Secure integration of Axis devices into Aruba networks

Manual del usuario

Índice

Secure integration of Axis devices into Aruba networks

Introducción

Introducción

Esta guía de integración tiene como objetivo describir la configuración de mejores prácticas sobre cómo incorporar y operar dispositivos Axis en redes de Aruba. 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 equipos y aplicaciones de red de Aruba. A continuación se detallan algunos de los beneficios que se pueden obtener al combinar dispositivos y software de Axis con una infraestructura de red de Aruba:

- 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 Aruba 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 la infraestructura de TI de la red empresarial de Aruba, incluidos los conmutadores de acceso de Aruba y Aruba ClearPass Policy Manager.
- 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 proporcionarán a lo largo de la guía.

Incorporación segura: IEEE 802.1AR/802.1X

Autenticación inicial

Conecte el dispositivo Axis compatible con Axis Edge Vault para autenticar el dispositivo en la red de Aruba. El dispositivo utilizará 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, Aruba 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 firmware en ejecución, se utiliza para tomar una decisión basada en políticas.

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

El dispositivo Axis se autentica en la red de Aruba 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, la red de Aruba moverá el dispositivo Axis a la red de aprovisionamiento (VLAN201) donde 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 firmware. 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 activará un nuevo intento de autenticación. Aruba ClearPass Policy Manager verificará los nuevos certificados y decidirá si mueve el dispositivo Axis a la red de producción o no.

Después de la configuración del dispositivo, el dispositivo Axis abandonará la red de aprovisionamiento e intentará volver a autenticarse en la red de Aruba.

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 conectará al dispositivo Axis y comenzará 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*

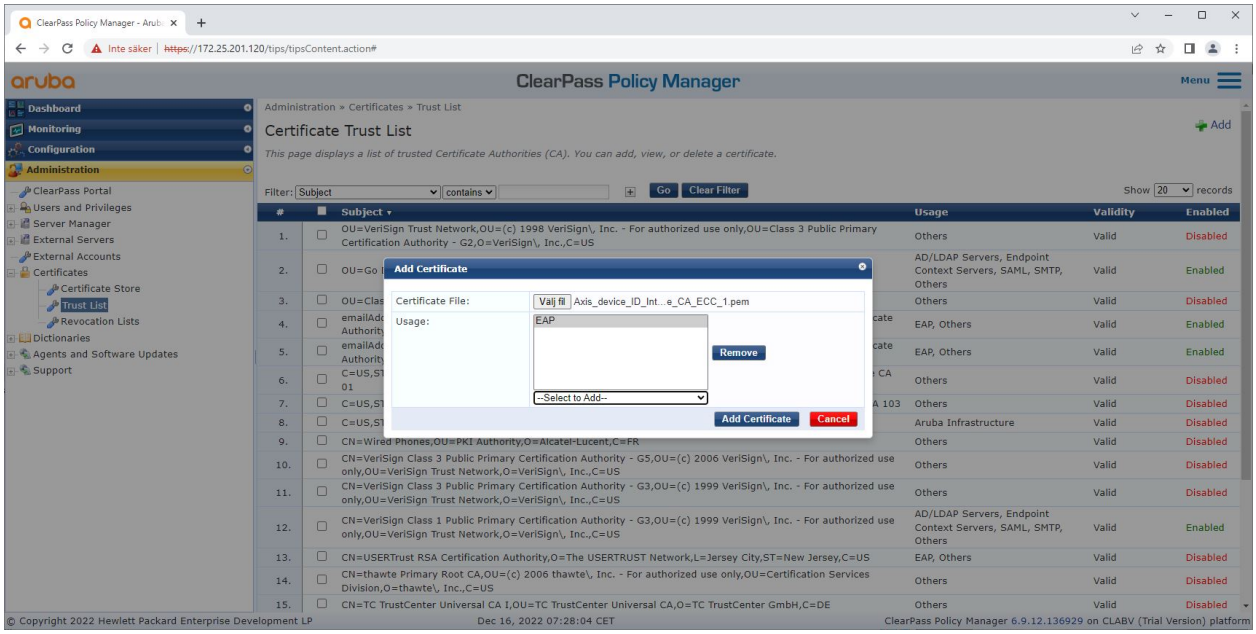
Configuration HPE Aruba

Aruba ClearPass Policy Manager

ClearPass Policy Manager de Aruba 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.

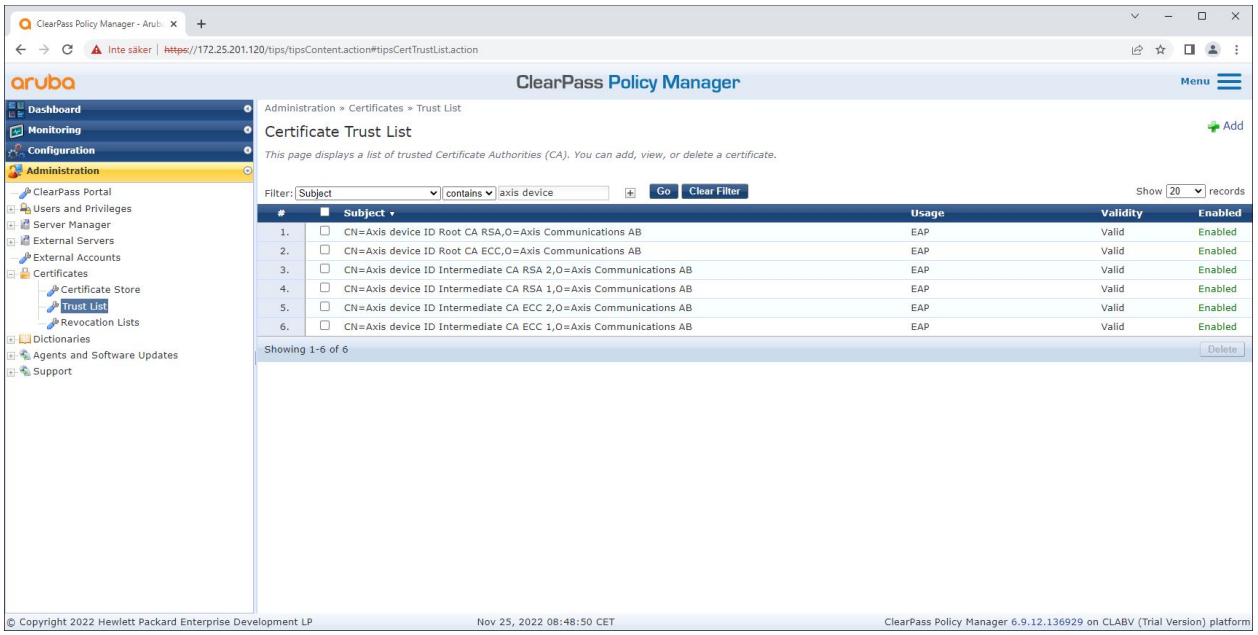
Configuración del almacén de certificados de confianza

1. Descargue la cadena de certificados IEEE 802.1AR específica de Axis desde axis.com.
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 Aruba 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 utilizarán para la autenticación IEEE 802.1X EAP-TLS.



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

Incorporación segura: IEEE 802.1AR/802.1X



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

Configuración de dispositivo/grupo de red

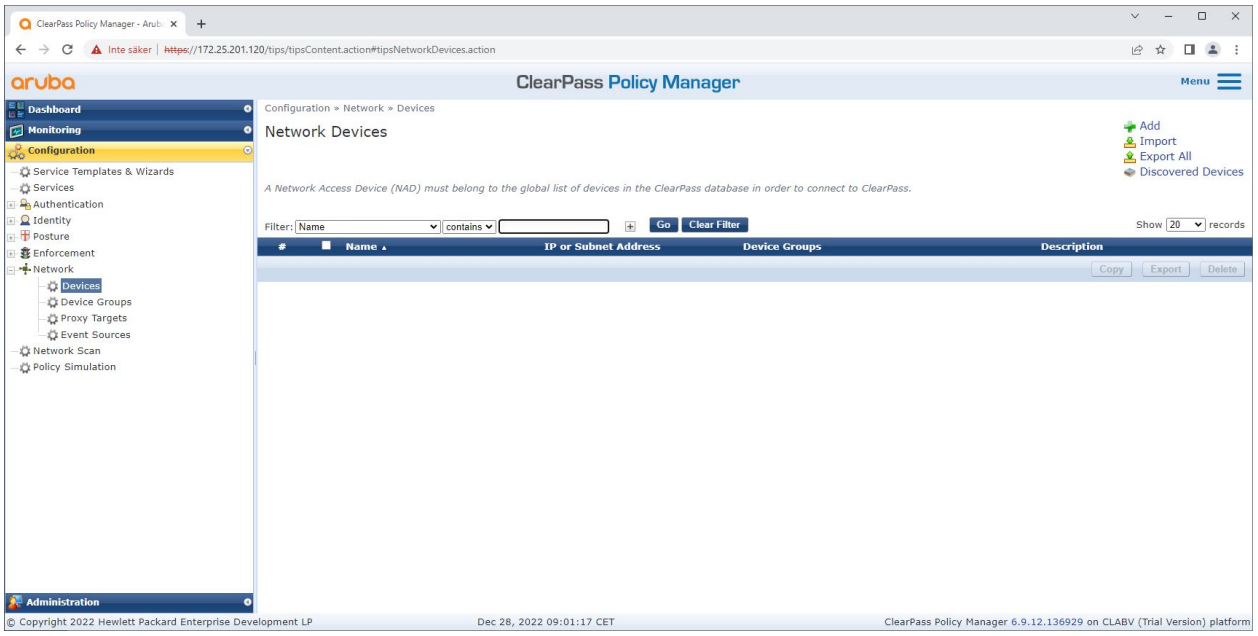
1. Agregue dispositivos de acceso a la red confiables, como switches de acceso de Aruba, al ClearPass Policy Manager. ClearPass Policy Manager necesita saber qué switches de acceso de Aruba en la red se utilizarán para la comunicación IEEE 802.1X.

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.

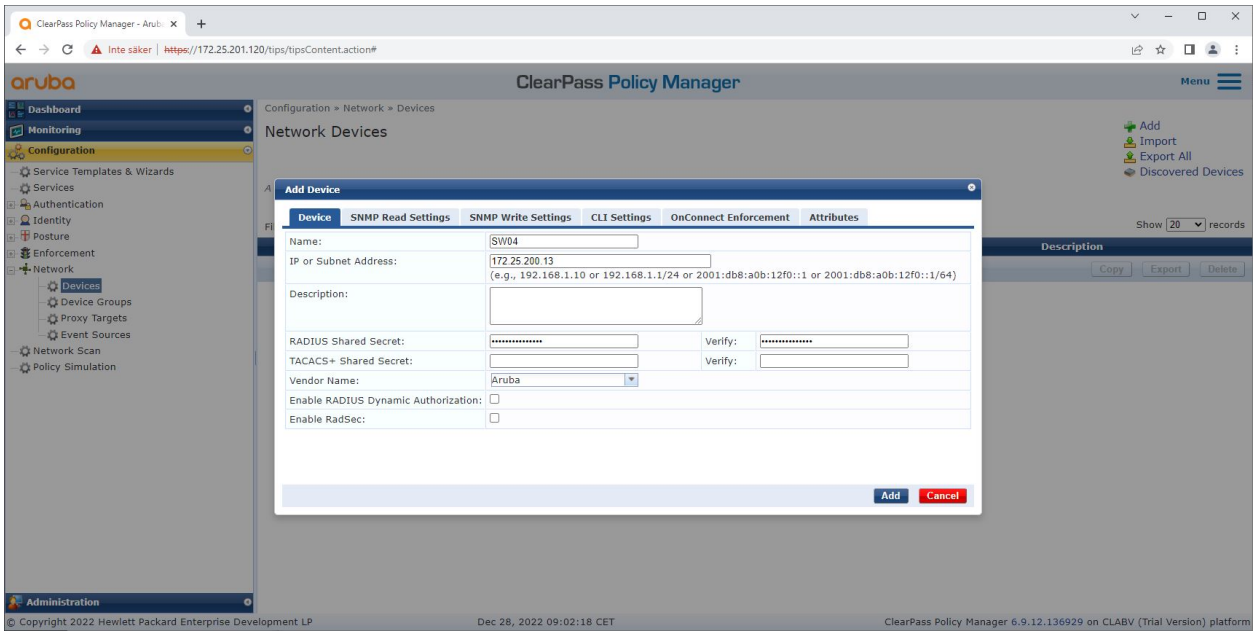
3. El secreto compartido de RADIUS debe coincidir con la configuración específica del conmutador IEEE 802.1X.

Secure integration of Axis devices into Aruba networks

Incorporación segura: IEEE 802.1AR/802.1X



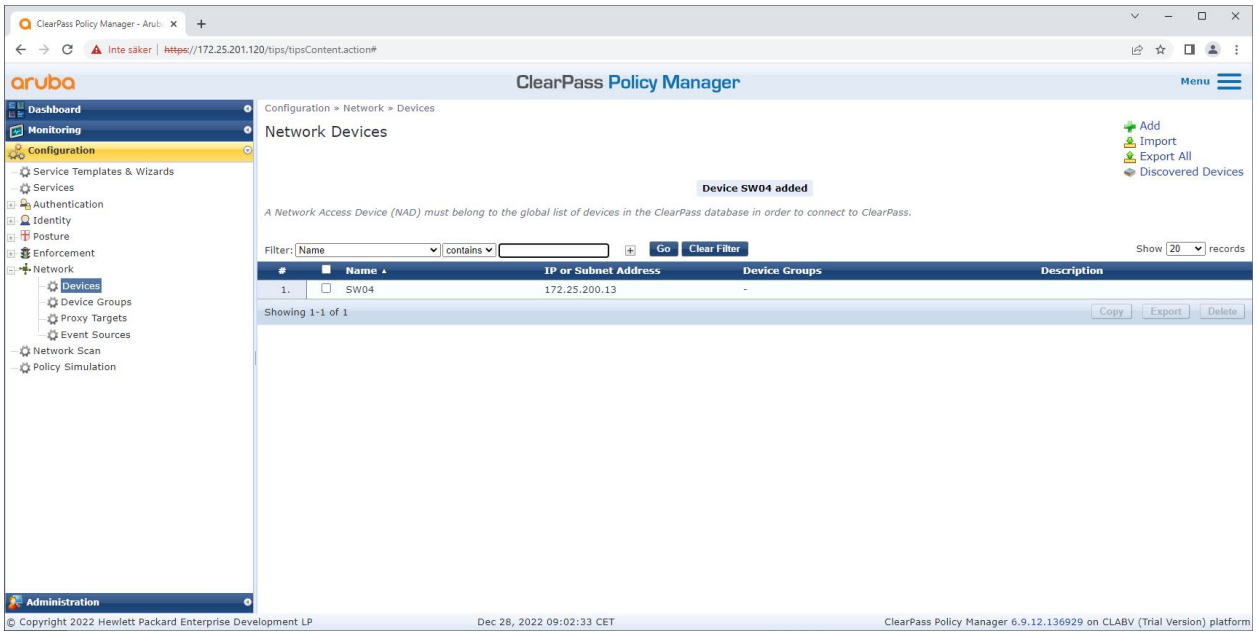
La interfaz de dispositivos de red confiables en Aruba ClearPass Policy Manager.



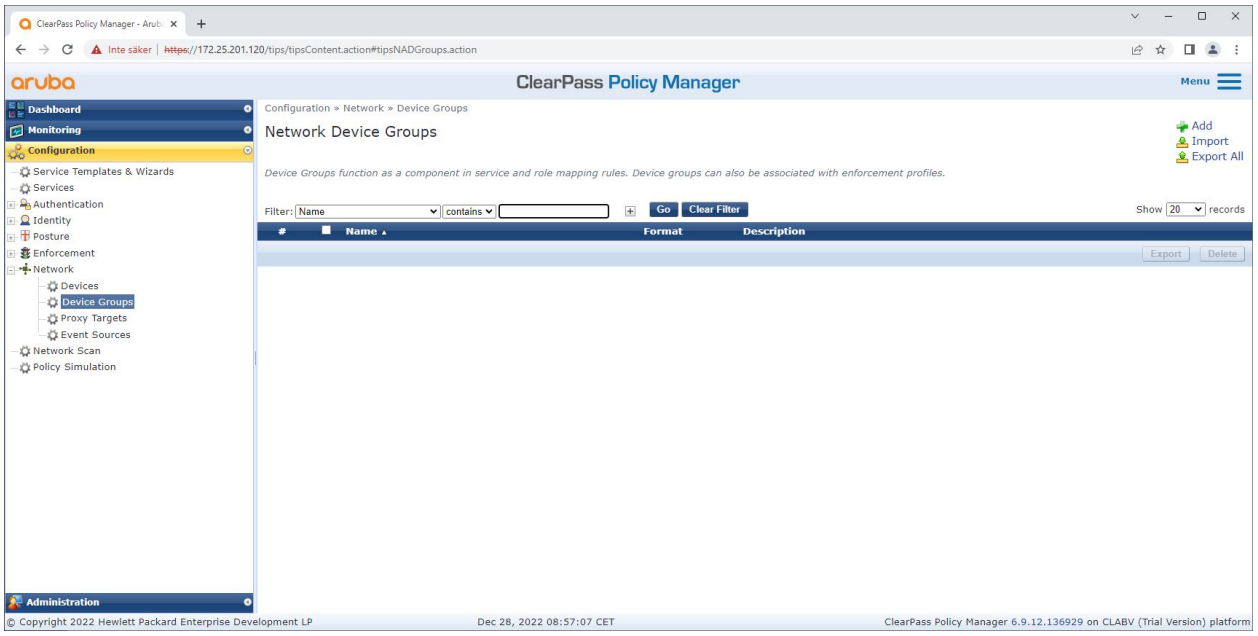
Agregar el conmutador de acceso de Aruba como dispositivo de red confiable en Aruba ClearPass Policy Manager. Tenga en cuenta que el secreto compartido de RADIUS debe coincidir con la configuración específica del switch IEEE 802.1X.

Secure integration of Axis devices into Aruba networks

Incorporación segura: IEEE 802.1AR/802.1X

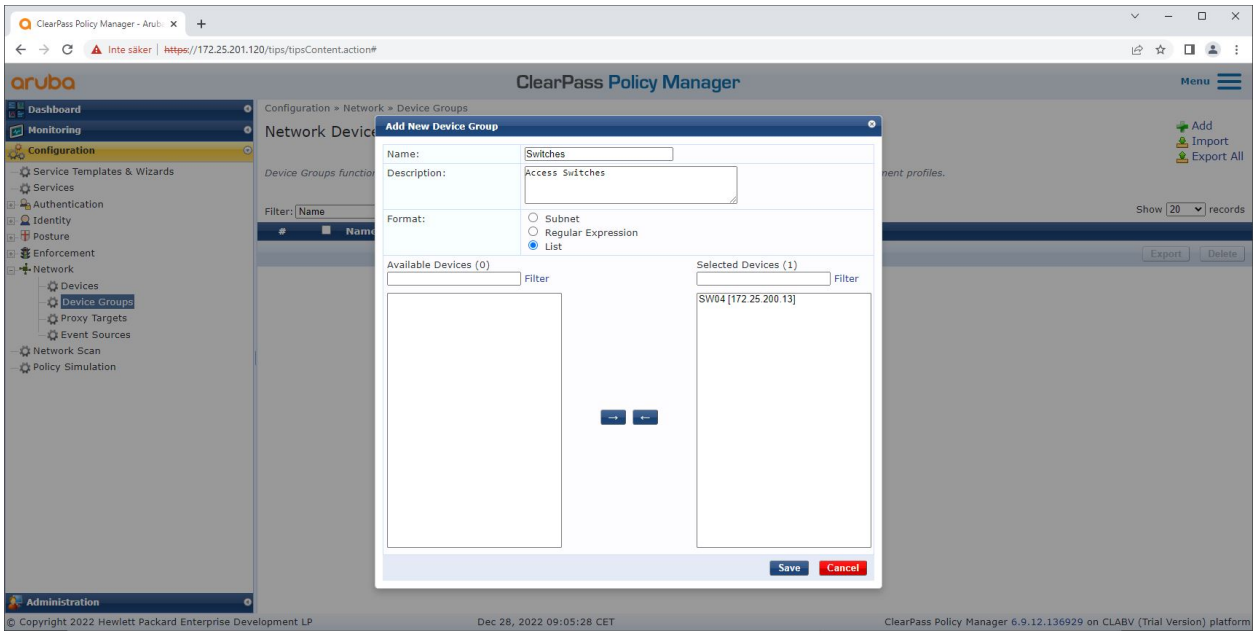


Aruba ClearPass Policy Manager con un dispositivo de red confiable configurado.

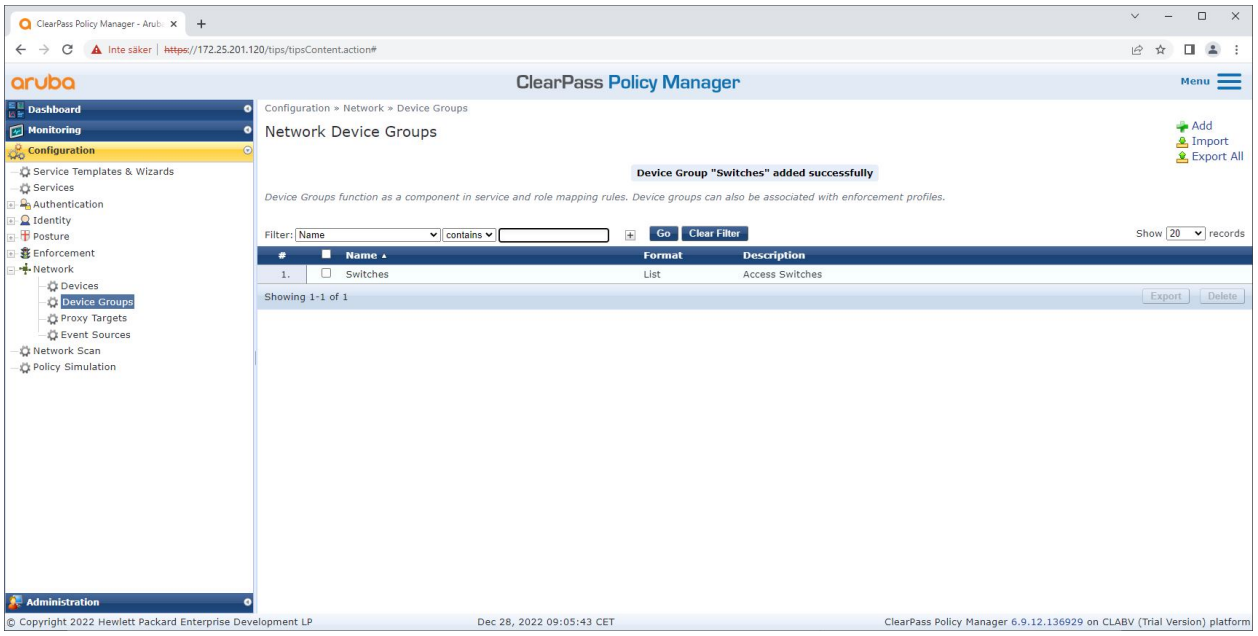


La interfaz de grupos de dispositivos de red confiables en Aruba ClearPass Policy Manager.

Incorporación segura: IEEE 802.1AR/802.1X



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



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

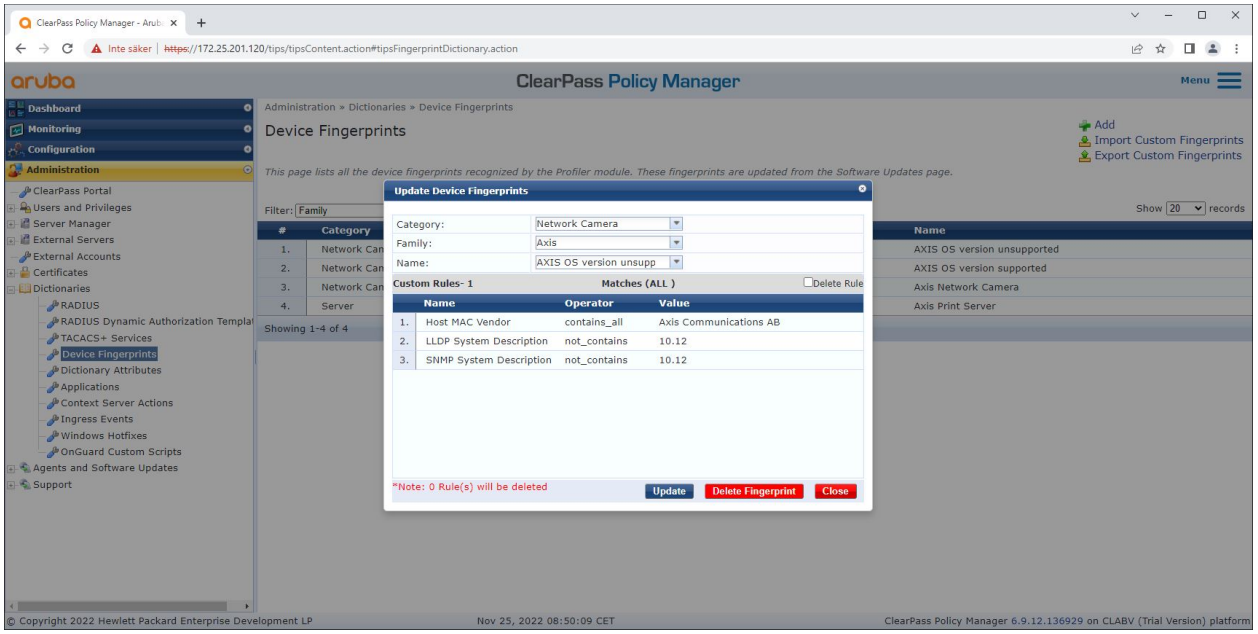
Configuración de huellas digitales del dispositivo

El dispositivo Axis puede distribuir información específica del dispositivo, como la dirección MAC y la versión del firmware, a través de la detección de red. Se puede crear una huella digital del dispositivo desde la interfaz de huellas digitales del dispositivo en Aruba ClearPass Policy Manager. Es posible actualizar y administrar la huella digital del dispositivo. Una de las cosas que es posible hacer es otorgar o denegar el acceso según la versión del sistema operativo AXIS.

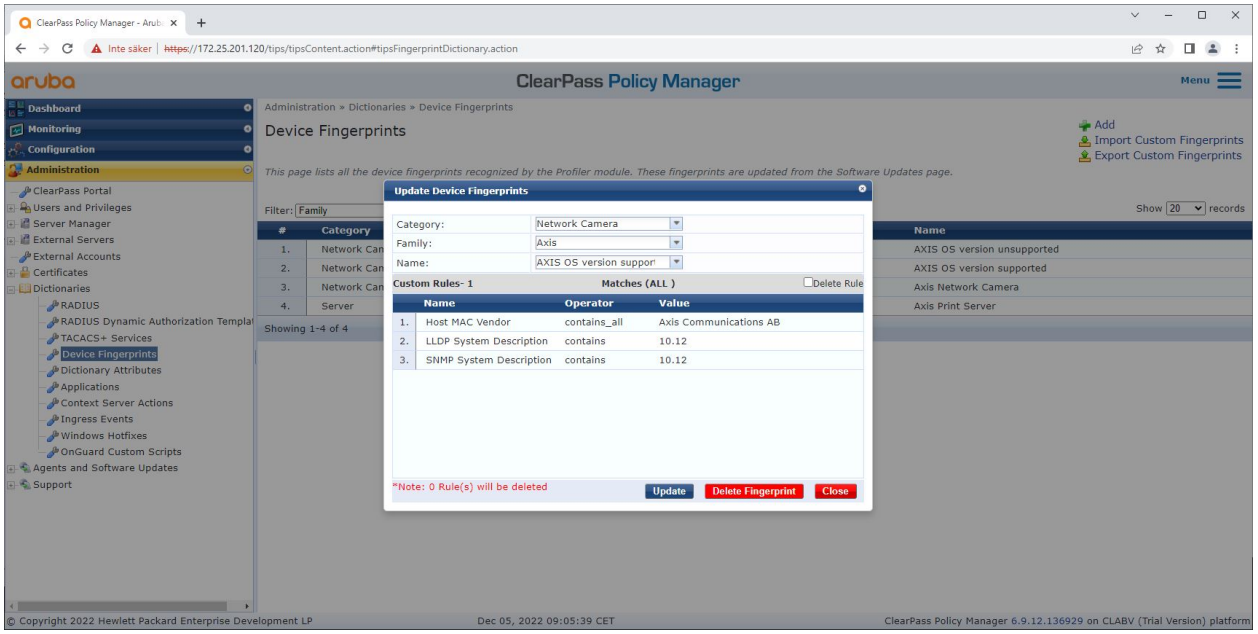
Es posible actualizar y administrar la huella digital del dispositivo. Una de las cosas que es posible hacer es otorgar o denegar el acceso según la versión del sistema operativo AXIS.

Incorporación segura: IEEE 802.1AR/802.1X

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. Establezca la configuración de huellas digitales del dispositivo.



La configuración de huellas digitales del dispositivo en Aruba ClearPass Policy Manager. Los dispositivos Axis que ejecutan cualquier otra versión de firmware distinta a la 10.12 se consideran no compatibles.



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

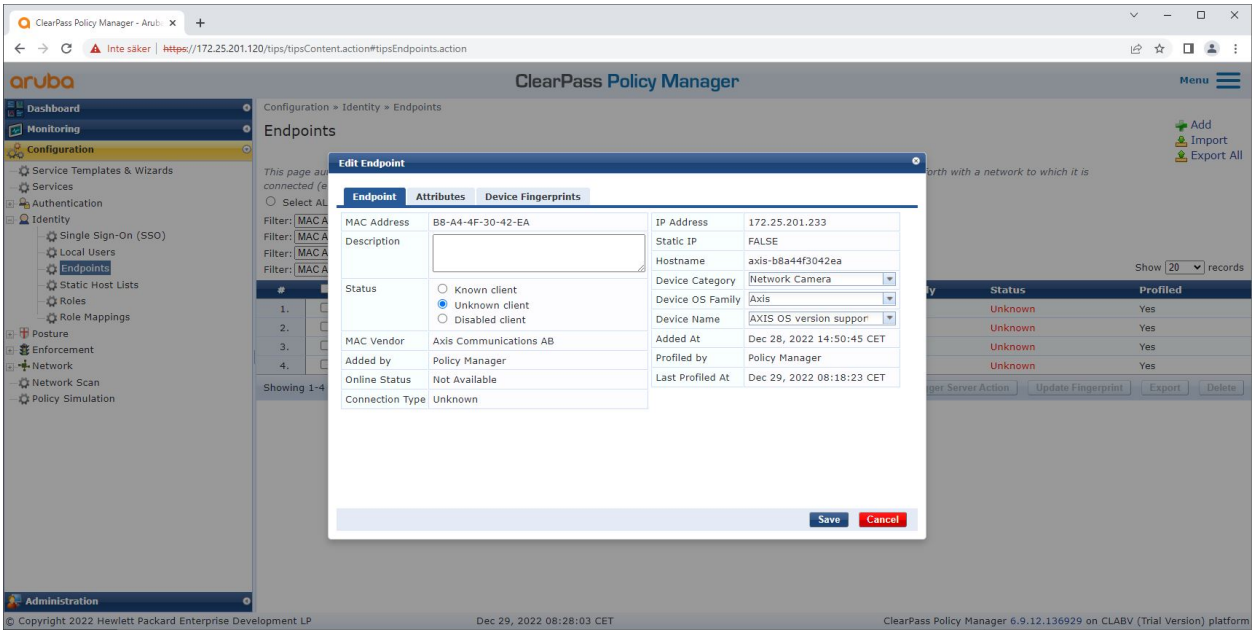
Incorporación segura: IEEE 802.1AR/802.1X

La información sobre la huella digital del dispositivo recopilada por Aruba ClearPass 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).

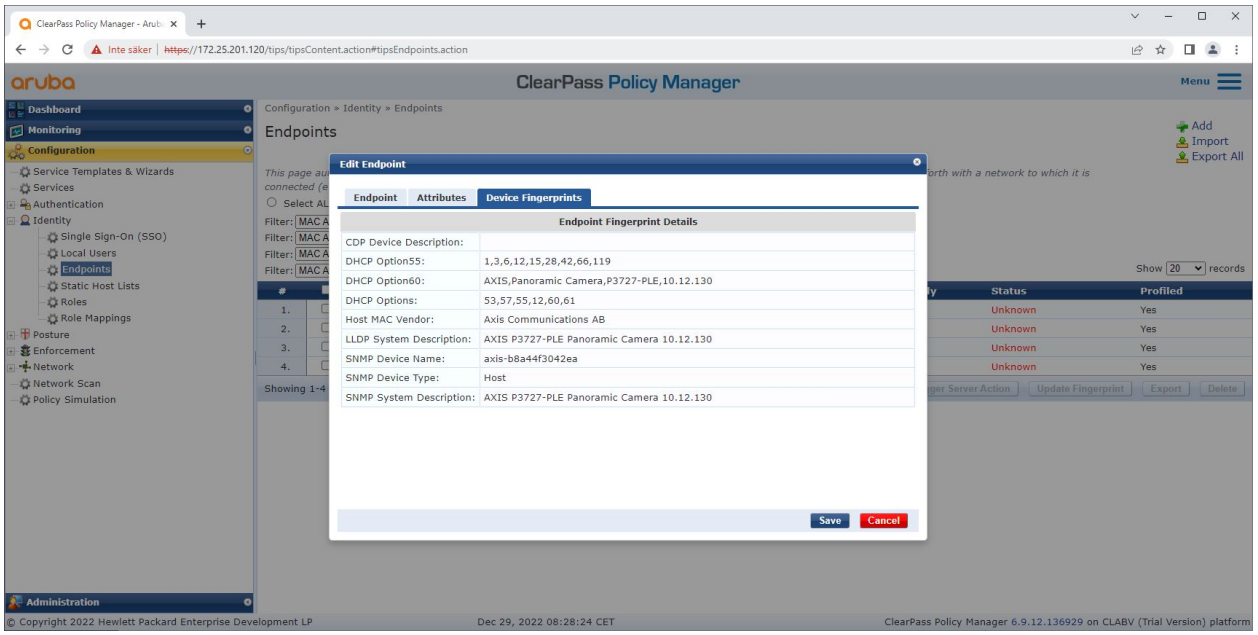
Nota

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



Un dispositivo Axis cuyo perfil ha sido perfilado por Aruba ClearPass Policy Manager.

Incorporación segura: IEEE 802.1AR/802.1X



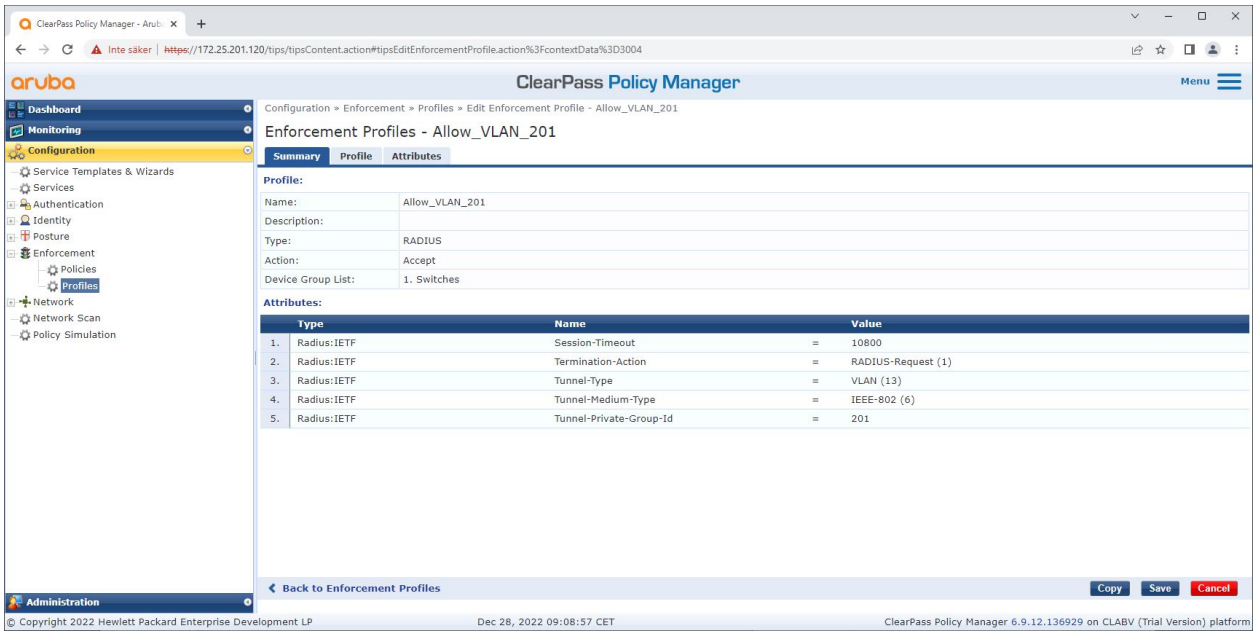
Las huellas dactilares detalladas del dispositivo de un dispositivo Axis perfilado. Tenga en cuenta que SNMP está deshabilitado de forma predeterminada en los dispositivos Axis. La información de detercción específica de LLDP, CDP y DHCP es compartida por el dispositivo Axis en el estado predeterminado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

Configuración del perfil de cumplimiento

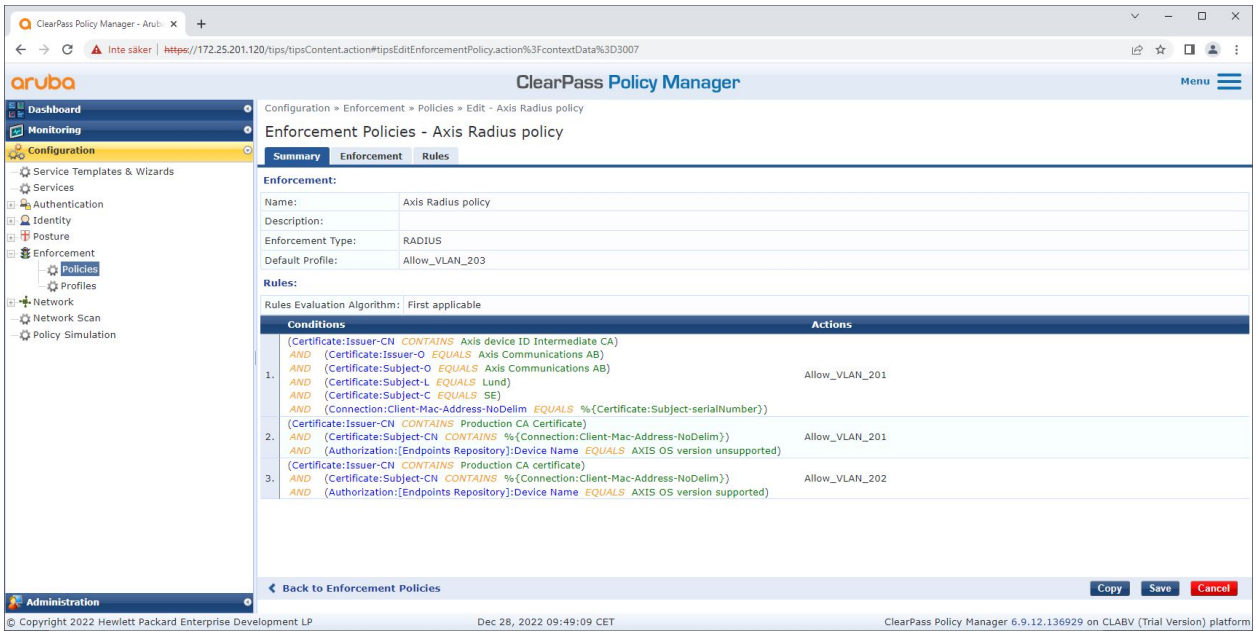
El perfil de cumplimiento se utiliza para permitir que Aruba ClearPass Policy Manager asigne una ID de VLAN específica a un puerto de acceso en el switch. Es una decisión basada en políticas que se aplica a los dispositivos de red en el grupo de dispositivos "switches". La cantidad necesaria de perfiles de cumplimiento depende de la cantidad de VLAN que se utilizarán. 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 Aruba ClearPass Policy Manager define si los dispositivos Axis tienen acceso a las redes de Aruba según cuatro perfiles de políticas de ejemplo.

Incorporación segura: IEEE 802.1AR/802.1X



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



La configuración de la política de cumplimiento en Aruba 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)

Secure integration of Axis devices into Aruba networks

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 firmware, certificados de nivel de producción y otras configuraciones. Aruba ClearPass Policy Manager verifica las siguientes condiciones:

- La versión de firmware 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)

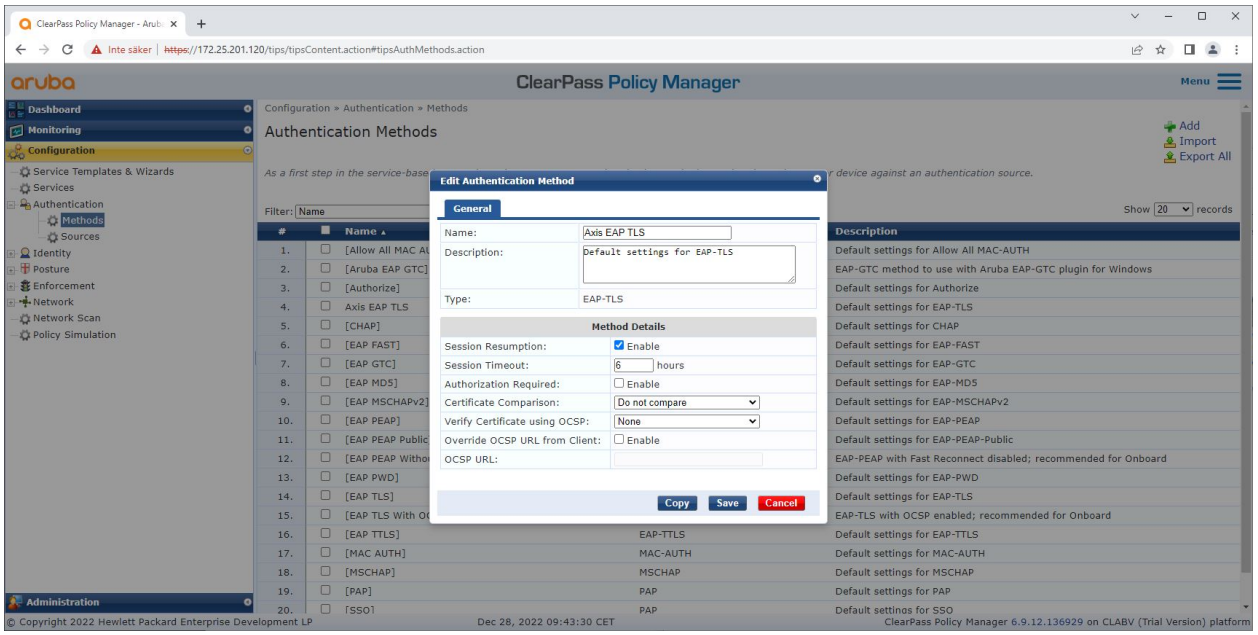
Al dispositivo Axis se le otorga acceso a la red de producción donde operará el dispositivo Axis. El acceso se otorga después de que se complete el aprovisionamiento del dispositivo desde dentro de la red de aprovisionamiento (VLAN 201). Aruba ClearPass Policy Manager verifica las siguientes condiciones:

- 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 firmware 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 intentará autenticarse en la red de Aruba. 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.

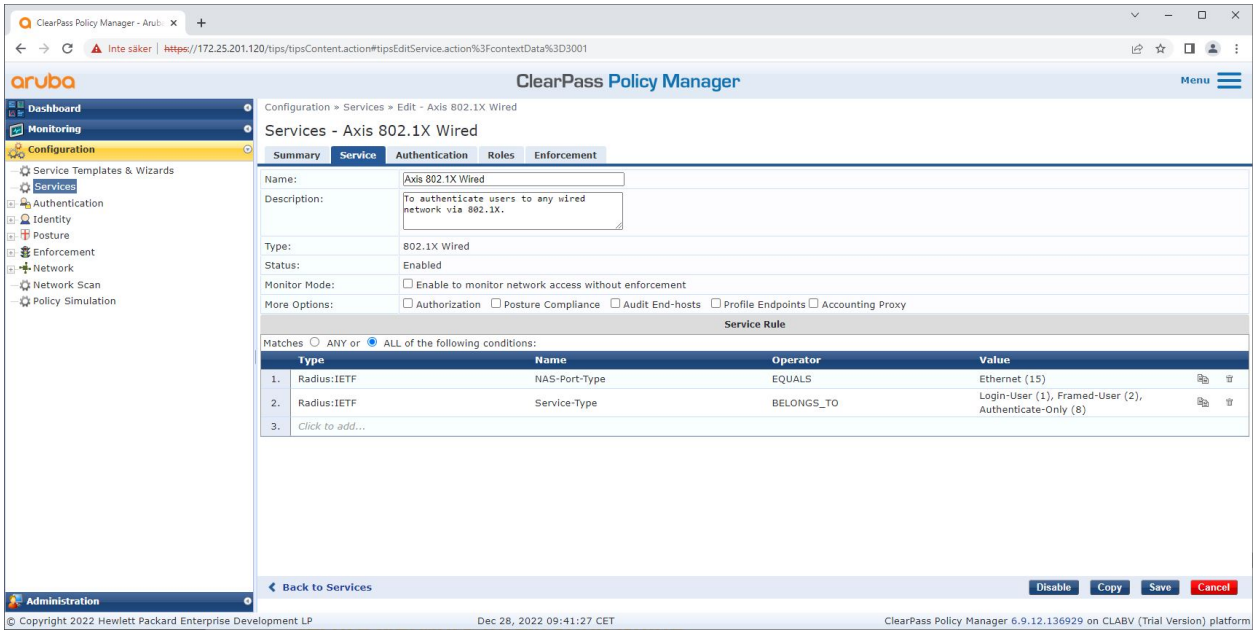
Incorporación segura: IEEE 802.1AR/802.1X



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

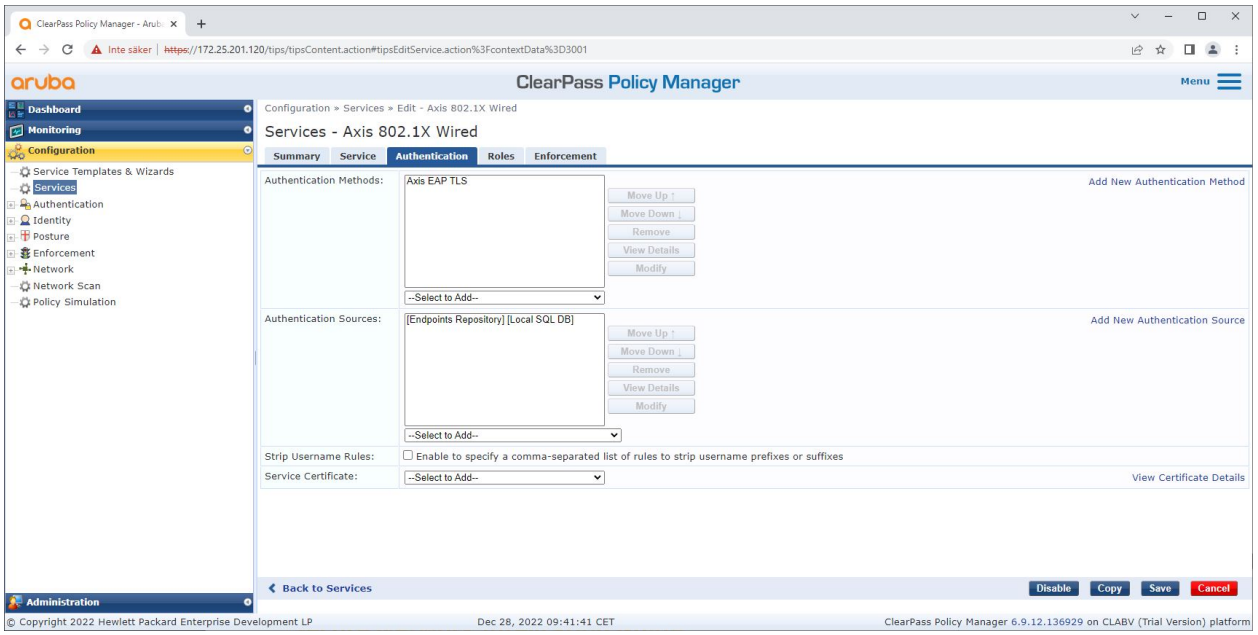
Configuración de servicio

En la interfaz de 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 Aruba.

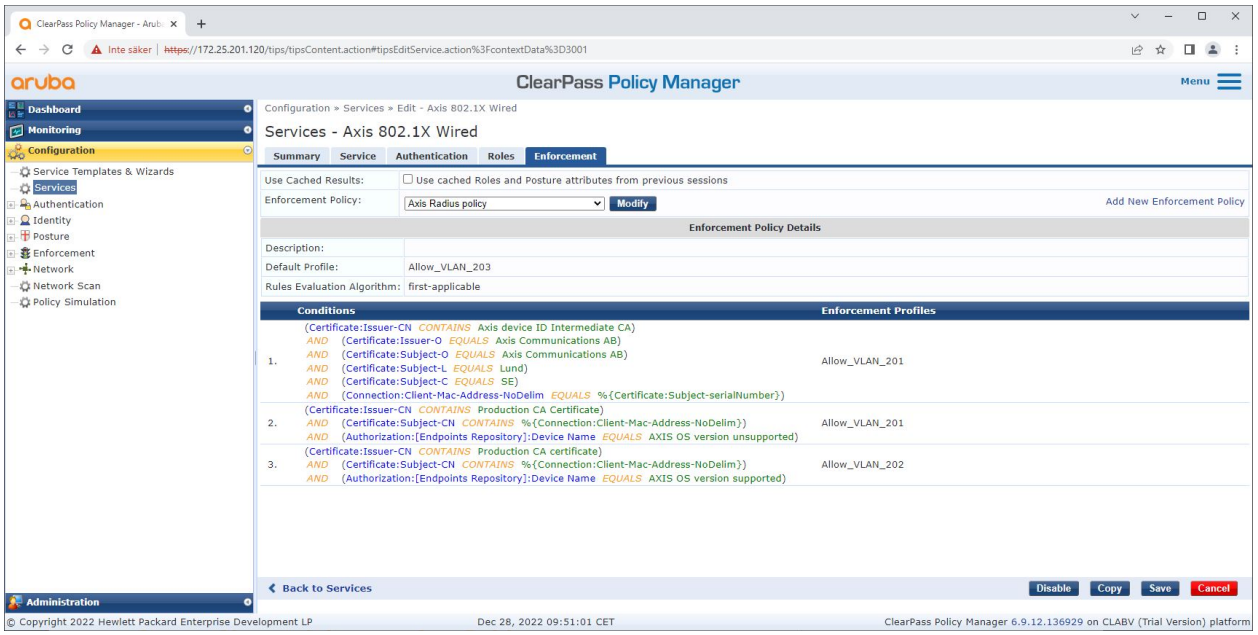


Se crea un servicio Axis dedicado que define IEEE 802.1X como método de conexión.

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 a Aruba

Los dispositivos Axis se conectan directamente a switches de acceso Aruba con capacidad PoE o mediante midspans PoE de Axis compatibles. Para incorporar de forma segura dispositivos Axis en las redes de Aruba, el switch de acceso debe configurarse para la comunicación IEEE 802.1X. El dispositivo Axis transmite la comunicación IEEE 802.1x EAP-TLS a Aruba 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 Aruba.

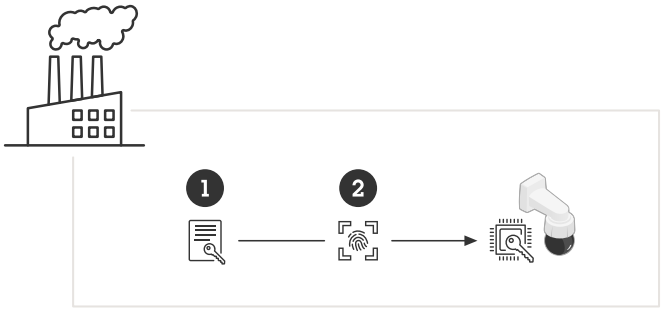
```
radius-server host MyRADIUSIPAddress key "MyRADIUSKey"

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*

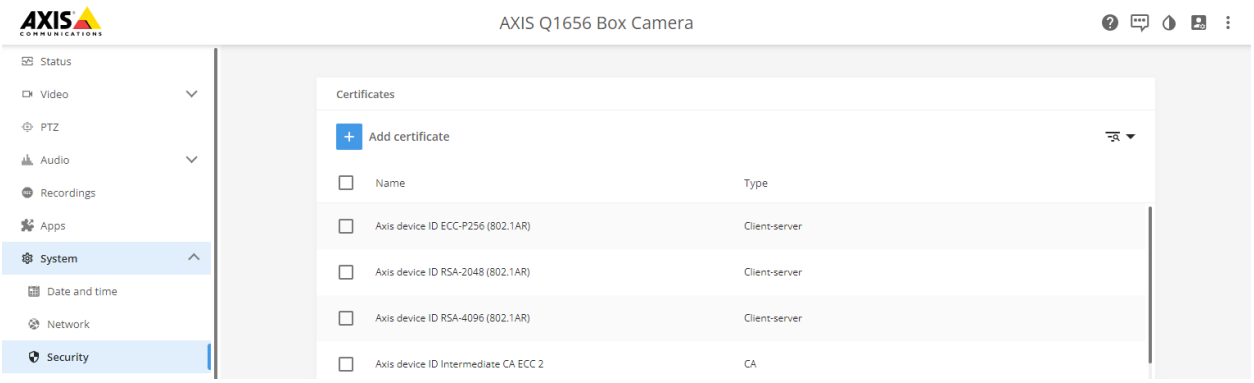
El almacén de claves seguro protegido por hardware proporcionado por un elemento seguro del dispositivo Axis se suministra de fábrica con un certificado exclusivo del dispositivo y las claves correspondientes (ID del dispositivo Axis) que pueden probar globalmente la autenticidad del dispositivo Axis. *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.

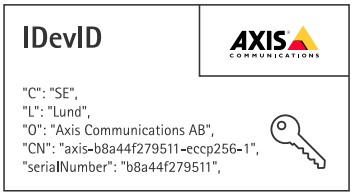
Secure integration of Axis devices into Aruba networks

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.

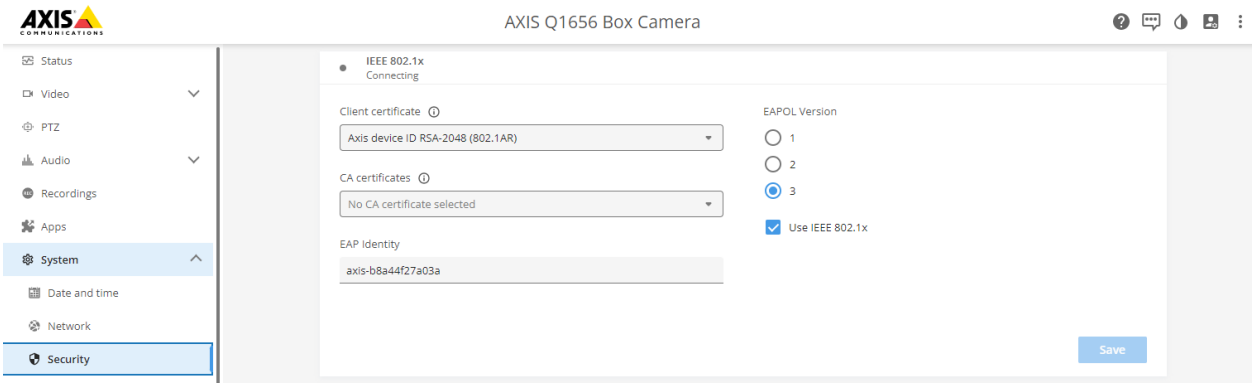
El certificado de identificación del dispositivo Axis compatible con IEEE 802.1AR incluye información sobre el número de serie y otra información específica del proveedor de Axis. La información es utilizada por Aruba ClearPass Policy Manager para análisis y toma de decisiones para otorgar acceso a la 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 sitios. Ambos ofrecen capacidades sencillas de administración y configuración para dispositivos Axis como:

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

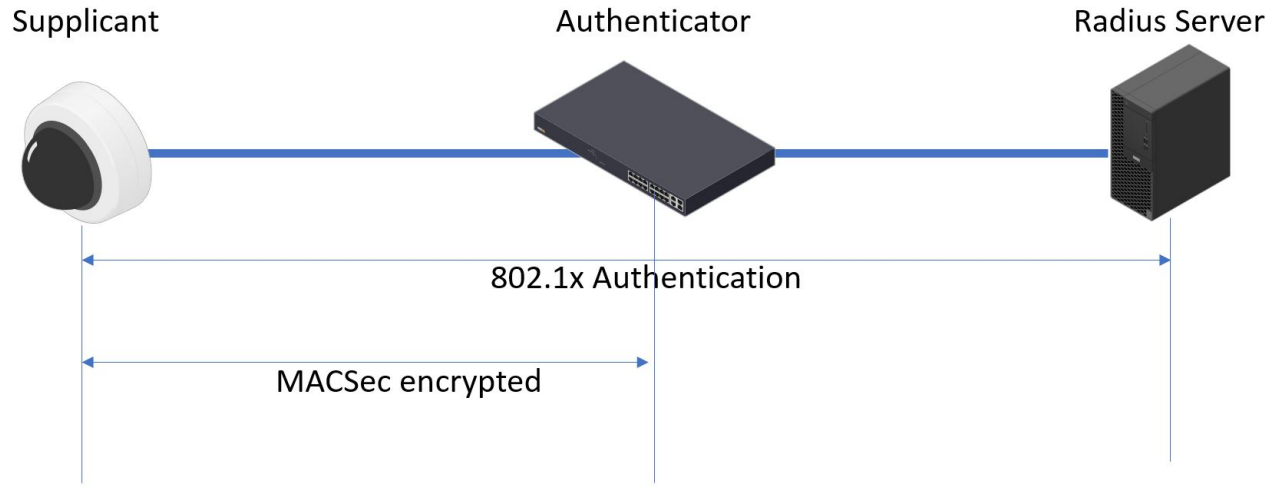
Operación de red segura: IEEE 802.1AE MACsec

Operación de red segura: 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 de Aruba (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 Aruba.

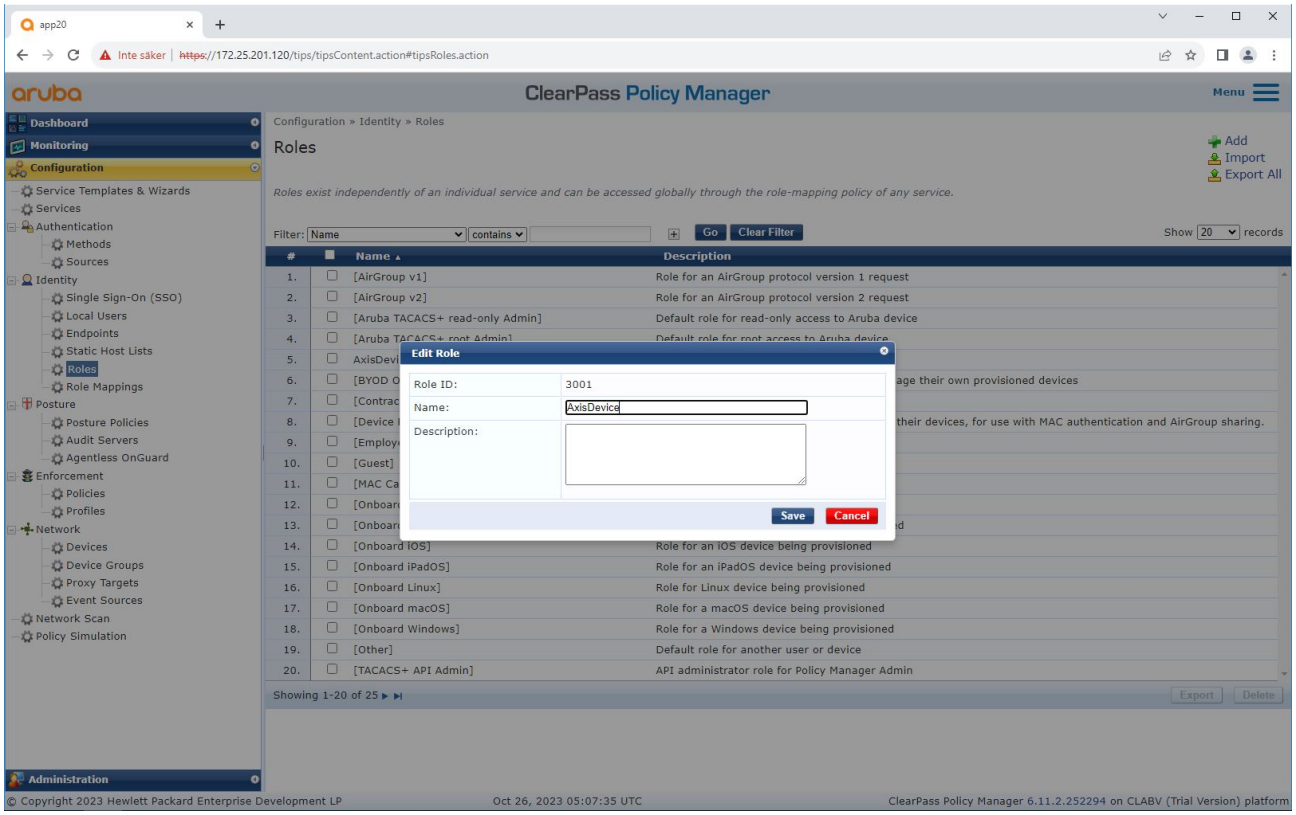
IEEE 802.1AE MACsec requiere preparaciones de configuración del switch de acceso de Aruba y de ClearPass Policy Manager. No se requiere ninguna configuración en el dispositivo Axis para permitir la comunicación cifrada con IEEE 802.1AE MACsec a través de EAP-TLS.

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

Operación de red segura: IEEE 802.1AE MACsec

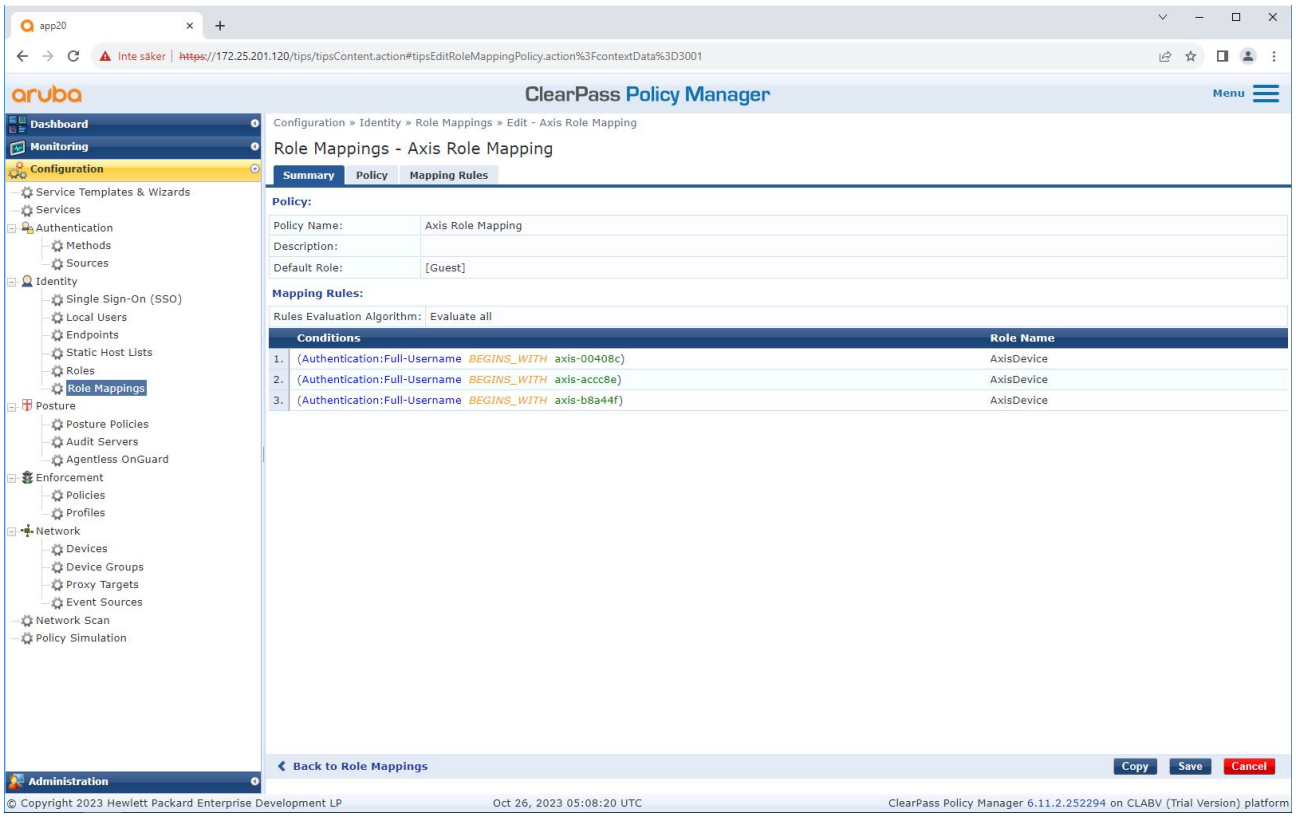
Aruba ClearPass Policy Manager

Política de asignación de roles y roles



Agregar un nombre de función para los dispositivos Axis. El nombre es el nombre de la función de acceso al puerto en la configuración del conmutador de acceso de Aruba.

Operación de red segura: IEEE 802.1AE MACsec

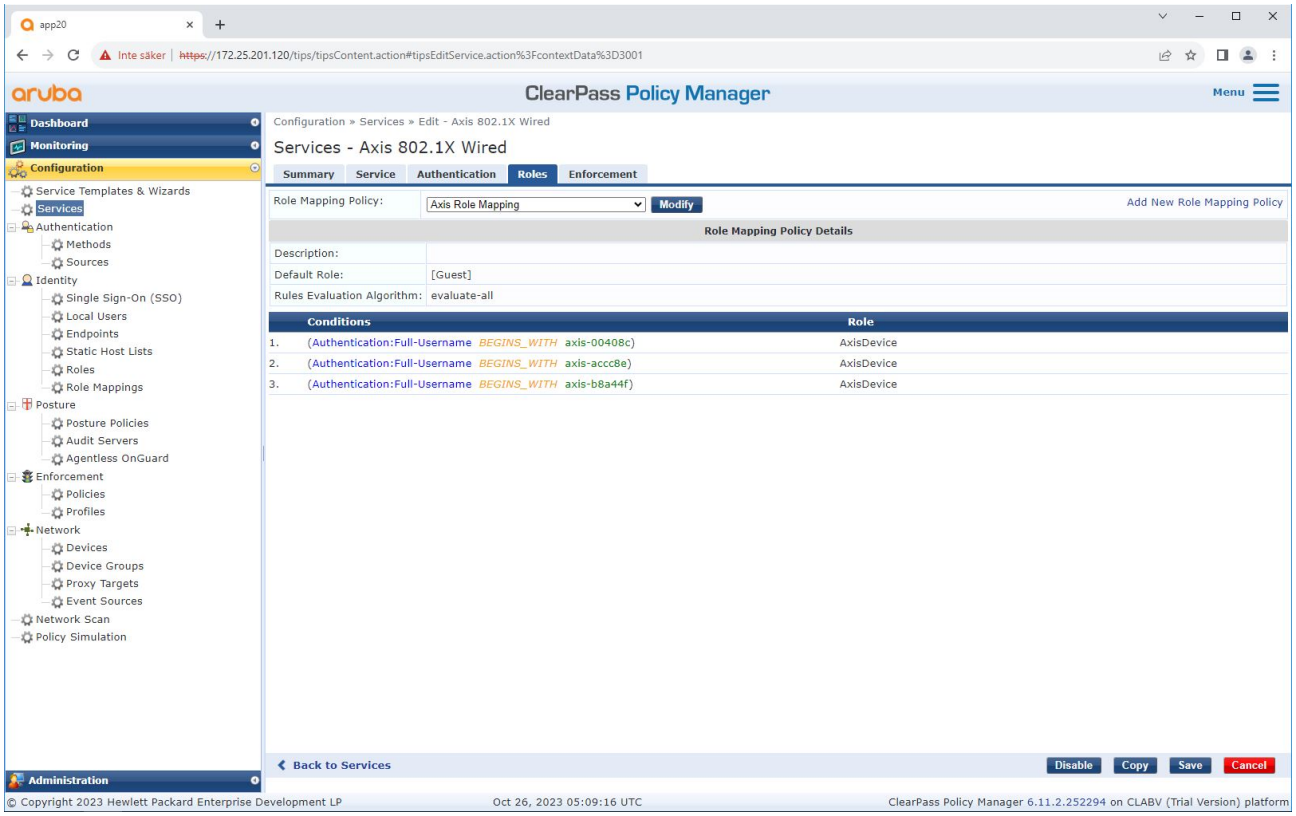


Agregar una política de asignación de roles de Axis para el rol de dispositivo de Axis creado anteriormente. Las condiciones definidas son necesarias para que un dispositivo se asigne a la función de dispositivo de Axis. Si no se cumplen las condiciones, el dispositivo formará parte del rol [Invitado].

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".

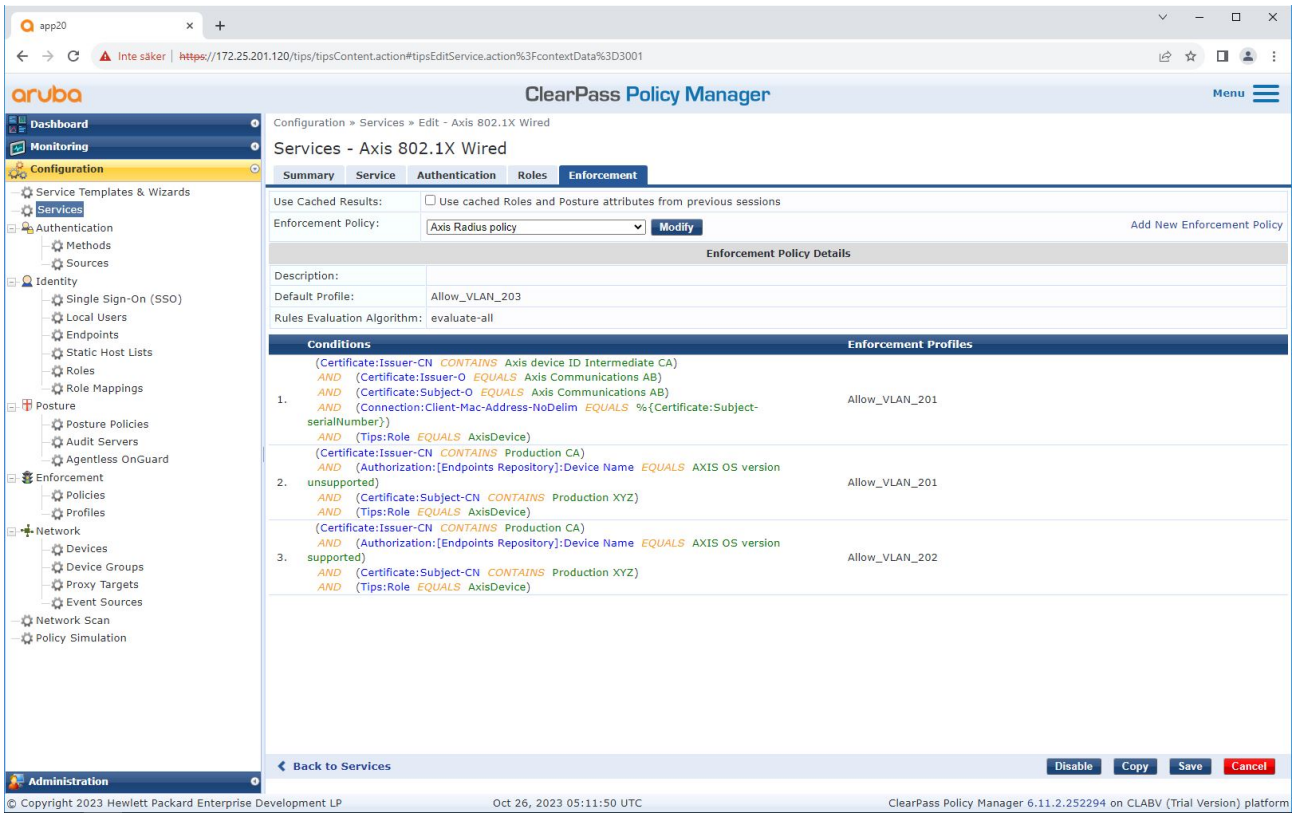
Operación de red segura: IEEE 802.1AE MACsec

Configuración de servicio



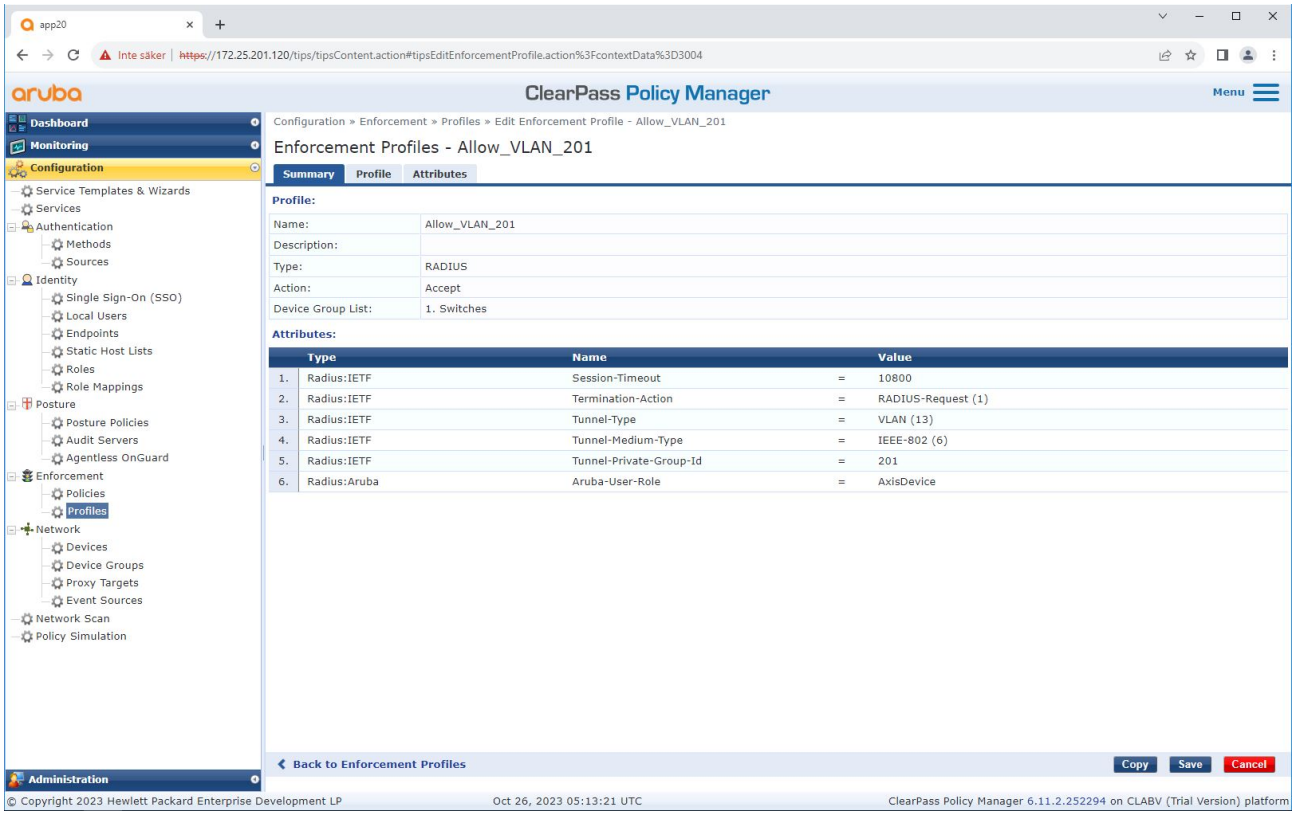
Agregar la política de asignación de roles de Axis creada anteriormente al servicio que define IEEE 802.1X como método de conexión para la incorporación de dispositivos Axis.

Operación de red segura: IEEE 802.1AE MACsec



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

Perfil de cumplimiento



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

Switch de acceso a Aruba

Además de la configuración de incorporación segura descrita en *Switch de acceso a Aruba en la página 16*, consulte el siguiente ejemplo de configuración de puerto para que el switch de acceso de Aruba configure IEEE 802.1AE MACsec.

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

port-access role AxisDevice
associate macsec-policy macsec-eap
auth-mode client-mode

aaa authentication port-access dot1x authenticator
macsec
mkacak-length 16
enable
```

Incorporación heredada: autenticación MAC

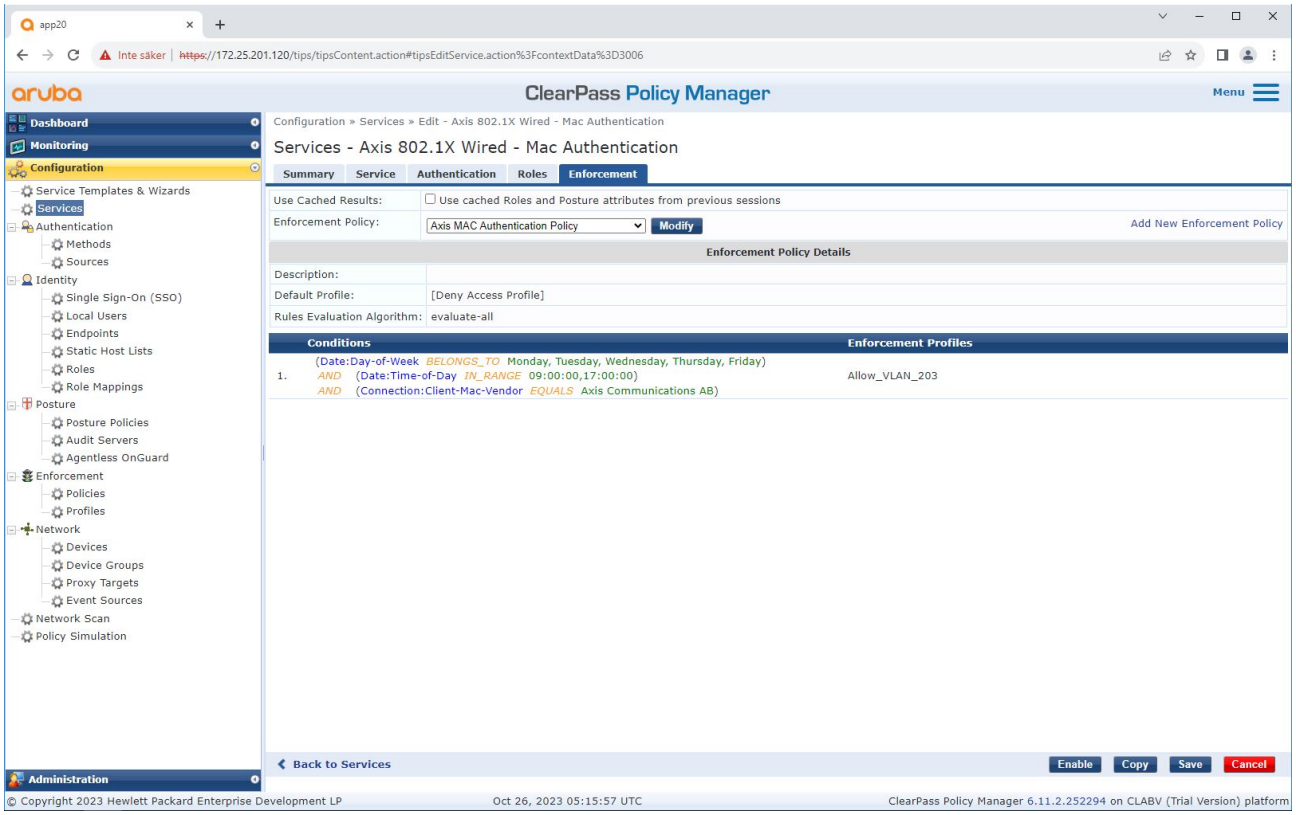
Puede utilizar MAC Authentication Bypass (MAB) para incorporar dispositivos Axis que no admitan la incorporación de IEEE 802.1AR con el certificado de identificación del dispositivo de Axis y IEEE 802.1X habilitado en el estado predeterminado de fábrica. Si falla la incorporación de 802.1X, Aruba ClearPass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

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

Aruba ClearPass Policy Manager

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 Aruba según cuatro 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.

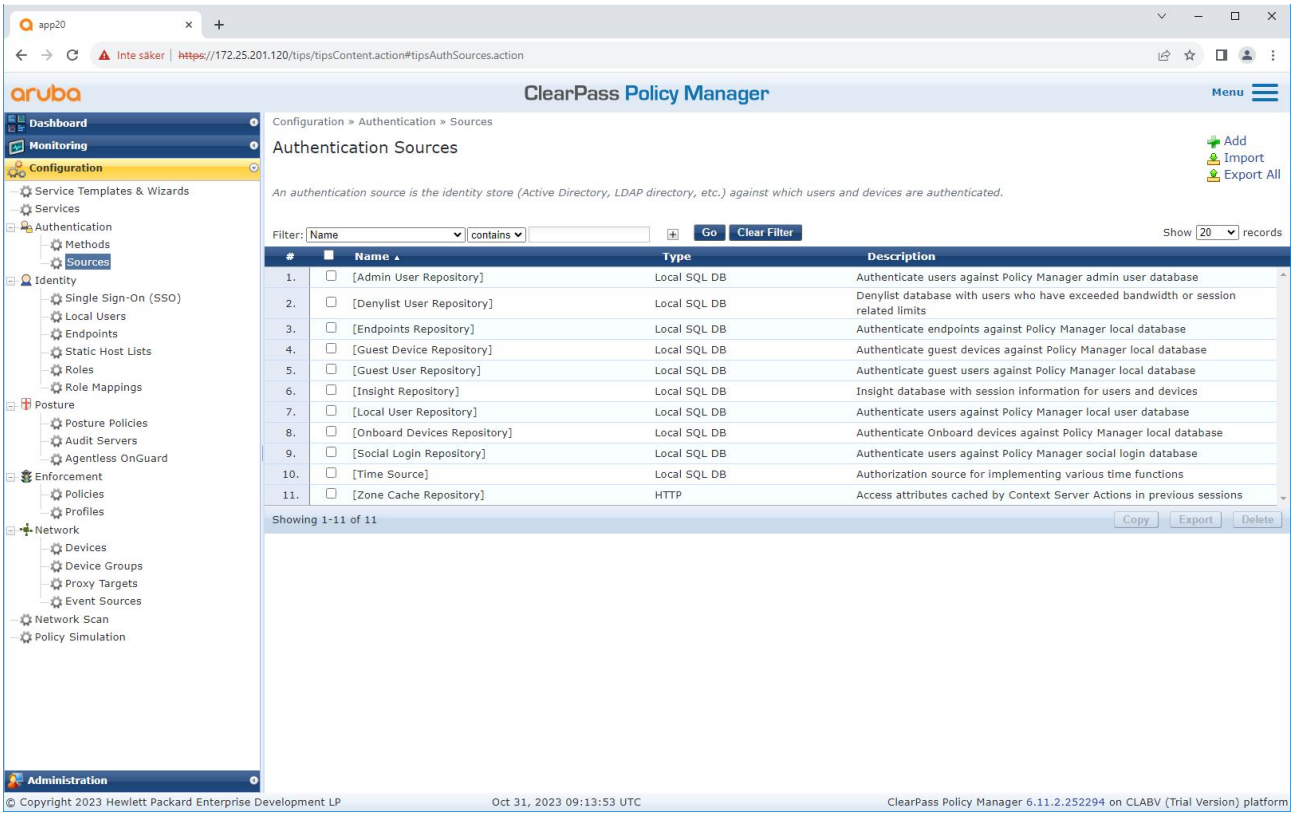
Incorporación heredada: autenticación MAC

- Es entre las 09:00 y las 17:00.
- El proveedor de la dirección MAC coincide con Axis Communications AB.

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.

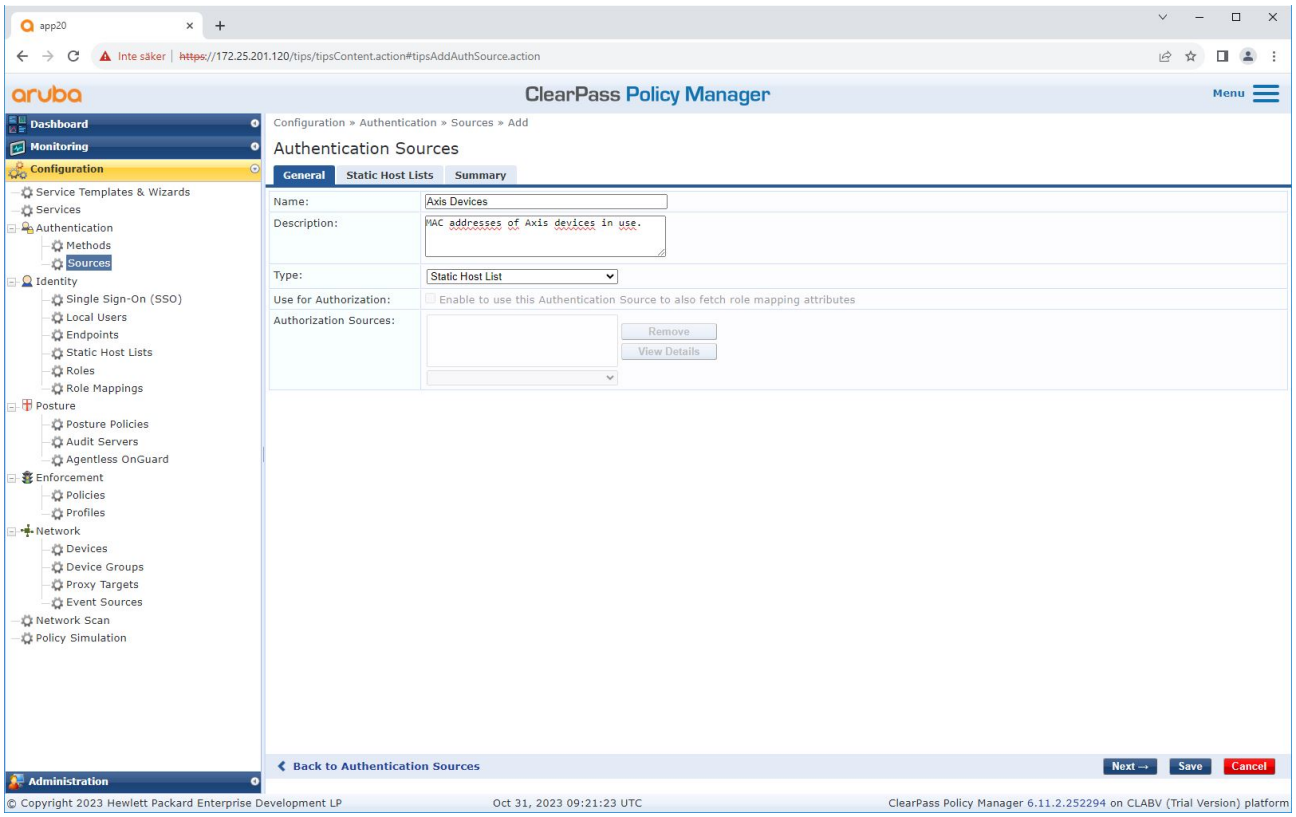
Configuración de fuente

En la interfaz de Fuentes, se crea una nueva fuente de autenticación para permitir solo direcciones MAC importadas manualmente.

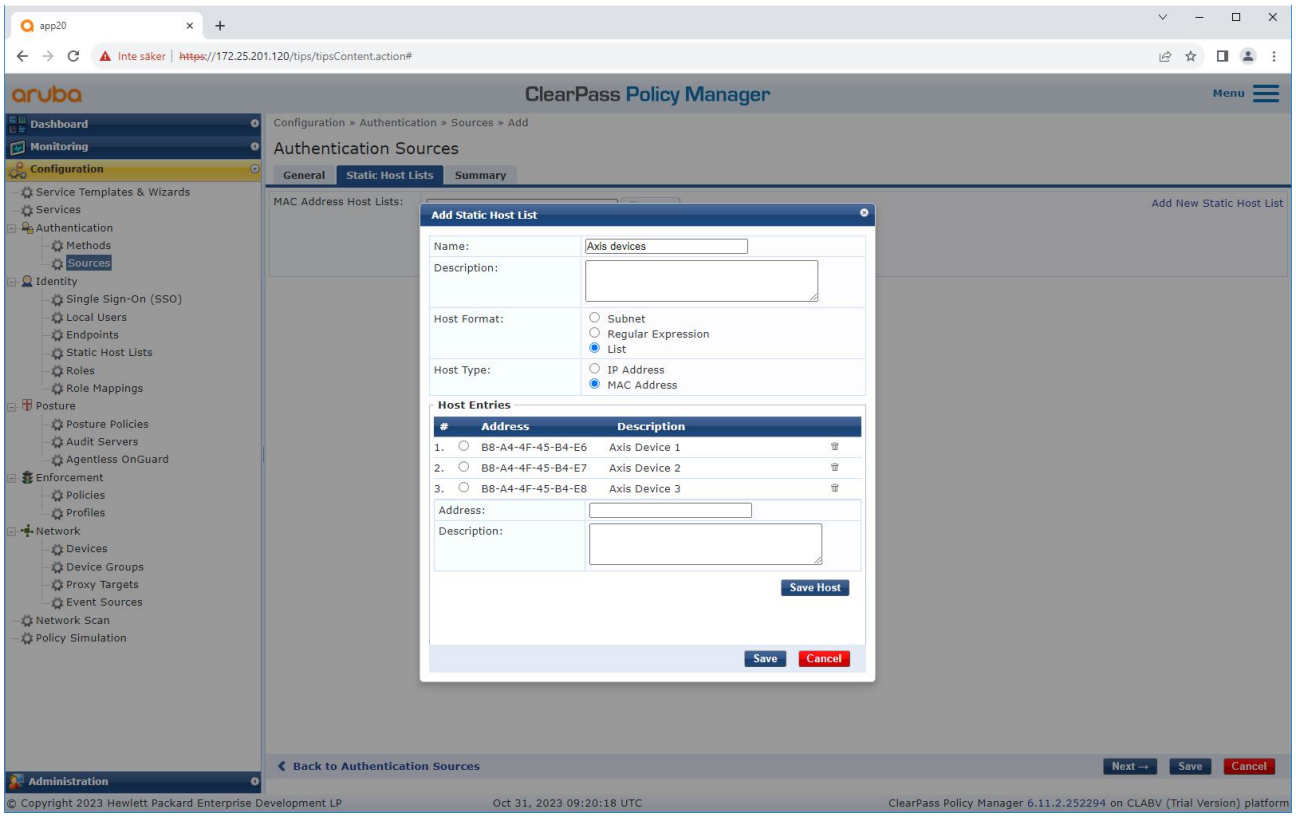


Secure integration of Axis devices into Aruba networks

Incorporación heredada: autenticación MAC



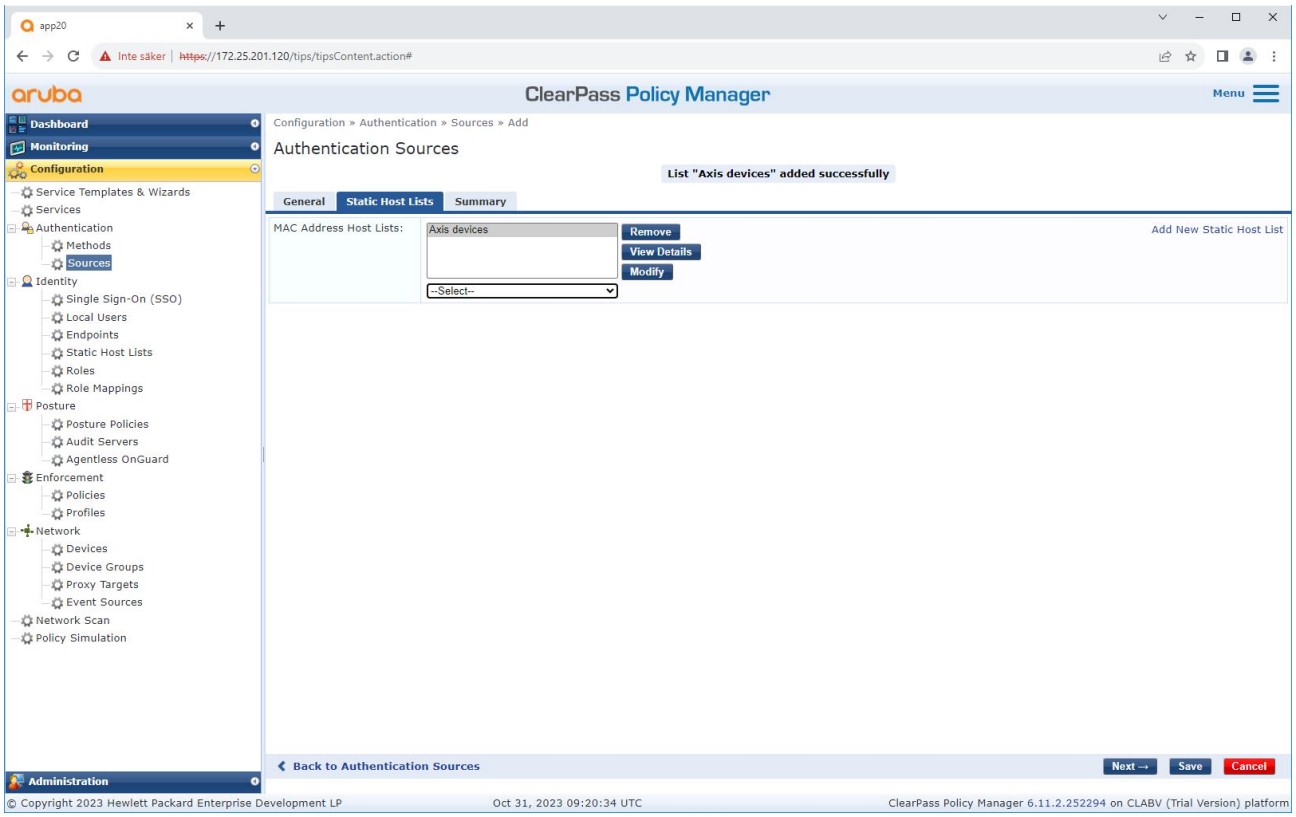
Incorporación heredada: autenticación MAC



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

Secure integration of Axis devices into Aruba networks

Incorporación heredada: autenticación MAC

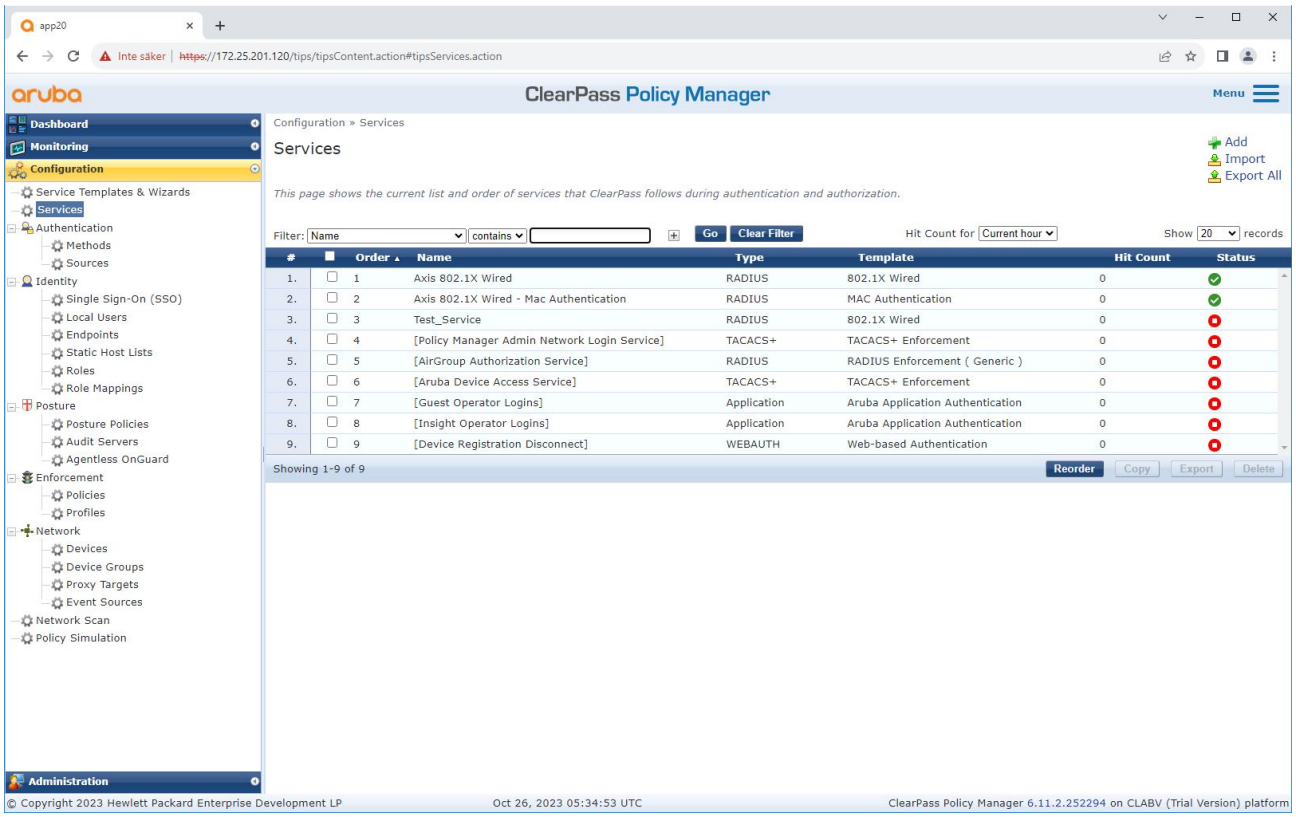


Configuración de servicio

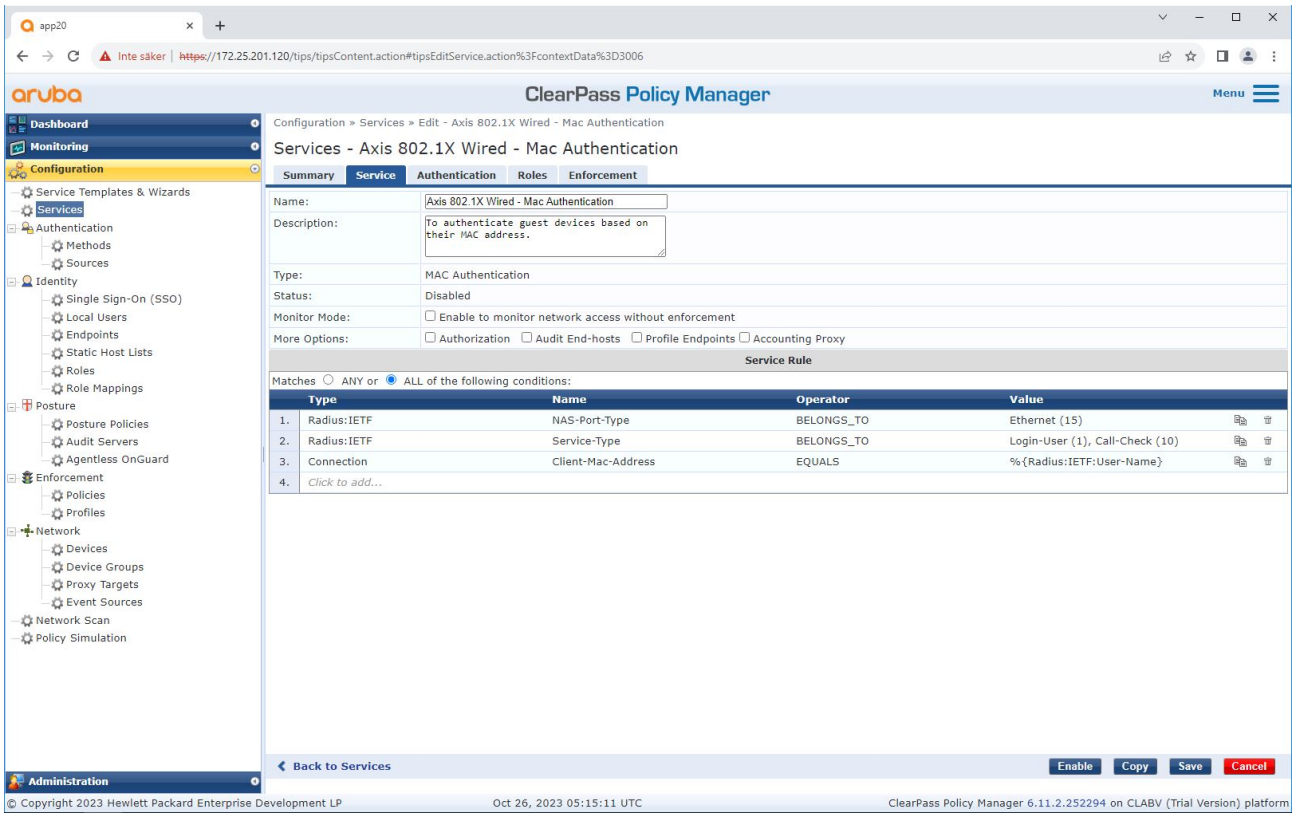
En la interfaz de Servicios, los pasos de configuración se combinan en un solo servicio que maneja la autenticación y autorización de los dispositivos Axis en las redes de Aruba.

Secure integration of Axis devices into Aruba networks

Incorporación heredada: autenticación MAC

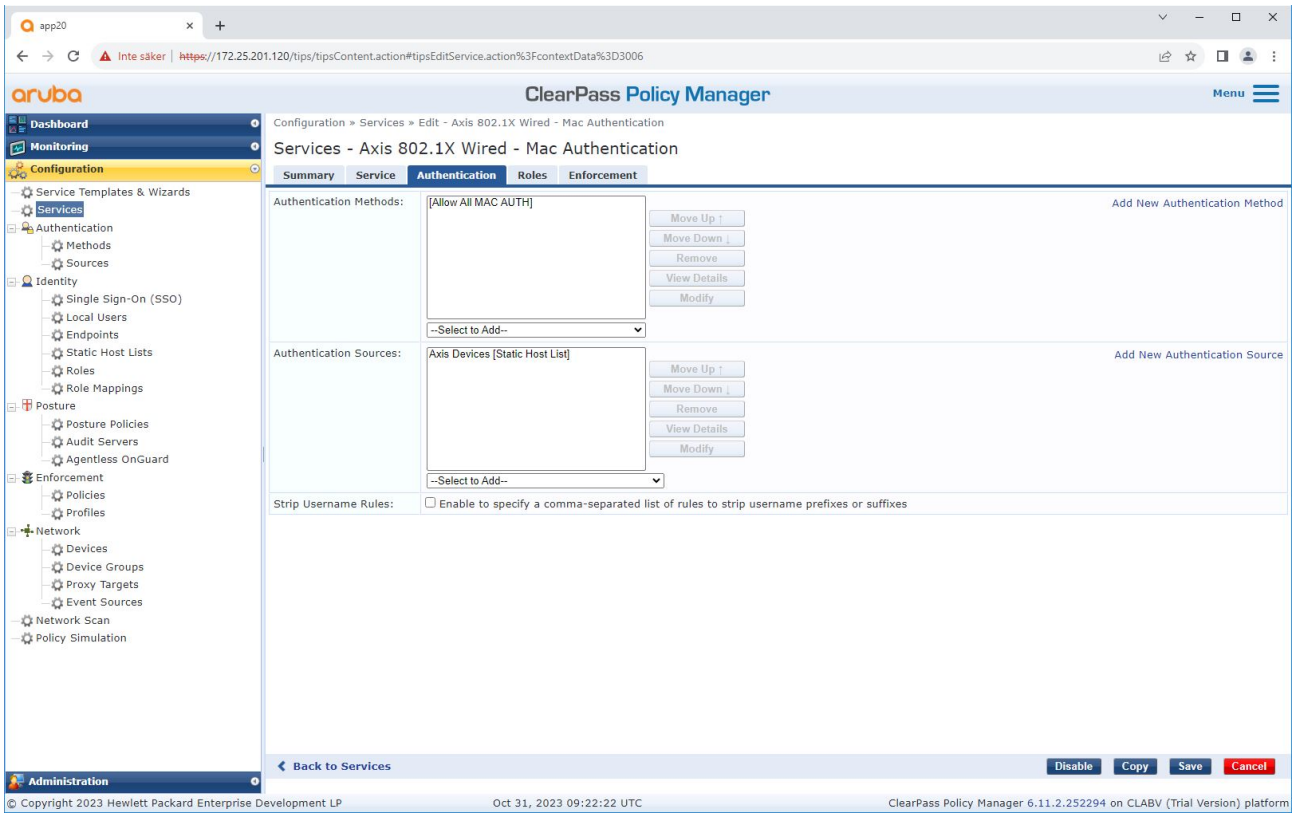


Incorporación heredada: autenticación MAC



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

Incorporación heredada: autenticación MAC

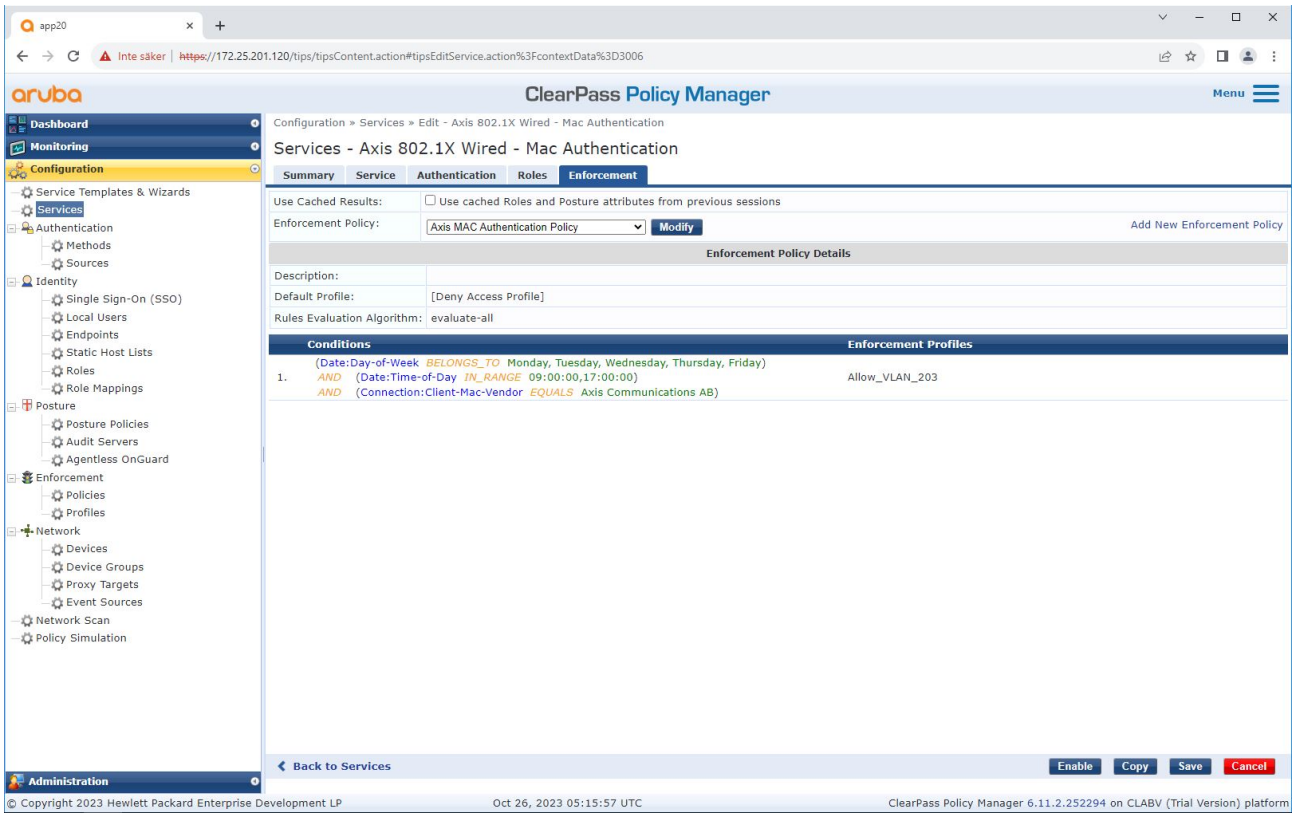


El método de autenticación MAC preconfigurado está configurado para el servicio. Además, se selecciona la fuente de autenticación creada previamente que contiene una lista de direcciones MAC de Axis.

Axis Communications AB 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

Incorporación heredada: autenticación MAC



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

Switch de acceso a Aruba

Además de la configuración de incorporación segura descrita en *Switch de acceso a Aruba en la página 16*, consulte el siguiente ejemplo de configuración de puerto para que el switch de acceso de Aruba 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
```

Manual del usuario
Secure integration of Axis devices into Aruba networks

Ver. M4.3
Fecha: Noviembre 2023
N.º de pieza T10197992