

DEPLOYMENT GUIDE

## Ruckus ICX Flexible Authentication with Cloudpath ES 5.0 Deployment Guide

Supporting FastIron 08.0.60

53-1005026-02 15 June 2017

#### <sup>©</sup> 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 <a href="https://www.brocade.com/en/legal/brocade-Legal-intellectual-property/brocade-legal-trademarks.html">www.brocade.com/en/legal/brocade-legal-trademarks.html</a>. 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

Preface	5
Introduction	5
Purpose of This Document	5
Audience	6
Related Documents	6
Document History	6
Overview	7
802.1X Authentication	7
Message Exchange During Authentication	7
MAC Authentication	9
Flexible Authentication	9
How Flexible Authentication Works	9
Platform Support for Flexible Authentication	
Configuring Cloudpath for RADIUS, HTTP, and Clients	
Use Case 1: Dynamic VLAN and ACL Assignment with MAC Authentication	
Cloudpath Configuration	
Switch Configuration	
Switch Show Commands and Syslog Information	
Cloudpath Information	26
Use Case 2: Dynamic VLAN and ACL Assignment with 802.1X Authentication	
Cloudpath Configuration	
Switch Configuration	
Switch Show Commands and Syslog Information	
Cloudpath Information	
Use Case 3: Guest VLAN with External Captive Portal (Web Authentication)	
Cloudpath Configuration	
Switch Configuration	
Switch Show Commands and Syslog Information	
Cloudpath Information	43
Use Case 4: Authentication of an IP Phone and a PC on the Same Port Using Flexible Authentication	47
Cloudpath Configuration	
Switch Configuration	
Switch Show Commands and Syslog Information	
Cloudpath Information	
MAC Authentication for an IP Phone	59
Use Case 5: Authentication of a Phone, PC, and Guest User Using Flexible Authentication	61
Cloudpath Configuration	63
Switch Configuration	64
Switch Show Commands and Syslog Information	
Combined Output for Both Ports e 1/1/1 (PC1) and e 1/1/2 (PC2 Behind the IP Phone)	67
Cloudpath Information	70
Summary	

# 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

Cloudpath Quick Start Guide

https://xpc.cloudpath.net/documents/ES\_QuickStartGuide.pdf

• IEEE 802.1X-2004

http://www.ieee802.org/1/pages/802.1x-2004.html

• PPP Extensible Authentication Protocol (EAP)

https://tools.ietf.org/html/rfc2284

- Remote Authentication Dial In User Service (RADIUS) https://tools.ietf.org/html/rfc2865
- RADIUS Extensions
   https://tools.ietf.org/html/rfc2869

### **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	
	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 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 authenticationfailure 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.

Co T Rhtp://cloudpathsqa.englab.brocade.com/admin/Togin	ア・C 区 Cloudpath ES ×
Cloudpath ES	
Cloudpath	
	SIGN IN
	Email Address:
	jchandra@brocade.com
	Password:
	Login
	Reset Password

After login, the welcome page is displayed.

C () Ktp://cloudpa	thsqs.englab.brocade.com/admin/dashboard/welcome	P - C  III Cloudpath ES ×	
Cloudpath	Cloudpath ES   Brocade Welcome Connections Enrollments Users & Devices Certificates No	Duffications	
<ul> <li>Dashboard</li> <li>Welcome</li> <li>Provides a general overview of the</li> </ul>	Welcome to the Cloudpath ES	environment. The Automated Device Enablement (ADE) approach gives	
system. Connections Review current connections.	network administrators control by blending traditional employee-centric capabili CA) with guest-centric capabilities (sponsorship, email, SMS, Facebook, and mo	ities (Active Directory, LDAP, RADIUS, and Integration with Microsoft re).	
Review enrolments, including the associated user, device, and certificate information. Users & Devices	Use the left menu tabs to begin setting up your workflow configuration.  • The Dashboard tab displays reporting information about the	Septer Concession Welcome To Sample Corporation	
Review users and devices, including MAC registrations. Certificates Review issued certificates.	<ul> <li>enrollments, users, devices, certificates, and more.</li> <li>The Configuration tab allows you to configure and deploy the enrollment workflow, including the look &amp; feel and the device configuration.</li> </ul>	Steph Sepuration Value         Unit and the second sec	
Notifications Review emails, SMSes, scheduled reports, and event logs. Event Response	From the Sponsorship tab, you can manage vouchers and voucher lists, and customize the look & feel of the sponsorship portal.     From the Certificate Authority tab. you can manually generate	Englityees August and Stagenets Signature Street St	
Provides the ability to manage access in batch to respond to network events.	certificates, view certificate details, revoke certificates, manage the characteristics of certificates to be issued, and manage certificate authorities (CAs).	Particul Extended Particul Extended Particul Extended Provide an interview Particul Extended Provide Particul P	
Sponsorship     Certificate Authority	<ul> <li>The Administration tab allows you to manage administrator accounts, system services, diagnostics and logs, and system updates.</li> <li>The Support tab provides access to the Quick Start Guide and several</li> </ul>	Hard a second seco	
Administration     Support	Setup Guides to help with common configurations along with licensing inf	ormation.	

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

🗲 🛞 🔣 http://cloudpa	sthsqa.englab. <b>brocade.com</b> /admin/system/status		□ <b>□</b> □ ▲ 命令
	Cloudpath ES   Brocade		n 🔯 Logout
Cloudpath	System Services		
Dashboard	Component: Web Server		J
Sponsorship     Sonsorship     Certificate Authority     Administration     Administration     Configue asministrator accounts     and privages     System     Optimum     System Revises     System     Administration     Advanced     Conspany Information     Freesel Requirements	Web Server Status: $\widehat{P}$ Running (ii)	r, a code signing certificate may be uploaded. <u>Upload</u>	
→ Support	SSL Cipher: HIGH\\aNULL\\$STRENGTH:+DH SSL Protocel: al-58.v2 -58.v3 Strict Transport Security: Disabled		
	Component: Network		
	Component: SSH		٥
	Component: Support Tunnel		Ó
	Component: Outbound Email		1
	Component: Outbound SMS		J
	Component: L0gs		J
	Component: External Reporting Server		J
	Component: Virtual Machine		

3. 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".



4. 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.

	Cloudpath ES   Brocade
<b>Cloudpath</b>	Status Policies Clients eduroam Attributes External Open Access Accounting
Dashboard	
▼ Configuration	Modify RADIUS Client Cancel Save
Workflow	
Specify the process and the requirements for end-users	Reference Information
accessing the network.	Reference Name: SICA-3STK     *
Deploy Specify where end-users access	🗄 Enabled: 📈
the enrollment wizards.	• IP Address: 10.21.240.23 *
Advanced	Shared Secret: Foundry1 *
RADIUS Server	Advanced COA Settings
Firewall & Web Filter Integration MAC Registrations API Keys	🖲 Enable COA: 🛛
Sponsorship	COA Attributes The following attributes will be sent to the switch or controller for a COA Disconnect.
Certificate Authority	COA Disconnect Attributes: The following attributes will be included in COA Disconnect packets such to the switch or AP
Administration	The default attributes of Callino-Station-1d. NAS-Io-Address, and Act-Session-1d will be sent
▶ Support	+
	· · · · · · · · · · · · · · · · · · ·
	Advanced Port Forwarding Settings
	🖲 Enable Port Forwarding: 🗹
	Port Forwards: NAS IP Address COA Port COA Shared Secret
	10.21.240.23 3799 Foundry1 X
	+

# 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.

	Cloudpath ES   Brocade	
Cloudpath	Workflow	
▶ Dashboard	Create Workflow	Save
Configuration     Workflow     Specify the process and the     requirements for end-users	Name:     Description:	
accessing the network. Deploy Specify where end-users access the enrollment wizards.	+ Enabled:	
Advanced Device Configurations	Sample Data	
Authentication Servers Firewall & Web Filter Integration MAC Registrations API Keys	🖲 Include Demo Data:	
▹ Sponsorship		
Certificate Authority		
Administration		
▶ Support		

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

A workflow defines the sequence a user must go through to register and connect to the net display of messages to the user, the acceptance of use policies, and authentication of the us Each item below represent a step within the process. To add additional steps, click the inser of row.	work. This includes the ser and/or device. t arrow on the left side
	Let's Get Started. This is where we define the workflow the user goes through to get on the network. Typically, the first step is to add an Acceptable Use Policy, followed by an authentication to Active Directory, LDAP, or AAA. The last step is normally to configure and connect the user to the secure network. Get Started

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

Cloudp	ath ES   Brocade
Cloudpath workf	low: Primary Workflow
ashboard	
onfiguration What	at type of step should be added to the workflow? Cancel Next >
kflow	
cify the process and the ()	Display an Acceptable Use Policy (AUP).
ssing the network.	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).
fy where end-users access	
noiment wizards.	) Authenticate to a traditional authentication server.
e Configurations US Server	Prompts the user to authenticate to an Active Directory server, and LDAP server, or a RADIUS server.
ntication Servers all & Web Filter Integration (	Ask the user about concurrent certificates.
eys	Prompts the user with information about previously issued certificates that are still valid. This may suggest that old certificates be
onsorship	removed or may limit the maximum number of concurrent certificates.
rtificate Authority (	) Split users into different branches.
ministration	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
pport	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.
C	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.
C	Register device for MAC-based authentication.
sqa.englab.brocade.com Borocade.com 0.3314 	Registers the MAC address of the device for MAC authenticaton 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.
is website signifies your nt to the <u>EULA</u>	

The workflow for registering the MAC address is displayed.



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

$\sim$	Cloudpath ES   Brocade	
Cloudpath	Workflow: Primary Workflow	
ashboard		
onfiguration	Modify MAC Registration	Cancel
the process and the	Reference Information	
irements for end-users ssing the network.	+ Name:	Wired Mac Auth 1 *
oy ify where end-users access moliment wizards.	E Description:	$\widehat{}$
ce Configurations IUS Server entication Servers	Registration Information	
vall & Web Filter Integration Registrations	• SSID Regex:	4
Keys	🖭 Expiration Date Basis:	Days After
noncouchin.	+ Offset:	1
ponsorship	Behavior:	Always redirect to authenticate user.
ertificate Authority	Config Shortcuts:	Ruckus SZ HTTP Ruckus ZD HTTP Cisco HTTP Aruba HTTP Aerohive HTTP
dministration		Ruckus SZ HTTPS Ruckus ZD HTTPS Cisco HTTPS Aruba HTTPS Aerohive HTTPS
upport	🗄 Redirect URL:	[ex. https://wlan.company.com]
	+ Use POST:	
	POST Parameters:	[ex. username=bob]
	+ Allow Continuation:	
	+ Kill Session:	
	Authentication Attributes	
	Success Reply Attributes:	When the RADIUS authentication is successful, an Access-Accept will be returned to the WLAN or wired infrastructure. If additional attributes are specified here, they will also be included in the reply.
		Tunnel-Type (integer) 🗸 Add Or Reple 💙 13 🗙
		Tunnel-Medium-Type (integer) 🗸 Add Or Repl: 🗸 6 🗙
		Tunnel-Private-Group-Id (strin 🗸 Add Or Repla 🗸 U:300 🗙
thoga, englab.brocade.com		Tunnel-Private-Group-Id (strin     Add Or Replay     U:300     X       Filter-Id (string)     Add Or Replay     ip.acl1.in     X

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



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

E		e [à	Ŧ							mac_te	mplate (1)	.xlsx - Ex	cel			
	FILE HOME	INSERT	PAGE LAYOUT	FORMULAS	DATA	REVIEW	VIEW	DEVELC	PER POWERP	IVOT						
		libri	* 11 ·	Ă Ă	=	=	***	Ē	Wrap Text		General				•	
	Paste	B I	<u>U</u> • 🖽 •	<u> </u>	• =	= =	€E	₹E	🚽 Merge & Center	*	\$ -	%	,	£.0 .00	.00. →.0	Conditional Formatting *
	Clipboard 🗔		Font		ra		Alignn	ient		rs.		Ν	lumber		5	
C	8 • :	X 🗸	fx													
1	A		В		с		D		E			F	4			G
1	MAC Address	Expirat	tion Date	Username		Email			Device Name		Locat	ion				
2	00:00:00:00:00:00		4/4/2015	bob		bob@	test.cloud	path.local	Test Device		Test	ocatio	n			
3	a0369f6e2d9f		4/4/2017	Jagadeesh		jchan	dra@broca	de.com	Test Device		SJ-HC	2				
4																
5																

7. Import the updated template.

Upload MAC Registrations	×
Select the file of MAC addresses to import.	
C:\Users\jchandra\Downloads\mac_template (1).xlsx	Browse
Cancel	Continue

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

Cloudpath ES   Brocade	Ω	0 Logout							
MAC Registration Lists									
2 MAC addresses were registered via the uploaded file.									
The entries below represent MAC registration databases. Each database has its own policies. When a device is registered, it is assigned to one of the databases.									

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

🔿 🚺 http://cloudp	athsqa.englab. <b>brocade.com</b> /admin/le	ocations/	×	・ の -  c  III Cloudpath ES	×				
<u> </u>	Cloudpath ES   Brocade						Ω 🔟 Logo		
Cloudpath	Deployment Locations								
shboard nfiguration	A deployment location repres variety of reasons. For examp configuration may be deploye	ents a URL to ble, a producti d to /test.	where a workflow is deployed. Multiple locations may be used i on configuration may be deployed to /production, and a test	Add Location					
flow ify the process and the	- Location 1: Product	ion					1 X I		
ements for end-users sing the network.	+ Enrollment Portal:	http://cloudpa	thsga.englab.brocade.com/						
y y where end-users access rollment wizards.	WLAN Redirect URL:     Reception OSU URL:	http://cloudpa	[pathsqa.englab.brocade.com/enroll/Brocade/Production/ Change ] thsqa.englab.brocade.com/enroll/Brocade/Production/redirect thera_anglab.brocade.com/enroll/Brocade/Production/redirect						
nced	Sponsorship Portal http://duddatheaa.anglib.krscatea.com/B0/sortal/angree/Breaded								
e Congulations US Server antication Servers rall & Web Filter Integration	Go To:	User Experie	nce Sponsor Portal Get QR Code Explain Chrome Setup						
ieys	Snapshots:		Name	Notes	Configuration	Version	Timestamp		
	Create New	Q, X @	Snapshot 64		Primary Workflow	5.0.607	20170301 1003 PST		
onsorship		Q X O	Snapshot 63		Primary Workflow	5.0.607	20170301 0929 PST		
rtificate Authority		Q, X ∅	Snapshot 62		Primary Workflow	5.0.607	20170227 0704 PST		
ministration		QXO	Snapshot 61		Primary Workflow	5.0.607	20170227 0659 PST		

9. Create a new snapshot.

Create New Snapshot? X
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**

lan 2 name AUTH-DEFAULT by port
lan 300 name MAC-AUTH by port
tagged ethe 1/1/10
Ithentication
auth-default-vlan 2
nac-authentication enable
nac-authentication enable ethe 1/1/1
aa authentication dotlx default radius
adius-server host 10.21.240.60 auth-port 1812 acct-port 1813 default key Foundryl dotlx mac-auth web-auth
o 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 \_\_\_\_\_ IP(v4/v6) VLAN Auth ACL Session Age Port MAC Addr Addr State Time \_\_\_\_\_ 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.

Control Le 1     India     Control Le 1     Control	E () M http://cloudpa	athsqa.englab.	brocade.com/adm	nin/dashboard/registrations/	💋 タマ さ 🔣 Cloudpath ES	×		8	200 X 合分链
Circle Control       Units       Oran Control       Control         0 addition of the control       0 <td< th=""><th></th><th>Cloudpa</th><th>th ES   Brocad</th><th></th><th></th><th></th><th></th><th>C</th><th>🚺 🔟 Logout</th></td<>		Cloudpa	th ES   Brocad					C	🚺 🔟 Logout
• caload         Weiles         Weiles         Consection         Revere was met sometards, folding to sometards was met sometards.         Revere was met sometards, folding to sometards was met sometards.         Nerver was met sometards, folding to sometards was met sometards.         Nerver was met sometards, folding to sometards was met sometards.         Nerver was met sometards, folding to sometards was met sometards.         Nerver was met sometards, folding to sometards was met sometards.         Nerver was met sometards.         Nerv	Cloudpath	Users	Device Types	Form Factors MAC Registrations					
Notices area of inversion is specificated with the field of the	* Dashboard	Filt	ers: 🗹 Show activ	e. 🗌 Show revoked. 🗌 Show expired.					
modes agrand owner of system.         M/C Address         Derman         Degration Date         Degration Date         Depration Date <thdep< th=""><th>Welcome</th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th></thdep<>	Welcome								
spin.         Q         A Alve         Alse \$46 alse \$10 alse \$46 alse \$10 als	Provides a general overview of the		Status	MAC Address	Usemame	Registration Date	Expiration Date	Registration List	
Came constructions         Q         Asia         00/24 (A-1280-14)         00/24 (A-4280-14)         00/24 (A-4280-14) <td>system.</td> <td>Q,</td> <td>Active</td> <td>A0:36:9F:6E:2D:9F</td> <td>jchandra@brocade.com</td> <td>20170301 1232 PST</td> <td>20170404 0000 PDT</td> <td>Wired Mac Auth 1</td> <td></td>	system.	Q,	Active	A0:36:9F:6E:2D:9F	jchandra@brocade.com	20170301 1232 PST	20170404 0000 PDT	Wired Mac Auth 1	
Name         All bit of the ELD of the All bits of the ELD of the All	Connections	Q,	Active	00:24:C4:42:B8:24	0024c442bb24	20170213 2036 PST	20200405 0700 PDT	Wired Mac Auth 1	
Eurodems/b         Q         Asive         00/12/41/28024         00/22/4428024         2020/449708 000 000         Wind Weak Ash 1           Berkew exclusions         Q         Asive         00/12/41/28024         00/22/4428024         2020/12/02/08107         2020/04/07/08007         Wind Weak Ash 1           Berkew exclusions         Q         Asive         00/12/41/28024         00/22/4428024         2020/12/02/08107         2020/04/97/08007         Wind Weak Ash 1           Berkew exclusions         Q         Asive         A0/16/46/28024         2020/46/97/0807         Wind Weak Ash 1           Berkew exclusions         Q         Asive         A0/16/46/28024         2020/46/97/0807         Wind Weak Ash 1           Berkew exclusions         A         Asive         A0/16/46/28024         2020/46/97/0807         Wind Weak Ash 1           Control         Q         Asive         A0/16/46/28024         2020/46/97/0807         Wind Weak Ash 1           Control         Q         Asive         A0/16/46/28024         2020/46/97/0807         Wind Weak Ash 1           Rever wash ownesh         MSR schwald         Q         Asive         A0/16/46/28024         2020/46/97/0907         Wind Weak Ash 1           Rever wash ownesh         A         Asive Hef E20 9F         2020/46/97/090707 </th <th>Review current connections.</th> <th>Q,</th> <th>Active</th> <th>A0:36:9F:6E:2D:9F</th> <th>a0369f6e2d9f</th> <th>20170213 2022 PST</th> <th>20200405 0700 PDT</th> <th>Wired Mac Auth 1</th> <th></th>	Review current connections.	Q,	Active	A0:36:9F:6E:2D:9F	a0369f6e2d9f	20170213 2022 PST	20200405 0700 PDT	Wired Mac Auth 1	
Internet Notion 1         Q         Activa         00/10/4/4/38.04/4         00/204/4/38.04/4         00/204/4/38.04/4         00/204/4/38.04/4         00/204/4/38.04/4         00/204/4/38.04/4         00/204/4/38.04/4         00/204/4/38.04/4         00/204/4/38.04/4         00/204/4/38.04/4         00/204/4/38.04/4         00/204/4/38.04/4         00/204/4/38.04/4         00/204/4/38.04/4         00/204/201/201/201/201/201/201/201/201/201/201	Enrollments	Q,	Active	00:24:C4:42:BB:24	0024c442bb24	20170213 2022 PST	20200405 0700 PDT	Wired Mac Auth 1	
certificate Normality Integration         Q         Active         Albide/#662.3/h3         2006/863.000 AU         2002006.000 AU         Wind wak Ah 1           User & Davies         Q         Active         Albide/#662.3/h3         2006/863.000 AU         2002006.000 AU         Wind wak Ah 1           User & Davies         Q         Active         Albide/#662.3/h3         2006/863.000 AU         2002006.000 AU         Wind wak Ah 1           Certificate         Q         Active         Albide/#662.1/h3         2006/863.000 AU         Wind wak Ah 1           Q         Active         Albide/#662.1/h3         2008/863.000 AU         2008/863.000 AU         Wind wak Ah 1           Q         Active         Albide/#662.1/h3         2008/863.000 AU         2008/863.000 AU         Wind wak Ah 1           Q         Active         Albide/#662.1/h3         2008/863.000 AU         2008/863.000 AU         Wind wak Ah 1           Q         Active         Albide/#662.1/h3         2008/863.000 AU         2008/863.000 AU         Wind wak Ah 1           Q         Active         Albide/#662.1/h3         2008/863.000 AU         2008/863.000 AU         Wind wak Ah 1           Q         Active         Albide/#662.1/h3         2008/863.000 AU         2008/863.000 AU         2008/863.000 AU         200	Review enrolments, including the associated user, device, and	Q,	Active	00:24:C4:42:B8:24	0024c442bb24	20170213 2018 PST	20200405 0700 PDT	Wired Mac Auth 1	
Long         Active         Altisty 64:1-100         200645200         2010 10070         Wind Wack Ach 1           Rever used official         Active         Altisty 64:20-20         200645200         2010 1071         20200405 0700 070         Wind Wack Ach 1           Certificate         Active         Altisty 64:20-20         2006454200         2011 1071         20200405 0700 070         Wind Wack Ach 1           Certificate         Active         Altisty 64:20-20         2006454200         2011 1071         20200405 0700 070         Wind Wack Ach 1           Rever inside officate         Active         Altisty 64:20-20         2006454200         2011 1071         20200405 0700 070         Wind Wack Ach 1           Rever inside officate         Active         Altisty 64:20-20         2006454200         20161210 1018         20200405 0700 070         Wind Wack Ach 1           Rever inside officate         Active         Altisty 64:20-20         2006454200         20080405 0700 070         Wind Wack Ach 1           Active         Altisty 64:20-20         200645200         2000400         20080400         20080400         Wind Wack Ach 1           Active         Altisty 64:20-20         jahardaploxade.com         2016121 0120 1051         20200405 0700 070         Wind Wack Ach 1           Active	certificate information.	۹,	Active	A0:36:9F:6E:2A:58	a0369f6a2a58	20161228 2011 PST	20200405 0700 PDT	Wired Mac Auth 1	
Norma         Active         Albite/sele         2016/sele         20	Users & Devices	۹,	Active	A0:36:9F:6E:1F:D0	a0369f6e1fd0	20161228 2011 PST	20200405 0700 PDT	Wired Mac Auth 1	
Induiting MC registrions.       Q       Active       Able \$466 ± 100       200645200 ± 116 * 100 ± 2000400 ± 2000 ± 10	Review users and devices,	Q,	Active	A0:36:9F:6E:2D:9F	a0369f6a2d9f	20161228 2011 PST	20200405 0700 PDT	Wired Mac Auth 1	
Certificates              Q             4 Arive             4 Altive             Altitit             Altive             Altititit	including MAC registrations.	٩,	Active	A0:36:9F:6E:1F:D0	a0369f6e1fd0	20161220 2311 PST	20200405 0700 PDT	Wired Mac Auth 1	
Rever sauce ordifactas:       Q       Activa       Ab15(#b1620)       ab15(#b1620)       ab16(#b1620)       ab16	Certificates	О,	Active	A0:36:9F:6E:2D:9F	a0369f6e2d9f	20161220 2311 PST	20200405 0700 PDT	Wired Mac Auth 1	
Notifications         Q         Adity         A016969620395         00004690700007         Wind Mac Auch 1           Review and SMESS Mediation         Q         Adity         A016969620395         202044050700007         Wind Mac Auch 1           Review and SMESS Mediation         Q         Adity         Adity<	Review issued certificates.	Q,	Active	A0:36:9F:6E:1F:D0	a0369f6e1fd0	20161217 0121 PST	20200405 0700 PDT	Wired Mac Auth 1	
Review mails, SURSus, schedulegt         Q         A dave         A0:3659/6651100         jobardra@booxade.com         20161127 0120 PST         20200409 20700 PUT         Wind Mac Auch 1           Event Response         Q         A dave         A0:3659/6651100         jobardra@booxade.com         20161217 0120 PST         20200409 20700 PUT         Wind Mac Auch 1           Poinds Response         Q         Adve         A0:3659/6651100         jobardra@booxade.com         20161217 0113 PST         20200409 20700 PUT         Wind Mac Auch 1           Poinds Response         Jobardra@booxade.com         20161217 0113 PST         20200409 20700 PUT         Wind Mac Auch 1           Image: Constrained C	Notifications	О,	Active	A0:36:9F:6E:2D:9F	a0369f6e2d9f	20161217 0121 PST	20200405 0700 PDT	Wired Mac Auth 1	
Image: Control Contro Control Control Contrel Control Control Control Control Control C	Review emails, SMSes, scheduled reports, and event logs	٩,	Active	A0:36:9F:6E:1F:D0	jchandra@brocade.com	20161217 0120 PST	20200405 0700 PDT	Wired Mac Auth 1	
C Adve       Adve       Addrefielder/E/DO       phade/addred/bockde.com       20151127 0115 PST       2020405 5700 PDT       Wred Mac Auch 1         Press/sector	Event Personne	٩,	Active	A0:36:9F:6E:2D:9F	jchandra@brocade.com	20161217 0120 PST	20200405 0700 PDT	Wired Mac Auth 1	
access table is reported in reduce werds.       i > Configuration       i > Sponsorship       i Cartificate Authority       i Administration	Provides the ability to manage	Q,	Active	A0:36:9F:6E:1F:D0	jchandra@brocade.com	20161217 0115 PST	20200405 0700 PDT	Wired Mac Auth 1	
Configuration C	access in batch to respond to network events.				🎼 🍈 Results 1 - 15 of 16. 🏟 🏟 🚺 15 💌 🗒	S			
Sponsorship     Cortificate Authority     Administration	Configuration								
Cartificate Authority     Administration	> Sponsorship								
) Administration	Certificate Authority								
	Administration								
r support	→ Support								

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

rtp://cloudpath	hsqa.englab. <b>brocade.com</b> /admin	/dashboard/reg	istrations/28/view		👧 ۵-۹ 🚬	Cloudpath ES	×			100
	Cloudpath ES   Brocade									<u> 0</u> Log
pàth	Users Device Types	Form Factors	MAC Registrations							
verview of the	View MAC Registration									Done
- U	▼ MAC Registration In	formation								
ctions.		F Status:	Valid through 20170404 0000 F	DT Revoke						
- L	(F)	MAC Address:	A0:36:9F:6E:2D:9F							
cluding the		• Username:	inhandra@brocade.com							
		Location:	51-80							
		E SSID(s):								
ces, tions	· Regi	stration Date:	20170301 1232							
	i fe	viration Date:	20170404 0000							
tes.	Last See		20170301 1227							
- L		r minestamp.	201/0301 125/							
s, scheduled										
		1								
manage		Username:	jchandra@brocade.com							
cond to		Email:	jchandra@brocade.com							
_	• BI	ocked Status:	No. Block							
	Disting	ished Name:	type=admin, cn=jchandra@bro	cade.com						
	Authentic	ation Server:	Brocade DB							
ority										
<u> </u>	<ul> <li>Device Information</li> </ul>									
		Device Name:	Test Device							
_										
	<ul> <li>All Registrations By</li> </ul>	MAC Address								
		Status		Registration List	MAC Address	Usemame	Creation Date	Expiration Date	Last Seen	Permitted SSID(s)
	Revoke Q	valid through 2017	70404 0000 PDT	Wired Mac Auth 1	A0:36:9F:6E:2D:9F	jchandra@brocade.com	20170301 1232 PST	20170404 0000 PDT	20170301 1237 PST	
	Revoke Q	valid through 2020	10405 0700 PD1	Wired Mac Auth 1	AU:36:9F:6E:2D:9F	aU369t6e2d9t	201/0213 2022 PST	20200405 0700 PDT	20170227 0634 PST	
	Revoke Q	valid through 2020 Evolved on 201012	10405 0700 PD1	Wired Mac Auth 1	AU:36:9F:6E:2D:9F	ausbarbezdar	20161228 2011 PST	20200405 0700 PDT	201/0213 2019 PST	
	Extend Q	Expired on 201612	21 2004 PD1	Wired Mac Auth 1	AU13619F16E12D19F	jonandra@orocade.com	20161220 2334 PST	20161221 2334 PST	20161220 2337 PST	
	Extend Q	Valid through 2020	0405 0700 PDT	Wired Mac Auth 1	A013619F16E12D19F	jonandraigerocade.com	20161220 2313 P51	20101221 2313 PST	20161220 2333 PST	
	Revoke Q	Valid through 2020	10405 0700 PDT	Wired Mac Auth 1	AU:36:9F:6E:2D:9F	a0307/06207/	20161220 2311 P51	20200405 0700 PDT	20161228 2000 PST	
	Revoke 4			WIND MAC HOULD	M013019F10E12D19F	#000310#2031	20101217 0121 951	20200403 0700 PDT	20101220 2300 951	
	Courses Q	Valid through 2020	10405 0700 PDT	Mined Mac Auth 1	40-36-9E-6E-2D-9E	ichandra@hmcade.com	20161217 0120 PET	20200405 0700 000	20161217 0120 PET	

# 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.

a second to second the		
< 🔿 🔣 http://cloudg	athrqs.englab.brocade.com/admin/workflow1/ 🙋 🔎 🖒 🕅 Cloudpath ES 🛛 🗴	合 ☆ 第
	Cloudpath ES Brocade	🚺 🧕 Logout
Cloudpath	Workflow         Primary Workflow         View:         Workflow         Look & Fed         Properties	×
<ul> <li>Dashboard</li> <li>Configuration</li> </ul>	A workflow defines the sequence a user must go through to register and connect to the network. This includes the display of messages to the user, the acceptance of use policies, and authentication of the user and/or device.	
Workflow Specify the process and the	Each item below represent a step within the process. To add additional steps, click the insert arrow on the left side of row.	
accessing the network.	Step 1: Require the user to accept the AUP Acceptable Use Policy	JX Q
Deploy Specify where end-users access the enrollment wizards.	All matches in:     X // 802.1X     Mac-Auth     Webauth     +	$\mathcal{I}\equivX\triangleleft$
Advanced		
RADIUS Server RADIUS Server Authentication Servers Firewall & Web Filter Integration MAC Registrations	L Step 2: All matches in: X / Employee Guest +	.∥ ≣ × Q
API Keys	Beep 4: Prompt the user for credentials from Brocade DB	II X Q
<ul> <li>P Sponsorsnip</li> <li>Certificate Authority</li> </ul>	Bassult Move user to Wired 3 Device Confl and assign certificate using username@defaultcert	
Administration		
Support		



	Cloudpath ES Brocade						Ω 🚺 Logout
Cloùdpath	Device Configuration Wired	3 Device C	onfic * Summary Network(s) Trust OS	Settings Passpoint			×
Dashboard     Configuration	Device Configuration: Net	vork(s)					
Workflow Specify the process and the requirements for end-users accessing the network.	WLAN & Wired Network In	formation					
Deploy Specify where end-users access the enrollment wizards.	Network(s) To Install: Add	./ ×	Network Wired Connection	Protocol 802.1X	Roaming	Behavior Configure and move to network. (Onsite)	
Advanced Device Configurations RADIUS Server Authentication Servers Filerwall & Web Filter Integration MAC Registrations API Keys	Conflicting SSID(s):     Post-Transition URL:	<none> <none></none></none>	9	Lerindad-Gase			
Sponsorship     Certificate Authority							
Support							



	Cloudpath ES   B	Brocade	<b>Q</b> 🚺 Logout
Cloudpath	Device Configurati	tion Wired 3 Device Config * Summary Network(s) Trust OS Settings Passpoint	×
→ Dashboard			
▼ Configuration	Device Configur	uration: OS-Specific Settings	
Workflow			
Specify the process and the requirements for end-users accessing the network.	Add Setting	B         Setting         XP         Vola         7         8         8.           J         J         User reprint options         Image: Setting split option         Image: Setting split option </th <th>10 Future</th>	10 Future
Deploy Specify where end-users access the enrollment wizards.		J Settings from the <u>Extension</u> bot will be applied to these versions:	•
Advanced	Mac OS X:		
Device Configurations RADIUS Server	Add Setting	Satting         10.7         10.8         10.9         10.1         10.1           Use respirate splene         0         10.9         10.3         10.1         10.1	10.12 Fotore
Authentication Servers Firewall & Web Filter Integration MAC Registrations API Keys		J Settings from the <u>independence</u> bit will be applied to these versions:	6
▶ Sponsorship	iOS:	2 Setting 6 / 7 / 8 0	10 Future
Certificate Authority	Add Setting	User experience options	
Administration		<i>I</i> Settings from the <u>Internation</u> to will be applied to these versions:	
▶ Support			
	Android:	f Setting 4.0.3 4.1 4.2 4.3 4.4 5.0 5.1 6.0	7.0 Future
	Add Setting	1         User reprinting splites         0	
		J Settings from the <u>Instanction</u> bit will be applied to these versions:	
	Chrome:	2 Setting	Chrome
	Add Setting	↓ User experience options	
		J Settings from the <u>listopric()</u> tab will be applied to these versions:	
	Add Setting	Setting         12.06         12.10         13.06         13.10         14.04         18.10         15.66         16.10         18         19         20         21         22         22           #         Incomparing         12.06         12.10         13.06         13.10         16.64         16.10         18         19         20         21         22         25	25 Future
	and setting	J         Settings from the <u>laction(s)</u> tob will be applied to three venions:         ID         ID <t< td=""><td>6</td></t<>	6
	Win Mobile:	Sation	5.0 6.0
		Settings from the <u>lotopoint</u> lab will be applied to these versions:	
		* Windows Hobie support is limited to specific devices. Contact support of mupported devices.	
	Other OSes		
		Satting General WeAT Backberry	Windows Phone
cloudpathsca.englab.brocade.com		J Settings from the Interest(s) tab will be applied to these versions:	
Version 5.0.3314 Use of this website signifies your agreement to the <u>EULA</u>			

2. Navigate to Certificate Authority > Manage Templates to edit the certificates.

pathsqa.englab. <b>brocade.com</b> /admin/t	emplate/	アークープ I Cloudpath ES ×			1
Cloudpath ES Brocade					<u> </u>
Certificate Templates					
The certificate templates list	ed below define the properties embedded into a certificate when it is is:	ued. Some			
properties are static and rem allowing them to differ per ce	ain the same for every certificate. Other properties are calculated or us rtificate based on the user and/or their device.	e variables, Add Template			
Template 1: Onboar	d template Server Template				J 🐵 🛍 🖓
<ul> <li>Template 2: Onboar</li> </ul>	d template username@defaultcert.www.brocade.com				.∥ @ ℡ Ç
Common Name:	\${USERNAME}@defaultcert.vvvv.brocade.com				
CA Reference Name:	Brocade Intermediate CA I				
CA Common Name:	Brocade Intermediate CA I				
Chain:	Name		Notes	Expires	
	G Brocade Intermediate CA I			20361123	
	G Brocade Koot CA 1			20361123	
N-10-10-10-10-10-10-10-10-10-10-10-10-10-					
Notifications:	No notifications currently exist. Add				
RADIUS Policies:	VLAN: 'U:300' Filter ID: 'ip.acl1.in'				
SCEP Keys:	No SCEP keys currently exist. Add				
					1 A Pr A
	J template username@guest.www.brocade.com				<i>ා</i> ම ංම දා
Common Name:	\${USERNAME}@guest.www.brocade.com				
CA Type: CA Reference Name:	Brocade Intermediate CA I				
CA Common Name:	Brocade Intermediate CA I				
Chain:	Name		Notes	Expires	
	Q Brocade Intermediate CA I			20361123	
	Q, Brocade Root CA I			20361123	
	No obligation constituential and a				
nouncations.					
RADIUS Policies:	Filter ID: 'ip.acl1.in'				
SCEP Keys:	No SCEP keys currently exist. Add				

3. Create a snapshot to save the changes.

a construction of the second second							1 m	
← 🔿 🔣 http://cloudpa	thsqa.englab.brocade.co	om/admin/locations/	<u> </u>	・ ク マ ♂ 🔣 Cloudpath ES	×			
$\sim$	Cloudpath ES	Brocade					Ω	0 Logout
Cloùdpath	Deployment Loca	ations						
<ul> <li>Dashboard</li> <li>Configuration</li> </ul>	A deployment location represents a URL to where a workflow is deployed. Multiple locations may be used for a variety of reasons. For example, a production configuration may be deployed to /production, and a test configuration may be deployed to /test.							
Workflow Specify the process and the		Production					I × 𝒞	
Accessing the network.	Errollment Portal: http://cloudpathsga.englab.brocade.com/ or http://cloudpathsga.englab.brocade.com/enroll/Brocade/Production/							
Advanced Device Configurations RADIUS Server Authentication Servers	Sponsors	Go To: User Exper	aansquaangabbacadaacan passoona o casay roodcon ano y aansquaangab.bracade.com:80/portal/sponsor/Brocade/ ience   Sponsor Portal   Get QR Code   Explain Chrome Setup					
Firewall & Web Filter Integration MAC Registrations API Keys		Snapshots:	Name	Notes	Configuration	Version	Timestamp	2 PST
▶ Sponsorship		QX0	Snapshot 64 Snapshot 63		Primary Workflow	5.0.60	20170301 092	9 PST
Certificate Authority		$\bigcirc \times \bigcirc$	Snapshot 62		Primary Workflow	5.0.60	20170227 070	4 PST
Administration		Q,× ∅	Snapshot 61		Primary Workflow	5.0.60	20170227 065	) PST
* Support		C X O	Snapshot 60		Primary Workflow	5.0.60	20170227 064	. PST

### **Switch Configuration**

```
vlan 2 name AUTH-DEFAULT by port
vlan 300 name 802.1X by port
tagged ethe 1/1/10
1
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
I
```

### 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 \_\_\_\_\_ MAC IP(v4/v6) User VLAN Auth ACL Session Age PAE Port. State Addr Addr Name Time 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 Addres	s V4	Ingress	V4 Eg	ress	V6 Ingre	ess V6	Egress
1/1/1 Refer fol ICX-Switc	a036.9f6e. lowing show h#show radi	2d9f ac command t us server	l1 o check s	tatus o	f radius	server		
Server	T	уое	Opens	Close	s Time	outs	Status	
10.21.240	.60 a:	ny	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.

1			
< 🕘 🔣 http://cloudp.	athsqa.englab.brocade.com/admin//enrollmentDat	a/Enrollment-BCC02A4A-5E86-4CE0-84DD-A68AE4AA7D11 🔁 🖉 🗸 🖉	6 🕁 🕸
	Cloudpath ES Brocade	n 👩 🔟 Lagari	t /
Cloudpath			
Ciocapani	In-Progress Completed Issued	Revoked Expired All Enrollments Paths • Range: 30 Minute •	
* Dashboard			_
Welcome	View Enrollment Record	Done	
Provides a general overview of the			
system.	Enrollment Information		
Review current connections.	🖲 Enrollment Status:	Certificate Issued [Block]	
Enrollments	🖲 Name:	jchandra@brocade.com 👤	
Review enrollments, including the	• Email Address:	jchandra@brocade.com	
certificate information.	+ Selections:	802.1X - Employee	
Users & Devices	Operating System:	Windows 7	
Review users and devices, including MAC registrations.	Browser:	Firefox	
Certificates	+ Form Factor:	Computer	
Review issued certificates.	🕀 MAC Address:	A0:36:9F:6E:2D:9F	
Notifications Review emails SMSes scheduled	• Notes:	J	
reports, and event logs.			
Event Response			
access in batch to respond to	E Connection State:	Connected	
network events.	• Session Start Time:	115 seconds app	
F Configuration	Session Last Update:	115 seconds ago	
> Sponsorship	🗄 WLAN Username:	jchandra@brocade.com@defaultcert.www.brocade.com	
) Contribute Authority	Session ID:		
Certificate Authority	• IP Address:		
Administration	• SSID:	Ethernet	
For Support	• NAS Identifier:	ICX-Switch (null)	
	NAS Port:	null	
	NAS Port Type:	Inn	
	Input Traffic:	0 Byces (0 packets)	
	Output Traffic:	0 Bytes (0 packets)	
	Enforced Certificate Template:	usemane@defaultcet.vvvv.brocade.com	
	VLAN ID:	U:300	
	• Filter ID:	ipadin (	
	+ Last OCSP:	9 minutes ago	
	E Last RADIUS Success:	116 seconds ago	
	RADIUS Log Level:	Normal [Debug]	
jchandra@brocade.com Version 5.0.3314			
Use of this website signifies your agreement to the <u>EULA</u>	↓ Identity Information		
	Tearnama.	uhgade@bhorsels.com	

# 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.

	Cloudpath ES   Brocade					
Cloudpath	Workflow         Primary Workflow         View         Workflow         Properties	×				
Dashboard     Configuration     Workflow     Specify the process and the	A workflow defines the sequence a user must go through to register and connect to the network. This includes the display of messages to the user, the acceptance of use policies, and authentication of the user and/or device. Each item below represent a step within the process. To add additional steps, click the insert arrow on the left side of row.					
requirements for end-users accessing the network.	Step 1: Require the user to accept the AUP Acceptable Use Policy	1 × Q				
Deploy Specify where end-users access the enrollment wizards.	Al step 2: All matches in: BD2.1X Harc-Auth X ≠ Wesseth +	ℓ ≡ × Q,				
Automiced Device Configurations RADIUS Server Authentication Servers Firewall & Web Filter Integration	Step 3: Prompt user for information using Login page for 'Brocade RADIUS'.	/ X Q.				
MAC Registrations API Keys	Step 41 Redirect the user based on cpsqa.	.ℓ × Q.				
> Sponsorship						
Certificate Authority						
Administration						
· support						

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

	Cloudpath ES Brocade							
Cloudpath	Workflow: Primary Workflow							
Dashboard								
▼ Configuration	Modify Data Prompt		Cancel Save					
Workflow	Reference Information							
requirements for end-users accessing the network.	Name:	Login page for 'Brocade RADIUS'	*					
Deploy Specify where end-users access the enrollment wizards.	• Description:	$\langle \rangle$						
Advanced								
RADIUS Server	Webpage Display Information							
Authentication Servers Firewall & Web Filter Integration	+ Title:	Welcome to Brocade !!						
MAC Registrations API Keys	Message HTML:	^						
Sponsorship		~						
	💿 Bottom Label:							
Certificate Authority     Administration	Continue Button Label:	Continue >						
	Input Field 1							
♥ Support	• Label:	Username						
	🖲 Regex:							
	🕂 Variable Name:	USERNAME						
	Input Field 2							
	Label:	Password						
	🖲 Regex:							
	🕑 Variable Name:	PASSWORD						

- 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.

	Cloudpath ES Brocade							
	Workflow: Primary Workflow							
▶ Dashboard								
	Modify Redirect		Cancel Save					
Workflow Specify the process and the	Reference Information							
requirements for end-users accessing the network.	Name:	cpsqa	*					
Deploy Specify where end-users access	Description:	^						
the enrollment wizards. Advanced Device Configurations RADIUS Server Authentication Servers	🖲 Redirect URL:	http://10.21.240.23/Forms/webauth_cpss						
Firewall & Web Filter Integration MAC Registrations API Keys	🖲 Use POST:							
> Sponsorship	POST Parameters:	webauth_user_id=\${USERNAME} webauth_password=\${PASSWORD} hidden_URL_str=http://www.brocade.com						
Certificate Authority     Administration	Allow Continuation:		J					
▶ Support	E Kill Session:	Z						
	<ul> <li>Filters &amp; Restrictions</li> </ul>							

#### 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/
Т
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 1/1/10enable Т 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 1 web-management https interface ve 200 ip address 10.21.80.130/27 ! ip access-list extended acl1 permit ip any any 1

#### 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

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

ICX-Switch#show webauth allowed-list

VLAN 200: Web Authentication, N	Mode: I = Internal	E = Ex	ternal		
Web Authenticated List Port MAC Address User 1	Jame	Mode	Configuration Static/Dynamic	Auth Duration HH:MM:SS	Dynamic ACL
1/1/1 a036.9f6e.2d9f jchand ICX-Switch#show webauth ip-acl	dra@brocade.com	E	D	07:59:57	Yes
VLAN Port MAC Address	V4 Ingress ACL	V4 Egre	ss 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, Prio Untagged Ports: (U1/M1) 1 Tagged Ports: (U1/M1) 10 Uplink Ports: None DualMode Ports: None Mac-Vlan Ports: None	prity level0, Span	ning tre	ee Off		

Monitoring: Disabled Refer following show command to check status of radius server. ICX-Switch#show radius server

Server	Туое	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**.

Cloudpath by Ruckus Wirel × +				ŀ₽	×
( cloudpathsqa.englab.brocade.com/enroll/Brocade/Production/pro	cess C Search	☆ 自	÷	♠	≡
Start Over	Powered by Ruckus Networks				
Welcome to Bro	Simply Better Wireless.				
Username:	jchandra@brocade.com				
Password:	Foundry1#				
Assistance ID #3C15	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.

C () M http://cloudp	athsqa.englab.brocade.com/admin/workflow/1/ 🖉 🖉 Cloudpath ES x	
	Cloudpath ES   Brocade	🚺 🔟 Logout
Cloudpath	Workflow         Primary Workflow         *         Vevra         Workflow         Look & Feel         Properties	×
<ul> <li>Dashboard</li> <li>Configuration</li> </ul>	A workflow defines the sequence a user must go through to register and connect to the network. This includes the display of messages to the user, the acceptance of use policies, and authentication of the user and/or device.	
Workflow Specify the process and the	Each item below represent a step within the process. To add additional steps, click the insert arrow on the left side of row.	
requirements for end-users accessing the network.	Step 1: Require the user to accept the AUP Acceptable Use Policy	.∥ × Q,
Deploy Specify where end-users access the enrolment wizards.	(h)     Step 2:     All matches in:     X Ø 802.1X     Mac-Auth     Webouth     +	∥ ≣ × Q,
Advanced Device Configurations RADIUS Server Authentication Servers Firewall & Web Filter Integration MAC Revisitations	▲     Step 3:     All matches in:     X // Employee     Guest     +	# ≣ × Q,
API Keys ▶ Sponsorship	A         Step 4:         Prompt the user for credentials from Brocade DB	I X Q
▶ Certificate Authority	Result: Move user to Wired 3 Device Confi and assign certificate using username@defaultcert	J
Administration     Support		
C ( ) M http://cloudpa	thisga englab. brocade.com/admin//advanced/networks/4/ssid/	
	Cloudpath ES Brocade	🔒 🧕 Logout
Cloudpath	Device Configuration Wired 3 Device Config * Summary Network(s) Trust DS Settings Passpoint	×
Dashboard     Configuration	Device Configuration: Network(s)	

orkflow pecify the process and the equirements for end-users coessing the network.	WLAN & Wired Network In	formation				
eploy	Network(s) To Install:		Network	Protocol	Roaming	Behavior
pecify where end-users access the enrollment wizards.	Add	J ×	Wired Connection	802.1X Certificate-based		Configure and move to network. (Onsite)
lvanced						
evice Configurations ADIUS Server uthentication Servers rewall & Web Filter Integration	Conflicting SSID(s):     Dect-Transition URL:	<none></none>	0			
AC Registrations PI Keys	e Post mansition ont.	sholes	y			

Contraction in the second state								1 m			
← 🕞 🔣 http://cloudpa	thsqa.englab. <b>brocade.com</b> /admin//adv	/anced/networks/4/tru	ust/	🖉 ター さ 🔣 Cloudpath ES	r						
	Cloudpath ES   Brocade										
Cloudpath	Device Configuration Wired	3 Device Config 👻	Summar	y Network(s) Trust OS Settings Passpoint					×		
<ul> <li>Dashboard</li> <li>▼ Configuration</li> </ul>	Device Configuration: Trus	t Settings									
Workflow Specify the process and the requirements for end-users	Wi-Fi Trust										
accessing the network. Deploy	Trusted RADIUS Server(s):	Onboard RADIUS	Server	Change							
Specify where end-users access the enrollment wizards. Advanced Device Configurations RADIUS Server	+ Trusted Common Name:	When connecting to the issuing CA. On some op- cloudpathsqa.englab.bro	enetwork, t erating sys ocade.com	he end-user's device will compare the server cartificate presented by the RADIUS server to the info tems, including Mac OS X, this value is case-sensitive.	mation specified here, in:	cluding both the common	n name of the RADIUS server (	ertificate and the ch	ain of the		
Authentication Servers Firewall & Web Filter Integration	<ul> <li>Trusted RADIUS Chain:</li> </ul>	Re Re	oot CA:	Brocade Root CA I	27F56FDBC125	20361123					
API Keys		Server Certi	tificate:	cloudpathsqa.englab.brocade.com	5B78421418A9	20211123	Brocade Root CA I				
→ Sponsorship	Web Browser Trust										
Certificate Authority     Administration	Install Additional CAs:	Install Additional CAss No additional CAs have been specified. Upload									
→ Support											

) 🔿 🔣 http://cloudp	athsqa.englab. <b>brocade.com</b>	admin//advanced/networks/4/setting/	Cloudpath ES ×	to a wind
	Cloudpath ES B	cade		<u> 0</u> Logo
Cloudpath	Device Configurati	n Wired 3 Device Config * Summary Network(s) Trust OS Settings Passpoint		
> Dashboard				
Configuration	Device Configur	ion: OS-Specific Settings		
Vorkflow	Windows			
requirements for end-users	Add Setting	Setting User experience options		XP Vista 7 8 8.1 10 Future
eploy Specify where end-users access		Settings from the <u>Network(s)</u> tab will be applied to these versions:		(b)
he enrollment wizards.				
dvanced Device Configurations	Mac OS X:	Setting		10.7 10.8 10.9 10.10 10.11 10.12 Future
RADIUS Server Authentication Servers	Add Setting	J User experience options		
Firewall & Web Filter Integration MAC Registrations API Keys		J Settings from the <u>Network(s)</u> tab will be applied to these versions:		000000000
Sponsorship	i05:	Casting		6 7 8 9 10 Estura
) Contificate Authority	Add Setting	User experience options		
Administration		Settings from the <u>Network(s)</u> tab will be applied to these versions:		
Support				
	Android:	Setting		4.0.3 4.1 4.2 4.3 4.4 5.0 5.1 6.0 7.0 Future
	Add Setting	J User experience options		
		Settings from the <u>Network(s)</u> tab will be applied to these versions:		
	Chrome:	Setting		Chrome
	Add Setting	J User experience options		
		Settings from the <u>Network(s)</u> tab will be applied to these versions:		
	Linux			
	Add Setting	Setting User experience options	12.04 12.10 13.04 13.10 14.04 14.10 15.04 15.10 16.0	24 16.10 18 19 20 21 22 23 24 25 Future
		Settings from the <u>Network(s)</u> tab will be applied to these versions:		(b)
	Win Mobile:	Setting		5.0 6.0
		J Settings from the <u>Network(s)</u> tab will be applied to these versions:		
udpathsqa.englab.brocade.com		* Windows Mobile support is limited to specific devices. Contact support for supported devices.		
sion 5.0.3314 e of this website signifies your				
contract to the <u>SMA</u>	Other OSes:	Setting		Generic WinRT Blackberry Windows Phone

🔶 🕣 🔣 http://cloudpa	athsqa.englab. <b>brocade.co</b>	m/admin/template/		🖉 タッ 👌 🚺 Cloudpath ES	×			
	Cloudpath ES	Brocade						Ω 🖸 Logo
Cloudpath	Certificate Temp	ates						
Dashboard     Configuration	The certificate ter properties are sta allowing them to	nplates listed below o tic and remain the sa differ per certificate b	define the properties embedded into a certificate when it ame for every certificate. Other properties are calculated based on the user and/or their device.	is issued. Some or use variables, Add Template				
<ul> <li>Sponsorship</li> <li>Certificate Authority</li> </ul>	Template 1:	Onboard templa	te Server Template					J @ Pa 🖓
Generate Certificate Allows a certificate to be generated manually. Issued Certificates	ad v Template 2: Onboard template username@defaultcert.www.brocade.com       ad     Common Name: \$(USERNAME)@defaultcert.www.brocade.com       CAType: Onboard       CAType: Onboard       CAType: Onboard       CAType: Onboard							/ (b) Più (c)
allows certificates to be revoked. Manage Templates	CA Comm	non Name: Brocade I Chain:	Intermediate CA I		Not	tes	Expires	_
Configures the certificate templates, which specify the characteristics of certificates to be issued.		Q, Q,	Brocade Intermediate CA I Brocade Root CA I				20361123 20361123	
Manage CA Configures the certificate authorities, which issue certificates.	No	tifications: No notific S Policies: VLAN: 'U:	cations currently exist. Add					
Administration     Support	s	Filter ID: SCEP Keys: No SCEP	'ip.acl1.in' keys currently exist. <u>Add</u>					
	Template 3:	Onboard templa	te username@guest.www.brocade.com					1 o 🖻 🗘

	Cloudpath ES   Brocade	
Cloudpath	Certificate Templates	
ashboard		
onfiguration	Modify Certificate Template	Cancel Save
kflow		
irements for end-users	Reference Information	
ov	Certificate Template Name: use	rname@defaultcert.www.brocade.com *
ify where end-users access	Certificate Authority: Broca	de Intermediate CA I
nrollment wizards.	Notes:	^
ce Configurations		~
entication Servers vall & Web Filter Integration	🗄 Enabled? ✔	
Registrations (eys	Identity	
	The following property is normally used to provide ide	entity information within the certificate. Variables, such as \${USERNAME}, will be replaced at the time of
	incurrence with the presentate walks from the second law	
ponsorship	issuance with the appropriate value from the enrollme	ent.
ponsorship ertificate Authority	issuance with the appropriate value from the enrollme	ent. JSERNAME}@defaultcert.www.brocade.com
ponsorship ertificate Authority dministration	issuance with the appropriate value from the enrollmw  Common Name Pattern: \${U Validity Period	ent. JSERNAME}@defaultcert.www.brocade.com
ponsorship ertificate Authority dministration upport	issuance with the appropriate value from the enrollmo Common Name Pattern: <u>s(u</u> Validity Period The following properties determine the lifespan of the user system clocks.	ent. JSERNAME}@defaultcert.www.brocade.com : issued certificates. We recommend setting the start date to 1 month before issuance to avoid issues with er
ponsorship ertificate Authority dministration apport	issuance with the appropriate value from the enrollme Common Name Pattern: \${U Validity Period The following properties determine the lifespan of the user system clocks. Start Date: 1	ant. JSERNAME}@defaultcert.www.brocade.com issued certificates. We recommend setting the start date to 1 month before issuance to avoid issues with er Months v before issuance.
consorship ertificate Authority dministration upport	issuance with the appropriate value from the enrollme Common Name Pattern: \${U Validity Period The following properties determine the lifespan of the user system clocks. Start Date: 1 Expiration Date: 10	ent. JSERNAME}@defaultcert.www.brocade.com : issued certificates. We recommend setting the start date to 1 month before issuance to avoid issues with er Months v before issuance. Years v after issuance.
consorship ertificate Authority dministration upport	issuance with the appropriate value from the enrollme Common Name Pattern: \$(U) Validity Period The following properties determine the lifespan of the user system clocks. Start Date: 1 Expiration Date: 10 OCSP Monitoring: _ p	ant. JSERNAME}@defaultcert.www.brocade.com a issued certificates. We recommend setting the start date to 1 month before issuance to avoid issues with er Months v before issuance. Years after issuance. Revoke if unseen for 30 days.
ponsorship ertificate Authority dministration upport	issuance with the appropriate value from the enrollme Common Name Pattern: \${U Validity Period The following properties determine the lifespan of the user system clocks. Start Date: 1 Expiration Date: 10 OCSP Monitoring: 5 Policy - RADIUS Attributes	ent. SERNAME}@defaultcert.www.brocade.com a issued certificates. We recommend setting the start date to 1 month before issuance to avoid issues with er Months v before issuance. Years v after issuance. Revoke if unseen for 30 days.
ponsorship ertificate Authority dministration upport	issuance with the appropriate value from the enrollme Common Name Pattern: \$(U) Validity Period The following properties determine the lifespan of the user system clocks. Start Date: 1 Expiration Date: 10 OCSP Monitoring: c Policy - RADIUS Attributes Allow Authentication via RADIUS : V	ant. JSERNAME}@defaultcert.www.brocade.com issued certificates. We recommend setting the start date to 1 month before issuance to avoid issues with er Months v before issuance. Years after issuance. Revoke if unseen for 30 days.
ponsorship ertificate Authority dministration upport	issuance with the appropriate value from the enrollme Common Name Pattern: $\underline{s}(\underline{u})$ Validity Period The following properties determine the lifespan of the user system clocks. Start Date: 1 Expiration Date: 10 OCSP Monitoring:F Policy - RADIUS Attributes Allow Authentication via RADIUS : V Login By Certificate	ant.  SERNAME}@defaultcert.www.brocade.com  issued certificates. We recommend setting the start date to 1 month before issuance to avoid issues with er  Months  before issuance. Years  after issuance. Revoke if unseen for 30 days.
ponsorship ertificate Authority dministration upport	issuance with the appropriate value from the enrollme Common Name Pattern: \$(U) Validity Period The following properties determine the lifespan of the user system clocks. Start Date: 1 Expiration Date: 10 OCSP Monitoring: p Policy - RADIUS Attributes Allow Authentication via RADIUS : Login By Certificate bob@typd.sample.com	ant.  SERNAME}@defaultcert.www.brocade.com  issued certificates. We recommend setting the start date to 1 month before issuance to avoid issues with er  Months v before issuance.  Years after issuance.  Revoke if unseen for 30 days.  When a device authenticates using a certificate from this template, Cloudpath will return RADIUS attributes based on the information below.
ponsorship ertificate Authority dministration upport	issuance with the appropriate value from the enrollme Common Name Pattern: $\underline{s}(\underline{u})$ Validity Period The following properties determine the lifespan of the user system clocks. Start Date: 1 Expiration Date: 10 OCSP Monitoring: $\underline{s}$ Policy - RADIUS Attributes Allow Authentication via RADIUS : $\underline{v}$ Login By Certificate bobilityodiample.com	ant.         SERNAME}@defaultcert.www.brocade.com         sissued certificates. We recommend setting the start date to 1 month before issuance to avoid issues with er         Months       before issuance.         Years       after issuance.         Revoke if unseen for 30       days.         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.
ponsorship ertificate Authority dministration upport	issuance with the appropriate value from the enrollme Common Name Pattern: $\oint (U$ Validity Period The following properties determine the lifespan of the user system clocks. Start Date: 1 Expiration Date: 10 OCSP Monitoring: c Policy - RADIUS Attributes Allow Authentication via RADIUS : Could be appropriate to the start of the star	ant.         JSERNAME}@defaultcert.www.brocade.com         a issued certificates. We recommend setting the start date to 1 month before issuance to avoid issues with er         Months       before issuance.         Years       after issuance.         Revoke if unseen for 30       days.         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.
consorship ertificate Authority dministration upport	issuance with the appropriate value from the enrollme Common Name Pattern: $\underline{s}(\underline{u})$ Validity Period The following properties determine the lifespan of the user system clocks. Start Date: 1 Expiration Date: 10 OCSP Monitoring: p Policy - RADIUS Attributes Allow Authentication via RADIUS : Login By Certificate Logiblyod sample.com RADIUS Policies ex. VLAN: 50	ant.         JSERNAME}@defaultcert.www.brocade.com         issued certificates. We recommend setting the start date to 1 month before issuance to avoid issues with er         Months       >         Months       >         Years       >         after issuance.         Revoke if unseen for 30       days.         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.
onsorship ertificate Authority dministration upport	issuance with the appropriate value from the enrollme Common Name Pattern: $\underbrace{s(u)}$ Validity Period The following properties determine the lifespan of the user system clocks. Start Date: 1 Expiration Date: 10 OCSP Monitoring: ] p Policy - RADIUS Attributes Allow Authentication via RADIUS : Allow Certificate Login By	ant.         JSERNAME}@defaultcert.www.brocade.com         a issued certificates. We recommend setting the start date to 1 month before issuance to avoid issues with er         Months       before issuance.         Years       after issuance.         Revoke if unseen for 30       days.         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.

		falls (
	Cloudpath ES Brocade	n 🧕 🛛 Logout
Dashboard     Configuration      Workflow     Specify the process and the	Workflow         Primary Workflow         •         View         Workflow         Look B. Feel         Properties           A workflow defines the sequence a user must go through to register and connect to the network. This includes the display of messages to the user, the acceptance of use policies, and authentication of the user and/or device.         Each item below represent a step within the process. To add additional steps, click the insert arrow on the left side of row.	×
requirements for end-users accessing the network. Deploy Specify where end-users access the enrollment wizards. Advanced	A     Step 1:     Require the user to accept the AUP Acceptable Use Policy       A     Step 2:     All matches in:     802.1X         X     MacAuth     *	ℓ × Q   ℓ ≡ × Q
Device Configurations RADIUS Server Authentocation Servers Firewall & Web Filter Integration MAC Registrations API Keys	Step 2: Prompt the user for credentials from Brocade DB     Step 4: Register the MAC address for Wired Mac Auth 1.	Я X Q. Я X
Sponsorship     Certificate Authority	Result: Move user to Wired 3 Device Confi and assign certificate using username@defaultcert	<b>A</b>



#### 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
T.
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
Т
!
aaa authentication dot1x default radius
I.
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
```

1

```
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

```
TCX-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
                         _____
            IP(v4/v6) User VLAN Auth ACL Session Age PAE
Port MAC
     Addr
                  Addr
                                  Name
                                              State
                                                              Time
                                                                           State
                                  N/A 300 init None 93 Ena HELD
1/1/2 0024.c442.bb24 N/A
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
                           _____
                               VLAN Auth ACL Session Age
State Time
    MAC
                  TP(v4/v6)
Port.
     Addr
                  Addr
_____
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
_____
      MAC Address V4 Ingress V4 Egress V6 Ingress V6 Egress
Port
      _____
                   _____
_____
1/1/2 0024.c442.bb24 - - -
                                             -
      a036.9f6e.1fd0
1/1/2
                   acl1
ICX-Switch#show mac-authentication ip-acl all
       _____
                     -------
Port MAC Address V4 Ingress V4 Egress V6 Ingress V6 Egress
```

1/1/20024.c442.bb24 acl1 1/1/20024.c442.bb24 acl1 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 : "ICX-Switch" : "GigabitEthernet1/1/2" + System name + Port description + 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) : Type 2 PSE device Power Type 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 unauthenticated user from console MED device type : Network Connectivity + MED Network Policy Application Type : Voice : Known Policy, Tagged Policy Flags : 3000 VLAN ID L2 Priority : 4 DSCP Value : 46 + MED Extended Power via MDI Power Type : PSE device Power Source : Unknown Power Source Power Priority : Low (3) : 12.0 watts (PSE equivalent: 13190 mWatts) Power Value + 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 ser	ver				
Server	Туое	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.





C () I http://cloudpath	hsga.englab.brocade.con	n/admin//enrollmentData/8	nrollment-5D3BAB91-8E30-4B9C-8434-DA4D31F5C948/4	ロー・C I Cloudoath ES ×	□□□ ×
		RADIUS Log Level: N	ormal Debug		
		ormation			
		Email Address: jo	handra@brocade.com		
		🗉 Blocked Status: 🛛 N	o. Block		
		Distinguished Name: ty	pe=admin, cn=jchandra@brocade.com		
		Server Name: B	rocade DB		
		🕑 User Groups: a	dministrator		
	Device Infor	mation			-
		formation			
	Com 1	Workflow Step		Result	
	Step 2	All matches in:	c the AUP Acceptable Use Policy	Accepted on 20170302 0922 PST     Will nommer user to select from: 802.1X, Mar-Jurb, Websurb	
				Selection: 802.1X	
	Step 3	All matches in:		Will prompt user to select from: Employee, Guest	
	0.01			Selection: Employee	
	Result	User has completed the	workflow.	✓ successru as jonanora@brocade.com The user is authorized to receive a certificate from 'username@defaultcert.www.brocade.com'.	
	Certificate	User has been issued a c	ertificate.	jchandra@brocade.com@defaultcert.www.brocade.com valid until 2027/0302.	
	Connection	User has authenticated.		Last authentication: 22 minutes ago	
	Notification:	5			-
	- Issued Costi	ficate			
	•	F Status: V	Nid. Revoke		
		Common Name: jc	handra@brocade.com@defaultcert.www.brocade.com View Details		
		Certificate Template: u	sername@defaultcert.www.brocade.com		
		🕑 Certificate Type: 🛛 U	ser + Device		
		Certificate Chain: B	rocade Intermediate CA I (61682C4342C3217C8C866C2C51A80EDF0D29583	9)	
		Expiration Date: 2	2270302 0924 PST		
		Begin Date: 2	0170202 0924 PST		
		E Key Length: 2	048		
		Serial Number: 8	711ba5e8391ec9a7df675cf2620c131241866dd		
jchandra@brocade.com Version 5.0.3314		🖲 Thumbprint: 🛛 E	4B1B9C167D066B401D715B505C2CFE2779B68EF		
Use of this website signifies your agreement to the <u>BULA</u>	BADTUS T-6				
	¥ KADIOS IIII	Simation			
					- 0 X
Carl B http://cloudpath	asga englab brocade con	n/admin//enrollmentData/F	nrollment-5D3BAR91-8E30-4R9C-8434-DA4D31E5C948A	O × C III Claudenth ES V	840
		Certificate			
		• Sta	tus: Valid. Revoke		
		Common Na	me: jchandra@brocade.com@defaultcert.www.brocade.com Vie	tw Details	
		Certificate Tempi	dle: username@defaultcert.wivw.brocade.com		
		Certificate I	/pe: User + Device		
		· certificate ch	Brocade Intermediate CA I (51582C4342C3217C8C856C2C51 Brocade Root CA I (27F56FFA1D06519743A9CFC28A86B1550	1400EDF00245834) 35DBC125)	
		Expiration D	ate: 20270302 0924 PST		
		🖲 Begin D	ate: 20170202 0924 PST		
		🖭 Key Len	gth: 2048		
		🖲 Serial Num	ber: 8711ba5e8391ec9a7df675cf2620c131241866dd		
		🖲 Thumbpr	int: E48189C167D0668401D7158505C2CFE2779868EF		
	+ RADIUS	5 Information			
	Attribute		Value		
	Acct-Session Callipo-Stat	n-10 ion-Id	40-36-95-65-15-00		
	Class				
	Cpn-Certific	ate-Pk	39		
	Cpn-Certific	ate-Template-Pk	2		

 Initial
 Initial

 Initial States
 Initial States

 Initial States
 Initial State

					NIR-	
http://cloudpa	athsqa.englab.brocade.com/admin/certificate/39/v	ew D V Cloudpath ES X	_			10 X 83
	Cloudpath ES Brocade				🖸 🔟 Logoul	· ^
Cloudpath	Active Certificates Revoked Expir	d All Active Trends Expiring Trends				
▼ Dashboard						
Welcome	View Certificate				Done	
Provides a general overview of the system.						
Connections						
Enrollments	E Common Name:	jchandra@brocade.com@defaultcert.www.brocade.com				
Review enrollments, including the	• Status:	Valid. Revoke				
certificate information.	Valid Not Before:	20170202 0924 MS1				
Users & Devices	Valid Not Arter:     Organization:	20270302 0324 PS1				
including MAC registrations.	Organizational Unit:	IP SOA				
Certificates	The Locality:	San Jose				
Review issued certificates.	+ State:	CA				
Notifications Review emails, SMSes, scheduled	🖲 Country:	US				
reports, and event logs.	Serial Number:	8711ba5e8391ec9a7df675cf2620c131241866dd				
Provides the ability to manage	SHA Fingerprint:	E4B1B9C167D066B401D715B505C2CFE2779B68EF				
access in batch to respond to network events.	+ Certificate Template:	username@defaultcert.www.brocade.com				
	🗄 Certificate Authority:	Brocade Intermediate CA I				
Free Providence Pr	Certificate Type:	User + Device				
> Sponsorship	+ Enrollment:	jchandra@brocade.com				
Certificate Authority	🖲 Notes:	J				
Administration						
Support	• Public Key:	View Download PEM Download DER View Details				
	Chain:	View Download PEM Download PKCS7				
	+ Issued:	130 minutes ago				
	• SSID:	Ethernet				
	NAS Identifier:	ICK-Switch				
	Enforced Certificate Template:	2 unannan Odafa daan uuuu kaanda aan				
		Urani ne ne eksete en eksete ekset				
	Filter ID:	ipadi.in				
rin disathana anglah honrada raw	E Last OCSP:	38 minutes ago				
jchandra@brocade.com Version 5.0.3314	Last RADIUS Success:	38 minutes ago				
Use of this website signifies your agreement to the <u>EULA</u>	🖲 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	

🛞 🔣 http://cloudpathsqa	xenglab brocade.com/schmin//enrollmentData/Enrollment-E77F6CSA-4880-4308-88F3-812088A36871/1 🔀 🔎 = 🐮 🔀 Cloudpath ES 🛛 🗴	
	Cloudpath ES Brocade	<b>Q</b> Logout
Cloudpath	In-Progress Completed Issued Revoked Expired All Enrollments Paths	- Range: 30 Minute 🗸
ashboard		
ome des a general overview of the m	View Enrollment Record	Done
ections	+ Enrollment Information	
ew current connections.	Enrollment Status: Abandoned	
Iments	Name: 0024c442bb24	
w enroliments, including the iated user, device, and	Eccation: 3310	
ate information.	MAC Address: 00:24:C4:42:BB:24	
a Devices	Last Seen by MAC Auth: 20170213 2019 PST	
ding MAC registrations.	🗈 Notes: 🥒	
icates		
ations	<ul> <li>Connection Information</li> </ul>	
w emails, SMSes, scheduled	Connection State: Connected	
, and event logs.	Session Start Time: 30 minutes app	
les the ability to manage	E Session Last Update: 30 minutes apo	
s in batch to respond to rk events.	WLAN Username: schandra@brocade.com	
	Session ID:	
nfiguration	IP Address:	
onsorship	SSID: therest	
rtificate Authority	NAS Identifier: ICX-Switch (null)	
ministration	NAS Port: null	
	NAS Port Type: null	
pport	Input Traffic: 0 Bytes (0 packets)	
	Output Traffic: 0 Bytes (0 packets)	
	MAC Registration	
	Struss         Reptoration Usc         MAC Address         Usersame         Creation Date           Revolat         Qu         Valid through 20200455 6700 90T         Wind Max Auch 1         00:241-0542389-24         002464329244         20310313 2018 99T	Expiration Date Last Seen Permitted SSID(s) 20200405 0700 PDT 20170213 2019 PST
sqa.englab.brocade.com 0brocade.com 0.3314	Notifications	
website signifies your to the <u>EULA</u>	- RADIUS Information	

	NAS Port Type: and	4500 0015 012000000			74			
	Input Traffic: A Day (2 and and							
	input frame. • systs (• packets)							
	Output Tramc: 0 Bytes (0 packets)							
<ul> <li>MAC Registrati</li> </ul>	ion							
	Status	Registration List	MAC Address	Username	Creation Date	Expiration Date	Last Seen	Permitted SSID(s)
Revoke Q	Valid through 20200405 0700 PDT	Wired Nac Auth 1	00:24:04:42:88:24	0024c442bb24	20170213 2018 PST	20200405 0700 PDT	20170213 2019 PST	
<ul> <li>Notifications</li> </ul>								
, nouncations								
<ul> <li>RADIUS Information</li> </ul>	nation							
Attribute	Value							
CallensStationald								
Class.	00124104142100124							
Con-Cartificate-Rk								
Con-Certificate-Templ	late-Pk							
Cpn-Enrolment-Pk	1774							
Cpn-Radius-Client-Pk								
Cpn-Registration-Pk	32							
Con-Ssid	Ethernet							
Filter-Id								
NAS-Identifier	ICX-Switch							
Session-Timeout	2011770							
Tunnel-Medium-Type	IEEE-802							
Tunnel-Private-Group	-td T13000							
Tunnel-Type	VLAN							
User-Name	jchandra@brocade.com							
accountPk	1							
action	authentication							
action	authentication							
Enrollment Var	riables							
System Data								

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

•	Cloudpath Configuration	63
•	Switch Configuration	
•	Switch Show Commands and Syslog Information	
•	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.

Cloudpath ES   Brocade	🚹 🚺 Logout
Workflow         *         View:         Workflow         Properties	×
A workflow defines the sequence a user must go through to register and connect to the network. This includes the display of messages to the user, the acceptance of use policies, and authentication of the user and/or device.	
Each item below represent a step within the process. To add additional steps, click the insert arrow on the left side of row.	
Step 1: Require the user to accept the AUP Acceptable Use Policy	/ × Q
All matches in:     X Ø 802.1X     Mac-Auth     Webauth     +	_∥≣×♀
All matches in:     X / Employee     Guest     +	∥ ≣ X Q
Stap 4: Prompt the user for credentials from Brocade DB	_/ X 4
Result: Move user to Wired 3 Device Confi and assign certificate using username@defaultcert	Ø

Cloudpath ES   Brocade	Ω	0 Logout
Workflow         Primary Workflow         *         View:         Workflow         Look & Feel         Properties		×
A workflow defines the sequence a user must go through to register and connect to the network. This includes the display of messages to the user, the acceptance of use policies, and authentication of the user and/or device. Each item below represent a step within the process. To add additional steps, dick the insert arrow on the left side of row.		
Step 1: Require the user to accept the AUP Acceptable Use Policy	_/ X Q	
All matches in:     X // 802.1X     Mac-Auth     Websath     +	/ ≣ × Q	
▲     Step 3:     All matches in:     Employee     ★	/ ≣ × Q	
Step 4: Send a verification code from Guest Voucher List	_/ × Q	
Result: Move user to Wired 3 Device Confi and assign certificate using username@guest.www.b	Ø	

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

					and the second se	
< l> <li>Http://cloudpa</li>	athsqa.englab. <b>brocade.com</b> /admin/	/template/	🖉 P+ 🖒 🚺 Cloudpath ES	×		6 7 8
	Cloudpath ES   Brocade				<u>c</u>	Logout
Cloudpath	Certificate Templates					
Dashboard     Configuration	The certificate templates list properties are static and ren allowing them to differ per c	ited below define the properties embedded into a certificate whe main the same for every certificate. Other properties are calculi certificate based on the user and/or their device.	en it is issued. Some ated or use variables, Add Template			
▶ Sponsorship	Template 1: Onboa	ard template Server Template			./ ()	la ⊖
* Certificate Authority	🗙 Template 2: Onboa	ard template username@defaultcert.www.brocade.cor	n		J (b)	a ç
Allows a certificate to be generated manually. Issued Certificates Displays issued certificates and allows certificates to be revoked.	Common Name: CA Type: CA Reference Name: CA Common Name:	a \$(USERNAME)@defaultcert.vvvv.brocade.com 11 Onboard 12 Brocade Intermediate CA I 21 Brocade Intermediate CA I				
Manage Templates	Chain:	Name		Notes	Expires	
Configures the certificate templates, which specify the characteristics of certificates to be		Q Brocade Intermediate CA I			20361123	
issued. Manage CA					LUUUILU	
Configures the certificate authorities, which issue certificates.	Notifications: RADIUS Policies: SCEP Keys:	s No notifications currently exist. <u>Add</u> H VLAN: 'U.300' Filter ID: 'ip.add.in' si No SCEP keys currently exist. <u>Add</u>				
Support		ard template username@guest.www.brocade.com			.1 (6)	à ŵ
	Common Name: CA Type: CA Reference Name: CA Common Name:	s {USERNAME}@guest.vvvv.brocade.com s Onboard s Brocade Intermediate CA I s Brocade Intermediate CA I				
	Chain:	11 Name		Notes	Expires	
		Q,         Brocade Intermediate CA I           Q,         Brocade Root CA I			20361123 20361123	
	Notifications:	a No notifications currently exist. Add				
	KADIUS POICIES:	Filter ID: 'ip.acl1.in'				
	SCEP Keys:	No SCEP keys currently exist. Add				
cloudpathaga englab Drocade.com Johandra@Drocade.com Version 5.0.3314 Use of this website signifies your agreement to the <u>BULA</u>						
Cloudpath ES Bro	ocade					🔒 🧻 Logout
Workflow Primary V	Workflow T					×

Workflow Primary Workflow * View Workflow Look & Feel Properties	×
A workflow defines the sequence a user must go through to register and connect to the network. This includes the display of messages to the user, the acceptance of use policies, and authentication of the user and/or device.	
Each item below represent a step within the process. To add additional steps, click the insert arrow on the left side of row.	
Step 1: Require the user to accept the AUP Acceptable Use Policy	I × Q,
Step 2: All matches in: 802.1X X / Mac-Auth Webauth +	_ℓ ≣ x Q
Step 3: Prompt the user for credentials from Brocade DB	.∥ X Q
Step 4: Register the MAC address for Wired Mac Auth 1.	J ×
Result: Move user to Wired 3 Device Confi and assign certificate using username@defaultcert	J.

### **Switch Configuration**

!

- 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 3 name 802.1X-GUEST by port
tagged ethe 1/1/10
 router-interface ve 3
webauth
 captive-portal profile cp-sqa1
 auth-mode captive-portal
 no secure-login
  trust-port ethernet 1/1/10
  enable
!
1
vlan 200 name GUEST by port
tagged ethe 1/1/10
 router-interface ve 200
I.
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
Т
!
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
Т
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
I.
interface ve 3
ip address 10.21.80.189/27
I.
interface ve 200
ip address 10.21.80.157/27
I.
interface ve 300
ip address 10.21.80.249/27
L.
interface ve 3000
ip address 10.21.80.125/27
I.
ip access-list extended acl1
permit ip any any
I
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
------
                              _____
     MAC
                                         User
                                                     VLAN Auth
Port
                     IP(v4/v6)
                                                                    ACL Session Age PAE
      Addr
                      Addr
                                         Name
                                                                           Time
                                                            State
                                                                                          State
  _____
                            ------
                                                           _____
                                                                                       _____
1/1/1 a036.9f6e.2d9f N/A
                                        N/A 3 init None 46 SO
                                                                                           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 AUTHENT ICX-Swi sdi show do	a036.9f6e.2d9f FICATED Ltch# Dt1x ip-acl all	10.21.80.161	jchandra@bro	c 200	permit	Yes	11	Ena	
Port	MAC Address	V4 Ingress	V4 Egress V6 Ir	gress	V6 Egress	3			
1/1/1	a036.9f6e.2d9f	acll			-				
ICX-Swi Total E Maximun	itch#show vlan 200 PORT-VLAN entries: n PORT-VLAN entries	8 s: 64							
Legend:	: [Stk=Stack-Id, S=	=Slot]							
PORT-VI Untago Tago Upli DualMo	LAN 200, Name GUEST ged Ports: None ged Ports: (U1/M1) lnk Ports: None ode Ports: None	7, Priority leve	elO, Spanning tree (	ff					

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

ICX-Switch#

Mac-Vlan Ports: (U1/M1)

Monitoring: Disabled

1

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: 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 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-Swi	tch#show dot1x ses	sions all										
Port	MAC Addr	IP(v4/v6) Addr		User Name		VLAN	Autl Stat	h te	ACL	Session Time	Age	PAE State
1/1/1 AUTHENT	a036.9f6e.2d9f 'ICATED	10.21.80.129		jchar	ndra@broc	200	peri	 nit	Yes	692	Ena	
1/1/2 1/1/2 AUTHENT	0024.c442.bb24 a036.9f6e.1fd0 TICATED	N/A 10.21.80.228		N/A jchar	ndra@broc	300 300	ini perr	t mit	None Yes	64 71	Ena Ena	HELD
Port	MAC Addr	IP(v4/v6) Addr		VLAN	Auth State	ACL		Sessior Time	n Age			
1/1/2 1/1/2	0024.c442.bb24 0024.c442.bb24	10.21.80.97 N/A		3000 300	Yes Yes	None None	e 2	258 270	Ena Ena			
ICX-Swi	tch#show dot1x ip-	acl all							_			
Port	MAC Address	V4 Ingress	V4 Eg	ress	V6 Ing	ress	V6 I	Egress	_			
$\frac{1}{1}$	a036.9f6e.2d9f	acl1 -	-		-		-					
1/1/2	a036.9f6e.1fd0	acl1	-		-		-					
ICX-Swi	tch#show mac-authe	entication ip-a	cl all						_			
Port	MAC Address	V4 Ingress	V4 Eg	ress	V6 Ing	ress	V6 I	Egress	_			
1/1/2 1/1/2	0024.c442.bb24 0024.c442.bb24	-	-		-		-					
ICX-Swi Total P Maximum	tch#show vlan 300 PORT-VLAN entries: PORT-VLAN entries	8 3: 64										
Legend:	[Stk=Stack-Id, S=	=Slot]										
PORT-VI Untagg Tagg Upli DualMc Mac-Vl Mc	AN 300, Name 802.1 red Ports: None red Ports: (U1/M1) nk Ports: None ode Ports: None an Ports: (U1/M1) nitoring: Disabled	X, Priority lev 10 2	vel0, S	pannir	ng tree O	ff						
ICX-Swi Total P Maximum	tch#show vlan 200 CORT-VLAN entries: N PORT-VLAN entries	8 s: 64										
Legend:	[Stk=Stack-Id, S=	-Slot]										
PORT-VI Untagg Tagg Upli DualMc Mac-Vl Mc	AN 200, Name GUEST red Ports: None red Ports: (U1/M1) nk Ports: None ode Ports: None an Ports: (U1/M1) nitoring: Disabled	2, Priority leve 10 1	elO, Sp	anning	g tree Of	f						
ICX-Swi Total P Maximum	tch#show vlan 3000 ORT-VLAN entries: @ PORT-VLAN entries	8 8: 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
SYSLOG: <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
 ------
                 Tyoe Opens Closes Timeouts Status
Server
_____
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.

Cloudpath by Ruckus Wirel × +					ð	x
Cloudpathsqa.englab.brocade.com/enrol	I/Brocade/Production/process	C Search	☆自	+	⋒	≡
	<u>Start Over</u>	Powered by Ruckus Networks				^
		uckus <sup>*</sup>				
	802.1X	802.1X Modify this option and add additional options as needed.				ш
	Mac-Auth	Mac-Auth				
	Webauth	Webauth				
	< Back	Network Connections				Ŧ

#### 3. Select Guest.

Cloudpath by Ruckus Wirel × +						×
( cloudpathsqa.englab.brocade.com/enroll/P	rocade/Production/process	C Search	☆ 自	÷	⋒	≡
	<u>Start Over</u>	Powered by Ruckus Network				
	Start Over	Powered by Ruckus Network				
-	Assistance ID #A7F4 cloudp	athsqa.englab.brocade.com (5.0.607.3314)				
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.



The following verification code is required to access the network. Verification Code: gucx

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

Cloudpath by Ruckus Wirel × +					ŀ₽	×
🜔 🛈 🔏 🛛 cloudpathsqa.englab.brocade.com/en	roll/Brocade/Production/process	V C Search	☆自	+	♠	≡
	<u>Start Over</u>	Powered by Ruckus Networks				
	A verification code was sent to johand code and enter it below. Verification Code:	ra@brocade.com.Retrieve the verification				

6. Download the application and install the certificate.



Opening NetworkWizardLoader-853363e	eb.exe	×
You have chosen to open:		
NetworkWizardLoader-853363	Beb.exe	
which is: Binary File (706 KB)		
from: http://cloudpathsqa.engla	b.brocade.com	
Would you like to save this file?		
	Save File	Cancel

Security Wa	arning	×
	You are about to install a certificate from a certification authority (CA) claiming to represent: Brocade Root CA I Windows cannot validate that the certificate is actually from "Brocade Root CA I". You should confirm its origin by contacting "Brocade Root CA I". The following number will assist you in this process: Thumbprint (sha1): 27F56FFA 1D065197 43A9CFC2 8A86B1E5 D5DBC125 Warning: If you install this root certificate, Windows will automatically trust any certificate issued by this CA. Installing a certificate with an unconfirmed thumbprint is a security risk. If you click "Yes" you acknowledge this risk. Do you want to install this certificate?	
	Yes No	



- 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.

E () M http://cloudp	athsqa.englab. <b>brocade.com</b> /admin/connectionD	ata/viewConnected	×	・ Cloudpath ES ×			(
Cloudpath	Cloudpath ES Brocade Connections Disconnects All					Ω 🖸 ι	Logout
Dashboard      Welcome      Provides a general overview of the     system.	Status Q. X O Connected	IP Address	MAC Address A0:36:9F:6E:2D:9F	Username johandra@brocade.com@guest.www.brocade.com	SSID Ethernet	Duration 70 seconds ago	
Connections Review current connections. Enrollments Review enrollments, including the associated user, device, and certificate information.			∳ ∲ Results	1-1d1.⊕⊕  13 v 🗍 🖗 ¥ 💥			

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://cloudpa	athsqa.englab. <b>brocade.com</b> /admin//enrollmentDat	x/Enrollment-4402.CF78-2980-40F2-8389-38626A78A7F4/vi 🔀 🌶 - 🖒 🔯 Cloudpath ES 🛛 🗴	
	Cloudpath ES Brocade	🖸 🔟 Loge	out
Cloudpath	In-Progress Completed Issued	Revoked Expired All Enrollments Paths • Range: 30 Minute	
ashboard	View Enrollmont Decord		
iome ides a general overview of the em.		001#	
nections	Enrollment Information		
iew current connections.	Enrollment Status:	Cernificate Issued Block	
oliments	Name:	jchandra@Brocade.com	
new enrollments, including the	Voucher Name:	jchandre@Procede.com	
ificate information.	+ Selections:	802.11 - Guest	
rs & Devices	Operating System:	Windows 7	
view users and devices, luding MAC registrations.	Browser:	Firefox	
tificates	Form Factor:	Computer	
view issued certificates.	MAC Address:	A0:36:9F:6E:20:9F	
ifications view emails, SMSes, scheduled orts, and event logs.	🖲 Notes:	J	
nt Response			_
ess in batch to respond to	E Connection State:	Connected	
vonk events.	Session Start Time:	129 seconds ago	
Configuration	Session Last Update:	129 seconds soo	
	+ WLAN Username:	chandra@becom@guest.www.brcade.com	
Sponsorship	Session ID:		
Certificate Authority	• IP Address:		
Administration	• SSID:	Ethemet	
Support	• NAS Identifier:	ID/Switch (null)	
	NAS Port:		
	NAS Port Type:	nd	
	Input Traffic:	0 Bytes (0 packets)	
	Output Traffic:	0 Bress (Dackets)	
	Enforced Certificate Template:	username@puset.www.brocade.com	
	VLAN ID:	200	
	Filter ID:	ipadlin	
	Last OCSP:		
	+ Last RADIUS Success:	130 seconds acc	
	BADIUS Log Level:	Normal Datasa	
pathsqa.englab.brocade.com dra⊚brocade.com ≥n 5.0.3314			
	<ul> <li>Voucher Information</li> </ul>		
	+ Voucher List:	Guert Voucher Liet	

excellationalis     e
• According Laboratio  • According Labor
• Verklow tarkwarts <ul> <li> <ul> <li></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul>
Interface     End       Note:     An ended on the second data Statistics St
001 Network have to same the out of same the law magnetic law hitigs   002 All match in the law
No.2 Af antices m   No.2
Bit All matters       Before MDL XL         Containe       User to ampleted the under All Lines         Containe       User to ampleted the under All Lines         Image: State MDL XL       The user kale Andre XL         Image: State MDL XL       The under kale Andre XL         Image: State MDL XL       The under kale Andre XL         Image: State MDL XL       The under kale Andre XL         Image: State MDL XL       The under kale Andre XL         Image: State MDL XL       The Under Kale MDL XL         Image: State MDL XL       The Under Kale MDL XL         Image: State MDL XL       The Under Kale MDL XL         Image: State MDL XL       The Under Kale MDL XL         Image: State MDL XL       The Under Kale MDL XL         Image: State MDL XL       Th
Br3       All radius m       Mill provide that while fine Endpuid, date:         Br4       Br4 and the million of the
Image: section code from Code Volume Volu
Br84     Sed a wardance cale fore float Nuclei Liss     Value dad Liss Sed a Value Liss       Value dad Liss Sed a Value Liss     Value dad Liss Sed a Value Liss       Value dad Liss Sed a Value Liss     Value dad Liss Sed a Value Liss       Value dad Liss Sed a Value Liss     Value dad Liss Sed a Value Liss       Value dad Liss Sed a Value Liss     Value dad Liss Sed a Value Liss       Value dad Liss Sed a Value Liss     Value dad Liss Sed a Value Liss       Value dad Liss Sed a Value Liss     Value dad Liss Sed a Value Liss S
<ul> <li></li></ul>
Image and public backed control in the series of an influe from the series of an
Multiple for a source and variable of the first and register on a source day part on a branche great on a branche day part on a branche great on a branche day 20100000000000000000000000000000000000
let function let function   let function let function   let function let function   let function let function     let function let function
benearie       base absences.         • statistics:             • statistics:         • statistics:             • statistics:             • statistics:             • statistics:             • statistics:             • statistic:             • statistic:             • statistic:         • statistic:             • statistic:             • statistic: </td
Notifications      Notifications      Notifications      Notifications      Notifications      Notifications      Notifications      Notification
• Netlification         Image: Status       Understatus       Status
V MINICIDANS   V MINICIDANS     V MINICIDANS     V MINICIDANS     V Minicipants        V Minicipants        V Minicipants              V Minicipants
Type       Addres       Bat Norm Status       Theosamp       Oxigat       Oxig
Image       jointrange       2017002 1224 MFT       Verification       Verification         • Lasured Certificate       Image       2017002 1224 MFT       Verification       Access         • Lasured Certificate       Image       2017002 1224 MFT       Verification       Access         • Common Neme:       Verification       Image       2017002 1224 MFT       Image       Imag
I saved Certificate    • I saved Certificate     © common Name: © devide@broads.com@geat.univ.broads.com © certificate Template: usrram@geat.univ.broads.com © certificate Template: © certificate Temp
I saved Cetificate   • I saved Cetificate   • I saved Cetificate   • I saved Cetificate   • Common Name: • Units • Exclassion Date: • 200002 128 PST • Begin Date: • 200002 128 PST • Begin Date: • Exclassion Date: • 200002 128 PST • Begin Date: • Exclassion Date: • 200002 128 PST • Begin Date: • Exclassion Date: • 200002 128 PST • Begin Date: • Exclassion Date: • 200002 128 PST • Begin Date: • Exclassion Date: • 200002 128 PST • Begin Date: • Exclassion Date: • 200002 128 PST • Begin Date: • Exclassion Date: • Exclassion Date: • Exclassion Date: • Exclassion Date: • 200002 128 PST • Begin Date: • Exclassion
Image: Status       Web: Image: I
Image: Balance in Verte Reade         Image: Balance in Verte Reade<
Image: Common Name:       jeterdragbesteamunk bracks com [Weinbells]         Image: Cortificate Type:       User = bolos         Image: Cortificate Type:       User > bolos         Image: Cortificate Type:       Value Type: Type: Cortificate Type:         Image: Cortificate Type:       Value Type: Type: Cortificate Type:         Image: Cortificate Type:       Value Type: Cortificate Typ
Image: Certificat Templete       user=am@gust::nnx.broads.com         Image: Certificat Templete       User 2 books         Image: Certificat Templete       200002 1228 597         Image: Degrin Date       2010002 1228 597         Image: Degrin Date
Image: extilicate Type:       User > Device         Image: Bream Date:       Discole Stream Date:<
Certificate Chain: Broads International CA 1 (6882C43440222)76C6862C231486E9F0293539) Broads Roc CA 10 (79789741405519744407C224868E150596C125) Broads Roc CA 10 (20097877421450519744407C224868E150596C125) Broads Roc CA 10 (2009777221510-07965358C22725E
evada Roc CA (27754774106513774349CFC844681E00080C123) E Expiration Date 3019021 228 9F Begin Date 3049 Serial Numberi 44826079300305395445415056956792 E Thumberii E TCA455550997772195047969305C2272E thrqasenglab bracede.com/admin/enrollment-4402CF78-2989-40F2-8989-386268A78A7F4/v  P C C Cloudpath ES × thrqasenglab bracede.com/admin/enrollment-4402CF78-2989-40F2-8989-386268A78A7F4/v  P C C Cloudpath ES ×
Expiration Date:       2019302 1228 957         Begin Date:       2017022 123 957         Serial Number:       44abcah936304453a4datadboxe984dbab1         Thumbprint:       ESCA453858049772219DA0796930EC22728E
Begin Date: 20170201228 95T     Key Length: 2018     Key Length: 2018     Serial Number: 4da2c4936020433846414.d50x498060991     Serial Number: 4da2c4936020433846414.d50x498060991     Thumbprint: ECCA45858099772219D007969330EC22728   thtiga.englab.bfoccade.com/admin/enrollmentJatz/Enrollment-4dD2CF78-2980-40F2-83898-38626A78A7F4/vi
Certificate     Status     Value     Serial     Serial     Value     Serial     Serial     Value     Serial     Serial     Value     Serial
Key Length: 2049     Second Centificate     Second Centificate Template     Second Centemate Centificate Template     Second Centificate Template     Se
Serial Number: 44480/9595024538-4414f.05xe95604911     Thumbprint: ECCA455550907722155007585358C227228  thrqa.engleb.brocade.com/admin/enrollmentData/Enrollment-4402CF78-2980-40F2-8389-38626A78A7F4/v
thispa engleb brocade.com/sdmin/enrollmentData/Enrollment-4402CF78-2980-40F2-8389-38626A78A7F4/ve 2 C C Cloudpath ES ×  ssued Certificate Status: Val. (Backs) Common Name: Va
Common Name (bydehoeds.com@puet.invibrocks.com <u>Ver besis</u> Common Name (bydehoeds.com@puet.invibrocks.com <u>Ver besis</u> Certificat Template     Use - Decis      Certificate Chain     Decitificate     Decitificate
Common Name: Shahddbocdda.com@yuet.unvbocdda.com ( <u>Veu Desits</u> ) Cortificate Template userae@yuet.unvbocdda.com User = Decic Cortificate Chain Bocda forematics A1 (51820-5142C217A0C8642231A00E9700295839) Bocda foreca A1 (51820-5142C217A0C8642231A00E9700295839) Bocda foreca A1 (51820-5142C217A0C864281500D0E125) Bocda foreca A1 (51820-5142C417A0C864281500D0E125) Bocda foreca A1 (51820-5142C417A0C864481500D0E125) Bocda foreca A1 (51820-5142C417A0C864481500D0E126444717A0C864481500000000000000000000000000000000000
Certificate Template User = megaguet.univ.broads.com User = Device User
Cartificate Type:         Use + Device           Cartificate Chain:         Strade Stratemadizes CA 1 (61820-0342021176058670259839)           Broade Rock CA 1 (27967FALD00513743ACFC26446851500506125)           Expiration Date:         2017020 1228 PST           Broade Rock CA 100000000000000000000000000000000000
Certificate Chain: Broade Intermediate CA 1 (51850-0542C221764D66FC0255859)     Broade Rear CA 1 (2759FFA1D05515742A9CFC28-4688180000BC123)     Expiration Date: 2018/0021 1228 PST     Begin Date: 2017/0021 1228 PST     Key Lengt: 2:09
Broade Rot CA 1 (27756774106515794345CrC28-6581E503D8C125)     Expiration Date: 30100202 1228 PST     Begin Date: 30170202 1228 PST     Key Length: 249
Expiration Date         20180002 1228 PGT           Begin Date         20170202 128 PGT           Key Length:         2048
Begin Date: 20170202 1228 95T
Begin Date: 20170201128 PST     Key Length: 2048
E Key Length: 2048
Serial Number: d488068/99602453bed41stdf0ce698dcf09s1
Thumborint EE7/AL995000007071150AAA2303007777795
C IIIIIIIIIIIII EACAASSEEMIY / 21/15/00/38/58/EL///2E
RADIUS Information
Attribute Value
Acc-Sesson-1d
Laing-station-lia A0136/9F682.2019F
Con-Cartilase-PA 40
Cpr-Certiface-Templea-Pk 3
Cpr-Enrollment-Pk 1777
Cpn-Radus-Clenc-Pk 4
Cpn-Registration-Pk
Cpn-Said Echemat
Filerid inatia
Markan Para Markan M
NA-stoentner IOX-Suitch
Sesion-Timeout
Tunne <sup>1</sup> -Medium <sup>-</sup> Type IEEE-802
Turnel-Private-Group-1d 200
Tunnel-Type VLAN
User-Name v havdnit Shorada mmitla user unvali mmada mm
johand ager ocade, com gobact, while o cade, com
accurd% 1
accurd% 1 action authentication
accurd% 1 action authentication
accumPk 1 accumPk a therefore a whereason
accountRk 1 accountRk authentidation action authentidation • Enrollment Variables
accountRk 1 accountRk addression activetodeson beneficient Variables beneficient Variabl
accountific     1       accountific     authenciation       accountific     authenciation
accurd\$k 1 accurd\$k 1 accurd\$k t

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

← ⊕ M http://cloudp	athsqa.englab.b	rocade.com/admin/connection	Data/viewConnected		ア・C I Cloudpath ES ×	1 P.	San Marth
	Cloudpat	h ES   Brocade					Ω 🛛 ιο
Cloudpath	Connect	ions Disconnects All					
▼ Dashboard							
Walcoma		Status	IP Address	MAC Address	Usemame	SSID	Duration
Provides a general overview of the	٩X	Connected		A0:36:9F:6E:1F:D0	jchandra@brocade.com@defaultcert.www.brocade.com	Etherne	10 minutes ago
system.	QΧ	Connected		A0:36:9F:6E:2D:9F	jchandra@brocade.com@guest.www.brocade.com	Etherne	20 minutes ago
Connections	QΧ	Connected		00:24:C4:42:BB:24	jchandra@brocade.com	Etherne	9 minutes ago
Review current connections.							
Enrollments				pp op Resu	15 1 - 3 67 3. (F (F) (F) (F) (F) (F) (F) (F) (F) (F)		
Review enrollments, including the associated user, device, and certificate information.							

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:	10 minutes ago
NAS Identifier:	ICX-Switch
NAS IP:	
NAS Port:	
NAS Port Type:	
Session ID:	
Last Accounting Update:	628601 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@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



## Ruckus ICX Flexible Authentication with Cloudpath ES 5.0 Deployment Guide 53-1005026-02

## 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).