

Benutzerhandbuch

# Inhalt

Einführung	3
Sicheres Onboarding – IEEE 802.1AR/802.1X	4
Erstauthentifizierung	4
Bereitstellung	4
Produktionsnetzwerk	4
Konfiguration von HPE Aruba	5
Konfiguration Axis	17
Sicherer Netzwerkbetrieb – IEEE 802.1AE MACsec	20
Aruba ClearPass Policy Manager	20
Aruba-Zugangsschalter	25
Legacy-Unboarding – MAC-Authentifizierung	26
Aruba ClearPass Policy Manager	26
Aruba-Zugangsschalter	34

### Einführung

### Einführung

Dieser Integrationsleitfaden soll die Best-Practice-Konfiguration für die Einbindung und den Betrieb von Axis Geräten in Aruba-Netzwerken skizzieren. Bewährt haben sich Konfigurationen mit modernen Sicherheitsstandards und Protokollen wie IEEE 802.1X, IEEE 802.1AR, IEEE 802.1AE und HTTPS.

Die Einrichtung einer geeigneten Automatisierung für die Netzwerkintegration kann Zeit und Geld sparen. Es ermöglicht die Beseitigung unnötiger Systemkomplexität bei der Verwendung von Anwendungen zur Verwaltung von Axis Geräten in Kombination mit Aruba-Netzwerkgeräten und -Anwendungen. Im Folgenden sind nur einige Vorteile aufgeführt, die durch die Kombination von Axis Geräten und Software mit einer Aruba-Netzwerkinfrastruktur erzielt werden können:

- Minimieren Sie die Systemkomplexität, indem Sie Netzwerke zur Bereitstellung von Geräten entfernen.
- Sparen Sie Kosten, indem Sie Einbindungsprozesse und Geräteverwaltung automatisieren.
- Profitieren Sie von den Zero-Touch-Netzwerksicherheitskontrollen der Axis Geräte.
- Erhöhen Sie die allgemeine Netzwerk-Sicherheit durch den Einsatz des Fachwissens von Aruba und Axis.

Die Netzwerkinfrastruktur muss darauf vorbereitet sein, die Integrität der Axis Geräte sicher zu überprüfen, bevor mit der Konfiguration begonnen wird. Dies ermöglicht einen reibungslosen softwaredefinierten Übergang zwischen logischen Netzwerken während des gesamten Onboarding-Prozesses. Vor der Konfiguration sind Kenntnisse in den folgenden Bereichen erforderlich:

- Verwaltung der IT-Infrastruktur des Aruba-Unternehmensnetzwerks, einschließlich Aruba Access Switches und Aruba ClearPass Policy Manager.
- Fachkenntnisse in modernen Netzwerkzugriffskontrolltechniken und Netzwerk-Sicherheitsrichtlinien.
- Grundkenntnisse über Axis Produkte sind wünschenswert, werden aber im gesamten Handbuch vermittelt.

### Sicheres Onboarding - IEEE 802.1AR/802.1X

### Sicheres Onboarding - IEEE 802.1AR/802.1X

### Erstauthentifizierung

Schließen Sie das von Axis Edge Vault unterstützte Axis Gerät an, um das Gerät gegenüber dem Aruba-Netzwerk zu authentifizieren. Das Gerät verwendet das Axis Geräte-ID-Zertifikat IEEE 802.1AR über die Netzwerkzugriffskontrolle IEEE 802.1X, um sich zu authentifizieren.

Um Zugriff auf das Netzwerk zu gewähren, überprüft der Aruba ClearPass Policy Manager die Axis Geräte-ID zusammen mit anderen gerätespezifischen Fingerabdrücken. Die Informationen, wie MAC Adresse und laufende Firmware, werden verwendet, um eine richtlinienbasierte Entscheidung zu treffen.

Das Axis Gerät authentifiziert sich beim Aruba-Netzwerk mithilfe des IEEE 802.1AR-kompatiblen Axis Geräte-ID-Zertifikats.

Das Axis Gerät authentifiziert sich beim Aruba-Netzwerk mithilfe des IEEE 802.1AR-kompatiblen Axis Geräte-ID-Zertifikats.

- 1 Axis Geräte-ID
- 2 IEEE 802,1x EAP-TLS-Netzwerkauthentifizierung
- 3 Zugangsschalter (Authentifikator)
- 4 ClearPass Policy Manager

### Bereitstellung

Nach der Authentifizierung verschiebt das Aruba-Netzwerk das Axis Gerät in das Bereitstellungsnetzwerk (VLAN201), in dem Axis Device Manager installiert ist. Über den Axis Device Manager können Gerätekonfiguration, Sicherheitshärtung und Firmware-Updates durchgeführt werden. Um die Gerätebereitstellung abzuschließen, werden neue kundenspezifische Zertifikate in Produktionsqualität für IEEE 802.1X und HTTPS auf das Gerät hochgeladen.

Nach erfolgreicher Authentifizierung wird das Axis Gerät zur Konfiguration in ein Bereitstellungsnetzwerk verschoben.

- 1 Zugangsschalter
- 2 Bereitstellung des Netzwerks
- 3 ClearPass Policy Manager
- 4 Anwendung zur Geräteverwaltung

### Produktionsnetzwerk

Die Bereitstellung des Axis Geräts mit neuen IEEE 802.1X-Zertifikaten löst einen neuen Authentifizierungsversuch aus. Der Aruba ClearPass Policy Manager überprüft die neuen Zertifikate und entscheidet, ob das Axis Gerät in das Produktionsnetzwerk verschoben wird oder nicht.

Nach der Gerätekonfiguration verlässt das Axis Gerät das Bereitstellungsnetzwerk und versucht, sich erneut beim Aruba-Netzwerk zu authentifizieren.

- 1 Axis Geräte-ID
- 2 IEEE 802,1x EAP-TLS-Netzwerkauthentifizierung
- 3 Zugangsschalter (Authentifikator)
- 4 ClearPass Policy Manager

Nach der erneuten Authentifizierung wird das Axis Gerät in das Produktionsnetzwerk (VLAN 202) verschoben. In diesem Netzwerk stellt das Video Management System (VMS) eine Verbindung zum Axis Gerät her und nimmt den Betrieb auf.

### Sicheres Onboarding - IEEE 802.1AR/802.1X

Dem Axis Gerät wird Zugriff auf das Produktionsnetzwerk gewährt.

- 1 Zugangsschalter
- 2 Produktionsnetzwerk
- 3 ClearPass Policy Manager
- 4 Video Management System

### Konfiguration von HPE Aruba

#### Aruba ClearPass Policy Manager

Der ClearPass Policy Manager von Aruba bietet rollen- und gerätebasierte sichere Netzwerkzugriffskontrolle für IoT, BYOD, Unternehmensgeräte, Mitarbeiter, Auftragnehmer und Gäste in der kabelgebundenen, kabellosen und VPN-Infrastruktur mehrerer Anbieter.

#### Konfiguration des vertrauenswürdigen Zertifikatspeichers

- 1. Laden Sie die Axis spezifische IEEE 802.1AR-Zertifikatskette von axis.com herunter.
- 2. Laden Sie die Axis spezifischen IEEE 802.1AR-Root-CA- und Intermediate-CA-Zertifikatketten in den vertrauenswürdigen Zertifikatspeicher hoch.
- 3. Aktivieren Sie den Aruba ClearPass Policy Manager zur Authentifizierung von Axis Geräten über IEEE 802.1X EAP-TLS.
- 4. Wählen Sie im Verwendungsfeld EAP aus. Die Zertifikate werden für die IEEE 802.1X EAP-TLS-Authentifizierung verwendet.

← → C A Inte säker   https://172.25.	201.120/tips/tips	Conter	nt.action#					6 4	Ш 🖀 🗄
aruba					ClearPass Policy Manager				Menu 🗮
Dashboard	o Adminis	tration	» Certifica	ates » Trust List					
Monitoring	Certif	icate	Trust	List					🛶 Add
🔗 Configuration	• This pag	je disp	lays a list	of trusted Certificate Aut	horities (CA). You can add, view, or delete a certificate.				
🔐 Administration	0								
- July ClearPass Portal	Filter: S	Subject		✓ contains ✓	Go Clear Filter			Show 20	✓ records
🗈 🔒 Users and Privileges	#		Subject	•			Usage	Validity	Enabled
Berver Manager     External Servers	1.		OU=Veri	Sign Trust Network,OU=(	c) 1998 VeriSign Inc For authorized use only,OU=Class 3 Public Primary	Ŷ	Others	Valid	Disabled
Æxternal Accounts     Gertificates     Ø Certificate Store     Ø Trust List	2.		OU=Go I	Add Certificate	•		AD/LDAP Servers, Endpoint Context Servers, SAML, SMTP, Others	Valid	Enabled
	3.		OU=Clas	Certificate File:	Valj fil Axis_device_ID_Inte_CA_ECC_1.pem		Others	Valid	Disabled
- PRevocation Lists	4.		emailAdd	Usage:	EAP	cate	EAP, Others	Valid	Enabled
Eu Dictionaries Agents and Software Updates	5.		emailAdo Authorita		Remove	cate	EAP, Others	Valid	Enabled
🗄 🐔 Support	6.		C=US,S1 01			CA	Others	Valid	Disabled
	7.		C=US,S1		Select to Add	A 103	Others	Valid	Disabled
	8.		C=US,S1		Add Certificate Cancel		Aruba Infrastructure	Valid	Disabled
	9.		CN=Wire	d Phones,OU=PKI Autho	rity,O=AlcateI-Lucent,C=FR		Others	Valid	Disabled
	10.		CN=Veris only,OU=	Sign Class 3 Public Prima VeriSign Trust Network,	ry Certification Authority - G5,OU=(c) 2006 VeriSign Inc For authorized D=VeriSign Inc.,C=US	l use	Others	Valid	Disabled
	11.		CN=Veris	Sign Class 3 Public Prima VeriSign Trust Network,0	ry Certification Authority - G3,OU=(c) 1999 VeriSign Inc For authorized D=VeriSign Inc.,C=US	l use	Others	Valid	Disabled
	12.		CN=Veris only,OU=	Sign Class 1 Public Prima VeriSign Trust Network,	ry Certification Authority - G3,OU=(c) 1999 VeriSign Inc For authorized D=VeriSign Inc.,C=US	l use	AD/LDAP Servers, Endpoint Context Servers, SAML, SMTP, Others	Valid	Enabled
	13.		CN=USE	RTrust RSA Certification	Authority,O=The USERTRUST Network,L=Jersey City,ST=New Jersey,C=US		EAP, Others	Valid	Disabled
	14.		CN=thaw Division,	rte Primary Root CA,OU= O=thawte Inc.,C=US	(c) 2006 thawte Inc For authorized use only,OU=Certification Services		Others	Valid	Disabled
	15.		CN=TC T	rustCenter Universal CA	I,OU=TC TrustCenter Universal CA,O=TC TrustCenter GmbH,C=DE		Others	Valid	Disabled

Hochladen der für Axis spezifischen IEEE 802.1AR-Zertifikate in den vertrauenswürdigen Zertifikatspeicher des Aruba ClearPass Policy Managers.

Sicheres Onboarding - IEEE 802.1AR/802.1X

Q ClearPass Policy Manager - Arub 🗙 🕂				~	- 🗆 ×
← → C ▲ Inte säker   https://172.25.201	1.120/tips/tipsContent.action#t	ipsCertTrustList.action		iê \$	- II 😩 E
aruba		ClearPass Policy Manage	er		Menu 📕
Dashboard	o Administration » Certifie	cates » Trust List			
Monitoring	<ul> <li>Certificate Trust</li> </ul>	List			🛶 Add
🐣 Configuration	• This page displays a list	of trusted Certificate Authorities (CA). You can add, view, or delete a c	certificate.		
Station Contraction	•				
- P ClearPass Portal	Filter: Subject	✓ contains      ✓ axis device     ✓ Go Clear File	lter	Show	20 v records
🖅 🚘 Users and Privileges	# 🗖 Subjec	t <del>v</del>	Usage	Validity	Enabled
External Server	1. 🗆 CN=Axi	s device ID Root CA RSA,O=Axis Communications AB	EAP	Valid	Enabled
- P External Accounts	2. CN=Axi	s device ID Root CA ECC,O=Axis Communications AB	EAP	Valid	Enabled
E Certificates	3. CN=Axi	s device ID Intermediate CA RSA 2,0=Axis Communications AB	EAP	Valid	Enabled
- 🖉 Certificate Store	4. CN=Axi	s device ID Intermediate CA RSA 1,0=Axis Communications AB	EAP	Valid	Enabled
— 🥜 Trust List	5. CN=Axi	s device ID Intermediate CA ECC 2,0=Axis Communications AB	EAP	Valid	Enabled
- Prevocation Lists	6. CN=Axi	s device ID Intermediate CA ECC 1,0=Axis Communications AB	EAP	Valid	Enabled
Dictionaries	Showing 1-6 of 6				Delete
· Support					
© Copyright 2022 Hewlett Packard Enterprise De	evelopment LP	Nov 25, 2022 08:48:50 CET	ClearPass Policy Manager 6.9.12.1	36929 on CLABV (Trial	Version) platform

Der vertrauenswürdige Zertifikatsspeicher im Aruba ClearPass Policy Manager mit für Axis spezifischer IEEE 802.1AR-Zertifikatskette.

#### Netzwerkgeräte-/Gruppenkonfiguration

- 1. Fügen Sie dem ClearPass Policy Manager vertrauenswürdige Netzwerkzugriffsgeräte wie Aruba Access Switches hinzu. Der ClearPass Policy Manager muss wissen, welche Aruba Access Switches im Netzwerk für die IEEE 802.1X-Kommunikation verwendet werden.
- 2. Verwenden Sie die Netzwerkgerätegruppenkonfiguration, um mehrere vertrauenswürdige Netzwerkzugriffsgeräte zu gruppieren. Das Gruppieren vertrauenswürdiger Netzwerkzugriffsgeräte ermöglicht eine einfachere Richtlinienkonfiguration.
- 3. Das gemeinsame RADIUS-Geheimnis muss mit der spezifischen IEEE 802.1X-Konfiguration des Switches übereinstimmen.

Sicheres Onboarding - IEEE 802.1AR/802.1X

Q ClearPass Policy Manager - Arub × +					× - 0	×
← → C ▲ Inte säker   https://172.25.20	1.120/tips/tipsContent.action#tipsNetworkDevices.action				ie 🛧 🗖 🖁	<b>1</b>
aruba		ClearPass Policy N	<i>l</i> lanager		Menu	
Dashboard	<ul> <li>Configuration » Network » Devices</li> </ul>					
Monitoring	<ul> <li>Network Devices</li> </ul>				🐥 Add	
Configuration	0				Export All	
🛱 Service Templates & Wizards					Discovered Descovered Descovered Descovered Descovered	Devices
- C Services	A Network Access Device (NAD) must belong to the	e global list of devices in the Clea	arPass database in order to connect to Cl	earPass.		
Authentication     Oldentity						
Besture	Filter: Name  v contains v	± Go	Clear Filter	Sec. (180)	Show 20 V	records
🗉 🔹 Enforcement	# Name 🖌	IP or Subnet Address	Device Groups	Descrip	tion	
					Copy Export E	Delete
- Device Groups						
Proxy Targets						
- C Event Sources						
- O Network Scan						
- gr 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

Die Schnittstelle für vertrauenswürdige Netzwerkgeräte im Aruba ClearPass Policy Manager.

Q ClearPass Policy Manager - Arub 🗙 🕂						✓ - □ X
← → C ▲ Inte säker   https://172.25.201.13	20/tips/tipsContent.action#					🖻 🛧 🗖 😩 :
aruba		ClearPass Policy	/ Manager			Menu 🗮
Dashboard     Deshboard     Monitoring     Configuration     Service Templates & Wizards     Services     Galdentity     Services     Focure     Service     Focure     Service     Provy Template     Service     Provy Targets     Service Scan     Proty Simulation	Configuration > Network > Devices Network Device  A Add Device  P Device SNMP Read Settings SN Name: IP or Subnet Address: Description: RADIUS Shared Secret: TACACS+ Shared Secret: Vendor Name: Enable RADIUS Dynamic Authorization: Enable RADIUS Dynamic Authorization: Enable RadSec:	Biblin PdSS PUIK           MP Write Settings         CLI Settings           [172 25 200 13         [172 25 200 13           [e.g., 192.168.1.10 or 192.168.1         [172 168.1.10 or 192.168.1           [minute content in the set of	OnConnect Enfor	reement Attributes	• :a0b:12f0::1/64)	Add Add Amport Copy Export I Copy Export Desires Copy Export Desires
Administration 0 © Copyright 2022 Hewlett Packard Enterprise Deve	elopment LP D	Dec 28, 2022 09:02:18 CET			ClearPass Policy Mana	ger 6.9.12.136929 on CLABV (Trial Version) platform

Hinzufügen des Aruba Access Switch als vertrauenswürdiges Netzwerkgerät im Aruba ClearPass Policy Manager. Bitte beachten Sie, dass das gemeinsame RADIUS-Geheimnis mit der spezifischen IEEE 802.1X-Konfiguration des Switches übereinstimmen muss.

Sicheres Onboarding – IEEE 802.1AR/802.1X

Q ClearPass Policy Manager - Arub: × +		✓ - □ ×
← → C ▲ Inte säker   https://172.25.201.1	20/tips/tipsContent.action#	🖻 🛧 🔲 😩 :
aruba	ClearPass Policy Manager	Menu 🗮
Dashboard	Configuration » Network » Devices	
Monitoring O	Network Devices	🚽 Add
Configuration •		A Import
- 🖧 Service Templates & Wizards		<ul> <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.	
Identity		
	Filter: Name v contains Go Clear Filter	Show 20 🗸 records
- + Network	* Name A IP or Subnet Address Device Groups	Description
- 🗘 Devices	1. SW04 172.25.200.13 -	A SHI A THE WARD
- Device Groups	Showing 1-1 of 1	Copy Export Delete
- Proxy largets		
-Q Network Scan		
- Delicy Simulation		
Administration 0		
© Copyright 2022 Hewlett Packard Enterprise Dev	elopment LP Dec 28, 2022 09:02:33 CET ClearPass Policy M	1anager 6.9.12.136929 on CLABV (Trial Version) platform

Der Aruba ClearPass Policy Manager mit einem konfigurierten vertrauenswürdigen Netzwerkgerät.

Q ClearPass Policy Manager - Arub × +		✓ - □ ×
← → C ▲ Inte säker   https://172.25.201.1	120/tips/tipsContent.action#tipsNADGroups.action	le ☆ □ ≗ :
aruba	ClearPass Policy Manager	Menu 🗮
Dashboard	Configuration » Network » Device Groups	
Monitoring O	Network Device Groups	🐥 Add
Configuration O		Evport All
- O Service Templates & Wizards	Device Groups function as a component in service and role mapping rules. Device groups can also be associated with enforcement profiles.	Export Air
Identity	Filter: Name  v contains v Go Clear Filter	Show 20 v records
Posture	# Name A Format Description	
🗉 🔹 Enforcement		Export Delete
🖻 🕂 Network		
- 🗘 Devices		
- Device Groups		
- C Event Sources		
- A Network Scan		
- Dicy Simulation		
🛃 Administration 🛛 🛛 🛛 🛛		
© Copyright 2022 Hewlett Packard Enterprise Dev	elegoment LP         Dec 28, 2022 08:57:07 CET         ClearPass Policy Manager 6.9.12.136929 on CLA	BV (Trial Version) platform

Die Schnittstelle für vertrauenswürdige Netzwerkgerätegruppen im Aruba ClearPass Policy Manager.

Sicheres Onboarding - IEEE 802.1AR/802.1X

O ClearPass Policy Manager - Arub × +					✓ - □ ×
← → C ▲ Inte säker   https://172.25.201.120/tips/tip	psContent.action#				🖻 🛧 🔲 😩 :
aruba		ClearPass Policy M	anager		Menu 🗮
Dashboard O Configu	uration » Network » Device Groups			_	
Monitoring • Netwo	work Device Add New Device Group		•		Add
Configuration O	Name:	Switches			Letter All
- C Service Templates & Wizards Device	Groups function Description:	Access Switches		nent profiles.	
- O Services					
E Q Identity	Name Format:	O Subnet			Show 20 V records
🕞 🖶 Posture 📃 🗮	Name	Regular Expression			
SE Enforcement	Available Devices (0)	0 100	Selected Devices (1)		
Devices		Filter	Filter		
Device Groups			SW04 [172.25.200.13]		
Proxy Targets					
- C Network Scan					
- Delicy Simulation					
			Save		
🖉 Administration 🛛 🔍					
© Copyright 2022 Hewlett Packard Enterprise Development	t LP Dec 2	8, 2022 09:05:28 CET		ClearPass Policy Manager 6.9.12.136929 on CLA	BV (Trial Version) platform

Hinzufügen eines vertrauenswürdigen Netzwerkzugriffsgeräts zu einer neuen Gerätegruppe im Aruba ClearPass Policy Manager.

ClearPass Policy Manager - Arub × +		~ - 🗆 X
← → C ▲ Inte säker   https://172.25.201.12	20/tips/UpsContent.action#	e 🖈 🛛 😩 :
aruba	ClearPass Policy Manager	Menu 🗮
Dashboard	Configuration > Network > Device Groups	
Monitoring O	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		
Posture	Filter: Name V contains Contains Go Clear Filter	Show 20 🗸 records
🗈 🔹 Enforcement	# Name A Format Description	
∃ + Network	1. Switches List Access Switches	
- Devices	Showing 1-1 of 1	Export Delete
Proxy Targets		
- C Event Sources		
- 🛱 Network Scan		
- C Policy Simulation		
Administration		
Converight 2022 Hewlett Packard Enterprise Dove	alonanat L9 Dac 28 2022 00:05:43 CET Clareford Pallor Manager 6 0.12 126/20 ap C	ABV (Trial Version) platform
Copyright 2022 newlett Packard Enterprise Deve	sopment EP Dec 20, 2022 05:05:45 CE1 ClearPass Policy Pidlager 0.9:12:130929 01 Cl	Aby (mai version) plation

Der Aruba ClearPass Policy Manager mit konfigurierter Netzwerkgerätegruppe, die ein oder mehrere vertrauenswürdige Netzwerkgeräte umfasst.

#### Konfiguration des Gerätefingerabdrucks

Das Axis Gerät kann gerätespezifische Informationen wie MAC Adresse und Firmware-Version über Netzwerkerkennung weiterleiten. Ein Gerätefingerabdruck kann über die Benutzeroberfläche für Gerätefingerabdrücke im Aruba ClearPass Policy Manager erstellt werden. Es ist möglich, den Gerätefingerabdruck zu aktualisieren und zu verwalten. Je nach AXIS OS Version kann unter anderem der Zugriff gewährt oder verweigert werden.

### Sicheres Onboarding - IEEE 802.1AR/802.1X

Es ist möglich, den Gerätefingerabdruck zu aktualisieren und zu verwalten. Je nach AXIS OS Version kann unter anderem der Zugriff gewährt oder verweigert werden.

- 1. Gehen Sie zu Administration > Dictionaries > Device Fingerprints (Verwaltung > Wörterbücher > Gerätefingerabdrücke).
- 2. Wählen Sie einen vorhandenen Gerätefingerabdruck aus oder erstellen Sie einen neuen Gerätefingerabdruck.
- 3. Legen Sie die Einstellungen für den Gerätefingerabdruck fest.

Q ClearPass Policy Manager - Arub × +								~ - 🗆 X
← → C ▲ Inte säker   https://172.25.201.1	20/tips/tip:	sContent.action#tip	osFingerprintDictionary.action					⋵ ☆ 🛛 😩 :
aruba			C	learPass Poli	cy Manager			Menu 🗮
Dushicoring     Monitoring     Monitoring     Monitoring     Configuration     Configuration	Adminis Devic This page Filter: [ 1. 2. 3. 4. Showing	tration * Dictions te Fingerprin <i>e lists all the de</i> anily <b>Category</b> Network Can Network Can Server 9 1-4 of 4	rifes + Device Fingerprints Internet ingerprints recognized I Update Device Fingerprints Category: Family: Name: Category: Tambi; Name: Category: Tambi; Name: Category: Tambi; Name: Category: Tambi; Name: Category: Tambi; Name: Category: Tambi; Name: Category: Sale Povice Fingerprints Category: Sale Povice Fingerprints Category: Ca	eted	these fingerprints are upda	ted from the Saftware Delete Rule	<ul> <li>Updates page.</li> <li>Name</li> <li>AXIS OS version unsupported</li> <li>AXIS OS version supported</li> <li>AXIS Network Camera</li> <li>AXIS Print Server</li> </ul>	Add Import Custom Fingerprints Export Custom Fingerprints Show 20 v records
<ul> <li>Copyright 2022 Hewlett Packard Enterprise Devi</li> </ul>	elopment	LP	Nov 25, 2	022 08:50:09 CET			ClearPass Policy Manager 6.9.12.136	929 on CLABV (Trial Version) platform

Die Konfiguration des Gerätefingerabdrucks im Aruba ClearPass Policy Manager. Axis Geräte mit einer anderen Firmware-Version als 10.12 gelten als nicht unterstützt.

Sicheres Onboarding - IEEE 802.1AR/802.1X

										~			×
ClearPass Policy Manager - Arub: × +													
← → C ▲ Inte säker   https://172.25.201.12	20/tips/tips	Content.action#ti	psFingerprintDictionar	y.action						E	? ☆		<b>1</b> :
aruba				Clear	rPass Po	licy Man	ager					Menu	$\equiv$
Dashboard O	Adminis	tration » Diction	aries » Device Finge	rprints									
Monitoring O	Devic	e Fingerpri	nts							🗣 Add	2.16.11		
👶 Configuration 🛛 🛛 🛛 O										Export C	Justom	Finger	prints
🔐 Administration 💿	This pag	ge lists all the de	vice fingerprints rec	ognized by the	Profiler module	. These finger	prints are updated fro	m the Softwar	e Updates page.				
- PClearPass Portal			Update Device Fin	gerprints				0					
🔄 🖴 Users and Privileges	Filter: F	amily								s	Show 2	) <b>v</b> r	records
Server Manager	#	Category	Category:	Netv	work Camera				Name				
External Accounts	1.	Network Can	Family:	Axis					AXIS OS version unsupported				
Gertificates	2.	Network Can	Name:	AXI	S OS version su	ipport 💌			AXIS OS version supported				
🖃 🛄 Dictionaries	з.	Network Can	Custom Rules- 1		Match	es (ALL )		Delete Rule	Axis Network Camera				
- J RADIUS	4.	Server	Name		Operator	Value			Axis Print Server				
- PRADIUS Dynamic Authorization Templat	Showing	1-4 of 4	1. Host MAC V	endor	contains_all	Axis Cor	nmunications AB						
Provide Engeroripte			2. LLDP System	m Description	contains	10.12							
- Dictionary Attributes			3. SNMP Syste	m Description	contains	10.12							
- Applications													
- Je Context Server Actions													
- Je Ingress Events													
- J <sup>®</sup> Windows Hottixes													
Agents and Software Updates													
🗈 🐁 Support			*Note: 0 Rule(s) w	vill be deleted		Update	Delete Fingerprint	Close					
			_	_	_	_							
<u>a</u>		-											
© Copyright 2022 Hewlett Packard Enterprise Deve	elopment l	LP	C	Dec 05, 2022 09	9:05:39 CET				ClearPass Policy Manager 6.9.12.136	929 on CLABV	Trial Ve	rsion) p	platform

Die Konfiguration des Gerätefingerabdrucks im Aruba ClearPass Policy Manager. Axis Geräte mit Firmware 10.12 gelten im obigen Beispiel als unterstützt.

Informationen zum Geräte-Fingerabdruck, der von Aruba ClearPass Manager erfasst wurde, finden Sie im Abschnitt "Endpunkte".

- 1. Gehen Sie zu Configuration > Identity > Endpoints (Konfiguration > Identität > Endpunkte).
- 2. Wählen Sie das Gerät, das Sie ansehen möchten.
- 3. Klicken Sie auf die Registerkarte Gerätefingerabdrücke.

#### Hinweis

SNMP ist in Axis Geräten standardmäßig deaktiviert und wird vom Aruba-Zugangsschalter erfasst.

Sicheres Onboarding – IEEE 802.1AR/802.1X



Ein Axis Gerät, das vom Aruba ClearPass Policy Manager profiliert wurde.

ClearPass Policy Manager - Arub × +						~ -	o ×
← → C ▲ Inte säker   https://172.25.201.12	20/tips/tipsConten	t.action#tipsEndpoints.action				₽ ☆ [	1 🛎 E
aruba			ClearPass Policy Man	ager		м	renu 🔳
Dashboard Deshboard Deshboard Deshboard Deshboard Deshboard Desrvices Desrv	Configuration - Endpoints This page an connected (e O select AL Filter: [MACA Filter: [MACA Filter: [MACA Filter: [MACA Showing 1-4	Identity > Endpoints  Edit Endpoint  Endpoint Attributes  CDP Device Description: DHCP Option5: DHCP Option5: Host MAC Vendor: LLDP System Description: SNMP Device Name: SNMP Device Type: SNMP System Description:	Device Fingerprints Endpoint Fingerprint Details 1,3,6,12,15,28,42,66,119 AXIS,Panoramic Camera,P3727-PLE,10.12.1 33,57,55,12,60,61 Axis Communications AB AXIS P3727-PLE Panoramic Camera 10.12.1 axis-b8a443042ea Host AXIS P3727-PLE Panoramic Camera 10.12.1	20 20 30 30	orth with a network to which it is Y Status Unknown Unknown Unknown ger Server Action Update Eingerprint	Show 20 Profiled Yes Yes Yes Export	Add Import Export All
Administration 0	lopment LP		Dec 29, 2022 08:28:24 CET	ClearPa	ss Policy Manager 6.9.12.136929 on CLAB	/ (Trial Vers	ion) platform

Die detaillierten Gerätefingerabdrücke eines profilierten Axis Geräts. Bitte beachten Sie, dass SNMP in Axis Geräten standardmäßig deaktiviert ist. LLDP-, CDP- und DHCP-spezifische Erkennungsinformationen werden vom Axis Gerät im werkseitigen Standardzustand gemeinsam genutzt und vom Aruba-Zugriffsschalter an den ClearPass Policy Manager weitergeleitet.

#### Konfiguration des Durchsetzungsprofils

Das Durchsetzungsprofil wird verwendet, um dem Aruba ClearPass Policy Manager zu ermöglichen, einem Zugriffsport am Switch eine bestimmte VLAN-ID zuzuweisen. Es handelt sich um eine richtlinienbasierte Entscheidung, die für die Netzwerkgeräte in der Gerätegruppe "Switches" gilt. Die erforderliche Anzahl an Durchsetzungsprofilen hängt von der Anzahl der verwendeten VLANs ab. In unserem Setup gibt es insgesamt drei VLANs (VLAN 201, 202, 203), die drei Durchsetzungsprofilen entsprechen.

### Sicheres Onboarding - IEEE 802.1AR/802.1X

Nachdem die Durchsetzungsprofile für das VLAN konfiguriert wurden, kann die eigentliche Durchsetzungsrichtlinie konfiguriert werden. Die Durchsetzungsrichtlinienkonfiguration im Aruba ClearPass Policy Manager definiert anhand von vier Beispielen für Richtlinienprofile, ob Axis Geräten Zugriff auf Aruba-Netzwerke gewährt wird.

ClearPass Policy Manager - Arub 🗙 🕂								~	-	• ×
← → C ▲ Inte säker   https://172.25.201.13	20/tips,	/tipsContent.action#ti	psEditEnforcementProfile.action%3	FcontextData%3D3004				Ŀ	☆	I 😩 E
aruba			Cle	arPass Policy Manag	jer					Menu 🔳
Dashboard	Conf	figuration » Enforcer	nent » Profiles » Edit Enforceme	ent Profile - Allow_VLAN_201						
Monitoring 0	Enf	forcement Pro	- increment Profiles - Allow VLAN 201							
Configuration 💿	Su	mmary Profile	Attributes							
- 🛱 Service Templates & Wizards	Prof	file:								
	Nam	ie.	Allow VIAN 201							
I Q Identity	Desc	cription:								
Posture	Type	21 J	RADIUS							
Enforcement	Actio	on:	Accept							
- D Policies	Devi	ice Group List:	1. Switches							
	Attri	ibutes:								
— 🛱 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			
	< 1	Back to Enforceme	nt Profiles				C	ору	Save	Cancel
🚰 Administration 🛛 🔍 🛛										
© Copyright 2022 Hewlett Packard Enterprise Deve	elopme	ent LP	Dec 28, 202	2 09:08:57 CET			ClearPass Policy Manager 6.9.12.136929 on C	LABV (Tr	rial Ver	sion) platform

Ein Beispiel für ein Durchsetzungsprofil, um den Zugriff auf VLAN 201 zu ermöglichen.

← → C         ▲ Inte säker   https://itps:/uips/uips/lips/cintent.action#tipsEditEnforcementPolicy.action%is3FcontextData%303007             Concloc           ClearPass Policy Manager             Configuration = Enforcement * Policies > Edit - Axis Radius policy           Configuration = Enforcement * Policies > Edit - Axis Radius policy             Configuration           Configuration = Enforcement * Policies - Axis Radius policy             Configuration           Configuration             Services           Configuration             Services           Configuration             Services           Fiforcement             Services           Configuration             Services           Configuration             Services           Fiforcement             Services           Configuration             Services           Configuration             Services           Fiforcement             Policies           Configuration Algorithm: First applicable             Onthions           Confificate::ssuer-On CONTAINS Axis Communications AB             Avp         (certifidate::s	년 ☆ 🛛 🌲 : Menu 🚞
ClearPass Policy Manager      Configuration > Enforcement > Policies > Edit - Axis Radius policy      Configuration > Enforcement Policies - Axis Radius policy      Configuration > Enforcement Rules      Configuration > Enforcement	Menu 🗮
Deskhoord     Onfiguration > Enforcement > Policies > Edit - Axis Radius policy     Enforcement Policies - Axis Radius policy     Enforcement Policies - Axis Radius policy     Enforcement Rules     Service Emplates & Wizards     Service Emplates & Wizards     Service Enforcement     Avis Radius policy     Service Rules     Enforcement     Avis Radius policy     Service Rules     Enforcement     Postre     Service Rules     Rules     Rules     Rules     Rules     Rules     Conflicient     Postre     Service Rules     Rules     Rules     Rules     Rules     Conflictes     Postre     Service Rules     Rules     Rules     Conflictes     Rules     Rules     Conflictes     Rules     Rules     Rules     Rules     Conflictes     Rules     Rules     Rules     Rules     Rules     Rules     Conflictes     Actions     Conflictes     Actions     Conflictes     Avis Radius policy     Service     Rules     Conflictes     Actions     Conflictes     Avis Radius policy     Service     Rules     Conflictes     Avis Radius policy     Service     Rules	
Monitoring       Enforcement Policies - Axis Radius policy         Service Templates & Wizards       Service Templates & Wizards         Service Templates & Wizards       Enforcement         Revice Templates & Urzards       Enforcement         Revice Templates & Urzards       Axis Radius policy         Description:       Enforcement         Description:       Enforcement Type:         Rational Profiles       Aulow_VLAN_203         Rules:       Rules:         Name:       Axis device ID Intermediate CA)         Avio (Certificate:Issuer-CN CONTAINS Axis device ID Intermediate CA)         Avio (Certificatexisuer-CN CONTAINS Axis demuninciations AB) </td <td></td>	
Configuration     Summary     Enforcement     Rules       © Services     Enforcement     Axis Radius policy       © Authentication     Name:     Axis Radius policy       © Inforcement     Description:       © Posture     Enforcement Type:       © Policies     Allow_VLAN_203       Policy Simulation     Rules       © Network Scan     Confitions       © Policy Simulation     Certificate:Issuer-CN_CONTAINS_Axis device ID Intermediate CA) AND       (Certificate:Issuer-CN_CONTAINS_Axis device ID Intermediate CA) AND     Certificate:Issuer-CN_CONTAINS_Axis device ID Intermediate CA) AND	
Conditions	
Authorization         Name:         Axis Radius policy         Description:         Identity         Description:         Enforcement         Default Profile:         Allow_VLAN_203         Conditions         Rules:         Rules:         Rules:         Rules:         Rules:         Conditions         Conditions AB()         Aution VLAN_204:         Actions         Actions Actions AB()         Aution VLAN_204:         Actions AB()         Actions         Actions AB()         Actions AB() </td <td></td>	
Image: Posture     Enforcement Type:     RADIUS       Image: Enforcement Profiles     Allow_VLAN_203       Image: Policy Simulation     Rules:       Image: Policy Simulation     Rules: First applicable       Image: Policy Simulation     Conditions       Image: Policy Simulation     Conditions AB()	
Senforcement     Default Profile: Allow_VLAN_203      Reules:     Conditions     Rules:     Conditions     Condition     Conditions     Conditions     Conditions     Conditions	
Avery of the set	
Average State     Conditions     Condititit     Conditions     Conditions     Conditions     Conditions	
Policy Simulation     (Certificate:Issuer-CN_CONTAINS_Axis device ID Intermediate CA)     AND (Certificate:Issuer-CD_EQUALS_Axis Communications AB)     AND (Certificate:Subject-D_EQUALS_Axis Communications AB)	
AND (Certificate:Subject- EQUALS Lund) AND (Certificate:Subject- EQUALS SE) AND (Connection:Client-MacAddress-HoDelim EQUALS %(Certificate:Subject-serialNumber))	
(Certificate:Issuer-CN CONTAINS Production CA Certificate)           2. AND (Certificate:Subject-CN CONTAINS % (Connection:Clinet-Mac-Address-NoDelim))         Allow_VLAN_201           AND (Authorization:[Endpoints Repository]:Device Name EQUALS AXIS 05 version unsupported)         Allow_VLAN_201	
(Certificate: Susject-CNL CONTAINS % Production CA certificate)           3.         AND         (Certificate: Subject-CNL CONTAINS % (Connection:Clinet-Mac-Address-NoDelim))         Allow_VLAN_202           AND         (Authorization: Endpoints Repository):Device Name EQUALS AXIS 05 version supported)         Allow_VLAN_202	
Back to Enforcement Policies	Copy Save Cancel
Concide 2023 Hould Backgraf Entergine Development I. Develop 2023 00:48:00 CET Concide 2023 00:48:00 CET	

Die Konfiguration für die Durchsetzungsrichtlinie im Aruba ClearPass Policy Manager.

Die vier Durchsetzungsrichtlinien und ihre Maßnahmen sind unten aufgeführt:

Netzwerkzugriff verweigert

### Sicheres Onboarding - IEEE 802.1AR/802.1X

Der Zugriff auf das Netzwerk wird verweigert, wenn keine IEEE 802.1X-Authentifizierung der Netzwerkzugriffskontrolle durchgeführt wird.

#### Gastnetzwerk (VLAN 203)

Dem Axis Gerät wird Zugriff auf ein begrenztes, isoliertes Netzwerk gewährt, wenn die IEEE 802.1X-Authentifizierung der Netzwerkzugriffskontrolle fehlschlägt. Um entsprechende Maßnahmen ergreifen zu können, ist eine manuelle Inspektion des Geräts erforderlich.

#### Bereitstellung des Netzwerks (VLAN 201)

Dem Axis Gerät wird Zugriff auf ein Bereitstellungsnetzwerk gewährt. So sollen Axis Geräteverwaltungsfunktionen durch *Axis Device Manager* und *Axis Device Manager Extend* bereitgestellt werden. Darüber hinaus ist es möglich, Axis Geräte mit Firmware-Updates, Produktionszertifikaten und anderen Konfigurationen zu konfigurieren. Die folgenden Bedingungen werden vom Aruba ClearPass Policy Manager überprüft:

- Die Firmware-Version des Axis Geräts.
- Die MAC Adresse des Geräts stimmt mit dem herstellerspezifischen Axis MAC Adressen-Schema mit dem Seriennummernattribut des Axis Geräte-ID-Zertifikats überein.
- Das Axis Geräte-ID-Zertifikat ist überprüfbar und entspricht den für Axis spezifischen Attributen wie Aussteller, Organisation, Standort, Land.

#### Produktionsnetzwerk (VLAN 202)

Dem Axis Gerät wird Zugriff auf das Produktionsnetzwerk gewährt, in dem das Axis Gerät betrieben wird. Der Zugriff wird gewährt, nachdem die Gerätebereitstellung innerhalb des Bereitstellungsnetzwerks (VLAN 201) abgeschlossen ist. Die folgenden Bedingungen werden vom Aruba ClearPass Policy Manager überprüft:

- Die MAC Adresse des Geräts stimmt mit dem herstellerspezifischen Axis MAC Adressen-Schema mit dem Seriennummernattribut des Axis Geräte-ID-Zertifikats überein.
- Die Firmware-Version des Axis Geräts.
- Das Produktionszertifikat kann vom vertrauenswürdigen Zertifikatsspeicher überprüft werden.

#### Konfiguration der Authentifizierungsmethode

In der Authentifizierungsmethode wird definiert, wie ein Axis Gerät versucht, sich gegenüber dem Aruba-Netzwerk zu authentifizieren. Die bevorzugte Authentifizierungsmethode sollte IEEE 802.1X EAP-TLS sein, da bei Axis Geräten mit Unterstützung für Axis Edge Vault standardmäßig IEEE 802.1X EAP-TLS aktiviert ist.

Sicheres Onboarding – IEEE 802.1AR/802.1X

O ClearPass Policy Manager - Arub × +						× -	o ×
← → C ▲ Inte säker   https://172.	25.201.120/tips/tips	Content.actio	on#tipsAuthMet	hods.action		년 🌣 🗖	<b>a</b> :
aruba				ClearPas	ss Policy Manager	Me	nu 🔳
Dashboard	O Configur	ation » Autl	hentication » M	1ethods			1
Monitoring	• Authe	nticatio	n Method	s		🐳 Ado Al Imp V. Exe	d port port All
- 🛱 Service Templates & Wizards - 🛱 Services	As a first	t step in the	e service-base	Edit Authentication Method		r device against an authentication source.	
- 🛱 Methods	Filter: N	ame		General		Show 20 V	records
- 🛱 Sources		Nat		Name: A	toris EAP TLS	Description	
Deture	1.		Who FAR CTCL	Description: D	efault settings for EAP-TLS	EABLCTC method to use with Aruba EABLCTC plugin for Windows	
Figure Fostore	2.		thorizol			Default settings for Authorize	
- + Network	4			Type: E	AP-TLS	Default settings for EAP-TLS	
- 🛱 Network Scan	5				Method Details	Default settings for CHAP	
- 🛱 Policy Simulation	6.		P FAST1	Session Resumption:	Enable	Default settings for EAP-FAST	
	7.		P GTC1	Session Timeout:	6 bours	Default settings for EAP-GTC	
	8.	[EA	P MD5]	Authorization Required:	Enable	Default settings for EAP-MD5	
	9.		P MSCHAPv2]	Certificate Comparison:	Do not compare V	Default settings for EAP-MSCHAPv2	
	10.		P PEAP]	Verify Certificate using OCSP:	None 🗸	Default settings for EAP-PEAP	
	11.	(EA	P PEAP Public	Override OCSP URL from Clie	nt: 🗆 Enable	Default settings for EAP-PEAP-Public	
	12.	[EA	P PEAP Withou	OCSP URL:		EAP-PEAP with Fast Reconnect disabled; recommended for Onboard	
	13.		P PWD]			Default settings for EAP-PWD	
	14.	. (EA	P TLS]		Copy Save Can	Default settings for EAP-TLS	
	15.	- (EA	P TLS With O			EAP-TLS with OCSP enabled; recommended for Onboard	
	16.	[EA]	P TTLS]		EAP-TTLS	Default settings for EAP-TTLS	
	17.	[MA	AC AUTH]		MAC-AUTH	Default settings for MAC-AUTH	
	18.	🗌 [MS	SCHAP]		MSCHAP	Default settings for MSCHAP	
Administration	19.	🗆 [PA	P]		PAP	Default settings for PAP	
Copyright 2022 Hewlett Packard Enterpr	20. ise Development L	P Iss	101	Dec 28, 2022 09:43:30	PAP D CET	Default settings for SSO ClearPass Policy Manager 6.9.12.136929 on CLABV (Trial Versio	n) platforn

Die Authentifizierungsmethoden-Schnittstelle des Aruba ClearPass Policy Managers, in der die EAP-TLS-Authentifizierungsmethode für Axis Geräte definiert wird.

#### Servicekonfiguration

In der Services-Schnittstelle werden die Konfigurationsschritte in einem einzigen Dienst zusammengefasst, der die Authentifizierung und Autorisierung von Axis Geräten in Aruba-Netzwerken übernimmt.

Q ClearPass Policy Manager - Arub × +				V	- 1	o x
← → ♂ ▲ Inte säker   https://172.25.201.12	20/tips/tipsContent.action#tip	osEditService.action%3FcontextData%3D3001		E	2 🖈 🗖	
aruba		ClearPass P	olicy Manager		Mei	nu <b>=</b>
Dashboard	Configuration » Services	» Edit - Axis 802.1X Wired				
Monitoring O	Services - Axis 8	02.1X Wired				
Configuration 📀	Summary Service	Authentication Roles Enforcement				
- 🛱 Service Templates & Wizards	Name:	Axis 802.1X Wired	]			
- C Services	Description:	To authenticate users to any wired network via 802.1X.				
Beforement	Туре:	802.1X Wired				
Network	Status:	Enabled				
- 🛱 Network Scan	Monitor Mode:	Enable to monitor network access without	enforcement			
—☆ Policy Simulation	More Options:	Authorization Posture Compliance	Audit End-hosts 🛛 Profile Endpoints 🗆 Accountin	g Proxy		
			Service Rule			
	Matches O ANY or 🔍 A	ALL of the following conditions:				
	Туре	Name	Operator	Value		
	1. Radius:IETF	NAS-Port-Type	EQUALS	Ethernet (15)		20 T
	2. Radius:IETF	Service-Type	BELONGS_TO	Authenticate-Only (8)	<u> </u>	6 <u>8</u> 17
	3. Click to add					
	Back to Services			Disable Copy	Save	Cancel
🚰 Administration 🔹 💿						
© Copyright 2022 Hewlett Packard Enterprise Deve	lopment LP	Dec 28, 2022 09:41:27 CET		ClearPass Policy Manager 6.9.12.136929 on CLABV	(Trial Version	n) platform

Es wird ein dedizierter Axis Dienst erstellt, der IEEE 802.1X als Verbindungsmethode definiert.

Sicheres Onboarding – IEEE 802.1AR/802.1X

ClearPass Policy Manager - Arub × +			× - 🗆 X
← → C ▲ Inte säker   https://172.25.201	1.120/tips/tipsContent.action#tips	ditService.action%3FcontextData%3D3001	년 ☆ 🛛 😩 :
aruba		ClearPass Policy Manager	Menu 🗮
Dashboard	Configuration » Services »	Edit - Axis 802.1X Wired	
Monitoring	<ul> <li>Services - Axis 80</li> </ul>	2.1X Wired	
Configuration	Summary Service	Authentication Roles Enforcement	
Corrice Templates & Wizards     Corrice Templates & Wizards     Corright Cation     Corright Cation	Authentication Methods:	Axis EAP TLS  Move Up 1  Move Down 1  Remove View Details  Modily  Select to Add-  (Endpoints Repository] [Local SQL DB]  Move Up 1  Move Up 1  Move Up 1  Remove View Details Modify  Select to Add-  View Details	Add New Authentication Method Add New Authentication Source
	Strin Username Rules:	Enable to energy a comma-senarated list of rules to strip username prefixes or suffixes	
	Service Certificate:	-Select to Add-	View Certificate Details
A Multi-Instead on	Back to Services		Disable Copy Save Cancel
Administration	evelopment I P	Dec 28, 2022 00:41:41 CET	ClearDace Policy Manager 6.9.12.136020 on CLABV (Trial Version) platform
© Copyright 2022 Hewlett Packard Enterprise De	evelopment LP	Dec 28, 2022 09:41:41 CET	ClearPass Policy Manager 6.9.12.136929 on CLABV (Trial Version) platform

Im nächsten Schritt wird die zuvor erstellte EAP-TLS-Authentifizierungsmethode für den Dienst konfiguriert.

Q ClearPass Policy Manager - Arub 🗙 🕂			✓ - □ X							
← → C ▲ Inte säker   https://172.25.201.12	20/tips/tipsContent.action#tips	EditService.action%3FcontextData%3D3001	@ 🖈 🗖 🚢 :							
aruba	ClearPass Policy Manager									
Dashboard O	Configuration » Services »	iguration » Services » Edit - Axis 802.1X Wired								
Monitoring O	Services - Axis 80	02.1X Wired								
Configuration O	Summary Service	Authentication Roles Enforcement								
- 🛱 Service Templates & Wizards	Use Cached Results:	Use cached Roles and Posture attributes from previous sessions								
Services     Authentication	Enforcement Policy:	Axis Radius policy V Modify	Add New Enforcement Policy							
🗈 🧕 Identity		Enforcement Dolicy Date	ile							
🕞 🖶 Posture	Description	Enforcement Policy Dea	115							
Enforcement	Default Brofiles	Allow MAN 202								
Network Scap	Delaut Frome.	Allow_veAw_zos								
	Rules Evaluation Algorithm	n instrappicable								
	(Certificate:Issue     AND (Certificate     AMD (Certificate     AMD (Certificate     AMD (Certificate     AMD (Certificate:Issuer     AND (Certificate:Issuer     AND (Certificate     AND (Certificate     AND (Authoriza     AND (Authoriza	-CN_CONTAINS Axis device ID Intermediate CA) Insurb.ec. 2014.5 Axis Communications AB) Insubject- EQUALS Axis Communications AB) Insubject- EQUALS Suid Insubject- CANALS Lund) Insubject- CANALS SUID (Cant-Mac-Address-NoDelim FQUALS % (Certificate:Subject-serialNumber)) -CN_CONTAINS Production CA Certificate) Insubject-CN_CONTAINS % (Connection:Client-Mac-Address-NoDelim)) Ion:Cliendpoints Repositor;):Device Name EQUALS AXIS OS version unsupported) CN_CONTAINS Production CA certificate) Ion:Endpoints Repository]:Device Name EQUALS AXIS OS version supported) Ion:Endpoints Repository]:Device Name EQUALS AXIS OS version supported)	Allow_VLAN_201 Allow_VLAN_201 Allow_VLAN_202							
Administration 0	K Back to Services		Disable Copy Save Cancel							
© Copyright 2022 Hewlett Packard Enterprise Deve	elopment LP	Dec 28, 2022 09:51:01 CET	ClearPass Policy Manager 6.9.12.136929 on CLABV (Trial Version) platform							

Im letzten Schritt wird die früher erstellte Durchsetzungsrichtlinie für den Dienst konfiguriert.

#### Aruba-Zugangsschalter

Axis Geräte werden entweder direkt mit PoE-fähigen Aruba-Zugangsschalter oder über kompatible Axis PoE-Midspans verbunden. Um Axis Geräte sicher in Aruba-Netzwerke einzubinden, muss der Zugriffsschalter für die IEEE 802.1X-Kommunikation konfiguriert werden. Das Axis Gerät leitet die IEEE 802,1x EAP-TLS-Kommunikation an den Aruba ClearPass Policy Manager weiter, der als RADIUS-Server fungiert.

### Sicheres Onboarding - IEEE 802.1AR/802.1X

#### Hinweis

Außerdem ist eine regelmäßige Neuauthentifizierung von 300 Sekunden für das Axis Gerät konfiguriert, um die allgemeine Portzugriffssicherheit zu erhöhen.

Sehen Sie sich das folgende Beispiel einer globalen und Portkonfiguration für Aruba-Zugangsschalter an.

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

### **Konfiguration Axis**

#### Axis Netzwerkgerät

Axis Geräte mit Unterstützung für Axis Edge Vault werden mit einer sicheren Geräteidentität hergestellt, der sogenannten Axis Geräte-ID. Die Axis Geräte-ID basiert auf dem internationalen Standard IEEE 802.1AR, der eine Methode zur automatisierten, sicheren Geräteidentifizierung und Netzwerkeinbindung über IEEE 802.1X definiert.



Axis Geräte werden mit dem IEEE 802.1AR-konformen Axis Geräte-ID-Zertifikat für vertrauenswürdige Geräteidentitätsdienste hergestellt

- 1 Axis Geräte-ID-Schlüsselinfrastruktur (PKI)
- 2 Axis Geräte-ID

Der hardwaregeschützte sichere Schlüsselspeicher, der von einem sicheren Element des Axis Geräts bereitgestellt wird, ist werkseitig mit einem gerätespezifischen Zertifikat und entsprechenden Schlüsseln (Axis Geräte-ID) ausgestattet, die die Authentizität des Axis Geräts global nachweisen können. Der Axis Product Selector kann verwendet werden, um zu erfahren, welche Axis Geräte Axis Edge Vault und Axis Geräte-ID unterstützen.

#### Hinweis

Die Seriennummer eines Axis Geräts ist seine MAC Adresse.

### Sicheres Onboarding - IEEE 802.1AR/802.1X

		AXIS Q1656 Box Camera	0 🐺 () 🖪 🗄
윤 Status			
□ Video	~	Certificates	
@ PTZ		+ Add certificate	<u>-a</u> ▼
🛓 Audio	~		
Recordings		Name Type	
🗱 Apps		Axis device ID ECC-P256 (802.1AR) Client-server	
尊 System	^	Axis device ID RSA-2048 (802,1AR) Client-server	
Date and time			
Network		Axis device ID RSA-4096 (802.1AR) Client-server	
Security	- 1	Axis device ID Intermediate CA ECC 2 CA	

Der Zertifikatspeicher des Axis Geräts im werkseitigen Standardzustand mit der Axis Geräte-ID.

Das IEEE 802.1AR-konforme Axis Geräte-ID-Zertifikat enthält Informationen zur Seriennummer und andere herstellerspezifische Informationen von Axis. Die Informationen werden vom Aruba ClearPass Policy Manager zur Analyse und Entscheidungsfindung zur Gewährung des Zugriffs auf das Netzwerk verwendet. Bitte beachten Sie die folgenden Informationen, die einem Axis Geräte-ID-Zertifikat entnommen werden können



Country (Land)	SE
Standort	Lund
Ausstellerorganisation	Axis Communications AB
Allgemeiner Name des Ausstellers	Axis Geräte-ID intermediär
Organisation	Axis Communications AB
Einfacher Name	axis-b8a44f279511-eccp256-1
Seriennummer	b8a44f279511

Der gebräuchliche Name setzt sich aus einer Kombination aus dem Firmennamen von Axis, der Seriennummer des Geräts und dem verwendeten Kryptoalgorithmus (ECC P256, RSA 2048, RSA 4096) zusammen. Seit AXIS OS 10.1 (2020-09 ist IEEE 802.1X standardmäßig mit vorkonfigurierter Axis Geräte–ID aktiviert. Dadurch kann sich das Axis Gerät in IEEE 802.1X-fähigen Netzwerken authentifizieren.

### Sicheres Onboarding - IEEE 802.1AR/802.1X

		AXIS Q1656 Box Camera	0 🖙 и 🖪	:
🖂 Status		IEEE 802.1x Connecting		
Video PTZ Audio Recordings	~	Client certificate ① EAPOL Version          Axis device ID RSA-2048 (802.1AR)       ① 1         CA certificates ①       ② 2         No CA certificate selected       • • • • • • • • • • • • • • • • • • •		
Se Apps	<u>^</u>	EAP Identity		
System     Date and time     Network	~	axis-b8a44f27a03a		
Security			Save	

Das Axis Gerät im werkseitigen Standardzustand mit aktiviertem IEEE 802.1X und vorab ausgewähltem Axis Geräte-ID-Zertifikat.

#### **Axis Device Manager**

AXIS Device Manager und AXIS Device Manager Extend können im Netzwerk verwendet werden, um mehrere Axis Geräte kostengünstig zu konfigurieren und zu verwalten. Axis Device Manager ist eine auf Microsoft Windows basierende Anwendung, die lokal auf einer Maschine im Netzwerk installiert werden kann, während Axis Device Manager Extend für die Geräteverwaltung an mehreren Standorten auf eine Cloud-Infrastruktur angewiesen ist. Beide bieten einfache Verwaltungs- und Konfigurationsfunktionen für Axis Geräte wie:

- Installation von Firmware-Updates.
- Anwendung von Cybersicherheitskonfigurationen wie HTTPS- und IEEE 802.1X-Zertifikaten.
- Konfiguration gerätespezifischer Einstellungen wie Bildeinstellungen und andere.

### Sicherer Netzwerkbetrieb – IEEE 802.1AE MACsec

### Sicherer Netzwerkbetrieb – IEEE 802.1AE MACsec

IEEE 802.1AE MACsec (Media Access Control Security) ist ein genau definiertes Netzwerkprotokoll, das Punkt-zu-Punkt-Ethernet-Verbindungen auf Netzwerkschicht 2 kryptografisch sichert. Es gewährleistet die Vertraulichkeit und Integrität der Datenübertragungen zwischen zwei Hosts.

Der IEEE 802.1AE MACsec-Standard beschreibt zwei Betriebsmodi:

- Manuell konfigurierbarer vorinstallierter Schlüssel/Static CAK-Modus
- Automatische Master-Sitzung/dynamischer CAK-Modus mit IEEE 802.1X EAP-TLS



In AXIS OS 10.1 (2020-09) und später, ist IEEE 802.1X standardmäßig für Geräte aktiviert, die mit der Axis Geräte-ID kompatibel sind. In AXIS OS 11.8 und höher unterstützen wir MACsec mit automatischem dynamischen Modus unter Verwendung von standardmäßig aktiviertem IEEE 802.1X EAP-TLS. Wenn Sie ein Axis Gerät mit werkseitigen Standardwerten anschließen, wird die IEEE 802.1X-Netzwerkauthentifizierung durchgeführt und bei Erfolg wird auch der MACsec Dynamische CAK-Modus ausprobiert.

Die sicher gespeicherte Axis Geräte-ID (1), eine IEEE 802.1AR-konforme sichere Geräteidentität, wird zur Authentifizierung im Aruba-Netzwerk (4, 5) durch IEEE 802.1X portbasierte EAP-TLS-Netzwerkzugriffskontrolle (2) verwendet. Über die EAP-TLS-Sitzung werden MACsec-Schlüssel automatisch ausgetauscht, um eine sichere Verbindung einzurichten (3), die den gesamten Netzwerkverkehr vom Axis Gerät zum Aruba-Switch schützt.

Für IEEE 802.1AE MACsec sind sowohl Konfigurationsvorbereitungen für den Aruba-Zugangsschalter als auch für den ClearPass Policy Manager erforderlich. Um IEEE 802.1AE MACsec-verschlüsselte Kommunikation über EAP-TLS zu ermöglichen, ist keine Konfiguration auf dem Axis Gerät erforderlich.

Wenn der Aruba-Zugangsschalter MACsec mit EAP-TLS nicht unterstützt, kann der Pre-Shared Key-Modus verwendet und manuell konfiguriert werden.

### Sicherer Netzwerkbetrieb – IEEE 802.1AE MACsec

## Aruba ClearPass Policy Manager

#### Rollen- und Rollenzuordnungsrichtlinie

Q app20 × +									∨ – □ X	
← → C ▲ Inte säker   https://172.	.25.201.120/tips	/tipsCc	ontent.action#	tipsRoles.action					ic ☆ □ 😩 :	
aruba					ClearPass	Policy Man	lager		Menu 🗮	
Dashboard	O Configu	ration	n » Identity »	Roles						
Monitoring	Roles	5	🖌 Ado							
S Configuration	0								Export All	
- 🛱 Service Templates & Wizards - 🖨 Services	Roles e	xist in	dependently	of an individual ser	vice and can be acce	essed globally throu	ugh the role-mapping po	licy of any service.	Export rul	
🖃 🗣 Authentication	Filter:	Name		✓ contains :	<b>v</b> 1		Clear Filter		Show 20 V records	
- 🛱 Methods	#		Name 🔺	J. COMMING		Descriptio	n			
- Q Sources	1.		AirGroup	vil		Role for an A	irGroup protocol version	1 request		
Single Sign-On (SSO)	2.		[AirGroup	v21		Role for an A	irGroup protocol version	2 request		
- C Local Users	3.		[Aruba TAC	ACS+ read-only Ad	minl	Default role f	for read-only access to A	uruba device		
- 🗘 Endpoints	4.		Aruba TAC	CACS+ root Admin]		Default role f	for root access to Aruba	device		
- 🛱 Static Host Lists	5.		AxisDevi	Edit Role				•		
Roles	6,		[BYOD O	Role ID:	2001			age their own provisioned devices		
- I Role Mappings	7.		Contrac	Kole ID.	3001			-		
Posture Policies	8.		[Device I	Name:	AxisDevice			their devices, for use with MAC authentic	ation and AirGroup sharing.	
- Audit Servers	9.		Employe	Description:					1 3	
- 🛱 Agentless OnGuard	10.		[Guest]							
🖃 💈 Enforcement	11.		[MAC Ca							
- O Policies	12.		Onboard							
- promes	13.		[Onboard				Save Can	icel d		
Devices	14.		[Onboard i	05]		Role for an iC	OS device being provision	ned		
- Device Groups	15.		[Onboard i	PadOS1		Role for an iP	adOS device being provi	isioned		
- C Proxy Targets	16.		[Onboard ]	inuxl		Role for Linu:	x device being provision	ed		
- 🛱 Event Sources	17.		[Onboard r	macOS1		Role for a ma	acOS device being provis	sioned		
- 🛱 Network Scan	18.		[Onboard )	Vindowsl		Role for a Wi	ndows device being prov	visioned		
- C Policy Simulation	19.		[Other]			Default role f	for another user or devic	e		
	20,		[TACACS+	API Admin1		API administ	rator role for Policy Mana	ager Admin		
	Showin	a 1-20	0 of 25 • •							
Administration	o	ant LD		0.4	26-2022-05:07:25-1			Claubur Dula, Maaaar 6 11 0 19300 d	n (1489/(TrialVersion) al-Farm	
Copyright 2023 Hewlett Packard Enterpr	ise Developme	SHE LP		Oct :	20, 2023 05:07:35 U	JIC		ClearPass Policy manager 6.11.2.252294 c	on CLABV (Irial Version) platform	

Hinzufügen eines Rollennamens für Axis Geräte. Der Name ist der Name der Port-Zugriffsrolle in der Aruba-Zugangsschalter-Konfiguration.

Sicherer Netzwerkbetrieb – IEEE 802.1AE MACsec

<b>Q</b> app20 × +				✓ - □ X
← → C ▲ Inte säker   https://172.25	5.201.120/tips/tipsContent.action#tipsEditRole	MappingPolicy.action%3FcontextData%3D3001		e ☆ □ ≗ :
aruba		ClearPass Policy Manager		Menu
Dashboard	<ul> <li>Configuration » Identity » Role Mappi</li> </ul>	ings » Edit - Axis Role Mapping		
Monitoring	Role Mannings - Axis Role	e Manning		
2 Configuration				
- D Service Templates & Wizards	Summary Policy Mapping Ru	les		
- Di Services	Policy:			
- Authentication	Policy Name: Axis Role	Mapping		
- 🛱 Methods	Description:			
- 🛱 Sources	Default Role: [Guest]			
🖃 🚨 Identity	Manalas Polas			
— 🋱 Single Sign-On (SSO)	Mapping Rules:			
Local Users	Rules Evaluation Algorithm: Evaluate	e all		
- C Endpoints	Conditions		Role Name	
Poloc	1. (Authentication:Full-Username	BEGINS_WITH axis-00408c)	AxisDevice	
Role Mannings	2. (Authentication:Full-Username E	BEGINS_WITH axis-accc8e)	AxisDevice	
	3. (Authentication:Full-Username	BEGINS_WITH axis-b8a44f)	AxisDevice	
🗩 Administration	Back to Role Mappings		Cor	oy Save Cancel
© Copyright 2023 Hewlett Packard Enterpris	e Development LP	Oct 26, 2023 05:08:20 UTC	ClearPass Policy Manager 6.11.2.252294 on CL	ABV (Trial Version) platform

Hinzufügen einer Axis Rollenzuordnungsrichtlinie für die zuvor erstellte Axis Geräterolle. Die definierten Bedingungen sind erforderlich, damit ein Gerät der Axis Geräterolle zugeordnet werden kann. Wenn die Bedingungen nicht erfüllt sind, wird das Gerät Teil der Rolle [Gast] sein.

Standardmäßig verwenden Axis Geräte das EAP-Identitätsformat "axis-serialnumber". Die Seriennummer eines Axis Geräts ist seine MAC Adresse. Zum Beispiel "axis-b8a44f45b4e6".

Sicherer Netzwerkbetrieb – IEEE 802.1AE MACsec

#### Servicekonfiguration



Hinzufügen der zuvor erstellten Axis Rollenzuordnungsrichtlinie zum Dienst, der IEEE 802.1X als Verbindungsmethode für die Einbindung von Axis Geräten definiert.

Sicherer Netzwerkbetrieb – IEEE 802.1AE MACsec

<b>Q</b> app20 × +			v – 🗆
← → 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	02.1X Wired	
Configuration	Summary Service	Authentication Roles Enforcement	
—	Use Cached Results:	Use cached Roles and Posture attributes from previous sessions	
	Enforcement Policy:	Axis Radius policy V Modify	Add New Enforcement Po
- C Methods		Enforcement Pol	licy Details
- Q Sources	Description:		
Single Sign-On (SSO)	Default Profile:	Allow_VLAN_203	
- 🗘 Local Users	Rules Evaluation Algorith	n: evaluate-all	
- 🛱 Endpoints	Conditions		Enforcement Profiles
Posture Policies     Audit Servers     Agentless OnGuard	1. AND (Certificat serialNumber}) AND (Tips:Role (Certificate:Issue AND (Authoriza	e:subject-0 EQUALS Axis Communications AB) m:Clent-Nac-Adress-NoDelim EQUALS %{Certificate:Subject- EQUALS AxisDevice) -CN CONTAINS Production CA) tion:(Endpoints Repositor):Device Name EQUALS AXIS OS version	Allow_VLAN_201
Enforcement     Oplicies     Oplicies     Oplicies	2. unsupported) AND (Certificat AND (Tips:Role	e:Subject-CN CONTAINS Production XYZ) EQUALS AxisDevice)	Allow_VLAN_201
<ul> <li>Network</li> <li>Devices</li> <li>Device Groups</li> <li>Proxy Targets</li> </ul>	(Certificate:Issue AND (Authoriza 3. supported) AND (Certificat AND (Tips:Role	-CN CONTAINS Production CA) tion:[Endpoints Repository]:Device Name EQUALS AXIS OS version e:Subject-CN CONTAINS Production XYZ) EQUALS AxisDevice)	Allow_VLAN_202
🚰 Administration	Back to Services		Disable Copy Save Cance
Copyright 2023 Hewlett Packard Enternr	ise Development I P	Oct 26, 2023 05:11:50 UTC	ClearPass Policy Manager 6 11 2 252294 on CLABV (Trial Version) plat
w soppling it 2020 Hemoti Facial d Enterpr	is bersiopment a	000 207 2020 00121.00 010	cical rate roncy menager of the second of CENDY (mail version) place

Hinzufügen des Axis Rollennamens als Bedingung zu den vorhandenen Richtliniendefinitionen.

Sicherer Netzwerkbetrieb – IEEE 802.1AE MACsec

#### Durchsetzungsprofil

Q app20 × +						∨ – □ ×	
← → C ▲ Inte säker   https://172.25.201.12	20/tips/tipsContent.action	#tipsEditEnforcementProfile.action%	FcontextData%3D3004			@ \$ 🛛 😩 i	
aruba	ClearPass Policy Manager						
Dashboard O C	Configuration » Enforcement » Profiles » Edit Enforcement Profile - Allow_VLAN_201						
Monitoring 0	Enforcement Profiles - Allow VLAN 201						
🛞 Configuration 📀	Supmary Profile Attributes						
- Service Templates & Wizards	Profile:						
Authentication N	Name:	Allow_VLAN_201					
- 🛱 Methods 🛛 D	Description:						
Sources T	Type:	RADIUS					
E Q Identity	Action:	Accept					
D Single Sign-On (SSO)	Device Group List:	1. Switches					
- T Endpoints	Attributes:						
- 🖧 Static Host Lists							
- 🛱 Roles	Type	Na	me		value		
- 🛱 Role Mappings	I. Radius:IETF	Se	ssion-limeout	=	10800		
- 🕀 Posture	2. Radius:IETF	Ter	mination-Action	=	RADIUS-Request (1)		
- C Posture Policies	3. Radius:IETF	Tur	inel-Type	=	VLAN (13)		
-Q Audit Servers	4. Radius:IETF	Tu	nel-Medium-Type	=	IEEE-802 (6)		
- C Agentiess OnGuard	5. Radius:IETF		nnel-Private-Group-Id	=	201		
- Policies	6. Radius:Aruba	Art	iba-User-Role	=	AxisDevice		
- Profiles							
- 🛱 Devices							
- 🛱 Device Groups							
- 🛱 Proxy Targets							
- 🛱 Event Sources							
- C Network Scan							
🙀 Policy Simulation							
	K Back to Enforceme	nt Profiles				Copy Save Cancel	
Administration 0							

Hinzufügen des Axis Rollennamens als Attribut zu den Durchsetzungsprofilen, die im IEEE 802.1X-Onboarding-Dienst zugewiesen sind.

### Aruba-Zugangsschalter

Zusätzlich zur sicheren Onboarding-Konfiguration, die in Aruba-Zugangsschalter auf Seite 16 beschrieben wird, finden Sie weitere Informationen in der folgenden Beispiel-Portkonfiguration für den zu konfigurierenden Aruba-Zugriffsschalter 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-Authentifizierung

### Legacy-Onboarding - MAC-Authentifizierung

Sie können MAC Authentifizierungs-Bypass (MAB) verwenden, um Axis Geräte einzubinden, die IEEE 802.1AR Onboarding mit dem Axis Geräte-ID-Zertifikat und im Werkszustand aktiviertem IEEE 802.1X nicht unterstützen. Wenn die 802.1X-Einbindung fehlschlägt, validiert Aruba ClearPass Policy Manager die MAC Adresse des Axis Geräts und gewährt Zugriff auf das Netzwerk.

Für MAB sind sowohl Konfigurationsvorbereitungen für den Aruba Access Switch als auch für den ClearPass Policy Manager erforderlich. Auf dem Axis Gerät ist keine Konfiguration erforderlich, um MAB für die Einbindung zu ermöglichen.

### Aruba ClearPass Policy Manager

#### Durchsetzungsrichtlinie

Die Durchsetzungsrichtlinienkonfiguration im Aruba ClearPass Policy Manager definiert anhand der folgenden zwei Beispiele für Richtlinienbedingungen, ob Axis Geräten Zugriff auf Aruba-Netzwerke gewährt wird.

Q app20 × +				✓ – □ ×
← → C ▲ Inte säker   https://172.25.20	01.120/tips/tipsContent.action	#tipsEditService.action%3FcontextData%3D3006		ie 🖈 🛛 😩 :
aruba		ClearPass Policy Manager		Menu 🗮
Dashboard O	Configuration » Services	» Edit - Axis 802.1X Wired - Mac Authentication		
Monitoring 0	Services - Axis 8	02.1X Wired - Mac Authentication		
Configuration C	Summary Service	Authentication Roles Enforcement		
<ul> <li>Service Templates &amp; Wizards</li> <li>Service</li> <li>Authentication <ul> <li>Authentication</li> <li>Authentication</li> <li>Sources</li> </ul> </li> <li>Identity <ul> <li>Called</li> <li>Called<!--</td--><td>Use Cached Results: Enforcement Policy: Description: Default Profile: Rules Evaluation Algorith Conditions (Date:Day-of-We 1. AND (Date:Tim AND (Connecti</td><td>Construction     Construction     C</td><td>Policy Details Enforcement Profiles Allow_VLAN_203</td><td>Add New Enforcement Policy</td></li></ul></li></ul>	Use Cached Results: Enforcement Policy: Description: Default Profile: Rules Evaluation Algorith Conditions (Date:Day-of-We 1. AND (Date:Tim AND (Connecti	Construction     C	Policy Details Enforcement Profiles Allow_VLAN_203	Add New Enforcement Policy
📌 Administration 🛛 🛛 🗘	Back to Services		Enable	Copy Save Cancel
Copyright 2023 Hewlett Packard Enterprise I	Development LP	Oct 26, 2023 05:15:57 UTC	ClearPass Policy Manager 6.11.2.25229	34 on CLABV (Trial Version) platform

#### Netzwerkzugriff verweigert

Wenn das Axis Gerät die konfigurierte Durchsetzungsrichtlinie nicht erfüllt, wird ihm der Zugriff auf das Netzwerk verweigert.

#### Gastnetzwerk (VLAN 203)

Dem Axis Gerät wird Zugriff auf ein begrenztes, isoliertes Netzwerk gewährt, wenn die folgenden Bedingungen erfüllt sind:

- Es ist ein Wochentag zwischen Montag und Freitag
- Es ist zwischen 09:00 und 17:00 Uhr

### Legacy-Onboarding - MAC-Authentifizierung

• Der Anbieter der MAC Adresse stimmt mit Axis Communications AB überein.

Da MAC Adressen gefälscht werden können, wird kein Zugriff auf das reguläre Bereitstellungsnetzwerk gewährt. Wir empfehlen, dass Sie MAB nur für das erste Onboarding und zur weiteren manuellen Überprüfung des Geräts verwenden.

#### Quellenkonfiguration

In der Quellenschnittstelle wird eine neue Authentifizierungsquelle erstellt, um nur manuell importierte MAC Adressen zuzulassen.



Legacy-Onboarding – MAC-Authentifizierung

<b>Q</b> app20 × +				✓ – □ ×
← → C ▲ Inte säker   https://172	2.25.201.120/tips/tipsContent.action#	tipsAddAuthSource.action		@☆□ 😩 :
aruba		ClearPass Policy Man	ager	Menu
Dashboard	• Configuration » Authentic	ation » Sources » Add		
Monitoring	Authentication Se	urces		
Configuration				
- C Service Templates & Wizards	General Static Host	ists Summary		
- T Services	Name:	Axis Devices		
- Authentication	Description:	MAC addresses of Axis devices in use.		
- 🛱 Methods				
- 🛱 Sources				
🖃 🧕 Identity	Type:	Static Host List		
– 🛱 Single Sign-On (SSO)	Use for Authorization:	Enable to use this Authentication Source to also fetch	role mapping attributes	
Local Users	Authorization Sources:	Remove		
Static Host Lists		View Details		
- Roles				
Role Mappings		×		
🖃 🖶 Posture				
- 🛱 Posture Policies				
- 🛱 Audit Servers				
- 🛱 Agentless OnGuard				
Enforcement				
- Q Policies				
Network				
The Devices				
Device Groups				
Proxy Targets				
- 🛱 Event Sources				
- 🛱 Network Scan				
- 🛱 Policy Simulation				
	K Back to Authenticat	ion Sources		lext → Save Cancel
Administration		0 + 31 2022 00.21.22 UTC		
Copyright 2023 Hewlett Packard Enterp	inse Development LP	OCC 31, 2023 09:21:23 UTC	ClearPass Policy Manager 6.11.2.252294 0	II CLABY (Inal version) platform

Legacy-Onboarding – MAC-Authentifizierung

Q app20 × +						∨ – □ X
← → C ▲ Inte säker   https://172.25.20	1.120/tips/tipsContent.action#					@ ☆ □ ≗ :
aruba		ClearF	ass Policy Mana	iger		Menu 🗮
Dashboard 0	Configuration » Authentical	tion » Sources » Add				
Monitoring 0	Authentication Sou	urces				
Configuration	General Static Host Li	sts Summary				
- 🛱 Service Templates & Wizards	MAC Address Hest Liste:					
Services	MAC AUDIESS HUST LISTS.	Add Static Host List		0	) 	dd New Static Host List
Authentication		Manual	Auto de dese	-		
- Sources		Name:	Axis devices			
🖃 🧕 Identity		Description:				
– 🛱 Single Sign-On (SSO)				12		
- C Local Users		Host Format:	O Subnet			
- C Endpoints			<ul> <li>Kegular Expression</li> <li>List</li> </ul>			
- Q Roles		Host Type:	O IP Address			
- 🛱 Role Mappings			MAC Address			
E Posture		Host Entries				
Posture Policies		# Address	Description			
- Agentless OnGuard		1. O B8-A4-4F-45-B4-E	5 Axis Device 1	압		
Enforcement		2. O B8-A4-4F-45-B4-E	7 Axis Device 2	E.		
- 🗘 Policies		3. O B8-A4-4F-45-B4-E	Axis Device 3			
- 🛱 Profiles		Address:				
Network		Description:				
- Device Groups						
- Proxy Targets				Save Host		
- 💭 Event Sources						
- 🗘 Network Scan						
- ar Policy Simulation				Course Coursel		
				Save		
	& Back to Authenticatio	on Sources			Next	Save Cancel
🛃 Administration 🛛 🛛 0	, Duck to Authenticult	Si oourees			HEAT -	Current
© Copyright 2023 Hewlett Packard Enterprise D	evelopment LP	Oct 31, 2023 09	20:18 UTC		ClearPass Policy Manager 6.11.2.252294 on CLAB	/ (Trial Version) platform

Es wird eine statische Hostliste erstellt, die Axis MAC Adressen enthält.

Legacy-Onboarding – MAC-Authentifizierung



#### Servicekonfiguration

In der Services-Schnittstelle werden die Konfigurationsschritte in einem einzigen Dienst zusammengefasst, der die Authentifizierung und Autorisierung von Axis Geräten in Aruba-Netzwerken übernimmt.

Legacy-Onboarding - MAC-Authentifizierung



Legacy-Onboarding – MAC-Authentifizierung

<b>Q</b> app20 × +				v –	□ ×			
← → C ▲ Inte säker   https://172		on#tipsEditService.action%3FcontextData%3D3006		19 k	🖬 😩 i			
aruba		ClearPass Policy Ma	anager		Menu <b>E</b>			
B Dashhoard	Configuration » Service	es » Edit - Axis 802.1X Wired - Mac Authentication	0					
Monitoring	9 Services - Avis	802 1X Wired - Mac Authentication						
Configuration	O Services - Axis	Services - Axis 602.1A Wired - Mac Authentication						
- 🛱 Service Templates & Wizards	Summary Service	Authentication Roles Enforcement						
_ O Services	Name:	Axis 802.1X Wired - Mac Authentication						
🖃 🚘 Authentication — 🗘 Methods	Description:	To authenticate guest devices based on their MAC address.						
- Q Sources	Type:	MAC Authentication						
Single Sign-On (SSO)	Status:	Disabled						
- O Local Users	Monitor Mode:	Enable to monitor network access without enforcer	nent					
- 🛱 Endpoints	More Options:	Authorization Audit End-hosts Profile Endpo	oints 🗆 Accounting Proxy					
- 🛱 Static Host Lists			Service Rule					
- CR Roles	Matches O ANY or 🧕	ALL of the following conditions:						
- Role Mappings	Туре	Name	Operator	Value				
- O Posture Policies	1. Radius:IETF	NAS-Port-Type	BELONGS_TO	Ethernet (15)	明治 甘			
- 🛱 Audit Servers	2. Radius:IETF	Service-Type	BELONGS_TO	Login-User (1), Call-Check (10)	Ba 8			
- 🛱 Agentless OnGuard	3. Connection	Client-Mac-Address	EQUALS	%{Radius:IETF:User-Name}	Ra 8			
Senforcement     Oricles     Arafiles	4. Click to add							
<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 © Copyright 2023 Hewlett Packard Enterpi	Back to Services  rise Development LP	Oct 26, 2023 05:15:11 UTC	ClearPass I	Enable Copy Save	Cancel ersion) platform			

Es wird ein dedizierter Axis Dienst erstellt, der MAB als Verbindungsmethode definiert.

Legacy-Onboarding – MAC-Authentifizierung

Q app20 × +					✓ – □ X
← → C ▲ Inte säker   https://172.25	.201.120/tips/tipsContent.action#t	ipsEditService.action%3FcontextData%3D300	06		e 🖈 🛛 😩 :
aruba		ClearPass F	Policy Manager		Menu 🗮
Dashboard	• Configuration » Services »	Edit - Axis 802.1X Wired - Mac Authentio	cation		
Monitoring	<ul> <li>Services - Axis 80</li> </ul>	2.1X Wired - Mac Authentio	cation		
Configuration	Summary Service	Authentication Roles Enforcement	t		
	Authentication Methods:	[Allow All MAC AUTH]	Move Up : Move Down I Remove View Details Modify		Add New Authentication Method
- 🛱 Endpoints		Select to Add	~		
O Static Host Lists     O Static Host Lists     O Roles     O Roles     O Roles     O Role Mappings     O Posture Policies     O Audit Servers     O Audit Servers	Authentication Sources:	Axis Devices [Static Host List]	Move Up † Move Down i Remove View Details Modify		Add New Authentication Source
E-St Enforcement		Select to Add	~		
- ☆ Policies - ☆ Poricies - ☆ Devices - ☆ Device Groups - ☆ Proxy Targets - ☆ Event Sources - ☆ Retwork Scan - ☆ Policy Simulation	Strip Username Rules:	Enable to specify a comma-separate	d list of rules to strip username prefixes or si	uffixes	
Administration	Back to Services			Disable	Copy Save Cancel
© Copyright 2023 Hewlett Packard Enterprise	e Development LP	Oct 31, 2023 09:22:22 UT	с	ClearPass Policy Manager 6.11.2.252294	on CLABV (Trial Version) platform

Die vorkonfigurierte MAC-Authentifizierungsmethode ist für den Dienst konfiguriert. Außerdem wird die zuvor erstellte Authentifizierungsquelle ausgewählt, die eine Liste der Axis MAC Adressen enthält.

Axis Communications AB verwendet die folgenden MAC Adressen-OUIs:

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

Legacy-Onboarding - MAC-Authentifizierung



Im letzten Schritt wird die vorher erstellte Durchsetzungsrichtlinie für den Dienst konfiguriert.

### Aruba-Zugangsschalter

Zusätzlich zur sicheren Onboarding-Konfiguration, die in Aruba-Zugangsschalter auf Seite 16 beschrieben wird, finden Sie weitere Informationen in der folgenden Beispiel-Portkonfiguration für den zu konfigurierenden Aruba-Zugriffsschalter für 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
```

Benutzerhandbuch Secure integration of Axis devices into Aruba networks © Axis Communications AB, 2023 Vers. M4.3 Datum: November 2023 Teil-Nr. T10197992