

AOS-CX VOIP Deployment Guide

AOS-CX VOIP DEployment guide

AOS-CX VERSION 10.5

Contents

[AOS-CX VOIP Deployment Guide 3](#_Toc47863860)

[Use Case 1: With Local authentication using local mac match, device-profile 4](#_Toc47863861)

[Use case 2: Authenticate phone using AAA radius server. 8](#_Toc47863862)

[Use case 3: VOIP deployment using Local User Role (LUR) 16](#_Toc47863863)

[Use case 3: VOIP Deployment using Download User Role (DUR). 19](#_Toc47863864)

Good day!

AOS-CX VOIP Deployment Guide

 **Prior condition or prerequisite (not mandatory):**

* Good know Power over Ethernet (PoE), LLDP, CDP, VLANs.
* Good know about Voice VLAN and it's Significance.
* Good know Local User Roles, Downloadable User Roles.

**Pre-Checklist:**

* **Check CX operating system version**

BLDG01-F1# show version

* **Verify Connectivity Check**

show lldp neighbor-info or show CDP neighbor-info

* **Before starting VOIP deployment, verify voice vlan assignment.**

BLDG01-F1(config)# vlan 10

BLDG01-F1(config-vlan-10)# voice

BLDG01-F1# show lldp neighbor-info 2/1/3

**Note:** Enabling Voice on Vlan context is must for CX VOIP deployment.

 **Flow of SIMPLE CX VOIP Deployment:**

* **Use Case 1: With Local authentication using local mac match, device-profile**
* **Use Case 2: With Remote AAA authentication using radius-attribute**
* **Use Case 3: With Remote AAA authentication using Local User Role**
* **Use Case 4: With Remote AAA authentication using Downloadable User Role**

**Reviewer:**

Thank you **Hasenaug, Holger** for quick review and format, much appreciate!

Use Case 1: With Local authentication using local mac match, device-profile

**Step1:**Configure local mac match and device profile as below.

BLDG01-F1# show running-config mac-group

mac-group localmacauth

     seq 10 match mac 00:04:f2:80:23:57

BLDG01-F1# show running-config port-access

port-access role localmacauthrole

    mtu 1600

    reauth-period 5

port-access device-profile localauthdp

    enable

    associate role localmacauthrole

    associate mac-group localmacauth

Step2: Enable authentication on interface connected to Phone.

interface 2/1/3

    no shutdown

    no routing

    vlan trunk native 1

    vlan trunk allowed 10

    spanning-tree port-type admin-edge

    aaa authentication port-access allow-cdp-bpdu

    aaa authentication port-access allow-lldp-bpdu

    aaa authentication port-access client-limit 2

    port-access security violation action shutdown

    aaa authentication port-access dot1x authenticator

        max-eapol-requests 3

        max-retries 1

        reauth

        enable

    aaa authentication port-access mac-auth

        cached-reauth

        cached-reauth-period 86400

        quiet-period 30

        enable

    exit

BLDG01-F1# show port-access clients

Port Access Clients

--------------------------------------------------------------------------------

Port     MAC Address       Onboarded      Status      Role

                           Method

--------------------------------------------------------------------------------

2/1/3    00:04:f2:80:23:57 device-profile Success     localmacauthrole

BLDG01-F1# sh port-access clients detail

Port Access Client Status Details:

Client 00:04:f2:80:23:57

============================

  Session Details

  ---------------

    Port         : 2/1/3

    Session Time : 558s

    IPv4 Address :

    IPv6 Address :

  Authentication Details

  ----------------------

    Status          : Authenticated

    Auth Precedence : dot1x - Authenticating, mac-auth - Unauthenticated

  Authorization Details

  ----------------------

    Role   : localmacauthrole

    Status : Applied

Role Information:

Name  : localmacauthrole

Type  : local

----------------------------------------------

    Reauthentication Period             : 5 secs

    Authentication Mode                 :

    Session Timeout                     :

    Client Inactivity Timeout           :

    Description                         :

    Gateway Zone                        :

    UBT Gateway Role                    :

    Access VLAN                         :

    Native VLAN                         :

    Allowed Trunk VLANs                 :

    Access VLAN Name                    :

    Native VLAN Name                    :

    Allowed Trunk VLAN Names            :

    MTU                                 : 1600

    QOS Trust Mode                      :

    STP Administrative Edge Port        :

    PoE Priority                        :

    Captive Portal Profile              :

    Policy                              :

**Note**: Authentication default order on AOS-CX is dot1x, mac-auth and then local mac match device-profile. You can always change the order of authentication.

Use case 2: authenticate phone using AAA radius server.

Step1: Make sure radius connectivity to switch is proper

BLDG01-F1# show radius-server detail

\*\*\*\*\*\*\* Global RADIUS Configuration \*\*\*\*\*\*\*

Shared-Secret: None

Timeout: 5

Auth-Type: pap

Retries: 1

TLS Timeout: 5

Tracking Time Interval (seconds): 60

Tracking Retries: 3

Tracking User-name: radius-tracking-user

Tracking Password: None

Number of Servers: 1

\*\*\*\*\*\* RADIUS Server Information \*\*\*\*\*\*

Server-Name              : aoss-cppm.tmelab.net

Auth-Port                : 1812

Accounting-Port          : 1813

VRF                      : mgmt

TLS Enabled              : No

Shared-Secret            : AQBapdAz4irjSK61Zg/CFArsNYWKbn1LObqDD/v9SH1eMQ6ABQAAADY26liu

Timeout (default)        : 5

Retries                  : 5

Auth-Type (default)      : pap

Server-Group (default)   : radius

Default-Priority         : 1

Tracking                 : enabled

Tracking-Mode            : any

Reachability-Status      : reachable

ClearPass-Username       : admin

ClearPass-Password       : AQBapYv/u3/YfG9vYRpFxmOTtsFLIWxuAX442RdG9j11jsZ6CQAAACZ5Y2/BK9FmhQ==

**Note**: In this demonstration I am using clearpass as Radius-server, you can use any other radius-server such Cisco ISE or free radius.

**Step2: Enable authentication on the interface.**

BLDG01-F1# show running-config interface 2/1/3

interface 2/1/3

    no shutdown

    no routing

    vlan trunk native 1

    vlan trunk allowed 10

    spanning-tree port-type admin-edge

    aaa authentication port-access allow-cdp-bpdu

    aaa authentication port-access allow-lldp-bpdu

    aaa authentication port-access client-limit 2

    port-access security violation action shutdown

    aaa authentication port-access dot1x authenticator

        max-eapol-requests 3

        max-retries 1

        reauth

        enable

    aaa authentication port-access mac-auth

        cached-reauth

        cached-reauth-period 86400

        quiet-period 30

        enable

    exit

BLDG01-F1# show port-access clients detail

Port Access Client Status Details:

Client 00:04:f2:80:23:57, 0004f2802357

============================

  Session Details

  ---------------

    Port         : 2/1/3

    Session Time : 75s

    IPv4 Address :

    IPv6 Address :

  Authentication Details

  ----------------------

    Status          : mac-auth Authenticated

    Auth Precedence : dot1x - Unauthenticated, mac-auth - Authenticated

  Authorization Details

  ----------------------

    Role   : RADIUS\_773420618

    Status : Applied

Role Information:

Name  : RADIUS\_773420618

Type  : radius

----------------------------------------------

    Reauthentication Period             :

    Authentication Mode                 :

    Session Timeout                     :

    Client Inactivity Timeout           :

    Description                         :

    Gateway Zone                        :

    UBT Gateway Role                    :

    Access VLAN                         :

    Native VLAN                         :

    Allowed Trunk VLANs                 :

    Access VLAN Name                    :

    Native VLAN Name                    :

    Allowed Trunk VLAN Names            :

    MTU                                 :

    QOS Trust Mode                      :

    STP Administrative Edge Port        :

    PoE Priority                        :

    Captive Portal Profile              :

    Policy                              :

BLDG01-F1# show vlan port 2/1/3

-------------------------------------------------------------------------------

VLAN  Name                            Mode            Mapping

-------------------------------------------------------------------------------

10    VLAN10                          trunk           port

BLDG01-F1# sh lldp neighbor-info 2/1/3

Port                           : 2/1/3

Neighbor Entries               : 1

Neighbor Entries Deleted       : 1

Neighbor Entries Dropped       : 0

Neighbor Entries Aged-Out      : 1

Neighbor Chassis-Name          : Polycom VVX 500

Neighbor Chassis-Description   : Polycom;VVX-VVX\_500;3111-44500-001,7;SIP/4.1.2.25646/13-Feb-13 17:14;UP/5.1.2.0869/13-Feb-13 17:28;

Neighbor Chassis-ID            : 0.0.0.0

Neighbor Management-Address    :

Chassis Capabilities Available : Bridge, Telephone

Chassis Capabilities Enabled   : Bridge, Telephone

Neighbor Port-ID               : 00:04:f2:80:23:57

Neighbor Port-Desc             : 1

Neighbor Port VLAN ID          :

TTL                            : 120

Neighbor PoE information       : MED

Neighbor Power Type            : PD

Neighbor Power Priority        : Unknown

Neighbor Power Source          : BOTH

PD Requested Power Value       : 8.0 W

PSE Allocated Power Value      : 8.0 W

Neighbor MED Capabilities

Neighbor Device class          : CLASS\_III

MED capabilities enabled       : Capabilities, Network Policy, PD, Inventory

MED capabilities supported     : Capabilities, Network Policy, PD, Inventory

Neighbor Med Network Policy

Neighbor Med Application type  : voice

Neighbor Med Policy VLAN ID    : 10

Neighbor Med Policy Priority   : 5

Neighbor Med Policy DSCP       : 46

Neighbor Med Policy Unknown    : false

Neighbor Med Policy Tagged     : true

Neighbor Med Application type  : voice-signaling

Neighbor Med Policy VLAN ID    : 10

Neighbor Med Policy Priority   : 5

Neighbor Med Policy DSCP       : 44

Neighbor Med Policy Unknown    : false

Neighbor Med Policy Tagged     : true

Neighbor Mac-Phy details

Neighbor Auto-neg Supported    : true

Neighbor Auto-Neg Enabled      : true

Neighbor Auto-Neg Advertised   : 1000 BASE\_TFD, 100 BASE\_TXFD, 100 BASE\_TX, 10 BASET\_FD, 10 BASE\_T

Neighbor MAU type              : 1000 BASETFD

BLDG01-F1#

**Note**: For Pre-standard Phone, enable below command on interface.

BLDG01-F1(config-if)# power-over-ethernet pre-std-detect

Use case 3: VOIP deployment using Local User Role (LUR)

Step1: Configure local user role

BLDG01-F1# show running-config port-access

port-access role **phone\_role**

    auth-mode client-mode

    vlan trunk allowed 10

BLDG01-F1# show running-config interface 2/1/3

interface 2/1/3

    no shutdown

    no routing

    vlan trunk native 1

    vlan trunk allowed all

    spanning-tree port-type admin-edge

    aaa authentication port-access allow-cdp-bpdu

    aaa authentication port-access allow-lldp-bpdu

    aaa authentication port-access client-limit 2

    port-access security violation action shutdown

    aaa authentication port-access dot1x authenticator

        max-eapol-requests 3

        max-retries 1

        reauth

        enable

    aaa authentication port-access mac-auth

        cached-reauth

        cached-reauth-period 86400

        quiet-period 30

        enable

    exit

Step2: On radius-server make sure same role name is configured and phone is authenticated.

BLDG01-F1# show port-access clients

Port Access Clients

--------------------------------------------------------------------------------

Port     MAC Address       Onboarded      Status      Role

                           Method

--------------------------------------------------------------------------------

2/1/3    00:04:f2:80:23:57 mac-auth       Success     phone\_role

BLDG01-F1#

BLDG01-F1# show port-access role

Role Information:

Name  : phone\_role

Type  : local

----------------------------------------------

    Reauthentication Period             :

    Authentication Mode                 : client-mode

    Session Timeout                     :

    Client Inactivity Timeout           :

    Description                         :

    Gateway Zone                        :

    UBT Gateway Role                    :

    Access VLAN                         :

    Native VLAN                         :

    Allowed Trunk VLANs                 : 10

    Access VLAN Name                    :

    Native VLAN Name                    :

    Allowed Trunk VLAN Names            :

    MTU                                 :

    QOS Trust Mode                      :

    STP Administrative Edge Port        :

    PoE Priority                        :

    Captive Portal Profile              :

    Policy                              :

Use case 4: VOIP Deployment using Download User Role (DUR).

Enable aaa authentication on the interface.

Configure downloadable user role “phone\_role” on Clearpass as below.

 



BLDG01-F1# sh port-access clients

Port Access Clients

--------------------------------------------------------------------------------

Port     MAC Address       Onboarded      Status      Role

                           Method

--------------------------------------------------------------------------------

2/1/3    00:04:f2:80:23:57 mac-auth       Success     DUR\_PY\_CX-3099-10

BLDG01-F1# show port-access role clearpass

Role Information:

Name  : DUR\_PY\_CX-3099-10

Type  : clearpass

Status: Completed

----------------------------------------------

    Reauthentication Period             :

    Authentication Mode                 : client-mode

    Session Timeout                     :

    Client Inactivity Timeout           :

    Description                         :

    Gateway Zone                        :

    UBT Gateway Role                    :

    Access VLAN                         :

    Native VLAN                         :

    Allowed Trunk VLANs                 : 10

    Access VLAN Name                    :

    Native VLAN Name                    :

    Allowed Trunk VLAN Names            :

    MTU                                 :

    QOS Trust Mode                      :

    STP Administrative Edge Port        :

    PoE Priority                        :

    Captive Portal Profile              :

    Policy                              :

**Attached CX switch Working Running configuration**



 **Note**: Please configure ip helper address on interface vlan if you looking to assign dhcp ip address to phone, will add dhcp section in next document.

Below Simple references will help during CX VOIP deployment:

* [**AOS-CX Simple steps to configure Radius-server**](https://community.arubanetworks.com/t5/Wired-Intelligent-Edge-Campus/AOS-CX-Radius-server-simple-steps-to-Configure/m-p/663009#M10219)
* [**AOS-CX Downloadable User Role (DUR) simple steps to Configure**](https://community.arubanetworks.com/t5/Wired-Intelligent-Edge-Campus/AOS-CX-Downloadable-User-Role-DUR-simple-steps-to-Configure/td-p/663721)
* [**AOS-CX Local User Role (LUR) simple steps to Configure**](https://community.arubanetworks.com/t5/Wired-Intelligent-Edge-Campus/AOS-CX-Local-User-Role-LUR-simple-steps-to-Configure/td-p/663150)

 Have a nice day!

Yash