HPE Aruba Networking

User manual

Table of Contents

Introduction

This integration guide outlines the best-practice configuration when onboarding and operating Axis devices in HPE Aruba Networking 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 you time and money. It removes unnecessary system complexity when using Axis device management applications with HPE Aruba Networking infrastructure and applications. When combining Axis devices and software with a HPE Aruba Networking infrastructure you can benefit in these ways:

- Removing device staging networks minimizes system complexity.
- Adding automating onboarding processes and device management reduces costs.
- Axis devices provide zero-touch network security controls.
- Increased overall network security through HPE and Axis expertise.

For a smooth software-defined transition between logical networks throughout the on-boarding process, the network infrastructure must be prepared to securely verify the integrity of the Axis devices before starting the configuration. You need the following before doing the configuration:

- Experience of 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.
- Previous basic knowledge about Axis products is desirable, but this is also provided throughout the guide.

Secure onboarding - IEEE 802.1AR/802.1X

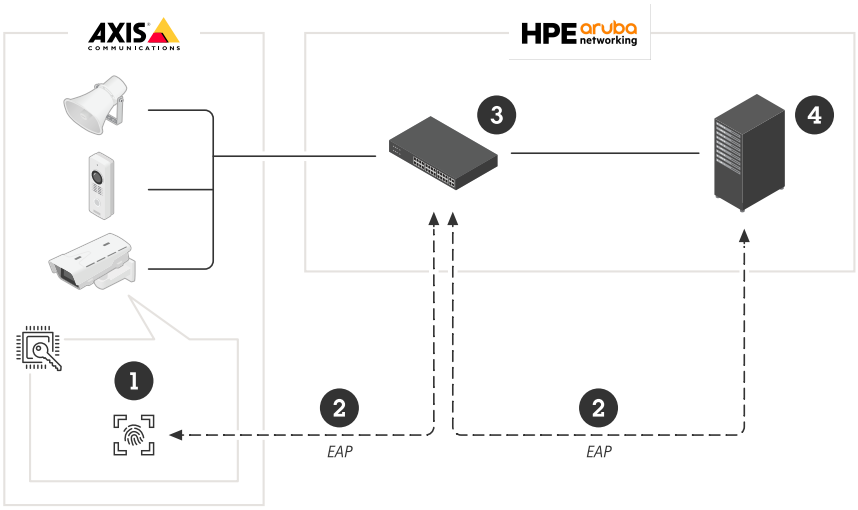
Secure device onboarding onto zero-trust networks with IEEE 802.1X/802.1AR

Initial authentication

When the Axis Edge Vault-supported Axis device is connected to the network, it uses 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. This information, such as the MAC-address and the device's AXIS OS version, is used to make a policy-based decision.

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

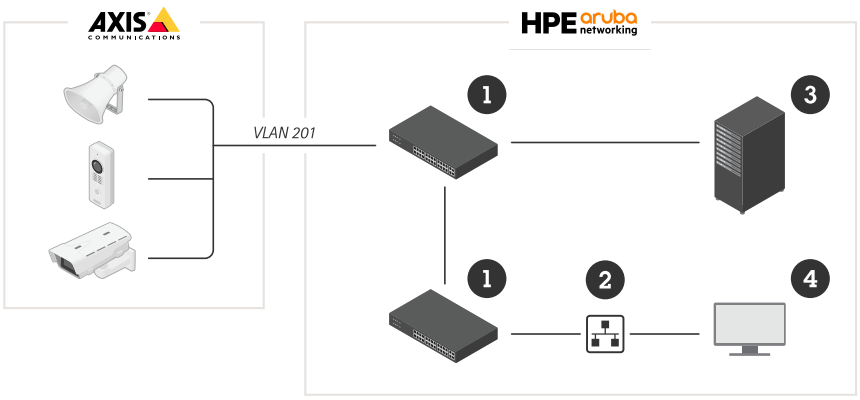


The Axis device authenticates against the HPE Aruba Networking network using the IEEE 802.1AR-compliant Axis device ID certificate.

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 onto the provisioning network (VLAN201). This network contains AXIS Device Manager, which performs device configuration, security hardening, and AXIS OS updates. To complete the device provisioning, new customer-specific production-grade certificates are uploaded to the device for IEEE 802.1X and HTTPS.

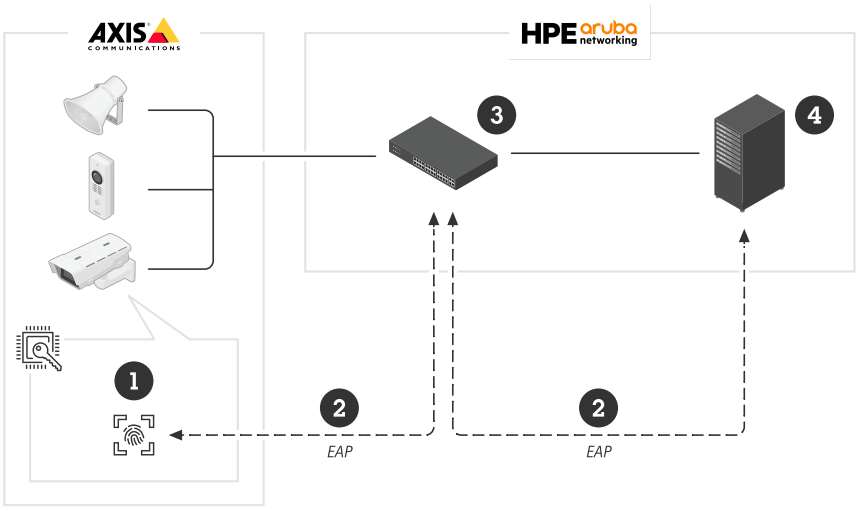


After successful authentication, the Axis device moves into a provisioning network for configuration.

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

Production network

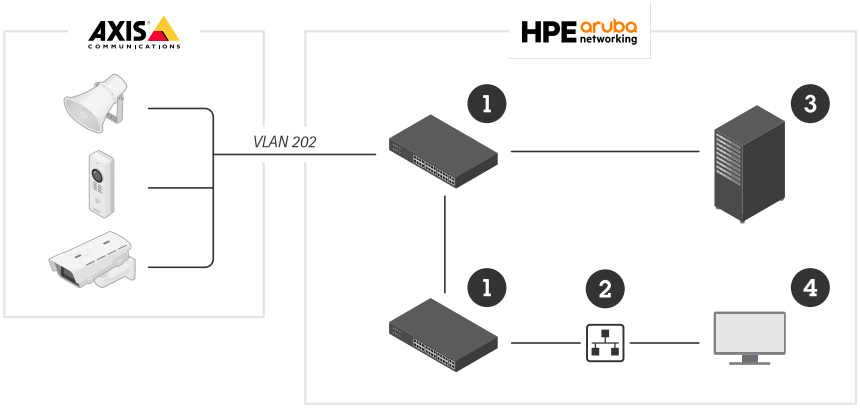
The provisioning of the Axis device with new IEEE 802.1X certificates triggers a new authentication attempt. ClearPass Policy Manager verifies the new certificates and decides whether or not to move the Axis device into the production network.



After being configured, the Axis device leaves the provisioning network and attempts to re-authenticate on the network.

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

After re-authentication, the Axis device moves into the production network (VLAN 202), where the Video Management System (VMS) connects to the device and starts operation.



The Axis device is granted access to the production network.

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

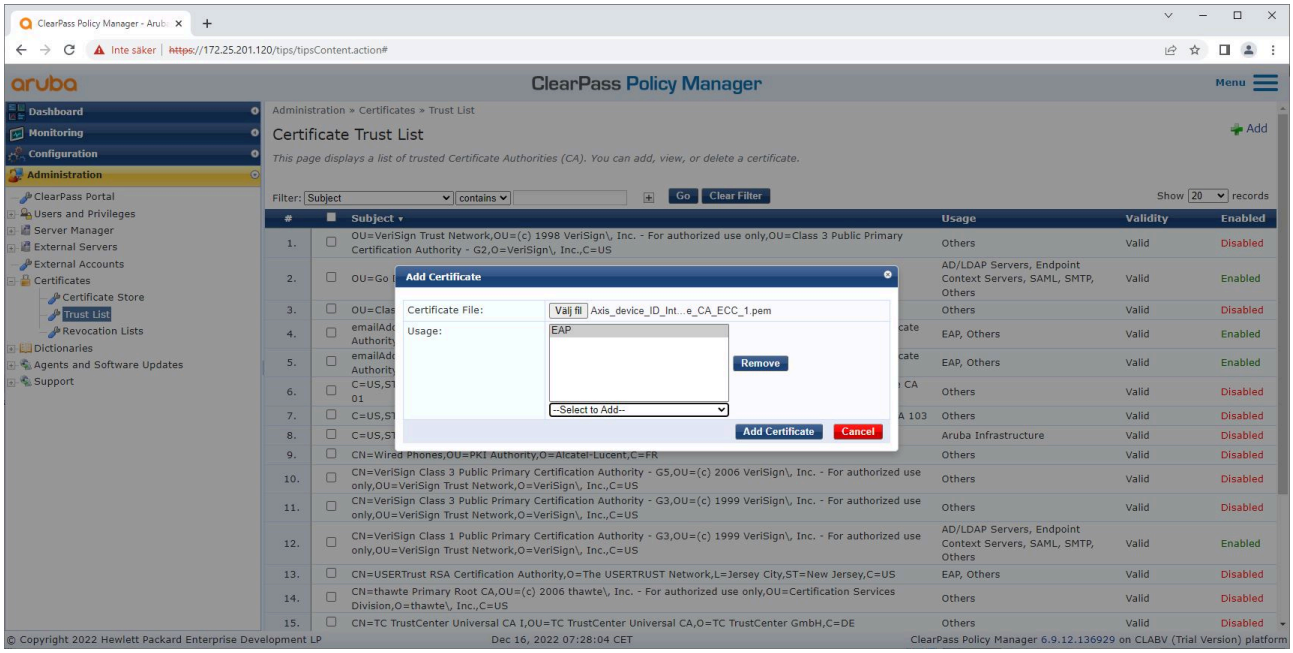
Configuration HPE Aruba Networking

HPE Aruba Networking ClearPass Policy Manager

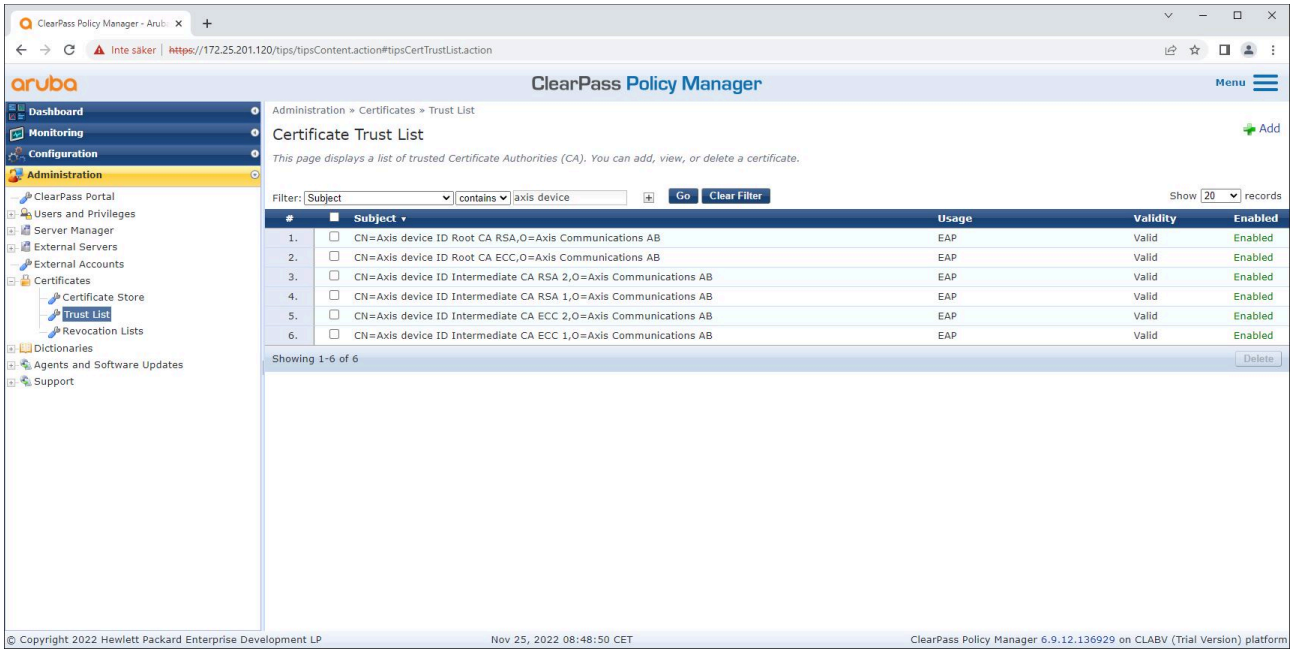
ClearPass Policy Manager provides role- and device-based secure network access control for IoT, BYOD, corporate devices, employees, contractors and guests, across multivendor wired, wireless, and VPN infrastructure.

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.



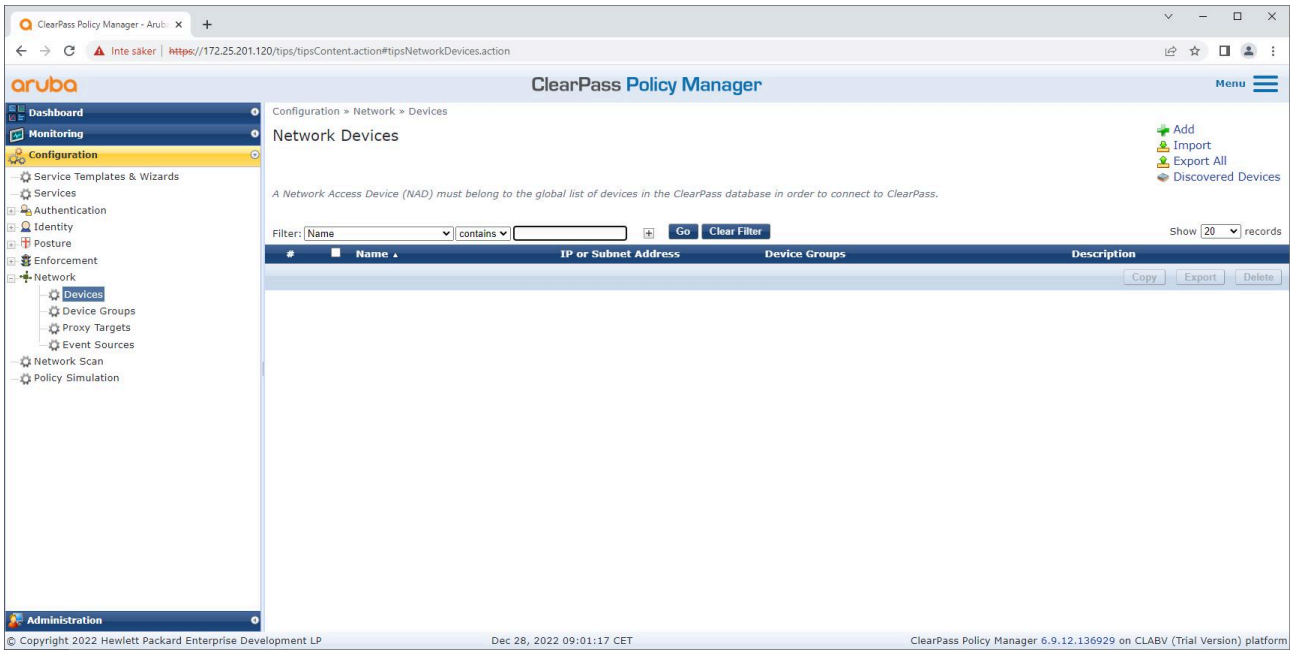
Upload the Axis-specific IEEE 802.1AR certificates to the trusted certificate store of ClearPass Policy Manager.



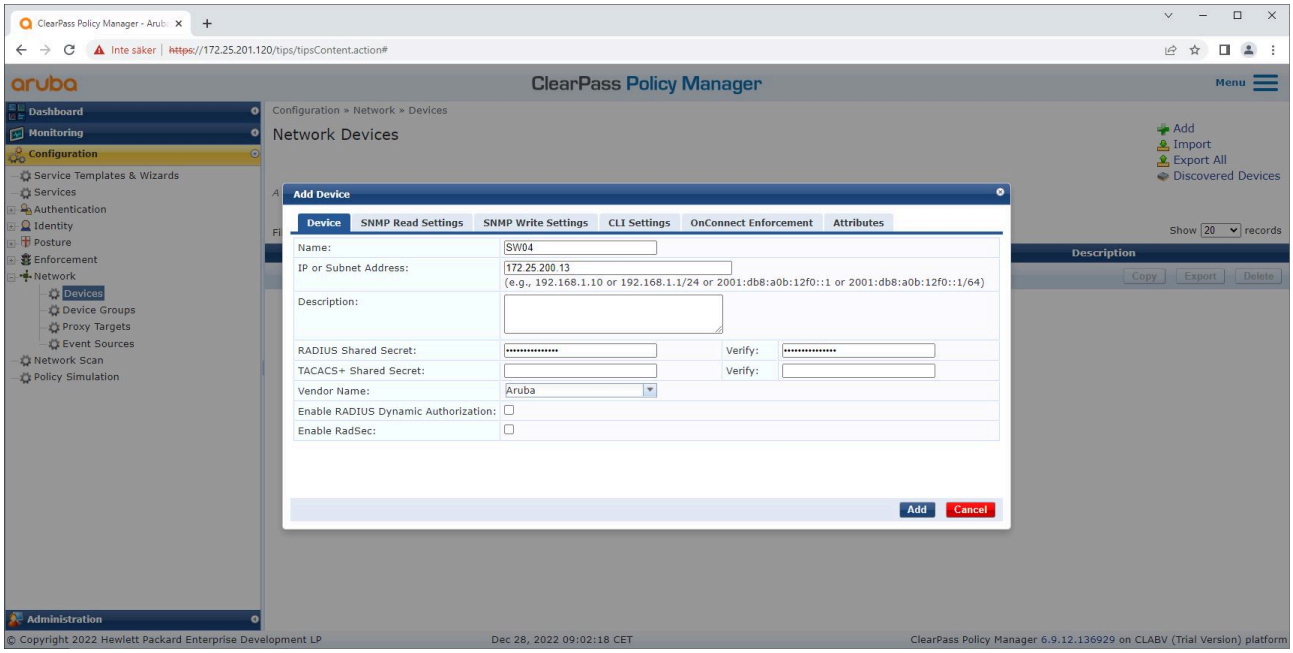
The trusted certificate store in ClearPass Policy Manager with Axis-specific IEEE 802.1AR certificate chain included.

Network device/group configuration

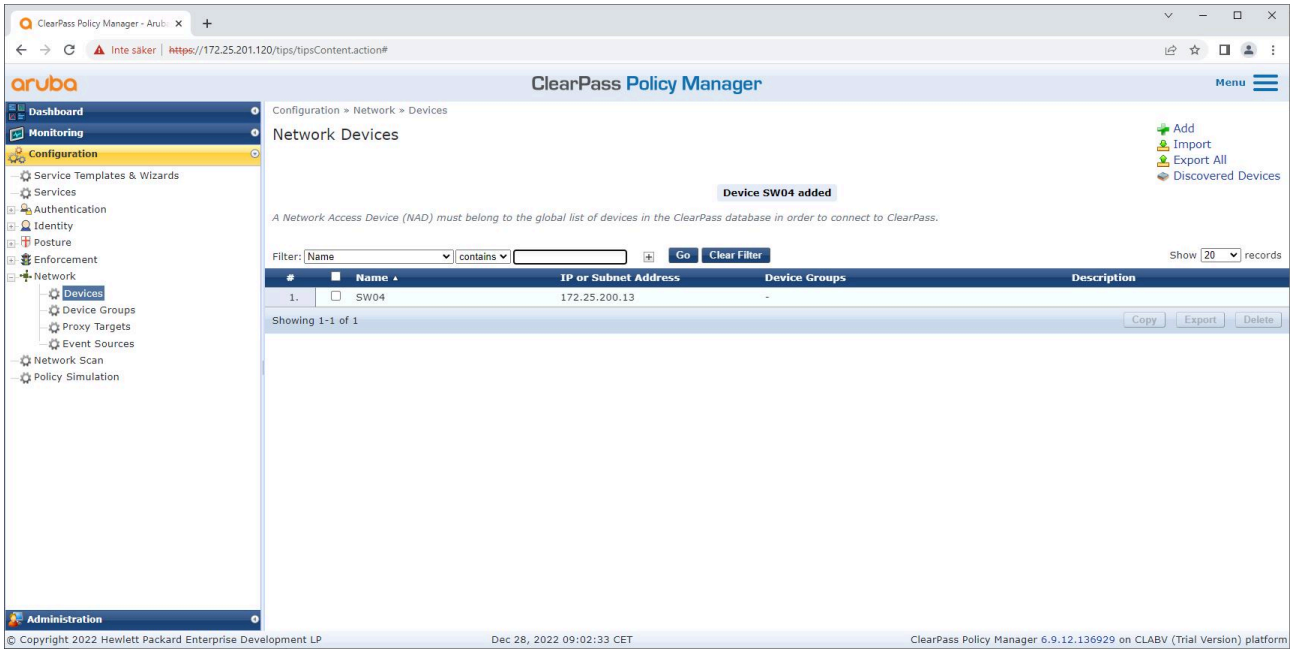
1. Add trusted network access devices such as HPE Aruba Networking access switches to ClearPass Policy Manager. ClearPass Policy Manager needs to know which access switches in the network are used for IEEE 802.1X communication. Note also that the RADIUS shared secret must match the specific switch IEEE 802.1X configuration
2. Use the network device group configuration to group multiple trusted network access devices. Grouping devices makes policy configuration easier.



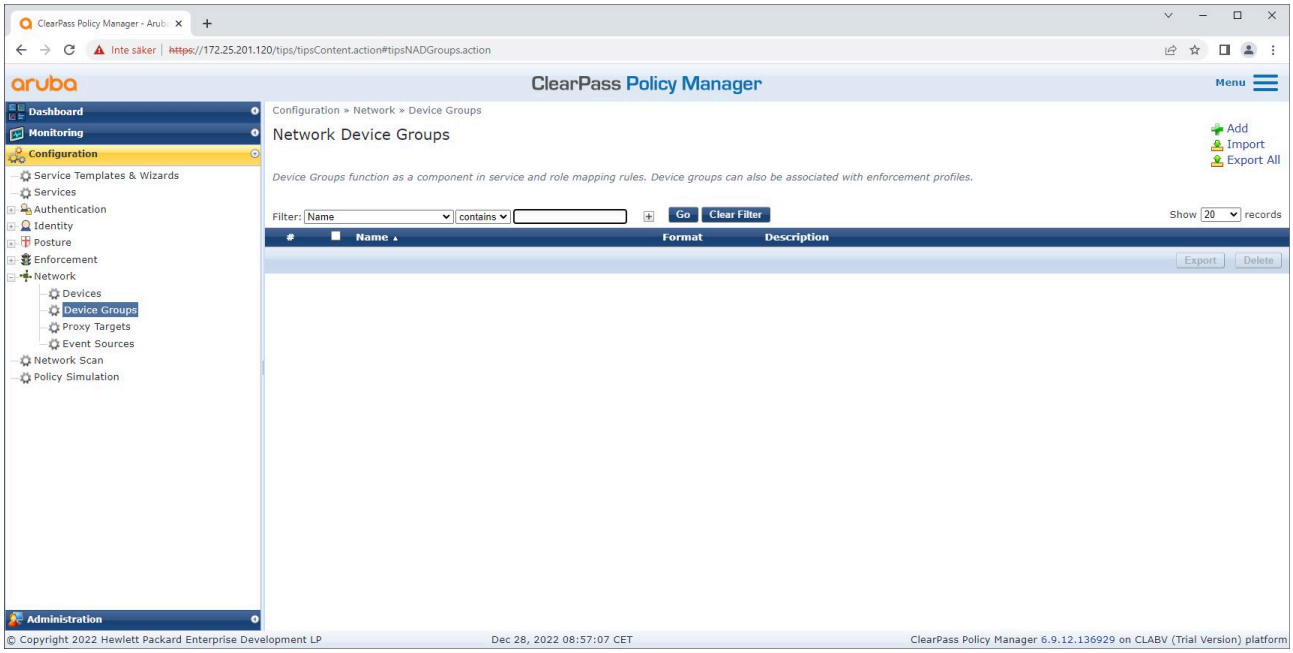
The trusted network devices interface in ClearPass Policy Manager.



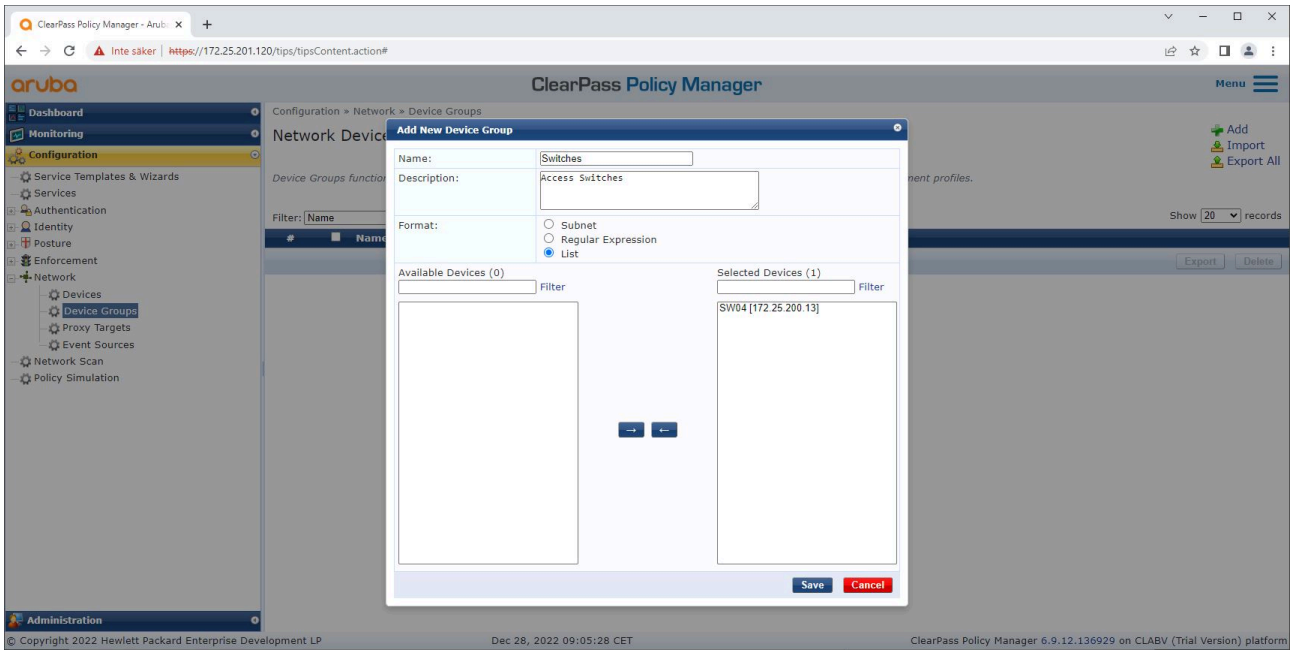
Add the HPE Aruba Networking access switch as a trusted device in ClearPass Policy Manager. Note that the RADIUS shared secret must match the specific switch IEEE 802.1X configuration.



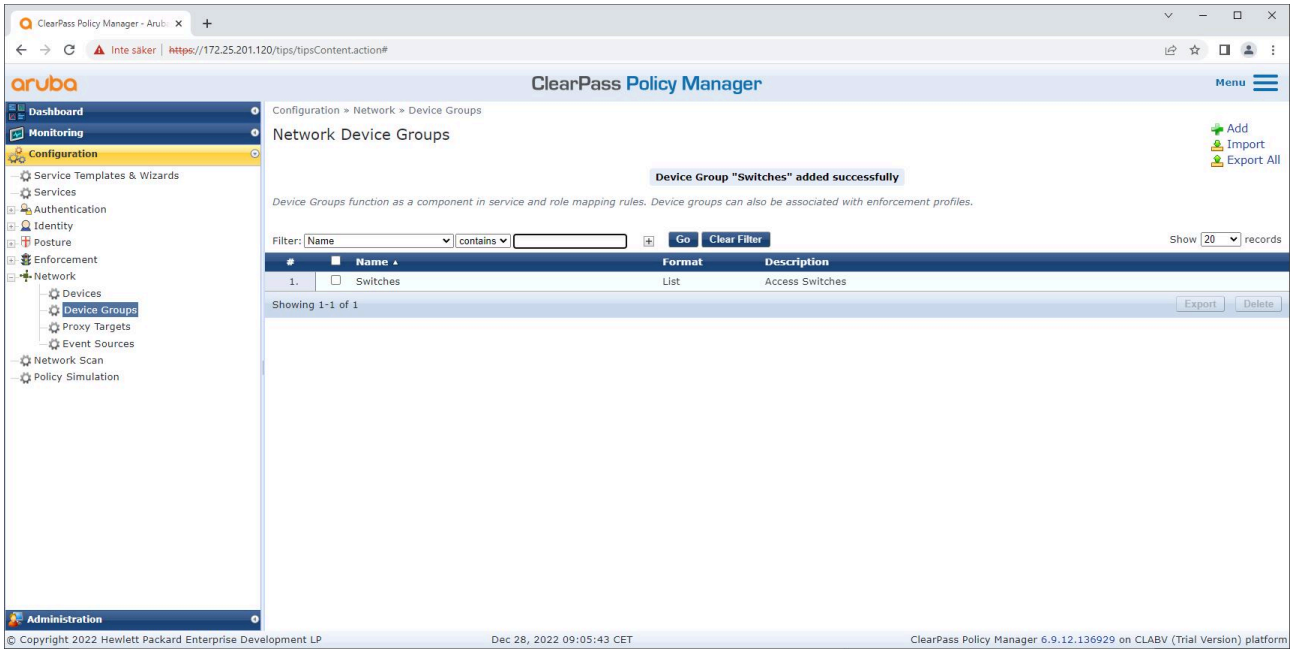
ClearPass Policy Manager with a single trusted network device configured.



The trusted network device groups interface in ClearPass Policy Manager.



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

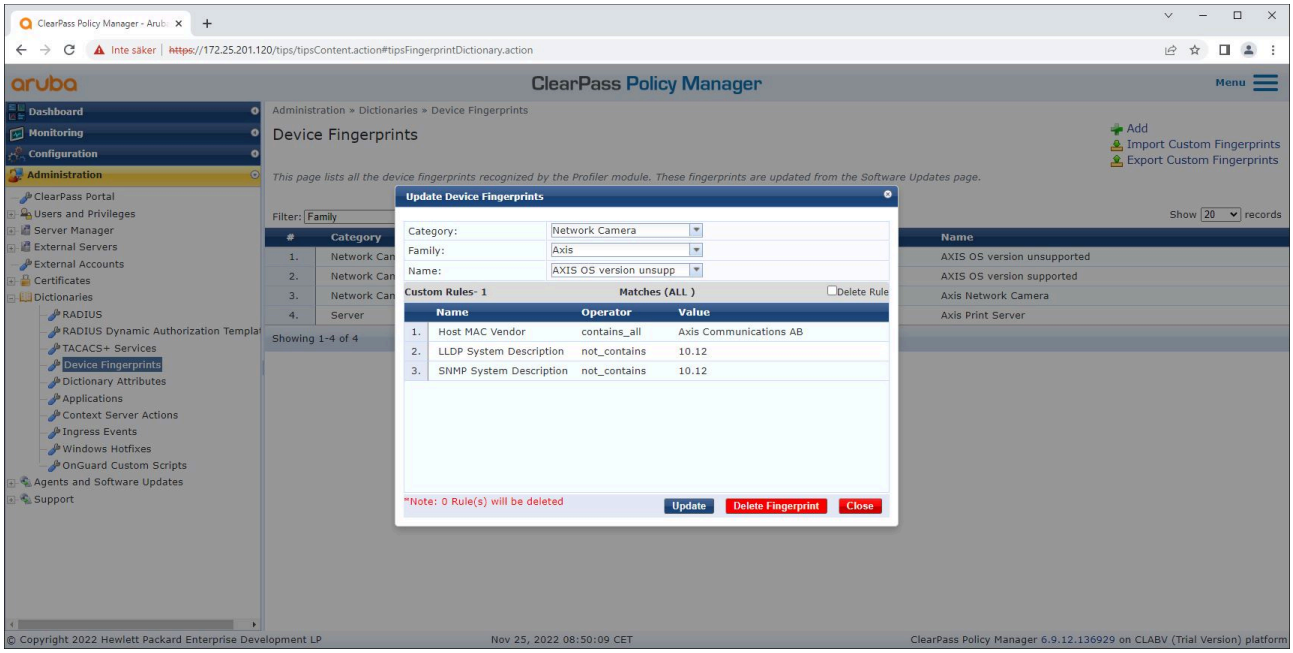


ClearPass Policy Manager with a configured network device group that includes one or more trusted network devices.

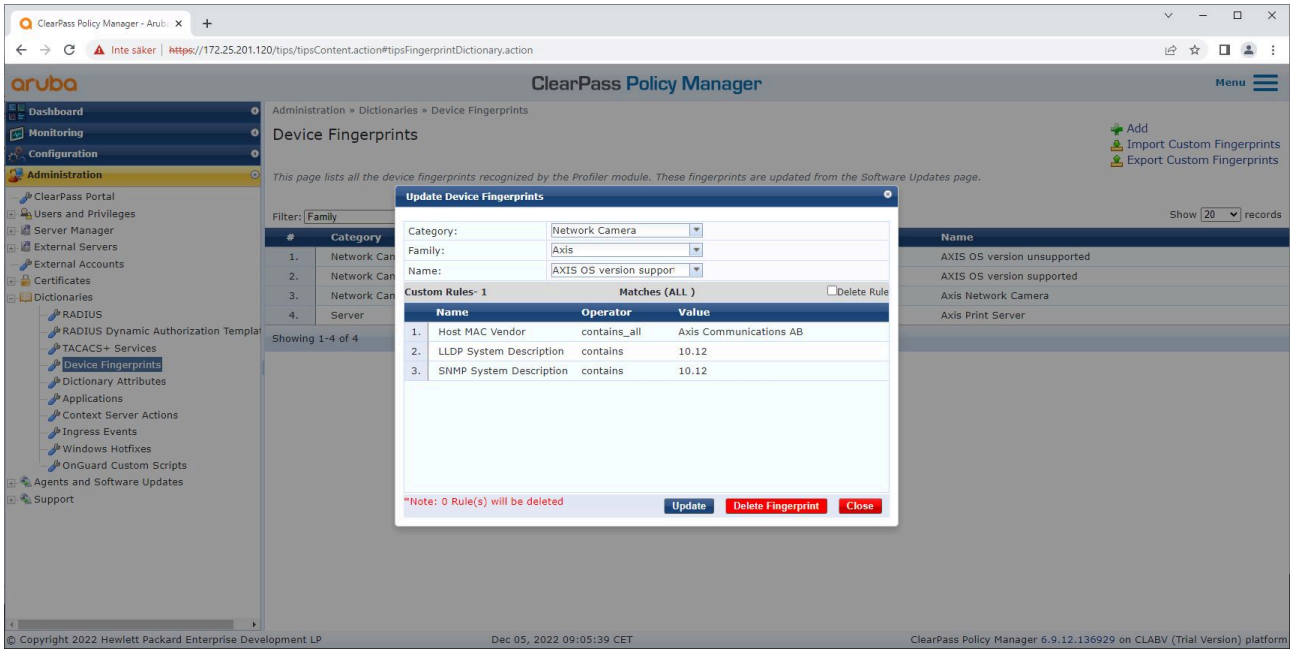
Device fingerprint configuration

The Axis device can, through network discovery, distribute device-specific information such as the MAC-address and the device software version. You can use this information to create, update, or manage a device fingerprint in ClearPass Policy Manager. 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. Make the device fingerprint settings.



The device fingerprint configuration in ClearPass Policy Manager. Axis devices running AXIS OS versions other than 10.12 are unsupported in this example.



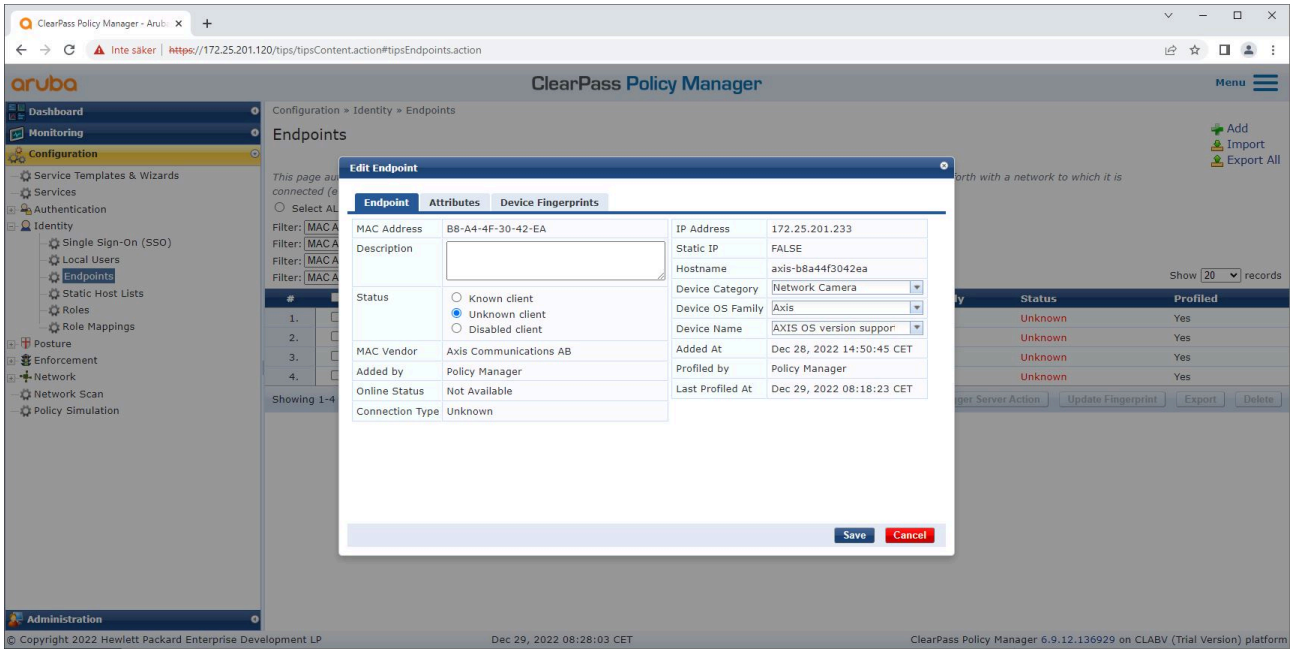
The device fingerprint configuration in ClearPass Policy Manager. Axis devices running AXIS OS versions other than 10.12 are supported in this example.

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

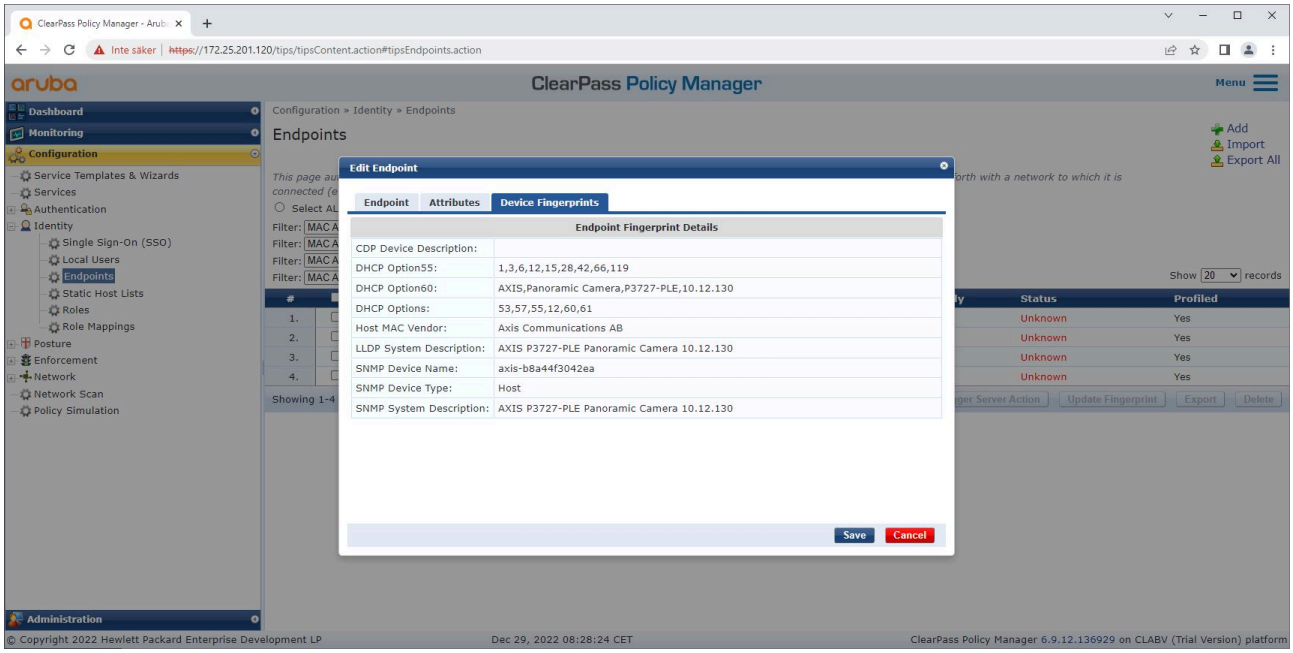
1. Go to **Configuration > Identity > Endpoints**.
2. Select the device you want to view.
3. Click on the **Device Fingerprints** tab.

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.

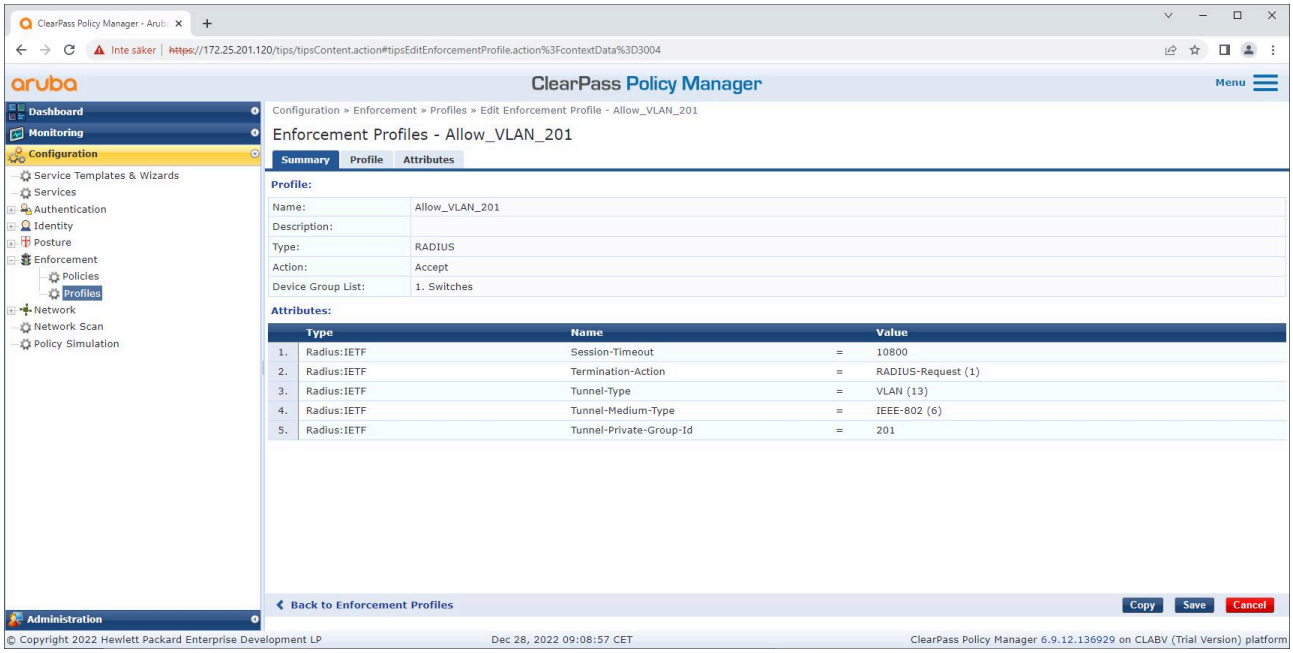


The detailed device fingerprints of a profiled Axis device. Note that SNMP is disabled by default in Axis devices. LLDP, CDP and DHCP-specific discovery information is shared by the Axis device in the factory-default state and is relayed by the HPE Aruba Networking access switch to ClearPass Policy Manager.

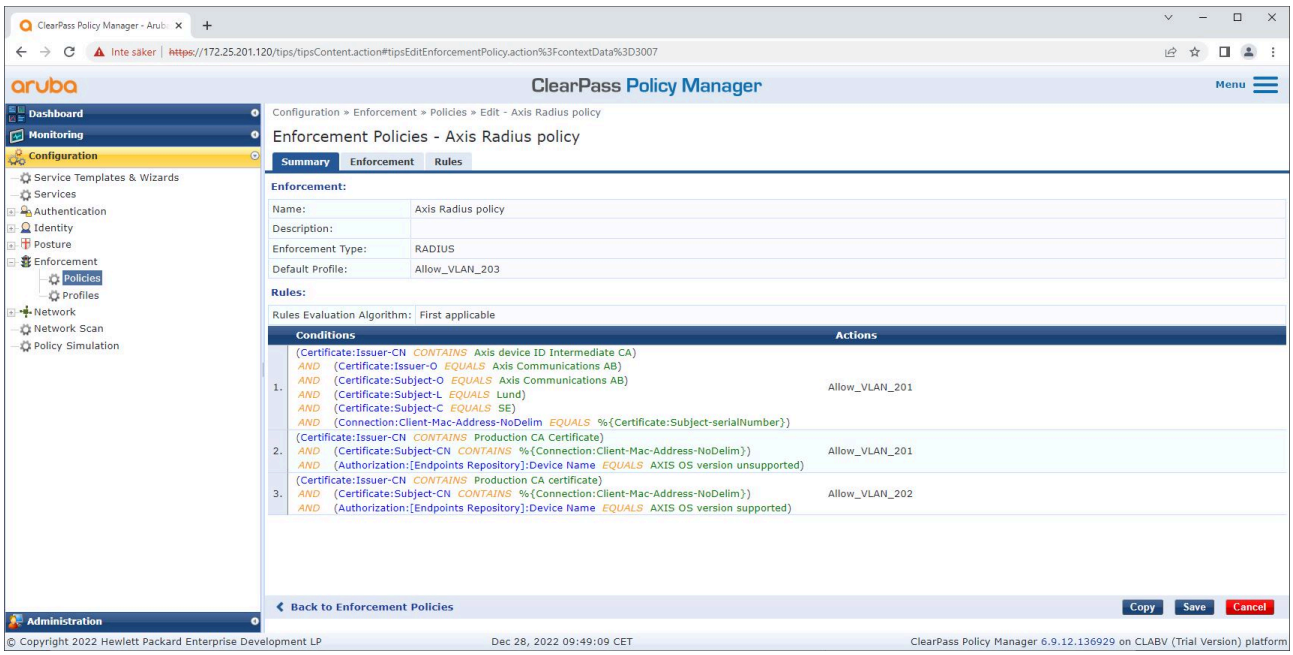
Enforcement profile configuration

Enforcement Profile allows ClearPass Policy Manager to assign a specific VLAN ID to an access port on the switch. This is a policy-based decision that applies to the network devices in the device group "Switches". The required number of enforcement profiles depends on the number of VLANs in use. Our setup has three VLANs (VLAN 201, 202, 203), which correlate to three enforcement profiles.

After the enforcement profiles for the VLAN are configured, the enforcement policy itself can be configured. The enforcement policy configuration in ClearPass Policy Manager defines if Axis devices are granted access to HPE Aruba Networking 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:

Denied network access

Access to the network is denied when IEEE 802.1X network access control authentication is not 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 then required, to decide on the 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 device's AXIS OS version.
- The device's MAC-address matches the vendor-specific 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.

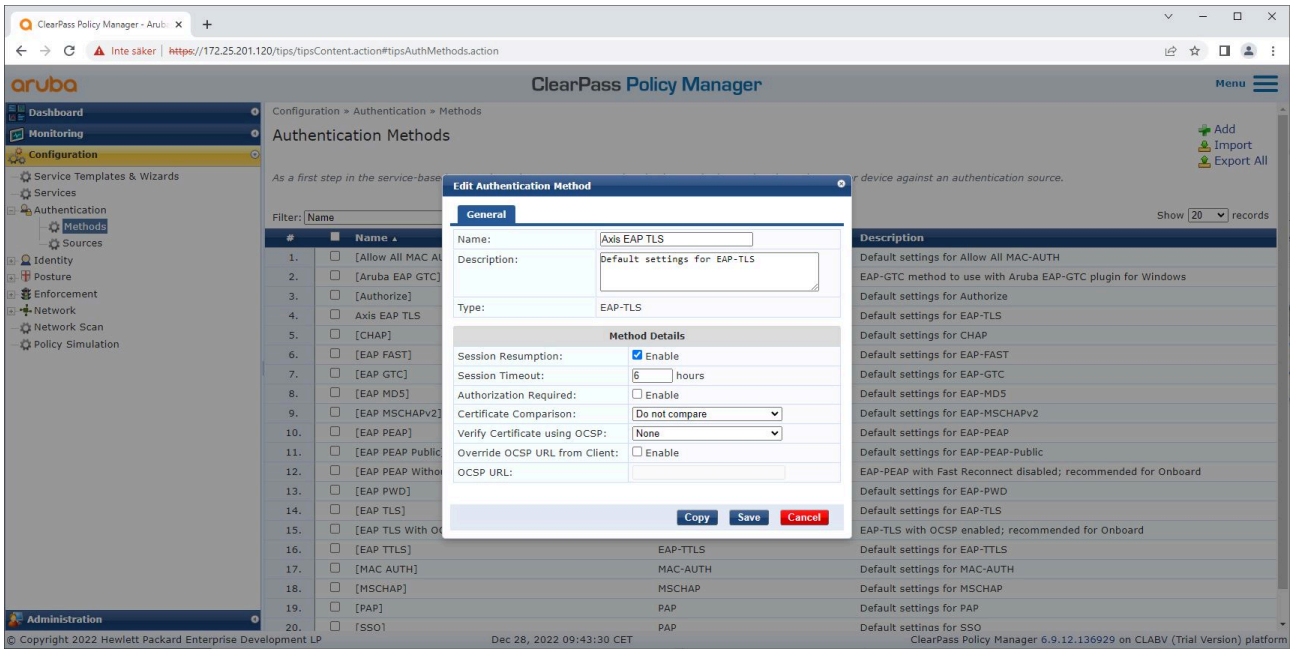
Production network (VLAN 202)

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

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

Authentication method configuration

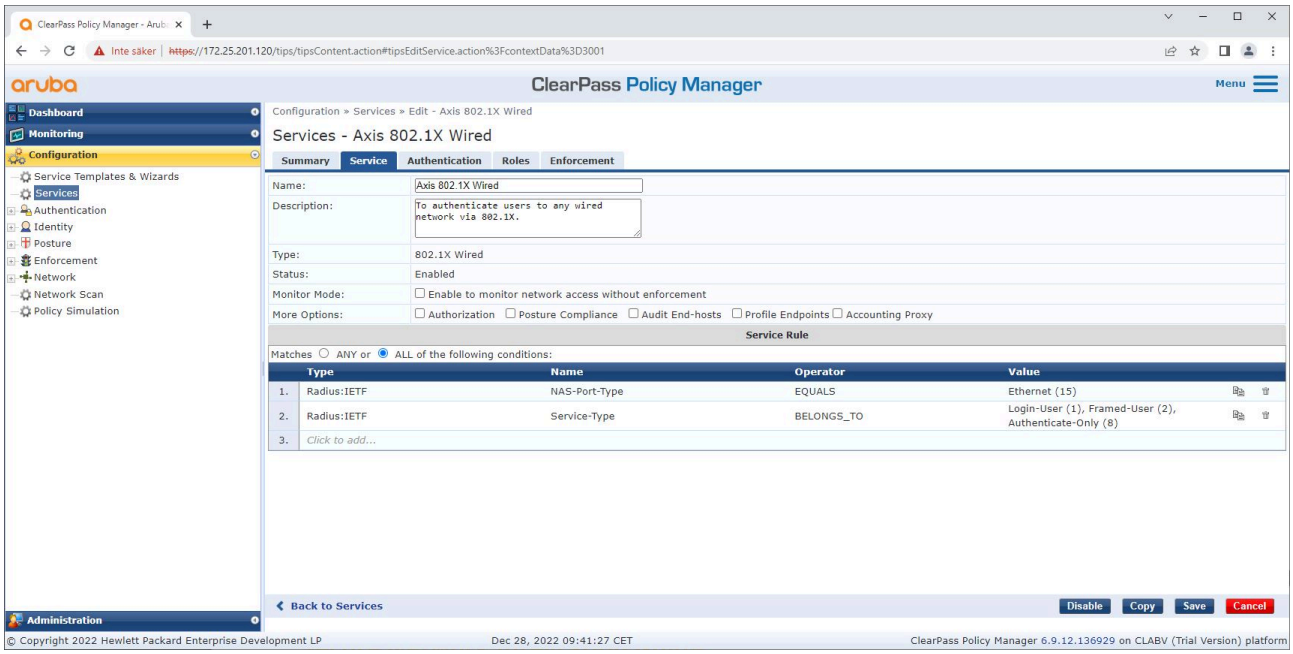
The authentication method defines how an Axis device attempts to authenticate itself on the network. The preferred method is IEEE 802.1X EAP-TLS, as Axis devices with Axis Edge Vault come with IEEE 802.1X EAP-TLS enabled by default.



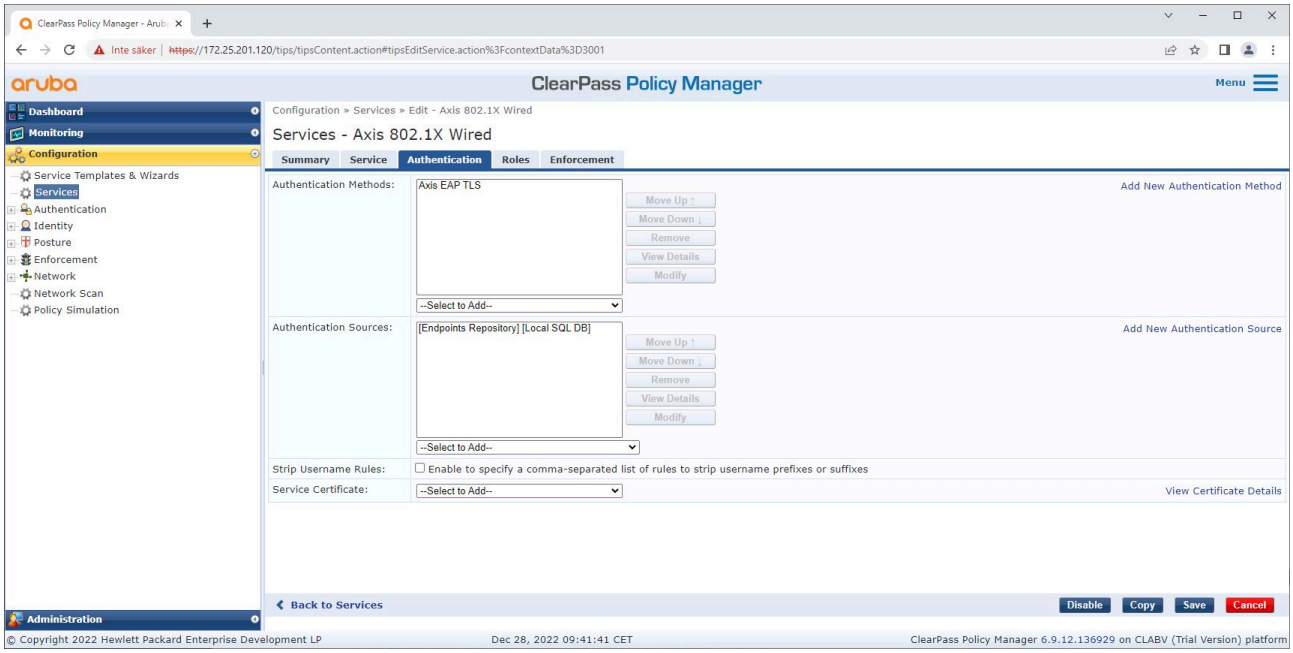
The authentication method interface of ClearPass Policy Manager, where the EAP-TLS authentication method for Axis devices is defined.

Service configuration

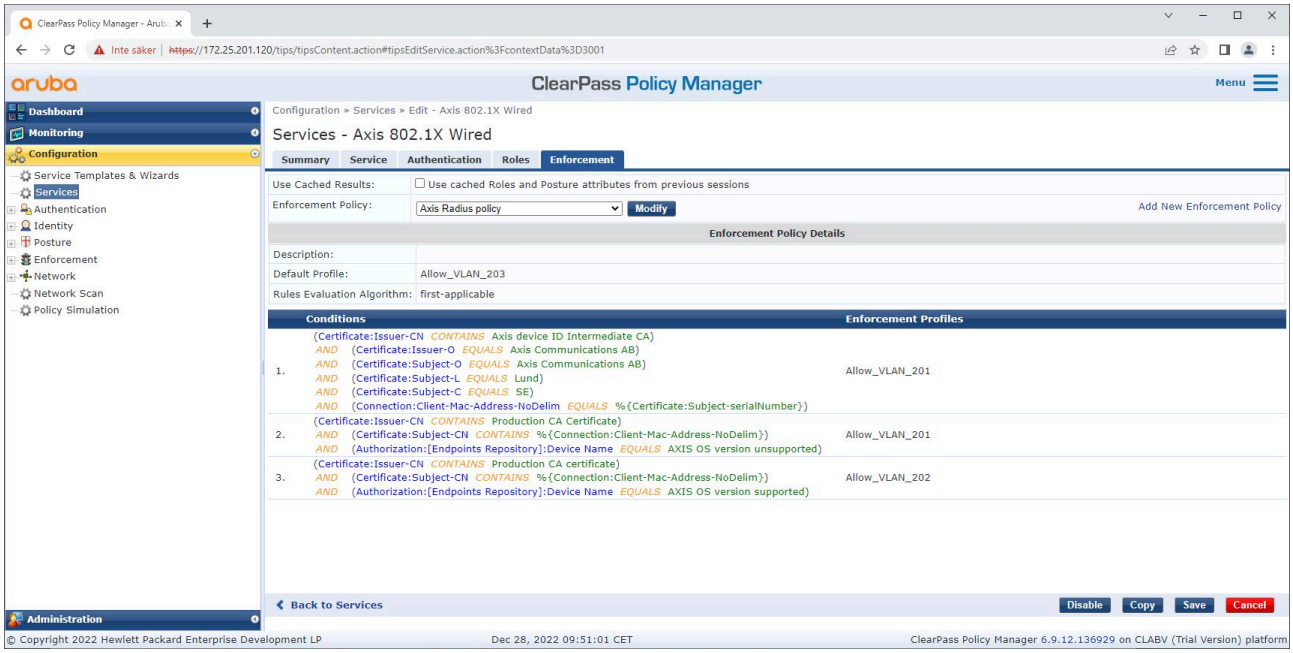
On the **Services** page, the configuration steps are combined into a single service that handles the authentication and authorization of Axis devices in HPE Aruba Networking networks.



A dedicated Axis service is created, with IEEE 802.1X as the connection method.



The EAP-TLS authentication method created earlier is configured for the service.



The enforcement policy created earlier is configured for the service.

HPE Aruba Networking access switch

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

Note

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

This example shows global and port configuration for HPE Aruba Networking access switches.

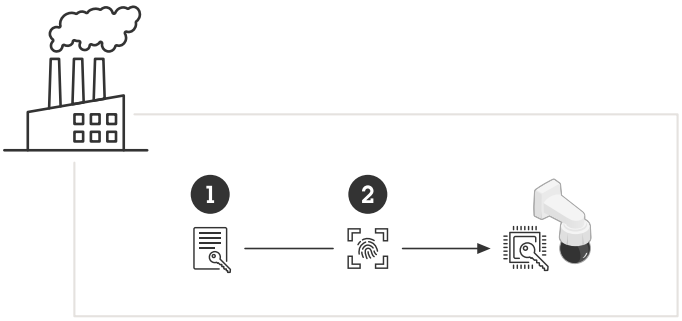
```
radius-server host MyRADIUSIPAddress key "MyRADIUSKey"
```

```
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
```

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.



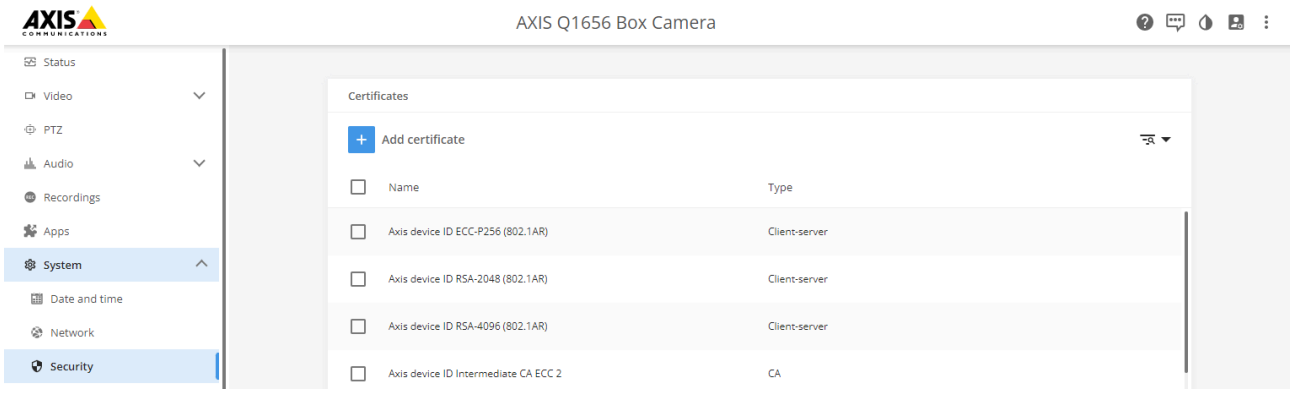
Axis devices are manufactured with the IEEE 802.1AR-compliant Axis device ID certificate for trusted device identity services

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), which can globally prove the authenticity of the Axis device. *Axis Product Selector* can be used to find which Axis devices have support for Axis Edge Vault and Axis device ID.

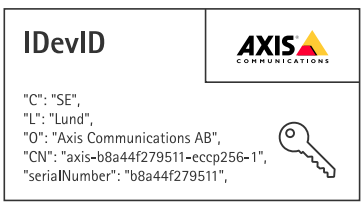
Note

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



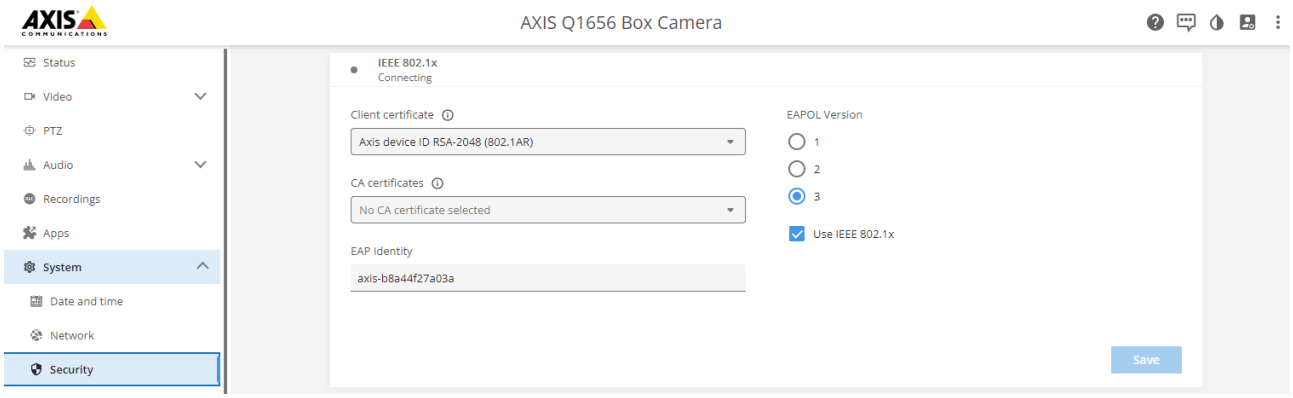
The certificate store of the Axis device in the factory default state, with Axis Device ID.

The IEEE 802.1AR-compliant Axis device ID certificate includes information about the serial number and other vendor-specific information. This information is used by ClearPass Policy Manager for analysis and decision making to grant access to the network. The information below 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 from a combination of the Axis company name, the device's serial number, followed by the crypto algorithm (ECC P256, RSA 2048, RSA 4096). As of AXIS OS 10.1 (2020-09), IEEE 802.1X is enabled by default with the Axis device ID pre-configured. This enables the device to authenticate itself on IEEE 802.1X-enabled networks.



The Axis device in the factory default 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 manner. AXIS Device Manager is a Microsoft Windows®-based application that is installed locally on a machine in the network, while AXIS Device Manager Extend relies on cloud infrastructure to perform multi-site device management. Both offer easy management and configuration capabilities, such as:

- Installation of AXIS OS updates.
- Application of cybersecurity configurations 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

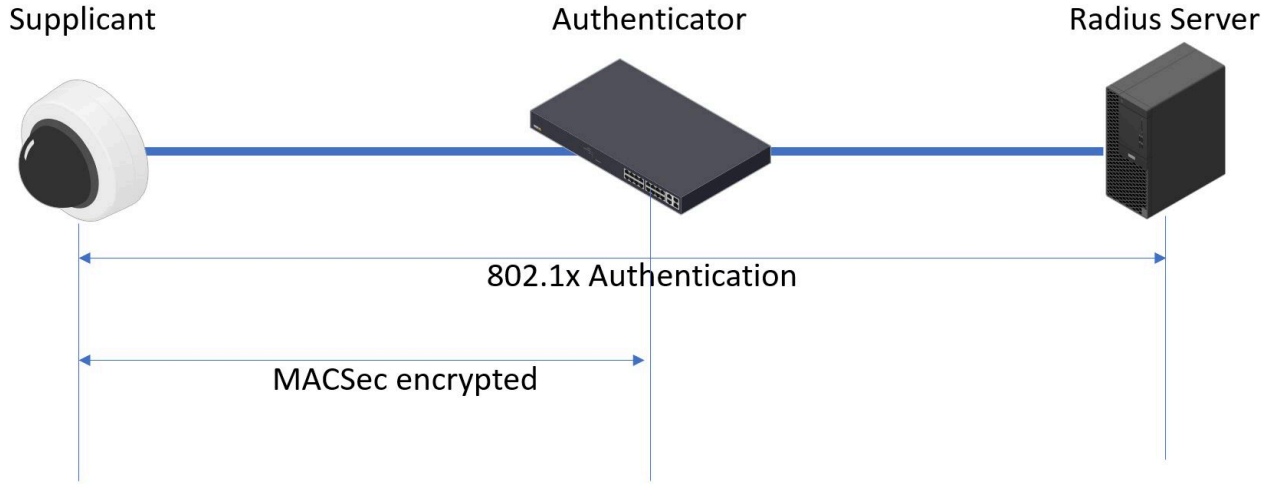
To watch this video, go to the web version of this document.

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

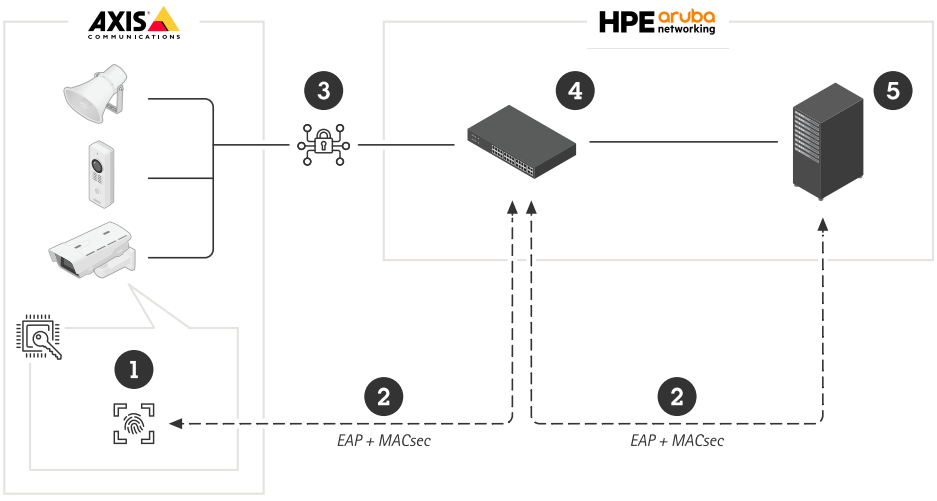
IEEE 802.1AE MACsec (Media Access Control Security) is a well-defined network protocol that cryptographically secures point-to-point Ethernet links on network layer 2. It ensures the confidentiality and integrity of data transmissions between two hosts.

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 on the network (4, 5) through IEEE 802.1X EAP-TLS port-based network access control (2). Through

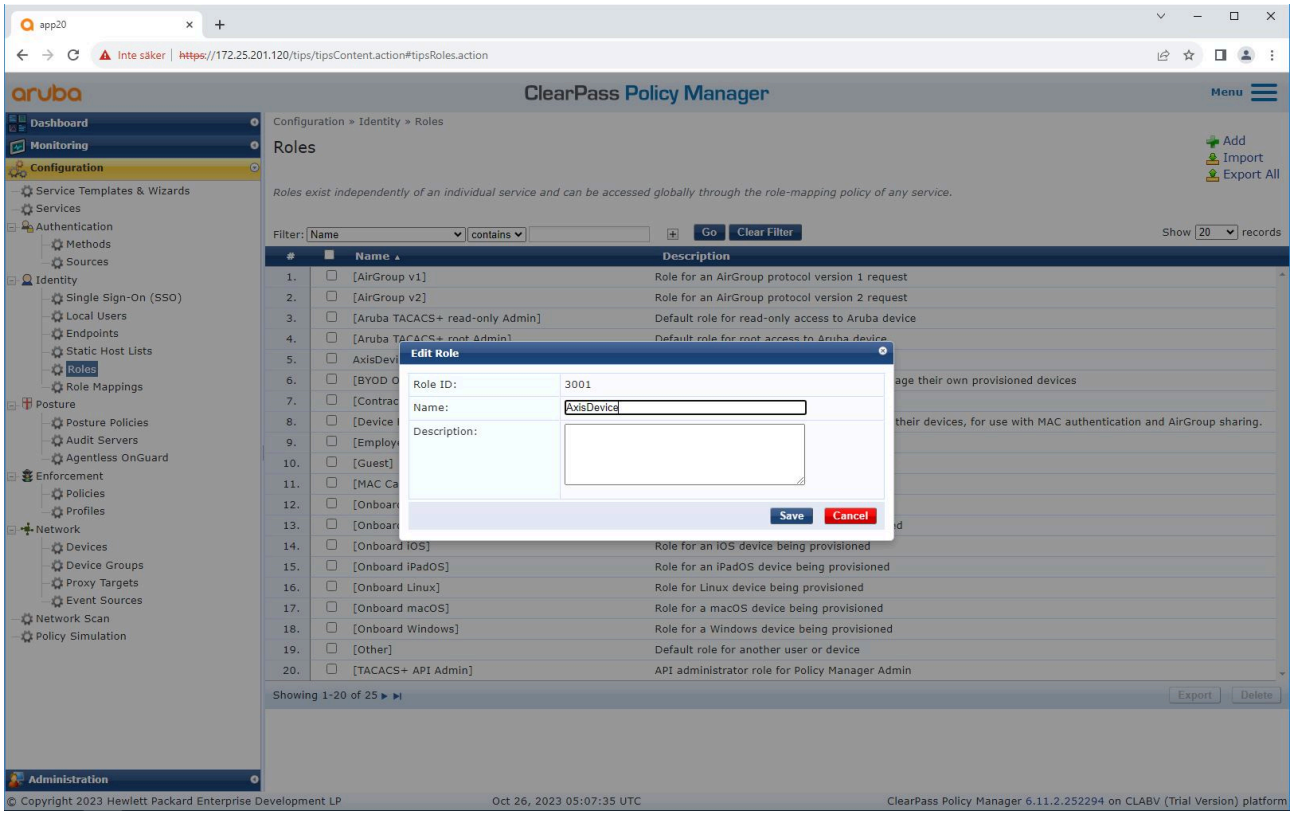
the EAP-TLS session, MACsec keys are exchanged automatically to set up a secure link (3), protecting all network traffic from the Axis device to the HPE Aruba Networking access switch.

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.

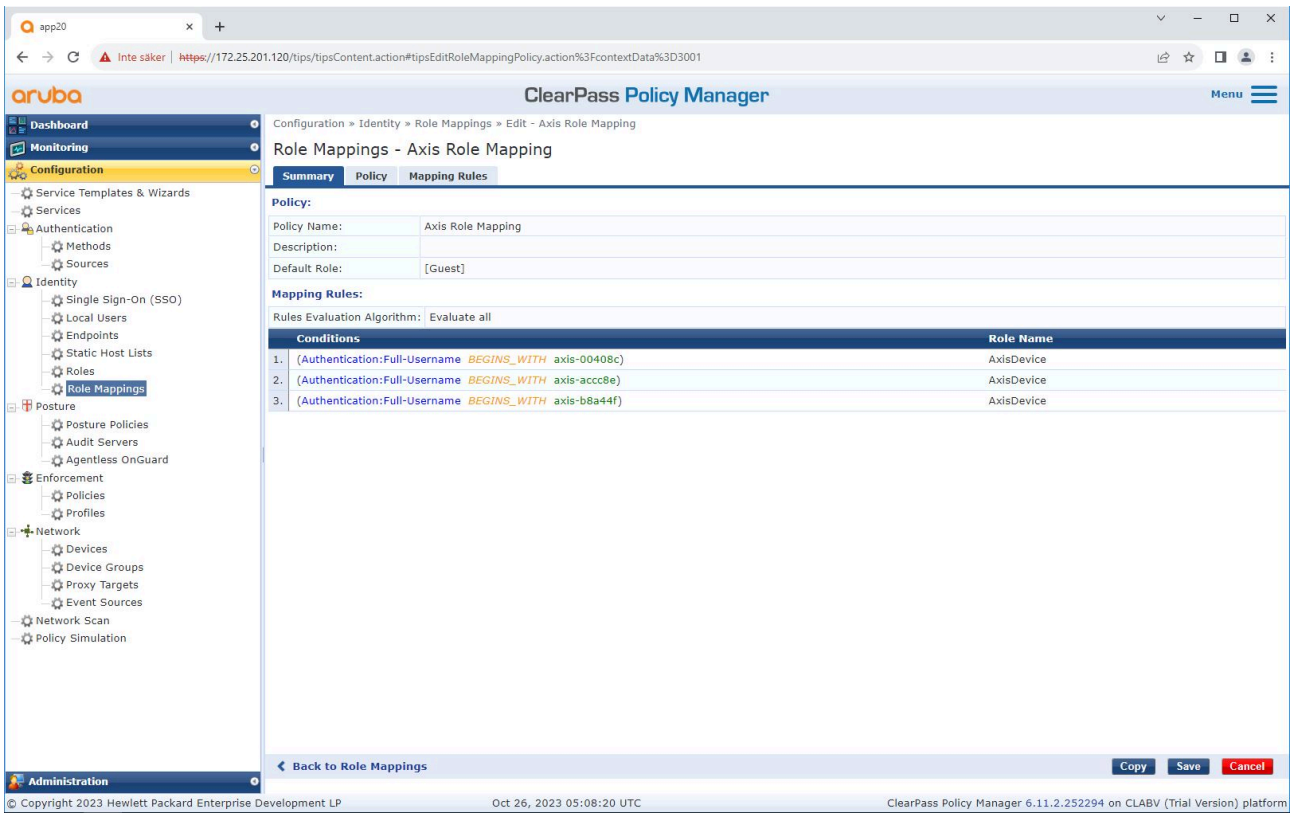
If the HPE Aruba Networking access switch doesn't support MACsec using EAP-TLS, then the Pre-Shared Key mode can be used and manually configured.

HPE Aruba Networking ClearPass Policy Manager

Role and role mapping policy



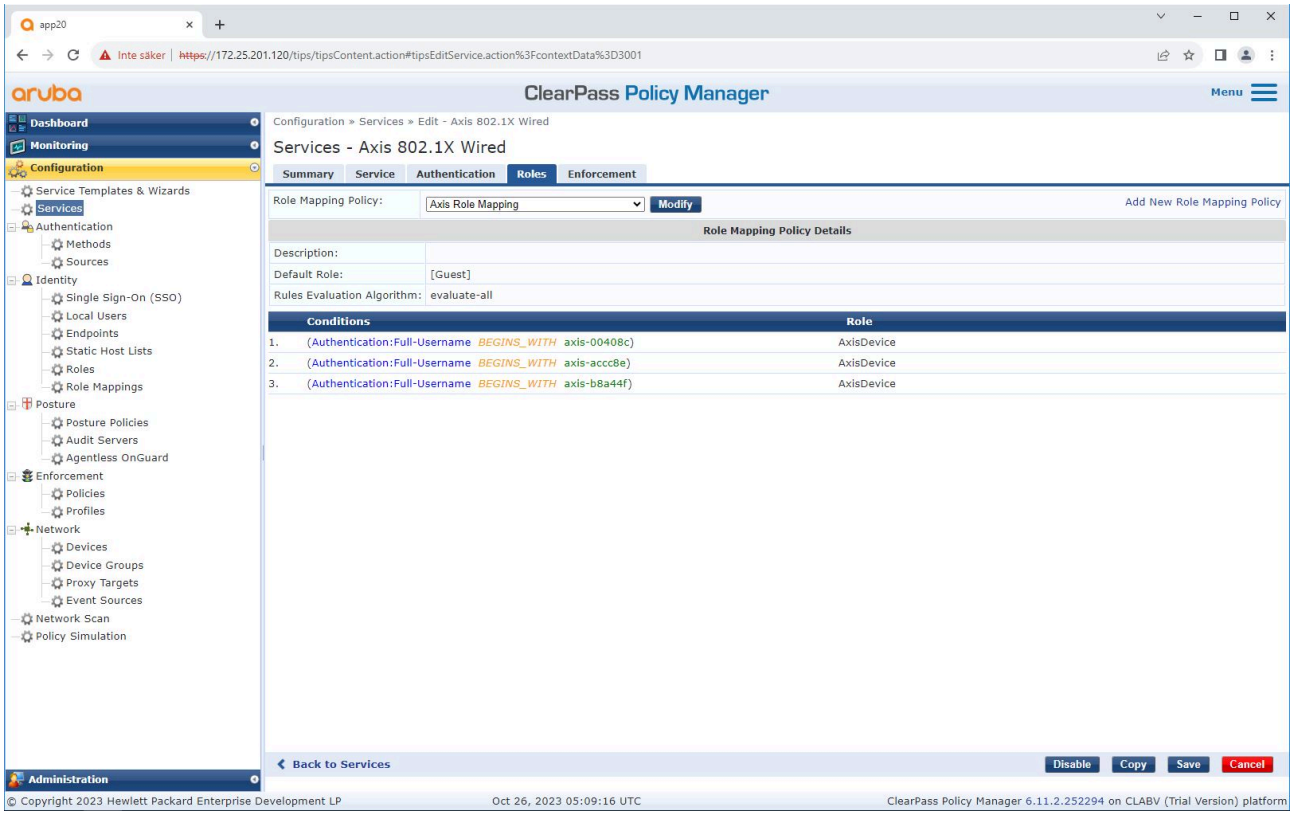
Add a role name for Axis devices. The name is the port access role name in the access switch configuration.



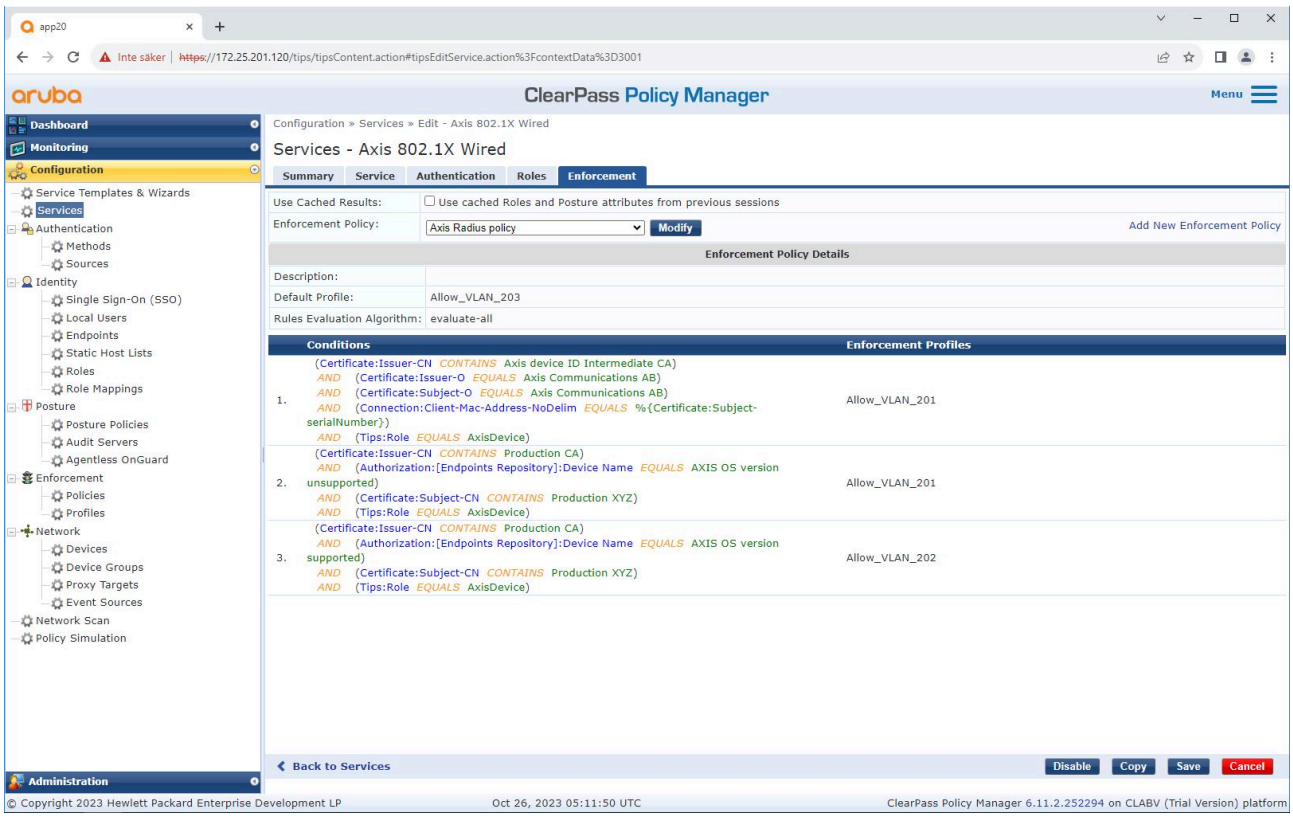
Add an Axis role mapping policy for the Axis device role created earlier. The conditions defined are required for a device to be mapped to the Axis device role. If the conditions are not met, the device becomes a part of the [Guest] role.

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

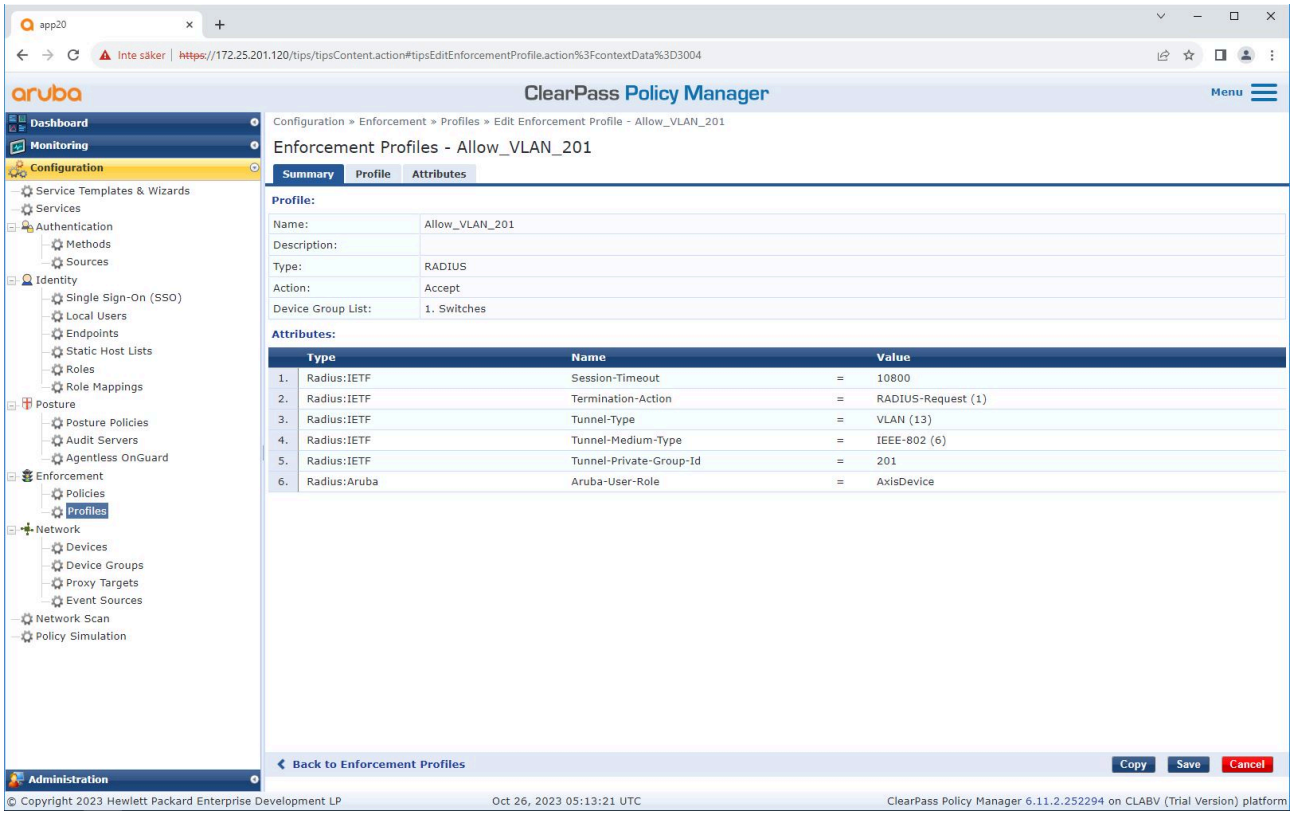


Add the Axis role mapping policy created earlier to the service that defines IEEE 802.1X as the connection method for the onboarding of Axis devices.



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

Enforcement profile



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

HPE Aruba Networking access switch

In addition to the secure onboarding configuration described in , see below the example port configuration for the HPE Aruba Networking access switch to configure 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
```

Legacy onboarding - MAC authentication

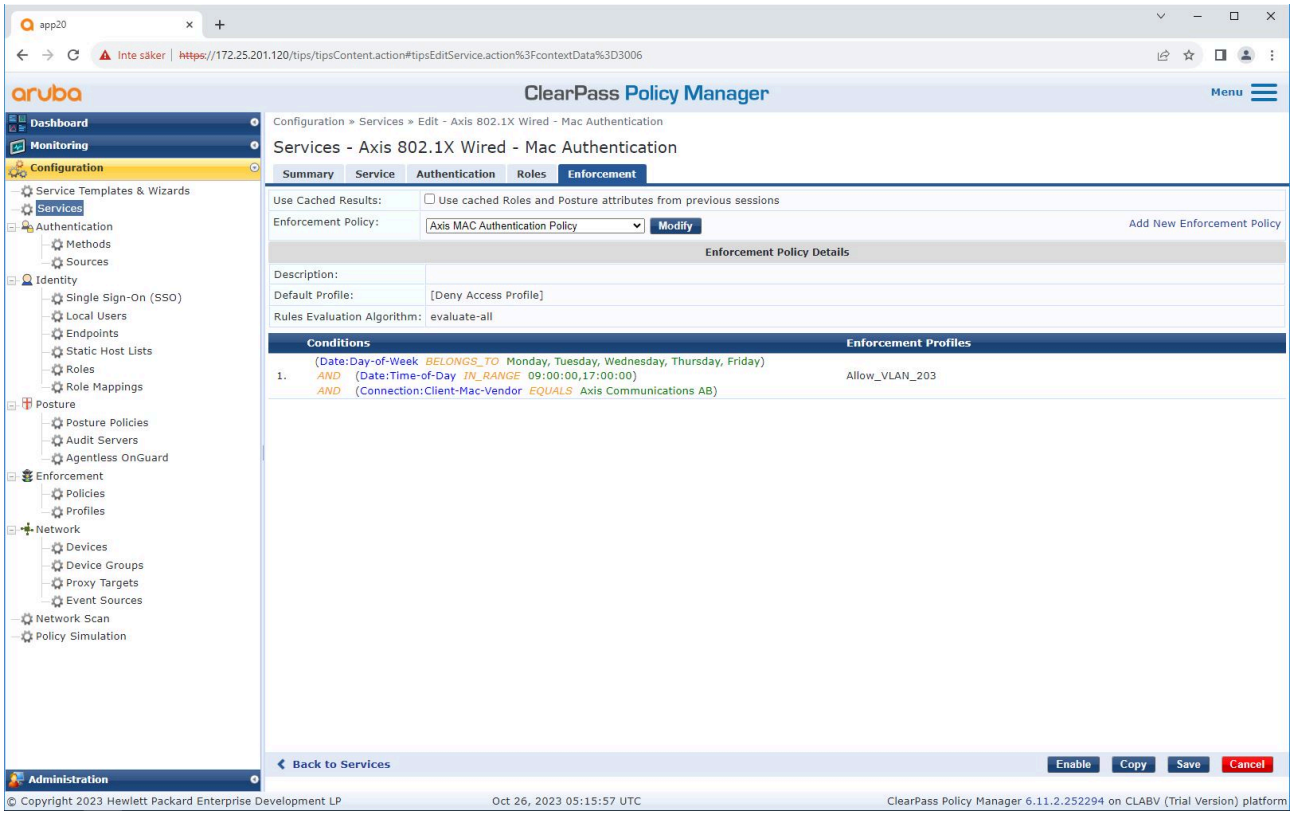
You can use MAC Authentication Bypass (MAB) to onboard Axis devices that don't support IEEE 802.1AR onboarding with the Axis device ID certificate and IEEE 802.1X enabled in the factory default state. If 802.1X onboarding fails, ClearPass Policy Manager validates the Axis device's MAC address and grants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

MAB requires both access switch and ClearPass Policy Manager configuration preparations. No configuration is required on the Axis device 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

If the Axis device does not meet the configured enforcement policy, it is denied access to the network.

Guest-network (VLAN 203)

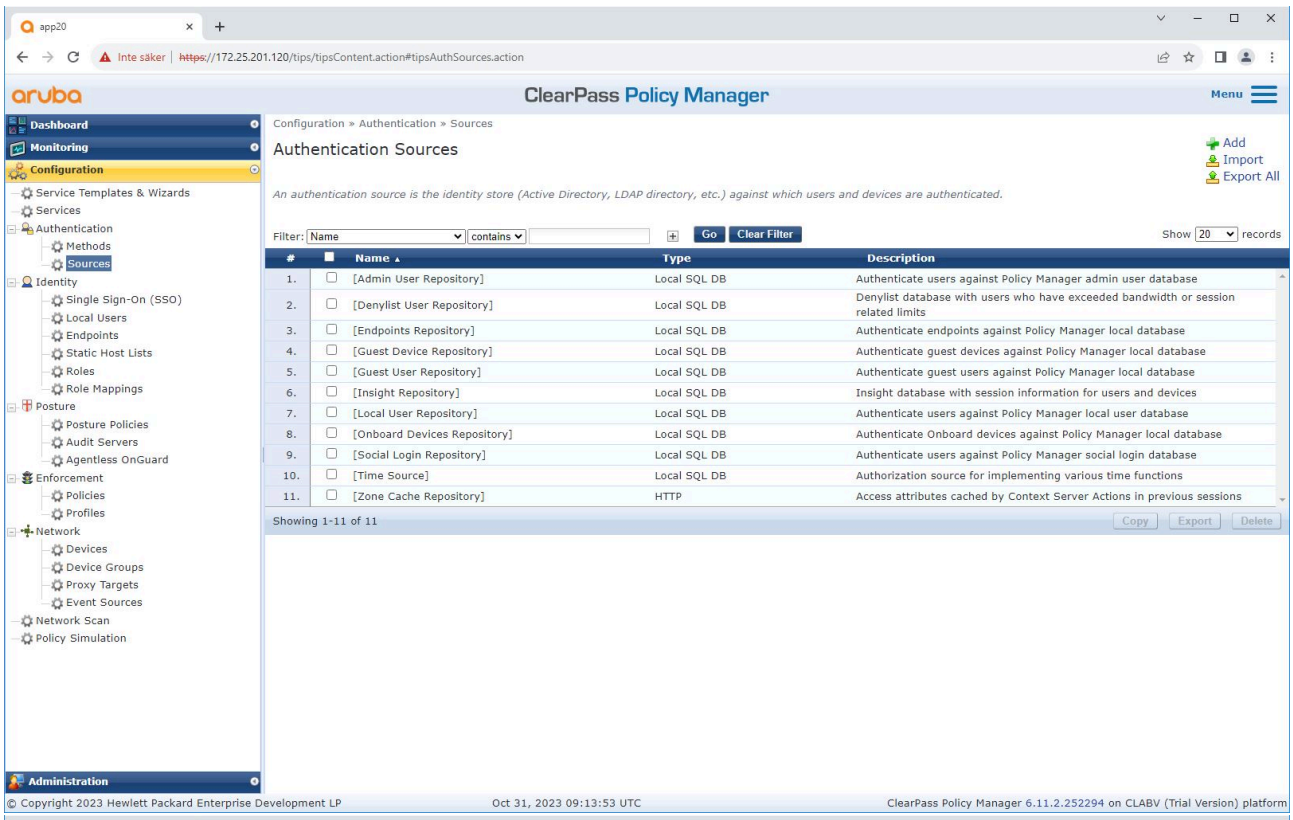
The Axis device is granted access to a limited, isolated network if the following conditions are met:

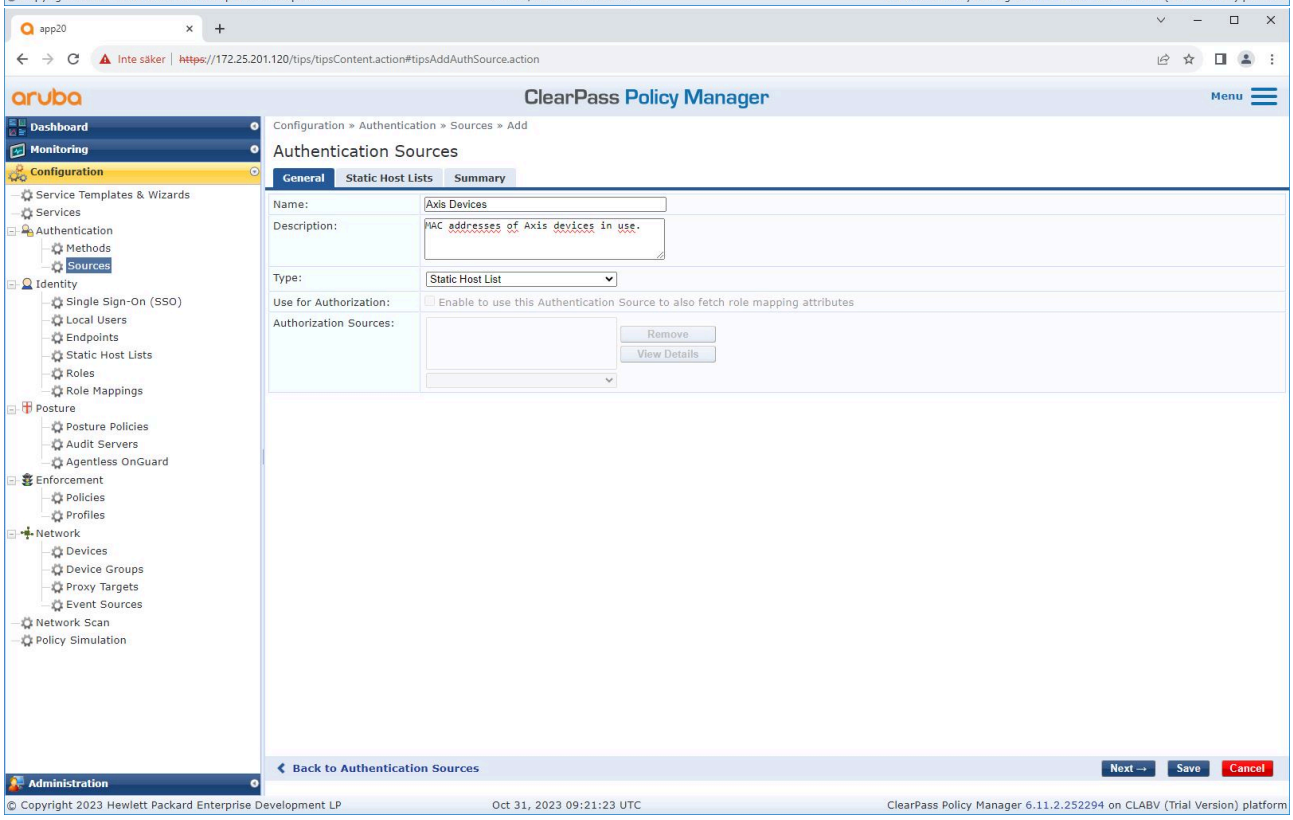
- The day is a weekday, Monday to Friday
- The time is between 09:00 and 17:00
- The MAC address vendor matches Axis Communications.

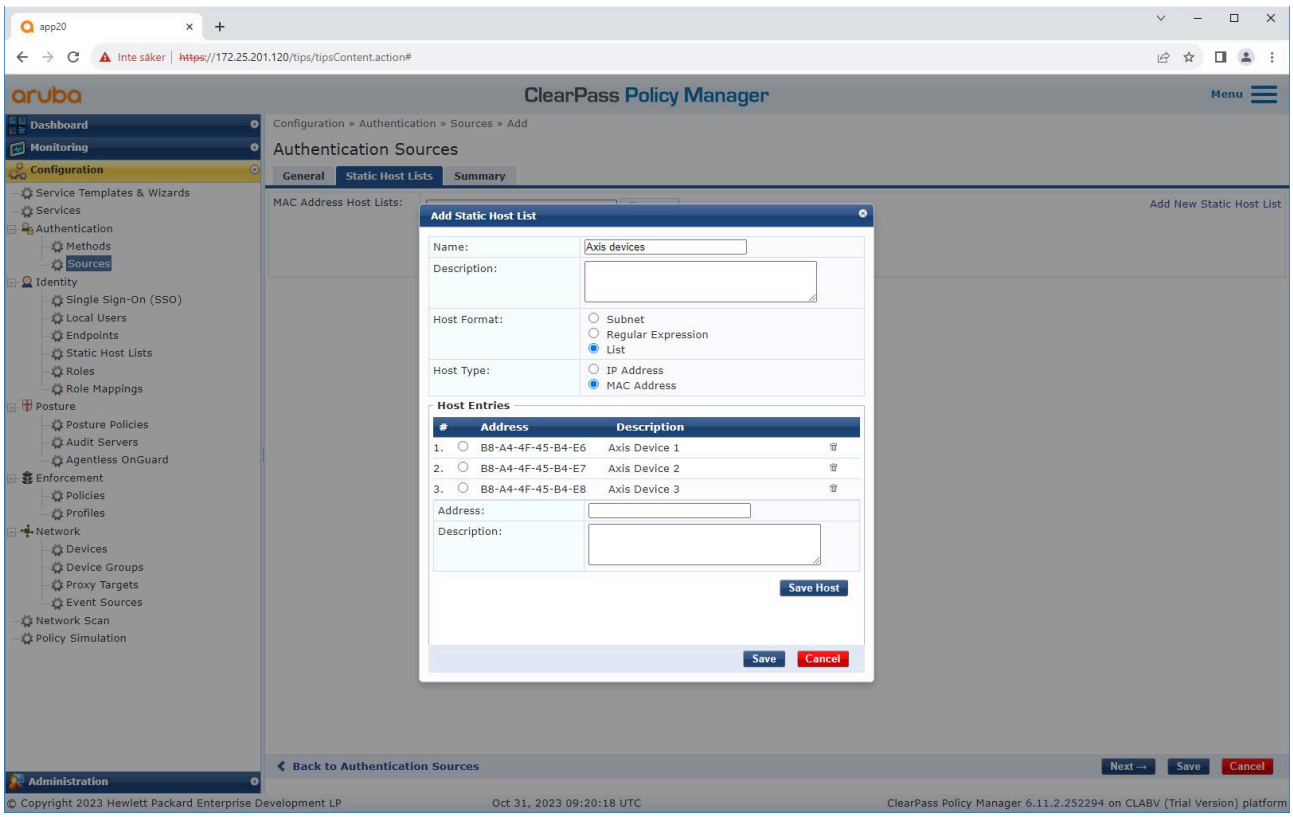
As it's possible to spoof a MAC addresses, access to the regular provisioning network is not granted. We recommend that you only use MAB for initial onboarding, and then manually inspect the device further.

Source configuration

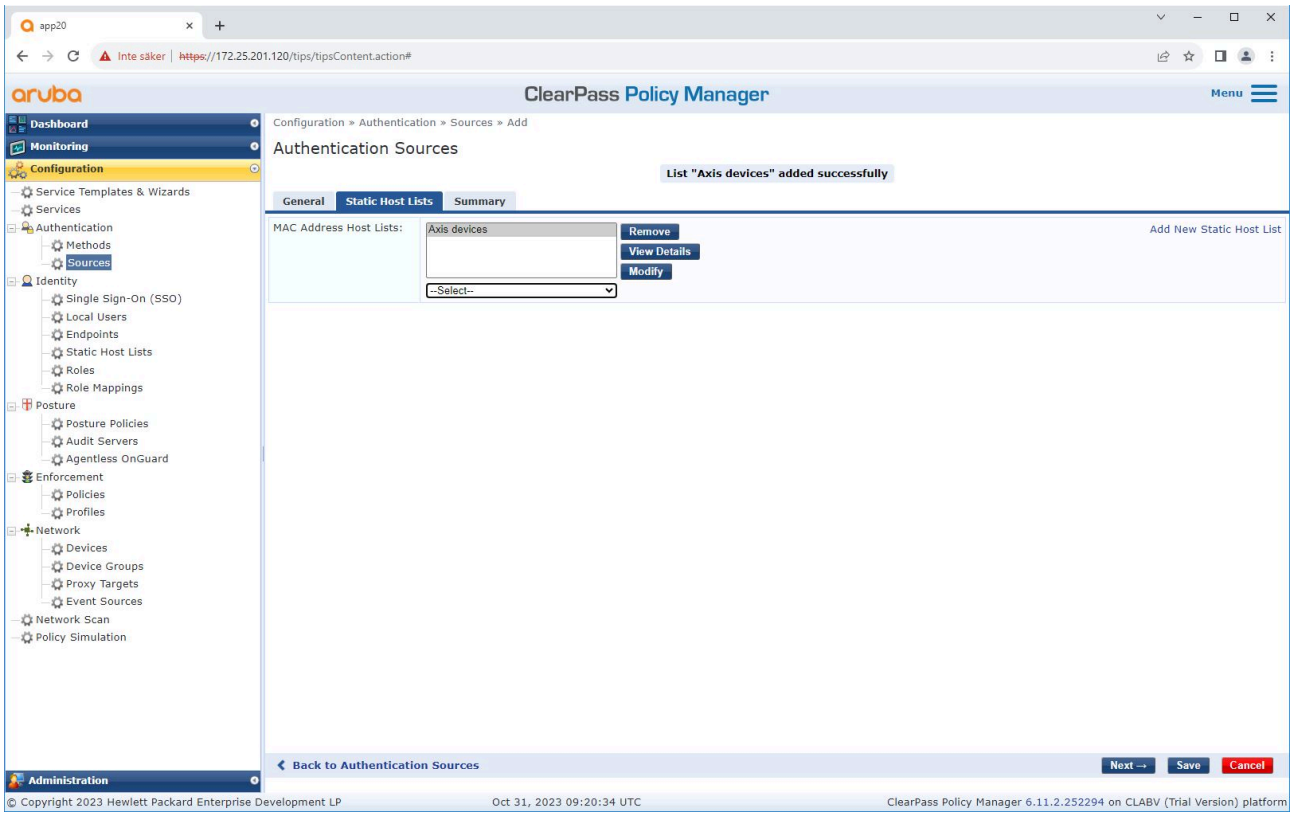
On the **Sources** page, a new authentication source is created to allow only manually imported MAC addresses.


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

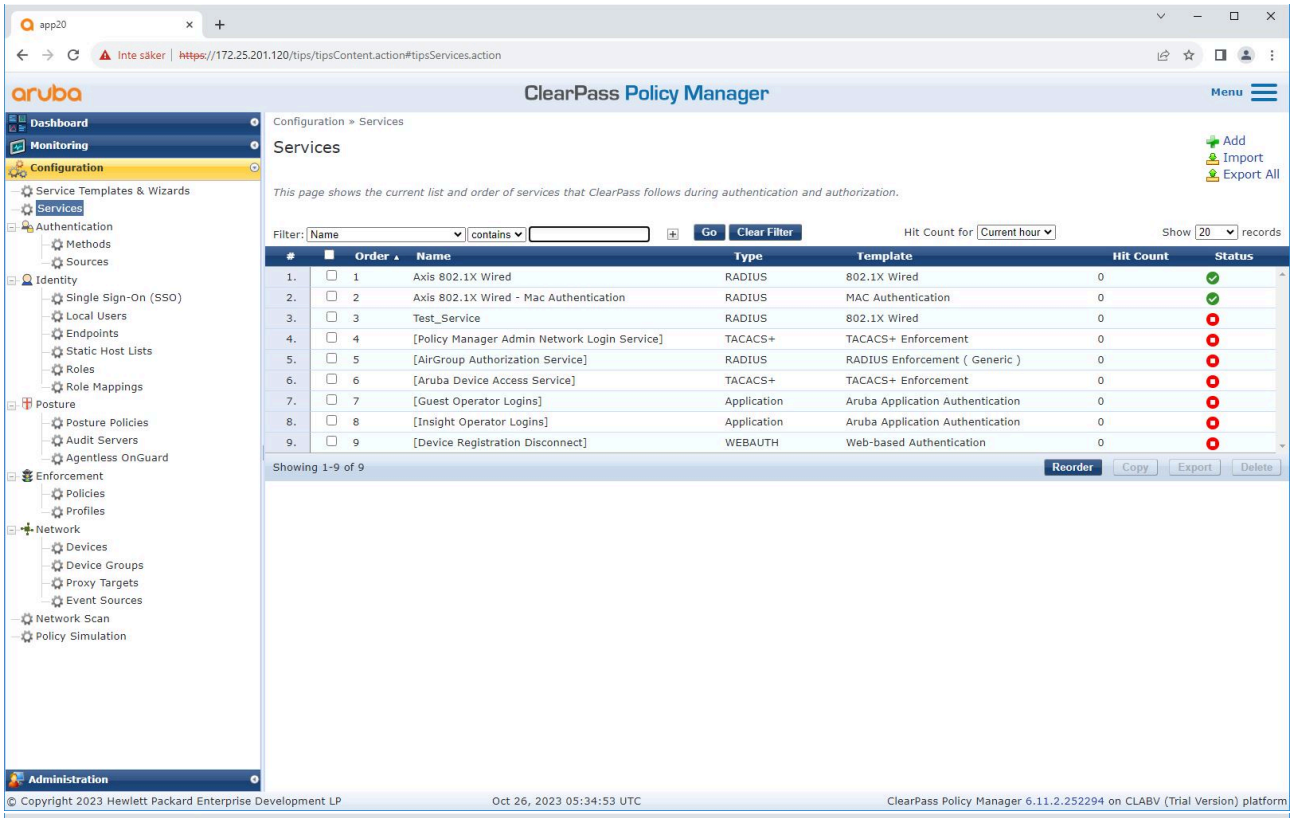


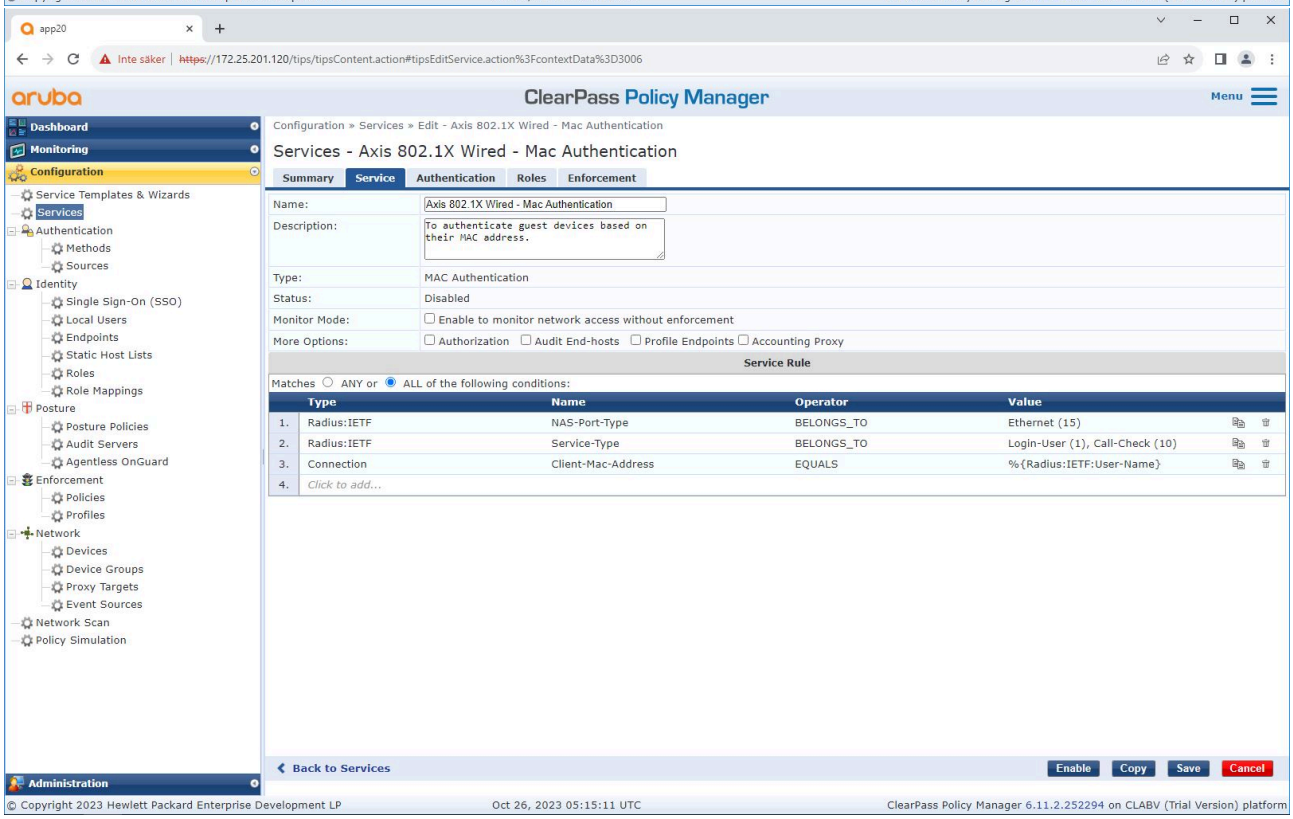
A static host list containing Axis MAC addresses is created.



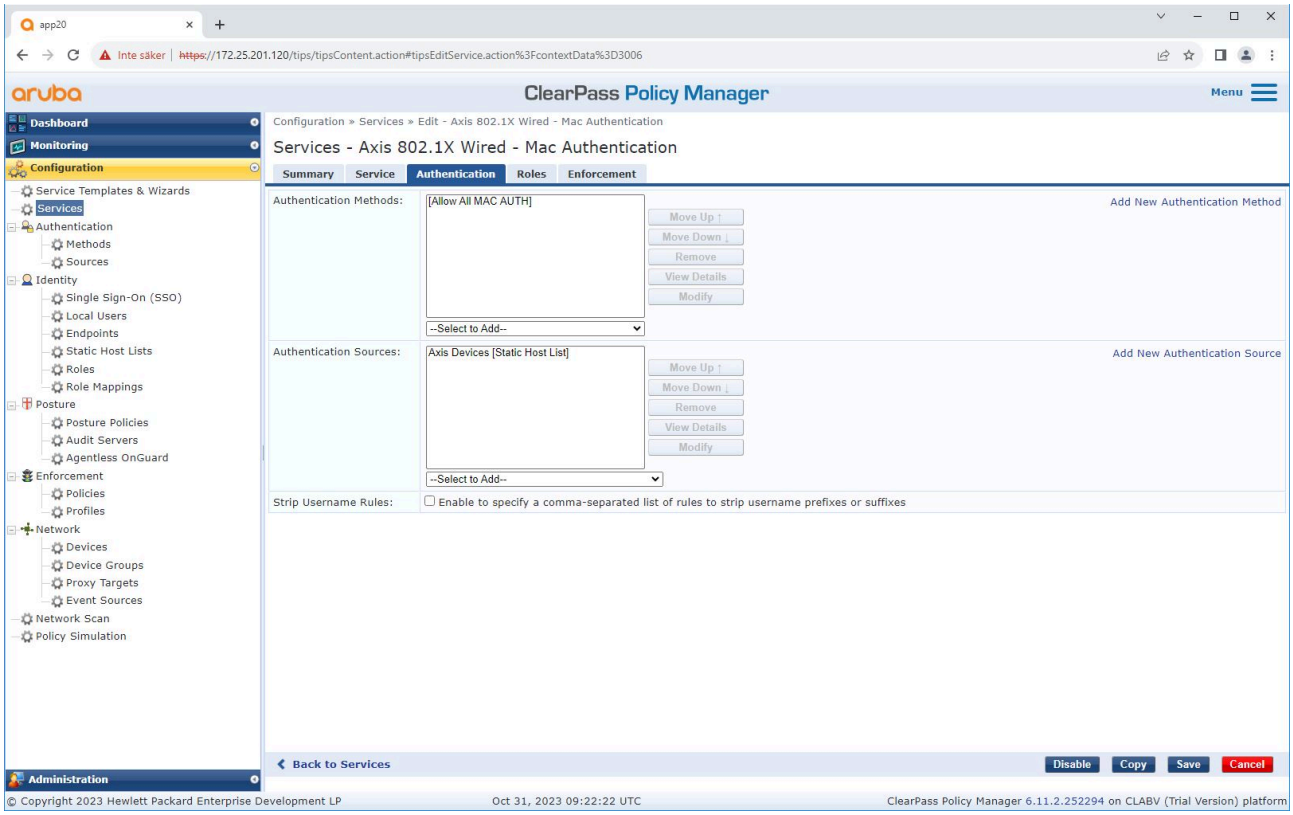
Service configuration

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





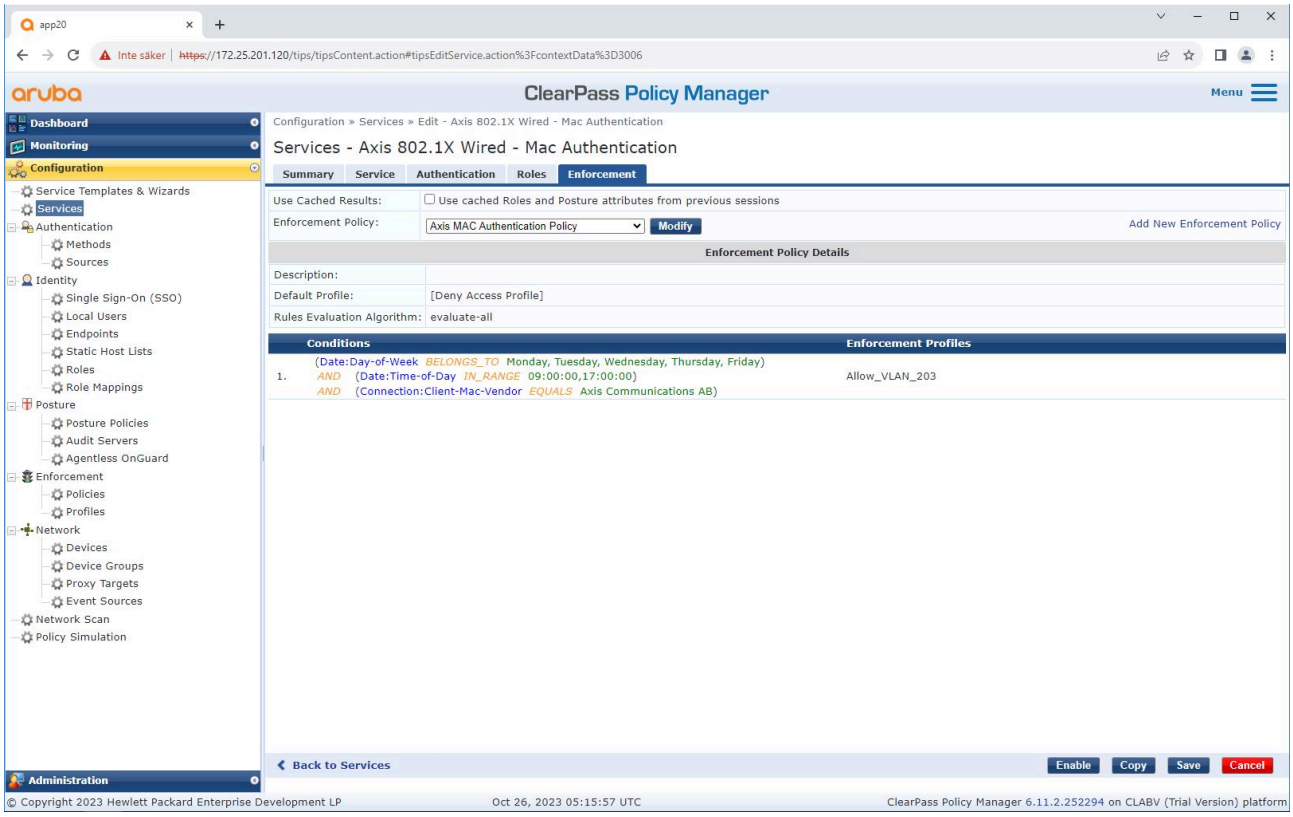
A dedicated Axis service that defines MAB as a connection method is created.



The pre-configured MAC authentication method is configured for the service. Also, the authentication source (created earlier) containing 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 enforcement policy created earlier is configured for the service.

HPE Aruba Networking access switch

In addition to the secure onboarding configuration described in , see the below example port configuration for the HPE Aruba Networking access switch to allow for 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

2025-11 (M7.2)