

Integration Guide

Table des matières

Présentation	3
Intégration sécurisée – IEEE 802.1AR/802.1X	4
Authentification initiale	4
Provisionnement	4
Réseau de production	4
Configuration de HPE Aruba Networking	5
Configuration Axis	16
Fonctionnement réseau sécurisé – IEEE 802.1AE MACsec	19
HPE Aruba Networking ClearPass Policy Manager	20
Commutateur d'accès HPE Aruba Networking	24
Intégration héritée – Authentification MAC	25
HPE Aruba Networking ClearPass Policy Manager	25
Commutateur d'accès HPE Aruba Networking	33

Présentation

Présentation

Ce guide d'intégration vise à décrire les meilleures pratiques de configuration pour intégrer et exploiter les périphériques Axis dans les réseaux HPE Aruba Networking. La configuration s'appuie sur des normes et des protocoles tels que IEEE 802.1X, IEEE 802.1AR, IEEE 802.1AE et HTTPS.

La mise en place d'une automatisation appropriée pour l'intégration du réseau peut permettre d'économiser du temps et de l'argent. Cela permet d'éviter une complexité inutile du système lors de l'utilisation d'applications de gestion de périphériques Axis combinées à l'infrastructure et aux applications HPE Aruba Networking. Voici quelques avantages pouvant être obtenus en combinant les périphériques et logiciels Axis avec une infrastructure HPE Aruba Networking :

- Réduire la complexité système en supprimant des réseaux intermédiaires de périphériques.
- Réduire les coûts en ajoutant l'automatisation des processus d'intégration et de gestion des périphériques.
- Tirer parti des commandes de sécurité réseau sans contact fournies par les périphériques Axis.
- Accroître la sécurité globale du réseau en appliquant l'expertise de HPE et d'Axis.

L'infrastructure réseau doit être prête à vérifier en toute sécurité l'intégrité des périphériques Axis avant de commencer la configuration. Cela permet la souplesse d'une transition définie par logiciel entre les réseaux logiques tout au long du processus d'intégration. Il est nécessaire d'avoir des connaissances dans les domaines suivants avant de procéder à la configuration :

- Gestion de l'infrastructure informatique du réseau d'entreprise à partir de HPE Aruba Networking, notamment les commutateurs d'accès HPE Aruba Networking, ainsi que HPE Aruba Networking ClearPass Policy Manager.
- Expertise dans les techniques modernes de contrôle d'accès au réseau et des politiques de sécurité des réseaux.
- Des connaissances de base sur les produits Axis sont souhaitables mais sont fournies tout au long du guide.

Intégration sécurisée - IEEE 802.1AR/802.1X

Intégration sécurisée - IEEE 802.1AR/802.1X



Périphérique sécurisé embarqué sur des réseaux « Zero-Trust » avec IEEE 802.1X/802.1AR

Authentification initiale

Connectez le périphérique Axis pris en charge par Axis Edge Vault pour authentifier le périphérique sur le réseau. Le périphérique utilise le certificat d'identification du périphérique Axis IEEE 802.1AR via le contrôle d'accès au réseau IEEE 802.1X pour s'authentifier.

Pour accorder l'accès au réseau, ClearPass Policy Manager vérifie l'ID du périphérique Axis ainsi que les autres empreintes digitales spécifiques au périphérique. Les informations, telles que l'adresse MAC et l'AXIS OS en cours d'exécution, sont utilisées pour prendre une décision basée sur des politiques.

Le périphérique Axis s'authentifie auprès du réseau à l'aide du certificat d'identification de périphérique Axis conforme à la norme IEEE 802.1AR.

Le périphérique Axis s'authentifie auprès du réseau HPE Aruba Networking à l'aide du certificat d'identification de périphérique Axis conforme à la norme IEEE 802.1AR.

- 1 Identifiant de périphérique Axis
- 2 Authentification réseau IEEE 802.1x EAP-TLS
- *3 Commutateur d'accès (authentificateur)*
- 4 Gestionnaire de politiques ClearPass

Provisionnement

Après l'authentification, le périphérique Axis se déplace vers le réseau de mise en service (VLAN201) où AXIS Device Manager est installé. Depuis AXIS Device Manager, il est possible de procéder à la configuration des périphériques, au renforcement de la sécurité et aux mises à jour d'AXIS OS. Pour terminer la mise en service du périphérique, de nouveaux certificats de qualité de production spécifiques au client sont téléchargés sur le périphérique pour IEEE 802.1X et HTTPS.

Une fois l'authentification effectuée, le périphérique Axis se déplace vers un réseau de mise en service pour la configuration.

- 1 Commutateur d'accès
- 2 Réseau de mise en oeuvre
- *3 Gestionnaire de politiques ClearPass*
- 4 Application de gestion des périphériques

Intégration sécurisée - IEEE 802.1AR/802.1X

Réseau de production

La mise en service du périphérique Axis avec de nouveaux certificats IEEE 802.1X déclenche une nouvelle tentative d'authentification. ClearPass Policy Manager vérifie les nouveaux certificats et décidera de déplacer ou non le périphérique Axis dans le réseau de production.

Après sa configuration, le périphérique Axis quitte le réseau de mise en service et tente de se réauthentifier sur le réseau.

- 1 Identifiant de périphérique Axis
- 2 Authentification réseau IEEE 802.1x EAP-TLS
- *3 Commutateur d'accès (authentificateur)*
- 4 Gestionnaire de politiques ClearPass

Après la réauthentification, le périphérique Axis est déplacé vers le réseau de production (VLAN 202). Au sein de ce réseau, le système de gestion vidéo (VMS) se connecte au périphérique Axis et commence à fonctionner.

Le périphérique Axis a accès au réseau de production.

- 1 Commutateur d'accès
- 2 Réseau de production
- 3 Gestionnaire de politiques ClearPass
- 4 Système de gestion vidéo

Configuration de HPE Aruba Networking

HPE Aruba Networking ClearPass Policy Manager

ClearPass Policy Manager fournit un contrôle d'accès réseau sécurisé basé sur les rôles et les périphériques pour l'IoT, le BYOD, les périphériques d'entreprise, les employés, les sous-traitants et les invités sur une infrastructure filaire, sans fil et VPN multifournisseur.

Configuration du magasin de certificats de confiance

- 1. Téléchargez la chaîne de certificats IEEE 802.1AR spécifique à Axis depuis axis.com.
- 2. Téléchargez les chaînes de certificats CA racine et CA intermédiaire IEEE 802.1AR spécifiques à Axis dans le magasin de certificats de confiance.
- 3. Activez ClearPass Policy Manager pour authentifier les périphériques Axis via IEEE 802.1X EAP-TLS.
- 4. Sélectionnez EAP dans le champ d'utilisation. Les certificats sont utilisés pour l'authentification IEEE 802.1X EAP-TLS.

Intégration sécurisée - IEEE 802.1AR/802.1X



Chargez des certificats IEEE 802.1AR spécifiques à Axis vers le magasin de certificats de confiance de ClearPass Policy Manager.

O ClearPass Policy Manager - Arub × +					~ -	- o ×					
← → C ▲ Inte säker https://172.25.201.1	120/tips/tips	sContent.action#t	psCertTrustList.action		ie 🛧	□ 🔺 :					
aruba	ClearPass Policy Manager										
Dashboard											
Monitoring • Certificate Trust List											
🔏 Configuration 🔹	This pag	ae displays a list	of trusted Certificate Authorities (CA). You can add, view, or delete a	certificate.							
🐉 Administration 💿											
- DearPass Portal	Filter: S	Subject	✓ contains ✓ axis device	liter	Show	20 v records					
🖃 🚘 Users and Privileges		Subjec	L 🔻	Usage	Validity	Enabled					
E Server Manager	1.	CN=Axi	s device ID Root CA RSA,O=Axis Communications AB	EAP	Valid	Enabled					
	2.	CN=Axi	s device ID Root CA ECC,O=Axis Communications AB	EAP	Valid	Enabled					
	з.	CN=Axi	s device ID Intermediate CA RSA 2,0=Axis Communications AB	EAP	Valid	Enabled					
- Dertificate Store	4.	CN=Axi	s device ID Intermediate CA RSA 1,0=Axis Communications AB	EAP	Valid	Enabled					
- Jan Trust List	5.	CN=Axi	s device ID Intermediate CA ECC 2,0=Axis Communications AB	EAP	Valid	Enabled					
- A Revocation Lists	6.	CN=Axi	s device ID Intermediate CA ECC 1,0=Axis Communications AB	EAP	Valid	Enabled					
Agents and Software Updates	Showing	g 1-6 of 6				Delete					
_ ¶ Support											
© Copyright 2022 Hewlett Packard Enterprise Dev	velopment l	LP	Nov 25, 2022 08:48:50 CET	ClearPass Policy Manager 6.9.1	2.136929 on CLABV (Trial \	ersion) platform					

Magasin de certificats de confiance dans ClearPass Policy Manager avec chaîne de certificats IEEE 802.1AR spécifique à Axis incluse.

Configuration du périphérique/groupe réseau

- Ajoutez des périphériques d'accès réseau fiables, tels que des commutateurs d'accès HPE Aruba Networking, à ClearPass Policy Manager. ClearPass Policy Manager doit connaître les commutateurs d'accès du réseau qui sont utilisés pour la communication IEEE 802.1X.
- 2. Utilisez la configuration du groupe de périphériques réseau pour regrouper plusieurs périphériques d'accès réseau approuvés. Le regroupement des périphériques d'accès réseau de confiance permet une configuration plus facile des politiques.

Intégration sécurisée - IEEE 802.1AR/802.1X

3. Le secret partagé RADIUS doit correspondre à la configuration IEEE 802.1X spécifique du commutateur.

		× – П Х
ClearPass Policy Manager - Arub × +		
← → C ▲ Inte säker https://172.25.201.1	20/tips/tipsContent.action#tipsNetworkDevices.action	🖻 🖈 🔲 😩 🗄
aruba	ClearPass Policy Manager	Menu 🗮
Dashboard 0	Configuration » Network » Devices	
Monitoring 0	Network Devices	\mu Add
🔏 Configuration 💿		Import Export All
☆ Service Templates & Wizards		Discovered Devices
- A Services	A Network Access Device (NAD) must belong to the global list of devices in the ClearPass database in order to connect to ClearPass.	
Authentication Jon Diagonal Di		
Posture	Filter: Name v contains + Go Clear Filter	Show 20 V records
Enforcement	* Name A IP or Subnet Address Device Groups	Description
E + Network		Copy Export Delete
- Devices		
- Proxy Targets		
- DE Event Sources		
- 🛱 Network Scan		
- 🛱 Policy Simulation		
Administration 0		
© Copyright 2022 Hewlett Packard Enterprise Deve	elopment LP Dec 28, 2022 09:01:17 CET ClearPass Policy Manager 6.9.1	2.136929 on CLABV (Trial Version) platform

Interface des périphériques réseau approuvés dans ClearPass Policy Manager.

Q ClearPass Policy Manager - Arub × +		~ - 🗆 X
← → C ▲ Inte säker https://172.25.	.201.120/tips/tipsContent.action#	⋵ ☆ 🛛 😩 :
aruba	ClearPass Policy Manager	Menu 🗮
Dashboard	O Configuration » Network » Devices	
Monitoring	Network Devices	🛖 Add
2 Configuration		Export All
- 🛱 Service Templates & Wizards		Discovered Devices
- Services	A Add Device	
■ Authentication ■ Q Identity	Device SNMP Read Settings SNMP Write Settings CLI Settings OnConnect Enforcement Attributes	Show 20 v records
🗉 🖶 Posture	Name: SW04	Description
Enforcement	IP or Subnet Address: 172.25.200.13	Conv Export Delete
- Devices	(e.g., 192.168.1.10 or 192.168.1.1/24 or 2001:db8:a0b:12f0::1 or 2001:db8:a0b:12f0::1/64)	
- 🛱 Device Groups	Description:	
- Droxy Targets		
- Q Network Scan	RADIUS Shared Secret: Verify:	
- Olicy Simulation	TACACS+ Shared Secret: Verify:	
	Vendor Name: Aruba	
	Enable RADIUS Dynamic Authorization:	
	Add Cancel	
Administration		
© Copyright 2022 Hewlett Packard Enterprise	e Development LP Dec 28, 2022 09:02:18 CET ClearPass Policy Manager	r 6.9.12.136929 on CLABV (Trial Version) platform

Ajoutez le commutateur d'accès HPE Aruba Networking en tant que périphérique réseau approuvé dans ClearPass Policy Manager. Notez que le secret partagé RADIUS doit correspondre à la configuration IEEE 802.1X spécifique du commutateur.

Intégration sécurisée - IEEE 802.1AR/802.1X

Q ClearPass Policy Manager - Arub × +					~ - O X
← → C ▲ Inte säker https://172.25.201	1.120/tips/tipsContent.action#				@ 🛧 🛛 😩 :
aruba		ClearPass Polic	y Manager		Menu 🗮
Dashboard	• Configuration » Network » Devices				
Monitoring	 Network Devices 				🚽 Add
Configuration	•				Export All
- 🛱 Service Templates & Wizards					Discovered Devices
- 🛱 Services			Device SW04 added		
Authentication	A Network Access Device (NAD) mu	st belong to the global list of devices in the	ClearPass database in order to connect to	ClearPass.	
Posture					
Enforcement	Filter: Name 🗸	contains V +	Go Clear Filter		Show 20 🗸 records
	# Name +	IP or Subnet Addres	ss Device Groups	Descriptio	n
- Devices	1. 🗆 SW04	172.25.200.13	-		
- Device Groups	Showing 1-1 of 1				Copy Export Delete
- C Event Sources					
- C Network Scan					
- Q Policy Simulation					
🚑 Administration	•				
© Copyright 2022 Hewlett Packard Enterprise De	evelopment LP	Dec 28, 2022 09:02:33 CET		ClearPass Policy Manager 6.9.12.136929 or	n CLABV (Trial Version) platform

ClearPass Policy Manager avec un périphérique réseau approuvé configuré.

Q ClearPass Policy Manager - Arub: × +		✓ - □ ×
← → C ▲ Inte säker https://172.25.201.1	20/tips/tipsContent.action#tipsNADGroups.action	@ * 🗖 😩 :
aruba	ClearPass Policy Manager	Menu 🗮
Dashboard	Configuration » Network » Device Groups	
Monitoring •	Network Device Groups	Add Simport Export All
- 🗘 Service Templates & Wizards - 🛱 Services	Device Groups function as a component in service and role mapping rules. Device groups can also be associated with enforcement profiles.	
Authentication	Filter: Name 🗸 contains V 🛨 Go Clear Filter	Show 20 🗸 records
B Posture	# Name 🖌 Format Description	
🗉 🔹 Enforcement		Export Delete
Autoidatedate		
Copyright 2022 Hewlett Packard Enterprise Deve	elonment i P Dec 28, 2022 08:57:07 CFT ClearPass Policy f	Manager 6.9.12.136929 on CLABV (Trial Version) platform
Soppringing 2022 newlett Packard Enterprise Deve	eleginarie de	ranager of stratestoors on centry (mail version) platform

Interface des groupes de périphériques réseau approuvés dans ClearPass Policy Manager.

Intégration sécurisée - IEEE 802.1AR/802.1X

Q ClearPass Policy Manager - Arub: × +					✓ - □ ×
← → C ▲ Inte säker https://172.2	5.201.120/tips/tipsContent.action#				🖻 🛧 🗖 😩 :
aruba			ClearPass Policy N	/lanager	Menu 🗮
Dashboard	O Configuration » Netwo	rk » Device Groups			
Monitoring	 Network Device 	Add New Device Grou	p		Add
Configuration	•	Name:	Switches]	👻 Import 🏩 Export A
- 🛱 Service Templates & Wizards	Device Groups function	Description:	Access Switches		nent profiles.
- C subset					
 Authentication Ω Identity 	Filter: Name	Format:	O Subnet		Show 20 v record
🗊 🖶 Posture	# 🗖 Name		Regular Expression		
Enforcement		Available Devices (0)	UIST UST	Selected Devices (1)	Export Delete
- * Network			Filter	Filter	
Device Groups				SW04 [172.25.200.13]	
- 🛱 Proxy Targets					
- Q Event Sources					
- Policy Simulation					
* /					
				Save	
Conversion 2022 Howlett Dackard Enterprise	se Development LP	Do	29, 2022,00:05:29 CET		ClaseDace Balicy Manager 6 0 12 126020 an CLABV (Trial Version) platfo
Copyright 2022 Hewlett Packard Enterpris	se bevelopment LP	De	L 20, 2022 09:05:28 CET		Clear Pass Policy Manager 0.3.12.130323 on CLABY (Inal Version) platto

Ajoutez un périphérique d'accès réseau approuvé à un nouveau groupe de périphériques dans ClearPass Policy Manager.

Q ClearPass Policy Manager - Arub × +		~ - 🗆 X
← → C ▲ Inte säker https://172.25.201.12	0/tips/tipsContentaction#	@☆□≗:
aruba	ClearPass Policy Manager	Menu
Dashboard	Configuration > Network > Device Groups	
Monitoring •	Network Device Groups	Add Import Export All
- 💭 Service Templates & Wizards - 💭 Services - 🖳 Authentication - 🔍 I dentity	Device Groups function as a component in service and role mapping rules. Device groups can also be associated with enforcement profiles.	
Bosture	Filter: Name V contains V E Go Clear Filter	Show 20 🗸 records
Enforcement	Format Description	
 → Retwork → C Devices → C Devices → C Proxy Targets → C Event Sources → R Network Scan → P Policy Simulation 	I. C Switches Showing 1-1 of 1	Export Delete
Convergent 2022 Hewlett Packard Enterprise Dave	Insment I.B. Dec 28, 2022 09:05:43 CET. ClassRass Policy Manager 6, 9, 12, 136929, op C	ABV (Trial Version) platform
Copyright 2022 newlett Packard Enterprise Deve	opinient LP Dec 28, 2022 03:05:43 CE1 ClearPass Policy Manager 6.9.12:136929 00 C	LABY (Inal version) platform

ClearPass Policy Manager avec un groupe de périphériques réseau configuré qui comprend un ou plusieurs périphériques réseau approuvés.

Configuration des empreintes digitales du périphérique

Le périphérique Axis peut distribuer des informations spécifiques au périphérique, telles que l'adresse MAC et la version du logiciel du périphérique, via la découverte réseau. Utilisez ces informations pour créer, mettre à jour ou gérer une empreinte de périphérique dans ClearPass Policy Manager. Vous pouvez également y accorder ou refuser l'accès à partir de la version d'AXIS OS.

- 1. Allez à Administration > Dictionnaires > Empreintes de périphérique.
- 2. Sélectionnez une empreinte de périphérique existante ou créez une nouvelle empreinte de périphérique.

Intégration sécurisée - IEEE 802.1AR/802.1X

												V	_		×
O ClearPass Policy Manager - Arub: × +												Ů		U	^
← → C ▲ Inte säker https://172.25.201.12	20/tips/tips	Content.action#tip	sFinge	rprintDictionary.action								6 1	t D	3 😩	:
aruba		ClearPass Policy Manager											м	enu	
Dashboard O	Adminis	tration » Dictiona	iries »	Device Fingerprints											
Monitoring O	Devic	e Fingerpri	nts								🛖 Add				
🔏 Configuration 🛛 🛛 O											Expo	ort Custo	im Fi	ngerpr	rints
Administration 💿	This pag	ge lists all the dev	vice fir	gerprints recognized by	the Prof	filer module.	These finger	prints are updated fr	om the Softwar	e Updates page.				.go.p.	
- PclearPass Portal			Upd	ate Device Fingerprints					8						
🗄 🔒 Users and Privileges	Filter: F	amily			-							Show	20	✓ rec	cords
III Server Manager III Servers	#	Category	Cate	agory:	Network	k Camera				Name					
- December Servers	1.	Network Can	Fam	ily:	AXIS					AXIS OS version unsupported					
🕢 🔒 Certificates	2.	Network Can	Nan	ne:	AXIS US	5 version uns	upp 💌			AXIS OS version supported					
🔄 🛄 Dictionaries	з.	Network Can	Cust	om Rules- 1	-	Matche	s (ALL)		Delete Rule	Axis Network Camera					
- ARADIUS	4.	Server		Name	0	perator	Value	1.11.10		Axis Print Server					
PTACACS+ Services	Showing	1-4 of 4	1.	Host MAC Vendor	co	ontains_all	AXIS CO	mmunications AB							
- Device Fingerprints			2.	ELDP System Descript	tion no	ot_contains	10.12								
- Dictionary Attributes			5.	Sivier System Descrip	aon ne	contains	10.12								
- Applications															
- Decontext Server Actions															
Windows Hotfixes															
- DonGuard Custom Scripts															
🖅 🌯 Agents and Software Updates															
🗉 🐔 Support			*Not	e: 0 Rule(s) will be dele	ted		Update	Delete Fingerprint	Close						
			-						_						
Convright 2022 Hewlett Packard Enterprise Deve	elonment	P		Nov 25, 201	22 08:50	:09 CFT				ClearPass Policy Manager 6 9 12 136	929 on CLA	BV (Trial	Vere	ion) pla	atform
S septimist rectard Enterprise beve		100		1101 23, 20.						indifficulty indif		and the second		and bio	Contract of the local division of the local

3. Définissez les paramètres d'empreinte du périphérique.

Configuration des empreintes de périphérique dans ClearPass Policy Manager. Les périphériques Axis exécutant une autre version d'AXIS OS autre que 10.12 sont considérés comme non pris en charge.

Q ClearPass Policy Manager - Arub × +								✓ - □ ×
← → C ▲ Inte säker https://172.25.201.12	20/tips/tip:	sContent.action#tip	psFingerprintDictionary.action					🖻 🛧 🔲 😩 :
aruba				Menu 🗮				
Dashboard O	Adminis	stration » Dictiona	aries » Device Fingerprints					
Definition of the second secon	Devid	ce Fingerpri	nts					Add Import Custom Fingerprints Export Custom Fingerprints
Administration U	This pag	ge lists all the de	vice fingerprints recognized	by the Profiler module.	These fingerprints are update	d from the Software	Updates page.	
ClearPass Portal	C'Incore (7		Update Device Fingerprint	5				Show 20 v recorde
🖅 📲 Server Manager	Filter:	Category	Category:	Network Camera	•		Nama	5//0W [20 +] Tecords
External Servers	**	Category	Family:	Axis	-		AVIC OF version unsupported	
- Je External Accounts	2	Network Can	Name:	AXIS OS version sup	pori 🔻		AXIS OS version supported	
Ertificates	3	Network Can	Custom Rules- 1	Matches	5 (ALL)	Delete Rule	Axis Network Camera	
ADIUS	4	Server	Name	Operator	Value		Axis Print Server	
ARADUS	Showing	1 1-4 of 4	Host MAC Vendor LDP System Descri SNMP System Descri "Note: 0 Rule(s) will be de	econtains_all ption contains iption contains	Axis Communications AB 10.12 10.12 Update Delete Fingerp	int Close		
© Copyright 2022 Hewlett Packard Enterprise Deve	lopment	LP	Dec 05, 2	022 09:05:39 CET			ClearPass Policy Manager 6.9.12.136	29 on CLABV (Trial Version) platform

Configuration des empreintes de périphérique dans ClearPass Policy Manager. Les périphériques Axis exécutant AXIS OS 10.12 sont considérés comme pris en charge dans l'exemple ci-dessus.

Les informations sur l'empreinte de périphérique collectées par ClearPass Policy Manager sont disponibles dans la section Points de terminaison.

1. Allez à Configuration > Identité > Points de terminaison.

Intégration sécurisée - IEEE 802.1AR/802.1X

- 2. Sélectionnez le périphérique que vous voulez afficher.
- 3. Cliquez sur l'onglet Empreintes de périphérique.

Remarque

SNMP est désactivé par défaut sur les périphériques Axis et collecté à partir du commutateur d'accès HPE Aruba Networking.

Q ClearPass Policy Manager - Arub × +							~	-		>	<	
← → C ▲ Inte säker https://172.25.201.12	20/tips/tipsConten	t.action#tipsEndpoir	nts.action				Ê	☆		1		
aruba			ClearPass Polic	y Manager					Menu		E	
Dashboard O	Configuration *	Identity » Endpoi	nts									
Monitoring O	Endpoints								Ada	d		
Configuration 📀						-			Exr	port A		
- 🛱 Service Templates & Wizards	This page au	Edit Endpoint				orth with a network to which it is						
- 🗘 Services	connected (e	Endpoint At	tributes Device Fingerprints									
Authentication	O Select AL	chapoint Pr	and the second s	1		-						
Single Sign-On (SSO)	Filter: MAC A	MAC Address	B8-A4-4F-30-42-EA	IP Address	172.25.201.233							
- CLOCAL Users	Filter: MAC A	er: MAC A		Static IP	FALSE							
- 🛱 Endpoints	Filter: MAC A			Hostname	axis-b8a44f3042ea		Sh	ow [2	0 ~	recon	ds	
- 🛱 Static Host Lists	#	Status	Known client Unknown client	Device Category	Avic .	ly Status	Pi	ofile	d			
- Role Mappings	1. C			Device US Pariliy	AXIS OS version support	Unknown	Ye	s				
Posture	2. 🕻			Added At	Doc 28, 2022 14:50:45 CET	Unknown	Ye	s				
🖅 🔹 Enforcement	з. С	MAC vendor	Axis Communications AB	Profiled by	Policy Manager	Unknown	Ye	s				
🖃 📫 Network	4. 🗆	4. C	Added by	Policy Manager	Last Profiled At	Dec 29, 2022 08:18:23 CET	Unknown	Ye	s			
- Q Network Scan	Showing 1-4	Connection Trees	Not Available	Last Homes At	000 207 2022 00110120 021	ger Server Action] Update Fingerprin						
- A Policy Simulation		Connection Type	Unknown									
					Save							
						_						
Administration 0												
Copyright 2022 Hewlett Packard Enterprise Deve	elopment LP		Dec 29, 2022 08:28:03 CET		Clear	Pass Policy Manager 6.9.12.136929 on CLA	BV (Tr	tal Ve	rsion)	platfo	rm	

Un périphérique Axis profilé par ClearPass Policy Manager.

Q ClearPass Policy Manager - Arub × +				~ - 🗆 X
← → C ▲ Inte säker https://172.25.201.1	120/tips/tipsContent.action#tipsEndpoints.action			@ ☆ □ ≗ :
aruba		ClearPass Policy Manager		Menu 🗮
Dashboard Monitoring Monitoring Service Templates & Wizards Gervices Ge	Configuration + Identity > Endpoints Endpoints This page au connected (C) Select AL Filter: MACA Filter: MACA This page au COP Device Description: DCP Device Description: DCP Option50: DHCP Option50: DHCP Option51: Host MAC Vendor: LLDP System Description SIMP Device Name: SIMP Device Type: SIMP System Description	Device Fingerprints Endpoint Fingerprint Details 1,3,6,12,15,28,42,66,119 AXIS,Panoramic Camera,P3727-PLE,10.12.130 53,57,55,12,60,61 Axis Communications AB : AXIS P3727-PLE Panoramic Camera 10.12.130 axis-b8a44f3042ea Host : AXIS P3727-PLE Panoramic Camera 10.12.130	orth with a network to which it is y Status Unknown Unknown Unknown Unknown Unknown Unknown Unknown Unknown Unknown	Add Export All Show 20 records Profiled Ves Ves Ves Ves If Export Delete
© Copyright 2022 Hewlett Packard Enterprise Dev	velopment LP	Dec 29, 2022 08:28:24 CET	ClearPass Policy Manager 6.9.12.136929 on Cl	ABV (Trial Version) platform

Empreintes détaillées d'un périphérique Axis profilé. Veuillez noter que SNMP est désactivé par défaut sur les périphériques Axis. Les informations de découverte spécifiques à LLDP, CDP et DHCP sont partagées par le périphérique Axis dans leur état d'usine par défaut et relayées par le commutateur d'accès HPE Aruba Networking vers ClearPass Policy Manager.

Intégration sécurisée - IEEE 802.1AR/802.1X

Configuration du profil d'application

Le profil d'application est utilisé pour permettre à Aruba ClearPass Policy Manager d'attribuer un ID VLAN spécifique à un port d'accès sur le commutateur. Il s'agit d'une décision basée sur des politiques qui s'applique aux périphériques réseau du groupe de périphériques « commutateurs ». Le nombre de profils d'application nécessaire dépend du nombre de réseaux VLAN. Dans notre configuration, il existe un total de trois réseaux VLAN (VLAN 201, 202, 203), qui correspondent à trois profils d'application.

Une fois les profils d'application configurés pour le réseau VLAN, la stratégie d'application réelle peut être configurée. La configuration de la politique d'application dans ClearPass Policy Manager définit si les périphériques Axis ont accès aux réseaux HPE Aruba Networking sur la base de quatre exemples de profils de politique.

ClearPass Policy Manager - Arub × +								~	-	• ×
← → C ▲ Inte säker https://172.25.201.1	20/tips,	/tipsContent.action#tip	sEditEnforcementProfile.action%3	contextData%3D3004				e t	7	± =
ontho			Cla	anDass Doliev Manag	on				Me	
aloba									. He	
Dashboard O	Conf	figuration » Enforcem	ent » Profiles » Edit Enforceme	nt Profile - Allow_VLAN_201						
Monitoring O	Enf	forcement Pro	files - Allow_VLAN_20	01						
🖧 Configuration 📀	Su	immary Profile	Attributes							
Gervice Templates & Wizards	Prof	file:								
Authentication	Nam	ie:	Allow_VLAN_201							
Identity	Desc	cription:								
🗉 📅 Posture	Туре	200	RADIUS							
Enforcement	Actio	on:	Accept							
- Policies	Devi	ice Group List:	1. Switches							
Network	Attributes:									
- 🛱 Network Scan		Туре		Name			Value			
- 🛱 Policy Simulation	1.	Radius:IETF		Session-Timeout		=	10800			
	2.	Radius:IETF		Termination-Action		=	RADIUS-Request (1)			
	з.	Radius:IETF		Tunnel-Type		=	VLAN (13)			
	4.	Radius:IETF		Tunnel-Medium-Type		=	IEEE-802 (6)			
	5.	Radius:IETF		Tunnel-Private-Group-Id		=	201			
	<	Rack to Enforcement	it Profiles				Con	v Sa	ve	Cancel
🚰 Administration 🛛 🛛 🛛		outer to Enforcement	it i formes				cop	50		Curroot
© Copyright 2022 Hewlett Packard Enterprise Dev	elopme	ent LP	Dec 28, 2022	09:08:57 CET			ClearPass Policy Manager 6.9.12.136929 on CL	BV (Trial	Versio	on) platform

Exemple de profil d'application pour autoriser l'accès au réseau VLAN 201.

Intégration sécurisée - IEEE 802.1AR/802.1X

.25.201.120/tips/tipsContent.action#	tipsEditEnforcementPolicy.action%3FcontextData%3D3007		🖻 🖈 🔲 😩 :	
	ClearPass Policy Manager			
• Configuration » Enforce	ement » Policies » Edit - Axis Radius policy			
 Enforcement Po 	licies - Axis Radius policy			
Summary Enforce	ment Rules			
Enforcement:				
Name:	Axis Radius policy			
Description:				
Enforcement Type:	RADIUS			
Default Profile:	Allow_VLAN_203			
Rules:				
Rules Evaluation Algori	thm: First applicable			
Conditions		Actions		
(Certificate:Issuer- AND (Certificate AND (Certificate AND (Certificate AND (Certificate AND (Certificate AND (Certificate	CH_CONTAINS Asis device ID Intermediate CA) ::subject-O_EQUALS Asis Communications AB) ::subject-O_EQUALS Asis Communications AB) ::subject-O_EQUALS Lund) ::Subject-C_EQUALS Subject-serialNumber))	Allow_VLAN_201		
2. AND (Certificate: Issuer- 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 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}) ion:Endpoints Repository:Device Name EQUALS AXIS OS version supported)	Allow_VLAN_202		
Sack to Enforcem	ent Policies		Copy Save Cancel	
	23:201.120/tips/tipsContent.action# Configuration * Enforce Enforcement Pro Summary Enforce Enforcement: Name: Default profile: Rules: Rules: Rules: Confilions (Certificate:Issuer AVD (Certificate:Issuer AVD (Certificate) AVD (Certi	22 201.120/tips/tipsContent.action#tipsEditEnforcementPolicy.action%34ContextData%3D307 Configuration * Enforcement * Policies * Edit - Axis Radius policy Configuration * Enforcement * Policies * Edit - Axis Radius policy Summary Enforcement Rules Enforcement Policies - Axis Radius policy Summary Enforcement Rules Enforcement Type: Axis Radius policy Default Profile: Allow_VLAN_203 Rules Rules Evaluation Algorithm: First applicable Confitions (Certificate:Issuer-Ch ConfYAINS Axis device 1D Intermediate CA) Arg (Certificate:Issuer-Ch ConfYAINS Production CA Certificate: Confitions (Certificate:Issuer-Ch ConfYAINS Production CA Certificate: Confitiane: Confitiane: Subject-Ch CONFAINS %(Connection:Client-Hake-Address-NoDelim)) Arg (Certificate:Subject-Ch CONFAINS %(Connection:Client-Hake-Address-NoDeli	22 201.120/tips/tips/Content.action#Ups/Stift.fntoreementPolicy.action%SF contextData%3D3007 Configuration = Enforcement = Policies = Edit - Axis Radius policy Enforcement Policies - Axis Radius policy Enforcement Name: Axis Radius policy Enforcement Name: Axis Radius policy Enforcement Name: Axis Radius policy Default Profile: Axis Radius Policy Defau	

Configuration de la politique d'application dans ClearPass Policy Manager.

Les quatre politiques d'application et leurs actions sont répertoriées ci-dessous :

Accès au réseau refusé

L'accès au réseau est refusé lorsqu'aucune authentification de contrôle d'accès au réseau IEEE 802.1X n'est effectuée.

Réseau invité (VLAN 203)

Le périphérique Axis a accès à un réseau limité et isolé si l'authentification du contrôle d'accès au réseau IEEE 802.1X échoue. Une inspection manuelle du périphérique est nécessaire pour prendre les mesures appropriées.

Réseau de mise en oeuvre (VLAN 201)

Le périphérique Axis a accès à un réseau de mise en service. Celui-ci permet de fournir des capacités de gestion des périphériques Axis via AXIS Device Manager et AXIS Device Manager Extend. Il permet également de configurer les périphériques Axis avec des mises à jour d'AXIS OS, des certificats de niveau production et d'autres configurations. Les conditions suivantes sont vérifiées par ClearPass Policy Manager :

- Version d'AXIS OS du périphérique Axis.
- L'adresse MAC du périphérique correspond au schéma d'adresse MAC Axis spécifique au fournisseur avec l'attribut de numéro de série du certificat d'identification du périphérique Axis.
- Le certificat d'ID de périphériques Axis est vérifiable et correspond aux attributs spécifiques à Axis tels que l'émetteur, l'organisation, l'emplacement et le pays.

Réseau de production (VLAN 202)

Le périphérique Axis peut accéder au réseau de production où le périphérique Axis doit fonctionner. L'accès est autorisé après la fin de la mise en service des périphériques au sein du réseau de mise en service (VLAN 201). Les conditions suivantes sont vérifiées par ClearPass Policy Manager :

- L'adresse MAC du périphérique correspond au schéma d'adresse MAC Axis spécifique au fournisseur avec l'attribut de numéro de série du certificat d'identification du périphérique Axis.
- Version d'AXIS OS du périphérique Axis.

Intégration sécurisée - IEEE 802.1AR/802.1X

• Le certificat de niveau production est vérifiable par le magasin de certificats de confiance.

Configuration de la méthode d'authentification

Dans la méthode d'authentification est définie la manière dont un périphérique Axis tente de s'authentifier sur le réseau. La méthode d'authentification préférée doit être IEEE 802.1X EAP-TLS, car les périphériques Axis prenant en charge Axis Edge Vault sont livrés avec IEEE 802.1X EAP-TLS activé par défaut.

Q ClearPass Policy Manager - Arub × +							∨ - □ X
← → C ▲ Inte säker https://172.25.201.1	120/tips/tip	sConter	it.action#tipsAuthMet	hods.action			
aruba		ClearPass Policy Manager					Menu 🗮
Dashboard O	Configu	Configuration » Authentication » Methods					
Monitoring 0	Auth	entic	ation Method	5			🐥 Add
Seconfiguration	>	Authentication Methods					A Import
- 🗘 Service Templates & Wizards - 🛟 Services	As a fir.	st step	in the service-base	Edit Authentication Method		• r device against an authentication source.	Export Air
Authentication	Filter:	Name		General			Show 20 🗸 records
- in Sources	#		Name 🔺	Name: A	xis EAP TLS	Description	
🗈 🧕 Identity	1.		[Allow All MAC AL	Description: De	fault settings for EAP-TLS	Default settings for Allow All MAC-AUTH	
🕞 📅 Posture	2.		[Aruba EAP GTC]			EAP-GTC method to use with Aruba EAP-GTC plugin for Wi	ndows
E S Enforcement	3.		[Authorize]	7		Default settings for Authorize	
Network	4.		Axis EAP TLS	Type: EA	AP-ILS	Default settings for EAP-TLS	
- Dolicy Simulation	5.		[CHAP]		Method Details	Default settings for CHAP	
Wroney Similation	6.		[EAP FAST]	Session Resumption:	🗹 Enable	Default settings for EAP-FAST	
	7.		[EAP GTC]	Session Timeout:	6 hours	Default settings for EAP-GTC	
	8.		[EAP MD5]	Authorization Required:	Enable	Default settings for EAP-MD5	
	9.		[EAP MSCHAPv2]	Certificate Comparison:	Do not compare 🗸	Default settings for EAP-MSCHAPv2	
	10.		[EAP PEAP]	Verify Certificate using OCSP:	None 🗸	Default settings for EAP-PEAP	
	11.		[EAP PEAP Public]	Override OCSP URL from Clien	t: 🗆 Enable	Default settings for EAP-PEAP-Public	
	12.		[EAP PEAP Without	OCSP URL:		EAP-PEAP with Fast Reconnect disabled; recommended for	Onboard
	13.		[EAP PWD]			Default settings for EAP-PWD	
	14.		[EAP TLS]		Conv Save Canc	Default settings for EAP-TLS	
	15.		[EAP TLS With OC			EAP-TLS with OCSP enabled; recommended for Onboard	
	16.		[EAP TTLS]		EAP-TTLS	Default settings for EAP-TTLS	
	17.		[MAC AUTH]		MAC-AUTH	Default settings for MAC-AUTH	
	18.		[MSCHAP]		MSCHAP	Default settings for MSCHAP	
	19.		[PAP]		PAP	Default settings for PAP	
© Copyright 2022 Hewlett Packard Enterprise Dev	20. velopment	LP	[SSO]	Dec 28, 2022 09:43:30	PAP	Default settings for SSO ClearPass Policy Manager 6.9.12.136929 on CLA	• IBV (Trial Version) platform

Interface de méthode d'authentification de ClearPass Policy Manager où est définie la méthode d'authentification EAP-TLS pour les périphériques Axis.

Configuration du service

Dans la page **Services** page, les étapes de configuration sont regroupées dans un seul service qui gère l'authentification et l'autorisation des périphériques Axis au sein des réseaux HPE Aruba Networking.

Intégration sécurisée - IEEE 802.1AR/802.1X

Q ClearPass Policy Manager - Arub × +				~ _	U ^		
← → C ▲ Inte säker https://172.2	25.201.120/tips/tipsContent.acti	on#tipsEditService.action%3FcontextData%3D3001		lê ☆			
aruba		ClearPass Policy Manager					
Dashboard	• Configuration » Ser	vices » Edit - Axis 802.1X Wired					
Monitoring	 Services - Ax 	is 802.1X Wired					
Configuration	O Summary Ser	vice Authentication Roles Enforcement					
🗘 Service Templates & Wizards	Name:	Axis 802.1X Wired					
- Gr Services - 🔓 Authentication - 🖵 Identity	Description:	To authenticate users to any wired network via 802.1X.					
Posture	Type:	802.1X Wired					
- S Enforcement	Status:	Enabled					
Network Scan	Monitor Mode:	Monitor Mode: Enable to monitor network access without enforcement					
2 Policy Simulation	More Options:	More Options: Authorization Desture Compliance Audit End-hosts Derofile Endpoints Accounting Proxy					
			Service Rule				
	Matches O ANY or	• ALL of the following conditions:					
	Туре	Name	Operator	Value			
	Radius:IETF Radius:IETF	NAS-Port-Type Service-Type	EQUALS BELONGS_TO	Ethernet (15) Login-User (1), Framed-User (2),	89 T 89 T		
	3. Click to add.			Autoenticate-Only (8)			
Administration	Back to Servic	es		Disable Copy Save	Cancel		

Un service Axis dédié est créé et définit IEEE 802.1X comme méthode de connexion.

O ClearPass Policy Manager - Arub × +				✓ - □ ×
← → C ▲ Inte säker https://172.25.201.	120/tips/tipsContent.action#tips	EditService.action%3FcontextData%3D3001		🖻 🛧 🔲 😩 :
aruba		ClearPass	Policy Manager	Menu 🗮
Dashboard	Configuration » Services »	Edit - Axis 802.1X Wired		
Monitoring	Services - Axis 80	2.1X Wired		
Configuration	Summary Service	Authentication Roles Enforcement		
	Authentication Methods:	Axis EAP TLS	Move Up : Move Down _ Remove View Datails Modify	Add New Authentication Method
	Authentication Sources:	[Endpoints Repository] [Local SOL DB]	Move Up 1 Move Down 1 Remove View Details Modify	Add New Authentication Source
	Strip Username Rules:	Enable to specify a comma-separated I	list of rules to strip username prefixes or suffixes	
	Service Certificate:	Select to Add		View Certificate Details
Administration (Back to Services			Disable Copy Save Cancel
© Copyright 2022 Hewlett Packard Enterprise De	velopment LP	Dec 28, 2022 09:41:41 C	ET	ClearPass Policy Manager 6.9.12.136929 on CLABV (Trial Version) platform

À l'étape suivante, la méthode d'authentification EAP-TLS créée précédemment est configurée pour le service.

Intégration sécurisée - IEEE 802.1AR/802.1X

ClearPass Policy Manager - Arub 🗙 🕂			× -	o x				
← → C ▲ Inte säker https://172.25	5.201.120/tips/tipsContent.action#tip	sEditService.action%3FcontextData%3D3001	년 ★ [I 🔺 :				
aruba		ClearPass Policy Manager	м	4enu 🔳				
Dashboard	 Configuration » Services Services - Axis 8 	» Edit - Axis 802.1X Wired 02.1X Wired						
Configuration	Summary Service	Authentication Roles Enforcement						
- C Service lemplates & Wizards	Use Cached Results:	Use cached Roles and Posture attributes from previous sessions						
Authentication	Enforcement Policy:	Axis Radius policy Modify	Add New Enforce	ement Policy				
Q Identity Protuce		Enforcement Policy Det	ails					
B Sture Sture	Description:							
-+- Network	Default Profile:	Allow_VLAN_203						
- 🛱 Network Scan	Rules Evaluation Algorithm: first-applicable							
- A roney annusuon	Conditions (Certificate:Issue AND (Certificate:Issue AND (Certificate:Issue AND (Certificate:Issue (Certificate:Issue AND (Certificate:Issue AND (Certificate:Is	In-CN CONTAINS Axis device ID Intermediate CA) tes:Subject-C EQUALS Axis Communications AB) tes:Subject-E EQUALS Land) tes:Subject-E EQUALS Section EQUALS %(Certificate:Subject-serialNumber)) in:CN CONTAINS Production CA Certificate) tes:Subject-C ICONTAINS %(Connection:Client-Mac-Address-NoDelim)) ation:Endpoints Repaitory):Device Name EQUALS AXIS OS version unsupported) tes:Subject-C IC CONTAINS %(Connection:Client-Mac-Address-NoDelim)) ation:Endpoints Repaitory):Device Name EQUALS AXIS OS version supported) tes:Subject-C IC CONTAINS %(Connection:Client-Mac-Address-NoDelim)) ation:Endpoints Repository):Device Name EQUALS AXIS OS version supported)	Enforcement Profiles Allow_VLAN_201 Allow_VLAN_201 Allow_VLAN_202 Disable Corr Serve	Cancel				
🐉 Administration	Back to Services		Disable Copy Save	Cancel				
© Copyright 2022 Hewlett Packard Enterprise	e Development LP	Dec 28, 2022 09:51:01 CET	ClearPass Policy Manager 6.9.12.136929 on CLABV (Trial Vers	sion) platform				

À la dernière étape, la stratégie d'application créée précédemment est configurée sur le service.

Commutateur d'accès HPE Aruba Networking

Les périphériques Axis sont directement connectés à des commutateurs d'accès compatibles PoE, ou via des médiateurs Axis PoE compatibles. Pour intégrer en toute sécurité les périphérique Axis au sein des réseaux HPE Aruba Networking, le commutateur d'accès doit être configuré pour la communication IEEE 802.1X. Le périphérique Axis relaie la communication IEEE 802.1x EAP-TLS vers ClearPass Policy Manager qui fait office de serveur RADIUS.

Remarque

Une réauthentification périodique de 300 secondes pour le périphérique Axis est également configurée pour renforcer la sécurité globale de l'accès aux ports.

Consultez ci-dessous un exemple de configuration globale et de port pour les commutateurs d'accès HPE Aruba Networking.

```
hôte du serveur radius Clé MyRADIUSIPAddress « 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

Périphérique réseau Axis

Les périphériques Axis avec prise en charge Axis Edge Vault sont fabriqués avec une identité de périphérique sécurisée, appelée ID de périphérique Axis. L'ID périphérique Axis repose sur la norme internationale IEEE 802.1AR, qui définit une méthode d'identification automatisée et sécurisée des périphériques et d'intégration au réseau via IEEE 802.1X.

Intégration sécurisée - IEEE 802.1AR/802.1X



Les périphériques Axis sont fabriqués avec le certificat d'ID de périphérique Axis conforme à la norme IEEE 802.1AR pour les services d'identité de périphérique fiables.

- 1 Infrastructure de clé d'ID de périphérique Axis (PKI)
- 2 ID de périphérique Axis

Le magasin de clés sécurisé protégé par matériel et fourni par un élément sécurisé du périphérique Axis est mis en service en usine avec un certificat unique au périphérique et des clés correspondantes (ID de périphérique Axis) qui peuvent globalement prouver l'authenticité du périphérique Axis. Le *sélecteur de produits Axis* peut être utilisé pour déterminer les périphériques Axis qui prennent en charge Axis Edge Vault et l'ID de périphérique Axis.

Remarque

Le numéro de série d'un périphérique Axis est son adresse MAC.

		AXIS Q1656 Box Camera	Ø 🐺 🛈 🖪 🗄
🔂 Status			
□ Video	~	Certificates	
PTZ		+ Add certificate	<u>न्द</u> 🔻
🛓 Audio	~		
Recordings		Name Type	
🗩 Apps		Axis device ID ECC-P256 (802.1AR) Client-server	
緣 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	

Magasin de certificats du périphérique Axis à l'état d'usine par défaut avec un ID de périphérique Axis.

Le certificat d'ID de périphérique Axis, conforme à la norme IEEE 802.1AR, comprend des informations sur le numéro de série et d'autres informations spécifiques au fournisseur Axis. Les informations sont utilisées par ClearPass Policy Manager à des fins d'analyse et de prise de décision pour accorder l'accès au réseau. Consultez les informations ci-dessous qui peuvent être obtenues à partir d'un certificat d'ID de périphérique Axis.

IDevID						
"C": "SE",	"C": "SE",					
"L": "Lund",	"L": "Lund",					
"O": "Axis Communications A	"O": "Axis Communications AB",					
"CN": "axis-b8a44f279511-ec	"CN": "axis-b8a44f279511-eccp256-1",					
"serialNumber": "b8a44f2795	"serialNumber": "b8a44f279511",					

Intégration sécurisée - IEEE 802.1AR/802.1X

Pays	SE	
Localisation	Lund	
Organisation émettrice	Axis Communications AB	
Nom commun de l'émetteur	Intermédiaire de l'ID de périphérique Axis	
Organisation	Axis Communications AB	
Nom commun	axis-b8a44f279511-eccp256-1	
Numéro de série	b8a44f279511	

Le nom commun est créé en combinant le nom de l'entreprise Axis, le numéro de série du périphérique suivi de l'algorithme de chiffrement (ECC P256, RSA 2048, RSA 4096) utilisé. À compter d'AXIS OS 10.1 (2020-09), IEEE 802.1X est activé par défaut avec l'ID de périphérique Axis préconfiguré. Cela permet au périphérique Axis de s'authentifier sur les réseaux compatibles IEEE 802.1X.

		AXIS Q1656 Box Camera	@ 🐺 🛈 🖪 :
🖂 Status		IEEE 802.1x Connecting	
□ Video	\sim	Client certificate	
PTZ		Axis device ID RSA-2048 (802.1AR)	
🛓 Audio	\sim	CA certificates ()	
Recordings		No CA certificate selected	
📽 Apps		■ Use IEEE 802.1x	
🕸 System	^	axis-b8a44f27a03a	
Date and time			
Network			
Security			Save

Périphérique Axis à son état d'usine par défaut avec IEEE 802.1X activé et un certificat d'ID de périphérique Axis présélectionné.

AXIS Device Manager

AXIS Device Manager and AXIS Device Manager Extend peut être utilisé sur le réseau pour configurer et gérer plusieurs périphériques Axis de manière économique. AXIS Device Manager est une application basée sur Microsoft Windows® qui peut être installée localement sur une machine du réseau, tandis qu'AXIS Device Manager Extend s'appuie sur l'infrastructure cloud pour gérer les périphériques multi-sites. Les deux offrent des fonctionnalités de gestion et de configuration simples pour les périphériques Axis tels que :

- Installation des mises à jour d'AXIS OS.
- Appliquez une configuration de cybersécurité, comme des certificats HTTPS et IEEE 802.1X.
- Configuration des paramètres spécifiques aux périphériques, comme des paramètres d'images et autres.

Fonctionnement réseau sécurisé - IEEE 802.1AE MACsec

Fonctionnement réseau sécurisé - IEEE 802.1AE MACsec



IEEE 802.1AE MACsec (Media Access Control Security) est un protocole réseau bien défini qui sécurise cryptographiquement les liaisons Ethernet point à point sur la couche réseau 2. Il garantit la confidentialité et l'intégrité des transmissions de données entre deux hôtes.

La norme IEEE 802.1AE MACsec décrit deux modes de fonctionnement :

- Mode clé pré-partagée/CAK statique configurable manuellement
- Mode session maître automatique/CAK dynamique utilisant IEEE 802.1X EAP-TLS



Dans AXIS OS 10.1 (2020-09) et versions ultérieures, IEEE 802.1X est activé par défaut pour les périphériques compatibles avec l'ID de périphérique Axis. Dans AXIS OS 11.8 et versions ultérieures, nous prenons en charge MACsec avec le mode dynamique automatique utilisant IEEE 802.1X EAP-TLS activé par défaut. Lorsque vous connectez un périphérique Axis avec les paramètres d'usine par défaut, une authentification réseau IEEE 802.1X est effectuée et en cas de succès, le mode MACsec Dynamic CAK est également tenté.

L'ID de périphérique Axis stocké de manière sécurisée (1), identité de périphérique sécurisée conforme IEEE 802.1AR, est utilisé pour l'authentification auprès du réseau (4, 5) via le contrôle d'accès au réseau basé sur le port EAP-TLS IEEE 802.1X (2). Lors de la session

Fonctionnement réseau sécurisé - IEEE 802.1AE MACsec

EAP-TLS, les clés MACsec sont échangées automatiquement pour établir un lien sécurisé (3), protégeant tout le trafic réseau depuis le périphérique Axis vers le commutateur d'accès HPE Aruba Networking.

IEEE 802.1AE MACsec requiert à la fois un commutateur d'accès HPE Aruba Networking et des préparations de configuration ClearPass Policy Manager. Aucune configuration n'est requise sur le périphérique Axis pour permettre une communication chiffrée MACsec IEEE 802.1AE via EAP-TLS.

Si le commutateur d'accès HPE Aruba Networking ne prend pas en charge MACsec à l'aide d'EAP-TLS, le mode Clé pré-partagée peut être utilisé et configuré manuellement.

HPE Aruba Networking ClearPass Policy Manager

Politique de rôle et de mappage de rôles



Ajoutez un nom de rôle pour les périphériques Axis. Le nom est le nom du rôle d'accès au port dans la configuration du commutateur d'accès.

Fonctionnement réseau sécurisé - IEEE 802.1AE MACsec

Q app20 × +		✓ - □ X
← → C ▲ Inte säker https://172.25.20	01.120/tips/tipsContent.action#tipsEditRoleMappingPolicy.action%3FcontextData%3D3001	년 🛧 🛛 😩 :
aruba	ClearPass Policy Manager	Menu 🗮
Dashboard 0	Configuration » Identity » Role Mappings » Edit - Axis Role Mapping	
Monitoring O	Role Mappings - Axis Role Mapping	
🔏 Configuration 💿	Summary Policy Mapping Rules	
- 🛱 Service Templates & Wizards	Policy:	
🖃 🚘 Authentication	Policy Name: Axis Role Mapping	
- 🗘 Methods	Description:	
- C Sources	Default Role: [Guest]	
E Gingle Size-On (SSO)	Mapping Rules:	
- it local Users	Rules Evaluation Algorithm: Evaluate all	
- 🛱 Endpoints	Conditions	Role Name
- 🛱 Static Host Lists	1. (Authentication:Full-Username BEGINS WITH axis-00408c)	AxisDevice
- 🛱 Roles	2. (Authentication:Full-Username BEGINS WITH axis-accc8e)	AxisDevice
- Role Mappings	3. (Authentication:Full-Username BEGINS_WITH axis-b8a44f)	AxisDevice
Administration 0	K Back to Role Mappings	Copy Save Cancel
© Copyright 2023 Hewlett Packard Enterprise I	Development LP Oct 26, 2023 05:08:20 UTC	ClearPass Policy Manager 6.11.2.252294 on CLABV (Trial Version) platform

Ajoutez une stratégie de mappage de rôle Axis pour le rôle de périphérique Axis créé précédemment. Les conditions définies sont nécessaire pour permettre le mappage d'un périphérique au rôle de périphérique Axis. Si les conditions ne sont pas remplies, le périphérique fait partie du rôle [Invité].

Par défaut, les périphériques Axis utilisent le format d'identité EAP « axis-serialnumber ». Le numéro de série d'un périphérique Axis est son adresse MAC. Par exemple « axis-b8a44f45b4e6".

Fonctionnement réseau sécurisé - IEEE 802.1AE MACsec

Configuration du service



Ajoutez la stratégie de mappage de rôle Axis créée précédemment au service qui définit IEEE 802.1X comme méthode de connexion pour l'intégration des périphériques Axis.

Fonctionnement réseau sécurisé - IEEE 802.1AE MACsec

Q app20 × +			v – 🗆 X
← → C ▲ Inte säker https://172	2.25.201.120/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 Boles Enforcement	
	Use Cached Results:	Use cached Roles and Posture attributes from previous sessions	
	Enforcement Policy:	Axis Radius policy V Modify	Add New Enforcement Policy
- 🛱 Methods		Enforcement Poli	cy Details
- Ö Identifu	Description:		
Single Sign-On (SSO)	Default Profile:	Allow VLAN 203	
- Q Local Users	Rules Evaluation Algorith	m: evaluate-all	
- 🛱 Endpoints	Conditions		Enforcement Brofiler
	AND (Certificat AND (Certificat AND (Conect serialNumber}) AND (Tips:Role (Certificate:Issue AND (Authoriz: unsupported) AND (Certificat	es:Subject-O EQUALS Axis Communications AB) on:Client-Mac-Address-NoDelim EQUALS %{Certificate:Subject- e EQUALS AxisDevice) n-CN CONTAINS Production CA) ation:[Endpoints Repository]:Device Name EQUALS AXIS OS version es:Subject-CN CONTAINS Production XYZ)	Allow_VLAN_201 Allow_VLAN_201
- ⇔ Profiles • ♣ Network - ♀ Devices - ♀ Device Groups - ♀ Proxy Targets	AND (Tips:Role (Certificate:Issue AND (Authoriz: 3. supported) AND (Certificat AND (Tips:Role	EQUALS AxisDevice) r-CN CONTAINS Production CA) tion;Endpoints Repository]:Device Name EQUALS AXIS OS version te:Subject-CN CONTAINS Production XYZ) te EQUALS AxisDevice)	Allow_VLAN_202
A Leven Soutles - ☆ Network Scan - ☆ Policy Simulation	Back to Services		Disable Copy Save Cancel
🚑 Administration	0		
© Copyright 2023 Hewlett Packard Enterp	rise Development LP	Oct 26, 2023 05:11:50 UTC	ClearPass Policy Manager 6.11.2.252294 on CLABV (Trial Version) platform

Ajoutez le nom du rôle Axis comme condition aux définitions de stratégie existantes.

Fonctionnement réseau sécurisé - IEEE 802.1AE MACsec

Profil d'application

Q app20 × +				~ - • ×				
	.201.120/tips/tipscontent.actic	Menu						
E	Configuration » Enforcement » Profiles » Edit Enforcement Profile - Allow, VLAN, 201							
Monitoring	 Enforcement Pr 	Enforcement Profiles - Allow VLAN 201						
Sconfiguration	Summary Profile	Attributes						
- 🛱 Service Templates & Wizards	Profile:	Rendered						
- Authentication	Name:	Allow_VLAN_201						
- 🛱 Methods	Description:							
- 🛱 Sources	Type:	RADIUS						
🖃 🚨 Identity	Action:	Accept						
_ Single Sign-On (SSO)	Device Group List:	1. Switches						
- Cocal Users	Attributes							
- 🛱 Static Host Lists	Attributes.		Malaa					
Roles	Type	Name Carrier Timoret	Value					
- 🛱 Role Mappings	I. Radius:IETF	Session-Timeout	= 10800					
🖃 📅 Posture	2. Radius:IETF	Termination-Action	= RADIOS-Request (1)					
- 🛱 Posture Policies	3. Radius:IETF	lunnel-lype	= VLAN (13)					
- Q Audit Servers	4. Radius:IETF	Tunnel-Medium-Type	= IEEE-802 (6)					
- Gragentiess OnGuard	5. Radius:IETF	Tunnel-Private-Group-Id	= 201					
- Dicies	6. Radius:Aruba	Aruba-User-Role	= AxisDevice					
Network								
- 💭 Devices								
- 🛱 Device Groups								
- 🛱 Proxy Targets								
- 🛱 Event Sources								
- Q Network Scan								
- Jus Policy Simulation								
Administration	Back to Enforcem	ent Profiles		Copy Save Cancel				
Convicts 2022 United Designed Enternain	a Davalanmant I D	Oct 26, 2022 05:12:21 UTC	ClasePass Policy Manager 6 11 2 253	204 on CLARY (Trial Version) platform				

Ajoutez le nom de rôle Axis en tant qu'attribut aux profils d'application affectés dans le service d'intégration IEEE 802.1X.

Commutateur d'accès HPE Aruba Networking

En plus de la configuration d'intégration sécurisée décrite dans , reportez-vous à l'exemple de configuration de port ci-dessous pour le commutateur d'accès HPE Aruba Networking afin de configurer 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
```

Intégration héritée – Authentification MAC

Intégration héritée – Authentification MAC

Vous pouvez utiliser MAC Authentication Bypass (MAB) pour intégrer des périphériques Axis qui ne prennent pas en charge l'intégration d'IEEE 802.1AR avec le certificat d'ID de périphérique Axis et IEEE 802.1X activé à l'état d'usine par défaut. Si l'intégration 802.1X échoue, ClearPass Policy Manager valide l'adresse MAC du périphérique Axis et accorde l'accès au réseau.

MAB requiert à la fois un commutateur d'accès et des préparations de configuration ClearPass Policy Manager. Sur le périphérique Axis, aucune configuration n'est requise pour permettre l'intégration de MAB.

HPE Aruba Networking ClearPass Policy Manager

Politique d'application

La configuration de la politique d'application dans ClearPass Policy Manager définit si les périphériques Axis ont accès aux réseaux HPE Aruba Networking sur la base des deux exemples de conditions de politique ci-après.

Q app20 × +			✓ - □ X
← → C ▲ Inte säker https://172.25.2	01.120/tips/tipsContent.action	#tipsEditService.action%3FcontextData%3D3006	년 🖈 🛛 😩 :
aruba		Menu 🗮	
Dashboard	Configuration » Services	» Edit - Axis 802.1X Wired - Mac Authentication	
Monitoring G	Services - Axis 8	302.1X Wired - Mac Authentication	
Configuration C	Summary Service	Authentication Roles Enforcement	
Gervice Templates & Wizards Gervices Gervic	Use Cached Results: Enforcement Policy: Description: Default Profile: Rules Evaluation Algorith Conditions (Date:Day-of-We 1. AND (Date:Tin AND (Connecti	Use cached Roles and Posture attributes from previous sessions Axis MAC Authentication Policy Inforcement P Deny Access Profile] (Deny Access Profile] (Den	Add New Enforcement Policy olicy Details Enforcement Profiles Allow_VLAN_203
→ 🗘 Network Scan → 🗘 Policy Simulation	Back to Services		Enable Copy Save Cancel
Administration 0			
Copyright 2023 Hewlett Packard Enterprise	Development LP	Oct 26, 2023 05:15:57 UTC	ClearPass Policy Manager 6.11.2.252294 on CLABV (Trial Version) platform

Accès au réseau refusé

Lorsque le périphérique Axis ne respecte pas la stratégie d'application configurée, l'accès au réseau lui est refusé.

Réseau invité (VLAN 203)

Le périphérique Axis a accès à un réseau limité et isolé si les conditions suivantes sont remplies :

- C'est un jour de semaine entre lundi et vendredi
- Il est entre 9h00 et 17h00

Intégration héritée – Authentification MAC

• Le fournisseur d'adresse MAC correspond à Axis Communications.

Étant donné que les adresses MAC peuvent être usurpées, l'accès au réseau de mise en service habituel n'est pas accordé. Nous vous recommandons d'utiliser MAB uniquement pour l'intégration initiale et d'inspecter manuellement le périphérique plus en détail.

Configuration source

Dans la page Sources, une nouvelle source d'authentification est créée pour autoriser uniquement les adresses MAC importées manuellement.



Intégration héritée – Authentification MAC

Q app20 × +			✓ - □ ×
← → C ▲ Inte säker https://172.2	25.201.120/tips/tipsContent.action#	tipsAddAuthSource.action	년 🖈 🛛 🏝 :
aruba		ClearPass Policy Manager	Menu 🗮
Dashboard	• Configuration » Authentic	ation » Sources » Add	
Monitoring	 Authentication Set 	ources	
Configuration	General Static Host	Lists Summary	
- 🛱 Service Templates & Wizards	Name:	Axis Devices	
- O Services	Description:	MAC addresses of Axis devices in use.	
- C 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 attribu-	utes
- Coal Users - Cale Endpoints - Cale Coale Coale - Cale Coale Cale Cale Cale Cale Cale Cale Cale C	Authorization Sources:	Remove View Details	
OPosture Policies Oposture Policies Oposture Policies Oposture Policies Oposture Policies Oposture Opostur			
Administration	Back to Authenticat	ion Sources	Next → Save Cancel
© Copyright 2023 Hewlett Packard Enterpris	se Development LP	Oct 31, 2023 09:21:23 UTC	ClearPass Policy Manager 6.11.2.252294 on CLABV (Trial Version) platform

Intégration héritée – Authentification MAC

Q app20 × +					✓ - □ ×
← → C ▲ Inte säker https://172.25.20	01.120/tips/tipsContent.action#				e 🖈 🔲 😩 :
orubo	Menu 💻				
Dashboard 0	Configuration » Authentica	tion » Sources » Add	door oney manager		
Monitoring 0	Authentication So				
Configuration	General Static Host Li	sts Summary			
- 🗘 Service Templates & Wizards	MAC Addross Host Liste:				
-# Services	MAC Address Host Lists.	Add Static Host List		•	Add New Static Host List
Authentication		Name:	Axis devices		
Sources		Description:		1	
🖃 🧕 Identity					
- C Single Sign-On (SSO)		Hast Format:	C Subpat	<u>a</u>	
- C Endpoints		nost ronnut.	O Regular Expression		
Static Host Lists			List	_	
Role Mannings		Host Type:	IP Address MAC Address		
⊡ 冊 Posture		Host Entries			
- C Posture Policies		# Address	Description		
- Audit Servers		1. O B8-A4-4F-45-B4-E	6 Axis Device 1	Ψ.	
Enforcement		2. O B8-A4-4F-45-B4-E	7 Axis Device 2	Ť	
- C Policies		3. O B8-A4-4F-45-B4-E	8 Axis Device 3	ti -	
- Department - Profiles		Address:			
- ** Network		Description:			
- Device Groups			Į		
- 🛱 Proxy Targets			Save	Host	
- C Event Sources					
- O Policy Simulation					
			Save	ancel	
		-		_	
	& Back to Authenticativ	on Sources			Next > Save Cancel
Administration 0					
© Copyright 2023 Hewlett Packard Enterprise D	evelopment LP	Oct 31, 2023 09	:20:18 UTC	ClearPass Policy Manag	er 6.11.2.252294 on CLABV (Trial Version) platform

Une liste d'hôtes statique, contenant les adresses MAC Axis, est créée.

Intégration héritée – Authentification MAC

Q app20 × +				✓ - □ X
← → C ▲ Inte säker https://172.2	25.201.120/tips/tipsContent.action#			ie 🖈 🛛 🚢 :
aruba		ClearPass	Policy Manager	Menu 🗮
Dashboard	Configuration » Authentica	tion » Sources » Add		
Monitoring	Authentication So	urces		
& Configuration	0		List "Axis dovisos" addod succossf	
Service Templates & Wizards	General Static Host Li	sts Summary	LISC AXIS GEVICES added Succession	any .
A authentication A authentication A methods C Single Sign-On (SSO) A cal Users A	MAC Address Host Lists:	Axis devices	Remove View Details Modify	Add New Static Host List
Administration	Back to Authentication	on Sources		Next → Save Cancel
© Copyright 2023 Hewlett Packard Enterpri	ise Development LP	Oct 31, 2023 09:20:34	UTC	ClearPass Policy Manager 6.11.2.252294 on CLABV (Trial Version) platform

Configuration du service

Dans la page **Services** page, les étapes de configuration sont regroupées dans un seul service qui gère l'authentification et l'autorisation des périphériques Axis au sein des réseaux HPE Aruba Networking.

Intégration héritée – Authentification MAC

	201.120/tip:	s/tipsCc	ontent.action	#tipsServices.action				L	₽ ☆	
aruba				ClearPass Poli	icv N	lanager				Menu
	Config	uration	» Convisos							a series and the series of
	Coning	·	# Services							Add 📥
Monitoring	Serv	ices								A Import
Configuration	•									😫 Export A
 Q Service Templates & Wizards Q Services 	This pa	age sho	ows the curi	ent list and order of services that ClearPass fol	llows du	ring authentication and	authorization.			
Authentication	Filter:	Name		✓ contains ✓	æ	Go Clear Filter	Hit Count for Current hour ¥]	Show [20 v record
- Q Methods	#		Order 🔺	Name		Туре	Template	Hit Cour	nt	Status
- Q Identity	1.		1	Axis 802.1X Wired		RADIUS	802.1X Wired	0		0
Single Sign-On (SSO)	2.	0	2	Axis 802.1X Wired - Mac Authentication		RADIUS	MAC Authentication	0		0
- O Local Users	3.		3	Test Service		RADIUS	802.1X Wired	0		0
- 🛱 Endpoints	4.		4	Policy Manager Admin Network Login Service	9]	TACACS+	TACACS+ Enforcement	0		
- 🛱 Static Host Lists	5.	0	5	[AirGroup Authorization Service]		RADIUS	RADIUS Enforcement (Generic)	0		0
- 🛱 Roles	6.		6	[Aruba Device Access Service]		TACACS+	TACACS+ Enforcement	0		
- CR Role Mappings	7.		7	[Guest Operator Logins]		Application	Aruba Application Authentication	0		
Posture Policies	8.	0	8	[Insight Operator Logins]		Application	Aruba Application Authentication	0		
- Ö Audit Servers	9		9	[Device Registration Disconnect]		WEBAUTH	Web-based Authentication	0		~
- Agentless OnGuard	-			[befree registration bisconnext]		incontri			C.C.	
B Enforcement	Snowir	1g 1-9	01.9					Reorder	Expo	Delete
- 🗘 Policies										
- 🛱 Profiles										
- Network										
Device Groups										
Proxy Targets										
- C Event Sources										
Q Network Scan										
Policy Simulation										
Administration	0									
	<u> </u>									

Intégration héritée – Authentification MAC



Un service Axis dédié et définissant MAB comme méthode de connexion est créé.

Intégration héritée – Authentification MAC

Q app20 × +				✓ - □ X			
← → C ▲ Inte säker https://172.	25.201.120/tips/tipsContent.action#t	ipsEditService.action%3FcontextData%3D30	006	ie 🖈 🛯 😩 :			
aruba		ClearPass	Policy Manager	Menu 🗮			
Dashboard	• Configuration » Services »	Configuration » Services » Edit - Axis 802.1X Wired - Mac Authentication					
🖂 Monitoring	Services - Axis 80	2.1X Wired - Mac Authenti	ication				
🝰 Configuration	Summary Service	Authentication Roles Enforcement	nt				
	Authentication Methods:	[Allow All MAC AUTH]	Move Up : Move Down L Remove View Details Modify	Add New Authentication Method			
- C Local Users		Select to Add	v				
C Claure Control Cont	Authentication Sources:	(Axis Devices [Static Host List]	Move Up † Move Down Remove View Details Modify	Add New Authentication Source			
Enforcement		Select to Add					
→ Policies → Profiles → Network → Devices → Device Groups → Proxy Targets → Cevent Sources → Retwork Scan → Policy Simulation	Strip Username Rules:	Enable to specify a comma-separat	ed list of rules to strip username prefixes or	Suffixes			
🚰 Administration	0			Disable Copy Save Califer			
© Copyright 2023 Hewlett Packard Enterpr	ise Development LP	Oct 31, 2023 09:22:22 U	TC	ClearPass Policy Manager 6.11.2.252294 on CLABV (Trial Version) platform			

La méthode d'authentification MAC préconfigurée est configurée pour le service. De plus, la source d'authentification créée précédemment et contenant une liste d'adresses MAC Axis est sélectionnée.

Axis Communications utilise les OUI d'adresse MAC suivantes :

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

Intégration héritée – Authentification MAC



À la dernière étape, la stratégie d'application créée précédemment est configurée sur le service.

Commutateur d'accès HPE Aruba Networking

Outre la configuration d'intégration sécurisée décrite dans , reportez-vous à l'exemple de configuration de port ci-dessous pour le commutateur d'accès HPE Aruba Networking afin d'autoriser 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 : Mai 2024 Référence T10197992