HPE Aruba Networking

移行ガイド

HPE Aruba Networking

目次

HPE Aruba Networking

はじめに

はじめに

この統合ガイドでは、HPE Aruba Networking基盤のネットワークにAxis装置を搭載して運用する方法について、ベストプラクティスの構成を概説します。ベストプラクティスの構成では、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ために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。適切な自動化の実施により、Axisの装置管理アプリケーションを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。Axis装置とAxisソフトウェアをHPE Aruba Networkingインフラストラクチャーと組み合わせることで生じるメリットには、次の点があります:

- 装置のステージングネットワークを削除することで、システムを極力シンプルに保つ。
- オンボーディングプロセスと装置管理に自動化を追加してコストを節約する。
- Axis装置が提供するゼロタッチネットワークセキュリティ制御を活用する。
- HPEとAxisの専門知識を適用し、ネットワーク全体のセキュリティを強化する。

構成を開始する前に、Axis装置の整合性を安全に検証するためのネットワークインフラストラクチャーの準備を完了しておく必要があります。これによりオンボーディングプロセス全体を通じて、ソフトウェア定義による論理ネットワーク間でのスムーズな移行が可能になります。設定を行う前に、次の領域に関する知識が不可欠です。

- HPE Aruba Networkingアクセススイッチ やHPE Aruba Networking ClearPass Policy Managerなど、HPE Aruba Networking基盤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。
- 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。
- Axis製品に関する基本的な知識はあることが望ましい (ただし、ガイドの中で提供されます)。

安全なオンボーディング - IEEE 802.1AR/802.1X

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がサポートするAxis装置をネットワークに接続して、ネットワーク認証を取得します。装置はIEEE 802.1AR AxisデバイスID証明書を使用し、IEEE 802.1Xネットワークアクセスコントロールを経由して自己認証します。

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と装置固有の他のフィンガープリントを検証します。MACアドレスや実行中のAXIS OSなどの情報は、ポリシーに基づく決定に使用されます。

Axis装置は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。

Axis装置はHPE Aruba Networking基盤の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装置はAXIS Device Managerがインストールされているプロビジョニングネットワーク (VLAN201) に移動します。AXIS Device Managerを使用して、装置の設定、セキュリティ強化、ファームウェアのアップデートを実行できます。装置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装置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装置を運用ネットワークに移行するか決定します。

装置の設定後、Axis装置はプロビジョニングネットワークから離脱し、ネットワークに対して再認証を試みます。

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*

再認証されると、Axis装置は運用ネットワーク (VLAN 202) に移行します。運用ネットワークではビデオ管理システム (VMS) がAxis装置に接続し、動作が開始します。

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*

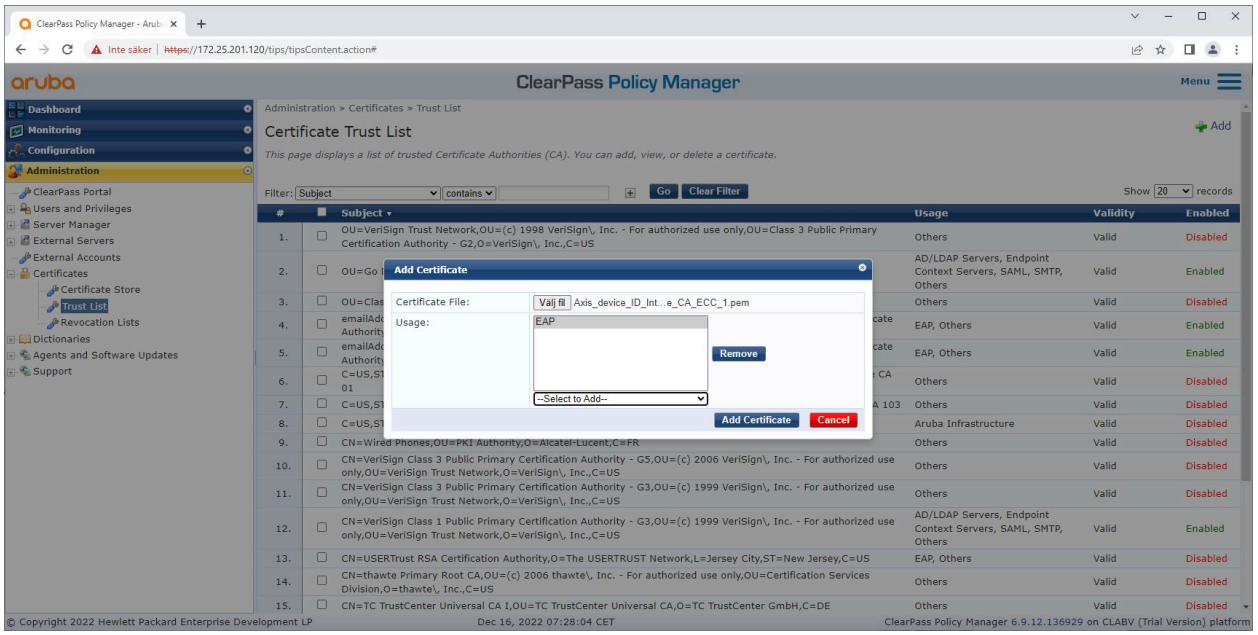
HPE Aruba Networkingの設定

HPE Aruba Networking ClearPass Policy Manager

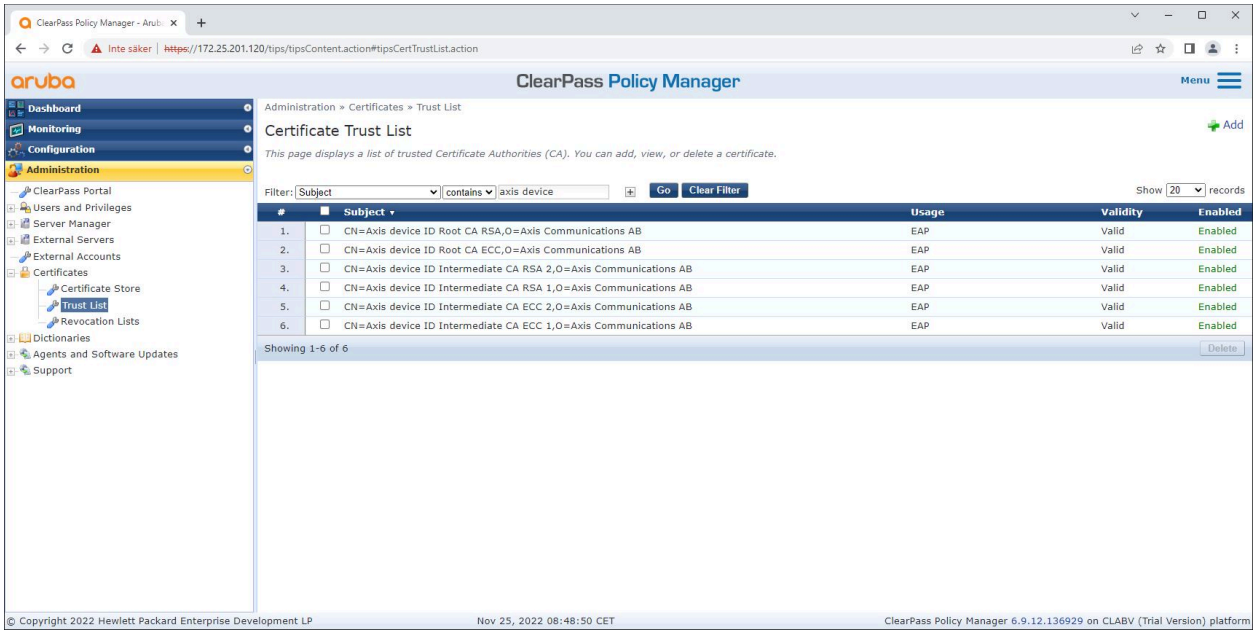
ClearPass Policy Managerは、マルチベンダーの有線、ワイヤレス、VPNインフラストラクチャー全体でIoT、BYOD、コーポレート装置、従業員、請負業者、ゲストを対象とする役割ベースと装置ベースの安全なネットワークアクセスコントロールを提供します。

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。



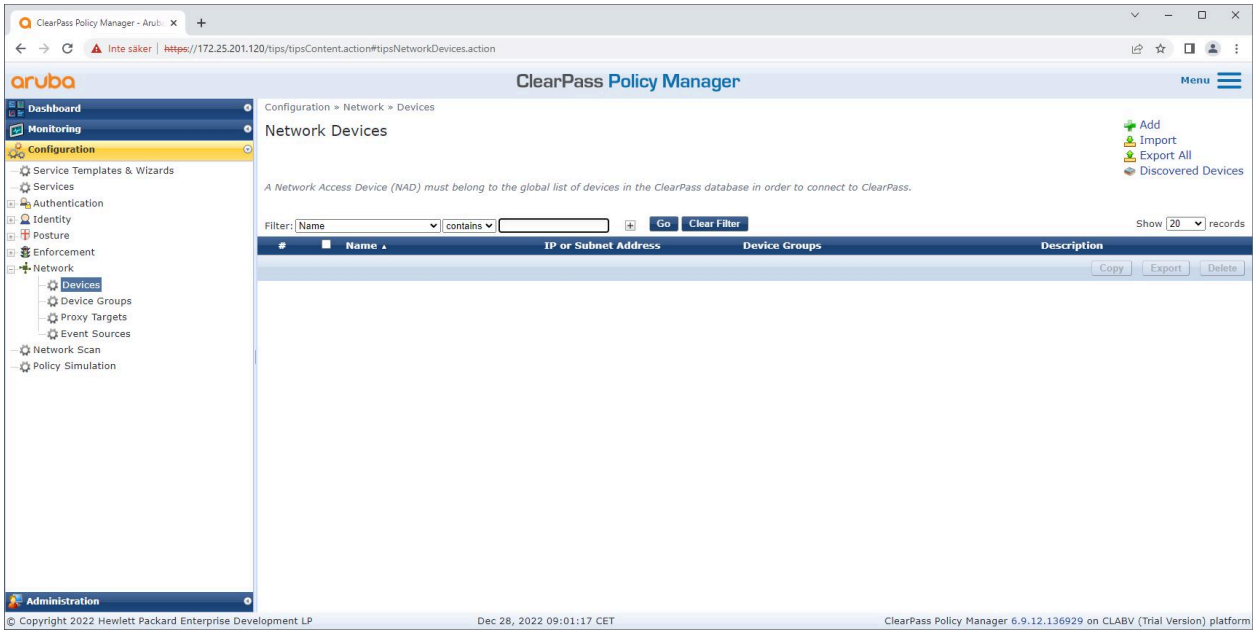
Axis固有のIEEE 802.1AR証明書チェーンを含む、ClearPass Policy Manager内の信頼された証明書ストア。

ネットワーク装置/グループの構成

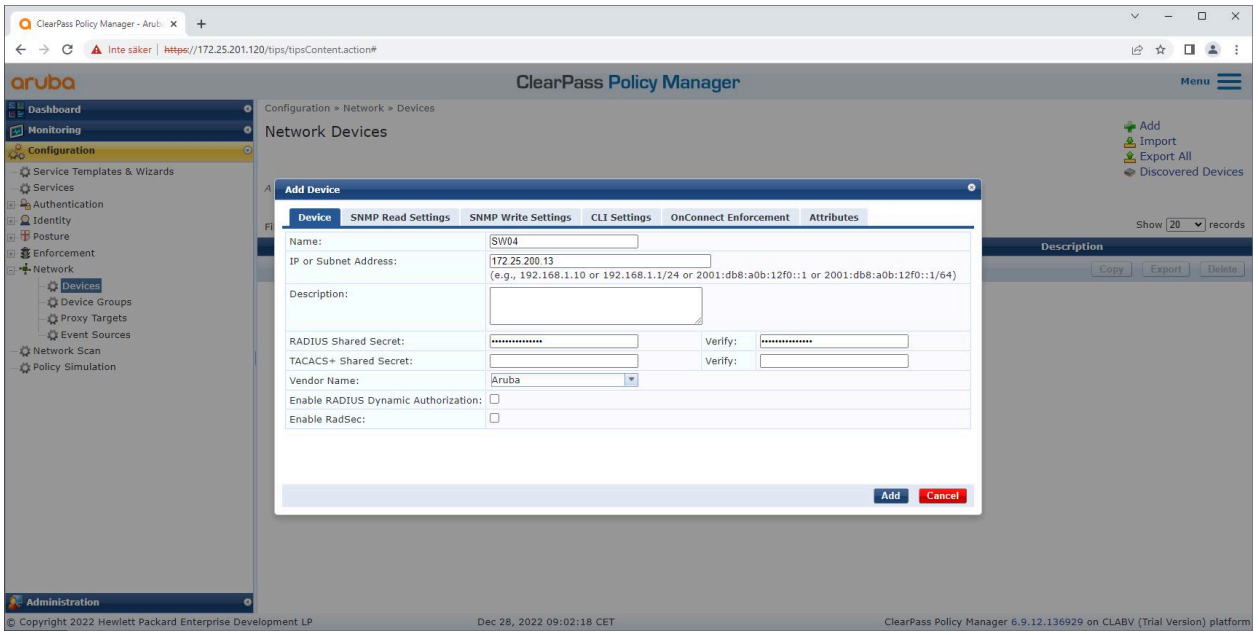
1. HPE Aruba Networkingアクセススイッチなどの信頼できるネットワークアクセス装置をClearPass Policy Managerに追加します。ClearPass Policy Managerは、ネットワーク内でIEEE 802.1X通信に使用されるアクセススイッチを把握する必要があります。

2. ネットワーク装置グループ構成を使用して、複数の信頼できるネットワークアクセス装置をグループ化します。信頼できるネットワークアクセス装置をグループ化ことで、ポリシーの構成を簡単に行うことができます。

3. RADIUS共有秘密は、特定のスイッチのIEEE 802.1X構成と一致させる必要があります。

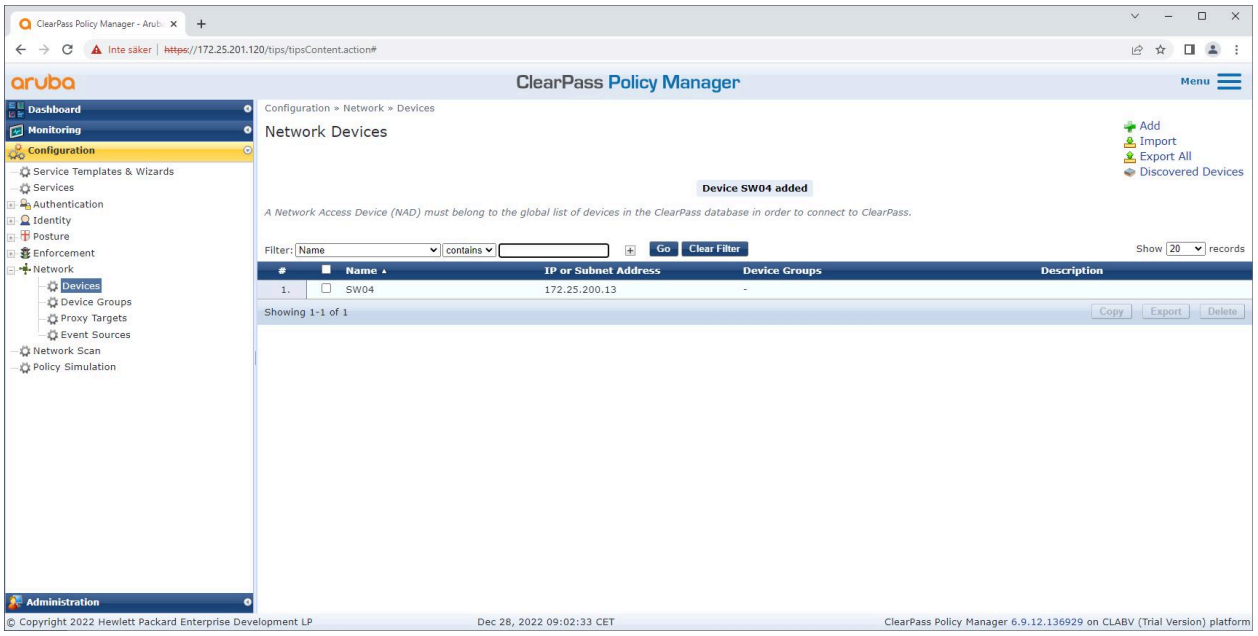


ClearPass Policy Managerの信頼されたネットワーク装置インターフェース。

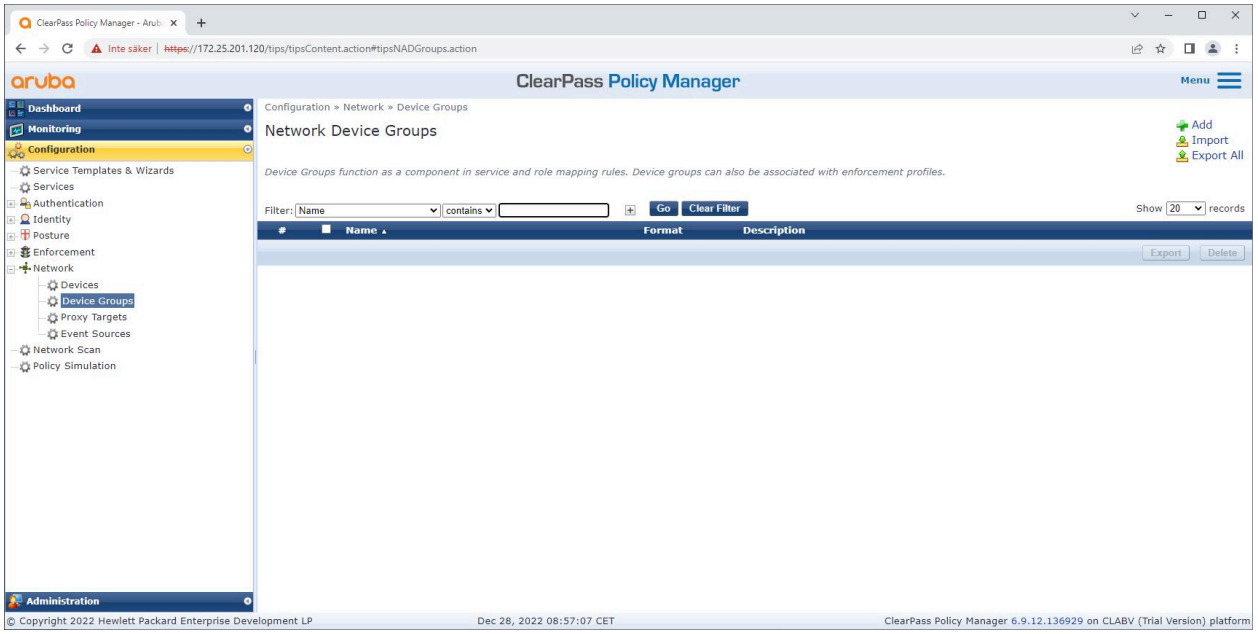


信頼できるネットワーク装置としてHPE Aruba Networkingアクセススイッチを ClearPass Policy Managerに追加します。RADIUS共有秘密は、特定のスイッチのIEEE 802.1X設定と一致させる必要があることに注意してください。

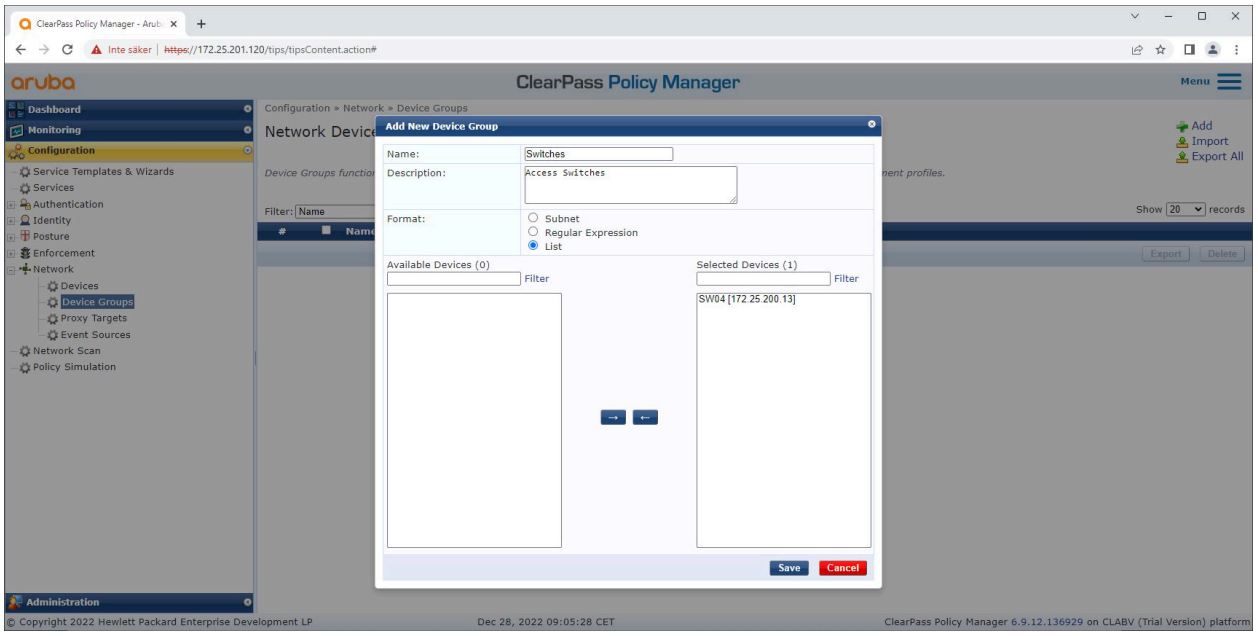
安全なオンボーディング - IEEE 802.1AR/802.1X



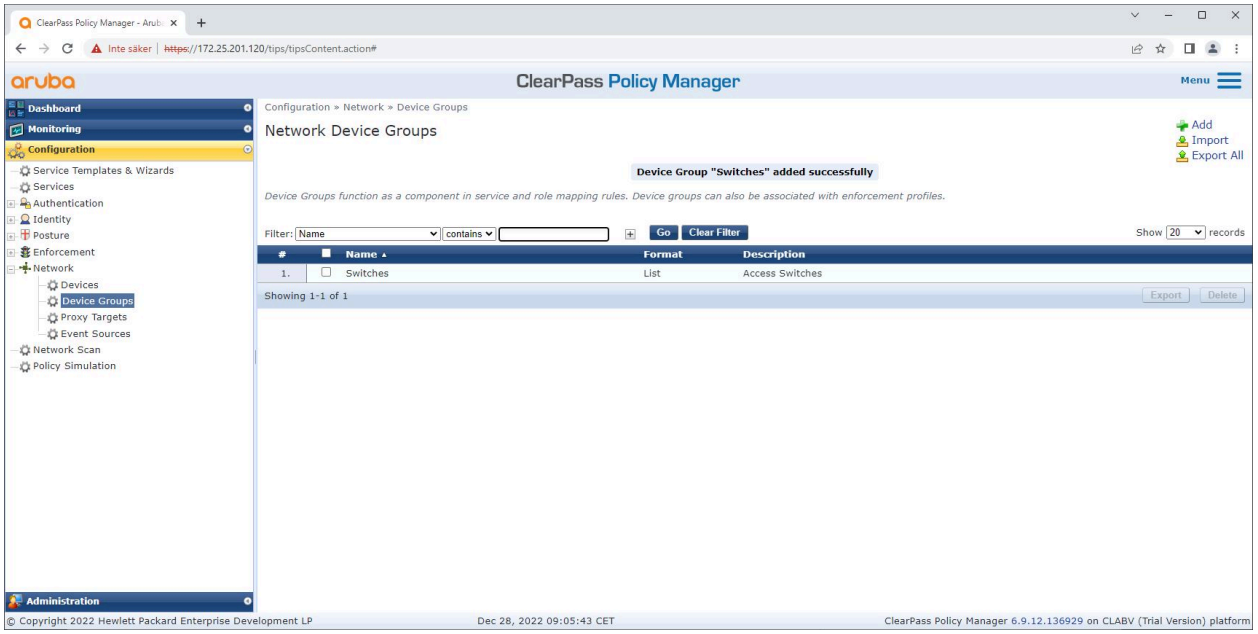
1つの信頼できるネットワーク装置が設定されたClearPass Policy Manager。



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の新規装置グループに、信頼されたネットワークアクセス装置を追加します。



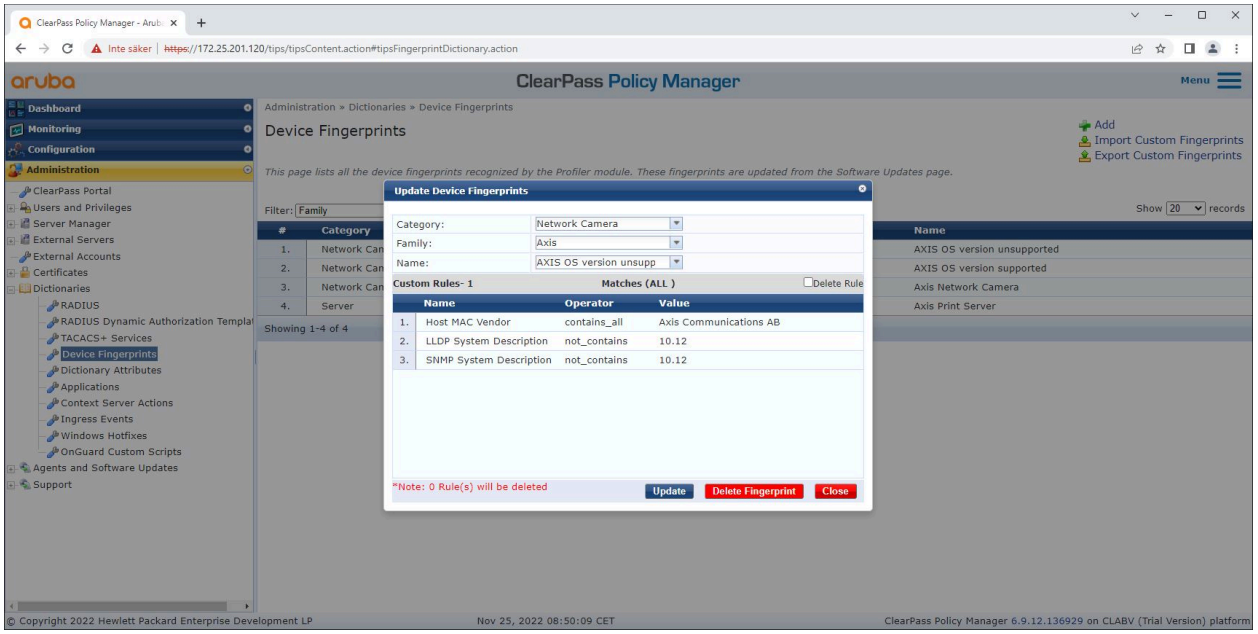
ClearPass Policy Managerで、1つまたは複数の信頼できるネットワーク装置を含むネットワーク装置グループが構成された状態。

装置のフィンガープリントの構成

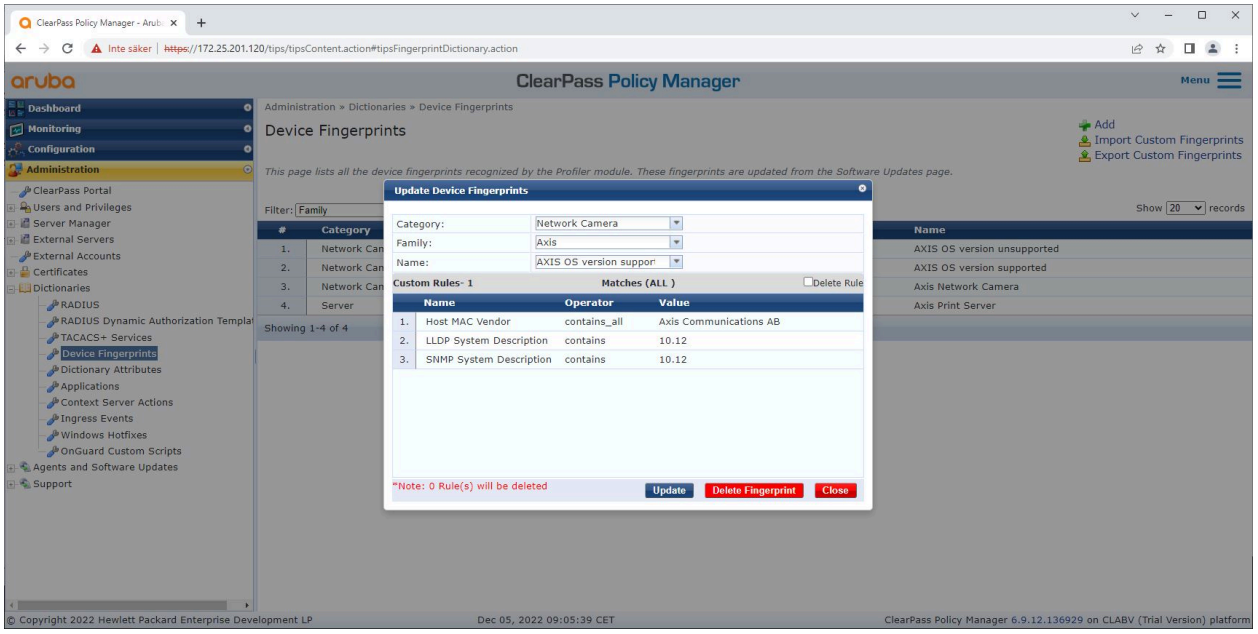
Axis装置は、ネットワーク検出を通じてMACアドレスや装置のソフトウェアバージョンなど装置固有の情報を配布できます。この情報を使用して、ClearPass Policy Managerで装置フィンガープリントを作成、更新、管理します。また、AXIS OSバージョンに基づいてアクセスを許可または拒否することもできます。

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. 装置のフィンガープリントの設定を行います。



ClearPass Policy Managerでの装置フィンガープリント設定。10.12以外のAXIS OSバージョンを実行するAxis装置はサポート対象外とみなされます。



ClearPass Policy Managerでの装置フィンガープリント設定。上記の例では、AXIS OS 10.12を実行するAxis装置がサポート対象と見なされています。

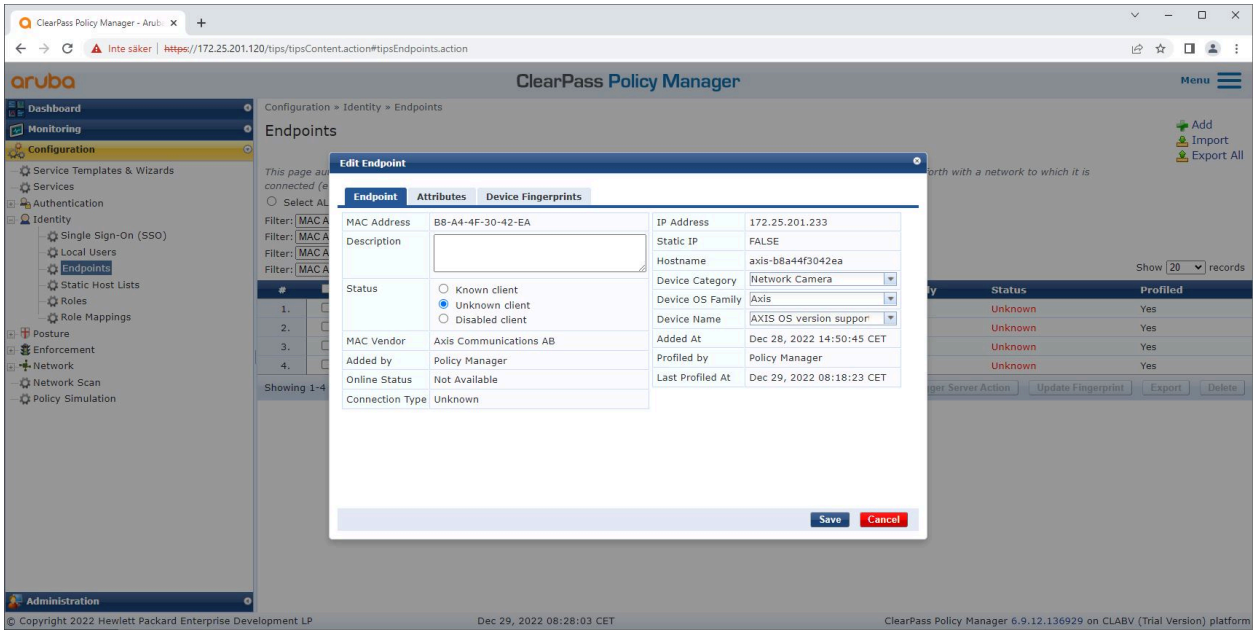
Aruba ClearPass Managerで収集された装置のフィンガープリントに関する情報は、エンドポイントセクションにあります。

安全なオンボーディング - IEEE 802.1AR/802.1X

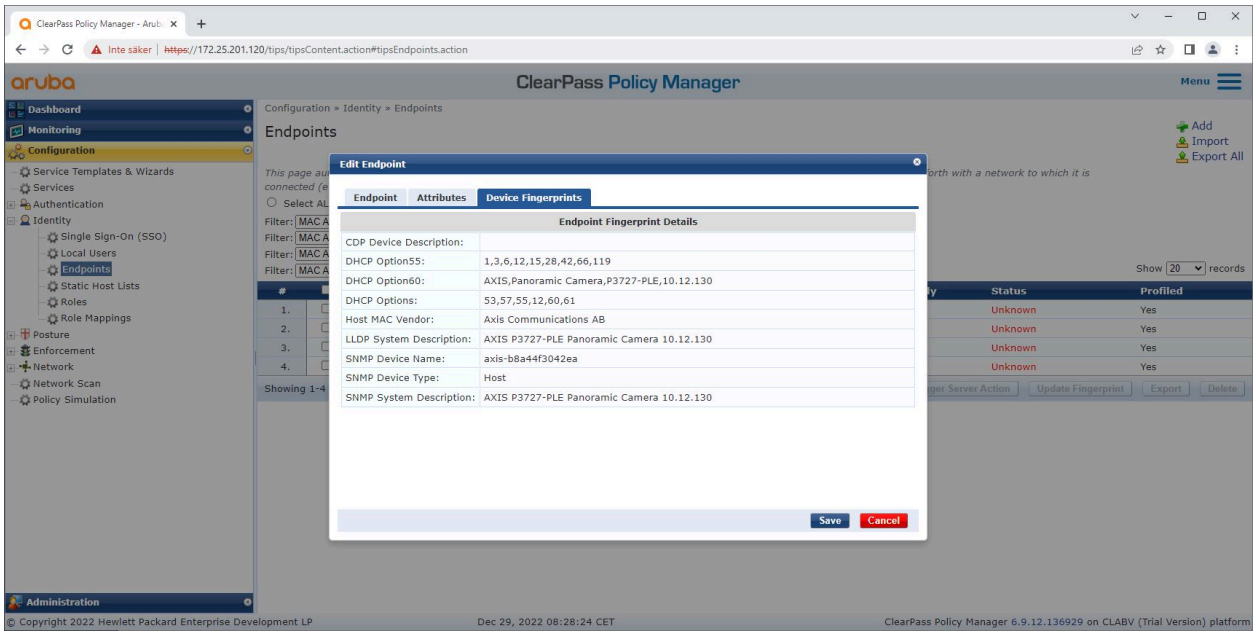
1. [Configuration（構成）] > [Identity（ID）] > [Endpoints（エンドポイント）] に進みます。
2. 表示する装置を選択します。
3. [Device Fingerprints（装置のフィンガープリント）] タブをクリックします。

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。

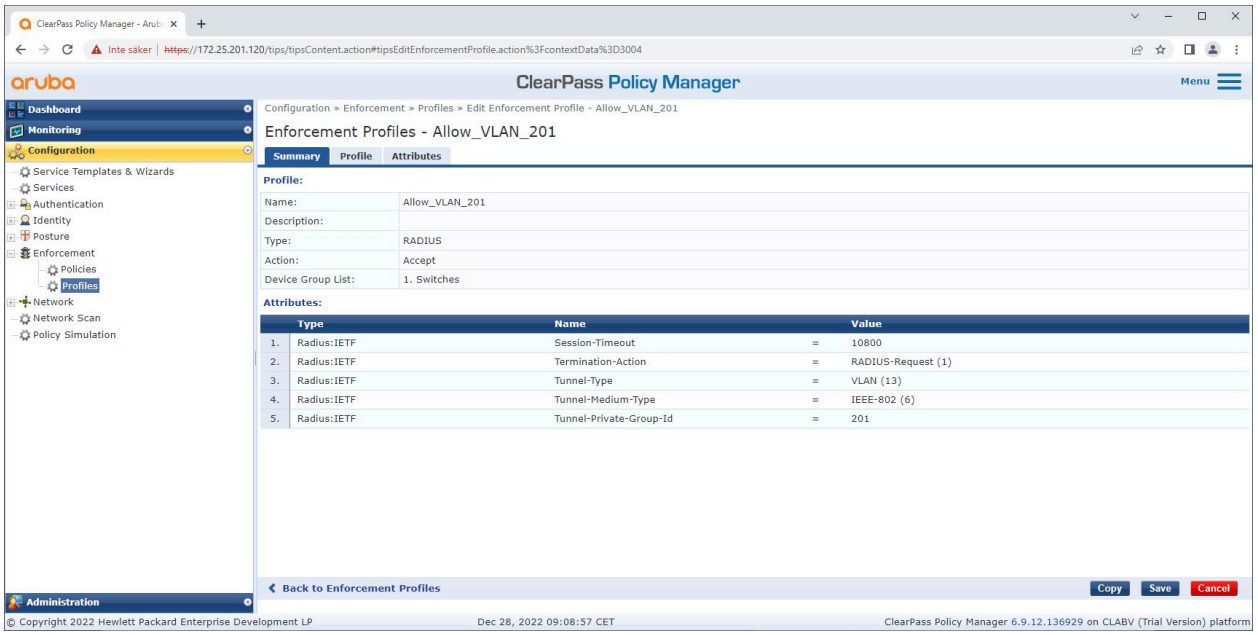


*プロファイルされたAxis装置の詳細な装置フィンガープリント。Axis装置ではSNMPがデフォルトで無効になっていることに注意してください。LLDP、CDP、およびDHCP固有の検出情報は、Axis装置によって工場出荷時の設定ステータスで共有され、HPE Aruba Networkingアクセススイッチによって*ClearPass Policy Managerに中継されます。

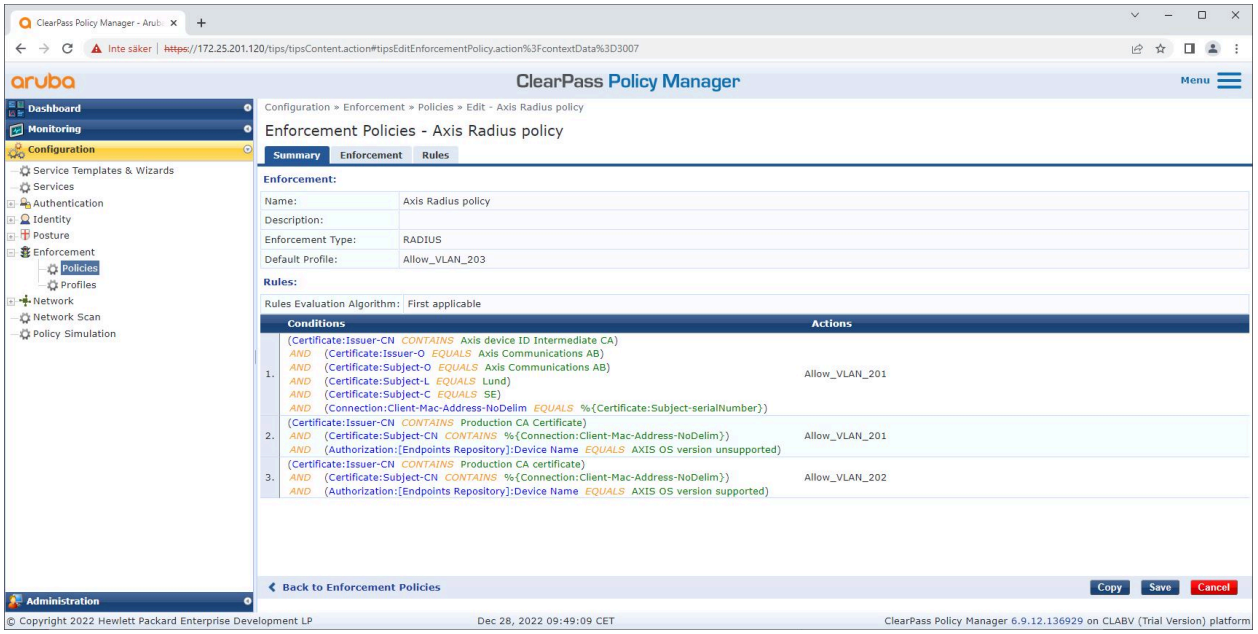
強制プロファイルの構成

[**Enforcement Profile (強制プロファイル)**] を用いることで、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。割り当てはポリシーに基づいて決定され、装置グループ「スイッチ」内のネットワーク装置に適用されます。必要な強制プロファイルの数は、使用されるVLANの数によって異なります。この設定には、合計で3つのVLAN (VLAN 201、202、203) があり、3つの強制プロファイルに関連付けられています。

VLANの強制プロファイル構成を完了すると、実際の強制ポリシーを設定できます。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基盤の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。



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)

HPE Aruba Networking

安全なオンボーディング - IEEE 802.1AR/802.1X

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。適切な対応を実施するためには、装置を手動で検査する必要があります。

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。これは、Axis装置の管理機能を*AXIS Device Manager*と*AXIS Device Manager Extend*経由で提供するためです。また、AXIS OSの更新、運用グレードの証明書、その他の構成を使用して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:

- Axis装置のAXIS OSバージョン。
- 装置の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Axis 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。

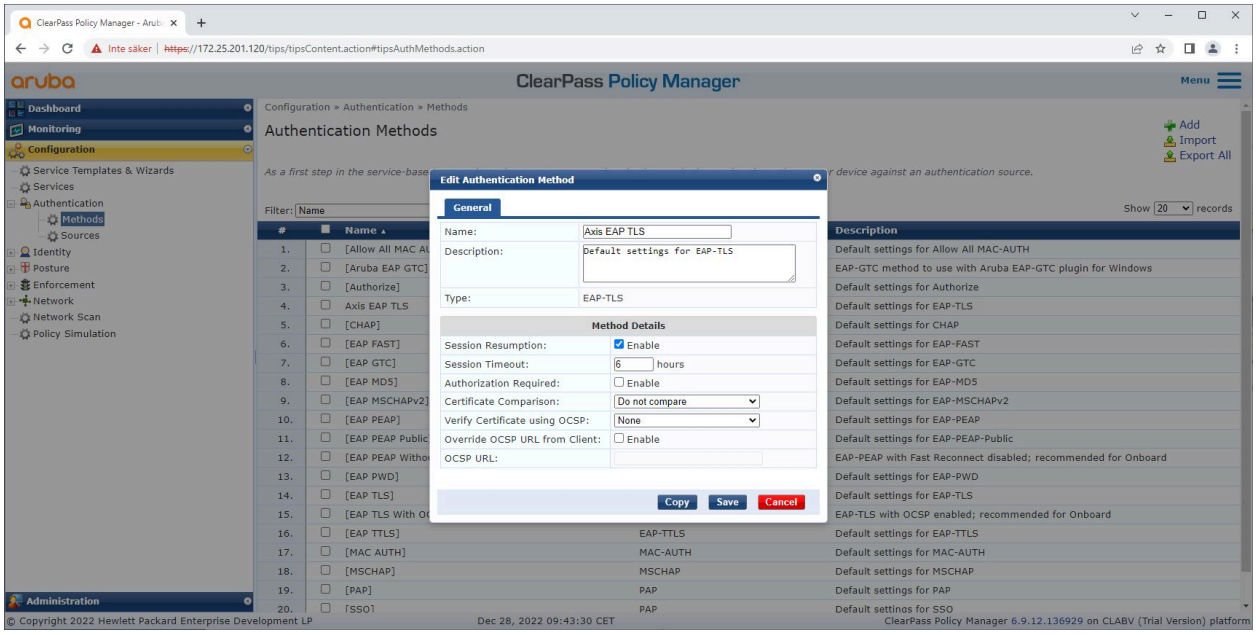
運用ネットワーク (VLAN 202)

Axis装置には、Axis装置が動作する運用環境ネットワークへのアクセス権が与えられます。アクセスは、プロビジョニングネットワーク (VLAN 201) 内から装置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:

- 装置の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Axis MACアドレススキームと一致すること。
- Axis装置のAXIS OSバージョン。
- 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

認証方式では、Axis装置がネットワークに対して認証を試行する方法が定義されます。Axis Edge Vaultをサポートするaxis装置では、デフォルトでIEEE 802.1X EAP-TLSが有効になっています。したがって望ましい認証方式は、IEEE 802.1X EAP-TLSです。

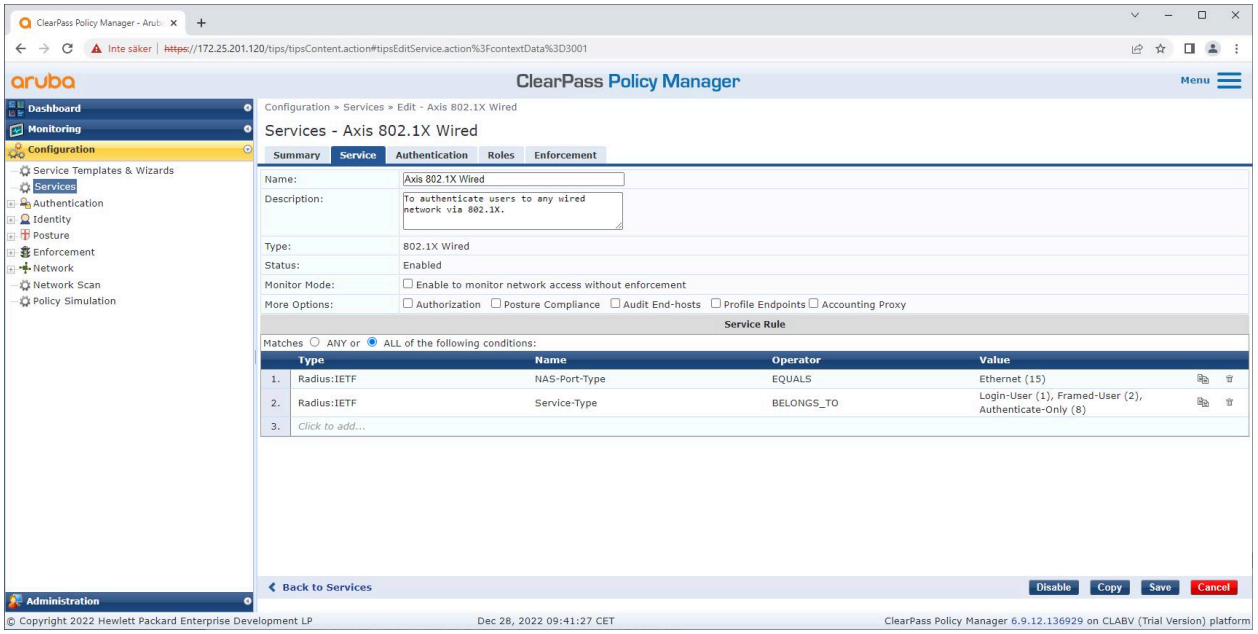


Axis装置のEAP-TLS認証方式が定義されているClearPass Policy Managerの認証方式インターフェース。

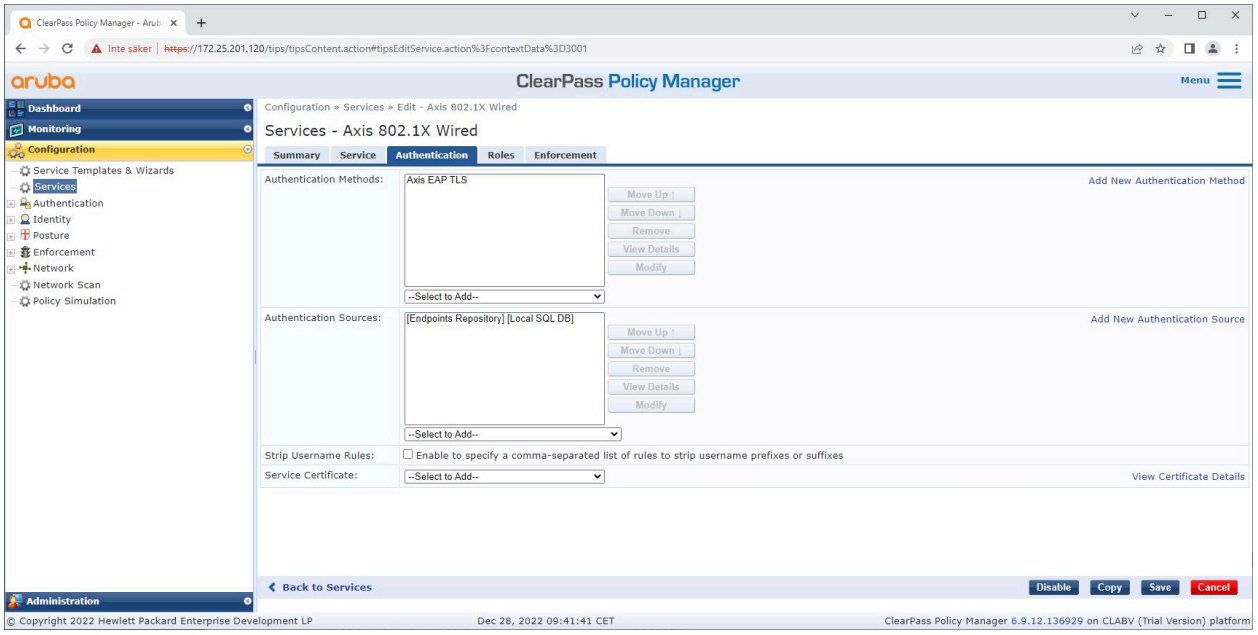
安全なオンボーディング - IEEE 802.1AR/802.1X

サービスの設定

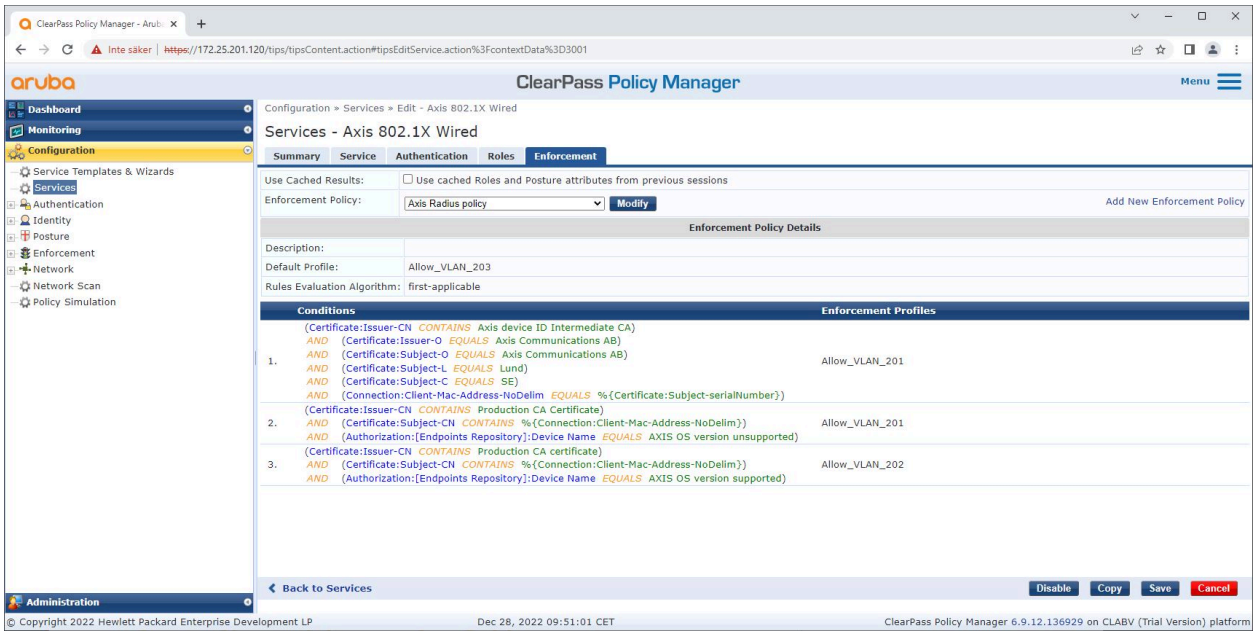
[**Services (サービス)**] ページでは、設定手順が1つのサービスに統合され、HPE Aruba Networking基盤のネットワーク内のAxis装置の認証と承認が処理されます。



専用のAxisサービスが作成され、IEEE 802.1Xが接続方式として定義されます。



次の手順では、前出の手順で作成したEAP-TLS認証方式をサービスに設定します。



最後の手順では、前出の手順で作成した適用ポリシーをサービスに設定します。

HPE Aruba Networkingアクセススイッチ

Axis装置は、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で稼動するネットワークにAxis装置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通信用に構成する必要があります。Axis装置は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秒の定期的なAxis装置の再認証も構成されます。

HPE Aruba Networkingアクセススイッチのグローバルおよびポート設定について、以下の事例を参照してください。

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

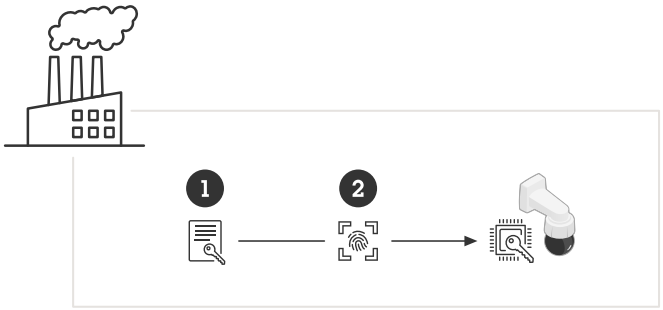
Axisの設定

Axisネットワーク装置

*Axis Edge Vault*をサポートするAxis装置は、Axisデバイスと呼ばれる安全なデバイスIDを製造時に付与されています。Axisデバイスは、IEEE 802.1X経由の自動化された安全な装置識別とネットワークオンボーディング手法の規格、国際IEEE 802.1AR標準に基づいています。

HPE Aruba Networking

安全なオンボーディング - IEEE 802.1AR/802.1X



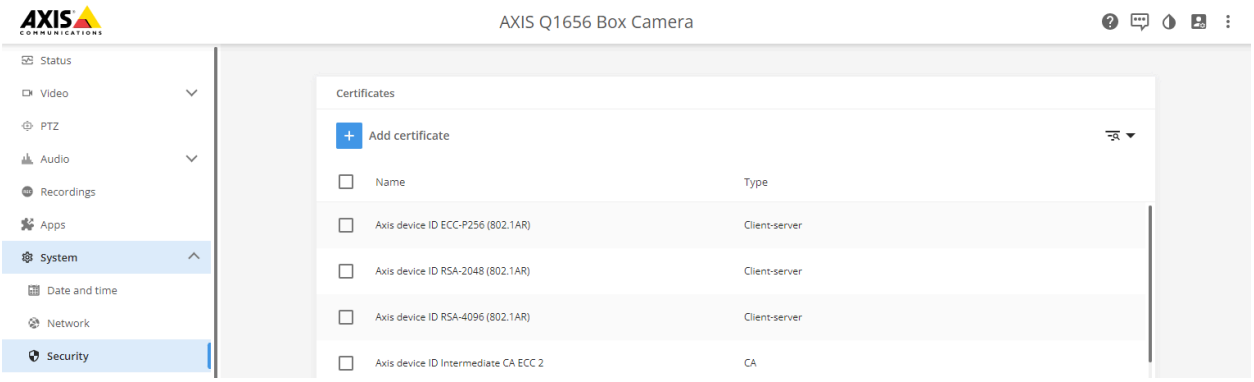
信頼できるデバイスIDサービス提供のため、Axis装置はIEEE 802.1AR準拠のAxisデバイスID証明書を製造時に付与されている

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

Axis装置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装置の信頼性をグローバルに証明する装置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をサポートする対象のAxis装置については、*Axis Product Selector*を使用して確認できます。

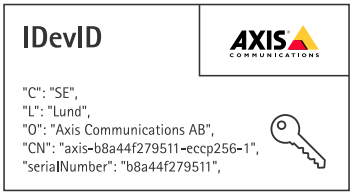
注

Axis装置のシリアル番号は、装置のMACアドレスです。



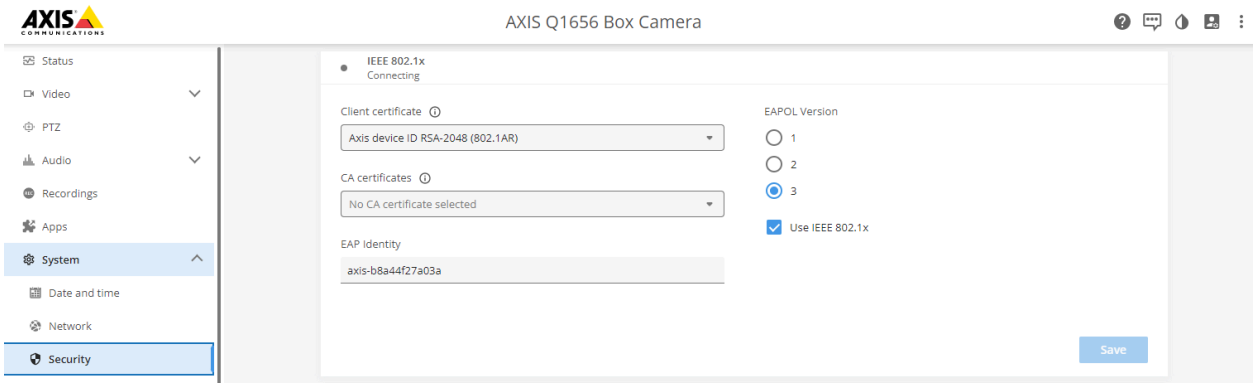
工場出荷時設定のAxis装置に搭載された証明書ストアと、Axisデバイス ID。

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、Axis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。Axisデバイス ID証明書から取得可能な以下の情報を参照してください



Country (国名)	SE
位置	Lund
Issuer Organization (発行者組織)	Axis Communications AB
Issuer Common Name (発行者の通称)	Axis device ID intermediate
Organization (AxisデバイスID中間組織)	Axis Communications AB
Common Name (通称)	axis-b8a44f279511-eccp256-1
Serial Number (シリアル番号)	b8a44f279511

通称は、Axisの会社名、装置のシリアル番号、使用される暗号化アルゴリズム (ECC P256、RSA 2048、RSA 4096) の順に組み合わせ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、Axis装置は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装置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て、コスト効率に優れた方法で複数のAxis装置を構成および管理できます。AXIS Device Managerは、ネットワーク内のマシンにローカルにインストールできるMicrosoft Windows®ベースのアプリケーションです。一方、AXIS Device Manager Extendは、クラウドインフラストラクチャーを利用してマルチサイトの装置管理を行います。いずれもAxis装置を手軽に管理、構成する機能を搭載しています。具体的には、次の機能が含まれます。

- AXIS OS更新のインストール。
- HTTPSおよびIEEE 802.1X証明書ほか、サイバーセキュリティ構成の適用。
- 画像設定など、装置固有の設定の構成。

安全なネットワーク運用 - IEEE 802.1AE MACsec

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。

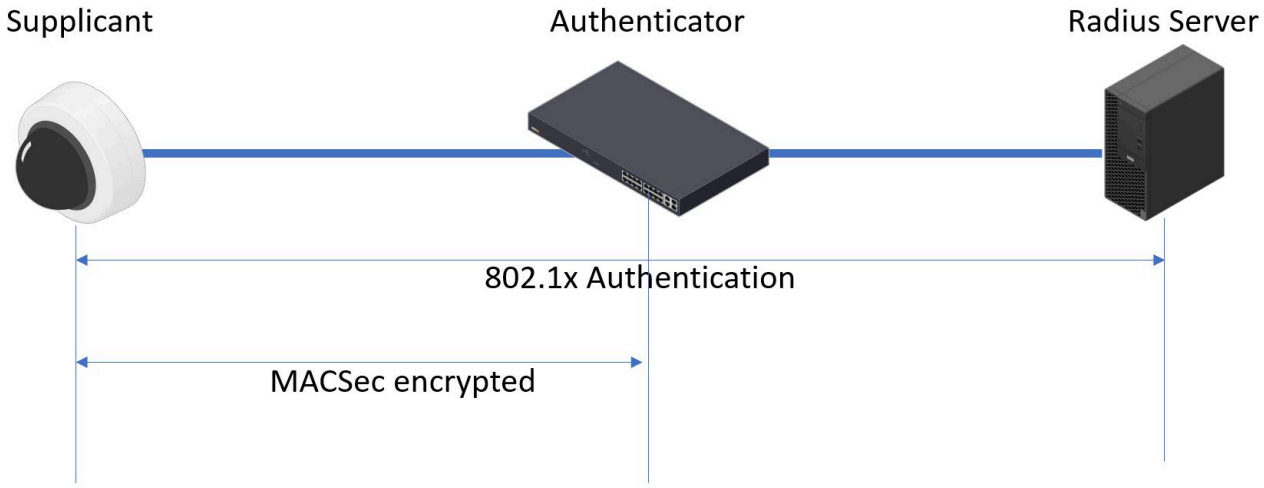
help.axis.com/?&piald=&section=secure-network-operation-ieee-802-1ae-macsec

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デバイス ID対応の装置向けに、デフォルトでIEEE 802.1Xが有効化されています。AXIS OS 11.8 以降ではMACsecがサポートされ、IEEE 802.1X EAP-TLSを使用するAutomatic Dynamicモードがデフォルトで有効化されています。工場出荷時の設定値でAxis装置を接続すると、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

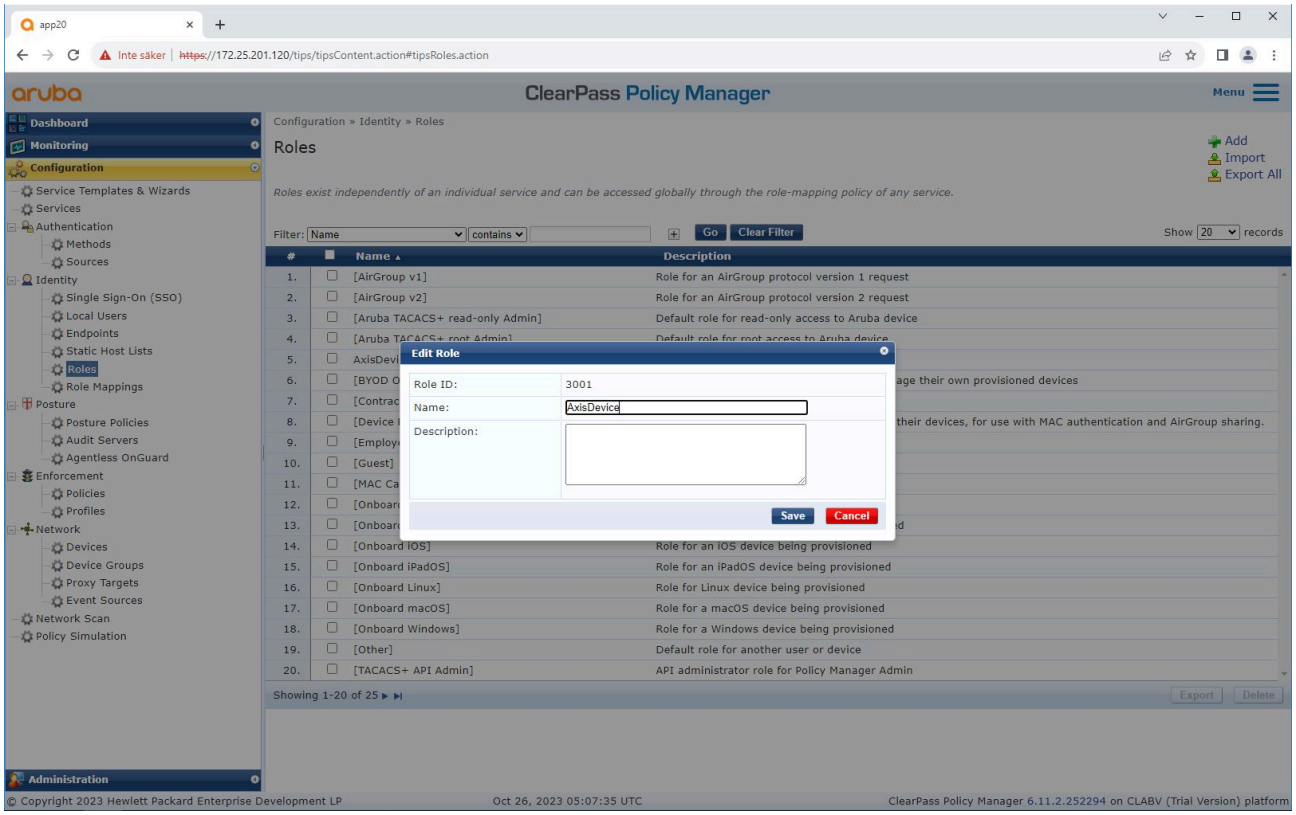
EAP-TLSセッションを通じてMACsecキーが自動的に交換され、安全なリンク (3) が設定されるほか、Axis装置からHPE Aruba Networkingアクセススイッチまでのすべてのネットワークトラフィックが保護されます。

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。

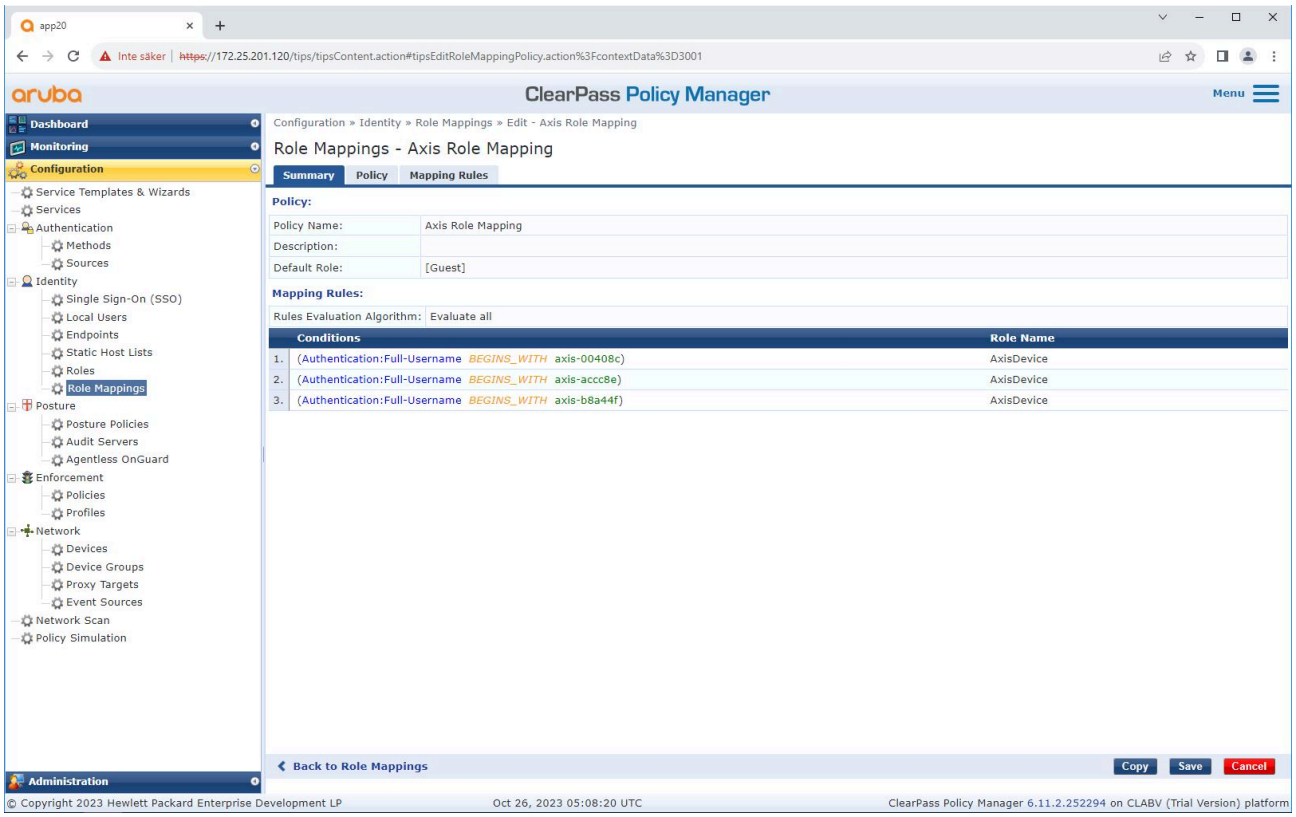
HPE Aruba NetworkingアクセススイッチがMACsecによるEAP-TLSの使用をサポートしていない場合は、Pre-Shared Keyモードを使用して手動で構成できます。

HPE Aruba Networking ClearPass Policy Manager

ロールとロールマッピングポリシー



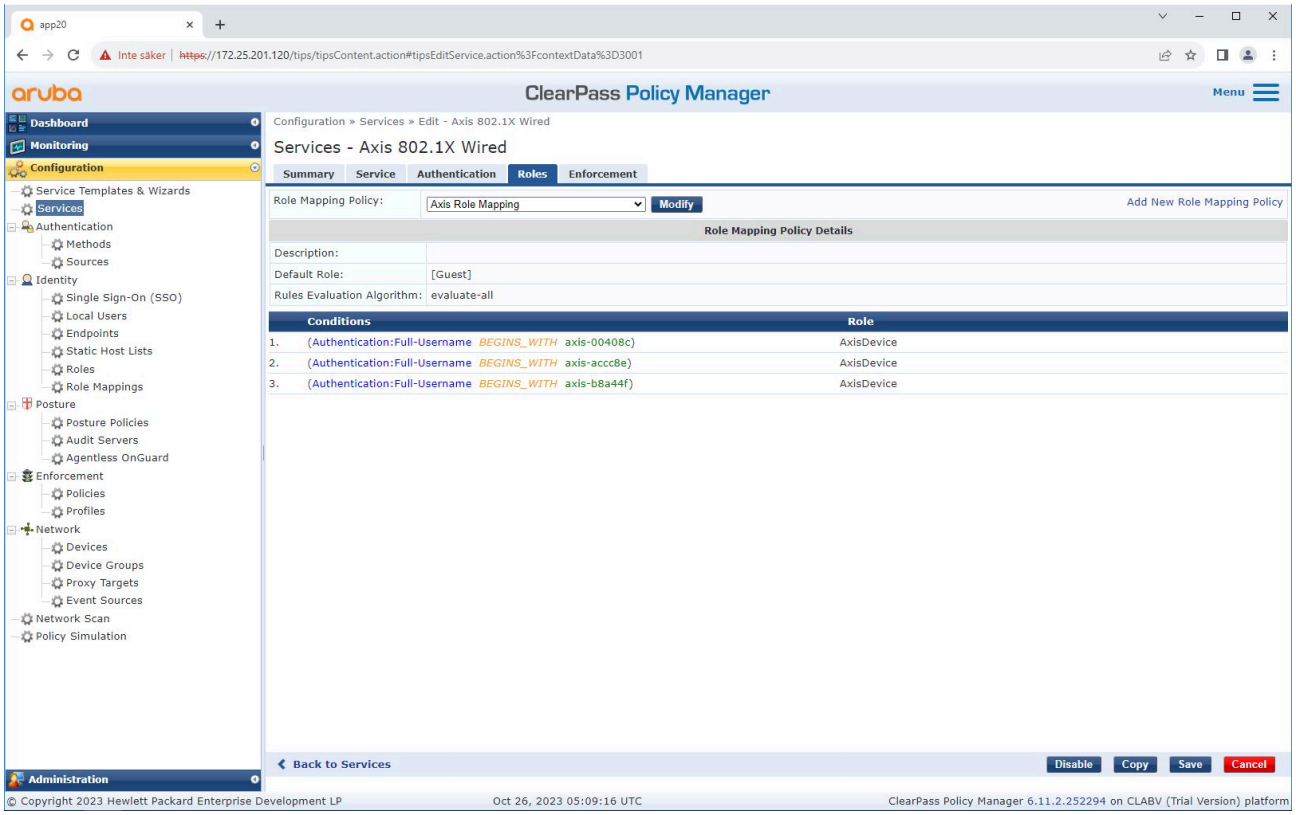
Axis装置の役割名を追加します。この名前は、アクセススイッチ構成のポートアクセス役割名です。



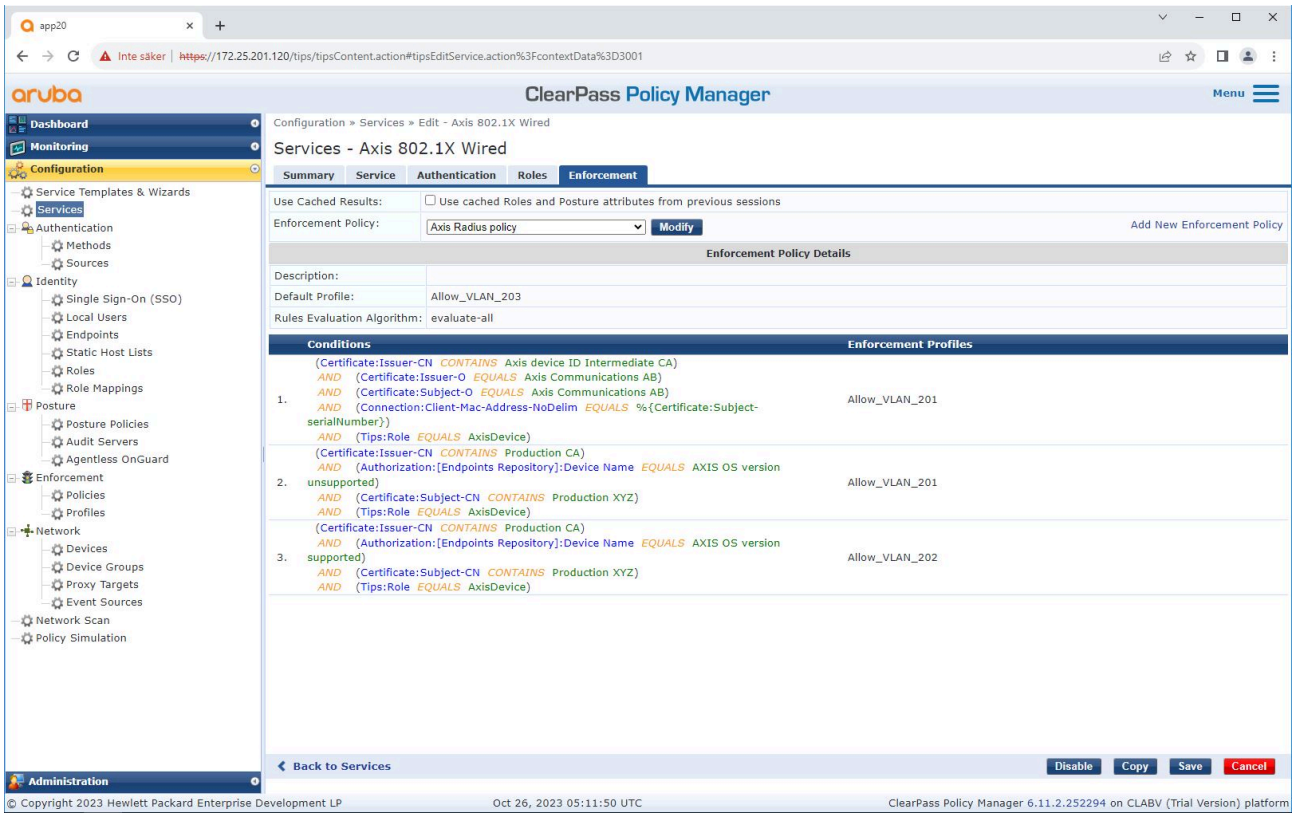
前出の手順で作成したAxis装置の役割向けに、Axis役割マッピングポリシーを追加します。この条件定義は、装置をAxis装置ロールにマッピングするために必要です。条件が満たされない場合、装置は [Guest (ゲスト)] 役割の一部になります。

デフォルトでは、Axis装置はEAP ID形式「axis-serialnumber」を使用します。Axis装置のシリアル番号は、装置の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

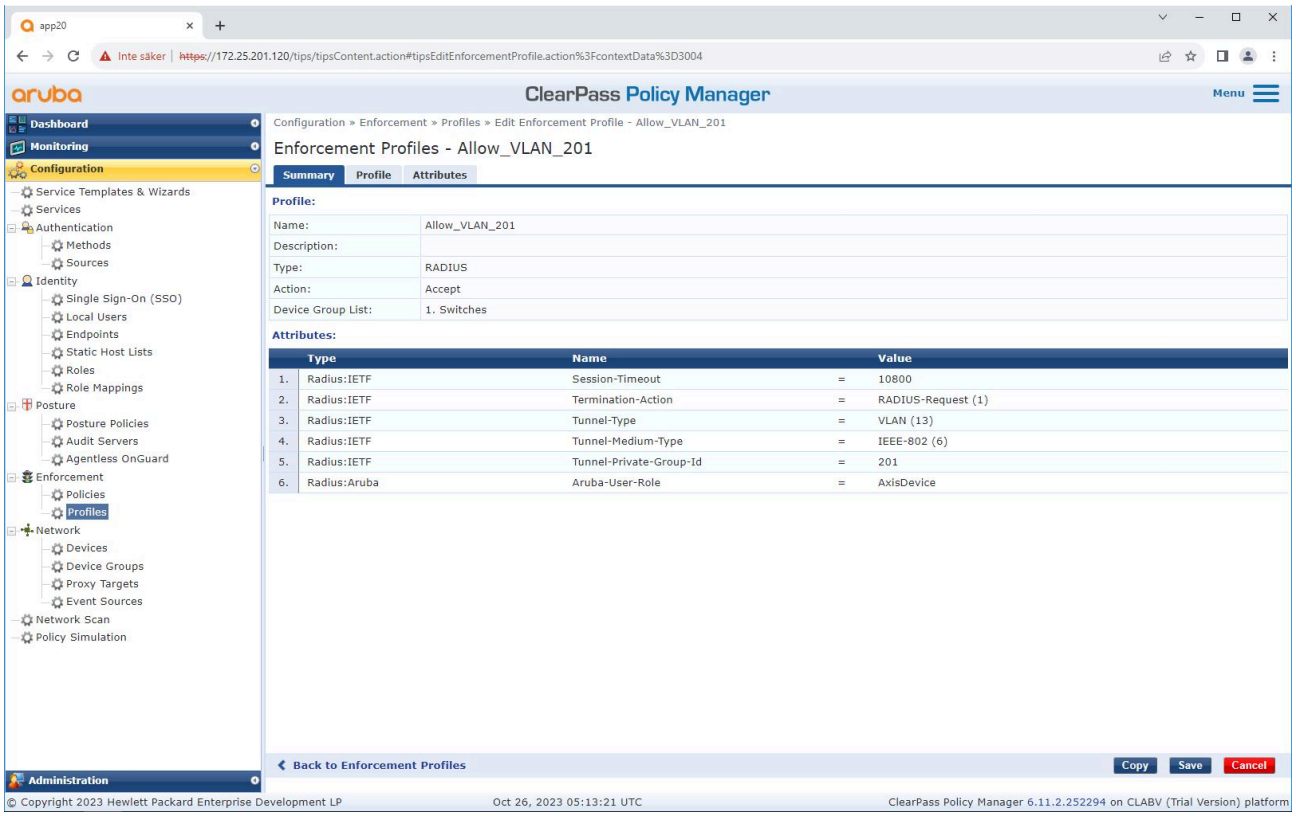


Axis装置のオンボーディングの接続方式としてIEEE 802.1Xを定義するサービスに、前出の手順でに作成したAxisロールマッピングポリシーを追加します。



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役割名を属性として追加します。

HPE Aruba Networkingアクセススイッチ

に記載された安全なオンボーディング構成に加えて、以下の HPE Aruba Networkingアクセススイッチのポート構成例を参照して、IEEE 802.1AE MACsecを設定してください。

```
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
```

レガシーオンボーディング - MAC認証

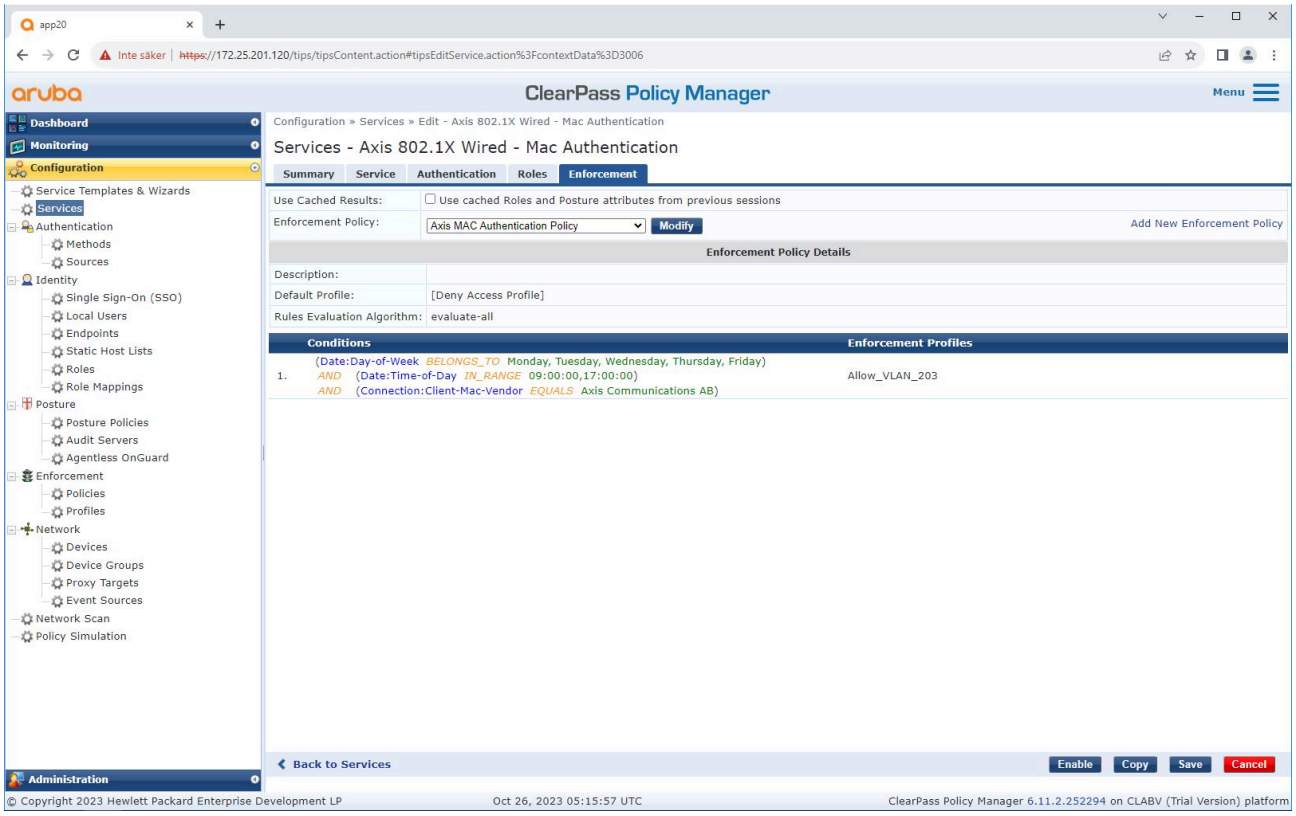
MAC Authentication Bypass (MAB) とAxisデバイスID証明書、工場出荷時の設定で有効化されているIEEE 802.1Xを使用して、IEEE 802.1ARをサポートしないAxis装置をオンボーディングすることができます。802.1Xオンボーディングが失敗した場合、ClearPass Policy ManagerはAxis装置のMACアドレスを検証し、ネットワークへのアクセスを付与します。

MABには、アクススイッチとClearPass Policy Manager構成の両方の準備が必要です。Axis装置には、MABのオンボーディングを許可するための構成は必要ありません。

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装置が設定された強制ポリシーを満たさない場合、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。

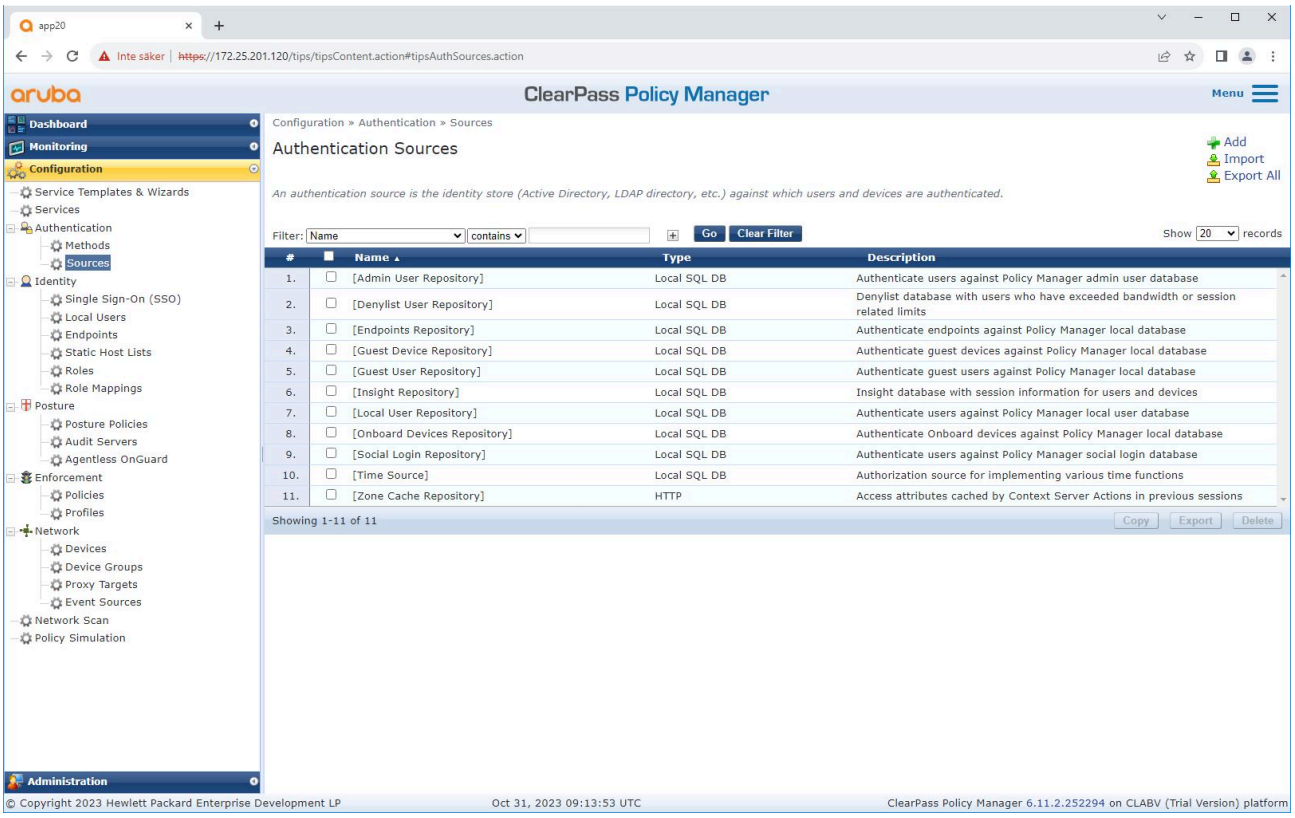
- 月曜日から金曜日までの平日である

- 9:00～17:00の間である
- MACアドレスのベンダーはAxis Communicationsと一致する

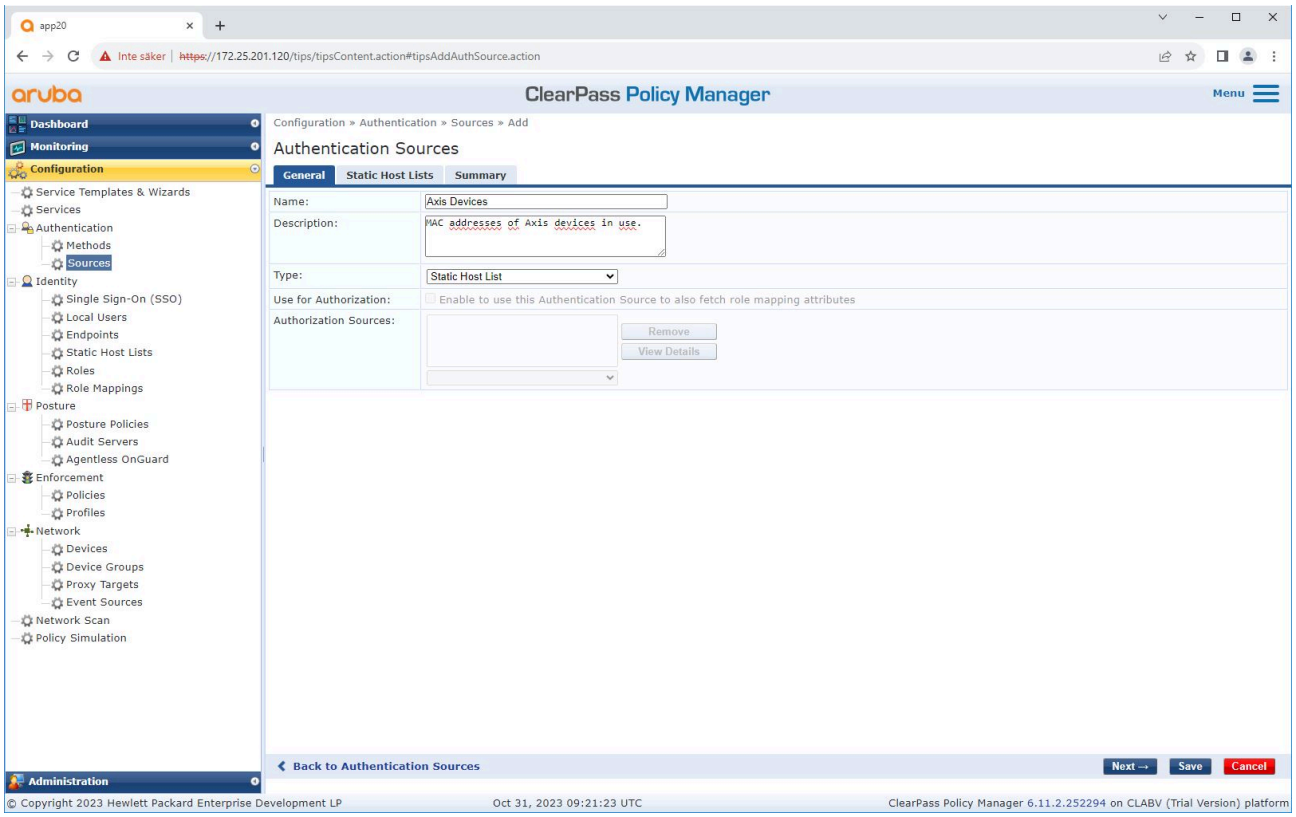
MACアドレスはスプーフィングされる可能性があるため、通常のプロビジョニングネットワークへのアクセスは付与されません。MABは初回オンボーディングにのみ使用し、装置をさらに手動で検査することをお勧めします。

ソースの設定

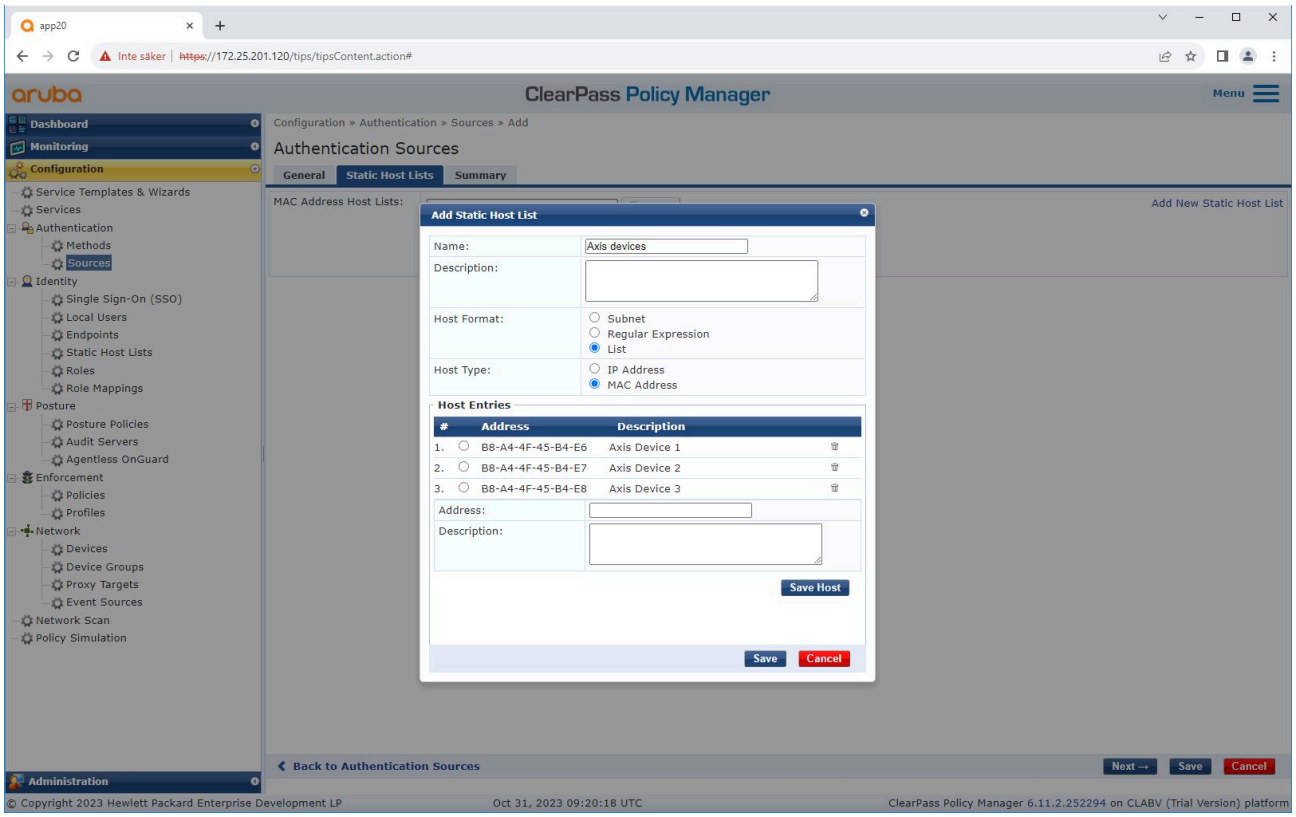
[Sources (ソース)] ページでは新しい認証ソースが作成され、手動でインポートされたMACアドレスのみを許可します。



レガシーオンボーディング - MAC認証

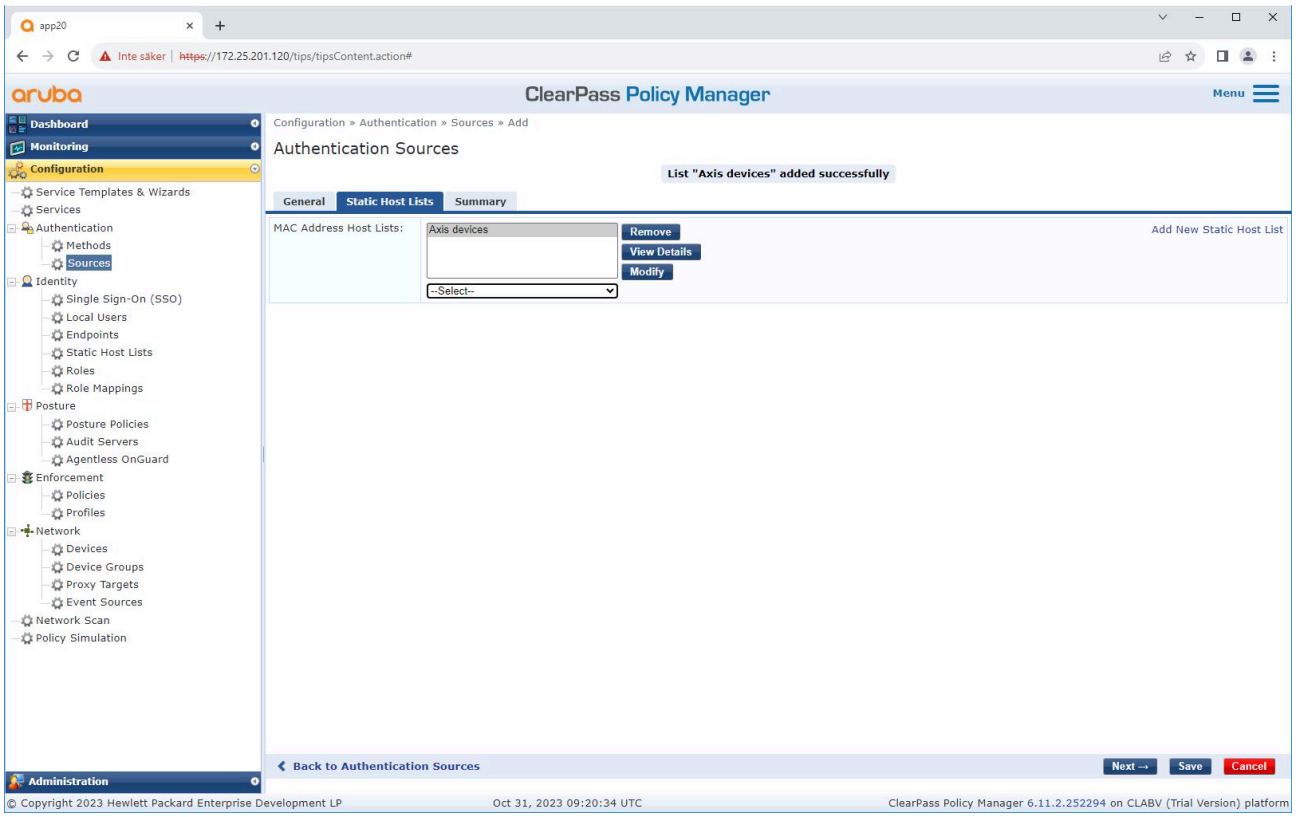


レガシーオンボーディング - MAC認証



Axis MACアドレスを含む静的ホストリストが作成されます。

レガシーオンボーディング - MAC認証

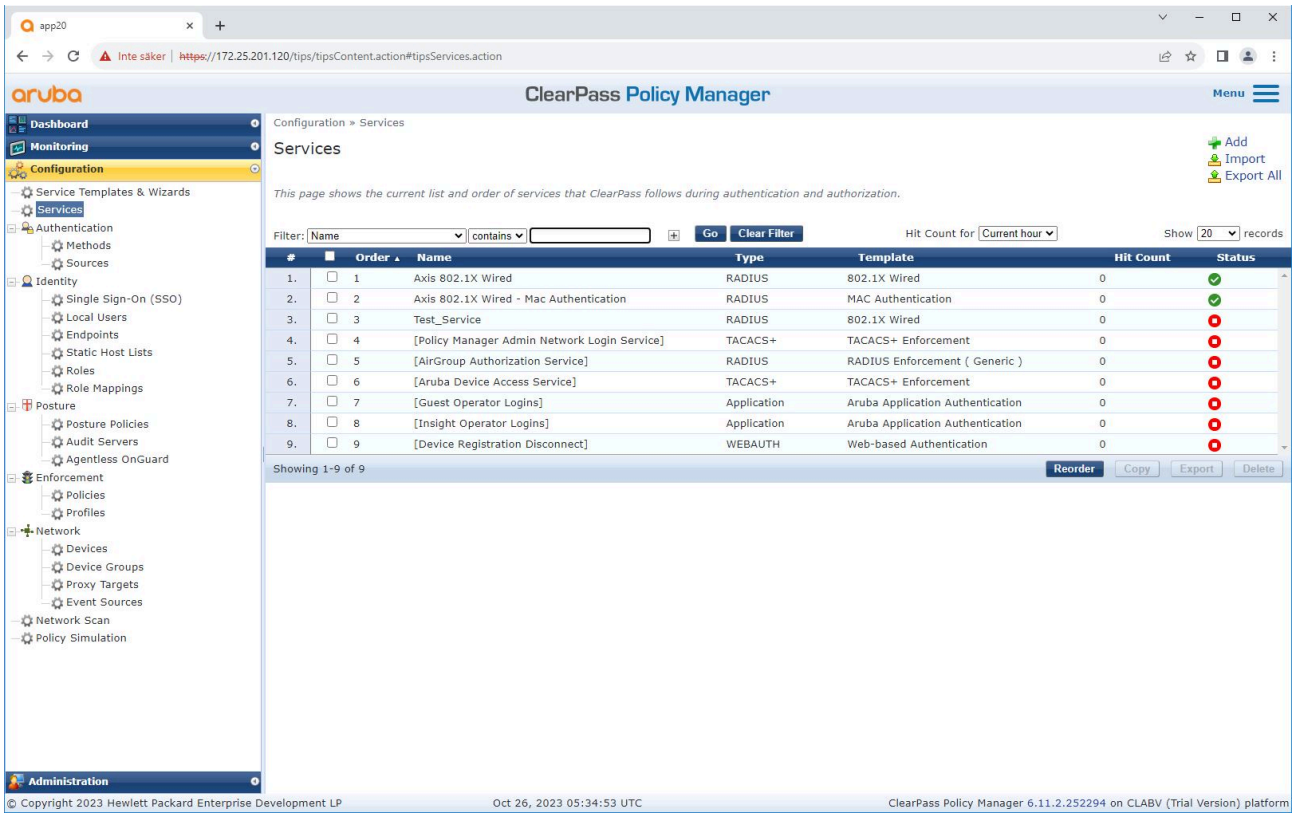


サービスの設定

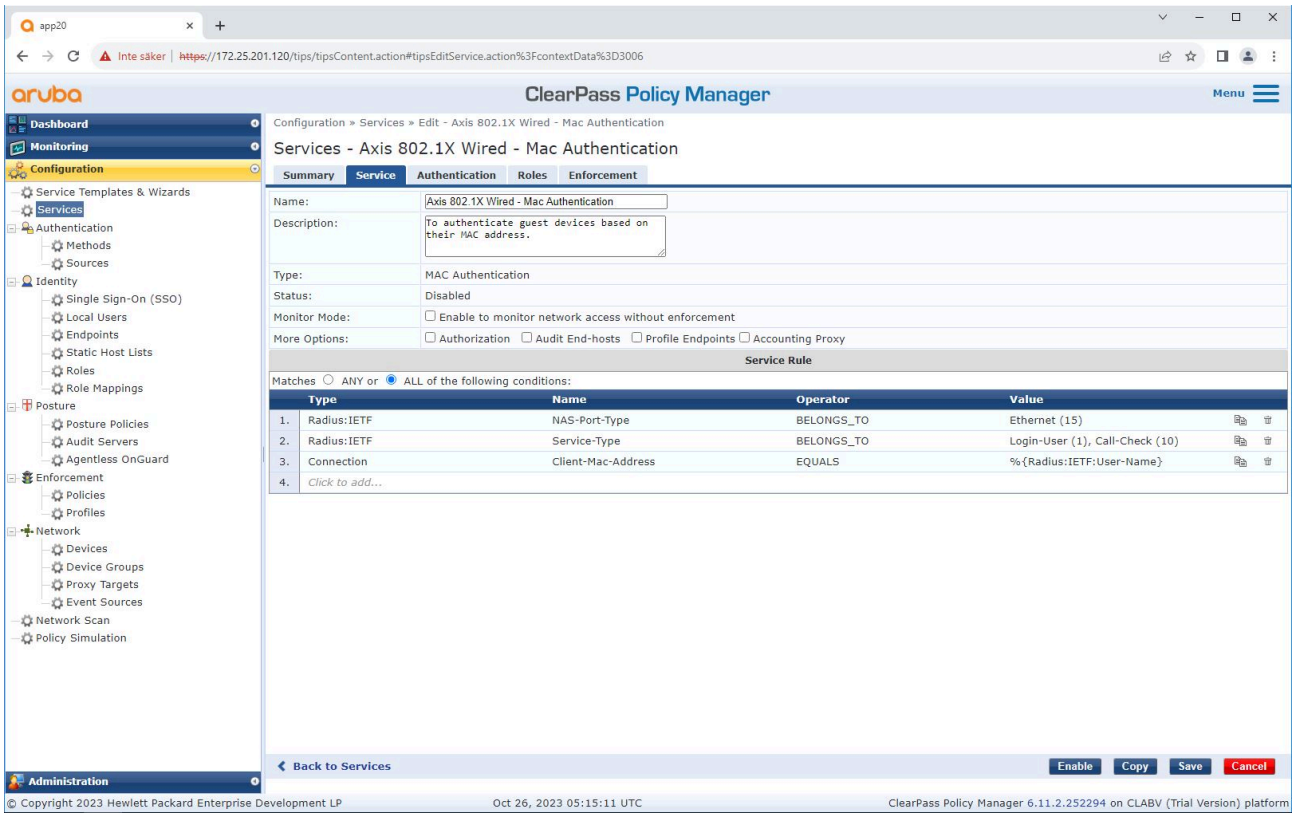
[**Services (サービス)**] ページでは、設定手順が1つのサービスに統合され、HPE Aruba Networking基盤のネットワーク内のAxis装置の認証と承認が処理されます。

HPE Aruba Networking

レガシーオンボーディング - MAC認証

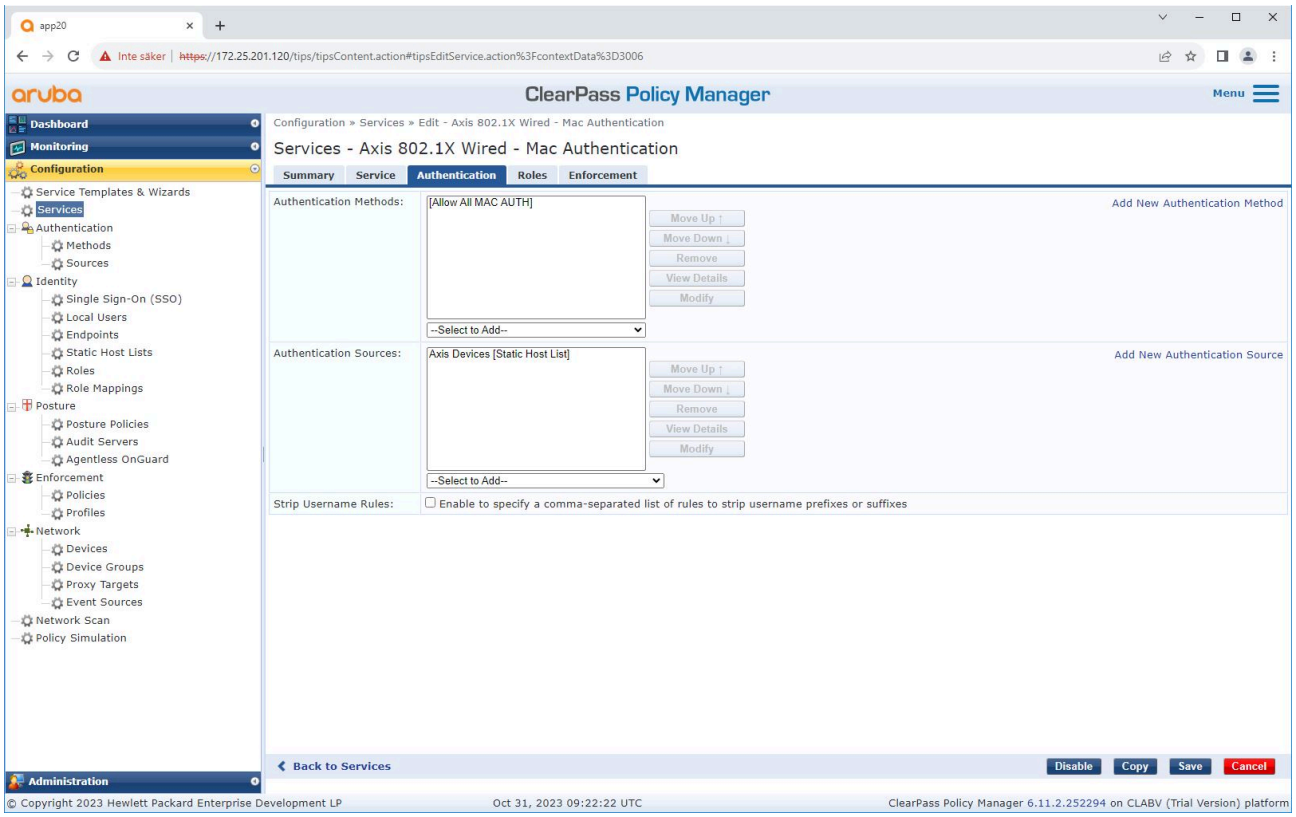


レガシーオンボーディング - MAC認証



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。

レガシーオンボーディング - MAC認証

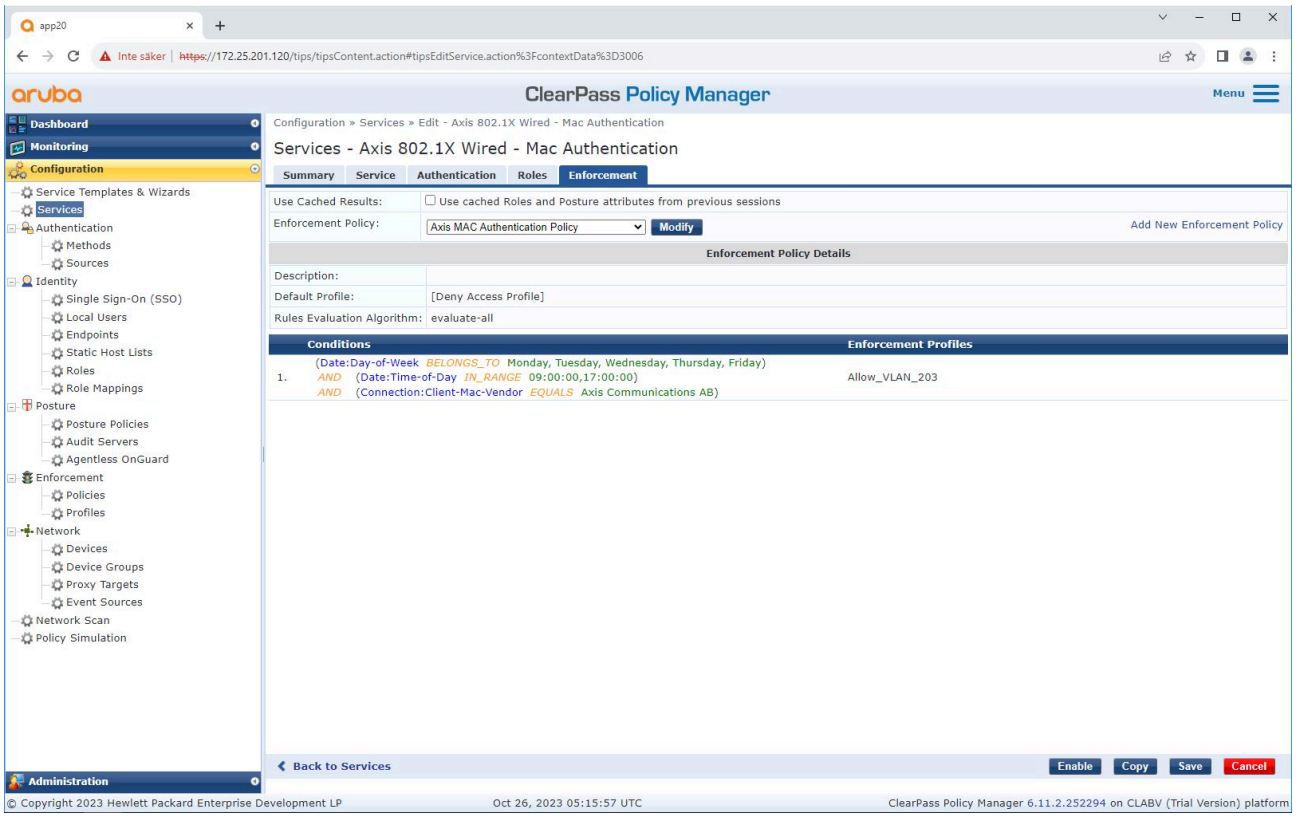


事前設定されたMAC認証方式がサービスに設定されます。またAxis MACアドレスのリストを含む、前出の手順で作成した認証ソースが選択されます。

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

レガシーオンボーディング - MAC認証



最後の手順では、前出の手順で作成した適用ポリシーをサービスに設定します。

HPE Aruba Networkingアクセススイッチ

に記載されている安全なオンボーディング構成に加えて、MABを許可するHPE Aruba Networkingアクセススイッチについて、以下のポート構成例を参照してください。

```
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
```

移行ガイド
HPE Aruba Networking

バージョン M6.2
日付: 2024年5月
製品番号 T10197992