

HPE Aruba Networking

Spis treści

Wprowadzenie.....	3
Bezpieczne wdrożenie — IEEE 802.1AR/802.1X.....	4
Wstępne uwierzytelnienie	4
Przygotowanie	4
Sieciowe środowisko produkcyjne	5
Konfigurowanie sieci HPE Aruba Networking.....	6
HPE Aruba Networking ClearPass Policy Manager	6
Switch dostępowy HPE Aruba Networking.....	15
Konfiguracja Axis	16
Urządzenie sieciowe Axis.....	16
AXIS Device Manager.....	17
Bezpieczne działanie sieci — IEEE 802.1AE MACsec	18
HPE Aruba Networking ClearPass Policy Manager	19
Role i zasady mapowania ról.....	19
Konfiguracja usług.....	20
Profil wykonawczy.....	21
Switch dostępowy HPE Aruba Networking	22
Wdrażanie starszej wersji — uwierzytelnianie MAC.....	23
HPE Aruba Networking ClearPass Policy Manager	23
Zasady wykonawcze.....	23
Konfiguracja źródła.....	24
Konfiguracja usług.....	25
Switch dostępowy HPE Aruba Networking	28

Wprowadzenie

W niniejszym przewodniku integracji opisano konfigurację opartą na najlepszych praktykach wykonywaną podczas wdrażania i obsługi urządzeń Axis w sieciach HPE Aruba Networking. Konfiguracja oparta na najlepszych praktykach wykorzystuje nowoczesne standardy zabezpieczeń i protokoły, takie jak IEEE 802.1X, IEEE 802.1AR, IEEE 802.1AE i HTTPS.

Odpowiednia automatyzacja integracji sieciowej pomaga zaoszczędzić czas i pieniądze. Eliminuje niepotrzebną złożoność systemu podczas korzystania z aplikacji do zarządzania urządzeniami Axis w połączeniu z infrastrukturą i aplikacjami HPE Aruba Networking. Łącząc urządzenia i oprogramowanie Axis z infrastrukturą HPE Aruba Networking, można uzyskać następujące korzyści:

- Eliminacja sieci do przygotowywania urządzeń minimalizuje złożoność systemu.
- Dodanie automatycznych procesów wdrażania i zarządzania urządzeniami pozwala obniżyć koszty.
- Urządzenia Axis zapewniają bezobsługową kontrolę bezpieczeństwa sieci.
- Zwiększone bezpieczeństwo ogólne sieci dzięki wiedzy specjalistycznej firm HPE i Axis.



Aby zapewnić płynne, zdefiniowane programowo przejście między sieciami logicznymi w całym procesie wdrażania, infrastruktura sieciowa musi być przygotowana do bezpiecznej weryfikacji integralności urządzeń Axis przed rozpoczęciem konfiguracji. Przed przystąpieniem do konfiguracji potrzebne są następujące elementy:

- Doświadczenie w zarządzaniu infrastrukturą informatyczną sieci korporacyjnych HPE Aruba Networking, w tym switchami dostępowymi HPE Aruba Networking oraz oprogramowaniem HPE Aruba Networking ClearPass Policy Manager.
- Znajomość nowoczesnych technik kontroli dostępu do sieci i zasad bezpieczeństwa w sieciach.
- Cenna jest również podstawowa wiedza na temat produktów Axis, ale te informacje są również zawarte w niniejszym przewodniku.

Bezpieczne wdrożenie — IEEE 802.1AR/802.1X



Aby obejrzeć ten film wideo, przejdź do internetowej wersji dokumentu.

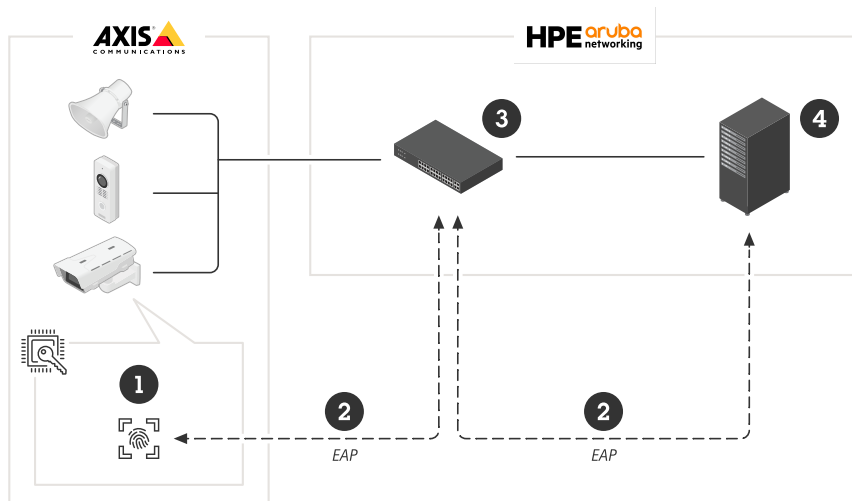
Bezpieczne wdrażanie urządzeń w sieciach o zerowym zaufaniu za pomocą protokołu IEEE 802.1X/802.1AR

Wstępne uwierzytelnienie

Gdy urządzenie Axis obsługiwane przez Axis Edge Vault łączy się z siecią, wykorzystuje certyfikat identyfikatora urządzenia Axis IEEE 802.1AR poprzez kontrolę dostępu do sieci IEEE 802.1X w celu uwierzytelnienia się.

Aby przyznać prawa dostępu do sieci, ClearPass Policy Manager weryfikuje ID urządzenia Axis wraz z innymi identyfikatorami unikalnymi dla urządzenia. Informacje te, takie jak adres MAC i wersja systemu operacyjnego AXIS OS urządzenia, są wykorzystywane do podejmowania decyzji opartych na zasadach.

Urządzenie Axis uwierzytelnia się w sieci za pomocą certyfikatu identyfikatora urządzenia Axis zgodnego ze standardem IEEE 802.1AR.

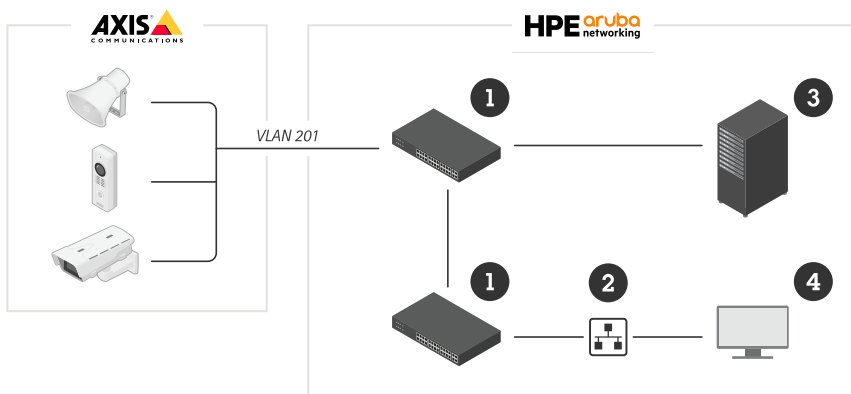


Urządzenie Axis uwierzytelnia się w sieci HPE Aruba Networking za pomocą certyfikatu identyfikatora urządzenia Axis zgodnego ze standardem IEEE 802.1AR.

- 1 Identyfikator urządzenia axis
- 2 Uwierzytelnianie sieci IEEE 802.1x EAP-TLS
- 3 Switch dostępowy (uwierzytelniający)
- 4 ClearPass Policy Manager

Przygotowanie

Po uwierzytelnieniu urządzenie Axis przechodzi do sieci obsługi administracyjnej (VLAN201). Zawiera ona program AXIS Device Manager, który służy do konfiguracji urządzeń, wzmacniania zabezpieczeń oraz aktualizacji systemu operacyjnego AXIS OS. Aby zakończyć obsługę administracyjną urządzenia, na urządzenie przesyłane są nowe, specyficzne dla klienta certyfikaty klasy produkcyjnej dla IEEE 802.1X i HTTPS.

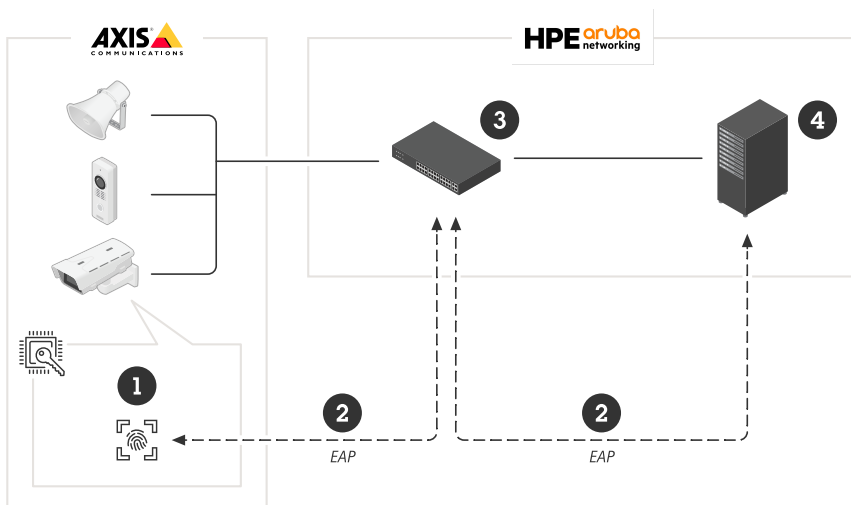


Po pomyślnym uwierzytelnieniu urządzenie Axis zostaje przeniesione do sieci obsługi administracyjnej w celu konfiguracji.

- 1 Switch dostępowy
- 2 Sieć administracyjna
- 3 ClearPass Policy Manager
- 4 Aplikacja do zarządzania urządzeniami

Sieciowe środowisko produkcyjne

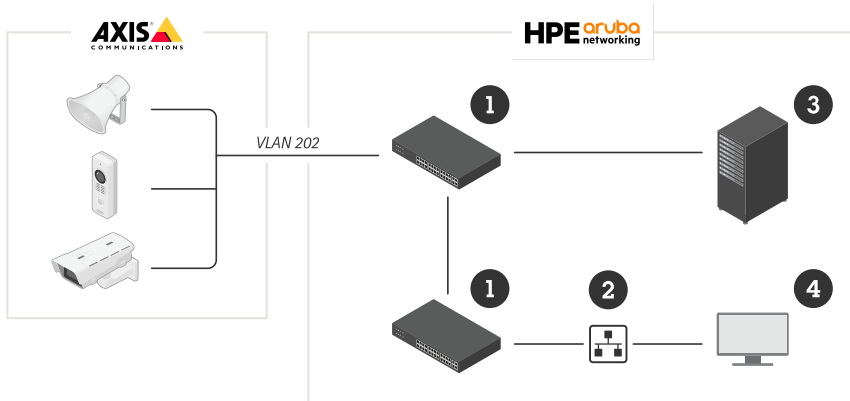
Udostępnienie urządzeniu Axis nowych certyfikatów IEEE 802.1X wyzwala kolejną próbę uwierzytelnienia. ClearPass Policy Manager zweryfikuje nowe certyfikaty i zdecyduje, czy przenieść urządzenie Axis do sieci produkcyjnej.



Po skonfigurowaniu urządzenie Axis opuszcza sieć obsługi administracyjnej i podejmuje ponowną próbę uwierzytelnienia w sieci.

- 1 Identyfikator urządzenia axis
- 2 Uwierzytelnianie sieci IEEE 802.1x EAP-TLS
- 3 Switch dostępowy (uwierzytelniający)
- 4 ClearPass Policy Manager

Po ponownym uwierzytelnieniu urządzenie Axis przechodzi do sieci produkcyjnej (VLAN 202), gdzie system zarządzania materiałem wizyjnym (VMS) nawiązuje z nim połączenie i rozpoczyna jego obsługę.



Urządzenie Axis uzyskuje prawa dostępu do sieci produkcyjnej.

- 1 Switch dostępowy
- 2 Sieciowe środowisko produkcyjne
- 3 ClearPass Policy Manager
- 4 System zarządzania materiałem wizyjnym

Konfigurowanie sieci HPE Aruba Networking

HPE Aruba Networking ClearPass Policy Manager

ClearPass Policy Manager zapewnia opartą na rolach i urządzeniach bezpieczną kontrolę dostępu do sieci dla IoT, BYOD, urządzeń firmowych, pracowników, wykonawców i gości w ramach infrastruktury przewodowej, bezprzewodowej i VPN wielu dostawców.

Konfiguracja zaufanej bazy certyfikatów

1. Pobierz specyficzny dla Axis łańcuch certyfikatów IEEE 802.1AR ze strony axis.com.
2. Prześlij specyficzne dla urządzeń Axis łańcuchy certyfikatów IEEE 802.1AR głównego urzędu certyfikacji i pośredniego urzędu certyfikacji do magazynu zaufanych certyfikatów.
3. Uruchom narzędzie ClearPass Policy Manager, aby uwierzytelniać urządzenia Axis za pośrednictwem IEEE 802.1X EAP-TLS.
4. W polu użytkownika wybierz opcję EAP. Certyfikaty są używane do uwierzytelniania IEEE 802.1X EAP-TLS.

The screenshot shows the ClearPass Policy Manager web interface. The left sidebar contains navigation links: Dashboard, Monitoring, Configuration, and Administration. The main content area is titled 'Certificate Trust List' and displays a table of trusted Certificate Authorities (CA). A dialog box titled 'Add Certificate' is open, showing a 'Certificate File' field with the value 'Axis_device_ID_Int...e_CA_ECC_1.pem' and a 'Usage' field with the value 'EAP'. The dialog also includes a 'Remove' button and an 'Add Certificate' button. The table below the dialog lists various CA entries with columns for #, Subject, Usage, Validity, and Enabled status.

#	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,O=VeriSign, Inc.,C=US	Others	Valid	Disabled
2.	OU=Go	AD/LDAP Servers, Endpoint Context Servers, SAML, SMTP, Others	Valid	Enabled
3.	OU=Class	Others	Valid	Disabled
4.	emailAddress=...	EAP, Others	Valid	Enabled
5.	emailAddress=...	EAP, Others	Valid	Enabled
6.	C=US,ST=01	Others	Valid	Disabled
7.	C=US,ST=...	Others	Valid	Disabled
8.	C=US,ST=...	Aruba Infrastructure	Valid	Disabled
9.	CN=Wired Phones,OU=PKI Authority,O=Alcatel-Lucent,C=FR	Others	Valid	Disabled
10.	CN=VeriSign Class 3 Public Primary Certification Authority - G5,OU=(c) 2006 VeriSign, Inc. - For authorized use only,OU=VeriSign Trust Network,O=VeriSign, Inc.,C=US	Others	Valid	Disabled
11.	CN=VeriSign Class 3 Public Primary Certification Authority - G3,OU=(c) 1999 VeriSign, Inc. - For authorized use only,OU=VeriSign Trust Network,O=VeriSign, Inc.,C=US	Others	Valid	Disabled
12.	CN=VeriSign Class 1 Public Primary Certification Authority - G3,OU=(c) 1999 VeriSign, Inc. - For authorized use only,OU=VeriSign Trust Network,O=VeriSign, Inc.,C=US	AD/LDAP Servers, Endpoint Context Servers, SAML, SMTP, Others	Valid	Enabled
13.	CN=USERTrust RSA Certification Authority,O=The USERTRUST Network,L=Jersey City,ST=New Jersey,C=US	EAP, Others	Valid	Disabled
14.	CN=thawte Primary Root CA,OU=(c) 2006 thawte, Inc. - For authorized use only,OU=Certification Services Division,O=thawte, Inc.,C=US	Others	Valid	Disabled
15.	CN=TC TrustCenter Universal CA 1,OU=TC TrustCenter Universal CA,O=TC TrustCenter GmbH,C=DE	Others	Valid	Disabled

Prześlij certyfikaty IEEE 802.1AR specyficzne dla firmy Axis do zaufanego magazynu certyfikatów narzędzia ClearPass Policy Manager.

ClearPass Policy Manager - 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 Go Clear Filter

Show 20 records

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

Zaufany magazyn certyfikatów w narzędziu ClearPass Policy Manager z dołączonym łańcuchem certyfikatów IEEE 802.1AR firmy Axis.

Konfiguracja urządzenia/grupy sieciowej

1. Dodawanie zaufanych urządzeń dostępu do sieci takich jak switchy dostępne HPE Aruba Networking do narzędzia ClearPass Policy Manager. Menedżer zasad ClearPass Policy Manager musi wiedzieć, które switchy dostępne w sieci są używane do komunikacji IEEE 802.1X. Uwaga: współdzielony sekret RADIUS musi odpowiadać konkretnej konfiguracji switcha IEEE 802.1X
2. Konfiguracja grupy urządzeń sieciowych służy do grupowania wielu zaufanych urządzeń dostępu do sieci. Grupowanie urządzeń ułatwia konfigurację zasad.

ClearPass Policy Manager - 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 Go Clear Filter

Show 20 records

#	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

Interfejs zaufanych urządzeń sieciowych w narzędziu ClearPass Policy Manager.

ClearPass Policy Manager - Aruba

Configuration » Network » Devices

Network Devices

Add Device

Device | SNMP Read Settings | SNMP Write Settings | CLI Settings | OnConnect Enforcement | Attributes

Name: SW04

IP or Subnet Address: 172.25.200.13
(e.g., 192.168.1.10 or 192.168.1.1/24 or 2001:db8:a0b:12f0::1 or 2001:db8:a0b:12f0::1/64)

Description:

RADIUS Shared Secret: [password field] Verify: [password field]

TACACS+ Shared Secret: [password field] Verify: [password field]

Vendor Name: Aruba

Enable RADIUS Dynamic Authorization: ☐

Enable RadSec: ☐

Add Cancel

Copyright 2022 Hewlett Packard Enterprise Development LP Dec 28, 2022 09:02:18 CET ClearPass Policy Manager 6.9.12.136929 on CLABV (Trial Version) platform

Dodawanie switcha dostępowego HPE Aruba Networking jako zaufanego urządzenia w narzędziu ClearPass Policy Manager. Uwaga: współdzielony sekret RADIUS musi odpowiadać konkretnej konfiguracji switcha IEEE 802.1X.

ClearPass Policy Manager - Aruba

Configuration » Network » Devices

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.

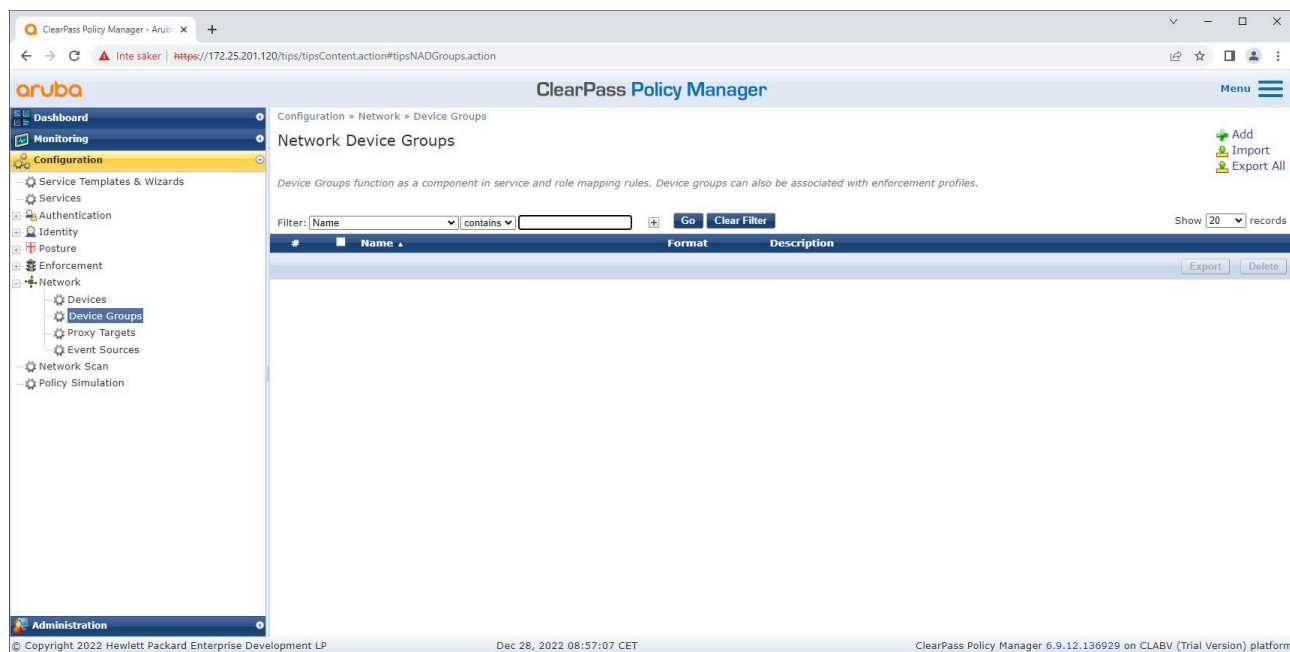
Filter: Name contains [] Go Clear Filter

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

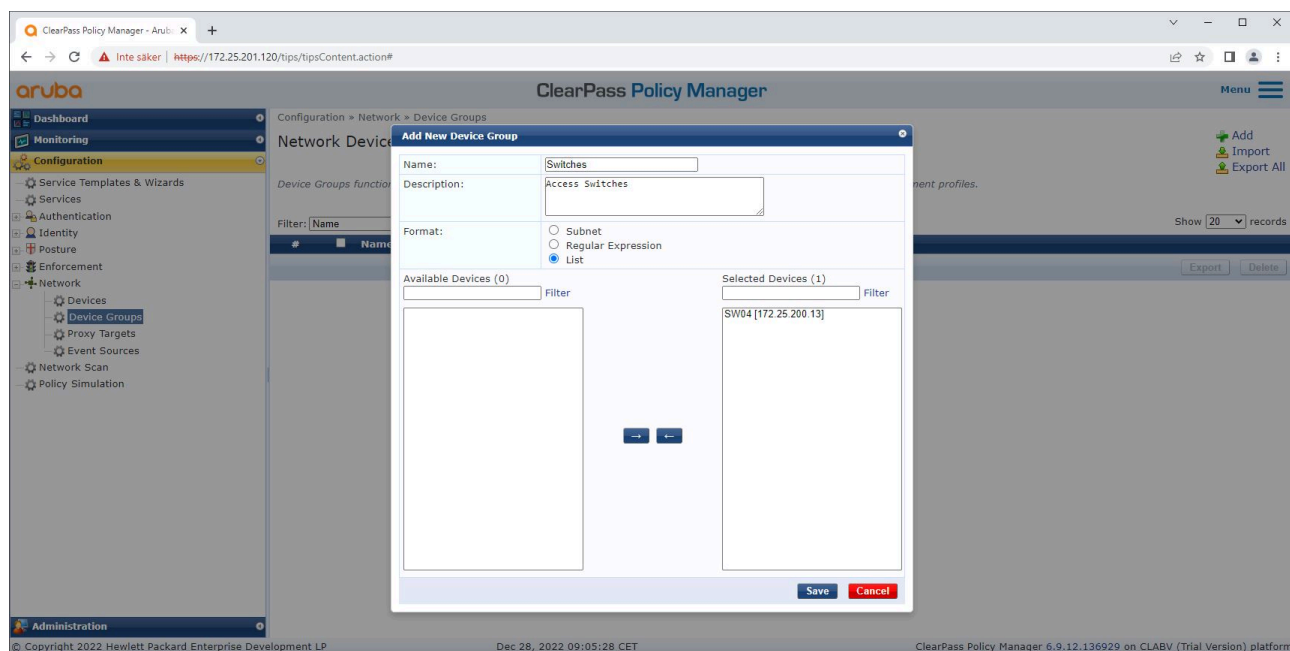
Showing 1-1 of 1

Copyright 2022 Hewlett Packard Enterprise Development LP Dec 28, 2022 09:02:33 CET ClearPass Policy Manager 6.9.12.136929 on CLABV (Trial Version) platform

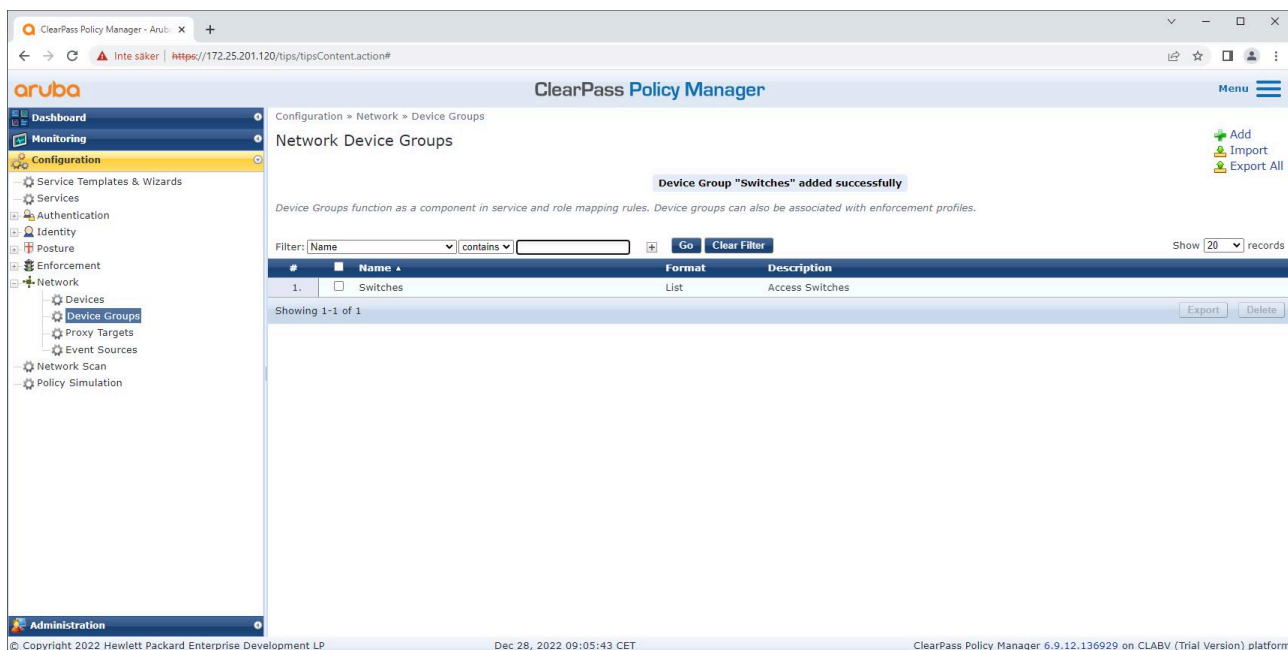
ClearPass Policy Manager ze skonfigurowanym jednym zaufanym urządzeniem sieciowym.



Interfejs zaufanych grup urządzeń sieciowych w narzędziu ClearPass Policy Manager.



Dodawanie zaufanego urządzenia dostępu do sieci do nowej grupy urządzeń w narzędziu ClearPass Policy Manager.

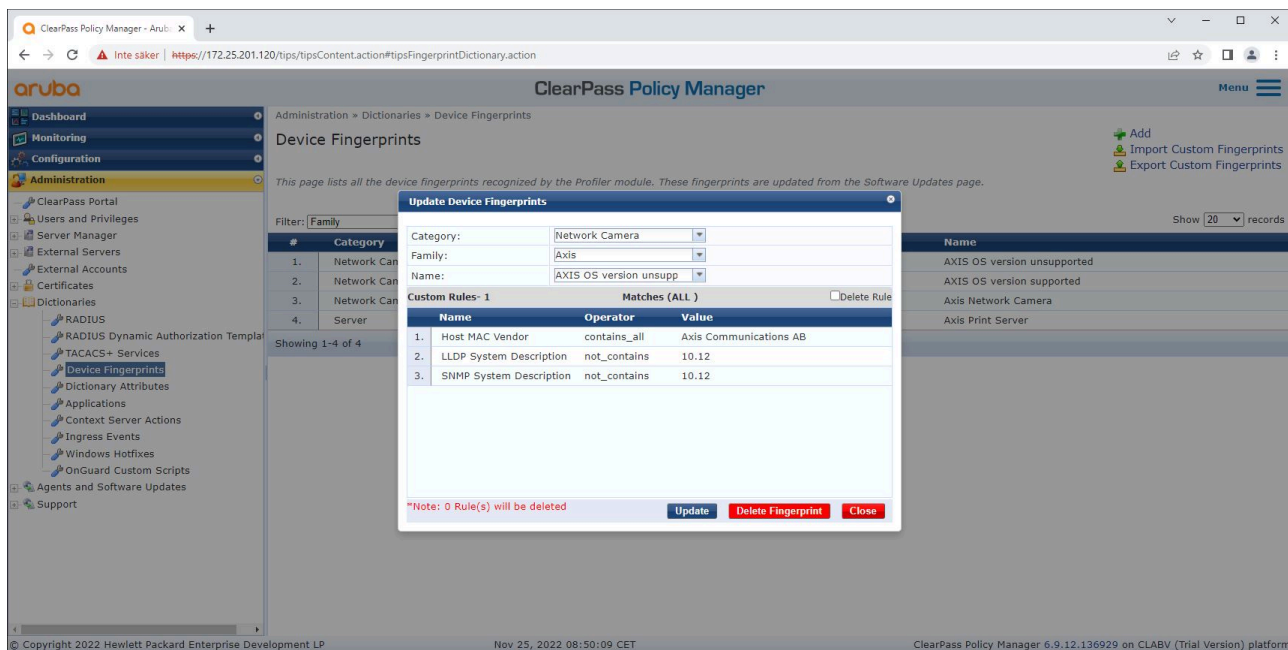


ClearPass Policy Manager ze skonfigurowaną grupą urządzeń sieciowych, która zawiera jedno lub więcej zaufanych urządzeń sieciowych.

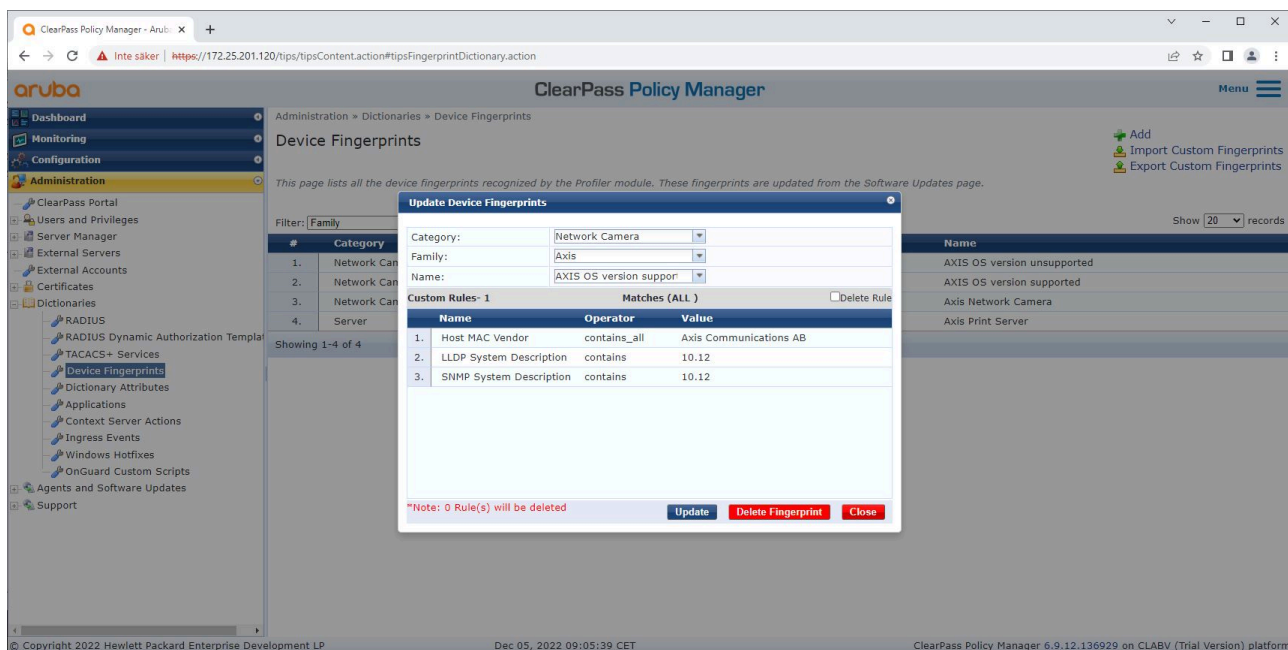
Konfiguracja odcisku palca urządzenia

Urządzenie Axis może, poprzez wykrywanie w sieci, rozsyłać unikalne dla siebie informacje, takie jak adres MAC czy wersja oprogramowania urządzenia. Informacje te można wykorzystywać do tworzenia i aktualizowania odcisku palca urządzenia oraz zarządzania nim w narzędziu ClearPass Policy Manager. Można również przyznać dostęp lub go odmówić w zależności od wersji systemu operacyjnego AXIS OS.

1. Przejdź do menu **Administration > Dictionaries > Device Fingerprints** (Administracja > Słowniki > Odciski palców urządzenia).
2. Wybierz istniejący odcisk palca urządzenia lub utwórz nowy.
3. Wprowadź ustawienia odcisku palca urządzenia.



Konfiguracja odcisku palca urządzenia w narzędziu ClearPass Policy Manager. Urządzenia Axis z systemem operacyjnym AXIS OS w wersji innej niż 10.12 nie są obsługiwane w tym przykładzie.



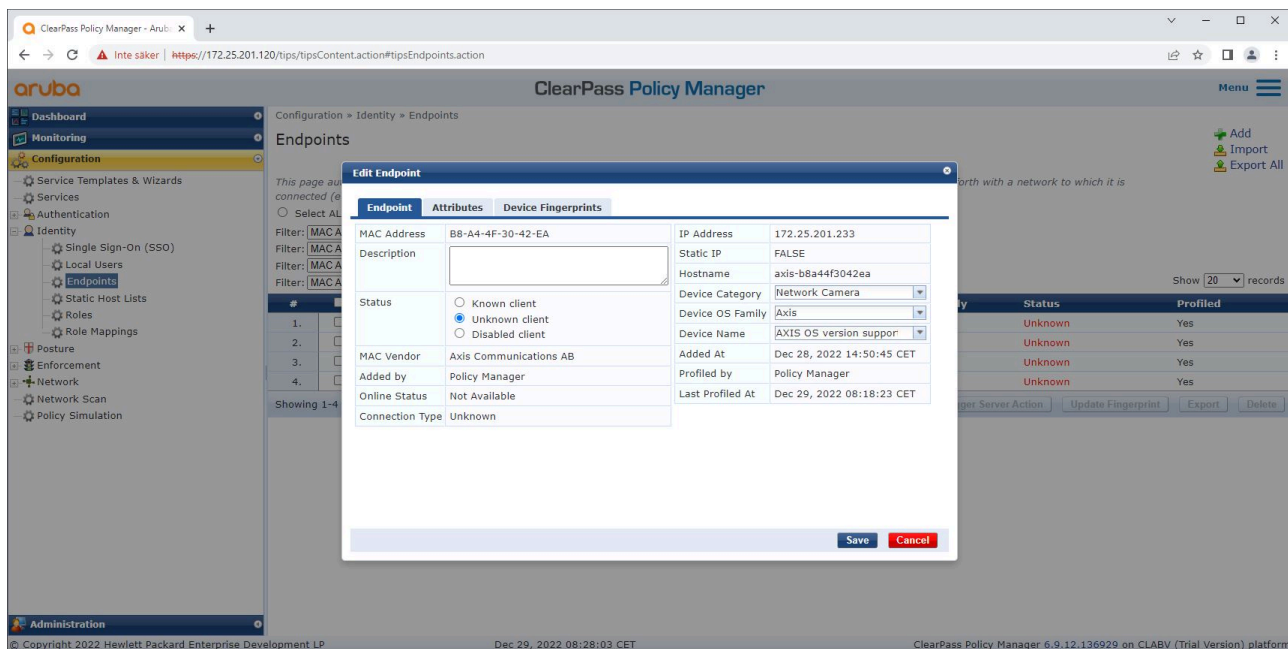
Konfiguracja odcisku palca urządzenia w narzędziu ClearPass Policy Manager. Urządzenia Axis z systemem operacyjnym AXIS OS w wersji innej niż 10.12 są obsługiwane w tym przykładzie.

Informacje o odcisku palca urządzenia zebranym przez narzędzie ClearPass Policy Manager można znaleźć w sekcji Punkty końcowe.

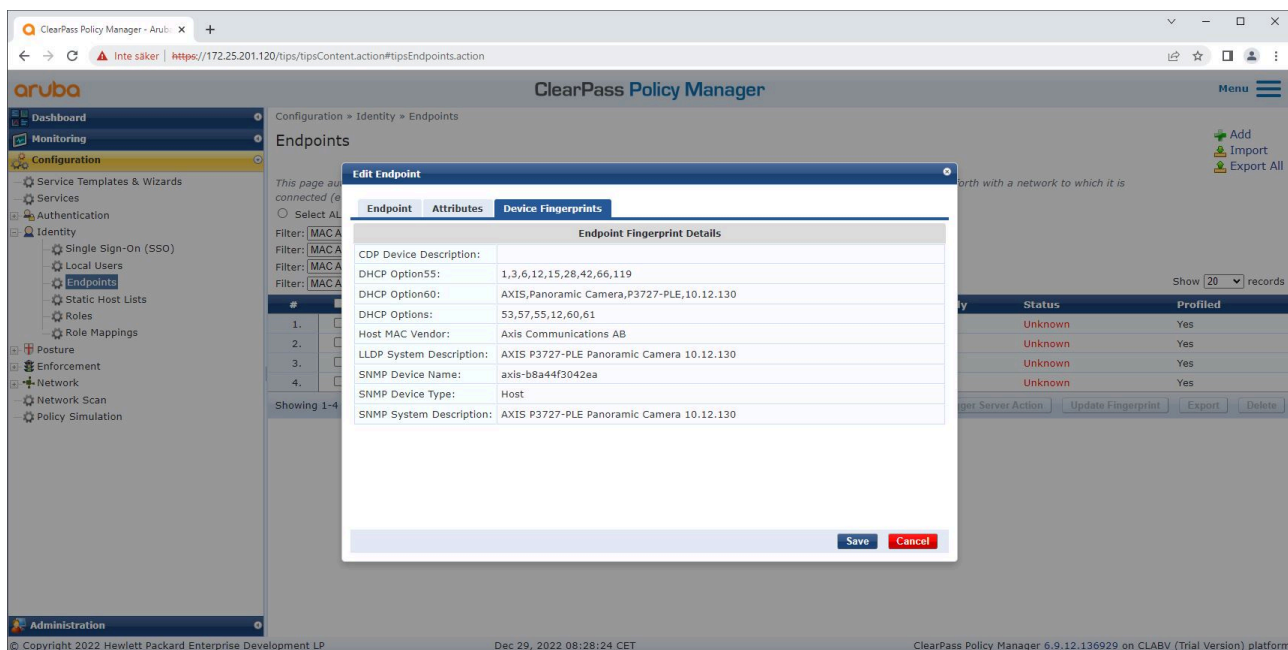
1. Otwórz menu Configuration > Identity > Endpoints (Konfiguracja > Tożsamość > Punkty końcowe).
2. Wybierz urządzenia, które chcesz wyświetlić.
3. Kliknij kartę Device Fingerprints (Odciski palca urządzenia).

Uwaga

Protokół SNMP jest domyślnie wyłączony w urządzeniach Axis i pobierany ze switcha dostępowego HPE Aruba Networking.



Urządzenie Axis sprofilowane przez narzędzie ClearPass Policy Manager.

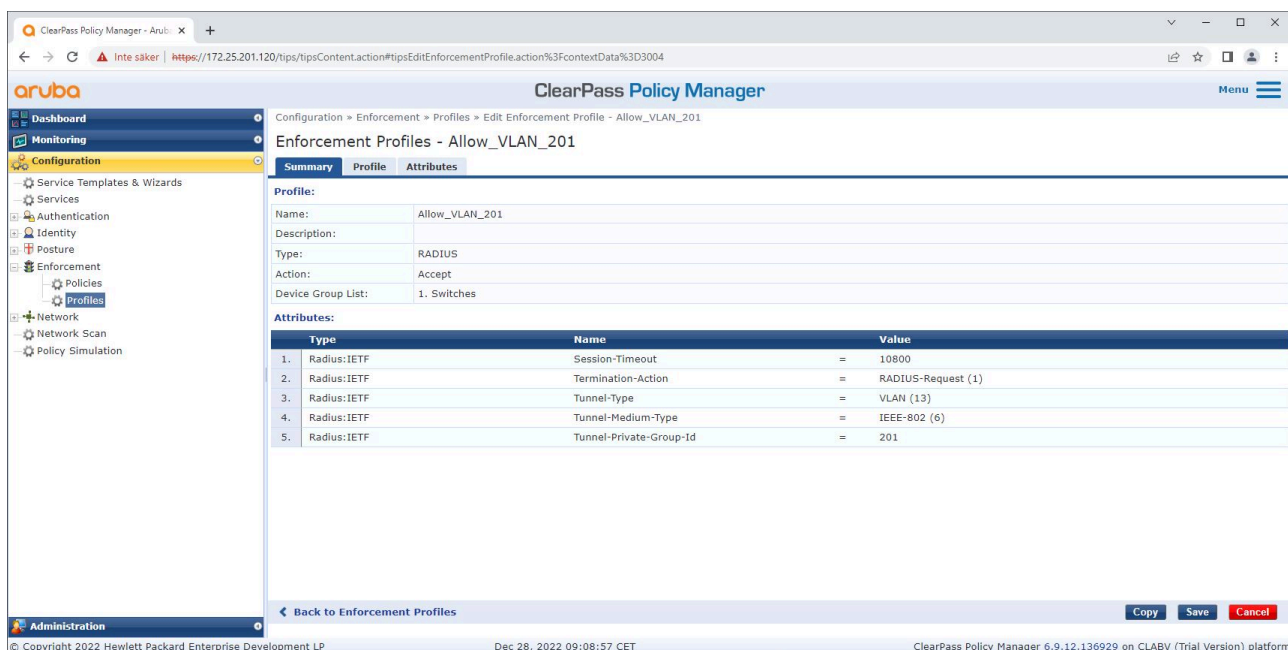


Szczegółowe odciski palców sprofilowanego urządzenia Axis. Należy pamiętać, że protokół SNMP jest domyślnie wyłączony w urządzeniach Axis. Informacje dotyczące wykrywania specyficzne dla protokołów LLDP, CDP i DHCP są udostępniane przez urządzenie Axis w domyślnym stanie fabrycznym i przekazywane przez switch dostępowy HPE Aruba Networking do narzędzia ClearPass Policy Manager.

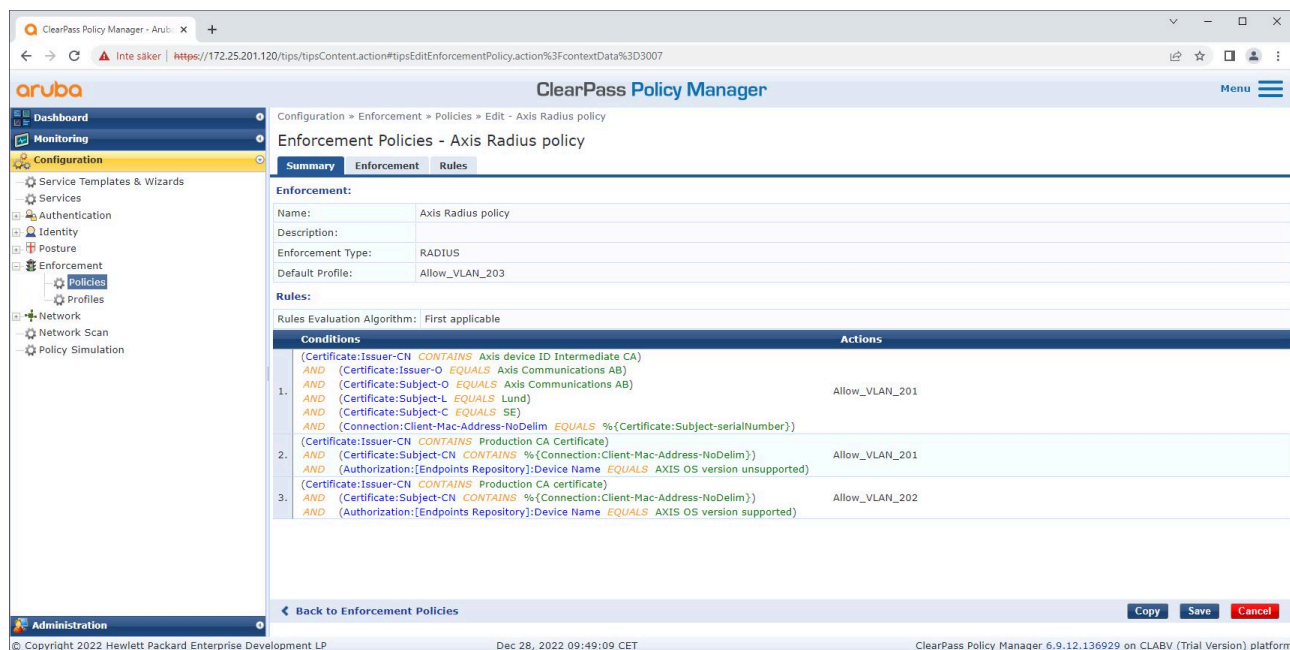
Konfiguracja profilu wykonywania

Za pomocą profilu wykonywania ClearPass Policy Manager może przypisywać określony identyfikator sieci VLAN do portu dostępu na switchu. Jest to decyzja oparta na zasadach, która ma zastosowanie do urządzeń sieciowych w grupie urządzeń „Switche”. Wymagana liczba profili wykonywania zależy od liczby używanych sieci VLAN. Nasza konfiguracja obejmuje trzy sieci VLAN (VLAN 201, 202, 203), które odpowiadają trzem profilom wykonywania.

Zasady wykonywania można skonfigurować po ustawieniu profili wykonywania dla sieci VLAN. Konfiguracja zasad wykonywania w ClearPass Policy Manager określa, czy urządzenia Axis uzyskują dostęp do sieci HPE Aruba Networking w oparciu o cztery przykładowe profile zasad.



Przykładowy profil wykonywania umożliwiający dostęp do sieci VLAN 201.



Konfiguracja zasad wykonywania w ClearPass Policy Manager.

Poniżej wymieniono cztery zasady wykonywania i związane z nimi działania:

Odmowa dostępu do sieci

Jeśli nie przeprowadzono uwierzytelniania kontroli dostępu do sieci w standardzie IEEE 802.1X, dostęp do sieci nie jest udzielany.

Sieć dla gości (VLAN 203)

Jeśli uwierzytelnienie kontroli dostępu IEEE 802.1X nie powiedzie się, urządzenie Axis uzyskuje dostęp do ograniczonej, odizolowanej sieci. Następnie należy wykonać ręczną kontrolę urządzenia w celu podjęcia decyzji co do odpowiednich działań.

Sieć administracyjna (VLAN 201)

Urządzenie Axis uzyskuje dostęp do sieci administracyjnej. Ma to na celu zapewnienie możliwości zarządzania urządzeniami Axis za pomocą *AXIS Device Manager* i *AXIS Device Manager Extend*. Umożliwia to również konfigurowanie urządzeń Axis za pomocą aktualizacji systemu operacyjnego AXIS OS, certyfikatów klasy produkcyjnej i innych konfiguracji. ClearPass Policy Manager sprawdza następujące warunki:

- Wersja systemu operacyjnego AXIS OS urządzenia.
- Adres MAC urządzenia jest zgodny ze schematem adresów MAC specyficznym dla dostawcy, z atrybutem numeru seryjnego certyfikatu identyfikatora urządzenia Axis.
- Certyfikat identyfikatora urządzenia Axis jest weryfikowalny i odpowiada atrybutom specyficznym dla Axis, takim jak wydawca, organizacja, lokalizacja i kraj.

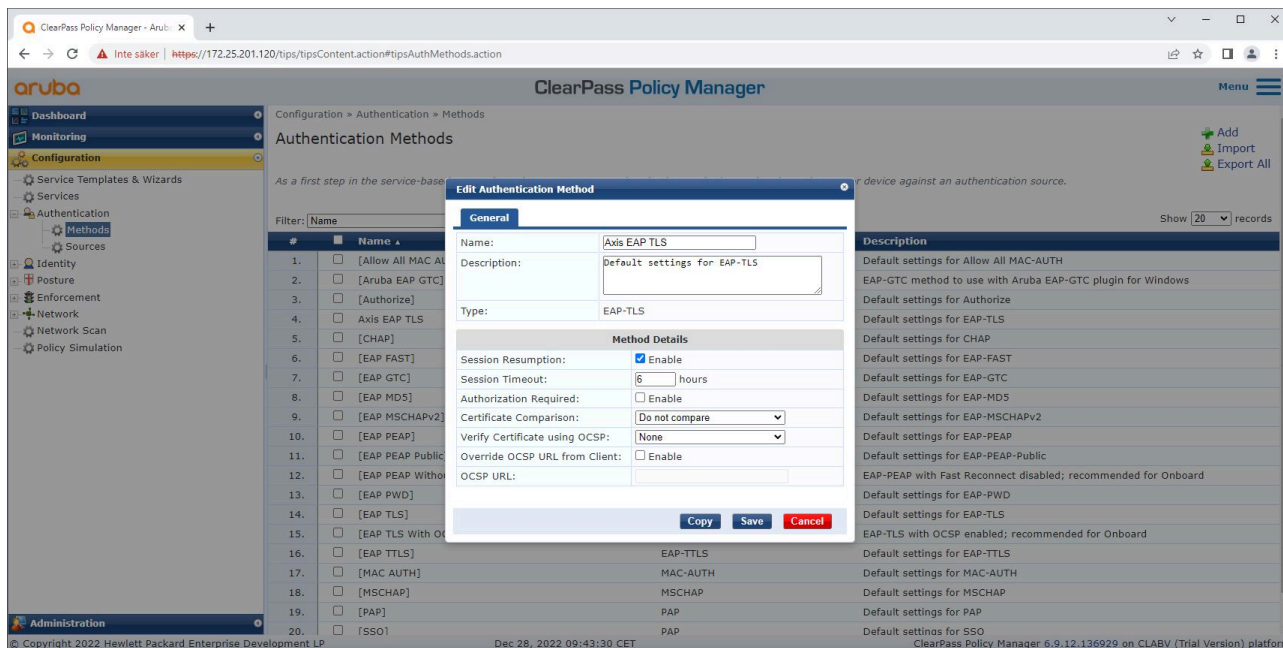
Sieć produkcyjna (VLAN 202)

Urządzenie Axis uzyskuje prawa dostępu do sieci produkcyjnej, w której będzie działać. Dostęp zostaje przyznany po zakończeniu działań administracyjnych na urządzeniu z poziomu sieci administracyjnej (VLAN 201). ClearPass Policy Manager sprawdza następujące warunki:

- Wersja systemu operacyjnego AXIS OS urządzenia.
- Adres MAC urządzenia jest zgodny ze schematem adresów MAC specyficznym dla dostawcy, z atrybutem numeru seryjnego certyfikatu identyfikatora urządzenia Axis.
- Certyfikat klasy produkcyjnej można zweryfikować w zaufanym magazynie certyfikatów.

Konfiguracja metody uwierzytelniania

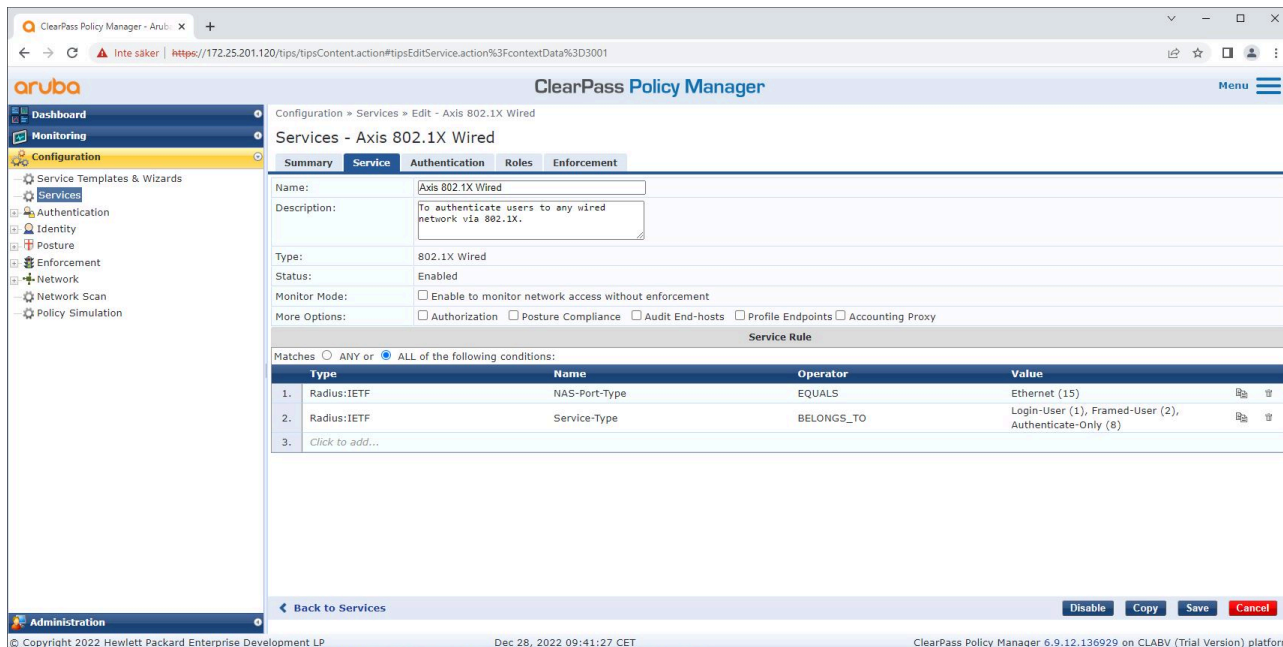
Metoda uwierzytelniania określa sposób, w jaki urządzenie Axis próbuje uwierzytelnić się w sieci. Preferowaną metodą jest IEEE 802.1X EAP-TLS, ponieważ urządzenia Axis z obsługą Axis Edge Vault mają domyślnie włączoną funkcję IEEE 802.1X EAP-TLS.



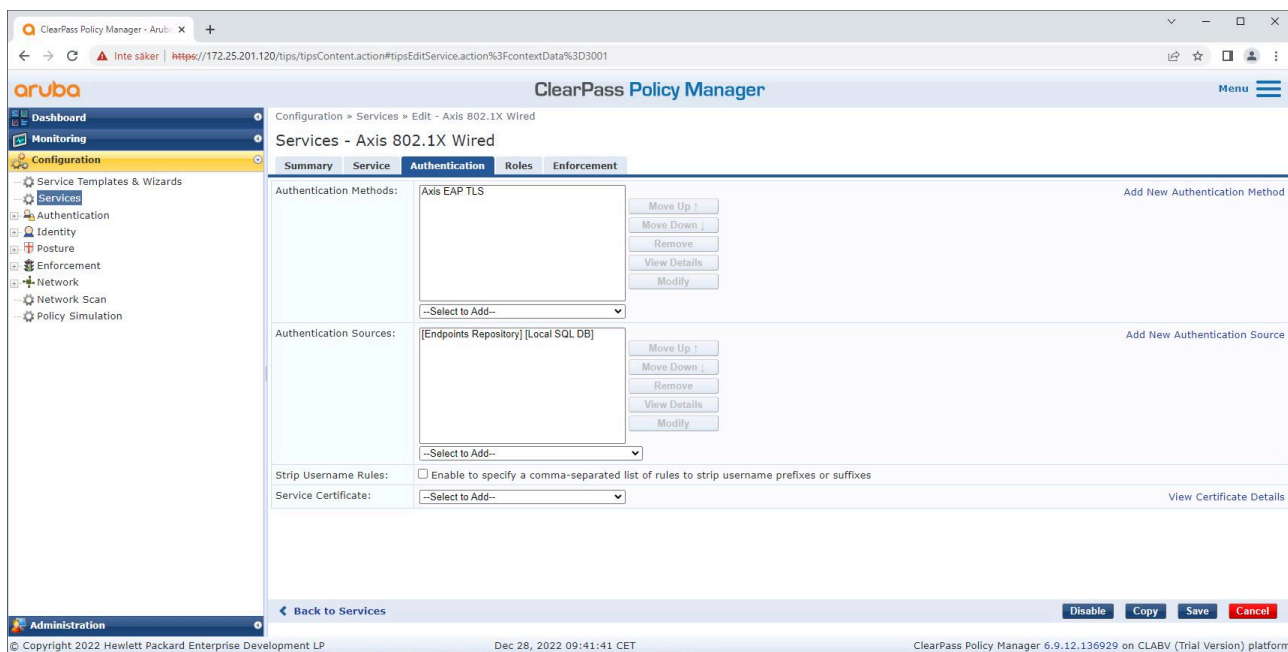
Interfejs metody uwierzytelniania narzędzia ClearPass Policy Manager, w którym zdefiniowana jest metoda uwierzytelniania EAP-TLS dla urządzeń Axis.

Konfiguracja usług

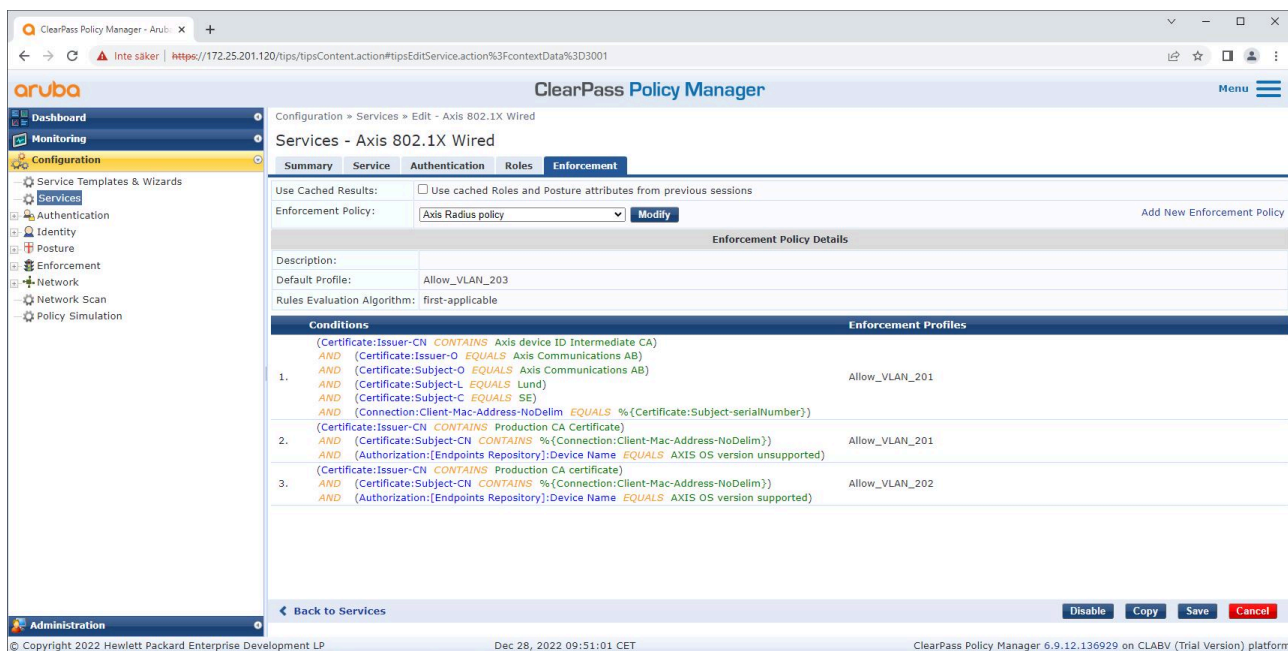
Na stronie Services (Usługi) kroki konfiguracji są połączone w jedną usługę, która obsługuje uwierzytelnianie i autoryzację urządzeń Axis w sieciach HPE Aruba Networking.



Tworzenie dedykowanej usługi Axis ze standardem IEEE 802.1X jako metodą połączenia.



Konfigurowanie utworzonej wcześniej metody uwierzytelniania EAP-TLS dla usługi.



Konfigurowanie utworzonych wcześniej zasad wykonywania dla usługi.

Switch dostępowy HPE Aruba Networking

Urządzenia Axis są podłączane bezpośrednio do switchy dostępowych obsługujących PoE lub za pośrednictwem kompatybilnych zasilaczy midspan PoE firmy Axis. Aby bezpiecznie włączyć urządzenia Axis do sieci HPE Aruba Networking, switch dostępowy musi być skonfigurowany pod kątem obsługi komunikacji w standardzie IEEE 802.1X. Urządzenie Axis przekazuje komunikację w standardzie IEEE 802.1x EAP-TLS do narzędzia ClearPass Policy Manager, które pełni funkcję serwera RADIUS.

Uwaga

Zostało także skonfigurowane okresowe ponowne uwierzytelnianie dla urządzenia Axis trwające 300 sekund. Ma to na celu poprawę ogólnego bezpieczeństwa dostępu do portu.

Ten przykład przedstawia konfigurację globalną oraz konfigurację portów dla switchy dostępowych HPE Aruba Networking.

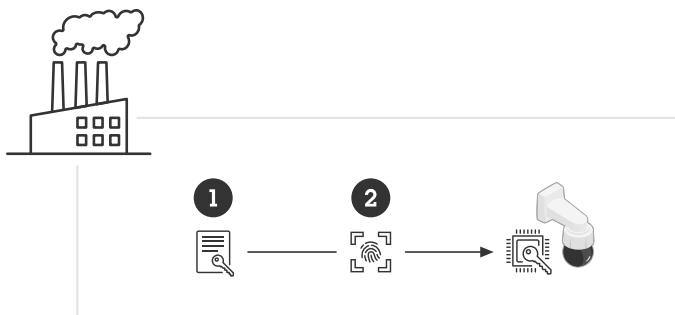
```
radius-server host MyRADIUSIPAddress key "MyRADIUSKey"
```

```
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
```

Konfiguracja Axis

Urządzenie sieciowe Axis

Urządzenia Axis z obsługą funkcji *Axis Edge Vault* są produkowane z bezpieczną tożsamością urządzenia nazywaną identyfikatorem urządzenia Axis. Identyfikator urządzenia Axis jest oparty na międzynarodowej normie IEEE 802.1AR, która definiuje metodę automatycznej, bezpiecznej identyfikacji urządzeń i podłączania ich do sieci za pomocą protokołu IEEE 802.1X.



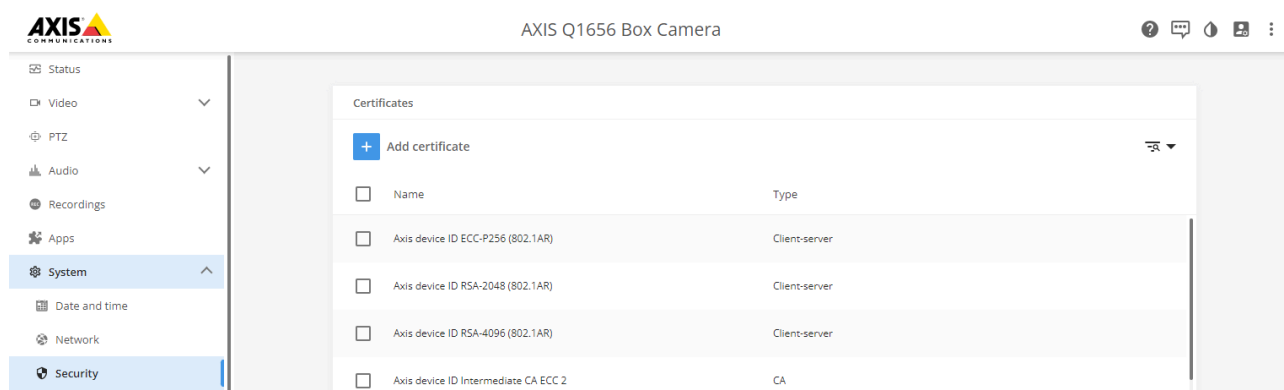
Urządzenia Axis mają fabryczne certyfikaty identyfikatorów urządzeń Axis zgodne z IEEE 802.1AR dla zaufanych usług identyfikacji urządzeń

- 1 *Infrastruktura kluczy (PKI) identyfikatorów urządzeń Axis*
- 2 *Identyfikator urządzenia Axis*

Chroniony sprzętowo bezpieczny magazyn kluczy dostarczany przez bezpieczny element urządzenia Axis jest fabrycznie wyposażony w unikalny dla urządzenia certyfikat i odpowiednie klucze (identyfikator urządzenia Axis), które globalnie mogą potwierdzić autentyczność urządzenia Axis. *Axis Product Selector* może pomóc w określeniu, które urządzenia Axis obsługują *Axis Edge Vault* i identyfikator urządzenia Axis.

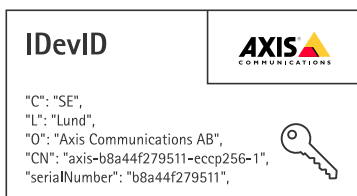
Uwaga

Numer seryjny urządzenia Axis jest jednocześnie jego adresem MAC.



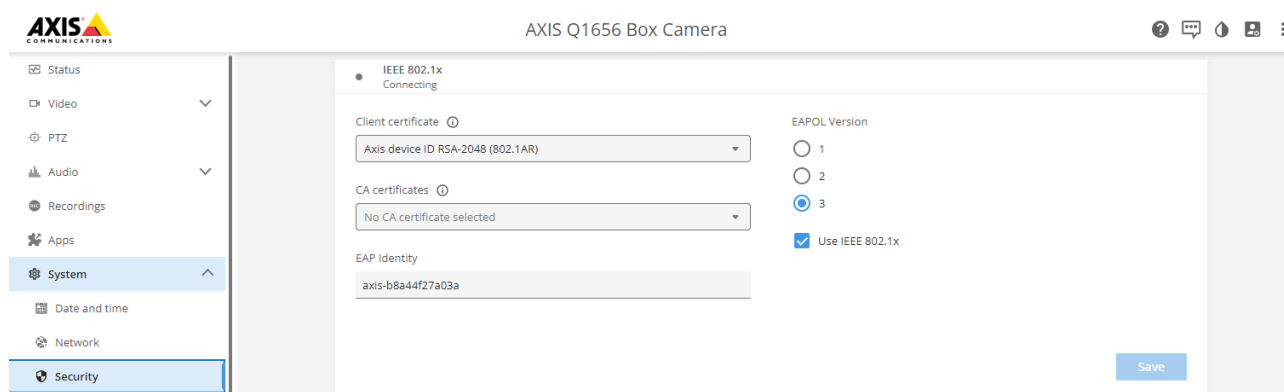
Magazyn certyfikatów urządzenia Axis w domyślnym stanie fabrycznym, z identyfikatorem urządzenia Axis.

Certyfikat ID urządzenia Axis zgodny z IEEE 802.1AR zawiera informacje o numerze seryjnym i inne informacje specyficzne dla dostawcy. ClearPass Policy Manager analizuje te informacje i podejmuje decyzję o przyznaniu dostępu do sieci. Poniższe informacje można uzyskać z certyfikatu identyfikatora urządzenia Axis.



Kraj	SE
Lokalizacja	Lund
Organizacja wydająca	Axis Communications AB
Nazwa pospolita organizacji wydającej	Certyfikat pośredniczący ID urządzenia Axis
Organizacja	Axis Communications AB
Nazwa pospolita	axis-b8a44f279511-eccp256-1
Numer seryjny	b8a44f279511

Nazwa pospolita składa się z połączenia nazwy firmy Axis, numeru seryjnego urządzenia oraz algorytmu kryptograficznego (ECC P256, RSA 2048, RSA 4096). Począwszy od wersji AXIS OS 10.1 (z września 2020 r.) standard IEEE 802.1X jest domyślnie włączony ze wstępnie skonfigurowanym identyfikatorem urządzenia Axis. Umożliwia to urządzeniu uwierzytelnianie się w sieciach obsługujących standard IEEE 802.1X.



Urządzenie Axis w domyślnej konfiguracji fabrycznej z włączoną obsługą IEEE 802.1X i wstępnie wybranym certyfikatem ID urządzenia Axis.

AXIS Device Manager

AXIS Device Manager i AXIS Device Manager Extend mogą być używane w sieci do konfiguracji i zarządzania wieloma urządzeniami Axis w ekonomiczny sposób. AXIS Device Manager to aplikacja działająca w systemie Microsoft Windows®, instalowana lokalnie na komputerze w sieci, natomiast AXIS Device Manager Extend wykorzystuje infrastrukturę chmury do zarządzania urządzeniami w wielu lokalizacjach. Oba te rozwiązania zapewniają łatwe konfigurowanie urządzeń i zarządzanie nimi, w tym:

- Instalowanie aktualizacji systemu operacyjnego AXIS OS.
- Stosowanie konfiguracji bezpieczeństwa cybernetycznego, takich jak certyfikaty HTTPS i IEEE 802.1X.
- Konfiguracja ustawień specyficznych dla urządzenia, takich jak ustawienia obrazów i inne.

Bezpieczne działanie sieci — IEEE 802.1AE MACsec



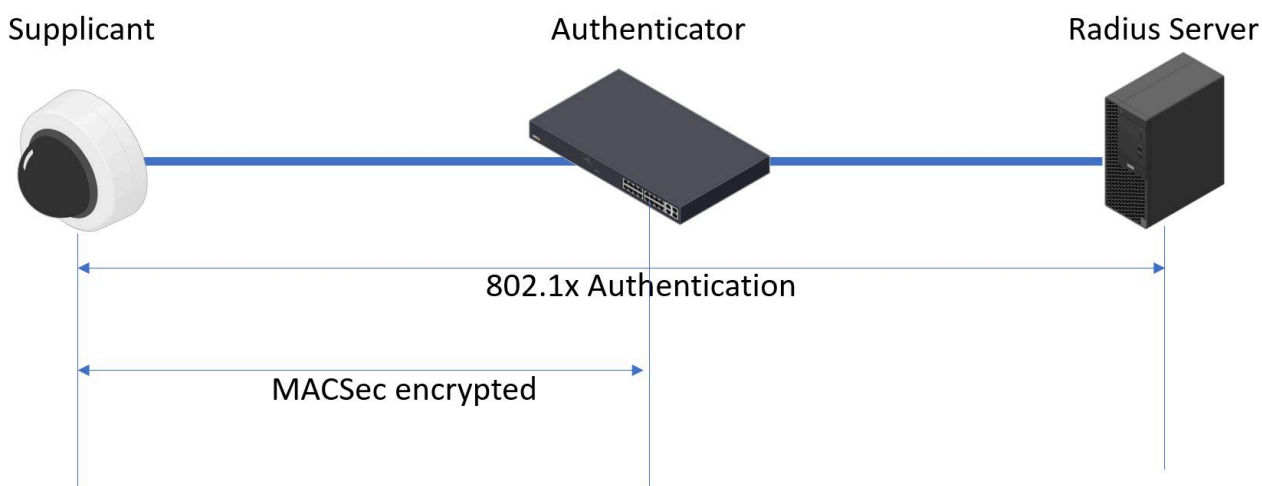
Aby obejrzeć ten film wideo, przejdź do internetowej wersji dokumentu.

Szyfrowanie sieci z zerowym zaufaniem za pomocą protokołu IEEE 802.1AE MACsec w warstwie 2

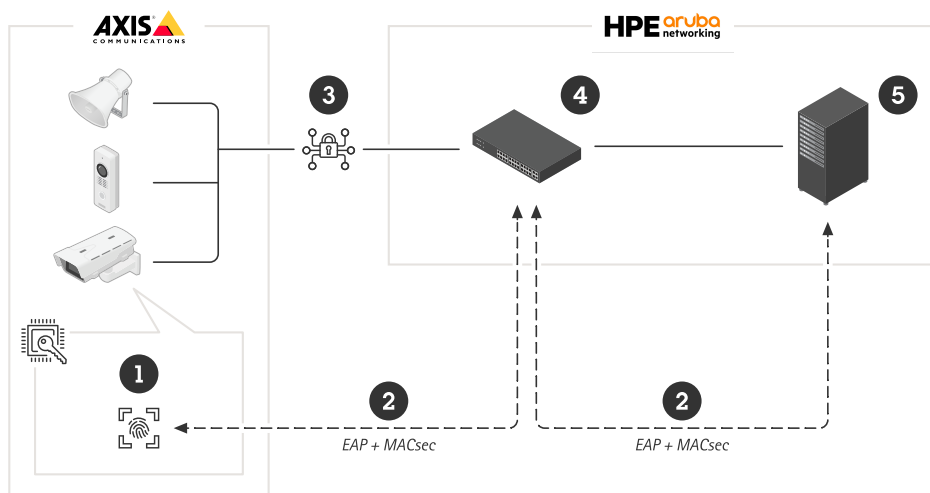
IEEE 802.1AE MACsec (Media Access Control Security) to dobrze zdefiniowany protokół sieciowy, który kryptograficznie zabezpiecza łącza Ethernet typu punkt-punkt w warstwie sieci 2. Zapewnia poufność i integralność transmisji danych pomiędzy dwoma hostami.

Standard IEEE 802.1AE MACsec opisuje dwa tryby działania:

- Ręcznie konfigurowany tryb klucza PSK / Static CAK
- Automatyczny tryb sesji głównej / Dynamic CAK z użyciem IEEE 802.1X EAP-TLS



W systemie AXIS OS w wersji 10.1 (wrzesień 2020 roku) i nowszych standard IEEE 802.1X jest domyślnie włączony dla urządzeń zgodnych z identyfikatorem urządzenia Axis. W systemie AXIS OS w wersji 11.8 i nowszych obsługujemy protokół MACsec z automatycznym trybem dynamicznym przy użyciu standardu IEEE 802.1X EAP-TLS, który jest domyślnie włączony. Po podłączeniu urządzenia Axis z domyślnymi wartościami fabrycznymi przeprowadzane jest uwierzytelnianie sieci za pomocą IEEE 802.1X, a jeśli się powiedzie, wypróbowywany jest także tryb MACsec Dynamic CAK.



Bezpiecznie przechowywany identyfikator urządzenia Axis ID (1) – tożsamość urządzenia zgodna ze standardem IEEE 802.1AR – służy do uwierzytelniania w sieci (4, 5) za pomocą kontroli dostępu do sieci IEEE 802.1X EAP-TLS w oparciu o porty (2). W trakcie całej sesji EAP-TLS automatycznie wymieniane są klucze MACsec, aby ustanowić bezpieczne połączenie (3), chroniąc cały ruch w sieci do urządzenia Axis do switcha HPE Aruba Networking.

IEEE 802.1AE MACsec wymaga przygotowań do konfiguracji switcha dostępowego HPE Aruba Networking i narzędzia ClearPass Policy Manager. Aby to umożliwić, na urządzeniu Axis nie jest wymagana żadna konfiguracja przez EAP-TLS z szyfrowaniem IEEE 802.1AE MACsec.

Jeśli switch dostępowy HPE Aruba Networking nie obsługuje szyfrowania MACsec przez EAP-TLS, można użyć trybu klucza PSK i skonfigurować ręcznie.

HPE Aruba Networking ClearPass Policy Manager

Role i zasady mapowania ról

The screenshot shows the ClearPass Policy Manager web interface. The 'Roles' section is selected in the left sidebar. A table lists various roles, including [AirGroup v1], [AirGroup v2], [Aruba TACACS+ read-only Admin], [Aruba TACACS+ root Admin], [AxisDevice], [BYOD], [Contract], [Device], [Employee], [Guest], [MAC Ca], [Onboard], [Onboard iOS], [Onboard iPadOS], [Onboard Linux], [Onboard macOS], [Onboard Windows], [Other], and [TACACS+ API Admin]. An 'Edit Role' modal is open for the role 'AxisDevice' (Role ID: 3001), showing fields for Name and Description. The bottom of the interface displays 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).

Dodawanie nazwy roli dla urządzeń Axis. Nazwa jest nazwą roli dostępu do portu w konfiguracji switcha dostępowego.

Configuration » Identity » Role Mappings » Edit - Axis Role Mapping

Role Mappings - Axis Role Mapping

Policy:

Policy Name: Axis Role Mapping

Description:

Default Role: [Guest]

Mapping Rules:

Rules Evaluation Algorithm: Evaluate all

Conditions	Role Name
1. (Authentication:Full-Username BEGINS_WITH axis-00408c)	AxisDevice
2. (Authentication:Full-Username BEGINS_WITH axis-acc8e)	AxisDevice
3. (Authentication:Full-Username BEGINS_WITH axis-b8a44f)	AxisDevice

Back to Role Mappings

Copy Save Cancel

Copyright 2023 Hewlett Packard Enterprise Development LP Oct 26, 2023 05:08:20 UTC ClearPass Policy Manager 6.11.2.252294 on CLABV (Trial Version) platform

Dodawanie zasad mapowania ról Axis do utworzonej wcześniej roli urządzenia Axis. Spełnienie określonych warunków jest wymagane, aby urządzenie mogło zostać zmapowane do roli urządzenia Axis. Jeśli warunki nie zostaną spełnione, urządzenie będzie częścią roli [Guest] (gość).

Urządzenia Axis używają domyślnie formatu tożsamości EAP „axis-numerseryjny”. Numer seryjny urządzenia Axis to jego adres MAC. Na przykład: „axis-b8a44f45b4e6”.

Konfiguracja usług

Configuration » Services » Edit - Axis 802.1X Wired

Services - Axis 802.1X Wired

Summary Service Authentication Roles Enforcement

Role Mapping Policy: Axis Role Mapping **Modify** Add New Role Mapping Policy

Role Mapping Policy Details

Description:

Default Role: [Guest]

Rules Evaluation Algorithm: evaluate-all

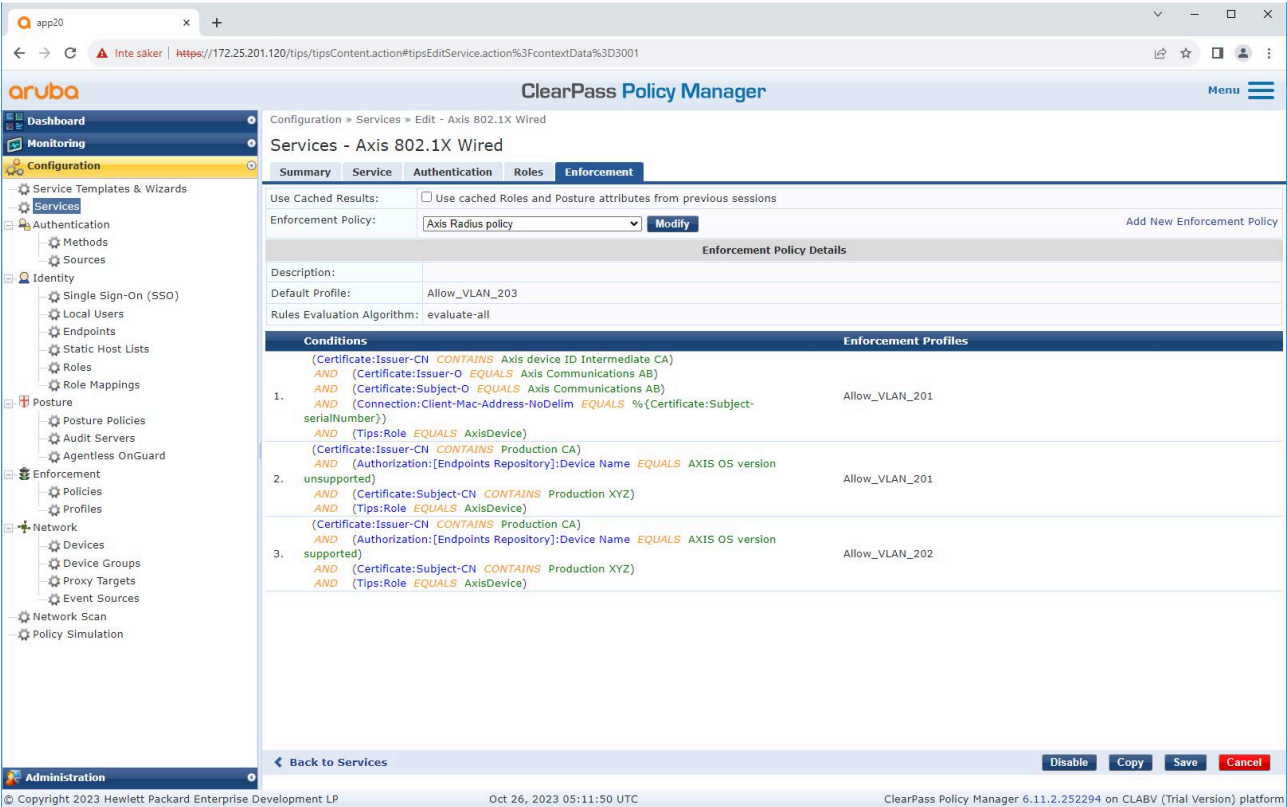
Conditions	Role
1. (Authentication:Full-Username BEGINS_WITH axis-00408c)	AxisDevice
2. (Authentication:Full-Username BEGINS_WITH axis-acc8e)	AxisDevice
3. (Authentication:Full-Username BEGINS_WITH axis-b8a44f)	AxisDevice

Back to Services

Disable Copy Save Cancel

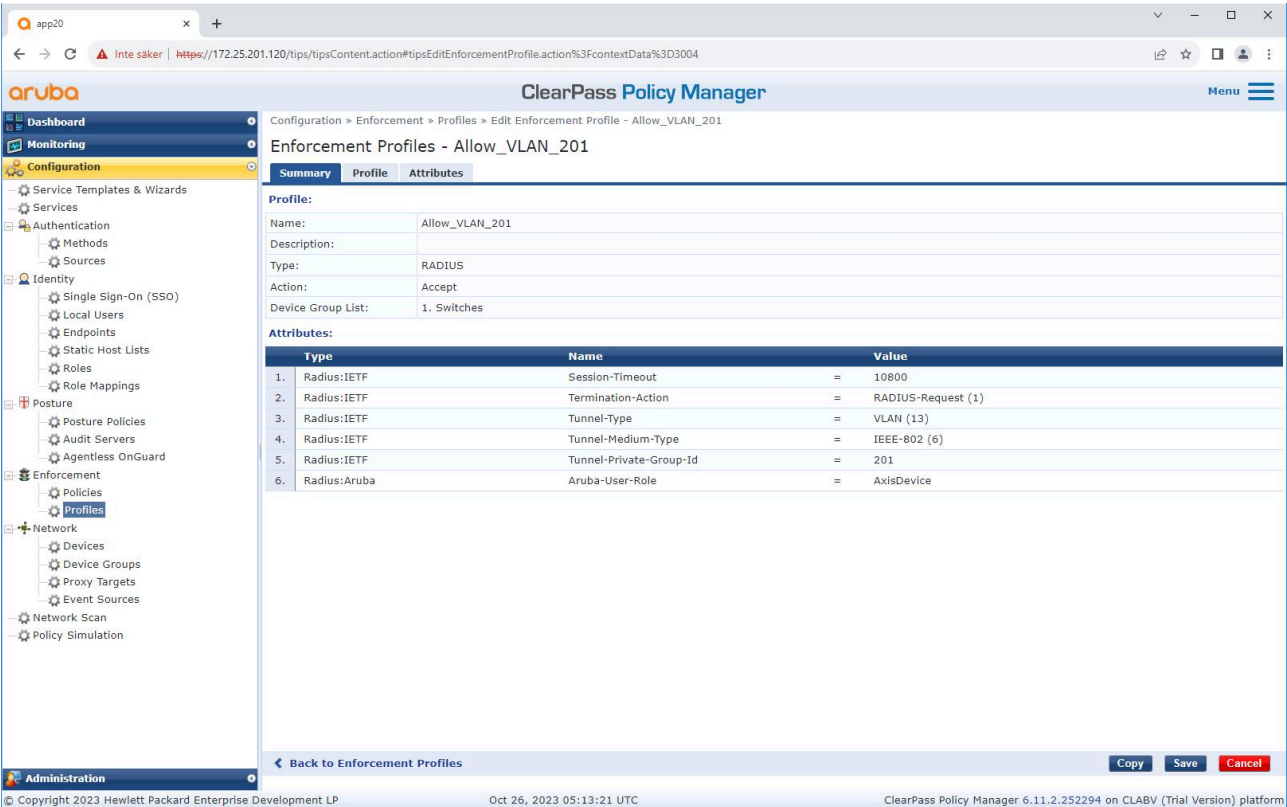
Copyright 2023 Hewlett Packard Enterprise Development LP Oct 26, 2023 05:09:16 UTC ClearPass Policy Manager 6.11.2.252294 on CLABV (Trial Version) platform

Dodawanie wcześniej utworzonej zasady mapowania ról Axis do usługi, która definiuje standard IEEE 802.1X jako metodę łączenia w przypadku wdrażania urządzeń Axis.



Dodawanie nazwy roli Axis jako warunku do istniejących definicji zasad.

Profil wykonawczy



Dodawanie nazwy roli Axis jako atrybutu do profili wykonywania przypisanych w usłudze wdrażania standardu IEEE 802.1X.

Switch dostępowy HPE Aruba Networking

Oprócz konfiguracji bezpiecznego wdrażania opisanej w sekcji zapoznaj się z poniższą przykładową konfiguracją portu dla switcha dostępowego HPE Aruba Networking, aby skonfigurować 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
```


Wdrażanie starszej wersji — uwierzytelnianie MAC

Za pomocą MAC Authentication Bypass (MAB) możesz wdrażać urządzenia Axis, które nie obsługują wdrażania IEEE 802.1AR z certyfikatem identyfikatora urządzenia Axis i włączonym IEEE 802.1X z ustawieniami fabrycznymi. Jeśli wdrożenie standardu 802.1X nie powiedzie się, ClearPass Policy Manager zweryfikuje adres MAC urządzenia Axis i przyzna mu dostęp do sieci.

MAB wymaga przygotowań do konfiguracji switcha dostępowego i narzędzia ClearPass Policy Manager. Zezwolenie na używanie standardu MAB do wdrożenia nie wymaga konfiguracji urządzenia Axis.

HPE Aruba Networking ClearPass Policy Manager

Zasady wykonawcze

Konfiguracja zasad wykonywania w ClearPass Policy Manager określa, czy urządzenia Axis uzyskują dostęp do sieci HPE Aruba Networking w oparciu o dwa przykładowe warunki zasad.

Odmowa dostępu do sieci

Jeśli urządzenie Axis nie spełnia skonfigurowanych zasad wykonywania, nie otrzymuje zezwolenia na dostęp do sieci.

Sieć dla gości (VLAN 203)

Urządzenie Axis uzyska dostęp do ograniczonej, odizolowanej sieci, jeśli spełnione są następujące warunki:

- Dzień jest dniem powszednim, od poniedziałku do piątku.
- Godzina mieści się w zakresie od 9:00 do 17:00.
- Dostawca adresu MAC jest zgodny z Axis Communications.

Ponieważ możliwe jest sfałszowanie adresów MAC, dostęp do zwykłej sieci administracyjnej nie jest przyznawany. Zalecamy korzystanie z MAB tylko do wstępnego wdrożenia i ręczne sprawdzanie urządzenia w przyszłości.

Konfiguracja źródeł

Na stronie Sources (Źródła) tworzone jest nowe źródło uwierzytelniania, które akceptuje tylko ręcznie importowane adresy MAC.

The first screenshot shows the 'Authentication Sources' page in the ClearPass Policy Manager. The left sidebar contains a navigation menu with options like Dashboard, Monitoring, Configuration, Identity, Posture, Enforcement, and Network. The main content area displays a table of existing authentication sources. A filter bar at the top allows searching by name. The table lists 11 sources, including various Local SQL DBs and an HTTP source.

#	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

The second screenshot shows the 'Add Authentication Source' page. The 'General' tab is active, showing fields for Name, Description, Type, and Use for Authorization. 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'. There are buttons for 'Remove' and 'View Details' under the Authorization Sources section.

ClearPass Policy Manager

Configuration » Authentication » Sources » Add

Authentication Sources

General Static Host Lists Summary

MAC Address Host Lists:

Add Static Host List

Name: Axis devices

Description:

Host Format: ☐ Subnet ☐ Regular Expression ☒ List

Host Type: ☐ IP Address ☒ MAC Address

Host 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

Address:

Description:

Save Host

Save Cancel

Back to Authentication Sources

Next → Save Cancel

Copyright 2023 Hewlett Packard Enterprise Development LP Oct 31, 2023 09:20:18 UTC ClearPass Policy Manager 6.11.2.252294 on CLABV (Trial Version) platform

Tworzona jest statyczna lista hostów zawierająca adresy MAC Axis.

ClearPass Policy Manager

Configuration » Authentication » Sources » Add

Authentication Sources

General Static Host Lists Summary

MAC Address Host Lists:

List "Axis devices" added successfully

Axis devices Remove View Details Modify

[-Select-]

Add New Static Host List

Back to Authentication Sources

Next → Save Cancel

Copyright 2023 Hewlett Packard Enterprise Development LP Oct 31, 2023 09:20:34 UTC ClearPass Policy Manager 6.11.2.252294 on CLABV (Trial Version) platform

Konfiguracja usług

Na stronie **Services (Usługi)** kroki konfiguracji są połączone w jedną usługę, która obsługuje uwierzytelnianie i autoryzację urządzeń Axis w sieciach HPE Aruba Networking.

ClearPass Policy Manager

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	✓
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

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

ClearPass Policy Manager

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

Services - 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

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

Tworzona jest dedykowana usługa Axis definiująca standard MAB jako metodę łączności.

The screenshot shows the 'ClearPass Policy Manager' web interface. The left sidebar contains navigation menus for Dashboard, Monitoring, Configuration, and Administration. The main content area is titled 'Services - Axis 802.1X Wired - Mac Authentication' and has tabs for Summary, Service, Authentication, Roles, and Enforcement. The 'Authentication' tab is active, showing 'Authentication Methods' with '[Allow All MAC AUTH]' and 'Authentication Sources' with 'Axis Devices [Static Host List]'. There are buttons for 'Move Up', 'Move Down', 'Remove', 'View Details', and 'Modify' for both methods and sources. A 'Strip Username Rules' section has a checkbox for 'Enable to specify a comma-separated list of rules to strip username prefixes or suffixes'. At the bottom, there are buttons for 'Back to Services', 'Disable', 'Copy', 'Save', and 'Cancel'. The footer shows copyright information and the platform version.

Dla usługi zostaje skonfigurowana metoda uwierzytelniania MAC z predefiniowanymi ustawieniami. Ponadto wybierane jest źródło uwierzytelniania (utworzone wcześniej) zawierające listę adresów MAC Axis.

Axis Communications korzysta z następujących adresów MAC OUI:

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

The screenshot shows the 'ClearPass Policy Manager' web interface, specifically the 'Enforcement' tab for 'Services - Axis 802.1X Wired - Mac Authentication'. The 'Use Cached Results' checkbox is unchecked. The 'Enforcement Policy' is set to 'Axis MAC Authentication Policy'. The 'Enforcement Policy Details' section shows a 'Description' field, a 'Default Profile' set to '[Deny Access Profile]', and a 'Rules Evaluation Algorithm' set to 'evaluate-all'. Below this, there is a table with two columns: 'Conditions' and 'Enforcement Profiles'. The table contains one rule with the following conditions: '(Date:Day-of-Week BELONGS_TO Monday, Tuesday, Wednesday, Thursday, Friday)', '(Date:Time-of-Day IN_RANGE 09:00:00,17:00:00)', and '(Connection:Client-Mac-Vendor EQUALS Axis Communications AB)'. The enforcement profile for this rule is 'Allow_VLAN_203'. At the bottom, there are buttons for 'Back to Services', 'Enable', 'Copy', 'Save', and 'Cancel'. The footer shows copyright information and the platform version.

W ostatnim kroku konfigurowane są utworzone wcześniej zasady wykonywania dla usługi.

Switch dostępowy HPE Aruba Networking

Oprócz konfiguracji bezpiecznego wdrażania opisanej w sekcji zapoznaj się z poniższą przykładową konfiguracją portu dla switcha dostępowego HPE Aruba Networking, aby zezwolić na używanie standardu 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_pl

2025-11 (M7.2)

© 2023 – 2025 Axis Communications AB