

Integration Guide

## Table of Contents

Introduction	3
Secure onboarding – IEEE 802.1AR/802.1X	4
Initial authentication	4
Provisioning	4
Production network	4
Configuration HPE Aruba NetworkingConfiguration Axis	5
Configuration Axis	
	19
	20
HPE Aruba Networking access switch	24
Legacy onboarding – MAC authentication	25
HPÉ Aruba Networking ClearPass Policy Manager	25
HPE Aruba Networking access switch	33

### Introduction

#### Introduction

This integration guide aims to outline the best-practice configuration of how to onboard and operate Axis devices in HPE Aruba Networking powered 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 HPE Aruba Networking infrastructure and applications. Below are some benefits that can be gained when combining Axis devices and software with a HPE Aruba Networking 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 HPE 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's necessary to have knowledge about the following areas before doing the configuration:

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

#### Secure onboarding - IEEE 802.1AR/802.1X

#### Secure onboarding - IEEE 802.1AR/802.1X



Secure device onboarding onto zero-trust networks with IEEE 802.1X/802.1AR

#### Initial authentication

Connect the Axis Edge Vault supported Axis device to authenticate the device against the network. The device 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, ClearPass Policy Manager verifies the Axis device ID together with other device specific fingerprints. The information, such as MAC-address and running AXIS OS, is used to make a policy-based decision.

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

The Axis device authenticates against the HPE Aruba Networking powered 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 Axis device moves into the provisioning network (VLAN201) where AXIS Device Manager is installed. Through AXIS Device Manager, device configuration, security hardening, and AXIS OS 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

#### Secure onboarding - IEEE 802.1AR/802.1X

#### **Production network**

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

After the device configuration, the Axis device leaves the provisioning network and attempts to reauthenticate against the 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 moves into the production network (VLAN 202). In that network, the Video Management System (VMS) connects to the Axis device and starts 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 Networking

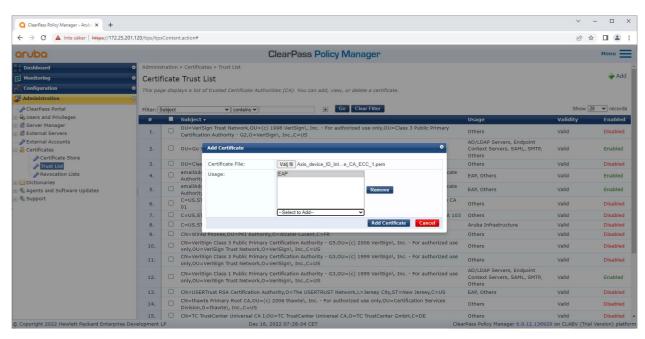
#### HPE Aruba Networking ClearPass Policy Manager

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 ClearPass Policy Manager to authenticate Axis devices through IEEE 802.1X EAP-TLS.
- 4. Select EAP in the usage field. The certificates are used for IEEE 802.1X EAP-TLS authentication.

### Secure onboarding - IEEE 802.1AR/802.1X



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

ClearPass Policy Manager cates * Trust List List of trusted Certificate Authonities (CA). You can add, view, or delete a certificate. Contains axis device  Contains axis de	Usage EAP EAP EAP EAP EAP EAP EAP EAP	Show 20 v recc Show 20 v recc Valid Enabl Valid Enabl Valid Enabl Valid Enabl Valid Enabl Valid Enabl Valid Enabl
List of trusted Certificate Authonities (CA). You can add, view, or delete a certificate. Contains axis device Go Clear Filter t s device ID Root CA RSA,0=Axis Communications AB s device ID Intermediate CA RSA 2,0=Axis Communications AB s device ID Intermediate CA RSA 1,0=Axis Communications AB s device ID Intermediate CA RSA 1,0=Axis Communications AB s device ID Intermediate CA SCA 2,0=Axis Communications AB	EAP EAP EAP EAP EAP	Show 20 V recc Validity Enab Valid Enabi Valid Enabi Valid Enabi Valid Enabi Valid Enabi
of trusted Certificate Authonities (CA). You can add, view, or delete a certificate.	EAP EAP EAP EAP EAP	Show 20 V recc Validity Enab Valid Enabi Valid Enabi Valid Enabi Valid Enabi Valid Enabi
Contains Caxis device  Go Clear Filter  Contains Caxis device  Go Clear Filter  Contains Caxis Communications AB  S device ID Root CA ECC,0-Axis Communications AB  S device ID Intermediate CA RSA 2,0=Axis Communications AB  S device ID Intermediate CA RSA 1,0=Axis Communications AB  S device ID Intermediate CA CASA 1,0=Axis Communications AB  S device ID Intermediate CA ECC 2,0=Axis Communications AB  S device ID Intermediate CA ECC 2,0=Axis Communications AB	EAP EAP EAP EAP EAP	Validity         Enable           Valid         Enable
Contains Caxis device  Go Clear Filter  Contains Caxis device  Go Clear Filter  Contains Caxis Communications AB  S device ID Root CA ECC,0-Axis Communications AB  S device ID Intermediate CA RSA 2,0=Axis Communications AB  S device ID Intermediate CA RSA 1,0=Axis Communications AB  S device ID Intermediate CA CASA 1,0=Axis Communications AB  S device ID Intermediate CA ECC 2,0=Axis Communications AB  S device ID Intermediate CA ECC 2,0=Axis Communications AB	EAP EAP EAP EAP EAP	Validity         Enable           Valid         Enable
s device ID Root CA RSA,0=Axis Communications AB s device ID Root CA ECC,0=Axis Communications AB s device ID Intermediate CA RSA 2,0=Axis Communications AB s device ID Intermediate CA RSA 1,0=Axis Communications AB s device ID Intermediate CA ECC 2,0=Axis Communications AB	EAP EAP EAP EAP EAP	Validity         Enable           Valid         Enable
s device ID Root CA RSA,O=Axis Communications AB s device ID Root CA ECC,O=Axis Communications AB s device ID Intermediate CA RSA 2,O=Axis Communications AB s device ID Intermediate CA RSA 1,O=Axis Communications AB s device ID Intermediate CA ECC 2,O=Axis Communications AB	EAP EAP EAP EAP EAP	Valid Enabl Valid Enabl Valid Enabl Valid Enabl Valid Enabl
s device ID Root CA ECC,O-Axis Communications AB s device ID Intermediate CA RSA 2,0-Axis Communications AB s device ID Intermediate CA RSA 1,0-Axis Communications AB s device ID Intermediate CA ECC 2,0-Axis Communications AB	EAP EAP EAP EAP	Valid Enabl Valid Enabl Valid Enabl Valid Enabl
s device ID Intermediate CA RSA 2,0=Axis Communications AB s device ID Intermediate CA RSA 1,0=Axis Communications AB s device ID Intermediate CA ECC 2,0=Axis Communications AB	EAP EAP EAP	Valid Enabl Valid Enabl Valid Enabl
s device ID Intermediate CA RSA 1,0=Axis Communications AB s device ID Intermediate CA ECC 2,0=Axis Communications AB	EAP	Valid Enabl Valid Enabl
s device ID Intermediate CA ECC 2,0=Axis Communications AB	EAP	Valid Enabl
s device ID Intermediate CA ECC 1,0=Axis Communications AB	EAP	Valid Enabl
		Dele

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

#### Network device/group configuration

- 1. Add trusted network access devices, such as HPE Aruba Networking access switches, to ClearPass Policy Manager. ClearPass Policy Manager needs to know which access switches in the network are 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.

## Secure onboarding - IEEE 802.1AR/802.1X

O ClearPass Policy Manager - Arub × +		✓ - □ X
← → C ▲ Inte säker   https://172.25.20	.120/tips/tipsContent.action#tipsNetworkDevices.action	년 🌶 🔲 😩 :
aruba	ClearPass Policy	Manager Menu 🗮
Dashboard	Configuration » Network » Devices	
Monitoring	Network Devices	🛶 Add
🖧 Configuration	0	<mark>≗</mark> Import <b>≰</b> Export All
		Export All
- 🛱 Services	A Network Access Device (NAD) must belong to the global list of devices in the C	learPass database in order to connect to ClearPass.
Authentication		
🗈 🧟 Identity	Filter: Name  v contains  +	Go Clear Filter Show 20 🗸 records
B Enforcement	# Name 🖌 IP or Subnet Address	Device Groups Description
- + Network		Copy Export Delete
- 🗘 Devices		
- Device Groups		
- 🛱 Proxy Targets - 🛱 Event Sources		
- O Network Scan		
- O Policy Simulation		
Administration	0	
© Copyright 2022 Hewlett Packard Enterprise D	evelopment 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 ClearPass Policy Manager.

Q ClearPass Policy Manager - Arub 🗙 🕂						~ - 🗆 X
← → C ▲ Inte säker   https://172.25.201.	120/tips/tipsContent.action#					ie 🛧 🗖 😩 :
aruba		ClearPass Polic	y Manager			Menu 🗮
Deshboard     Monitoring     Monitoring     Service Templates & Wizards     Services     Authentication     Gervices     Authentication     Gervices     Service Templates     Service Templates     Service Templates     Service Templates     Service Templates     Service Templates     Service Service     Service	Add Device				•	Add Triport Export All Discovered Devices
	Perke SNMP Read Settings SN Name: IP or Subnet Address: Description:	MP Write Settings         CLI Settings           (SW04         (172 25 200.13)           (e.g., 192.168.1.10 or 192.168.1)		a0b:12f0::1 or 2001:db8:a0	0b:12f0::1/64)	Show 20 v records Description Copy Export Delete
	RADIUS Shared Secret: TACACS+ Shared Secret: Vendor Name: Enable RADIUS Dynamic Authorization: Enable RadSec:	Aruba ×	Verify: Verify:		Add Cancel	
Administration C	velopment LP D	Dec 28, 2022 09:02:18 CET			ClearPass Policy Manage	r 6.9.12.136929 on CLABV (Trial Version) platform

Add the HPE Aruba Networking access switch as trusted network device in ClearPass Policy Manager. Please note that the RADIUS shared secret must match the specific switch IEEE 802.1X configuration.

# Secure onboarding - IEEE 802.1AR/802.1X

O ClearPass Policy Manager - Arub: × +		✓ - □ ×
← → C ▲ Inte säker   https://172.25.201.1	20/tips/tipsContent.action#	ie 🛧 🛛 😩 :
aruba	ClearPass Policy Manager	Menu 🗮
Dashboard O	Configuration » Network » Devices	
Monitoring 0	Network Devices	🚽 Add
Configuration O		Landon All & All
- 🛱 Service Templates & Wizards		<ul> <li>Export All</li> <li>Discovered Devices</li> </ul>
- 🛱 Services	Device SW04 added	
🗉 🚘 Authentication	A Network Access Device (NAD) must belong to the global list of devices in the ClearPass database in order to connect to ClearPass.	
Gentity     Fosture		
	Filter: Name   Contains   Go Clear Filter	Show 20 🗸 records
	# Name A IP or Subnet Address Device Groups	Description
- 🗘 Devices	1. Sw04 172.25.200.13 -	
- 🛱 Device Groups - 🛱 Proxy Targets	Showing 1-1 of 1	Copy Export Delete
- Ö Event Sources		
- 🛱 Network Scan		
- 🛱 Policy Simulation		
Administration 0		
© Copyright 2022 Hewlett Packard Enterprise Devi	elopment LP Dec 28, 2022 09:02:33 CET ClearPa	ss Policy Manager 6.9.12.136929 on CLABV (Trial Version) platform
Copyright 2022 newlett Packard Enterprise Devi	expriment Er DEC 20, 2022 05:02:33 CE1 Cled Pd3	ss Policy manager 0.5.12.130525 on CLABV (mail version) platform

ClearPass Policy Manager with one trusted network device configured.

Q ClearPass Policy Manager - Arub × +		~ - 🗆 X
← → C ▲ Inte säker   https://172.25.201.12	20/tips/LipsContent.action#tipsNADGroups.action	@ 🖈 🛛 😩 :
aruba	ClearPass Policy Manager	Menu 🗮
Dashboard O	Configuration » Network » Device Groups	
Monitoring O	Network Device Groups	Add Amport Amport All
- 🛱 Service Templates & Wizards - 🛱 Services	Device Groups function as a component in service and role mapping rules. Device groups can also be associated with enforcement profiles.	Export rul
<ul> <li>Authentication</li> <li>Identity</li> </ul>	Filter: Name v contains v Go Clear Filter	Show 20 🗸 records
Besture	# Name 🖌 Format Description	
🗉 🔹 Enforcement		Export Delete
Administration		
© Copyright 2022 Hewlett Packard Enterprise Deve	elopment LP Dec 28, 2022 08:57:07 CET ClearPass Policy Manager 6.9.12.136929	on CLABV (Trial Version) platform
a septimise core included i dendra enterprise peve	Clear Pass Folicy Hanager 0.5.12.130525	an all are (mar version) placionin

The trusted network device groups interface in ClearPass Policy Manager.

# Secure onboarding - IEEE 802.1AR/802.1X

ClearPass Policy Manager - Arub × +						✓ - □ ×
← → C ▲ Inte säker   https://172.25.20	01.120/tips/tipsContent.action#					🖻 🖈 🔲 😩 :
aruba			ClearPass Policy M	anager		Menu 🗮
Dashboard	• Configuration » Netwo	rk » Device Groups				
Monitoring	<ul> <li>Network Device</li> </ul>	Add New Device Group			•	🚽 Add
2 Configuration	0	Name:	Switches			La Export All
- 🛱 Service Templates & Wizards	Device Groups function	Description:	Access Switches		nent profiles.	
- 🛱 Services						
Q Identity	Filter: Name	Format:	O Subnet			Show 20 🗸 records
🗉 🖶 Posture	# 🗖 Name		<ul> <li>Regular Expression</li> <li>List</li> </ul>			
Senforcement     Network		Available Devices (0)	Cist Cist	Selected Devices (1)		Export Delete
- C Devices			Filter	Filter		
- Device Groups				SW04 [172.25.200.13]		
- 🛱 Proxy Targets						
- C Event Sources						
- O Policy Simulation						
			$\cdots \rightarrow \cdots$			
				Save		
Administration	0					
© Copyright 2022 Hewlett Packard Enterprise D	evelopment LP	Dec 21	B, 2022 09:05:28 CET		ClearPass Policy Manager 6.9.12.136929 on C	LABV (Trial Version) platform

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

Q ClearPass Policy Manager - Arub x +		~ - 🗆 X
← → C ▲ Inte säker   https://172.25.201.1	20/tips/tipsContentaction#	@ ☆ 🛛 😩 :
aruba	ClearPass Policy Manager	Menu 🗮
ि में Dashboard O	Configuration » Network » Device Groups	
Monitoring O	Network Device Groups	🐥 Add
Configuration 📀		Import Export All
- 🛱 Service Templates & Wizards	Device Group "Switches" added successfully	Export Air
- 🛱 Services	Device Groups function as a component in service and role mapping rules. Device groups can also be associated with enforcement profiles.	
Authentication     Q Identity		
Posture	Filter: Name V contains Contains Go Clear Filter	Show 20 v records
B Enforcement	# Name A Format Description	
🖻 📲 Network	1. Switches List Access Switches	
- Devices - Device Groups	Showing 1-1 of 1	Export Delete
- C Proxy Targets		
Event Sources		
- 🛱 Network Scan		
- 🛱 Policy Simulation		
Administration 0		
	elopment LP Dec 28, 2022 09:05:43 CET ClearPass Policy Manager 6.9.12.136929 on CL	A DV (Total Vania a) alabér ma
© Copyright 2022 Hewlett Packard Enterprise Dev	elopment LP Dec 28, 2022 09:05:43 CET ClearPass Policy Manager 6.9.12.136929 on CL	ABV (IIIal Version) platform

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 device software version, through network discovery. Use this information to create, update, or manage a device fingerprint in ClearPass Policy Manager. There you can also grant or deny access based on the AXIS OS version.

- 1. Go to Administration > Dictionaries > Device Fingerprints.
- 2. Select an existing device fingerprint or create a new device fingerprint.

## Secure onboarding - IEEE 802.1AR/802.1X

3. Set the device fingerprint settings.

Q ClearPass Policy Manager - Arub: × +								~ - 🗆 X
← → C ▲ Inte säker   https://172.25.201.12	20/tips/tips0	Content.action#tip	osFingerprintDictionary.action					e 🛧 🛛 😩 :
aruba	rubo ClearPass Policy Manager							
Dashboard     Monitoring     Monitoring     Configuration	Device	e Fingerprin	ries » Device Fingerprints	y the Profiler module. 1	These fingerprints are upda	ated from the Software (	Updates page. Name AXIS OS version unsupported AXIS OS version supported Axis Network Camero	Add Import Custom Fingerprints Export Custom Fingerprints Show 20 v records
Ciclicionaries  Ciclicionaries  Ciclicionaries  Ciclicionary Attributes  Ciclicionary Attribute	3. 4. Showing	Server	Name      Host MAC Vendor      LLDP System Descrip      SNMP System Descrip      Note: 0 Rule(s) will be deleted	Operator contains_all tion not_contains abtion not_contains	Value Axis Communications 10.12 10.12 Update Detect Finge	AB	Axis Print Server	
© Copyright 2022 Hewlett Packard Enterprise Deve	elopment L	P	Nov 25, 20	22 08:50:09 CET			ClearPass Policy Manager 6.9.12.1369	29 on CLABV (Trial Version) platform

The device fingerprint configuration in ClearPass Policy Manager. Axis devices that run any other AXIS OS version other than 10.12 are considered unsupported.

O ClearPass Policy Manager - Arub × +								× - □ :	×
← → C ▲ Inte säker   https://172.25.201.12	20/tips/tip:	sContent.action#tip	psFingerprintDictionary.action					e 🛧 🛯 😩	:
aruba			(	ClearPass Poli	icy Manager			Menu	E
Deskboard     Deskboard	Devic This pay Filter: [ # 1. 2. 3. 4.	ce Fingerpri	aries » Device Fingerprints	by the Profiler module.  Network Camera Axis Axis OS version sup Hatche Operator contains_all iption contains iption contains	These fingerprints are upda	Delete Rufe AB	Ipdates page. Name AXIS OS version unsupported AXIS OS version supported AXIS Network Camera Axis Print Server	Henu Add Import Custom Fingerprin Export Custom Fingerprin Show 20 ♥ record	nts its
d									
© Copyright 2022 Hewlett Packard Enterprise Deve	elopment	LP	Dec 05, 2	022 09:05:39 CET		C	ClearPass Policy Manager 6.9.12.136	29 on CLABV (Trial Version) platf	orm

The device fingerprint configuration in ClearPass Policy Manager. Axis devices that run AXIS OS 10.12 are considered supported in above example.

Information about the device fingerprint collected by ClearPass Policy Manager can be found in the Endpoints section.

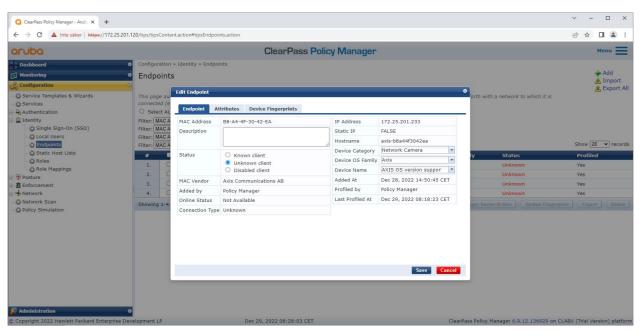
1. Go to Configuration > Identity > Endpoints.

#### Secure onboarding - IEEE 802.1AR/802.1X

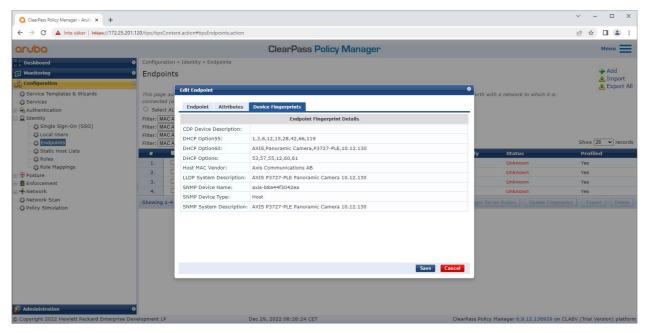
- 2. Select the device you want to view.
- 3. Click on the Device Fingerprints tab.

#### Note

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



An Axis device profiled by ClearPass Policy Manager.



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 HPE Aruba Networking access switch to ClearPass Policy Manager.

### Secure onboarding - IEEE 802.1AR/802.1X

#### Enforcement profile configuration

**Enforcement Profile** is used to allow ClearPass Policy Manager to assign a specific VLAN ID to an access port on the switch. It's 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 used VLANs. 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 ClearPass Policy Manager defines if Axis devices are granted access to HPE Aruba Networking powered networks based on four example policy profiles.

aruba		ClearPass Policy Manager						
Dashboard	• Configuration » Enforce	iguration » Enforcement » Profiles » Edit Enforcement Profile - Allow_VLAN_201						
Monitoring	<ul> <li>Enforcement Pr</li> </ul>	ofiles - Allow_VLAN_201						
Configuration	Summary Profile	Attributes						
🗘 Service Templates & Wizards	Profile:							
🛱 Services 🗣 Authentication	Name:	Allow_VLAN_201						
Identity	Description:							
🕆 Posture	Type:	RADIUS						
Enforcement	Action:							
- 🛱 Policies - 🛱 Profiles	Device Group List:	1. Switches						
Network	Attributes:	Attributes:						
🛱 Network Scan	Туре	Name		Value				
Policy Simulation	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				
Administration	Back to Enforcem	ent Profiles			Copy Save Ca			

An example enforcement profile to allow access to VLAN 201.

### Secure onboarding - IEEE 802.1AR/802.1X

ClearPass Policy Manager - Arub: × +				∨ - □ ×					
← → C ▲ Inte säker   https://172.	25.201.120/tips/tipsContent.action#	tipsEditEnforcementPolicy.action%3FcontextData%3D3007		🖻 🖈 🔲 😩 :					
aruba		ClearPass Policy Manager							
Dashboard	O Configuration » Enforce	nfiguration » Enforcement » Policies » Edit - Axis Radius policy							
Monitoring	<ul> <li>Enforcement Po</li> </ul>	nforcement Policies - Axis Radius policy							
Configuration	Summary Enforce								
<ul> <li>         —</li></ul>	Enforcement:								
Authentication	Name:	Axis Radius policy							
💿 🚨 Identity	Description:								
Posture	Enforcement Type:	RADIUS							
Brforcement     Policies	Default Profile:	Allow_VLAN_203							
- Ö Profiles	Rules:	tules:							
	Rules Evaluation Algori								
- 🛱 Network Scan	Conditions		Actions						
- 🎝 Policy Simulation	1. AND (Certificate AND (Certificate AND (Certificate AND (Certificate	CN CONTAINS Axis device ID Intermediate CA) Issuerb CFUXIS Axis Communications AB) Issubject- CFUXIS Evant Issubject- CFUXIS Evant Issubject- CFUXIS Evant Issubject- CFUXIS Evant Issubject- CFUXIS Evant Issubject- CFUXIS Evant Issubject- Second S	Allow_VLAN_201						
	2. AND (Certificate	-CN CONTAINS Production CA Certificate) :Subject-CN CONTAINS %{Connection:Client-Mac-Address-NoDelim})) ion:[Endpoints Repository]:Device Name EQUALS AXIS OS version unsupported)	Allow_VLAN_201						
	3. AND (Certificate:Issue	-CN CONTAINS Production CA certificate) :Subject-CN CONTAINS %{Connection:Client-Mac-Address-NoDelim})) ion:Endpoints Repository]:Device Name EQUALS AXIS OS version supported)	Allow_VLAN_202						
🏂 Administration	Back to Enforcem	ent Policies	G	opy Save Cancel					
© Copyright 2022 Hewlett Packard Enterpr	ise Development LP	Dec 28, 2022 09:49:09 CET	ClearPass Policy Manager 6.9.12.136929 on C	LABV (Trial Version) platform					

The enforcement policy configuration in 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 AXIS OS updates, production-grade certificates, and other configurations. The following conditions are verified by ClearPass Policy Manager:

- The Axis device's AXIS OS version.
- 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 ID certificate is verifiable and matches the Axis-specific attributes such as issuer, organization, location, and country.

#### Production network (VLAN 202)

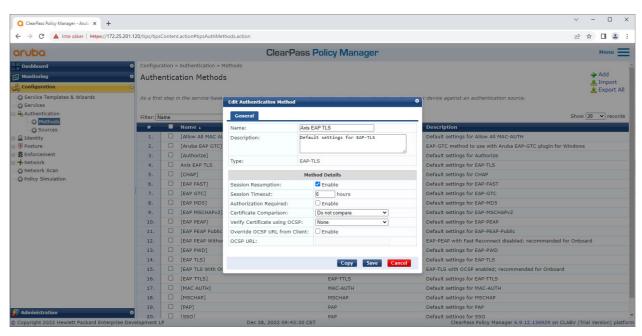
The Axis device is granted access to the production network where the Axis device should operate. Access is granted after the device provisioning is completed from within the provisioning network (VLAN 201). The following conditions are verified by ClearPass Policy Manager:

- 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 AXIS OS 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's defined how an Axis device attempts to authenticate against the 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.



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

#### Service configuration

On the Services page, the configuration steps are combined into one single service that handles the authentication and authorization of Axis devices in HPE Aruba Networking powered networks.

# Secure onboarding - IEEE 802.1AR/802.1X

← → C ▲ Inte säker https://172.25.20	1.120/tips/tipsContent.acti	ion#tipsEditService.action%3FcontextData%3D3001		16 \$					
aruba			Monoren		Menu =				
aroba		ClearPass Polic	y Manager		Hend =				
Dashboard	• Configuration » Ser	rvices » Edit - Axis 802.1X Wired							
Monitoring	<ul> <li>Services - Ax</li> </ul>	kis 802.1X Wired							
Configuration	Summary Ser	vice Authentication Roles Enforcement							
Service Templates & Wizards Services	Name:	Axis 802.1X Wired							
Authentication	Description:	To authenticate users to any wired network via 802.1X.							
TP Posture	Type:	802.1X Wired							
- 3 Enforcement - 4 Network	Status:	Enabled							
🛱 Network Scan	Monitor Mode:	Enable to monitor network access without enfo	rcement						
C Policy Simulation	More Options:	Authorization Posture Compliance Audit	End-hosts 🗌 Profile Endpoints 🗌 Accounting Proxy						
		Service Rule							
	Matches O ANY or	r 🖲 ALL of the following conditions:							
	Туре	Name	Operator	Value					
	1. Radius:IETF	NAS-Port-Type	EQUALS	Ethernet (15)	82 1				
	2. Radius:IETF	Service-Type	BELONGS_TO	Login-User (1), Framed-User (2), Authenticate-Only (8)	82 10				
	3. Click to add.								
	3. Click to add.								

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

Q ClearPass Policy Manager - Arub: × +					× - 🗆 ×
← → C ▲ Inte säker   https://172.25.201	120/tips/tipsContent.action#tips	EditService.action%3FcontextData%3D3001			ic ☆ 🛛 😩 :
aruba		ClearPass	Policy Manager		Menu 🗮
Dashboard	Configuration » Services »	Edit - Axis 802.1X Wired			
Monitoring	Services - Axis 80	2.1X Wired			
Configuration	Summary Service	Authentication Roles Enforcement			
Corrice Templates & Wizards     Corrice Templates & Wizards     Corrice     Corrice     Corrice     Corrice     Corright     Corr	Authentication Methods:	Axis EAP TLS	Move Up 1 Move Down 1 Remove View Details Modify		Add New Authentication Method
- Q Policy Simulation	Authentication Sources:	[Endpoints Repository] [Local SQL DB]			Add New Authentication Source
			Move Up 1 Move Down 1 Remove View Details Modify		
		Select to Add	~		
	Strip Username Rules:	Enable to specify a comma-separated I	ist of rules to strip username prefixes or suffixes		
	Service Certificate:	Select to Add			View Certificate Details
🎉 Administration 💦	Back to Services			Disable	Copy Save Cancel
© Copyright 2022 Hewlett Packard Enterprise De	velopment LP	Dec 28, 2022 09:41:41 CE	T	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.

#### Secure onboarding - IEEE 802.1AR/802.1X

ClearPass Policy Manager - Arub × +			✓ - □ X
← → C ▲ Inte säker   https://172.25.201.1	20/tips/tipsContent.action#tips	ditService.action%3FcontextData%3D3001	🖻 🖈 🔲 🌲 🗄
aruba		ClearPass Policy Manager	Menu 🗮
Dashboard	Configuration » Services »	Edit - Axis 802.1X Wired	
Monitoring O	Services - Axis 80	2.1X Wired	
Configuration O	Summary Service	Authentication Roles Enforcement	
- 🛱 Service Templates & Wizards	Use Cached Results:	Use cached Roles and Posture attributes from previous sessions	
- 🛱 Services	Enforcement Policy:	Axis Radius policy V Modify	Add New Enforcement Policy
🗉 🧕 Identity		Enforcement Policy Det	ils
Posture     Strengthered	Description:		
Behorcement     Friedmann	Default Profile:	Allow_VLAN_203	
- 🛱 Network Scan	Rules Evaluation Algorithm	: first-applicable	
- 🛱 Policy Simulation	Conditions		Enforcement Profiles
	AND (Certificate AND (Certificate AND (Certificate AND (Certificate AND (Certificate	CN CONTAINS Axis device ID Intermediate CA) Issuero EQUALS Axis Communications AB) Subject- EQUALS Axis Communications AB) Subject- EQUALS Lund) Subject- EQUALS Lund) (Subject- EQUALS Subject-serialNumber)	Allow_VLAN_201
	(Certificate:Issuer- 2. AND (Certificate	(CN CONTAINS Production CA Certificate) :Subject-CN CONTAINS %(Connection:Client-Mac-Address-NoDelim)) ion:[Endpoints Repository]:Device Name EQUALS AXIS OS version unsupported)	Allow_VLAN_201
	3. AND (Certificate	CN CONTAINS Production CA certificate) :Subject-CN CONTAINS %{Connection:Client-Mac-Address-NoDelim})) ion:Endpoints Repository]:Device Name <i>EQUALS</i> AXIS OS version supported)	Allow_VLAN_202
	Back to Services		Disable Copy Save Cancel
Administration 0	alarmant 10	D 00 0000 00-F1-01 CFT	
© Copyright 2022 Hewlett Packard Enterprise Dev	elopment 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.

#### HPE Aruba Networking access switch

Axis devices are either directly connected to PoE-capable access switches or via compatible Axis PoE midspans. To securely onboard Axis devices into HPE Aruba Networking powered networks, the access switch needs to be configured for IEEE 802.1X communication. The Axis device relays IEEE 802.1x EAP-TLS communication to 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 HPE Aruba Networking access switches.

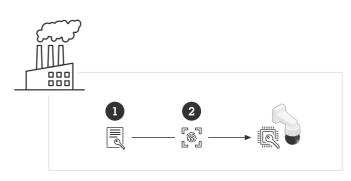
```
radius-server host MyRADIUSIPAddress key "MyRADIUSKey"
aaa authentication port-access eap-radius
aaa port-access authenticator 18-19
aaa port-access authenticator 18 reauth-period 300
aaa port-access authenticator 19 reauth-period 300
aaa port-access authenticator active
```

#### **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.

		AXIS Q1656 Box Camera				
🔁 Status						
□ Video	~	Certificates				
⊕ PTZ		+ Add certificate		- <u>a</u> •		
🛓 Audio	~	17				
Recordings		Name	Туре			
🗱 Apps		Axis device ID ECC-P256 (802.1AR)	Client-server			
鑗 System	^	Axis device ID RSA-2048 (802.1AR)	Client-server			
Date and time						
Network		Axis device ID RSA-4096 (802.1AR)	Client-server			
Security		Axis device ID Intermediate CA ECC 2	CA			



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 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



	Country	SE
	Location	Lund
Ī	Issuer Organization	Axis Communications AB

### Secure onboarding - IEEE 802.1AR/802.1X

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.

		AXIS Q1656 Box Camera	Ø 🐺 () 🖪 🗄
22 Status □ Video ⊕ PTZ ▲ Audio © Recordings	~ ~	IEEE 802.1x Connecting      Client certificate ①     EAPOL Version      Axis device ID R5A-2048 (802.1AR)     O 1      CA certificates ①     CA certificates ①     Xo CA certificate selected     v	
System System Date and time Network	^	EAP Identity Use IEEE 802.1 axis-b8a44f27a03a	
Security			Save

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 AXIS OS 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

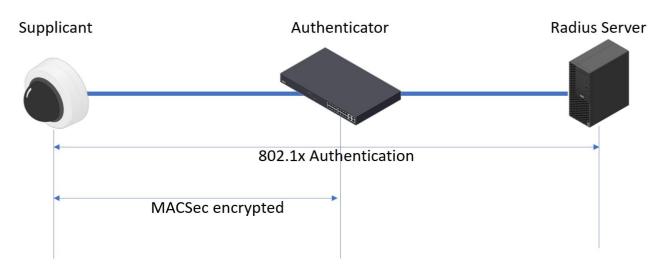


IEEE 802.1AE MACsec (Media Access Control Security) is a well-defined network protocol that cryptographically secures

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 the 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 HPE Aruba Networking access switch.

### Secure network operation - IEEE 802.1AE MACsec

IEEE 802.1AE MACsec requires both HPE Aruba Networking 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 HPE Aruba Networking access switch doesn't support MACsec using EAP-TLS, then the Pre-Shared Key mode can be used and manually configured.

## HPE Aruba Networking ClearPass Policy Manager

#### Role and role mapping policy

aruba				ClearPa	ss Policy Manager		Menu
Dashboard	O Config	Configuration » Identity » Roles					
Monitoring	Role	s					🚽 Add
Configuration							🐣 Import 🏩 Export A
- 🛱 Service Templates & Wizards - 🙀 Services	Roles e	exist in	dependently of an indi	vidual service and can be	accessed globally through the role	e-mapping policy of any service.	
Authentication	Filter:	Name	~	contains 🗸	🕂 🛛 🕞 🕞	ter	Show 20 V record
Methods	#		Name 🛦		Description		
- 🛱 Sources	1.		[AirGroup v1]		Role for an AirGroup pro	otocol version 1 request	
Single Sign-On (SSO)	2.					otocol version 2 request	
- O Local Users	3.			d-only Admin1		ly access to Aruba device	
- 🛱 Endpoints	4.				Default role for root acc		
- 🛱 Static Host Lists	5.					•	
- 🛱 Roles	6,					age their own provision	ed devices
- CROINE Mappings	7.		Contrac	3001			
Posture     Osture     Posture	8.		Name:	AxisDe	vice	their devices for use w	ith MAC authentication and AirGroup sharing.
- Q Audit Servers	9.		Descriptio	in:		their devices, for use w	and Androup sharing.
Agentless OnGuard	10.						
B Enforcement							
- 🛱 Policies	11.			1			
- C Profiles	12.					Save Cancel	
- + Network	13.						
- Devices	14.				Role for an iOS device b		
— Device Groups — Device Groups	15.				Role for an iPadOS devi	2. S.	
- C Event Sources	16.				Role for Linux device be		
- Q Network Scan	17.				Role for a macOS device		
- Delicy Simulation	18.		-		Role for a Windows devi		
	19.				Default role for another	user or device	
	20.		[TACACS+ API Admir	1]	API administrator role fo	or Policy Manager Admin	
	Showin	ng 1-20	0 of 25 🕨 🕨				

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

## Secure network operation - IEEE 802.1AE MACsec

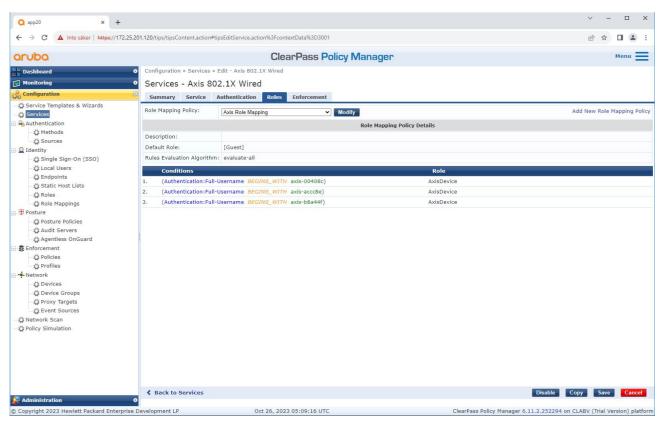
<b>Q</b> app20 × +				✓ - □ X
← → C ▲ Inte säker   https://172.	25.201.120/tips/tipsContent.acti	on#tipsEditRoleMappingPolicy.action%3FcontextData%3D3001		@☆□:
aruba		ClearPass Policy Mana	ager	Menu
Dashboard	• Configuration » Identit	y » Role Mappings » Edit - Axis Role Mapping		
Honitoring	Role Mappings	- Axis Role Mapping		
& Configuration	Summary Policy			
- C Service Templates & Wizards - C Services	Policy:	наррину кинез		
🖃 🚘 Authentication	Policy Name:	Axis Role Mapping		
— 🛱 Methods	Description:			
- O Sources	Default Role:	[Guest]		
Identity	Mapping Rules:			
- O Local Users	Rules Evaluation Algor	ithm: Evaluate all		
- 🛱 Endpoints	Conditions		Role Name	
- 🛱 Static Host Lists	1. (Authentication:Fu	III-Username BEGINS_WITH axis-00408c)	AxisDevice	
- 🗘 Roles	2. (Authentication:Fu	III-Username BEGINS_WITH axis-accc8e)	AxisDevice	
Role Mappings	3. (Authentication:Fu	III-Username BEGINS_WITH axis-b8a44f)	AxisDevice	
→ Posture Policies     → Addit Servers     → Addit Servers     → Policies     → Profiles     → Profiles     → Profiles     → Porox Targets     → Proxy Targets     → Policy Simulation				
	K Back to Role Map	pings		Copy Save Cancel
Administration	•			
© Copyright 2023 Hewlett Packard Enterpri	ise Development LP	Oct 26, 2023 05:08:20 UTC	ClearPass Policy Manager 6.11.2.252294 on	CLABV (Trial Version) platform

Add 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 becomes a 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



Add 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

Q app20 × +			∨ - □ X
← → C ▲ Inte säker   https://172.	25.201.120/tips/tipsContent.action	#tipsEditService.action%3FcontextData%3D3001	ie 🖈 🗖 😩 :
aruba		ClearPass Policy Manager	Menu
Dashboard	• Configuration » Services	» Edit - Axis 802.1X Wired	
Monitoring	Services - Axis 8	802.1X Wired	
Configuration	Summary Service	Authentication Roles Enforcement	
—      —      Q Service Templates & Wizards     —      —      Services	Use Cached Results: Enforcement Policy:	Use cached Roles and Posture attributes from previous sessions	Add New Enforcement Polic
Authentication	Enforcement Policy.	Axis Radius policy V Modify	Add New Enforcement Polic
- Sources		Enforcement Pol	licy Details
🖃 🧕 Identity	Description:		
- 🛱 Single Sign-On (SSO)	Default Profile:	Allow_VLAN_203	
Cocal Users	Rules Evaluation Algorith	nm: evaluate-all	
- 🛱 Endpoints - 🛱 Static Host Lists	Conditions		Enforcement Profiles
- ☆ Roles - ☆ Role Mappings - ☆ Posture - ☆ Posture Policies - ☆ Audit Servers	1. AND (Certifica AND (Connect serialNumber}) AND (Tips:Rol	te:Issuer-D EQUALS Axis Communications AB) te:Subject-D EQUALS Axis Communications AB) ion:Client-Mac-Address-NoDelim EQUALS %{Certificate:Subject- e EQUALS AxisDevice) archl CORTENS Enduction CA)	Allow_VLAN_201
- 🖧 Agentless OnGuard - 😵 Enforcement - 🛱 Policies - 🎝 Profiles	AND (Authoriz 2. unsupported) AND (Certifica	er-CN CONTAINS Production CA) ation:[Endpoints Repository]:Device Name EQUALS AXIS OS version te:Subject-CN CONTAINS Production XYZ) e EQUALS AxisDevice)	Allow_VLAN_201
	(Certificate:Issue AND (Authoriz 3. supported) AND (Certifica	ar-CN CONTAINS Production CA) ation: [Endpoints Repository]: Device Name EQUALS AXIS OS version te: Subject-CN CONTAINS Production XYZ) e EQUALS AvisDevice)	Allow_VLAN_202
- ☆ Event Sources - ☆ Network Scan - ☆ Policy Simulation			
Administration	Back to Services		Disable Copy Save Cancel
© Copyright 2023 Hewlett Packard Enterpri	ise Development LP	Oct 26, 2023 05:11:50 UTC	ClearPass Policy Manager 6.11.2.252294 on CLABV (Trial Version) platfo

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

#### Secure network operation - IEEE 802.1AE MACsec

#### **Enforcement profile**

Q app20 × +				∨ – □ X					
← → C ▲ Inte säker   https://172.25.20	1.120/tips/tipsContent.action	#tipsEditEnforcementProfile.action%3FcontextData%3D3004		@ ☆ 🛛 🏝 :					
aruba		ClearPass Policy Manager							
Dashboard 0	Configuration » Enforcen	Configuration » Enforcement » Profiles » Edit Enforcement Profile - Allow_VLAN_201							
Monitoring 0	Enforcement Pro	files - Allow_VLAN_201							
Configuration		Attributes							
- 🛱 Service Templates & Wizards - 🛱 Services	Profile:	HIGH DICE							
- Authentication	Name:	Allow_VLAN_201							
- 🗘 Methods	Description:								
- 🛱 Sources	Type:	RADIUS							
🖃 🗕 Identity 👘 Single Sign-On (SSO)	Action:	Accept							
- 🛱 Local Users	Device Group List:	1. Switches							
- C Endpoints	Attributes:								
- 🛱 Static Host Lists	Туре	Name	Value						
- 🛱 Roles	1. Radius:IETF	Session-Timeout	= 10800						
- 🎝 Role Mappings	2. Radius:IETF	Termination-Action	= RADIUS-Request (1)						
Posture     Posture Policies	3. Radius:IETF	Tunnel-Type	= VLAN (13)						
- O Audit Servers	4. Radius:IETF	Tunnel-Medium-Type	= IEEE-802 (6)						
Agentless OnGuard	5. Radius:IETF	Tunnel-Private-Group-Id	= 201						
Enforcement	6. Radius:Aruba	Aruba-User-Role	= AxisDevice						
- 🗘 Policies									
Profiles									
Devices									
- O Device Groups									
- 🛱 Proxy Targets									
- 🛱 Event Sources									
- 🛱 Network Scan									
- C Policy Simulation									
	d Darlaha Fafa	at Desfiles							
Administration 0	& Back to Enforceme	nt Profiles		Copy Save Cancel					
© Copyright 2023 Hewlett Packard Enterprise D	evelopment LP	Oct 26, 2023 05:13:21 UTC	ClearPass Policy Manage	r 6.11.2.252294 on CLABV (Trial Version) platform					

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

### HPE Aruba Networking access switch

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

## 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, ClearPass Policy Manager validates the Axis device's MAC address and grant access to the network.

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

### HPE Aruba Networking ClearPass Policy Manager

#### **Enforcement policy**

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

1.120/tips/tipsContent.action	+tipsEditService.action%3FcontextData%3D3006	🖻 🛧 🔳	<b>a</b> :
	ClearPass Policy Manager	Men	"
Configuration » Services	» Edit - Axis 802.1X Wired - Mac Authentication		
Services - Axis 8	02.1X Wired - Mac Authentication		
Summary Service	Authentication Roles Enforcement		
Conditions (Date:Day-of-We 1. AND (Date:Tim	[Deny Access Profile] m: evaluate-all ek <u>BELONGS_TO</u> Monday, Tuesday, Wednesday, Thursday, Friday) e-of-Day <u>IN_RANGE</u> 09:00:00,17:00:00)		nt Policy
Back to Services evelopment   P	0+26-2023-05-15-57 UTC		ancel
	Configuration > Services Services - Axis 8 Summary Service Use Cached Results: Enforcement Policy: Description: Default Profile: Rules Evaluation Algorith Coate:Day-of-We 1. AND (Date:Tim AND (Connection)	Configuration » Services » Edit - Axis 802.1X Wired - Mac Authentication Services - Axis 802.1X Wired - Mac Authentication Summary Service Authentication Roles Enforcement Use Cached Results: Use cached Results: Lose cached Reles and Posture attributes from previous sessions Enforcement Policy: Axis MAC Authentication Policy Modify Description: Default Profile: [Deny Access Profile] Rules Evaluation Algorithm: evaluate-all Conditions (Date:Day-of-Nay IN_CAAKE 09:08:00.17:00:00) AND (Connection:Client-Mac-Vendor EQUALS Axis Communications AB)  AND (Connection:Client-Mac-Vendor EQUALS Axis Communications AB)	ClearPase Doicy Managen Memi   Configuration + Services + Edit - Adis 802.112 Wired - Nac Authentication   Services - Axis 802.112 Wired - Mac Authentication   Test Cached Results: Use cached Roles and Posture attributes from previous sessions   Enforcement Policy: Los Gached Roses Profile]   Rescription: Description:   Description: (Denry Access Profile]   Ruite Stabulation Algo (Cannettion: Cleant-Mac Vendor: EQUALS Axis Communications AB)   Add New Enforcement Policy:   Image: Cleant Policy: Los Gached Roses Artification Policy:   Image: Cleant Policy: Los Gached Roses Profile]   Ruite: Cleant Policy:   Cleant Policy: Cleant Policy:   Image: Cleant Policy: Cleant Policy:   Image: Cleant Policy: Cleant Policy:   Ruite: Cleant:   Ruite: Ruite:   Ruite: Cleant:   Ruite: Ruite:   Ruite: Ruite:   Ruite: Ruite:   Ruite: Ruite:   Ruite: Ruite:   Ruite: Ruite:   R

#### 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's a weekday between Monday and Friday
- It's between 09:00 and 17:00

## Legacy onboarding - MAC authentication

• The MAC address vendor matches with Axis Communications.

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

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

aruba			ClearP	ass Policy Manager				Menu	' =
Dashboard	O Config	uration	» Authentication » Sources						
Monitoring	O Auth	entic	ation Sources					🛖 Ad	d
Configuration	0								port
🖞 Service Templates & Wizards	An aut	thentica	tion source is the identity store (Active Direc	tory, LDAP directory, etc.) against which user	s and devices are authenticated			😩 Ex	рогт
C Services	Anada	inentica	uon source is the identity store (Active Direc	tory, LDAF directory, etc.) against which user	s and devices are authenticated.				
Authentication	-11			+ Go Clear Filter		c	how	20 🗸	raca
- 🗘 Methods	Filter:	-	✓ contains ✓			31	now	20 •	Tecor
- 🛱 Sources	#		Name 🔺	Туре	Description				
Q Identity	1.		[Admin User Repository]	Local SQL DB	Authenticate users against Policy Manager admin u				
- 🛱 Single Sign-On (SSO) - 🛱 Local Users	2.		[Denylist User Repository]	Local SQL DB	Denylist database with users who have exceeded b related limits	andwidt	h or s	ession	
- C Endpoints	з.		[Endpoints Repository]	Local SQL DB	Authenticate endpoints against Policy Manager loca	al databa	ase		
- 🛱 Static Host Lists	4.		[Guest Device Repository]	Local SQL DB	Authenticate guest devices against Policy Manager	local da	tabas	e	
- Q Roles	5.	0	[Guest User Repository]	Local SQL DB	Authenticate guest users against Policy Manager local database				
- 🛱 Role Mappings	6.		[Insight Repository]	Local SQL DB	Insight database with session information for users and devices				
🕆 Posture	7.	0	[Local User Repository]	Local SQL DB	Authenticate users against Policy Manager local us				
- 🛱 Posture Policies	8.	0	[Onboard Devices Repository]	Local SQL DB	Authenticate Onboard devices against Policy Manager local database				
- 🛱 Audit Servers	9.	0	[Social Login Repository]	Local SQL DB	Authenticate users against Policy Manager social login database				
Agentless OnGuard	10.		[Time Source]	Local SQL DB	Authorization source for implementing various time functions				
Enforcement Dicies	10.		The second s	HTTP					
- Profiles			[Zone Cache Repository]	HTTP	Access attributes cached by Context Server Actions				
Network	Showin	ng 1-11	of 11			ору	Exp	ort	Delet
- Ö Devices									
Device Groups									
- O Proxy Targets									
Event Sources									
🗘 Network Scan									
D Policy Simulation									
· · · · · / -									
Administration	0								
					ClearPass Policy Manager 6.11.2.252294 on 0				

# Legacy onboarding - MAC authentication

<b>Q</b> app20 × +			✓ - □ X			
← → C ▲ Inte säker   https://172.2	5.201.120/tips/tipsContent.action#	tipsAddAuthSource.action	e 🖈 🛛 😩 :			
aruba		ClearPass Policy Manager	Menu 🗮			
Dashboard	<ul> <li>Configuration » Authentic</li> </ul>	ation » Sources » Add				
Monitoring	<ul> <li>Authentication So</li> </ul>	Authentication Sources				
& Configuration		Lists Summary				
- 🛱 Service Templates & Wizards	-					
- 🛱 Services	Name:	Axis Devices				
🖃 🗣 Authentication	Description:	MAC addresses of Axis devices in use.				
- 🛱 Methods						
- 🛱 Sources	Туре:	Static Host List				
□- Q Identity Single Sign-On (SSO)	Use for Authorization:	Enable to use this Authentication Source to also fetch role mapping attributes				
- C Local Users	Authorization Sources:	Enable to use this Autoentication Source to also retch fore mapping attributes				
- 🛱 Endpoints	Authorization Sources.	Remove				
- 🛱 Static Host Lists		View Details				
- 🛱 Roles		×				
🔤 🛱 Role Mappings						
🖃 📅 Posture						
- C Posture Policies						
- 🛱 Audit Servers - 🛱 Agentless OnGuard						
- Ö Policies						
Drofiles						
- 🛱 Devices						
- 🛱 Device Groups						
- 🛱 Proxy Targets						
- 🛱 Event Sources						
- 🛱 Network Scan						
- C Policy Simulation						
	Sack to Authenticat	ion Sources	Next → Save Cancel			
🚑 Administration	O Back to Authenticat					
© Copyright 2023 Hewlett Packard Enterpris	se 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

					✓ - □ X
Q app20 × +					
← → C ▲ Inte säker   https://172.25.20	1.120/tips/tipsContent.action#				ie 🛧 🔲 😩 :
aruba		Clear	Pass Policy Manager	•	Menu 🗮
Dashboard 0	Configuration » Authentica	tion » Sources » Add			
Monitoring 0	Authentication So	urces			
Configuration 📀	General Static Host Li	sts Summary			
- 🛱 Service Templates & Wizards	MAC Address Host Lists:	-			Add New Static Host List
- Services	The Address host clots.	Add Static Host List		0	Add New Static Host List
Authentication		Name:	Axis devices		
- Sources		Description:			
🖃 🧕 Identity		beschption.			
- 🛱 Single Sign-On (SSO)			ļ	A	
- 🛱 Local Users - 🛱 Endpoints		Host Format:	O Subnet O Regular Expression		
- 🛱 Static Host Lists			List		
- 🛱 Roles		Host Type:	O IP Address		
- 🛱 Role Mappings		1999	MAC Address		
🖃 🖶 Posture		Host Entries			
- C Posture Policies - C Audit Servers		# Address	Description		
- Agentless OnGuard		1. O B8-A4-4F-45-B4-E		8	
Enforcement		2. O B8-A4-4F-45-B4-E		<u></u>	
- 🛱 Policies		3. O B8-A4-4F-45-B4-E	8 Axis Device 3	U	
- C Profiles		Address:			
- 🖧 Devices		Description:			
- Device Groups					
- Proxy Targets				Save Host	
- 🛱 Event Sources					
- 🛱 Network Scan - 🗘 Policy Simulation					
- La Policy Simulation				ve Cancel	
			34	Cancer	
	K Back to Authentication	on Sources			Next → Save Cancel
🐉 Administration 🛛 🛛 🛛 🛛					
© Copyright 2023 Hewlett Packard Enterprise D	evelopment LP	Oct 31, 2023 09	:20:18 UTC		ClearPass Policy Manager 6.11.2.252294 on CLABV (Trial Version) platform

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

## Legacy onboarding - MAC authentication

<b>Q</b> app20 × +			✓ - □ ×					
← → C ▲ Inte säker   https://172.2	5.201.120/tips/tipsContent.action#		ie 🛧 🛛 😩 :					
aruba		ClearPass Policy Manager	Menu 🗮					
Dashboard	• Configuration » Authentication »	Sources » Add						
Monitoring	<ul> <li>Authentication Source</li> </ul>	Authentication Sources						
& Configuration		List "Axis devices" added succes	sfully					
- & Service Templates & Wizards								
- 🗘 Services	General Static Host Lists	Summary						
Authentication     Authentication     Authentication     C Sources     C Sources     C Local Users     C Local Users     C Static Host Lists     C Static Host Lists     C Roles     C Role Mappings		elect-	Add New Static Host List					
Posture     Policies     Audit Servers     Agentless OnGuard								
- 🎝 Policy Simulation	o Seck to Authentication Se		Next→ Save Cancel					
© Copyright 2023 Hewlett Packard Enterpris	e Development LP	Oct 31, 2023 09:20:34 UTC	ClearPass Policy Manager 6.11.2.252294 on CLABV (Trial Version) platfor					

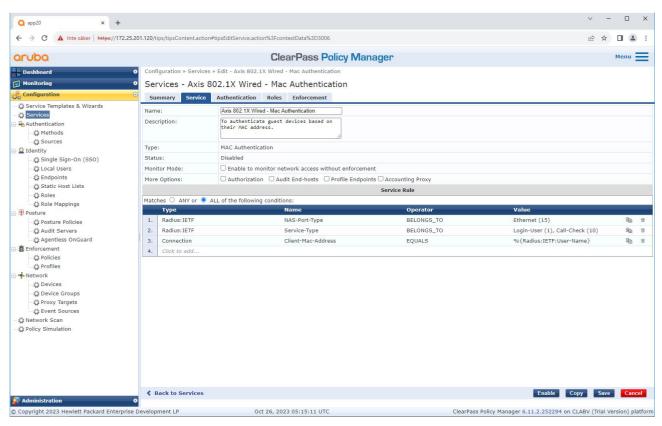
### Service configuration

On the Services page, the configuration steps are combined into one single service that handles the authentication and authorization of Axis devices in HPE Aruba Networking powered networks.

# Legacy onboarding - MAC authentication

aruba	ClearPass Policy Manager								
Dashboard O	onfigura	ation >	<ul> <li>Services</li> </ul>						
🖅 Monitoring 🛛 🛛 🤤	Servic	es							Add
Configuration 📀									Import Export A
Service Templates & Wizards     7       Services     7	his page	∍ shov	vs the cun	rent list and order of services that ClearPass follo	ws during authentication and	l authorization.		<u> </u>	Export A
Authentication F	ilter: Na	ame		✓ contains ✓	Go Clear Filter	Hit Count for Current hour 🗸		Show 20	✓ record
- 🛱 Methods - 🛱 Sources			Order 🔺	Name	Туре	Template	Hit	Count S	Status
Q Identity	1.		1	Axis 802.1X Wired	RADIUS	802.1X Wired	0	0	( )
Single Sign-On (SSO)	2.	0	2	Axis 802.1X Wired - Mac Authentication	RADIUS	MAC Authentication	0	0	
Local Users	3.		3	Test Service	RADIUS	802.1X Wired	0	0	
- 🛱 Endpoints	4.	0	4	[Policy Manager Admin Network Login Service]	TACACS+	TACACS+ Enforcement	0	ō	
- 🛱 Static Host Lists	5.	0	5	[AirGroup Authorization Service]	RADIUS	RADIUS Enforcement ( Generic )	0	ō	
- 🛱 Roles	6.		6	[Aruba Device Access Service]	TACACS+	TACACS+ Enforcement	0	ŏ	
- 🛱 Role Mappings	7.		7	[Guest Operator Logins]	Application	Aruba Application Authentication	0	ŏ	
Posture Policies	8.		8	[Insight Operator Logins]	Application	Aruba Application Authentication	0	ŏ	
- Q Audit Servers	9.		9	[Device Registration Disconnect]	WEBAUTH	Web-based Authentication	0		
Agentless OnGuard	128			[Device Registration Disconnect]	WEBAOTH				
S Enforcement S	howing	1-9 of	19			R	eorder Co	py Export	Delete
- 🛱 Policies									
- 🛱 Profiles									
+ Network									
- 🛱 Devices									
- 🛱 Device Groups									
Proxy Targets									
- C Event Sources									
- C Event Sources									
Event Sources									
- C Event Sources									
Event Sources									
Event Sources									
- C Event Sources									
- C Event Sources									
- C Event Sources									
- C Event Sources									

## Legacy onboarding - MAC authentication



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

## Legacy onboarding - MAC authentication

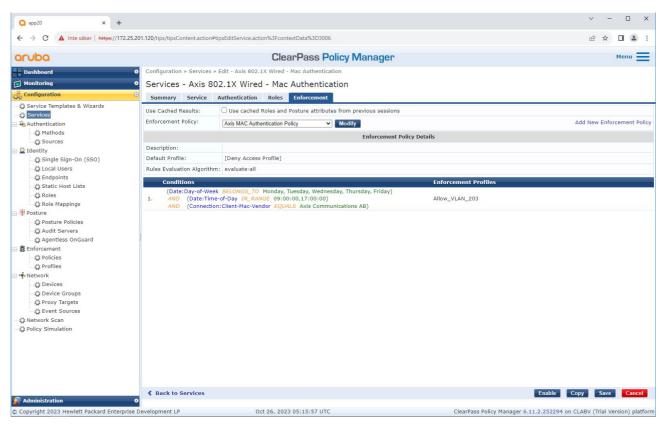
Q app20 × +					✓ – □ ×
← → C ▲ Inte säker   https://172.2	25.201.120/tips/tipsContent.action#t	ipsEditService.action%3FcontextData%3D	/3006		ig ☆ 🛛 😩 :
aruba		ClearPass	Policy Manager		Menu
Dashboard	• Configuration » Services »	Edit - Axis 802.1X Wired - Mac Authe	ntication		
Monitoring	Services - Axis 80	2.1X Wired - Mac Authen	itication		
🝰 Configuration	Summary Service	Authentication Roles Enforcem	ient		
	Authentication Methods:	[Allow All MAC AUTH]	Move Up : Move Down L Remove View Details Modify	Add	New Authentication Method
- 🛱 Local Users - 🛱 Endpoints		Select to Add	~		
-☆ Static Host Lists -☆ Roles -♀ Role Mappings -♀ Posture -♀ Posture Policies -♀ Audit Servers -♀ Audit Servers	Authentication Sources:	Axis Devices [Static Host List]	Move Up † Move Down L Remove View Details Modify	Add	d New Authentication Source
Enforcement		Select to Add	~		
Policies     Orofiles     Network	Strip Username Rules:	Enable to specify a comma-separa	ated list of rules to strip username prefixes	or suffixes	
Cevices     Cevice Groups     Cevice Groups     Proxy Targets     Ceven Sources     Qent Sources     One Sources     One Sources     One Sources					
🚰 Administration © Copyright 2023 Hewlett Packard Enterpri	Back to Services     Services	Oct 31, 2023 09:22:22	UTC	Disable C ClearPass Policy Manager 6.11.2.252294 on 0	opy Save Cancel

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 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



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

#### HPE Aruba Networking access switch

In addition to the secure onboarding configuration described in *HPE Aruba Networking access switch on page 16*, refer to the below example port configuration for the HPE Aruba Networking 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
```

Integration Guide HPE Aruba Networking © Axis Communications AB, 2023 - 2024 Ver. M6.2 Date: May 2024 Part no. T10197992