Secure integration of Axis devices into Aruba networks

User manual

Table of Contents

Introduction

Introduction

This integration guide aims to outline the best-practice configuration of how to onboard and operate Axis devices in Aruba networks. The configuration uses modern security standards and protocols such as IEEE 802.1X, IEEE 802.1AR, IEEE 802.1AE, and HTTPS.

Establishing proper automation for network integration can save time and money. It allows the removal of unnecessary system complexity when using Axis device management applications combined with Aruba network equipment and applications. Below are just some benefits that can be gained when combining Axis devices and software with an Aruba network infrastructure:

- Minimize system complexity by removing device staging networks.
- Save costs by adding automating onboarding processes and device management.
- Take advantage of zero-touch network security controls provided by Axis devices.
- Increase overall network security by applying Aruba and Axis expertise.

The network infrastructure must be prepared to securely verify the integrity of the Axis devices before starting the configuration. This allows a smooth software defined transition between logical networks throughout the on-boarding process. It is necessary to have knowledge about the following areas before doing the configuration:

- Managing Aruba enterprise network IT-infrastructure including Aruba access switches and Aruba ClearPass Policy Manager.
- Expertise in modern network access control techniques and network security policies.
- Basic knowledge about Axis products is desirable but will be provided throughout the guide.

Secure onboarding - IEEE 802.1AR/802.1X

Initial authentication

Connect the Axis Edge Vault supported Axis device to authenticate the device against the Aruba network. The device will use the IEEE 802.1AR Axis device ID certificate through the IEEE 802.1X network access control to authenticate itself.

To grant access to the network, the Aruba ClearPass Policy Manager verifies the Axis device ID together with other device specific fingerprints. The information, such as MAC-address and running firmware, is used to make a policy-based decision.

The Axis device authenticates against the Aruba network using the IEEE 802.1AR compliant Axis device ID certificate.

The Axis device authenticates against the Aruba network using the IEEE 802.1AR-compliant Axis device ID certificate.

1 Axis device ID
2 IEEE 802.1x EAP-TLS network authentication
3 Access switch (authenticator)
4 ClearPass policy manager

Provisioning

After authentication, the Aruba network will move the Axis device into the provisioning network (VLAN201) where Axis Device Manager is installed. Through the Axis Device Manager, device configuration, security hardening, and firmware updates can be performed. To complete the device provisioning, new customer specific production-grade certificates are uploaded onto the device for IEEE 802.1X and HTTPS.

After successful authentication, the Axis device moves into a provisioning network for configuration.

1 Access switch
2 Provisioning network
3 ClearPass policy manager
4 Device management application

Production network

The provisioning of the Axis device with new IEEE 802.1X certificates will trigger a new authentication attempt. The Aruba ClearPass Policy Manager will verify the new certificates and decide whether to move the Axis device into the production network or not.

After the device configuration, the Axis device will leave the provisioning network and attempt to reauthenticate against the Aruba network.

1 Axis device ID
2 IEEE 802.1x EAP-TLS network authentication
3 Access switch (authenticator)
4 ClearPass Policy Manager

After reauthentication, the Axis device is moved into the production network (VLAN 202). In that network, the Video Management System (VMS) will connect to the Axis device and start to operate.

The Axis device is granted access to the production network.

1 Access switch
2 Production network
3 ClearPass policy manager
4 Video management system

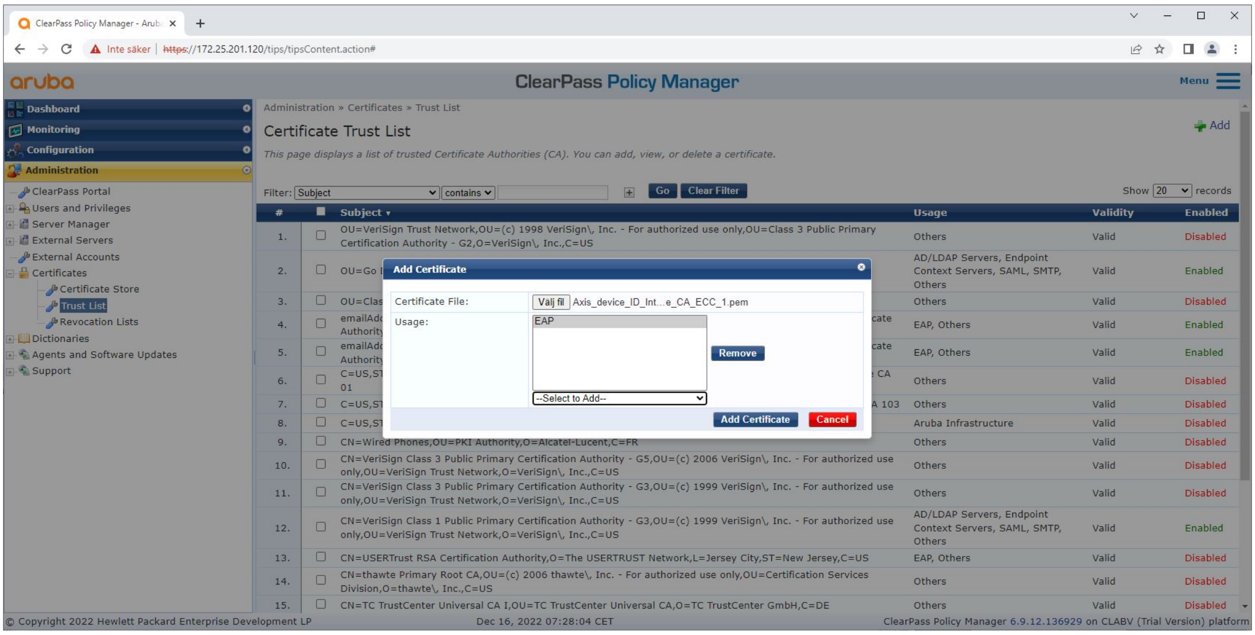
Configuration HPE Aruba

Aruba ClearPass Policy Manager

Aruba's ClearPass Policy Manager provides role- and device based secure network access control for IoT, BYOD, corporate devices, employees, contractors, and guests across and multivendor wired, wireless, and VPN infrastructure.

Trusted certificate store configuration

1. Download the Axis-specific IEEE 802.1AR certificate chain from axis.com.
2. Upload the Axis-specific IEEE 802.1AR Root CA and Intermediate CA certificate chains into the trusted certificate store.
3. Enable the Aruba ClearPass Policy Manager to authenticate Axis devices through IEEE 802.1X EAP-TLS.
4. Select EAP in the usage field. The certificates will be used for IEEE 802.1X EAP-TLS authentication.



Administration » Certificates » Trust List

Certificate Trust List

This page displays a list of trusted Certificate Authorities (CA). You can add, view, or delete a certificate.

Filter: Subject contains

Show 20 records

#		Subject ▾	Usage	Validity	Enabled
1.	□	OU=VeriSign Trust Network,OU=(c) 1998 VeriSign\, Inc. - For authorized use only,OU=Class 3 Public Primary Certification Authority - G2,O=VeriSign\, Inc.,C=US	Others	Valid	Disabled
2.	□	OU=Go	AD/LDAP Servers, Endpoint Context Servers, SAML, SMTP, Others	Valid	Enabled
3.	□	OU=Clas	Others	Valid	Disabled
4.	□	emailAdc Authority … cate	EAP, Others	Valid	Enabled
5.	□	emailAdc Authority … cate	EAP, Others	Valid	Enabled
6.	□	C=US,ST 01 … CA	Others	Valid	Disabled
7.	□	C=US,ST … A 103	Others	Valid	Disabled
8.	□	C=US,ST	Aruba Infrastructure	Valid	Disabled
9.	□	CN=Wired Phones,OU=PKI Authority,O=Alcatel-Lucent,C=FR	Others	Valid	Disabled
10.	□	CN=VeriSign Class 3 Public Primary Certification Authority - G5,OU=(c) 2006 VeriSign\, Inc. - For authorized use only,OU=VeriSign Trust Network,O=VeriSign\, Inc.,C=US	Others	Valid	Disabled
11.	□	CN=VeriSign Class 3 Public Primary Certification Authority - G3,OU=(c) 1999 VeriSign\, Inc. - For authorized use only,OU=VeriSign Trust Network,O=VeriSign\, Inc.,C=US	Others	Valid	Disabled
12.	□	CN=VeriSign Class 1 Public Primary Certification Authority - G3,OU=(c) 1999 VeriSign\, Inc. - For authorized use only,OU=VeriSign Trust Network,O=VeriSign\, Inc.,C=US	AD/LDAP Servers, Endpoint Context Servers, SAML, SMTP, Others	Valid	Enabled
13.	□	CN=USERTrust RSA Certification Authority,O=The USERTRUST Network,L=Jersey City,ST=New Jersey,C=US	EAP, Others	Valid	Disabled
14.	□	CN=thawte Primary Root CA,OU=(c) 2006 thawte\, Inc. - For authorized use only,OU=Certification Services Division,O=thawte\, Inc.,C=US	Others	Valid	Disabled
15.	□	CN=TC TrustCenter Universal CA I,OU=TC TrustCenter Universal CA,O=TC TrustCenter GmbH,C=DE	Others	Valid	Disabled

Add Certificate

Certificate File: Välj fil Axis_device_ID_Int...e_CA_ECC_1.pem

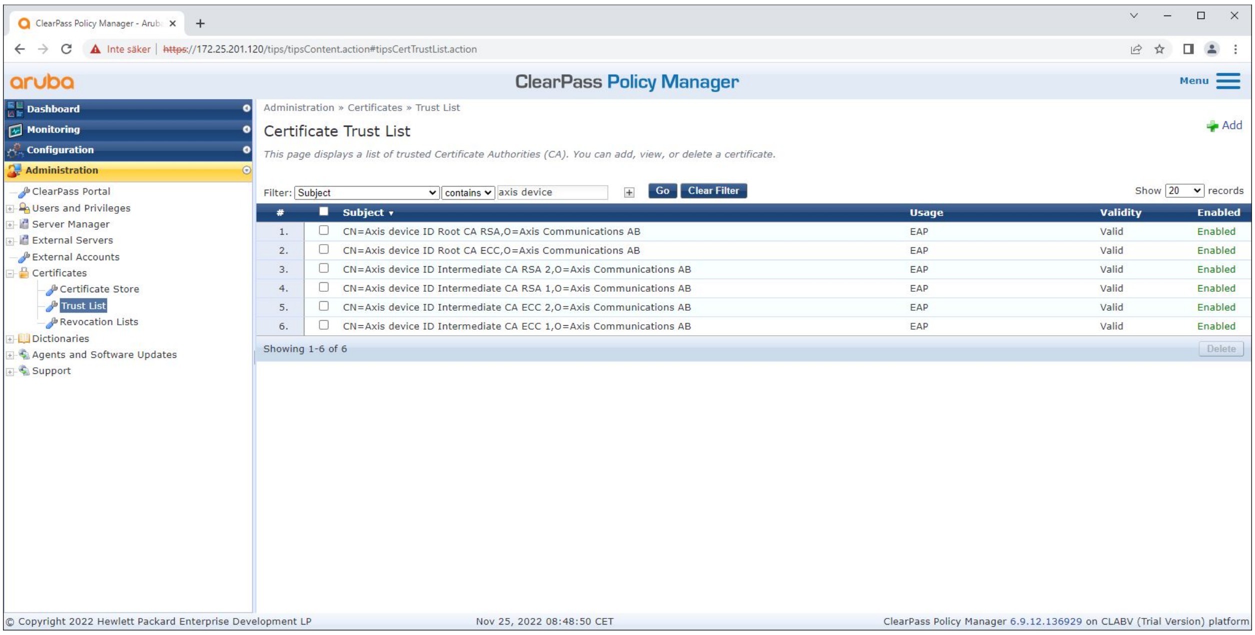
Usage: EAP

--Select to Add--

© Copyright 2022 Hewlett Packard Enterprise Development LP   Dec 16, 2022 07:28:04 CET   ClearPass Policy Manager 6.9.12.136929 on CLABV (Trial Version) platform

Uploading the Axis-specific IEEE 802.1AR certificates to the trusted certificate store of the Aruba ClearPass Policy Manager.

Secure onboarding - IEEE 802.1AR/802.1X



Administration » Certificates » Trust List

Certificate Trust List

This page displays a list of trusted Certificate Authorities (CA). You can add, view, or delete a certificate.

#	□	Subject ▾	Usage	Validity	Enabled
1.	□	CN=Axis device ID Root CA RSA,O=Axis Communications AB	EAP	Valid	Enabled
2.	□	CN=Axis device ID Root CA ECC,O=Axis Communications AB	EAP	Valid	Enabled
3.	□	CN=Axis device ID Intermediate CA RSA 2,O=Axis Communications AB	EAP	Valid	Enabled
4.	□	CN=Axis device ID Intermediate CA RSA 1,O=Axis Communications AB	EAP	Valid	Enabled
5.	□	CN=Axis device ID Intermediate CA ECC 2,O=Axis Communications AB	EAP	Valid	Enabled
6.	□	CN=Axis device ID Intermediate CA ECC 1,O=Axis Communications AB	EAP	Valid	Enabled

Showing 1-6 of 6

© Copyright 2022 Hewlett Packard Enterprise Development LP   Nov 25, 2022 08:48:50 CET   ClearPass Policy Manager 6.9.12.136929 on CLABV (Trial Version) platform

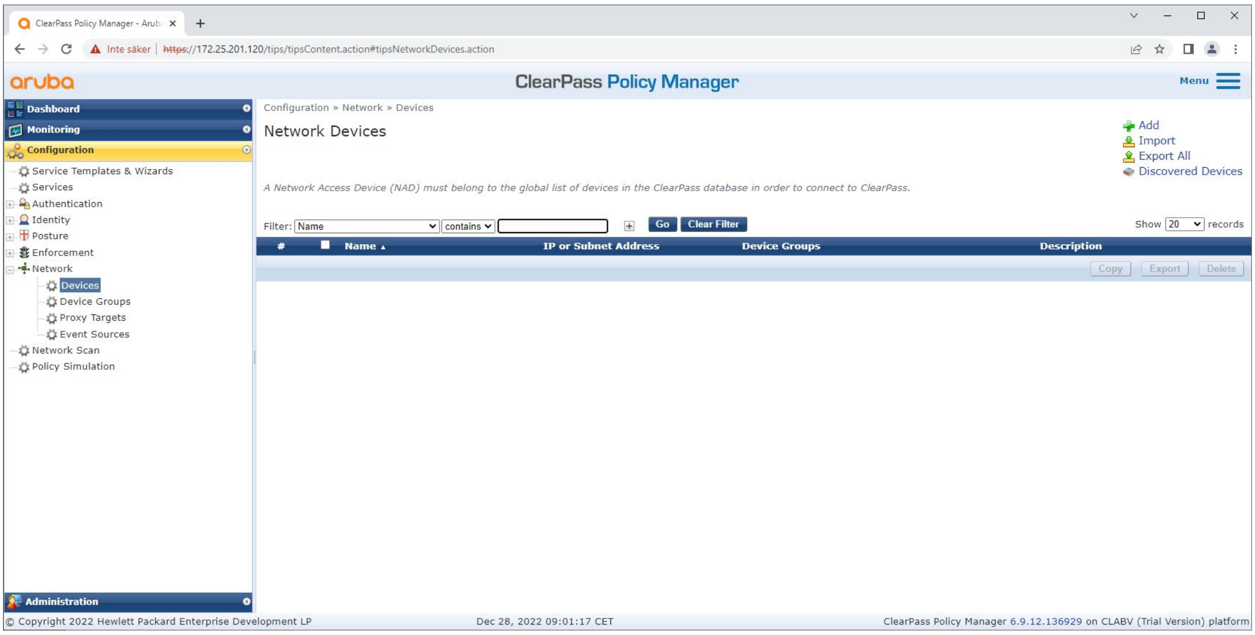
The trusted certificate store in Aruba ClearPass Policy Manager with Axis-specific IEEE 802.1AR certificate chain included.

Network device/group configuration

1. Add trusted network access devices, such as Aruba access switches, to the ClearPass Policy Manager. The ClearPass Policy Manager needs to know which Aruba access switches in the network will be used for IEEE 802.1X communication.

2. Use the network device group configuration to group several trusted network access devices. Grouping trusted network access devices allows easier policy configuration.

3. The RADIUS shared secret needs to match the specific switch IEEE 802.1X configuration.



Configuration » Network » Devices

Network Devices

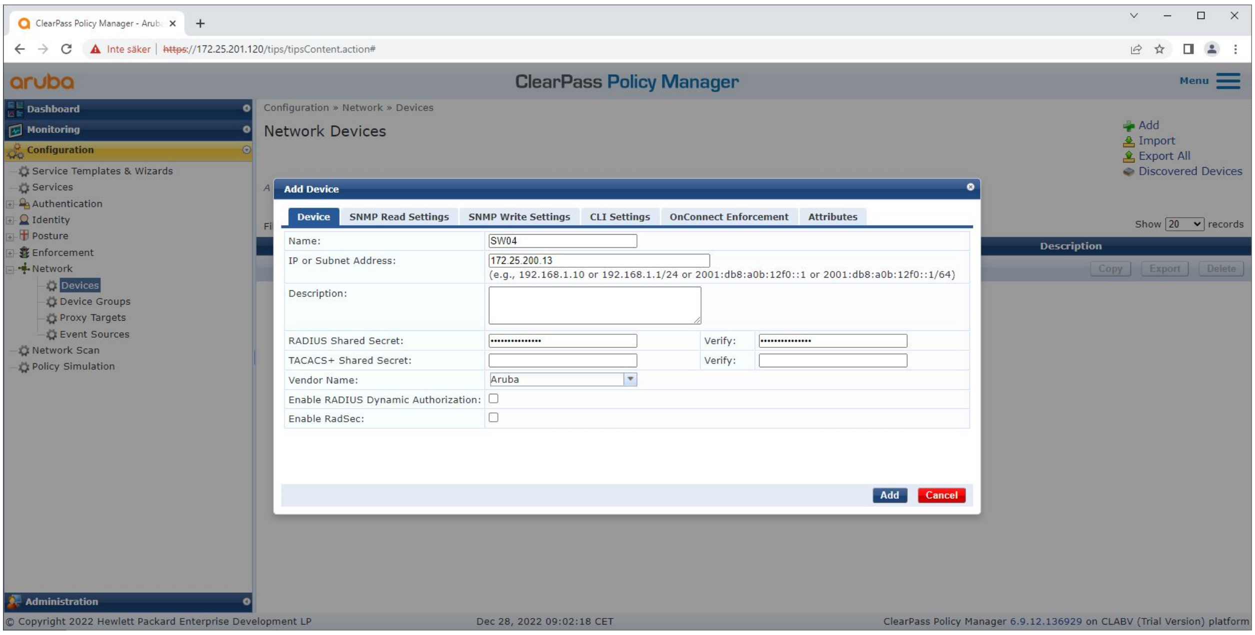
A Network Access Device (NAD) must belong to the global list of devices in the ClearPass database in order to connect to ClearPass.

#	□	Name ▴	IP or Subnet Address	Device Groups	Description

© Copyright 2022 Hewlett Packard Enterprise Development LP   Dec 28, 2022 09:01:17 CET   ClearPass Policy Manager 6.9.12.136929 on CLABV (Trial Version) platform

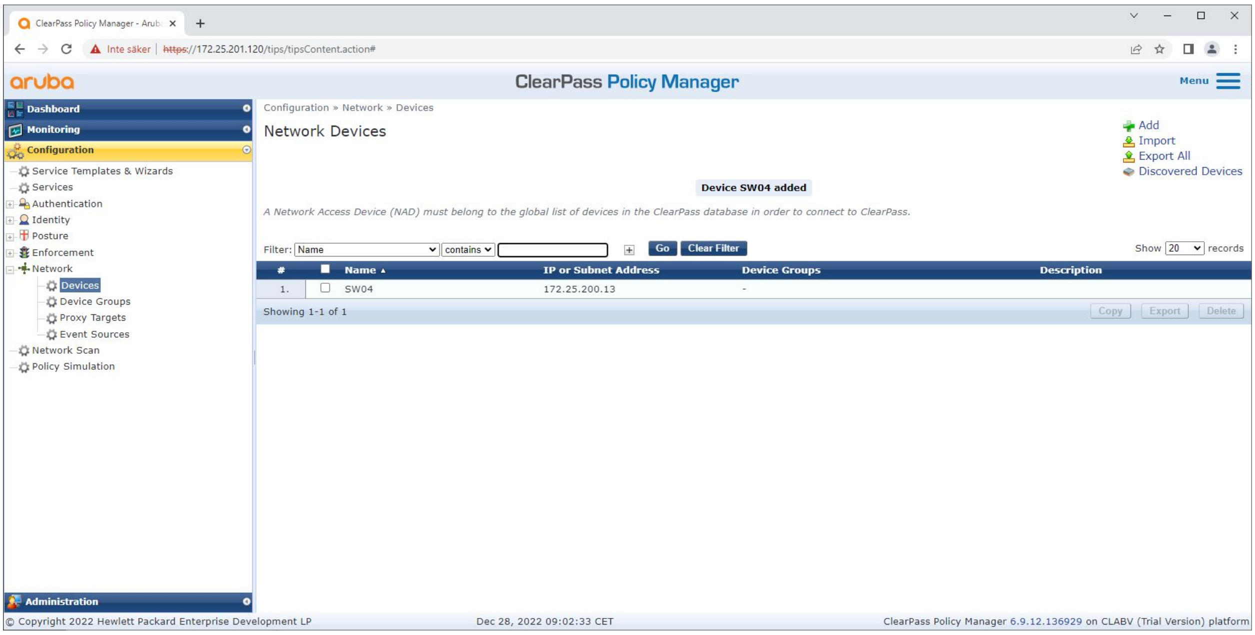
The trusted network devices interface in Aruba ClearPass Policy Manager.

Secure onboarding - IEEE 802.1AR/802.1X



Name:	SW04		
IP or Subnet Address:	172.25.200.13 (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)		
Description:			
RADIUS Shared Secret:	•••••••••••••••	Verify:	•••••••••••••••
TACACS+ Shared Secret:		Verify:	
Vendor Name:	Aruba		
Enable RADIUS Dynamic Authorization:	☐		
Enable RadSec:	☐		

Adding the Aruba access switch as trusted network device in Aruba ClearPass Policy Manager. Please note that the RADIUS shared secret needs to match the specific switch IEEE 802.1X configuration.


ClearPass Policy Manager - Arub
https://172.25.201.120/tips/tipsContent.action#
aruba
ClearPass Policy Manager
Menu
Dashboard
Monitoring
Configuration
Service Templates & Wizards
Services
Authentication
Identity
Posture
Enforcement
Network
Devices
Device Groups
Proxy Targets
Event Sources
Network Scan
Policy Simulation
Administration
Configuration » Network » Devices
Network Devices
Add
Import
Export All
Discovered Devices
Go
Clear Filter
Copy
Export
Delete
© Copyright 2022 Hewlett Packard Enterprise Development LP
Dec 28, 2022 09:02:33 CET
ClearPass Policy Manager 6.9.12.136929 on CLABV (Trial Version) platform

Device SW04 added

A Network Access Device (NAD) must belong to the global list of devices in the ClearPass database in order to connect to ClearPass.

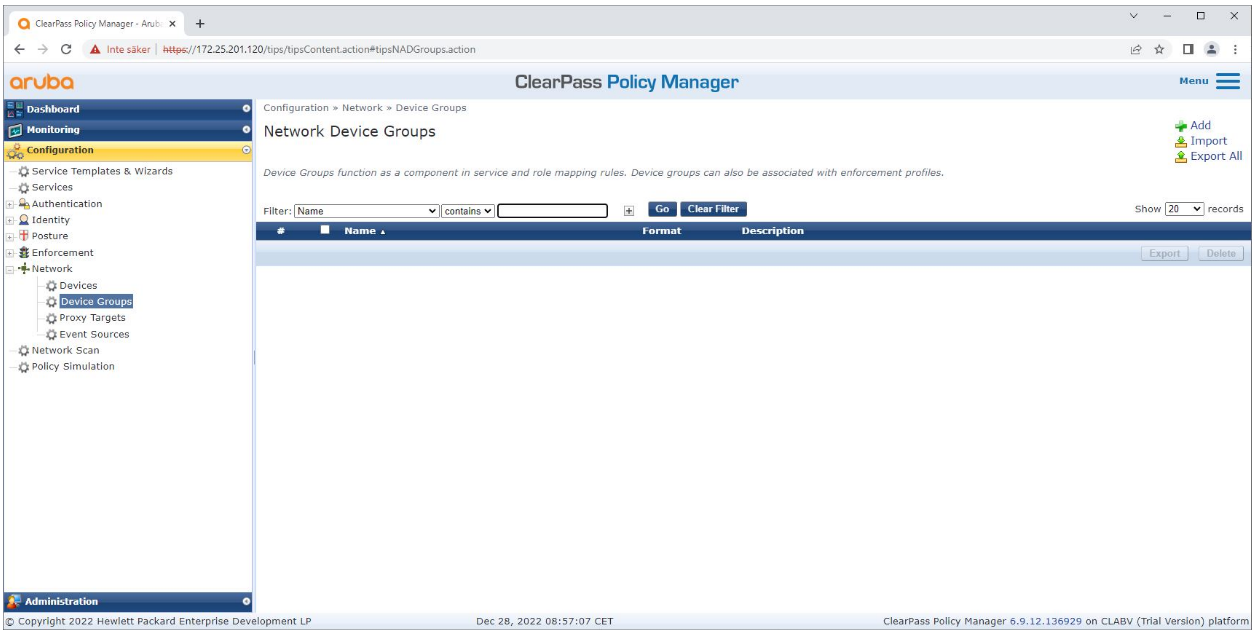
Filter: Name contains   Show 20 records

#	☐	Name ▴	IP or Subnet Address	Device Groups	Description
1.	☐	SW04	172.25.200.13	-	

Showing 1-1 of 1

The Aruba ClearPass Policy Manager with one trusted network device configured.

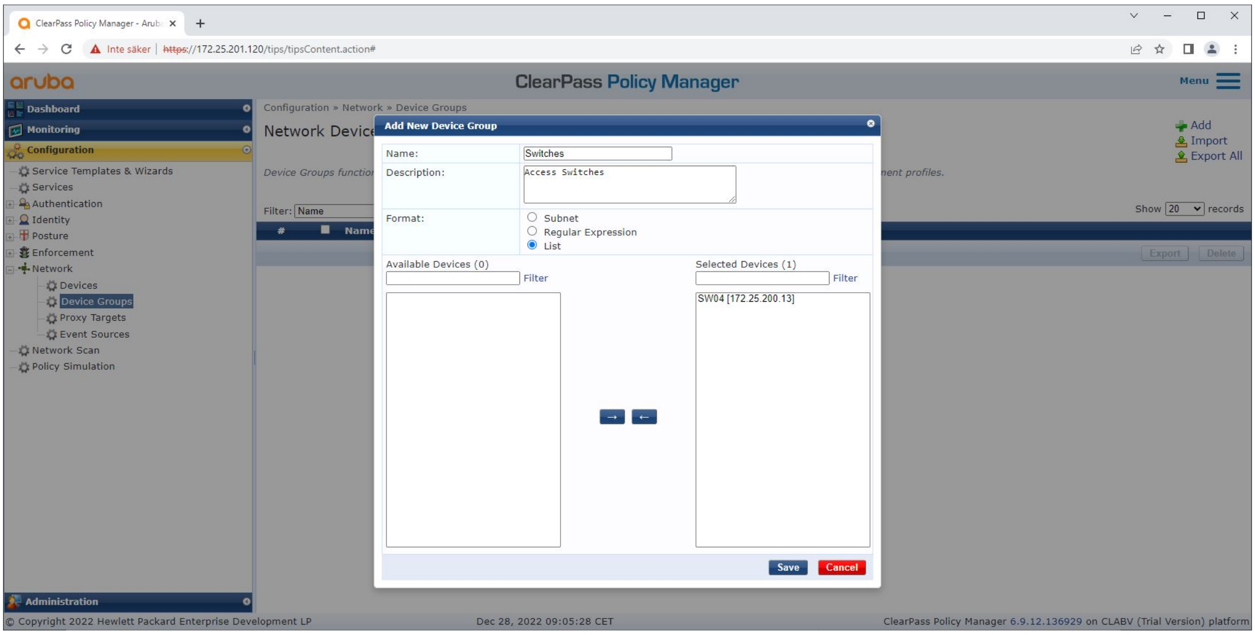
Secure onboarding - IEEE 802.1AR/802.1X



Device Groups function as a component in service and role mapping rules. Device groups can also be associated with enforcement profiles.

© Copyright 2022 Hewlett Packard Enterprise Development LP Dec 28, 2022 08:57:07 CET ClearPass Policy Manager 6.9.12.136929 on CLABV (Trial Version) platform

The trusted network device groups interface in Aruba ClearPass Policy Manager.



Name: Switches

Description: Access Switches

Format: ○ Subnet ○ Regular Expression ● List

Available Devices (0)

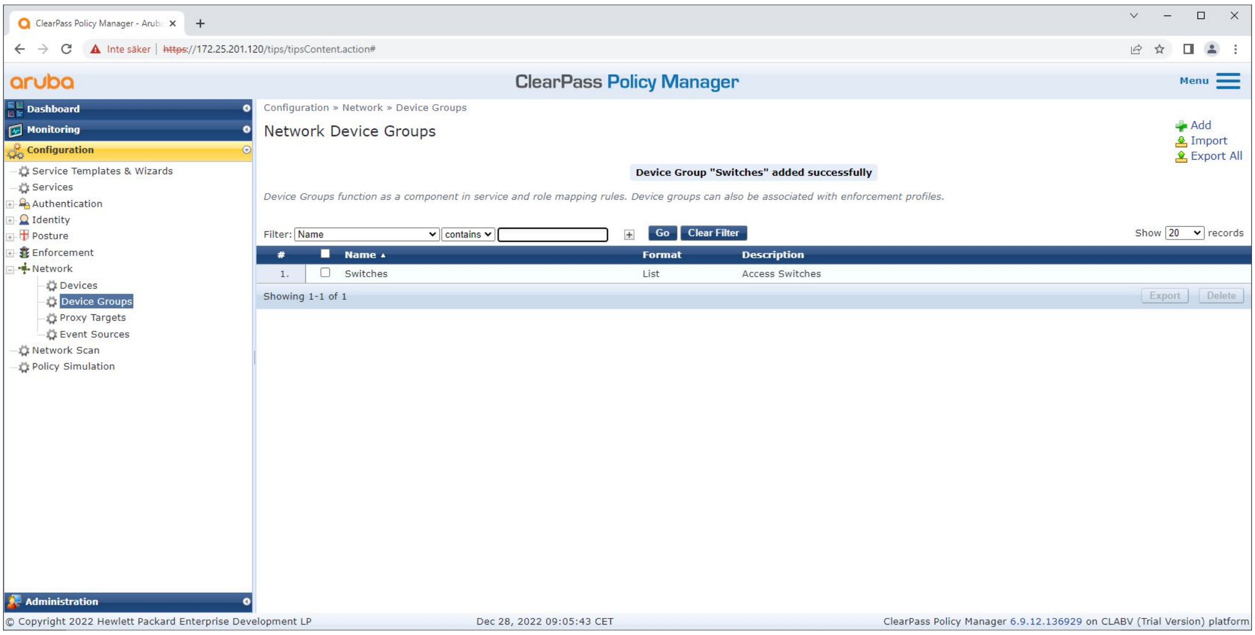
Selected Devices (1)

SW04 [172.25.200.13]

© Copyright 2022 Hewlett Packard Enterprise Development LP Dec 28, 2022 09:05:28 CET ClearPass Policy Manager 6.9.12.136929 on CLABV (Trial Version) platform

Adding a trusted network access device into a new device group in Aruba ClearPass Policy Manager.

Secure onboarding - IEEE 802.1AR/802.1X



Configuration » Network » Device Groups

Network Device Groups

Device Group "Switches" added successfully

Device Groups function as a component in service and role mapping rules. Device groups can also be associated with enforcement profiles.

Filter: Name contains   Show 20 records

#	□	Name ▴	Format	Description
1.	□	Switches	List	Access Switches

Showing 1-1 of 1

© Copyright 2022 Hewlett Packard Enterprise Development LP   Dec 28, 2022 09:05:43 CET   ClearPass Policy Manager 6.9.12.136929 on CLABV (Trial Version) platform

The Aruba ClearPass Policy Manager with configured network device group that includes one or several trusted network devices.

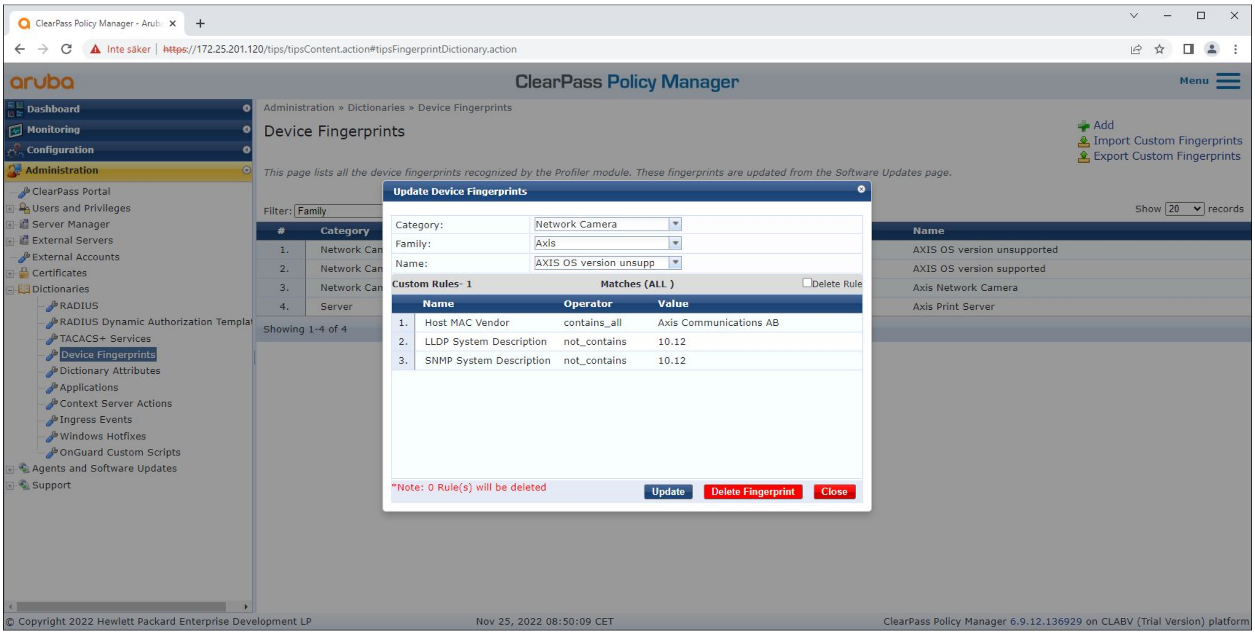
Device fingerprint configuration

The Axis device can distribute device specific information, such as MAC-address and firmware version, through network discovery. A device fingerprint can be created from the device fingerprints interface in the Aruba ClearPass Policy Manager. It is possible to update and manage the Device Fingerprint. One of the things that is possible to do is to grant or deny access depending on the AXIS OS version.

It is possible to update and manage the Device Fingerprint. One of the things that is possible to do is to grant or deny access depending on the AXIS OS version.

1. Go to **Administration** > **Dictionaries** > **Device Fingerprints**.
2. Select an existing device fingerprint or create a new device fingerprint.
3. Set the Device Fingerprint settings.

Secure onboarding - IEEE 802.1AR/802.1X



Administration » Dictionaries » Device Fingerprints

Device Fingerprints

This page lists all the device fingerprints recognized by the Profiler module. These fingerprints are updated from the Software Updates page.

Filter: Family

Show 20 records

#	Category	Name
1.	Network Can	AXIS OS version unsupported
2.	Network Can	AXIS OS version supported
3.	Network Can	Axis Network Camera
4.	Server	Axis Print Server

Showing 1-4 of 4

Update Device Fingerprints

Category:	Network Camera
Family:	Axis
Name:	AXIS OS version unsupp

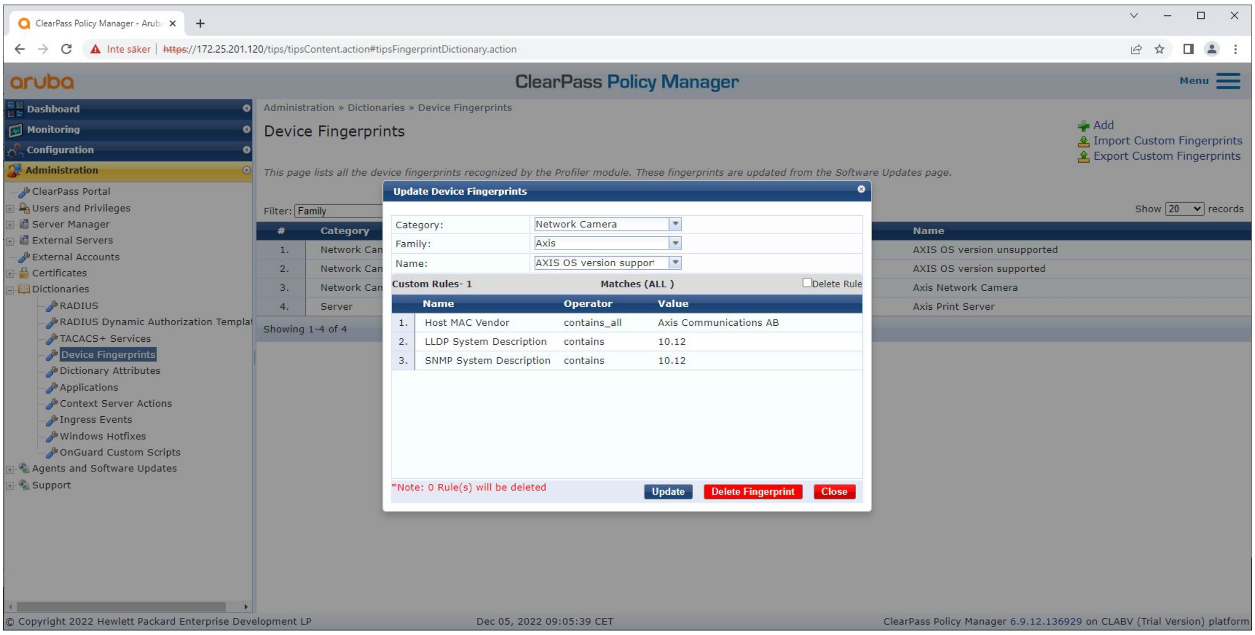
Custom Rules- 1 Matches (ALL) □Delete Rule

	Name	Operator	Value
1.	Host MAC Vendor	contains_all	Axis Communications AB
2.	LLDP System Description	not_contains	10.12
3.	SNMP System Description	not_contains	10.12

*Note: 0 Rule(s) will be deleted

© Copyright 2022 Hewlett Packard Enterprise Development LP Nov 25, 2022 08:50:09 CET ClearPass Policy Manager 6.9.12.136929 on CLABV (Trial Version) platform

The device fingerprint configuration in Aruba ClearPass Policy Manager. Axis devices running any other firmware version other than 10.12 are considered unsupported.



Administration » Dictionaries » Device Fingerprints

Device Fingerprints

This page lists all the device fingerprints recognized by the Profiler module. These fingerprints are updated from the Software Updates page.

Filter: Family

Show 20 records

#	Category	Name
1.	Network Can	AXIS OS version unsupported
2.	Network Can	AXIS OS version supported
3.	Network Can	Axis Network Camera
4.	Server	Axis Print Server

Showing 1-4 of 4

Update Device Fingerprints

Category:	Network Camera
Family:	Axis
Name:	AXIS OS version suppor

Custom Rules- 1 Matches (ALL) □Delete Rule

	Name	Operator	Value
1.	Host MAC Vendor	contains_all	Axis Communications AB
2.	LLDP System Description	contains	10.12
3.	SNMP System Description	contains	10.12

*Note: 0 Rule(s) will be deleted

© Copyright 2022 Hewlett Packard Enterprise Development LP Dec 05, 2022 09:05:39 CET ClearPass Policy Manager 6.9.12.136929 on CLABV (Trial Version) platform

The device fingerprint configuration in Aruba ClearPass Policy Manager. Axis devices running firmware 10.12 are considered supported in above example.

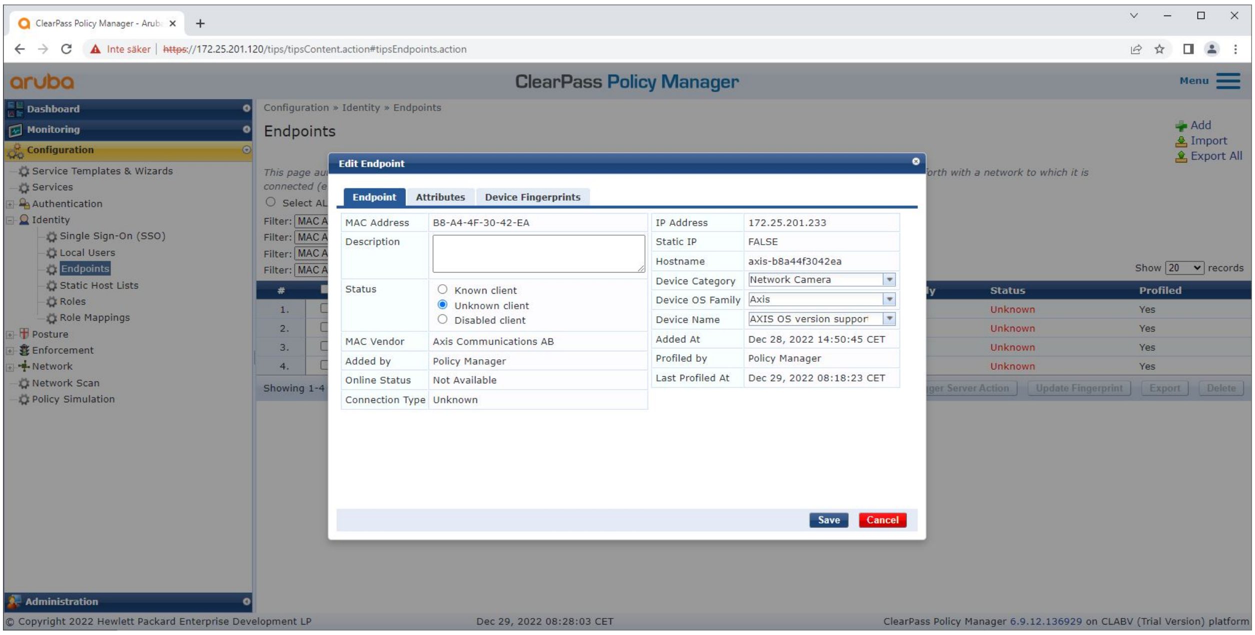
Information about the Device Fingerprint that has been collected by Aruba ClearPass Manager can be found in the Endpoints section.

1. Go to **Configuration > Identity > Endpoints**.
2. Select the device you want to view.
3. Click on the Device Fingerprints tab.

Secure onboarding - IEEE 802.1AR/802.1X

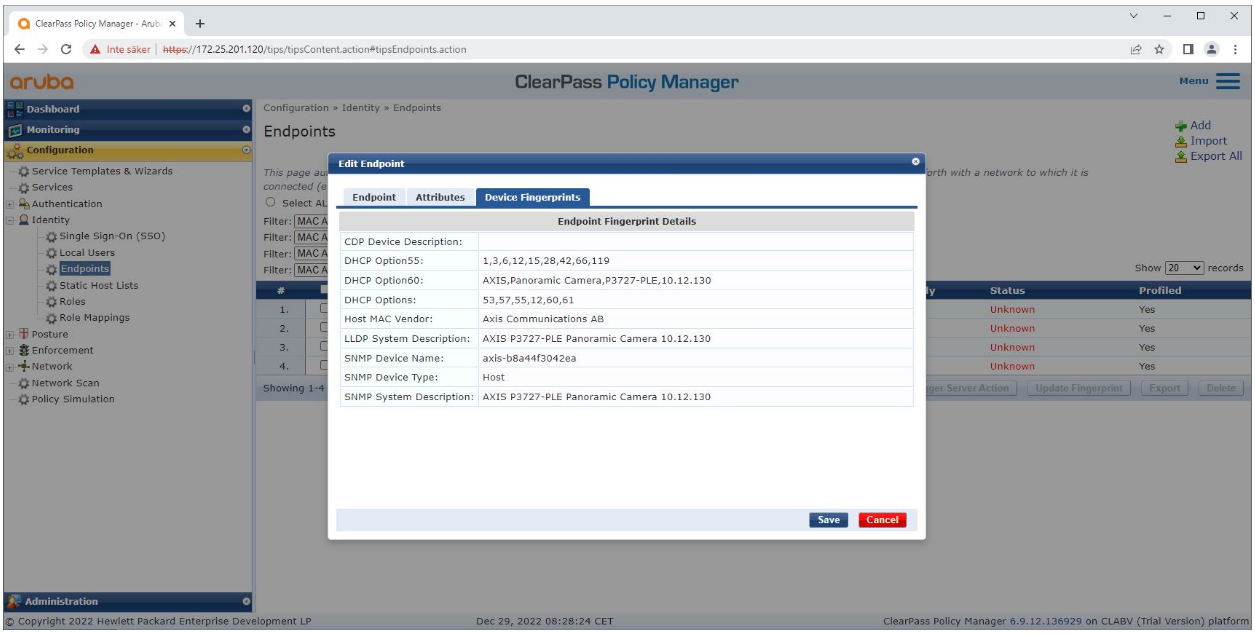
Note

SNMP is disabled by default in Axis devices and collected from the Aruba access switch.


ClearPass Policy Manager - Aruba
Inte säker | https://172.25.201.120/tips/tipsContent.action#tipsEndpoints.action
aruba
ClearPass Policy Manager
Menu
Dashboard
Monitoring
Configuration
Service Templates & Wizards
Services
Authentication
Identity
Single Sign-On (SSO)
Local Users
Endpoints
Static Host Lists
Roles
Role Mappings
Posture
Enforcement
Network
Network Scan
Policy Simulation
Administration
Configuration » Identity » Endpoints
Endpoints
Add
Import
Export All
Edit Endpoint
Endpoint
Attributes
Device Fingerprints
Save
Cancel
© Copyright 2022 Hewlett Packard Enterprise Development LP
Dec 29, 2022 08:28:03 CET
ClearPass Policy Manager 6.9.12.136929 on CLABV (Trial Version) platform

MAC Address	B8-A4-4F-30-42-EA	IP Address	172.25.201.233
Description		Static IP	FALSE
		Hostname	axis-b8a44f3042ea
Status	○ Known client ● Unknown client ○ Disabled client	Device Category	Network Camera
		Device OS Family	Axis
		Device Name	AXIS OS version suppor
MAC Vendor	Axis Communications AB	Added At	Dec 28, 2022 14:50:45 CET
Added by	Policy Manager	Profiled by	Policy Manager
Online Status	Not Available	Last Profiled At	Dec 29, 2022 08:18:23 CET
Connection Type	Unknown		

An Axis device that has been profiled by the Aruba ClearPass Policy Manager.


ClearPass Policy Manager - Aruba
Inte säker | https://172.25.201.120/tips/tipsContent.action#tipsEndpoints.action
aruba
ClearPass Policy Manager
Menu
Dashboard
Monitoring
Configuration
Service Templates & Wizards
Services
Authentication
Identity
Single Sign-On (SSO)
Local Users
Endpoints
Static Host Lists
Roles
Role Mappings
Posture
Enforcement
Network
Network Scan
Policy Simulation
Administration
Configuration » Identity » Endpoints
Endpoints
Add
Import
Export All
Edit Endpoint
Endpoint
Attributes
Device Fingerprints
Save
Cancel
© Copyright 2022 Hewlett Packard Enterprise Development LP
Dec 29, 2022 08:28:24 CET
ClearPass Policy Manager 6.9.12.136929 on CLABV (Trial Version) platform

Endpoint Fingerprint Details

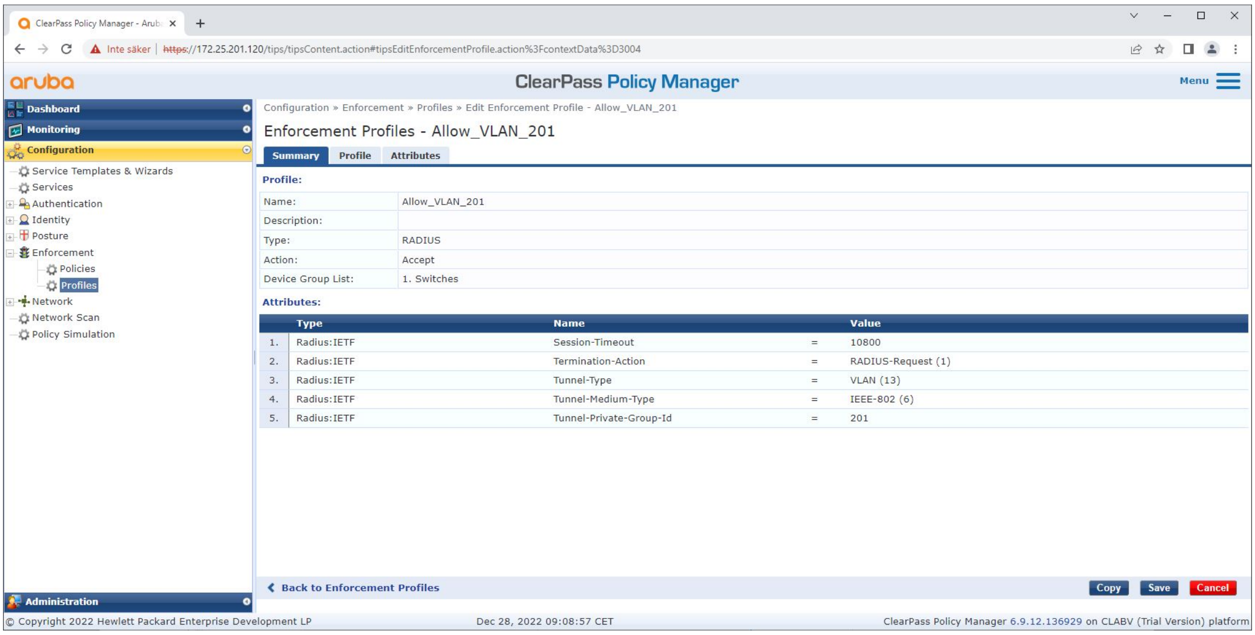
CDP Device Description:	
DHCP Option55:	1,3,6,12,15,28,42,66,119
DHCP Option60:	AXIS,Panoramic Camera,P3727-PLE,10.12.130
DHCP Options:	53,57,55,12,60,61
Host MAC Vendor:	Axis Communications AB
LLDP System Description:	AXIS P3727-PLE Panoramic Camera 10.12.130
SNMP Device Name:	axis-b8a44f3042ea
SNMP Device Type:	Host
SNMP System Description:	AXIS P3727-PLE Panoramic Camera 10.12.130

The detailed device fingerprints of a profiled Axis device. Please note that SNMP is disabled by default in Axis devices. LLDP, CDP and DHCP-specific discovery information are shared by the Axis device in factory defaulted state and relayed by the Aruba access switch to the ClearPass Policy Manager.

Enforcement profile configuration

The Enforcement Profile is used to allow the Aruba ClearPass Policy Manager to assign a specific VLAN ID to an access port on the switch. It is a policy-based decision that applies to the network devices in the device group "switches". The necessary number of enforcement profiles depends on the number of VLANs that will be used. In our setup there is a total of three VLANs (VLAN 201, 202, 203), that correlates to three enforcement profiles.

After the enforcement profiles for the VLAN are configured, the actual enforcement policy can be configured. The enforcement policy configuration in the Aruba ClearPass Policy Manager defines if Axis devices are granted access to Aruba networks based on four example policy profiles.


ClearPass Policy Manager - Arub
Inte säker
https://172.25.201.120/tips/tipsContent.action#tipsEditEnforcementProfile.action%3FcontextData%3D3004
aruba
ClearPass Policy Manager
Menu
Dashboard
Monitoring
Configuration
Service Templates & Wizards
Services
Authentication
Identity
Posture
Enforcement
Policies
Profiles
Network
Network Scan
Policy Simulation
Administration
Configuration » Enforcement » Profiles » Edit Enforcement Profile - Allow_VLAN_201
Summary
Profile
Attributes
Back to Enforcement Profiles
Copy
Save
Cancel
© Copyright 2022 Hewlett Packard Enterprise Development LP
Dec 28, 2022 09:08:57 CET
ClearPass Policy Manager 6.9.12.136929 on CLABV (Trial Version) platform

Enforcement Profiles - Allow_VLAN_201

Profile:

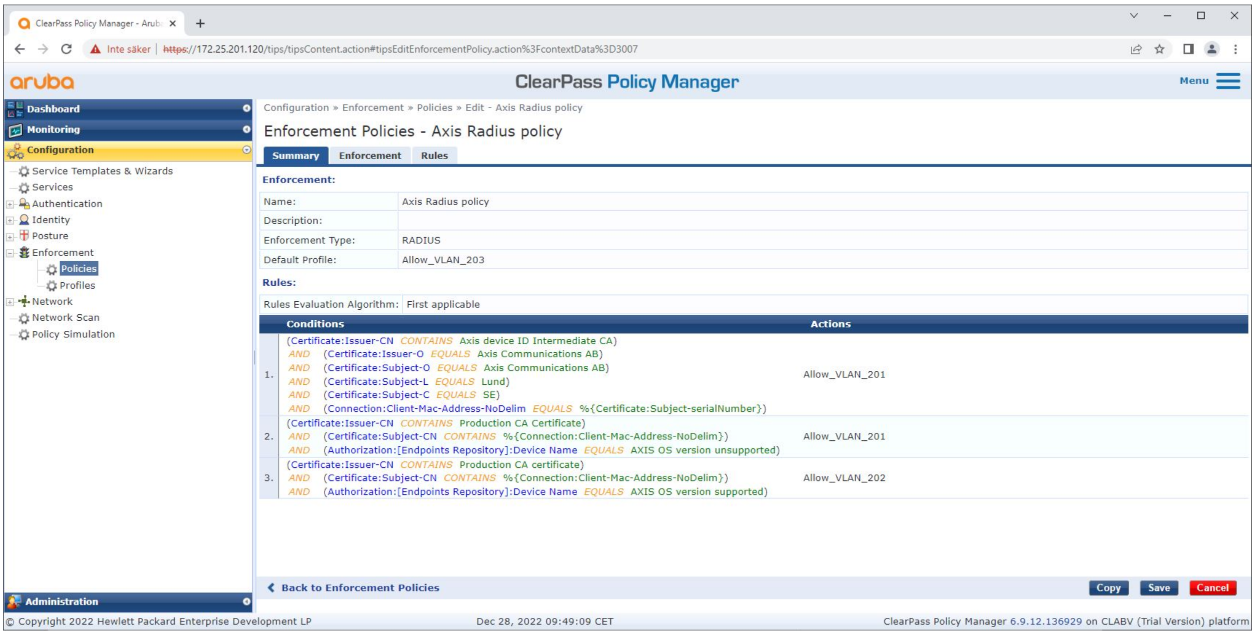
Name:	Allow_VLAN_201
Description:	
Type:	RADIUS
Action:	Accept
Device Group List:	1. Switches

Attributes:

	Type	Name		Value
1.	Radius:IETF	Session-Timeout	=	10800
2.	Radius:IETF	Termination-Action	=	RADIUS-Request (1)
3.	Radius:IETF	Tunnel-Type	=	VLAN (13)
4.	Radius:IETF	Tunnel-Medium-Type	=	IEEE-802 (6)
5.	Radius:IETF	Tunnel-Private-Group-Id	=	201

An example enforcement profile to allow access to VLAN 201.

Secure onboarding - IEEE 802.1AR/802.1X


ClearPass Policy Manager - Arub
Inte säker | https://172.25.201.120/tips/tipsContent.action#tipsEditEnforcementPolicy.action%3FcontextData%3D3007
aruba
ClearPass Policy Manager
Menu
Dashboard
Monitoring
Configuration
Service Templates & Wizards
Services
Authentication
Identity
Posture
Enforcement
Policies
Profiles
Network
Network Scan
Policy Simulation
Administration
Configuration » Enforcement » Policies » Edit - Axis Radius policy
Summary
Enforcement
Rules
Back to Enforcement Policies
Copy
Save
Cancel
© Copyright 2022 Hewlett Packard Enterprise Development LP
Dec 28, 2022 09:49:09 CET
ClearPass Policy Manager 6.9.12.136929 on CLABV (Trial Version) platform

Enforcement Policies - Axis Radius policy

Enforcement:

Name:	Axis Radius policy
Description:	
Enforcement Type:	RADIUS
Default Profile:	Allow_VLAN_203

Rules:

Rules Evaluation Algorithm: First applicable

	Conditions	Actions
1.	(Certificate:Issuer-CN *CONTAINS* Axis device ID Intermediate CA) *AND* (Certificate:Issuer-O *EQUALS* Axis Communications AB) *AND* (Certificate:Subject-O *EQUALS* Axis Communications AB) *AND* (Certificate:Subject-L *EQUALS* Lund) *AND* (Certificate:Subject-C *EQUALS* SE) *AND* (Connection:Client-Mac-Address-NoDelim *EQUALS* %{Certificate:Subject-serialNumber})	Allow_VLAN_201
2.	(Certificate:Issuer-CN *CONTAINS* Production CA Certificate) *AND* (Certificate:Subject-CN *CONTAINS* %{Connection:Client-Mac-Address-NoDelim}) *AND* (Authorization:[Endpoints Repository]:Device Name *EQUALS* AXIS OS version unsupported)	Allow_VLAN_201
3.	(Certificate:Issuer-CN *CONTAINS* Production CA certificate) *AND* (Certificate:Subject-CN *CONTAINS* %{Connection:Client-Mac-Address-NoDelim}) *AND* (Authorization:[Endpoints Repository]:Device Name *EQUALS* AXIS OS version supported)	Allow_VLAN_202

The enforcement policy configuration in Aruba ClearPass Policy Manager.

The four enforcement policies and their actions are listed below:

Denied network access

Access to the network is denied when no IEEE 802.1X network access control authentication is performed.

Guest-network (VLAN 203)

The Axis device is granted access to a limited, isolated network if the IEEE 802.1X network access control authentication fails. Manual inspection of the device is required to take appropriate actions.

Provisioning network (VLAN 201)

The Axis device is granted access to a provisioning network. This is to provide Axis device management capabilities through *Axis Device Manager* and *Axis Device Manager Extend*. It also makes it possible to configure Axis devices with firmware updates, production-grade certificates, and other configurations. The following conditions are verified by the Aruba ClearPass Policy Manager:

- The Axis device's firmware version.
- The MAC-address of the device matches the vendor-specific Axis MACaddress scheme with the serial number attribute of the Axis device ID certificate.
- The Axis device ID certificate is verifiable and matches the Axis-specific attributes such as issuer, organization, location, country.

Production network (VLAN 202)

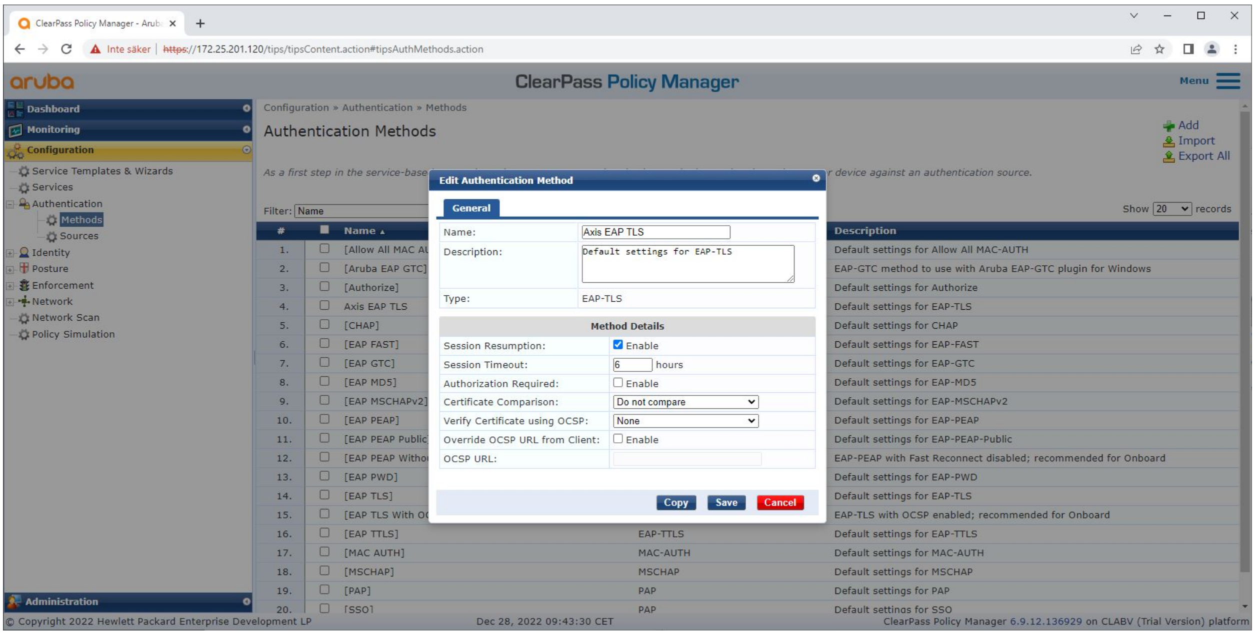
The Axis device is granted access to the production network where the Axis device will operate in. Access is granted after the device provisioning is completed from within the provisioning network (VLAN 201). The following conditions are verified by the Aruba ClearPass Policy Manager:

- The MAC-address of the device matches the vendor-specific Axis MAC address scheme with the serial number attribute of the Axis device ID certificate.
- The Axis device's firmware version.
- The production-grade certificate is verifiable by the trusted certificate store.

Secure onboarding - IEEE 802.1AR/802.1X

Authentication method configuration

In the authentication method it is defined how an Axis device will attempt to authenticate against the Aruba network. The preferred method of authentication should be IEEE 802.1X EAP-TLS since Axis devices with support for Axis Edge Vault come with IEEE 802.1X EAP-TLS enabled by default.



Authentication Methods

As a first step in the service-base… r device against an authentication source.

Edit Authentication Method

Name:	Axis EAP TLS
Description:	Default settings for EAP-TLS
Type:	EAP-TLS

Method Details

Session Resumption:	☑ Enable
Session Timeout:	6 hours
Authorization Required:	☐ Enable
Certificate Comparison:	Do not compare
Verify Certificate using OCSP:	None
Override OCSP URL from Client:	☐ Enable
OCSP URL:	

#	☐	Name ▲	Type	Description
1.	☐	[Allow All MAC AU		Default settings for Allow All MAC-AUTH
2.	☐	[Aruba EAP GTC]		EAP-GTC method to use with Aruba EAP-GTC plugin for Windows
3.	☐	[Authorize]		Default settings for Authorize
4.	☐	Axis EAP TLS		Default settings for EAP-TLS
5.	☐	[CHAP]		Default settings for CHAP
6.	☐	[EAP FAST]		Default settings for EAP-FAST
7.	☐	[EAP GTC]		Default settings for EAP-GTC
8.	☐	[EAP MD5]		Default settings for EAP-MD5
9.	☐	[EAP MSCHAPv2]		Default settings for EAP-MSCHAPv2
10.	☐	[EAP PEAP]		Default settings for EAP-PEAP
11.	☐	[EAP PEAP Public]		Default settings for EAP-PEAP-Public
12.	☐	[EAP PEAP Witho		EAP-PEAP with Fast Reconnect disabled; recommended for Onboard
13.	☐	[EAP PWD]		Default settings for EAP-PWD
14.	☐	[EAP TLS]		Default settings for EAP-TLS
15.	☐	[EAP TLS With OC		EAP-TLS with OCSP enabled; recommended for Onboard
16.	☐	[EAP TTLS]	EAP-TTLS	Default settings for EAP-TTLS
17.	☐	[MAC AUTH]	MAC-AUTH	Default settings for MAC-AUTH
18.	☐	[MSCHAP]	MSCHAP	Default settings for MSCHAP
19.	☐	[PAP]	PAP	Default settings for PAP
20.	☐	[SSO]	PAP	Default settings for SSO

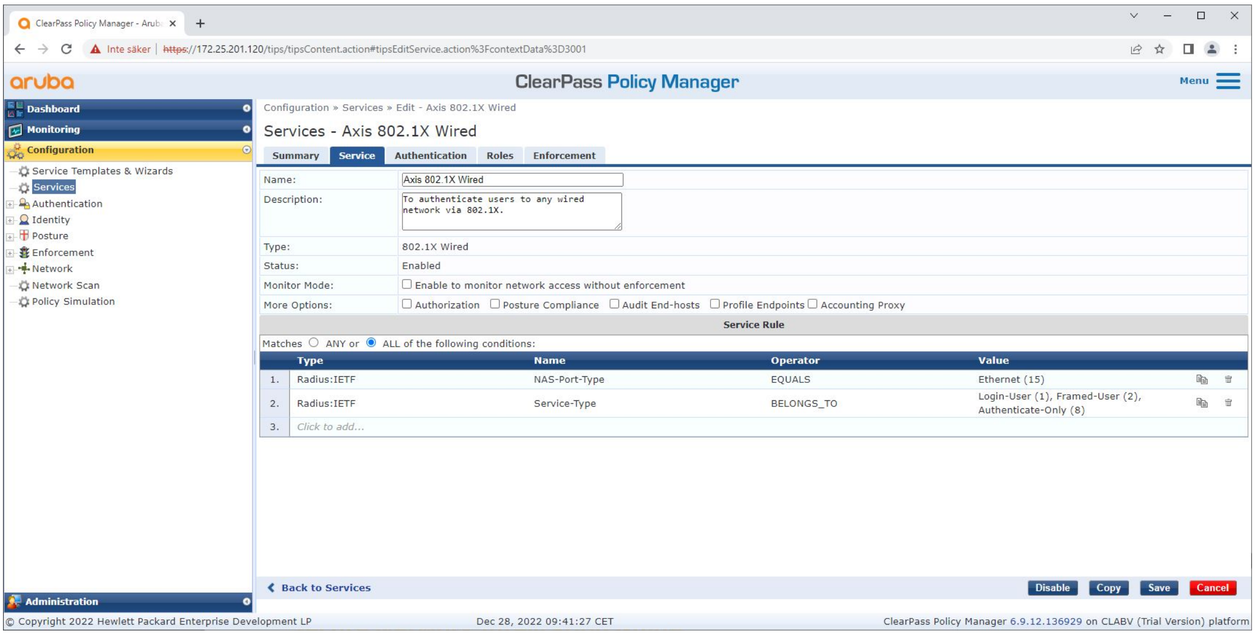
© Copyright 2022 Hewlett Packard Enterprise Development LP
Dec 28, 2022 09:43:30 CET
ClearPass Policy Manager 6.9.12.136929 on CLABV (Trial Version) platform

The authentication method interface of the Aruba ClearPass Policy Manager where the EAP-TLS authentication method for Axis devices is defined.

Service configuration

In the Services interface, the configuration steps are combined into one single service that handles the authentication and authorization of Axis devices in Aruba networks.

Secure onboarding - IEEE 802.1AR/802.1X



Services - Axis 802.1X Wired

Name:	Axis 802.1X Wired
Description:	To authenticate users to any wired network via 802.1X.
Type:	802.1X Wired
Status:	Enabled
Monitor Mode:	□ Enable to monitor network access without enforcement
More Options:	□ Authorization □ Posture Compliance □ Audit End-hosts □ Profile Endpoints □ Accounting Proxy

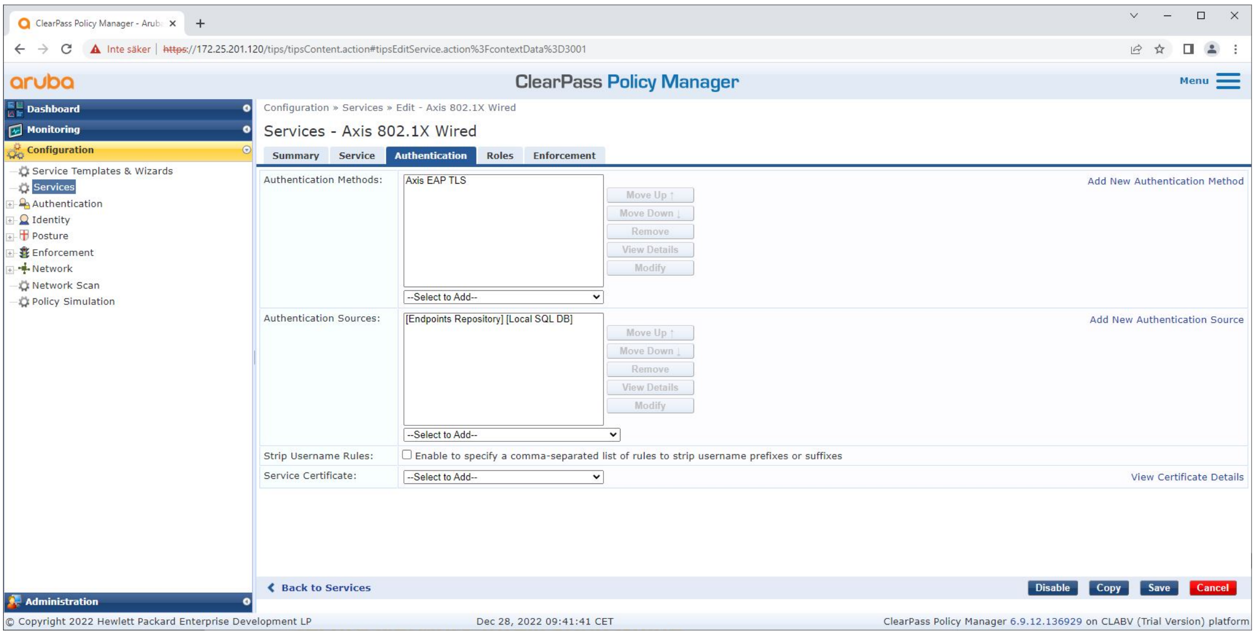
Service Rule

Matches ○ ANY or ● 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)
3.	Click to add...			

© Copyright 2022 Hewlett Packard Enterprise Development LP Dec 28, 2022 09:41:27 CET ClearPass Policy Manager 6.9.12.136929 on CLABV (Trial Version) platform

A dedicated Axis services is created that defines IEEE 802.1X as connection method.

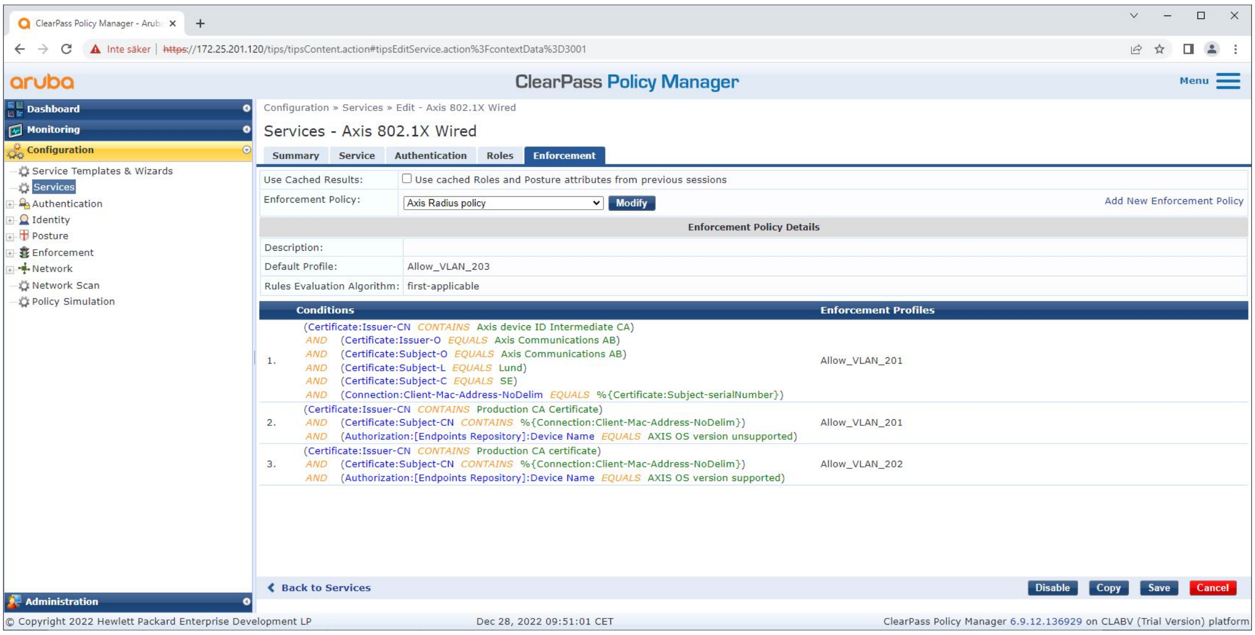


Services - Axis 802.1X Wired

Authentication Methods:	Axis EAP TLS --Select to Add--
Authentication Sources:	[Endpoints Repository] [Local SQL DB] --Select to Add--
Strip Username Rules:	□ Enable to specify a comma-separated list of rules to strip username prefixes or suffixes
Service Certificate:	--Select to Add--

© Copyright 2022 Hewlett Packard Enterprise Development LP Dec 28, 2022 09:41:41 CET ClearPass Policy Manager 6.9.12.136929 on CLABV (Trial Version) platform

In the next step, the earlier created EAP-TLS authentication method is configured to the service.



Configuration » Services » Edit - Axis 802.1X Wired

Services - Axis 802.1X Wired

Use Cached Results: ☐ Use cached Roles and Posture attributes from previous sessions

Enforcement Policy: Axis Radius policy

Enforcement Policy Details

Description:

Default Profile: Allow_VLAN_203

Rules Evaluation Algorithm: first-applicable

	Conditions	Enforcement Profiles
1.	(Certificate:Issuer-CN *CONTAINS* Axis device ID Intermediate CA) *AND* (Certificate:Issuer-O *EQUALS* Axis Communications AB) *AND* (Certificate:Subject-O *EQUALS* Axis Communications AB) *AND* (Certificate:Subject-L *EQUALS* Lund) *AND* (Certificate:Subject-C *EQUALS* SE) *AND* (Connection:Client-Mac-Address-NoDelim *EQUALS* %{Certificate:Subject-serialNumber})	Allow_VLAN_201
2.	(Certificate:Issuer-CN *CONTAINS* Production CA Certificate) *AND* (Certificate:Subject-CN *CONTAINS* %{Connection:Client-Mac-Address-NoDelim}) *AND* (Authorization:[Endpoints Repository]:Device Name *EQUALS* AXIS OS version unsupported)	Allow_VLAN_201
3.	(Certificate:Issuer-CN *CONTAINS* Production CA certificate) *AND* (Certificate:Subject-CN *CONTAINS* %{Connection:Client-Mac-Address-NoDelim}) *AND* (Authorization:[Endpoints Repository]:Device Name *EQUALS* AXIS OS version supported)	Allow_VLAN_202

© Copyright 2022 Hewlett Packard Enterprise Development LP   Dec 28, 2022 09:51:01 CET   ClearPass Policy Manager 6.9.12.136929 on CLABV (Trial Version) platform

In the last step, the earlier created enforcement policy is configured to the service.

Aruba access switch

Axis devices are either directly connected to PoE-capable Aruba access switches or via compatible Axis PoE midspans. To securely onboard Axis devices into Aruba networks, the access switch needs to be configured for IEEE 802.1X communication. The Axis device relays IEEE 802.1x EAP-TLS communication to the Aruba ClearPass Policy Manager that acts as a RADIUS server.

Note

A periodic re-authentication of 300 seconds for the Axis device is configured as well to increase overall port-access security.

Refer to the below example global and port configuration for Aruba access switches.

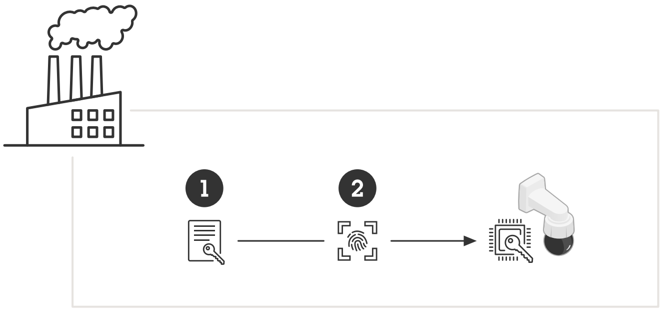
```
radius-server host MyRADIUSIPAddress key "MyRADIUSKey"

aaa authentication port-access eap-radius
aaa port-access authenticator 18-19
aaa port-access authenticator 18 reauth-period 300
aaa port-access authenticator 19 reauth-period 300
aaa port-access authenticator active
```

Configuration Axis

Axis network device

Axis devices with support for *Axis Edge Vault* are manufactured with a secure device identity, called Axis device ID. The Axis device ID is based on the international IEEE 802.1AR standard, which defines a method for automated, secure device identification and network onboarding through IEEE 802.1X.

Secure onboarding - IEEE 802.1AR/802.1X



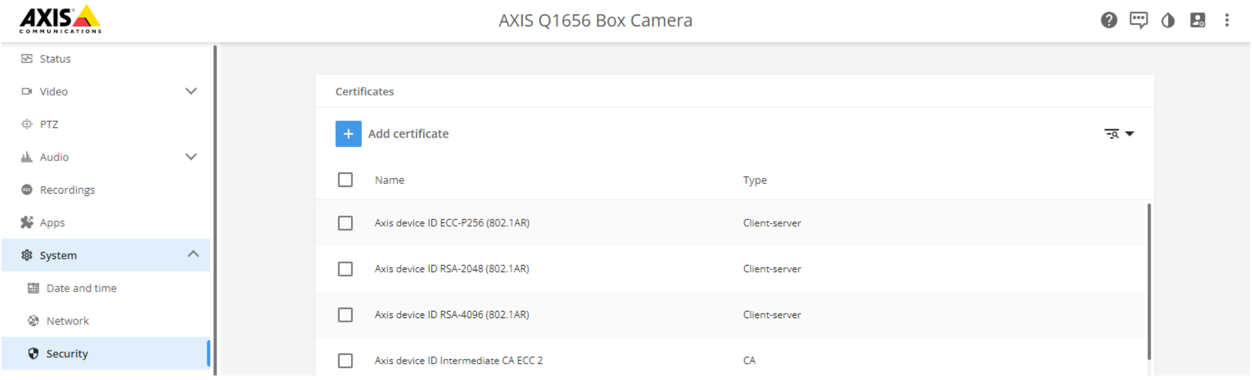
Axis devices are manufactured with the IEEE 802.1AR-compliant Axis device ID certificate for trusted device identity services

1 *Axis device ID key infrastructure (PKI)*
2 *Axis device ID*

The hardware-protected secure keystore provided by a secure element of the Axis device is factory provisioned with a device-unique certificate and corresponding keys (Axis device ID) that globally can prove the authenticity of the Axis device. The *Axis Product Selector* can be used to learn which Axis devices have support for Axis Edge Vault and Axis device ID.

Note

The serial number of an Axis device is its MAC-address.

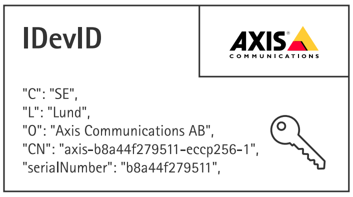


Certificates

Name	Type
Axis device ID ECC-P256 (802.1AR)	Client-server
Axis device ID RSA-2048 (802.1AR)	Client-server
Axis device ID RSA-4096 (802.1AR)	Client-server
Axis device ID Intermediate CA ECC 2	CA

The certificate store of the Axis device in factory defaulted state with Axis Device ID.

The IEEE 802.1AR-compliant Axis device ID certificate includes information about the serial number and other Axis-vendor specific information. The information is used by the Aruba ClearPass Policy Manager for analysis and decision making to grant access to the network. Please refer to the below information that can be obtained from an Axis device ID certificate



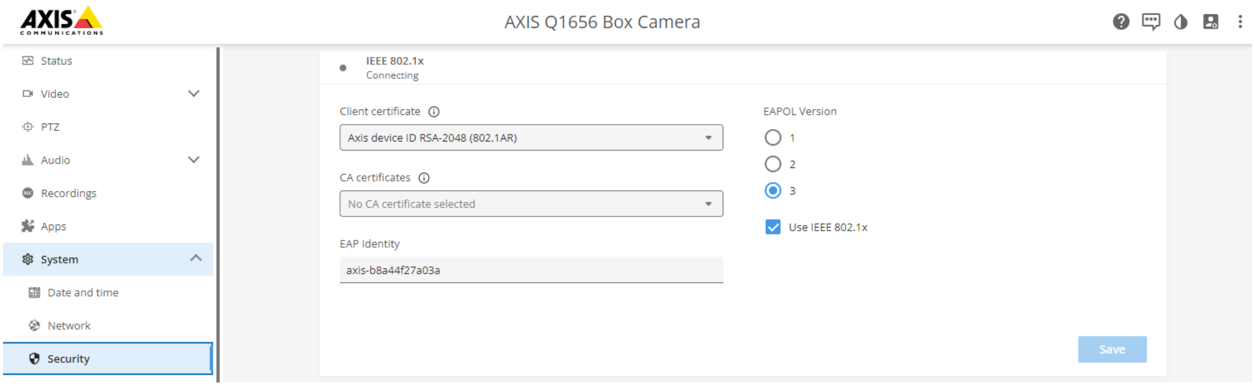
IDevID

"C": "SE",
"L": "Lund",
"O": "Axis Communications AB",
"CN": "axis-b8a44f279511-eccp256-1",
"serialNumber": "b8a44f279511",

Country	SE
Location	Lund
Issuer Organization	Axis Communications AB

Issuer Common Name	Axis device ID intermediate
Organization	Axis Communications AB
Common Name	axis-b8a44f279511-eccp256-1
Serial Number	b8a44f279511

The common name is constructed by a combination of Axis company name, the serial number of the device followed by the crypto algorithm (ECC P256, RSA 2048, RSA 4096) used. Since AXIS OS 10.1 (2020-09), IEEE 802.1X is enabled by default with the Axis device ID pre-configured. This enables the Axis device to authenticate itself onto IEEE 802.1X-enabled networks.



● IEEE 802.1x
Connecting

Client certificate: Axis device ID RSA-2048 (802.1AR)

CA certificates: No CA certificate selected

EAP Identity: axis-b8a44f27a03a

EAPOL Version
○ 1
○ 2
● 3

☑ Use IEEE 802.1x

The Axis device in factory defaulted state with IEEE 802.1X enabled and Axis Device ID certificate pre-selected.

Axis Device Manager

AXIS Device Manager and *AXIS Device Manager Extend* can be used on the network to configure and manage multiple Axis devices in a cost-effective way. Axis Device Manager is a Microsoft Windows-based application that can be installed locally on a machine in the network, while Axis Device Manager Extend relies on cloud infrastructure to do multi-site device management. Both offer easy management and configuration capabilities for Axis devices such as:

- Installation of firmware updates.
- Apply cybersecurity configuration such as HTTPS and IEEE 802.1X certificates.
- Configuration of device-specific settings such as Images Settings and others.

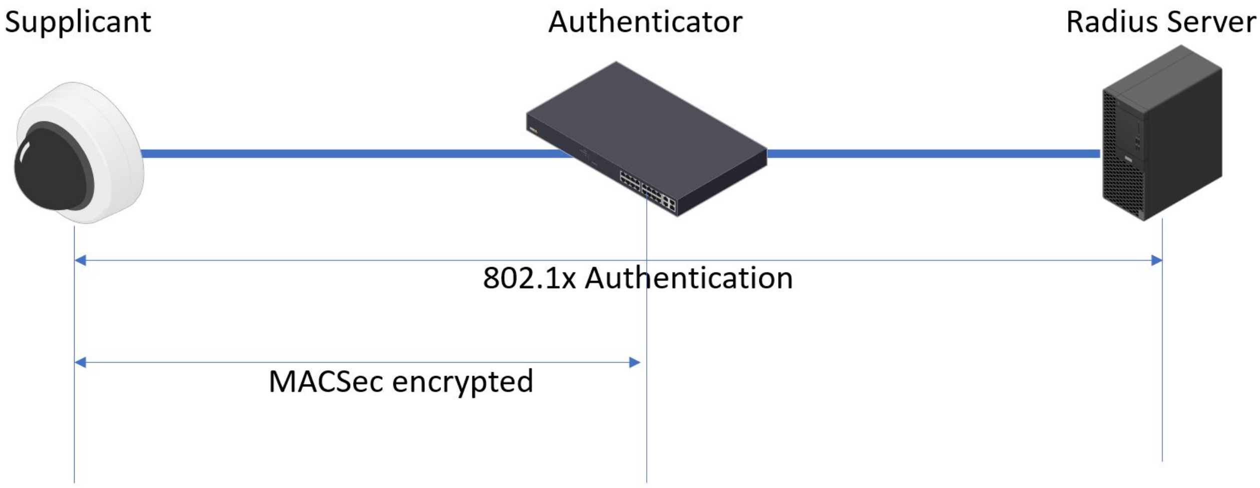
Secure network operation - IEEE 802.1AE MACsec

Secure network operation - IEEE 802.1AE MACsec

IEEE 802.1AE MACsec (Media Access Control Security) is a well-defined network protocol that cryptographically secures point-to-point Ethernet links on network layer 2. It ensures the confidentiality and integrity of data transmissions between two hosts.

The IEEE 802.1AE MACsec standard describes two modes of operation:

- Manually configurable Pre-Shared Key/Static CAK mode
- Automatic Master Session/Dynamic CAK mode using IEEE 802.1X EAP-TLS



In AXIS OS 10.1 (2020-09) and later, IEEE 802.1X is enabled by default for devices that are compatible with Axis device ID. In AXIS OS 11.8 and later, we support MACsec with automatic dynamic mode using IEEE 802.1X EAP-TLS enabled by default. When you connect an Axis device with factory default values, IEEE 802.1X network authentication is performed and when successful, MACsec Dynamic CAK mode is tried as well.

The securely stored Axis device ID (1), an IEEE 802.1AR-compliant secure device identity, is used to authenticate into Aruba network (4, 5) through IEEE 802.1X EAP-TLS port-based network access control (2). Through the EAP-TLS session, MACsec keys are exchanged automatically to set up a secure link (3), protecting all network traffic from the Axis device to the Aruba switch.

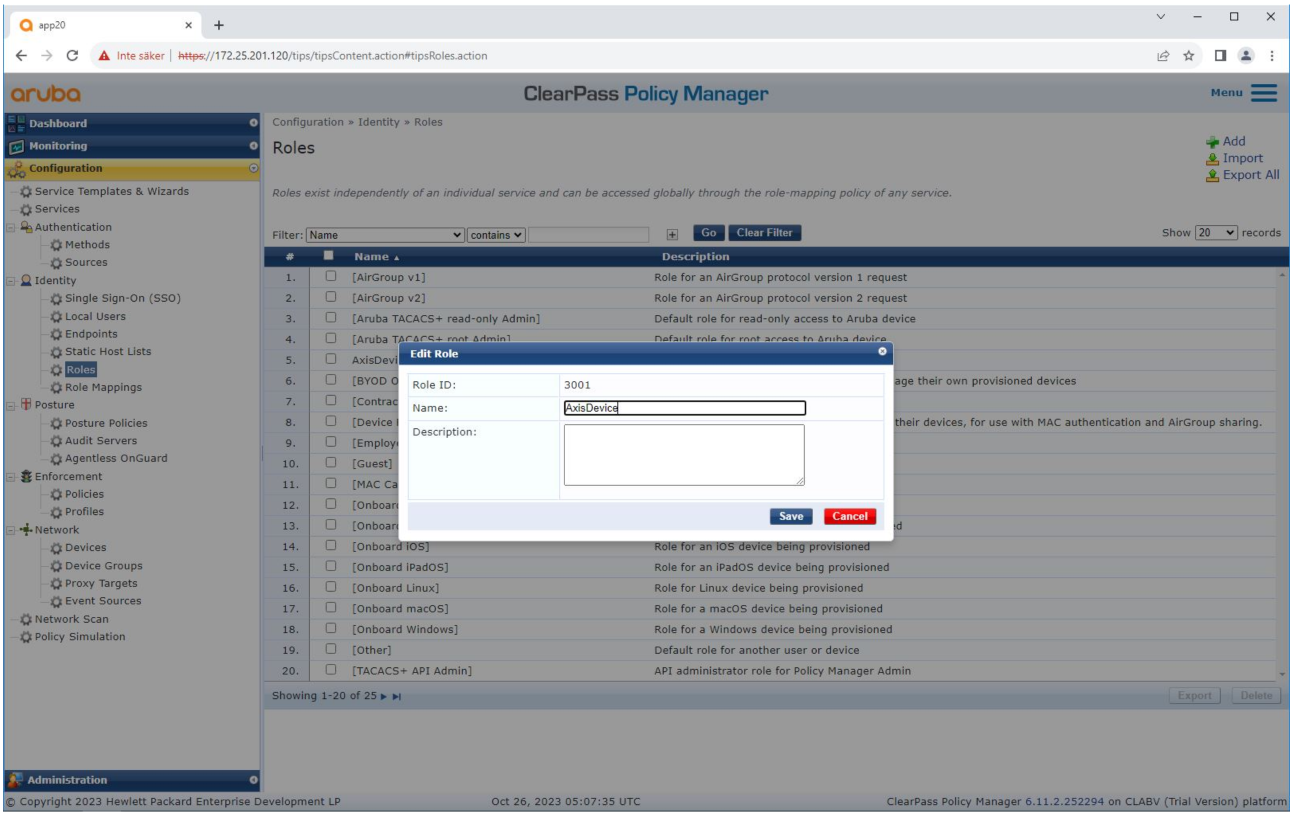
IEEE 802.1AE MACsec requires both Aruba access switch and ClearPass Policy Manager configuration preparations. No configuration is required on the Axis device to allow IEEE 802.1AE MACsec encrypted communication via EAP-TLS.

If the Aruba access switch doesn't support MACsec using EAP-TLS, then the Pre-Shared Key mode can be used and manually configured.

Secure network operation - IEEE 802.1AE MACsec

Aruba ClearPass Policy Manager

Role and role mapping policy



Configuration » Identity » Roles

Roles

Roles exist independently of an individual service and can be accessed globally through the role-mapping policy of any service.

Filter: Name contains Show 20 records

#	□	Name ▴	Description
1.	□	[AirGroup v1]	Role for an AirGroup protocol version 1 request
2.	□	[AirGroup v2]	Role for an AirGroup protocol version 2 request
3.	□	[Aruba TACACS+ read-only Admin]	Default role for read-only access to Aruba device
4.	□	[Aruba TACACS+ root Admin]	Default role for root access to Aruba device
5.	□	AxisDevi	
6.	□	[BYOD O	age their own provisioned devices
7.	□	[Contrac	
8.	□	[Device I	their devices, for use with MAC authentication and AirGroup sharing.
9.	□	[Employ	
10.	□	[Guest]	
11.	□	[MAC Ca	
12.	□	[Onboar	
13.	□	[Onboar	d
14.	□	[Onboard iOS]	Role for an iOS device being provisioned
15.	□	[Onboard iPadOS]	Role for an iPadOS device being provisioned
16.	□	[Onboard Linux]	Role for Linux device being provisioned
17.	□	[Onboard macOS]	Role for a macOS device being provisioned
18.	□	[Onboard Windows]	Role for a Windows device being provisioned
19.	□	[Other]	Default role for another user or device
20.	□	[TACACS+ API Admin]	API administrator role for Policy Manager Admin

Showing 1-20 of 25 ▸ ▸|

Edit Role

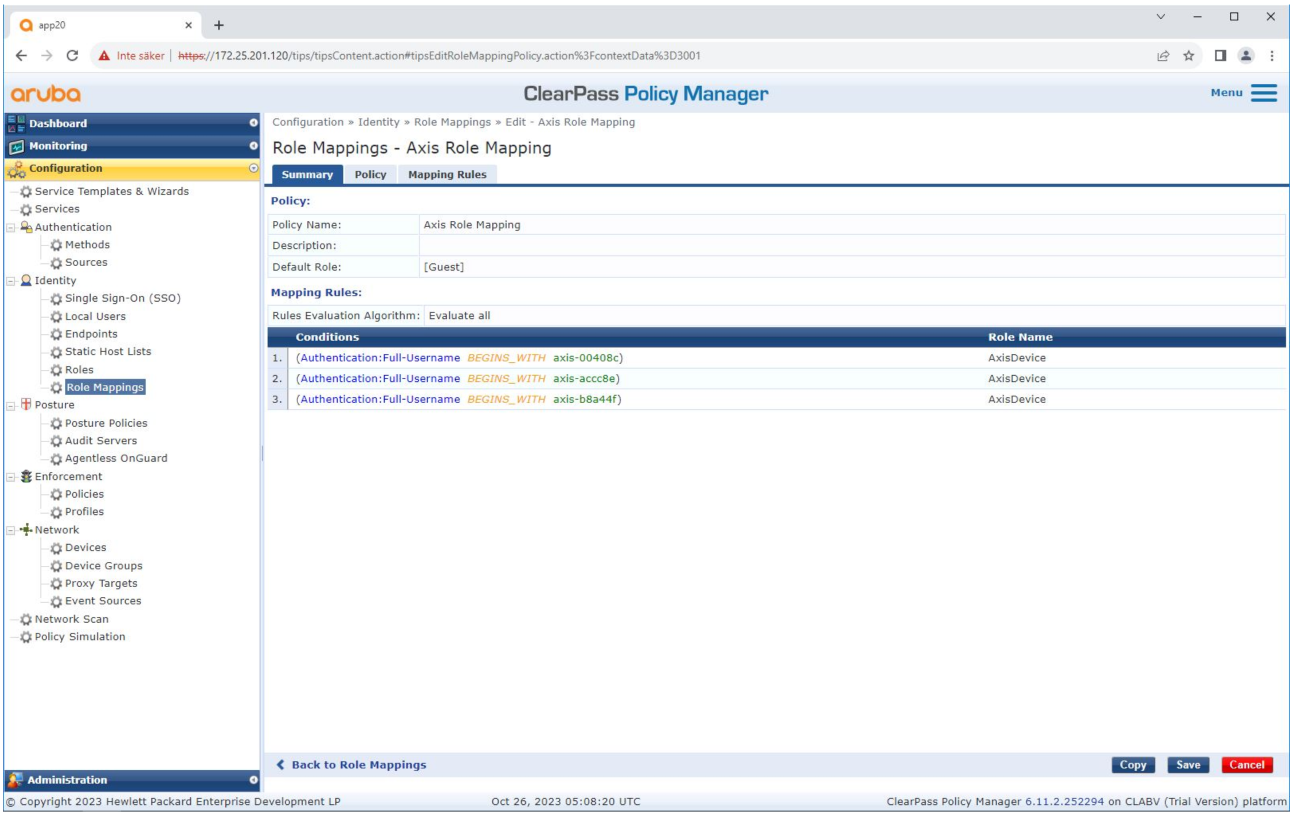
Role ID:	3001
Name:	AxisDevice
Description:	

Save Cancel

© Copyright 2023 Hewlett Packard Enterprise Development LP Oct 26, 2023 05:07:35 UTC ClearPass Policy Manager 6.11.2.252294 on CLABV (Trial Version) platform

Adding a role name for Axis devices. The name is the port access role name in the Aruba access switch configuration.

Secure network operation - IEEE 802.1AE MACsec



Configuration » Identity » Role Mappings » Edit - Axis Role Mapping

Role Mappings - Axis Role Mapping

Policy:

Policy Name:	Axis Role Mapping
Description:	
Default Role:	[Guest]

Mapping Rules:

Rules Evaluation Algorithm: Evaluate all

	Conditions	Role Name
1.	(Authentication:Full-Username BEGINS_WITH axis-00408c)	AxisDevice
2.	(Authentication:Full-Username BEGINS_WITH axis-accc8e)	AxisDevice
3.	(Authentication:Full-Username BEGINS_WITH axis-b8a44f)	AxisDevice

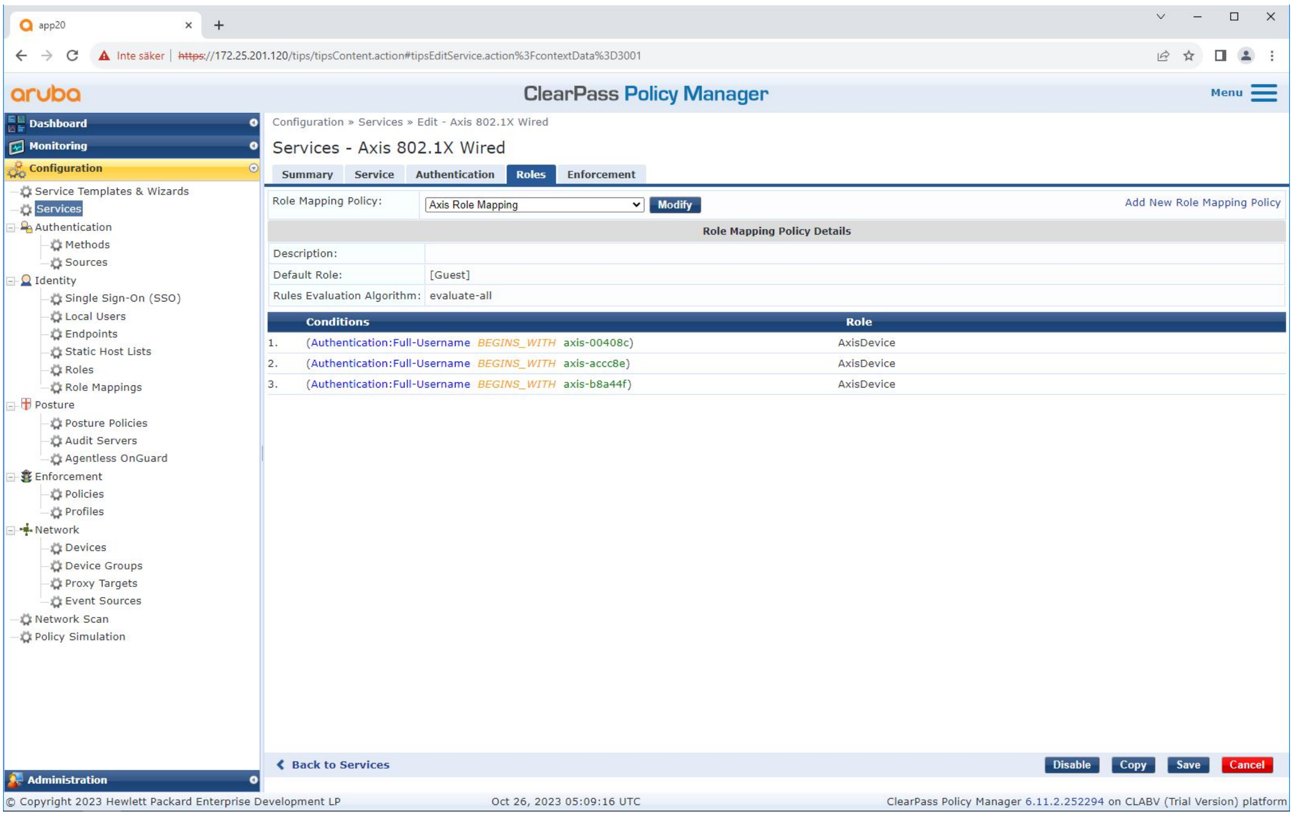
© Copyright 2023 Hewlett Packard Enterprise Development LP Oct 26, 2023 05:08:20 UTC ClearPass Policy Manager 6.11.2.252294 on CLABV (Trial Version) platform

Adding an Axis role mapping policy for the earlier created Axis device role. The conditions defined are required for a device to be mapped to the Axis device role. If the conditions aren't met, the device will be part of the [Guest] role.

By default, Axis devices use the EAP identity format "axis-serialnumber". The serial number of an Axis device is its MAC-address. For example "axis-b8a44f45b4e6".

Secure network operation - IEEE 802.1AE MACsec

Service configuration



Services - Axis 802.1X Wired

Role Mapping Policy: Axis Role Mapping

Role Mapping Policy Details

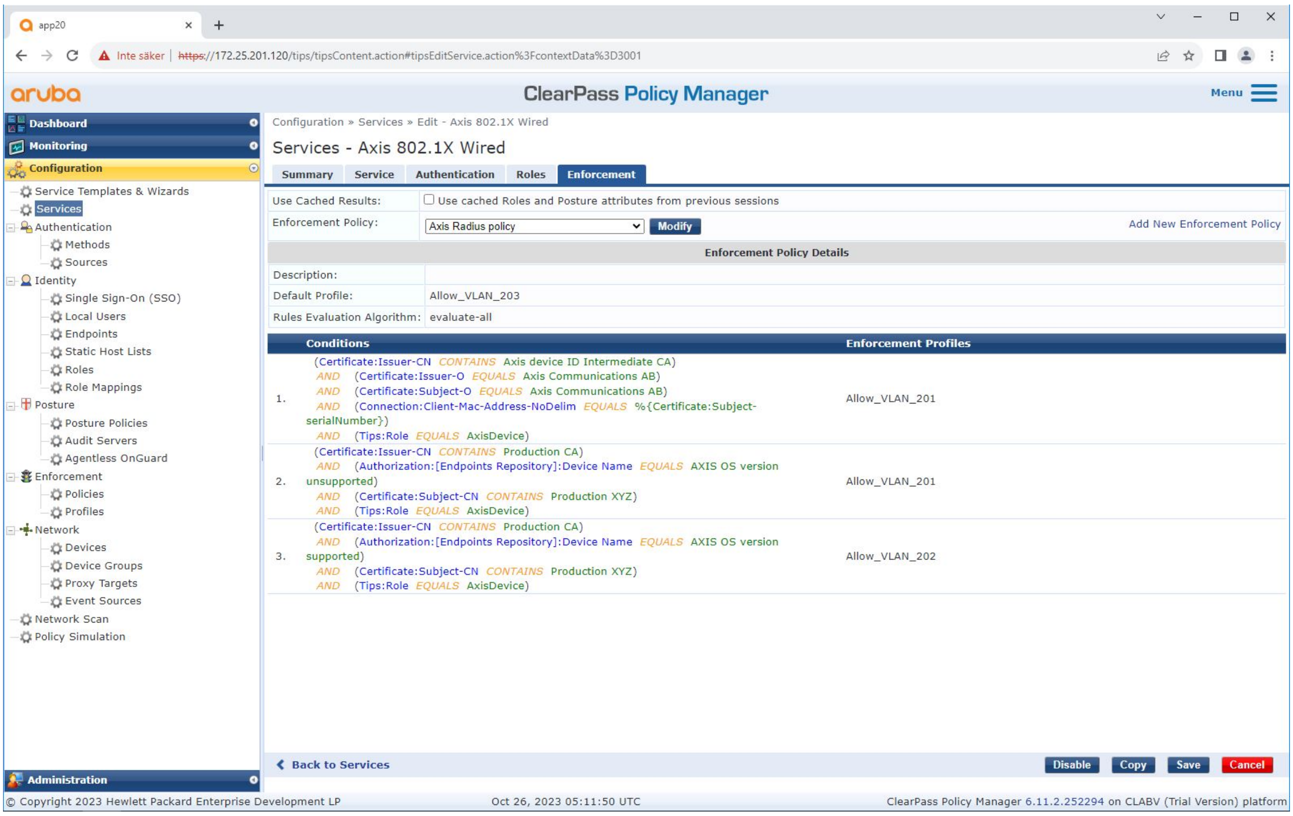
Description:	
Default Role:	[Guest]
Rules Evaluation Algorithm:	evaluate-all

	Conditions	Role
1.	(Authentication:Full-Username BEGINS_WITH axis-00408c)	AxisDevice
2.	(Authentication:Full-Username BEGINS_WITH axis-accc8e)	AxisDevice
3.	(Authentication:Full-Username BEGINS_WITH axis-b8a44f)	AxisDevice

© Copyright 2023 Hewlett Packard Enterprise Development LP Oct 26, 2023 05:09:16 UTC ClearPass Policy Manager 6.11.2.252294 on CLABV (Trial Version) platform

Adding the earlier created Axis role mapping policy to the service that defines IEEE 802.1X as connection method for the onboarding of Axis devices.

Secure network operation - IEEE 802.1AE MACsec



Services - Axis 802.1X Wired

Use Cached Results: □ Use cached Roles and Posture attributes from previous sessions

Enforcement Policy: Axis Radius policy [Modify] Add New Enforcement Policy

Enforcement Policy Details

Description:	
Default Profile:	Allow_VLAN_203
Rules Evaluation Algorithm:	evaluate-all

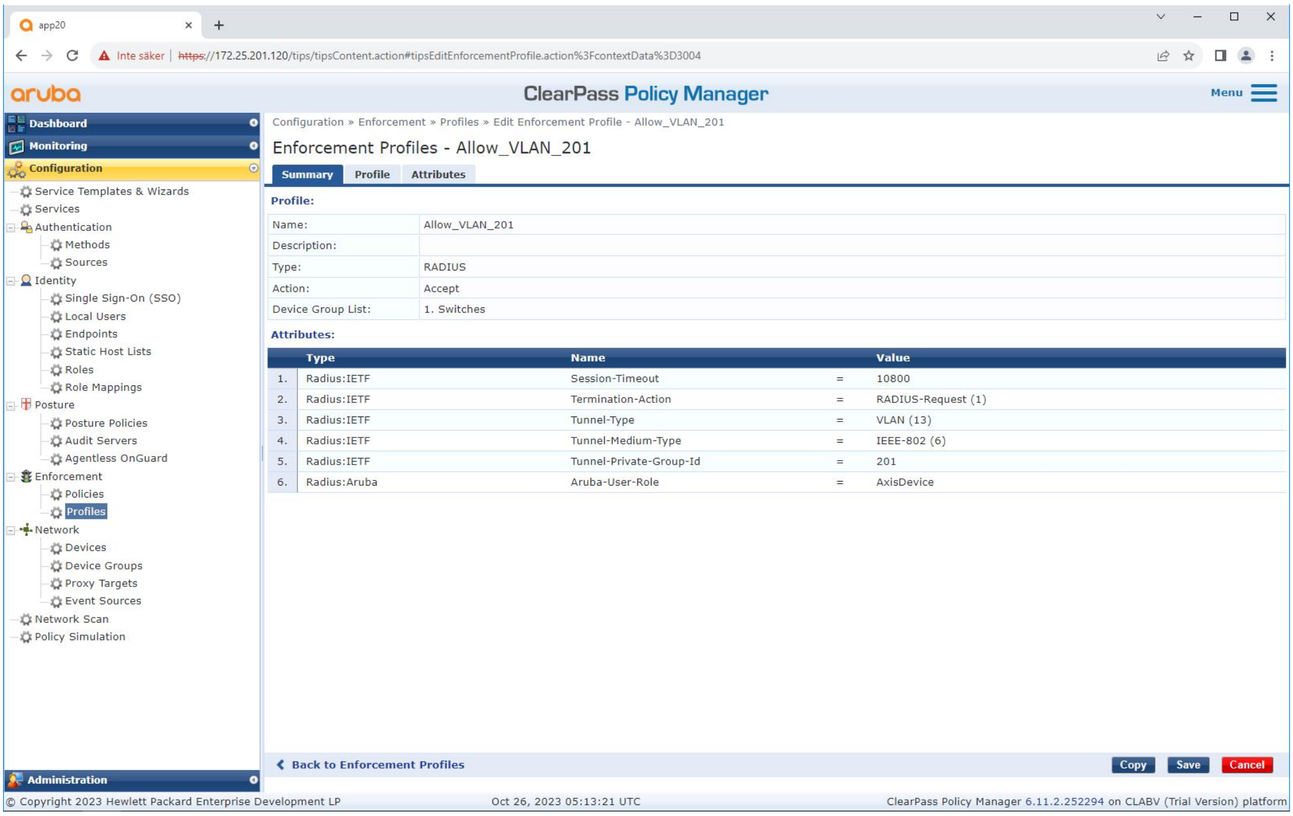
	Conditions	Enforcement Profiles
1.	(Certificate:Issuer-CN CONTAINS Axis device ID Intermediate CA) AND (Certificate:Issuer-O EQUALS Axis Communications AB) AND (Certificate:Subject-O EQUALS Axis Communications AB) AND (Connection:Client-Mac-Address-NoDelim EQUALS %{Certificate:Subject-serialNumber}) AND (Tips:Role EQUALS AxisDevice)	Allow_VLAN_201
2.	(Certificate:Issuer-CN CONTAINS Production CA) AND (Authorization:[Endpoints Repository]:Device Name EQUALS AXIS OS version unsupported) AND (Certificate:Subject-CN CONTAINS Production XYZ) AND (Tips:Role EQUALS AxisDevice)	Allow_VLAN_201
3.	(Certificate:Issuer-CN CONTAINS Production CA) AND (Authorization:[Endpoints Repository]:Device Name EQUALS AXIS OS version supported) AND (Certificate:Subject-CN CONTAINS Production XYZ) AND (Tips:Role EQUALS AxisDevice)	Allow_VLAN_202

© Copyright 2023 Hewlett Packard Enterprise Development LP Oct 26, 2023 05:11:50 UTC ClearPass Policy Manager 6.11.2.252294 on CLABV (Trial Version) platform

Adding the Axis role name as a condition to the existing policy definitions.

Secure network operation - IEEE 802.1AE MACsec

Enforcement profile



Configuration » Enforcement » Profiles » Edit Enforcement Profile - Allow_VLAN_201

Enforcement Profiles - Allow_VLAN_201

Profile:

Name:	Allow_VLAN_201
Description:	
Type:	RADIUS
Action:	Accept
Device Group List:	1. Switches

Attributes:

	Type	Name		Value
1.	Radius:IETF	Session-Timeout	=	10800
2.	Radius:IETF	Termination-Action	=	RADIUS-Request (1)
3.	Radius:IETF	Tunnel-Type	=	VLAN (13)
4.	Radius:IETF	Tunnel-Medium-Type	=	IEEE-802 (6)
5.	Radius:IETF	Tunnel-Private-Group-Id	=	201
6.	Radius:Aruba	Aruba-User-Role	=	AxisDevice

© Copyright 2023 Hewlett Packard Enterprise Development LP   Oct 26, 2023 05:13:21 UTC   ClearPass Policy Manager 6.11.2.252294 on CLABV (Trial Version) platform

Adding the Axis role name as attribute to the enforcement profiles that are assigned in the IEEE 802.1X onboarding service.

Aruba access switch

In addition to the secure onboarding configuration described in *Aruba access switch on page 16*, refer to the below example port configuration for the Aruba access switch to configure IEEE 802.1AE MACsec.

```
macsec policy macsec-eap
cipher-suite gcm-aes-128

port-access role AxisDevice
associate macsec-policy macsec-eap
auth-mode client-mode

aaa authentication port-access dot1x authenticator
macsec
mkacak-length 16
enable
```

Legacy onboarding - MAC authentication

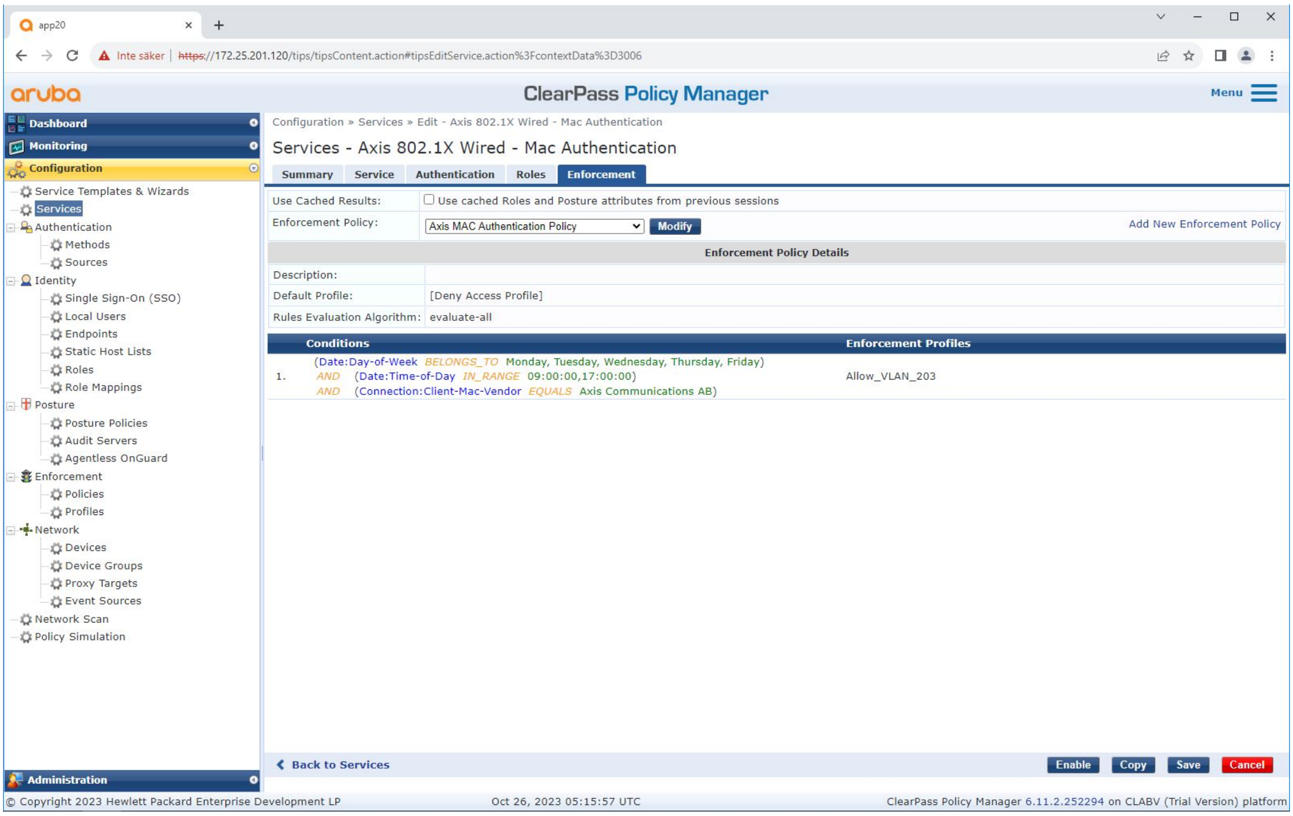
You can use MAC Authentication Bypass (MAB) to onboard Axis devices that don't support IEEE 802.1AR onboarding with the Axis device ID certificate and IEEE 802.1X enabled in factory default state. If 802.1X onboarding fails, Aruba ClearPass Policy Manager validates the Axis device's MAC address and grant access to the network.

MAB requires both Aruba access switch and ClearPass Policy Manager configuration preparations. On the Axis device, no configuration is required to allow MAB for onboarding.

Aruba ClearPass Policy Manager

Enforcement policy

The enforcement policy configuration in the Aruba ClearPass Policy Manager defines if Axis devices are granted access to Aruba networks based on the following two example policy conditions.



Configuration » Services » Edit - Axis 802.1X Wired - Mac Authentication

Services - Axis 802.1X Wired - Mac Authentication

Use Cached Results: □ Use cached Roles and Posture attributes from previous sessions

Enforcement Policy: Axis MAC Authentication Policy

Enforcement Policy Details

Description:

Default Profile: [Deny Access Profile]

Rules Evaluation Algorithm: evaluate-all

	Conditions	Enforcement Profiles
1.	(Date:Day-of-Week *BELONGS_TO* Monday, Tuesday, Wednesday, Thursday, Friday) *AND* (Date:Time-of-Day *IN_RANGE* 09:00:00,17:00:00) *AND* (Connection:Client-Mac-Vendor *EQUALS* Axis Communications AB)	Allow_VLAN_203

© Copyright 2023 Hewlett Packard Enterprise Development LP Oct 26, 2023 05:15:57 UTC ClearPass Policy Manager 6.11.2.252294 on CLABV (Trial Version) platform

Denied network access

When the Axis device doesn't meet the configured enforcement policy, it's denied access to the network.

Guest-network (VLAN 203)

The Axis device is granted access to a limited, isolated network if the following conditions are met:

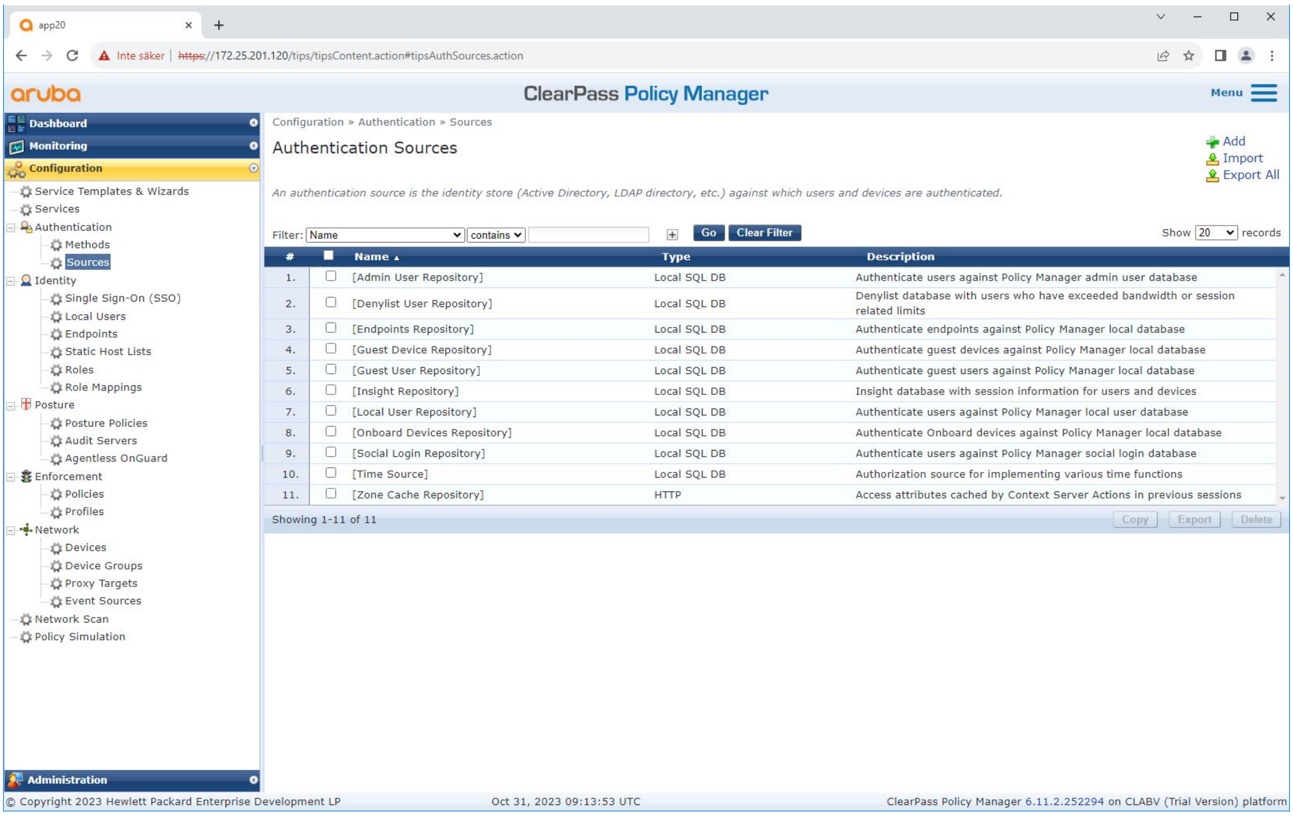
- It is a weekday between Monday and Friday
- It is between 09:00 and 17:00

- The MAC address vendor matches with Axis Communications AB.

Since MAC addresses can be spoofed, access to the regular provisioning network isn't granted. We recommend that you only use MAB for initial onboarding, and to manually inspect the device further.

Source configuration

In the Sources interface, a new authentication source is created to allow only manually imported MAC addresses.



Configuration » Authentication » Sources

Authentication Sources

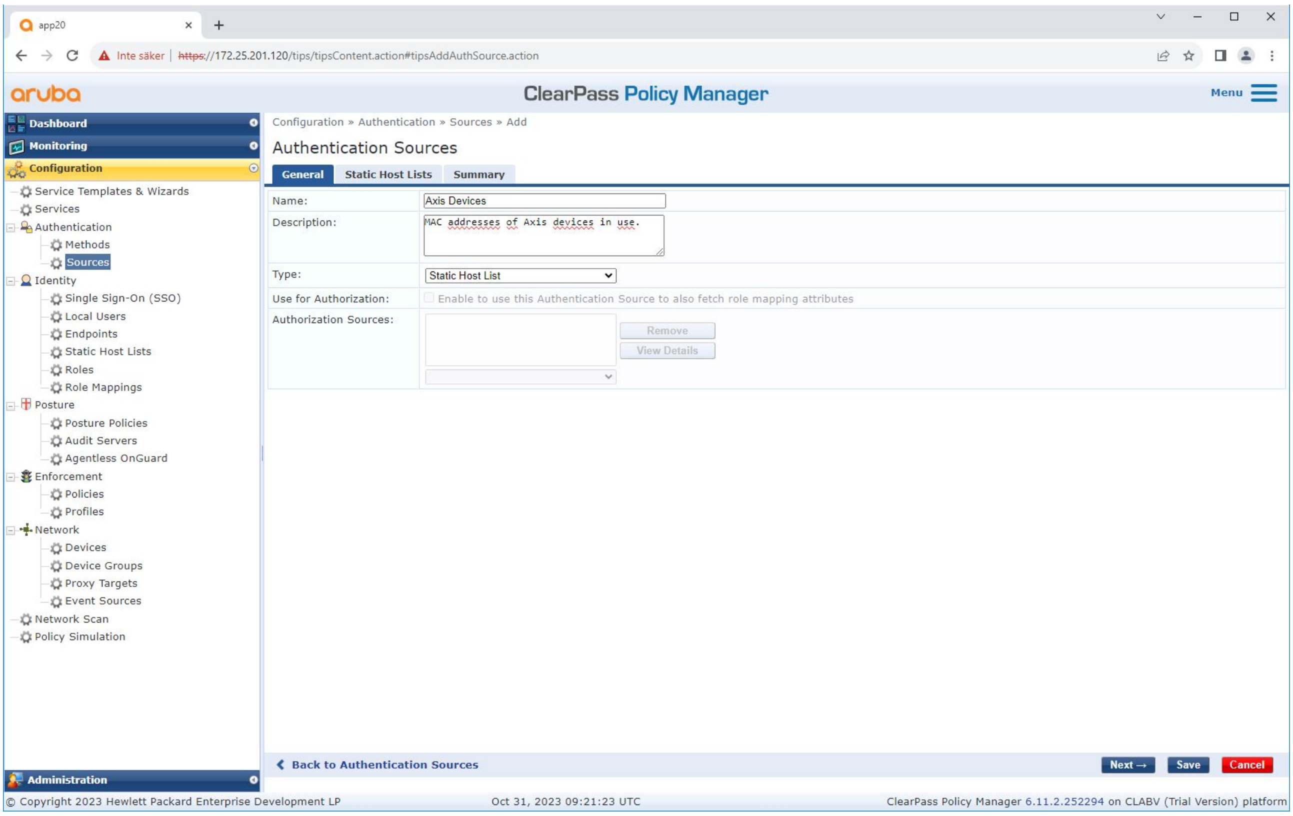
An authentication source is the identity store (Active Directory, LDAP directory, etc.) against which users and devices are authenticated.

#	□	Name ▲	Type	Description
1.	□	[Admin User Repository]	Local SQL DB	Authenticate users against Policy Manager admin user database
2.	□	[Denylist User Repository]	Local SQL DB	Denylist database with users who have exceeded bandwidth or session related limits
3.	□	[Endpoints Repository]	Local SQL DB	Authenticate endpoints against Policy Manager local database
4.	□	[Guest Device Repository]	Local SQL DB	Authenticate guest devices against Policy Manager local database
5.	□	[Guest User Repository]	Local SQL DB	Authenticate guest users against Policy Manager local database
6.	□	[Insight Repository]	Local SQL DB	Insight database with session information for users and devices
7.	□	[Local User Repository]	Local SQL DB	Authenticate users against Policy Manager local user database
8.	□	[Onboard Devices Repository]	Local SQL DB	Authenticate Onboard devices against Policy Manager local database
9.	□	[Social Login Repository]	Local SQL DB	Authenticate users against Policy Manager social login database
10.	□	[Time Source]	Local SQL DB	Authorization source for implementing various time functions
11.	□	[Zone Cache Repository]	HTTP	Access attributes cached by Context Server Actions in previous sessions

Showing 1-11 of 11

© Copyright 2023 Hewlett Packard Enterprise Development LP   Oct 31, 2023 09:13:53 UTC   ClearPass Policy Manager 6.11.2.252294 on CLABV (Trial Version) platform

Legacy onboarding - MAC authentication

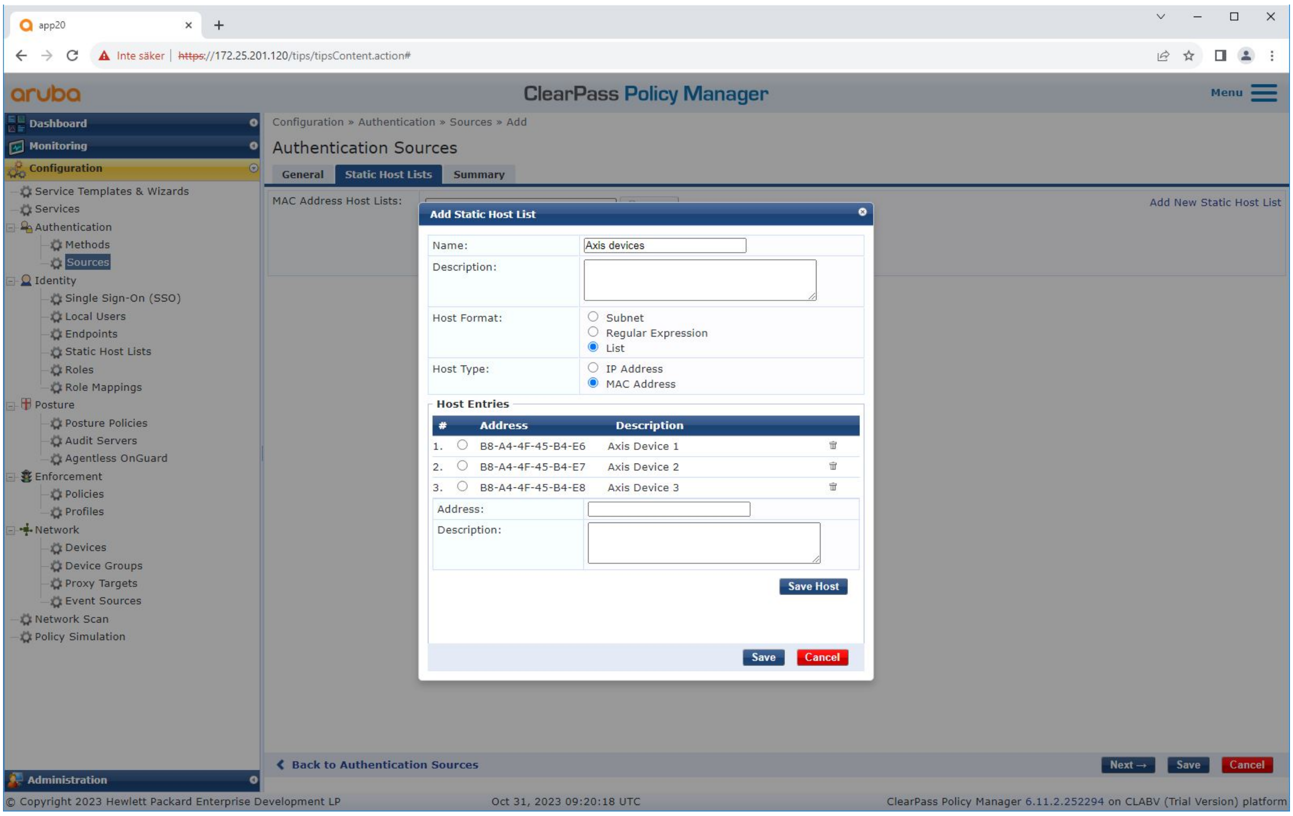


Authentication Sources

Name:	Axis Devices
Description:	MAC addresses of Axis devices in use.
Type:	Static Host List
Use for Authorization:	□ Enable to use this Authentication Source to also fetch role mapping attributes
Authorization Sources:	

© Copyright 2023 Hewlett Packard Enterprise Development LP Oct 31, 2023 09:21:23 UTC ClearPass Policy Manager 6.11.2.252294 on CLABV (Trial Version) platform

Legacy onboarding - MAC authentication



Add Static Host List

Name: Axis devices

Description:

Host Format: ○ Subnet ○ Regular Expression ● List

Host Type: ○ IP Address ● MAC Address

Host Entries

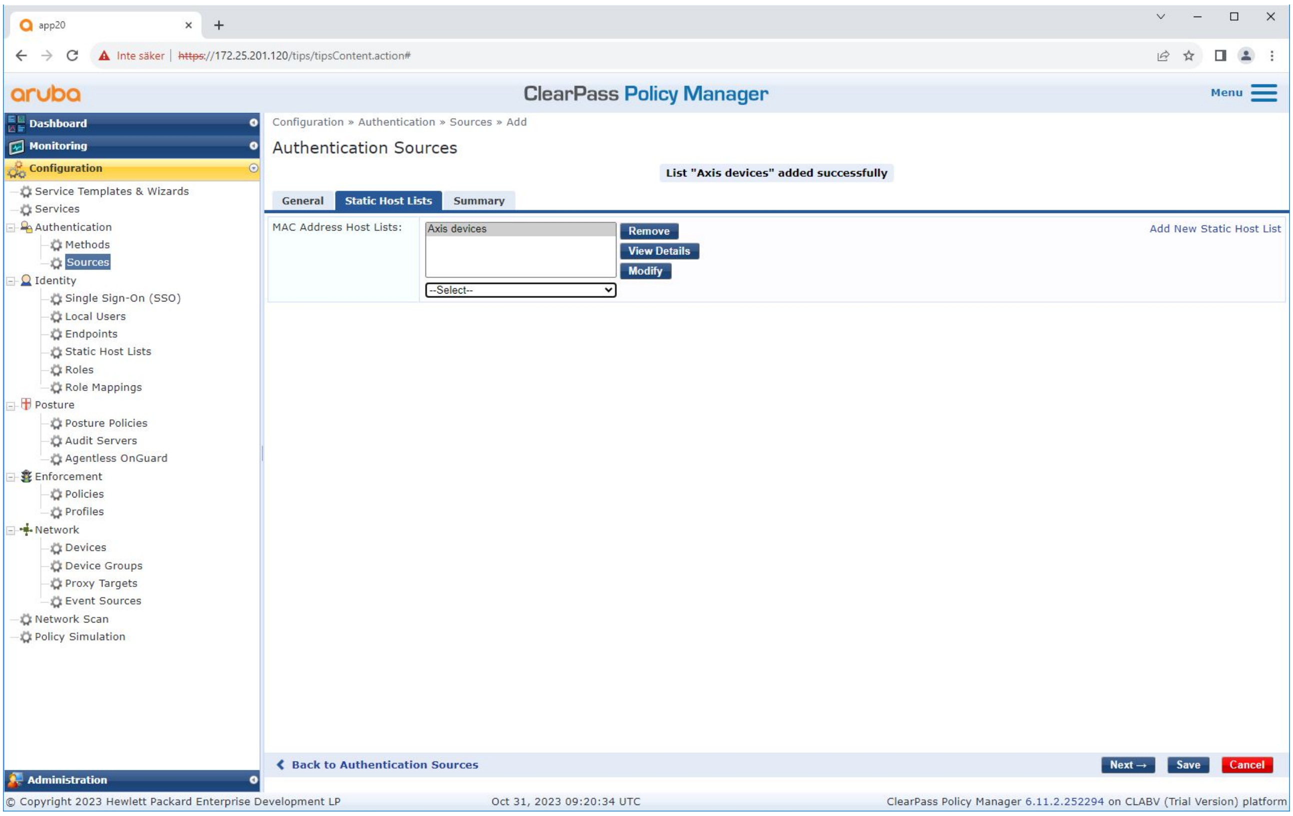
#		Address	Description
1.	○	B8-A4-4F-45-B4-E6	Axis Device 1
2.	○	B8-A4-4F-45-B4-E7	Axis Device 2
3.	○	B8-A4-4F-45-B4-E8	Axis Device 3

Address:

Description:

A static host list, which contains Axis MAC addresses, is created.

Legacy onboarding - MAC authentication



Configuration » Authentication » Sources » Add

Authentication Sources

List "Axis devices" added successfully

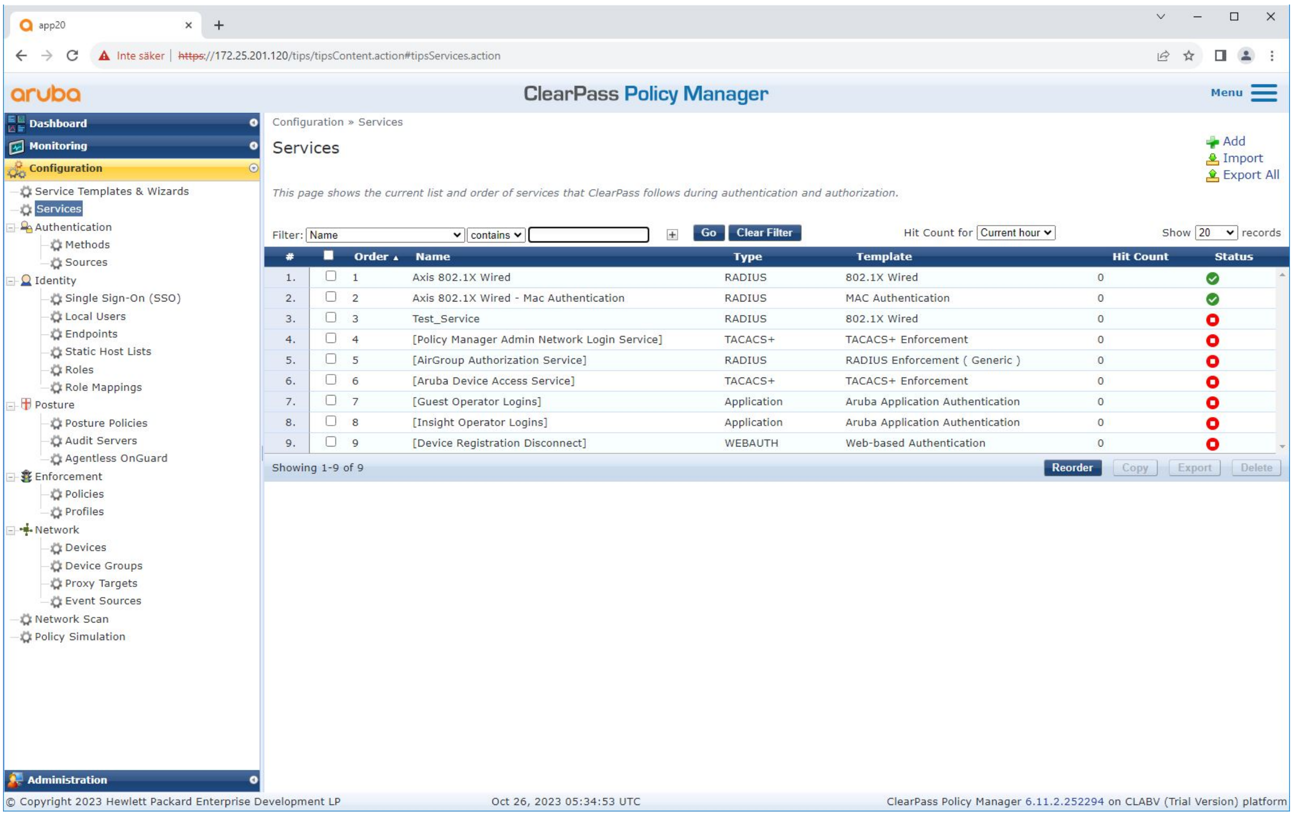
MAC Address Host Lists: Axis devices

--Select--

Service configuration

In the Services inferface, the configuration steps are combined into one single service that handles the authentication and authorization of Axis devices in Aruba networks.

Legacy onboarding - MAC authentication



Configuration » Services

Services

This page shows the current list and order of services that ClearPass follows during authentication and authorization.

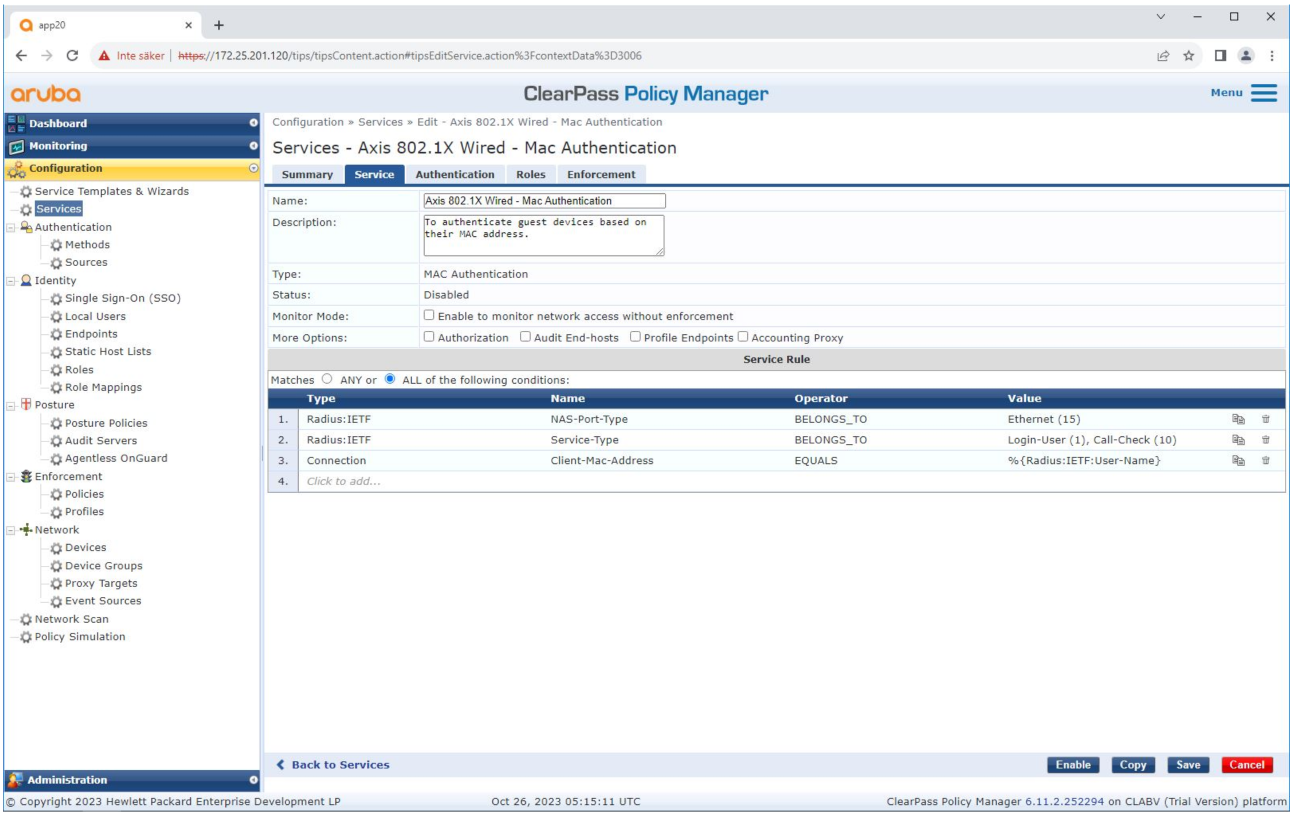
Filter: Name contains Hit Count for Current hour Show 20 records

#	□	Order ▴	Name	Type	Template	Hit Count	Status
1.	□	1	Axis 802.1X Wired	RADIUS	802.1X Wired	0	✓
2.	□	2	Axis 802.1X Wired - Mac Authentication	RADIUS	MAC Authentication	0	✓
3.	□	3	Test_Service	RADIUS	802.1X Wired	0	●
4.	□	4	[Policy Manager Admin Network Login Service]	TACACS+	TACACS+ Enforcement	0	●
5.	□	5	[AirGroup Authorization Service]	RADIUS	RADIUS Enforcement (Generic)	0	●
6.	□	6	[Aruba Device Access Service]	TACACS+	TACACS+ Enforcement	0	●
7.	□	7	[Guest Operator Logins]	Application	Aruba Application Authentication	0	●
8.	□	8	[Insight Operator Logins]	Application	Aruba Application Authentication	0	●
9.	□	9	[Device Registration Disconnect]	WEBAUTH	Web-based Authentication	0	●

Showing 1-9 of 9

© Copyright 2023 Hewlett Packard Enterprise Development LP Oct 26, 2023 05:34:53 UTC ClearPass Policy Manager 6.11.2.252294 on CLABV (Trial Version) platform

Legacy onboarding - MAC authentication



Services - Axis 802.1X Wired - Mac Authentication

Name:	Axis 802.1X Wired - Mac Authentication
Description:	To authenticate guest devices based on their MAC address.
Type:	MAC Authentication
Status:	Disabled
Monitor Mode:	□ Enable to monitor network access without enforcement
More Options:	□ Authorization □ Audit End-hosts □ Profile Endpoints □ Accounting Proxy

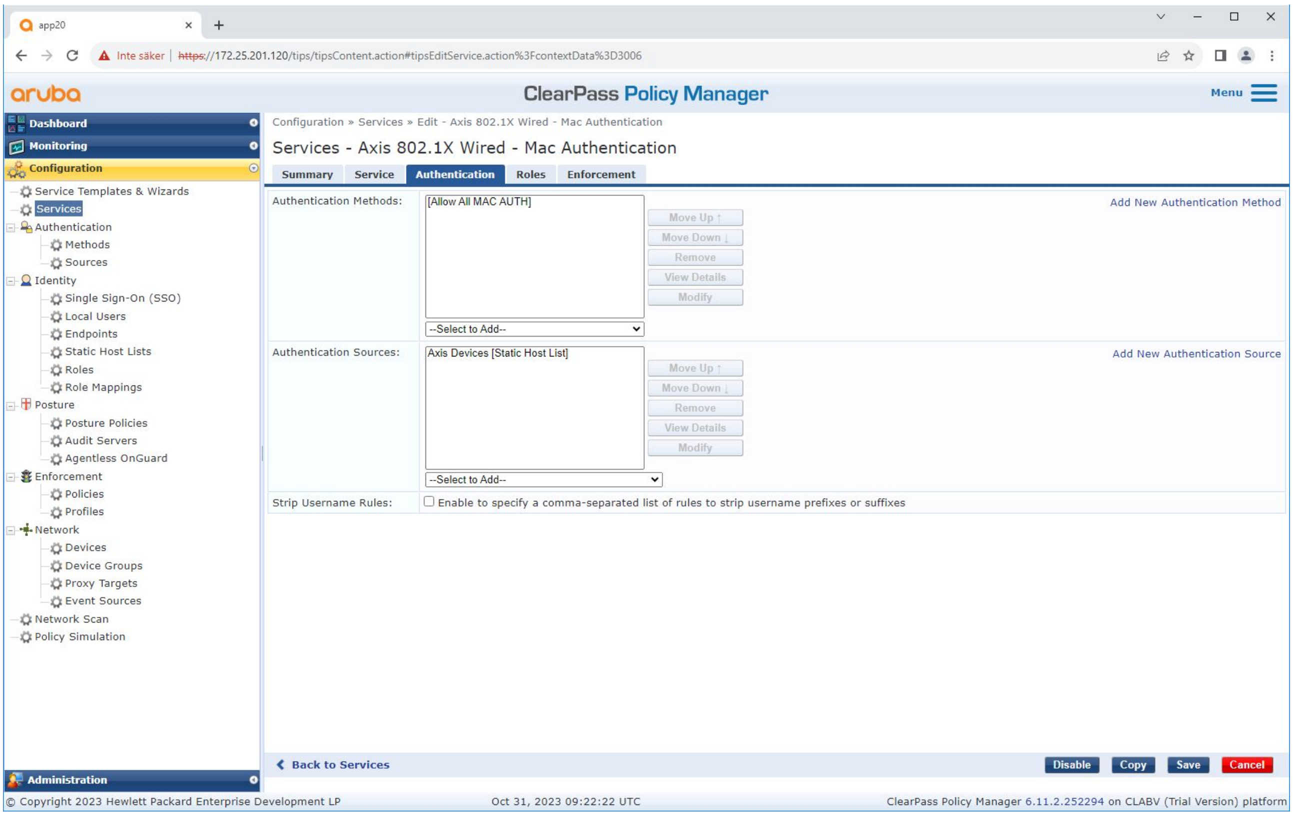
Service Rule

Matches ○ ANY or ● ALL of the following conditions:

	Type	Name	Operator	Value
1.	Radius:IETF	NAS-Port-Type	BELONGS_TO	Ethernet (15)
2.	Radius:IETF	Service-Type	BELONGS_TO	Login-User (1), Call-Check (10)
3.	Connection	Client-Mac-Address	EQUALS	%{Radius:IETF:User-Name}
4.	*Click to add...*			

A dedicated Axis service that defines MAB as connection method is created.

Legacy onboarding - MAC authentication



Services - Axis 802.1X Wired - Mac Authentication

Authentication Methods: [Allow All MAC AUTH]
--Select to Add--

Authentication Sources: Axis Devices [Static Host List]
--Select to Add--

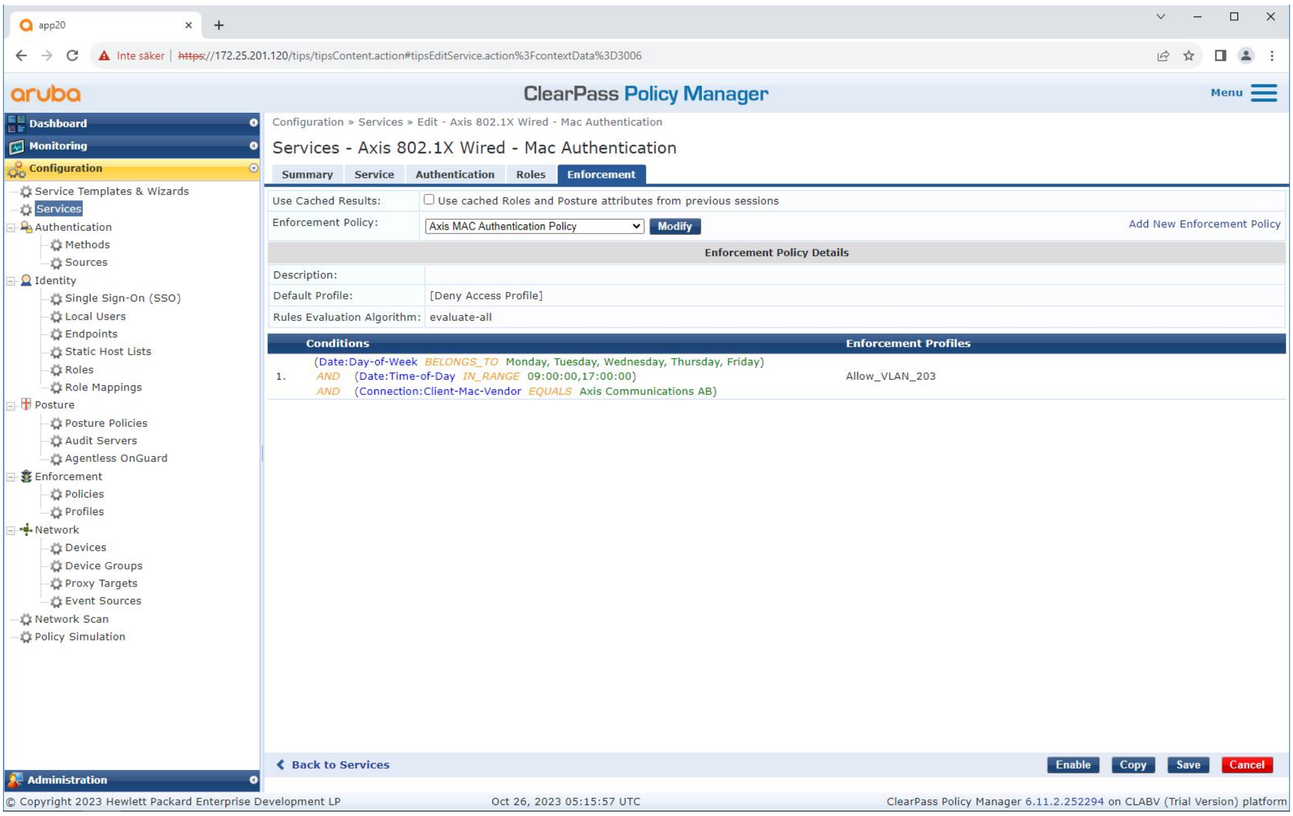
Strip Username Rules: □ Enable to specify a comma-separated list of rules to strip username prefixes or suffixes

The pre-configured MAC authentication method is configured to the service. Also, the previously created authentication source which contains a list of Axis MAC addresses is selected.

Axis Communications AB uses the following MAC address OUIs:

- B8:A4:4F:XX:XX:XX
- AA:C8:3E:XX:XX:XX
- 00:40:8C:XX:XX:XX

Legacy onboarding - MAC authentication



Configuration » Services » Edit - Axis 802.1X Wired - Mac Authentication

Services - Axis 802.1X Wired - Mac Authentication

Use Cached Results: □ Use cached Roles and Posture attributes from previous sessions

Enforcement Policy: Axis MAC Authentication Policy

Add New Enforcement Policy

Enforcement Policy Details

Description:

Default Profile: [Deny Access Profile]

Rules Evaluation Algorithm: evaluate-all

	Conditions	Enforcement Profiles
1.	(Date:Day-of-Week BELONGS_TO Monday, Tuesday, Wednesday, Thursday, Friday) AND (Date:Time-of-Day IN_RANGE 09:00:00,17:00:00) AND (Connection:Client-Mac-Vendor EQUALS Axis Communications AB)	Allow_VLAN_203

© Copyright 2023 Hewlett Packard Enterprise Development LP Oct 26, 2023 05:15:57 UTC ClearPass Policy Manager 6.11.2.252294 on CLABV (Trial Version) platform

In the last step, the previously created enforcement policy is configured to the service.

Aruba access switch

In addition to the secure onboarding configuration described in *Aruba access switch on page 16*, refer to the below example port configuration for the Aruba access switch to allow for MAB.

```
aaa port-access authenticator 18 tx-period 5
aaa port-access authenticator 19 tx-period 5
aaa port-access authenticator 18 max-requests 3
aaa port-access authenticator 19 max-requests 3
aaa port-access authenticator 18 client-limit 1
aaa port-access authenticator 19 client-limit 1
aaa port-access mac-based 18-19
aaa port-access 18 auth-order authenticator mac-based
aaa port-access 19 auth-order authenticator mac-based
aaa port-access 18 auth-priority authenticator mac-based
aaa port-access 19 auth-priority authenticator mac-based
```

User manual
Secure integration of Axis devices into Aruba networks
© Axis Communications AB, 2023

Ver. M4.3
Date: November 2023
Part no. T10197992