HPE Aruba Networking

Integration Guide

HPE Aruba Networking

Table of Contents

HPE Aruba Networking

Introduction

Introduction

This integration guide aims to outline the best-practice configuration of how to onboard and operate Axis devices in HPE Aruba Networking powered networks. The configuration uses modern security standards and protocols such as IEEE 802.1X, IEEE 802.1AR, IEEE 802.1AE, and HTTPS.

Establishing proper automation for network integration can save time and money. It allows the removal of unnecessary system complexity when using Axis device management applications combined with HPE Aruba Networking infrastructure and applications. Below are some benefits that can be gained when combining Axis devices and software with a HPE Aruba Networking infrastructure:

- Minimize system complexity by removing device staging networks.
- Save costs by adding automating onboarding processes and device management.
- Take advantage of zero-touch network security controls provided by Axis devices.
- Increase overall network security by applying HPE and Axis expertise.

The network infrastructure must be prepared to securely verify the integrity of the Axis devices before starting the configuration. This allows a smooth software defined transition between logical networks throughout the on-boarding process. It's necessary to have knowledge about the following areas before doing the configuration:

- Managing enterprise network IT-infrastructure from HPE Aruba Networking including HPE Aruba Networking access switches and HPE Aruba Networking ClearPass Policy Manager.
- Expertise in modern network access control techniques and network security policies.
- Basic knowledge about Axis products is desirable but is provided throughout the guide.

Secure onboarding - IEEE 802.1AR/802.1X

To watch this video, go to the web version of this document.

help.axis.com/?&tpiaId=&section=secure-onboarding-ieee802-1ar-802-1x

Secure device onboarding onto zero-trust networks with IEEE 802.1X/802.1AR

Initial authentication

Connect the Axis Edge Vault supported Axis device to authenticate the device against the network. The device use the IEEE 802.1AR Axis device ID certificate through the IEEE 802.1X network access control to authenticate itself.

To grant access to the network, ClearPass Policy Manager verifies the Axis device ID together with other device specific fingerprints. The information, such as MAC-address and running AXIS OS, is used to make a policy-based decision.

The Axis device authenticates against the network using the IEEE 802.1AR compliant Axis device ID certificate.

The Axis device authenticates against the HPE Aruba Networking powered network using the IEEE 802.1AR-compliant Axis device ID certificate.

1. *Axis device ID*
2. *IEEE 802.1x EAP-TLS network authentication*
3. *Access switch (authenticator)*
4. *ClearPass Policy Manager*

Provisioning

After authentication, the Axis device moves into the provisioning network (VLAN201) where AXIS Device Manager is installed. Through AXIS Device Manager, device configuration, security hardening, and AXIS OS updates can be performed. To complete the device provisioning, new customer specific production-grade certificates are uploaded onto the device for IEEE 802.1X and HTTPS.

After successful authentication, the Axis device moves into a provisioning network for configuration.

1. *Access switch*
2. *Provisioning network*
3. *ClearPass Policy Manager*
4. *Device management application*

Production network

The provisioning of the Axis device with new IEEE 802.1X certificates triggers a new authentication attempt. ClearPass Policy Manager verifies the new certificates and decide whether to move the Axis device into the production network or not.

After the device configuration, the Axis device leaves the provisioning network and attempts to reauthenticate against the network.

1 *Axis device ID*
2 *IEEE 802.1x EAP-TLS network authentication*
3 *Access switch (authenticator)*
4 *ClearPass Policy Manager*

After reauthentication, the Axis device moves into the production network (VLAN 202). In that network, the Video Management System (VMS) connects to the Axis device and starts to operate.

The Axis device is granted access to the production network.

1 *Access switch*
2 *Production network*
3 *ClearPass Policy Manager*
4 *Video management system*

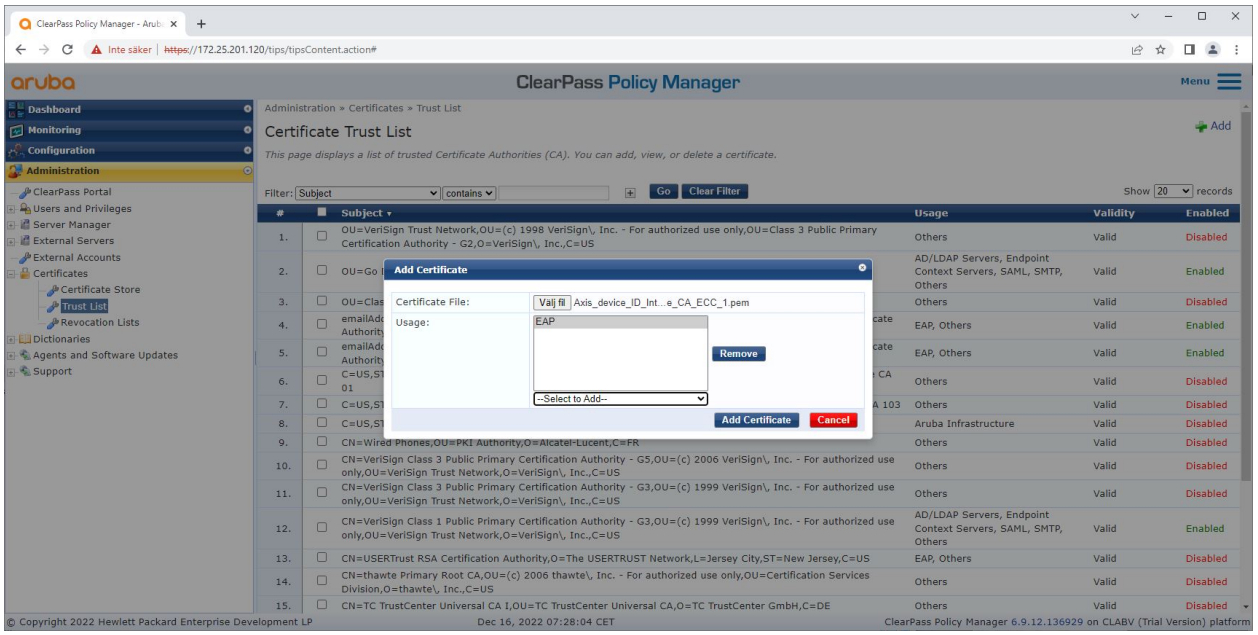
Configuration HPE Aruba Networking

HPE Aruba Networking ClearPass Policy Manager

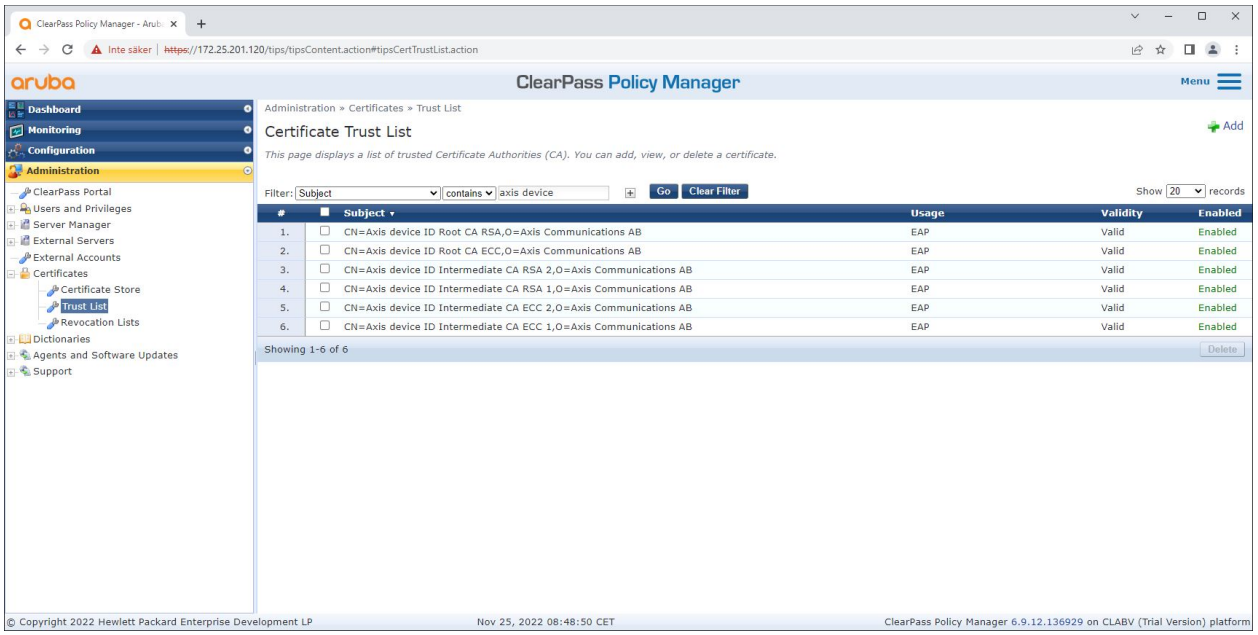
ClearPass Policy Manager provides role- and device based secure network access control for IoT, BYOD, corporate devices, employees, contractors, and guests across and multivendor wired, wireless, and VPN infrastructure.

Trusted certificate store configuration

1. Download the Axis-specific IEEE 802.1AR certificate chain from axis.com.
2. Upload the Axis-specific IEEE 802.1AR Root CA and Intermediate CA certificate chains into the trusted certificate store.
3. Enable ClearPass Policy Manager to authenticate Axis devices through IEEE 802.1X EAP-TLS.
4. Select EAP in the usage field. The certificates are used for IEEE 802.1X EAP-TLS authentication.



Upload the Axis-specific IEEE 802.1AR certificates to the trusted certificate store of ClearPass Policy Manager.



The trusted certificate store in ClearPass Policy Manager with Axis-specific IEEE 802.1AR certificate chain included.

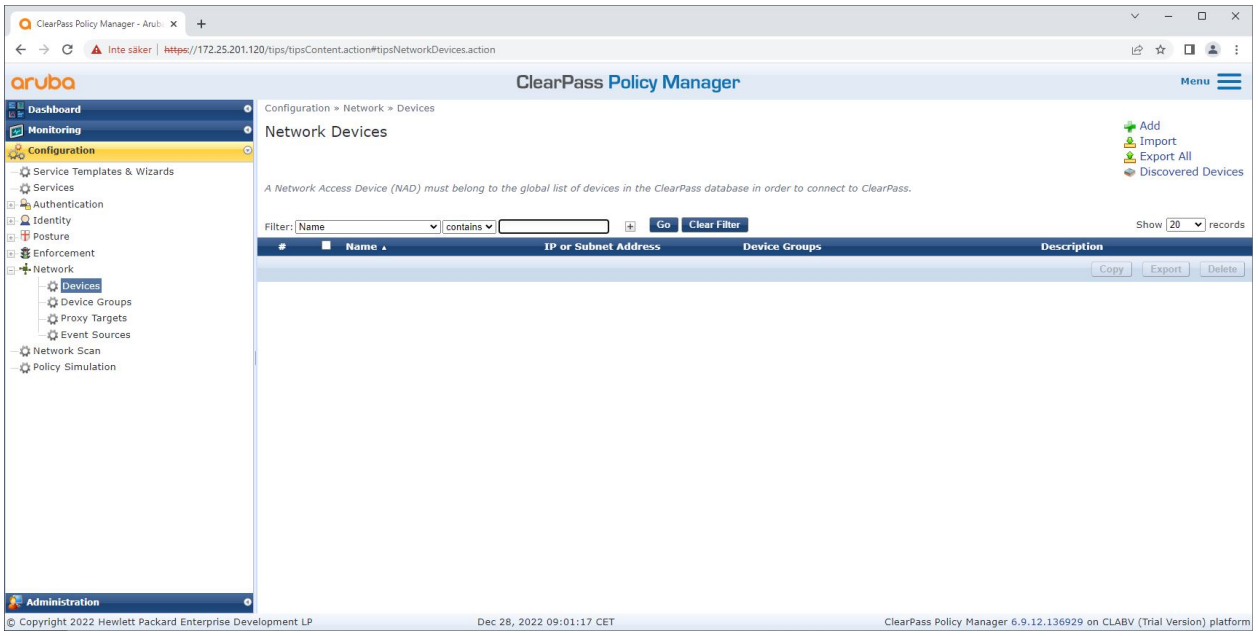
Network device/group configuration

1. Add trusted network access devices, such as HPE Aruba Networking access switches, to ClearPass Policy Manager. ClearPass Policy Manager needs to know which access switches in the network are used for IEEE 802.1X communication.

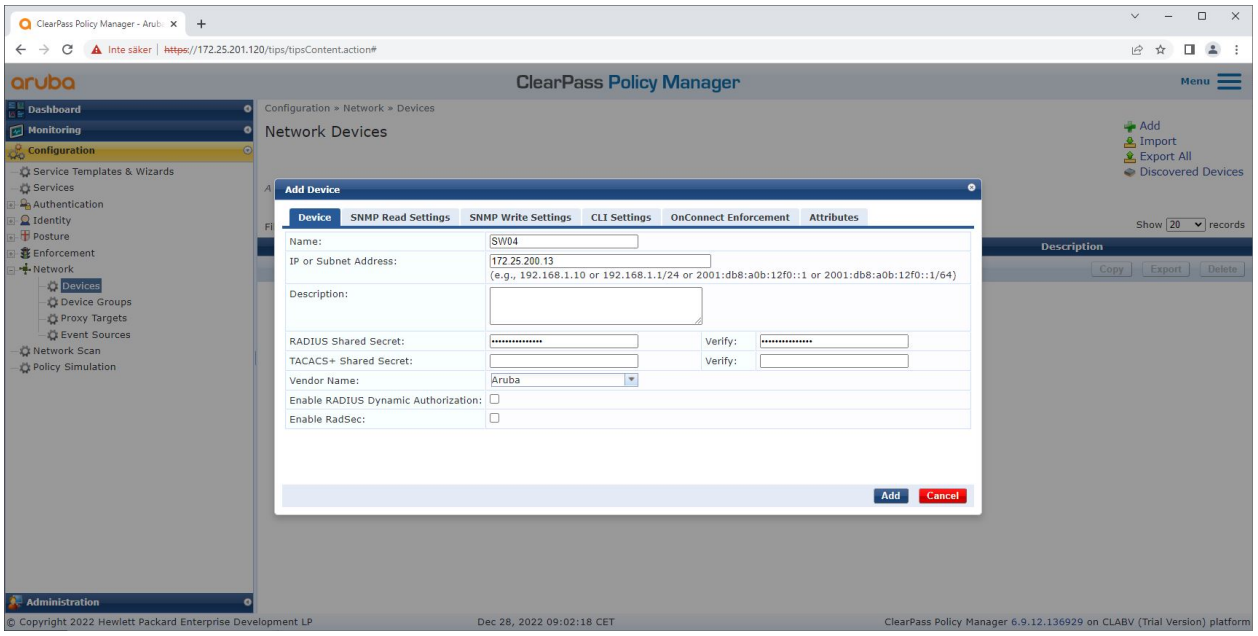
2. Use the network device group configuration to group several trusted network access devices. Grouping trusted network access devices allows easier policy configuration.

3. The RADIUS shared secret needs to match the specific switch IEEE 802.1X configuration.

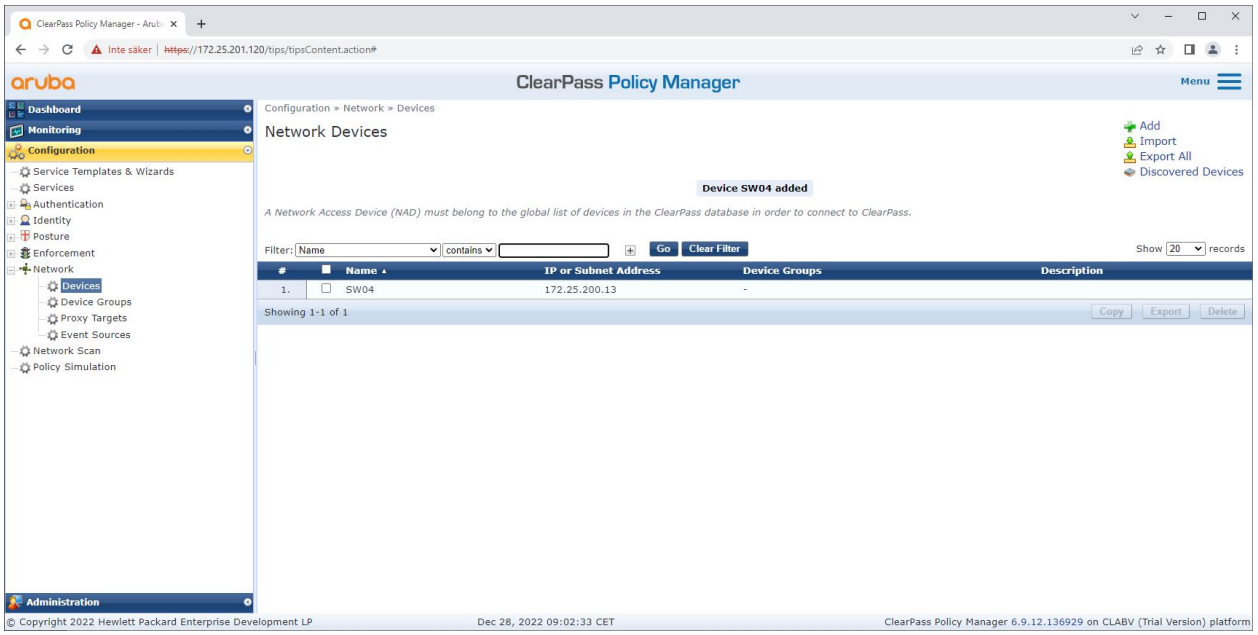
Secure onboarding - IEEE 802.1AR/802.1X



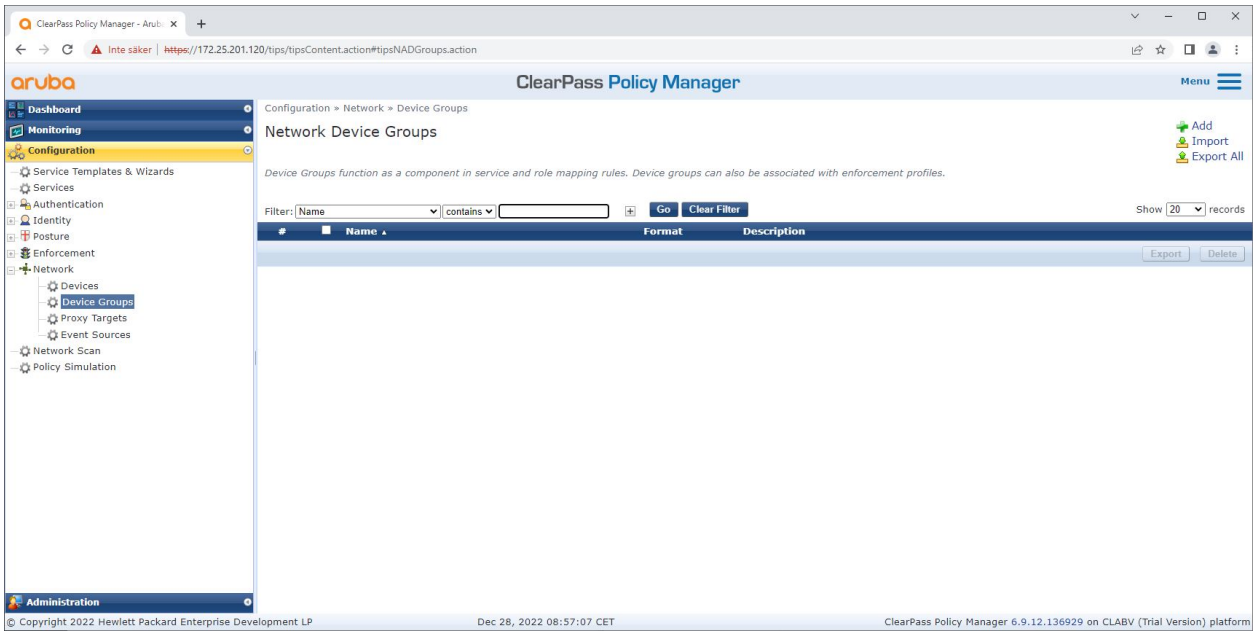
The trusted network devices interface in ClearPass Policy Manager.



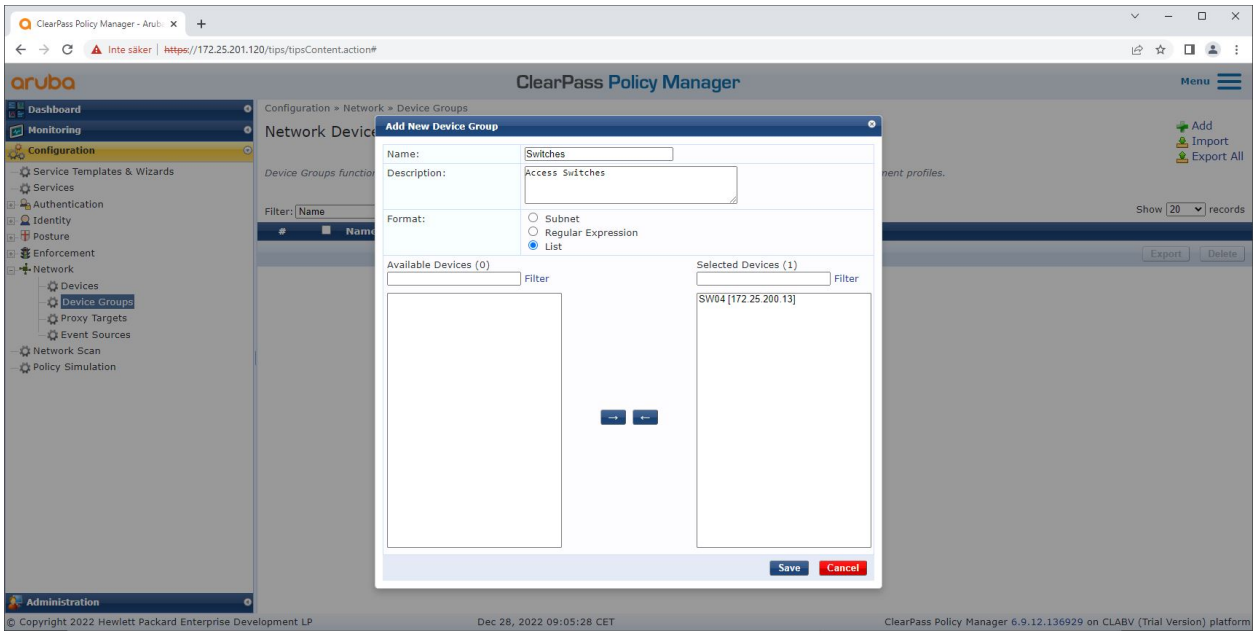
Add the HPE Aruba Networking access switch as trusted network device in ClearPass Policy Manager. Please note that the RADIUS shared secret must match the specific switch IEEE 802.1X configuration.



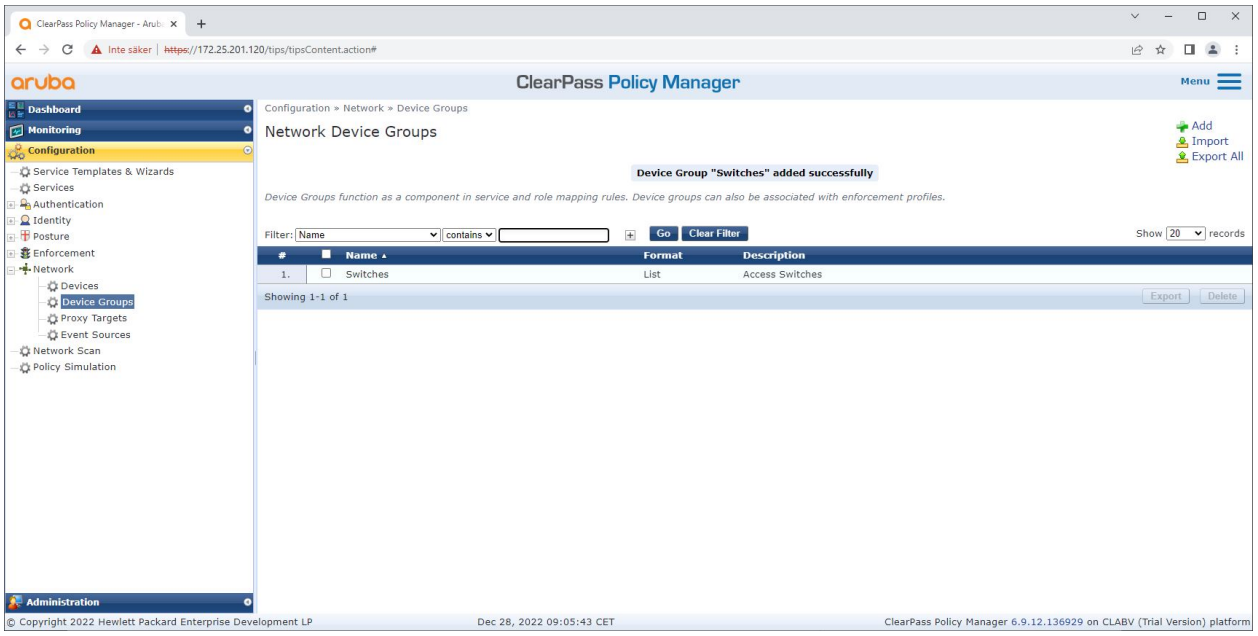
ClearPass Policy Manager with one trusted network device configured.



The trusted network device groups interface in ClearPass Policy Manager.



Add a trusted network access device into a new device group in ClearPass Policy Manager.



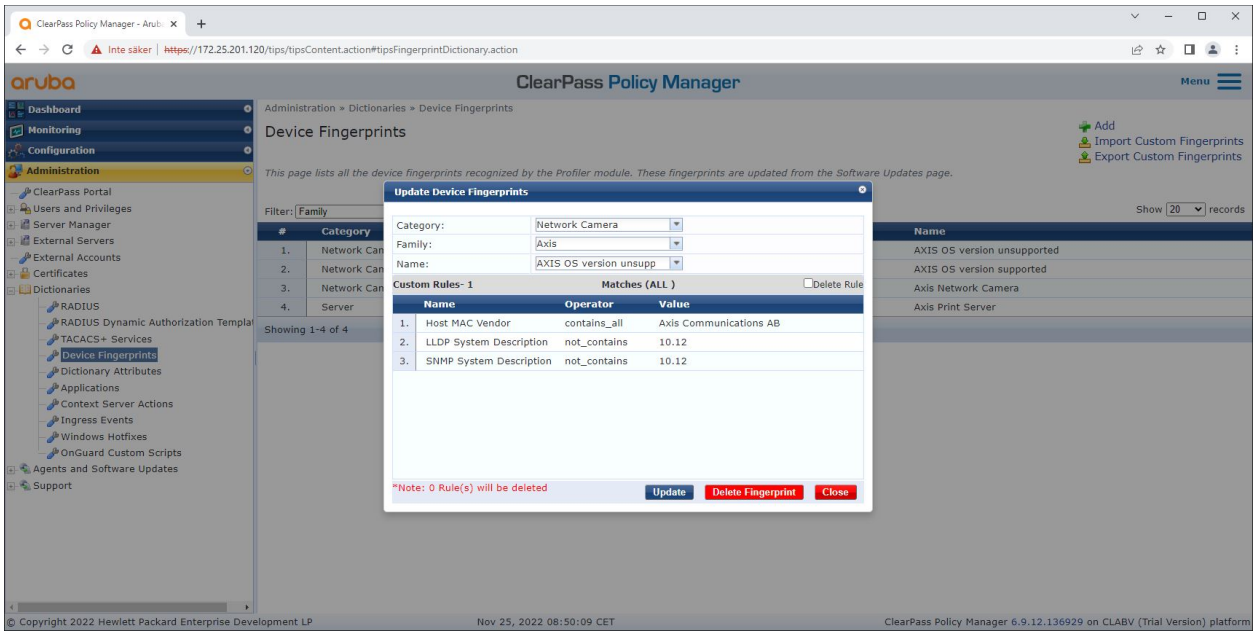
ClearPass Policy Manager with configured network device group that includes one or several trusted network devices.

Device fingerprint configuration

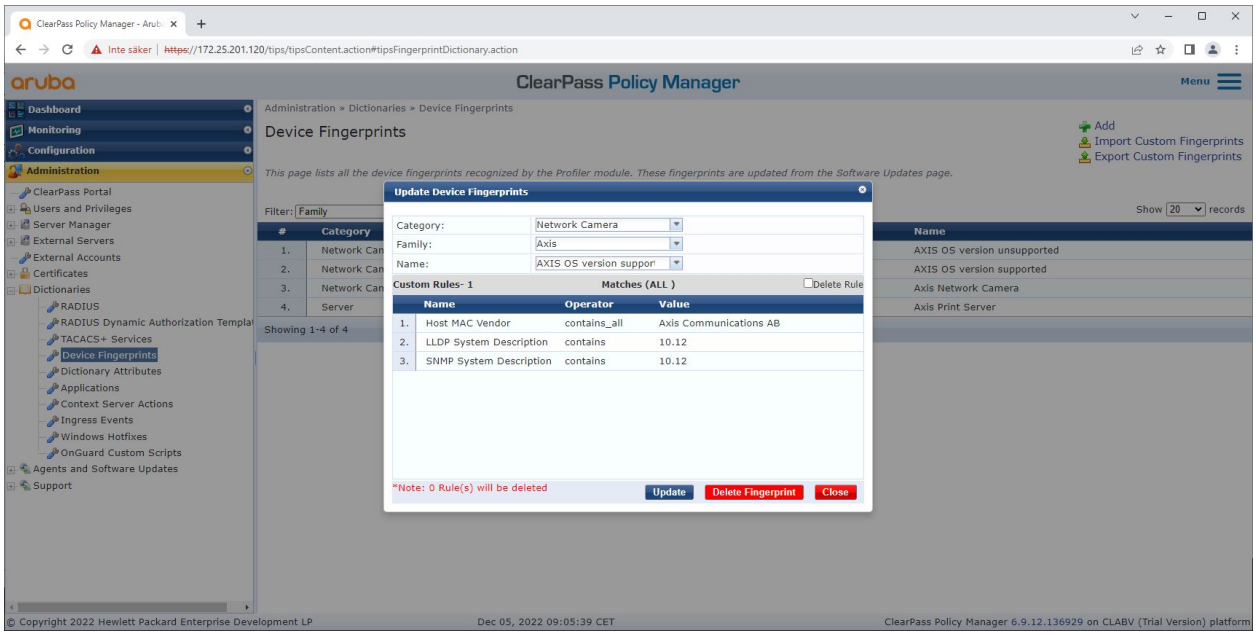
The Axis device can distribute device specific information, such as MAC-address and device software version, through network discovery. Use this information to create, update, or manage a device fingerprint in ClearPass Policy Manager. There you can also grant or deny access based on the AXIS OS version.

1. Go to **Administration > Dictionaries > Device Fingerprints**.
2. Select an existing device fingerprint or create a new device fingerprint.

3. Set the device fingerprint settings.



The device fingerprint configuration in ClearPass Policy Manager. Axis devices that run any other AXIS OS version other than 10.12 are considered unsupported.



The device fingerprint configuration in ClearPass Policy Manager. Axis devices that run AXIS OS 10.12 are considered supported in above example.

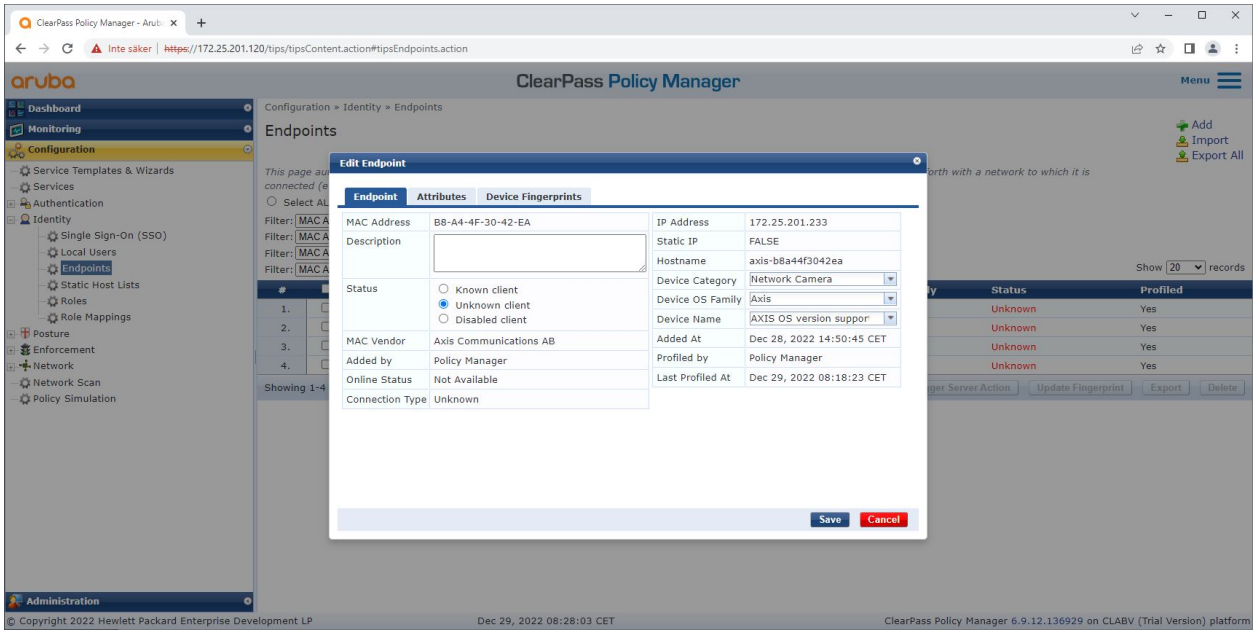
Information about the device fingerprint collected by ClearPass Policy Manager can be found in the Endpoints section.

1. Go to **Configuration > Identity > Endpoints**.

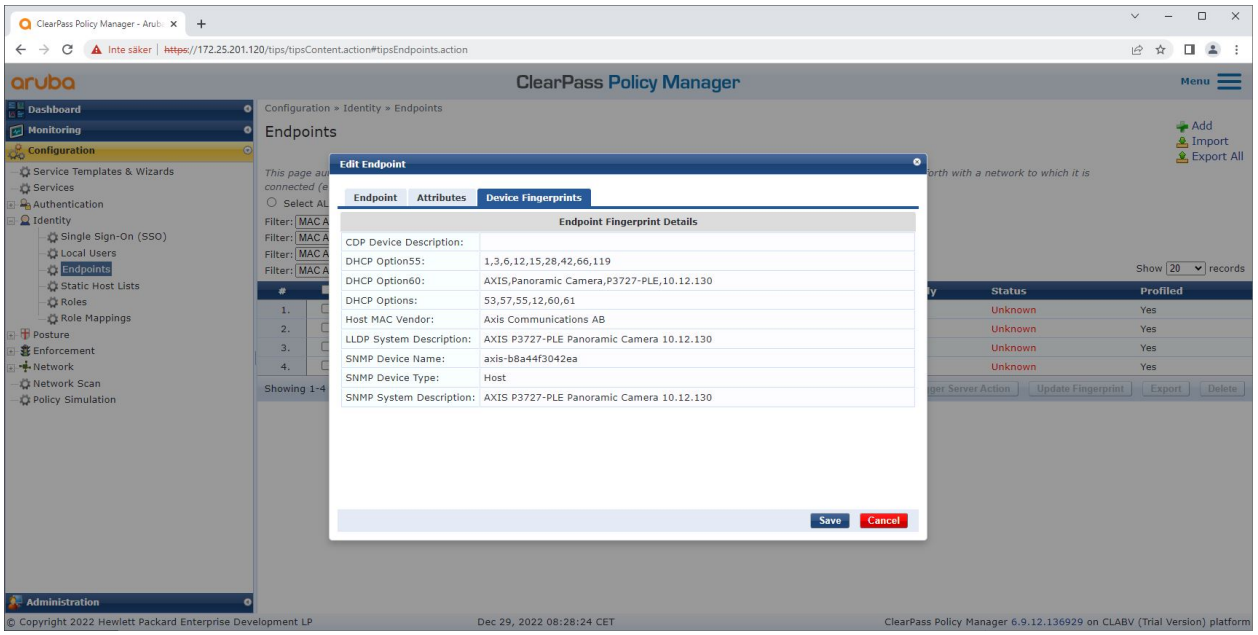
2. Select the device you want to view.
3. Click on the **Device Fingerprints** tab.

Note

SNMP is disabled by default in Axis devices and collected from the HPE Aruba Networking access switch.



An Axis device profiled by ClearPass Policy Manager.

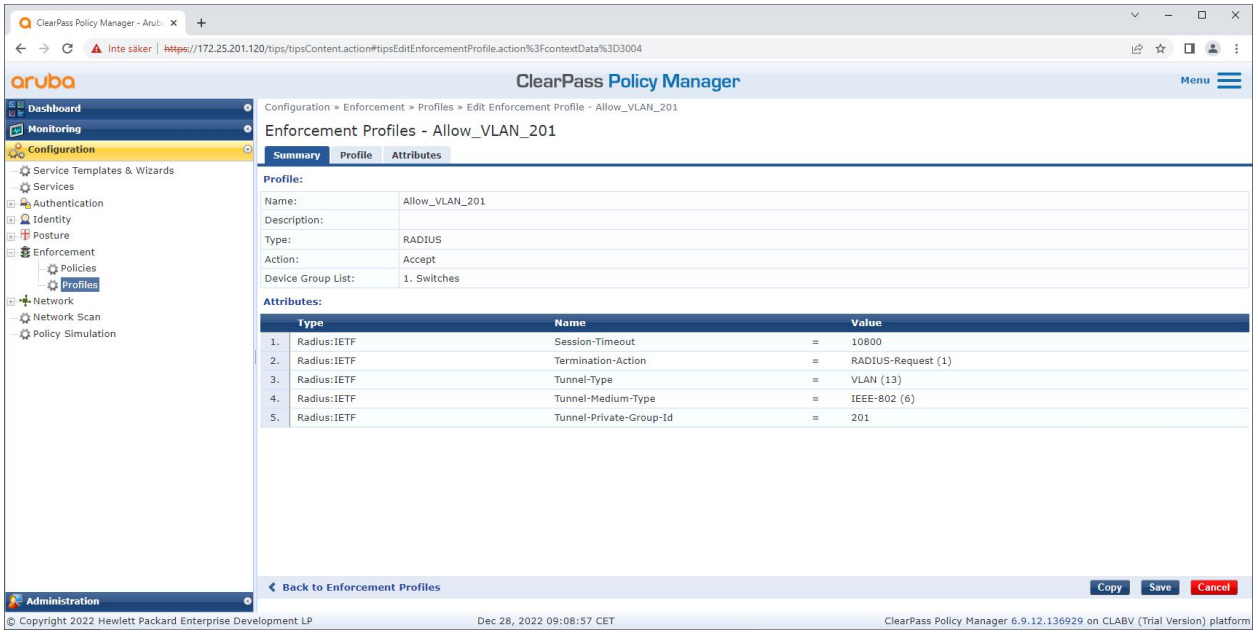


The detailed device fingerprints of a profiled Axis device. Please note that SNMP is disabled by default in Axis devices. LLDP, CDP and DHCP-specific discovery information are shared by the Axis device in factory defaulted state and relayed by the HPE Aruba Networking access switch to ClearPass Policy Manager.

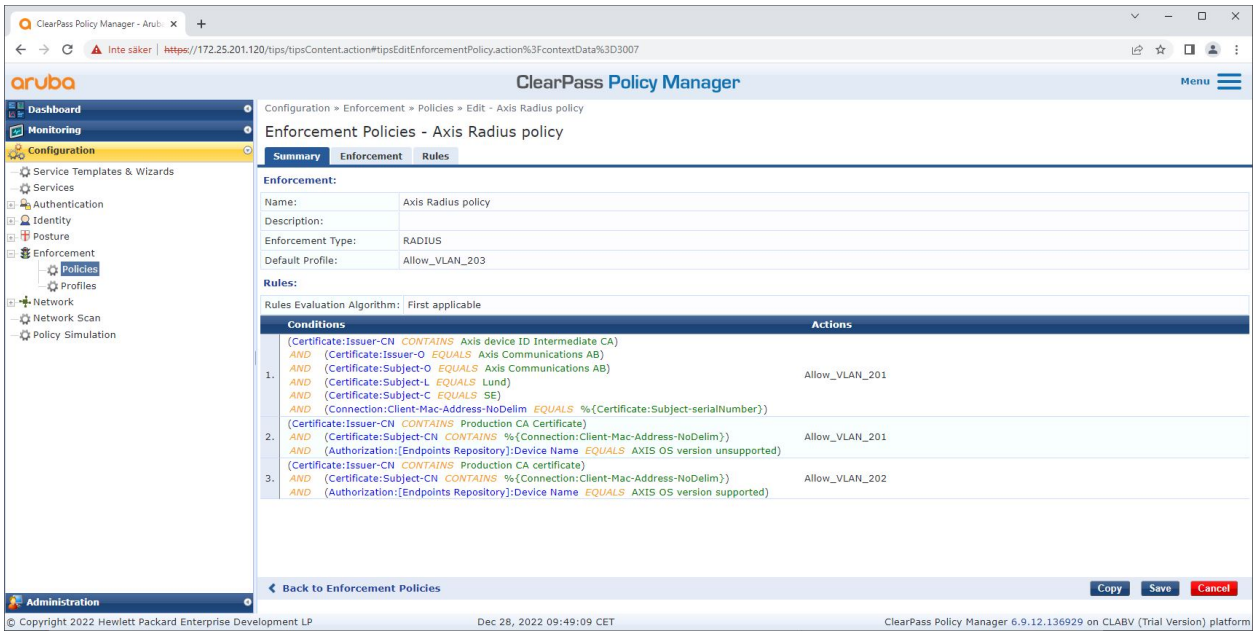
Enforcement profile configuration

Enforcement Profile is used to allow ClearPass Policy Manager to assign a specific VLAN ID to an access port on the switch. It's a policy-based decision that applies to the network devices in the device group "switches". The necessary number of enforcement profiles depends on the number of used VLANs. In our setup there is a total of three VLANs (VLAN 201, 202, 203), that correlates to three enforcement profiles.

After the enforcement profiles for the VLAN are configured, the actual enforcement policy can be configured. The enforcement policy configuration in ClearPass Policy Manager defines if Axis devices are granted access to HPE Aruba Networking powered networks based on four example policy profiles.



An example enforcement profile to allow access to VLAN 201.



The enforcement policy configuration in ClearPass Policy Manager.

The four enforcement policies and their actions are listed below:

Denied network access

Access to the network is denied when no IEEE 802.1X network access control authentication is performed.

Guest-network (VLAN 203)

The Axis device is granted access to a limited, isolated network if the IEEE 802.1X network access control authentication fails. Manual inspection of the device is required to take appropriate actions.

Provisioning network (VLAN 201)

The Axis device is granted access to a provisioning network. This is to provide Axis device management capabilities through *AXIS Device Manager* and *AXIS Device Manager Extend*. It also makes it possible to configure Axis devices with AXIS OS updates, production-grade certificates, and other configurations. The following conditions are verified by ClearPass Policy Manager:

- The Axis device's AXIS OS version.
- The MAC-address of the device matches the vendor-specific Axis MAC-address scheme with the serial number attribute of the Axis device ID certificate.
- The Axis device ID certificate is verifiable and matches the Axis-specific attributes such as issuer, organization, location, and country.

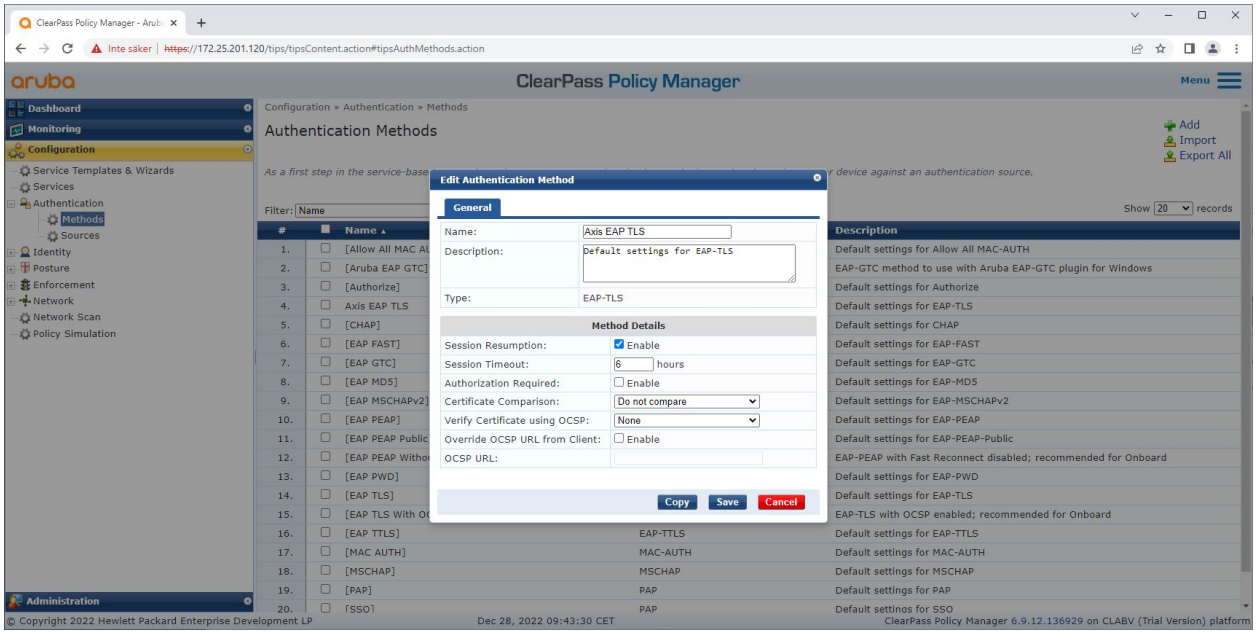
Production network (VLAN 202)

The Axis device is granted access to the production network where the Axis device should operate. Access is granted after the device provisioning is completed from within the provisioning network (VLAN 201). The following conditions are verified by ClearPass Policy Manager:

- The MAC-address of the device matches the vendor-specific Axis MAC-address scheme with the serial number attribute of the Axis device ID certificate.
- The Axis device's AXIS OS version.
- The production-grade certificate is verifiable by the trusted certificate store.

Authentication method configuration

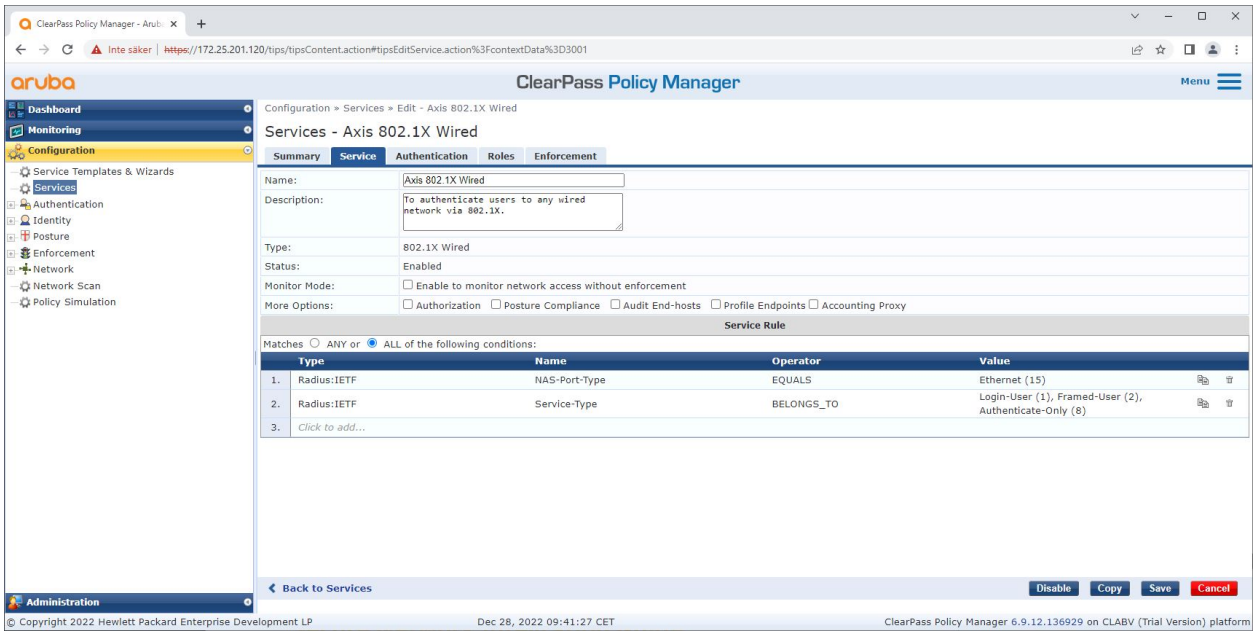
In the authentication method it's defined how an Axis device attempts to authenticate against the network. The preferred method of authentication should be IEEE 802.1X EAP-TLS since Axis devices with support for Axis Edge Vault come with IEEE 802.1X EAP-TLS enabled by default.



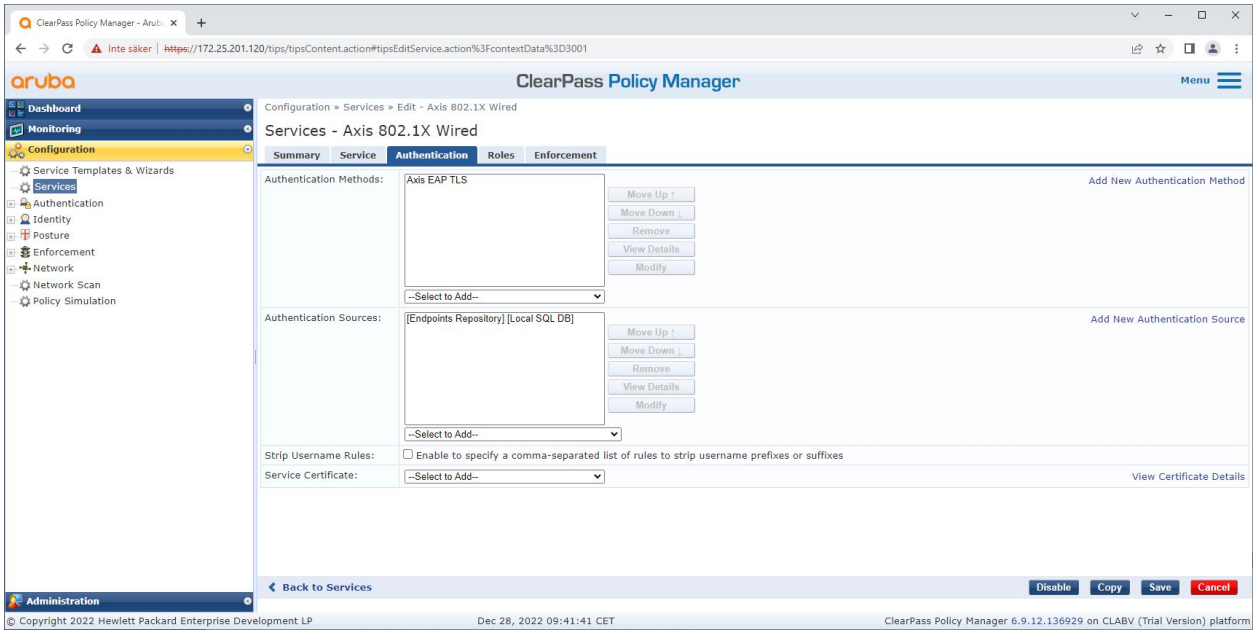
The authentication method interface of ClearPass Policy Manager where the EAP-TLS authentication method for Axis devices is defined.

Service configuration

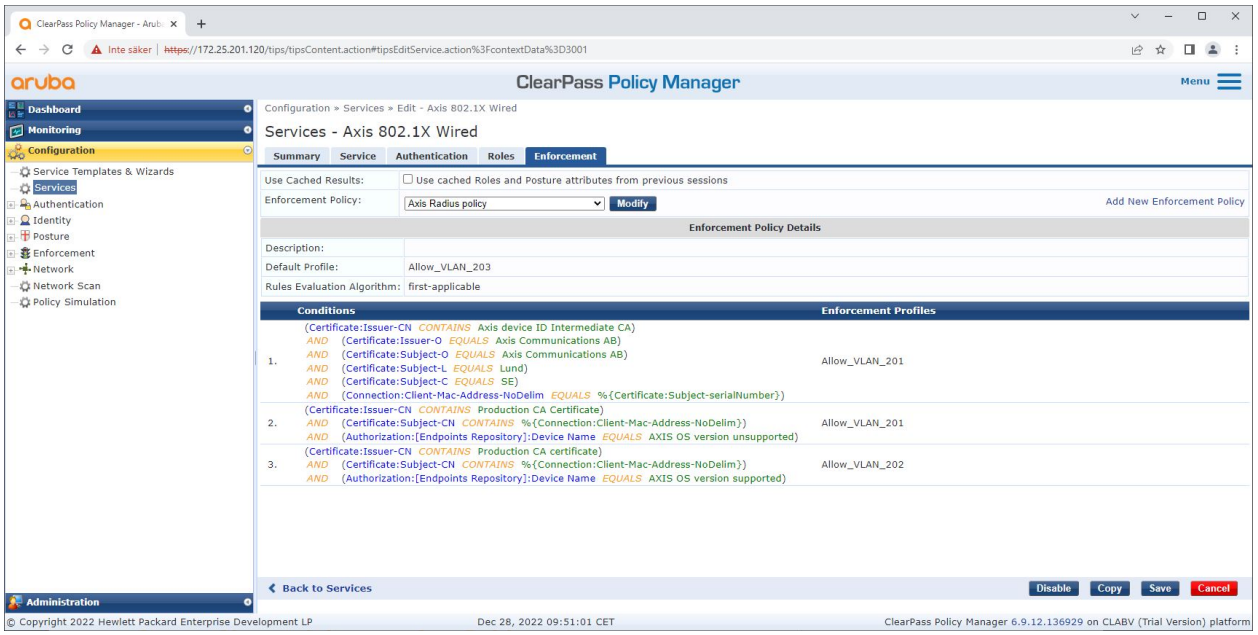
On the **Services** page, the configuration steps are combined into one single service that handles the authentication and authorization of Axis devices in HPE Aruba Networking powered networks.



A dedicated Axis services is created that defines IEEE 802.1X as connection method.



In the next step, the earlier created EAP-TLS authentication method is configured to the service.



In the last step, the earlier created enforcement policy is configured to the service.

HPE Aruba Networking access switch

Axis devices are either directly connected to PoE-capable access switches or via compatible Axis PoE midspans. To securely onboard Axis devices into HPE Aruba Networking powered networks, the access switch needs to be configured for IEEE 802.1X communication. The Axis device relays IEEE 802.1x EAP-TLS communication to ClearPass Policy Manager that acts as a RADIUS server.

Note

A periodic re-authentication of 300 seconds for the Axis device is configured as well to increase overall port-access security.

Refer to the below example global and port configuration for HPE Aruba Networking access switches.

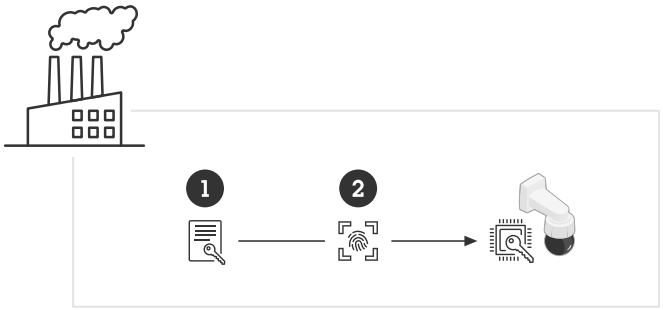
```
radius-server host MyRADIUSIPAddress key "MyRADIUSKey"

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
```

Configuration Axis

Axis network device

Axis devices with support for *Axis Edge Vault* are manufactured with a secure device identity, called Axis device ID. The Axis device ID is based on the international IEEE 802.1AR standard, which defines a method for automated, secure device identification and network onboarding through IEEE 802.1X.

Secure onboarding - IEEE 802.1AR/802.1X



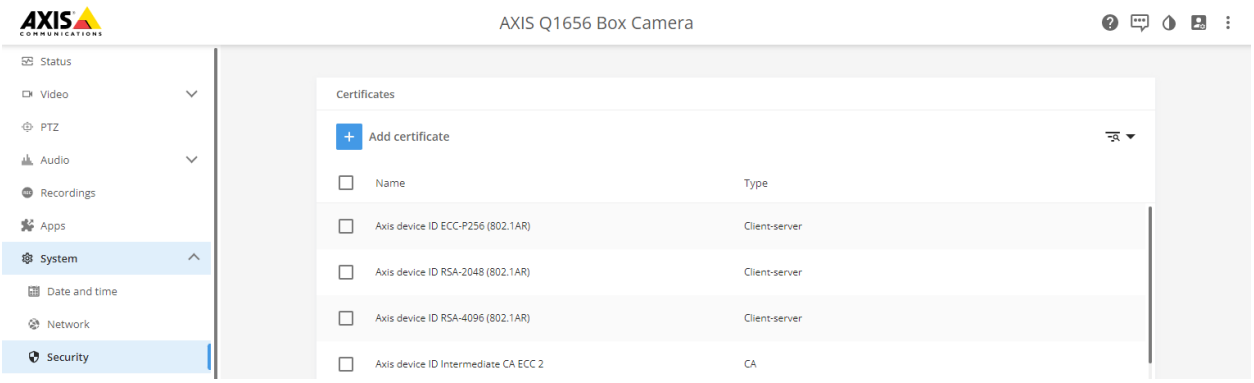
Axis devices are manufactured with the IEEE 802.1AR-compliant Axis device ID certificate for trusted device identity services

1 *Axis device ID key infrastructure (PKI)*
2 *Axis device ID*

The hardware-protected secure keystore provided by a secure element of the Axis device is factory provisioned with a device-unique certificate and corresponding keys (Axis device ID) that globally can prove the authenticity of the Axis device. The *Axis Product Selector* can be used to learn which Axis devices have support for Axis Edge Vault and Axis device ID.

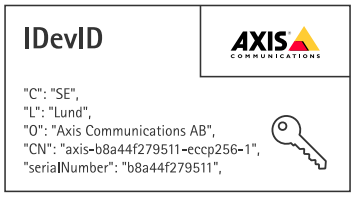
Note

The serial number of an Axis device is its MAC-address.



The certificate store of the Axis device in factory defaulted state with Axis Device ID.

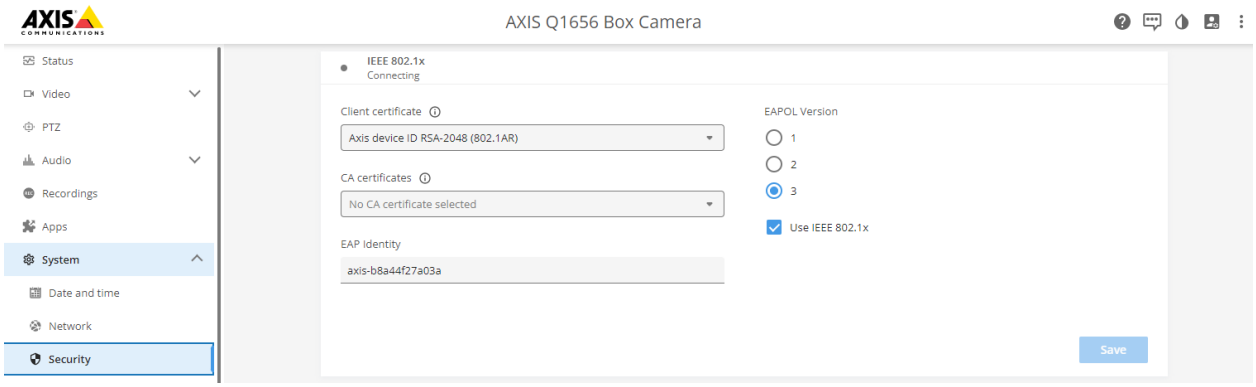
The IEEE 802.1AR-compliant Axis device ID certificate includes information about the serial number and other Axis-vendor specific information. The information is used by ClearPass Policy Manager for analysis and decision making to grant access to the network. Please refer to the below information that can be obtained from an Axis device ID certificate



Country	SE
Location	Lund
Issuer Organization	Axis Communications AB

Issuer Common Name	Axis device ID intermediate
Organization	Axis Communications AB
Common Name	axis-b8a44f279511-eccp256-1
Serial Number	b8a44f279511

The common name is constructed by a combination of Axis company name, the serial number of the device followed by the crypto algorithm (ECC P256, RSA 2048, RSA 4096) used. Since AXIS OS 10.1 (2020-09), IEEE 802.1X is enabled by default with the Axis device ID pre-configured. This enables the Axis device to authenticate itself onto IEEE 802.1X-enabled networks.



The Axis device in factory defaulted state with IEEE 802.1X enabled and Axis Device ID certificate pre-selected.

AXIS Device Manager

AXIS Device Manager and *AXIS Device Manager Extend* can be used on the network to configure and manage multiple Axis devices in a cost-effective way. AXIS Device Manager is a Microsoft Windows®-based application that can be installed locally on a machine in the network, while AXIS Device Manager Extend relies on cloud infrastructure to do multi-site device management. Both offer easy management and configuration capabilities for Axis devices such as:

- Installation of AXIS OS updates.
- Apply cybersecurity configuration such as HTTPS and IEEE 802.1X certificates.
- Configuration of device-specific settings such as images settings and others.

Secure network operation - IEEE 802.1AE MACsec

To watch this video, go to the web version of this document.

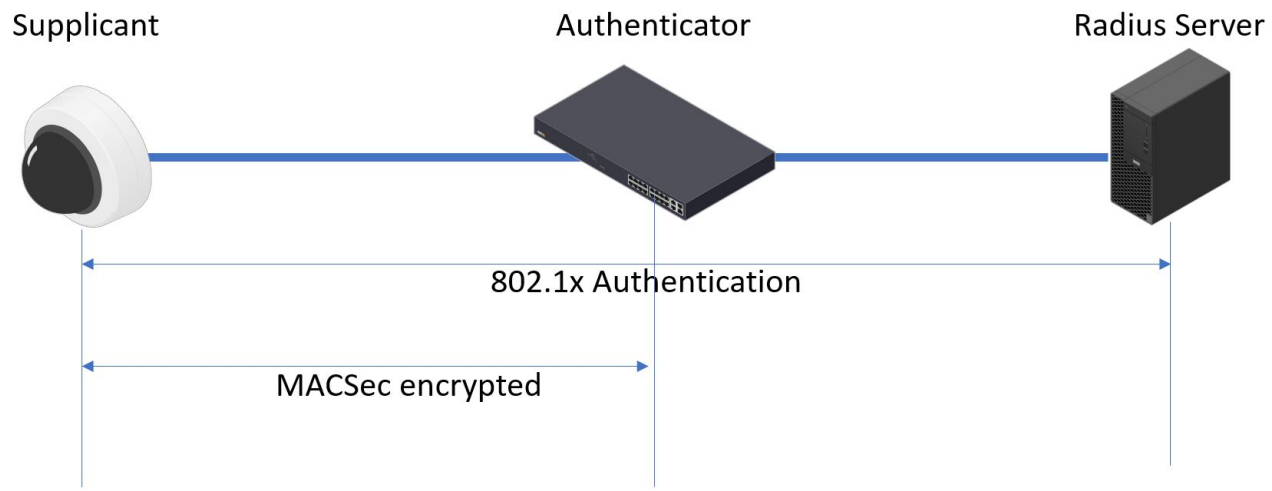
help.axis.com/?&tpiaId=&tsection=secure-network-operation-ieee-802-1ae-macsec

Zero-trust network encryption with IEEE 802.1AE MACsec layer-2 security

IEEE 802.1AE MACsec (Media Access Control Security) is a well-defined network protocol that cryptographically secures point-to-point Ethernet links on network layer 2. It ensures the confidentiality and integrity of data transmissions between two hosts.

The IEEE 802.1AE MACsec standard describes two modes of operation:

- Manually configurable Pre-Shared Key/Static CAK mode
- Automatic Master Session/Dynamic CAK mode using IEEE 802.1X EAP-TLS



In AXIS OS 10.1 (2020-09) and later, IEEE 802.1X is enabled by default for devices that are compatible with Axis device ID. In AXIS OS 11.8 and later, we support MACsec with automatic dynamic mode using IEEE 802.1X EAP-TLS enabled by default. When you connect an Axis device with factory default values, IEEE 802.1X network authentication is performed and when successful, MACsec Dynamic CAK mode is tried as well.

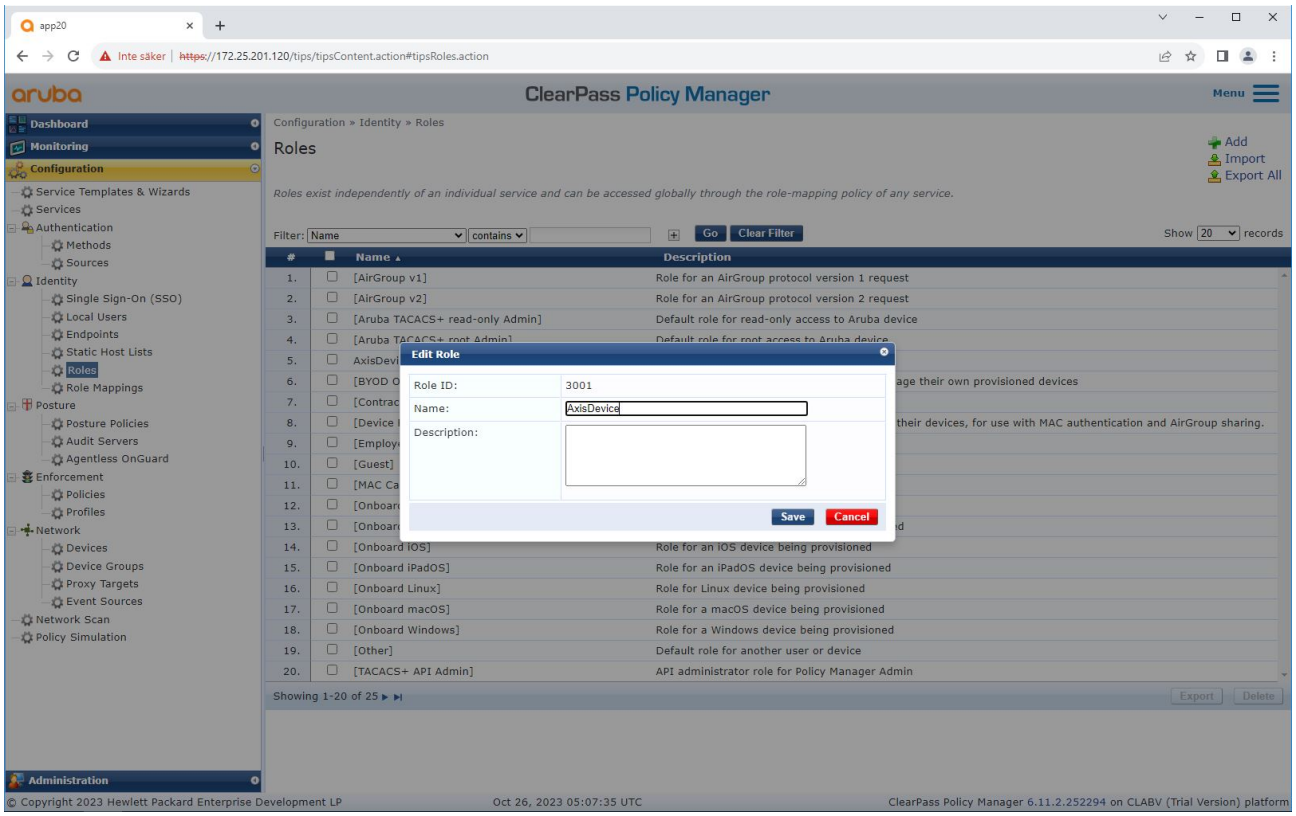
The securely stored Axis device ID (1), an IEEE 802.1AR-compliant secure device identity, is used to authenticate into the network (4, 5) through IEEE 802.1X EAP-TLS port-based network access control (2). Through the EAP-TLS session, MACsec keys are exchanged automatically to set up a secure link (3), protecting all network traffic from the Axis device to the HPE Aruba Networking access switch.

IEEE 802.1AE MACsec requires both HPE Aruba Networking access switch and ClearPass Policy Manager configuration preparations. No configuration is required on the Axis device to allow IEEE 802.1AE MACsec encrypted communication via EAP-TLS.

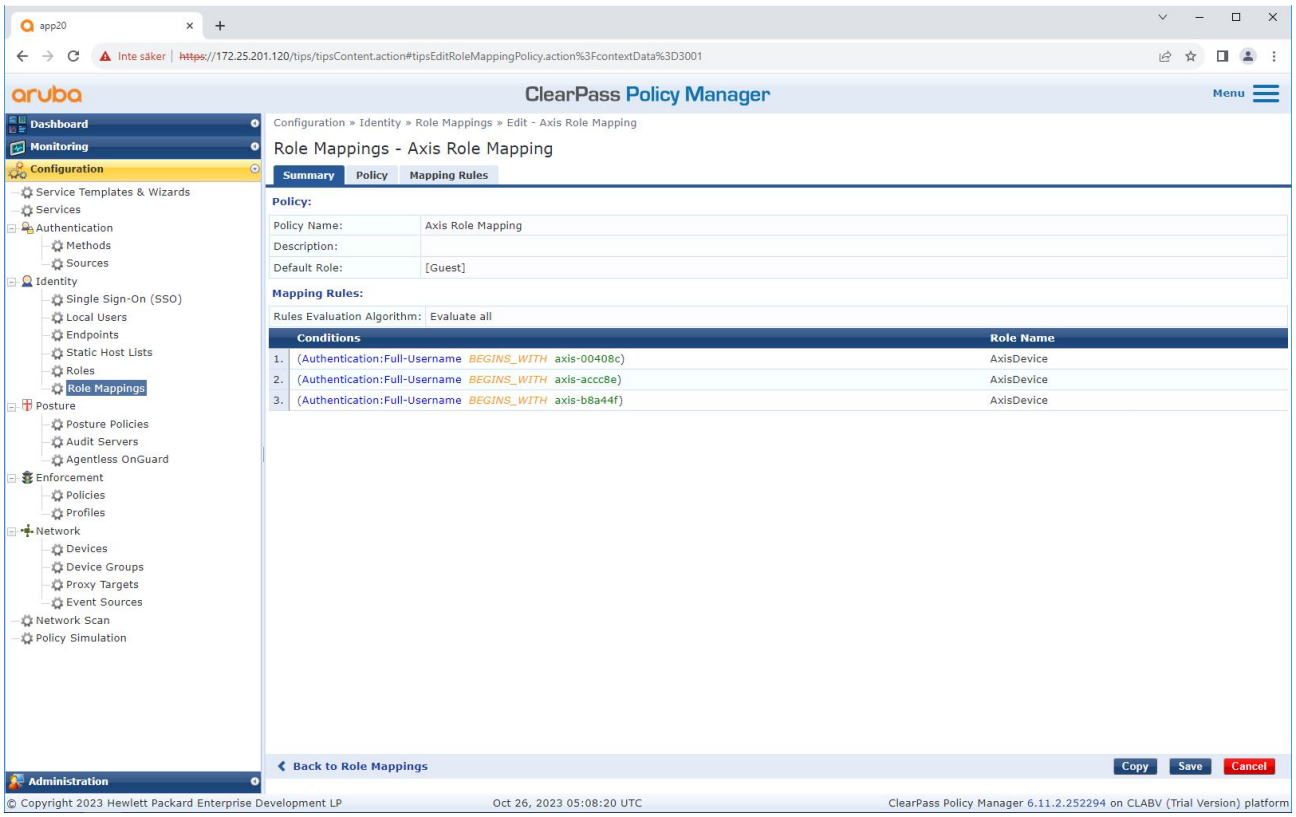
If the HPE Aruba Networking access switch doesn't support MACsec using EAP-TLS, then the Pre-Shared Key mode can be used and manually configured.

HPE Aruba Networking ClearPass Policy Manager

Role and role mapping policy



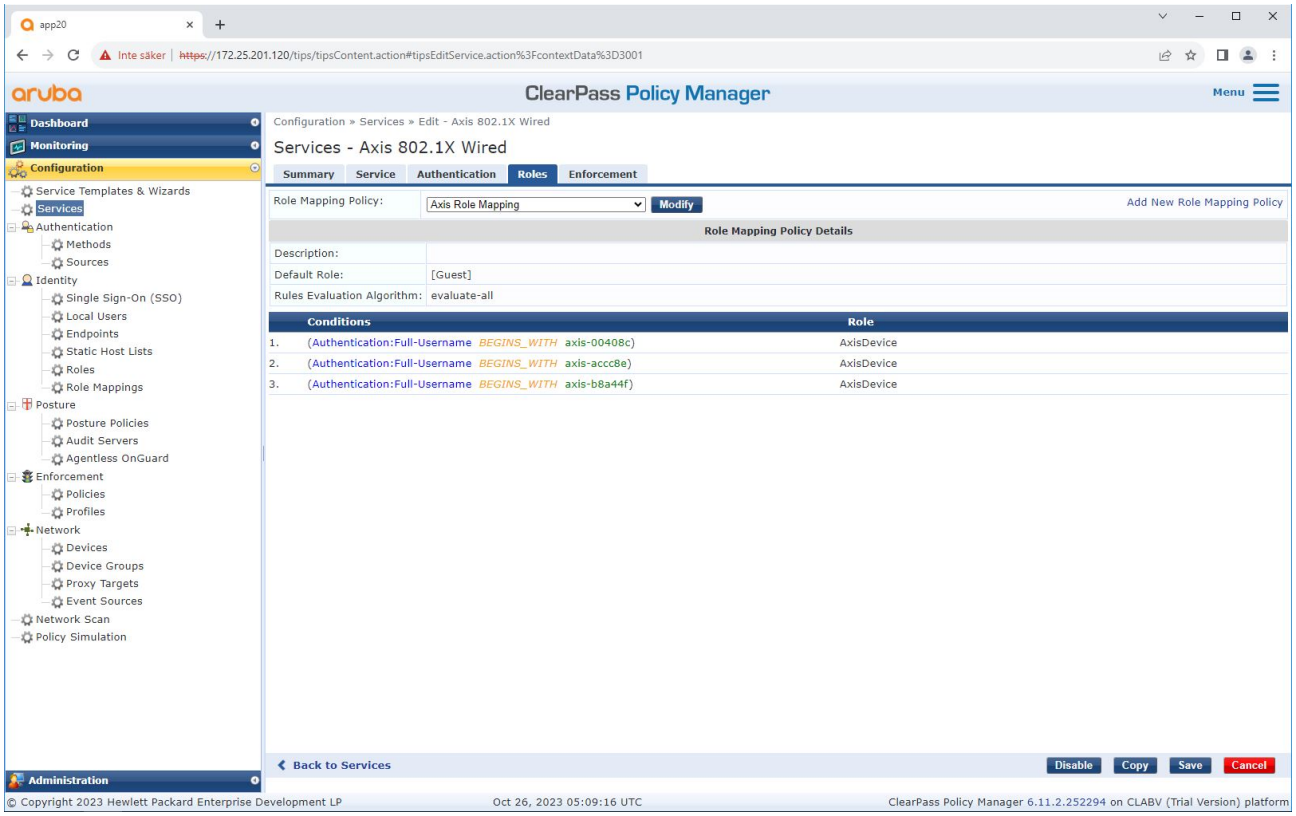
Add a role name for Axis devices. The name is the port access role name in the access switch configuration.



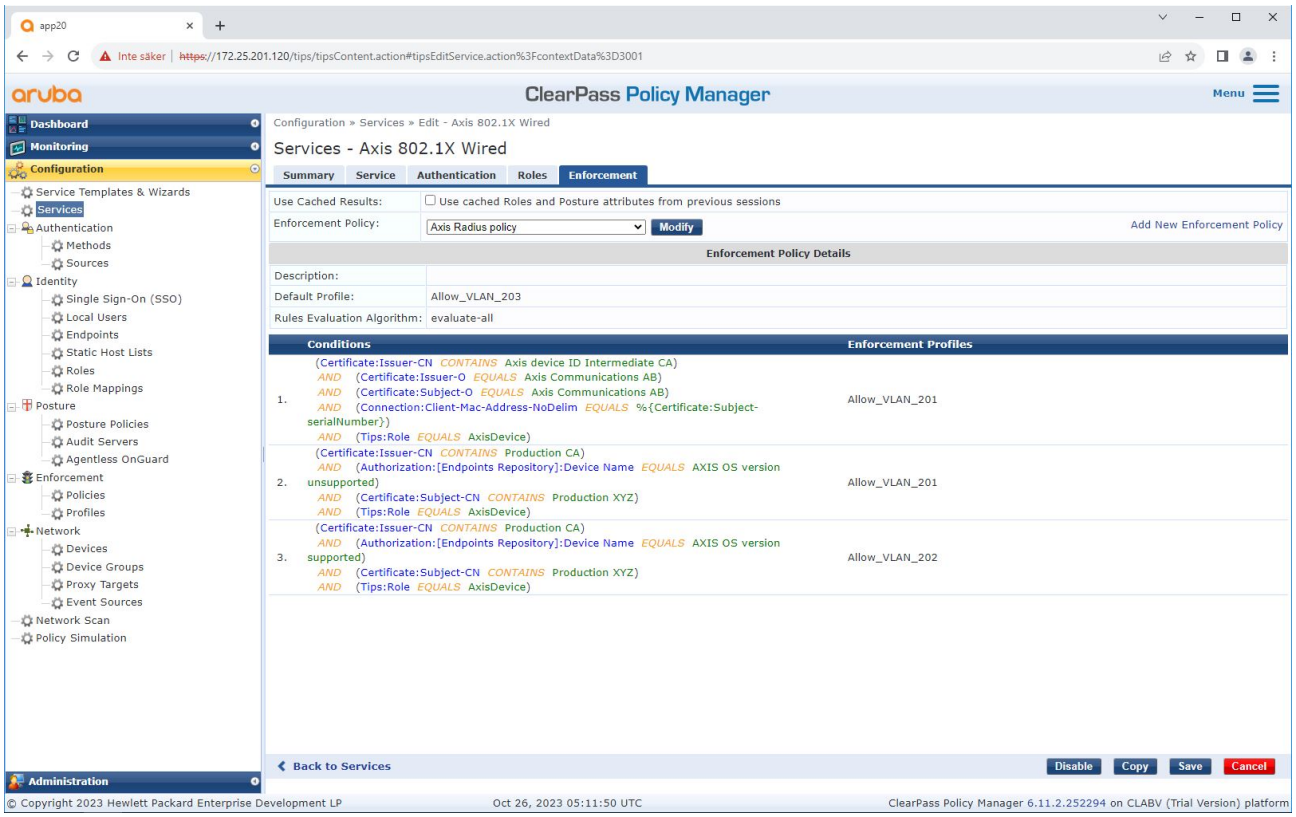
Add an Axis role mapping policy for the earlier created Axis device role. The conditions defined are required for a device to be mapped to the Axis device role. If the conditions aren't met, the device becomes a part of the [Guest] role.

By default, Axis devices use the EAP identity format "axis-serialnumber". The serial number of an Axis device is its MAC-address. For example "axis-b8a44f45b4e6".

Service configuration

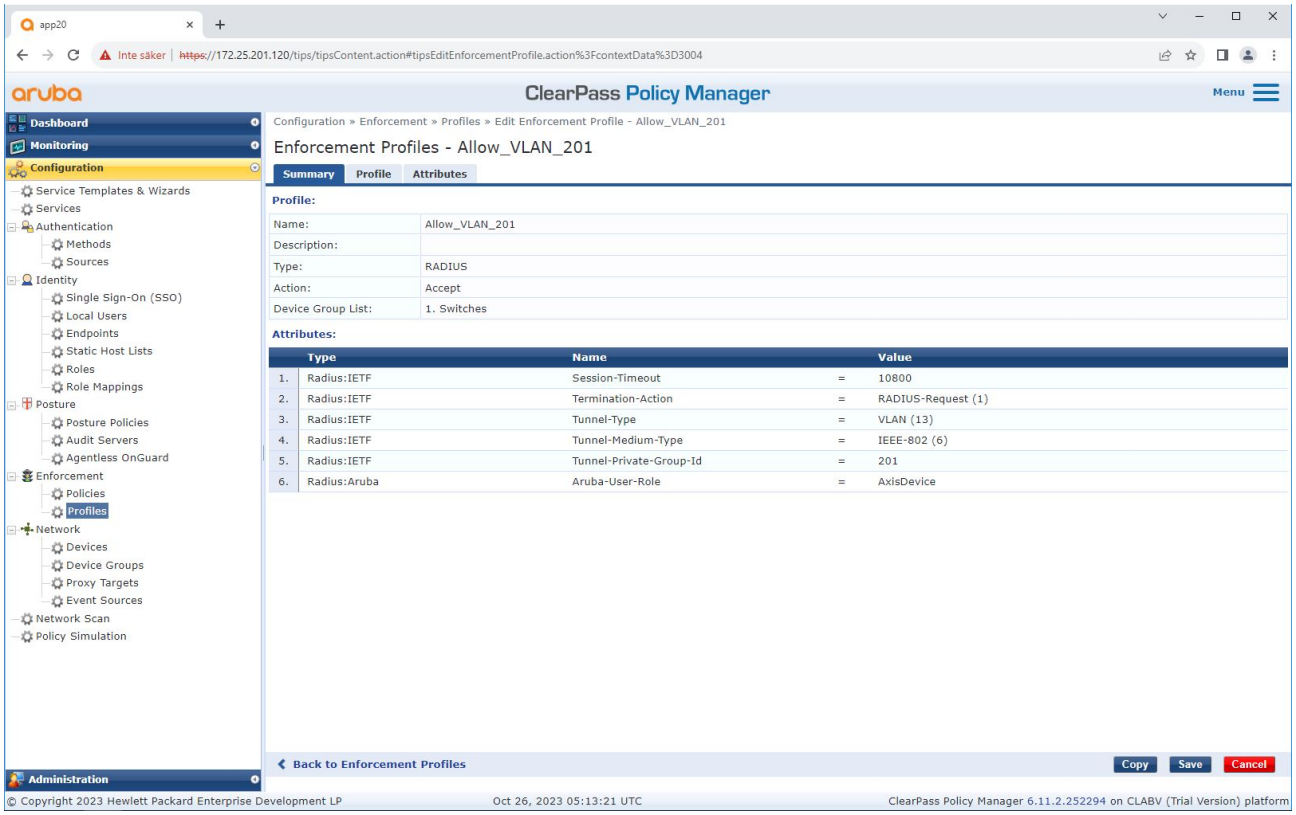


Add the earlier created Axis role mapping policy to the service that defines IEEE 802.1X as connection method for the onboarding of Axis devices.



Add the Axis role name as a condition to the existing policy definitions.

Enforcement profile



Add the Axis role name as attribute to the enforcement profiles that are assigned in the IEEE 802.1X onboarding service.

HPE Aruba Networking access switch

In addition to the secure onboarding configuration described in *HPE Aruba Networking access switch on page 16*, refer to the below example port configuration for the HPE Aruba Networking access switch to configure IEEE 802.1AE MACsec.

```
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
```

Legacy onboarding - MAC authentication

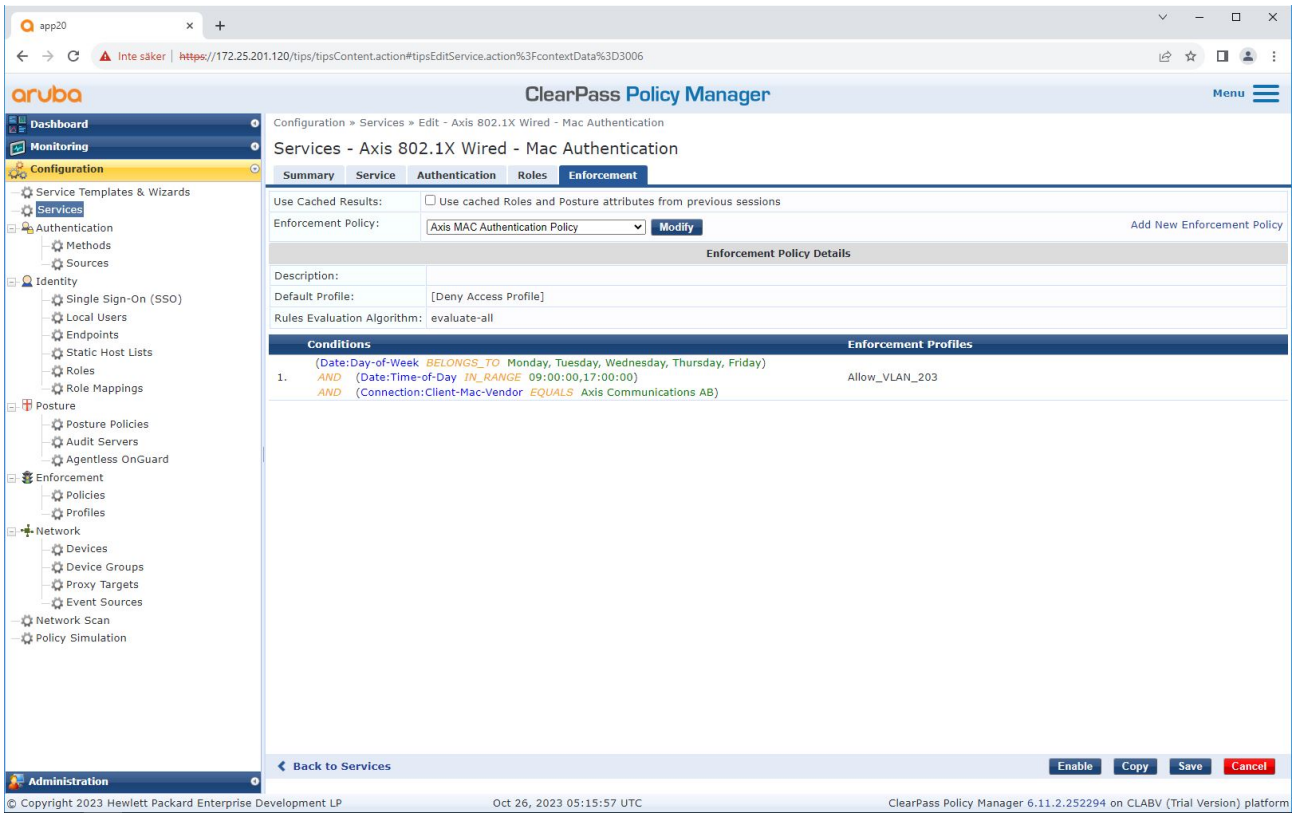
You can use MAC Authentication Bypass (MAB) to onboard Axis devices that don't support IEEE 802.1AR onboarding with the Axis device ID certificate and IEEE 802.1X enabled in factory default state. If 802.1X onboarding fails, ClearPass Policy Manager validates the Axis device's MAC address and grant access to the network.

MAB requires both access switch and ClearPass Policy Manager configuration preparations. On the Axis device, no configuration is required to allow MAB for onboarding.

HPE Aruba Networking ClearPass Policy Manager

Enforcement policy

The enforcement policy configuration in ClearPass Policy Manager defines if Axis devices are granted access to HPE Aruba Networking powered networks based on the following two example policy conditions.



Denied network access

When the Axis device doesn't meet the configured enforcement policy, it's denied access to the network.

Guest-network (VLAN 203)

The Axis device is granted access to a limited, isolated network if the following conditions are met:

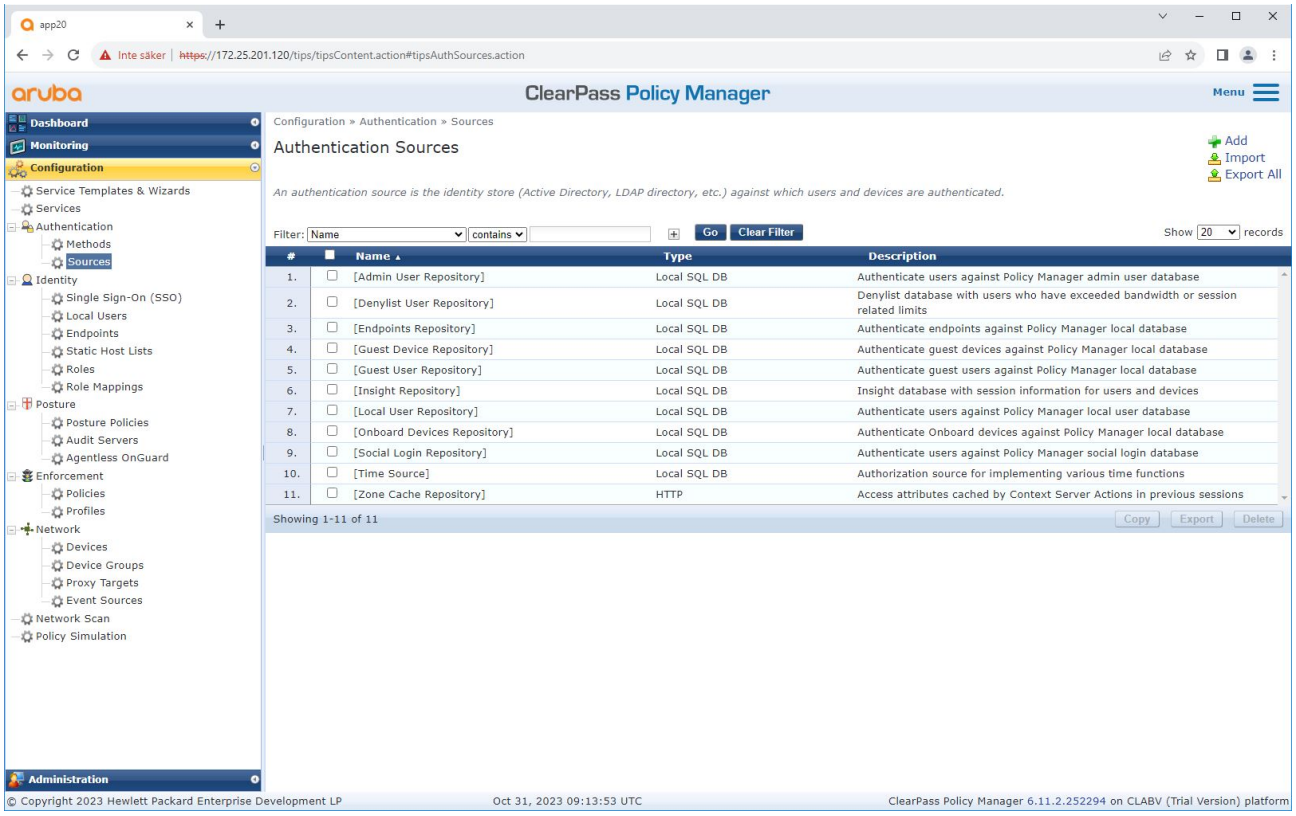
- It's a weekday between Monday and Friday
- It's between 09:00 and 17:00

- The MAC address vendor matches with Axis Communications.

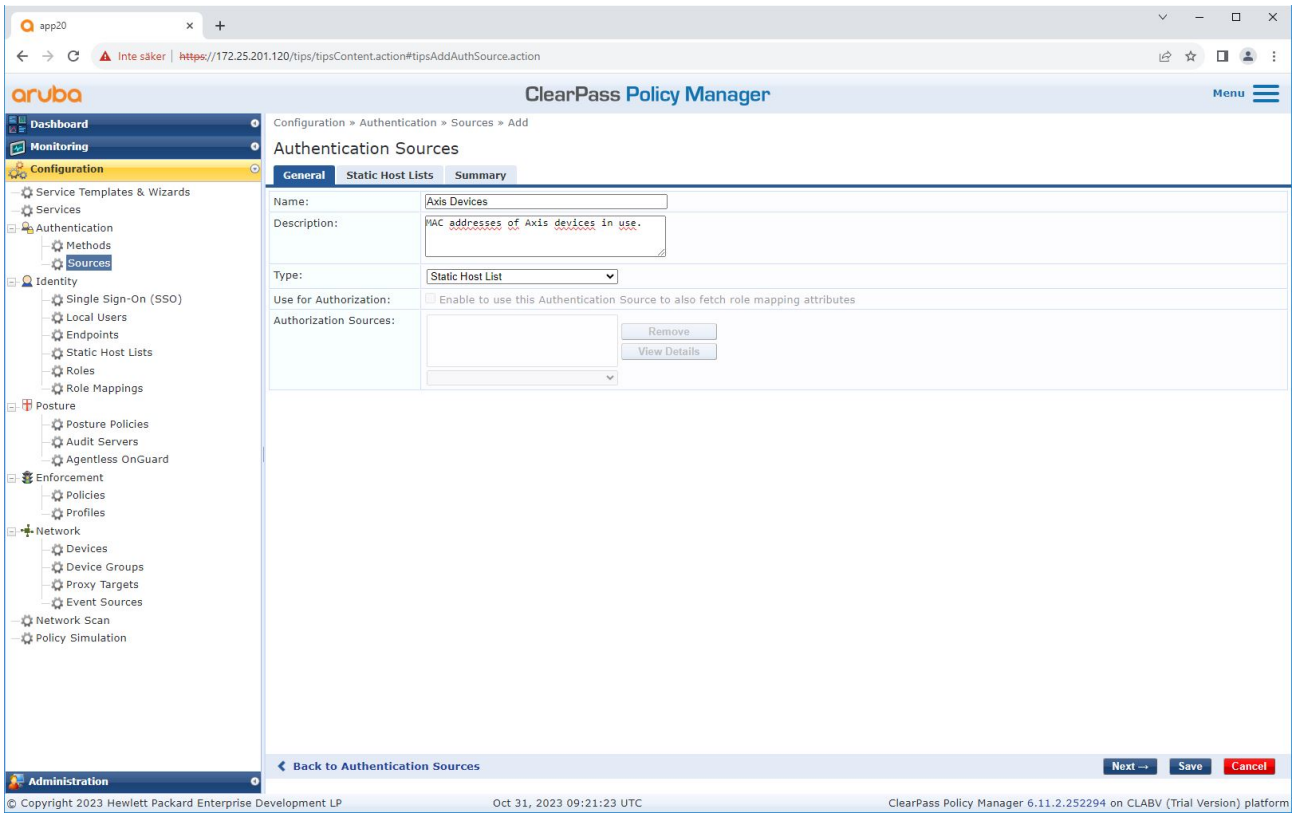
Since MAC addresses can be spoofed, access to the regular provisioning network isn't granted. We recommend that you only use MAB for initial onboarding, and to manually inspect the device further.

Source configuration

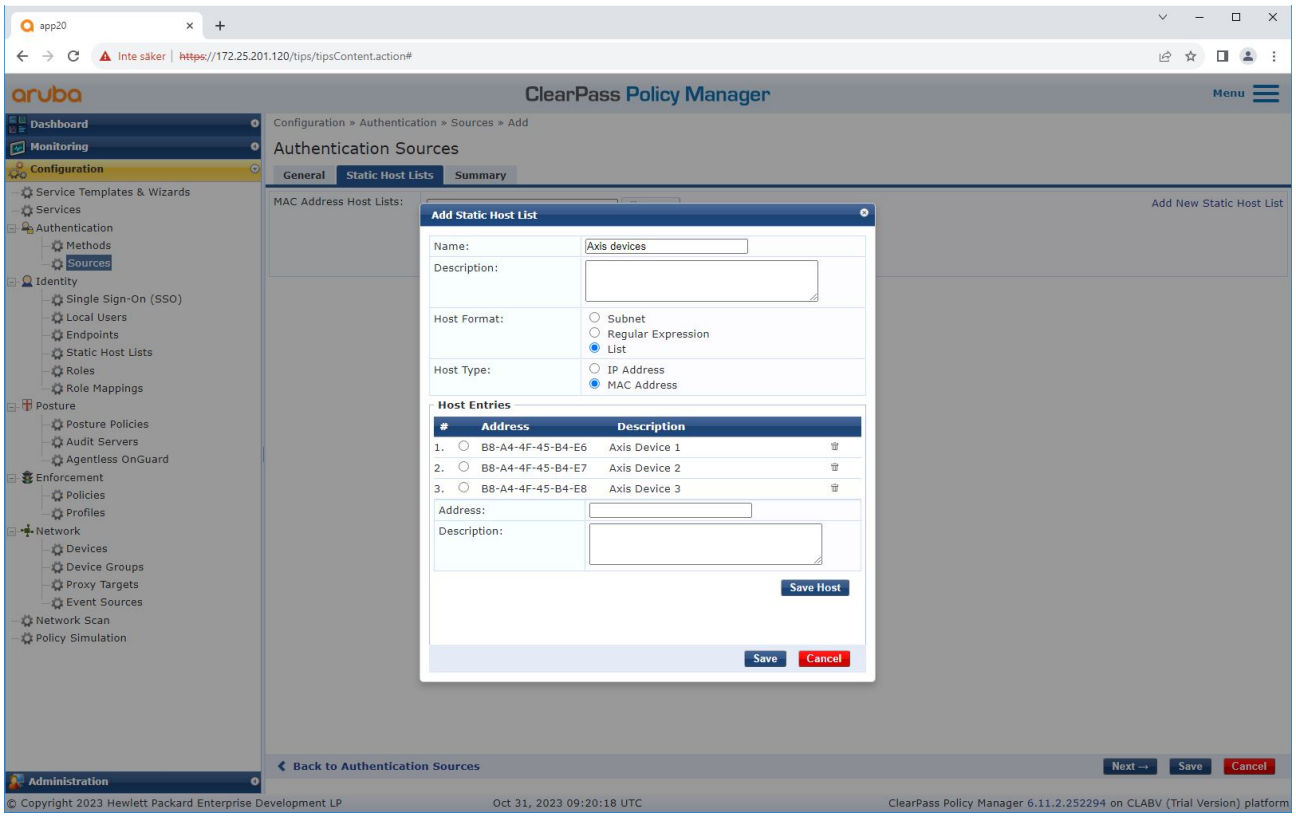
On the **Sources** page, a new authentication source is created to allow only manually imported MAC addresses.



Legacy onboarding - MAC authentication

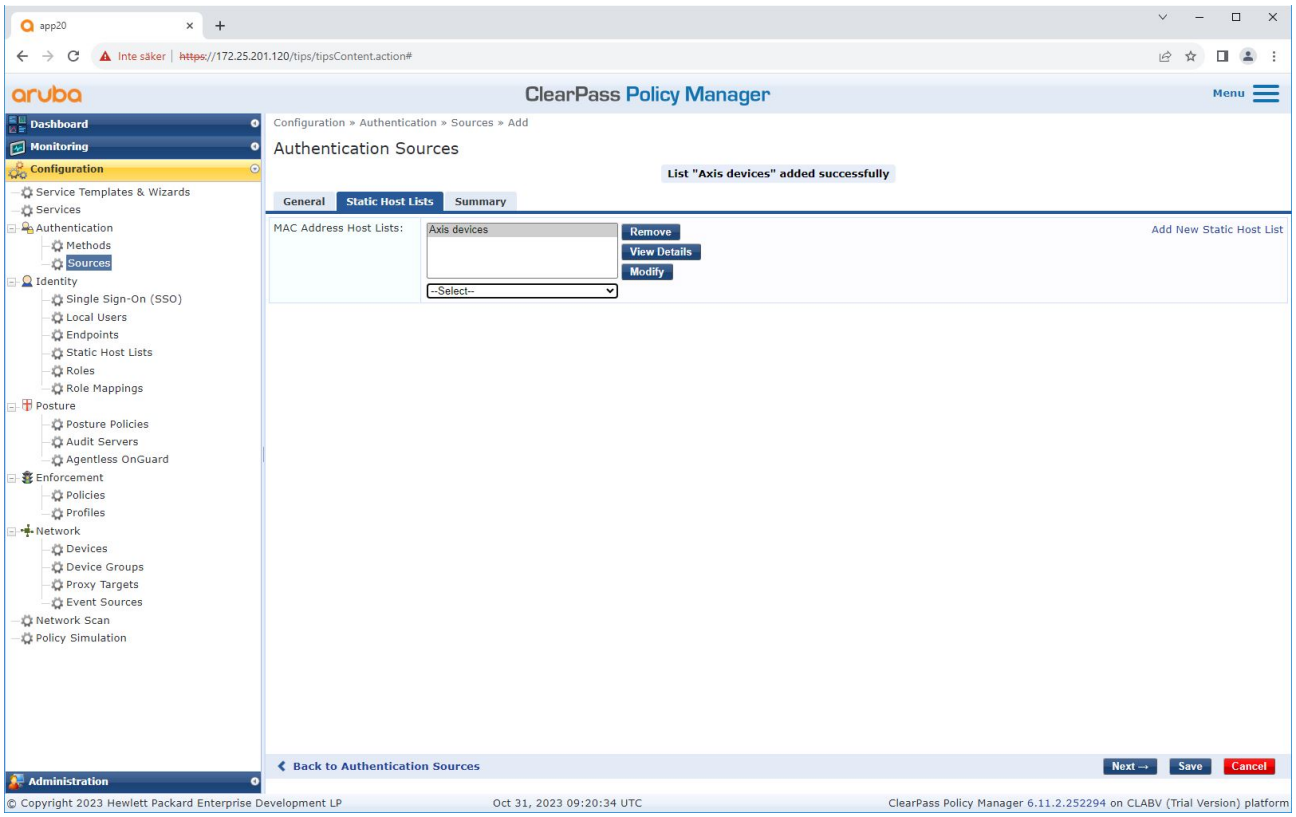


Legacy onboarding - MAC authentication



A static host list, which contains Axis MAC addresses, is created.

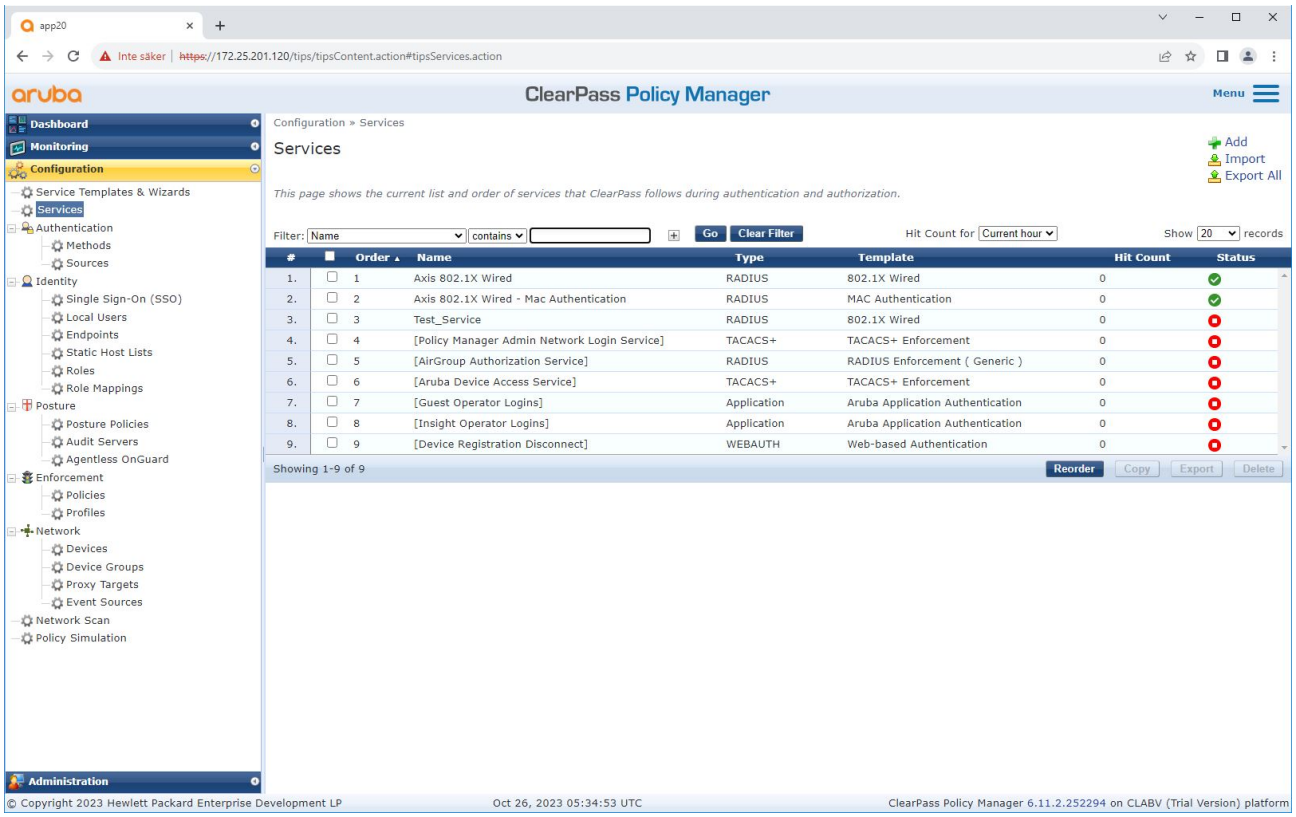
Legacy onboarding - MAC authentication



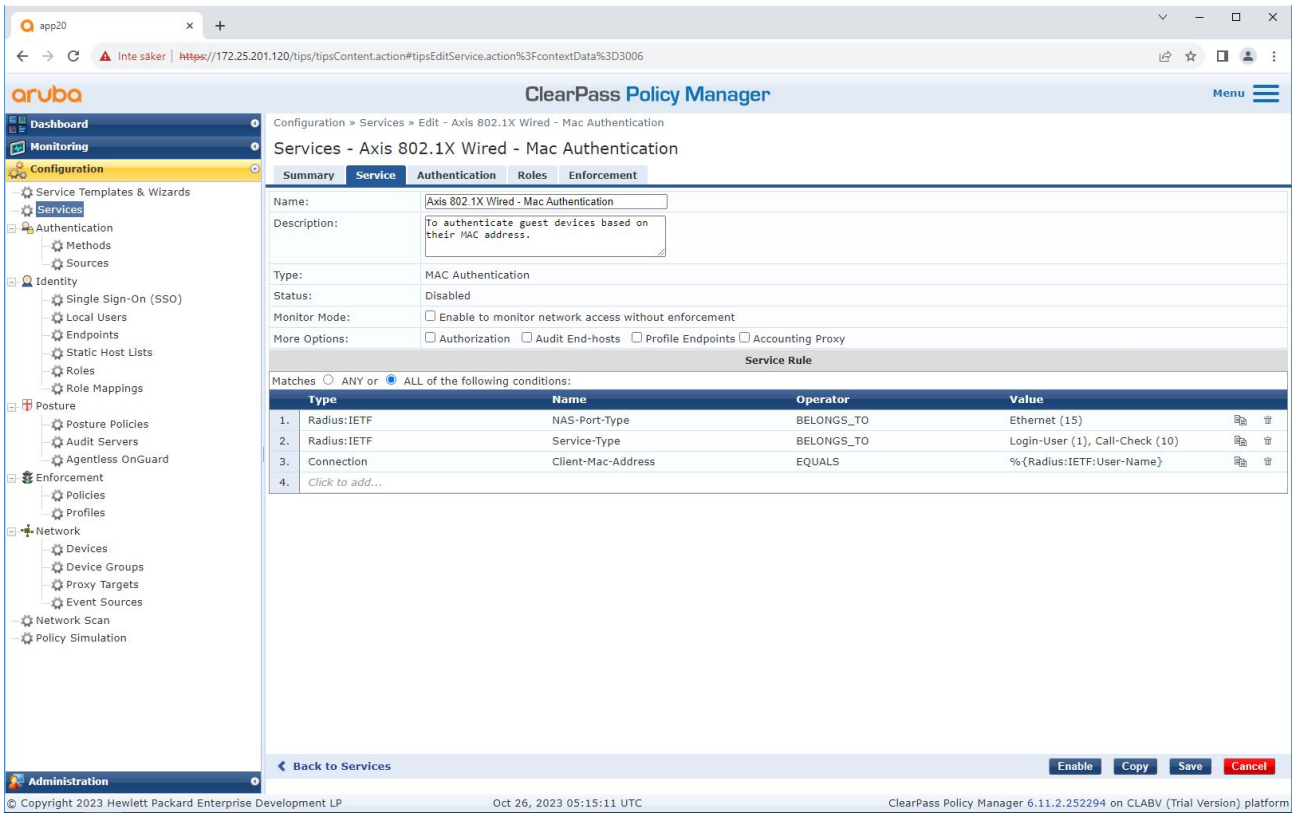
Service configuration

On the **Services** page, the configuration steps are combined into one single service that handles the authentication and authorization of Axis devices in HPE Aruba Networking powered networks.

Legacy onboarding - MAC authentication

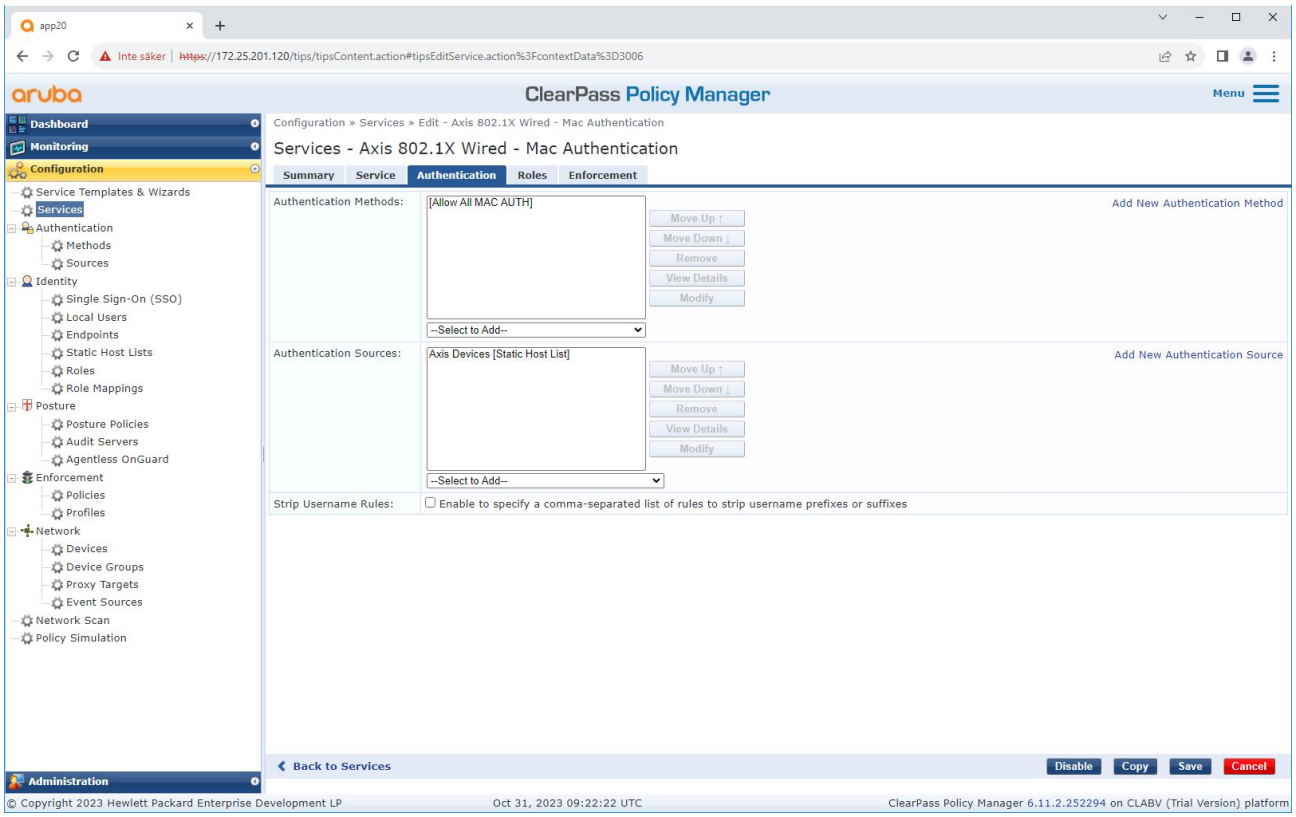


Legacy onboarding - MAC authentication



A dedicated Axis service that defines MAB as connection method is created.

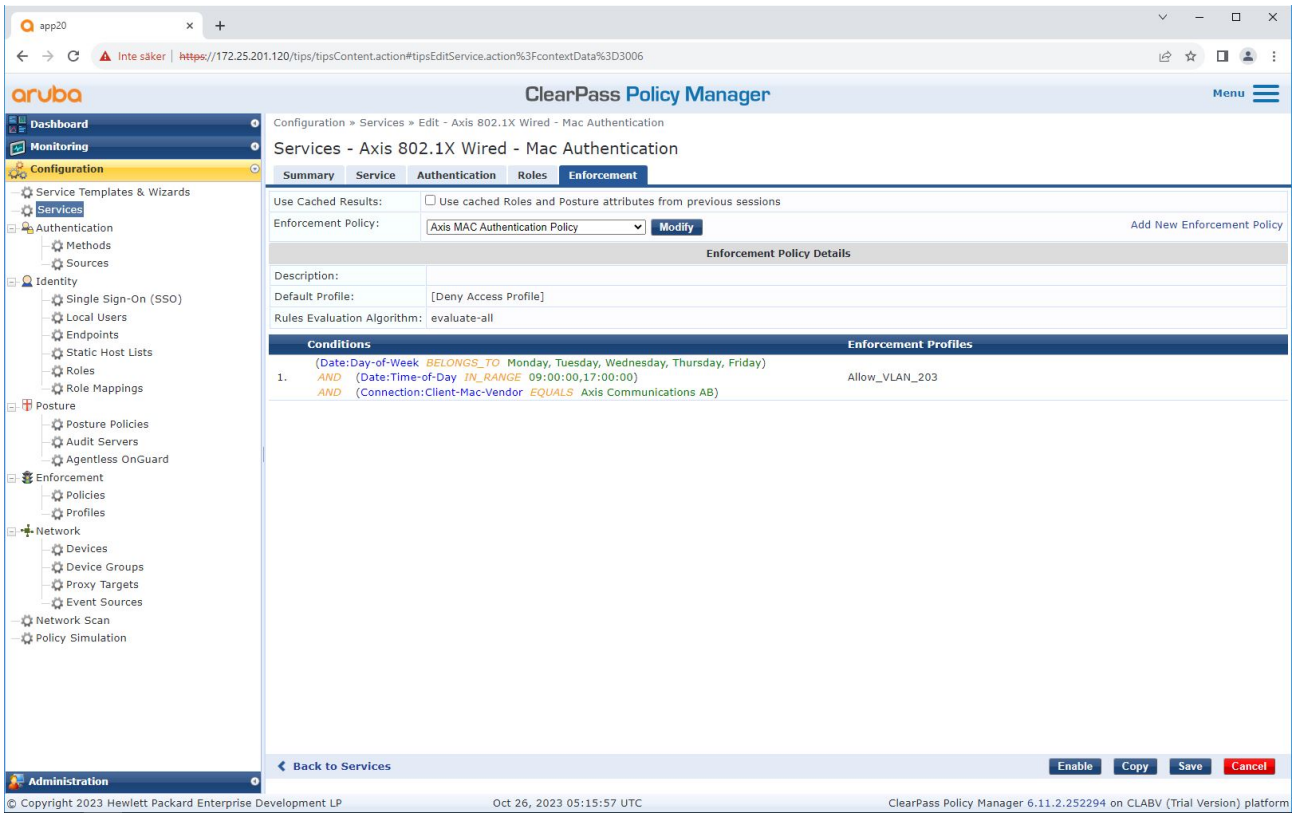
Legacy onboarding - MAC authentication



The pre-configured MAC authentication method is configured to the service. Also, the previously created authentication source which contains a list of Axis MAC addresses is selected.

Axis Communications uses the following MAC address OUIs:

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



In the last step, the previously created enforcement policy is configured to the service.

HPE Aruba Networking access switch

In addition to the secure onboarding configuration described in *HPE Aruba Networking access switch on page 16*, refer to the below example port configuration for the HPE Aruba Networking access switch to allow for MAB.

```
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
```

Integration Guide
HPE Aruba Networking

Ver. M6.2
Date: May 2024
Part no. T10197992