HPE Aruba Networking

Manuel d'utilisation

Table des matières

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.

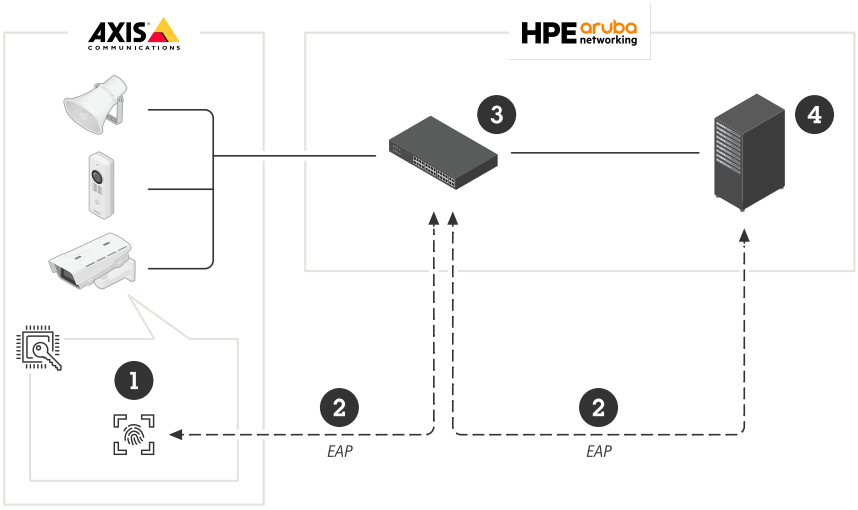
Périphérique sécurisé embarqué sur des réseaux « Zero-Trust » avec IEEE 802.1X/802.1AR

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 d'AXIS OS du dispositif, 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.

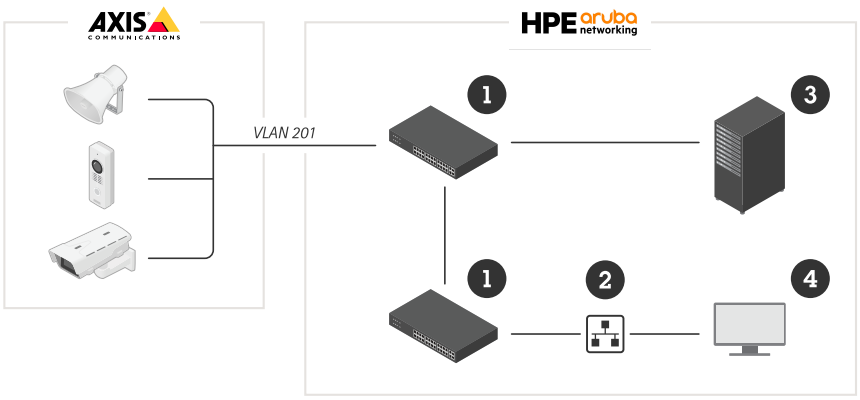


Le périphérique Axis s'authentifie auprès du réseau HPE Aruba Networking à l'aide du certificat d'identification de périphérique Axis conforme à la norme IEEE 802.1AR.

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.

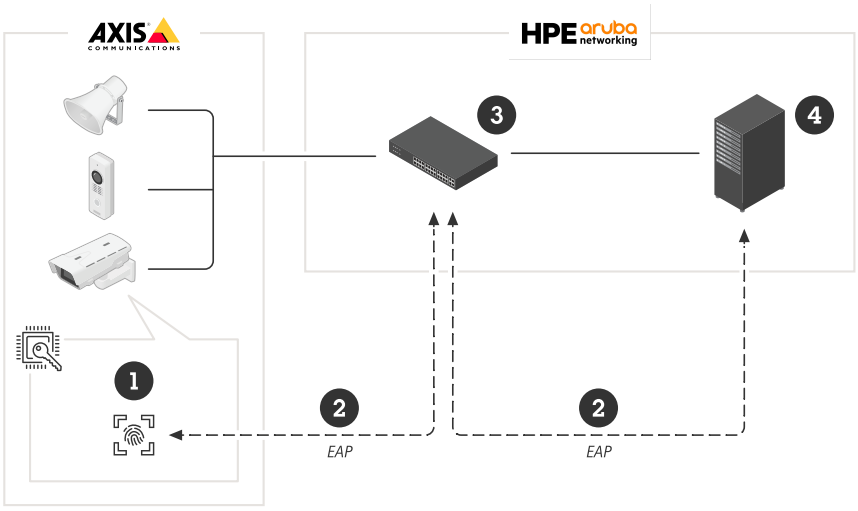


Une fois l'authentification effectuée, le périphérique Axis se déplace vers un réseau de mise en service pour la configuration.

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

Réseau de production

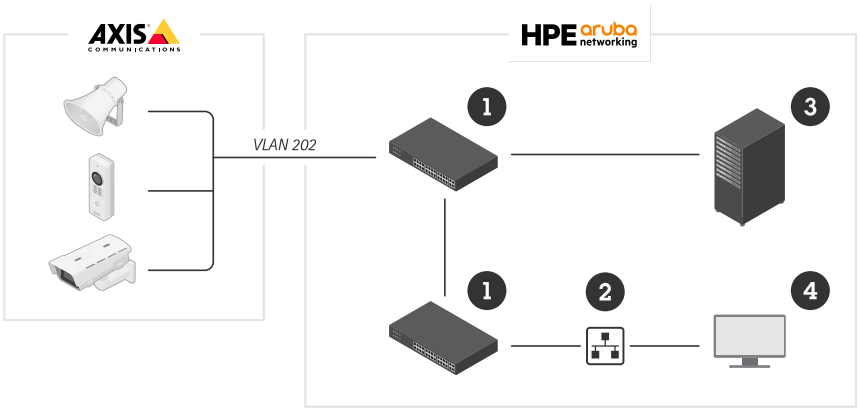
La mise en service du périphérique Axis avec de nouveaux certificats IEEE 802.1X déclenche une nouvelle tentative d'authentification. ClearPass Policy Manager vérifie les nouveaux certificats et décide de déplacer ou non le périphérique Axis dans le réseau de production.



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*

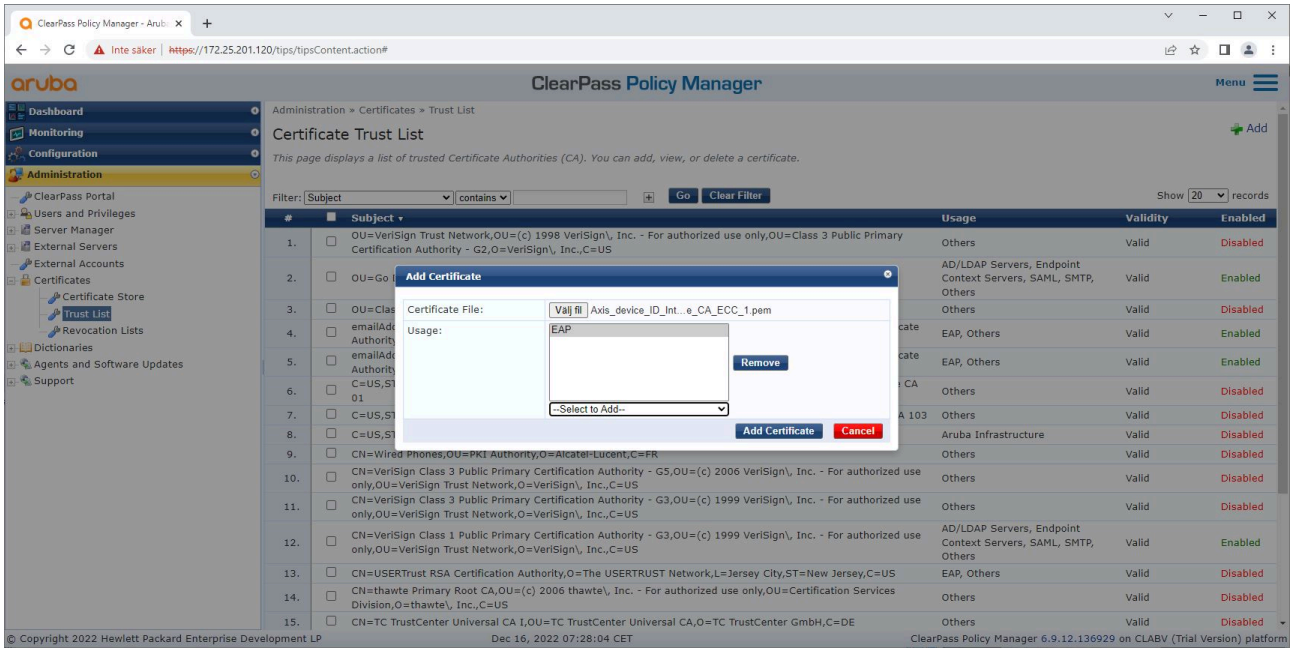
Configuration de HPE Aruba Networking

HPE Aruba Networking ClearPass Policy Manager

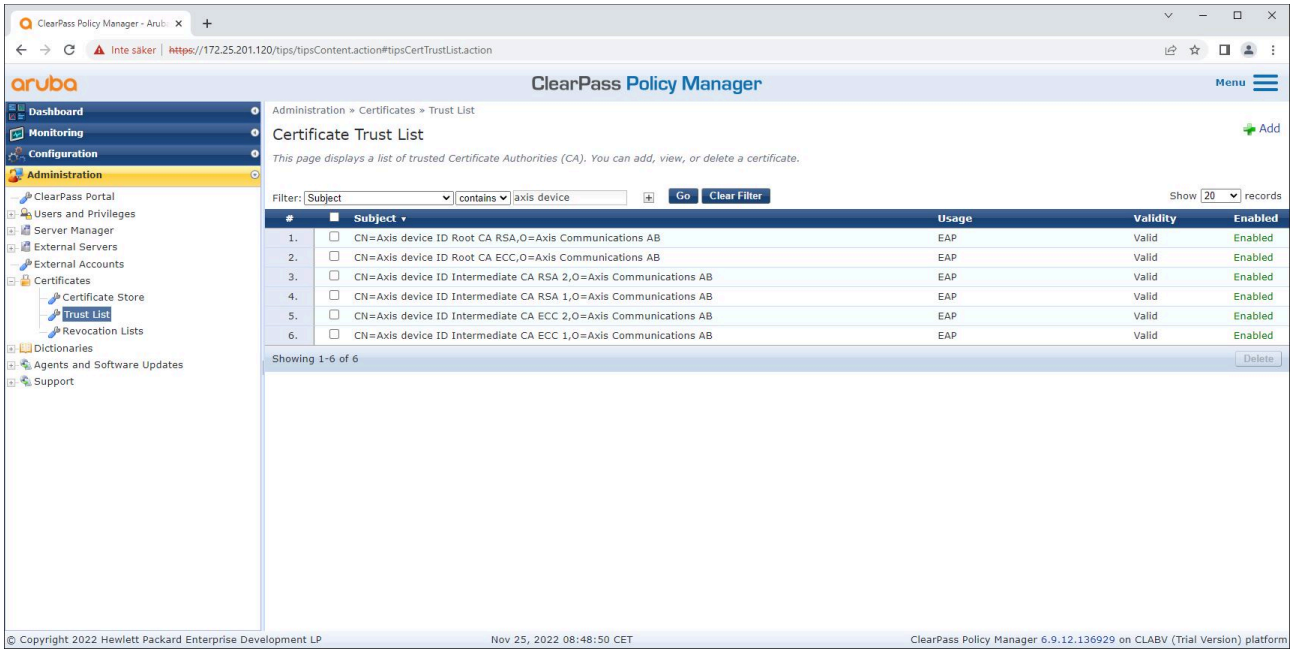
ClearPass Policy Manager fournit un contrôle d'accès réseau sécurisé basé sur les rôles et les périphériques pour l'IoT, le BYOD, les périphériques d'entreprise, les employés, les sous-traitants et les invités, sur une infrastructure filaire, sans fil et VPN multifournisseur.

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.



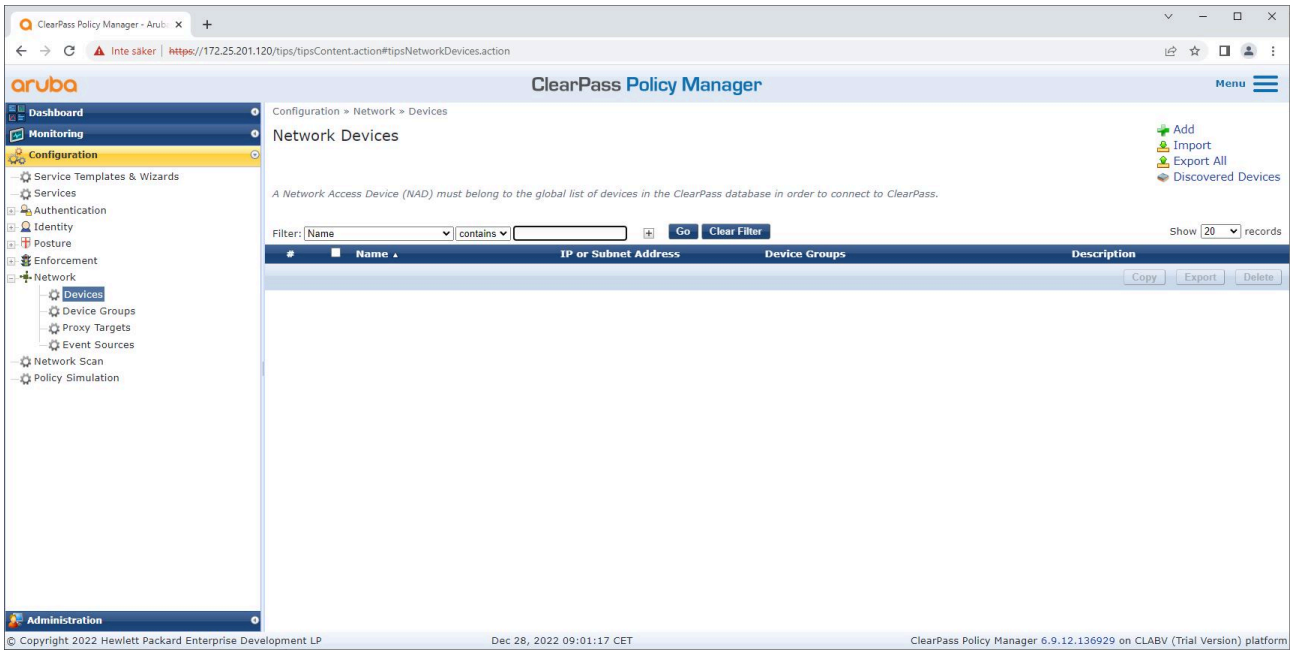
Chargez des certificats IEEE 802.1AR spécifiques à Axis vers le magasin de certificats de confiance de ClearPass Policy Manager.



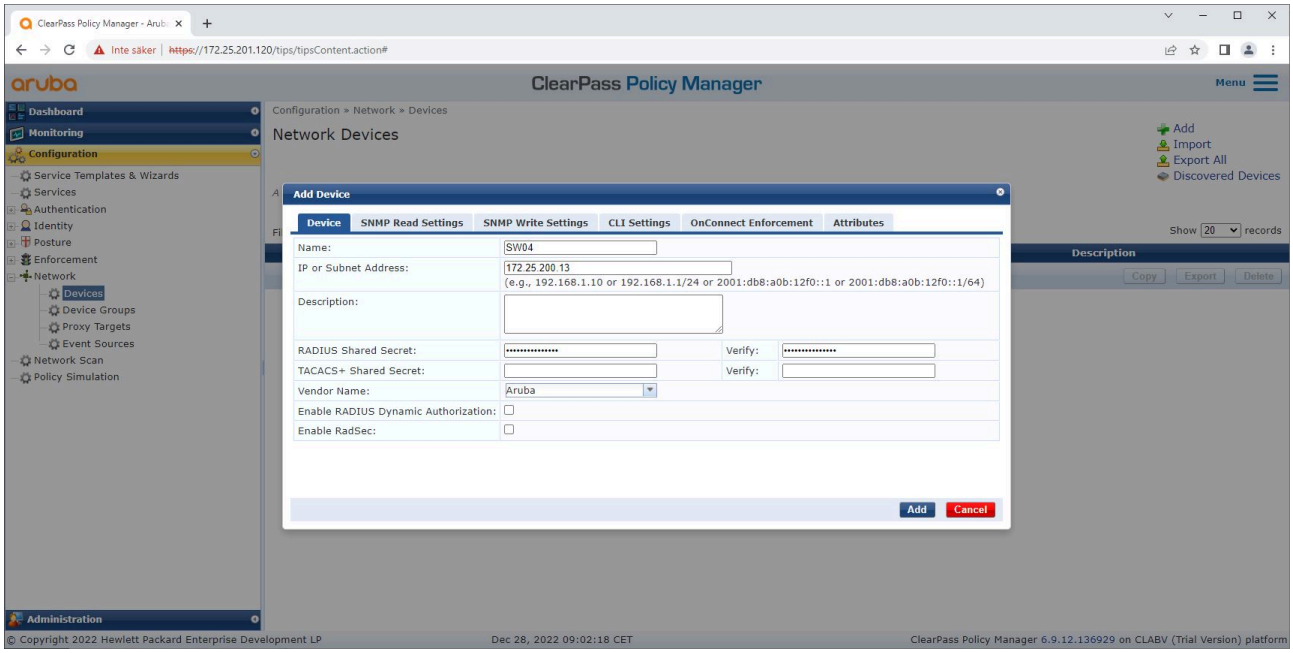
Magasin de certificats de confiance dans ClearPass Policy Manager avec chaîne de certificats IEEE 802.1AR spécifique à Axis incluse.

Configuration du périphérique/groupe réseau

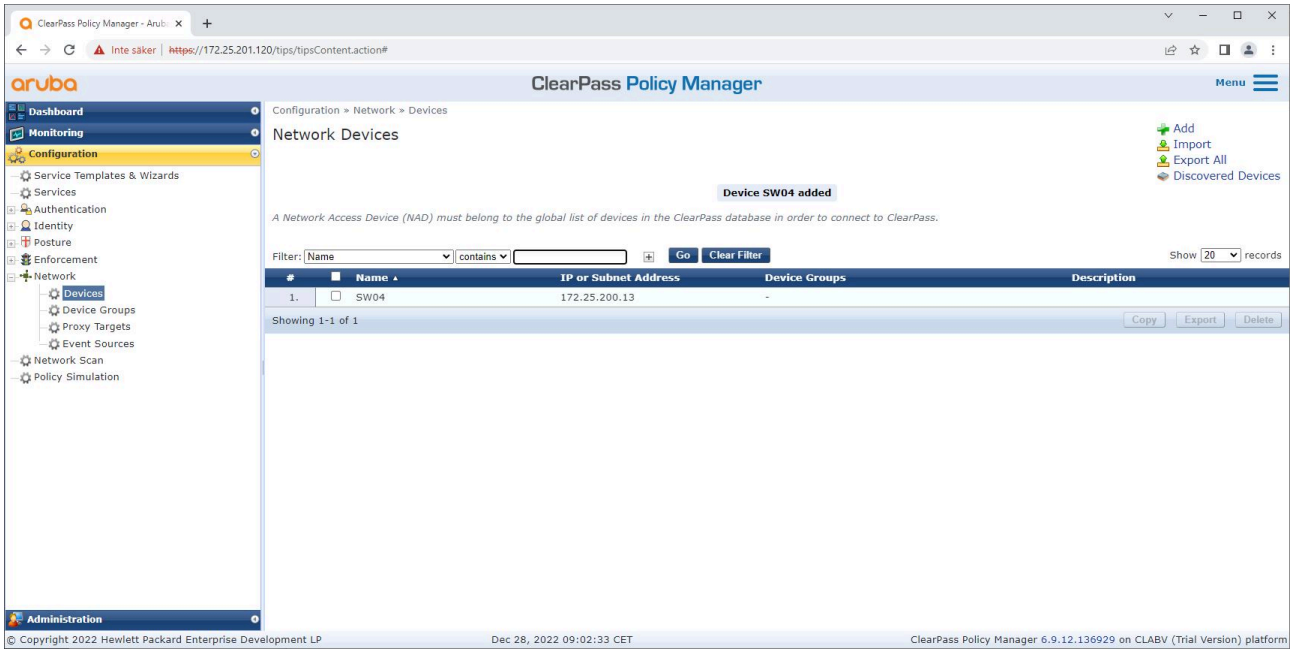
1. Ajoutez des périphériques d'accès réseau fiables tels que des commutateurs d'accès HPE Aruba Networking à ClearPass Policy Manager. ClearPass Policy Manager doit connaître les commutateurs d'accès du réseau qui sont utilisés pour la communication IEEE 802.1X. Notez également que le secret partagé 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.



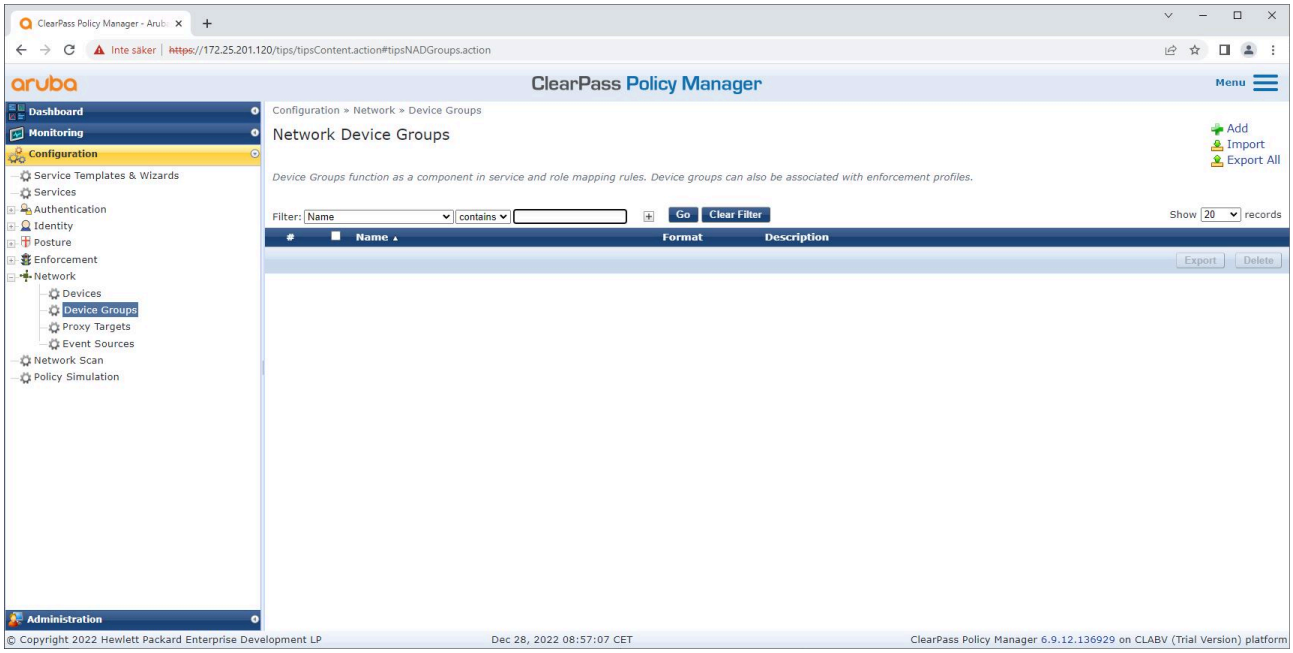
Interface des périphériques réseau approuvés dans ClearPass Policy Manager.



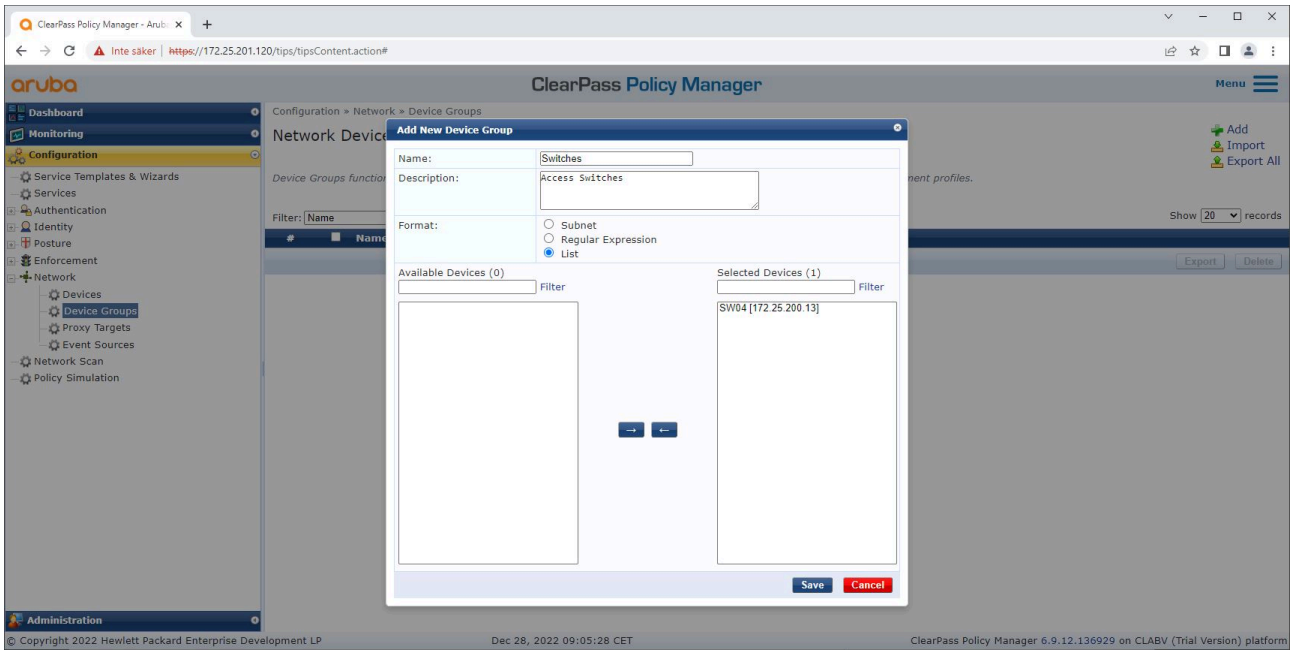
Ajoutez le commutateur d'accès HPE Aruba Networking en tant que périphérique approuvé dans ClearPass Policy Manager. Notez que le secret partagé RADIUS doit correspondre à la configuration IEEE 802.1X spécifique du commutateur.



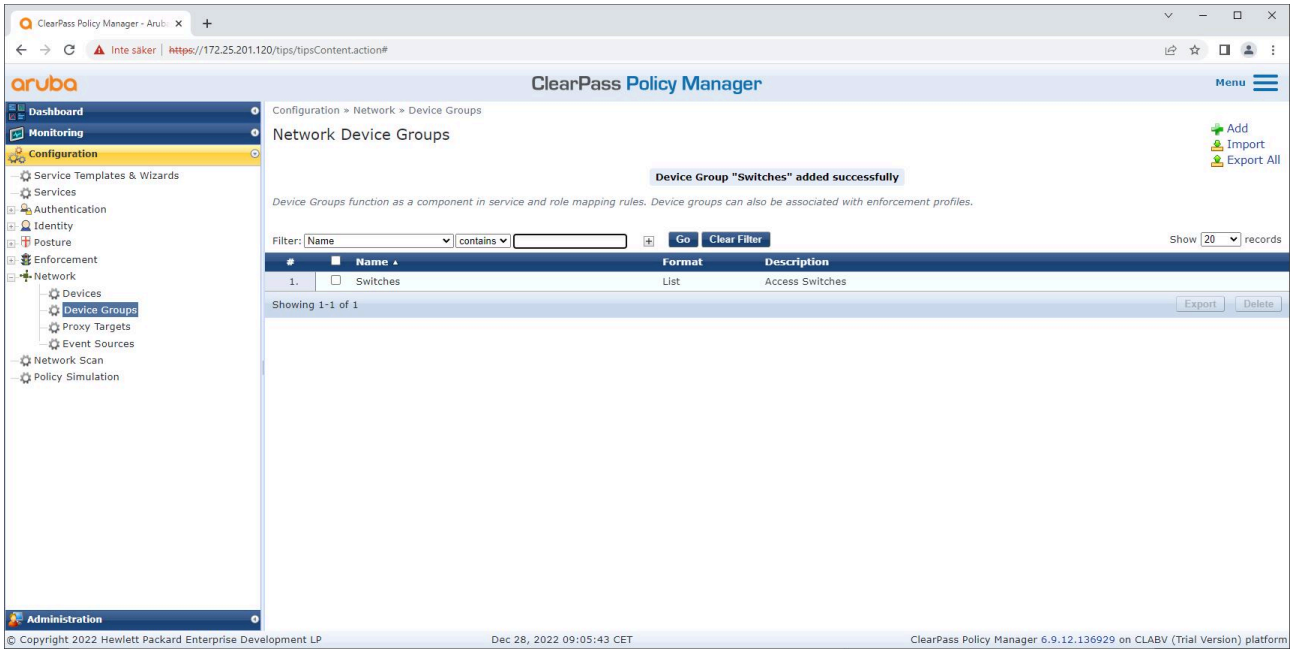
ClearPass Policy Manager avec un seul périphérique réseau approuvé configuré.



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.

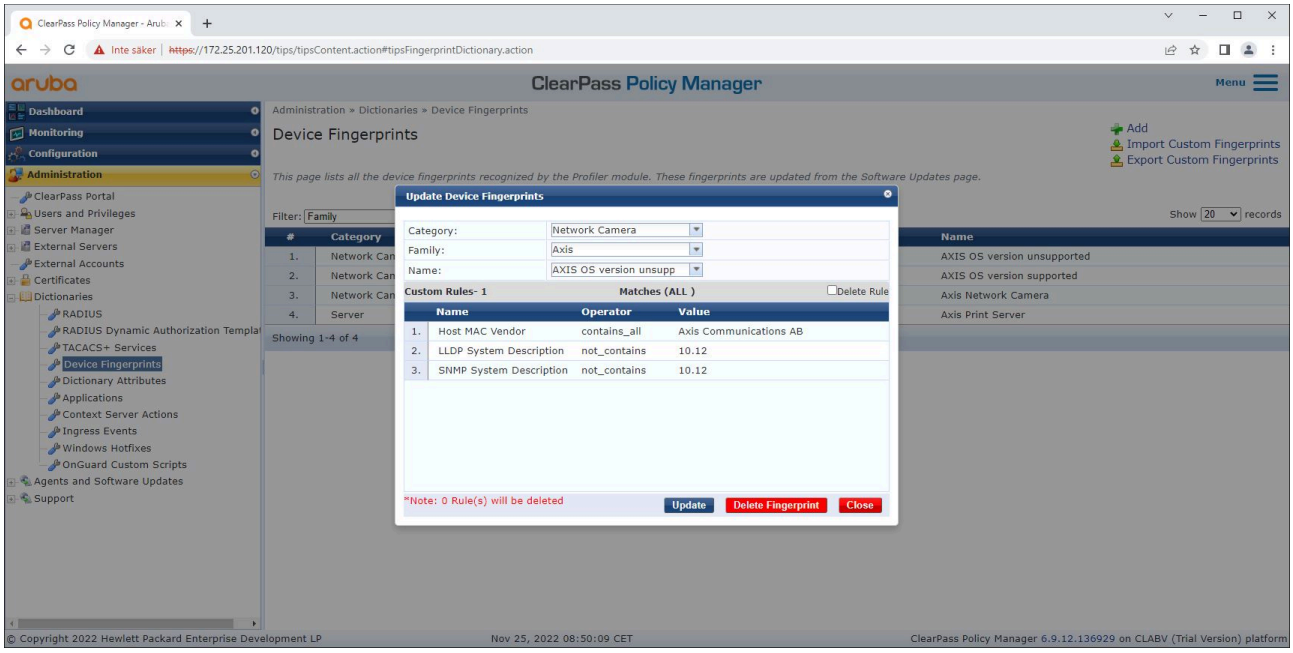


ClearPass Policy Manager avec un groupe de périphériques réseau configuré qui comprend un ou plusieurs périphériques réseau approuvés.

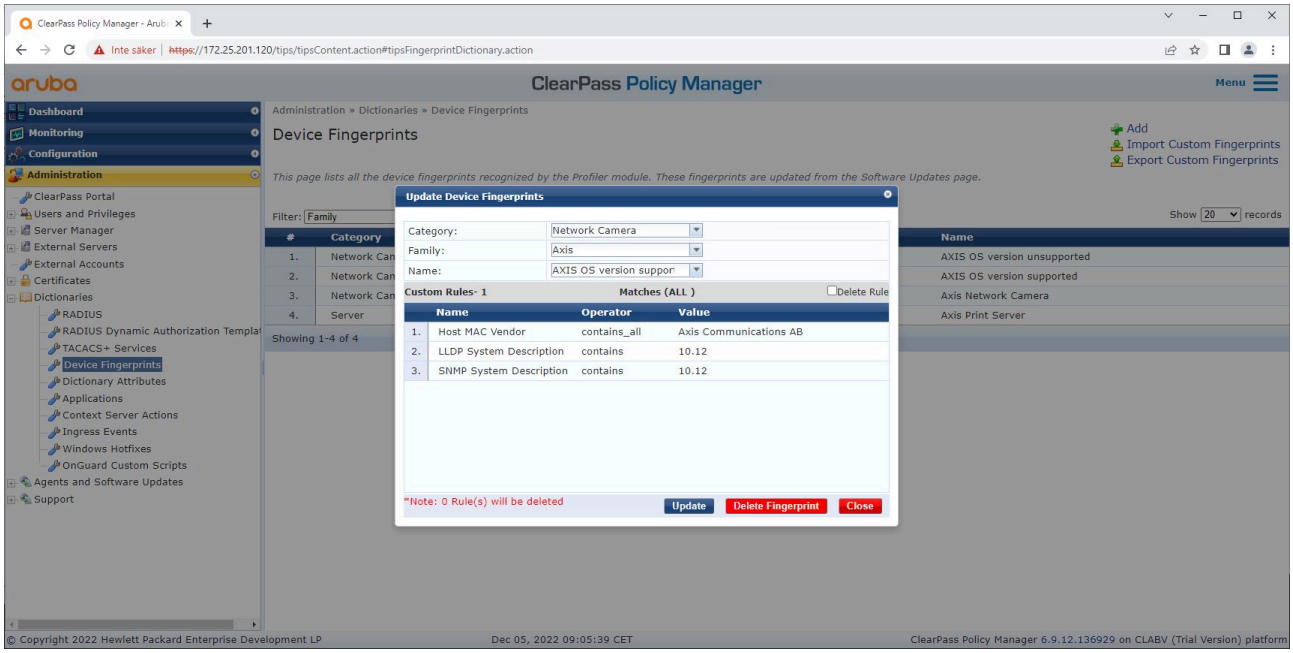
Configuration des empreintes digitales du périphérique

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.



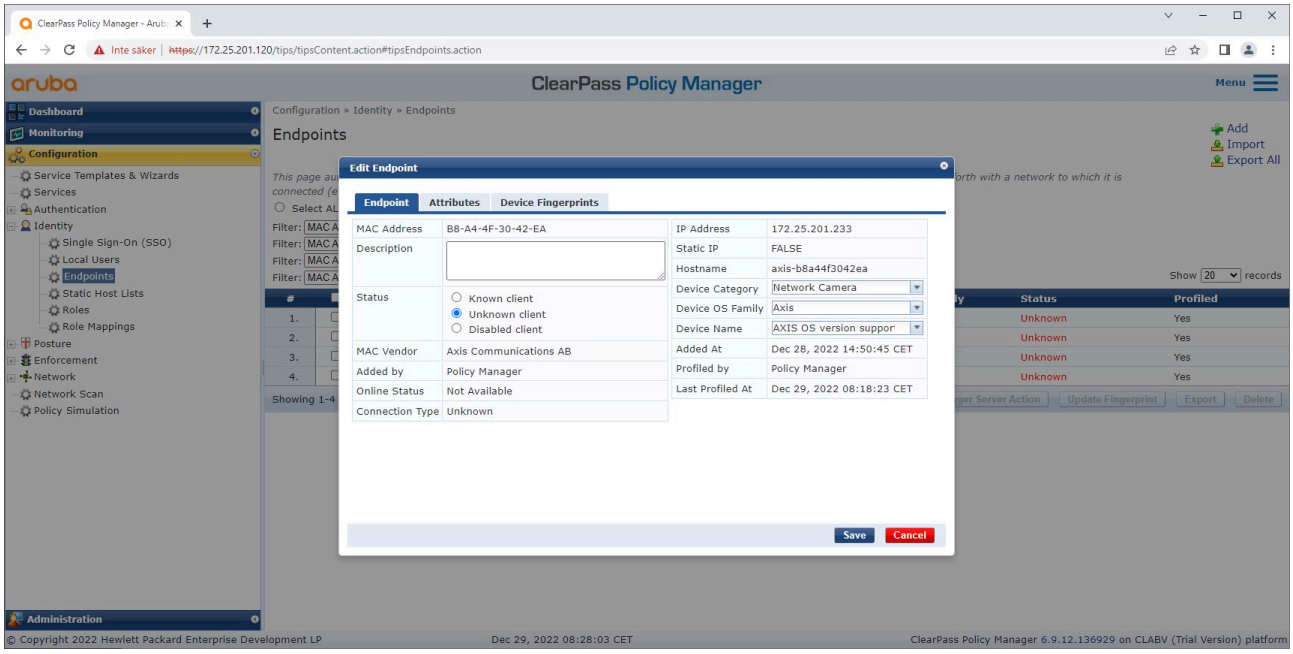
Configuration des empreintes de périphérique dans ClearPass Policy Manager. Les périphériques Axis fonctionnant sous des versions d'AXIS OS autres que la version 10.12 sont pris en charge dans cet exemple.

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

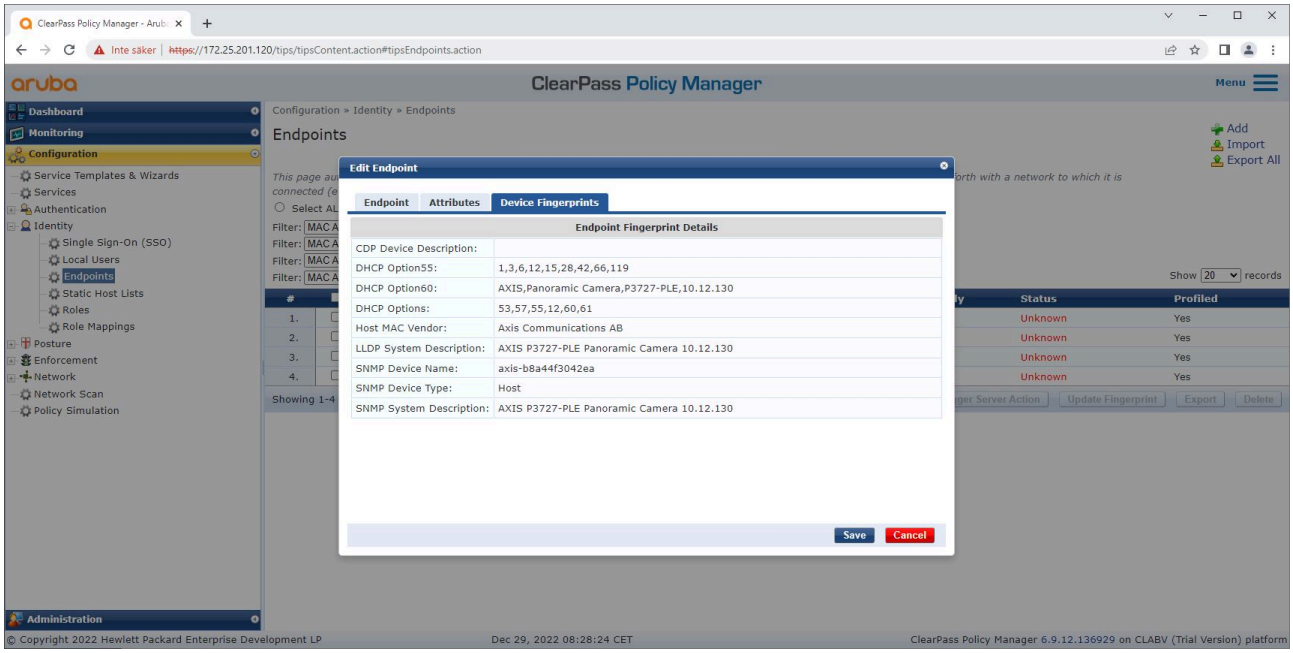
1. Allez à **Configuration > Identité > Points de terminaison**.
2. Sélectionnez le périphérique que vous voulez afficher.
3. Cliquez sur l'onglet **Empreintes de périphérique**.

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.

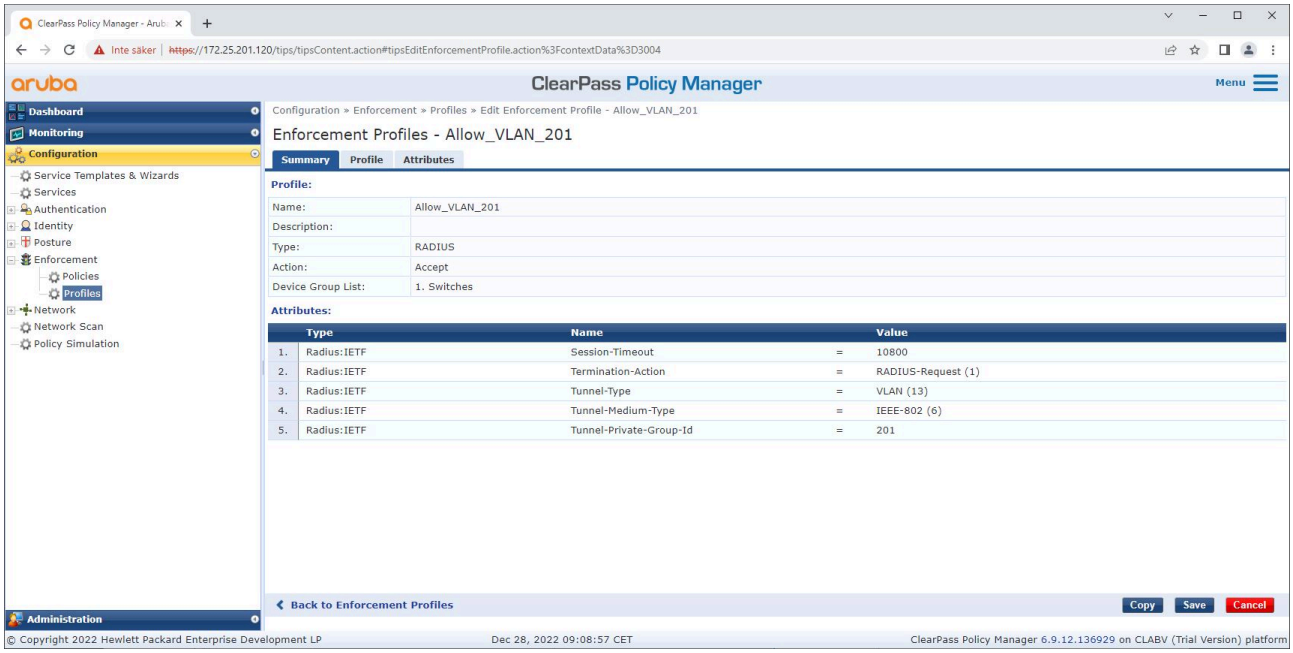


Empreintes détaillées d'un périphérique Axis profilé. Veuillez noter que le protocole SNMP est désactivé par défaut sur les périphériques Axis. Les informations de découverte spécifiques aux protocoles LLDP, CDP et DHCP sont partagées par le périphérique Axis dans son état de valeurs par défaut et sont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

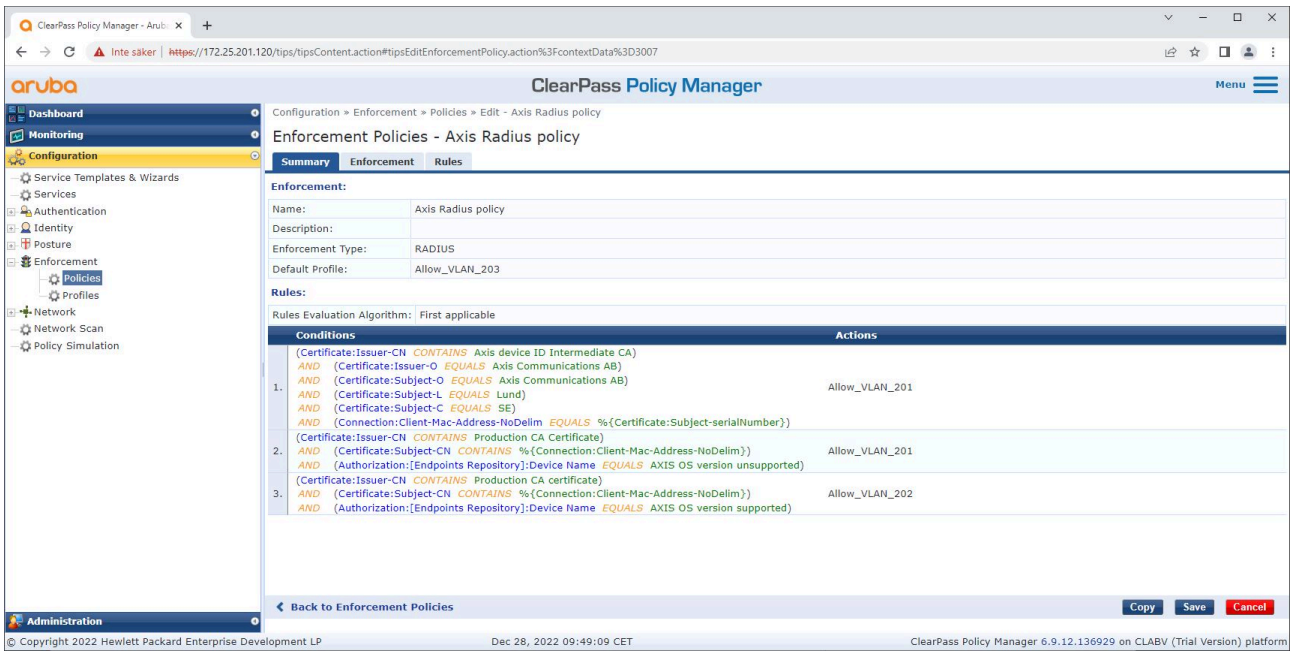
Configuration du profil d'application

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.

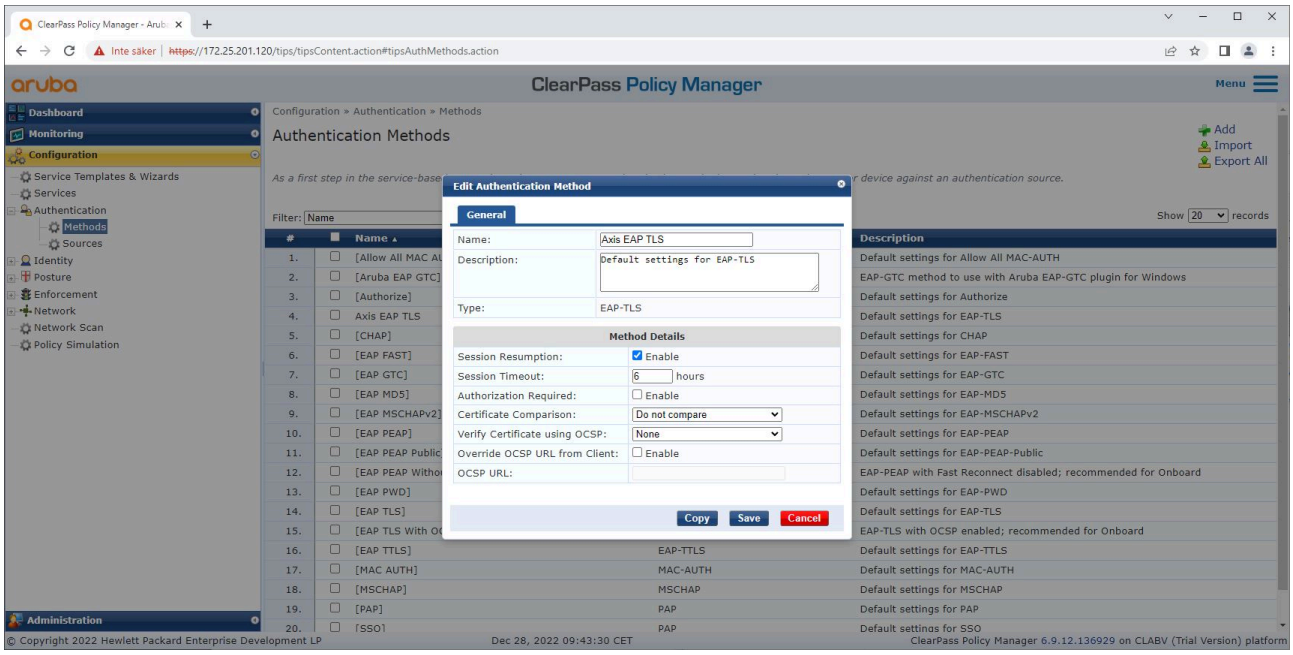
Réseau de production (VLAN 202)

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

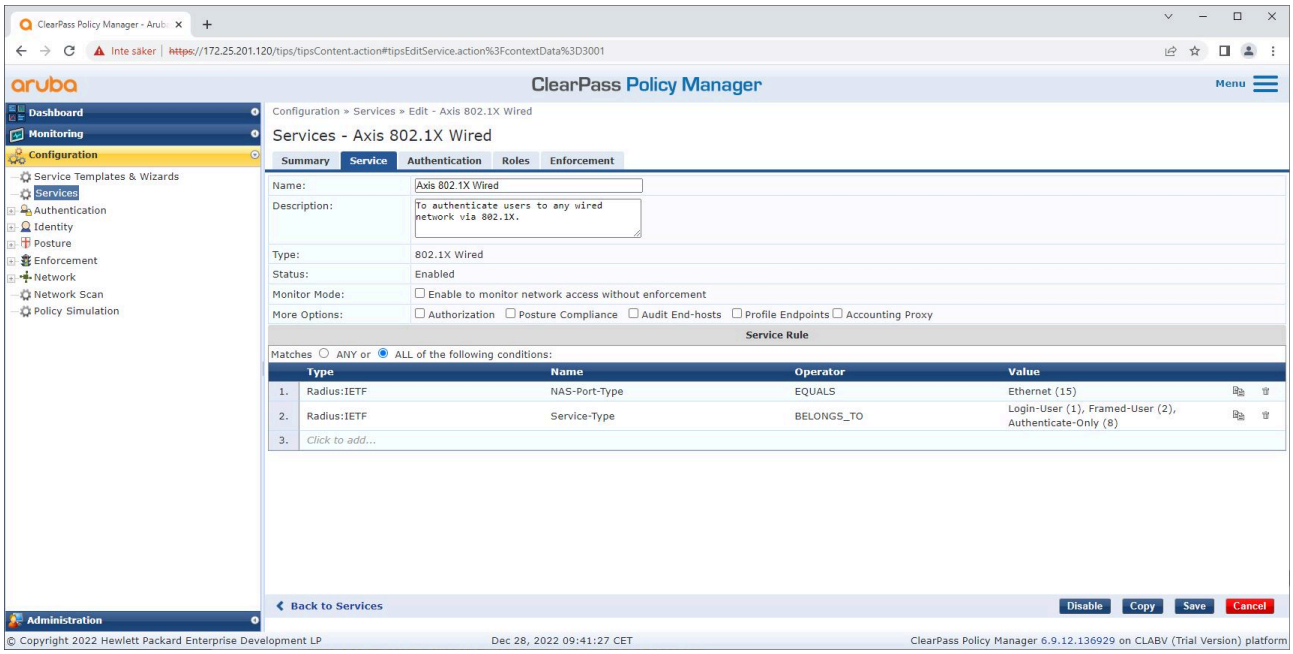
La méthode d'authentification définit la manière dont un périphérique Axis tente de s'authentifier sur le réseau. La méthode préférée est IEEE 802.1X EAP-TLS car les périphériques Axis avec Axis Edge Vault sont livrés avec IEEE 802.1X EAP-TLS activé par défaut.



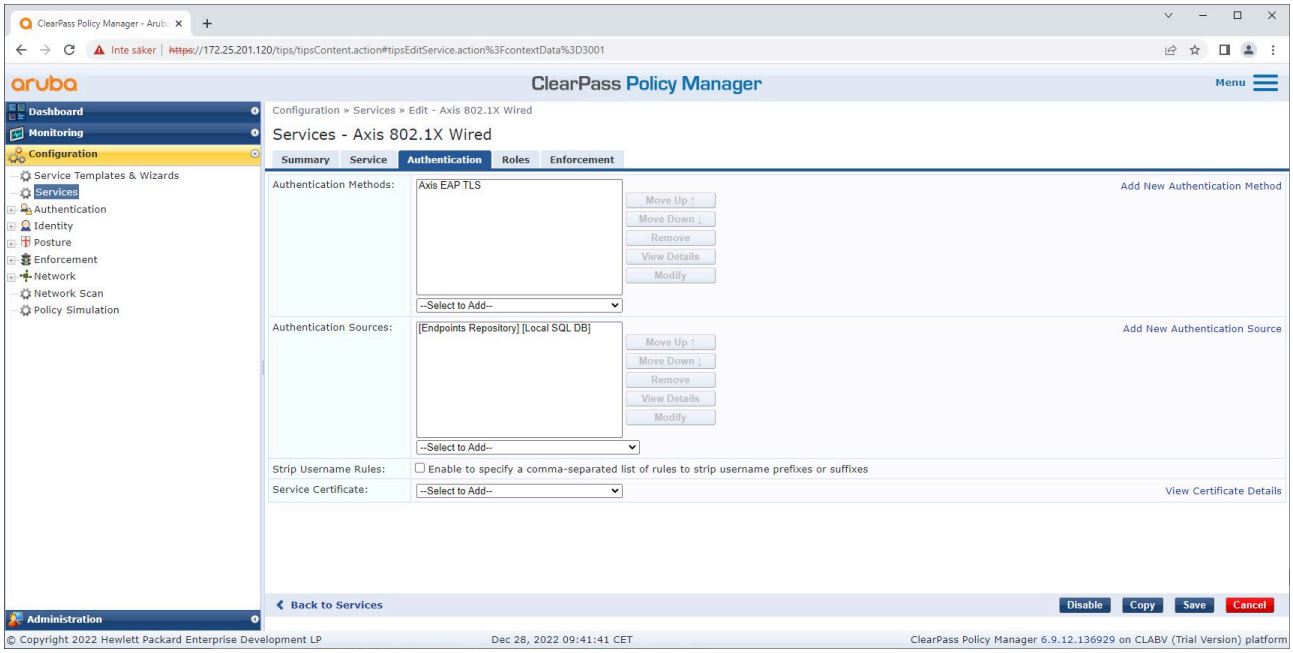
Interface de méthode d'authentification de ClearPass Policy Manager où est définie la méthode d'authentification EAP-TLS pour les périphériques Axis.

Configuration du service

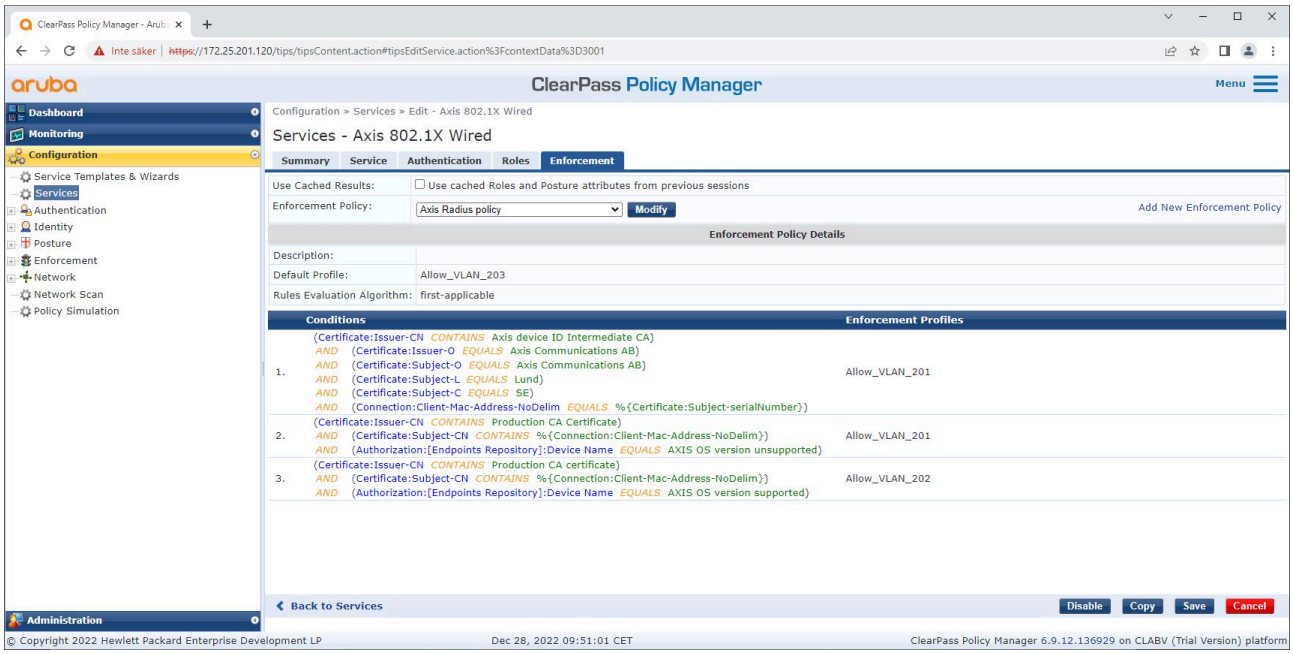
Dans la page **Services**, les étapes de configuration sont regroupées dans un seul service qui gère l'authentification et l'autorisation des périphériques Axis au sein des réseaux HPE Aruba Networking.



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.

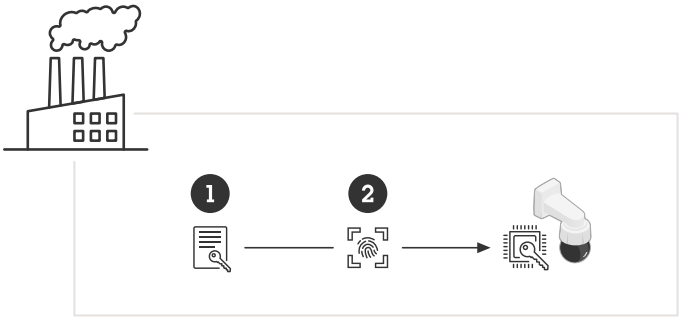
```
radius-server host MyRADIUSIPAddress key "MyRADIUSKey"
```

```
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.



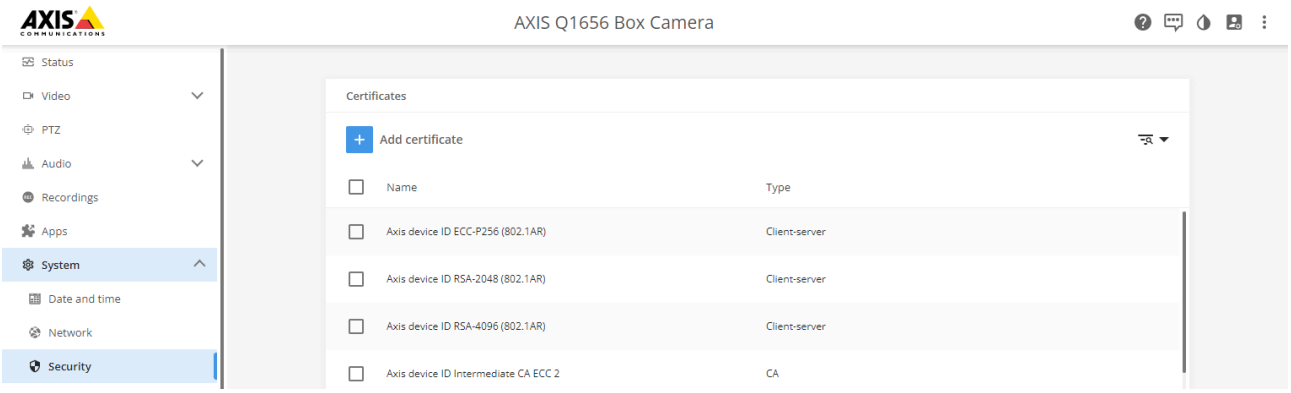
Les périphériques Axis sont fabriqués avec le certificat d'ID de périphérique Axis conforme à la norme IEEE 802.1AR pour les services d'identité de périphérique fiables.

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.

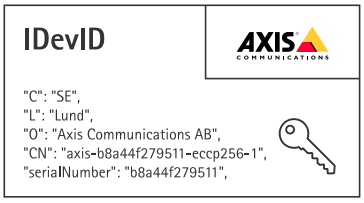
Remarque

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



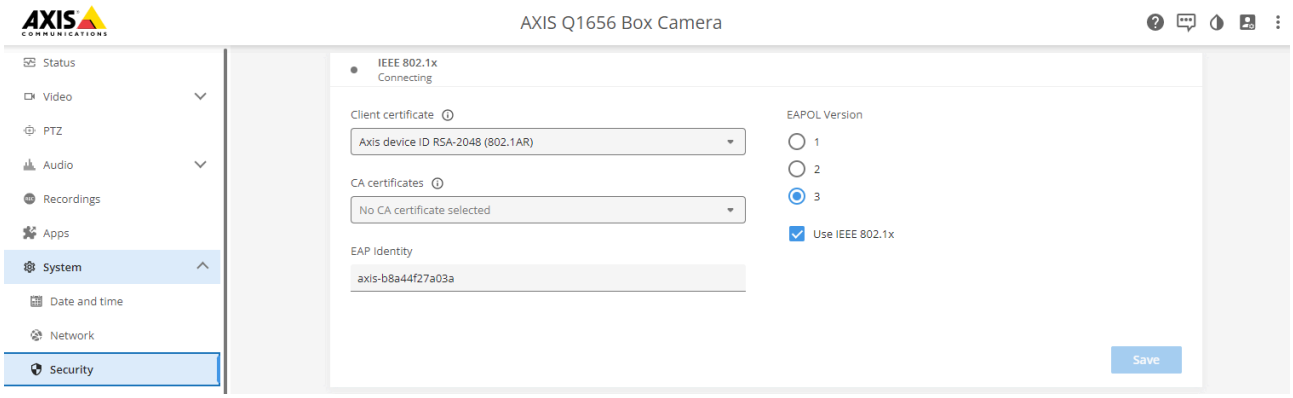
Magasin de certificats du périphérique Axis à l'état d'usine par défaut, avec un ID de périphérique Axis.

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

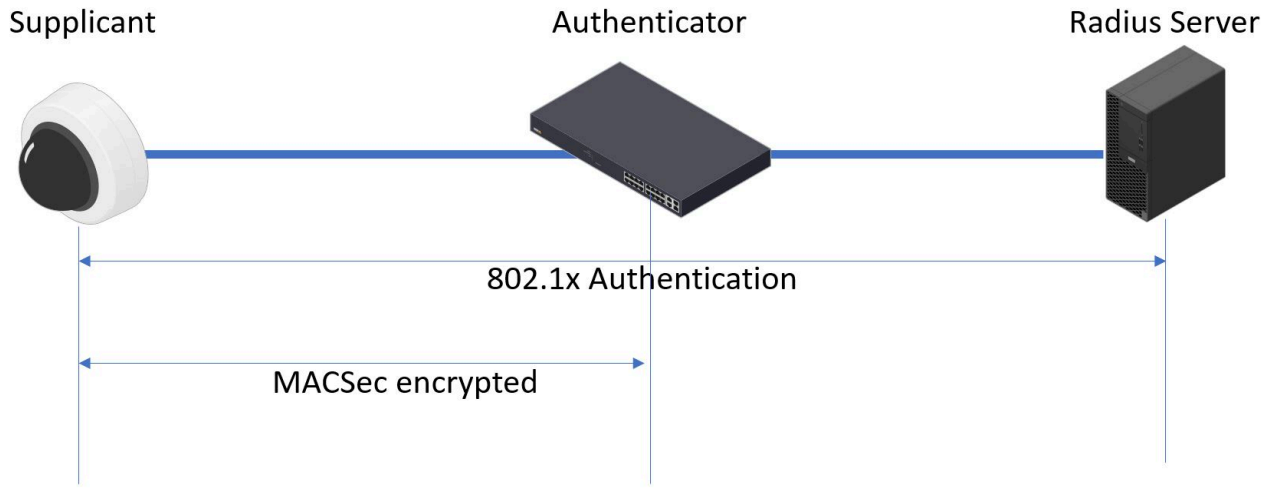
Pour regarder cette vidéo, accédez à la version Web de ce document.

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

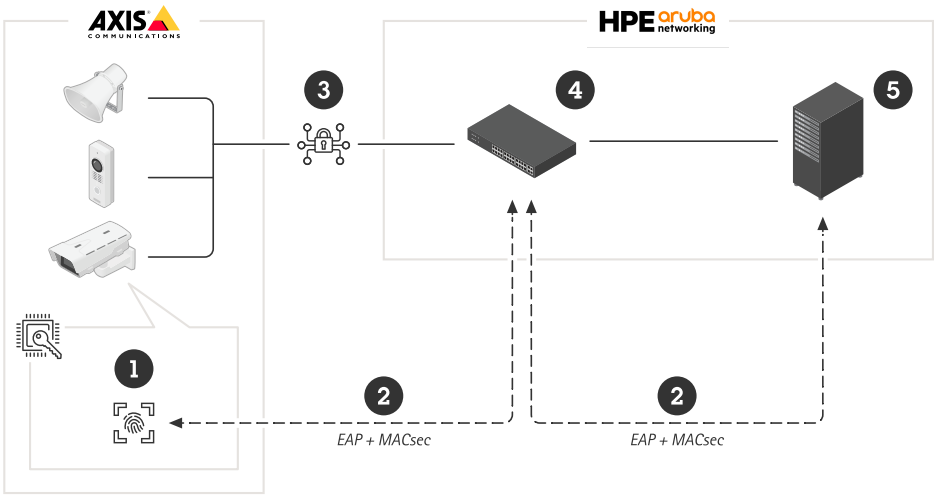
IEEE 802.1AE MACsec (Media Access Control Security) est un protocole réseau bien défini qui sécurise cryptographiquement les liaisons Ethernet point à point sur la couche réseau 2. Il garantit la confidentialité et l'intégrité des transmissions de données entre deux hôtes.

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

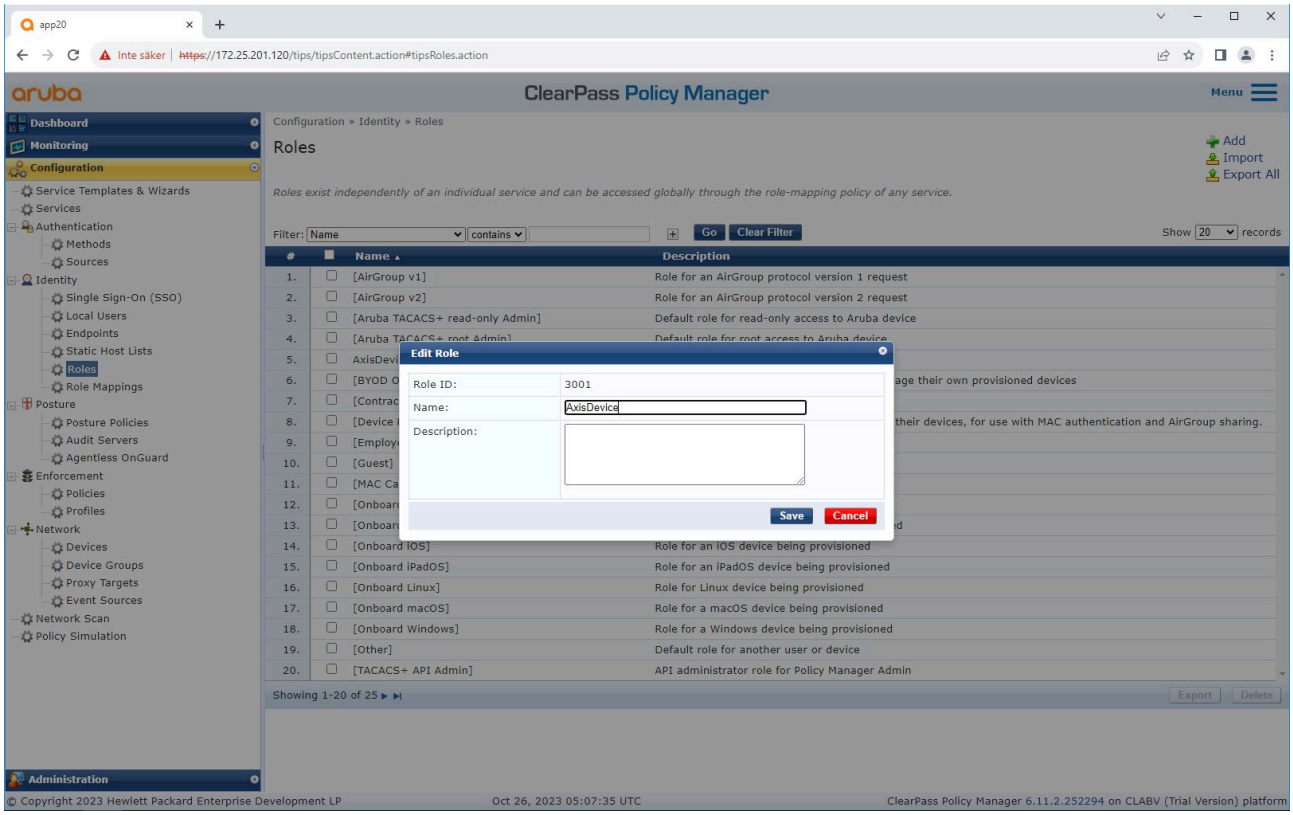
le port EAP-TLS IEEE 802.1X (2). Lors de la session EAP-TLS, les clés MACsec sont échangées automatiquement pour établir un lien sécurisé (3), protégeant tout le trafic réseau depuis le périphérique Axis vers le commutateur d'accès HPE Aruba Networking.

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.

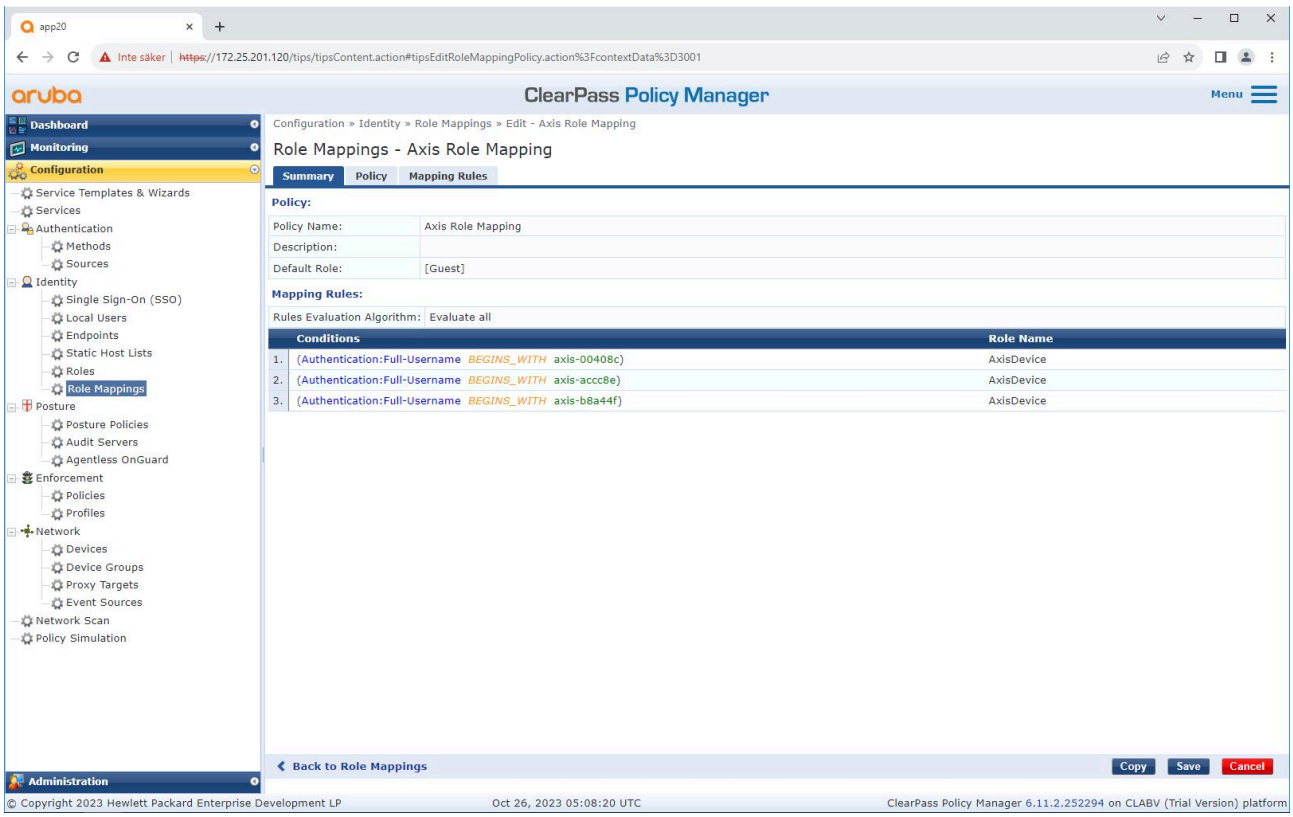
Si le commutateur d'accès HPE Aruba Networking ne prend pas en charge MACsec à l'aide d'EAP-TLS, le mode Clé pré-partagée peut être utilisé et configuré manuellement.

HPE Aruba Networking ClearPass Policy Manager

Politique de rôle et de mappage de rôles



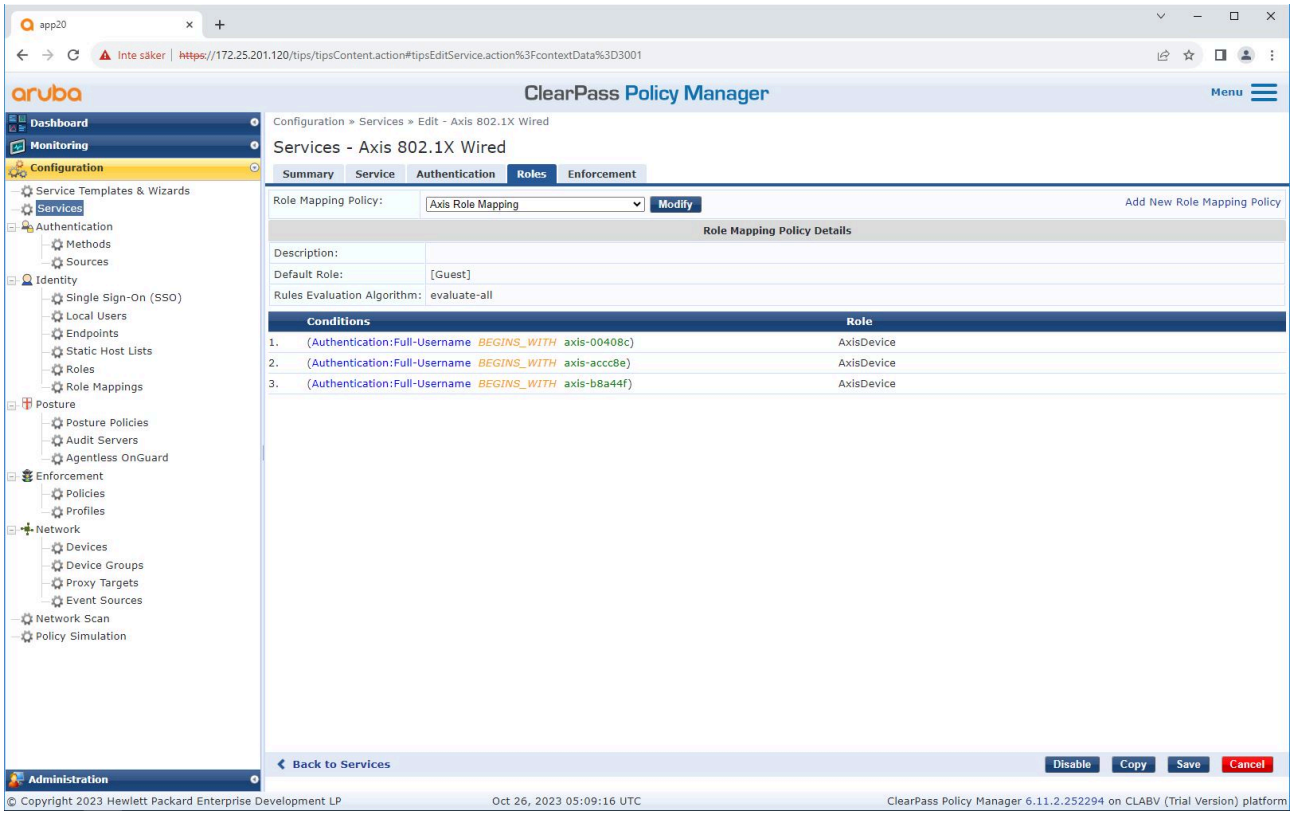
Ajoutez un nom de rôle pour les périphériques Axis. Le nom est le nom du rôle d'accès au port dans la configuration du commutateur d'accès.



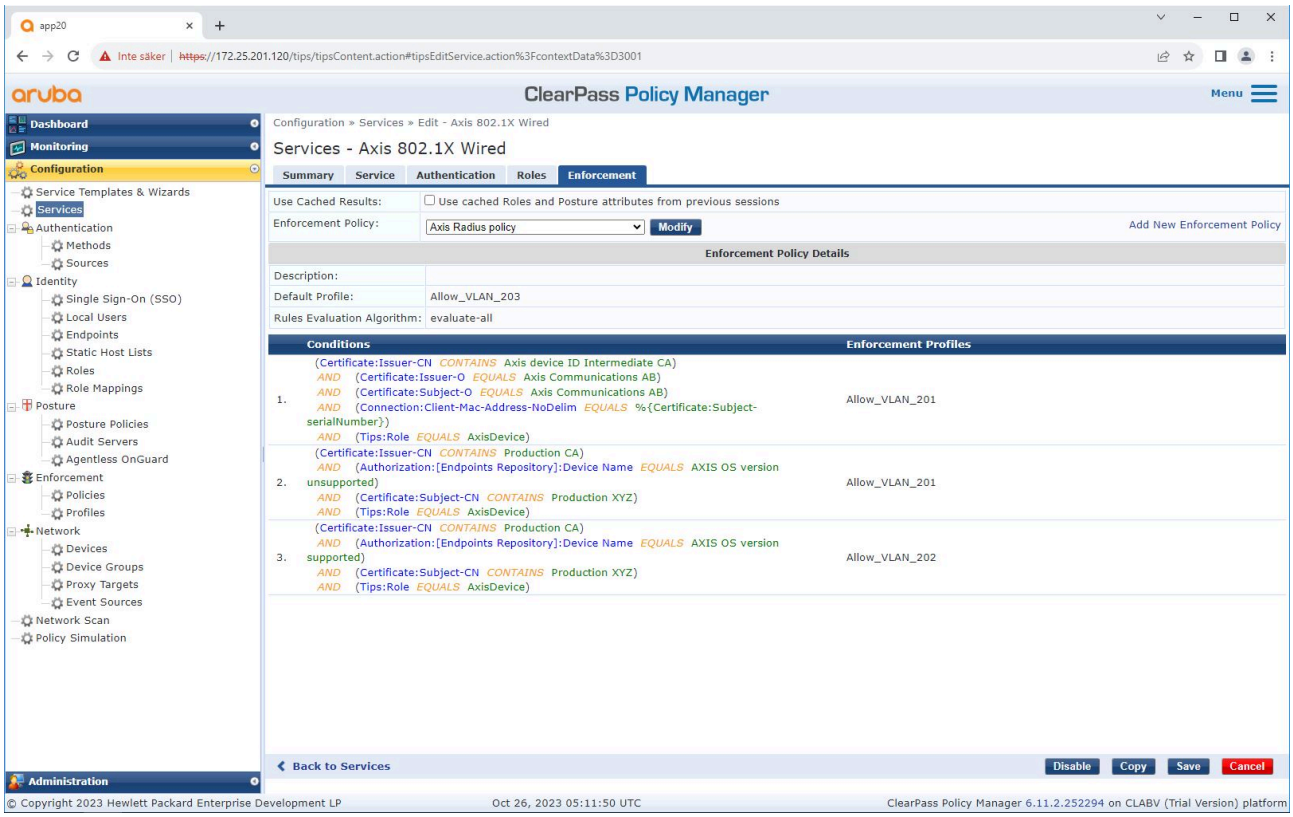
Ajoutez une stratégie de mappage des rôles Axis pour le rôle de périphérique Axis créé précédemment. Les conditions définies sont nécessaire pour permettre le mappage d'un périphérique au rôle de périphérique Axis. Si les conditions ne sont pas remplies, le périphérique fait partie du rôle [Invité].

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

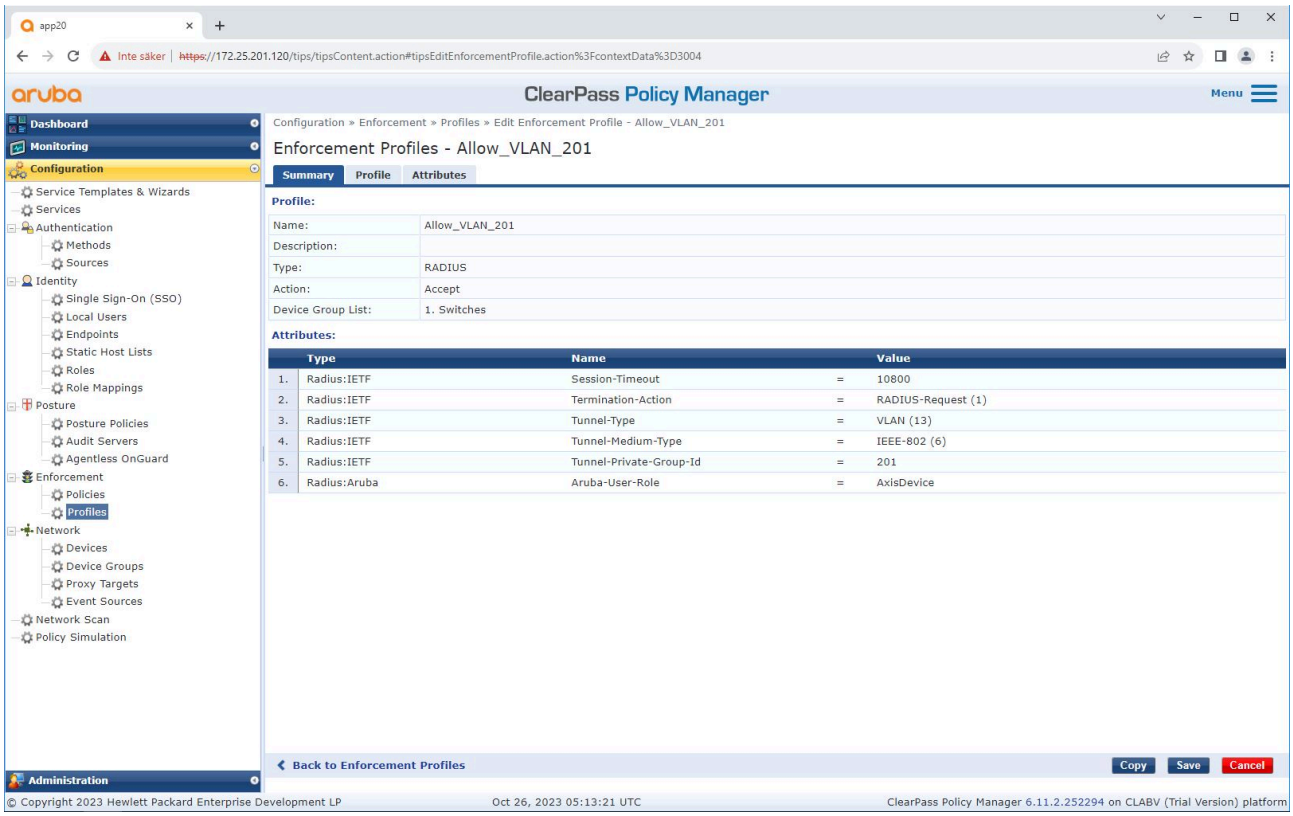


Ajoutez la stratégie de mappage de rôle Axis créée précédemment au service qui définit IEEE 802.1X comme méthode de connexion pour l'intégration des périphériques Axis.



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 *Commutateur d'accès HPE Aruba Networking, on page 15*, 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
```

Gestion des certificats – Inscription via un transport sécurisé (Enrollment over Secure Transport – EST)

Les certificats numériques sont essentiels pour sécuriser les dispositifs et les réseaux, mais leur gestion peut s'avérer complexe et prendre beaucoup de temps. Les certificats ont une durée de validité limitée et doivent être renouvelés régulièrement. Sans automatisation, ce processus est répétitif et manuel, en particulier dans le cas de déploiements à grande échelle ou d'environnements comprenant différents types de dispositifs.

AXIS OS 12.9 prend désormais en charge le protocole EST (Enrollment over Secure Transport), qui permet de fournir des certificats aux dispositifs de manière sécurisée. Défini dans la norme RFC 7030, le protocole EST est une solution basée sur des normes et conçue pour simplifier et automatiser l'ensemble du cycle de vie des certificats, y compris :

- Inscription – délivrance sécurisée de nouveaux certificats aux dispositifs
- Renouvellement – remplacement automatique des certificats arrivant à expiration
- Réinscription – mise à jour des certificats conformément aux politiques informatiques

Le protocole EST prend en charge les politiques définies par l'informatique pour les attributs des certificats, tels que la période de validité, le type de clé (RSA/ECC) ou la taille de la clé, et utilise exclusivement HTTPS.

Principaux avantages du protocole EST

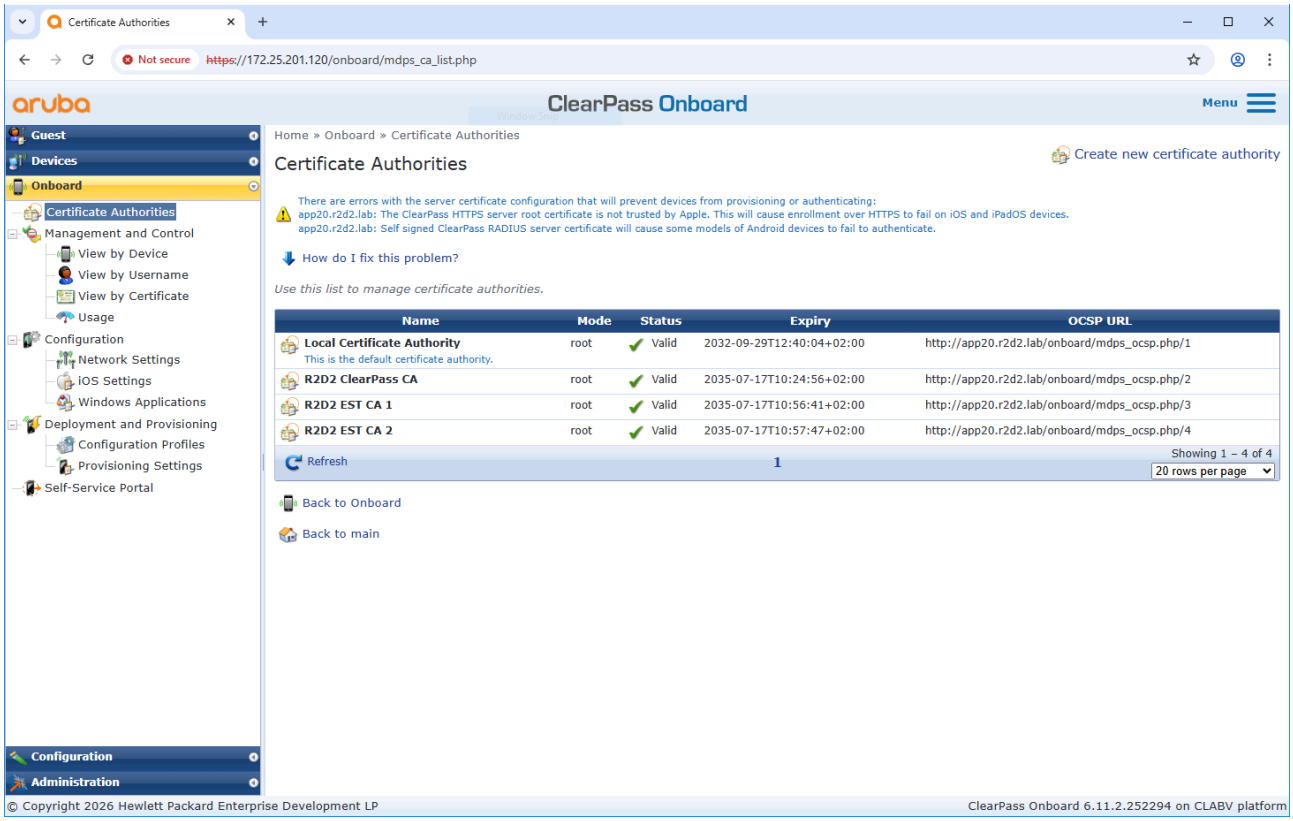
- La politique informatique gère l'inscription, le renouvellement et la réinscription automatisés des certificats, et par conséquent, il n'est plus du tout nécessaire de procéder à une configuration manuelle chronophage.
- Communication sécurisée de pointe via TLS 1.2/1.3 HTTPS uniquement.
- Visibilité/Surveillance centralisée pour les équipes informatiques.
  Basé sur des normes (RFC 7030) et intégré à l'Infrastructure informatique.
- Solution évolutive pour l'IoT, les réseaux d'entreprise et la gestion des dispositifs.

Veuillez vous reporter à notre *base de connaissances AXIS OS* pour obtenir la documentation générale sur le protocole EST.

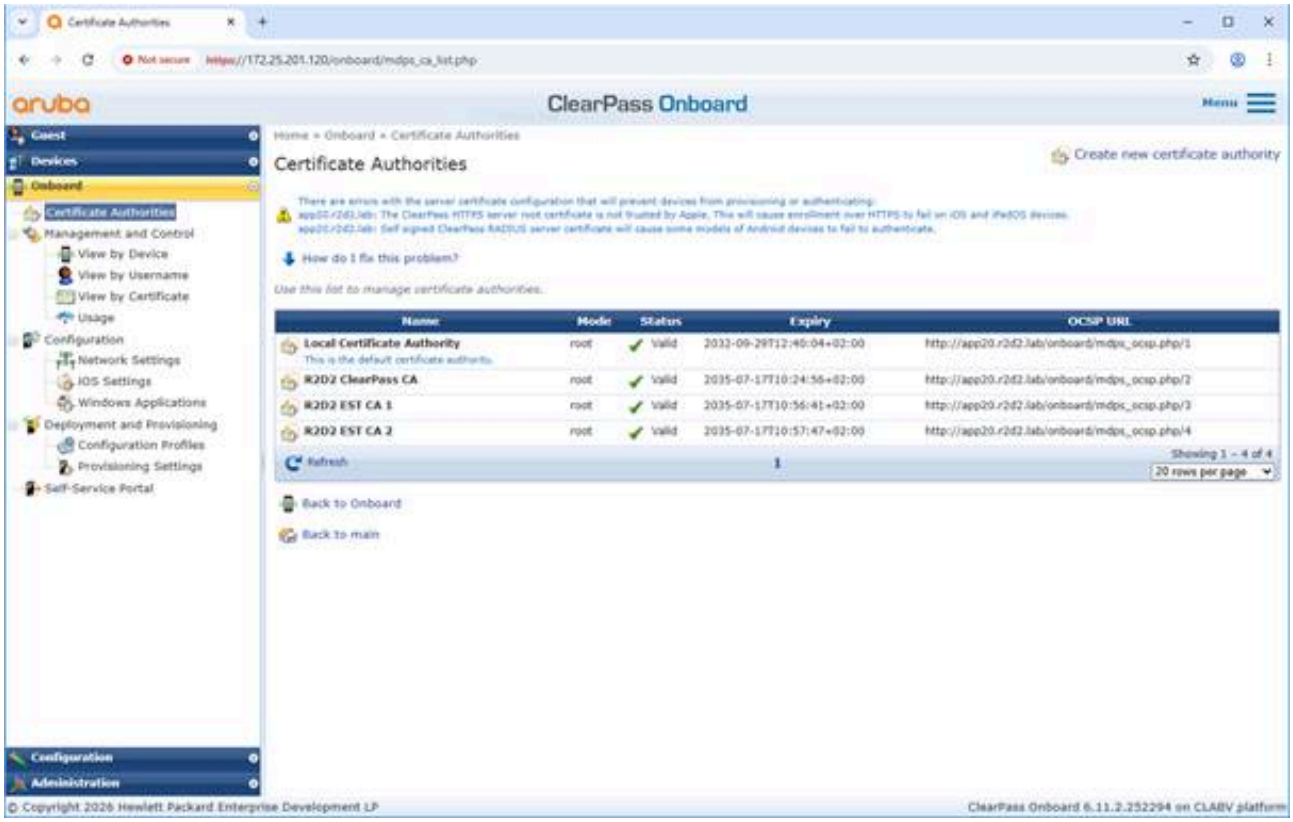
Configuration de HPE Aruba ClearPass Onboard

Aruba ClearPass Onboard s'intègre au protocole EST pour distribuer et gérer de manière sécurisée les certificats des dispositifs pour l'accès au réseau. À l'aide du protocole EST, les terminaux s'authentifient auprès de ClearPass et s'inscrivent pour obtenir un certificat unique via un canal TLS sécurisé, qui est ensuite utilisé pour l'authentification basée sur un certificat 802.1X et pour d'autres services. Il en résulte une méthode automatisée, basée sur des normes, sans mot de passe, et destinées à l'application de politiques d'accès sécurisées fondées sur l'identité du dispositif.

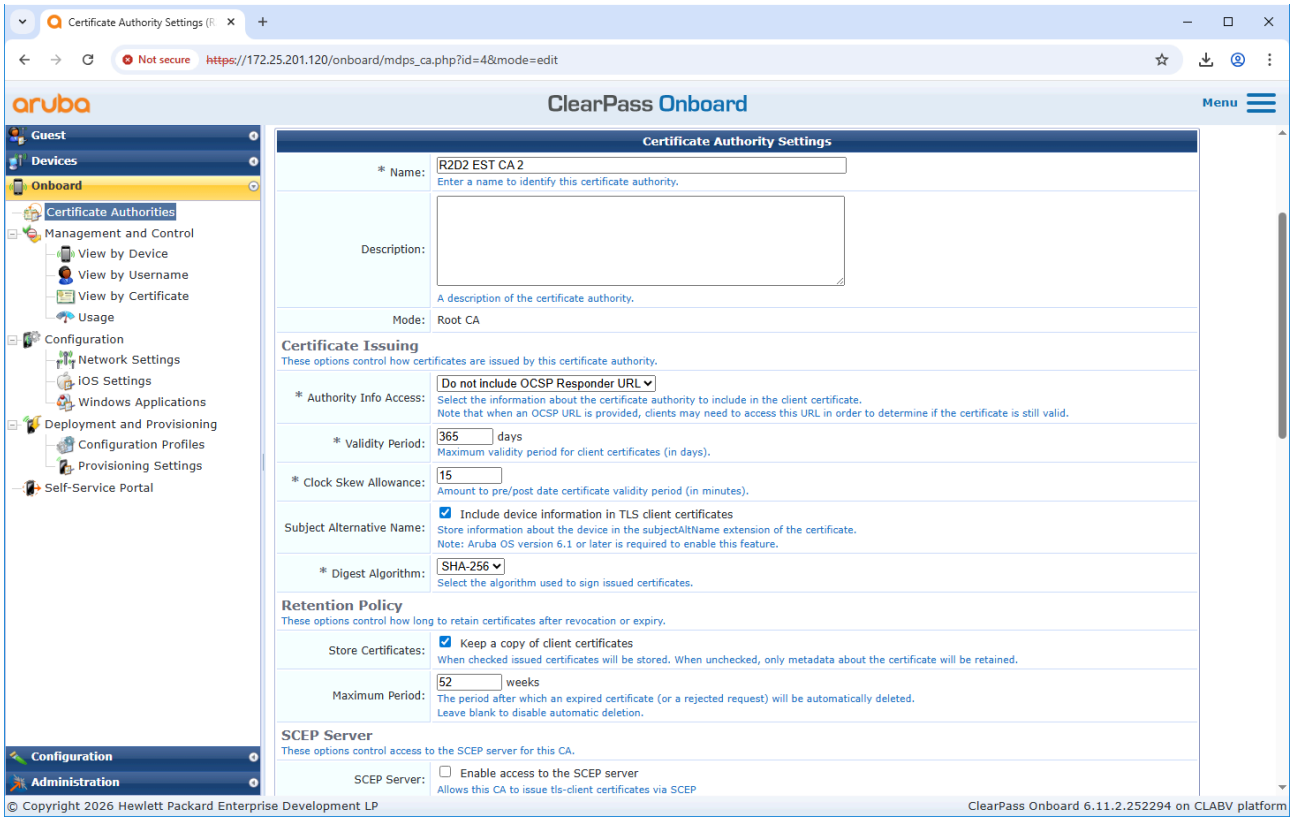
Configuration de l'autorité de certification



Veuillez créer une nouvelle autorité de certification dans ClearPass Onboard.



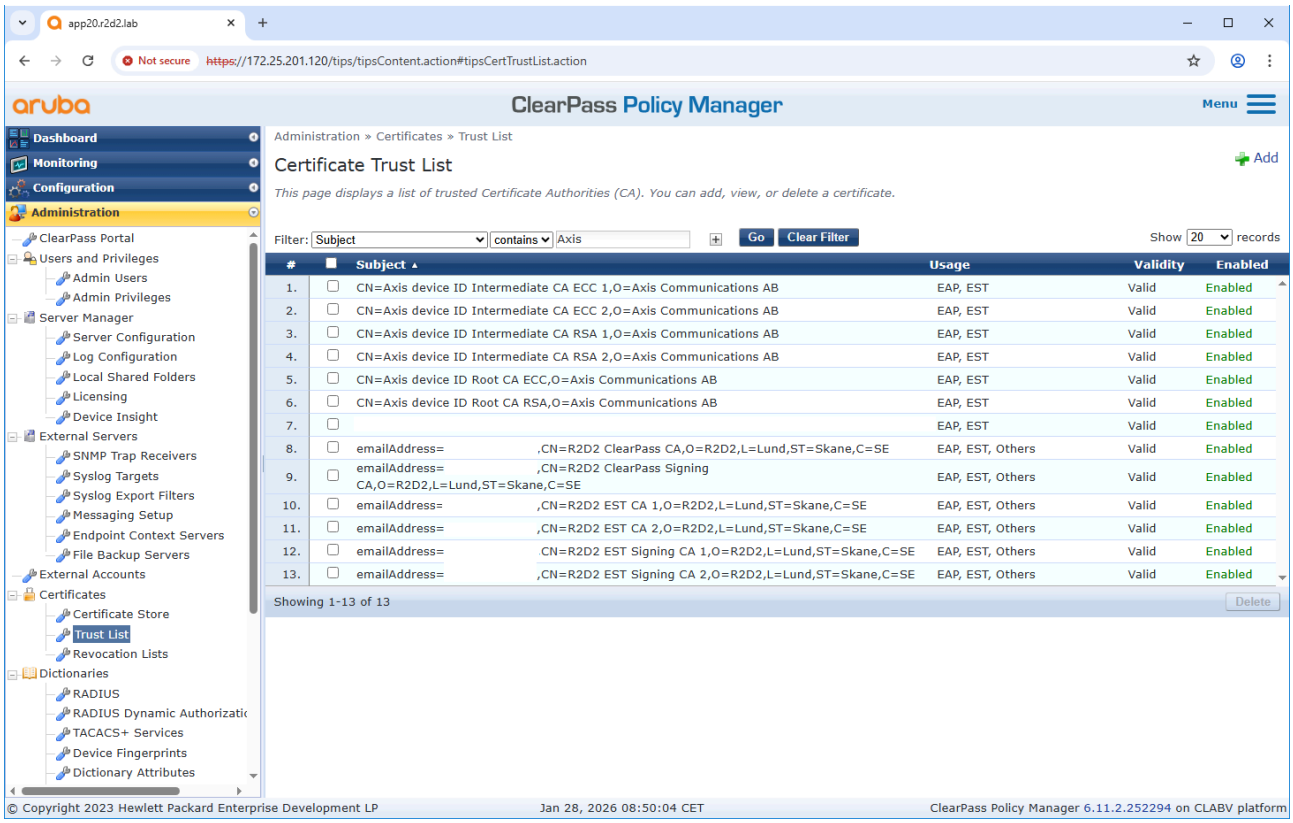
Le type de clé, la taille de la clé, la période de validité et d'autres paramètres sont définis dans l'autorité de certification créée.



Veuillez activer la fonctionnalité EST Server pour l'autorité de certification créée. Veuillez configurer la méthode d'authentification EST pour l'utilisation du certificat client.

Configuration de Aruba ClearPass Policy Manager

Configuration du magasin de certificats de confiance

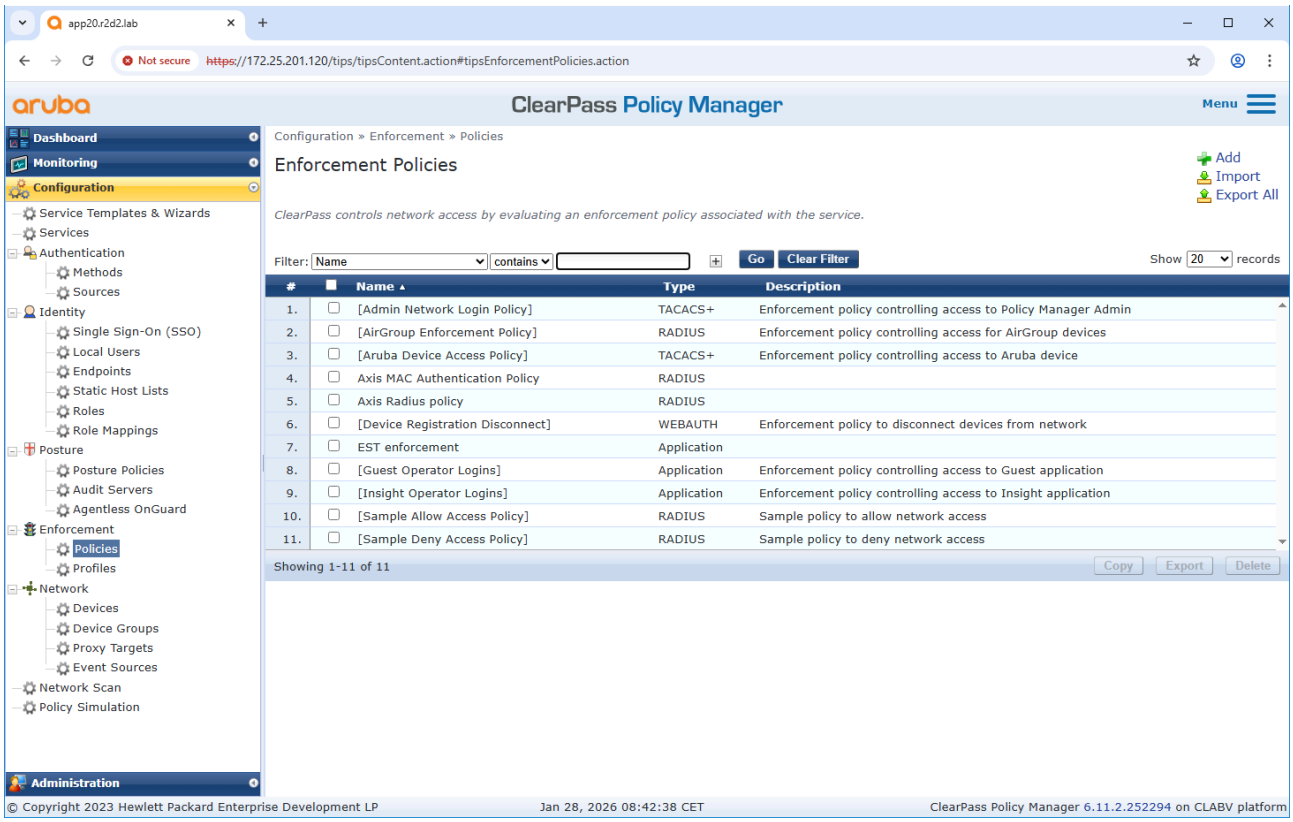


Si cela n'a pas encore été fait, veuillez charger les *certificats IEEE 802.1AR spécifiques à Axis* dans le magasin de certificats de confiance de ClearPass Policy Manager. Veuillez vous assurer que l'utilisation du protocole EST a

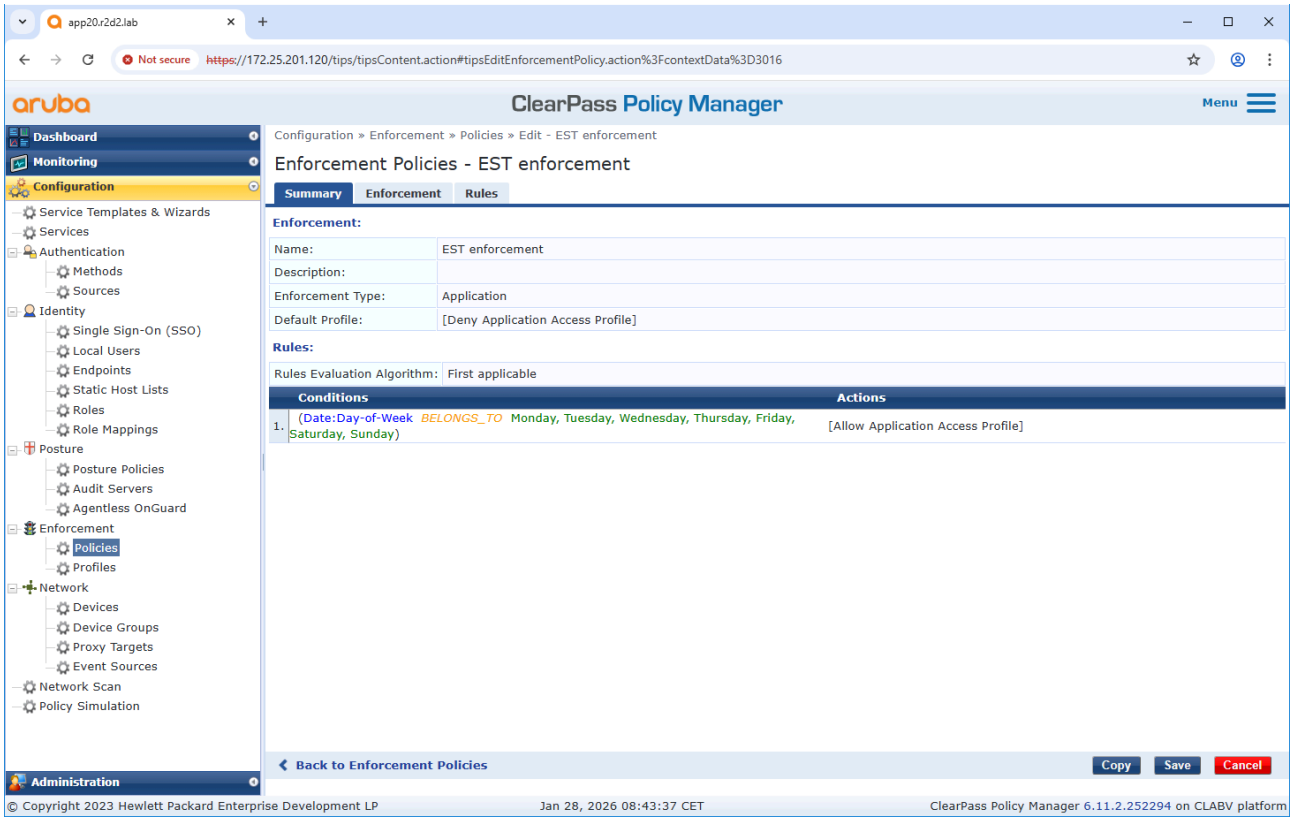
été ajoutée. Veuillez également le vérifier pour l'autorité de certification précédemment créée à partir de ClearPass Onboard.

Configuration de la politique d'application

Le profil d'application permet à ClearPass Policy Manager d'assigner des applications spécifiques à l'application EST. Par exemple, les nouveaux certificats ne peuvent être enregistrés qu'à partir de points de terminaison spécifiques ou uniquement certains jours de la semaine.

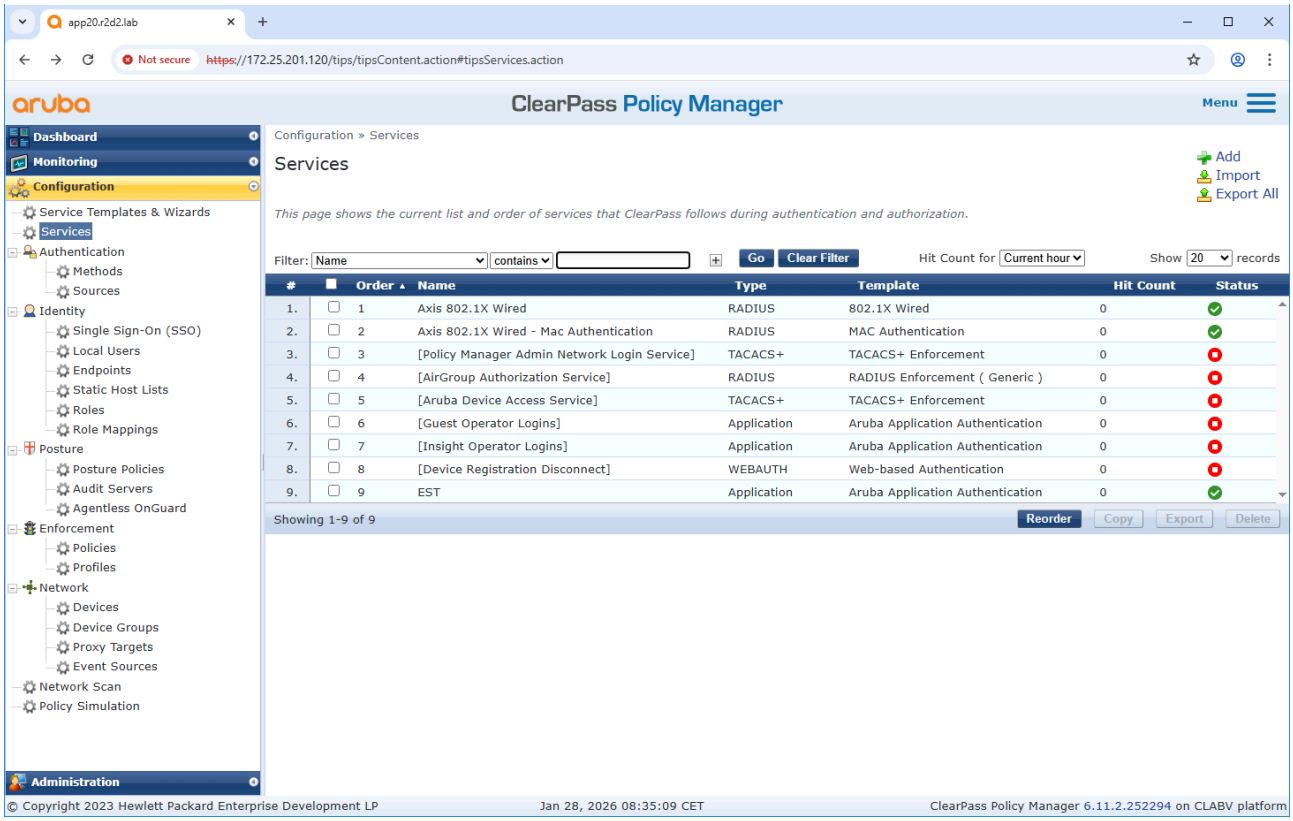


Aperçu des politiques d'application dans ClearPass Policy Manager.

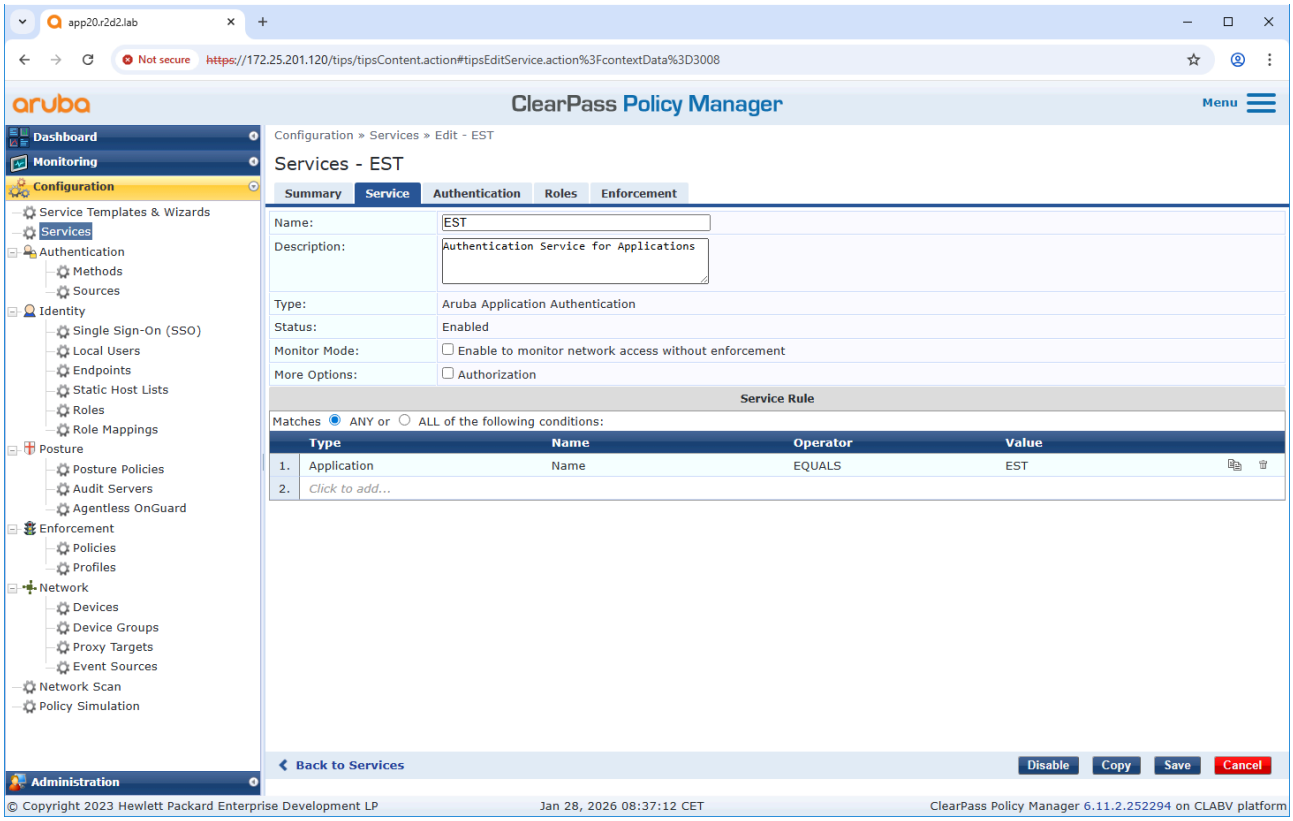


Dans cet exemple de politique, l'application EST est autorisée tous les jours de la semaine.

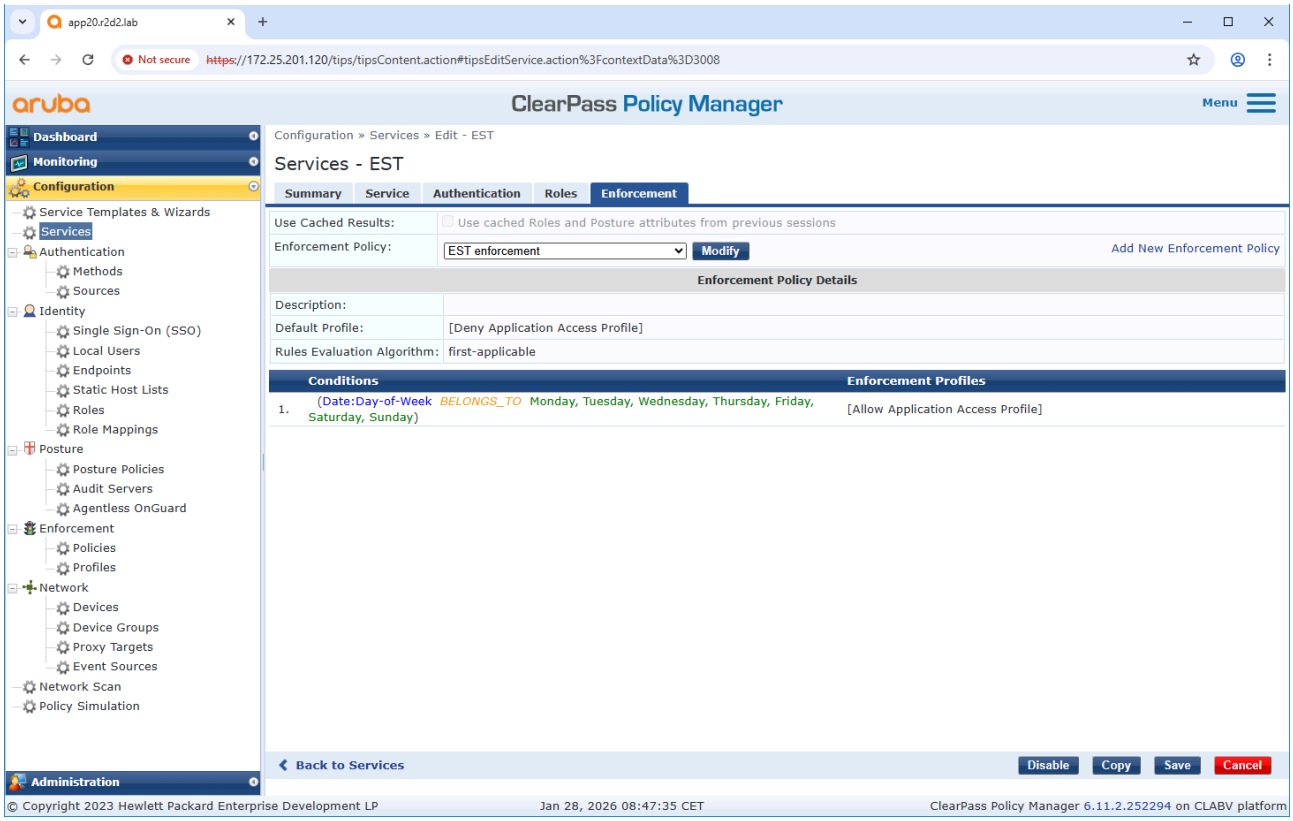
Configuration du service



Il est nécessaire de créer un service EST dédié.



Le service doit être configuré pour l'application EST.



Veuillez sélectionner la politique d'application EST précédemment créée.

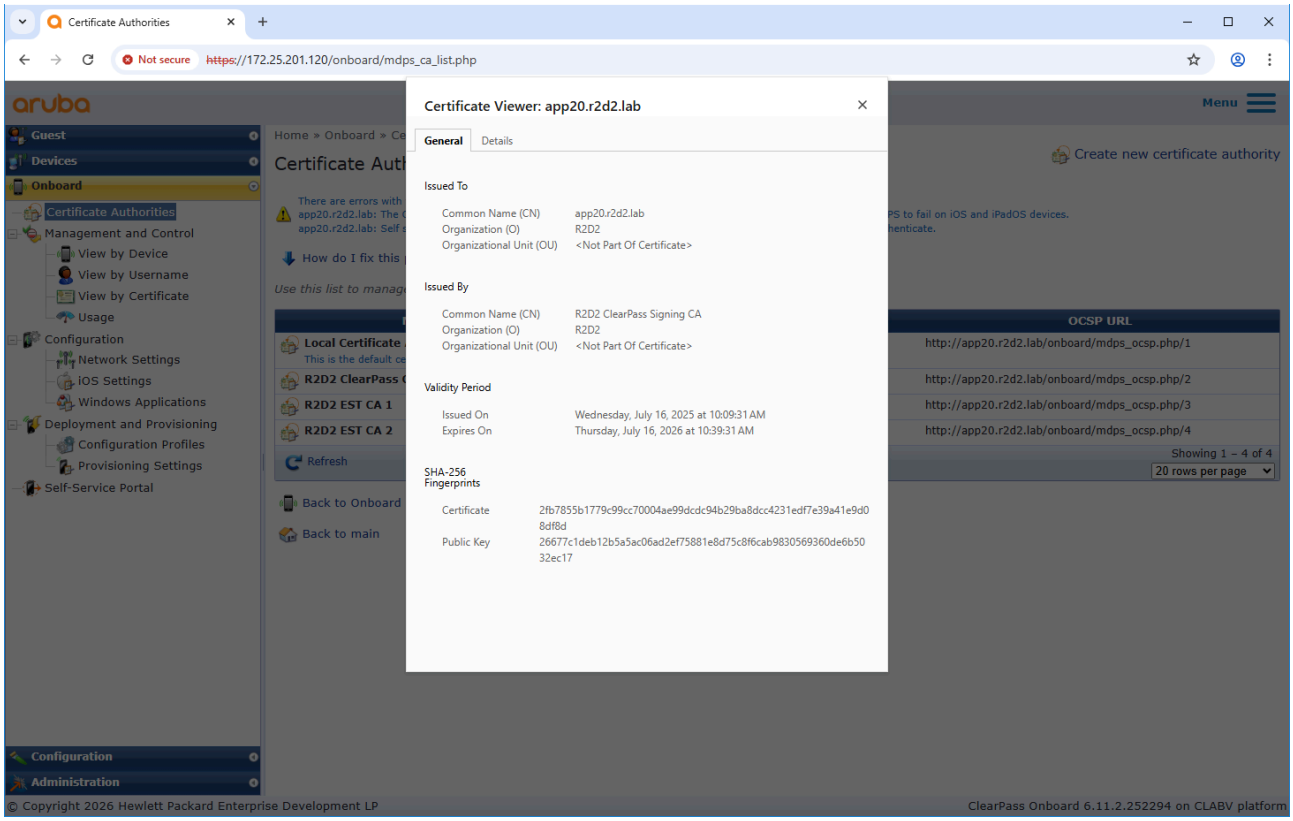
Configuration Axis

La configuration sur le dispositif Axis s'effectue en deux étapes.

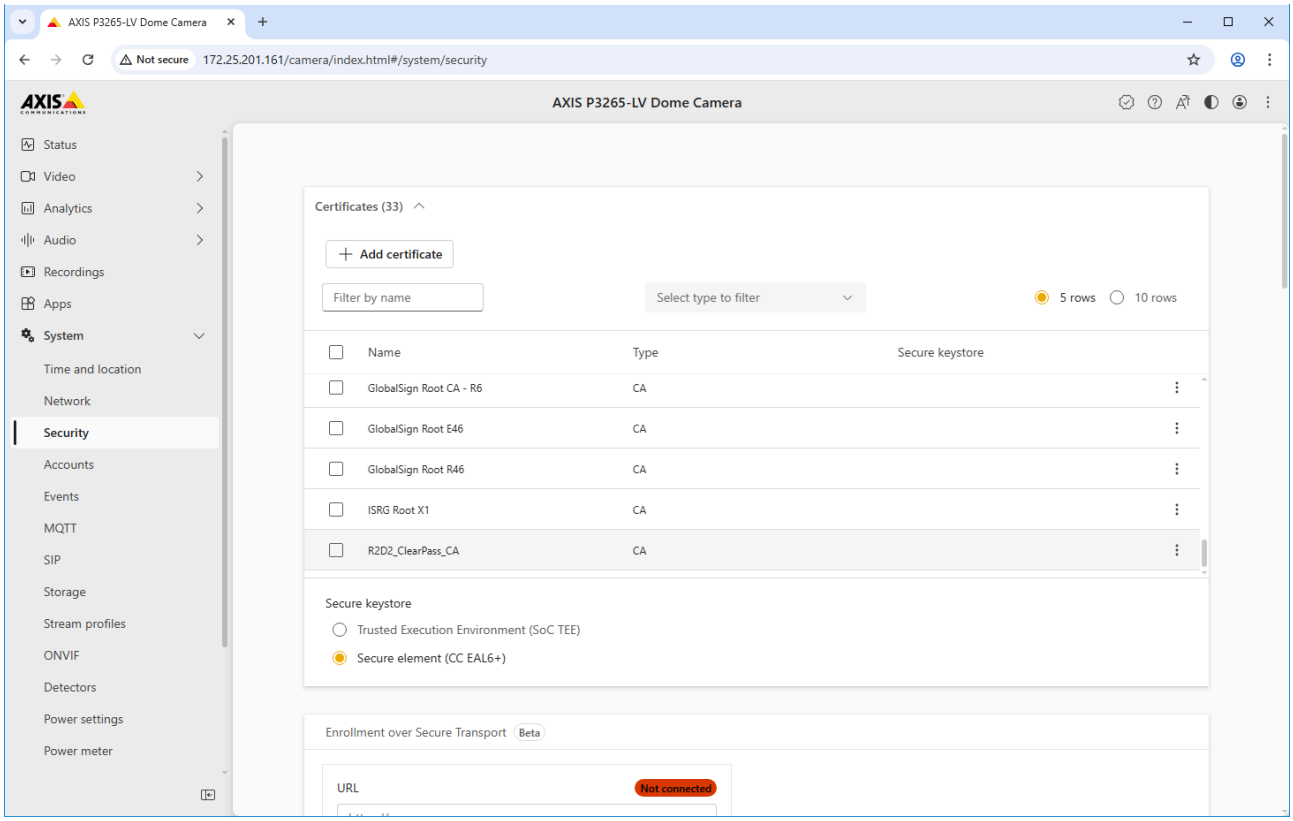
1. Veuillez établir une relation de confiance avec le point de terminaison HTTPS ClearPass Onboard.

2. Veuillez configurer le client EST sur le dispositif Axis.

Configuration du certificat de confiance

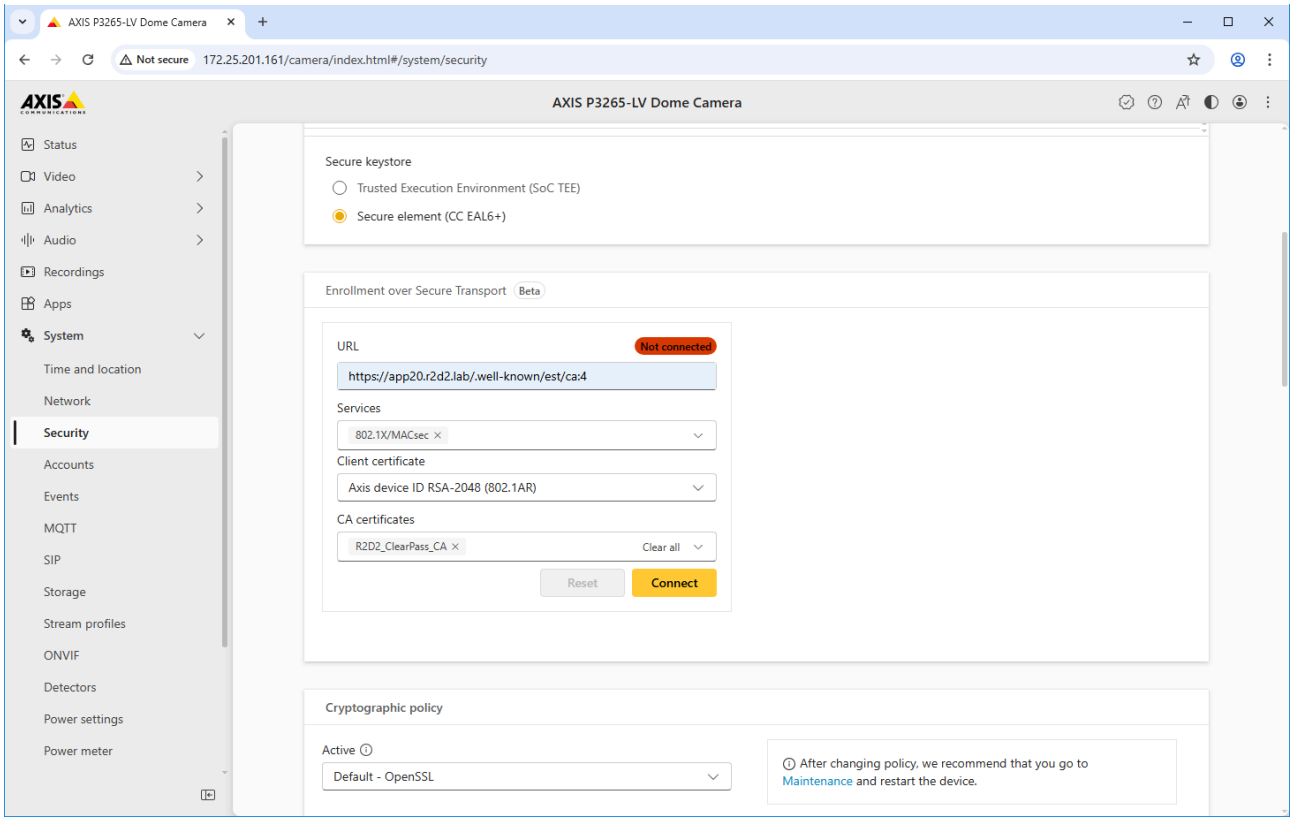


Veuillez vérifier la chaîne de certificats à partir du point de terminaison HTTPS ClearPass Onboard.

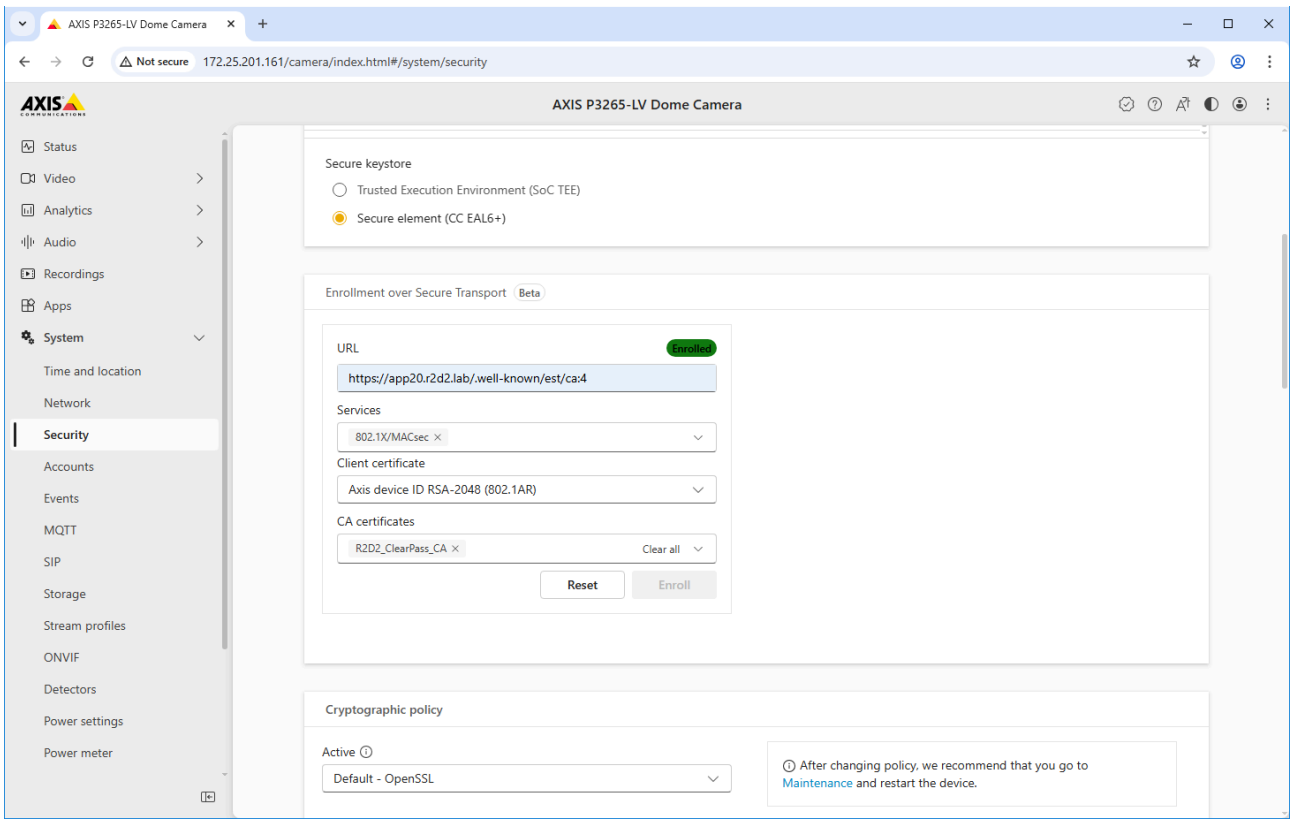


Veuillez charger l'autorité de certification dans le dispositif Axis, à partir du point de terminaison HTTPS ClearPass Onboard.

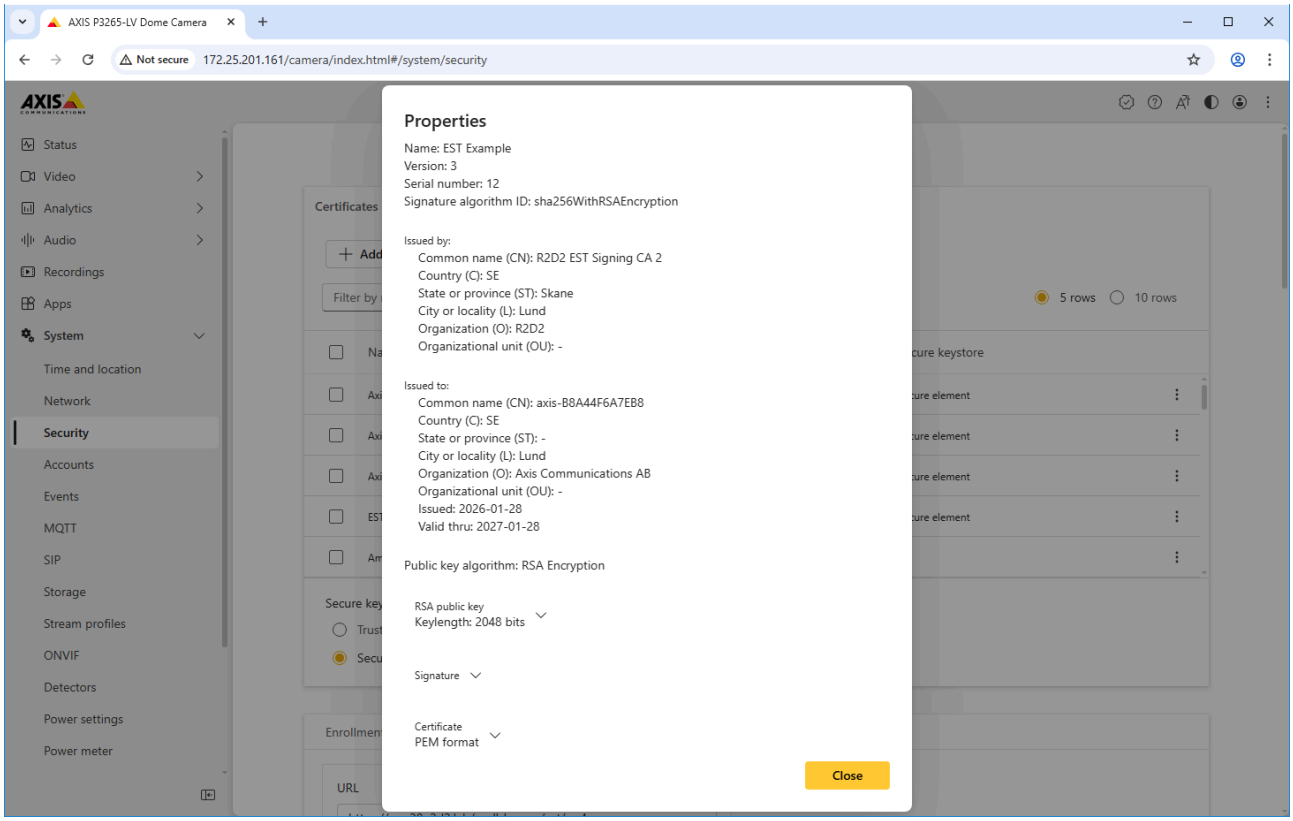
Configuration du client EST



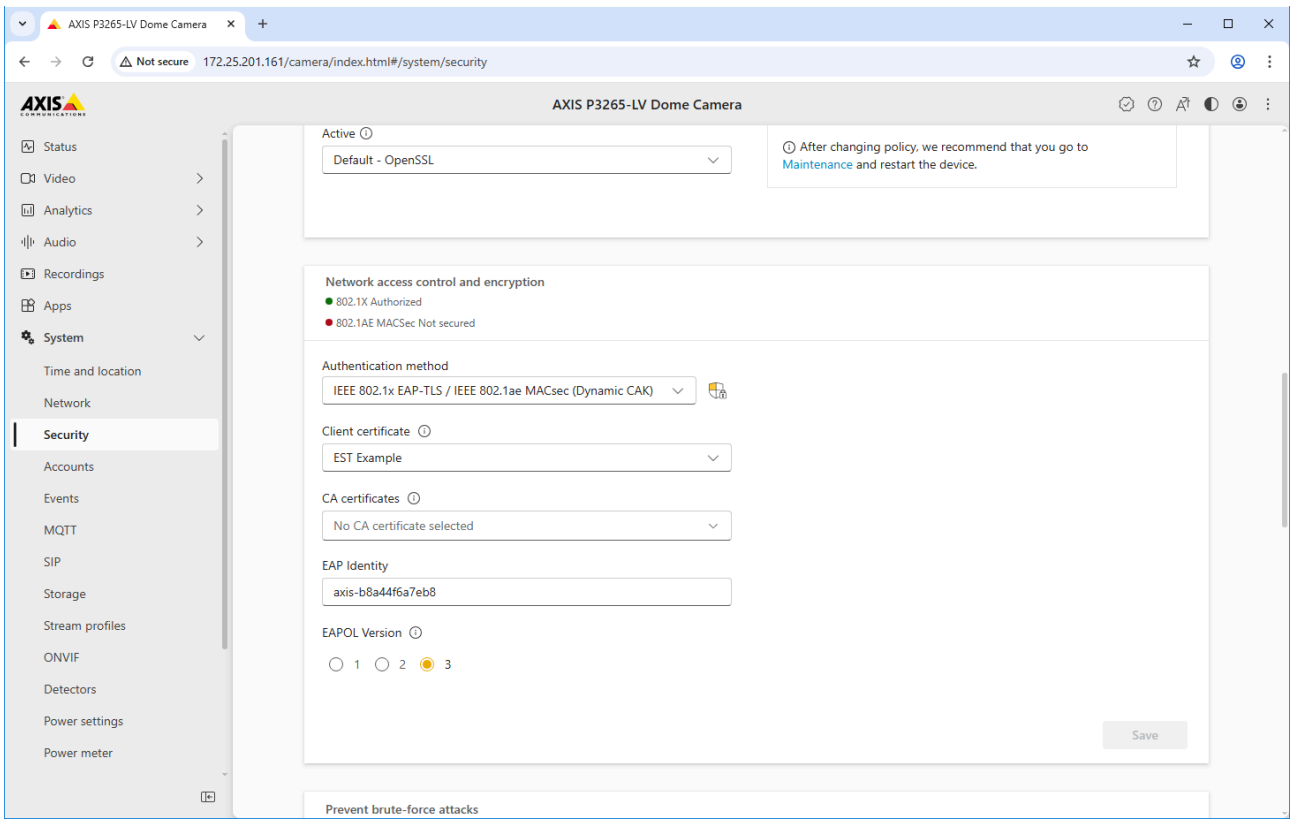
Paramètre	Valeur
URL	L'URL EST se trouve dans l'autorité de certification créée pour EST dans ClearPass Onboard.
Services	Veuillez sélectionner les services qui doivent être automatiquement configurés avec le certificat inscrit.
Certificat client	Veuillez sélectionner un certificat client pour l'authentification auprès du serveur EST ClearPass Onboard. Les dispositifs dotés de l'identifiant de périphérique Axis sont automatiquement considérés comme fiables pour l'inscription, car la chaîne de certificats IEEE 802.1AR spécifique à Axis a été ajoutée au magasin de certificats de confiance dans ClearPass Policy Manager.
Certificats CA	Veuillez sélectionner le Certificat CA à partir du point de terminaison HTTPS ClearPass Onboard, afin que le dispositif Axis fasse confiance à ce point de terminaison.



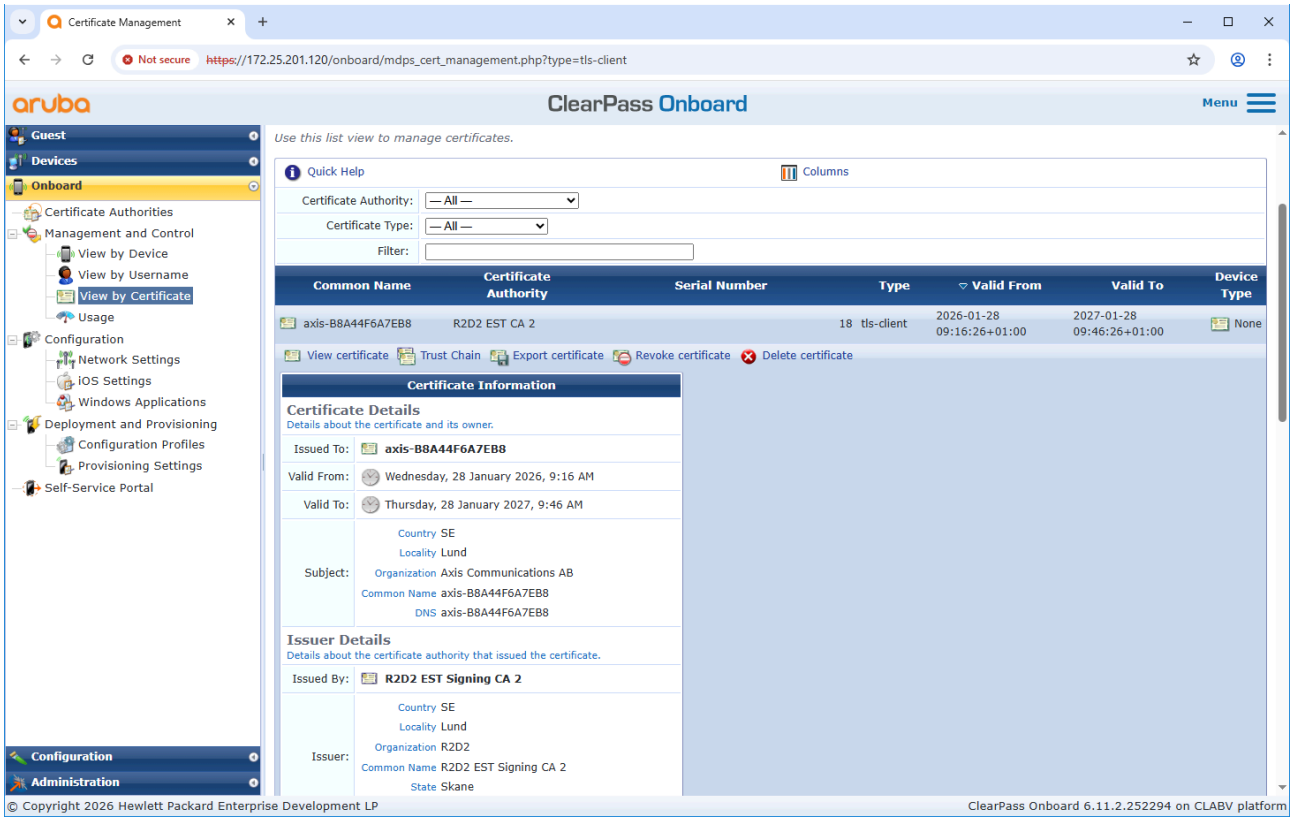
L'inscription a été effectuée avec succès.



Le certificat EST inscrit sur le dispositif Axis.



Le certificat inscrit est automatiquement assigné au service précédemment sélectionné.



Vous pouvez également consulter le certificat inscrit dans ClearPass Onboard.

Intégration héritée – Authentification MAC

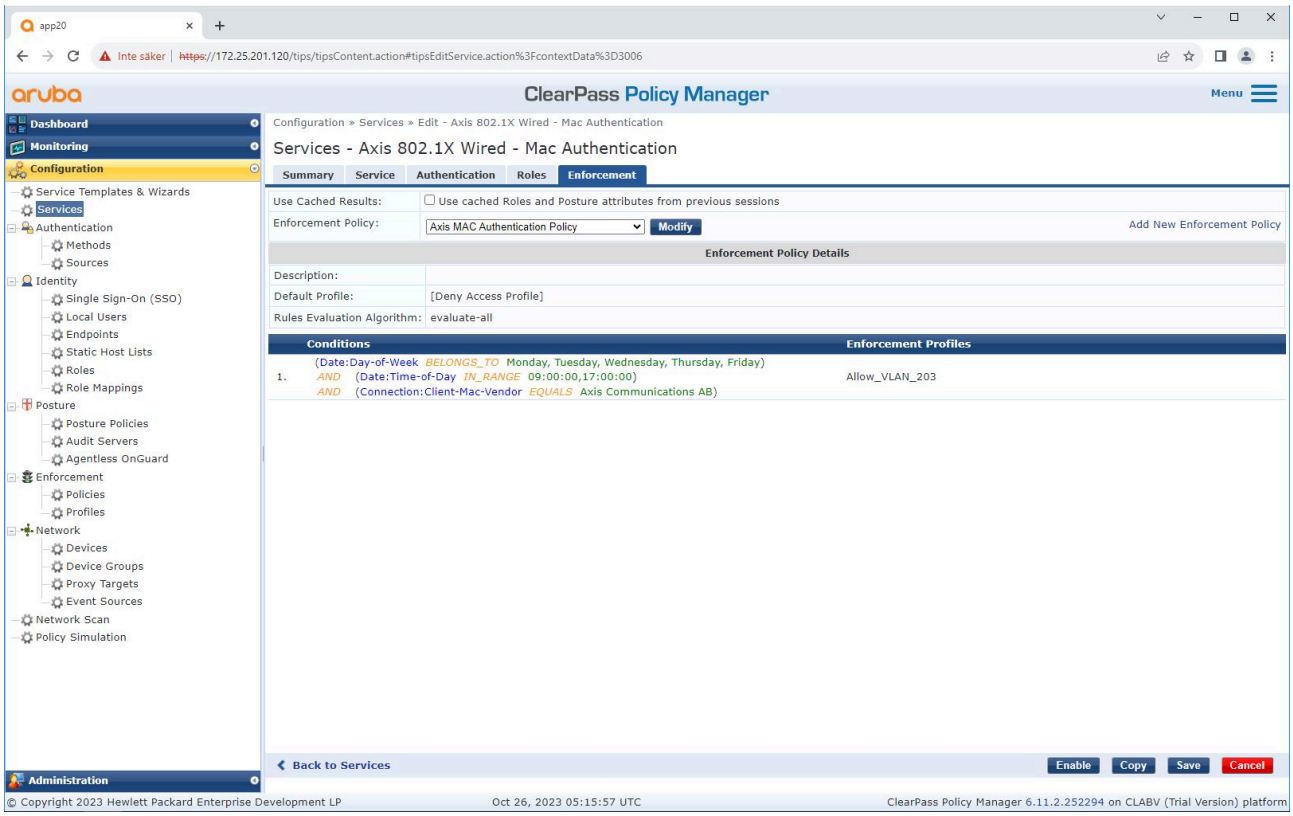
Vous pouvez utiliser MAC Authentication Bypass (MAB) pour intégrer des périphériques Axis qui ne prennent pas en charge l'intégration d'IEEE 802.1AR avec le certificat d'ID de périphérique Axis et IEEE 802.1X activé à l'état d'usine par défaut. Si l'intégration 802.1X échoue, ClearPass Policy Manager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

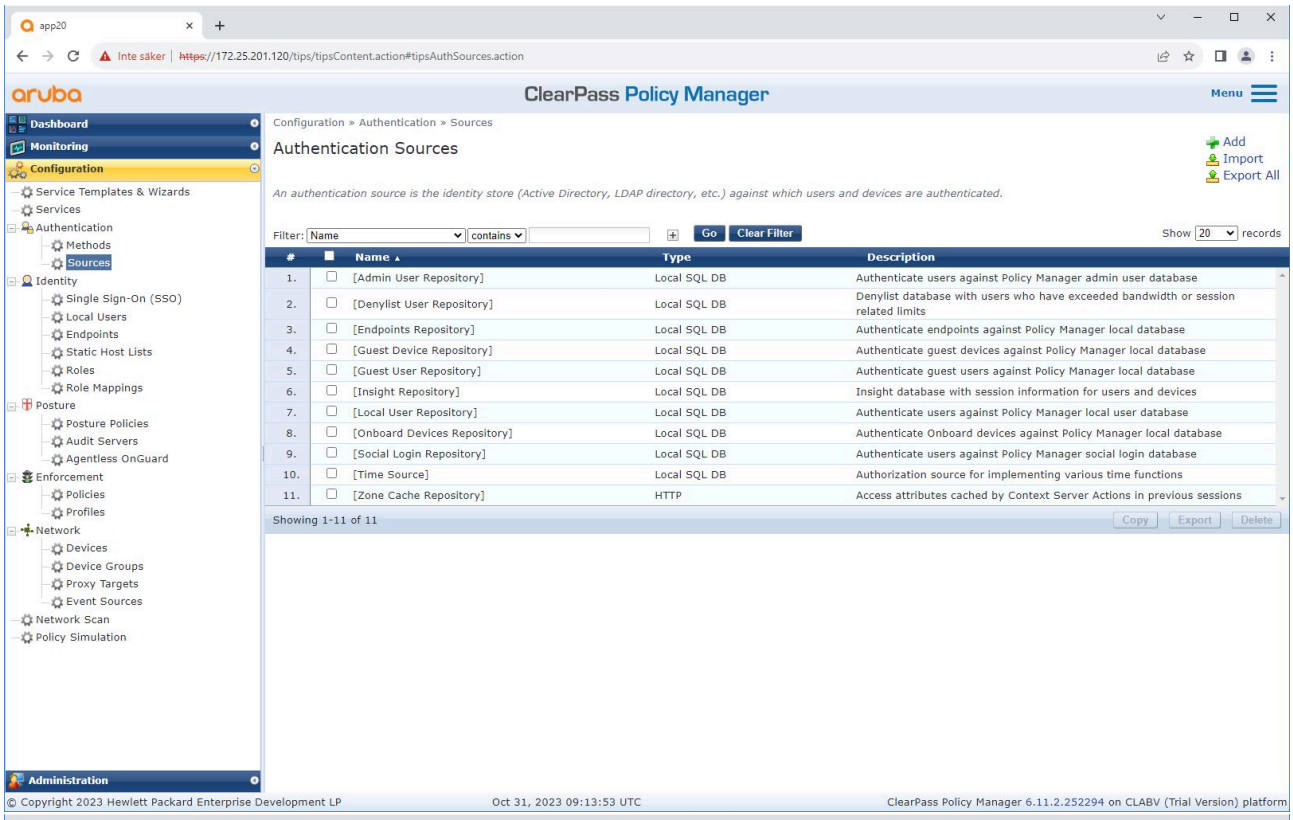
Le périphérique Axis a accès à un réseau limité et isolé si les conditions suivantes sont remplies :

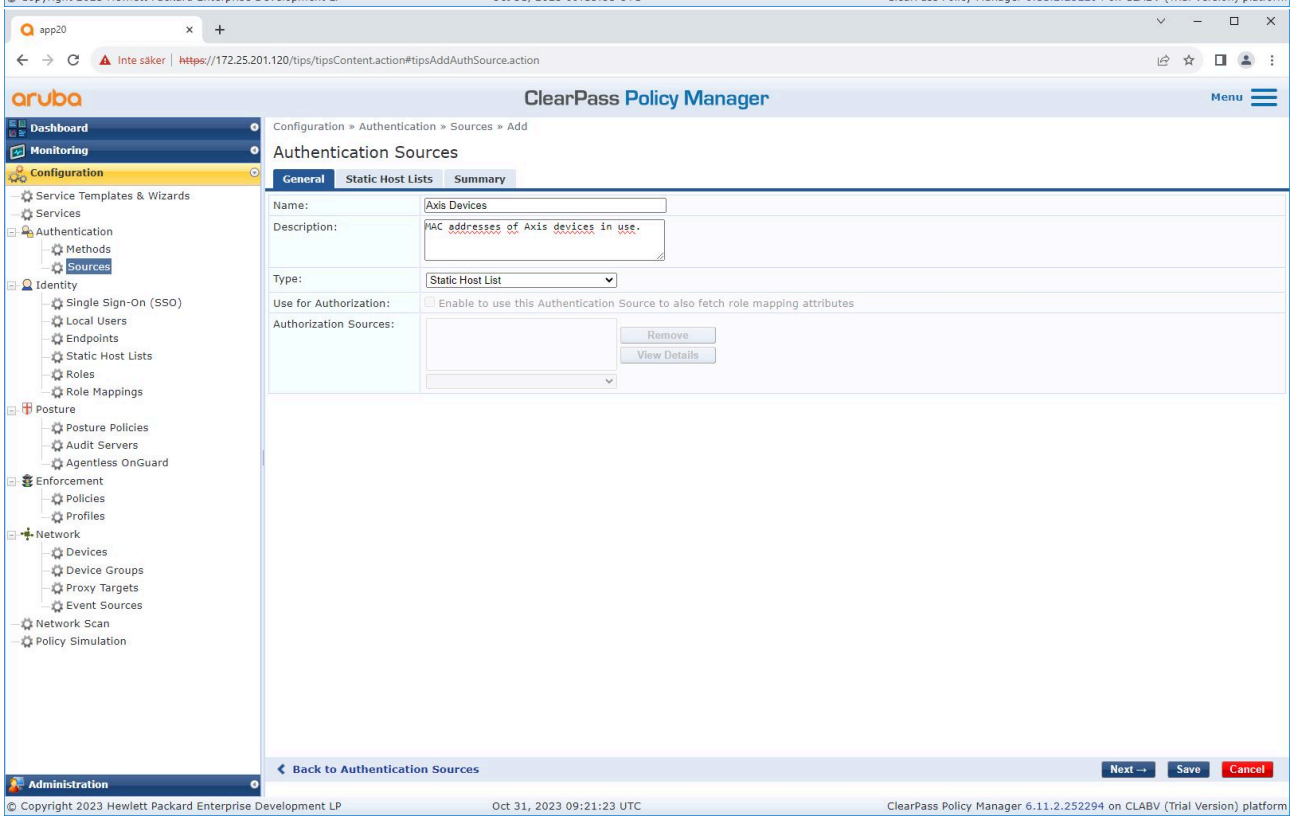
- Le jour est un jour de semaine, du lundi au vendredi.
- L'heure est comprise entre 9 h et 17 h.
- Le fournisseur d'adresse MAC correspond à Axis Communications.

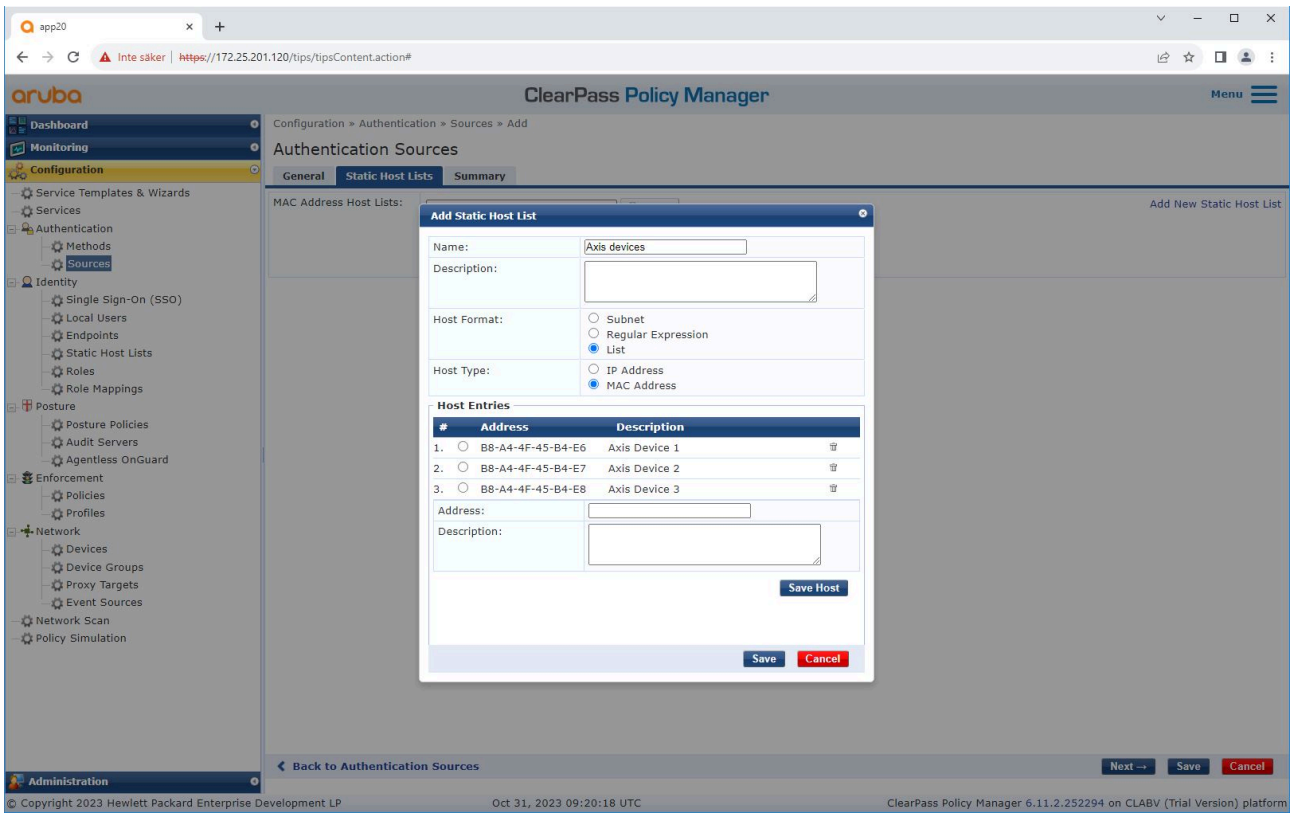
Étant donné qu'il est possible de falsifier une adresse MAC, l'accès au réseau de provisionnement standard n'est pas autorisé. Nous vous recommandons d'utiliser MAB uniquement pour l'intégration initiale, puis d'inspecter manuellement le périphérique plus en détail.

Configuration source

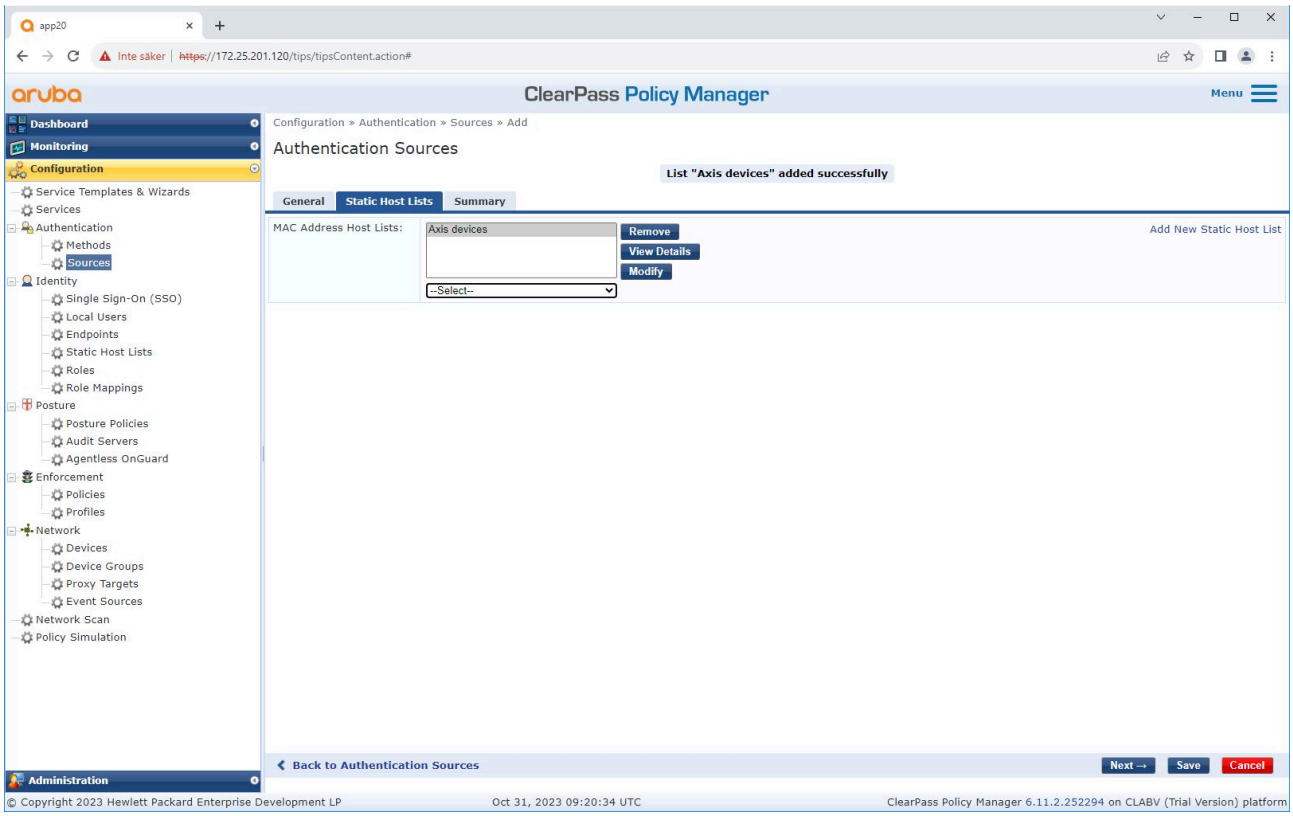
Dans la page **Sources**, une nouvelle source d'authentification est créée pour autoriser uniquement les adresses MAC importées manuellement.





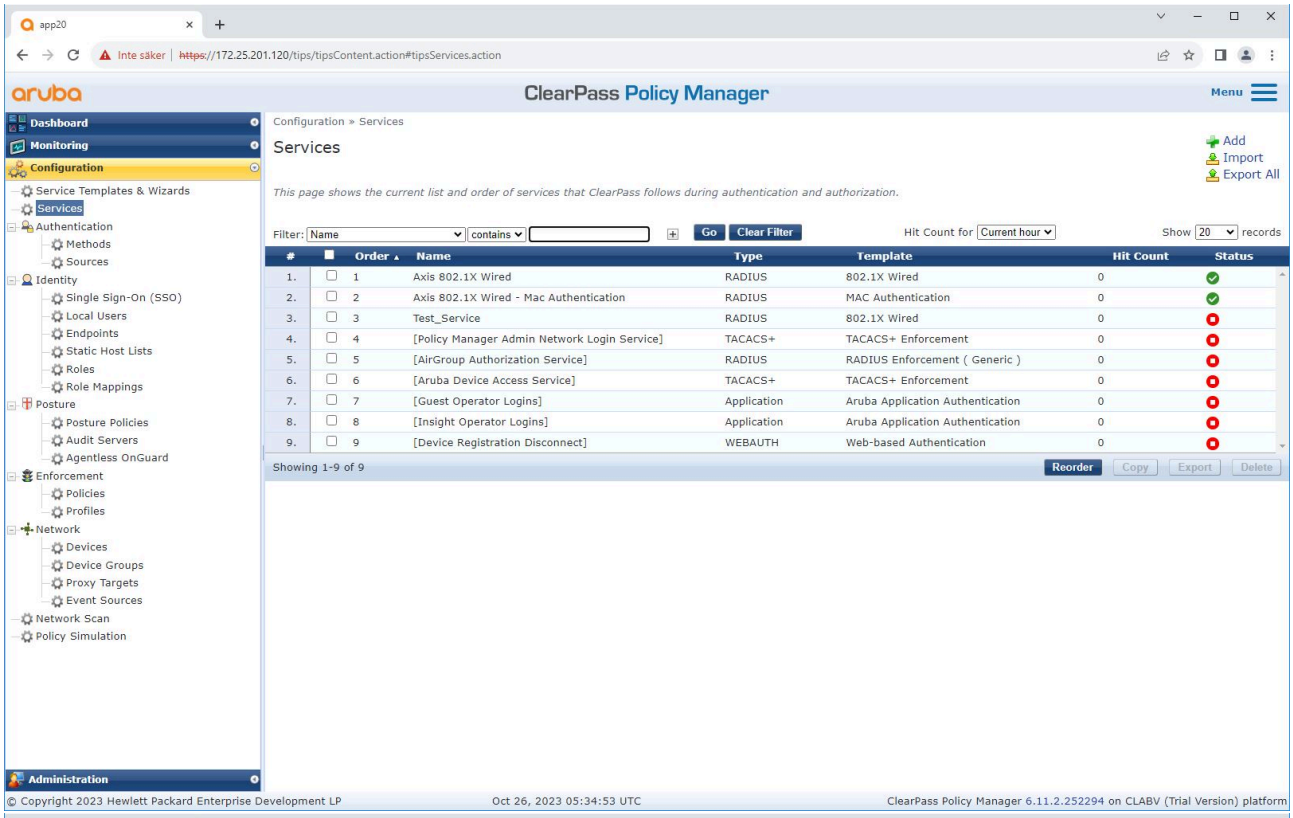


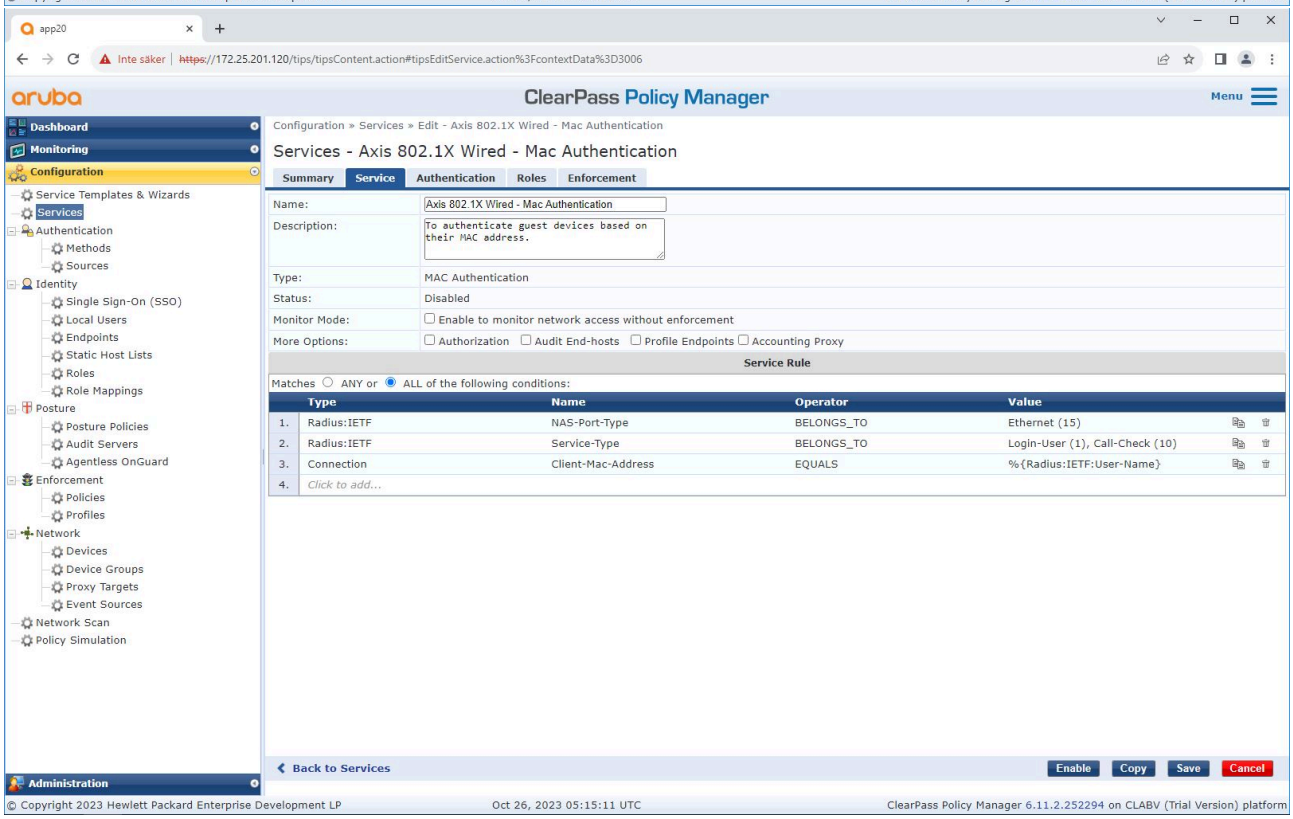
Une liste d'hôtes statique contenant les adresses MAC Axis, est créée.



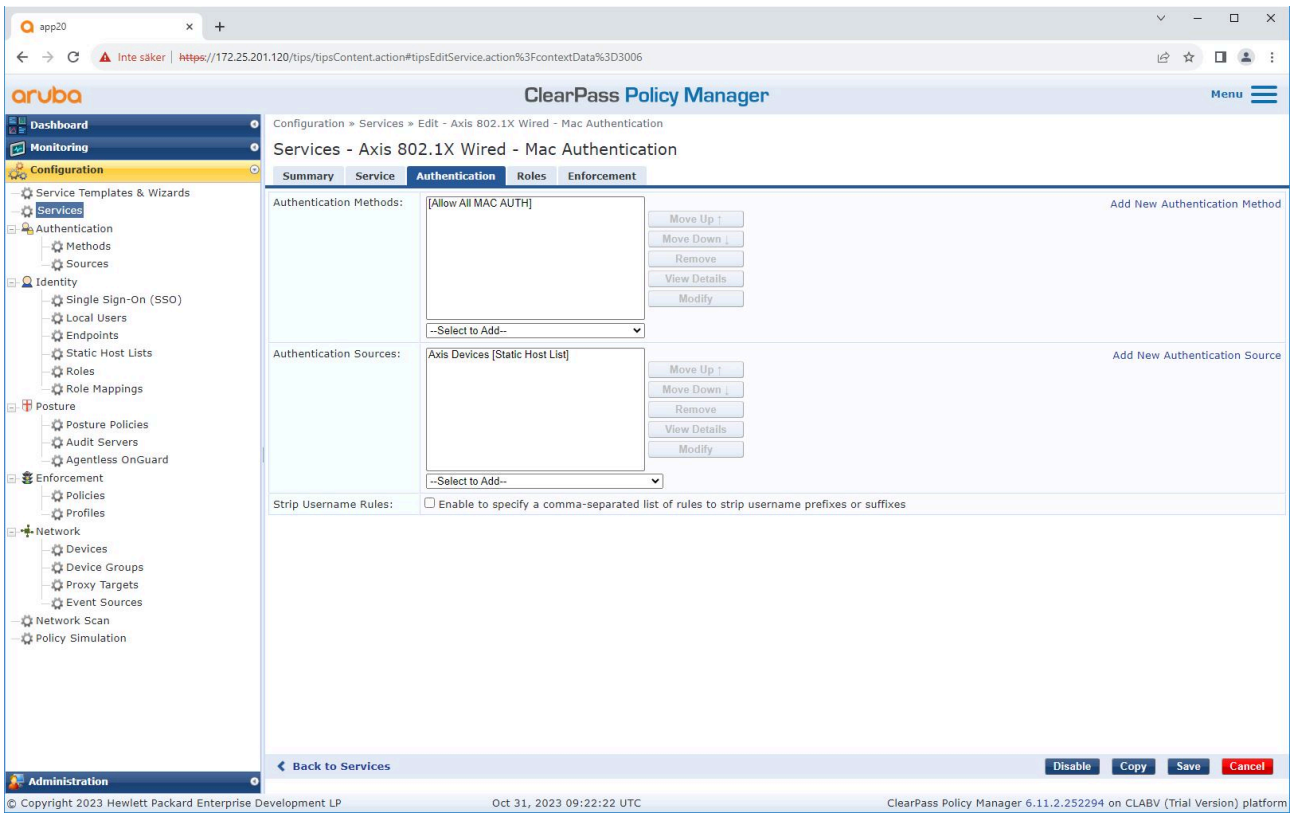
Configuration du service

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.





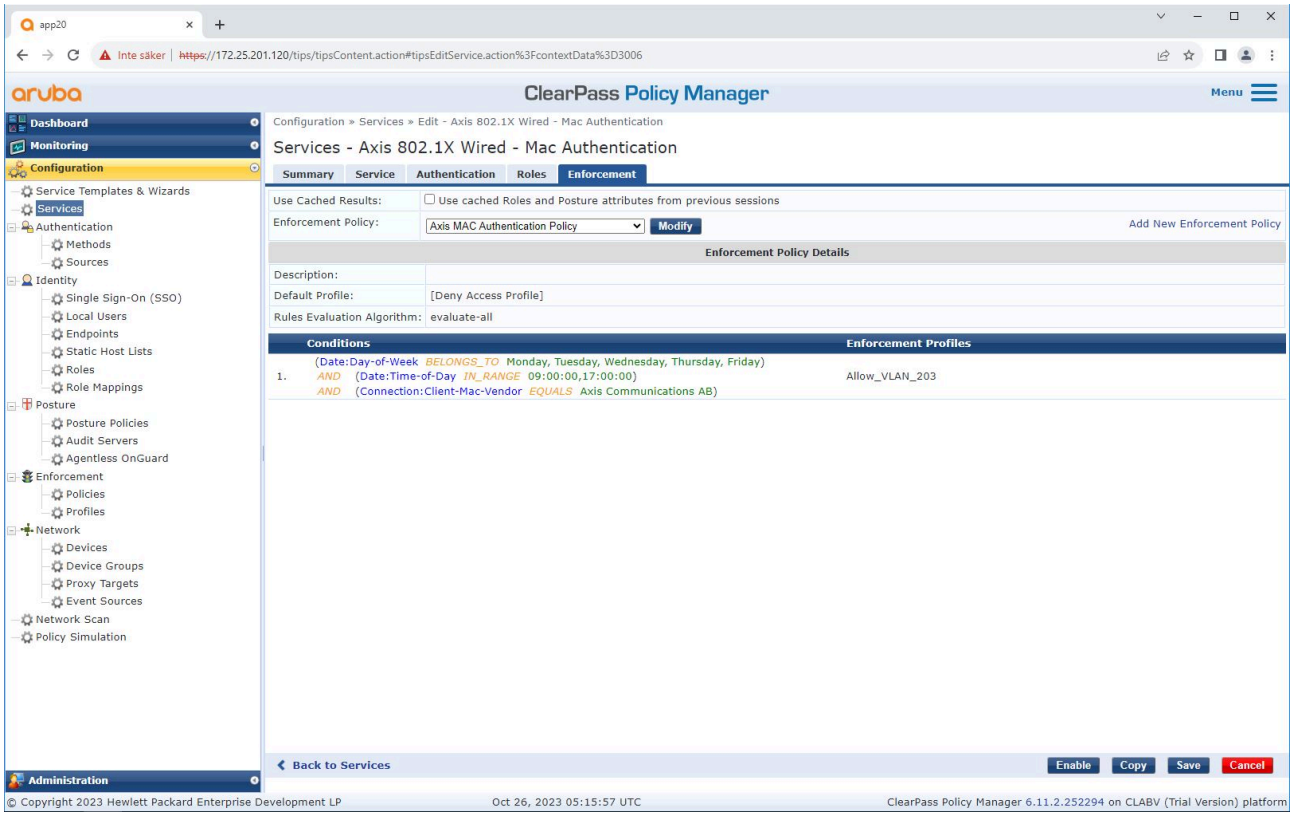
Un service Axis dédié et définissant MAB comme méthode de connexion est créé.



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



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 *Commutateur d'accès HPE Aruba Networking, on page 15*, 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

2026-02 (M8.3)