Secure integration of Axis devices into Aruba networks

Manual do usuário

Secure integration of Axis devices into Aruba networks

Sumário

Secure integration of Axis devices into Aruba networks

Introdução

Introdução

Este guia de integração tem como objetivo descrever as práticas recomendadas de configuração para integrar e operar dispositivos Axis em redes Aruba. A configuração usa padrões e protocolos de segurança modernos, como IEEE 802.1X, IEEE 802.1AR, IEEE 802.1AE e HTTPS.

Estabelecer a automação adequada para integração de rede pode economizar tempo e dinheiro. Ela permite remover a complexidade desnecessária do sistema ao usar aplicativos de gerenciamento de dispositivos Axis combinados com equipamentos e aplicativos de rede Aruba. Abaixo estão apenas alguns benefícios que podem ser obtidos ao combinar dispositivos e software Axis com uma infraestrutura de rede Aruba:

- Minimize a complexidade do sistema removendo redes de staging de dispositivos.
- Economize custos adicionando processos de integração automatizados e gerenciamento de dispositivos.
- Aproveite os controles de segurança de rede sem toque fornecidos pelos dispositivos Axis.
- Aumente a segurança geral da rede aplicando a experiência da Aruba e da Axis.

A infraestrutura de rede deve estar preparada para verificar com segurança a integridade dos dispositivos Axis antes de iniciar a configuração. Isso permite uma transição suave definida por software entre redes lógicas durante todo o processo de integração. É necessário ter conhecimento das seguintes áreas antes de fazer a configuração:

- Gerenciamento da infraestrutura de TI de redes corporativas da Aruba, incluindo switches de acesso Aruba e o Aruba ClearPass Policy Manager.
- Conhecimento em técnicas modernas de controle de acesso à rede e políticas de segurança de rede.
- Conhecimento básico sobre os produtos Axis é desejável, mas será fornecido ao longo do guia.

Integração segura – IEEE 802.1AR/802.1X

Autenticação inicial

Conecte o dispositivo Axis compatível com o Axis Edge Vault para autenticar o dispositivo na rede Aruba. O dispositivo usará o certificado de ID de dispositivo IEEE 802.1AR Axis por meio do controle de acesso à rede IEEE 802.1X para se autenticar.

Para conceder acesso à rede, o Aruba ClearPass Policy Manager verifica o ID do dispositivo Axis em conjunto com outras impressões digitais específicas do dispositivo. As informações, como endereço MAC e firmware em execução, são usadas para tomar uma decisão baseada em políticas.

O dispositivo Axis é autenticado na rede Aruba usando o certificado de ID de dispositivo Axis compatível com IEEE 802.1AR.

O dispositivo Axis é autenticado na rede Aruba usando o certificado de ID de dispositivo Axis compatível com IEEE 802.1AR.

1. *ID de dispositivo Axis*
2. *Autenticação de rede IEEE 802.1x EAP-TLS*
3. *Switch de acesso (autenticador)*
4. *ClearPass Policy Manager*

Provisionamento

Após a autenticação, a rede Aruba moverá o dispositivo Axis para a rede de provisionamento (VLAN201) onde o Axis Device Manager está instalado. Com o Axis Device Manager, é possível realizar a configuração do dispositivo, o reforço da segurança e atualizações de firmware. Para concluir o provisionamento do dispositivo, novos certificados de nível de produção específicos do cliente são carregados no dispositivo para IEEE 802.1X e HTTPS.

Após a autenticação bem-sucedida, o dispositivo Axis passa para uma rede de provisionamento para configuração.

1. *Switch de acesso*
2. *Rede de provisionamento*
3. *ClearPass Policy Manager*
4. *Aplicativo de gerenciamento de dispositivos*

Rede de produção

O provisionamento do dispositivo Axis com novos certificados IEEE 802.1X acionará uma nova tentativa de autenticação. O Aruba ClearPass Policy Manager verificará os novos certificados e decidirá se o dispositivo Axis será movido para a rede de produção ou não.

Após a configuração do dispositivo, o dispositivo Axis sairá da rede de provisionamento e tentará se autenticar novamente na rede Aruba.

1. *ID de dispositivo Axis*
2. *Autenticação de rede IEEE 802.1x EAP-TLS*
3. *Switch de acesso (autenticador)*
4. *ClearPass Policy Manager*

Após a reautenticação, o dispositivo Axis é movido para a rede de produção (VLAN 202). Nessa rede, o sistema de gerenciamento de vídeo (VMS) se conectará ao dispositivo Axis e começará a operar.

O dispositivo Axis recebe acesso à rede de produção.

1 *Switch de acesso*
2 *Rede de produção*
3 *ClearPass Policy Manager*
4 *Sistema de gerenciamento de vídeo*

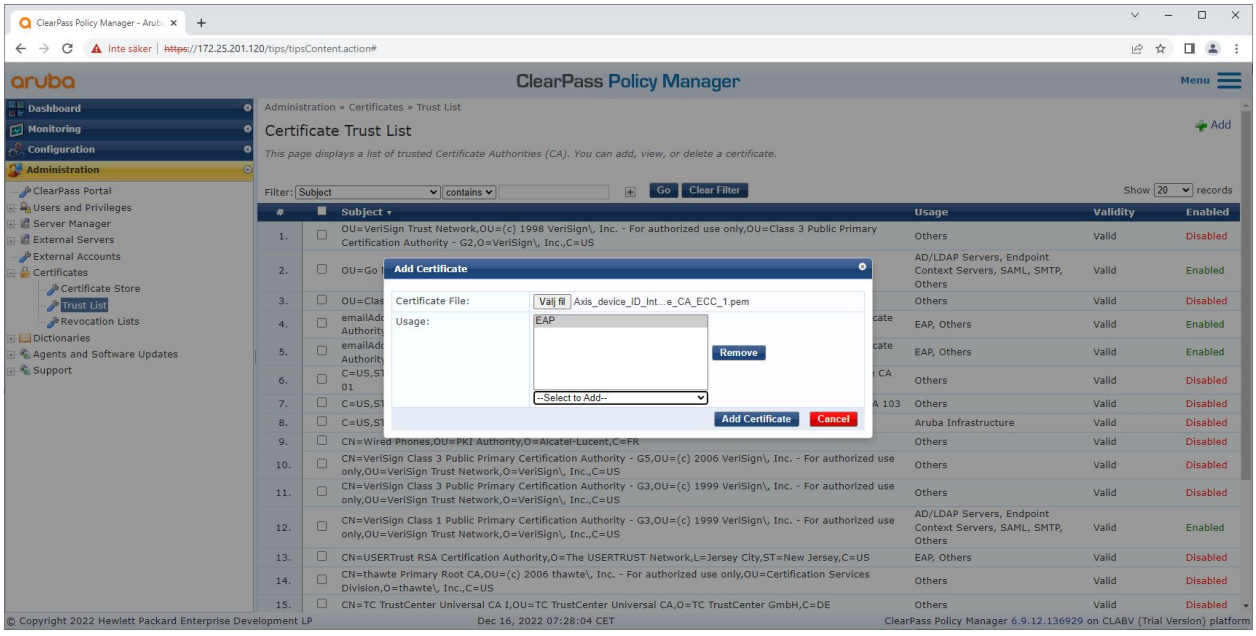
Configuração do HPE Aruba

Aruba ClearPass Policy Manager

O ClearPass Policy Manager da Aruba fornece controle de acesso à rede seguro baseado em função e dispositivo para IoT, BYOD, dispositivos corporativos, funcionários, prestadores de serviços e convidados em infraestrutura com fio, sem fio e VPN de vários fornecedores.

Configuração de armazenamento de certificados confiável

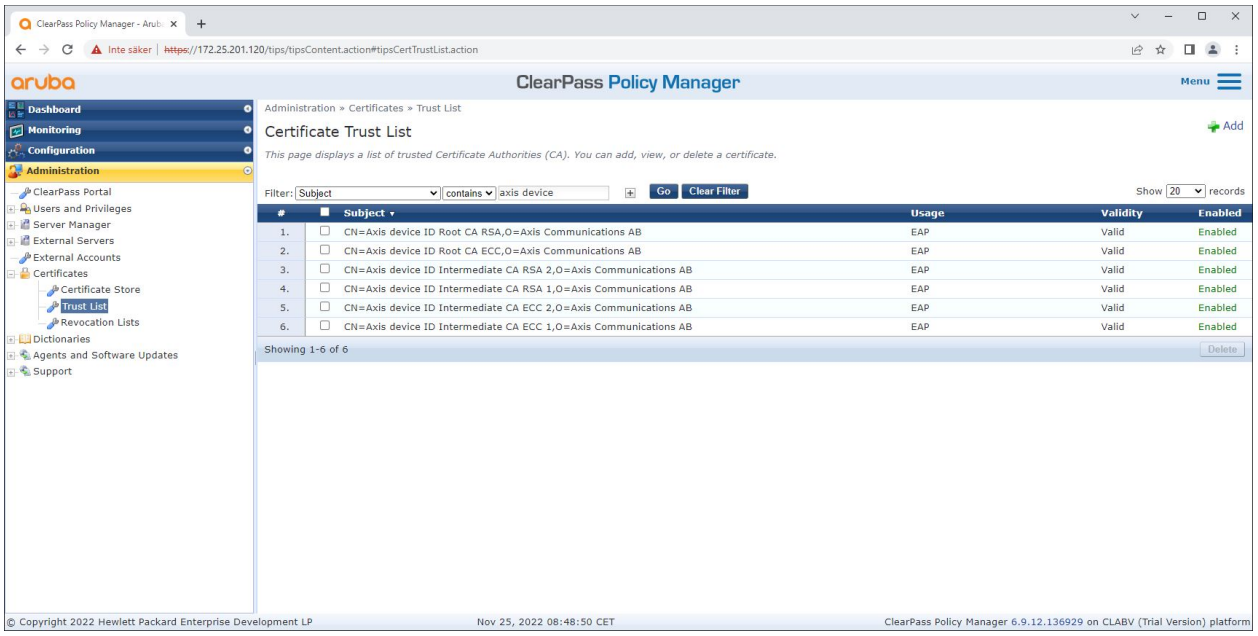
1. Baixe a cadeia de certificados IEEE 802.1AR específica da Axis em axis.com.
2. Carregue as cadeias de certificados de CA raiz e CA intermediária IEEE 802.1AR específicas da Axis no armazenamento de certificados confiáveis.
3. Habilite o Aruba ClearPass Policy Manager para autenticar dispositivos Axis via IEEE 802.1X EAP-TLS.
4. Selecione EAP no campo de uso. Os certificados serão usados para autenticação IEEE 802.1X EAP-TLS.



Carregando os certificados IEEE 802.1AR específicos da Axis para o armazenamento de certificados confiáveis do Aruba ClearPass Policy Manager.

Secure integration of Axis devices into Aruba networks

Integração segura – IEEE 802.1AR/802.1X



O armazenamento de certificados confiável no Aruba ClearPass Policy Manager com cadeia de certificados IEEE 802.1AR específica da Axis incluída.

Configuração de dispositivo/grupo de rede

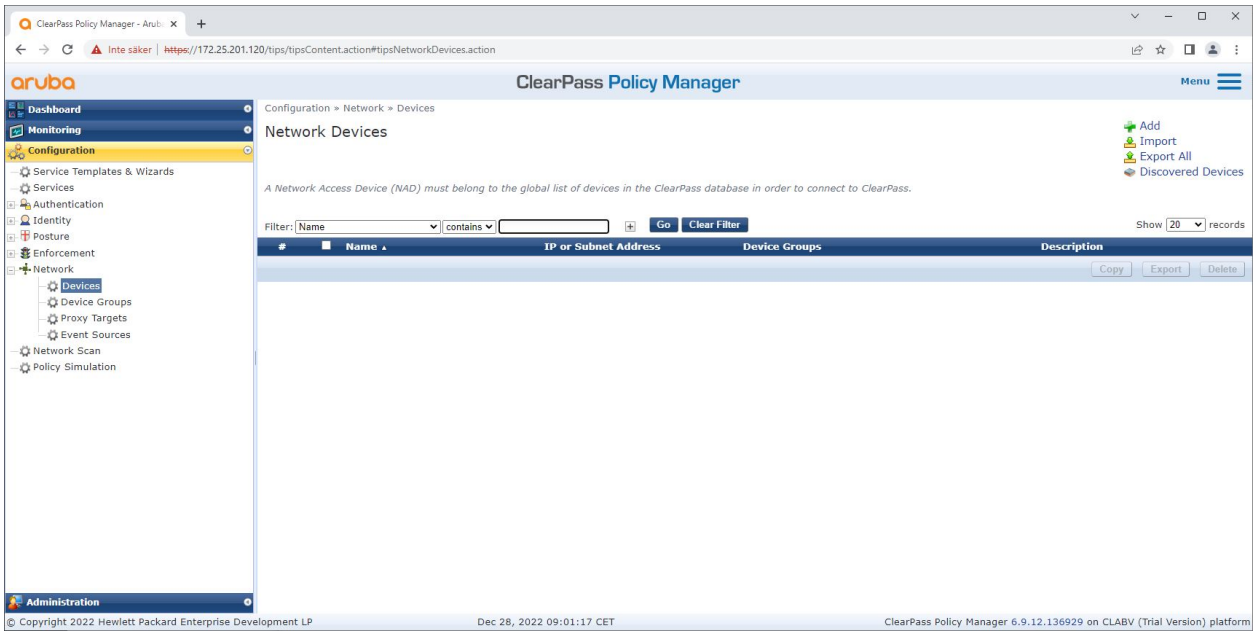
1. Adicione dispositivos de acesso à rede confiáveis, como switches de acesso Aruba, ao ClearPass Policy Manager. O ClearPass Policy Manager precisa saber quais switches de acesso Aruba na rede serão usados para comunicação IEEE 802.1X.

2. Use a configuração de grupo de dispositivos de rede para agrupar vários dispositivos de acesso à rede confiáveis. O agrupamento de dispositivos de acesso à rede confiáveis facilita a configuração de políticas.

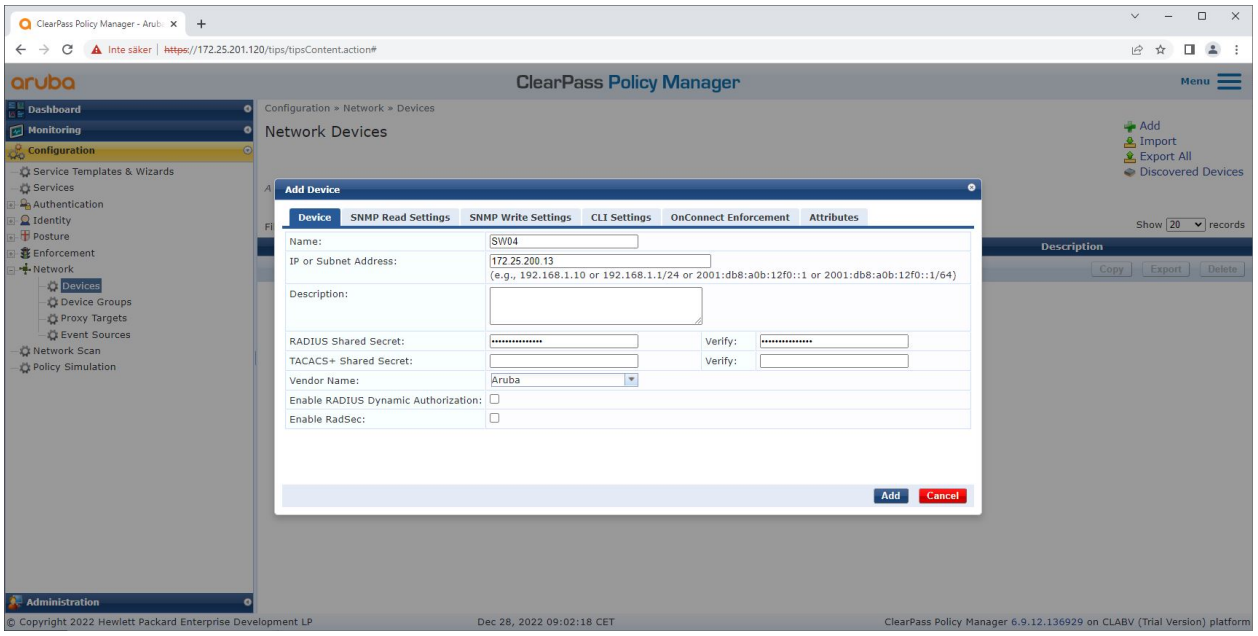
3. O segredo compartilhado RADIUS precisa corresponder à configuração específica do switch IEEE 802.1X.

Secure integration of Axis devices into Aruba networks

Integração segura – IEEE 802.1AR/802.1X



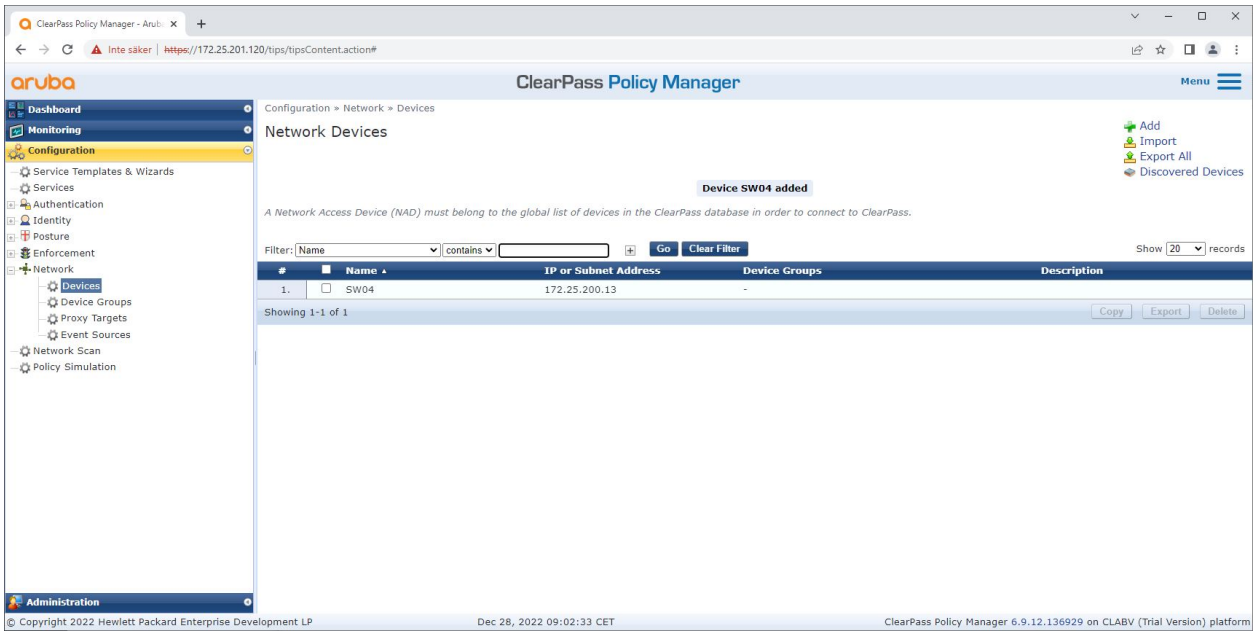
A interface de dispositivos de rede confiáveis no Aruba ClearPass Policy Manager.



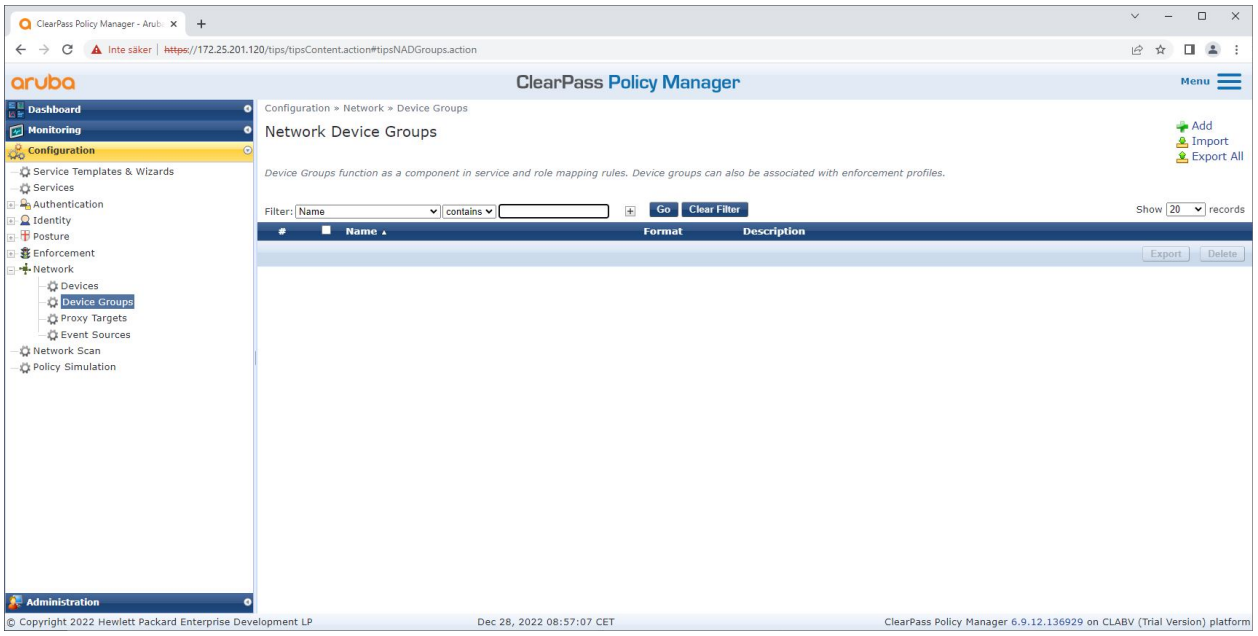
Adicionando o switch de acesso Aruba como dispositivo de rede confiável no Aruba ClearPass Policy Manager. Observe que o segredo compartilhado RADIUS precisa corresponder à configuração específica do switch IEEE 802.1X.

Secure integration of Axis devices into Aruba networks

Integração segura – IEEE 802.1AR/802.1X

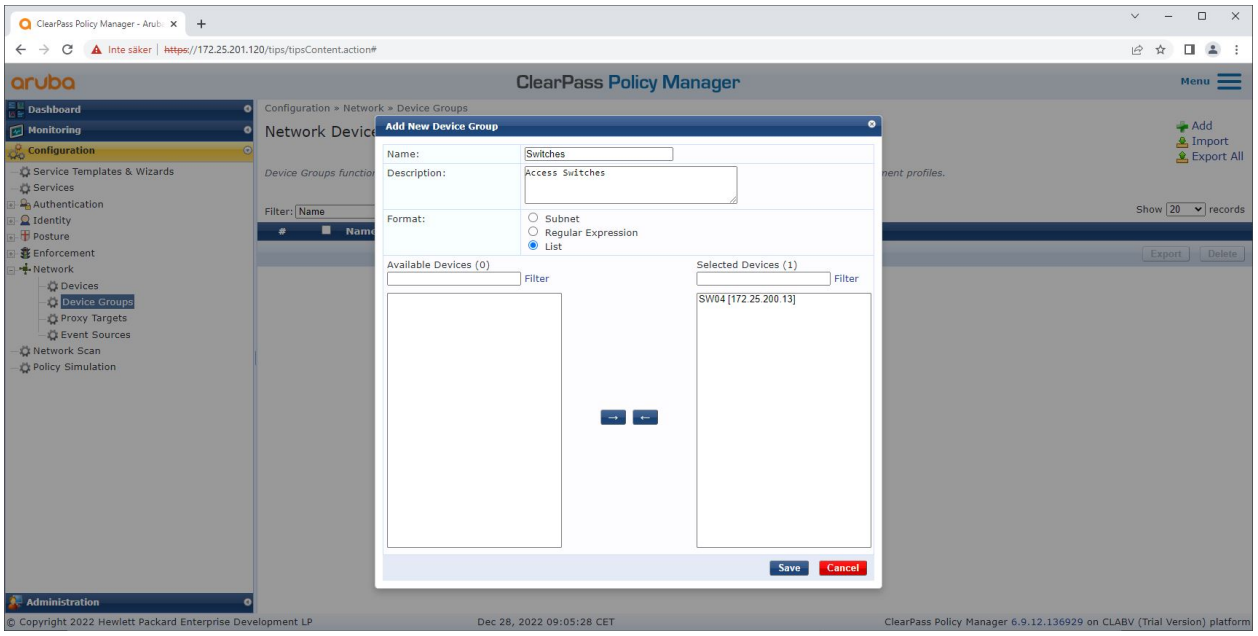


O Aruba ClearPass Policy Manager com um dispositivo de rede confiável configurado.

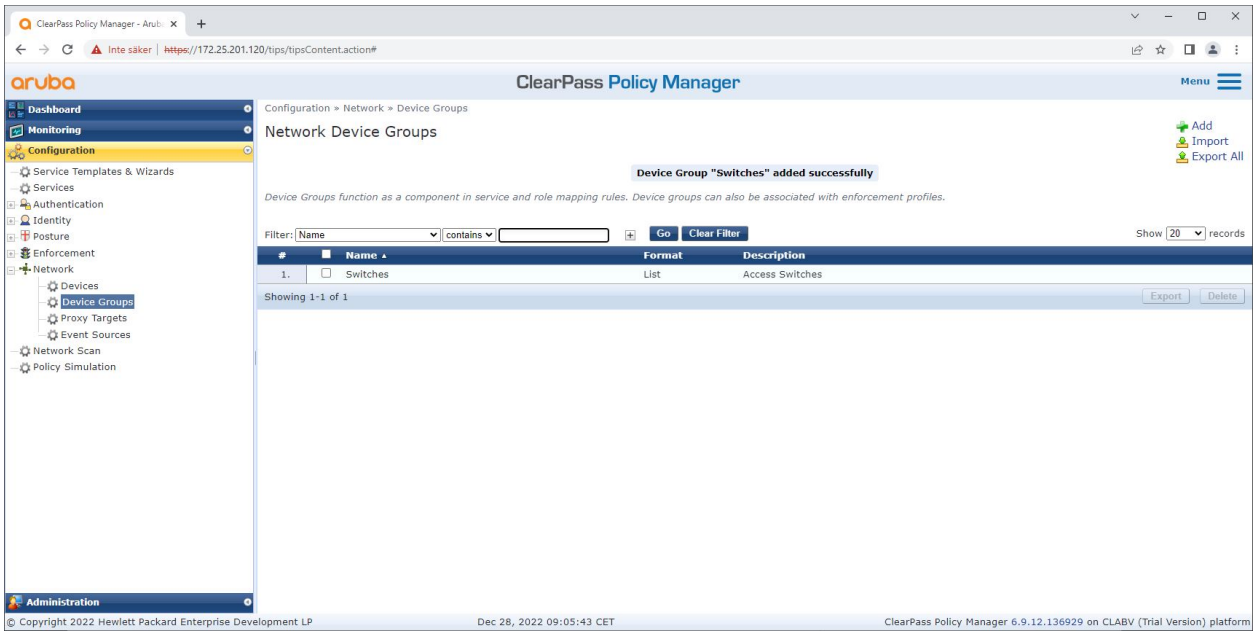


A interface de grupos de dispositivos de rede confiáveis no Aruba ClearPass Policy Manager.

Integração segura – IEEE 802.1AR/802.1X



Adicionando um dispositivo de acesso à rede confiável a um novo grupo de dispositivos no Aruba ClearPass Policy Manager.



O Aruba ClearPass Policy Manager com grupo de dispositivos de rede configurado que inclui um ou vários dispositivos de rede confiáveis.

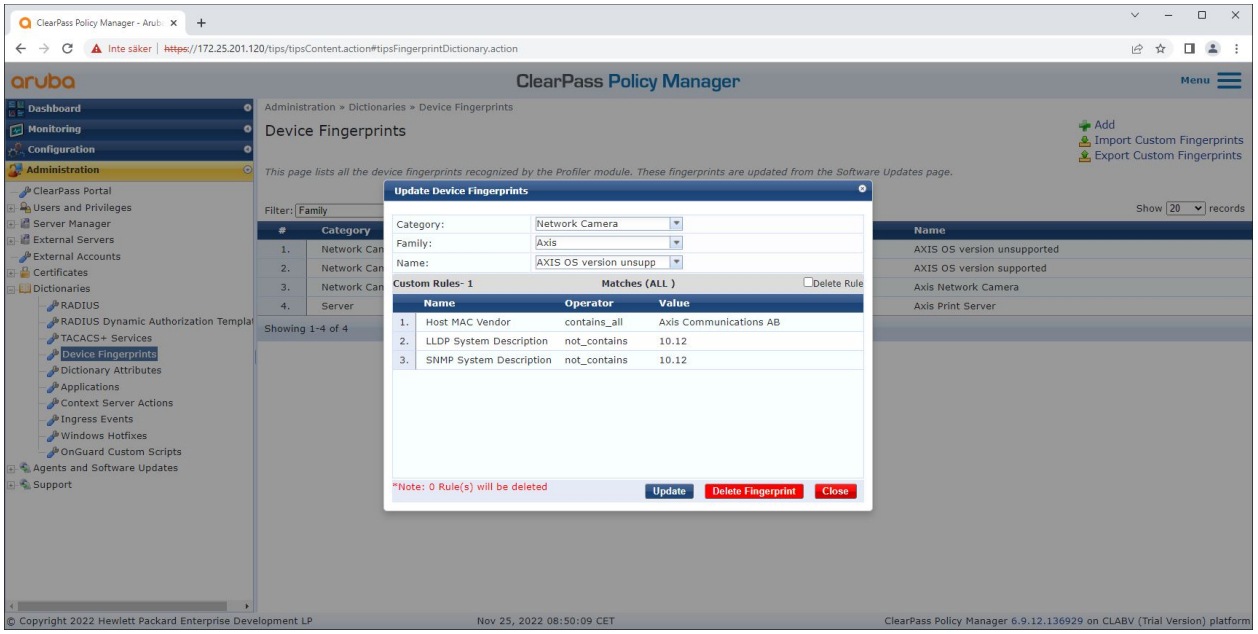
Configuração de impressão digital do dispositivo

O dispositivo Axis pode distribuir informações específicas do dispositivo, como endereço MAC e versão do firmware, por meio da descoberta de rede. Uma impressão digital do dispositivo pode ser criada na interface de impressões digitais de dispositivos no Aruba ClearPass Policy Manager. É possível atualizar e gerenciar a impressão digital do dispositivo. Uma das coisas que é possível fazer é conceder ou negar acesso dependendo da versão do sistema operacional AXIS.

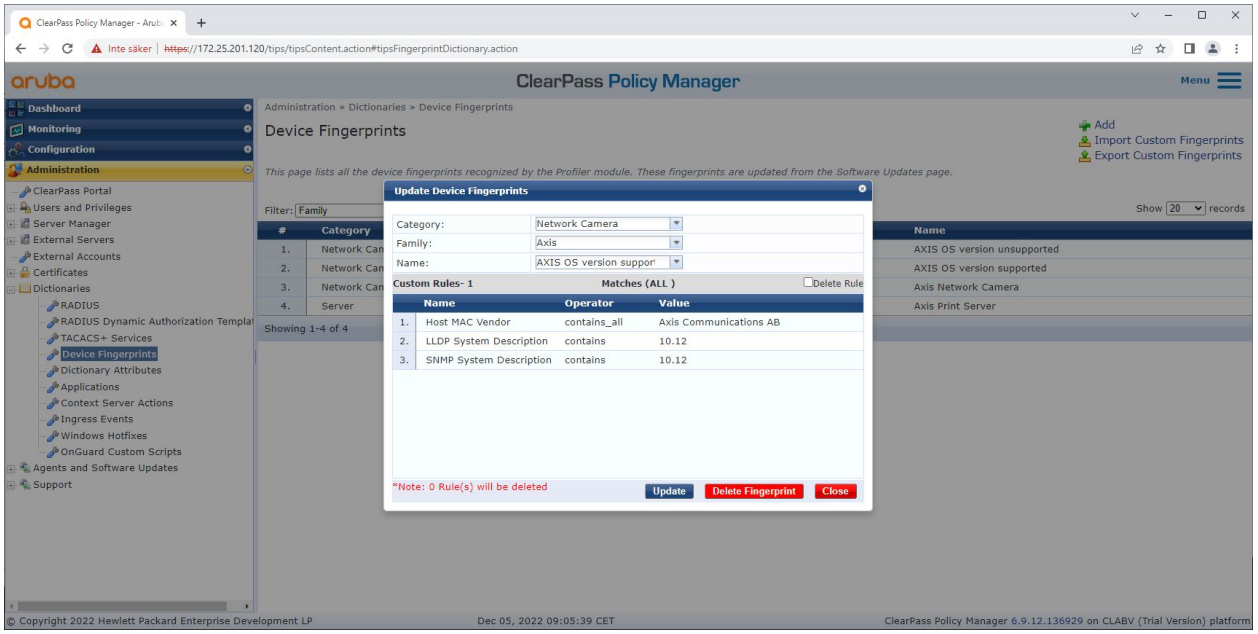
É possível atualizar e gerenciar a impressão digital do dispositivo. Uma das coisas que é possível fazer é conceder ou negar acesso dependendo da versão do sistema operacional AXIS.

Integração segura – IEEE 802.1AR/802.1X

1. Vá para **Administration > Dictionaries > Device Fingerprints (Administração > Dicionários > Impressões digitais de dispositivos)**.
2. Selecione uma impressão digital de dispositivo existente ou crie uma nova impressão digital de dispositivo.
3. Defina as configurações de impressão digital do dispositivo.



A configuração da impressão digital do dispositivo no Aruba ClearPass Policy Manager. Os dispositivos Axis que executam qualquer outra versão de firmware diferente de 10.12 são considerados sem suporte.



A configuração da impressão digital do dispositivo no Aruba ClearPass Policy Manager. Os dispositivos Axis que executam o firmware 10.12 são considerados compatíveis no exemplo acima.

Secure integration of Axis devices into Aruba networks

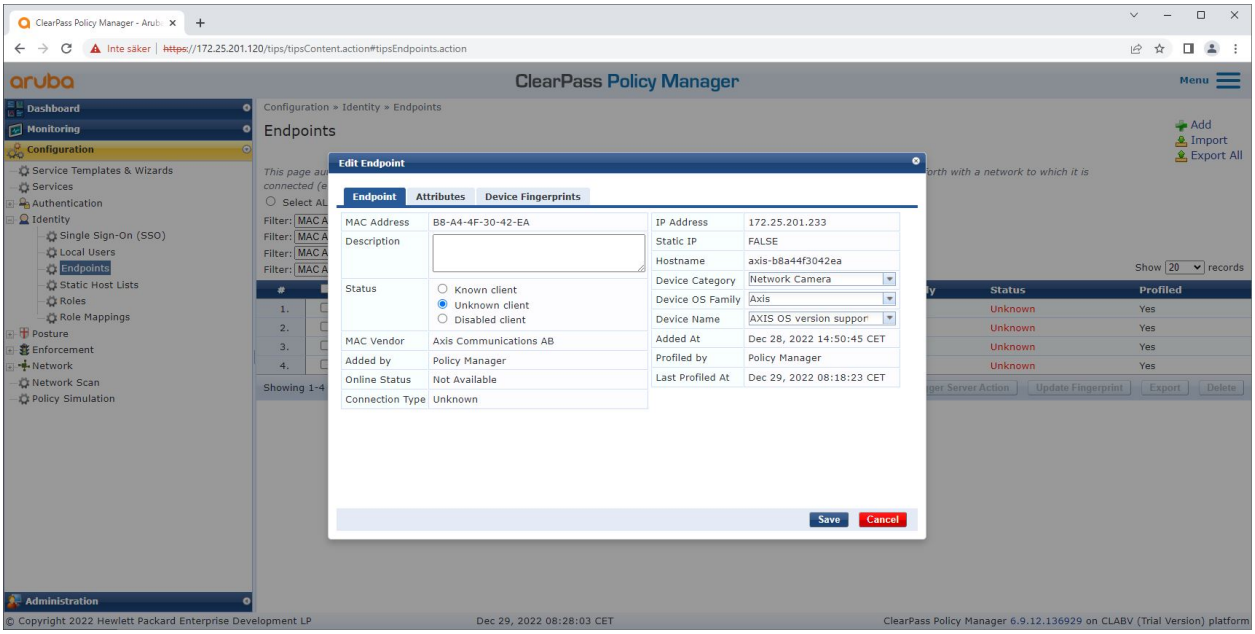
Integração segura – IEEE 802.1AR/802.1X

As informações sobre a impressão digital do dispositivo coletada pelo Aruba ClearPass Manager podem ser encontradas na seção Endpoints.

1. Vá para **Configuration > Identity > Endpoints (Configuração > Identidade > Endpoints)**.
2. Selecione o dispositivo que deseja visualizar.
3. Clique na guia Device Fingerprints (Impressões digitais de dispositivos).

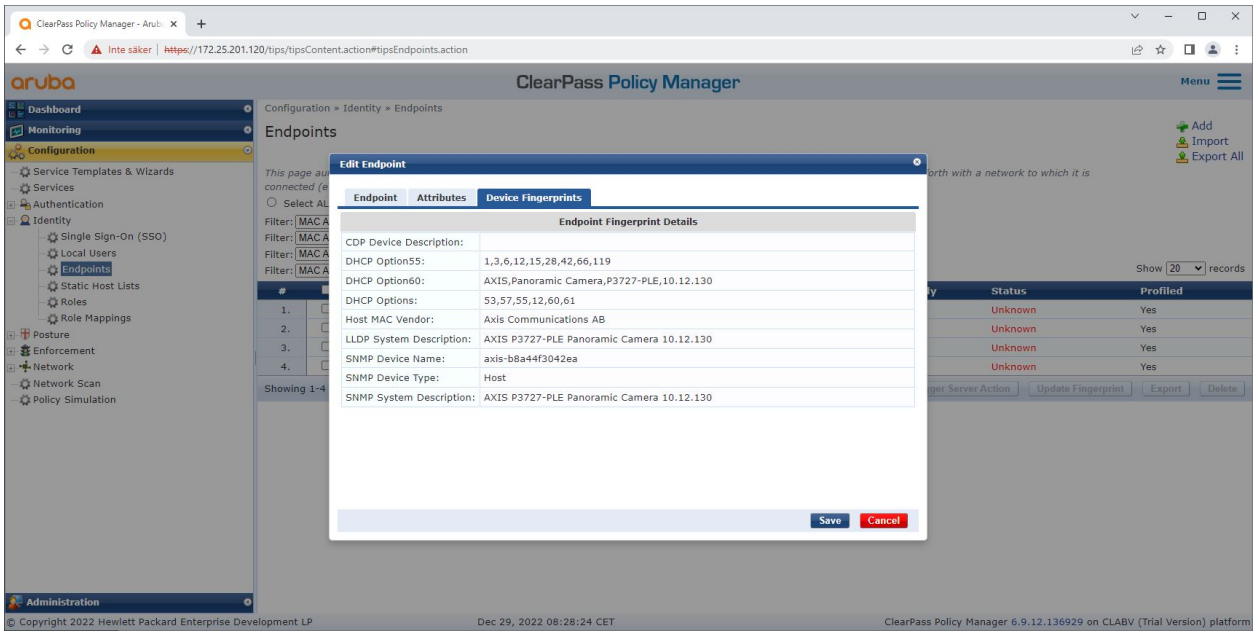
Observação

O SNMP é desabilitado por padrão em dispositivos Axis e coletado do switch de acesso Aruba.



Um dispositivo Axis cujo perfil foi criado pelo Aruba ClearPass Policy Manager.

Integração segura – IEEE 802.1AR/802.1X



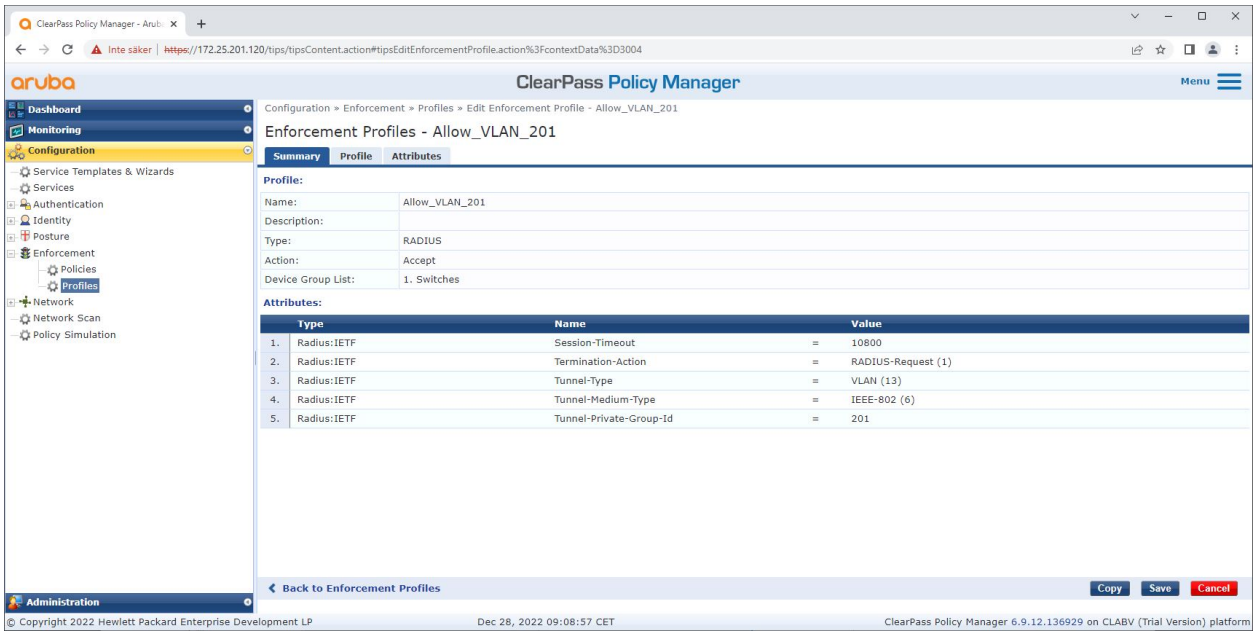
As impressões digitais detalhadas de um dispositivo Axis com perfil estabelecido. Observe que o SNMP está desabilitado por padrão nos dispositivos Axis. As informações de descoberta específicas de LLDP, CDP e DHCP são compartilhadas pelo dispositivo Axis no estado padrão de fábrica e retransmitidas pelo switch de acesso Aruba para o ClearPass Policy Manager.

Configuração do perfil de imposição

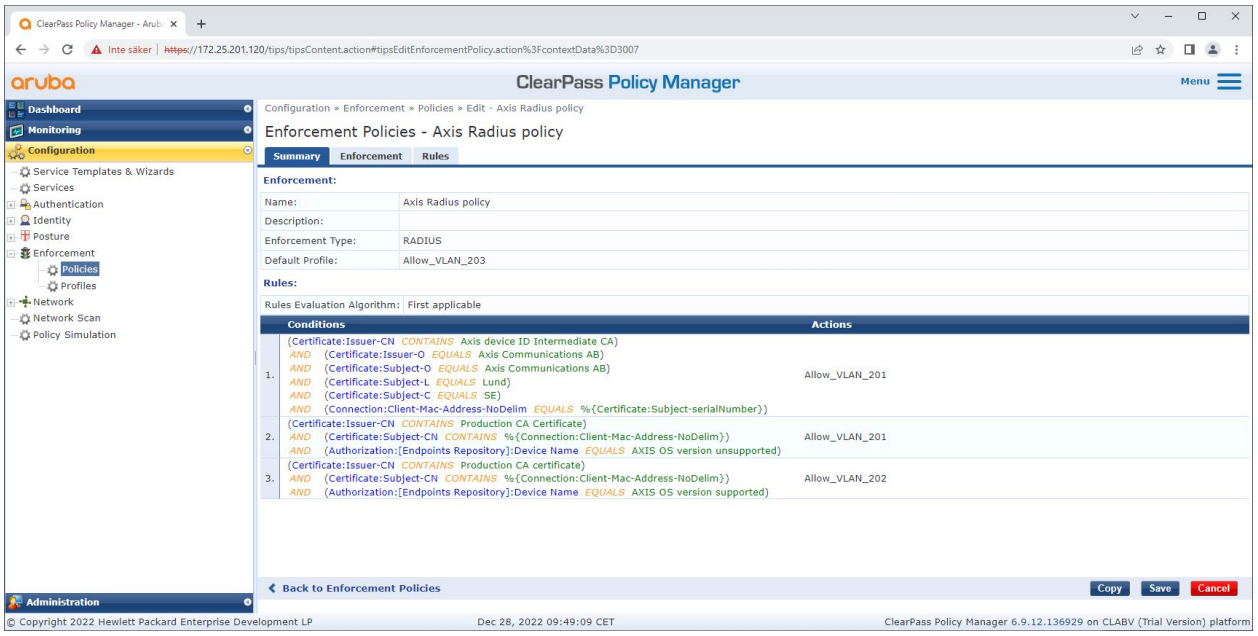
O perfil de imposição é usado para permitir que o Aruba ClearPass Policy Manager atribua um ID de VLAN específico a uma porta de acesso no switch. É uma decisão baseada em políticas que se aplica aos dispositivos de rede no grupo de dispositivos "switches". O número necessário de perfis de imposição depende do número de VLANs que serão utilizadas. Na nossa configuração, há um total de três VLANs (VLAN 201, 202, 203), que se correlacionam com três perfis de imposição.

Depois que os perfis de imposição da VLAN forem configurados, a política de imposição real poderá ser configurada. A configuração da política de imposição no Aruba ClearPass Policy Manager define se os dispositivos Axis recebem acesso às redes Aruba com base em quatro exemplos de perfis de política.

Integração segura – IEEE 802.1AR/802.1X



Um exemplo de perfil de imposição para permitir acesso à VLAN 201.



A configuração da política de imposição no Aruba ClearPass Policy Manager.

As quatro políticas de imposição e suas ações estão listadas abaixo:

Acesso à rede negado

O acesso à rede é negado quando nenhuma autenticação de controle de acesso à rede IEEE 802.1X é executada.

Rede de convidados (VLAN 203)

Secure integration of Axis devices into Aruba networks

Integração segura – IEEE 802.1AR/802.1X

O dispositivo Axis terá acesso a uma rede limitada e isolada se a autenticação de controle de acesso à rede IEEE 802.1X falhar. A inspeção manual do dispositivo é necessária para tomar as ações apropriadas.

Rede de provisionamento (VLAN 201)

O dispositivo Axis recebe acesso a uma rede de provisionamento. O objetivo é fornecer recursos de gerenciamento de dispositivos Axis via *Axis Device Manager* e *Axis Device Manager Extend*. Isso também permite configurar dispositivos Axis com atualizações de firmware, certificados de nível de produção e outras configurações. As seguintes condições são verificadas pelo Aruba ClearPass Policy Manager:

- A versão do firmware do dispositivo Axis.
- O endereço MAC do dispositivo compara o esquema de endereços MAC da Axis específico do fornecedor com o atributo de número de série do certificado de ID do dispositivo Axis.
- O certificado de ID do dispositivo Axis é verificável e corresponde aos atributos específicos da Axis, como emissor, organização, local, país.

Rede de produção (VLAN 202)

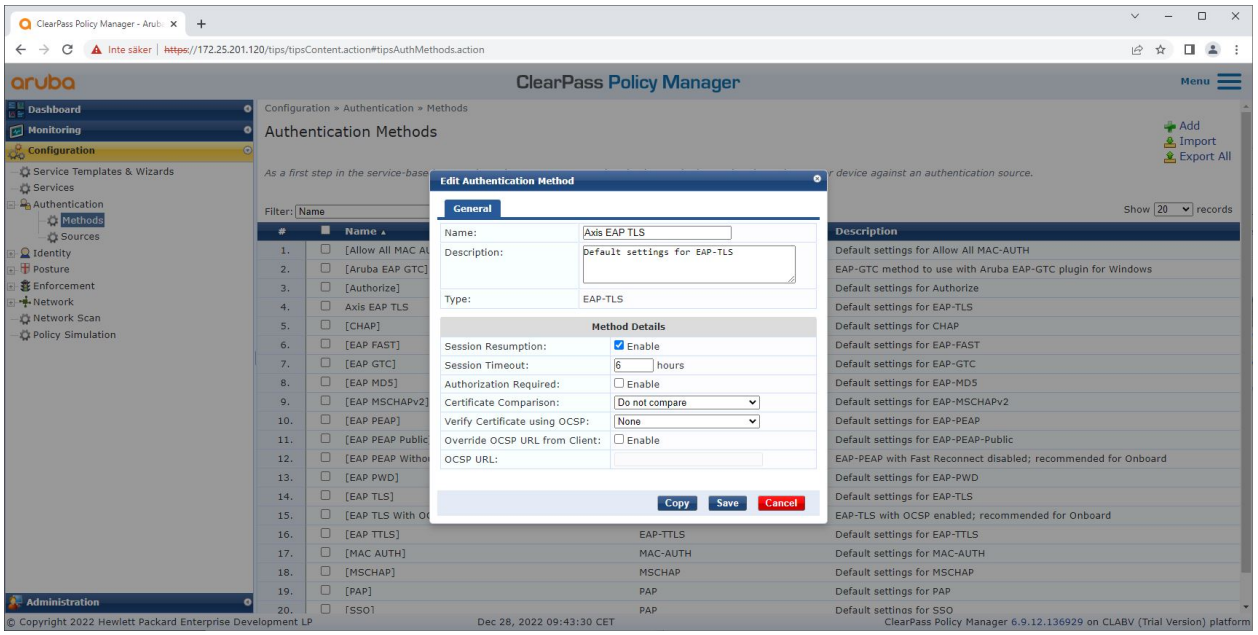
O dispositivo Axis recebe acesso à rede de produção em que o dispositivo Axis irá operar. O acesso é concedido após a conclusão do provisionamento do dispositivo na rede de provisionamento (VLAN 201). As seguintes condições são verificadas pelo Aruba ClearPass Policy Manager:

- O endereço MAC do dispositivo compara o esquema de endereços MAC da Axis específico do fornecedor com o atributo de número de série do certificado de ID do dispositivo Axis.
- A versão do firmware do dispositivo Axis.
- O certificado de nível de produção pode ser verificado pelo armazenamento de certificados confiável.

Configuração do método de autenticação

A forma como um dispositivo Axis tentará se autenticar na rede Aruba é definida no método de autenticação. O método preferido de autenticação deve ser IEEE 802.1X EAP-TLS, já que os dispositivos Axis com suporte a Axis Edge Vault são fornecidos com IEEE 802.1X EAP-TLS habilitado por padrão.

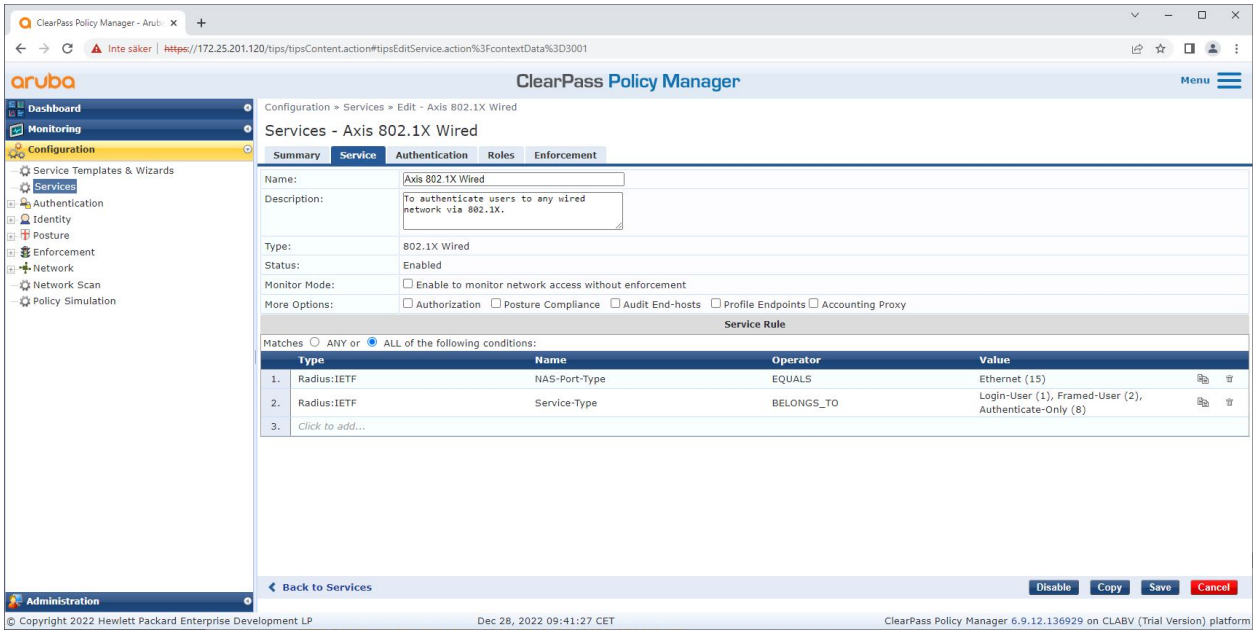
Integração segura – IEEE 802.1AR/802.1X



A interface do método de autenticação do Aruba ClearPass Policy Manager em que o método de autenticação EAP-TLS para dispositivos Axis é definido.

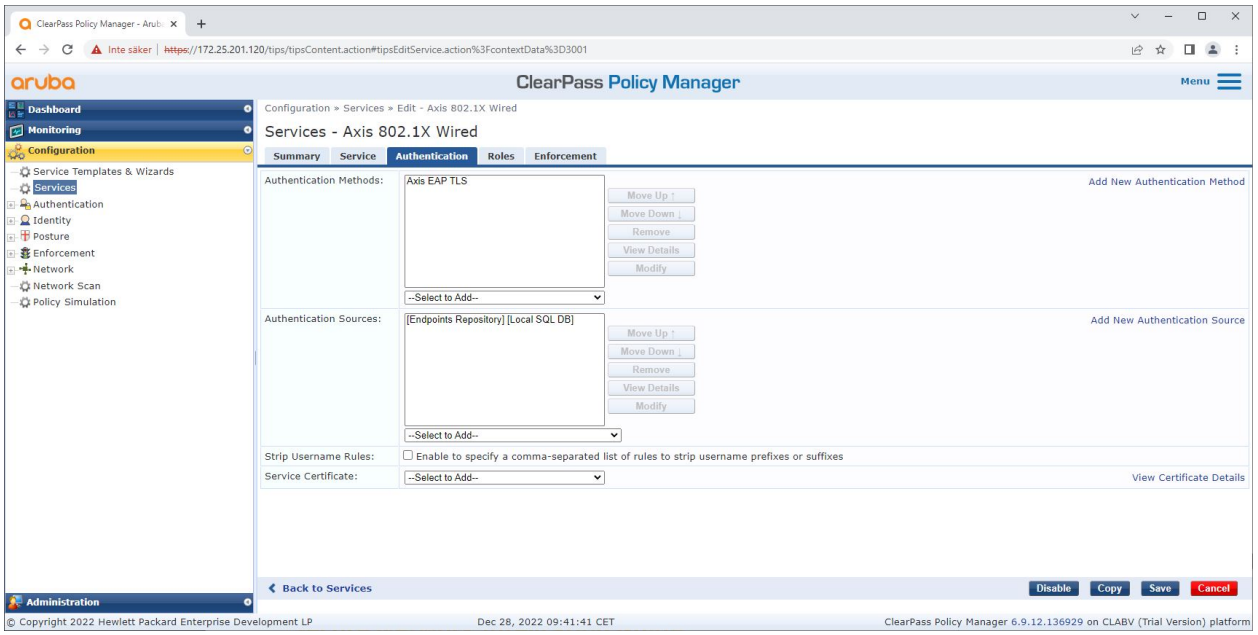
Configuração do serviço

Na interface de serviços, as etapas de configuração são combinadas em um único serviço que trata da autenticação e autorização de dispositivos Axis em redes Aruba.

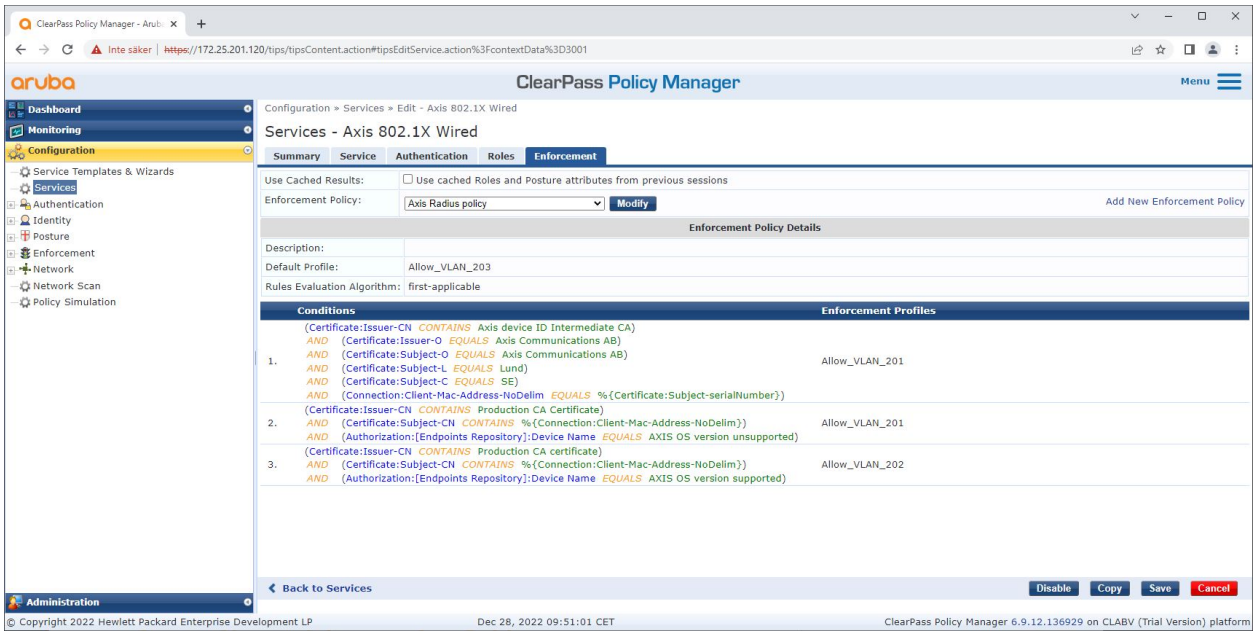


Um serviço Axis dedicado é criado e define IEEE 802.1X como método de conexão.

Integração segura – IEEE 802.1AR/802.1X



Na próxima etapa, o método de autenticação EAP-TLS criado anteriormente é configurado para o serviço.



Na última etapa, a política de imposição criada anteriormente é configurada para o serviço.

Switch de acesso Aruba

Os dispositivos Axis são conectados diretamente a switches de acesso Aruba compatíveis com PoE ou por meio de midspans Axis PoE compatíveis. Para integrar dispositivos Axis com segurança às redes Aruba, o switch de acesso precisa ser configurado para comunicação IEEE 802.1X. O dispositivo Axis retransmite a comunicação IEEE 802.1x EAP-TLS para o Aruba ClearPass Policy Manager, que atua como um servidor RADIUS.

Integração segura – IEEE 802.1AR/802.1X

Observação

Uma reautenticação periódica de 300 segundos para o dispositivo Axis também é configurada para aumentar a segurança geral do acesso à porta.

Consulte o exemplo abaixo de configuração global e de porta para switches de acesso Aruba.

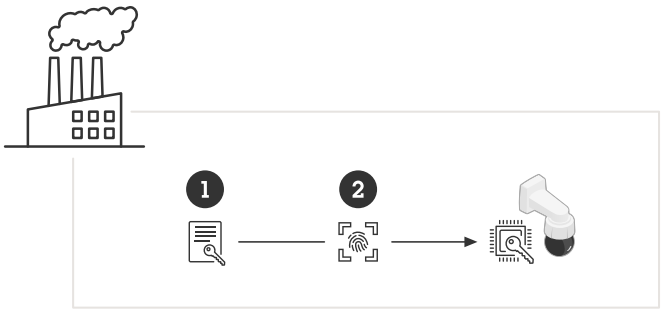
```
radius-server host MyRADIUSIPAddress key "MyRADIUSKey"

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
```

Configuração Axis

Dispositivo de rede Axis

Os dispositivos Axis compatíveis com o *Axis Edge Vault* são fabricados com uma identidade de dispositivo segura chamada ID de dispositivo Axis. O ID do dispositivo Axis é baseado no padrão internacional IEEE 802.1AR, que define um método para identificação automatizada e segura de dispositivos e integração de rede por meio do IEEE 802.1X.



Os dispositivos Axis são fabricados com o certificado de ID de dispositivo Axis compatível com IEEE 802.1AR para serviços de identidade de dispositivos confiáveis

1 *Infraestrutura de chave de ID de dispositivo Axis (PKI)*
2 *ID de dispositivo Axis*

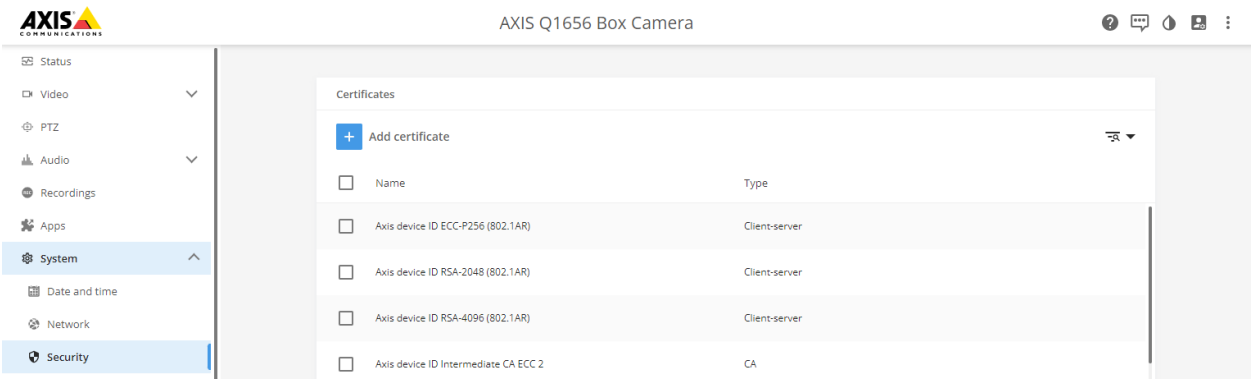
O armazenamento de chaves seguro protegido por hardware fornecido por um elemento seguro do dispositivo Axis é fornecido de fábrica com um certificado exclusivo do dispositivo e chaves correspondentes (ID do dispositivo Axis) que podem comprovar globalmente a autenticidade do dispositivo Axis. O *Seletor de produtos Axis* pode ser usado para identificar quais dispositivos Axis oferecem suporte ao Axis Edge Vault e ao ID de dispositivo Axis.

Observação

O número de série de um dispositivo Axis é o seu endereço MAC.

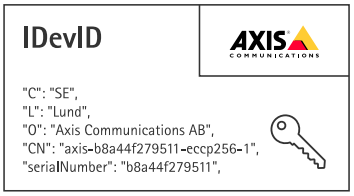
Secure integration of Axis devices into Aruba networks

Integração segura – IEEE 802.1AR/802.1X



O armazenamento de certificados do dispositivo Axis no estado padrão de fábrica com o ID de dispositivo Axis.

O certificado de ID de dispositivo Axis compatível com IEEE 802.1AR inclui informações sobre o número de série e outras informações específicas do fornecedor Axis. As informações são usadas pelo Aruba ClearPass Policy Manager para fins de análise e tomada de decisões de concessão de acesso à rede. Consulte as informações abaixo que podem ser obtidas em um certificado de ID de dispositivo Axis

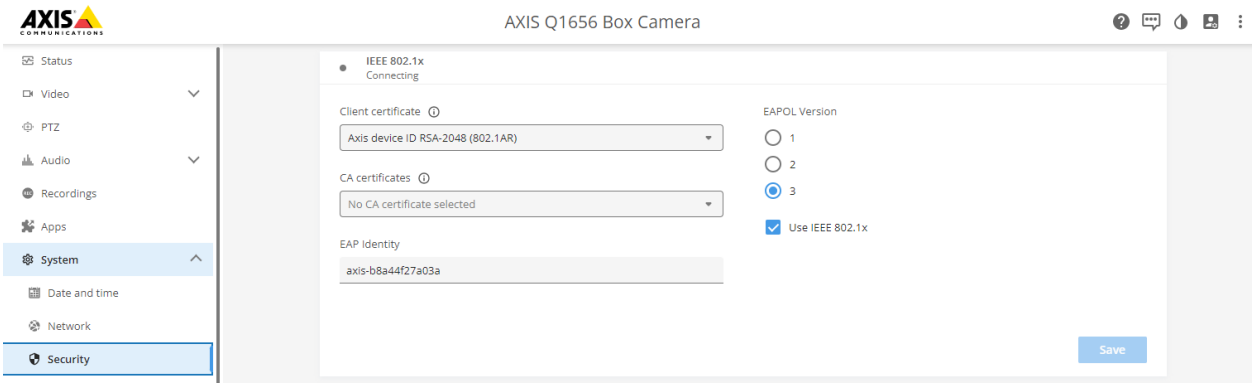


País	SE
Localização	Lund
Organização emissora	Axis Communications AB
Nome comum de emissor	Intermediário de ID de dispositivo Axis
Organização	Axis Communications AB
Nome comum	axis-b8a44f279511-eccp256-1
Número de série	b8a44f279511

O nome comum é construído por uma combinação do nome da empresa Axis e o número de série do dispositivo seguido pelo algoritmo de criptografia (ECC P256, RSA 2048, RSA 4096) usado. Começando no AXIS OS 10.1 (2020-09), o IEEE 802.1X é habilitado por padrão com o ID do dispositivo Axis pré-configurado. Isso permite que o dispositivo Axis se autentique em redes habilitadas para IEEE 802.1X.

Secure integration of Axis devices into Aruba networks

Integração segura – IEEE 802.1AR/802.1X



O dispositivo Axis no estado padrão de fábrica com IEEE 802.1X habilitado e certificado de ID do dispositivo Axis pré-selecionado.

Axis Device Manager

O *AXIS Device Manager* e o *AXIS Device Manager Extend* podem ser usados na rede para configurar e gerenciar vários dispositivos Axis de maneira econômica. O Axis Device Manager é um aplicativo baseado em Microsoft Windows que pode ser instalado localmente em uma máquina na rede, enquanto o Axis Device Manager Extend depende da infraestrutura em nuvem para fazer o gerenciamento de dispositivos em vários locais. Ambos oferecem recursos fáceis de gerenciamento e configuração para dispositivos Axis, como:

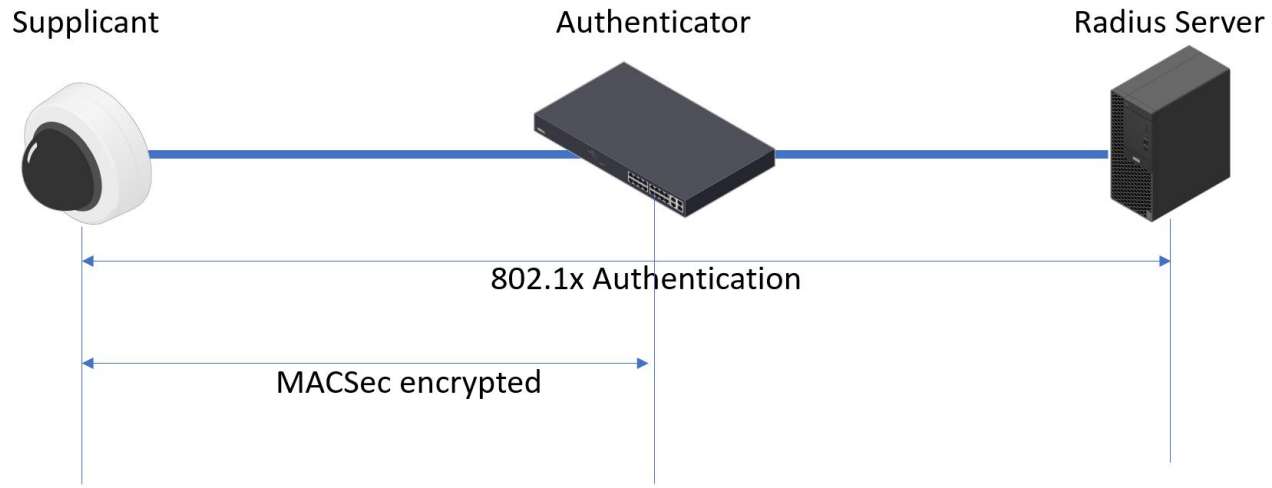
- Instalação de atualizações de firmware.
- Aplicação de configurações de segurança cibernética, como certificados HTTPS e IEEE 802.1X.
- Configuração de opções específicas do dispositivo, como configurações de imagens e outras.

Operação de rede segura – IEEE 802.1AE MACsec

O IEEE 802.1AE MACsec (Media Access Control Security) é um protocolo de rede bem definido que protege criptograficamente links Ethernet ponto a ponto na camada de rede 2. Ele garante a confidencialidade e integridade das transmissões de dados entre dois hosts.

O padrão IEEE 802.1AE MACsec descreve dois modos de operação:

- Modo de chave pré-compartilhada configurável manualmente/modo CAK estático
- Modo de sessão principal automática/CAK dinâmico usando IEEE802.1X EAP-TLS



No AXIS OS 10.1 (2020-09) e posteriores, o IEEE802.1X é habilitado por padrão para dispositivos compatíveis com ID do dispositivo Axis. No AXIS OS 11.8 e posterior, oferecemos suporte a MACsec com modo dinâmico automático usando IEEE802.1X EAP-TLS habilitado por padrão. Ao conectar um dispositivo Axis com valores padrão de fábrica, a autenticação de rede IEEE802.1X é executada e, quando bem-sucedida, o modo MACsec Dynamic CAK também é tentado.

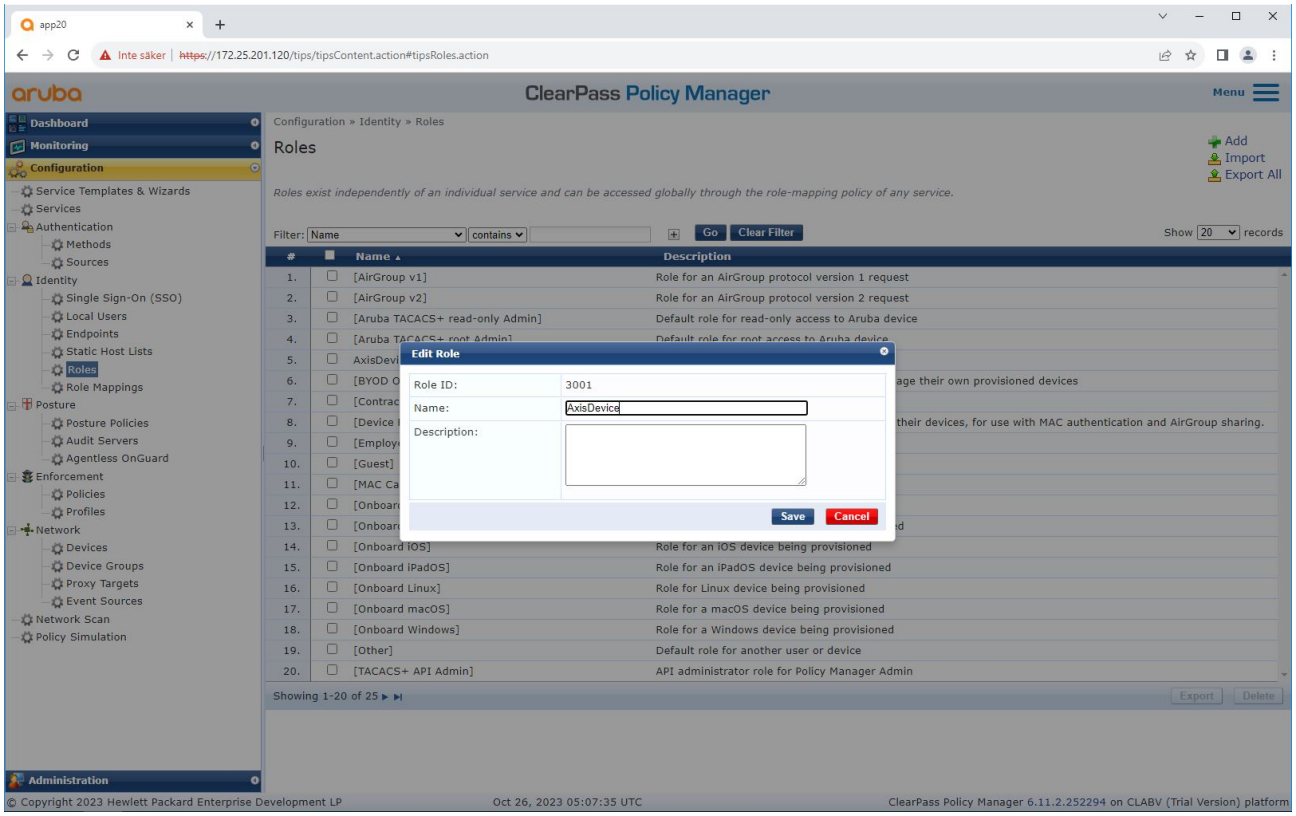
O ID do dispositivo Axis armazenado com segurança (1), uma identidade de dispositivo segura compatível com IEEE 802.1AR, é usado para autenticar na rede Aruba (4, 5) via controle de acesso à rede baseado em porta IEEE 802.1X EAP-TLS (2). Por meio da sessão EAP-TLS, as chaves MACsec são trocadas automaticamente para configurar um link seguro (3), protegendo todo o tráfego de rede do dispositivo Axis para o switch Aruba.

O IEEE 802.1AE MACsec requer preparações de configuração do switch de acesso Aruba e do ClearPass Policy Manager. Nenhuma configuração é necessária no dispositivo Axis para permitir a comunicação criptografada IEEE 802.1AE MACsec via EAP-TLS.

Se o switch de acesso Aruba não oferecer suporte ao MACsec usando EAP-TLS, o modo de chave pré-compartilhada poderá ser usado e configurado manualmente.

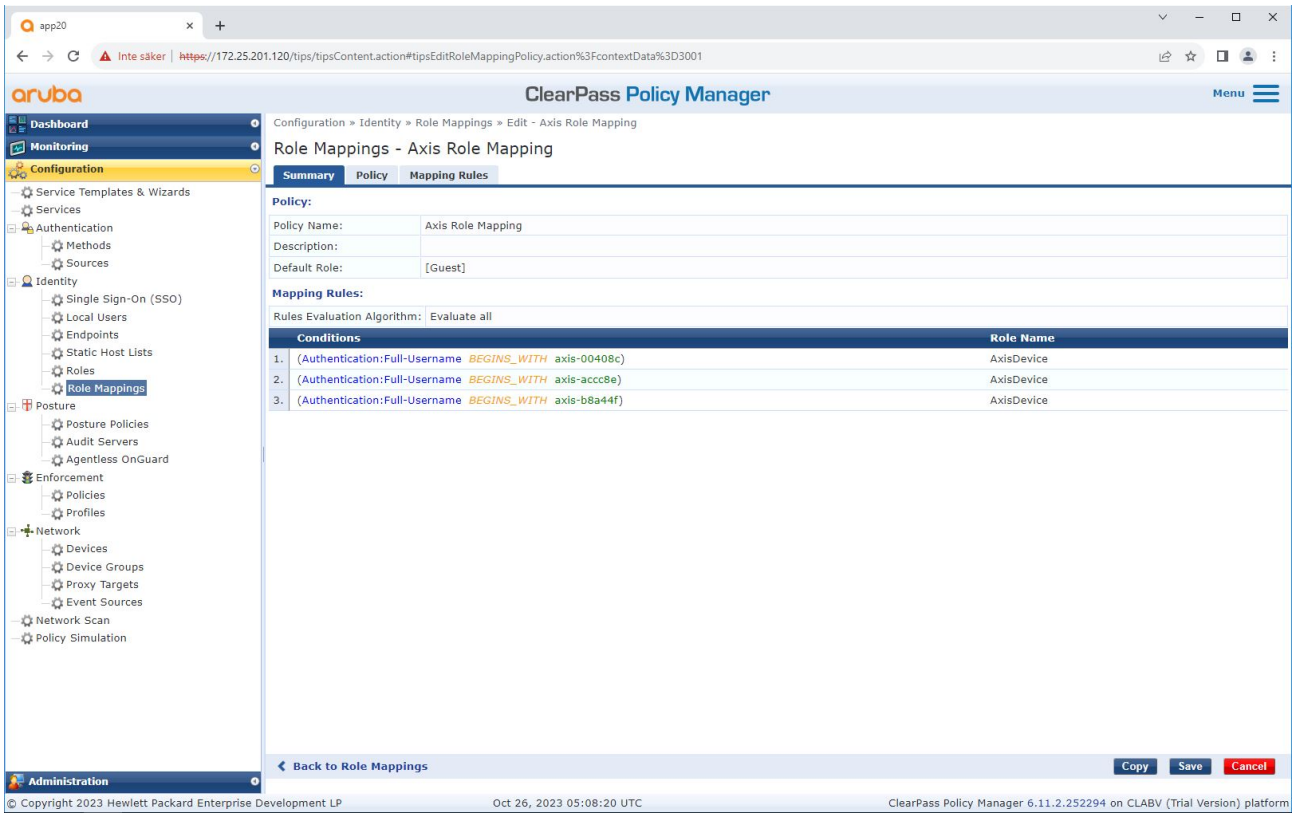
Aruba ClearPass Policy Manager

Política de funções e mapeamento de funções



Adicionando um nome de função para dispositivos Axis. O nome é o nome da função de acesso à porta na configuração do switch de acesso Aruba.

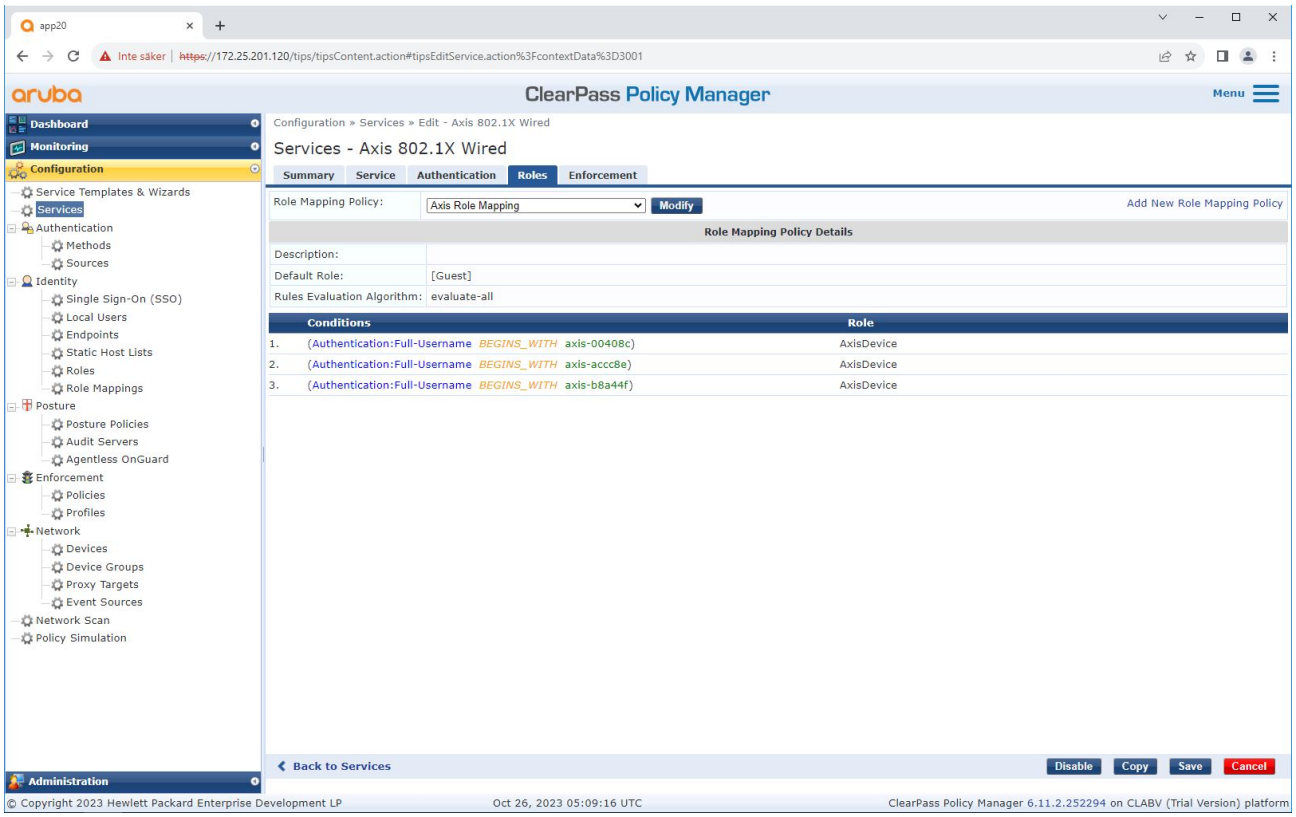
Operação de rede segura – IEEE 802.1AE MACsec



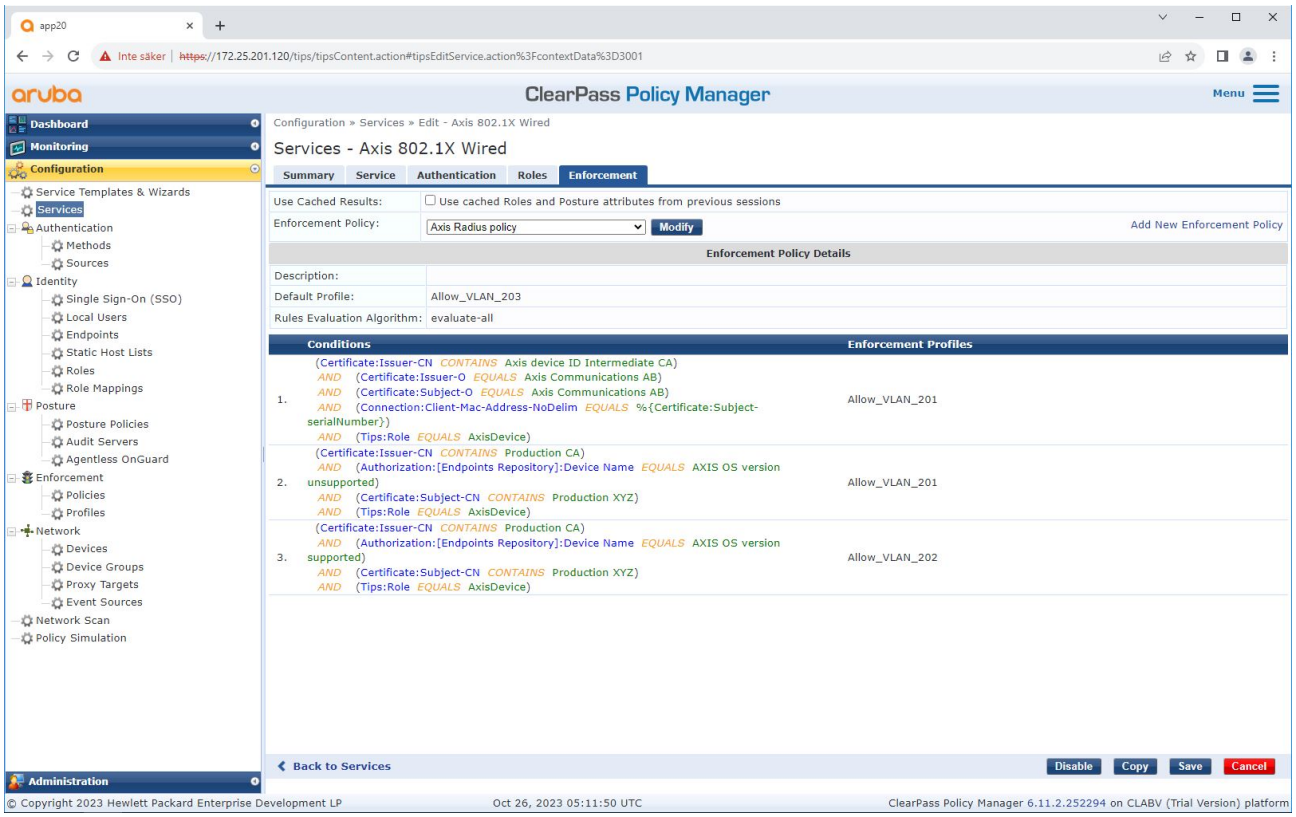
Adicionando uma política de mapeamento de função Axis para a função de dispositivo Axis criada anteriormente. As condições definidas são necessárias para que um dispositivo seja mapeado para a função de dispositivo Axis. Se as condições não forem atendidas, o dispositivo fará parte da função [Convidado].

Por padrão, os dispositivos Axis usam o formato de identidade EAP "axis-número_de_série". O número de série de um dispositivo Axis é o seu endereço MAC. Por exemplo, "axis-b8a44f45b4e6".

Configuração do serviço

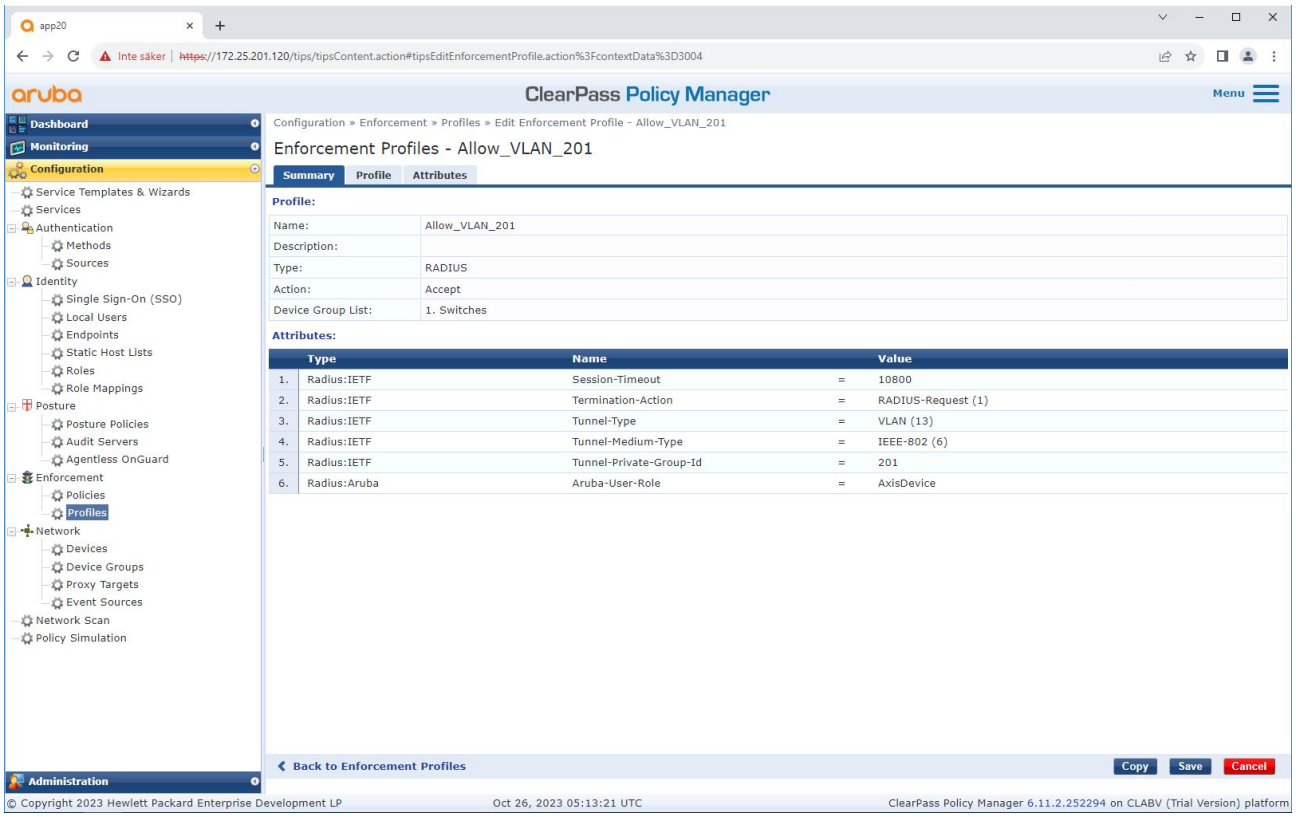


Adicionar a política de mapeamento de funções Axis criada anteriormente ao serviço que define IEEE 802.1X como método de conexão para integração de dispositivos Axis.



Adicionar o nome da função da Axis como uma condição às definições de política existentes.

Perfil de imposição



Adicionar o nome da função Axis como atributo aos perfis de imposição atribuídos no serviço de integração IEEE 802.1X.

Switch de acesso Aruba

Além da configuração de integração segura descrita em *Switch de acesso Aruba na página 16*, consulte o exemplo de configuração de porta abaixo para o switch de acesso Aruba configurar o 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
```

Integração legada – Autenticação MAC

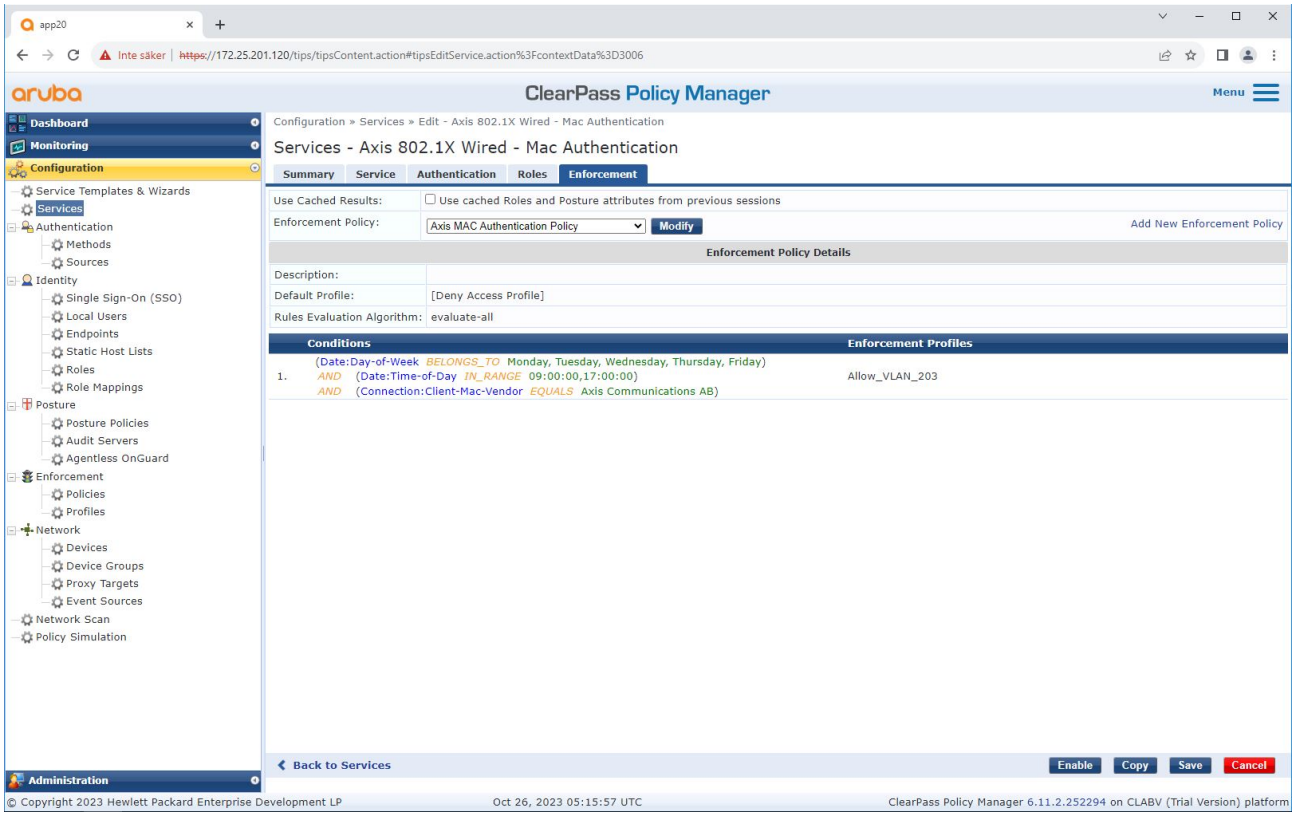
Você pode usar o MAC Authentication Bypass (MAB) para integrar dispositivos Axis que não são compatíveis com a integração do IEEE 802.1AR com o certificado de ID do dispositivo Axis e IEEE802.1X ativado no estado padrão de fábrica. Se a integração do 802.1X falhar, o Aruba ClearPass Policy Manager validará o endereço MAC do dispositivo Axis e concederá acesso à rede.

O MAB requer preparações de configuração do switch de acesso Aruba e do ClearPass Policy Manager. No dispositivo Axis, nenhuma configuração é necessária para permitir a integração do MAB.

Aruba ClearPass Policy Manager

Política de imposição

A configuração da política de imposição no Aruba ClearPass Policy Manager define se os dispositivos Axis recebem acesso às redes Aruba com base nos dois exemplos de condições de política a seguir.



Acesso à rede negado

Quando o dispositivo Axis não atende à política de imposição configurada, seu acesso à rede é negado.

Rede de convidados (VLAN 203)

O dispositivo Axis terá acesso a uma rede limitada e isolada se as seguintes condições forem atendidas:

- É um dia de semana entre segunda e sexta-feira
- É entre 9h e 17h

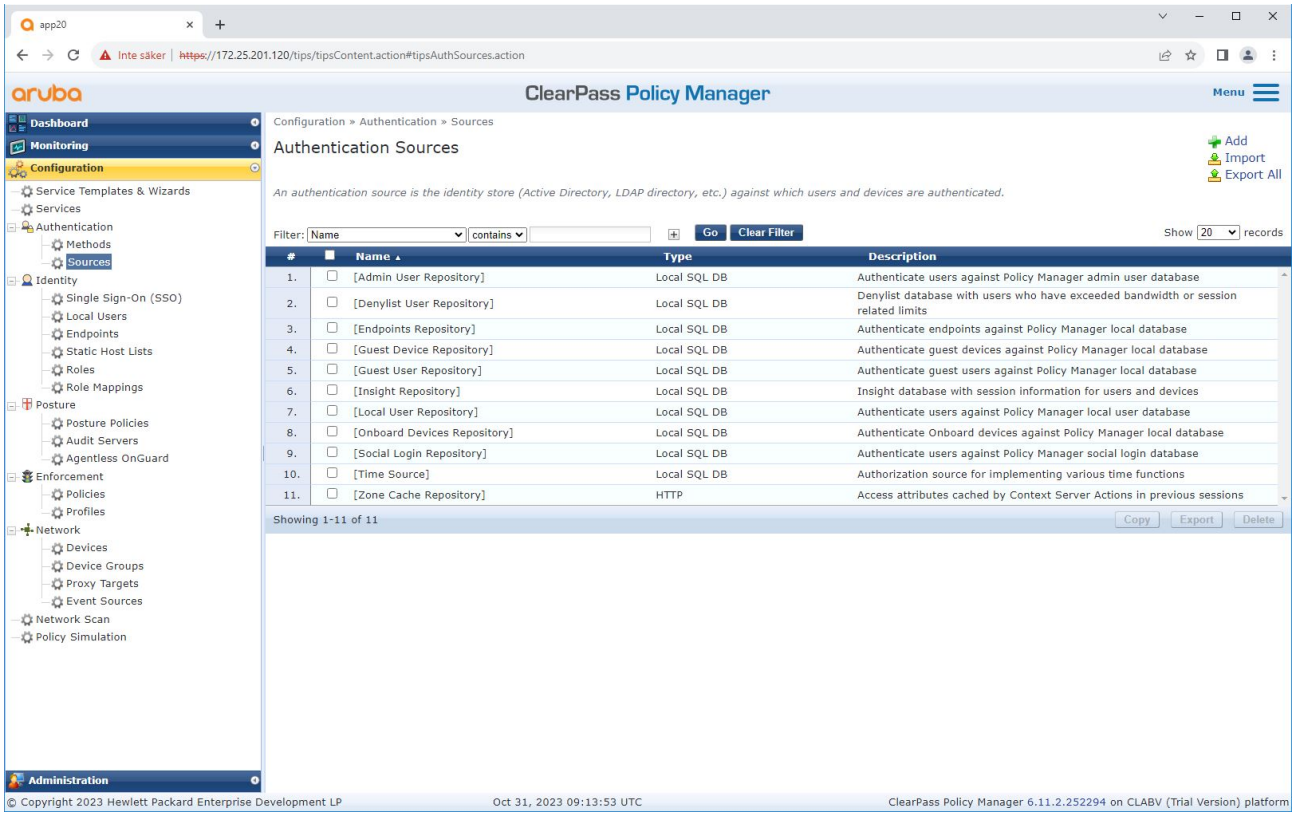
Integração legada – Autenticação MAC

- O fornecedor do endereço MAC corresponde à Axis Communications AB.

Como os endereços MAC podem ser falsificados, acesso à rede de provisionamento regular não é concedido. Recomendamos usar o MAB apenas para a integração inicial e para inspecionar manualmente o dispositivo em mais detalhes.

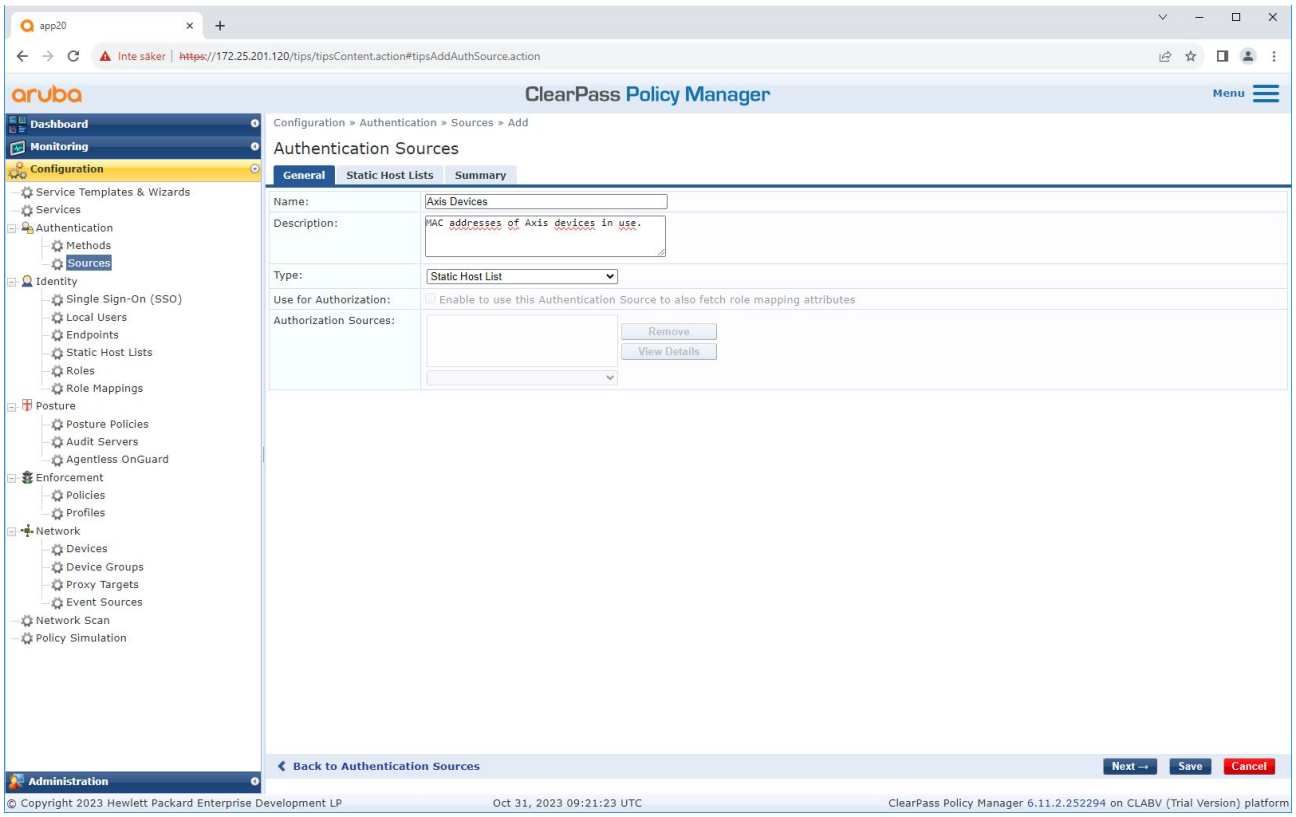
Configuração da origem

Na interface Origens, uma nova origem de autenticação é criada para permitir apenas endereços MAC importados manualmente.

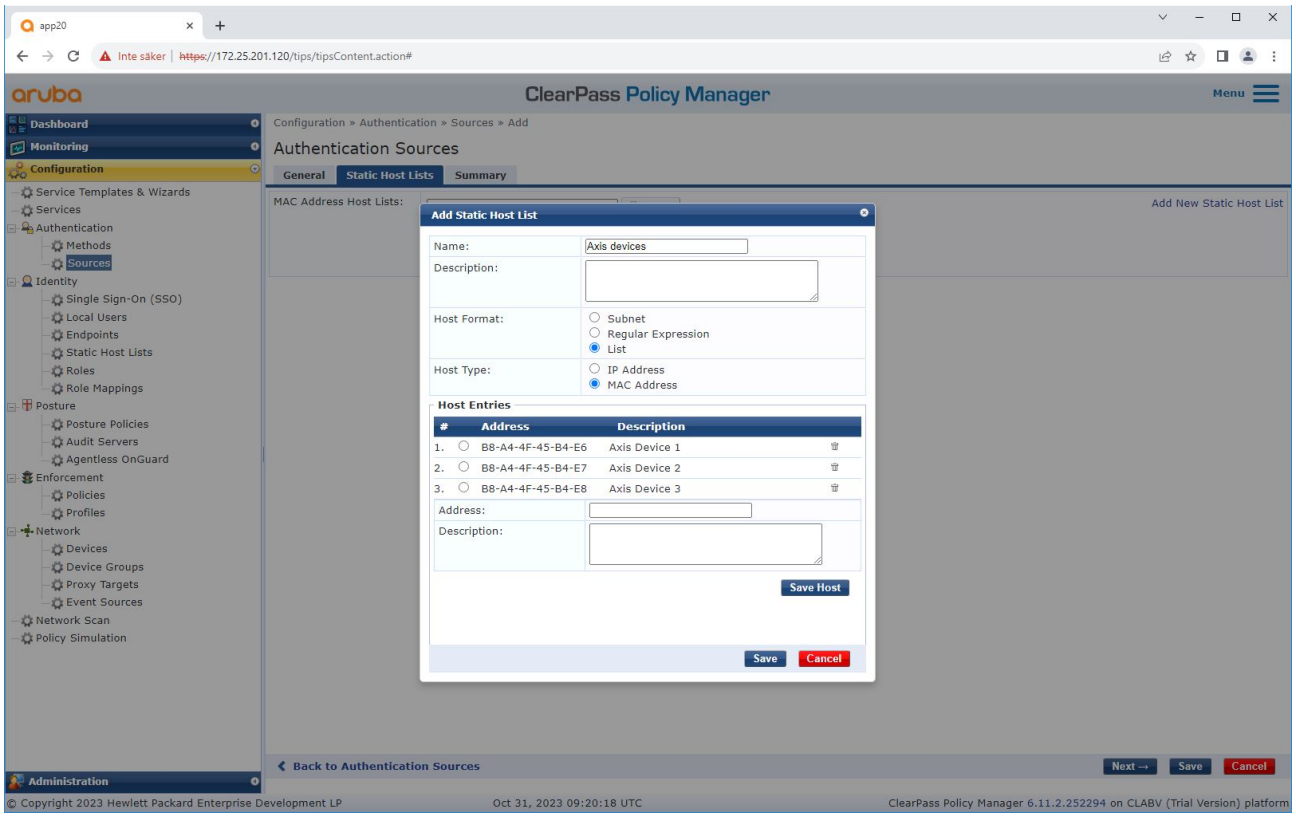


Secure integration of Axis devices into Aruba networks

Integração legada – Autenticação MAC

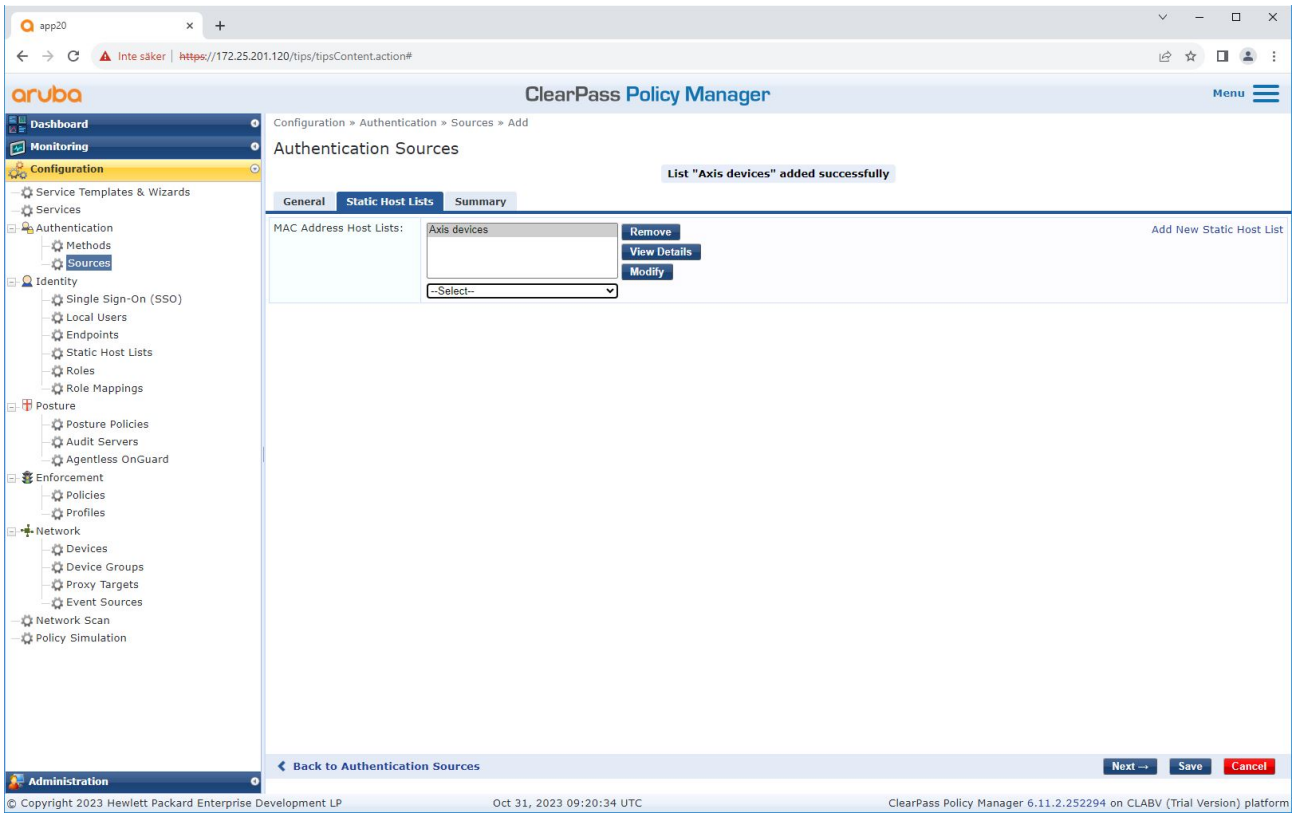


Integração legada – Autenticação MAC



Uma lista de hosts estáticos, que contém endereços MAC da Axis, é criada.

Integração legada – Autenticação MAC

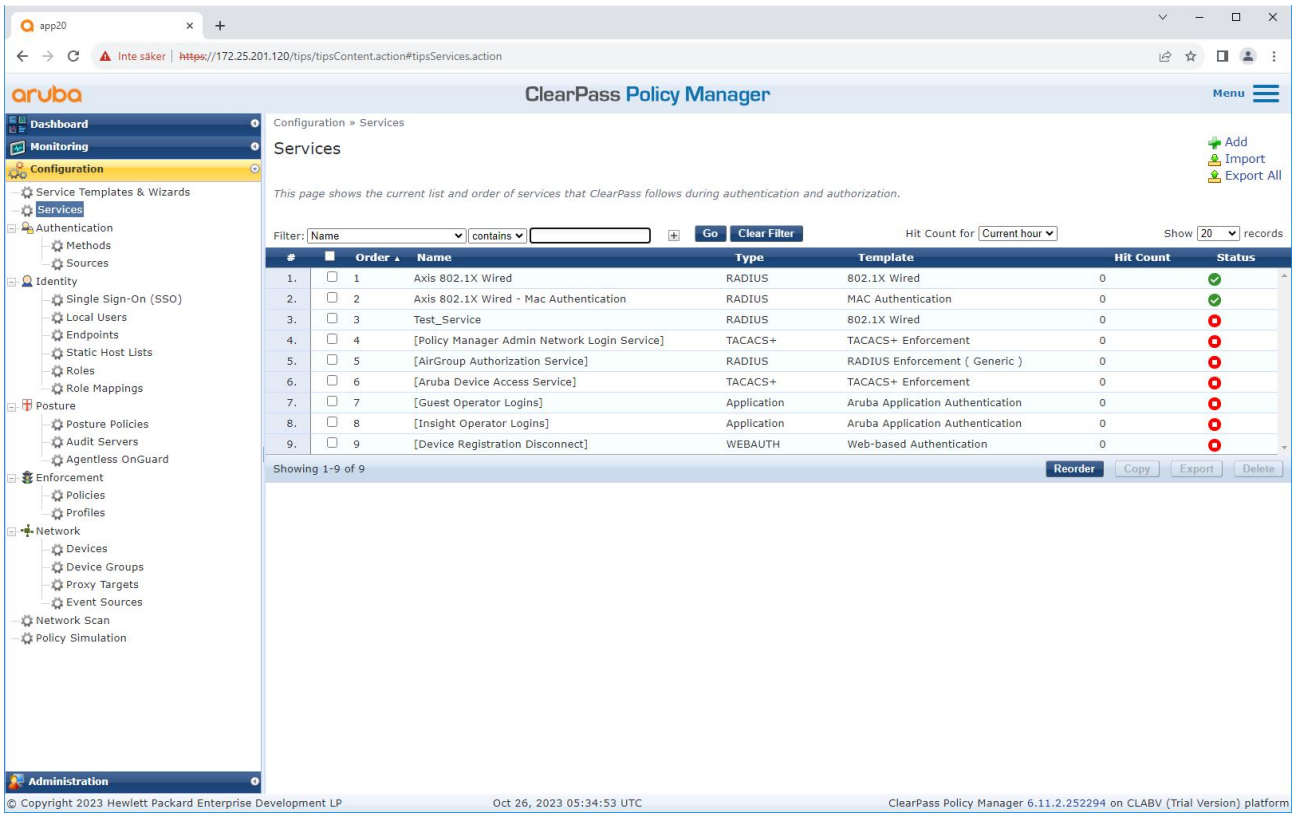


Configuração do serviço

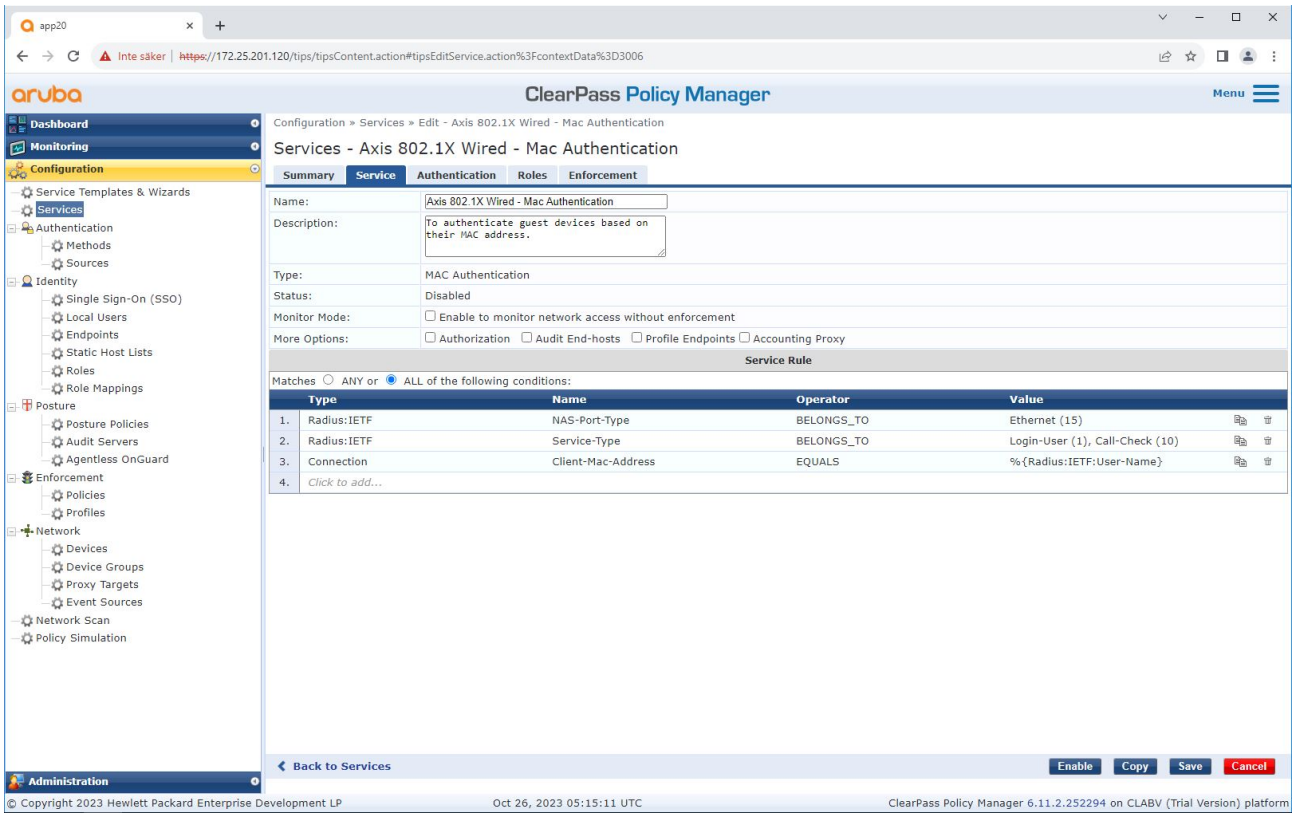
Na interface de serviços, as etapas de configuração são combinadas em um único serviço que trata da autenticação e autorização de dispositivos Axis em redes Aruba.

Secure integration of Axis devices into Aruba networks

Integração legada – Autenticação MAC

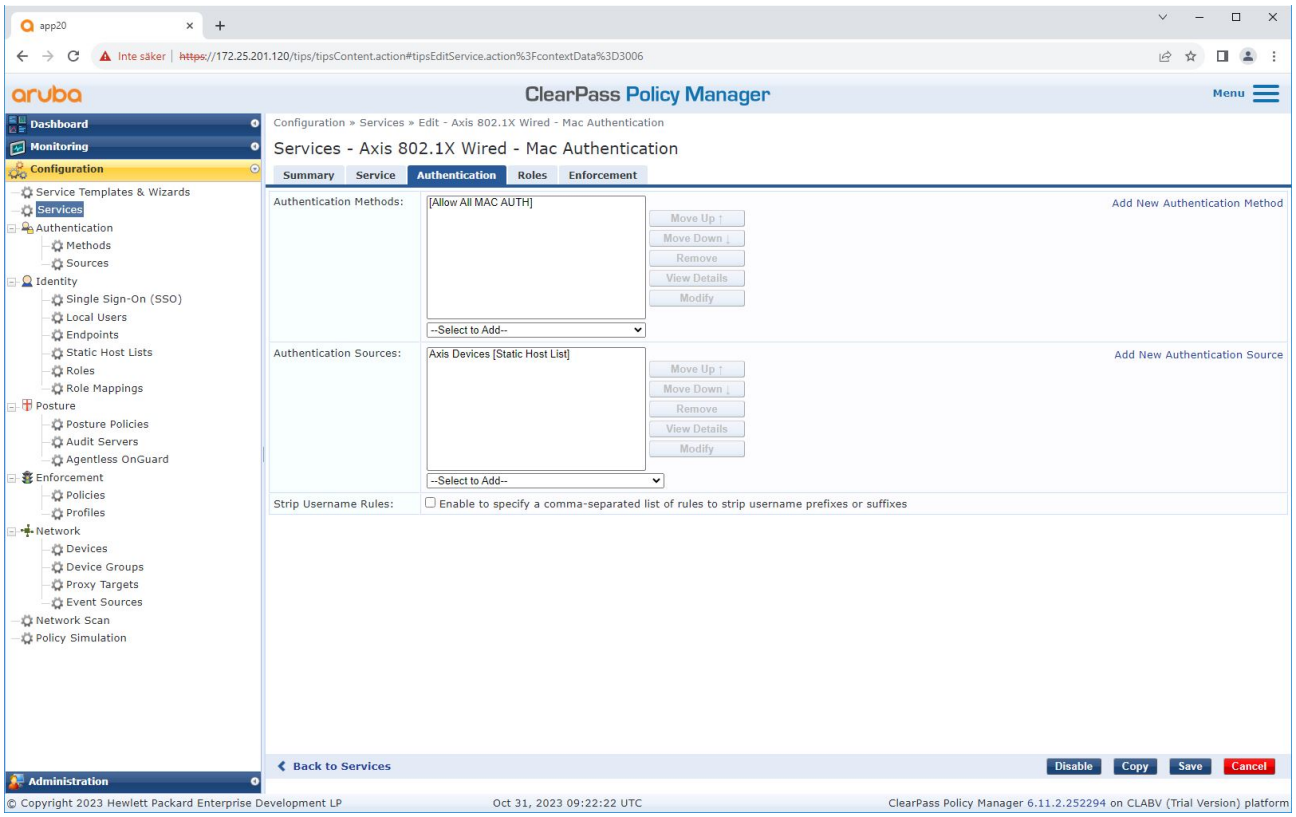


Integração legada – Autenticação MAC



Um serviço Axis dedicado que o MAB como método de conexão é criado.

Integração legada – Autenticação MAC

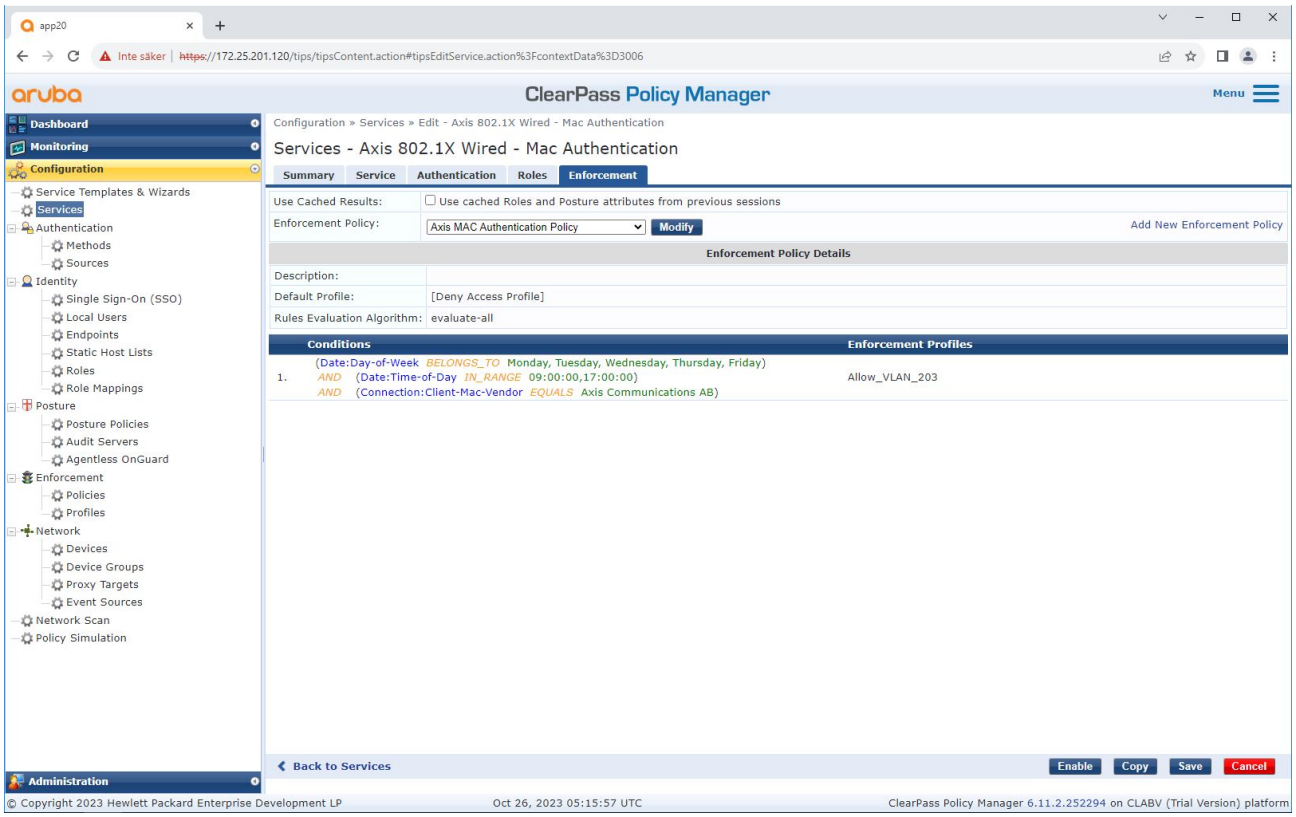


O método de autenticação MAC pré-configurado é configurado para o serviço. Além disso, a fonte de autenticação criada anteriormente que contém uma lista de endereços MAC da Axis é selecionada.

A Axis Communications AB usa os seguintes OUIs de endereço MAC:

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

Integração legada – Autenticação MAC



Na última etapa, a política de imposição criada anteriormente é configurada para o serviço.

Switch de acesso Aruba

Além da configuração de integração segura descrita em *Switch de acesso Aruba na página 16*, consulte o exemplo de configuração de porta abaixo para o switch de acesso Aruba para permitir 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 do usuário
Secure integration of Axis devices into Aruba networks

Ver. M4.3
Data: Novembro 2023
Nº da peça T10197992