

CX Port-Access Multi Domain Authentication (MDA)

Presenters

- Yash, TME

aruba

a Hewlett Packard
Enterprise company



Agenda

- 1 Overview
- 2 Use Cases
- 3 Details and Caveats
- 4 Configuration
- 5 Best Practices
- 6 Troubleshooting
- 7 Demo
- 8 Additional Resources






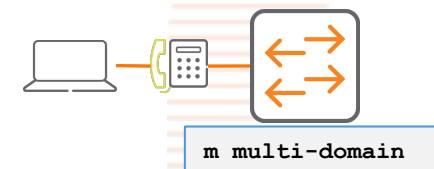
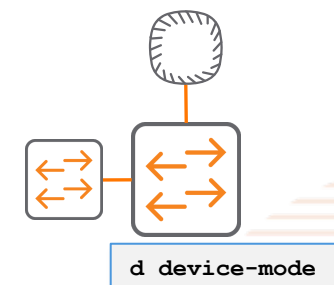
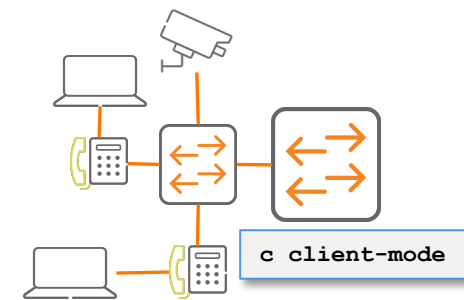
The background features a solid dark blue field. In the top-left corner, a large, solid red circle is partially visible. A large, irregular shape in the center-right is filled with a dense pattern of small red dots, creating a halftone effect.

Overview & Use Cases

CX Port Access Auth Mode

– Overview: 10.8 port-access multi-domain to allow only one voice client per port

CX Port-Access Auth-Mode	Description
<p>Client-mode (10.4) N Auth Clients</p> 	<p>When port is in this auth-mode, all clients connecting to the port are sent for authentication.</p> <p>Note: All client needs to go through the authentication process, but no strict restriction per port number of voice or data devices. This is the default auth-mode.</p> <p>In other words, all are allowed for authentication.</p>
<p>Device-mode (10.4) 1 Auth Client + N</p> 	<p>In this mode, only the first client connecting to the port is sent for authentication.</p> <p>Note: Port is open just after first client is authenticated as per client-limit.</p>
<p>Multi-domain (10.8) Only one Voice client + 5 Data clients</p> 	<p>In this mode, only one voice device can be authenticated along with the configured <u>data devices</u>.</p> <p>Note: Only one voice client and a maximum of five data clients are allowed for authentication.</p> <p>Multi-domain mode is same as client mode except the one voice and data client limit restriction.</p>





Details and Caveats

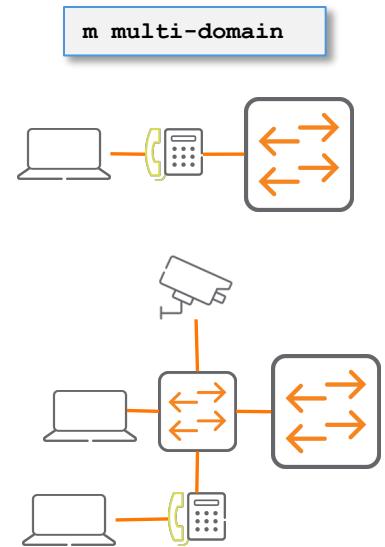
Multi Domain Authentication (MDA) Sub Features

– Multi Domain Authentication Sub features

- Auth-mode multi-domain
- Multi-Domain data client-limit
- New special role:
 - **Critical voice Role**, Used when voice client auth has been failed due to radius not reachable.
 - **Note that**, role is applicable only after first authentication.
- **Aruba VSA:**
 - Aruba-Port-Auth-Mode = Multi-Domain-Mode

Below Features are supported across three auth-modes

- User Role voice attribute
 - device-traffic-class
- Auth auto VLAN feature.
- Port-access security violation.
- **Aruba VSA:**
 - Aruba-Device-Traffic-Class(63)= 1



Note: ClearPass Radius Dictionary file update required for these VSA

Multi Domain Authentication (MDA)

- Multidomain authentication allows a combination of voice data clients to be authenticated on a port. Only one voice client and a maximum of five data clients **are allowed for authentication**.
- By default, only one data device is allowed on the `multi-domain` enabled port along with a voice device. If second voice device or data device greater than the configured data client limit onboards, triggers violation.
- Admin can enable the multidomain authentication mode with the `aaa authentication port-access auth-mode` command.
- Admin can configure only the number of data clients supported with the command. `aaa authentication port-access client-limit multi-domain`
- To authorize a voice device, the AAA server must be configured to send an Aruba Attribute-Value (AV) `Aruba-Device-Traffic-Class` with value **1** or role to be applied should have device type (*device-traffic-class* as voice) that indicates voice device.
- Without this value VSA or device type in role, the switch treats the voice device as a data device.
- admin can configure only the number of data clients supported with the `aaa authentication port-access client-limit multi-domain` command.



Multi Domain Authentication (MDA)

- In case client mode is set and clients limits is configured, and mode changes to multi-domain mode, then configured client limit is ignored.
- Violation will occur on multi-domain enabled port in the following conditions
 - More than one voice device authenticates on the port
 - Data devices beyond configured data client limit authenticates on the port.
- Device-profile clients can also inter-op with MDA or in stand-alone mode with security (A.K.A Mac-Match mode).



Configuration and Supported Platforms

Multi Domain Authentication (MDA) Configuration!

– MDA features

- **Multi Domain Mode, only one voice device is allowed on the port while data device limit is configurable.**

```
(config-if)# aaa authentication port-access auth-mode multi-domain
```

"Aruba-Port-Auth-Mode"

- By default, one voice and data client is allowed on the port.
- **Maximum 5 data clients** can be configured on the port. **Only one voice client is allowed on the port always** and not configurable.
- Client-limit configured of client mode will be ignored when mode is changed to multi-domain mode.

```
(config-if)# aaa authentication port-access client-limit multi-domain  
<1-5> Specify the number of data clients to allow on multi-domain enabled  
port for network access. (Default: 1)
```

- **New Aruba VSA or `device-traffic-class` in role.**

- Without the VSA or device-traffic-class in role, device will be treated as data device

```
port-access role phone_role  
auth-mode multi-domain  
device-traffic-class voice  
vlan access 10
```

NEW VSA "Aruba-Device-Traffic-Class" (63)

*How to add new VSA attribute in ClearPass refer to ToI

- **Port-access security violation**

```
(config-if)# port-access security violation action  
notify Configure notify violation action on the port.  
shutdown Configure shutdown violation action on the port. (Default: notify)
```



Multi Domain Authentication (MDA)

– MDA features

- **Critical voice Role, Used when voice client auth has been failed due to radius not reachable**

```
(config-if)# aaa authentication port-access critical-role <ROLE-STR>
```

- **Auth Auto Vlan feature**

```
(config)# port-access auto-vlan
```

Platform	4100i	6100	6200	6300	6400	8320	8325	8360	8400	Simulator
Multi-Domain Authentication	Yes	Yes	Yes	Yes	Yes	No	No	No	No	Yes

Troubleshooting

The background features a solid red circle on the left side. On the right side, there is a large, irregular shape filled with a pattern of small, light blue dots, set against a dark blue background.

Troubleshooting - Mirror

Mirror session 1

Source interface 1/1/1 both

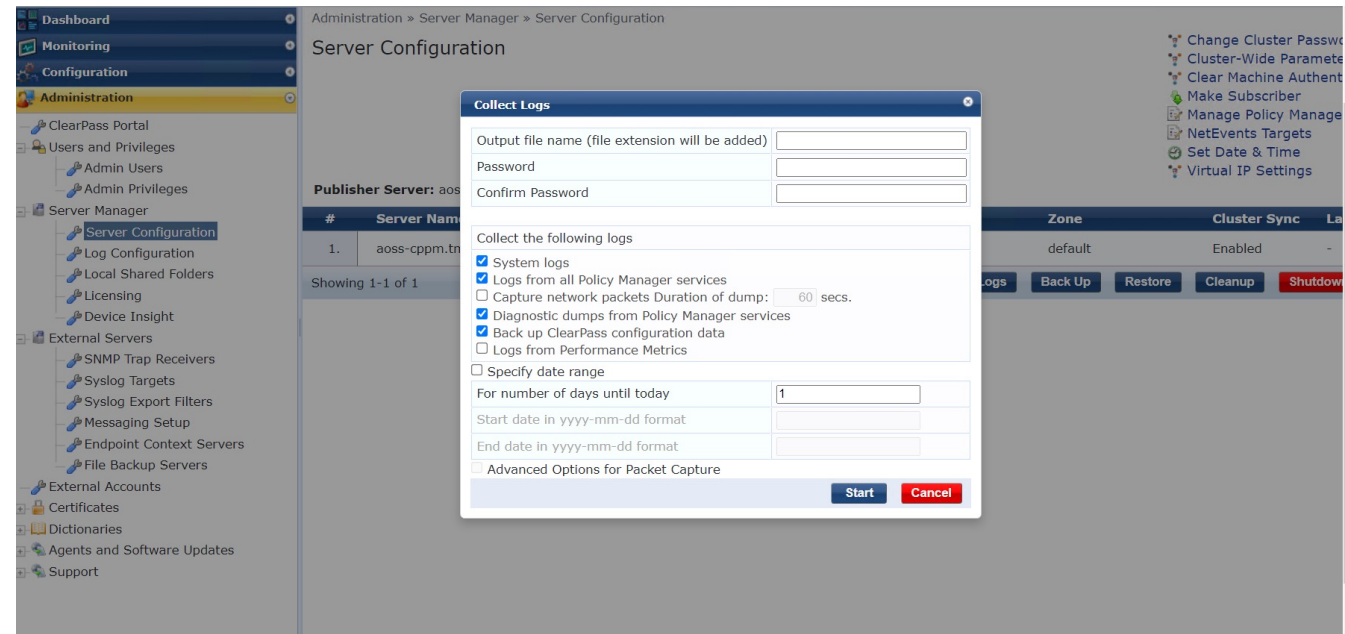
Destination CPU

enable

diag utilities tshark file

copy tshark-pcap tftp://10.80.2.187/djky.pcap vrf mgmt

Note: Once done disable or delete mirror session



Feature/Solution Troubleshooting

Basic level

6300-1-VSF#

- show mac-address-table detail
- show lldp neighbor-info
- show cdp neighbor-info
- show radius-server detail
- show port-access clients detail
- show aaa authentication port-access dot1x authenticator interface all client-status
- show aaa authentication port-access mac-auth interface all client-status
- show aaa authentication port-access interface all client-status

6300-1-VSF#

show events -r -d port-accesssd

- Diagdump

6300-1-VSF# diagnostics

diag-dump port-access basic

diag-dump dot1x-authenticator basic

diag-dump mac-auth basic

- Debugs

6300-1-VSF#

debug radius all

debug port access all

debug destination buffer

6300-1-VSF#

show debug buffer

Feature/Solution Troubleshooting

6300-1-VSF#

- show mac-address-table detail
- show lldp neighbor-info
- show cdp neighbor-info
- show radius-server detail
- show port-access clients detail
- show aaa authentication port-access dot1x authenticator interface all client-status
- show aaa authentication port-access mac-auth interface all client-status
- show aaa authentication port-access interface all client-status

- Diagdum

6300-1-VSF# diagnostics

diag-dump port-access basic

diag-dump dot1x-authenticator basic

diag-dump mac-auth basic

- Debugs

6300-1-VSF#

debug radius all

debug port access all

debug destination buffer

6300-1-VSF#

show debug buffer

Feature/Solution Troubleshooting

Advance level

- start-shell - Are you ready ☺!

```
6300-1-VSF# start-shell
```

```
6300-1-VSF:~$ pwd
```

```
/home/admin
```

```
6300-1-VSF:~$ sudo bash
```

```
6300-1-VSF:/home/admin#
```

```
6300-1-VSF:/home/admin# ovs-appctl -t port-accessd fastlog show
```

```
6300:~$ cd /var/log/
```

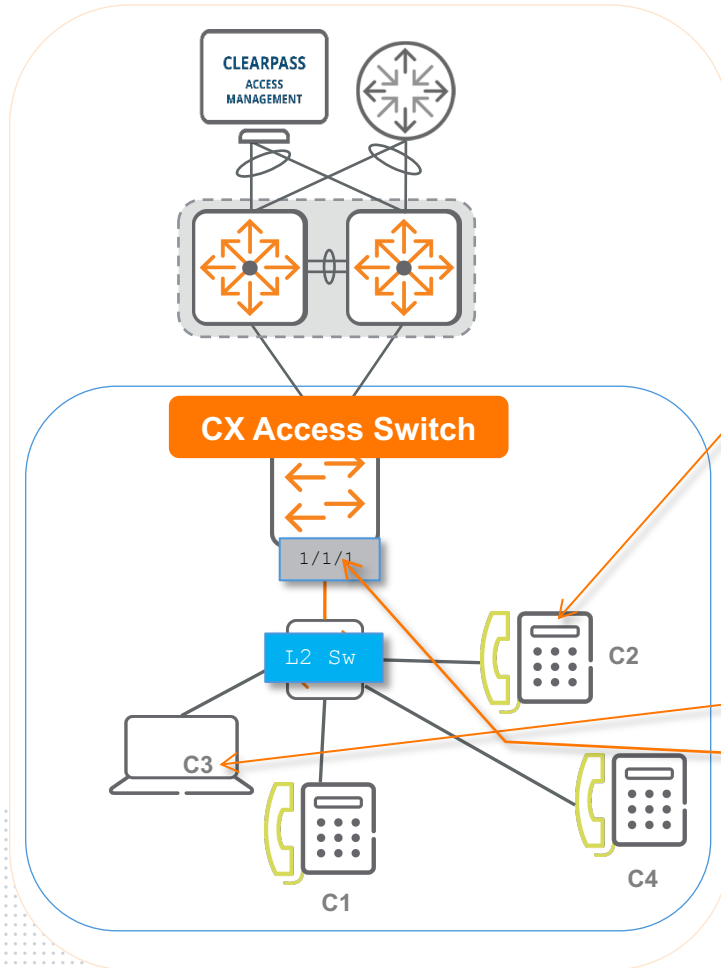
```
6300:/var/log$ ls -l
```

```
6300:/var/log$ journalctl -n 100 | grep lldpd
```

The background features a solid red circle on the left side. On the right side, there is a large, irregular shape filled with a blue dotted pattern, resembling a halftone effect. The word "Demo" is written in white, bold, sans-serif font, positioned over the red circle.

Demo

MDA Demonstration



```
port-access role phone_role  
  auth-mode multi-domain  
  reauth-period 100  
  cached-reauth-period 200  
  device-traffic-class voice  
  vlan trunk native 10  
  vlan trunk allowed 10,112
```

1

```
port-access role data_role  
  associate captive-portal-profile TEST  
  associate policy cp_policy  
  vlan access 10
```

2

```
interface 1/1/1  
  no shutdown  
  no routing  
  vlan access 1  
  aaa authentication port-access mac-auth  
    enable  
  exit
```

3

Looking Configure VSA from ClearPass ? Wait!!

Aruba VSA Configuration from ClearPass (Radius-Server)

aruba

ClearPass Policy Manager

Dashboard

Monitoring

Configuration

Service Templates & Wizards

Services

Authentication

Identity

Posture

Enforcement

Policies

Profiles

Configuration » Enforcement » Profiles » Edit Enforcement Profile - LUR_PY_CX_Data

Enforcement Profiles - LUR_PY_CX_Data

SummaryProfileAttributes

Type	Name	Value
1. Radius:Aruba	Aruba-User-Role	= data_role
2. Radius:Aruba	Aruba-Device-Traffic-Cla	= 1
3.	Click to add...	

Aruba-Device-Traffic-Class

<Attribute profile="in out" type="Unsigned32" name="Aruba-Device-Traffic-Class" id="63"/>

Configuration

Administration

ClearPass Portal

Users and Privileges

Server Manager

Server Configuration

Log Configuration

Local Shared Folders

Licensing

Device Insight

External Servers

External Accounts

Certificates

Dictionaries

RADIUS

RADIUS Dynamic Authorization

TACACS+ Services

Device Fingerprints

Dictionary Attributes

Applications

Context Server Actions

Ingress Events

Windows Hotfixes

OnGuard Custom Scripts

This page allows admins to view the list of RADIUS dictionaries, view attributes and enable or export dictionaries.

Filter: Vendor Name contains aruba Go Clear Filter

#	Vendor Name	Vendor ID	Vendor Prefix	Enab
1.	Aruba	14823	Aruba	true

Showing 1-1

RADIUS Attributes

Vendor Name: Aruba (14823)

19.	Aruba-Captive-Portal-URL	43	String	in out
20.	Aruba-Command-String	46	String	in out
21.	Aruba-Device-Traffic-Class	63	Unsigned32	in out
22.	Aruba-Device-Type	12	String	in out
23.	Aruba-Essid-Name	5	String	in out
24.	Aruba-Framed-IPv6-Address	11	String	in out
25.	Aruba-Gateway-Zone	54	String	in out
26.	Aruba-Location-Id	6	String	in out
27.	Aruba-MPSK-Passphrase	44	OctetArray	in out
28.	Aruba-Mdps-Device-Iccid	17	String	in out
29.	Aruba-Mdps-Device-Imei	16	String	in out

Disable Export Close

Aruba-Device-Traffic-Class



Aruba VSA Configuration from ClearPass (Radius-Server)

aruba

Dashboard

Monitoring

Configuration

Service Templates & Wizards

Services

Authentication

Identity

Posture

Enforcement

- Policies
- Profiles

ClearPass Policy Manager

2

Configuration » Enforcement » Profiles » Edit Enforcement Profile - LUR_PY_CX_Data

Enforcement Profiles - LUR_PY_CX_Data

Summary

Profile

Attributes

	Type	Name		Value
1.	Radius:Aruba	Aruba-User-Role	=	data_role
2.	Radius:Aruba	Aruba-Device-Traffic-Class	=	1
3.	Radius:Aruba	Aruba-Port-Auth-Mode (=	<div>Aruba-Port-Auth-Mode</div>
4.	Click to add...			

Infrastructure-Mode (1)

Client-Mode (2)

Multi-Domain-Mode (3)

MDA

```
<Attribute profile="in out" type="Unsigned32" name="Aruba-Port-Auth-Mode" id="50">
  <ValidValues>
    <ValidValue enumOrdinal="1" value="Infrastructure-Mode" />
    <ValidValue enumOrdinal="2" value="Client-Mode" />
    <ValidValue enumOrdinal="3" value="Multi-Domain-Mode" />
  </ValidValues>
</Attribute>
```

1

Multi-Domain-Mode



RadiusDictionary.xml

20





a Hewlett Packard
Enterprise company

Thank you

yashavanth.n.n@hpe.com