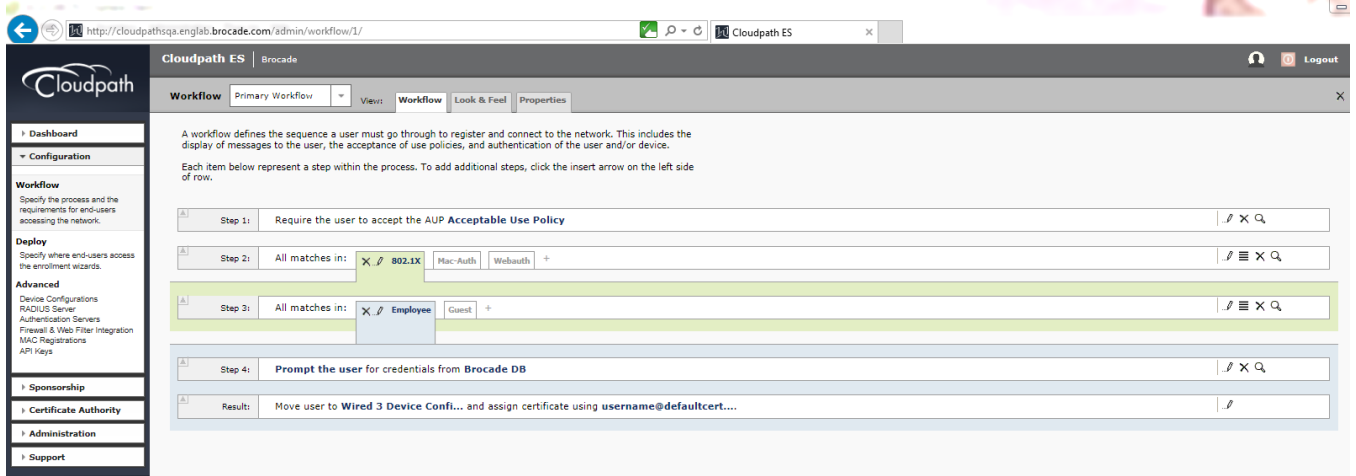




# Cloudpath Configuration

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

The following screenshots demonstrate steps for configuring the workflow.



**Device Configuration: OS-Specific Settings**

**Windows:** Settings for XP, Vista, 7, 8, 8.1, 10, Future. Includes 'User experience options' and 'Settings from the Network(s) tab will be applied to these versions'.

**Mac OS X:** Settings for 10.7, 10.8, 10.9, 10.10, 10.11, 10.12, Future. Includes 'User experience options' and 'Settings from the Network(s) tab will be applied to these versions'.

**IOS:** Settings for 6, 7, 8, 9, 10, Future. Includes 'User experience options' and 'Settings from the Network(s) tab will be applied to these versions'.

**Android:** Settings for 4.0.3, 4.1, 4.2, 4.3, 4.4, 5.0, 5.1, 6.0, 7.0, Future. Includes 'User experience options' and 'Settings from the Network(s) tab will be applied to these versions'.

**Chrome:** Settings for Chrome. Includes 'User experience options' and 'Settings from the Network(s) tab will be applied to these versions'.

**Linux:** Settings for 12.04, 12.10, 13.04, 13.10, 14.04, 14.10, 15.04, 15.10, 16.04, 16.10, 18, 19, 20, 21, 22, 23, 24, 25, Future. Includes 'User experience options' and 'Settings from the Network(s) tab will be applied to these versions'.

**Win Mobile:** Settings for 5.0, 6.0. Includes 'Settings from the Network(s) tab will be applied to these versions' and a note: '\* Windows Mobile support is limited to specific devices. Contact support for supported devices.'

**Other OSes:** Settings for Generic, WinRT, Blackberry, Windows Phone.

**Certificate Templates**

The certificate templates listed below define the properties embedded into a certificate when it is issued. Some properties are static and remain the same for every certificate. Other properties are calculated or use variables, allowing them to differ per certificate based on the user and/or their device.

Template 1: Onboard template **Server Template**

Template 2: Onboard template **username@defaultcert.www.brocade.com**

Template 3: Onboard template **username@guest.www.brocade.com**

**Common Name:** \$(USERNAME)@defaultcert.www.brocade.com  
**CA Type:** Onboard  
**CA Reference Name:** Brocade Intermediate CA 1  
**CA Common Name:** Brocade Intermediate CA 1

Name	Notes	Expires
Brocade Intermediate CA 1		20361123
Brocade Root CA 1		20361123

**Notifications:** No notifications currently exist. [Add](#)

**RADIUS Policies:** VLAN: 'U:300'  
Filter ID: 'ip.ac1.in'

**SCEP Keys:** No SCEP keys currently exist. [Add](#)

Browser address bar: http://cloudpathsqa.englishlab.brocade.com/admin/template/2/edit

Cloudpath ES | Brocade

### Certificate Templates

**Modify Certificate Template** [Cancel] [Save]

**Reference Information**

**Certificate Template Name:**  \*

**Certificate Authority:** Brocade Intermediate CA I

**Notes:**

**Enabled?**

**Identity**

The following property is normally used to provide identity information within the certificate. Variables, such as \${USERNAME}, will be replaced at the time of issuance with the appropriate value from the enrollment.

**Common Name Pattern:**

**Validity Period**

The following properties determine the lifespan of the issued certificates. We recommend setting the start date to 1 month before issuance to avoid issues with end-user system clocks.

**Start Date:**   before issuance.

**Expiration Date:**   after issuance.

**OCSP Monitoring:**  Revoke if unseen for  days.

**Policy - RADIUS Attributes**

**Allow Authentication via RADIUS:**

**Login By Certificate**  
bob@byod.sample.com

When a device authenticates using a certificate from this template, Cloudpath will return RADIUS attributes based on the information below.

These attributes may be used to apply a dynamic VLAN, an ACL, or other connection policies.

**Reply Username:**

**Allowed SSID(s):**

## Switch Configuration

```

!
vlan 2 name AUTH-DEFAULT by port
!
!
vlan 300 name 802.1X by port
  tagged ethe 1/1/10
  router-interface ve 300
!
vlan 3000 name VOICE by port
  tagged ethe 1/1/2 ethe 1/1/10
  router-interface ve 3000
!
authentication
  auth-default-vlan 2
  dot1x enable
  dot1x enable ethe 1/1/2
  mac-authentication enable
  mac-authentication enable ethe 1/1/2
!
!
aaa authentication dot1x default radius
!
radius-server host 10.21.240.60 auth-port 1812 acct-port 1813 default key Foundry1 dot1x mac-auth web-auth
!
interface ethernet 1/1/2

```

```

dot1x port-control auto
port-name PHONE-G06
inline power
!
!
ip access-list extended acl1
 permit ip any any
!
!
lldp med network-policy application voice tagged vlan 3000 priority 4 dscp 46 ports ethe 1/1/2
lldp run
!

```

## Switch Show Commands and Syslog Information

ICX-Switch#

PoE: Power enabled on port 1/1/2.

SYSLOG: <14> Mar 2 15:54:40 ICX-Switch System: PoE: Power adjustment done: decreased power by 14600 mwatts on port 1/1/2 .

SYSLOG: <14> Mar 2 15:54:40 ICX-Switch System: PoE: Power enabled on port 1/1/2.

SYSLOG: <14> Mar 2 15:54:45 ICX-Switch System: Interface ethernet 1/1/2, state up

SYSLOG: <14> Mar 2 15:54:53 ICX-Switch DOT1X: Port 1/1/2 - mac 0024.c442.bb24 AuthControlledPortStatus change: unauthorized

SYSLOG: <14> Mar 2 15:54:59 ICX-Switch DOT1X: Port 1/1/2 - mac a036.9f6e.1fd0 AuthControlledPortStatus change: unauthorized

SYSLOG: <14> Mar 2 15:54:59 ICX-Switch DOT1X: Port 1/1/2 - mac a036.9f6e.1fd0, AuthControlledPortStatus change: authorized

SYSLOG: <13> Mar 2 15:54:59 ICX-Switch FLEXAUTH: Port ethe 1/1/2 is added into VLAN 300 as MAC-VLAN member

SYSLOG: <13> Mar 2 15:54:59 ICX-Switch FLEXAUTH: Port ethe 1/1/2 is deleted from VLAN 2 as MAC-VLAN member

SYSLOG: <13> Mar 2 15:55:50 ICX-Switch MAC Authentication succeeded for [0024.c442.bb24 ] on port 1/1/2

ICX-Switch#show dot1x sessions all

Port	MAC Addr	IP (v4/v6) Addr	User Name	VLAN	Auth State	ACL	Session Time	Age	PAE State
1/1/2	0024.c442.bb24	N/A	N/A	300	init	None	93	Ena	HELD
1/1/2	a036.9f6e.1fd0	10.21.80.228	jchandra@broc	300	permit	Yes	87	Ena	

AUTHENTICATED

ICX-Switch#show mac-auth sessions all

Port	MAC Addr	IP (v4/v6) Addr	VLAN	Auth State	ACL	Session Time	Age
1/1/2	0024.c442.bb24	10.21.80.97	3000	Yes	Yes	24	Ena
1/1/2	0024.c442.bb24	N/A	300	Yes	Yes	36	Ena

ICX-Switch#show dot1x ip-acl all

Port	MAC Address	V4 Ingress	V4 Egress	V6 Ingress	V6 Egress
1/1/2	0024.c442.bb24	-	-	-	-
1/1/2	a036.9f6e.1fd0	acl1	-	-	-

ICX-Switch#show mac-authentication ip-acl all

Port	MAC Address	V4 Ingress	V4 Egress	V6 Ingress	V6 Egress
1/1/2	0024.c442.bb24	-	-	-	-
1/1/2	a036.9f6e.1fd0	acl1	-	-	-

Switch Show Commands and Syslog Information

```
1/1/2      0024.c442.bb24    ac11      -        -        -
1/1/2      0024.c442.bb24    ac11      -        -        -
ICX-Switch#show vlan 300
Total PORT-VLAN entries: 8
Maximum PORT-VLAN entries: 64
```

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

```
PORT-VLAN 300, Name 802.1X, Priority level0, Spanning tree Off
Untagged Ports: None
Tagged Ports: (U1/M1)  10
Uplink Ports: None
DualMode Ports: None
Mac-Vlan Ports: (U1/M1)  2
Monitoring: Disabled
```

```
ICX-Switch#show vlan 3000
Total PORT-VLAN entries: 8
Maximum PORT-VLAN entries: 64
```

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

```
PORT-VLAN 3000, Name VOICE, Priority level0, Spanning tree Off
Untagged Ports: None
Tagged Ports: (U1/M1)  2  10
Uplink Ports: None
DualMode Ports: None
Mac-Vlan Ports: None
Monitoring: Disabled
```

```
ICX-Switch#show lldp local-info port e 1/1/2
Local port: 1/1/2
+ Chassis ID (MAC address): cc4e.24b4.7b30
+ Port ID (MAC address): cc4e.24b4.7b31
+ Time to live: 120 seconds
+ System name      : "ICX-Switch"
+ Port description : "GigabitEthernet1/1/2"
+ System capabilities : bridge, router
  Enabled capabilities: bridge, router
+ 802.3 MAC/PHY      : auto-negotiation enabled
  Advertised capabilities: 10BaseT-HD, 10BaseT-FD, 100BaseTX-HD,
                          100BaseTX-FD, fdxSPause, fdxBPause, 1000BaseT-HD,
                          1000BaseT-FD
  Operational MAU type   : 1000BaseT-FD
+ 802.3 Power via MDI: PSE port, power enabled, class 3
  Power Pair           : A (not controllable)
  Power Type          : Type 2 PSE device
  Power Source        : Unknown Power Source
  Power Priority      : Low (3)
  Power Requested    : 12.0 watts (PSE equivalent: 13190 mWatts)
  Power Allocated    : 12.0 watts (PSE equivalent: 13190 mWatts)
+ Link aggregation: not capable
+ Maximum frame size: 1522 octets
+ MED capabilities: capabilities, networkPolicy, location, extendedPSE
```

SYSLOG: <14> Mar 2 15:56:43 ICX-Switch CLI CMD: "show lldp local-info ports ethernet 1/1/2" by un-

```
authenticated user from console
MED device type : Network Connectivity
+ MED Network Policy
  Application Type : Voice
  Policy Flags    : Known Policy, Tagged
  VLAN ID        : 3000
  L2 Priority     : 4
  DSCP Value     : 46
+ MED Extended Power via MDI
  Power Type     : PSE device
  Power Source   : Unknown Power Source
  Power Priority : Low (3)
  Power Value    : 12.0 watts (PSE equivalent: 13190 mWatts)
+ Port VLAN ID: none
+ Management address (IPv4): 10.21.80.249
```

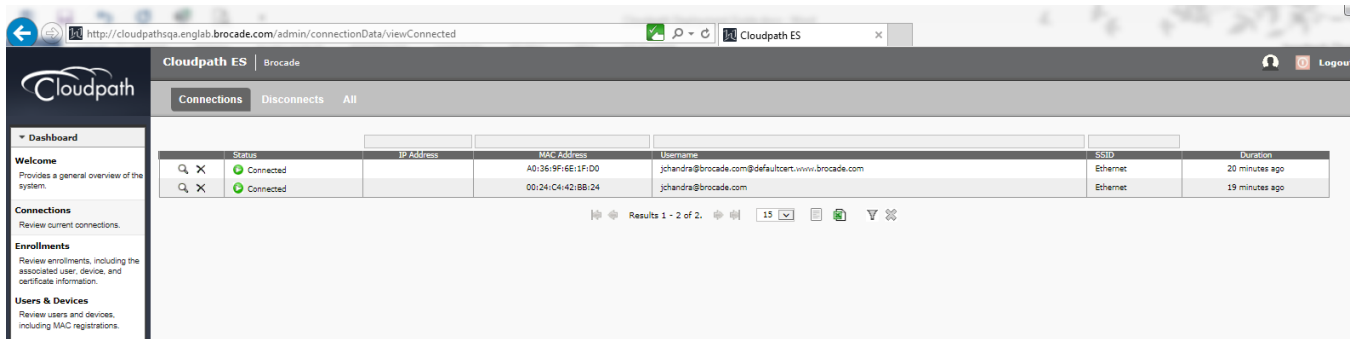
Refer following show command to check status of radius server.

```
ICX-Switch#show radius server
```

Server	Type	Opens	Closes	Timeouts	Status
10.21.240.60	any	0	0	0	active

## Cloudpath Information

1. Navigate to **Dashboard > Connections** and click the search button to view the connection details for both 802.1X authentication for the PC and MAC authentication for an IP phone.



2. Configure 802.1X authentication for a PC.

**View Connection** Done

**Status:** ● Connected

**Username:** jchandra@brocade.com@defaultcert.www.brocade.com

**IP Address:**

**MAC Address:** A0:36:9F:6E:1F:D0

**SSID:** Ethernet

**Session Start Time:** 21 minutes ago

**NAS Identifier:** ICX-Switch

**NAS IP:**

**NAS Port:**

**NAS Port Type:**

**Session ID:**

**Last Accounting Update:** 1264018 millis

**Input Traffic:** 0 Bytes (0 packets)

**Output Traffic:** 0 Bytes (0 packets)

**Accumulated Session Time:** 0 seconds

**Additional Information:** [Enrollment Record](#)

The screenshot shows the Cloudpath ES web interface. The main content area displays the 'View Enrollment Record' for a user. The interface includes a sidebar with navigation options like Dashboard, Welcome, Connections, Enrollments, Users & Devices, Certificates, Notifications, Event Response, Configuration, Sponsorship, Certificate Authority, Administration, and Support. The main content is organized into sections: Enrollment Information, Connection Information, and Identity Information.

**Enrollment Information:**

- Enrollment Status:** Certificate Issued [Block]
- Name:** jchandra@brocade.com
- Email Address:** jchandra@brocade.com
- Selections:** 802.1X - Employee
- Operating System:** Windows 7
- Browser:** Firefox
- Form Factors:** Computer
- MAC Address:** A0:36:9F:6E:1F:D0
- Notes:**

**Connection Information:**

- Connection State:** Connected
- Session Start Time:** 22 minutes ago
- Session Last Update:** 22 minutes ago
- WLAN Username:** jchandra@brocade.com@defaultcert.www.brocade.com
- Session ID:**
- IP Address:**
- SSID:** Ethernet
- NAS Identifier:** ICX-Switch (null)
- NAS Port:** null
- NAS Port Type:** null
- Input Traffic:** 0 Bytes (0 packets)
- Output Traffic:** 0 Bytes (0 packets)
- Enforced Certificate Template:** username@defaultcert.www.brocade.com
- VLAN ID:** U:300
- Filter ID:** ipad1.in
- Last OCSP:** 22 minutes ago
- Last RADIUS Success:** 22 minutes ago
- RADIUS Log Level:** Normal [Debug]

**Identity Information:**

- Username:** jchandra@brocade.com



http://cloudpathsqa.english.brocade.com/admin/enrollmentData/Enrollment-5D38AB91-8E30-489C-8434-DA4D31F5C948/ Cloudpath ES

RADIUS Log Level: Normal

**Identity Information**

- Username:** jchandra@brocade.com
- Email Address:** jchandra@brocade.com
- Blocked Status:** No
- Distinguished Name:** type=admin, cn=jchandra@brocade.com
- Server Name:** Brocade DB
- User Groups:** administrator

**Device Information**

**Workflow Information**

Step	Workflow Step	Result
Step 1	Require the user to accept the AUP Acceptable Use Policy	Accepted on 20170302 0922 PST
Step 2	All matches in:	Will prompt user to select from: 802.1X, Mac-Auth, Webauth Selection: 802.1X
Step 3	All matches in:	Will prompt user to select from: Employee, Guest Selection: Employee
Step 4	Prompt the user for credentials from Brocade DB	Successful as 'jchandra@brocade.com'
Result:	User has completed the workflow.	The user is authorized to receive a certificate from 'username@defaultcert.www.brocade.com'.
Certificate	User has been issued a certificate.	jchandra@brocade.com@defaultcert.www.brocade.com valid until 20270302.
Connection	User has authenticated.	Last authentication: 22 minutes ago

**Notifications**

**Issued Certificate**

- Status:** Valid
- Common Name:** jchandra@brocade.com@defaultcert.www.brocade.com
- Certificate Template:** username@defaultcert.www.brocade.com
- Certificate Type:** User + Device
- Certificate Chain:** Brocade Intermediate CA 1 (61E82C43423217C8CB66C2C51A80EDF0D295839)  
Brocade Root CA 1 (27F56FFA1D06519743A9CFC2A86B1E5D9D8C125)
- Expiration Date:** 20270302 0924 PST
- Begin Date:** 20170202 0924 PST
- Key Length:** 2048
- Serial Number:** 8711ba5e8391e9a7df975df2620c131241866dd
- Thumbprint:** E481B9C167D066B401D715B505C2CFE2779868EF

**RADIUS Information**

cloudpathsqa.english.brocade.com  
jchandra@brocade.com  
Version 5.0.3314  
Use of this website signifies your agreement to the EULA

http://cloudpathsqa.english.brocade.com/admin/enrollmentData/Enrollment-5D38AB91-8E30-489C-8434-DA4D31F5C948/ Cloudpath ES

**Issued Certificate**

- Status:** Valid
- Common Name:** jchandra@brocade.com@defaultcert.www.brocade.com
- Certificate Template:** username@defaultcert.www.brocade.com
- Certificate Type:** User + Device
- Certificate Chain:** Brocade Intermediate CA 1 (61E82C43423217C8CB66C2C51A80EDF0D295839)  
Brocade Root CA 1 (27F56FFA1D06519743A9CFC2A86B1E5D9D8C125)
- Expiration Date:** 20270302 0924 PST
- Begin Date:** 20170202 0924 PST
- Key Length:** 2048
- Serial Number:** 8711ba5e8391e9a7df975df2620c131241866dd
- Thumbprint:** E481B9C167D066B401D715B505C2CFE2779868EF

**RADIUS Information**

Attribute	Value
Acct-Session-Id	
Calling-Station-Id	A0:36:9F:6E:1F:D0
Class	
Cpn-Certificate-Pk	39
Cpn-Certificate-Template-Pk	2
Cpn-Enrollment-Pk	1775
Cpn-Radius-Client-Pk	4
Cpn-Registration-Pk	
Cpn-Ssid	Ethernet
Filter-Id	ip-acl:in
NAS-Identifier	ICV-Switch
Session-Timeout	
Tunnel-Medium-Type	IEEE-802
Tunnel-Private-Group-Id	UI300
Tunnel-Type	VLAN
User-Name	jchandra@brocade.com@defaultcert.www.brocade.com
accountPk	1
action	authentication

**Enrollment Variables**

**Authorization Data**

cloudpathsqa.english.brocade.com  
jchandra@brocade.com  
Version 5.0.3314  
Use of this website signifies your agreement to the EULA

The screenshot displays the Cloudpath ES administration interface. The browser address bar shows the URL: `http://cloudpathsqa.english.brocade.com/admin/certificate/39/view`. The page title is "View Certificate" and it includes a "Done" button in the top right corner.

The interface is divided into a left sidebar and a main content area. The sidebar contains a "Dashboard" section with links to various system management functions: Welcome, Connections, Enrollments, Users & Devices, Certificates, Notifications, Event Response, Configuration, Sponsorship, Certificate Authority, Administration, and Support. At the bottom of the sidebar, there is a small disclaimer: "cloudpathsqa.english.brocade.com (jchandra@brocade.com) Version 5.0.3114. Use of this website signifies your agreement to the EULA."

The main content area is titled "View Certificate" and features a "Certificate" section with the following details:

- Common Name:** jchandra@brocade.com@defaultcert.vvww.brocade.com
- Status:** Valid (Revoke)
- Valid Not Before:** 20170202 0924 PST
- Valid Not After:** 20270302 0924 PST
- Organization:** Brocade
- Organizational Unit:** IP SQA
- Locality:** San Jose
- State:** CA
- Country:** US
- Serial Number:** 8711ba5e8391ec9a7df675cf2620c131241866dd
- SHA Fingerprint:** E481B9C167D066B401D715B505C2CFE2779B68EF
- Certificate Template:** username@defaultcert.vvww.brocade.com
- Certificate Authority:** Brocade Intermediate CA 1
- Certificate Type:** User + Device
- Enrollment:** jchandra@brocade.com
- Notes:** .#

Below the certificate details, there are sections for "Download" and "Usage":

- Download:** Includes buttons for "Public Key" (View, Download PEM, Download DER, View Details) and "Chain" (View, Download PEM, Download PKCS7).
- Usage:**
  - Issued:** 130 minutes ago
  - SSID:** Ethernet
  - NAS Identifier:** IDU-Switch
  - NAS Port ID:** 2
  - Enforced Certificate Template:** username@defaultcert.vvww.brocade.com
  - VLAN ID:** U:300
  - Filter ID:** ipad1.in
  - Last OCSP:** 38 minutes ago
  - Last RADIUS Success:** 38 minutes ago
  - RADIUS Log Level:** Normal (Debug)

# MAC Authentication for an IP Phone

Configure MAC authentication for an IP phone.

**View Connection**
Done

**Status:** ● Connected

**Username:** jchandra@brocade.com

**IP Address:**

**MAC Address:** 00:24:C4:42:BB:24

**SSID:** Ethernet

**Session Start Time:** 26 minutes ago

**NAS Identifier:** ICX-Switch

**NAS IP:**

**NAS Port:**

**NAS Port Type:**

**Session ID:**

**Last Accounting Update:** 1580779 millis

**Input Traffic:** 0 Bytes (0 packets)

**Output Traffic:** 0 Bytes (0 packets)

**Accumulated Session Time:** 0 seconds

**Additional Information:** Enrollment Record

The screenshot shows the Cloudpath ES web interface. The main content area is titled "View Enrollment Record" and contains the following sections:

- Enrollment Information:**
  - Enrollment Status: Abandoned
  - Name: 0024442824
  - Location: 3110
  - MAC Address: 00:24:C4:42:BB:24
  - Last Seen by MAC Auth: 20170213 2019 PST
  - Notes:
- Connection Information:**
  - Connection State: Connected
  - Session Start Time: 30 minutes ago
  - Session Last Update: 30 minutes ago
  - WLAN Username: jchandra@brocade.com
  - Session ID:
    - IP Address:
    - SSID: Ethernet
    - NAS Identifier: ICX-Switch (null)
    - NAS Port: null
    - NAS Port Type: null
    - Input Traffic: 0 Bytes (0 packets)
    - Output Traffic: 0 Bytes (0 packets)
- MAC Registration:**

Status	Registration List	MAC Address	Username	Creation Date	Expiration Date	Last Seen	Network SSID(s)
Valid through 20200405 0700 PDT	Wired Mac Auth 1	00:24:C4:42:BB:24	0024442824	20170213 2019 PST	20200405 0700 PDT	20170213 2019 PST	
- Notifications:**
- RADIUS Information:**

The screenshot displays the Cloudpath ES administration console. At the top, it shows the 'NAS Port Type' as 'null' and traffic statistics: 'Input Traffic: 0 Bytes (0 packets)' and 'Output Traffic: 0 Bytes (0 packets)'. Below this, the 'MAC Registration' section contains a table with one entry:

Status	Registration List	MAC Address	Username	Creation Date	Expiration Date	Last Seen	Permitted SSID(s)
Valid through 20200403 0700 PDT	Wired Mac Auth 1	00:24:CA:42:88:24	01240420204	20170213 2018 PST	20200403 0700 PDT	20170213 2018 PST	

The 'RADIUS Information' section provides a detailed list of attributes and their values:

Attribute	Value
Acct-Session-Id	
Calling-Station-Id	00:24:CA:42:88:24
Class	
Con-Certificate-Pk	
Con-Certificate-Templates-Pk	
Con-Enrollment-Pk	1774
Con-Radius-Client-Pk	
Con-Registration-Pk	32
Con-Std	Ethernet
Fiber-Id	
ISP-Identifier	ICX-6-xxxx
Session-Time-out	2811778
Tunnel-Medium-Type	IEEE-802
Tunnel-Private-Group-Id	13000
Tunnel-Type	VLAN
User-Name	johndra@brocade.com
accountPk	1
ssidon	authentication

Additional sections like 'Enrollment Variables', 'System Data', and 'Cleanup' are visible but currently empty.

# Use Case 5: Authentication of a Phone, PC, and Guest User Using Flexible Authentication

---

• Cloudpath Configuration.....	63
• Switch Configuration .....	64
• Switch Show Commands and Syslog Information.....	66
• Combined Output for Both Ports e 1/1/1 (PC1) and e 1/1/2 (PC2 Behind the IP Phone).....	67
• Cloudpath Information.....	70

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. Refer to [Use Case 4: Authentication of an IP Phone and a PC on the Same Port Using Flexible Authentication](#) on page 47 for the PC behind the IP phone. Additionally, when the guest user PC1 needs to be enabled for 802.1X certificate-based authentication, the following example shows the configuration and validation of this use case.

## Client PC1 (Guest User)

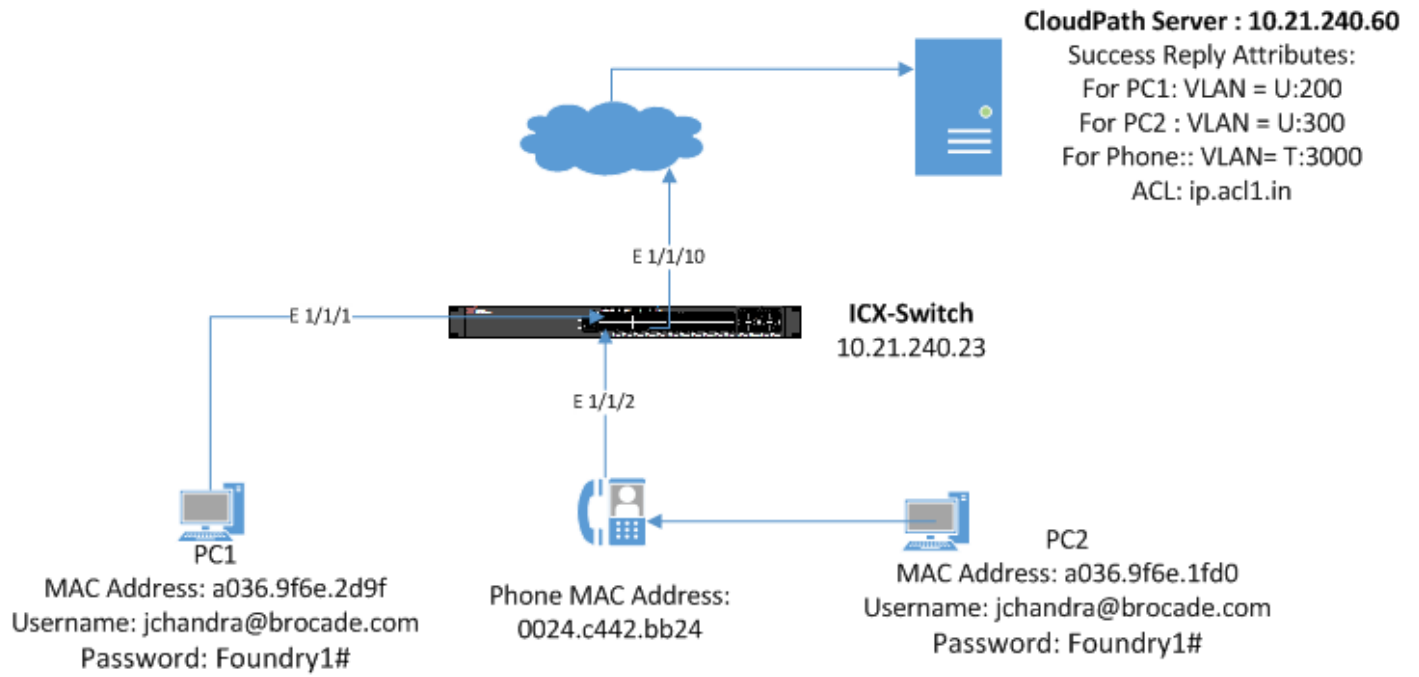
- 802.1X username: jchandra@brocade.com
- Password: Foundry1#
- After authentication:
  - The client should be placed in VLAN 200.
  - Incoming traffic from the client should be filtered by ACL "acl1".

**IP Phone:** The IP phone MAC address is 0024.c442.bb24, and the IP phone is in tagged VLAN 3000.

## Client PC2

- 802.1X username: jchandra@brocade.com
- Password: Foundry1#
- After authentication:
  - The client should be placed in VLAN 300.
  - Incoming traffic from the client should be filtered by ACL "acl1".

FIGURE 8 Example of Authenticating an IP Phone, a PC, and a Guest User Using Flexible Authentication



# Cloudpath Configuration

1. Configure the workflow for 802.1X guest user authentication for PC1, 802.1X authentication for PC2 (Employee), and MAC authentication for the IP phone.

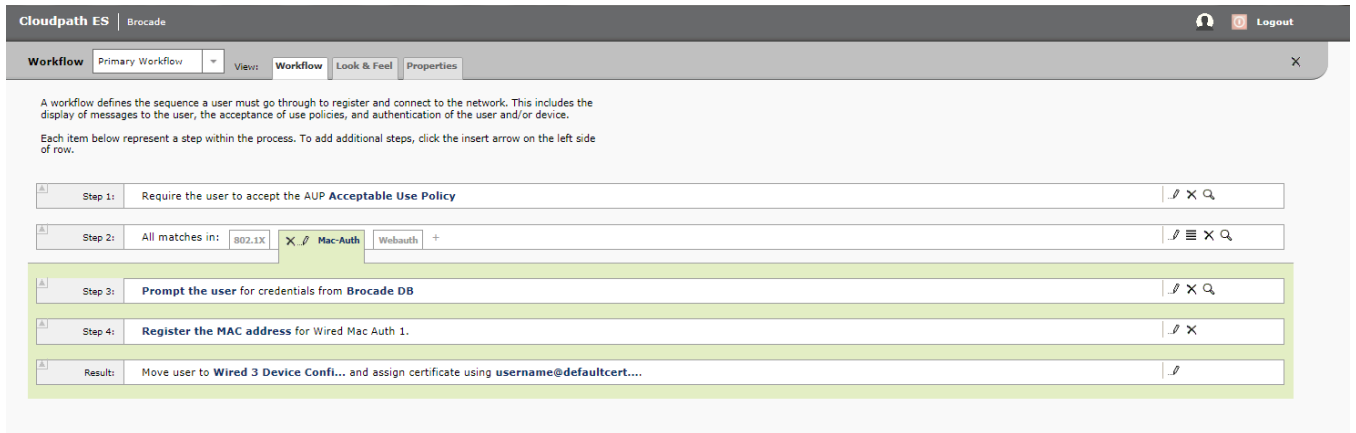
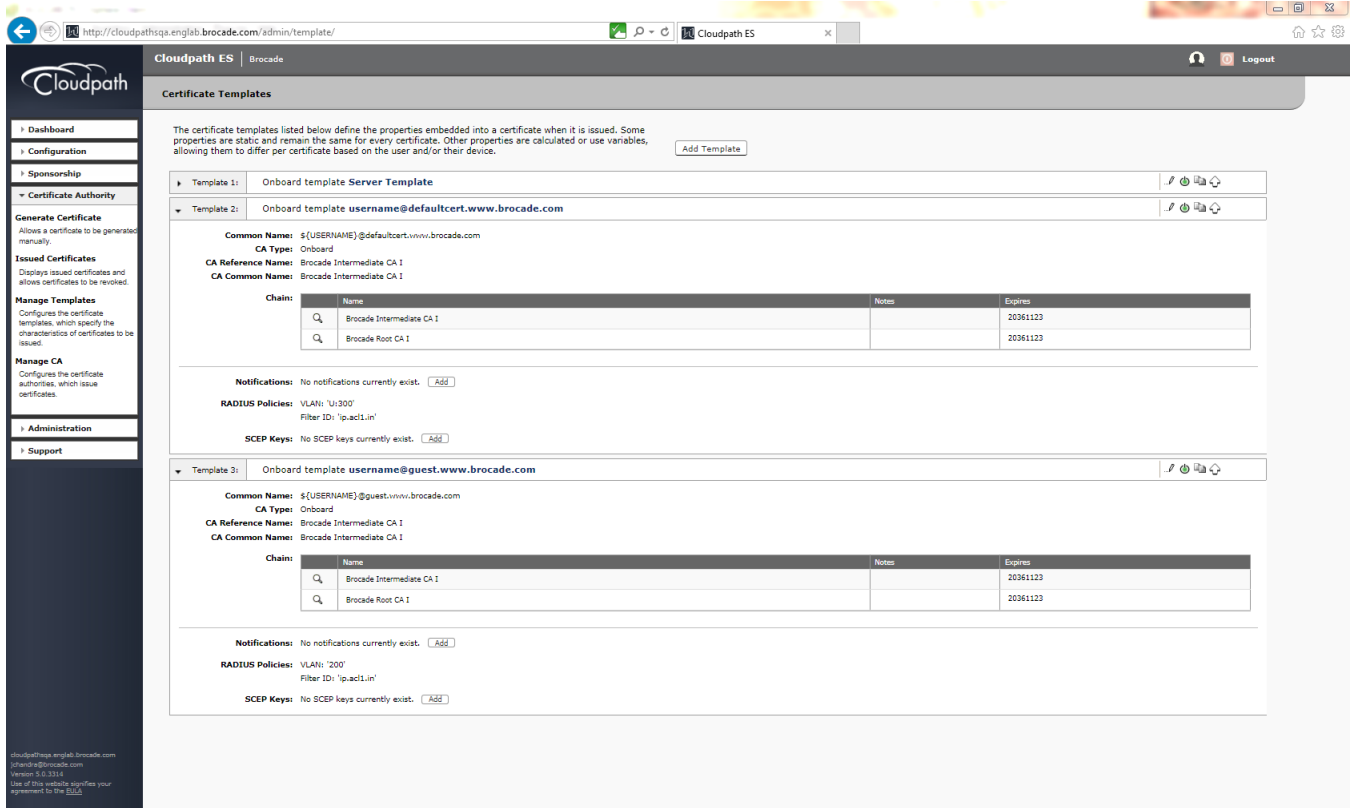
The screenshot shows the Cloudpath ES configuration page for a workflow. The interface includes a header with 'Cloudpath ES | Brocade' and a 'Logout' button. Below the header, there are tabs for 'Workflow', 'Look & Feel', and 'Properties'. The 'Workflow' tab is active, showing a list of steps:

- Step 1:** Require the user to accept the AUP **Acceptable Use Policy**
- Step 2:** All matches in: **802.1X** (selected), Mac-Auth, Webauth
- Step 3:** All matches in: **Employee** (selected), Guest
- Step 4:** Prompt the user for credentials from **Brocade DB**
- Result:** Move user to **Wired 3 Device Confi...** and assign certificate using **username@defaultcert...**

The screenshot shows the Cloudpath ES configuration page for a workflow. The interface includes a header with 'Cloudpath ES | Brocade' and a 'Logout' button. Below the header, there are tabs for 'Workflow', 'Look & Feel', and 'Properties'. The 'Workflow' tab is active, showing a list of steps:

- Step 1:** Require the user to accept the AUP **Acceptable Use Policy**
- Step 2:** All matches in: **802.1X** (selected), Mac-Auth, Webauth
- Step 3:** All matches in: **Employee**, **Guest** (selected)
- Step 4:** Send a **verification code** from **Guest Voucher List**
- Result:** Move user to **Wired 3 Device Confi...** and assign certificate using **username@guest.www.b....**

- Navigate to **Certificate Authority > Manage Templates** and verify the RADIUS policies.



# Switch Configuration

```
!
captive-portal cp-sqal
virtual-ip Cloudpathsqa.englab.brocade.com
virtual-port 80
login-page /enroll/Brocade/Production/
```



```

!
vlan 2 name AUTH-DEFAULT by port
!
vlan 3 name 802.1X-GUEST by port
  tagged ethe 1/1/10
  router-interface ve 3
  webauth
    captive-portal profile cp-sqal
    auth-mode captive-portal
    no secure-login
    trust-port ethernet 1/1/10
    enable
!
!
vlan 200 name GUEST by port
  tagged ethe 1/1/10
  router-interface ve 200
!
vlan 300 name 802.1X by port
  tagged ethe 1/1/10
  router-interface ve 300
!
vlan 3000 name VOICE by port
  tagged ethe 1/1/2 ethe 1/1/10
  router-interface ve 3000
!
!
authentication
  auth-default-vlan 2
  dot1x enable
  dot1x enable ethe 1/1/1 to 1/1/2
  dot1x guest-vlan 3
  mac-authentication enable
  mac-authentication enable ethe 1/1/2
!
!
aaa authentication dot1x default radius
radius-server host 10.21.240.60 auth-port 1812 acct-port 1813 default key Foundry1 dot1x mac-auth web-auth
!
interface ethernet 1/1/1
  dot1x port-control auto
!
interface ethernet 1/1/2
  dot1x port-control auto
  port-name PHONE-G06
  inline power
!
!
interface ve 3
  ip address 10.21.80.189/27
!
interface ve 200
  ip address 10.21.80.157/27
!
interface ve 300
  ip address 10.21.80.249/27
!
interface ve 3000
  ip address 10.21.80.125/27
!
ip access-list extended acl1
  permit ip any any
!
lldp med network-policy application voice tagged vlan 3000 priority 4 dscp 46 ports ethe 1/1/2
lldp run
!

```

## Switch Show Commands and Syslog Information

**For PC1 Guest User:** The client is enabled for 802.1X certificate-based authentication. Without a certificate, the guest user will be placed in the 802.1X Guest VLAN. To perform captive-portal authentication, download and install the certificate. Disconnect the client and, while reconnecting, the user will be placed in VLAN 200.

**For PC2 behind the IP Phone:** Refer to [Use Case 4: Authentication of an IP Phone and a PC on the Same Port Using Flexible Authentication](#) on page 47.

```
ICX-Switch#
SYSLOG: <14> Mar  2 17:18:30 ICX-Switch System: Interface ethernet 1/1/1, state up

SYSLOG: <14> Mar  2 17:18:31 ICX-Switch DOT1X: Port 1/1/1 - mac a036.9f6e.2d9f AuthControlledPortStatus change:
unauthorized

SYSLOG: <13> Mar  2 17:19:00 ICX-Switch DOT1X: Port 1/1/1 Mac a036.9f6e.2d9f - is moved to guest vlan

SYSLOG: <13> Mar  2 17:19:00 ICX-Switch FLEXAUTH: Port ethe 1/1/1  is added into VLAN 3 as MAC-VLAN member

SYSLOG: <13> Mar  2 17:19:00 ICX-Switch FLEXAUTH: Port ethe 1/1/1  is deleted from VLAN 2 as MAC-VLAN member

ICX-Switch#sds
show dot1x sessions all
-----
Port      MAC              IP (v4/v6)      User      VLAN  Auth   ACL   Session  Age  PAE
  Addr                    Addr          Name                                     State   State Time    State
-----
1/1/1    a036.9f6e.2d9f   N/A             N/A       3     init   None    46      S0    HELD

ICX-Switch#show vlan 3
Total PORT-VLAN entries: 8
Maximum PORT-VLAN entries: 64

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

PORT-VLAN 3, Name 802.1X-GUEST, Priority level0, Spanning tree Off
  Untagged Ports: None
  Tagged Ports: (U1/M1)  10
  Uplink Ports: None
  DualMode Ports: None
  Mac-Vlan Ports: (U1/M1)  1
  Monitoring: Disabled

ICX-Switch#
SYSLOG: <14> Mar  2 17:19:29 ICX-Switch CLI CMD: "show vlan 3" by un-authenticated user from console

SYSLOG: <13> Mar  2 17:27:15 ICX-Switch FLEXAUTH: Port ethe 1/1/1  is added into VLAN 2 as MAC-VLAN member

SYSLOG: <13> Mar  2 17:27:15 ICX-Switch FLEXAUTH: Port ethe 1/1/1  is deleted from VLAN 3 as MAC-VLAN member

SYSLOG: <14> Mar  2 17:27:16 ICX-Switch DOT1X: Port 1/1/1 - mac a036.9f6e.2d9f AuthControlledPortStatus change:
unauthorized

SYSLOG: <14> Mar  2 17:28:00 ICX-Switch System: Interface ethernet 1/1/1, state down

SYSLOG: <14> Mar  2 17:28:07 ICX-Switch System: Interface ethernet 1/1/1, state up

SYSLOG: <14> Mar  2 17:28:07 ICX-Switch DOT1X: Port 1/1/1 - mac a036.9f6e.2d9f AuthControlledPortStatus change:
unauthorized

SYSLOG: <13> Mar  2 17:28:35 ICX-Switch DOT1X: Port 1/1/1 Mac a036.9f6e.2d9f - is moved to guest vlan

SYSLOG: <13> Mar  2 17:28:35 ICX-Switch FLEXAUTH: Port ethe 1/1/1  is added into VLAN 3 as MAC-VLAN member

SYSLOG: <13> Mar  2 17:28:35 ICX-Switch FLEXAUTH: Port ethe 1/1/1  is deleted from VLAN 2 as MAC-VLAN member

SYSLOG: <13> Mar  2 17:28:52 ICX-Switch FLEXAUTH: Port ethe 1/1/1  is added into VLAN 2 as MAC-VLAN member
```

```

SYSLOG: <13> Mar  2 17:28:52 ICX-Switch FLEXAUTH: Port ethe 1/1/1  is deleted from VLAN 3 as MAC-VLAN member
SYSLOG: <14> Mar  2 17:28:52 ICX-Switch DOT1X: Port 1/1/1 - mac a036.9f6e.2d9f AuthControlledPortStatus change: unauthorized
SYSLOG: <14> Mar  2 17:28:58 ICX-Switch DOT1X: Port 1/1/1 - mac a036.9f6e.2d9f, AuthControlledPortStatus change: authorized
SYSLOG: <13> Mar  2 17:28:58 ICX-Switch FLEXAUTH: Port ethe 1/1/1  is added into VLAN 200 as MAC-VLAN member
SYSLOG: <13> Mar  2 17:28:58 ICX-Switch FLEXAUTH: Port ethe 1/1/1  is deleted from VLAN 2 as MAC-VLAN member

```

ICX-Switch#show dot1x sessions all

Port	MAC Addr	IP (v4/v6) Addr	User Name	VLAN	Auth State	ACL	Session Time	Age	PAE State
1/1/1	a036.9f6e.2d9f	10.21.80.161	jchandra@broc	200	permit	Yes	11		Ena

```

AUTHENTICATED
ICX-Switch#
sdi
show dot1x ip-acl all

```

Port	MAC Address	V4 Ingress	V4 Egress	V6 Ingress	V6 Egress
1/1/1	a036.9f6e.2d9f	acl1	-	-	-

```

ICX-Switch#show vlan 200
Total PORT-VLAN entries: 8
Maximum PORT-VLAN entries: 64

```

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

```

PORT-VLAN 200, Name GUEST, Priority level0, Spanning tree Off
Untagged Ports: None
Tagged Ports: (U1/M1)  10
Uplink Ports: None
DualMode Ports: None
Mac-Vlan Ports: (U1/M1)  1
Monitoring: Disabled

```

## Combined Output for Both Ports e 1/1/1 (PC1) and e 1/1/2 (PC2 Behind the IP Phone)

ICX-Switch#

```

SYSLOG: <14> Mar  2 17:39:07 ICX-Switch System: PoE: Allocated power of 30000 mwatts on port 1/1/2.
SYSLOG: <14> Mar  2 17:39:09 ICX-Switch System: PoE: Power adjustment done: decreased power by 14600 mwatts on port 1/1/2 .
SYSLOG: <14> Mar  2 17:39:09 ICX-Switch System: PoE: Power enabled on port 1/1/2.
SYSLOG: <14> Mar  2 17:39:13 ICX-Switch System: Interface ethernet 1/1/2, state up
SYSLOG: <14> Mar  2 17:39:14 ICX-Switch DOT1X: Port 1/1/2 - mac a036.9f6e.1fd0 AuthControlledPortStatus change: unauthorized
SYSLOG: <14> Mar  2 17:39:21 ICX-Switch DOT1X: Port 1/1/2 - mac 0024.c442.bb24 AuthControlledPortStatus change: unauthorized
SYSLOG: <14> Mar  2 17:39:26 ICX-Switch DOT1X: Port 1/1/2 - mac a036.9f6e.1fd0, AuthControlledPortStatus change: authorized
SYSLOG: <13> Mar  2 17:39:26 ICX-Switch FLEXAUTH: Port ethe 1/1/2  is added into VLAN 300 as MAC-VLAN member

```

SYSLOG: <13> Mar 2 17:39:26 ICX-Switch FLEXAUTH: Port ethe 1/1/2 is deleted from VLAN 2 as MAC-VLAN member

SYSLOG: <13> Mar 2 17:40:20 ICX-Switch MAC Authentication succeeded for [0024.c442.bb24 ] on port 1/1/2

ICX-Switch#show dot1x sessions all

Port	MAC Addr	IP (v4/v6) Addr	User Name	VLAN	Auth State	ACL	Session Time	Age	PAE State
1/1/1	a036.9f6e.2d9f	10.21.80.129	jchandra@broc	200	permit	Yes	692	Ena	
AUTHENTICATED									
1/1/2	0024.c442.bb24	N/A	N/A	300	init	None	64	Ena	HELD
1/1/2	a036.9f6e.1fd0	10.21.80.228	jchandra@broc	300	permit	Yes	71	Ena	
AUTHENTICATED									

ICX-Switch#show mac-auth sessions all

Port	MAC Addr	IP (v4/v6) Addr	VLAN	Auth State	ACL	Session Time	Age
1/1/2	0024.c442.bb24	10.21.80.97	3000	Yes	None	258	Ena
1/1/2	0024.c442.bb24	N/A	300	Yes	None	270	Ena

ICX-Switch#show dot1x ip-acl all

Port	MAC Address	V4 Ingress	V4 Egress	V6 Ingress	V6 Egress
1/1/1	a036.9f6e.2d9f	acl1	-	-	-
1/1/2	0024.c442.bb24	-	-	-	-
1/1/2	a036.9f6e.1fd0	acl1	-	-	-

ICX-Switch#show mac-authentication ip-acl all

Port	MAC Address	V4 Ingress	V4 Egress	V6 Ingress	V6 Egress
1/1/2	0024.c442.bb24	-	-	-	-
1/1/2	0024.c442.bb24	-	-	-	-

ICX-Switch#show vlan 300  
 Total PORT-VLAN entries: 8  
 Maximum PORT-VLAN entries: 64

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

PORT-VLAN 300, Name 802.1X, Priority level0, Spanning tree Off  
 Untagged Ports: None  
 Tagged Ports: (U1/M1) 10  
 Uplink Ports: None  
 DualMode Ports: None  
 Mac-Vlan Ports: (U1/M1) 2  
 Monitoring: Disabled

ICX-Switch#show vlan 200  
 Total PORT-VLAN entries: 8  
 Maximum PORT-VLAN entries: 64

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

PORT-VLAN 200, Name GUEST, Priority level0, Spanning tree Off  
 Untagged Ports: None  
 Tagged Ports: (U1/M1) 10  
 Uplink Ports: None  
 DualMode Ports: None  
 Mac-Vlan Ports: (U1/M1) 1  
 Monitoring: Disabled

ICX-Switch#show vlan 3000  
 Total PORT-VLAN entries: 8  
 Maximum PORT-VLAN entries: 64

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

```
PORT-VLAN 3000, Name VOICE, Priority level0, Spanning tree Off
Untagged Ports: None
Tagged Ports: (U1/M1) 2 10
Uplink Ports: None
DualMode Ports: None
Mac-Vlan Ports: None
Monitoring: Disabled
```

```
ICX-Switch#show lldp local-info port e 1/1/2
Local port: 1/1/2
+ Chassis ID (MAC address): cc4e.24b4.7b30
+ Port ID (MAC address): cc4e.24b4.7b31
+ Time to live: 120 seconds
+ System name : "ICX-Switch"
+ Port description : "GigabitEthernet1/1/2"
+ System capabilities : bridge, router
Enabled capabilities: bridge, router
+ 802.3 MAC/PHY : auto-negotiation enabled
Advertised capabilities: 10BaseT-HD, 10BaseT-FD, 100BaseTX-HD,
100BaseTX-FD, fdxSPause, fdxBPause, 1000BaseT-HD,
1000BaseT-FD
Operational MAU type : 10BaseT-FD
+ 802.3 Power via MDI: PSE port, power enabled, class 3
Power Pair : A (not controllable)
Power Type : Type 2 PSE device
Power Source : Unknown Power Source
Power Priority : Low (3)
Power Requested: 12.0 watts (PSE equivalent: 13190 mWatts)
Power Allocated: 12.0 watts (PSE equivalent: 13190 mWatts)
+ Link aggregation: not capable
+ Maximum frame size: 1522 octets
+ MED capabilities: capabilities, networkPolicy, location, extendedPSE
```

SYSLLOG: <14> Mar 2 17:43:04 ICX-Switch CLI CMD: "show lldp local-info ports ethernet 1/1/2" by un-authenticated user from console

```
MED device type : Network Connectivity
+ MED Network Policy
Application Type : Voice
Policy Flags : Known Policy, Tagged
VLAN ID : 3000
L2 Priority : 4
DSCP Value : 46
+ MED Extended Power via MDI
Power Type : PSE device
Power Source : Unknown Power Source
Power Priority : Low (3)
Power Value : 12.0 watts (PSE equivalent: 13190 mWatts)
+ Port VLAN ID: none
+ Management address (IPv4): 10.21.80.249
```

Refer following show command to check status of radius server.

```
ICX-Switch#show radius server
```

```
-----
```

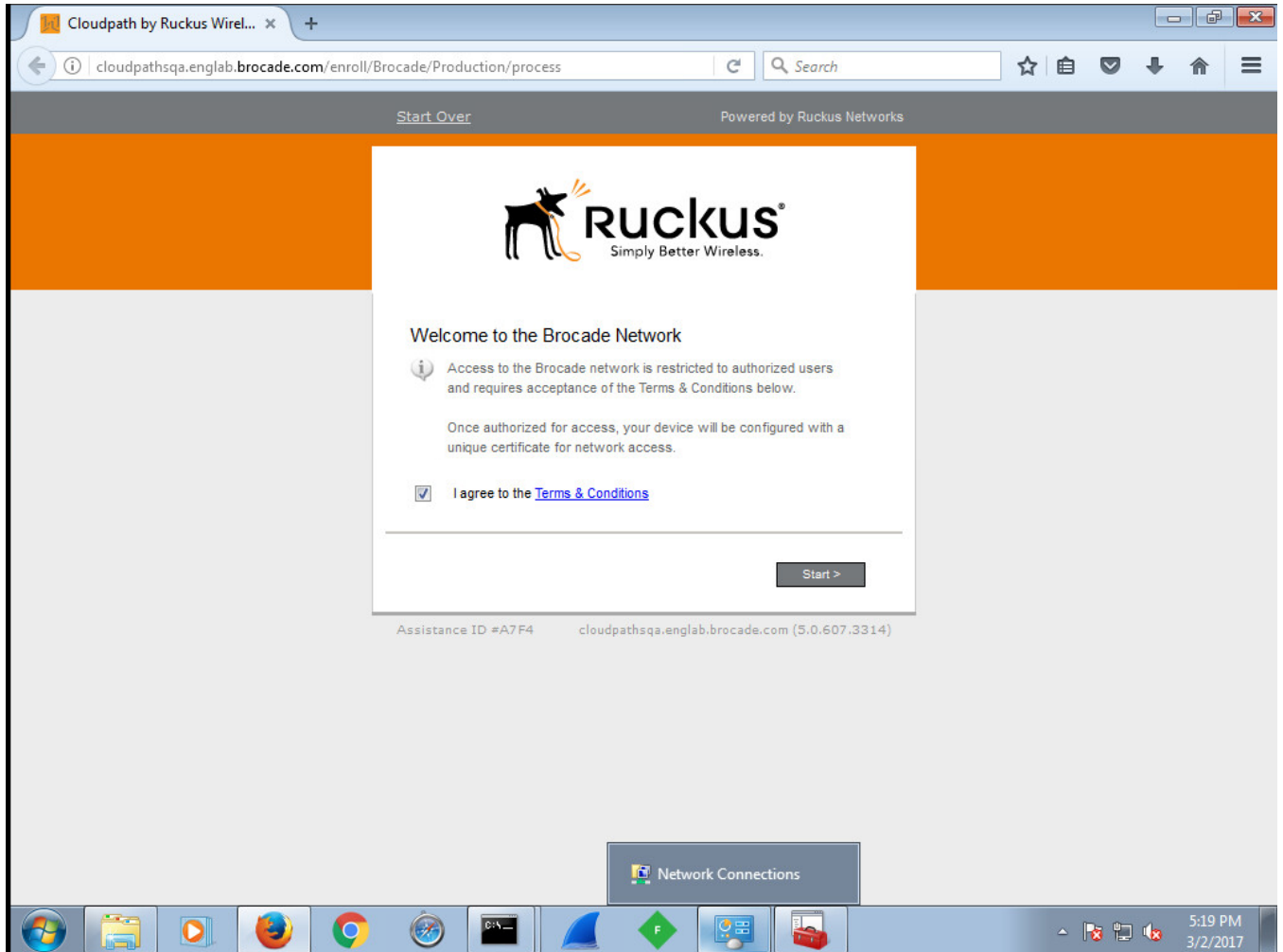
Server	Tyoe	Opens	Closes	Timeouts	Status
10.21.240.60	any	0	0	0	active

```
-----
```

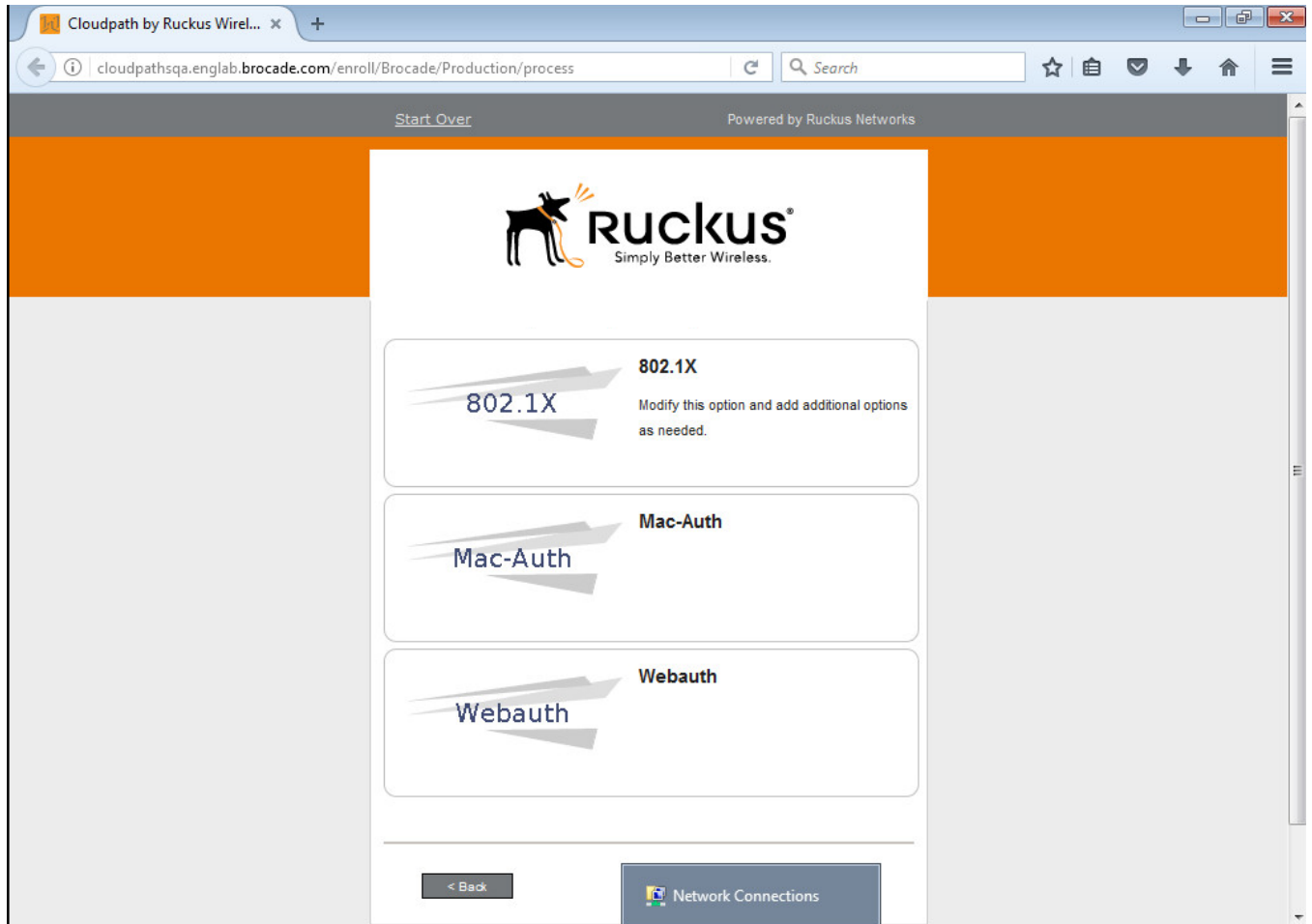
# Cloudpath Information

For **Guest User PC1**: Once the user is moved to the 802.1X Guest VLAN, perform captive-portal authentication.

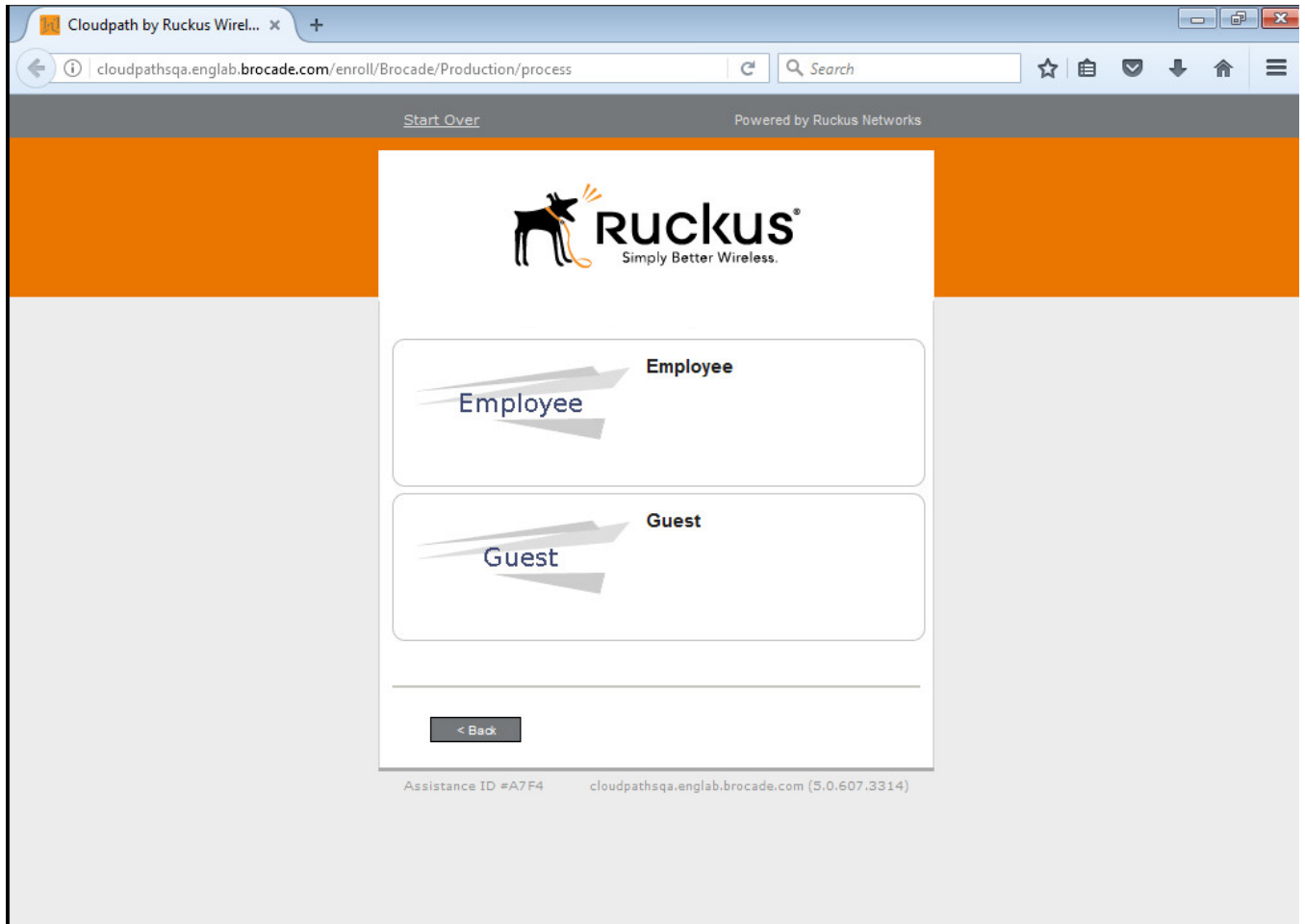
1. Accept the user policy and click **Start**.



2. Select **802.1X**.

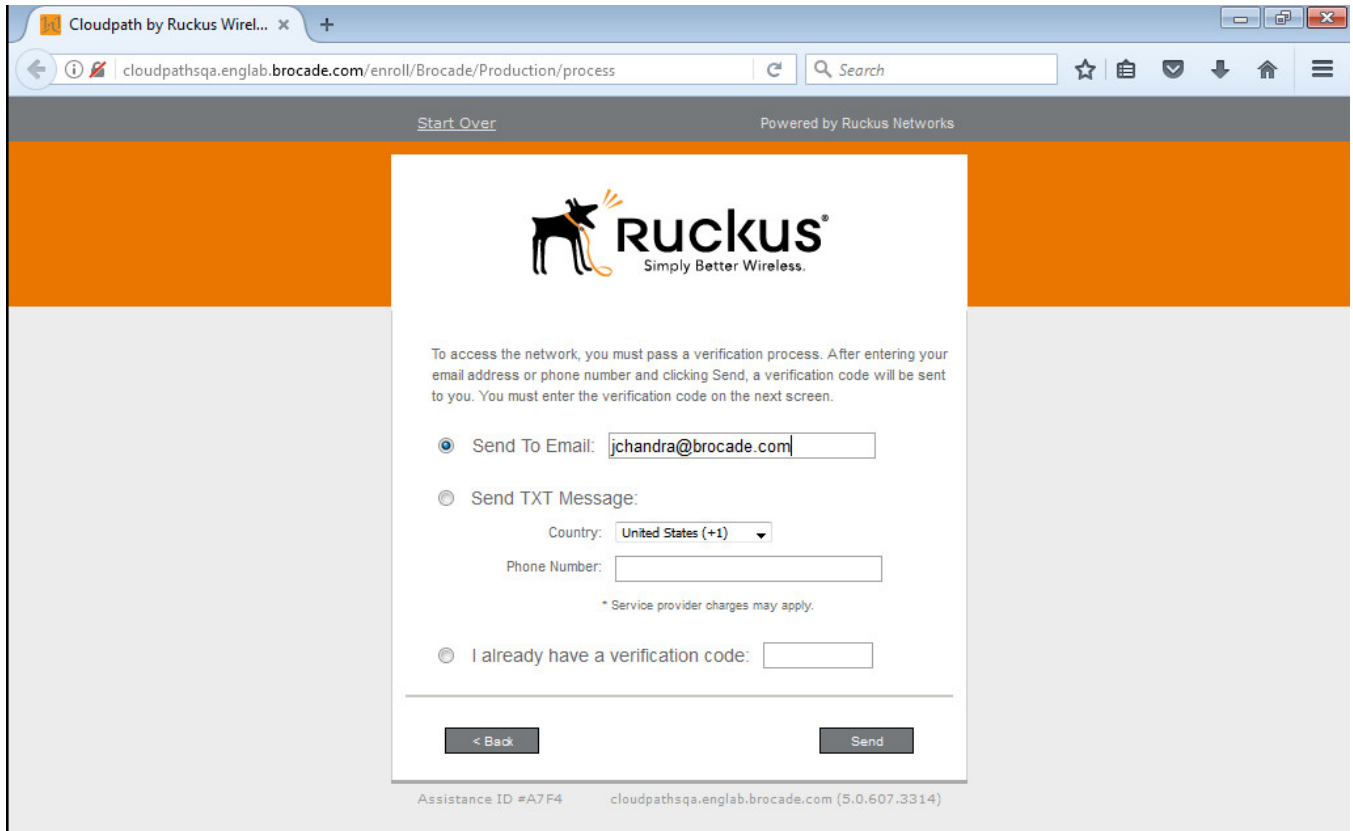


3. Select **Guest**.

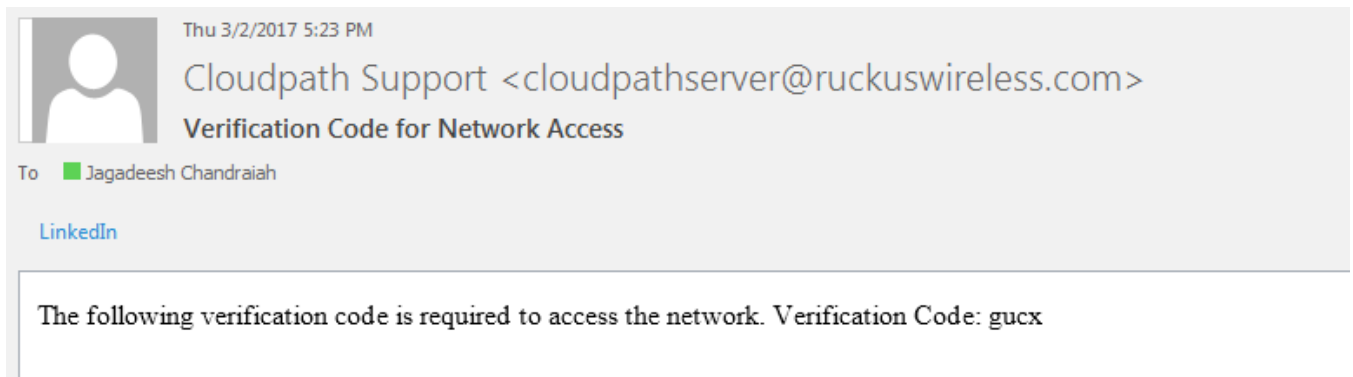




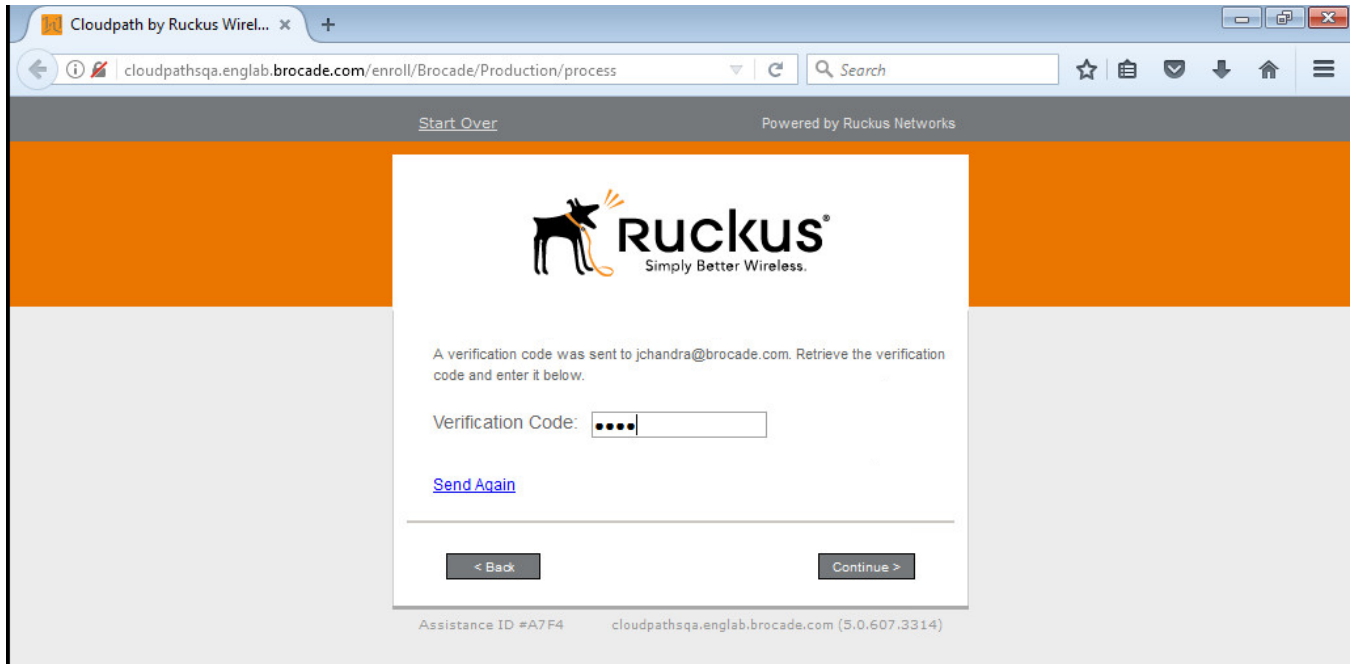
4. Provide an email address or phone number, and click **Send**.



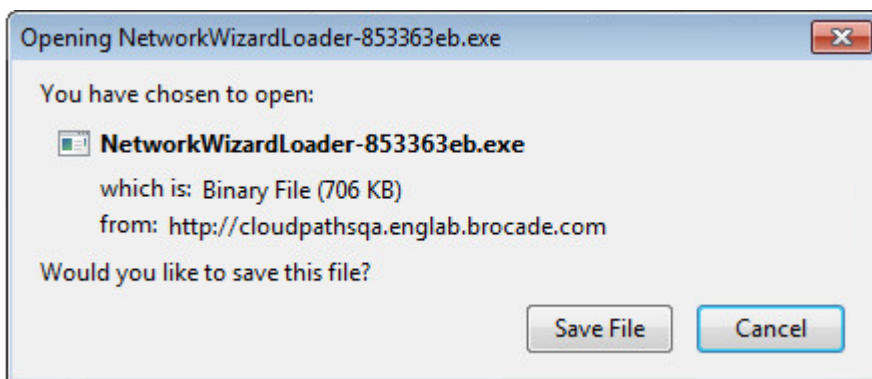
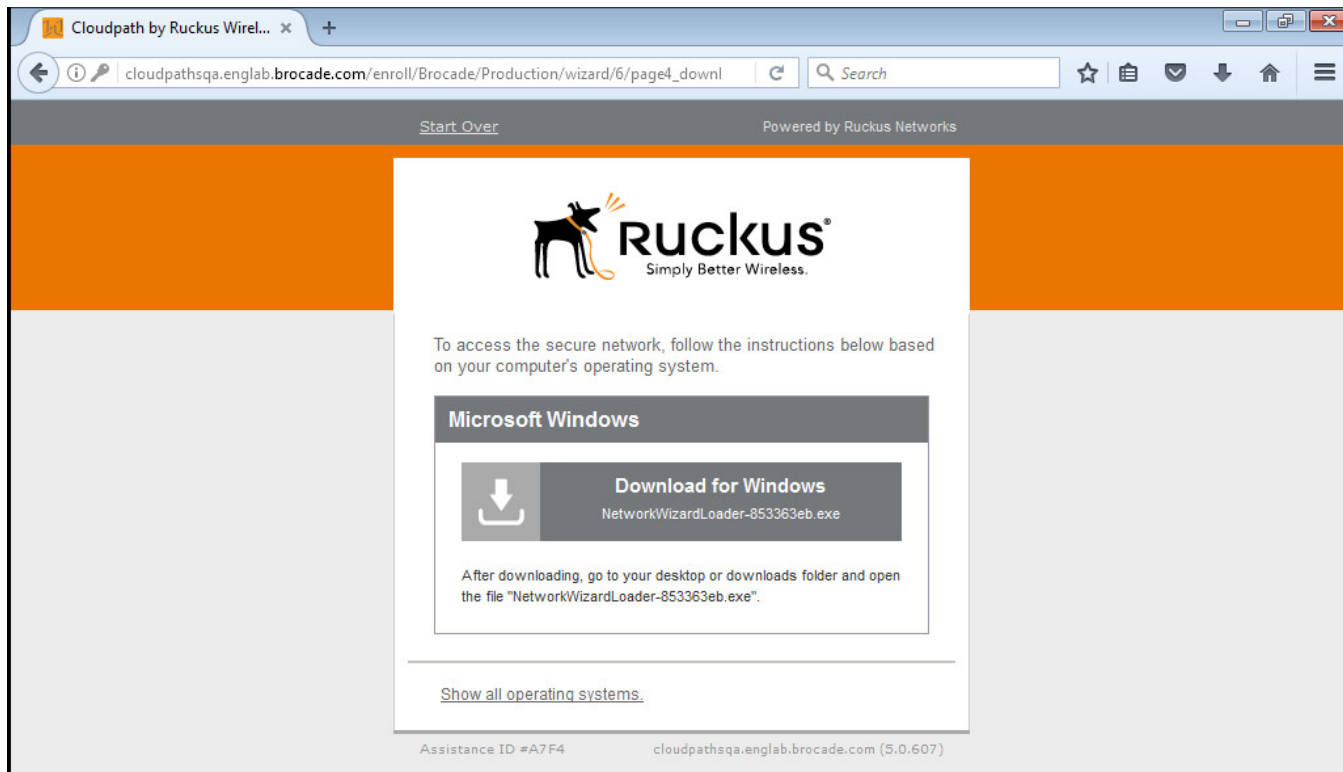
Depending on the email or phone number, the user will receive the email or text notification with a verification code.

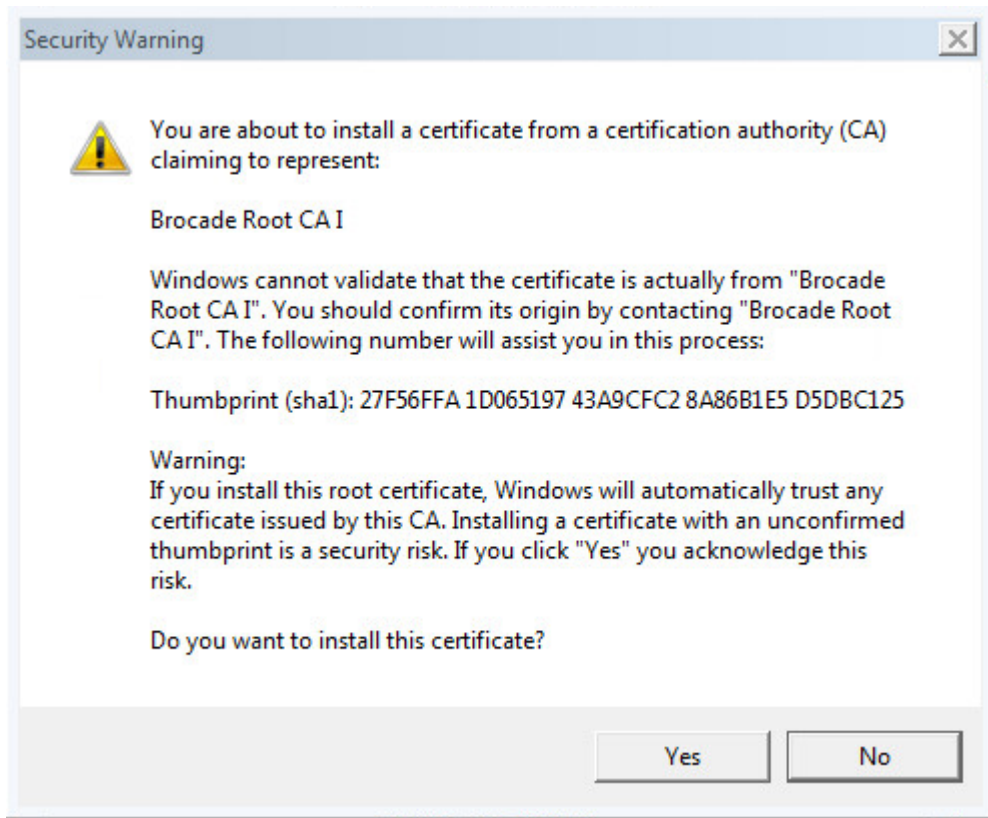


5. Provide the verification code and press **Continue**.



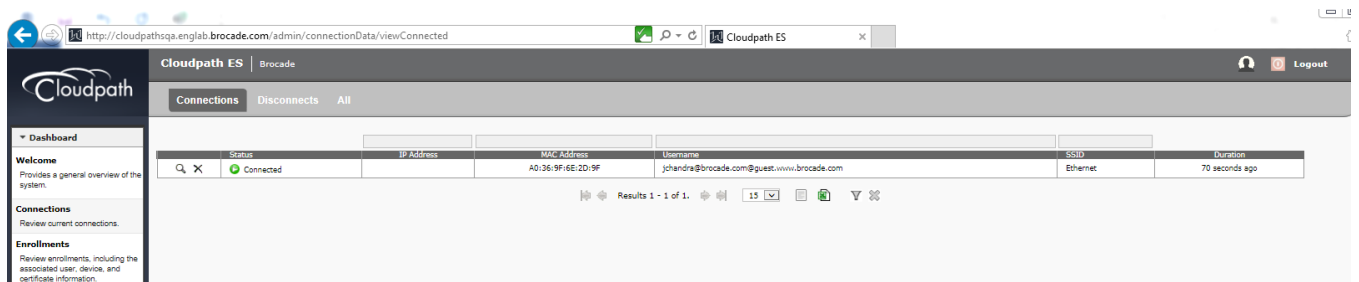
6. Download the application and install the certificate.







7. Disconnect and enable the network connection on the client.
8. Navigate to **Connections** and look for the guest user authentication. Click the search button to view the connection.



9. Click **Enrollment Record** for additional information.

**View Connection** Done

**Status:** ● Connected

**Username:** jchandra@brocade.com@guest.www.brocade.com

**IP Address:**

**MAC Address:** A0:36:9F:6E:2D:9F

**SSID:** Ethernet

**Session Start Time:** 102 seconds ago

**NAS Identifier:** ICX-Switch

**NAS IP:**

**NAS Port:**

**NAS Port Type:**

**Session ID:**

**Last Accounting Update:** 101770 millis

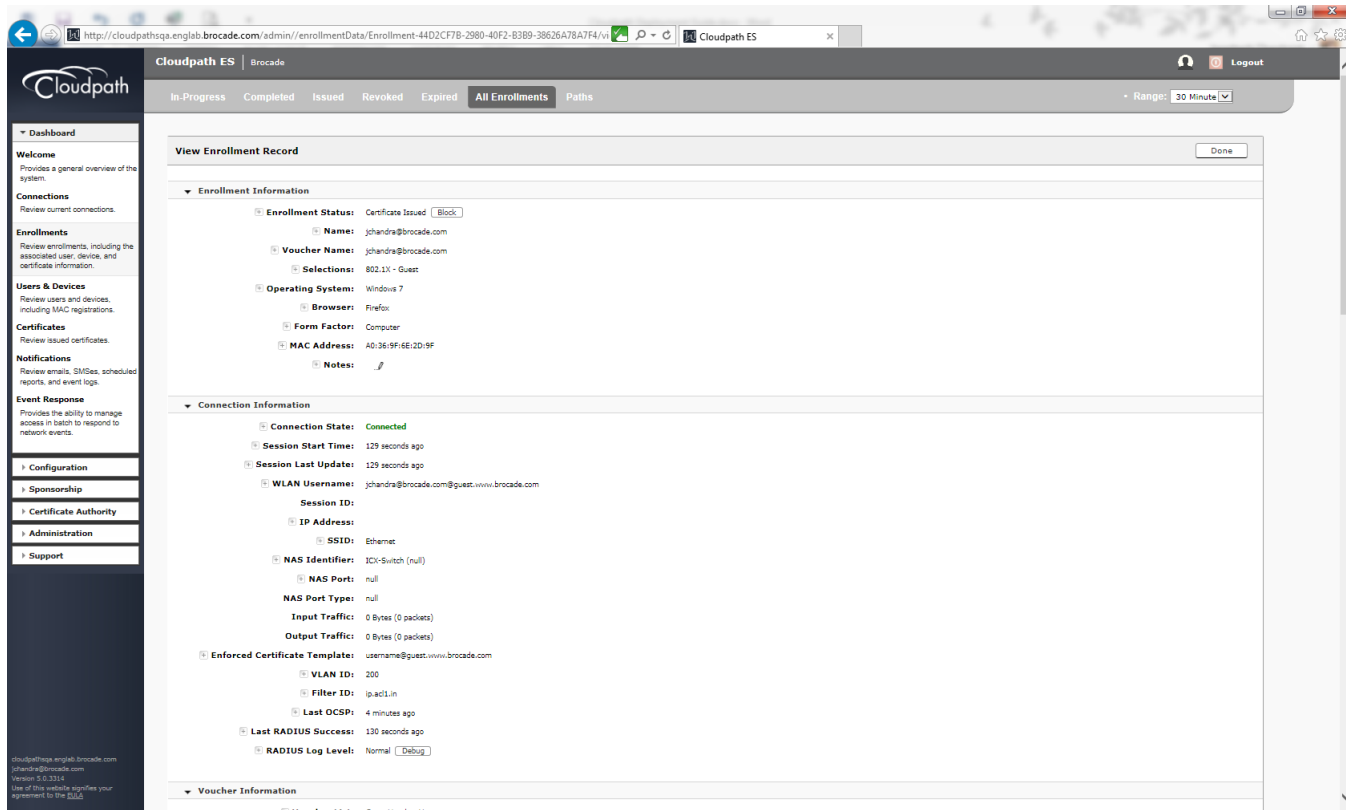
**Input Traffic:** 0 Bytes (0 packets)

**Output Traffic:** 0 Bytes (0 packets)

**Accumulated Session Time:** 0 seconds

**Additional Information:** [Enrollment Record](#)

10. Check for VLAN ID, Filter ID, voucher, device and workflow information for more details.



http://cloudpathsqa.englishlab.brocade.com/admin/enrollmentData/Enrollment-44D2CF7B-2980-40F2-83B9-38626A78A7F4/vi Cloudpath ES

**Voucher Information**

- Voucher List: Guest Voucher List
- Voucher: guox
- Status: Consumed
- Name: jchandra@brocade.com
- Email: jchandra@brocade.com
- Date Consumed: 20170302 1226 PST

**Device Information**

**Workflow Information**

Step	Workflow Step	Result
Step 1	Require the user to accept the AUP Acceptable Use Policy	Accepted on 20170302 1221 PST
Step 2	All matches in:	Will prompt user to select from: 802.1X, Mac-Auth, Webauth Selection: 802.1X
Step 3	All matches in:	Will prompt user to select from: Employee, Guest Selection: Guest
Step 4	Send a verification code from Guest Voucher List	Voucher code 'guox' emailed to 'jchandra@brocade.com'. Successfully submitted voucher code 'guox'. Name: jchandra@brocade.com
Result	User has completed the workflow.	The user is authorized to receive a certificate from 'username@guest.www.brocade.com'.
Certificate	User has been issued a certificate.	jchandra@brocade.com@guest.www.brocade.com valid until 20180302.
Connection	User has authenticated.	Last authentication: 130 seconds ago

**Notifications**

Type	Address	Last Known Status	Timestamp	Subject	Skip Reason
Email	jchandra@brocade.com	Email sent.	20170302 1224 PST	Verification Code for Network Access	

**Issued Certificate**

- Status: Valid [Revoke](#)
- Common Name: jchandra@brocade.com@guest.www.brocade.com [View Details](#)
- Certificate Template: username@guest.www.brocade.com
- Certificate Type: User + Device
- Certificate Chain: Brocade Intermediate CA 1 (61E82C4342C3217C9CB66C2C31A80EDF0D295839)  
Brocade Root CA 1 (27F56FFA1D06519743A9CF28A8681E5D5D6C125)
- Expiration Date: 20180302 1228 PST
- Begin Date: 20170202 1228 PST
- Key Length: 2048
- Serial Number: 4448a0a393602c453be41e1cf0ad98df9a1
- Thumbprint: EE7CA45856809677221F5D4DF369530EC22725E

cloudpathsqa.englishlab.brocade.com  
jchandra@brocade.com  
Version 5.0.3314  
Use of this website signifies your agreement to the [EULA](#)

http://cloudpathsqa.englishlab.brocade.com/admin/enrollmentData/Enrollment-44D2CF7B-2980-40F2-83B9-38626A78A7F4/vi Cloudpath ES

**Issued Certificate**

- Status: Valid [Revoke](#)
- Common Name: jchandra@brocade.com@guest.www.brocade.com [View Details](#)
- Certificate Template: username@guest.www.brocade.com
- Certificate Type: User + Device
- Certificate Chain: Brocade Intermediate CA 1 (61E82C4342C3217C9CB66C2C31A80EDF0D295839)  
Brocade Root CA 1 (27F56FFA1D06519743A9CF28A8681E5D5D6C125)
- Expiration Date: 20180302 1228 PST
- Begin Date: 20170202 1228 PST
- Key Length: 2048
- Serial Number: 4448a0a393602c453be41e1cf0ad98df9a1
- Thumbprint: EE7CA45856809677221F5D4DF369530EC22725E

**RADIUS Information**

Attribute	Value
Acc-Session-Id	
Calling-Station-Id	AD:36:19F:6E:2D:9F
Class	
Cpn-Certificate-Pk	40
Cpn-Certificate-Template-Pk	3
Cpn-Enrollment-Pk	1777
Cpn-Radius-Client-Pk	4
Cpn-Registration-Pk	
Cpn-SeqId	Ethemet
Filter-Id	ip-ac1.in
NAS-Identifier	ICX-Switch
Session-Timeout	
Tunnel-Medium-Type	IEEE-802
Tunnel-Private-Group-Id	200
Tunnel-Type	VLAN
User-Name	jchandra@brocade.com@guest.www.brocade.com
accountPk	1
action	authentication

**Enrollment Variables**

**Authorization Data**

**System Data**

cloudpathsqa.englishlab.brocade.com  
jchandra@brocade.com  
Version 5.0.3314  
Use of this website signifies your agreement to the [EULA](#)



The combined output for port e 1/1/1 (PC1) and e 1/1/2 (PC behind the IP Phone) is displayed.

The screenshot shows the Cloudpath ES admin interface. The main content area displays a table of active connections. The table has columns for Status, IP Address, MAC Address, Username, SSID, and Duration. There are three rows of data, all with a 'Connected' status.

Status	IP Address	MAC Address	Username	SSID	Duration
Connected		A0:36:9F:6E:1F:D0	jchandra@brocade.com@defaultcert.www.brocade.com	Ethernet	10 minutes ago
Connected		A0:36:9F:6E:2D:9F	jchandra@brocade.com@guest.www.brocade.com	Ethernet	20 minutes ago
Connected		00:24:C4:42:BB:24	jchandra@brocade.com	Ethernet	9 minutes ago

The 'View Connection' dialog box provides detailed information about a specific connection. The status is 'Connected'. The username is 'jchandra@brocade.com@defaultcert.www.brocade.com'. The IP address is not explicitly shown, but the MAC address is 'A0:36:9F:6E:1F:D0'. The SSID is 'Ethernet'. The session started 10 minutes ago. The NAS identifier is 'ICX-Switch'. Other fields include NAS IP, NAS Port, NAS Port Type, Session ID, Last Accounting Update (628601 millis), Input Traffic (0 Bytes), Output Traffic (0 Bytes), and Accumulated Session Time (0 seconds). There is a link for 'Additional Information' pointing to an 'Enrollment Record'.

**View Connection**
Done

**Status:** ● Connected

**Username:** jchandra@brocade.com@guest.www.brocade.com

**IP Address:**

**MAC Address:** A0:36:9F:6E:2D:9F

**SSID:** Ethernet

**Session Start Time:** 22 minutes ago

**NAS Identifier:** ICX-Switch

**NAS IP:**

**NAS Port:**

**NAS Port Type:**

**Session ID:**

**Last Accounting Update:** 1304155 millis

**Input Traffic:** 0 Bytes (0 packets)

**Output Traffic:** 0 Bytes (0 packets)

**Accumulated Session Time:** 0 seconds

**Additional Information:** Enrollment Record

**View Connection**
Done

**Status:** ● Connected

**Username:** jchandra@brocade.com

**IP Address:**

**MAC Address:** 00:24:C4:42:BB:24

**SSID:** Ethernet

**Session Start Time:** 11 minutes ago

**NAS Identifier:** ICX-Switch

**NAS IP:**

**NAS Port:**

**NAS Port Type:**

**Session ID:**

**Last Accounting Update:** 651229 millis

**Input Traffic:** 0 Bytes (0 packets)

**Output Traffic:** 0 Bytes (0 packets)

**Accumulated Session Time:** 0 seconds

**Additional Information:** Enrollment Record

# 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).