HPE Aruba Networking

Przewodnik integracji

HPE Aruba Networking

Spis treści

HPE Aruba Networking

Wprowadzenie

Wprowadzenie

Niniejszy przewodnik integracji zawiera opis najlepszych rozwiązań w zakresie konfiguracji urządzeń Axis i ich obsługi w sieciach HPE Aruba Networking. Konfiguracja oparta na najlepszych praktykach wykorzystuje nowoczesne standardy zabezpieczeń i protokoły, takie jak EEE 802.1X, IEEE 802.1AR, IEEE 802.1AE i HTTPS.

Odpowiednia automatyzacja integracji sieciowej pomoże zaoszczędzić czas i pieniądze. Umożliwia pozbycie się niepotrzebnej złożoności systemu podczas korzystania z aplikacji do zarządzania urządzeniami Axis w połączeniu z infrastrukturą i aplikacjami HPE Aruba Networking. Poniżej zostały opisane niektóre korzyści płynące z łączenia urządzeń i aplikacji Axis z infrastrukturą HPE Aruba Networking:

- Minimalizowanie złożoności systemu poprzez usuwanie sieci pośredniczących urządzeń.
- Redukcja kosztów dzięki automatyzacji procesów wdrażania i zarządzania urządzeniami.
- Możliwość korzystania ze wszystkich zalet automatycznej kontroli bezpieczeństwa sieci (typu „zero-touch") obsługiwanej przez urządzenia Axis.
- Poprawa ogólnego bezpieczeństwa sieci dzięki korzystaniu ze specjalistycznej wiedzy i doświadczeń firm HPE i Axis.

Przed rozpoczęciem konfiguracji infrastruktura sieciowa musi być przygotowana do bezpiecznej weryfikacji integralności urządzeń Axis. Umożliwi to płynne, oparte na definicjach oprogramowania przejście pomiędzy sieciami logicznymi w całym procesie wdrażania. Przed wykonaniem konfiguracji należy zapoznać się z następującymi obszarami tematycznymi:

- Zarządzanie 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 zawarte w niniejszym przewodniku.

Bezpieczne wdrożenie — IEEE 802.1AR/802.1X

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

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

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

Wstępne uwierzytelnienie

Podłącz urządzenie Axis obsługujące Axis Edge Vault, aby uwierzytelnić je w sieci. Urządzenie korzysta z certyfikatu identyfikatora urządzenia Axis IEEE 802.1AR poprzez kontrolę dostępu do sieci IEEE 802.1X w celu uwierzytelnienia.

Aby przyznać prawa dostępu do sieci, ClearPass Policy Manager weryfikuje identyfikator urządzenia Axis wraz z innymi identyfikatorami unikalnymi dla urządzenia. Informacje, takie jak adres MAC i używany system operacyjny AXIS OS, są wykorzystywane do podejmowania decyzji opartych na zasadach.

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

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

1. *ID urządzenia Axis*
2. *Uwierzytelnianie sieci IEEE 802.1x EAP-TLS*
3. *Switch dostępowy (uwierzytelniający)*
4. *ClearPass Policy Manager*

Obsługa administracyjna

Po uwierzytelnieniu urządzenie Axis przechodzi do sieci obsługi administracyjnej (VLAN201), w której jest zainstalowany program AXIS Device Manager. AXIS Device Manager umożliwia przeprowadzenie konfiguracji urządzenia, wzmocnienie zabezpieczeń i aktualizacje 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 urządzenia Axis jest zwalniane z sieci, w której było konfigurowane, po czym podejmie próbę ponownego uwierzytelnienia w sieci.

1 *ID 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). W tej sieci system zarządzania materiałem wizyjnym (VMS) łączy się z urządzeniem Axis i zaczyna działać.

Urządzenie Axis uzyskuje prawa dostępu do sieci produkcyjnej.

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

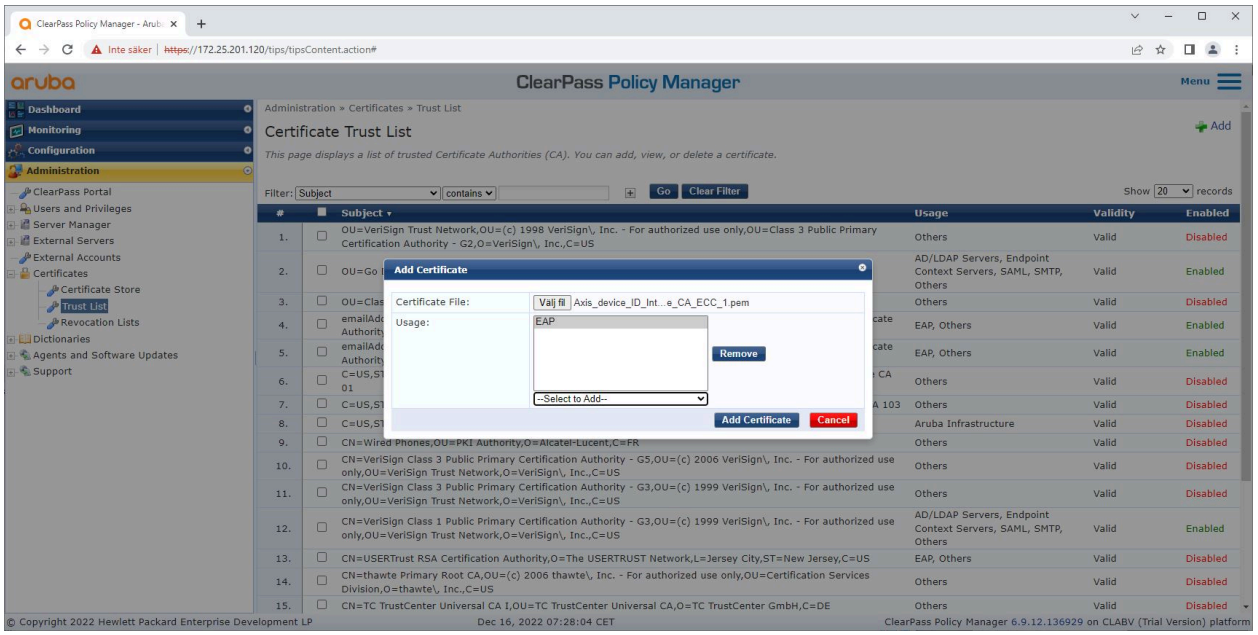
Konfigurowanie sieci HPE Aruba Networking

HPE Aruba Networking ClearPass Policy Manager

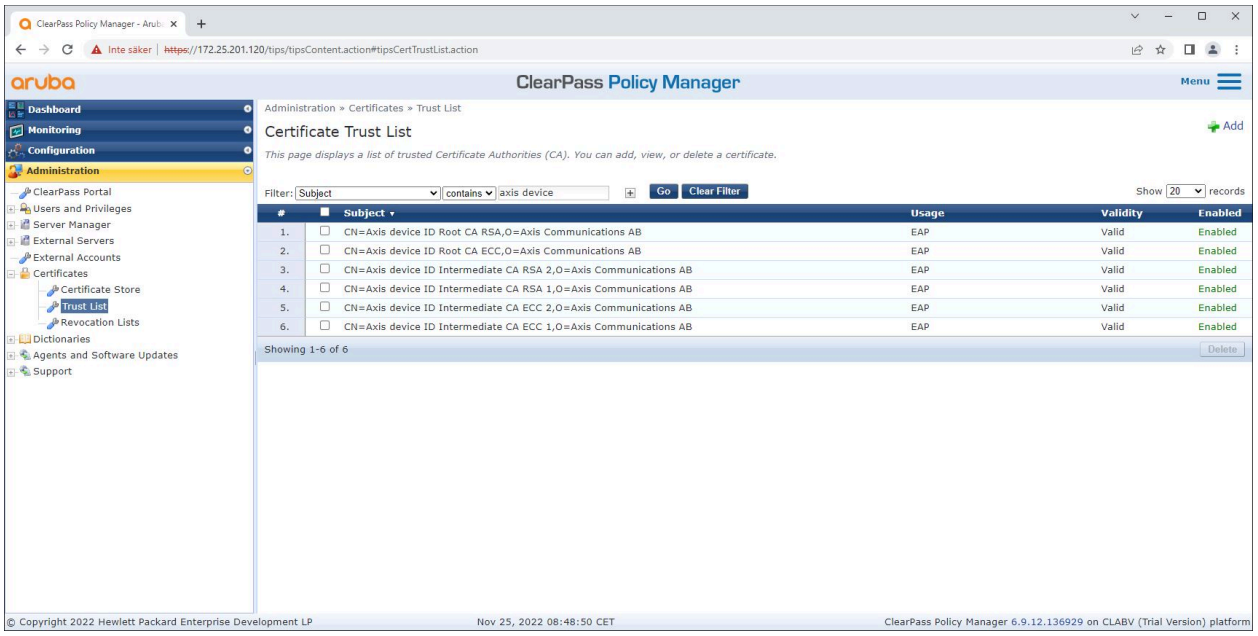
ClearPass Policy Manager zapewnia opartą na rolach i urządzeniach bezpieczną kontrolę dostępu do sieci dla IoT, BYOD, urządzeń firmowych, pracowników, wykonawców i gości w ramach infrastruktury przewodowej, bezprzewodowej i VPN wielu dostawców.

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 użytkowania wybierz opcję EAP. Certyfikaty są używane do uwierzytelniania IEEE 802.1X EAP-TLS.



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



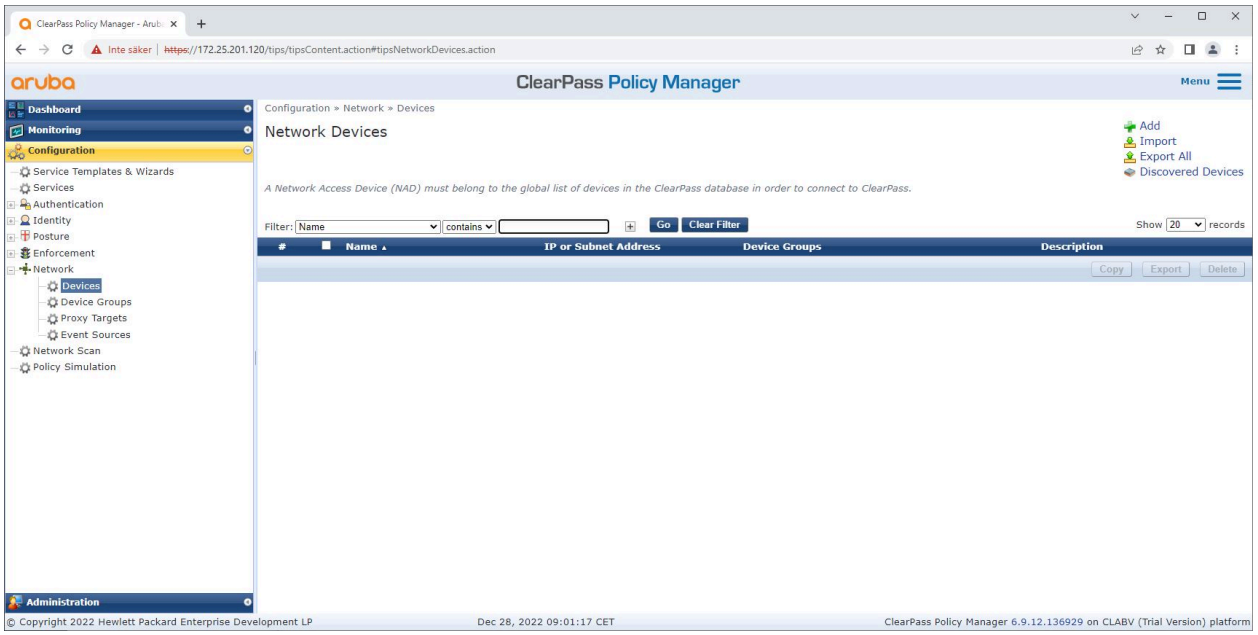
Zaufany magazyn certyfikatów w narzędziu ClearPass Policy Manager z dołączonym łańcuchem certyfikatów IEEE 802.1AR firmy Axis.

Konfiguracja urządzenia/grupy sieciowej

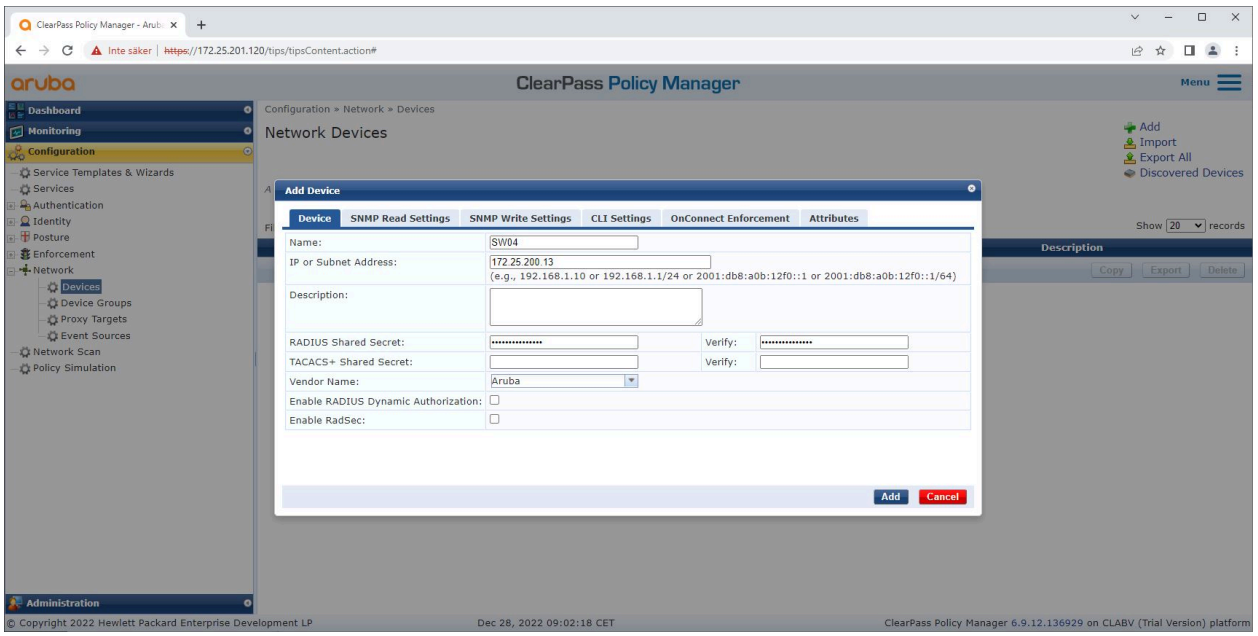
1. Dodawanie zaufanych urządzeń dostępu do sieci, takich jak switche dostępowe HPE Aruba Networking, do narzędzia ClearPass Policy Manager. Menedżer zasad ClearPass Policy Manager musi wiedzieć, które switche dostępowe w sieci są używane do komunikacji IEEE 802.1X.

2. Konfiguracja grupy urządzeń sieciowych służy do grupowania kilku zaufanych urządzeń dostępu do sieci. Grupowanie zaufanych urządzeń dostępu do sieci ułatwia konfigurację zasad.

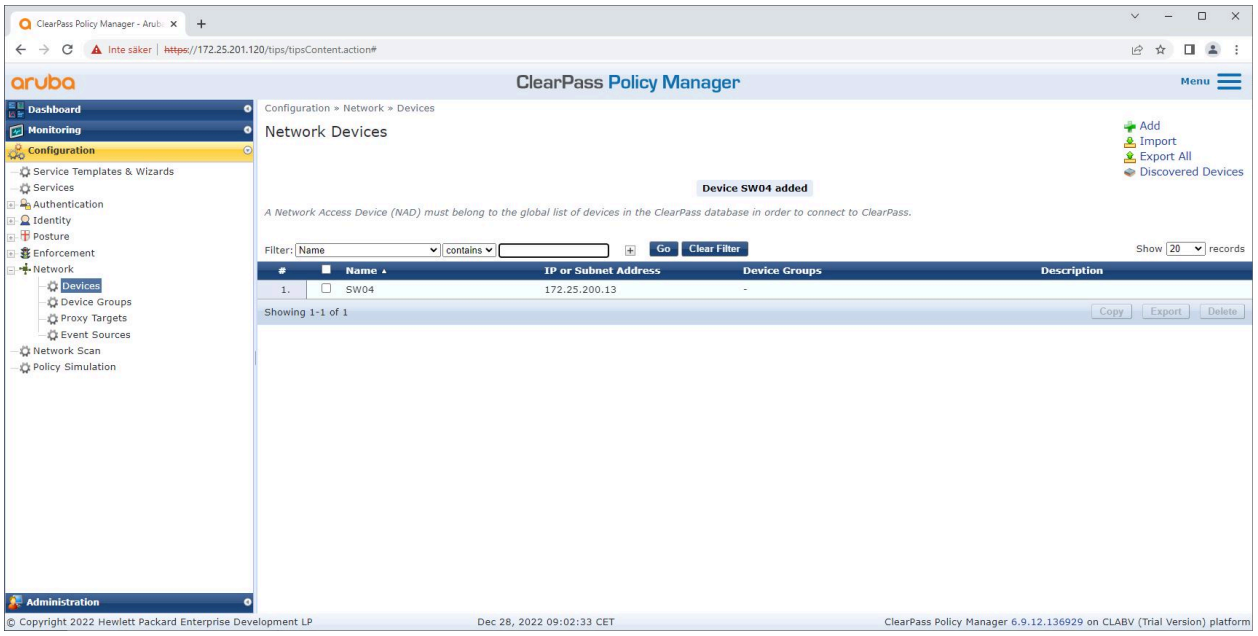
3. Współdzielony sekret RADIUS musi być zgodny z określoną konfiguracją switcha IEEE 802.1X.



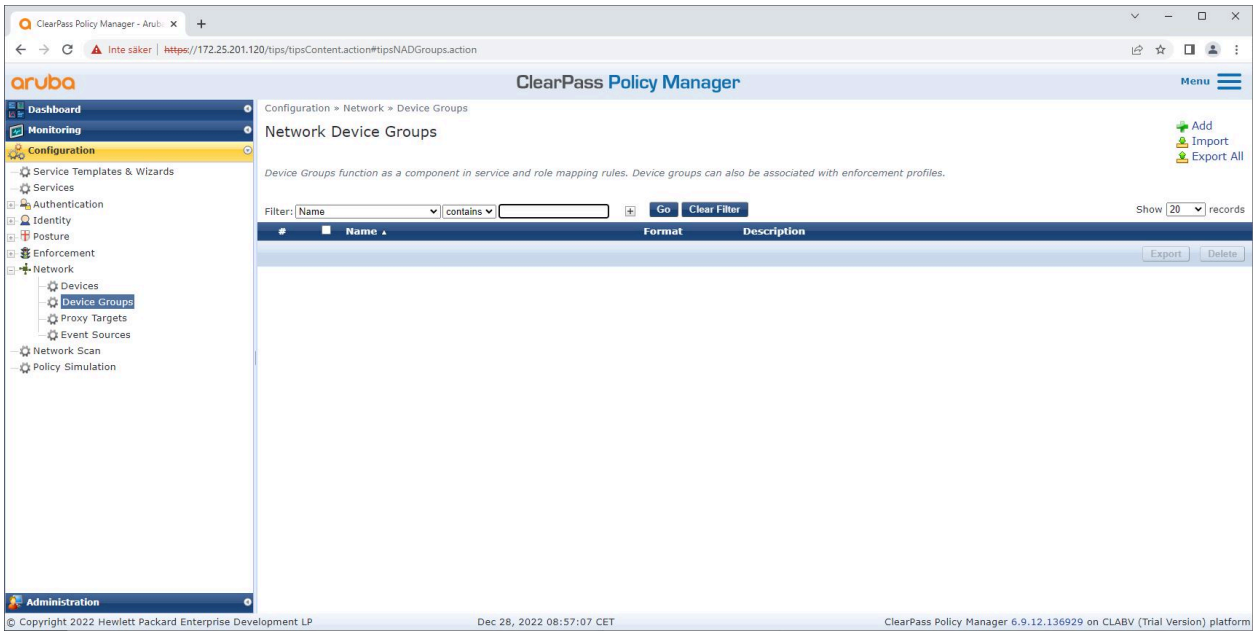
Interfejs zaufanych urządzeń sieciowych w narzędziu ClearPass Policy Manager.



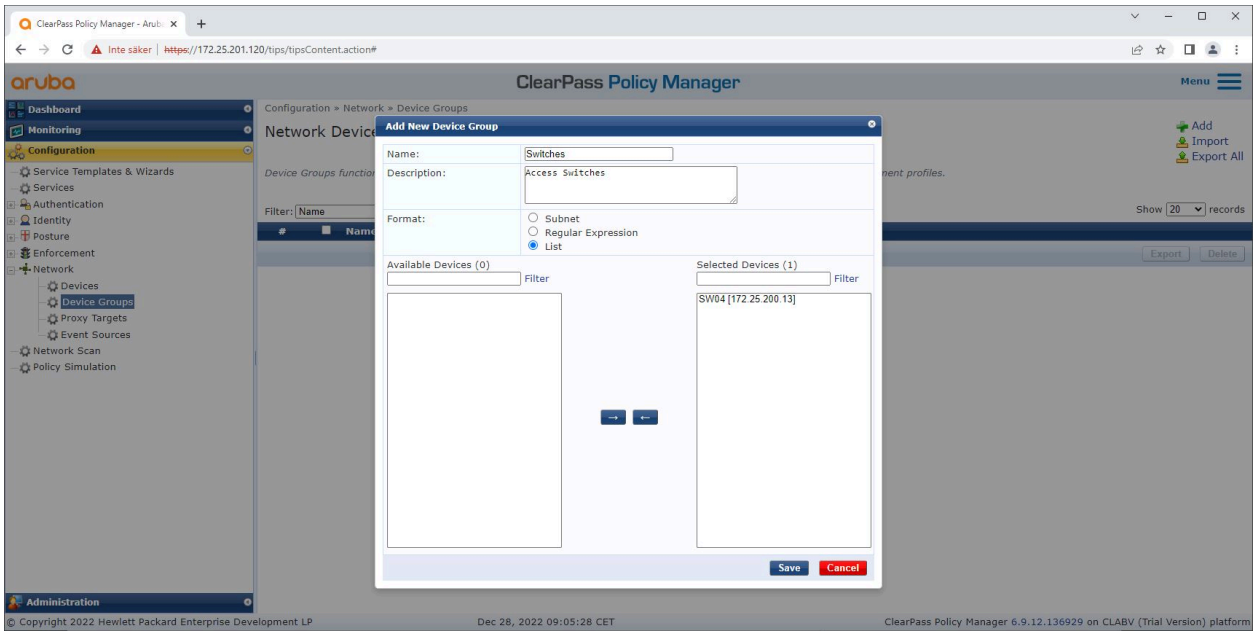
Dodawanie switcha dostępowego HPE Aruba Networking jako zaufanego urządzenia sieciowego w narzędziu ClearPass Policy Manager. Uwaga: współdzielony sekret RADIUS musi odpowiadać konkretnej konfiguracji switcha IEEE 802.1X.



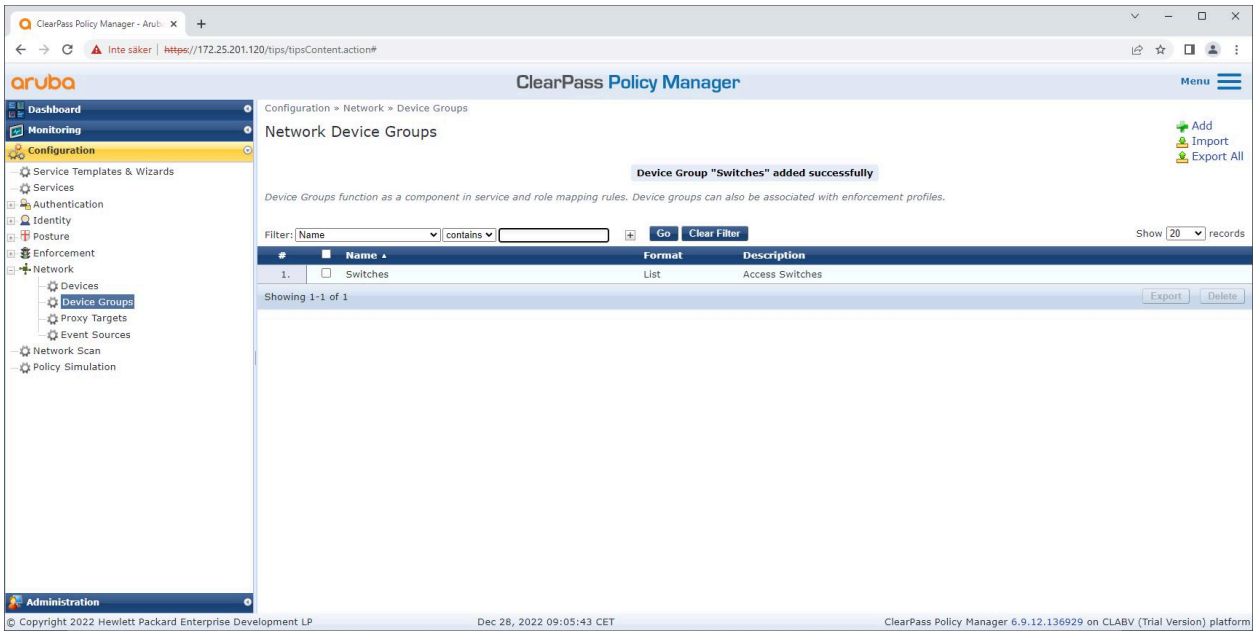
ClearPass Policy Manager ze skonfigurowanym jednym zaufanym urządzeniem sieciowym.



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.



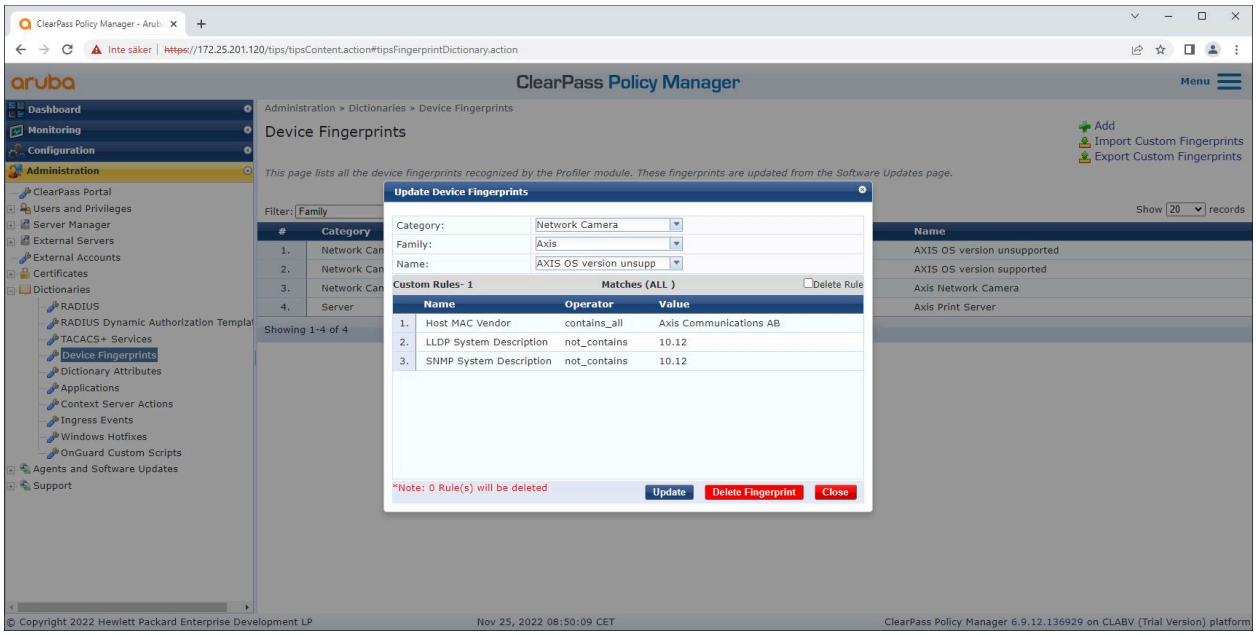
ClearPass Policy Manager ze skonfigurowaną grupą urządzeń sieciowych, która zawiera jedno lub kilka zaufanych urządzeń sieciowych.

Konfiguracja odcisku palca urządzenia

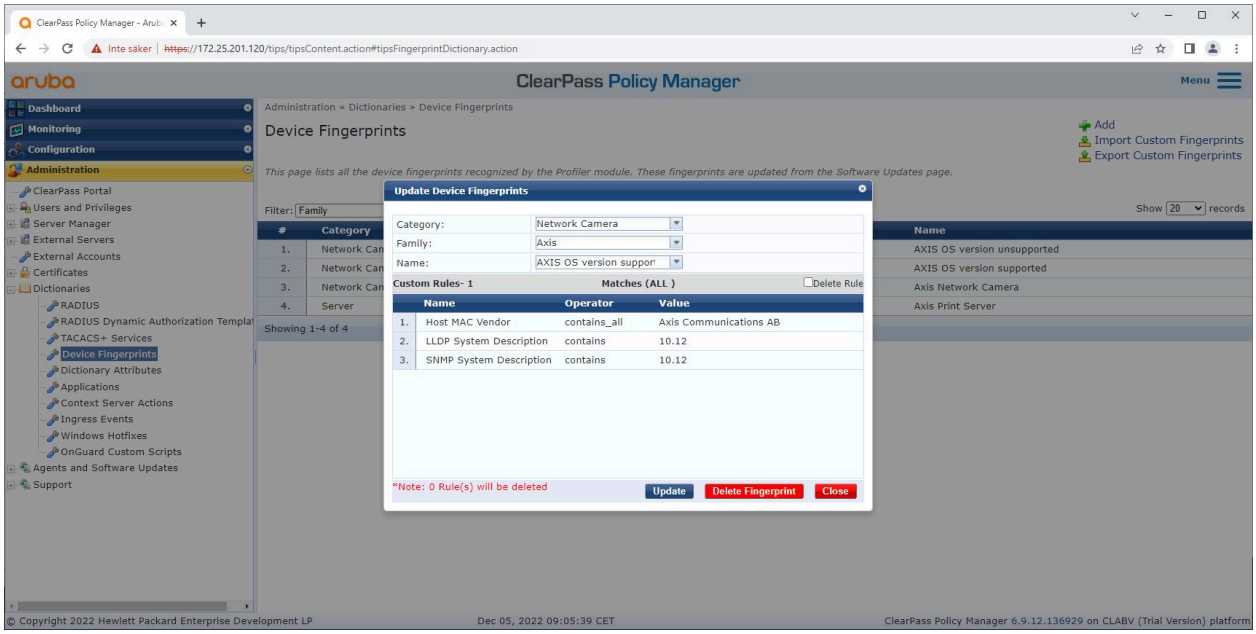
Urządzenie Axis może poprzez wykrywanie sieci dystrybuować specyficzne dla siebie informacje, takie jak adres MAC i wersja oprogramowania urządzenia. Informacje te można wykorzystywać do tworzenia i aktualizowania odcisku palca urządzenia oraz zarządzania nim w programie ClearPass Policy Manager. Można tam 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. Skonfiguruj ustawienia odcisku palca urządzenia.



Konfiguracja odcisku palca urządzenia w narzędziu ClearPass Policy Manager. Urządzenia Axis z wersją systemu operacyjnego AXIS OS inną niż 10.12 są uznawane za nieobsługiwane.



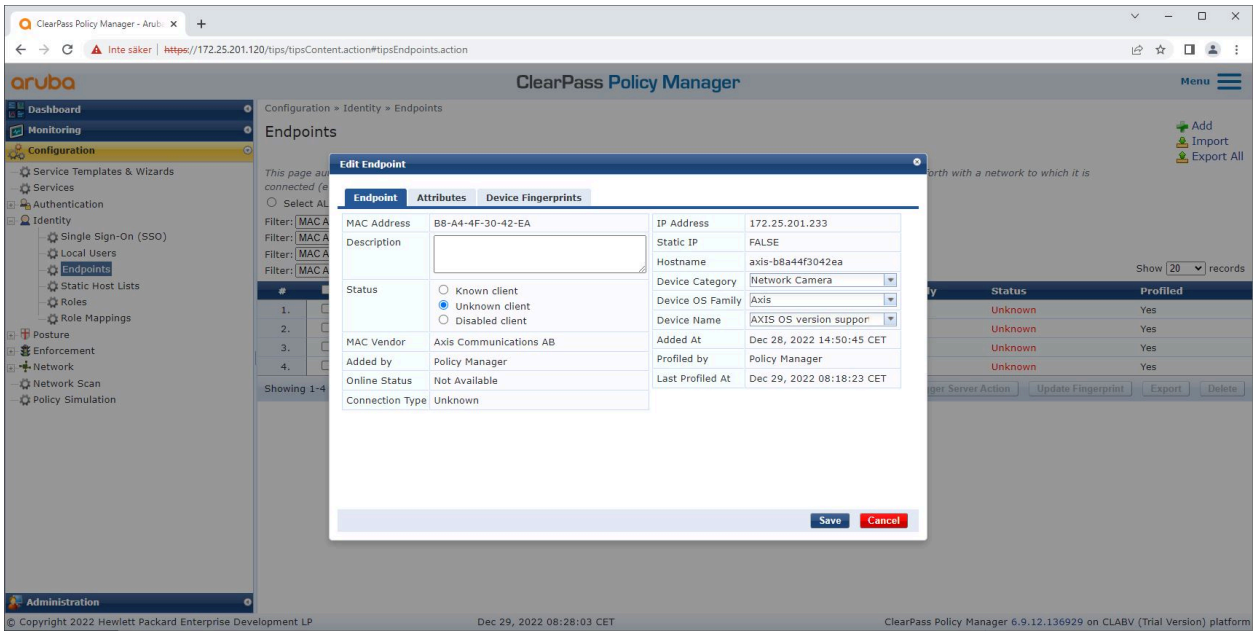
Konfiguracja odcisku palca urządzenia w narzędziu ClearPass Policy Manager. W powyższym przykładzie urządzenia Axis z systemem operacyjnym AXIS OS 10.12 są uważane za obsługiwane.

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

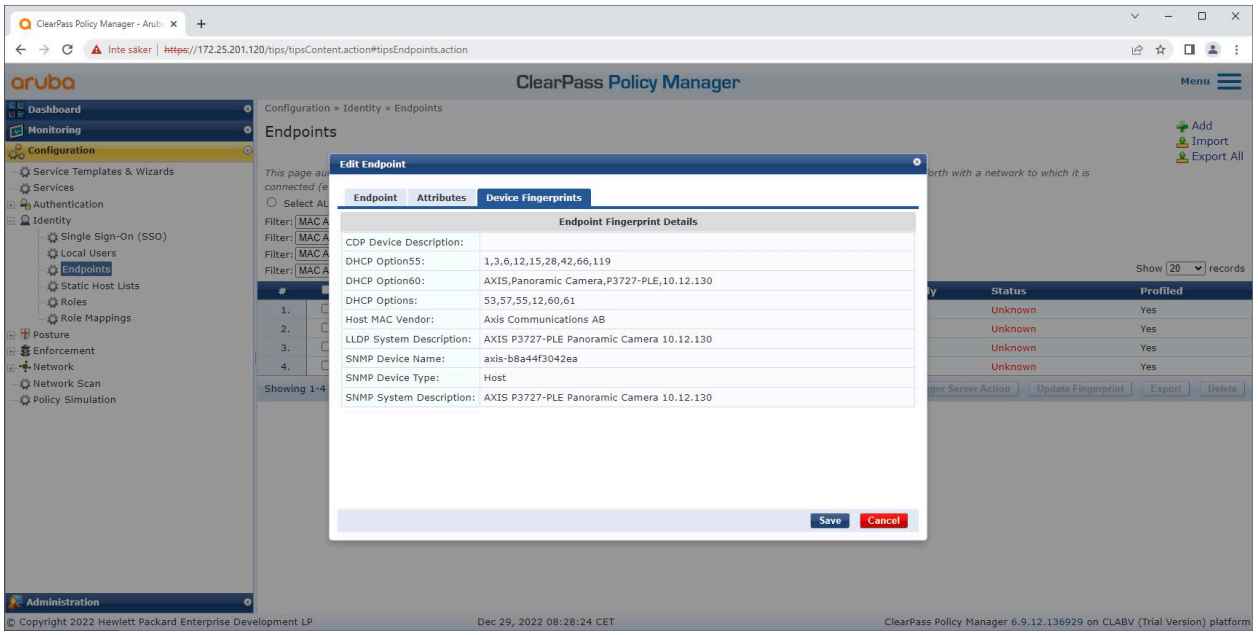
1. Otwórz menu **Configuration > Identity > Endpoints (Konfiguracja > Tożsamość > Punkty końcowe)**.
2. Wybierz urządzenia, które chcesz wyświetlić.
3. Kliknij kartę **Device Fingerprints (Odciski palca urządzenia)**.

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.

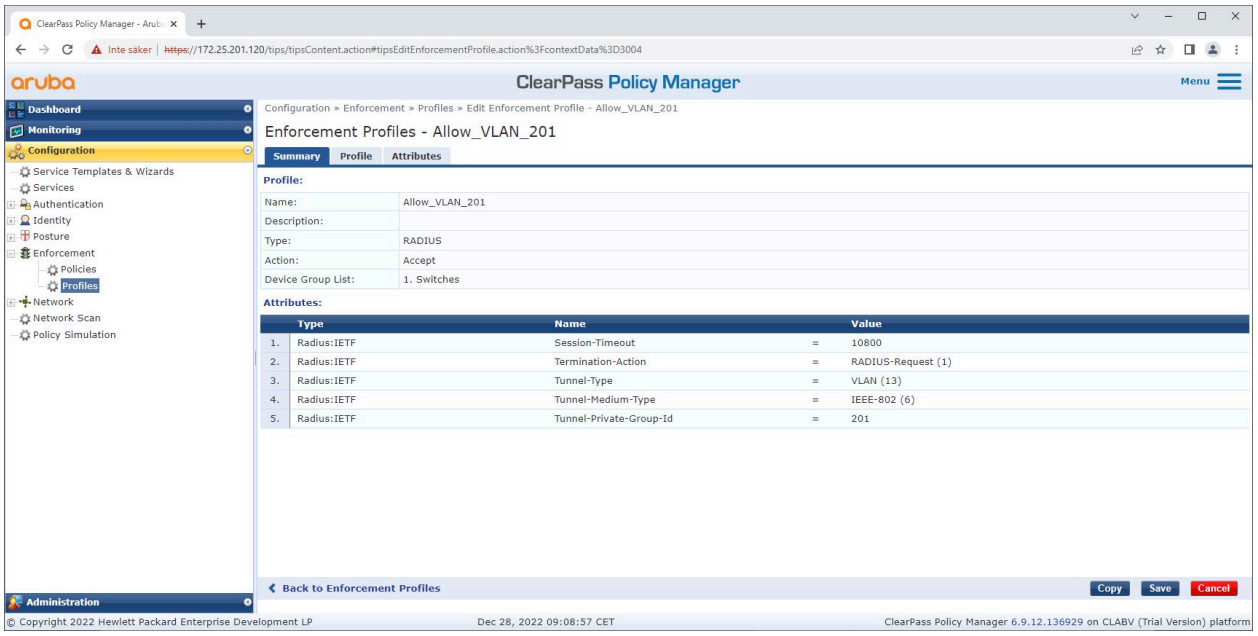


Szczegółowe odciski palców sprofilowanego urządzenia Axis. Uwaga: protokół SNMP jest domyślnie wyłączony w urządzeniach Axis. Informacje LLDP, CDP i specyficzne dla DHCP są udostępniane przez urządzenie Axis w formie domyślnych ustawień fabrycznych i przekazywane przez switch dostępowy HPE Aruba Networking do narzędzia ClearPass Policy Manager.

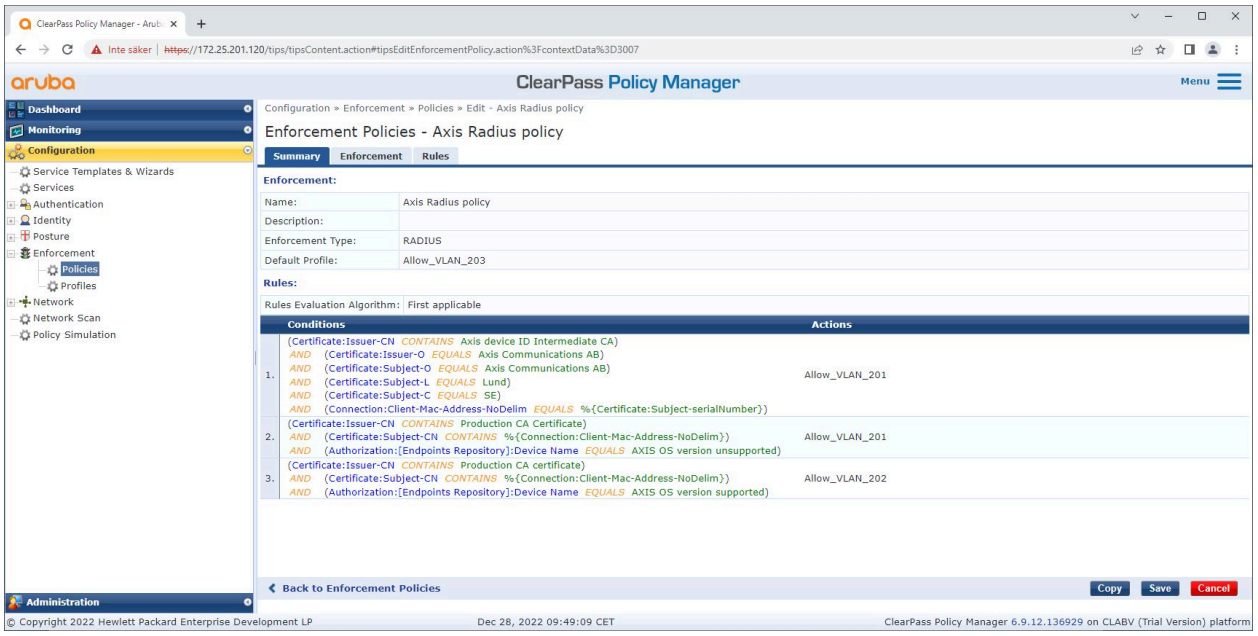
Konfiguracja profilu wykonywania

Za pomocą **profilu wykonywania** ClearPass Policy Manager może przypisywać określony identyfikator sieci VLAN do portu dostępu na switchu. Decyzja ta jest oparta na zasadach i ma zastosowanie do urządzeń sieciowych w grupie „switche". Niezbędna liczba profili wykonywania zależy od liczby używanych sieci VLAN. W naszej konfiguracji znajdują się w sumie trzy sieci VLAN (VLAN 201, 202, 203), co odpowiada trzem profilom wykonywania.

Właściwe 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. Do podjęcia odpowiednich działań wymagana jest ręczna inspekcja urządzenia.

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

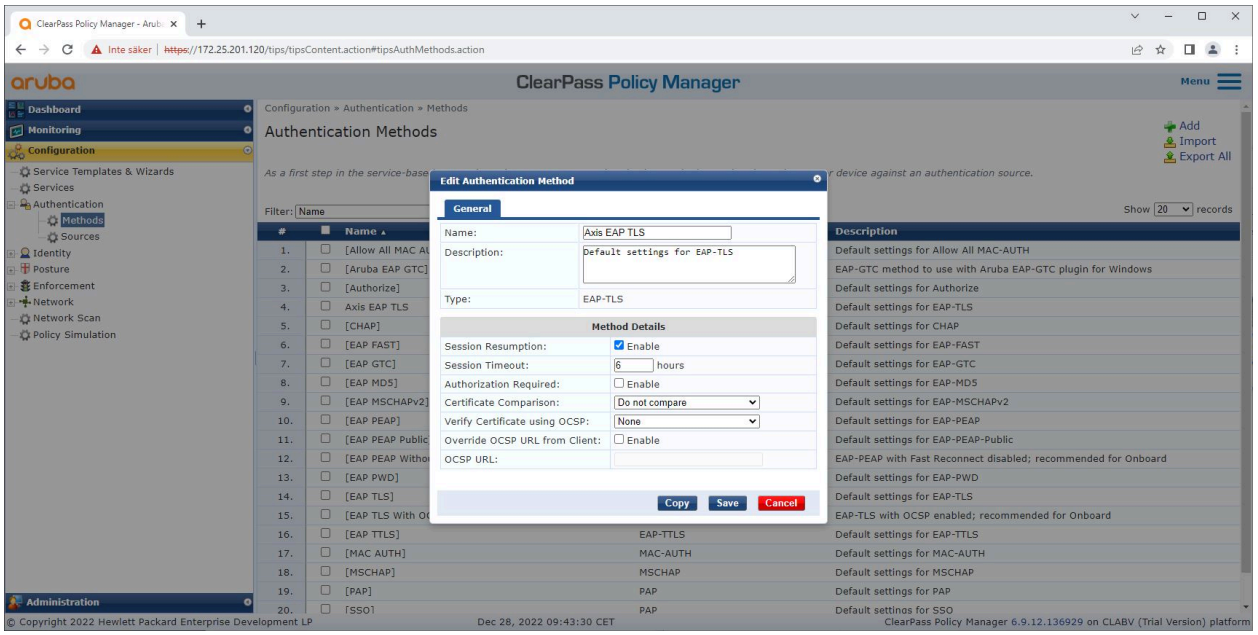
Sieć produkcyjna (VLAN 202)

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

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

Konfiguracja metody uwierzytelniania

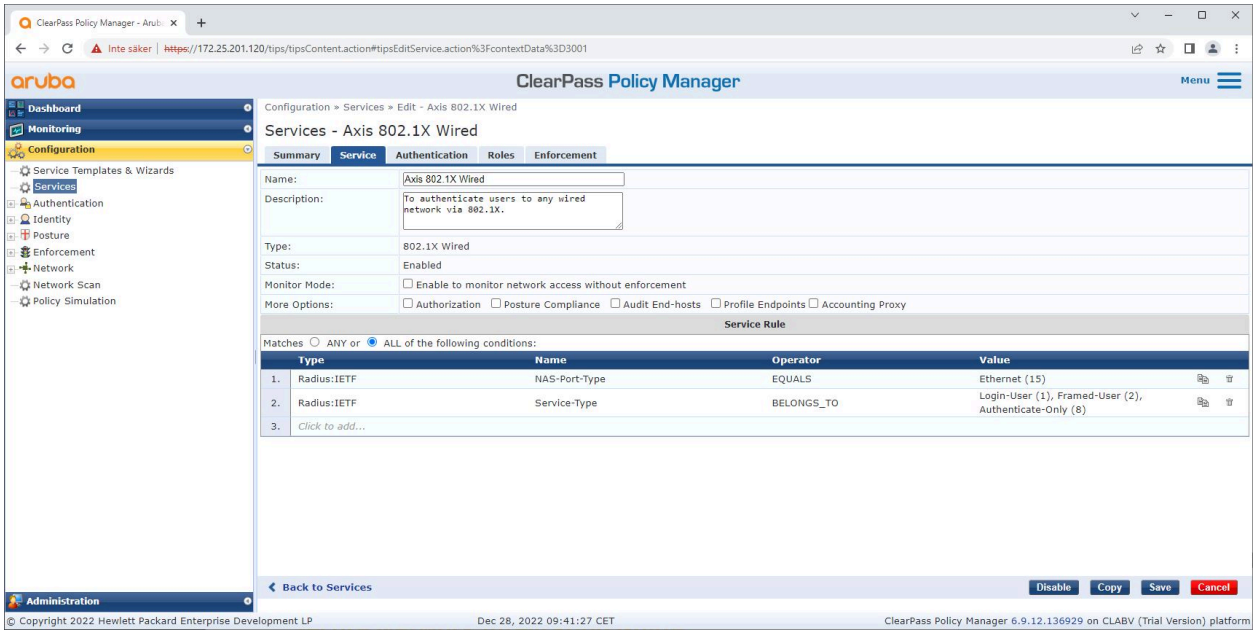
W metodzie uwierzytelniania określa się, w jaki sposób urządzenie Axis próbuje uwierzytelnić się w sieci. Preferowaną metodą uwierzytelniania powinna być IEEE 802.1X EAP-TLS, ponieważ urządzenia Axis z obsługą Axis Edge Vault mają domyślnie włączoną funkcję IEEE 802.1X EAP-TLS.



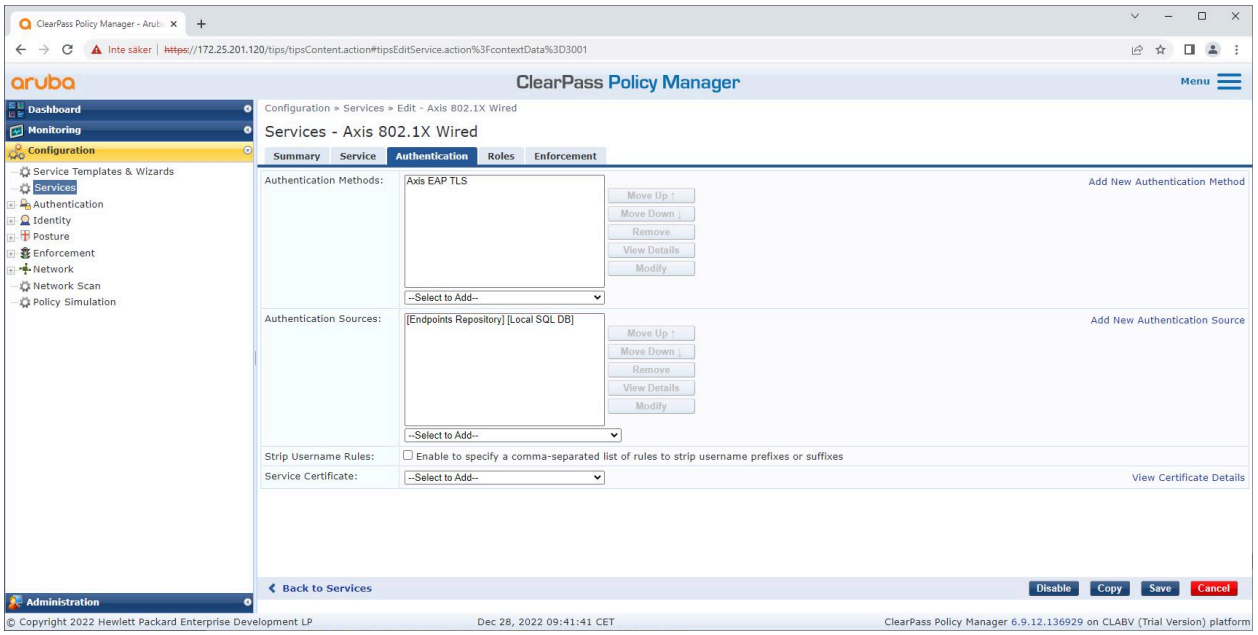
Interfejs metody uwierzytelniania narzędzia ClearPass Policy Manager, w którym zdefiniowana jest metoda uwierzytelniania EAP-TLS dla urządzeń Axis.

Konfiguracja usług

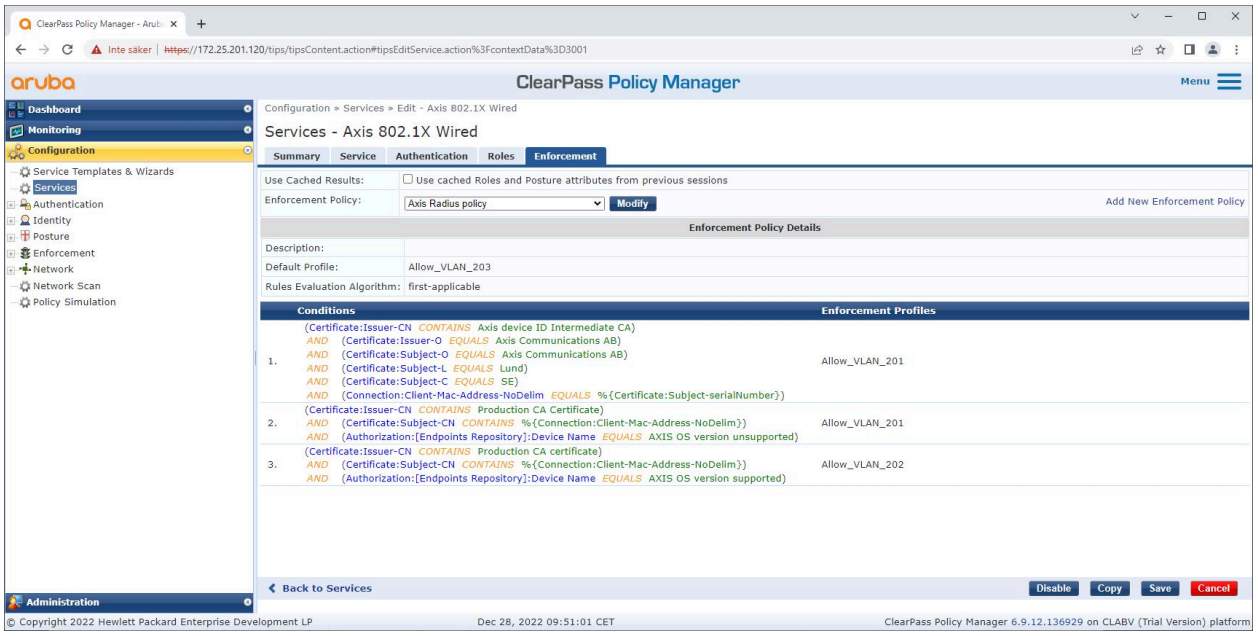
Na stronie **Services (Usługi)** kroki konfiguracji są połączone w jedną usługę, która obsługuje uwierzytelnianie i autoryzację urządzeń Axis w sieciach HPE Aruba Networking.



Tworzone są dedykowane usługi Axis definiujące standard IEEE 802.1X jako metodę łączności.



W kolejnym kroku następuje konfiguracja wcześniej utworzonej metody uwierzytelniania EAP-TLS pod kątem usługi.



W ostatnim kroku następuje skonfigurowanie dla usługi wcześniej utworzonej polityki wykonywania.

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 do 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.

Zapoznaj się z poniższym przykładem konfiguracji globalnej i konfiguracji portów dla switchy dostępowych HPE Aruba Networking.

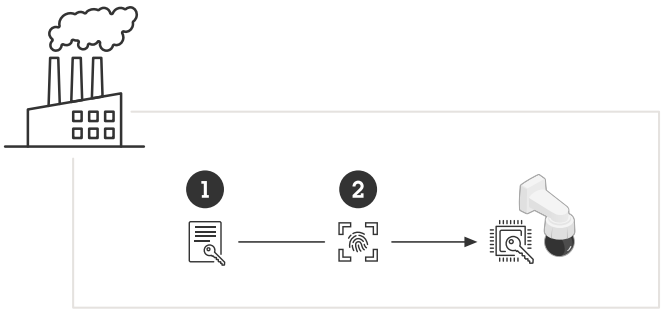
```
radius-server host MyRADIUSIPAddress key "MyRADIUSKey"

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

Konfiguracja Axis

Urządzenie sieciowe Axis

Urządzenia Axis obsługujące *Axis Edge Vault* są fabrycznie wyposażone w bezpieczną tożsamość urządzenia, zwaną identyfikatorem urządzenia Axis. Identyfikator urządzenia Axis jest oparty na międzynarodowym standardzie IEEE 802.1AR. Standard ten określa metodę zautomatyzowanej, bezpiecznej identyfikacji urządzeń i włączania do sieci za pośrednictwem IEEE 802.1X.



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

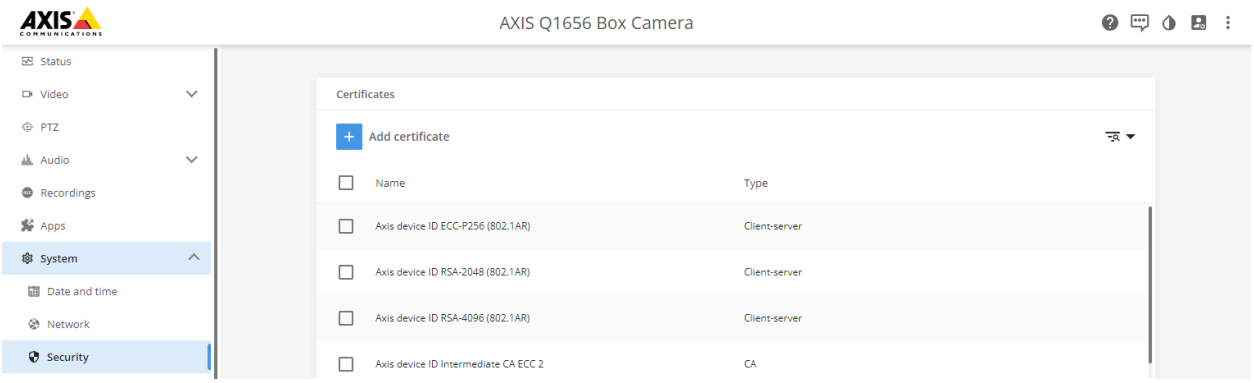
1 *Infrastruktura kluczy identyfikacyjnych urządzeń Axis (PKI)*
2 *ID urządzenia Axis*

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 zorientowaniu się, które urządzenia Axis obsługują Axis Edge Vault i identyfikator urządzenia Axis.

Uwaga

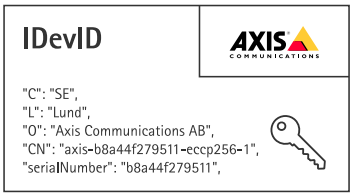
Numer seryjny urządzenia Axis jest jednocześnie jego adresem MAC.

Bezpieczne wdrożenie — IEEE 802.1AR/802.1X



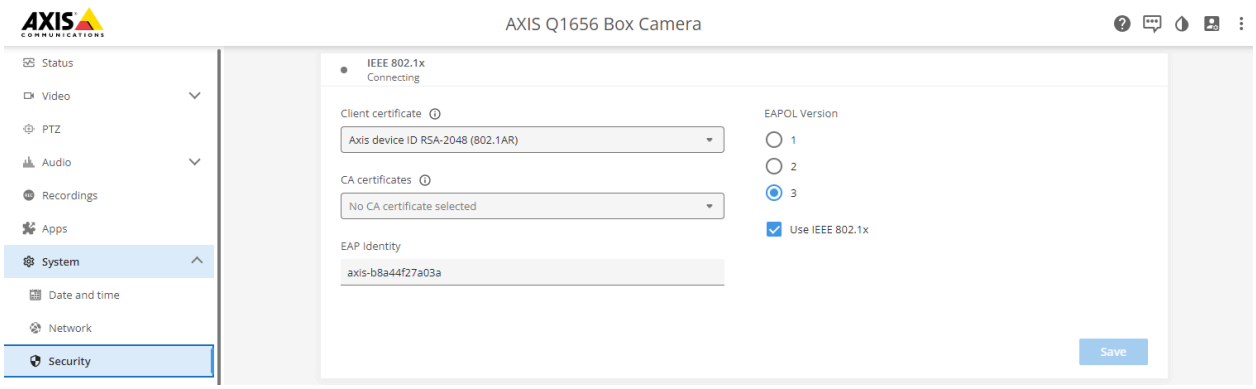
Magazyn certyfikatów urządzenia Axis w domyślnym stanie fabrycznym z identyfikatorem urządzenia Axis.

Certyfikat ID urządzenia Axis zgodny z IEEE 802.1AR zawiera informacje o numerze seryjnym i inne informacje specyficzne dla dostawcy Axis. ClearPass Policy Manager analizuje te informacje i podejmuje decyzję o przyznaniu dostępu do sieci. Poniżej przedstawiono informacje, które można uzyskać z certyfikatu identyfikacyjnego 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 jest tworzona przez połączenie nazwy firmy Axis, numeru seryjnego urządzenia, a następnie używanego 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 Axis 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 konfigurowania wielu urządzeń Axis i zarządzania nimi w ekonomiczny sposób. AXIS Device Manager to aplikacja oparta na Microsoft Windows®, którą można zainstalować lokalnie na komputerze w sieci, natomiast AXIS Device Manager Extend opiera się na infrastrukturze chmurowej i służy do zarządzania urządzeniami w wielu lokalizacjach. Oba te rozwiązania zapewniają łatwe konfigurowanie urządzeń Axis (i zarządzanie nimi), takich jak:

- Instalowanie aktualizacji systemu operacyjnego AXIS OS.
- Zastosuj konfigurację cyberbezpieczeństwa, taką jak HTTPS i certyfikaty 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.

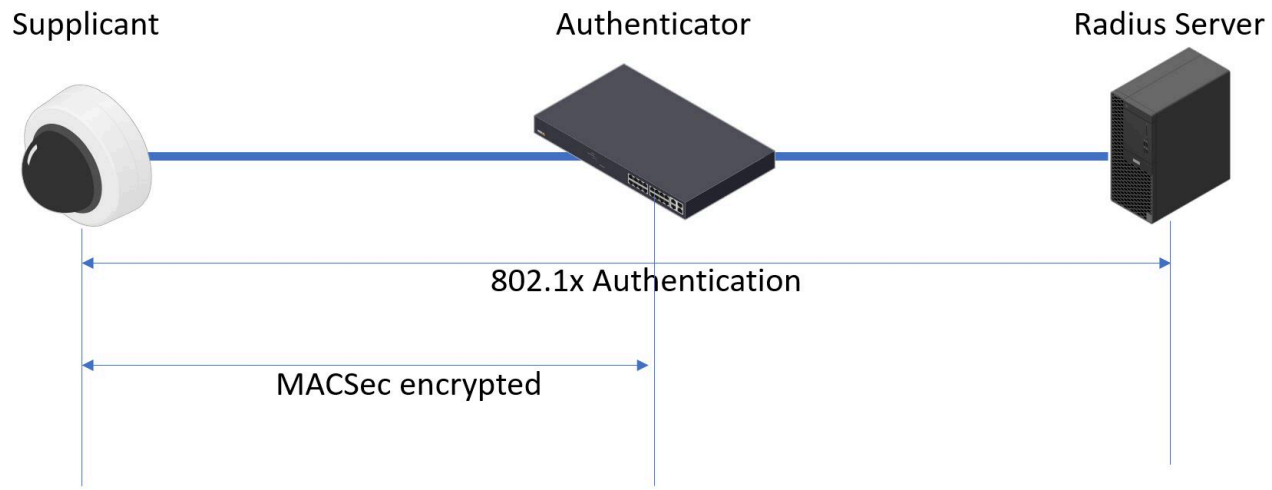
help.axis.com/?&tpiaId=&tsection=secure-network-operation-ieee-802-1ae-macsec

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 10.1 (2020-09) i nowszych IEEE 802.1X jest domyślnie włączony dla urządzeń zgodnych z identyfikatorem urządzenia Axis. W systemie AXIS OS 11.8 i nowszych obsługujemy MACsec przy użyciu automatycznego trybu dynamicznego za pomocą domyślnie włączonego IEEE 802.1X EAP-TLS. 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

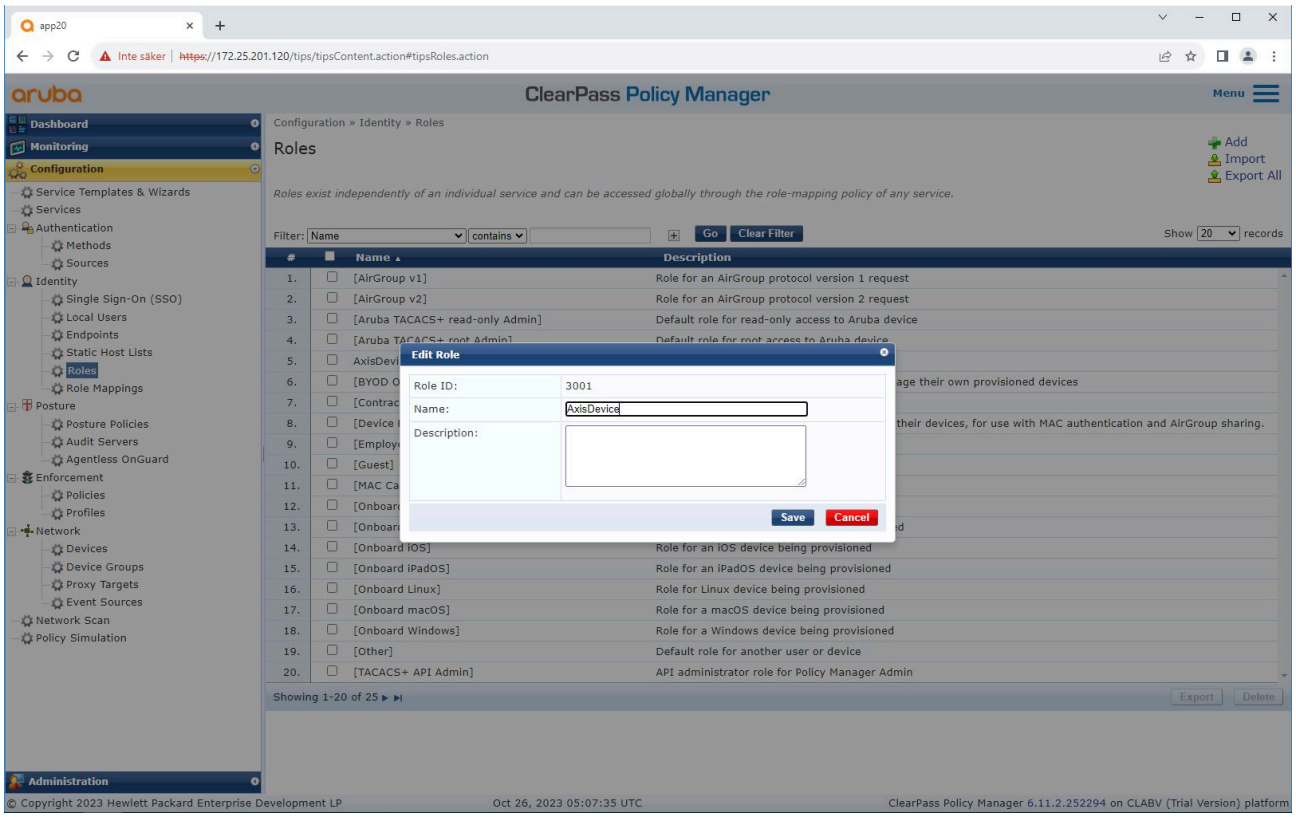
całej sesji EAP-TLS automatycznie wymieniane są klucze MACsec, aby ustanowić bezpieczne połączenie (3), chroniąc cały ruch w sieci do urządzenia Axis do switcha HPE Aruba Networking.

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.

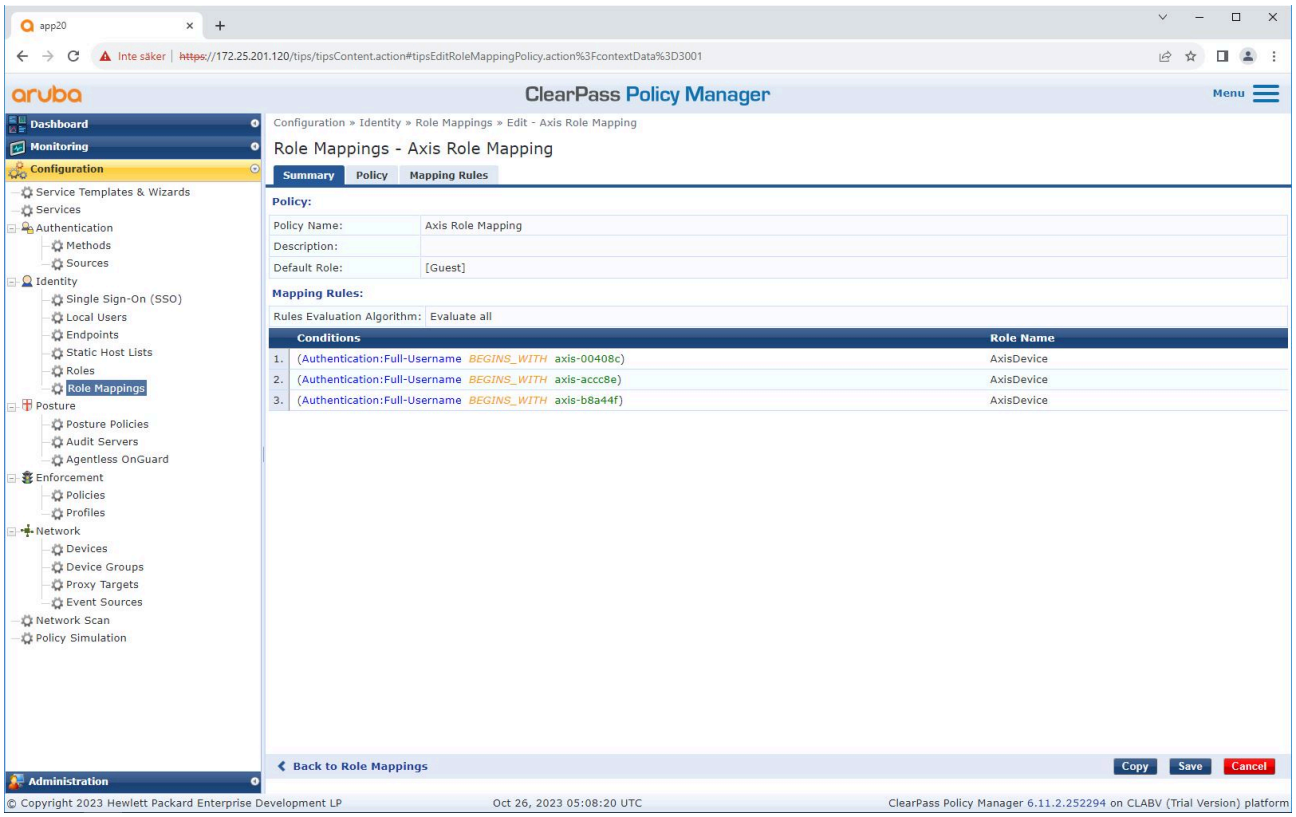
Jeśli switch dostępowy HPE Aruba Networking nie obsługuje szyfrowania MACsec przez EAP-TLS, można użyć trybu klucza PSK i skonfigurować ręcznie.

HPE Aruba Networking ClearPass Policy Manager

Role i zasady mapowania ról



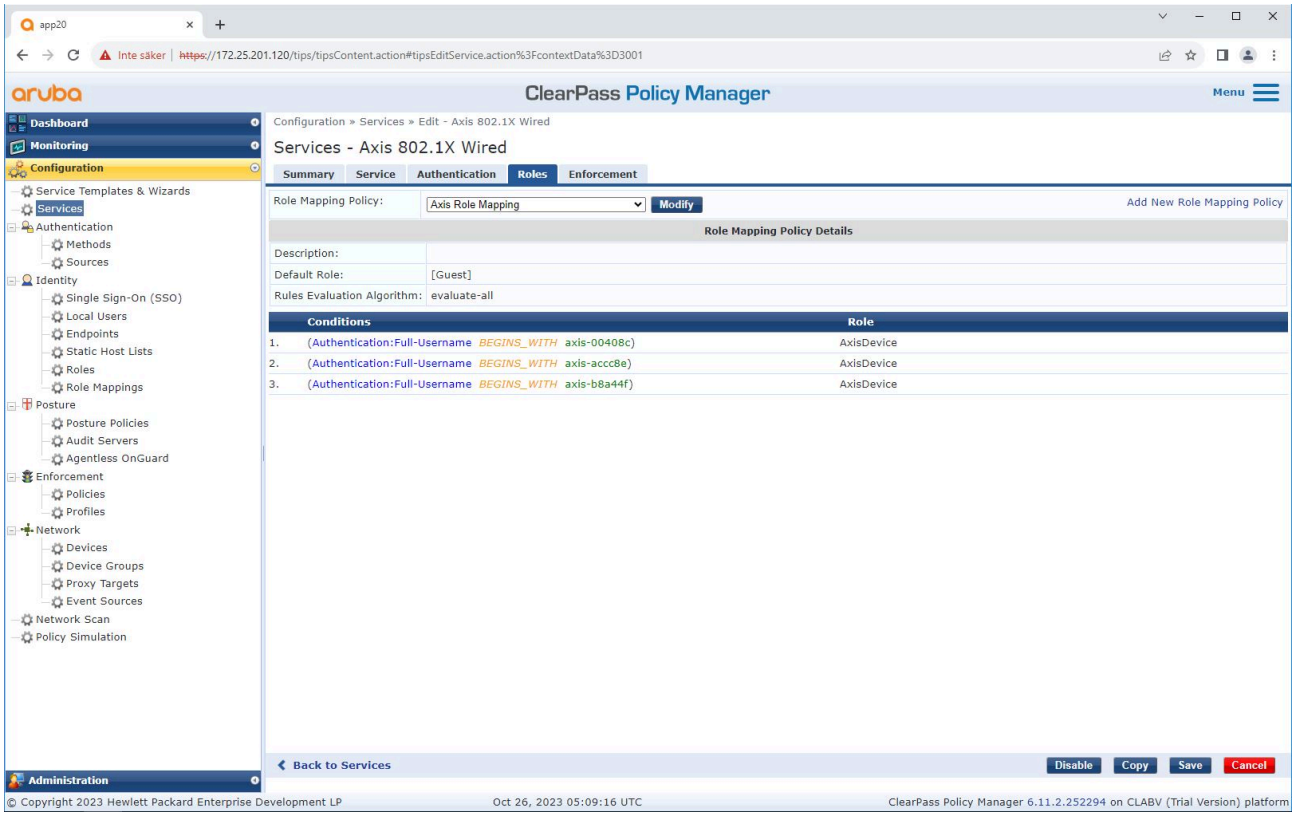
Dodawanie nazwy roli dla urządzeń Axis. Nazwa jest nazwą roli dostępu do portu w konfiguracji switcha dostępowego.



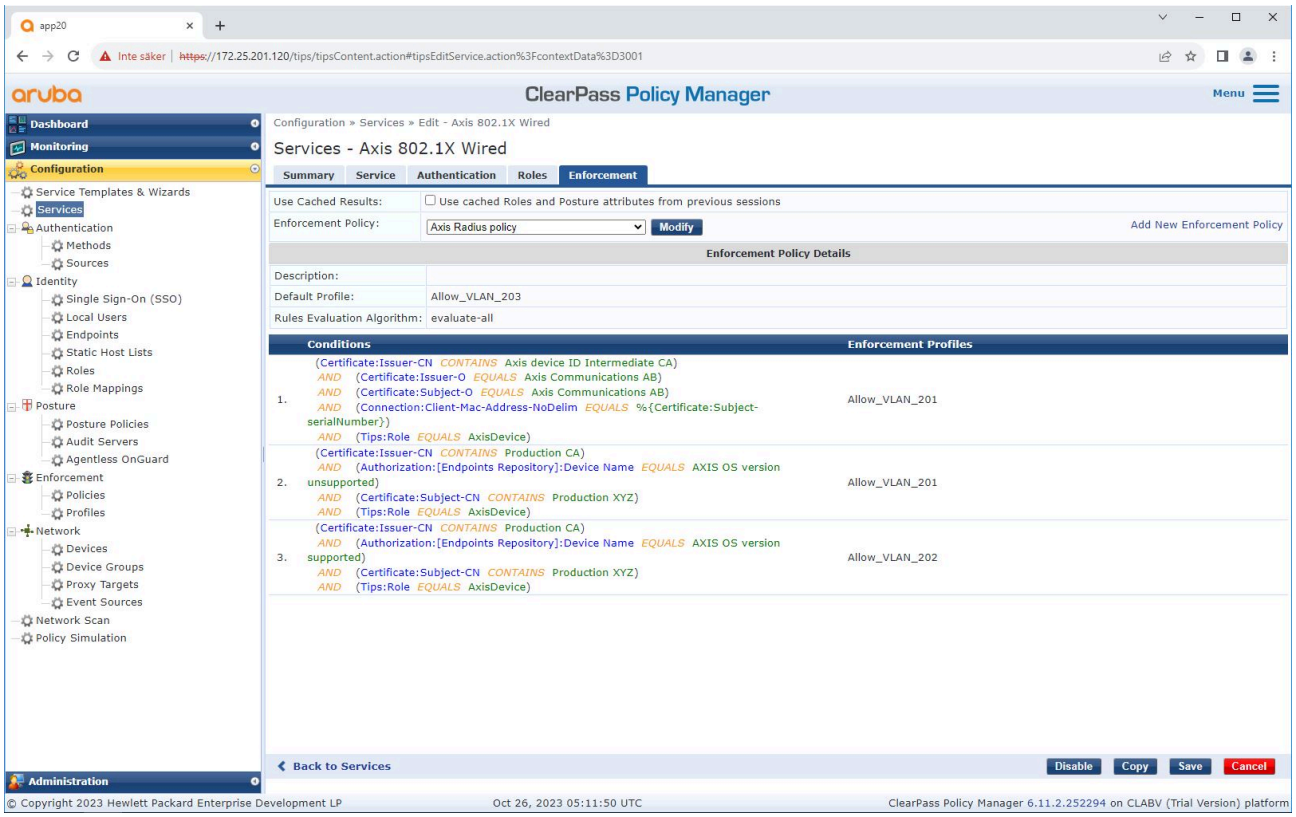
Dodawanie zasad mapowania ról Axis dla wcześniej utworzonej roli urządzenia Axis. Spełnienie określonych warunków jest wymagane, aby urządzenie mogło zostać zmapowane do roli urządzenia Axis. Jeśli warunki nie zostaną spełnione, urządzenie będzie częścią roli [Guest] (gość).

Domyślnie urządzenia Axis używają formatu tożsamości EAP „numer seryjny Axis". Numer seryjny urządzenia Axis jest jednocześnie jego adresem MAC. Na przykład: „axis-b8a44f45b4e6".

Konfiguracja usług

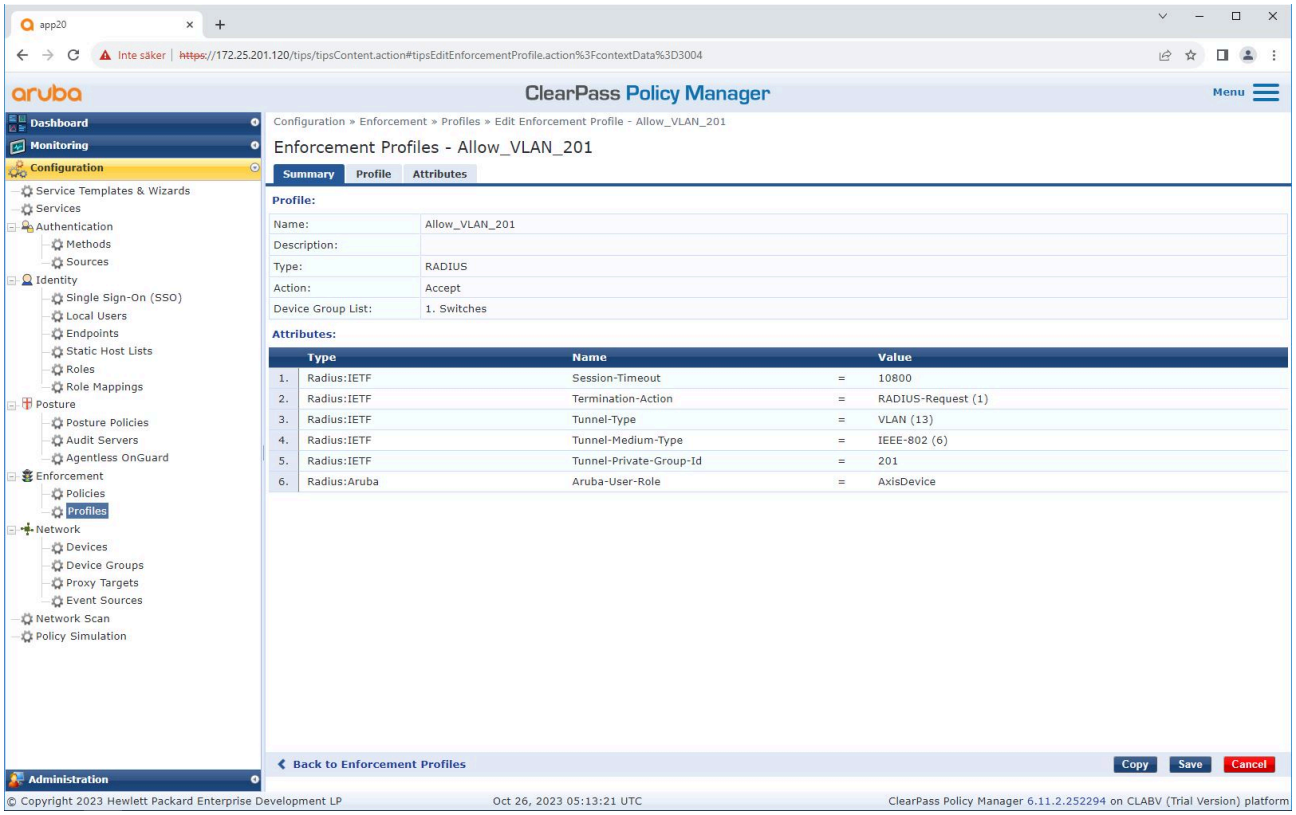


Dodawanie wcześniej utworzonej zasady mapowania ról Axis do usługi, która definiuje standard IEEE 802.1X jako metodę łączenia w przypadku wdrażania urządzeń Axis.



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-eap
cipher-suite gcm-aes-128

port-access role AxisDevice
associate macsec-policy macsec-eap
auth-mode client-mode

aaa authentication port-access dot1x authenticator
macsec
mkacak-length 16
enable
```

Wdrażanie starszej wersji — uwierzytelnianie MAC

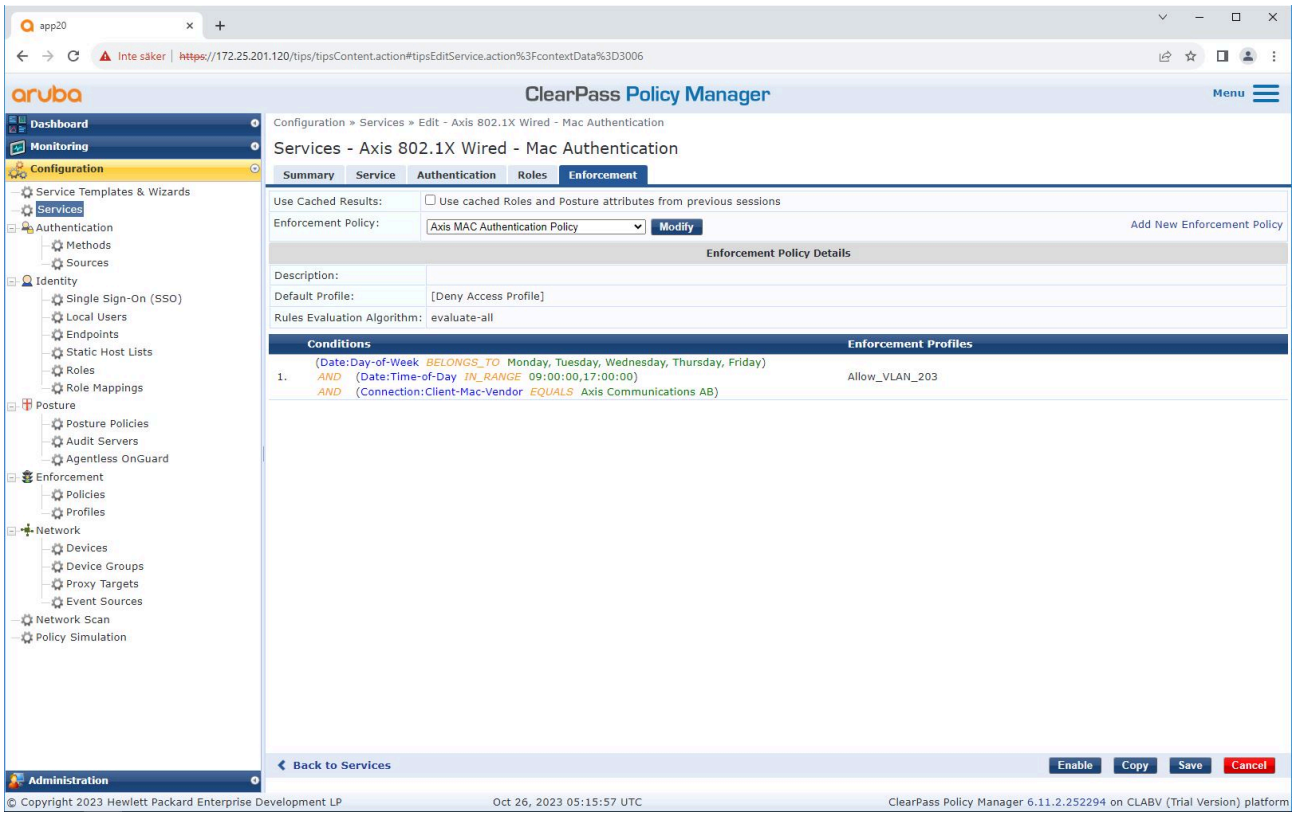
Za pomocą MAC Authentication Bypass (MAB) możesz wdrażać urządzenia Axis, które nie obsługują wdrażania IEEE 802.1AR z certyfikatem identyfikatora urządzenia Axis i włączonym IEEE 802.1X z ustawieniami fabrycznymi. Jeśli wdrożenie standardu 802.1X nie powiedzie się, ClearPass Policy Manager zweryfikuje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

MAB wymaga przygotowań do konfiguracji switcha dostępowego i narzędzia ClearPass Policy Manager. Aby umożliwić wdrożenie MAB, na urządzeniu Axis nie jest wymagana żadna konfiguracja.

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

Gdy 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:

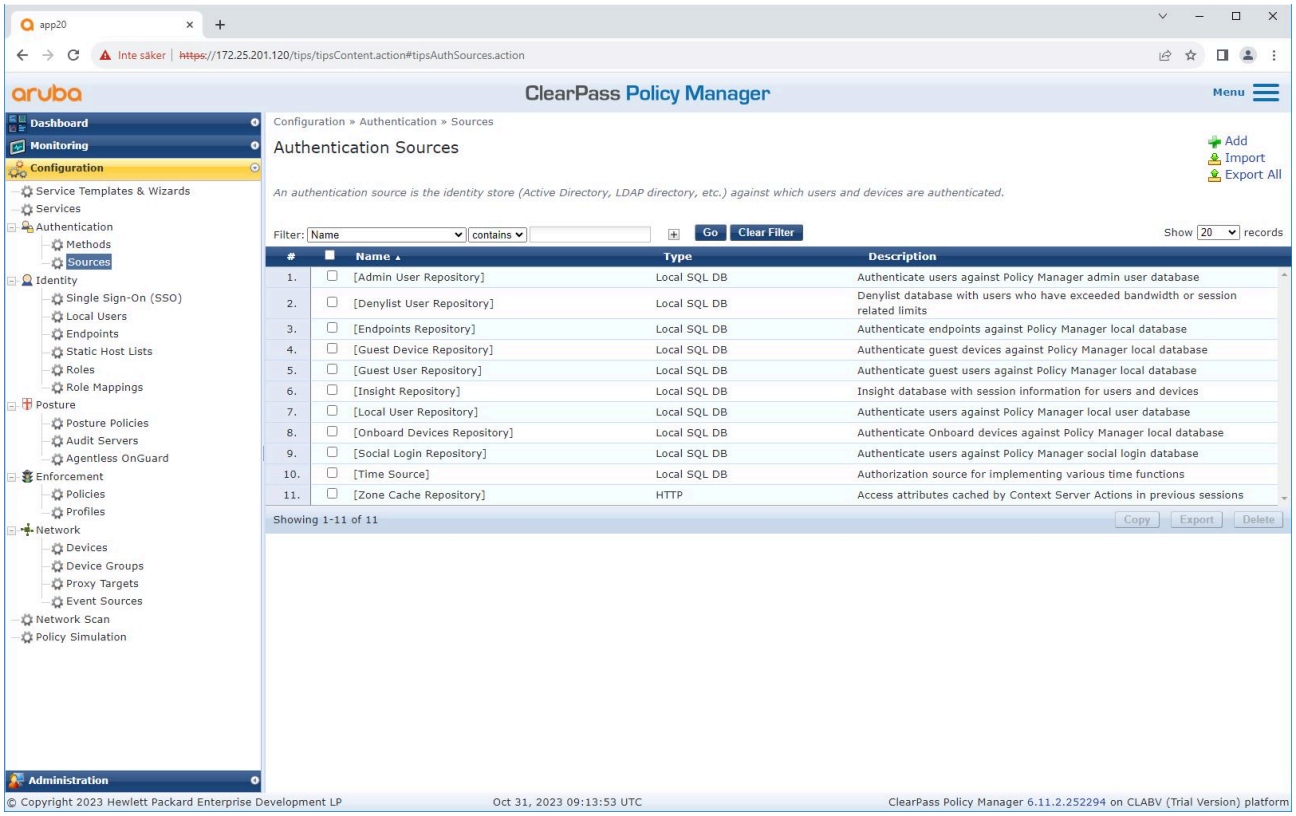
- Jest dzień powszedni (od poniedziałku do piątku)
- Jest godzina od 09:00 do 17:00

- Dostawca adresu MAC jest zgodny z Axis Communications.

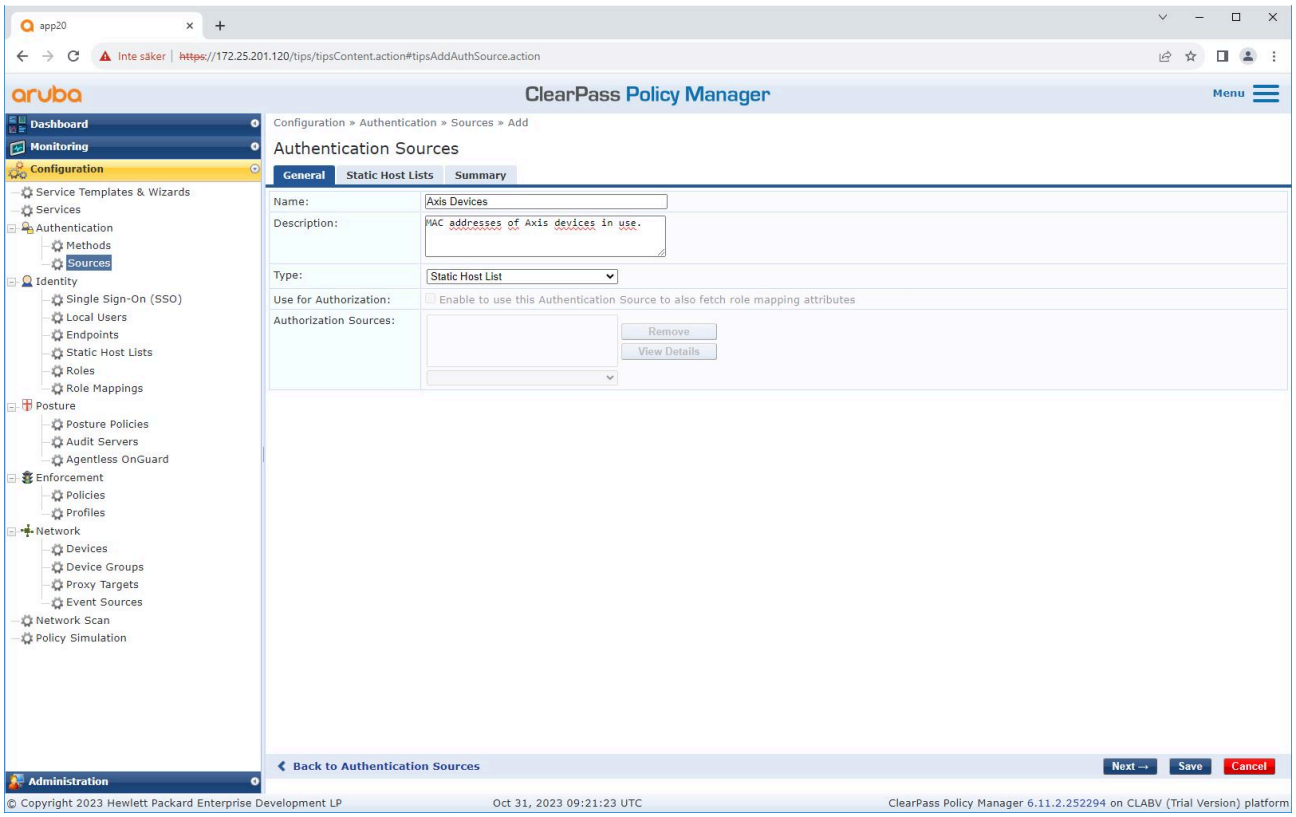
Ze względu na ryzyko sfałszowania adresów MAC dostęp do zwykłej sieci administracyjnej nie jest przyznawany. Zalecamy korzystanie z MAB tylko do wstępnego wdrożenia i ręczne sprawdzanie urządzenia w przyszłości.

Konfiguracja źródła

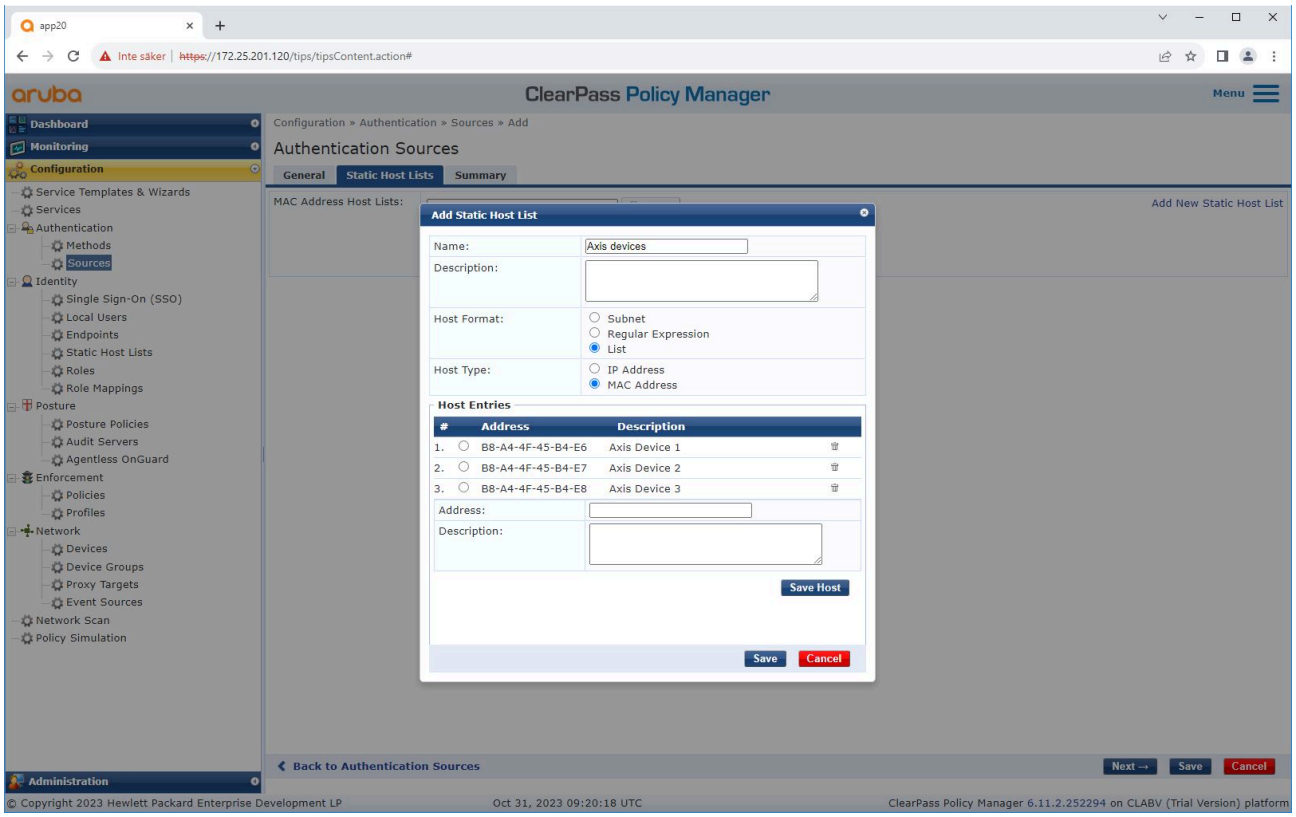
Na stronie **Sources (Źródła)** tworzone jest nowe źródło uwierzytelniania, które akceptuje tylko ręcznie importowane adresy MAC.



Wdrażanie starszej wersji — uwierzytelnianie MAC

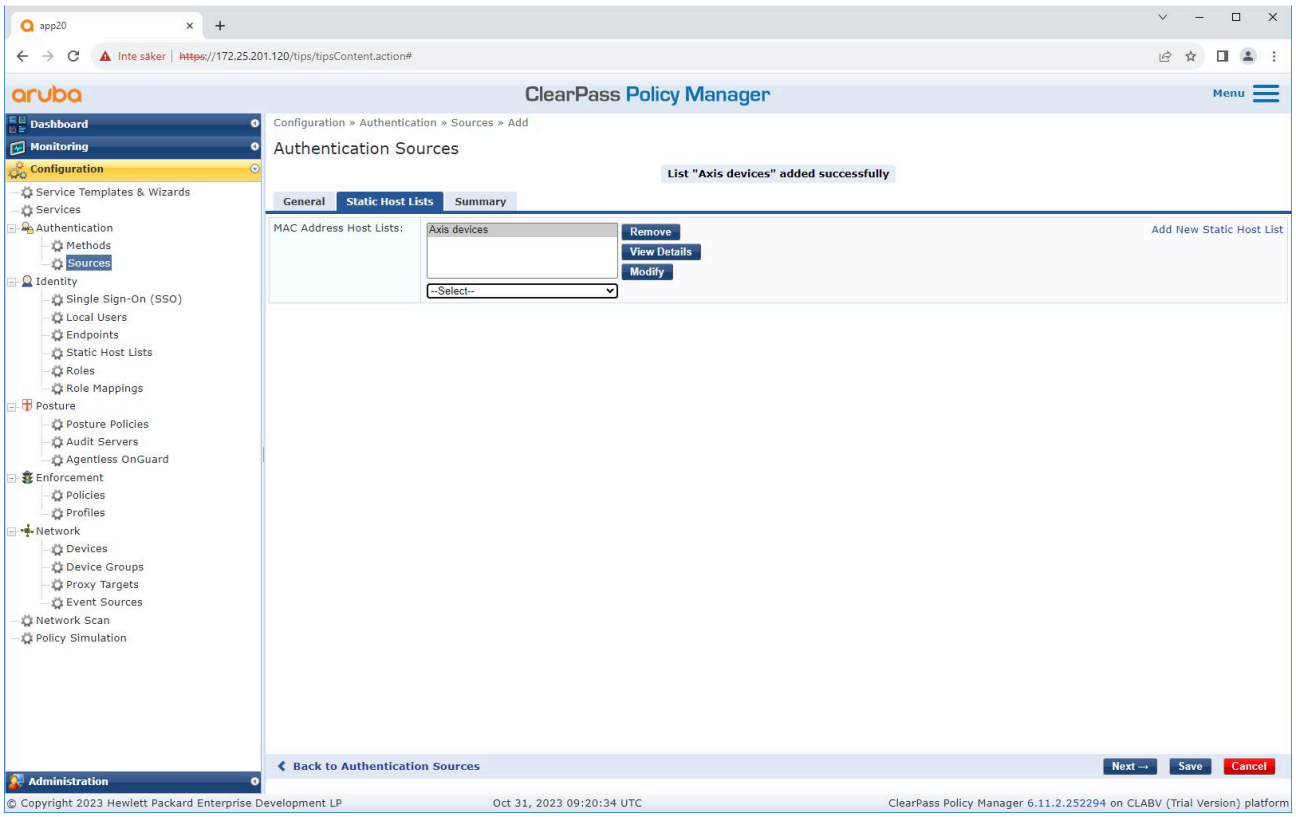


Wdrażanie starszej wersji — uwierzytelnianie MAC



Tworzona jest statyczna lista hostów zawierająca adresy MAC Axis.

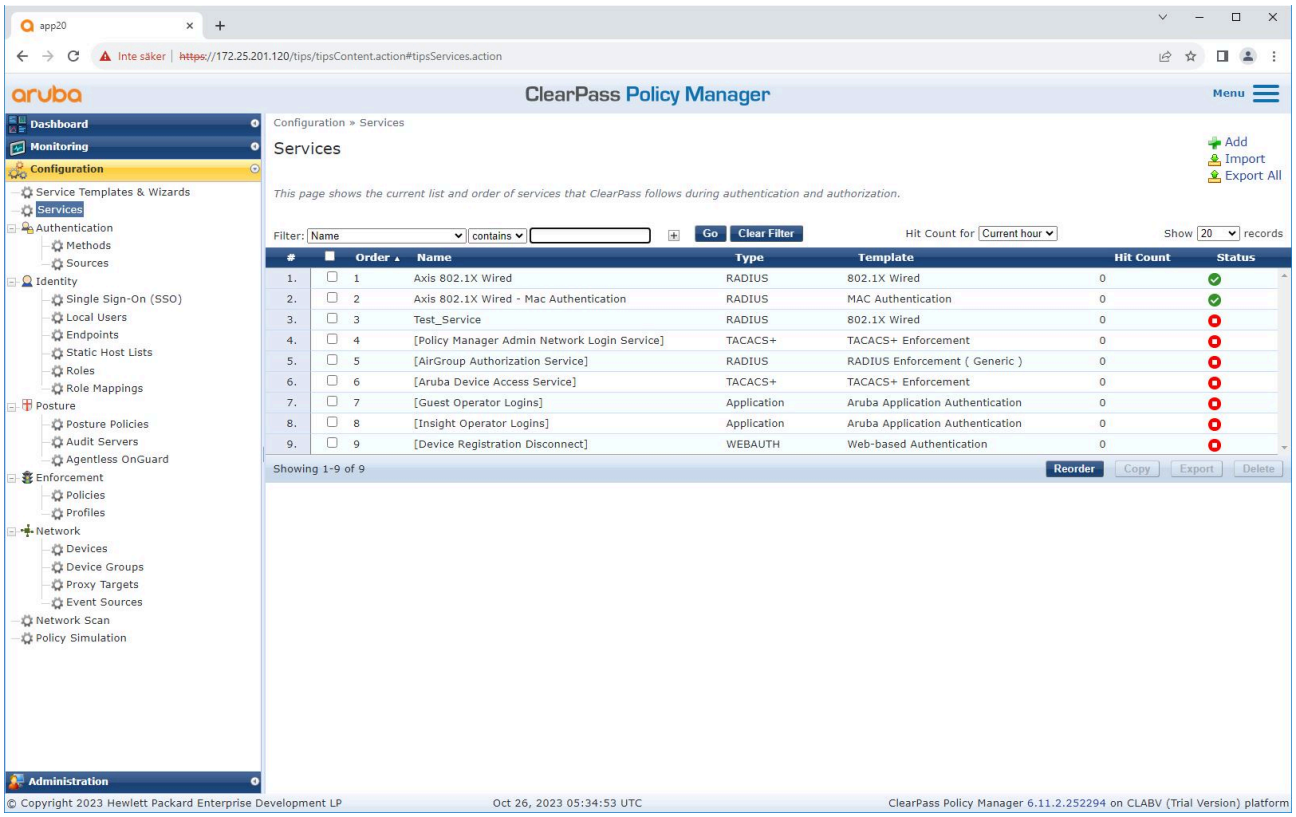
Wdrażanie starszej wersji — uwierzytelnianie MAC



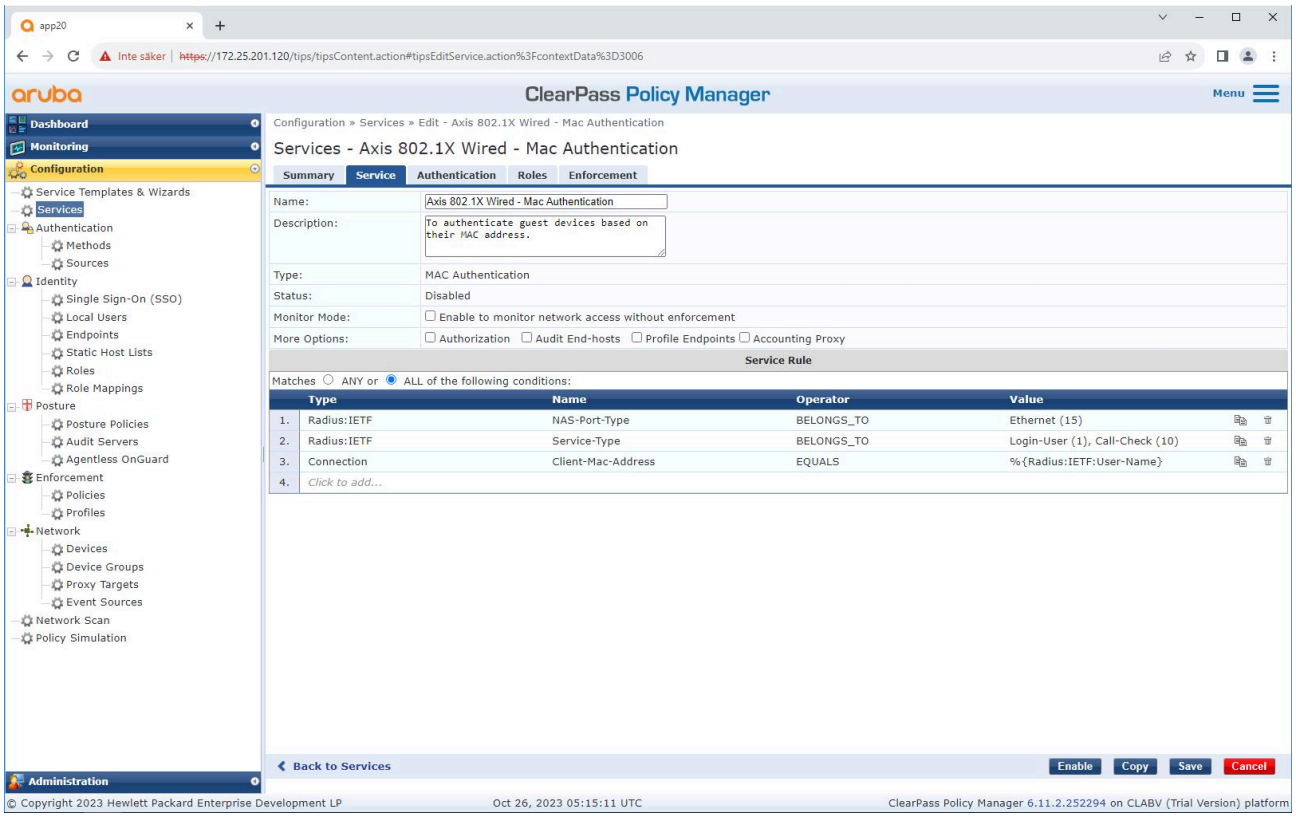
Konfiguracja usług

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

Wdrażanie starszej wersji — uwierzytelnianie MAC

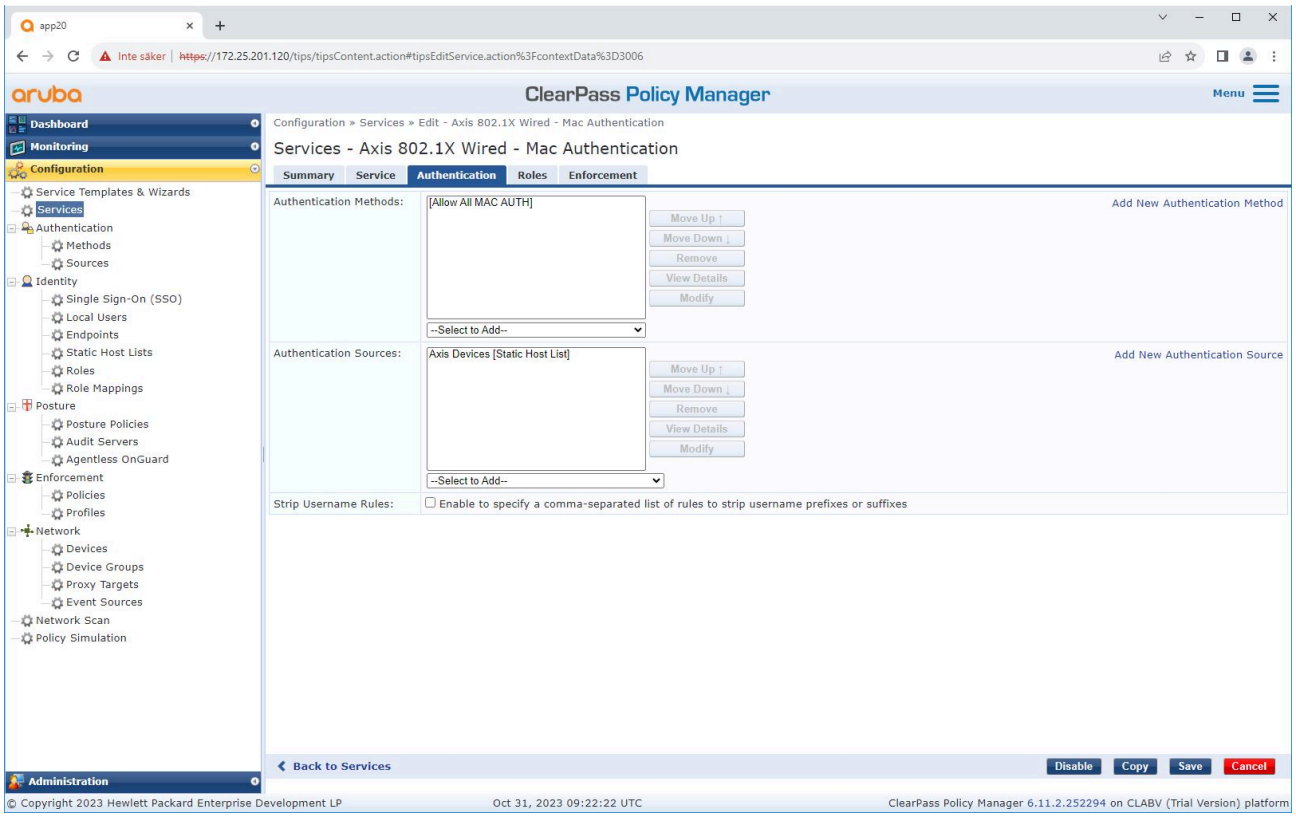


Wdrażanie starszej wersji — uwierzytelnianie MAC



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

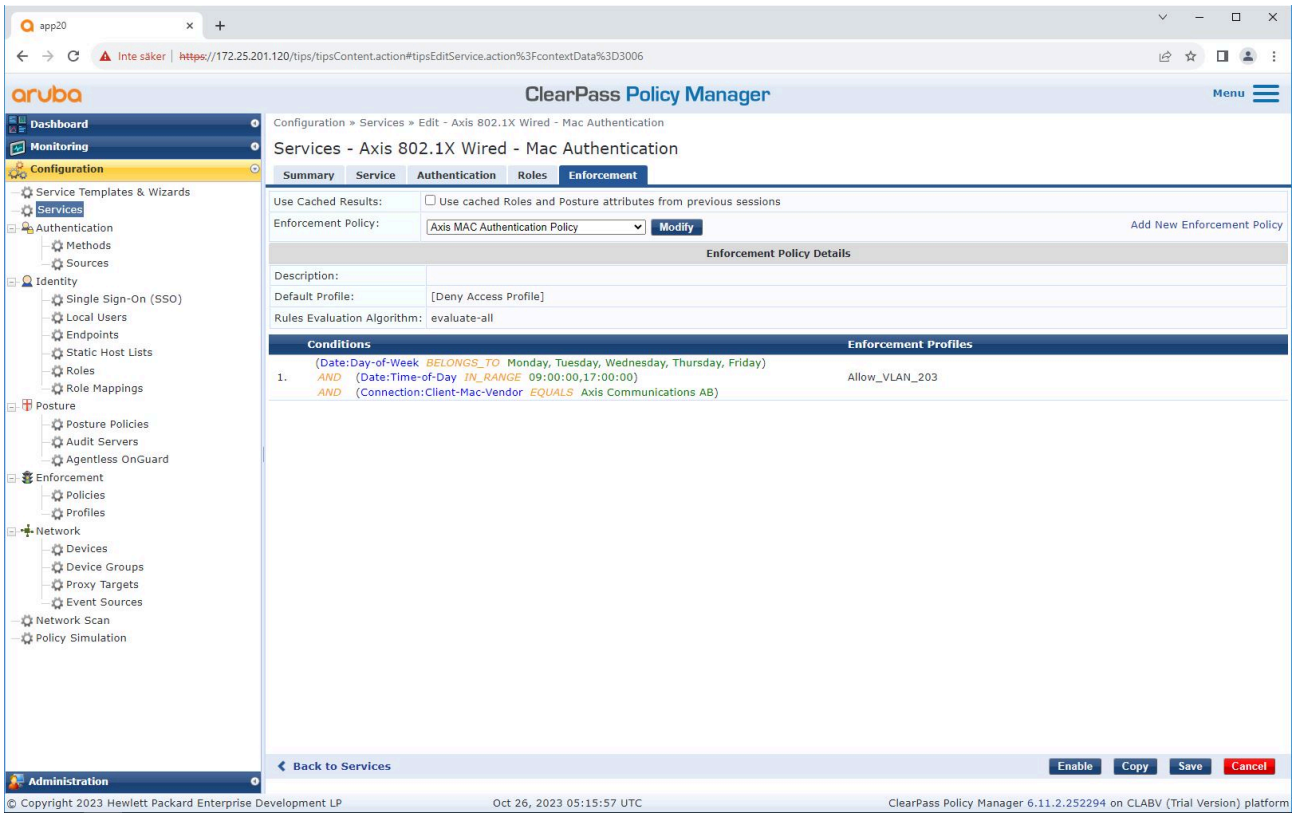
Wdrażanie starszej wersji — uwierzytelnianie MAC



Dla usługi zostaje skonfigurowana metoda uwierzytelniania MAC z predefiniowanymi ustawieniami. Ponadto zostaje wybrane wcześniej utworzone źródło uwierzytelniania 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



W ostatnim kroku następuje skonfigurowanie dla usługi poprzednio utworzonej polityki wykonywania.

Switch dostępowy HPE Aruba Networking

Oprócz konfiguracji bezpiecznego wdrażania opisanej w części zapoznaj się z poniższą przykładową konfiguracją portu dla switcha dostępowego HPE Aruba Networking, aby umożliwić łączność z użyciem MAB.

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

Przewodnik integracji
HPE Aruba Networking

Wer. M6.2
Data: Maj 2024
Numer części T10197992