

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 Networking	5
Configuration Axis	16
Secure network operation – IEEE 802.1AE MACsec	19
HPE Aruba Networking ClearPass Policy Manager	20
HPE Aruba Networking access switch	24
Legacy onboarding – MAC authentication	25
HPE 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.

Q ClearPass Policy Manager - Arub: × +				∨ - □ X								
← → C ▲ Inte säker   https://172.25.201.1	120/tips/tip	Content.action#tipsCertTrustList.action		ie 🛧 🛛 😩 :								
aruba	ClearPass Policy Manager											
E II Dashboard O	Adminis	ninistration » Certificates » Trust List										
Monitoring O	Certi	icate Trust List		👍 Add								
🔗 Configuration 🔹 💿	This pa	ge displays a list of trusted Certificate Authorities (CA). You can add, view, or delete a certificate.										
🚱 Administration 💿												
P ClearPass Portal	Filter:	subject		Show 20 v records								
🗄 🚘 Users and Privileges		Subject •	Usage	Validity Enabled								
Server Manager	1.	CN=Axis device ID Root CA RSA,O=Axis Communications AB	EAP	Valid Enabled								
- P External Accounts	2.	CN=Axis device ID Root CA ECC,O=Axis Communications AB	EAP	Valid Enabled								
E 🔓 Certificates	з.	CN=Axis device ID Intermediate CA RSA 2,0=Axis Communications AB	EAP	Valid Enabled								
- 🖉 Certificate Store	4.	CN=Axis device ID Intermediate CA RSA 1,0=Axis Communications AB	EAP	Valid Enabled								
- Just List	5.	CN=Axis device ID Intermediate CA ECC 2,0=Axis Communications AB	EAP	Valid Enabled								
- A Revocation Lists	6.	CN=Axis device ID Intermediate CA ECC 1,0=Axis Communications AB	EAP	Valid Enabled								
Agents and Software Updates	Showin	1-6 of 6		Delete								
🗈 🗣 Support												
© Copyright 2022 Hewlett Packard Enterprise Dev	velopment	P Nov 25, 2022 08:48:50 CET	ClearPass Policy Manager 6.9	.12.136929 on CLABV (Trial Version) platfor								

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 × +		✓ - □ ×
← → C ▲ Inte säker   https://172.25.20	1.120/tips/tipsContent.action#tipsNetworkDevices.action	@ 🛧 🔲 😩 :
aruba	ClearPass Policy N	lanager Menu 🗮
Dashboard	o Configuration » Network » Devices	
Monitoring	<ul> <li>Network Devices</li> </ul>	🛶 Add
& Configuration		Limport
		Copyre and     Support     Support and     Support and     Support and
- 🛱 Services	A Network Access Device (NAD) must belong to the global list of devices in the Clea	Pass database in order to connect to ClearPass.
Authentication		
Desture	Filter: Name v contains v Go	Clear Filter Show 20 👻 records
	# Name A IP or Subnet Address	Device Groups Description
- + Network		Copy Export Delete
- 🗘 Devices		
- Device Groups		
Proxy Targets		
- O Network Scan		
- O Policy Simulation		
Administration	0	

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#					e 🛧 🗖 😩 :
aruba		ClearPass Policy	y Manager			Menu 🗮
Deshboard     Deshboard     Configuration     Configuration     Service Templates & Wizards     Services	Configuration > Network > Devices Network Devices Add Device				•	Add Limport Export All Discovered Devices
A subtraction     A subtraction     A subtraction     A construct     A construct     A construct     A construct     A construct     A construct     C	F. Device SNMP Read Settings SN Name: IP or Subnet Address: Description:	MP Write Settings         CLI Settings           SW04	OnConnect Enfo	a0b:12f0::1 or 2001:db8:a0	0b:12f0::1/64)	Show 20 v records Description Copy Export Delete
	RADIUS Shared Secret: TACAC5+ Shared Secret: Vendor Name: Enable RADIUS Dynamic Authorization: Enable RADES C:	Aruba 💌	Verify: Verify;		Add Cancel	
Administration	o velopment LP D	ec 28, 2022 09:02:18 CET			ClearPass Policy Manager	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

Cachese being Manager-Ance: x	P		
C → C ▲ Inte saker   Maper/17225201120/htps://pac.ontent.action#     ClearPass Policy Manager     Configuration = Network + Devices     Contains > Device SW0 addet     A Network Access Device (NAD) must belong to the global list of devices in the ClearPass.     Filter: Name → UP or Submet Address     Device Groups     Configuration     Contains > Device Groups     Device Groups     Device Groups     Contains > Device Groups     Device Groups     Device Groups     Contains > Device Groups     Devic	Q ClearPass Policy Manager - Arub × +		✓ - □ ×
ClearPass Policy Manager     Deskboard   Configuration > Network > Devices     Configuration > Network > Devices   Configuration > Network > Devices   Configuration > Network > Devices SW04 added  A Network Access Device (NAD) must belong to the global list of devices in the ClearPass database in order to clearPass.   Configuration   Policy Simulation   Policy Simulation   Configuration > Network > Device SW04 added   A Network Access Device (NAD) must belong to the global list of devices in the ClearPass database in order to clearPass.   Policy Simulation   Policy Simulation   Policy Simulation   O Name +   Policy Simulation   Policy Policy Policy Policy P	← → C ▲ Inte säker   https://172.25.201.12	0/tips/tipsContent.action#	🖻 🖈 🔲 😩 :
□ Dashboard       ○         □ Dashboard       ○         □ Dashboard       ○         □ Dashboard       ○         □ Service Structes       □         □ Identify       □         □ Identify       □         □ Device Structes       □         □ Identify       □         □ Identify       □         □ Device Structes       □         □ Postree       □         □ Efforcement       □         □ Device Groups       □         □ Power Torsts       □	aruba	ClearPass Policy Manager	Menu 🗮
Wonktoring       ● Add         Configuration       ● Lise of the remplates & Wizards       ● Export All         ● Service Templates & Wizards       ● Discovered Devices         ● Authentication       ● Lise of the remplates & Wizards       ● Discovered Devices         ● Lise for coment       ● Overice Groups       ● Overice Groups       ● Discovered Device (NAD) must belong to the global list of devices in the ClearPass database in order to connect to ClearPass.         ● Network       Name •       IP or Subnet Address       Device Groups         ● Discovered       ● Discovered       ● Discovered         ● Discovered       Image: Discovered       ● Discovered         ● Discovered       ● Discovered       ● Discovered       ● Discovered         ● Discovered       ● Discovered       ● Discovered       ● Discovered         ● Discovered       ● Discovered       ● Discovered       ● Discovered         ● Discovered       ● Discovered       ● Discovered       ● Discovered         ● Discovered       ● Discovered       ● Discovered       ● Discovered         ● Discovered	Dashboard	Configuration » Network » Devices	
Configuration     Config	Monitoring O	Network Devices	🚽 Add
© Service Templates & Wizards © Service Templates & Wizards © Authentications © Authentications © Tenstruct © Prover Forumes © Device Groups © Device Groups © Device Groups © Device Groups © Prover Scan © Policy Simulation © Policy Simulation © Device Service Scan © Device Scan © Device Scan © Policy Simulation © Device Scan © Device Scan © Device Scan © Device Scan © Policy Simulation © Device Scan © Device Scan © Device Scan © Device Scan © Policy Simulation © Device Scan © D	Configuration O		Export All
Authentication     Authenti	- Ör Service Templates & Wizards		<ul> <li>Discovered Devices</li> </ul>
A Network Access Device (NAD) must belong to the global list of devices in the ClearPass database in order to connect to ClearPass.  Retwork  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 Concerning Concernin	- 🛱 Services	Device SW04 added	
Image: Contains	Authentication	A Network Access Device (NAD) must belong to the global list of devices in the ClearPass database in order to connect to ClearPass.	
Image: Stand Stan	Questine		
Image: Network     Image: Name Network </td <td></td> <td>Filter: Name  Contains  Go Clear Filter</td> <td>Show 20 v records</td>		Filter: Name  Contains  Go Clear Filter	Show 20 v records
Image: Control of Devices       1.       Sw04       172.25.200.13       -         Image: Control of Devices       Image: Control of Devices       Image: Control of Devices       Image: Control of Devices         Image: Control of Devices       Image: Control of Devices       Image: Control of Devices       Image: Control of Devices         Image: Control of Devices       Image: Control of Devices       Image: Control of Devices       Image: Control of Devices         Image: Control of Devices       Image: Control of Devices       Image: Control of Devices       Image: Control of Devices         Image: Control of Devices       Image: Control of Devices       Image: Control of Devices       Image: Control of Devices         Image: Control of Devices       Image: Control of Devices       Image: Control of Devices       Image: Control of Devices         Image: Control of Devices       Image: Control of Devices       Image: Control of Devices       Image: Control of Devices         Image: Control of Devices       Image: Control of Devices       Image: Control of Devices       Image: Control of Devices         Image: Control of Devices       Image: Control of Devices       Image: Control of Devices       Image: Control of Devices         Image: Control of Devices       Image: Control of Devices       Image: Control of Devices       Image: Control of Devices         Image: Control of Devices		# Name A IP or Subnet Address Device Groups	Description
A Device Groups → Q Proving Stands → Q Proving Stands → Q Policy Simulation → Policy Simulation → Q Policy Simulation → Q Policy Simulation	Devices	1. SW04 172.25.200.13 -	
- ♀ Event Sources - ♥ Network Scan - ♥ Policy Simulation	- In Proxy Targets	Showing 1-1 of 1	Copy Export Delete
- Q Netvork Scan	- Die Event Sources		
- Q Policy Simulation	- 🛱 Network Scan		
	- 🛱 Policy Simulation		
💏 Administration 0	🛃 Administration 🛛 🔍 O		
© 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	© Copyright 2022 Hewlett Packard Enterprise Deve	lopment LP Dec 28, 2022 09:02:33 CET ClearPass Policy	Manager 6.9.12.136929 on CLABV (Trial 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/UpsContent.action#tipsNADGroups.action	@ 🖈 🛛 😩 :
aruba	ClearPass Policy Manager	Menu 🗮
Dashboard	Configuration » Network » Device Groups	
Monitoring O	Network Device Groups	Add
- 🗘 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
Authentication	Filter: Name v contains v Go Clear Filter	Show 20 🗸 records
Dentity     Posture	# Name 🖌 Format Description	
🗉 🔹 Enforcement		Export Delete
Autobiol coston		
C Copyright 2022 Hewlett Packard Enterprise Deve	elopment LP Dec 28, 2022 08:57:07 CET ClearPace Policy Manager 6, 9, 12, 136929	on CLABV (Trial Version) platform
to copyright zozz nemett Packald Enterprise Deve	appricit a book of clear assisting realized book of the clear assisting realized book	on cener (mar version) placionni

The trusted network device groups interface in ClearPass Policy Manager.

# Secure onboarding - IEEE 802.1AR/802.1X

ClearPass Policy Manager - Arub 🗙 🕂						~ – 🗆 X
← → C ▲ Inte säker   https://172.25.201.1	20/tips/tipsContent.action#					🖻 🖈 🔲 😩 :
aruba			ClearPass Policy M	anager		Menu 🗮
Dashboard O	Configuration » Networ	k » Device Groups				
Monitoring O	Network Device	Add New Device Group			2	Add
Configuration		Name:	Switches			Export All
— 🛱 Service Templates & Wizards	Device Groups function	Description:	Access Switches		nent profiles.	
- Services						
S → Automitication S → Automitication S → Automitication S → Automitication	Filter: Name	Format:	O Subnet			Show 20 v records
🗊 📅 Posture	# Name		Regular Expression			
SEnforcement		Available Devices (0)	Cist Cist	Selected Devices (1)		Export Delete
- Devices			Filter	Filter		
- Device Groups				SW04 [172.25.200.13]		
- Droxy Targets						
- Li Event Sources						
Policy Simulation						
				Save		
Administration O						
© Copyright 2022 Hewlett Packard Enterprise Dev	elopment LP	Dec 28	, 2022 09:05:28 CET		ClearPass Policy Manager 6.9.12.136929 on CL	ABV (Trial Version) platform

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

O ClearPass Policy Manager - Arub × +		~ - 🗆 X
← → C ▲ Inte säker   https://172.25.201.1	20/tips/tipsContent.action#	ê ☆ ∎ ≗ :
aruba	ClearPass Policy Manager	Menu 📕
Dashboard	Configuration » Network » Device Groups	
Monitoring 0	Network Device Groups	🐥 Add
🔏 Configuration 📀		Export All
—☆ Service Templates & Wizards	Device Group "Switches" added successfully	
- Services	Device Groups function as a component in service and role mapping rules. Device groups can also be associated with enforcement profiles.	
Authentication		
B Posture	Filter: Name Contains Contains Go Clear Filter	Show 20 👻 records
🗉 🔹 Enforcement	# Name • Format Description	
	1.         Switches         List         Access Switches	
- C Devices	Showing 1-1 of 1	Export Delete
- 🛱 Proxy Targets		
- C Event Sources		
- Q Network Scan		
- Q Policy Simulation		
🛃 Administration 🛛 🛛 🛛		
© 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 (Trial 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/tips	Content.action#tip	osFingerprintDictionary.action					🖻 🏠 🖬 😩 🗄		
aruba	ClearPass Policy Manager									
	Administ Devic This pag	tration » Dictiona e Fingerpri e lists all the de amily	ries » Device Fingerprints nts vice fingerprints recognized by Update Device Fingerprints Category:	r the Profiler module.	These fingerprints are upo	lated from the Software (	Updates page.	Add Import Custom Fingerprints Export Custom Fingerprints Show 20 v records		
Berver Manager     Context Servers     Preserver Manager     Preserver Manager     Preserves     Provide Engeneration     Provide Engenet	# 1. 2. 3. 4. Showing	Category Network Can Network Can Network Can Server 1:4 of 4	Category: Family: Name: Custom Rules- 1 Name 1. Host MAC Vendor 2. LLDP System Descrip 3. SNMP System Descrip *Note: 0 Rule(s) will be delet	Netrork Camera Axis Axis 05 version uns Matche Operator contains_all tion not_contains tion not_contains	s (ALL ) Value Axis Communications 10.12 10.12 Update Delete Fing	Delete Rule AB etprint Cose	Name AXIS OS version unsupported AXIS OS version supported Axis Network Camera 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://172.25.201.13	20/tips/tips	sContent.action#tip	osFingerprintDictionary.action					iê \$		<b>a</b> :
aruba			C	ClearPass Poli	cy Manager				Menu	
Dashboard     Dashboard	Adminis Devic This page Filter: [F 1, 2, 3, 4, 4, Showing	tration * Diction: te Fingerpri anily Category Network Can Network Can Server 1 -4 of 4	Curries > Device Fingerprints Ints Update Device Fingerprint Category: Family: Name: Custom Rules 1  Tuber Source Vendor C. LDP System Descri S. SNMP System Descri "Note: O Rule(s) will be de	ClearPass Poli by the Profiler module. s Network Camera Axis Axis OS version sup Hatche Operator contains_all ption contains iption contains	Cy Manager These fingerprints are upda (AL) Value Axis Communications # 10.12 10.12 10.12	eted from the Software U Delete Rule Delete Rule	Ipdates page. Nome AXIS OS version unsupported AXIS OS version supported AXIS Network Camera AXIS Print Server	Add Import Custon Export Custon	Menu Finge Finge	a erprints rprints records
© Copyright 2022 Hewlett Packard Enterprise Deve	elopment I	LP	Dec 05, 2	022 09:05:39 CET		c	ClearPass Policy Manager 6.9.12.1369	29 on CLABV (Trial V	ersion)	platform

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.

Q ClearPass Policy Manager - Arub × +								~ ·	- 0 ×
← → C ▲ Inte säker   https://172.25.201.12	20/tips,	/tipsContent.action#tip	sEditEnforcementProfile.action%3	FcontextData%3D3004				@ ☆	
aruba			Cle	arPass Policy Manag	jer				Menu 🔳
Dashboard	Conf	figuration » Enforcem	ent » Profiles » Edit Enforceme	nt Profile - Allow_VLAN_201					
Monitoring 0	Enf	forcement Pro	files - Allow VLAN 20	01					
Configuration O	Su	mmary Profile	Attributes						
- 🛱 Service Templates & Wizards	Duct	llou	ritinoites			_			
- C Services	PIO	ne.							
Authentication	Nam	ie:	Allow_VLAN_201						
Posture	Tupo	cription.	PADIUS						
🖃 🔹 Enforcement	Actio		Accent						
- Delicies	Devi	ce Group List:	1. Switches						
Profiles	Attri	ibutes:							
- 🛱 Network Scan	Autoutes								
- 🛱 Policy Simulation	1	Radius: IETE		Session-Timeout		-	10800		
	2	Radius: IETE		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		
		Trok to Enfancement	nt Restler					Const Course	
🚑 Administration 🛛 🔍 🛛	< 1	Back to Enforcement	it Profiles				<u>c</u>	.opy Sav	Cancel
© Copyright 2022 Hewlett Packard Enterprise Deve	elopme	ent LP	Dec 28, 2022	09:08:57 CET			ClearPass Policy Manager 6.9.12.136929 on	CLABV (Trial	version) platform

An example enforcement profile to allow access to VLAN 201.

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

ClearPass Policy Manager - Arub: × +				~ - 🗆 X						
← → C ▲ Inte säker   https://172.	25.201.120/tips/tipsContent.action#	tipsEditEnforcementPolicy.action%3FcontextData%3D3007		e 🖈 🛛 😩 :						
aruba		ClearPass Policy Manager								
Dashboard	O Configuration » Enforce	ement » Policies » Edit - Axis Radius policy								
Monitoring	<ul> <li>Enforcement Po</li> </ul>	olicies - Axis Radius policy								
Configuration	Summary Enforce	ment Rules								
- 🛱 Service Templates & Wizards	Enforcement:									
Authentication	Name:	Axis Radius policy								
🗉 🧕 Identity	Description:									
Posture	Enforcement Type:	RADIUS								
Enforcement	Default Profile:	Allow_VLAN_203								
- Ö Profiles	Rules:									
🖅 📫 Network	Rules Evaluation Algori	Rules Evaluation Algorithm: First applicable								
- 🛱 Network Scan	Conditions		Actions							
🎝 Policy Simulation	1. (Certificate:Issuer AND (Certificate AND (Certificate AND (Certificate AND (Certificate AND (Connection)	-CN CONTAINS Axis device ID Intermediate CA) :Issuer O EQUALS Axis Communications AB) :Subject-E LeQUALS Axis Communications AB) :Subject-L EQUALS Lund) :Subject-C EQUALS Sund) :Subject-C EQUALS Sund)	Allow_VLAN_201							
	2. (Certificate:Issuer AND (Certificate AND (Authorizat	-CN CONTAINS Production CA Certificate) ::Subject-CN CONTAINS %{Connection:Client-Mac-Address-NoDelim})) tion:[Endpoints Repository]:Device Name EQUALS AXIS OS version unsupported)	Allow_VLAN_201							
	3. AND (Certificate:Issuer AND (Certificate AND (Authorizat	-CN CONTAINS Production CA certificate) ::Subject-CN CONTAINS %{Connection:Client-Mac-Address-NoDelim})) tion:[Endpoints Repository]:Device Name EQUALS AXIS OS version supported)	Allow_VLAN_202							
🏂 Administration	Back to Enforcem	ent Policies	Co	py 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 Cl	ABV (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

ClearPass Policy Manager - Arub X +	2004 400 PC							
← → G ▲ Inte saker   nttps://1/2.	25.201.120/tips/tipsContent.actic	nmtipsEditService.action%3FcontextData%3D3001		는 보 <b>□</b>				
aruba		ClearPass Policy Ma	anager	Men	.u 📃			
Dashboard	• Configuration » Serv	vices » Edit - Axis 802.1X Wired						
Monitoring	Services - Ax	is 802.1X Wired						
Configuration	Summary Servi	ice Authentication Roles Enforcement						
🗘 Service Templates & Wizards	Name:	Axis 802.1X Wired						
C Services A Authentication C Identity	Description:	To authenticate users to any wired network via 802.1X.						
- TP Posture	Type:	802.1X Wired						
- Senorcement	Status:	Enabled						
🛱 Network Scan	Monitor Mode:	Enable to monitor network access without enforcement	E)					
🛱 Policy Simulation	More Options:	Authorization Posture Compliance Audit End-h	osts 🛛 Profile Endpoints 🗆 Accounting Proxy					
		Service Rule						
	Matches O ANY or	ALL of the following conditions:		- 10 A + 19 -				
	Туре	Name	Operator	Value				
	1. Radius:IETF	NAS-Port-Type	EQUALS	Ethernet (15)	<u>е</u> п			
	2. Radius:IETF	Service-Type	BELONGS_TO	Authenticate-Only (8)	<b>治</b> 官			
	3. Click to add							
	S Back to Service	85		Disable Copy Save	cancel			
Administration	0							

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

Q ClearPass Policy Manager - Arub × +					~ - 🗆 X
← → C ▲ Inte säker   https://172.25.201.12	0/tips/tipsContent.action#tips	EditService.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 📀	Summary Service	Authentication Roles Enforcement			
C Service Templates & Wizards     C Services     Authentication     C dentity     Posture     Frosture     Fersonue     Fersonue     Vetwork     C Network	Authentication Methods:	Axis EAP TLS	Move Up : Move Down ; Remove View Details Modify		Add New Authentication Method
- Q Policy Simulation	Authentication Sources:	[Endpoints Papasiton/] [Local SOL DB]			Add New Authentication Course
		[Endonina repositor] [Eocal oue bo]	Move Up 1 Move Down j Remove View Details Modify		Add New Addrenocation Source
		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 🛛 🛛 Ø	Back to Services			Disable	Copy Save Cancel
© Copyright 2022 Hewlett Packard Enterprise Deve	lopment 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	
Authentication	Enforcement Policy:	Axis Radius policy V Modify	Add New Enforcement Policy
🗉 🧕 Identity		Enforcement Policy Det	ils
Posture     Sefercement	Description:		
Behorcement     Friedmann	Default Profile:	Allow_VLAN_203	
- 🛱 Network Scan	Rules Evaluation Algorithm	: first-applicable	
- 🛱 Policy Simulation	Conditions		Enforcement Profiles
	(Certificate:Issuer- AND (Certificate AND (Certificate AND (Certificate AND (Certificate AND (Certificate AND (Certificate	CN CONTAINS Axis device ID Intermediate CA) Issuero EQUALS Axis Communications AB) Subject- OCUALS Axis Communications AB) Subject- EQUALS Exist Subject- EQUALS Exist (Cleart Mar-cademas-Subplem, EQUALS %-(Certificate-Subject-serialNumber))	Allow_VLAN_201
	(Certificate:Issuer- 2. AND (Certificate AND (Authorizat	(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
	(Certificate:Issuer- 3. AND (Certificate AND (Authorizat	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
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	(x
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				ClearPas	s Policy Manager		Menu
Dashboard	O Config	uration	a » Identity » Roles				
Monitoring	Role	s					Add A
Configuration							Export A
<ul> <li>         — Service Templates &amp; Wizards         <ul> <li></li></ul></li></ul>	Roles e	exist in	dependently of an indivi	idual service and can be	accessed globally through the role	e-mapping policy of any service.	
- 🔒 Authentication	Filter:	Name	<b>~</b>	contains 🗸	∓ Go Clear Filt	er	Show 20 v record
Methods	#		Name 🛦		Description	_	
- Q Identity	1.		[AirGroup v1]		Role for an AirGroup pro	tocol version 1 request	
Single Sign-On (SSO)	2.		[AirGroup v2]		Role for an AirGroup pro	tocol version 2 request	
- Local Users	3.		[Aruba TACACS+ read	-only Admin]	Default role for read-on	v access to Aruba device	
- 🛱 Endpoints	4.		[Aruba TACACS+ root	Admin1	Default role for root acc	ess to Aruba device	
- 🎝 Static Host Lists	5.		AxisDevi Edit Role			•	
Roles	6		[BYOD O			ane their own provision	ed devices
Role Mappings	7		[Contrac	3001			
T Posture			[Dovice	AxisDev	ice	their devices for use w	ith MAC authentication and AirCroup charing
- Audit Servers	0.		Description			then devices, for use w	in the automotion and Androup sharing.
Agentless OnGuard	9.		[Employ				
B Enforcement	10.		[Guest]				
- 🛱 Policies	11.		[MAC Ca				
- C Profiles	12.		[Unboard		2	Save Cancel	
- •••• Network	13.		Unboard			id	
- Oevices	14.		[Onboard IOS]		Role for an IOS device b	eing provisioned	
Provy Targets	15.		[Onboard iPadOS]		Role for an iPadOS devic	e being provisioned	
- Li Event Sources	16.		[Onboard Linux]		Role for Linux device be	ing provisioned	
	17.		[Onboard macOS]		Role for a macOS device	e being provisioned	
- Delicy Simulation	18.		[Onboard Windows]		Role for a Windows devi	ce being provisioned	
	19.		[Other]		Default role for another	user or device	
	20.		[TACACS+ API Admin]		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 × +				∨ – □ ×
← → C ▲ Inte säker   https://172.25.20	01.120/tips/tipsContent.actio	n#tipsEditRoleMappingPolicy.action%3FcontextData%3D3001		@☆□:
aruba		ClearPass Policy Mana	ager	Menu 📕
Dashboard	Configuration » Identity	» Role Mappings » Edit - Axis Role Mapping		
Monitoring 0	Role Mappings -	Axis Role Mapping		
& Configuration 💿	Cummony Deligy	Manning Buller		
- 🛱 Service Templates & Wizards - 🛱 Services	Policy:	Hupping Kines		
🖃 🚘 Authentication	Policy Name:	Axis Role Mapping		
- 🛱 Methods	Description:			
- Q Sources	Default Role:	[Guest]		
Single Sign-On (SSO)	Mapping Rules:			
- C Local Users	Rules Evaluation Algorit	hm: Evaluate all		
- C Endpoints	Conditions	Tear-of Charles Million Contraction	Role Name	
- 🛱 Static Host Lists	1. (Authentication:Ful	I-Username BEGINS WITH axis-00408c)	AxisDevice	
- 🛱 Roles	2. (Authentication:Ful	-Username BEGINS WITH axis-accc8e)	AxisDevice	
- Role Mappings	3. (Authentication:Ful	I-Username BEGINS WITH axis-b8a44f)	AxisDevice	
Agenties OnGuard     Agentiess OnGuard     Agentiess OnGuard     Agentiess OnGuard     Agentiess OnGuard     Agentiess     Agentiess				
Administration 0	K Back to Role Mapp	ings	C	opy Save Cancel
© Copyright 2023 Hewlett Packard Enterprise D	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	e 🖈 🛛 😩 :
aruba		ClearPass Policy Manager	Menu 🗮
Dashboard	• Configuration » Services	» Edit - Axis 802.1X Wired	
Monitoring	<ul> <li>Services - Axis 8</li> </ul>	02.1X Wired	
Configuration	Summary Service	Authentication Roles Enforcement	
- 🌣 Service Templates & Wizards - 🏟 Services	Use Cached Results:	Use cached Roles and Posture attributes from previous sessions	
🖃 🗣 Authentication	Enforcement Policy:	Axis Radius policy V Modify	Add New Enforcement Policy
- Q Methods		Enforcement Poli	cy Details
Identity	Description:		
- 🛱 Single Sign-On (SSO)	Default Profile:	Allow_VLAN_203	
- 🗘 Local Users	Rules Evaluation Algorith	nm: evaluate-all	
- 🛱 Endpoints	Conditions		Enforcement Profiles
Color Happings     Color Ha	AND (Cennect serialNumber})     AND (Tips:Rol (Certificate:Issue AND (Authoriz 2. unsupported)	es JOBJECTO EQUATORS COMMUNICATION ADJ on:Client-MacAddress-NoDelim EQUALS % (Certificate:Subject- e EQUALS AxisDevice) er-CN <u>CONTAINS</u> Production CA) ation:[Endpoints Repository]:Device Name <u>EQUALS</u> AXIS OS version	Allow_VLAN_201
	AND (Certifica AND (Tips:Rol (Certificate:Issue AND (Authoriz 3. supported) AND (Certificate:Issue AND (Certificate)	tes:Subject-CN CONTAINS Production XYZ) a EQUALS AxisDevice) 	Allow_VLAN_202
- 🖧 Event Sources - 🌣 Network Scan - 🌣 Policy Simulation	Back to Services		Disable Copy Save Cancel
🚰 Administration	0		
© Copyright 2023 Hewlett Packard Enterpris	e Development LP	Oct 26, 2023 05:11:50 UTC	ClearPass Policy Manager 6.11.2.252294 on CLABV (Trial Version) platform

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

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

#### **Enforcement profile**

Q app20 × +				✓ - □ ×					
← → C ▲ Inte säker   https://172.25.20	1.120/tips/tipsContent.action	#tipsEditEnforcementProfile.action%3FcontextData%3D3004		id ☆ 🛛 🏝 :					
aruba		ClearPass Policy Manag	er	Menu 🗮					
Dashboard 0	Configuration » Enforcen	Configuration » Enforcement » Profiles » Edit Enforcement Profile - Allow_VLAN_201							
Monitoring 0	Enforcement Pro	files - Allow VLAN 201							
Configuration 💿	Summany Profile	Attributos							
- 🛱 Service Templates & Wizards - 🛱 Services	Profile:	HIGH DICES							
	Name:	Allow_VLAN_201							
- 🛱 Methods	Description:								
- C Sources	Type:	RADIUS							
- V Identity	Action:	Accept							
- C Local Users	Device Group List:	1. Switches							
- C Endpoints	Attributes:								
- 🛱 Static Host Lists	Туре	Name	Value						
- 🛱 Roles	1. Radius:IETF	Session-Timeout	= 10800						
- Q Role Mappings	2. Radius:IETF	Termination-Action	= RADIUS-Request (1)						
- D 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						
- C Policies									
- profiles									
- T Devices									
Device Groups									
- 🛱 Proxy Targets									
- 🛱 Event Sources									
- C Network Scan									
	A Rack to Enforceme	at Brofiles		Copy Saya Carrol					
Administration 0	Back to Enforceme	it promes		copy save cancer					
© Copyright 2023 Hewlett Packard Enterprise D	evelopment LP	Oct 26, 2023 05:13:21 UTC	ClearPass Policy Manager	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.

Q app20 × +			v =	
← → C ▲ Inte säker   https://172.25.20	1.120/tips/tipsContent.action	#tipsEditService.action%3FcontextData%3D3006	ie ★ E	I 🗷 E
aruba		ClearPass Policy Manager	м	enu <b>=</b>
Dashboard	Configuration » Services	» Edit - Axis 802.1X Wired - Mac Authentication		
Monitoring 0	Services - Axis 8	02.1X Wired - Mac Authentication		
Configuration O	Summary Service	Authentication Roles Enforcement		
Construction     Construction	Use Cached Results: Enforcement Policy: Description: Default Profile: Rules Evaluation Algorith Conditions (Date:Day-of-We 1. AND (Date:Tim AND (Connection)	Use cached Roles and Posture attributes from previous sessions          Axis MAC Authentication Policy       Modify         Enforcement Policy       Modify         [Deny Access Profile]       Image: Comparison of the second	Add New Enforce icy Details Enforcement Profiles Allow_VLAN_203	ment Policy
Administration     O     Convribt 2023 Hewlett Packard Entermise D	Back to Services  evelopment LP	Oct 26, 2023 05:15:57 UTC	Enable Copy Save	Cancel

#### 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.

0 mm20						∨ – □ X			
← → C ▲ Inte säker   https://172.25.20	ker   https://172.25.201.120/tips/LipsContent.action#LipsAuthSources.action								
aruba			Clear		Menu 🗮				
Dashboard	Configu	ration	Authentication » Sources						
Monitoring 0	Authe	entic	ation Sources			🚽 Add 🐣 Import			
- 🖞 Service Templates & Wizards	An auth	entical	ion source is the identity store (Active Di	rectory, LDAP directory, etc.) against	which users and devices are authenticated.				
- 🛱 Services			, ,						
	Filter: N	amo	× contains ×	Go Clear F	ilter	Show 20 V records			
- 🛱 Methods	#		Name .	Type	Description				
- Q Sources	1		[Admin Licer Repositon/]	Local SQL DR	Authenticate users against Bolicy Manager adm	in upor database			
□ Q Identity - ☆ Single Sign-On (SSO)	2.	0	[Denylist User Repository]	Local SQL DB	Denylist database with users who have exceede related limits	ed bandwidth or session			
- CLocal Users	3.		[Endpoints Repository]	Local SQL DB	Authenticate endpoints against Policy Manager	local database			
- C Static Host Lists	4.		[Guest Device Repository]	Local SOL DB	Authenticate quest devices against Policy Mana	ger local database			
- C Roles	5.		[Guest User Repository]	Local SOL DB	Authenticate quest users against Policy Manage	er local database			
- 🛱 Role Mappings	6		[Insight Repository]	Local SQL DB	Insight database with session information for u	sers and devices			
🖃 🖶 Posture	7		[Local Liser Renository]	Local SQL DB	Authenticate users against Policy Manager local	user database			
- 🗘 Posture Policies	8	-	[Onboard Devices Repository]	Local SQL DB	Authenticate Ophoard devices against Policy Ma	anager local database			
- 🗘 Audit Servers	0	0	[Social Login Repository]	Local SQL DB	Authenticate users against Policy Manager socia	al login database			
Agentless OnGuard	3.	0	[Social Login Repository]	Level SQL DB	Authenization source for implementing uprious t	ime functions			
- B Enforcement	10.	0	[Time Source]	LOCAL SQL DB	Authorization source for implementing various t				
- Profiles	11.	0	[20ile Cacile Repository]	HIIP	Access attributes cached by Context Server Act	ions in previous sessions			
Network	Showing	1-11	of 11			Copy Export Delete			
_ Devices									
- Device Groups									
- 🗘 Proxy Targets									
- 🛱 Event Sources									
- 🛱 Network Scan									
- Or Policy Simulation									
🚰 Administration 🛛 🛛 🧿									
© Copyright 2023 Hewlett Packard Enterprise D	evelopme	nt LP	Oct 31, 2023 (	9:13:53 UTC	ClearPass Policy Manager 6.11.2.252294	on CLABV (Trial Version) platform			

# Legacy onboarding - MAC authentication

Q app20 × +			✓ - □ X
← → C ▲ Inte säker   https://172.25.201.120	0/tips/tipsContent.action#t	ipsAddAuthSource.action	년 ☆ 🛛 😩 :
aruba		ClearPass Policy Manager	Menu 🗮
Dashboard O Co	onfiguration » Authentica	tion » Sources » Add	
Monitoring O A	uthentication So	urces	
& Configuration	Conorol Static Host I		
- 🗘 Service Templates & Wizards	General Static Host L	sts summary	
- O Services Na	ame:	Axis Devices	
E-Authentication De	escription:	MAC addresses of Axis devices in use.	
- 🗘 Methods			
- Cources	/pe:	Static Host List	
E Z Identity	en fos Authorizations	Canble to use this Authentication Course to also fatch cale manning attailutes	
- TL ocal Lisers	se for Authorization:	Enable to use this Authentication Source to also retch role mapping attributes	
- C Endpoints	uthorization Sources:	Remove	
- 🗘 Static Host Lists		View Details	
- 🗘 Roles			
- 🛱 Role Mappings			
E- T Posture			
- O Posture Policies			
Adentiess OnGuard			
- O Policies			
- 🛱 Profiles			
Network			
- 🛱 Devices			
- O Device Groups			
- IC Proxy Targets			
- The Network Scan			
- C Policy Simulation			
220 H			
<	Back to Authenticati	on Sources	Next → Save Cancel
Copyright 2023 Hewlett Packard Enterprise Devel	lopment 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#				🖻 🛧 🔲 😩 :
aruba		Clearl	Pass Policy Manage	er	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 Statis Heat List
- Services	The Address host clots.	Add Static Host List		0	Add New Static Host List
Authentication		Name:	Axie devices		
Sources		Description:			
🖃 🧕 Identity		beschption.			
- 🎝 Single Sign-On (SSO)			ļ		
- CLocal Users		Host Format:	O Subnet		
- The Static Host Lists			List		
- 🛱 Roles		Host Type:	O IP Address		
- 🛱 Role Mappings		1999	MAC Address		
E- H Posture		Host Entries			
Audit Servers		# Address	Description		
- Agentless OnGuard		1. O B8-A4-4F-45-B4-E	6 Axis Device 1	8	
🖃 💈 Enforcement		2. 0 B8-A4-4F-45-B4-E	7 Axis Device 2	<b>U</b>	
- 🛱 Policies		3. O B8-A4-4F-45-B4-E	8 Axis Device 3		
Profiles		Address:			
- The Network		Description:			
- Device Groups					
- 🗘 Proxy Targets				Save Host	
- C Event Sources					
- Chevron Scan					
- A Policy Simulation				Save	
				Current	
	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 × +			✓ - □ X
← → C ▲ Inte säker   https://172.	25.201.120/tips/tipsContent.action#		ie 🖈 🖬 😩 🗄
aruba		ClearPass Policy Manager	Menu 🗮
Dashboard	• Configuration » Authentica	tion » Sources » Add	
Monitoring	<ul> <li>Authentication So</li> </ul>	urces	
& Configuration	<u>○</u>	List "Avis devices"	added successfully
- C Service Templates & Wizards	General Static Host L	sts Summary	accession y
<ul> <li>Authentication         <ul> <li>Authentication</li> <li>Authentication</li> <li>Authentication</li> <li>Authentication</li> <li>Courses</li> <li>Identity</li> <li>Courses</li> <li>Courses</li></ul></li></ul>	MAC Address Host Lists:	Axis devices	Add New Static Host List
	Back to Authenticati	on Sources	Next → Save Cancel
Administration	0		
Copyright 2023 Hewlett Packard Enterpr	ise Development LP	Oct 31, 2023 09:20:34 UTC	ClearPass Policy Manager 6.11.2.252294 on CLABV (Trial Version) platform

### 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

Dashboard     Monitoring     Monitoring     Monitoring     Service Templates & Wizards     Service & Wizar	Configues Config	uration ices age sho Name	» Services	ClearPass Pol	icy Manager	f authorization.		Menu Add Menu Add Menu Menu Menu
Dashboard O Monitoring O Configuration O Service Templates & Wizards Services Authentication C Methods Survices C Identity C Single Sign-On (SSO) C Local Users C Local Users C Static Host Lists C Roles C Roles C Role Mappings	Config Serv This pa Filter: [ # 1. 2. 3.	uration ices age sho Name	» Services	rent list and order of services that ClearPass fo	llows during authentication and	f authorization.		Add 😤 Import 🙎 Export
Monitoring     O	Serv This pa Filter: 1. 2. 3.	ices age sho Name	ws the cur	rent list and order of services that ClearPass fo	lows during authentication and	l authorization.		Add 🐣 Import 🚖 Export
Configuration Service Templates & Wizards Services Authentication → Methods → Sources Identity ↓ Cocal Users → Local Users → Endpoints → Static Host Lists → Roles → Role Mappings ↓ Posture	Filter:	Name	ws the cur	rent list and order of services that ClearPass fo	llows during authentication and	l authorization.		A Import
Service Templates & Wizards     Services     Services     Authentication     Sources     Sources     Sources     Gidentity     Call Users     Call Use	This pa Filter: [ # 1. 2. 3.	Name	ws the cur	rent list and order of services that ClearPass fo	llows during authentication and	authorization.		Export
Authentication     Authentication     Q Sources     Gources     Gources     Gources     Could Users     Q Endonits     Q Static Host Lists     Q Roles     Q Role     Q RoleMappings     Posture	Filter: [ # 1. 2. 3.	Name						
- ☆ Methods     - ☆ Sources     Surces     Identity     - ☆ Single Sign-On (SSO)     - ☆ Local Users     - ☆ Local Users     - ☆ Endpoints     - ☆ Role S     - ☆ Role Mappings     Posture	Filter:	Name						(TTT)
- ☆ Sources Sources - ☆ Single Sign-On (S50) - ☆ Local Users - ☆ Endpoints - ☆ Roles - ☆ Role Mappings - ☆ Posture	# 1. 2. 3.			✓ contains ✓	H Go Clear Filter	Hit Count for Current hour	Sh	Jw 20 ♥ reco
Q Identity       -☆ Single Sign-On (SSO)       -☆ Local Users       -☆ Endpoints       -☆ Static Host Lists       -☆ Roles       ☆ Role       ☆ Role       ☆ Role       ☆ Posture	1. 2. 3.		Order 🔺	Name	Туре	Template	Hit Count	Status
- ☆ Single Sign-On (SSO) - ☆ Local Users - ☆ Endpoints - ☆ Static Host Lists - ☆ Roles - ☆ Role Mappings - ♥ Posture	2. 3.		1	Axis 802.1X Wired	RADIUS	802.1X Wired	0	0
- Q Local Users - Q Endpoints - Q Static Host Lists - Q Roles - Q Role Mappings - Posture	3.		2	Axis 802.1X Wired - Mac Authentication	RADIUS	MAC Authentication	0	0
- 🗘 Endpoints - 🗘 Static Host Lists - 🖓 Roles - 🖓 Role Mappings - 📅 Posture			3	Test_Service	RADIUS	802.1X Wired	0	0
Control Contro	4.		4	[Policy Manager Admin Network Login Service	] TACACS+	TACACS+ Enforcement	0	0
- 🖓 Roles 🎝 Role Mappings 🕆 Posture	5.		5	[AirGroup Authorization Service]	RADIUS	RADIUS Enforcement ( Generic )	0	0
Posture	6.		6	[Aruba Device Access Service]	TACACS+	TACACS+ Enforcement	0	0
- (prostare	7.		7	[Guest Operator Logins]	Application	Aruba Application Authentication	0	0
- Posture Policies	8.		8	[Insight Operator Logins]	Application	Aruba Application Authentication	0	0
- Q Audit Servers	9.		9	[Device Registration Disconnect]	WEBAUTH	Web-based Authentication	0	ŏ
Agentless OnGuard	Charles I.	-						
- S Enforcement	Snowir	ig 1-9 (	01.9			R	corder Copy	Export Dele
- 🛱 Policies								
— 🛱 Profiles								
•••• Network								
- O Devices								
- Q Device Groups								
- C Proxy Targets								
- g Event Sources								
The Network Scan								
- Lt Policy Simulation								
Administration 0								

## Legacy onboarding - MAC authentication



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

# Legacy onboarding - MAC authentication

Q app20 × +				✓ - □ X				
← → C ▲ Inte säker   https://172.2	5.201.120/tips/tipsContent.action#t	ipsEditService.action%3FcontextData%3D300	5	년 🖈 🔲 😩 :				
aruba		ClearPass P	olicy Manager	Menu 🗮				
Dashboard	• Configuration » Services »	Configuration » Services » Edit - Axis 802.1X Wired - Mac Authentication						
Monitoring	Services - Axis 80	Axis 802.1X Wired - Mac Authentication						
🖧 Configuration	Summary Service	Authentication Roles Enforcement						
Gervice Templates & Wizards     Gervices	Authentication Methods:	[Allow All MAC AUTH]	Move Up : Move Down ] Remove View Details Modify	Add New Authentication Method				
- 🛱 Endpoints		Select to Add	•					
	Authentication Sources:	Axis Devices (Static Host List)	Move Up † Move Down ↓ Remove View Details Modify	Add New Authentication Source				
Enforcement		Select to Add	▼					
- C Policies	Strip Username Rules:	$\Box$ Enable to specify a comma-separated	list of rules to strip username prefixes or su	ffixes				
<ul> <li>➡ Network</li> <li>➡ Devices</li> <li>➡ Device Groups</li> <li>➡ Proxy Targets</li> <li>➡ Event Sources</li> <li>➡ Network Scan</li> <li>➡ Policy Simulation</li> </ul>								
Administration	Back to Services			Disable Copy Save Cancel				
© Copyright 2023 Hewlett Packard Enterpris	se Development LP	Oct 31, 2023 09:22:22 UTC		ClearPass Policy Manager 6.11.2.252294 on CLABV (Trial Version) platform				

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