

## HPE Aruba Networking

## Guía de integración

## Índice

---

<b>Introducción</b> .....	3
<b>Incorporación segura: IEEE 802.1AR/802.1X</b> .....	4
Autenticación inicial .....	4
Aprovisionamiento .....	4
Red de producción .....	4
Configuración de HPE Aruba Networking .....	5
Configuración Axis .....	17
<b>Operación de red segura: IEEE 802.1AE MACsec</b> .....	20
ClearPass Policy Manager de HPE Aruba Networking .....	21
Switch de acceso de HPE Aruba Networking .....	25
<b>Incorporación heredada: autenticación MAC</b> .....	26
ClearPass Policy Manager de HPE Aruba Networking .....	26
Switch de acceso de HPE Aruba Networking .....	34

### Introducción

Esta guía de integración tiene como objetivo describir la configuración de mejores prácticas sobre cómo integrar y operar dispositivos Axis en redes de HPE Aruba Networking. La configuración utiliza estándares y protocolos de seguridad modernos, como IEEE 802.1X, IEEE 802.1AR, IEEE 802.1AE y HTTPS.

Establecer una automatización adecuada para la integración de la red puede ahorrar tiempo y dinero. Permite eliminar la complejidad innecesaria del sistema cuando se utilizan aplicaciones de gestión de dispositivos de Axis combinadas con la infraestructura y las aplicaciones de HPE Aruba Networking. A continuación se detallan algunos de los beneficios que se pueden obtener al combinar dispositivos y software de Axis con una infraestructura de HPE Aruba Networking:

- Minimice la complejidad del sistema eliminando las redes provisionales de dispositivos.
- Ahorre costes agregando procesos de incorporación y gestión de dispositivos automatizados.
- Aproveche los controles de seguridad de red sin intervención proporcionados por los dispositivos Axis.
- Aumente la seguridad general de la red aplicando la experiencia de HPE y Axis.

La infraestructura de red debe estar preparada para verificar de forma segura la integridad de los dispositivos Axis antes de comenzar la configuración. Esto permite una transición fluida definida por software entre redes lógicas durante todo el proceso de incorporación. Es necesario tener conocimientos sobre las siguientes áreas antes de realizar la configuración:

- Gestión de infraestructuras de TI de redes empresariales de HPE Aruba Networking, incluidos los switches de acceso de HPE Aruba Networking y el gestor de políticas ClearPass de HPE Aruba Networking.
- Experiencia en técnicas modernas de control de acceso a redes y políticas de seguridad de redes.
- Es deseable tener conocimientos básicos sobre los productos de Axis, pero se proporcionan a lo largo de la guía.

### Incorporación segura: IEEE 802.1AR/802.1X



Para ver este vídeo, vaya a la versión web de este documento.

[help.axis.com/?&pid=etsection=secure-onboarding-ieee802-1ar-802-1x](http://help.axis.com/?&pid=etsection=secure-onboarding-ieee802-1ar-802-1x)

*Integración de dispositivos segura en redes de confianza cero con IEEE 802.1X/802.1AR*

## Autenticación inicial

Conecte el dispositivo Axis compatible con Axis Edge Vault para autenticar el dispositivo en la red. El dispositivo utiliza el certificado de identificación del dispositivo IEEE 802.1AR Axis a través del control de acceso a la red IEEE 802.1X para autenticarse.

Para otorgar acceso a la red, ClearPass Policy Manager verifica el ID del dispositivo Axis junto con otras huellas digitales específicas del dispositivo. La información, como la dirección MAC y el AXIS OS en ejecución, se utiliza para tomar una decisión basada en políticas.

El dispositivo Axis se autentica en la red utilizando el certificado de ID de dispositivo Axis compatible con IEEE 802.1AR.

*El dispositivo Axis se autentica en la red de HPE Aruba Networking utilizando el certificado de ID de dispositivo Axis compatible con IEEE 802.1AR.*

- 1 ID de dispositivo de AXIS
- 2 Autenticación de red IEEE 802.1x EAP-TLS
- 3 Interruptor de acceso (autenticador)
- 4 ClearPass Policy Manager

## Aprovisionamiento

Después de la autenticación, el dispositivo Axis se traslada a la red de aprovisionamiento (VLAN201) en la que está instalado AXIS Device Manager. A través de AXIS Device Manager se pueden realizar la configuración del dispositivo, el refuerzo de la seguridad y las actualizaciones de AXIS OS. Para completar el aprovisionamiento del dispositivo, se cargan en el dispositivo nuevos certificados de producción específicos del cliente para IEEE 802.1X y HTTPS.

*Después de una autenticación exitosa, el dispositivo Axis pasa a una red de aprovisionamiento para su configuración.*

- 1 Switch de acceso
- 2 Red de aprovisionamiento
- 3 ClearPass Policy Manager
- 4 Aplicación de gestión de dispositivos

### Red de producción

El aprovisionamiento del dispositivo Axis con nuevos certificados IEEE 802.1X activa un nuevo intento de autenticación. ClearPass Policy Manager verifica los nuevos certificados y decide si mueve el dispositivo Axis a la red de producción o no.

*Después de la configuración del dispositivo, el dispositivo Axis abandona la red de aprovisionamiento e intenta volver a autenticarse en la red.*

- 1 ID de dispositivo de AXIS
- 2 Autenticación de red IEEE 802.1x EAP-TLS
- 3 Interruptor de acceso (autenticador)
- 4 ClearPass Policy Manager

Después de la reautenticación, el dispositivo Axis se traslada a la red de producción (VLAN 202). En esa red, el sistema de gestión de vídeo (VMS) se conecta al dispositivo Axis y empieza a funcionar.

*El dispositivo Axis tiene acceso a la red de producción.*

- 1 Switch de acceso
- 2 Red de producción
- 3 ClearPass Policy Manager
- 4 Sistema de gestión de vídeo

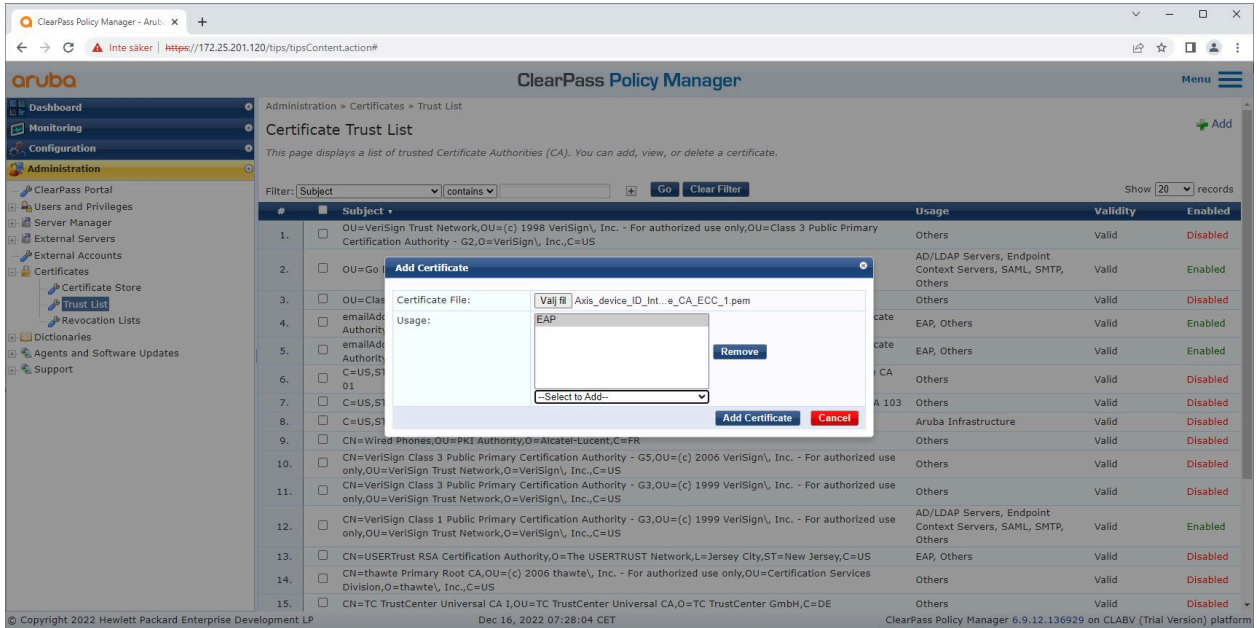
### Configuración de HPE Aruba Networking

#### ClearPass Policy Manager de HPE Aruba Networking

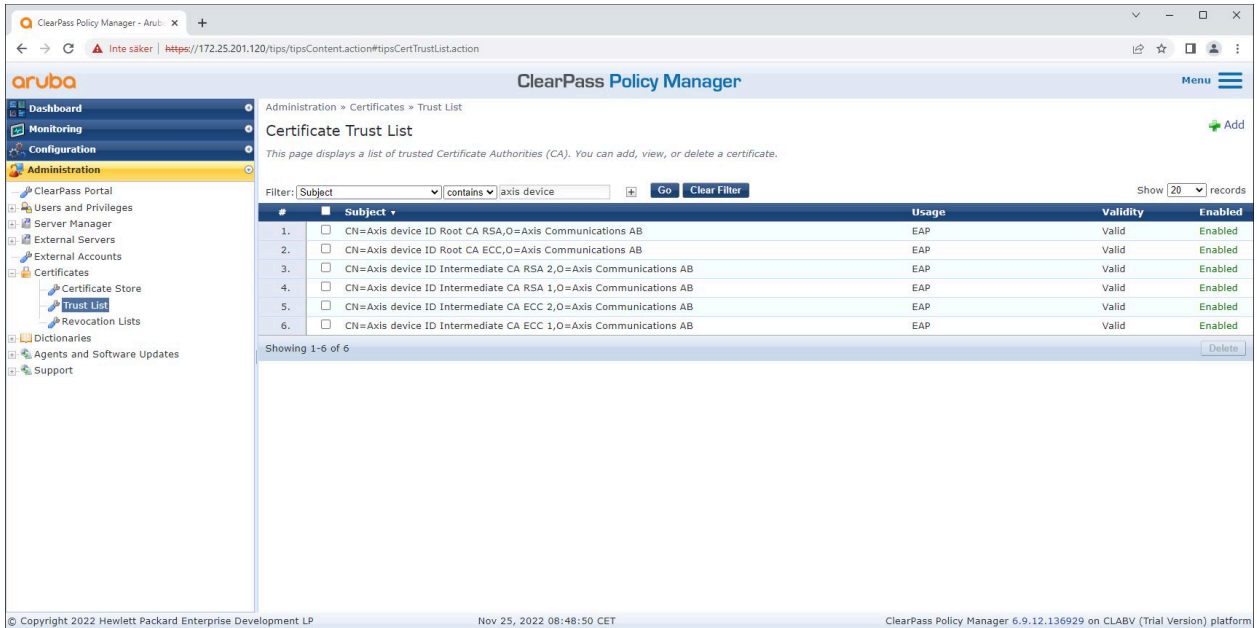
ClearPass Policy Manager proporciona control de acceso seguro a la red basado en roles y dispositivos para IoT, BYOD, dispositivos corporativos, empleados, contratistas e invitados en infraestructura cableada, inalámbrica y VPN de múltiples proveedores.

#### Configuración del almacén de certificados de confianza

1. Descargue la cadena de certificados IEEE 802.1AR específica de Axis desde [axis.com](http://axis.com).
2. Cargue las cadenas de certificados de CA raíz y CA intermedia IEEE 802.1AR específicas de Axis en el almacén de certificados de confianza.
3. Habilite ClearPass Policy Manager para autenticar dispositivos Axis a través de IEEE 802.1X EAP-TLS.
4. Seleccione EAP en el campo de uso. Los certificados se utilizan para la autenticación IEEE 802.1X EAP-TLS.



Cargue los certificados IEEE 802.1AR específicos de Axis en el almacén de certificados confiable de ClearPass Policy Manager.



Almacén de certificados confiable en ClearPass Policy Manager con cadena de certificados IEEE 802.1AR específica de Axis incluida.

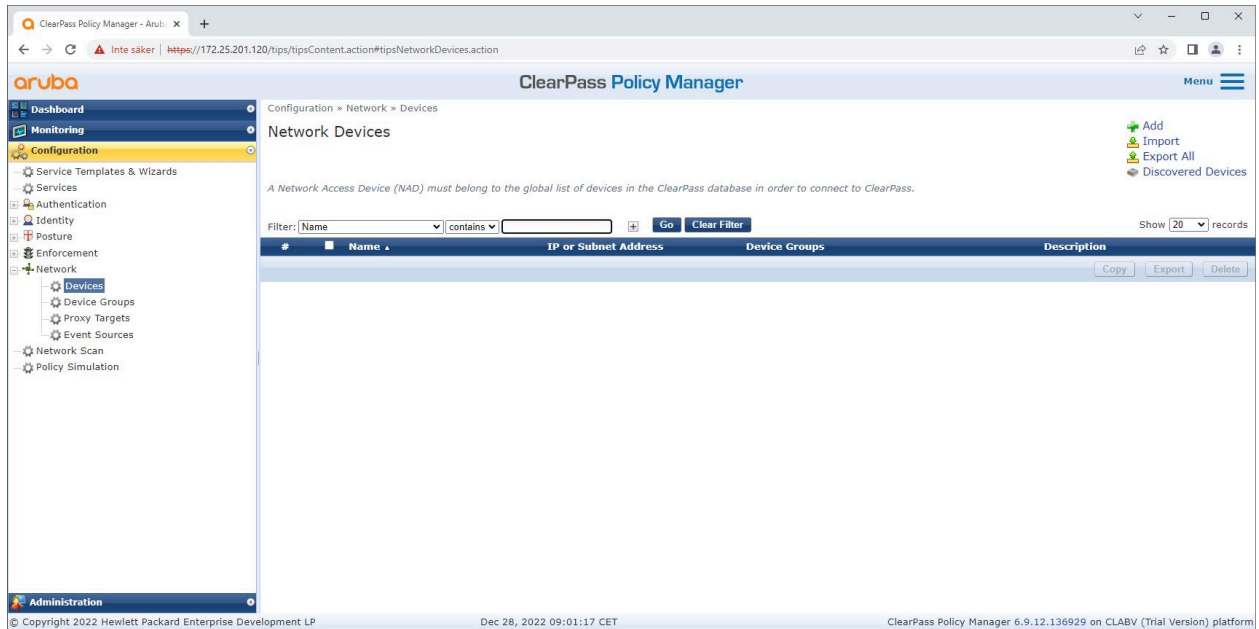
### Configuración de dispositivo/grupo de red

1. Agregue dispositivos de acceso a la red confiables, como switches de acceso de HPE Aruba Networking, al ClearPass Policy Manager. ClearPass Policy Manager necesita saber qué switches de acceso en la red se utilizan para la comunicación IEEE 802.1X.
2. Utilice la configuración del grupo de dispositivos de red para agrupar varios dispositivos de acceso a la red confiables. La agrupación de dispositivos de acceso a la red confiables permite una configuración de políticas más sencilla.

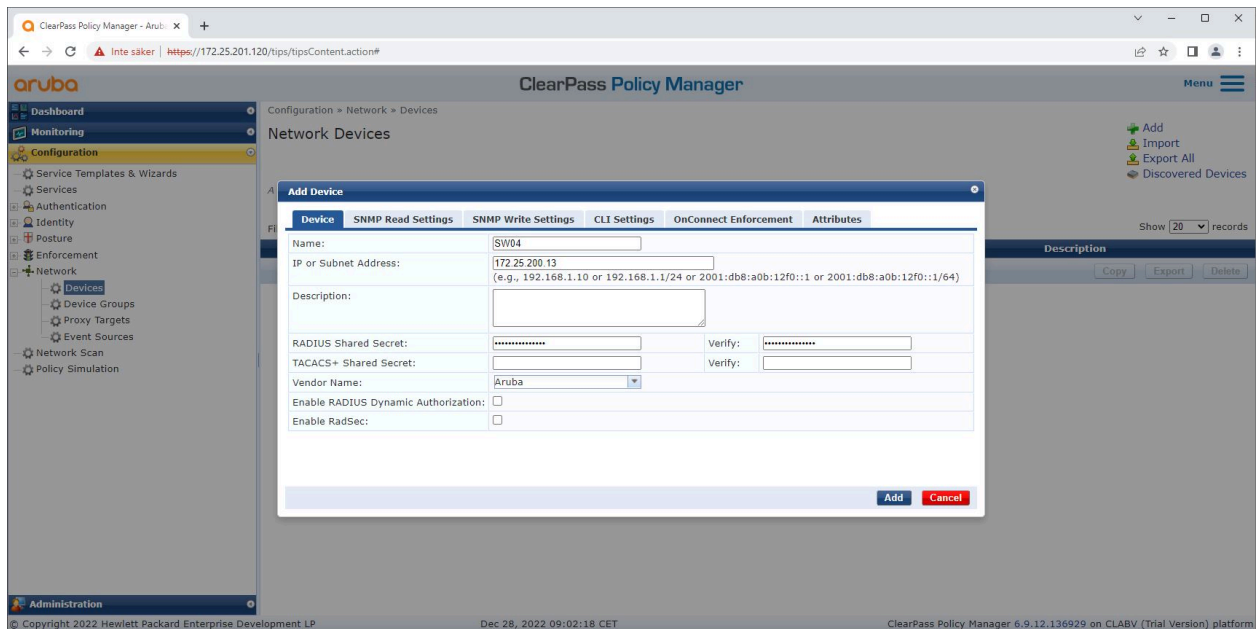
# HPE Aruba Networking

## Incorporación segura: IEEE 802.1AR/802.1X

3. El secreto compartido de RADIUS debe coincidir con la configuración específica del conmutador IEEE 802.1X.



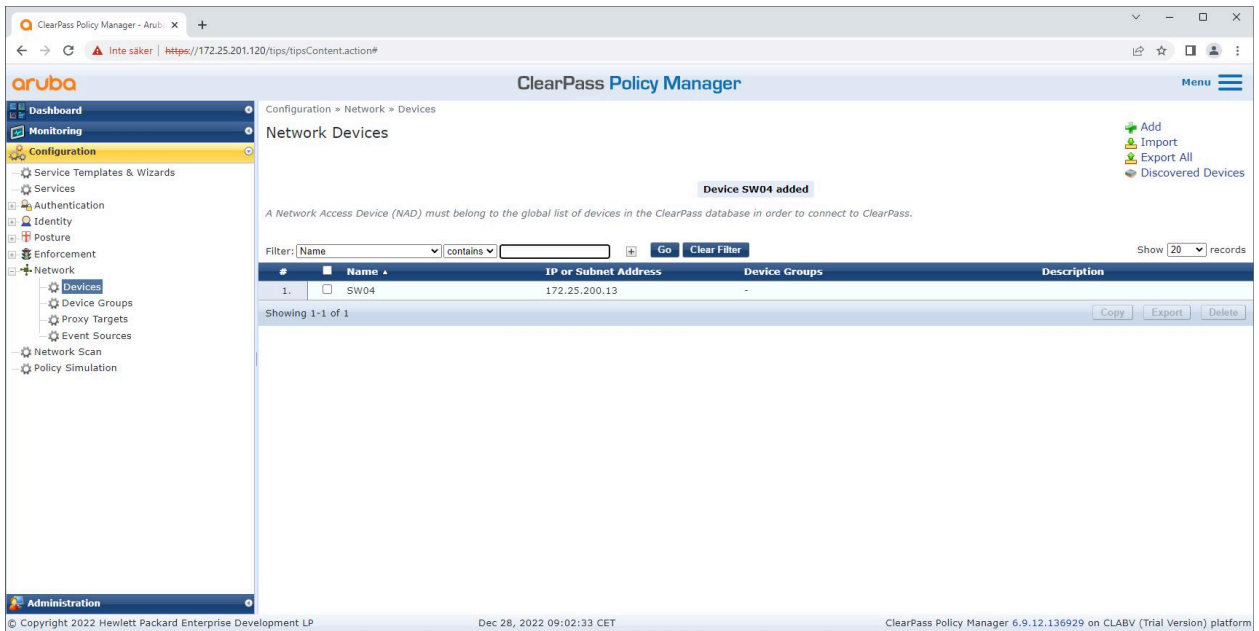
*La interfaz de dispositivos de red confiables en ClearPass Policy Manager.*



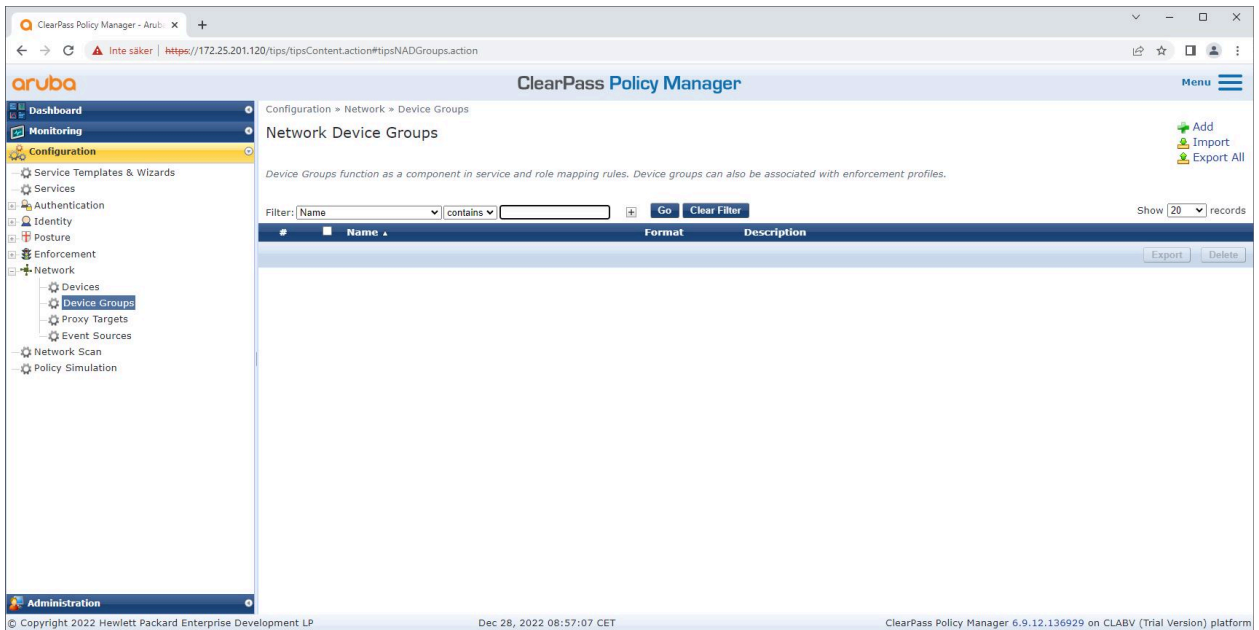
*Agregar el conmutador de acceso de HPE Aruba Networking como dispositivo de red confiable en ClearPass Policy Manager. Tenga en cuenta que el secreto compartido de RADIUS debe coincidir con la configuración específica del switch IEEE 802.1X.*

# HPE Aruba Networking

## Incorporación segura: IEEE 802.1AR/802.1X



*ClearPass Policy Manager con un dispositivo de red confiable configurado.*

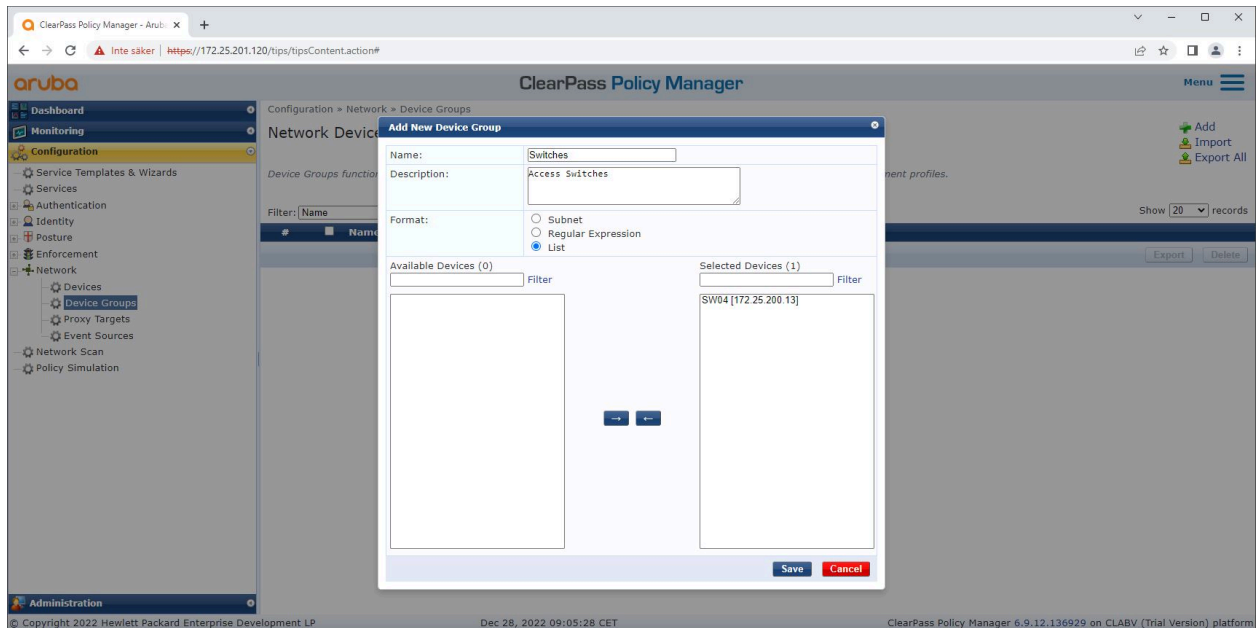


*La interfaz de grupos de dispositivos de red confiables en ClearPass Policy Manager.*

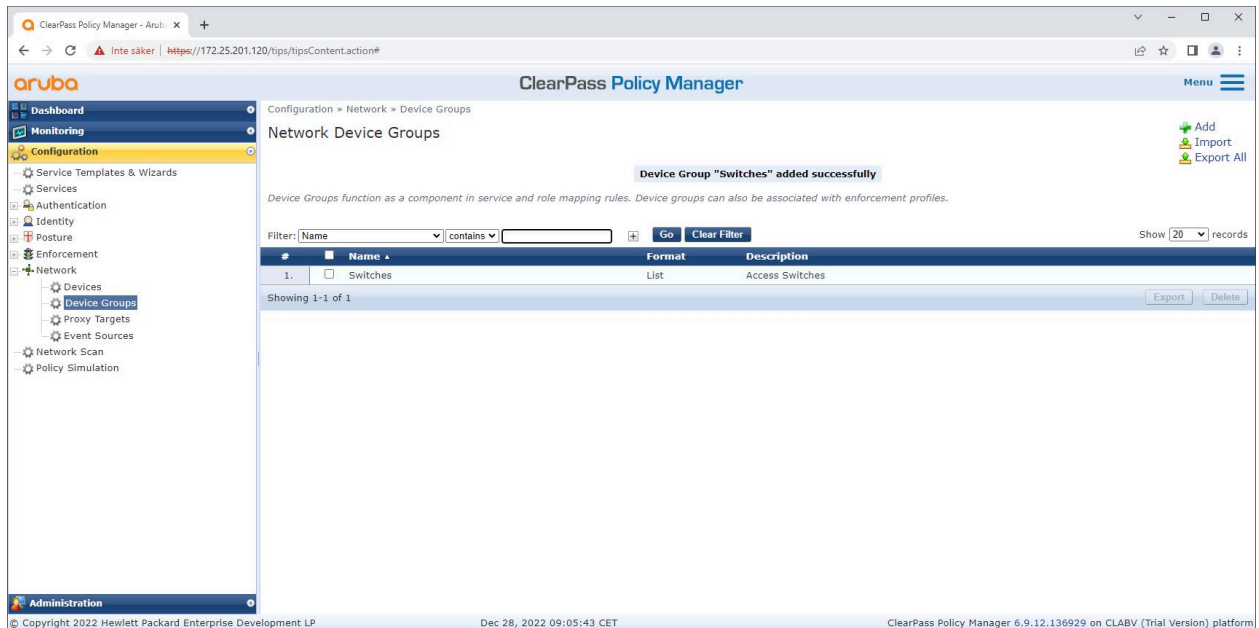


# HPE Aruba Networking

## Incorporación segura: IEEE 802.1AR/802.1X



*Agregue un dispositivo de acceso a la red confiable a un nuevo grupo de dispositivos en ClearPass Policy Manager.*



*ClearPass Policy Manager con un grupo de dispositivos de red configurado que incluye uno o varios dispositivos de red confiables.*

### Configuración de huellas digitales del dispositivo

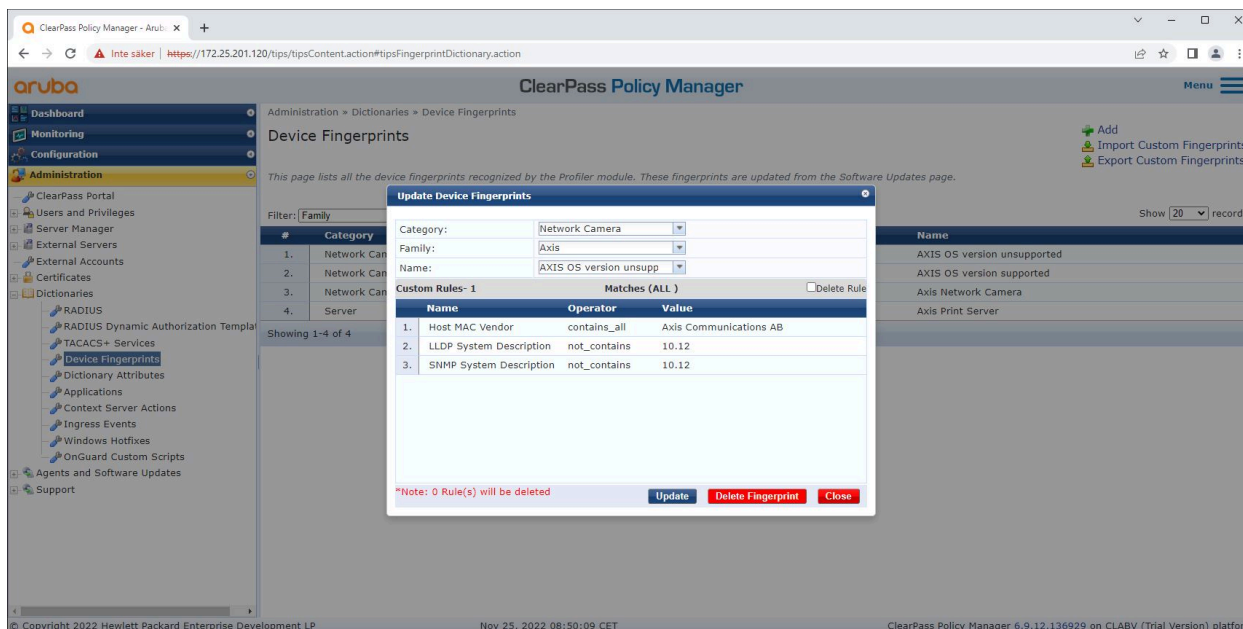
El dispositivo Axis puede distribuir información específica del dispositivo, como la dirección MAC y la versión del software, a través de la detección de red. Use esta información para crear, actualizar o gestionar huellas de dispositivo en ClearPass Policy Manager. También puede conceder o denegar el acceso en función de la versión de AXIS OS.

1. Vaya a **Administration > Dictionaries > Device Fingerprints (Administración > Diccionarios > Huellas digitales del dispositivo)**.

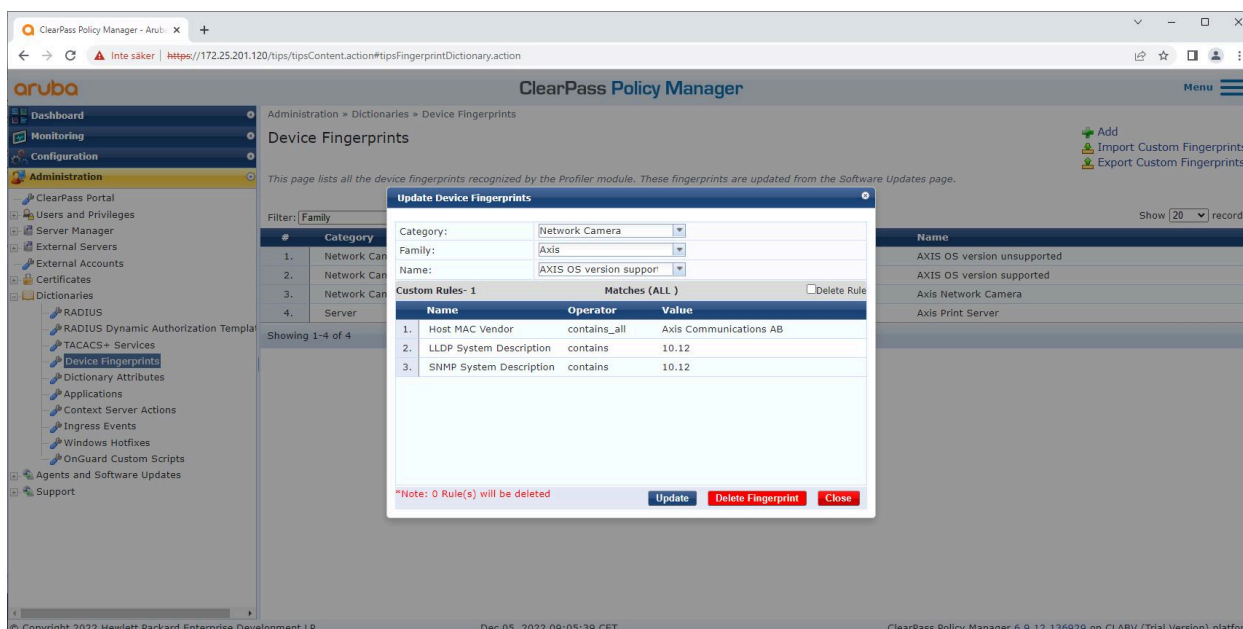
# HPE Aruba Networking

## Incorporación segura: IEEE 802.1AR/802.1X

2. Seleccione una huella digital de dispositivo existente o cree una nueva huella digital de dispositivo.
3. Establezca la configuración de huellas digitales del dispositivo.



La configuración de huellas digitales del dispositivo en ClearPass Policy Manager. Los dispositivos Axis que ejecutan una versión de AXIS OS que no sea la 10.12 se consideran no compatibles.



La configuración de huellas digitales del dispositivo en ClearPass Policy Manager. Los dispositivos Axis que ejecutan AXIS OS 10.12 se consideran compatibles en el ejemplo anterior.

La información sobre la huella digital del dispositivo recopilada por ClearPass Policy Manager se puede encontrar en la sección Puntos finales.

# HPE Aruba Networking

## Incorporación segura: IEEE 802.1AR/802.1X

1. Vaya a **Configuration > Identity > Endpoints** (Configuración > Identidad > Puntos finales).
2. Seleccione el dispositivo que desee ver.
3. Haga clic en la pestaña **Device Fingerprints** (Huellas digitales del dispositivo).

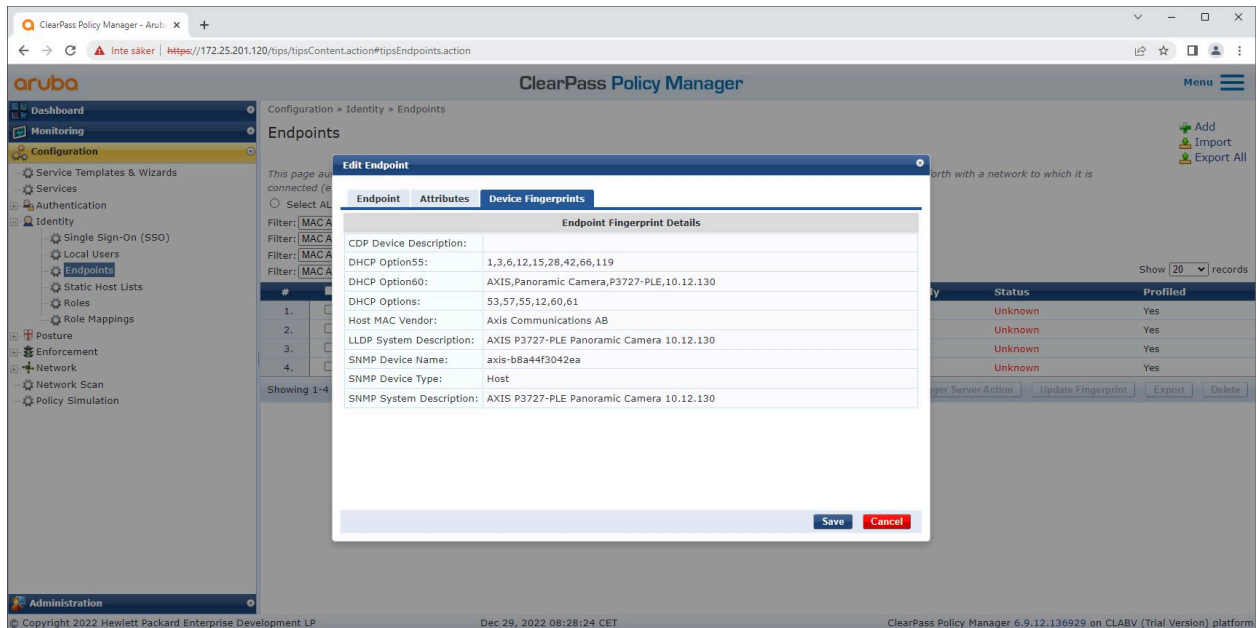
### Nota

SNMP está deshabilitado de forma predeterminada en los dispositivos Axis y se recopila desde el switch de acceso de HPE Aruba Networking.

The screenshot displays the ClearPass Policy Manager web interface. The main navigation menu on the left includes Dashboard, Monitoring, Configuration, Identity, Posture, Enforcement, Network, and Administration. The 'Configuration > Identity > Endpoints' path is active. A modal window titled 'Edit Endpoint' is open, showing details for a device with MAC Address B8-A4-4F-30-42-EA. The 'Device Fingerprints' tab is selected, showing fields for IP Address (172.25.201.233), Static IP (FALSE), Hostname (axis-b8a44f3042ea), Device Category (Network Camera), Device OS Family (Axis), Device Name (AXIS OS version support), Added At (Dec 28, 2022 14:50:45 CET), Profiled by (Policy Manager), Last Profiled At (Dec 29, 2022 08:18:23 CET), Online Status (Not Available), and Connection Type (Unknown). The status is set to 'Unknown client'. A table in the background shows a list of endpoints with columns for #, Status, and Profiled.

#	Status	Profiled
1.	Unknown	Yes
2.	Unknown	Yes
3.	Unknown	Yes
4.	Unknown	Yes

*Un dispositivo Axis con perfil de ClearPass Policy Manager.*

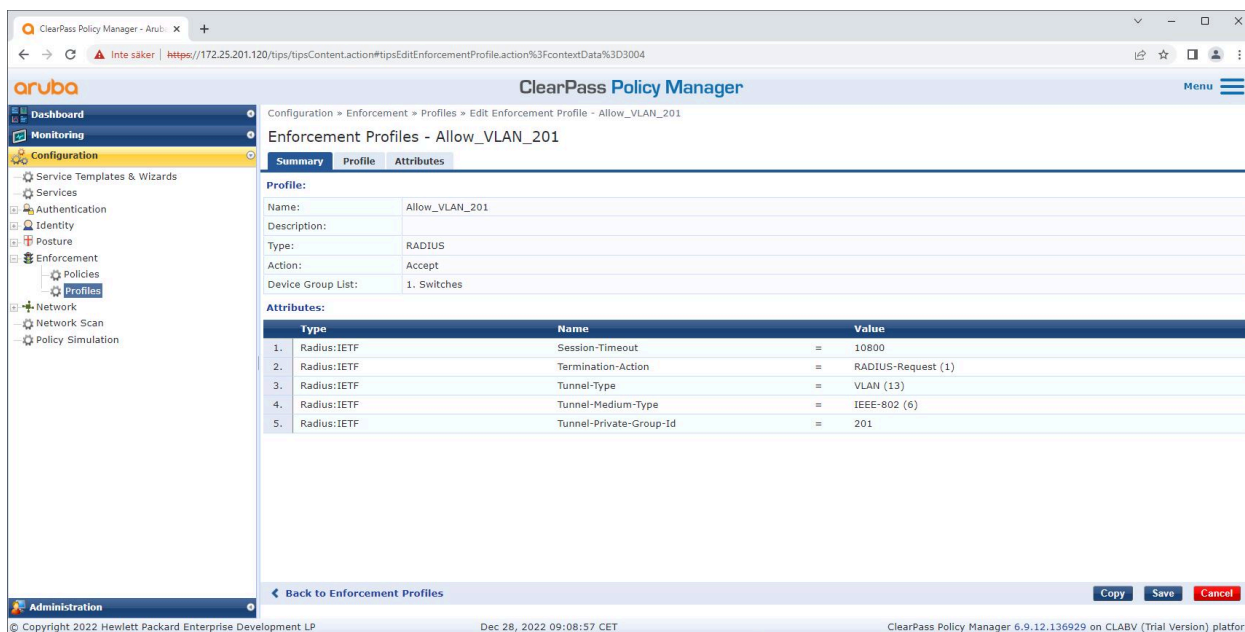


Las huellas dactilares detalladas del dispositivo de un dispositivo Axis perfilado. Tenga en cuenta que SNMP está deshabilitado de forma predeterminada en los dispositivos Axis. La información de detección específica de LLDP, CDP y DHCP es compartida por el dispositivo Axis en el estado predeterminado de fábrica y transmitida por el conmutador de acceso de HPE Aruba Networking a ClearPass Policy Manager.

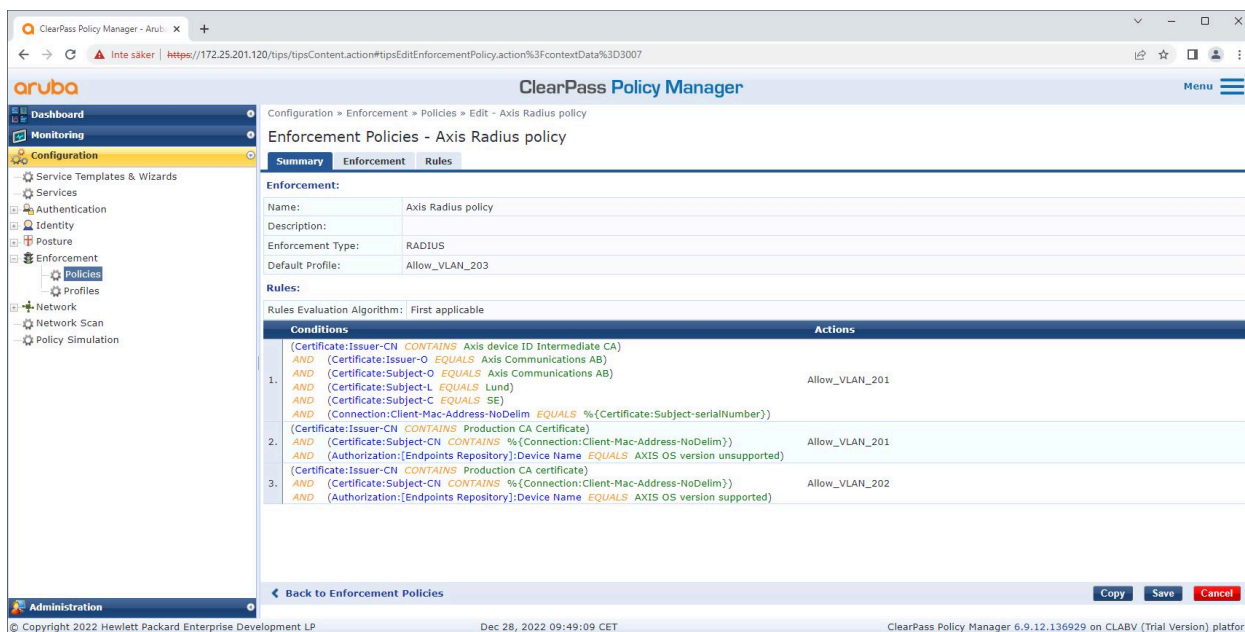
### Configuración del perfil de cumplimiento

Un **Enforcement Profile (Perfil de cumplimiento)** se utiliza para permitir que ClearPass Policy Manager asigne una ID de VLAN específica a un puerto de acceso en el switch. Es una decisión basada en políticas que se aplica a los dispositivos de red en el grupo de dispositivos "switches". La cantidad necesaria de perfiles de cumplimiento depende de la cantidad de VLAN que se utilizan. En nuestra configuración hay un total de tres VLAN (VLAN 201, 202, 203), que se correlacionan con tres perfiles de cumplimiento.

Una vez configurados los perfiles de cumplimiento para la VLAN, se puede configurar la política de cumplimiento real. La configuración de la política de cumplimiento en ClearPass Policy Manager define si los dispositivos Axis tienen acceso a las redes de HPE Aruba Networking según cuatro perfiles de políticas de ejemplo.



Un ejemplo de perfil de cumplimiento para permitir el acceso a la VLAN 201.



La configuración de la política de cumplimiento en ClearPass Policy Manager.

Las cuatro políticas de cumplimiento y sus acciones se enumeran a continuación:

**Acceso denegado a la red**

Se deniega el acceso a la red cuando no se realiza la autenticación de control de acceso a la red IEEE 802.1X.

**Red de invitados (VLAN 203)**

## Incorporación segura: IEEE 802.1AR/802.1X

---

Al dispositivo Axis se le concede acceso a una red limitada y aislada si falla la autenticación de control de acceso a la red IEEE 802.1X. Es necesaria una inspección manual del dispositivo para tomar las medidas adecuadas.

### Red de aprovisionamiento (VLAN 201)

El dispositivo Axis tiene acceso a una red de aprovisionamiento. Esto es para proporcionar capacidades de administración de dispositivos de Axis a través de *AXIS Device Manager* y *AXIS Device Manager Extend*. También permite configurar dispositivos Axis con actualizaciones de AXIS OS, certificados de nivel de producción y otras configuraciones. ClearPass Policy Manager verifica las siguientes condiciones:

- La versión de AXIS OS del dispositivo Axis.
- La dirección MAC del dispositivo coincide con el esquema de dirección MAC de Axis específico del proveedor con el atributo de número de serie del certificado de ID del dispositivo de Axis.
- El certificado de ID del dispositivo de Axis es verificable y coincide con los atributos específicos de Axis, como emisor, organización, ubicación y país.

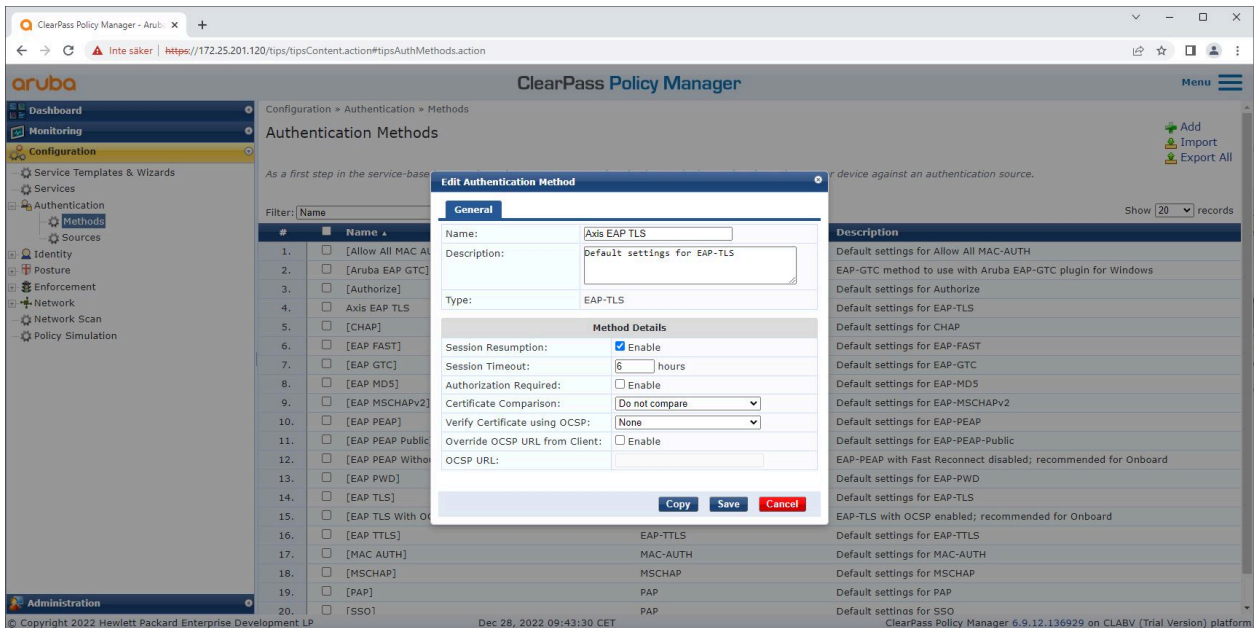
### Red de producción (VLAN 202)

El dispositivo Axis recibe acceso a la red de producción en la que debe funcionar. El acceso se concede cuando finaliza el aprovisionamiento del dispositivo desde la red de aprovisionamiento (VLAN 201). ClearPass Policy Manager verifica las siguientes condiciones:

- La dirección MAC del dispositivo coincide con el esquema de dirección MAC de Axis específico del proveedor con el atributo de número de serie del certificado de ID del dispositivo de Axis.
- La versión de AXIS OS del dispositivo Axis.
- El certificado de grado de producción es verificable por el almacén de certificados de confianza.

### Configuración del método de autenticación

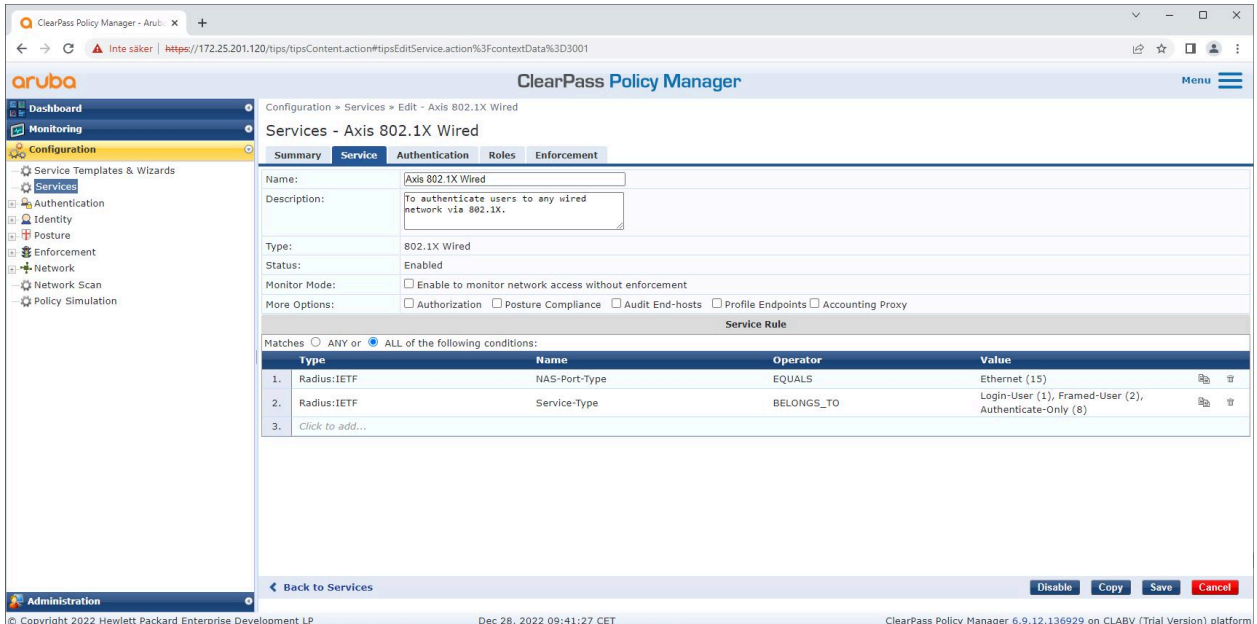
En el método de autenticación se define cómo un dispositivo Axis intenta autenticarse en la red. El método de autenticación preferido debe ser IEEE 802.1X EAP-TLS, ya que los dispositivos Axis compatibles con Axis Edge Vault cuentan con IEEE 802.1X EAP-TLS habilitado de forma predeterminada.



La interfaz del método de autenticación de ClearPass Policy Manager donde se define el método de autenticación EAP-TLS para dispositivos Axis.

### Configuración de servicio

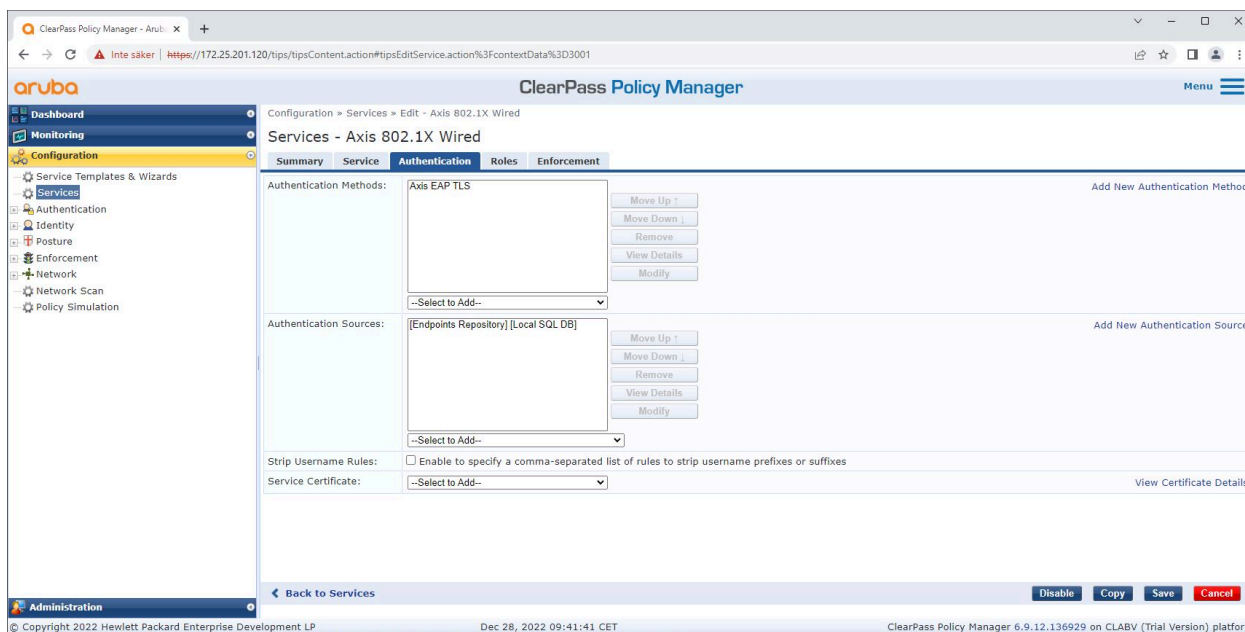
En la página Services (Servicios), los pasos de configuración se combinan en un solo servicio que maneja la autenticación y autorización de los dispositivos Axis en las redes de HPE Aruba Networking.



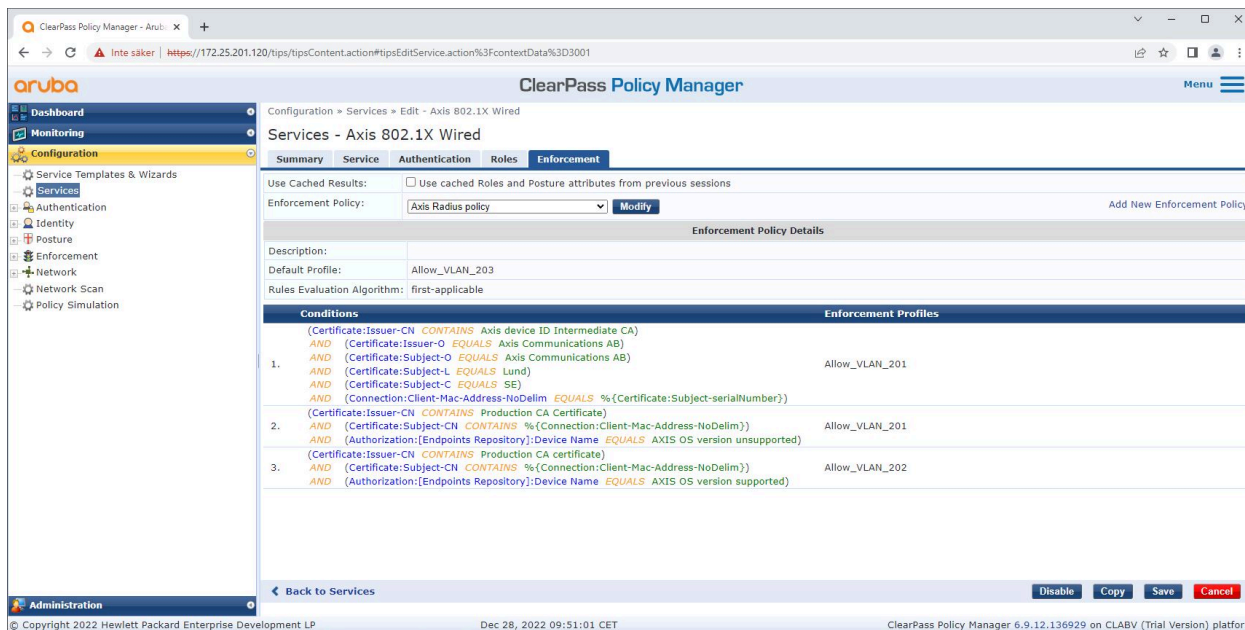
Se crea un servicio Axis dedicado que define IEEE 802.1X como método de conexión.

# HPE Aruba Networking

## Incorporación segura: IEEE 802.1AR/802.1X



En el siguiente paso, se configura para el servicio el método de autenticación EAP-TLS creado anteriormente.



En el último paso, la política de aplicación creada anteriormente se configura para el servicio.

## Switch de acceso de HPE Aruba Networking

Los dispositivos Axis se conectan directamente a switches de acceso con capacidad PoE o mediante midspans PoE de Axis compatibles. Para integrar de forma segura dispositivos Axis a las redes de HPE Aruba Networking, el switch de acceso debe configurarse para la comunicación IEEE 802.1X. El dispositivo Axis transmite la comunicación IEEE 802.1x EAP-TLS a ClearPass Policy Manager, que actúa como servidor RADIUS.



## Incorporación segura: IEEE 802.1AR/802.1X

### Nota

También se configura una reautenticación periódica de 300 segundos para el dispositivo Axis para aumentar la seguridad general del acceso al puerto.

Consulte el siguiente ejemplo de configuración global y de puertos para switches de acceso de HPE Aruba Networking.

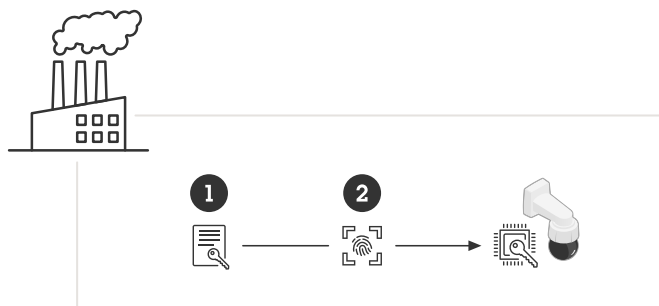
```
radius-server host MyRADIUSIPAddress key "MyRADIUSKey"

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
```

## Configuración Axis

### Dispositivo en red de Axis

Los dispositivos Axis compatibles con *Axis Edge Vault* se fabrican con una identidad de dispositivo segura, llamada ID de dispositivo de Axis. La identificación del dispositivo Axis se basa en el estándar internacional IEEE 802.1AR, que define un método para la identificación de dispositivos segura y automatizada y la incorporación de redes a través de IEEE 802.1X.



*Los dispositivos Axis se fabrican con el certificado de identificación de dispositivo Axis compatible con IEEE 802.1AR para servicios de identidad de dispositivos confiables.*

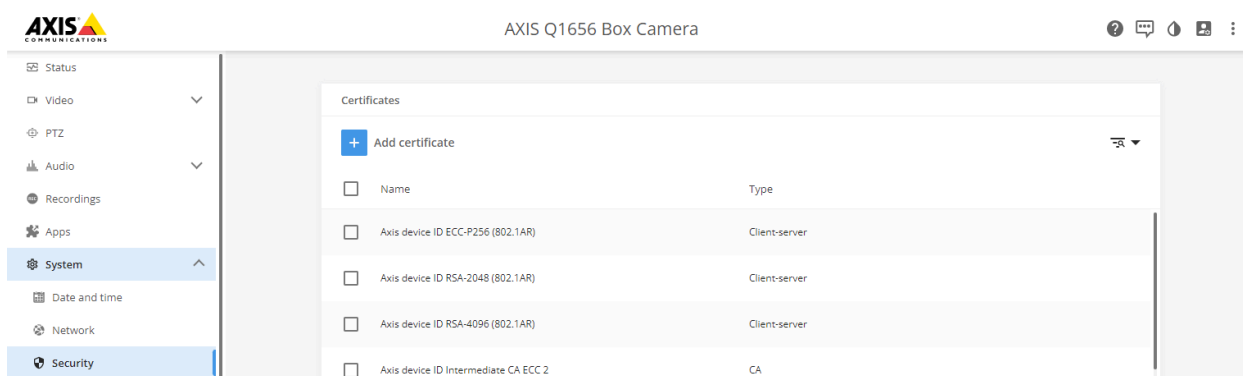
- 1 *Infraestructura de claves de identificación de dispositivos (PKI) de Axis*
- 2 *ID de dispositivo de AXIS*

El almacén de claves seguro protegido por hardware proporcionado por un elemento seguro del dispositivo Axis se suministra de fábrica con un certificado exclusivo del dispositivo y las claves correspondientes (ID del dispositivo Axis) que pueden probar globalmente la autenticidad del dispositivo Axis. *Axis Product Selector* se puede utilizar para saber qué dispositivos Axis son compatibles con *Axis Edge Vault* y el ID de dispositivo Axis.

### Nota

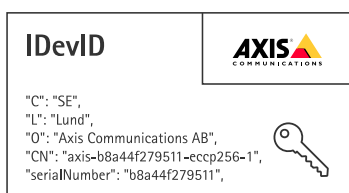
El número de serie de un dispositivo Axis es su dirección MAC.

## Incorporación segura: IEEE 802.1AR/802.1X



El almacén de certificados del dispositivo Axis en el estado predeterminado de fábrica con el ID del dispositivo Axis.

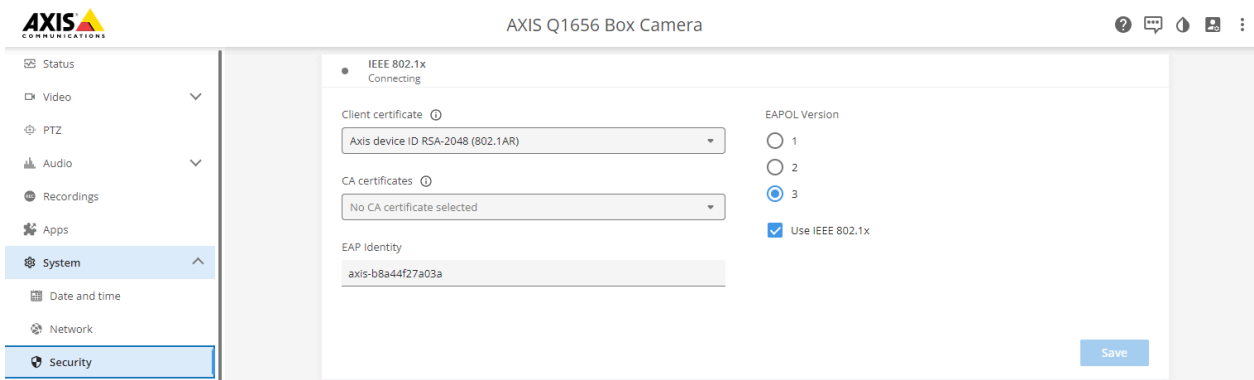
El certificado de identificación del dispositivo Axis compatible con IEEE 802.1AR incluye información sobre el número de serie y otra información específica del proveedor de Axis. La información es utilizada por ClearPass Policy Manager para análisis y toma de decisiones para otorgar acceso a la red. Consulte la siguiente información que se puede obtener de un certificado de identificación de dispositivo de Axis.



País	SE
Ubicación	Lund
Organización emisora	Axis Communications AB
Nombre común del emisor	ID del dispositivo Axis intermedio
Organización	Axis Communications AB
Nombre común	axis-b8a44f279511-eccp256-1
Número de serie	b8a44f279511

El nombre común se construye mediante una combinación del nombre de la empresa Axis, el número de serie del dispositivo seguido del algoritmo criptográfico (ECC P256, RSA 2048, RSA 4096) utilizado. Desde AXIS OS 10.1 (2020-09), IEEE 802.1X está habilitado de forma predeterminada con el ID del dispositivo Axis preconfigurado. Esto permite que el dispositivo Axis se autentique en redes habilitadas para IEEE 802.1X.

## Incorporación segura: IEEE 802.1AR/802.1X



*Dispositivo Axis en el estado predeterminado de fábrica con IEEE 802.1X habilitado y el certificado de ID de dispositivo Axis preseleccionado.*

### AXIS Device Manager

AXIS Device Manager y AXIS Device Manager Extend se pueden utilizar en la red para configurar y gestionar varios dispositivos Axis de forma rentable. AXIS Device Manager es una aplicación basada en Microsoft Windows® que se puede instalar localmente en una máquina de la red, mientras que AXIS Device Manager Extend se basa en la infraestructura en la nube para realizar la gestión de dispositivos en múltiples instalaciones. Ambos ofrecen capacidades sencillas de administración y configuración para dispositivos Axis como:

- Instalación de actualizaciones de AXIS SO.
- Aplicar configuración de ciberseguridad como certificados HTTPS e IEEE 802.1X.
- Configuración de ajustes específicos del dispositivo, como ajustes de imágenes y otros.

### Operación de red segura: IEEE 802.1AE MACsec

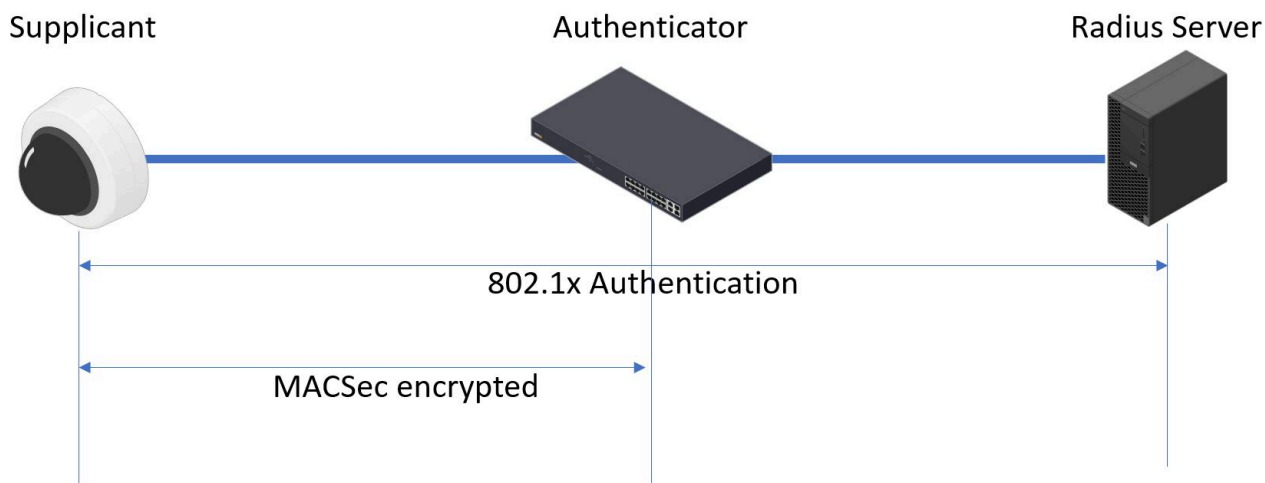


Cifrado de red de confianza cero con seguridad de capa 2 IEEE 802.1AE MACsec

IEEE 802.1AE MACsec (Media Access Control Security) es un protocolo de red bien definido que protege criptográficamente los enlaces Ethernet punto a punto en la capa de red 2. Garantiza la confidencialidad y la integridad de las transmisiones de datos entre dos hosts.

El estándar IEEE 802.1AE MACsec describe dos modos de funcionamiento:

- Modo CAK estático/clave precompartida configurable manualmente
- Sesión maestra automática/modo CAK dinámico usando IEEE 802.1X EAP-TLS



En AXIS OS 10.1 (2020-09) y posteriores, IEEE 802.1X está habilitado de forma predeterminada para dispositivos que son compatibles con el ID de dispositivo de Axis. In AXIS OS 11.8 y posteriores, admitimos MACsec con modo dinámico automático usando IEEE 802.1X EAP-TLS habilitado de forma predeterminada. Cuando conecta un dispositivo Axis con los valores predeterminados de fábrica, se realiza la autenticación de la red IEEE 802.1X y si tiene éxito, también se prueba el modo MACsec Dynamic CAK.

El ID del dispositivo Axis almacenado de forma segura (1), una identidad de dispositivo segura compatible con IEEE 802.1AR, se utiliza para autenticarse en la red (4, 5) a través de Control de acceso a la red basado en puertos IEEE 802.1X EAP-TLS (2). A través de la sesión EAP-TLS, las claves MACsec se intercambian automáticamente para configurar un enlace seguro (3), protegiendo todo el tráfico de red desde el dispositivo Axis hasta el switch de acceso de HPE Aruba Networking.

# HPE Aruba Networking

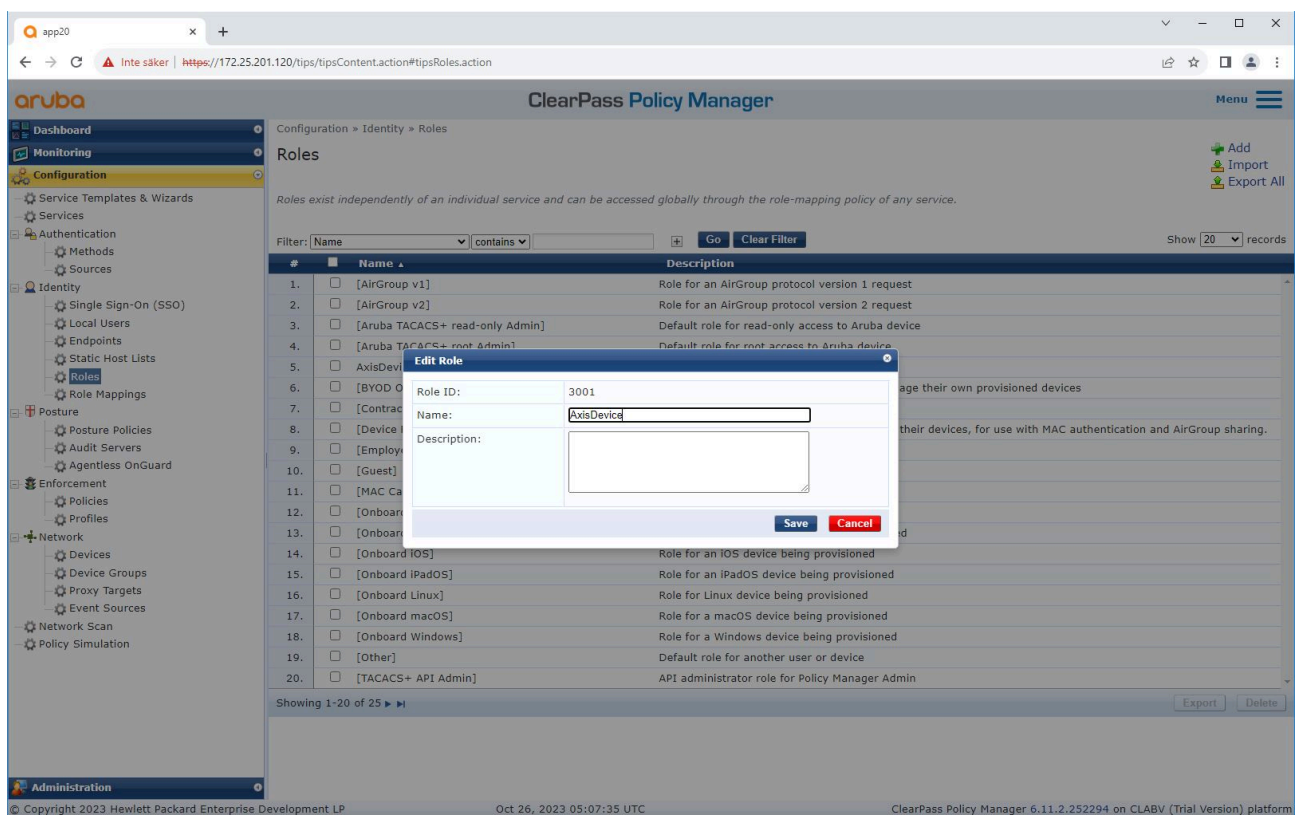
## Operación de red segura: IEEE 802.1AE MACsec

IEEE 802.1AE MACsec requiere preparar la configuración del switch de acceso de HPE Aruba Networking y de ClearPass Policy Manager. No se requiere ninguna configuración en el dispositivo Axis para permitir la comunicación cifrada con IEEE 802.1AE MACsec a través de EAP-TLS.

Si el switch de acceso de HPE Aruba Networking no admite MACsec mediante EAP-TLS, se puede utilizar y configurar manualmente el modo de clave precompartida.

## ClearPass Policy Manager de HPE Aruba Networking

### Política de asignación de roles y roles



The screenshot displays the ClearPass Policy Manager web interface. The main content area shows the 'Roles' configuration page. A table lists various roles, including [AirGroup v1], [AirGroup v2], [Aruba TACACS+ read-only Admin], [Aruba TACACS+ not Admin], [AxisDevice], [BYOD O], [Contract], [Device], [Employ], [Guest], [MAC Ca], [Onboard], [Onboard iOS], [Onboard iPadOS], [Onboard Linux], [Onboard macOS], [Onboard Windows], [Other], and [TACACS+ API Admin]. An 'Edit Role' dialog box is open over the [AxisDevice] role, showing the following fields: Role ID: 3001, Name: AxisDevice, and Description: (empty). The dialog box has 'Save' and 'Cancel' buttons. The background interface includes a navigation menu on the left, a top navigation bar with 'ClearPass Policy Manager' and 'Menu', and a footer with copyright information and the version number 'ClearPass Policy Manager 6.11.2.252294 on CLABV (Trial Version) platform'.

*Agregue un nombre de función para los dispositivos Axis. El nombre es el nombre de la función de acceso al puerto en la configuración del switch de acceso.*

# HPE Aruba Networking

## Operación de red segura: IEEE 802.1AE MACsec

The screenshot displays the ClearPass Policy Manager web interface. The left sidebar shows the navigation menu with categories like Dashboard, Monitoring, Configuration, and Administration. The main content area is titled "Role Mappings - Axis Role Mapping" and shows the configuration for a policy named "Axis Role Mapping". The policy details include a description, a default role of "[Guest]", and a rules evaluation algorithm of "Evaluate all". A table lists the mapping rules with conditions and role names.

Conditions	Role Name
1. (Authentication:Full-Username <i>BEGINS_WITH</i> axis-00408c)	AxisDevice
2. (Authentication:Full-Username <i>BEGINS_WITH</i> axis-acc89e)	AxisDevice
3. (Authentication:Full-Username <i>BEGINS_WITH</i> axis-b8a44f)	AxisDevice

*Agregue una política de asignación de roles de Axis para el rol de dispositivo de Axis creado anteriormente. Las condiciones definidas son necesarias para que un dispositivo se asigne a la función de dispositivo de Axis. Si no se cumplen las condiciones, el dispositivo forma parte del rol [Invitado].*

De forma predeterminada, los dispositivos Axis utilizan el formato de identidad EAP "número de serie de Axis". El número de serie de un dispositivo Axis es su dirección MAC. Por ejemplo "axis-b8a44f45b4e6".

### Configuración de servicio

The screenshot displays the Aruba ClearPass Policy Manager web interface. The left sidebar shows the navigation menu with categories like Dashboard, Monitoring, Configuration, and Administration. The main content area is titled 'Services - Axis 802.1X Wired' and has tabs for Summary, Service, Authentication, Roles, and Enforcement. The 'Roles' tab is active, showing a 'Role Mapping Policy' dropdown set to 'Axis Role Mapping'. Below this, the 'Role Mapping Policy Details' section includes fields for Description, Default Role (set to '[Guest]'), and Rules Evaluation Algorithm (set to 'evaluate-all'). A table lists three conditions for role assignment, all resulting in the 'AxisDevice' role:

Conditions	Role
1. (Authentication:Full-Username BEGINS_WITH axis-00408c)	AxisDevice
2. (Authentication:Full-Username BEGINS_WITH axis-acc08e)	AxisDevice
3. (Authentication:Full-Username BEGINS_WITH axis-b8a44f)	AxisDevice

At the bottom of the interface, there are buttons for 'Disable', 'Copy', 'Save', and 'Cancel', along with a 'Back to Services' link. The footer contains copyright information for Hewlett Packard Enterprise Development LP and the version number 'ClearPass Policy Manager 6.11.2.252294 on CLABV (Trial Version) platform'.

*Agregue la política de asignación de roles de Axis creada anteriormente al servicio que define IEEE 802.1X como método de conexión para la integración de dispositivos Axis.*

# HPE Aruba Networking

## Operación de red segura: IEEE 802.1AE MACsec

The screenshot displays the ClearPass Policy Manager interface. The left sidebar shows the navigation menu with categories like Dashboard, Monitoring, Configuration, Identity, Posture, Enforcement, Network, and Administration. The main content area is titled 'Services - Axis 802.1X Wired' and is currently on the 'Enforcement' tab. It shows the configuration for an enforcement policy named 'Axis Radius policy'. The 'Use Cached Results' checkbox is unchecked. The 'Enforcement Policy' dropdown is set to 'Axis Radius policy'. The 'Enforcement Policy Details' section shows a description, default profile 'Allow\_VLAN\_203', and rules evaluation algorithm 'evaluate-all'. A table lists three conditions and their corresponding enforcement profiles:

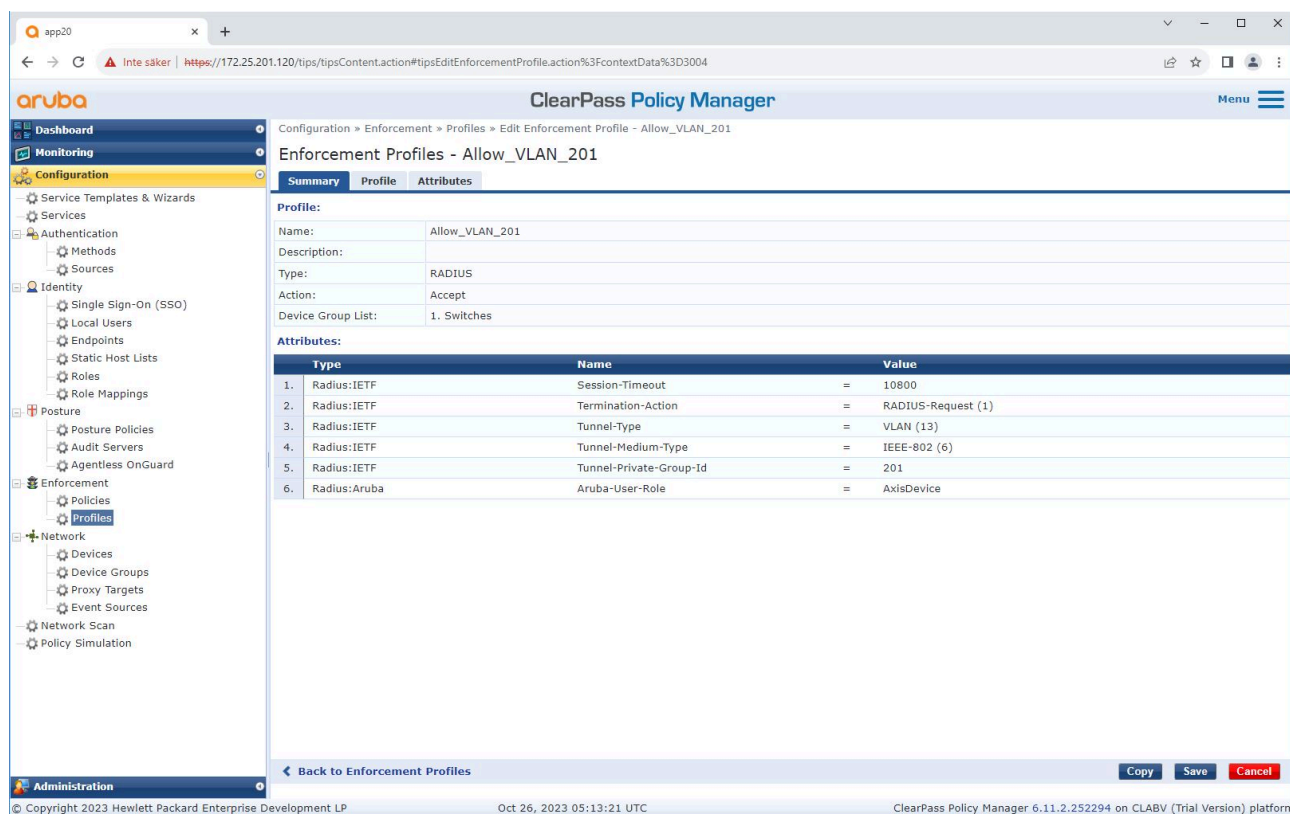
Conditions	Enforcement Profiles
1. (Certificate:Issuer-CN CONTAINS Axis device ID Intermediate CA) AND (Certificate:Issuer-O EQUALS Axis Communications AB) AND (Certificate:Subject-O EQUALS Axis Communications AB) AND (Connection:Client-Mac-Address-NoDelim EQUALS %(Certificate:Subject-serialNumber)) AND (Tips:Role EQUALS AxisDevice)	Allow_VLAN_201
2. unsupported) (Certificate:Issuer-CN CONTAINS Production CA) AND (Authorization:[Endpoints Repository]:Device Name EQUALS AXIS OS version AND (Certificate:Subject-CN CONTAINS Production XYZ) AND (Tips:Role EQUALS AxisDevice)	Allow_VLAN_201
3. supported) (Certificate:Issuer-CN CONTAINS Production CA) AND (Authorization:[Endpoints Repository]:Device Name EQUALS AXIS OS version AND (Certificate:Subject-CN CONTAINS Production XYZ) AND (Tips:Role EQUALS AxisDevice)	Allow_VLAN_202

At the bottom of the interface, there are buttons for 'Disable', 'Copy', 'Save', and 'Cancel', along with a 'Back to Services' link. The footer contains copyright information for Hewlett Packard Enterprise Development LP and the ClearPass Policy Manager version (6.11.2.252294) on the CLABV (Trial Version) platform.

*Agregue el nombre del rol de Axis como condición a las definiciones de políticas existentes.*



### Perfil de cumplimiento



Agregue el nombre de la función de Axis como atributo a los perfiles de cumplimiento asignados en el servicio de integración IEEE 802.1X.

### Switch de acceso de HPE Aruba Networking

Además de la configuración de integración segura descrita en , consulte el siguiente ejemplo de configuración de puerto para que el switch de acceso de HPE Aruba Networking 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  
mkacac-length 16  
enable
```

### Incorporación heredada: autenticación MAC

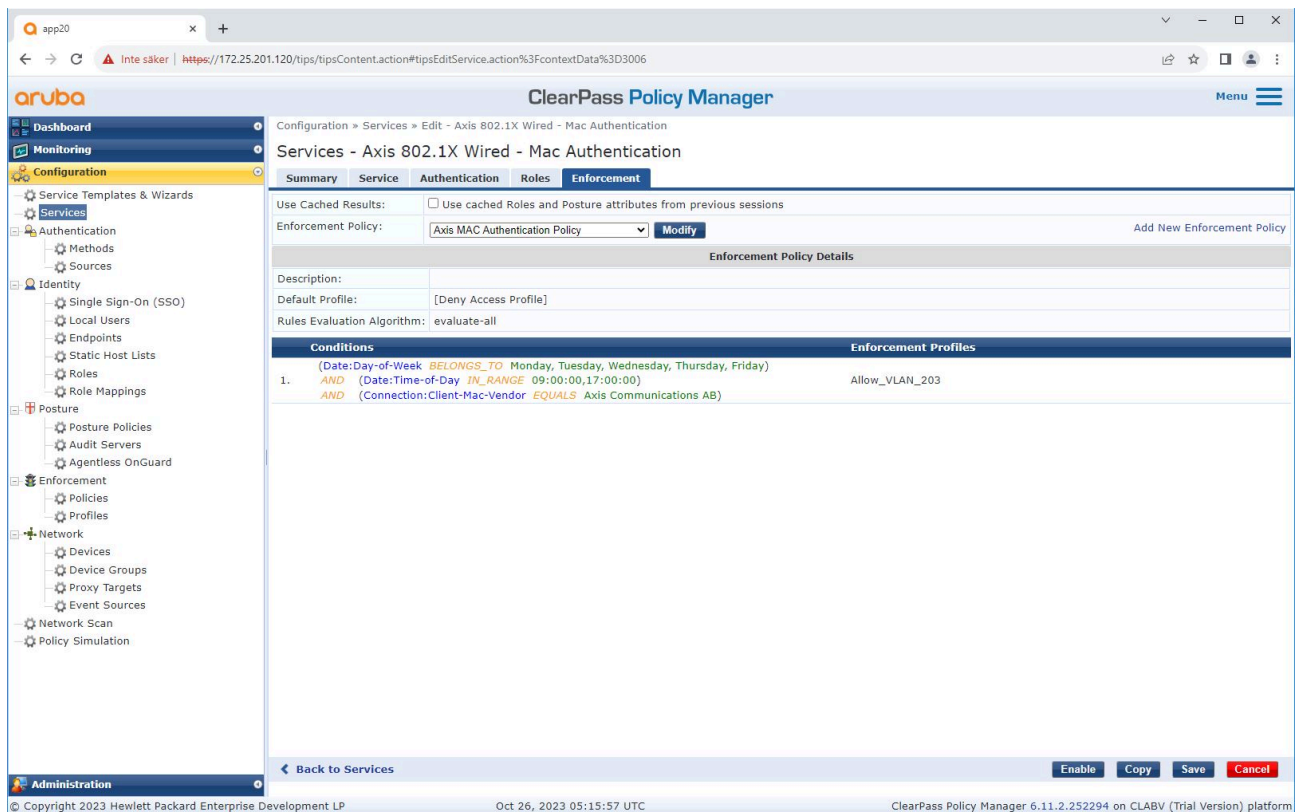
Puede utilizar MAC Authentication Bypass (MAB) para incorporar dispositivos Axis que no admitan la incorporación de IEEE 802.1AR con el certificado de identificación del dispositivo de Axis y IEEE 802.1X habilitado en el estado predeterminado de fábrica. Si falla la integración de 802.1X, ClearPass Policy Manager valida la dirección MAC del dispositivo Axis y otorga acceso a la red.

MAB requiere preparaciones de configuración del switch de acceso y de ClearPass Policy Manager. En el dispositivo Axis, no se requiere ninguna configuración para permitir la incorporación de MAB.

### ClearPass Policy Manager de HPE Aruba Networking

#### Política de cumplimiento

La configuración de la política de cumplimiento en Aruba ClearPass Policy Manager define si los dispositivos Axis tienen acceso a las redes de HPE Aruba Networking según las siguientes dos condiciones de política de ejemplo.



#### Acceso denegado a la red

Cuando el dispositivo Axis no cumple con la política de aplicación configurada, se le niega el acceso a la red.

#### Red de invitados (VLAN 203)

Al dispositivo Axis se le concede acceso a una red aislada y limitada si se cumplen las siguientes condiciones:

- Es un día laborable entre lunes y viernes.
- Es entre las 09:00 y las 17:00.

## Incorporación heredada: autenticación MAC

- El proveedor de la dirección MAC coincide con Axis Communications.

Dado que las direcciones MAC pueden falsificarse, no se concede acceso a la red de aprovisionamiento habitual. Le recomendamos que utilice MAB solo para la incorporación inicial y para inspeccionar más a fondo el dispositivo manualmente.

### Configuración de fuente

En la página Sources (Fuentes), se crea una nueva fuente de autenticación para permitir solo direcciones MAC importadas manualmente.

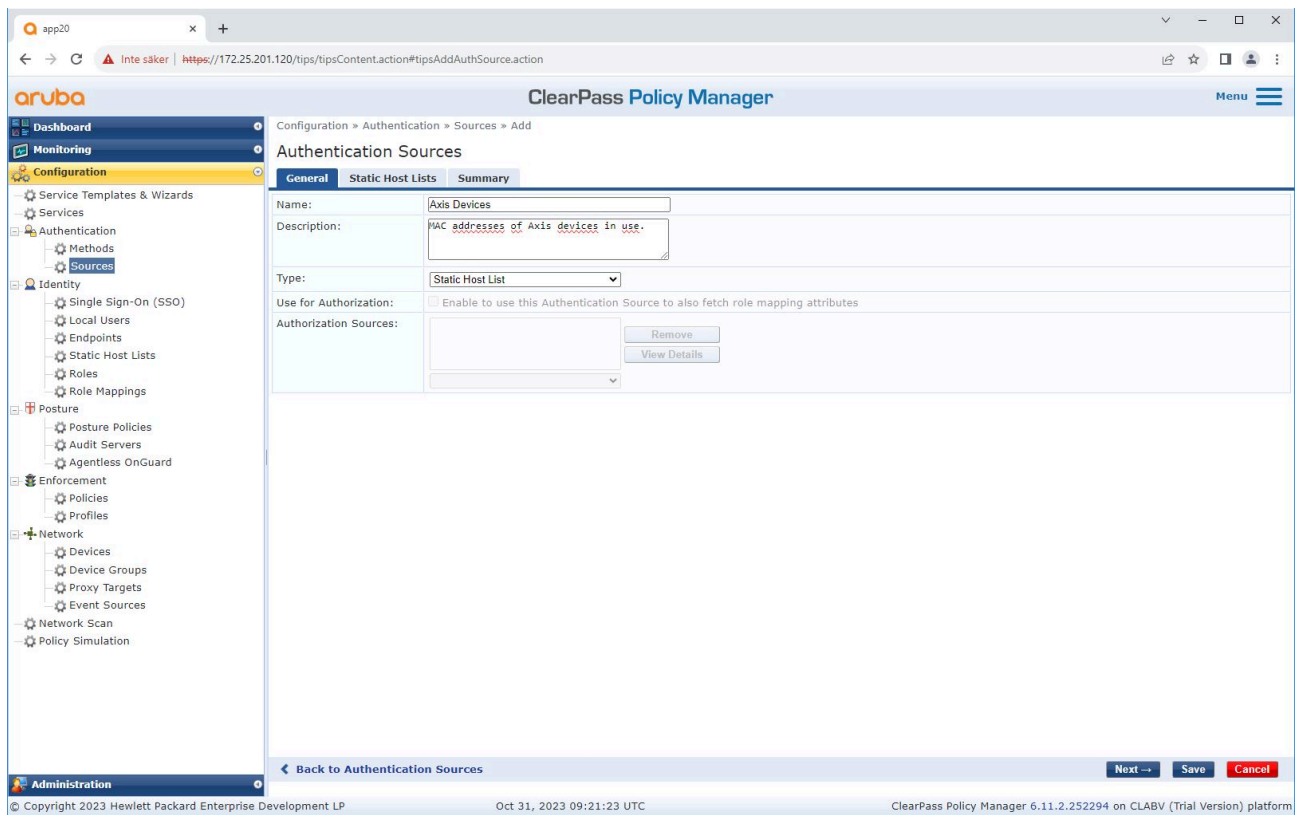
The screenshot shows the ClearPass Policy Manager web interface. The main content area is titled "Authentication Sources" and contains a table of 11 authentication sources. The table has columns for #, Name, Type, and Description. The sources listed are:

#	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

The interface also includes a navigation menu on the left, a search filter, and a table with columns for #, Name, Type, and Description. The footer contains copyright information for Hewlett Packard Enterprise Development LP, the date Oct 31, 2023 09:13:53 UTC, and the version ClearPass Policy Manager 6.11.2.252294 on CLABV (Trial Version) platform.

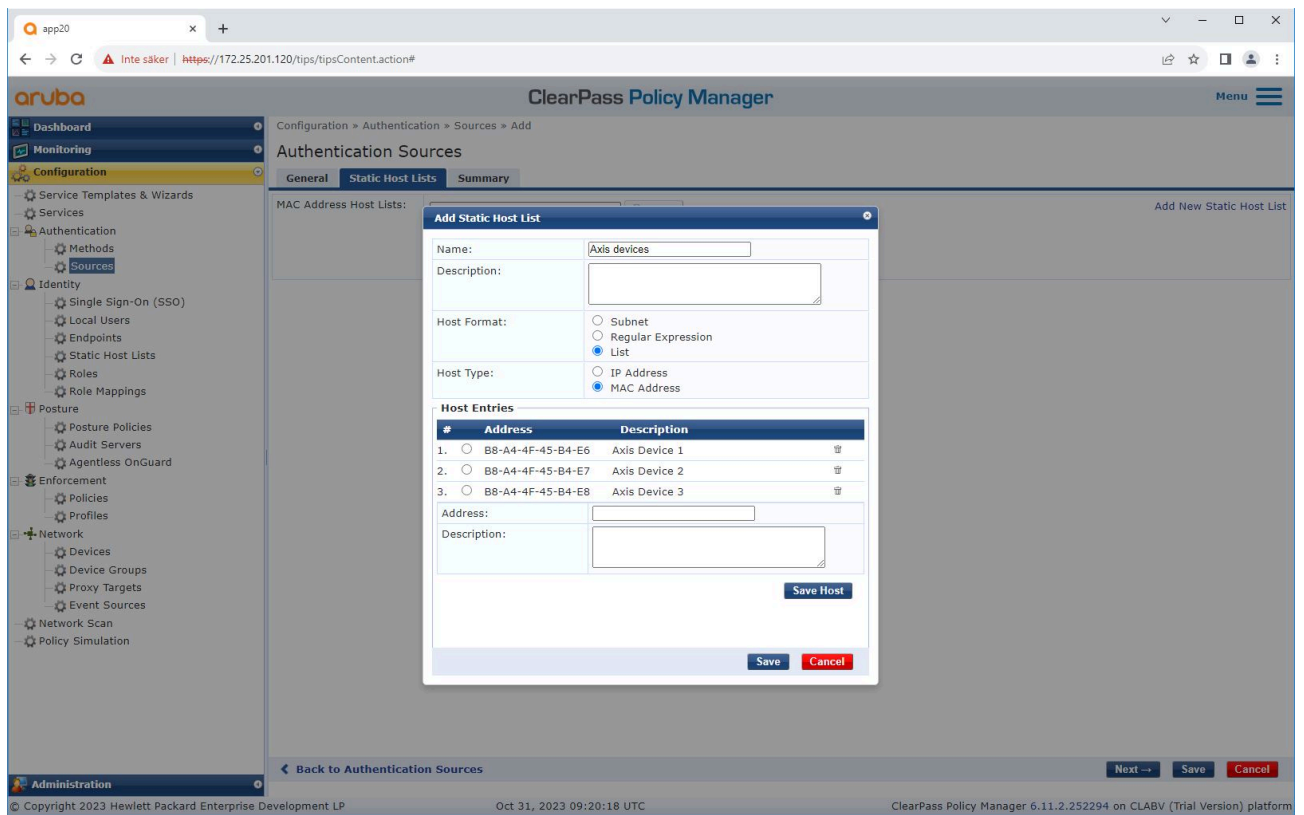
# HPE Aruba Networking

## Incorporación heredada: autenticación MAC



# HPE Aruba Networking

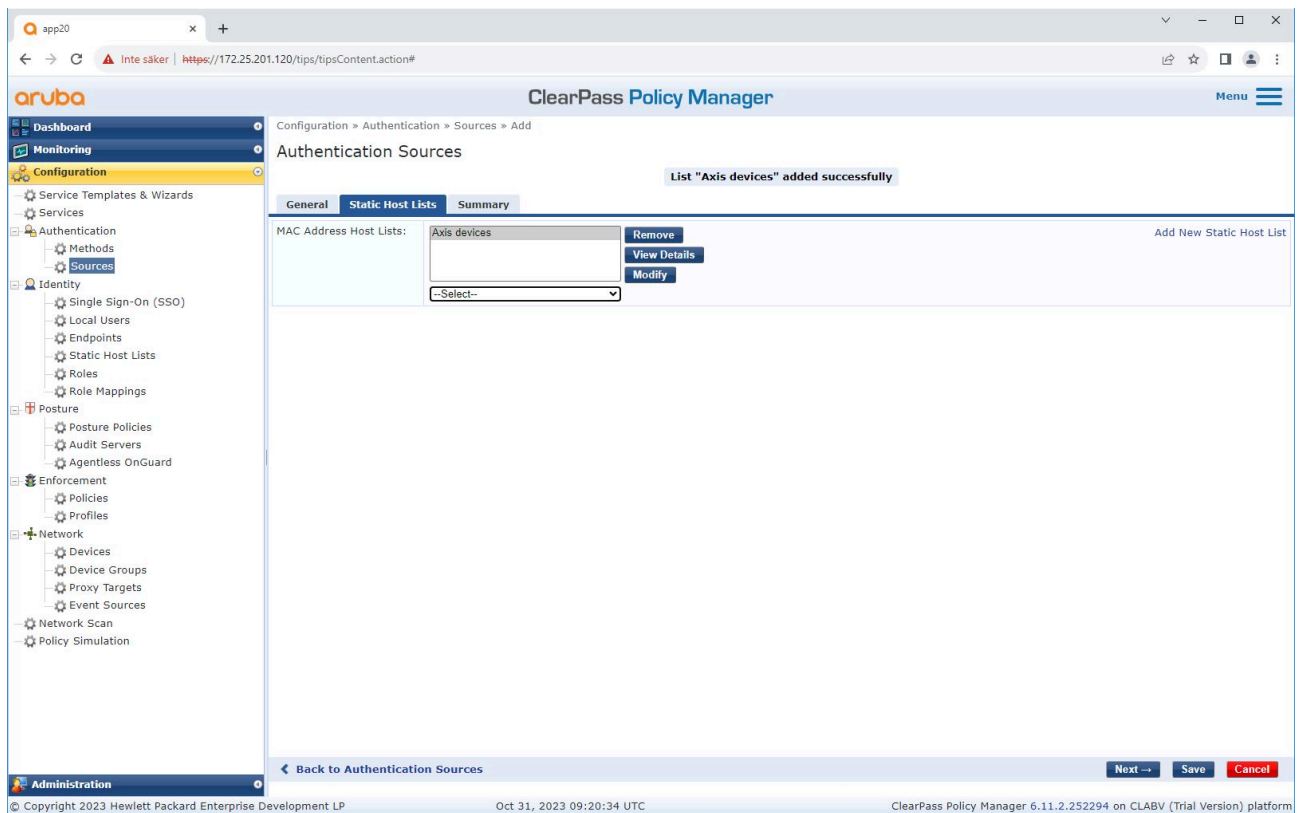
## Incorporación heredada: autenticación MAC



*Se crea una lista de hosts estática, que contiene direcciones MAC de Axis.*

# HPE Aruba Networking

## Incorporación heredada: autenticación MAC



### Configuración de servicio

En la página Services (Servicios), los pasos de configuración se combinan en un solo servicio que maneja la autenticación y autorización de los dispositivos Axis en las redes de HPE Aruba Networking.

# HPE Aruba Networking

## Incorporación heredada: autenticación MAC

Configuration » Services

### Services

This page shows the current list and order of services that ClearPass follows during authentication and authorization.

Filter: Name contains [ ] Go Clear Filter Hit Count for [Current hour] Show [20] records

#	Order	Name	Type	Template	Hit Count	Status
1.	1	Axis 802.1X Wired	RADIUS	802.1X Wired	0	OK
2.	2	Axis 802.1X Wired - Mac Authentication	RADIUS	MAC Authentication	0	OK
3.	3	Test_Service	RADIUS	802.1X Wired	0	Error
4.	4	[Policy Manager Admin Network Login Service]	TACACS+	TACACS+ Enforcement	0	Error
5.	5	[AirGroup Authorization Service]	RADIUS	RADIUS Enforcement ( Generic )	0	Error
6.	6	[Aruba Device Access Service]	TACACS+	TACACS+ Enforcement	0	Error
7.	7	[Guest Operator Logins]	Application	Aruba Application Authentication	0	Error
8.	8	[Insight Operator Logins]	Application	Aruba Application Authentication	0	Error
9.	9	[Device Registration Disconnect]	WEBAUTH	Web-based Authentication	0	Error

Showing 1-9 of 9 Reorder Copy Export Delete

© Copyright 2023 Hewlett Packard Enterprise Development LP Oct 26, 2023 05:34:53 UTC ClearPass Policy Manager 6.11.2.252294 on CLABV (Trial Version) platform

# HPE Aruba Networking

## Incorporación heredada: autenticación MAC

The screenshot displays the Aruba ClearPass Policy Manager web interface. The left sidebar shows the navigation menu with categories like Dashboard, Monitoring, Configuration, and Administration. The main content area is titled 'Services - Axis 802.1X Wired - Mac Authentication' and shows the configuration for a service. The 'Service' tab is active, displaying the following details:

- Name: Axis 802.1X Wired - Mac Authentication
- Description: To authenticate guest devices based on their MAC address.
- Type: MAC Authentication
- Status: Disabled
- Monitor Mode:  Enable to monitor network access without enforcement
- More Options:  Authorization  Audit End-hosts  Profile Endpoints  Accounting Proxy

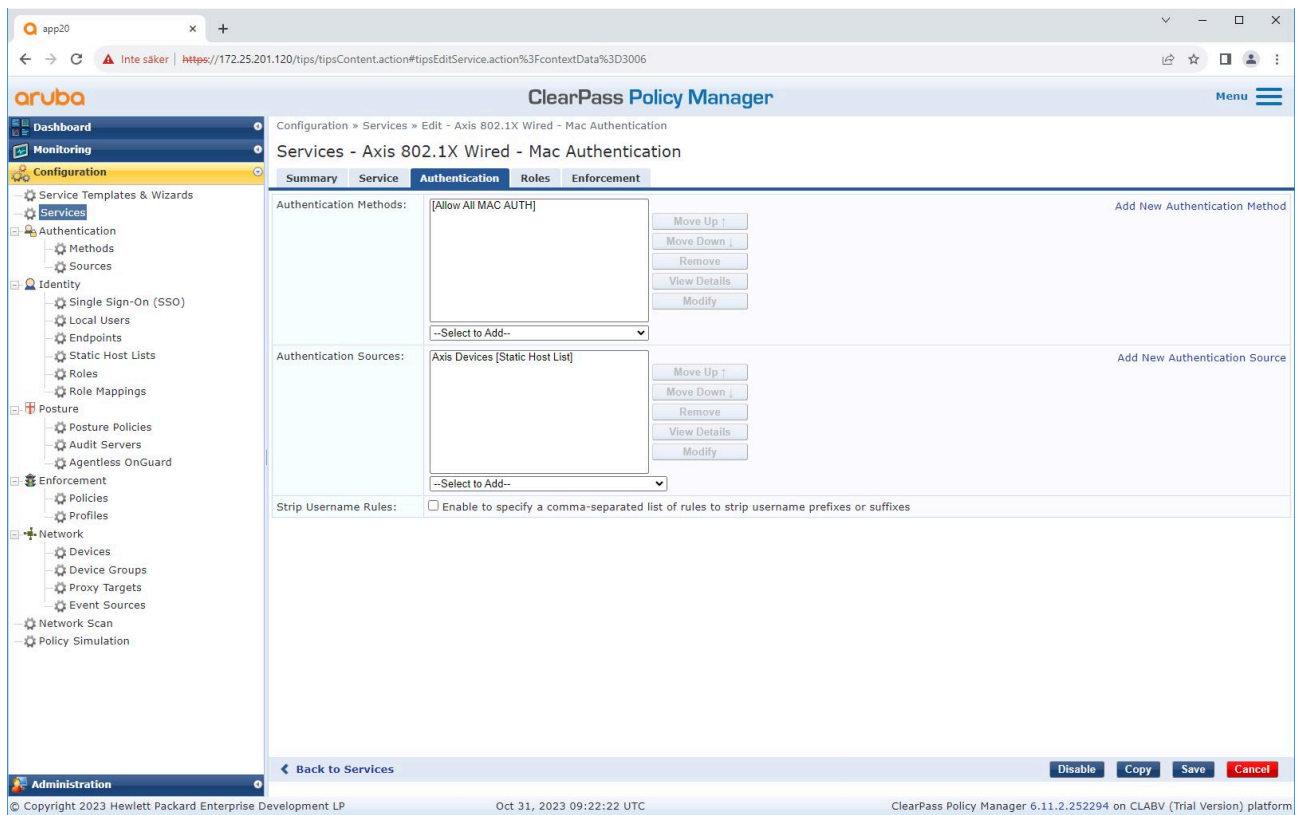
Below these details is the 'Service Rule' section, which defines the conditions for the service. It is set to match 'ALL of the following conditions':

Type	Name	Operator	Value
1.	Radius:IETF	NAS-Port-Type	BELONGS_TO Ethernet (15)
2.	Radius:IETF	Service-Type	BELONGS_TO Login-User (1), Call-Check (10)
3.	Connection	Client-Mac-Address	EQUALS % {Radius:IETF:User-Name}
4.	Click to add...		

At the bottom of the configuration page, there are buttons for 'Enable', 'Copy', 'Save', and 'Cancel'. The footer of the interface shows the copyright information for Hewlett Packard Enterprise Development LP and the version of the ClearPass Policy Manager (6.11.2.252294).

Se crea un servicio Axis dedicado que define MAB como método de conexión.

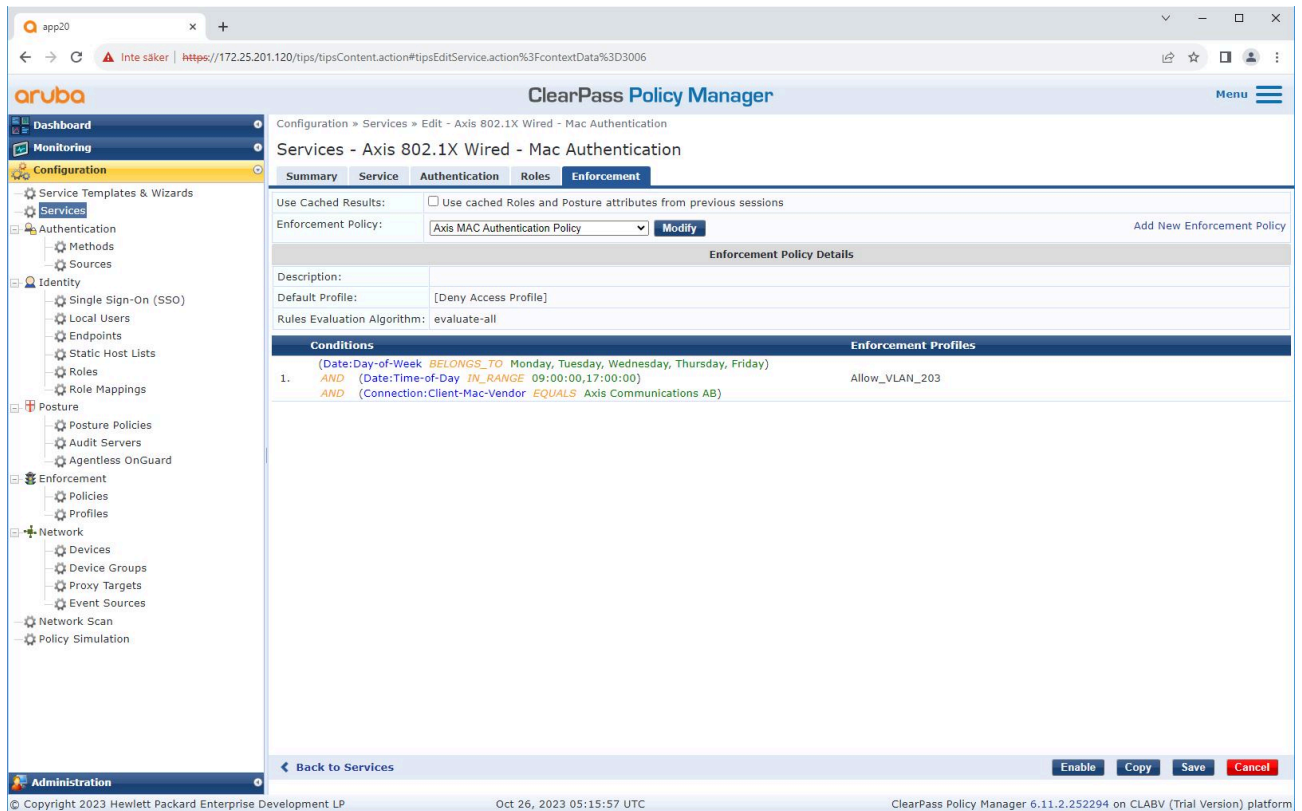




*El método de autenticación MAC preconfigurado está configurado para el servicio. Además, se selecciona la fuente de autenticación creada previamente que contiene una lista de direcciones MAC de Axis.*

Axis Communications utiliza las siguientes OUI de direcciones MAC:

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



*En el último paso, la política de aplicación creada anteriormente se configura para el servicio.*

### Switch de acceso de HPE Aruba Networking

Además de la configuración de integración segura descrita en , consulte el siguiente ejemplo de configuración de puerto para que el switch de acceso de HPE Aruba Networking permita 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
```

