

HPE Aruba Networking

Índice

Introducción.....	3
Incorporación segura: IEEE 802.1AR/802.1X.....	4
Autenticación inicial.....	4
Aprovisionamiento	4
Red de producción.....	5
Configuración de HPE Aruba Networking	6
ClearPass Policy Manager de HPE Aruba Networking	6
Switch de acceso de HPE Aruba Networking.....	15
Configuración Axis	16
Dispositivo en red de Axis.....	16
AXIS Device Manager.....	17
Operación de red segura: IEEE 802.1AE MACsec	18
ClearPass Policy Manager de HPE Aruba Networking.....	19
Política de asignación de roles y roles	19
Configuración de servicio	20
Perfil de cumplimiento.....	21
Switch de acceso de HPE Aruba Networking.....	22
Incorporación heredada: autenticación MAC.....	23
ClearPass Policy Manager de HPE Aruba Networking.....	23
Política de cumplimiento.....	23
Configuración de fuente.....	24
Configuración de servicio	25
Switch de acceso de HPE Aruba Networking.....	28

Introducción

Esta guía de integración describe la configuración recomendada para la incorporación y el funcionamiento de dispositivos Axis en redes HPE Aruba Networking. La configuración utiliza estándares y protocolos de seguridad modernos, como IEEE 802.1X, IEEE 802.1AR, IEEE 802.1AE y HTTPS.

La automatización adecuada para la integración de la red le permite ahorrar tiempo y dinero. Elimina la complejidad innecesaria del sistema cuando se utilizan aplicaciones de gestión de dispositivos de Axis con la infraestructura y las aplicaciones de HPE Aruba Networking. Al combinar dispositivos y software Axis con una infraestructura de HPE Aruba Networking, podrá beneficiarse de las siguientes ventajas:

- La eliminación de las redes de almacenamiento temporal de dispositivos minimiza la complejidad del sistema.
- La automatización de los procesos de incorporación y la gestión de dispositivos reduce los costes.
- Los dispositivos Axis proporcionan controles de seguridad de red automatizados.
- Mayor seguridad de red gracias a la experiencia de HPE y Axis.



Para una transición fluida entre redes lógicas definida por software durante el proceso de incorporación, la infraestructura de red debe estar preparada para verificar de forma segura la integridad de los dispositivos Axis antes de iniciar la configuración. Antes de la configuración, debe asegurar los siguientes aspectos:

- Experiencia de 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 previos sobre los productos Axis, aunque también se facilitan 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.

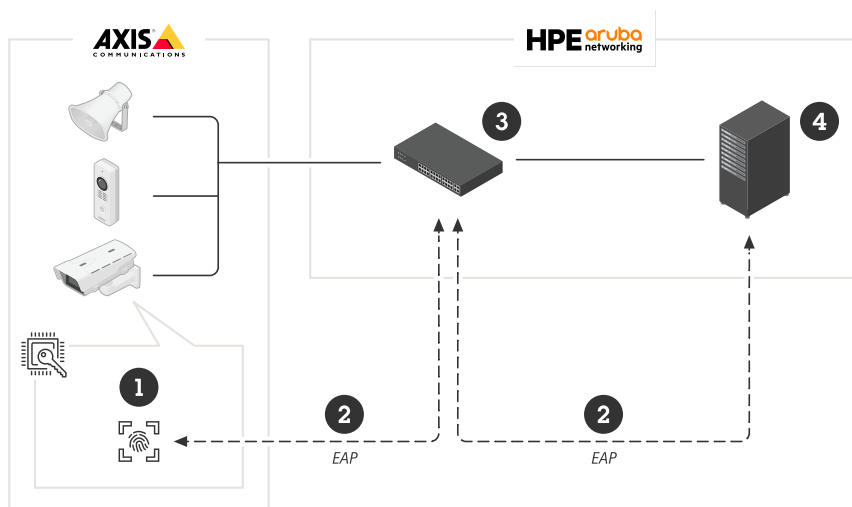
Integración de dispositivos segura en redes de confianza cero con IEEE 802.1X/802.1AR

Autenticación inicial

Cuando el dispositivo Axis compatible con Axis Edge Vault se conecta a la red, utiliza el certificado de identificación de dispositivo Axis IEEE 802.1AR 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. Esta información, como la dirección MAC y la versión del sistema operativo AXIS del dispositivo, se utiliza para tomar decisiones basadas en políticas.

El dispositivo Axis se autentifica a si mismo en la red mediante el certificado de ID de dispositivo Axis compatible con IEEE 802.1AR.

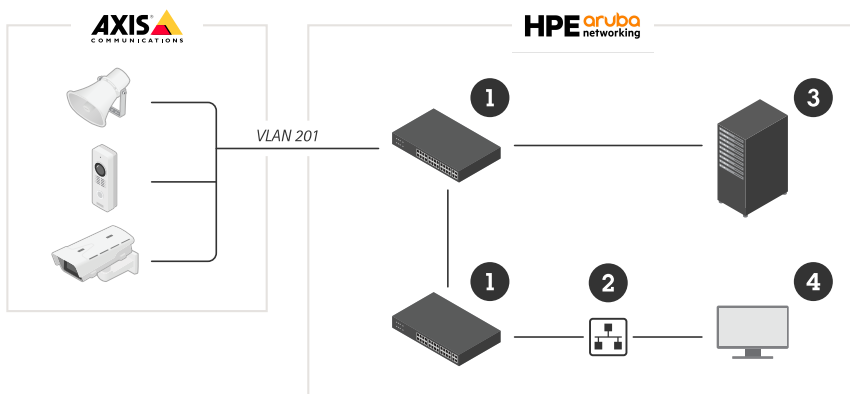


El dispositivo Axis se autentifica en la red de HPE Aruba Networking utilizando el certificado de ID de dispositivo Axis compatible con IEEE 802.1AR.

- 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 conecta a la red de aprovisionamiento (VLAN 201). Esta red contiene AXIS Device Manager, que realiza la configuración del dispositivo, el refuerzo de la seguridad y las actualizaciones del sistema operativo AXIS. Para completar el aprovisionamiento del dispositivo, se cargan en él nuevos certificados de producción específicos del cliente para IEEE 802.1X y HTTPS.

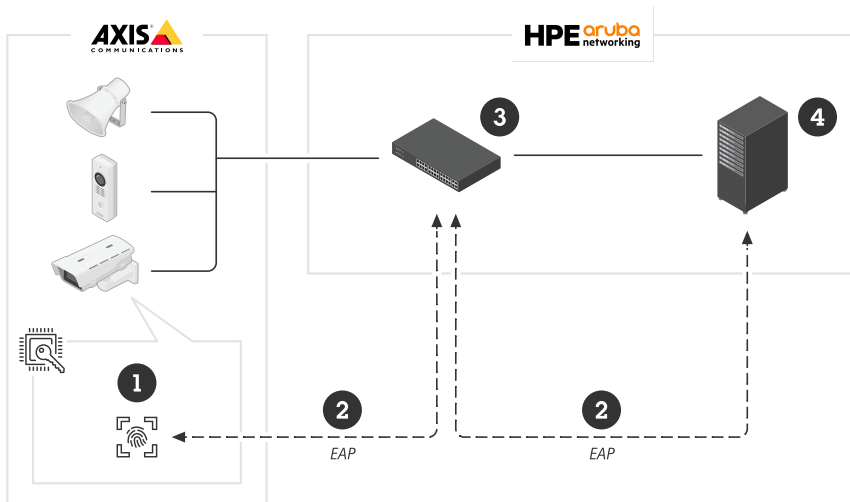


Después de una autenticación exitosa, el dispositivo Axis pasa a una red de aprovisionamiento para su configuración.

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

Red de producción

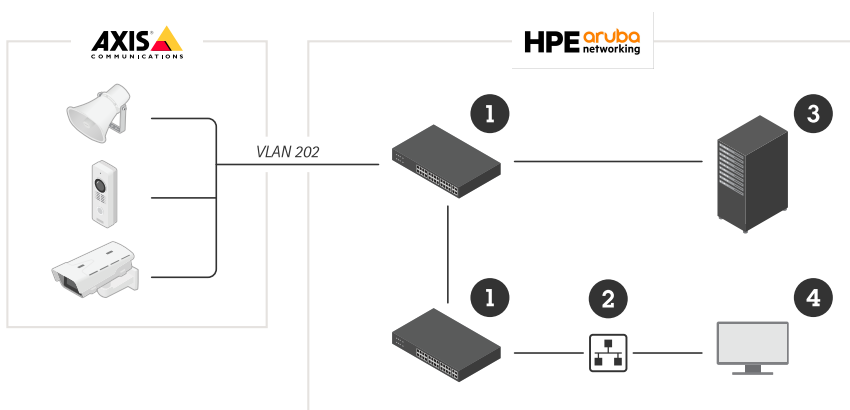
El aprovisionamiento del dispositivo Axis con nuevos certificados IEEE 802.1X activa un nuevo intento de autenticación. ClearPass Policy Manager verifica los nuevos certificados y decide si mueve o no el dispositivo Axis a la red de producción.



Una vez configurado, 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

Tras la reautenticación, el dispositivo Axis se conecta a la red de producción (VLAN 202), donde el Sistema de gestión de vídeo (VMS) se conecta al dispositivo e inicia el funcionamiento.



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 infraestructuras cableadas, inalámbricas 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.
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.

The screenshot shows the ClearPass Policy Manager web interface. The left sidebar contains navigation links: Dashboard, Monitoring, Configuration, and Administration. The main content area is titled 'Certificate Trust List' and shows a table of trusted Certificate Authorities (CA). A dialog box titled 'Add Certificate' is open, showing the 'Certificate File' field with the value 'Axis_device_ID_int...e_CA_ECC_1.pem' and the 'Usage' field with the value 'EAP'. The dialog also has 'Add Certificate' and 'Cancel' buttons.

#	Subject	Usage	Validity	Enabled
1.	OU=VeriSign Trust Network,OU=(c) 1998 VeriSign, Inc. - For authorized use only,OU=Class 3 Public Primary Certification Authority - G2,O=VeriSign, Inc.,C=US	Others	Valid	Disabled
2.	OU=Go	AD/LDAP Servers, Endpoint Context Servers, SAML, SMTP, Others	Valid	Enabled
3.	OU=Class	Others	Valid	Disabled
4.	emailAd	EAP, Others	Valid	Enabled
5.	emailAd	EAP, Others	Valid	Enabled
6.	Authority C=US,S	Others	Valid	Disabled
7.	01	Others	Valid	Disabled
8.	C=US,S	Others	Valid	Disabled
9.	C=US,S	Aruba Infrastructure	Valid	Disabled
10.	CN=Wired Phones,OU=PKI Authority,O=Alcatel-Lucent,C=FR	Others	Valid	Disabled
11.	CN=VeriSign Class 3 Public Primary Certification Authority - G5,OU=(c) 2006 VeriSign, Inc. - For authorized use only,OU=VeriSign Trust Network,O=VeriSign, Inc.,C=US	Others	Valid	Disabled
12.	CN=VeriSign Class 3 Public Primary Certification Authority - G3,OU=(c) 1999 VeriSign, Inc. - For authorized use only,OU=VeriSign Trust Network,O=VeriSign, Inc.,C=US	Others	Valid	Disabled
13.	CN=VeriSign Class 1 Public Primary Certification Authority - G3,OU=(c) 1999 VeriSign, Inc. - For authorized use only,OU=VeriSign Trust Network,O=VeriSign, Inc.,C=US	AD/LDAP Servers, Endpoint Context Servers, SAML, SMTP, Others	Valid	Enabled
14.	CN=USERTrust RSA Certification Authority,O=The USERTRUST Network,L=Jersey City,ST=New Jersey,C=US	EAP, Others	Valid	Disabled
15.	CN=thawte Primary Root CA,OU=(c) 2006 thawte, Inc. - For authorized use only,OU=Certification Services Division,O=thawte, Inc.,C=US	Others	Valid	Disabled
16.	CN=TC TrustCenter Universal CA 1,OU=TC TrustCenter Universal CA,O=TC TrustCenter GmbH,C=DE	Others	Valid	Disabled

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

The screenshot shows the ClearPass Policy Manager web interface. The left sidebar contains navigation options: Dashboard, Monitoring, Configuration, and Administration. The main content area is titled 'Administration » Certificates » Trust List' and 'Certificate Trust List'. It includes a filter bar with 'Subject' selected and a search term 'axis device'. Below the filter is a table with 6 records, each showing a checkbox, a subject name, usage, validity, and enabled status. The table is titled 'Showing 1-6 of 6' and has a 'Delete' button.

#	Subject	Usage	Validity	Enabled
1.	☐ CN=Axis device ID Root CA RSA,O=Axis Communications AB	EAP	Valid	Enabled
2.	☐ CN=Axis device ID Root CA ECC,O=Axis Communications AB	EAP	Valid	Enabled
3.	☐ CN=Axis device ID Intermediate CA RSA 2,O=Axis Communications AB	EAP	Valid	Enabled
4.	☐ CN=Axis device ID Intermediate CA RSA 1,O=Axis Communications AB	EAP	Valid	Enabled
5.	☐ CN=Axis device ID Intermediate CA ECC 2,O=Axis Communications AB	EAP	Valid	Enabled
6.	☐ CN=Axis device ID Intermediate CA ECC 1,O=Axis Communications AB	EAP	Valid	Enabled

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

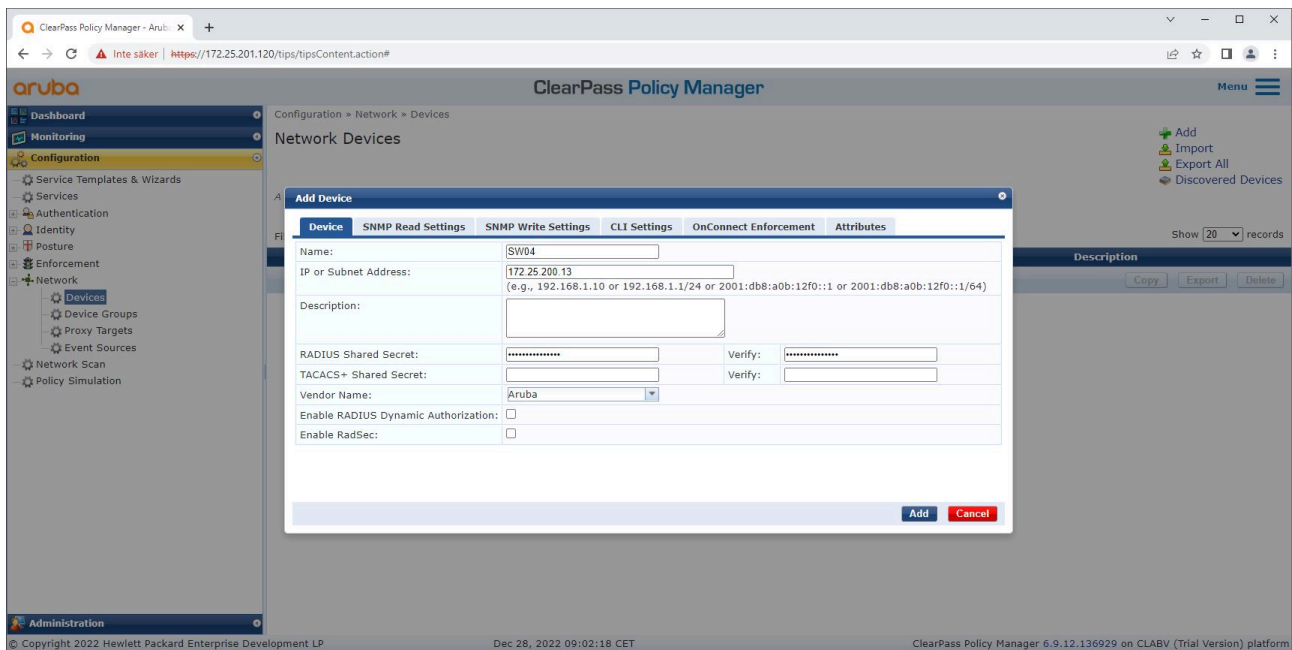
Configuración de dispositivo/grupo de red

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. Recuerde también que el secreto compartido de RADIUS debe coincidir con la configuración específica del switch IEEE 802.1X.
2. Utilice la configuración del grupo de dispositivos de red para agrupar múltiples dispositivos de acceso a la red fiables. Agrupar dispositivos facilita la configuración de políticas.

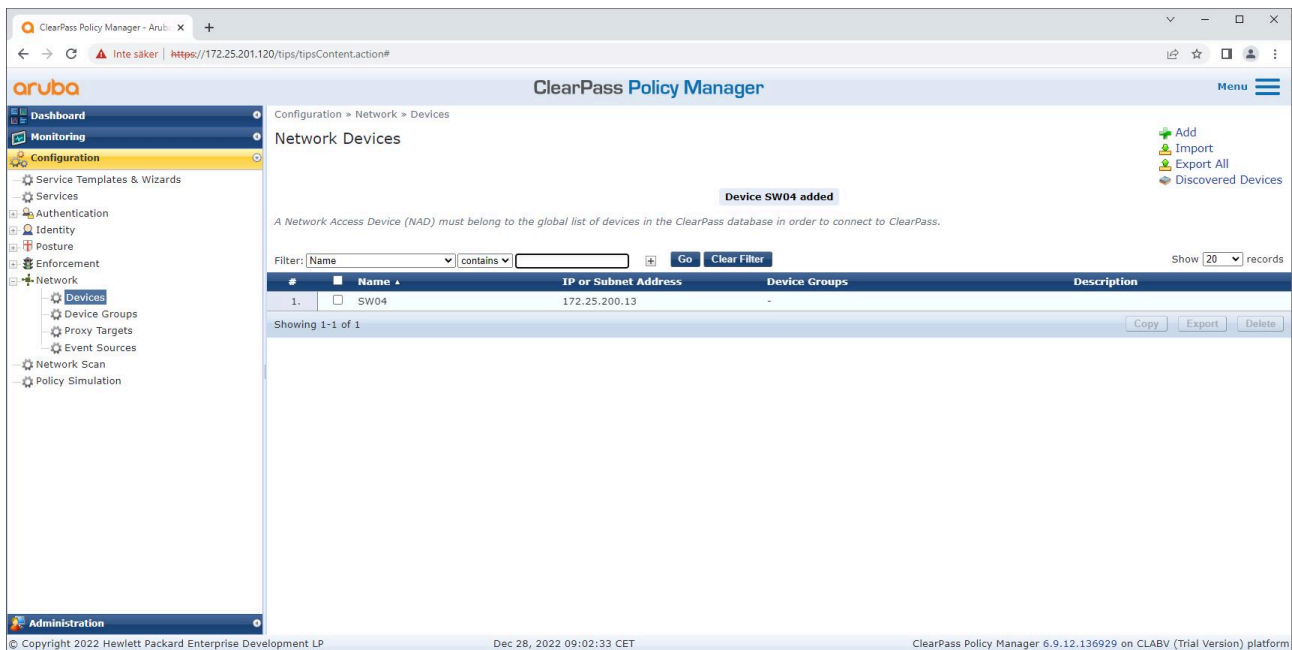
The screenshot shows the ClearPass Policy Manager web interface. The left sidebar contains navigation options: Dashboard, Monitoring, Configuration, and Administration. The main content area is titled 'Configuration » Network » Devices' and 'Network Devices'. It includes a filter bar with 'Name' selected and a search term. Below the filter is a table with 4 records, each showing a checkbox, a name, IP or Subnet Address, device groups, and description. The table is titled 'Showing 1-4 of 4' and has buttons for 'Copy', 'Export', and 'Delete'.

#	Name	IP or Subnet Address	Device Groups	Description
1.	☐			
2.	☐			
3.	☐			
4.	☐			

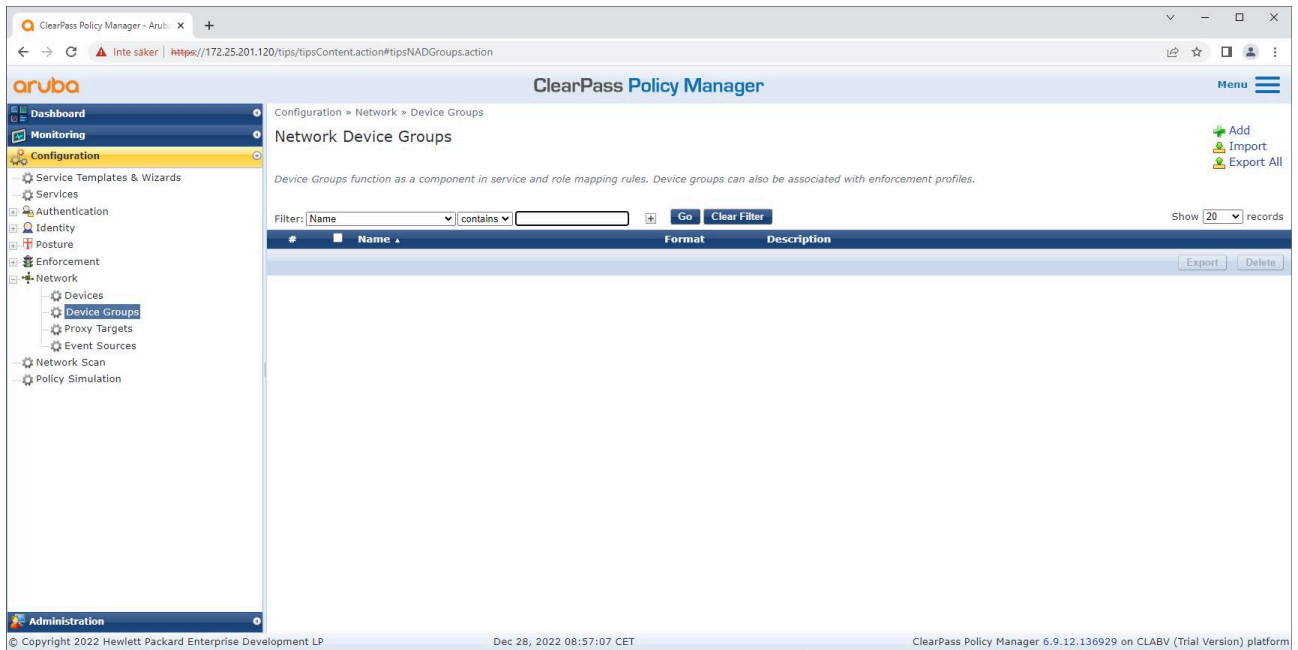
La interfaz de dispositivos de red confiables en ClearPass Policy Manager.



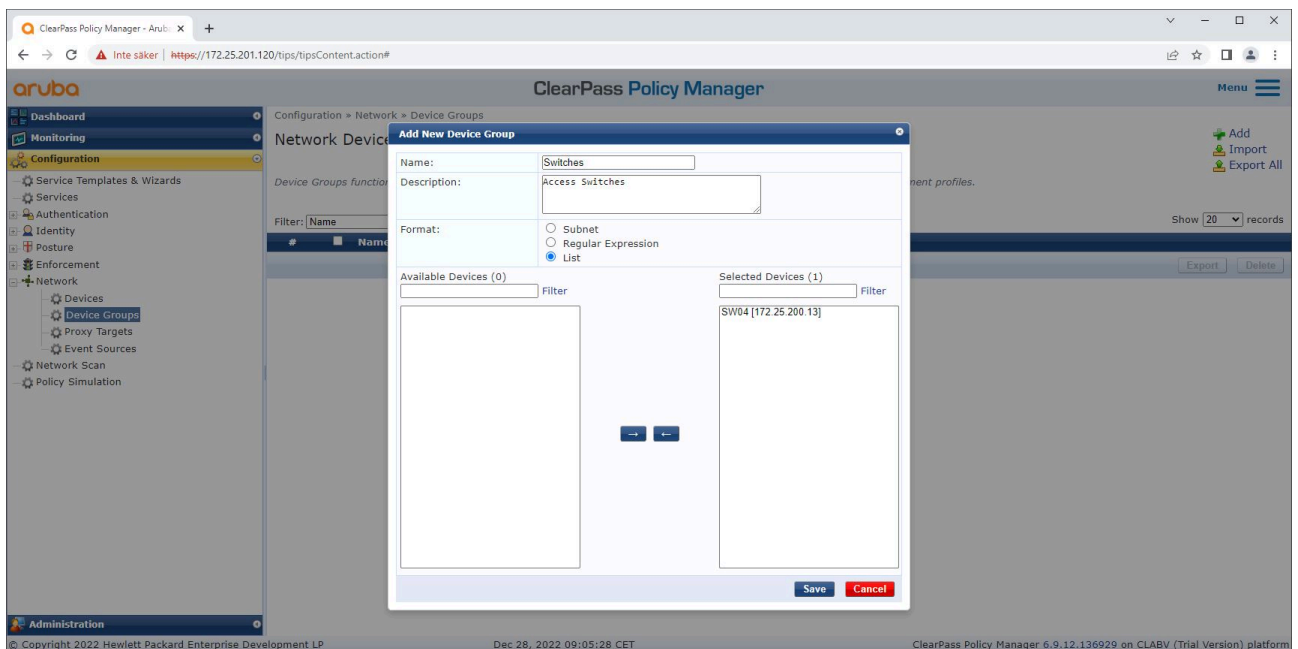
Añada el switch de acceso de red HPE Aruba como dispositivo de confianza en ClearPass Policy Manager. Recuerde que el secreto compartido de RADIUS debe coincidir con la configuración específica del switch IEEE 802.1X.



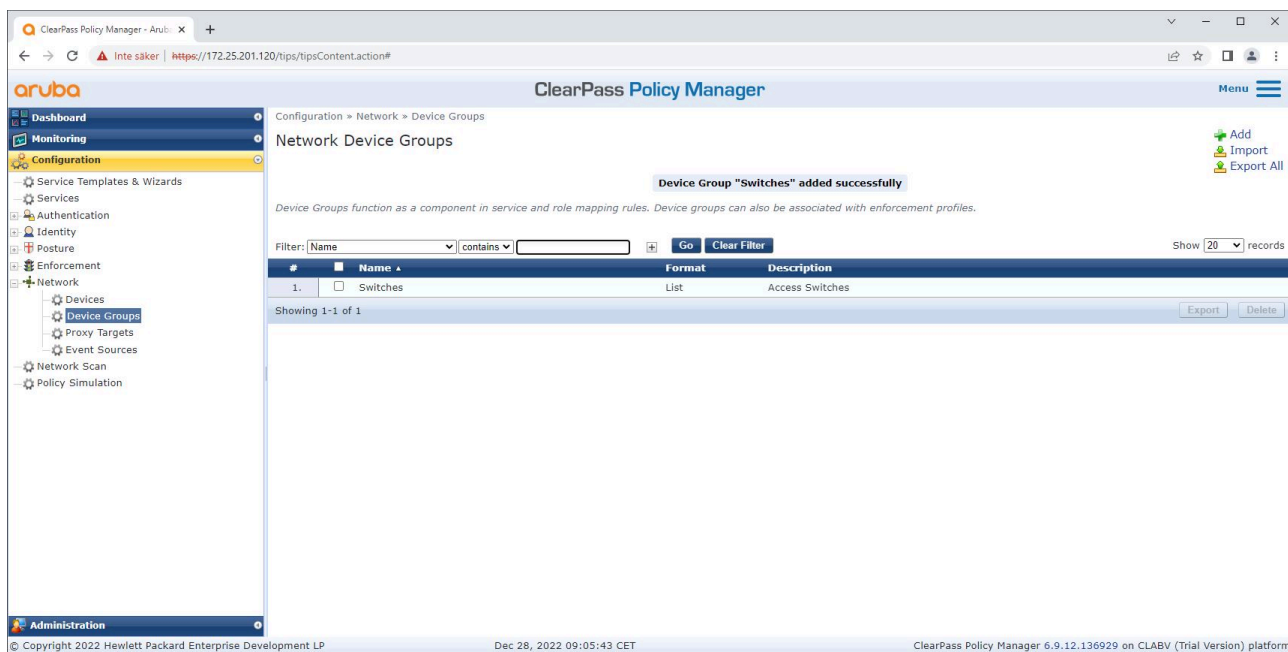
ClearPass Policy Manager con un único dispositivo de red fiable configurado.



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



Añada un dispositivo de acceso a la red fiable a un nuevo grupo de dispositivos en ClearPass Policy Manager.

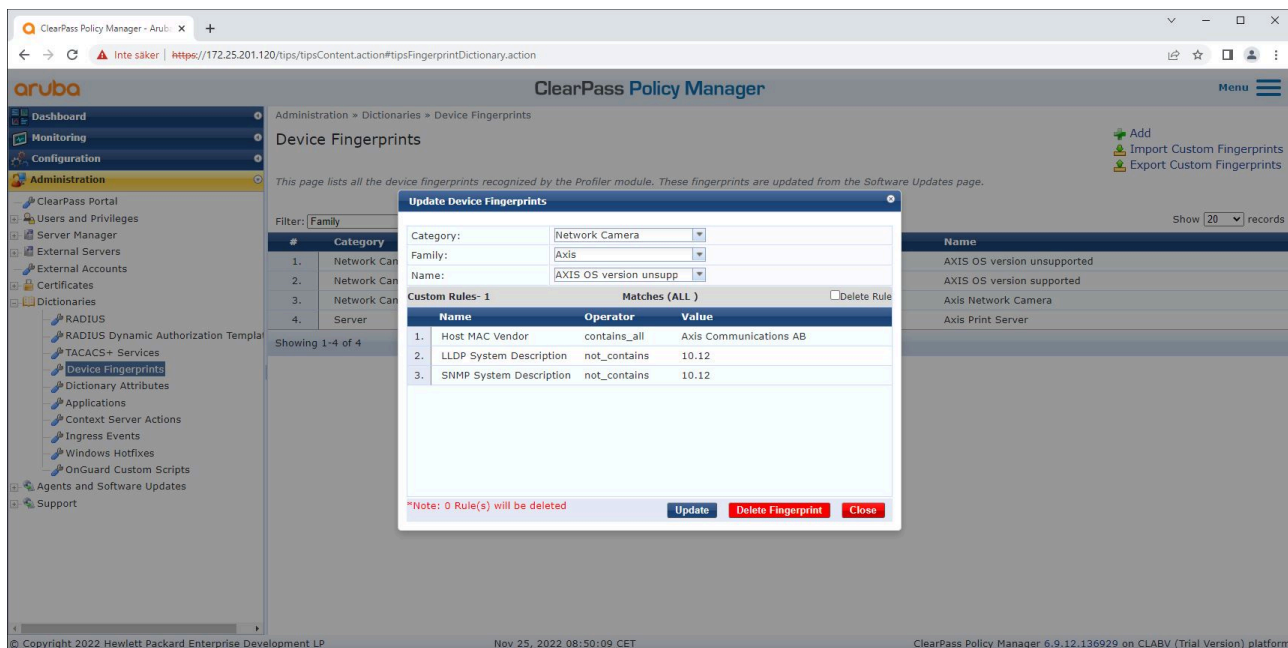


ClearPass Policy Manager con un grupo de dispositivos de red configurado que incluye uno o más dispositivos de red fiables.

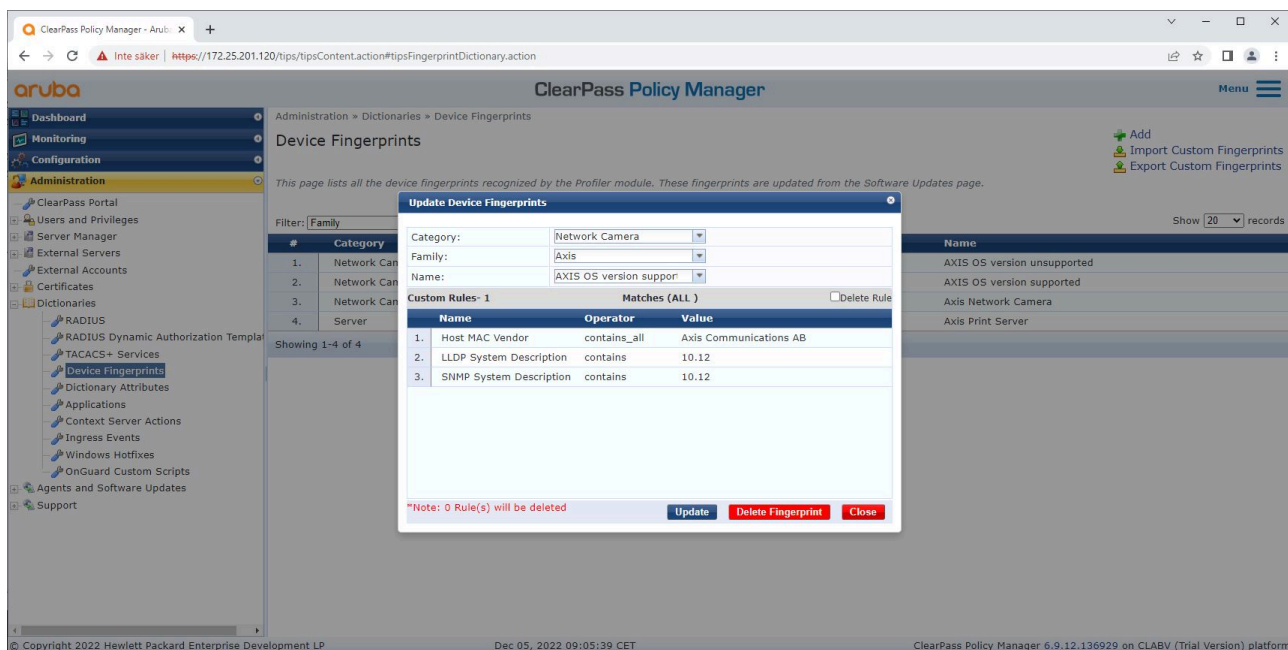
Configuración de huellas digitales del dispositivo

El dispositivo Axis puede, mediante la detección de red, distribuir información específica del dispositivo, como la dirección MAC y la versión del software. Puede usar 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 del AXIS OS.

1. Vaya a **Administration > Dictionaries > Device Fingerprints** (Administración > Diccionarios > Huellas digitales del dispositivo).
2. Seleccione una huella digital de dispositivo existente o cree una nueva huella digital de dispositivo.
3. Configure los ajustes de huella digital del dispositivo.



La configuración de huellas digitales del dispositivo en ClearPass Policy Manager. Los dispositivos Axis con versiones del AXIS OS distintas a 10.12 no son compatibles con este ejemplo.



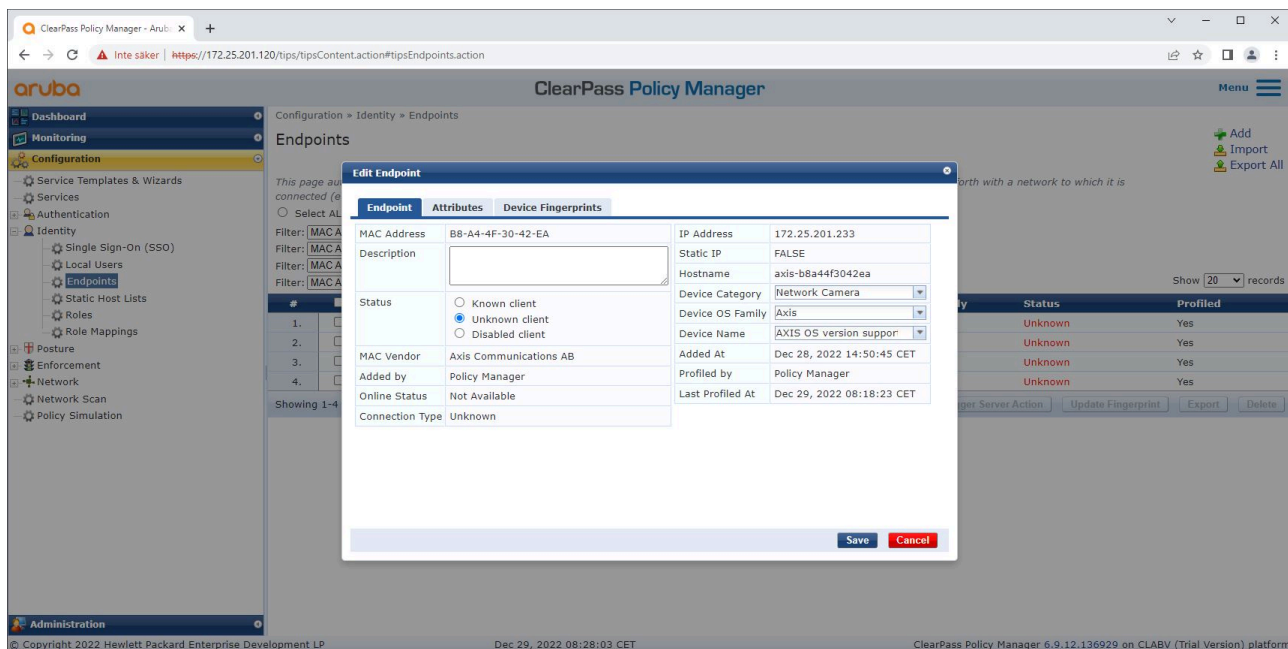
La configuración de huellas digitales del dispositivo en ClearPass Policy Manager. Los dispositivos Axis con versiones del AXIS OS distintas a 10.12 son compatibles con este ejemplo.

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

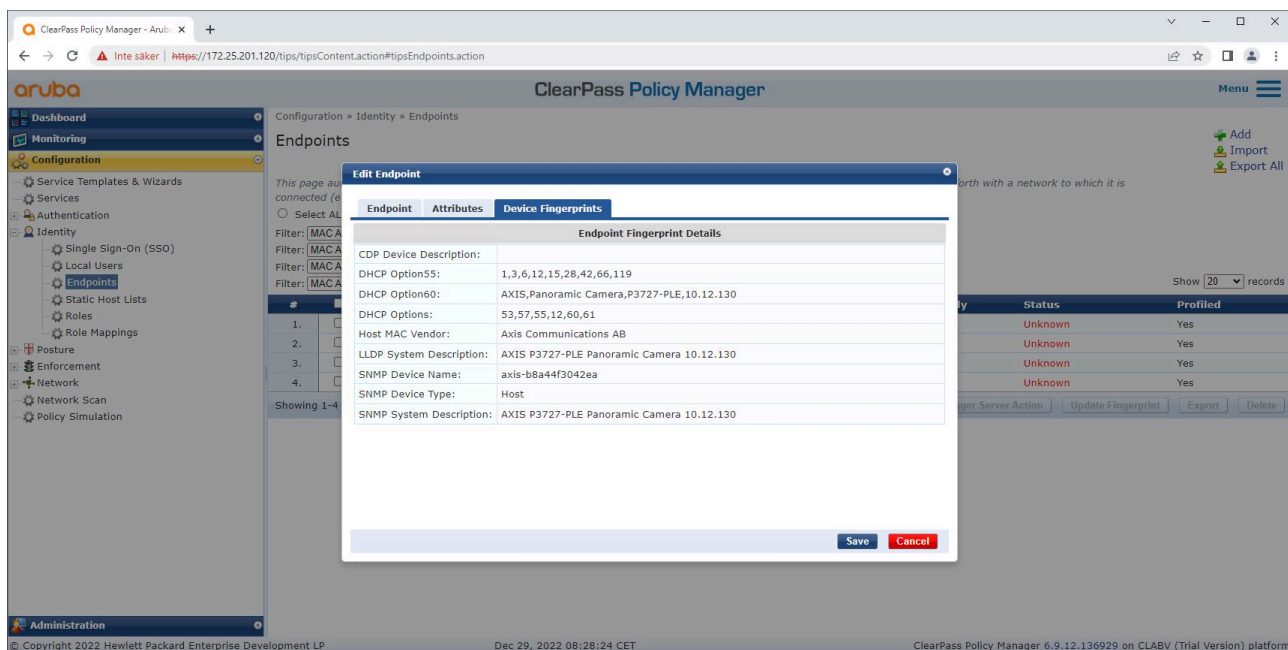
1. Vaya a **Configuration > Identity > Endpoints** (Configuración > Identidad > Puntos finales).
2. Seleccione el dispositivo que desee ver.
3. Haga clic en la pestaña **Device Fingerprints** (Huellas digitales del dispositivo).

Nota

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



Un dispositivo Axis con perfil de ClearPass Policy Manager.

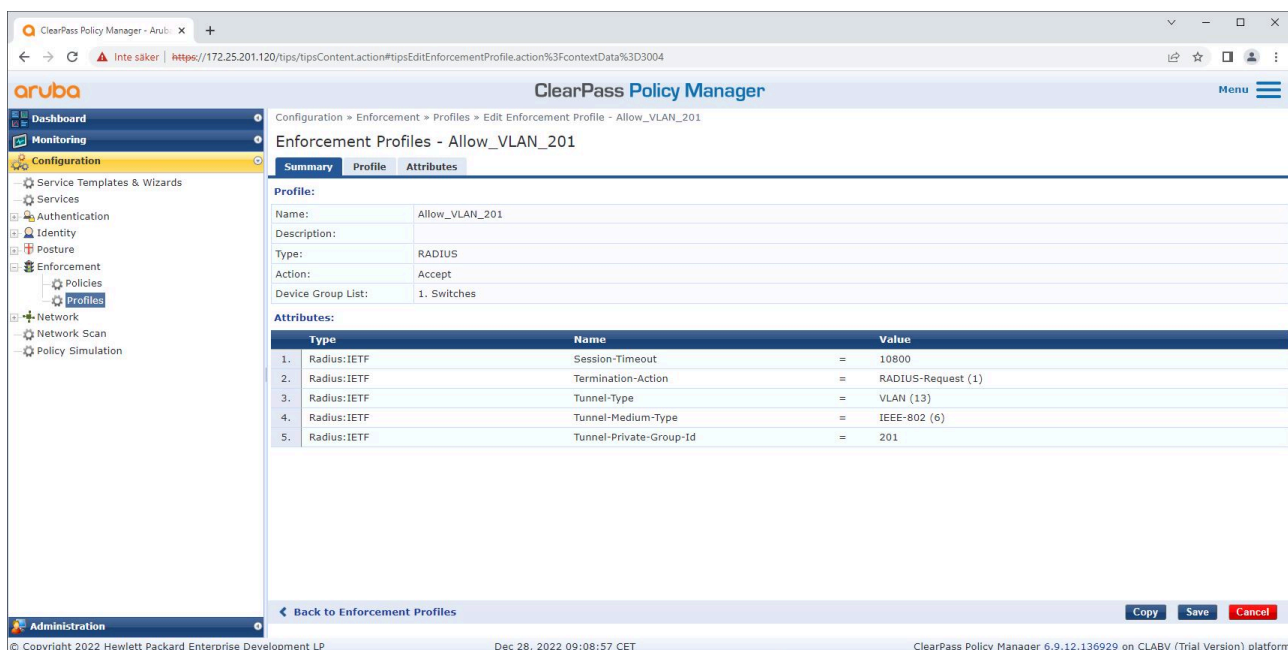


Las huellas dactilares detalladas del dispositivo de un dispositivo Axis perfilado. Recuerde que SNMP está deshabilitado de forma predeterminada en los dispositivos Axis. La información de detección específica de LLDP, CDP y DHCP se comparte desde el dispositivo Axis en su estado predeterminado de fábrica y se retransmite desde el switch de acceso de red HPE Aruba a ClearPass Policy Manager.

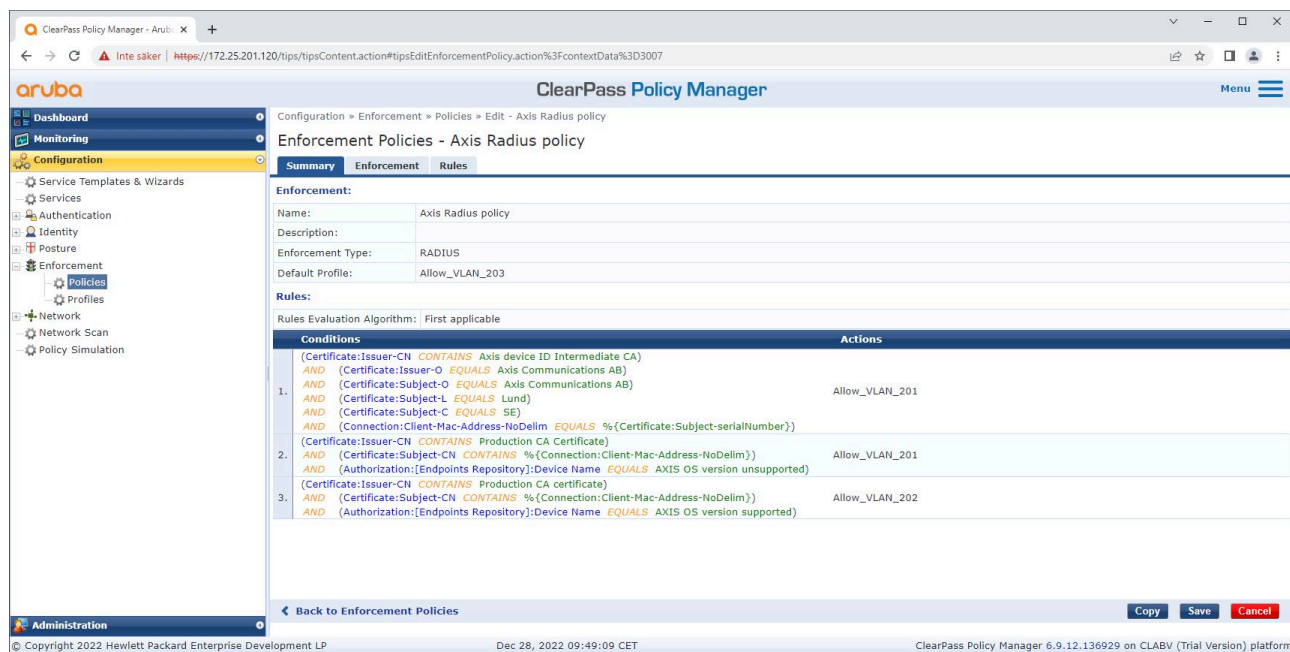
Configuración del perfil de cumplimiento

Un Enforcement Profile (Perfil de cumplimiento) permite que ClearPass Policy Manager asigne una ID de VLAN específica a un puerto de acceso en el switch. Esta es una decisión basada en políticas que se aplica a los dispositivos de red del grupo de dispositivos "Switches". El número de perfiles de aplicación necesarios depende del número de VLAN en uso. Nuestra configuración tiene tres VLAN (VLAN 201, 202, 203), que responden a tres perfiles de aplicación.

Una vez configurados los perfiles de cumplimiento para la VLAN, se puede configurar la política de aplicación. La configuración de la política de aplicación 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 aplicación y sus acciones son:

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)

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. Posteriormente, se requiere una inspección manual del dispositivo para determinar las acciones apropiadas.

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 del AXIS OS del dispositivo.
- La dirección MAC del dispositivo coincide con el esquema de dirección MAC 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.

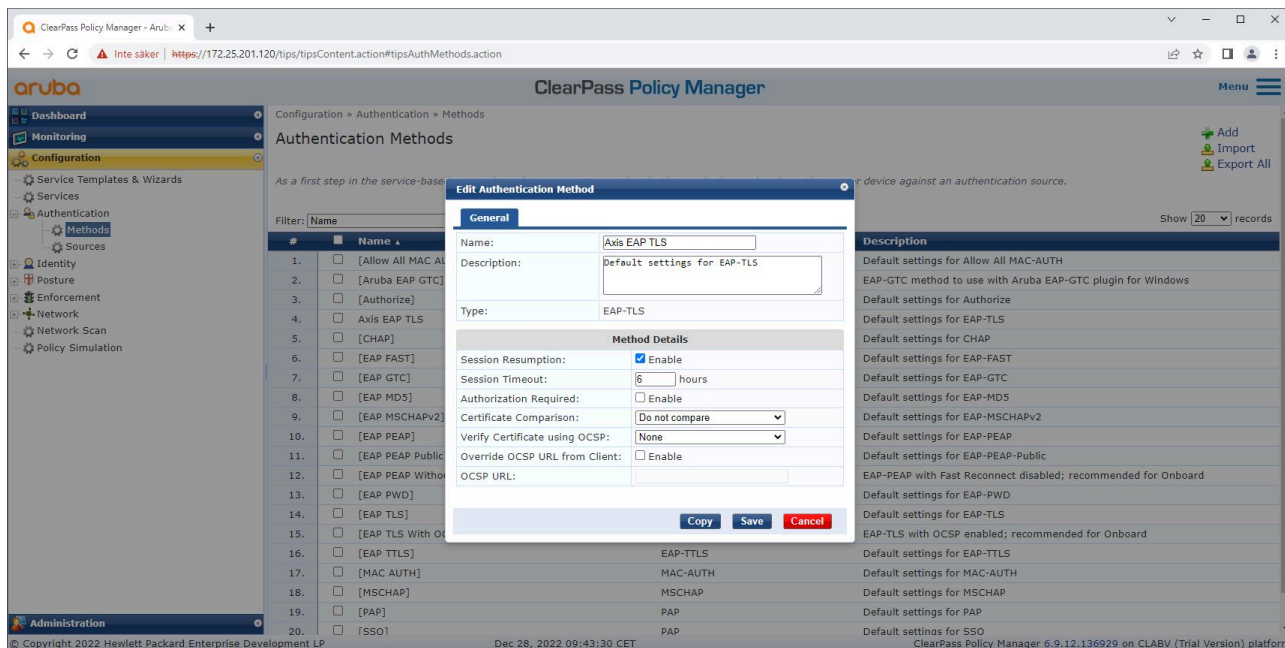
Red de producción (VLAN 202)

Se concede acceso al dispositivo Axis a la red de producción en la que operará. 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 versión del AXIS OS del dispositivo.
- La dirección MAC del dispositivo coincide con el esquema de dirección MAC específico del proveedor con el atributo de número de serie del certificado de ID del dispositivo de Axis.
- El certificado de grado de producción es verificable por el almacén de certificados de confianza.

Configuración del método de autenticación

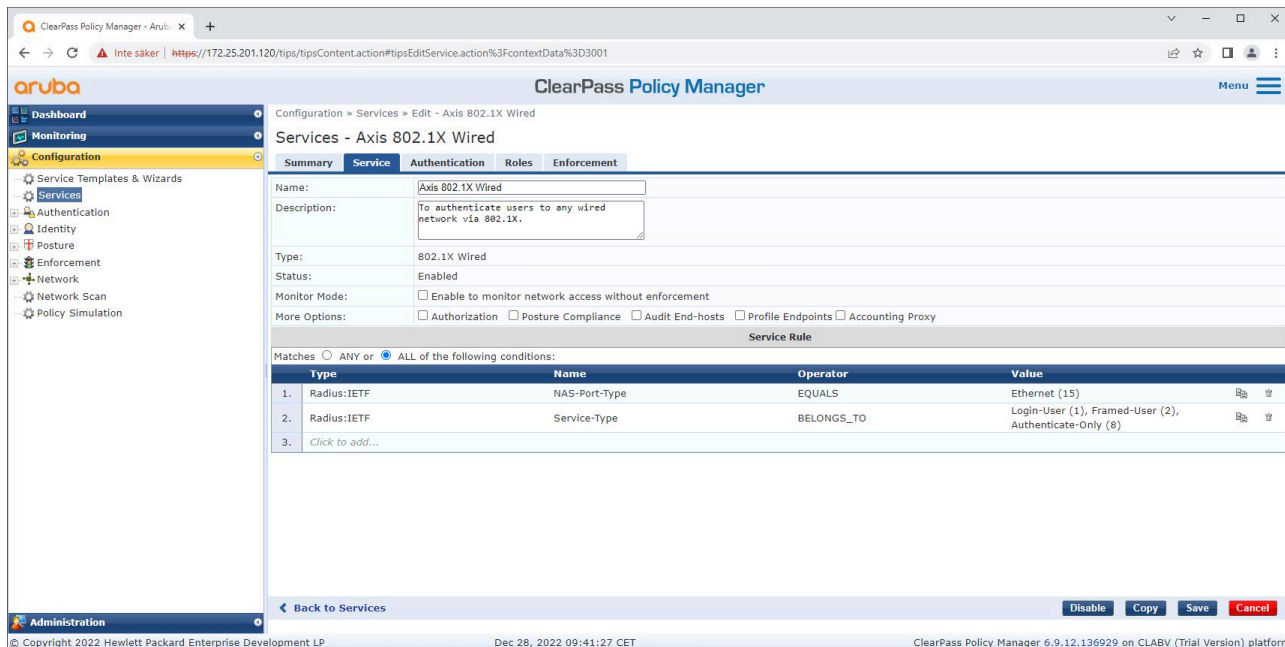
El método de autenticación define cómo un dispositivo Axis intenta autenticarse en la red. El método preferido es IEEE 802.1X EAP-TLS, dado que los dispositivos Axis con Axis Edge Vault cuentan con IEEE 802.1X EAP-TLS habilitado de forma predeterminada.



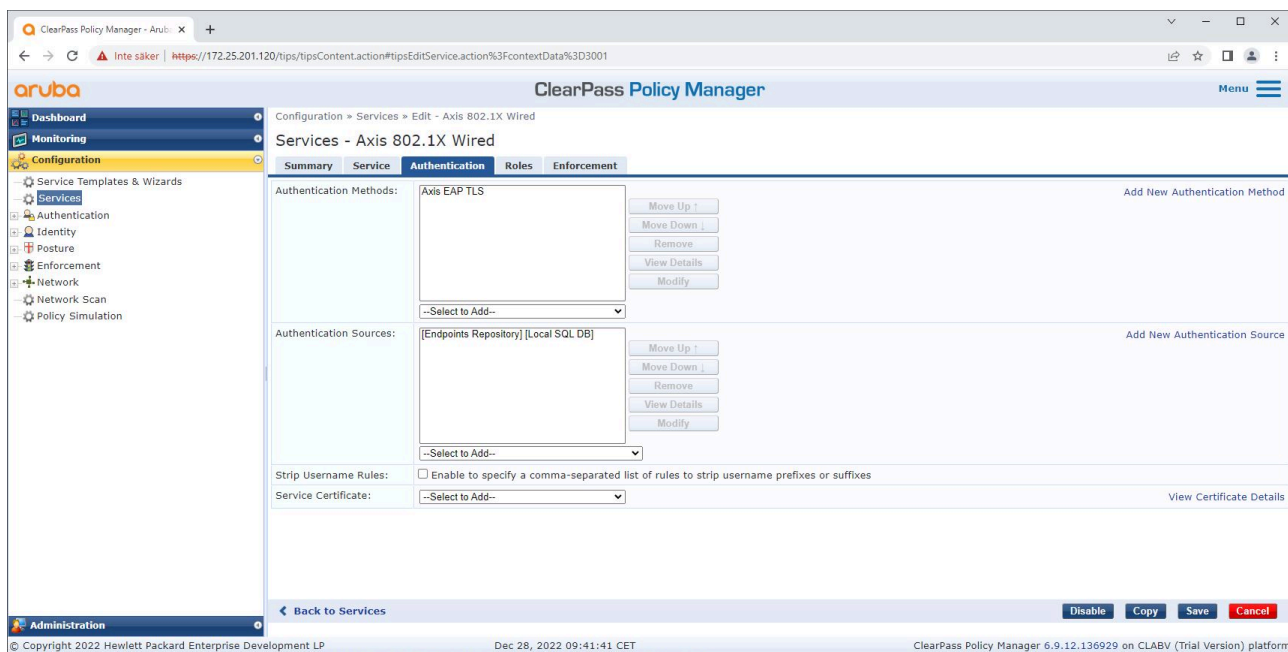
La interfaz del método de autenticación de ClearPass Policy Manager, donde se define el método de autenticación EAP-TLS para dispositivos Axis.

Configuración de servicio

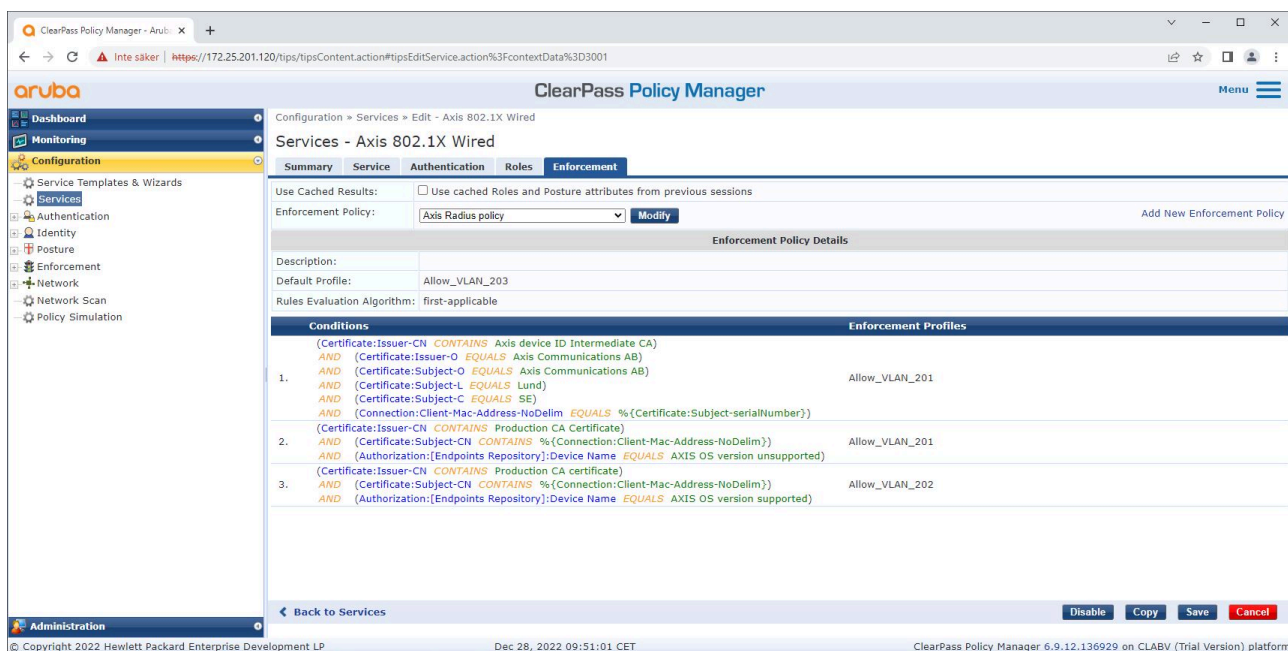
En la página Services (Servicios), los pasos de configuración se combinan en un solo servicio que maneja la autenticación y autorización de los dispositivos Axis en las redes de HPE Aruba Networking.



Se crea un servicio Axis específico con IEEE 802.1X como método de conexión.



Se configura el método de autenticación EAP-TLS creado anteriormente para el servicio.



Se configura la política de aplicación creada anteriormente 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, es preciso configurar el switch de acceso 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.

Nota

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

Este ejemplo muestra la configuración global y de puertos para los switches de acceso de HPE Aruba Networking.

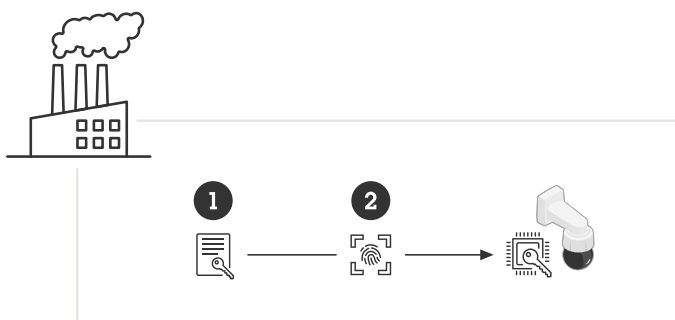
```
radius-server host MyRADIUSIPAddress key "MyRADIUSKey"
```

```
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
```

Configuración Axis

Dispositivo en red de Axis

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



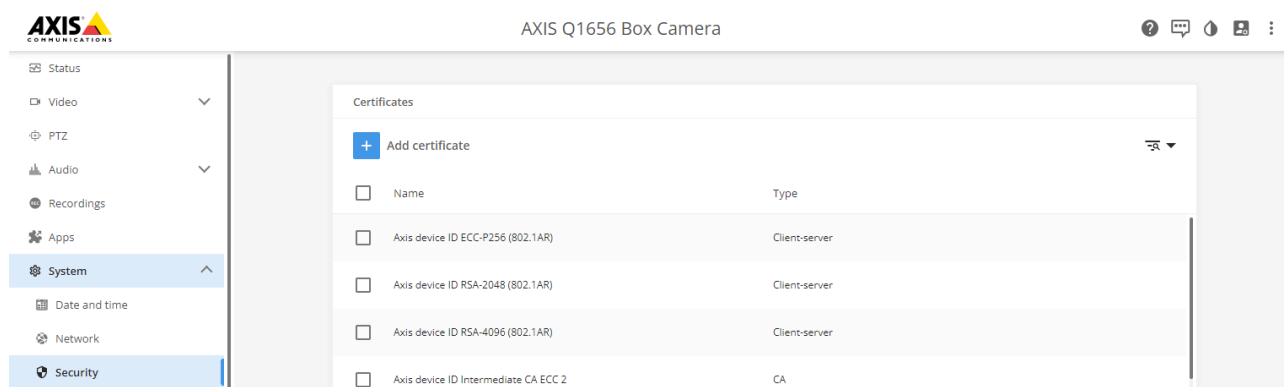
Los dispositivos Axis se fabrican con el certificado de identificación de dispositivo Axis compatible con IEEE 802.1AR para servicios de identidad de dispositivos confiables.

- 1 Infraestructura de clave de ID de dispositivo Axis (PKI)
- 2 ID de dispositivo de Axis

El almacén de claves seguro con protección por hardware, proporcionado por un elemento seguro del dispositivo Axis, se suministra configurado de fábrica con un certificado exclusivo del dispositivo y las claves correspondientes (ID del dispositivo Axis), que permiten demostrar globalmente la autenticidad del dispositivo Axis. *Axis Product Selector* permite encontrar qué dispositivos Axis son compatibles con *Axis Edge Vault* y el ID de dispositivo Axis.

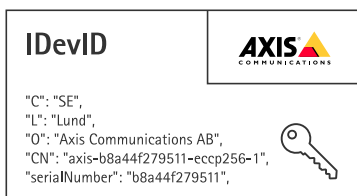
Nota

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



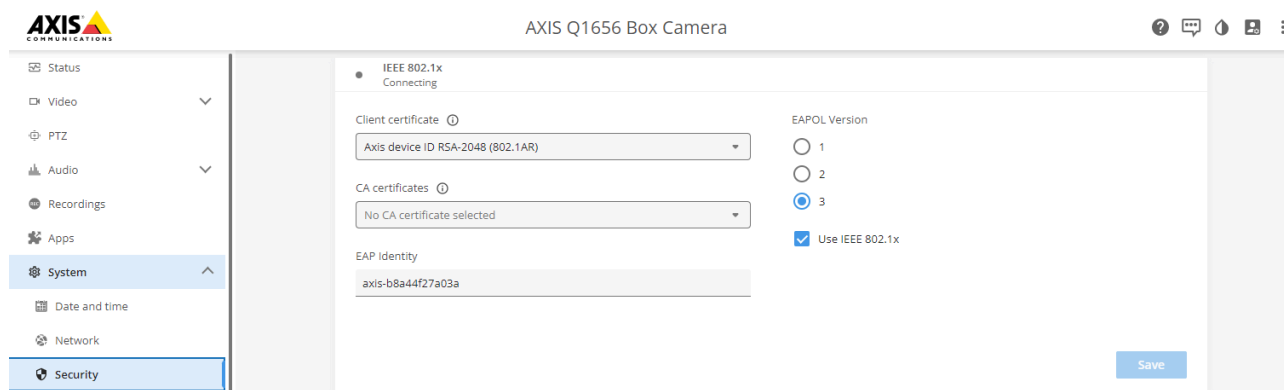
El almacén de certificados del dispositivo Axis en su estado predeterminado de fábrica, con el ID del dispositivo Axis.

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. Esta información es utilizada por ClearPass Policy Manager para realizar análisis y tomar decisiones para otorgar acceso a la red. La siguiente información se puede obtener de un certificado de identificación de dispositivo Axis.



País	SE
Establecimiento	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 compone del nombre de la empresa Axis, el número de serie del dispositivo y el algoritmo criptográfico (ECC P256, RSA 2048, RSA 4096). A partir de 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 se autentique en redes habilitadas para IEEE 802.1X.



Dispositivo Axis en 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 usar en la red para configurar y gestionar varios dispositivos Axis de forma rentable. *AXIS Device Manager* es una aplicación para Microsoft Windows® que se instala localmente en un equipo de la red, mientras que *AXIS Device Manager Extend* utiliza una infraestructura en la nube para la gestión de dispositivos en múltiples ubicaciones. Ambos ofrecen capacidades sencillas de gestión y configuración, como:

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

Operación de red segura: IEEE 802.1AE MACsec



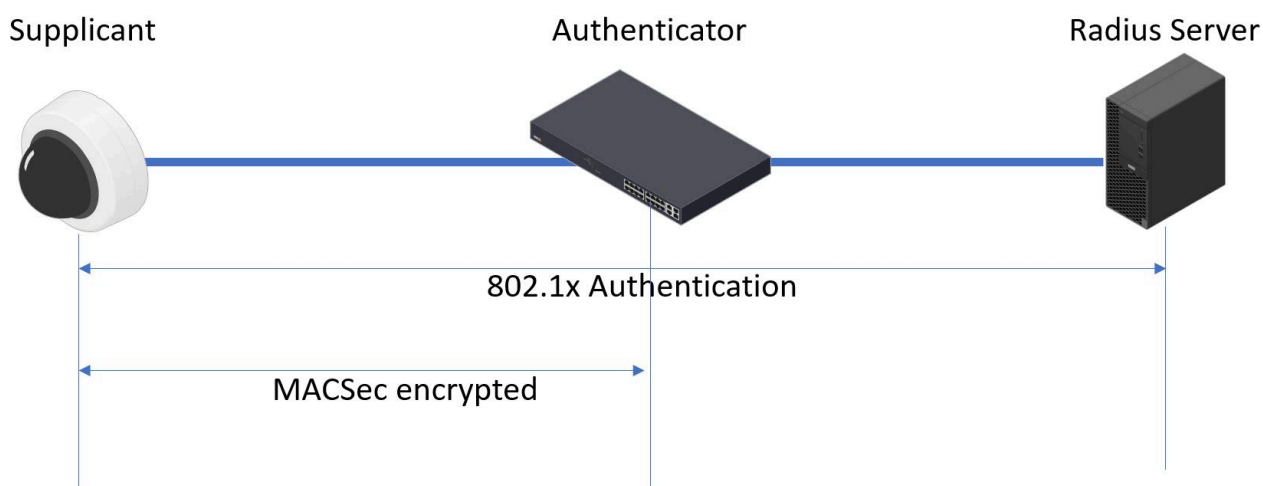
Para ver este vídeo, vaya a la versión web de este documento.

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

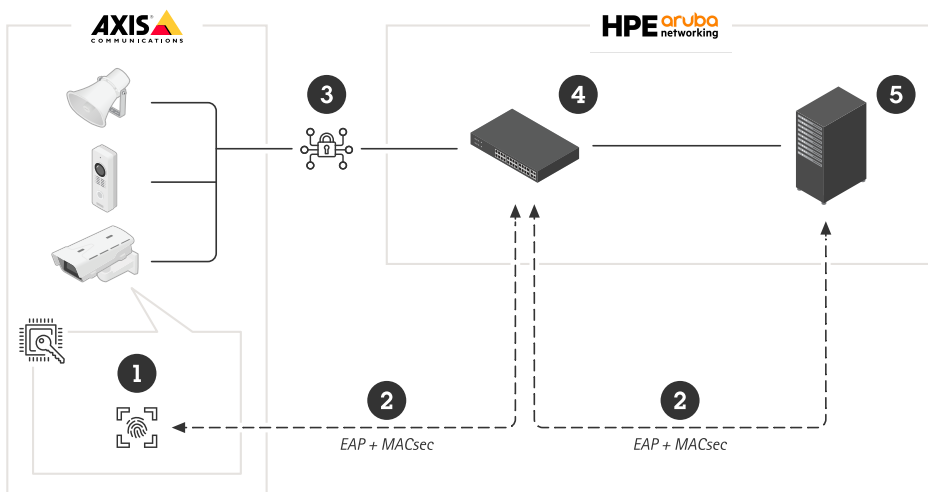
IEEE 802.1AE MACsec (Media Access Control Security) es un protocolo de red bien definido que protege criptográficamente los enlaces Ethernet punto a punto en la capa de red 2. Garantiza la confidencialidad y la integridad de las transmisiones de datos entre dos hosts.

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 versiones posteriores, IEEE 802.1X está habilitado de forma predeterminada para los dispositivos compatibles con la ID del dispositivo Axis. En AXIS OS 11.8 y versiones posteriores, se admite MACsec con modo dinámico automático mediante IEEE 802.1X EAP-TLS, que está 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 es correcta, 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) mediante el control de acceso a la red basado en el puerto 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.

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 left sidebar shows the navigation menu with options like Dashboard, Monitoring, Configuration, Authentication, Identity, Posture, Enforcement, Network, and Administration. The main content area is titled 'Roles' and shows a list of roles. An 'Edit Role' dialog box is open, showing the following details:

- Role ID: 3001
- Name: AxisDevice
- Description: (empty text area)

The background table lists roles with columns for #, Name, and Description. The roles listed include [AirGroup v1], [AirGroup v2], [Aruba TACACS+ read-only Admin], [Aruba TACACS+ root Admin], [AxisDevice], [BYOD], [Contract], [Device], [Employee], [Guest], [MAC Ca], [Onboard], [Onboard iOS], [Onboard iPadOS], [Onboard Linux], [Onboard macOS], [Onboard Windows], [Other], and [TACACS+ API Admin].

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.

Configuration » Identity » Role Mappings » Edit - Axis Role Mapping

Role Mappings - Axis Role Mapping

Summary Policy Mapping Rules

Policy:

Policy Name: Axis Role Mapping

Description:

Default Role: [Guest]

Mapping Rules:

Rules Evaluation Algorithm: Evaluate all

Conditions	Role Name
1. (Authentication:Full-Username BEGINS_WITH axis-00408c)	AxisDevice
2. (Authentication:Full-Username BEGINS_WITH axis-acc8e)	AxisDevice
3. (Authentication:Full-Username BEGINS_WITH axis-b8a44f)	AxisDevice

Back to Role Mappings Copy Save Cancel

Copyright 2023 Hewlett Packard Enterprise Development LP Oct 26, 2023 05:08:20 UTC ClearPass Policy Manager 6.11.2.252294 on CLABV (Trial Version) platform

Añada una política de asignación de roles de Axis para el rol de dispositivo 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].

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

Configuración de servicio

Configuration » Services » Edit - Axis 802.1X Wired

Services - Axis 802.1X Wired

Summary Service Authentication Roles Enforcement

Role Mapping Policy: Axis Role Mapping Modify Add New Role Mapping Policy

Role Mapping Policy Details

Description:

Default Role: [Guest]

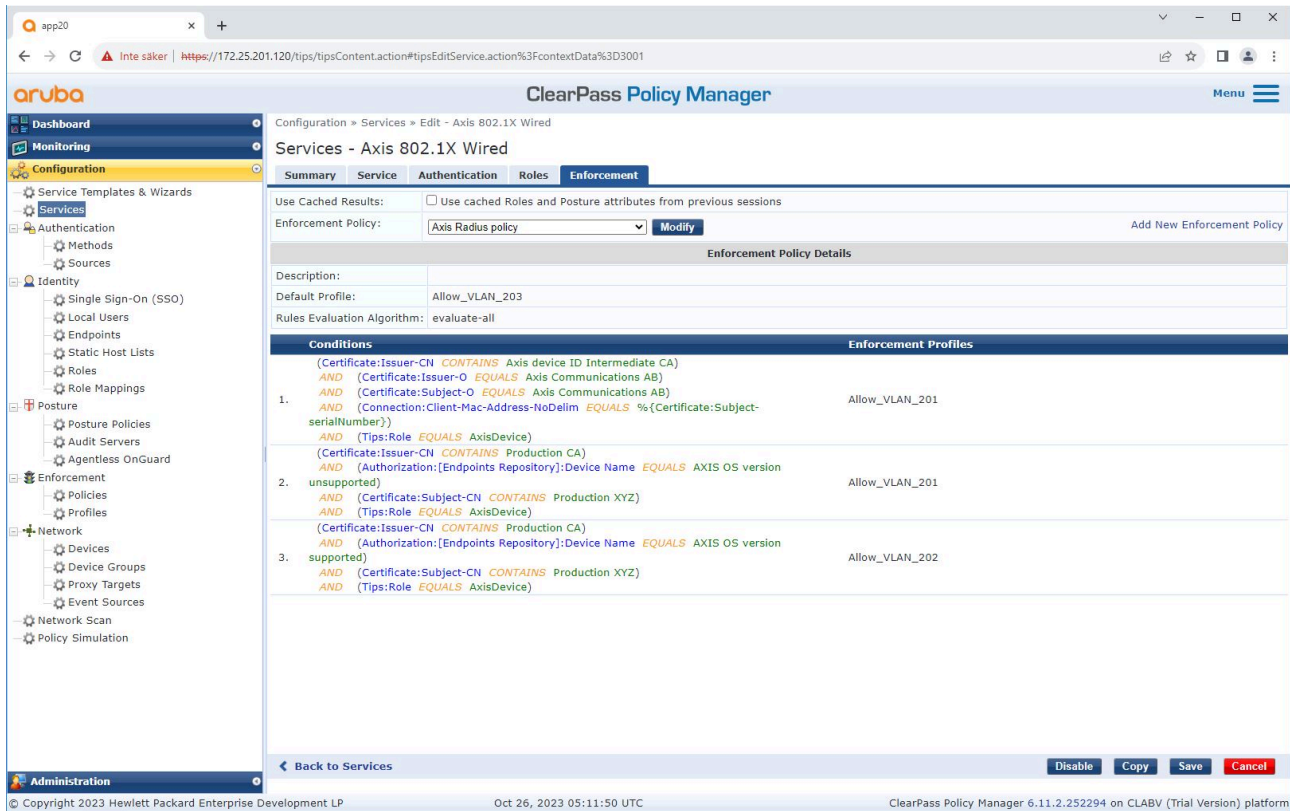
Rules Evaluation Algorithm: evaluate-all

Conditions	Role
1. (Authentication:Full-Username BEGINS_WITH axis-00408c)	AxisDevice
2. (Authentication:Full-Username BEGINS_WITH axis-acc8e)	AxisDevice
3. (Authentication:Full-Username BEGINS_WITH axis-b8a44f)	AxisDevice

Back to Services Disable Copy Save Cancel

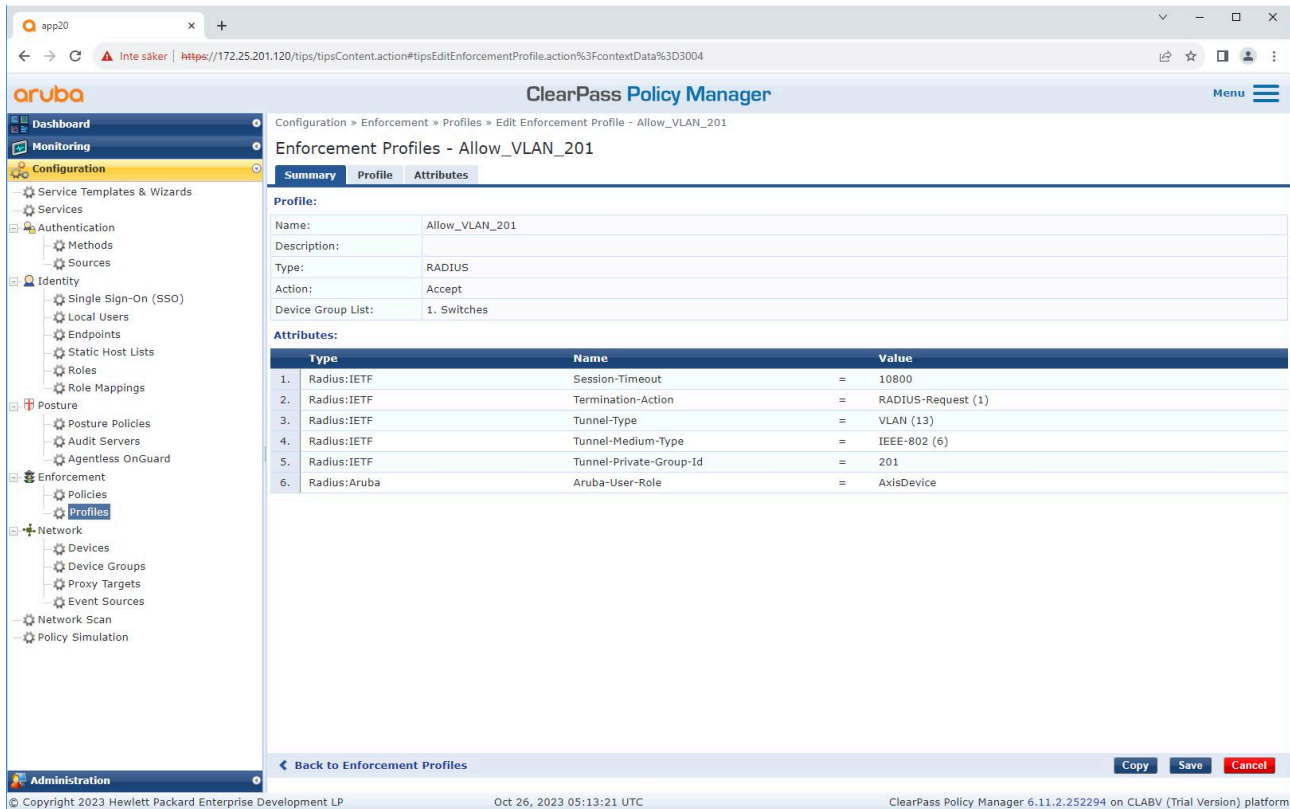
Copyright 2023 Hewlett Packard Enterprise Development LP Oct 26, 2023 05:09:16 UTC ClearPass Policy Manager 6.11.2.252294 on CLABV (Trial Version) platform

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



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

Perfil de cumplimiento



Añada el nombre de la función de Axis como un 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-eapcipher-suite gcm-aes-128
port-access role AxisDeviceassociate macsec-policy macsec-eapauth-mode client-mode
aaa authentication port-access dot1x authenticatormacsecmkacak-length 16enable
```

Incorporación heredada: autenticación MAC

Puede utilizar MAC Authentication Bypass (MAB) para incorporar dispositivos Axis que no admiten la incorporación IEEE 802.1AR con el certificado de identificación de dispositivo Axis y con 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. No es preciso realizar ninguna configuración en el dispositivo Axis para permitir la incorporación integrada 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.

The screenshot shows the Aruba ClearPass Policy Manager interface. The left sidebar contains navigation menus for Dashboard, Monitoring, Configuration, and Administration. The main content area is titled 'Services - Axis 802.1X Wired - Mac Authentication' and includes tabs for Summary, Service, Authentication, Roles, and Enforcement. The 'Enforcement' tab is active, displaying the 'Enforcement Policy Details' for the 'Axis MAC Authentication Policy'. The policy is configured with 'Use Cached Results' and 'Use cached Roles and Posture attributes from previous sessions' both unchecked. The 'Enforcement Policy Details' section shows a 'Description' field, a 'Default Profile' set to '[Deny Access Profile]', and a 'Rules Evaluation Algorithm' set to 'evaluate-all'. Below this, a table lists the enforcement profiles and their conditions:

Conditions	Enforcement Profiles
1. (Date:Day-of-Week BELONGS_TO Monday, Tuesday, Wednesday, Thursday, Friday) AND (Date:Time-of-Day IN_RANGE 09:00:00,17:00:00) AND (Connection:Client-Mac-Vendor EQUALS Axis Communications AB)	Allow_VLAN_203

At the bottom of the interface, there are buttons for 'Back to Services', 'Enable', 'Copy', 'Save', and 'Cancel'. The footer indicates the copyright is © Copyright 2023 Hewlett Packard Enterprise Development LP, the date is Oct 26, 2023 05:15:57 UTC, and the version is ClearPass Policy Manager 6.11.2.252294 on CLABV (Trial Version) platform.

Acceso denegado a la red

Si el dispositivo Axis no cumple con la política de aplicación configurada, se le denegará 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:

- El día es uno laborable, de lunes a viernes.
- La hora está comprendida entre las 09:00 y las 17:00.
- El proveedor de la dirección MAC coincide con Axis Communications.

Dado que es posible suplantar una dirección MAC, no se concede acceso a la red de aprovisionamiento habitual. Le recomendamos utilizar MAB únicamente para la incorporación inicial y, posteriormente, inspeccionar 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 image displays two screenshots of the ClearPass Policy Manager web interface, showing the configuration of authentication sources.

Top Screenshot: Authentication Sources List

The interface shows the 'Authentication Sources' page. A table lists 11 sources:

#	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

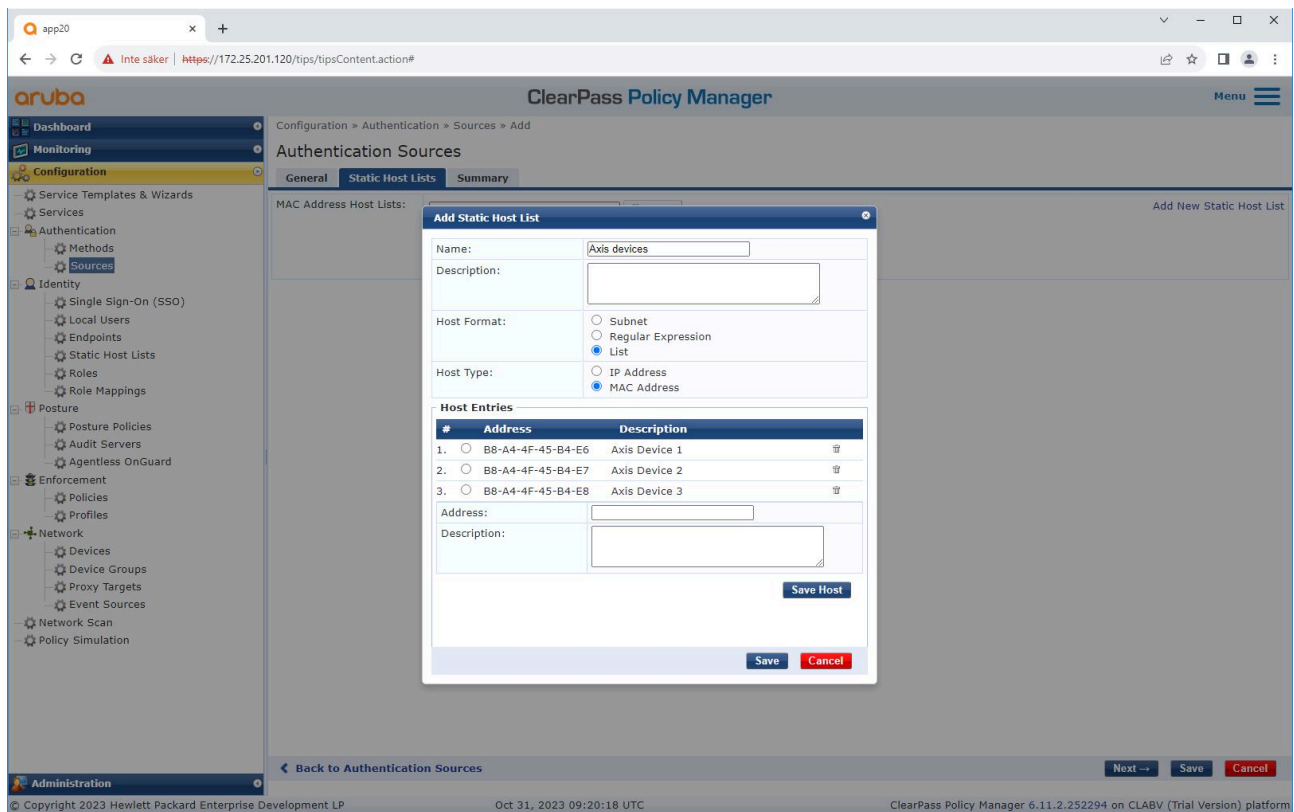
Showing 1-11 of 11

Bottom Screenshot: Add Authentication Source Form

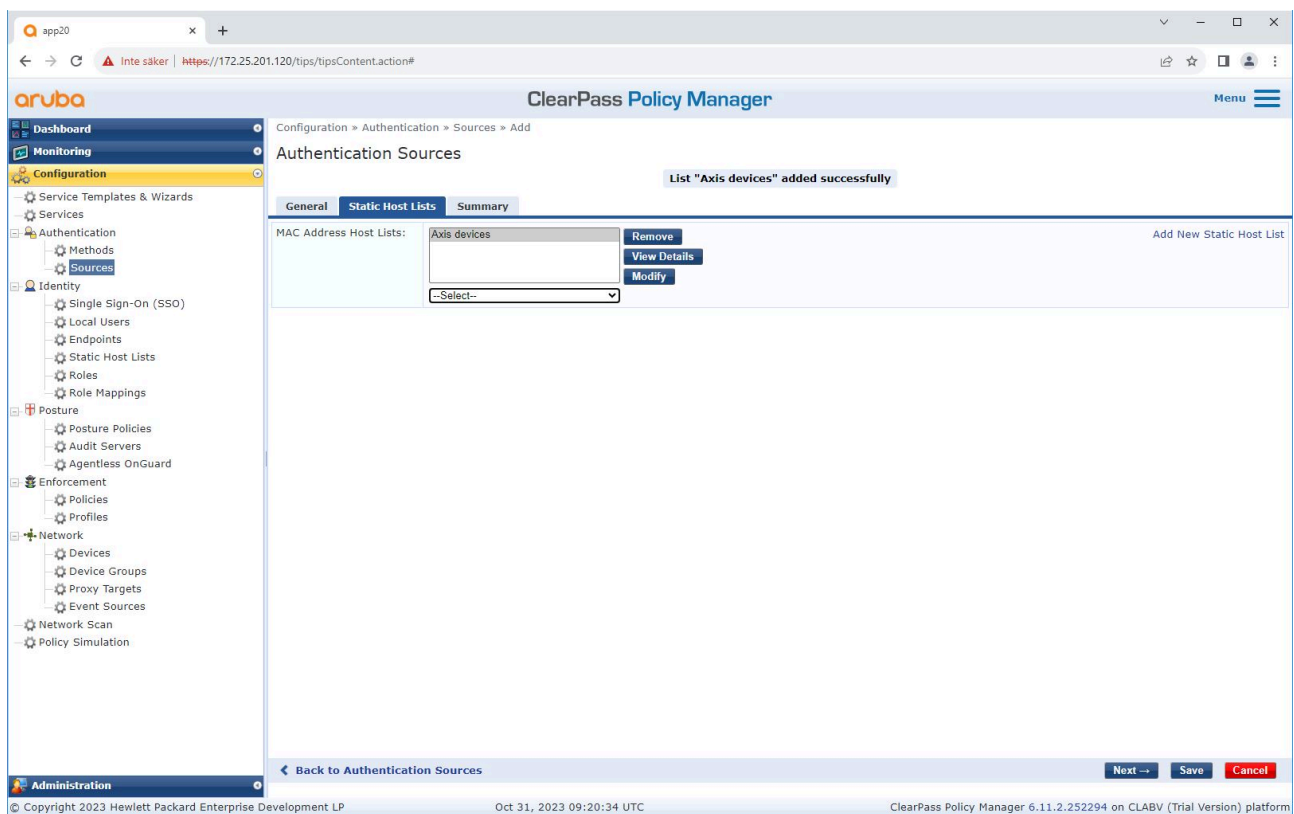
The interface shows the 'Add Authentication Source' form. The fields are:

- 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: (Empty list)

Buttons: Back to Authentication Sources, Next, Save, Cancel



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

app20

Inte saker | https://172.25.201.120/tips/tipsContent.action#tipsServices.action

aruba

ClearPass Policy Manager

Menu

Dashboard

Monitoring

Configuration

Administration

Service Templates & Wizards

Services

Authentication

Identity

Posture

Enforcement

Network

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	✓
2.	☐	2	Axis 802.1X Wired - Mac Authentication	RADIUS	MAC Authentication	0	✓
3.	☐	3	Test_Service	RADIUS	802.1X Wired	0	✗
4.	☐	4	[Policy Manager Admin Network Login Service]	TACACS+	TACACS+ Enforcement	0	✗
5.	☐	5	[AirGroup Authorization Service]	RADIUS	RADIUS Enforcement (Generic)	0	✗
6.	☐	6	[Aruba Device Access Service]	TACACS+	TACACS+ Enforcement	0	✗
7.	☐	7	[Guest Operator Logins]	Application	Aruba Application Authentication	0	✗
8.	☐	8	[Insight Operator Logins]	Application	Aruba Application Authentication	0	✗
9.	☐	9	[Device Registration Disconnect]	WEBAUTH	Web-based Authentication	0	✗

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

app20

Inte saker | https://172.25.201.120/tips/tipsContent.action#tipsEditService.action%3FcontextData%3D30006

aruba

ClearPass Policy Manager

Menu

Dashboard

Monitoring

Configuration

Administration

Service Templates & Wizards

Services

Authentication

Identity

Posture

Enforcement

Network

Configuration > Services > Edit - Axis 802.1X Wired - Mac Authentication

Services - Axis 802.1X Wired - Mac Authentication

Summary Service Authentication Roles Enforcement

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

Service Rule

Matches ANY or 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...		

Back to Services Enable Copy Save Cancel

Copyright 2023 Hewlett Packard Enterprise Development LP

Oct 26, 2023 05:15:11 UTC

ClearPass Policy Manager 6.11.2.252294 on CLABV (Trial Version) platform

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

Configuration » Services » Edit - Axis 802.1X Wired - Mac Authentication

Services - Axis 802.1X Wired - Mac Authentication

Summary Service Authentication Roles Enforcement

Authentication Methods: [Allow All MAC AUTH] Add New Authentication Method

Authentication Sources: Axis Devices [Static Host List] Add New Authentication Source

Strip Username Rules: ☐ Enable to specify a comma-separated list of rules to strip username prefixes or suffixes

Back to Services Disable Copy Save Cancel

Copyright 2023 Hewlett Packard Enterprise Development LP Oct 31, 2023 09:22:22 UTC ClearPass Policy Manager 6.11.2.252294 on CLABV (Trial Version) platform

El método de autenticación MAC preconfigurado está configurado para el servicio. Además, se selecciona la fuente de autenticación (creada anteriormente) 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

Configuration » Services » Edit - Axis 802.1X Wired - Mac Authentication

Services - Axis 802.1X Wired - Mac Authentication

Summary Service Authentication Roles Enforcement

Use Cached Results: ☐ Use cached Roles and Posture attributes from previous sessions

Enforcement Policy: Axis MAC Authentication Policy Modify Add New Enforcement Policy

Enforcement Policy Details

Description:

Default Profile: [Deny Access Profile]

Rules Evaluation Algorithm: evaluate-all

Conditions	Enforcement Profiles
1. (Date:Day-of-Week BELONGS_TO Monday, Tuesday, Wednesday, Thursday, Friday) AND (Date:Time-of-Day IN_RANGE 09:00:00,17:00:00) AND (Connection:Client-Mac-Vendor EQUALS Axis Communications AB)	Allow_VLAN_203

Back to Services Enable Copy Save Cancel

Copyright 2023 Hewlett Packard Enterprise Development LP Oct 26, 2023 05:15:57 UTC ClearPass Policy Manager 6.11.2.252294 on CLABV (Trial Version) platform

En el último paso, se configura la política de aplicación creada anteriormente 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 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_es

2025-11 (M7.2)

© 2023 – 2025 Axis Communications AB