

Solution Document for 802.1X

Switch

HFCL

Table of Contents

1.	Introduction.....	3
1.1	1.1 Purpose Of this document.....	3
2.	Purposed solution.....	3
3.	BOQ.....	3
4.	Network Topology.....	4
5.	Switch Configuration.....	5
5.1	802.1X system configuration with Guest VLAN, Auth Fail VLAN and Server Unreachable VLAN.....	5
5.2	Enable CoA in switch.....	5
5.3	802.1X Based configuration.....	6
5.4	MAC Based configuration.....	9
5.5	802.1X with MAB based configuration.....	12
6.	CPPM Configuration.....	18
6.1	Add Network Device.....	18
6.2	Profile.....	18
6.3	Policies.....	19
6.4	Services.....	22
7.	Expected and Actual Results.....	29
7.1	Successfully authentication with 802.1X based.....	29
7.2	Successfully authentication with MAC based.....	30
8.	Limitation or Pre-requisites.....	31
9.	Conclusion & Recommendation.....	31

1. Introduction

802.1X is an IEEE standard for network access control, providing authentication before a device can connect to a network. This document outlines the implementation of 802.1X authentication on network switches to enhance security and prevent unauthorized access.

1.1 Purpose Of this document

The purpose of this document is to provide a structured approach for implementing 802.1X authentication on network switches. It serves as a guideline for network administrators to ensure secure and efficient deployment of authentication mechanisms, protecting the network from unauthorized access and ensuring compliance with security policies.

2. Purposed solution

To implement a secure and efficient 802.1X authentication framework, the following approach is proposed:

- Deploy **802.1X-capable switches** as authenticators to control network access.
- Utilize a **RADIUS authentication server** to validate user credentials and enforce security policies.
- Configure **supplicant devices** (endpoints) to support 802.1X authentication using EAP (Extensible Authentication Protocol).
- Implement **VLAN assignment policies** to segregate authorized and unauthorized devices dynamically.
- Enable **fallback mechanisms** such as MAC authentication bypass (MAB) for non-802.1X-compliant devices.
- Integrate with **directory services (Active Directory, LDAP)** to streamline user authentication and policy enforcement.
- Monitor authentication logs and implement **automated alerting** for authentication failures or anomalies.

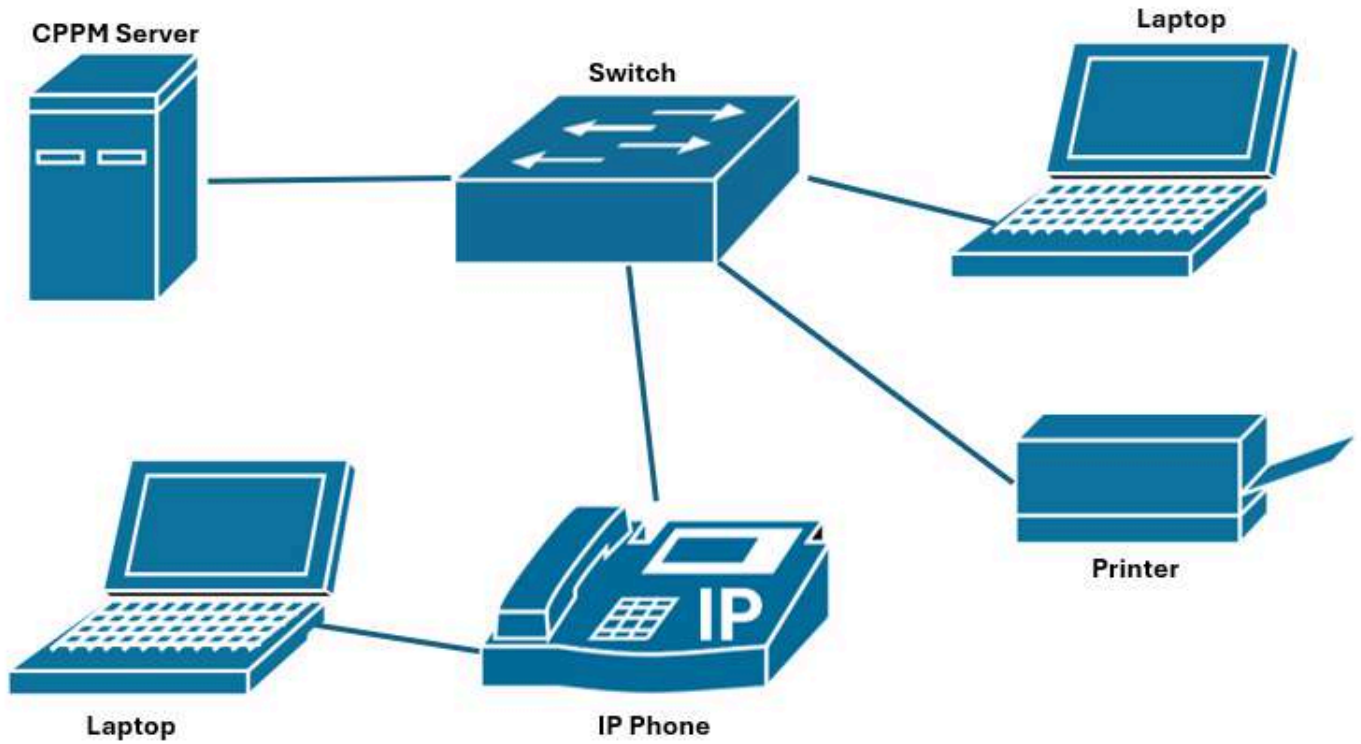
3. BOQ

HW	Software
Switch family (HSP-IO-24GE4XS-C3A+) or (HSP-IO-24GE4XS-C3PA+)	v24.01.241 or later
Aruba ClearPass (CPPM)	6.12.0.300732
Laptop	

Table 1: BOQ

4. Network Topology

802.1x Setup Diagram



5. Switch Configuration

5.1 802.1X system configuration with Guest VLAN, Auth Fail VLAN and Server Unreachable VLAN

```
dot1x authentication timer inactivity 60
dot1x system-auth-control
dot1x timeout quiet-period 35
dot1x guest-vlan 100
dot1x max-reauth-req 1
dot1x feature guest-vlan
dot1x feature authfail-vlan
dot1x authfail-vlan 150
dot1x feature svr-unreach-vlan
dot1x svr-unreach-vlan 200
```

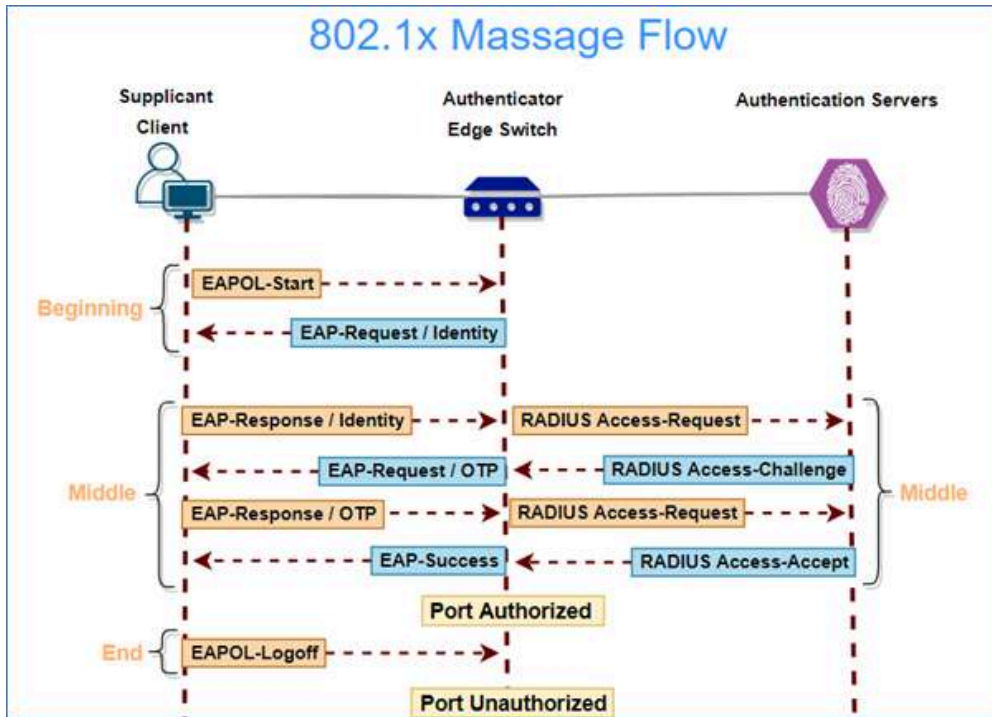
5.2 Enable CoA in switch

Configure CoA port 3799

```
RADIUS Server #1:
Host name   : 192.168.180.12
Auth port   : 1812
Acct port   : 1813
CoA port    : 3799
Timeout     : 5 seconds
Retransmit  : 3 times
```

5.3 802.1X Based configuration

Detailed call flow diagram of 802.1X-based authentication



All mandatory AVP (Attribute value pairs)

- 1: **User-Name (1)** – Identity of the user/device (e.g., username or MAC address for MAB)
- 2: **NAS-IP-Address (4)** – IP address of the authenticator (switch or wireless controller)
- 3: **NAS-Port (5)** – Physical or logical port number on which the request came in
- 4: **Called-Station-Id (30)** – MAC address of the NAS (e.g., AP or switch port)
- 5: **Calling-Station-Id (31)** – MAC address of the endpoint (user device)
- 6: **NAS-Port-Type (61)** – Type of port (e.g., Ethernet = 15, Wireless = 19)
- 7: **EAP-Message (79)** – Carries EAP payload used in 802.1X authentication
- 8: **Message-Authenticator (80)** – Ensures message integrity and security
- 9: **State (24)** – Used during multi-round authentication (e.g., EAP challenge/response)

Configure Switch port for 802.1X Based authentication

```
interface GigabitEthernet 1/5
no spanning-tree
dot1x port-control single
```

802.1X Authentication Status in switch

```
HSP-I0-24GE4XS-C3PA# show dot1x status
Interface  Admin Port State      Last Src          Last ID           QoS VLAN Guest Monitor Whitelist Fallback
-----
Gi 1/1     MAB   Down    -           -                 -                 -   -   -   Disabled Disabled Dot1X-MAB
Gi 1/2     Auth Down    -           -                 -                 -   -   -   Disabled Disabled Disabled
Gi 1/3     MAB   Down    -           -                 -                 -   -   -   Disabled Disabled Dot1X-MAB
Gi 1/4     Auth Down    -           -                 -                 -   -   -   Disabled Disabled Disabled
Gi 1/5     Sigle Auth    6c-2b-59-60-8d-c9 hfcl              -   -   -   Disabled Disabled Disabled
Gi 1/6     MAC   Down    -           -                 -                 -   -   -   Disabled Disabled Disabled
Gi 1/7     Auth Down    -           -                 -                 -   -   -   Disabled Disabled Disabled
```

Authentication status in CPPM

The screenshot shows the 'Access Tracker' page in the ClearPass Policy Manager interface. The page title is 'Access Tracker May 14, 2025 10:07:07 IST'. Below the title, there is a filter bar with '[All Requests]' selected and 'CPPMNAAC (192.168.180.12)' as the target. A date range of 'Last 1 week before Today' is also visible. A filter box shows 'Request ID' contains. The main content is a table with the following data:

#	Server Name	Source	Username	Service	Login Status	Request Timestamp	Enforcement Profiles
1.	CPPMNAAC	RADIUS	hfd	Switch_802.1x_Wired	ACCEPT	2025/05/14 10:06:04	Downloadable ACL

The screenshot shows the 'Request Details' dialog box in the ClearPass Policy Manager interface. The dialog has three tabs: 'Summary', 'Input', and 'Output'. The 'Summary' tab is active, displaying the following information:

- Login Status: ACCEPT
- Session Identifier: R00000003-01-58241db3
- Date and Time: May 14, 2025 10:06:04 IST
- End-Host Identifier: 6C-2B-59-60-8D-C9
- End-Host Profile: Generic / Dell / Unclassified Device
- End-Host Status: Unknown (with a 'Mark as Known' button)
- Username: hfd
- Access Device IP (Port): 192.168.180.170 (5)
- Access Device Name: Switch_C3PA+ (Switch_C3PA+ / Cisco)
- System Posture Status: UNKNOWN (100)

Below this information, there is a section titled 'Policies Used -' with the following details:

- Service: Switch_802.1x_Wired
- Authentication Method: EAP-PEAP
- Authentication Source: Local:localhost
- Authorization Source: [Local User Repository], Switch_Static_MAC
- Tips Role: Employee, [User Authenticated]
- Enforcement Profiles: Downloadable ACL
- Service Monitor Mode: Disabled
- Online Status: Not Available

At the bottom of the dialog, it shows 'Showing 1 of 1-303 records' and buttons for 'Change Status', 'Show Configuration', 'Export', 'Show Logs', and 'Close'. The background shows the same table as the previous screenshot, with the first row highlighted.

Packet capture

Attribute Value Pairs

- > AVP: t=Framed-MTU(12) l=6 val=1344
- > AVP: t=EAP-Message(79) l=11 Last Segment[1]
- > AVP: t=User-Name(1) l=6 val=hfcl
- > AVP: t=Service-Type(6) l=6 val=Framed(2)
- > AVP: t=NAS-Port-Type(61) l=6 val=Ethernet(15)
- > AVP: t=NAS-Port(5) l=6 val=5
- > AVP: t=NAS-Port-Id(87) l=8 val=Port 5
- > AVP: t=Calling-Station-Id(31) l=19 val=6c-2b-59-60-8d-c9
- > AVP: t=Called-Station-Id(30) l=19 val=00-06-ae-80-f4-ee
- > AVP: t=Acct-Session-Id(44) l=10 val=010000AB
- > AVP: t=NAS-IP-Address(4) l=6 val=192.168.180.170
- > AVP: t=Message-Authenticator(80) l=18 val=885a024f7e3d445624a17e4f5b13810c

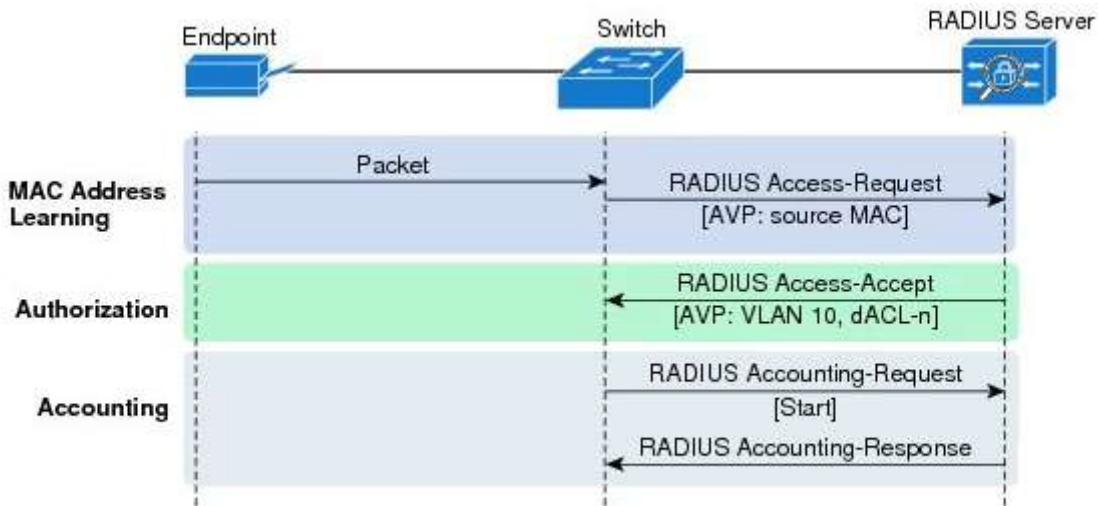


802.1X

Authentication .pca

5.4 MAC Based configuration

Detailed call flow diagram of MAC-based authentication



All mandatory AVP (Attribute value pairs)

- 1: **User-Name (1)** – Identity of the user/device (e.g., username or MAC address for MAB)
- 2: **NAS-IP-Address (4)** – IP address of the authenticator (switch or wireless controller)
- 3: **NAS-Port (5)** – Physical or logical port number on which the request came in
- 4: **Called-Station-Id (30)** – MAC address of the NAS (e.g., AP or switch port)
- 5: **Calling-Station-Id (31)** – MAC address of the endpoint (user device)
- 6: **NAS-Port-Type (61)** – Type of port (e.g., Ethernet = 15, Wireless = 19)
- 7: **EAP-Message (79)** – Carries EAP payload used in 802.1X authentication
- 8: **Message-Authenticator (80)** – Ensures message integrity and security
- 9: **State (24)** – Used during multi-round authentication (e.g., EAP challenge/response)

Configure Switch port for MAC Based authentication

```
interface GigabitEthernet 1/6
no spanning-tree
dot1x port-control mac-based
```

MAC Based Authentication Status in switch

```
HSP-I0-24GE4XS-C3PA# show dot1x status
```

Interface	Admin	Port	State	Last Src	Last ID	QoS	VLAN	Guest	Monitor	Whitelist	Fallback
Gi 1/1	MAB	Down	-	-	-	-	-	-	Disabled	Disabled	Dot1X-MAB
Gi 1/2	Auth	Down	-	-	-	-	-	-	Disabled	Disabled	Disabled
Gi 1/3	MAB	Down	-	-	-	-	-	-	Disabled	Disabled	Dot1X-MAB
Gi 1/4	Auth	Down	-	-	-	-	-	-	Disabled	Disabled	Disabled
Gi 1/5	Sigle	Down	-	-	-	-	-	-	Disabled	Disabled	Disabled
Gi 1/6	MAC	1 A/0 unA	6c-2b-59-60-8d-c9	6c-2b-59-60-8d-c9	-	-	-	-	Disabled	Disabled	Disabled
Gi 1/7	Auth	Down	-	-	-	-	-	-	Disabled	Disabled	Disabled
Gi 1/8	Auth	Down	-	-	-	-	-	-	Disabled	Disabled	Disabled

Authentication status in CPPM

The screenshot shows the 'Access Tracker' page in ClearPass Policy Manager. The page title is 'Access Tracker May 14, 2025 10:28:51 IST'. Below the title, there is a search bar with '[All Requests]' and 'CPPMNAAC (192.168.180.12)'. A filter section shows 'Request ID' contains. The main table displays the following data:

#	Server Name	Source	Username	Service	Login Status	Request Timestamp	Enforcement Profiles
1.	CPPMNAAC	RADIUS	6c-2b-59-60-8d-c9	Switch_MAC_Based	ACCEPT	2025/05/14 10:27:54	[Allow Access Profile]

The screenshot shows the 'Request Details' dialog box for the selected request. The dialog has tabs for 'Summary', 'Input', and 'Output'. The 'Summary' tab is active, showing the following details:

- Login Status: ACCEPT
- Session Identifier: R00000011-01-682422d1
- Date and Time: May 14, 2025 10:27:54 IST
- End-Host Identifier: 6C-2B-59-60-8D-C9
- End-Host Profile: Generic / Dell / Unclassified Device
- End-Host Status: Unknown (with a 'Mark as Known' link)
- Username: 6c-2b-59-60-8d-c9
- Access Device IP (Port): 192.168.180.170 (6)
- Access Device Name: Switch_C3PA+ (Switch_C3PA+ / Cisco)
- System Posture Status: UNKNOWN (100)

Below the summary, there is a section for 'Policies Used' with the following details:

- Service: Switch_MAC_Based
- Authentication Method: EAP-MD5
- Authentication Source: SHL:Switch_Static_MAC
- Authorization Source: Switch_Static_MAC
- Tips Role: [Employee], [User Authenticated]
- Enforcement Profiles: [Allow Access Profile]
- Service Monitor Mode: Disabled
- Online Status: Not Available

At the bottom of the dialog, it shows 'Showing 1 of 1-317 records' and buttons for 'Change Status', 'Show Configuration', 'Export', 'Show Logs', and 'Close'.

Packet capture

Attribute Value Pairs

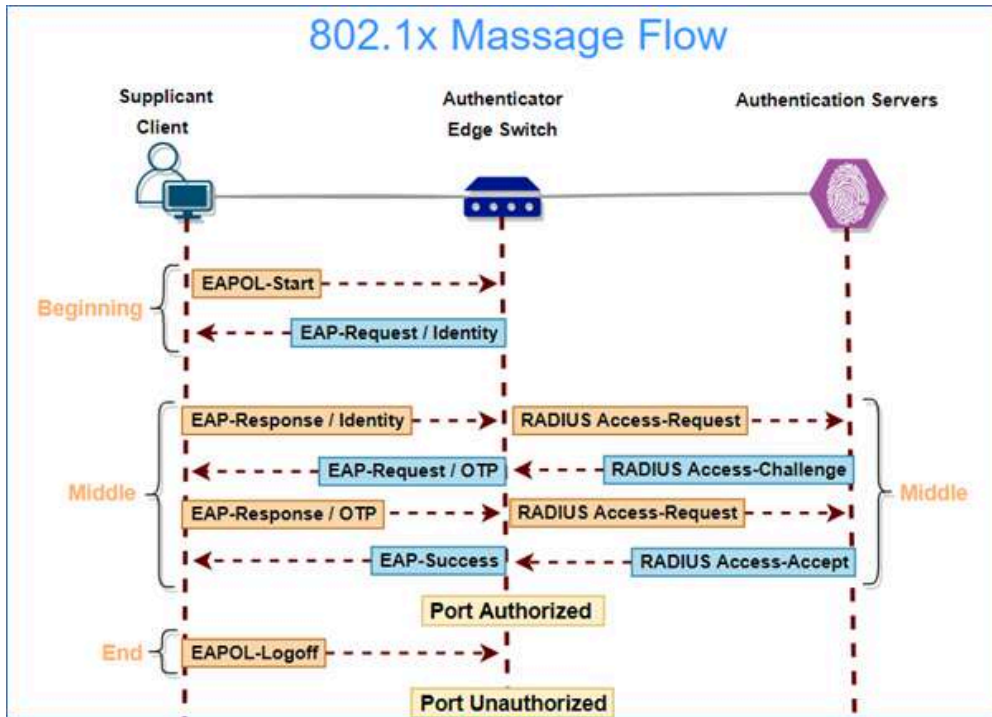
- > AVP: t=Framed-MTU(12) l=6 val=1344
- > AVP: t=EAP-Message(79) l=24 Last Segment[1]
- > AVP: t=User-Name(1) l=19 val=6c-2b-59-60-8d-c9
- > AVP: t=Service-Type(6) l=6 val=Call-Check(10)
- > AVP: t=NAS-Port-Type(61) l=6 val=Ethernet(15)
- > AVP: t=NAS-Port(5) l=6 val=6
- > AVP: t=NAS-Port-Id(87) l=8 val=Port 6
- > AVP: t=Calling-Station-Id(31) l=19 val=6c-2b-59-60-8d-c9
- > AVP: t=Called-Station-Id(30) l=19 val=00-06-ae-80-f4-ee
- > AVP: t=Acct-Session-Id(44) l=10 val=010000B0
- > AVP: t=NAS-IP-Address(4) l=6 val=192.168.180.170
- > AVP: t=Message-Authenticator(80) l=18 val=95ec79aaa2681b1d2e68d90eea6f1e8b



MAC Based
Authentication.pcap

5.5 802.1X with MAB based configuration

Detailed call flow diagram of 802.1X-based authentication



All mandatory AVP (Attribute value pairs)

- 1: **User-Name (1)** – Identity of the user/device (e.g., username or MAC address for MAB)
- 2: **NAS-IP-Address (4)** – IP address of the authenticator (switch or wireless controller)
- 3: **NAS-Port (5)** – Physical or logical port number on which the request came in
- 4: **Called-Station-Id (30)** – MAC address of the NAS (e.g., AP or switch port)
- 5: **Calling-Station-Id (31)** – MAC address of the endpoint (user device)
- 6: **NAS-Port-Type (61)** – Type of port (e.g., Ethernet = 15, Wireless = 19)
- 7: **EAP-Message (79)** – Carries EAP payload used in 802.1X authentication
- 8: **Message-Authenticator (80)** – Ensures message integrity and security
- 9: **State (24)** – Used during multi-round authentication (e.g., EAP challenge/response)

Configure Switch port for 802.1X with MAB Based authentication

```
interface GigabitEthernet 1/3
no spanning-tree
dot1x port-control mac-auth-bypass
dot1x fallback dot1x-mab
```

802.1X Authentication Status in switch

```
HSP-I0-24GE4XS-C3PA#
HSP-I0-24GE4XS-C3PA# show dot1x status
Interface  Admin Port State      Last Src          Last ID           QoS VLAN Guest Monitor Whitelist Fallback
-----
Gi 1/1    MAB    1 A/0 unA    6c-2b-59-60-8d-c9 hfc1              -   -   -   Disabled Disabled Dot1X-MAB
Gi 1/2    Auth   Down         -                 -                 -   -   -   Disabled Disabled Disabled
Gi 1/3    MAB    Down         -                 -                 -   -   -   Disabled Disabled Dot1X-MAB
Gi 1/4    Auth   Down         -                 -                 -   -   -   Disabled Disabled Disabled
Gi 1/5    Sigle Down         -                 -                 -   -   -   Disabled Disabled Disabled
```

Authentication status in CPPM

The screenshot shows the 'Access Tracker' page in ClearPass Policy Manager. The page title is 'Access Tracker May 14, 2025 10:34:40 IST'. Below the title, there is a search bar with filters for 'Request ID', 'Server Name', 'Source', 'Username', 'Service', 'Login Status', 'Request Timestamp', and 'Enforcement Profiles'. A table displays the following data:

#	Server Name	Source	Username	Service	Login Status	Request Timestamp	Enforcement Profiles
1.	CPPMNAC	RADIUS	hfd	Switch_802.1x_Wired	ACCEPT	2025/05/14 10:34:20	Downloadable ACL

The screenshot shows the 'Request Details' dialog box for the selected request. The dialog has tabs for 'Summary', 'Input', and 'Output'. The 'Summary' tab is active, displaying the following details:

- Login Status: ACCEPT
- Session Identifier: R00000013-01-68242451
- Date and Time: May 14, 2025 10:34:20 IST
- End-Host Identifier: GC-2B-59-60-6D-C9
- End-Host Profile: Generic / Dell / Unclassified Device
- End-Host Status: Unknown (Mark as Known)
- Username: hfd
- Access Device IP (Port): 192.168.180.170 (1)
- Access Device Name: Switch_C3PA+ (Switch_C3PA+ / Cisco)
- System Posture Status: UNKNOWN (100)
- Service: Switch_802.1x_Wired
- Authentication Method: EAP-PEAP,EAP-MSCHAPv2
- Authentication Source: Local:localhost
- Authorization Source: [Local User Repository], Switch_Static_MAC
- Tips Role: Employee, [User Authenticated]
- Enforcement Profiles: Downloadable ACL
- Service Monitor Mode: Disabled
- Online Status: Not Available

At the bottom of the dialog, it shows 'Showing 1 of 1-319 records' and buttons for 'Change Status', 'Show Configuration', 'Export', 'Show Logs', and 'Close'.

Packet capture

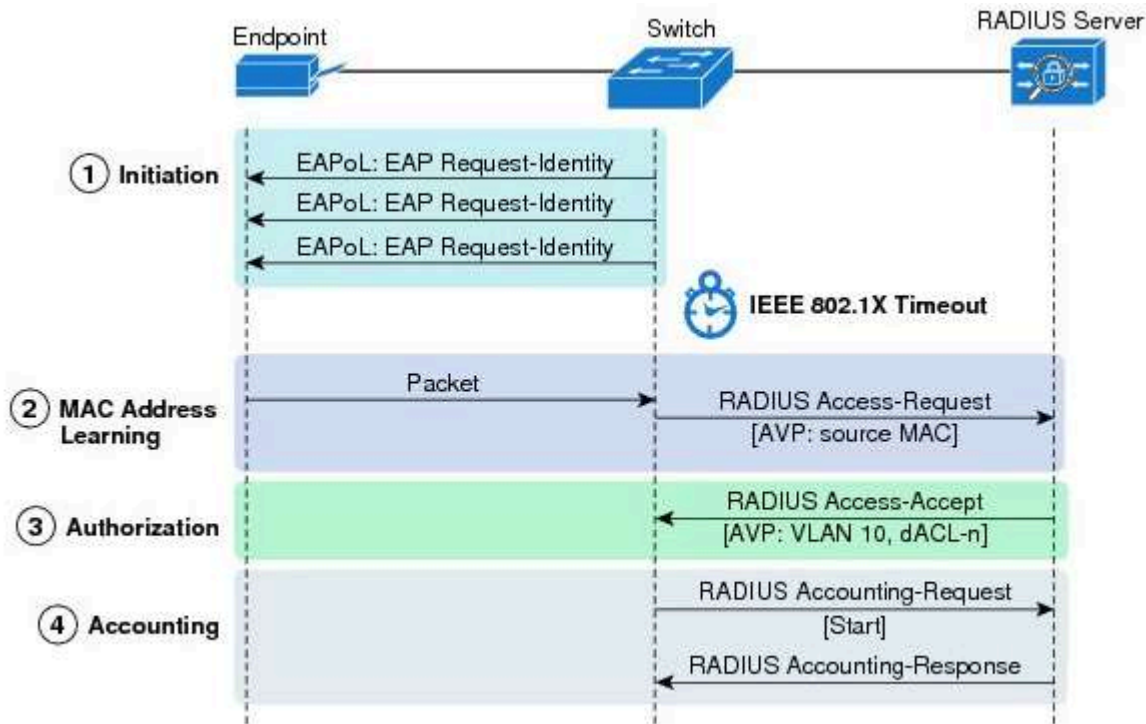
Attribute Value Pairs

- > AVP: t=Framed-MTU(12) l=6 val=1344
- > AVP: t=EAP-Message(79) l=11 Last Segment[1]
- > AVP: t=User-Name(1) l=6 val=hfcl
- > AVP: t=Service-Type(6) l=6 val=Framed(2)
- > AVP: t=NAS-Port-Type(61) l=6 val=Ethernet(15)
- > AVP: t=NAS-Port(5) l=6 val=3
- > AVP: t=NAS-Port-Id(87) l=8 val=Port 3
- > AVP: t=Calling-Station-Id(31) l=19 val=6c-2b-59-60-8d-c9
- > AVP: t=Called-Station-Id(30) l=19 val=00-06-ae-80-f4-ee
- > AVP: t=Acct-Session-Id(44) l=10 val=010000B1
- > AVP: t=NAS-IP-Address(4) l=6 val=192.168.180.170
- > AVP: t=Message-Authenticator(80) l=18 val=87bef19619d87a720666ea8a631db152



802.1X-MAB
Authentication(802.

Detailed call flow diagram of 802.1X with MAB-based authentication



All mandatory AVP (Attribute value pairs)

- 1: **User-Name (1)** – Identity of the user/device (e.g., username or MAC address for MAB)
- 2: **NAS-IP-Address (4)** – IP address of the authenticator (switch or wireless controller)
- 3: **NAS-Port (5)** – Physical or logical port number on which the request came in
- 4: **Called-Station-Id (30)** – MAC address of the NAS (e.g., AP or switch port)
- 5: **Calling-Station-Id (31)** – MAC address of the endpoint (user device)
- 6: **NAS-Port-Type (61)** – Type of port (e.g., Ethernet = 15, Wireless = 19)
- 7: **EAP-Message (79)** – Carries EAP payload used in 802.1X authentication
- 8: **Message-Authenticator (80)** – Ensures message integrity and security
- 9: **State (24)** – Used during multi-round authentication (e.g., EAP challenge/response)

MAC Based Authentication status in switch

```
HSP-IO-24GE4XS-C3PA# show dot1x status
Interface  Admin Port State      Last Src      Last ID      QoS  VLAN  Guest  Monitor  Whitelist  Fallback
-----
Gi 1/1    MAB    1 A/0 unA    6c-2b-59-60-8d-c9  6c2b59608dc9  -   -   -     Disabled Disabled Dot1X-MAB
Gi 1/2    Auth   Down         -              -              -   -   -     Disabled Disabled Disabled
Gi 1/3    MAB    Down         -              -              -   -   -     Disabled Disabled Dot1X-MAB
Gi 1/4    Auth   Down         -              -              -   -   -     Disabled Disabled Disabled
Gi 1/5    Sigle  Down         -              -              -   -   -     Disabled Disabled Disabled
```

Authentication status in CPPM

Monitoring > Live Monitoring > Access Tracker

Access Tracker May 14, 2025 10:32:45 IST Auto Refresh

The Access Tracker page provides a real-time display of per-session access activity on the selected server or domain.

[All Requests] CPPMNAAC (192.168.180.12) Last 1 week before Today Edit

Filter: Request ID contains Go Clear Filter Show 1000 records

#	Server Name	Source	Username	Service	Login Status	Request Timestamp	Enforcement Profiles
1.	CPPMNAAC	RADIUS	6c2b59608dc9	Switch_MAC_Based	ACCEPT	2025/05/14 10:31:58	[Allow Access Profile]

Request Details

Summary Input Output

Login Status: ACCEPT

Session Identifier: R00000012-01-682423c6

Date and Time: May 14, 2025 10:31:58 IST

End-Host Identifier: 6C-2B-59-60-8D-C9

End-Host Profile: Generic / Dell / Unclassified Device

End-Host Status: Unknown Mark as Known

Username: 6c2b59608dc9

Access Device IP (Port): 192.168.180.170 (1)

Access Device Name: Switch_C3PA+ (Switch_C3PA+ / Cisco)

System Posture Status: UNKNOWN (1.00)

Policies Used -

Service: Switch_MAC_Based

Authentication Method: MAC-AUTH

Authentication Source: SHL:Switch_Static_MAC

Authorization Source: Switch_Static_MAC

Tips Role: [Employee], [User Authenticated]

Enforcement Profiles: [Allow Access Profile]

Service Monitor Mode: Disabled

Online Status: Not Available

Showing 1 of 1-318 records Change Status Show Configuration Export Show Logs Close

Packet capture

▼ Attribute Value Pairs

- > AVP: t=Framed-MTU(12) l=6 val=1344
- > AVP: t=User-Name(1) l=14 val=6c2b59608dc9
- > AVP: t=User-Password(2) l=18 val=Decrypted: 6c2b59608dc9
- > AVP: t=Service-Type(6) l=6 val=Call-Check(10)
- > AVP: t=NAS-Port-Type(61) l=6 val=Ethernet(15)
- > AVP: t=NAS-Port(5) l=6 val=3
- > AVP: t=NAS-Port-Id(87) l=8 val=Port 3
- > AVP: t=Calling-Station-Id(31) l=19 val=6c-2b-59-60-8d-c9
- > AVP: t=Called-Station-Id(30) l=19 val=00-06-ae-80-f4-ee
- > AVP: t=Acct-Session-Id(44) l=10 val=010000B3
- > AVP: t=NAS-IP-Address(4) l=6 val=192.168.180.170
- > AVP: t=Message-Authenticator(80) l=18 val=7d218104192dd3723dd8bb1441bc5101



802.1X-MAB
Authentication(MAC)

6. CPPM Configuration

6.1 Add Network Device

Go to Configuration > Network > Devices

Edit Device Details ✕

Device	SNMP Read Settings	SNMP Write Settings	CLI Settings	OnConnect Enforcement	Attributes
Name:	<input type="text" value="HFCL Switch_C3A+"/>				
IP or Subnet Address:	<input type="text" value="192.168.180.109"/> <small>(e.g., 192.168.1.10 or 192.168.1.1/24 or 2001:db8:a0b:12f0::1 or 2001:db8:a0b:12f0::1/64)</small>				
Device Groups:	-				
Description:	<input style="width: 100%;" type="text" value="HFCL Switch 24 Port non-PoE"/>				
RADIUS Shared Secret:	<input type="password" value="....."/>	Verify:	<input type="password" value="....."/>		
TACACS+ Shared Secret:	<input type="text"/>	Verify:	<input type="text"/>		
Vendor Name:	<input type="text" value="Cisco"/>				
Enable RADIUS Dynamic Authorization:	<input checked="" type="checkbox"/> Port: <input type="text" value="3799"/>				
Enable RadSec:	<input type="checkbox"/>				

Copy
Save
Cancel

6.2 Profile

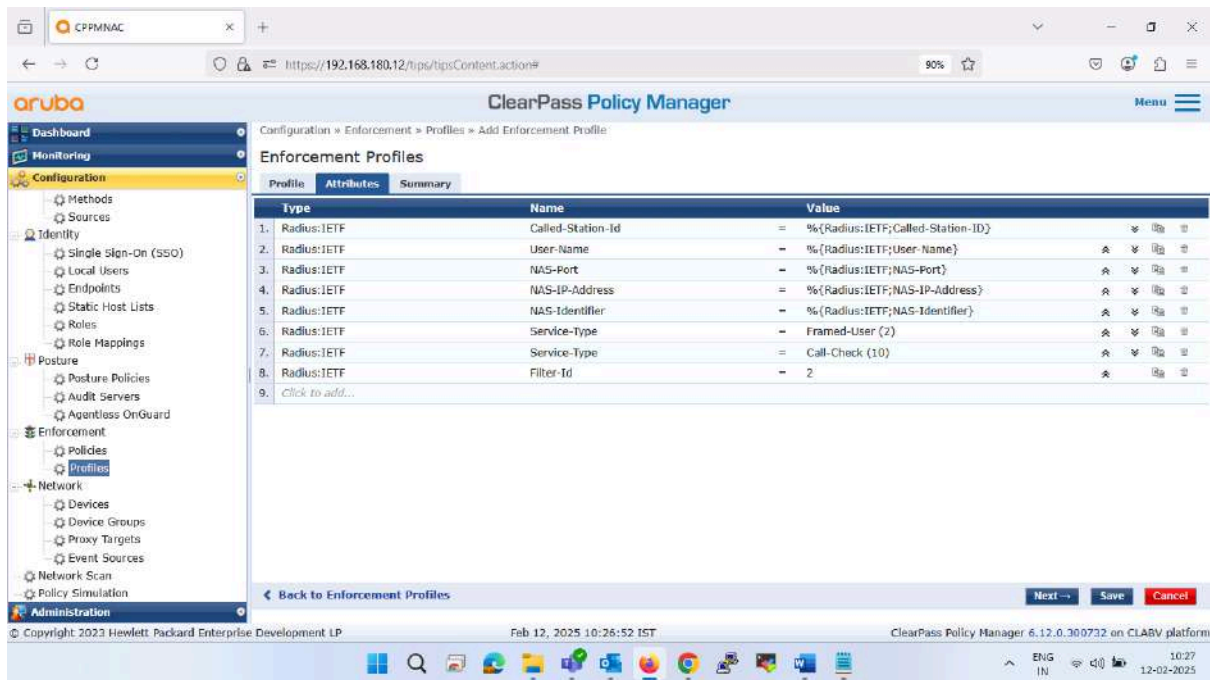
Add Enforcement profile

The screenshot shows the Aruba ClearPass Policy Manager web interface. The breadcrumb navigation is Configuration > Enforcement > Profiles > Add Enforcement Profile. The page title is 'Enforcement Profiles'. The 'Profile' tab is active, showing the following configuration details:

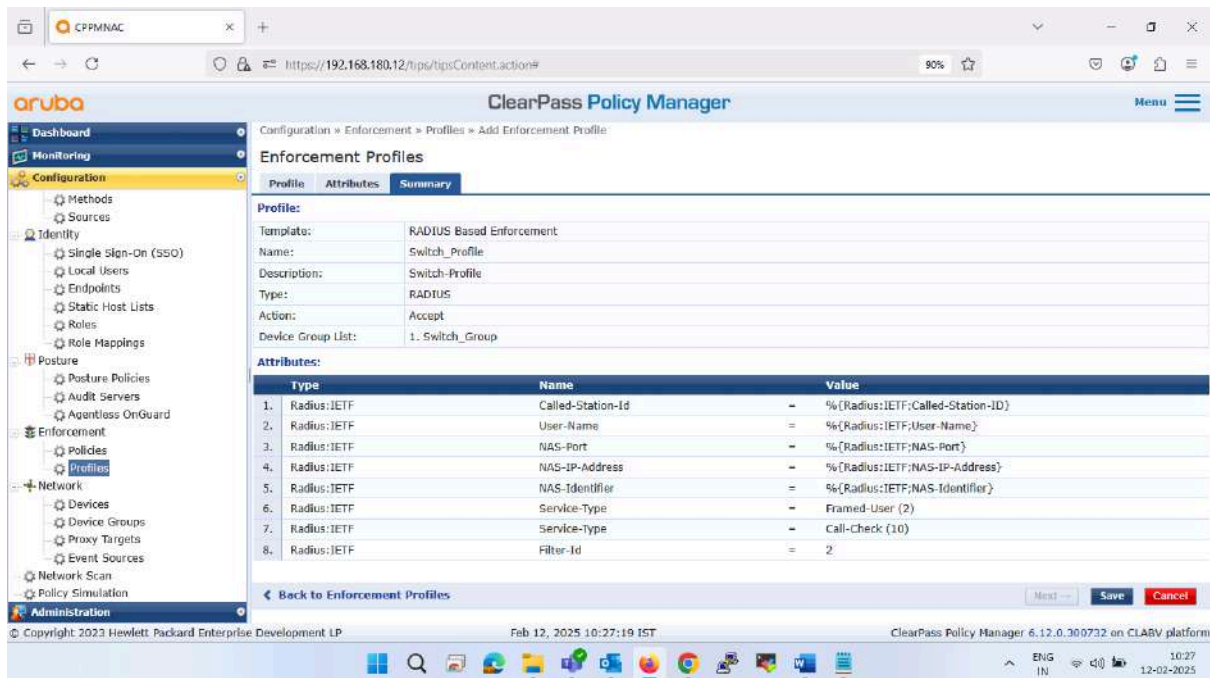
- Template: RADIUS Based Enforcement
- Name: Switch_Profile
- Description: Switch_Profile
- Type: RADIUS
- Action: Accept Reject Drop
- Device Group List: (with buttons for Remove, View Details, and Modify) and a dropdown menu set to --Select--.

At the bottom of the configuration area, there are buttons for 'Back to Enforcement Profiles', 'Next', 'Save', and 'Cancel'. The footer of the browser window shows the date and time as Feb 12, 2025 10:21:17 IST and the version as ClearPass Policy Manager 6.12.0.300732 on CLABV platform.

Add Attributes

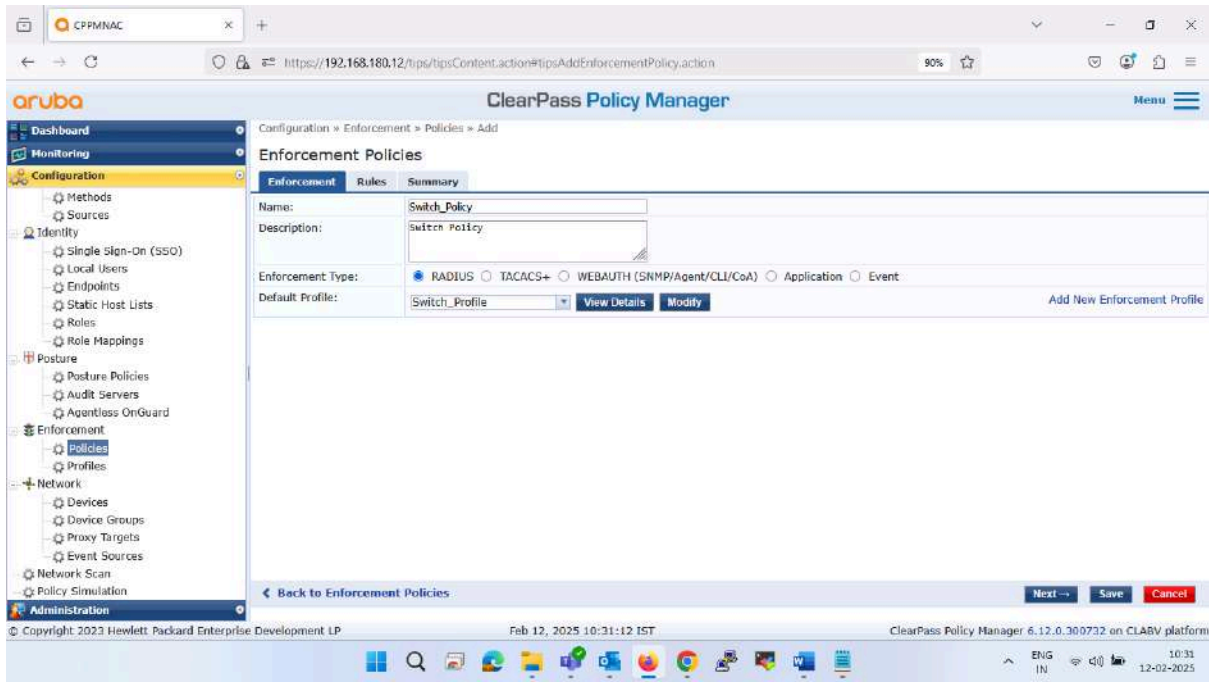


All configured parameters are showing in summary

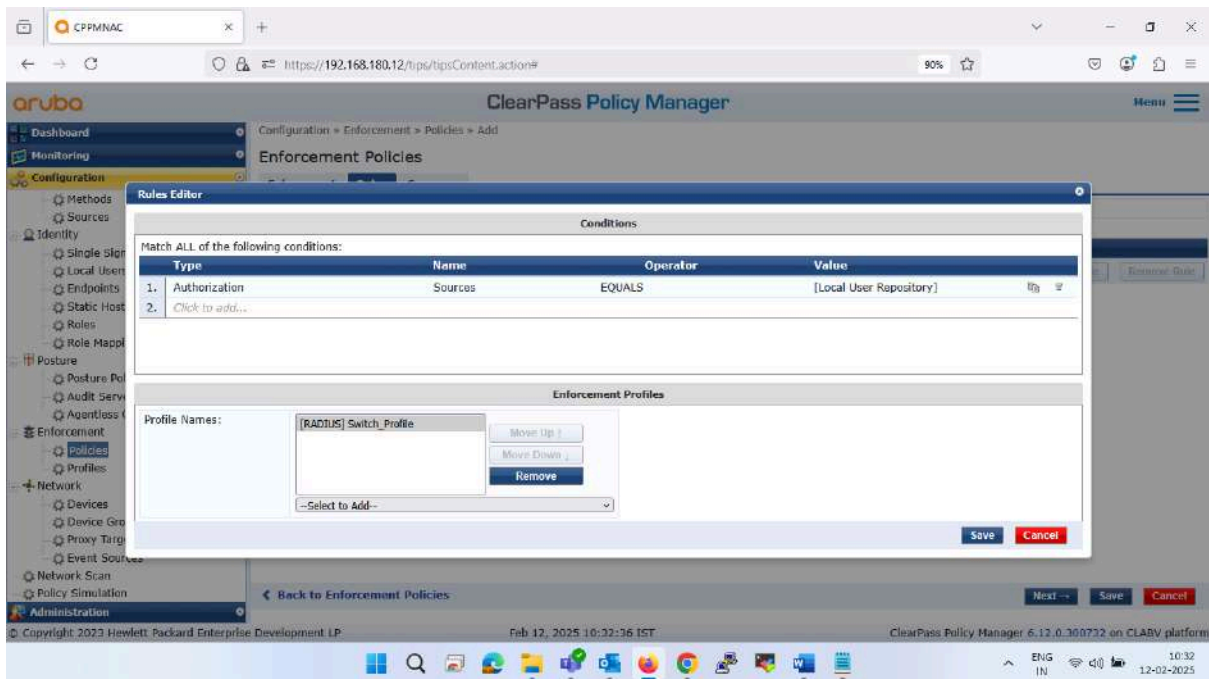


6.3 Policies

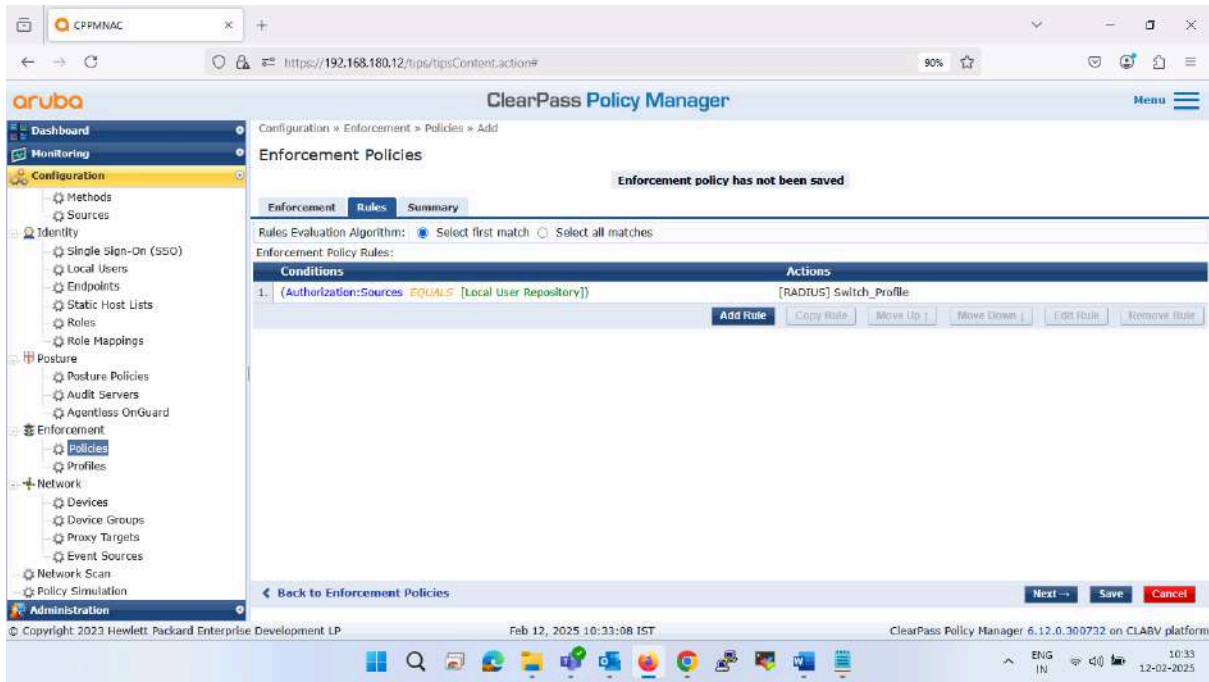
Add Enforcement policies



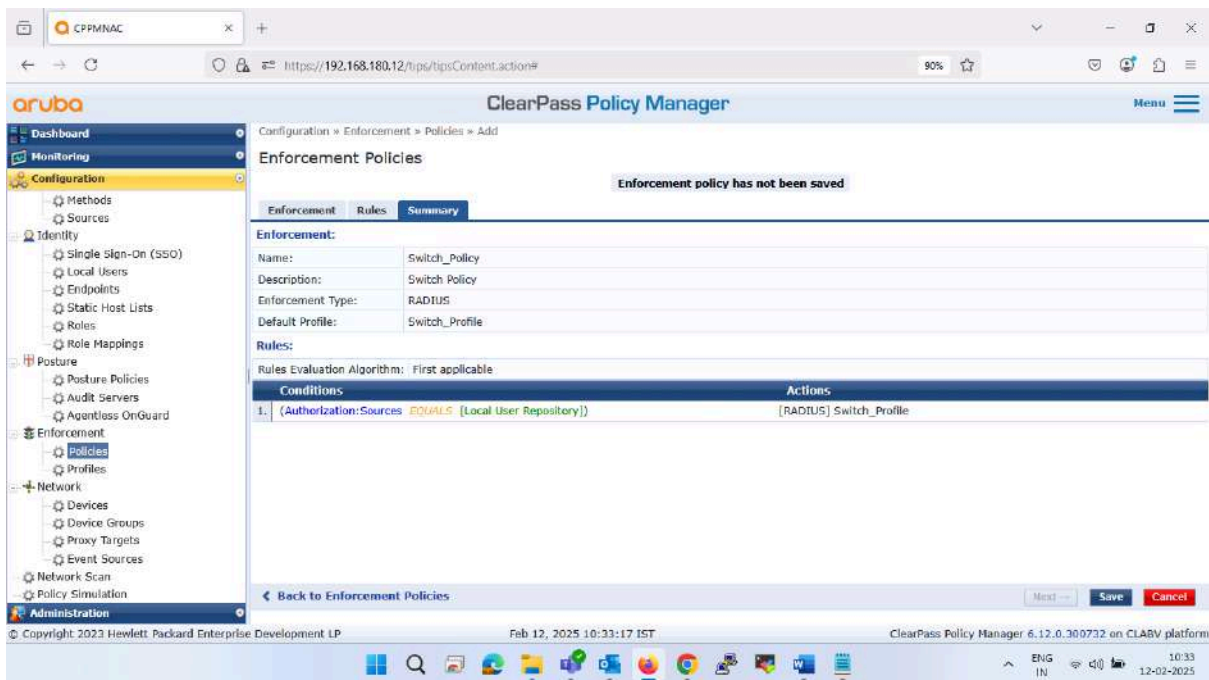
Now Add rules and select created profile



Rule Shown as per below screenshot after created

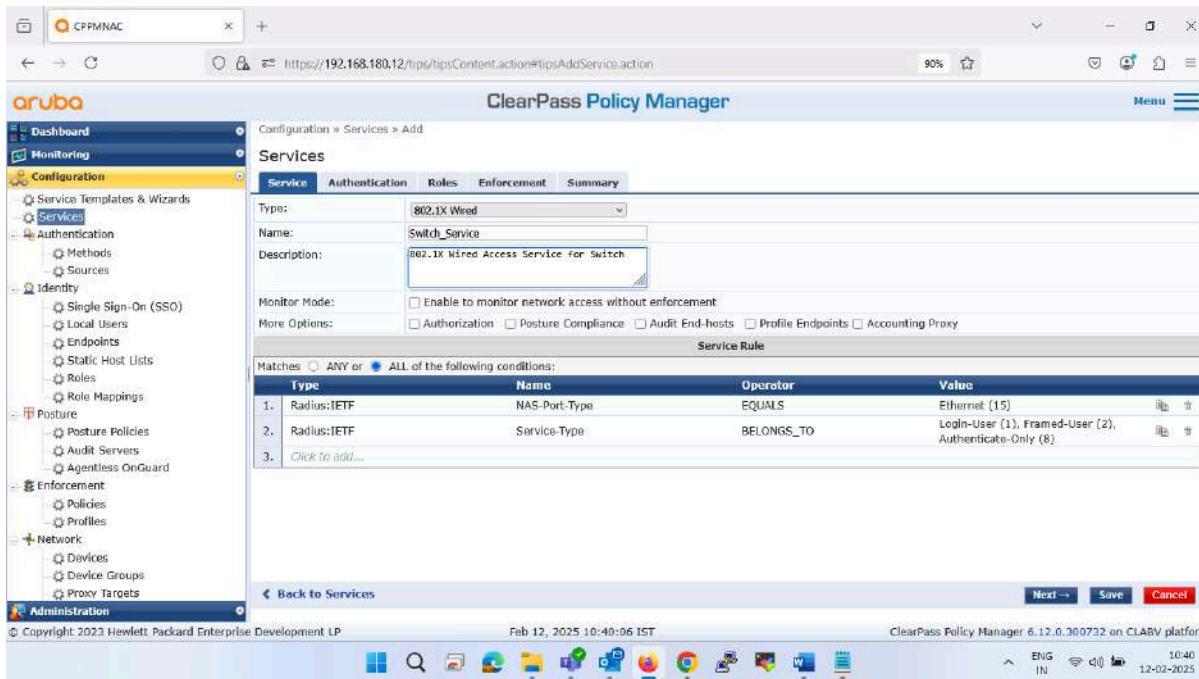


Configured parameters are shown in policies

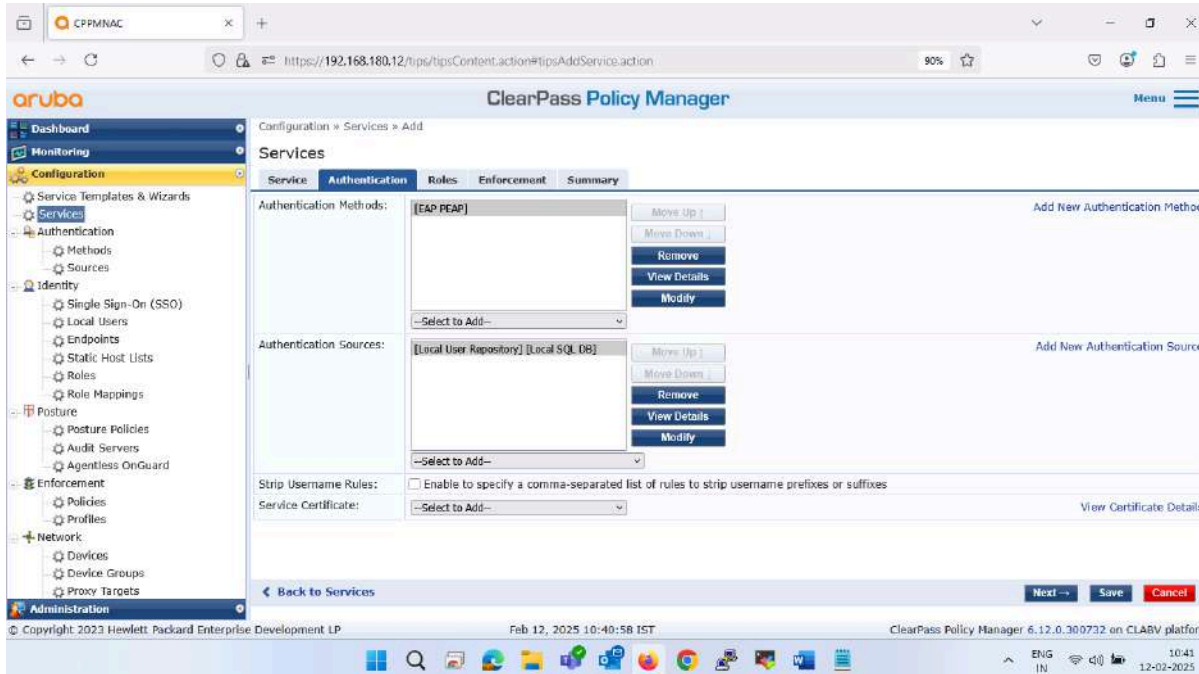


6.4 Services

Add Service



Add Authentication method and Authentication source



Click on Add New Role Mapping Policy

The screenshot shows the ClearPass Policy Manager interface. The breadcrumb trail is 'Configuration > Services > Add'. The 'Services' section is active, with sub-tabs for 'Service', 'Authentication', 'Roles', 'Enforcement', and 'Summary'. The 'Roles' tab is selected, showing a 'Role Mapping Policy' dropdown set to '--Select--' and a 'Modify' button. Below this is the 'Role Mapping Policy Details' section with fields for 'Description', 'Default Role', and 'Rules Evaluation Algorithm', all currently empty. A table with columns 'Conditions' and 'Role' is visible below. At the bottom, there are 'Back to Services', 'Next', 'Save', and 'Cancel' buttons. The footer shows 'Copyright 2023 Hewlett Packard Enterprise Development LP', the date 'Feb 12, 2025 10:41:45 IST', and the version 'ClearPass Policy Manager 6.12.0.300732 on CLABV platform'.

The screenshot shows the ClearPass Policy Manager interface. The breadcrumb trail is 'Configuration > Identity > Role Mappings > Add'. The 'Role Mappings' section is active, with sub-tabs for 'Policy', 'Mapping Rules', and 'Summary'. The 'Policy' tab is selected, showing a 'Policy Name' field with the value 'Switch_Policy', a 'Description' field with the value 'Switch Policy', and a 'Default Role' dropdown set to '[Employee]'. There are 'View Details' and 'Modify' buttons next to the dropdown. An 'Add New Role' link is also present. At the bottom, there are 'Back to Services', 'Next', 'Save', and 'Cancel' buttons. The footer shows 'Copyright 2023 Hewlett Packard Enterprise Development LP', the date 'Feb 12, 2025 10:43:09 IST', and the version 'ClearPass Policy Manager 6.12.0.300732 on CLABV platform'.

The screenshot shows the Aruba ClearPass Policy Manager interface. The main page is titled "Role Mappings" and is in the "Add" configuration mode. A "Rules Editor" dialog box is open, showing a table of conditions. The table has columns for "Type", "Name", "Operator", and "Value". The first row shows "Authorization" for "Sources" with the operator "EQUALS" and the value "[Local User Repository]". The second row is a placeholder "Click to add...". Below the conditions table, the "Role Name" is set to "[Employee]". The dialog has "Save" and "Cancel" buttons.

Type	Name	Operator	Value
1. Authorization	Sources	EQUALS	[Local User Repository]
2. Click to add...			

The screenshot shows the "Summary" tab of the "Role Mappings" configuration page. A message at the top states "Role mapping policy has not been saved". The "Policy" section shows "Policy Name: Switch_Policy", "Description: Switch Policy", and "Default Role: [Employee]". The "Mapping Rules" section shows "Rules Evaluation Algorithm: First applicable". Below this is a table of conditions and role names.

Conditions	Role Name
1. [Authorization:Sources EQUALS [Local User Repository]]	[Employee]

The screenshot shows the ClearPass Policy Manager interface. The left sidebar contains a navigation menu with categories like Dashboard, Monitoring, Configuration, Authentication, Identity, Posture, Enforcement, Network, and Administration. The main content area is titled 'Services' and shows a configuration page for a 'Role mapping policy "Switch_Policy" added'. The 'Roles' tab is selected, displaying a table with columns for 'Conditions' and 'Role'. A single rule is listed: 1. (Authorization:Sources EQUALS [Local User Repository]) [Employee]. At the bottom, there are 'Next', 'Save', and 'Cancel' buttons.

Click on Add New Enforcement Policy

The screenshot shows the ClearPass Policy Manager interface with the 'Enforcement' tab selected. The main content area is titled 'Services' and shows a configuration page for an 'Enforcement Policy'. The 'Enforcement Policy' dropdown is set to '[Sample Allow Access Policy]'. The 'Enforcement Policy Details' section includes fields for Description, Default Profile, and Rules Evaluation Algorithm. Below this is a table with columns for 'Conditions' and 'Enforcement Profiles'. A single rule is listed: 1. (Date:Day-of-Week #BELOW\$\$_Y0 Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, Sunday) [Allow Access Profile]. At the bottom, there are 'Next', 'Save', and 'Cancel' buttons.

The screenshot shows the 'ClearPass Policy Manager' interface. The left sidebar contains a navigation menu with categories like Dashboard, Monitoring, Configuration, Authentication, Identity, Posture, Enforcement, and Network. The main content area is titled 'Enforcement Policies' and has tabs for 'Enforcement', 'Rules', and 'Summary'. The 'Enforcement' tab is active, showing a form for a policy named 'Switch_Policy'. The 'Description' field contains 'Switch Policy'. Under 'Enforcement Type', the 'RADIUS' radio button is selected. The 'Default Profile' is set to 'Switch_Profile'. At the bottom of the form, there are 'View Details' and 'Modify' buttons. Below the form, there are 'Back to Services', 'Next', 'Save', and 'Cancel' buttons. The footer of the browser window shows the date 'Feb 12, 2025 10:45:56 IST' and the version 'ClearPass Policy Manager 6.12.0.300732 on CLABV platform'.

The screenshot shows the 'Rules Editor' dialog box overlaid on the 'Enforcement Policies' configuration page. The dialog has a 'Conditions' section with the instruction 'Match ALL of the following conditions:'. Below this is a table with the following data:

Type	Name	Operator	Value
1. Authorization	Sources	EQUALS	[Local User Repository]
2.	Click to add...		

Below the conditions table is the 'Enforcement Profiles' section. It contains a list box with the entry '[RADIUS] Switch_Profile'. To the right of the list box are three buttons: 'Move Up', 'Move Down', and 'Remove'. Below the list box is a dropdown menu with the text '--Select to Add--'. At the bottom right of the dialog are 'Save' and 'Cancel' buttons. The background shows the same 'Enforcement Policies' configuration page as the first screenshot, but dimmed.

The screenshot shows the 'Enforcement Policies' configuration page in the Aruba ClearPass Policy Manager. The breadcrumb trail is 'Configuration > Enforcement > Policies > Add'. A message at the top states 'Enforcement policy has not been saved'. The page has three tabs: 'Enforcement', 'Rules', and 'Summary', with 'Summary' selected. The 'Enforcement' section contains the following fields:

- Name: Switch_Policy
- Description: Switch Policy
- Enforcement Type: RADIUS
- Default Profile: Switch_Profile

The 'Rules' section shows a 'Rules Evaluation Algorithm' of 'First applicable'. Below this is a table with two columns: 'Conditions' and 'Actions'.

Conditions	Actions
1. (Authorization:Sources EQUALS [Local User Repository])	[RADIUS] Switch_Profile

At the bottom, there is a 'Back to Services' link and 'Next', 'Save', and 'Cancel' buttons. The footer includes 'Copyright 2023 Hewlett Packard Enterprise Development LP', the date 'Feb 12, 2025 10:46:41 IST', and the version 'ClearPass Policy Manager 6.12.0.300732 on CLABV platform'.

The screenshot shows the 'Services' configuration page in the Aruba ClearPass Policy Manager. The breadcrumb trail is 'Configuration > Services > Add'. The page has five tabs: 'Service', 'Authentication', 'Roles', 'Enforcement', and 'Summary', with 'Enforcement' selected. The 'Enforcement' section contains the following fields:

- Use Cached Results: Use cached Roles and Posture attributes from previous sessions
- Enforcement Policy: Switch_Policy (with a 'Modify' button)

Below these fields is an 'Add New Enforcement Policy' link. The 'Enforcement Policy Details' section contains the following fields:

- Description: Switch Policy
- Default Profile: Switch_Profile
- Rules Evaluation Algorithm: first-applicable

The 'Enforcement Profiles' section shows a table with two columns: 'Conditions' and 'Enforcement Profiles'.

Conditions	Enforcement Profiles
1. (Authorization:Sources EQUALS [Local User Repository])	Switch_Profile

At the bottom, there is a 'Back to Services' link and 'Next', 'Save', and 'Cancel' buttons. The footer includes 'Copyright 2023 Hewlett Packard Enterprise Development LP', the date 'Feb 12, 2025 10:47:52 IST', and the version 'ClearPass Policy Manager 6.12.0.300732 on CLABV platform'.

The screenshot shows the Aruba ClearPass Policy Manager web interface. The left sidebar contains a navigation menu with categories like Dashboard, Monitoring, Configuration, Authentication, Identity, Posture, Enforcement, and Network. The main content area is titled 'Services' and shows configuration details for a service named 'Switch_Service'. The 'Summary' tab is active, displaying the following information:

- Service:**
 - Type: 802.1X Wired
 - Name: Switch_Service
 - Description: 802.1X Wired Access Service for Switch
 - Monitor Mode: Disabled
 - More Options: -
- Service Rule:**

Match ALL of the following conditions:

Type	Name	Operator	Value
1. Radius:IETF	NAS-Port-Type	EQUALS	Ethernet (15)
2. Radius:IETF	Service-Type	BELONGS_TO	Login-User (1), Framed-User (2), Authenticate-Only (8)
- Authentication:**
 - Authentication Methods: [EAP PEAP]
 - Authentication Sources: [Local User Repository] [Local SQL DB]
 - Strip Username Rules: -
 - Service Certificate: -

At the bottom of the configuration area, there are buttons for 'Back to Services', 'Next', 'Save', and 'Cancel'. The footer of the browser window shows the date 'Feb 12, 2025 10:47:59 IST' and the version 'ClearPass Policy Manager 6.12.0.300732 on CLABV platform'.

This screenshot shows the same Aruba ClearPass Policy Manager interface, but with the 'Roles' and 'Enforcement' tabs visible. The configuration details are as follows:

- Monitor Mode:** Disabled
- More Options:** -
- Service Rule:**

Match ALL of the following conditions:

Type	Name	Operator	Value
1. Radius:IETF	NAS-Port-Type	EQUALS	Ethernet (15)
2. Radius:IETF	Service-Type	BELONGS_TO	Login-User (1), Framed-User (2), Authenticate-Only (8)
- Authentication:**
 - Authentication Methods: [EAP PEAP]
 - Authentication Sources: [Local User Repository] [Local SQL DB]
 - Strip Username Rules: -
 - Service Certificate: -
- Roles:**
 - Role Mapping Policy: Switch_Policy
- Enforcement:**
 - Use Cached Results: Enabled
 - Enforcement Policy: Switch_Policy

The 'Back to Services', 'Next', 'Save', and 'Cancel' buttons are also present at the bottom. The footer shows the date 'Feb 12, 2025 10:48:05 IST' and the version 'ClearPass Policy Manager 6.12.0.300732 on CLABV platform'.

7. Expected and Actual Results

As per the expected results, 802.1X authentication functioned as expected across all test cases—EAPOL exchange, RADIUS communication, VLAN assignment, fallback to MAB, and reauthentication were successfully verified with no discrepancies observed.

7.1 Successfully authentication with 802.1X based

The screenshot shows the ClearPass Policy Manager interface. The 'Access Tracker' page displays a real-time display of per-session access activity. The selected server is CPPMNC (192.168.180.12) and the time range is 'Last 1 week before Today'. A table of requests is shown below.

#	Server Name	Source	Username	Service	Login Status	Request Timestamp	Enforcement Profiles
1.	CPPMNC	RADIUS	hfd	Switch_802.1x_Wired	ACCEPT	2025/05/14 10:34:20	Downloadable ACL

The screenshot shows the 'Request Details' dialog box for the selected request. The 'Summary' tab is active, displaying the following information:

- Login Status: ACCEPT
- Session Identifier: R00000013-01-68242451
- Date and Time: May 14, 2025 10:34:20 IST
- End-Host Identifier: GC-2B-59-60-6D-C9
- End-Host Profile: Generic / Dell / Unclassified Device
- End-Host Status: Unknown (Mark as Known)
- Username: hfd
- Access Device IP (Port): 192.168.180.170 (1)
- Access Device Name: Switch_C3PA+ (Switch_C3PA+ / Cisco)
- System Posture Status: UNKNOWN (100)
- Service: Switch_802.1x_Wired
- Authentication Method: EAP-PEAP, EAP-MSCHAPv2
- Authentication Source: Local:localhost
- Authorization Source: [Local User Repository], Switch_Static_MAC
- Tips Role: Employee, [User Authenticated]
- Enforcement Profiles: Downloadable ACL
- Service Monitor Mode: Disabled
- Online Status: Not Available

The background shows a list of requests with the selected request highlighted in yellow.

7.2 Successfully authentication with MAC based

Monitoring » Live Monitoring » Access Tracker

Access Tracker May 14, 2025 10:32:45 IST Auto Refresh

The Access Tracker page provides a real-time display of per-session access activity on the selected server or domain.

[All Requests] CPMNAC (192.168.180.12) Last 1 week before Today Edit

Filter: Request ID contains Go Clear Filter Show 1000 records

#	Server Name	Source	Username	Service	Login Status	Request Timestamp	Enforcement Profiles
1.	CPMNAAC	RADIUS	6c2b59608dc9	Switch_MAC_Based	ACCEPT	2025/05/14 10:31:58	[Allow Access Profile]

Request Details

Summary	Input	Output
Login Status:		ACCEPT
Session Identifier:		R00000012-01-682423c6
Date and Time:		May 14, 2025 10:31:58 IST
End-Host Identifier:		6C-2B-59-60-8D-C9
End-Host Profile:		Generic / Dell / Unclassified Device
End-Host Status:		Unknown Mark as Known
Username:		6c2b59608dc9
Access Device IP (Port):		192.168.180.170 (1)
Access Device Name:		Switch_C3PA+ (Switch_C3PA+ / Cisco)
System Posture Status:		UNKNOWN (100)
Policies Used -		
Service:		Switch_MAC_Based
Authentication Method:		MAC-AUTH
Authentication Source:		SHL:Switch_Static_MAC
Authorization Source:		Switch_Static_MAC
Tips Role:		[Employee], [User Authenticated]
Enforcement Profiles:		[Allow Access Profile]
Service Monitor Mode:		Disabled
Online Status:		Not Available

Showing 1 of 1-318 records Change Status Show Configuration Export Show Logs Close

#	Request Timestamp	Enforcement Profiles
1.	2025/05/14 10:31:58	[Allow Access Profile]
2.	2025/05/14 10:27:54	[Allow Access Profile]
3.	2025/05/14 10:26:22	[Deny Access Profile]
4.	2025/05/14 10:24:36	[Deny Access Profile]
5.	2025/05/14 10:22:50	[Deny Access Profile]
6.	2025/05/14 10:21:20	[Deny Access Profile]
7.	2025/05/14 10:19:34	[Deny Access Profile]
8.	2025/05/14 10:19:07	[Deny Access Profile]
9.	2025/05/14 10:17:16	[Deny Access Profile]
10.	2025/05/14 10:16:34	[Deny Access Profile]
11.	2025/05/14 10:16:12	[Deny Access Profile]
12.	2025/05/14 10:14:32	[Deny Access Profile]
13.	2025/05/14 10:12:47	[Deny Access Profile]
14.	2025/05/14 10:11:03	[Deny Access Profile]
15.	2025/05/14 10:09:10	[Deny Access Profile]

Copyright 2023 Hewlett Packard Enterprise Development LP May 14, 2025 10:33:15 IST ClearPass Policy Manager 6.12.0.300732 on CLARV platform

8. Limitation or Pre-requisites

802.1X requires compatible supplicant devices, a properly configured RADIUS server, switch support, and fallback mechanisms like MAB for non-802.1X devices; network access is restricted until authentication succeeds.

9. Conclusion & Recommendation

802.1X authentication effectively enhances network security by ensuring only authorized devices gain access. It performed reliably across test scenarios, including EAP authentication, VLAN assignment, and MAB fallback. For production deployment, it is recommended to ensure proper supplicant configuration, RADIUS redundancy, and robust fallback policies like guest VLAN or fail-open to accommodate non-802.1X endpoints.

Copyright Notice

This document is copyright of HFCL Limited, All Rights Reserved. No part of this document, in whole or in part, may be used, reproduced, stored in a retrieval system, or transmitted, in any form, or by any means, electronic or otherwise, including photocopying, reprinting, or recording, for any purpose, without the express written permission of HFCL Limited.

Legal Disclaimer

The information contained in this document is subject to change without notice. The information in this document is provided for informational purposes only. HFCL Limited specifically disclaims all warranties, express or limited, including, but not limited, to the implied warranties of merchantability and fitness for a particular purpose, except as provided for in a separate software license agreement.

About HFCL Limited

HFCL is a leading technology company specializing in creating digital networks for telcos, enterprises, and governments. Over the years, HFCL has emerged as a trusted partner offering sustainable high-tech solutions with a commitment to provide the latest technology products to its customers. Our strong R&D expertise coupled with our global system integration services and decades of experience in fibre optics enable us to deliver innovative digital network solutions required for the most advanced networks.

The Company's in-house R&D Centers located at Gurgaon & Bengaluru along with invested R&D Houses and other R&D collaborators at different locations in India and abroad, innovate a futuristic range of technology products and solutions. HFCL has developed capabilities to provide premium quality Optical Fiber and Optical Fiber Cables, state-of-the-art telecom products including 5G Radio Access Network (RAN) products, 5G Transport Products, WiFi Systems (WiFi 6, WiFi 7), Unlicensed Band Radios, Switches, Routers and Software Defined Radios.

The Company has state-of-the-art Optical Fiber and Optical Fiber Cable manufacturing plants at Hyderabad, Optical Fiber Cable manufacturing plant in Goa and in its subsidiary HTL Limited at Chennai.

We are a partner of choice for our customers across India, Europe, Asia Pacific, Middle East, Africa, and USA. Our commitment to quality and environmental sustainability inspires us to innovate solutions for the ever-evolving customer needs.

Correspondence

HFCL Limited
8, Commercial Complex,
Masjid Moth, Greater Kailash II, New
Delhi-110048, India Tel: +91-11-
30882624/2626

Mail us at:Sales: iosales@hfcl.comEnquiry: ioenquiry@hfcl.comSupport: iosupport@hfcl.com

Toll Free (Domestic): 8792701100

Revision History

Date	Rev No.	Description	Owner
04/06/2025	A0-00	Initial Draft Release	HFCL
	A0-01		HFCL
	A0-02		HFCL
	A0-03		HFCL