CONFIGURATION GUIDE

Cloudpath Onboard RADIUS Server Change of Authorization (CoA)

Supporting Software Release 5.2

Part Number: 800-71660-001
Publication Date: September 2017

Copyright Notice and Proprietary Information

Destination Control Statement

Technical data contained in this publication may be subject to the export control laws of the United States of America. Disclosure to nationals of other countries contrary to United States law is prohibited. It is the reader's responsibility to determine the applicable regulations and to comply with them.

Disclaimer

THIS DOCUMENTATION AND ALL INFORMATION CONTAINED HEREIN ("MATERIAL") IS PROVIDED FOR GENERAL INFORMATION PURPOSES ONLY. BROCADE and RUCKUS WIRELESS, INC. AND THEIR LICENSORS MAKE NO WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, WITH REGARD TO THE MATERIAL, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT AND FITNESS FOR A PARTICULAR PURPOSE, OR THAT THE MATERIAL IS ERROR-FREE, ACCURATE OR RELIABLE. BROCADE and RUCKUS RESERVE THE RIGHT TO MAKE CHANGES OR UPDATES TO THE MATERIAL AT ANY TIME.

Limitation of Liability

IN NO EVENT SHALL BROCADE or RUCKUS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL OR CONSEQUENTIAL DAMAGES, OR DAMAGES FOR LOSS OF PROFITS, REVENUE, DATA OR USE, INCURRED BY YOU OR ANY THIRD PARTY, WHETHER IN AN ACTION IN CONTRACT OR TORT, ARISING FROM YOUR ACCESS TO, OR USE OF, THE MATERIAL.

Trademarks

Ruckus Wireless, Ruckus, the bark logo, BeamFlex, ChannelFly, Dynamic PSK, FlexMaster, Simply Better Wireless, SmartCell, SmartMesh, SmartZone, Unleashed, ZoneDirector and ZoneFlex are trademarks of Ruckus Wireless, Inc. in the United States and in other countries. Brocade, the B-wing symbol, MyBrocade, and ICX are trademarks of Brocade Communications Systems, Inc. in the United States and in other countries. Other trademarks may belong to third parties.

Contents

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.

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 is a client to the Cloudpath server.

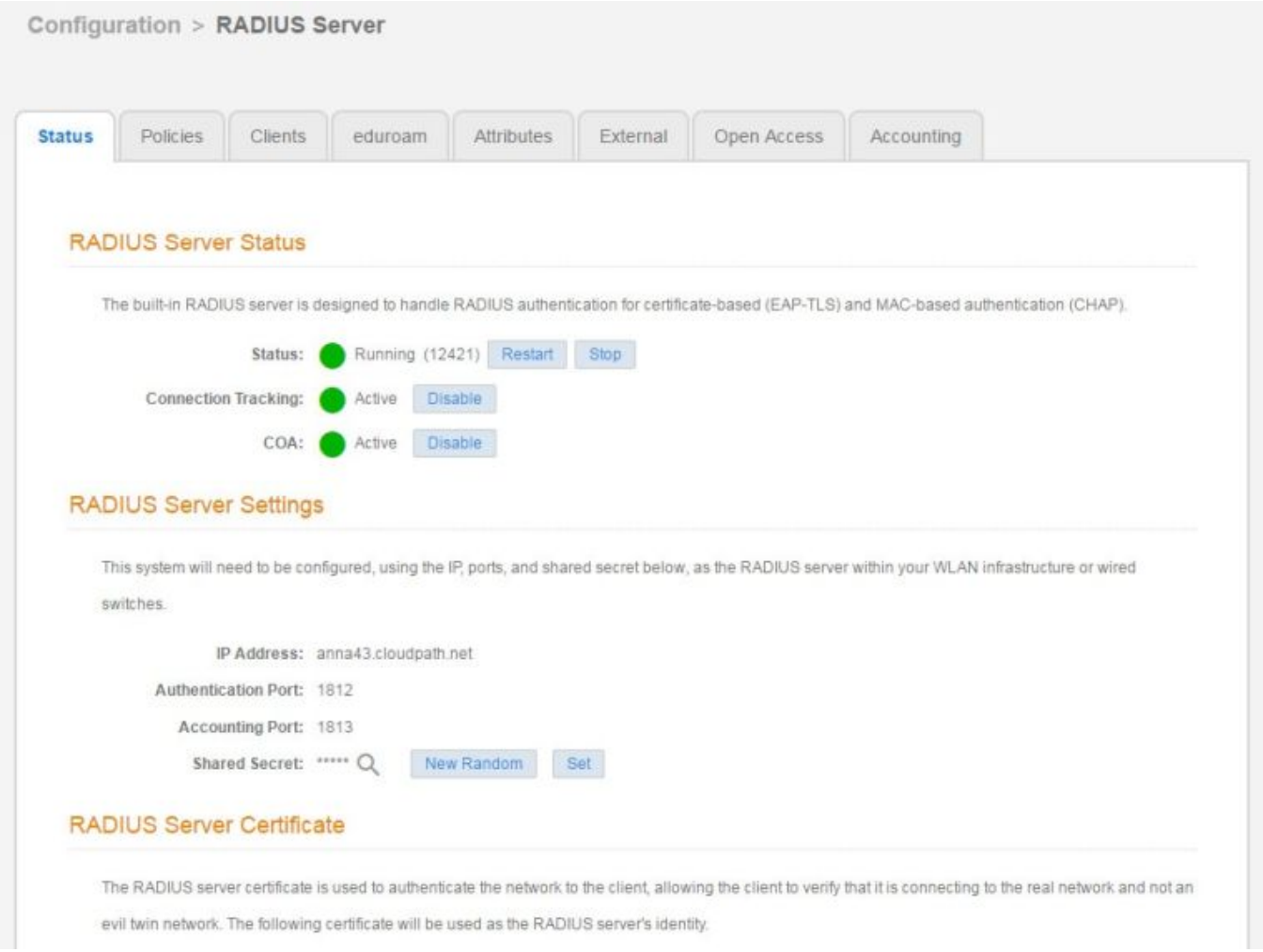
In the client list, the order is configurable. Cloudpath uses first match.

Enable CoA

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

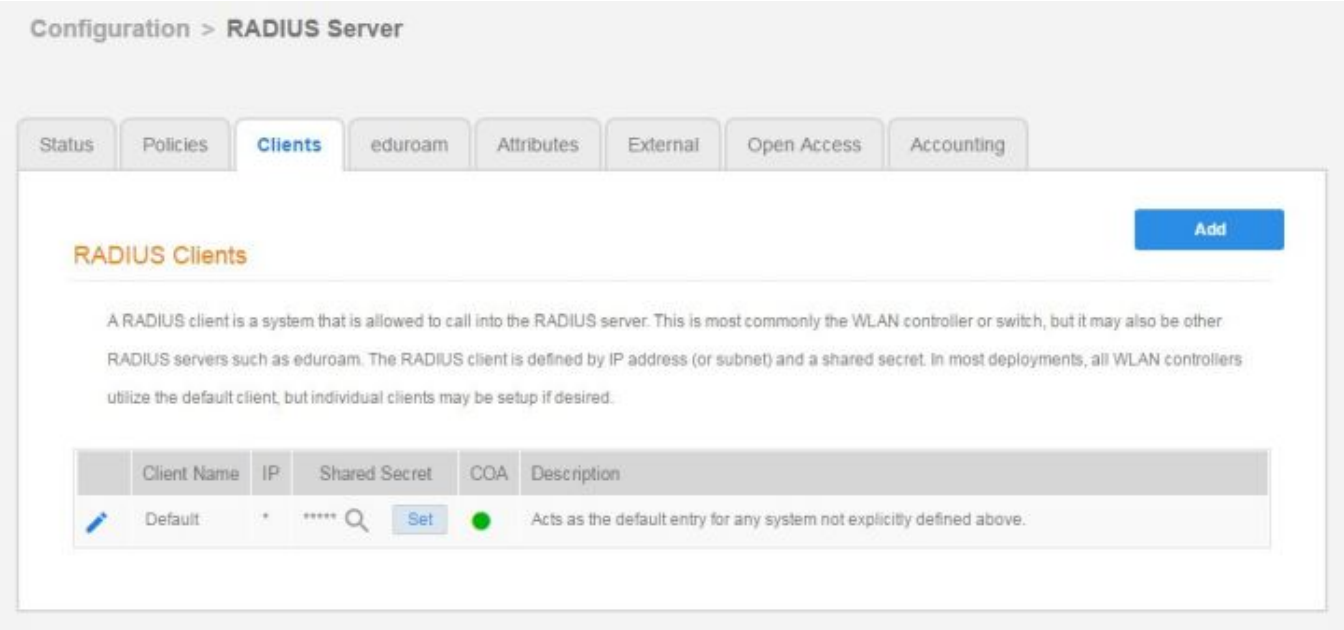
2. Enable CoA for the Cloudpath RADIUS server. (Enabled by default).

FIGURE 1 Cloudpath RADIUS Server Status



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

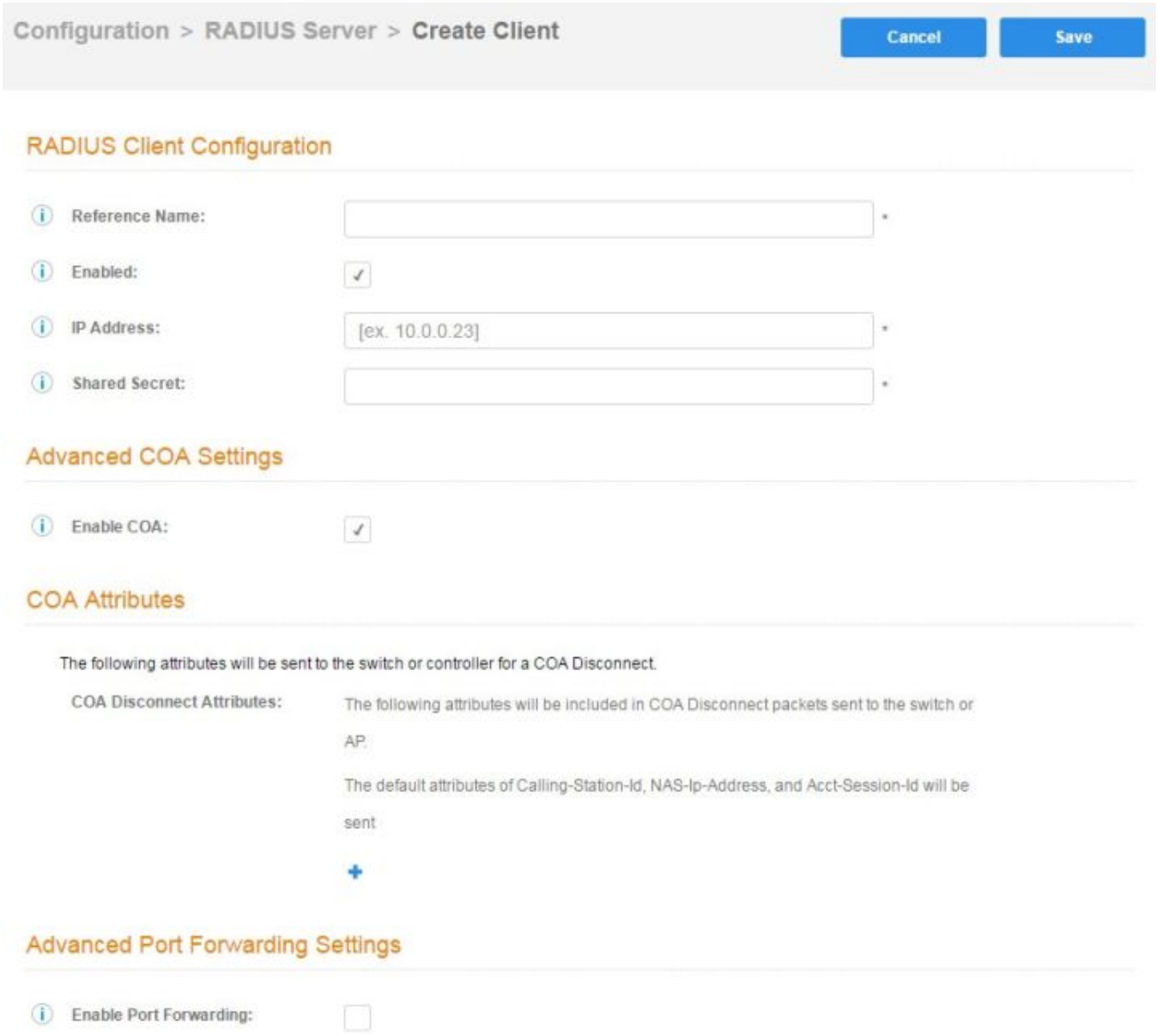
FIGURE 2 RADIUS Clients Tab



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. See the CoA Configuration for Brocade Switches for details.

6. **Enable COA** must be checked.

FIGURE 3 Add RADIUS Clients



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.

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.