

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
Integração legada – Autenticação MAC.....	23
ClearPass Policy Manager do HPE Aruba Networking.....	23
Política de imposição	23
Configuração da origem	24
Configuração do serviço	25
Switch de acesso do HPE Aruba Networking.....	28

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.

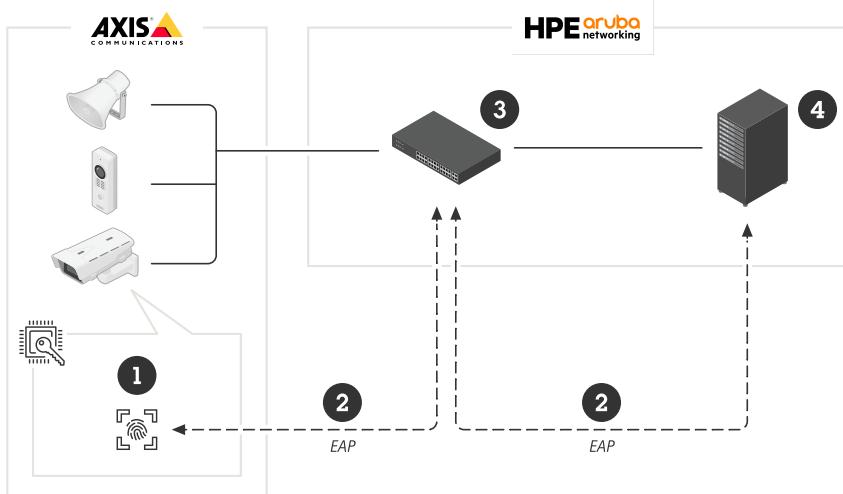
Integração segura de dispositivo em redes de confiança zero com IEEE 802.1X/802.1AR

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.

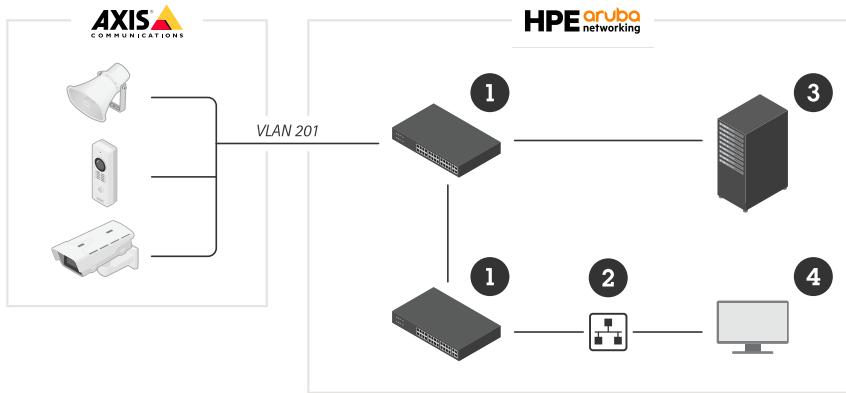


O dispositivo Axis é autenticado na rede HPE Aruba Networking usando o certificado de ID do dispositivo Axis compatível com IEEE 802.1AR.

- 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.

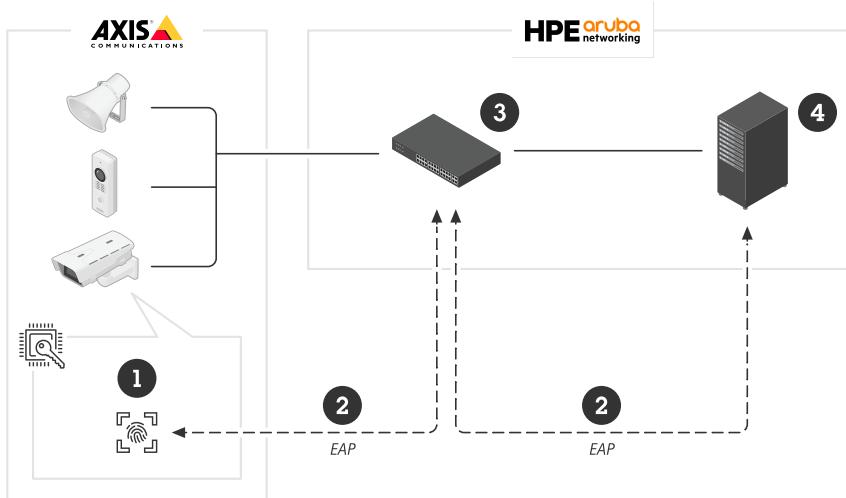


Após a autenticação bem-sucedida, o dispositivo Axis passa para uma rede de provisionamento para configuração.

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

Rede de produção

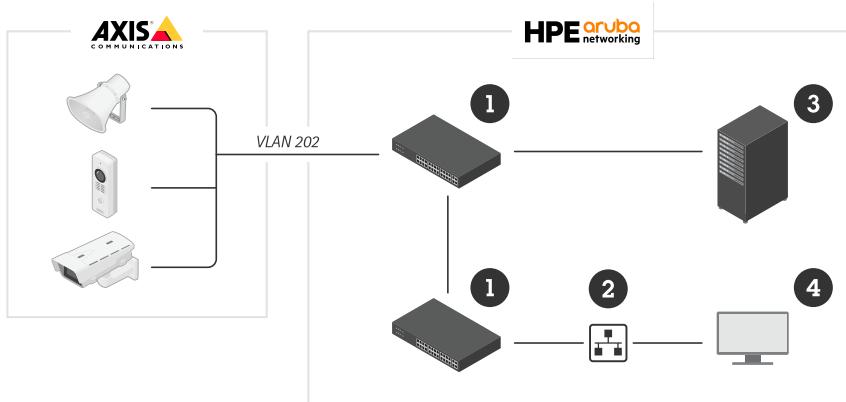
O provisionamento do dispositivo Axis com novos certificados IEEE 802.1X aciona uma nova tentativa de autenticação. O ClearPass Policy Manager verifica os novos certificados e decide se o dispositivo Axis será ou não movido para a rede de produção.



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.

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

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

ClearPass Policy Manager - Aruba

Administration > Certificates > Trust List

Certificate Trust List

This page displays a list of trusted Certificate Authorities (CA). You can add, view, or delete a certificate.

Filter: Subject contains axis device

#	Subject	Usage	Validity	Enabled
1.	CN=Axis device ID Root CA RSA,0=Axis Communications AB	EAP	Valid	Enabled
2.	CN=Axis device ID Root CA ECC,0=Axis Communications AB	EAP	Valid	Enabled
3.	CN=Axis device ID Intermediate CA RSA 2,0=Axis Communications AB	EAP	Valid	Enabled
4.	CN=Axis device ID Intermediate CA RSA 1,0=Axis Communications AB	EAP	Valid	Enabled
5.	CN=Axis device ID Intermediate CA ECC 2,0=Axis Communications AB	EAP	Valid	Enabled
6.	CN=Axis device ID Intermediate CA ECC 1,0=Axis Communications AB	EAP	Valid	Enabled

Showing 1-6 of 6

Copyright 2022 Hewlett Packard Enterprise Development LP Nov 25, 2022 08:48:50 CET ClearPass Policy Manager 6.9.12.136929 on CLABV (Trial Version) platform

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.

ClearPass Policy Manager - Aruba

Configuration > Network > Devices

Network Devices

A Network Access Device (NAD) must belong to the global list of devices in the ClearPass database in order to connect to ClearPass.

Filter: Name contains

#	Name	IP or Subnet Address	Device Groups	Description

Copy | Export | Delete

Copyright 2022 Hewlett Packard Enterprise Development LP Dec 28, 2022 09:01:17 CET ClearPass Policy Manager 6.9.12.136929 on CLABV (Trial Version) platform

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

ClearPass Policy Manager

Add Device

Device

Name: SW04

IP or Subnet Address: 172.25.200.13

Description:

RADIUS Shared Secret: Verify:

TACACS+ Shared Secret: Verify:

Vendor Name: Aruba

Enable RADIUS Dynamic Authorization:

Enable RadSec:

Add Cancel

ClearPass Policy Manager

Network Devices

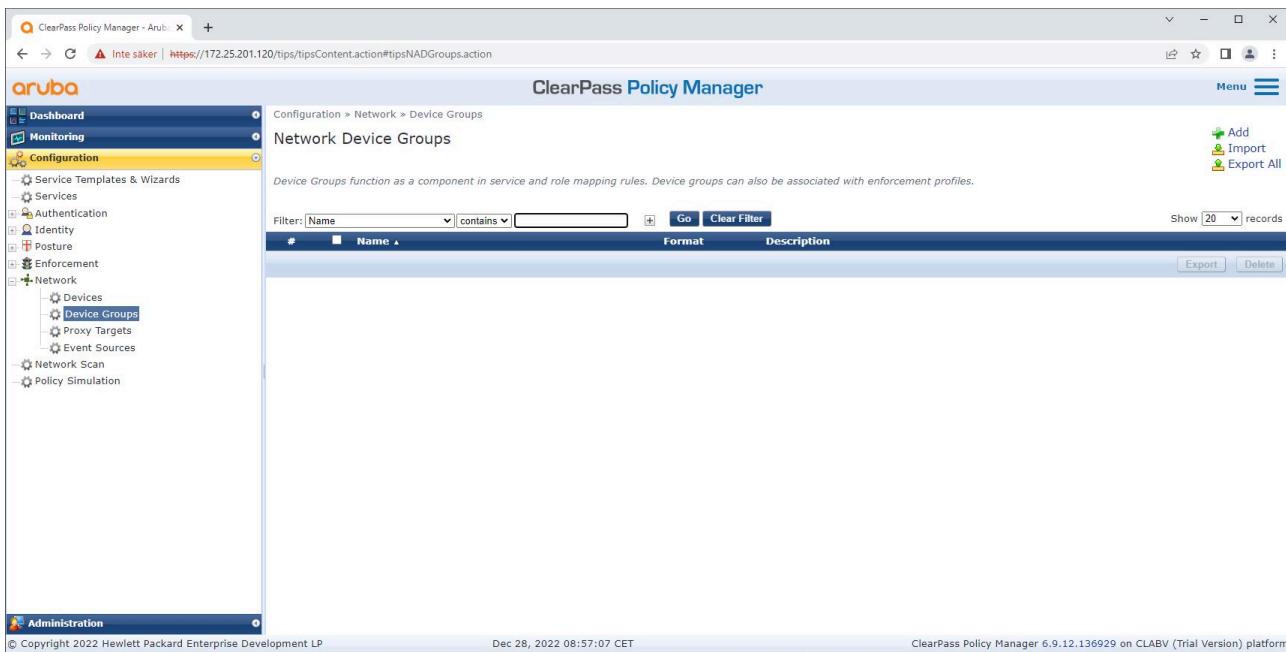
Device SW04 added

A Network Access Device (NAD) must belong to the global list of devices in the ClearPass database in order to connect to ClearPass.

#	Name	IP or Subnet Address	Device Groups	Description
1.	SW04	172.25.200.13	-	

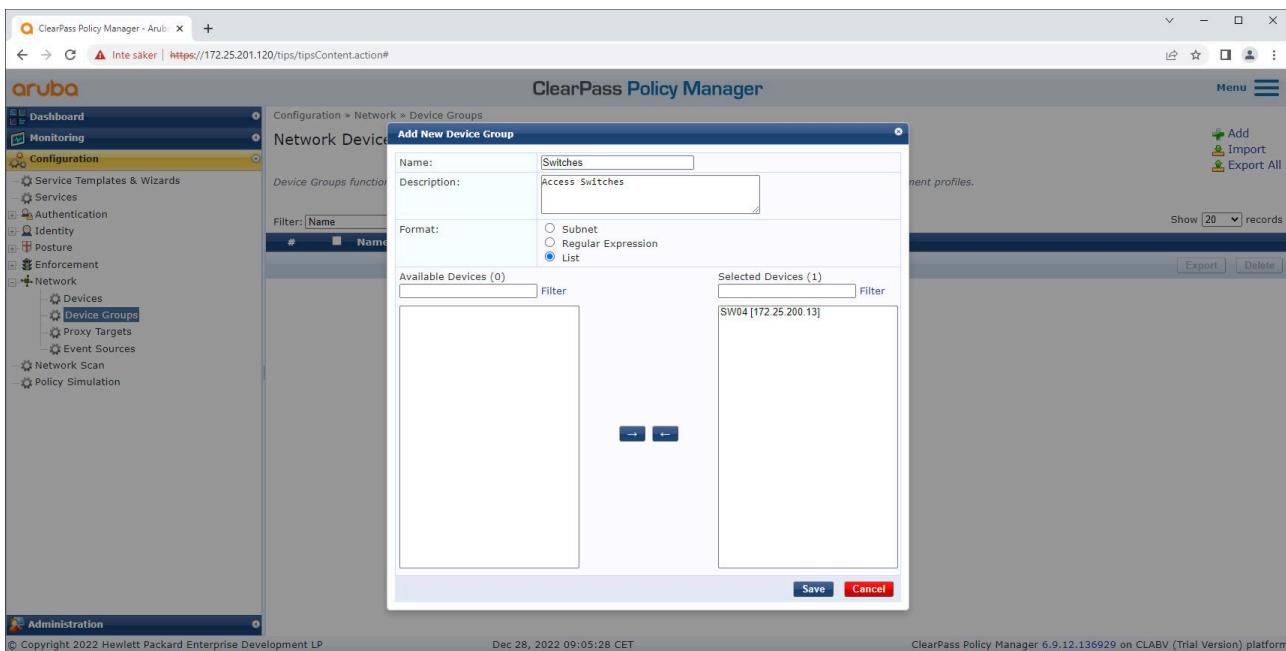
Showing 1-1 of 1

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



The screenshot shows the ClearPass Policy Manager interface. The left sidebar is titled 'aruba' and contains sections for Dashboard, Monitoring, Configuration, and Network. The Configuration section is expanded, showing Service Templates & Wizards, Services, Authentication, Identity, Posture, Enforcement, and Network. The Network section is further expanded to show Devices, Device Groups, Proxy Targets, and Event Sources. The main content area is titled 'Network Device Groups' and contains a table with columns for #, Name, Format, and Description. A filter bar at the top of the table allows searching by Name. A toolbar at the top right includes 'Add', 'Import', and 'Export All' buttons. The status bar at the bottom indicates the date and time as Dec 28, 2022 08:57:07 CET, and the software version as ClearPass Policy Manager 6.9.12.136929 on CLABV (Trial Version) platform.

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



The screenshot shows the 'Add New Device Group' dialog box. It has fields for 'Name' (set to 'Switches') and 'Description' (set to 'Access Switches'). The 'Format' section has three radio buttons: 'Subnet', 'Regular Expression', and 'List', with 'List' selected. Below these are two lists: 'Available Devices (0)' and 'Selected Devices (1)'. The 'Selected Devices' list contains one item: 'SW04 [172.25.200.13]'. At the bottom of the dialog are 'Save' and 'Cancel' buttons. The background shows the same ClearPass Policy Manager interface as the previous screenshot.

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.

The screenshot shows the 'Edit Endpoint' dialog for an Axis camera. The 'Endpoint' tab is selected, showing details such as CDP Device Description, DHCP Options, Host MAC Vendor, and SNMP Device Type. The 'Attributes' and 'Device Fingerprints' tabs are also visible. In the background, the main 'Endpoints' list shows four entries, all marked as 'Unknown' in the 'Status' column and 'Yes' in the 'Profiled' column. The interface is a web-based management tool for HPE Aruba Networking, specifically for managing endpoints and their profiles.

As impressões digitais detalhadas de um dispositivo Axis com perfil estabelecido. Observe que o SNMP está desativado 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 política que se aplica aos dispositivos de rede no grupo de dispositivos "Switches". O número necessário de perfis de imposição 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.

The screenshot shows the 'Edit Enforcement Profile' dialog for 'Allow_VLAN_201'. The 'Profile' tab is selected, showing the profile name 'Allow_VLAN_201', type 'RADIUS', action 'Accept', and device group list '1. Switches'. The 'Attributes' tab is selected, showing a table of attributes for Radius: IETF. The table includes columns for Type, Name, and Value, with entries for Session-Timeout, Termination-Action, Tunnel-Type, Tunnel-Medium-Type, and Tunnel-Private-Group-Id. The main pane shows a list of enforcement profiles. The interface is a web-based management tool for HPE Aruba Networking, specifically for managing enforcement profiles and their attributes.

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.

ClearPass Policy Manager - Aruba

Configuration > Services > Edit - Axis 802.1X Wired

Services - Axis 802.1X Wired

Summary Service Authentication Roles Enforcement

Authentication Methods: Axis EAP TLS

Authentication Sources: [Endpoints Repository] [Local SQL DB]

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

Service Certificate: -Select to Add-

Add New Authentication Method Add New Authentication Source View Certificate Details

Move Up ↑ Move Down ↓ Remove View Details Modify

Move Up ↑ Move Down ↓ Remove View Details Modify

Move Up ↑ Move Down ↓ Remove View Details Modify

Move Up ↑ Move Down ↓ Remove View Details Modify

Back to Services

Disable Copy Save Cancel

Administration

© Copyright 2022 Hewlett Packard Enterprise Development LP Dec 28, 2022 09:41:41 CET ClearPass Policy Manager 6.9.12.136929 on CLABV (Trial Version) platform

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

ClearPass Policy Manager - Aruba

Configuration > Services > Edit - Axis 802.1X Wired

Services - Axis 802.1X Wired

Summary Service Authentication Roles Enforcement

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

Enforcement Policy: Axis Radius policy

Add New Enforcement Policy

Enforcement Policy Details

Description:

Default Profile: Allow_VLAN_203

Rules Evaluation Algorithm: first-applicable

Conditions	Enforcement Profiles
$(\text{Certificate:Issuer-CN} \text{ CONTAINS} \text{ Axis device ID Intermediate CA})$ AND $(\text{Certificate:Issuer-O} \text{ EQUALS} \text{ Axis Communications AB})$ AND $(\text{Certificate:Subject-O} \text{ EQUALS} \text{ Axis Communications AB})$ AND $(\text{Certificate:Subject-L} \text{ EQUALS} \text{ Lund})$ AND $(\text{Certificate:Subject-C} \text{ EQUALS} \text{ SE})$ AND $(\text{Connection:Client-Mac-Address-NoDelim} \text{ EQUALS} \%(\text{Certificate:Subject-serialNumber}))$ $(\text{Certificate:Issuer-CN} \text{ CONTAINS} \text{ Production CA Certificate})$ AND $(\text{Certificate:Subject-CN} \text{ CONTAINS} \%(\text{Connection:Client-Mac-Address-NoDelim}))$ AND $(\text{Authorization:[Endpoints Repository]:Device Name EQUALS} \text{ AXIS OS version unsupported})$ $(\text{Certificate:Issuer-CN} \text{ CONTAINS} \text{ Production CA certificate})$ AND $(\text{Certificate:Subject-CN} \text{ CONTAINS} \%(\text{Connection:Client-Mac-Address-NoDelim}))$ AND $(\text{Authorization:[Endpoints Repository]:Device Name EQUALS} \text{ AXIS OS version supported})$	Allow_VLAN_201 Allow_VLAN_201 Allow_VLAN_202

Back to Services

Disable Copy Save Cancel

Administration

© Copyright 2022 Hewlett Packard Enterprise Development LP Dec 28, 2022 09:51:01 CET ClearPass Policy Manager 6.9.12.136929 on CLABV (Trial Version) platform

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.

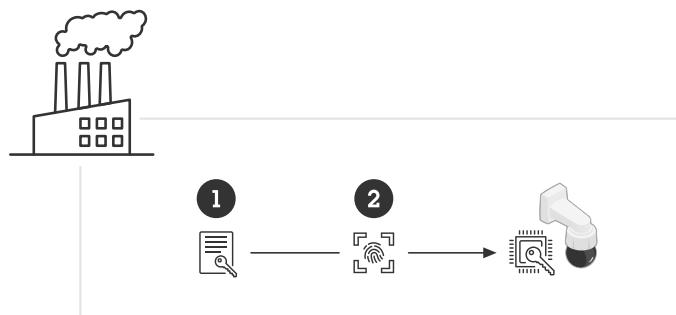
```
radius-server host MyRADIUSIPAddress key "MyRADIUSKey"
```

```
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.

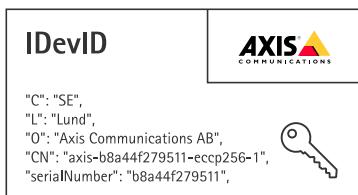
Observação

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

Name	Type
Axis device ID ECC-P256 (802.1AR)	Client-server
Axis device ID RSA-2048 (802.1AR)	Client-server
Axis device ID RSA-4096 (802.1AR)	Client-server
Axis device ID Intermediate CA ECC 2	CA

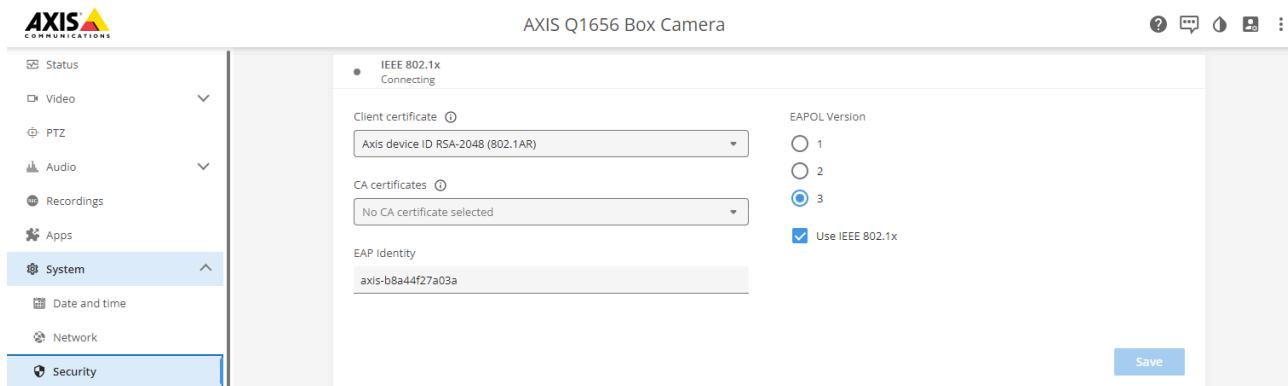
O armazenamento de certificados do dispositivo Axis no estado padrão de fábrica com a ID de dispositivo Axis.

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 utilizados na rede para configurar e gerenciar vários dispositivos Axis de maneira econômica. O AXIS Device Manager é um aplicativo baseado no Microsoft Windows® que é instalado localmente em um computador na rede, enquanto o AXIS Device Manager Extend depende da infraestrutura em nuvem para realizar o gerenciamento de dispositivos em vários sites. 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



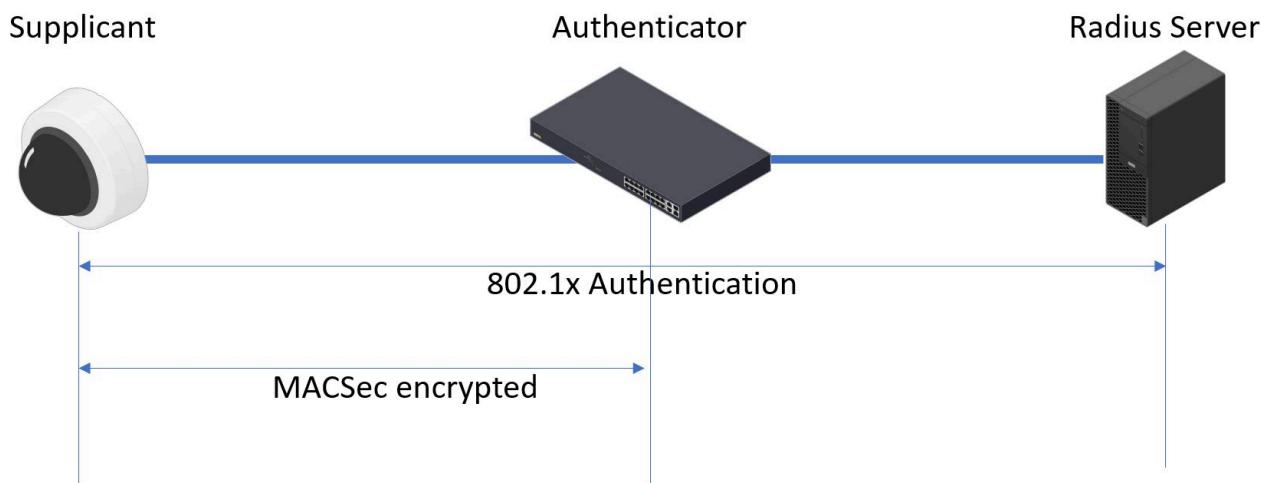
Para assistir a este vídeo, vá para a versão Web deste documento.

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

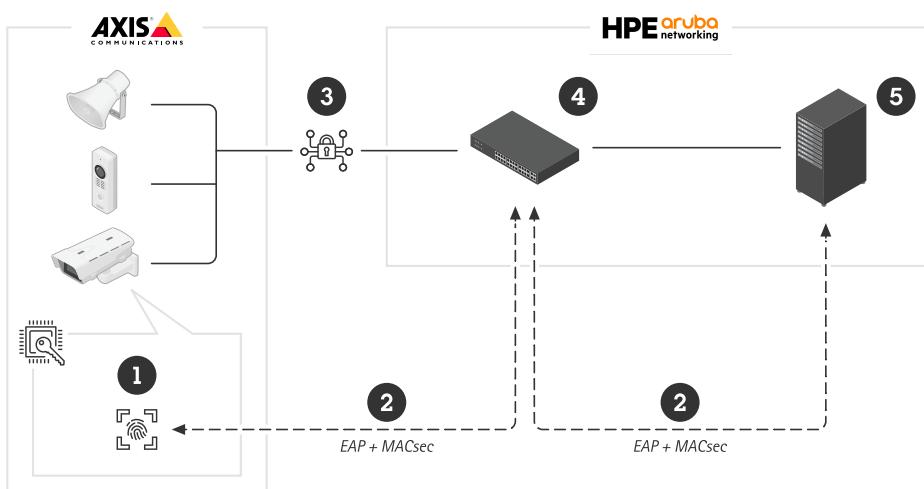
O IEEE 802.1AE MACsec (Media Access Control Security) é um protocolo de rede bem definido que protege criptograficamente links Ethernet ponto a ponto na camada de rede 2. Ele garante a confidencialidade e integridade das transmissões de dados entre dois hosts.

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 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

The screenshot shows the ClearPass Policy Manager interface with the following details:

- Left Sidebar:** Shows the navigation menu with sections like Dashboard, Monitoring, Configuration, Identity, Posture, Enforcement, Network, and Administration.
- Header:** Shows the URL <https://172.25.201.120/tips/tipsContent.action#tipsRoles.action>.
- Central Content:**
 - Section Title:** Configuration > Identity > Roles
 - Description:** Roles exist independently of an individual service and can be accessed globally through the role-mapping policy of any service.
 - Table:** A list of 20 roles, including [AirGroup v1], [AirGroup v2], [Aruba TACACS+ read-only Admin], [Aruba TACACS+ root Admin], AxisDevice, [BYOD O], [Contractor], [Device I], [Employee], [Guest], [MAC Ca], [Onboard], [Onboard], [Onboard iOS], [Onboard iPadOS], [Onboard Linux], [Onboard macOS], [Onboard Windows], [Other], and [TACACS+ API Admin].
 - Dialog Box:** An 'Edit Role' dialog box is open, showing the following fields:
 - Role ID:** 3001
 - Name:** AxisDevice
 - Description:** Configure access for Axis devices
- Bottom:** Shows copyright information (Copyright 2023 Hewlett Packard Enterprise Development LP), the date (Oct 26, 2023 05:07:35 UTC), and the software version (ClearPass Policy Manager 6.11.2.252294 on CLAV (Trial Version) platform).

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 utilizam 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 , veja abaixo o exemplo de configuração de porta do switch de acesso HPE Aruba Networking para configurar o 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 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 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.

The screenshot shows two instances of the ClearPass Policy Manager web interface. The top instance displays the 'Authentication Sources' list, and the bottom instance shows the 'Add Authentication Source' dialog.

Top Window: Authentication Sources List

The 'Authentication Sources' list table shows 11 entries:

#	Name	Type	Description
1.	[Admin User Repository]	Local SQL DB	Authenticate users against Policy Manager admin user database
2.	[Denylist User Repository]	Local SQL DB	Denylist database with users who have exceeded bandwidth or session related limits
3.	[Endpoints Repository]	Local SQL DB	Authenticate endpoints against Policy Manager local database
4.	[Guest Device Repository]	Local SQL DB	Authenticate guest devices against Policy Manager local database
5.	[Guest User Repository]	Local SQL DB	Authenticate guest users against Policy Manager local database
6.	[Insight Repository]	Local SQL DB	Insight database with session information for users and devices
7.	[Local User Repository]	Local SQL DB	Authenticate users against Policy Manager local user database
8.	[Onboard Devices Repository]	Local SQL DB	Authenticate Onboard devices against Policy Manager local database
9.	[Social Login Repository]	Local SQL DB	Authenticate users against Policy Manager social login database
10.	[Time Source]	Local SQL DB	Authorization source for implementing various time functions
11.	[Zone Cache Repository]	HTTP	Access attributes cached by Context Server Actions in previous sessions

Bottom Window: Add Authentication Source Dialog

The 'Add Authentication Source' dialog is open, showing the 'General' tab. The 'Name' field is set to 'Axis Devices' and the 'Description' field contains 'MAC addresses of Axis devices in use.' The 'Type' is set to 'Static Host List'. The 'Authorization Sources' section is empty.

The screenshot shows the 'Add Static Host List' dialog box. The 'Name' field is set to 'Axis devices'. The 'Host Format' is set to 'List' and 'Host Type' is set to 'MAC Address'. The 'Host Entries' table contains three entries:

#	Address	Description
1.	B8-A4-4F-45-B4-E6	Axis Device 1
2.	B8-A4-4F-45-B4-E7	Axis Device 2
3.	B8-A4-4F-45-B4-E8	Axis Device 3

At the bottom of the dialog, there are 'Save' and 'Cancel' buttons. The 'Save' button is highlighted in blue.

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

The screenshot shows the 'Authentication Sources' page. The 'Static Host Lists' tab is selected. A message at the top right says 'List "Axis devices" added successfully'. The 'MAC Address Host Lists' table has one entry: 'Axis devices'. To the right of the table are buttons for 'Remove', 'View Details', and 'Modify'. A dropdown menu is open, showing the option '--Select--'. At the bottom of the page, there are 'Save' and 'Cancel' buttons.

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.

Aruba ClearPass Policy Manager

Configuration > Services

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

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

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

Showing 1-9 of 9

Reorder Copy Export Delete

Administration

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

Aruba ClearPass Policy Manager

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

Summary Service Authentication Roles Enforcement

Name: Axis 802.1X Wired - Mac Authentication

Description: To authenticate guest devices based on their MAC address.

Type: MAC Authentication

Status: Disabled

Monitor Mode: Enable to monitor network access without enforcement

More Options: Authorization Audit End-hosts Profile Endpoints Accounting Proxy

Service Rule

Matches ANY or ALL of the following conditions:

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

Back to Services

Enable Copy Save Cancel

Administration

Copyright 2023 Hewlett Packard Enterprise Development LP Oct 26, 2023 05:15:11 UTC ClearPass Policy Manager 6.11.2.252294 on CLABV (Trial Version) platform

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

ClearPass Policy Manager

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

Services - Axis 802.1X Wired - Mac Authentication

Summary Service Authentication Roles Enforcement

Authentication Methods: [Allow All MAC AUTH]

Authentication Sources: Axis Devices [Static Host List]

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

Move Up ↑ Move Down ↓ Remove View Details Modify

Move Up ↑ Move Down ↓ Remove View Details Modify

Move Up ↑ Move Down ↓ Remove View Details Modify

Back to Services

Disable Copy Save Cancel

Administration

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

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

ClearPass Policy Manager

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

Services - Axis 802.1X Wired - Mac Authentication

Summary Service Authentication Roles Enforcement

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

Enforcement Policy: Axis MAC Authentication Policy Add New Enforcement Policy

Enforcement Policy Details

Description:

Default Profile: [Deny Access Profile]

Rules Evaluation Algorithm: evaluate-all

Conditions

(Date:Day-of-Week BELONGS_TO Monday, Tuesday, Wednesday, Thursday, Friday)

1. AND (Date:Time-of-Day IN_RANGE 09:00:00,17:00:00)

AND (Connection:Client-Mac-Vendor EQUALS Axis Communications AB)

Enforcement Profiles

Allow_VLAN_203

Back to Services

Enable Copy Save Cancel

Administration

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

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 , 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

2025-11 (M7.2)

© 2023 – 2025 Axis Communications AB