

Cloudpath Enrollment System Onboard RADIUS Server CoA Configuration Guide, 5.9

Supporting Cloudpath Software Release 5.9

Copyright, Trademark and Proprietary Rights Information

© 2021 CommScope, Inc. All rights reserved.

No part of this content may be reproduced in any form or by any means or used to make any derivative work (such as translation, transformation, or adaptation) without written permission from CommScope, Inc. and/or its affiliates ("CommScope"). CommScope reserves the right to revise or change this content from time to time without obligation on the part of CommScope to provide notification of such revision or change.

Export Restrictions

These products and associated technical data (in print or electronic form) may be subject to export control laws of the United States of America. It is your responsibility to determine the applicable regulations and to comply with them. The following notice is applicable for all products or technology subject to export control:

These items are controlled by the U.S. Government and authorized for export only to the country of ultimate destination for use by the ultimate consignee or end-user(s) herein identified. They may not be resold, transferred, or otherwise disposed of, to any other country or to any person other than the authorized ultimate consignee or end-user(s), either in their original form or after being incorporated into other items, without first obtaining approval from the U.S. government or as otherwise authorized by U.S. law and regulations.

Disclaimer

THIS CONTENT AND ASSOCIATED PRODUCTS OR SERVICES ("MATERIALS"), ARE PROVIDED "AS IS" AND WITHOUT WARRANTIES OF ANY KIND, WHETHER EXPRESS OR IMPLIED. TO THE FULLEST EXTENT PERMISSIBLE PURSUANT TO APPLICABLE LAW, COMMSCOPE DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, TITLE, NON-INFRINGEMENT, FREEDOM FROM COMPUTER VIRUS, AND WARRANTIES ARISING FROM COURSE OF DEALING OR COURSE OF PERFORMANCE. CommScope does not represent or warrant that the functions described or contained in the Materials will be uninterrupted or error-free, that defects will be corrected, or are free of viruses or other harmful components. CommScope does not make any warranties or representations regarding the use of the Materials in terms of their completeness, correctness, accuracy, adequacy, usefulness, timeliness, reliability or otherwise. As a condition of your use of the Materials, you warrant to CommScope that you will not make use thereof for any purpose that is unlawful or prohibited by their associated terms of use.

Limitation of Liability

IN NO EVENT SHALL COMMSCOPE, COMMSCOPE AFFILIATES, OR THEIR OFFICERS, DIRECTORS, EMPLOYEES, AGENTS, SUPPLIERS, LICENSORS AND THIRD PARTY PARTNERS, BE LIABLE FOR ANY DIRECT, INDIRECT, SPECIAL, PUNITIVE, INCIDENTAL, EXEMPLARY OR CONSEQUENTIAL DAMAGES, OR ANY DAMAGES WHATSOEVER, EVEN IF COMMSCOPE HAS BEEN PREVIOUSLY ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, WHETHER IN AN ACTION UNDER CONTRACT, TORT, OR ANY OTHER THEORY ARISING FROM YOUR ACCESS TO, OR USE OF, THE MATERIALS. Because some jurisdictions do not allow limitations on how long an implied warranty lasts, or the exclusion or limitation of liability for consequential or incidental damages, some of the above limitations may not apply to you.

Trademarks

ARRIS, the ARRIS logo, COMMSCOPE, RUCKUS, RUCKUS WIRELESS, the Ruckus logo, the Big Dog design, BEAMFLEX, CHANNELFLY, FASTIRON, ICX, SMARTCELL and UNLEASHED are trademarks of CommScope, Inc. and/or its affiliates. Wi-Fi Alliance, Wi-Fi, the Wi-Fi logo, Wi-Fi Certified, the Wi-Fi CERTIFIED logo, Wi-Fi Protected Access, the Wi-Fi Protected Setup logo, Wi-Fi Protected Setup, Wi-Fi Multimedia and WPA2 and WMM are trademarks or registered trademarks of Wi-Fi Alliance. All other trademarks are the property of their respective owners.

Contents

- RADIUS Change of Authorization (CoA)..... 4**
- CoA Configuration..... 4**
 - Supported CoA Configurations..... 4
 - CoA Configuration for Ruckus Switches..... 4
 - CoA Configuration for Cloudpath Enrollment System..... 5

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 Ruckus 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.

1. Enable CoA

```
aaa authorization coa enable
```

2. 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.

3. 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 or the controller is a client to the Cloudpath server.

In the client list, the order is configurable. Cloudpath uses first match.

Enable CoA

1. Navigate to **Configuration > RADIUS Server**, Status tab.

CoA Configuration

CoA Configuration for Cloudpath Enrollment System

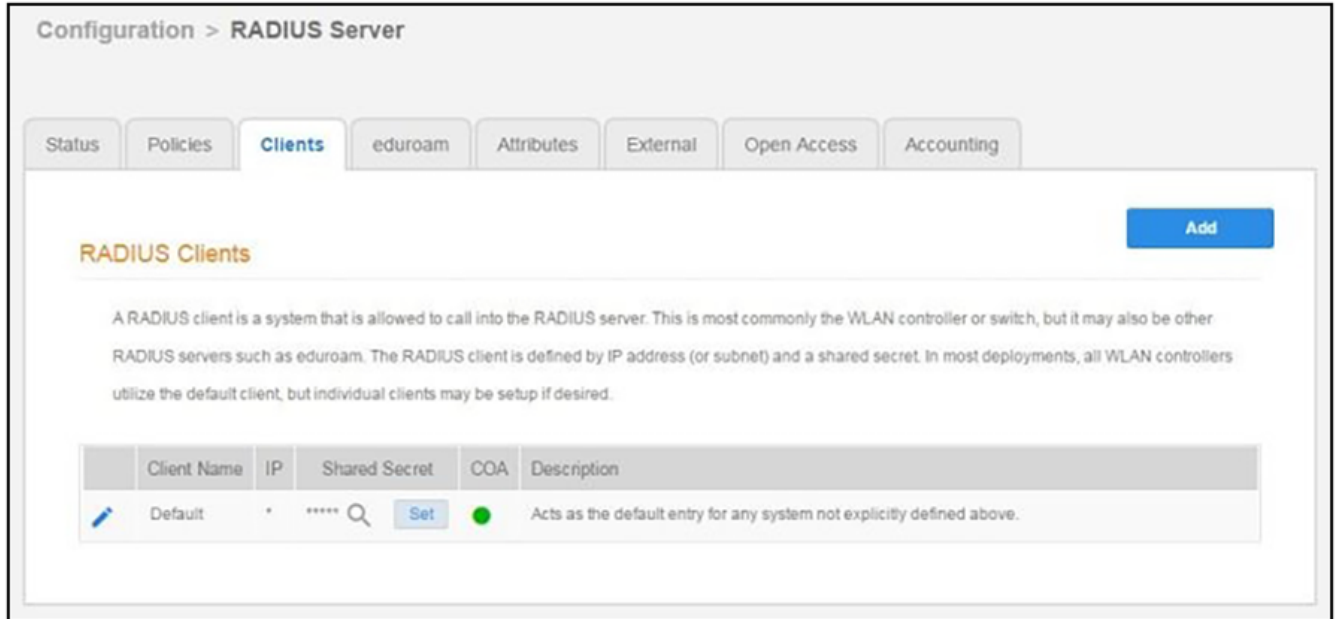
2. Enable CoA for the Cloudpath RADIUS server. (Enabled by default).

FIGURE 1 Cloudpath RADIUS Server Status

The screenshot shows the 'Configuration > RADIUS Server' page. At the top, there are tabs for 'Status', 'Policies', 'Clients', 'eduroam', 'Attributes', 'External', 'Open Access', and 'Accounting'. The 'Status' tab is selected. Below the tabs, the 'RADIUS Server Status' section is displayed. It includes a description: 'The built-in RADIUS server is designed to handle RADIUS authentication for certificate-based (EAP-TLS) and MAC-based authentication (CHAP)'. Below this, there are four status indicators with corresponding buttons: 'Status: Running (11512)' with 'Restart' and 'Stop' buttons; 'Connection Tracking: Active' with a 'Disable' button; 'COA: Active' with a 'Disable' button; and 'RadSec: Disabled' with an 'Enable' button. The 'RADIUS Server Settings' section follows, with a note: 'This system will need to be configured, using the IP, ports, and shared secret below, as the RADIUS server within your WLAN infrastructure or wired switches.' The settings listed are: 'IP Address: jeff243.cloudpath.net', 'Authentication Port: 1812', 'Accounting Port: 1813', and 'Shared Secret: *****' with a search icon and 'New Random' and 'Set' buttons. The 'RADIUS Server Certificate' section is at the bottom, with a note: '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.'

3. On the RADIUS **Clients** tab, click **Add**.

FIGURE 2 RADIUS Clients Tab



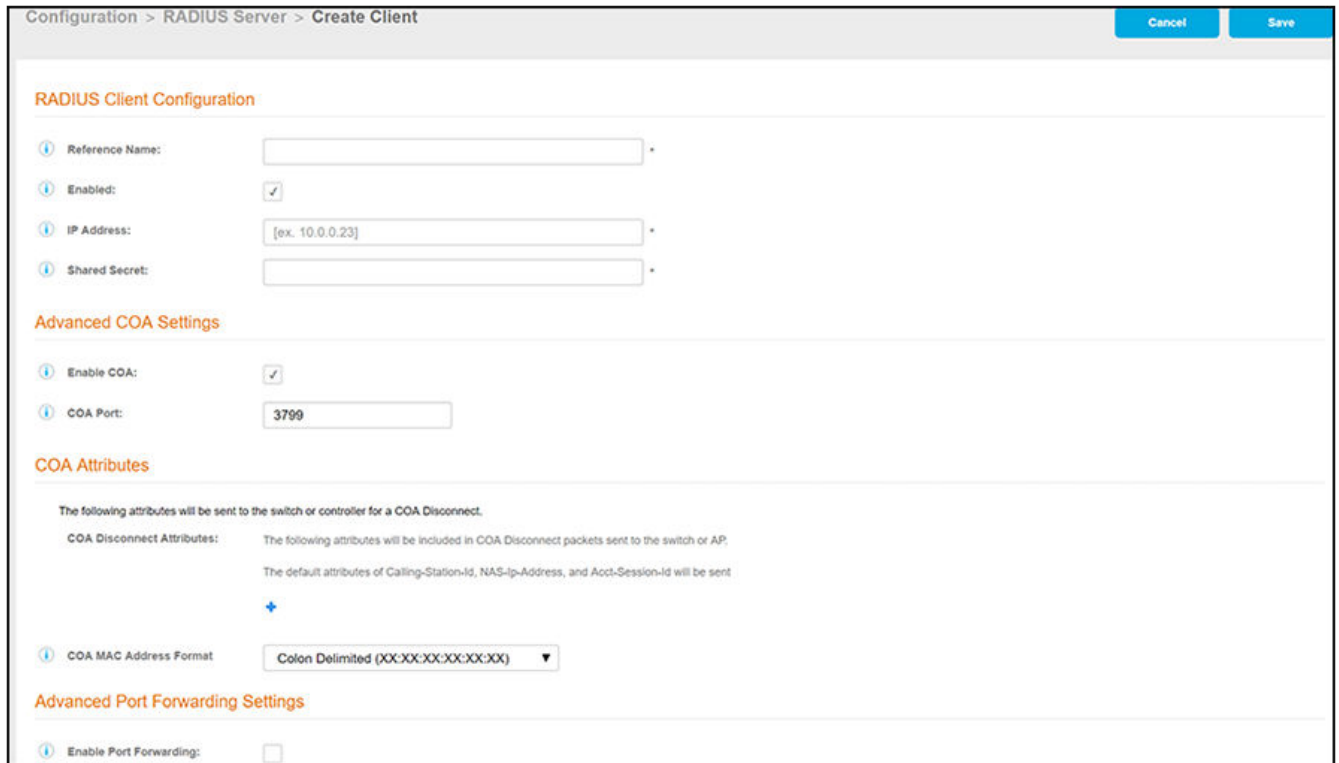
4. Enter the **IP Address** of the RADIUS client. The RADIUS client might be an AP, or a NAT device if the AP is behind a firewall.
5. Enter the **Shared Secret** of the RADIUS client. This must match the key value on the switch or the controller.
6. **Enable COA** must be checked.

CoA Configuration

CoA Configuration for Cloudpath Enrollment System

7. The CoA port is configurable. Its default is 3799, which is used for most CoA configurations. In RADSEC configurations, port 2083 is typically used; some Cisco equipment uses port 1700.

FIGURE 3 Add RADIUS Clients



Configuration > RADIUS Server > Create Client

RADIUS Client Configuration

Reference Name:

Enabled:

IP Address:

Shared Secret:

Advanced COA Settings

Enable COA:

COA Port:

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.
The default attributes of Calling-Station-Id, NAS-Ip-Address, and Acct-Session-Id will be sent

+

COA MAC Address Format:

Advanced Port Forwarding Settings

Enable Port Forwarding:

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

Adding Attributes

If your switch, AP vendor or controller requires additional CoA Disconnect attributes, they can be added here. If you cannot locate the attribute you need, you can go to **Configuration > Radius Server**, "Attributes" tab on the Cloudpath UI to locate and enable the desired attribute.

Attribute Needed for SmartZone 5.1

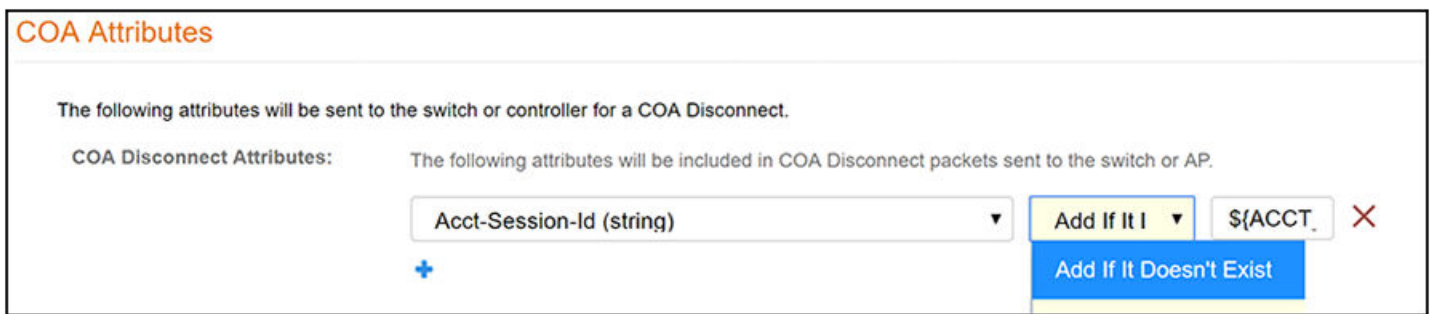
If you are using a SmartZone 5.1 controller, you must do the following:

1. In the **Configuration > Radius Server** portion of the UI, click the "Clients" tab.
2. Either click **Add** to add a new client, or click the pencil icon next to an existing client to modify the configuration.

3. In the ensuing screen, scroll to the COA Attributes section.
4. Click + to add a new attribute, then do the following:
 - a. From the left-most drop down list, select **Acct-Session-Id (string)**
 - b. From the drop-down list to the right, select **And If It Doesn't Exist**.
 - c. In the box to the right, enter the exact following characters: **#{ACCT_SESSION_ID}**
 - d. Click **Save**.

The following illustration depicts the attribute settings described above, but note that the box on the right does not display all the characters of the entry **#{ACCT_SESSION_ID}** simultaneously .

FIGURE 4 CoA Attribute to Send to SmartZone 5.1



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.

1. **Enable Port Forwarding** must be checked.
2. 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.
3. Save the configuration.
Configuration changes for the RADIUS require a new snapshot.

