HPE Aruba Networking

ユーザーマニュアル

目次

はじめに 3
安全なオンボーディング - IEEE 802.1AR/802.1X 4
初期認証 4
プロビジョニング 4
運用ネットワーク 5
HPE Aruba Networkingの設定 6
HPE Aruba Networking ClearPass Policy Manager 6
HPE Aruba Networkingアクセススイッチ 15
Axisの設定 16
Axisネットワーク装置 16
AXIS Device Manager 17
安全なネットワーク運用 - IEEE 802.1AE MACsec 18
HPE Aruba Networking ClearPass Policy Manager 19
ロールとロールマッピングポリシー 19
サービスの設定 20
強制プロファイル 21
HPE Aruba Networkingアクセススイッチ 22
証明書の管理 – セキュアトランスポート経由の登録 (EST) 23
ESTの主な利点 23
HPE Aruba ClearPass のオンボード設定 23
HPE Aruba ClearPass Policy Managerの設定 25
Axisの設定 28
レガシーオンボーディング - MAC認証 33
HPE Aruba Networking ClearPass Policy Manager 33
強制ポリシー 33
ソースの設定 34
サービスの設定 35
HPE Aruba Networkingアクセススイッチ 38

はじめに

この統合ガイドでは、HPE Aruba NetworkingネットワークへのAxisデバイスのオンボーディングと操作における最適な設定について説明しています。この設定では、IEEE 802.1X、IEEE 802.1AR、IEEE 802.1AE、HTTPSなどの最新のセキュリティ標準とプロトコルを使用します。

ネットワーク統合の適切な自動化を確立することにより、時間とコストを節約できます。これにより、Axisデバイス管理アプリケーションをを HPE Aruba Networkingインフラストラクチャーやアプリケーションと合わせて使用する際に、システムの不必要な複雑化を回避できます。HPE Aruba NetworkingインフラストラクチャーとAxisデバイスおよびソフトウェアを組み合わせることで、以下のメリットが得られます。

- デバイスのステージングネットワークの削除によって、システムの複雑性を最小限に抑えられる。
- オンボーディングプロセスの自動化とデバイス管理の追加によって、コストを削減できる。
- Axisデバイスは、ゼロタッチのネットワークセキュリティ管理を提供する。
- HPEとAxisの専門性によって、ネットワーク全体のセキュリティが強化される。

オンボーディングプロセス全体を通じて論理ネットワーク間のソフトウェア定義による円滑な移行を実現するためには、設定を開始する前に、Axisデバイスの完全性を安全に検証できるようにネットワークインフラストラクチャーを準備する必要があります。設定を行う前に以下が必要です。

- HPE Aruba Networkingアクセススイッチや HPE Aruba Networking ClearPass Policy Managerなど、HPE Aruba Networkingのエンタープライズネットワーク ITインフラストラクチャーの管理の経験。
- 最新のネットワークアクセス制御技術とネットワークセキュリティポリシーに関する専門知識。
- できればAxis製品に関する事前の基本知識 (ただし、これはガイドでも提供される)。

安全なオンボーディング - IEEE 802.1AR/802.1X

このビデオを見るには、このドキュメントのWebバージョンにアクセスしてください。

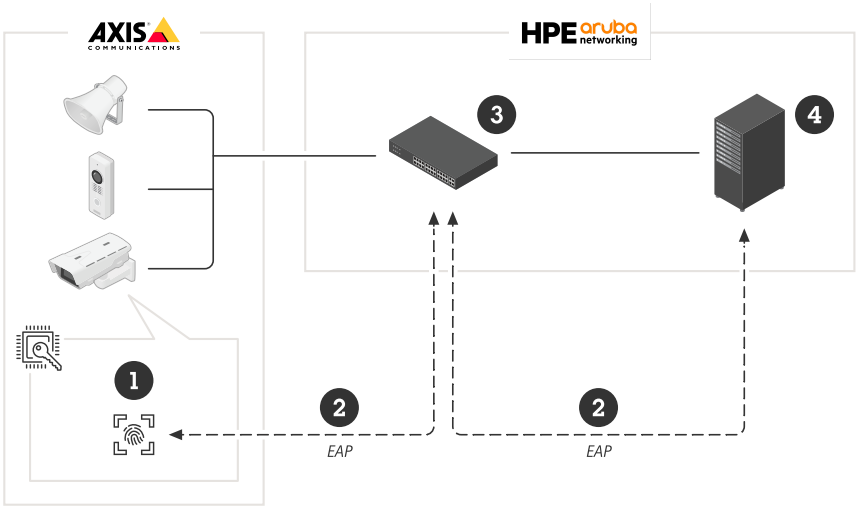
IEEE 802.1X/802.1ARによるゼロトラストネットワークへの安全な装置オンボーディング

初期認証

Axis Edge Vaultに対応するAxisデバイスがネットワークに接続されると、デバイスはIEEE 802.1Xネットワークアクセスコントロールを通じてIEEE 802.1AR Axisデバイス ID証明書を使用し、自己認証を行います。

ネットワークへのアクセスの付与に際し、ClearPass Policy ManagerはAxisデバイスIDとデバイス固有の他のフィンガープリントを検証します。この情報 (MACアドレスやデバイスのAXIS OSバージョンなど) は、ポリシーに基づく決定に使用されます。

Axisデバイスは、ネットワーク上での自己認証に、IEEE 802.1AR準拠のAxisデバイスID証明書を使用します。

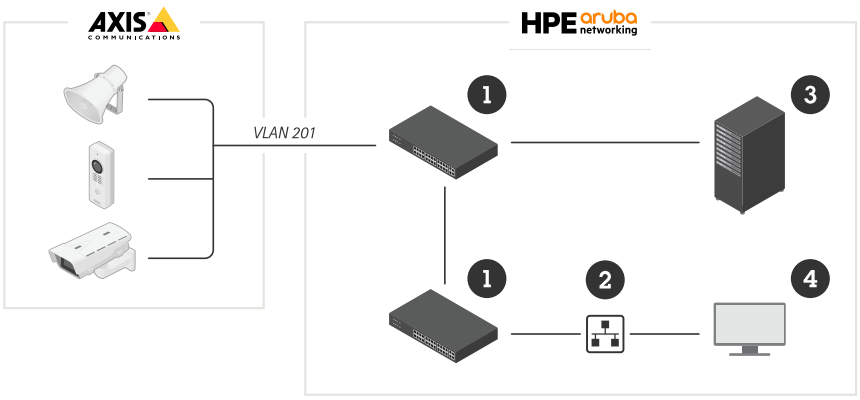


AxisデバイスはHPE Aruba Networkingネットワークに対する認証に、IEEE 802.1AR準拠のAxisデバイスID証明書を使用します。

1. *Axisデバイス ID*
2. *IEEE 802.1x EAP-TLSネットワーク認証*
3. *アクセススイッチ (認証者)*
4. *ClearPass Policy Manager*

プロビジョニング

認証後、Axisデバイスはプロビジョニングネットワーク (VLAN201) に移行します。このネットワークには、AXIS Device Managerが含まれています。これは、デバイス設定、セキュリティ強化、AXIS OSの更新を実行します。デバイスのプロビジョニングを完了するには、IEEE 802.1XおよびHTTPSに対応する、新規顧客固有の運用グレード証明書をデバイスにアップロードします。

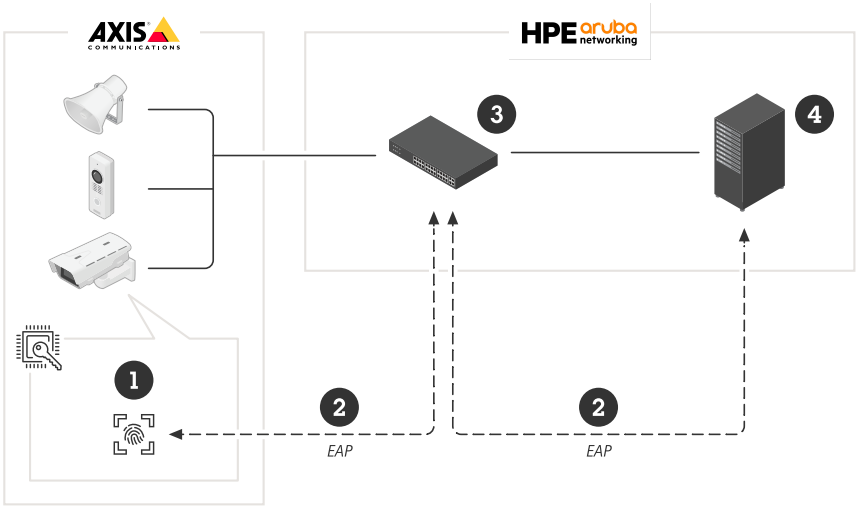


認証が成功すると、Axis装置は構成のためにプロビジョニングネットワークに移行します。

1 *アクセススイッチ*
2 *プロビジョニングネットワーク*
3 *ClearPass Policy Manager*
4 *装置管理アプリケーション*

運用ネットワーク

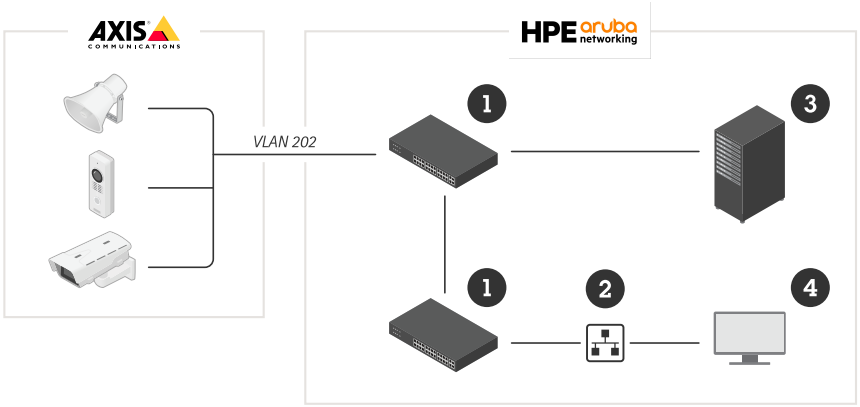
新規のIEEE 802.1X証明書を使用してAxis装置をプロビジョニングすると、新規認証の試行がトリガーされます。ClearPass Policy Managerは、新規の証明書を検証し、Axisデバイスを運用ネットワークに移行するかどうかを決定します。



設定が完了した後、Axisデバイスはプロビジョニングネットワークを離れ、ネットワーク上で再認証を試みます。

1 *AxisデバイスID*
2 *IEEE 802.1x EAP-TLSネットワーク認証*
3 *アクセススイッチ (認証者)*
4 *ClearPass Policy Manager*

再認証後、Axisデバイスは運用ネットワーク (VLAN 202) に移行し、そこでビデオ管理ソフトウェア (VMS) がデバイスに接続し、動作を開始します。



Axis装置には、運用ネットワークへのアクセスが付与されています。

1 *アクセススイッチ*
2 *運用ネットワーク*
3 *ClearPass Policy Manager*
4 *ビデオ管理システム*

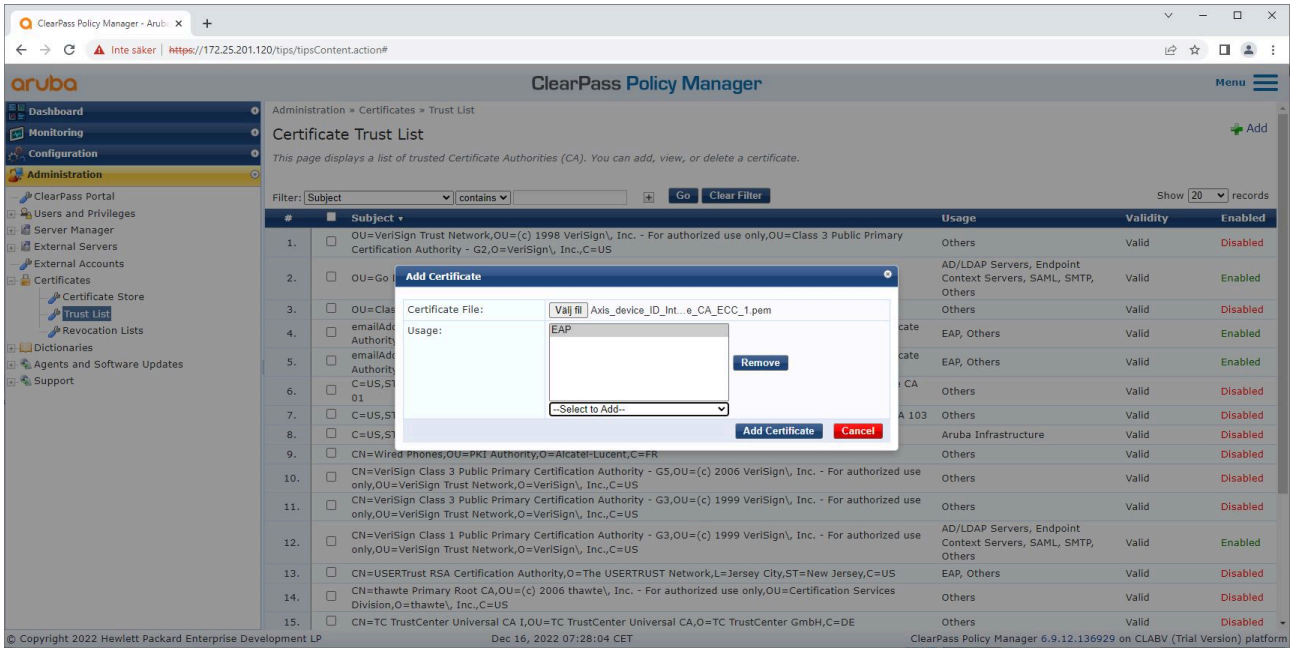
HPE Aruba Networkingの設定

HPE Aruba Networking ClearPass Policy Manager

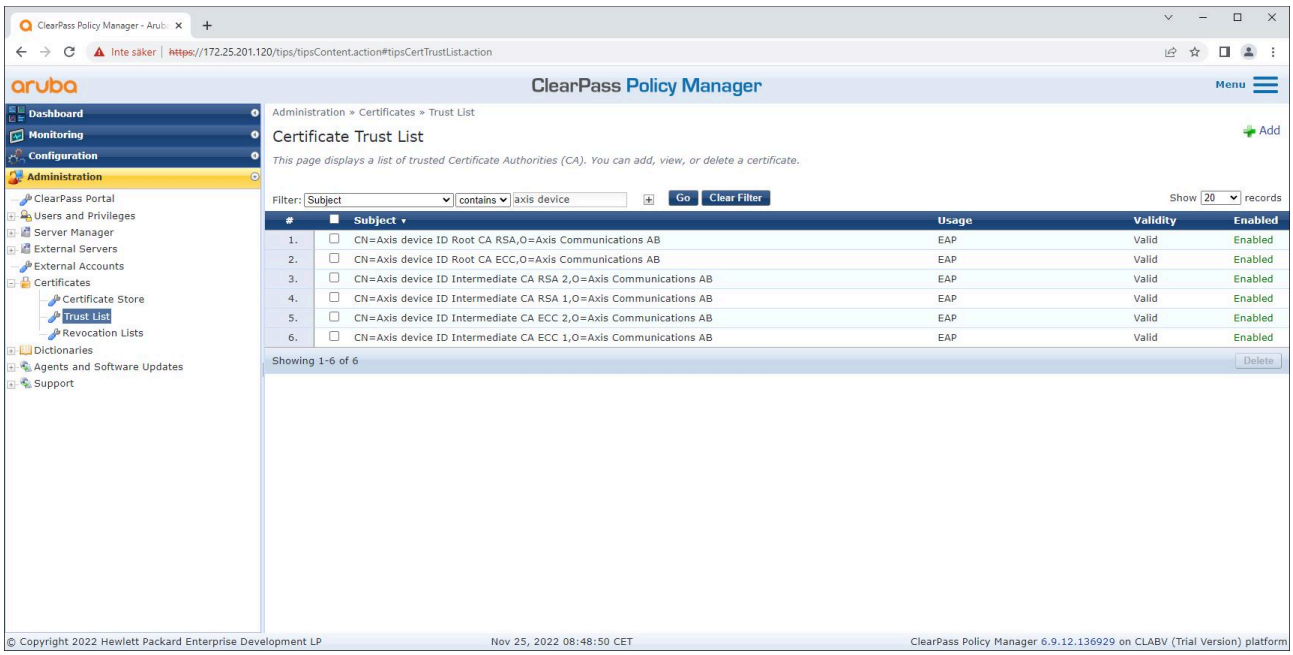
ClearPass Policy Managerは、マルチベンダーの有線、ワイヤレス、VPNインフラストラクチャー全体でIoT、BYOD、コーポレートデバイス、従業員、請負業者、ゲストを対象とする役割ベースとデバイスベースの安全なネットワークアクセスコントロールを提供します。

信頼できる証明書ストアの構成

1. axis.comで、Axis固有のIEEE 802.1AR証明書チェーンをダウンロードします。
2. Axis固有のIEEE 802.1AR Root CAおよび中間CA証明書チェーンを、信頼できる証明書ストアにアップロードします。
3. ClearPass Policy Managerを有効化し、IEEE 802.1X EAP-TLS経由でAxis装置を認証します。
4. 使用フィールドでEAPを選択します。証明書はIEEE 802.1X EAP-TLS認証に使用されます。



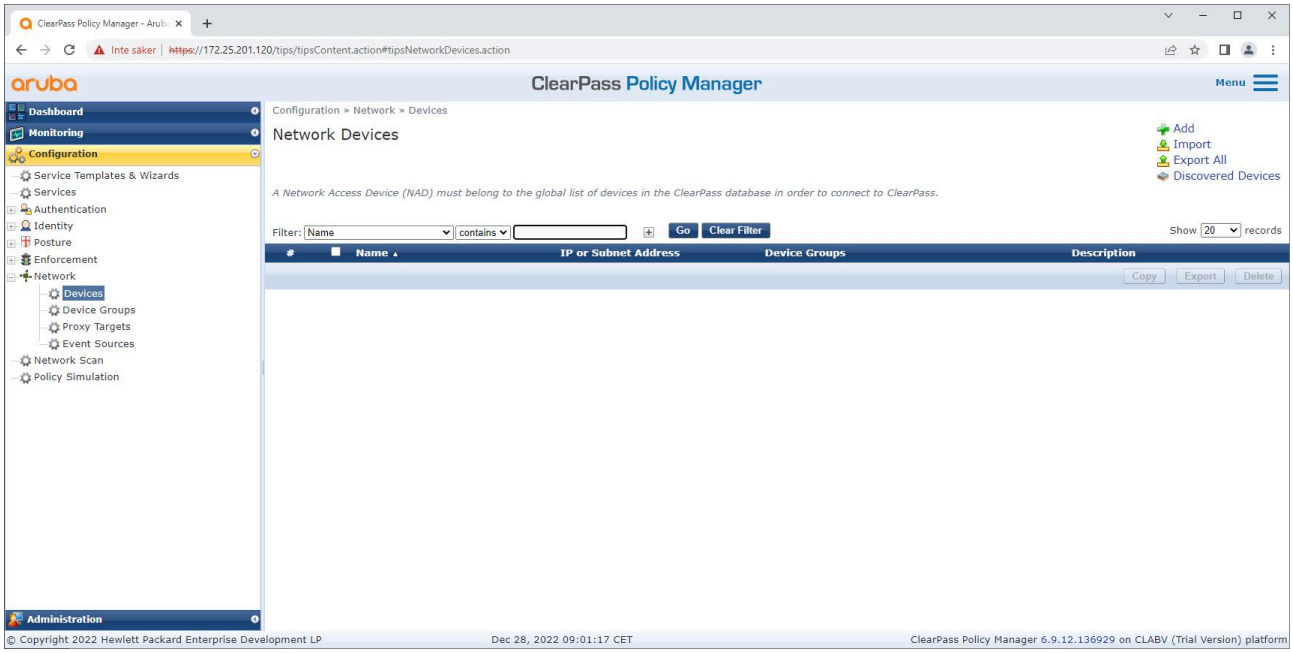
Axis固有のIEEE 802.1AR証明書を、Aruba ClearPass Policy Managerの信頼できる証明書ストアにアップロードします。



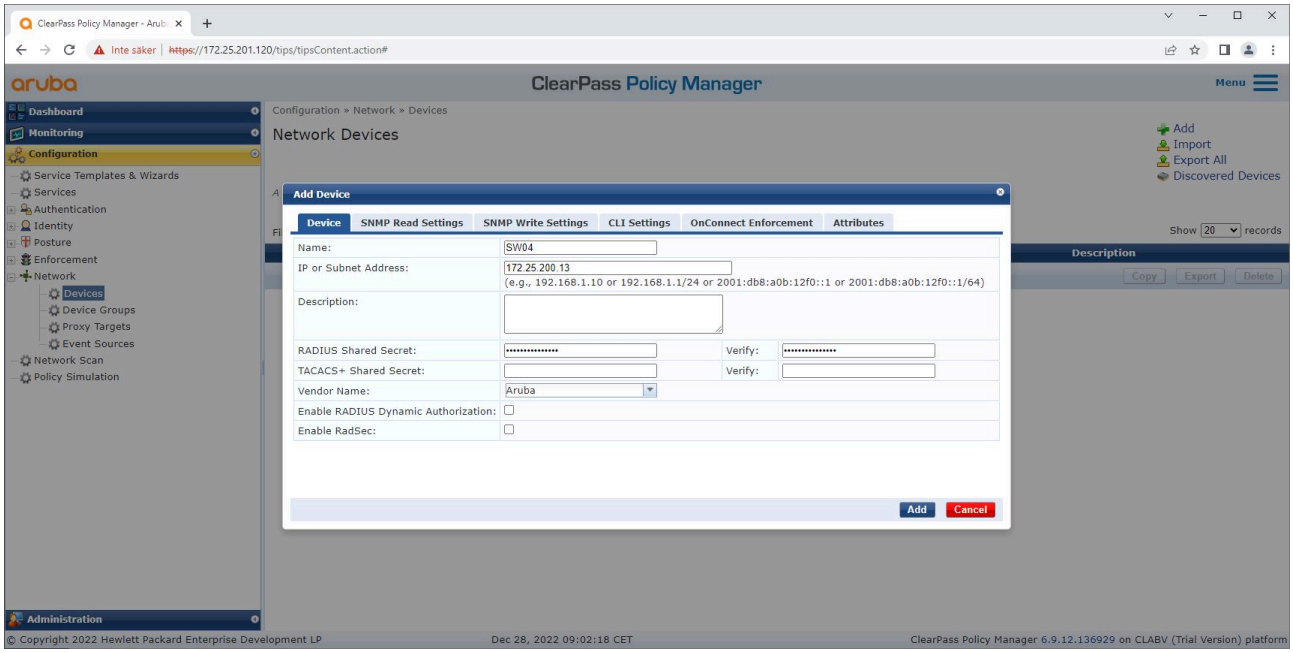
Axis固有のIEEE 802.1AR証明書チェーンを含む、ClearPass Policy Manager内の信頼された証明書ストア。

ネットワーク装置/グループの構成

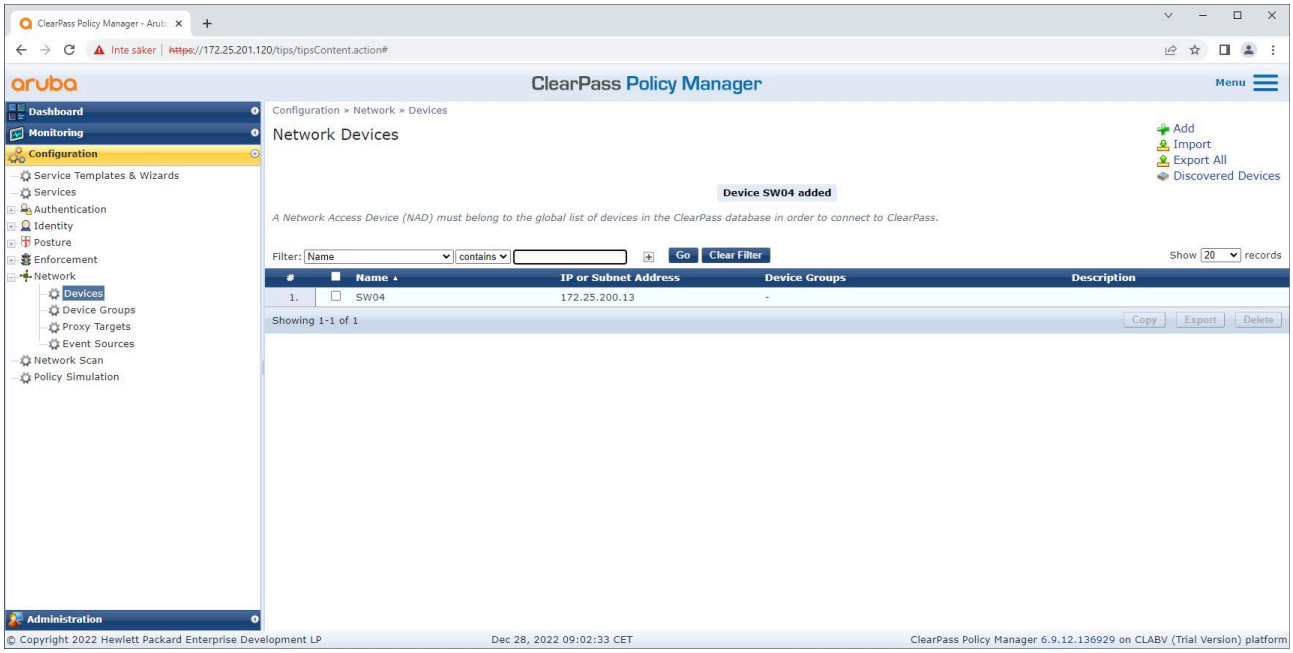
1. HPE Aruba Networkingアクセススイッチなどの信頼できるネットワークアクセス装置をClearPass Policy Managerに追加します。ClearPass Policy Managerは、ネットワーク内でIEEE 802.1X通信に使用されるアクセススイッチを把握する必要があります。RADIUS共有秘密は、特定のスイッチのIEEE 802.1X設定と一致させる必要があることに注意してください。
2. ネットワークデバイスグループ設定を使用して、複数の信頼できるネットワークアクセスデバイスをグループ化します。デバイスをグループ化することで、ポリシー設定が容易になります。



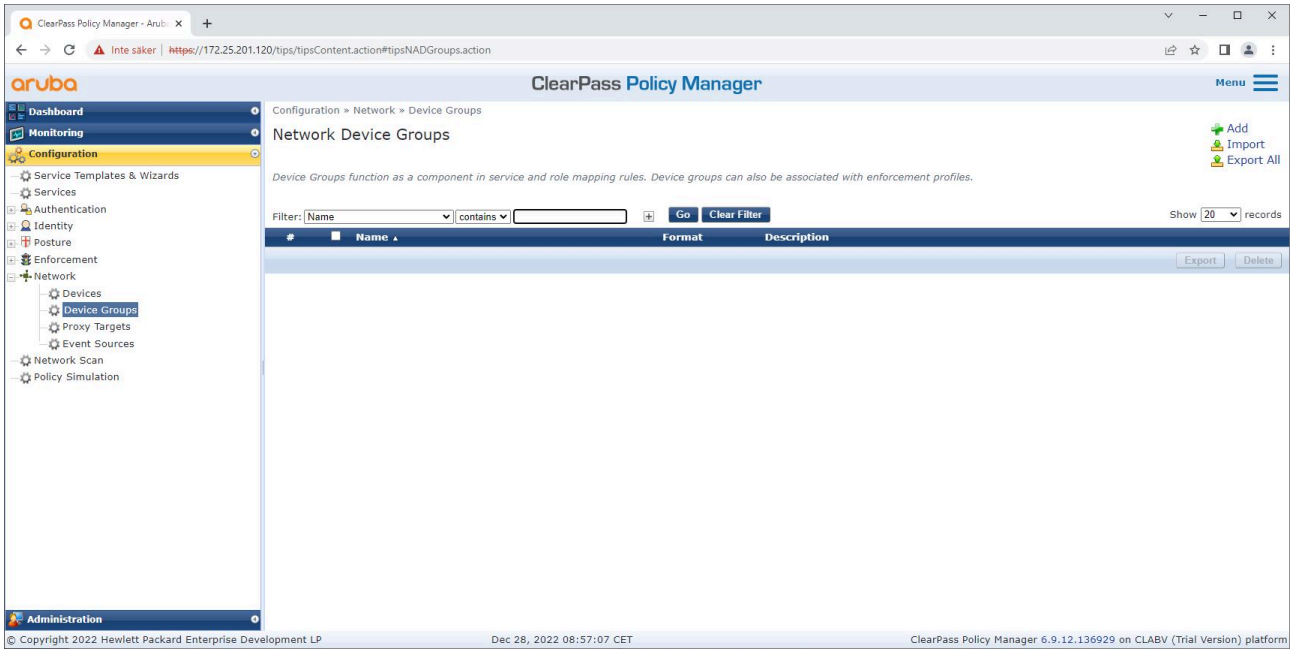
ClearPass Policy Managerの信頼されたネットワーク装置インターフェース。



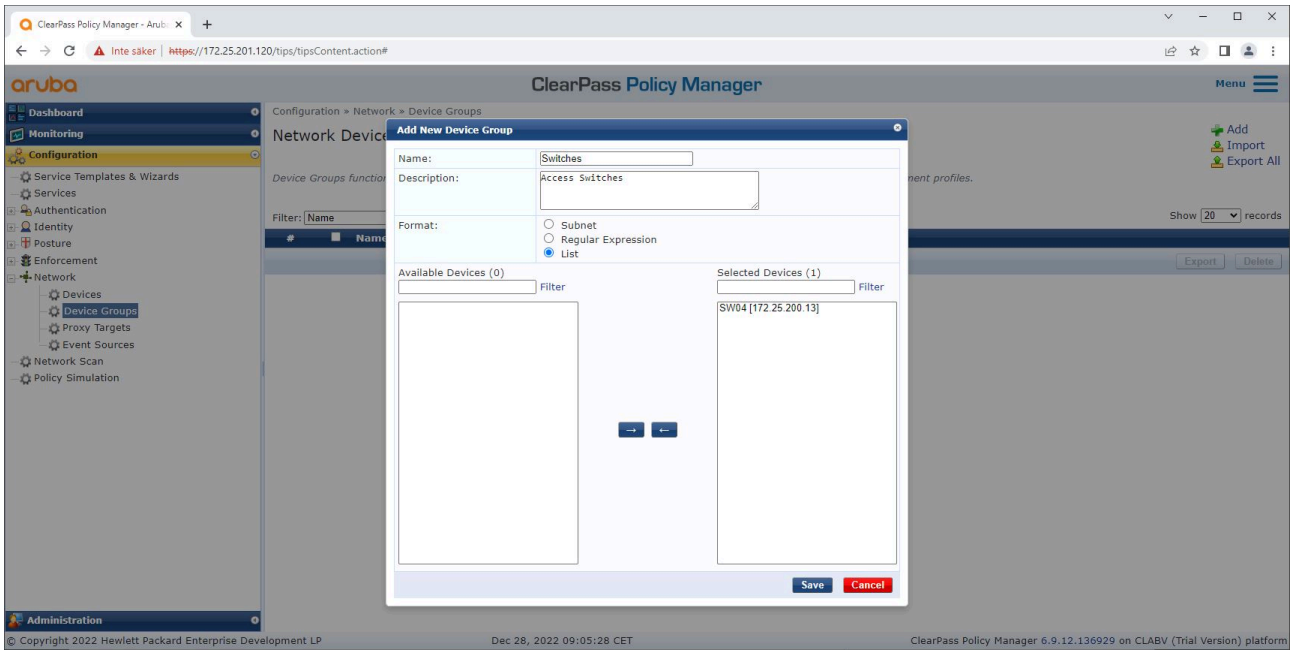
*信頼できるデバイスとしてHPE Aruba Networkingアクセススイッチを*ClearPass Policy Manager*に追加します。RADIUS共有秘密は、特定のスイッチのIEEE 802.1X設定と一致させる必要があることに注意してください。*



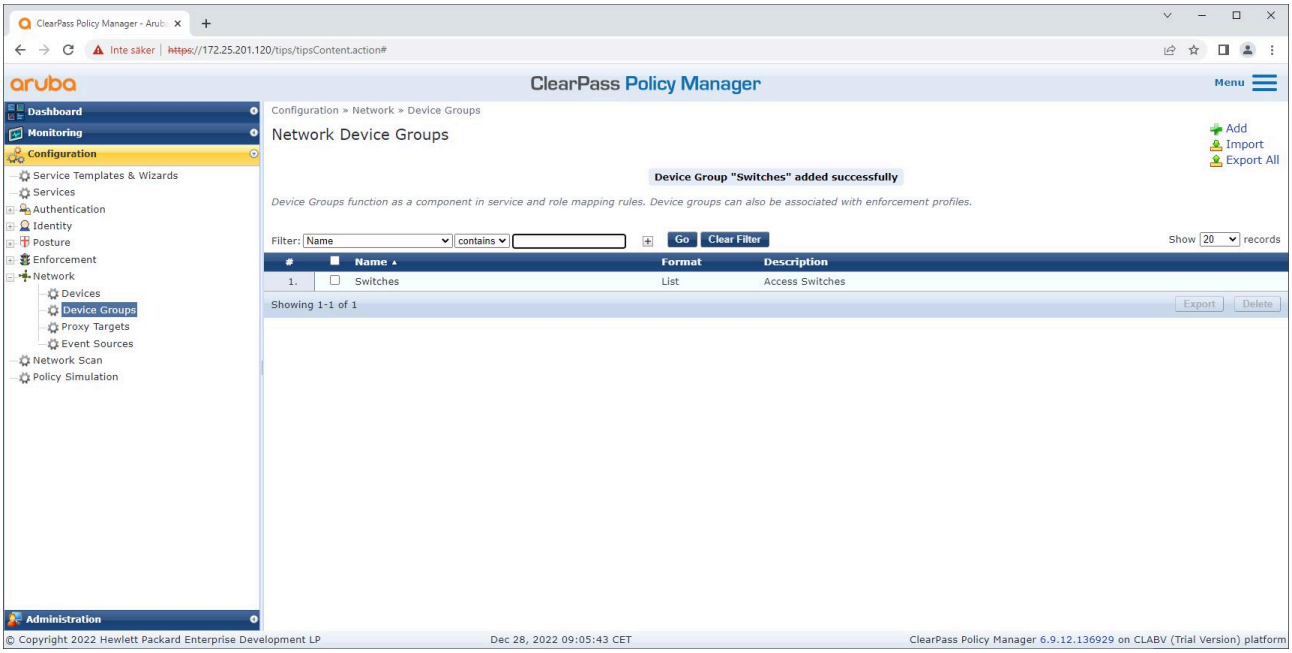
*1つの信頼できるネットワークデバイスが設定された*ClearPass Policy Manager*。*



ClearPass Policy Managerの信頼されたネットワーク装置グループインターフェース。



ClearPass Policy Managerの新規デバイスグループに、信頼されたネットワークアクセスデバイスを追加します。

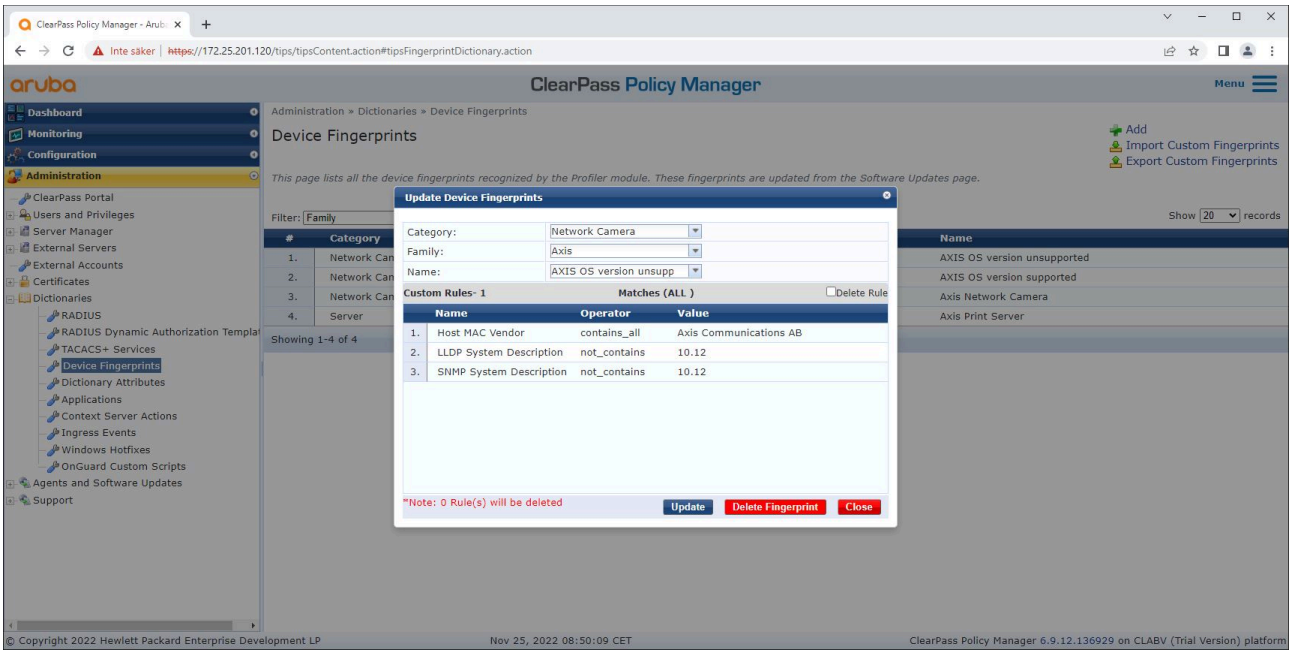


ClearPass Policy Managerで、1つまたは複数の信頼できるネットワークデバイスを含むネットワークデバイスグループが設定された状態。

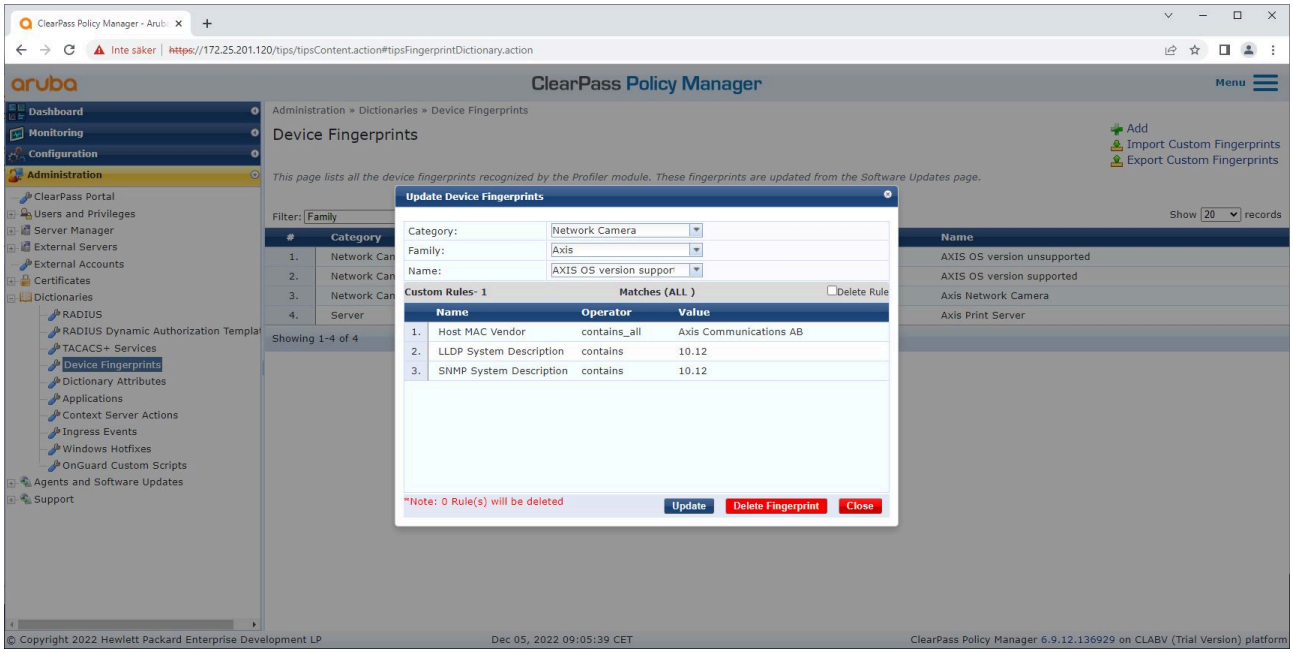
装置のフィンガープリントの構成

Axisデバイスは、ネットワーク検出を通じて、MACアドレスやデバイスソフトウェアのバージョンなど、デバイス固有の情報を配布することが可能です。この情報を使用して、ClearPass Policy Managerでデバイスフィンガープリントを作成、更新、管理します。また、AXIS OSバージョンに基づいてアクセスを許可または拒否することもできます。

1. **[Administration (管理者)] > [Dictionaries (辞書)] > [Device Fingerprints (装置のフィンガープリント)]** に進みます。
2. 既存の装置フィンガープリントを選択するか、新規の装置フィンガープリントを作成します。
3. デバイスフィンガープリントの設定を行います。



ClearPass Policy Managerでの装置のフィンガープリント設定。この例では、AXIS OS バージョン 10.12以外のバージョンを実行しているAxisデバイスはサポートされていません。



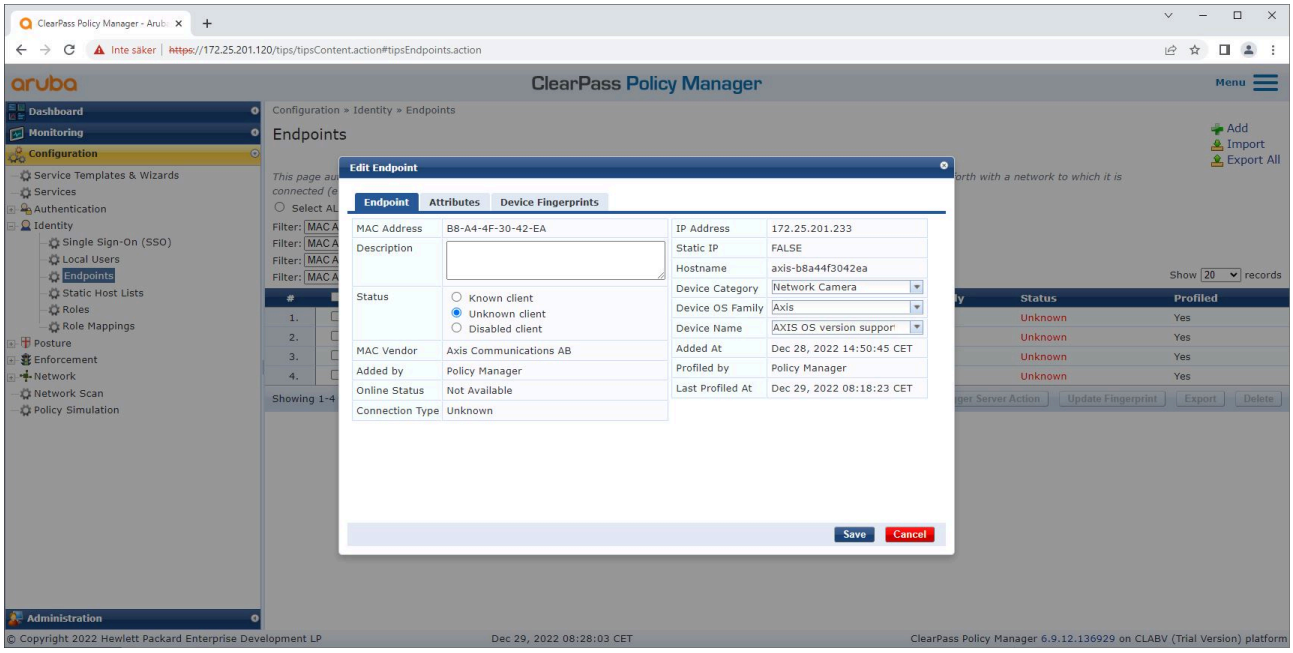
ClearPass Policy Managerでの装置のフィンガープリント設定。この例では、AXIS OS バージョン 10.12以外のバージョンを実行しているAxisデバイスはサポートされています。

ClearPass Policy Managerによって収集された装置のフィンガープリントに関する情報は、エンドポイントセクションにあります。

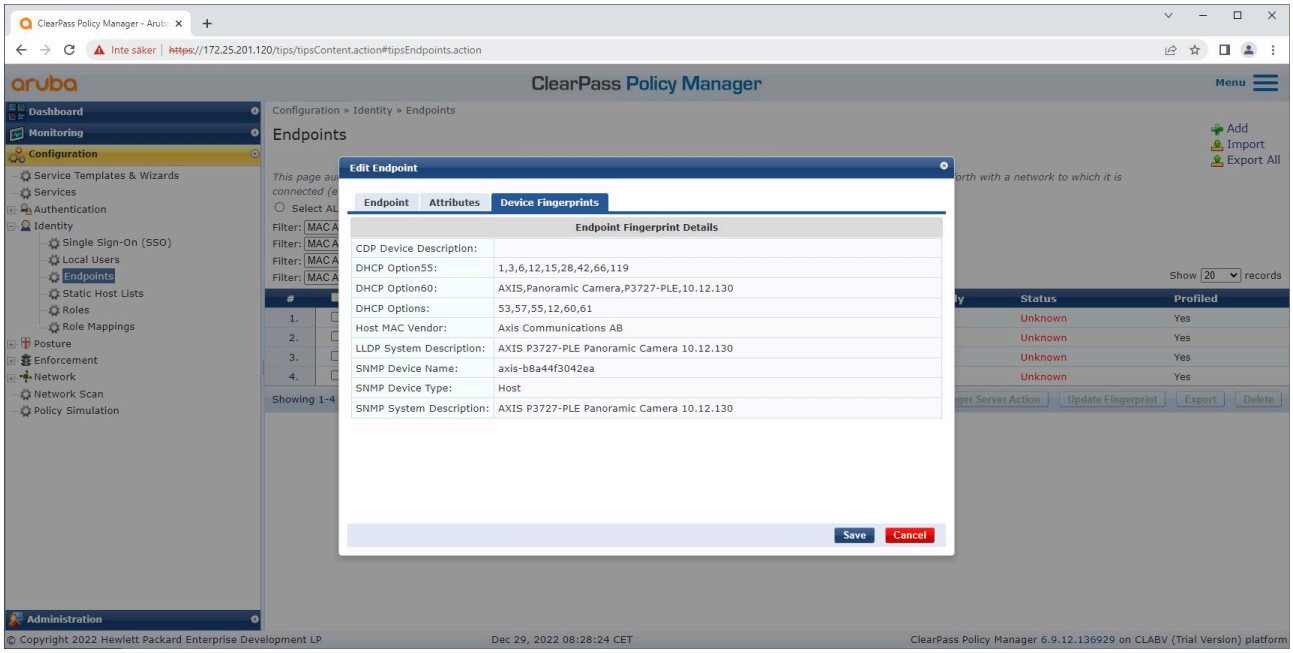
1. **[Configuration (設定)] > [Identity (ID)] > [Endpoints (エンドポイント)]** に移動します。
2. 表示する装置を選択します。
3. **[Device Fingerprints (装置のフィンガープリント)]** タブをクリックします。

注

SNMPは、Axis装置ではデフォルトで無効になっており、HPE Aruba Networkingのアクセススイッチから収集されます。



ClearPass Policy Managerによってプロファイルされたaxis装置。

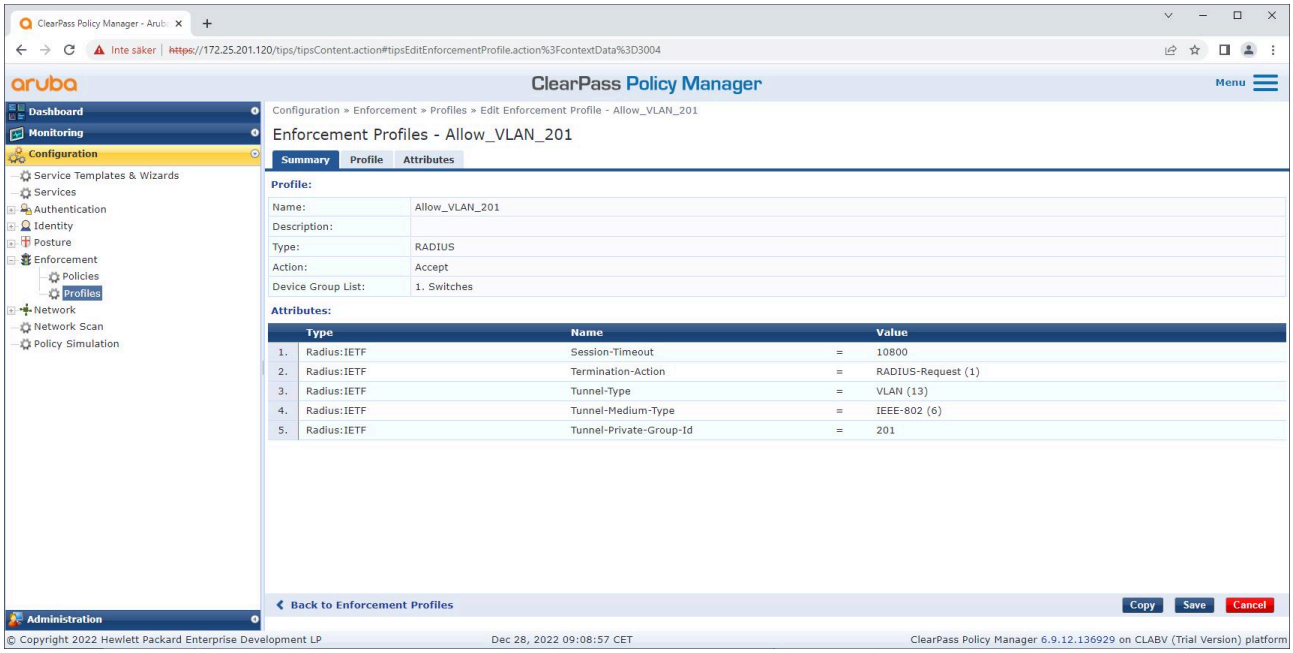


プロファイルされたAxis装置の詳細な装置フィンガープリント。Axisデバイスでは、SNMPがデフォルトで無効になっています。LLDP、CDP、DHCP固有の検出情報は、工場出荷時状態のAxisデバイスによって共有され、HPE Aruba Networkingアクセススイッチを経由してClearPass Policy Managerへ中継されます。

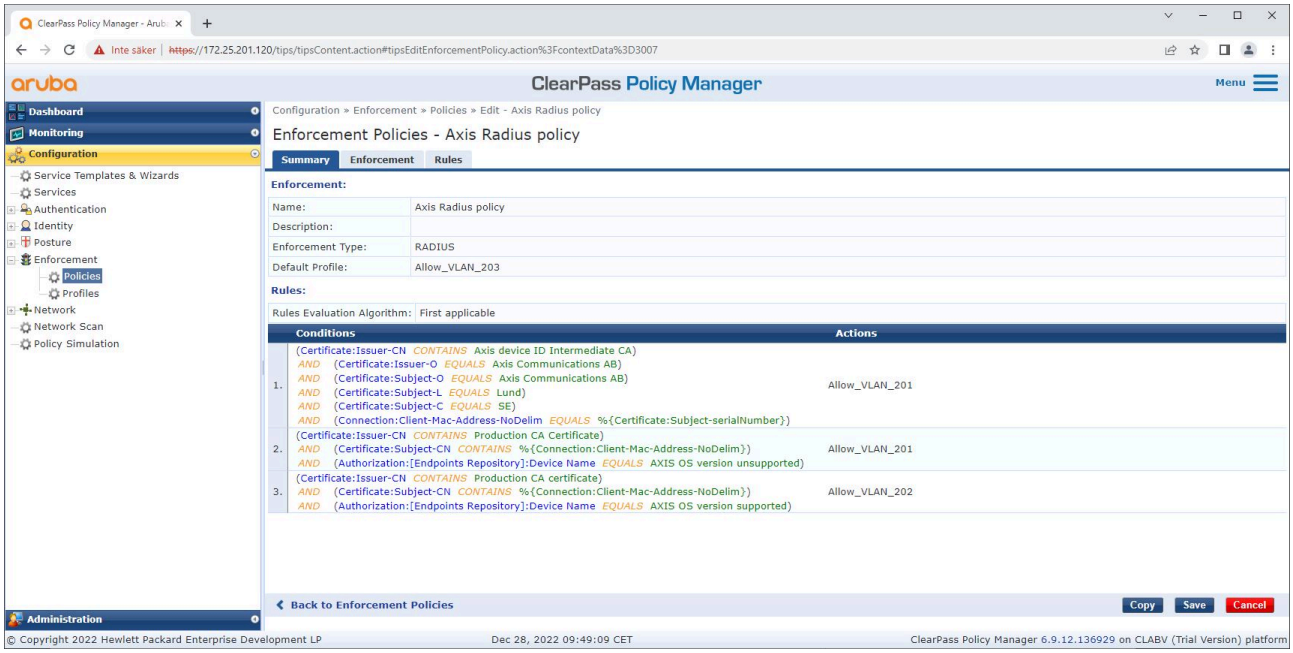
強制プロファイルの構成

強制プロファイルによって、ClearPass Policy Managerはスイッチ上のアクセスポートに特定のVLAN IDを割り当てることが可能になります。これはポリシーに基づく決定であり、デバイスグループ「スイッチ」内のネットワークデバイスに適用されます。必要な強制プロファイル数は、使用されているVLANの数によって異なります。設定には3つのVLAN (VLAN 201、202、203) があります。これらは3つの強制プロファイルに対応しています。

VLANの強制プロファイル設定を完了すると強制ポリシー自体を設定できます。ClearPass Policy Managerの強制ポリシー設定は、4つのサンプルポリシープロファイルに基づき、HPE Aruba Networkingネットワークへのアクセスを Axisデバイスに付与するかどうかを判断します。



VLAN 201へのアクセスを許可する強制プロファイルの例。



ClearPass Policy Managerrの強制ポリシー構成。

4つの強制ポリシーとそのアクションは以下の通りです。

ネットワークアクセスの拒否

IEEE 802.1Xネットワークアクセスコントロール認証が実行されない場合、ネットワークへのアクセスは拒否されます。

ゲストネットワーク (VLAN 203)

IEEE 802.1Xネットワークアクセスコントロール認証が失敗した場合、Axis装置には限定的な隔離ネットワークへのアクセスが付与されます。その後、適切なアクションを決定するために、デバイスの手動検査が必要になります。

プロビジョニングネットワーク (VLAN 201)

Axis装置に、プロビジョニングネットワークへのアクセスが付与されます。これにより、*AXIS Device Manager*と*AXIS Device Manager Extend*を通じてAxis装置の管理機能が提供されます。また、AXIS OSの更新、運用グレードの証明書、その他の設定を使用してAxis装置を設定することも可能になります。ClearPass Policy Managerは、以下の状態を検証します:

- デバイスのAXIS OSバージョン。
- デバイスのMACアドレスが、AxisデバイスID証明書のシリアル番号属性を持つベンダー固有のMACアドレススキームと一致すること。
- AxisデバイスID証明書が検証可能であり、発行者、組織、場所、国などのAxis固有の属性が一致すること。

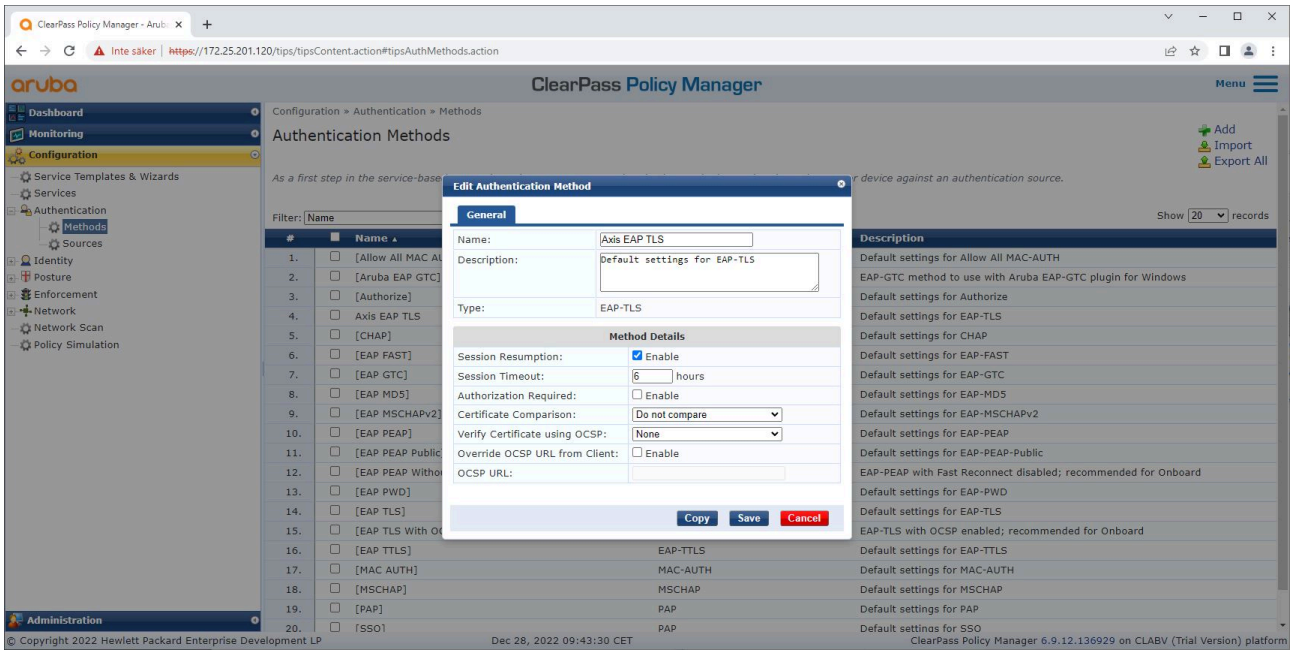
運用ネットワーク (VLAN 202)

Axisデバイスには、動作する運用ネットワークへのアクセスが付与されます。アクセスは、プロビジョニングネットワーク (VLAN 201) 内からデバイスのプロビジョニングが完了した後に許可されます。ClearPass Policy Managerは、以下の状態を検証します:

- デバイスのAXIS OSバージョン。
- デバイスのMACアドレスが、AxisデバイスID証明書のシリアル番号属性を持つベンダー固有のMACアドレススキームと一致すること。
- 運用グレードの証明書が、信頼できる証明書ストアによって検証できること。

認証方式の構成

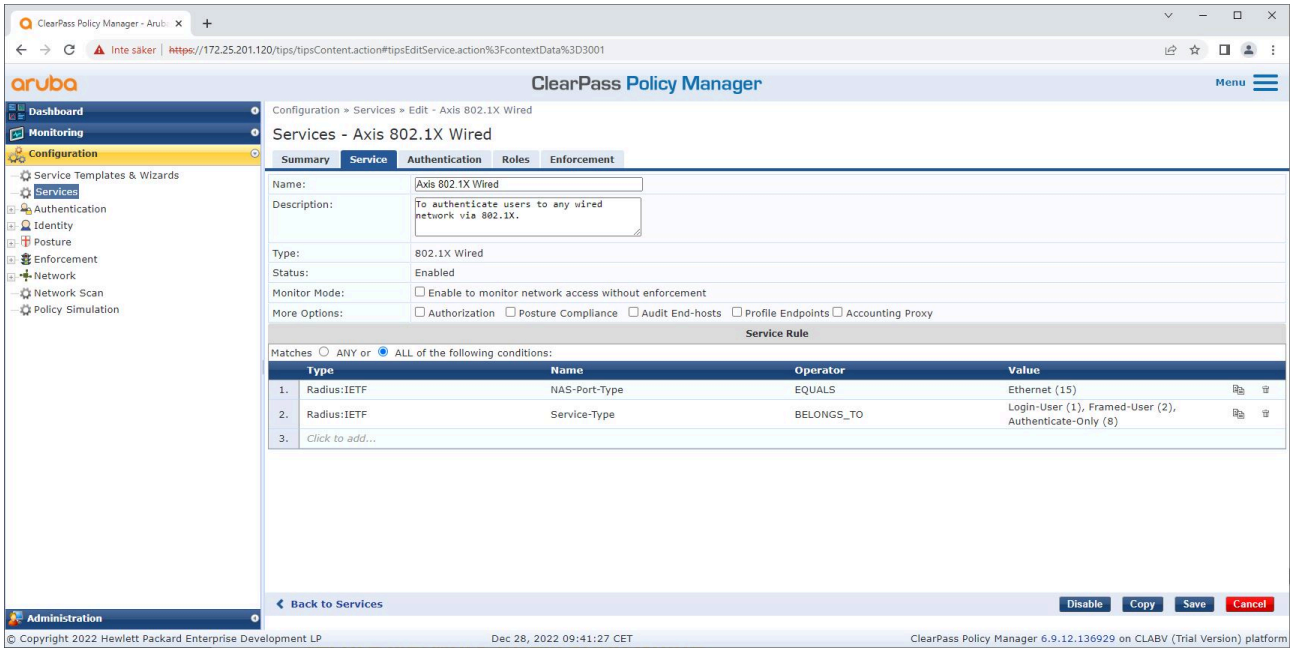
認証方式は、Axisデバイスがネットワーク上で自己認証を試みる方法を定義します。Axis Edge Vaultを搭載するAxisデバイスは、デフォルトでIEEE 802.1X EAP-TLSが有効になっているため、望ましい方式はIEEE 802.1X EAP-TLSです。



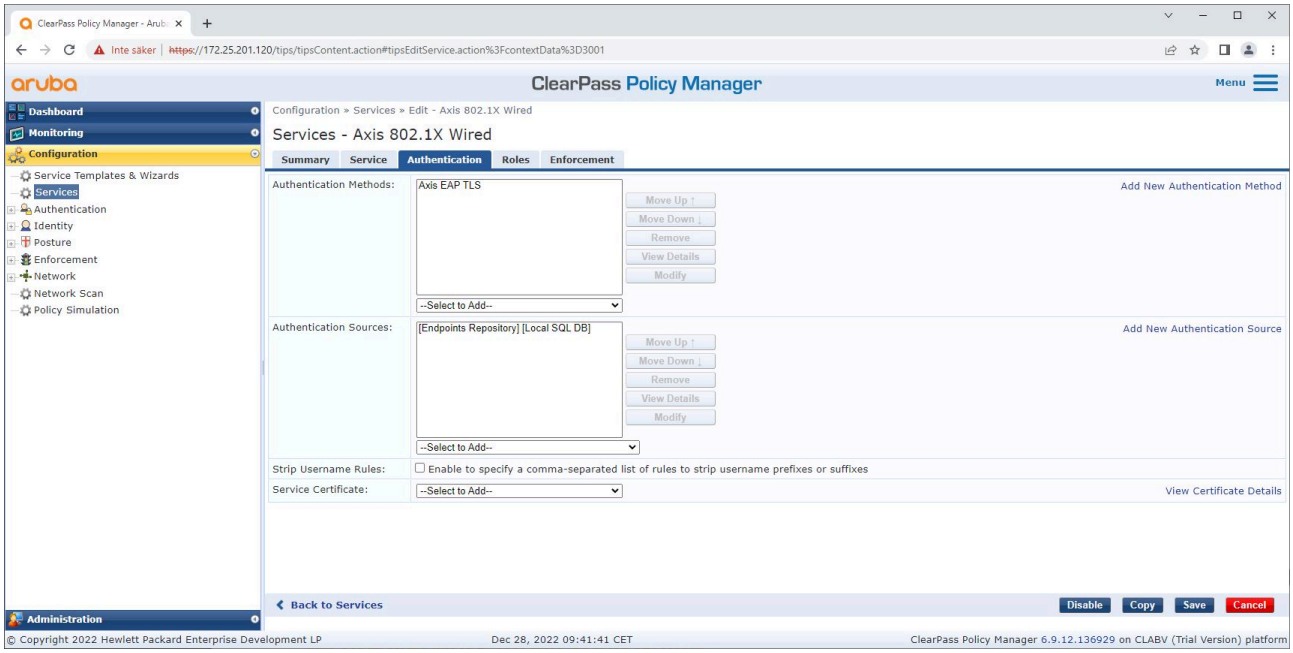
AxisデバイスのEAP-TLS認証方式が定義されているClearPass Policy Managerの認証方式インターフェース。

サービスの設定

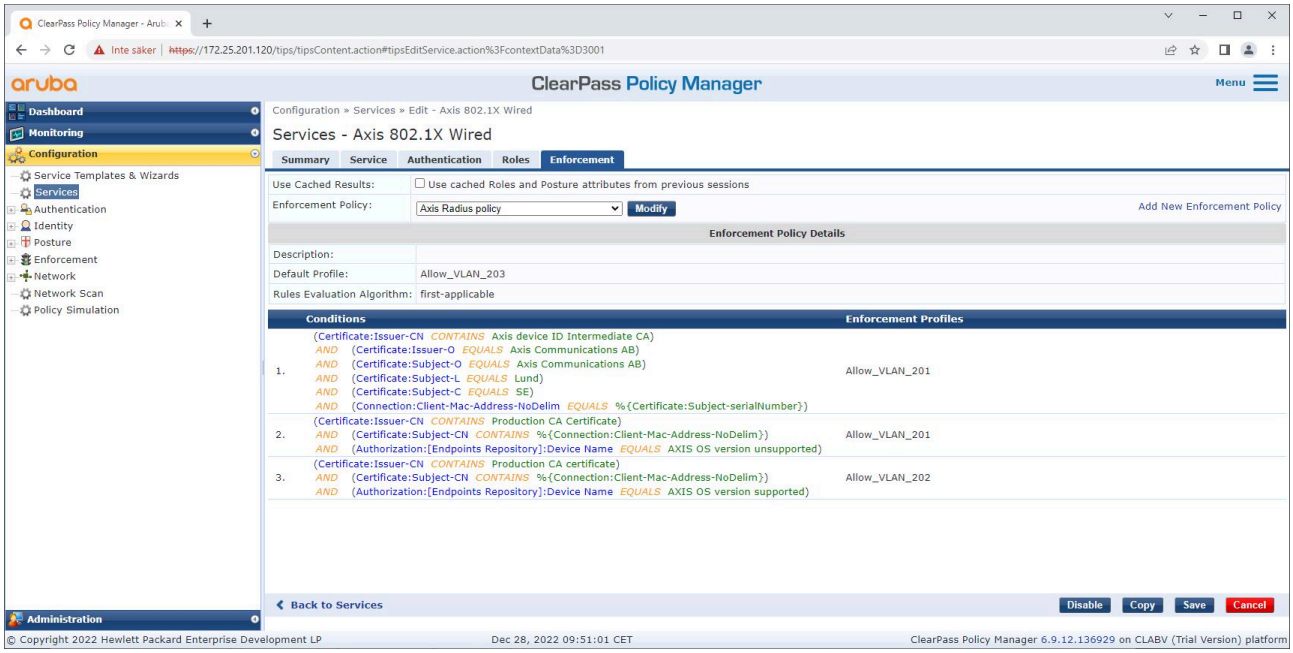
[Services (サービス)] ページでは、設定手順がHPE Aruba Networkingネットワーク内のAxisデバイスの認証と承認を処理する1つのサービスに統合されています。



専用Axisサービスが作成され、接続方式としてIEEE 802.1Xが採用されます。



先に作成したEAP-TLS認証方式が、サービスに設定されます。



先に作成した強制ポリシーが、サービスに設定されます。

HPE Aruba Networkingアクセススイッチ

Axisデバイスは、PoE対応のアクセススイッチに直接接続することも、互換性のあるAxis PoEミッドスパンを経由して接続することもできます。HPE Aruba Networkingネットワークに Axisデバイスを安全にオンボードするには、アクセススイッチをIEEE 802.1X通信用に設定する必要があります。AxisデバイスはIEEE 802.1x EAP-TLS通信をClearPass Policy Managerに中継します。ClearPass Policy Managerは、RADIUSサーバーとして動作します。

注

ポートアクセス全体のセキュリティを強化する目的で、300秒の周期的なAxisデバイスの再認証も設定されます。

この例は、HPE Aruba Networkingアクセススイッチのグローバル設定およびポート設定を示しています。

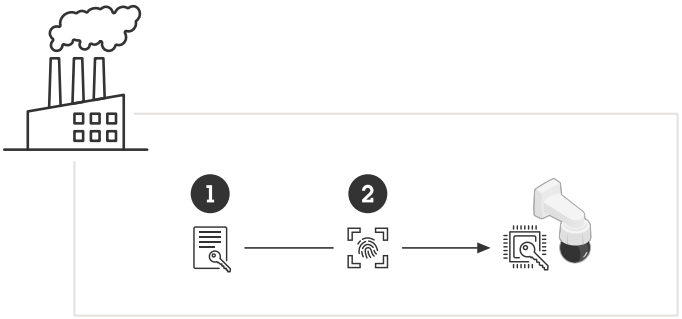
```
radius-server host MyRADIUSIPAddress key "MyRADIUSKey"
```

```
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
```

Axisの設定

Axisネットワーク装置

*Axis Edge Vault*に対応するAxisデバイスは、製造時にAxisデバイスIDと呼ばれる安全なデバイス識別子が付与されます。AxisデバイスIDは、IEEE 802.1Xによる自動化された安全なデバイス識別およびネットワークオンボーディングの方法を定義する国際規格IEEE 802.1ARに基づいています。



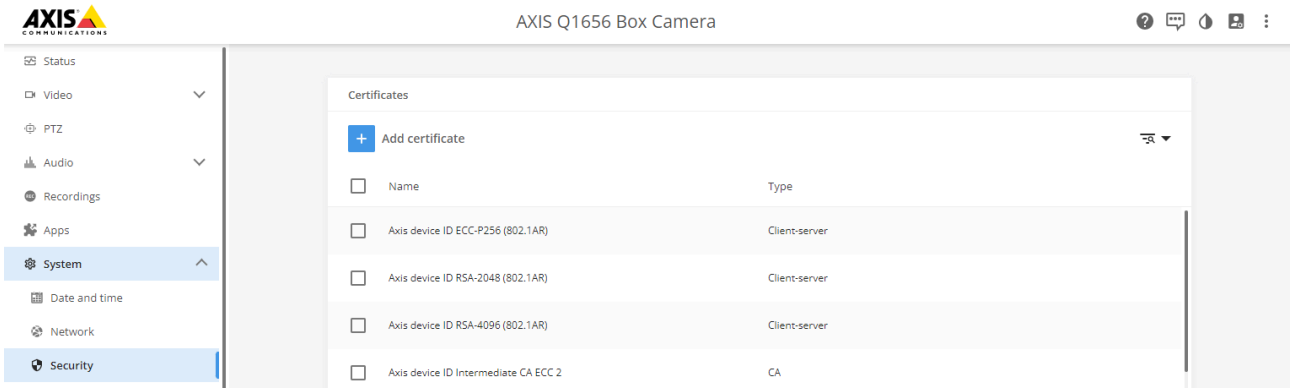
信頼できるデバイスIDサービス提供のため、Axis装置はIEEE 802.1AR準拠のAxisデバイスID証明書を製造時に付与されている

1 *AxisデバイスIDキーインフラストラクチャー（PKI）*
2 *AxisデバイスID*

Axisデバイスのセキュアエレメントにより提供されるハードウェア保護型の安全なキーストアは、工場でプロビジョニングされています。さらに、Axisデバイスの信頼性をグローバルに証明するデバイス固有の証明書と対応キー (AxisデバイスID) が付属します。Axis Edge VaultとAxisデバイスIDに対応するAxisデバイスは、*Axis Product Selector*を使用して確認できます。

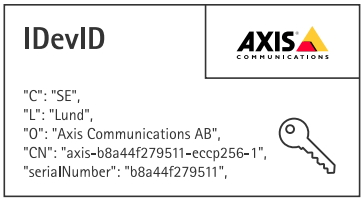
注

Axis装置のシリアル番号は、装置のMACアドレスです。



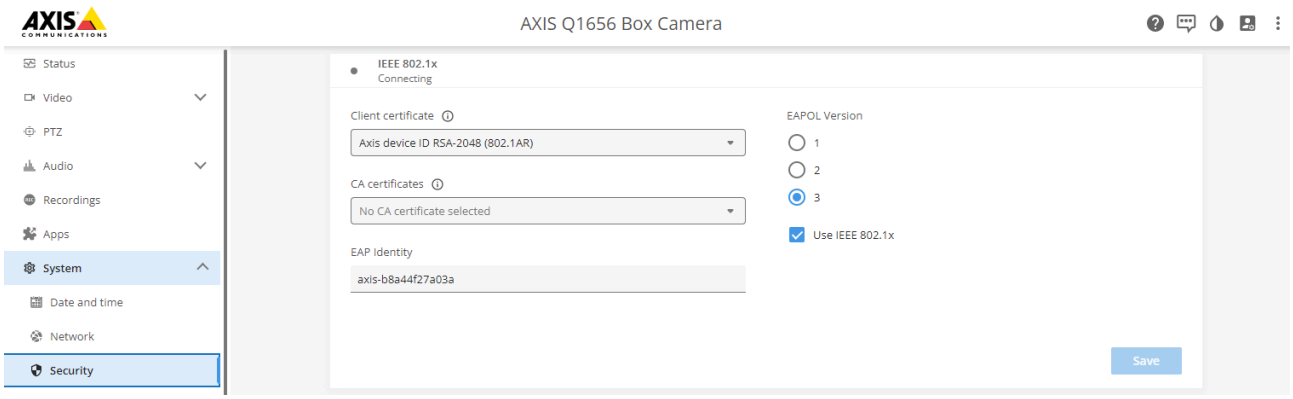
工場出荷時設定のAxisデバイスに搭載された証明書ストアとAxisデバイスID。

IEEE 802.1AR準拠のAxisデバイスID証明書には、シリアル番号に関する情報および、ベンダー固有のその他の情報が含まれています。ClearPass Policy Managerは、ネットワークへのアクセスを付与する際の分析と判断にこの情報を使用します。以下の情報は、AxisデバイスのID証明書から取得できます。



国名	SE
場所	ルンド
Issuer Organization (発行者組織)	アクシスコミュニケーションズ AB
Issuer Common Name (発行者の通称)	Axis device ID intermediate
組織	アクシスコミュニケーションズ AB
Common Name (通称)	axis-b8a44f279511-eccp256-1
シリアル番号	b8a44f279511

一般名称は、Axis社名とデバイスのシリアル番号を組み合わせ、そのシリアル番号の後に暗号アルゴリズム (ECC P256、RSA 2048、RSA 4096) を付加して構成されています。AXIS OS 10.1 (2020-09) 以降、IEEE 802.1Xは事前設定されたAxisデバイスIDでデフォルトで有効になっています。これにより、デバイスはIEEE 802.1X対応ネットワーク上で自己認証を行うことができます。



Axisデバイスは工場出荷時のデフォルト設定でIEEE 802.1Xが有効化されており、AxisデバイスID証明書が事前選択されています。

AXIS Device Manager

*AXIS Device Manager*と*AXIS Device Manager Extend*をネットワーク上で使用し、複数のAxisデバイスをコスト効率の良い方法で設定、管理することができます。AXIS Device Managerは、Microsoft Windows® ベースのアプリケーションでネットワーク内のマシンにローカルにインストールされます。AXIS Device Manager Extendはクラウドインフラストラクチャーに依存し、複数サイトのデバイス管理を実行します。いずれも手軽に管理、設定でき、以下などが可能です。

- AXIS OS更新のインストール。
- HTTPSやIEEE 802.1X証明書などのサイバーセキュリティ設定の適用。
- 画像の設定など、デバイス固有の設定の実行。

安全なネットワーク運用 - IEEE 802.1AE MACsec

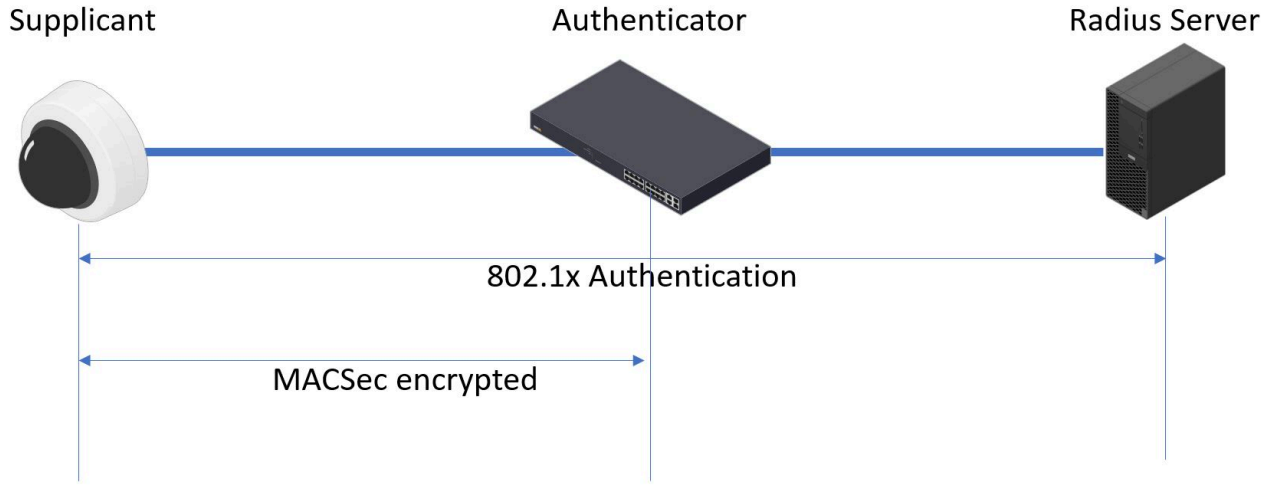
このビデオを見るには、このドキュメントのWebバージョンにアクセスしてください。

IEEE 802.1AE MACsec Layer-2 Securityによるゼロトラストネットワーク暗号化

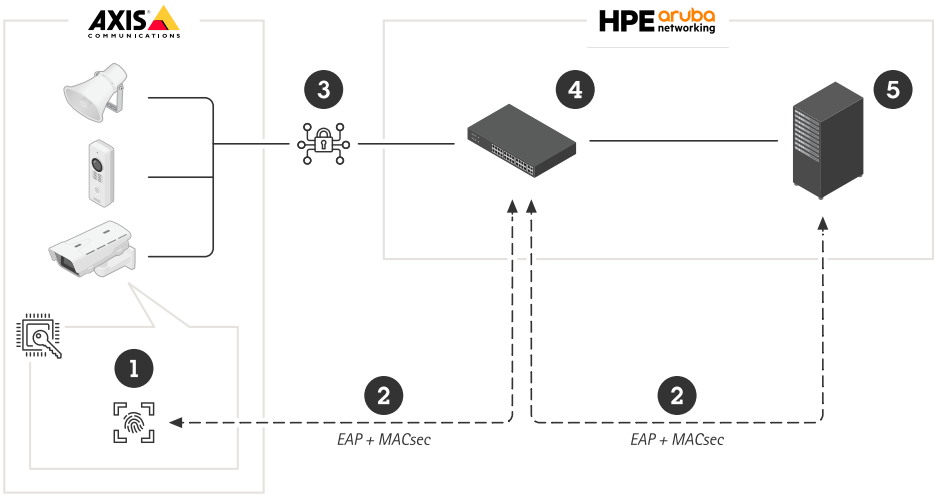
IEEE 802.1AE MACsec (Media Access Control Security) は明確に定義されたネットワークプロトコルであり、ネットワークレイヤー2にあるポイントツーポイントイーサネットリンクを暗号的に保護します。これにより、2つのホスト間のデータ送信の機密性と完全性が保証されます。

IEEE 802.1AE MACsec規格は、次の2つの運用モードを提供します。

- 手動で構成可能なPre-Shared Key/Static CAKモード
- IEEE 802.1X EAP-TLSを使用するAutomatic Master Session/Dynamic CAKモード



AXIS OS 10.1 (2020-09) 以降では、Axis device IDに対応するデバイスにおいてIEEE 802.1Xがデフォルトで有効になっています。AXIS OS 11.8以降では、デフォルトで有効になっているIEEE 802.1Xを使用する自動動的モードによってMACsecに対応しています。工場出荷時の設定値でAxisデバイスを接続すると、IEEE 802.1Xネットワーク認証が実行され、成功するとMACsec Dynamic CAKモードも試行されます。



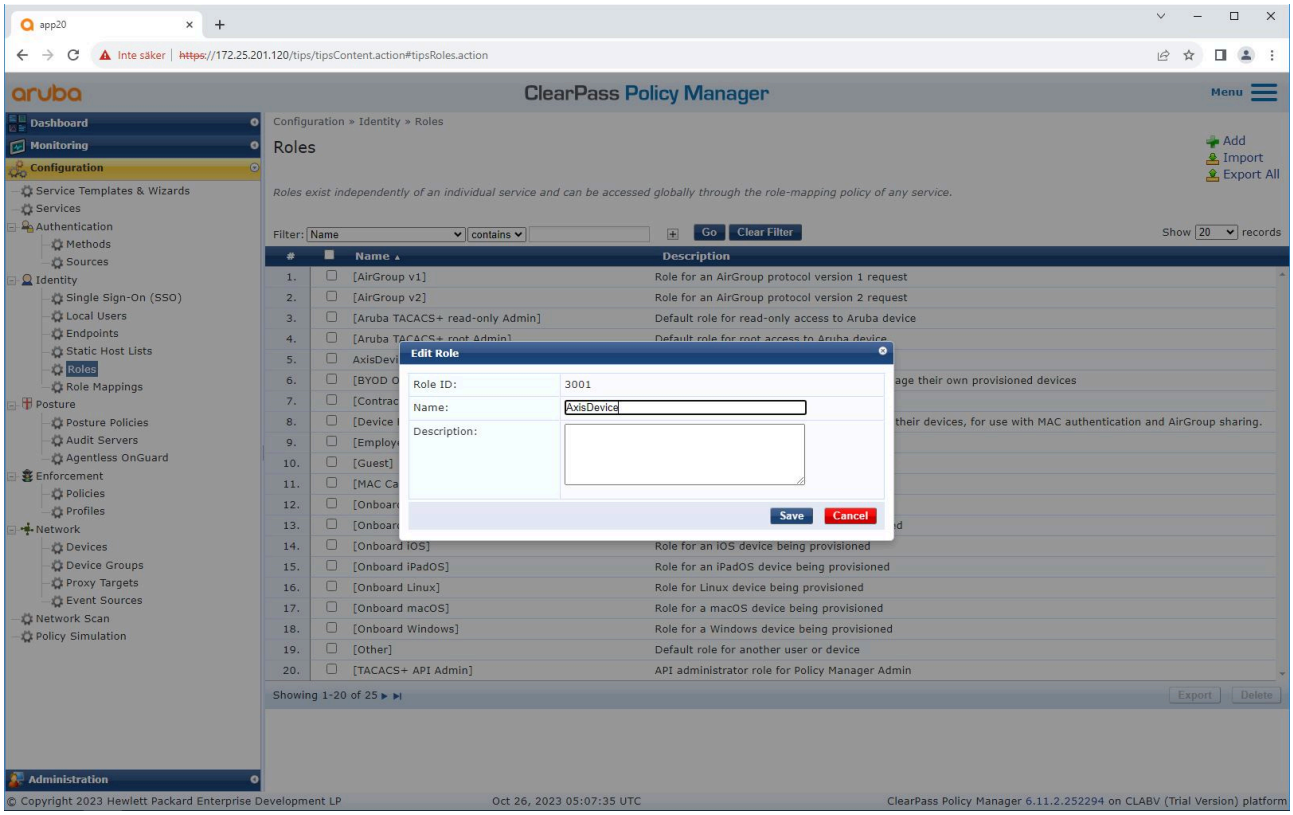
安全に保存されたAxisデバイスID (1) (IEEE 802.1AR準拠の安全なデバイスID) は、IEEE 802.1X EAP-TLSポートベースのネットワークアクセスコントロール (2) を経由して、ネットワーク (4、5) への認証に使用されます。このEAP-TLSセッションを通じてMACsecキーが自動的に交換され、安全なリンク (3) が設定されるほか、Axis装置からHPE Aruba Networkingアクセススイッチまでのすべてのネットワークトラフィックが保護されます。

IEEE 802.1AE MACsecには、HPE Aruba Networkingアクセススイッチと ClearPass Policy Manager構成の両方の準備が必要です。EAP-TLS経由のIEEE 802.1AE MACsec暗号化通信を許可する上で、Axis装置で必要な構成はありません。

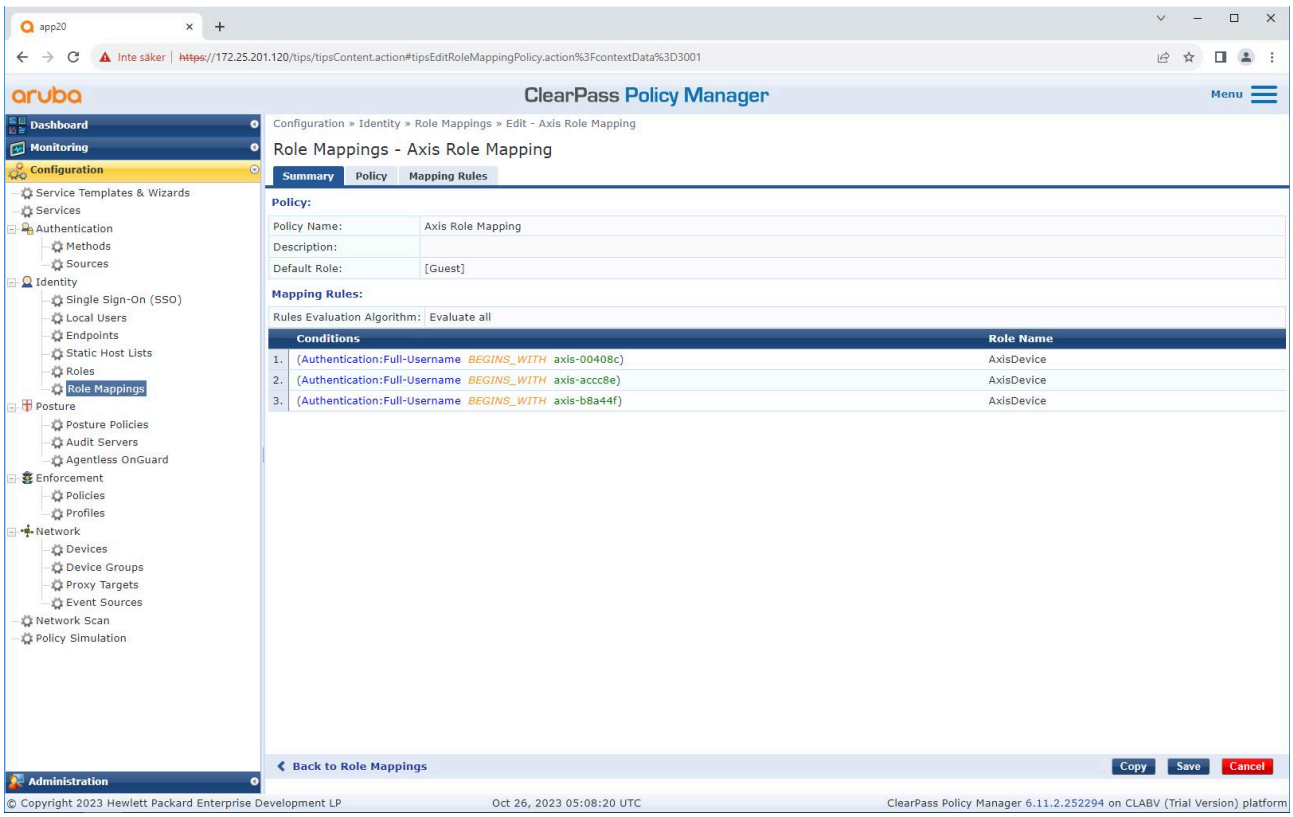
HPE Aruba NetworkingアクセススイッチがMACsecによるEAP-TLSの使用をサポートしていない場合は、Pre-Shared Keyモードを使用して手動で構成できます。

HPE Aruba Networking ClearPass Policy Manager

ロールとロールマッピングポリシー



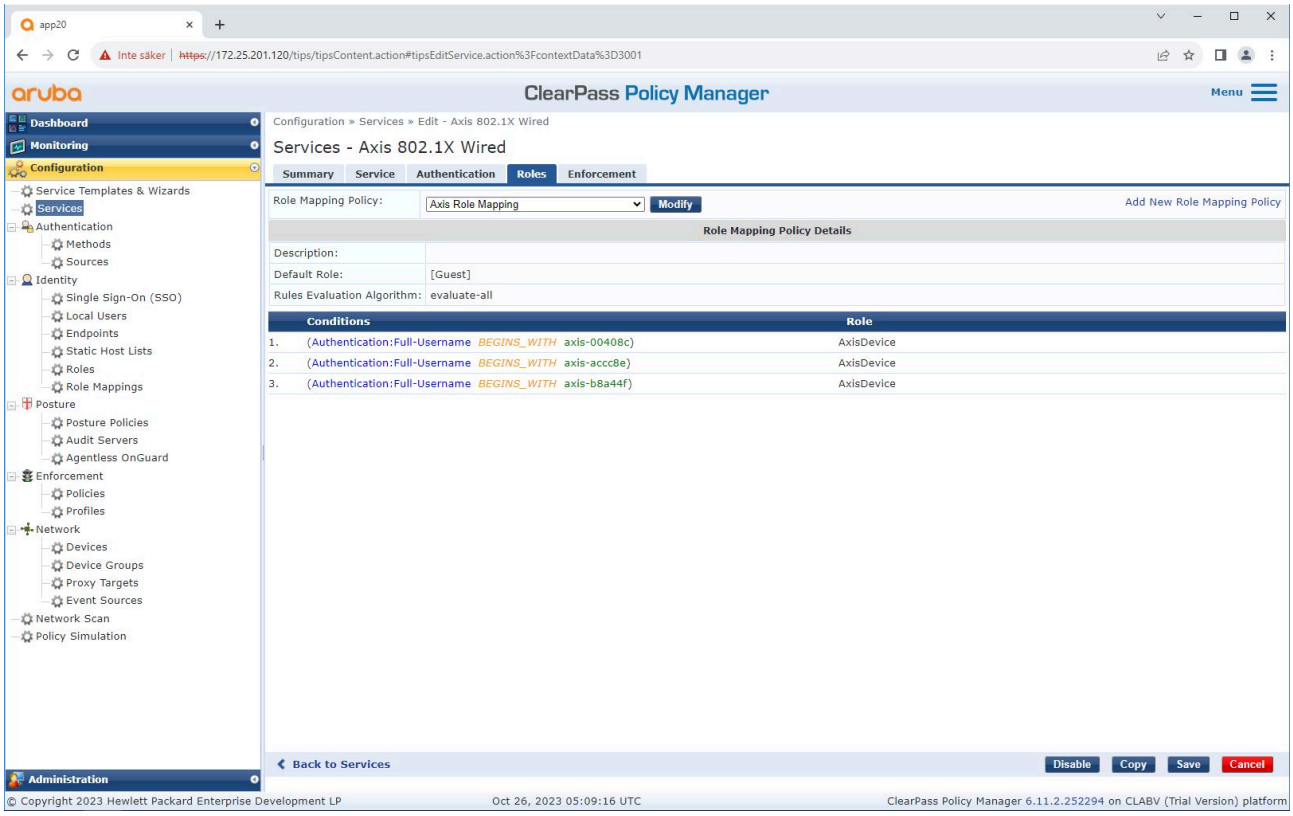
Axis装置の役割名を追加します。この名前は、アクセススイッチ構成のポートアクセス役割名です。



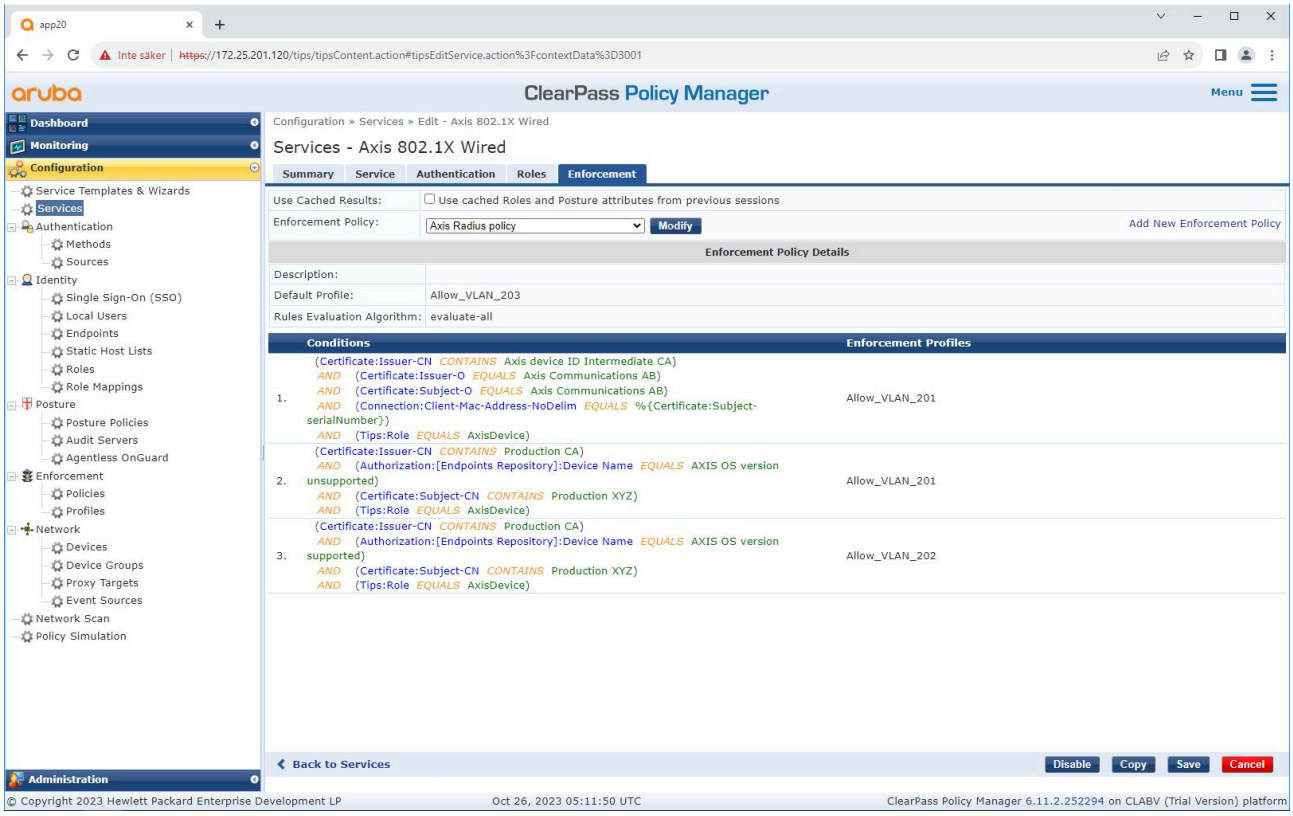
先に作成したAxisデバイスロールに対して、Axisロールマッピングポリシーを追加します。この条件定義は、装置をAxis装置ロールにマッピングするために必要です。条件が満たされない場合、デバイスは [Guest (ゲスト)] ロールの一部になります。

デフォルトでは、AxisデバイスはEAP識別子形式"axis-serialnumber"を使用します。Axisデバイスのシリアル番号はデバイスのMACアドレスです。たとえば、「axis-b8a44f45b4e6」のようになります。

サービスの設定

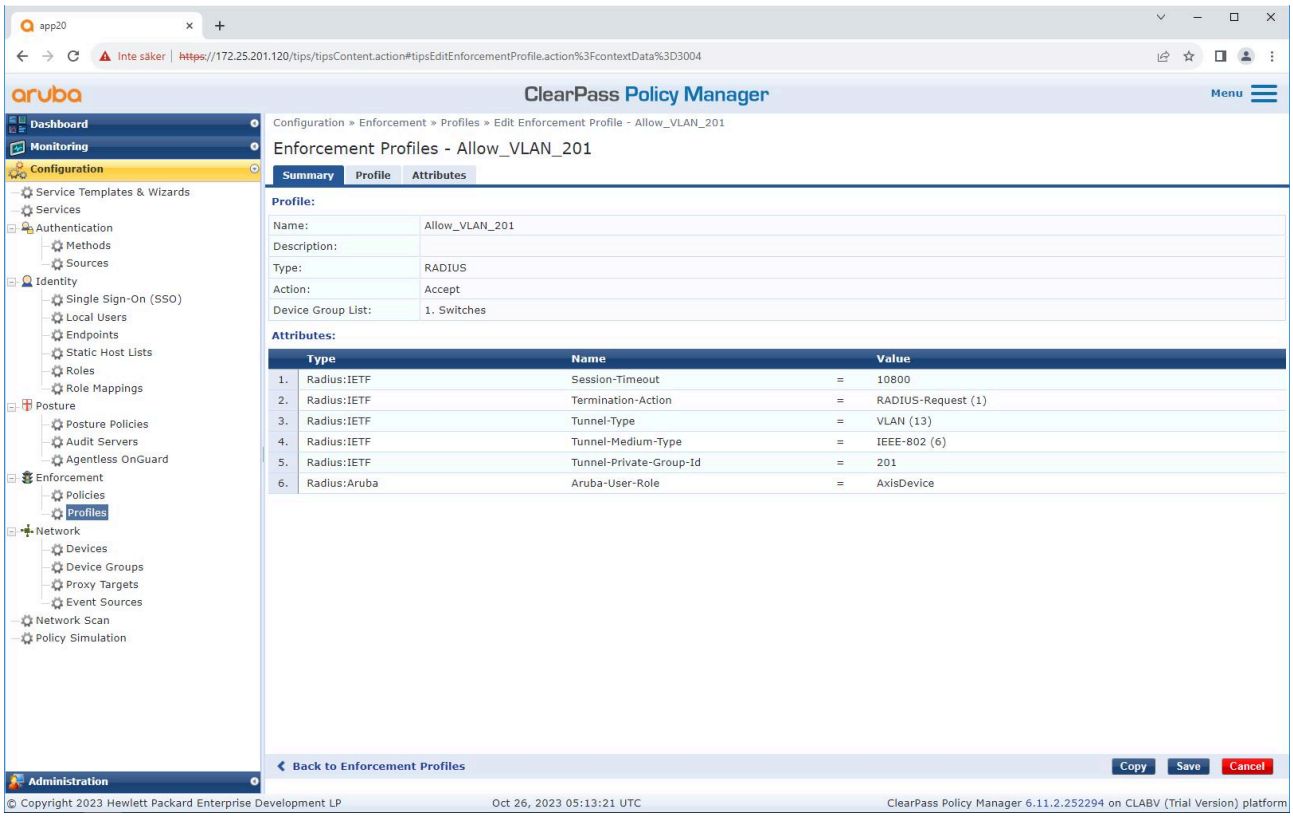


Axisデバイスのオンボーディングの接続方式としてIEEE 802.1Xを定義するサービスに、先の手順で作成したAxisロールマッピングポリシーを追加します。



既存のポリシー定義に、Axis役割名を条件として追加します。

強制プロファイル



IEEE 802.1Xオンボーディングサービスで割り当てられる強制プロファイルに、Axisロール名を属性として追加します。

HPE Aruba Networkingアクセススイッチ

*HPE Aruba Networkingアクセススイッチ, on page 15*に記載された安全なオンボーディング設定に加えて、以下の HPE Aruba Networkingアクセススイッチのポート設定例を参照してIEEE 802.1AE MACsecを設定します。

```
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
```

証明書の管理 – セキュアトランスポート経由の登録 (EST)

デジタル証明書は、デバイスやネットワークのセキュリティ確保に不可欠ですが、その管理は複雑で時間がかかる場合があります。証明書には有効期限があり、定期的に更新する必要があります。自動化されていない場合、このプロセスは手動で反復する必要があります。特に大規模な導入や、複数のデバイスタイプが混在する環境では、その傾向が強まります。

AXIS OS 12.9は、デバイスへの証明書を安全にプロビジョニングするためのプロトコルである Enrollment over Secure Transport (EST) に対応しています。RFC 7030で定義されているESTは、標準規格ベースのソリューションであり、以下の内容を含む証明書のライフサイクル全体を簡素化および自動化することを目的として設計されています。

- 登録 – デバイスへの新規証明書を安全に発行する
- 更新 – 期限切れになる証明書を自動的に置き換える
- 再登録 – ITポリシーに基づいて証明書を更新する

ESTは、有効期間、鍵のタイプ (RSA/ECC) や鍵サイズなどの証明書属性に関するITポリシーをサポートし、HTTPSのみを使用します。

ESTの主な利点

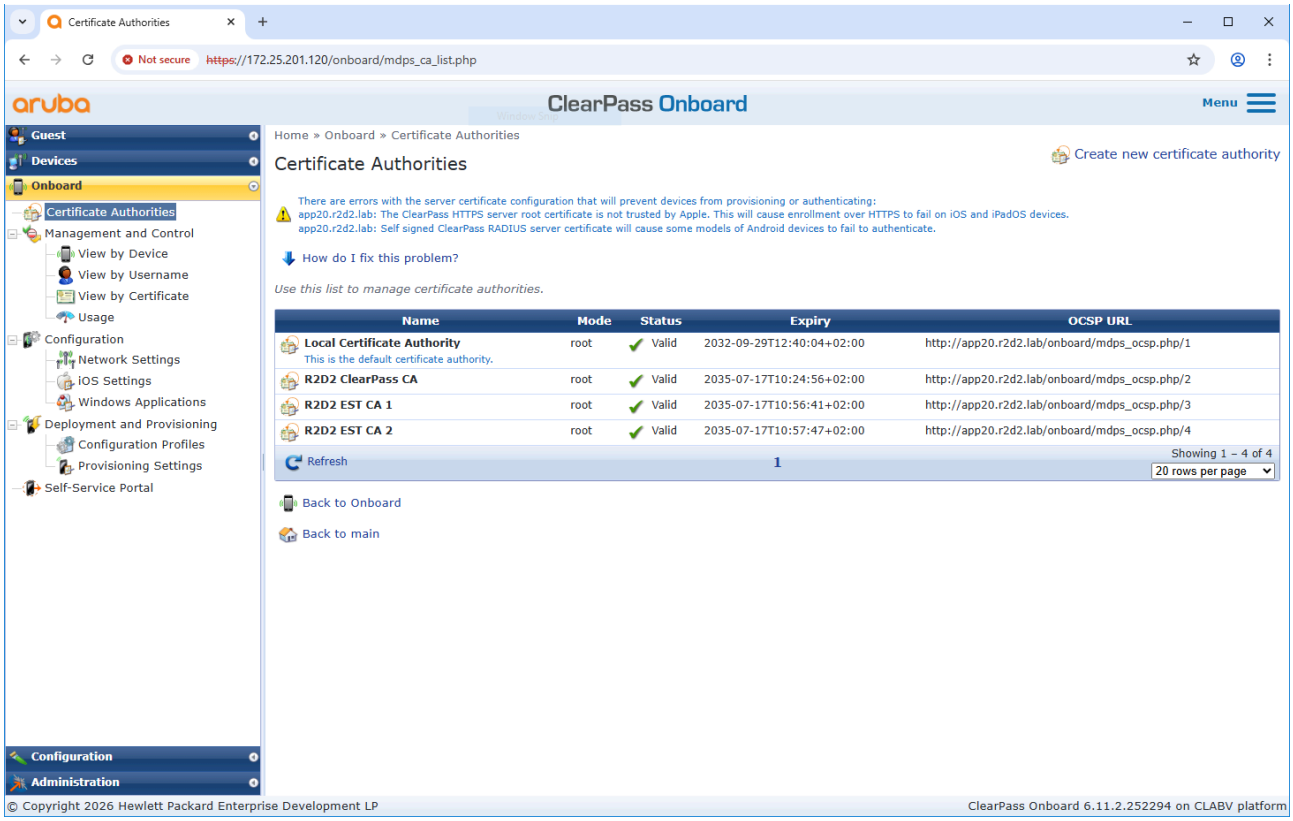
- 証明書の登録、更新、再登録がITポリシーに基づいて自動的に行われるため、時間のかかる手動での設定作業を完全になくすことができます。
- HTTPS限定のTLS 1.2/1.3を介して、最新の安全な通信が実現します。
- ITチームのための集中管理型可視化・監視ソリューションが得られます。
  標準規格ベース (RFC 7030) であるため、ITインフラストラクチャーと統合することができます。
- IoT、企業ネットワーク、デバイス管理に対応する拡張可能なソリューションが得られます。

ESTに関する一般的なドキュメントについては、当社の*AXIS OSナレッジベース*を参照してください。

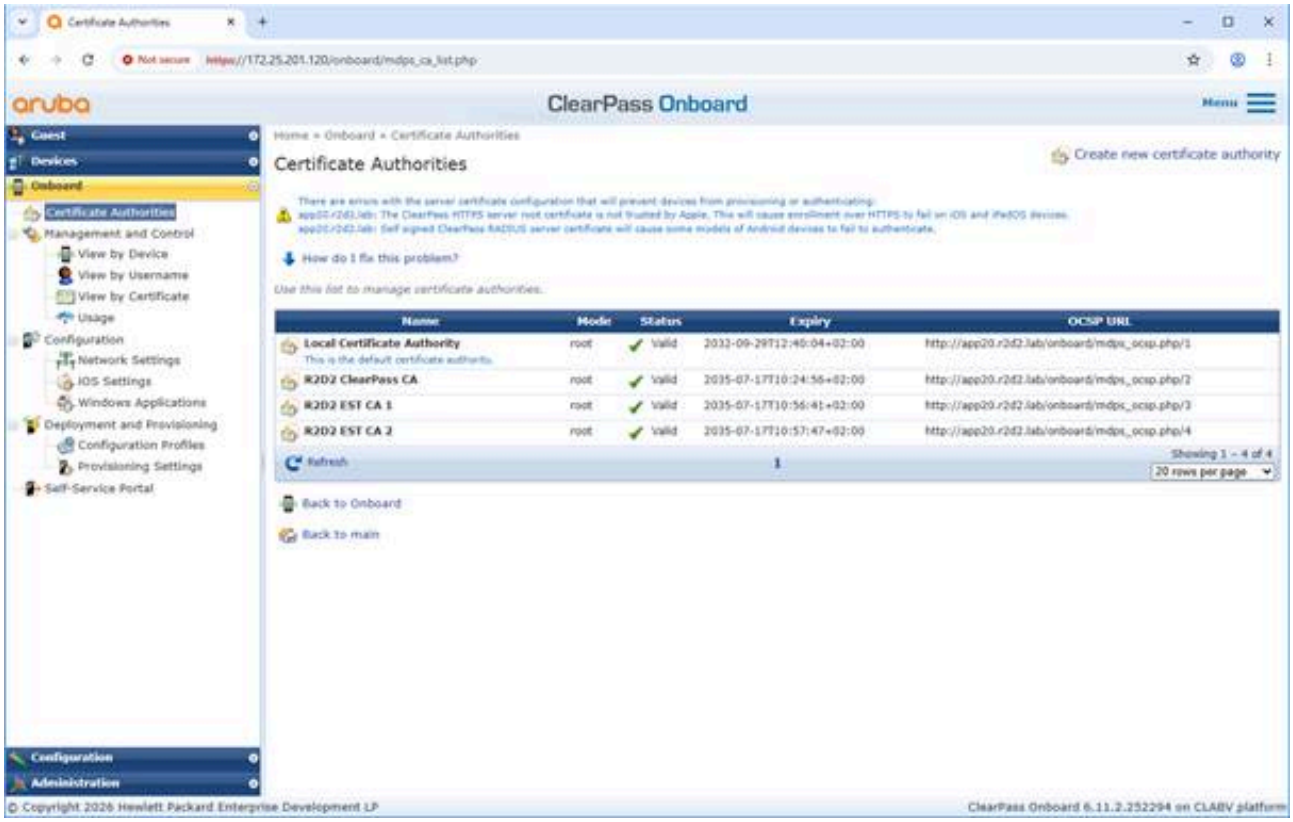
HPE Aruba ClearPass のオンボード設定

Aruba ClearPass Onboardは、ESTと連携し、ネットワークアクセス用のデバイス証明書を安全に配布・管理します。エンドポイントはESTを使用してClearPassに対する認証を行い、安全なTLSチャンネルを介して一意の証明書を取得します。この証明書は、802.1X証明書ベースの認証やその他のサービスに使用されます。これにより、デバイス識別情報に基づく安全なアクセスポリシーを適用するための、標準規格ベースの自動化されたパスワード不要の手法が提供されます。

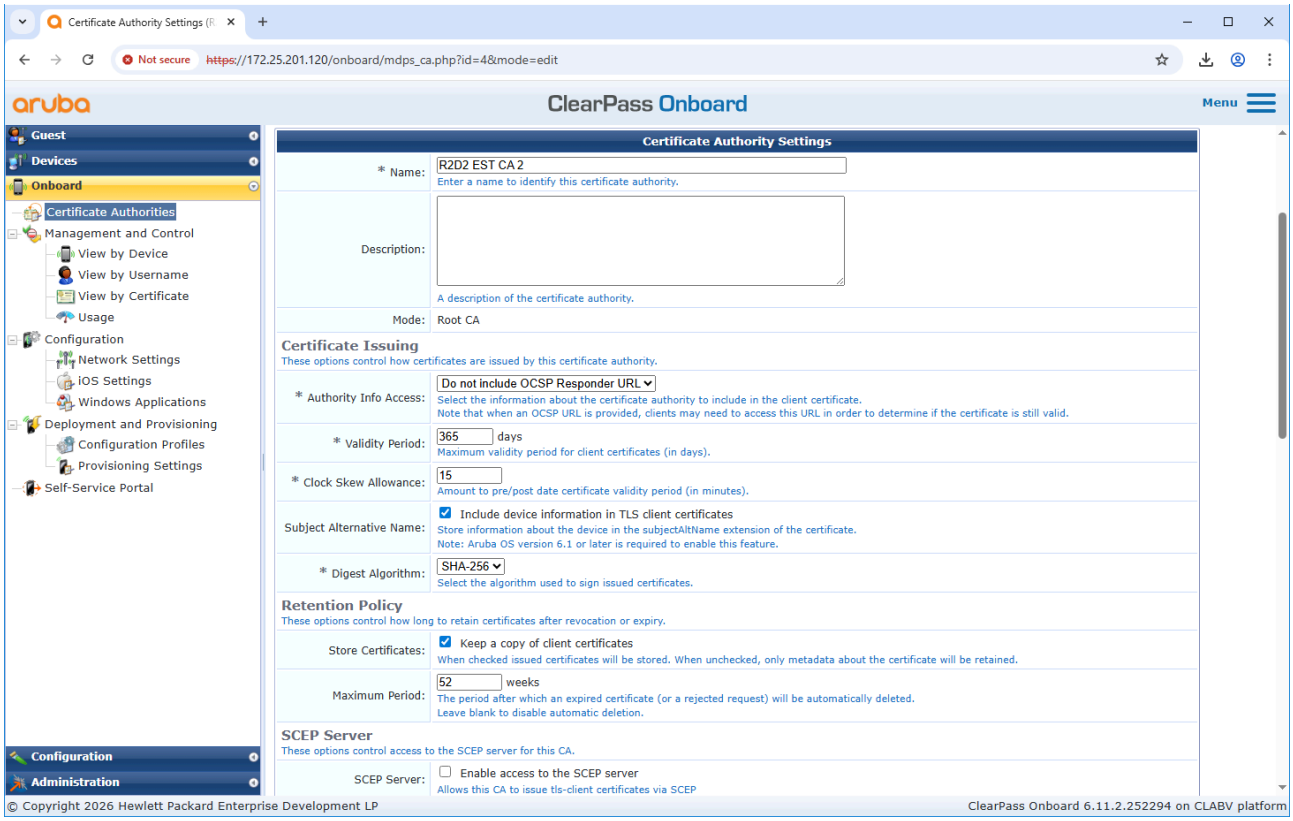
認証局の設定



ClearPass Onboard内に新規の認証局を作成します。



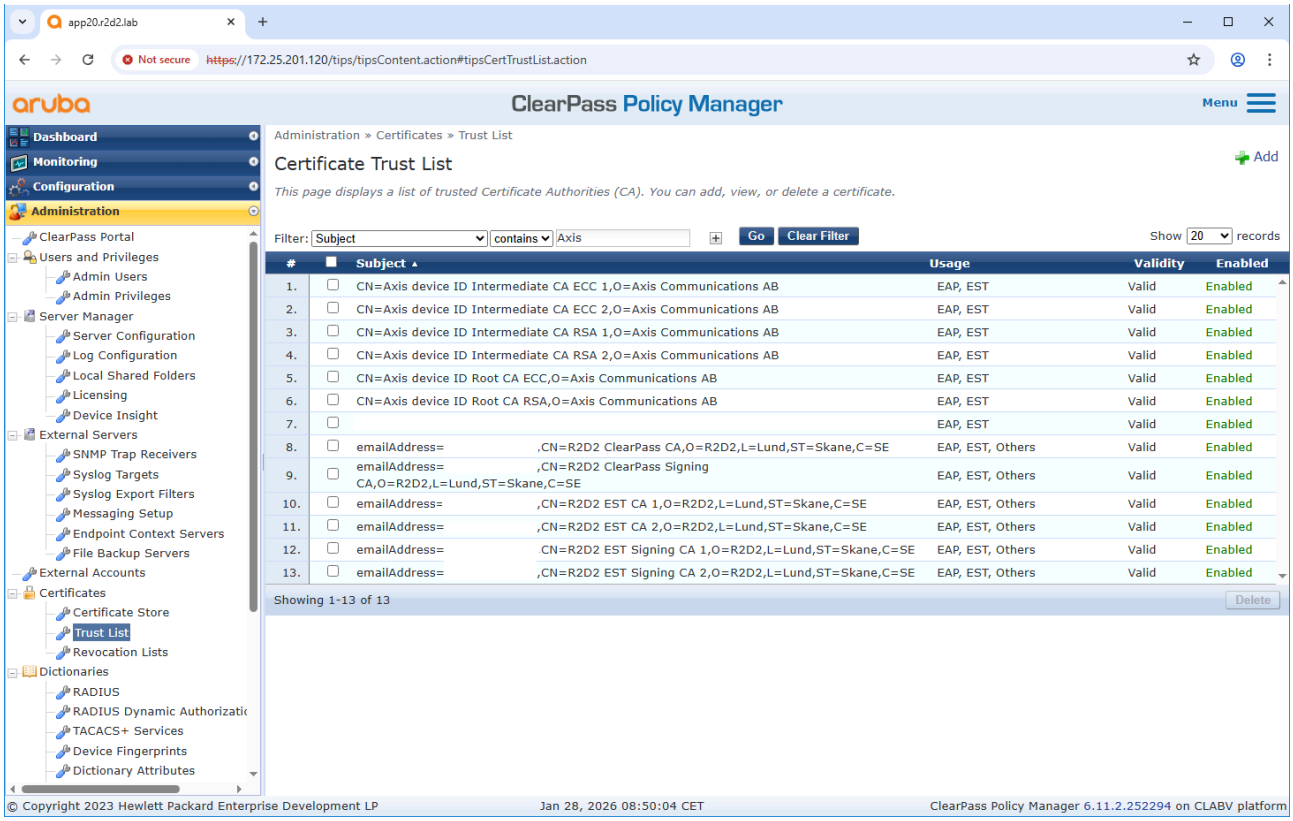
作成した認証局内では、鍵のタイプ、鍵サイズ、有効期間などが定義されます。



作成した認証局に対して、ESTサーバー機能を有効にします。クライアント証明書を使用するようにEST認証方法を設定します。

HPE Aruba ClearPass Policy Managerの設定

信頼できる証明書ストアの構成

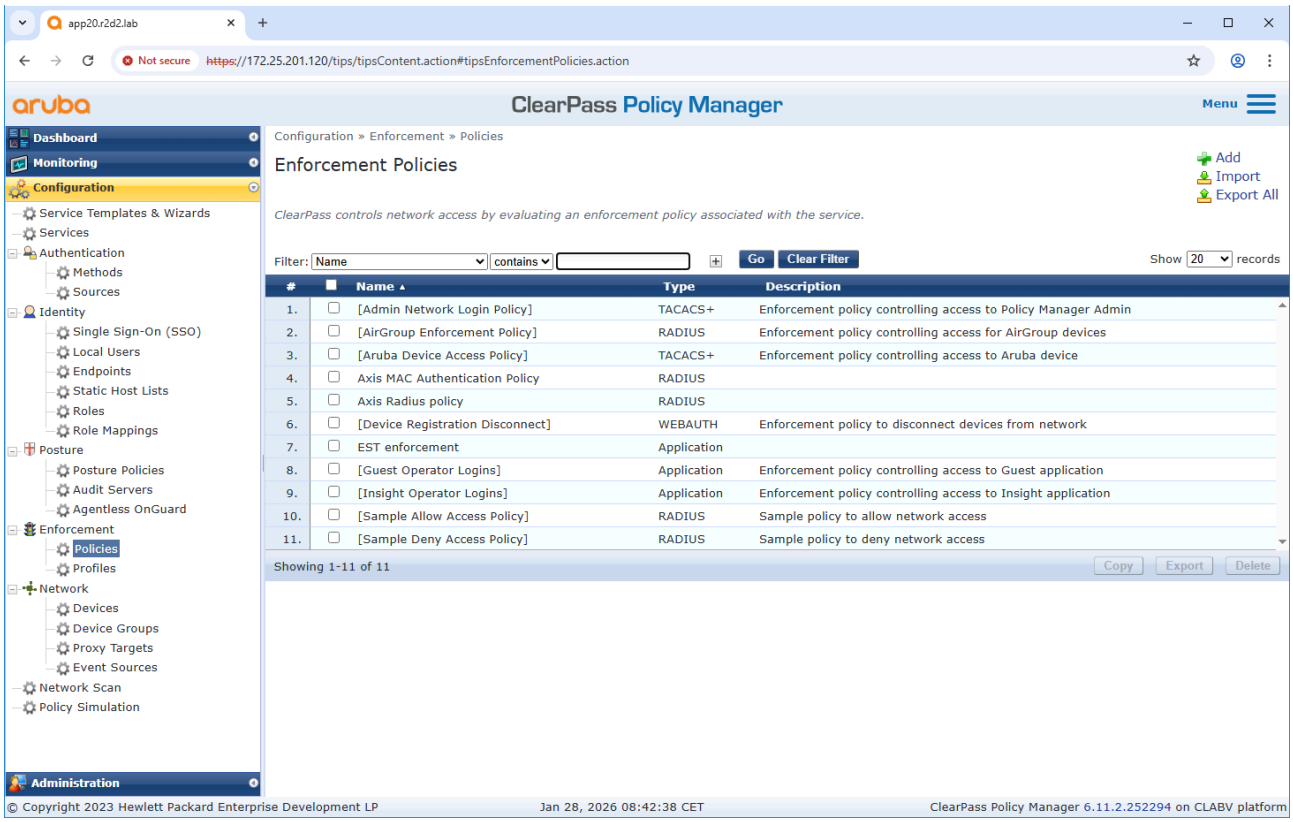


*Axis固有のIEEE 802.1AR証明書*を、Aruba ClearPass Policy Managerの信頼できる証明書ストアにアップロードします (まだアップロードしていない場合)。ESTの使用が追加されていることを確認

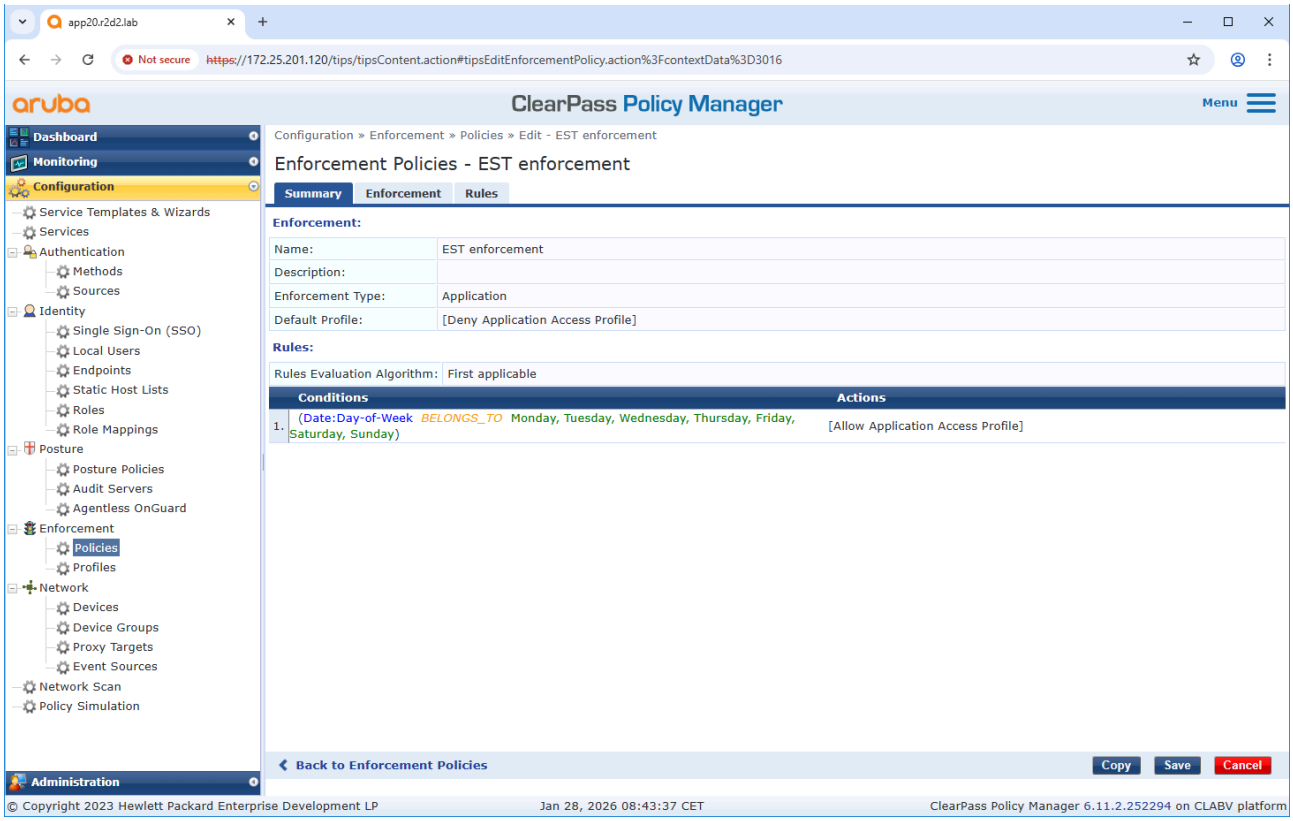
してください。ClearPass Onboardで事前に作成した認証局についても、同様に確認してください。

強制ポリシーの設定

強制プロファイルにより、ClearPass Policy ManagerはESTアプリケーションに対して特定の強制事項を割り当てることが可能となります。例えば、新規の証明書は特定のエンドポイントからのみ登録可能、または特定の曜日のみ登録可能といった事項です。

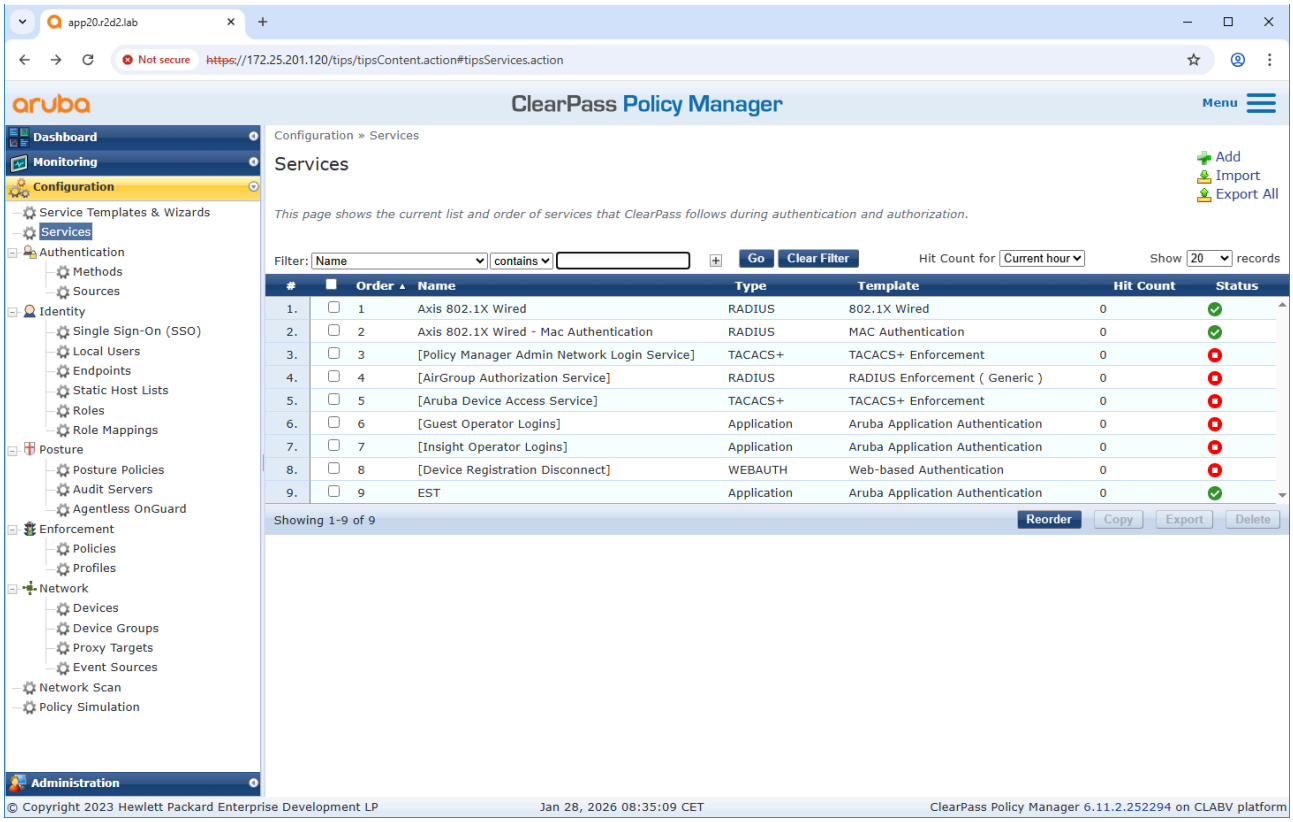


ClearPass Policy Managerの強制ポリシーの概要。

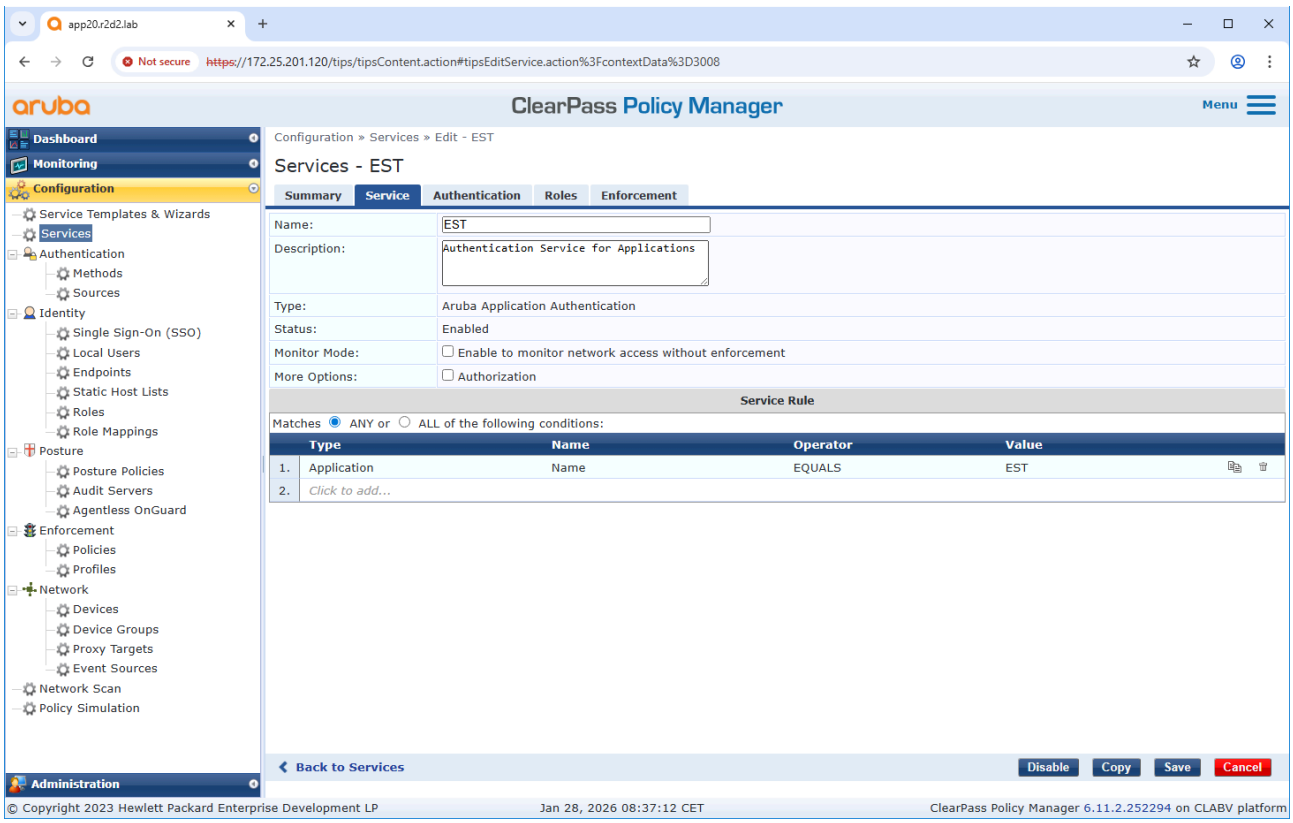


このサンプルポリシーでは、ESTアプリケーションはすべての曜日で許可されます。

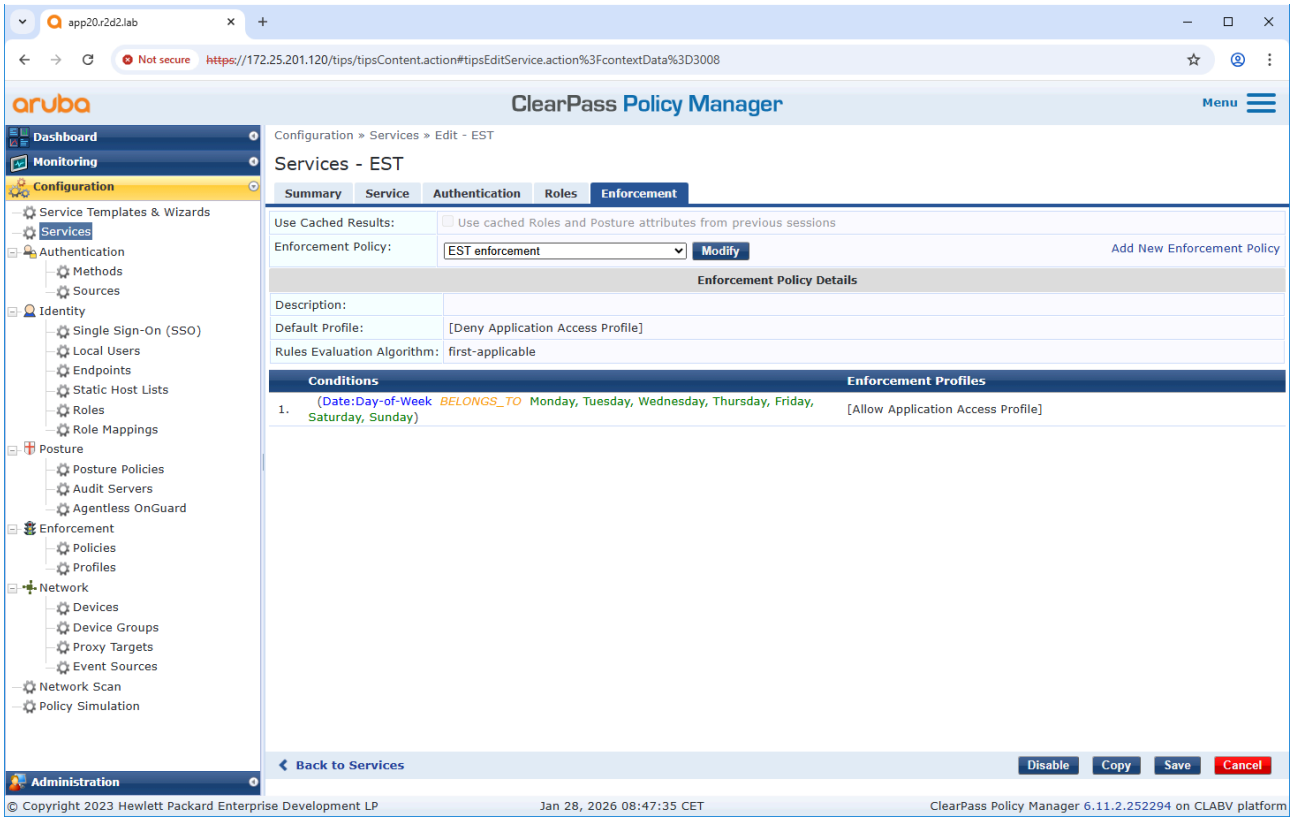
サービスの設定



専用のESTサービスを作成する必要があります。



このサービスはESTアプリケーション向けに設定されるべきです。



以前に作成したEST強制ポリシーを選択します。

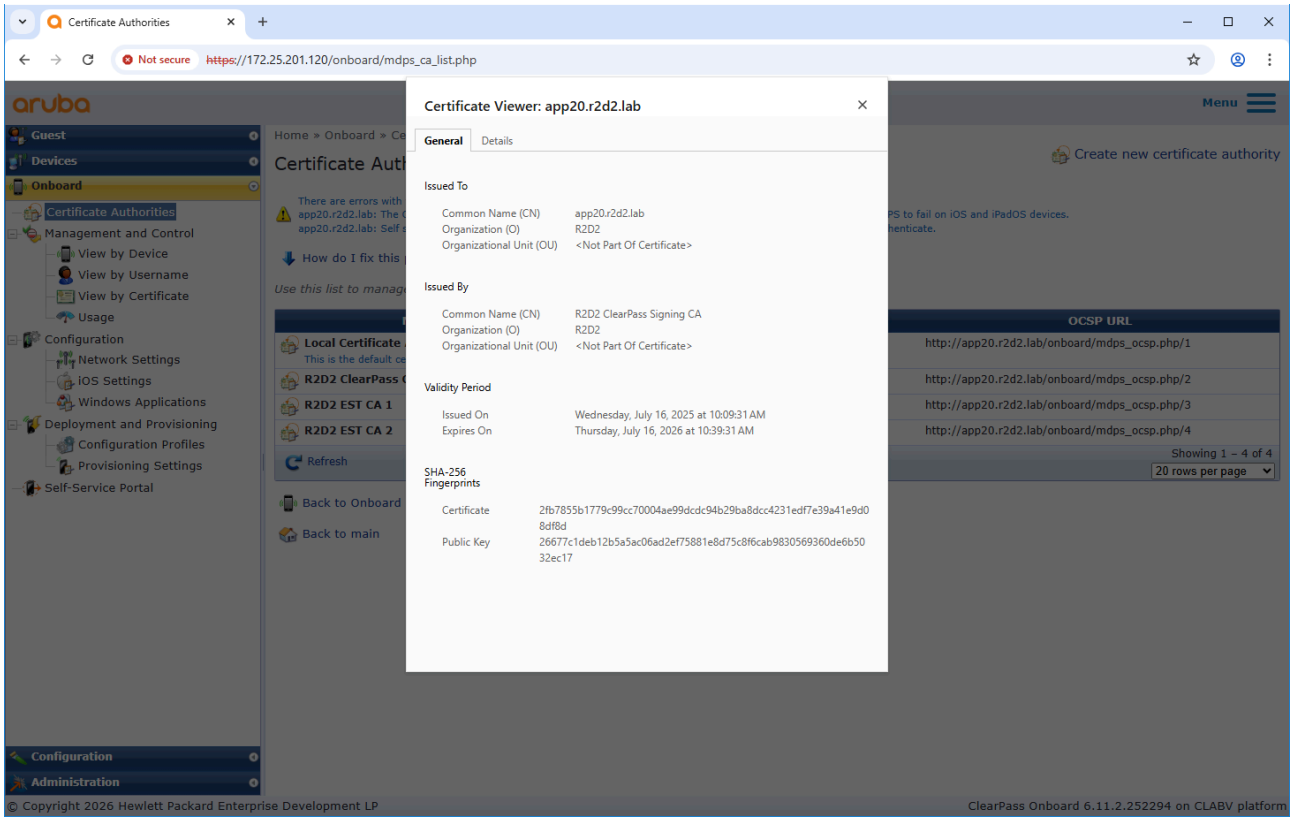
Axisの設定

Axisデバイスの設定は、2つのステップで行われます。

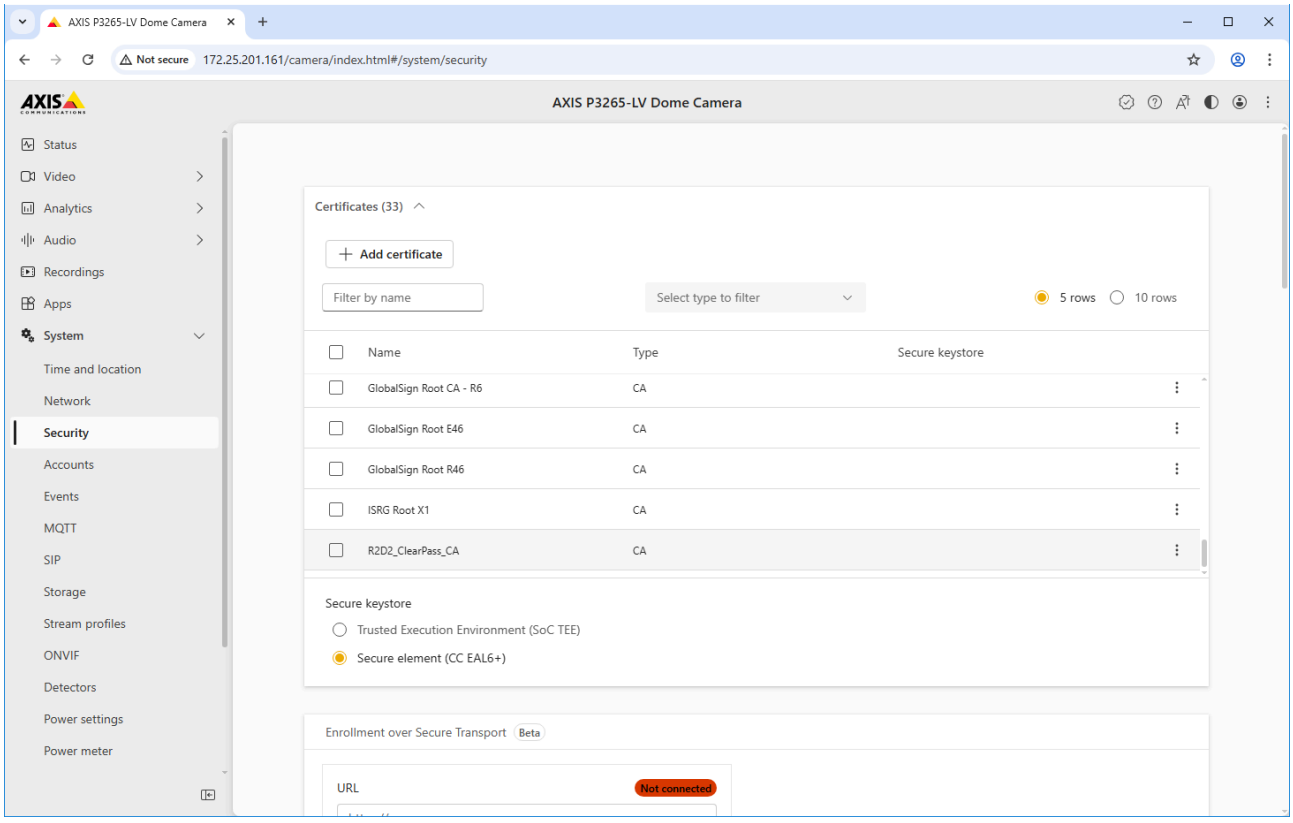
1. ClearPass OnboardのHTTPSエンドポイントとの信頼関係を確立します。

2. Axisデバイス上でESTクライアントの設定を行います。

信頼できる証明書ストアの設定

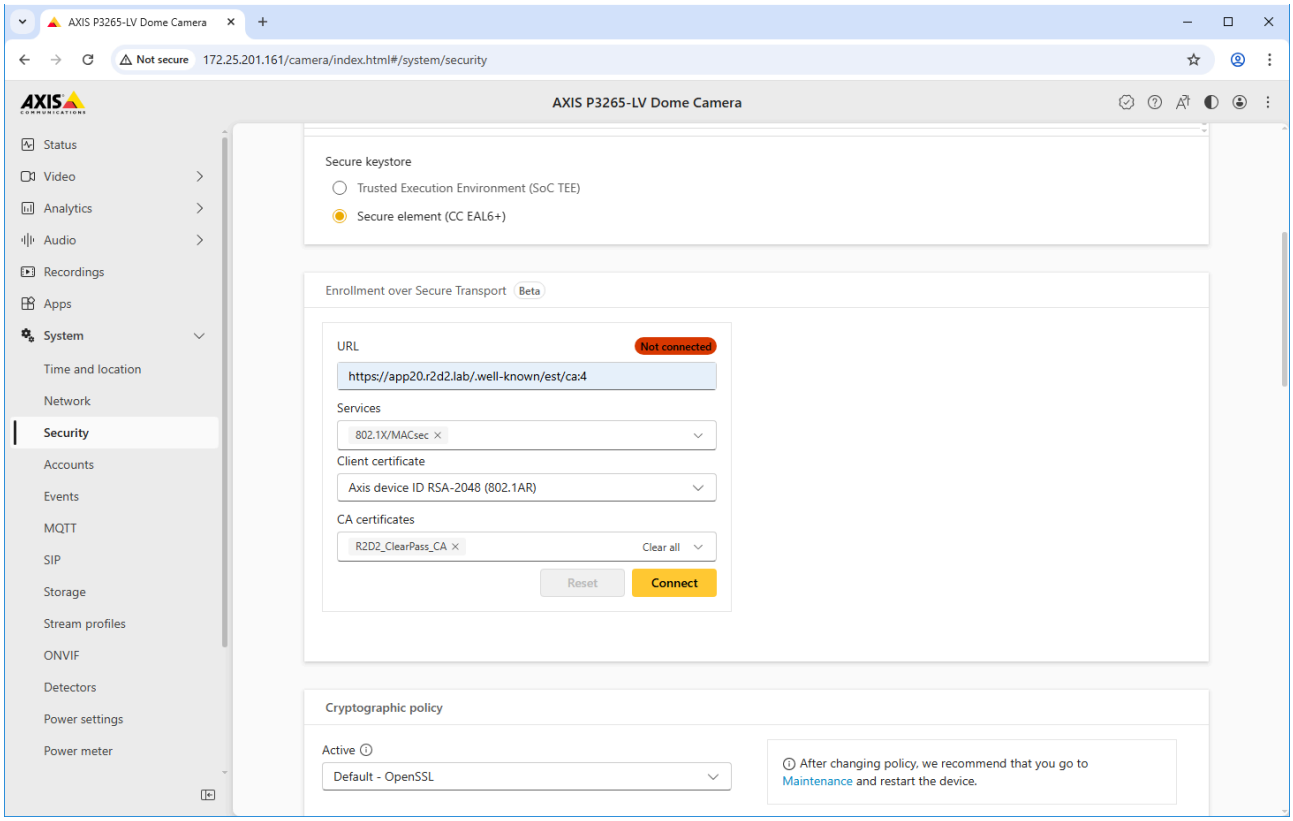


ClearPass OnboardのHTTPSエンドポイントからの証明書チェーンを確認します。

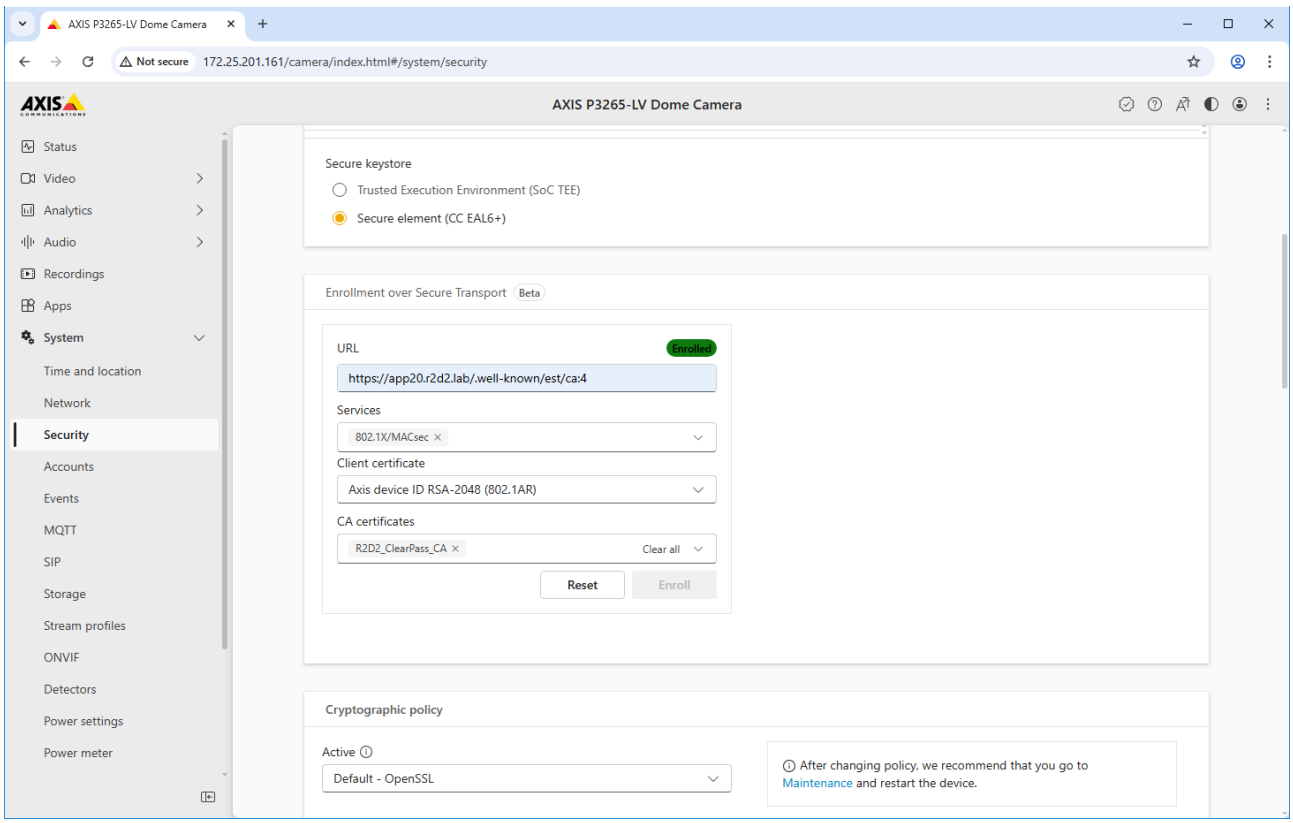


ClearPass Onboard HTTPSエンドポイントからCAをAxisデバイスにアップロードします。

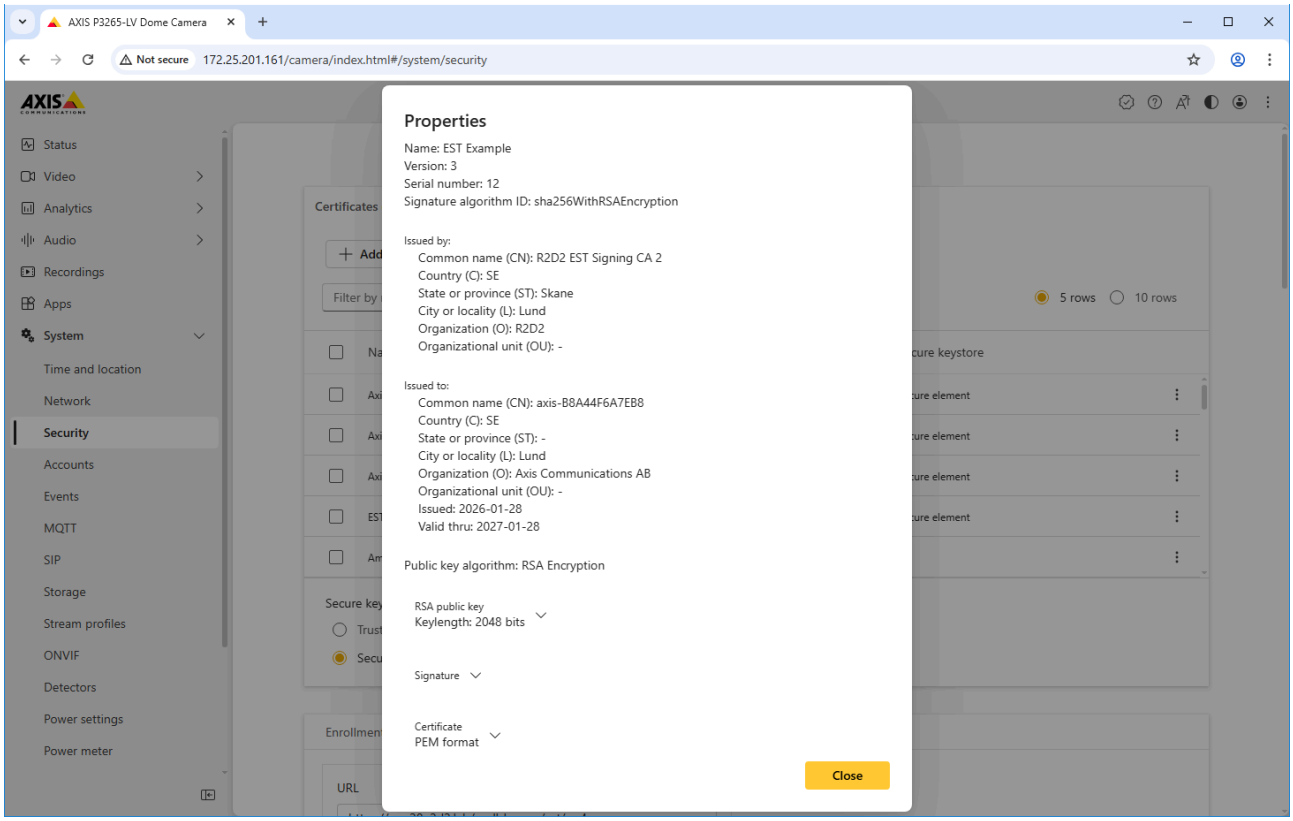
ESTクライアントの設定



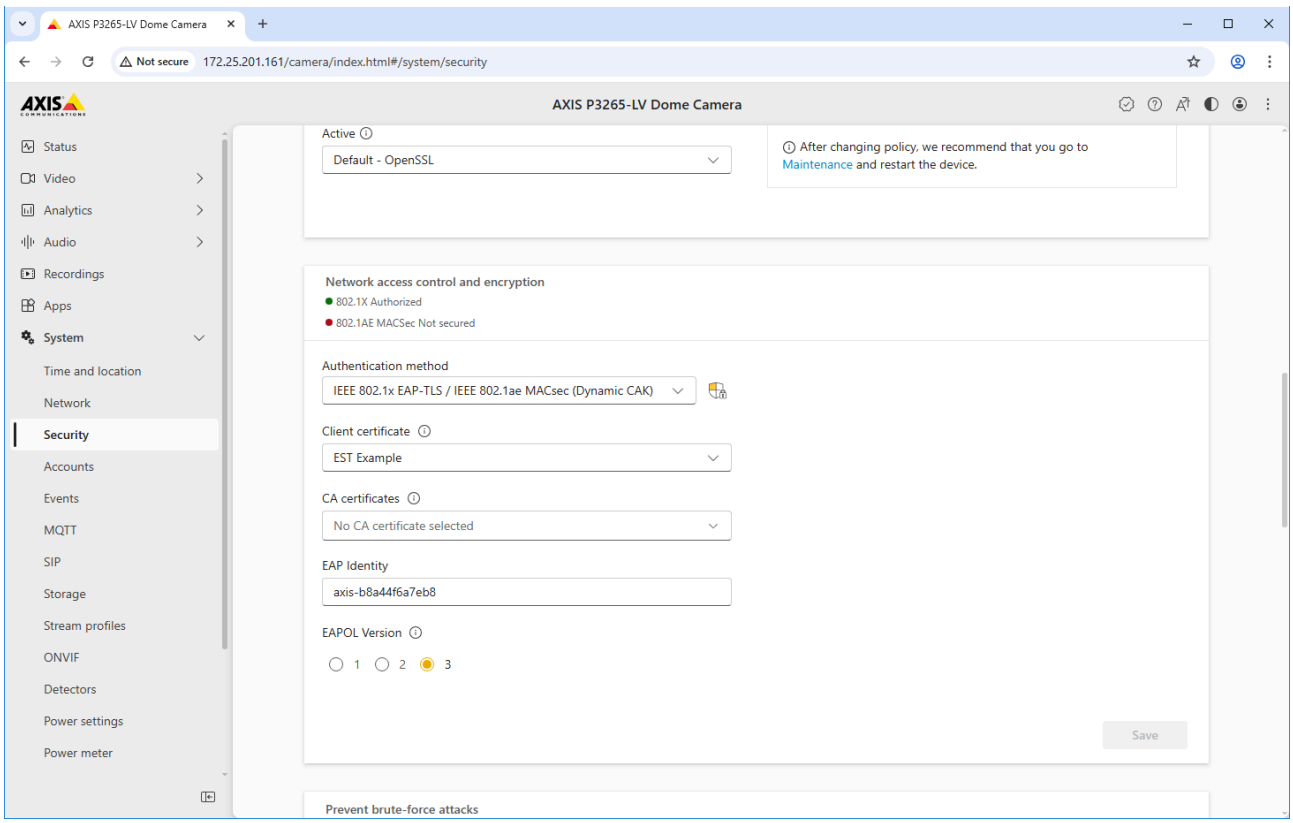
パラメーター	値
URL	ESTのURLは、ClearPass Onboardで作成したEST用認証局 (CA) 内に記載されています。
サービス	登録された証明書で自動的に設定するサービスを選択します。
クライアント証明書	ClearPass Onboard ESTサーバーに対する認証に使用するクライアント証明書を選択します。AxisデバイスIDを持つデバイスは、登録時に自動的に信頼されます。これは、Axis固有のIEEE 802.1AR証明書チェーンがClearPass Policy Managerの信頼済み証明書ストアに追加されたためです。
CA証明書	ClearPass Onboard HTTPSエンドポイントからCA証明書を選択し、Axisデバイスがそのエンドポイントを信頼するように設定します。



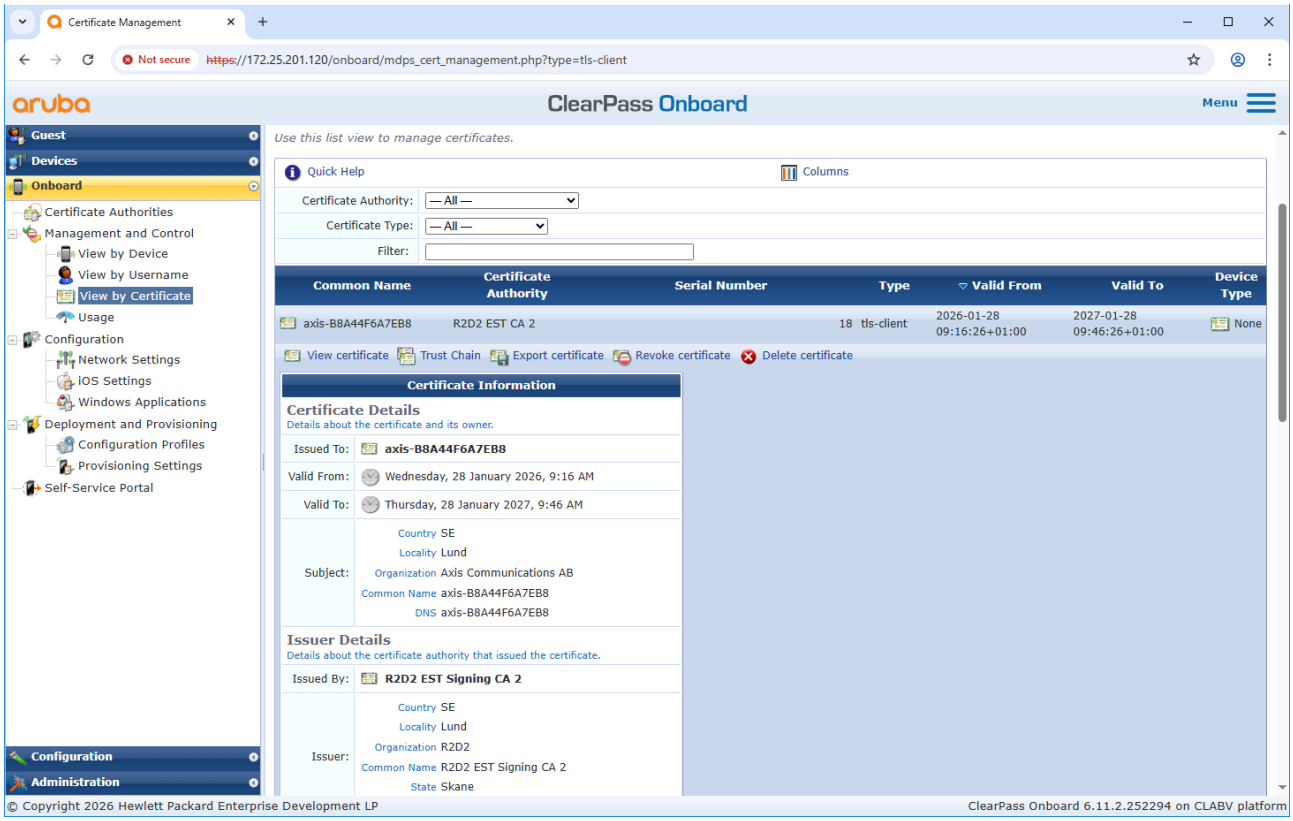
登録が完了しました。



Axisデバイス上のEST登録証明書。



登録された証明書は、事前に選択されたサービスに自動的に割り当てられます。



ClearPass Onboardで、登録済みの証明書を確認することもできます。

レガシーオンボーディング - MAC認証

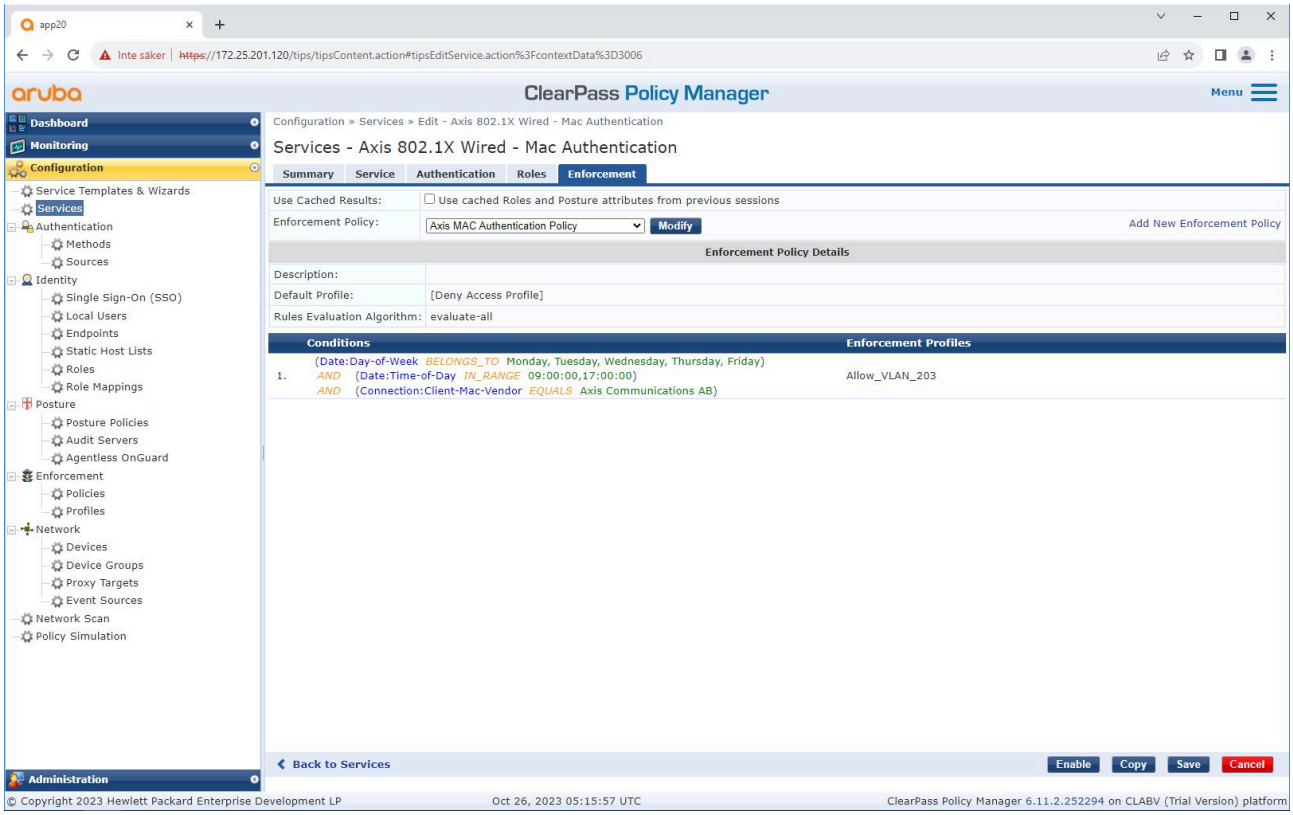
MAC Authentication Bypass (MAB) とAxisデバイスID証明書、工場出荷時の設定で有効化されているIEEE 802.1Xを使用して、IEEE 802.1ARをサポートしないAxisデバイスをオンボーディングすることができます。802.1Xオンボーディングが失敗した場合、ClearPass Policy ManagerはAxisデバイスのMACアドレスを検証し、ネットワークへのアクセスを付与します。

MABには、アクセススイッチとClearPass Policy Manager構成の両方の準備が必要です。Axisデバイスで MABによるオンボーディングを有効にするための設定は不要です。

HPE Aruba Networking ClearPass Policy Manager

強制ポリシー

ClearPass Policy Managerの強制ポリシー設定は、次の2つのサンプルポリシー条件に基づき、HPE Aruba Networkingによるネットワークへのアクセスを Axis装置に付与するか判断します。



ネットワークアクセスの拒否

Axisデバイスが設定された強制ポリシーの条件を満たさない場合、ネットワークへのアクセスは拒否されます。

ゲストネットワーク (VLAN 203)

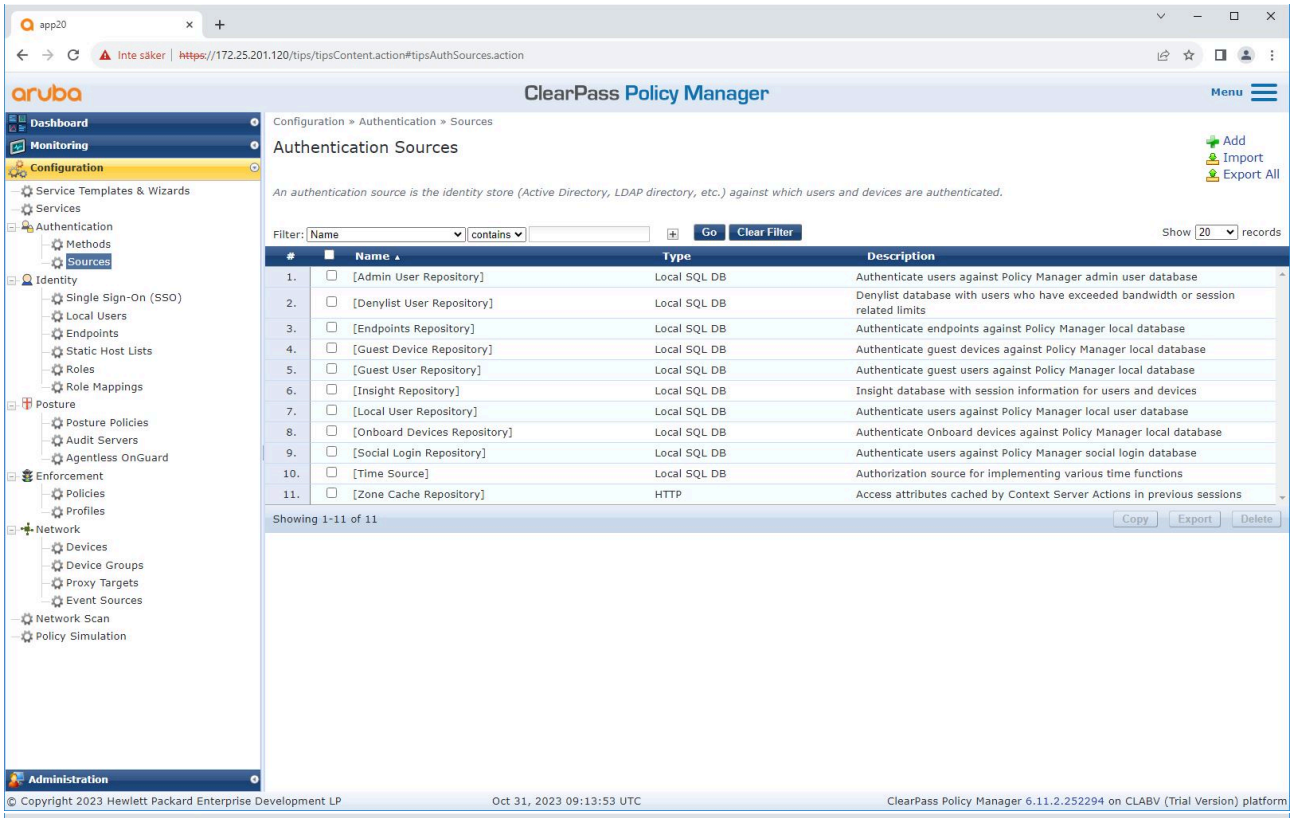
次の条件が満たされる場合、Axis装置に限定的な隔離ネットワークへのアクセスが付与されます。

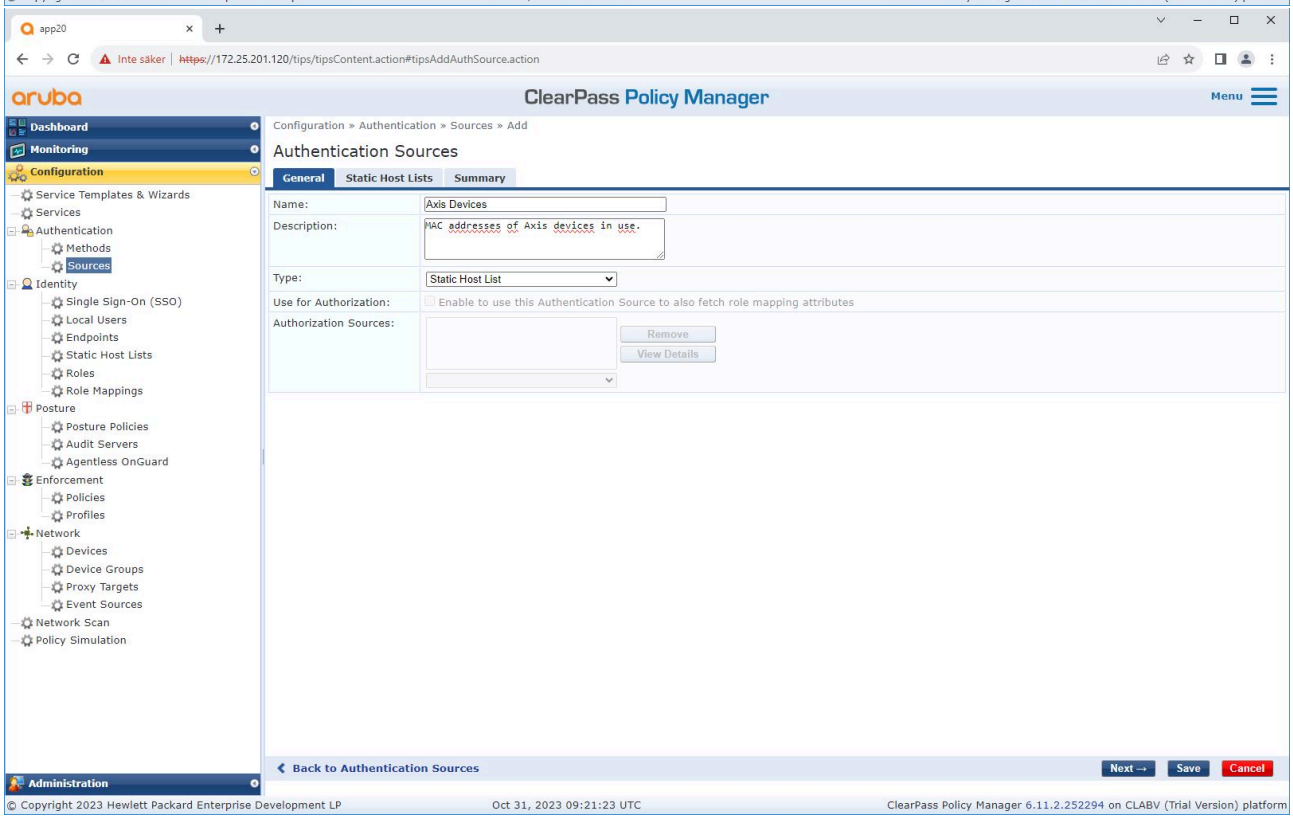
- 日が平日（月曜日～金曜日）である。
- 時間が9時～17時である。
- MACアドレスのベンダーがAxis Communicationsと一致する。

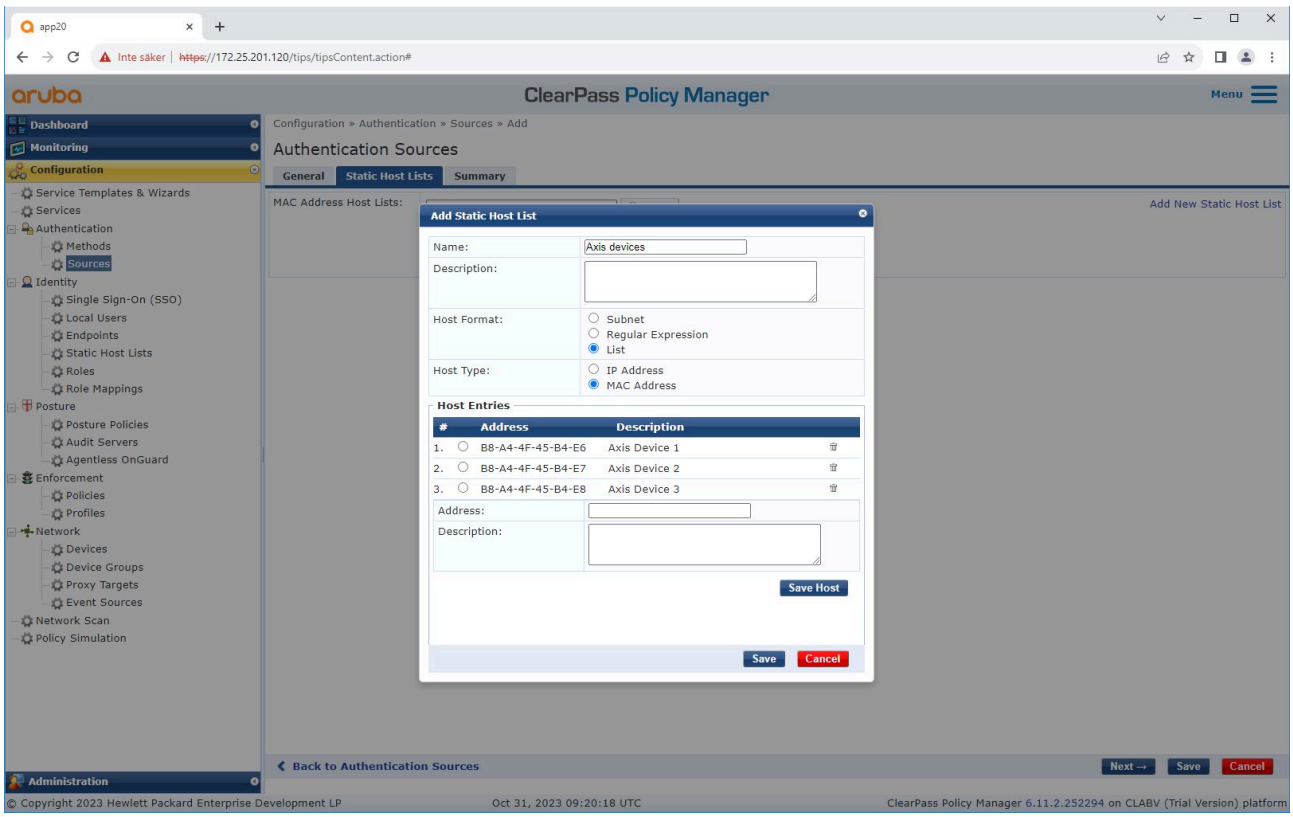
MACアドレスを偽装できるため、通常のプロビジョニングネットワークへのアクセスは付与されません。MABは初回オンボーディングにのみ使用し、デバイスをさらに手動で検査することをお勧めします。

ソースの設定

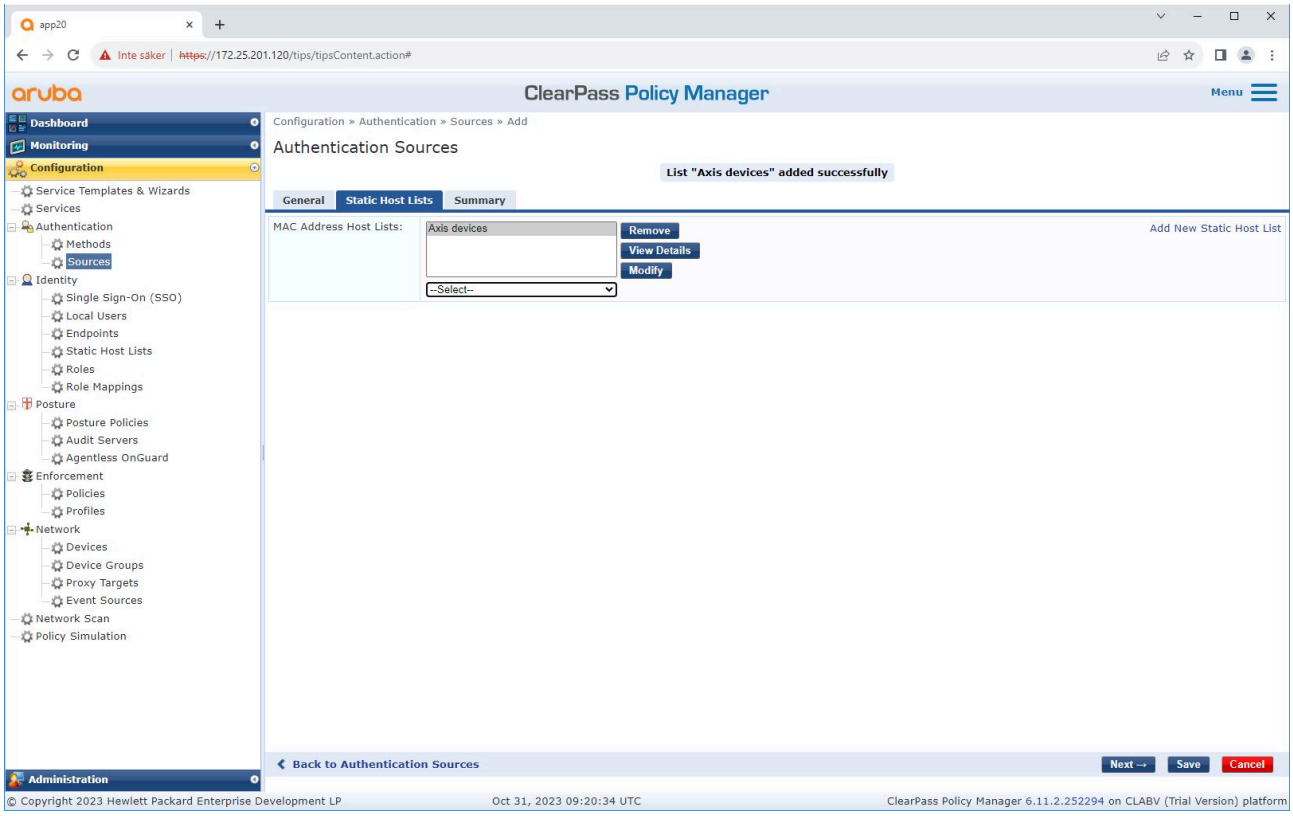
[Sources (ソース)] ページでは新しい認証ソースが作成され、手動でインポートされたMACアドレスのみを許可します。





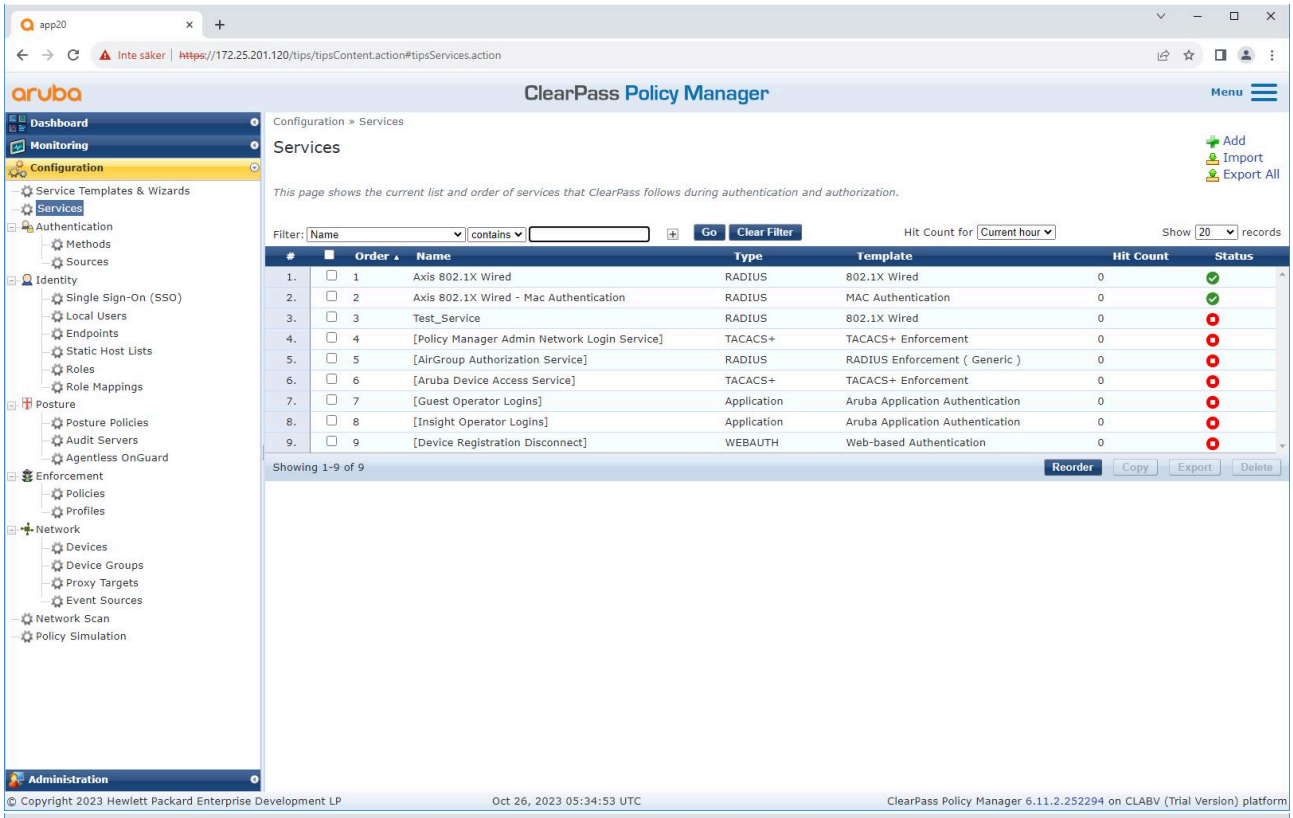


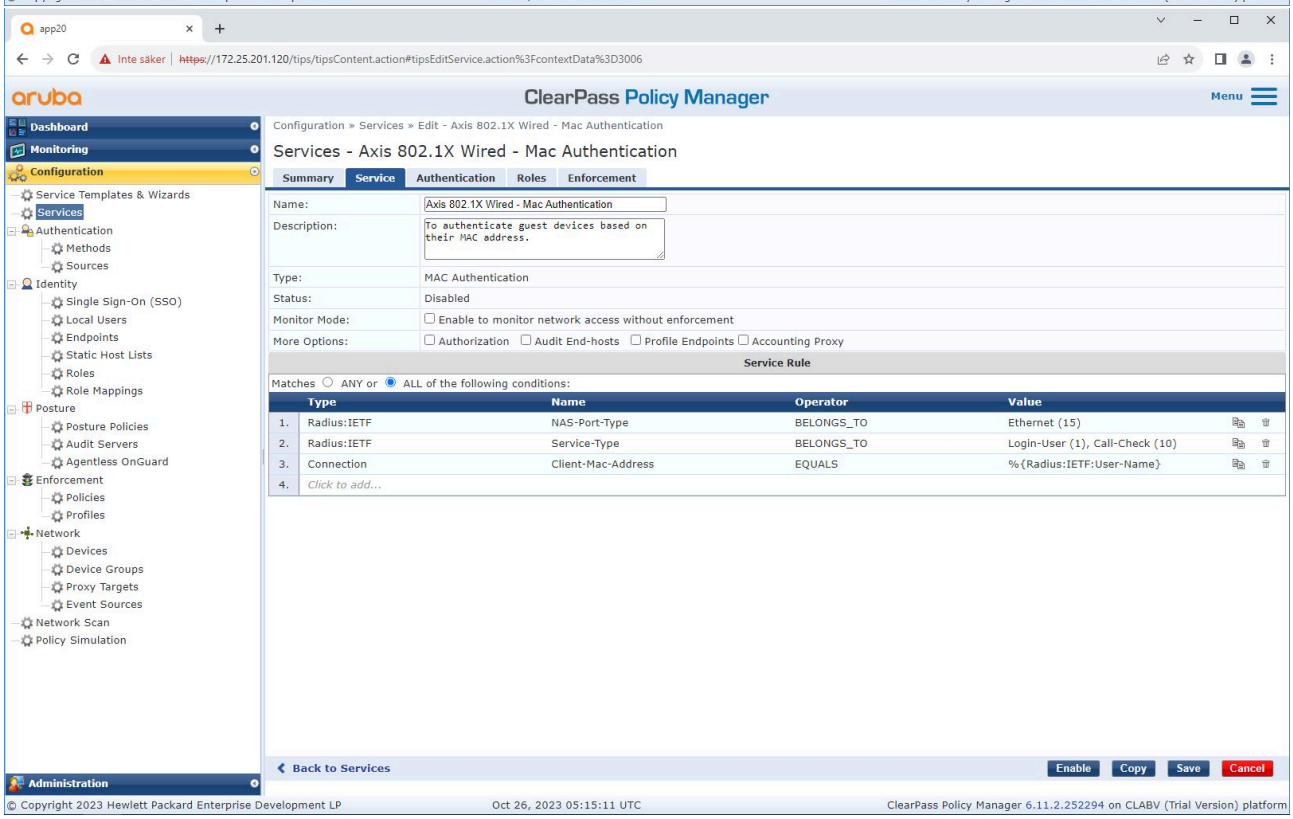
Axis MACアドレスを含む静的ホストのリストが作成されます。



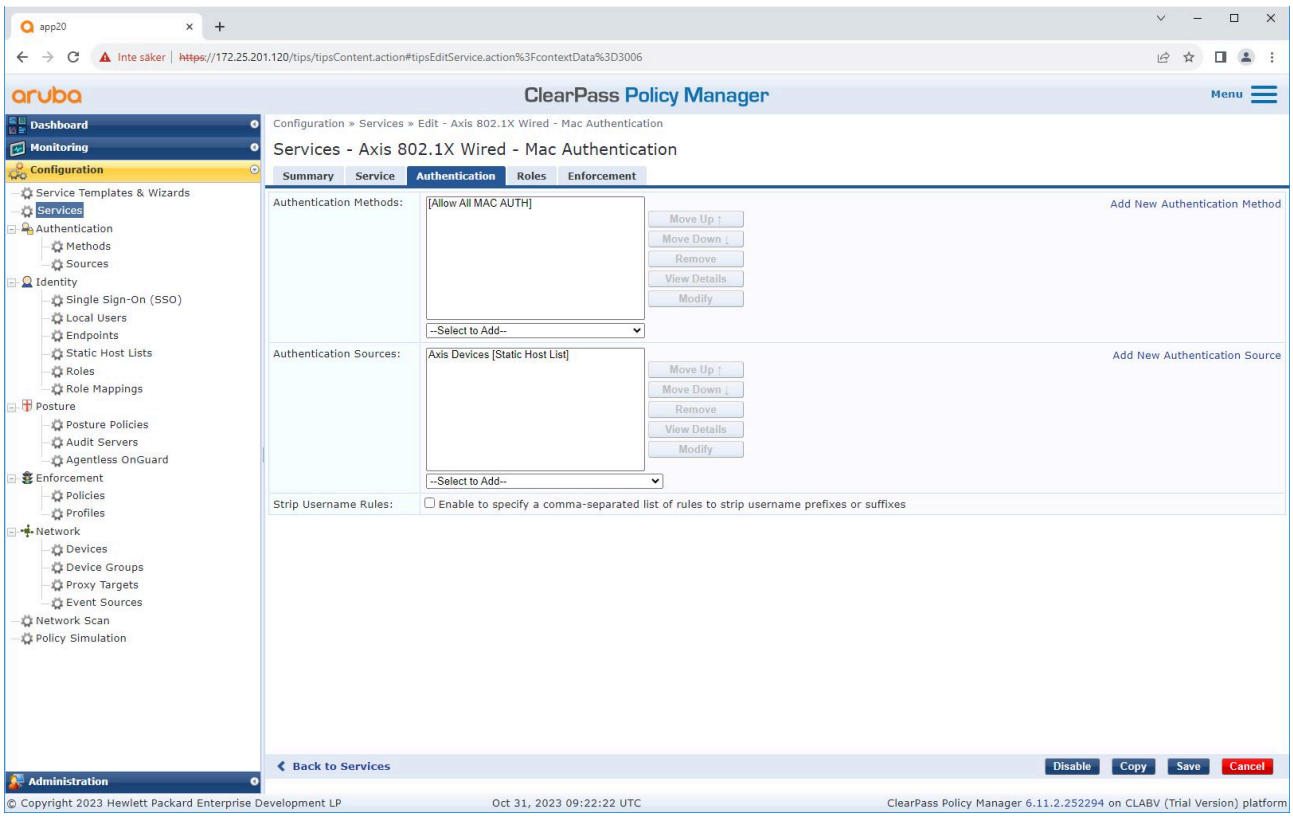
サービスの設定

[Services (サービス)] ページでは、設定手順がHPE Aruba Networkingネットワーク内のAxisデバイスの認証と承認を処理する1つのサービスに統合されています。





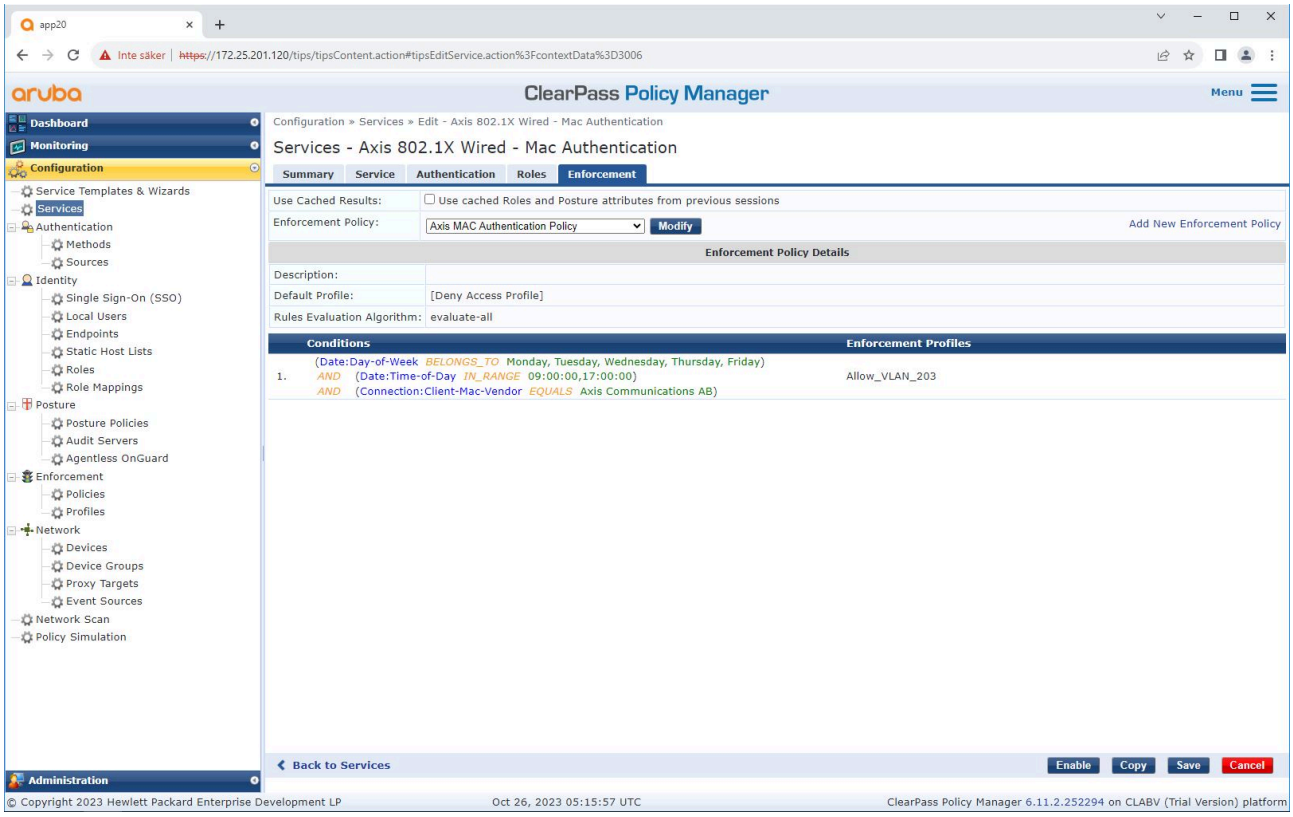
接続方式としてMABを定義する専用のAxisサービスが作成されます。



事前設定されたMAC認証方式がサービスに設定されます。また、AXISのMACアドレスのリストを含む (先に作成された) 認証ソースが選択されます。

Axis Communicationsは、次のMACアドレスOUIを使用します:

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



最後のステップで、先に作成した強制ポリシーがサービスに設定されます。

HPE Aruba Networkingアクセススイッチ

*HPE Aruba Networkingアクセススイッチ, on page 15*に記載された安全なオンボーディング設定に加えて、以下の HPE Aruba Networkingアクセススイッチのポート設定例を参照してMABを許可します。

```
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_ja

2026-02 (M8.3)