# Secure integration of Axis devices into Aruba networks

用户手册

## 目录

# 简介

## 简介

### 简介

本集成指南旨在概述如何在 Aruba 网络中加入和操作 Axis 设备的理想实践配置。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时间和财力。当将 Axis 设备管理应用程序与 Aruba 网络设备和应用程序结合使用时，它可以消除不必要的系统复杂性。以下是将 Axis 设备和软件与 Aruba 网络基础设施相结合时可以获得的一些优势：

- 通过移除设备分级网络，尽可能地降低系统复杂性。
- 通过添加自动化入网流程和设备管理来节省成本。
- 利用 Axis 设备提供的零接触网络安全控制。
- 通过应用 Aruba 和 Axis 专业知识来提高整体网络安全性。

在开始配置之前，必须准备好网络基础设施以安全地验证 Axis 设备的完整性。这允许在整个入网过程中逻辑网络之间进行软件定义的平滑过渡。在进行配置之前，有必要了解以下方面的知识：

- 管理 Aruba 企业网络 IT 基础设施，包括 Aruba 接入交换机和 Aruba ClearPass 策略管理器。
- 现代网络访问控制技术和网络安全策略的专业知识。
- 有关 Axis 产品的基本知识是必要的，但将在整个指南中提供。

## 安全加入 - IEEE 802.1AR/802.1X

### 初始认证

连接 Axis Edge Vault 支持的 Axis 设备，以根据 Aruba 网络对设备进行身份验证。设备将使用 IEEE 802.1AR Axis 设备 ID 证书通过 IEEE 802.1X 网络访问控制来验证自身身份。

为了授予网络访问权限，Aruba ClearPass 策略管理器会验证 Axis 设备 ID 以及其他设备特定的指纹。MAC 地址和运行固件等信息用于做出基于策略的决策。

Axis 设备使用符合 IEEE 802.1AR 的 Axis 设备 ID 证书针对 Aruba 网络进行身份验证。

*Axis 设备使用符合 IEEE 802.1AR 的 Axis 设备 ID 证书针对 Aruba 网络进行身份验证。*

1. *Axis 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

身份验证后，Aruba 网络会将 Axis 设备移动到安装了 Axis Device Manager 的配置网络（VLAN201）中。通过 Axis 设备管理器，可以执行设备配置、安全强化和固件更新。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上以用于 IEEE 802.1X 和 HTTPS。

*身份验证成功后，Axis 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 Axis 设备配置新的 IEEE 802.1X 证书将触发新的身份验证尝试。Aruba ClearPass 策略管理器将验证新证书并决定是否将 Axis 设备移至生产网络中。

*设备配置后，Axis 设备将离开配置网络并尝试针对 Aruba 网络重新进行身份验证。*

1. *Axis 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*

重新验证后，Axis 设备将移至生产网络（VLAN 202）。在该网络中，视频管理系统（VMS）将连接到 Axis 设备并开始运行。

*Axis 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*

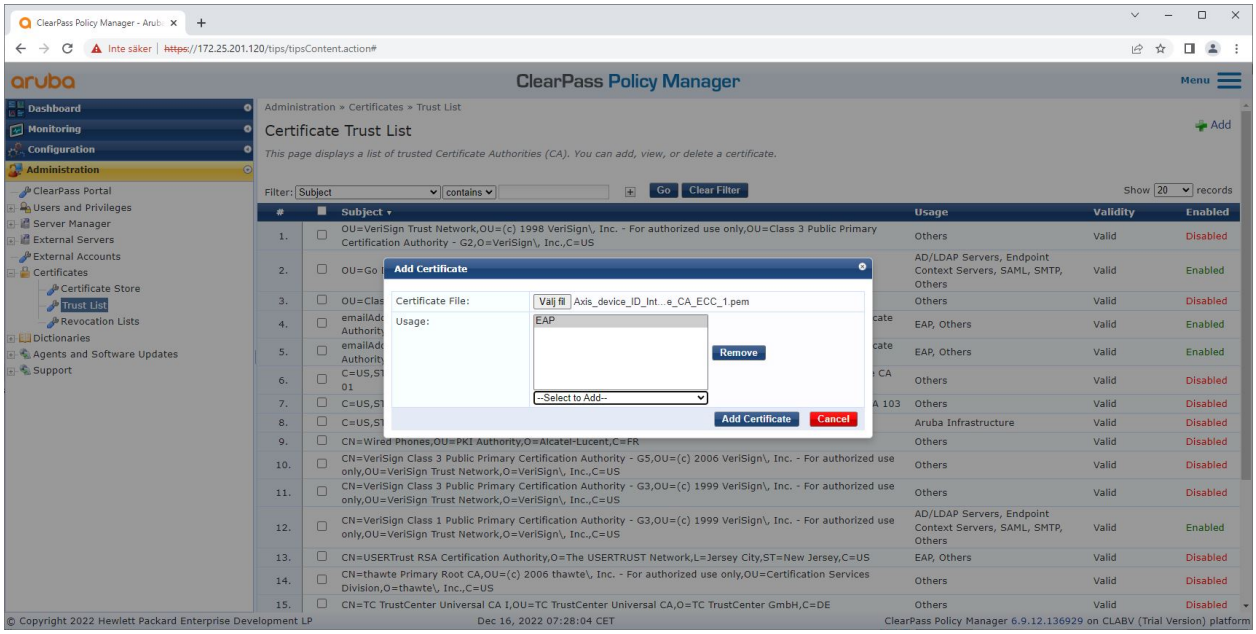
# 配置 HPE Aruba

## Aruba ClearPass 策略管理器

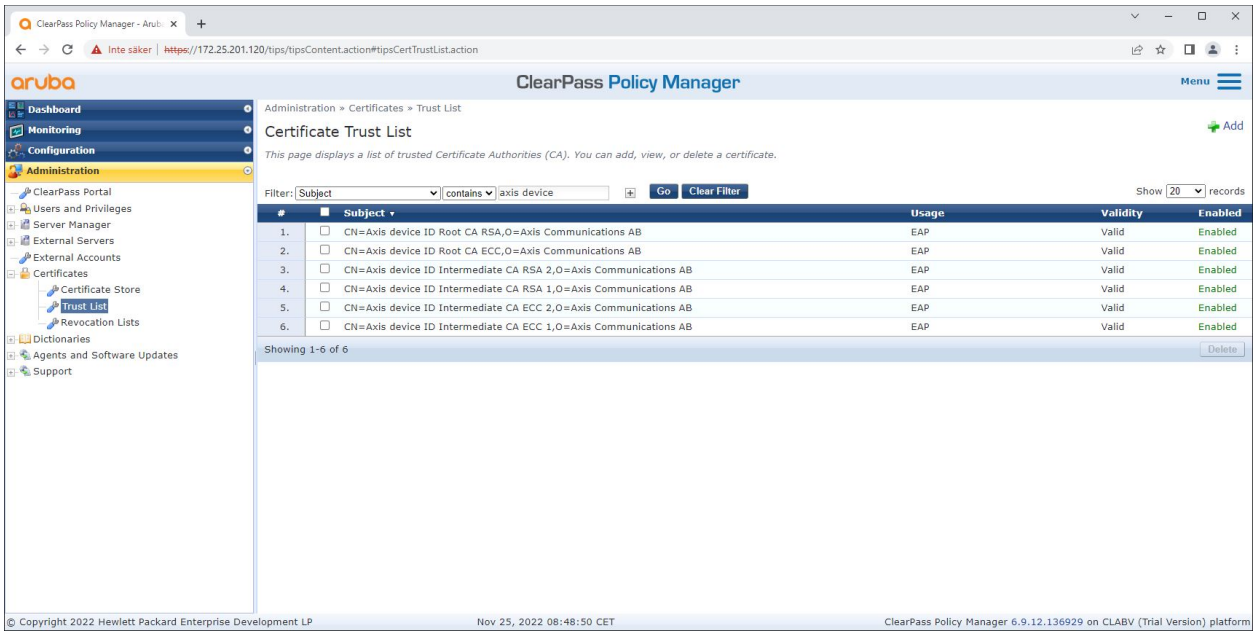
Aruba 的 ClearPass 策略管理器为跨多供应商的有线、无线和 VPN 基础设施的 IoT、BYOD、企业设备、员工、承包商和访客提供基于角色和设备的安全网络访问控制。

### 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 Aruba ClearPass 策略管理器以通过 IEEE 802.1X EAP–TLS 对 Axis 设备进行身份验证。
4. 在使用字段中选择 EAP。这些证书将用于 IEEE 802.1X EAP–TLS 身份验证。



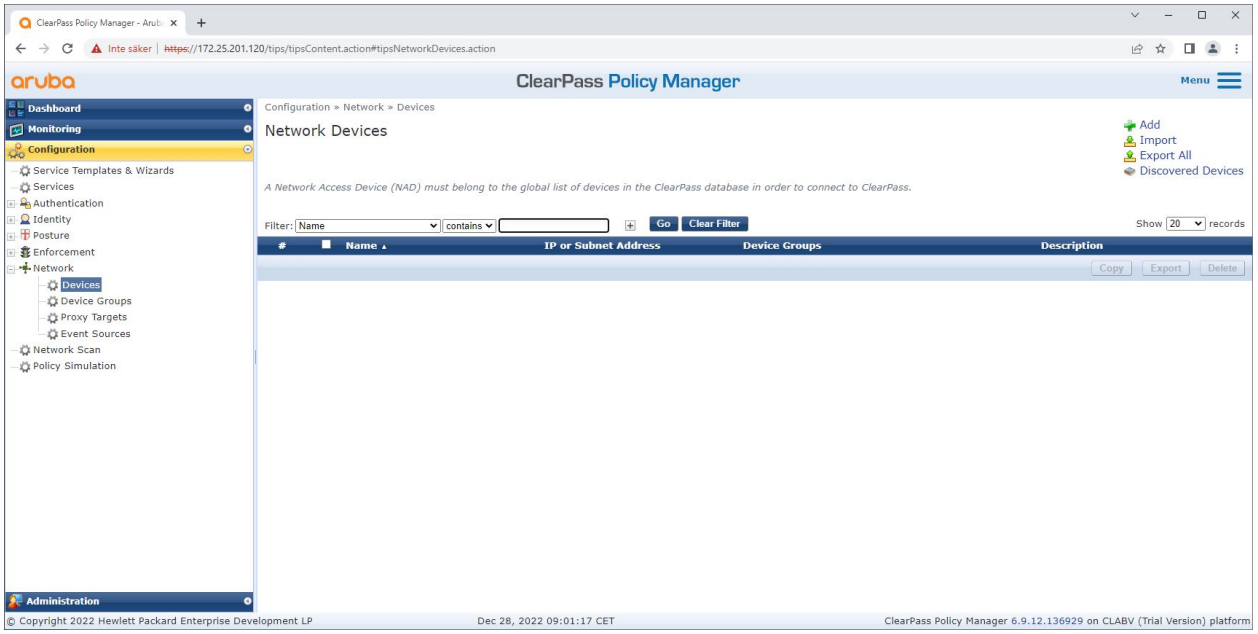

*将特定于 Axis 的 IEEE 802.1AR 证书上传到 Aruba ClearPass 策略管理器的可信证书存储区。*




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

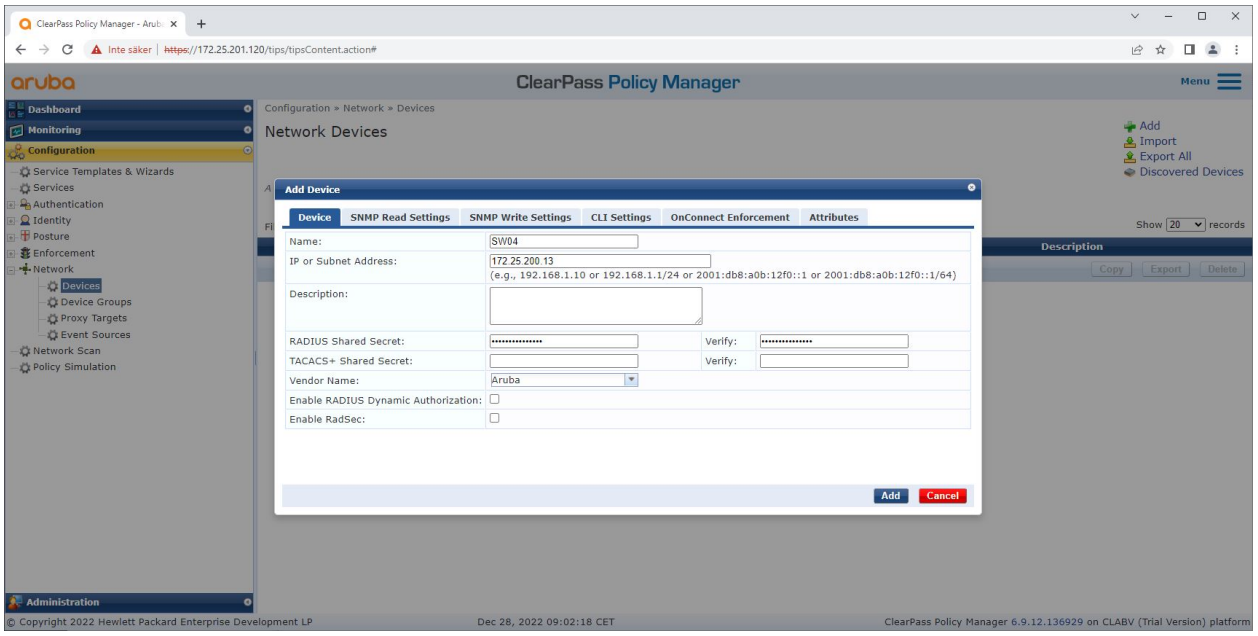
**网络设备/组配置**

1. 将受信任的网络访问设备（例如 Aruba 访问交换机）添加到 ClearPass 策略管理器。ClearPass 策略管理器需要知道网络中的哪些 Aruba 接入交换机将用于 IEEE 802.1X 通信。
2. 使用网络设备组配置将多个可信网络访问设备分组。对受信任的网络访问设备进行分组可以更轻松地进行策略配置。
3. RADIUS 共享密钥需要与特定交换机 IEEE 802.1X 配置相匹配。

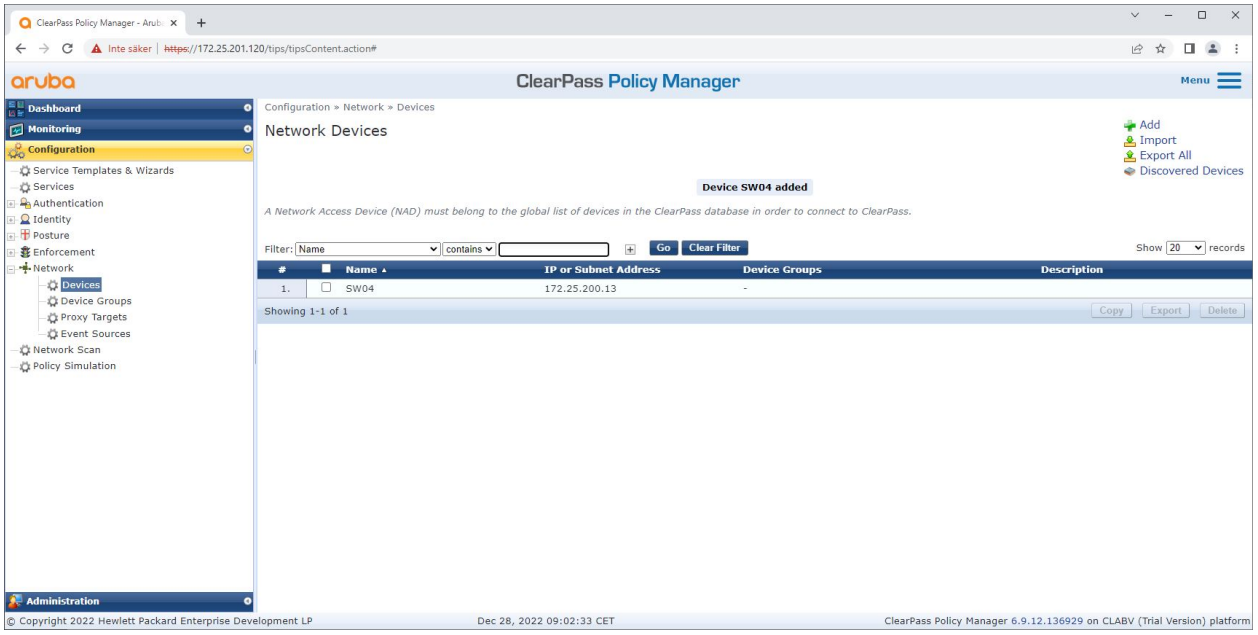



*Aruba ClearPass 策略管理器中的可信网络设备接口。*

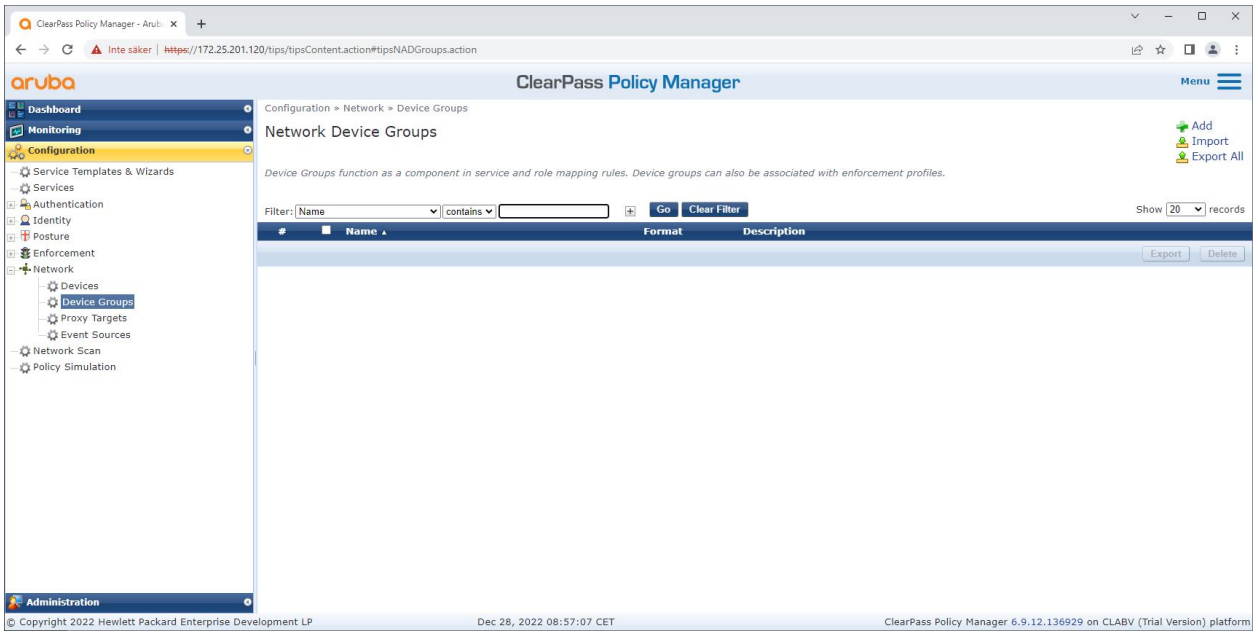
## 安全加入 - IEEE 802.1AR/802.1X



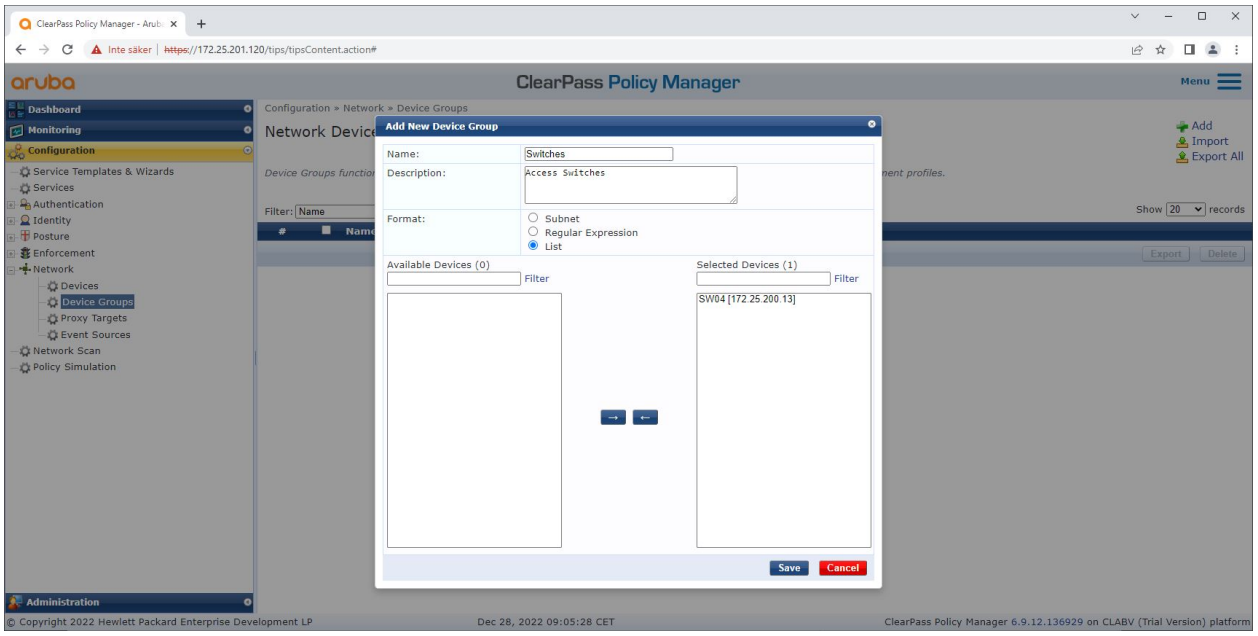

*在 Aruba ClearPass 策略管理器中将 Aruba 接入交换机添加为可信网络设备。请注意，RADIUS 共享密钥需要与特定交换机 IEEE 802.1X 配置匹配。*



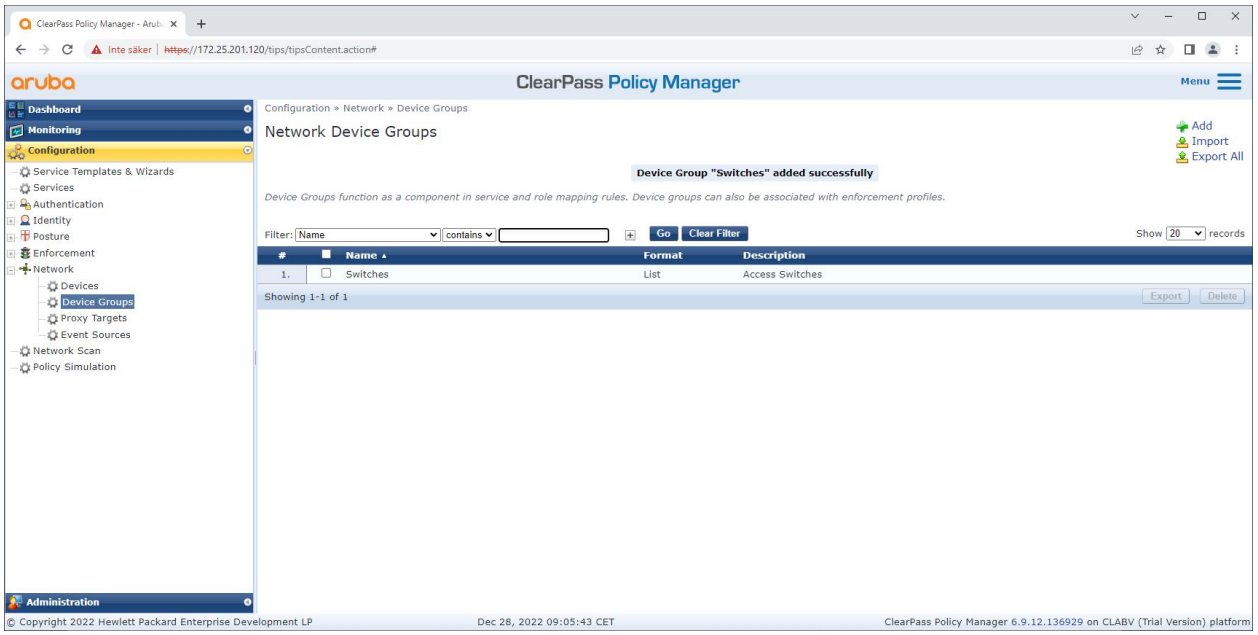

*配置了一台受信任网络设备的 Aruba ClearPass 策略管理器。*




*Aruba ClearPass 策略管理器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 Aruba ClearPass 策略管理器中的新设备组中。*



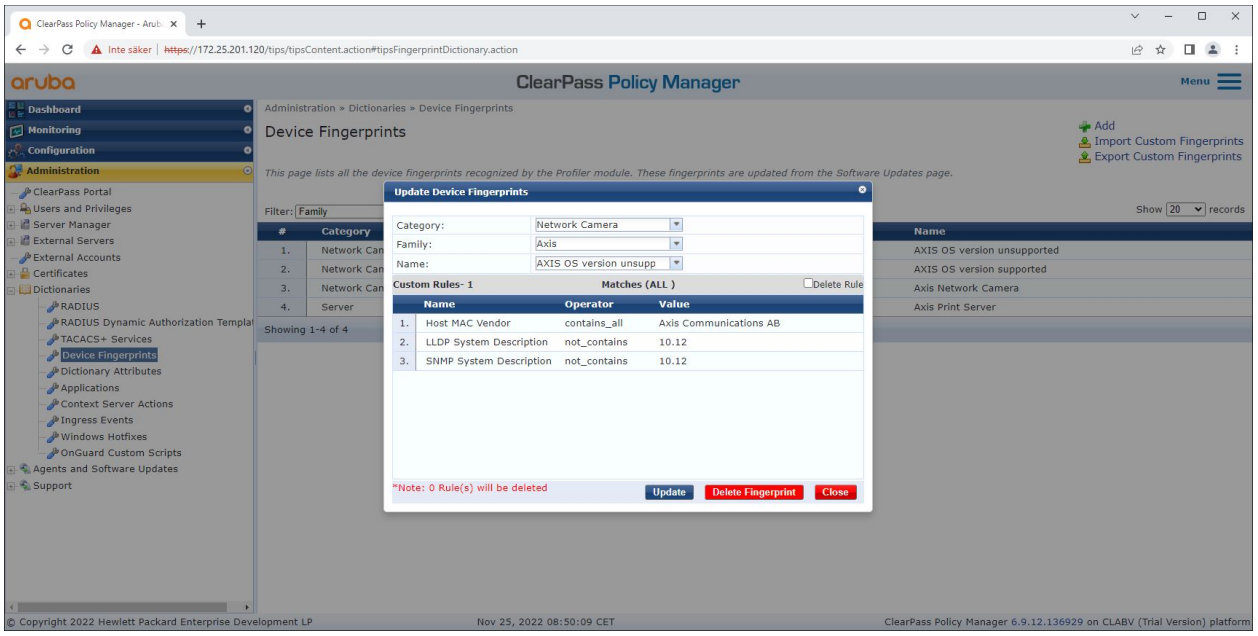

*Aruba ClearPass 策略管理器已配置网络设备组，其中包括一个或多个受信任的网络设备。*

### 设备指纹配置

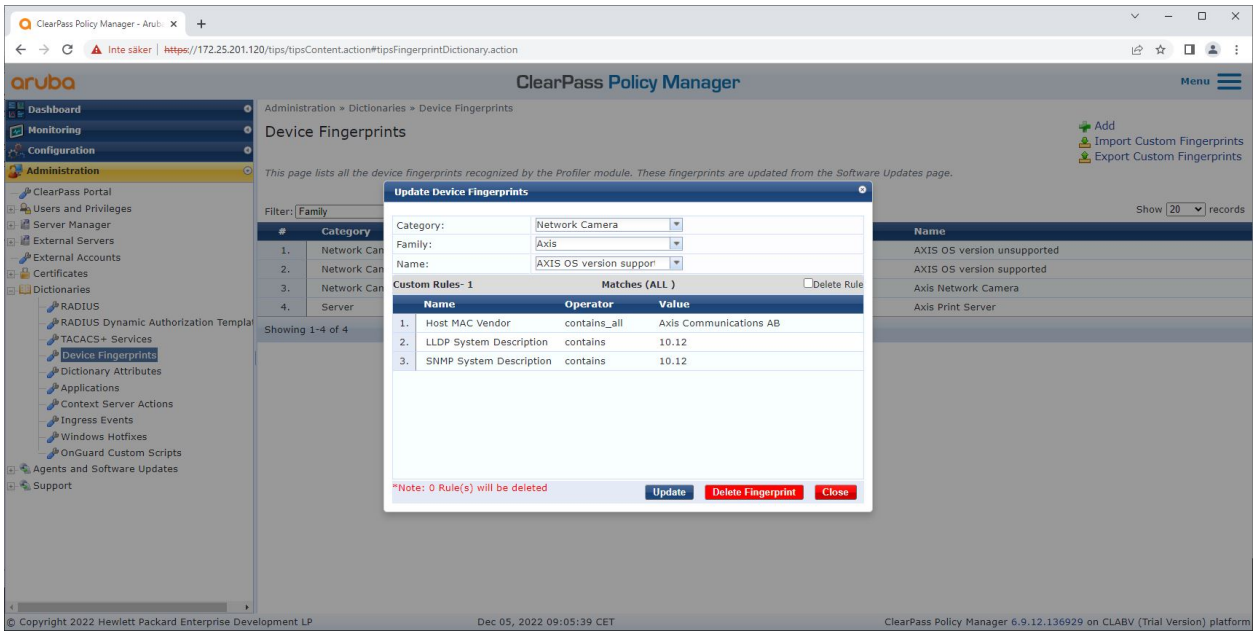
Axis 设备可以通过网络发现分发设备特定信息，例如 MAC 地址和固件版本。可以从 Aruba ClearPass 策略管理器中的设备指纹界面创建设备指纹。可以更新和管理设备指纹。可以操作的是根据 AXIS 操作系统版本授予或拒绝访问权限。

可以更新和管理设备指纹。可以操作的是根据 AXIS 操作系统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. 设置设备指纹设置。




*Aruba ClearPass 策略管理器中的设备指纹配置。运行除 10.12 之外的其他固件版本的 Axis 设备均被视为不受支持。*




*Aruba ClearPass 策略管理器中的设备指纹配置。在上例中，运行固件 10.12 的 Axis 设备被视为受支持。*

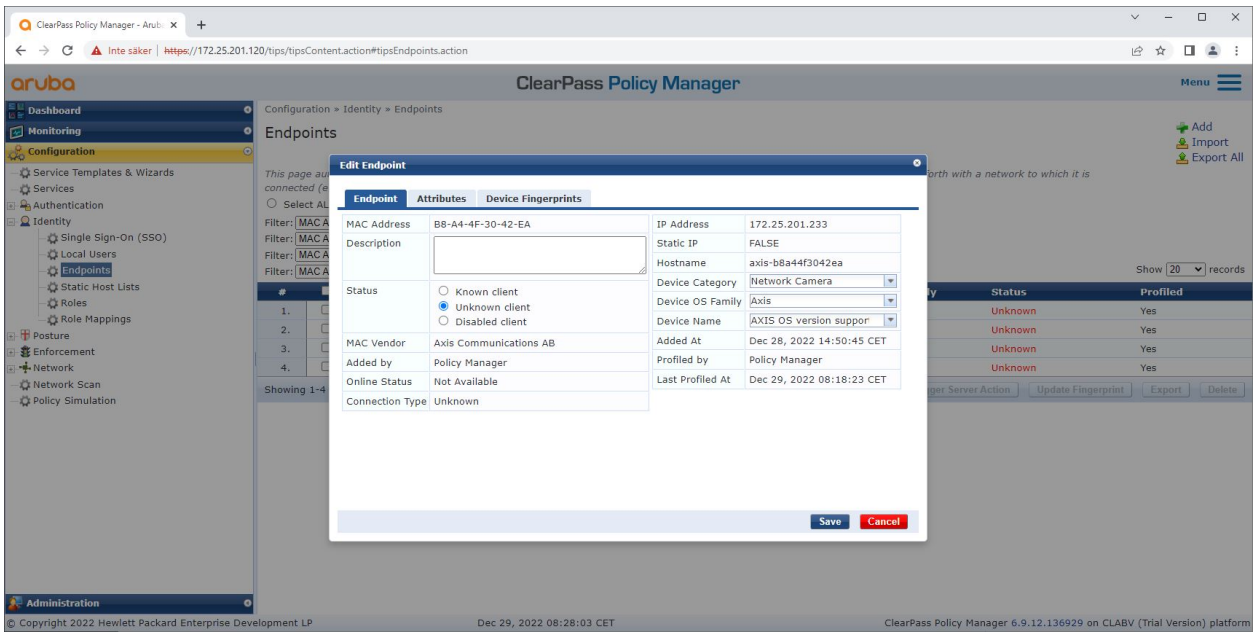
有关 Aruba ClearPass Manager 收集的设备指纹的信息可以在端点部分找到。

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

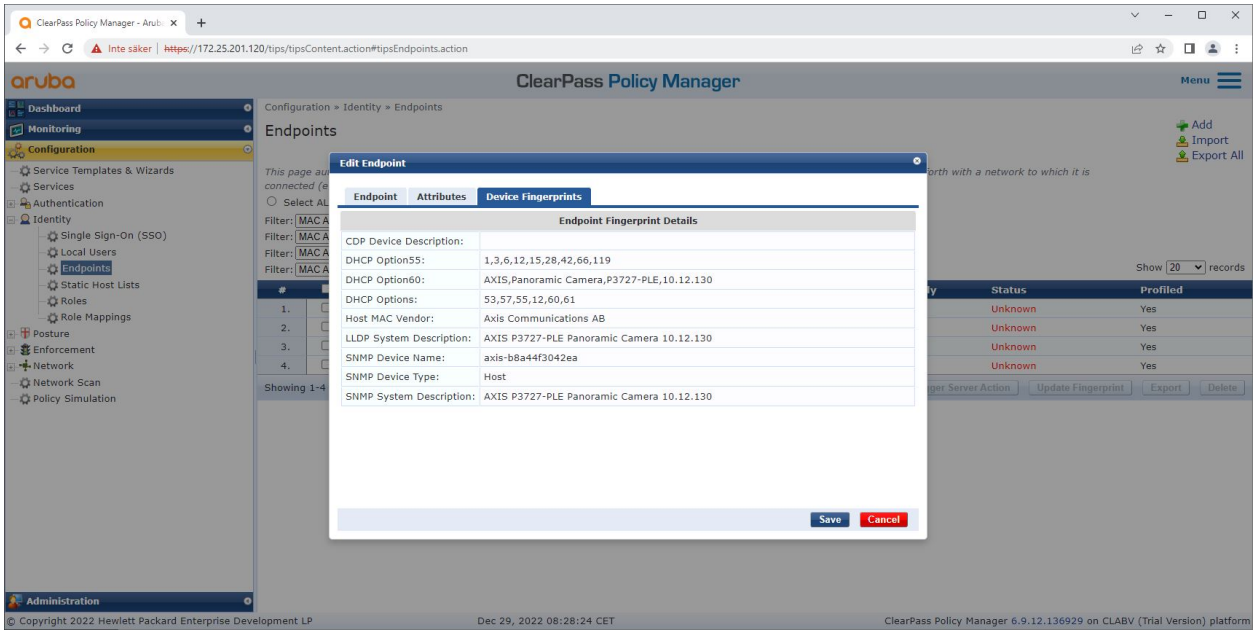
## 安全加入 - IEEE 802.1AR/802.1X

注

默认情况下，SNMP 在 Axis 设备中处于禁用状态，并从 Aruba 接入交换机收集。




*已由 Aruba ClearPass 策略管理器配置文件的 Axis 设备。*

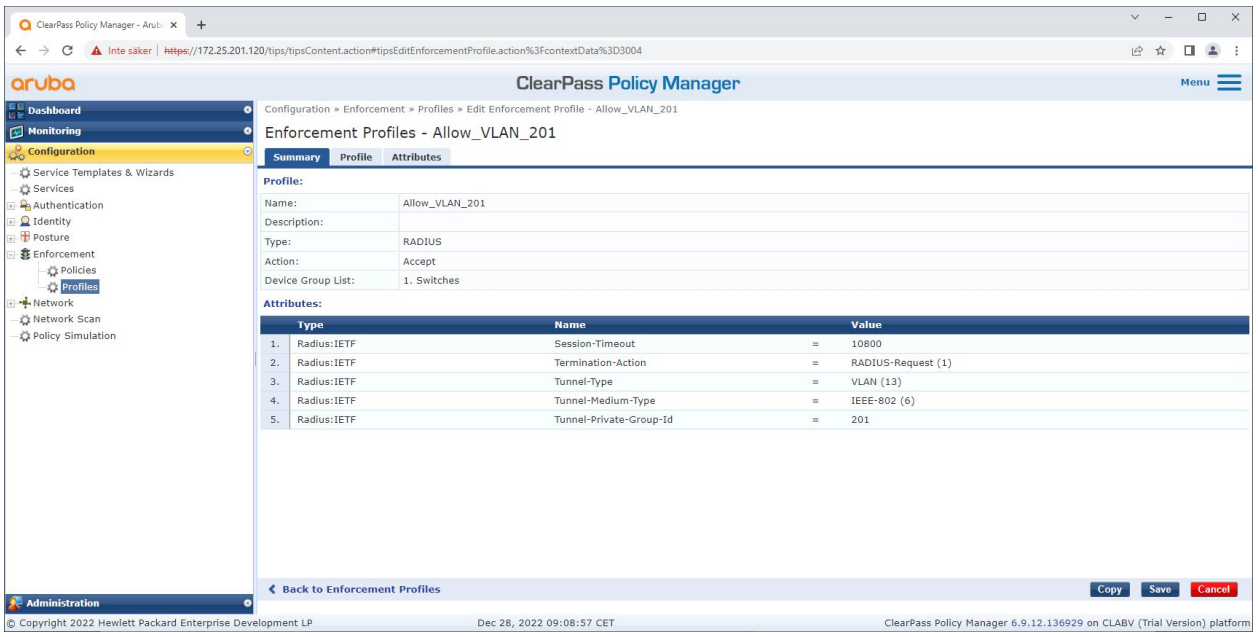



*配置文件的 Axis 设备的详细设备指纹。请注意，默认情况下，Axis 设备中禁用 SNMP。LLDP、CDP 和 DHCP 特定的发现信息由处于出厂默认状态的 Axis 设备共享，并由 Aruba 接入交换机中继到 ClearPass 策略管理器。*

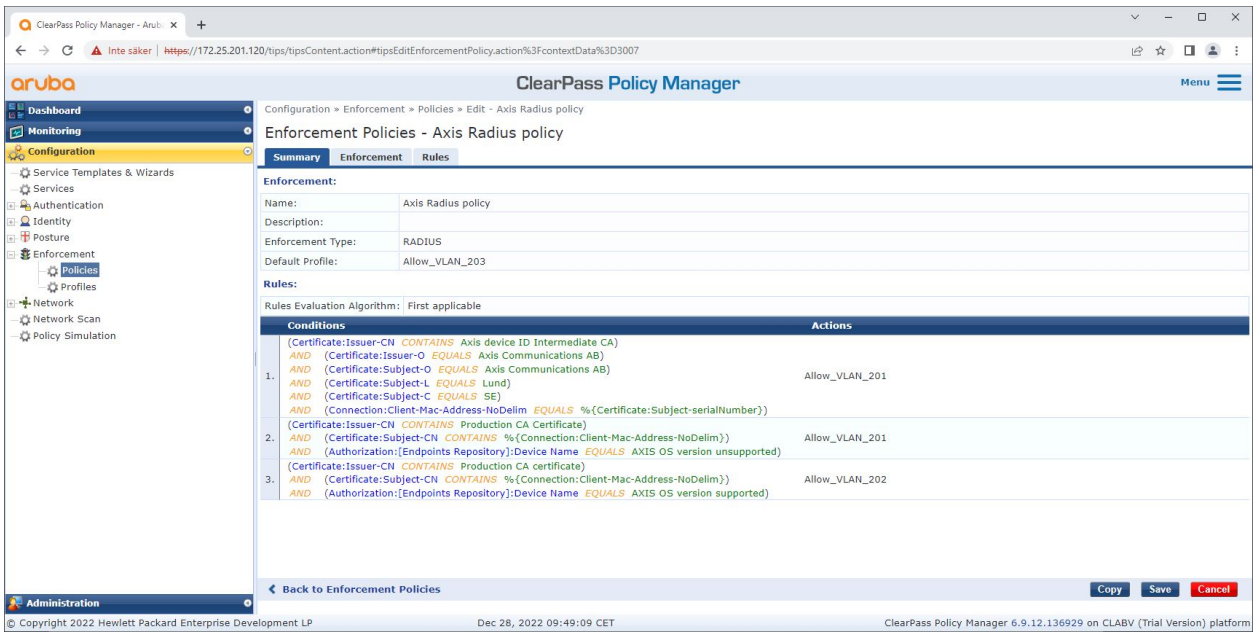
### 强制配置文件配置

强制配置文件用于允许 Aruba ClearPass 策略管理器将特定 VLAN ID 分配给交换机上的访问端口。这是一个基于策略的决策，适用于设备组“交换机”中的网络设备。必要的强制配置文件数量取决于将使用的 VLAN 数量。在我们的设置中，共有三个 VLAN（VLAN 201、202、203）与三个强制配置文件相关。

配置完 VLAN 的强制文件后，就可以配置实际的强制策略了。Aruba ClearPass 策略管理器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 Aruba 网络的权限。




*允许访问 VLAN 201 的强制配置文件示例。*




*Aruba ClearPass 策略管理器中的强制策略配置。*

## 安全加入 - IEEE 802.1AR/802.1X

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 Axis 设备将被授予访问受限、隔离网络的权限。需要对设备进行手动检查以采取适当的措施。

配置网络 (VLAN 201)

Axis 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 Axis 设备管理功能 *Axis Device Manager* 和 *Axis Device Manager Extend*。它还可以使用固件更新、生产级证书和其他配置来配置 Axis 设备。以下条件已由 Aruba ClearPass 策略管理器验证：

- Axis 设备的固件版本。
- 设备的 MAC 地址与供应商特定的 Axis MAC 地址方案与 Axis 设备 ID 证书的序列号属性相匹配。
- Axis 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、国家/地区）相匹配。

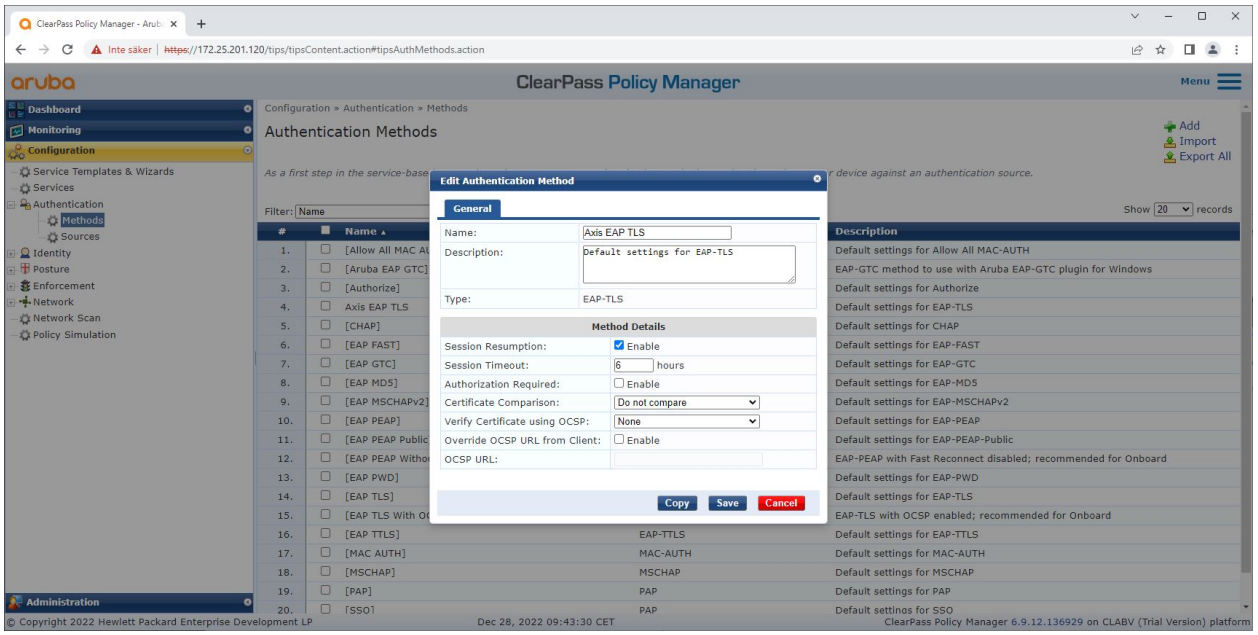
生产网络 (VLAN 202)

Axis 设备被授予对 Axis 设备将在其中运行的生产网络的访问权限。在配置网络（VLAN 201）内完成设备配置后，将授予访问权限。以下条件已由 Aruba ClearPass 策略管理器验证：

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

**认证方式配置**

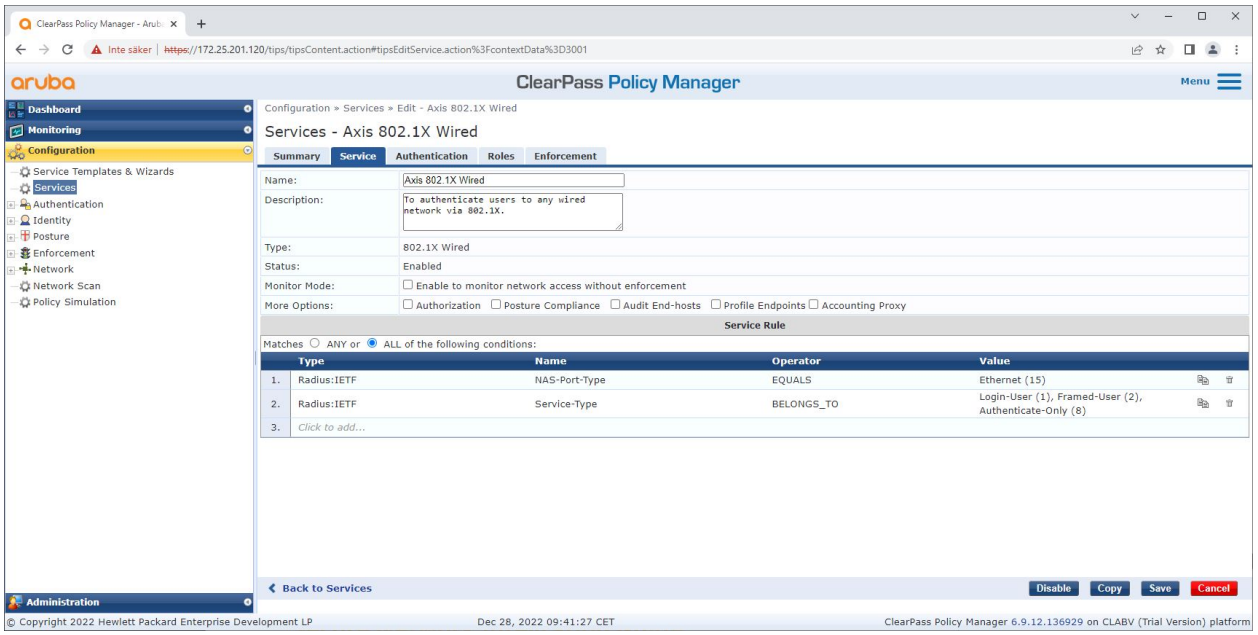
在身份验证方法中，定义了 Axis 设备如何尝试针对 Aruba 网络进行身份验证。理想的身份验证方法应为 IEEE 802.1X EAP–TLS，因为支持 Axis Edge Vault 的 Axis 设备默认启用了 IEEE 802.1X EAP–TLS。



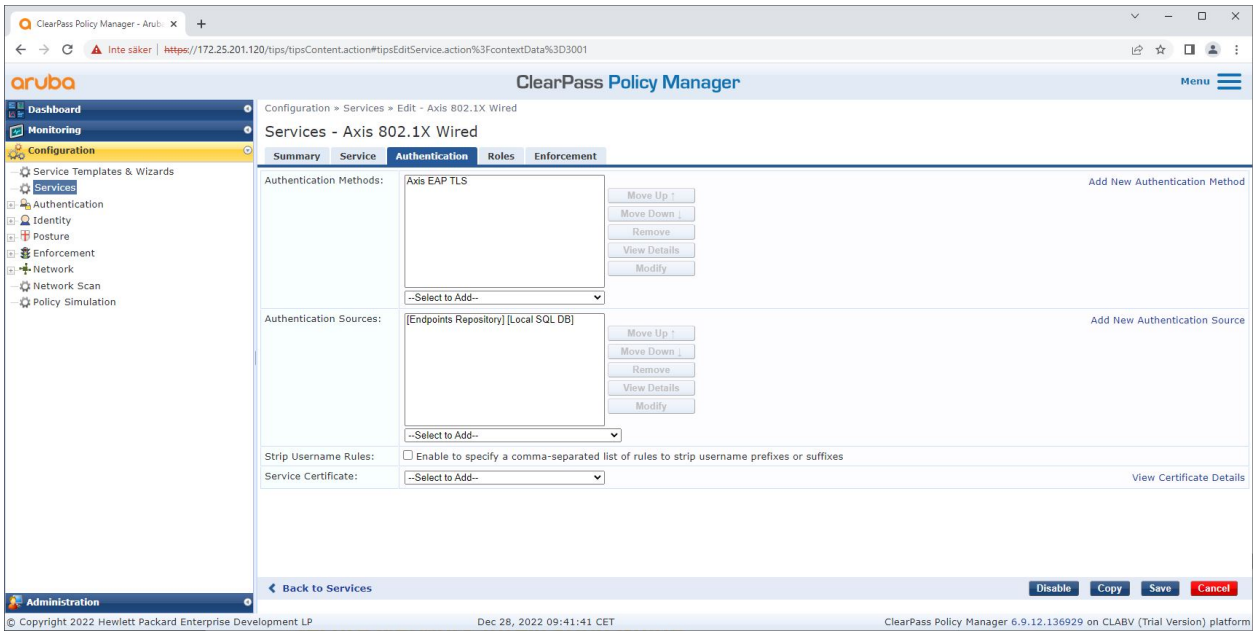

*Aruba ClearPass 策略管理器的身份验证方法接口，其中定义了 Axis 设备的 EAP–TLS 身份验证方法。*

**设备配置**

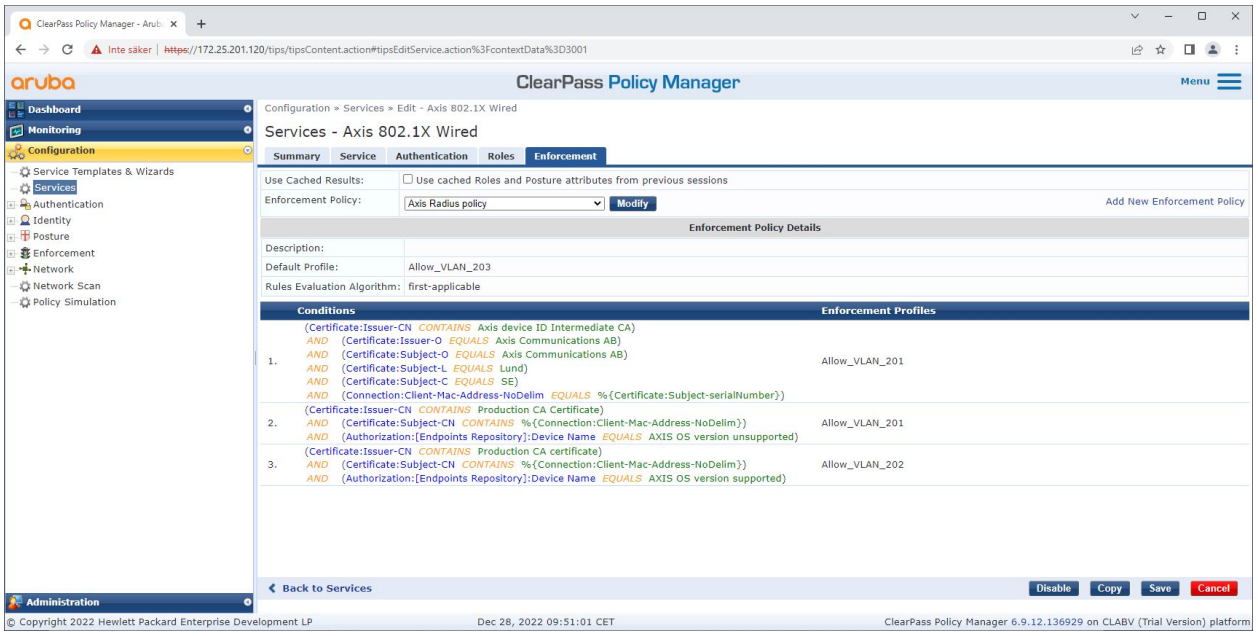
在服务界面中，配置步骤合并为一项服务，用于处理 Aruba 网络中 Axis 设备的身份验证和授权。




*创建了专用的 Axis 服务，将 IEEE 802.1X 定义为连接方法。*




*在下一步中，将之前创建的 EAP-TLS 身份验证方法配置到服务。*




*在尾部步骤中，将之前创建的强制策略配置到服务。*

## Aruba 接入交换机

Axis 设备可以直接连接到支持 PoE 的 Aruba 接入交换机，也可以通过兼容的 Axis PoE 中跨连接。要将 Axis 设备安全地接入 Aruba 网络，需要将接入交换机配置为 IEEE 802.1X 通信。Axis 设备将 IEEE 802.1x EAP-TLS 通信中继到充当 RADIUS 服务器的 Aruba ClearPass 策略管理器。

注

还为 Axis 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。

## 安全加入 - IEEE 802.1AR/802.1X

请参阅以下 Aruba 接入交换机的全局和端口配置示例。

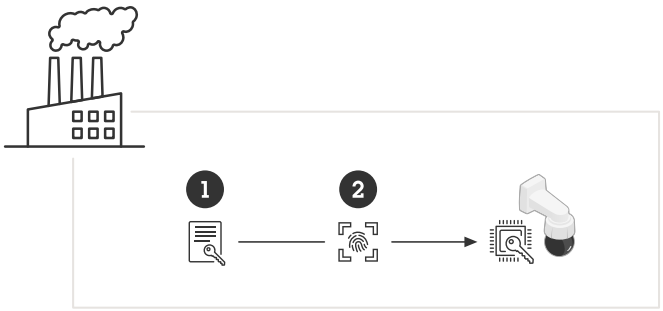
```
radius-server 主机 MyRADIUSIPAddress 密钥"MyRADIUSKey"

AAA 身份验证端口访问 eap-radius
AAA 端口访问验证器 18-19
AAA 端口访问验证器 18 reauth-period 300
AAA 端口访问验证器 19 reauth-period 300
AAA 端口访问验证器处于活动状态
```

## 配置 Axis

### Axis 网络设备

支持 *Axis Edge Vault* 的 Axis 设备制造时带有安全设备标识，称为 Axis 设备 ID。Axis 设备 ID 基于国际 IEEE 802.1AR 标准，该标准定义了一种通过 IEEE 802.1X 进行自动化、安全设备识别和网络接入的方法。



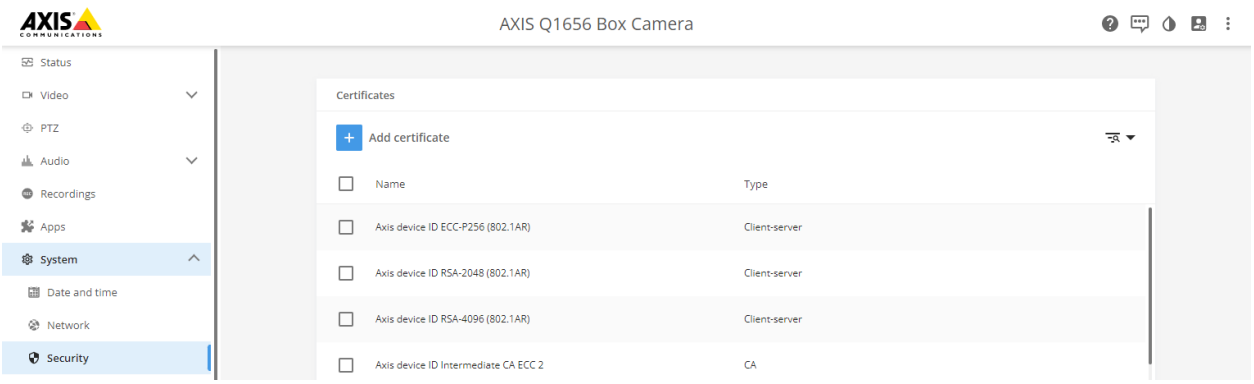

*Axis 设备在制造时带有符合 IEEE 802.1AR 标准的 Axis 设备 ID 证书，用于可信设备身份服务*

1 *Axis 设备 ID 密钥基础设施（PKI）*
2 *Axis 设备 ID*

Axis 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 Axis 设备的真实性。*Axis Product Selector* 可用于了解哪些 Axis 设备支持 Axis Edge Vault 和 Axis 设备 ID。

注

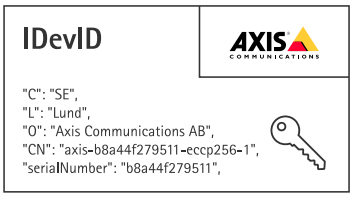
Axis 设备的序列号是其 MAC 地址。




*处于出厂默认状态的 Axis 设备的证书存储以及 Axis 设备 ID。*

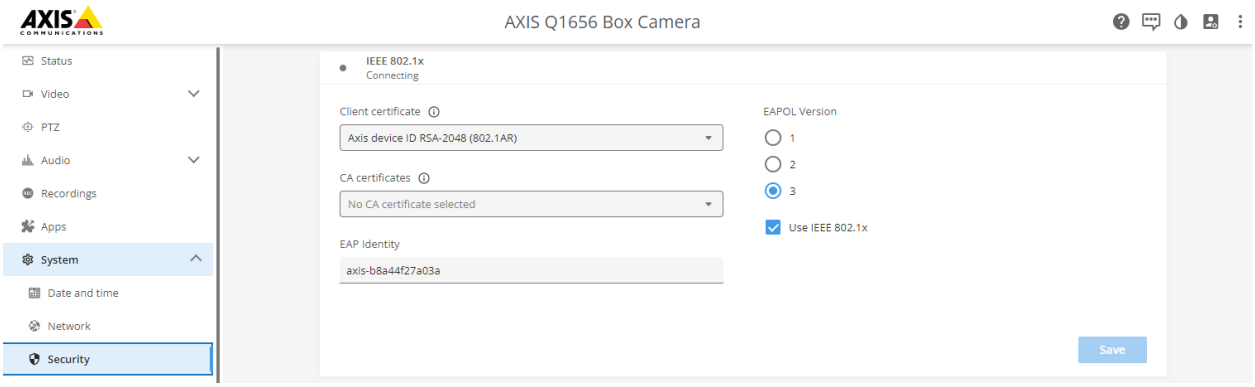
## 安全加入 - IEEE 802.1AR/802.1X

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 Axis 供应商特定信息。该信息由 Aruba ClearPass 策略管理器使用以进行分析和决策以授予网络访问权限。请参阅以下可从 Axis 设备 ID 证书获取的信息




| | |
|---|---|
| 国家/地区 | SE |
| 位置 | 隆德 |
| 发行人组织 | Axis Communications AB |
| 发行人通用名称 | Axis 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 Axis 公司名称、设备序列号和所使用的加密算法（ECC P256、RSA 2048、RSA 4096）组合而成。自 AXIS OS 10.1（2020-09）起，默认情况下启用 IEEE 802.1X，并预先配置 Axis 设备 ID。这使得 Axis 设备能够在支持 IEEE 802.1X 的网络上对自身进行身份验证。




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

### Axis 设备管理器

*AXIS Device Manager* 和 *AXIS Device Manager Extend* 可在网络上以经济高效的方式配置和管理多个 Axis 设备。Axis Device Manager 是一款基于 Microsoft Windows 的应用程序，可以本地安装在网络中的计算机上，而 Axis Device Manager Extend 则依赖云基础设施进行多站点设备管理。两者都为 Axis 设备提供简单的管理和配置功能，例如：

- 安装固件更新。
- 应用网络安全配置，例如 HTTPS 和 IEEE 802.1X 证书。

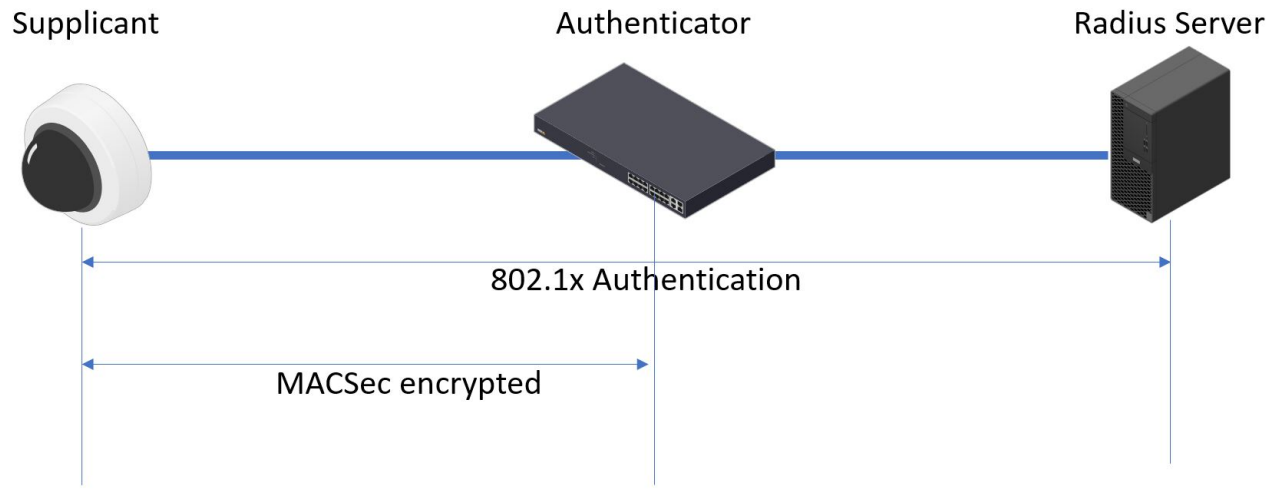
- 配置特定设备的设置，例如图像设置等。

## 安全网络操作 - IEEE 802.1AE MACsec

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 OS10.1（2020–09）及更高版本， IEEE 802.1X 对于与 Axis 设备 ID 兼容的设备，默认启用。在 AXIS OS 11.8 及更高版本，我们使用自动动态模式支持 MACsec IEEE 802.1X 默认情况下启用 EAP–TLS。当您使用出厂默认值连接 Axis 设备时，IEEE 802.1X 执行网络身份验证，成功后还会尝试 MACsec 动态 CAK 模式。

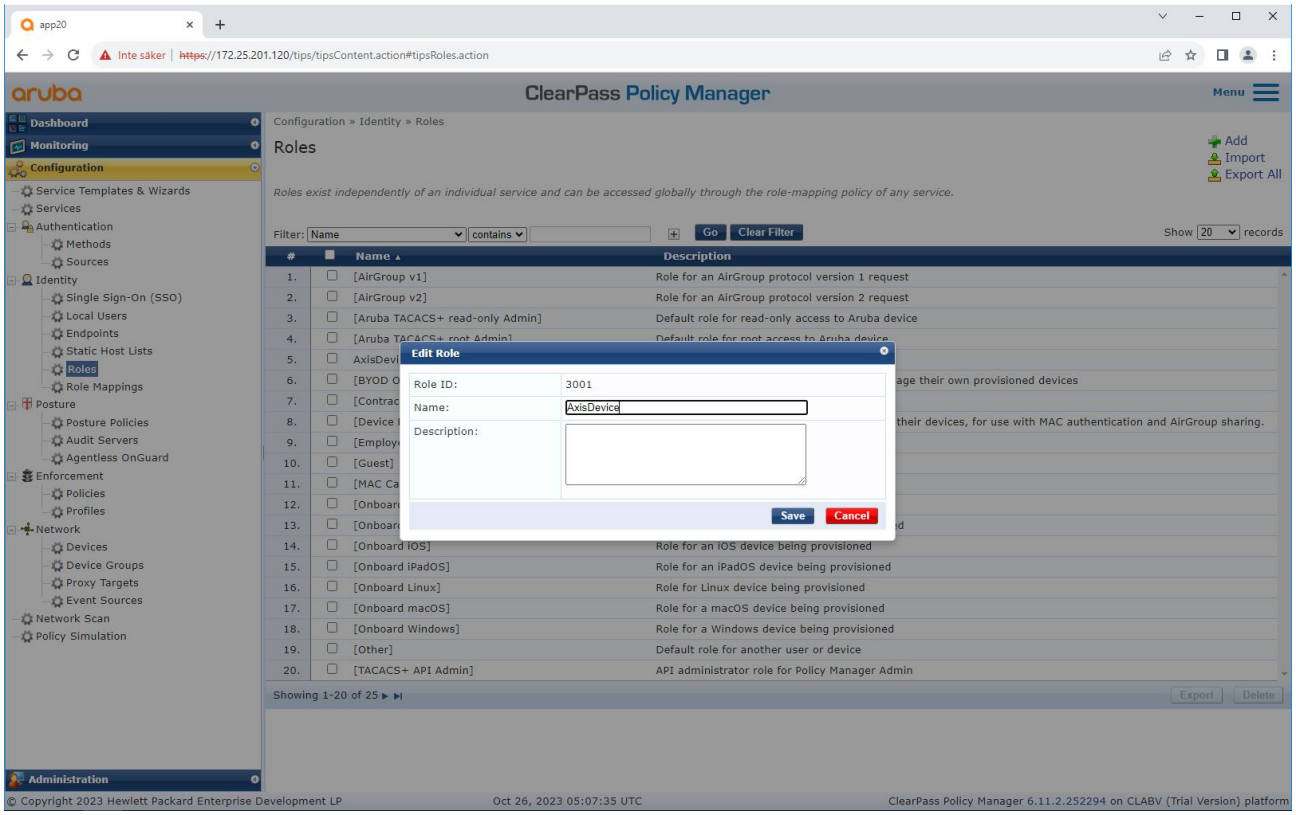
安全存储的 Axis 设备 ID (1) 是与 IEEE 802.1AR 兼容的安全设备身份，用于通过 IEEE 802.1X EAP–TLS 基于端口的网络访问控制 (2) 对 Aruba 网络（4、5）进行身份验证。通过 EAP–TLS 会话，自动交换 MACsec 密钥以建立安全链路 (3)，从而保护从 Axis 设备到 Aruba 交换机的网络流量。

IEEE 802.1AE MACsec 要求 Aruba 接入交换机和 ClearPass Policy Manager 配置准备。无需在 Axis 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。

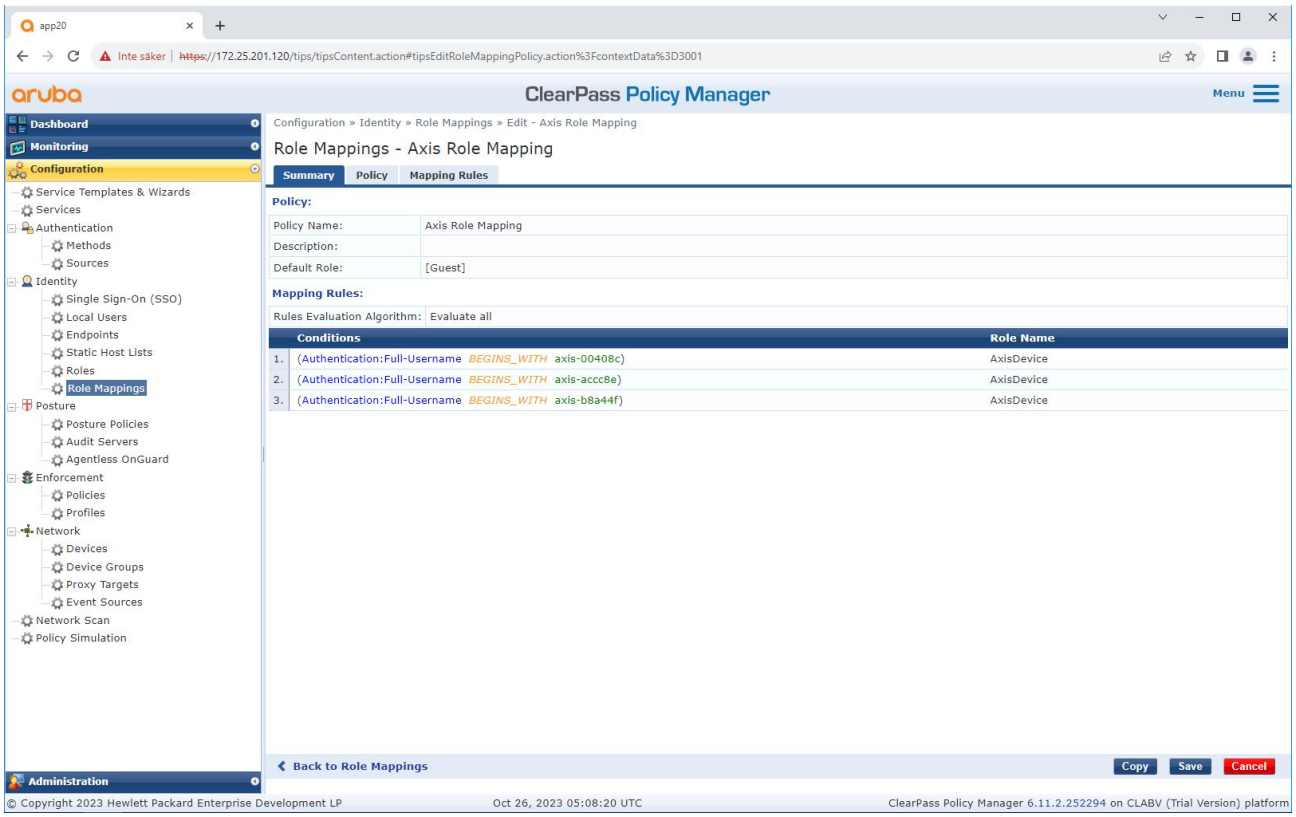
如果 Aruba 接入交换机不支持使用 EAP–TLS 的 MACsec，则可以使用预共享密钥模式并手动配置。

## Aruba ClearPass 策略管理器

### 角色和角色映射策略



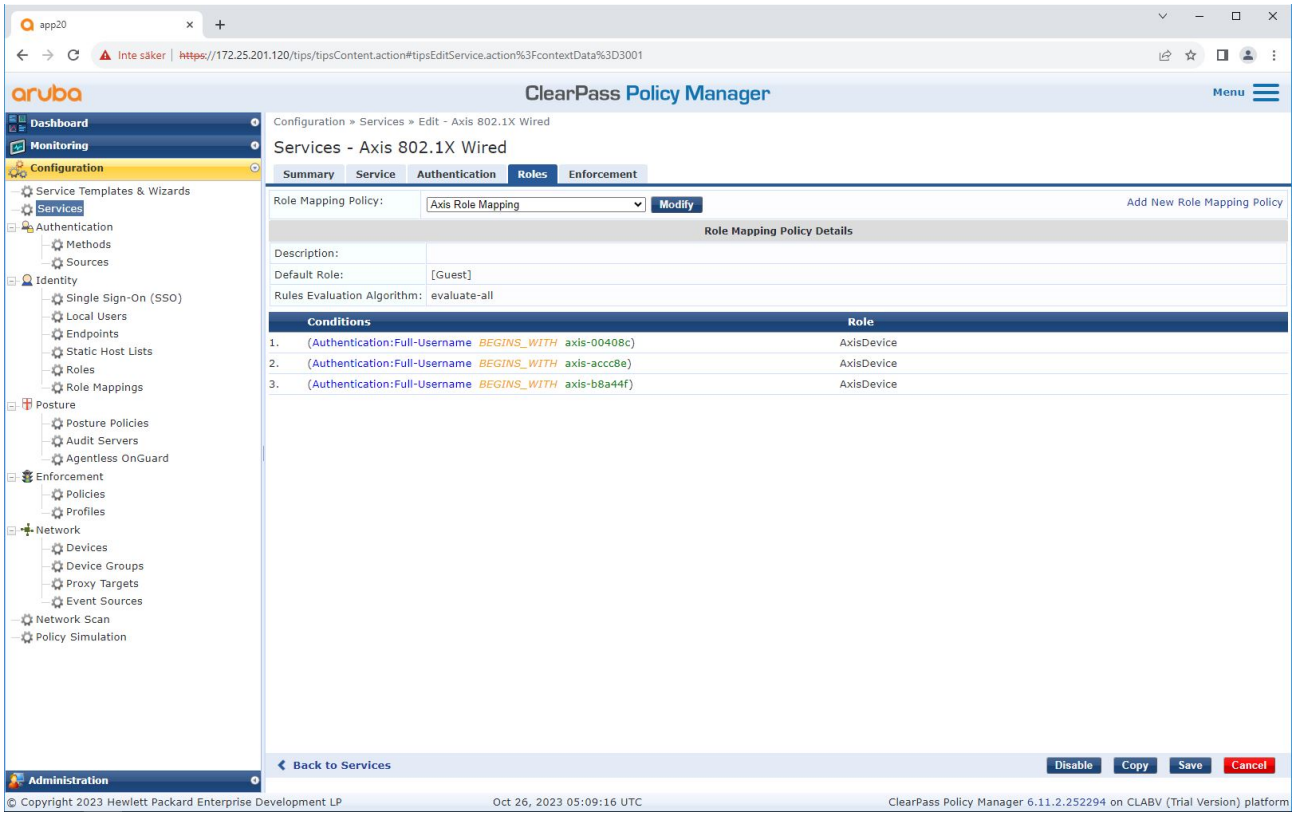

*添加 Axis 设备的角色名称。该名称是 Aruba 接入交换机配置中的端口访问角色名称。*



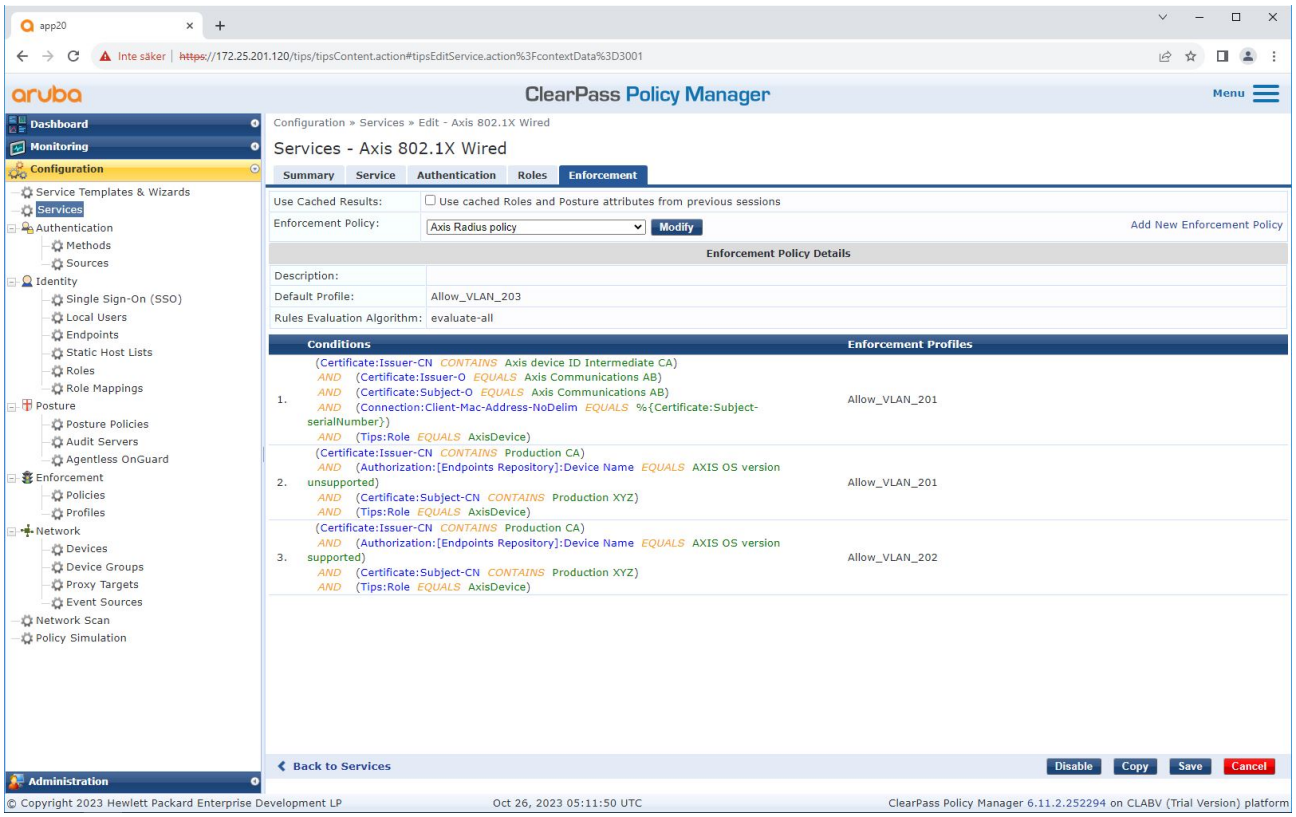

*为之前创建的 Axis 设备角色添加 Axis 角色映射策略。设备映射到 Axis 设备角色需要定义的条件。如果不满足条件，设备将成为 [Guest] 角色的一部分。*

默认情况下，Axis 设备使用 EAP 身份格式“axis-serialnumber”。Axis 设备的序列号是其 MAC 地址。例如“axis-b8a44f45b4e6”。

## 设备配置

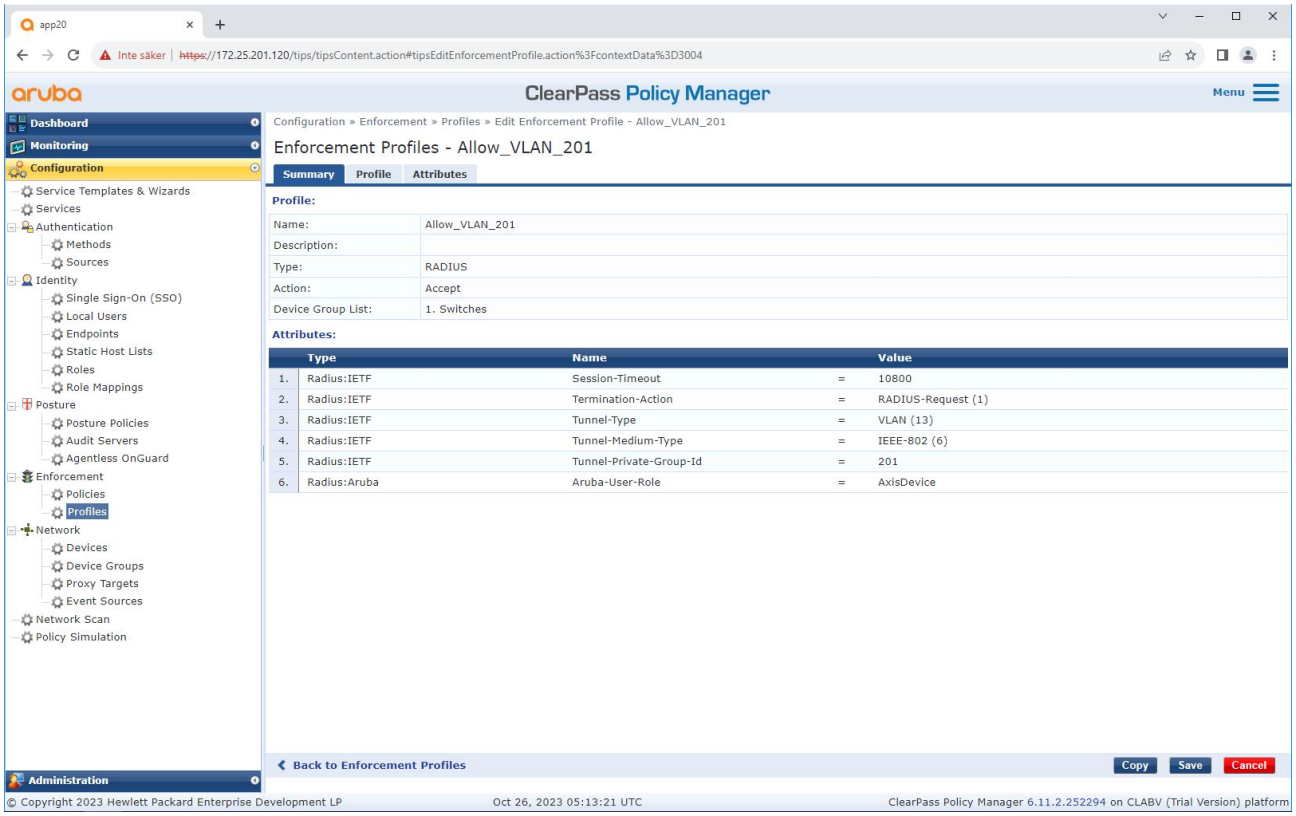



*将之前创建的 Axis 角色映射策略添加到将 IEEE 802.1X 定义为 Axis 设备加入的连接方法的服务中。*




*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。*

## Aruba 接入交换机

除了*Aruba 接入交换机 15*中描述的安全登录配置之外，参考下面 Aruba 接入交换机的端口配置示例进行配置 IEEE 802.1AE MACsec。

```
macsec 策略 macsec-eap
cipher-suite gcm-aes-128

端口访问角色 AxisDevice
关联 macsec-policy macsec-eap
验证模式客户端模式

AAA 身份验证端口访问 dot1x 身份验证器
macsec
mkacak-length 16
启用
```

## 旧版板载 - MAC 身份验证

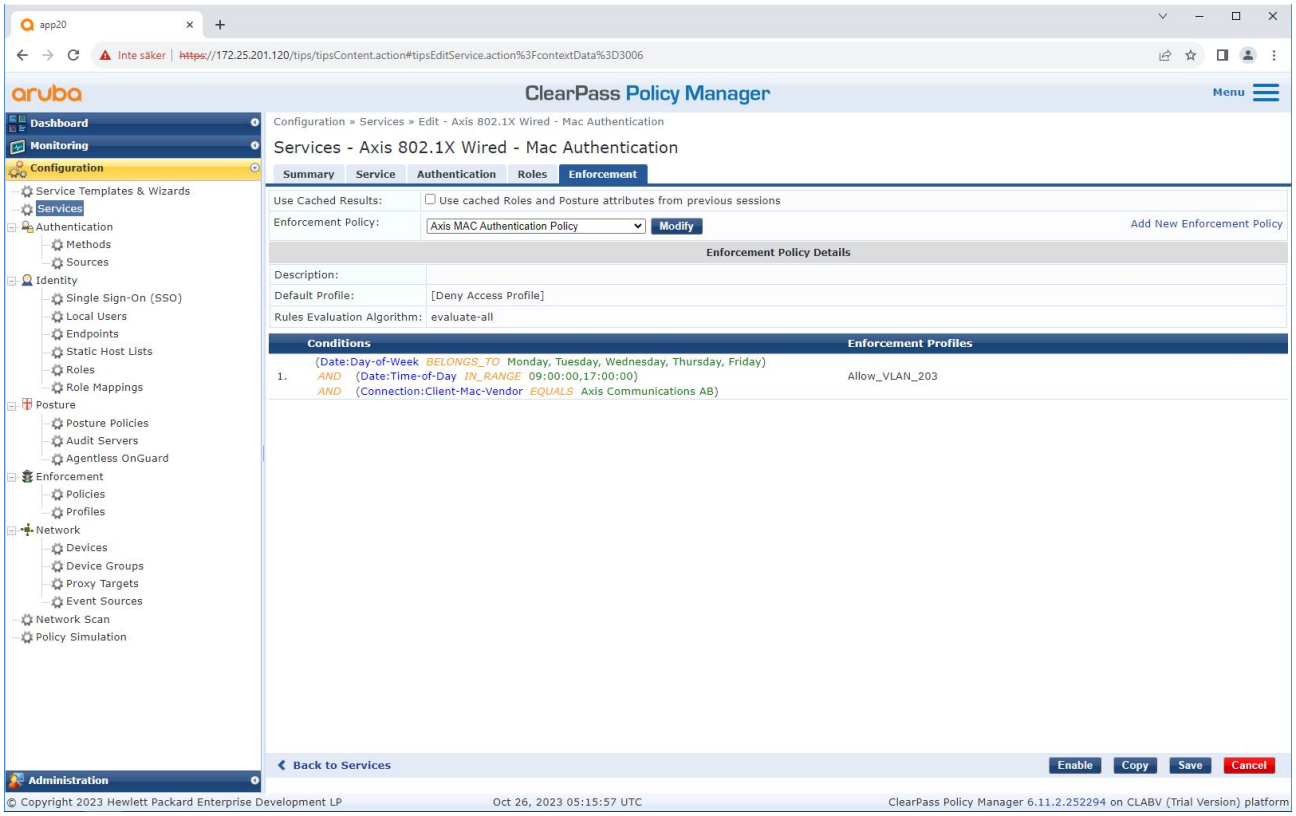
您可以使用 MAC 身份验证绕过（MAB）来板载不支持 IEEE 802.1AR的 Axis 设备，使用 Axis 设备 ID 证书进行注册，以及在出厂默认状态下启用 IEEE 802.1X。如果 802.1X 板载失败，Aruba ClearPass Policy Manager 会验证 Axis 设备的 MAC 地址并授予对网络的访问权限。

MAB 需要 Aruba 接入交换机和 ClearPass Policy Manager 配置准备。在 Axis 设备上，无需配置即可允许 MAB 载入。

### Aruba ClearPass 策略管理器

#### 强制政策

Aruba ClearPass 策略管理器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 Axis 设备访问 Aruba 网络的权限。




##### 拒绝网络访问

当 Axis 设备不符合配置的强制策略时，它会被拒绝访问网络。

##### 访客网络（VLAN 203）

如果满足以下条件，Axis 设备将被授予访问受限、隔离网络的权限：

- 这是周一到周五之间的一个工作日
- 时间为 09:00 至 17:00

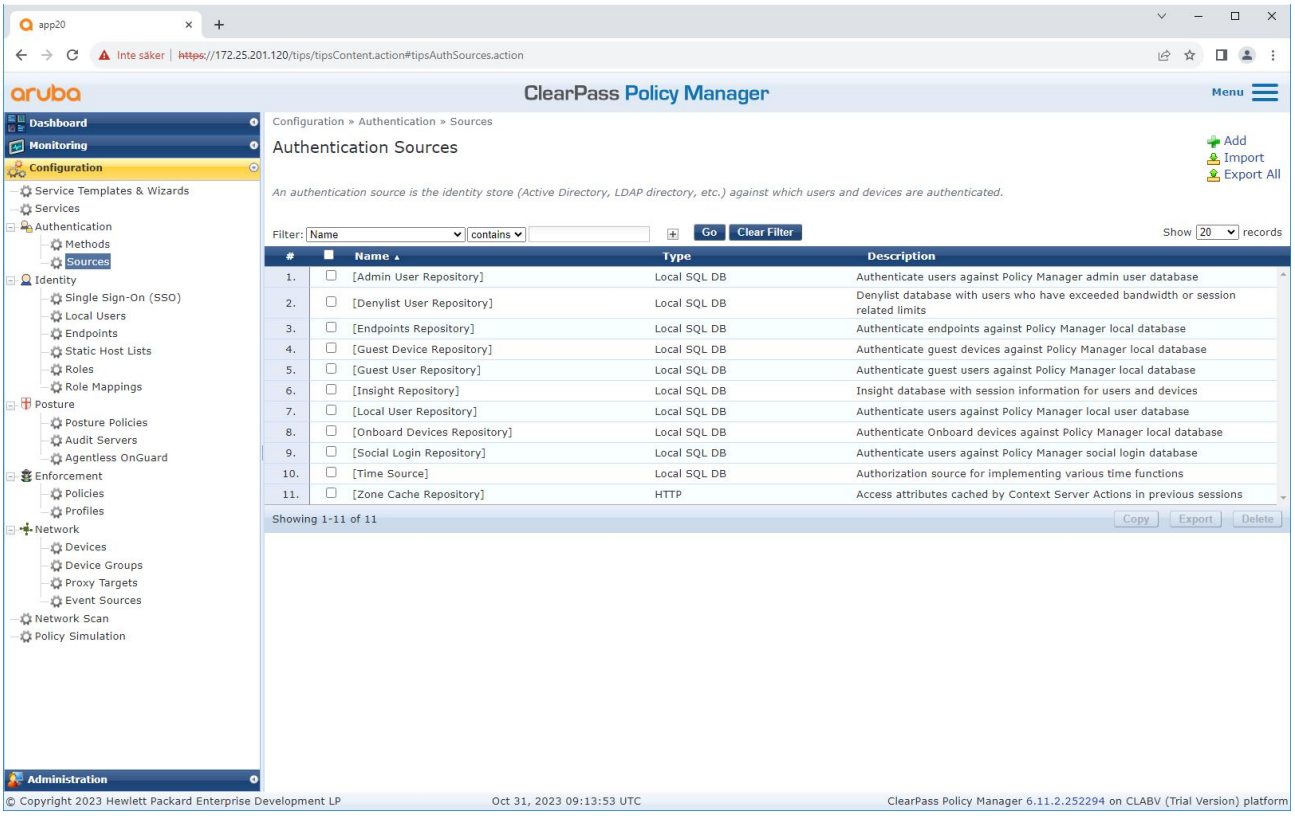
## 旧版板载 - MAC 身份验证

- MAC 地址供应商与 Axis Communications AB 匹配。

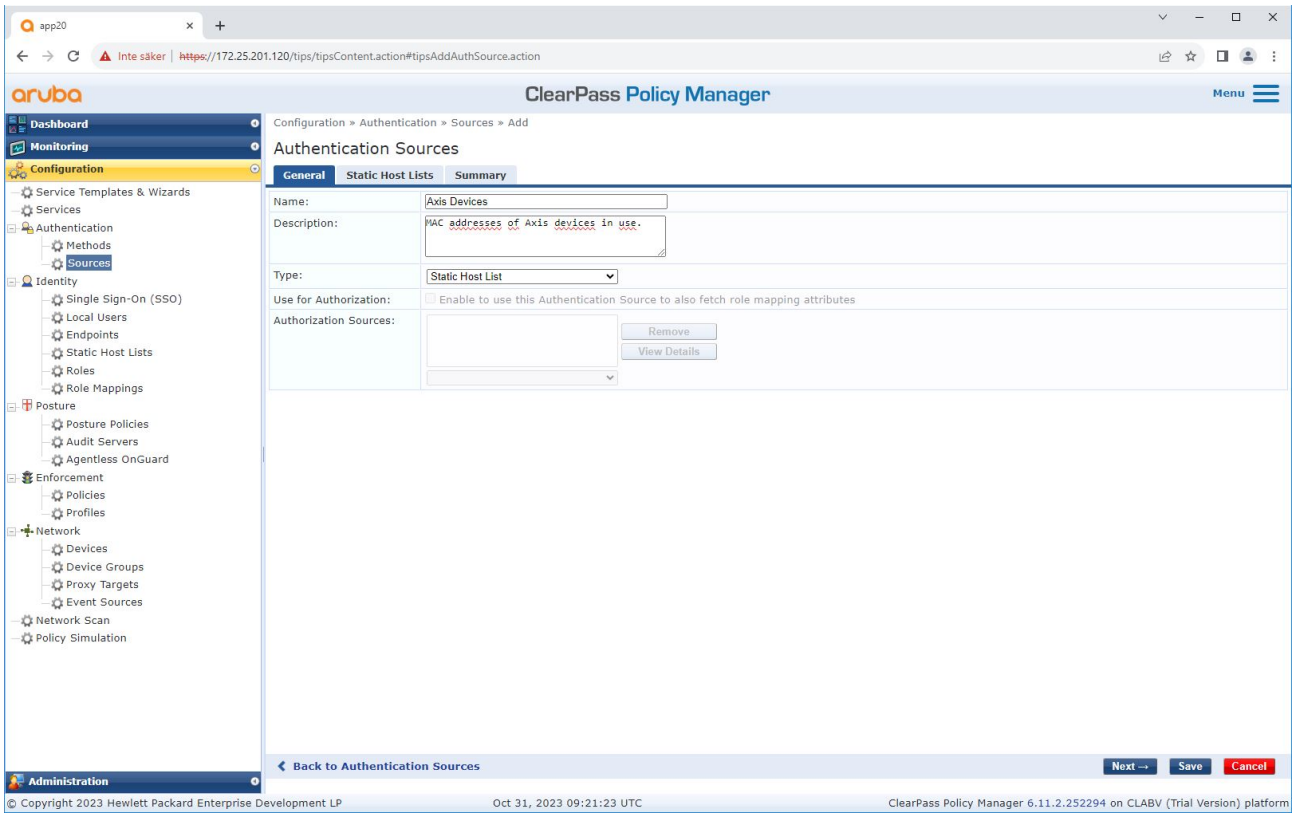
由于 MAC 地址可能被欺骗，因此不会授予对常规配置网络的访问权限。我们建议您仅使用 MAB 进行初始启动，并进一步手动检查设备。

### 来源配置

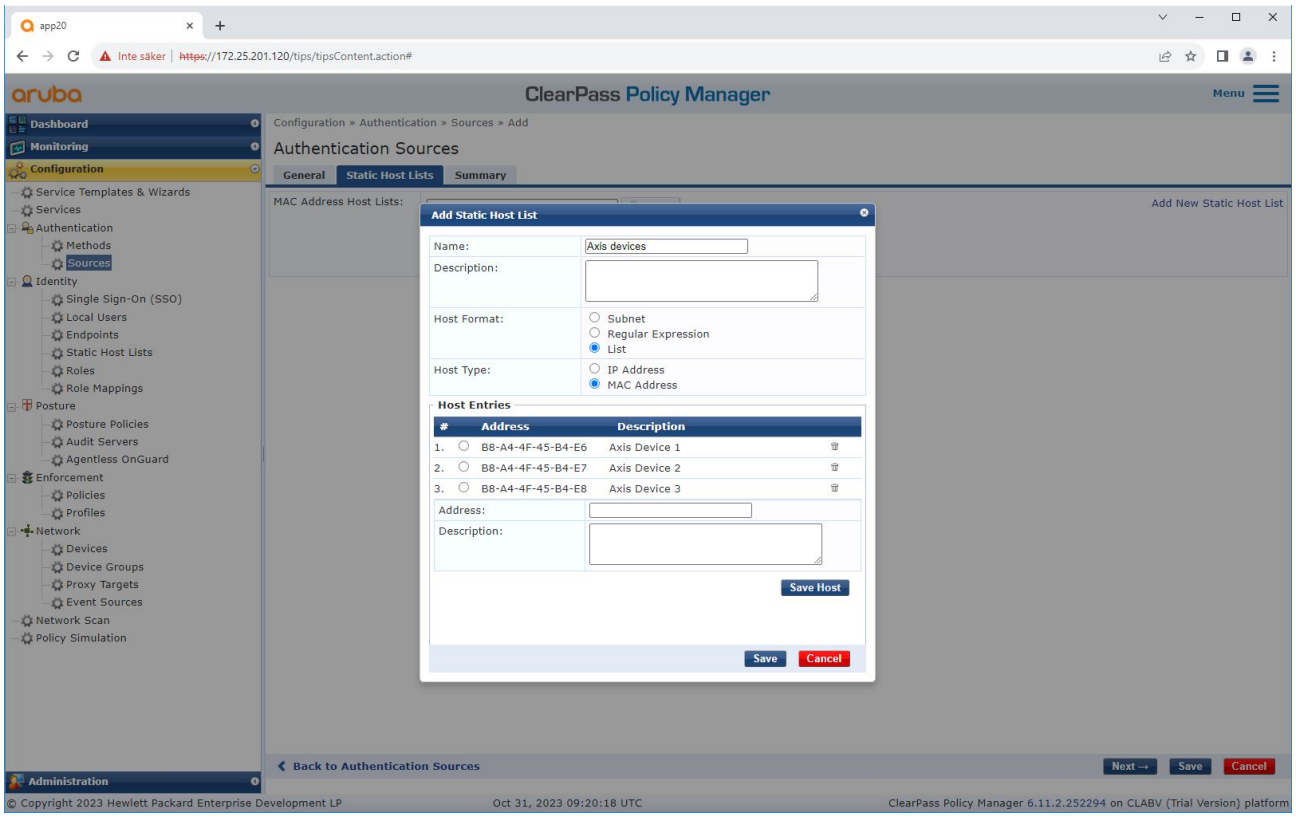
在来源界面中，创建一个新的身份验证源，仅允许手动导入的 MAC 地址。



## 旧版板载 - MAC 身份验证

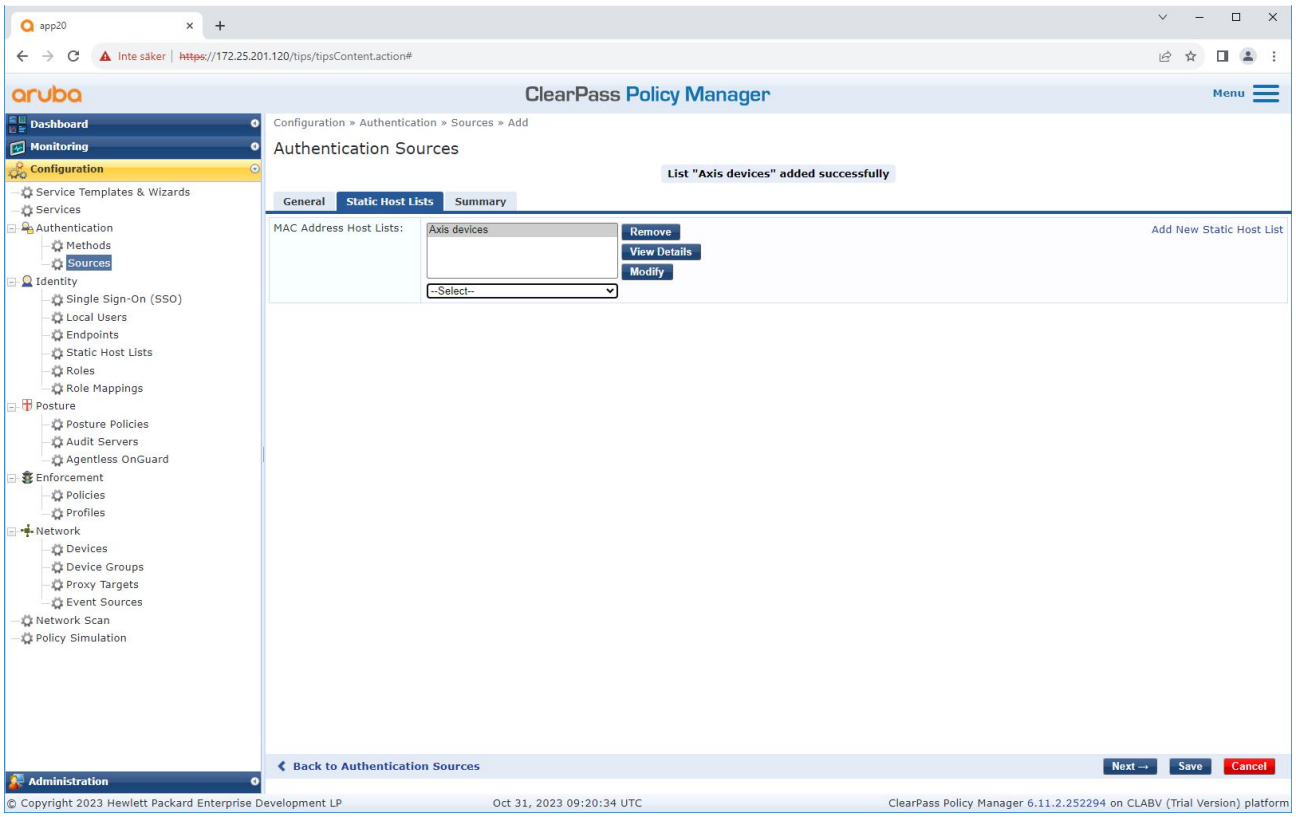


## 旧版板载 - MAC 身份验证




*创建了包含 Axis MAC 地址的静态主机列表。*

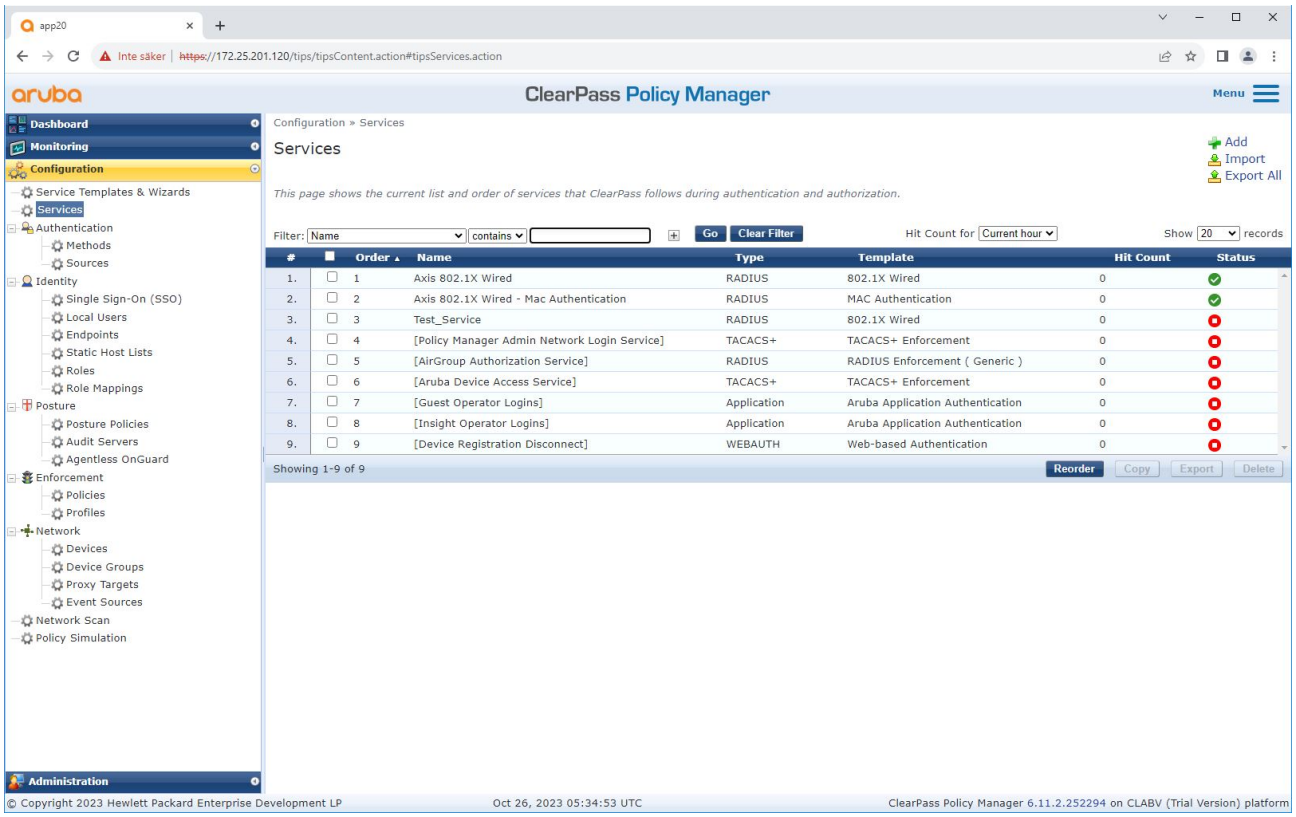
## 旧版板载 - MAC 身份验证



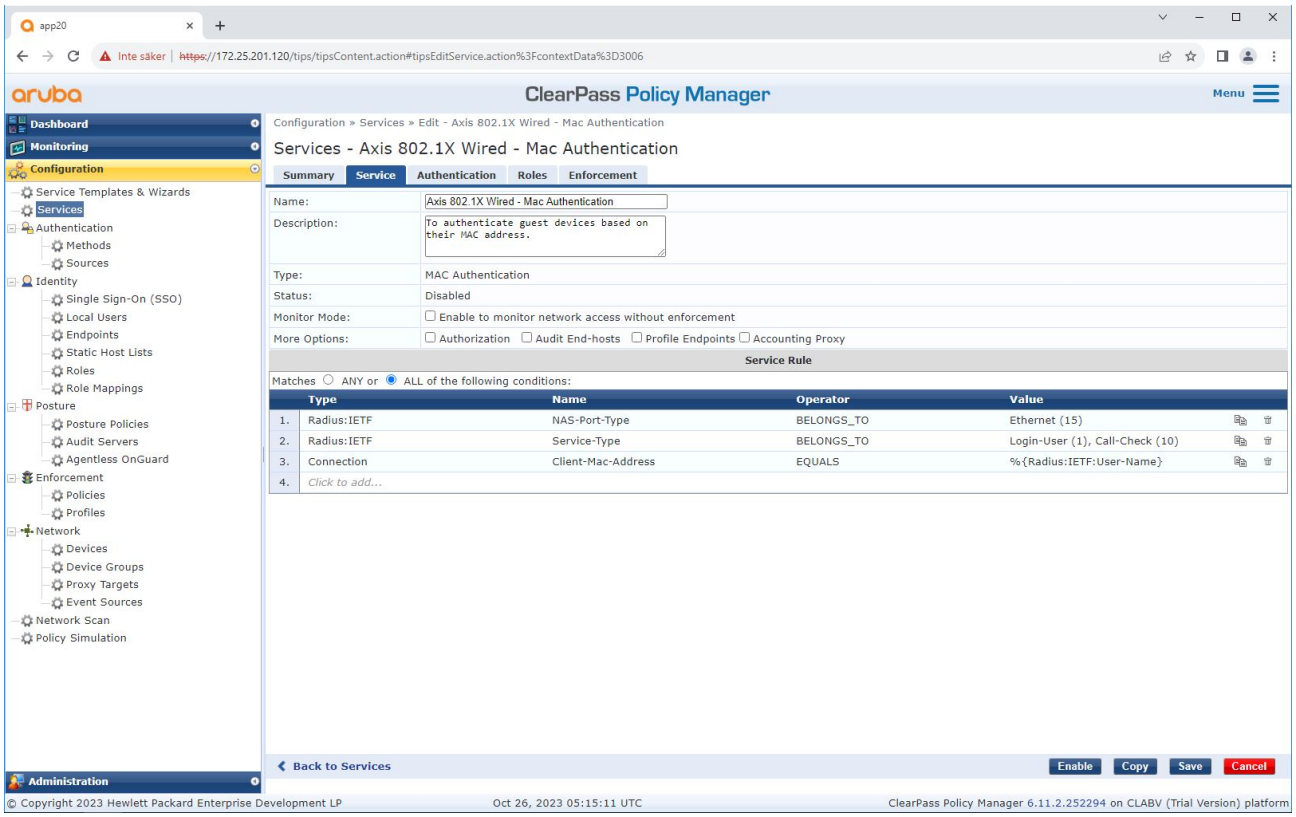

### 设备配置

在服务界面中，配置步骤合并为一项服务，用于处理 Aruba 网络中 Axis 设备的身份验证和授权。

## 旧版板载 - MAC 身份验证

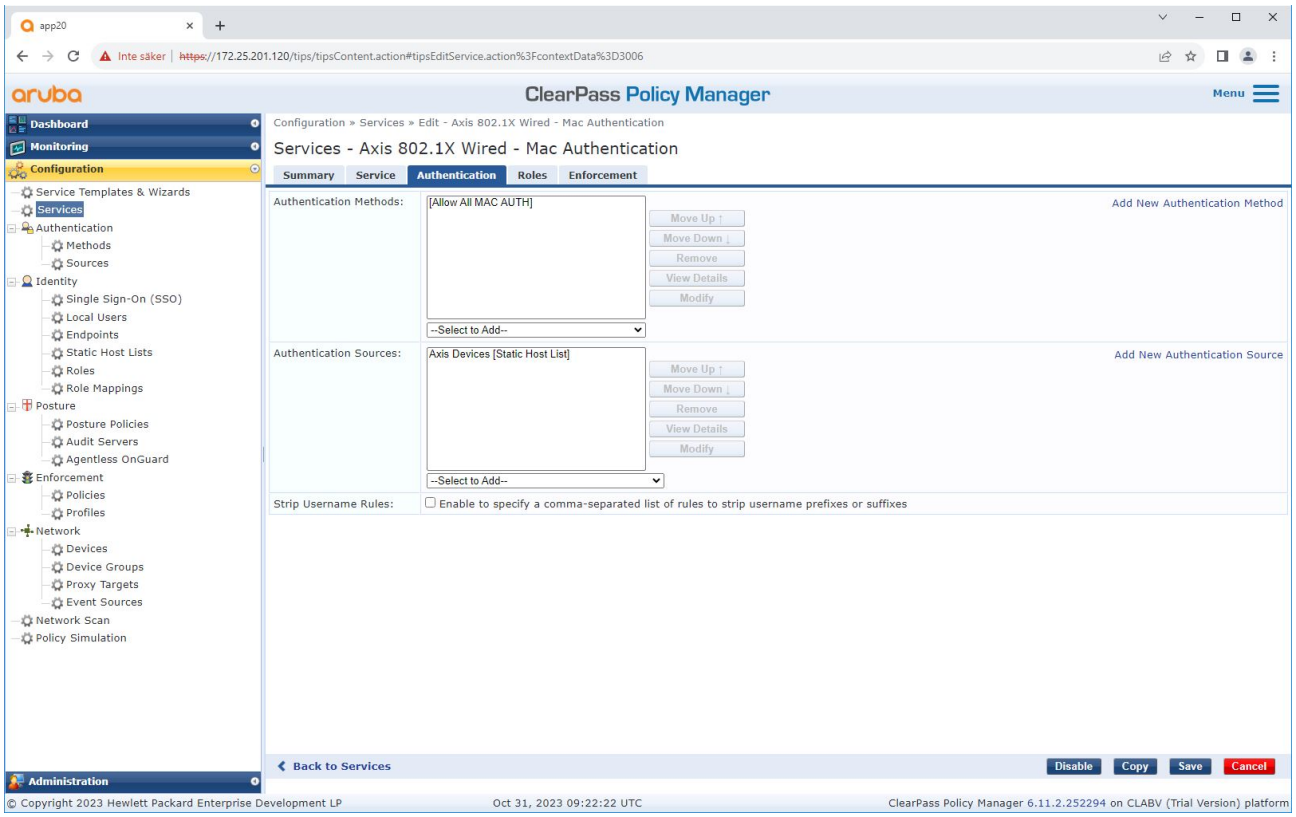


## 旧版板载 - MAC 身份验证




*创建了将 MAB 定义为连接方法的专用的 Axis 服务。*

## 旧版板载 - MAC 身份验证

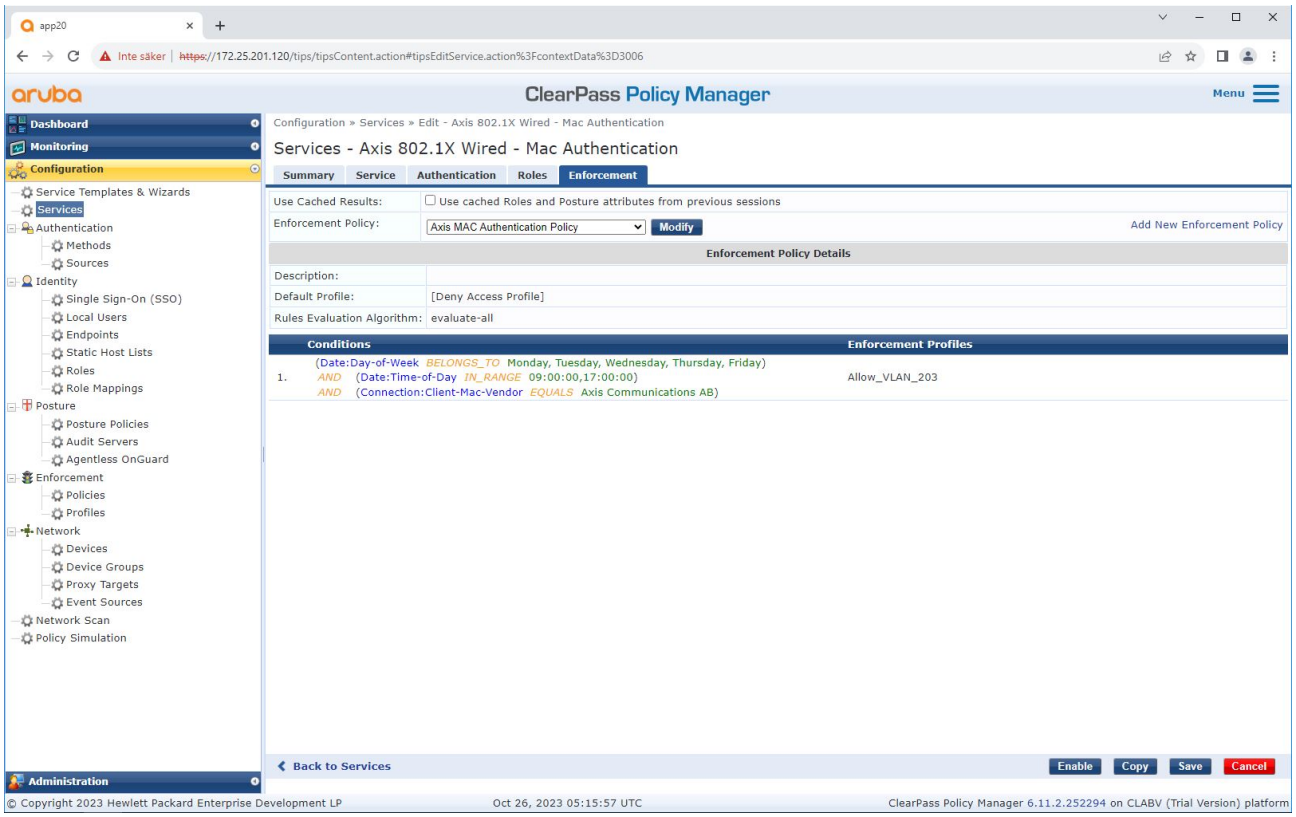



*将预先配置的 MAC 认证方法配置到服务中。此外，还会选择先前创建的包含 Axis MAC 地址列表的身份验证源。*

Axis Communications AB 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

## 旧版板载 - MAC 身份验证




*在尾部步骤中，之前创建的强制策略配置到服务。*

## Aruba 接入交换机

除了*Aruba 接入交换机 15*中描述的安全登录配置之外，请参阅以下 Aruba 接入交换机的端口配置示例以允许 MAB。

```
AAA 端口访问验证器 18 发送周期 5
AAA 端口访问验证器 19 发送周期 5
AAA 端口访问验证器 18 上限请求数 3
AAA 端口访问验证器 19 上限请求数 3
AAA 端口访问验证器 18 客户端限制 1
AAA 端口访问验证器 19 客户端限制 1
AAA 端口访问基于 mac 的 18-19
AAA 端口访问 18 身份验证顺序验证器基于 mac
AAA 端口访问 19 auth-order 验证器基于 mac
AAA 端口访问 18 身份验证优先级验证器基于 mac
AAA 端口访问 19 身份验证优先级验证器基于 mac
```

用户手册
Secure integration of Axis devices into Aruba networks

版本 M4.3
日期：十一月 2023
零件号 T10197992