

HPE Aruba Networking

Table des matières

Introduction.....	3
Intégration sécurisée - IEEE 802.1AR/802.1X	4
Authentification initiale.....	4
Provisionnement	4
Réseau de production	5
Configuration de HPE Aruba Networking	6
HPE Aruba Networking ClearPass Policy Manager	6
Commutateur d'accès HPE Aruba Networking.....	15
Configuration Axis.....	16
Périphérique réseau Axis	16
AXIS Device Manager.....	17
Fonctionnement réseau sécurisé - IEEE 802.1AE MACsec	18
HPE Aruba Networking ClearPass Policy Manager	19
Politique de rôle et de mappage de rôles	19
Configuration du service	20
Profil d'application	21
Commutateur d'accès HPE Aruba Networking.....	22
Intégration héritée - Authentification MAC.....	23
HPE Aruba Networking ClearPass Policy Manager	23
Politique d'application	23
Configuration source	24
Configuration du service	25
Commutateur d'accès HPE Aruba Networking.....	28

Introduction

Ce guide d'intégration décrit la configuration recommandée pour l'intégration embarquée et le fonctionnement des 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 vous permettre d'économiser du temps et de l'argent. Cela évite une complexité inutile du système lors de l'utilisation d'applications de gestion de périphériques Axis avec l'infrastructure et les applications HPE Aruba Networking. En combinant les périphériques et le logiciel Axis avec une infrastructure HPE Aruba Networking, vous pouvez bénéficier des avantages suivants :

- Supprimer les réseaux d'activation des périphériques réduit la complexité du système.
- L'automatisation des processus embarqués et la gestion des périphériques permettent de réduire les coûts.
- Les périphériques Axis offrent des contrôles de sécurité réseau sans intervention.
- Renforcement de la sécurité réseau globale grâce à l'expertise de HPE et d'Axis.



Afin d'assurer une transition fluide et définie par logiciel entre les réseaux logiques tout au long du processus d'intégration, l'infrastructure réseau doit être prête à vérifier de manière sécurisée l'intégrité des périphériques Axis avant de commencer la configuration. Avant de procéder à la configuration, vous devez disposer des éléments suivants :

- Expérience en matière de 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 antérieures de base sur les produits Axis sont souhaitables mais elles sont également fournies tout au long du guide.

Intégration sécurisée - IEEE 802.1AR/802.1X



Pour regarder cette vidéo, accédez à la version Web de ce document.

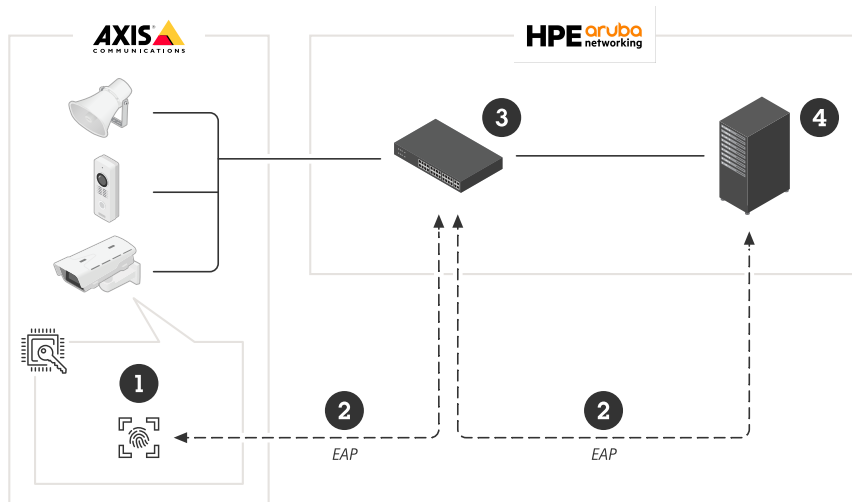
Périphérique sécurisé embarqué sur des réseaux « Zero-Trust » avec IEEE 802.1X/802.1AR

Authentification initiale

Lorsque le périphérique Axis pris en charge par Axis Edge Vault est connecté au réseau, il utilise le certificat d'identifiant de périphérique Axis IEEE 802.1AR via le contrôle d'accès 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. Ces informations, telles que l'adresse MAC et la version du système d'exploitation AXIS du périphérique, sont utilisées pour prendre une décision fondée sur des politiques.

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

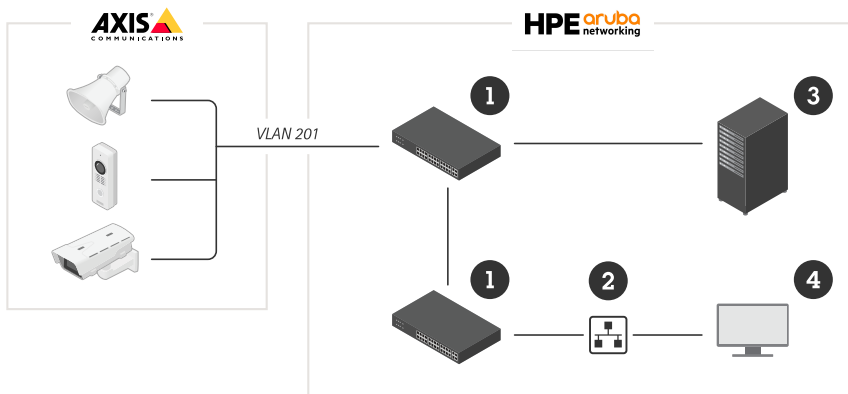


Le périphérique Axis s'authentifie auprès du réseau HPE Aruba Networking à l'aide du certificat d'identification de périphérique Axis conforme à la norme IEEE 802.1AR.

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

Provisionnement

Après authentification, le périphérique Axis passe sur le réseau de provisionnement (VLAN201). Ce réseau comprend AXIS Device Manager, qui assure la configuration des périphériques, le renforcement de la sécurité et met à jour 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.

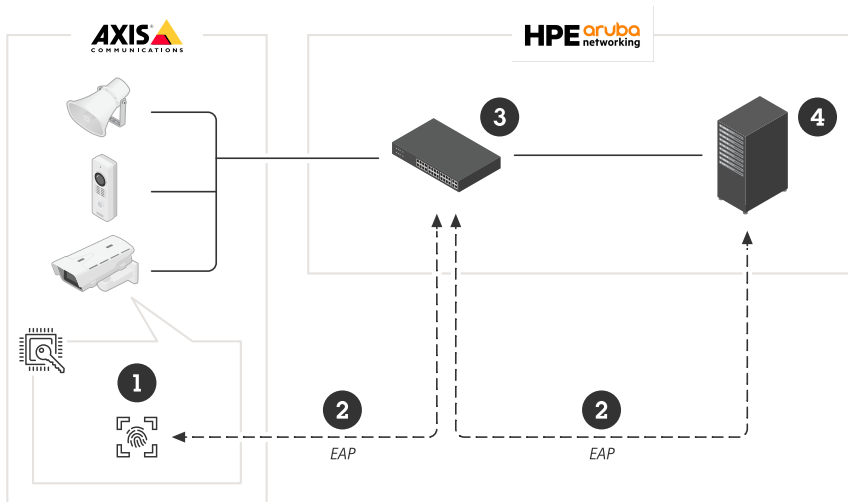


Une fois l'authentification effectuée, le périphérique Axis se déplace vers un réseau de mise en service pour la configuration.

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

Réseau de production

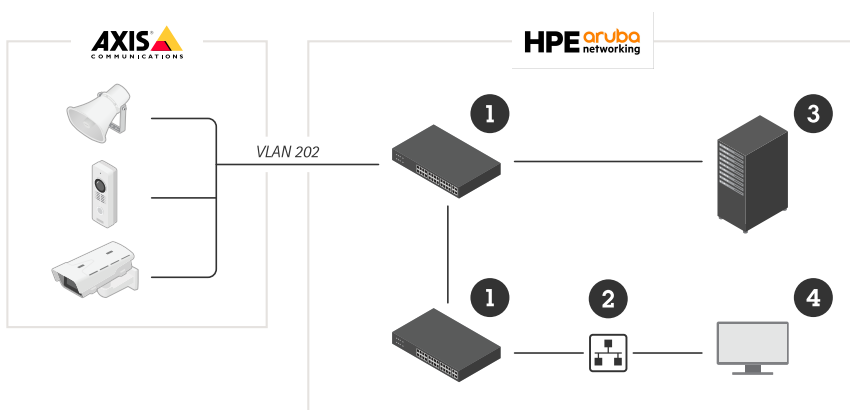
La mise en service du périphérique Axis avec de nouveaux certificats IEEE 802.1X déclenche une nouvelle tentative d'authentification. ClearPass Policy Manager vérifie les nouveaux certificats et décide de déplacer ou non le périphérique Axis dans le réseau de production.



Une fois configuré, le périphérique Axis quitte le réseau de provisionnement et tente de se réauthentifier sur le réseau.

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

Après réauthentification, le périphérique Axis est transféré vers le réseau de production (VLAN 202), où le système de gestion vidéo (VMS) se connecte au périphérique 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.

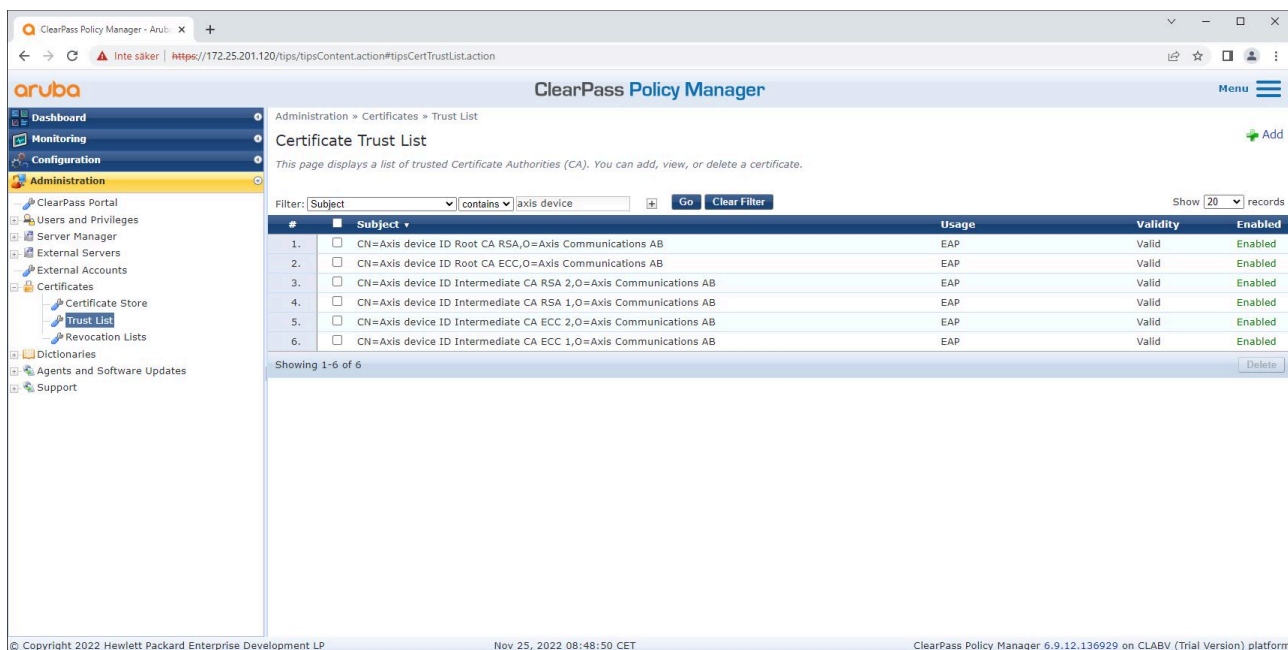
Configuration du magasin de certificats de confiance

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.

The screenshot shows the ClearPass Policy Manager web interface. The left sidebar contains navigation links: Dashboard, Monitoring, Configuration, and Administration. Under Administration, there are links for ClearPass Portal, Users and Privileges, Server Manager, External Servers, External Accounts, Certificates, Certificate Store, Trust List, and Revocation Lists. The main content area is titled 'Administration > Certificates > Trust List' and 'Certificate Trust List'. It displays a table of trusted Certificate Authorities (CA) with columns for #, Subject, Usage, Validity, and Enabled. A dialog box 'Add Certificate' is open, showing a 'Certificate File' field with the value 'Axis_device_ID_Int...e_CA_ECC_1.pem' and a 'Usage' dropdown set to 'EAP'. The dialog also has 'Remove', 'Add Certificate', and 'Cancel' buttons.

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

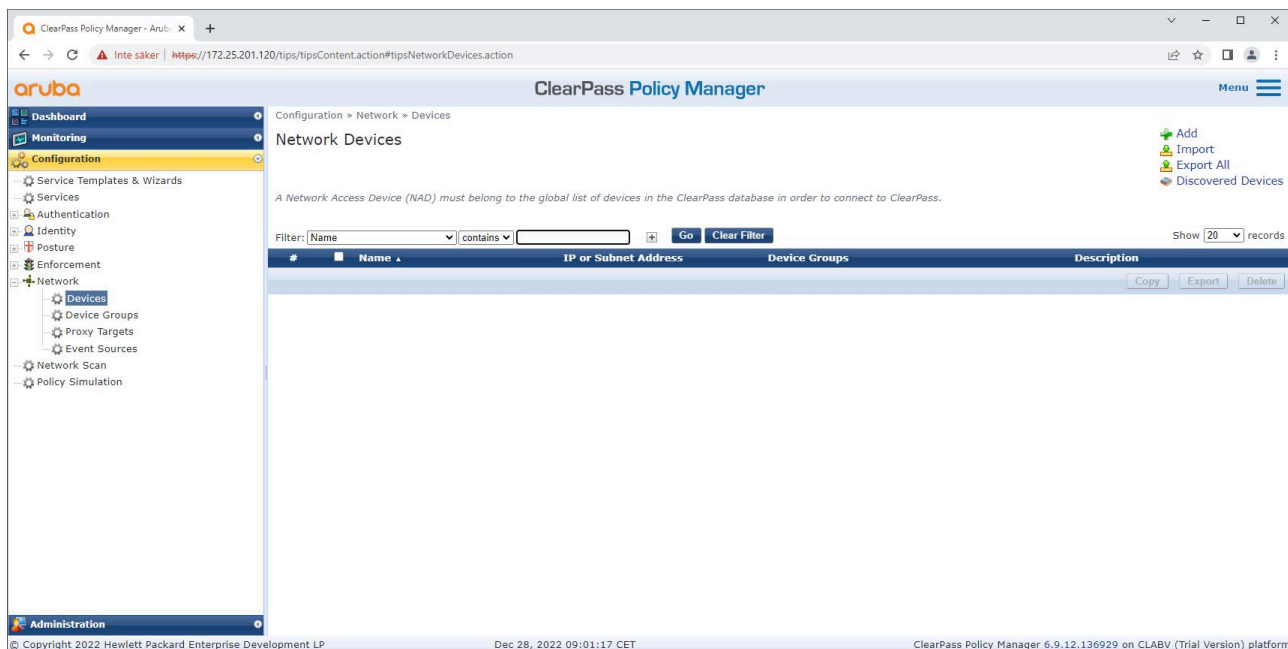
Chargez des certificats IEEE 802.1AR spécifiques à Axis vers le magasin de certificats de confiance de ClearPass Policy Manager.



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

1. 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. Notez également que le secret partagé RADIUS doit correspondre à la configuration IEEE 802.1X spécifique du commutateur.
2. Utilisez la configuration du groupe de périphériques réseau pour regrouper divers périphériques d'accès réseau approuvés. Le regroupement des périphériques facilite la configuration des politiques.



Interface des périphériques réseau approuvés dans ClearPass Policy Manager.

ClearPass Policy Manager - Aruba

Configuration » Network » Devices

Network Devices

Add Device

Device | SNMP Read Settings | SNMP Write Settings | CLI Settings | OnConnect Enforcement | Attributes

Name: SW04

IP or Subnet Address: 172.25.200.13
(e.g., 192.168.1.10 or 192.168.1.1/24 or 2001:db8:a0b:12f0::1 or 2001:db8:a0b:12f0::1/64)

Description:

RADIUS Shared Secret: [password] Verify: [password]

TACACS+ Shared Secret: [password] Verify: [password]

Vendor Name: Aruba

Enable RADIUS Dynamic Authorization: ☐

Enable RadSec: ☐

Add Cancel

Copyright 2022 Hewlett Packard Enterprise Development LP Dec 28, 2022 09:02:18 CET ClearPass Policy Manager 6.9.12.136929 on CLABV (Trial Version) platform

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

ClearPass Policy Manager - Aruba

Configuration » Network » Devices

Network Devices

Device SW04 added

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

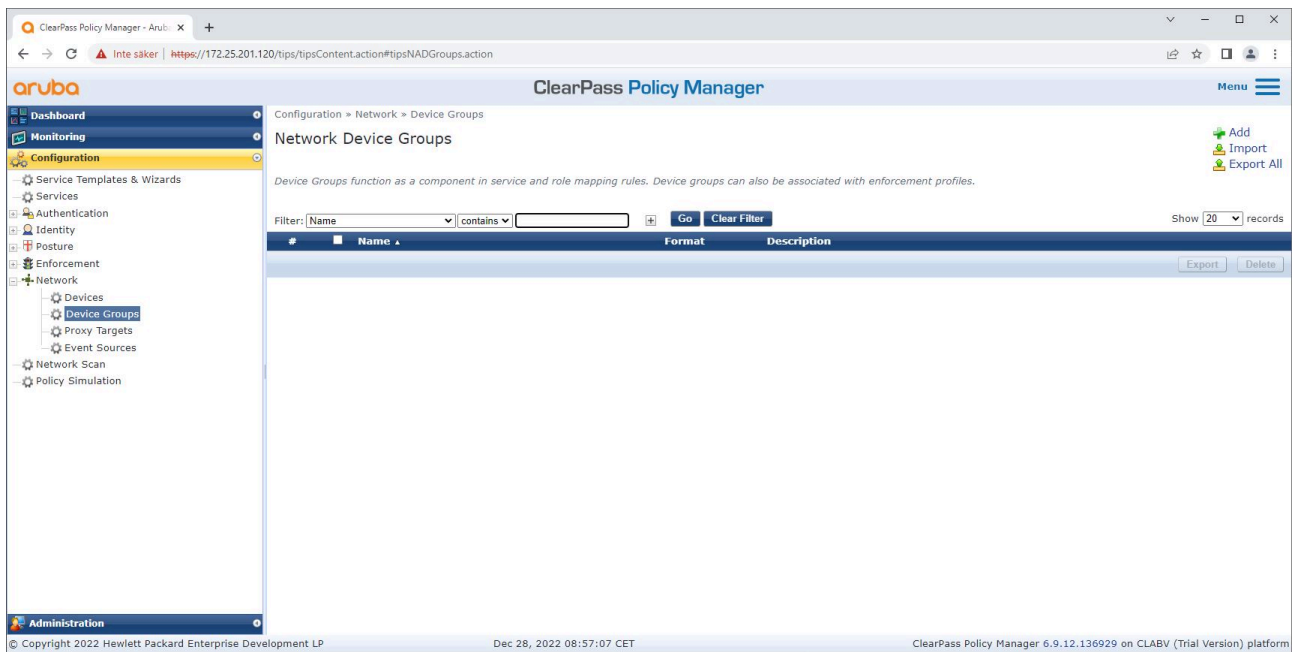
Filter: Name contains [] Go Clear Filter

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

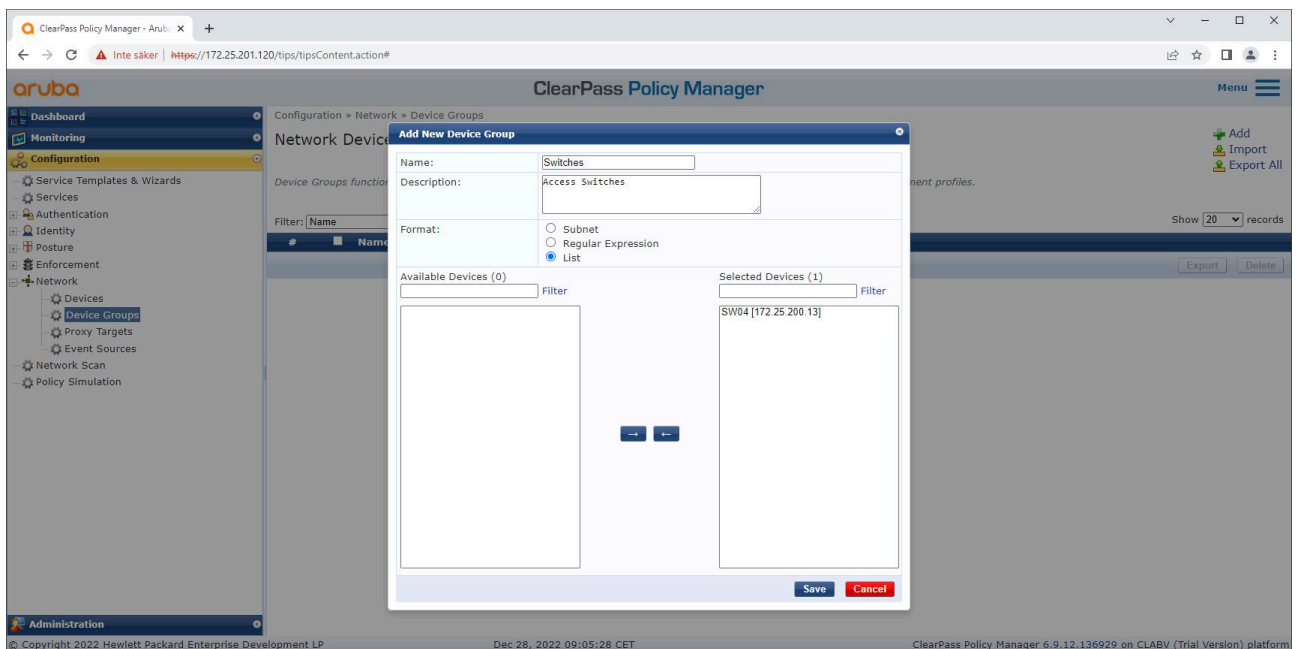
Showing 1-1 of 1

Copyright 2022 Hewlett Packard Enterprise Development LP Dec 28, 2022 09:02:33 CET ClearPass Policy Manager 6.9.12.136929 on CLABV (Trial Version) platform

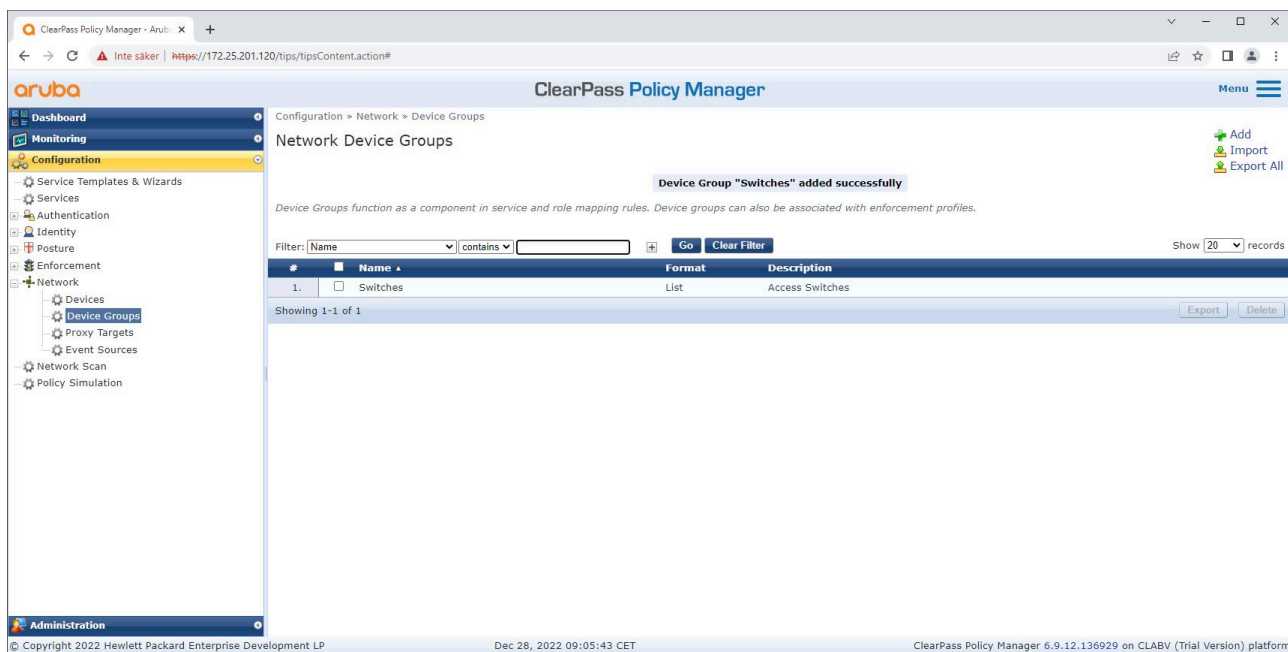
ClearPass Policy Manager avec un seul périphérique réseau approuvé configuré.



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



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

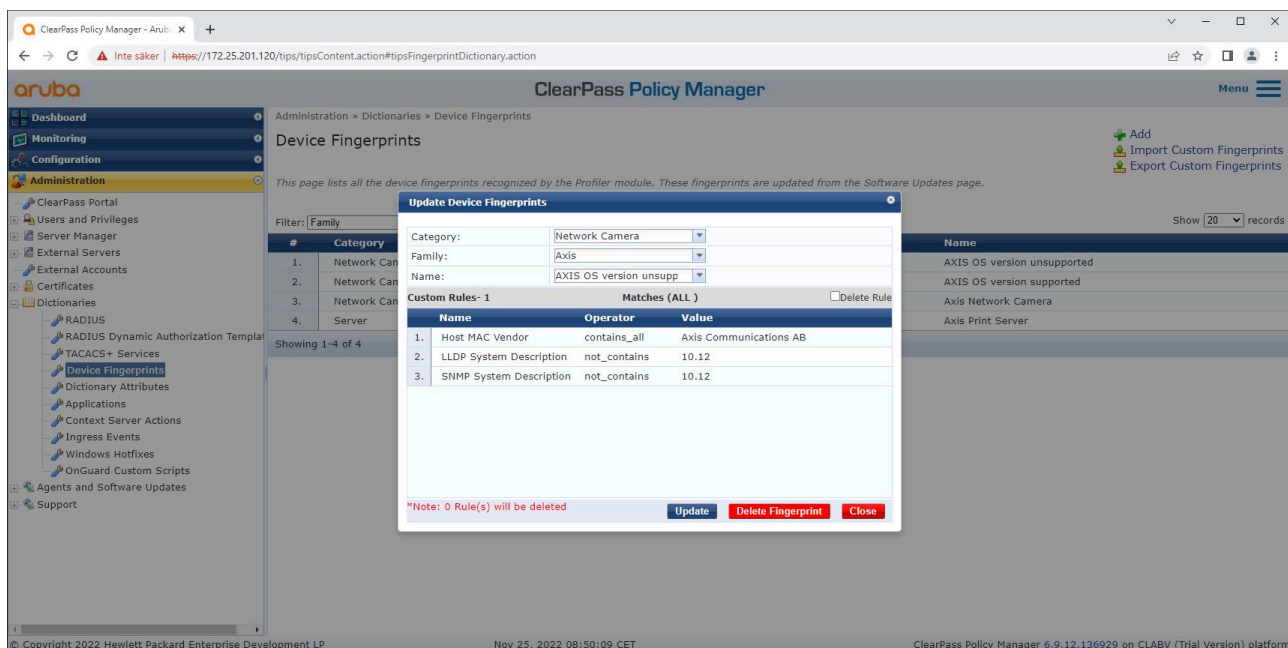


ClearPass Policy Manager avec un groupe de périphériques réseau configuré qui comprend un ou plusieurs périphériques réseau approuvés.

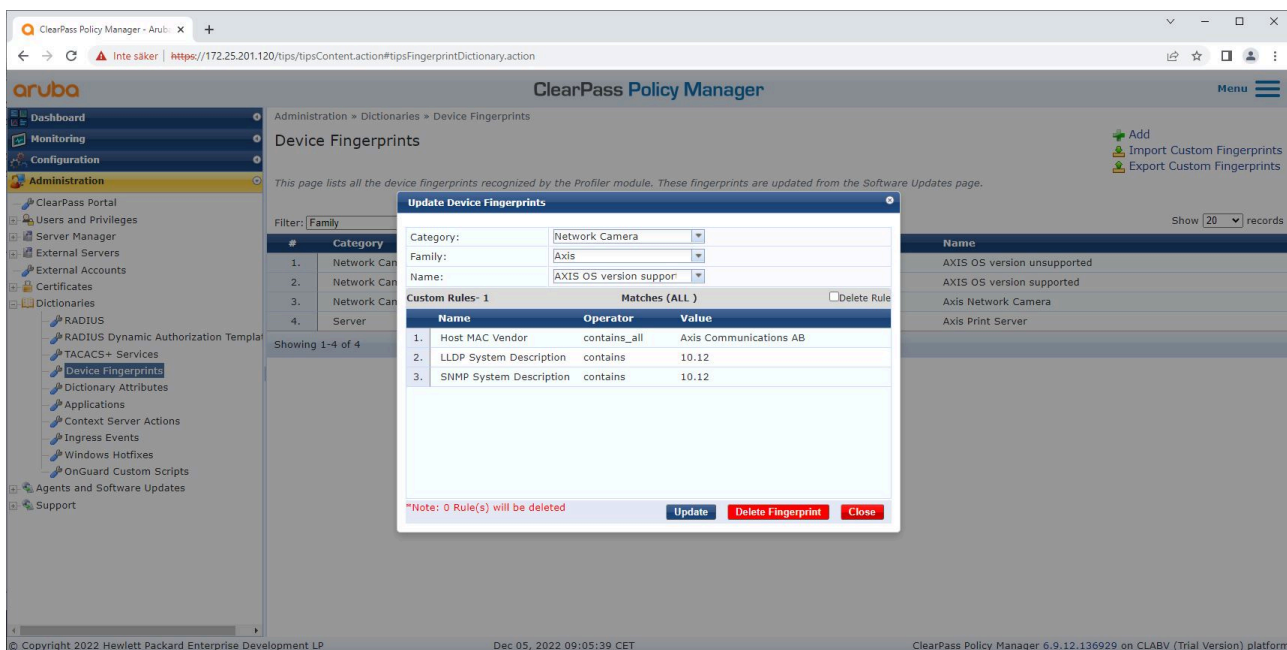
Configuration des empreintes digitales du périphérique

Le périphérique Axis peut, grâce à la découverte réseau, distribuer des informations spécifiques au périphérique telles que l'adresse MAC et la version du logiciel du périphérique. Vous pouvez utiliser ces informations pour créer, mettre à jour ou gérer une empreinte de périphérique dans ClearPass Policy Manager. Vous pouvez également 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.
3. Définissez les paramètres d'empreinte du périphérique.



Configuration des empreintes de périphérique dans ClearPass Policy Manager. Les périphériques Axis fonctionnant sous des versions d'AXIS OS autres que la version 10.12 ne sont pas pris en charge dans cet exemple.



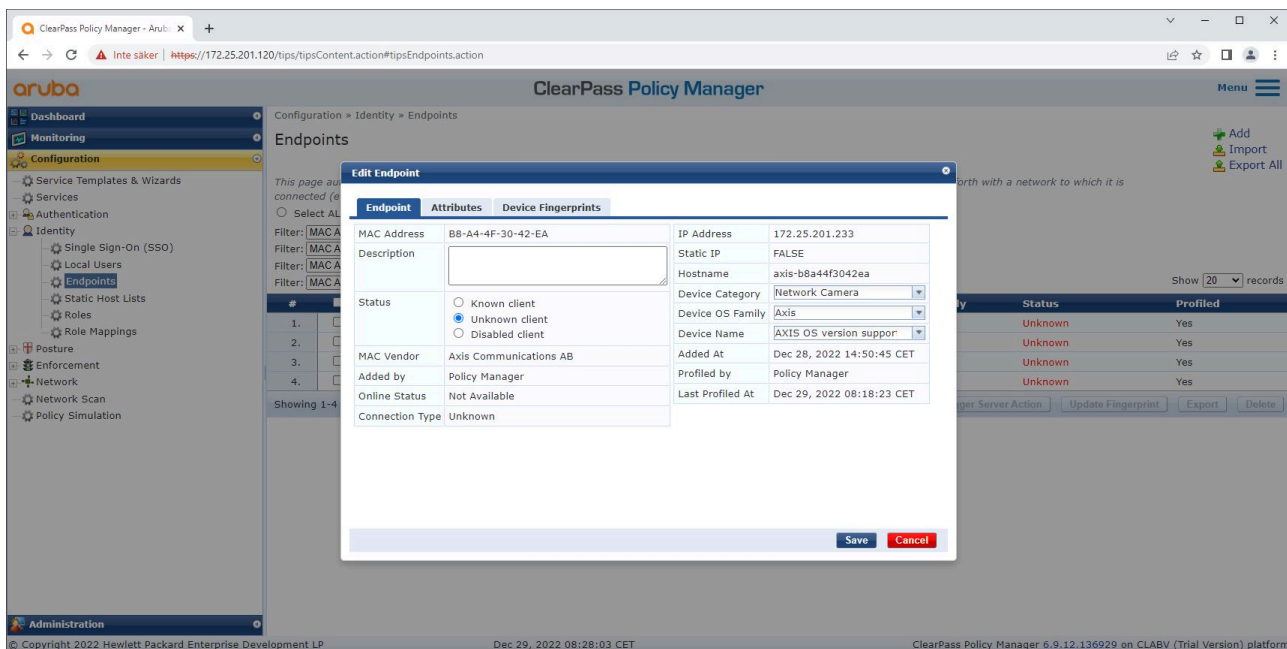
Configuration des empreintes de périphérique dans ClearPass Policy Manager. Les périphériques Axis fonctionnant sous des versions d'AXIS OS autres que la version 10.12 sont pris en charge dans cet exemple.

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

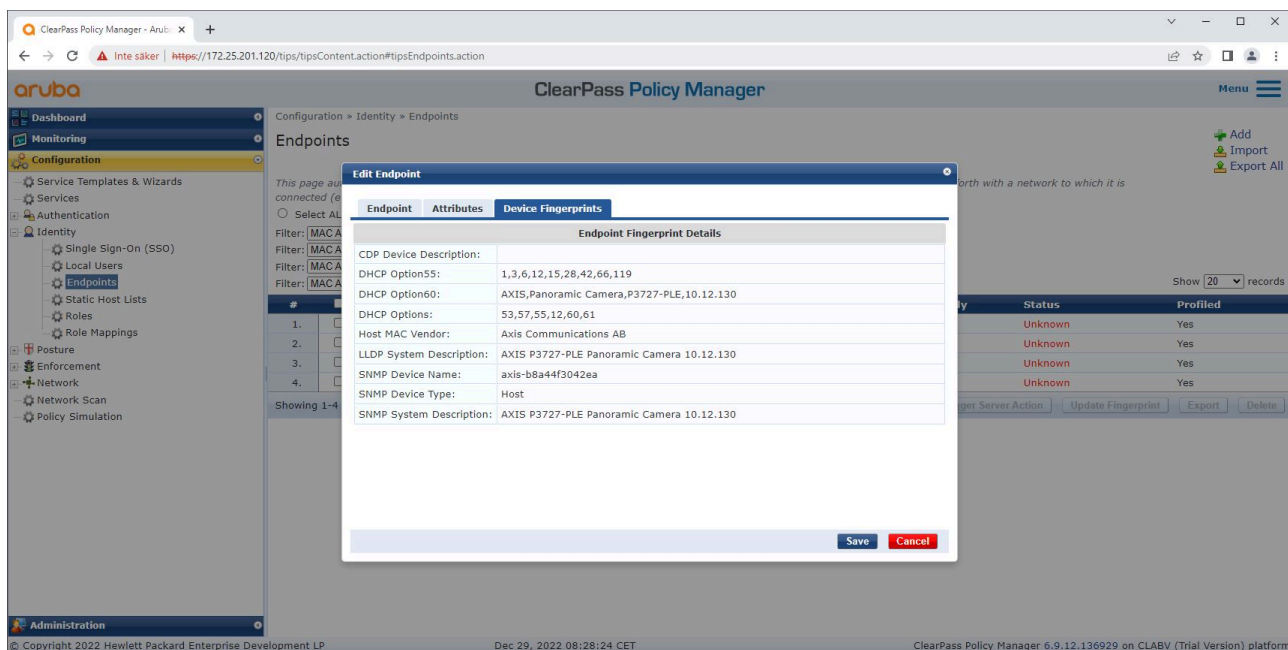
1. Allez à Configuration > Identité > Points de terminaison.
2. Sélectionnez le périphérique que vous voulez afficher.
3. Cliquez sur l'onglet Empreintes de périphérique.

Remarque

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



Un périphérique Axis profilé par ClearPass Policy Manager.

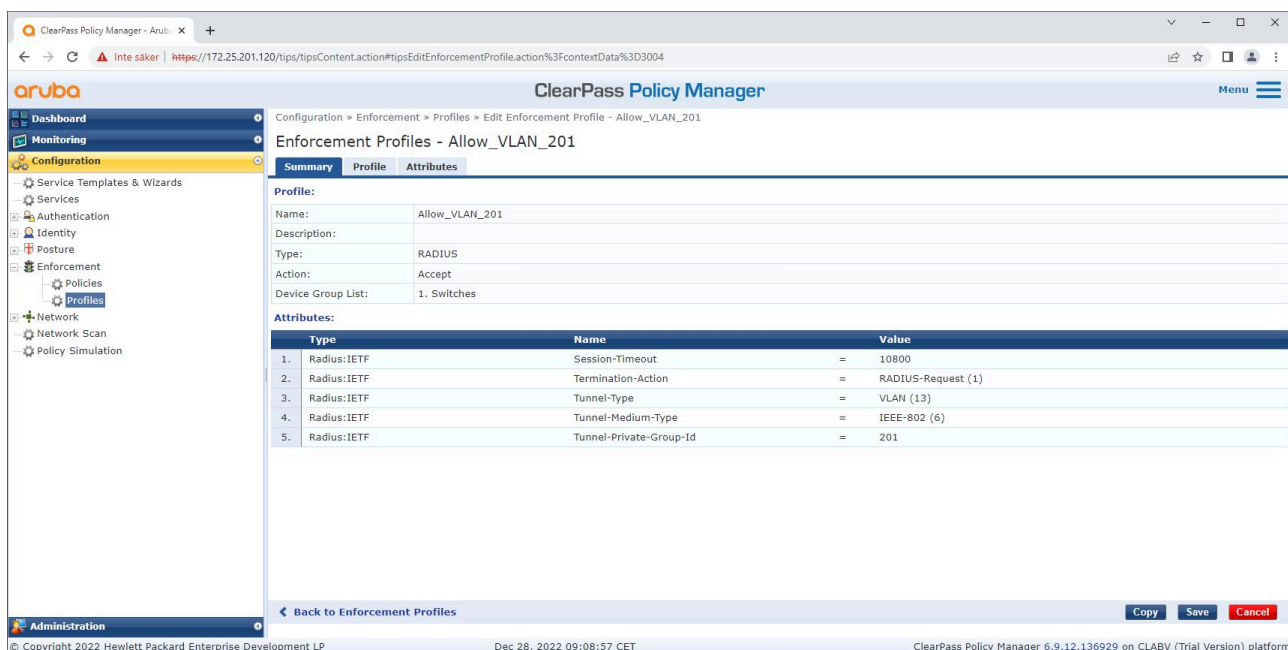


Empreintes détaillées d'un périphérique Axis profilé. Veuillez noter que le protocole SNMP est désactivé par défaut sur les périphériques Axis. Les informations de découverte spécifiques aux protocoles LLDP, CDP et DHCP sont partagées par le périphérique Axis dans son état de valeurs par défaut et sont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

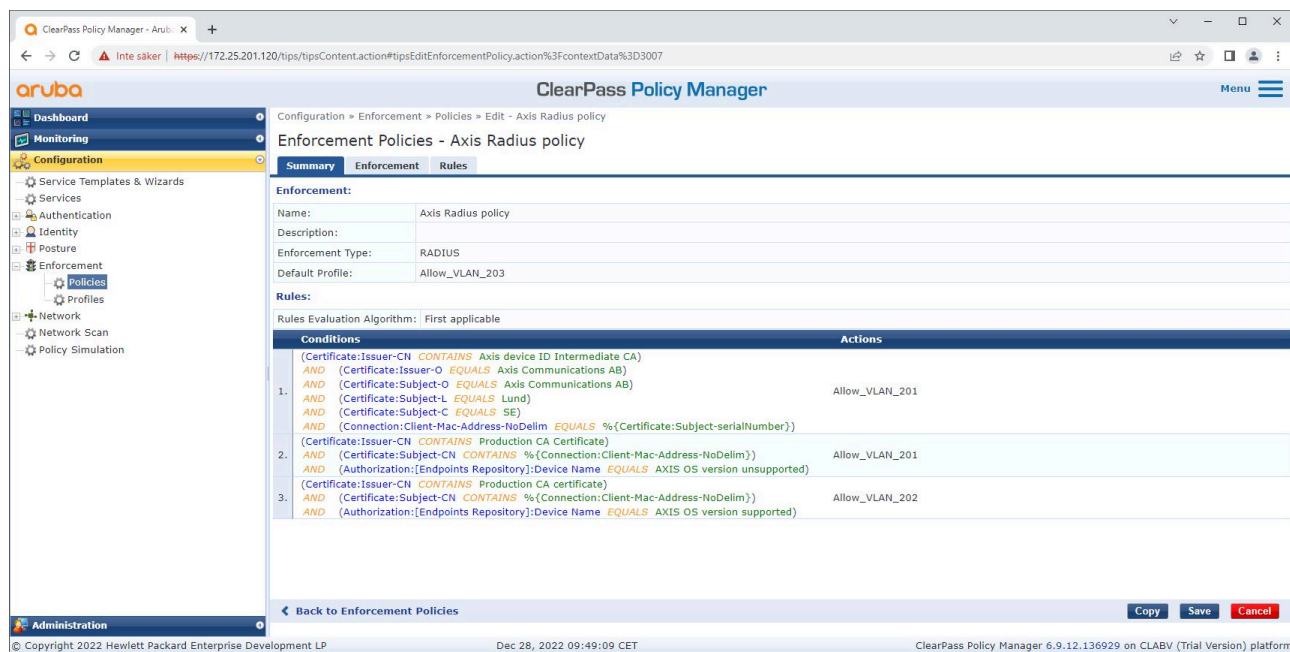
Configuration du profil d'application

Le profil d'application permet à 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 une politique qui s'applique aux périphériques réseau du groupe de périphériques « commutateurs ». Le nombre requis de profils d'application dépend du nombre de réseaux locaux virtuels (VLAN) utilisés. Notre configuration comprend trois réseaux locaux virtuels (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 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.



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



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

Les quatre politiques d'application et leurs actions sont les suivantes :

Accès au réseau refusé

L'accès au réseau est refusé lorsque l'authentification de contrôle d'accès au réseau IEEE 802.1X n'est pas 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 alors nécessaire afin de déterminer l'action appropriée à mener.

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.
- L'adresse MAC du périphérique correspond au schéma d'adresse MAC 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.

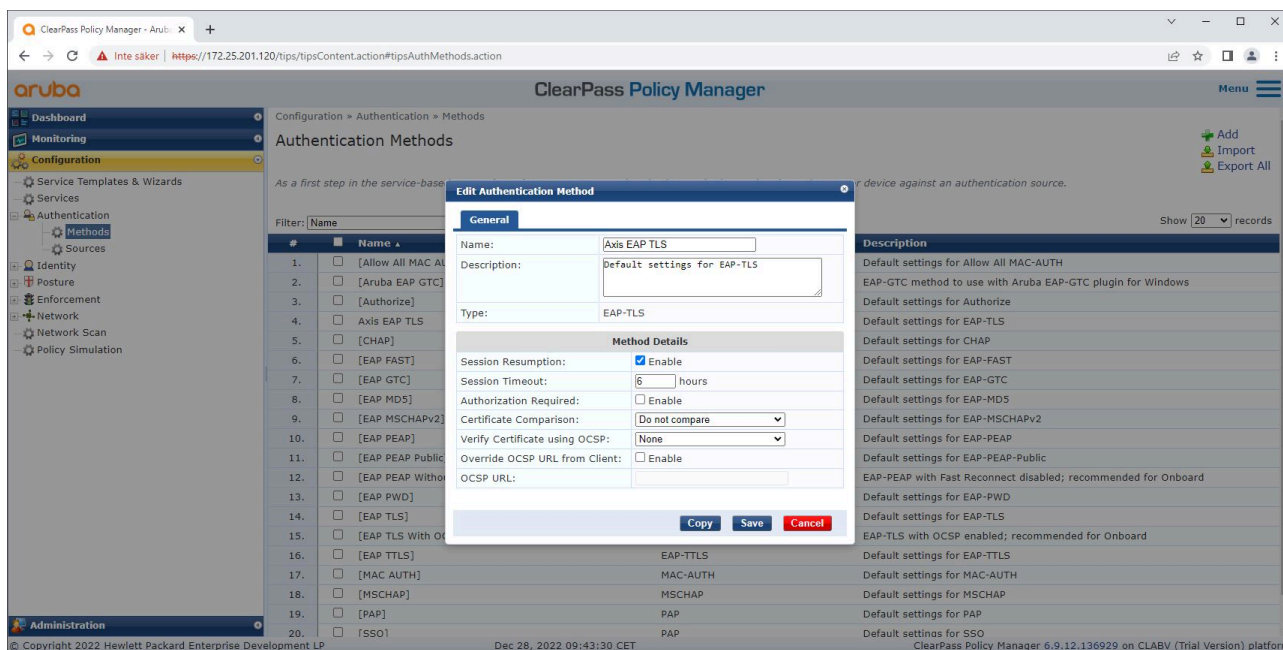
Réseau de production (VLAN 202)

Le périphérique Axis est autorisé à obtenir l'accès au réseau de production sur lequel il fonctionnera. 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 :

- Version d'AXIS OS du périphérique.
- L'adresse MAC du périphérique correspond au schéma d'adresse MAC spécifique au fournisseur avec l'attribut de numéro de série du certificat d'identification du périphérique Axis.
- Le certificat de niveau production est vérifiable par le magasin de certificats de confiance.

Configuration de la méthode d'authentification

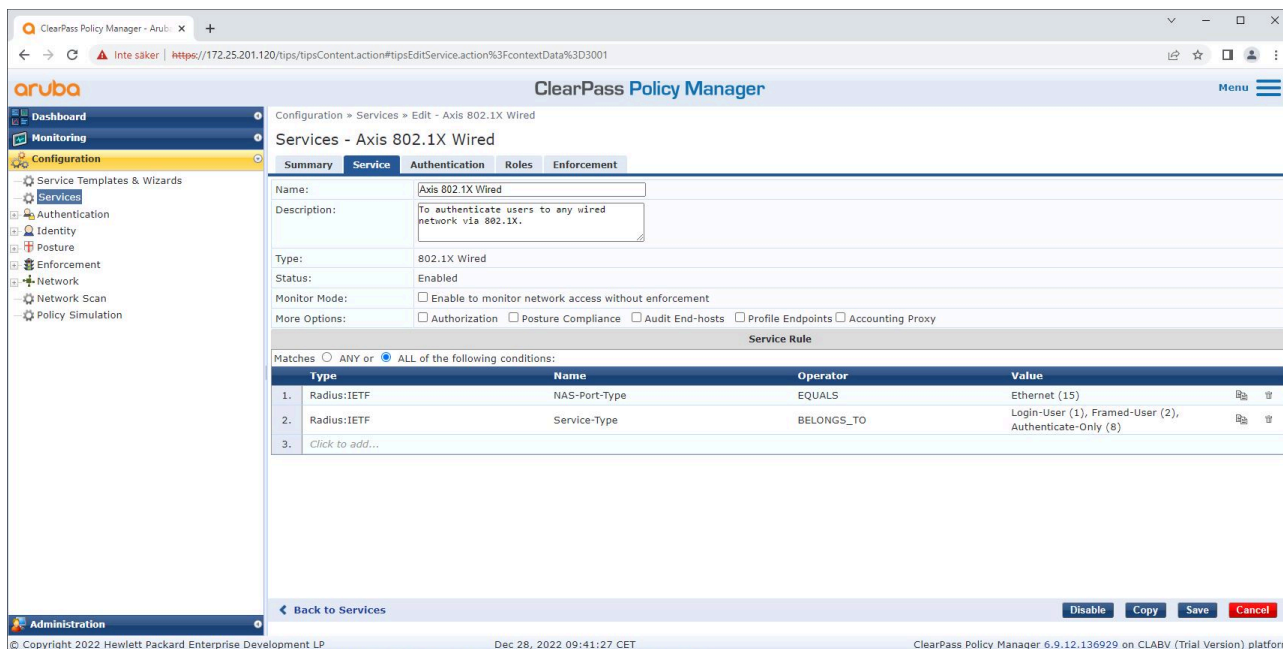
La méthode d'authentification définit la manière dont un périphérique Axis tente de s'authentifier sur le réseau. La méthode préférée est IEEE 802.1X EAP-TLS car les périphériques Axis avec Axis Edge Vault sont livrés avec IEEE 802.1X EAP-TLS activé par défaut.



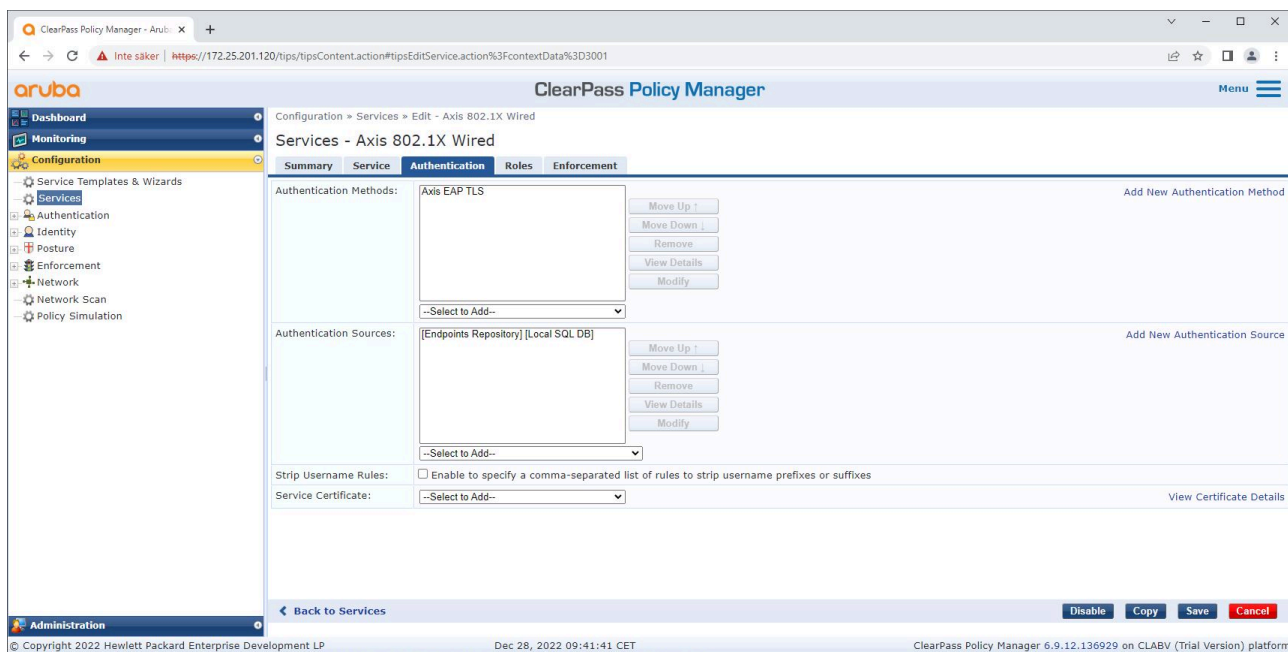
Interface de méthode d'authentification de ClearPass Policy Manager où est définie la méthode d'authentification EAP-TLS pour les périphériques Axis.

Configuration du service

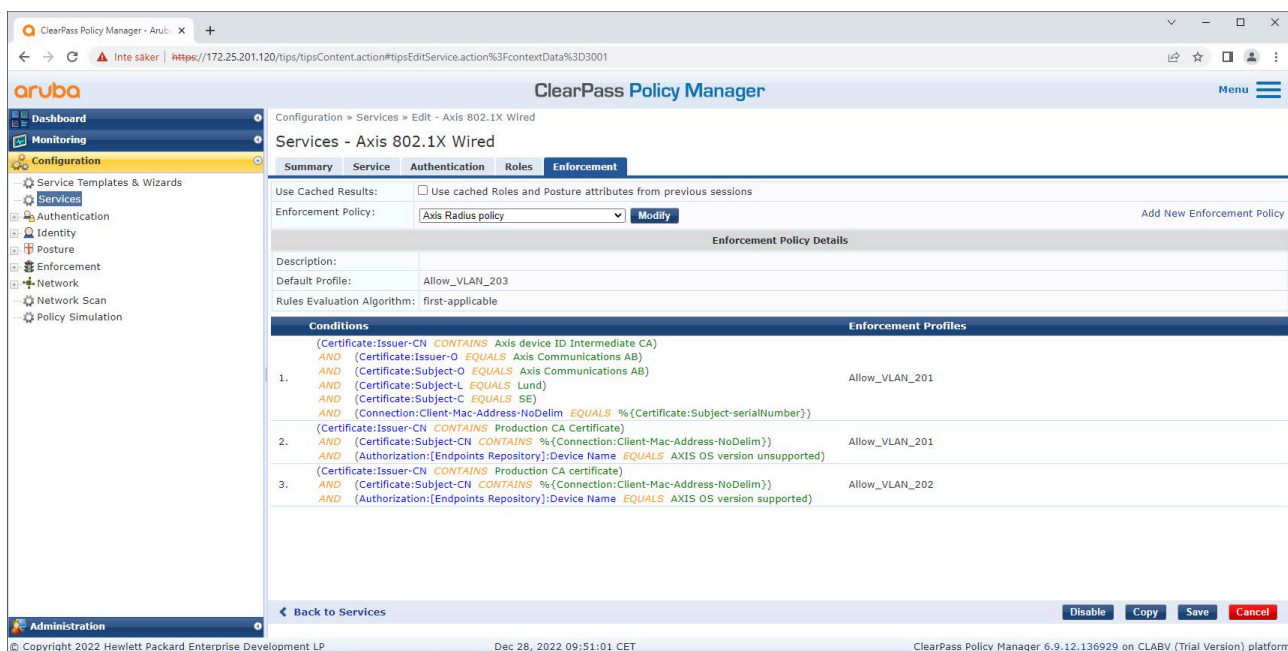
Dans la page Services, les étapes de configuration sont regroupées dans un seul service qui gère l'authentification et l'autorisation des périphériques Axis au sein des réseaux HPE Aruba Networking.



Un service Axis dédié est créé, avec IEEE 802.1X comme méthode de connexion.



La méthode d'authentification EAP-TLS créée précédemment est configurée pour le service.



La politique d'application créée précédemment est configurée pour 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 périphériques 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, lequel 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.

Cet exemple présente la configuration globale et la configuration des ports pour les commutateurs d'accès HPE Aruba Networking.

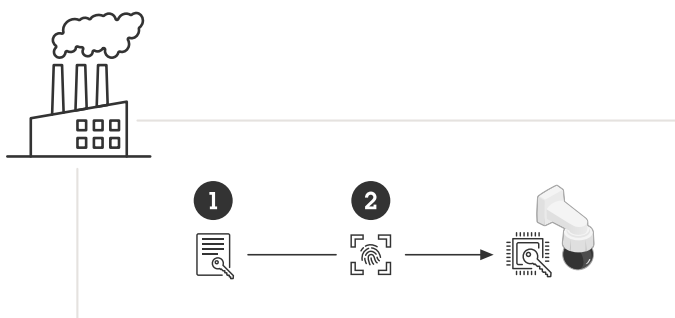
```
radius-server host MyRADIUSIPAddress key "MyRADIUSKey"
```

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

Configuration Axis

Périphérique réseau Axis

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



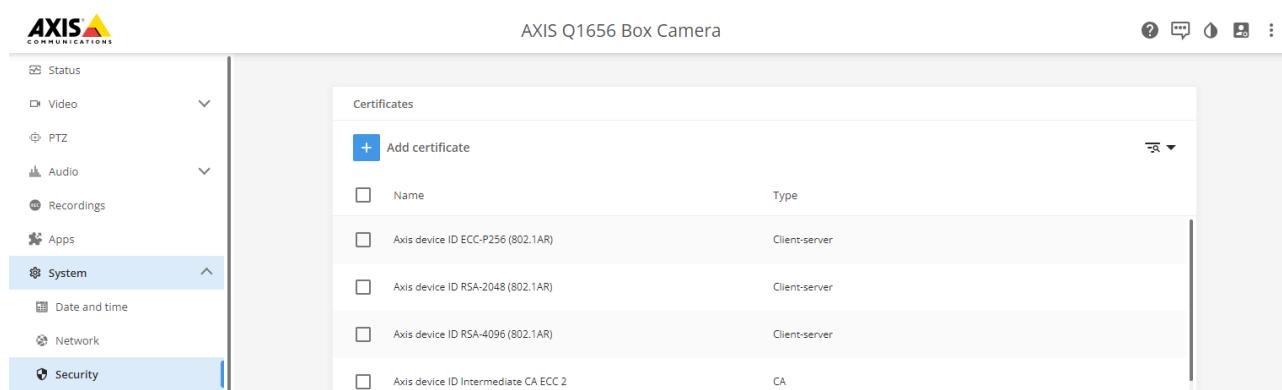
Les périphériques Axis sont fabriqués avec le certificat d'ID de périphérique Axis conforme à la norme IEEE 802.1AR pour les services d'identité de périphérique fiables.

- 1 Infrastructure de clés d'ID de dispositif Axis (PKI)
- 2 Identifiant du 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.

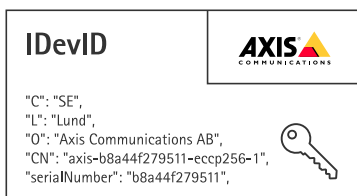
Remarque

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



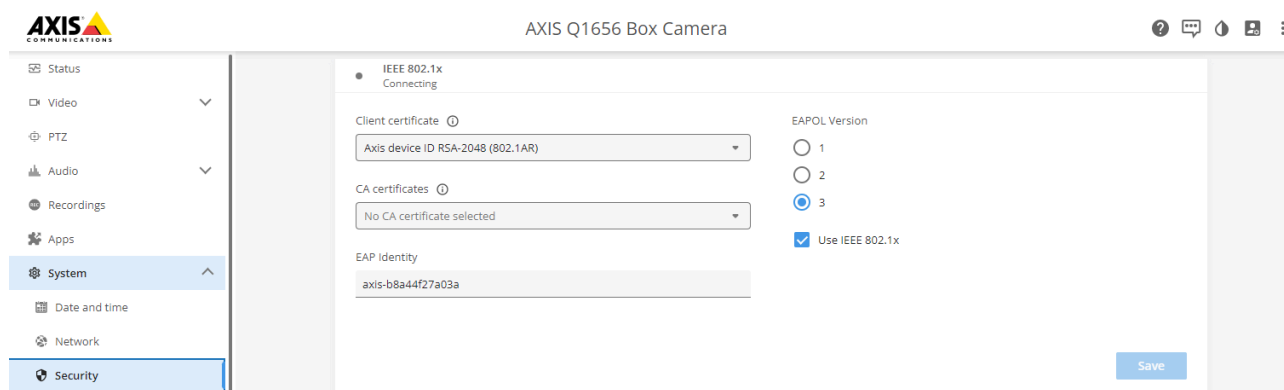
Magasin de certificats du périphérique Axis à l'état d'usine par défaut, avec un ID de périphérique Axis.

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. Ces informations sont utilisées par ClearPass Policy Manager à des fins d'analyse et de prise de décision pour accorder l'accès au réseau. Les informations ci-dessous peuvent être obtenues à partir d'un certificat d'ID de périphérique Axis.



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

Le nom commun est constitué d'une combinaison du nom de la société Axis, du numéro de série du périphérique, suivi de l'algorithme de chiffrement (ECC P256, RSA 2048, RSA 4096). 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 de s'authentifier sur les réseaux compatibles IEEE 802.1X.



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 et AXIS Device Manager Extend peuvent être utilisés sur le réseau pour configurer et gérer plusieurs périphériques Axis de manière économique. AXIS Device Manager est une application Microsoft Windows® installée localement sur un ordinateur du réseau, tandis qu'AXIS Device Manager Extend s'appuie sur une infrastructure cloud pour gérer des périphériques sur plusieurs sites. Les deux offrent des fonctionnalités de gestion et de configuration simples, telles que :

- Installation des mises à jour d'AXIS OS.
- Application de configuration de cybersécurité telles que les 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



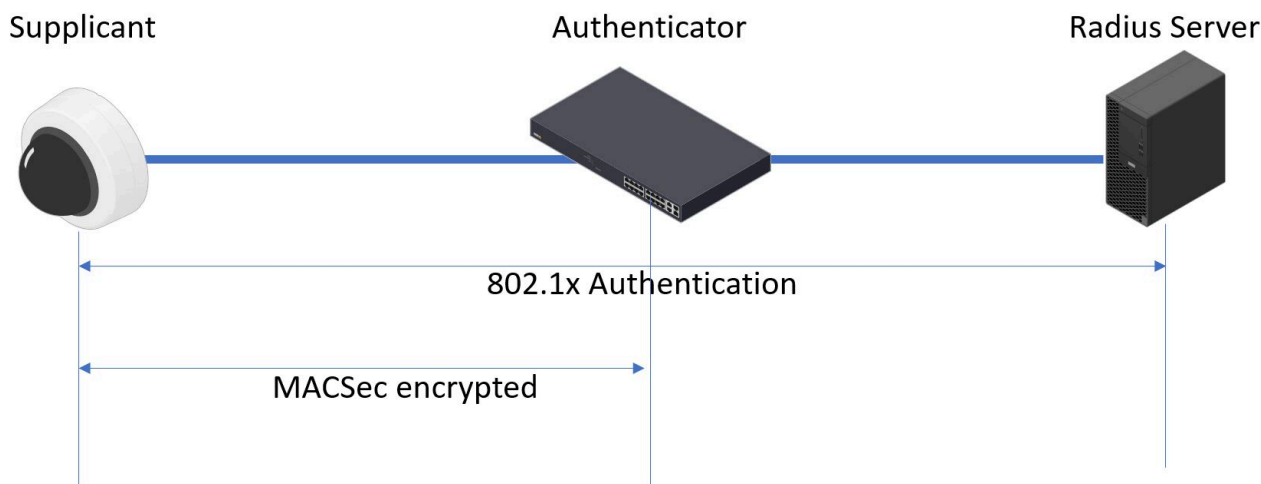
Pour regarder cette vidéo, accédez à la version Web de ce document.

Cryptage réseau « Zero-Trust » avec la sécurité IEEE 802.1AE MACsec layer-2

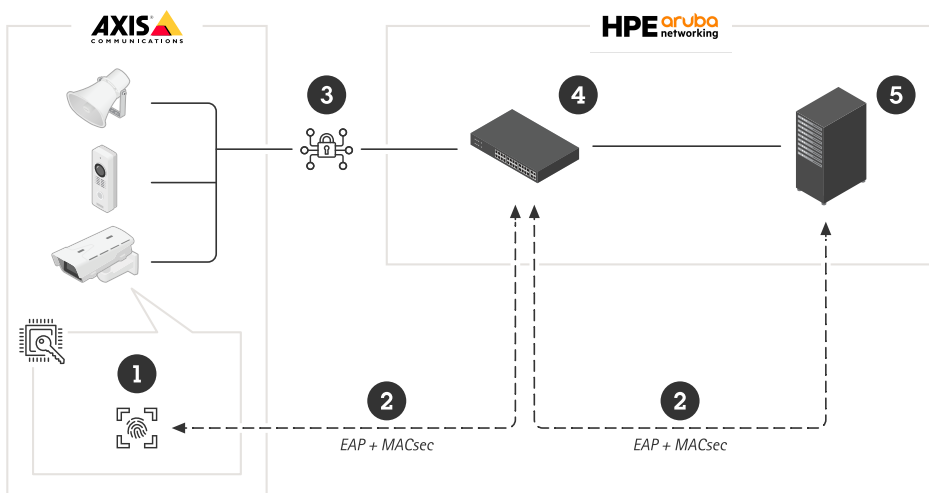
IEEE 802.1AE MACsec (Media Access Control Security) est un protocole réseau bien défini qui sécurise cryptographiquement les liaisons Ethernet point à point sur la couche réseau 2. Il garantit la confidentialité et l'intégrité des transmissions de données entre deux hôtes.

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'identifiant 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

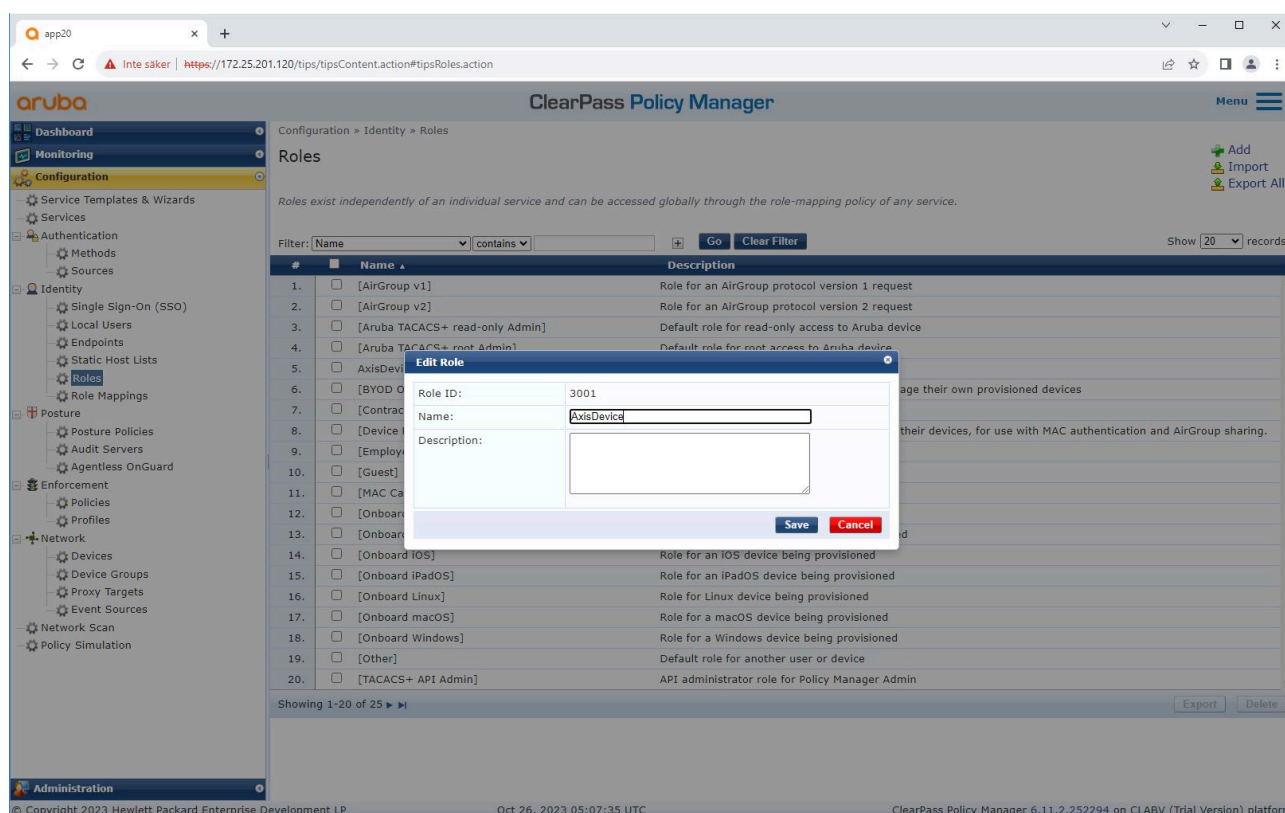
le port EAP-TLS IEEE 802.1X (2). Lors de la session EAP-TLS, les clés MACsec sont échangées automatiquement pour établir un lien sécurisé (3), protégeant tout le trafic réseau depuis le périphérique Axis vers le commutateur d'accès HPE Aruba Networking.

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



The screenshot displays the ClearPass Policy Manager web interface. The left sidebar shows the navigation menu with options like Dashboard, Monitoring, Configuration, Services, Authentication, Identity, Posture, Enforcement, and Network. The main content area is titled 'Roles' and shows a list of roles. An 'Edit Role' dialog box is open, showing the following details:

- Role ID: 3001
- Name: AxisDevice
- Description: (empty field)

The dialog has 'Save' and 'Cancel' buttons. The background list of roles includes entries like [AirGroup v1], [AirGroup v2], [Aruba TACACS+ read-only Admin], [Aruba TACACS+ root Admin], [AxisDevice], [BYOD], [Contract], [Device], [Employee], [Guest], [MAC], [Onboard], [Onboard iOS], [Onboard iPadOS], [Onboard Linux], [Onboard macOS], [Onboard Windows], [Other], and [TACACS+ API Admin].

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.

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

Role Mappings - Axis Role Mapping

Summary Policy Mapping Rules

Policy:

Policy Name: Axis Role Mapping

Description:

Default Role: [Guest]

Mapping Rules:

Rules Evaluation Algorithm: Evaluate all

Conditions	Role Name
1. (Authentication:Full-Username BEGINS_WITH axis-00408c)	AxisDevice
2. (Authentication:Full-Username BEGINS_WITH axis-acc8e)	AxisDevice
3. (Authentication:Full-Username BEGINS_WITH axis-b8a44f)	AxisDevice

Back to Role Mappings Copy Save Cancel

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

Ajoutez une stratégie de mappage des rôles 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-numéro de série ». Le numéro de série d'un périphérique Axis correspond à son adresse MAC. Par exemple « axis-b8a44f45b4e6 ».

Configuration du service

Configuration » Services » Edit - Axis 802.1X Wired

Services - Axis 802.1X Wired

Summary Service Authentication Roles Enforcement

Role Mapping Policy: Axis Role Mapping Modify Add New Role Mapping Policy

Role Mapping Policy Details

Description:

Default Role: [Guest]

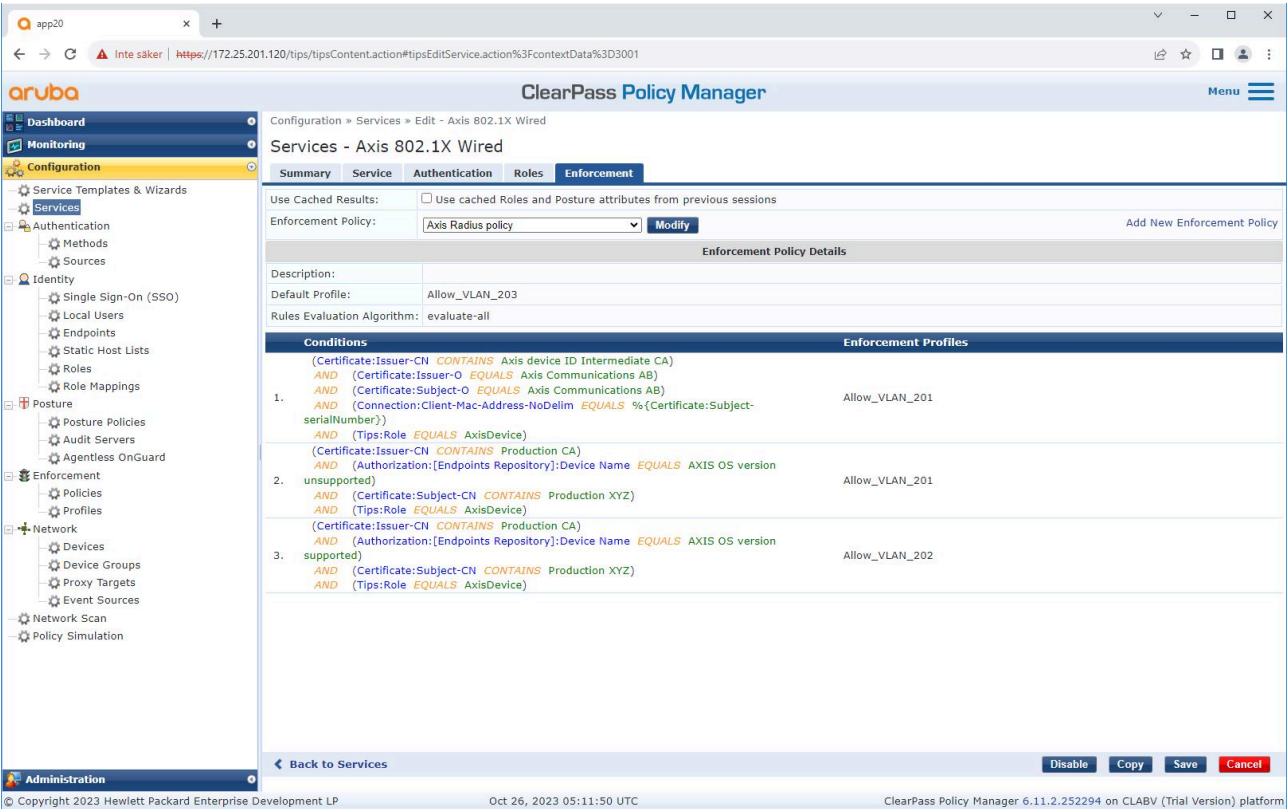
Rules Evaluation Algorithm: evaluate-all

Conditions	Role
1. (Authentication:Full-Username BEGINS_WITH axis-00408c)	AxisDevice
2. (Authentication:Full-Username BEGINS_WITH axis-acc8e)	AxisDevice
3. (Authentication:Full-Username BEGINS_WITH axis-b8a44f)	AxisDevice

Back to Services Disable Copy Save Cancel

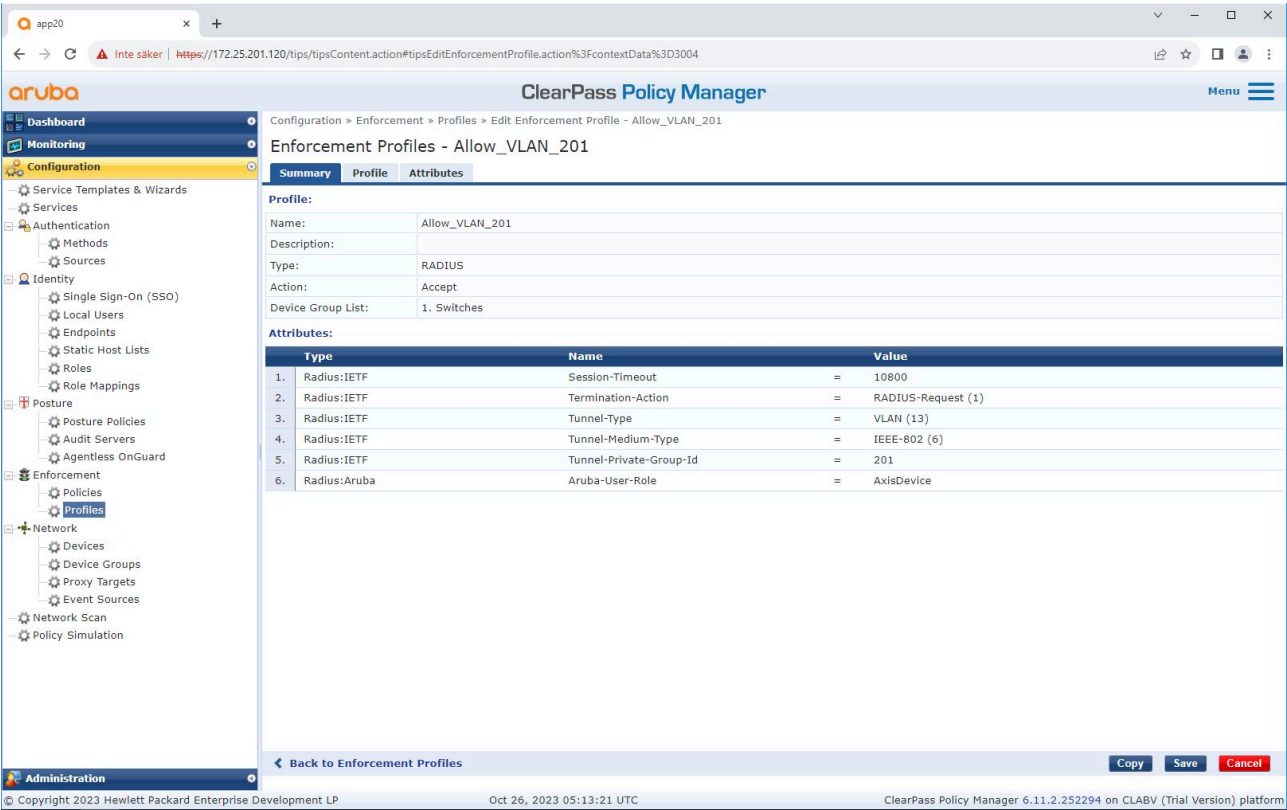
Copyright 2023 Hewlett Packard Enterprise Development LP Oct 26, 2023 05:09:16 UTC ClearPass Policy Manager 6.11.2.252294 on CLABV (Trial Version) platform

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.



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

Profil d'application



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 ci-dessous à l'exemple de configuration de port pour le commutateur d'accès HPE Aruba Networking afin de configurer IEEE 802.1AE MACsec.

```
macsec policy macsec-eapcipher-suite gcm-aes-128
port-access role AxisDeviceassociate macsec-policy macsec-eapauth-mode client-mode
aaa authentication port-access dot1x authenticatormacsecmkacak-length 16enable
```

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. Aucune configuration n'est nécessaire sur le périphérique Axis pour permettre l'intégration embarquée 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.

Accès au réseau refusé

Si 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 :

- Le jour est un jour de semaine, du lundi au vendredi.
- L'heure est comprise entre 9 h et 17 h.
- Le fournisseur d'adresse MAC correspond à Axis Communications.

Étant donné qu'il est possible de falsifier une adresse MAC, l'accès au réseau de provisionnement standard n'est pas autorisé. Nous vous recommandons d'utiliser MAB uniquement pour l'intégration initiale, puis 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.

The image displays two screenshots of the ClearPass Policy Manager web interface, showing the configuration of authentication sources.

Top Screenshot: Authentication Sources List

The interface shows the 'Authentication Sources' page. A filter is applied: Name contains [blank]. The list displays 11 sources:

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

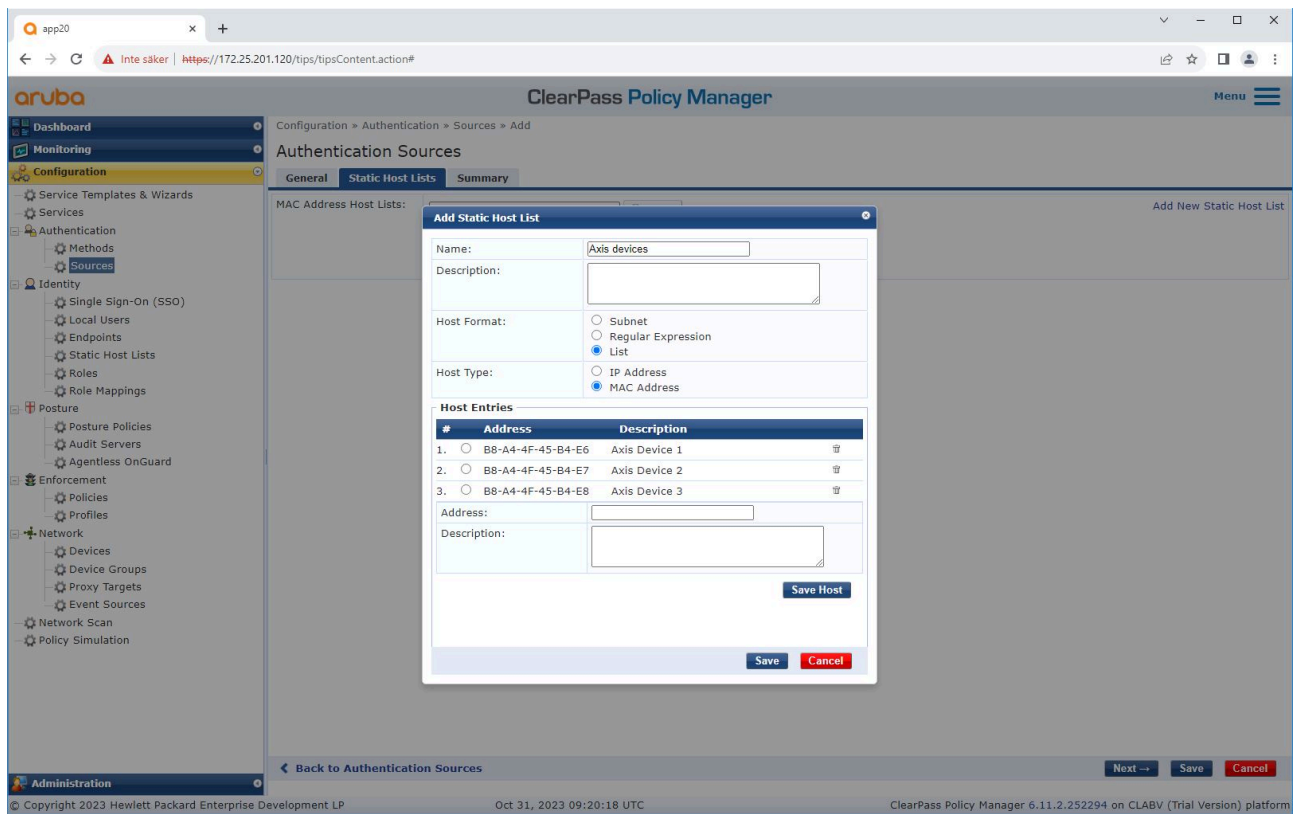
Showing 1-11 of 11. Actions: Copy, Export, Delete.

Bottom Screenshot: Add Authentication Source Form

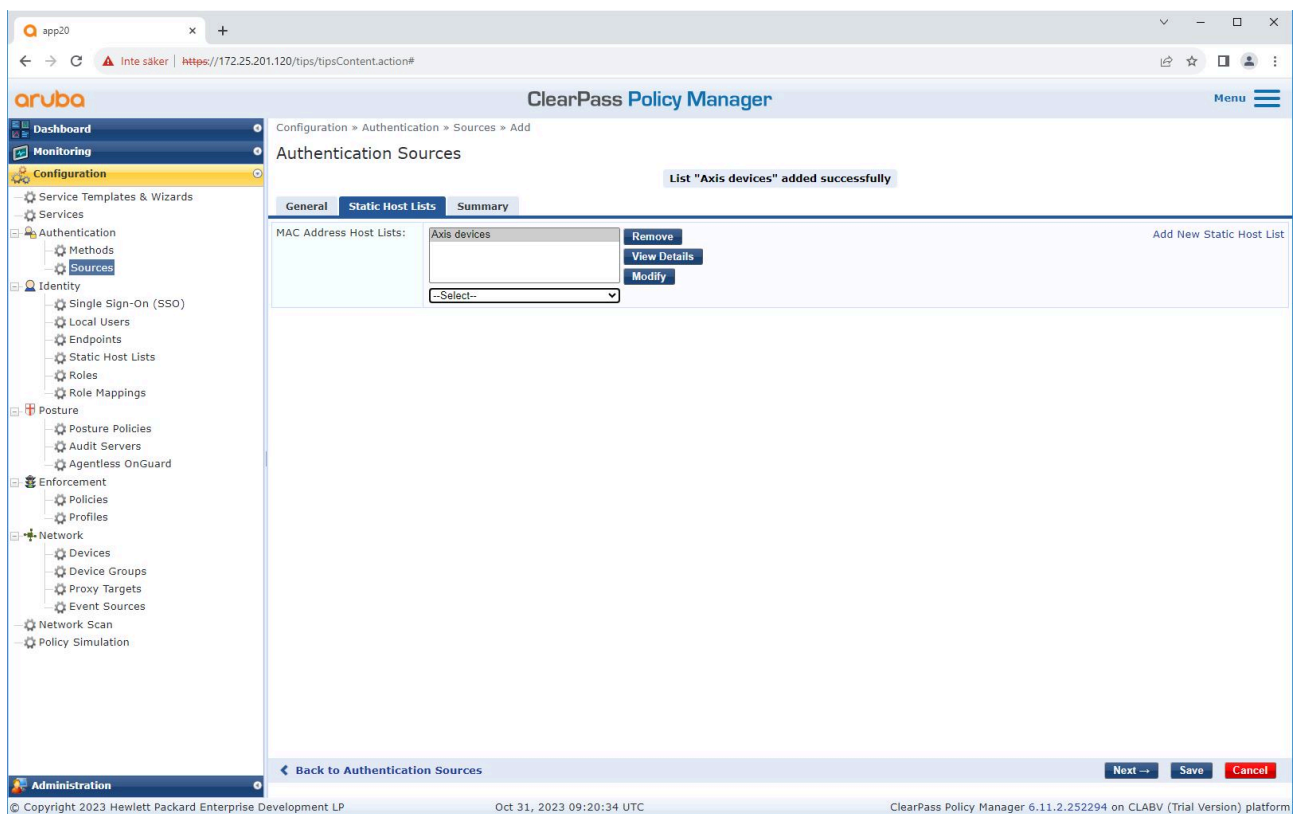
The interface shows the 'Add Authentication Source' page. The form fields are:

- Name: Axis Devices
- Description: MAC addresses of Axis devices in use.
- Type: Static Host List
- Use for Authorization: ☐ Enable to use this Authentication Source to also fetch role mapping attributes
- Authorization Sources: (Empty list with Remove and View Details buttons)

Navigation: Back to Authentication Sources, Next, Save, Cancel.



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



Configuration du service

Dans la page Services, 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.

app20

Inte saker | https://172.25.201.120/tips/tipsContent.action#tipsServices.action

aruba

ClearPass Policy Manager

Menu

Dashboard

Monitoring

Configuration

Administration

Service Templates & Wizards

Services

Authentication

Identity

Posture

Enforcement

Network

Configuration » Services

Services

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

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

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

Showing 1-9 of 9 Reorder Copy Export Delete

Copyright 2023 Hewlett Packard Enterprise Development LP

Oct 26, 2023 05:34:53 UTC

ClearPass Policy Manager 6.11.2.252294 on CLABV (Trial Version) platform

app20

Inte saker | https://172.25.201.120/tips/tipsContent.action#tipsEditService.action%3FcontextData%3D3006

aruba

ClearPass Policy Manager

Menu

Dashboard

Monitoring

Configuration

Administration

Service Templates & Wizards

Services

Authentication

Identity

Posture

Enforcement

Network

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

Services - Axis 802.1X Wired - Mac Authentication

Summary Service Authentication Roles Enforcement

Name: Axis 802.1X Wired - Mac Authentication

Description: To authenticate guest devices based on their MAC address.

Type: MAC Authentication

Status: Disabled

Monitor Mode: ☐ Enable to monitor network access without enforcement

More Options: ☐ Authorization ☐ Audit End-hosts ☐ Profile Endpoints ☐ Accounting Proxy

Service Rule

Matches ANY or ALL of the following conditions:

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

Back to Services Enable Copy Save Cancel

Copyright 2023 Hewlett Packard Enterprise Development LP

Oct 26, 2023 05:15:11 UTC

ClearPass Policy Manager 6.11.2.252294 on CLABV (Trial Version) platform

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

The screenshot shows the Aruba ClearPass Policy Manager interface. The left sidebar contains navigation menus for Dashboard, Monitoring, Configuration, and Administration. The main content area is titled 'Services - Axis 802.1X Wired - Mac Authentication' and has tabs for Summary, Service, Authentication, Roles, and Enforcement. The 'Authentication' tab is active, showing 'Authentication Methods' with '[Allow All MAC AUTH]' and 'Authentication Sources' with 'Axis Devices [Static Host List]'. Buttons for 'Move Up', 'Move Down', 'Remove', 'View Details', and 'Modify' are visible. At the bottom, there are buttons for 'Back to Services', 'Disable', 'Copy', 'Save', and 'Cancel'. The footer indicates the copyright is 2023 Hewlett Packard Enterprise Development LP, the date is Oct 31, 2023 09:22:22 UTC, and the version is 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) 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

The screenshot shows the 'Enforcement' tab of the 'Services - Axis 802.1X Wired - Mac Authentication' configuration. It displays 'Use Cached Results' and 'Enforcement Policy' set to 'Axis MAC Authentication Policy'. Below, the 'Enforcement Policy Details' section shows a 'Description' field, a 'Default Profile' set to '[Deny Access Profile]', and a 'Rules Evaluation Algorithm' set to 'evaluate-all'. A table lists conditions and enforcement profiles. The table has two columns: 'Conditions' and 'Enforcement Profiles'. The first row shows a condition '1. (Date:Day-of-Week BELONGS_TO Monday, Tuesday, Wednesday, Thursday, Friday) AND (Date:Time-of-Day IN_RANGE 09:00:00,17:00:00) AND (Connection:Client-Mac-Vendor EQUALS Axis Communications AB)' and an enforcement profile 'Allow_VLAN_203'. At the bottom, there are buttons for 'Back to Services', 'Enable', 'Copy', 'Save', and 'Cancel'. The footer indicates the copyright is 2023 Hewlett Packard Enterprise Development LP, the date is Oct 26, 2023 05:15:57 UTC, and the version is ClearPass Policy Manager 6.11.2.252294 on CLABV (Trial Version) platform.

Dans la dernière étape, la politique d'application créée précédemment est configurée pour le service.

Commutateur d'accès HPE Aruba Networking

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

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


T10197992_fr

2025-11 (M7.2)

© 2023 – 2025 Axis Communications AB