Secure integration of Axis devices into Aruba networks

Podręcznik użytkownika

Secure integration of Axis devices into Aruba networks

Spis treści

Secure integration of Axis devices into Aruba networks

Wprowadzenie

Wprowadzenie

Niniejszy przewodnik integracji zawiera opis najlepszych rozwiązań w zakresie konfiguracji urządzeń Axis i ich obsługi w sieciach Aruba. 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 ze sprzętem i aplikacjami sieciowymi Aruba. Poniżej zostały opisane niektóre korzyści płynące z łączenia urządzeń i aplikacji Axis z infrastrukturą sieciową Aruba:

- 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 Aruba 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 korporacyjnej Aruba, w tym switchami dostępowymi Aruba i Aruba 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

Wstępne uwierzytelnienie

Podłącz urządzenie Axis obsługujące Axis Edge Vault, aby uwierzytelnić je w sieci Aruba. Urządzenie będzie korzystać 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, Aruba ClearPass Policy Manager weryfikuje identyfikator urządzenia Axis wraz z innymi identyfikatorami unikalnymi dla urządzenia. Informacje, takie jak adres MAC i uruchomione oprogramowanie sprzętowe, są wykorzystywane do podejmowania decyzji opartych na zasadach.

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

Urządzenie Axis uwierzytelnia się w sieci Aruba 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 sieć Aruba przeniesie urządzenie Axis do sieci obsługi administracyjnej (VLAN201), w której zainstalowany jest Axis Device Manager. Axis Device Manager umożliwia przeprowadzenie konfiguracji urządzenia, wzmocnienie zabezpieczeń i aktualizacje oprogramowania układowego. 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 wyzwoli kolejną próbę uwierzytelnienia. Aruba 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 Aruba.

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 zostaje przeniesione do sieci produkcyjnej (VLAN 202). W tej sieci system zarządzania materiałem wizyjnym (VMS) połączy się z urządzeniem Axis i zacznie 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*

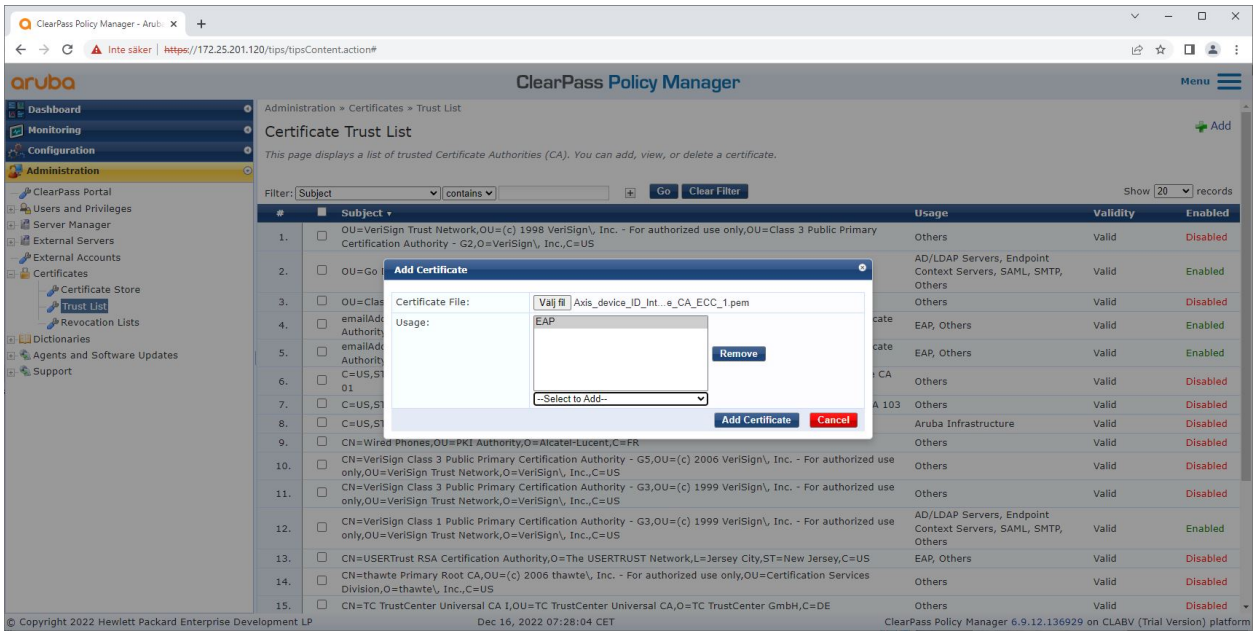
Konfiguracja HPE Aruba

Aruba ClearPass Policy Manager

Aruba's 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.

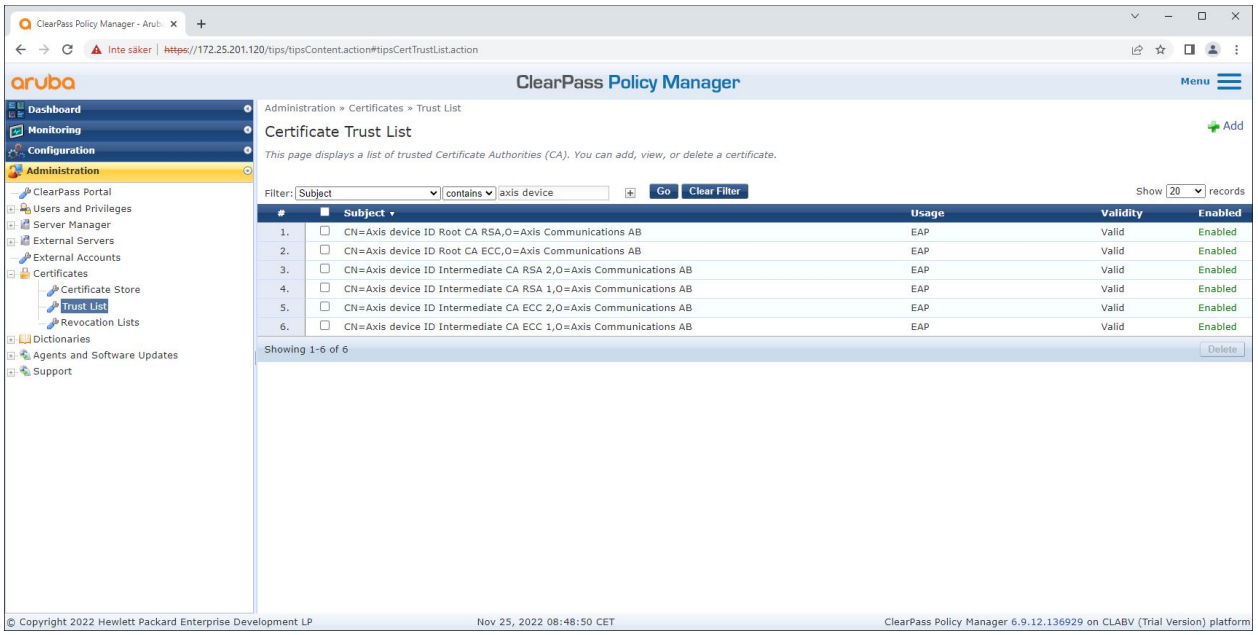
Konfiguracja zaufanej bazy certyfikatów

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 Aruba ClearPass Policy Manager, aby uwierzytelniać urządzenia Axis za pośrednictwem IEEE 802.1X EAP-TLS.
4. W polu użytkowania wybierz opcję EAP. Certyfikaty będą używane do uwierzytelniania IEEE 802.1X EAP-TLS.



Przesyłanie certyfikatów IEEE 802.1AR specyficznych dla firmy Axis do zaufanego magazynu certyfikatów narzędzia Aruba ClearPass Policy Manager.

Bezpieczne wdrożenie — IEEE 802.1AR/802.1X



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

Konfiguracja urządzenia/grupy sieciowej

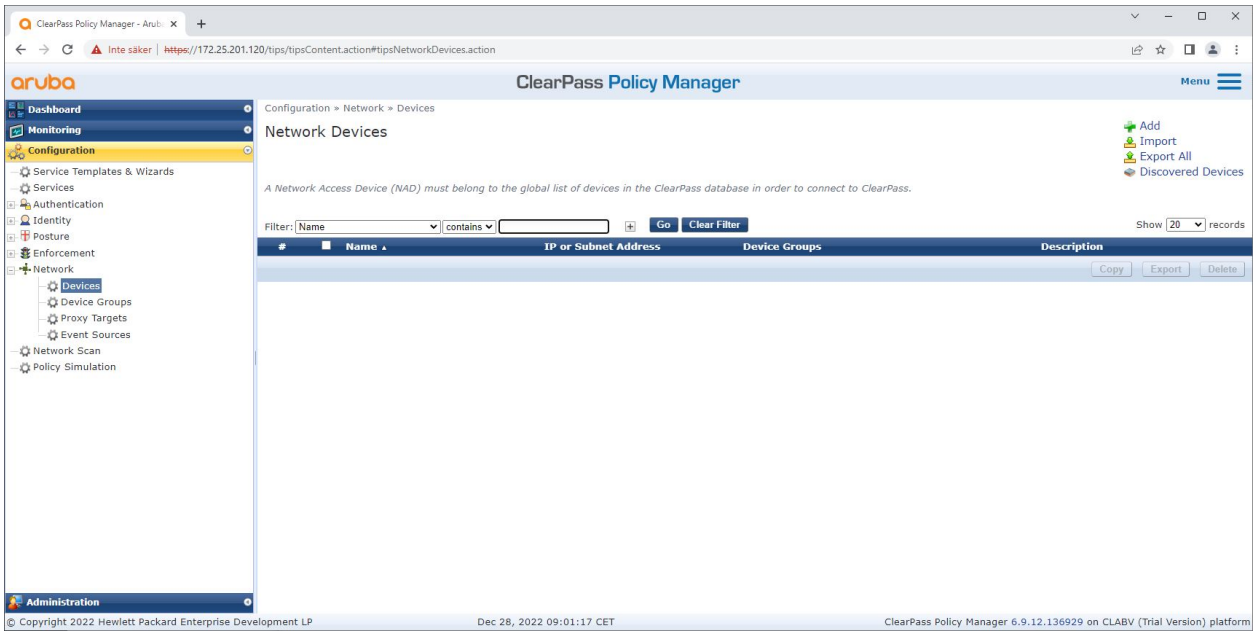
1. Dodaj zaufane urządzenia dostępu do sieci, takie jak switche dostępowe Aruba, do narzędzia ClearPass Policy Manager. Menedżer zasad ClearPass musi wiedzieć, które switche dostępowe Aruba w sieci będą używane do komunikacji IEEE 802.1X.

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

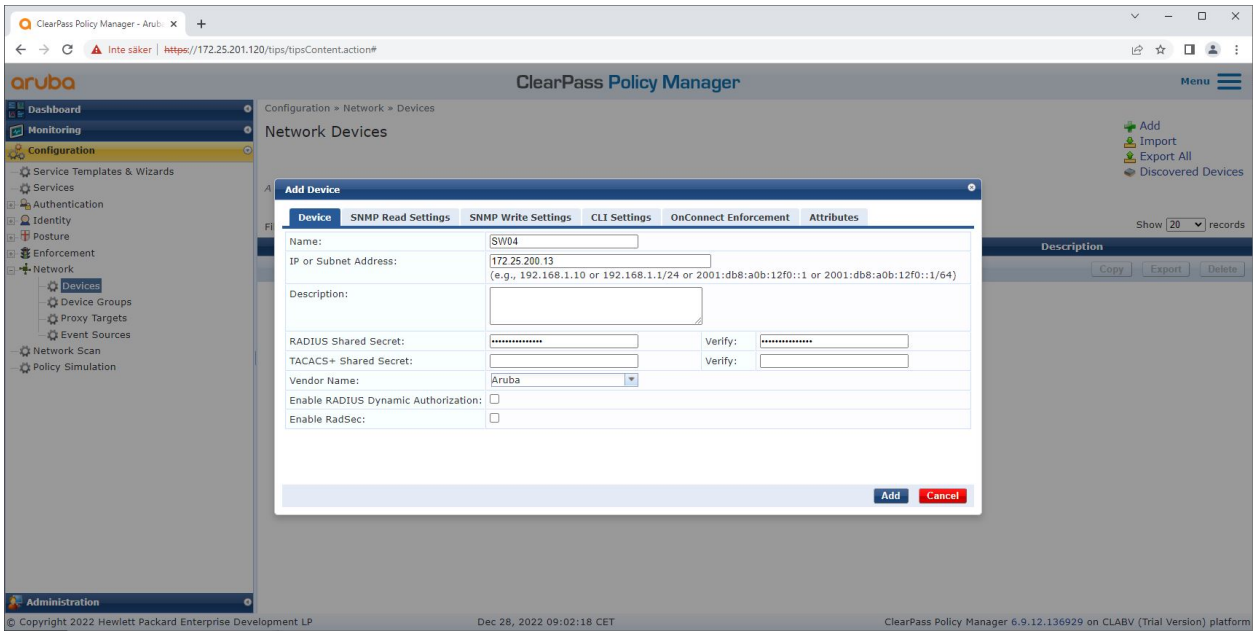
3. Współdzielony sekret RADIUS musi być zgodny z określoną konfiguracją switcha IEEE 802.1X.

Secure integration of Axis devices into Aruba networks

Bezpieczne wdrożenie — IEEE 802.1AR/802.1X



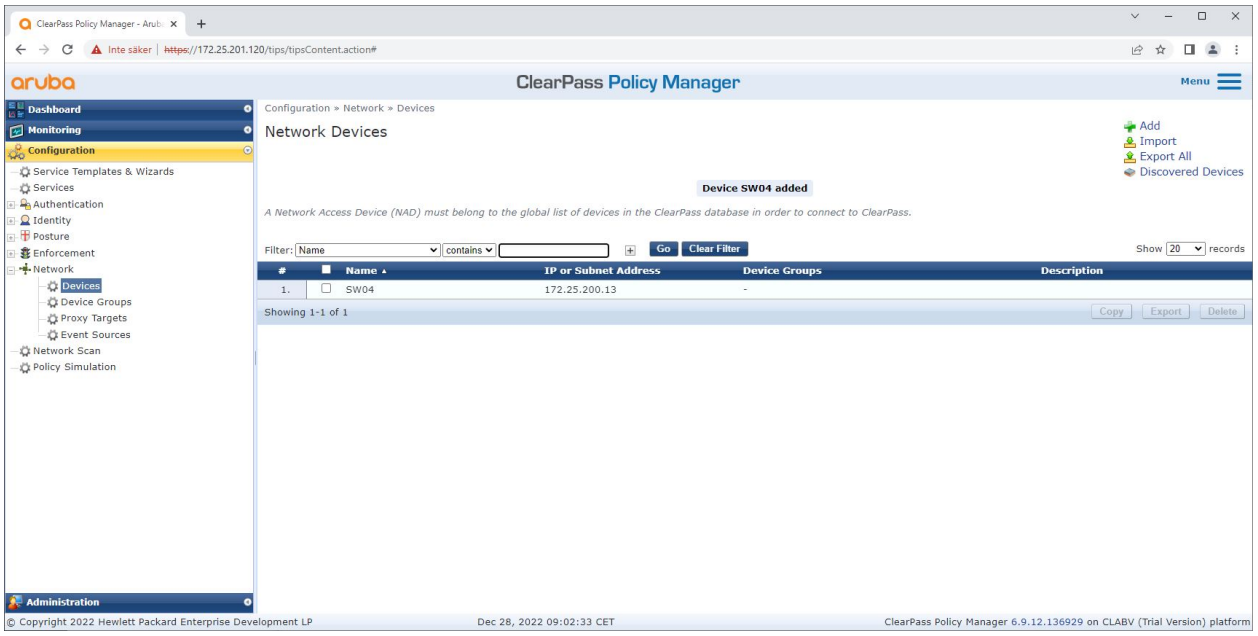
Interfejs zaufanych urządzeń sieciowych w narzędziu Aruba ClearPass Policy Manager.



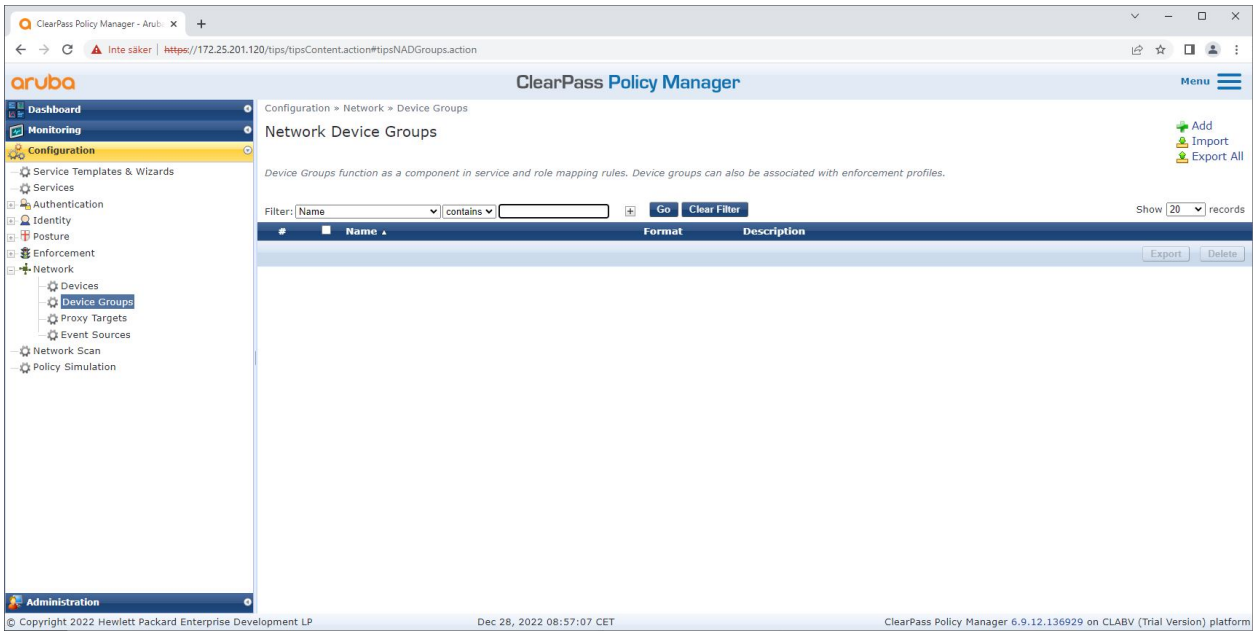
Dodanie switcha dostępowego Aruba jako zaufanego urządzenia sieciowego w narzędziu Aruba ClearPass Policy Manager. Uwaga: współdzielony sekret RADIUS musi odpowiadać konkretnej konfiguracji switcha IEEE 802.1X.

Secure integration of Axis devices into Aruba networks

Bezpieczne wdrożenie — IEEE 802.1AR/802.1X

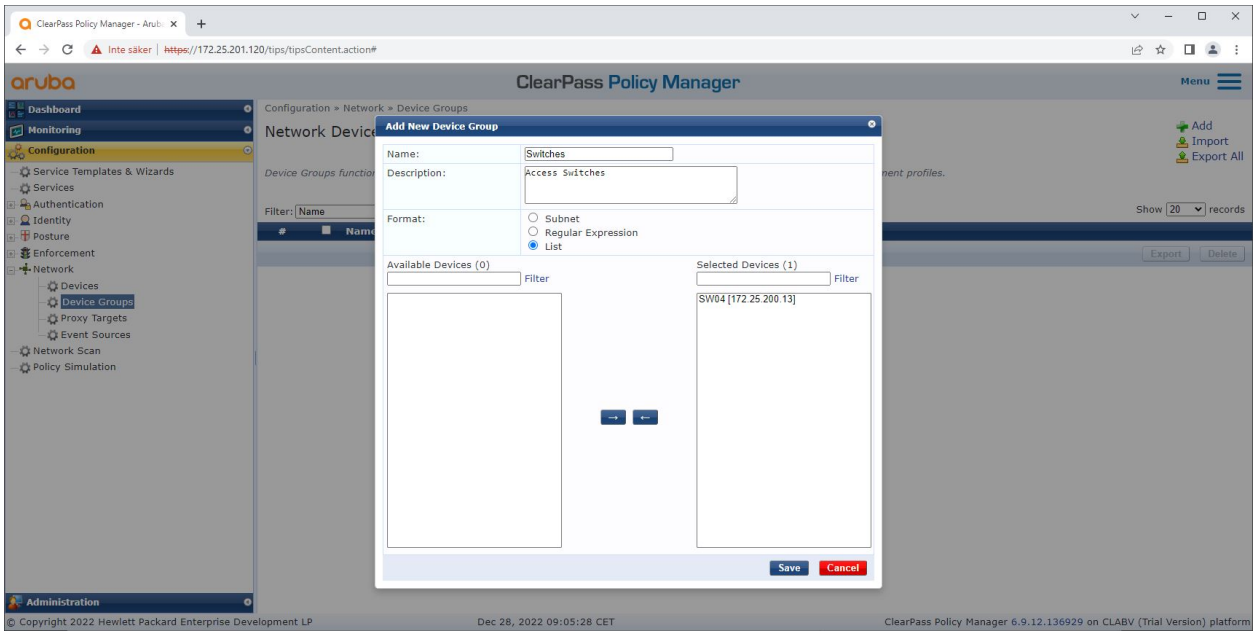


The Aruba ClearPass Policy Manager ze skonfigurowanym jednym zaufanym urządzeniem sieciowym.

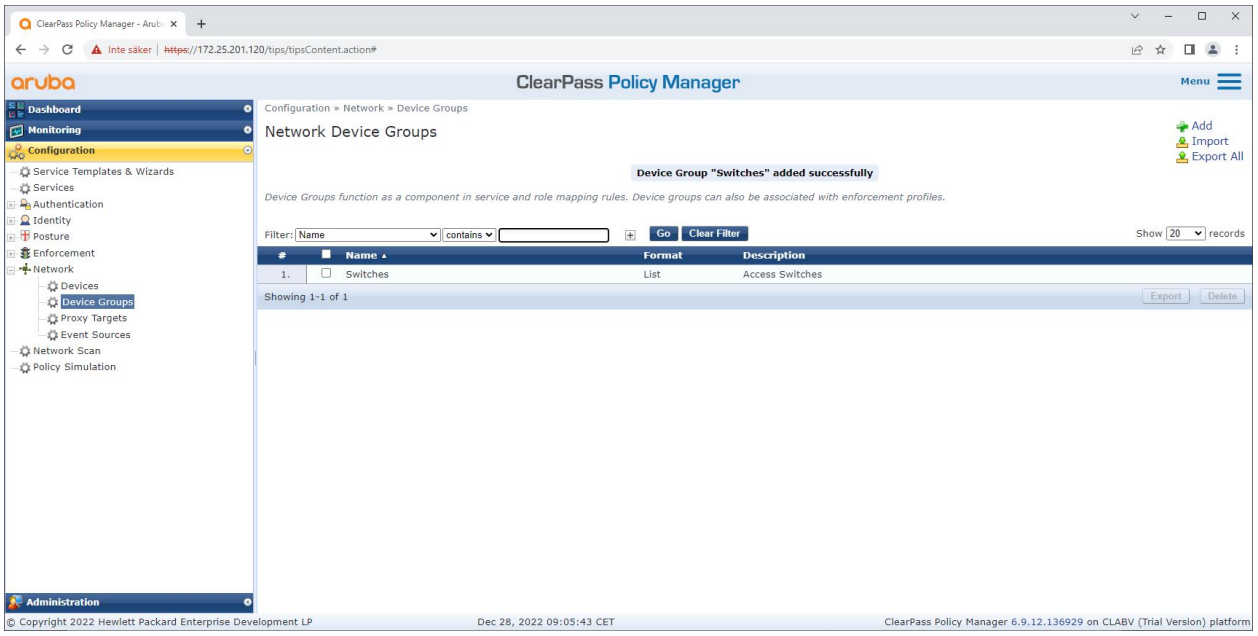


Interfejs zaufanych grup urządzeń sieciowych w narzędziu Aruba ClearPass Policy Manager.

Bezpieczne wdrożenie — IEEE 802.1AR/802.1X



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



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

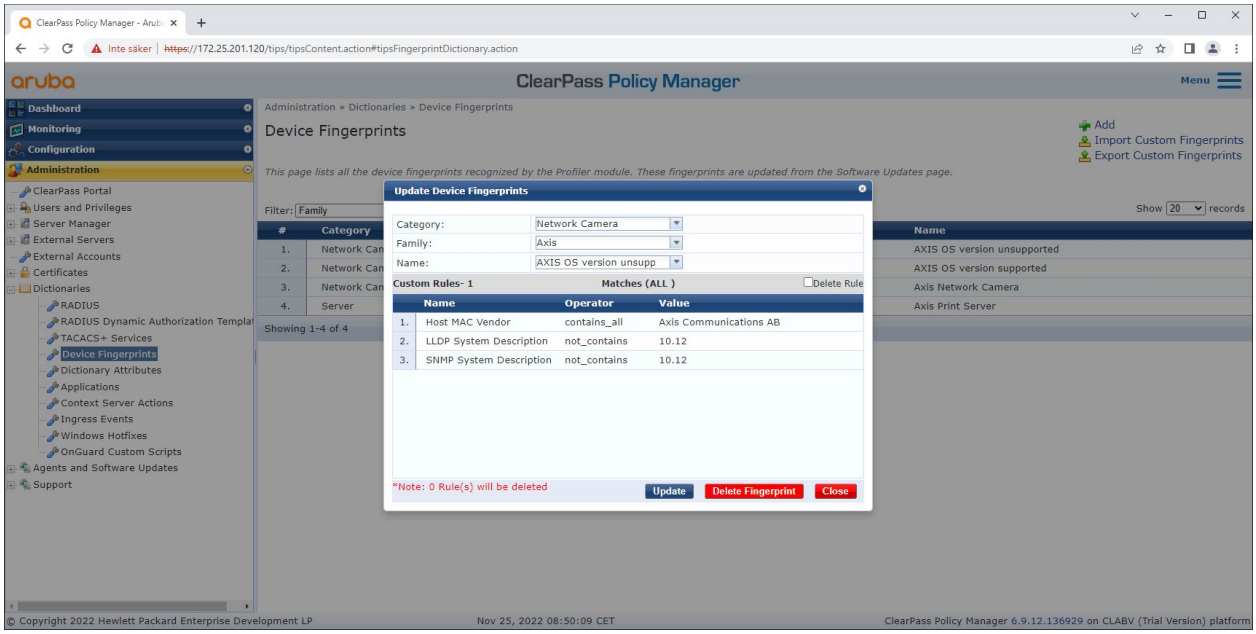
Konfiguracja odcisku palca urządzenia

Urządzenie Axis może poprzez wykrywanie sieci dystrybuować specyficzne dla siebie informacje, takie jak adres MAC i wersja oprogramowania układowego. Odcisk palca urządzenia można utworzyć za pomocą interfejsu odcisków palców w narzędziu Aruba ClearPass Policy Manager. Odciski palców urządzeń można uaktualniać i można nimi zarządzać. Można na przykład przyznać lub zablokować dostęp, w zależności od wersji AXIS OS.

Bezpieczne wdrożenie — IEEE 802.1AR/802.1X

Odciski palców urządzeń można uaktualniać i można nimi zarządzać. Można na przykład przyznać lub zablokować dostęp, w zależności od wersji AXIS OS.

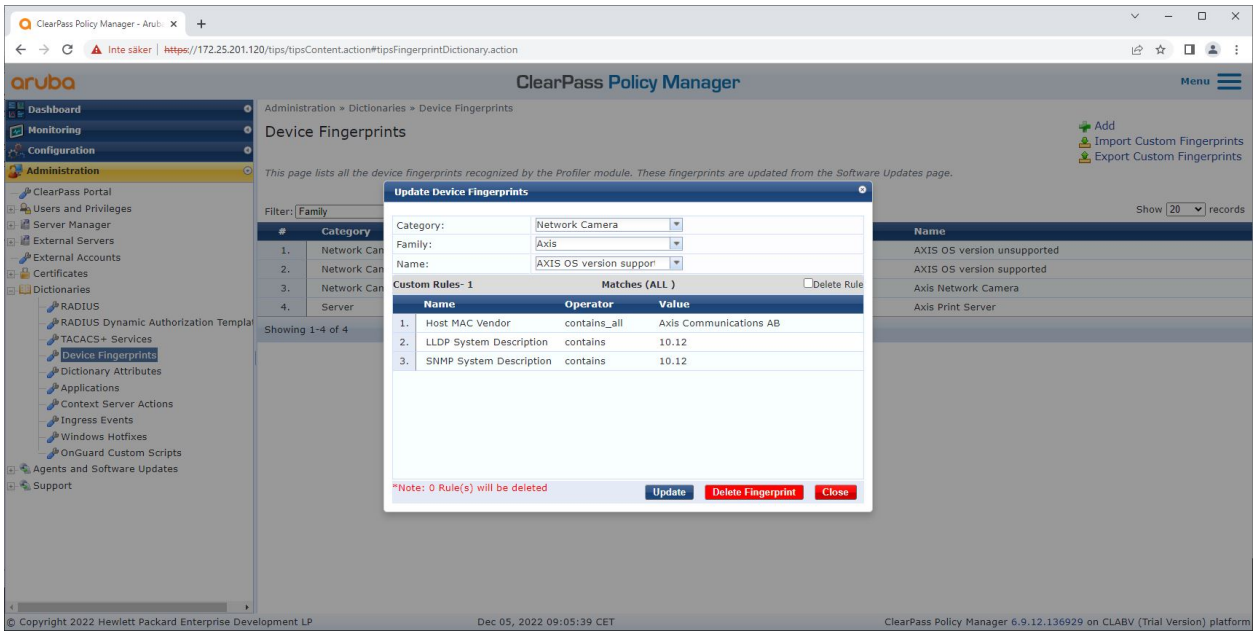
1. Przejdź do menu **Administration > Dictionaries > Device Fingerprints (Administracja > Słowniki > Odciski palców urządzenia)**.
2. Wybierz istniejący odcisk palca urządzenia lub utwórz nowy.
3. Skonfiguruj ustawienia odcisku palca urządzenia.



Konfiguracja odcisku palca urządzenia w narzędziu Aruba ClearPass Policy Manager. Urządzenia Axis z wersją oprogramowania sprzętowego inną niż 10.12 są uznawane za nieobsługiwane.

Secure integration of Axis devices into Aruba networks

Bezpieczne wdrożenie — IEEE 802.1AR/802.1X



Konfiguracja odcisku palca urządzenia w narzędziu Aruba ClearPass Policy Manager. W powyższym przykładzie urządzenia Axis z oprogramowaniem sprzętowym 10.12 są uważane za obsługiwane.

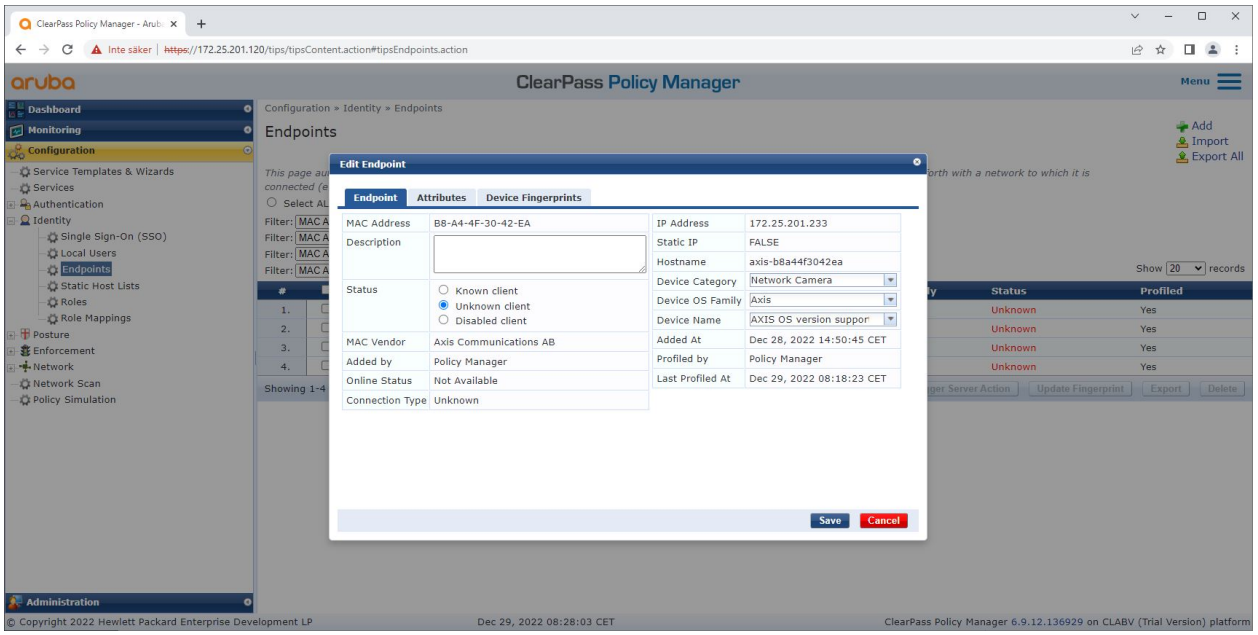
Informacje o odcisku palca urządzenia zebranym przez narzędzie Aruba ClearPass Manager można znaleźć w sekcji Punkty końcowe.

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

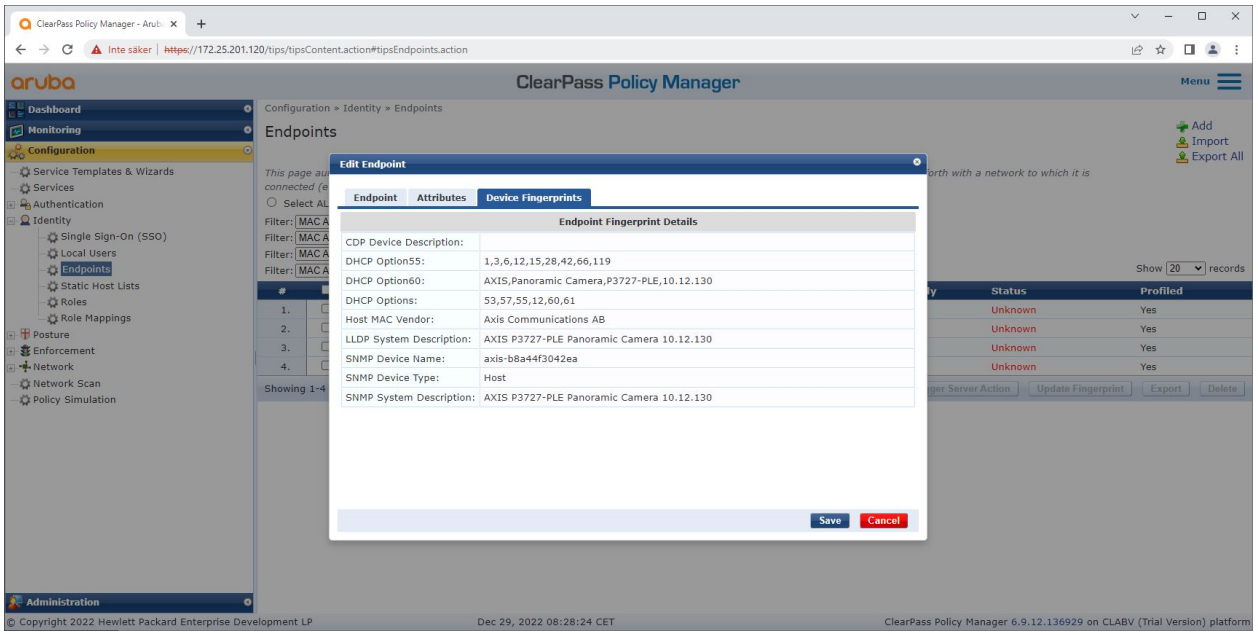
Uwaga

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

Bezpieczne wdrożenie — IEEE 802.1AR/802.1X



Urządzenie Axis sprofilowane przez narzędzie Aruba ClearPass Policy Manager.



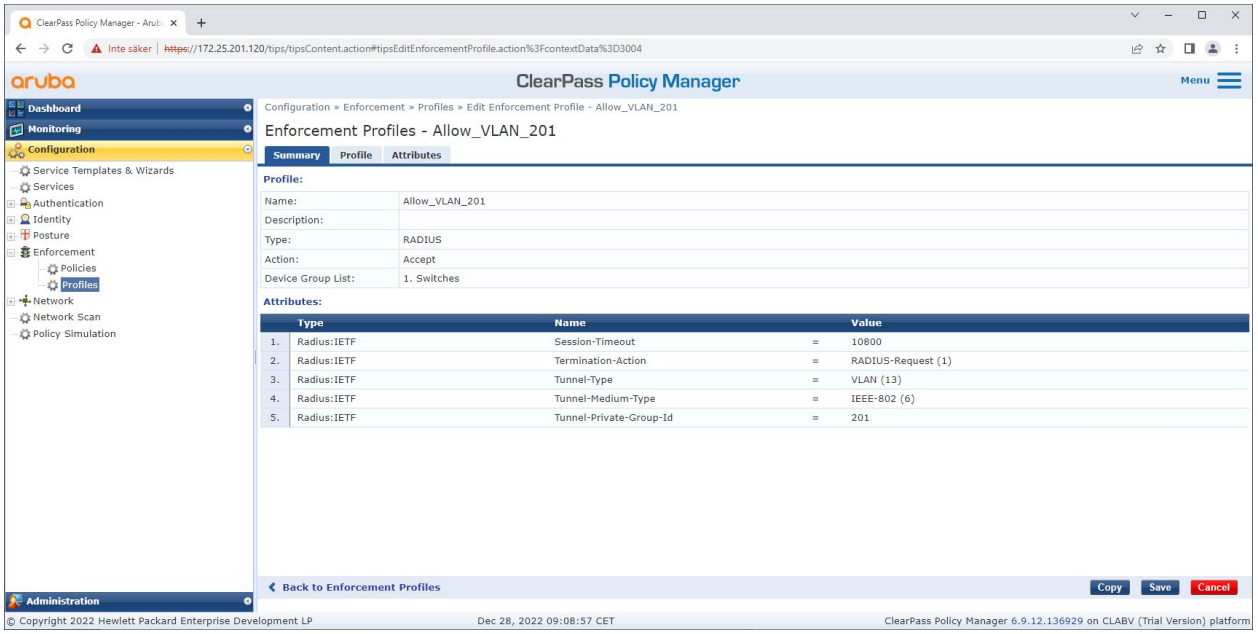
Szczegółowe odciski palców sprofilowanego urządzenia Axis. Uwaga: protokół SNMP jest domyślnie wyłączony w urządzeniach Axis. Informacje LLDP, CDP i specyficzne dla DHCP są udostępniane przez urządzenie Axis w formie domyślnych ustawień fabrycznych i przekazywane przez switch dostępowy Aruba do narzędzia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

Konfiguracja profilu wykonywania

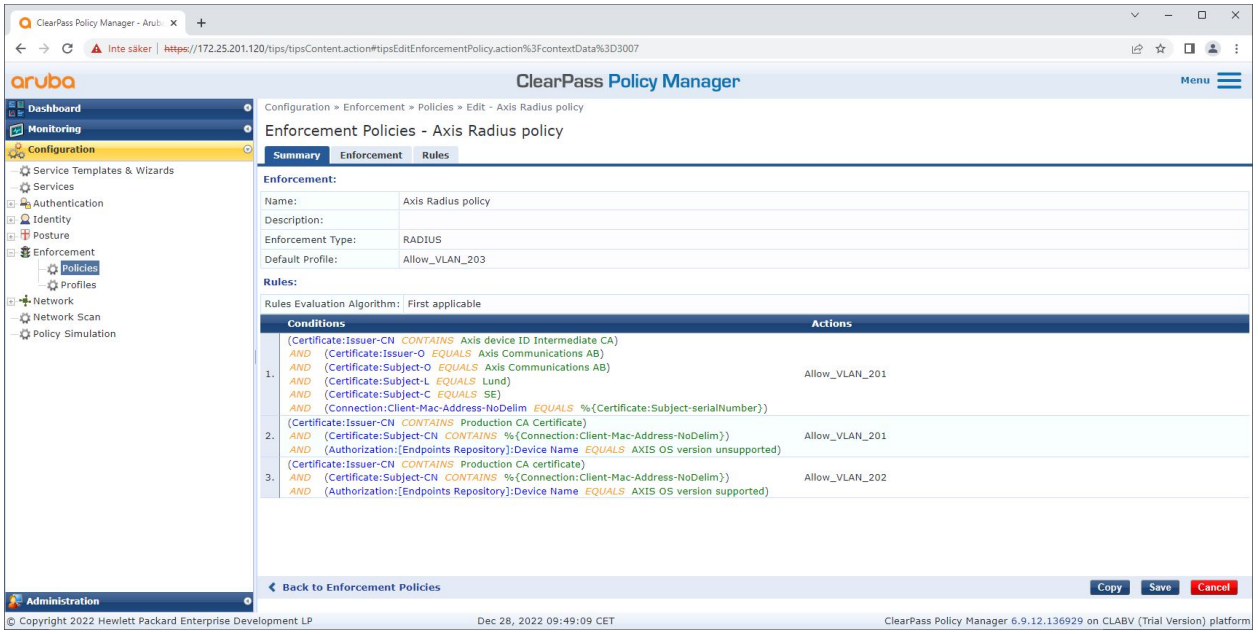
Za pomocą profilu wykonywania Aruba ClearPass Policy Manager może przypisywać określony identyfikator sieci VLAN do portu dostępu na switchu. Decyzja ta jest oparta na zasadach i ma zastosowanie do urządzeń sieciowych w grupie „switche". Niezbędna liczba profili wykonywania zależy od liczby używanych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

Bezpieczne wdrożenie — IEEE 802.1AR/802.1X

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



Przykładowy profil wykonywania umożliwiający dostęp do sieci VLAN 201.



Konfiguracja zasad wykonywania w Aruba ClearPass Policy Manager.

Poniżej wymieniono cztery zasady wykonywania i związane z nimi działania:

Odmowa dostępu do sieci

Secure integration of Axis devices into Aruba networks

Bezpieczne wdrożenie — IEEE 802.1AR/802.1X

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 oprogramowania sprzętowego, certyfikatów klasy produkcyjnej i innych konfiguracji. Aruba ClearPass Policy Manager sprawdza następujące warunki:

- Wersja oprogramowania sprzętowego 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)

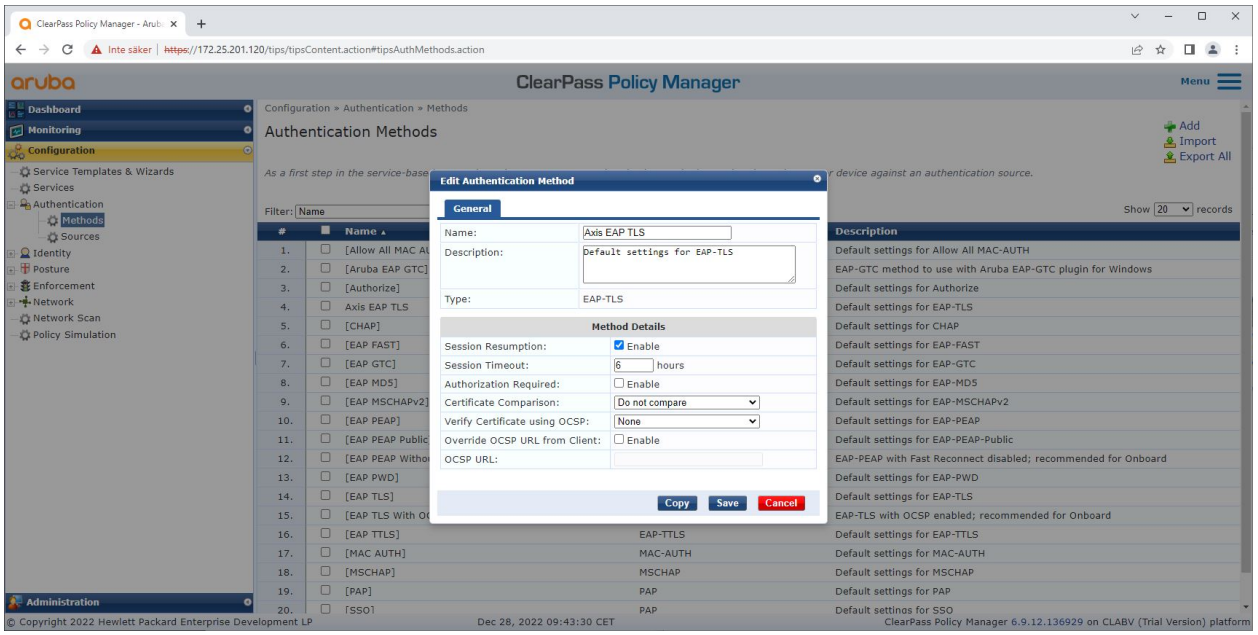
Urządzenie Axis uzyskuje dostęp do sieci produkcyjnej, w której będzie działać. Dostęp zostaje przyznany po zakończeniu działań administracyjnych na urządzeniu z poziomu sieci administracyjnej (VLAN 201). Aruba ClearPass Policy Manager sprawdza następujące warunki:

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

Konfiguracja metody uwierzytelniania

W metodzie uwierzytelniania określa się, w jaki sposób urządzenie Axis będzie próbowało uwierzytelnić się w sieci Aruba. 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.

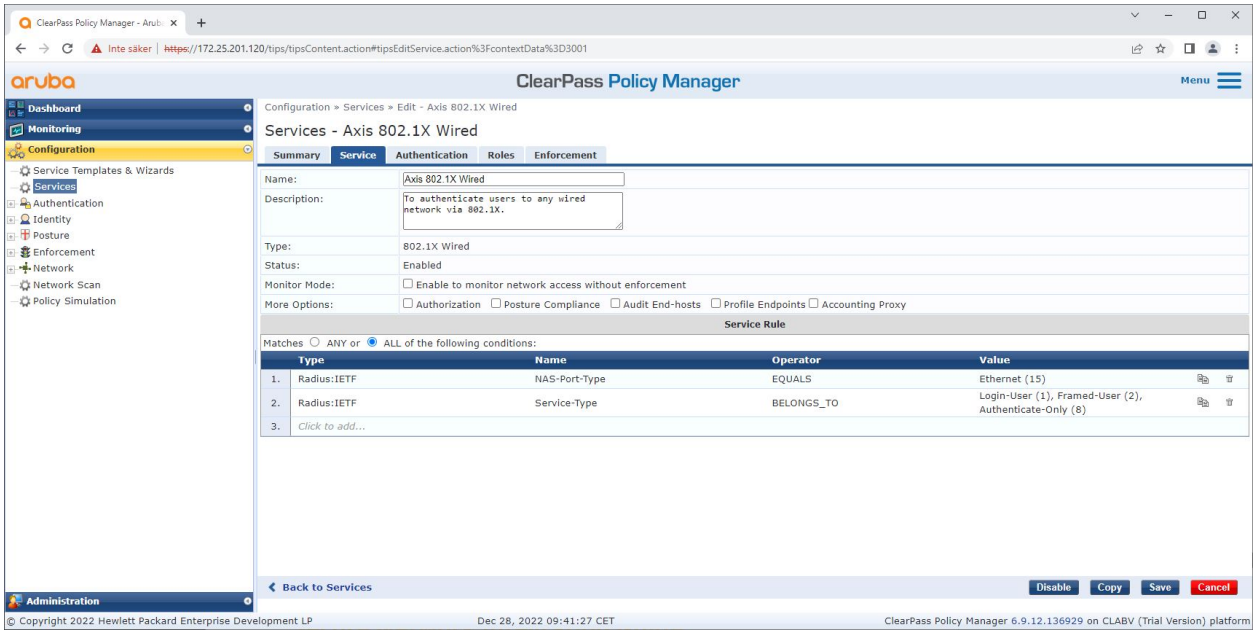
Bezpieczne wdrożenie — IEEE 802.1AR/802.1X



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

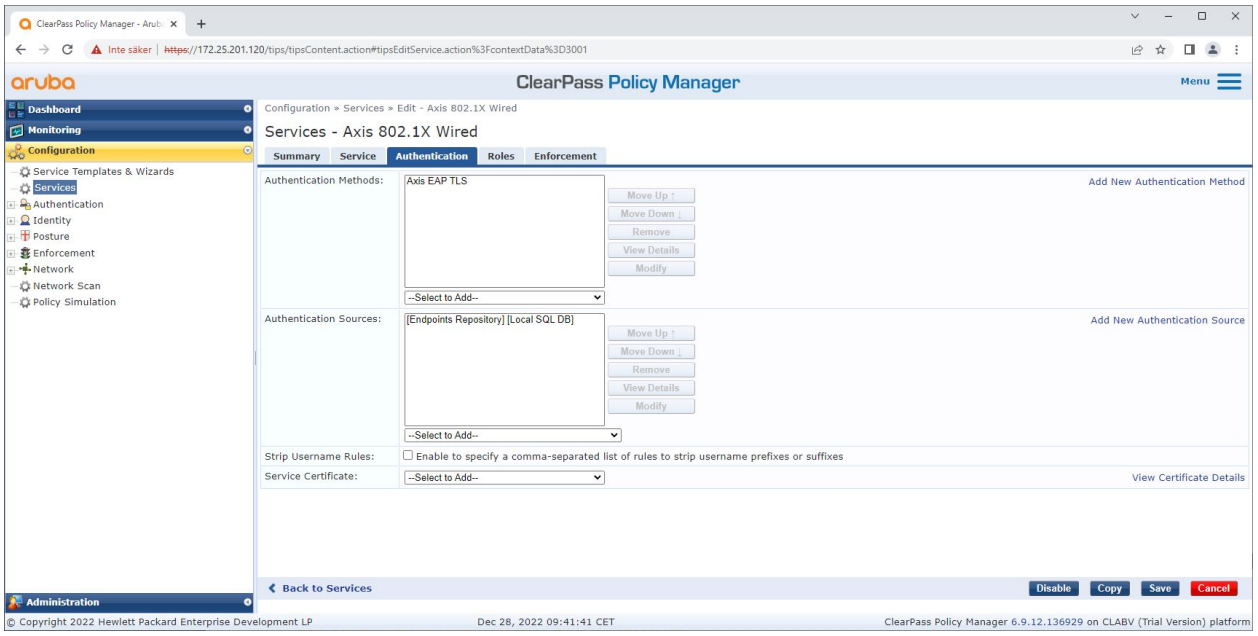
Konfiguracja usług

W interfejsie usług kroki konfiguracji są połączone w jedną usługę, która obsługuje uwierzytelnianie i autoryzację urządzeń Axis w sieciach Aruba.

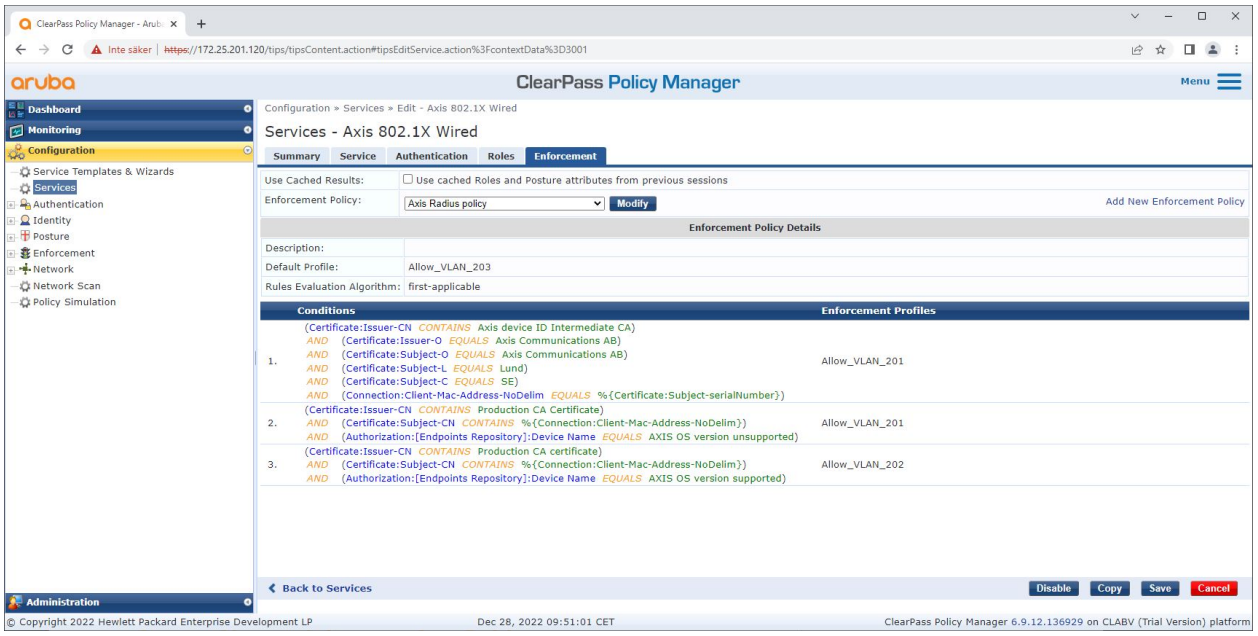


Tworzone są dedykowane usługi Axis definiujące standard IEEE 802.1X jako metodę łączności.

Bezpieczne wdrożenie — IEEE 802.1AR/802.1X



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 Aruba

Urządzenia Axis są podłączane bezpośrednio do switchy dostępowych Aruba obsługujących PoE lub za pośrednictwem kompatybilnych zasilaczy midspan PoE firmy Axis. Aby bezpiecznie włączyć urządzenia Axis do sieci Aruba, 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 Aruba 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 Aruba.

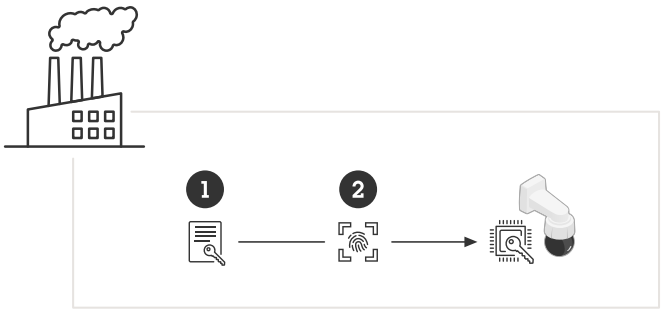
```
radius-server host MyRADIUSIPAddress key "MyRADIUSKey"

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*

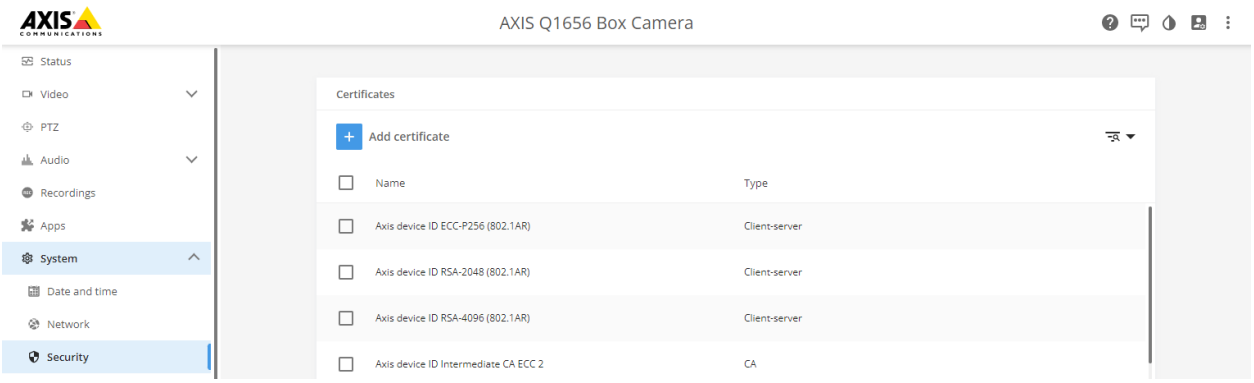
Chroniony sprzętowo bezpieczny magazyn kluczy dostarczany przez bezpieczny element urządzenia Axis jest fabrycznie wyposażony w unikalny dla urządzenia certyfikat i odpowiednie klucze (identyfikator urządzenia Axis), które globalnie mogą potwierdzić autentyczność urządzenia Axis. *Axis Product Selector*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

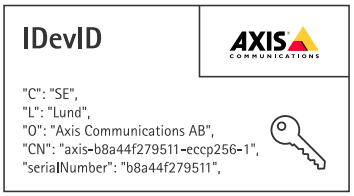
Secure integration of Axis devices into Aruba networks

Bezpieczne wdrożenie — IEEE 802.1AR/802.1X



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

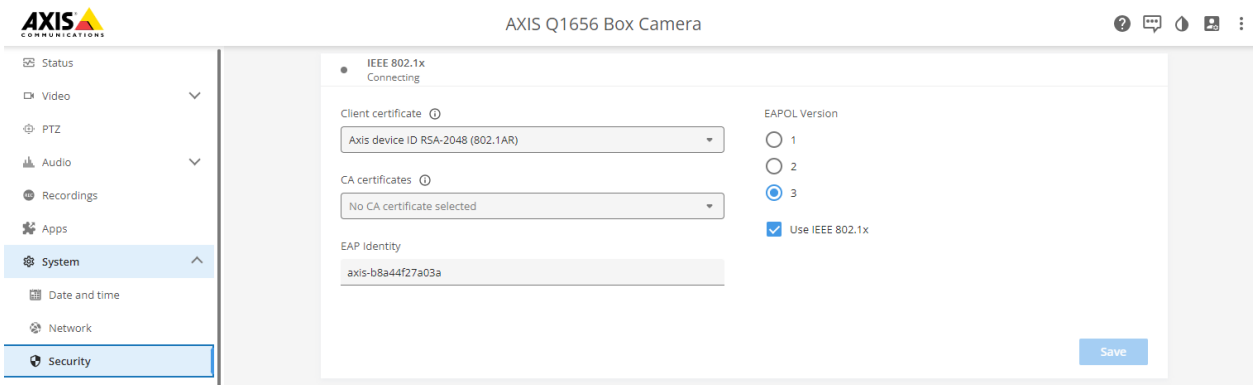
Certyfikat ID urządzenia Axis zgodny z IEEE 802.1AR zawiera informacje o numerze seryjnym i inne informacje specyficzne dla dostawcy Axis. Aruba ClearPass Policy Manager analizuje te informacje i podejmuje decyzję o przyznaniu dostępu do sieci. Poniżej przedstawiono informacje, które można uzyskać z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

Bezpieczne wdrożenie — IEEE 802.1AR/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 gdy 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:

- Instalacja aktualizacji oprogramowania sprzętowego.
- Zastosuj konfigurację cyberbezpieczeństwa, taką jak HTTPS i certyfikaty IEEE 802.1X.
- Konfiguracja ustawień specyficznych dla urządzenia, takich jak ustawienia obrazów i inne.

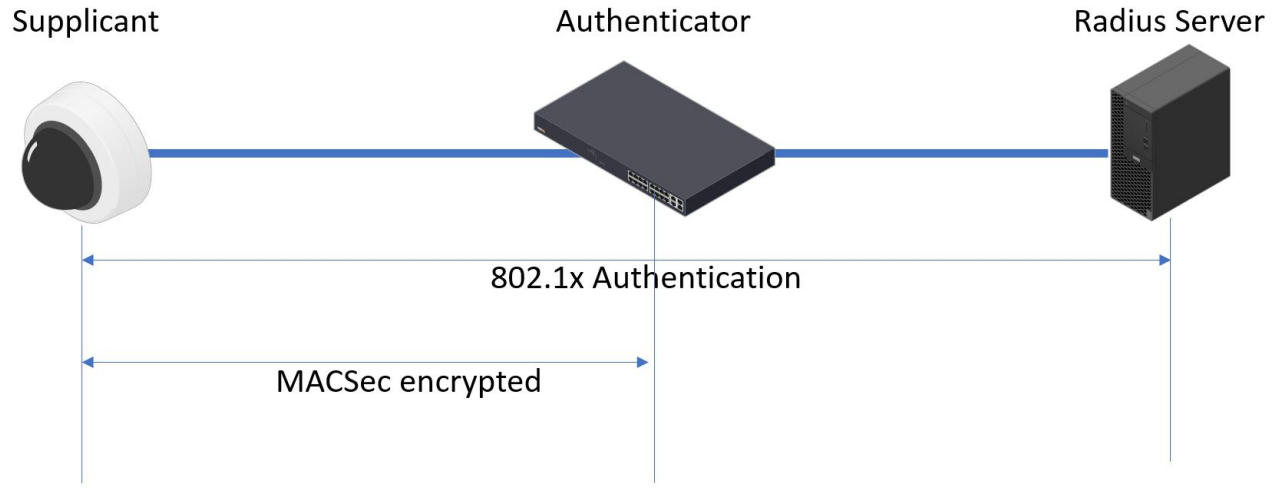
Bezpieczne działanie sieci — IEEE 802.1AE MACsec

Bezpieczne działanie sieci — IEEE 802.1AE MACsec

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.

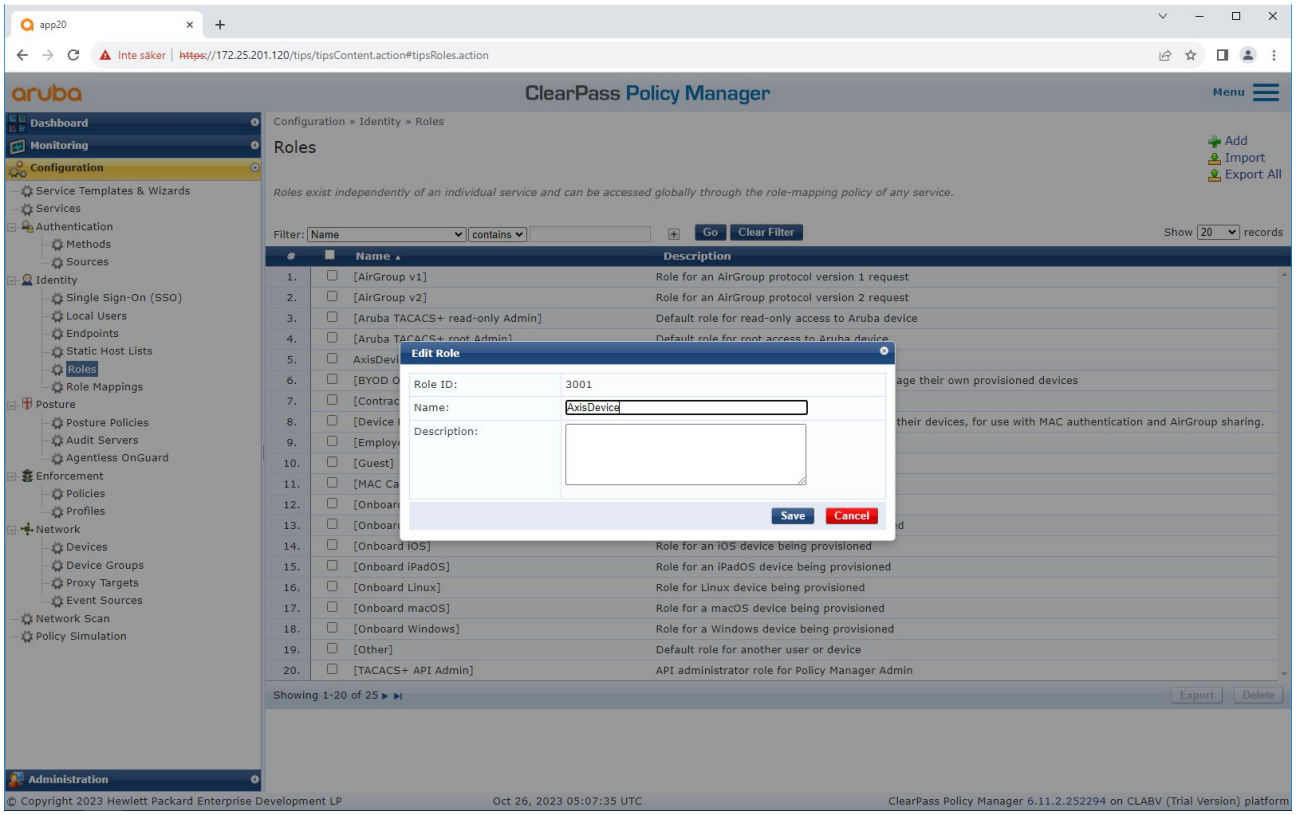
Bezpiecznie przechowywany identyfikator urządzenia Axis ID (1) (tożsamość urządzenia zgodna ze standardem IEEE 802.1AR) służy do uwierzytelniania w sieci Aruba (4, 5) za pomocą kontroli dostępu do sieci IEEE 802.1X EAP-TLS w oparciu o porty (2). W trakcie całej sesji EAP-TLS automatycznie wymieniane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

IEEE 802.1AE MABsec wymaga przygotowań do konfiguracji switcha dostępowego Aruba 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 Aruba nie obsługuje szyfrowania MACsec przez EAP-TLS, można użyć trybu klucza PSK i skonfigurować ręcznie.

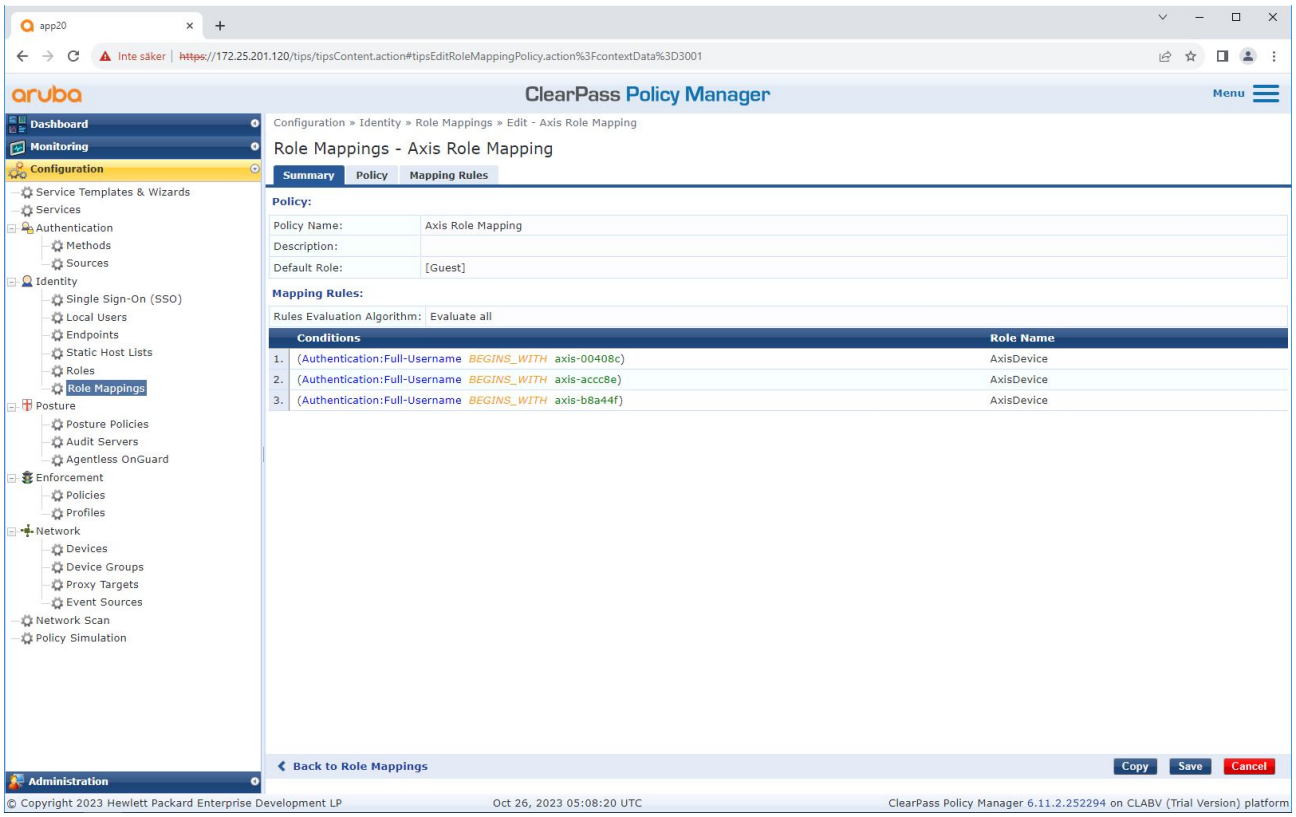
Aruba ClearPass Policy Manager

Role i zasady mapowania ról



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

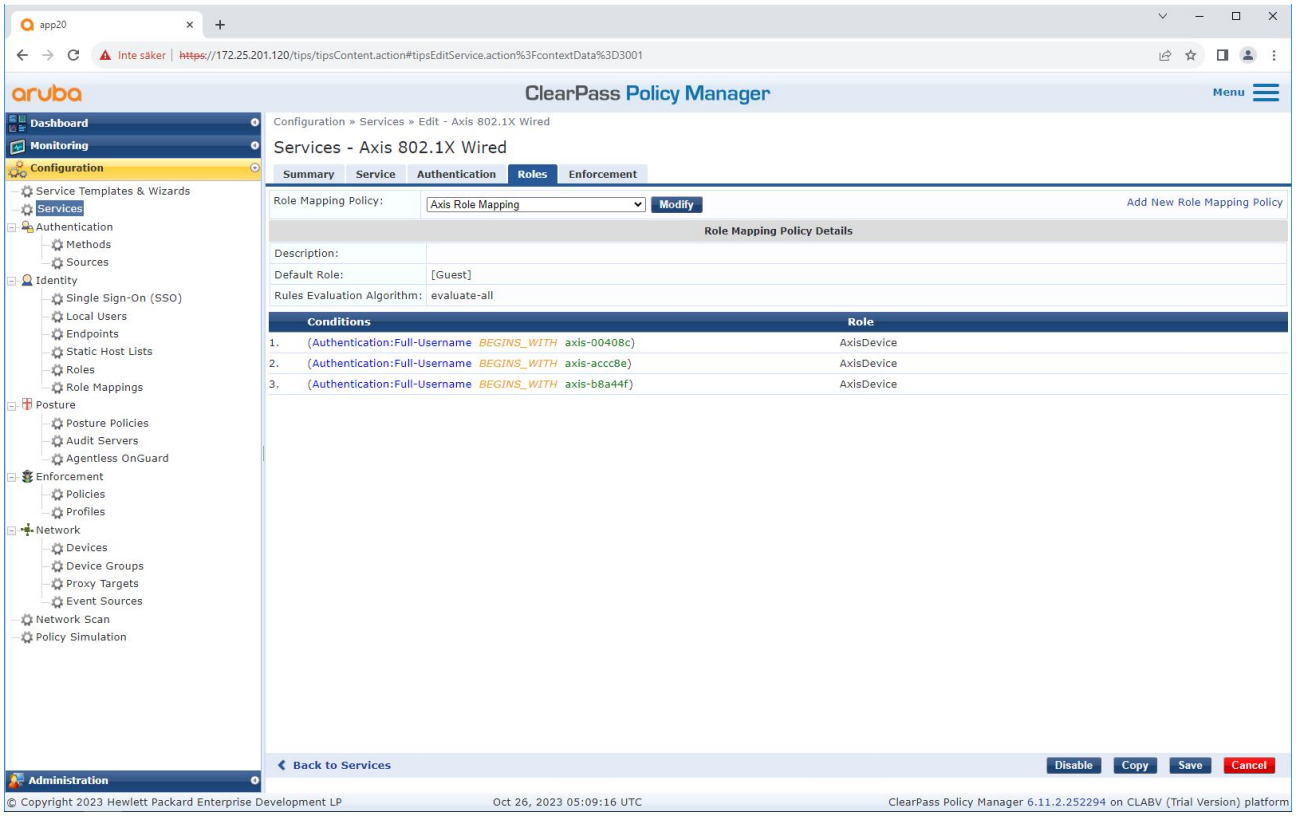
Bezpieczne działanie sieci — IEEE 802.1AE MACsec



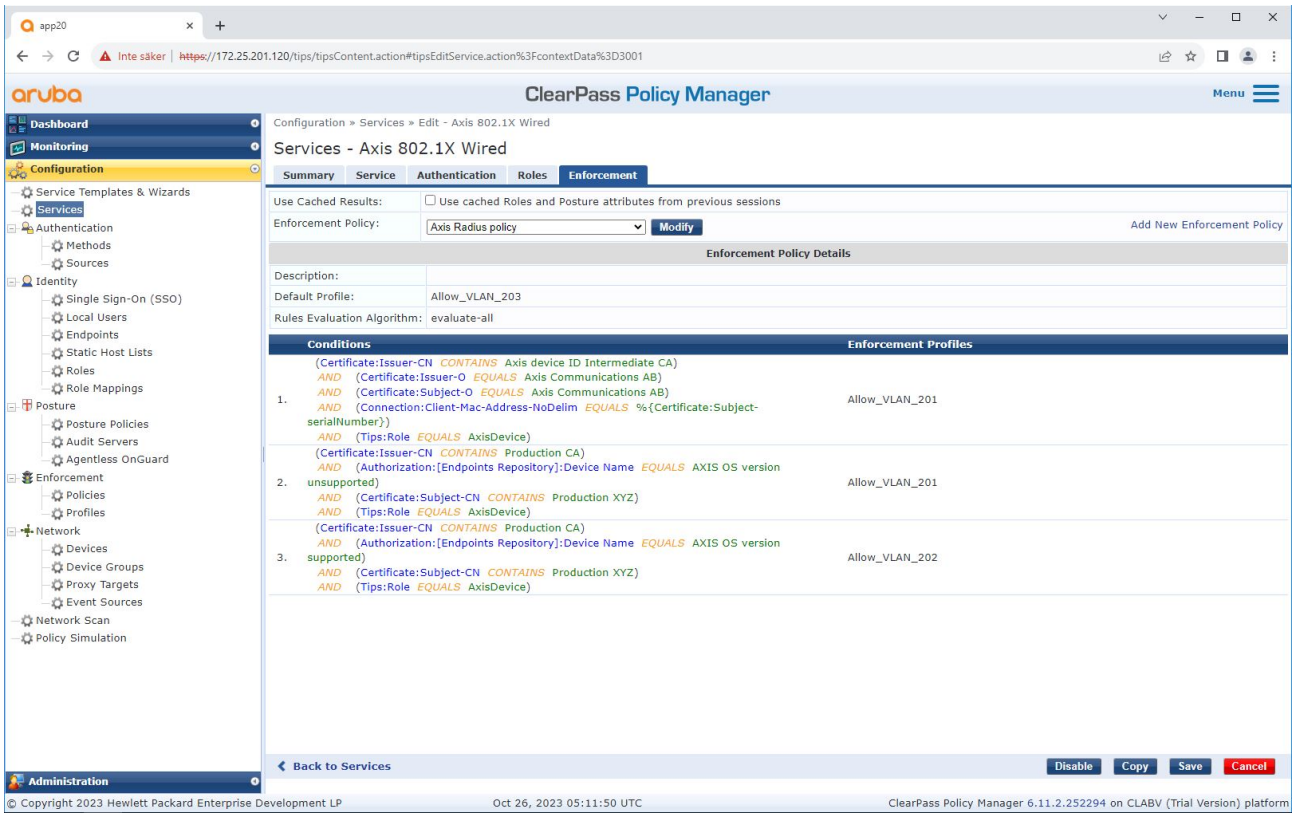
Dodanie zasad mapowania ról Axis dla wcześniej utworzonej roli urządzenia Axis. Spełnienie określonych warunków jest wymagane, aby urządzenie mogło zostać zmapowane do roli urządzenia Axis. Jeśli warunki nie zostaną spełnione, urządzenie będzie częścią roli [Guest] (gość).

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

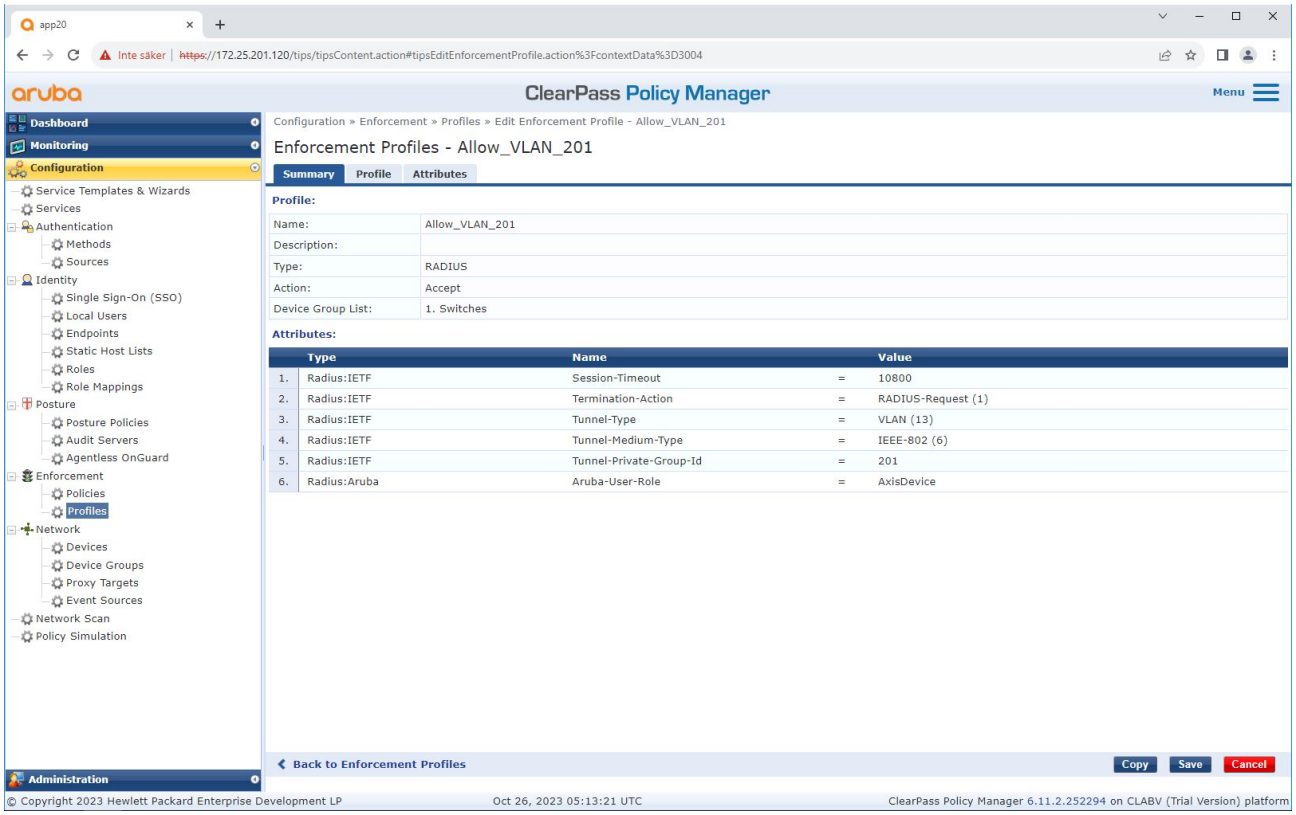


Dodanie wcześniej utworzonej zasady mapowania ról Axis do usługi, która definiuje standard IEEE 802.1X jako metodę łączenia w przypadku wdrażania urządzeń Axis.



Dodanie nazwy roli Axis jako warunku do istniejących definicji zasad.

Profil wykonawczy



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

Switch dostępowy Aruba

Oprócz konfiguracji bezpiecznego wdrażania opisanej w sekcji *Switch dostępowy Aruba na stronie 16* zapoznaj się z poniższą przykładową konfiguracją portu dla switcha dostępowego Aruba, 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

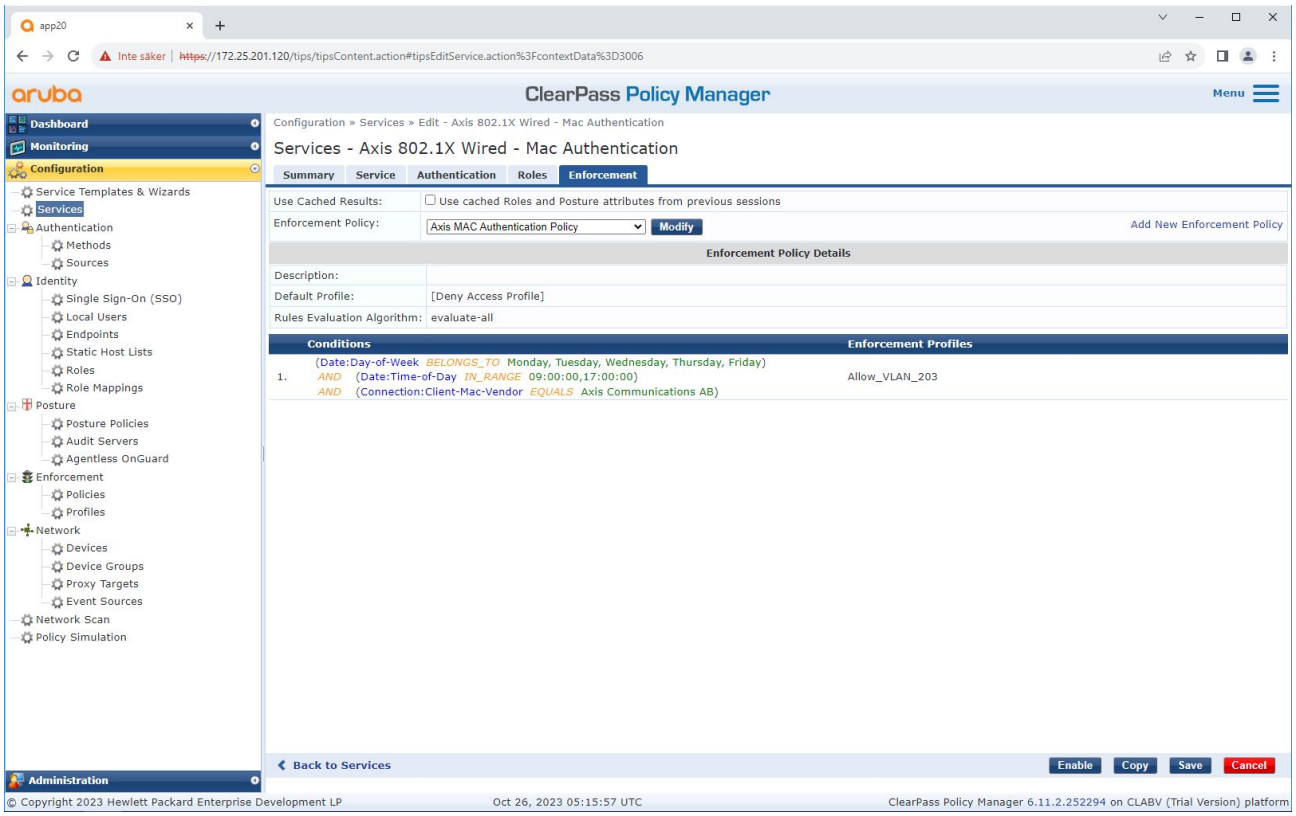
Za pomocą MAC Authentication Bypass (MAB) możesz wdrażać urządzenia Axis, które nie obsługują wdrażania IEEE 802.1AR z certyfikatem identyfikatora urządzenia Axis i włączonym IEEE 802.1X z ustawieniami fabrycznymi. Jeśli wdrożenie standardu 802.1X nie powiedzie się, Aruba ClearPass Policy Manager zweryfikuje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

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

Aruba ClearPass Policy Manager

Zasady wykonawcze

Konfiguracja zasad wykonywania w Aruba ClearPass Policy Manager określa, czy urządzenia Axis uzyskują dostęp do sieci Aruba 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

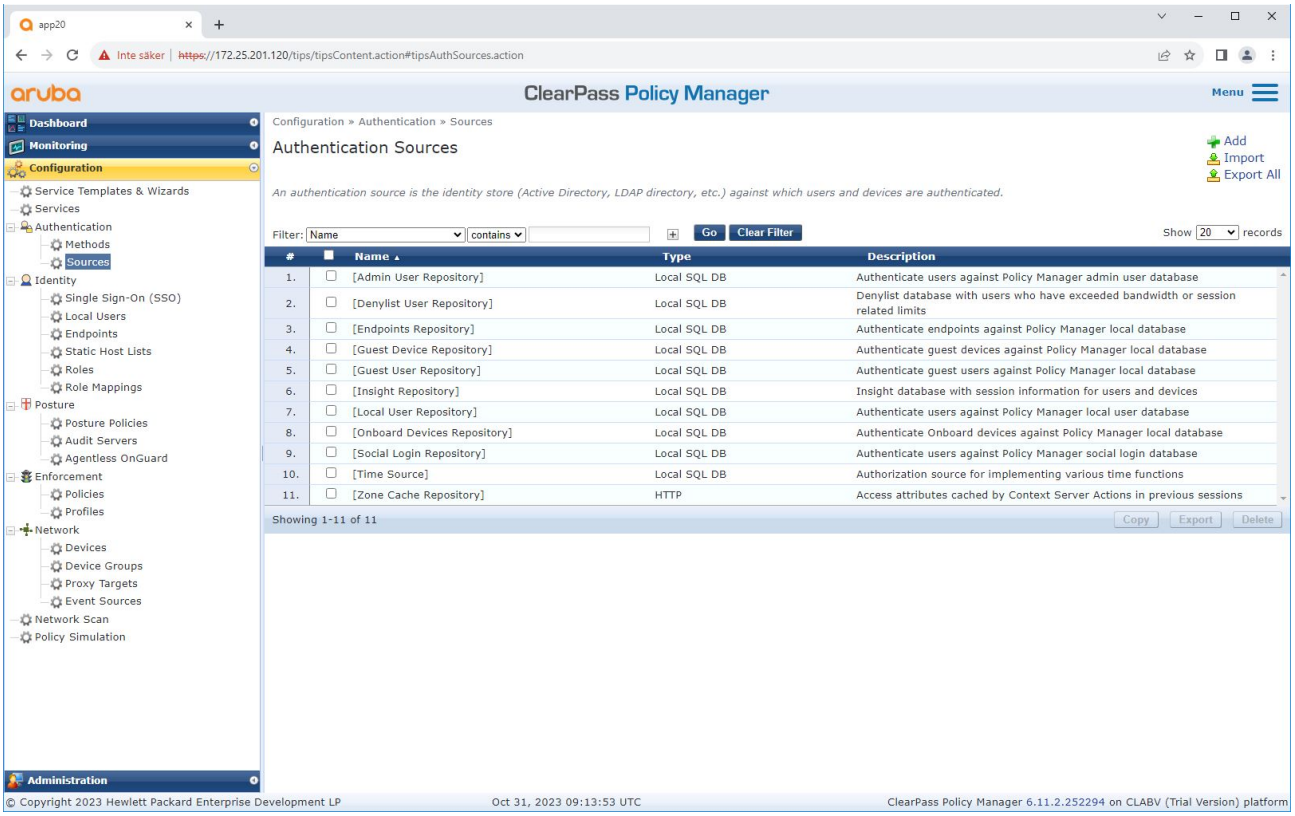
Wdrażanie starszej wersji — uwierzytelnianie MAC

- Dostawca adresu MAC jest zgodny z Axis Communications AB.

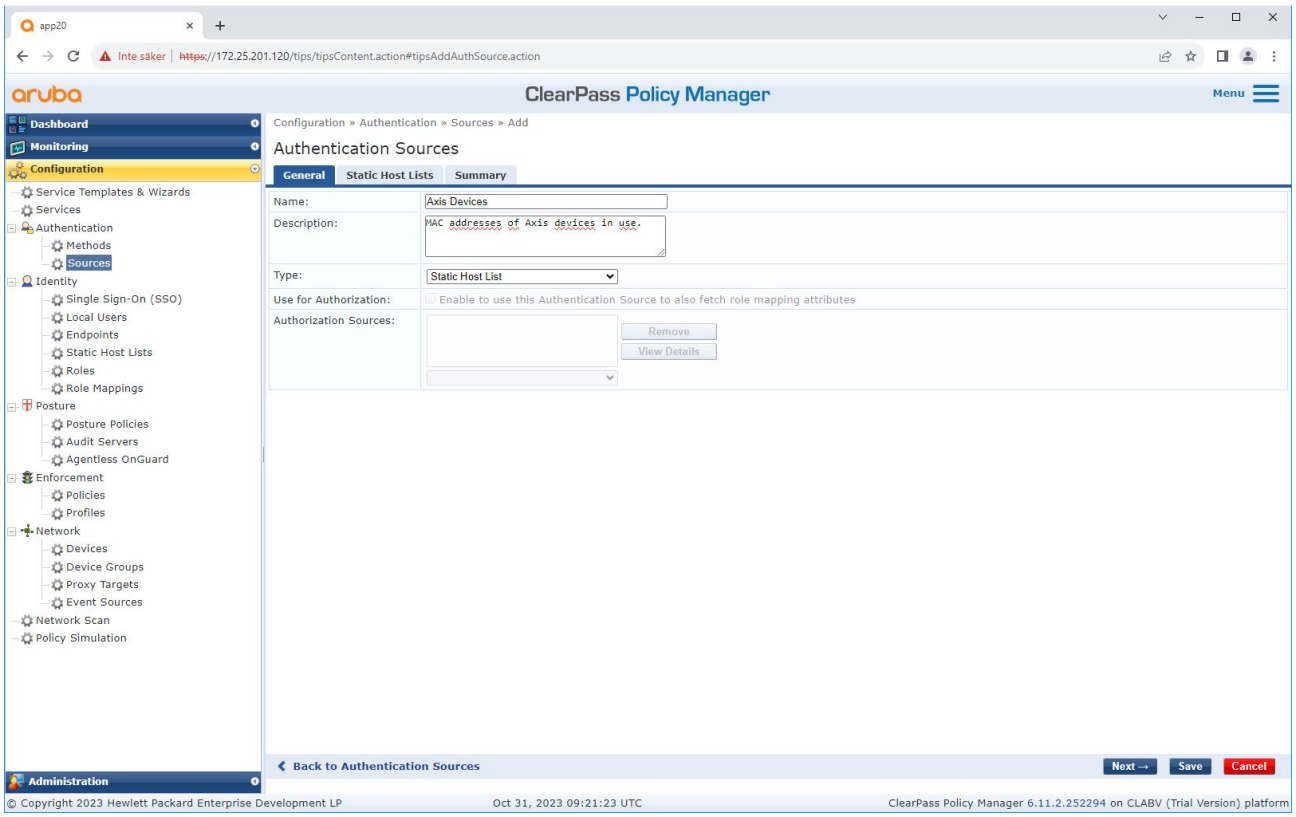
Ze względu na ryzyko sfałszowania adresów MAC dostęp do zwykłej sieci administracyjnej nie jest przyznawany. Zalecamy korzystanie z MAB tylko do wstępnego wdrożenia i ręczne sprawdzanie urządzenia w przyszłości.

Konfiguracja źródła

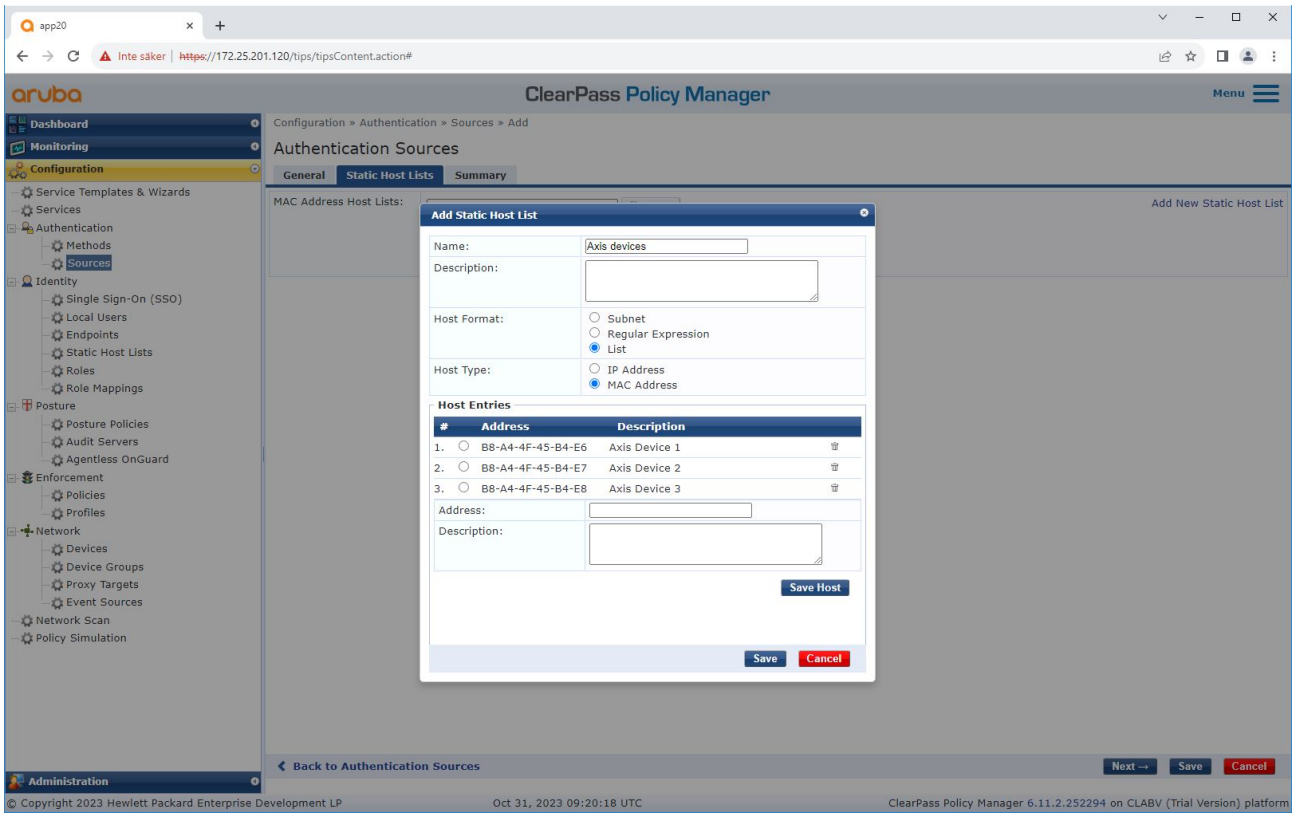
W interfejsie źródeł tworzone jest nowe źródło uwierzytelniania, które akceptuje tylko ręcznie importowane adresy MAC.



Wdrażanie starszej wersji — uwierzytelnianie MAC

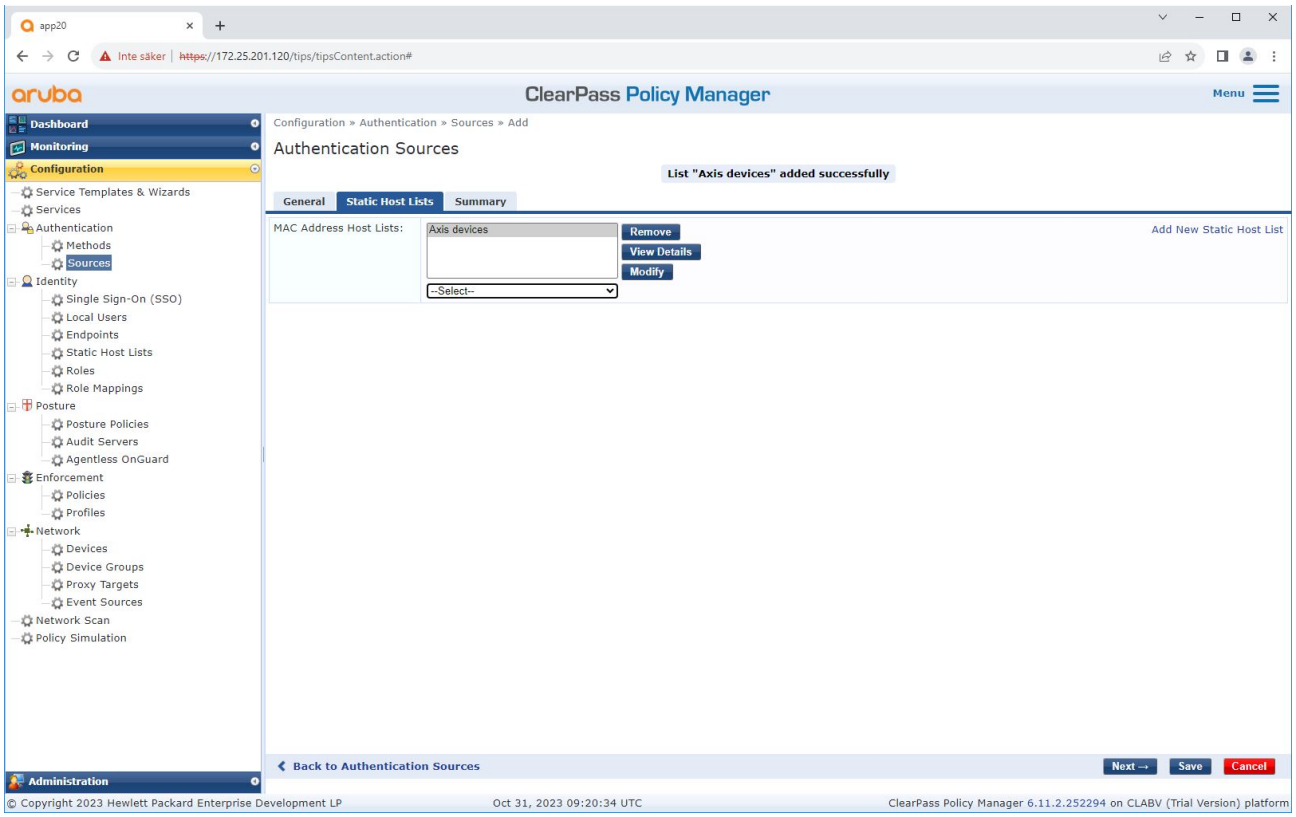


Wdrażanie starszej wersji — uwierzytelnianie MAC



Tworzona jest statyczna lista hostów zawierająca adresy MAC Axis.

Wdrażanie starszej wersji — uwierzytelnianie MAC

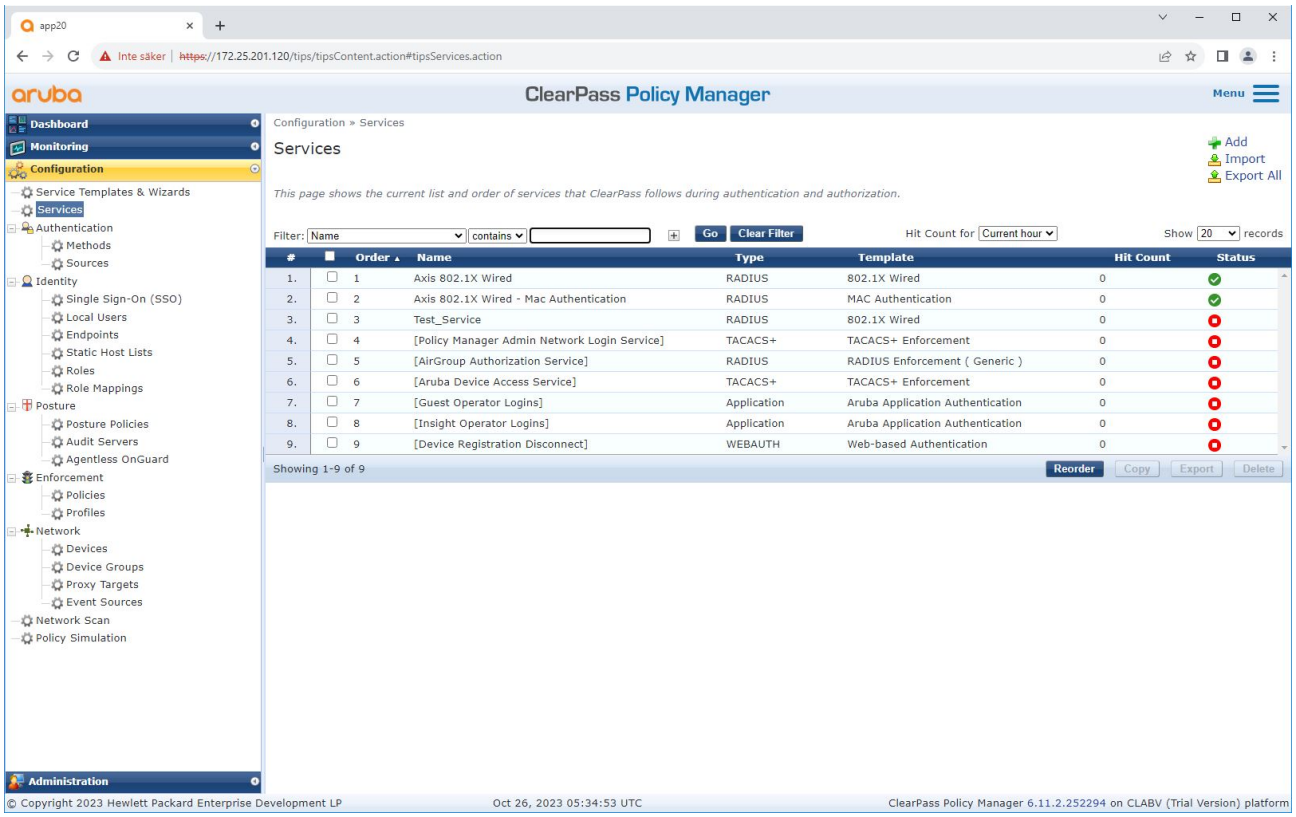


Konfiguracja usług

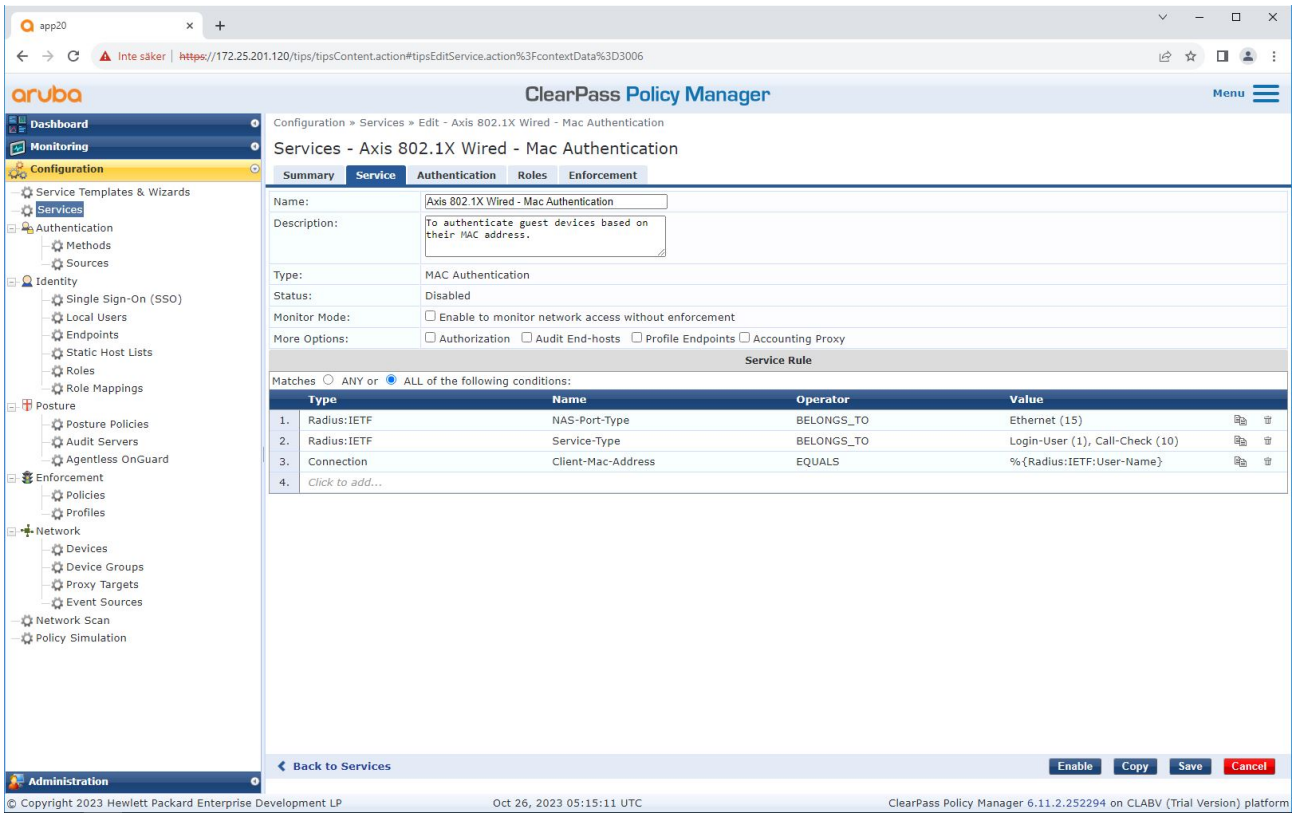
W interfejsie usług kroki konfiguracji są połączone w jedną usługę, która obsługuje uwierzytelnianie i autoryzację urządzeń Axis w sieciach Aruba.

Secure integration of Axis devices into Aruba networks

Wdrażanie starszej wersji — uwierzytelnianie MAC

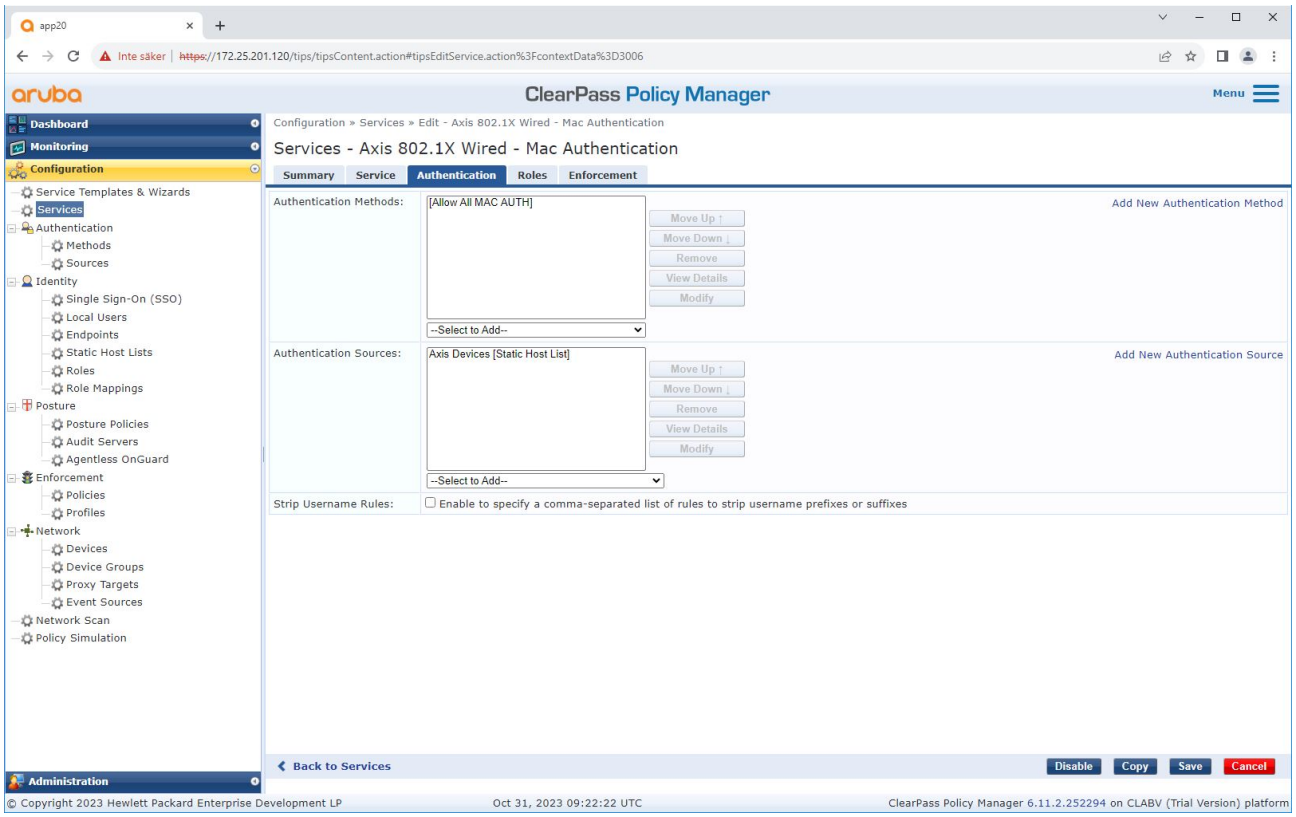


Wdrażanie starszej wersji — uwierzytelnianie MAC



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

Wdrażanie starszej wersji — uwierzytelnianie MAC

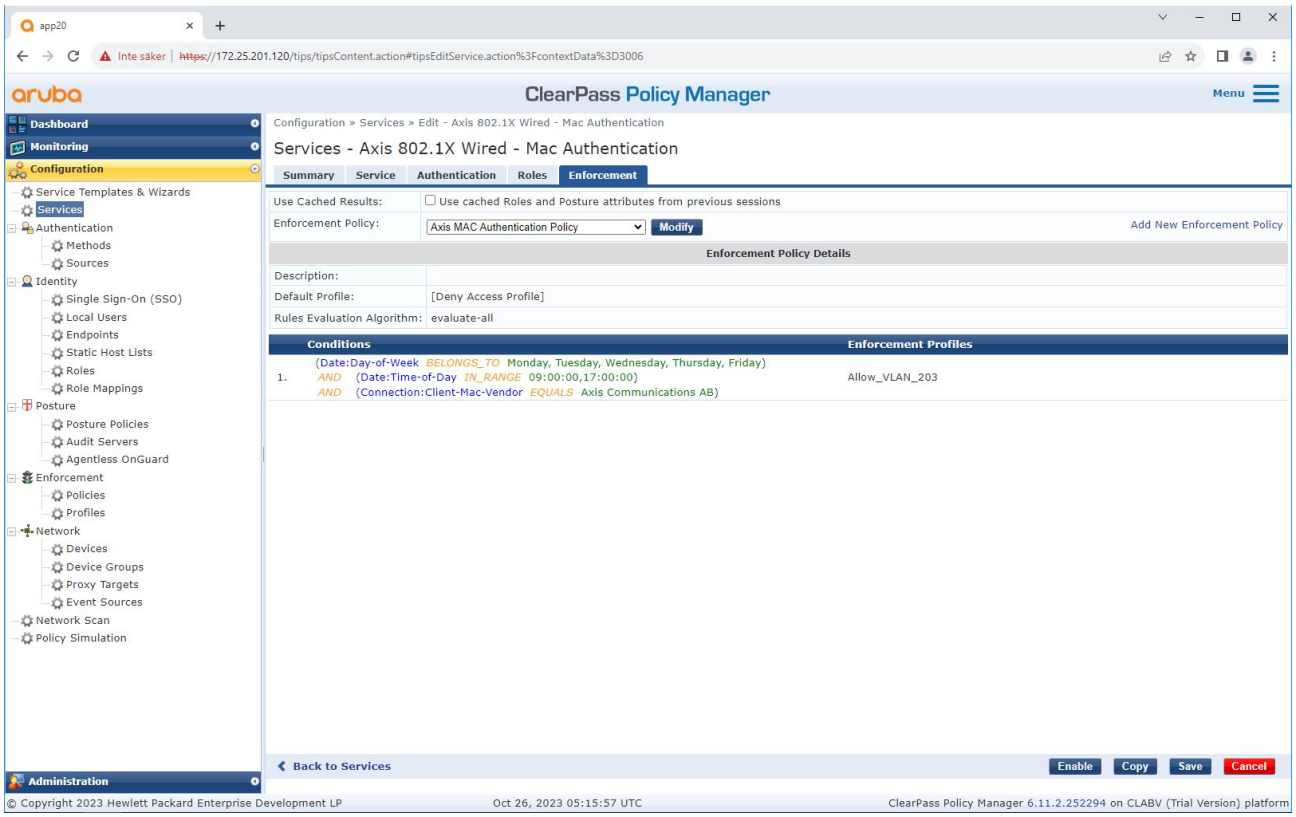


Dla usługi zostaje skonfigurowana metoda uwierzytelniania MAC z predefiniowanymi ustawieniami. Ponadto zostaje wybrane wcześniej utworzone źródło uwierzytelniania zawierające listę adresów MAC Axis.

Axis Communications AB korzysta z następujących adresów MAC OUI:

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

Wdrażanie starszej wersji — uwierzytelnianie MAC



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

Switch dostępowy Aruba

Oprócz konfiguracji bezpiecznego wdrażania opisanej w części *Switch dostępowy Aruba na stronie 16* zapoznaj się z poniższą przykładową konfiguracją portu dla switcha dostępowego Aruba, 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
```

Podręcznik użytkownika
Secure integration of Axis devices into Aruba networks

Wer. M4.3
Data: Listopad 2023
Numer części T10197992