Secure integration of Axis devices into Aruba networks

ユーザーマニュアル

Secure integration of Axis devices into Aruba networks

目次

Secure integration of Axis devices into Aruba networks

はじめに

はじめに

ArubaネットワークへのAxis装置のオンボーディング手順、および、ArubaネットワークでAxis装置を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する統合ガイドです。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装置管理アプリケーションをArubaネットワーク機器や各種アプリケーションと組み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Arubaネットワーク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。
- Aruba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。構成を行う前に、次の領域に関する知識が不可欠です。

- ArubaアクセススイッチとAruba ClearPass Policy Managerを含むAruba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方法。
- 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る。

Secure integration of Axis devices into Aruba networks

安全なオンボーディング - IEEE 802.1AR/802.1X

安全なオンボーディング - IEEE 802.1AR/802.1X

初期認証

Axis Edge VaultがサポートするAxis装置をAruba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装置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、Aruba ClearPass Policy ManagerはAxis装置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ファームウェアなどの情報は、ポリシーに基づく決定に使用されます。

Axis装置はArubaネットワークに対する認証に、IEEE 802.1AR準拠のAxis装置ID証明書を使用します。

Axis装置はArubaネットワークに対する認証に、IEEE 802.1AR準拠のAxis装置ID証明書を使用します。

1 *Axis装置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ポリシー管理者*

プロビジョニング

認証後、Arubaネットワークは、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Axis装置を移行します。Axis Device Managerを使用して、装置の構成、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ポリシー管理者*
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。Aruba 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。

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

1 *Axis装置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ポリシー管理者*
4 *ビデオ管理システム*

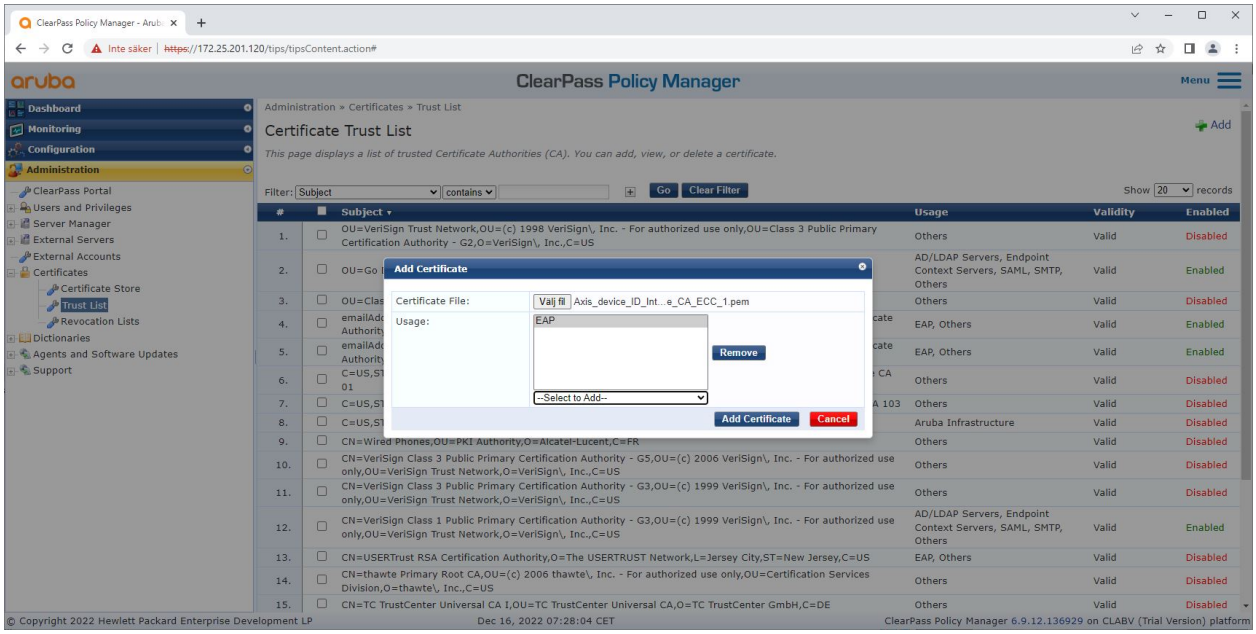
HPE Arubaの構成

Aruba ClearPass Policy Manager

ArubaのClearPass Policy Managerを使用して、マルチベンダーの有線、無線、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ロール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実施できます。

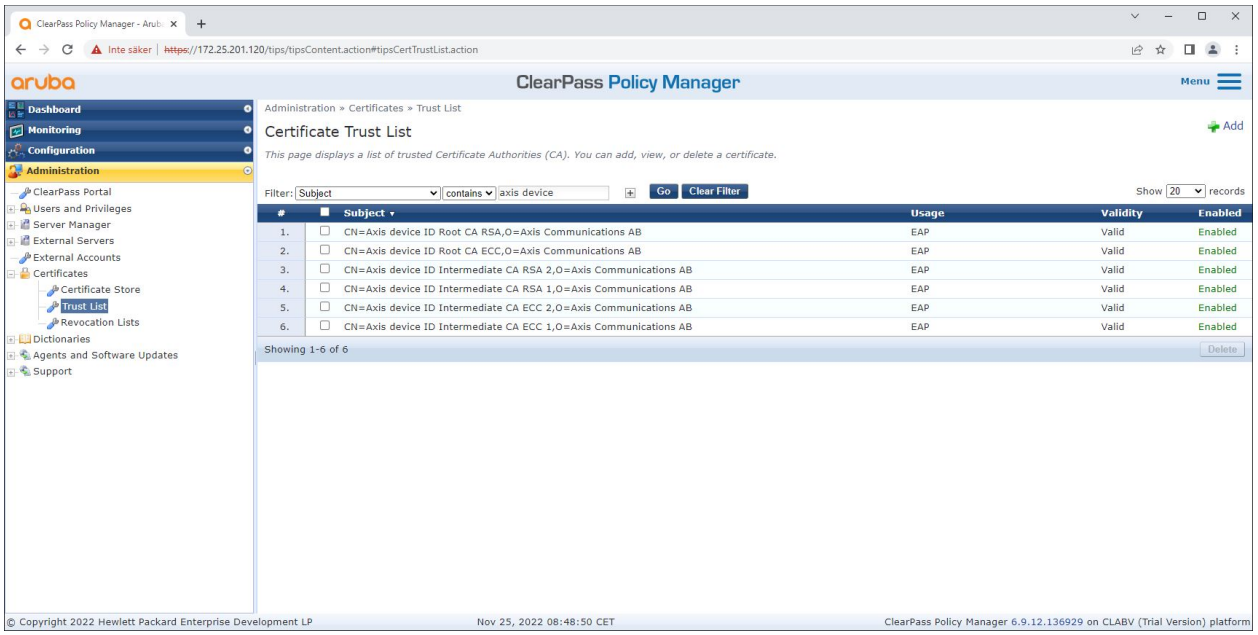
信頼できる証明書ストアの構成

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. Aruba 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。

安全なオンボーディング - IEEE 802.1AR/802.1X



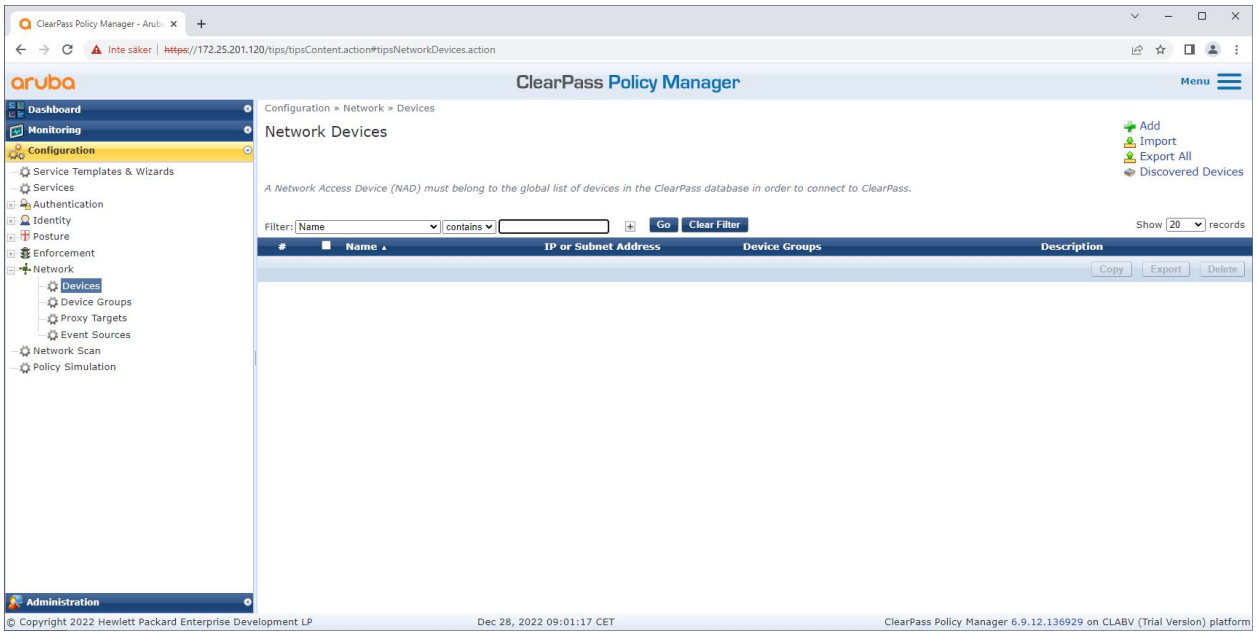
Aruba ClearPass Policy Manager内の信頼された証明書ストアに格納された、Axis固有のIEEE 802.1AR証明書チェーン。

ネットワーク装置/グループの構成

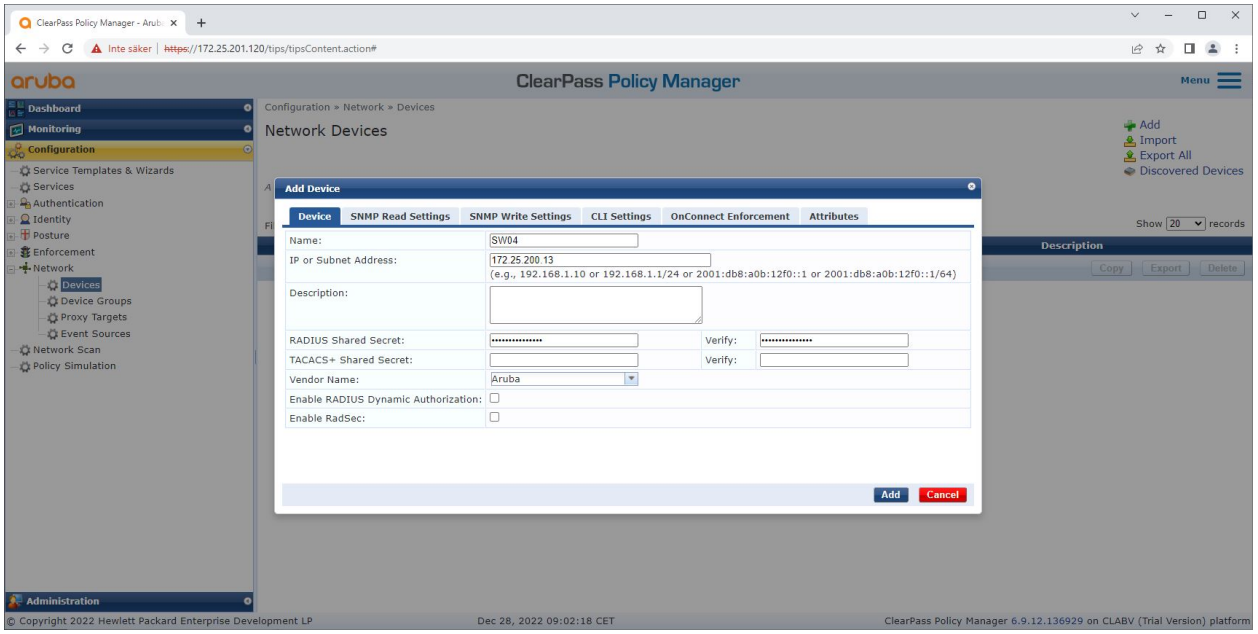
1. Arubaアクセススイッチなどの信頼できるネットワークアクセス装置をClearPass Policy Managerに追加します。ClearPass Policy Managerは、ネットワーク内でIEEE 802.1X通信に使用されるArubaアクセススイッチを把握する必要があります。
2. ネットワーク装置グループ構成を使用して、複数の信頼できるネットワークアクセス装置をグループ化します。信頼できるネットワークアクセス装置をグループ化ことで、ポリシーの構成を簡単に行うことができます。
3. RADIUS共有秘密は、特定のスイッチのIEEE 802.1X構成と一致させる必要があります。

Secure integration of Axis devices into Aruba networks

安全なオンボーディング - IEEE 802.1AR/802.1X

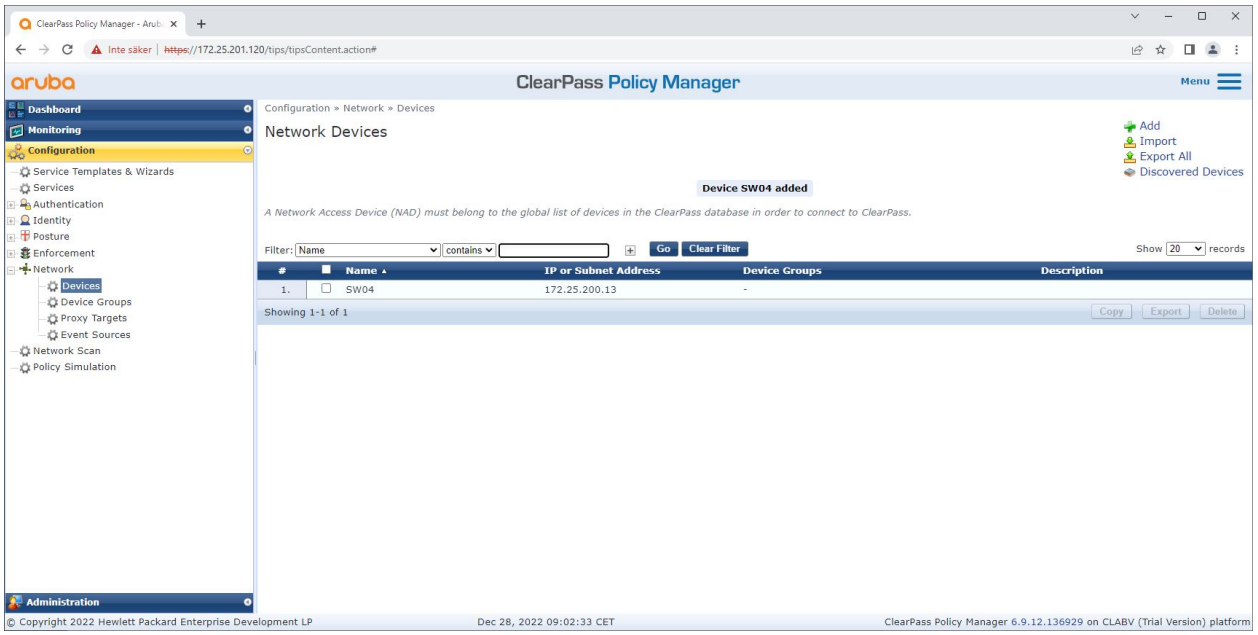


Aruba ClearPass Policy Managerの信頼されたネットワーク装置インターフェース。

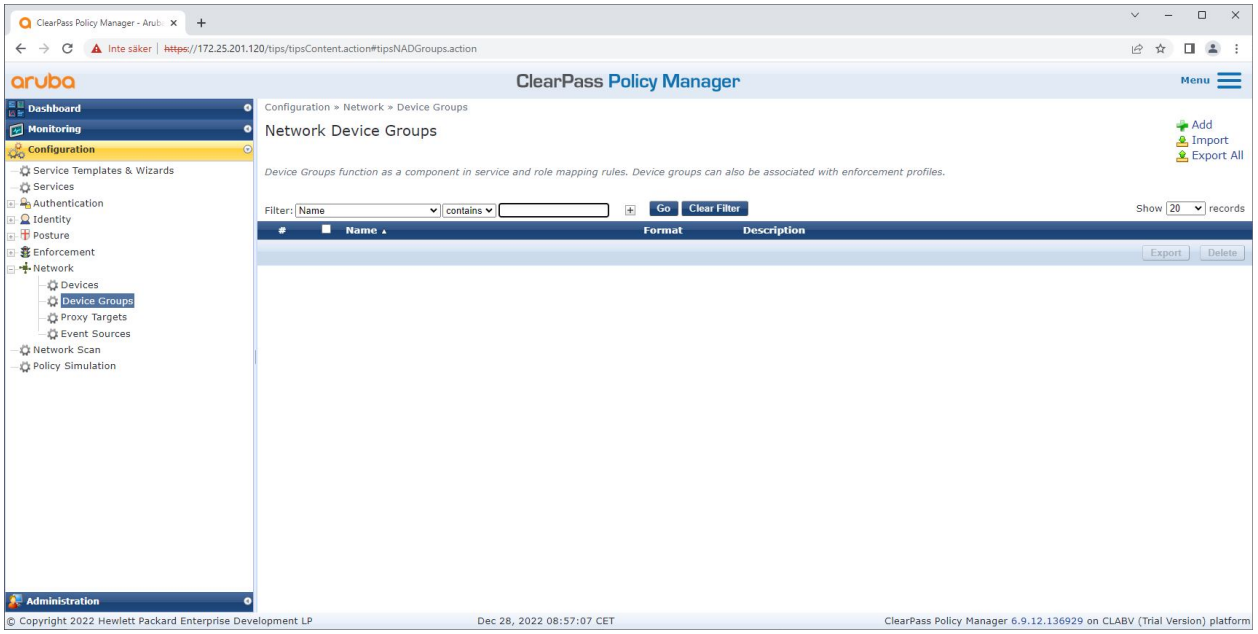


Aruba ClearPass Policy Managerに、信頼できるネットワーク装置としてArubaアクセススイッチを追加します。RADIUS共有秘密は、特定のスイッチのIEEE 802.1X構成と一致させる必要があることに注意してください。

安全なオンボーディング - IEEE 802.1AR/802.1X

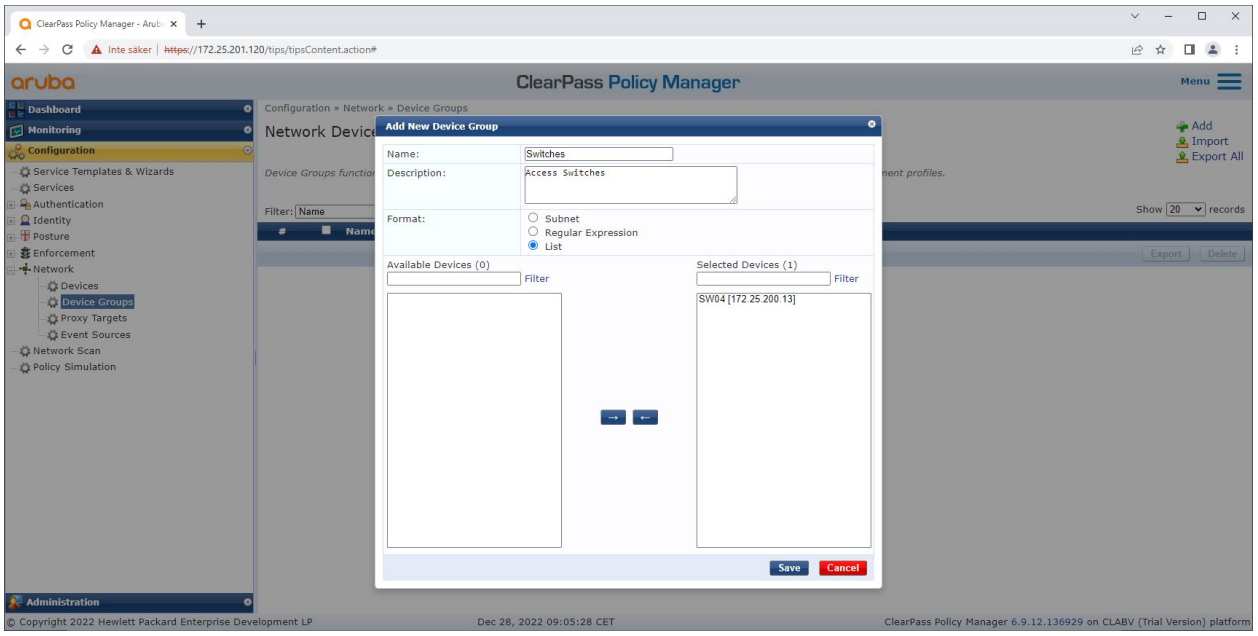


1つの信頼できるネットワーク装置が構成されたAruba ClearPass Policy Manager。

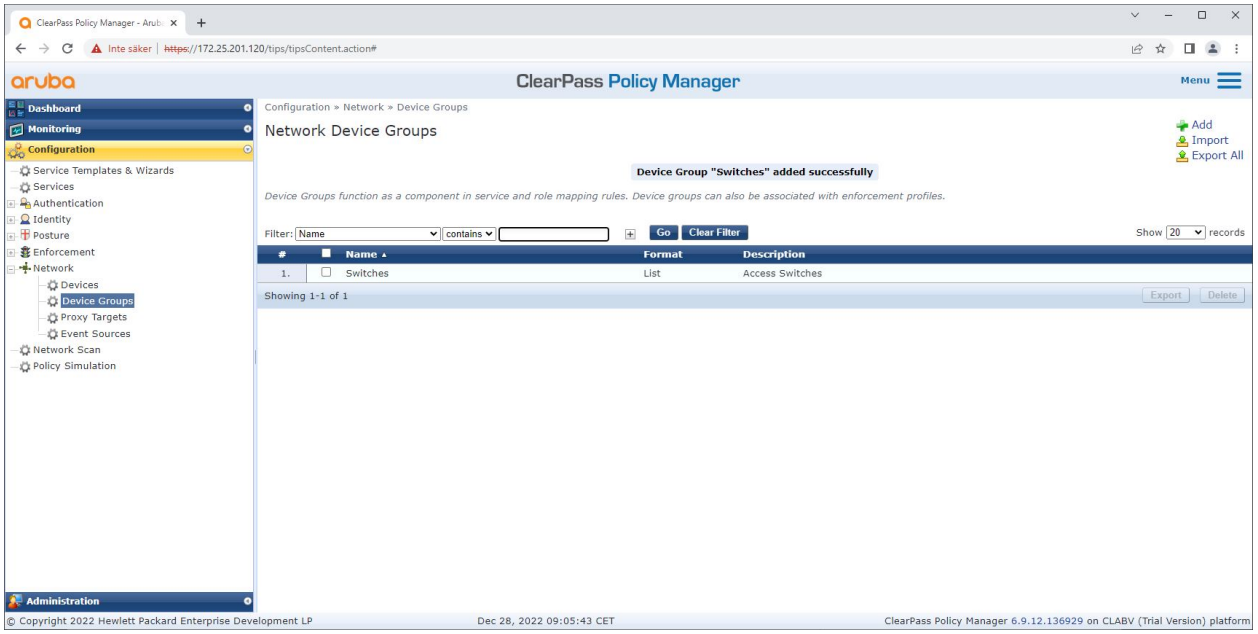


Aruba ClearPass Policy Managerの信頼されたネットワーク装置グループインターフェース。

安全なオンボーディング - IEEE 802.1AR/802.1X



Aruba 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。



Aruba 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。

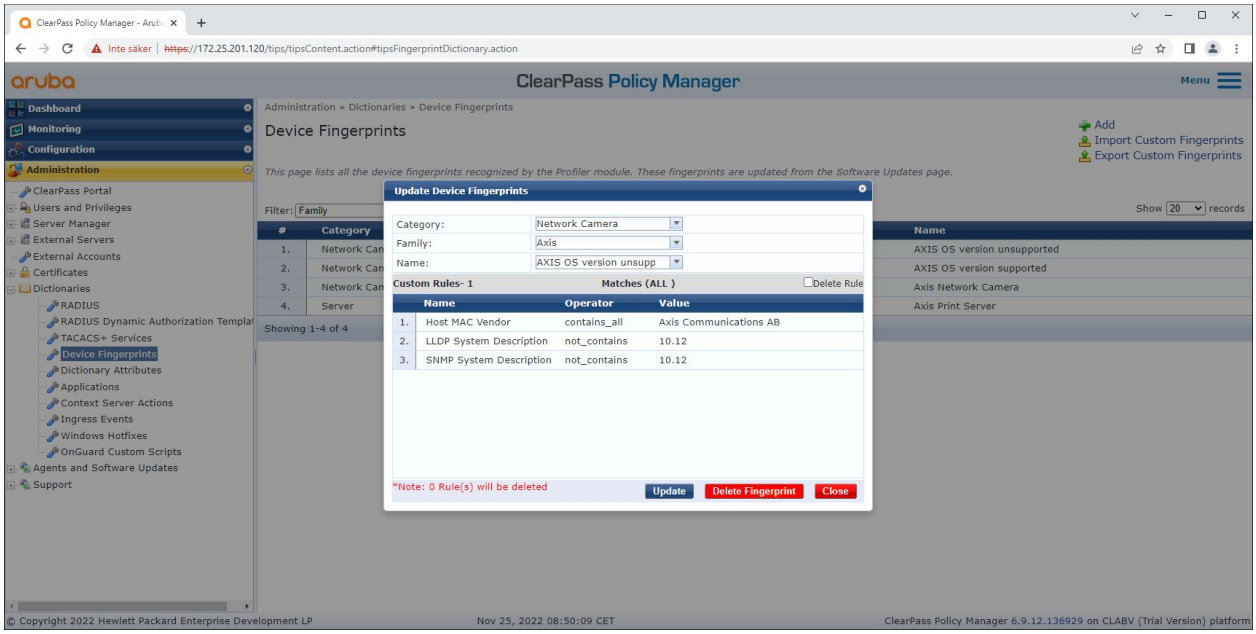
装置のフィンガープリントの構成

Axis装置は、ネットワーク検出を通じてMACアドレスやファームウェアのバージョンなど装置固有の情報を配布できます。装置のフィンガープリントは、Aruba ClearPass Policy Managerの装置のフィンガープリントインターフェースで作成できます。装置のフィンガープリントを更新および管理することができます。実行できるアクションの1つに、AXIS OSのバージョンに応じたアクセスの付与または拒否があります。

安全なオンボーディング - IEEE 802.1AR/802.1X

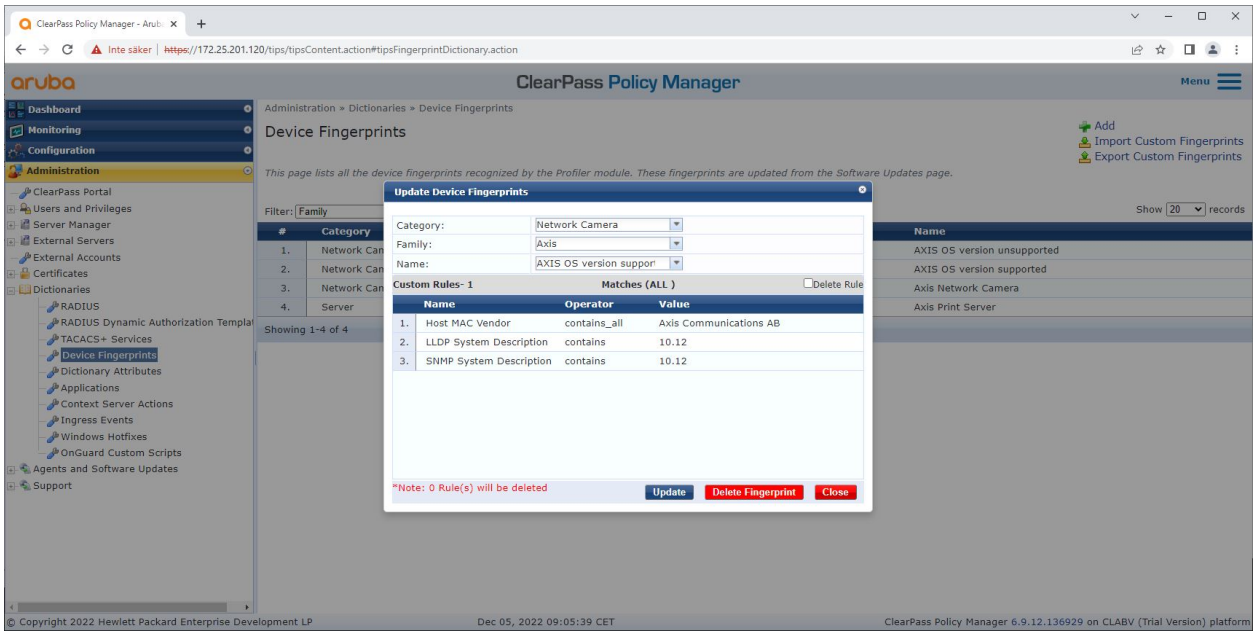
装置のフィンガープリントを更新および管理することができます。実行できるアクションの1つに、AXIS OSのバージョンに応じたアクセスの付与または拒否があります。

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. [Device Fingerprint (装置のフィンガープリント)] の設定を構成します。



Aruba ClearPass Policy Managerの装置のフィンガープリント構成。10.12以外のファームウェア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。

安全なオンボーディング - IEEE 802.1AR/802.1X



Aruba ClearPass Policy Managerの装置のフィンガープリント構成。上記の例では、ファームウェア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。

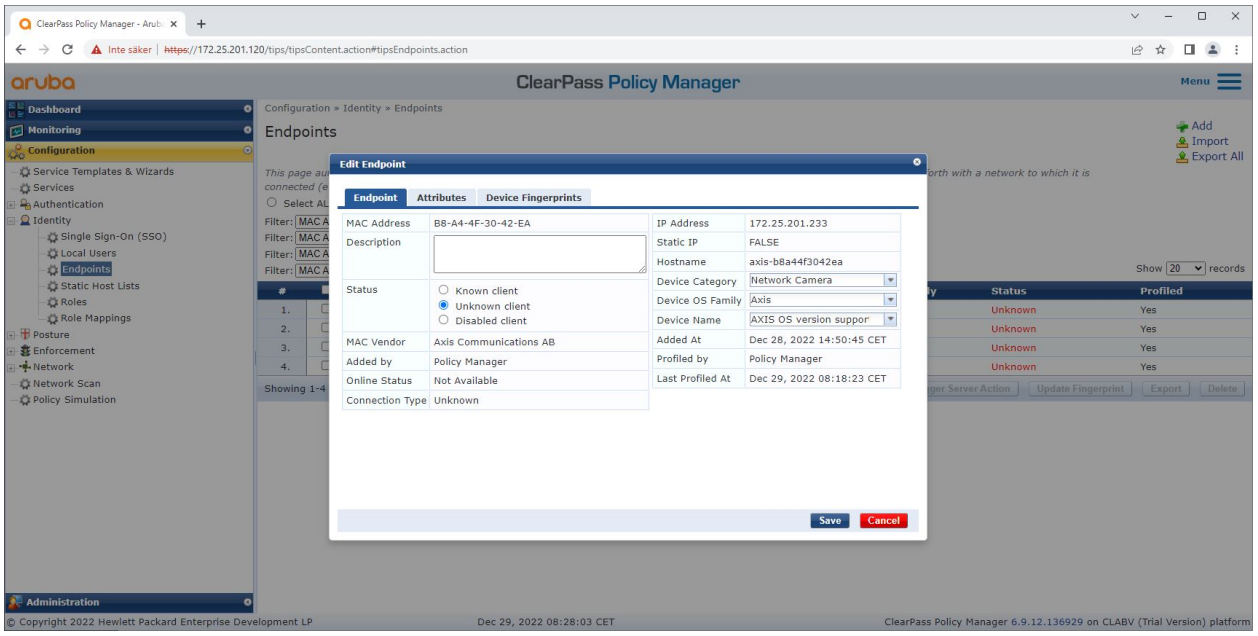
Aruba ClearPass Managerが収集した[Device Fingerprint (装置のフィンガープリント)] に関する情報は、[Endpoints (エンドポイント)] セクションにあります。

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。

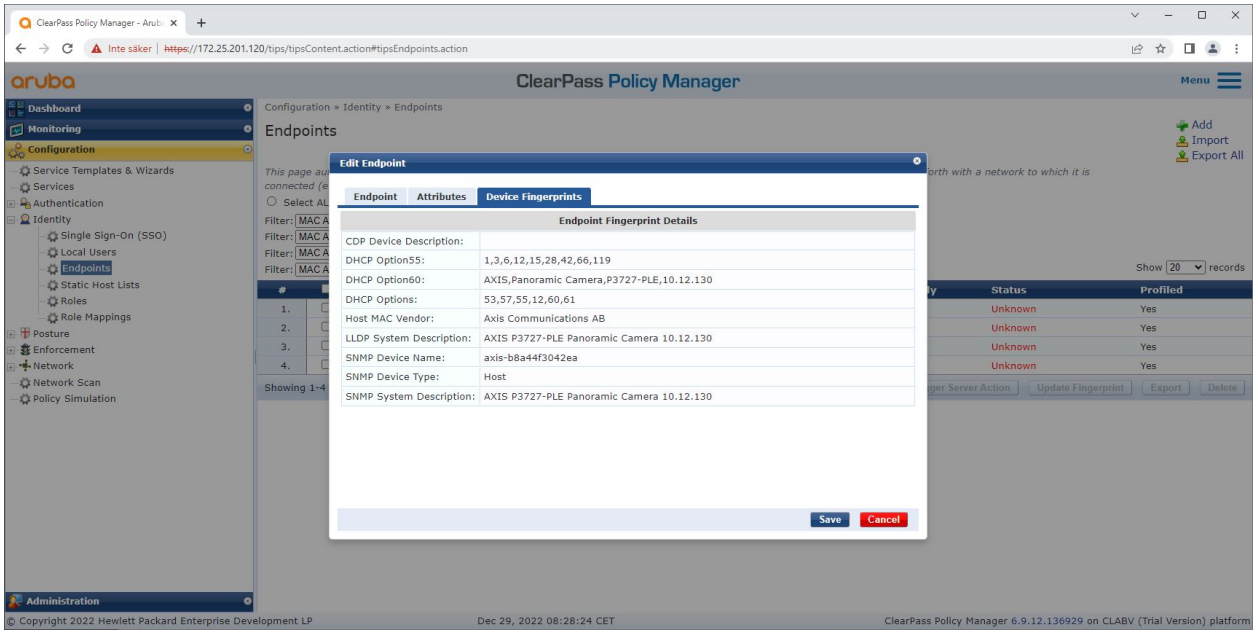
注

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

安全なオンボーディング - IEEE 802.1AR/802.1X



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



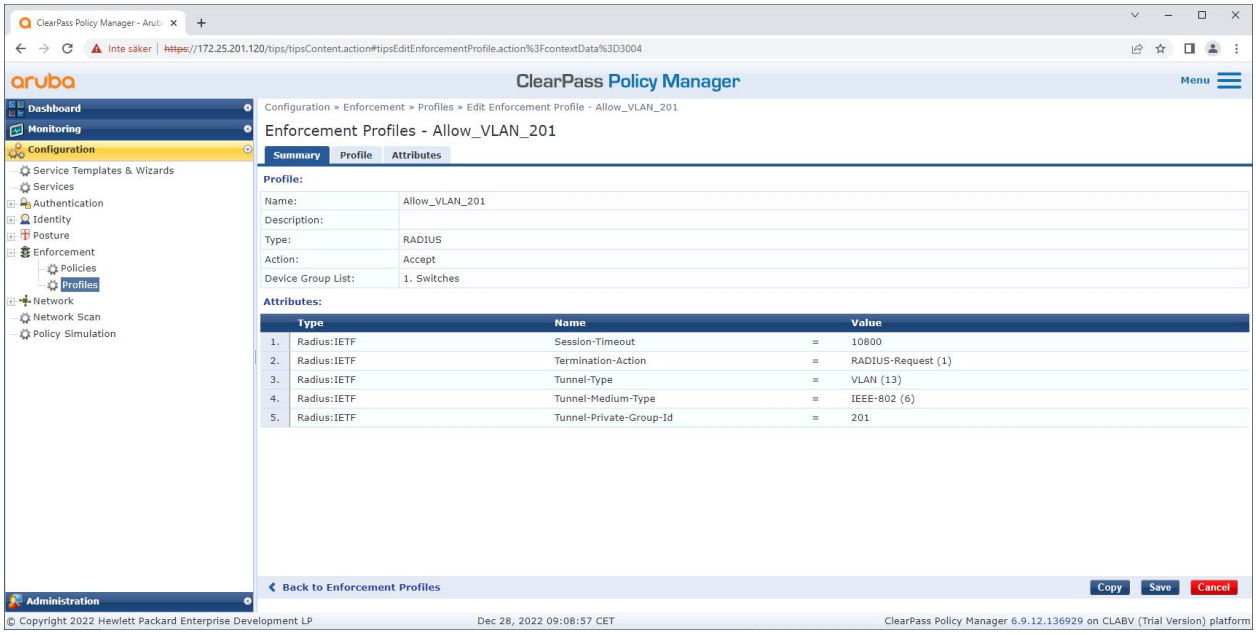
*プロファイルされた*Axis*装置の詳細な装置フィンガープリント。Axis装置ではSNMPがデフォルトで無効になっていることに注意してください。LLDP、CDP、およびDHCP固有の検出情報は、Axis装置によって工場出荷時の設定ステータスで共有され、Arubaアクセススイッチによって*ClearPass Policy Managerに中継されます。

強制プロファイルの構成

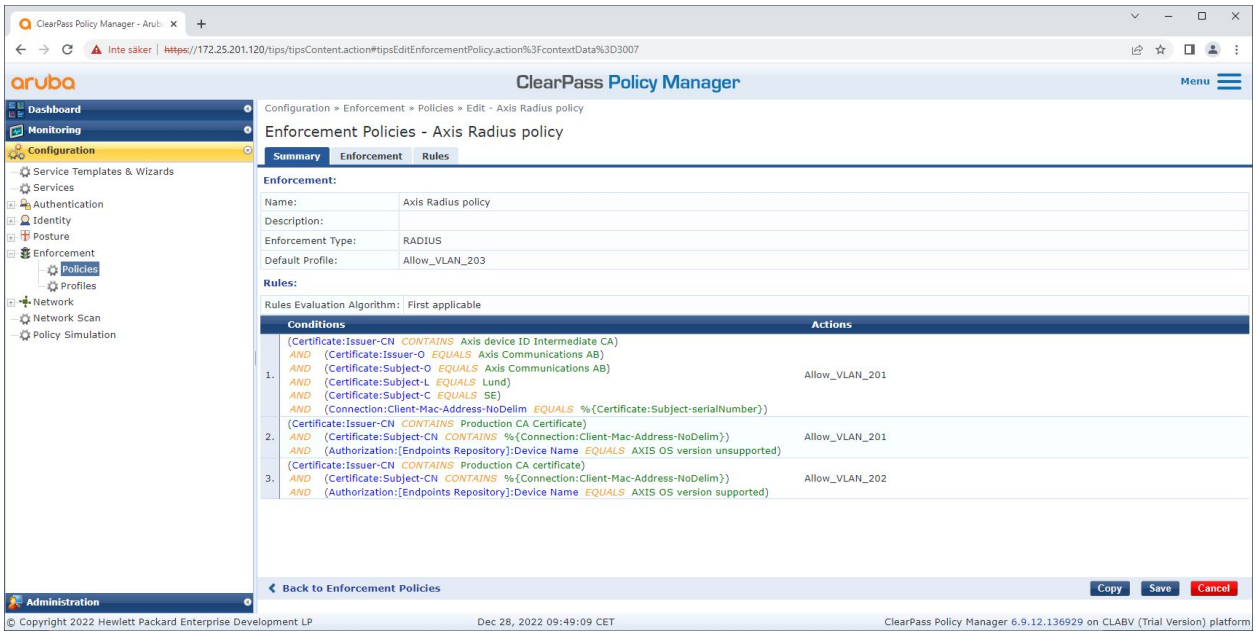
強制プロファイルを用いることで、Aruba ClearPass Policy Managerはスイッチ上のアクセスポートに特定のVLAN IDを割り当てることが可能になります。割り当てはポリシーに基づいて決定され、装置グループ「スイッチ」内のネットワーク装置に適用されます。必要な強制プロファイルの数は、使用するVLANの数によって異なります。この設定には、合計で3つのVLAN (VLAN 201、202、203) があり、3つの強制プロファイルに関連付けられています。

安全なオンボーディング - IEEE 802.1AR/802.1X

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。Aruba 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、Aruba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。



Aruba ClearPass Policy Manager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

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。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、ファームウェアのアップデート、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。Aruba ClearPass Policy Managerは、以下の状態を検証します。

- Axis装置のファームウェアのバージョン。
- 装置のMACアドレスが、Axis装置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)

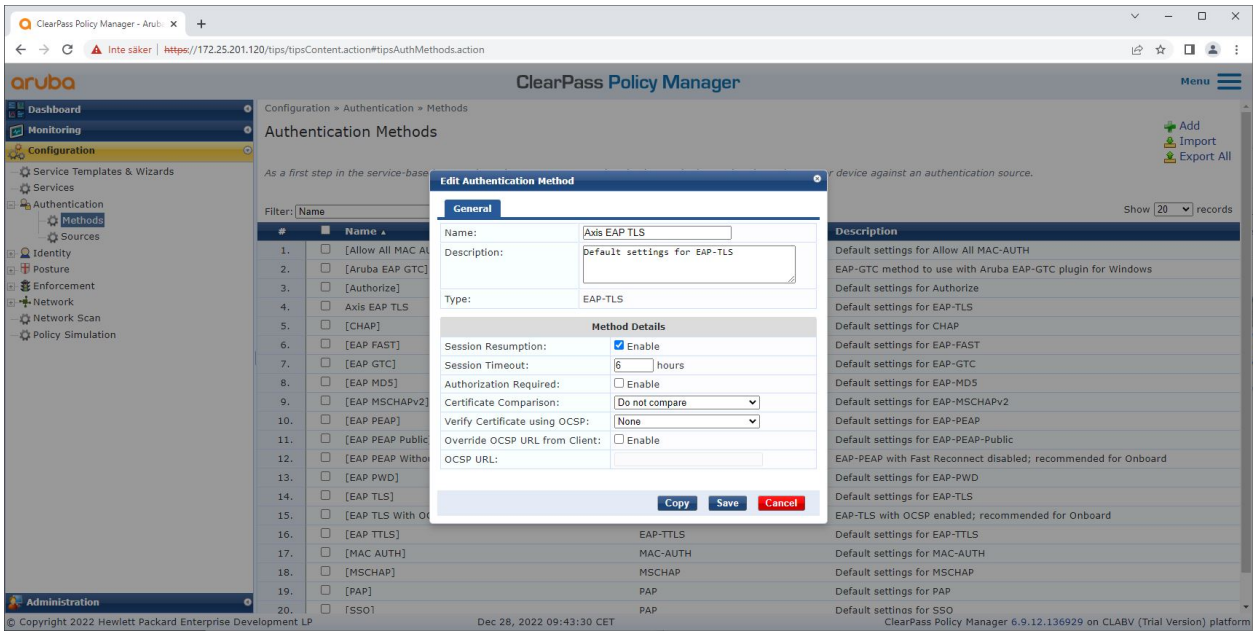
Axis装置に、Axis装置が稼働する運用ネットワークへのアクセスが付与されます。アクセスは、プロビジョニングネットワーク (VLAN 201) で装置のプロビジョニングが完了した後に付与されます。Aruba ClearPass Policy Managerは、以下の状態を検証します。

- 装置のMACアドレスが、Axis装置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装置のファームウェアのバージョン。
- 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

Axis装置がArubaネットワークで認証を試行する方法は、認証方式で定義されます。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。

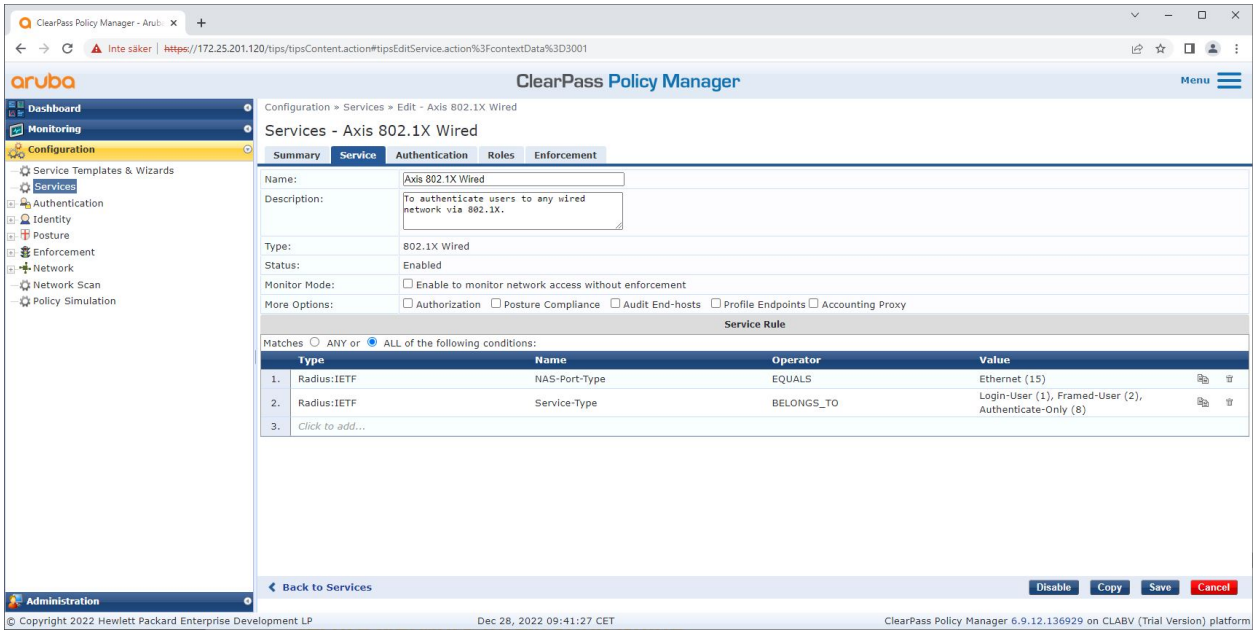
安全なオンボーディング - IEEE 802.1AR/802.1X



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

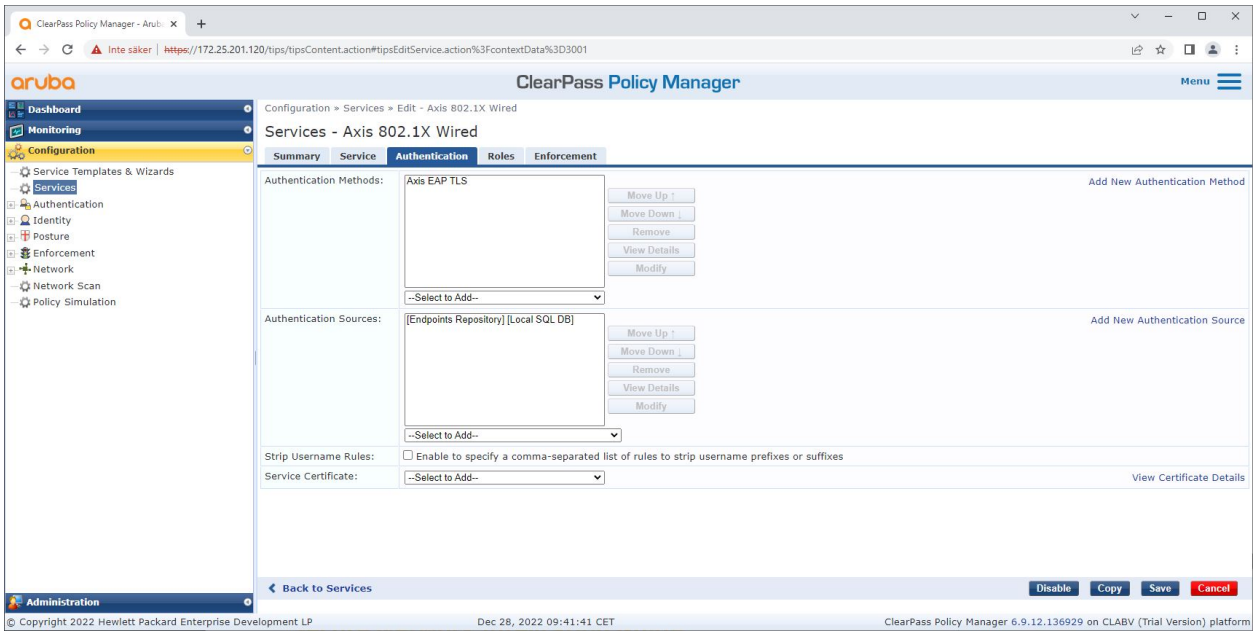
サービスの設定

[Services (サービス)] インターフェースでは、設定手順が1つのサービスに結合されています。このサービスが、Arubaネットワーク内のAxis装置の認証と認可を処理します。

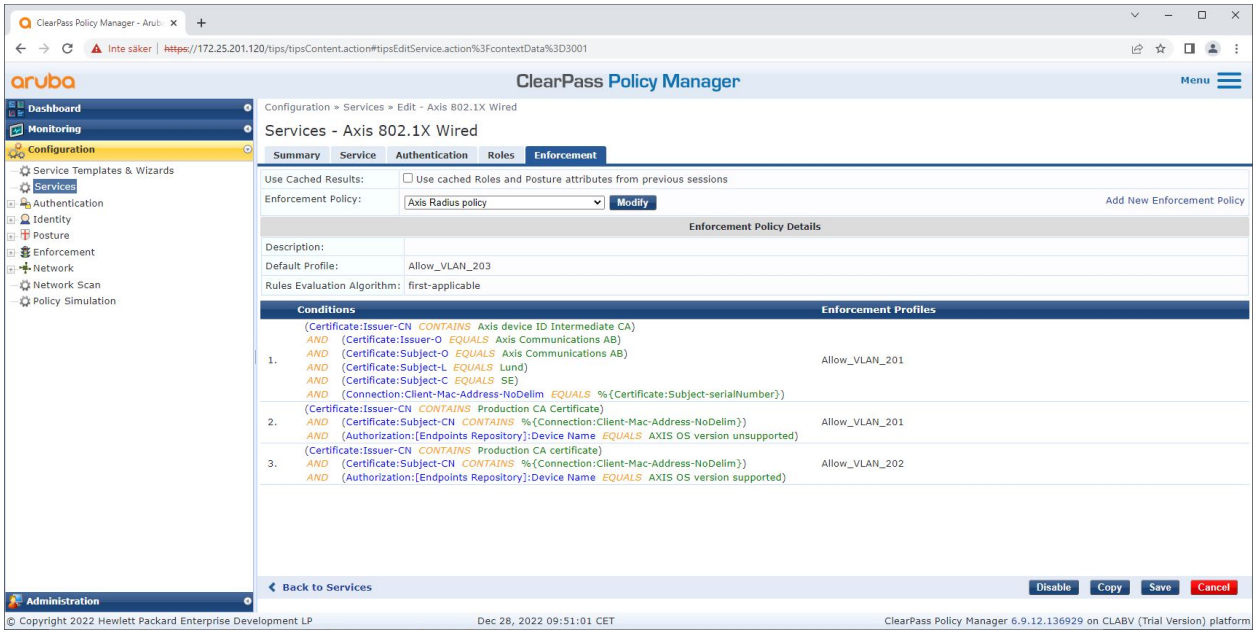


専用のAxisサービスが作成され、IEEE 802.1Xが接続方式として定義されます。

安全なオンボーディング - IEEE 802.1AR/802.1X



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。

Arubaアクセススイッチ

Axis装置は、直接PoE対応のArubaアクセススイッチに接続することも、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。Aruba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Aruba ClearPass Policy Managerに中継します。Aruba 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。

安全なオンボーディング - IEEE 802.1AR/802.1X

Aruba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。

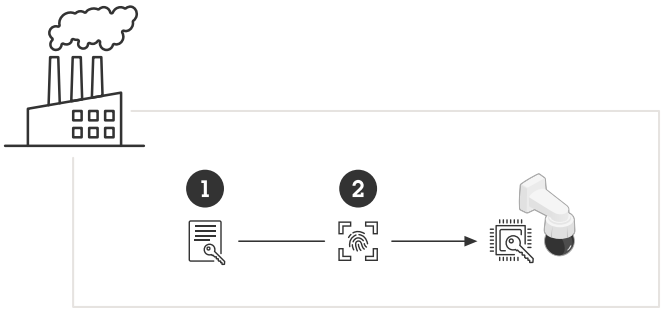
```
radius-server host MyRADIUSIPAddress key "MyRADIUSKey"

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装置IDと呼ばれる安全な装置IDを製造時に付与されています。Axis装置ID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。



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

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

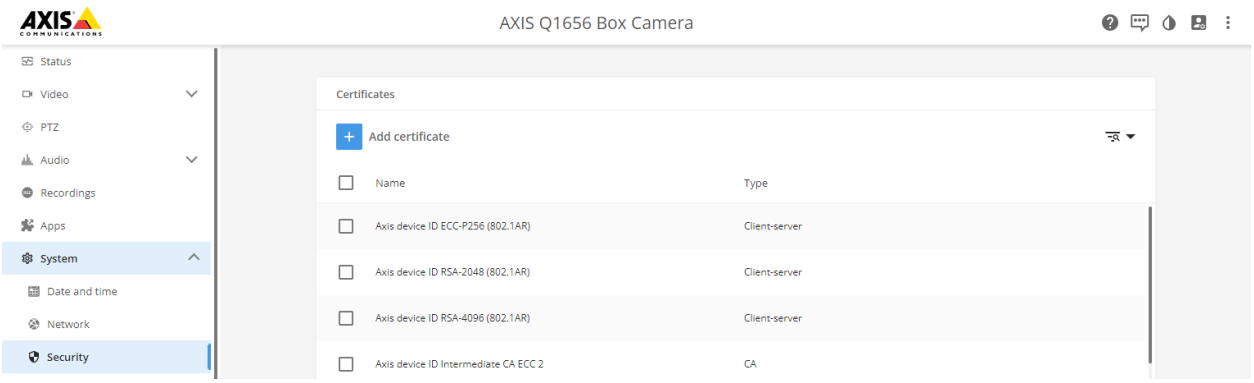
Axis装置のセキュアエレメントにより提供されるハードウェア保護型の安全なキーストアは、工場でプロビジョニングされています。さらに、Axis装置の信頼性をグローバルに証明する装置固有の証明書と対応キー (Axis装置ID) が付属します。Axis Edge VaultとAxis装置IDをサポートする対象のAxis装置については、*Axis Product Selector*を使用して確認できます。

注

Axis装置のシリアル番号は、装置のMACアドレスです。

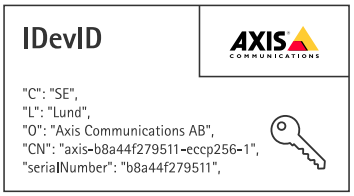
Secure integration of Axis devices into Aruba networks

安全なオンボーディング - IEEE 802.1AR/802.1X



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装置ID。

IEEE 802.1AR準拠のAxis装置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。Aruba 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装置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

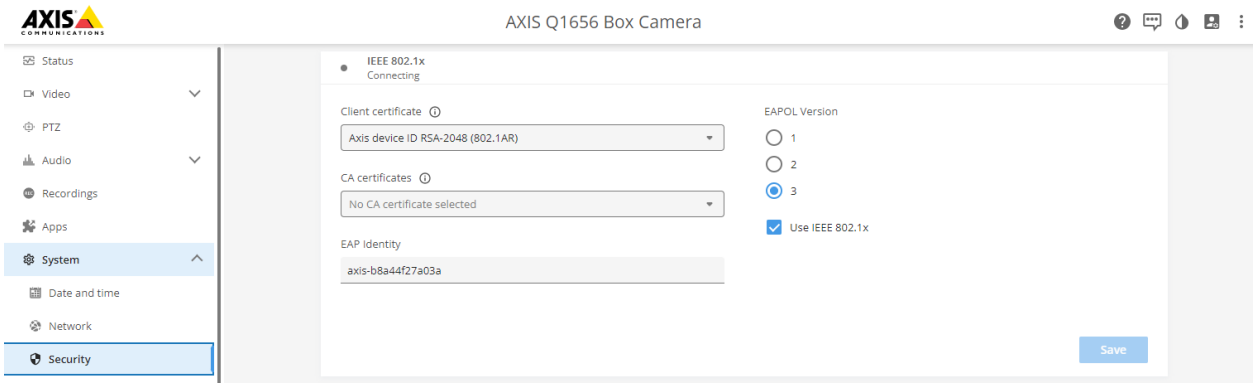


Country (国名)	SE
位置	Lund
Issuer Organization (発行者組織)	Axis Communications AB
Issuer Common Name (発行者の通称)	Axis device ID intermediate
Organization (Axis装置ID中間組織)	Axis Communications AB
Common Name (通称)	axis-b8a44f279511-eccp256-1
Serial Number (シリアル番号)	b8a44f279511

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装置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。

Secure integration of Axis devices into Aruba networks

安全なオンボーディング - IEEE 802.1AR/802.1X



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装置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。

- ファームウェアアップデートのインストール。
- 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。

Secure integration of Axis devices into Aruba networks

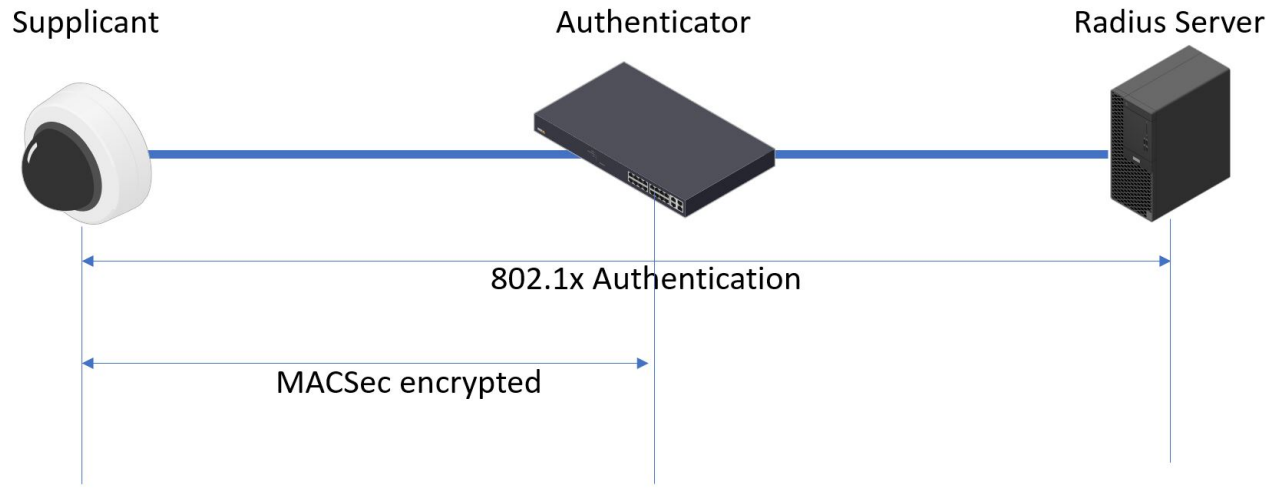
安全なネットワーク運用 - IEEE 802.1AE MACsec

安全なネットワーク運用 - IEEE 802.1AE MACsec

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装置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。

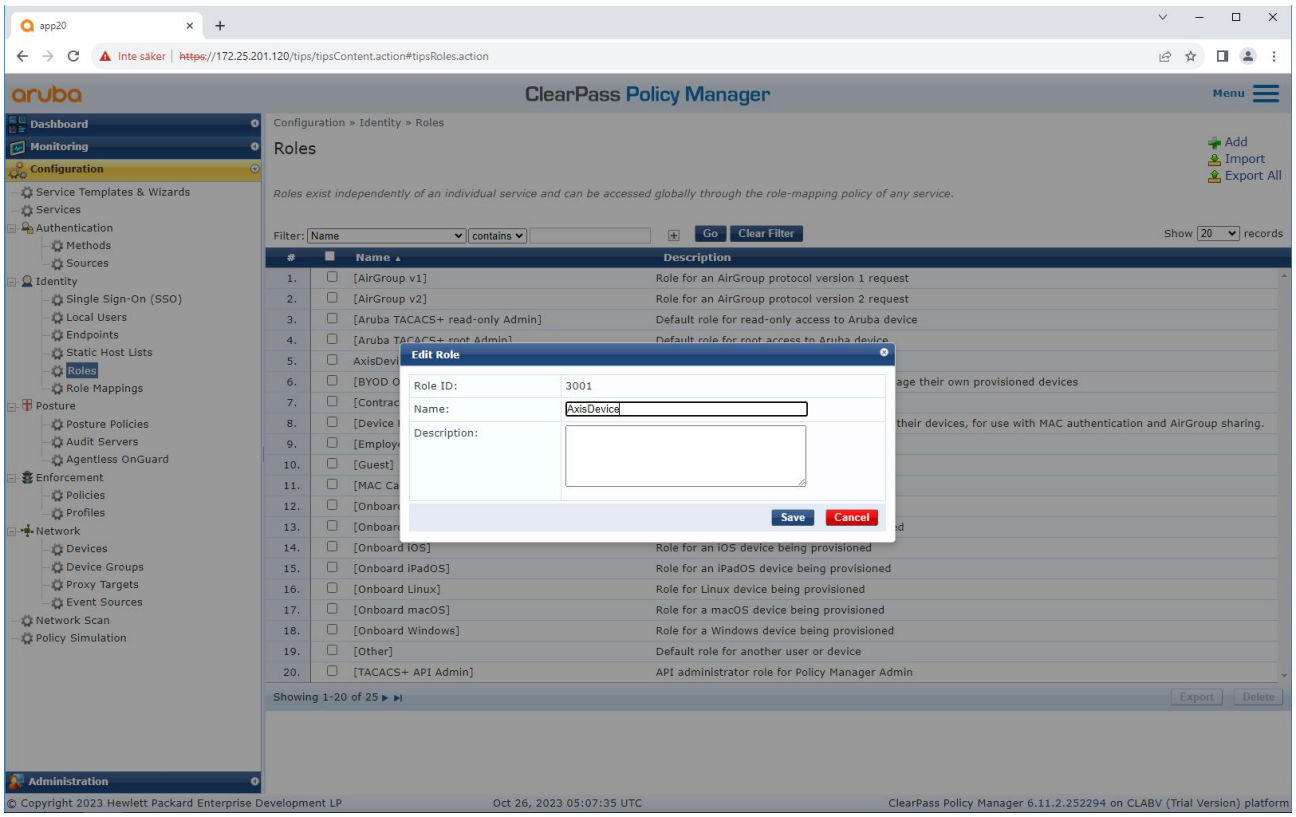
安全に保存されたIEEE 802.1AR準拠の安全な装置ID、Axis装置ID (1) は、IEEE 802.1X EAP-TLSポートベースのネットワークアクセスコントロール (2) を経由したArubaネットワーク (4, 5) への認証に使用されます。このEAP-TLSセッションを通じてMACsecキーが自動的に交換され、安全なリンク (3) が設定されるほか、Axis装置からArubaスイッチまでのすべてのネットワークトラフィックが保護されます。

IEEE 802.1AE MACsecには、Aruba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。

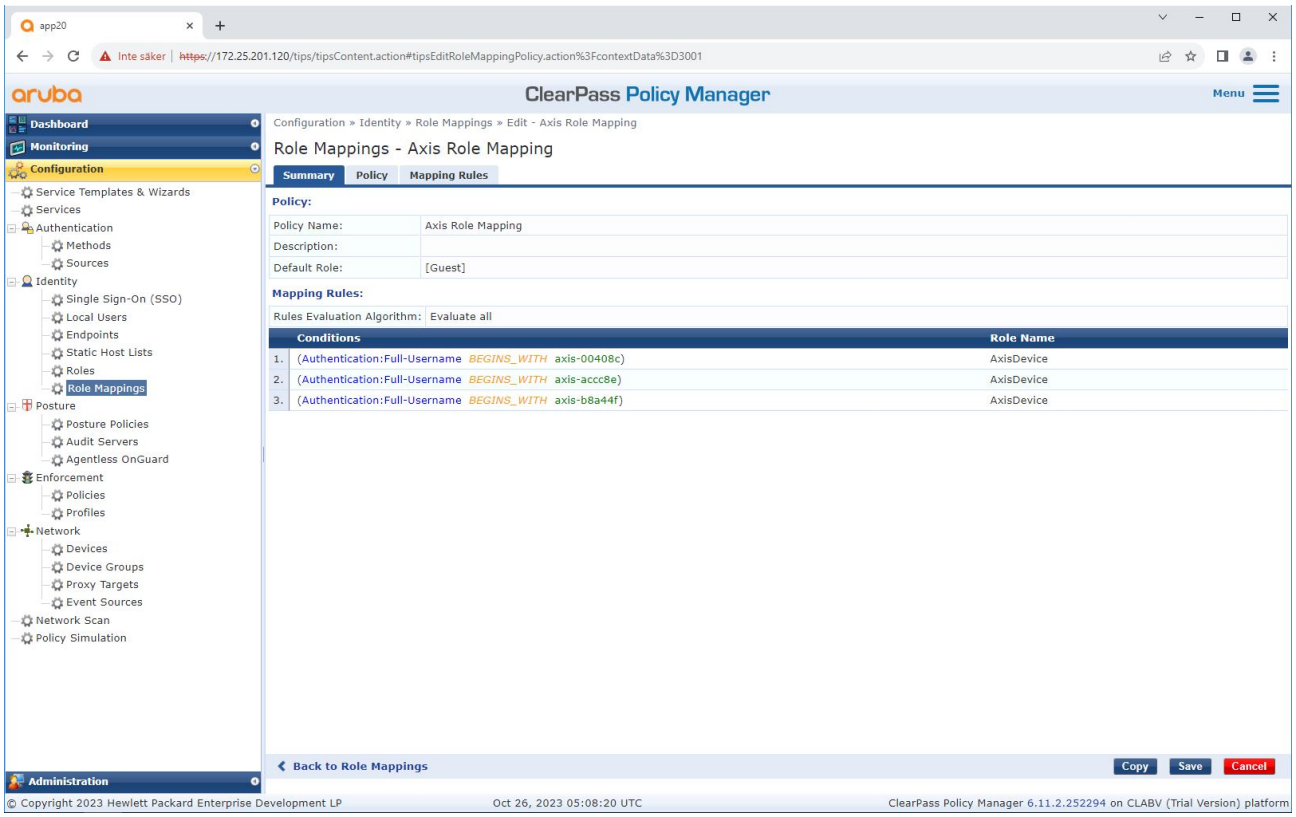
ArubaアクセススイッチがMACsecによるEAP-TLSの使用をサポートしていない場合は、Pre-Shared Keyモードを使用して手動で設定できます。

Aruba ClearPass Policy Manager

ロールとロールマッピングポリシー



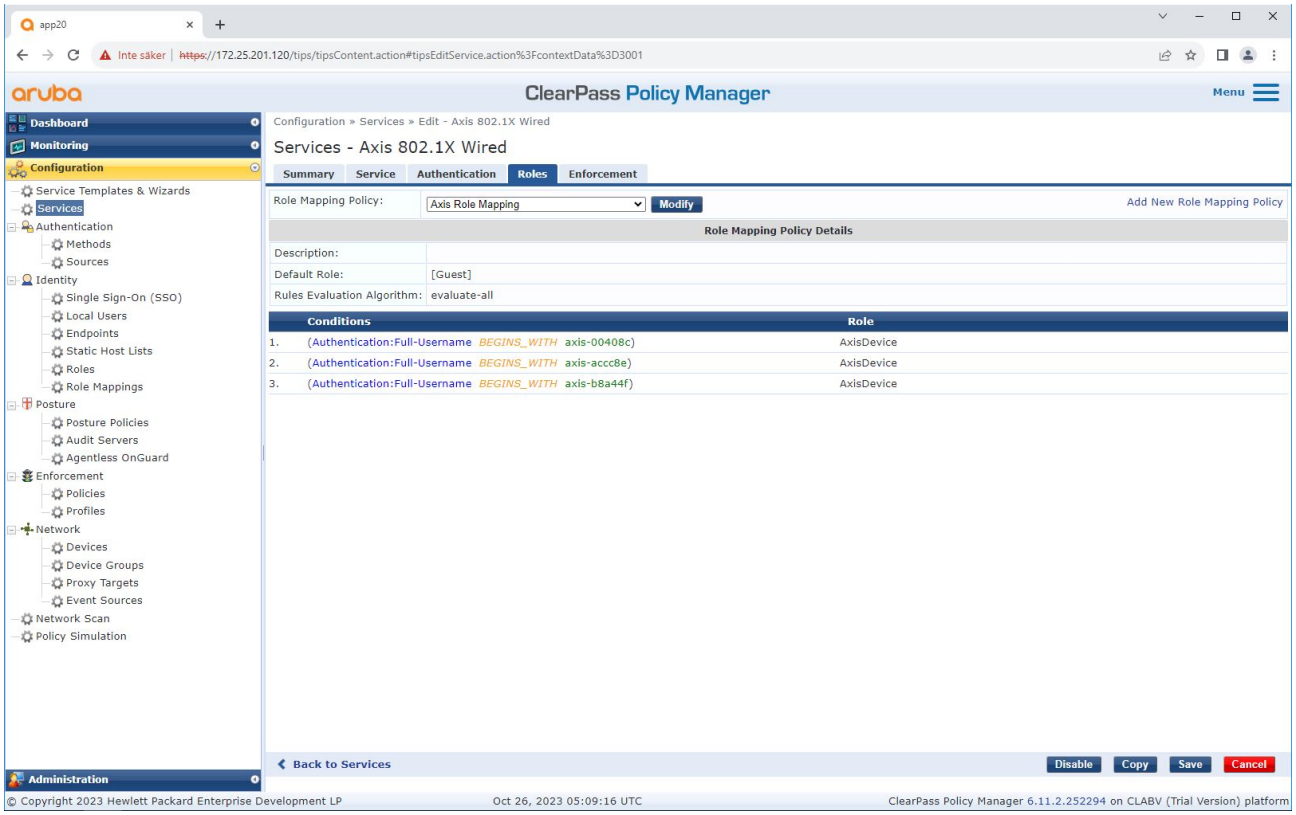
Axis装置のロール名を追加します。この名前は、Arubaアクセススイッチ構成のポートアクセスロール名です。



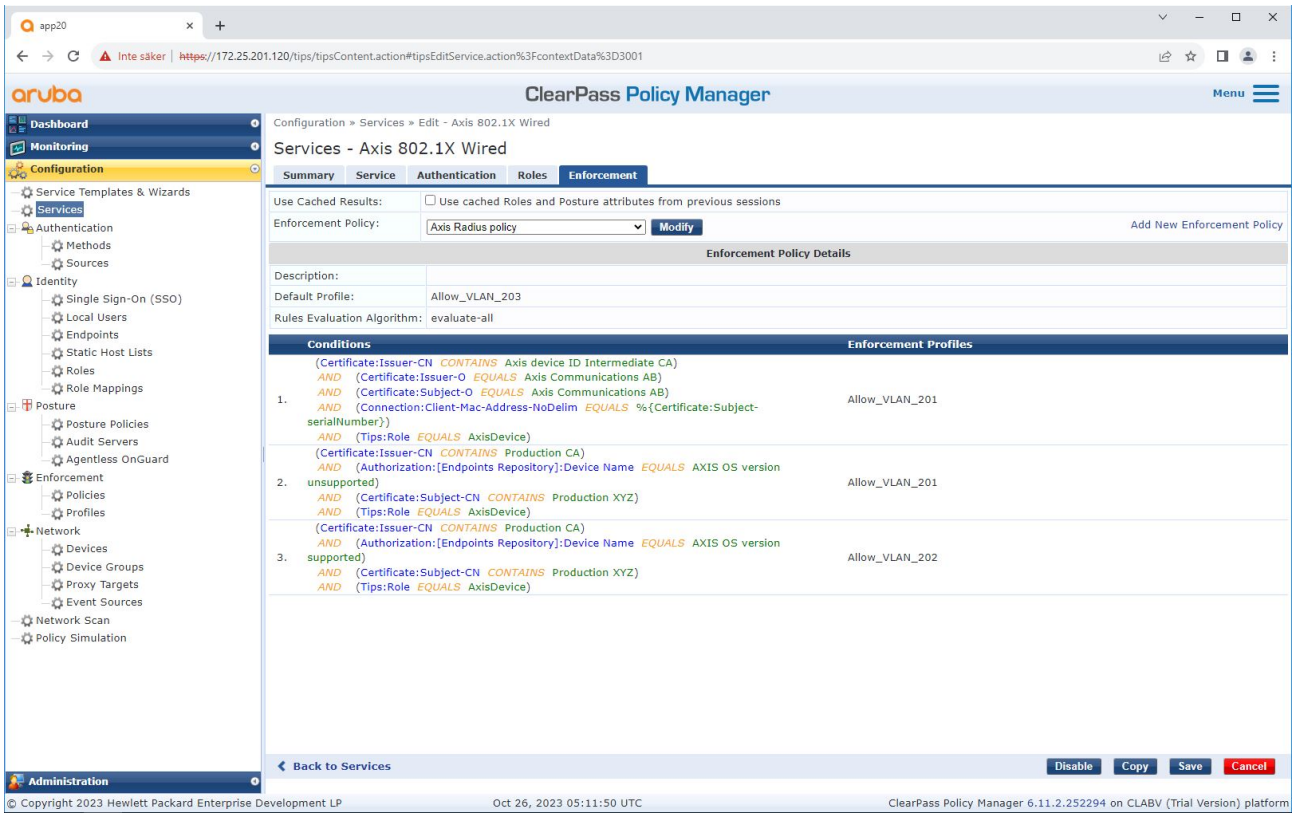
前出の手順で作成したAxis装置のロール向けに、Axisロールマッピングポリシーを追加します。この条件定義は、装置をAxis装置ロールにマッピングするために必要です。条件が満たされない場合、装置は [ゲスト] ロールの一部になります。

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

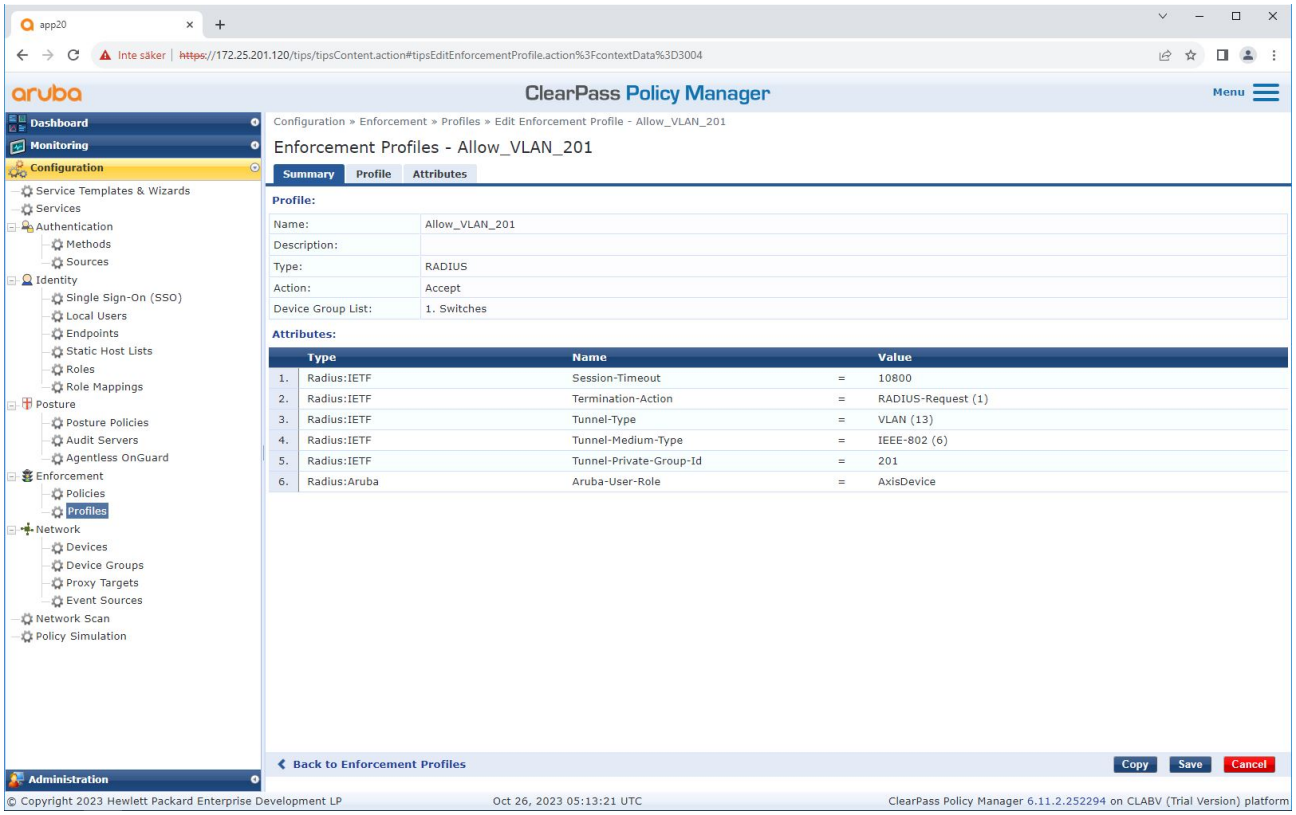


Axis装置のオンボーディングの接続方式としてIEEE 802.1Xを定義するサービスに、前出の手順でに作成したAxisロールマッピングポリシーを追加します。



既存のポリシー定義に、Axisロール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。

Arubaアクセススイッチ

*16ページAruba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、IEEE 802.1AE MACsecをArubaアクセススイッチに設定するための次のポート構成事例を参照してください。

```
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

レガシーオンボーディング - MAC認証

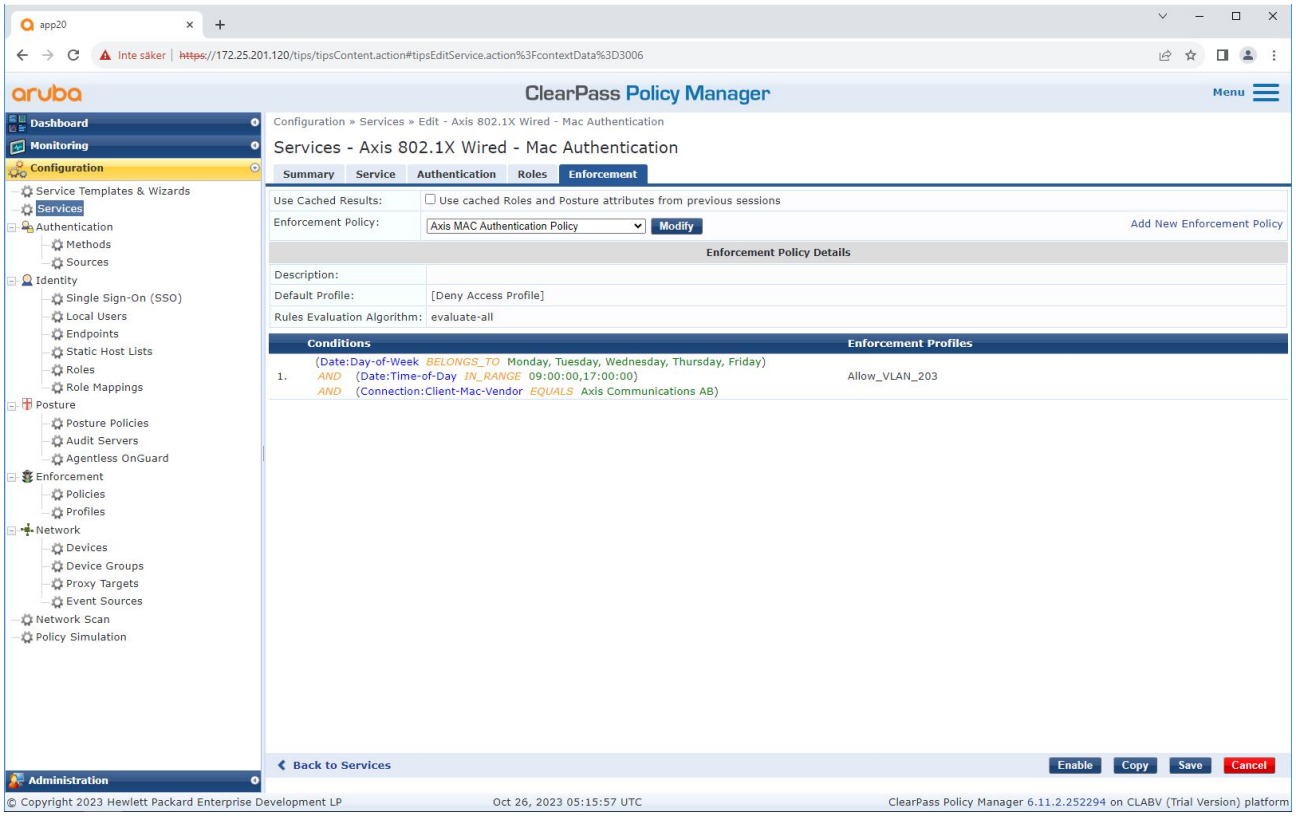
MAC Authentication Bypass (MAB) とAxis装置ID証明書、工場出荷時の設定で有効化されているIEEE 802.1Xを使用して、IEEE 802.1ARをサポートしないAxis装置をオンボーディングすることができます。802.1Xオンボーディングが失敗した場合、Aruba ClearPass Policy ManagerはAxis装置のMACアドレスを検証し、ネットワークへのアクセスを付与します。

MABには、Aruba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。

Aruba ClearPass Policy Manager

強制ポリシー

Aruba 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、Aruba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

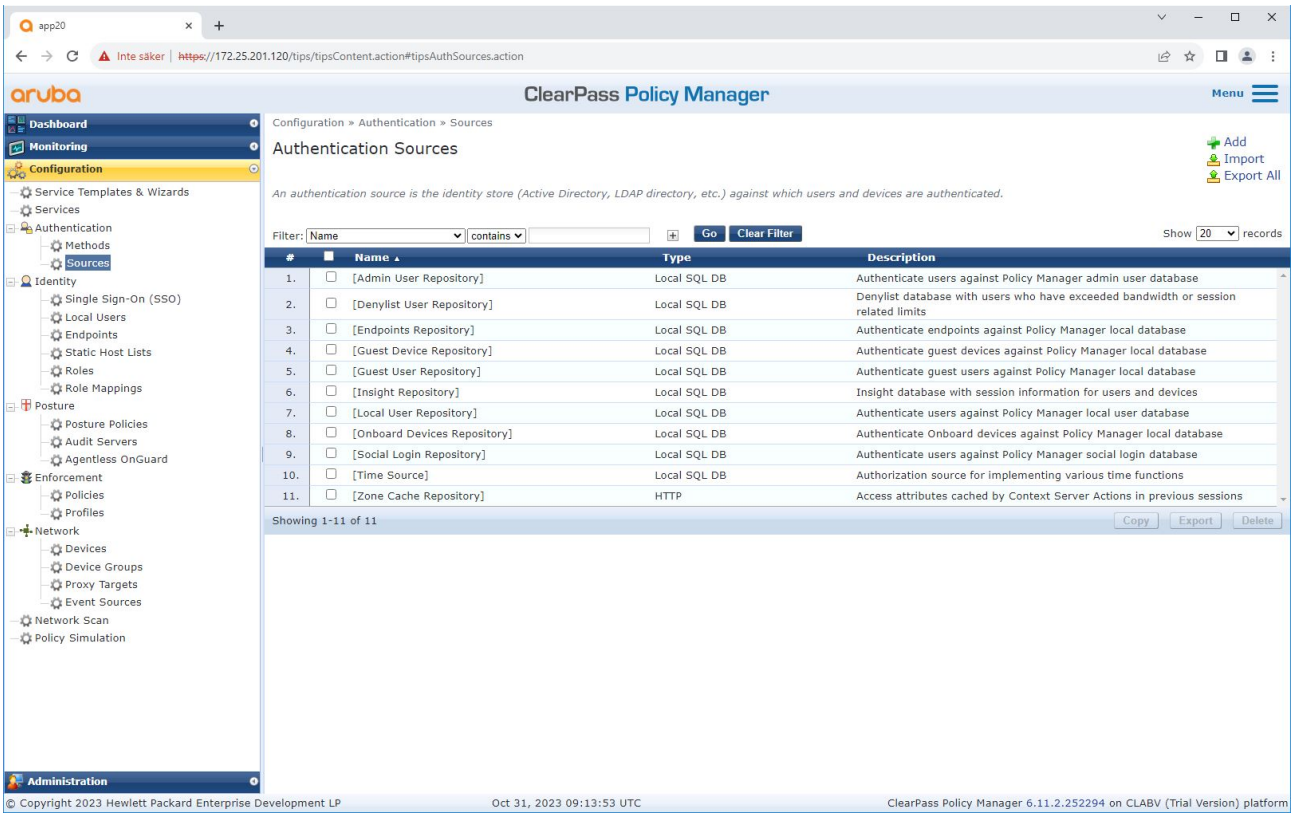
レガシーオンボーディング - MAC認証

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

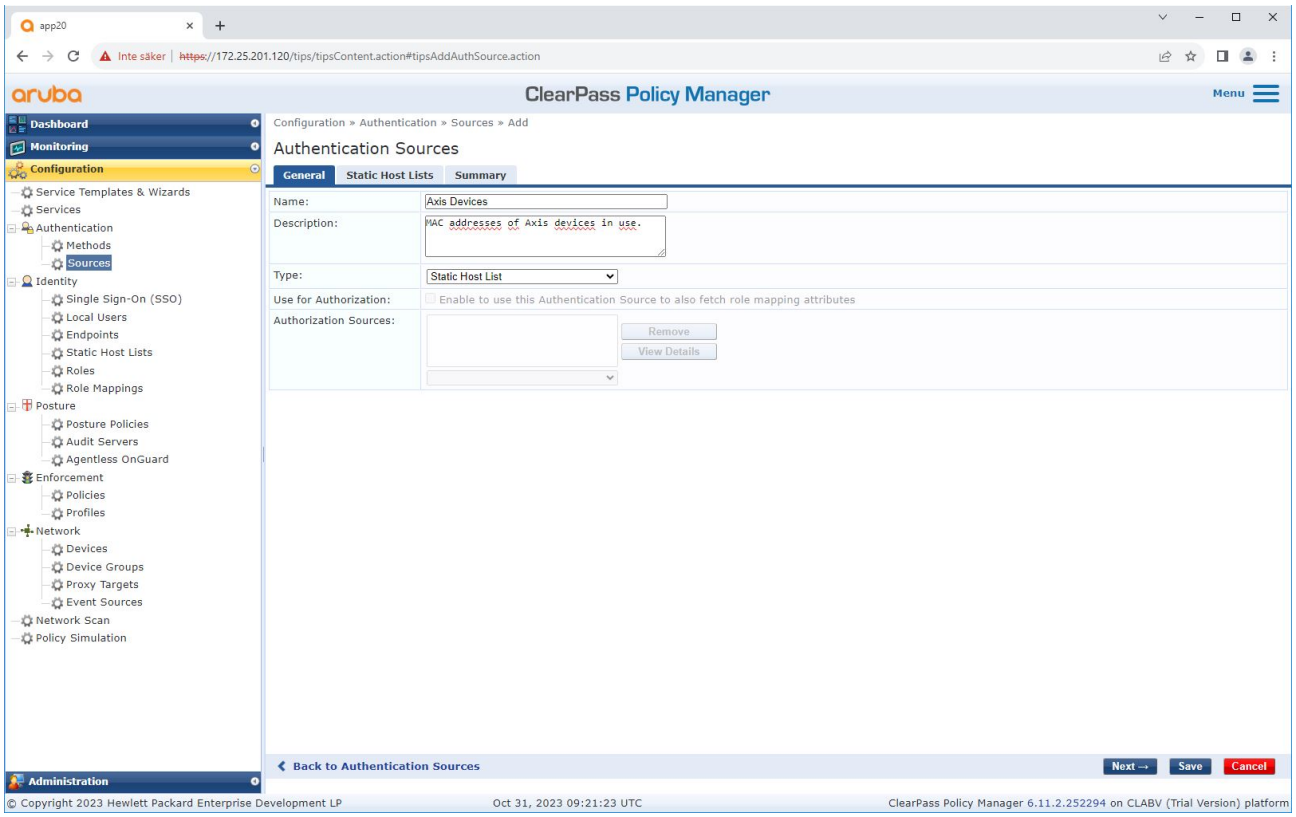
MACアドレスはスプーフィングされる可能性があるため、通常のプロビジョニングネットワークへのアクセスは付与されません。MABは初回オンボーディングにのみ使用し、装置をさらに手動で検査することをお勧めします。

ソースの設定

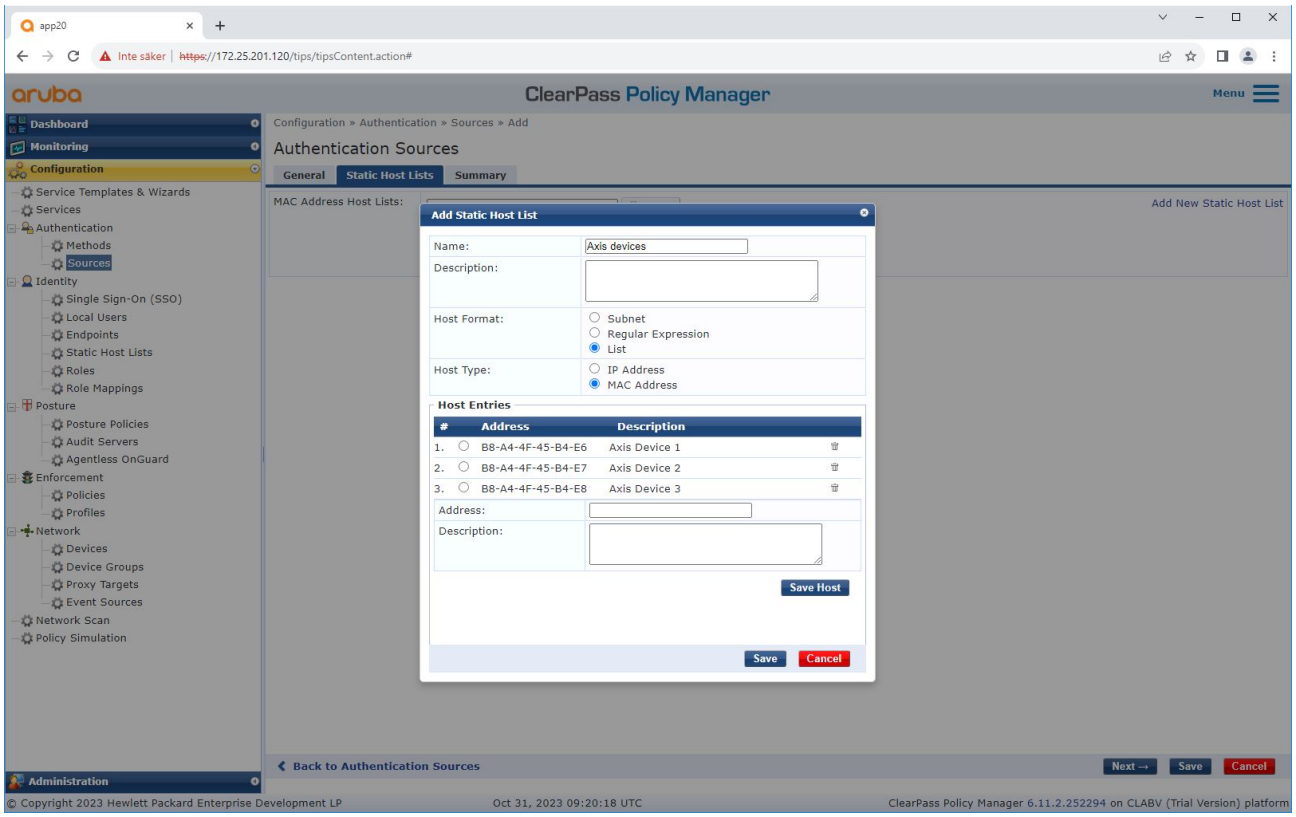
[Sources (ソース)] インターフェースでは新しい認証ソースが作成され、手動でインポートされたMACアドレスのみを許可します。



レガシーオンボーディング - MAC認証

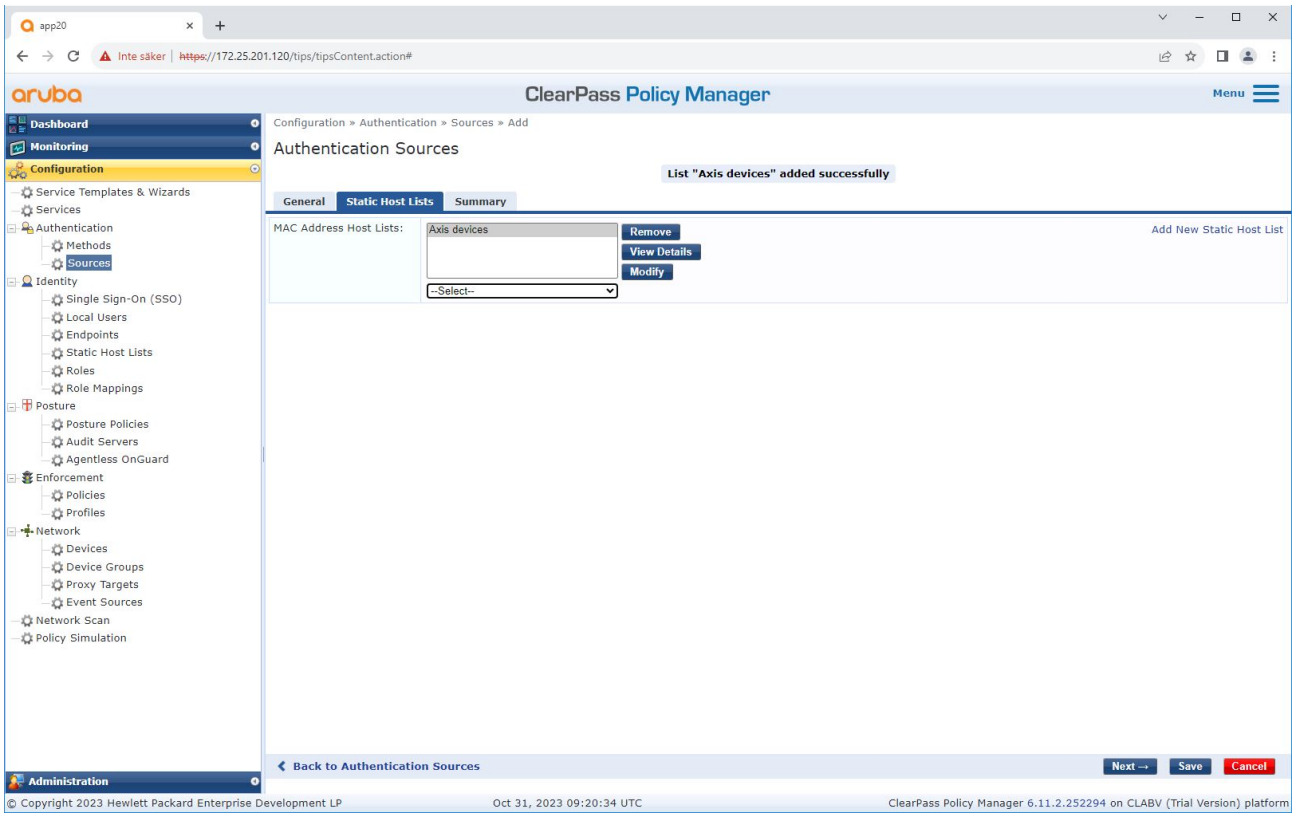


レガシーオンボーディング - MAC認証



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

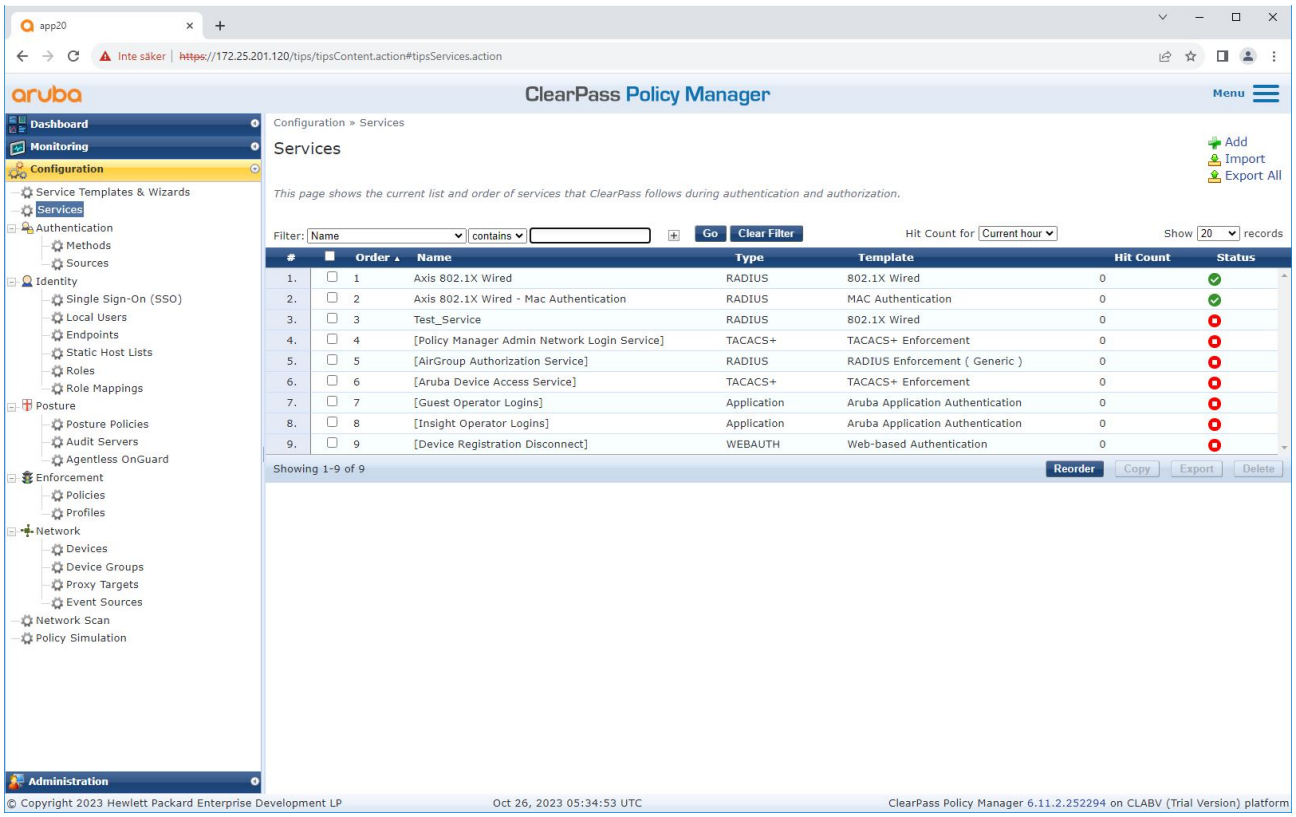


サービスの設定

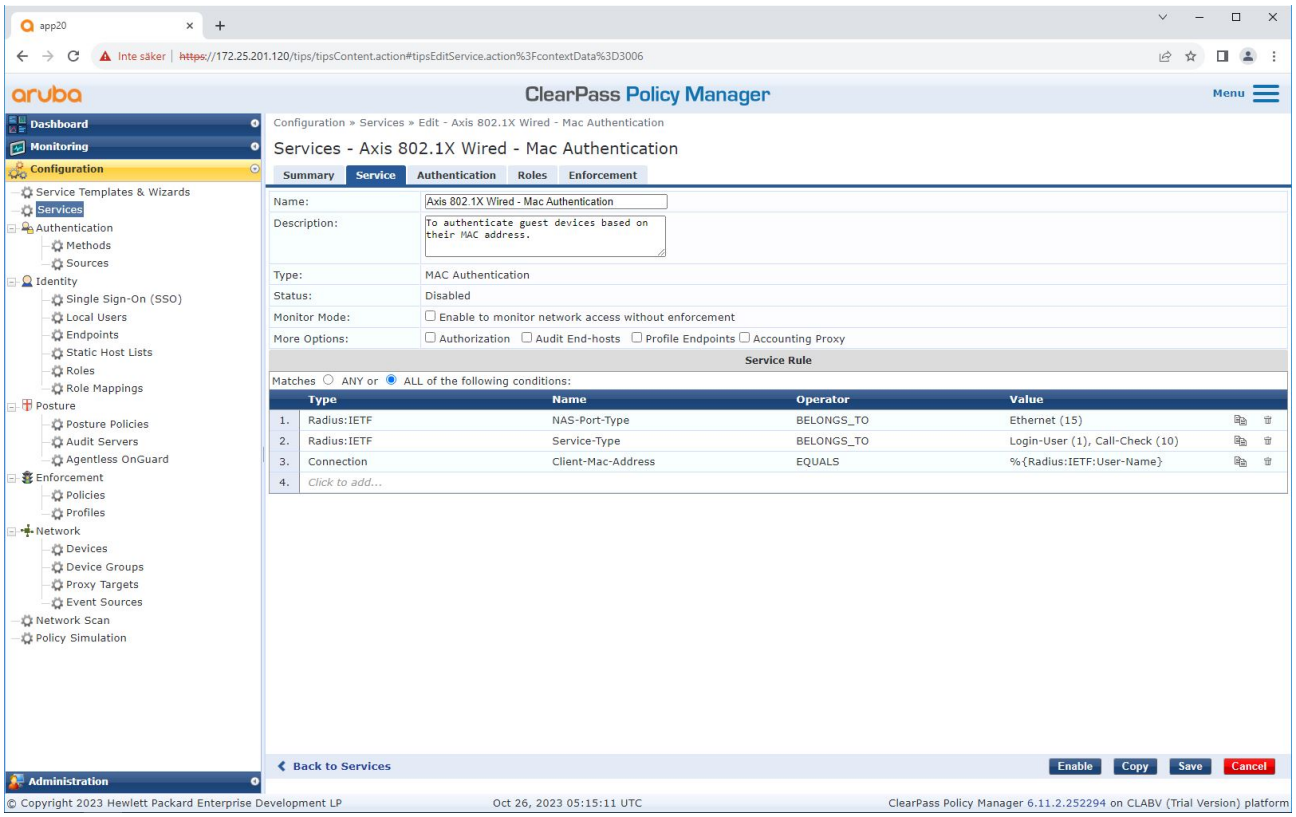
[Services (サービス)] インターフェースでは、設定手順が1つのサービスに結合されています。このサービスが、Arubaネットワーク内のAxis装置の認証と認可を処理します。

Secure integration of Axis devices into Aruba networks

レガシーオンボーディング - MAC認証

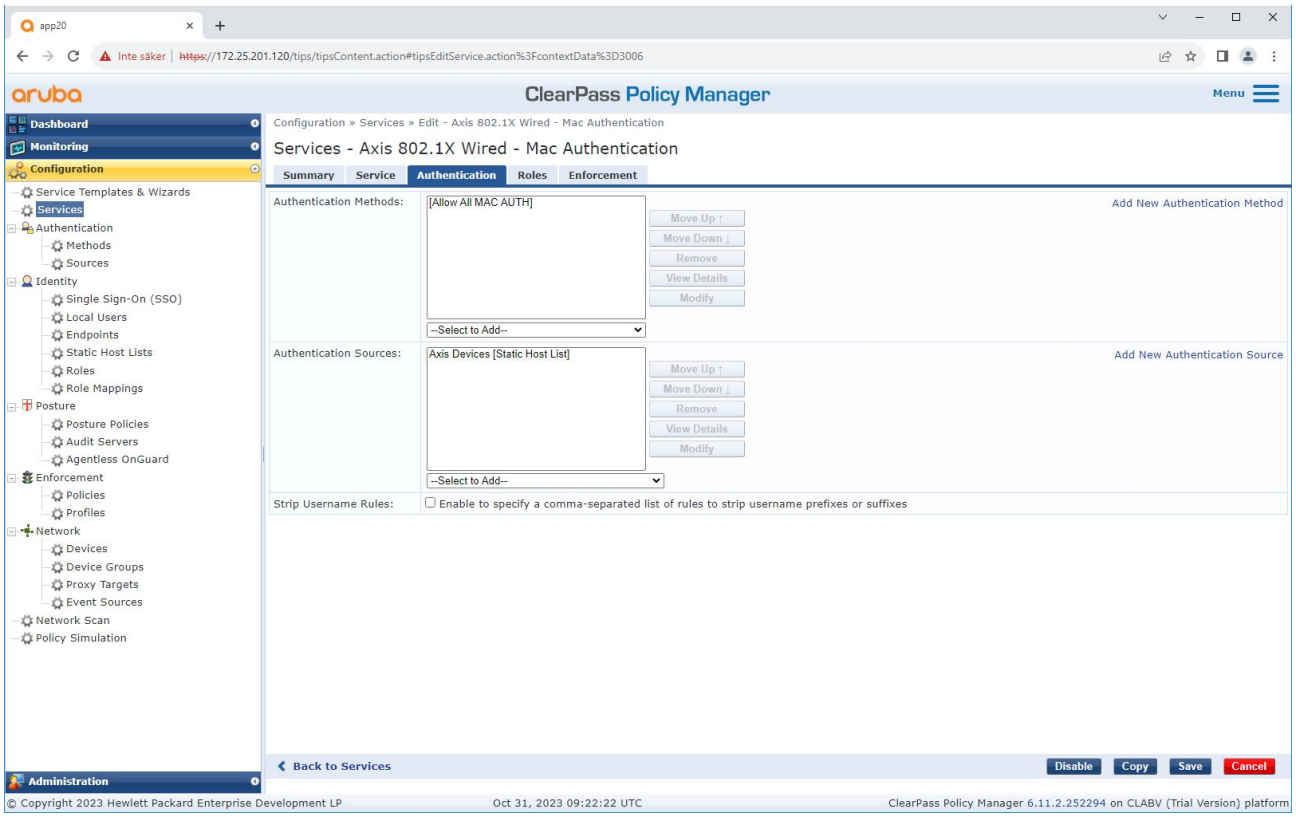


レガシーオンボーディング - MAC認証



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

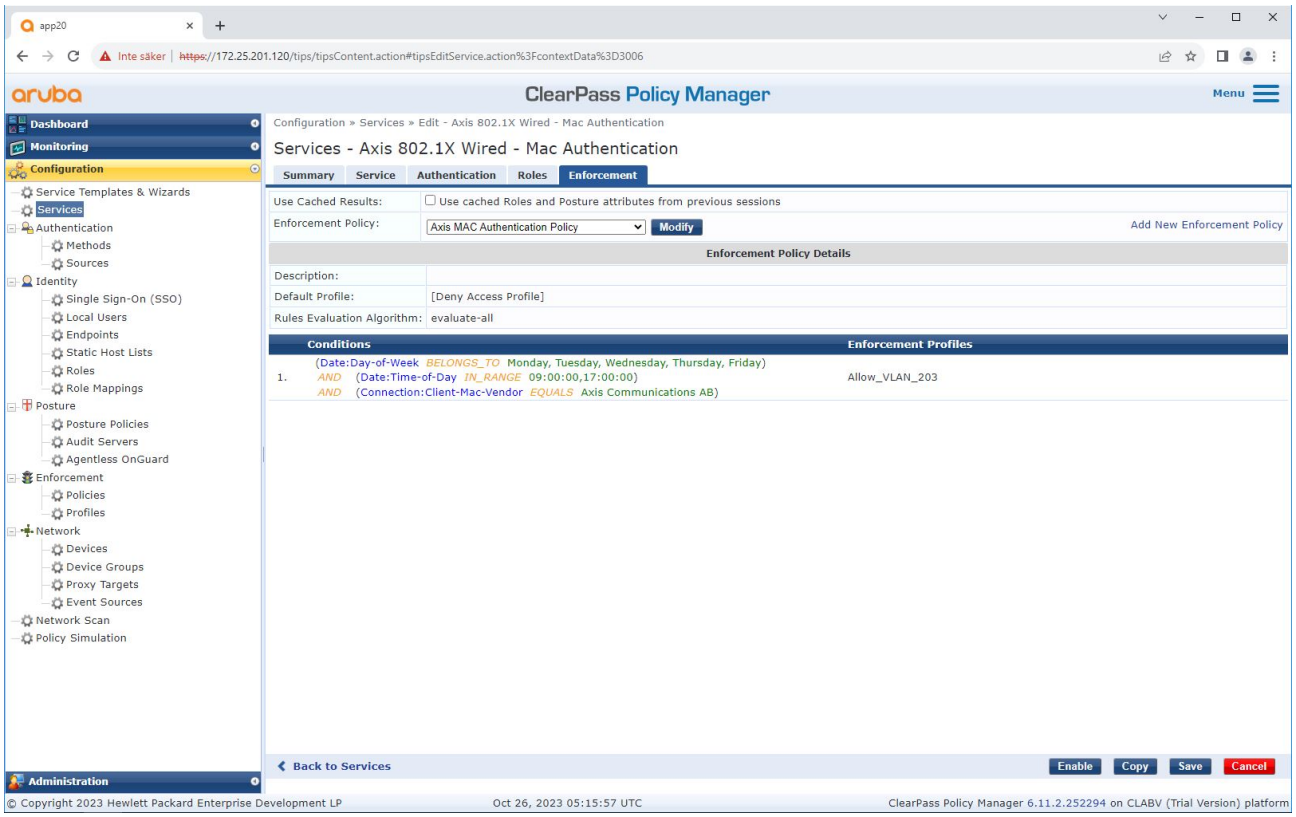


事前設定されたMAC認証方式がサービスに設定されます。またAxis MACアドレスのリストを含む、前出の手順で作成した認証ソースが選択されます。

Axis Communications AB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。

Arubaアクセススイッチ

*16ページAruba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Aruba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
```

ユーザーマニュアル
Secure integration of Axis devices into Aruba networks

バージョン M4.3
日付: 2023年11月
製品番号 T10197992