Solution Document for 802.1X

Switch

HFCL

Table of Contents

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 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:

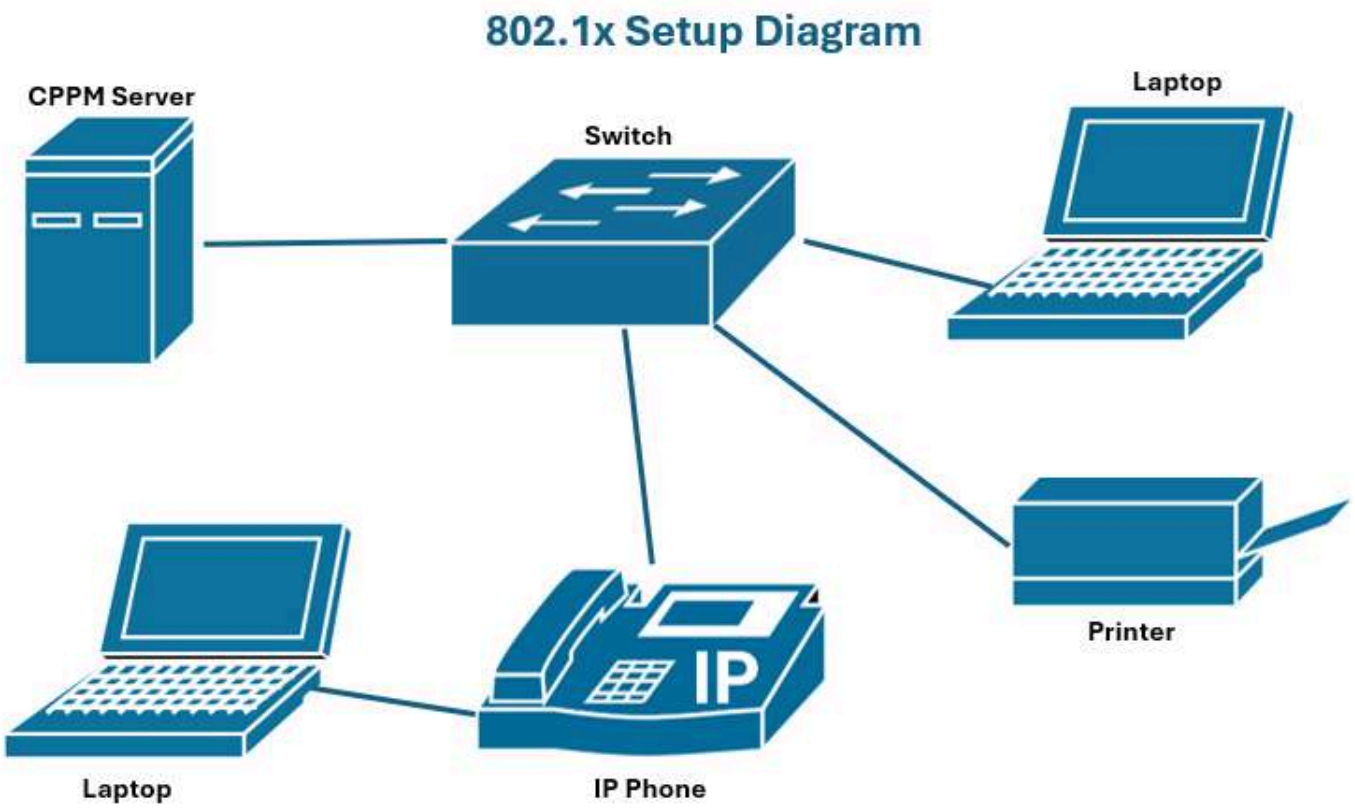
- Deploy **802.1X-capable switches** as authenticators to control network access.
- Utilize a **RADIUS authentication server** to validate user credentials and enforce security policies.
- Configure **supplicant devices** (endpoints) to support 802.1X authentication using EAP (Extensible Authentication 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



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
!
```

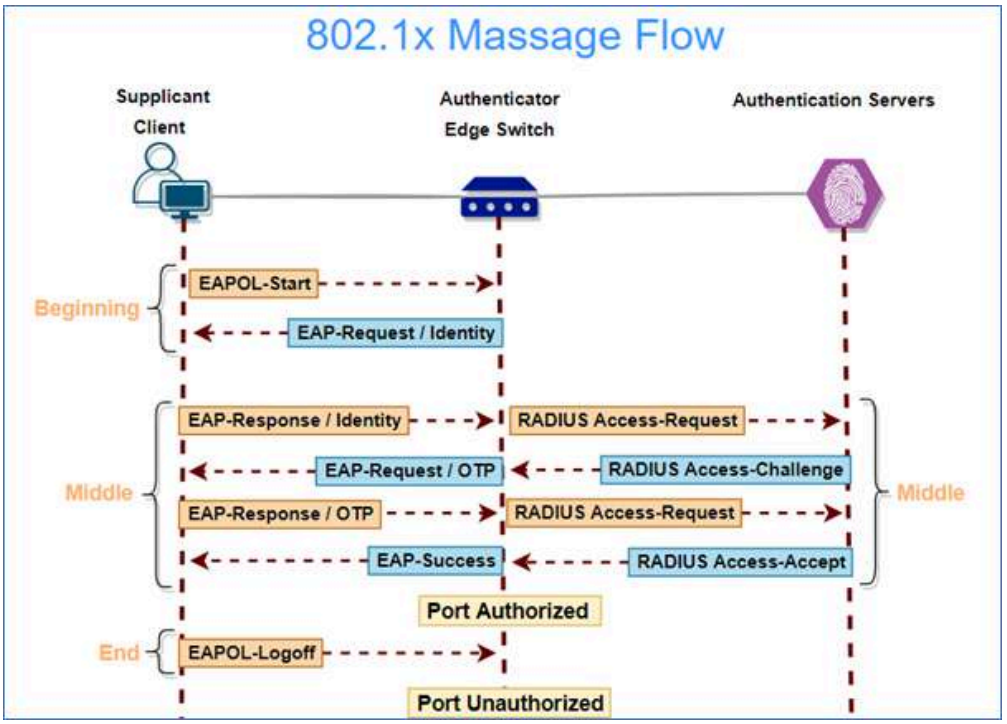
5.2 Enable CoA in switch

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)

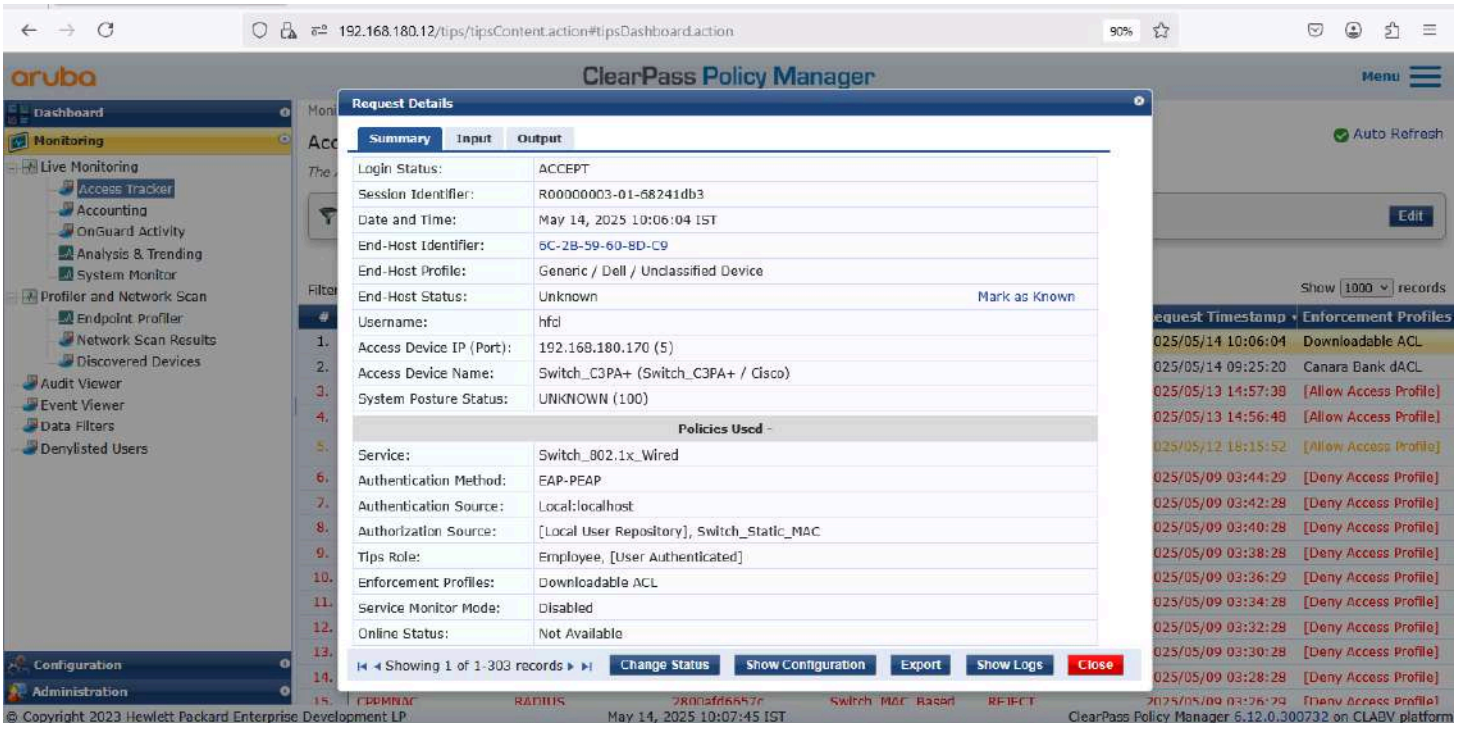
Configure Switch port for 802.1X Based authentication

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

802.1X Authentication Status in switch

```
HSP-IO-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



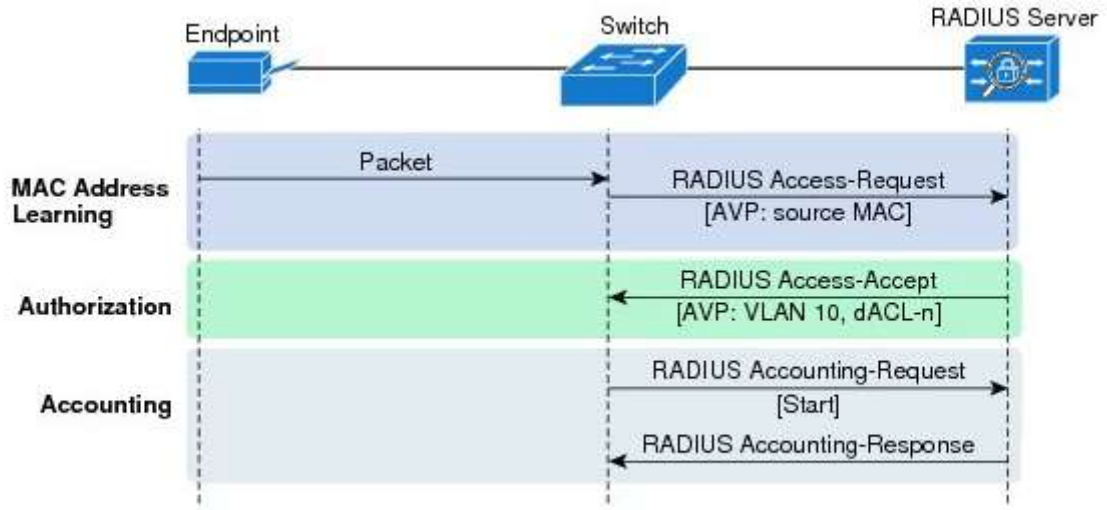
Packet capture

```
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)

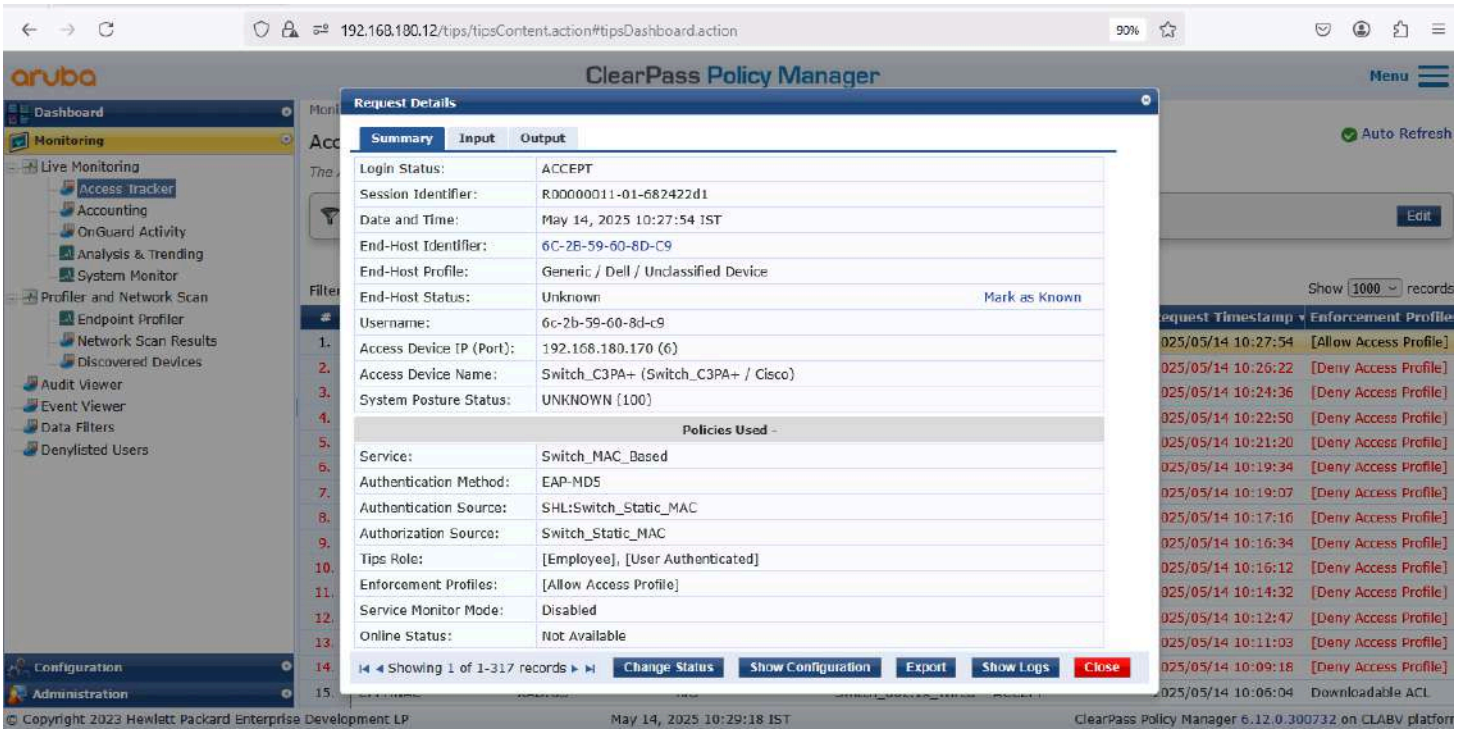
Configure Switch port for MAC Based authentication

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

MAC Based Authentication Status in switch

```
HSP-IO-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



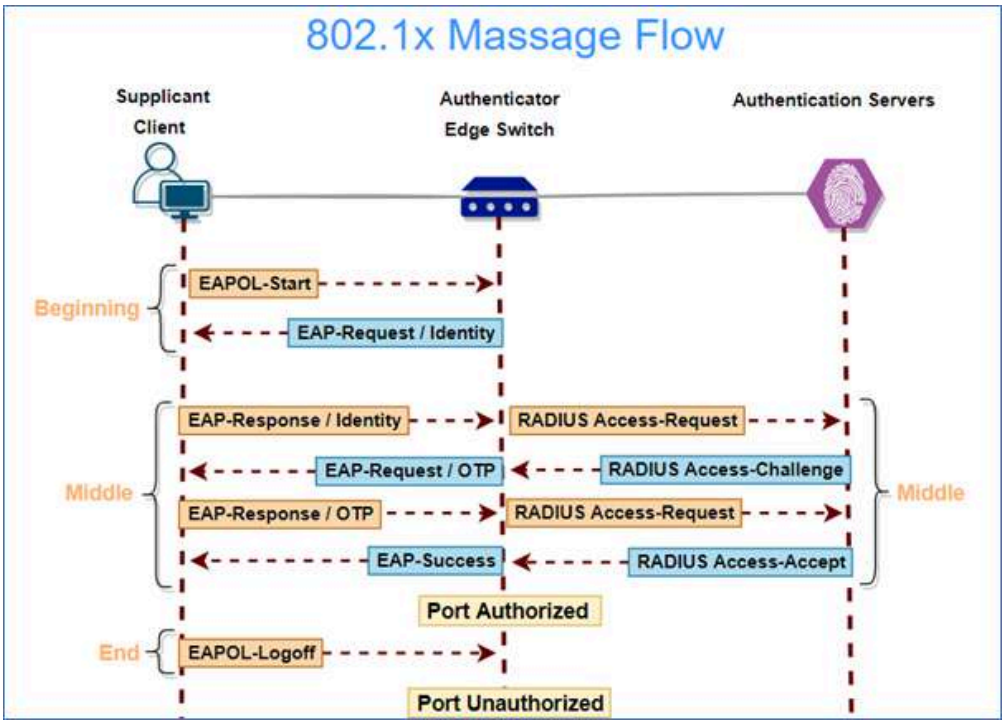
Packet capture

```
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)

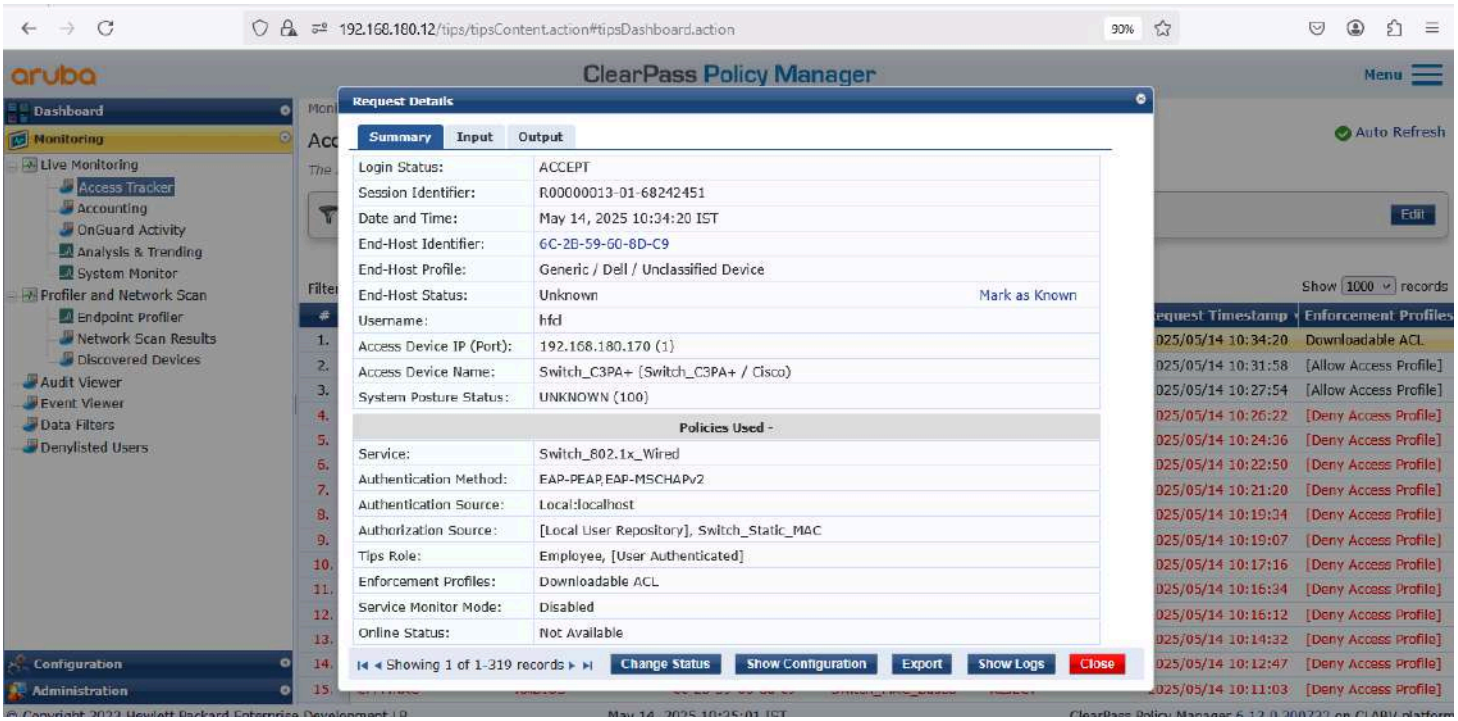
Configure Switch port for 802.1X with MAB Based authentication

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

802.1X Authentication Status in switch

```
HSP-IO-24GE4XS-C3PA#
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 hfcl             -   -    -     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

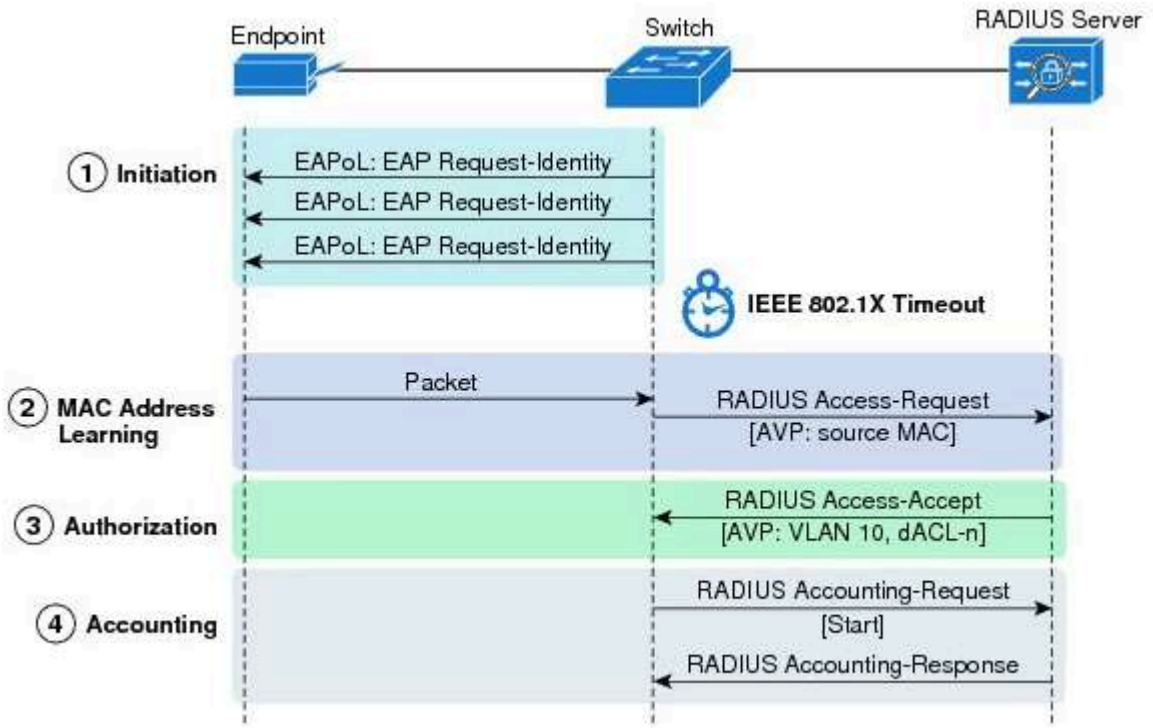


Packet capture

```
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



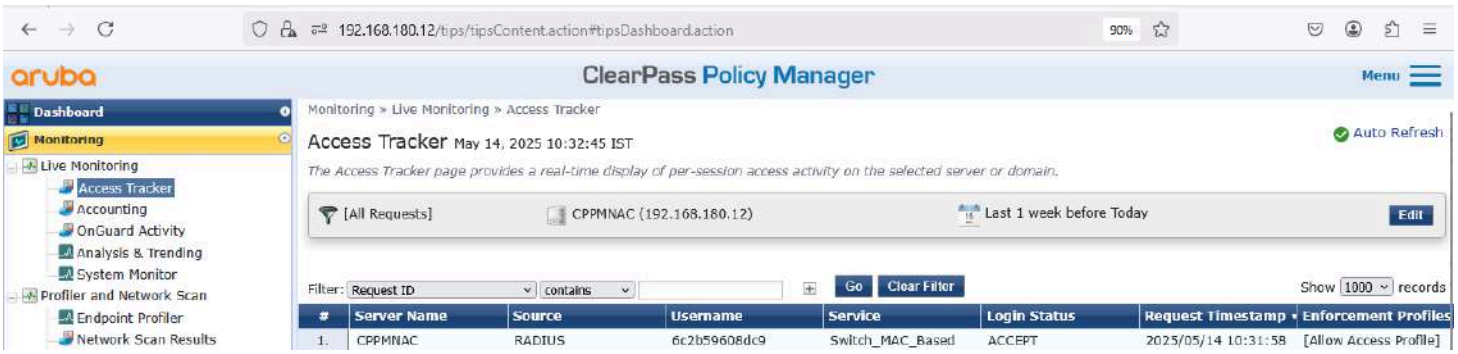
All mandatory AVP (Attribute value pairs)

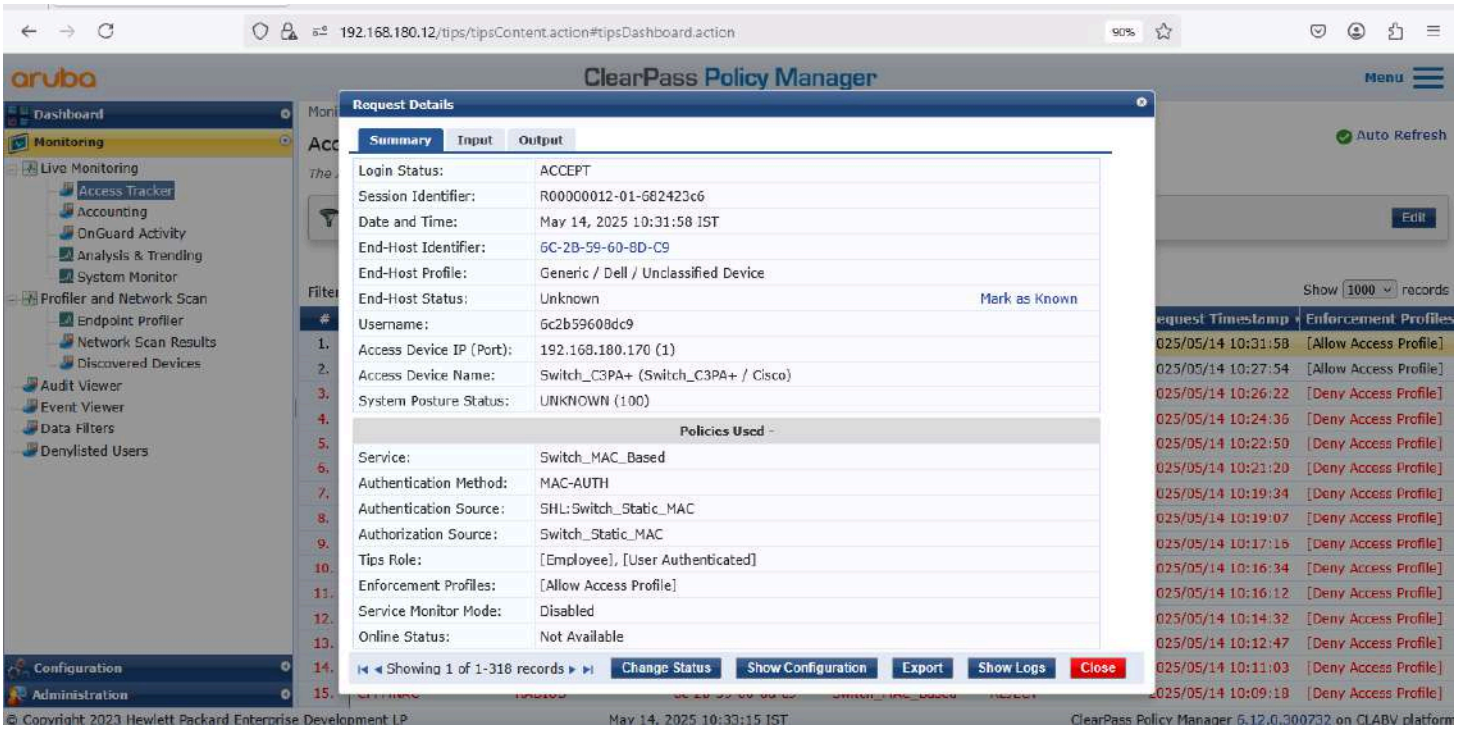
1: **User-Name (1)** – Identity of the user/device (e.g., username or MAC address for MAB)
2: **NAS-IP-Address (4)** – IP address of the authenticator (switch or wireless controller)
3: **NAS-Port (5)** – Physical or logical port number on which the request came in
4: **Called-Station-Id (30)** – MAC 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





Packet capture

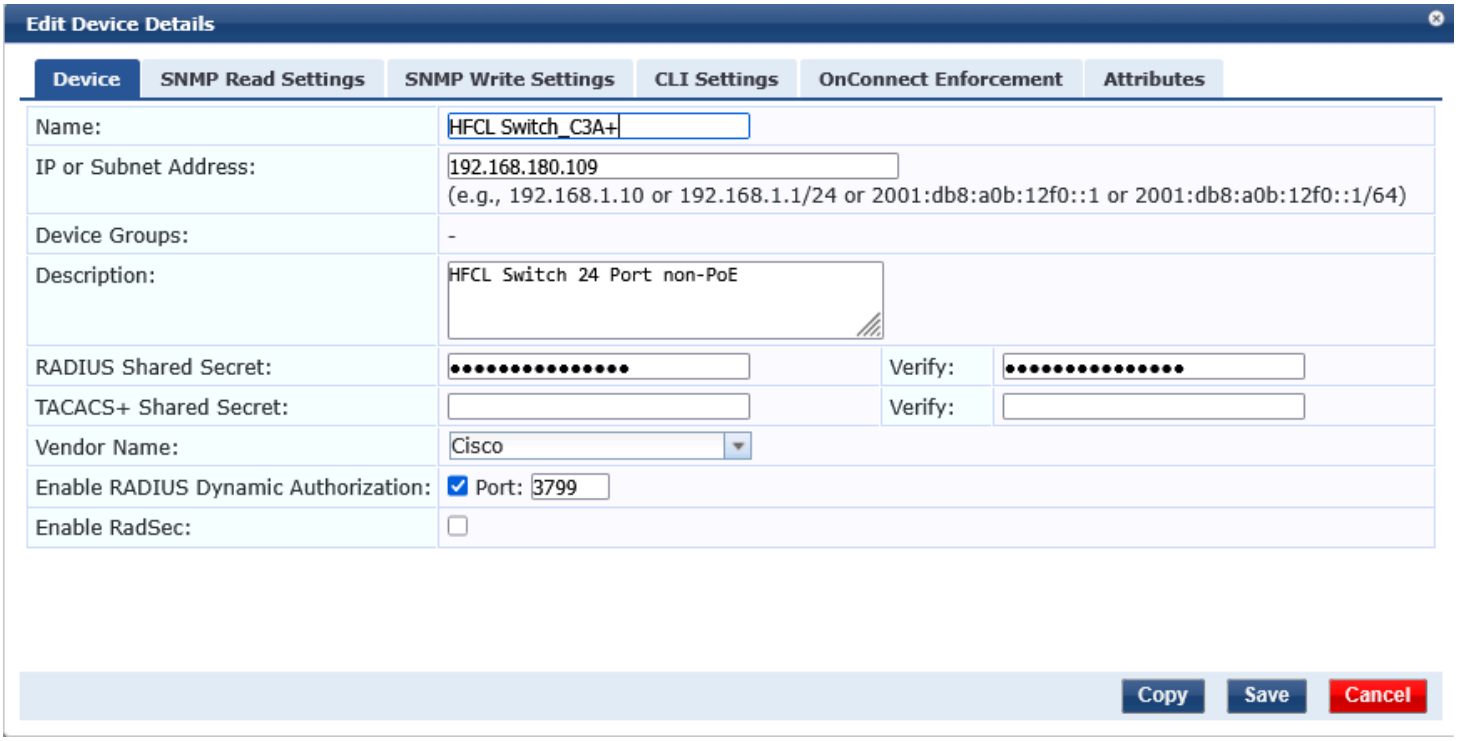
```
Attribute Value Pairs
  AVP: t=Framed-MTU(12) l=6 val=1344
  AVP: t=User-Name(1) l=14 val=6c2b59608dc9
  AVP: t=User-Password(2) l=18 val=Decrypted: 6c2b59608dc9
  AVP: t=Service-Type(6) l=6 val=Call-Check(10)
  AVP: t=NAS-Port-Type(61) l=6 val=Ethernet(15)
  AVP: t=NAS-Port(5) l=6 val=3
  AVP: t=NAS-Port-Id(87) 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

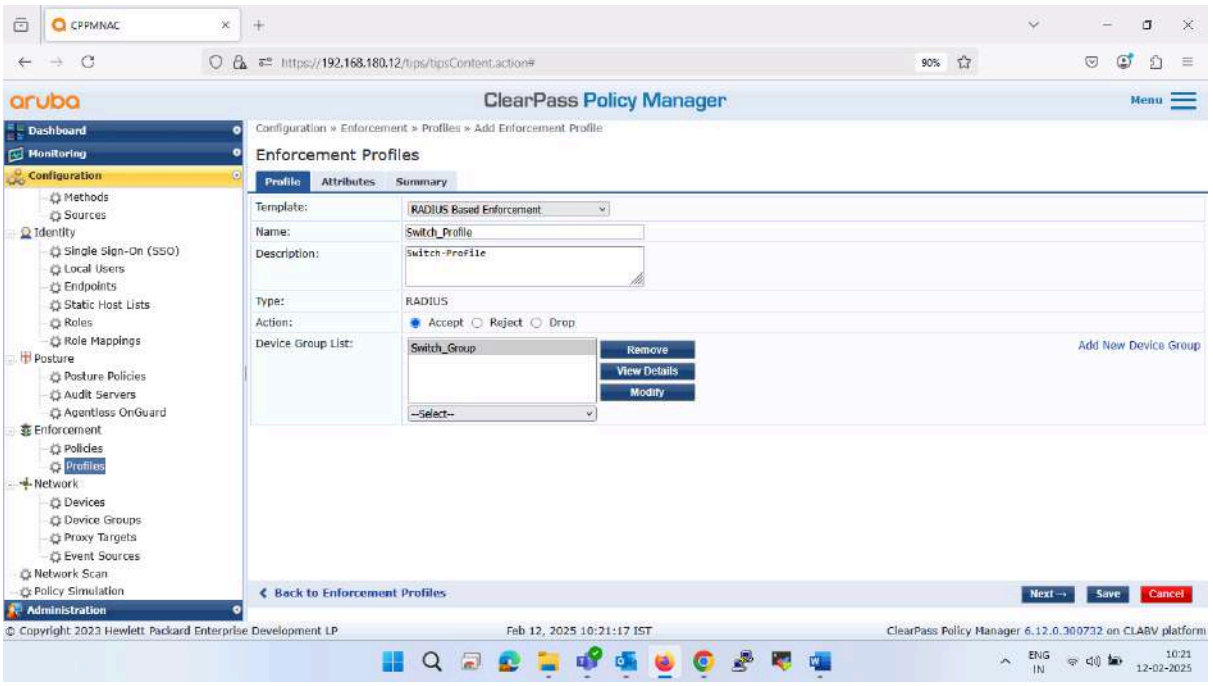
6.1 Add Network Device

Go to Configuration > Network > Devices

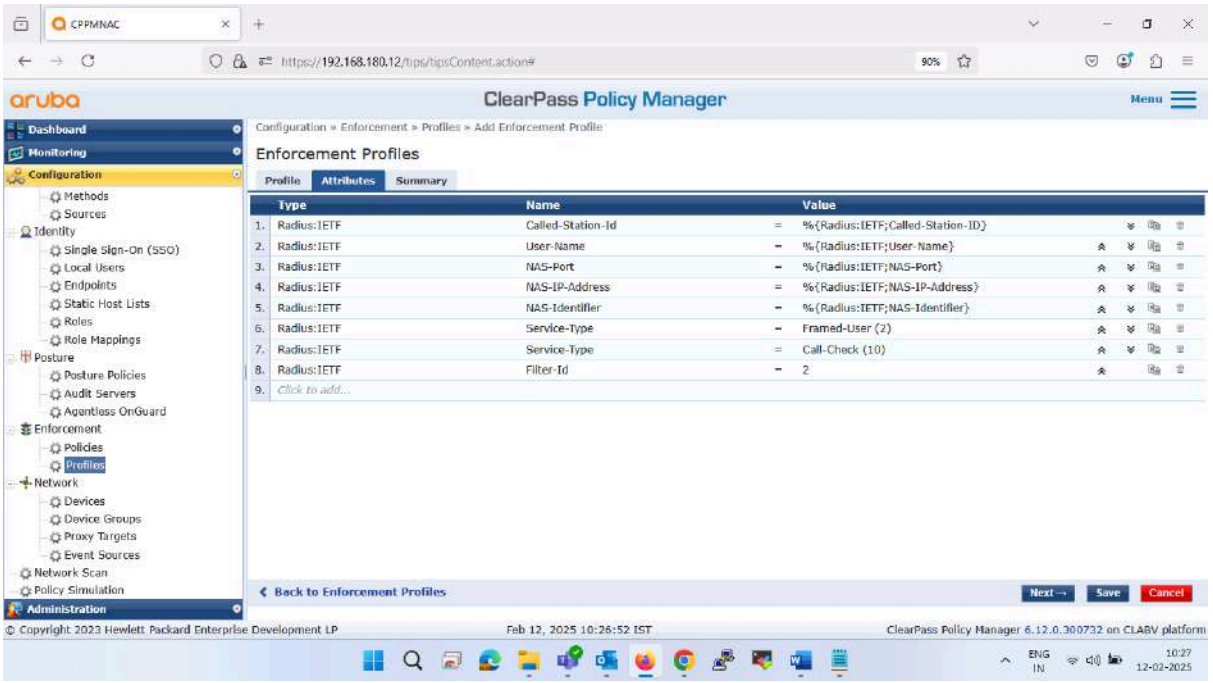


6.2 Profile

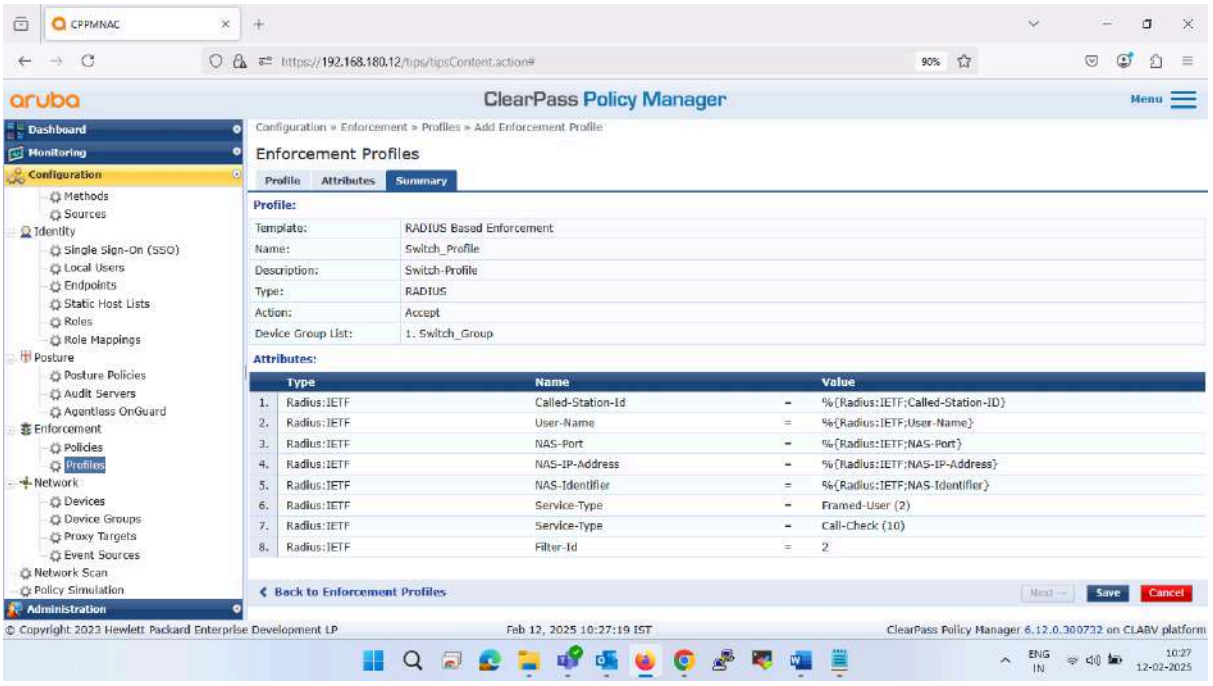
Add Enforcement profile



Add Attributes

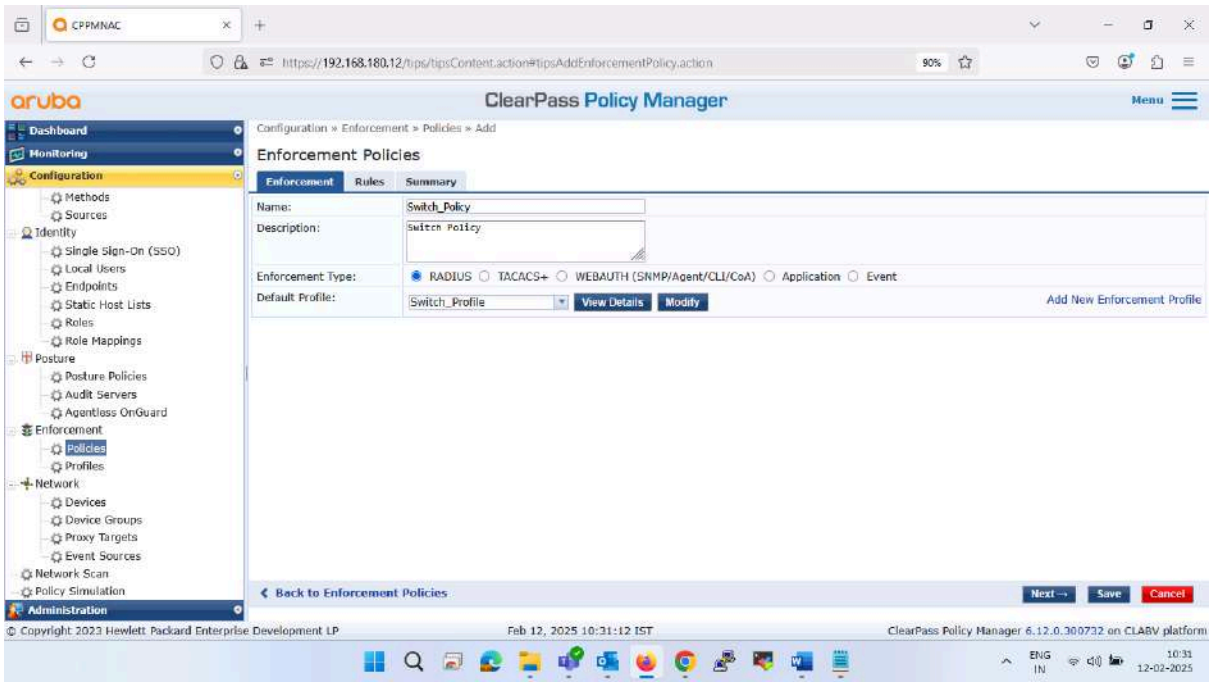


All configured parameters are showing in summary

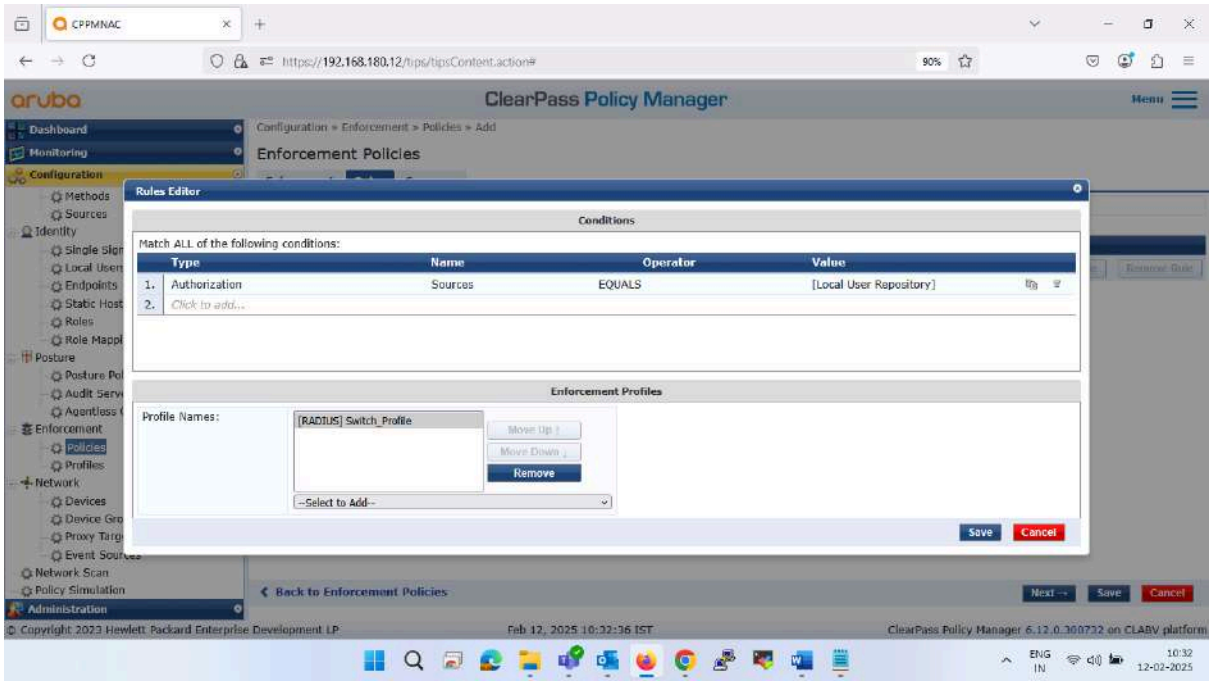


6.3 Policies

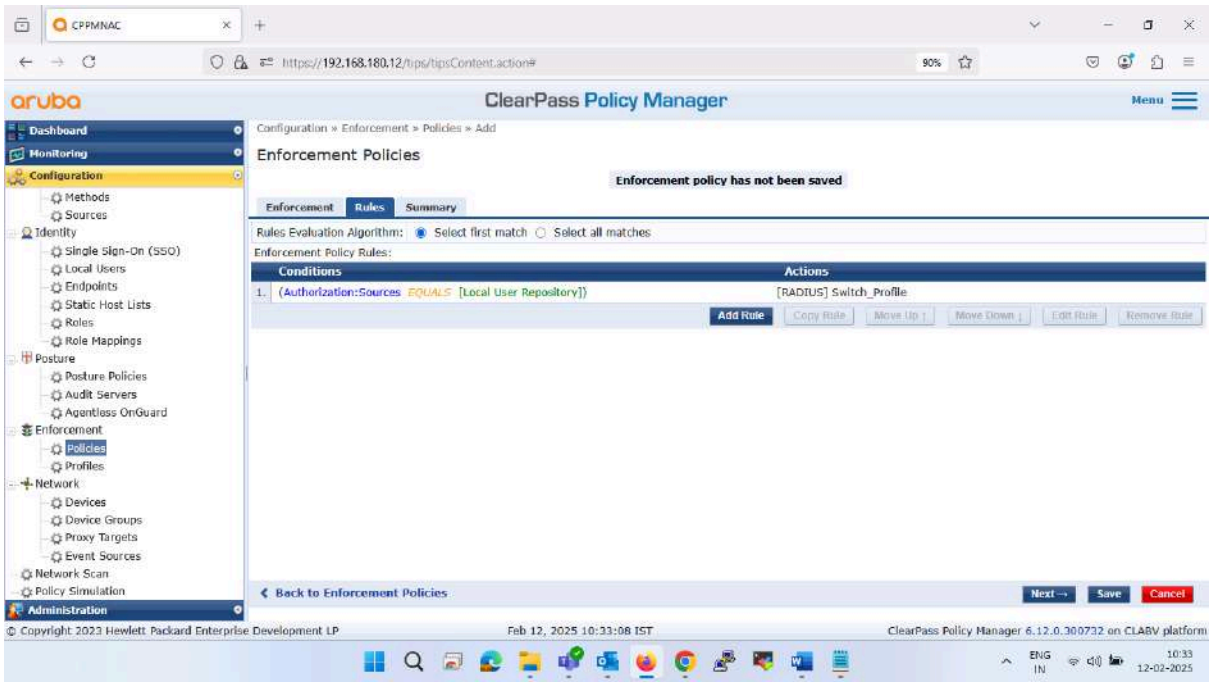
Add Enforcement policies



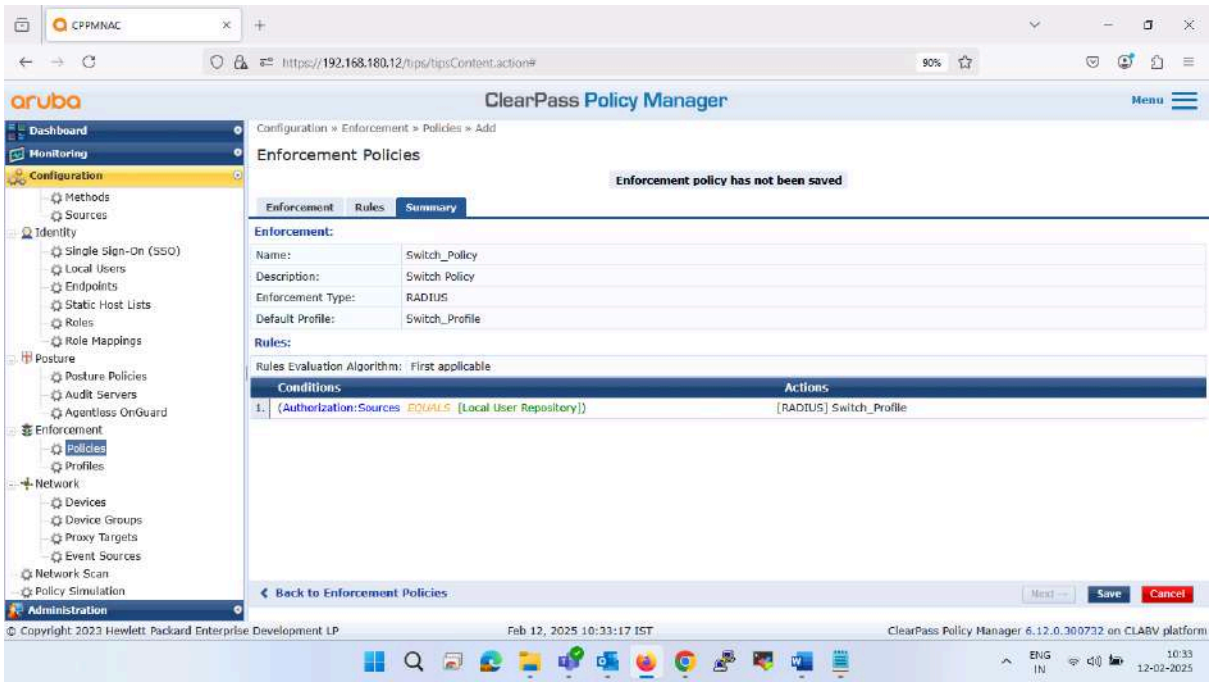
Now Add rules and select created profile



Rule Shown as per below screenshot after created

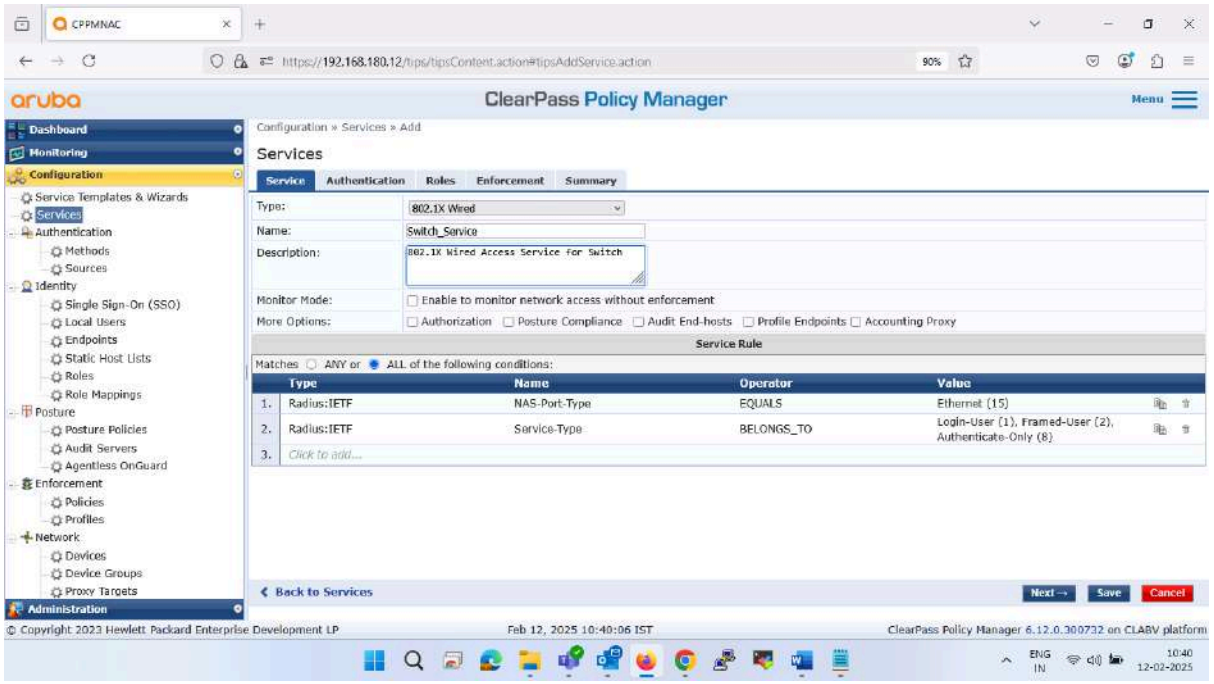


Configured parameters are shown in policies

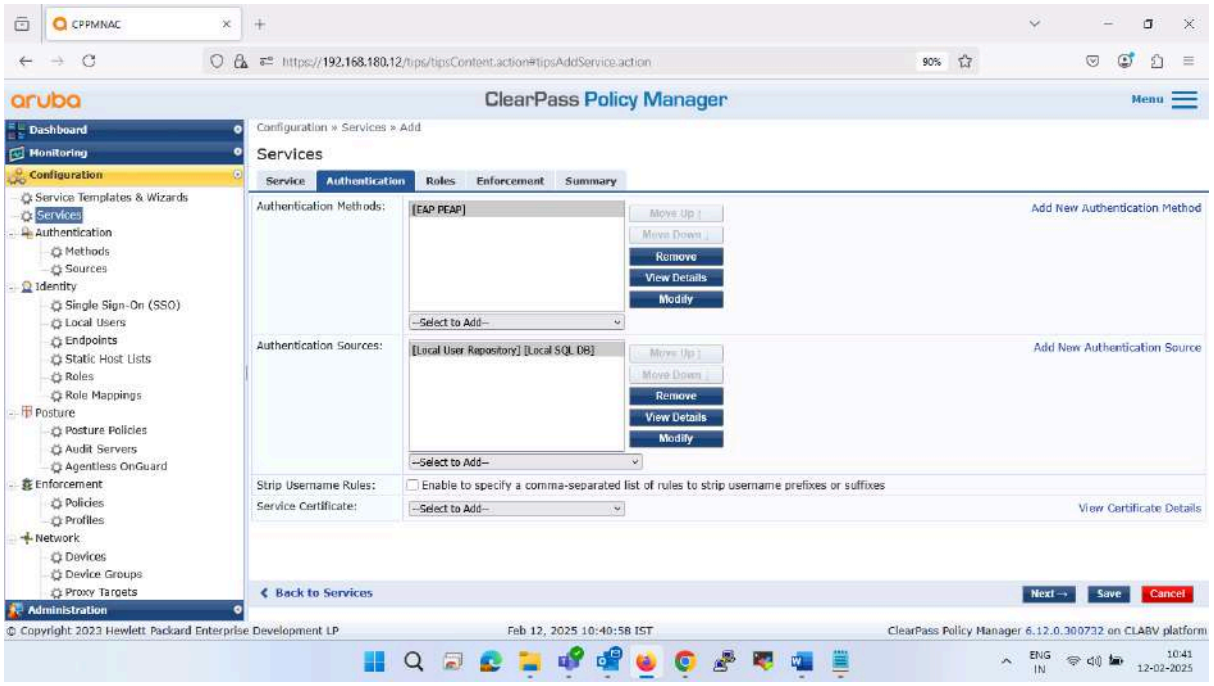


6.4 Services

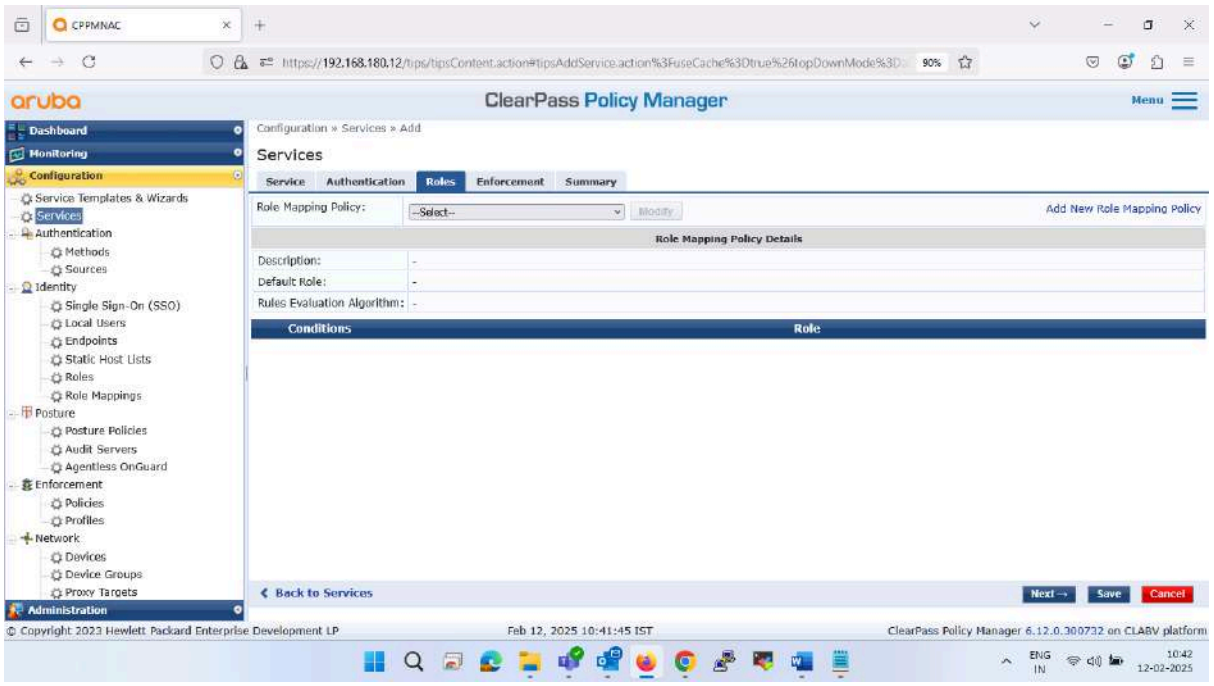
Add Service

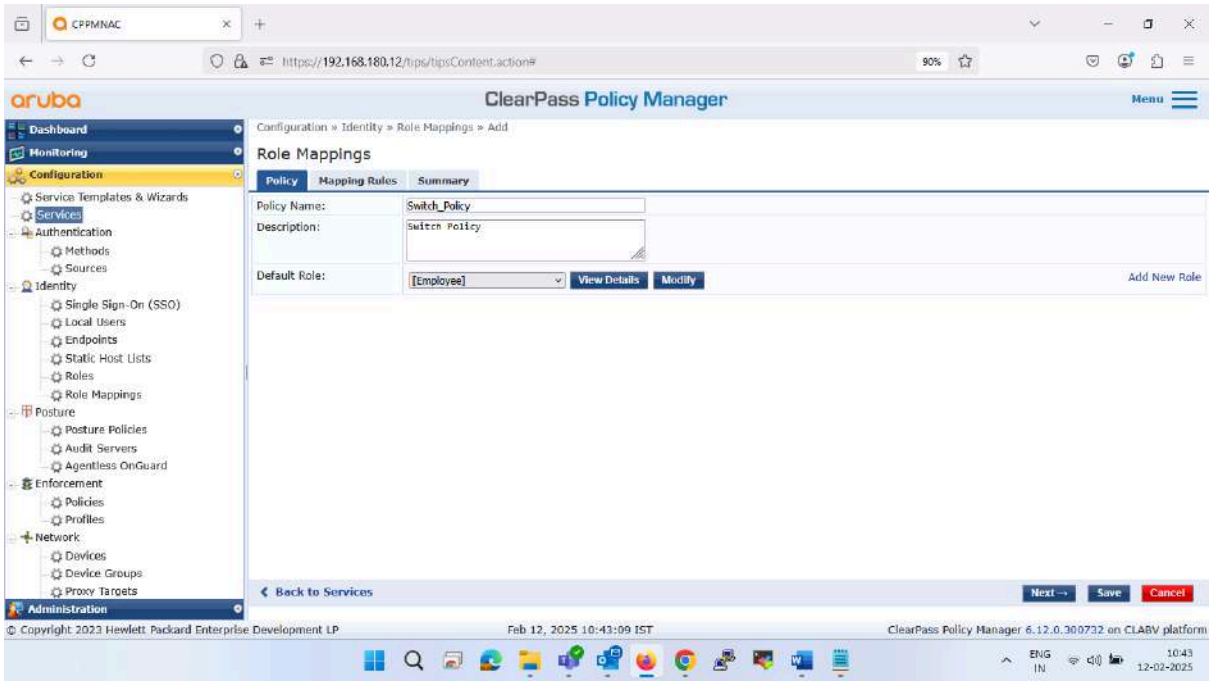


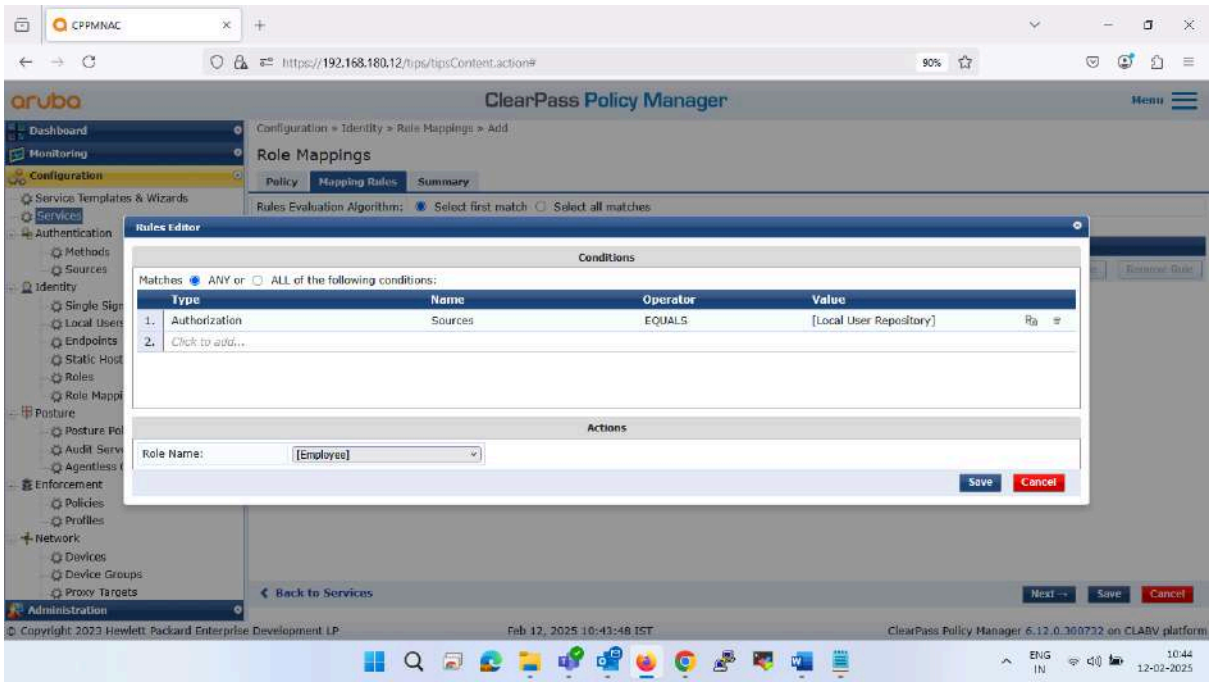
Add Authentication method and Authentication source

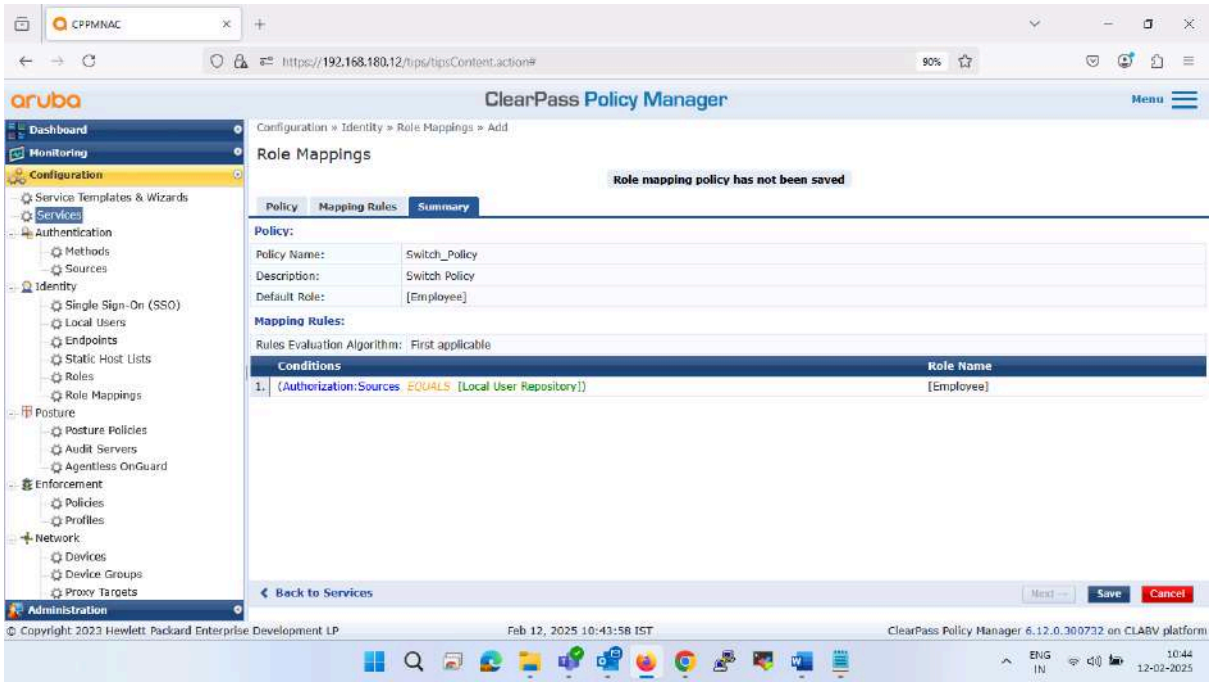


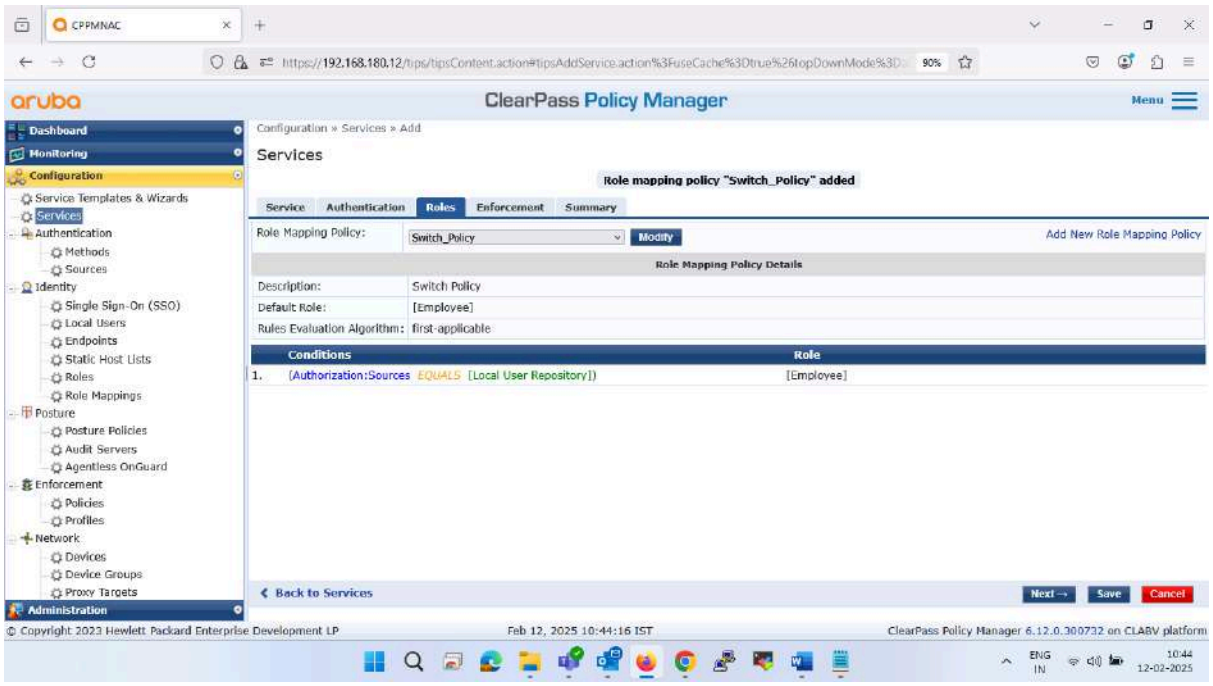
Click on Add New Role Mapping Policy


CPPMNAC
https://192.168.180.12/tips/tipsContent.action#tipsAddService.action%3FuseCache%3Dtrue%26topDownMode%3D
90%
aruba
ClearPass Policy Manager
Menu
Dashboard
Monitoring
Configuration
Service Templates & Wizards
Services
Authentication
Methods
Sources
Identity
Single Sign-On (SSO)
Local Users
Endpoints
Static Host Lists
Roles
Role Mappings
Posture
Posture Policies
Audit Servers
Agentless OnGuard
Enforcement
Policies
Profiles
Network
Devices
Device Groups
Proxy Targets
Administration
Configuration » Services » Add
Services
Service
Authentication
Roles
Enforcement
Summary
Role Mapping Policy:
--Select--
Modify
Add New Role Mapping Policy
Role Mapping Policy Details
Description:
Default Role:
Rules Evaluation Algorithm:
Conditions
Role
Back to Services
Next →
Save
Cancel
© Copyright 2023 Hewlett Packard Enterprise Development LP
Feb 12, 2025 10:41:45 IST
ClearPass Policy Manager 6.12.0.300732 on CLABV platform
ENG
IN
10:42
12-02-2025

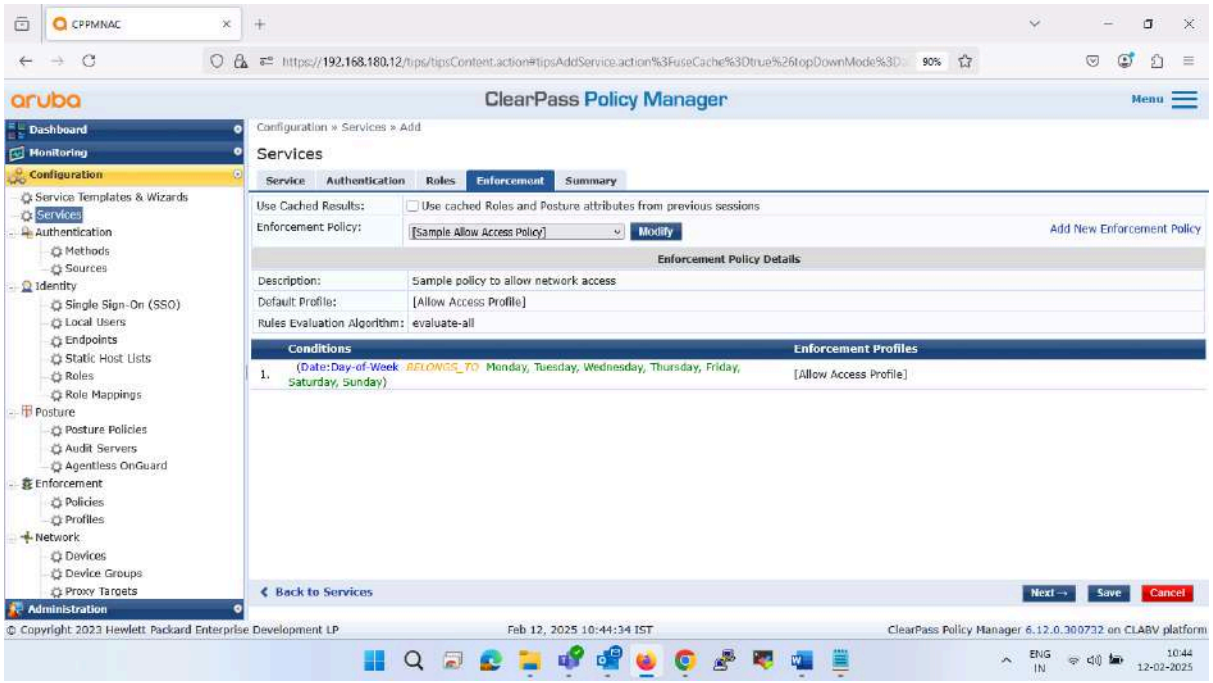

CPPMNAC
https://192.168.180.12/tips/tipsContent.action#
90%
aruba
ClearPass Policy Manager
Menu
Dashboard
Monitoring
Configuration
Service Templates & Wizards
Services
Authentication
Methods
Sources
Identity
Single Sign-On (SSO)
Local Users
Endpoints
Static Host Lists
Roles
Role Mappings
Posture
Posture Policies
Audit Servers
Agentless OnGuard
Enforcement
Policies
Profiles
Network
Devices
Device Groups
Proxy Targets
Administration
Configuration » Identity » Role Mappings » Add
Role Mappings
Policy
Mapping Rules
Summary
Policy Name:
Switch_Policy
Description:
Switch Policy
Default Role:
[Employee]
View Details
Modify
Add New Role
Back to Services
Next →
Save
Cancel
© Copyright 2023 Hewlett Packard Enterprise Development LP
Feb 12, 2025 10:43:09 IST
ClearPass Policy Manager 6.12.0.300732 on CLABV platform
ENG
IN
10:43
12-02-2025

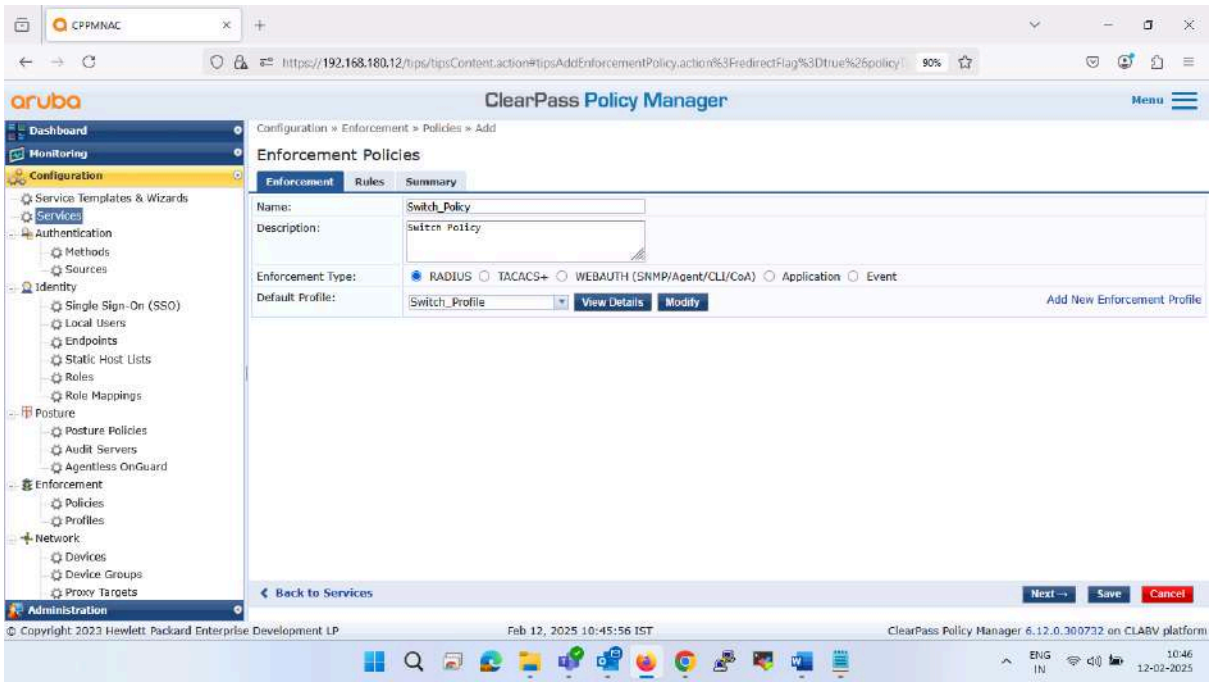

CPPMNAC
https://192.168.180.12/tips/tipsContent.action#
ClearPass Policy Manager
Menu
Configuration » Identity » Role Mappings » Add
Role Mappings
Policy
Mapping Rules
Summary
Rules Evaluation Algorithm: Select first match Select all matches
Rules Editor
Conditions
Matches ANY or ALL of the following conditions:
Type
Name
Operator
Value
1. Authorization
Sources
EQUALS
[Local User Repository]
2. Click to add...
Actions
Role Name:
[Employee]
Save
Cancel
Back to Services
Next
Save
Cancel
Copyright 2023 Hewlett Packard Enterprise Development LP
Feb 12, 2025 10:43:48 IST
ClearPass Policy Manager 6.12.0.300732 on CLABV platform

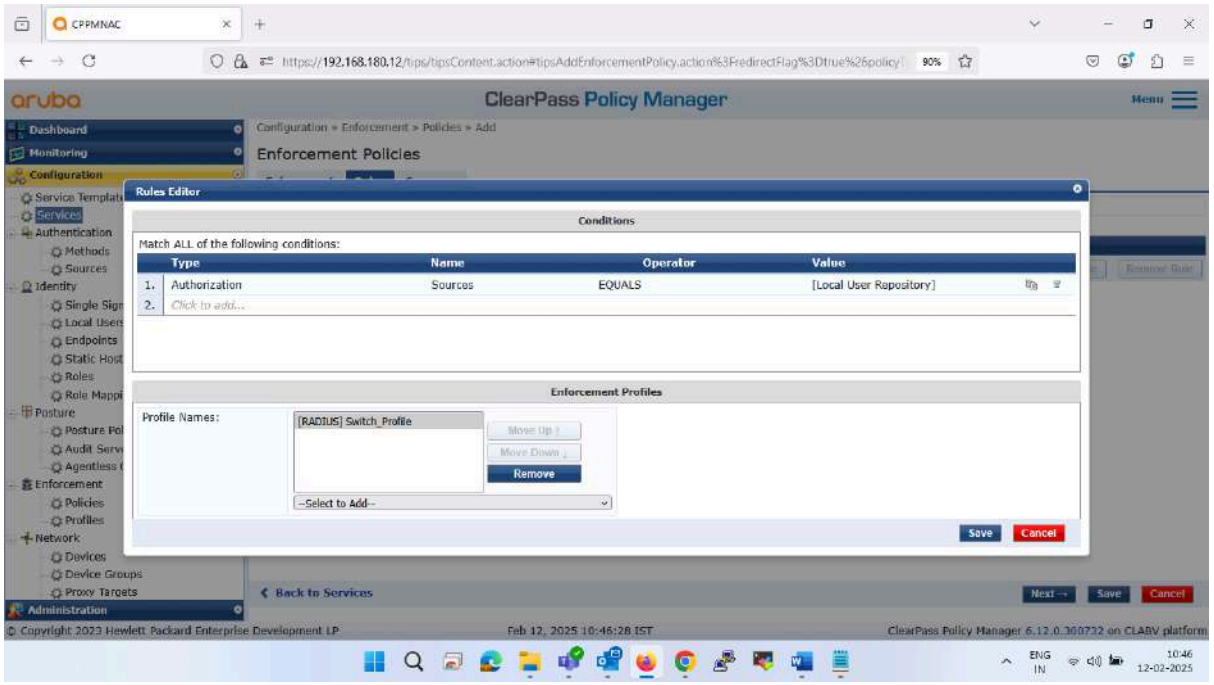

CPPMNAC
https://192.168.180.12/tips/tipsContent.action#
ClearPass Policy Manager
Menu
Configuration » Identity » Role Mappings » Add
Role Mappings
Role mapping policy has not been saved
Policy
Mapping Rules
Summary
Policy:
Policy Name: Switch_Policy
Description: Switch Policy
Default Role: [Employee]
Mapping Rules:
Rules Evaluation Algorithm: First applicable
Conditions
Role Name
1. (Authorization:Sources EQUALS [Local User Repository])
[Employee]
Back to Services
Next
Save
Cancel
Copyright 2023 Hewlett Packard Enterprise Development LP
Feb 12, 2025 10:43:58 IST
ClearPass Policy Manager 6.12.0.300732 on CLABV platform

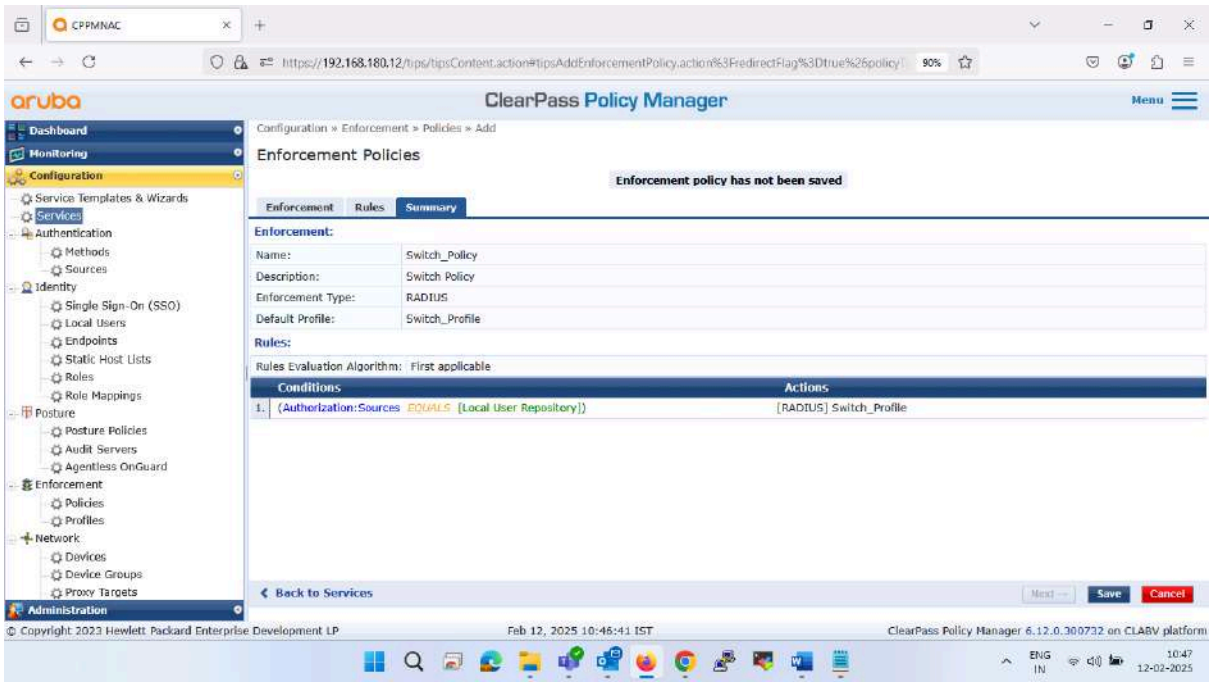


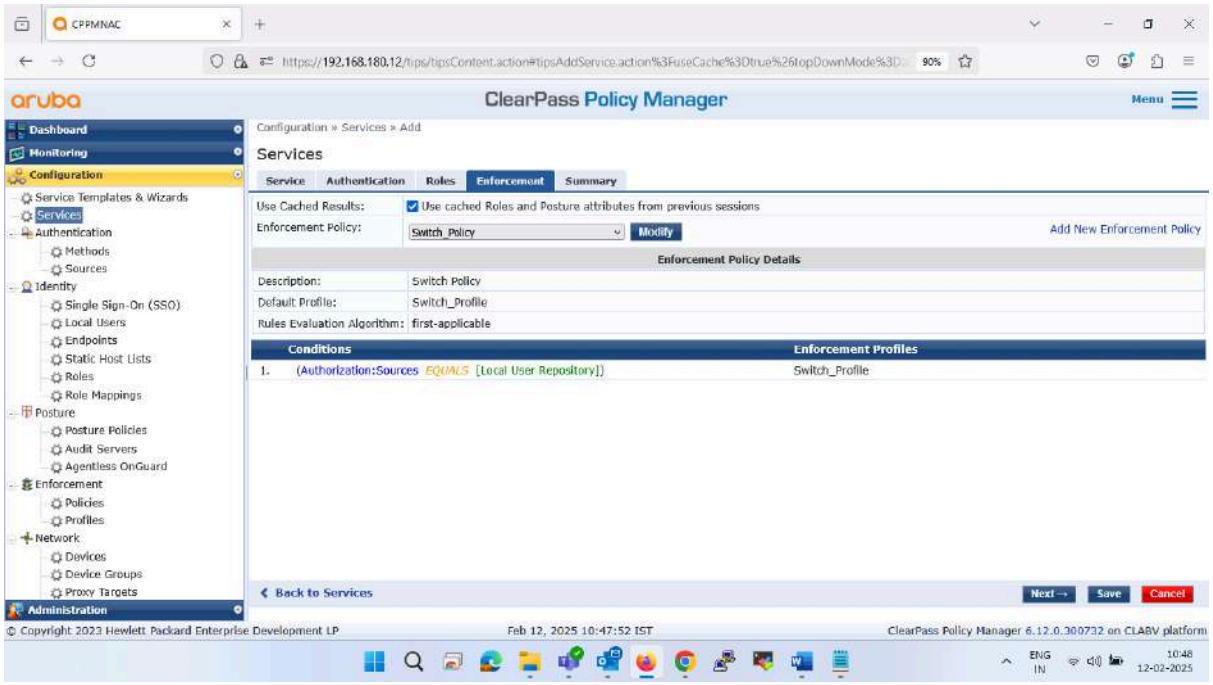
Click on Add New Enforcement Policy

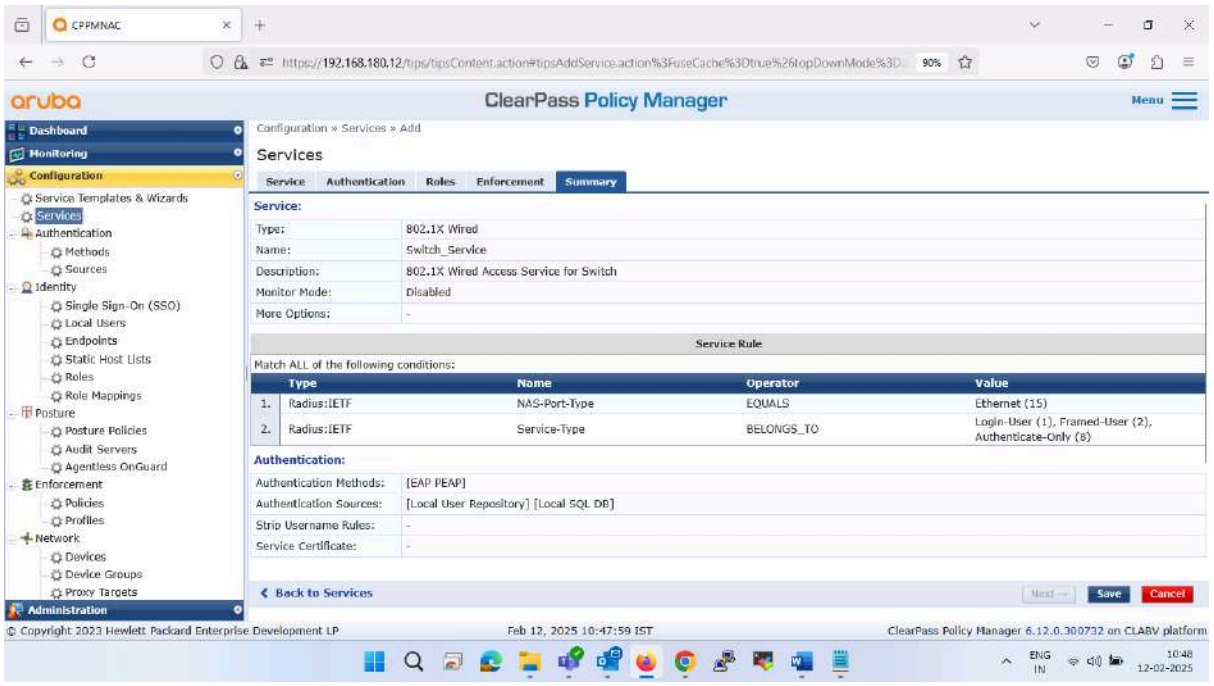


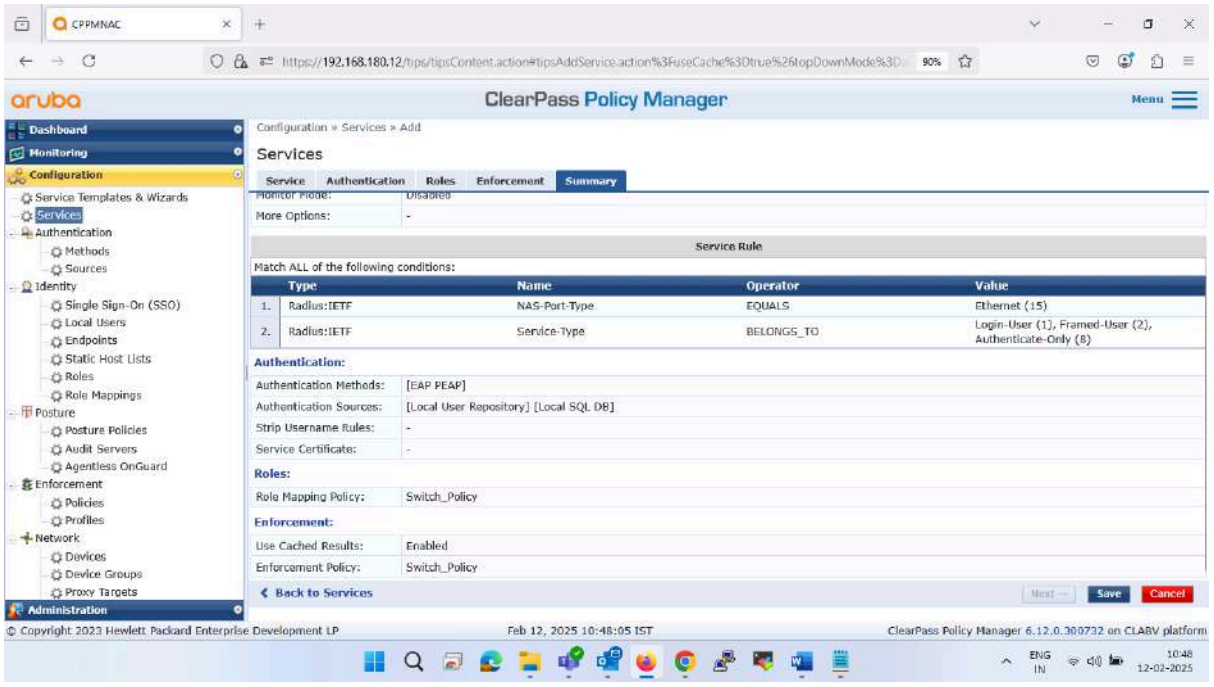

CPPMNAC
https://192.168.180.12/tips/tipsContent.action#tipsAddEnforcementPolicy.action%3FredirectFlag%3Dtrue%26policy
90%
aruba
ClearPass Policy Manager
Menu
Dashboard
Monitoring
Configuration
Service Templates & Wizards
Services
Authentication
Methods
Sources
Identity
Single Sign-On (SSO)
Local Users
Endpoints
Static Host Lists
Roles
Role Mappings
Posture
Posture Policies
Audit Servers
Agentless OnGuard
Enforcement
Policies
Profiles
Network
Devices
Device Groups
Proxy Targets
Administration
Configuration » Enforcement » Policies » Add
Enforcement Policies
Enforcement
Rules
Summary
Name:
Switch_Policy
Description:
Switch Policy
Enforcement Type:
RADIUS
TACACS+
WEBAUTH (SNMP/Agent/CLI/CoA)
Application
Event
Default Profile:
Switch_Profile
View Details
Modify
Add New Enforcement Profile
Back to Services
Next
Save
Cancel
© Copyright 2023 Hewlett Packard Enterprise Development LP
Feb 12, 2025 10:45:56 IST
ClearPass Policy Manager 6.12.0.300732 on CLABV platform
ENG
IN
10:46
12-02-2025


CPPMNAC
https://192.168.180.12/tips/tipsContent.action#tipsAddEnforcementPolicy.action%3FredirectFlag%3Dtrue%26policy
90%
aruba
ClearPass Policy Manager
Menu
Configuration » Enforcement » Policies » Add
Enforcement Policies
Rules Editor
Conditions
Match ALL of the following conditions:
Type
Name
Operator
Value
1.
Authorization
Sources
EQUALS
[Local User Repository]
2.
Click to add...
Enforcement Profiles
Profile Names:
[RADIUS] Switch_Profile
Move Up ↑
Move Down ↓
Remove
--Select to Add--
Save
Cancel
Back to Services
Next
Save
Cancel
© Copyright 2023 Hewlett Packard Enterprise Development LP
Feb 12, 2025 10:46:28 IST
ClearPass Policy Manager 6.12.0.300732 on CLABV platform
ENG
IN
10:46
12-02-2025


CPPMNAC
https://192.168.180.12/tips/tipsContent.action#tipsAddEnforcementPolicy.action%3FredirectFlag%3Dtrue%26policy
90%
aruba
ClearPass Policy Manager
Menu
Dashboard
Monitoring
Configuration
Service Templates & Wizards
Services
Authentication
Methods
Sources
Identity
Single Sign-On (SSO)
Local Users
Endpoints
Static Host Lists
Roles
Role Mappings
Posture
Posture Policies
Audit Servers
Agentless OnGuard
Enforcement
Policies
Profiles
Network
Devices
Device Groups
Proxy Targets
Administration
Configuration » Enforcement » Policies » Add
Enforcement Policies
Enforcement policy has not been saved
Enforcement
Rules
Summary
Enforcement:
Name: Switch_Policy
Description: Switch Policy
Enforcement Type: RADIUS
Default Profile: Switch_Profile
Rules:
Rules Evaluation Algorithm: First applicable
Conditions
Actions
1. (Authorization:Sources EQUALS [Local User Repository])
[RADIUS] Switch_Profile
Back to Services
Next →
Save
Cancel
© Copyright 2023 Hewlett Packard Enterprise Development LP
Feb 12, 2025 10:46:41 IST
ClearPass Policy Manager 6.12.0.300732 on CLABV platform
ENG
IN
10:47
12-02-2025


CPPMNAC
https://192.168.180.12/tips/tipsContent.action#tipsAddService.action%3FuseCache%3Dtrue%26topDownMode%3D
90%
aruba
ClearPass Policy Manager
Menu
Dashboard
Monitoring
Configuration
Service Templates & Wizards
Services
Authentication
Methods
Sources
Identity
Single Sign-On (SSO)
Local Users
Endpoints
Static Host Lists
Roles
Role Mappings
Posture
Posture Policies
Audit Servers
Agentless OnGuard
Enforcement
Policies
Profiles
Network
Devices
Device Groups
Proxy Targets
Administration
Configuration » Services » Add
Services
Service
Authentication
Roles
Enforcement
Summary
Use Cached Results:
Use cached Roles and Posture attributes from previous sessions
Enforcement Policy:
Switch_Policy
Modify
Add New Enforcement Policy
Enforcement Policy Details
Description: Switch Policy
Default Profile: Switch_Profile
Rules Evaluation Algorithm: first-applicable
Conditions
Enforcement Profiles
1. (Authorization:Sources EQUALS [Local User Repository])
Switch_Profile
Back to Services
Next →
Save
Cancel
© Copyright 2023 Hewlett Packard Enterprise Development LP
Feb 12, 2025 10:47:52 IST
ClearPass Policy Manager 6.12.0.300732 on CLABV platform
ENG
IN
10:48
12-02-2025

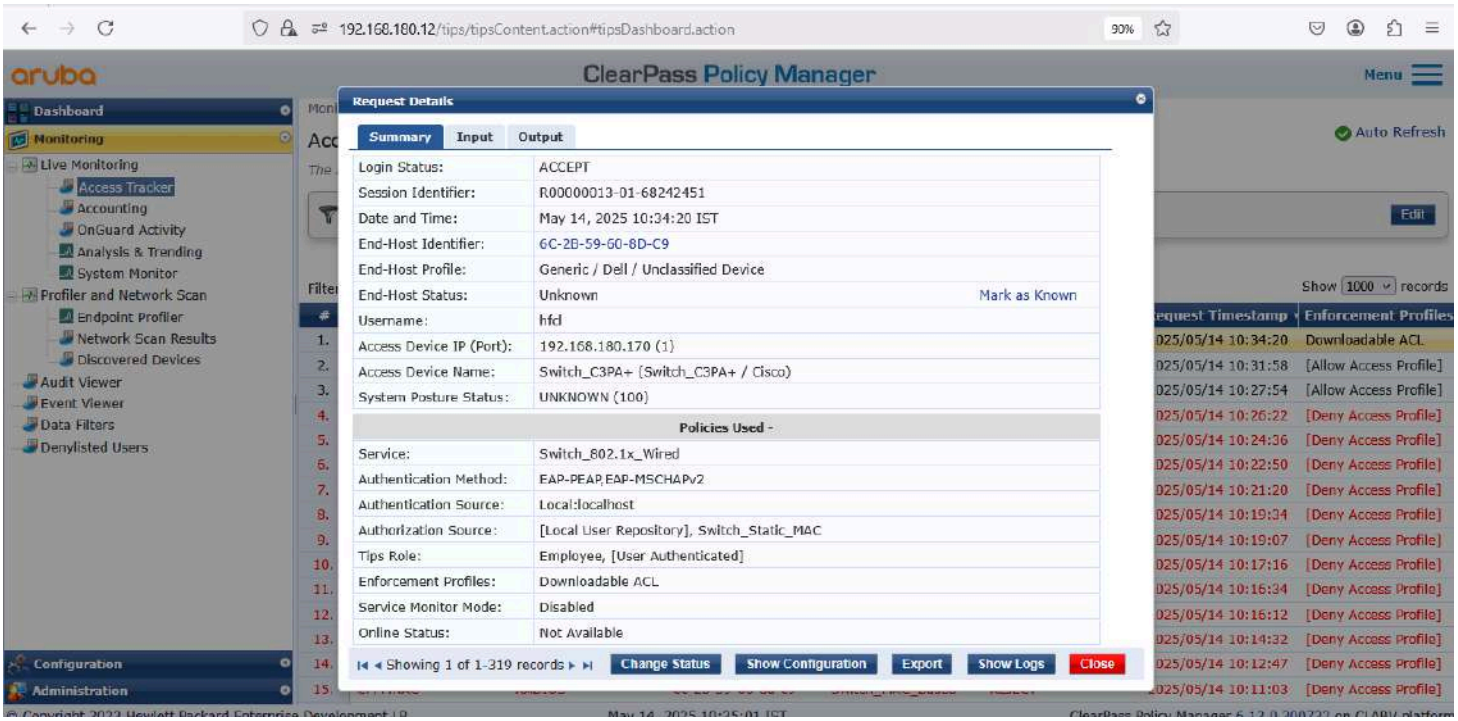

CPPMNAC
https://192.168.180.12/tips/tipsContent.action#tipsAddService.action%3FuseCache%3Dtrue%26topDownMode%3D
90%
aruba
ClearPass Policy Manager
Menu
Dashboard
Monitoring
Configuration
Service Templates & Wizards
Services
Authentication
Methods
Sources
Identity
Single Sign-On (SSO)
Local Users
Endpoints
Static Host Lists
Roles
Role Mappings
Posture
Posture Policies
Audit Servers
Agentless OnGuard
Enforcement
Policies
Profiles
Network
Devices
Device Groups
Proxy Targets
Administration
Configuration » Services » Add
Services
Service
Authentication
Roles
Enforcement
Summary
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: -
Back to Services
Next
Save
Cancel
© Copyright 2023 Hewlett Packard Enterprise Development LP
Feb 12, 2025 10:47:59 IST
ClearPass Policy Manager 6.12.0.300732 on CLABV platform
ENG
IN
10:48
12-02-2025


CPPMNAC
https://192.168.180.12/tips/tipsContent.action#tipsAddService.action%3FuseCache%3Dtrue%26topDownMode%3D
90%
aruba
ClearPass Policy Manager
Menu
Dashboard
Monitoring
Configuration
Service Templates & Wizards
Services
Authentication
Methods
Sources
Identity
Single Sign-On (SSO)
Local Users
Endpoints
Static Host Lists
Roles
Role Mappings
Posture
Posture Policies
Audit Servers
Agentless OnGuard
Enforcement
Policies
Profiles
Network
Devices
Device Groups
Proxy Targets
Administration
Configuration » Services » Add
Services
Service
Authentication
Roles
Enforcement
Summary
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
Back to Services
Next
Save
Cancel
© Copyright 2023 Hewlett Packard Enterprise Development LP
Feb 12, 2025 10:48:05 IST
ClearPass Policy Manager 6.12.0.300732 on CLABV platform
ENG
IN
10:48
12-02-2025

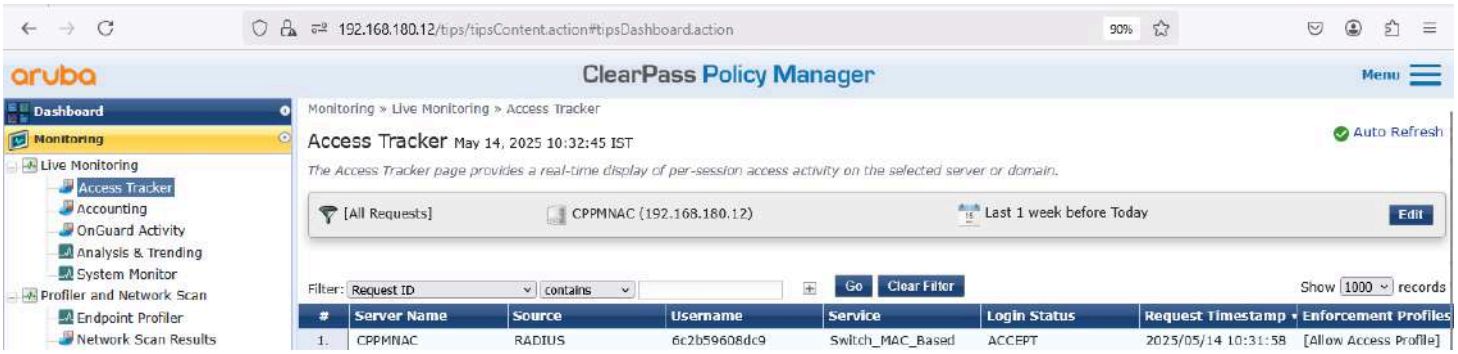
7. Expected and Actual Results

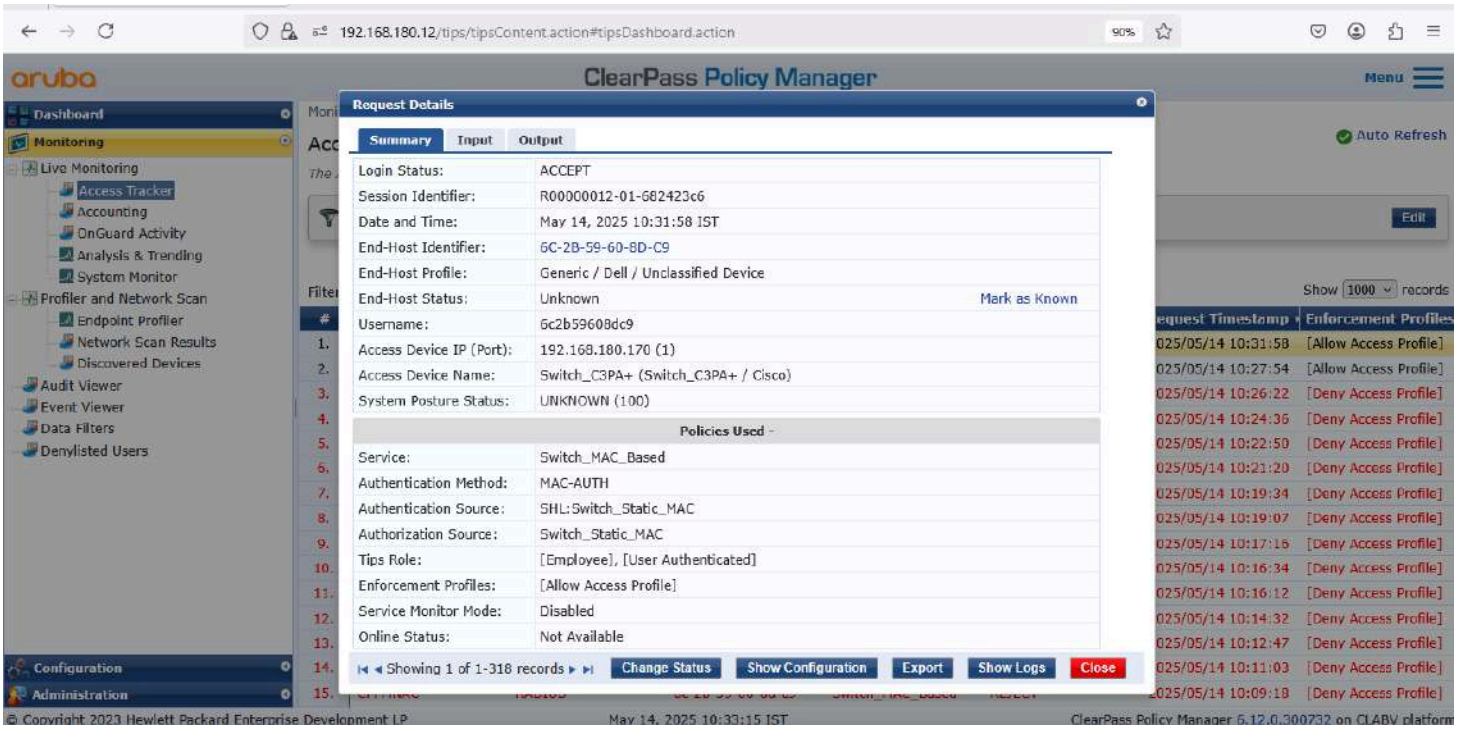
As per the expected results, 802.1X authentication functioned as expected across all test cases—EAPOL exchange, RADIUS communication, VLAN assignment, fallback to MAB, and reauthentication were successfully verified with no discrepancies observed.

7.1 Successfully authentication with 802.1X based



7.2 Successfully authentication with MAC based





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.

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.com
Enquiry: ioenquiry@hfcl.com
Support: 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