HPE Aruba Networking

Podręcznik użytkownika

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
Zarządzanie certyfikatami – protokół Enrollment over Secure Transport (EST)....23
Główne zalety protokołu EST....23
Konfiguracja HPE Aruba ClearPass Onboard....23
Konfiguracja HPE Aruba ClearPass Policy Manager....25
Konfiguracja Axis....28
Wdrażanie starszej wersji — uwierzytelnianie MAC....33
HPE Aruba Networking ClearPass Policy Manager....33
Zasady wykonawcze....33
Konfiguracja źródła....34
Konfiguracja usług....35
Switch dostępowy HPE Aruba Networking....38

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 EEE 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.

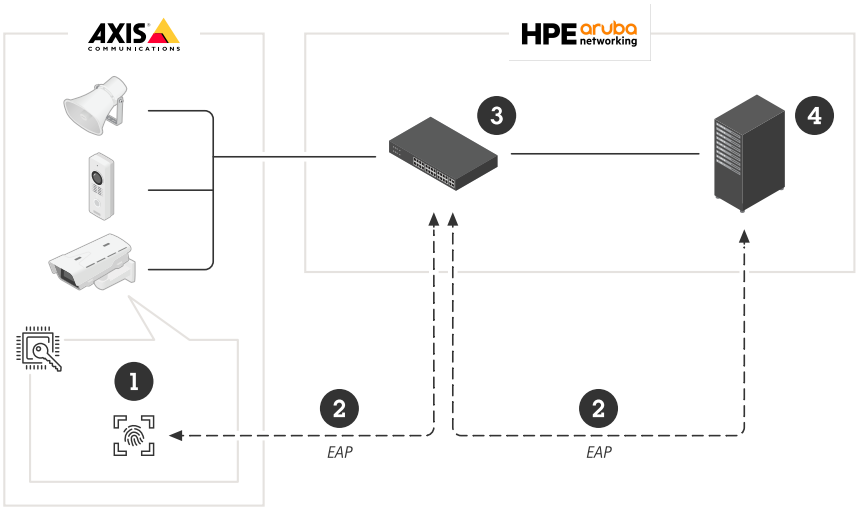
Bezpieczne wdrażanie urządzeń w sieciach o zerowym zaufaniu za pomocą protokołu IEEE 802.1X/802.1AR

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.

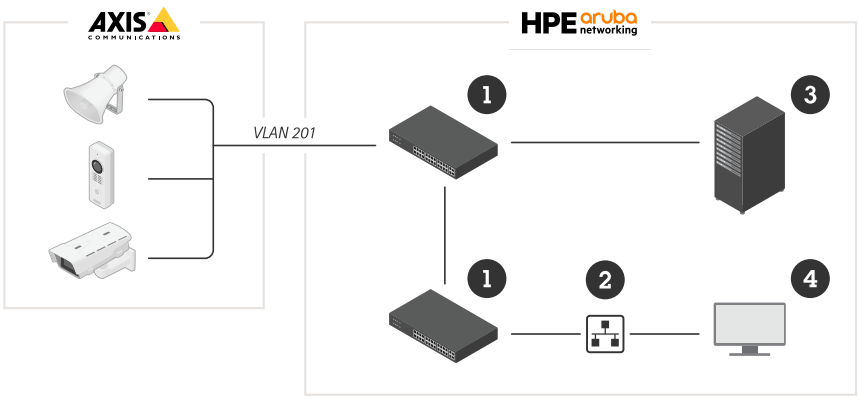


Urządzenie Axis uwierzytelnia się w sieci HPE Aruba Networking za pomocą certyfikatu identyfikatora urządzenia Axis zgodnego ze standardem IEEE 802.1AR.

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.

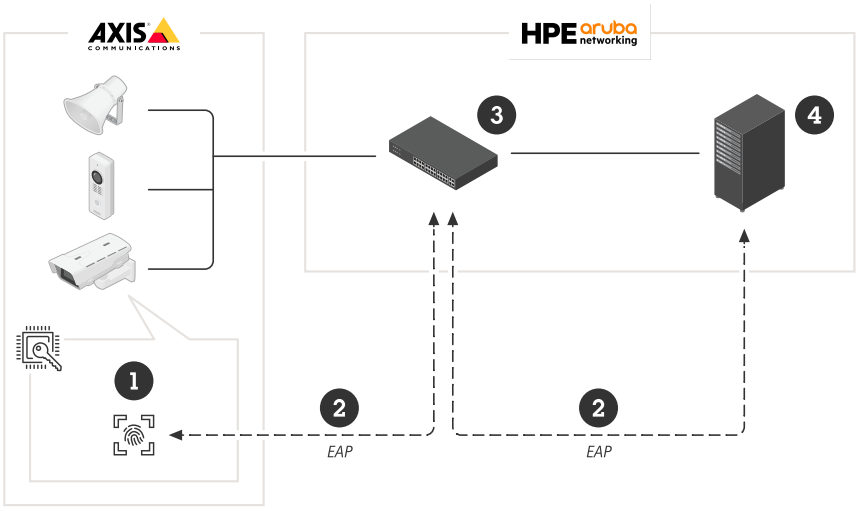


Po pomyślnym uwierzytelnieniu urządzenie Axis zostaje przeniesione do sieci obsługi administracyjnej w celu konfiguracji.

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

Sieciowe środowisko produkcyjne

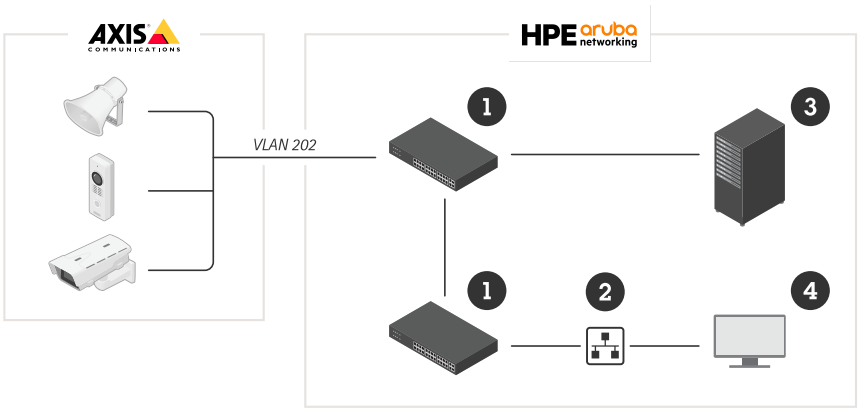
Udostępnienie urządzeniu Axis nowych certyfikatów IEEE 802.1X wyzwala kolejną próbę uwierzytelnienia. ClearPass Policy Manager zweryfikuje nowe certyfikaty i zdecyduje, czy przenieść urządzenie Axis do sieci produkcyjnej.



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*

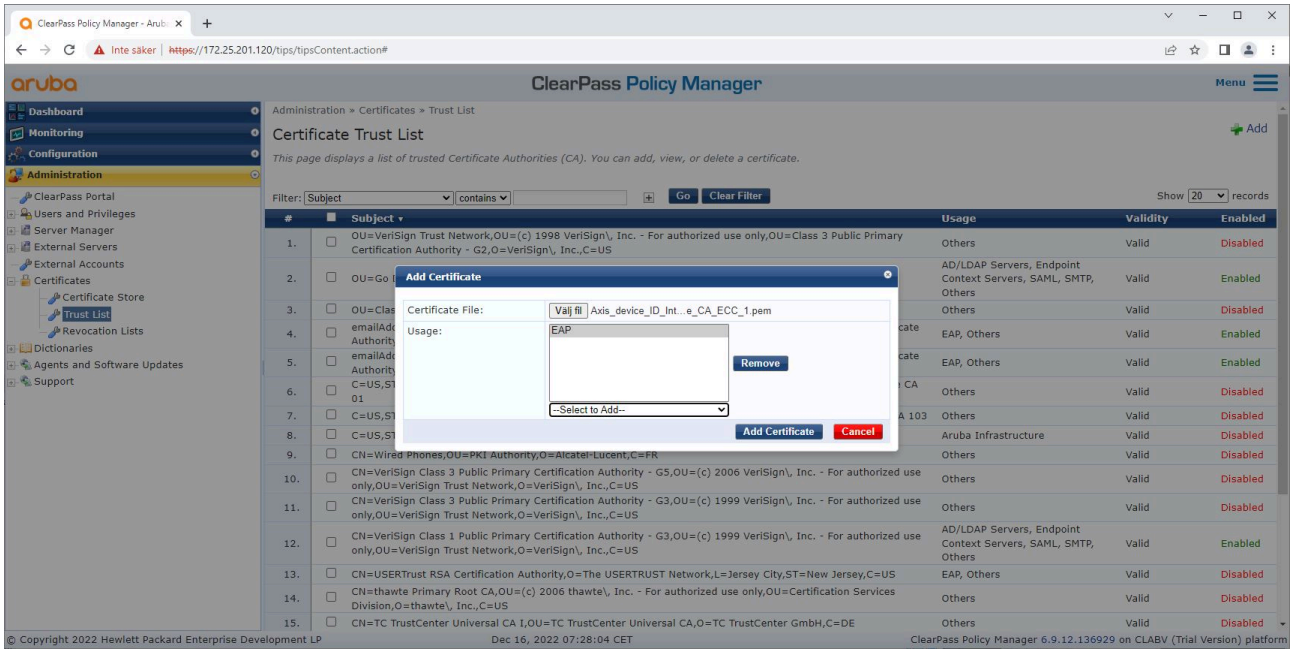
Konfigurowanie sieci HPE Aruba Networking

HPE Aruba Networking ClearPass Policy Manager

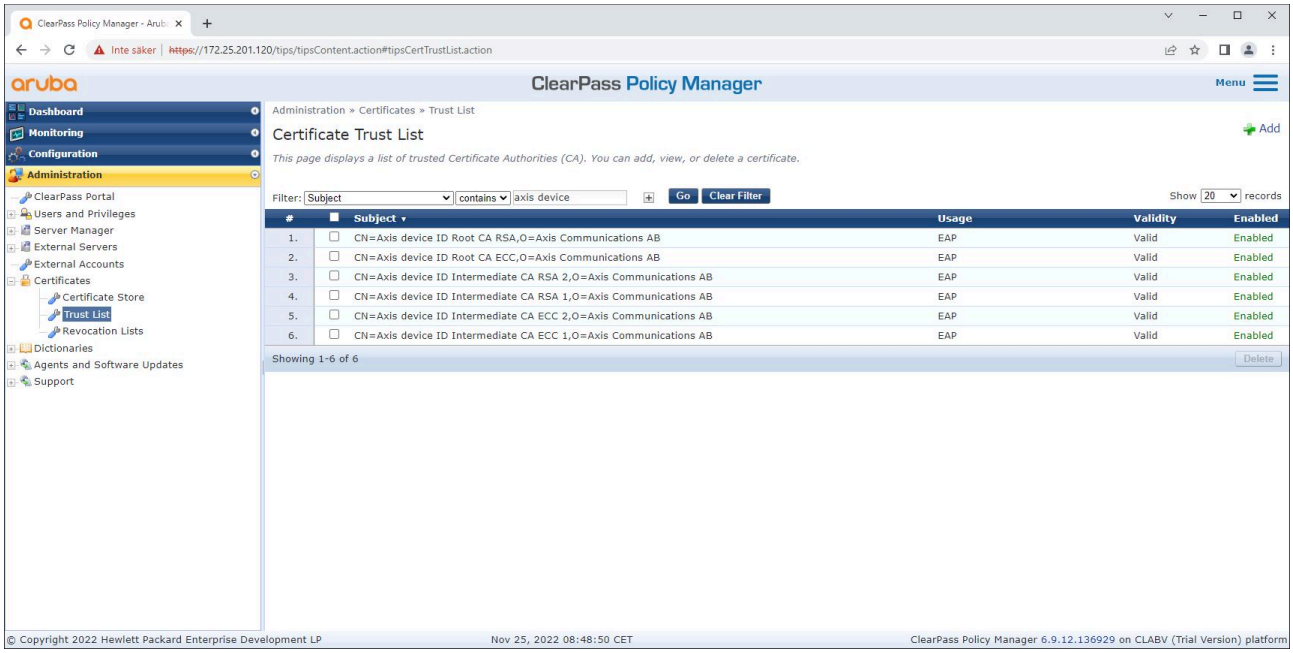
ClearPass Policy Manager zapewnia opartą na rolach i urządzeniach bezpieczną kontrolę dostępu do sieci dla IoT, BYOD, urządzeń firmowych, pracowników, wykonawców i gości w ramach infrastruktury przewodowej, bezprzewodowej i VPN wielu dostawców.

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



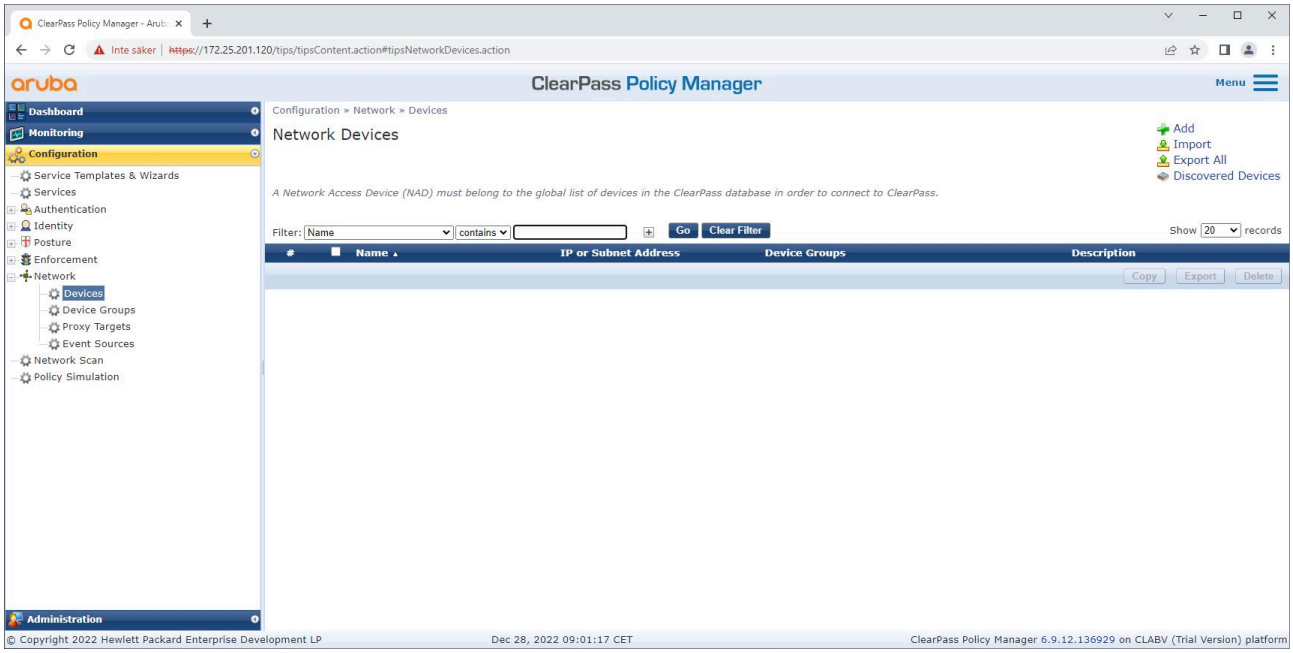
Prześlij certyfikaty IEEE 802.1AR specyficzne dla firmy Axis do zaufanego magazynu certyfikatów narzędzia ClearPass Policy Manager.



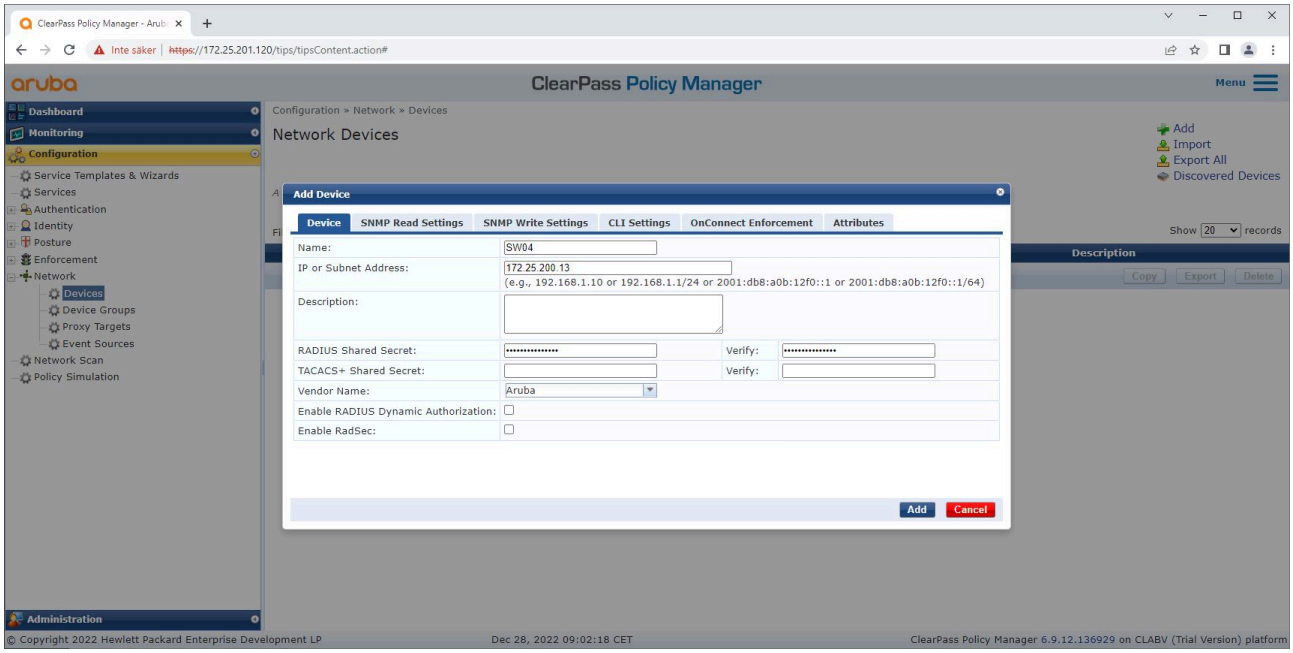
Zaufany magazyn certyfikatów w narzędziu ClearPass Policy Manager z dołączonym łańcuchem certyfikatów IEEE 802.1AR firmy Axis.

Konfiguracja urządzenia/grupy sieciowej

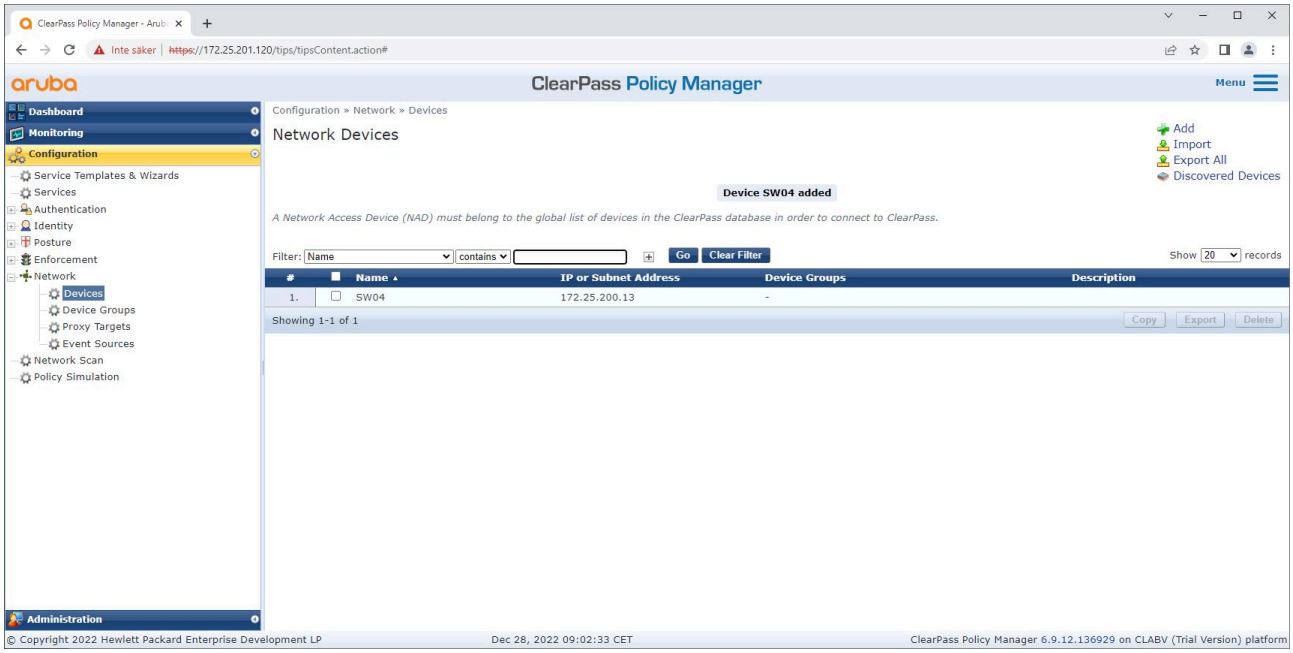
1. Dodawanie zaufanych urządzeń dostępu do sieci takich jak switche dostępowe HPE Aruba Networking do narzędzia ClearPass Policy Manager. Menedżer zasad ClearPass Policy Manager musi wiedzieć, które switche dostępowe w sieci są używane do komunikacji IEEE 802.1X. Uwaga: współdzielony sekret RADIUS musi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



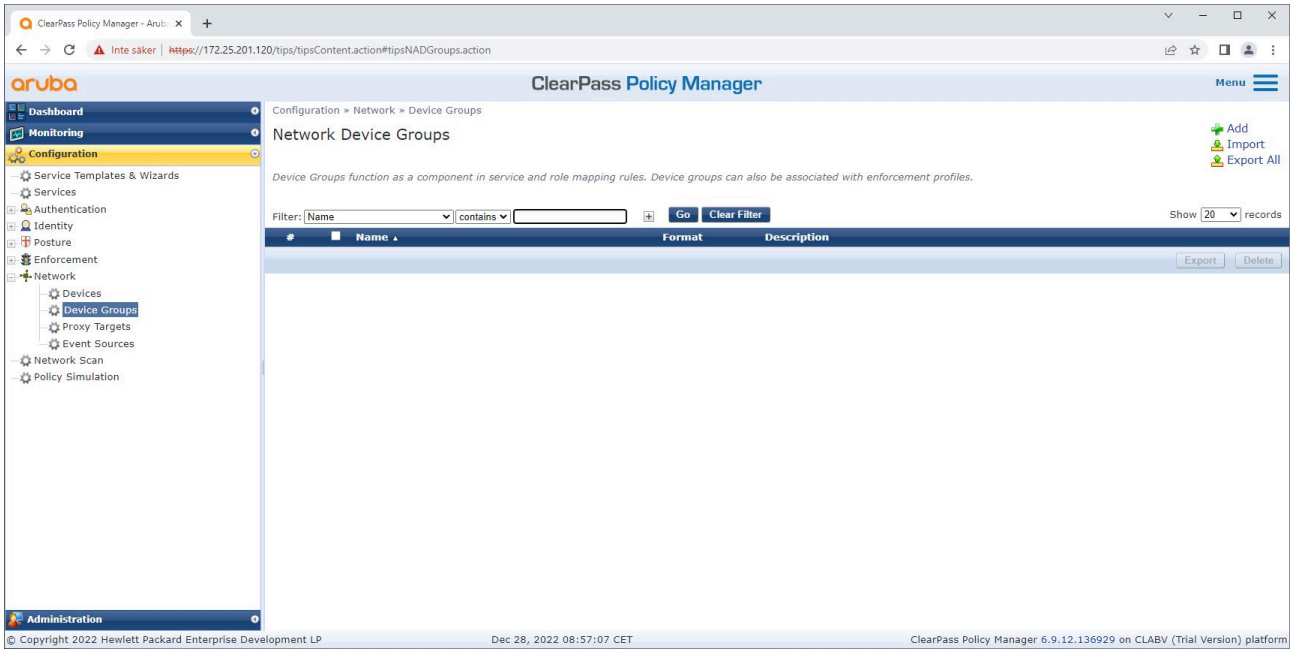
Interfejs zaufanych urządzeń sieciowych w narzędziu ClearPass Policy Manager.



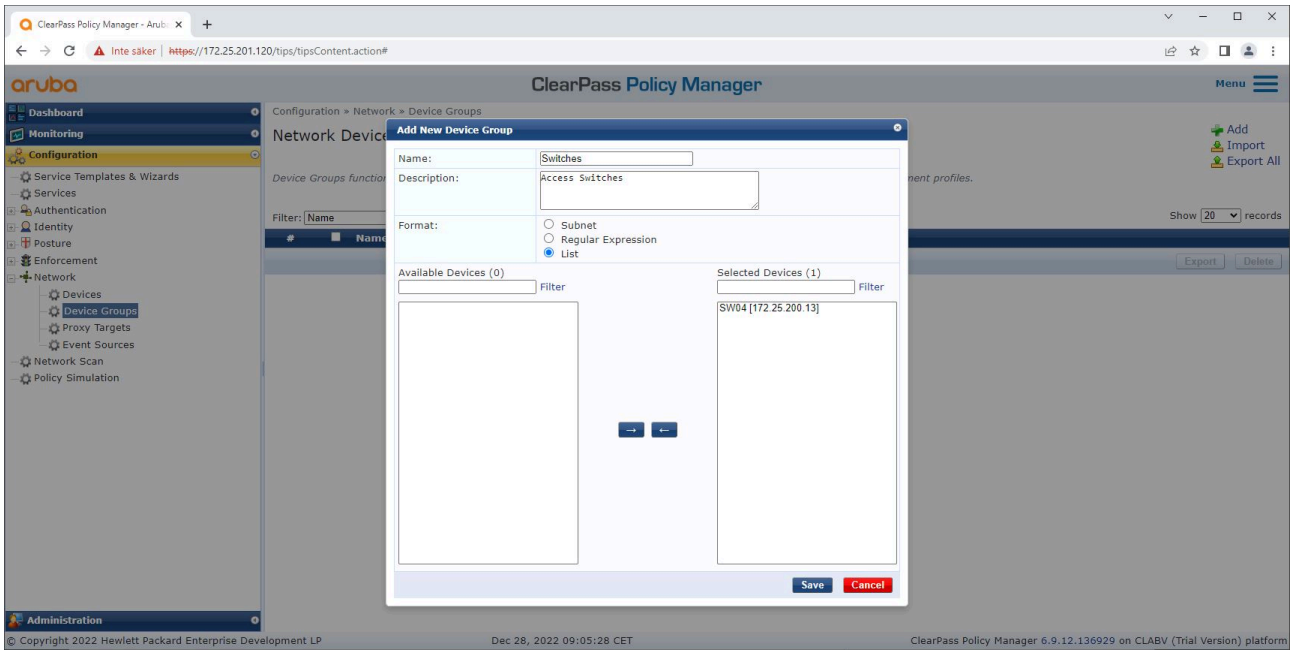
Dodawanie switcha dostępowego HPE Aruba Networking jako zaufanego urządzenia w narzędziu ClearPass Policy Manager. Uwaga: współdzielony sekret RADIUS musi odpowiadać konkretnej konfiguracji switcha IEEE 802.1X.



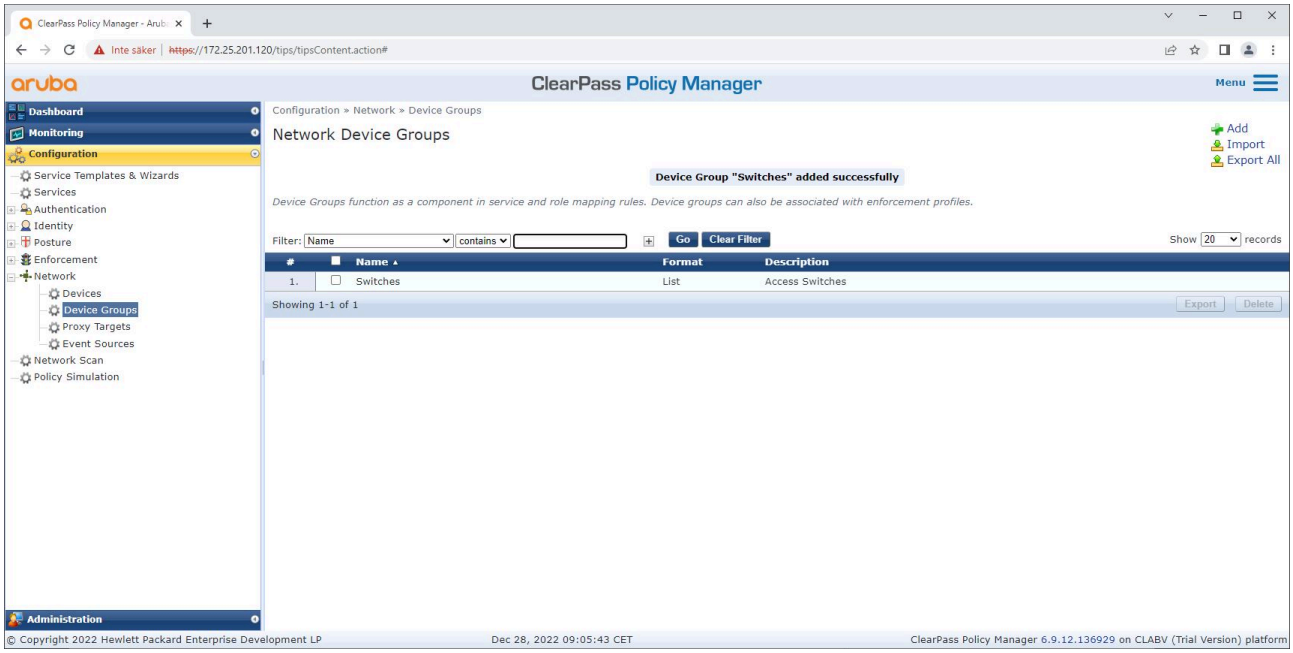
ClearPass Policy Manager ze skonfigurowanym jednym zaufanym urządzeniem sieciowym.



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.

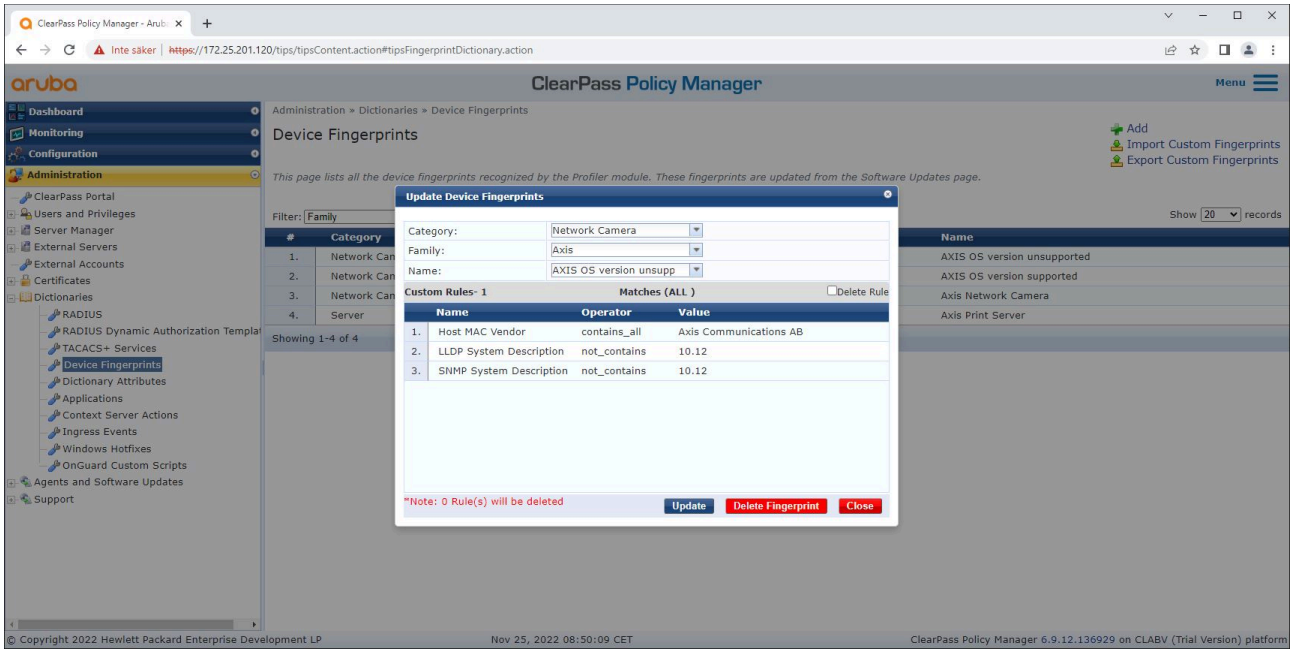


ClearPass Policy Manager ze skonfigurowaną grupą urządzeń sieciowych, która zawiera jedno lub więcej zaufanych urządzeń sieciowych.

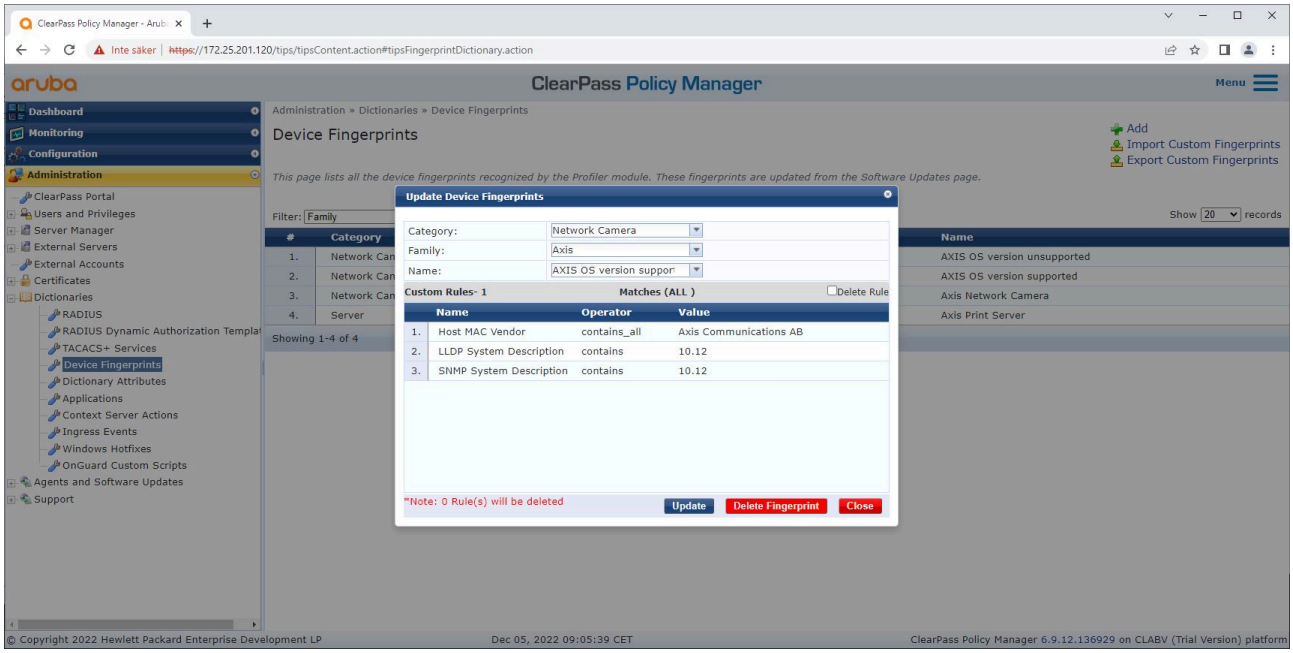
Konfiguracja odcisku palca urządzenia

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.



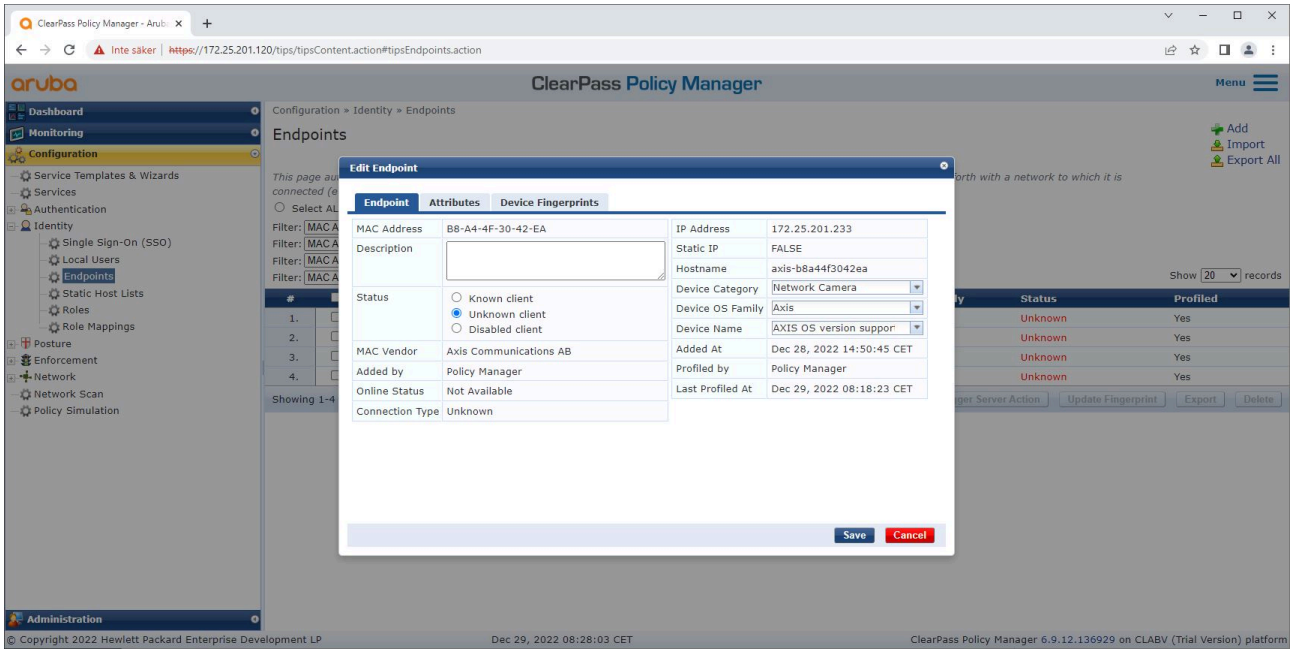
Konfiguracja odcisku palca urządzenia w narzędziu ClearPass Policy Manager. Urządzenia Axis z systemem operacyjnym AXIS OS w wersji innej niż 10.12 są obsługiwane w tym przykładzie.

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

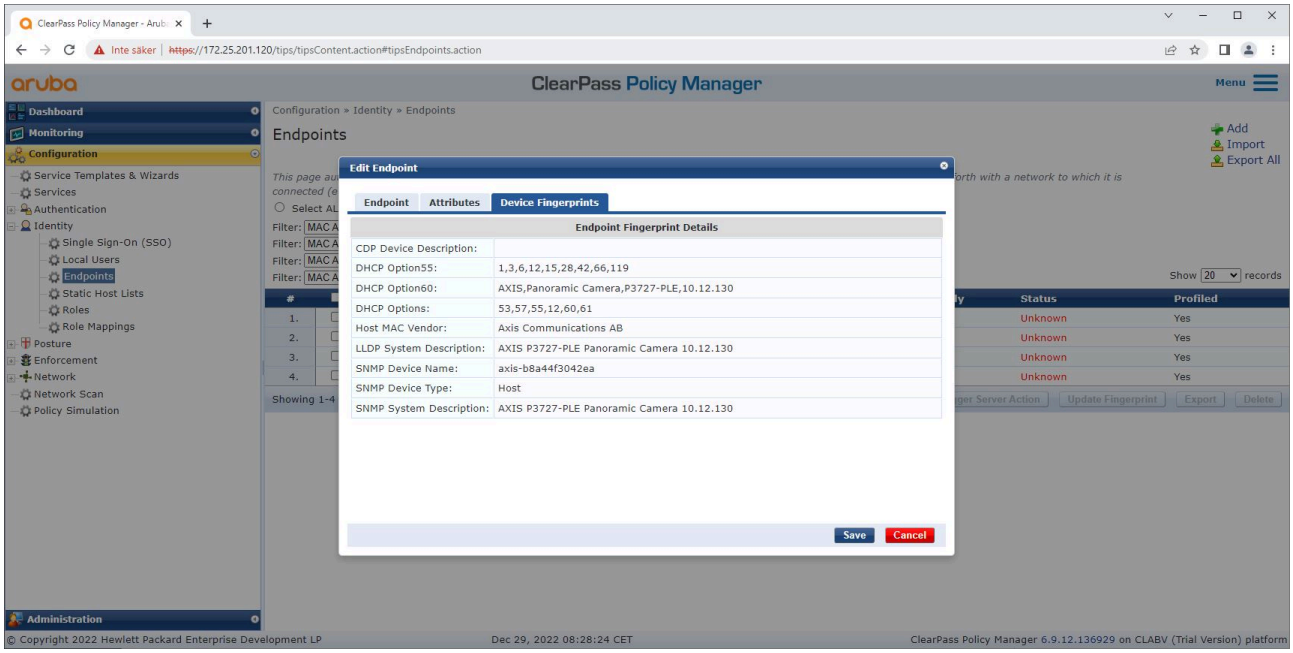
1. Otwórz menu **Configuration > Identity > Endpoints (Konfiguracja > Tożsamość > Punkty końcowe)**.
2. Wybierz urządzenia, które chcesz wyświetlić.
3. Kliknij kartę **Device Fingerprints (Odciski palca urządzenia)**.

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.

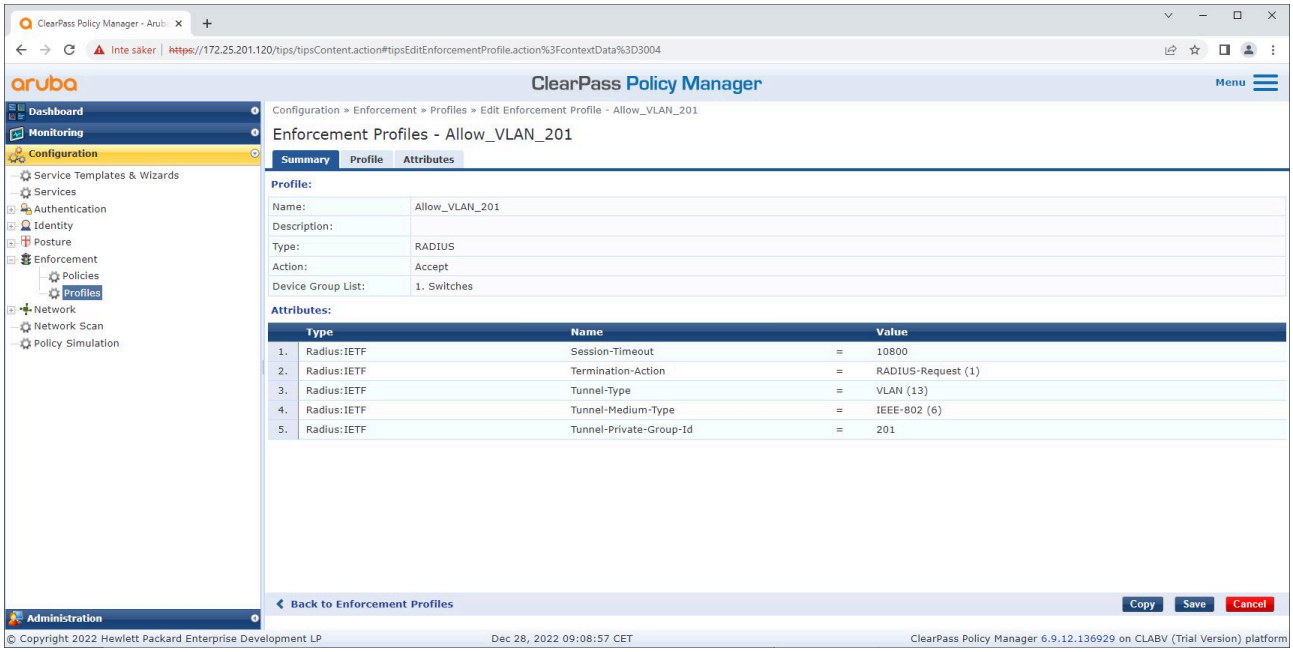


Szczegółowe odciski palców sprofilowanego urządzenia Axis. Należy pamiętać, że protokół SNMP jest domyślnie wyłączony w urządzeniach Axis. Informacje dotyczące wykrywania specyficzne dla protokołów LLDP, CDP i DHCP są udostępniane przez urządzenie Axis w domyślnym stanie fabrycznym i przekazywane przez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

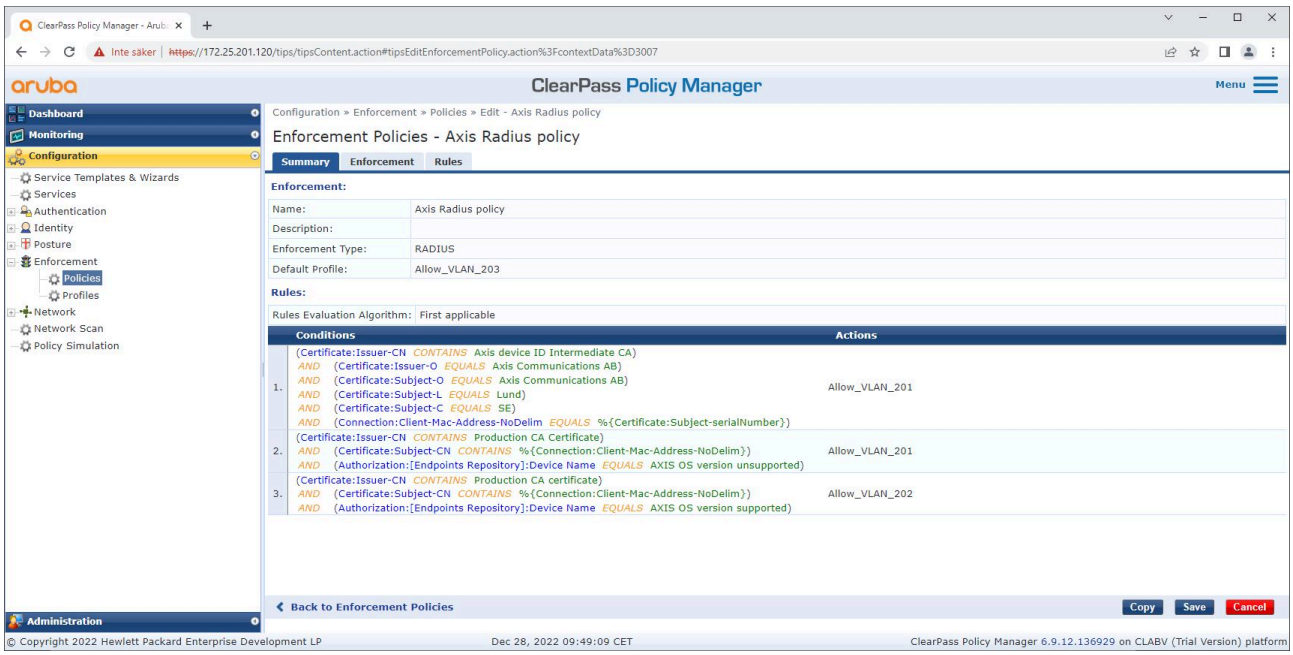
Konfiguracja profilu wykonywania

Za pomocą profilu wykonywania ClearPass Policy Manager może przypisywać określony identyfikator sieci VLAN do portu dostępu na switchu. Decyzja ta jest oparta na zasadach i ma zastosowanie do urządzeń sieciowych w grupie „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.

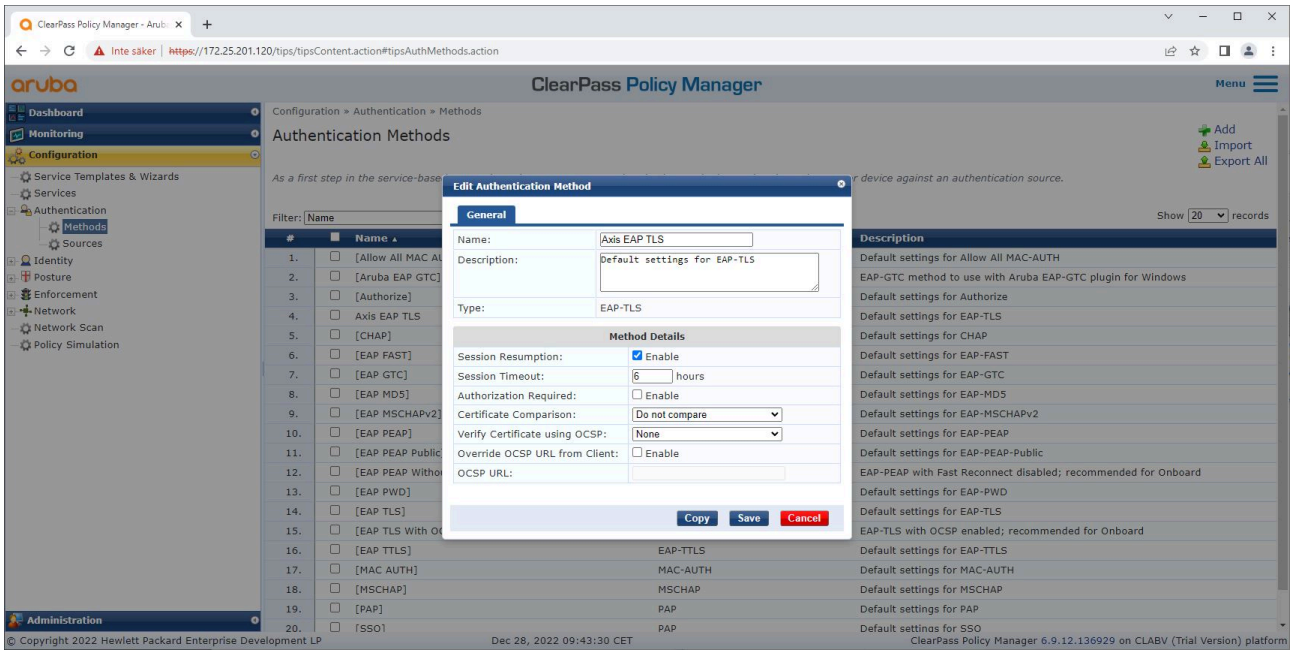
Sieć produkcyjna (VLAN 202)

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

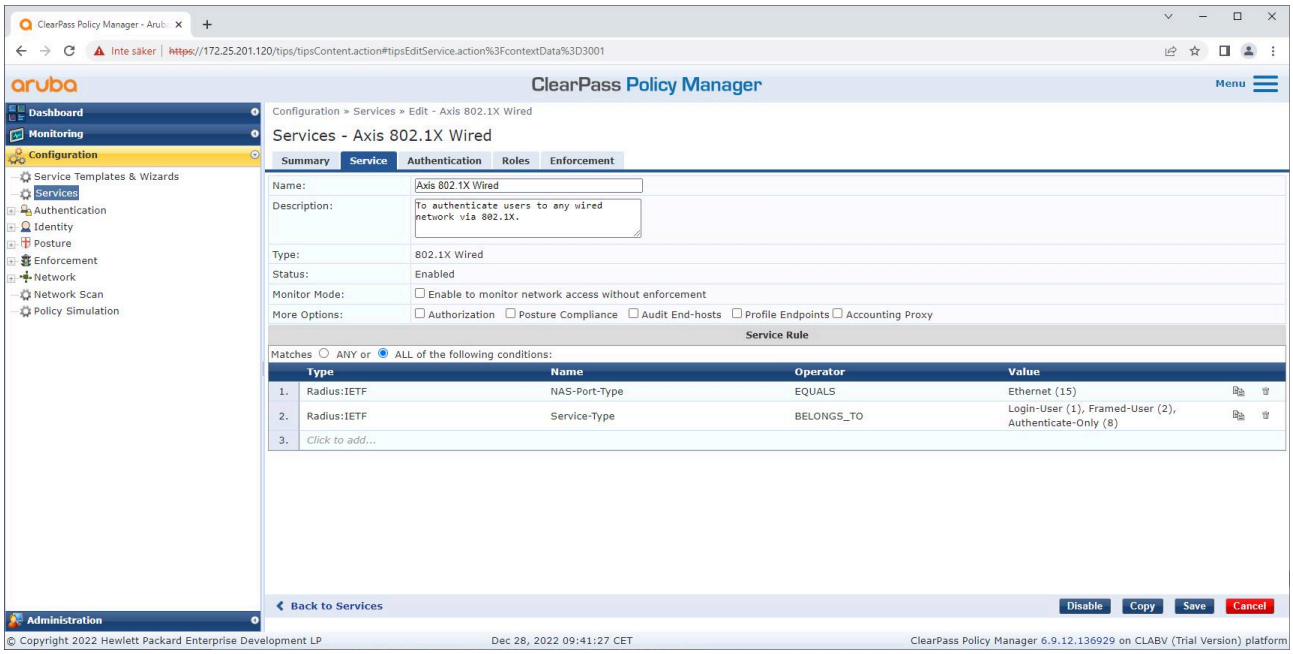
Metoda uwierzytelniania określa sposób, w jaki urządzenie Axis próbuje uwierzytelnić się w sieci. Preferowaną metodą jest IEEE 802.1X EAP-TLS, ponieważ urządzenia Axis z obsługą Axis Edge Vault mają domyślnie włączoną funkcję IEEE 802.1X EAP-TLS.



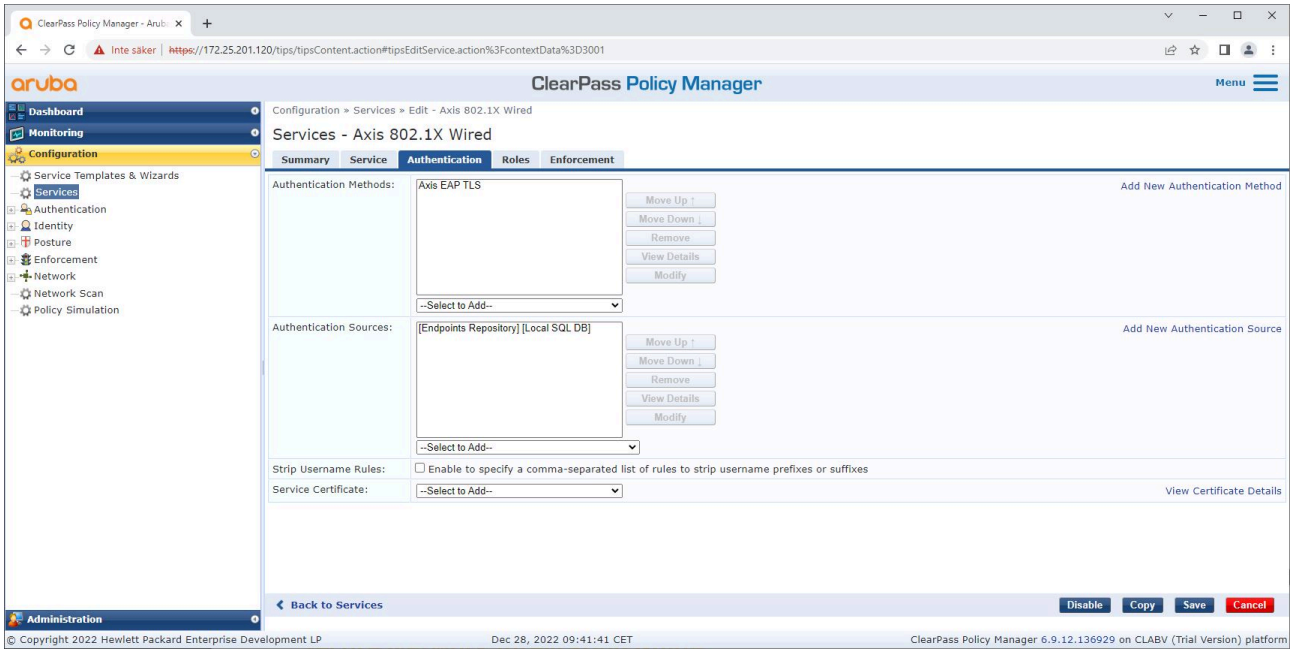
Interfejs metody uwierzytelniania narzędzia ClearPass Policy Manager, w którym zdefiniowana jest metoda uwierzytelniania EAP-TLS dla urządzeń Axis.

Konfiguracja usług

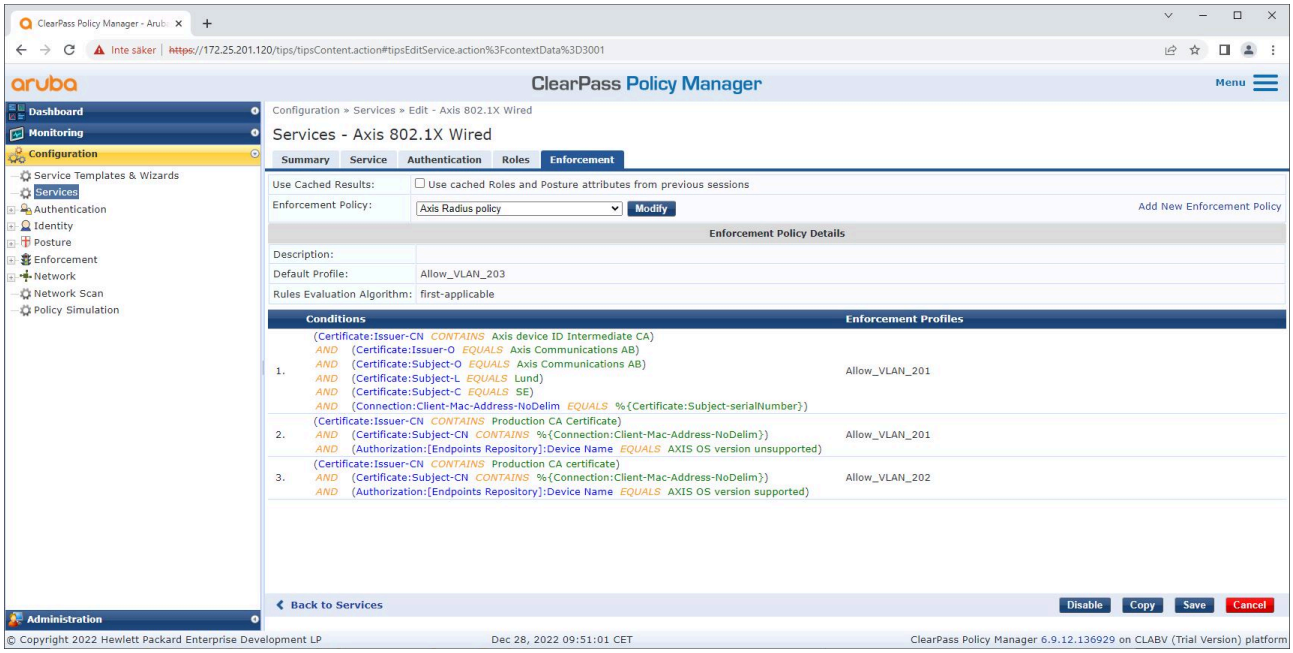
Na stronie **Services (Usługi)** kroki konfiguracji są połączone w jedną usługę, która obsługuje uwierzytelnianie i autoryzację urządzeń Axis w sieciach HPE Aruba Networking.



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.

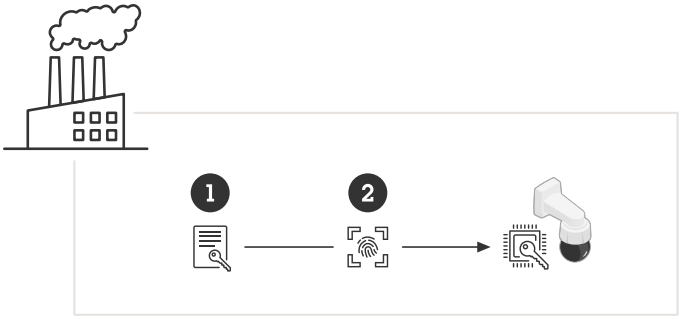
```
radius-server host MyRADIUSIPAddress key "MyRADIUSKey"
```

```
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.



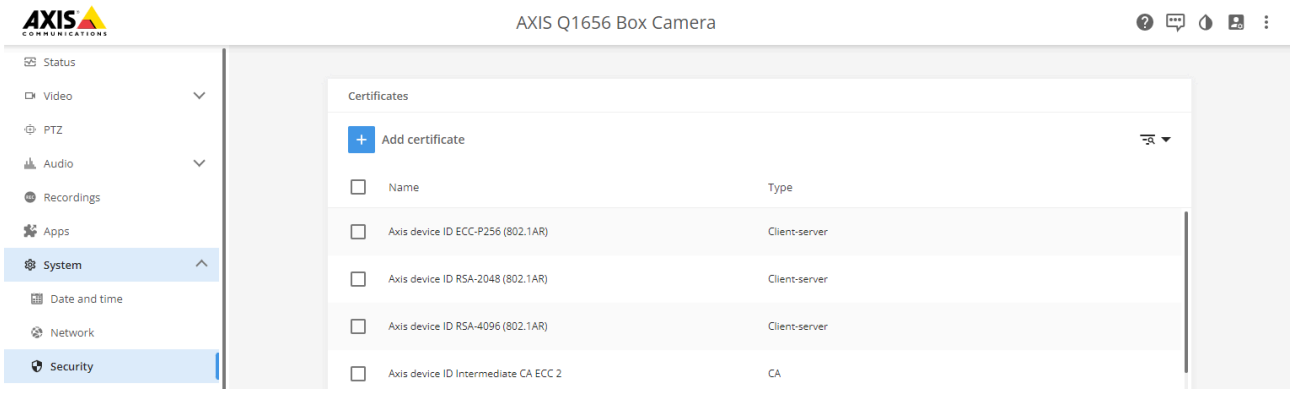
Urządzenia Axis mają fabryczne certyfikaty identyfikatorów urządzenia Axis zgodne z IEEE 802.1AR dla zaufanych usług identyfikacji urządzeń

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.

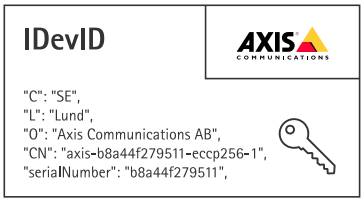
Uwaga

Numer seryjny urządzenia Axis jest jednocześnie jego adresem MAC.



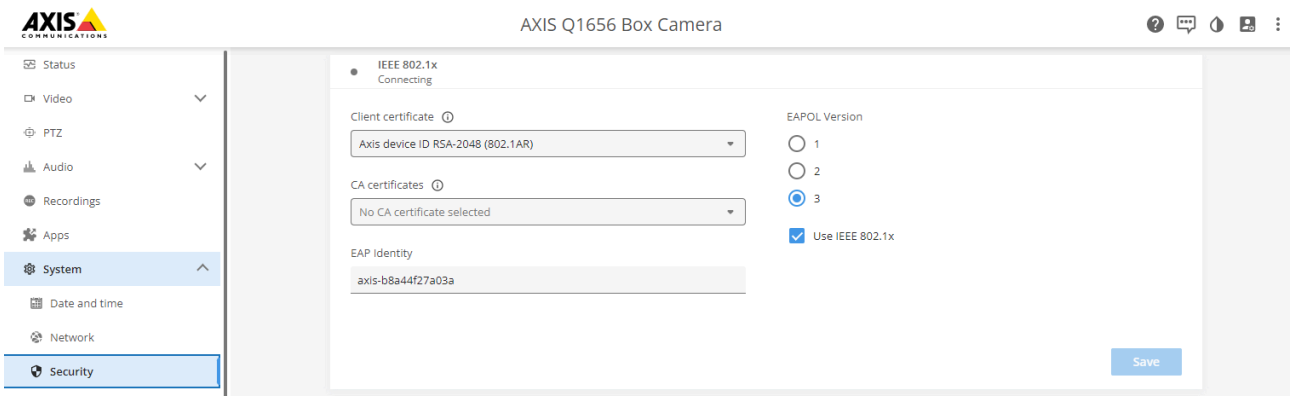
Magazyn certyfikatów urządzenia Axis w domyślnym stanie fabrycznym, z identyfikatorem urządzenia Axis.

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 konfigurowania wielu urządzeń Axis i zarządzania nimi w ekonomiczny sposób. AXIS Device Manager to aplikacja oparta na Microsoft Windows®, która jest instalowana 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 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

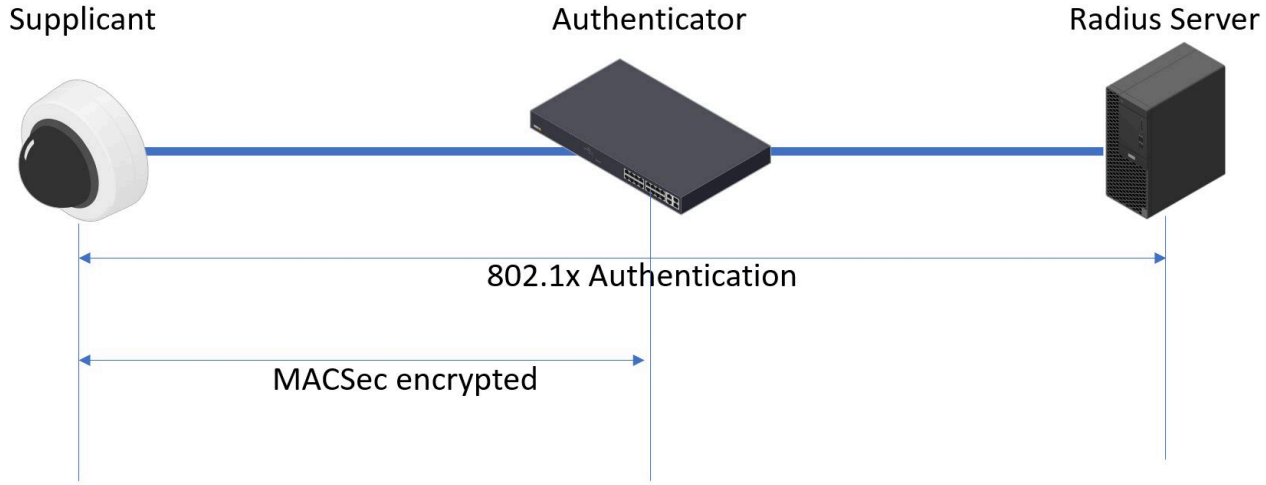
Aby obejrzeć ten film wideo, przejdź do internetowej wersji dokumentu.

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

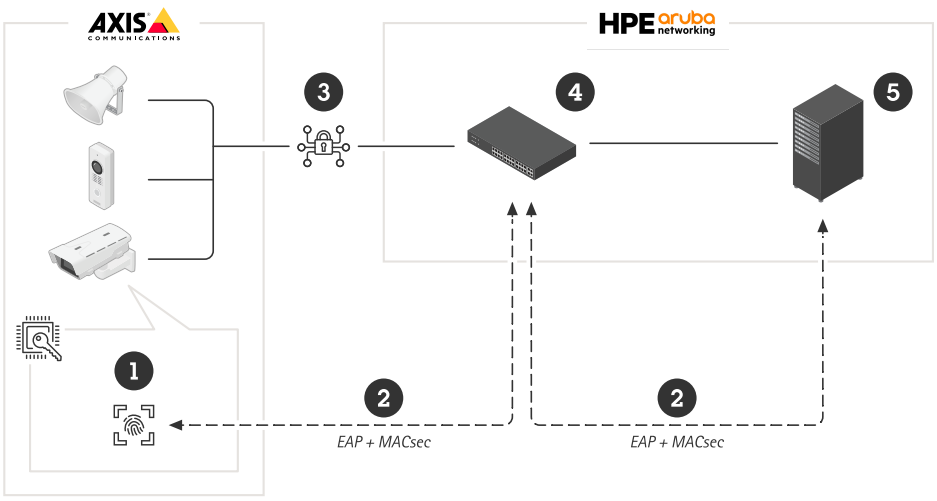
IEEE 802.1AE MACsec (Media Access Control Security) to precyzyjnie zdefiniowany protokół sieciowy, który kryptograficznie zabezpiecza połączenia Ethernet typu punkt-punkt w warstwie sieciowej 2. Zapewnia poufność i integralność transmisji danych między dwoma hostami.

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.



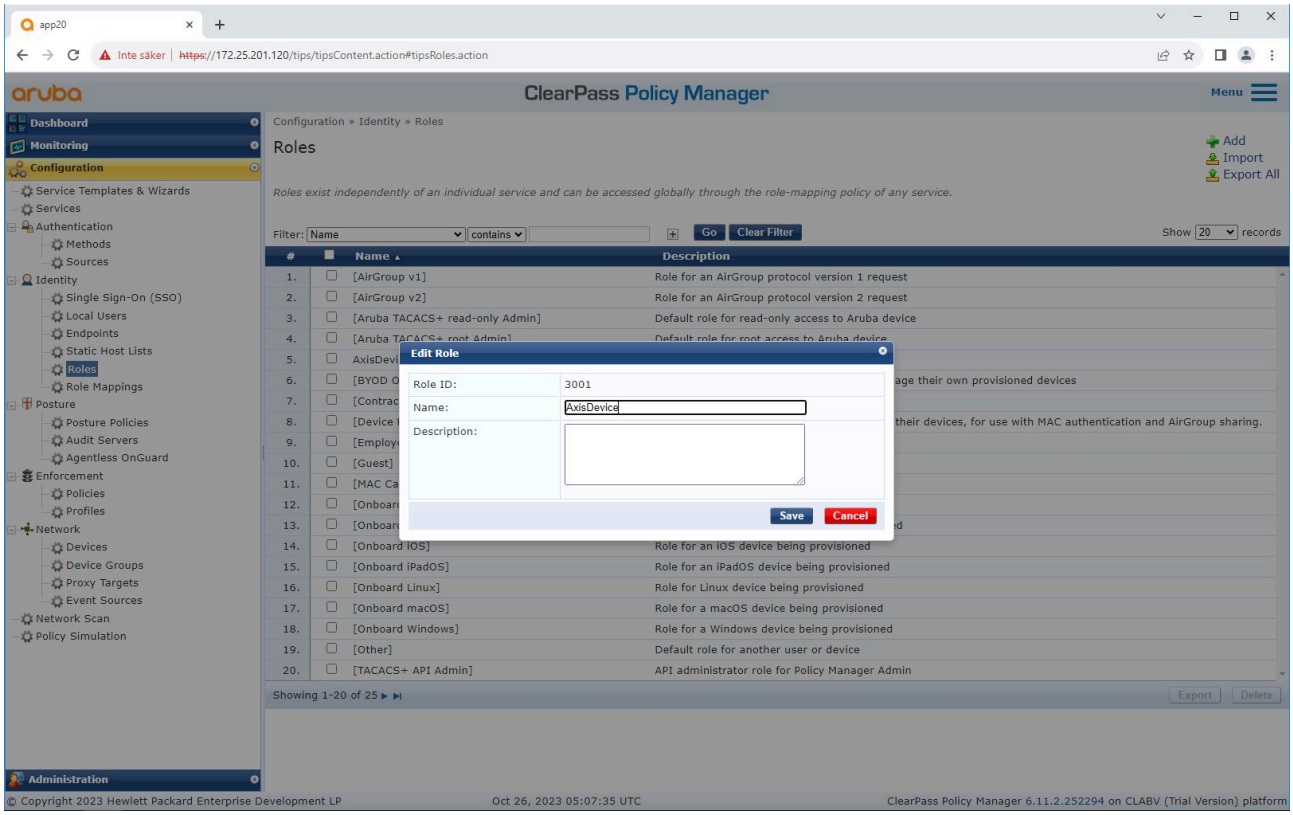
Bezpiecznie przechowywany identyfikator urządzenia Axis ID (1) – tożsamość urządzenia zgodna ze standardem IEEE 802.1AR – służy do uwierzytelniania w sieci (4, 5) za pomocą kontroli dostępu do sieci IEEE 802.1X EAP-TLS w oparciu o porty (2). W trakcie całej sesji EAP-TLS automatycznie wymieniane są klucze 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.

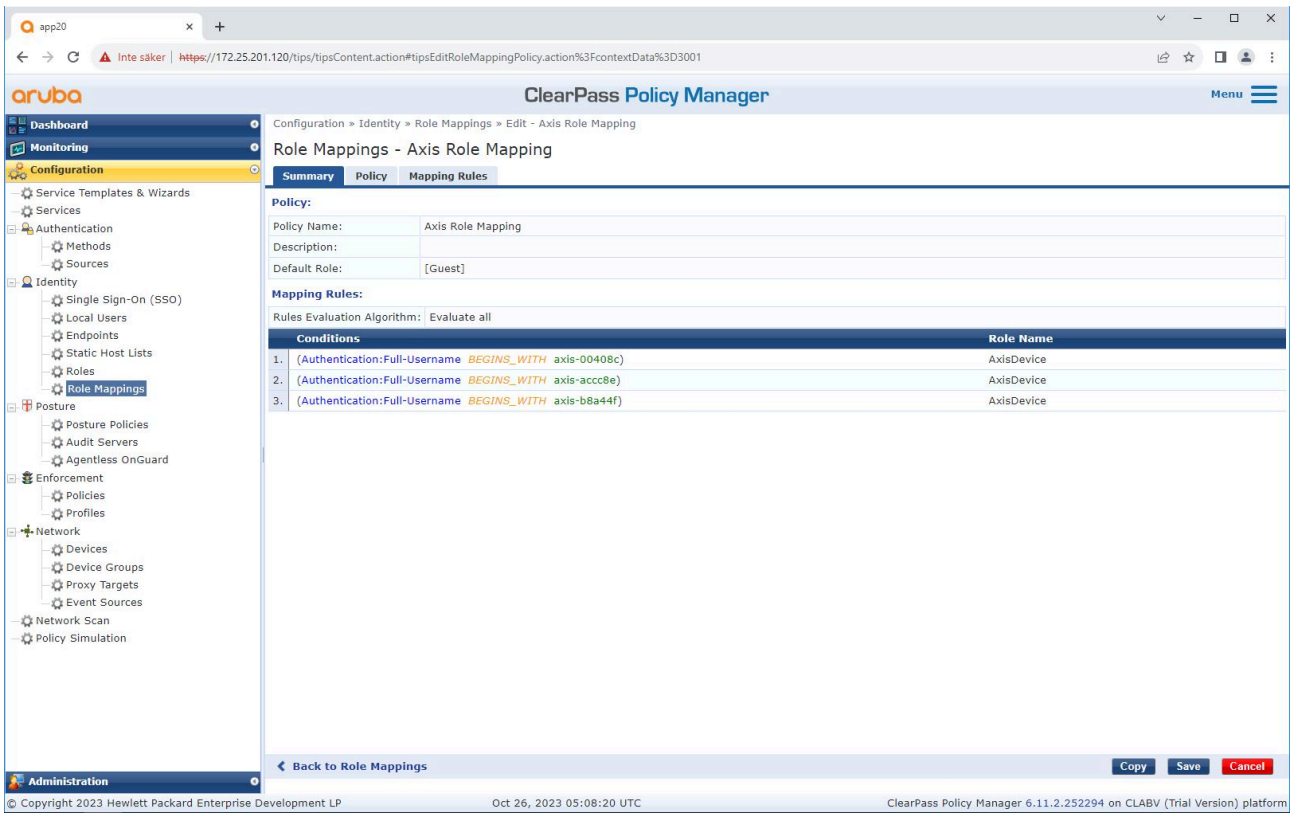
Jeśli switch dostępowy HPE Aruba Networking nie obsługuje szyfrowania MACsec przez EAP-TLS, można użyć trybu klucza PSK i skonfigurować ręcznie.

HPE Aruba Networking ClearPass Policy Manager

Role i zasady mapowania ról



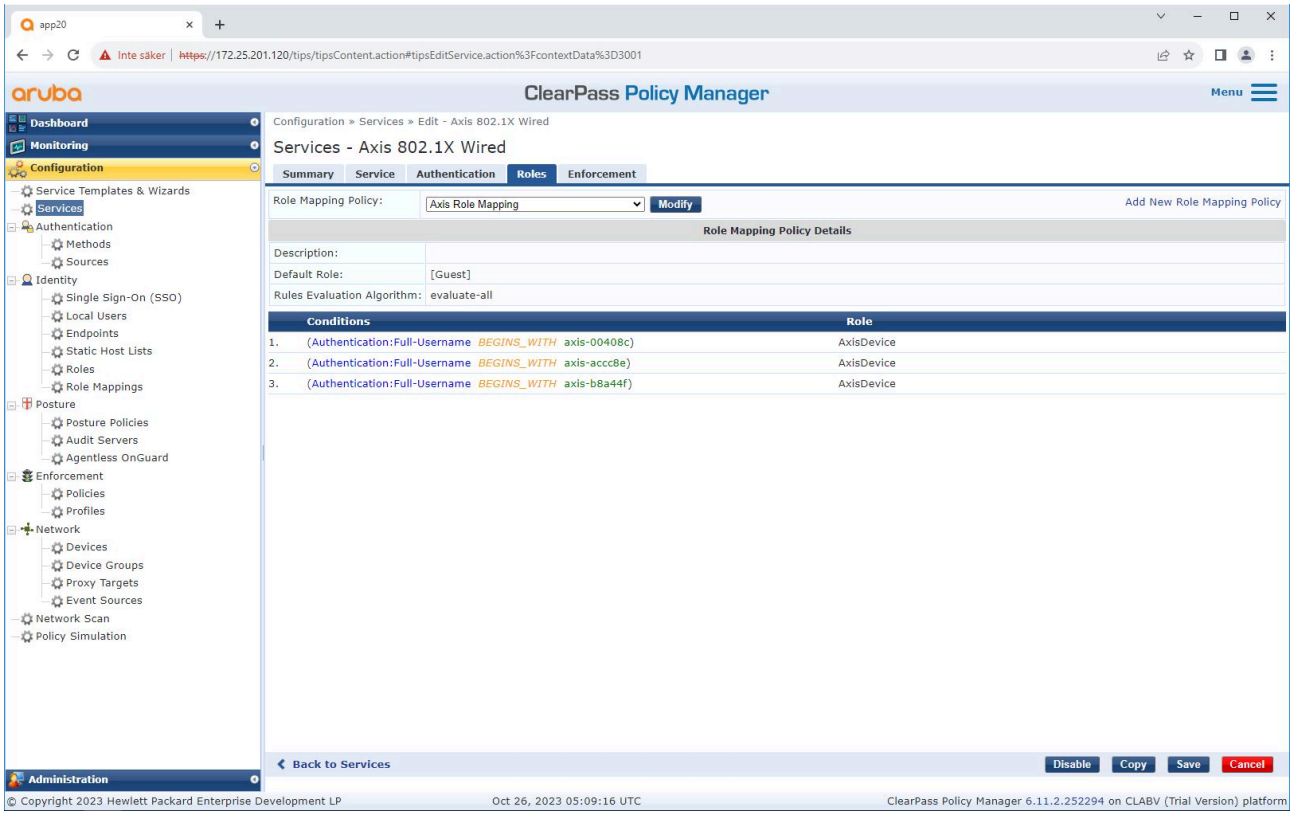
Dodawanie nazwy roli dla urządzeń Axis. Nazwa jest nazwą roli dostępu do portu w konfiguracji switcha dostępowego.



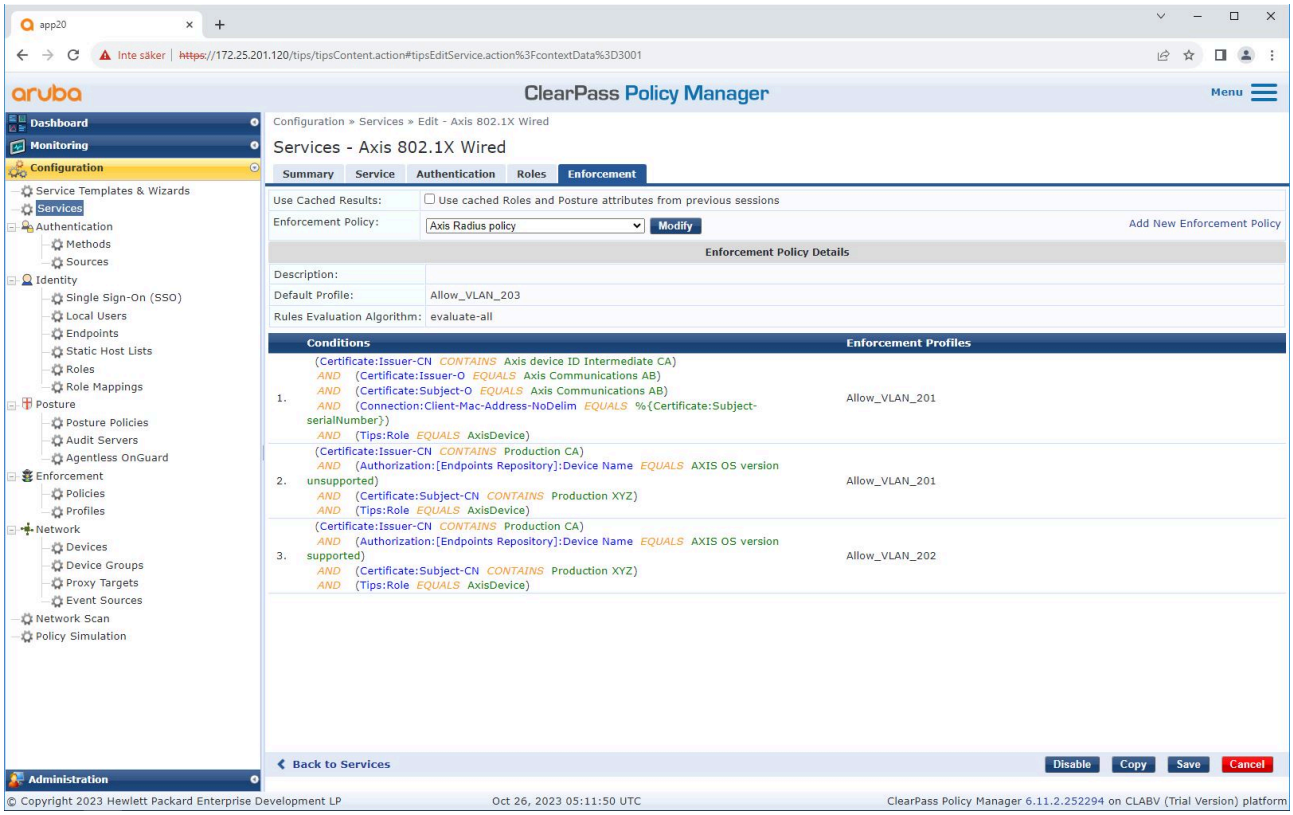
Dodawanie zasad mapowania ról Axis do utworzonej wcześniej roli urządzenia Axis. Spełnienie określonych warunków jest wymagane, aby urządzenie mogło zostać zmapowane do roli urządzenia Axis. Jeśli warunki nie zostaną spełnione, urządzenie będzie częścią roli [Guest] (gość).

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

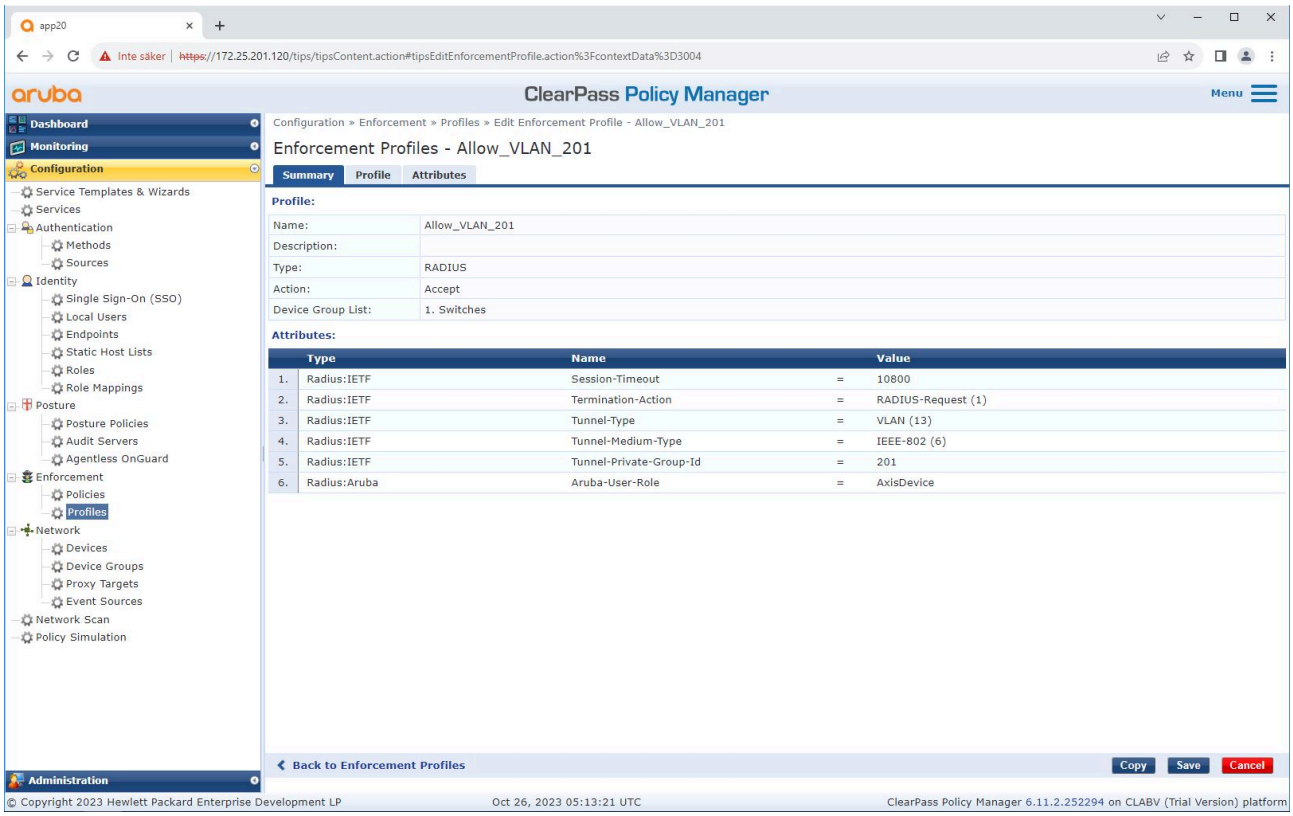


Dodawanie wcześniej utworzonej zasady mapowania ról Axis do usługi, która definiuje standard IEEE 802.1X jako metodę łączenia w przypadku wdrażania urządzeń Axis.



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 *Switch dostępowy HPE Aruba Networking, on page 15* zapoznaj się z poniższą przykładową konfiguracją portu dla switcha dostępowego HPE Aruba Networking, aby skonfigurować protokół 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
```

Zarządzanie certyfikatami – protokół Enrollment over Secure Transport (EST)

Certyfikaty cyfrowe mają kluczowe znaczenie dla zabezpieczania urządzeń i sieci, ale zarządzanie nimi może być skomplikowane i czasochłonne. Certyfikaty tracą ważność i muszą być regularnie odnawiane. Bez automatyzacji proces ten jest powtarzalny i wykonywany ręcznie, zwłaszcza w przypadku dużych wdrożeń lub środowisk z różnymi typami urządzeń.

System operacyjny AXIS OS 12.9 wprowadza obsługę protokołu Enrollment over Secure Transport (EST), który służy do bezpiecznego dostarczania certyfikatów do urządzeń. Zdefiniowany w RFC 7030 protokół EST jest opartym na standardach rozwiązaniem zaprojektowanym w celu uproszczenia i automatyzacji pełnego cyklu życia certyfikatu obejmującego:

- Rejestrację – bezpieczne wydawanie nowych certyfikatów dla urządzeń
- Odnowienie – automatyczną wymianę wygasających certyfikatów
- Ponowną rejestrację – aktualizację certyfikatów zgodnie z zasadami IT

EST obsługuje określone przez IT zasady dotyczące atrybutów certyfikatów, takich jak okres ważności, typ klucza (RSA/ECC) lub rozmiar klucza, i korzysta wyłącznie z protokołu HTTPS.

Główne zalety protokołu EST

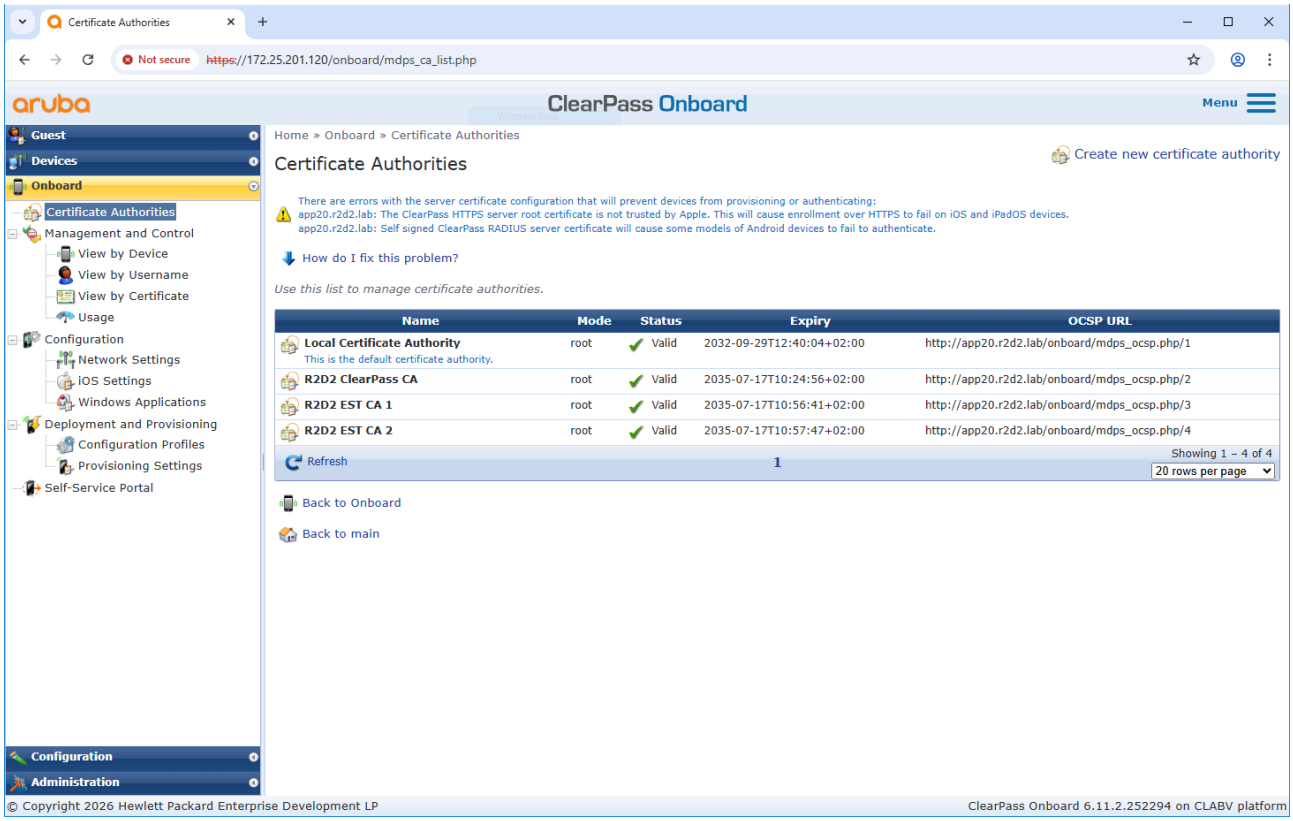
- Automatyczna rejestracja, odnawianie i ponowna rejestracja certyfikatów zarządzane według zasad określonych przez IT całkowicie eliminują konieczność manualnej, czasochłonnej konfiguracji.
- Najnowocześniejsza, bezpieczna komunikacja wyłącznie poprzez protokół HTTPS TLS 1.2/1.3.
- Scentralizowana widoczność/dozór dla zespołów IT.
  Oparty na standardach (RFC 7030) i zintegrowany z infrastrukturą IT.
- Skalowalne rozwiązanie dla Internetu rzeczy, sieci korporacyjnych i zarządzania urządzeniami.

Ogólną dokumentację protokołu EST można znaleźć w naszej *bazie wiedzy systemu operacyjnego AXIS OS*.

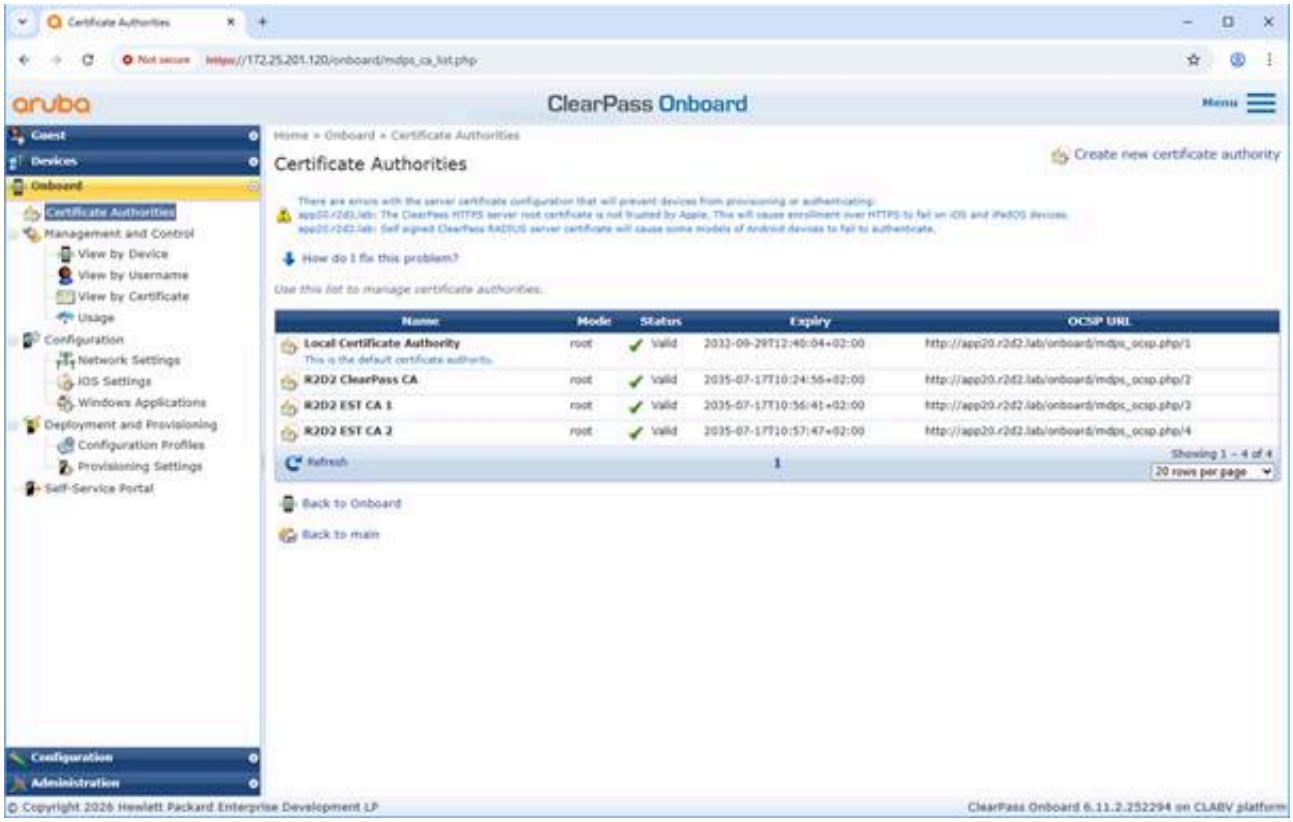
Konfiguracja HPE Aruba ClearPass Onboard

Aruba ClearPass Onboard integruje się z EST w celu bezpiecznej dystrybucji certyfikatów urządzeń i zarządzania nimi w zakresie dostępu do sieci. Korzystając z protokołu EST, punkty końcowe uwierzytelniają się w ClearPass i rejestrują się w celu uzyskania unikalnego certyfikatu za pośrednictwem bezpiecznego kanału TLS, który jest następnie wykorzystywany do uwierzytelniania opartego na certyfikacie 802.1X i innych usług. Zapewnia to opartą na standardach, zautomatyzowaną i niewymagającą hasła metodę wykonywania zasad bezpiecznego dostępu w oparciu o tożsamość urządzenia.

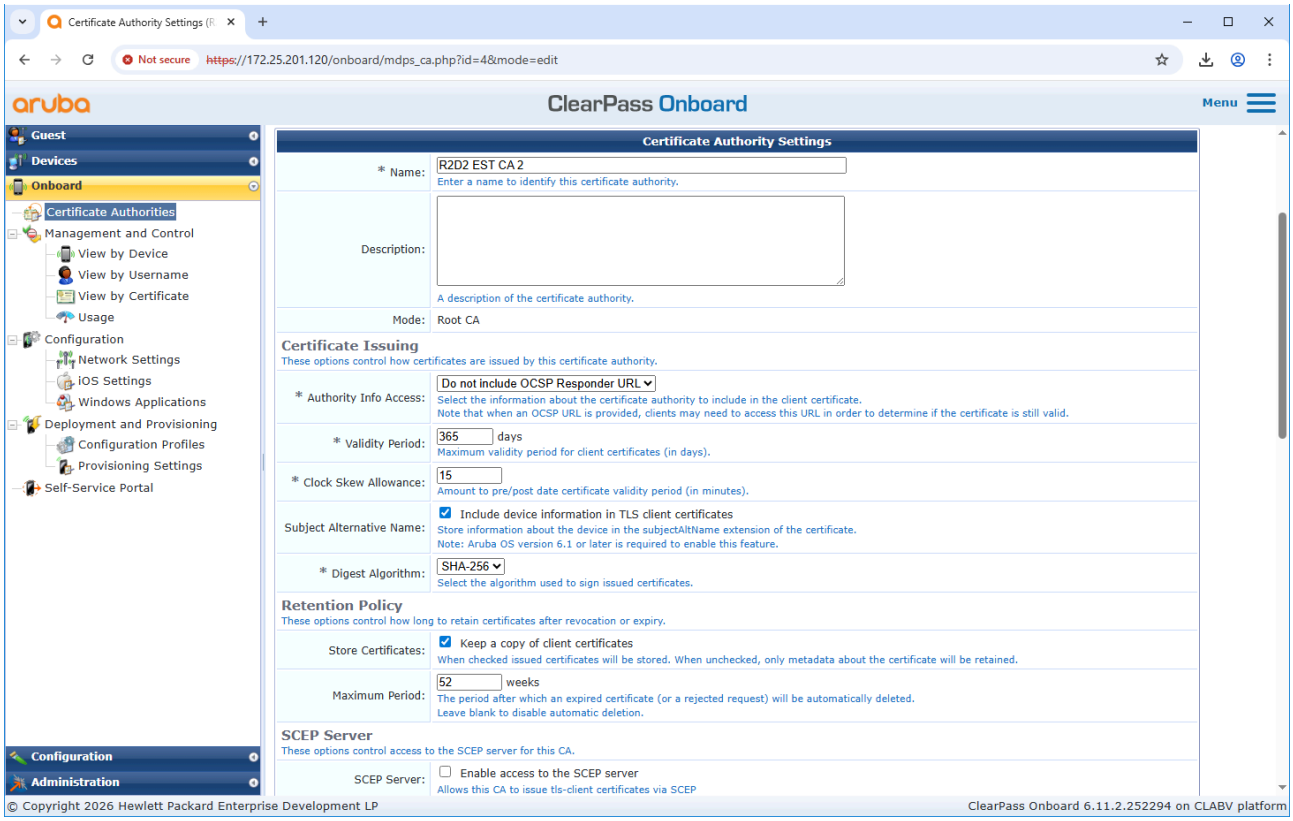
Konfiguracja organu wydającego certyfikat



Utwórz nowy organ wydający certyfikat w ClearPass Onboard.



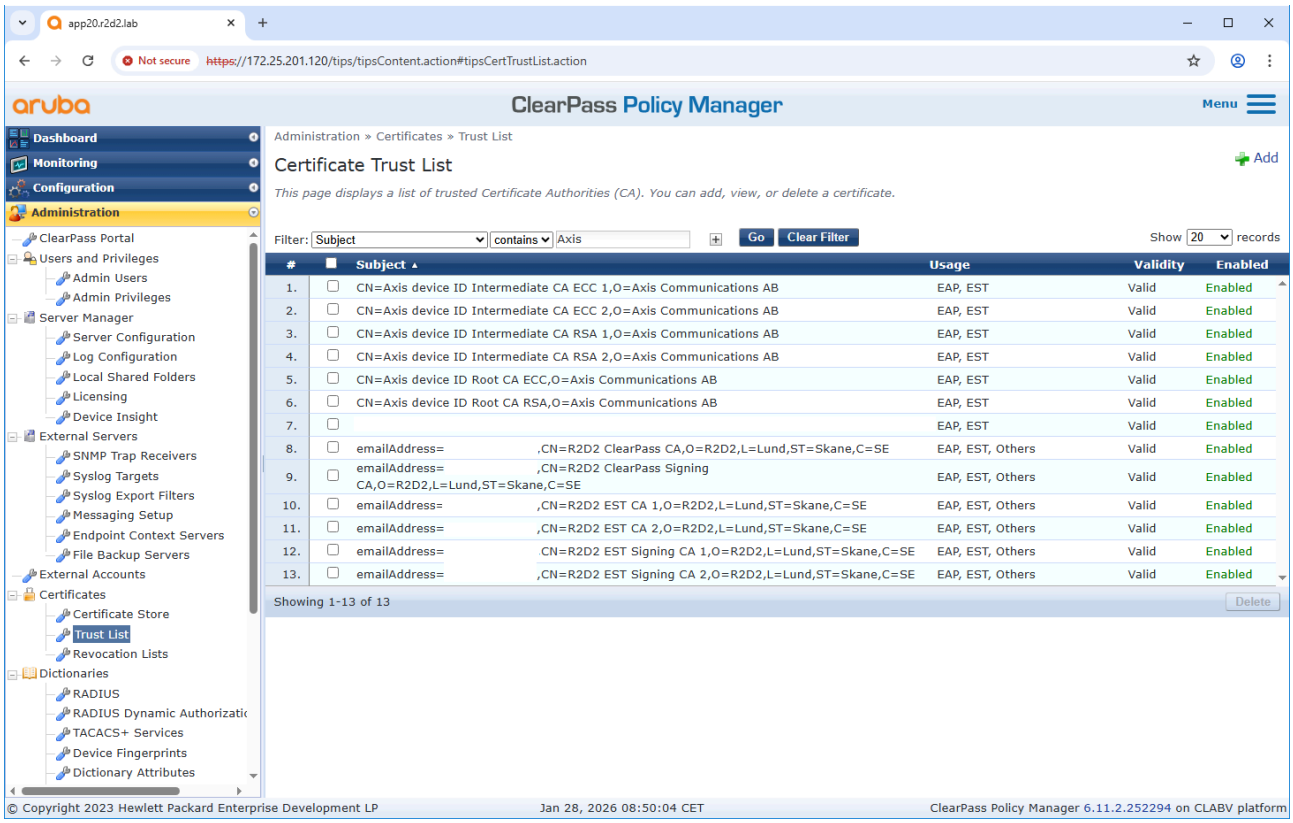
W ramach utworzonego organu wydającego certyfikat definiuje się typ klucza, rozmiar klucza, okres ważności i inne parametry.



Włącz funkcję serwera EST dla utworzonego organu wydającego certyfikat. Skonfiguruj metodę uwierzytelniania EST, aby używać certyfikatu klienta.

Konfiguracja HPE Aruba ClearPass Policy Manager

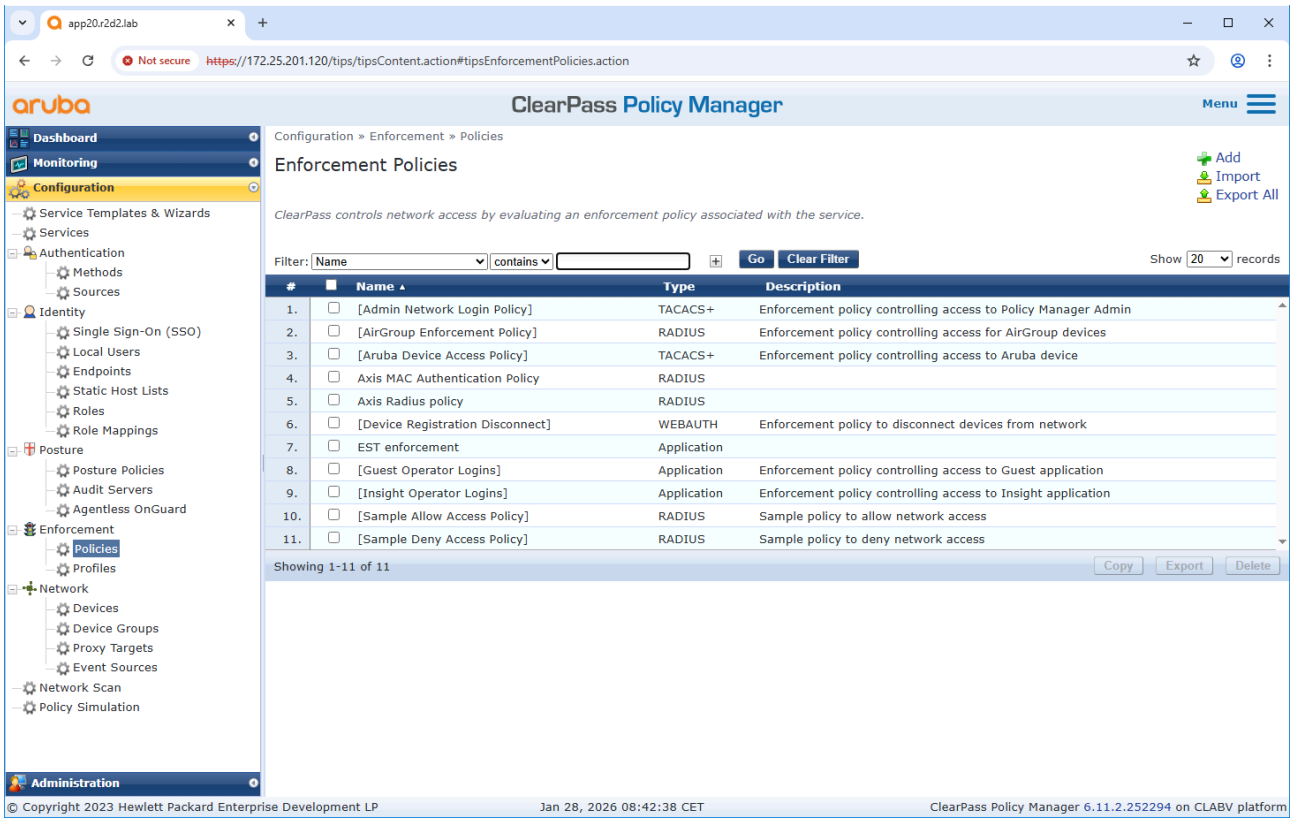
Konfiguracja zaufanej bazy certyfikatów



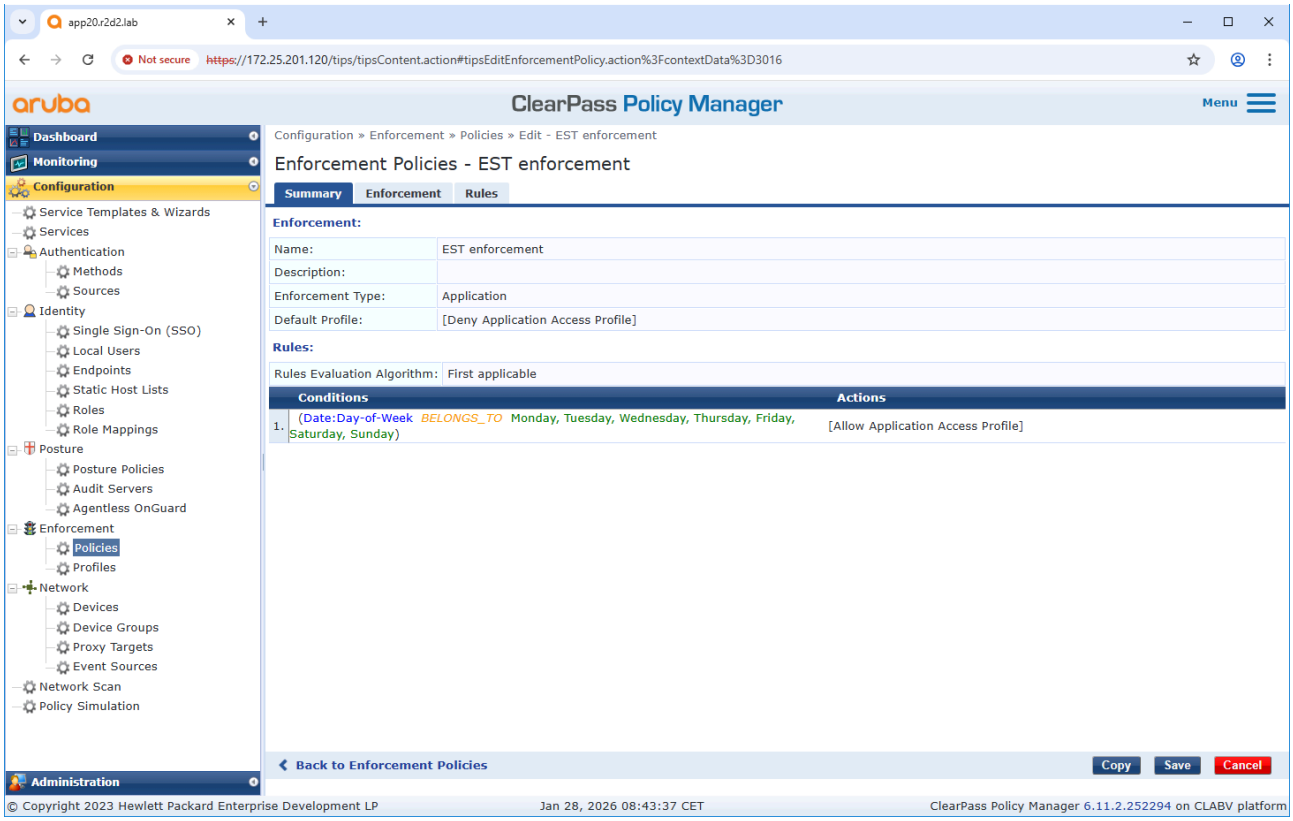
Jeśli nie zostało to jeszcze zrobione, prześlij *certyfikaty IEEE 802.1AR specyficzne dla firmy Axis* do zaufanego magazynu certyfikatów narzędzia ClearPass Policy Manager. Upewnij się, że dodano wykorzystanie EST. Sprawdź to również dla wcześniej utworzonego organu wydającego certyfikat z ClearPass Onboard.

Konfiguracja zasad wykonywania

Profil wykonywania umożliwia programowi ClearPass Policy Manager przydzielanie określonych wykonań do aplikacji EST. Na przykład nowe certyfikaty mogą być rejestrowane tylko z określonych punktów końcowych lub tylko w określone dni tygodnia.

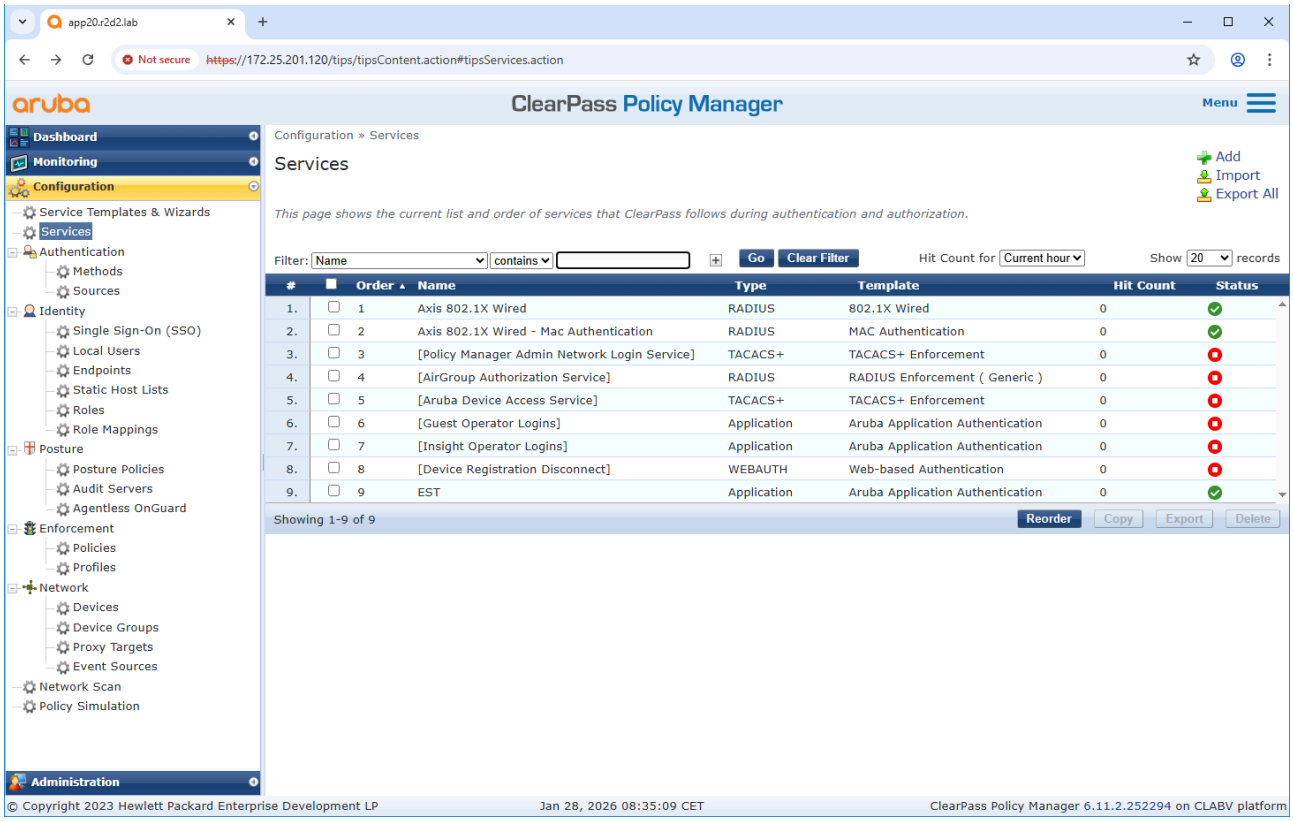


Przegląd zasad wykonywania w narzędziu ClearPass Policy Manager.

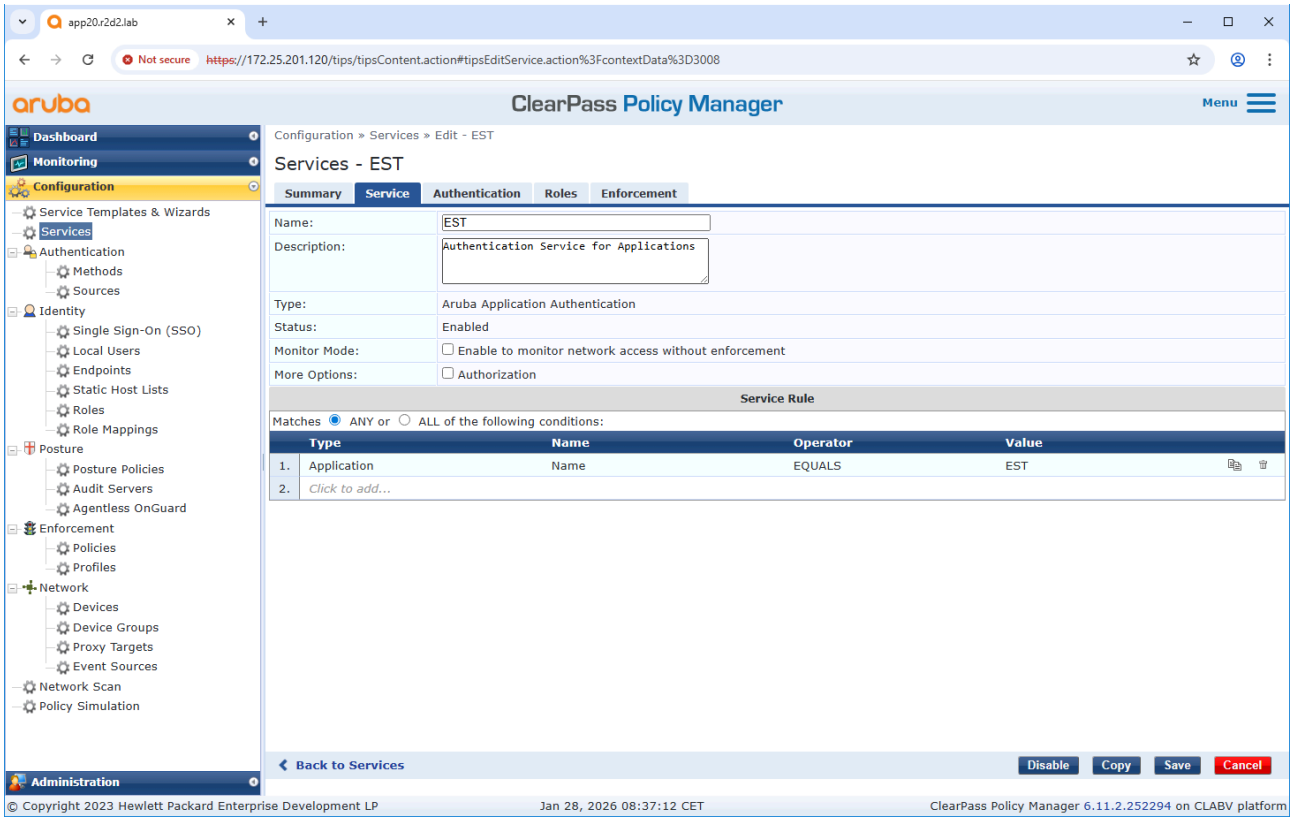


W tej przykładowej zasadzie aplikacja EST jest dozwolona we wszystkie dni tygodnia.

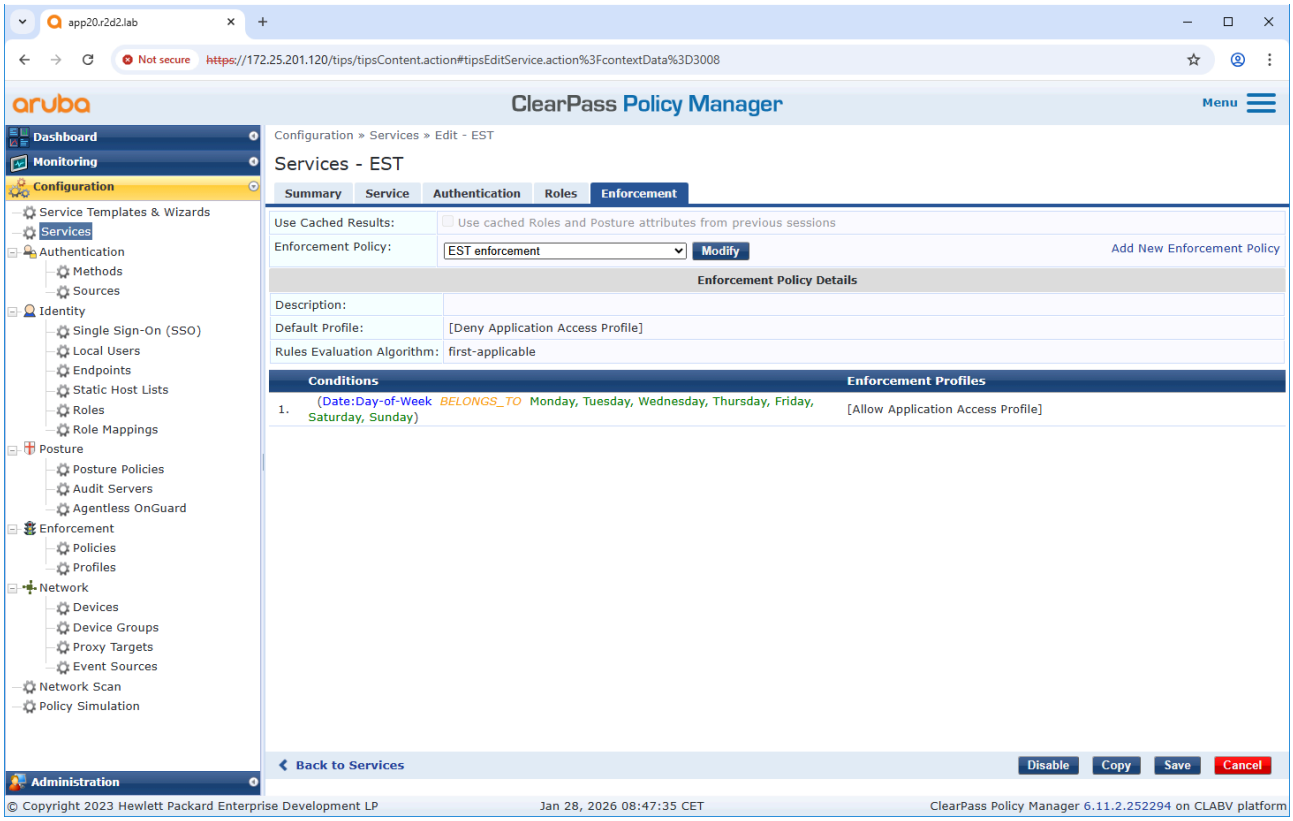
Konfiguracja usług



Należy stworzyć dedykowaną usługę EST.



Usługa powinna być skonfigurowana dla aplikacji EST.



Wybierz wcześniej utworzoną zasadę wykonywania EST.

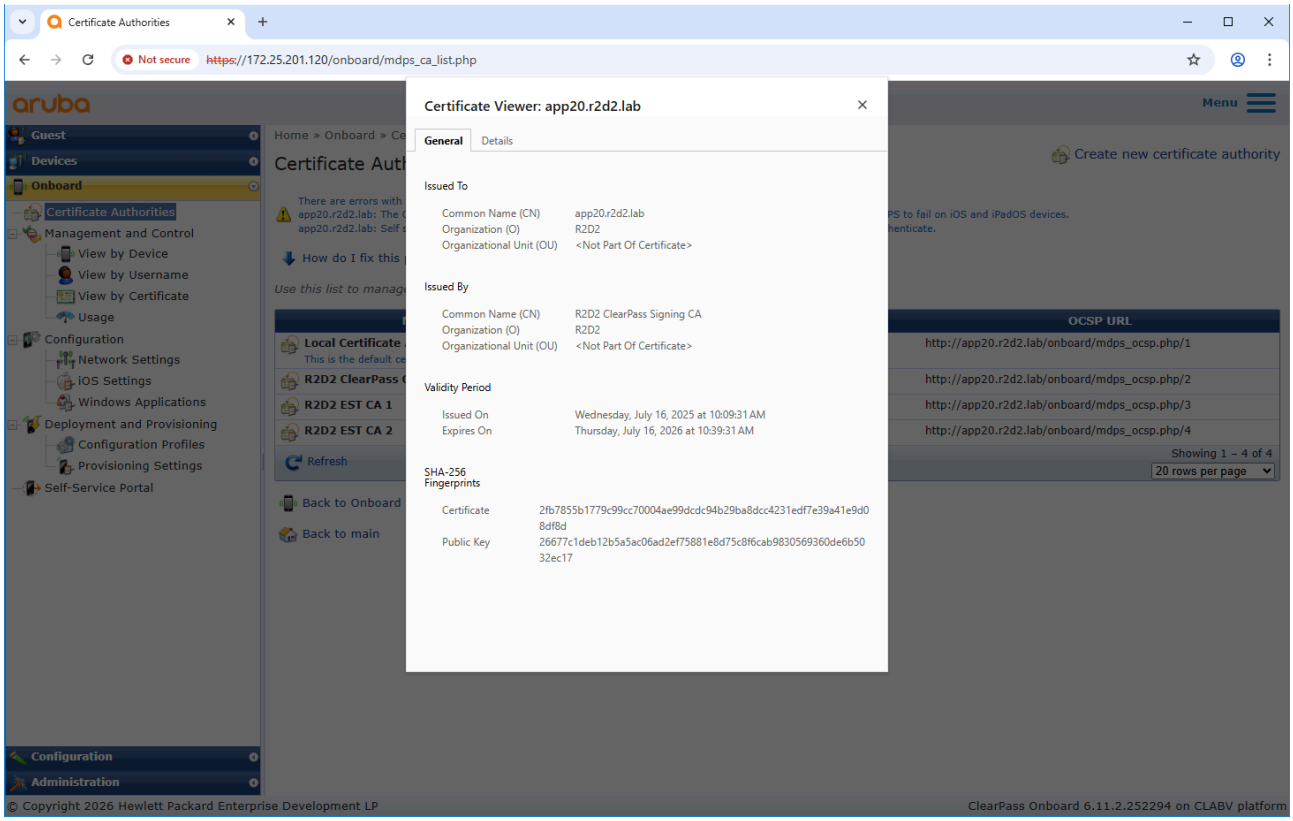
Konfiguracja Axis

Konfiguracja urządzenia Axis odbywa się w dwóch krokach.

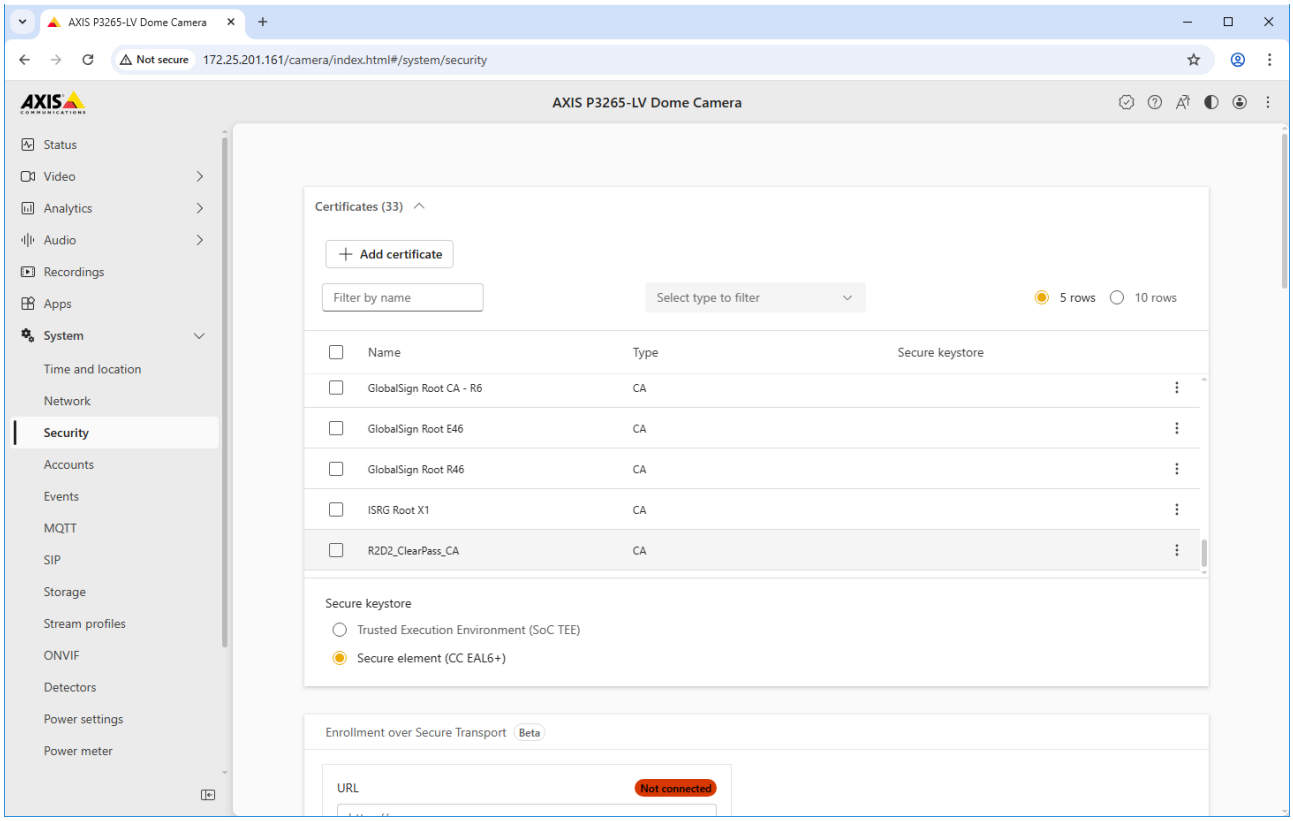
1. Ustanów zaufanie z punktem końcowym ClearPass Onboard HTTPS.

2. Skonfiguruj klienta EST na urządzeniu Axis.

Konfiguracja zaufanego certyfikatu

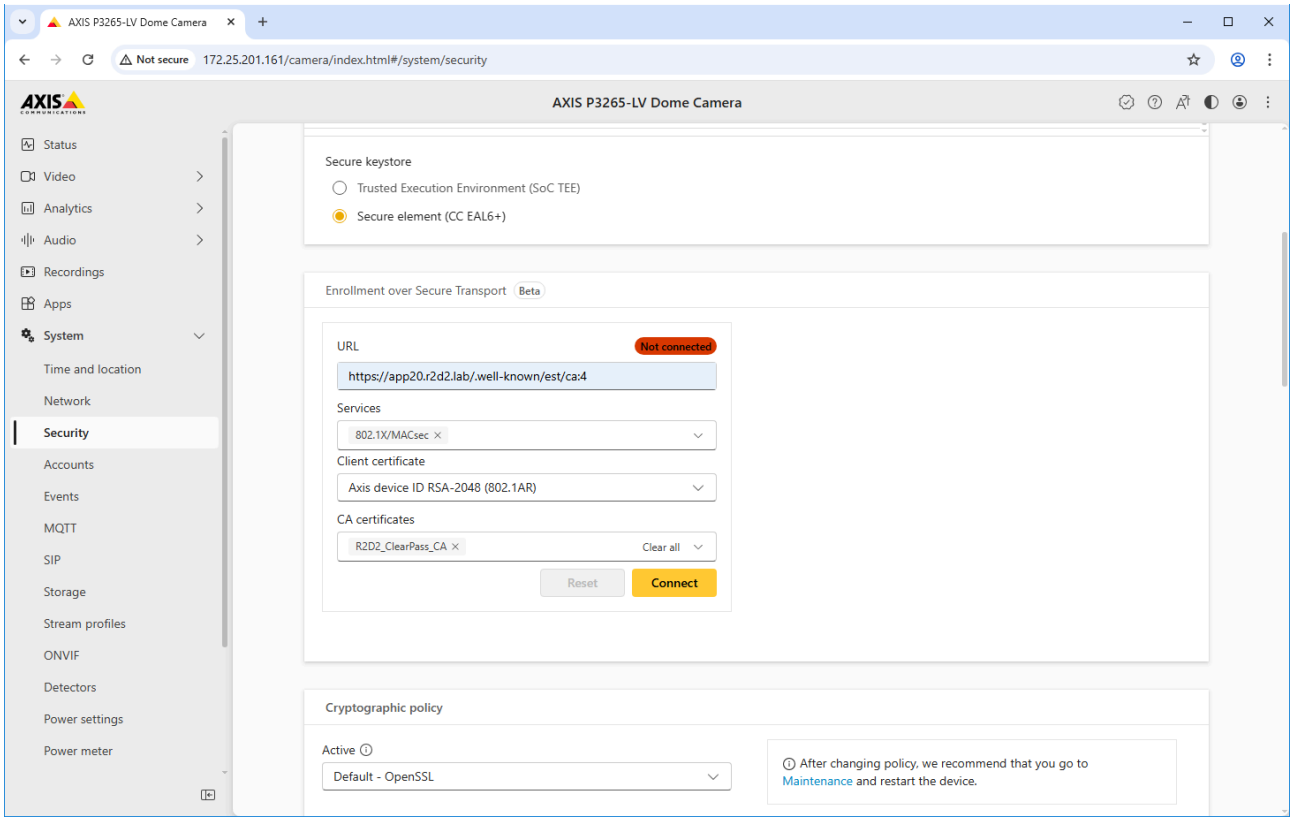


Zweryfikuj łańcuch certyfikatu z punktu końcowego ClearPass Onboard HTTPS.

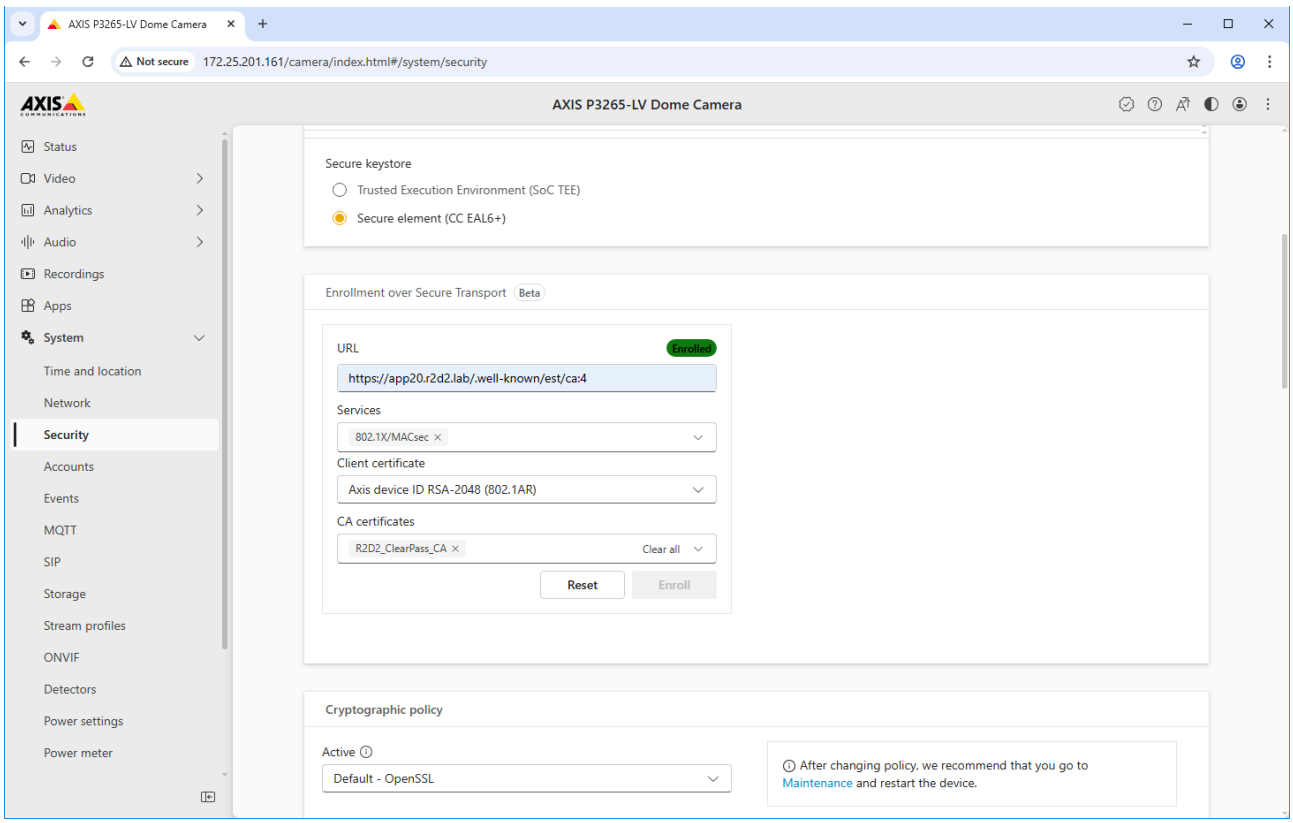


Prześlij certyfikat CA z punktu końcowego ClearPass Onboard HTTPS do urządzenia Axis.

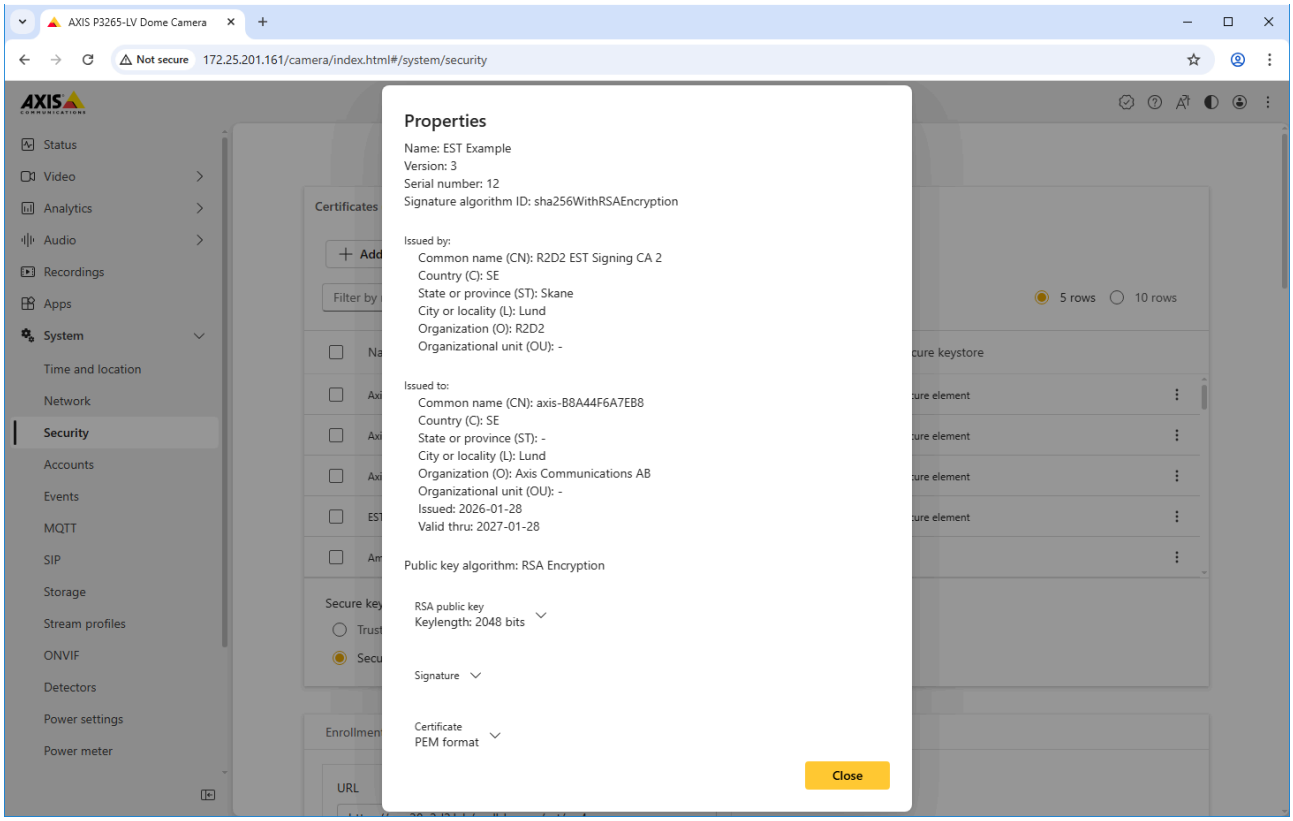
Konfiguracja klienta EST



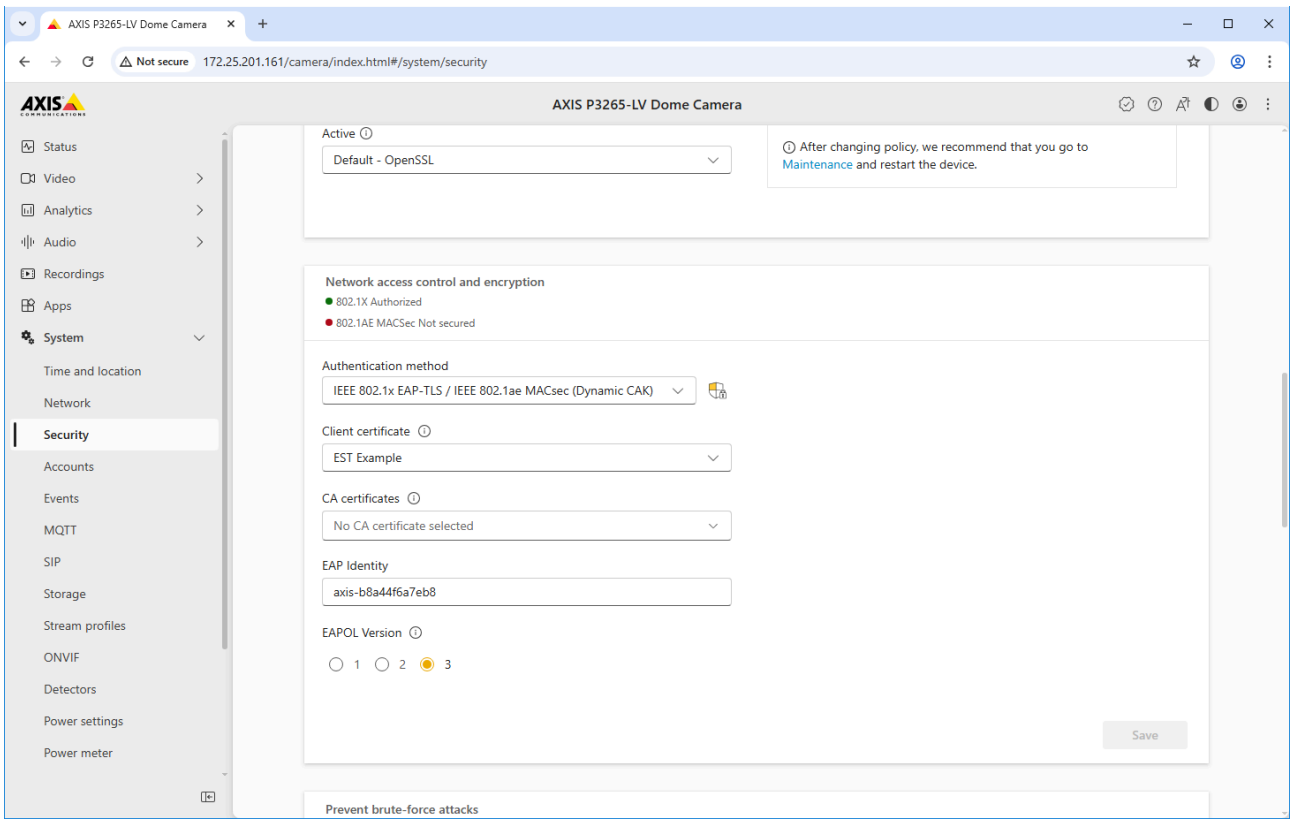
Parametr	Wartość
Adres URL	Adres URL EST można znaleźć w utworzonym organie wydającym certyfikat dla EST w ClearPass Onboard.
Usługi	Wybierz usługi, które powinny zostać automatycznie skonfigurowane za pomocą zarejestrowanego certyfikatu.
Certyfikat klienta	Wybierz certyfikat klienta do uwierzytelniania w serwerze ClearPass Onboard EST. Urządzenia z identyfikatorem urządzenia Axis są automatycznie uznawane za zaufane na potrzeby rejestracji, ponieważ łańcuch certyfikatów IEEE 802.1AR specyficzny dla Axis został dodany do magazynu zaufanych certyfikatów w ClearPass Policy Manager.
Certyfikaty CA	Wybierz certyfikat CA z punktu końcowego ClearPass Onboard HTTPS, aby urządzenie Axis ufało temu punktowi końcowemu.



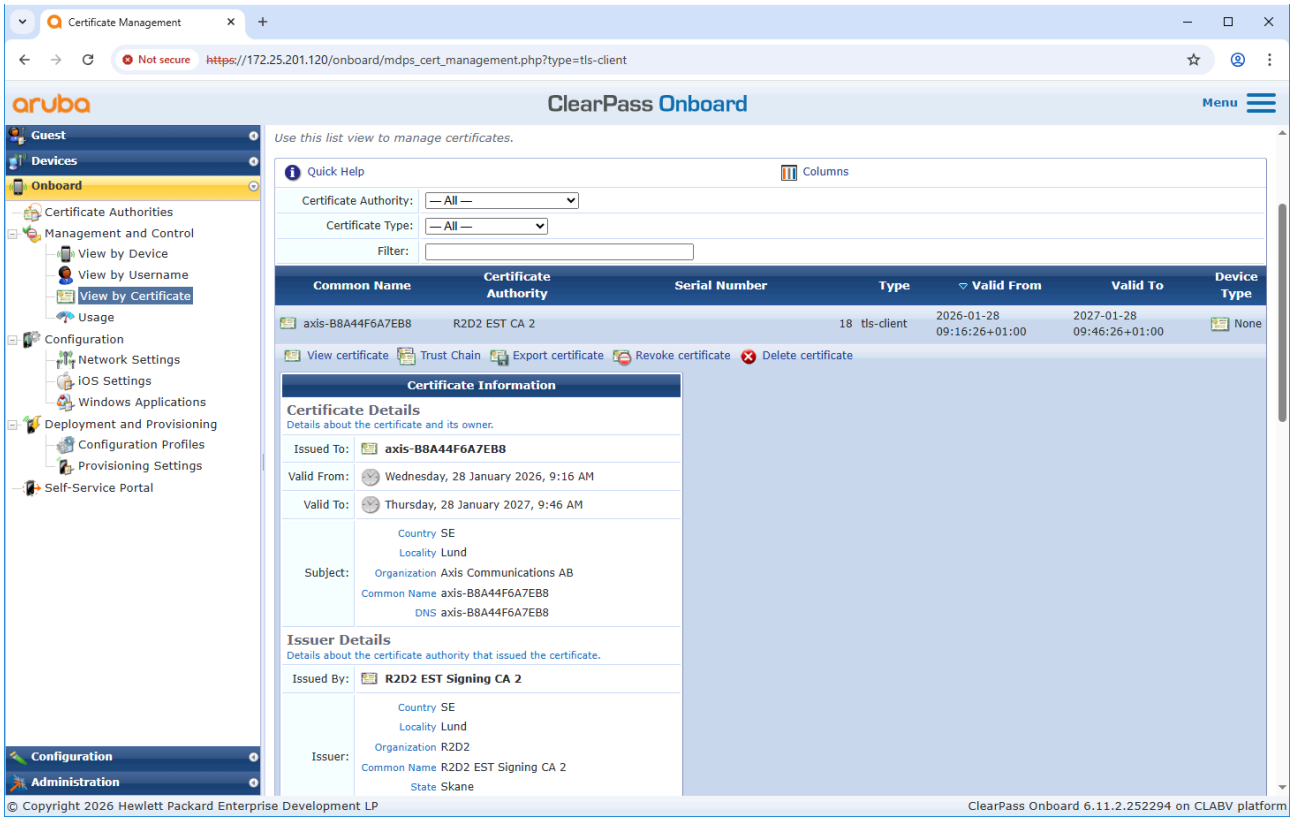
Rejestracja przebiegła pomyślnie.



Certyfikat EST zarejestrowany na urządzeniu Axis.



Zarejestrowany certyfikat jest automatycznie przydzielany do wcześniej wybranej usługi.



Zarejestrowany certyfikat można również przejrzeć w ClearPass Onboard.

Wdrażanie starszej wersji — uwierzytelnianie MAC

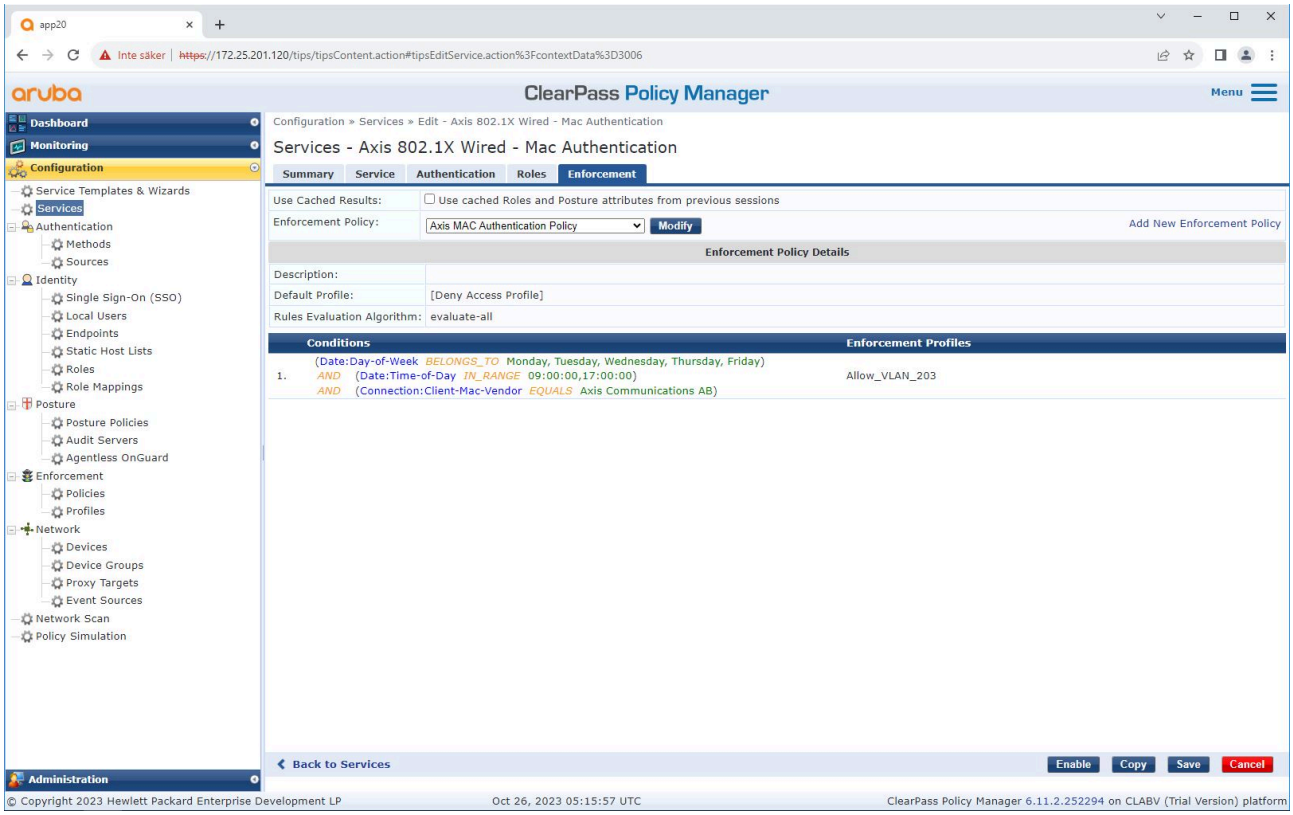
Za pomocą MAC Authentication Bypass (MAB) możesz wdrażać urządzenia Axis, które nie obsługują wdrażania IEEE 802.1AR z certyfikatem identyfikatora urządzenia Axis i włączonym IEEE 802.1X z ustawieniami fabrycznymi. Jeśli wdrożenie standardu 802.1X nie powiedzie się, ClearPass Policy Manager zweryfikuje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

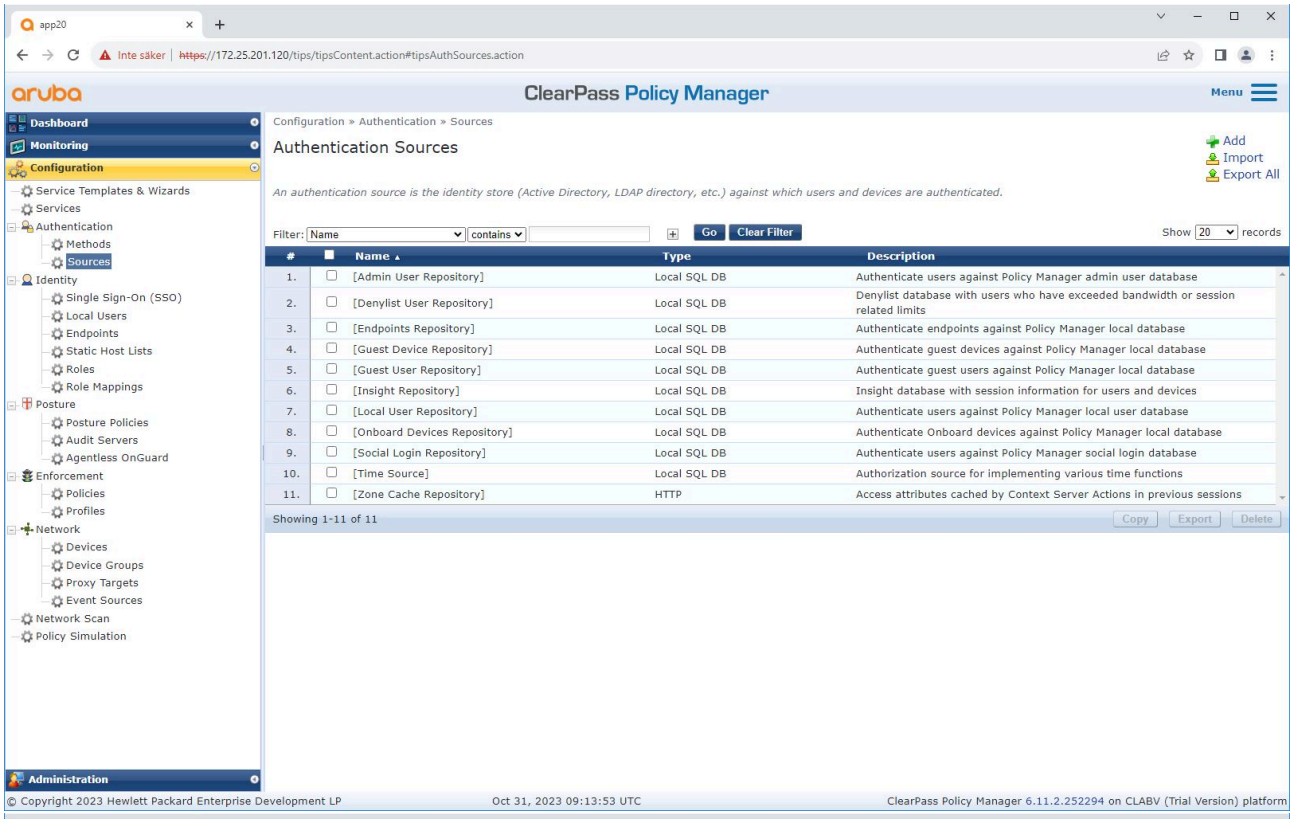
Urządzenie Axis uzyska dostęp do ograniczonej, odizolowanej sieci, jeśli spełnione są następujące warunki:

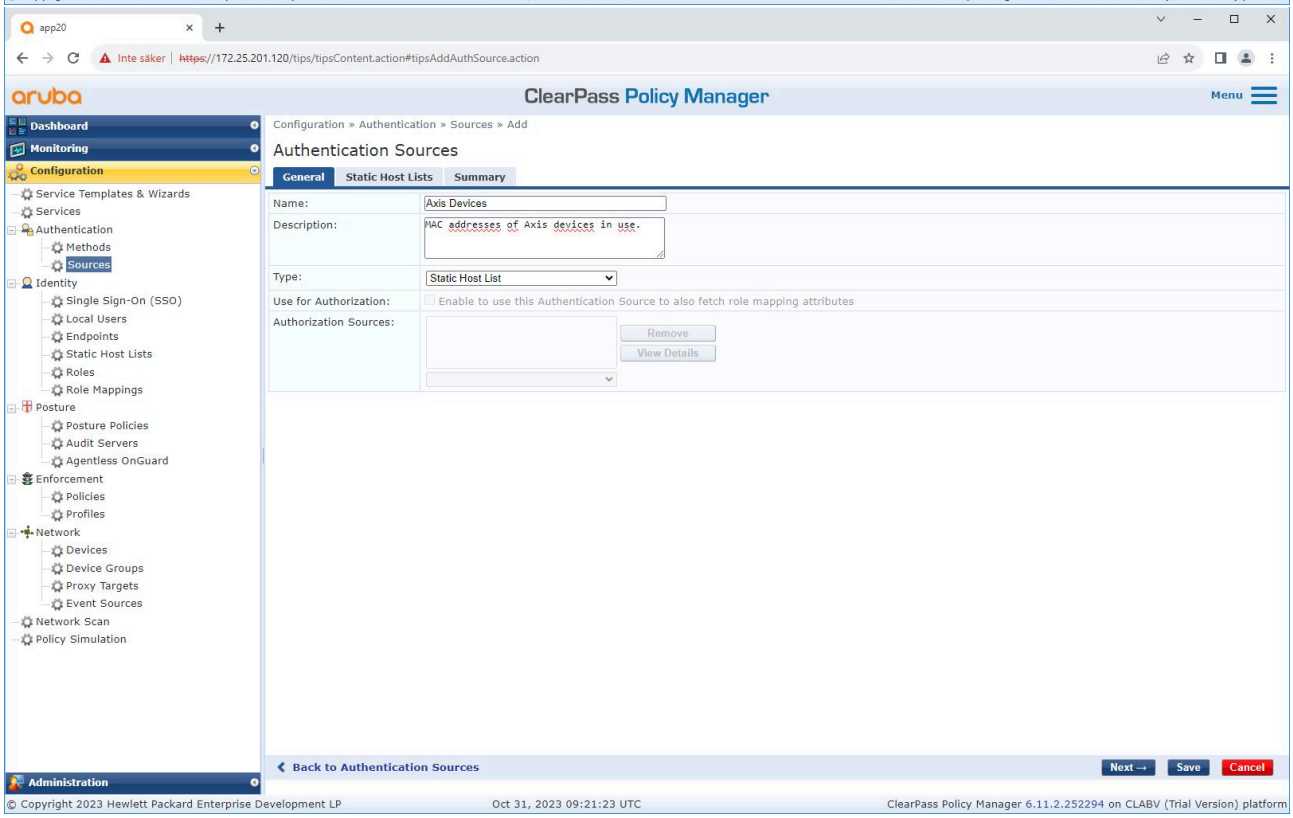
- Dzień jest dniem powszednim, od poniedziałku do piątku.
- Godzina mieści się w zakresie od 9:00 do 17:00.
- Dostawca adresu MAC jest zgodny z Axis Communications.

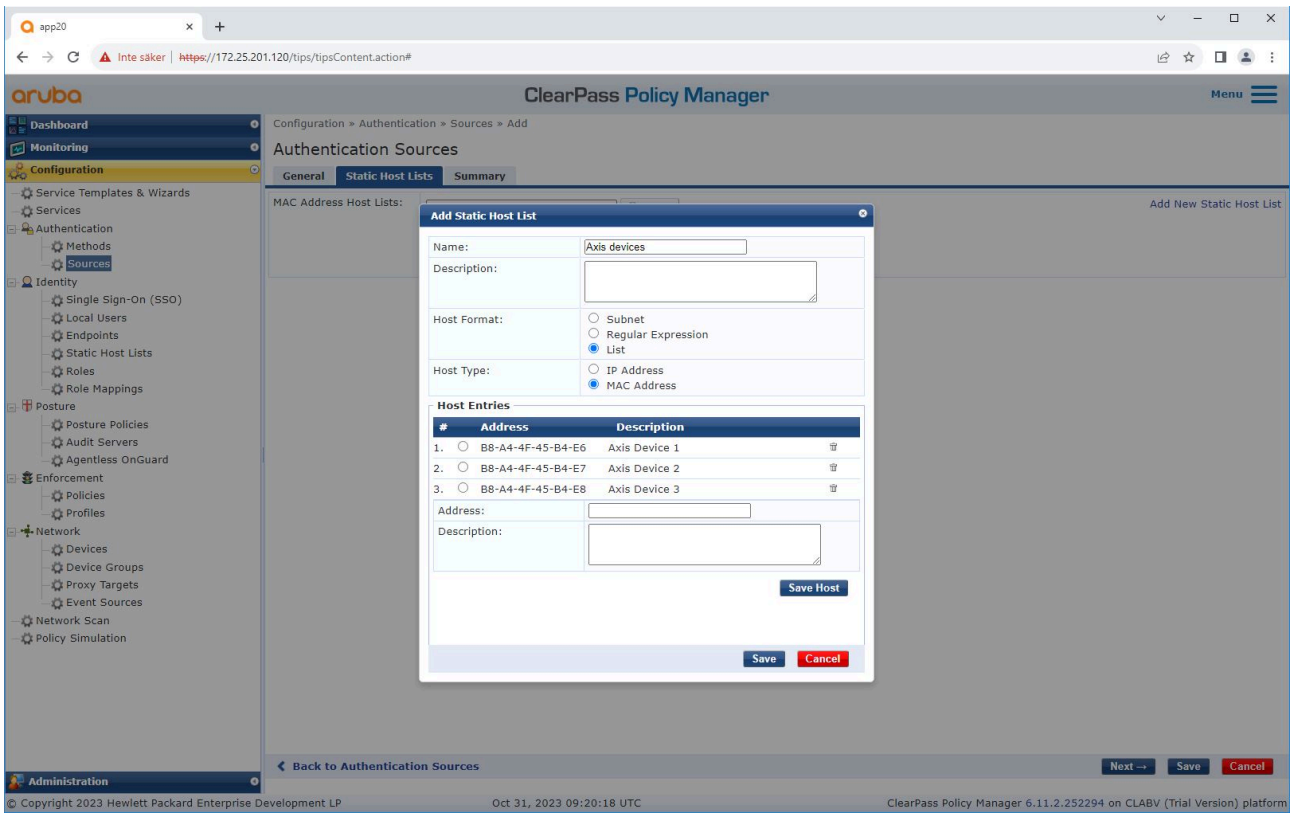
Ponieważ możliwe jest sfałszowanie adresów MAC, dostęp do zwykłej sieci administracyjnej nie jest przyznawany. Zalecamy korzystanie z MAB tylko do wstępnego wdrożenia i ręczne sprawdzanie urządzenia w przyszłości.

Konfiguracja źródła

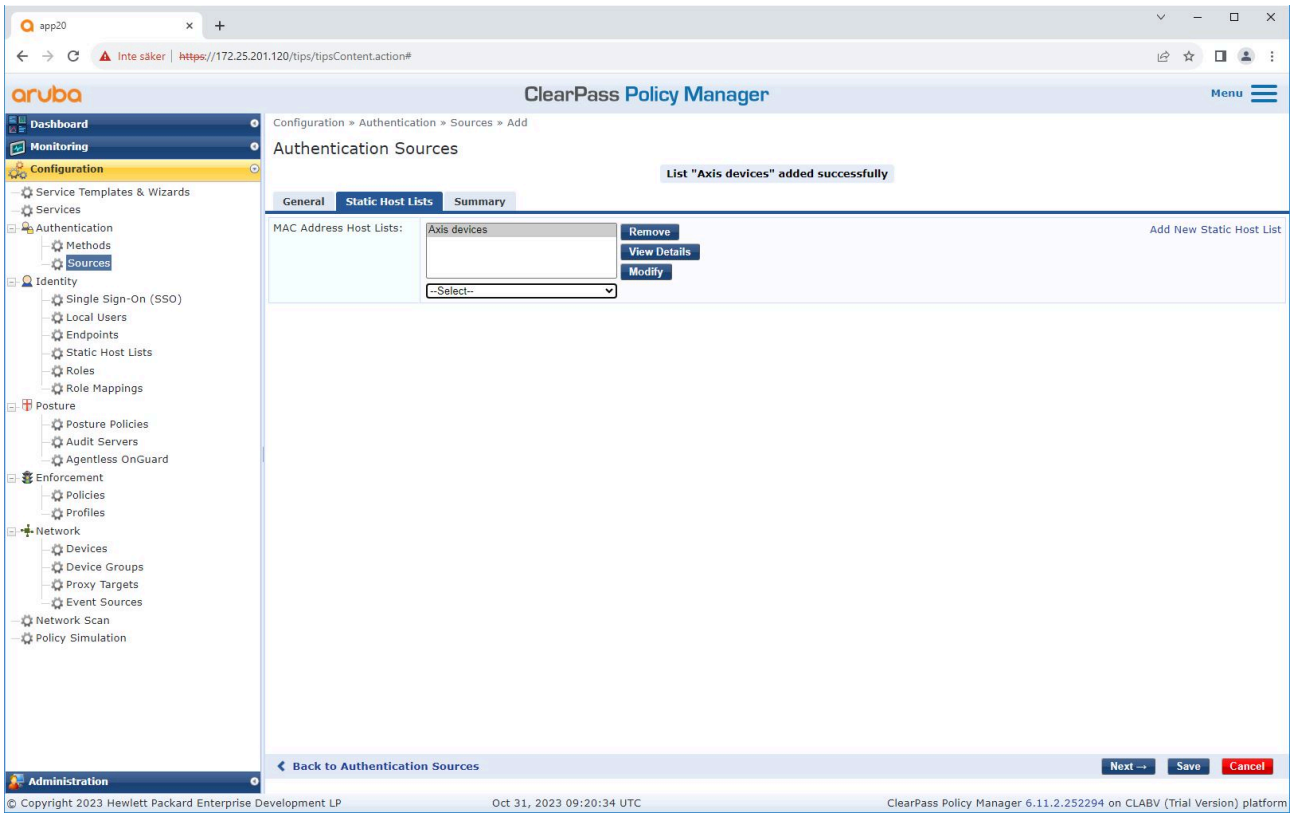
Na stronie **Sources (Źródła)** tworzone jest nowe źródło uwierzytelniania, które akceptuje tylko ręcznie importowane adresy MAC.





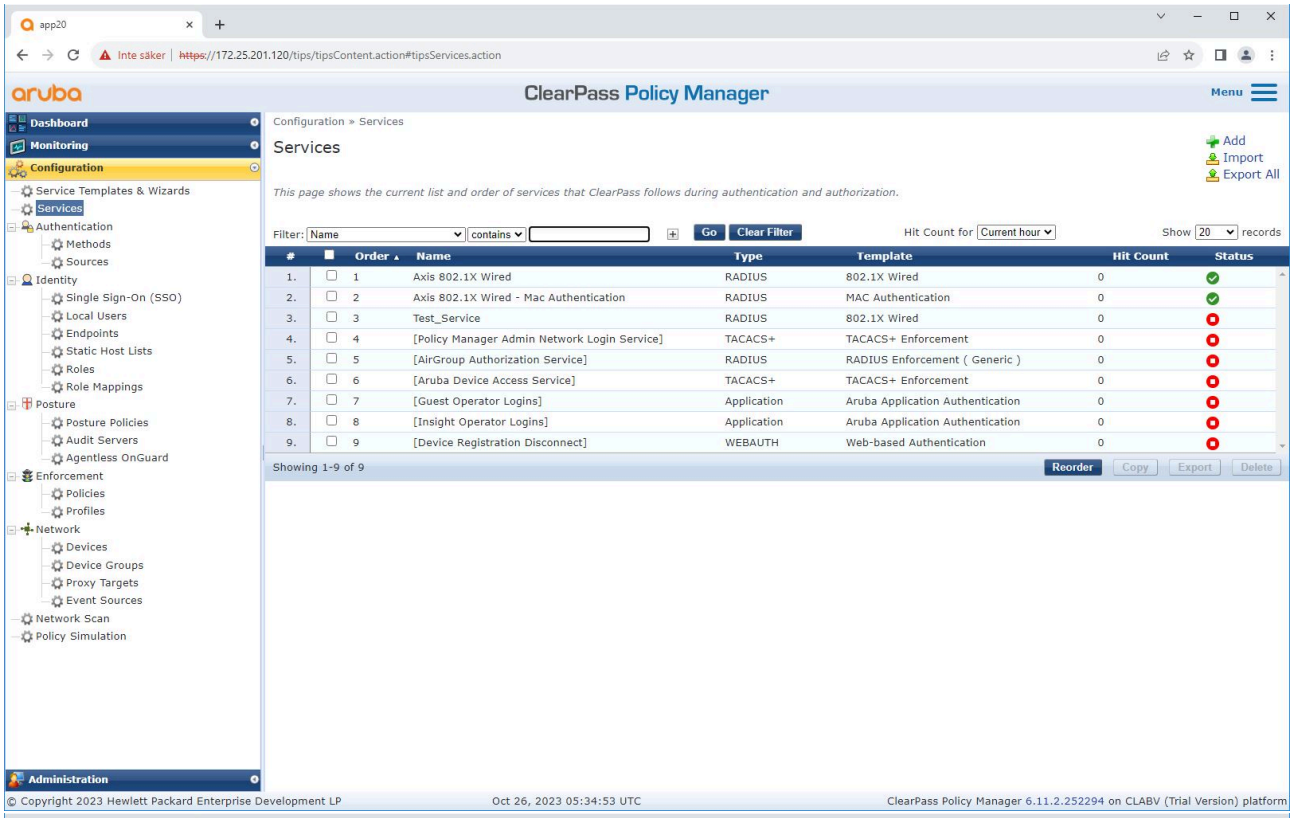


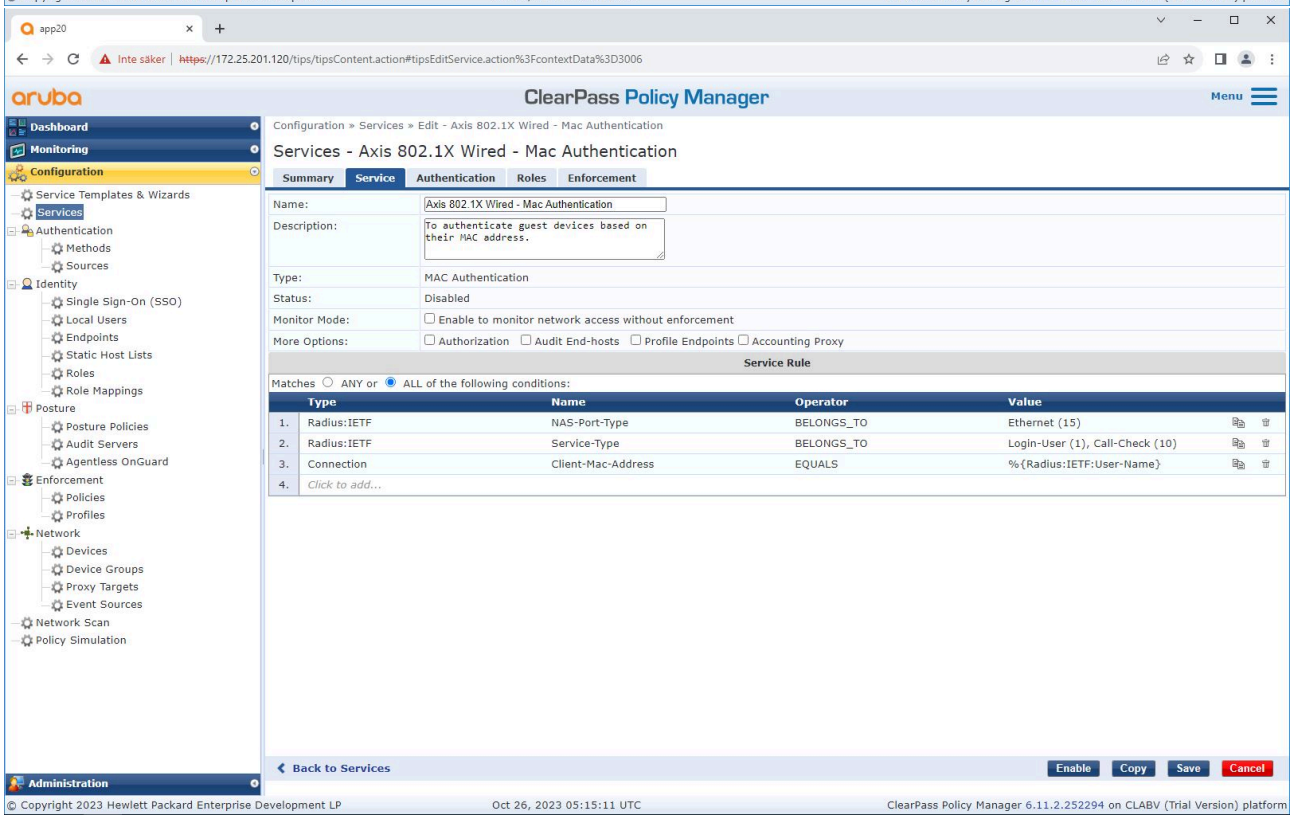
Tworzona jest statyczna lista hostów zawierająca adresy MAC Axis.



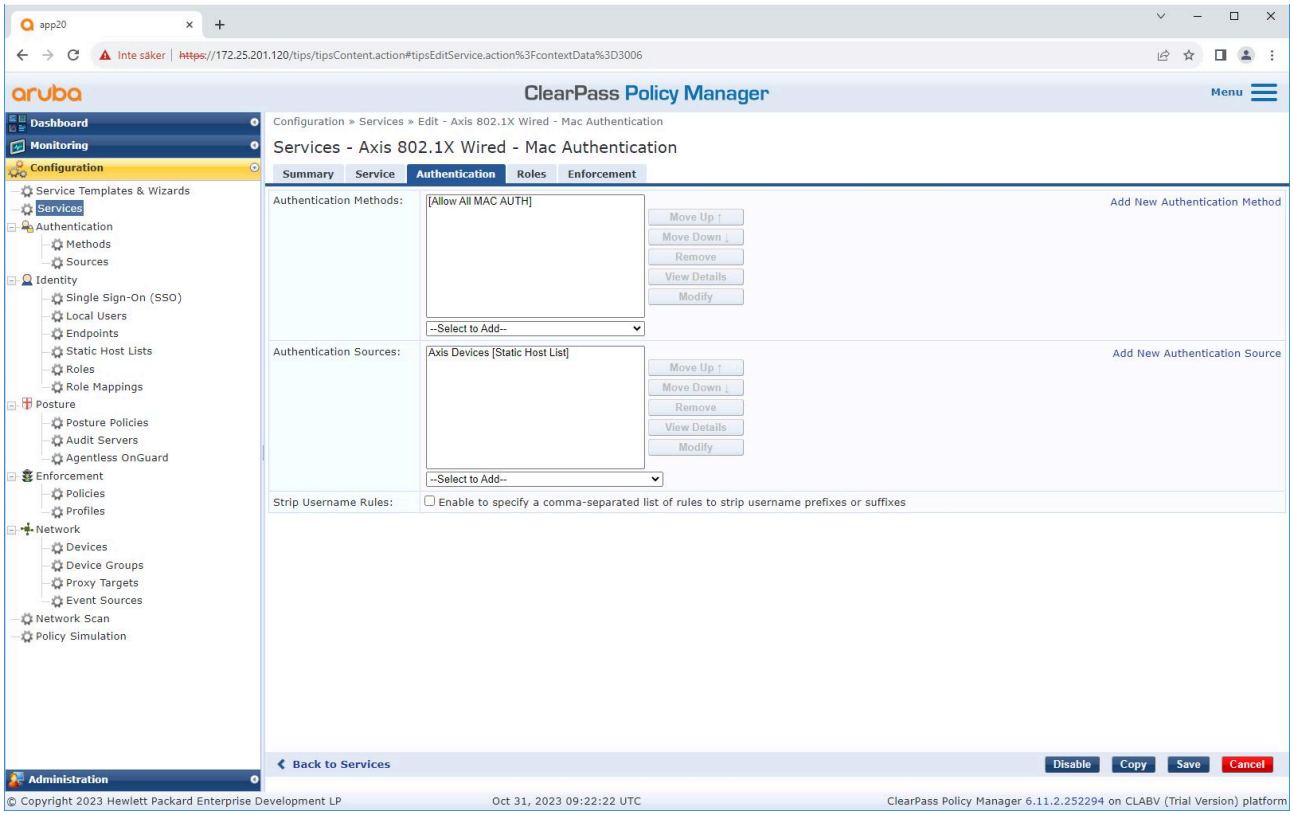
Konfiguracja usług

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





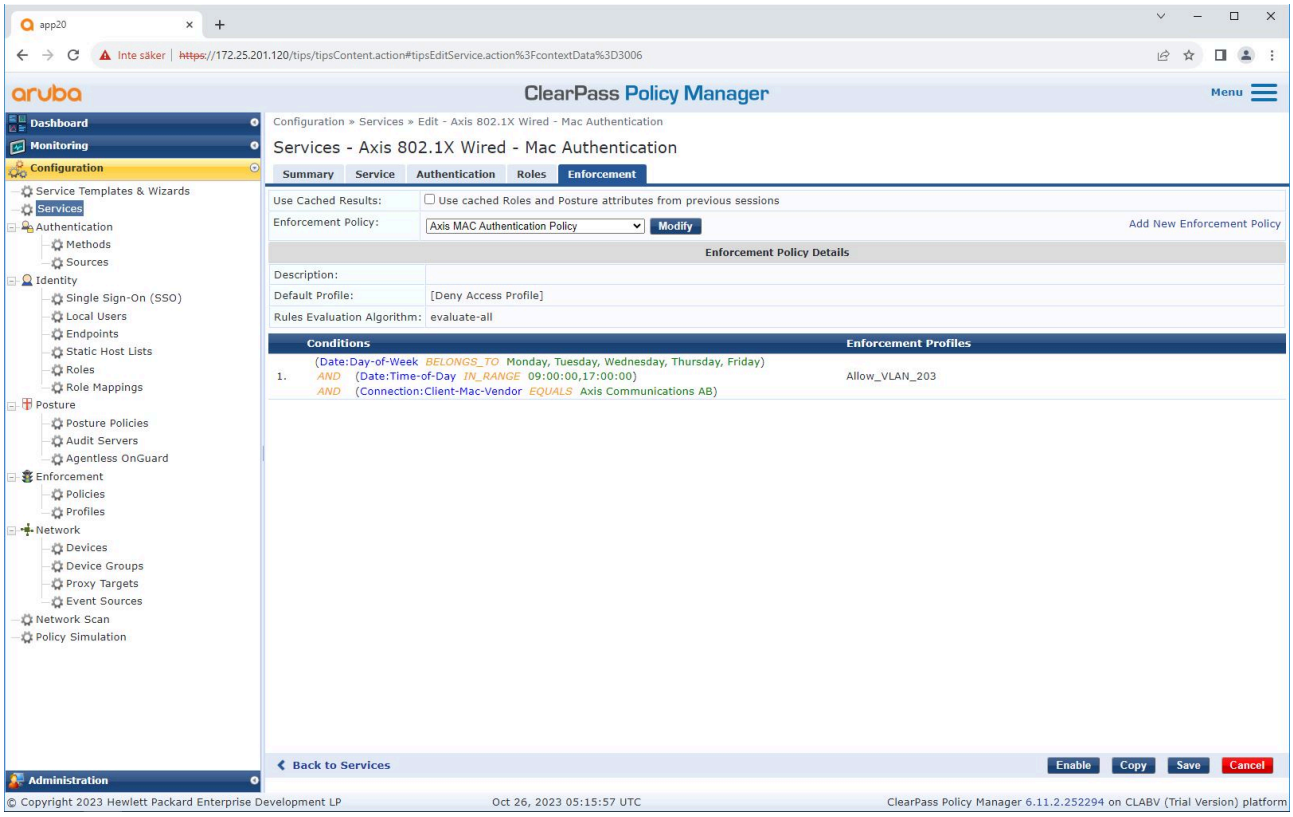
Tworzona jest dedykowana usługa Axis definiująca standard MAB jako metodę łączności.



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



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

Switch dostępowy HPE Aruba Networking

Oprócz konfiguracji bezpiecznego wdrażania opisanej w sekcji *Switch dostępowy HPE Aruba Networking, on page 15* 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

2026-02 (M8.3)

© 2023 – 2026 Axis Communications AB