HPE Aruba Networking

Manual do Usuário

Índice

Introdução 3
Integração segura – IEEE 802.1AR/802.1X 4
Autenticação inicial 4
Provisionamento 4
Rede de produção 5
Configuração do HPE Aruba Networking 6
ClearPass Policy Manager do HPE Aruba Networking 6
Switch de acesso do HPE Aruba Networking 15
Configuração Axis 16
Dispositivo de rede Axis 16
AXIS Device Manager 17
Operação de rede segura – IEEE 802.1AE MACsec 18
ClearPass Policy Manager do HPE Aruba Networking 19
Política de funções e mapeamento de funções 19
Configuração do serviço 20
Perfil de imposição 21
Switch de acesso do HPE Aruba Networking 22
Gerenciamento de certificados – Enrollment over Secure Transport (EST) 23
Principais benefícios do EST 23
Configuração do HPE Aruba ClearPass Onboard 23
Configuração do HPE Aruba ClearPass Policy Manager 25
Configuração Axis 28
Integração legada – Autenticação MAC 33
ClearPass Policy Manager do HPE Aruba Networking 33
Política de imposição 33
Configuração da origem 34
Configuração do serviço 35
Switch de acesso do HPE Aruba Networking 38

Introdução

Este guia de integração descreve as melhores práticas de configuração ao incorporar e operar dispositivos Axis em redes 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 poupar tempo e dinheiro. Isso remove a complexidade desnecessária do sistema ao usar aplicativos de gerenciamento de dispositivos Axis em conjunto com os aplicativos e a infraestrutura HPE Aruba Networking. Ao combinar dispositivos e software Axis com uma infraestrutura HPE Aruba Networking, você pode se beneficiar das seguintes maneiras:

- Remover as redes de preparação de dispositivos minimiza a complexidade do sistema.
- A adição de processos automatizados de integração e gerenciamento de dispositivos contribui para a redução de custos.
- Os dispositivos Axis oferecem controles de segurança em rede sem intervenção humana.
- Maior segurança em rede por meio da competência da Axis e da HPE.

Para uma transição suave definida por software entre redes lógicas durante todo o processo de integração, a infraestrutura de rede deve estar preparada para verificar com segurança a integridade dos dispositivos Axis antes de iniciar a configuração. É necessário o seguinte antes de realizar a configuração:

- Experiência no gerenciamento de infraestruturas de TI em rede corporativa da HPE Aruba Networking, incluindo switches de acesso HPE Aruba Networking e o HPE Aruba Networking ClearPass Policy Manager.
- Conhecimento em técnicas modernas de controle de acesso à rede e políticas de segurança de rede.
- Conhecimento prévio básico dos produtos Axis é desejável, mas também 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.

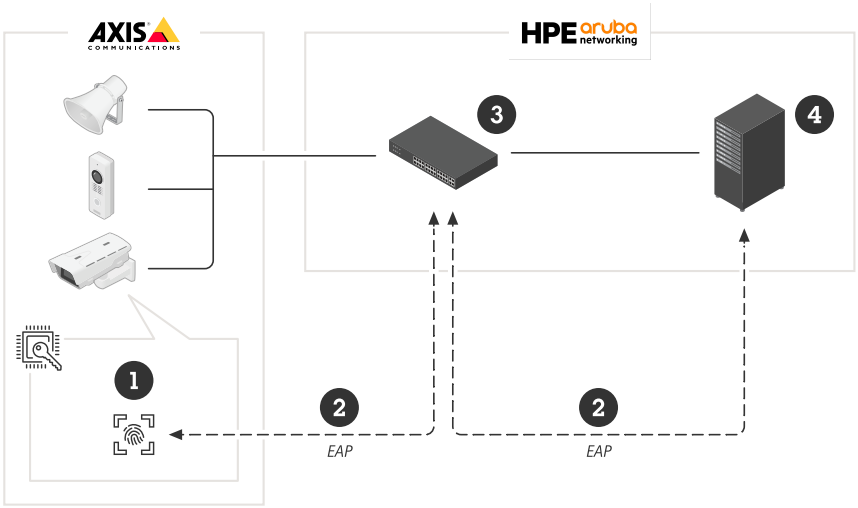
Integração segura de dispositivo em redes de confiança zero com IEEE 802.1X/802.1AR

Autenticação inicial

Quando o dispositivo Axis compatível com o Axis Edge Vault é conectado à rede, ele utiliza 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 a ID do dispositivo Axis em conjunto com outras impressões digitais específicas do dispositivo. Essas informações, como o endereço MAC e a versão do AXIS OS do dispositivo, são utilizadas para tomar uma decisão baseada nas políticas.

O dispositivo Axis se autentica na rede usando o certificado de ID do dispositivo Axis compatível com IEEE 802.1AR.

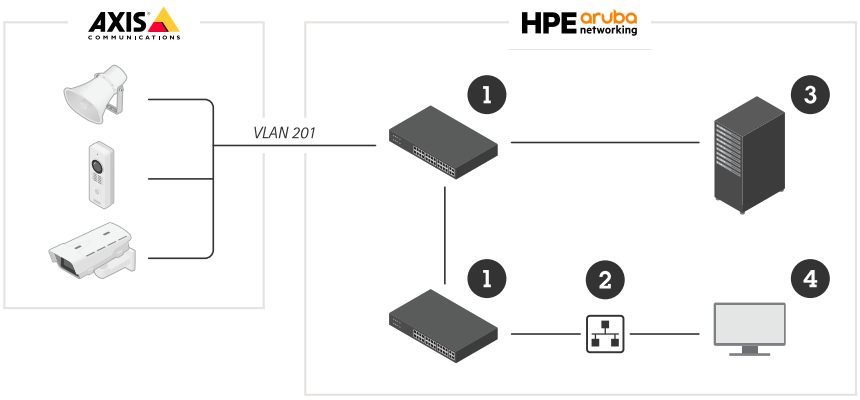


O dispositivo Axis é autenticado na rede HPE Aruba Networking usando o certificado de ID do dispositivo Axis compatível com IEEE 802.1AR.

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). Esta rede contém o AXIS Device Manager, que realiza a configuração do dispositivo, o reforço da segurança e as 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.

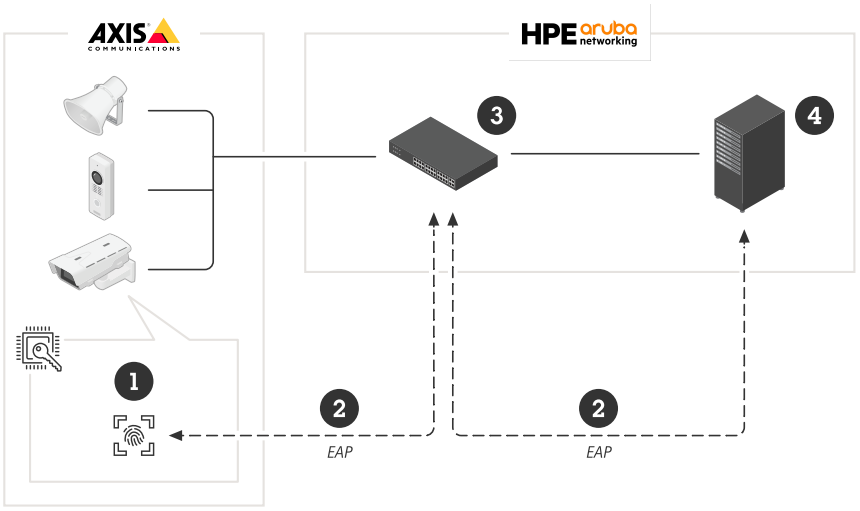


Após a autenticação bem-sucedida, o dispositivo Axis passa para uma rede de provisionamento para configuração.

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

Rede de produção

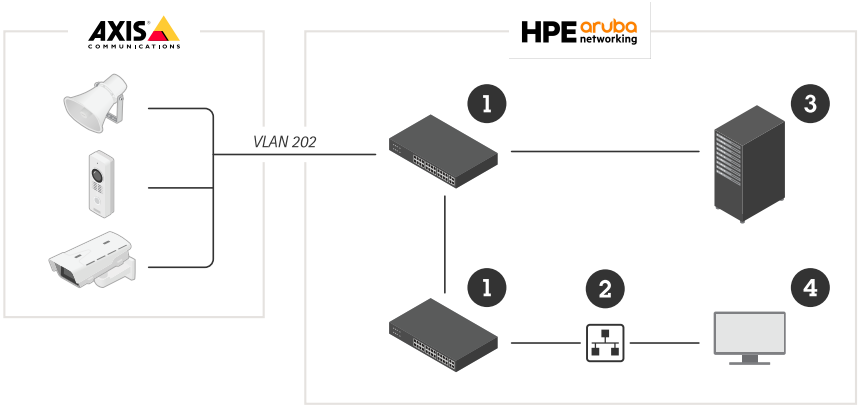
O provisionamento do dispositivo Axis com novos certificados IEEE 802.1X aciona uma nova tentativa de autenticação. O ClearPass Policy Manager verifica os novos certificados e decide se o dispositivo Axis será ou não movido para a rede de produção.



Após a configuração, 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), onde o Sistema de Gerenciamento de Vídeo (VMS) se conecta ao dispositivo e inicia a operação.



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*

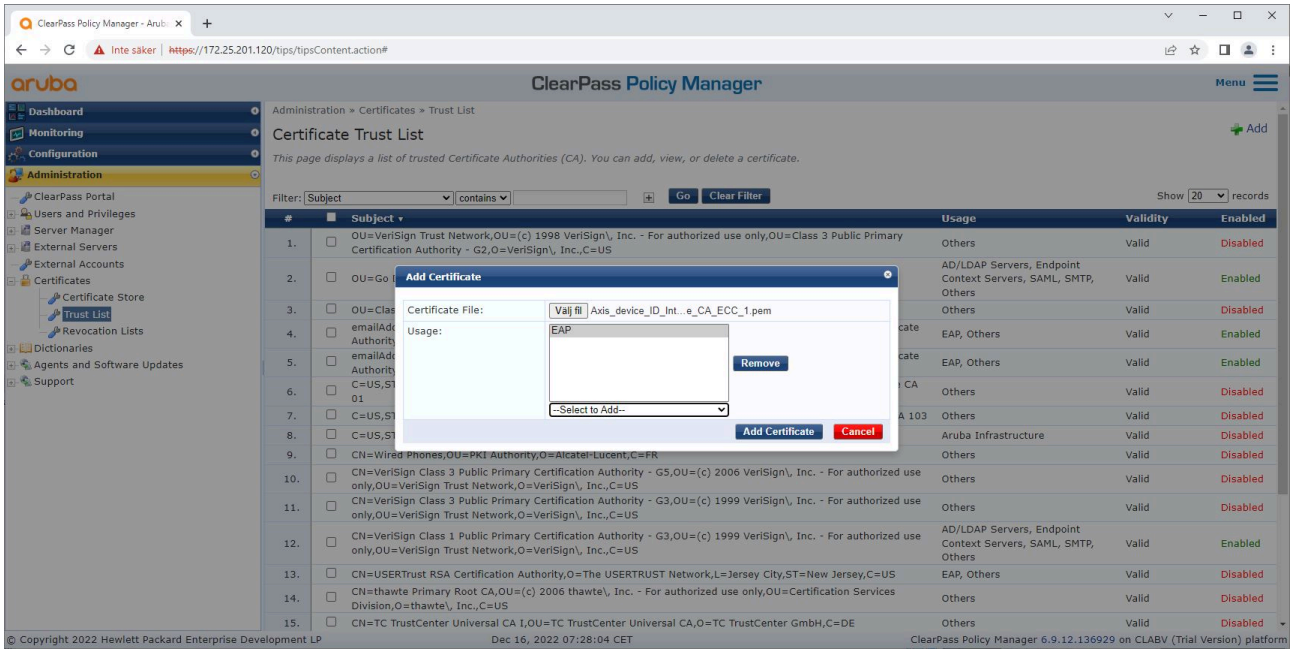
Configuração do HPE Aruba Networking

ClearPass Policy Manager do HPE Aruba Networking

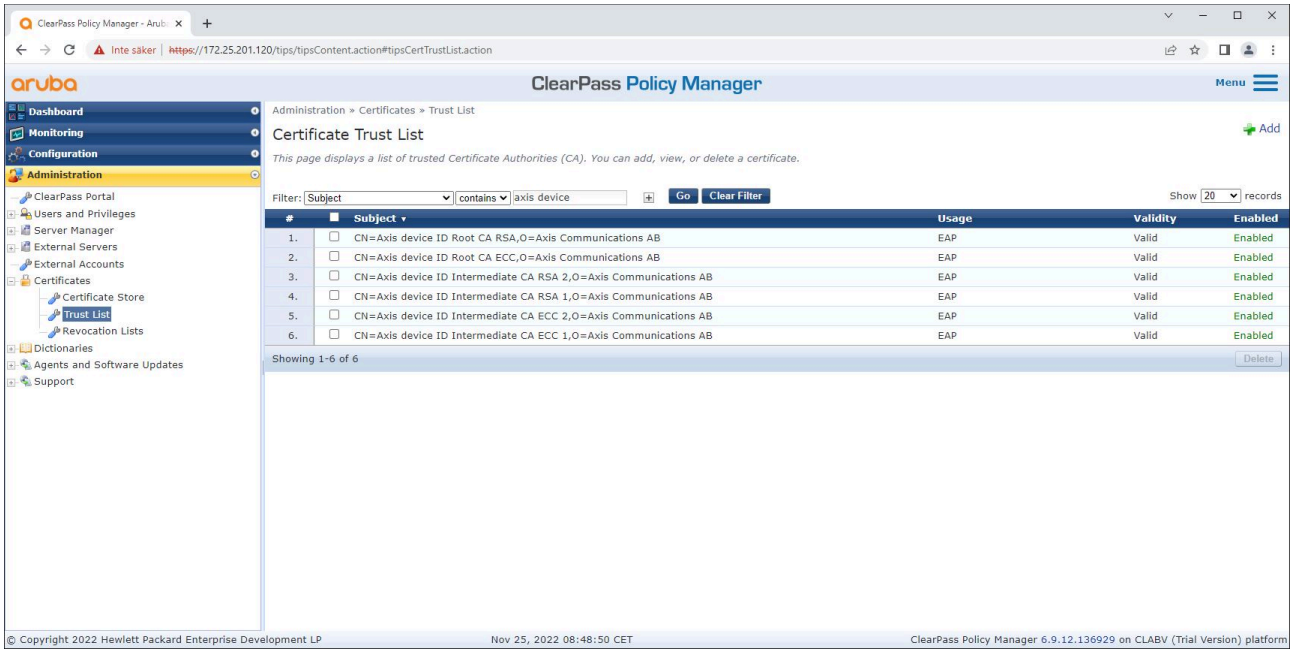
O ClearPass Policy Manager fornece controle de acesso à rede seguro baseado em função e dispositivo para IoT, BYOD, dispositivos corporativos, funcionários, prestadores de serviços e convidados na infraestrutura de rede com fio, sem fio e VPN de vários fornecedores.

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 de 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.



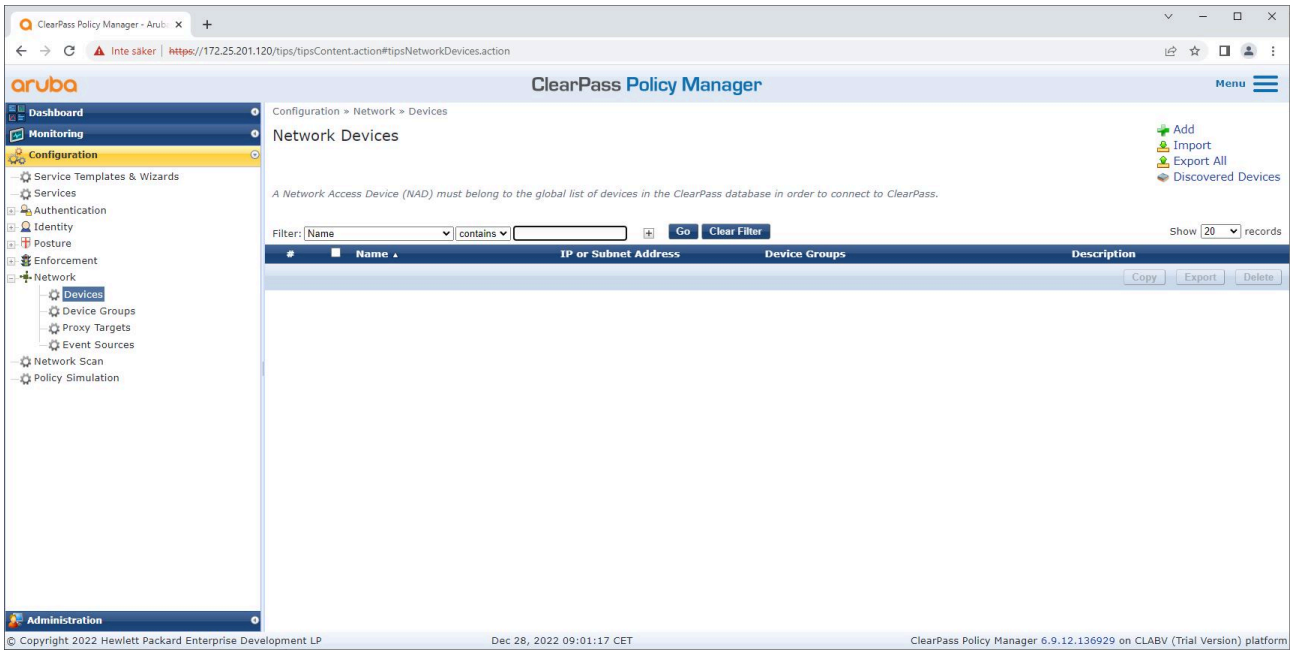
Carregue os certificados IEEE 802.1AR específicos da Axis para o armazenamento de certificados confiável do ClearPass Policy Manager.



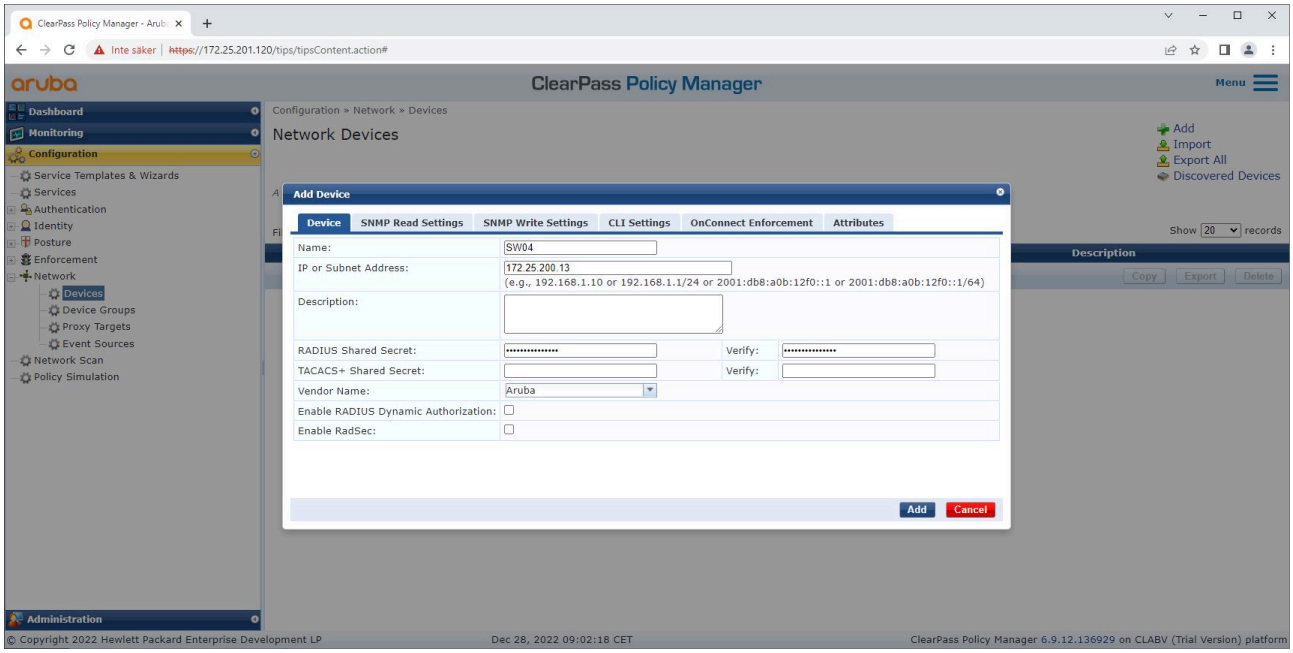
O armazenamento de certificados confiável no ClearPass Policy Manager com cadeia de certificados IEEE 802.1AR específica da Axis incluída.

Configuração de dispositivo/grupo de rede

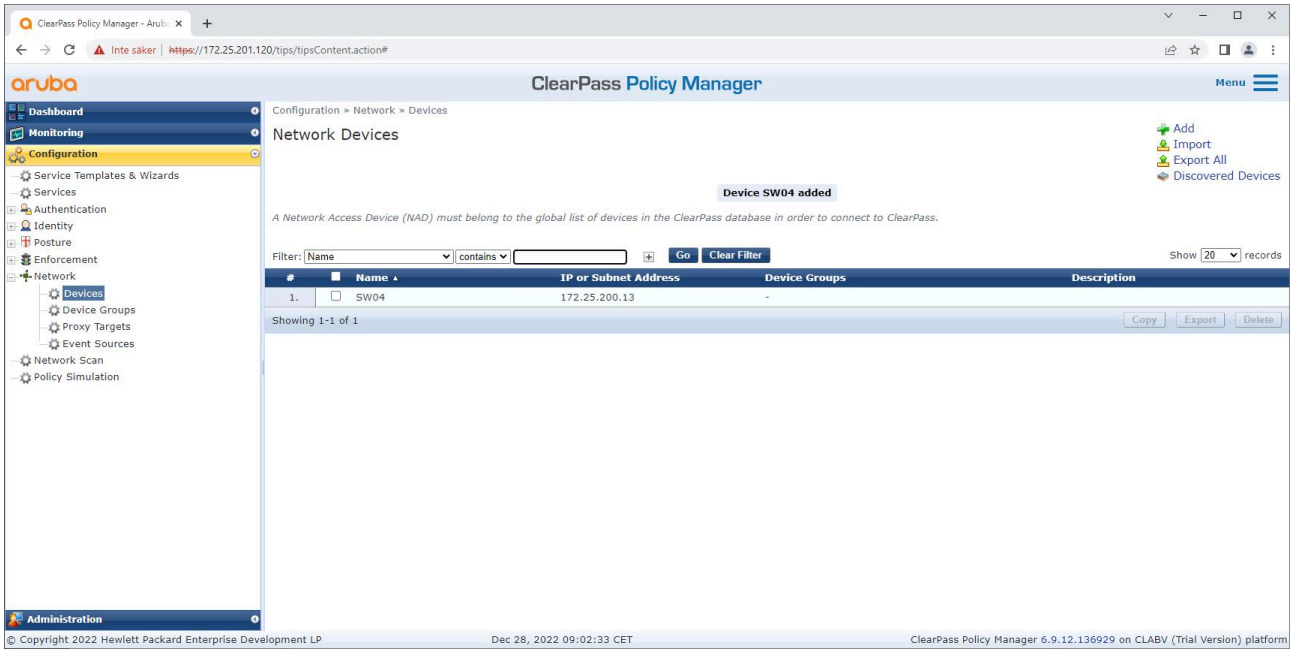
1. Adicione dispositivos de acesso à rede confiáveis como switches de acesso do HPE Aruba Networking ao ClearPass Policy Manager. O ClearPass Policy Manager precisa saber quais switches de acesso na rede são usados para comunicação IEEE 802.1X. Observe também que o segredo compartilhado RADIUS precisa corresponder à configuração IEEE 802.1X específica do switch.
2. Use a configuração de grupo de dispositivos de rede para agrupar vários dispositivos de acesso à rede confiáveis. Agrupar dispositivos facilita a configuração de políticas.



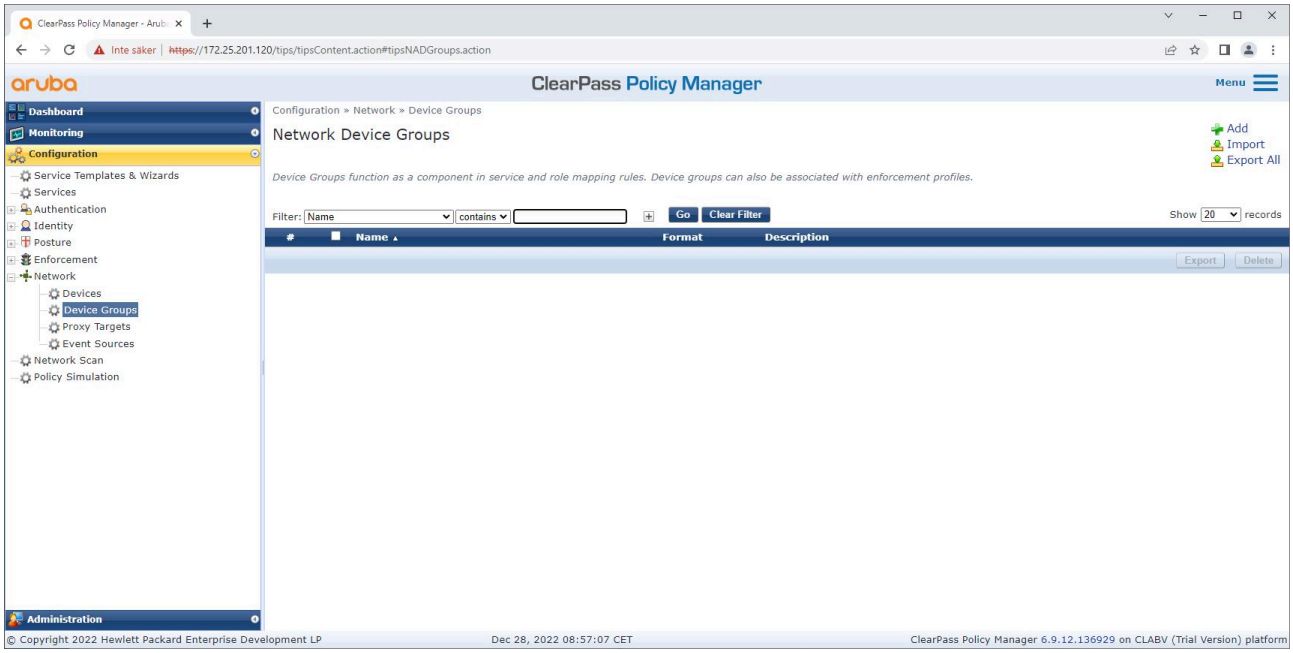
A interface de dispositivos de rede confiáveis no ClearPass Policy Manager.



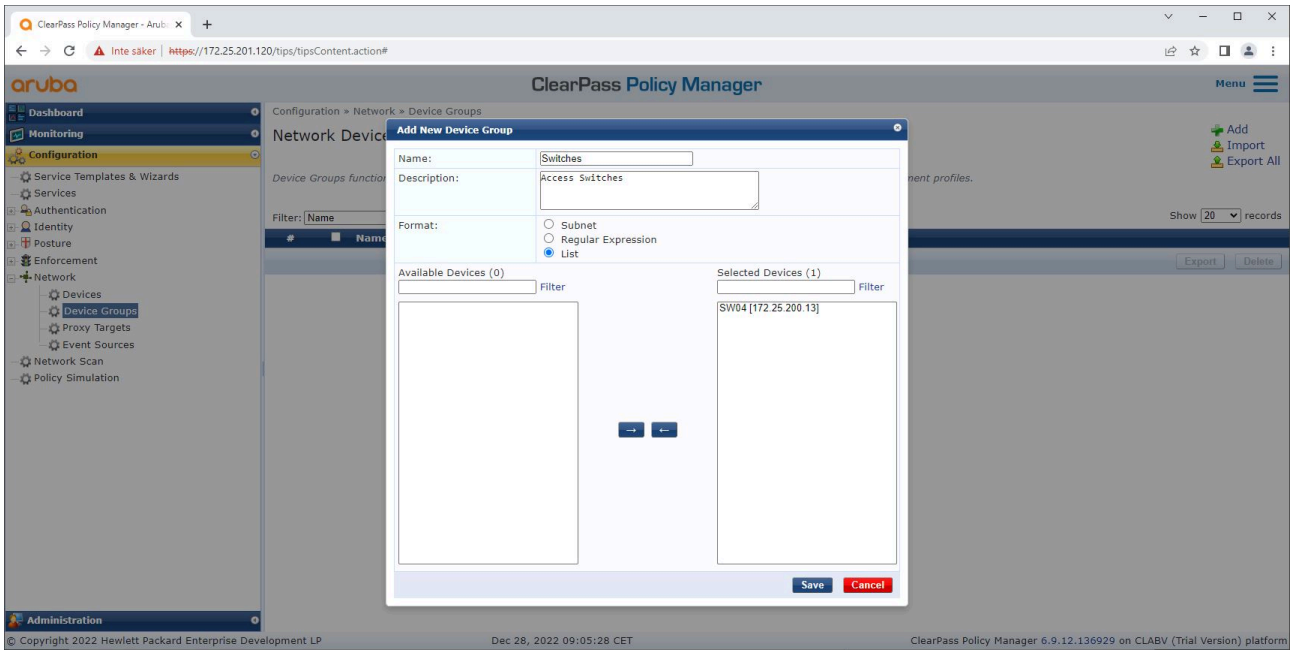
Adicione o switch de acesso HPE Aruba Networking como um dispositivo confiável no ClearPass Policy Manager. Observe que o segredo compartilhado RADIUS precisa corresponder à configuração IEEE 802.1X específica do switch.



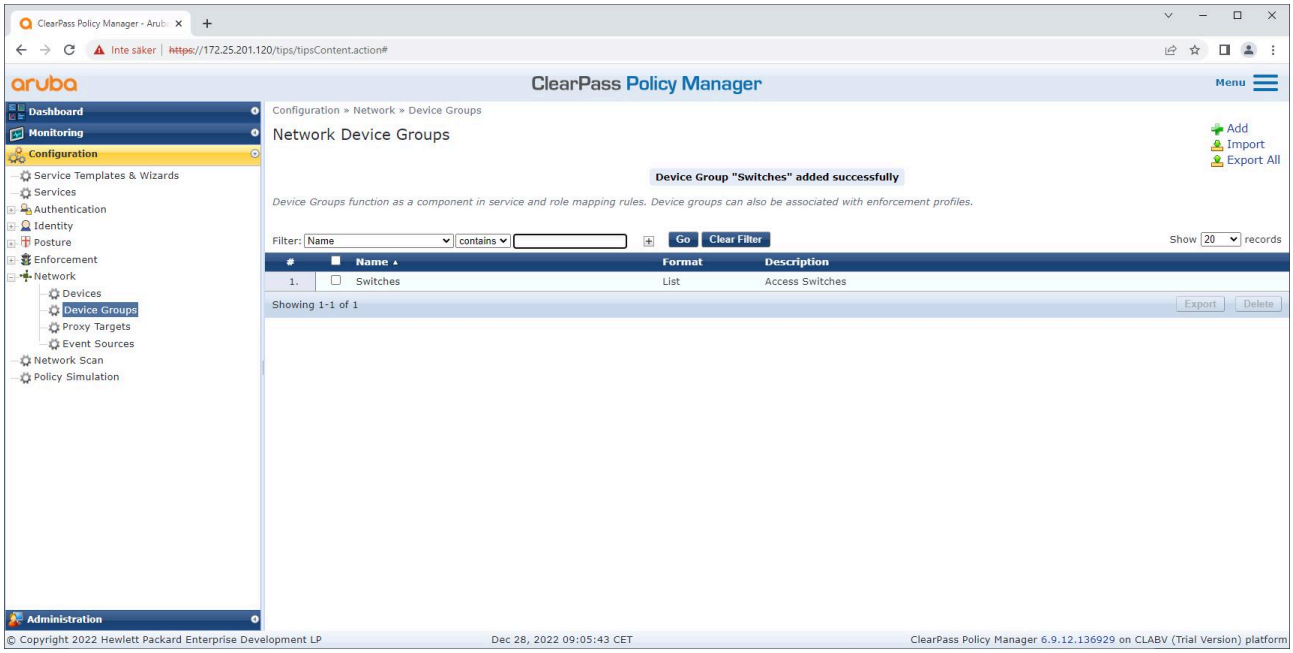
O ClearPass Policy Manager com um único dispositivo de rede confiável configurado.



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



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

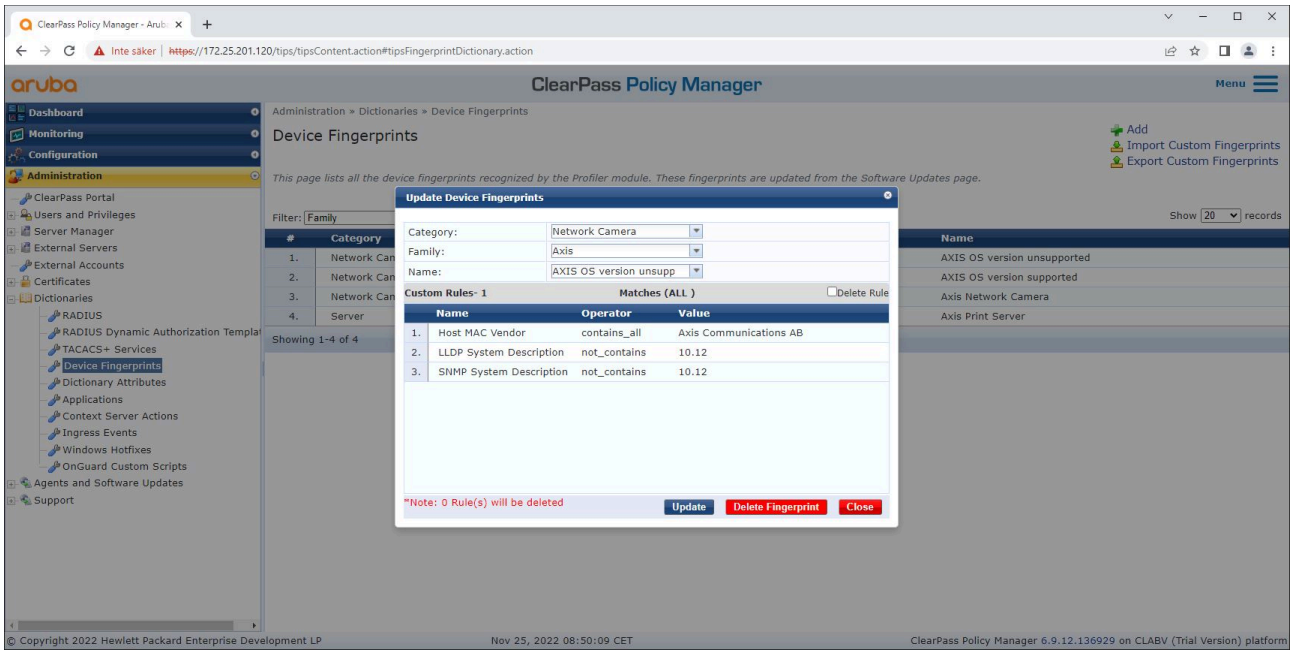


O ClearPass Policy Manager com um grupo de dispositivos de rede configurado, que inclui um ou mais dispositivos de rede confiáveis.

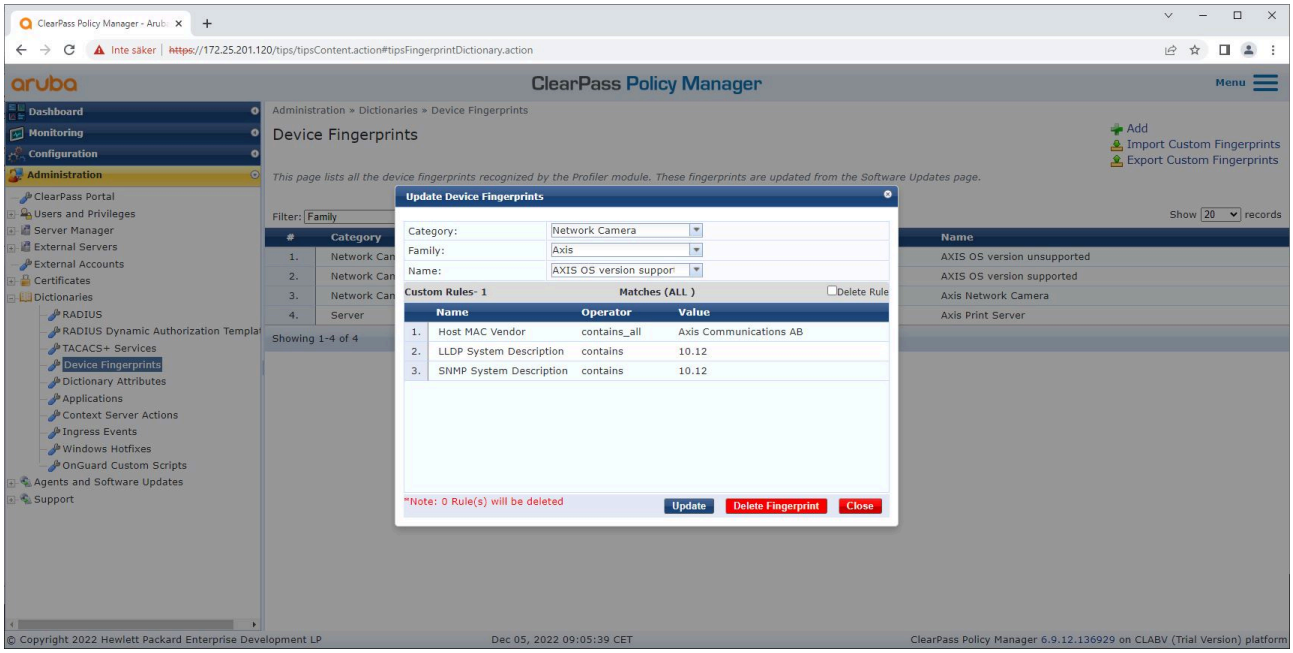
Configuração de impressão digital do dispositivo

O dispositivo Axis pode, por meio da descoberta de rede, distribuir informações específicas do dispositivo, como o endereço MAC e a versão do software do dispositivo. Você pode usar essas informações para criar, atualizar ou gerenciar uma impressão digital do dispositivo no ClearPass Policy Manager. 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)**.
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 versões do AXIS OS diferentes da 10.12 não são suportados neste exemplo.



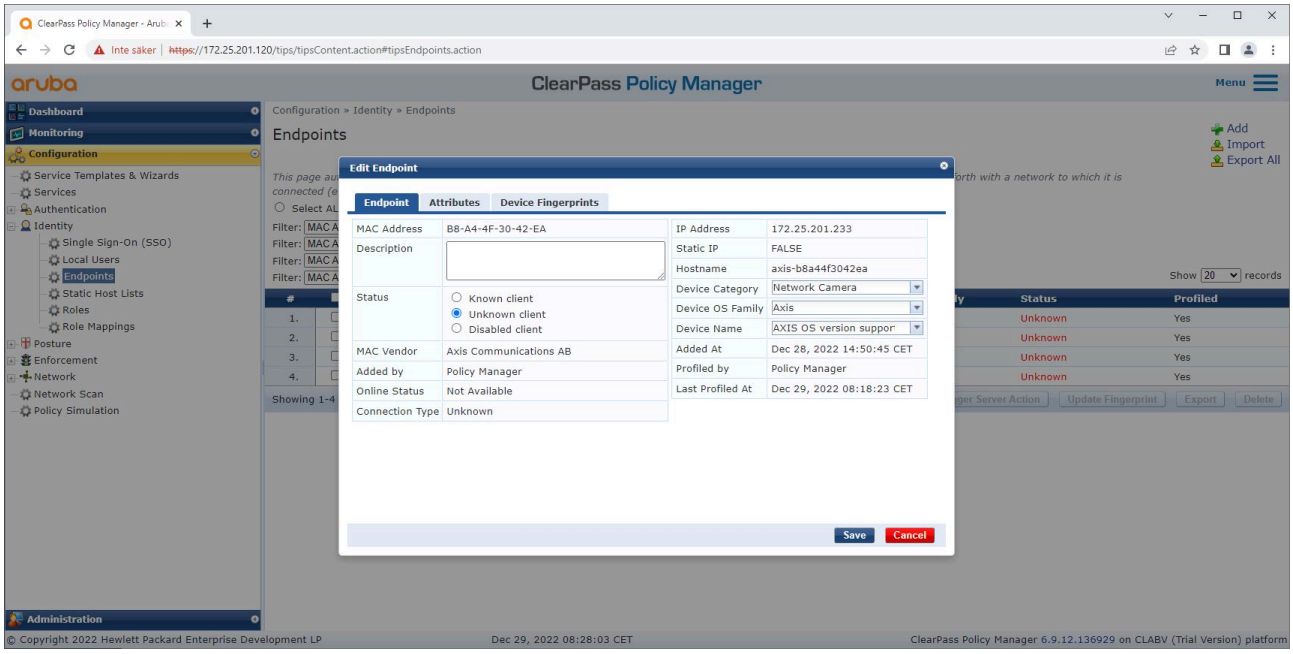
A configuração da impressão digital do dispositivo no ClearPass Policy Manager. Os dispositivos Axis que executam versões do AXIS OS diferentes da 10.12 são suportados neste exemplo.

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

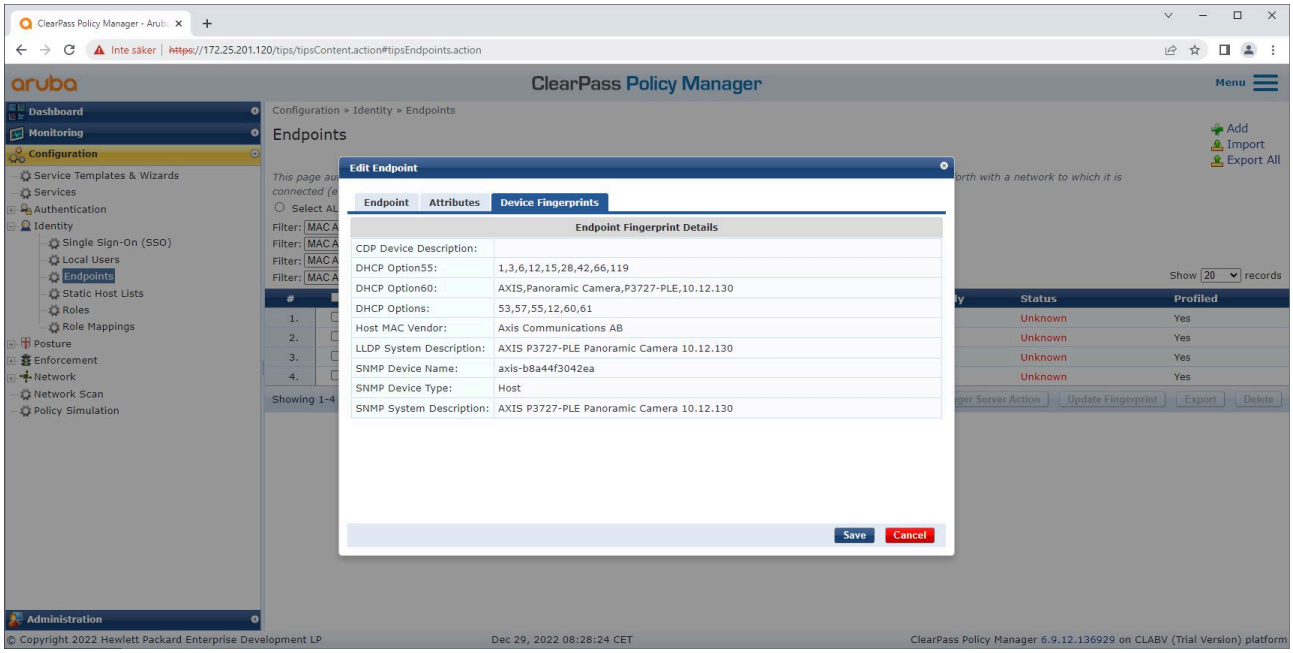
1. Vá para **Configuration > Identity > Endpoints (Configuração > Identidade > Endpoints)**.
2. Selecione o dispositivo que deseja visualizar.
3. Clique na guia **Device Fingerprints (Impressões digitais de dispositivos)**.

Observação

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



Um dispositivo Axis com perfil criado pelo ClearPass Policy Manager.

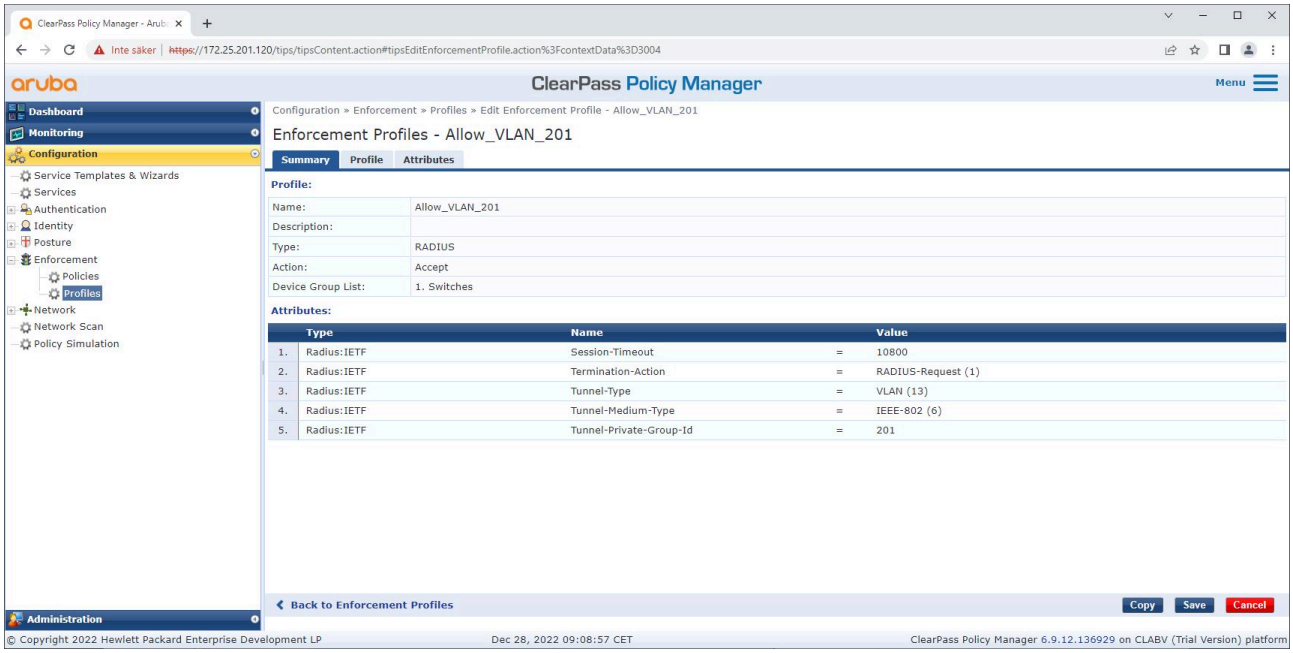


As impressões digitais detalhadas de um dispositivo Axis com perfil estabelecido. Note que o SNMP está desabilitado por padrão nos dispositivos Axis. As informações de descoberta específicas de LLDP, CDP e DHCP são compartilhadas pelo dispositivo Axis no estado padrão de fábrica e são retransmitidas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

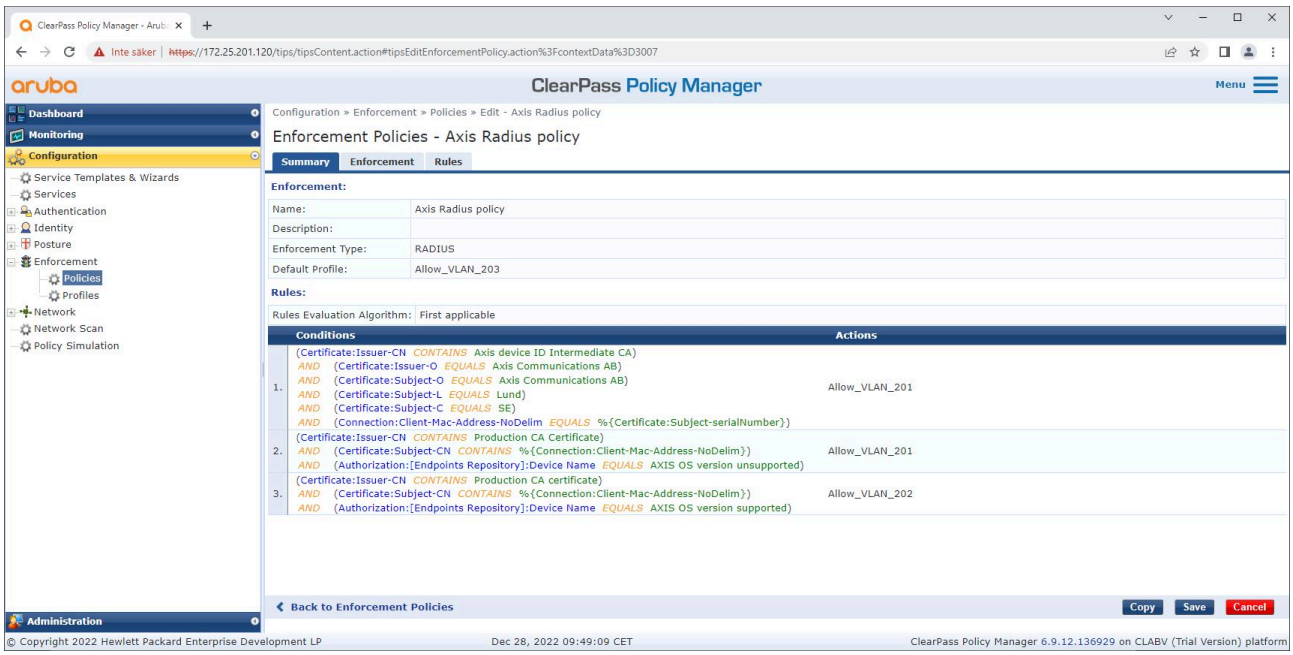
Configuração do perfil de imposição

O Perfil de imposição permite que o ClearPass Policy Manager atribua um ID de VLAN específico a uma porta de acesso no switch. Esta 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 aplicação depende do número de VLANs em uso. Nossa configuração possui três VLANs (VLAN 201, 202, 203), que correspondem a três perfis de imposição.

Depois que os perfis de imposição da VLAN forem configurados, a política de imposição propriamente dita 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 são:

Acesso à rede negado

O acesso à rede é negado quando a autenticação de controle de acesso à rede IEEE 802.1X não 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. É necessária uma inspeção manual do dispositivo para determinar 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.
- O endereço MAC do dispositivo corresponde ao esquema de endereços MAC 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 e país.

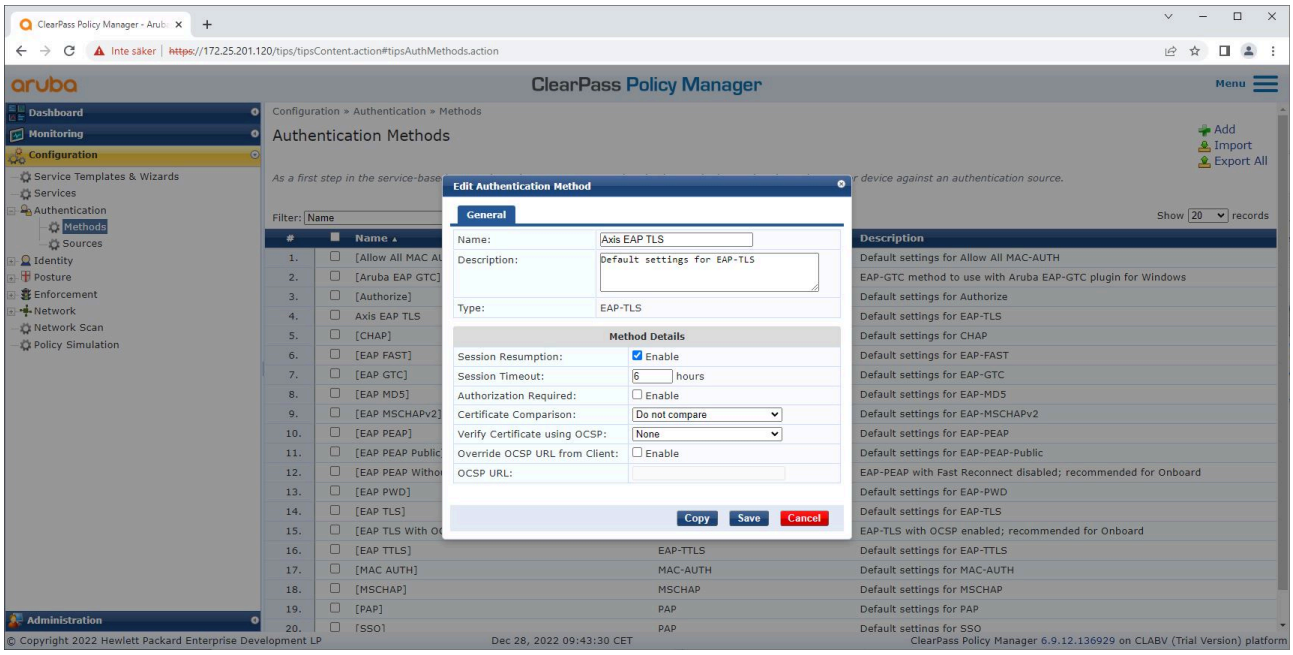
Rede de produção (VLAN 202)

O dispositivo Axis recebe acesso à rede de produção na qual vai 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:

- A versão do AXIS OS do dispositivo.
- O endereço MAC do dispositivo corresponde ao esquema de endereços MAC específico do fornecedor, com o atributo de número de série do certificado de ID do dispositivo Axis.
- O certificado de nível de produção pode ser verificado pelo armazenamento de certificados confiável.

Configuração do método de autenticação

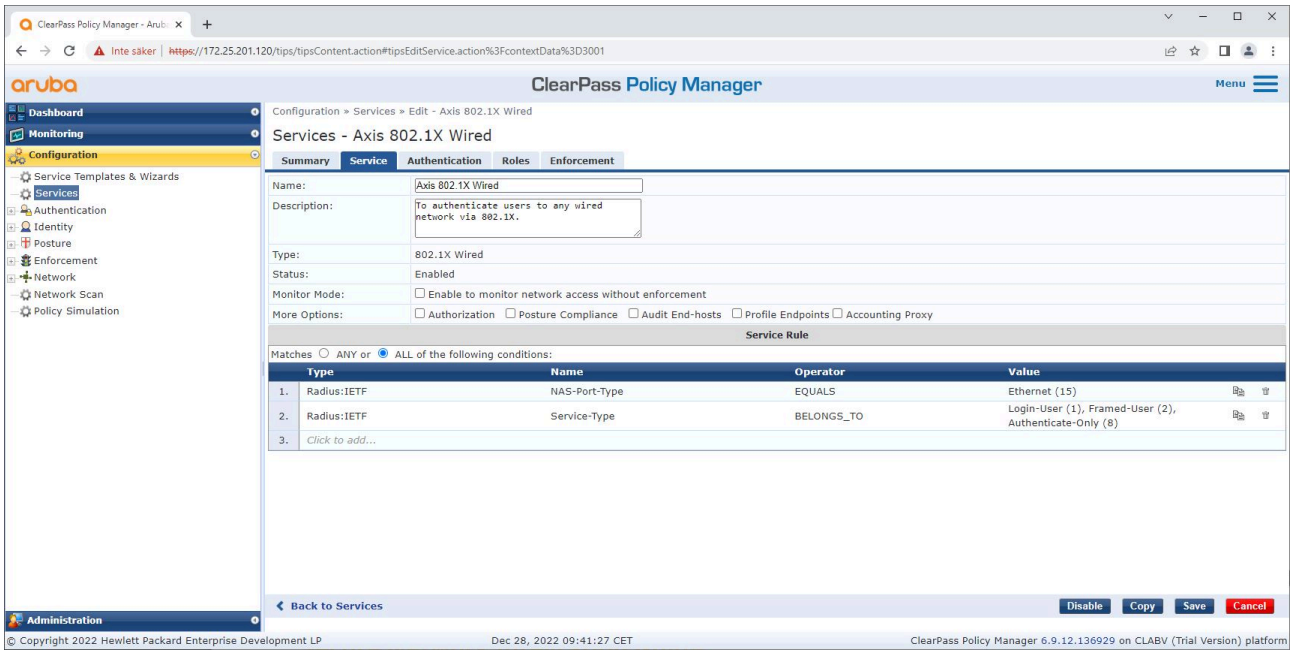
O método de autenticação define como um dispositivo Axis tenta se autenticar na rede. O método preferencial é IEEE 802.1X EAP-TLS, já que os dispositivos Axis com Axis Edge Vault são fornecidos com IEEE 802.1X EAP-TLS habilitado por padrão.



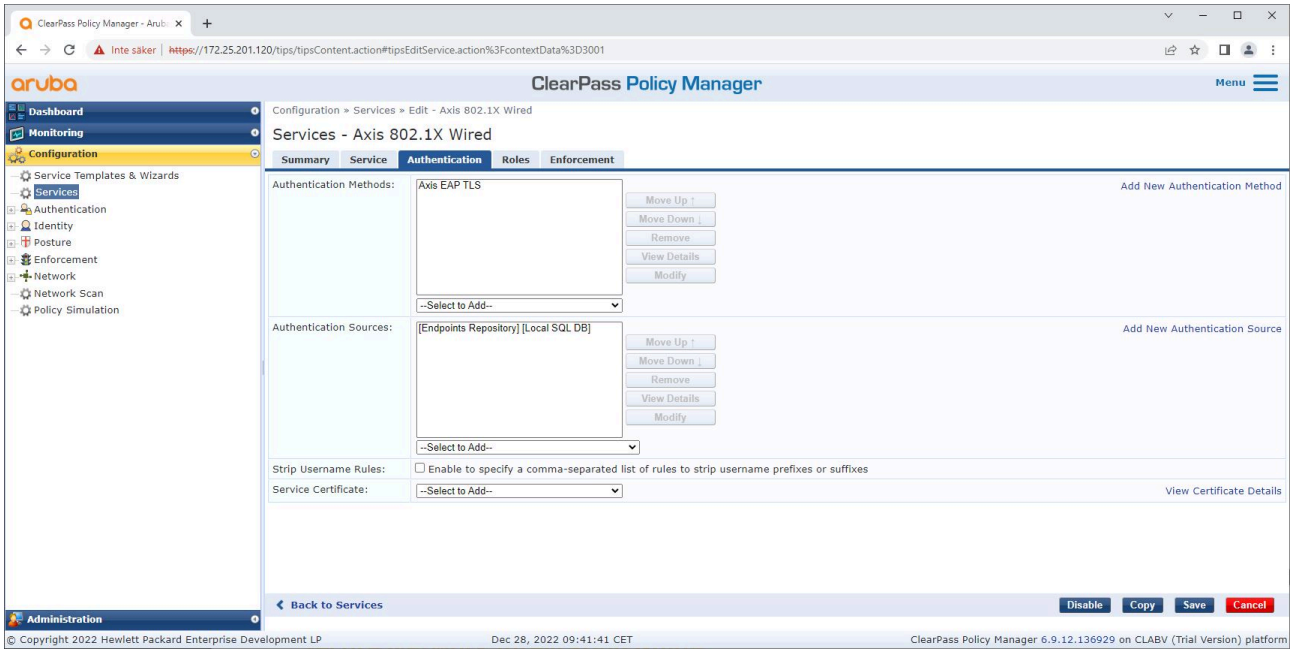
A interface do método de autenticação do ClearPass Policy Manager, em que o método de autenticação EAP-TLS para dispositivos Axis é definido.

Configuração do serviço

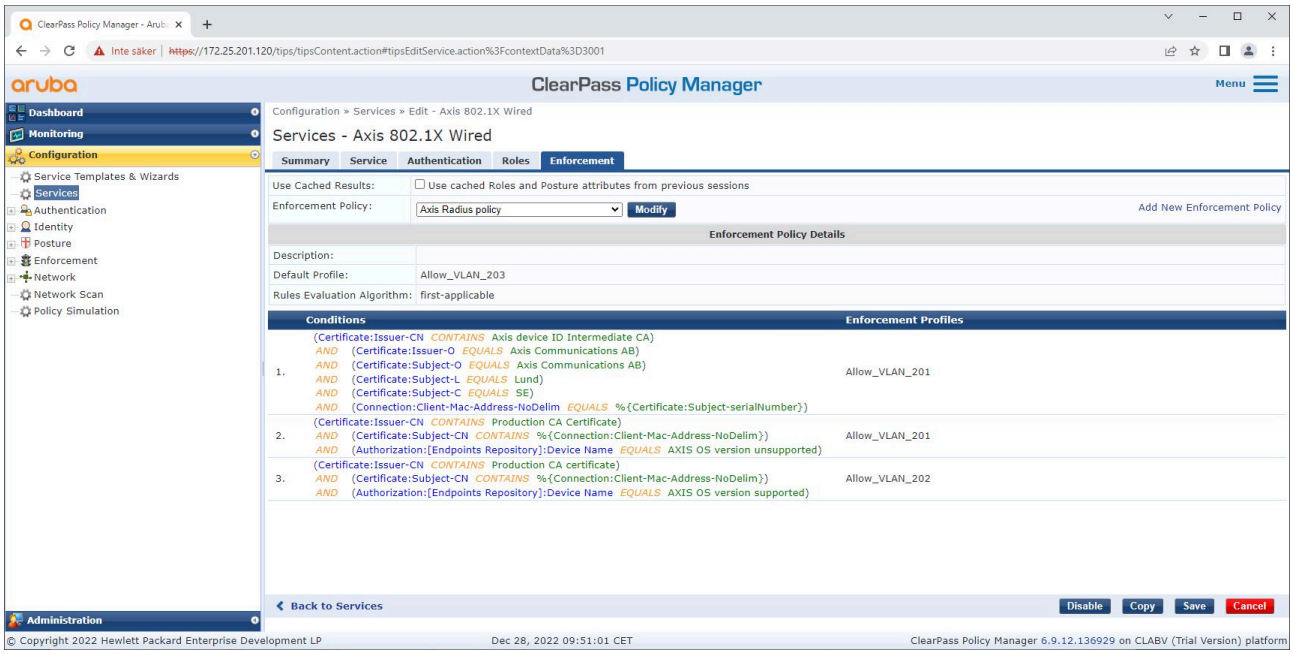
Na página **Services (Serviços)**, as etapas de configuração são combinadas em um único serviço, que lida com a autenticação e a autorização de dispositivos Axis em redes HPE Aruba Networking.



Um serviço Axis dedicado é criado, com IEEE 802.1X como método de conexão.



O método de autenticação EAP-TLS criado anteriormente está configurado para o serviço.



A política de aplicação criada anteriormente está 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 PoE Axis compatíveis. Para integrar dispositivos Axis com segurança às redes HPE Aruba Networking, o switch de acesso deve 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.

Este exemplo demonstra a configuração global e de porta dos switches de acesso HPE Aruba Networking.

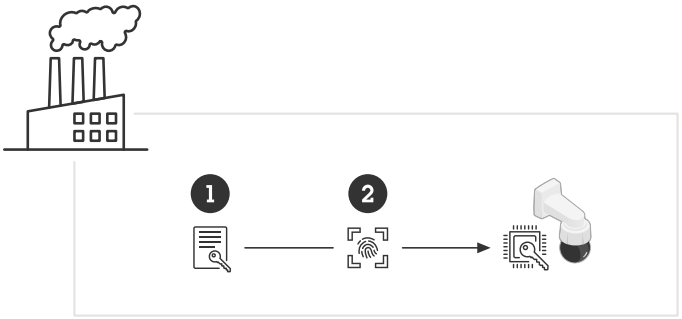
```
radius-server host MyRADIUSIPAddress key "MyRADIUSKey"
```

```
aaa authentication port-access eap-radiusaaa port-access authenticator 18-19aaa port-access
authenticator 18 reauth-period 300aaa port-access authenticator 19 reauth-period 300aaa port-
-access authenticator active
```

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 do dispositivo Axis. A ID do dispositivo Axis é baseada no padrão internacional IEEE 802.1AR, que define um método para identificação automatizada e segura de dispositivos e integração à rede por meio de IEEE 802.1X.



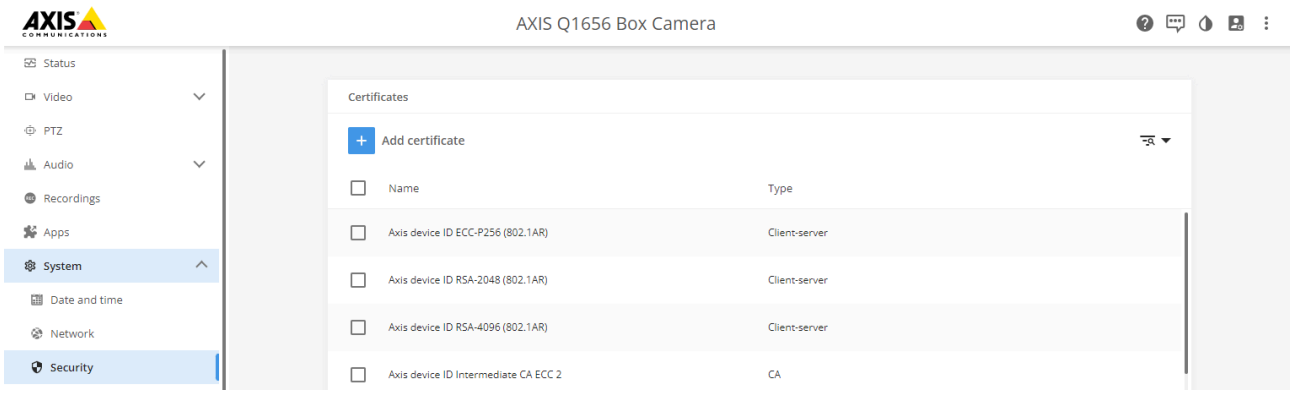
Os dispositivos Axis são fabricados com o certificado de ID de dispositivo Axis compatível com IEEE 802.1AR para serviços de identidade de dispositivos confiáveis

1 *Infraestrutura da chave da 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 são compatíveis com o Axis Edge Vault e com a ID de dispositivo Axis.

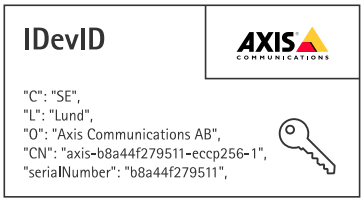
Observação

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



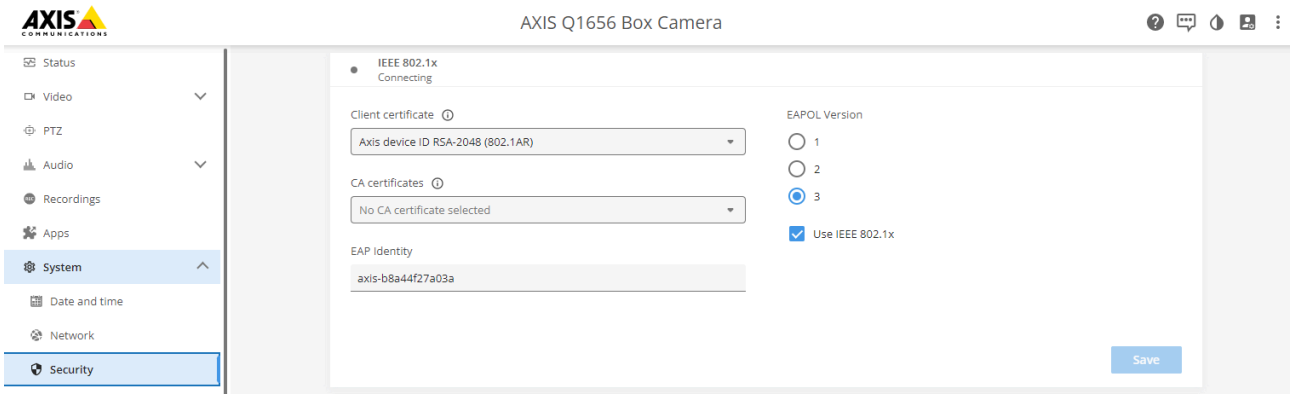
O armazenamento de certificados do dispositivo Axis no estado padrão de fábrica com a ID de dispositivo Axis.

O certificado de ID do dispositivo Axis compatível com IEEE 802.1AR inclui informações sobre o número de série e outras informações específicas do fornecedor. Essas informações são usadas pelo ClearPass Policy Manager para fins de análise e tomada de decisões de concessão de acesso à rede. As informações abaixo podem ser obtidas a partir de um certificado de ID do 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 formado pela combinação do nome da empresa Axis, o número de série do dispositivo, seguido do algoritmo criptográfico (ECC P256, RSA 2048, RSA 4096). A partir do AXIS OS 10.1 (2020-09), o IEEE 802.1X é habilitado por padrão com a ID do dispositivo Axis pré-configurado. Isso permite que o dispositivo 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 forma econômica. O AXIS Device Manager é um aplicativo baseado em Microsoft Windows® que é instalado localmente em uma máquina na rede, enquanto o AXIS Device Manager Extend depende da infraestrutura em nuvem para realizar o gerenciamento de dispositivos em vários locais. Ambos oferecem recursos fáceis de gerenciamento e configuração, tais como:

- Instalação das atualizações do AXIS OS.
- Aplicação de configurações de segurança cibernética, como certificados HTTPS e IEEE 802.1X.
- Definição de configurações específicas do dispositivo, como configurações de imagens, entre outras.

Operação de rede segura – IEEE 802.1AE MACsec

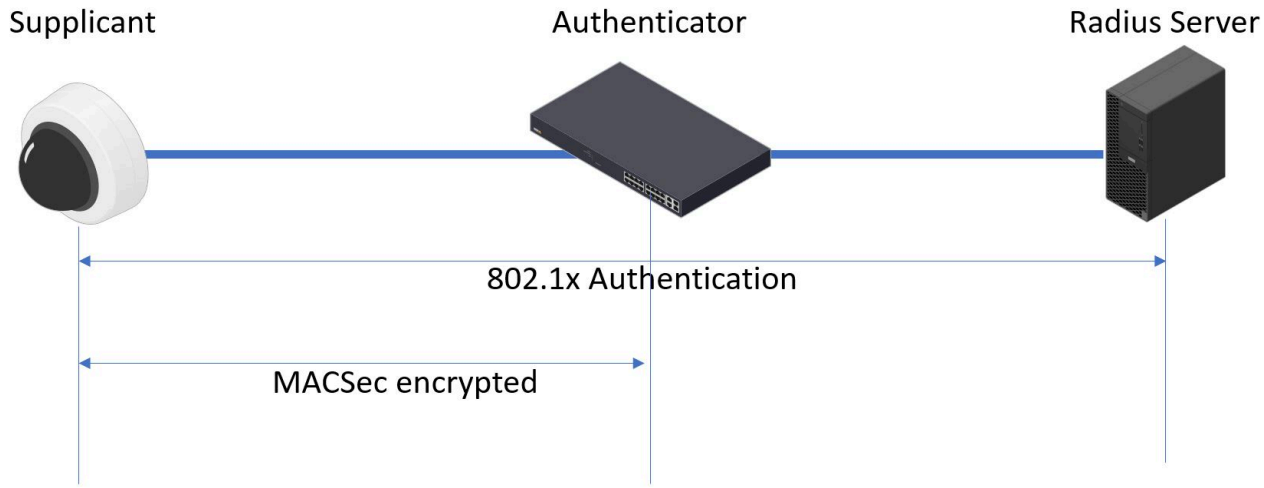
Para assistir a este vídeo, vá para a versão Web deste documento.

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

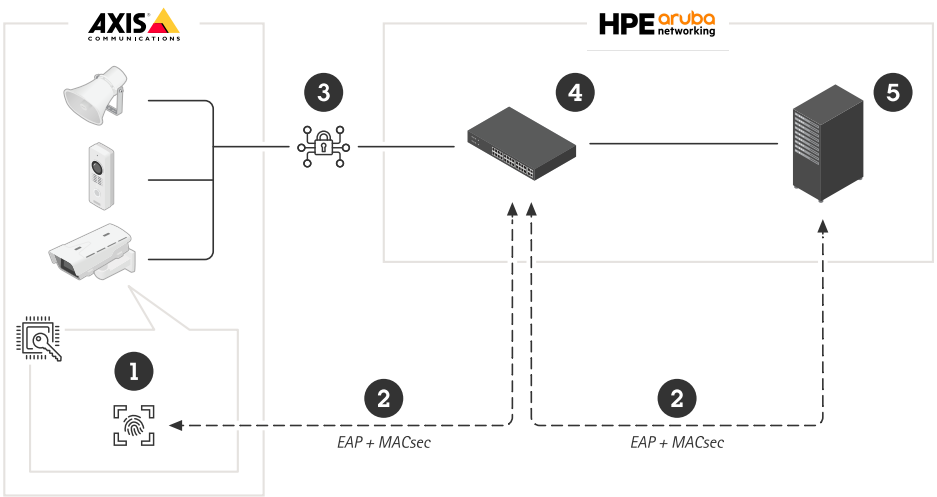
O IEEE 802.1AE MACsec (Media Access Control Security) é um protocolo de rede bem definido que protege criptograficamente os links de ethernet ponto a ponto na camada 2 da rede. Ele garante a confidencialidade e a integridade das transmissões de dados entre dois hosts.

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 versões posteriores, o IEEE 802.1X está habilitado por padrão nos dispositivos compatíveis com a ID do dispositivo Axis. No AXIS OS 11.8 e versões posteriores, oferecemos suporte ao MACsec com modo automático usando IEEE 802.1X 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.



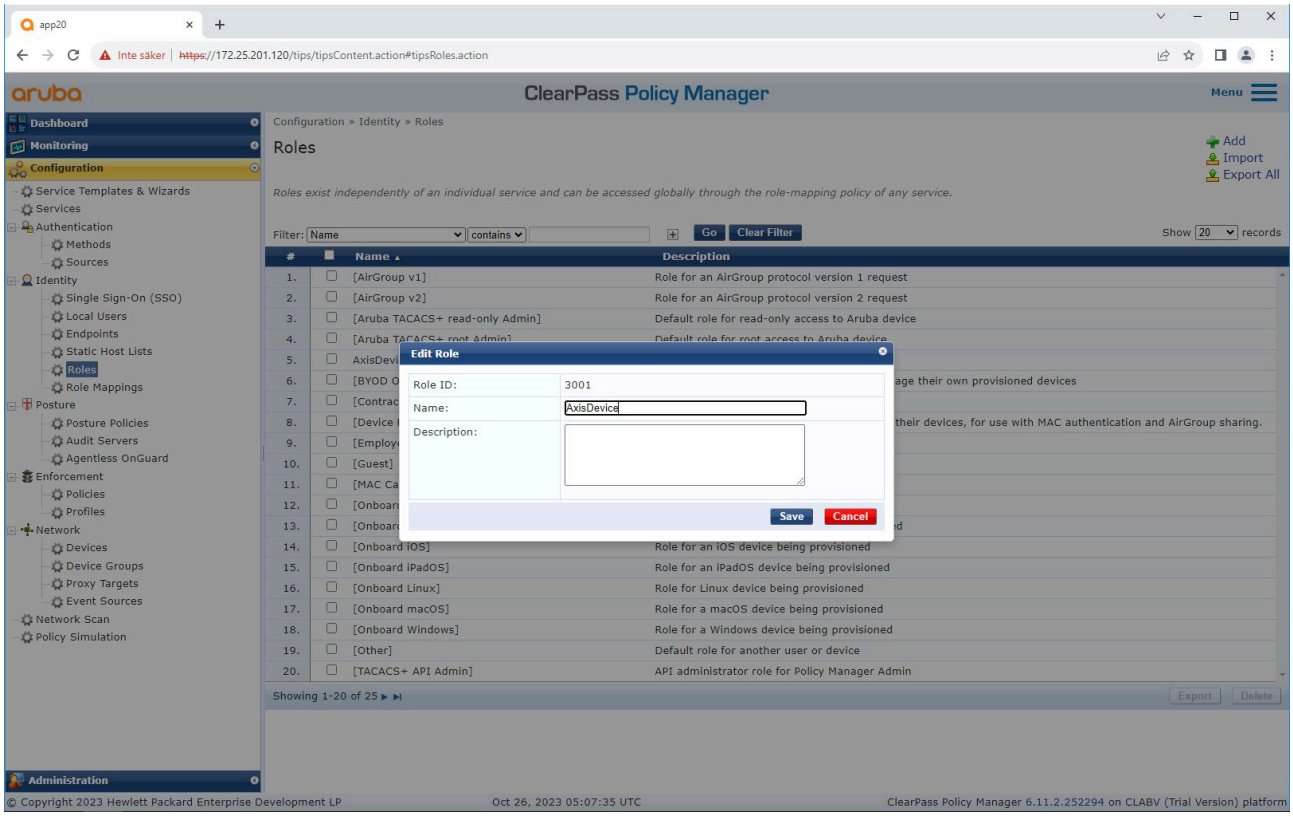
A ID do dispositivo Axis armazenada com segurança (1) – uma identidade de dispositivo segura compatível com IEEE 802.1AR – é usada para autenticação na rede (4, 5) via controle de acesso à rede baseado em porta IEEE 802.1X EAP-TLS (2). Por meio da sessão EAP-TLS, as chaves MACsec são trocadas automaticamente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

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.

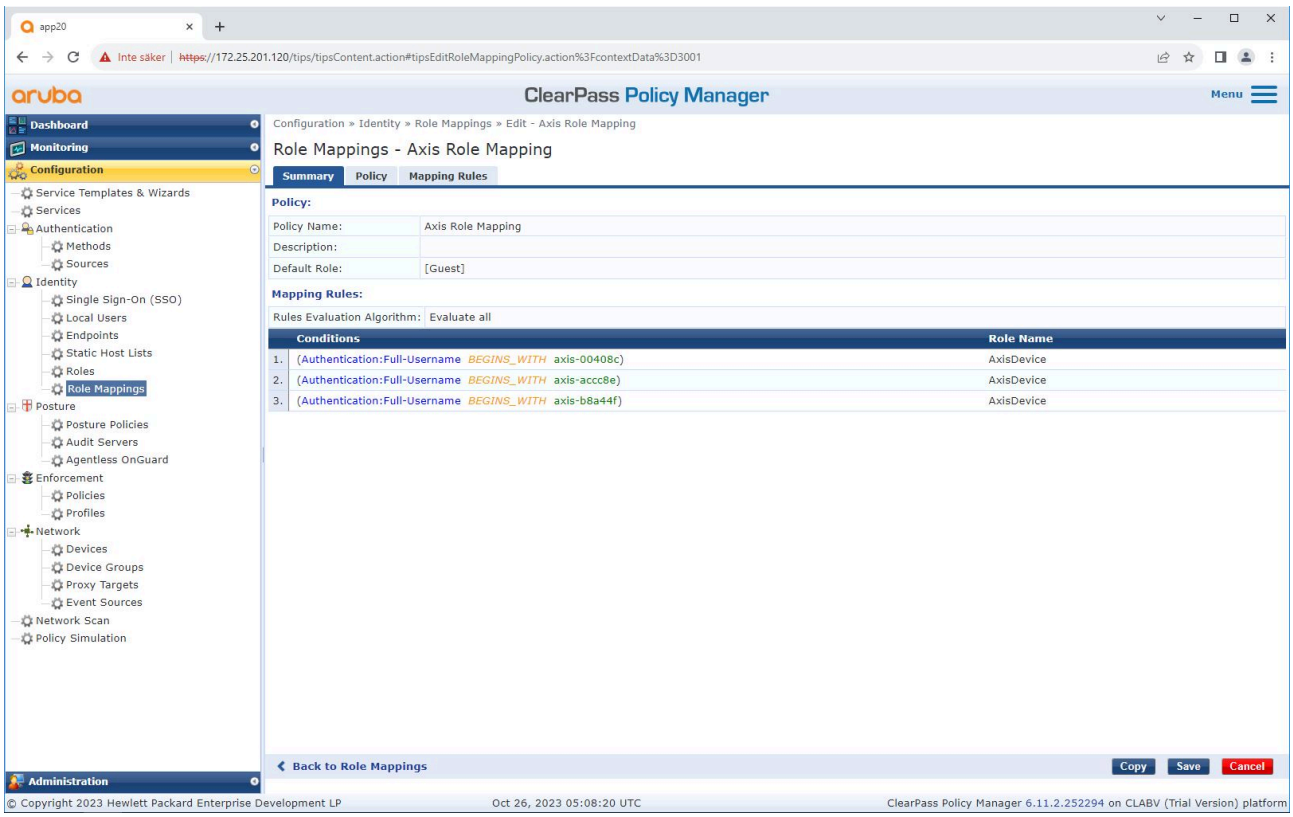
Se o switch de acesso do HPE Aruba Networking não comporta o MACsec usando EAP-TLS, o modo de chave pré-compartilhada poderá ser usado e configurado manualmente.

ClearPass Policy Manager do HPE Aruba Networking

Política de funções e mapeamento de funções



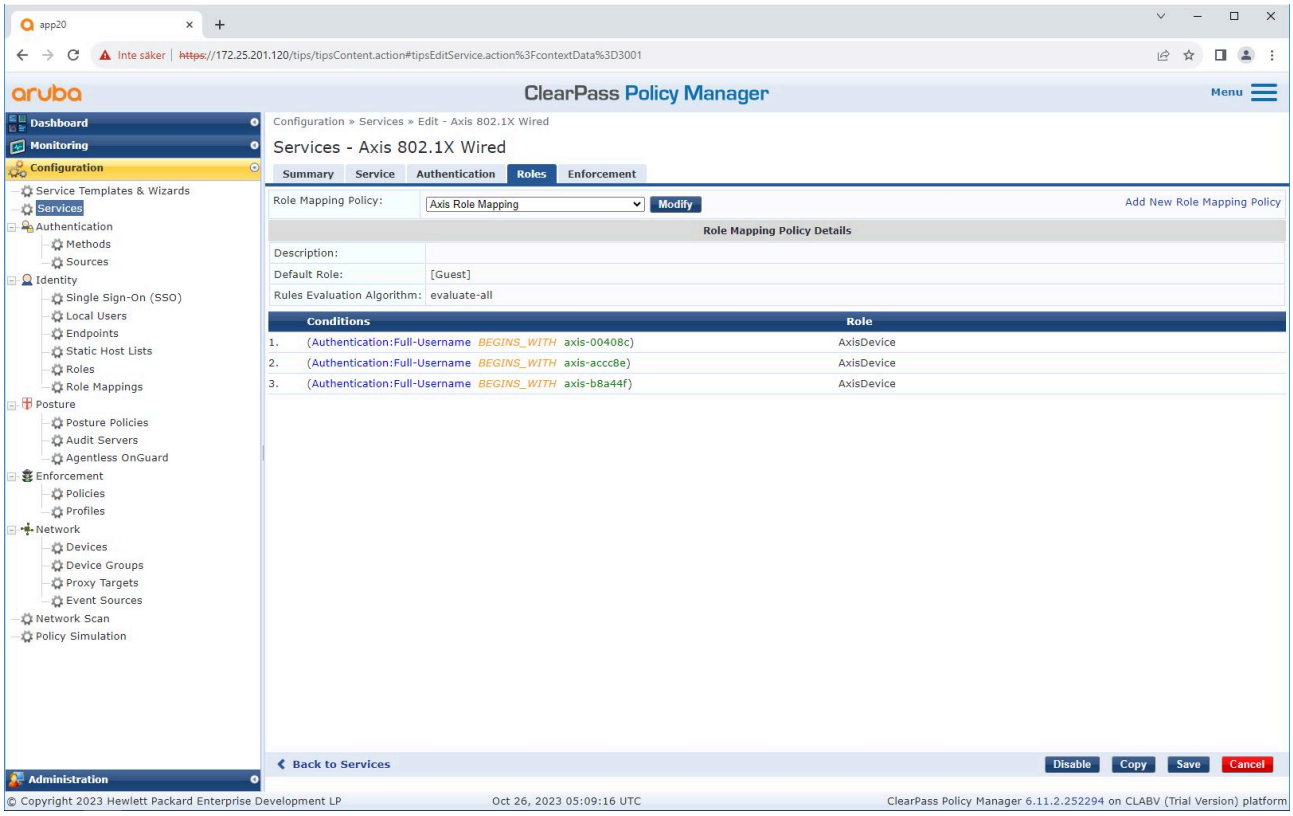
Adicione um nome de função para dispositivos Axis. O nome é o nome da função de acesso à porta na configuração do switch de acesso.



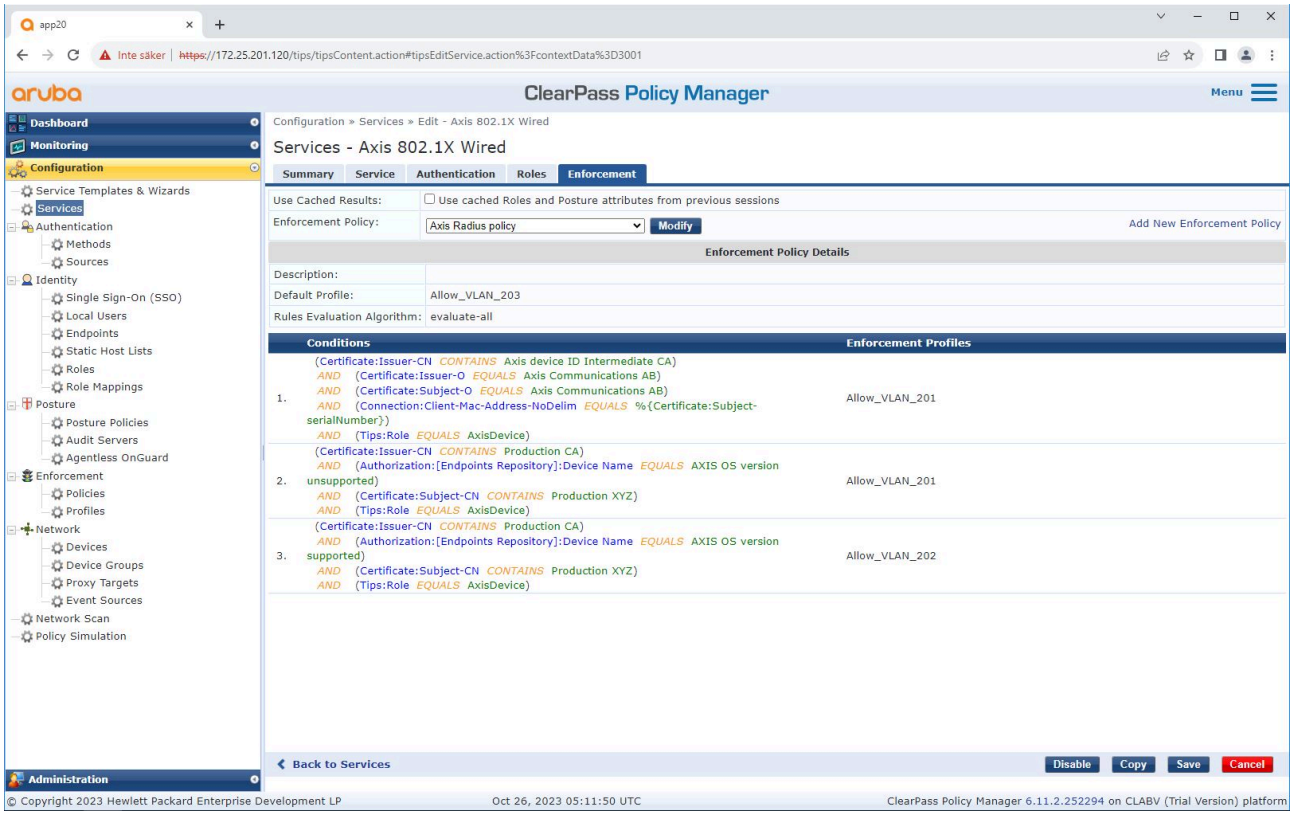
Adicione uma política de mapeamento de funções Axis para a função de dispositivo Axis criada anteriormente. As condições definidas são necessárias para que um dispositivo seja mapeado para a função de dispositivo Axis. Se as condições não forem atendidas, o dispositivo torna-se parte da função [Guest] (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

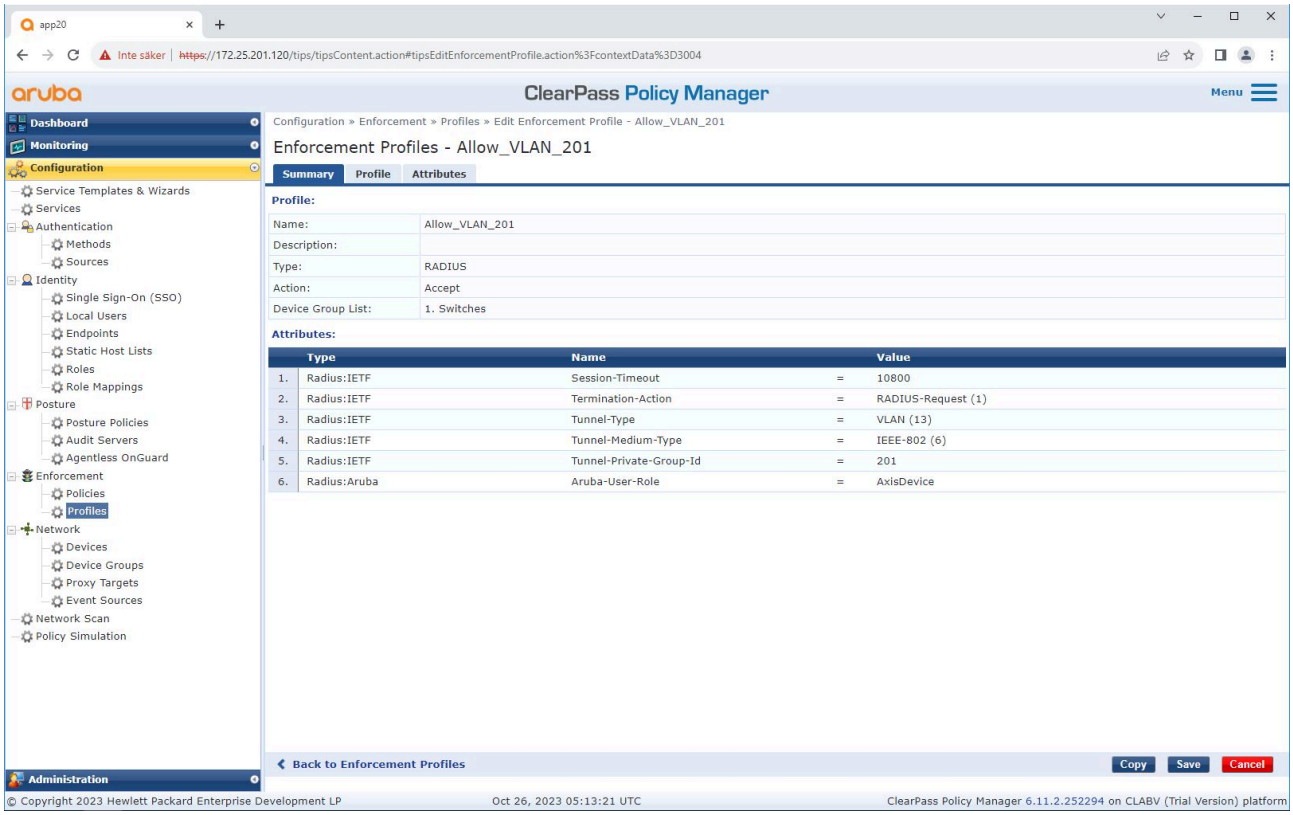


Adicione a política de mapeamento de funções Axis criada anteriormente ao serviço que define IEEE 802.1X como o método de conexão para integração de dispositivos Axis.



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

Perfil de imposição



Adicione o nome da função Axis como um 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 *Switch de acesso do HPE Aruba Networking, on page 15*, veja o exemplo de configuração de porta do switch de acesso HPE Aruba Networking abaixo para configurar IEEE 802.1AE MACsec.

```
macsec policy macsec-eapcipher-suite gcm-aes-128

port-access role AxisDeviceassociate macsec-policy macsec-eapauth-mode client-mode

aaa authentication port-access dot1x authenticatormacsecmkacak-length 16enable
```

Gerenciamento de certificados – Enrollment over Secure Transport (EST)

Os certificados digitais são essenciais para proteger dispositivos e redes, mas o gerenciamento deles pode ser complexo e demorado. Os certificados expiram e devem ser renovados regularmente. Sem automação, esse processo é repetitivo e manual, especialmente em grandes implantações ou ambientes com diferentes tipos de dispositivos combinados.

O AXIS OS 12.9 apresenta suporte para Enrollment over Secure Transport (EST), um protocolo para o provisionamento seguro de certificados para dispositivos. Definido na RFC 7030, o EST é uma solução baseada em padrão projetada para simplificar e automatizar todo o ciclo de vida do certificado, incluindo:

- Registro – emissão segura de novos certificados para dispositivos
- Renovação – substituição automática de certificados que estão expirando
- Novo registro – atualização de certificados com base em políticas de TI

O EST suporta políticas definidas por TI para atributos de certificados, tais como período de validade, tipo de chave (RSA/ECC) ou tamanho da chave, e utiliza exclusivamente HTTPS.

Principais benefícios do EST

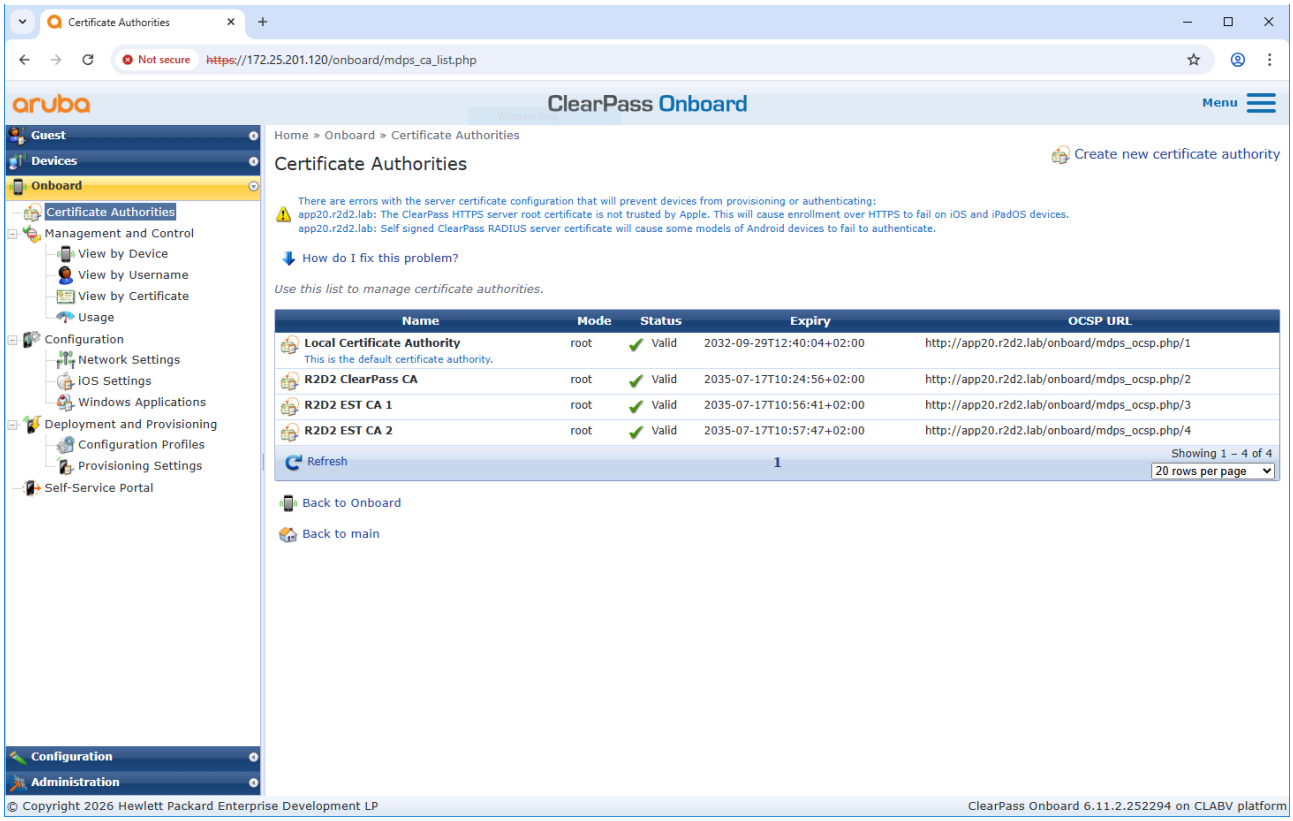
- A política de TI gerencia o registro, a renovação e o novo registro de certificados de forma automatizada, removendo completamente a necessidade de configurações manuais e demoradas.
- Comunicação segura de última geração via somente HTTPS TLS 1.2/1.3.
- Visibilidade/monitoramento centralizado para equipes de TI.
  Baseado em padrões (RFC 7030) e integra-se à infraestrutura de TI.
- Solução dimensionável para IoT, redes empresariais e gerenciamento de dispositivos.

Consulte nossa *Base de Conhecimento do AXIS OS* para obter a documentação geral do EST.

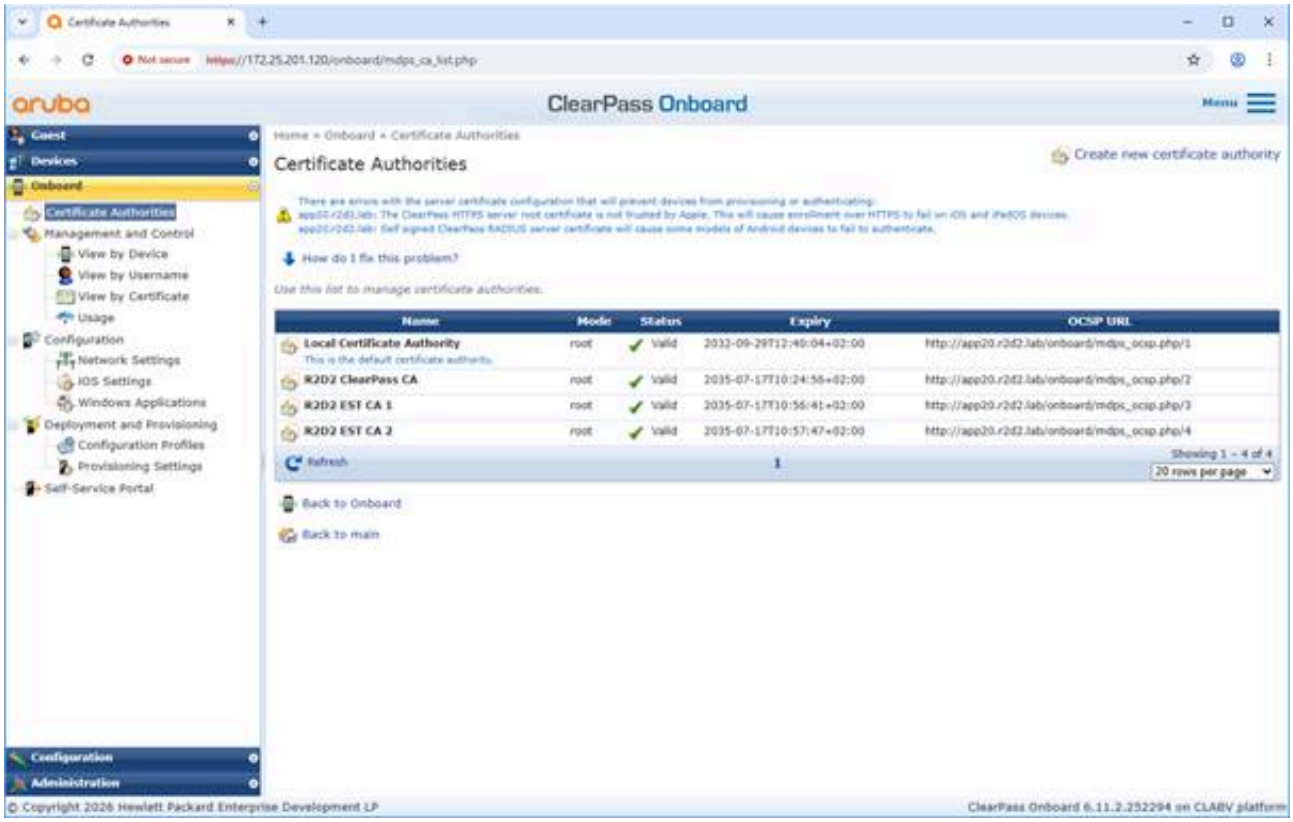
Configuração do HPE Aruba ClearPass Onboard

O Aruba ClearPass Onboard integra-se ao EST para distribuir e realizar o gerenciamento seguro de certificados de dispositivos para acesso à rede. Utilizando o EST, os pontos de extremidade autenticam-se no ClearPass e registam-se para obter um certificado exclusivo através de um canal TLS seguro, que é então utilizado para autenticação baseada em certificado 802.1X e outros serviços. Isso fornece um método baseado em padrões, automatizado e sem senha para aplicar políticas de acesso seguro com base na identidade do dispositivo.

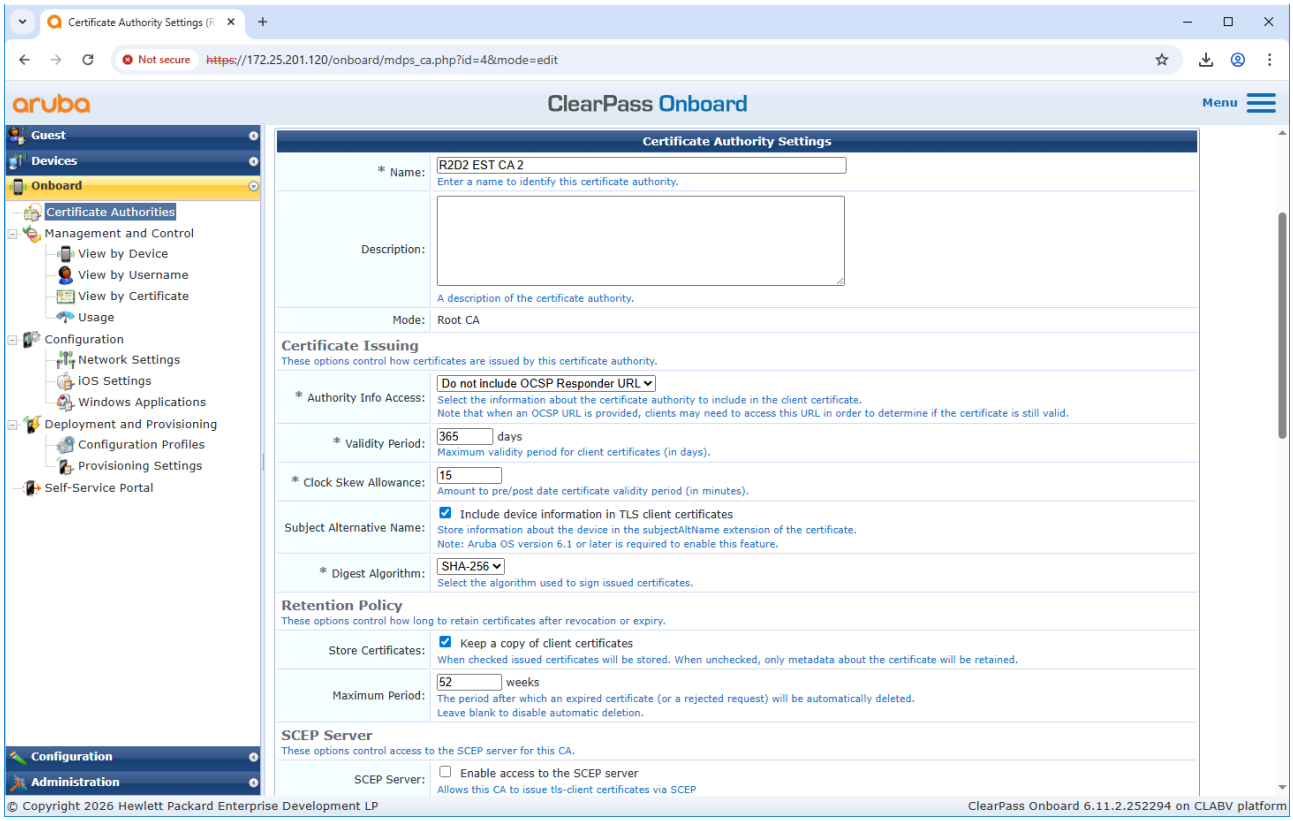
Configuração da autoridade certificadora



Crie uma nova autoridade certificadora no ClearPass Onboard.



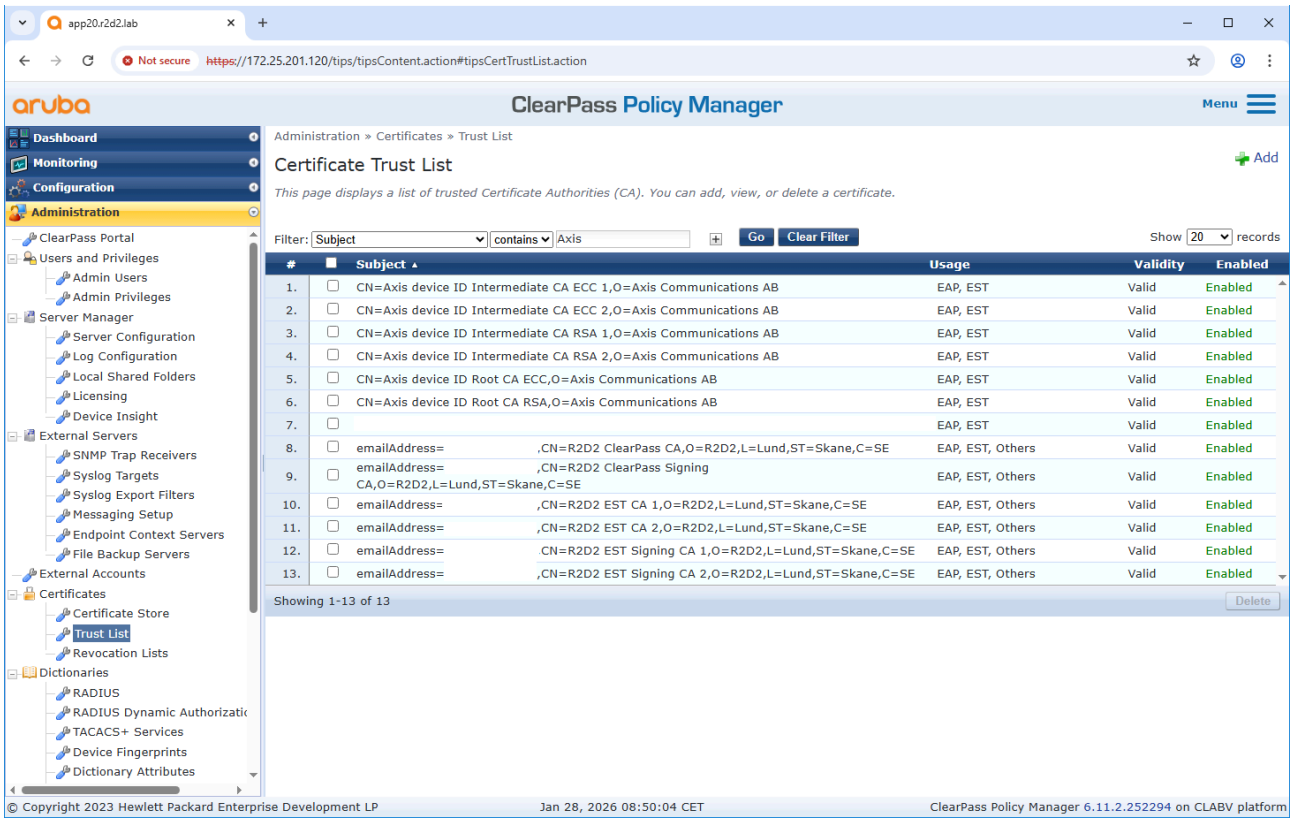
Dentro da autoridade certificadora criada, são definidos o tipo de chave, o tamanho da chave, o período de validade e outros detalhes.



Ative a funcionalidade do servidor EST para a autoridade certificadora criada. Configure o método de autenticação EST para utilizar o certificado do cliente.

Configuração do HPE Aruba ClearPass Policy Manager

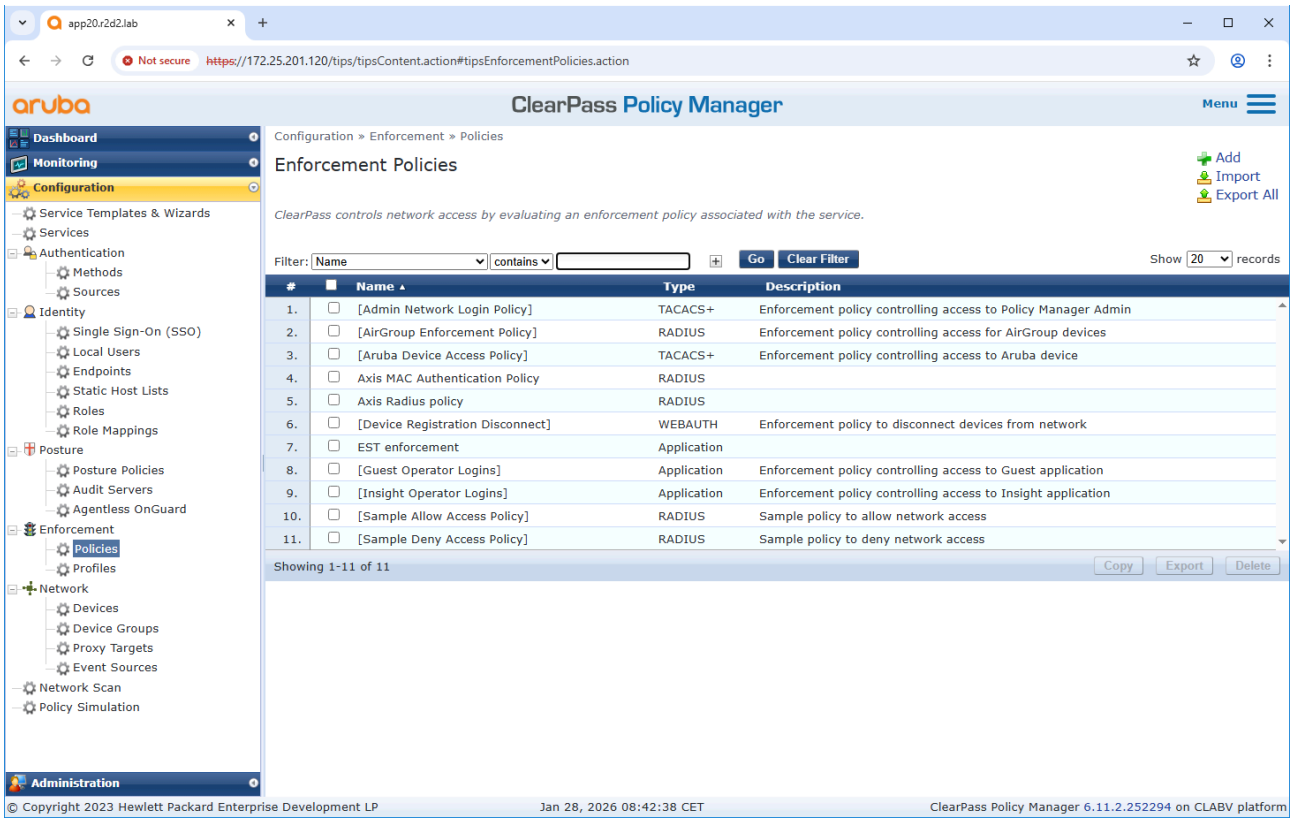
Configuração de armazenamento de certificados confiável



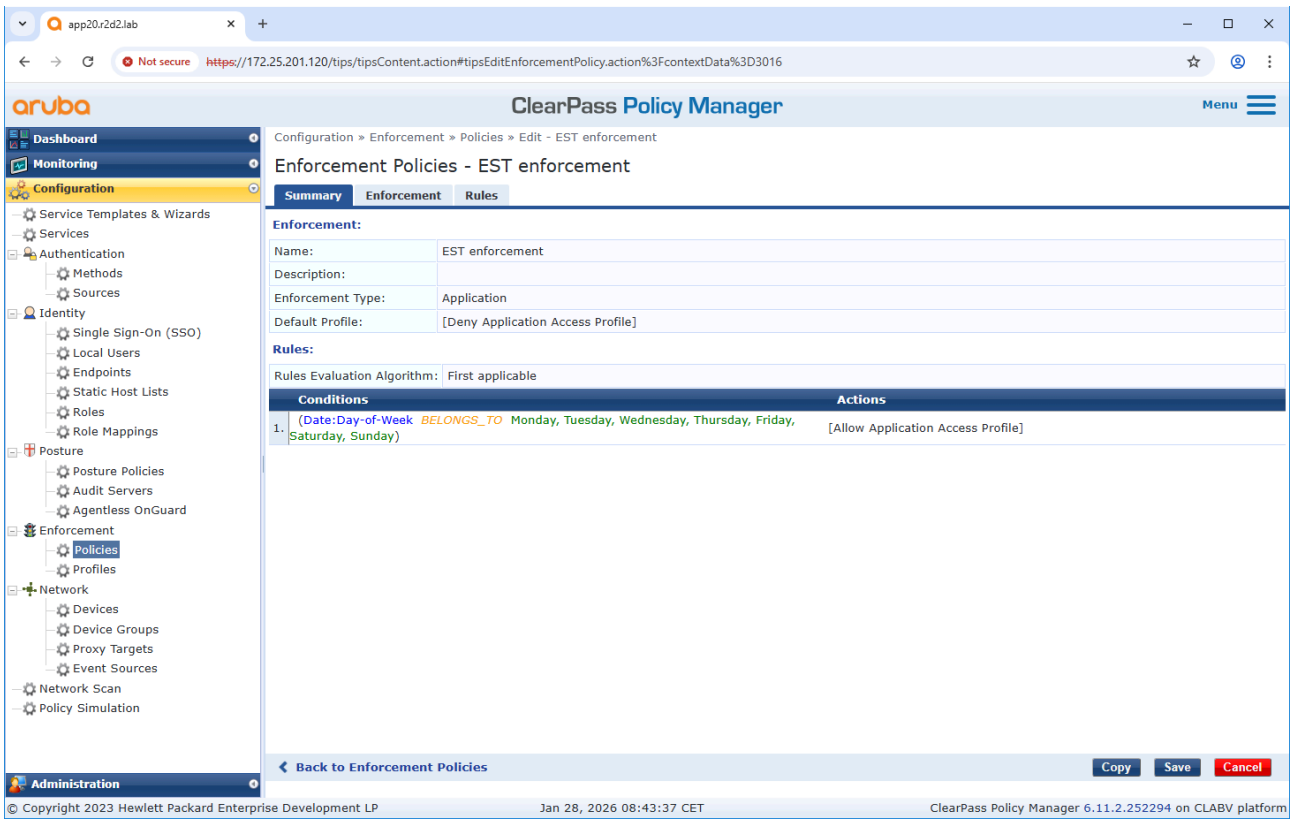
Caso ainda não o tenha feito, carregue os *certificados IEEE 802.1AR* específicos da Axis para o armazenamento de certificados confiável do ClearPass Policy Manager. Certifique-se de que o uso do EST seja adicionado. Verifique isso também para a autoridade certificadora criada anteriormente no ClearPass Onboard.

Configuração da política de imposição

O Perfil de imposição permite que o ClearPass Policy Manager atribua imposições específicas ao aplicativo EST. Por exemplo, novos certificados só podem ser registrados a partir de pontos de extremidade específicos ou apenas em dias específicos da semana.

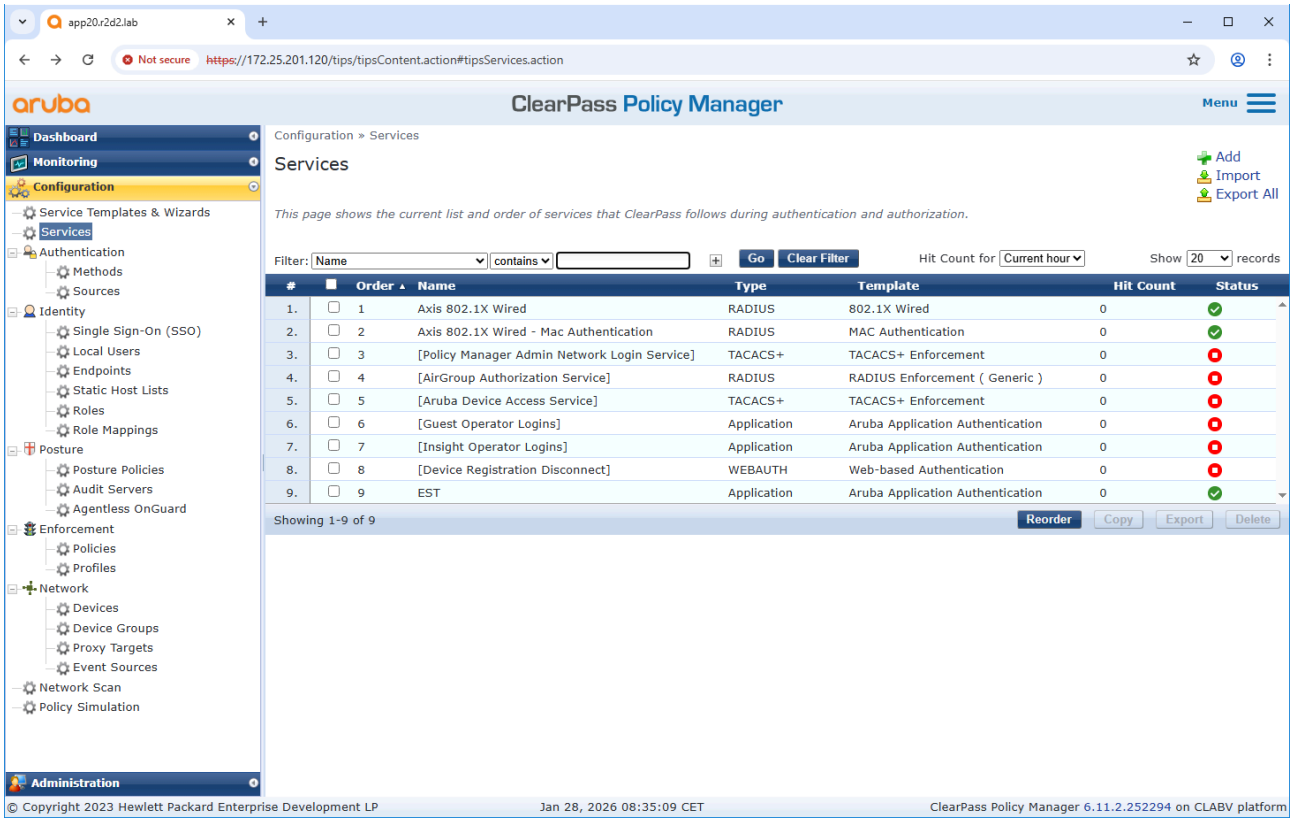


A visão geral das políticas de imposição no ClearPass Policy Manager.

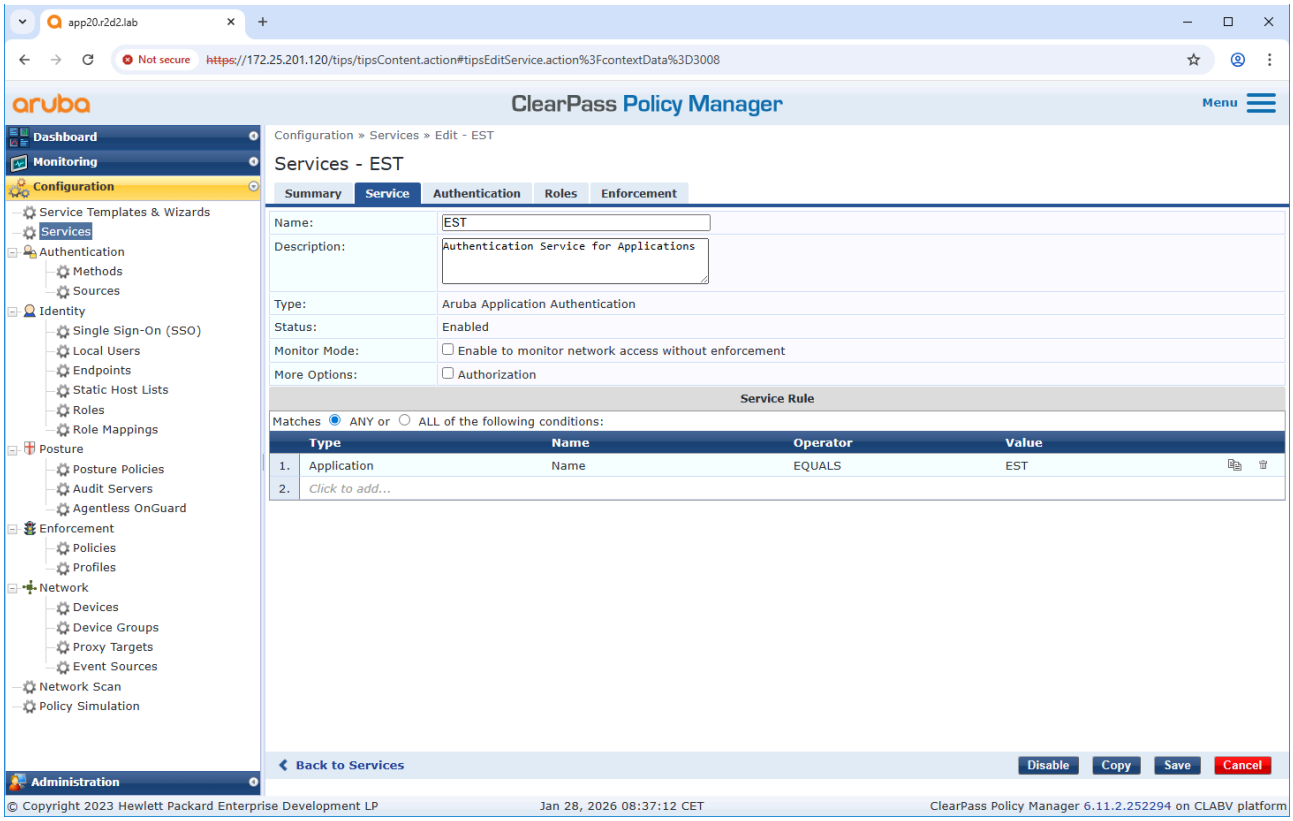


Neste exemplo de política, o aplicativo EST é permitido todos os dias da semana.

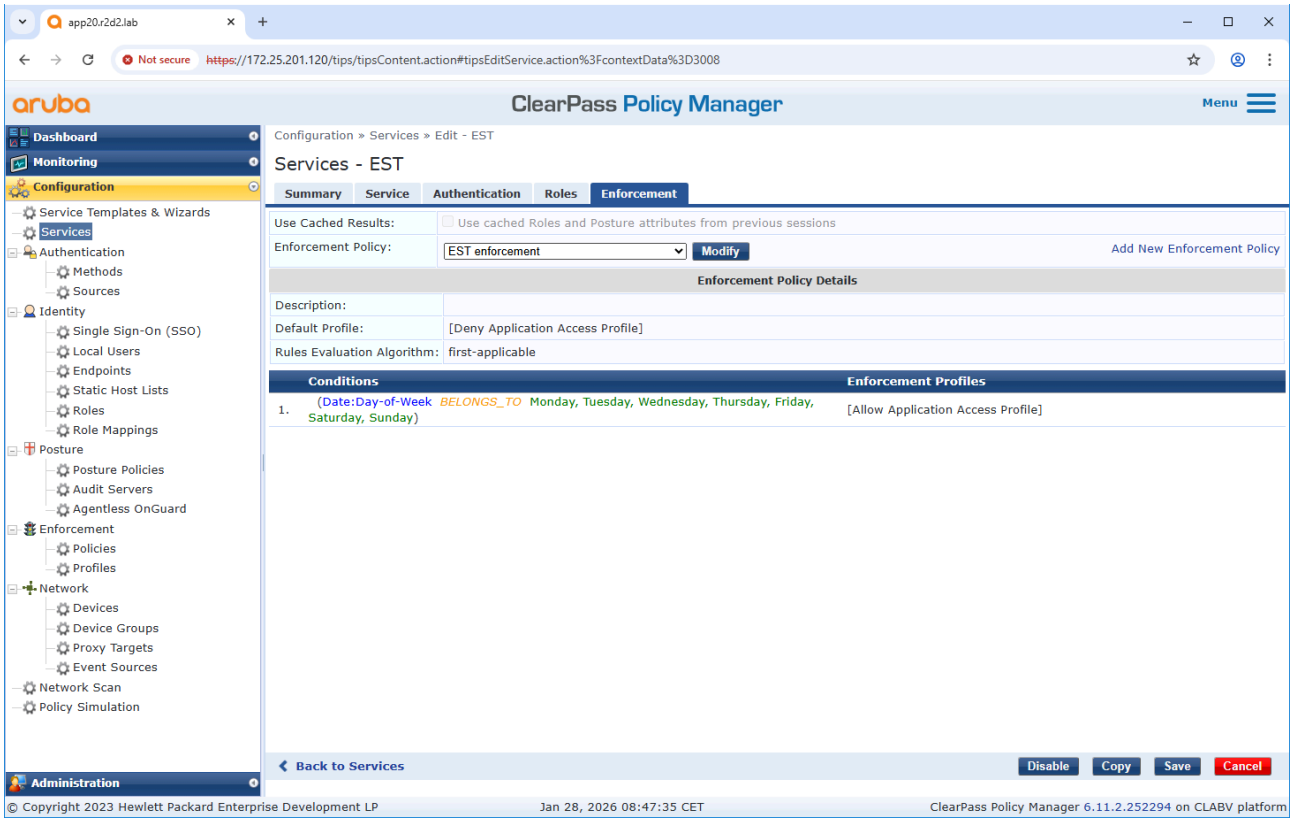
Configuração do serviço



É necessário criar um serviço EST dedicado.



O serviço deve configurado para o aplicativo EST.



Selecione a política de imposição de EST criada anteriormente.

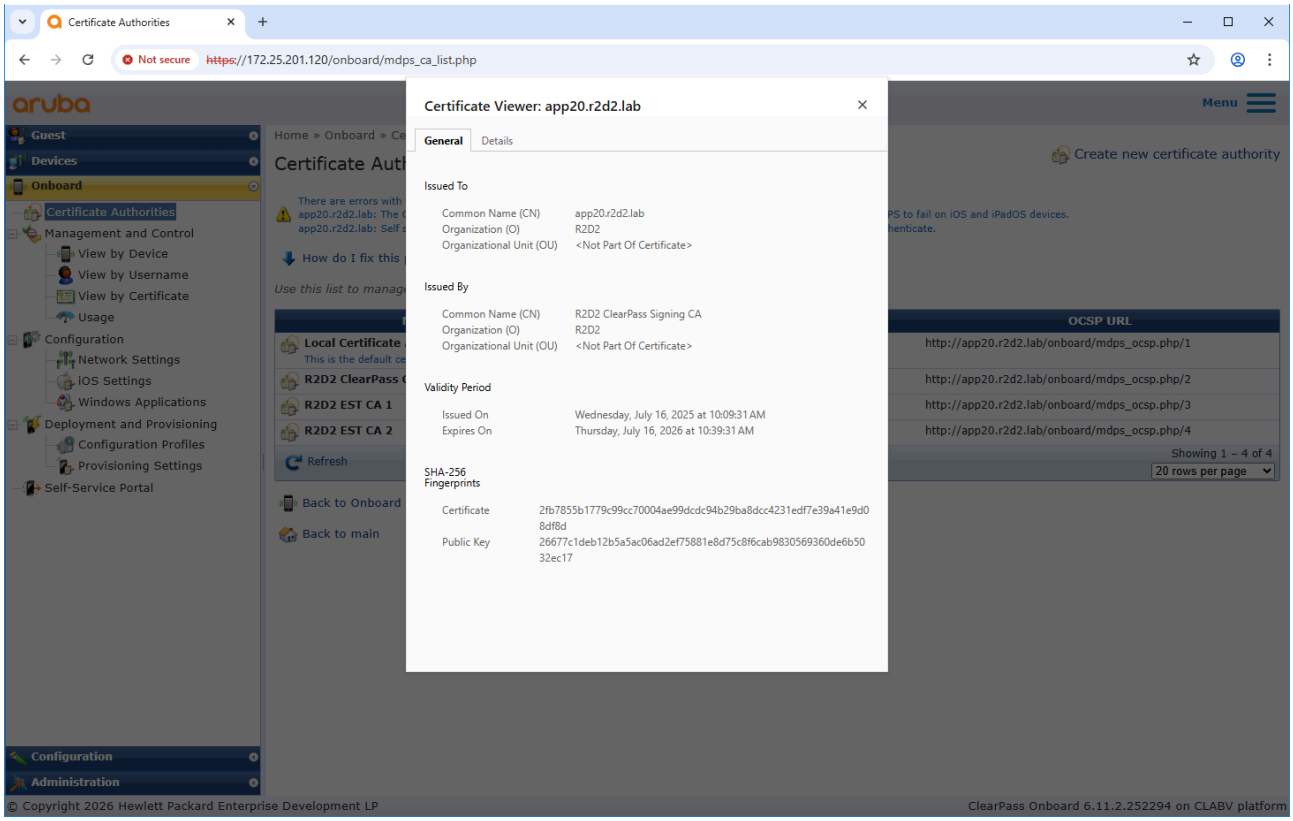
Configuração Axis

A configuração no dispositivo Axis é realizada em duas etapas.

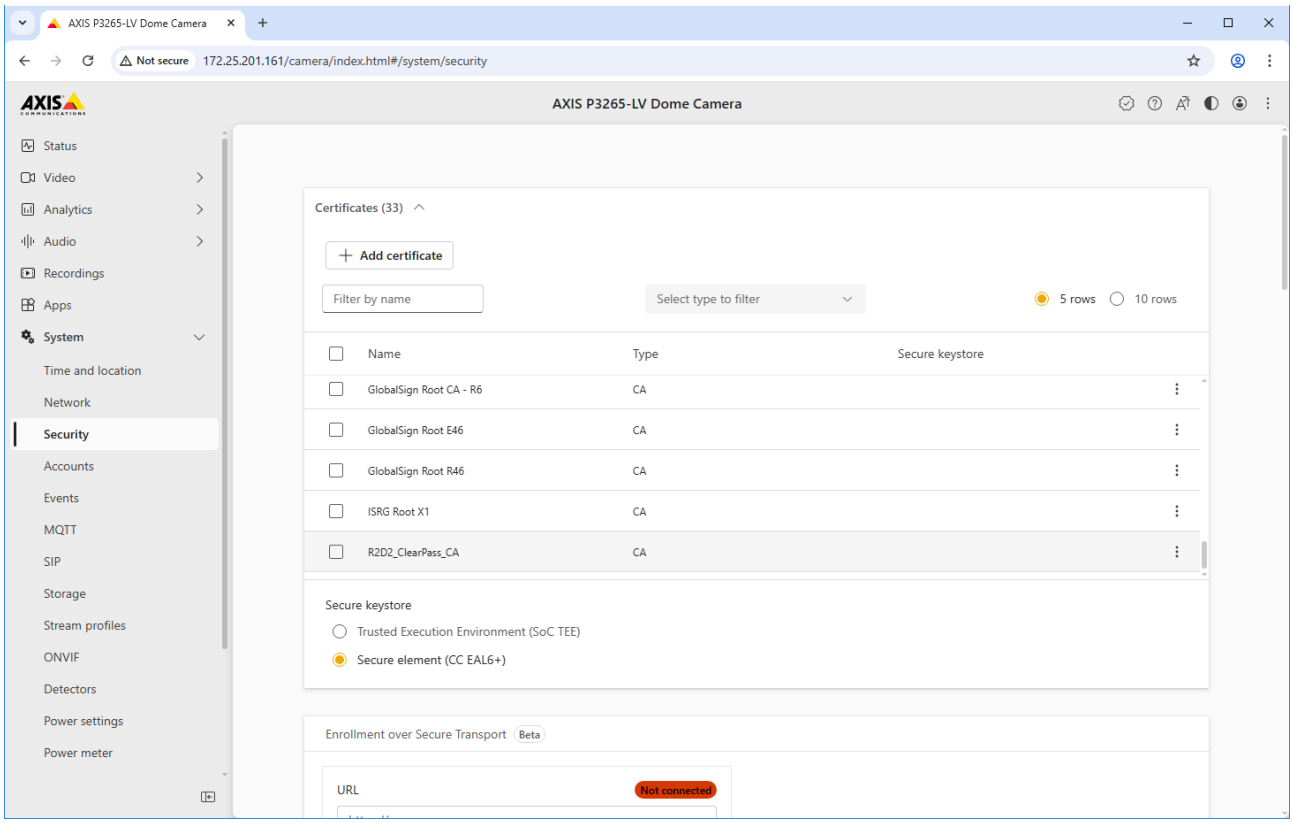
1. Estabeleça confiança com o ponto de extremidade HTTPS do ClearPass Onboard.

2. Configure o cliente EST no dispositivo Axis.

Configuração de certificado confiável

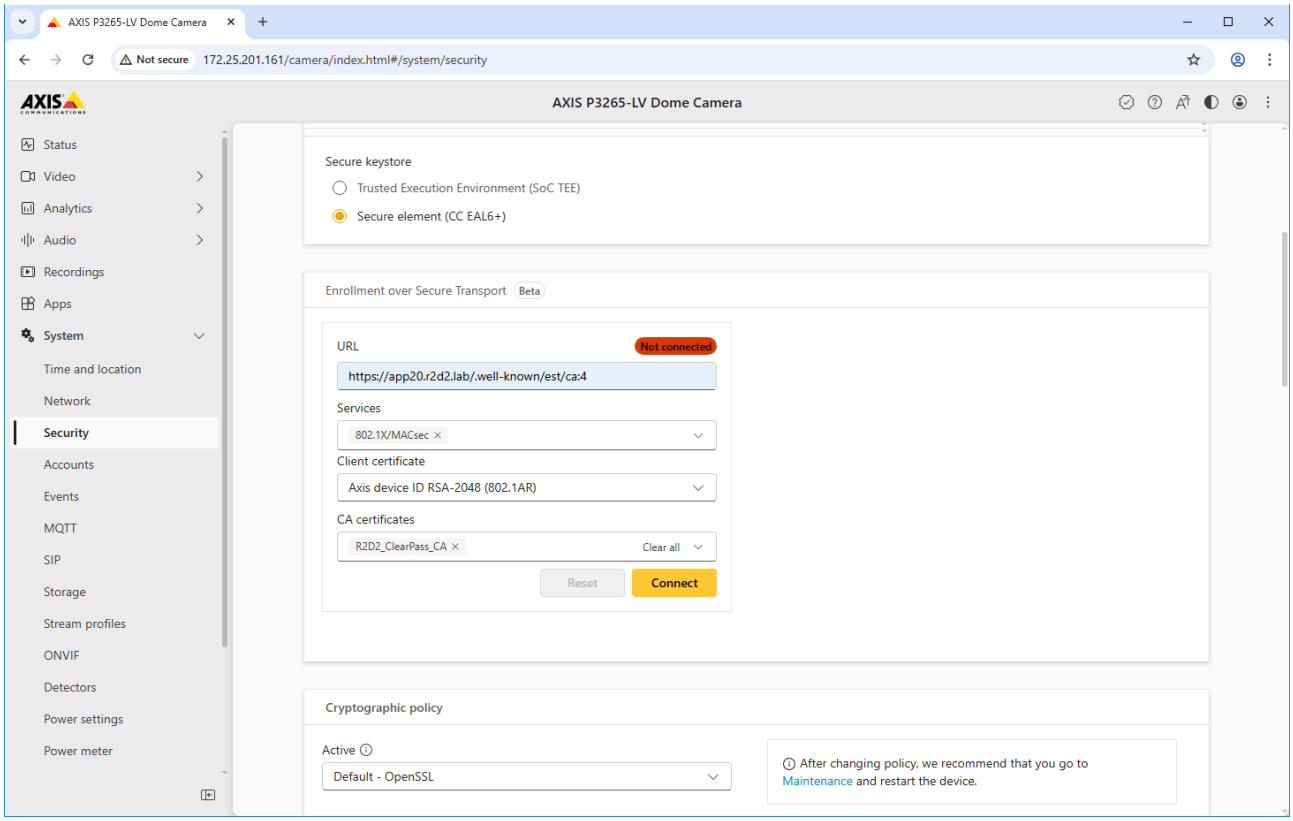


Verifique a cadeia de certificados do ponto de extremidade HTTPS do ClearPass Onboard.

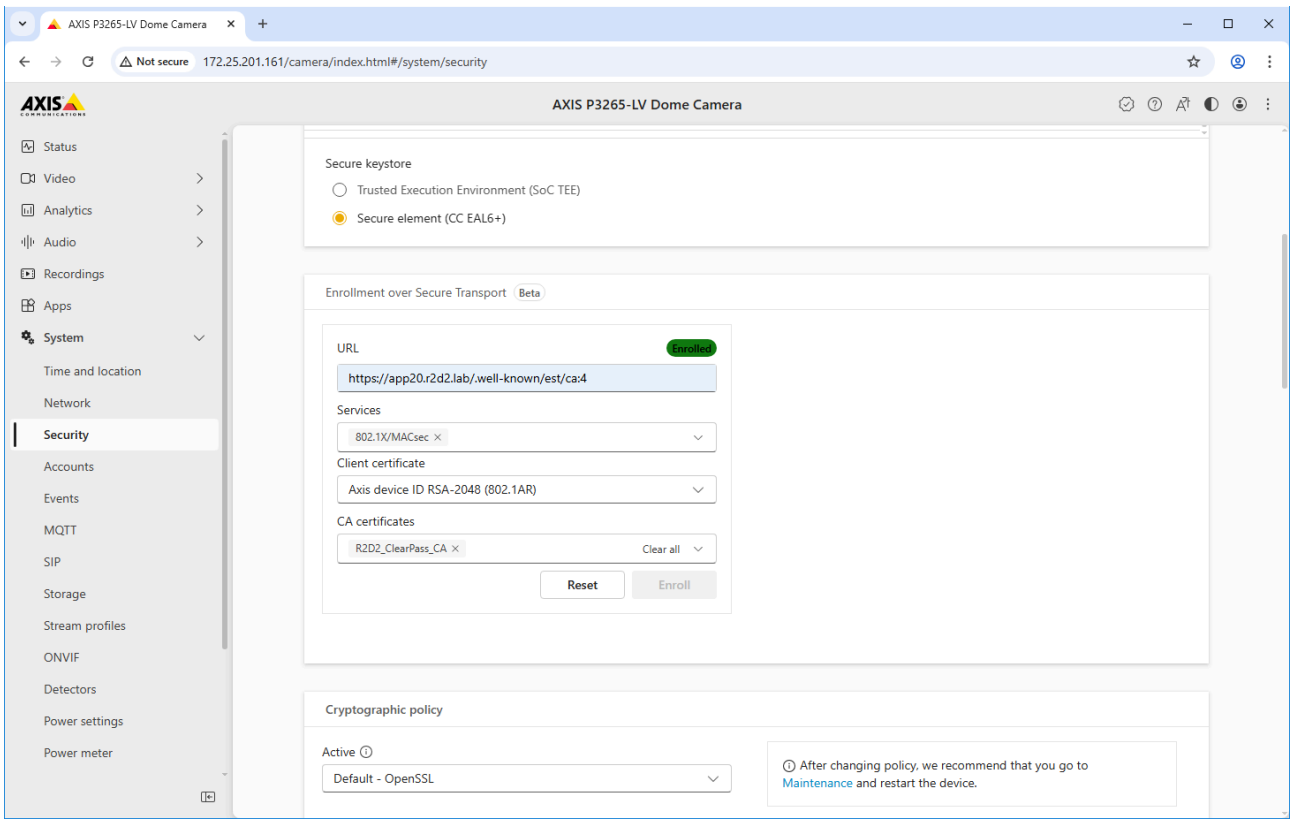


Carregue a CA do ponto de extremidade HTTPS do ClearPass Onboard para o dispositivo Axis.

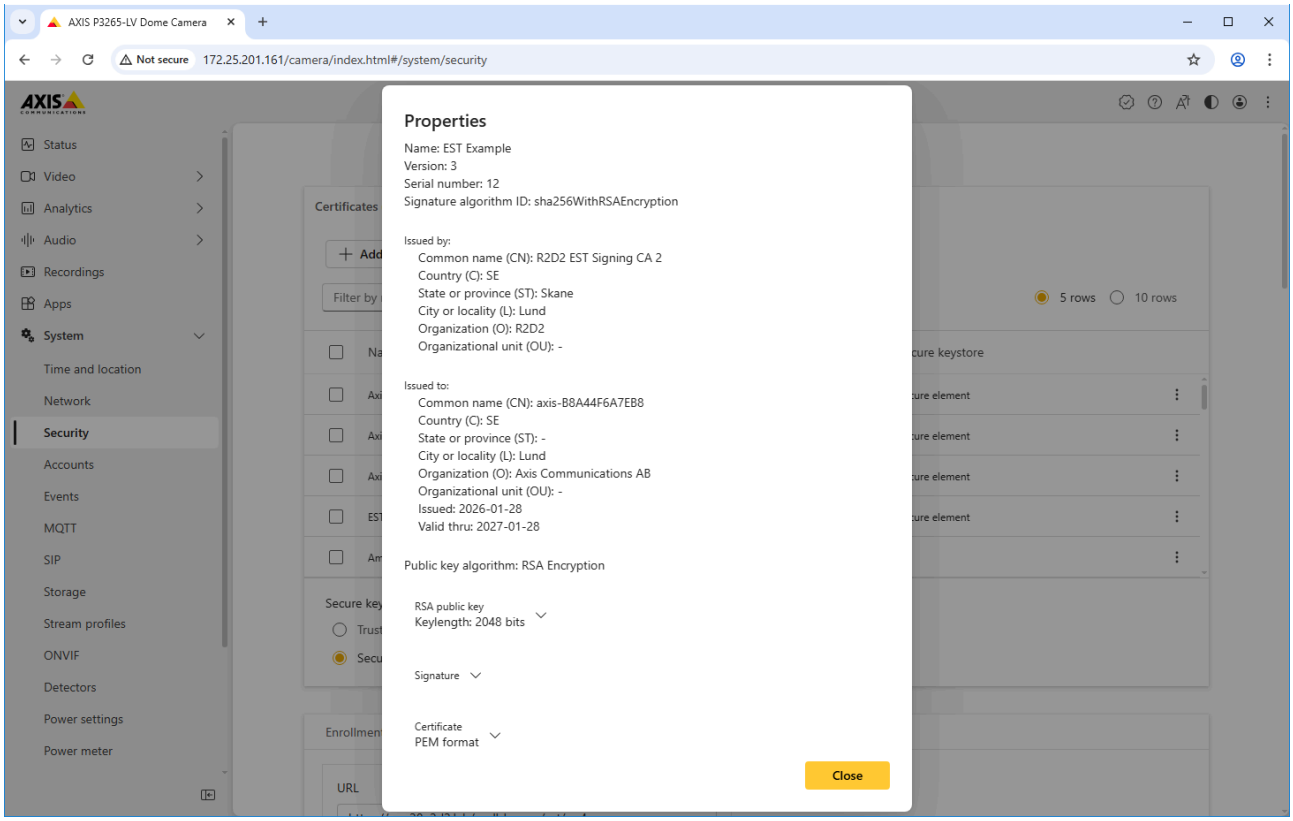
Configuração do cliente EST



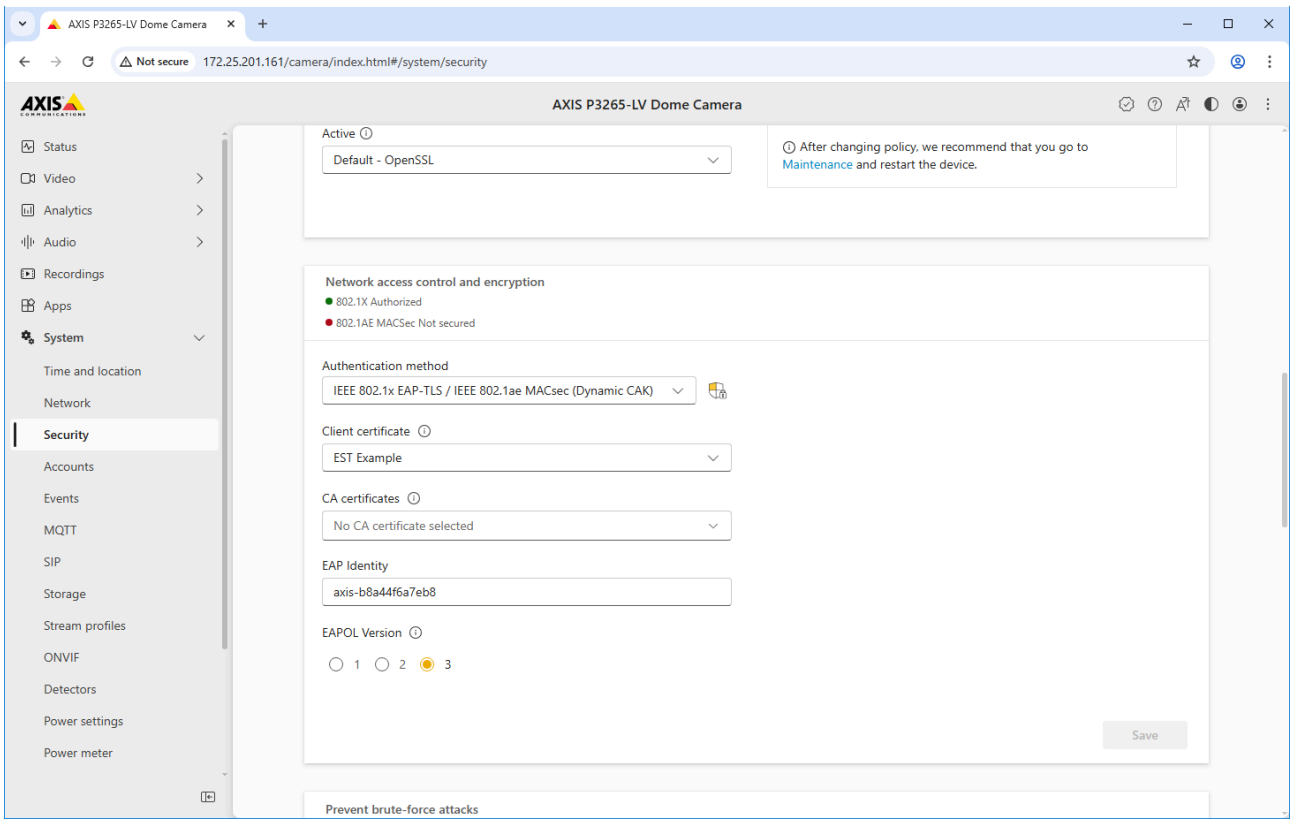
Parâmetro	Valor
URL	A URL do EST pode ser encontrada na autoridade certificadora criada para o EST no ClearPass Onboard.
Serviços	Selecione os serviços que devem ser configurados automaticamente com o certificado registrado.
Certificado de cliente	Selecione um certificado de cliente para a autenticação no servidor EST do ClearPass Onboard. Os dispositivos com o ID do dispositivo Axis são automaticamente considerados confiáveis para registro, uma vez que a cadeia de certificados IEEE 802.1AR específica da Axis foi adicionada ao armazenamento de certificados confiáveis no ClearPass Policy Manager.
CA certificates (Certificados CA):	Selecione o certificado CA do ponto de extremidade HTTPS do ClearPass Onboard para que o dispositivo Axis confie nesse ponto de extremidade.



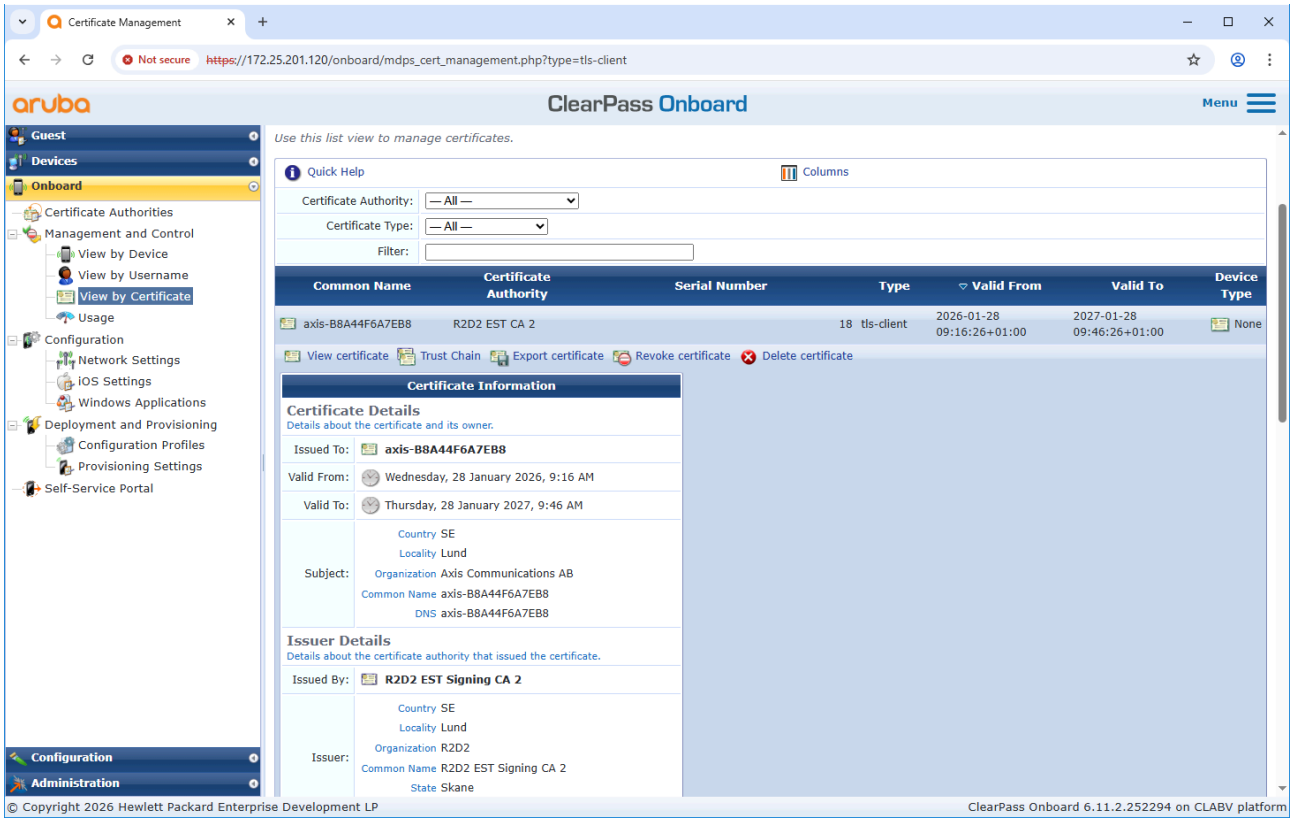
O registro foi bem-sucedido.



O certificado EST registrado no dispositivo Axis.



O certificado registrado é automaticamente atribuído ao serviço selecionado anteriormente.



Você também pode revisar o certificado registrado no ClearPass Onboard.

Integração legada – Autenticação MAC

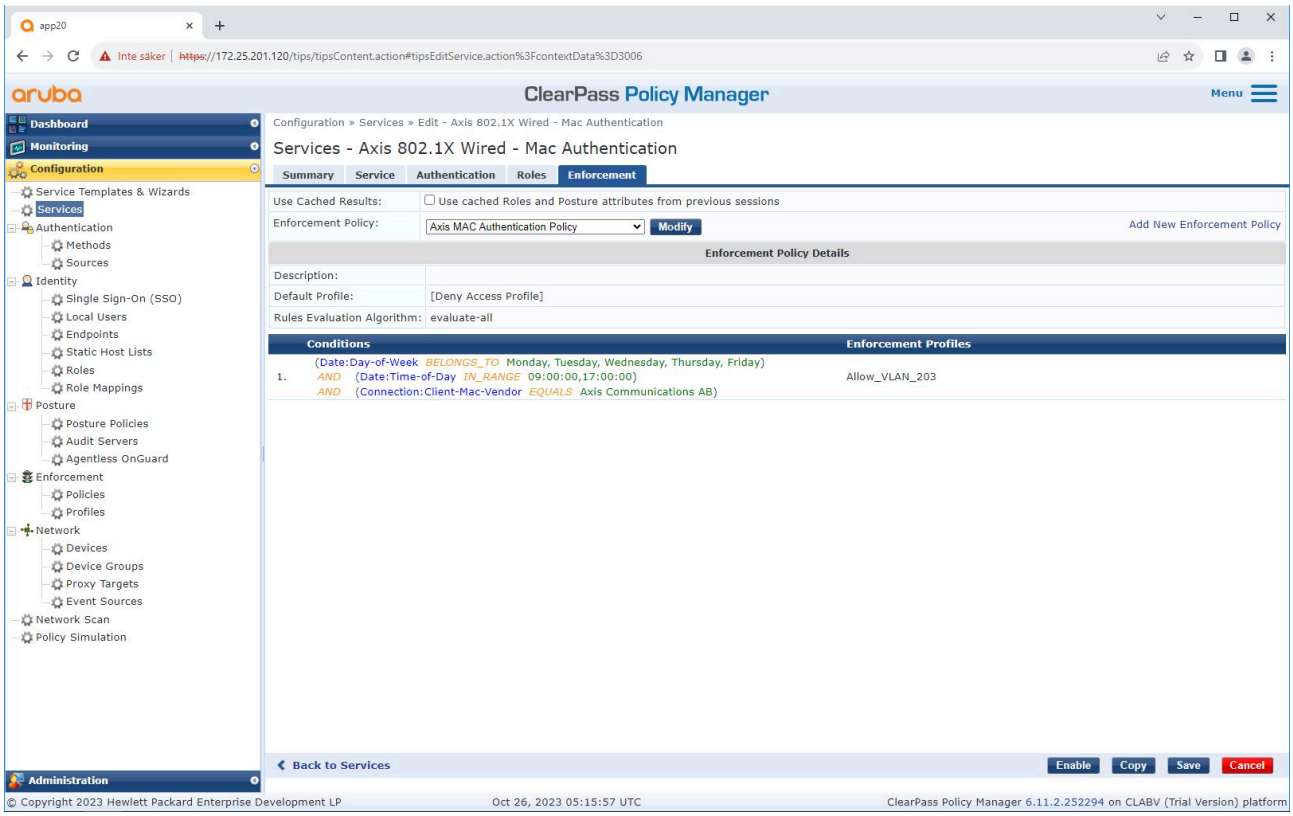
Você pode usar o MAC Authentication Bypass (MAB) para integrar dispositivos Axis que não são compatíveis com a integração IEEE 802.1AR com o certificado de ID do dispositivo Axis e IEEE802.1X habilitado no estado padrão de fábrica. Se a integração do 802.1X falhar, o ClearPass Policy Manager validará 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. Não é necessária nenhuma configuração no dispositivo Axis para permitir o MAB para integração.

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

Se o dispositivo Axis não atender à política de imposição configurada, o acesso à rede é negado.

Rede de convidados (VLAN 203)

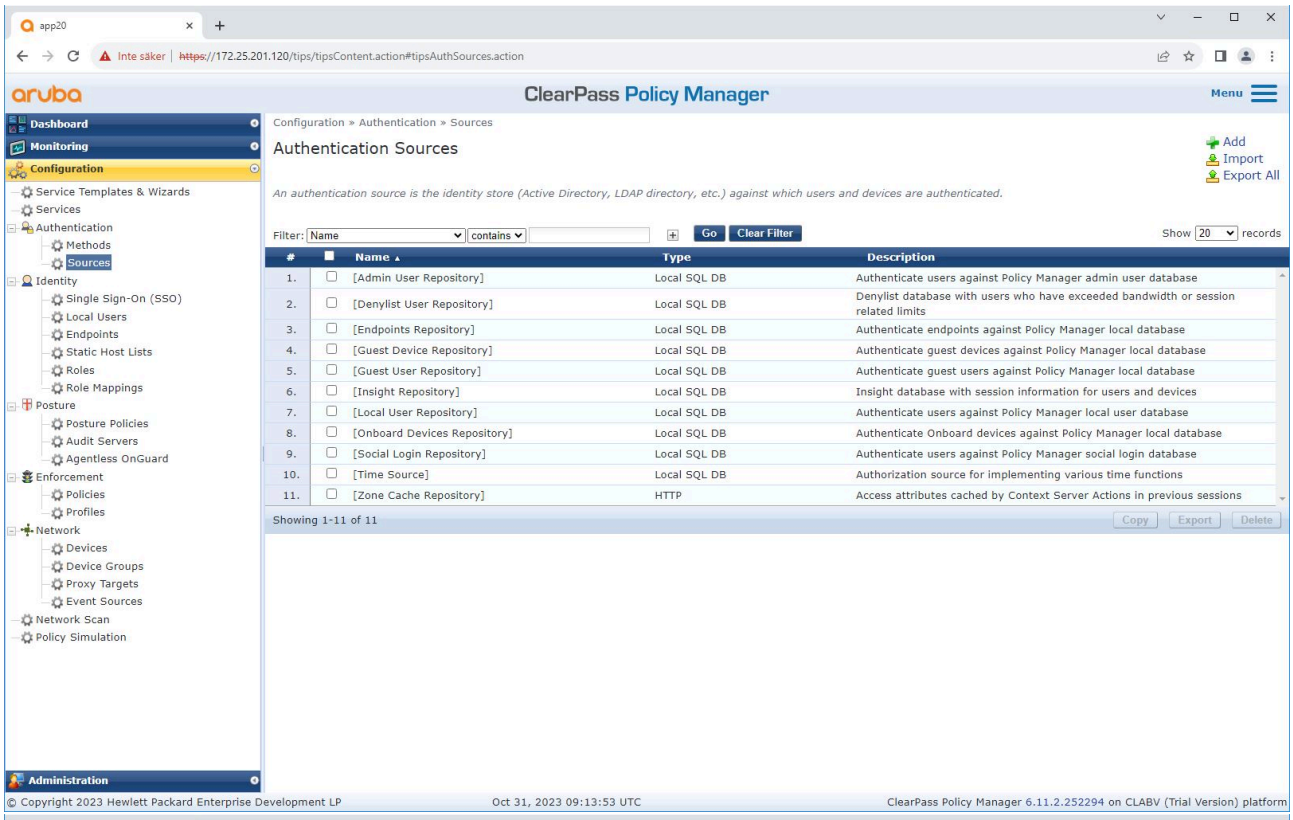
O dispositivo Axis terá acesso a uma rede limitada e isolada se as seguintes condições forem atendidas:

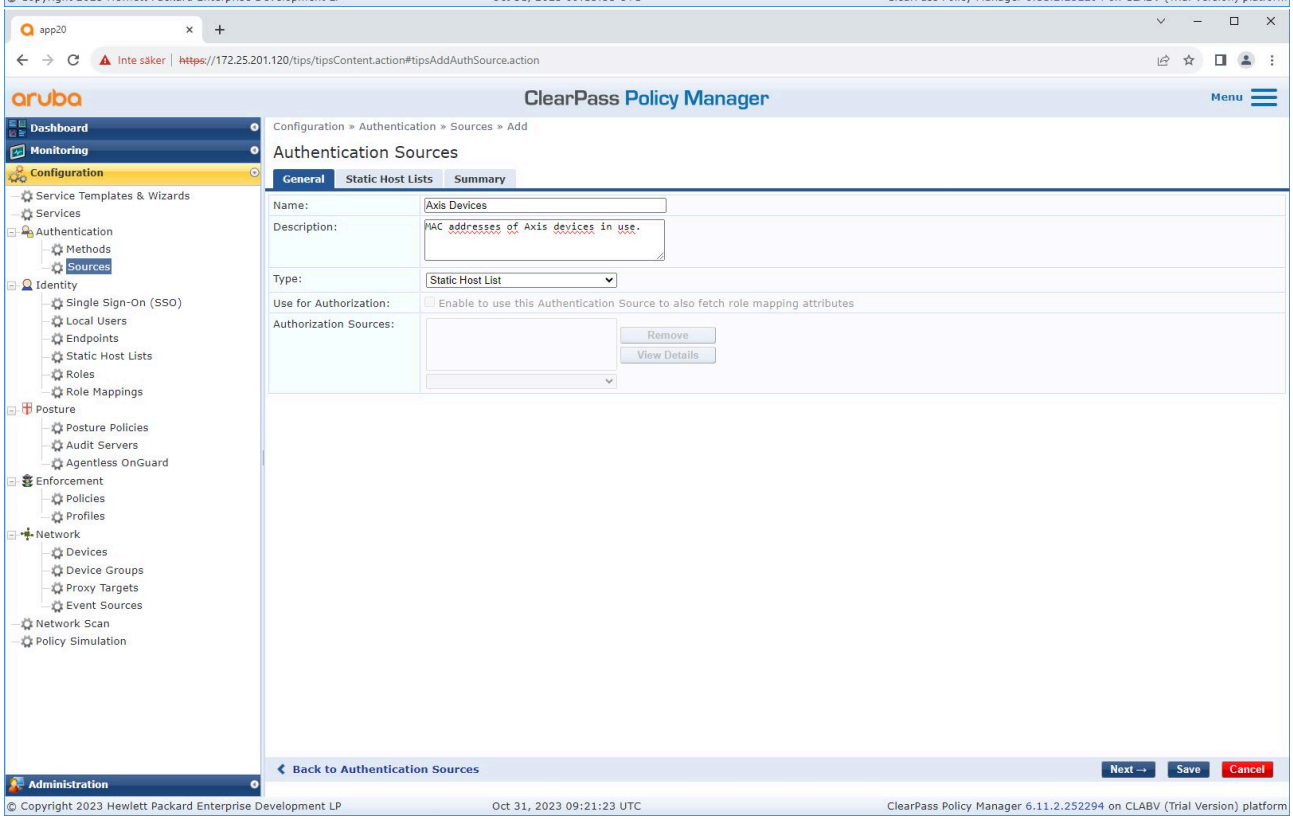
- O dia é um dia da semana, de segunda a sexta-feira.
- A hora é das 09:00 às 17:00.
- O fornecedor do endereço MAC corresponde à Axis Communications.

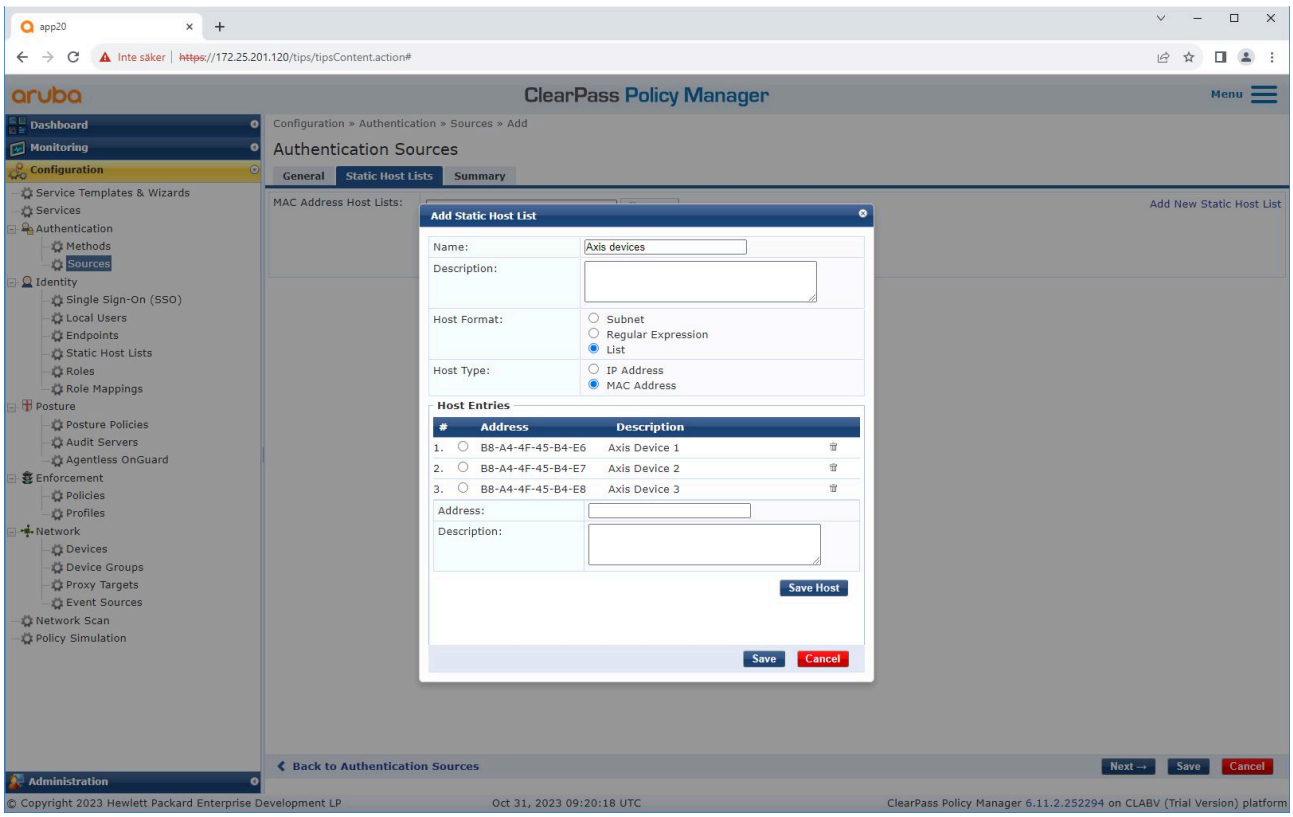
Como é possível falsificar endereços MAC, o acesso à rede de provisionamento regular não é concedido. Recomendamos usar o MAB apenas para a integração inicial e para inspecionar manualmente o dispositivo em mais detalhes.

Configuração da origem

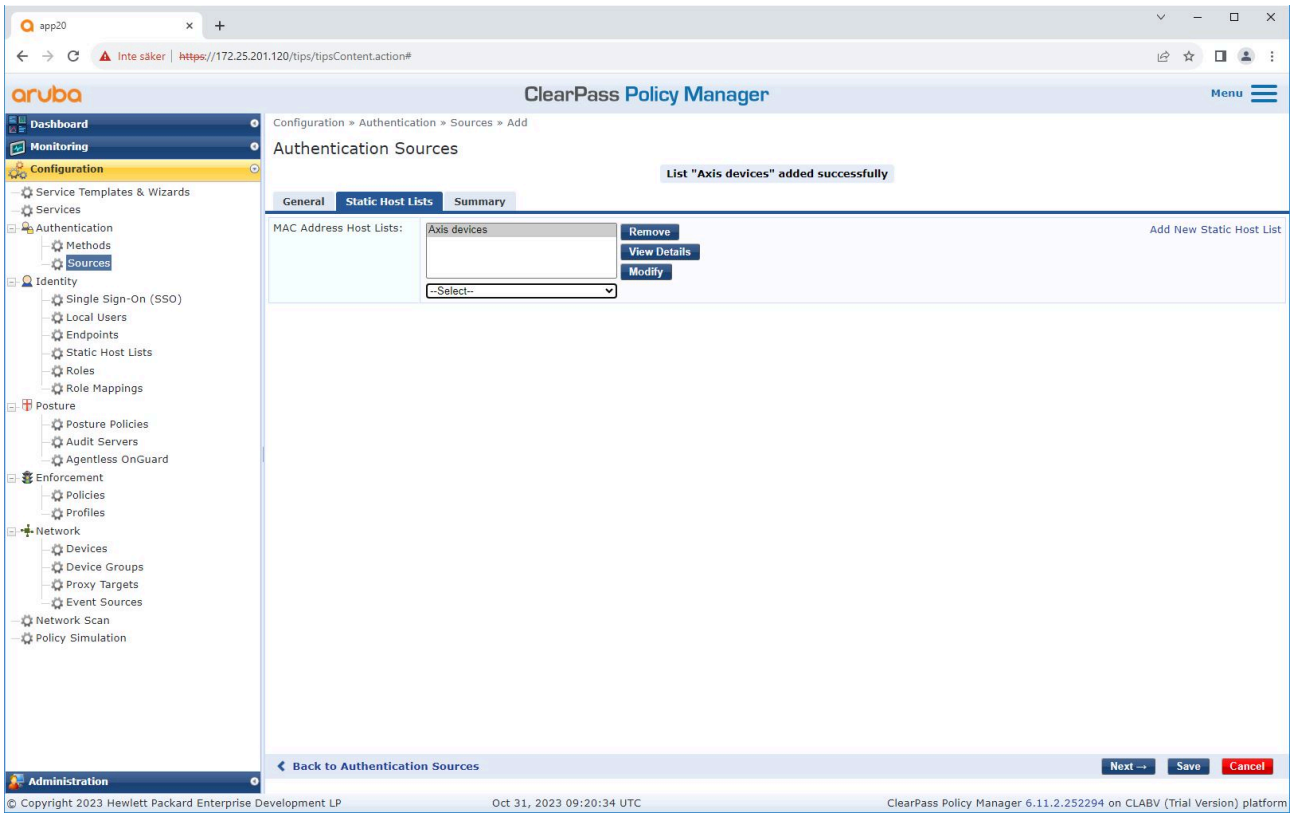
Na página **Sources (Fontes)**, uma nova fonte de autenticação é criada para permitir apenas endereços MAC importados manualmente.





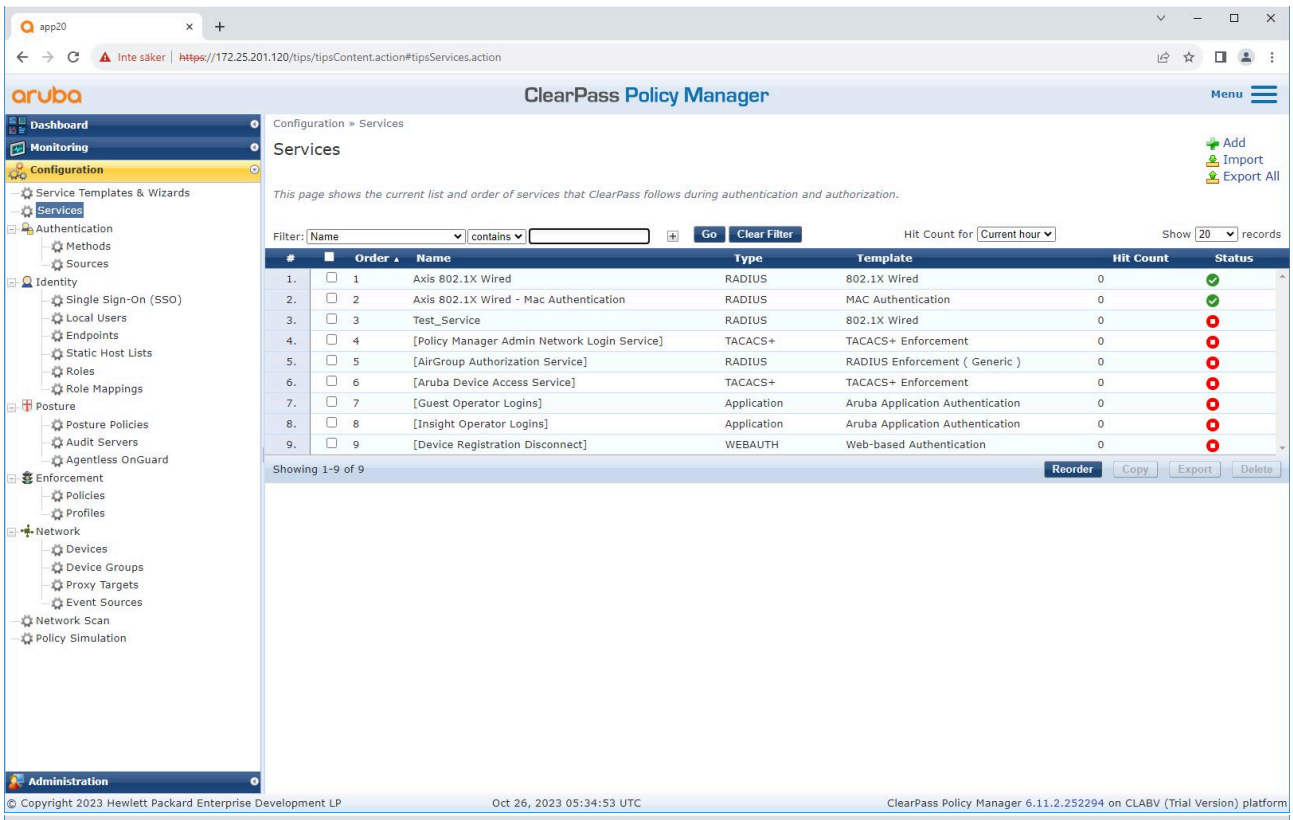


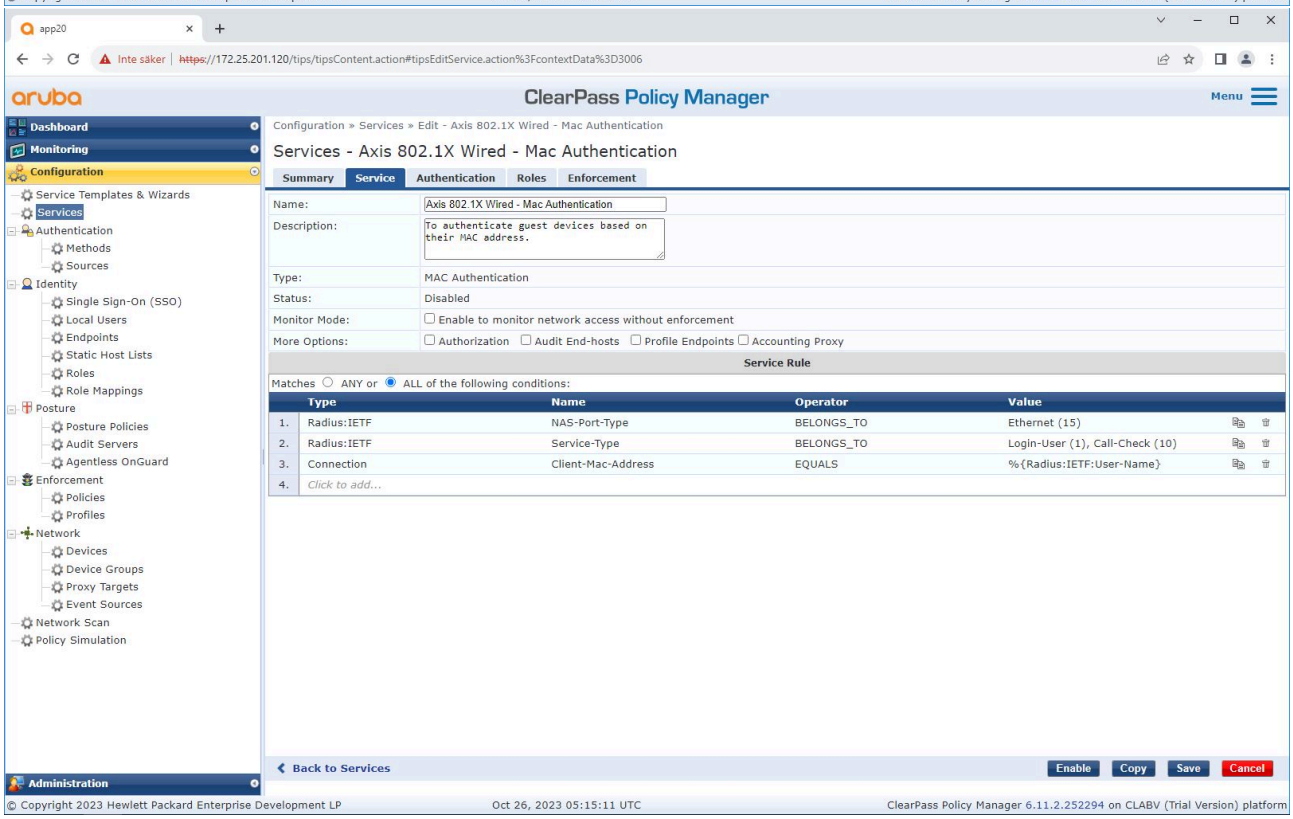
Uma lista de hosts estáticos, que contém endereços MAC da Axis, é criada.



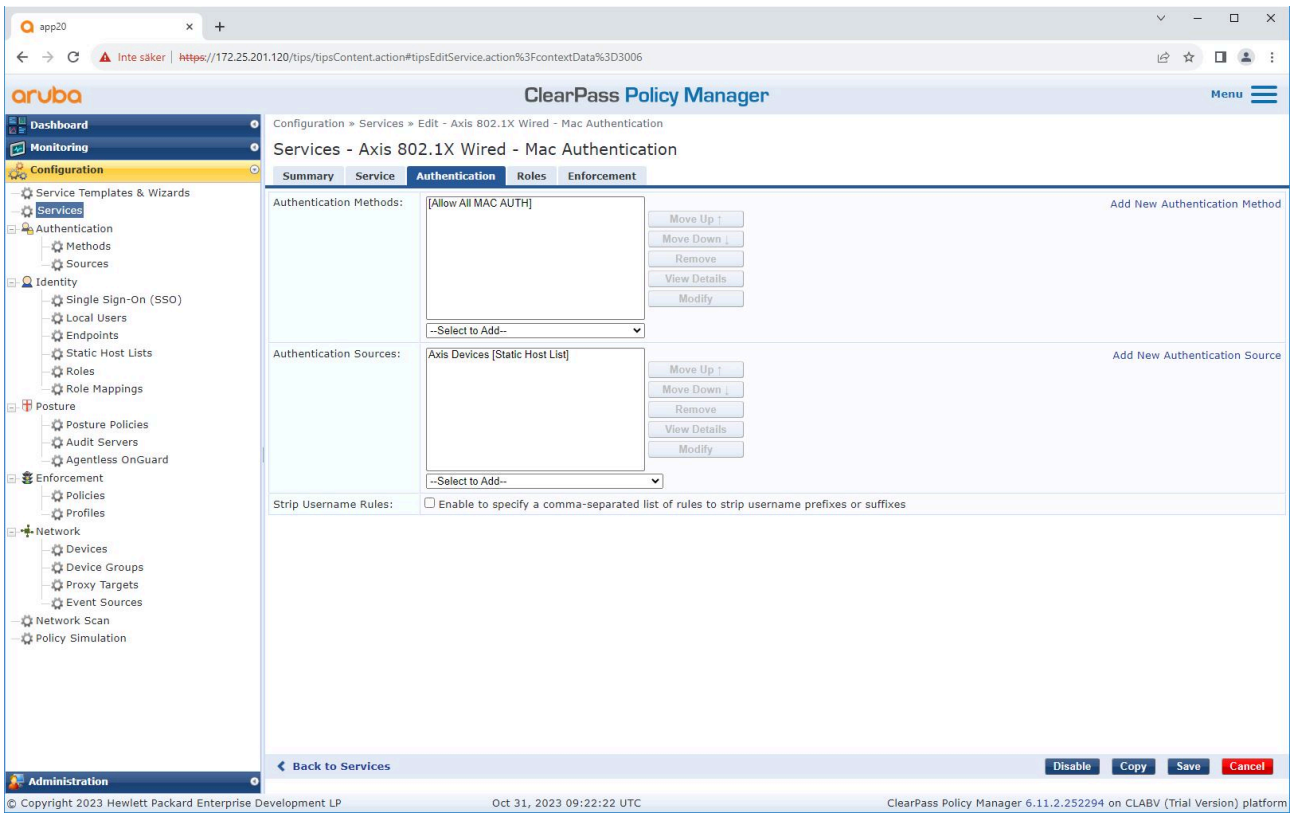
Configuração do serviço

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 HPE Aruba Networking.





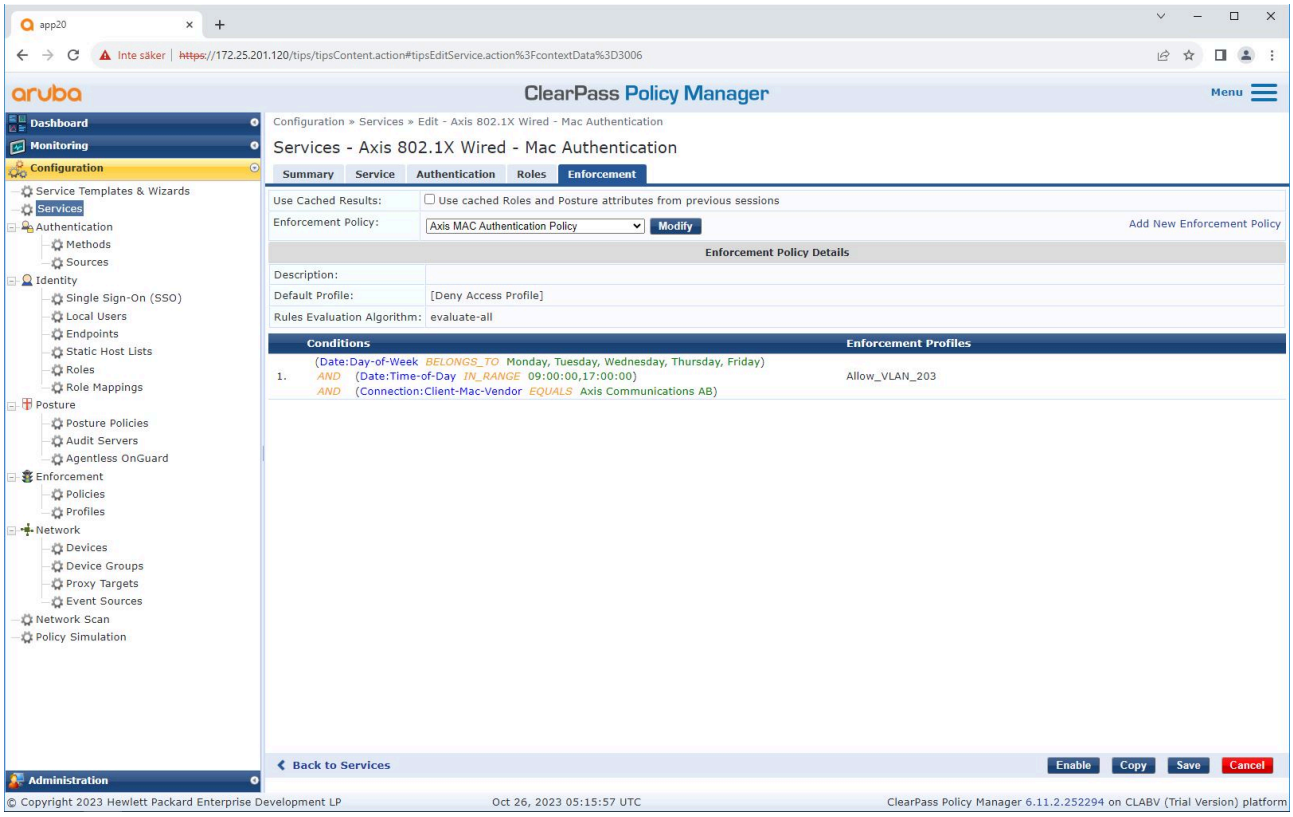
Um serviço Axis dedicado que define o MAB como um método de conexão é criado.



O método de autenticação MAC pré-configurado é configurado para o serviço. Além disso, a fonte de autenticação (criada anteriormente) contendo uma lista de endereços MAC do 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 aplicação criada anteriormente é configurada para o serviço.

Switch de acesso do HPE Aruba Networking

Além da configuração de integração segura descrita em *Switch de acesso do HPE Aruba Networking, on page 15*, veja abaixo o exemplo de configuração de porta do switch de acesso HPE Aruba Networking para permitir MAB.

```
aaa port-access authenticator 18 tx-period 5aaa port-access authenticator 19 tx-period 5aaa
port-access authenticator 18 max-requests 3aaa port-access authenticator 19 max-requests 3aaa
port-access authenticator 18 client-limit 1aaa port-access authenticator 19 client-limit 1aaa
port-access mac-based 18-19aaa port-access 18 auth-order authenticator mac-basedaaa port-
-access 19 auth-order authenticator mac-basedaaa port-access 18 auth-priority authenticator
mac-basedaaa port-access 19 auth-priority authenticator mac-based
```

T10197992_pt

2026-02 (M8.3)

© 2023 – 2026 Axis Communications AB