# HPE Aruba Networking

用户手册

目录

## 引言

本集成指南概述了在 HPE Aruba Networking 网络中引入和操作安讯士设备的最佳实践配置。配置使用现代安全标准和协议，如 IEEE 802.1X、IEEE 802.1AR、IEEE 802.1AE 和 HTTPS。

建立适当的网络集成自动化可以节省您的时间和金钱。当将安讯士设备管理应用程序与 HPE Aruba Networking 基础设施和应用结合使用时，它可以消除不必要的系统复杂性。将安讯士设备和软件与 HPE Aruba Networking 基础设施结合使用时，您将获得以下好处：

- 删除设备暂存网络可大幅降低系统复杂性。
- 新增自动化配置入网流程和设备管理，有效降低成本。
- 安讯士设备提供零接触网络安全控制。
- 凭借 HPE 和安讯士专业知识，全面提升网络安全性。

为了在整个配置入网过程中在逻辑网络之间实现软件定义的平稳过渡，网络基础设施建设必须先行，以便在开始配置之前安全地验证安讯士设备的完整性。在进行配置之前，您需要具备以下条件：

- 通过 HPE Aruba Networking 管理企业网络 IT 基础设施的经验，包括 HPE Aruba Networking 接入交换机和 HPE Aruba Networking ClearPass Policy Manager。
- 现代网络访问控制技术和网络安全策略的专业知识。
- 最好是事先了解安讯士产品的基本知识，而这部分也在整个指南中提供。

## 安全加入 – IEEE 802.1AR/802.1X

要观看此视频，请转到本文档的网页版本。

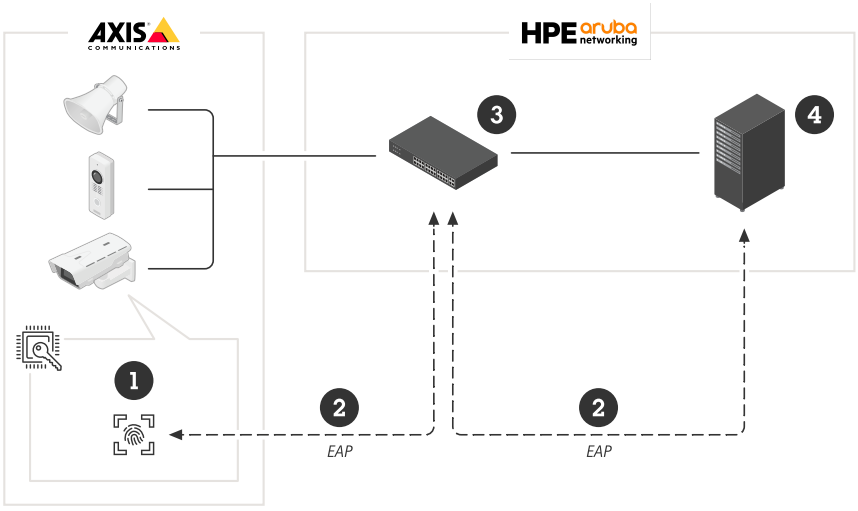
*使用 IEEE 802.1X/802.1AR 将设备安全载入到零信任网络*

### 初始认证

当支持 Axis Edge Vault 的安讯士设备连接到网络时，它会通过 IEEE 802.1X 网络访问控制，使用 IEEE 802.1AR 安讯士设备 ID 证书对自身进行身份验证。

为了授予网络访问权限，ClearPass Policy Manager 会验证安讯士设备 ID 及其他设备特定的指纹。此类信息（例如 MAC 地址和设备的 AXIS OS 版本）用于做出基于策略的决策。

安讯士设备使用符合 IEEE 802.1AR 的安讯士设备 ID 证书在网络上对自身进行身份验证。

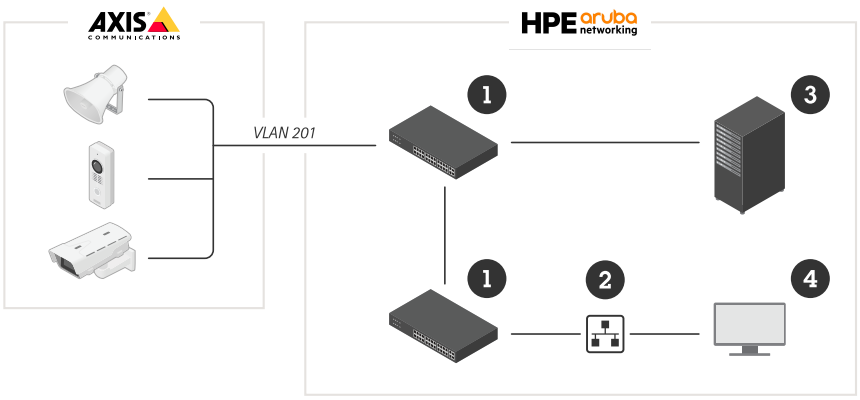



*安讯士设备使用符合 IEEE 802.1AR 的安讯士设备 ID 证书针对 HPE Aruba Networking 网络进行身份验证。*

1. *安讯士设备ID*
2. *IEEE 802.1x EAP–TLS 网络身份验证*
3. *接入交换机（验证器）*
4. *ClearPass 策略管理器*

### 配置

通过身份验证后，安讯士设备进入到配置网络 (VLAN201)。该网络包含 AXIS Device Manager，可进行设备配置、安全强化配置及 AXIS OS 更新。为了完成设备配置，新的客户特定生产级证书将上传到设备以用于 IEEE 802.1X 和 HTTPS。

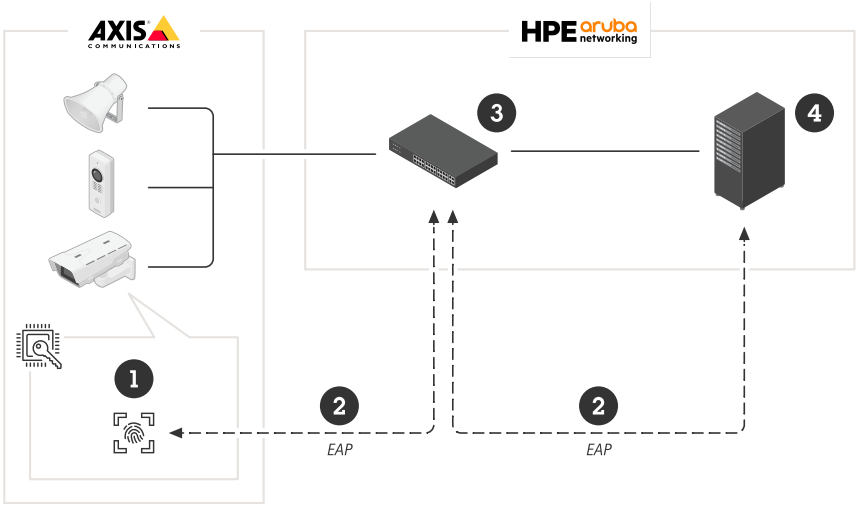



*身份验证成功后，安讯士设备将进入配置网络进行配置。*

1 *接入开关*
2 *配置网络*
3 *ClearPass 策略管理器*
4 *设备管理应用*

## 生产网络

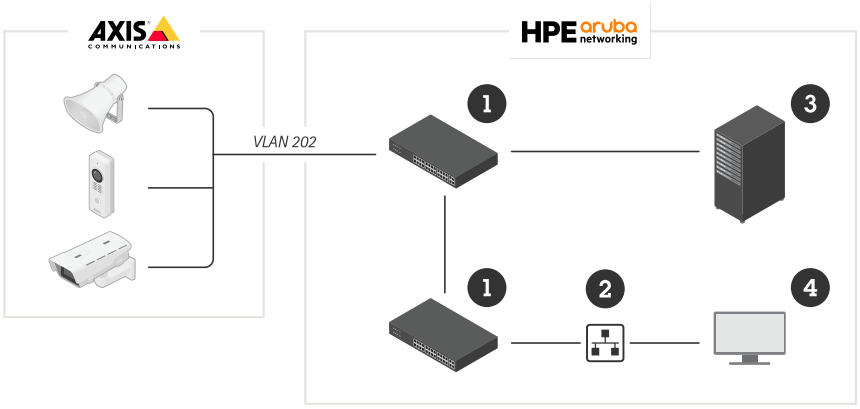
为安讯士设备配置新的 IEEE 802.1X 证书会触发新的身份验证尝试。ClearPass Policy Manager 验证新证书并决定是否将安讯士设备移至生产网络中。




*完成配置后，安讯士设备将离开配置网络，并尝试在该网络上重新进行身份验证。*

1 *安讯士设备ID*
2 *IEEE 802.1x EAP–TLS 网络身份验证*
3 *接入交换机（验证器）*
4 *ClearPass 策略管理器*

重新进行身份验证后，安讯士设备进入生产网络 (VLAN 202)，视频管理系统 (VMS) 则连接至该设备并开始工作。




*安讯士设备被授予对生产网络的访问权限。*

1 *接入开关*
2 *生产网络*
3 *ClearPass 策略管理器*
4 *视频管理系统*

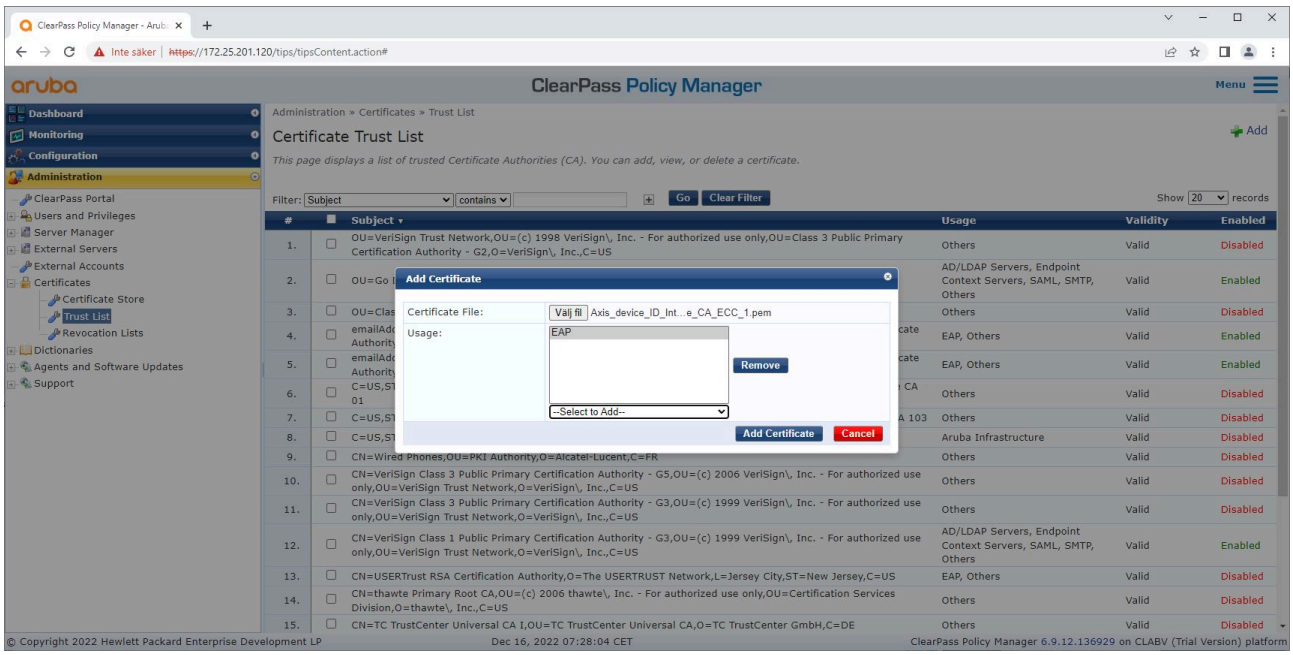
## 配置 HPE Aruba Networking

### HPE Aruba Networking ClearPass Policy Manager

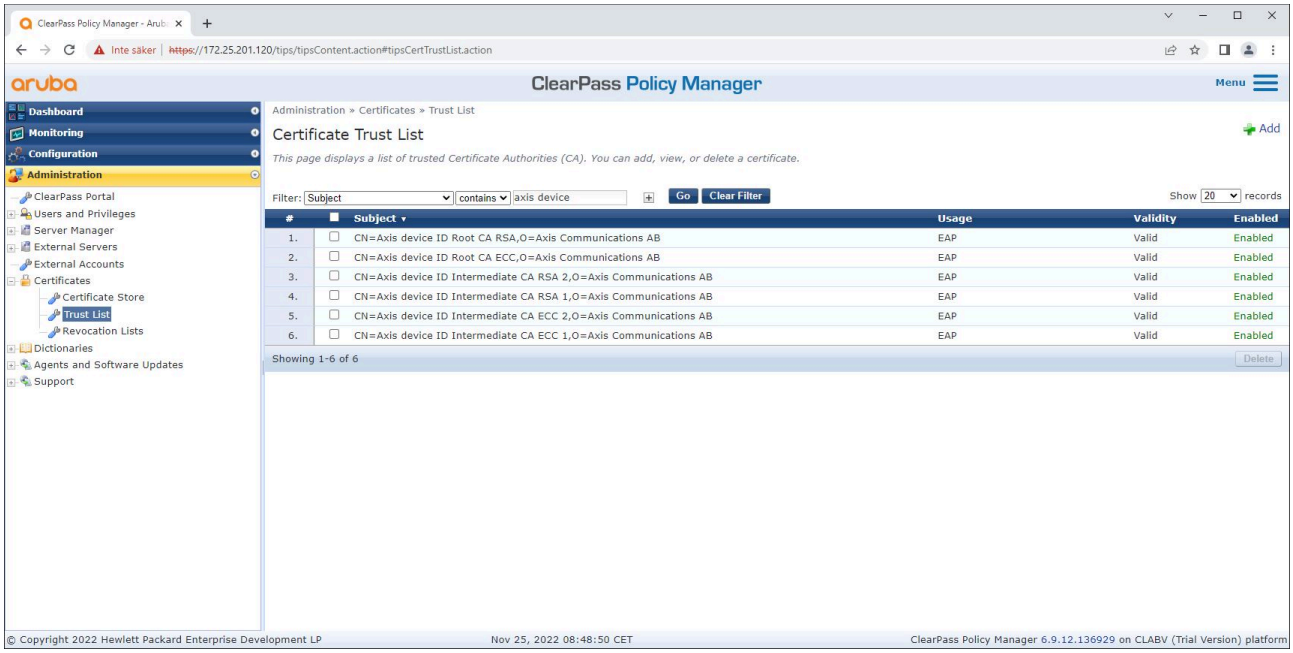
ClearPass Policy Manager 为跨多供应商的有线、无线和 VPN 基础设施的 IoT、BYOD、企业设备、员工、承包商和访客提供基于角色和设备的安全网络访问控制。

#### 可信证书存储配置

1. 从 axis.com 下载 Axis 特定的 IEEE 802.1AR 证书链。
2. 将 Axis 特定的 IEEE 802.1AR 根 CA 和中间 CA 证书链上传到受信任的证书存储中。
3. 启用 ClearPass Policy Manager 以通过 IEEE 802.1X EAP–TLS 对安讯士设备进行身份验证。
4. 在使用字段中选择 EAP。这些证书用于 IEEE 802.1X EAP–TLS 身份验证。



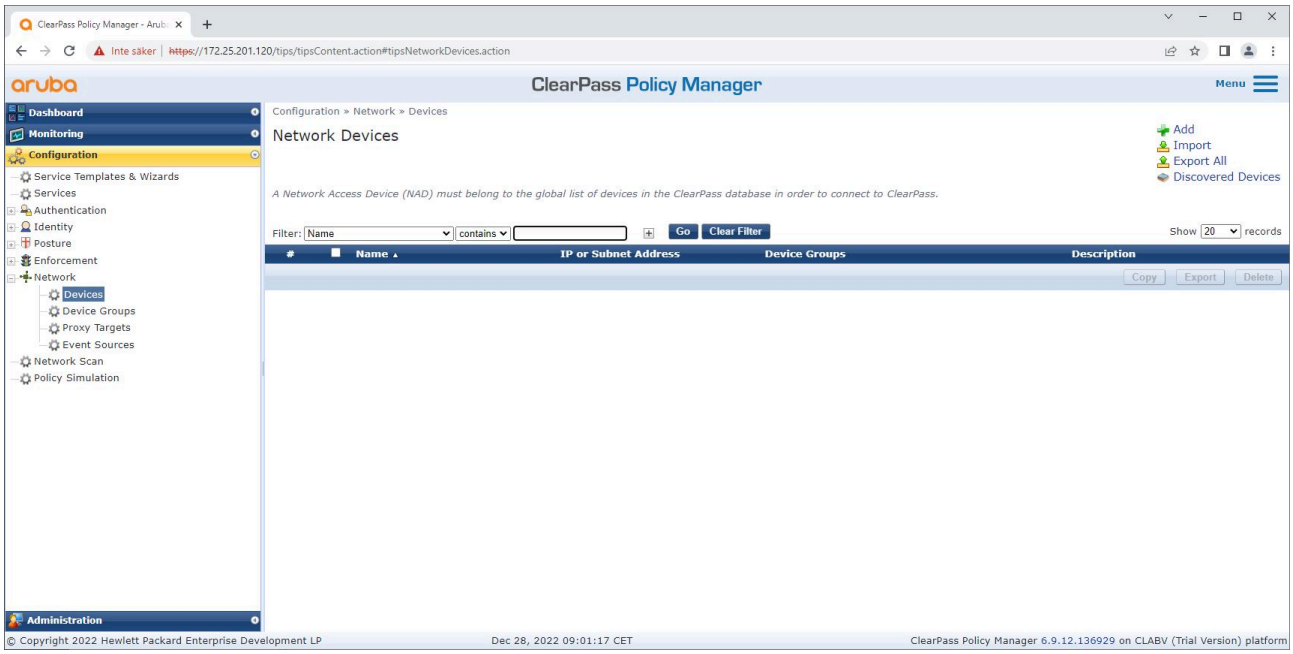

*将特定于 Axis 的 IEEE 802.1AR 证书上传到 ClearPass Policy Manager 的可信证书存储区。*



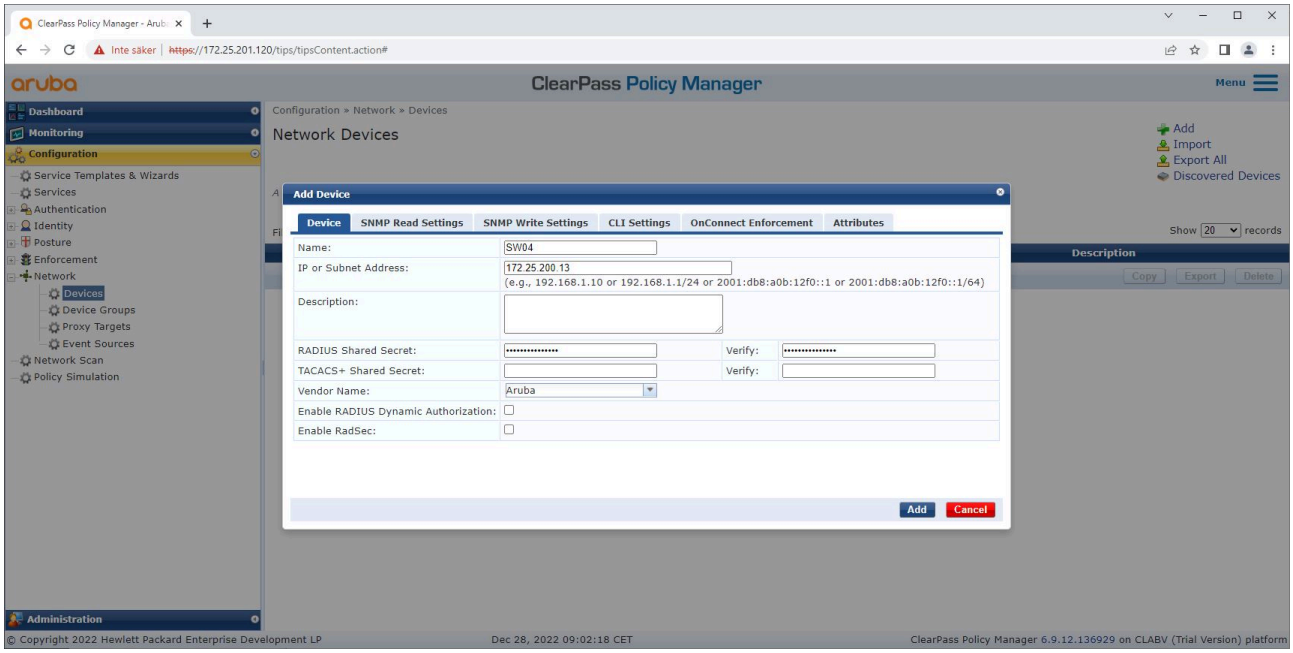

*ClearPass Policy Manager 中的可信证书存储包含特定于 Axis 的 IEEE 802.1AR 证书链。*

## 网络设备/组配置

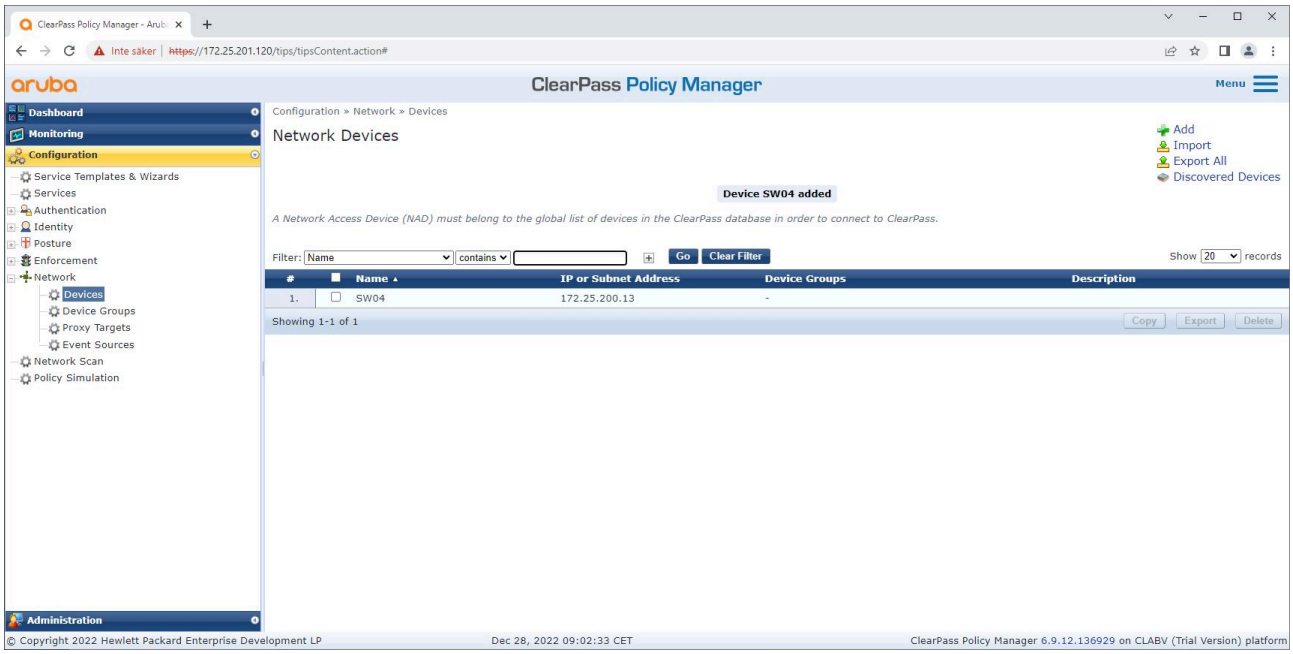
1. 将受信任的网络访问设备（例如 HPE Aruba Networking 访问交换机）添加到 ClearPass Policy Manager。ClearPass Policy Manager 需要知道网络中的哪些接入交换机用于 IEEE 802.1X 通信。另请注意，RADIUS 共享密钥必须与特定交换机 IEEE 802.1X 配置匹配
2. 使用网络设备组配置将多个可信网络访问设备分组。设备分组可简化策略配置。



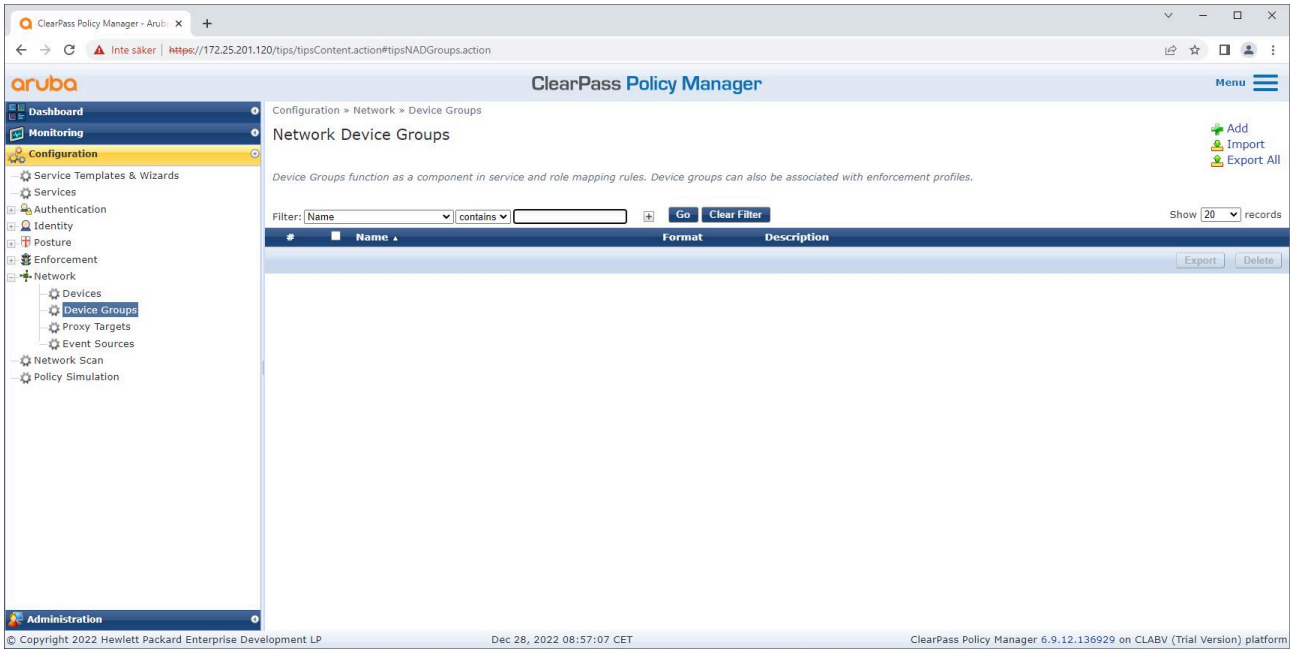

*ClearPass Policy Manager 中的可信网络设备接口。*



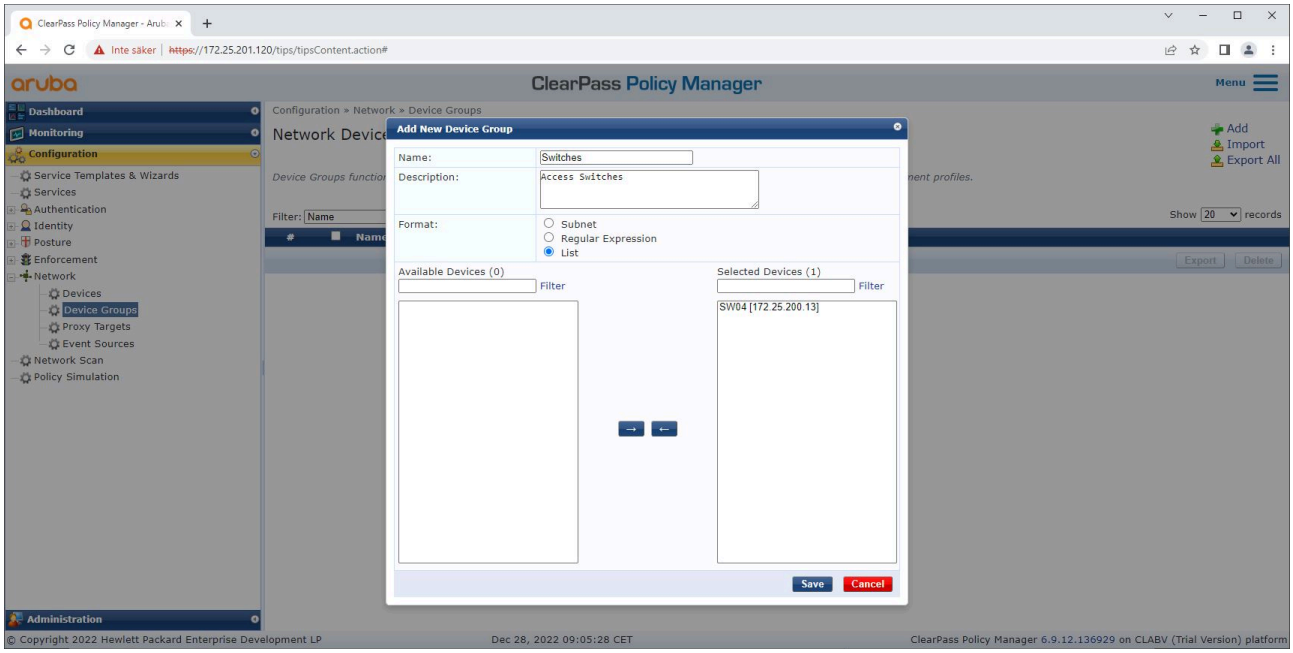

*在 ClearPass Policy Manager 中将 HPE Aruba Networking 接入交换机添加为可信设备。请注意，RADIUS 共享密钥必须与特定交换机 IEEE 802.1X 配置匹配。*



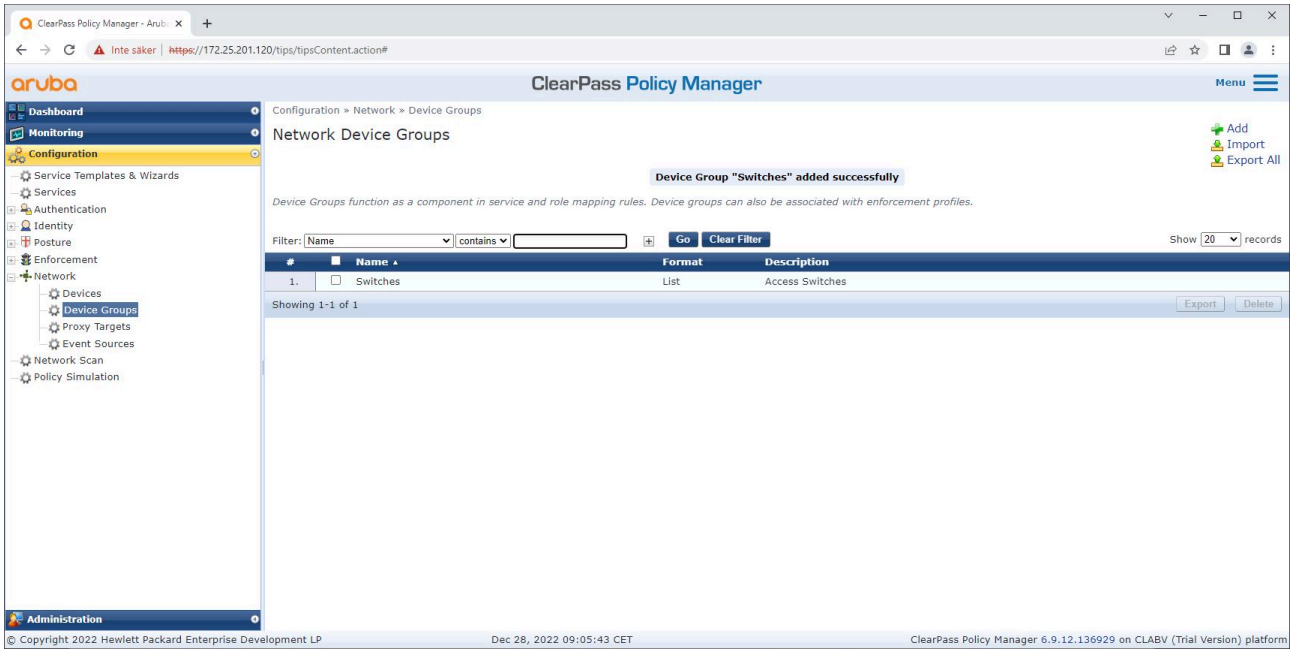

*配置了一台受信任网络设备的 ClearPass Policy Manager。*




*ClearPass Policy Manager 中的可信网络设备组接口。*




*将受信任的网络访问设备添加到 ClearPass Policy Manager 中的新设备组中。*

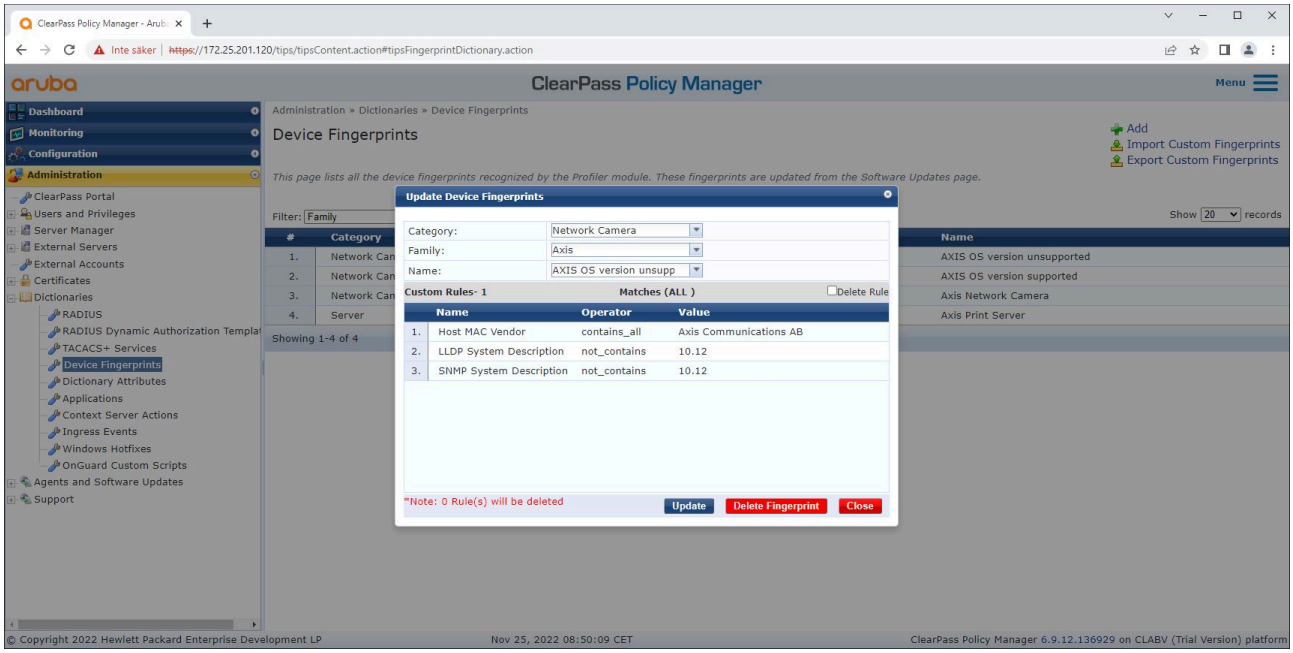



*ClearPass Policy Manager 已配置一个网络设备组，其中包括一台或多台受信任的网络设备。*

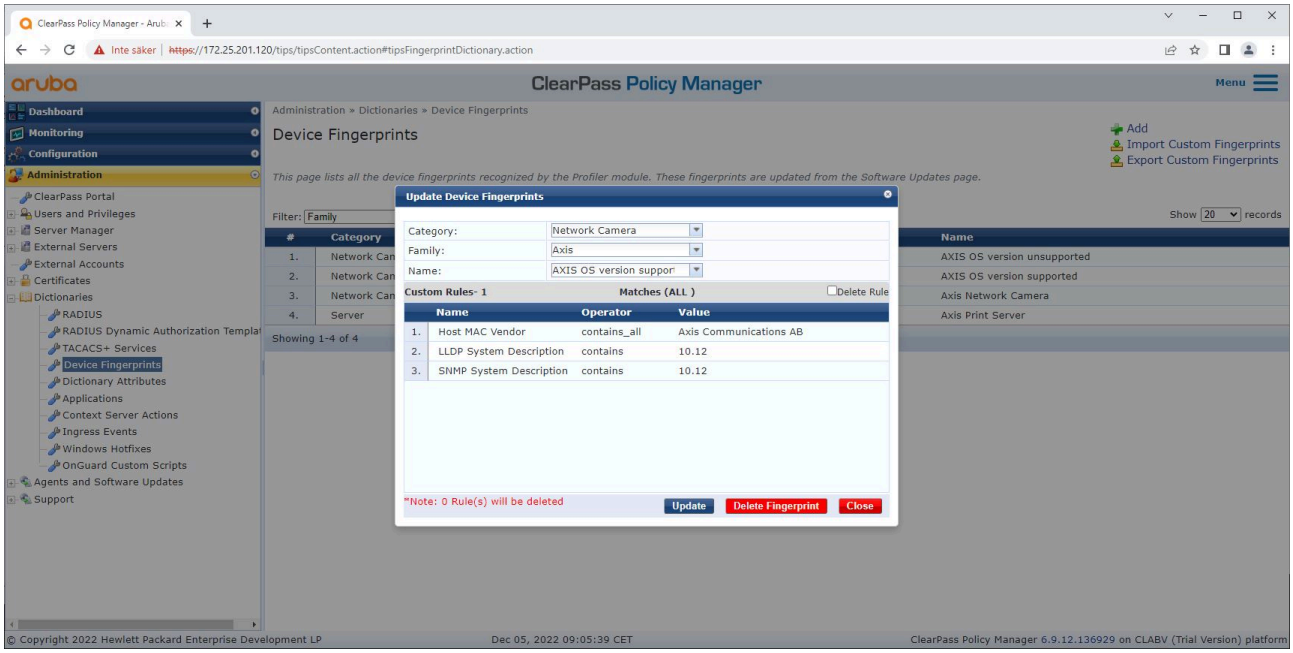
## 设备指纹配置

安讯士设备可通过网络发现功能，分发设备专属信息，例如：MAC地址和设备软件版本。您可以使用此信息在 ClearPass Policy Manager 中创建、更新或管理设备指纹。您还可以根据 AXIS OS 版本授予或拒绝访问权限。

1. 转往**管理 > 词典 > 设备指纹**。
2. 选择现有的设备指纹或创建新的设备指纹。
3. 进行设备指纹设置。




*ClearPass Policy Manager 中的设备指纹配置。在本示例中，不支持运行非 10.12 版本 AXIS OS 的安讯士设备。*



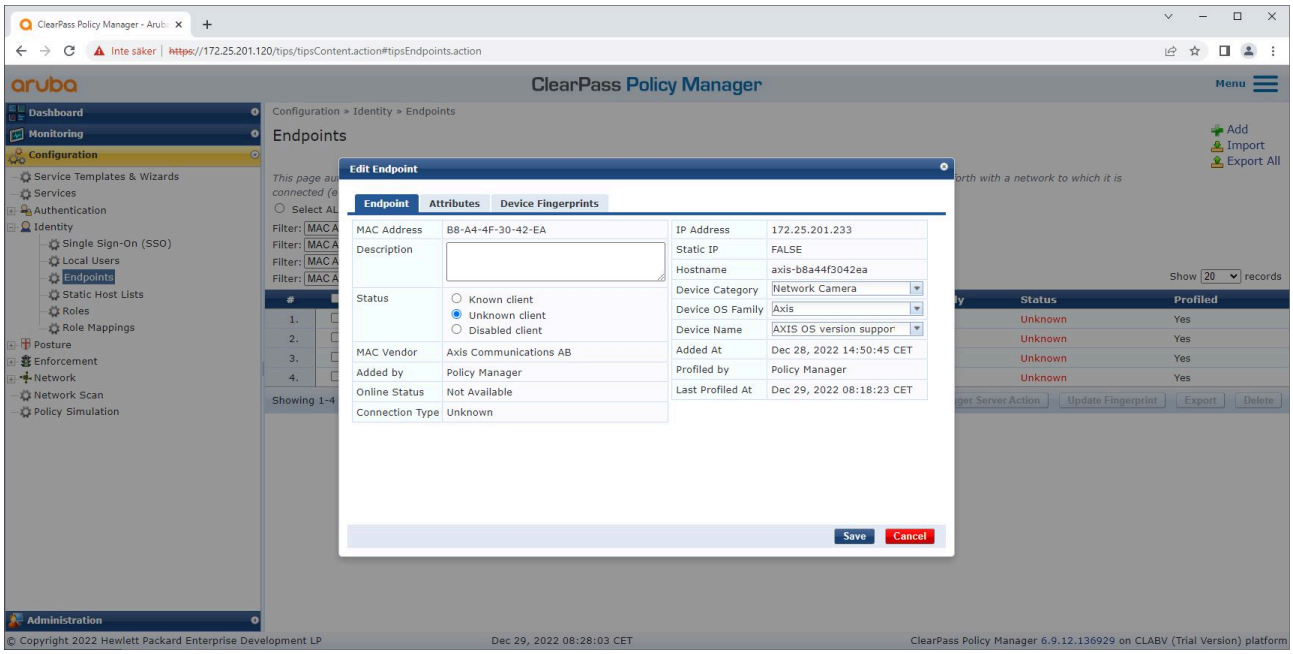

*ClearPass Policy Manager 中的设备指纹配置。在本示例中，支持运行非 10.12 版本 AXIS OS 的安讯士设备。*

有关 ClearPass Policy Manager 收集的设备指纹的信息可以在端点部分找到。

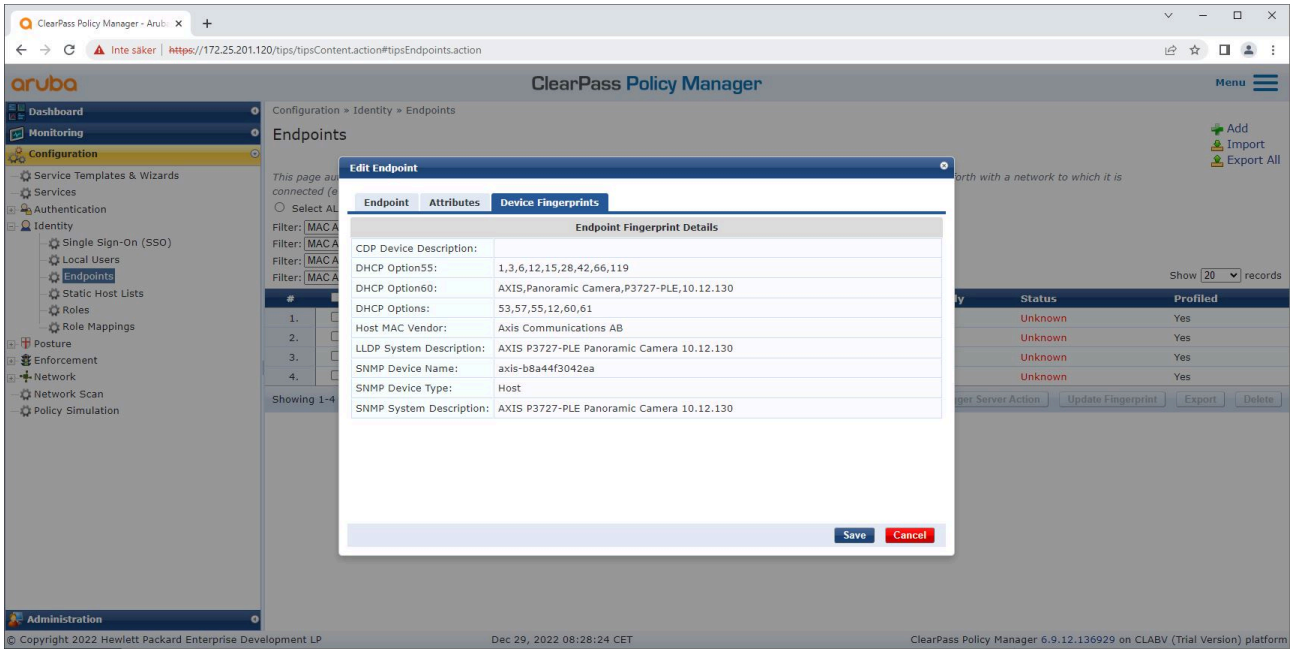
1. 转往**配置 > 身份 > 端点**。
2. 选择要浏览的设备。
3. 单击**设备指纹**选项。

注意

默认情况下，SNMP 在安讯士设备中处于禁用状态，并从HPE Aruba Networking 接入交换机收集。




*由 ClearPass Policy Manager 配置的安讯士设备。*

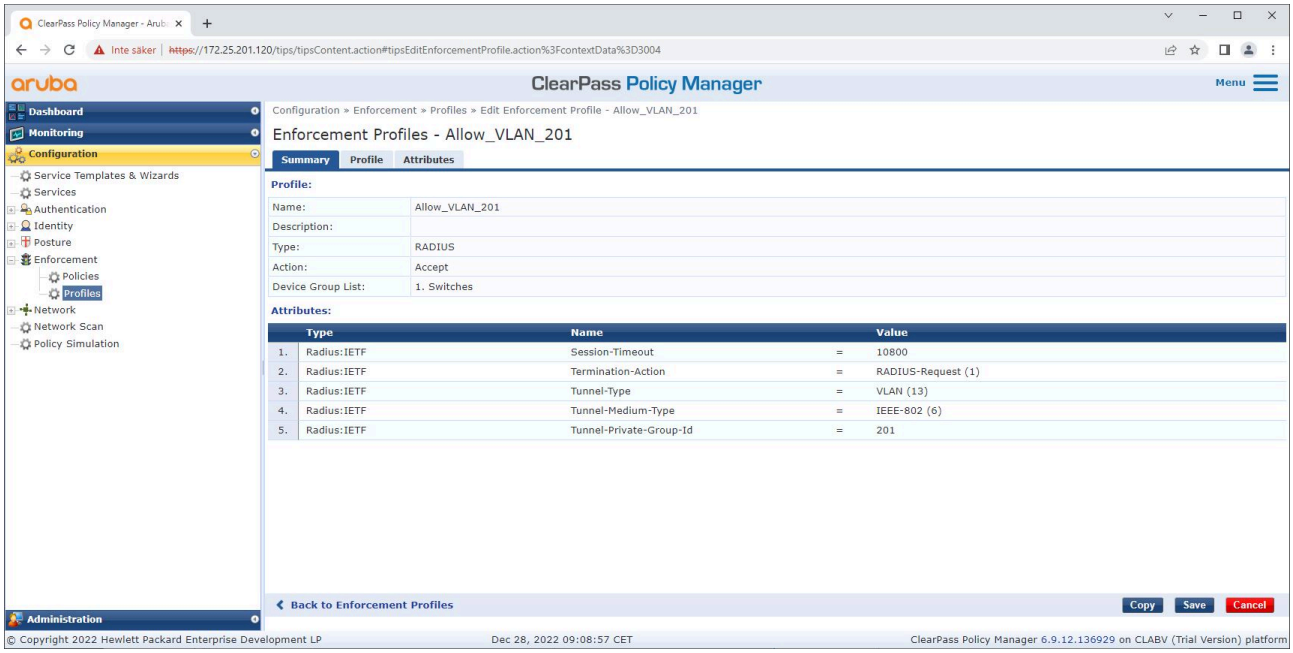



*配置文件的安讯士设备的详细设备指纹。请注意，安讯士设备默认禁用简单网络管理协议 (SNMP)。在出厂默认状态下，安讯士设备共享LLDP、CDP及DHCP特定的发现信息。这些信息由 HPE Aruba Networking 接入交换机转发给 ClearPass 策略管理器。*

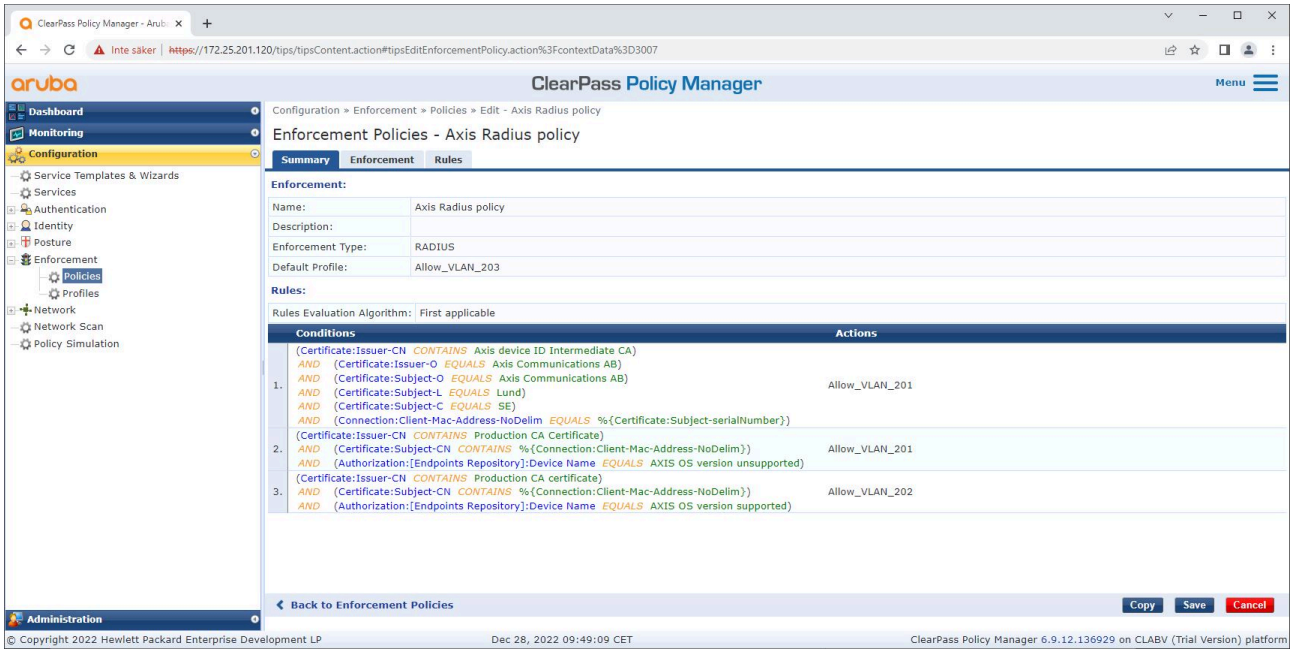
## 强制配置文件配置

强制配置文件允许 ClearPass Policy Manager 将特定 VLAN ID 分配给交换机上的访问端口。这是一项基于策略的决策，适用于设备组“交换机”中的网络设备。所需的强制配置文件数量取决于使用的虚拟局域网 (VLAN) 数量。我们的设置包含三个虚拟局域网（VLAN 201、202、203），分别对应三个强制配置文件。

配置完 VLAN 的强制配置文件后，就可以自行配置强制策略了。ClearPass Policy Manager 中的强制策略配置定义是否根据四个示例策略配置文件授予 Axis 设备访问 HPE Aruba Networking 网络的权限。




*允许访问 VLAN 201 的强制配置文件示例。*




*ClearPass Policy Manager 中的强制策略配置。*

四项强制策略及其行动如下：

### 拒绝网络访问

当未进行 IEEE 802.1X 网络访问控制认证时，网络将被拒绝访问。

### 访客网络（VLAN 203）

如果 IEEE 802.1X 网络访问控制身份验证失败，则安讯士设备将被授予访问受限、隔离网络的权限。此时需要对设备进行手动检查，以决定采取适当的响应。

### 配置网络 (VLAN 201)

安讯士设备被授予对配置网络的访问权限。这是为了通过以下方式提供安讯士设备管理功能：*AXIS Device Manager* 和 *AXIS Device Manager Extend*。它还可以使用 AXIS OS 更新、生产级证书和其他配置来配置安讯士设备。以下条件已由 ClearPass Policy Manager 验证：

- 设备的 AXIS OS 版本。
- 设备的 MAC 地址与供应商特定的 MAC 地址方案与安讯士设备 ID 证书的序列号属性相匹配。
- 安讯士设备 ID 证书是可验证的，并且与 Axis 特定属性（例如颁发者、组织、位置及国家/地区）相匹配。

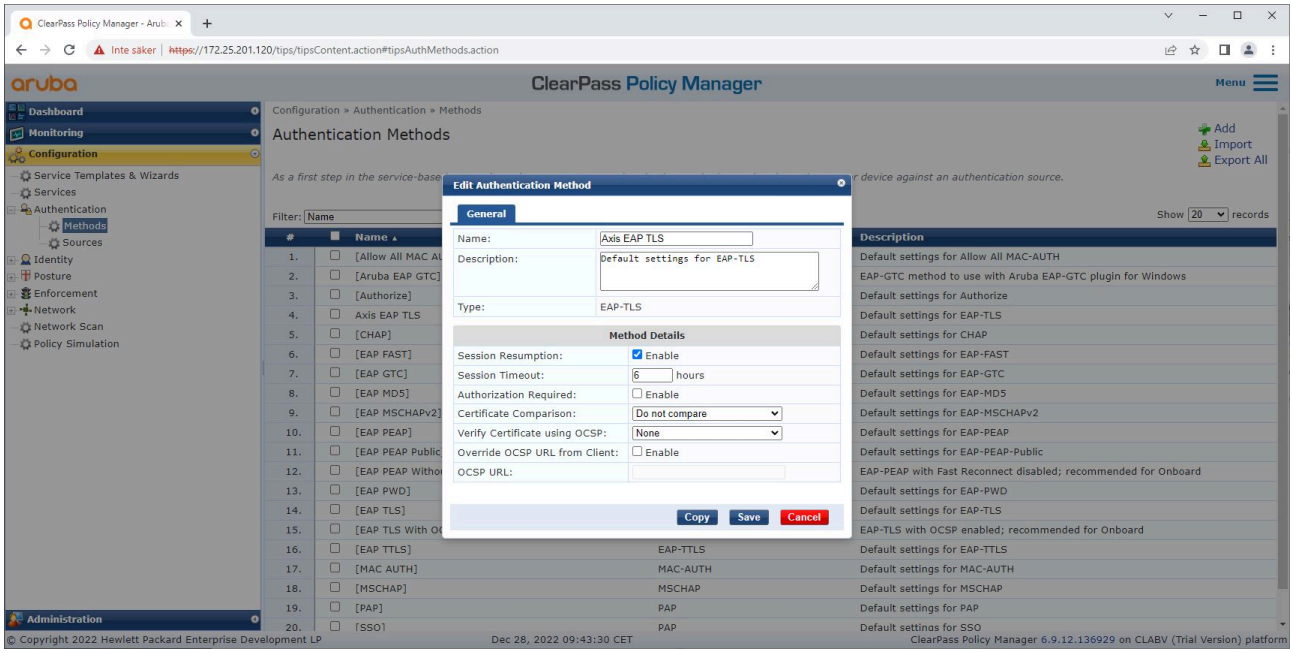
### 生产网络 (VLAN 202)

安讯士设备被授予对生产网络的访问权限，其将在该生产网络中运行。从配置网络 (VLAN 201) 内完成设备配置后，将被授予访问权限。以下条件已由 ClearPass Policy Manager 验证：

- 设备的 AXIS OS 版本。
- 设备的 MAC 地址与供应商特定的 MAC 地址方案与安讯士设备 ID 证书的序列号属性相匹配。
- 生产级证书可由受信任的证书存储区验证。

### 认证方式配置

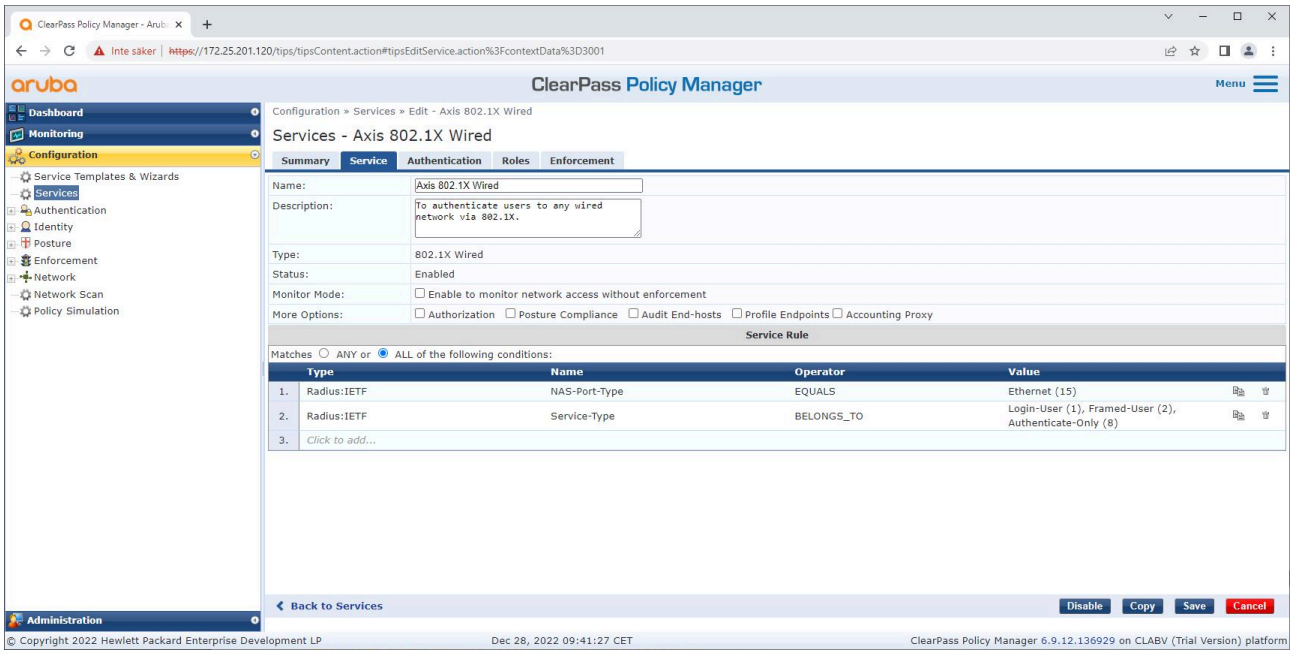
身份验证方法定义了安讯士设备尝试在网络上对自身进行身份验证的方式。理想的方法是 IEEE 802.1X EAP–TLS，因为支持 Axis Edge Vault 的安讯士设备默认启用了 IEEE 802.1X EAP–TLS。



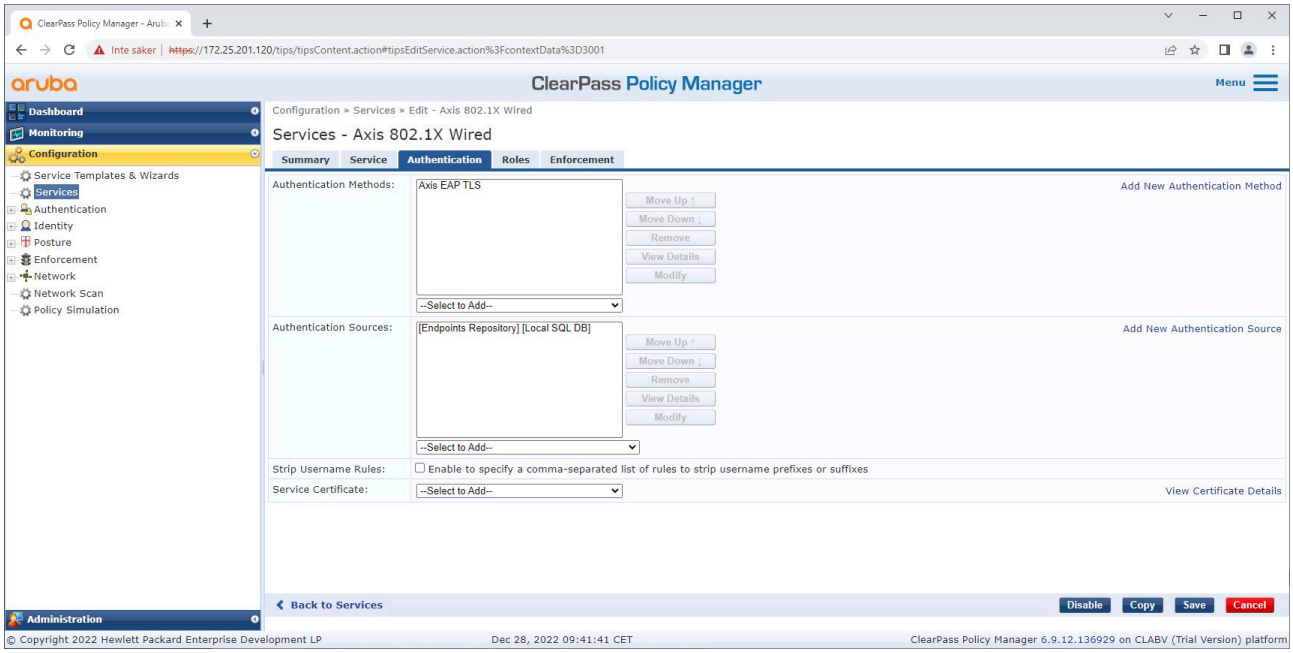

*ClearPass Policy Manager 的身份验证方法接口，其中定义了安讯士设备的 EAP–TLS 身份验证方法。*

## 设备配置

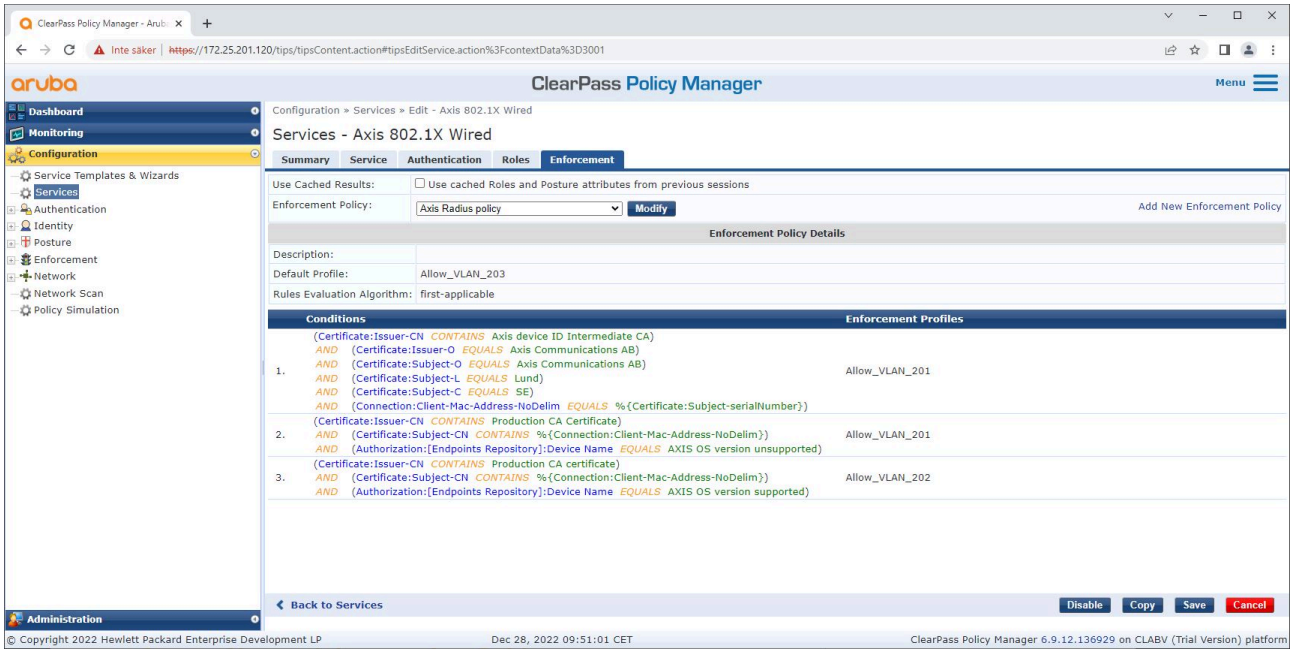
在**服务**界面中，配置步骤合并为一项服务，用于处理 HPE Aruba Networking 网络中安讯士设备的身份验证和授权。




*创建了一项专用的安讯士服务，采用 IEEE 802.1X 作为连接方式。*




*为该服务配置先前创建的 EAP–TLS 身份验证方法。*




*为该服务配置先前创建的强制策略。*

## HPE Aruba Networking 接入交换机

安讯士设备可以直接连接到支持 PoE 的接入交换机，也可以通过兼容的 Axis PoE 中跨连接。要将安讯士设备安全地接入 HPE Aruba Networking 网络，必须将接入交换机配置为 IEEE 802.1X 通信。安讯士设备将 IEEE 802.1x EAP–TLS 通信中继到充当 RADIUS 服务器的 ClearPass Policy Manager。

**注意**

还为安讯士设备配置了 300 秒的定期重新验证，以提高整体端口访问安全性。

本示例展示了 HPE Aruba Networking 接入交换机的全局和端口配置。

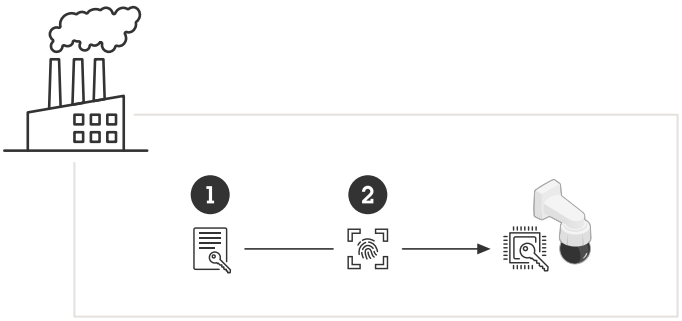
```
radius-server host MyRADIUSIPAddress key "MyRADIUSKey"

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
```

# 配置 Axis

## Axis 网络设备

支持 *Axis Edge Vault* 的安讯士设备均配备名为安讯士设备 ID 的安全设备标识。安讯士设备 ID 基于国际 IEEE 802.1AR 标准，该标准通过 IEEE 802.1X 定义了自动化安全设备确认与网络板载的方法。



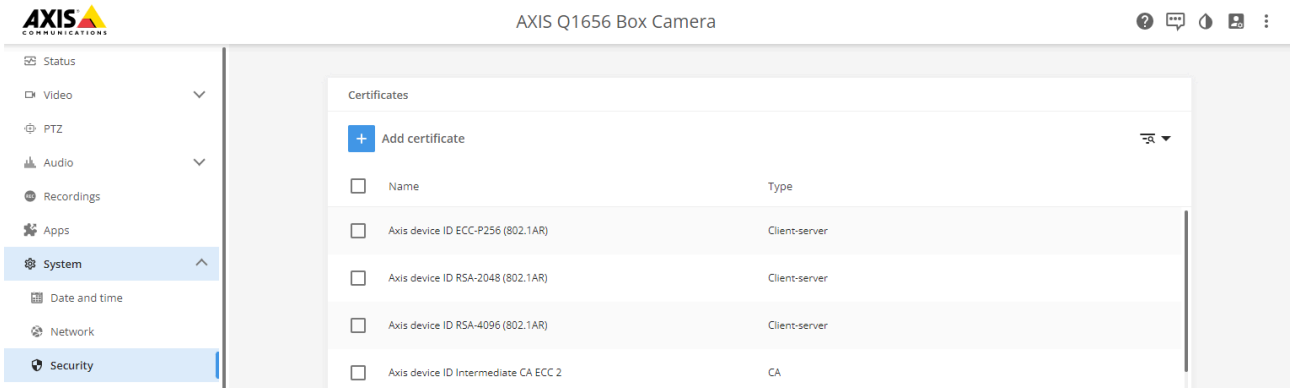

*安讯士设备在制造时带有符合 IEEE 802.1AR 标准的安讯士设备 ID 证书，用于可信设备身份服务*

1 *安讯士设备ID基础设施 (PKI)*
2 *安讯士设备ID*

安讯士设备的安全元件提供的受硬件保护的安全密钥库在出厂时就预配了设备单独的证书和相应的密钥（Axis 设备 ID），可在全局范围内证明安讯士设备的身份真实性。*Axis Product Selector* 可用于了解哪些安讯士设备支持 Axis Edge Vault 和安讯士设备 ID。

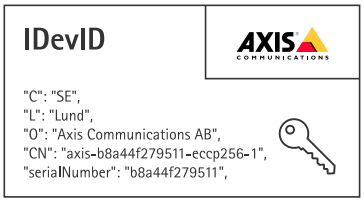
注意

安讯士设备的序列号是其 MAC 地址。




*处于出厂默认状态的安讯士设备的证书存储以及安讯士设备 ID。*

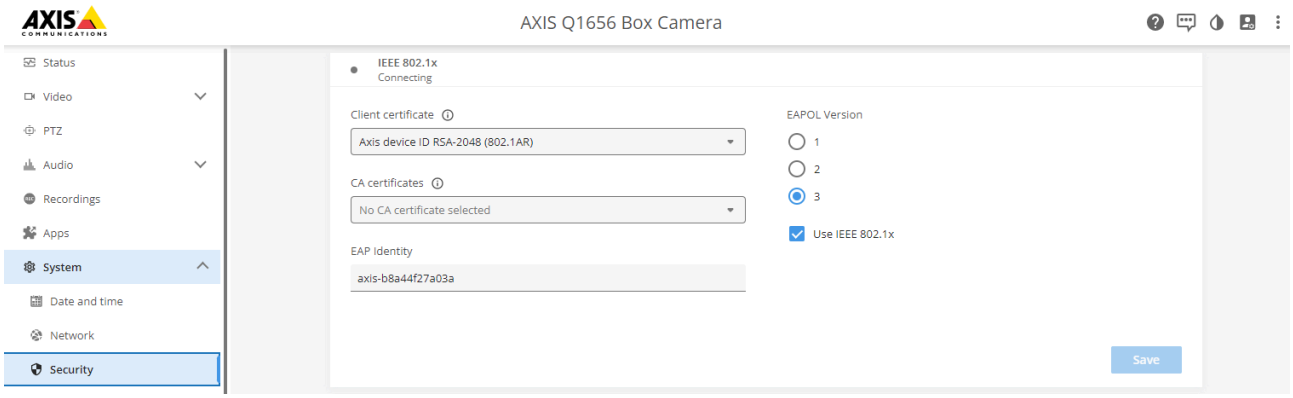
符合 IEEE 802.1AR 标准的 Axis 设备 ID 证书包含有关序列号的信息和其他供应商特定信息。该信息由 ClearPass Policy Manager 用于进行分析和决策以授予网络访问权限。以下信息可从安讯士设备 ID 证书中获取




| | |
|---|---|
| 国家/地区 | SE |
| 位置 | 隆德 |
| 发行人组织 | Axis Communications AB |
| 发行人通用名称 | 安讯士设备 ID 中介 |

| | |
|---|---|
| 组织 | Axis Communications AB |
| 常用名称 | Axis-b8a44f279511-eccp256-1 |
| 序列号 | b8a44f279511 |

通用名称由安讯士公司名称、设备序列号后面接加密算法（ECC P256、RSA 2048、RSA 4096）组合构成。自 AXIS OS 10.1（2020-09）起，默认情况下启用 IEEE 802.1X，并预先配置安讯士设备 ID。这使设备能够在支持 IEEE 802.1X 的网络上对自身进行身份验证。




*安讯士设备处于出厂默认状态，启用 IEEE 802.1X 并预先选择安讯士设备 ID 证书。*

## AXIS Device Manager

*AXIS Device Manager* 和 *AXIS Device Manager Extend* 可在网络上使用，以经济高效的方式配置和管理多台安讯士设备。AXIS Device Manager 是一款基于 Microsoft Windows® 的应用程序，需在网络中的机器上进行本地安装；而 AXIS Device Manager Extend 则依托云基础设施实现多站点设备管理。两者均设备提供简单的管理和配置功能，例如：

- 安装 AXIS OS 更新。
- 应用网络安全配置，例如：安全超文本传输协议 (HTTPS) 和 IEEE 802.1X 证书。
- 配置特定设备的设置，例如图像设置等。

## 安全网络操作 – IEEE 802.1AE MACsec

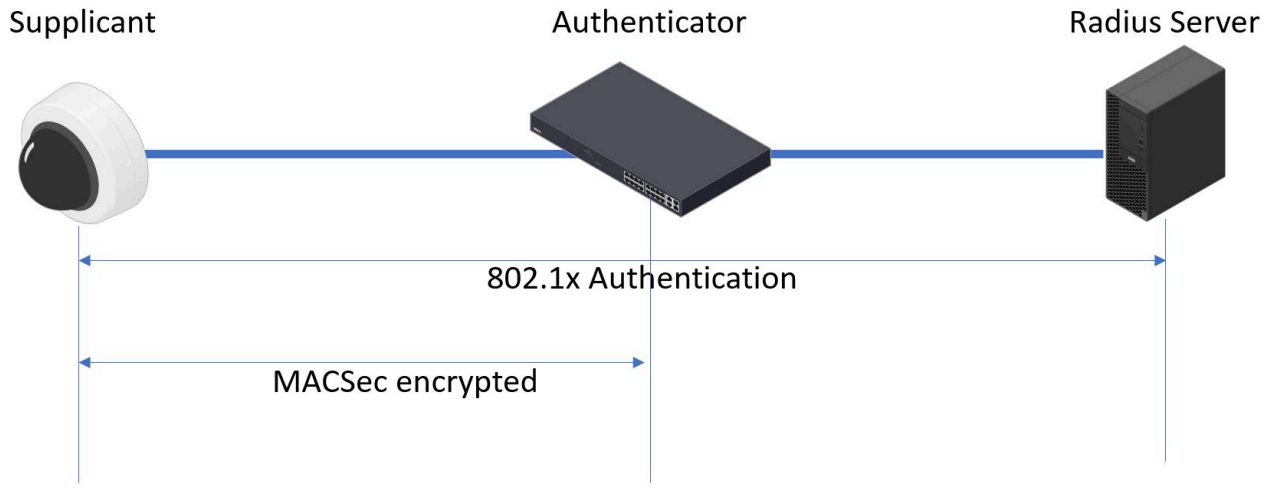
要观看此视频，请转到本文档的网页版本。

*采用 IEEE 802.1AE MACsec 第 2 层安全性的零信任网络加密*

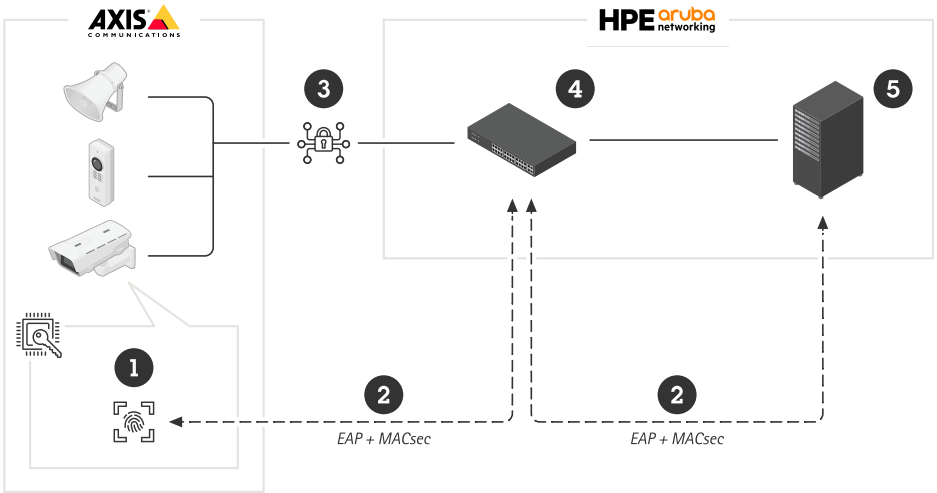
IEEE 802.1AE MACsec（媒体访问控制安全）是一种定义明确的网络协议，它以加密方式保护网络第 2 网络层上的点对点以太网链路。它确保两个主机之间数据传输的机密性和完整性。

IEEE 802.1AE MACsec 标准描述了两种操作模式：

- 手动配置预共享密钥/静态 CAK 模式
- 自动主会话/动态 CAK 模式使用 IEEE 802.1X EAP–TLS




在 AXIS OS 10.1 (2020–09) 及更高版本中，对于兼容安讯士设备 ID 的设备，默认启用 IEEE 802.1X。在 AXIS OS 11.8 及更高版本中，我们支持采用 IEEE 802.1X EAP–TLS 的 MACsec 自动动态模式，该模式默认处于启用状态。当您使用出厂默认值连接安讯士设备时，IEEE 802.1X 进行网络身份验证，成功后还会尝试 MACsec 动态 CAK 模式。



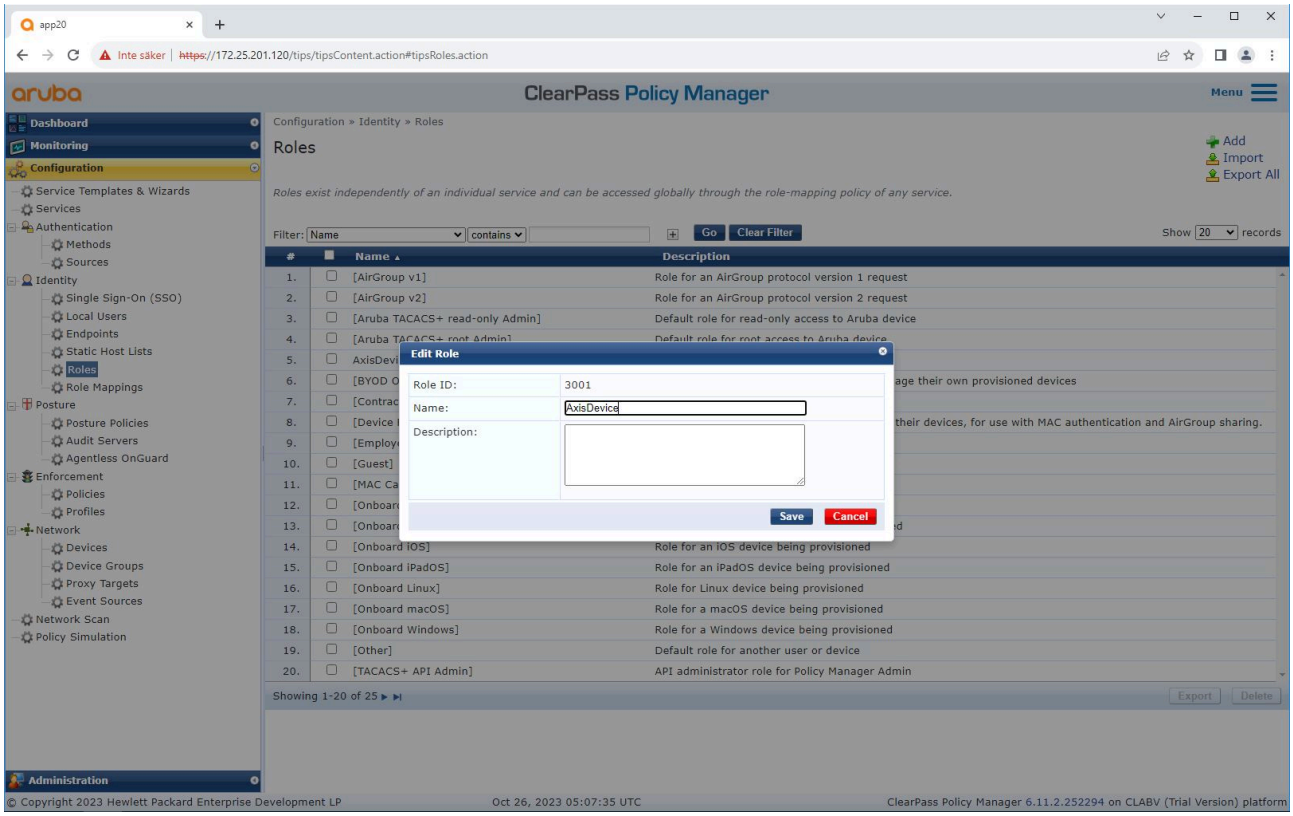

安全存储的安讯士设备 ID (1) – 与 IEEE 802.1AR 兼容的一种安全设备身份 – 用于通过 IEEE 802.1X EAP–TLS 基于端口的网络访问控制 (2) 对 网络（4、5）进行身份验证。通过 EAP–TLS 会话，自动交换 MACsec 密钥以建立安全链路 (3)，从而保护从安讯士设备到HPE Aruba Networking 接入交换机的网络流量。

IEEE 802.1AE MACsec 要求 HPE Aruba Networking 接入交换机和 ClearPass Policy Manager 配置准备。无需在安讯士设备上进行配置即可允许 IEEE 802.1AE通过 EAP–TLS 进行 MACsec 加密通信。

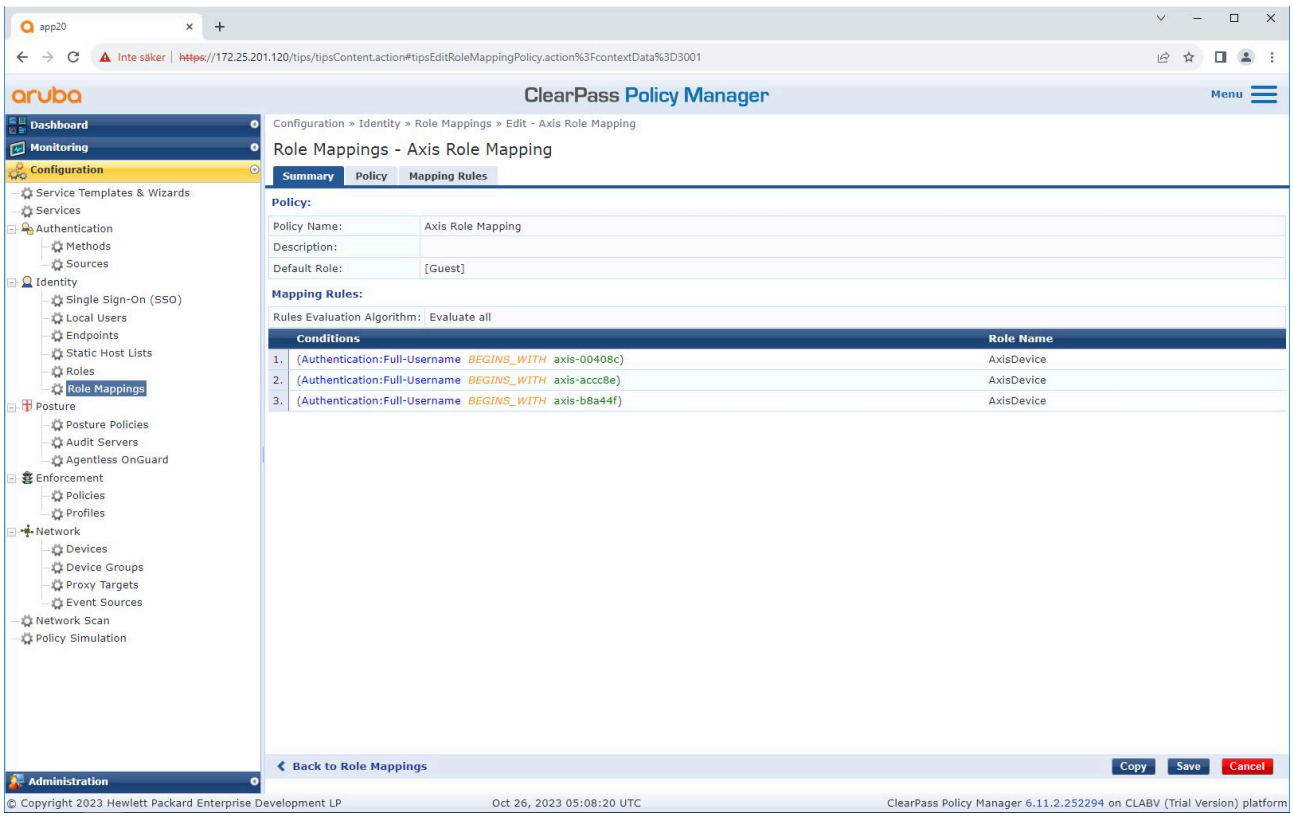
如果 HPE Aruba Networking 接入交换机不支持使用 EAP–TLS 的 MACsec，则可以使用预共享密钥模式并手动配置。

## HPE Aruba Networking ClearPass Policy Manager

### 角色和角色映射策略



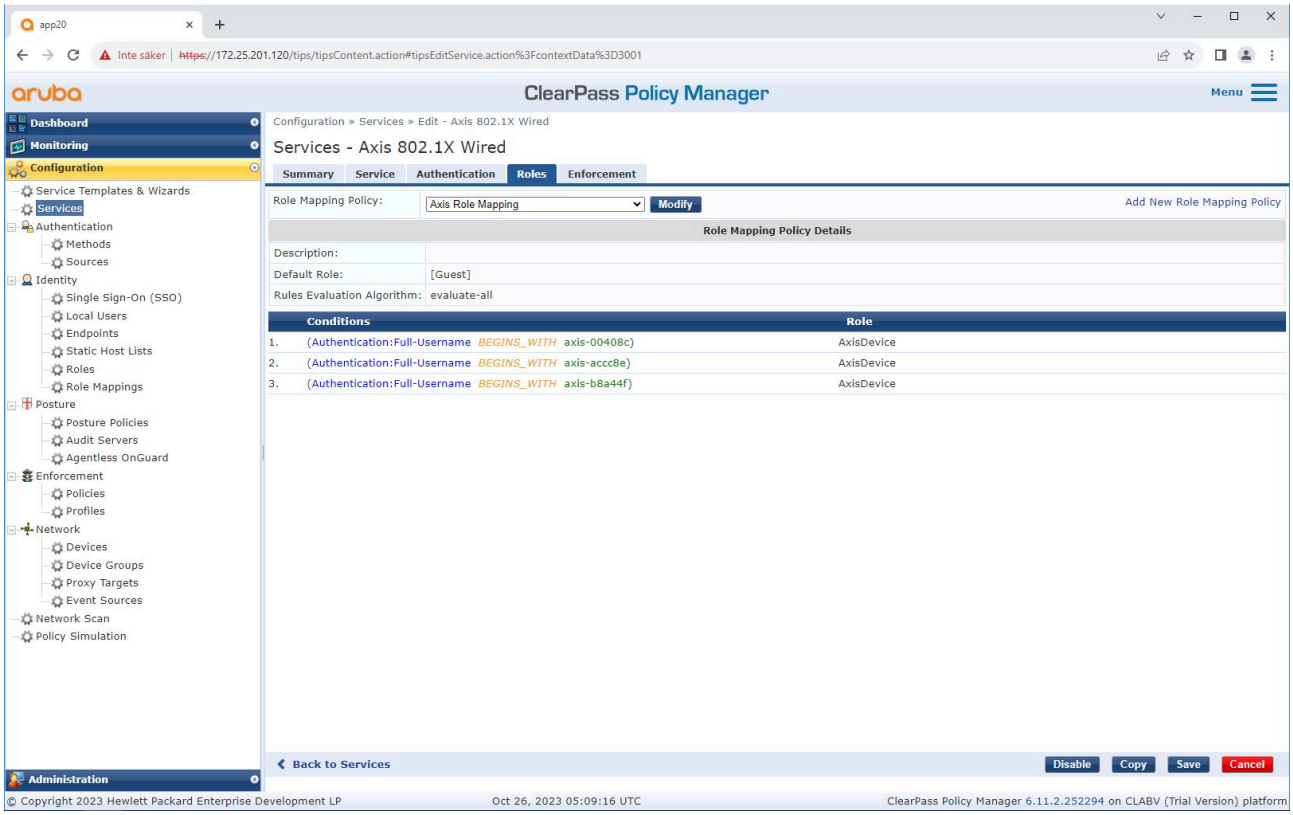

*添加安讯士设备的角色名称。该名称是接入交换机配置中的端口访问角色名称。*



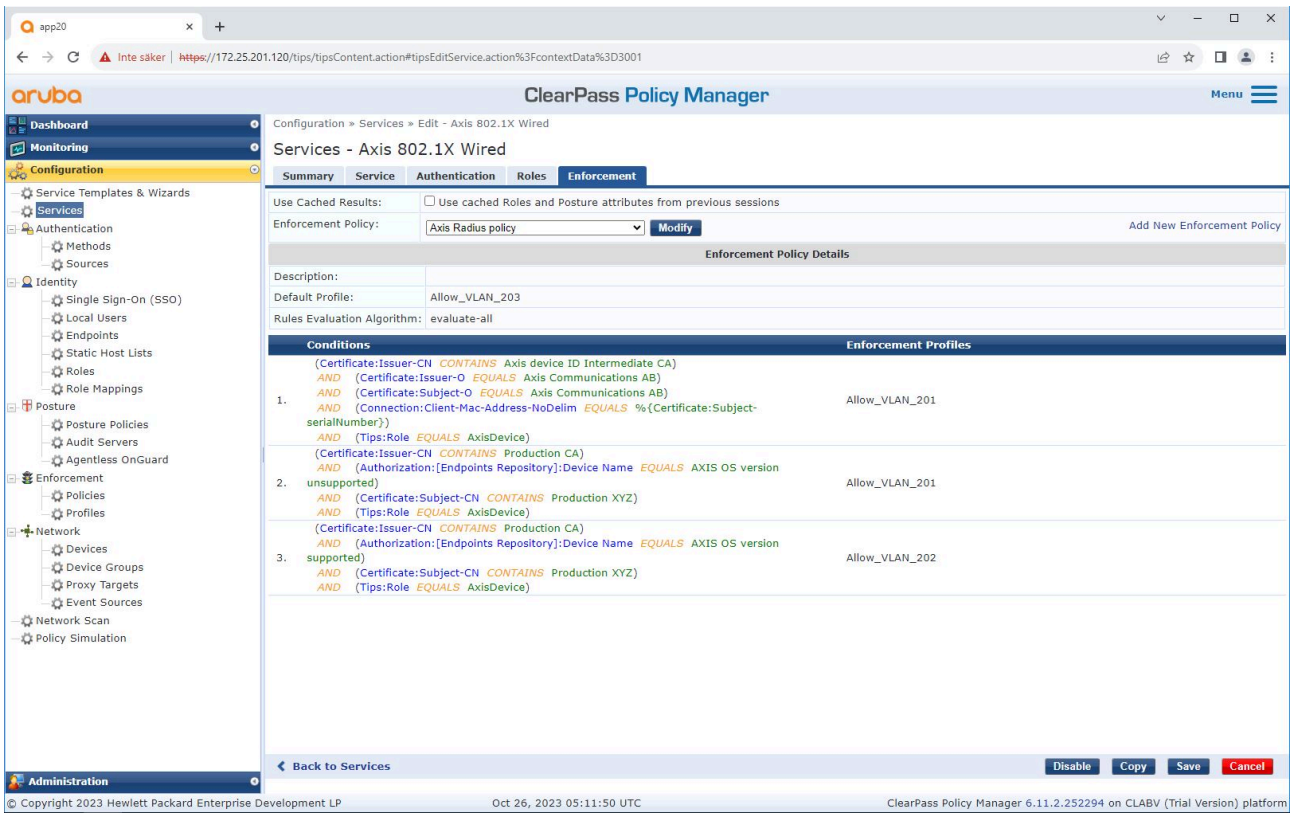

*为先前创建的安讯士设备角色添加 Axis 角色映射策略。设备映射到安讯士设备角色需要定义的条件。如果不满足条件，设备成为 [Guest] 角色的一部分。*

默认情况下，安讯士设备使用 EAP 身份格式“axis-序列号”。安讯士设备的序列号即为其 MAC 地址。例如“axis-b8a44f45b4e6”。

## 设备配置

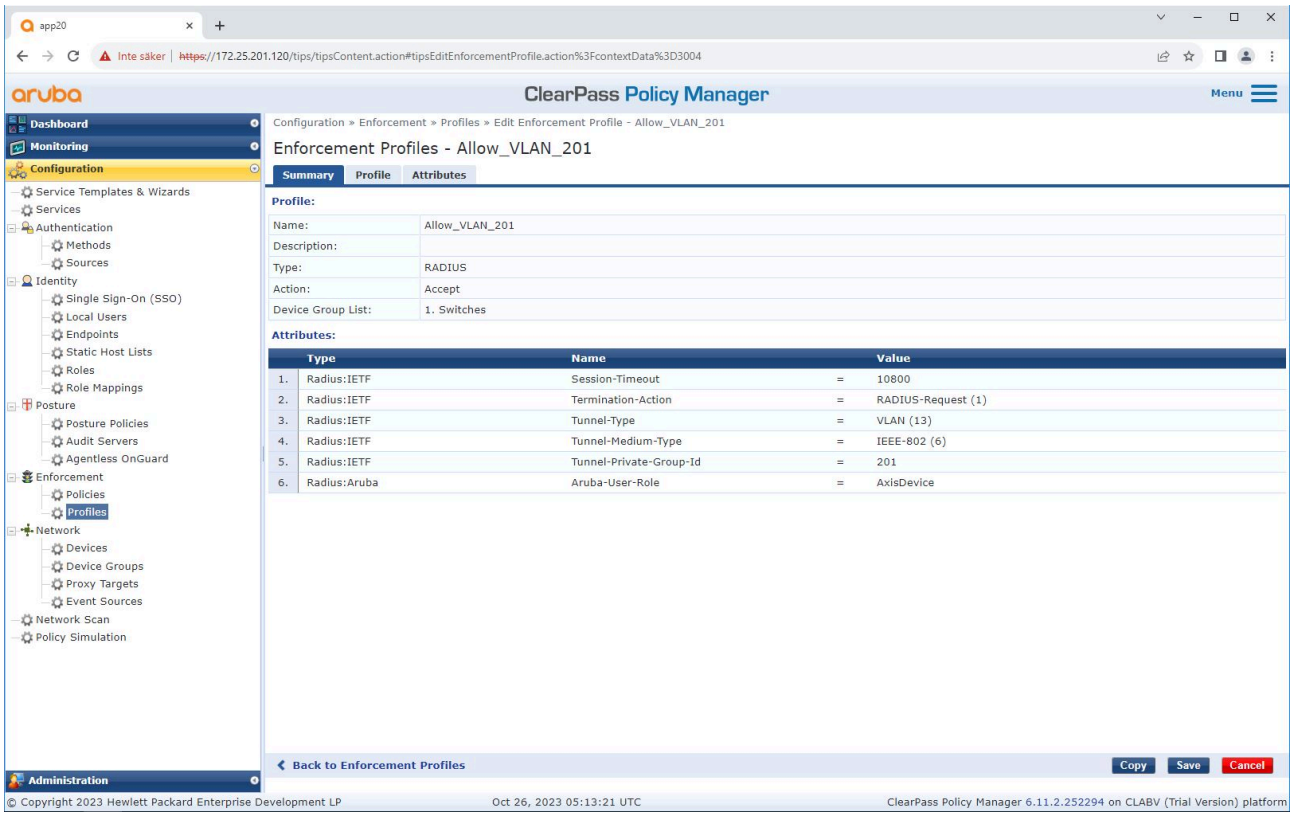



*将之前创建的 Axis 角色映射策略添加到将 IEEE 802.1X 定义为 Axis 设备加入的连接方法的服务中。*




*将 Axis 角色名称作为条件添加到现有策略定义中。*

## 强制配置文件




*将 Axis 角色名称作为属性添加到在 IEEE 802.1X 加入服务中分配的强制配置文件。*

## HPE Aruba Networking 接入交换机

除了 中描述的安全接入配置之外，请参阅下面 HPE Aruba Networking 接入交换机的端口配置示例以配置 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
```

## 旧版板载 – MAC 身份验证

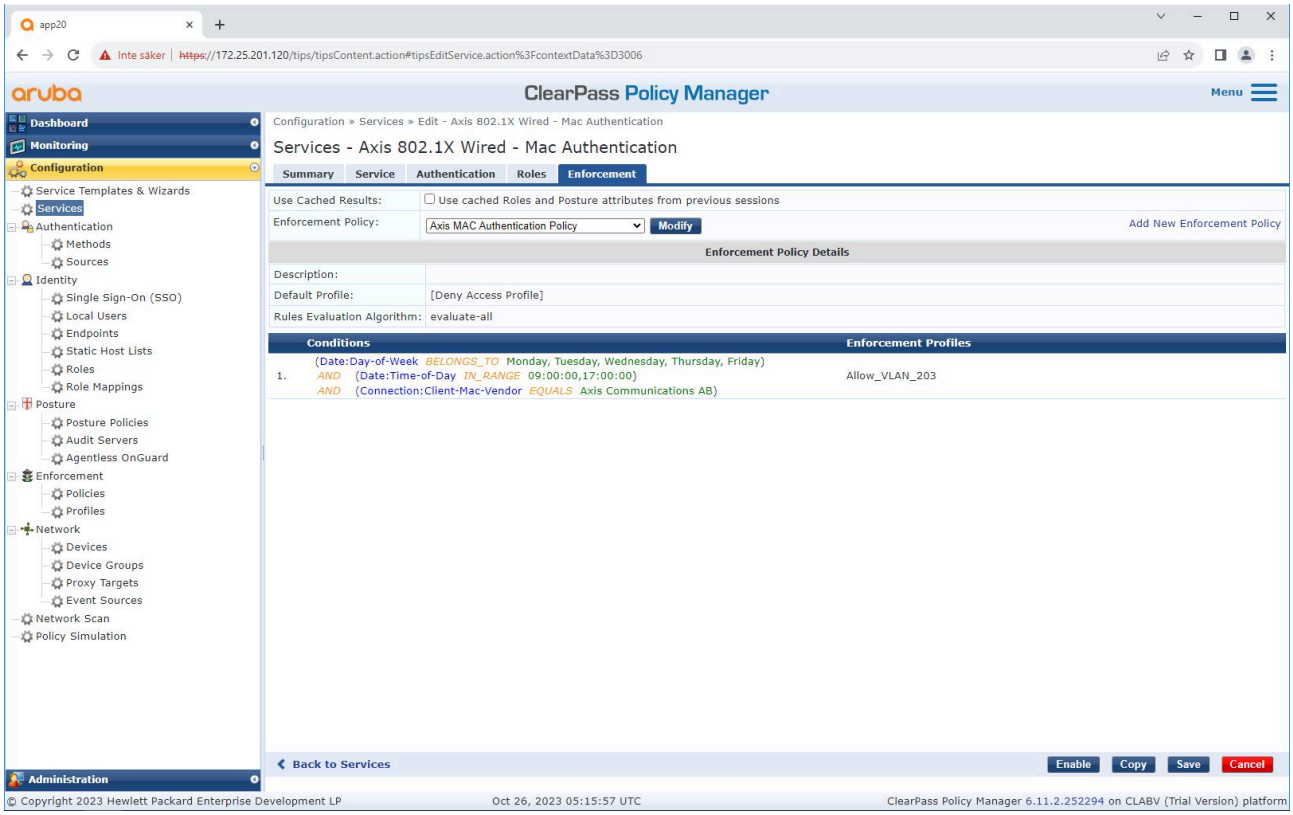
您可以使用 MAC 身份验证绕过（MAB）来板载不支持 IEEE 802.1AR 的安讯士设备，使用安讯士设备 ID 证书进行注册，以及在出厂默认状态下启用 IEEE 802.1X。如果 802.1X 板载失败，ClearPass Policy Manager 会验证 Axis 设备的 MAC 地址并授予对网络的访问权限。

MAB 需要接入交换机和 ClearPass Policy Manager 配置准备。无需在安讯士设备上进行任何配置即可允许 MAB 以实现接入。

### HPE Aruba Networking ClearPass Policy Manager

#### 强制政策

ClearPass Policy Manager 中的强制策略配置定义是否根据以下两个示例策略条件授予安讯士设备访问 HPE Aruba Networking 网络的权限。




#### 拒绝网络访问

如果安讯士设备不符合配置的强制策略，它会被拒绝访问网络。

#### 访客网络（VLAN 203）

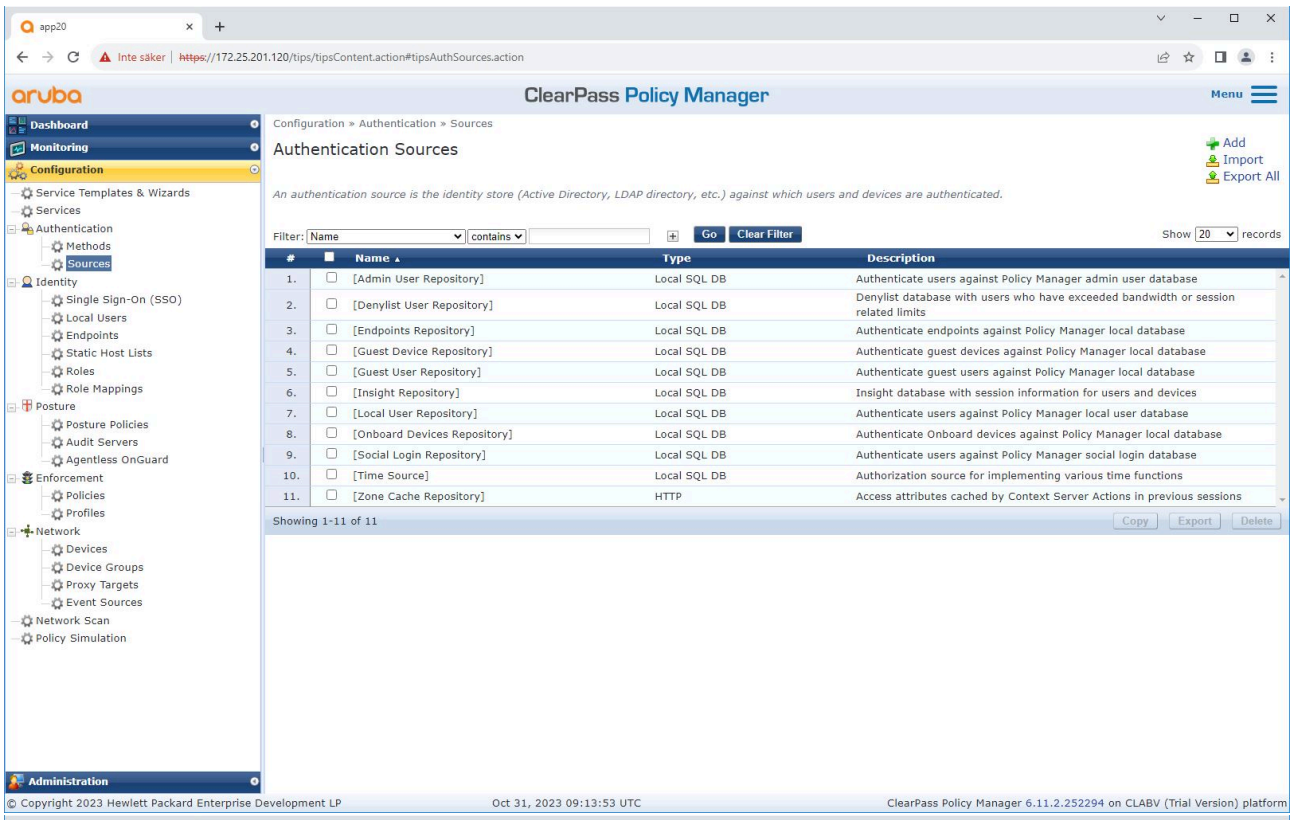
如果满足以下条件，安讯士设备将被授予访问受限、隔离网络的权限：

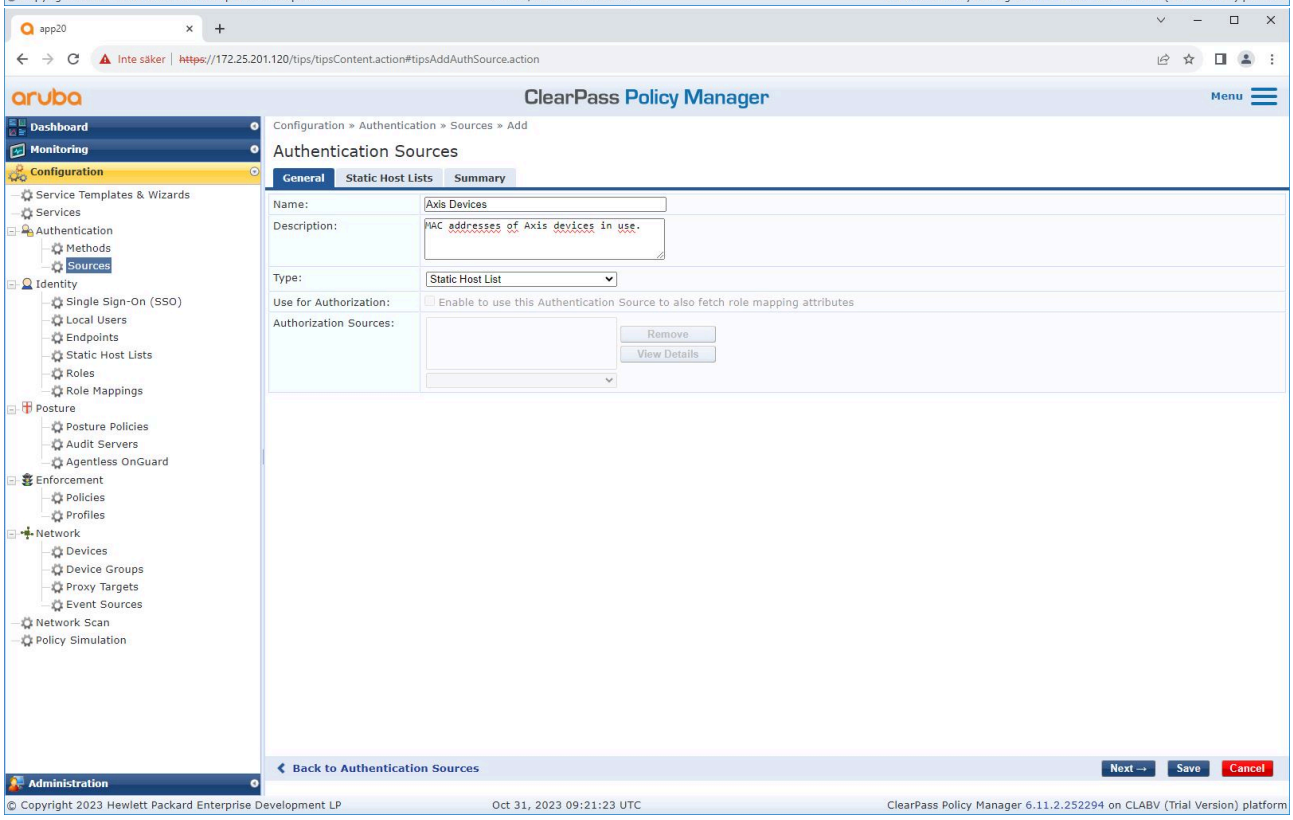
- 当天为工作日，即周一至周五
- 时间为上午9点至下午5点。
- MAC 地址供应商与安讯士公司匹配。

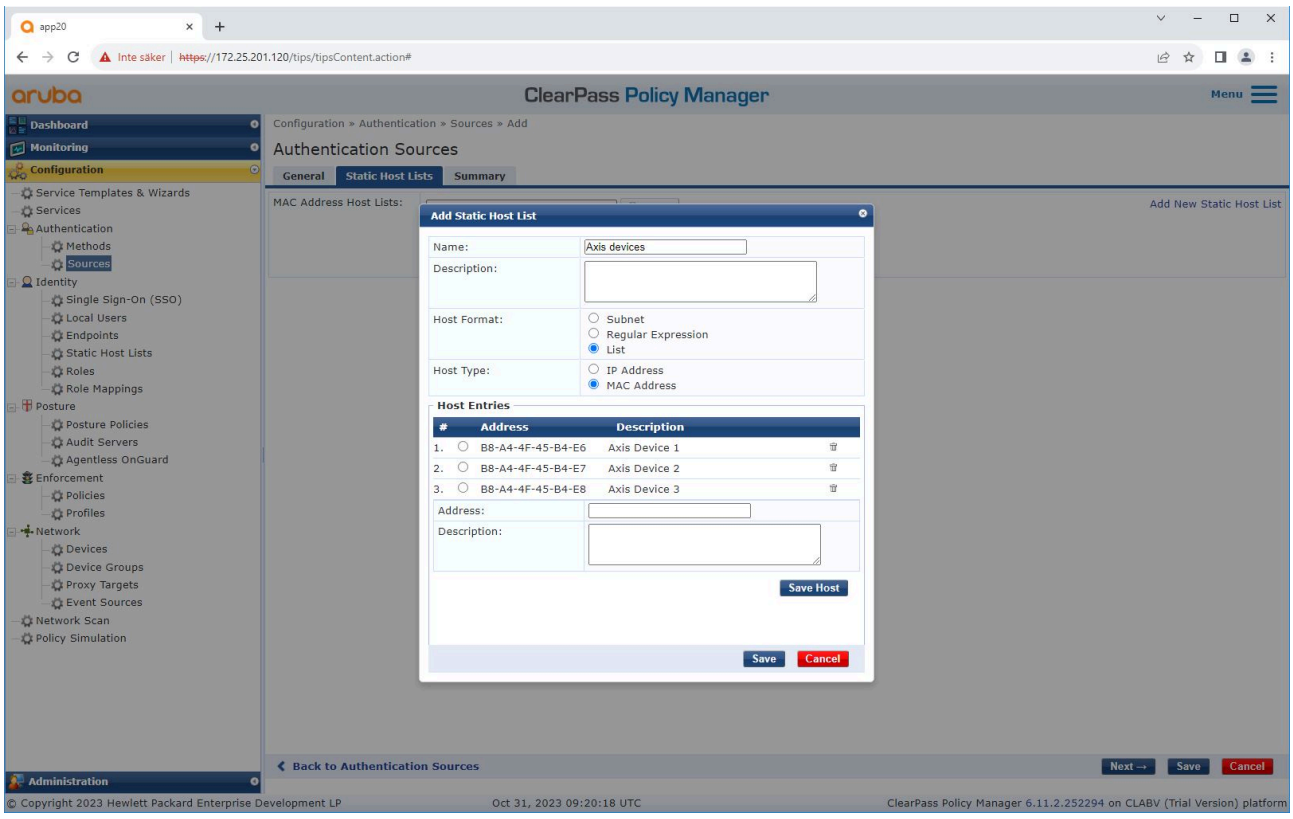
由于存在伪造 MAC 地址的可能性，因此未授予常规配置网络的访问权限。我们建议您仅使用 MAB 进行初始启动，然后进一步手动检查设备。

#### 来源配置

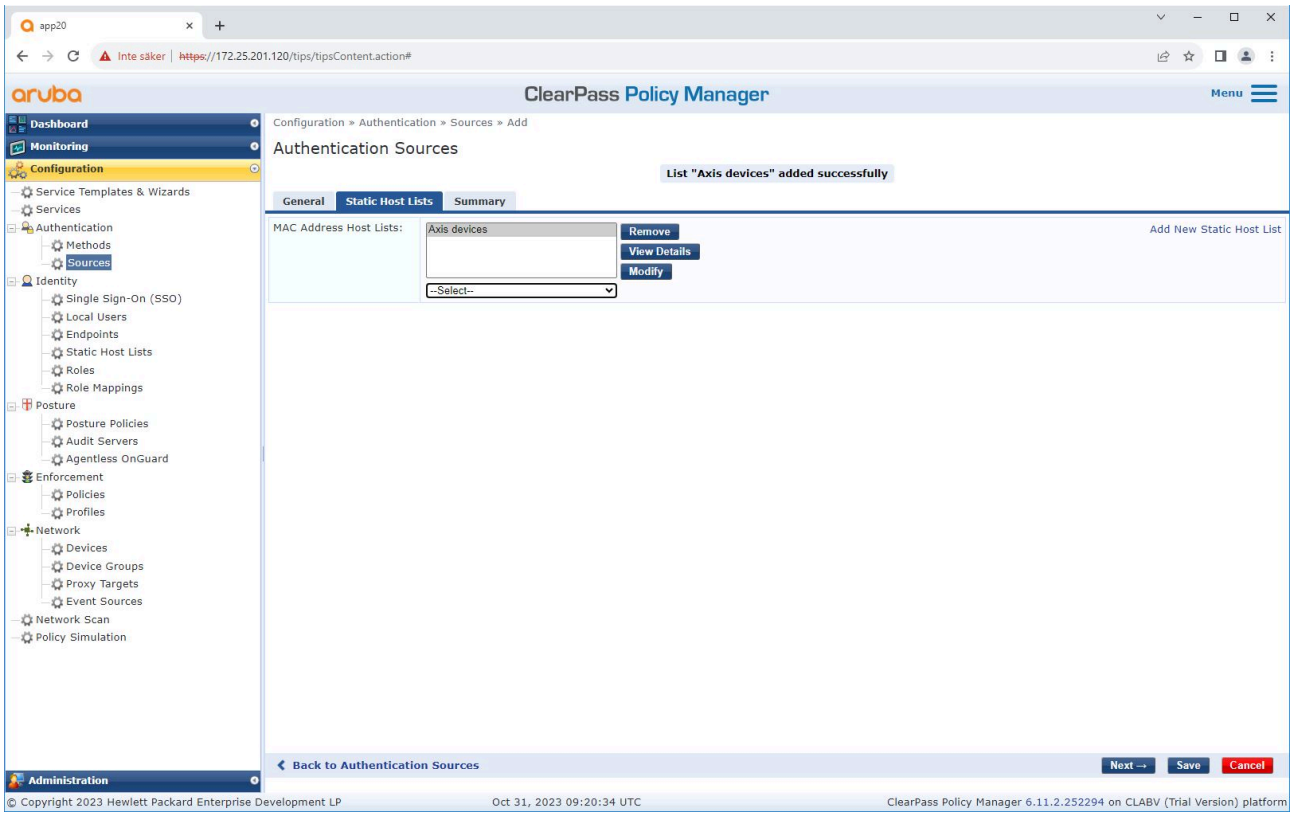
在**来源**界面中，创建一个新的身份验证源，仅允许手动导入的 MAC 地址。


app20
Inte säker | https://172.25.201.120/tips/tipsContent.action#tipsAuthSources.action
aruba
ClearPass Policy Manager
Menu
Dashboard
Monitoring
Configuration
Service Templates & Wizards
Services
Authentication
Methods
Sources
Identity
Single Sign-On (SSO)
Local Users
Endpoints
Static Host Lists
Roles
Role Mappings
Posture
Posture Policies
Audit Servers
Agentless OnGuard
Enforcement
Policies
Profiles
Network
Devices
Device Groups
Proxy Targets
Event Sources
Network Scan
Policy Simulation
Administration
Configuration » Authentication » Sources
Authentication Sources
Add
Import
Export All
An authentication source is the identity store (Active Directory, LDAP directory, etc.) against which users and devices are authenticated.
Filter: Name contains Go Clear Filter
Show 20 records
# Name Type Description
1. [Admin User Repository] Local SQL DB Authenticate users against Policy Manager admin user database
2. [Denylist User Repository] Local SQL DB Denylist database with users who have exceeded bandwidth or session related limits
3. [Endpoints Repository] Local SQL DB Authenticate endpoints against Policy Manager local database
4. [Guest Device Repository] Local SQL DB Authenticate guest devices against Policy Manager local database
5. [Guest User Repository] Local SQL DB Authenticate guest users against Policy Manager local database
6. [Insight Repository] Local SQL DB Insight database with session information for users and devices
7. [Local User Repository] Local SQL DB Authenticate users against Policy Manager local user database
8. [Onboard Devices Repository] Local SQL DB Authenticate Onboard devices against Policy Manager local database
9. [Social Login Repository] Local SQL DB Authenticate users against Policy Manager social login database
10. [Time Source] Local SQL DB Authorization source for implementing various time functions
11. [Zone Cache Repository] HTTP Access attributes cached by Context Server Actions in previous sessions
Showing 1-11 of 11
Copy Export Delete
© Copyright 2023 Hewlett Packard Enterprise Development LP
Oct 31, 2023 09:13:53 UTC
ClearPass Policy Manager 6.11.2.252294 on CLABV (Trial Version) platform


app20
Inte säker | https://172.25.201.120/tips/tipsContent.action#tipsAddAuthSource.action
aruba
ClearPass Policy Manager
Menu
Dashboard
Monitoring
Configuration
Service Templates & Wizards
Services
Authentication
Methods
Sources
Identity
Single Sign-On (SSO)
Local Users
Endpoints
Static Host Lists
Roles
Role Mappings
Posture
Posture Policies
Audit Servers
Agentless OnGuard
Enforcement
Policies
Profiles
Network
Devices
Device Groups
Proxy Targets
Event Sources
Network Scan
Policy Simulation
Administration
Configuration » Authentication » Sources » Add
Authentication Sources
General Static Host Lists Summary
Name: Axis Devices
Description: MAC addresses of Axis devices in use.
Type: Static Host List
Use for Authorization: Enable to use this Authentication Source to also fetch role mapping attributes
Authorization Sources:
Remove
View Details
Back to Authentication Sources
Next → Save Cancel
© Copyright 2023 Hewlett Packard Enterprise Development LP
Oct 31, 2023 09:21:23 UTC
ClearPass Policy Manager 6.11.2.252294 on CLABV (Trial Version) platform

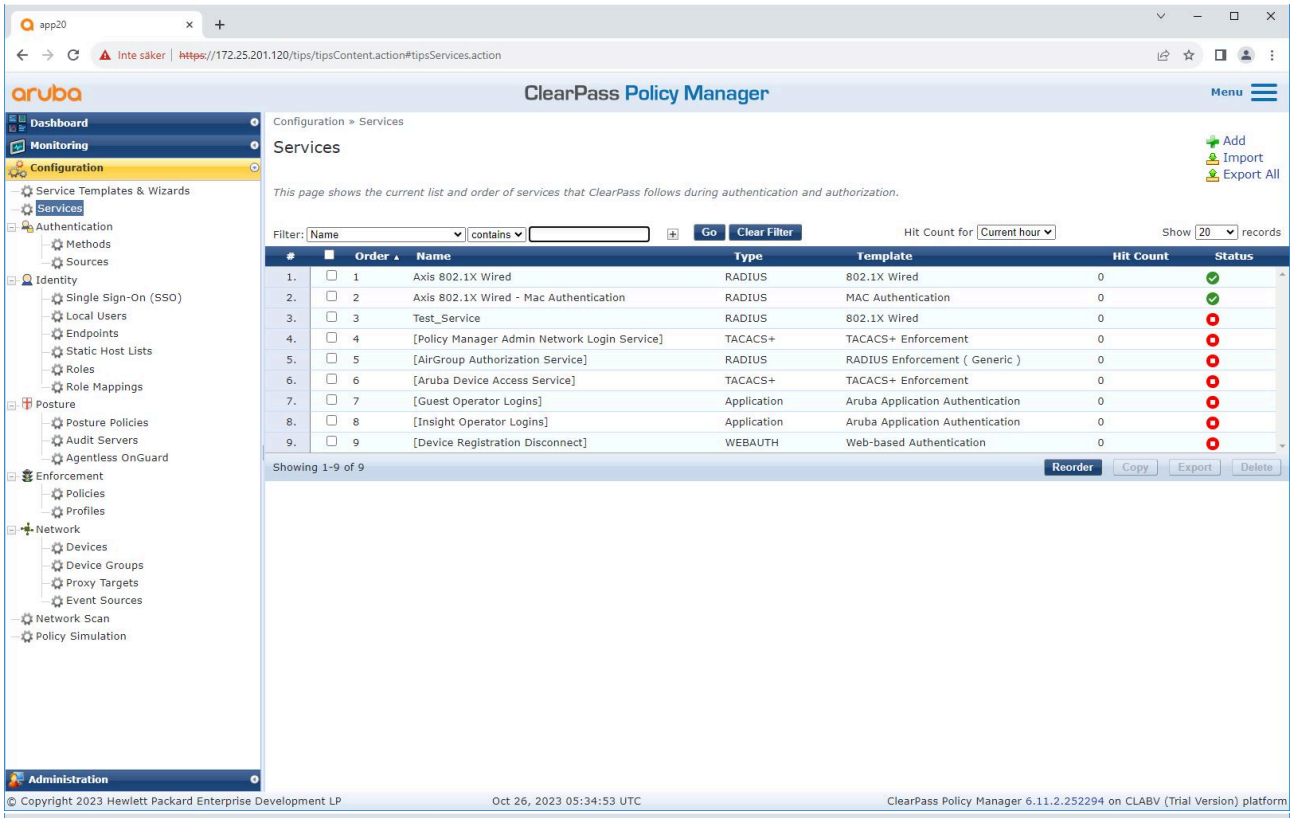


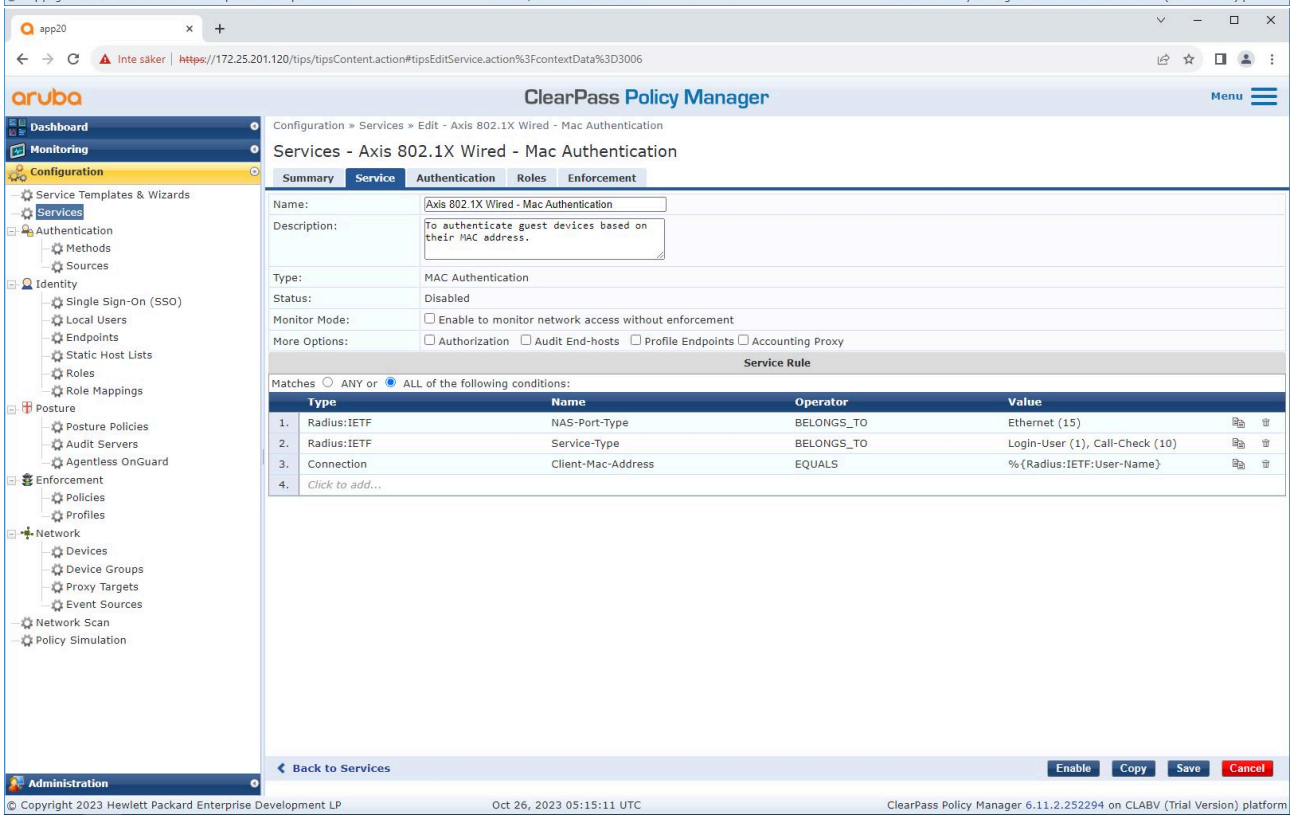

*创建了包含 Axis MAC 地址的静态主机列表。*



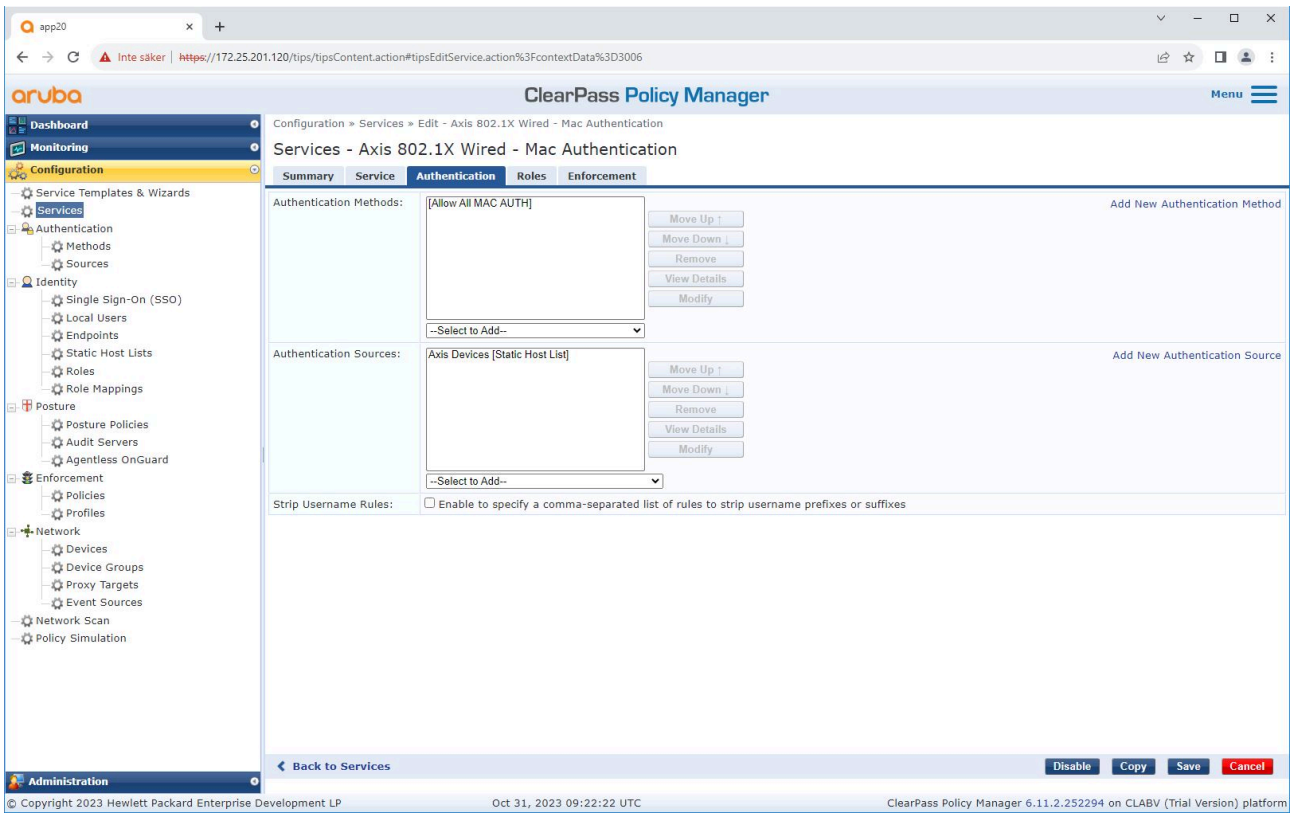

## 设备配置

在**服务**界面中，配置步骤合并为一项服务，用于处理 HPE Aruba Networking 网络中安讯士设备的身份验证和授权。



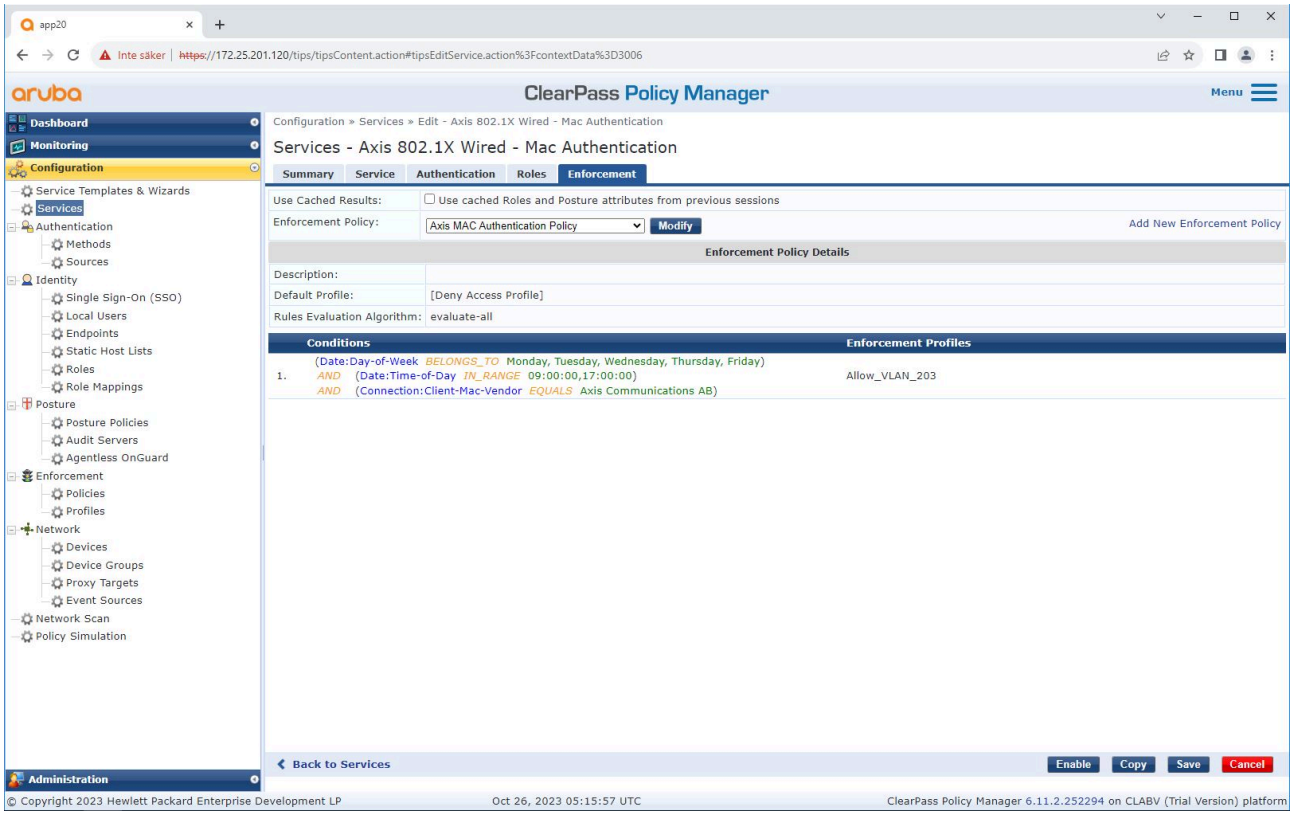

*创建了将 MAB 定义为连接方法的专用的安讯士服务。*




*将预先配置的 MAC 认证方法配置到服务中。此外，还选中了包含 AXIS MAC 地址列表的身份验证源（先前创建）。*

Axis Communications 使用以下 MAC 地址 OUI：

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




*在最后一步中，为该服务配置先前创建的强制策略。*

## HPE Aruba Networking 接入交换机

除了 中描述的安全接入配置之外，请参阅下面 HPE Aruba Networking 接入交换机的端口配置示例以允许进行 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_zh

2025-11 (M7.2)