TECHNICAL DOCUMENTATION

Cloudpath

Enrollment System

Cloudpath Onboard RADIUS Server Change of Authorization (CoA)

Software Release 5.0

December 2016

Summary: This document describes how to configure CoA on Ruckus Wireless Controllers and Brocade Switches to work with Cloudpath CoA and Connection Tracking.
Document Type: Configuration
Audience: Network Administrator

Cloudpath Onboard RADIUS Server Change of Authorization (CoA)

Software Release 5.0

December 2016

This document contains Ruckus Wireless confidential and proprietary information. It is not to be copied, disclosed or distributed in any manner, in whole or in part, without express written authorization of a Customer Advocacy representative of Ruckus Wireless, Inc. While the information in this document is believed to be accurate and reliable, except as otherwise expressly agreed to in writing, RUCKUS WIRELESS PROVIDES THIS DOCUMENT "AS IS" WITHOUT WARRANTY OR CONDITION OF ANY KIND, EITHER EXPRESS OR IMPLIED. The information and/or products described in this document are subject to change without notice.

Cloudpath Change of Authorization (CoA) Configuration Guide

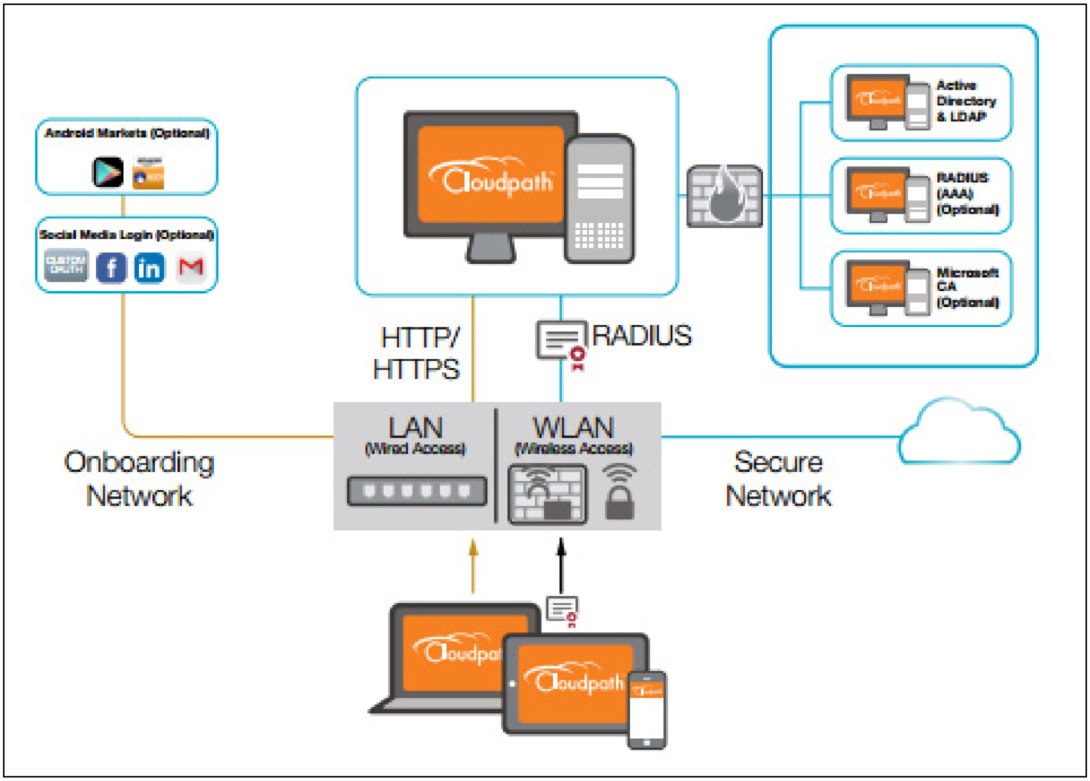
Cloudpath Security and Management Platform

Cloudpath Enrollment System (ES) software is a security and policy management platform that enables any IT organization to protect the network by easily and definitively securing users and their wired and wireless devices—while freeing those users and IT itself from the tyranny of passwords.

Available cloud-managed or as a virtual instance and priced per user, Cloudpath software lets IT do with one system what usually requires many, while easily and automatically integrating with existing access and network security infrastructure.

Cloudpath software consolidates and simplifies the deployment of multiple services that are typically disparate and complex to manage: Certificate Management, Policy Management and Device Enablement.

FIGURE 1. Cloudpath Security and Policy Management Platform



RADIUS Change of Authorization (CoA)

The Cloudpath onboard RADIUS server can send CoA disconnect messages using two triggers. The first is a manual disconnect of an active connection. The second is when a certificate is revoked for a user. The Cloudpath onboard RADIUS server sends the CoA disconnect to the AP, which evaluates the authentication status of the connection.

If COA is active, the system will attempt to send COA requests. This option is only available if RADIUS is enabled and Connection Tracking is enabled on the Cloudpath system.

CoA traffic is sent over UDP port 3799.

CoA Configuration

Supported CoA Configurations

- Cloudpath communicates directly to the AP over port 3799
- Cloudpath through the cloud and a firewall with NATing to APs (with port forwarding)
- Cloudpath through the cloud with NATing to APs on a subnet (with port forwarding)

CoA Configuration for Brocade Switches

When configuring the switch, Cloudpath is a RADIUS client to the switch, and the Cloudpath onboard RADIUS server is a RADIUS server to the switch, so both must be configured.

Enable CoA

```
aaa authorization coa enable
```

Configure Cloudpath as RADIUS Client

```
radius-client coa host 192.168.xx.xx key pass
```

Where host is the IP address of the Cloudpath system and pass is the CoA shared secret.

Configure Cloudpath Onboard RADIUS Server as RADIUS Server

Cloudpath RADIUS server listens on port 1812 for RADIUS authentication, and port 1813 for RADIUS accounting.

```
radius-server host 192.168.xx.xx auth-port 1812 acct-port 1813 default key pass
dot1x
```

Where host is the IP address of the Cloudpath system, 1812 and 1813 are the authentication and accounting ports, respectively, and pass is the shared secret.

If you are configuring an external RADIUS server (as in the command above) you must also configure:

```
aaa authentication dot1x default radius
```

This command disables authentication. The client is automatically authenticated by other means, without the device using information supplied by the client.

Example Configuration for an ICX 7250 Switch

```
authentication
 auth-default-vlan 1000
 dot1x enable
 dot1x enable ethe 1/1/2 to 1/1/10
 dot1x timeout tx-period 10
 dot1x timeout quiet-period 10
 dot1x timeout supplicant 10
 mac-authentication enable
 mac-authentication enable ethe 1/1/2 to 1/1/10
!
aaa authentication dot1x default radius
aaa authentication login default tacacs+ local
aaa authorization coa enable
aaa accounting exec default start-stop radius
aaa accounting dot1x default start-stop radius
enable super-user-password .....
hostname ICX7250
ip address 192.168.xx.xx 255.255.252.0
ip dns server-address 192.168.xx.xx 75.75.75.75 8.8.8.8
no ip dhcp-client enable
ip default-gateway 192.168.xx.xx
!
logging buffered 1000
radius-client coa host 192.168.xx.xx key 2 $b24tb29uLW8=
radius-client coa host 192.168.xx.xx key 2 $b24tbw==
radius-client coa port 1700
radius-server host 192.168.xx.xx auth-port 1812 acct-port 1813 default key 2
$b24tbw== dot1x
radius-server test test

ntp
 server 17.16.xx.xx
```

```
!
interface ethernet 1/1/2
 dot1x port-control auto
!
interface ethernet 1/1/24
 port-name UPLINK to Cisco Lab Switch
!
interface ethernet 1/2/1
 disable
 speed-duplex 1000-full
!
interface ethernet 1/2/2
 disable
 speed-duplex 1000-full
!
interface ethernet 1/2/3
 disable
 speed-duplex 1000-full
!
interface ethernet 1/2/4
 disable
 speed-duplex 1000-full
!
interface ethernet 1/2/5
 disable
 speed-duplex 1000-full
!
interface ethernet 1/2/6
 disable
 speed-duplex 1000-full
!
interface ethernet 1/2/7
 disable
 speed-duplex 1000-full
!
```

```
interface ethernet 1/2/8
 disable
 speed-duplex 1000-full
```

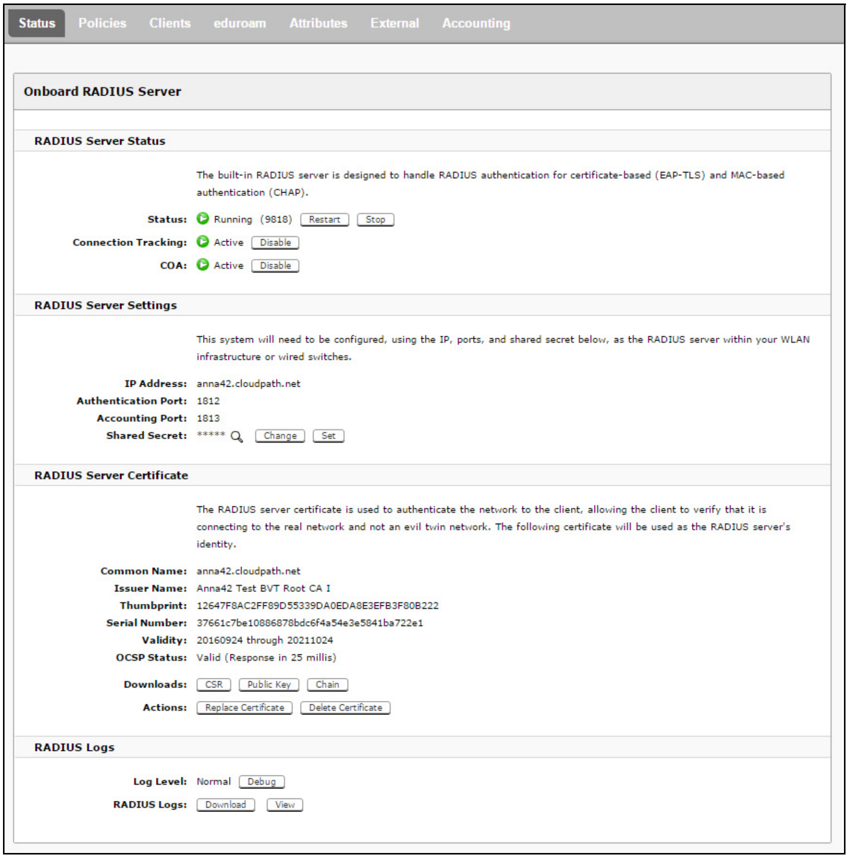
CoA Configuration for Cloudpath Enrollment System

When configuring Cloudpath, the switch is a client to the Cloudpath server. In the client list, the order is configurable. Cloudpath uses first match.

Enable CoA

1. Enable CoA for the Cloudpath RADIUS server. (Enabled by default).

FIGURE 2. Cloudpath RADIUS Server Status



Onboard RADIUS Server

RADIUS Server Status

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

Status: Running (9818)
Connection Tracking: Active
COA: Active

RADIUS Server Settings

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

IP Address: anna42.cloudpath.net
Authentication Port: 1812
Accounting Port: 1813
Shared Secret: *****

RADIUS Server Certificate

The RADIUS server certificate is used to authenticate the network to the client, allowing the client to verify that it is connecting to the real network and not an evil twin network. The following certificate will be used as the RADIUS server's identity.

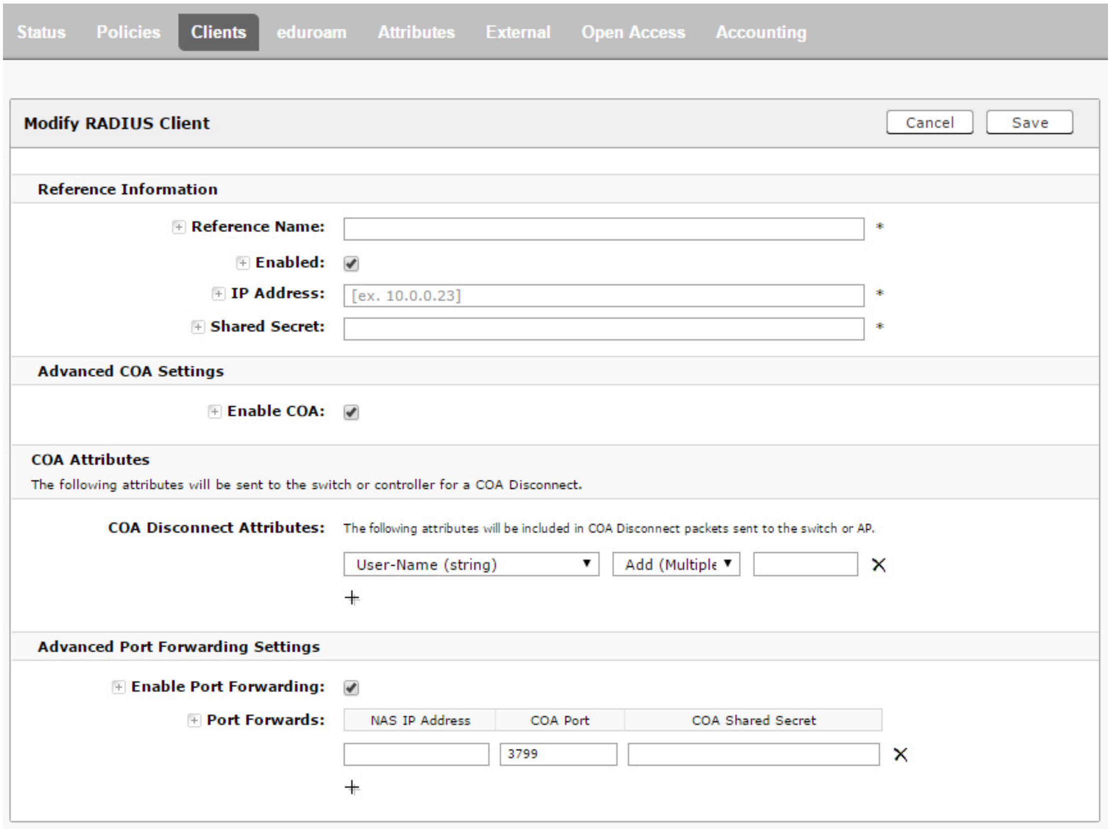
Common Name: anna42.cloudpath.net
Issuer Name: Anna42 Test BVT Root CA I
Thumbprint: 12647F8AC2FF89D55339DA0EDA8E3EFB3F80B222
Serial Number: 37661c7be10886878bdc6f4a54e3e5841ba722e1
Validity: 20160924 through 20211024
OCSP Status: Valid (Response in 25 millis)
Downloads:
Actions:

RADIUS Logs

Log Level: Normal
RADIUS Logs:

2. On the RADIUS Clients page, click Add.

FIGURE 3. Add RADIUS Client



Modify RADIUS Client

Reference Information

Reference Name: *

Enabled: ☑

IP Address: [ex. 10.0.0.23] *

Shared Secret: *

Advanced COA Settings

Enable COA: ☑

COA Attributes

The following attributes will be sent to the switch or controller for a COA Disconnect.

COA Disconnect Attributes: The following attributes will be included in COA Disconnect packets sent to the switch or AP.

User-Name (string) ▼ | Add (Multiple ▼ | ✕

+

Advanced Port Forwarding Settings

Enable Port Forwarding: ☑

Port Forwards:

NAS IP Address	COA Port	COA Shared Secret
	3799	

+

3. Enter the IP Address of the RADIUS client. The RADIUS client might be an AP, or a NAT device if the AP is behind a firewall.
4. Enter the Shared Secret of the RADIUS client. This must match the *key* value on the switch. See the CoA Configuration for Brocade Switches for details.
5. Enable COA must be checked.

CoA Attributes

By default, Cloudpath sends the following CoA disconnect attributes to the switch or AP:

- Calling-Station-Id
- NAS-Ip-Address
- Acct-Session-Id

If your switch or AP vendor requires additional CoA Disconnect attributes, they can be added here. If you don't see the attribute you need to add, go to the RADIUS server *Attributes* tab to enable it.

Port Forwarding

If the ES is communicating with the AP through the cloud or using 1:1 NAT behind a firewall, you can configure port forwarding for the AP.

Enable Port Forwarding must be checked.

Enter the IP address defined locally on the NAS, the Port to use for CoA and the Shared Secret for CoA.

- If a CoA shared secret is left blank, the Shared Secret of the RADIUS client is used.
- If no port forward entry is found for a specified NAS IP address, the default port is used.

Save the configuration. Configuration changes for the RADIUS require a new snapshot.