# Secure integration of Axis devices into Aruba networks

## Manuel d'utilisation

# Secure integration of Axis devices into Aruba networks

## Table des matières

# Secure integration of Axis devices into Aruba networks

## Présentation

### Présentation

Ce guide d'intégration vise à décrire les meilleures pratiques de configuration pour intégrer et exploiter les périphériques Axis dans les réseaux Aruba. 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 des équipements et applications du réseau Aruba. Voici quelques avantages pouvant être obtenus en combinant les périphériques et logiciels Axis avec une infrastructure réseau Aruba :

- 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 d'Aruba 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 Aruba, y compris des commutateurs d'accès Aruba et Aruba 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 seront fournies tout au long du guide.

# Intégration sécurisée - IEEE 802.1AR/802.1X

## Authentification initiale

Connectez le périphérique Axis pris en charge par Axis Edge Vault pour authentifier le périphérique sur le réseau Aruba. Le périphérique utilisera 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, Aruba 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 le firmware en cours d'exécution, sont utilisées pour prendre une décision basée sur des politiques.

Le périphérique Axis s'authentifie auprès du réseau Aruba 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 Aruba 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 réseau Aruba déplacera le périphérique Axis vers le réseau d'approvisionnement (VLAN201) sur lequel 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 du micrologiciel. 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 déclenchera une nouvelle tentative d'authentification. Aruba ClearPass Policy Manager vérifiera les nouveaux certificats et décidera de déplacer ou non le périphérique Axis dans le réseau de production.

*Après sa configuration, le périphérique Axis quittera le réseau de mise en service et tentera de se réauthentifier sur le réseau Aruba.*

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 connectera au périphérique Axis et commencera 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*

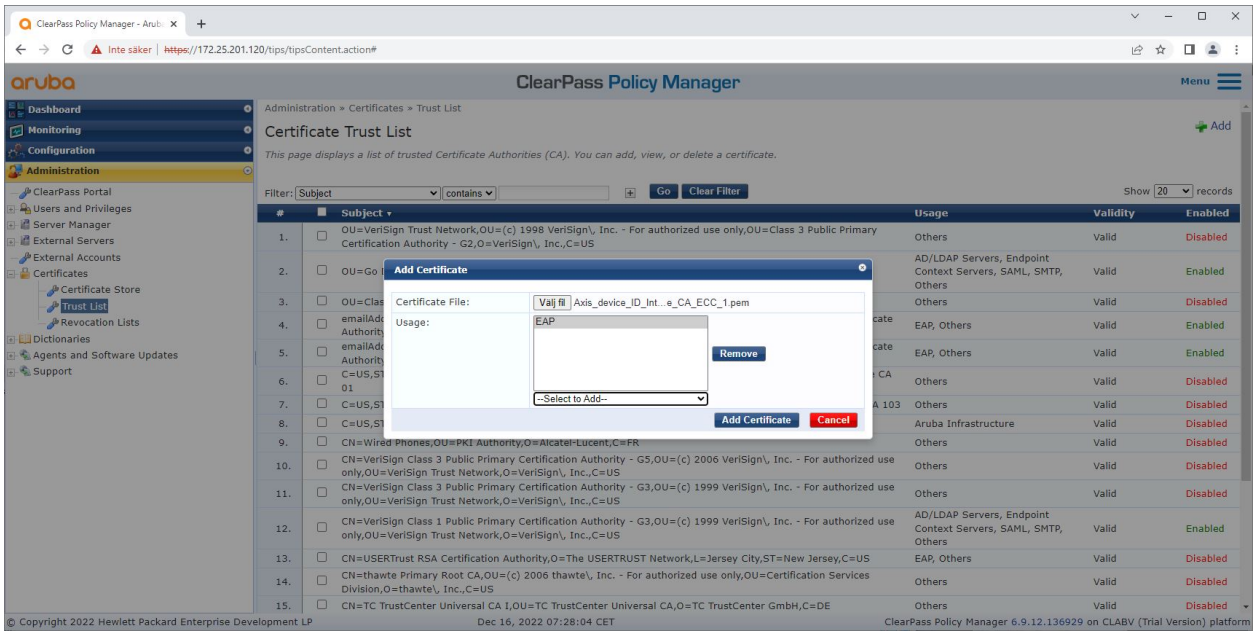
## Configuration HPE Aruba

### Gestionnaire de politiques Aruba ClearPass

ClearPass Policy Manager d'Aruba 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

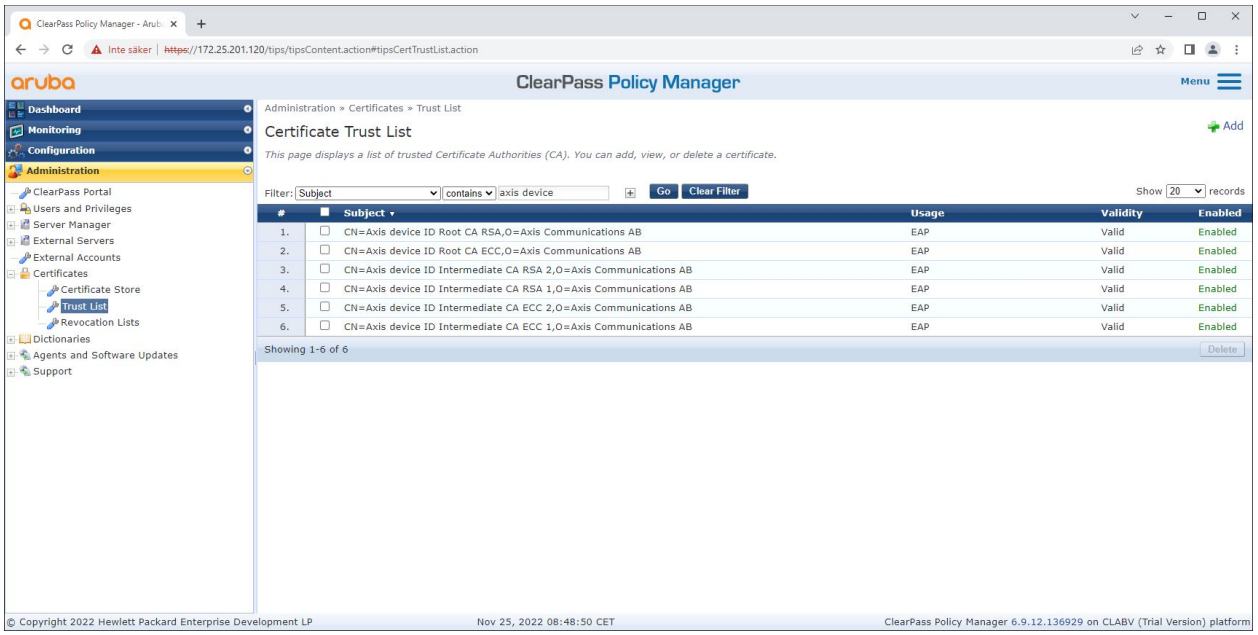
1. Téléchargez la chaîne de certificats IEEE 802.1AR spécifique à Axis depuis axis.com.
2. Téléchargez les chaînes de certificats CA racine et CA intermédiaire IEEE 802.1AR spécifiques à Axis dans le magasin de certificats de confiance.
3. Activez Aruba ClearPass Policy Manager pour authentifier les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




*Téléchargement des certificats IEEE 802.1AR spécifiques à Axis vers le magasin de certificats de confiance d'Aruba ClearPass Policy Manager.*

# Secure integration of Axis devices into Aruba networks

## Intégration sécurisée - IEEE 802.1AR/802.1X




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

**Configuration du périphérique/groupe réseau**

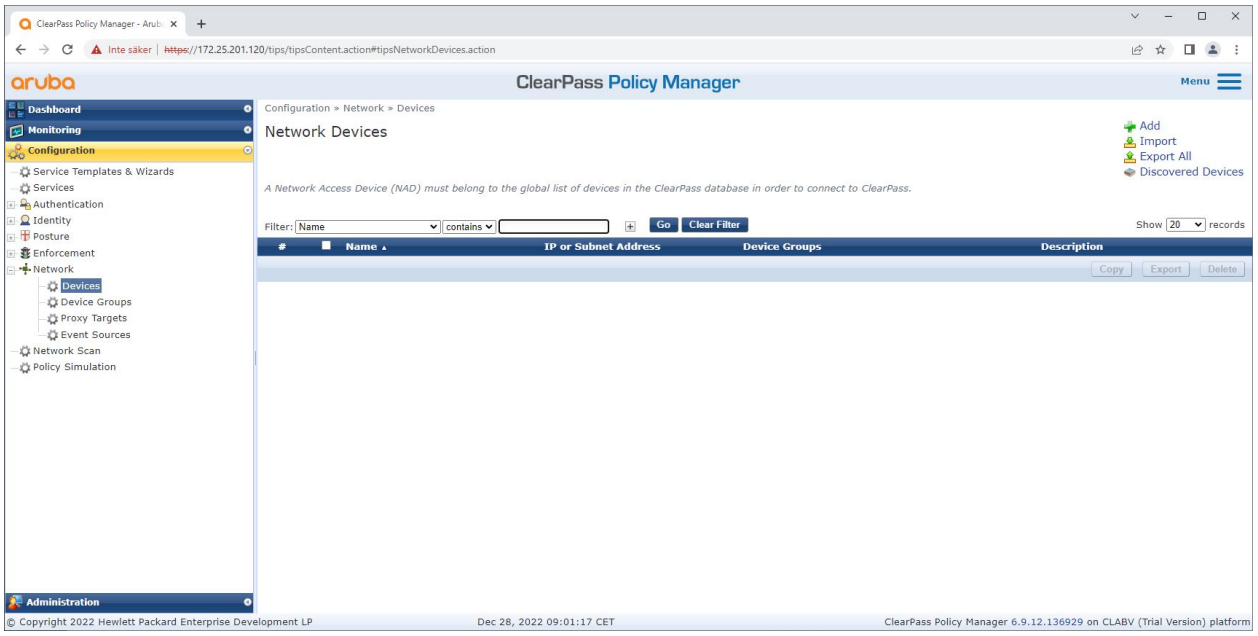
1. Ajoutez des périphériques d'accès réseau fiables, tels que des commutateurs d'accès Aruba, à ClearPass Policy Manager. ClearPass Policy Manager doit connaître les commutateurs d'accès Aruba du réseau qui seront utilisés pour la communication IEEE 802.1X.

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.

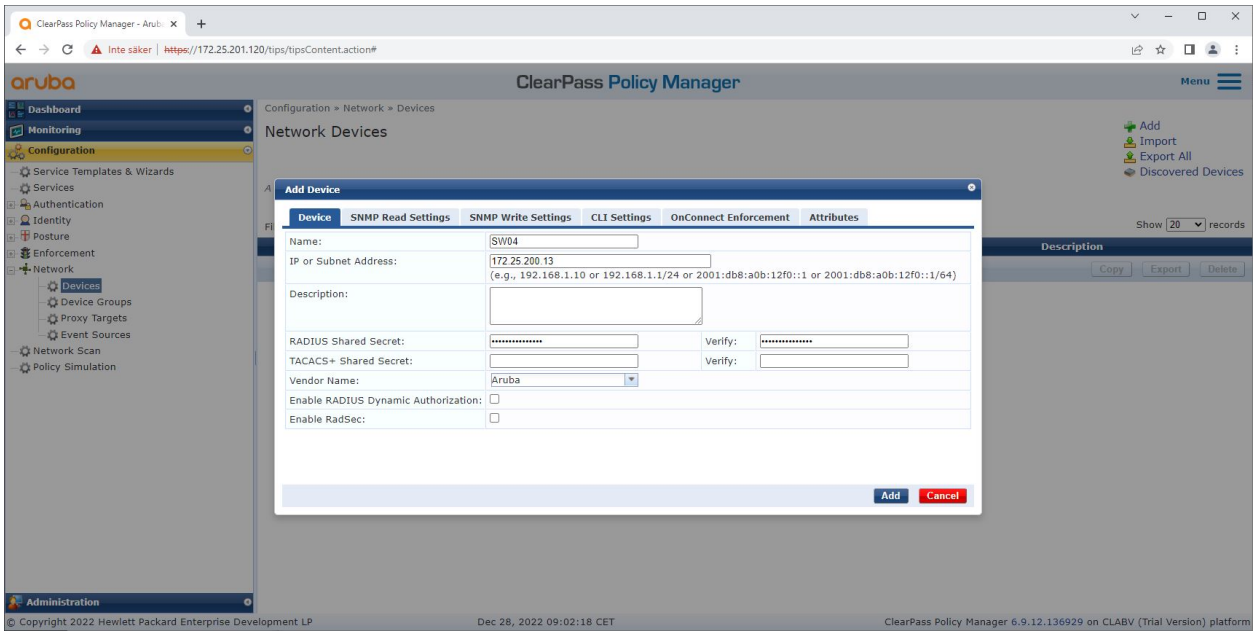
3. Le secret partagé RADIUS doit correspondre à la configuration IEEE 802.1X spécifique du commutateur.

# Secure integration of Axis devices into Aruba networks

## Intégration sécurisée - IEEE 802.1AR/802.1X



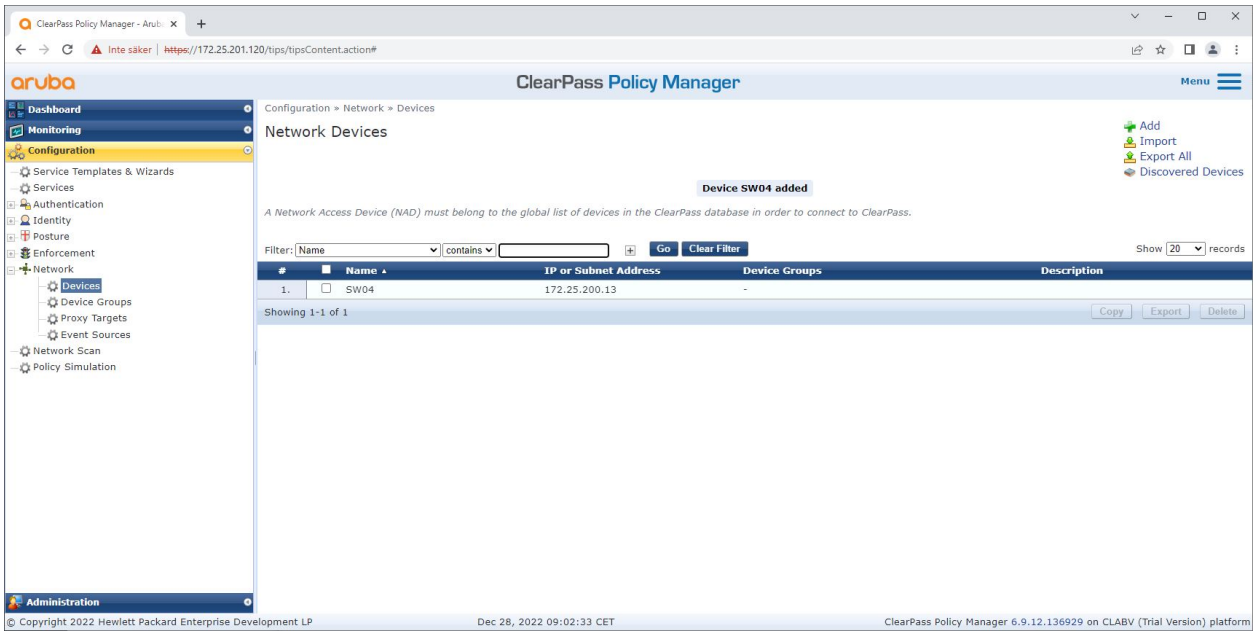

*Interface des périphériques réseau approuvés dans Aruba ClearPass Policy Manager.*



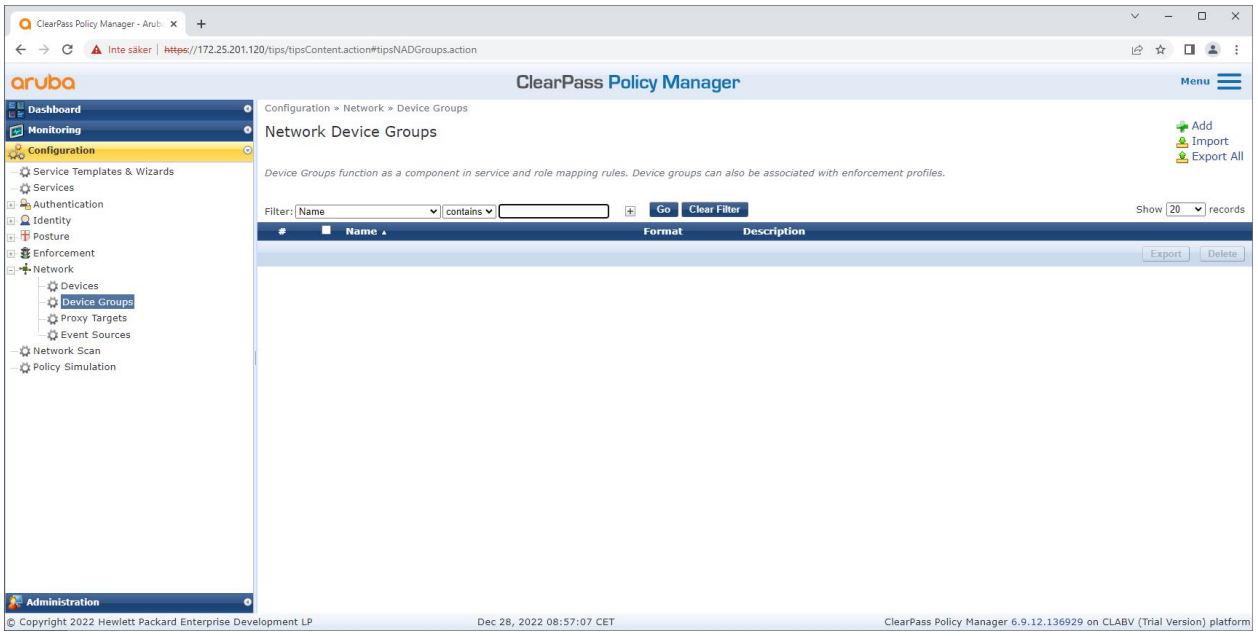

*Ajout du commutateur d'accès Aruba en tant que périphérique réseau approuvé dans Aruba ClearPass Policy Manager. Notez que le secret partagé RADIUS doit correspondre à la configuration IEEE 802.1X spécifique du commutateur.*

# Secure integration of Axis devices into Aruba networks

## Intégration sécurisée - IEEE 802.1AR/802.1X



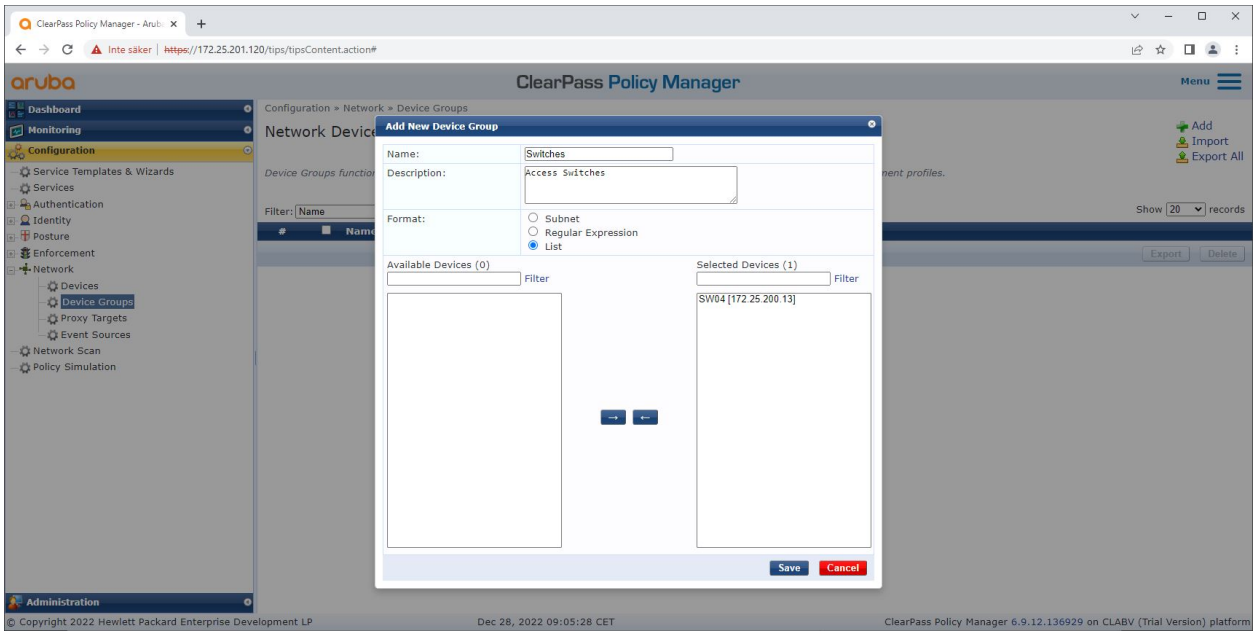

*Aruba ClearPass Policy Manager avec un périphérique réseau approuvé configuré.*



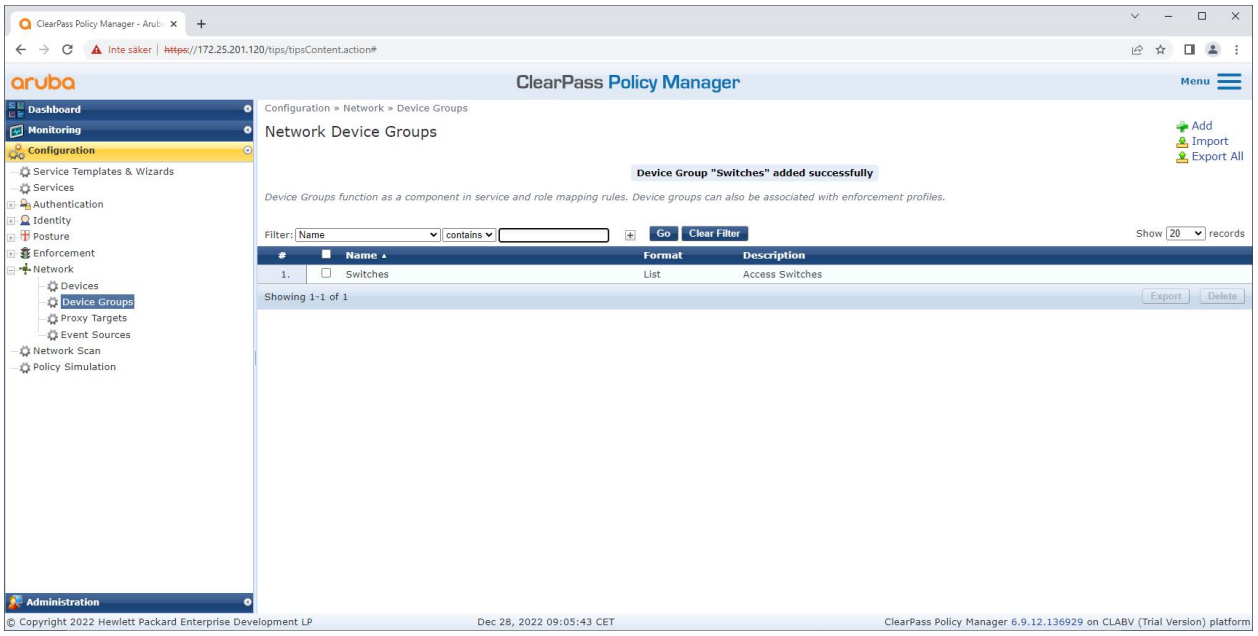

*Interface des groupes de périphériques réseau approuvés dans Aruba ClearPass Policy Manager.*

# Secure integration of Axis devices into Aruba networks

## Intégration sécurisée - IEEE 802.1AR/802.1X




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




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

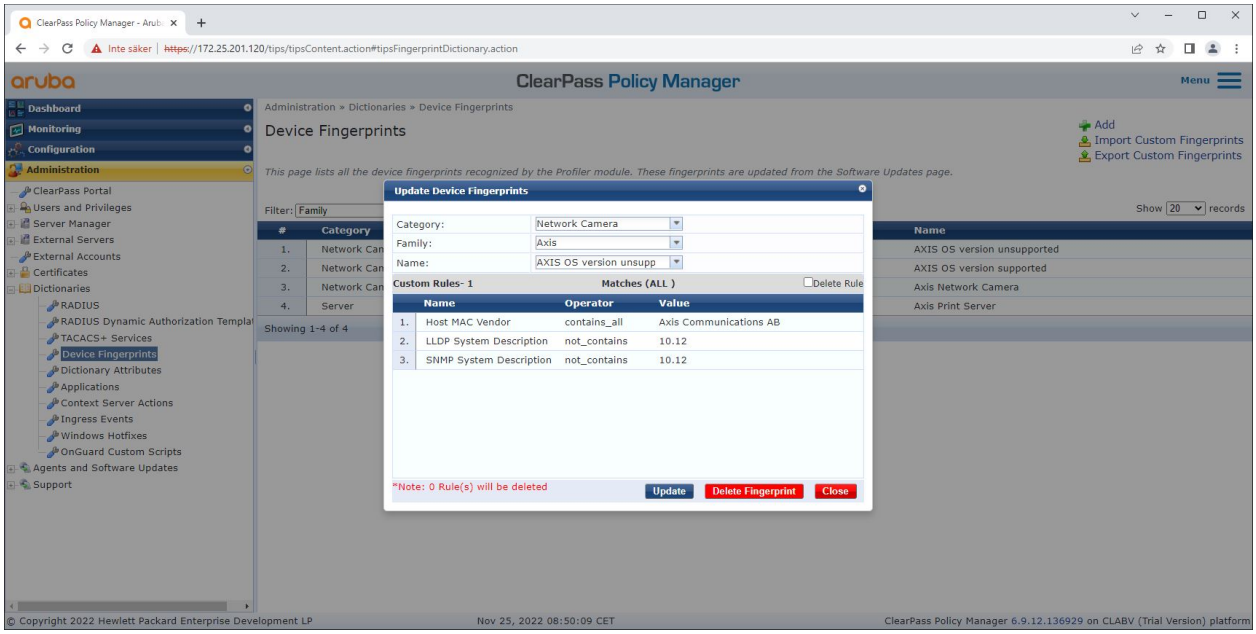
**Configuration des empreintes digitales du périphérique**

Le périphérique Axis peut distribuer des informations spécifiques au périphérique, telles que l'adresse MAC et la version du micrologiciel, via la découverte réseau. Une empreinte de périphérique peut être créée à partir de l'interface des empreintes de périphérique dans Aruba ClearPass Policy Manager. Il est possible de mettre à jour et de gérer l'empreinte du périphérique. Il est possible par exemple d'accorder ou de refuser l'accès en fonction de la version du système d'exploitation AXIS.

## Intégration sécurisée - IEEE 802.1AR/802.1X

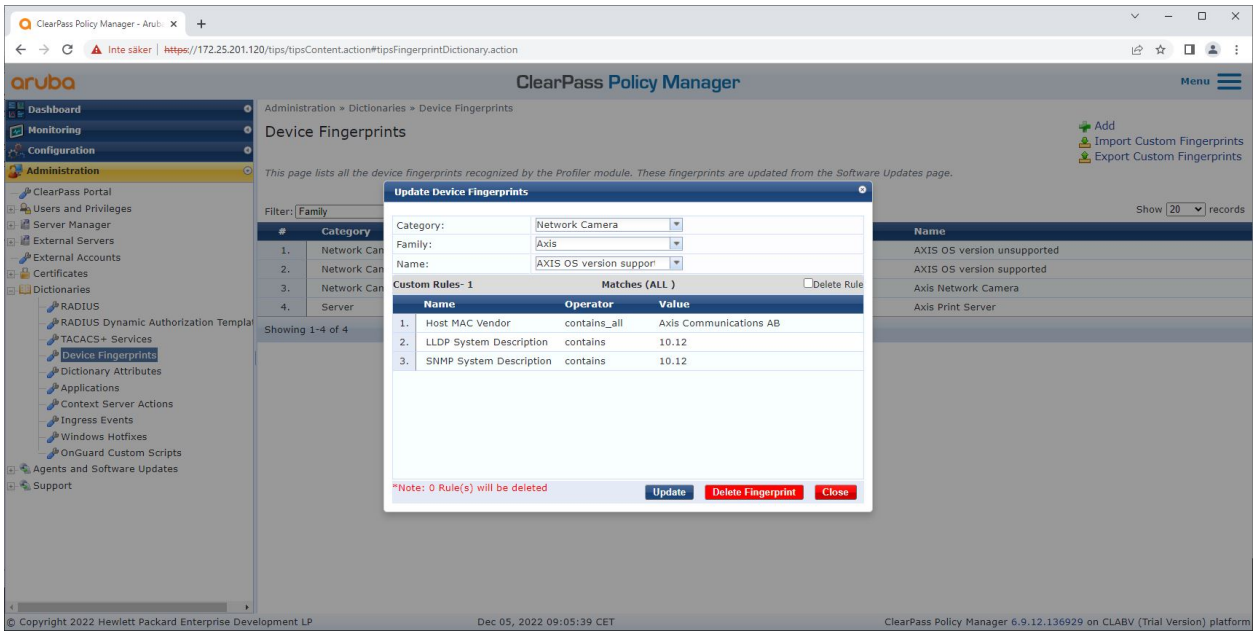
Il est aussi possible de mettre à jour et de gérer l'empreinte du périphérique. Il est possible par exemple d'accorder ou de refuser l'accès en fonction de la version du système d'exploitation AXIS.

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 Aruba ClearPass Policy Manager. Les périphériques Axis exécutant une autre version du firmware autre que 10.12 sont considérés comme non pris en charge.*

## Intégration sécurisée - IEEE 802.1AR/802.1X




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

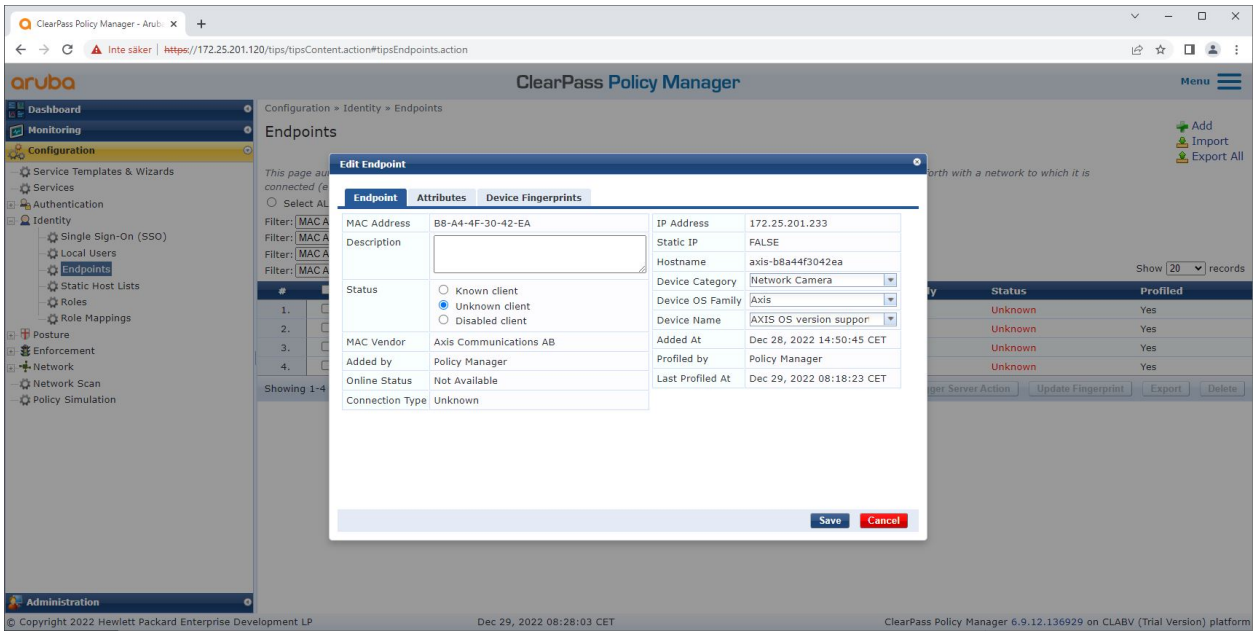
Les informations sur l'empreinte de périphérique collectées par Aruba ClearPass Manager sont disponibles dans la section Points de terminaison.

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

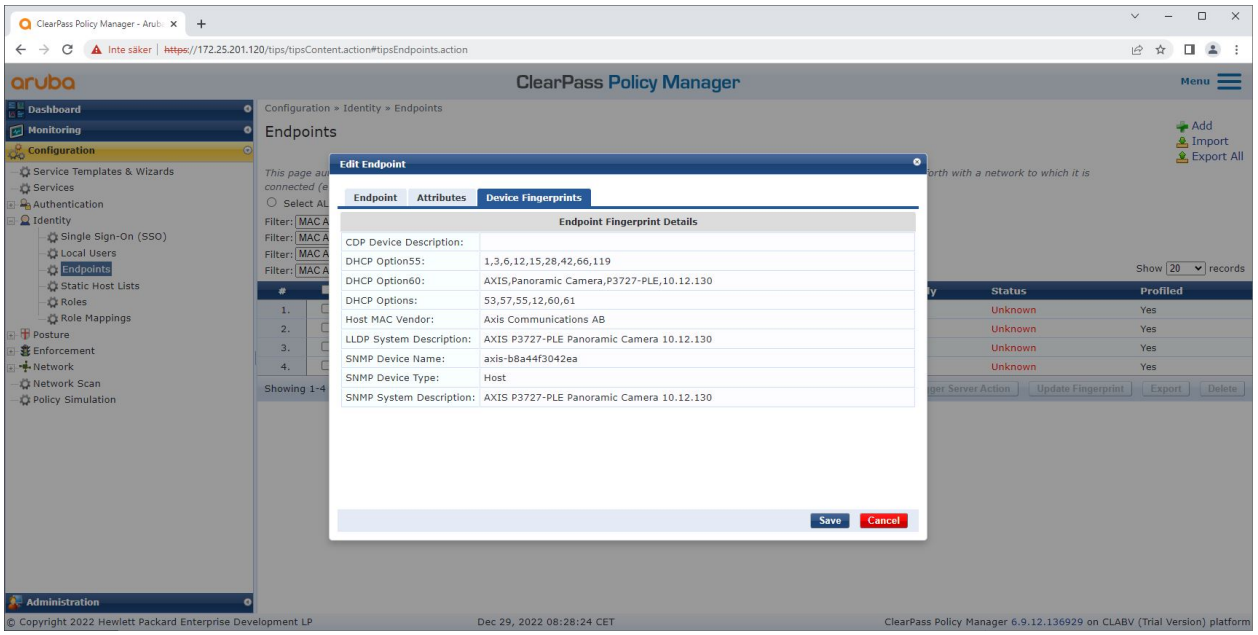
Remarque

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

## Intégration sécurisée - IEEE 802.1AR/802.1X




*Périphérique Axis qui a été profilé par Aruba ClearPass Policy Manager.*



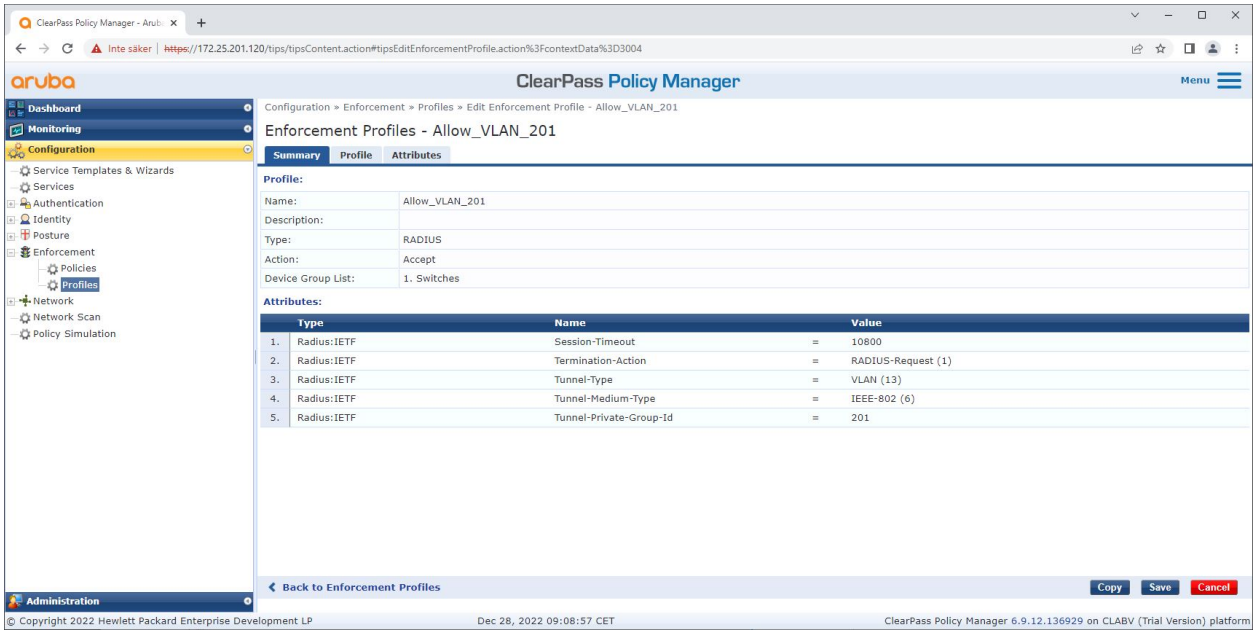

*Empreintes détaillées d'un périphérique Axis profilé. Veuillez noter que SNMP est désactivé par défaut sur les périphériques Axis. Les informations de découverte spécifiques à LLDP, CDP et DHCP sont partagées par le périphérique Axis dans leur état d'usine par défaut et relayées par le commutateur d'accès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

### Configuration du profil d'application

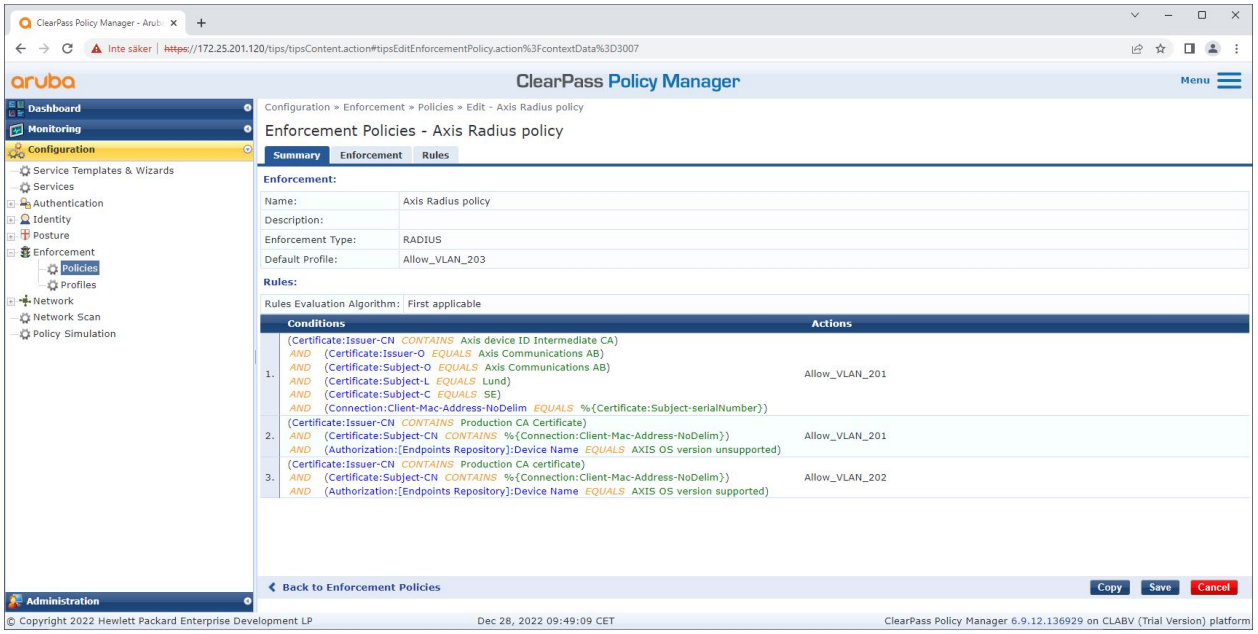
Le profil d'application est utilisé pour permettre à Aruba ClearPass Policy Manager d'attribuer un ID VLAN spécifique à un port d'accès sur le commutateur. Il s'agit d'une décision basée sur des politiques qui s'applique aux périphériques réseau du groupe de périphériques « commutateurs ». Le nombre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

## Intégration sécurisée - IEEE 802.1AR/802.1X

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 Aruba ClearPass Policy Manager définit si les périphériques Axis ont accès aux réseaux Aruba 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 Aruba ClearPass Policy Manager.*

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

**Accès au réseau refusé**

# Secure integration of Axis devices into Aruba networks

## Intégration sécurisée - IEEE 802.1AR/802.1X

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 de firmware, des certificats de niveau production et d'autres configurations. Les conditions suivantes sont vérifiées par Aruba ClearPass Policy Manager :

- Version de firmware 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)**

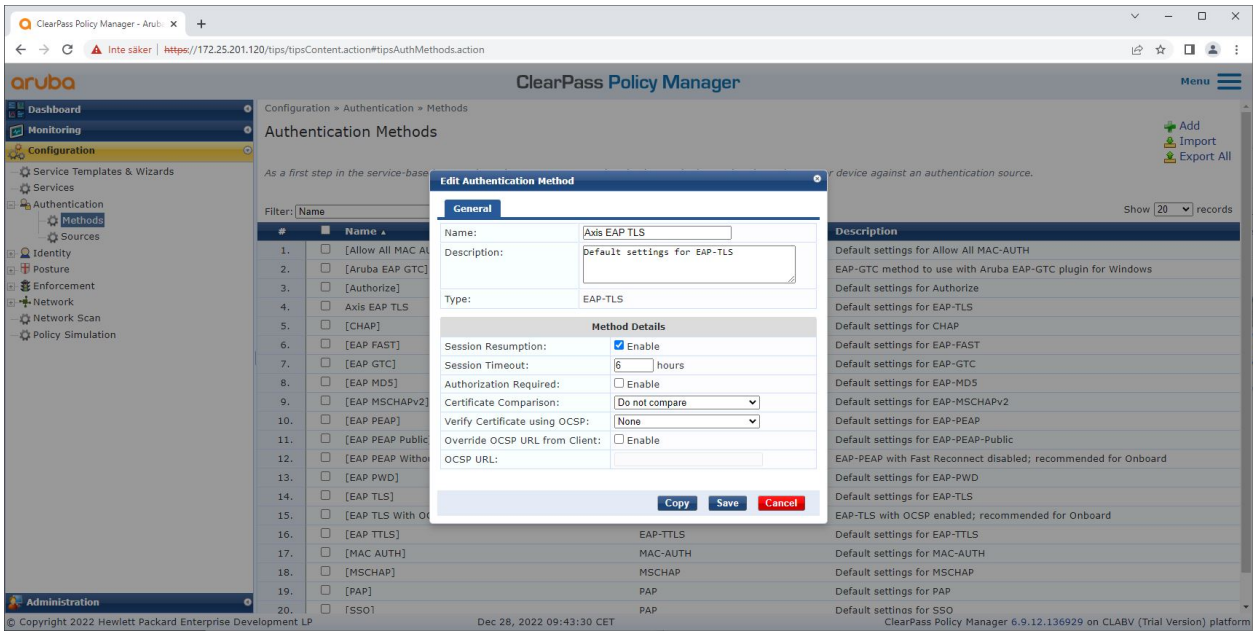
Le périphérique Axis a accès au réseau de production au sein duquel il fonctionnera. L'accès est accordé une fois la mise en service du périphérique effectuée à partir du réseau de mise en service (VLAN 201). Les conditions suivantes sont vérifiées par Aruba ClearPass Policy Manager :

- 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 de firmware du périphérique Axis.
- 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 tentera de s'authentifier sur le réseau Aruba. 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.

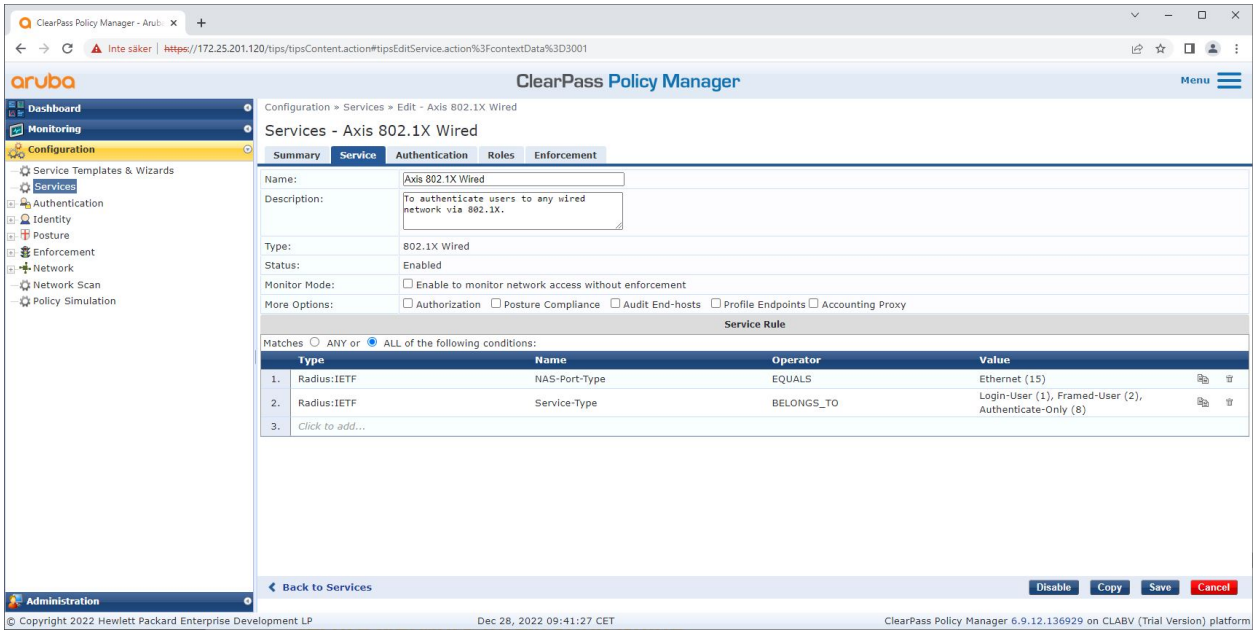
## Intégration sécurisée - IEEE 802.1AR/802.1X




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

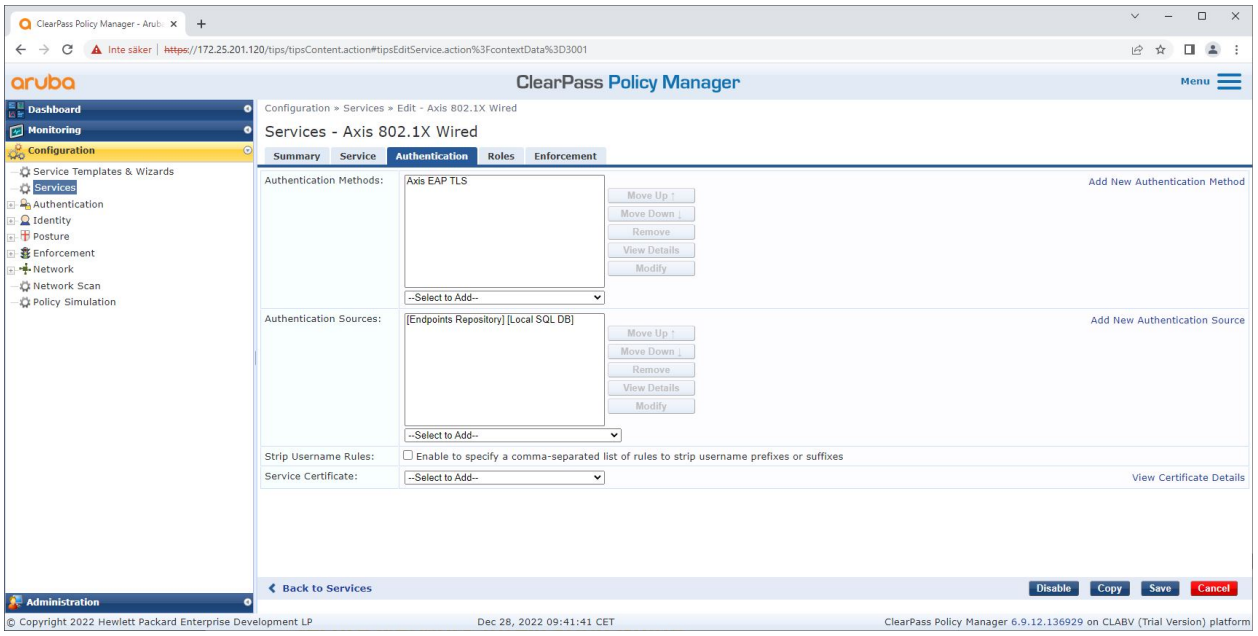
### Configuration du service

Dans l'interface 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 Aruba.

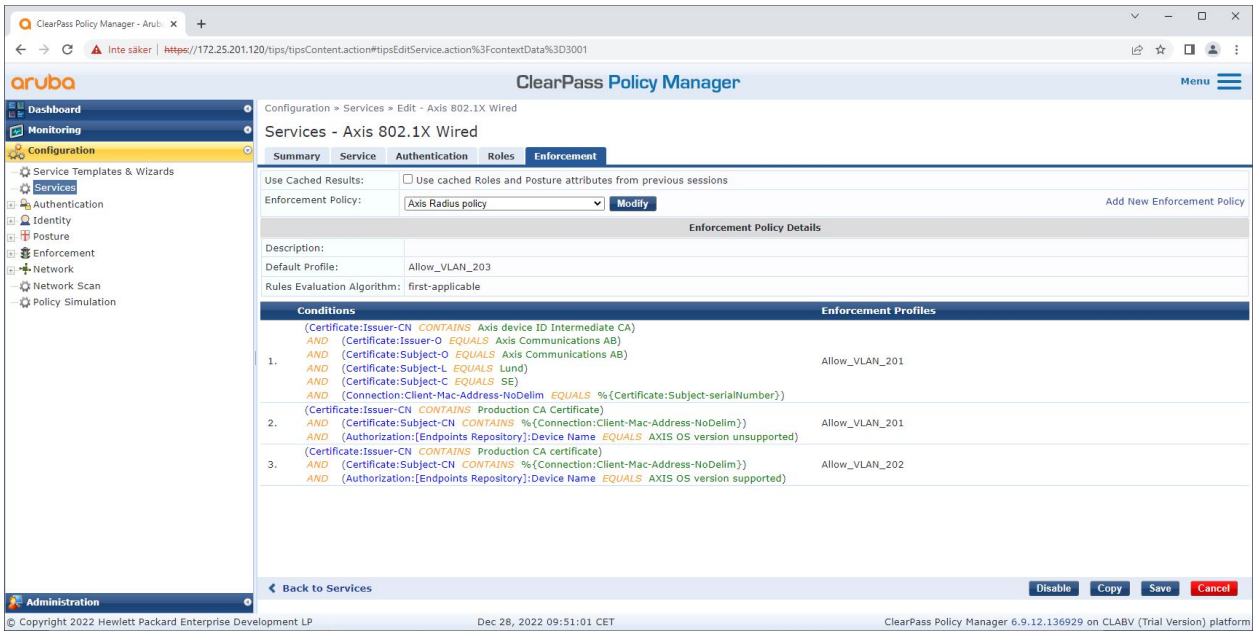



*Un service Axis dédié est créé et définit IEEE 802.1X comme méthode de connexion.*

## Intégration sécurisée - IEEE 802.1AR/802.1X




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




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

### Commutateur d'accès Aruba

Les périphériques Axis sont directement connectés à des commutateurs d'accès Aruba compatibles PoE, ou via des médiateurs Axis PoE compatibles. Pour intégrer en toute sécurité les périphérique Axis au sein des réseaux Aruba, 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 Aruba ClearPass Policy Manager qui fait office de serveur RADIUS.

# Intégration sécurisée - IEEE 802.1AR/802.1X

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 Aruba.

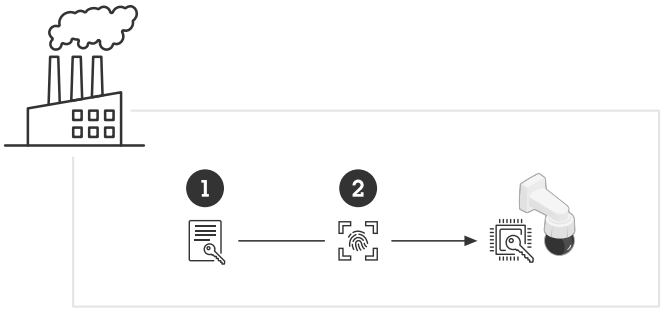
```
hôte du serveur radius Clé MyRADIUSIPAddress « MyRADIUSKey »

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.




*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*

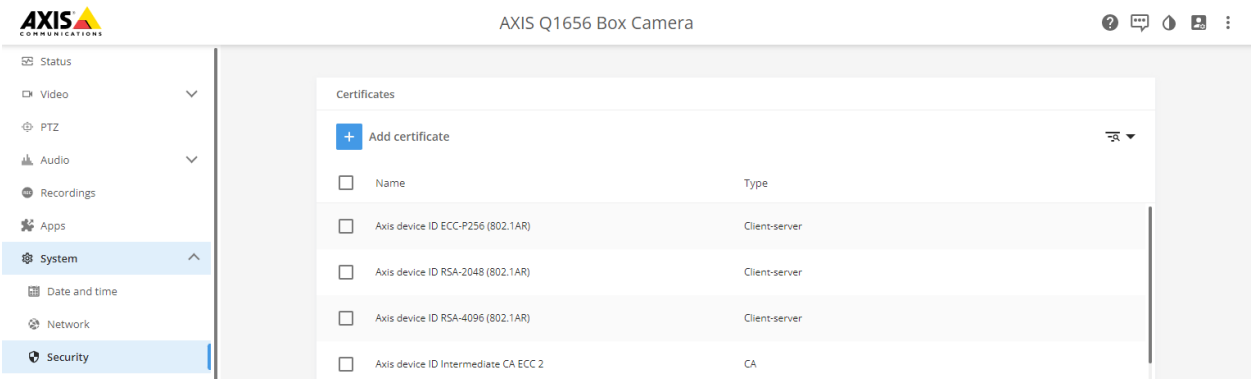
Le magasin de clés sécurisé protégé par matériel et fourni par un élément sécurisé du périphérique Axis est mis en service en usine avec un certificat unique au périphérique et des clés correspondantes (ID de périphérique Axis) qui peuvent globalement prouver l'authenticité du périphérique Axis. Le *sélecteur 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.

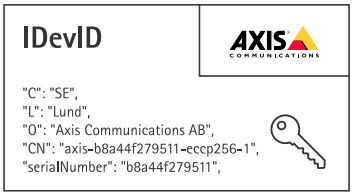
# Secure integration of Axis devices into Aruba networks

## Intégration sécurisée - IEEE 802.1AR/802.1X




*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 Aruba 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.

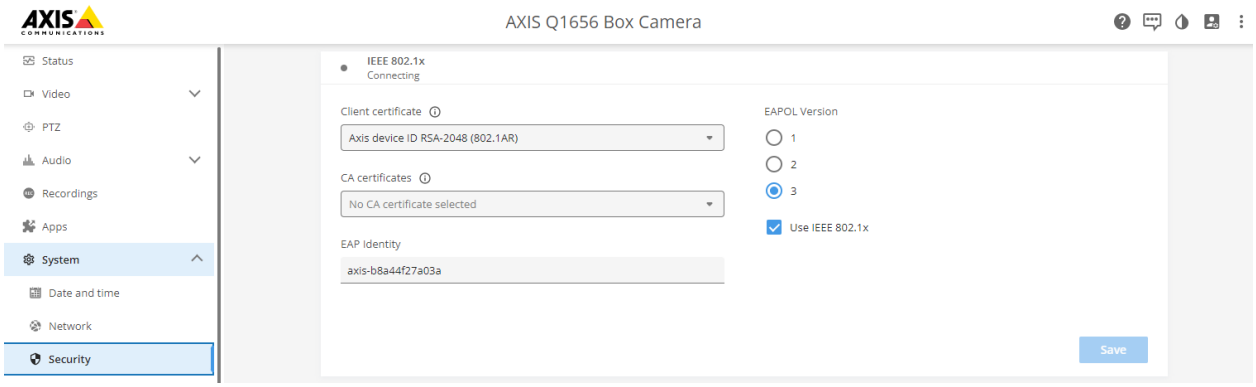



| | |
|---|---|
| Pays | SE |
| Localisation | Lund |
| Organisation émettrice | Axis Communications AB |
| Nom commun de l'émetteur | Intermédiaire de l'ID de périphérique Axis |
| Organisation | Axis Communications AB |
| Nom commun | axis-b8a44f279511-eccp256-1 |
| Numéro de série | b8a44f279511 |

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.

# Secure integration of Axis devices into Aruba networks

## Intégration sécurisée - IEEE 802.1AR/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* 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 du firmware.
- 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.

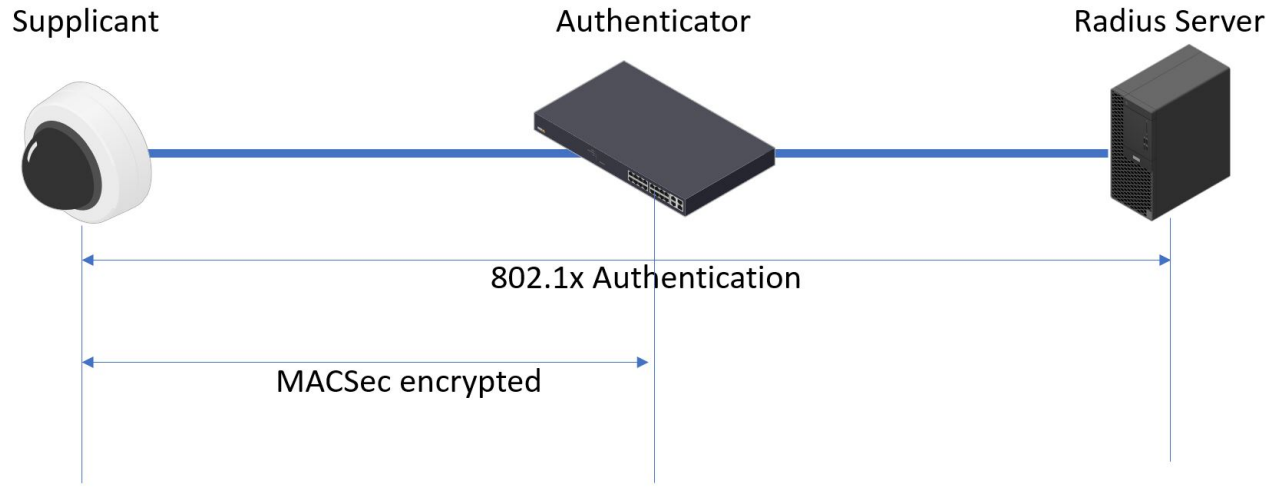
## Fonctionnement réseau sécurisé - IEEE 802.1AE MACsec

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.

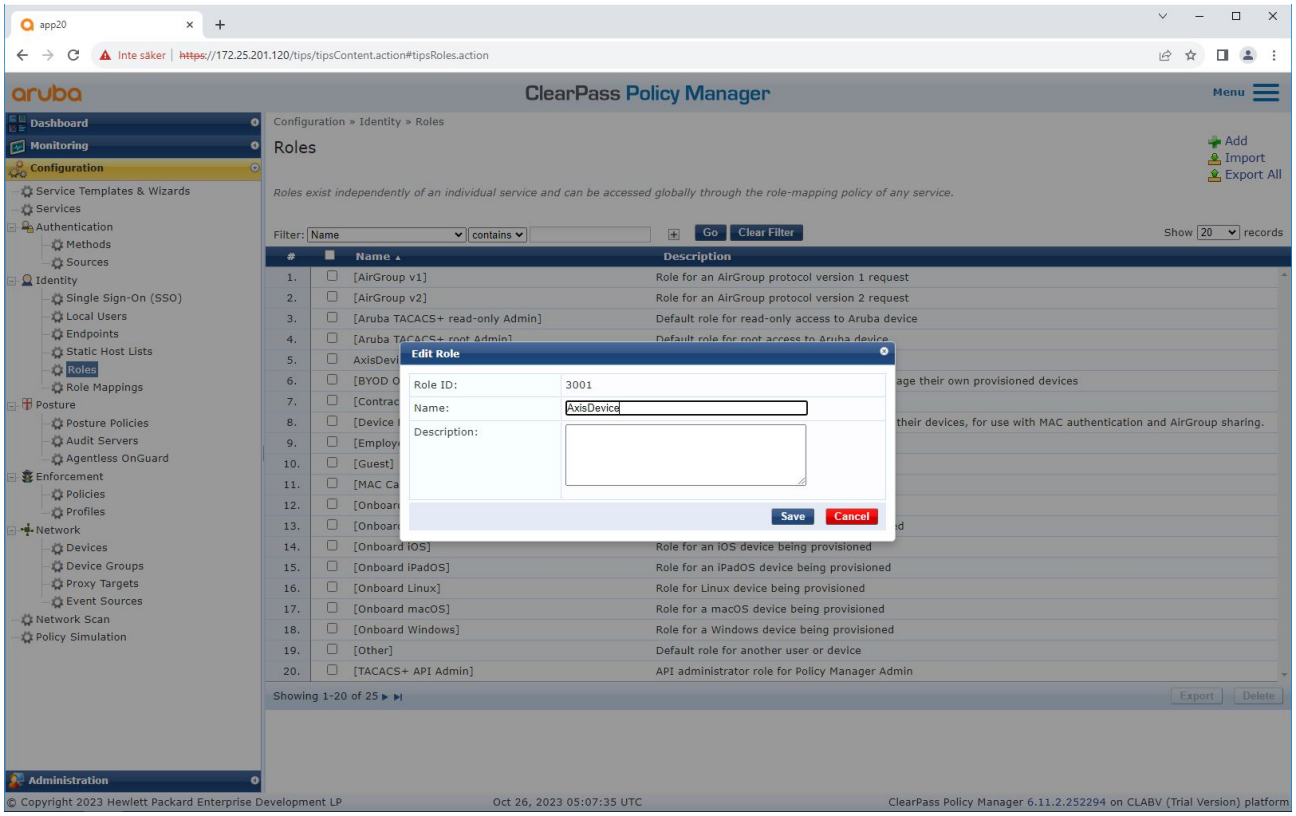
L'ID de périphérique Axis stocké de manière sécurisée (1), identité de périphérique sécurisée conforme IEEE 802.1AR, est utilisé pour l'authentification auprès du réseau Aruba (4, 5) via le contrôle d'accès au réseau basé sur le port EAP-TLS IEEE 802.1X (2). Lors de la session EAP-TLS, les clés MACsec sont échangées automatiquement pour établir un lien sécurisé (3), protégeant tout le trafic réseau depuis le périphérique Axis vers le commutateur Aruba.

IEEE 802.1AE MACsec requiert à la fois un commutateur d'accès Aruba 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 Aruba ne prend pas en charge MACsec à l'aide d'EAP-TLS, le mode Clé pré-partagée peut être utilisé et configuré manuellement.

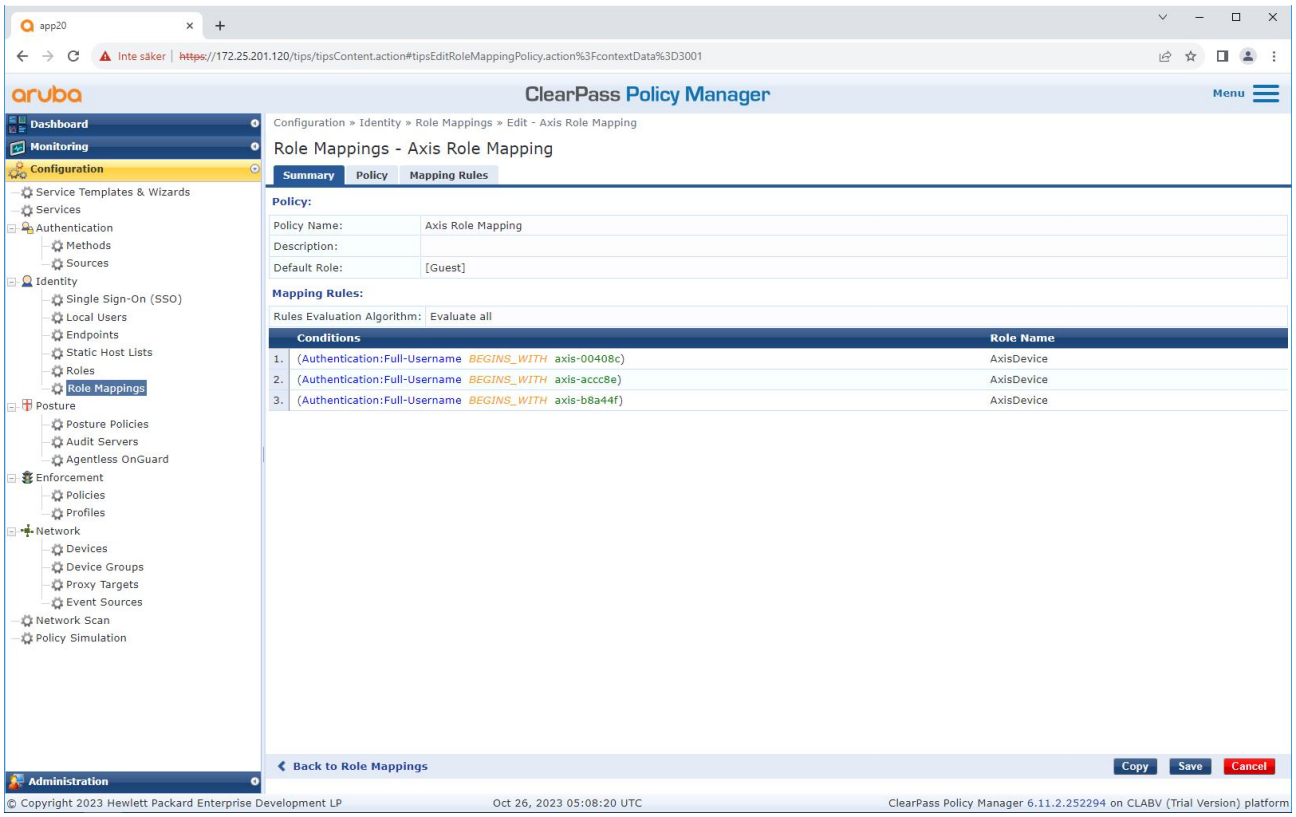
## Gestionnaire de politiques Aruba ClearPass

### Politique de rôle et de mappage de rôles




*Ajout d'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 Aruba.*

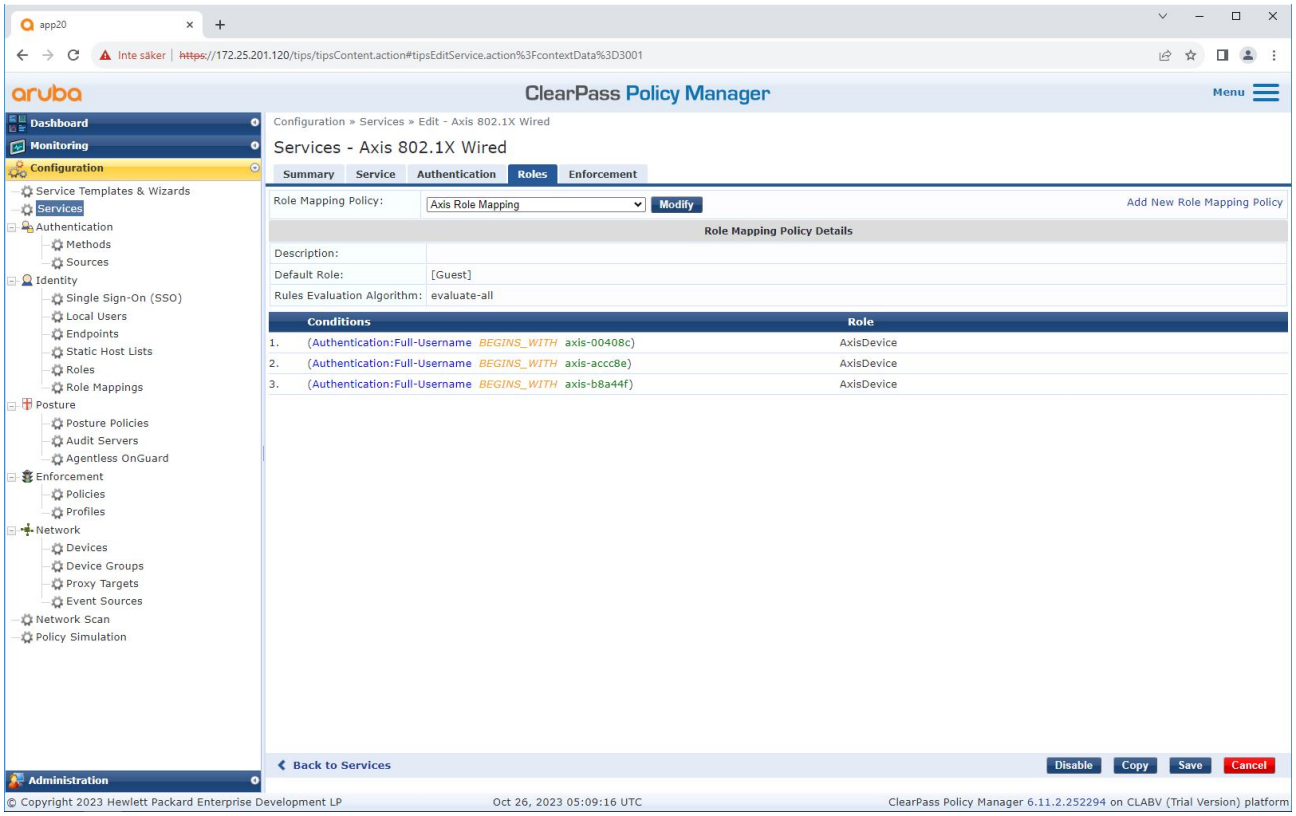
## Fonctionnement réseau sécurisé - IEEE 802.1AE MACsec




*Ajout d'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 fera partie du rôle [Invité].*

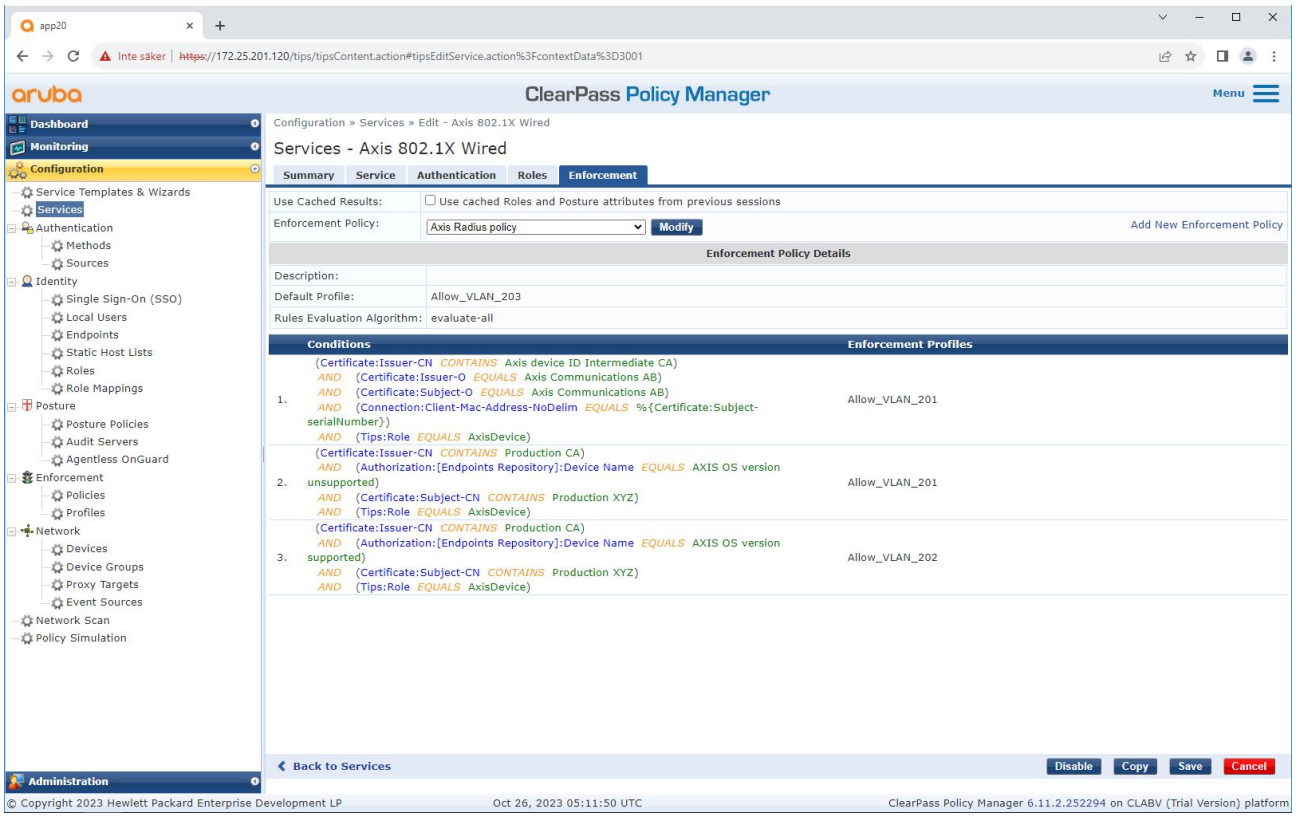
Par défaut, les périphériques Axis utilisent le format d'identité EAP « axis-serialnumber ». Le numéro de série d'un périphérique Axis est son adresse MAC. Par exemple « axis-b8a44f45b4e6".

### Configuration du service



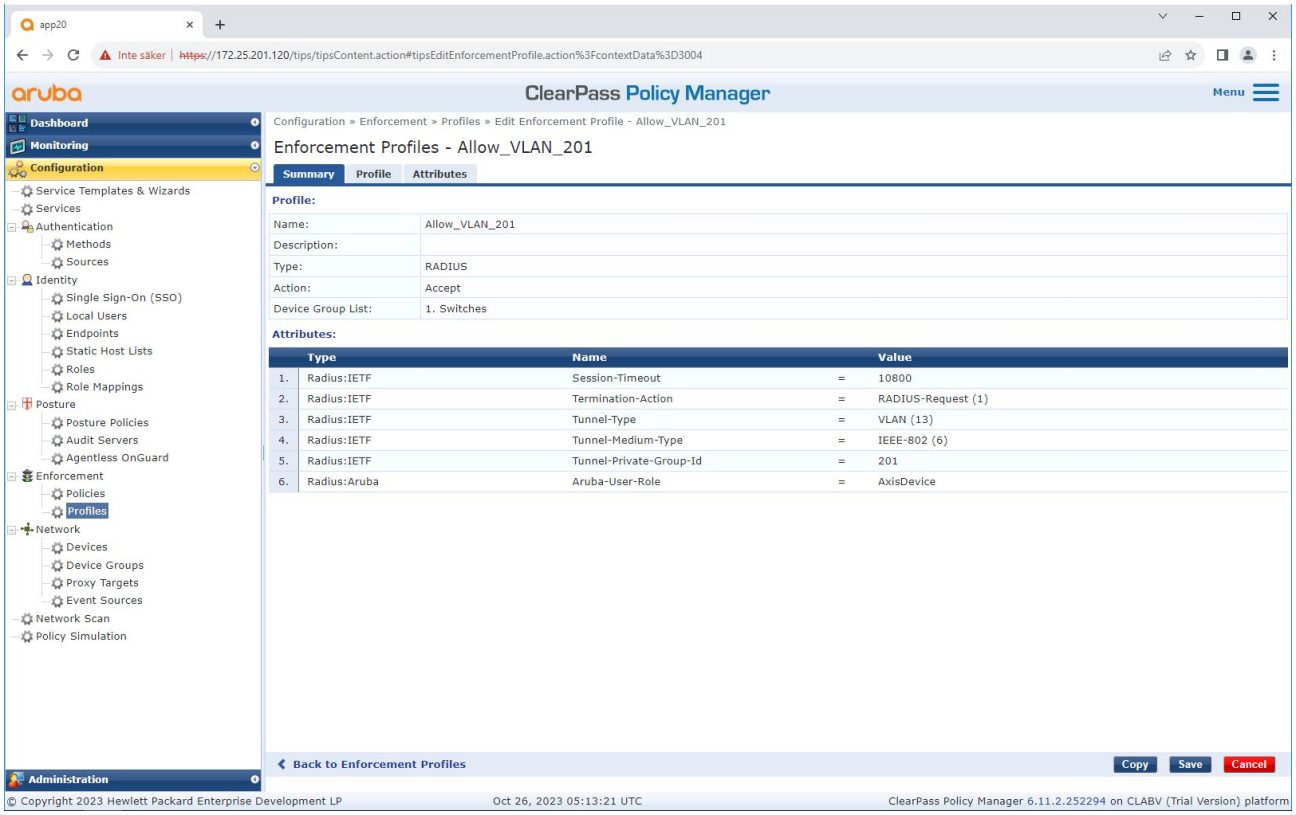

*Ajout de la stratégie de mappage de rôle Axis créée précédemment au service qui définit IEEE 802.1X comme méthode de connexion pour l'intégration des périphériques Axis.*

## Fonctionnement réseau sécurisé - IEEE 802.1AE MACsec




*Ajout du nom du rôle Axis comme condition aux définitions de stratégie existantes.*

### Profil d'application




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

## Commutateur d'accès Aruba

En plus de la configuration d'intégration sécurisée décrite dans *Commutateur d'accès Aruba à la page 16*, reportez-vous à l'exemple de configuration de port ci-dessous pour le commutateur d'accès Aruba 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

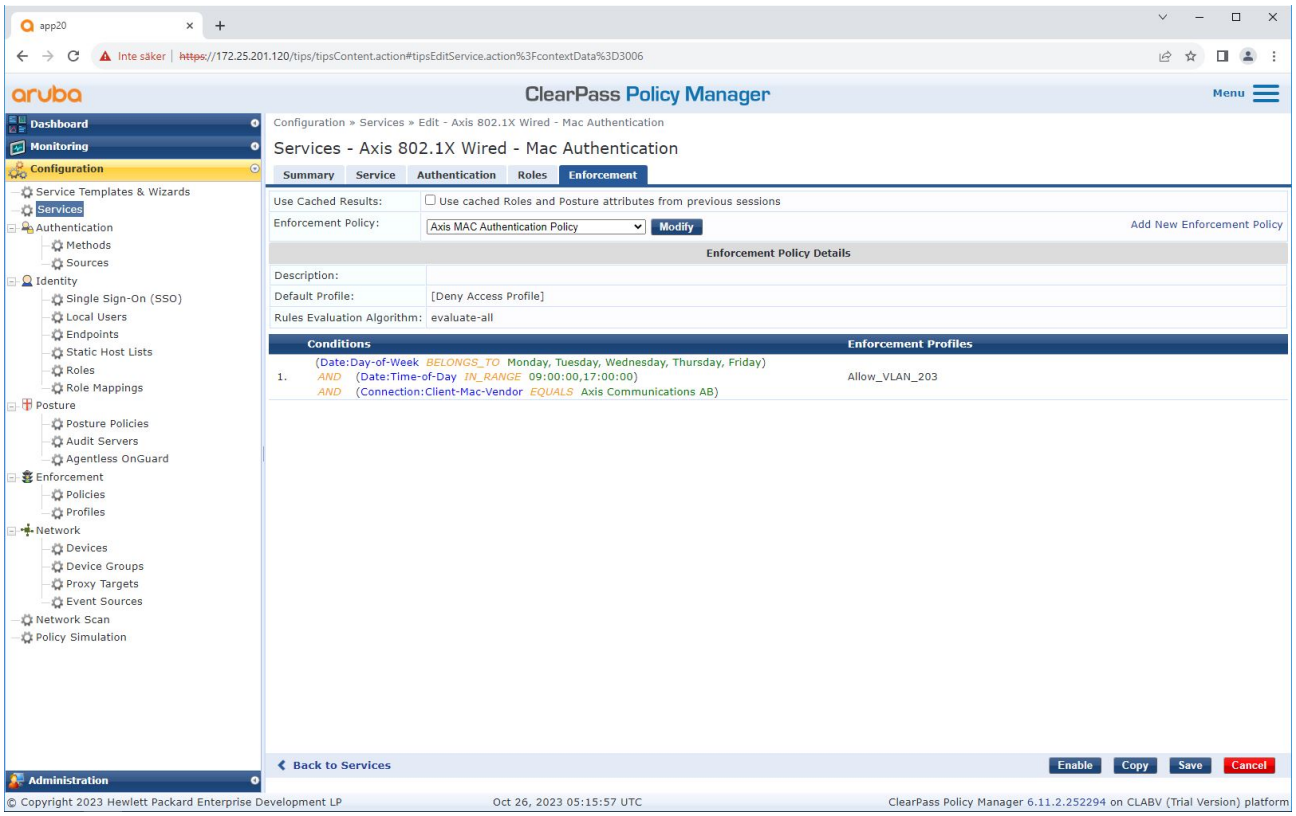
Vous pouvez utiliser MAC Authentication Bypass (MAB) pour intégrer des périphériques Axis qui ne prennent pas en charge l'intégration d'IEEE 802.1AR avec le certificat d'ID de périphérique Axis et IEEE 802.1X activé à l'état d'usine par défaut. Si l'intégration 802.1X échoue, Aruba ClearPass Policy Manager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

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

## Gestionnaire de politiques Aruba ClearPass

### Politique d'application

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




#### 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

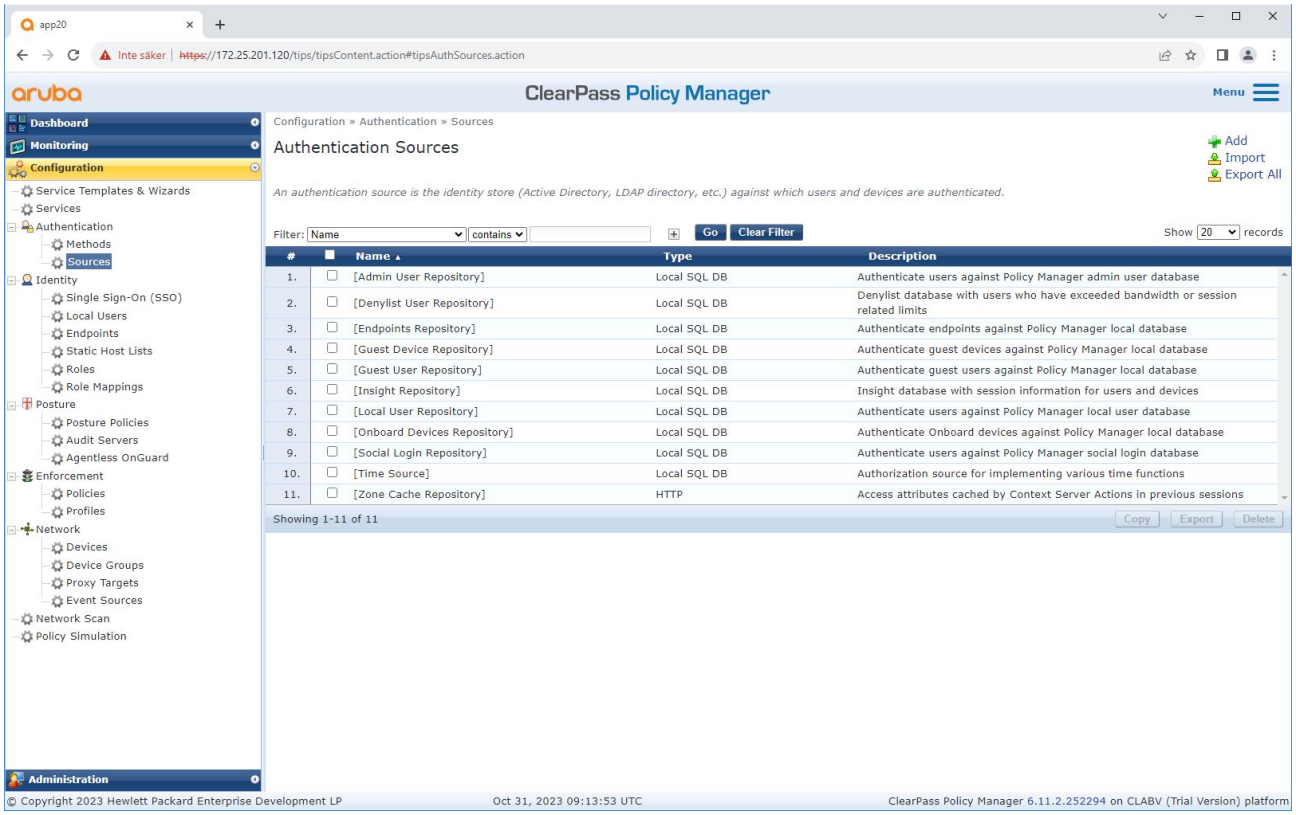
## Intégration héritée – Authentification MAC

- Le fournisseur d'adresse MAC correspond à Axis Communications AB.

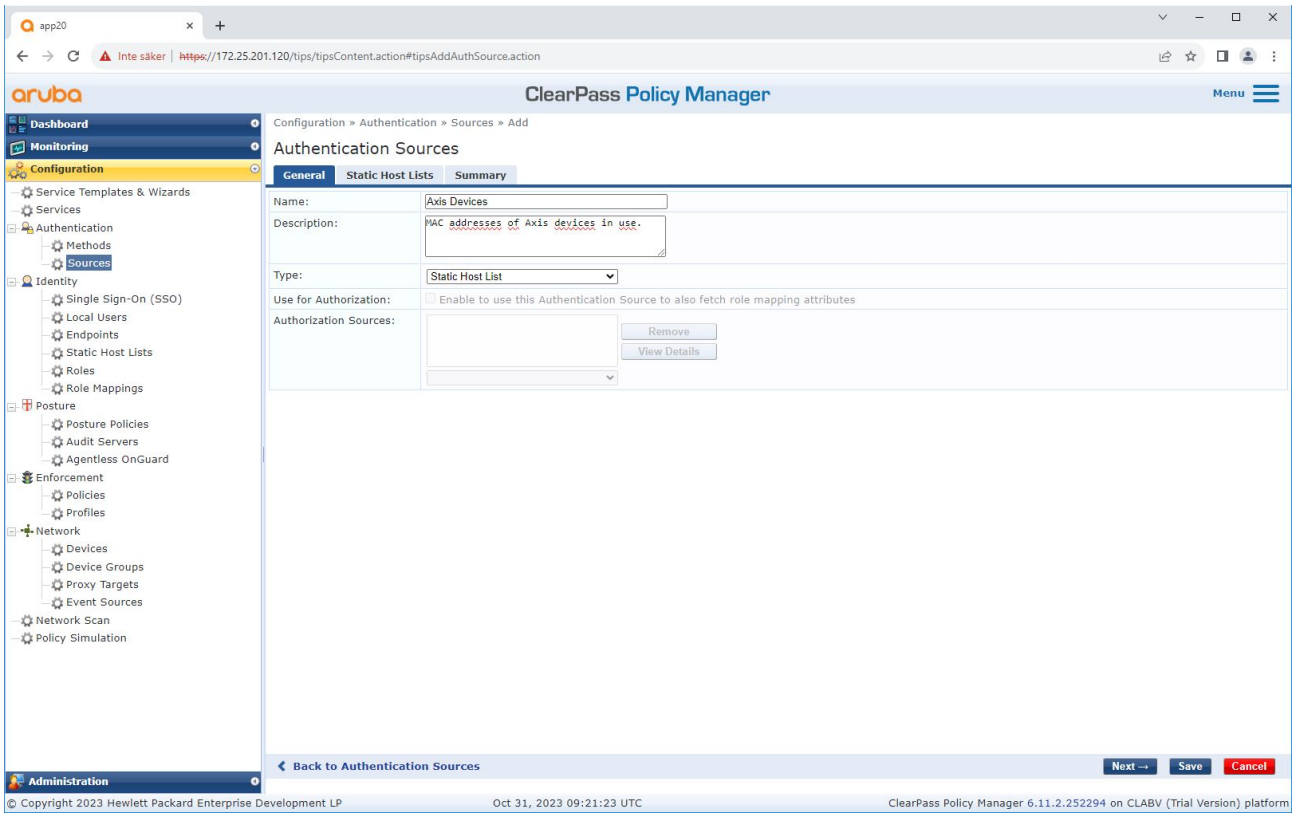
Étant donné que les adresses MAC peuvent être usurpées, l'accès au réseau de mise en service habituel n'est pas accordé. Nous vous recommandons d'utiliser MAB uniquement pour l'intégration initiale et d'inspecter manuellement le périphérique plus en détail.

### Configuration source

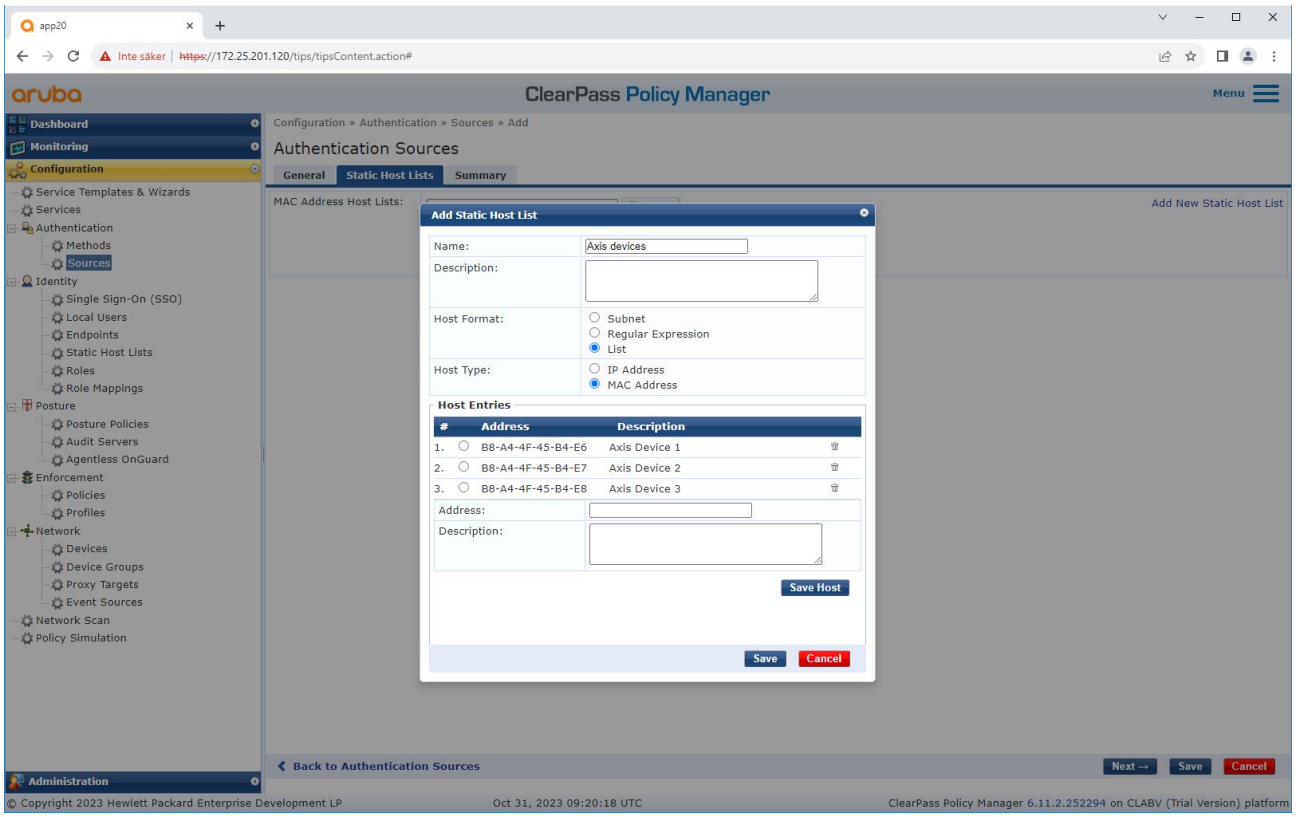
Dans l'interface Sources, une nouvelle source d'authentification est créée pour autoriser uniquement les adresses MAC importées manuellement.



## Intégration héritée – Authentification MAC

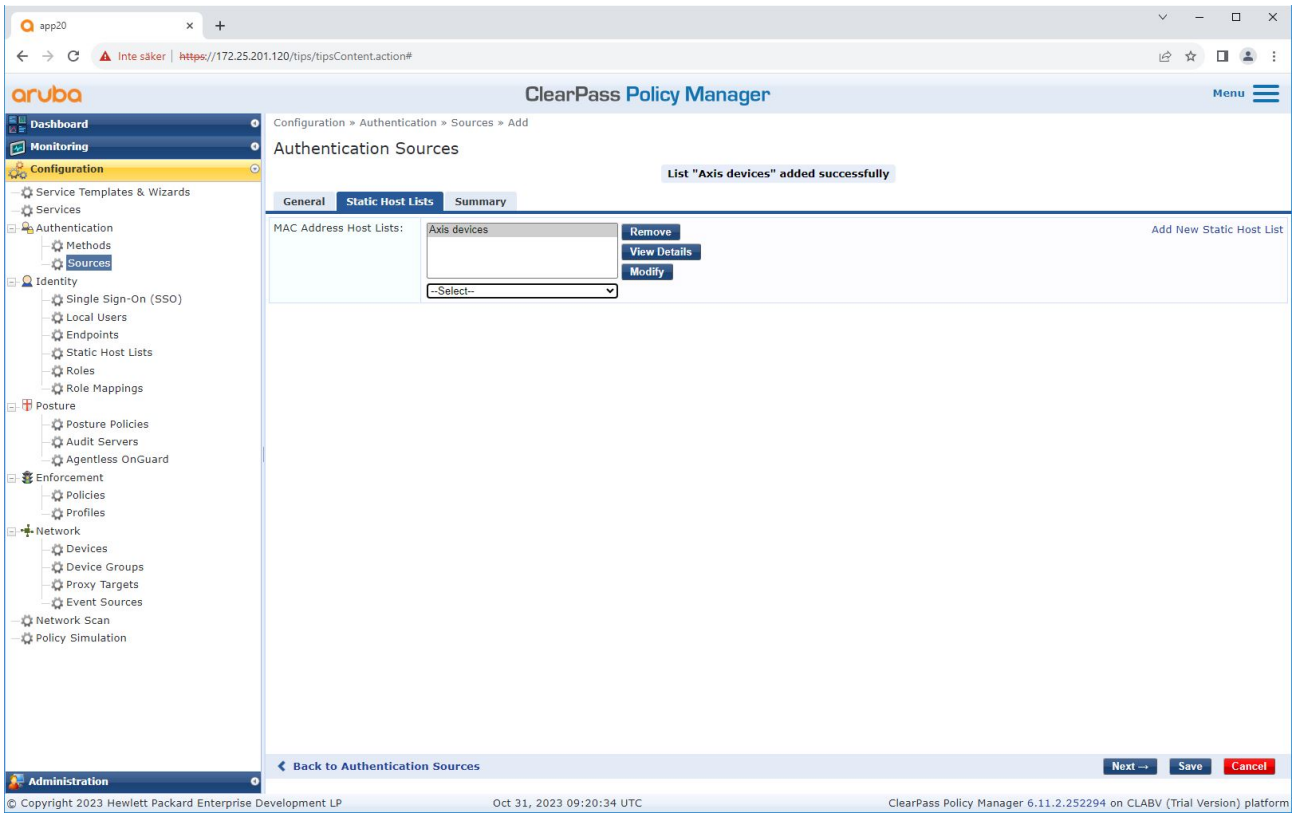


## Intégration héritée – Authentification MAC




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

## Intégration héritée – Authentification MAC

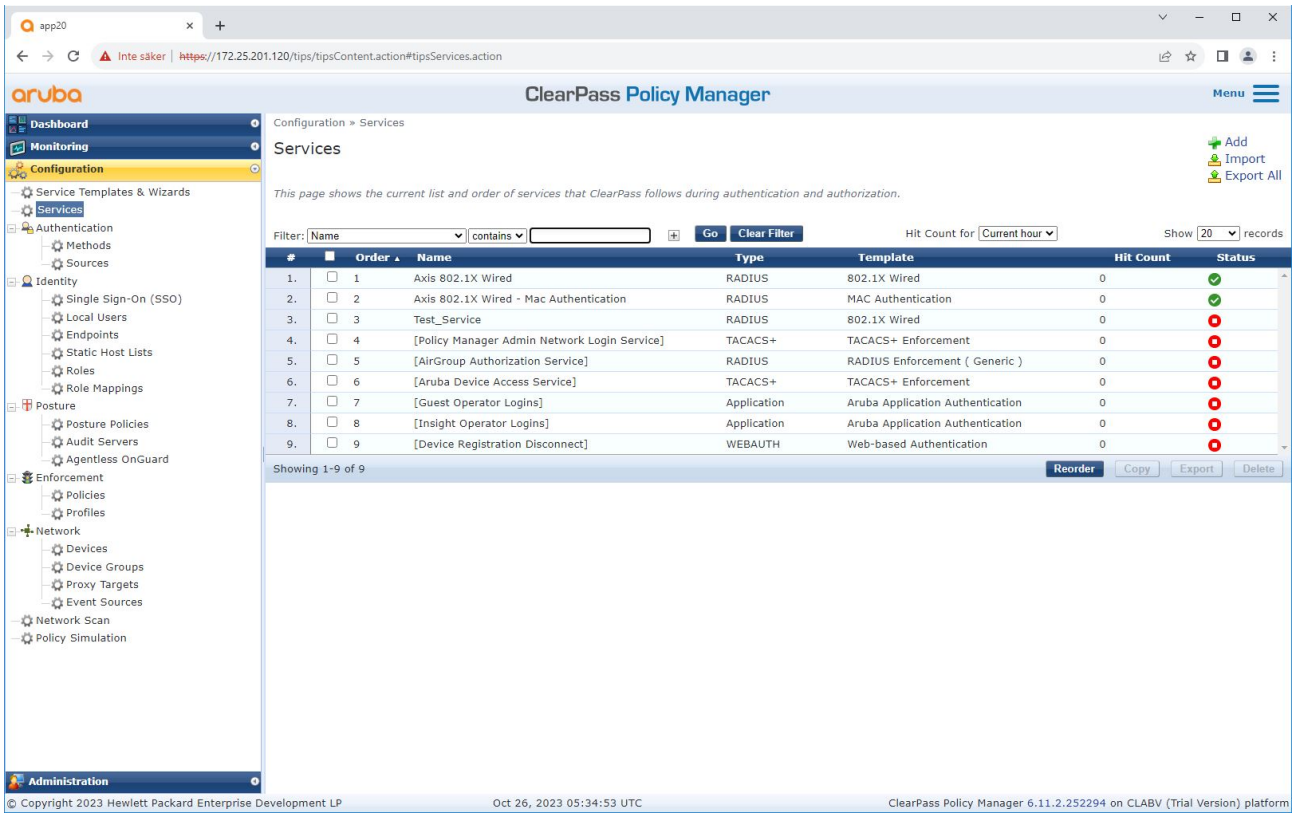



### Configuration du service

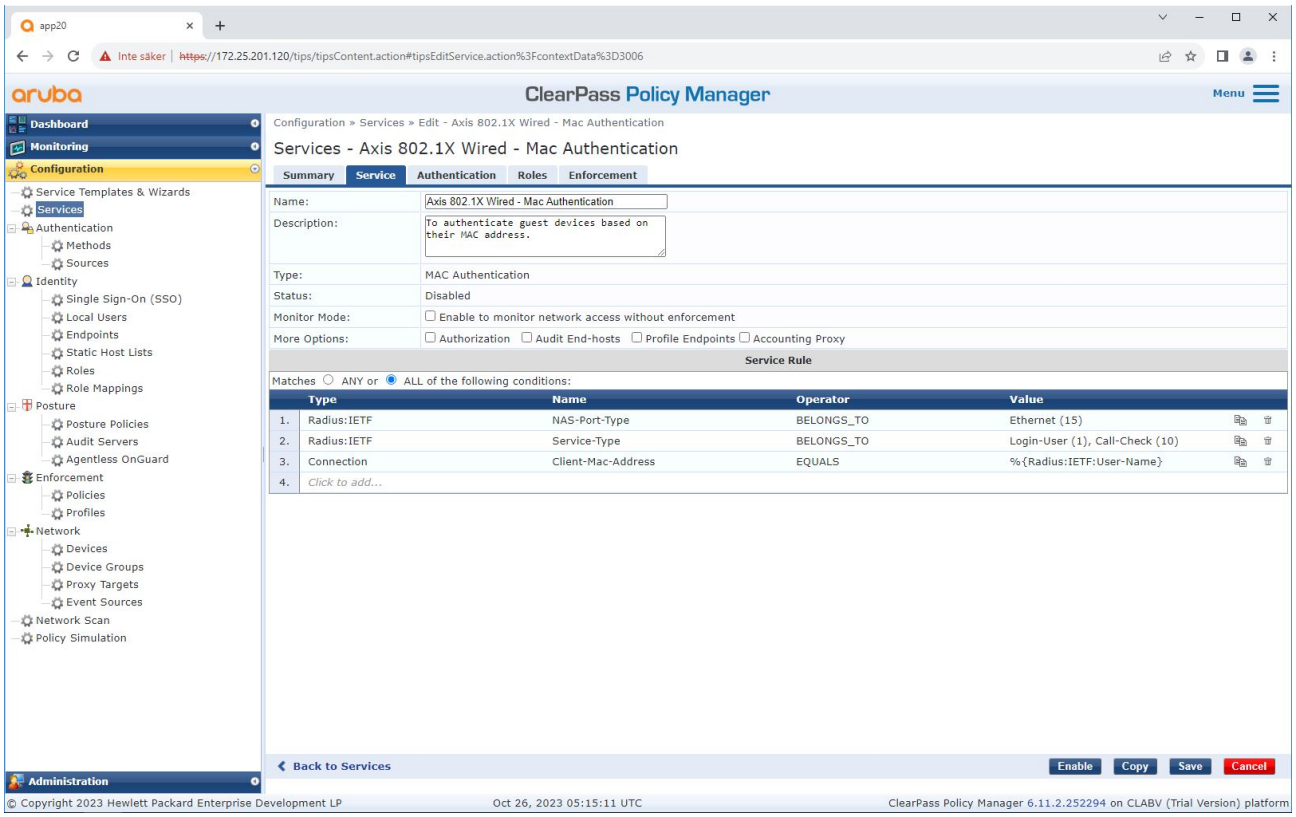
Dans l'interface Services, les étapes de configuration sont regroupées dans un seul service qui gère l'authentification et l'autorisation des périphériques Axis au sein des réseaux Aruba.

# Secure integration of Axis devices into Aruba networks

## Intégration héritée – Authentification MAC

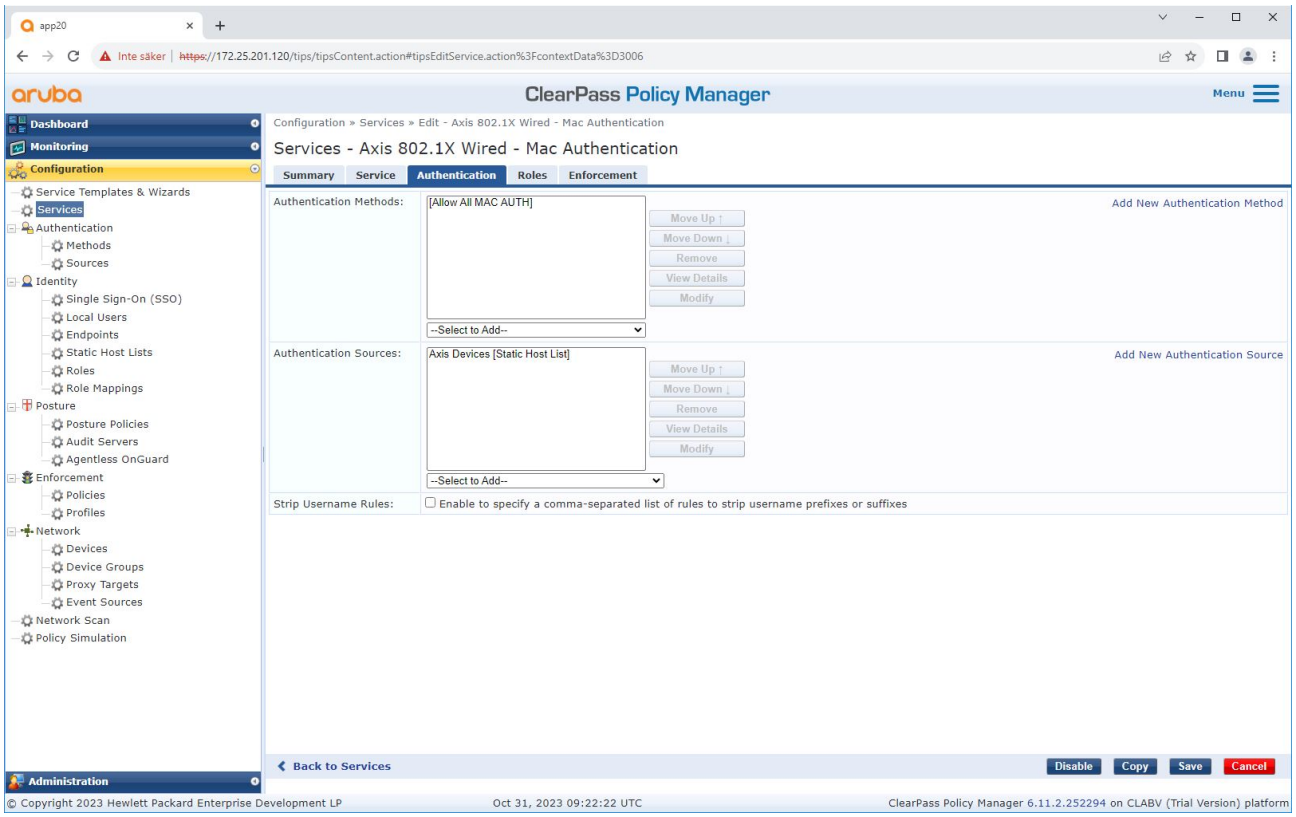


## Intégration héritée – Authentification MAC




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

## Intégration héritée – Authentification MAC

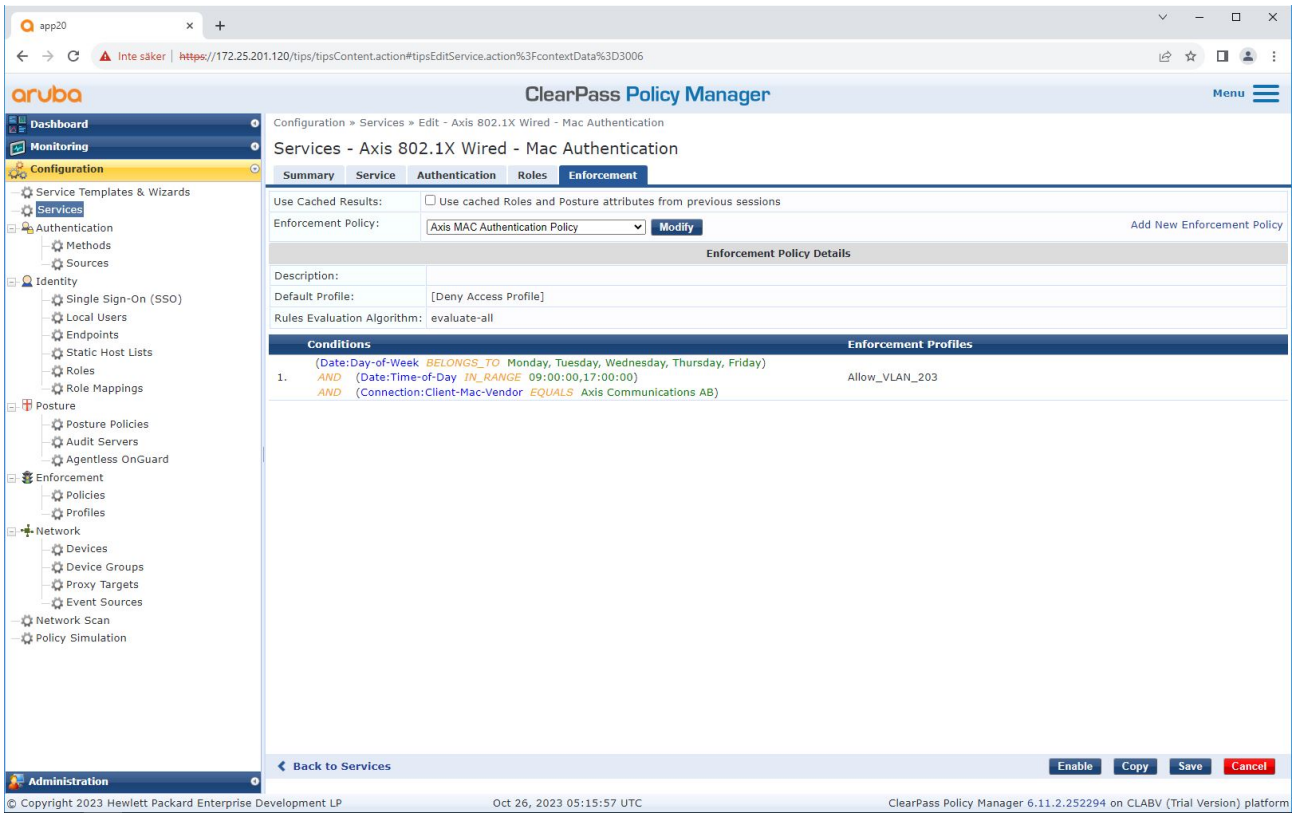



*La méthode d'authentification MAC préconfigurée est configurée pour le service. De plus, la source d'authentification créée précédemment et contenant une liste d'adresses MAC Axis est sélectionnée.*

Axis Communications AB 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 Aruba

Outre la configuration d'intégration sécurisée décrite dans *Commutateur d'accès Aruba à la page 16*, reportez-vous à l'exemple de configuration de port ci-dessous pour le commutateur d'accès Aruba 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
```

Manuel d'utilisation
Secure integration of Axis devices into Aruba networks

Ver. M4.3
Date : Novembre 2023
Référence T10197992