

HPE Aruba Networking

Guia de integração

HPE Aruba Networking

Sumário

Introdução	3
Integração segura – IEEE 802.1AR/802.1X	4
Autenticação inicial	4
Provisionamento	4
Rede de produção	4
Configuração do HPE Aruba Networking	5
Configuração Axis	16
Operação de rede segura – IEEE 802.1AE MACsec	19
ClearPass Policy Manager do HPE Aruba Networking	20
Switch de acesso do HPE Aruba Networking	24
Integração legada – Autenticação MAC	25
ClearPass Policy Manager do HPE Aruba Networking	25
Switch de acesso do HPE Aruba Networking	33

Introdução

Este guia de integração tem como objetivo descrever as configurações recomendadas para integrar e operar dispositivos Axis em redes que usam HPE Aruba Networking. 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 aplicativos e a infraestrutura do HPE Aruba Networking. Abaixo estão alguns benefícios que é possível ganhar ao combinar dispositivos e software Axis com uma infraestrutura do HPE Aruba Networking:

- 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 as experiências da HPE 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 de infraestrutura de TI em rede corporativa pelo HPE Aruba Networking, incluindo switches de acesso ao HPE Aruba Networking e ao HPE Aruba Networking 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 é fornecido ao longo do guia.

Integração segura – IEEE 802.1AR/802.1X



Para assistir a este vídeo, vá para a versão Web deste documento.

help.axis.com/?&pid=etsection=secure-onboarding-ieee802-1ar-802-1x

Integração segura de dispositivo em redes de confiança zero com IEEE 802.1X/802.1AR

Autenticação inicial

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

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

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

O dispositivo Axis é autenticado na rede que usa HPE Aruba Networking por meio do 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, o dispositivo Axis passa 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 do AXIS OS. 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 aciona uma nova tentativa de autenticação. O ClearPass Policy Manager verifica os novos certificados e decide se o dispositivo Axis será ou não movido para a rede de produção.

Após a configuração do dispositivo, o dispositivo Axis sai da rede de provisionamento e tenta se autenticar novamente na rede.

- 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 passa para a rede de produção (VLAN 202). Nessa rede, o sistema de gerenciamento de vídeo (VMS) se conecta ao dispositivo Axis e começa 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

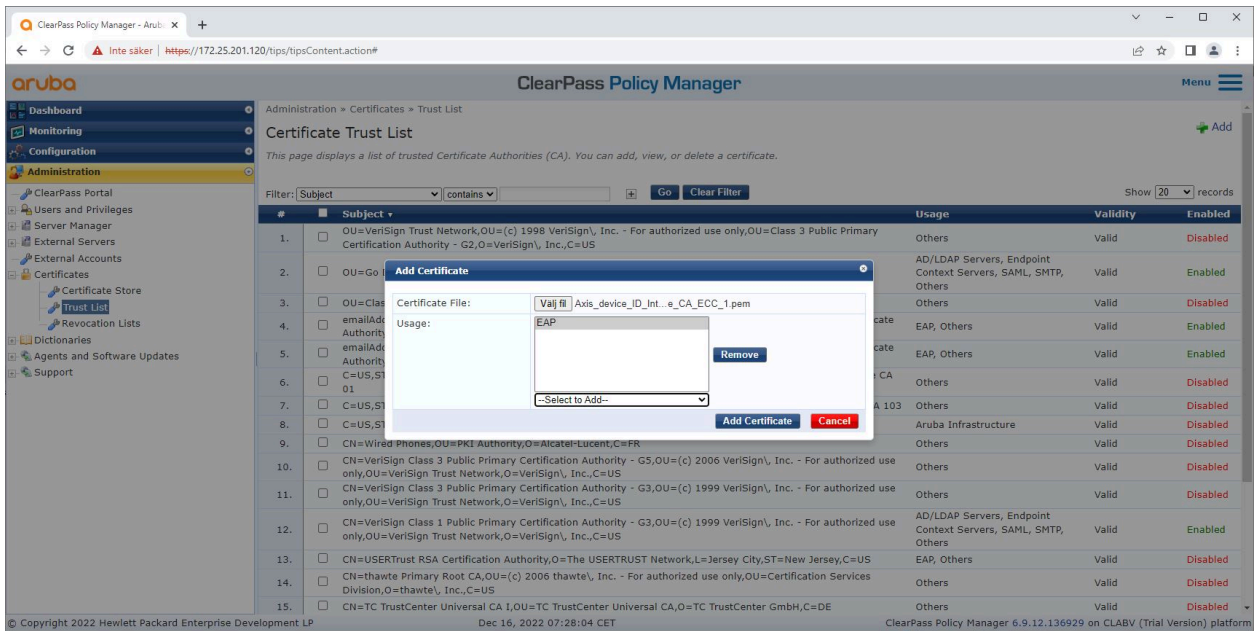
Configuração do HPE Aruba Networking

ClearPass Policy Manager do HPE Aruba Networking

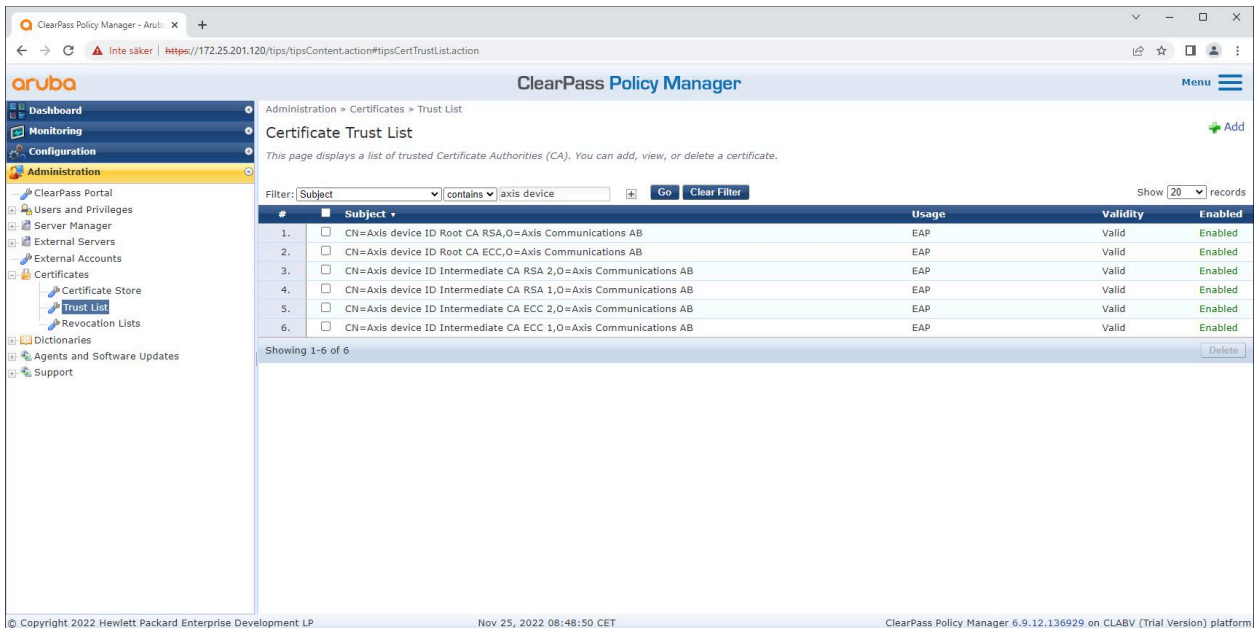
O ClearPass Policy Manager fornece controle de acesso à rede seguro baseado em função e dispositivo para IoT, BYOD, dispositivos corporativos, funcionários, prestadores de serviços e convidados em infraestrutura de rede com fio, sem fio e VPN de vários fornecedores.

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 CA raiz e CA intermediária IEEE 802.1AR específicas da Axis no armazenamento de certificados confiáveis.
3. Ative o ClearPass Policy Manager para autenticar dispositivos Axis via IEEE 802.1X EAP-TLS.
4. Selecione EAP no campo de uso. Os certificados são usados para autenticação IEEE 802.1X EAP-TLS.



Carregue os certificados IEEE 802.1AR específicos da Axis para o armazenamento de certificados confiável do ClearPass Policy Manager.



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

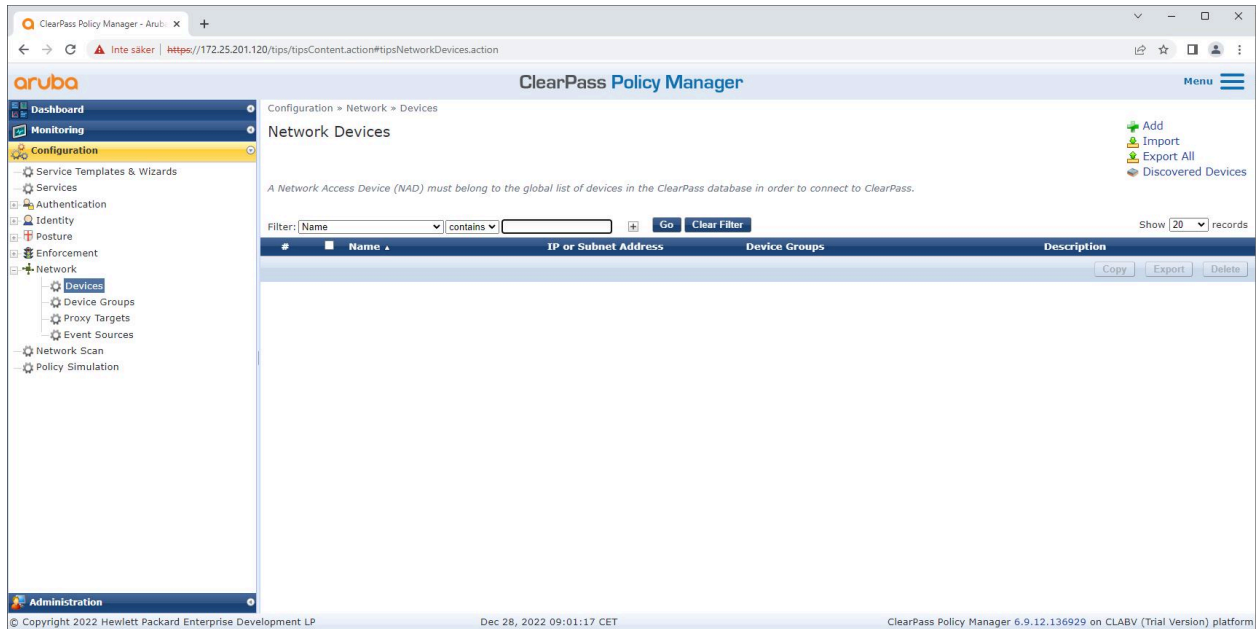
Configuração de dispositivo/grupo de rede

1. Adicione dispositivos de acesso à rede confiáveis, como switches de acesso do HPE Aruba Networking, ao ClearPass Policy Manager. O ClearPass Policy Manager precisa saber quais switches de acesso na rede são 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.

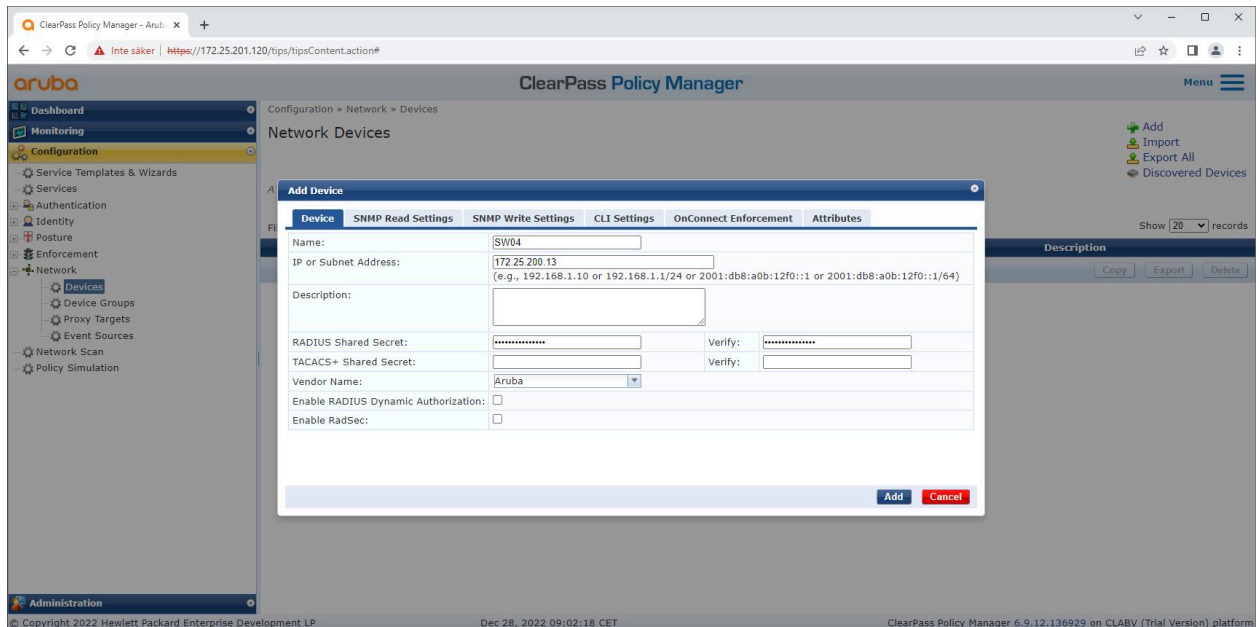
HPE Aruba Networking

Integração segura – IEEE 802.1AR/802.1X

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



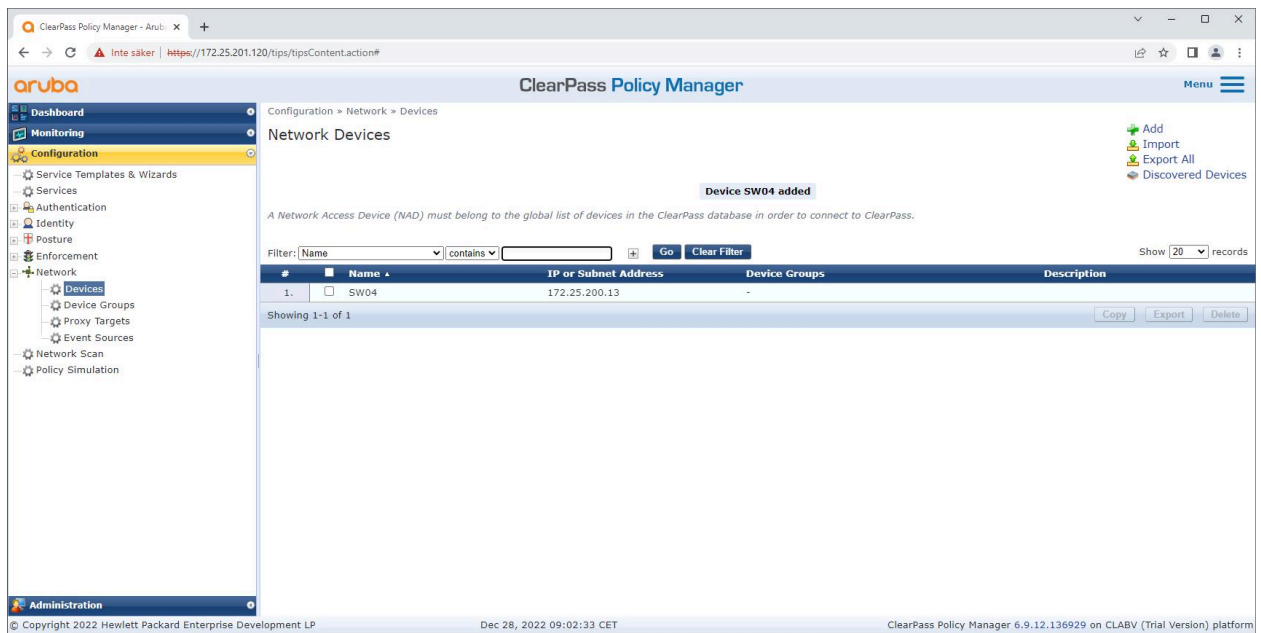
A interface de dispositivos de rede confiáveis no ClearPass Policy Manager.



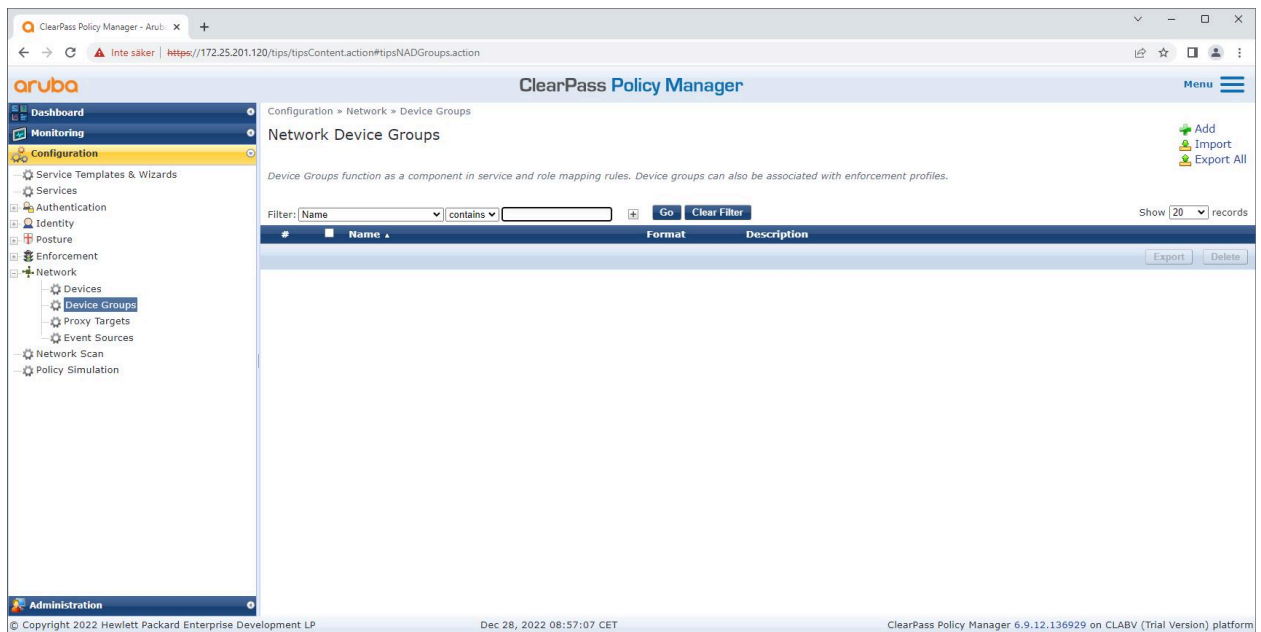
Adicione o switch de acesso do HPE Aruba Networking como dispositivo de rede confiável no ClearPass Policy Manager. Observe que o segredo compartilhado RADIUS precisa corresponder à configuração IEEE 802.1X específica do switch.

HPE Aruba Networking

Integração segura – IEEE 802.1AR/802.1X



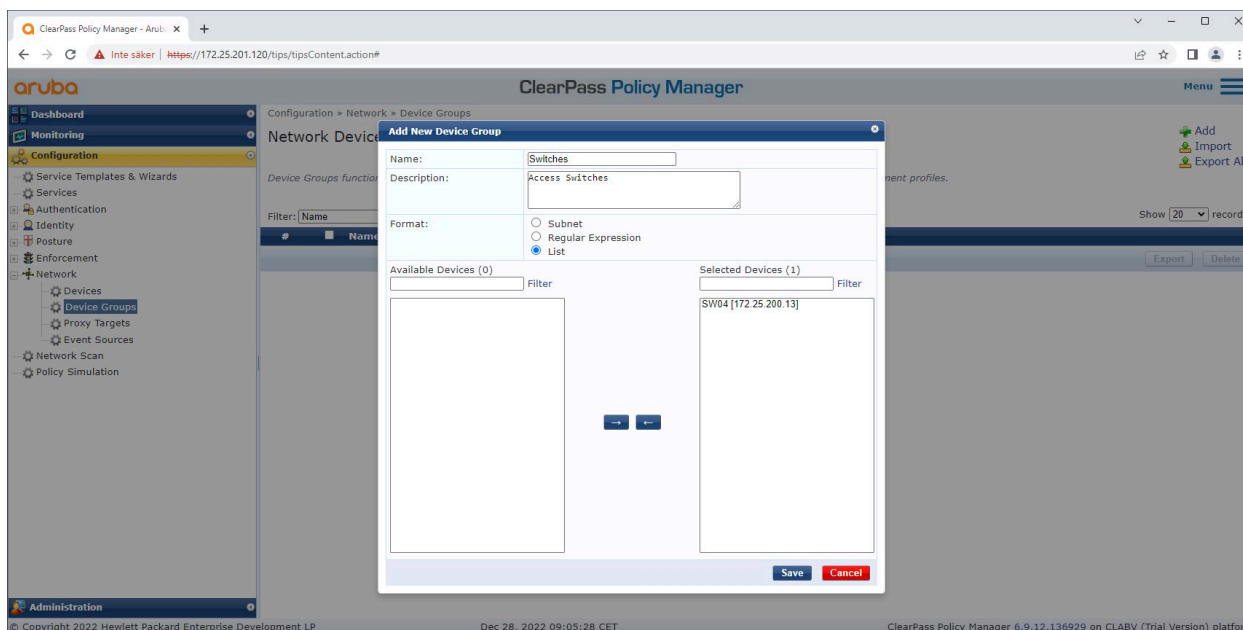
O ClearPass Policy Manager com um dispositivo de rede confiável configurado.



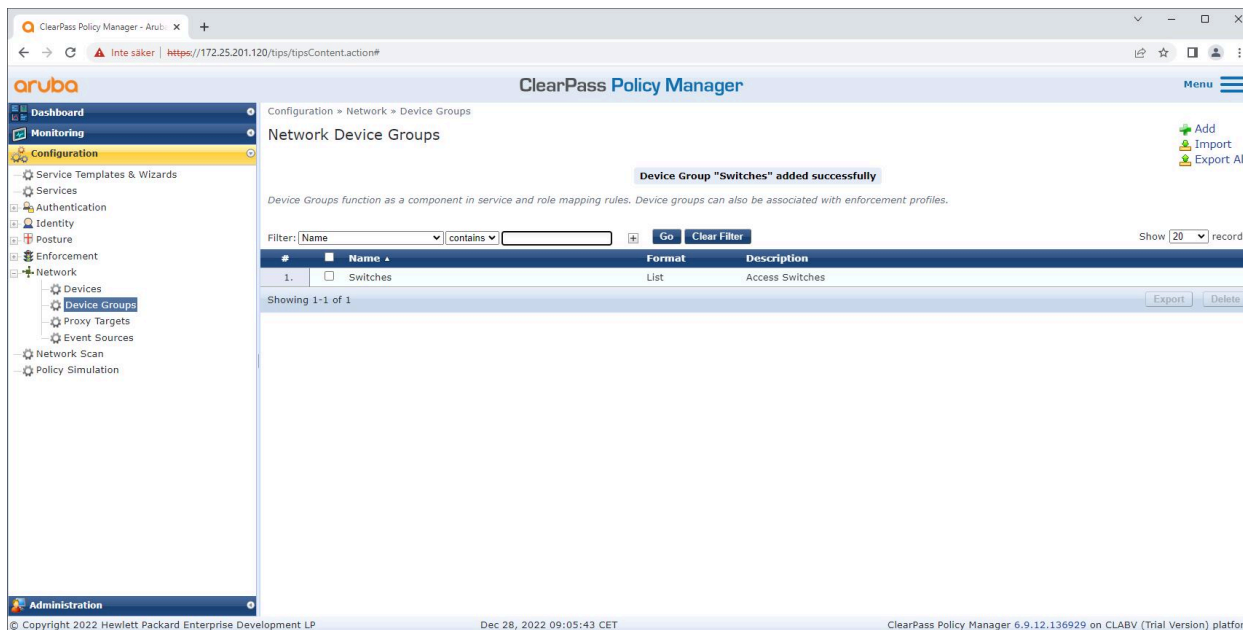
A interface de grupos de dispositivos de rede confiáveis no ClearPass Policy Manager.

HPE Aruba Networking

Integração segura – IEEE 802.1AR/802.1X



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



O 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

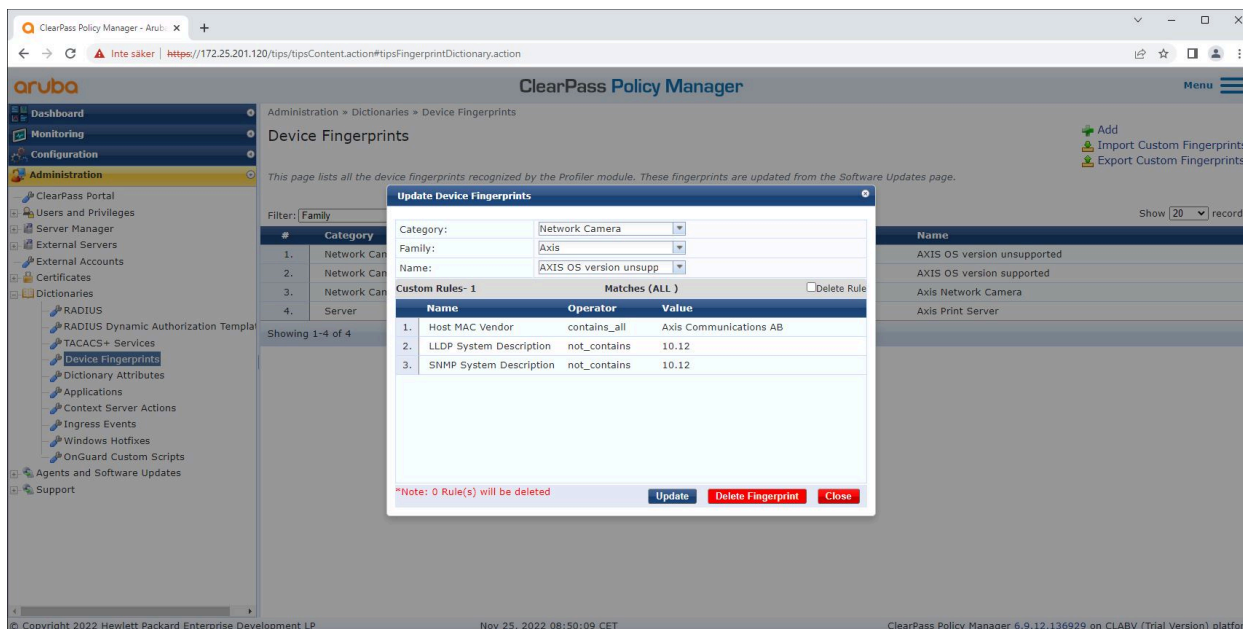
O dispositivo Axis pode distribuir informações específicas do dispositivo, como endereço MAC e versão do software, por meio da descoberta de rede. Use essas informações para criar, atualizar ou gerenciar uma impressão digital do dispositivo no ClearPass Policy Manager. Lá, você também pode conceder ou negar acesso com base na versão do AXIS OS.

1. Vá para Administration > Dictionaries > Device Fingerprints (Administração > Dicionários > Impressões digitais de dispositivos).

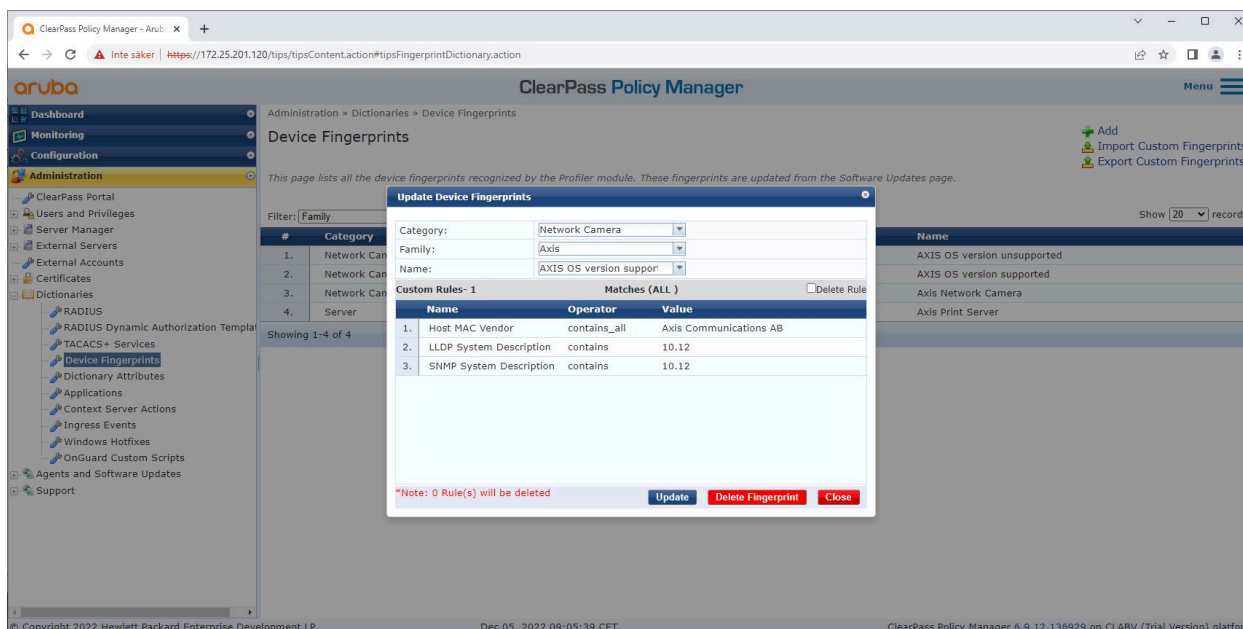
HPE Aruba Networking

Integração segura – IEEE 802.1AR/802.1X

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 ClearPass Policy Manager. Os dispositivos Axis que executam qualquer outra versão do AXIS OS diferente da 10.12 são considerados incompatíveis.



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

As informações sobre a impressão digital do dispositivo coletada pelo ClearPass Manager estão na seção Endpoints.

HPE Aruba Networking

Integração segura – IEEE 802.1AR/802.1X

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

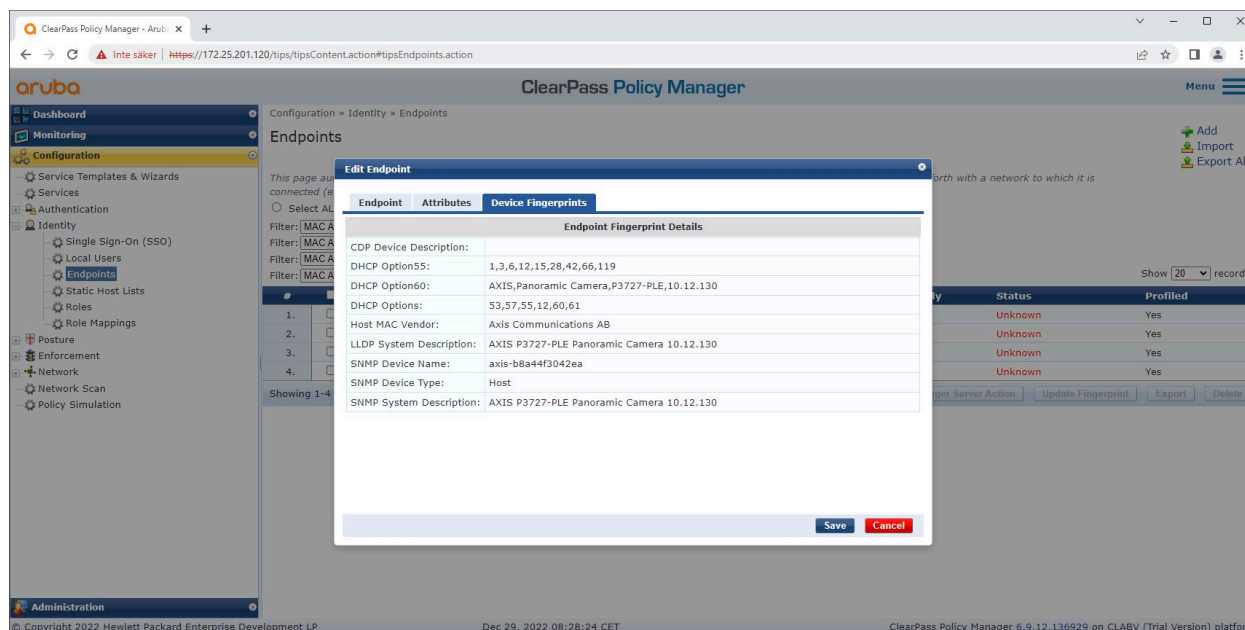
O SNMP é desativado por padrão em dispositivos Axis e coletado do switch de acesso do HPE Aruba Networking.

The screenshot displays the ClearPass Policy Manager interface. The 'Edit Endpoint' dialog box is open, showing the 'Device Fingerprints' tab. The dialog contains the following information:

Field	Value
MAC Address	B8-A4-4F-30-42-EA
IP Address	172.25.201.233
Static IP	FALSE
Hostname	axis-b8a44f3042ea
Device Category	Network Camera
Device OS Family	Axis
Device Name	AXIS OS version support
Added At	Dec 28, 2022 14:50:45 CET
Profiled by	Policy Manager
Last Profiled At	Dec 29, 2022 08:18:23 CET
MAC Vendor	Axis Communications AB
Added by	Policy Manager
Online Status	Not Available
Connection Type	Unknown

The status is set to 'Unknown client'. The background shows the 'Endpoints' list with columns for Status and Profiled.

Um dispositivo Axis com perfil criado pelo ClearPass Policy Manager.

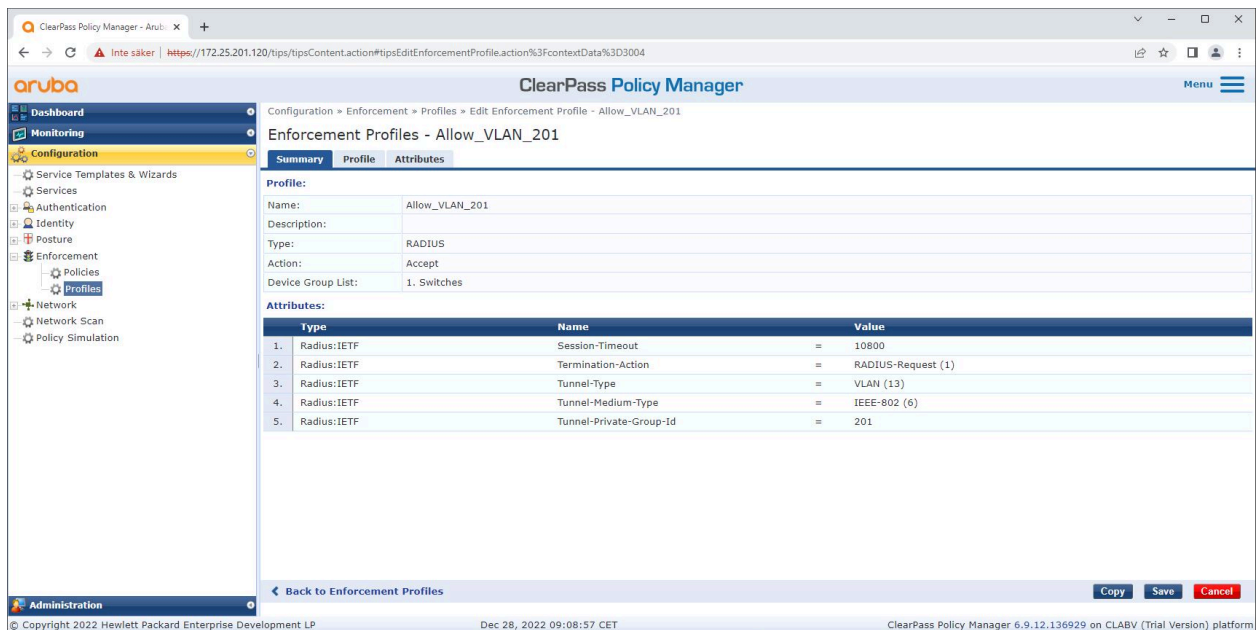


As impressões digitais detalhadas de um dispositivo Axis com perfil estabelecido. Observe que o SNMP está desabilitado por padrão nos dispositivos Axis. As informações de descoberta específicas de LLDP, CDP e DHCP são compartilhadas pelo dispositivo Axis no estado padrão de fábrica e retransmitidas pelo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

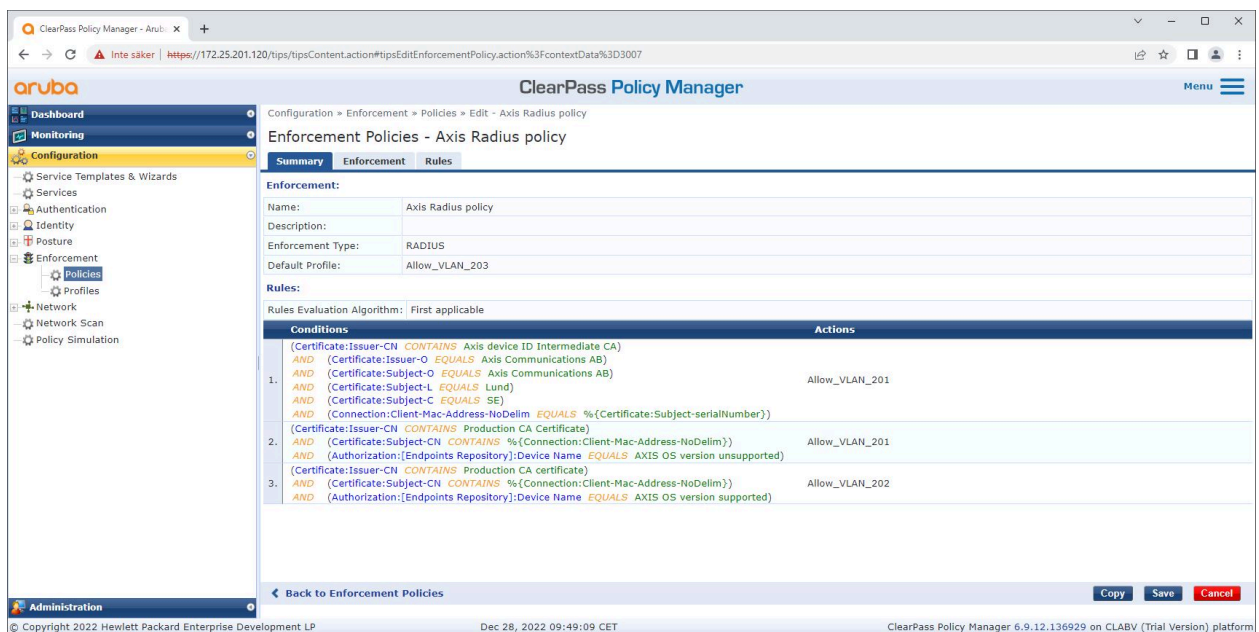
Configuração do perfil de imposição

Enforcement Profile (Perfil de imposição) é usado para permitir que o 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 nos "switches" do grupo de dispositivos. O número necessário de perfis de imposição depende do número de VLANs 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 ClearPass Policy Manager define se os dispositivos Axis recebem acesso às redes que usam HPE Aruba Networking com base em quatro exemplos de perfis de política.



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



A configuração da política de imposição no 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)

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 do AXIS OS, certificados de nível de produção e outras configurações. As seguintes condições são verificadas pelo ClearPass Policy Manager:

- A versão do AXIS OS do dispositivo Axis.
- O endereço MAC do dispositivo faz a correspondência entre o esquema de endereços MAC da Axis específico do fornecedor e 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 e país.

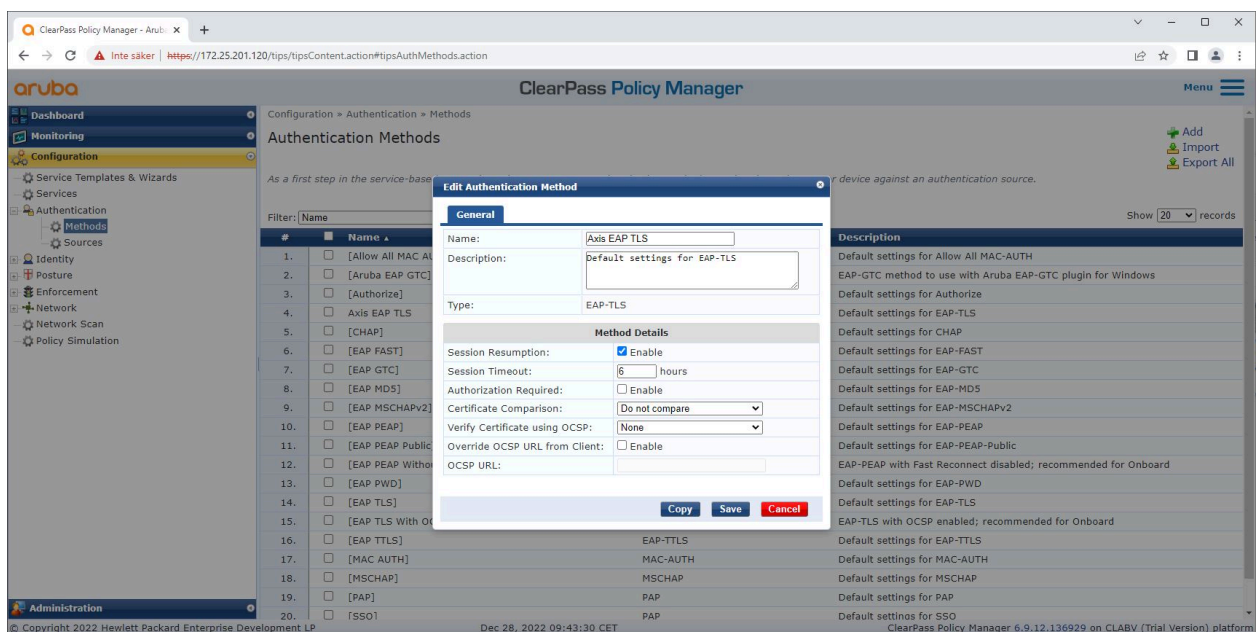
Rede de produção (VLAN 202)

O dispositivo Axis recebe acesso à rede de produção onde deve operar. O acesso é concedido após a conclusão do provisionamento do dispositivo de dentro da rede de provisionamento (VLAN 201). As seguintes condições são verificadas pelo ClearPass Policy Manager:

- O endereço MAC do dispositivo faz a correspondência entre o esquema de endereços MAC da Axis específico do fornecedor e o atributo de número de série do certificado de ID do dispositivo Axis.
- A versão do AXIS OS do dispositivo Axis.
- O certificado de nível de produção pode ser verificado pelo armazenamento de certificados confiável.

Configuração do método de autenticação

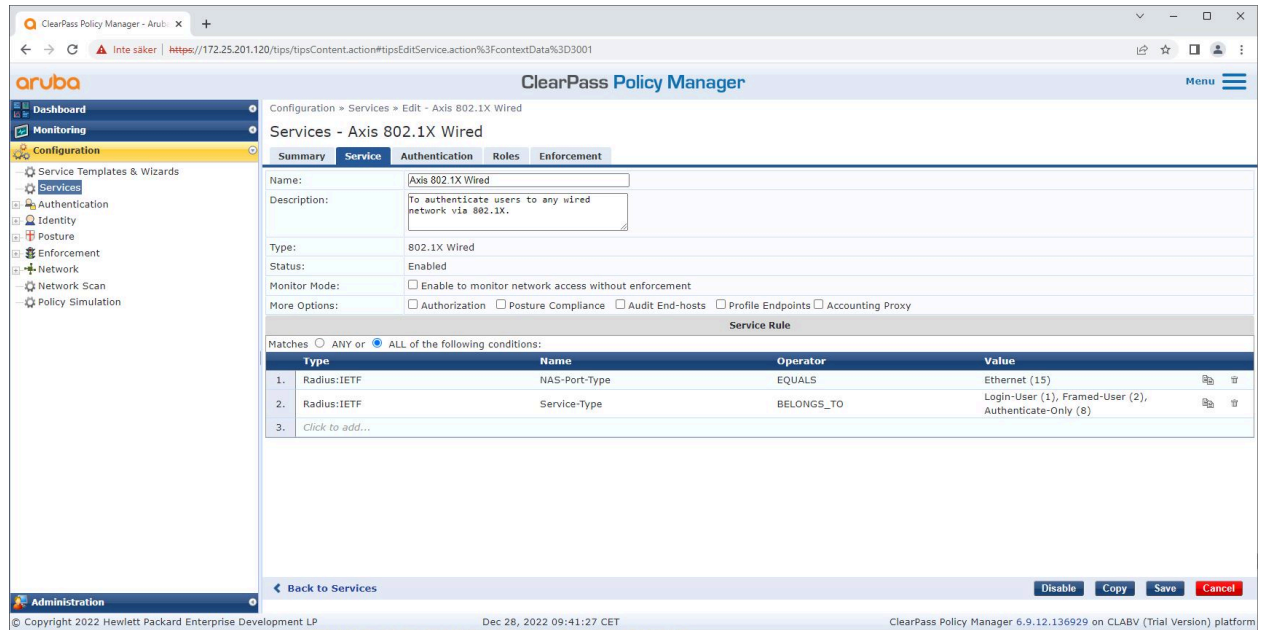
A forma como um dispositivo Axis tenta se autenticar na rede é definida no método de autenticação. O método preferido de autenticação deve ser IEEE 802.1X EAP-TLS, já que os dispositivos Axis com suporte a Axis Edge Vault são fornecidos com IEEE 802.1X EAP-TLS ativado por padrão.



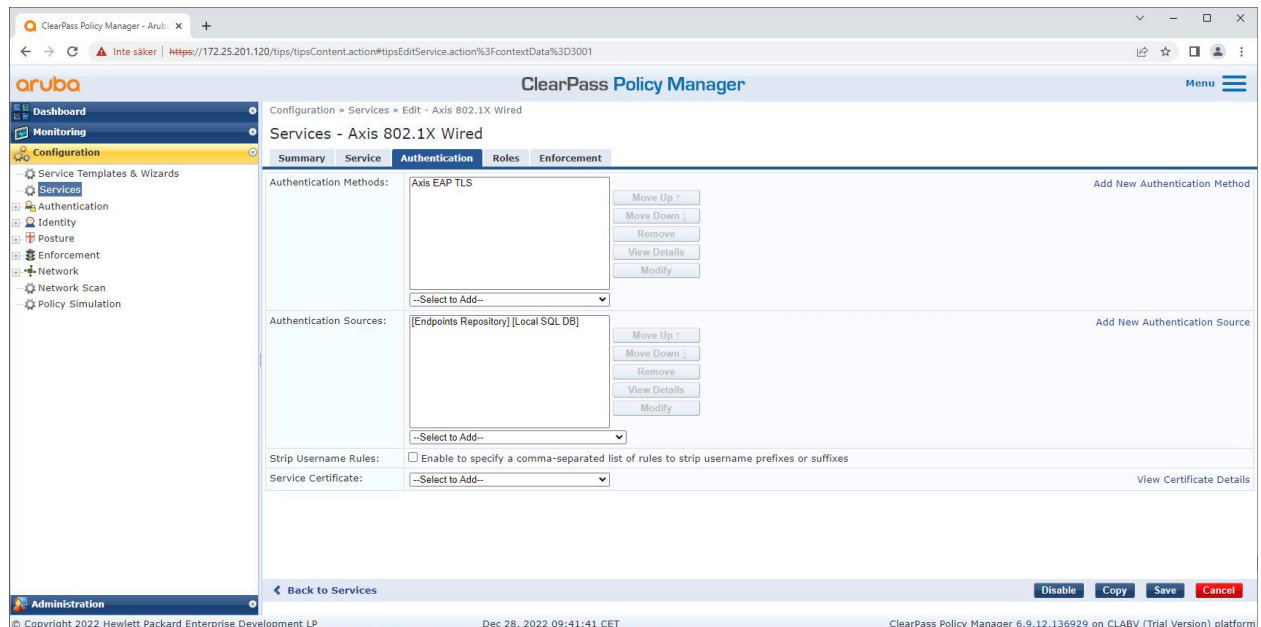
A interface do método de autenticação do ClearPass Policy Manager em que o método de autenticação EAP-TLS para dispositivos Axis é definido.

Configuração do serviço

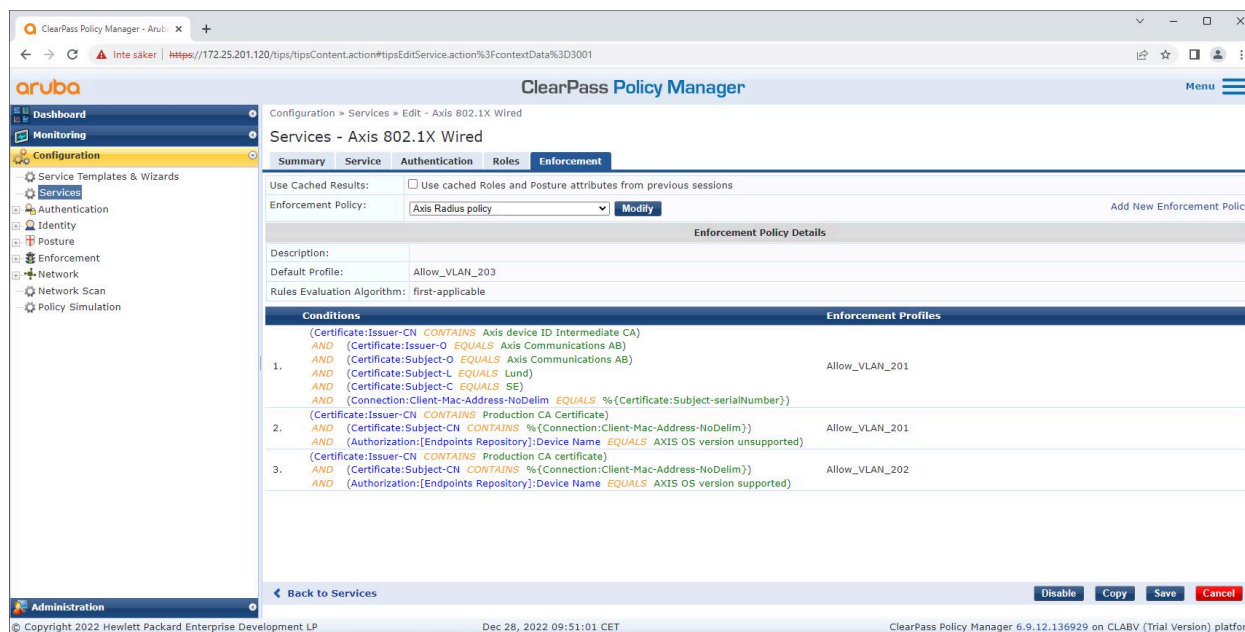
Na página Services (Serviços), as etapas de configuração são combinadas em um único serviço, que lida com a autenticação e a autorização de dispositivos Axis em redes que usam HPE Aruba Networking.



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



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 do HPE Aruba Networking

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

Observação

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

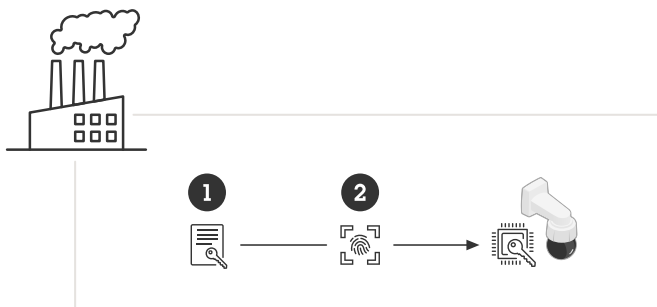
Consulte o exemplo abaixo de configuração global e de porta para switches de acesso do HPE Aruba Networking.

```
radius-server host MyRADIUSIPAddress key "MyRADIUSKey"  
  
aaa authentication port-access eap-radius  
aaa port-access authenticator 18-19  
aaa port-access authenticator 18 reauth-period 300  
aaa port-access authenticator 19 reauth-period 300  
aaa port-access authenticator active
```

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.



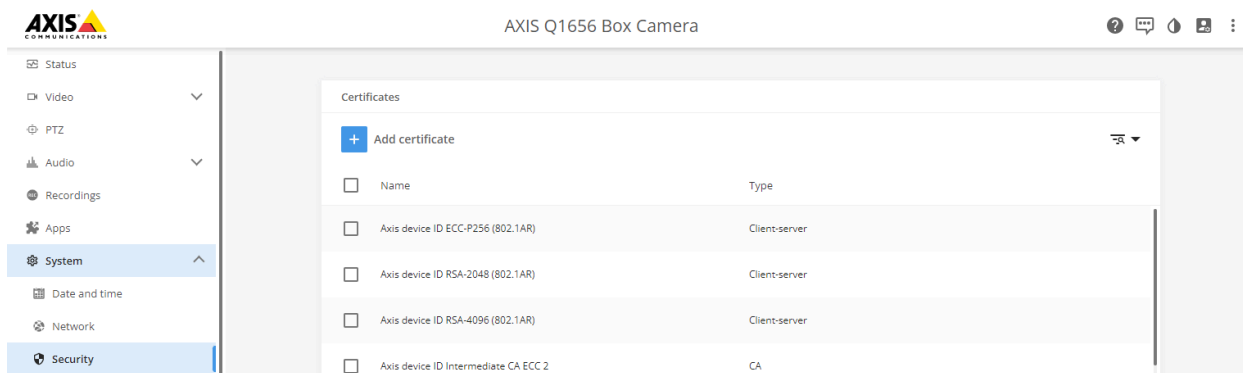
Os dispositivos Axis são fabricados com o certificado de ID de dispositivo Axis compatível com IEEE 802.1AR para serviços de identidade de dispositivos confiáveis

- 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.

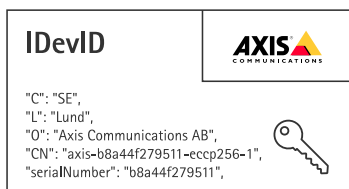
Observação

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



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

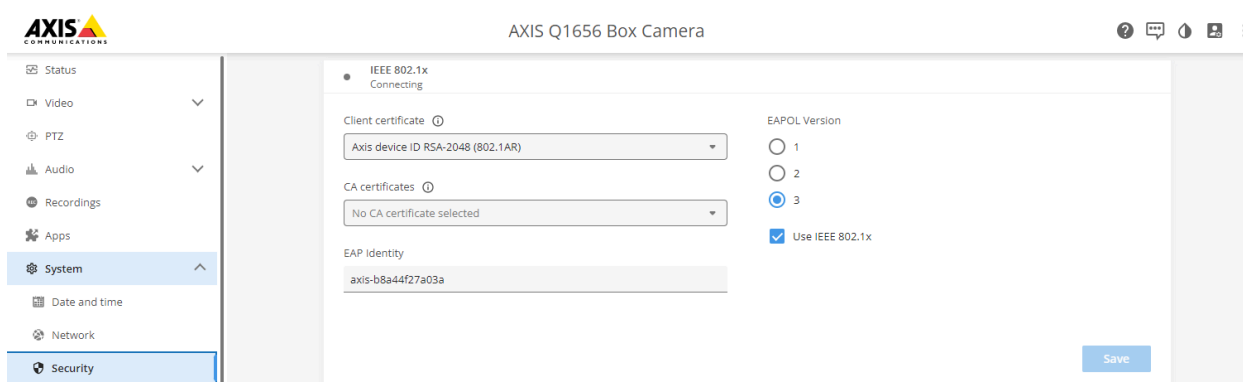
O certificado de ID de dispositivo Axis compatível com IEEE 802.1AR inclui informações sobre o número de série e outras informações específicas do fornecedor Axis. As informações são usadas pelo ClearPass Policy Manager para fins de análise e tomada de decisões de concessão de acesso à rede. Consulte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



Pais	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.



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 das atualizações do AXIS OS.
- 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

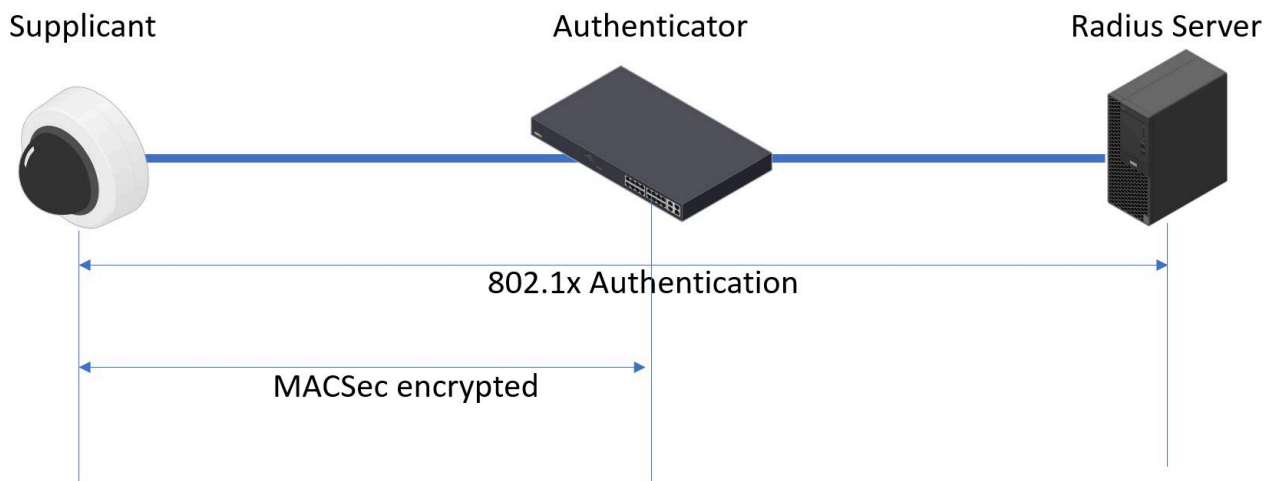


Criptografia de rede de confiança zero com segurança MACsec IEEE 802.1AE camada 2

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 autenticação na rede (4, 5) via controle de acesso à rede baseado em porta EAP-TLS IEEE 802.1X (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 de acesso do HPE Aruba Networking.

HPE Aruba Networking

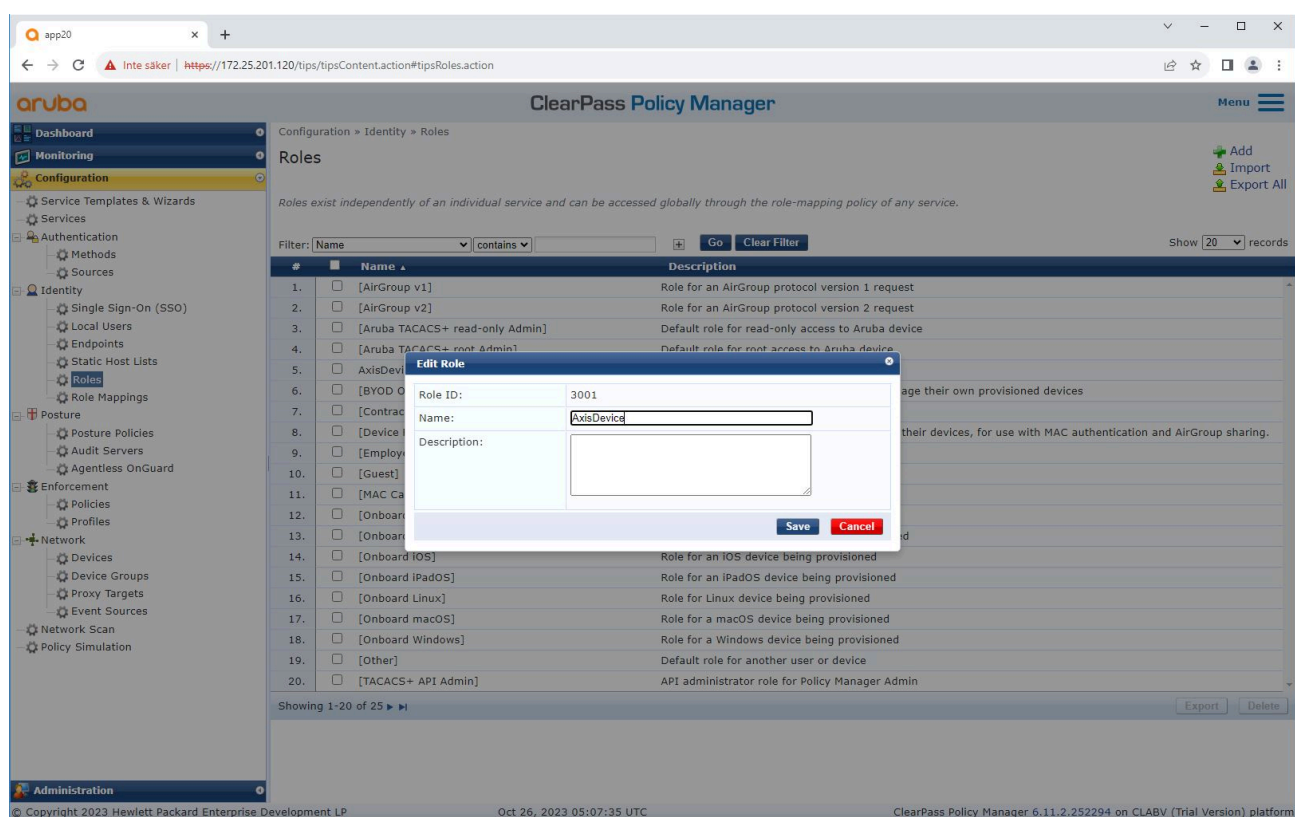
Operação de rede segura – IEEE 802.1AE MACsec

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

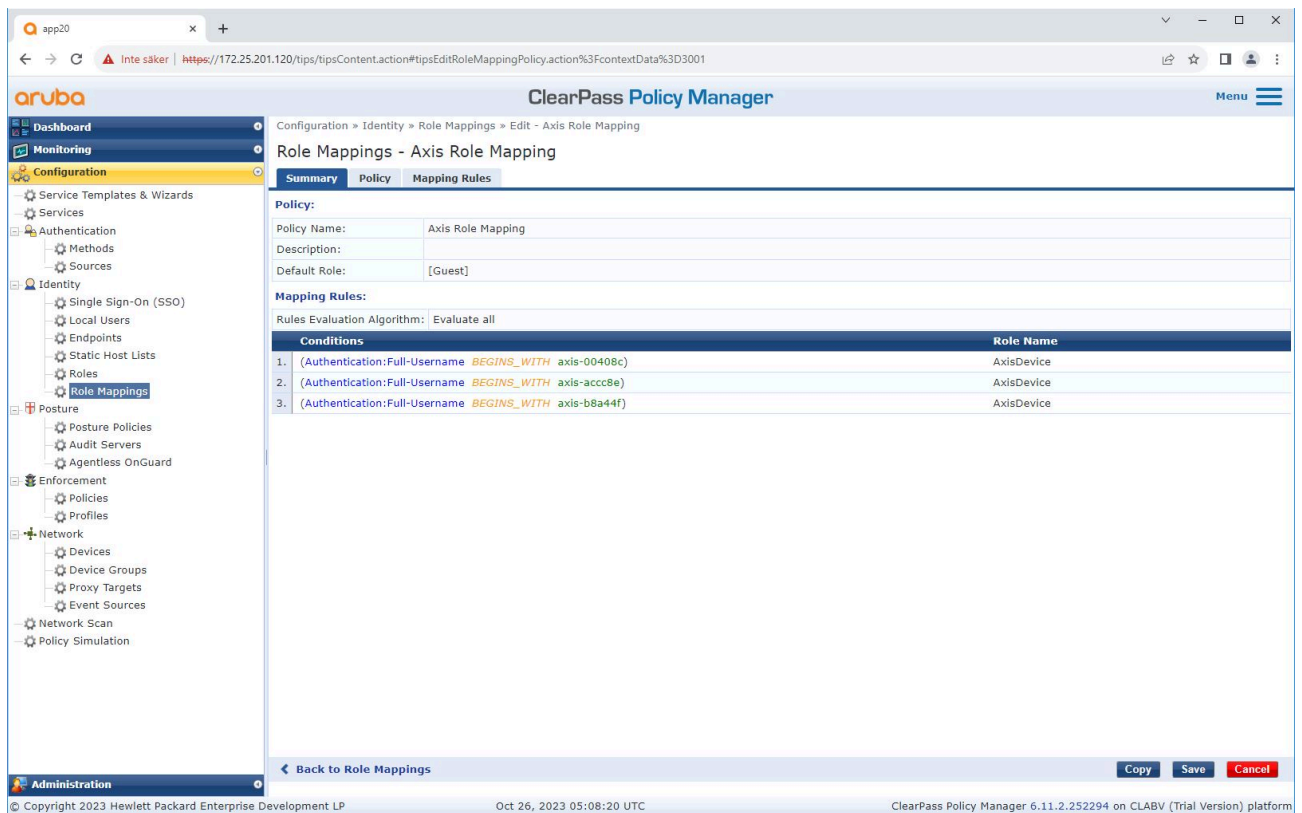
Se o switch de acesso do HPE Aruba Networking não comporta o MACsec usando EAP-TLS, o modo de chave pré-compartilhada poderá ser usado e configurado manualmente.

ClearPass Policy Manager do HPE Aruba Networking

Política de funções e mapeamento de funções



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



The screenshot displays the ClearPass Policy Manager web interface. The left-hand navigation menu is expanded to show the 'Configuration' section, with 'Role Mappings' selected. The main content area is titled 'Role Mappings - Axis Role Mapping' and has three tabs: 'Summary', 'Policy', and 'Mapping Rules'. The 'Mapping Rules' tab is active, showing a table of conditions and role names. The table has two columns: 'Conditions' and 'Role Name'. There are three rows of conditions, each mapping to the role 'AxisDevice'.

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

Adicione 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 torna-se parte da função [Guest] (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

The screenshot displays the ClearPass Policy Manager web interface. The left sidebar shows the navigation menu with 'Configuration' selected. The main content area is titled 'Services - Axis 802.1X Wired' and shows the 'Roles' tab. A 'Role Mapping Policy' dropdown is set to 'Axis Role Mapping'. Below this, the 'Role Mapping Policy Details' section shows the following information:

- 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-acc08a)	AxisDevice
3. (Authentication:Full-Username BEGINS_WITH axis-b8a44f)	AxisDevice

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

Adicione 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.

HPE Aruba Networking

Operação de rede segura – IEEE 802.1AE MACsec

The screenshot shows the ClearPass Policy Manager interface for editing the 'Axis 802.1X Wired' service. The 'Enforcement' tab is selected, showing the following configuration:

- Use Cached Results: Use cached Roles and Posture attributes from previous sessions
- Enforcement Policy: Axis Radius policy (Modify)
- Enforcement Policy Details:
 - Description:
 - Default Profile: Allow_VLAN_203
 - Rules Evaluation Algorithm: evaluate-all
- Conditions and Enforcement Profiles table:

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

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

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

Perfil de imposição

The screenshot shows the ClearPass Policy Manager web interface. The left sidebar contains a navigation menu with categories like Dashboard, Monitoring, Configuration, and Administration. The main content area is titled 'Enforcement Profiles - Allow_VLAN_201' and has tabs for Summary, Profile, and Attributes. The 'Attributes' tab is active, displaying a table of attributes for the profile.

Type	Name	Value
1. RADIUS:IETF	Session-Timeout	= 10800
2. RADIUS:IETF	Termination-Action	= RADIUS-Request (1)
3. RADIUS:IETF	Tunnel-Type	= VLAN (13)
4. RADIUS:IETF	Tunnel-Medium-Type	= IEEE-802 (6)
5. RADIUS:IETF	Tunnel-Private-Group-Id	= 201
6. RADIUS:Aruba	Aruba-User-Role	= AxisDevice

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

Switch de acesso do HPE Aruba Networking

Além da configuração de integração segura descrita em , consulte o exemplo de configuração de porta abaixo do switch de acesso do HPE Aruba Networking para configurar o MACsec IEEE 802.1AE.

```
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

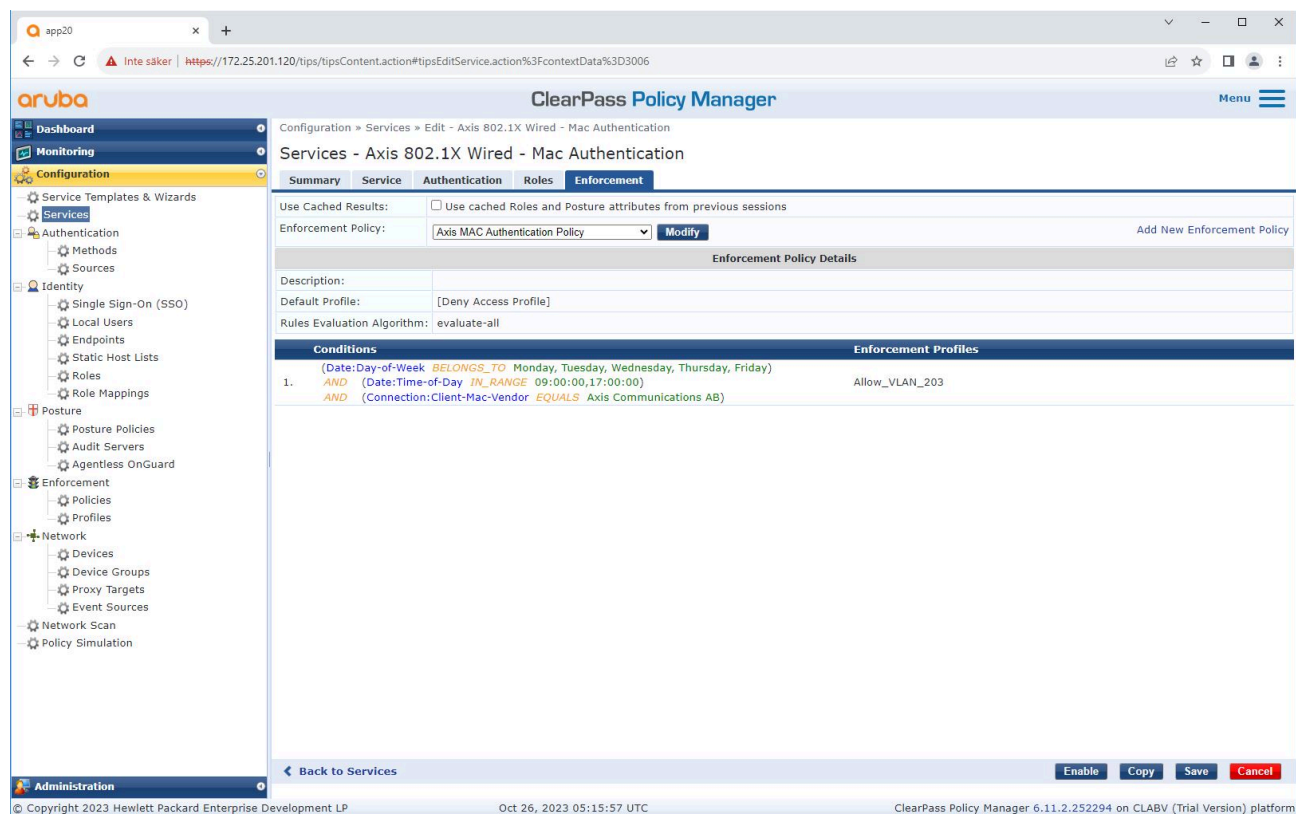
Você pode usar o MAC Authentication Bypass (MAB) para integrar dispositivos Axis que não são compatíveis com a integração do IEEE 802.1AR com o certificado de ID do dispositivo Axis e IEEE 802.1X ativado no estado padrão de fábrica. Se a integração do 802.1X falhar, o ClearPass Policy Manager validará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

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

ClearPass Policy Manager do HPE Aruba Networking

Política de imposição

A configuração da política de imposição no ClearPass Policy Manager define se os dispositivos Axis recebem acesso às redes que usam HPE Aruba Networking 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 um horário entre 9h e 17h

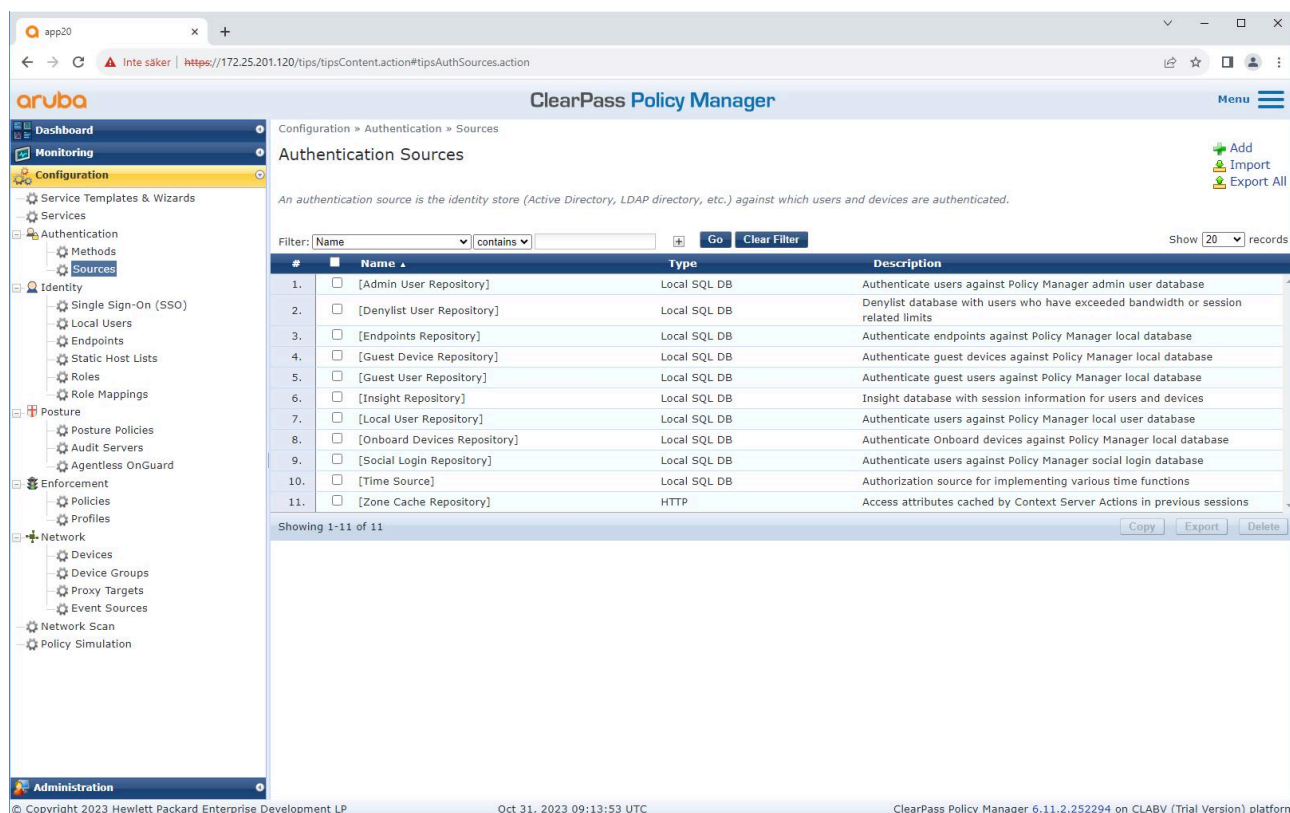
Integração legada – Autenticação MAC

- O fornecedor do endereço MAC corresponde à Axis Communications.

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 página Sources (Fontes), uma nova fonte de autenticação é criada para permitir apenas endereços MAC importados manualmente.



HPE Aruba Networking

Integração legada – Autenticação MAC

The screenshot displays the Aruba ClearPass Policy Manager web interface. The browser address bar shows the URL: `https://172.25.201.120/tips/tipsContent.action#tipsAddAuthSource.action`. The interface is titled "ClearPass Policy Manager" and shows the navigation menu on the left with "Configuration" selected. The main content area is titled "Authentication Sources" and has tabs for "General", "Static Host Lists", and "Summary". The "General" tab is active, showing the configuration for an authentication source named "Axis Devices".

Configuration Details:

- 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 with "Remove" and "View Details" buttons)

At the bottom of the configuration area, there are buttons for "Next ->", "Save", and "Cancel". The footer of the interface includes the copyright notice: "© Copyright 2023 Hewlett Packard Enterprise Development LP", the date and time: "Oct 31, 2023 09:21:23 UTC", and the version information: "ClearPass Policy Manager 6.11.2.252294 on CLABV (Trial Version) platform".

HPE Aruba Networking

Integração legada – Autenticação MAC

The screenshot displays the Aruba ClearPass Policy Manager web interface. The main navigation menu on the left includes Dashboard, Monitoring, Configuration, Services, Authentication, Identity, Posture, Enforcement, Network, and Administration. The current view is 'Authentication Sources' under 'Configuration', with tabs for 'General', 'Static Host Lists', and 'Summary'. A modal window titled 'Add Static Host List' is open, showing the following configuration:

- Name: Axis devices
- Description: (empty text area)
- Host Format: Subnet, Regular Expression, List
- Host Type: IP Address, MAC Address
- Host Entries table:

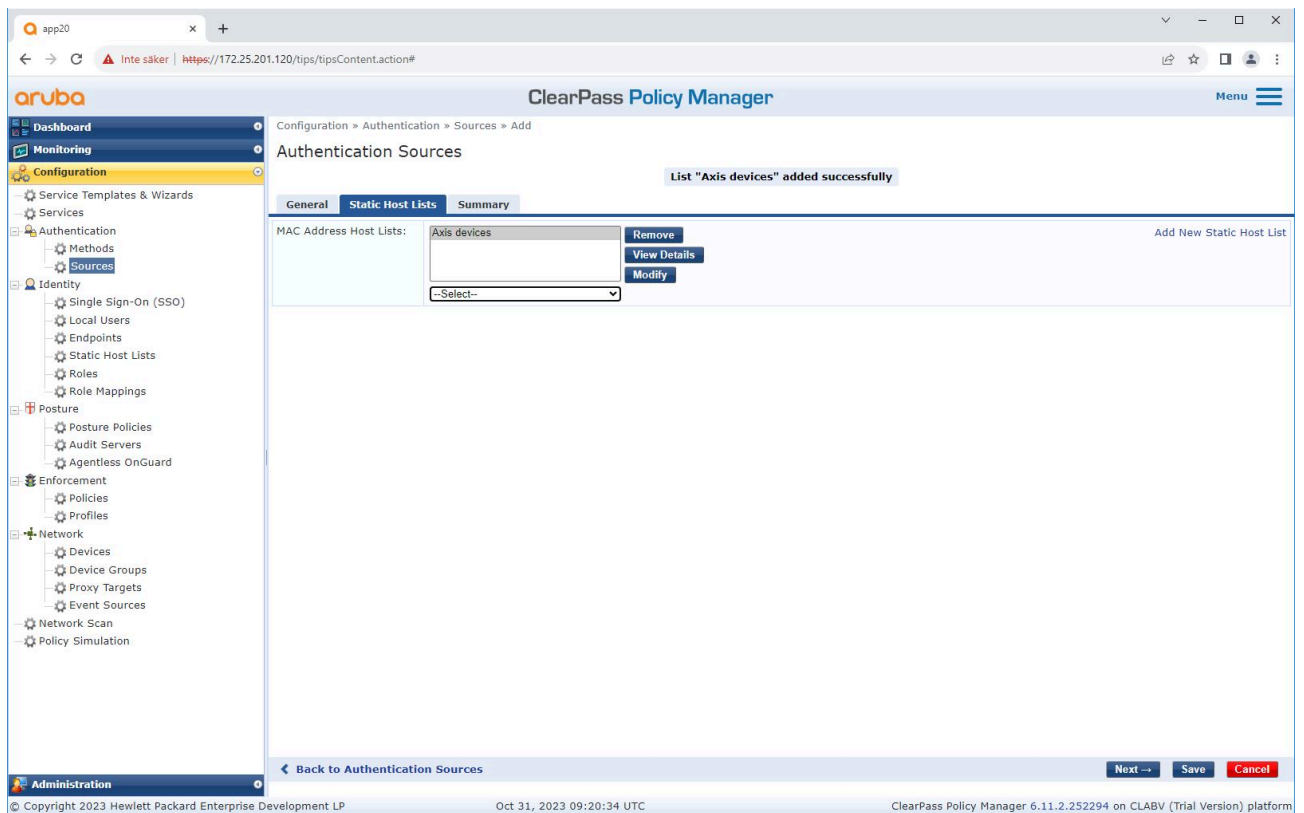
#	Address	Description
1.	<input type="radio"/> B8-A4-4F-45-B4-E6	Axis Device 1
2.	<input type="radio"/> B8-A4-4F-45-B4-E7	Axis Device 2
3.	<input type="radio"/> B8-A4-4F-45-B4-E8	Axis Device 3
- Additional fields: Address (text input), Description (text area)
- Buttons: Save Host, Save, Cancel

At the bottom of the modal, there are 'Save' and 'Cancel' buttons. Below the modal, there are navigation buttons: 'Back to Authentication Sources', 'Next ->', 'Save', and 'Cancel'. The footer of the interface shows copyright information for Hewlett Packard Enterprise Development LP, the date 'Oct 31, 2023 09:20:18 UTC', and the version 'ClearPass Policy Manager 6.11.2.252294 on CLABV (Trial Version) platform'.

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

HPE Aruba Networking

Integração legada – Autenticação MAC



Configuração do serviço

Na página Services (Serviços), as etapas de configuração são combinadas em um único serviço, que lida com a autenticação e a autorização de dispositivos Axis em redes que usam HPE Aruba Networking.

HPE Aruba Networking

Integração legada – Autenticação MAC

Configuration » Services

Services

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

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

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

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

The screenshot displays the Aruba ClearPass Policy Manager web interface. The left sidebar shows a navigation menu with categories like 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 'Service' tab is active, showing the following configuration details:

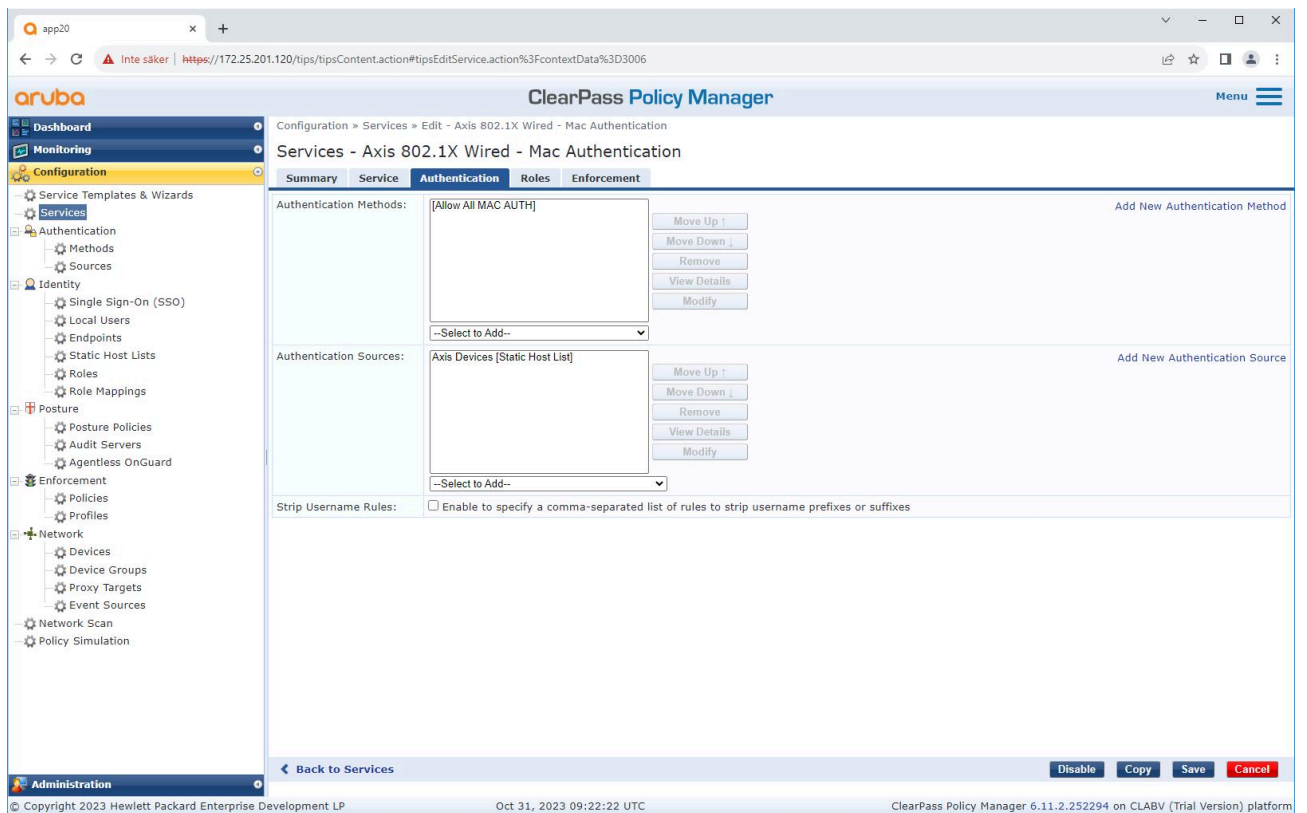
- Name:** Axis 802.1X Wired - Mac Authentication
- Description:** To authenticate guest devices based on their MAC address.
- Type:** MAC Authentication
- Status:** Disabled
- Monitor Mode:** Enable to monitor network access without enforcement
- More Options:** Authorization Audit End-hosts Profile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

Below these fields is a 'Service Rule' section with a table of conditions:

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

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

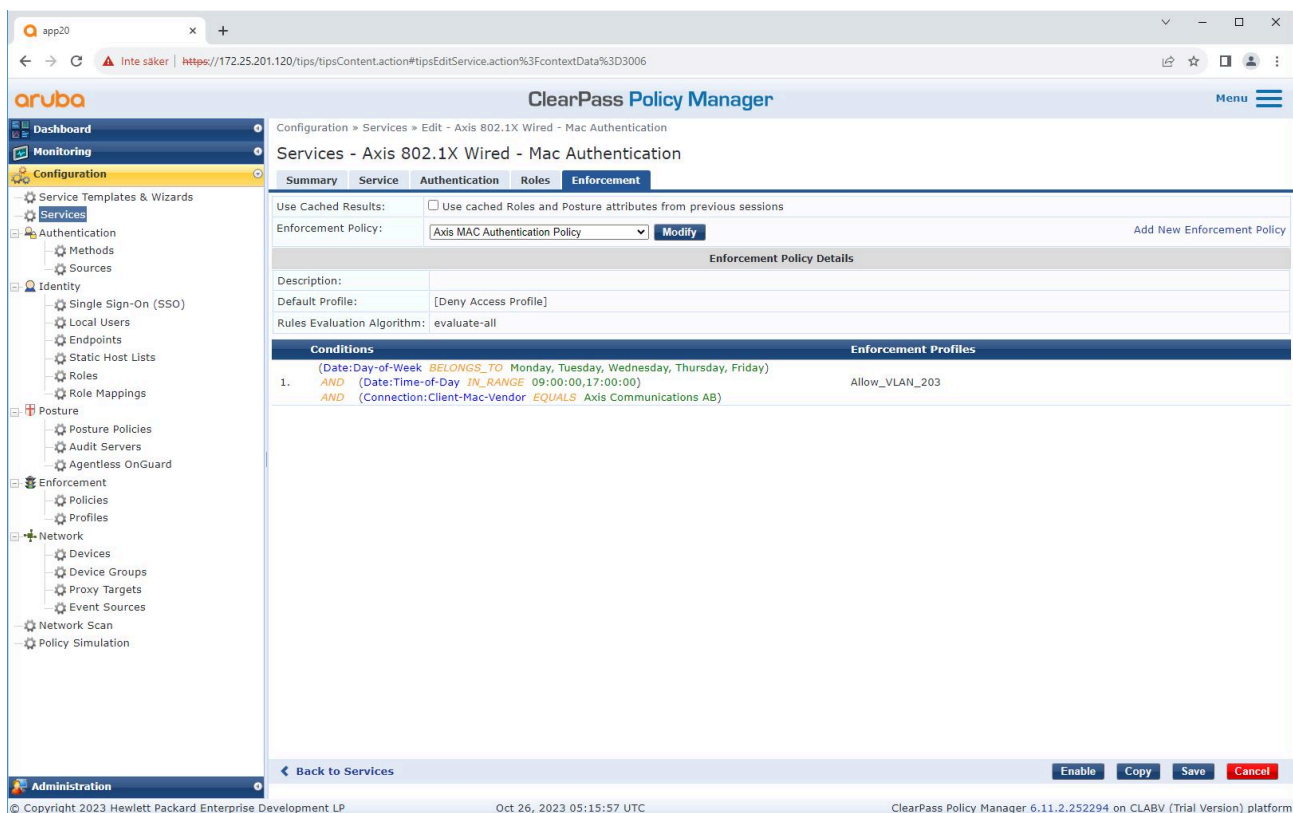
Um serviço Axis dedicado que o MAB como método de conexão é criado.



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 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



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

Switch de acesso do HPE Aruba Networking

Além da configuração de integração segura descrita em , consulte o exemplo de configuração de porta abaixo para o switch de acesso do HPE Aruba Networking 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
```

