HPE Aruba Networking

사용자 설명서

목차

서론

이 통합 가이드는 HPE Aruba Networking 네트워크에서 Axis 장치를 온보딩하고 운영할 때의 모범 사례 구성을 간략히 설명합니다. 모범 사례 구성은 IEEE 802.1X, IEEE 802.1AR, IEEE 802.1AE 및 HTTPS와 같은 최신 보안 표준 및 프로토콜을 사용합니다.

네트워크 통합을 위한 적절한 자동화를 구축하면 시간과 비용을 절약할 수 있습니다. HPE Aruba Networking 인프라 및 애플리케이션과 함께 Axis 장치 관리 애플리케이션을 사용하면 불필요한 시스템 복잡성이 제거됩니다. Axis 장치 및 소프트웨어를 HPE Aruba Networking 인프라와 결합하면 다음과 같은 이점을 얻을 수 있습니다.

- 장치 스테이징 네트워크를 제거하여 시스템 복잡성을 최소화합니다.
- 온보딩 프로세스 및 장치 관리를 자동화하여 비용을 절감합니다.
- Axis 장치는 제로 터치 네트워크 보안 제어를 제공합니다.
- HPE와 Axis의 전문 지식을 통해 전반적인 네트워크 보안이 향상됩니다.

온보딩 프로세스 전반에 걸쳐 논리적 네트워크 간의 원활한 소프트웨어 정의 전환을 위해, 구성을 시작하기 전에 네트워크 인프라가 Axis 장치의 무결성을 안전하게 검증할 준비가 되어 있어야 합니다. 구성을 수행하기 전에 다음 사항이 필요합니다.

- HPE Aruba Networking 액세스 스위치 및 HPE Aruba Networking ClearPass Policy Manager를 포함한 HPE Aruba Networking의 엔터프라이즈 네트워크 IT 인프라 관리 경험.
- 최신 네트워크 접근 제어 기술 및 네트워크 보안 정책에 대한 전문 지식.
- Axis 제품에 대한 사전 기본 지식이 권장되지만, 본 가이드 전반에 걸쳐 관련 정보가 제공됩니다.

보안 온보딩 - IEEE 802.1AR/802.1X

이 비디오를 시청하려면 이 문서의 웹 버전으로 이동하십시오.

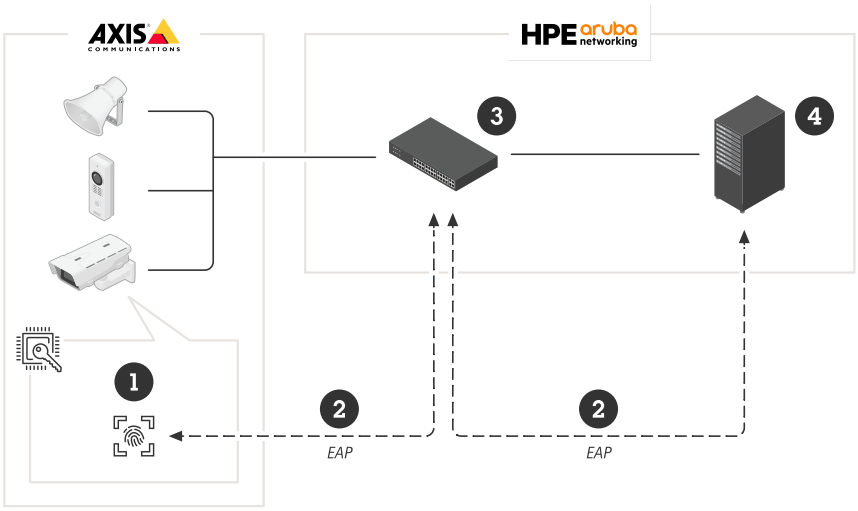
IEEE 802.1X/802.1AR을 사용하여 제로 트러스트 네트워크에 장치를 안전하게 온보딩

초기 인증

Axis Edge Vault를 지원하는 Axis 장치가 네트워크에 연결되면, IEEE 802.1X 네트워크 접근 제어를 통해 IEEE 802.1AR Axis 장치 ID 인증서를 사용하여 자체 인증합니다.

네트워크 액세스 권한을 부여하기 위해 ClearPass Policy Manager는 Axis 장치 ID를 다른 장치별 지문과 함께 확인합니다. MAC 주소 및 장치의 AXIS OS 버전과 같은 이 정보는 정책 기반 결정을 내리는 데 사용됩니다.

Axis 장치는 IEEE 802.1AR 호환 Axis 장치 ID 인증서를 사용하여 네트워크에서 자체 인증합니다.

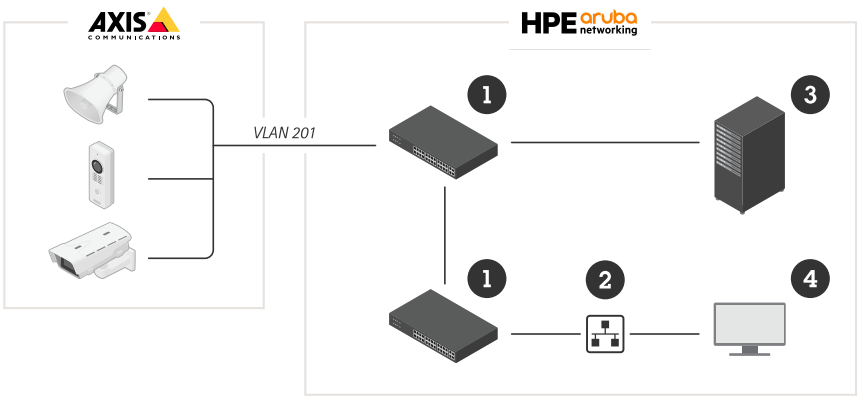


Axis 장치는 IEEE 802.1AR 호환 Axis 장치 ID 인증서를 사용하여 HPE Aruba Networking 네트워크에 대해 인증합니다.

1. *Axis device ID*
2. *IEEE 802.1x EAP-TLS 네트워크 인증*
3. *액세스 스위치(인증자)*
4. *ClearPass Policy Manager*

프로비저닝

인증 후 Axis 장치는 프로비저닝 네트워크(VLAN201)로 이동합니다. 이 네트워크에는 장치 구성, 보안 강화 및 AXIS OS 업데이트를 수행하는 AXIS Device Manager가 포함됩니다. 장치 프로비저닝을 완료하기 위해 새로운 고객별 운영 환경용 인증서가 IEEE 802.1X 및 HTTPS용 장치에 업로드됩니다.

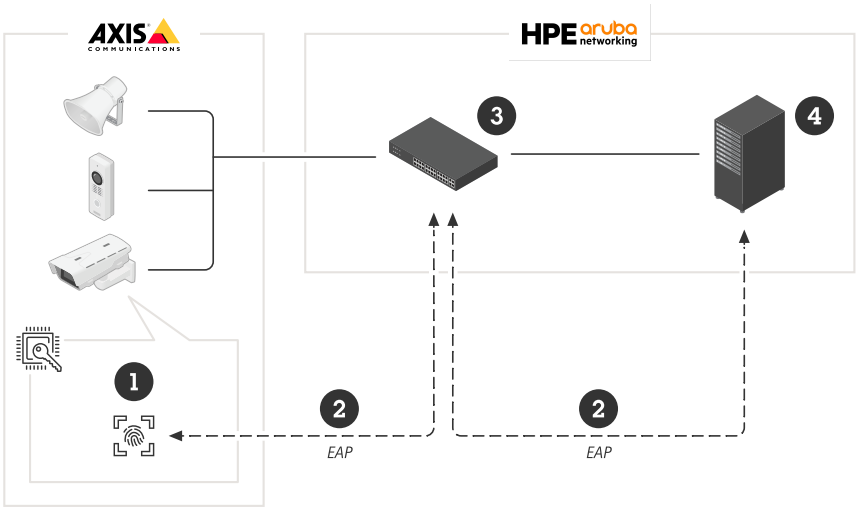


인증에 성공하면 Axis 장치는 구성을 위해 프로비저닝 네트워크로 이동합니다.

1 *액세스 스위치*
2 *네트워크 프로비저닝*
3 *ClearPass Policy Manager*
4 *장치 관리 애플리케이션*

운영 네트워크

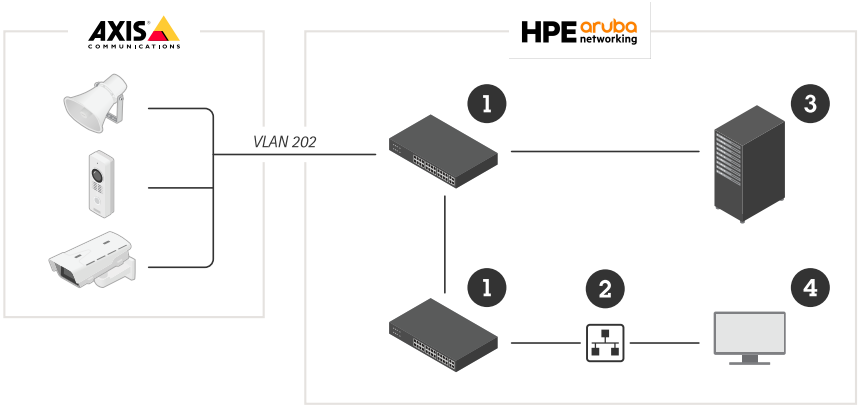
새로운 IEEE 802.1X 인증서로 Axis 장치를 프로비저닝하면 새로운 인증 시도가 트리거됩니다. ClearPass Policy Manager는 새 인증서를 확인하고 Axis 장치를 운영 네트워크로 이동할지 여부를 결정합니다.



구성이 완료되면 Axis 장치는 프로비저닝 네트워크를 벗어나 네트워크에서 재인증을 시도합니다.

1 *Axis device ID*
2 *IEEE 802.1x EAP-TLS 네트워크 인증*
3 *액세스 스위치(인증자)*
4 *ClearPass Policy Manager*

재인증 후 Axis 장치는 운영 네트워크(VLAN 202)로 이동하며, 영상 관리 시스템(VMS)이 장치에 연결되어 작동을 시작합니다.



Axis 장치에는 운영 네트워크에 대한 액세스 권한이 부여됩니다.

1 *액세스 스위치*
2 *운영 네트워크*
3 *ClearPass Policy Manager*
4 *영상 관리 시스템*

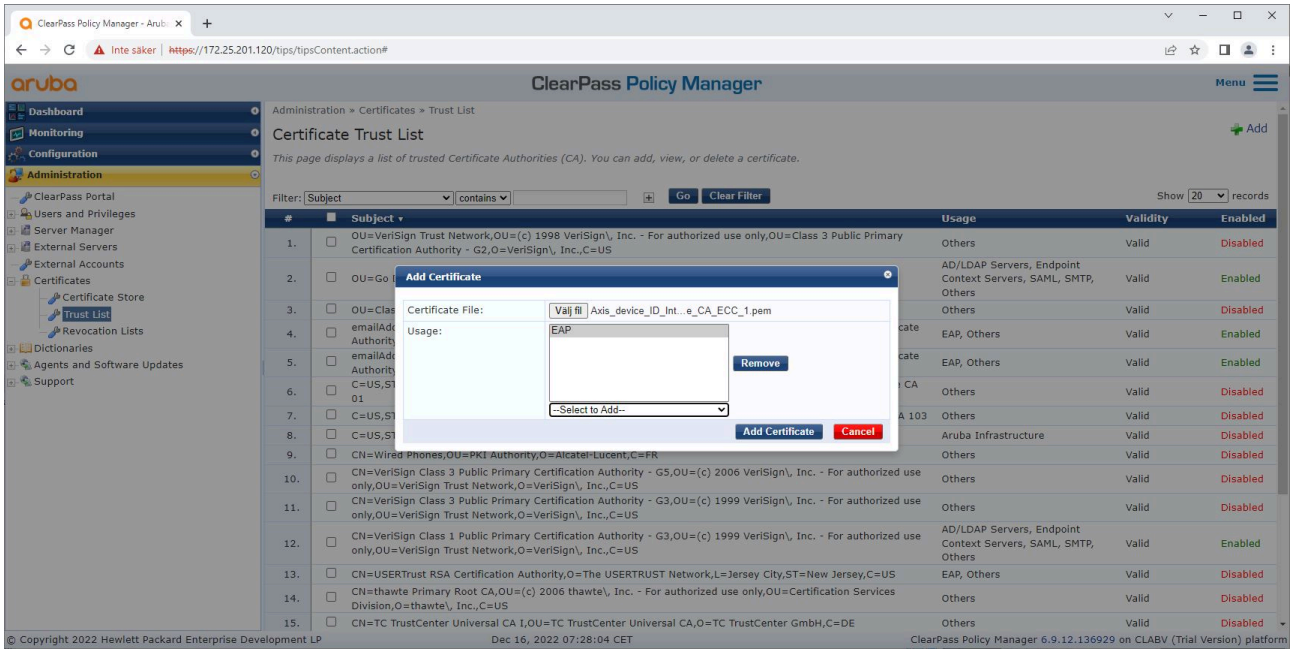
HPE Aruba Networking 구성

HPE Aruba Networking ClearPass Policy Manager

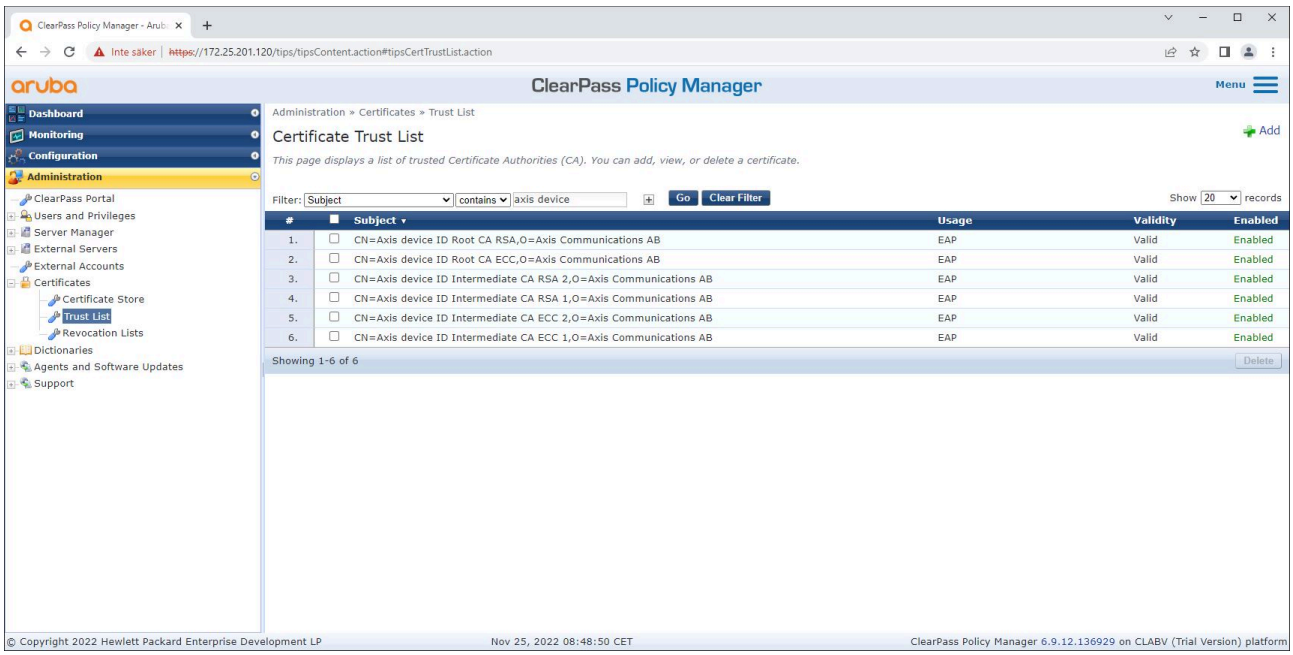
ClearPass Policy Manager는 다중 공급업체 유선, 무선 및 VPN 인프라 전반에 걸쳐 IoT, BYOD, 회사 장치, 직원, 계약자 및 게스트를 위한 역할 및 장치 기반의 보안 네트워크 접근 제어를 제공합니다.

신뢰할 수 있는 인증서 저장소 구성

1. axis.com에서 Axis 관련 IEEE 802.1AR 인증서 체인을 다운로드하십시오.
2. Axis 특정 IEEE 802.1AR 루트 CA 및 중간 CA 인증서 체인을 신뢰할 수 있는 인증서 저장소에 업로드합니다.
3. ClearPass Policy Manager를 활성화하여 IEEE 802.1X EAP-TLS를 통해 Axis 장치를 인증합니다.
4. 사용량 필드에서 EAP를 선택합니다. 인증서는 IEEE 802.1X EAP-TLS 인증에 사용됩니다.



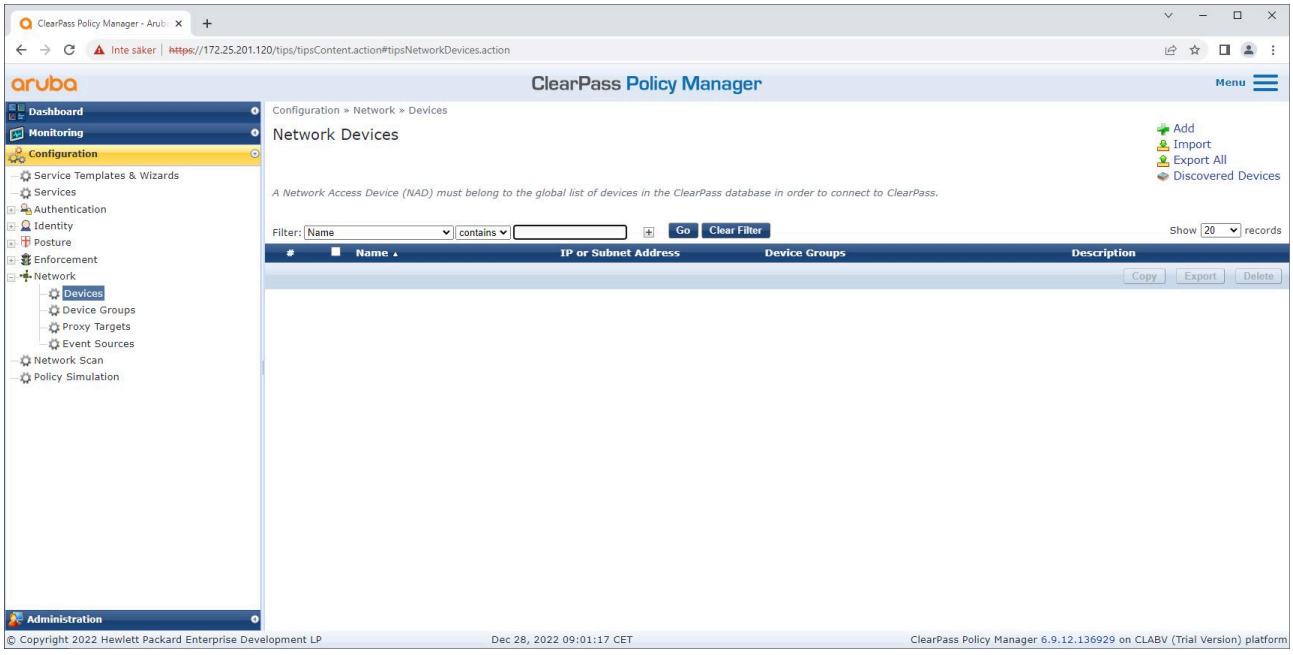
ClearPass Policy Manager의 신뢰할 수 있는 인증서 저장소에 Axis 관련 IEEE 802.1AR 인증서를 업로드합니다.



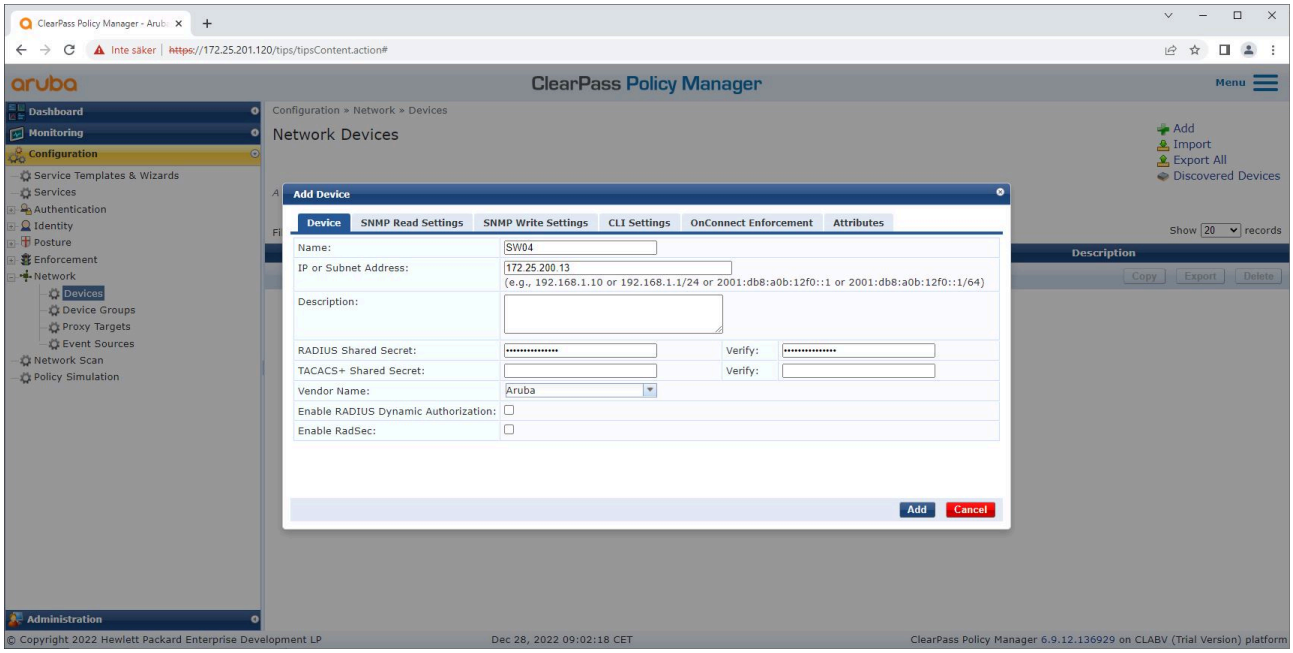
Axis 특정 IEEE 802.1AR 인증서 체인이 포함된 ClearPass Policy Manager의 신뢰할 수 있는 인증서 저장소입니다.

네트워크 장치/그룹 구성

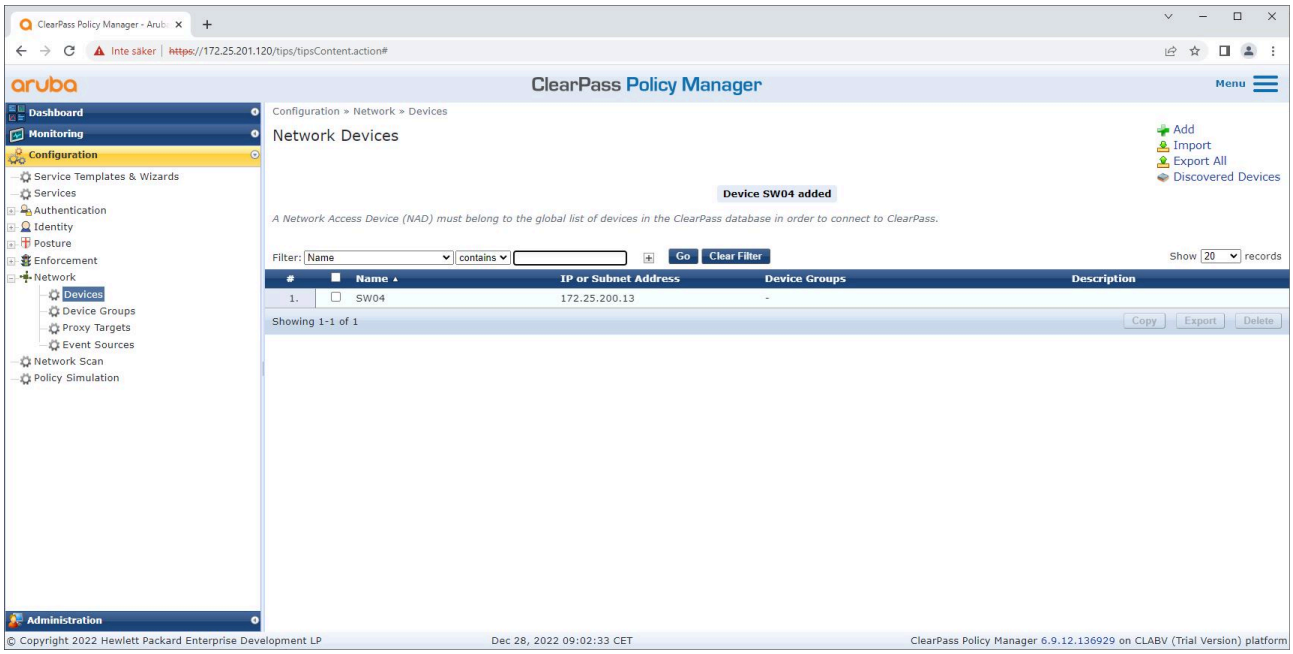
1. HPE Aruba Networking 액세스 스위치와 같은 신뢰할 수 있는 네트워크 액세스 장치를 ClearPass Policy Manager에 추가합니다. ClearPass Policy Manager는 네트워크에서 IEEE 802.1X 통신에 사용될 액세스 스위치를 알아야 합니다. 또한 RADIUS 공유 암호는 특정 스위치 IEEE 802.1X 구성과 일치해야 합니다.
2. 네트워크 장치 그룹 구성을 사용하여 신뢰할 수 있는 여러 네트워크 액세스 장치를 그룹화합니다. 장치를 그룹화하면 정책 구성을 더 쉽게 할 수 있습니다.



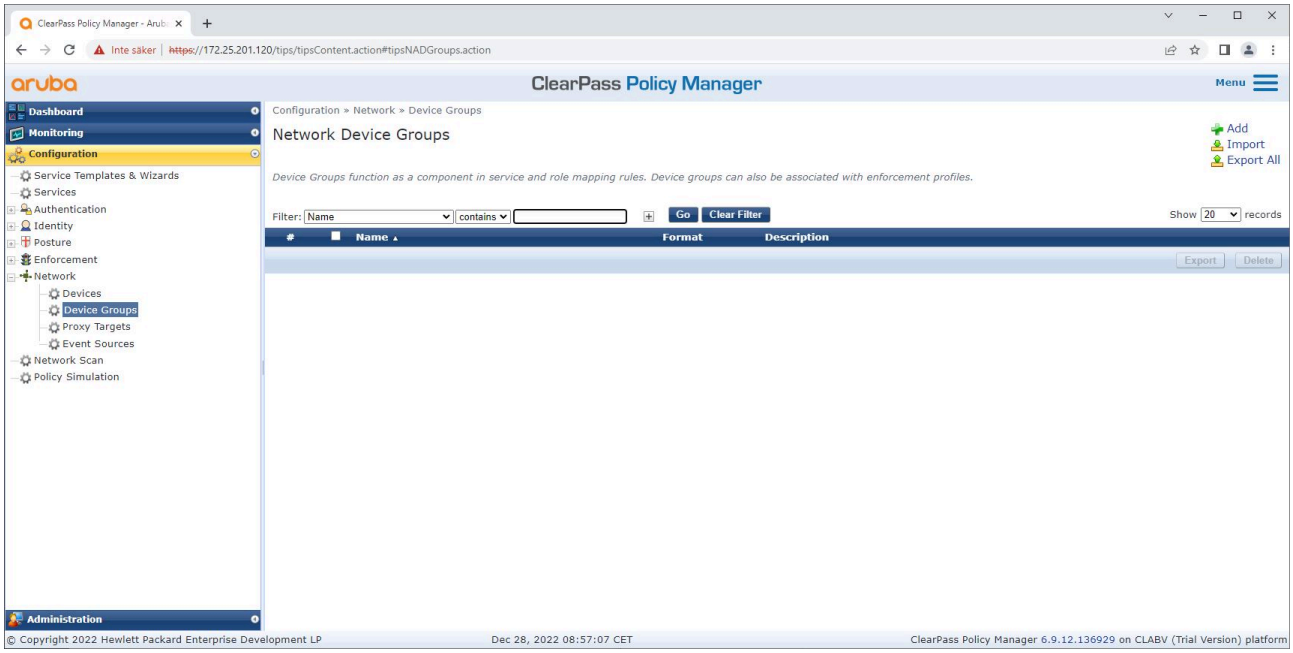
ClearPass Policy Manager의 신뢰할 수 있는 네트워크 장치 인터페이스입니다.



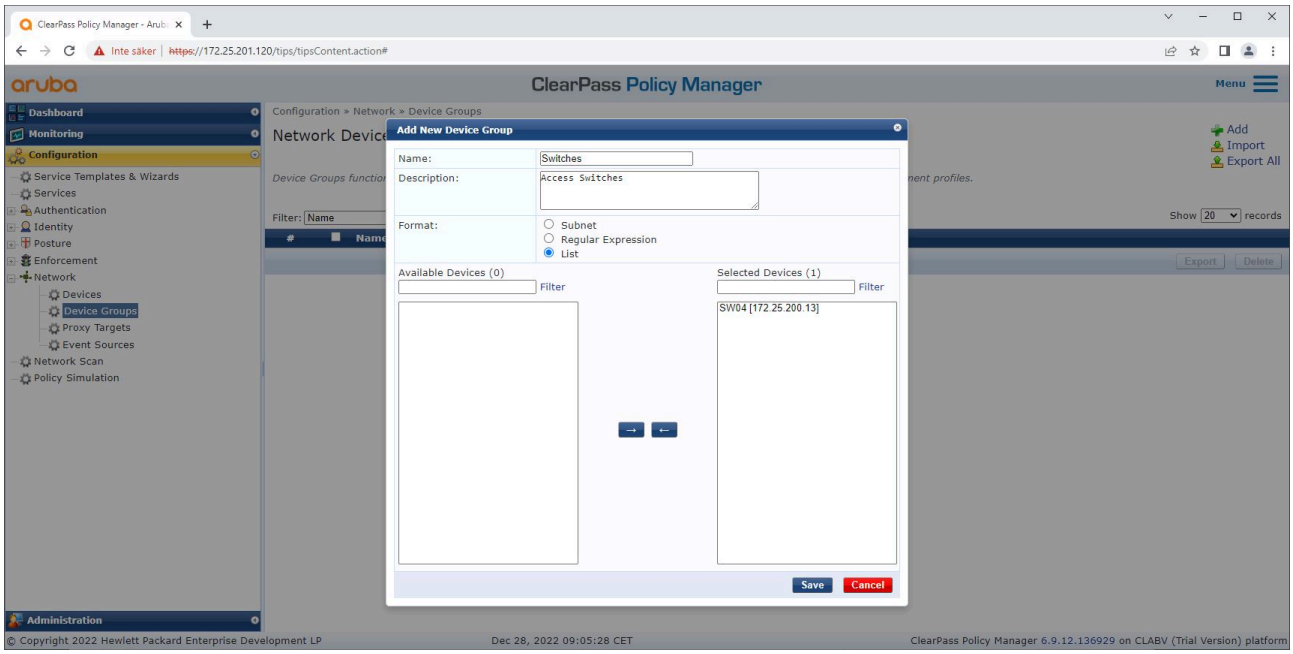
HPE Aruba Networking 액세스 스위치를 ClearPass Policy Manager에 신뢰할 수 있는 장치로 추가하십시오. RADIUS 공유 암호는 특정 스위치 IEEE 802.1X 구성과 일치해야 합니다.



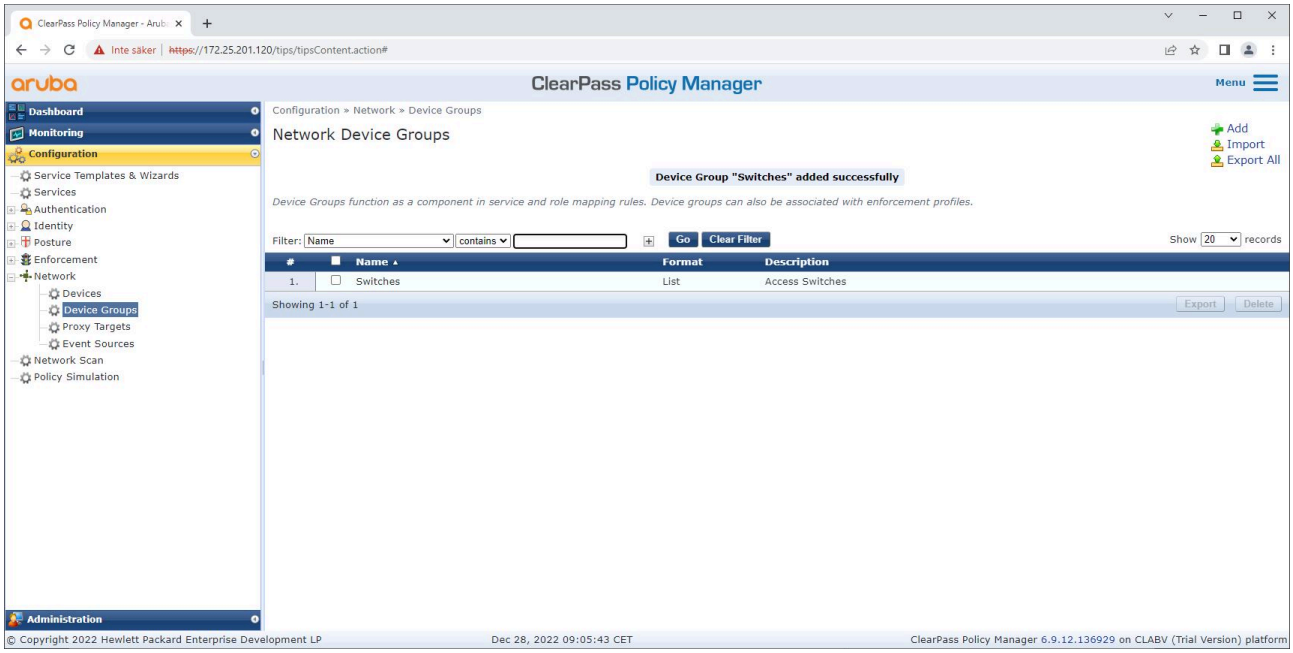
신뢰할 수 있는 단일 네트워크 장치가 구성된 ClearPass Policy Manager입니다.



ClearPass Policy Manager의 신뢰할 수 있는 네트워크 장치 그룹 인터페이스입니다.



신뢰할 수 있는 네트워크 액세스 장치를 ClearPass Policy Manager의 새 장치 그룹에 추가합니다.

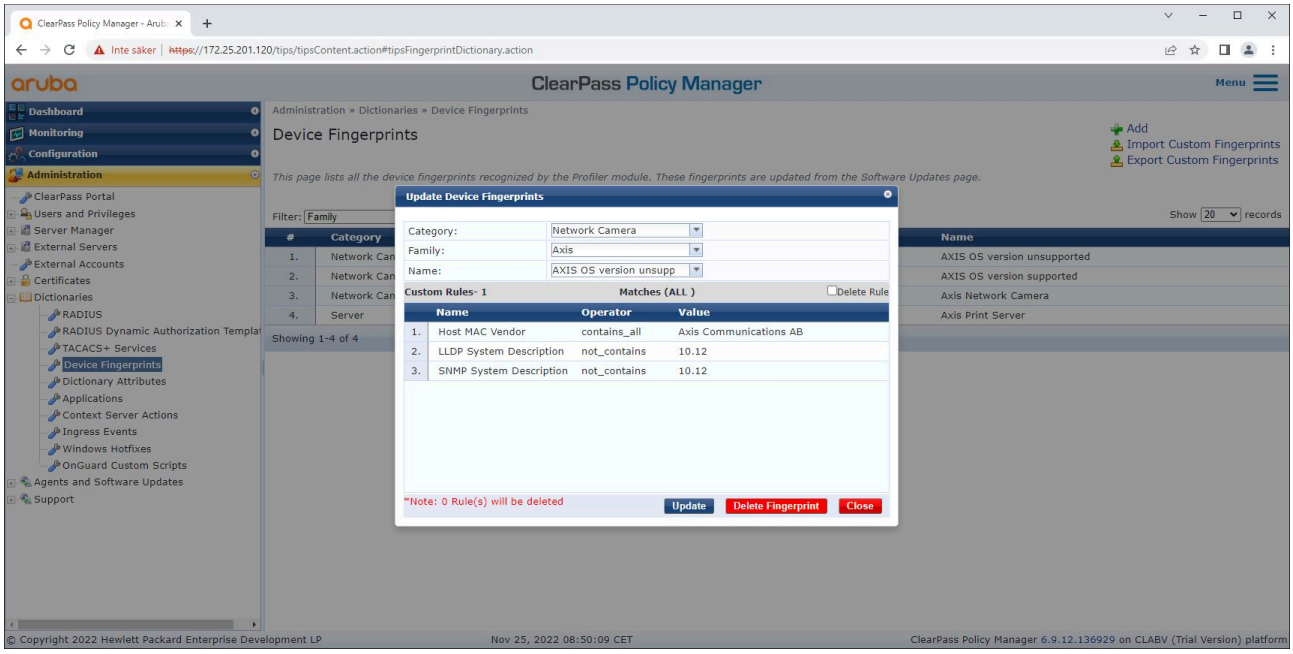


하나 이상의 신뢰할 수 있는 네트워크 장치를 포함하는 네트워크 장치 그룹이 구성된 ClearPass Policy Manager입니다.

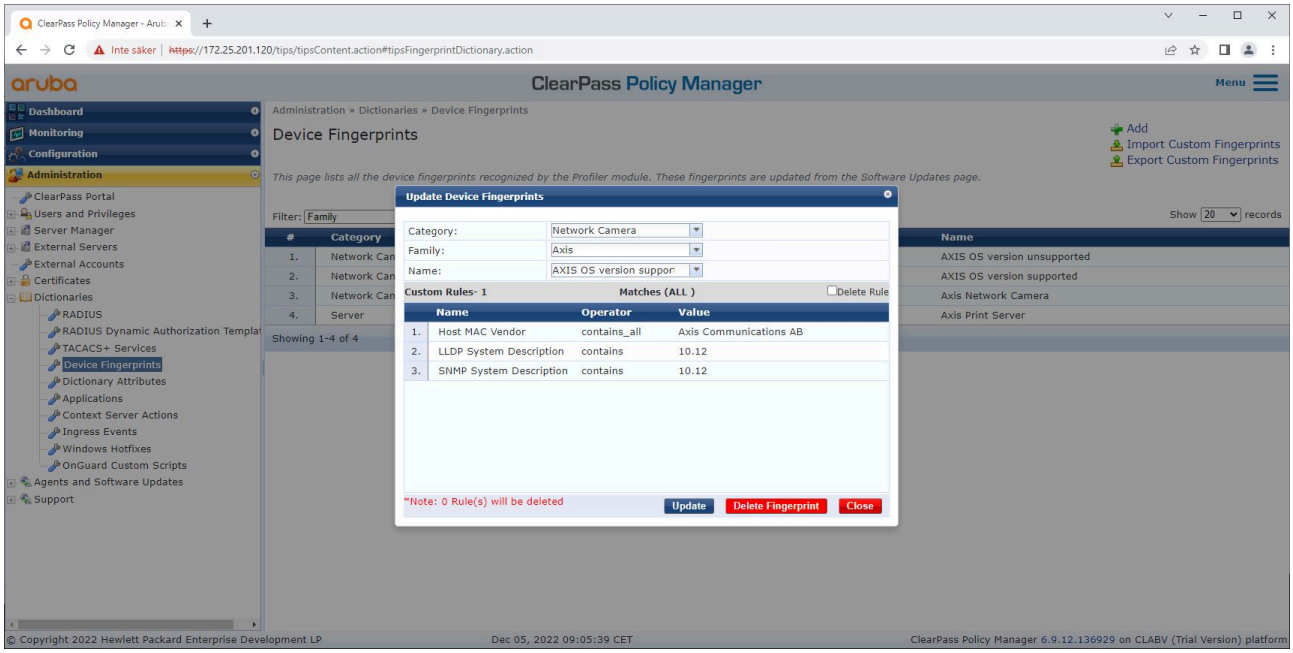
장치 지문 구성

Axis 장치는 네트워크 검색을 통해 MAC 주소 및 장치 소프트웨어 버전과 같은 장치별 정보를 배포할 수 있습니다. 이 정보를 사용하여 ClearPass Policy Manager에서 장치 지문을 생성, 업데이트 또는 관리할 수 있습니다. AXIS OS 버전에 따라 액세스를 허용하거나 거부할 수도 있습니다.

1. **Administration > Dictionaries > Device Fingerprints(관리 > 사전 > 장치 지문)**로 이동합니다.
2. 기존 장치 지문을 선택하거나 새 장치 지문을 생성합니다.
3. 장치 지문 설정을 구성합니다.



ClearPass Policy Manager의 장치 지문 구성입니다. 이 예시에서는 AXIS OS 10.12 이외의 버전을 실행하는 Axis 장치는 지원되지 않습니다.



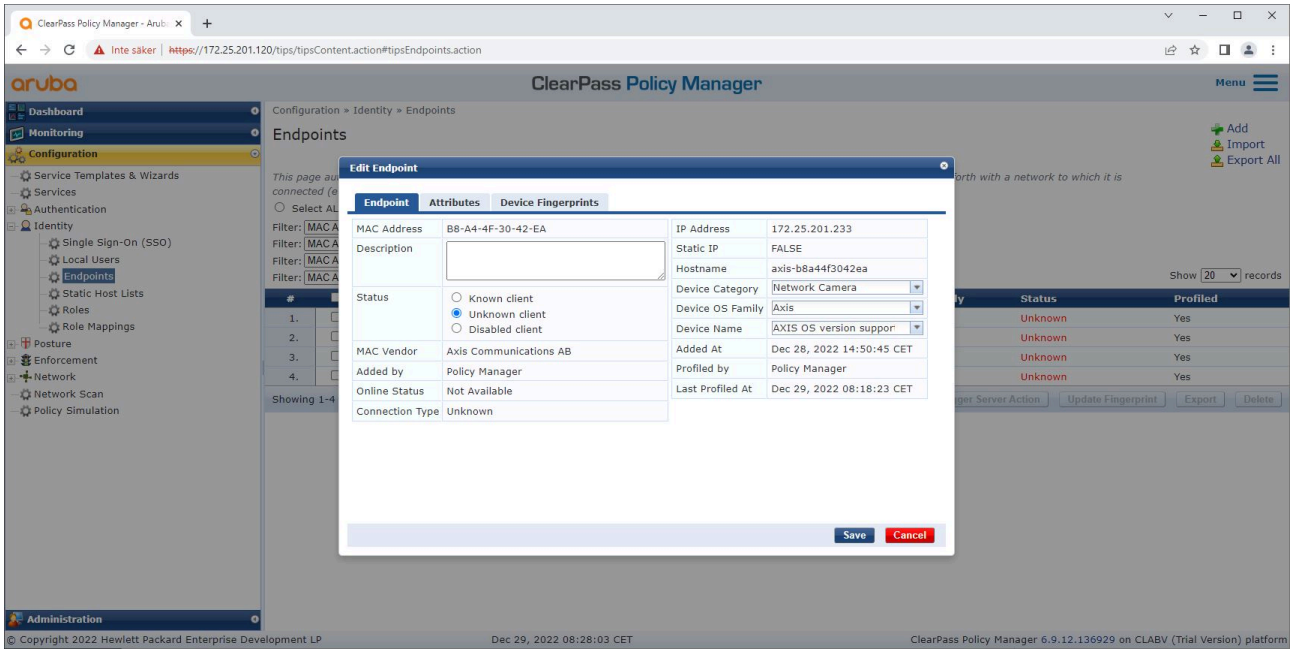
ClearPass Policy Manager의 장치 지문 구성입니다. 이 예시에서는 AXIS OS 10.12 이외의 버전을 실행하는 Axis 장치가 지원됩니다.

ClearPass Policy Manager가 수집한 장치 지문에 대한 정보는 엔드포인트 섹션에서 확인할 수 있습니다.

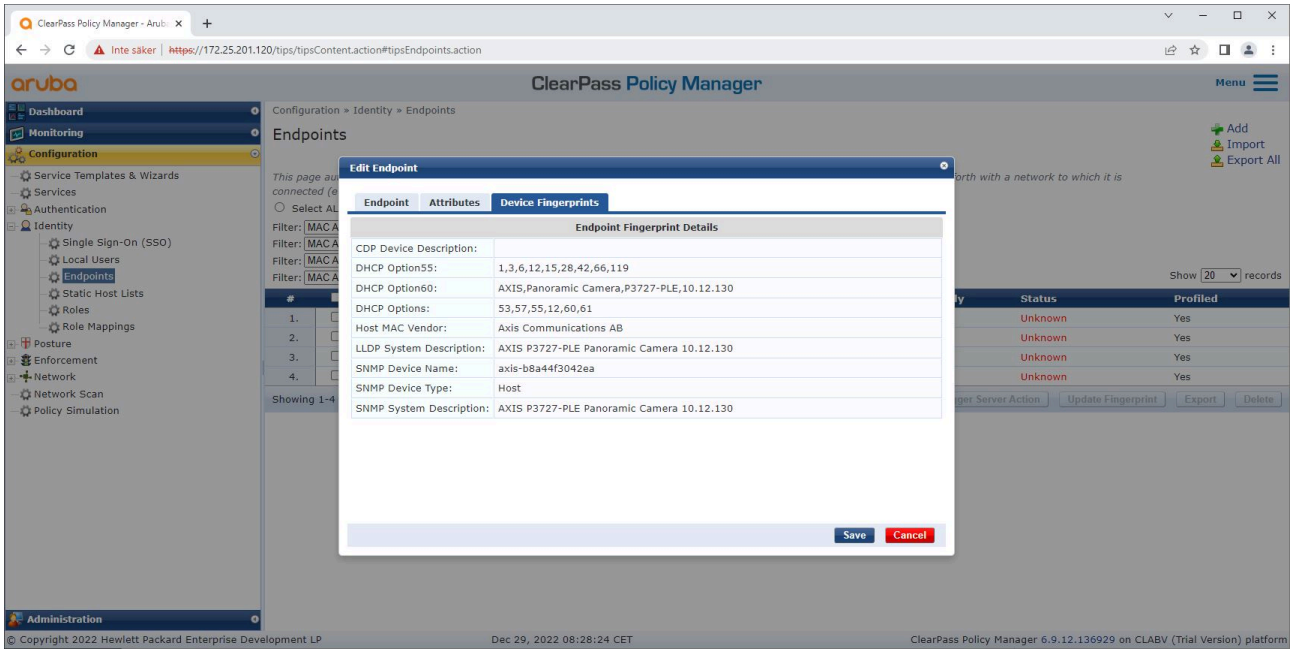
1. **Configuration > Identity > Endpoints(구성 > ID > 엔드포인트)**로 이동합니다.
2. 보려는 장치를 선택합니다.
3. **Device Fingerprints(장치 지문)** 탭을 클릭합니다.

비고

SNMP는 Axis 장치에서 기본적으로 비활성화되어 있으며, HPE Aruba Networking 액세스 스위치에서 수집됩니다.



ClearPass Policy Manager가 프로파일링한 Axis 장치입니다.

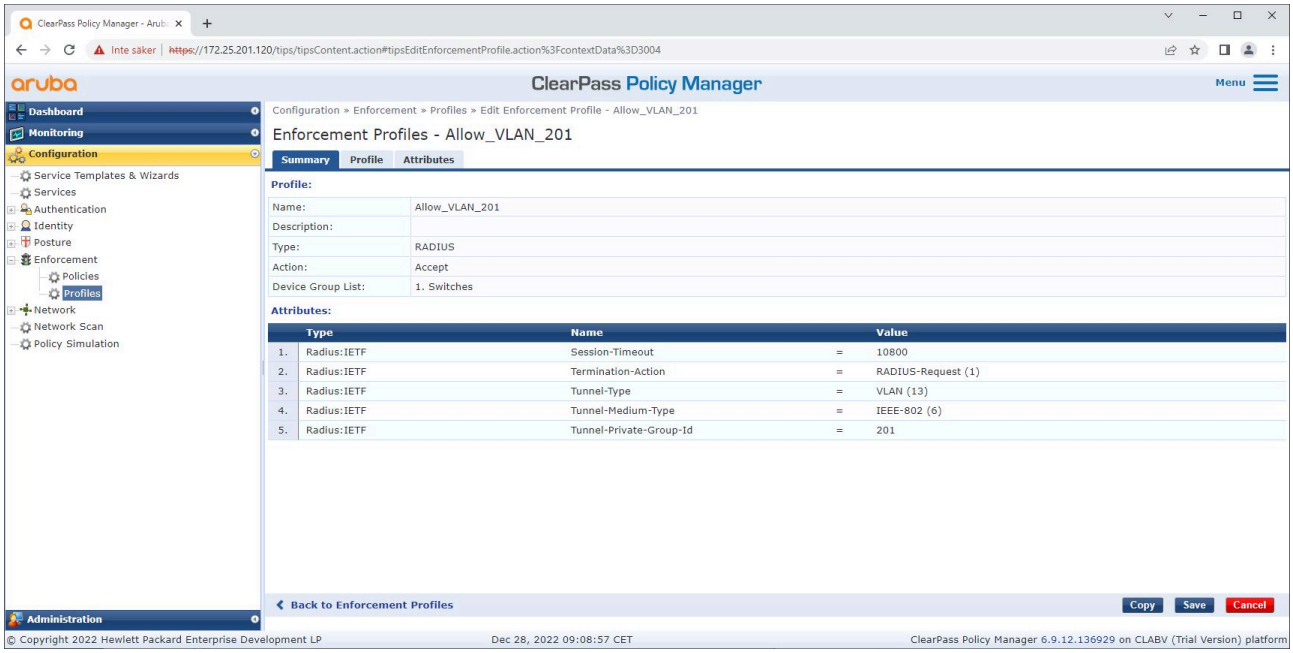


프로파일링된 Axis 장치의 자세한 장치 지문입니다. Axis 장치에서는 기본적으로 SNMP가 비활성화되어 있습니다. LLDP, CDP 및 DHCP 관련 검색 정보는 공장 출하 시 기본값 상태의 Axis 장치에서 공유되며 HPE Aruba Networking 액세스 스위치에 의해 ClearPass Policy Manager로 전달됩니다.

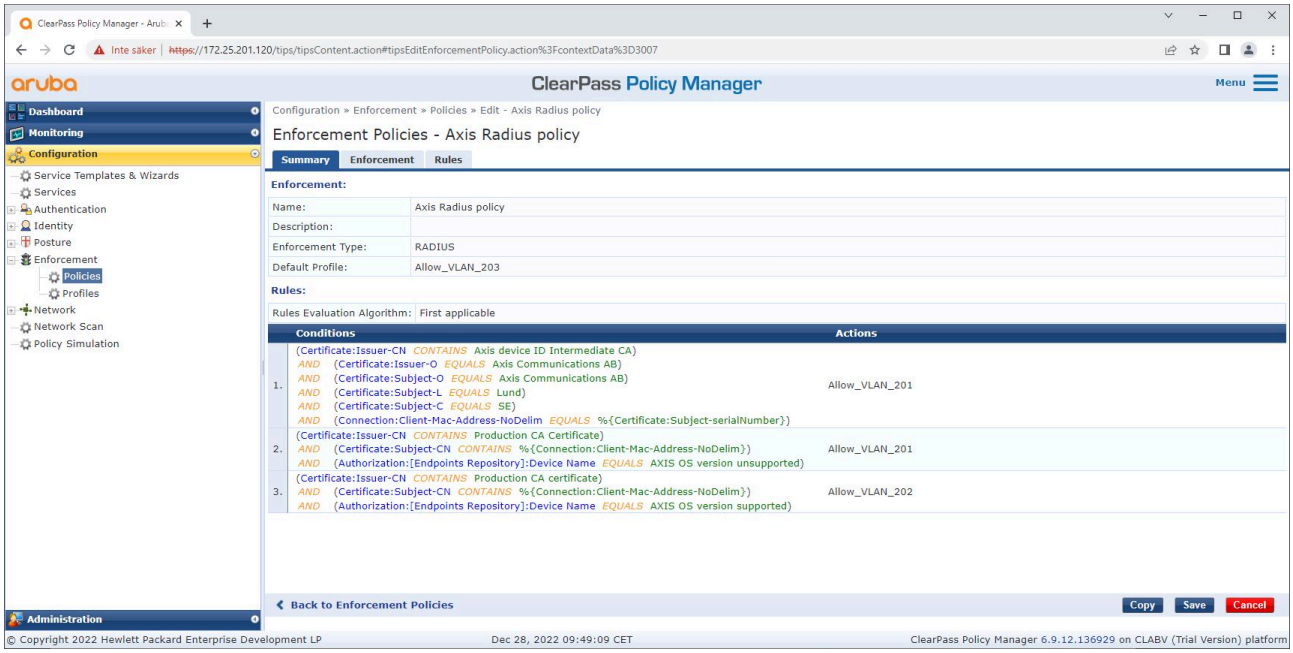
정책 적용 프로파일 구성

Enforcement Profile(정책 적용 프로파일)을 사용하면 ClearPass Policy Manager가 스위치의 액세스 포트에 특정 VLAN ID를 할당할 수 있습니다. 이것은 장치 그룹 "Switches(스위치)"의 네트워크 장치에 적용되는 정책 기반 결정입니다. 필요한 정책 적용 프로파일의 수는 사용 중인 VLAN의 수에 따라 달라집니다. Axis의 설정에는 3개의 VLAN(VLAN 201, 202, 203)이 있으며, 이는 3개의 정책 적용 프로파일에 해당합니다.

VLAN에 대한 정책 적용 프로파일이 구성되면 적용 정책 자체를 구성할 수 있습니다. ClearPass Policy Manager의 적용 정책 구성은 4개의 예시 정책 프로파일을 기반으로 Axis 장치에 HPE Aruba Networking 네트워크 액세스 권한 부여 여부를 정의합니다.



VLAN 201에 대한 액세스를 허용하는 정책 적용 프로파일의 예입니다.



ClearPass Policy Manager의 정책 적용 정책 구성입니다.

4가지 적용 정책과 해당 조치는 다음과 같습니다.

네트워크 액세스를 거부

IEEE 802.1X 네트워크 접근 제어 인증이 수행되지 않으면 네트워크 액세스가 거부됩니다.

게스트 네트워크(VLAN 203)

IEEE 802.1X 네트워크 접근 제어 인증이 실패하면 Axis 장치에는 제한되고 격리된 네트워크에 대한 접근 권한이 부여됩니다. 이후 적절한 조치를 결정하기 위해 장치에 대한 수동 검사가 필요합니다.

네트워크 프로비저닝(VLAN 201)

Axis 장치에는 프로비저닝 네트워크에 대한 접근 권한이 부여됩니다. 이는 *AXIS Device Manager* 및 *AXIS Device Manager Extend*를 통해 Axis 장치 관리 기능을 제공하기 위한 것입니다. 또한 AXIS OS 업데이트, 운영 환경용 인증서 및 기타 구성을 사용하여 Axis 장치를 구성할 수 있습니다. ClearPass Policy Manager는 다음 조건을 확인합니다.

- 장치의 AXIS OS 버전.
- 장치의 MAC 주소는 공급업체별 MAC 주소 체계 및 Axis 장치 ID 인증서의 일련 번호 속성과 일치합니다.
- Axis device ID 인증서가 검증 가능하며 발급자, 조직, 위치, 국가 등 Axis 관련 속성과 일치하는지 여부

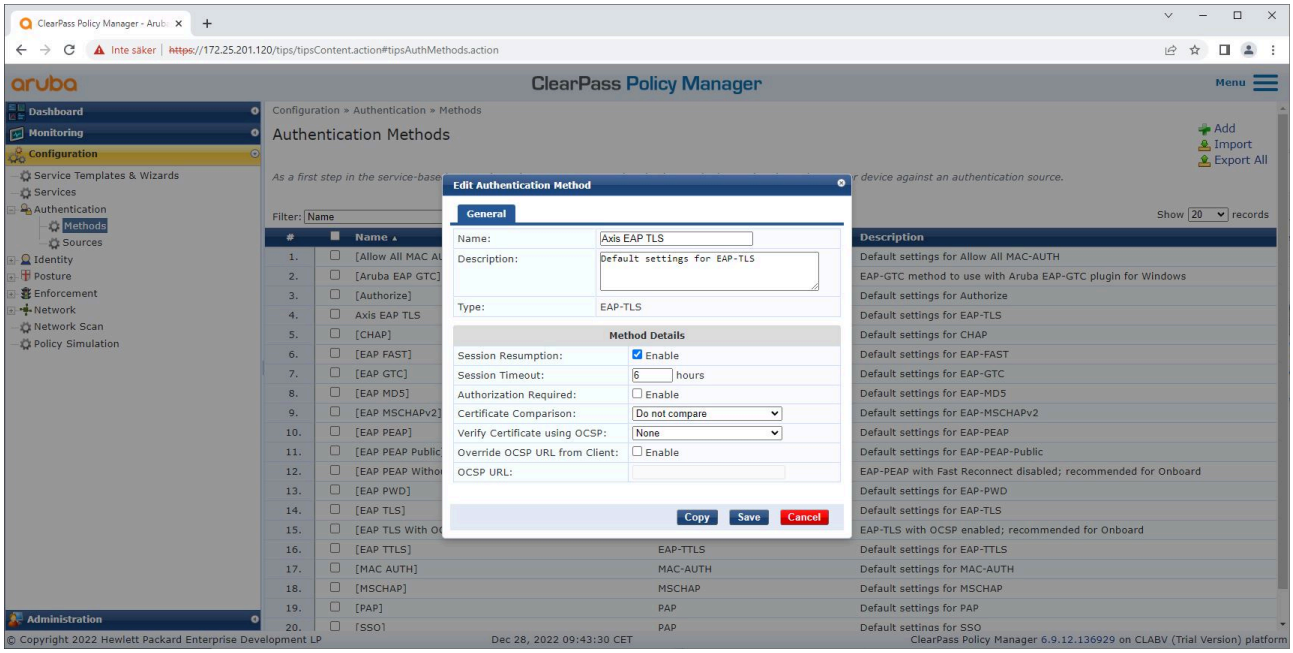
운영 네트워크(VLAN 202)

Axis 장치에는 운영 환경인 운영 네트워크에 대한 액세스 권한이 부여됩니다. 프로비저닝 네트워크(VLAN 201) 내에서 장치 프로비저닝이 완료된 후에 액세스 권한이 부여됩니다. ClearPass Policy Manager는 다음 조건을 확인합니다.

- 장치의 AXIS OS 버전.
- 장치의 MAC 주소는 공급업체별 MAC 주소 체계 및 Axis 장치 ID 인증서의 일련 번호 속성과 일치합니다.
- 프로덕션 등급 인증서는 신뢰할 수 있는 인증서 저장소에서 확인할 수 있습니다.

인증 방법 구성

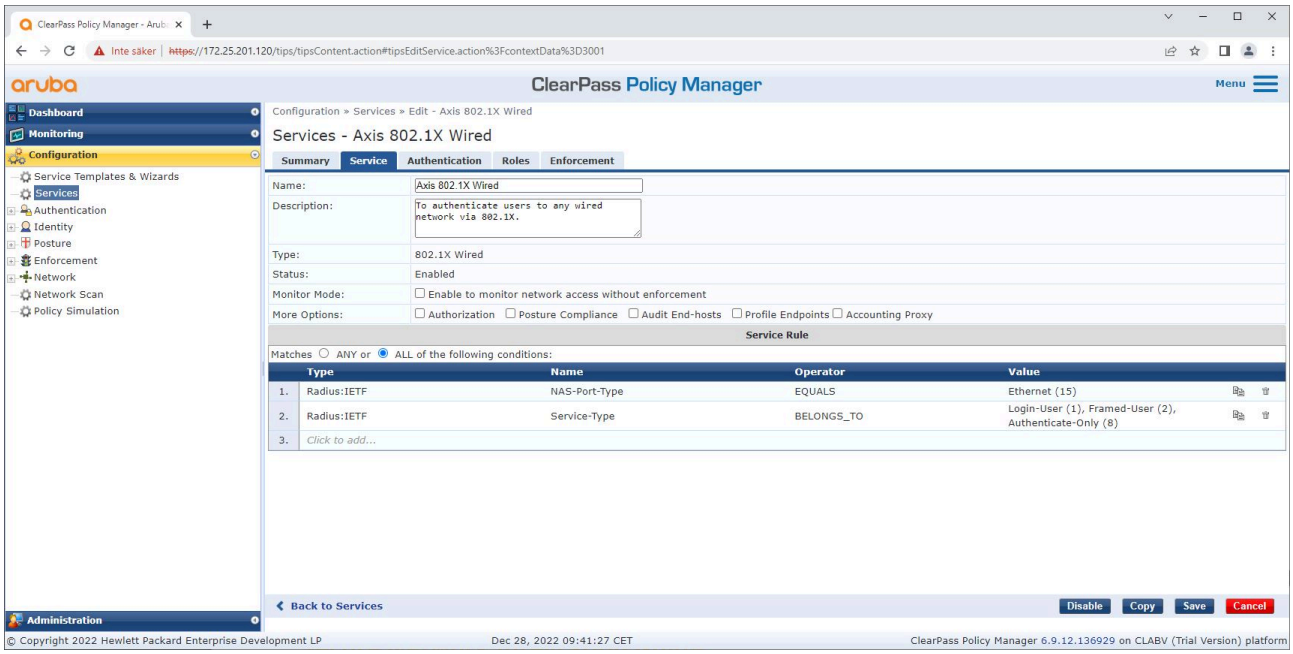
인증 방법은 Axis 장치가 네트워크에서 자체 인증하는 방법을 정의합니다. Axis Edge Vault가 탑재된 Axis 장치는 기본적으로 IEEE 802.1X EAP-TLS가 활성화되어 있으므로, IEEE 802.1X EAP-TLS가 선호되는 방법입니다.



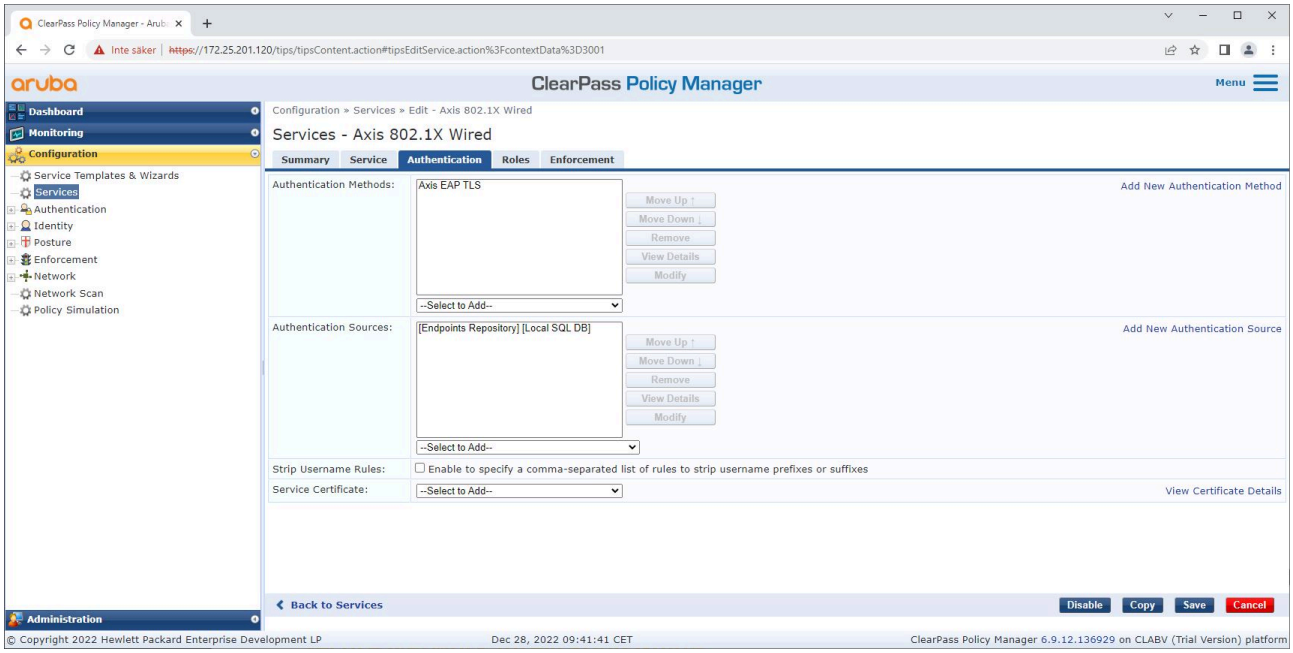
Axis 장치에 대한 EAP-TLS 인증 방법이 정의된 ClearPass Policy Manager의 인증 방법 인터페이스입니다.

서비스 구성

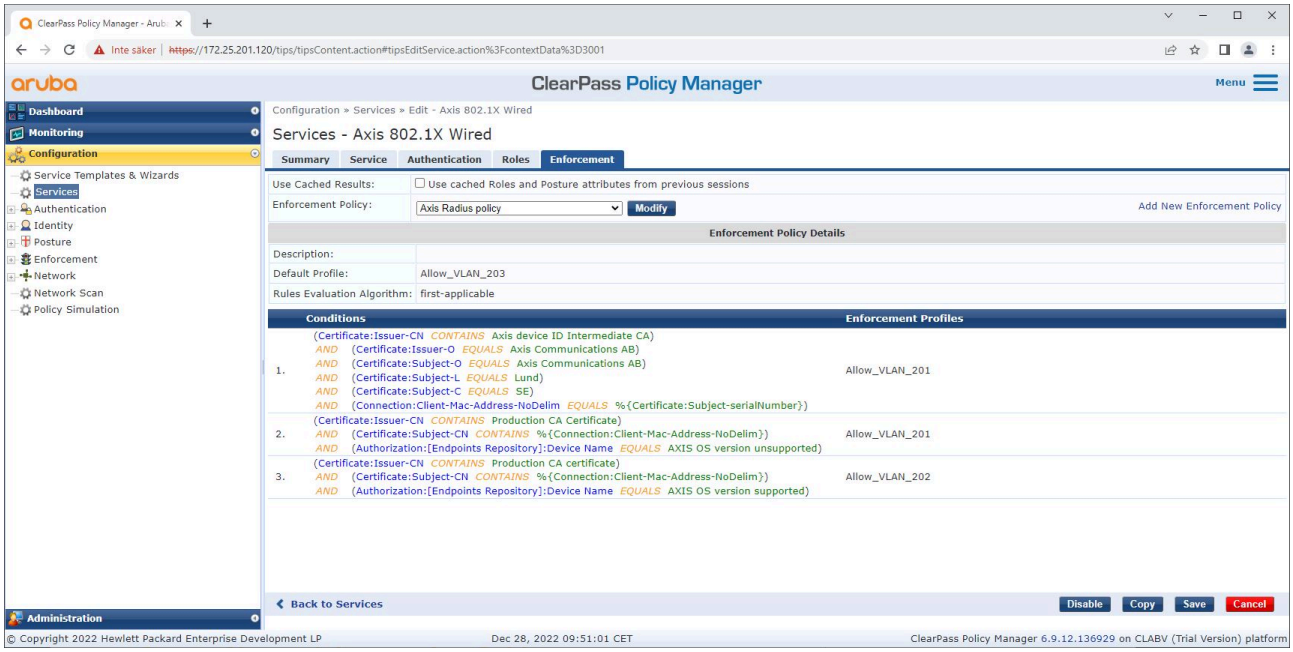
Services(서비스) 페이지에서 구성 단계는 HPE Aruba Networking 네트워크에서 Axis 장치의 인증 및 권한 부여를 처리하는 단일 서비스로 결합됩니다.



IEEE 802.1X를 연결 방법으로 사용하는 전용 Axis 서비스가 생성됩니다.



이전에 생성된 EAP-TLS 인증 방법이 서비스에 대해 구성됩니다.



이전에 생성된 적용 정책이 서비스에 대해 구성됩니다.

HPE Aruba Networking 액세스 스위치

Axis 장치는 PoE 지원 액세스 스위치에 직접 연결되거나 호환되는 Axis PoE 미드스팬을 통해 연결됩니다. Axis 장치를 HPE Aruba Networking 네트워크에 안전하게 온보딩하려면 액세스 스위치가 IEEE 802.1X 통신을 위해 구성되어야 합니다. Axis 장치는 IEEE 802.1x EAP-TLS 통신을 RADIUS 서버 역할을 하는 ClearPass Policy Manager로 전달합니다.

비고

전체 포트 액세스 보안을 높이기 위해 Axis 장치에 대해 300초의 주기적인 재인증도 구성됩니다.

이 예시는 HPE Aruba Networking 액세스 스위치에 대한 글로벌 및 포트 구성을 보여줍니다.

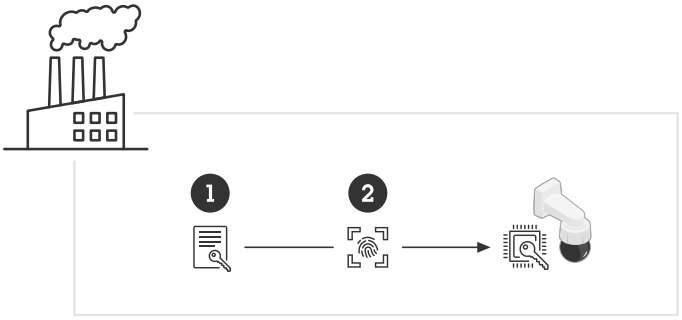
```
radius-server host MyRADIUSIPAddress key "MyRADIUSKey"

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
```

Axis 구성

Axis 네트워크 장치

*Axis Edge Vault*를 지원하는 Axis 장치는 Axis 장치 ID라는 보안 장치 ID와 함께 제조됩니다. Axis 장치 ID는 IEEE 802.1AR 국제 표준을 기반으로 하며, IEEE 802.1X를 통한 자동화된 보안 장치 식별 및 네트워크 온보딩 방법을 정의합니다.



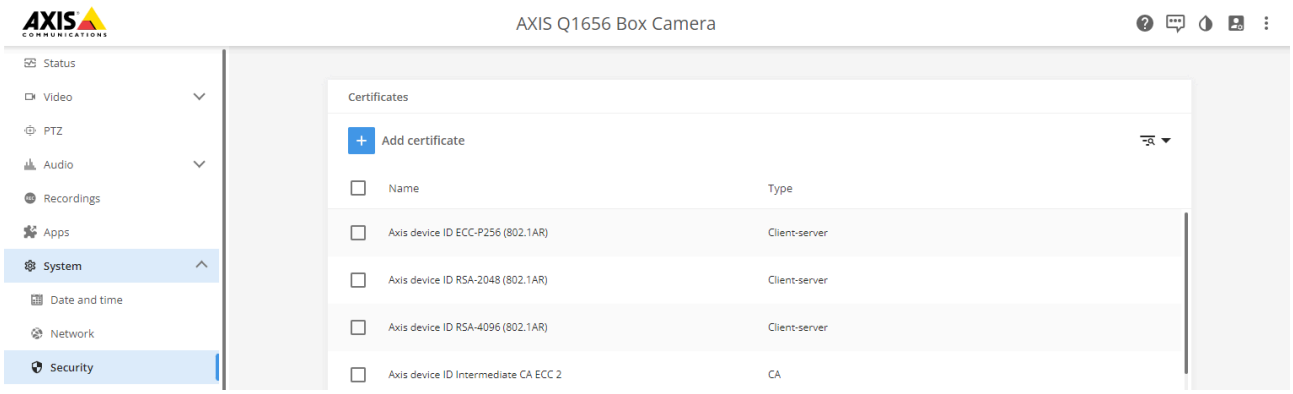
Axis 장치는 신뢰할 수 있는 장치 ID 서비스를 위해 IEEE 802.1AR 호환 Axis device ID 인증서로 제조됩니다.

1 *Axis 장치 ID key infrastructure(PKI)*
2 *Axis device ID*

Axis 장치의 보안 요소가 제공하는 하드웨어 보호 보안 키스토어는 장치 고유 인증서 및 해당 키(Axis 장치 ID)와 함께 공장에서 프로비저닝되어 Axis 장치의 진위 여부를 전 세계적으로 증명할 수 있습니다. *Axis Product Selector*를 사용하면 Axis Edge Vault 및 Axis 장치 ID를 지원하는 Axis 장치를 찾을 수 있습니다.

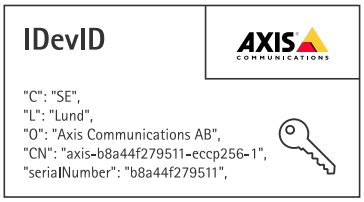
비고

Axis 장치의 일련 번호는 MAC 주소입니다.



Axis 장치 ID가 포함된, 공장 출하 시 기본값 상태의 Axis 장치 인증서 저장소입니다.

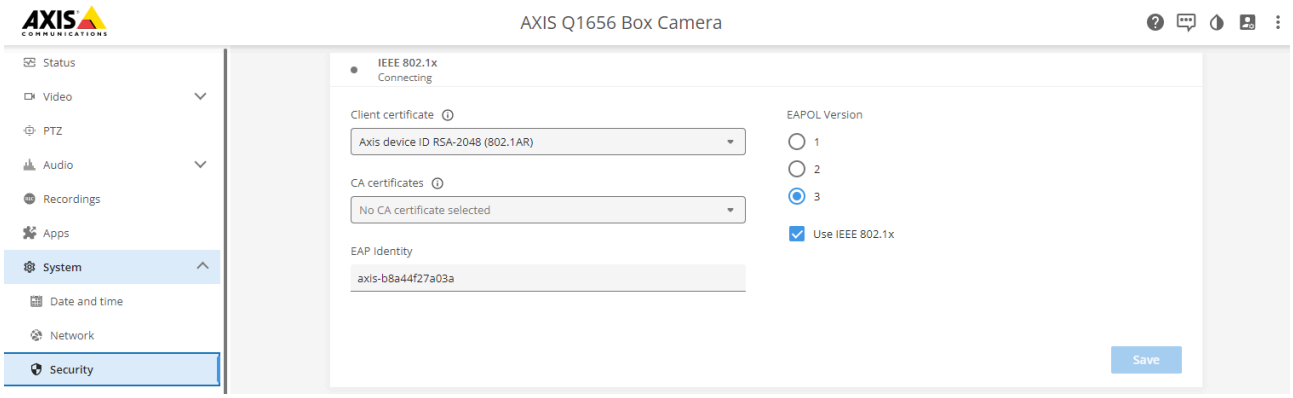
IEEE 802.1AR 호환 Axis 장치 ID 인증서에는 일련 번호 및 기타 공급업체별 정보가 포함됩니다. 이 정보는 ClearPass Policy Manager에서 네트워크 액세스 권한을 부여하기 위한 분석 및 의사 결정에 사용됩니다. 다음 정보는 Axis 장치 ID 인증서에서 얻을 수 있습니다.



국가	SE
위치	룬드

발급자 조직	Axis Communications AB
발급자 일반 이름	Axis device ID 중간
조직	Axis Communications AB
일반 이름	axis-b8a44f279511-eccp256-1
일련 번호	b8a44f279511

일반 이름은 Axis 회사 이름, 장치 일련 번호, 암호화 알고리즘(ECC P256, RSA 2048, RSA 4096)의 조합으로 구성됩니다. AXIS OS 10.1(2020-09)부터 IEEE 802.1X는 Axis 장치 ID가 사전 구성된 상태로 기본 활성화됩니다. 이를 통해 장치는 IEEE 802.1X 지원 네트워크에서 자체 인증할 수 있습니다.



IEEE 802.1X가 활성화되고 Axis 장치 ID 인증서가 사전 선택된, 공장 기본 상태의 Axis 장치입니다.

AXIS Device Manager

*AXIS Device Manager*와 *AXIS Device Manager Extend*는 네트워크에서 여러 Axis 장치를 비용 효율적으로 구성하고 관리하는 데 사용할 수 있습니다. AXIS Device Manager는 네트워크의 시스템에 로컬로 설치되는 Microsoft Windows® 기반 애플리케이션이며, AXIS Device Manager Extend는 클라우드 인프라를 기반으로 다중 사이트 장치 관리를 수행합니다. 두 솔루션 모두 다음과 같은 간편한 관리 및 구성 기능을 제공합니다.

- AXIS OS 업데이트를 설치합니다.
- HTTPS 및 IEEE 802.1X 인증서와 같은 사이버 보안 구성 적용.
- 이미지 설정 등 장치별 설정 구성.

안전한 네트워크 운영 - IEEE 802.1AE MACsec

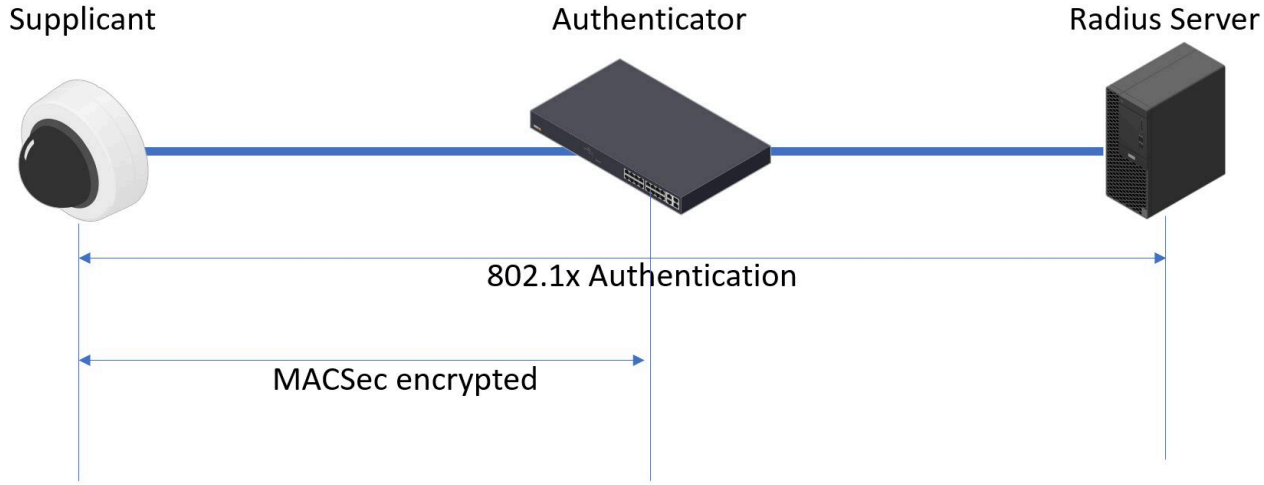
이 비디오를 시청하려면 이 문서의 웹 버전으로 이동하십시오.

IEEE 802.1AE MACsec 레이어 2 보안을 통한 제로 트러스트 네트워크 암호화

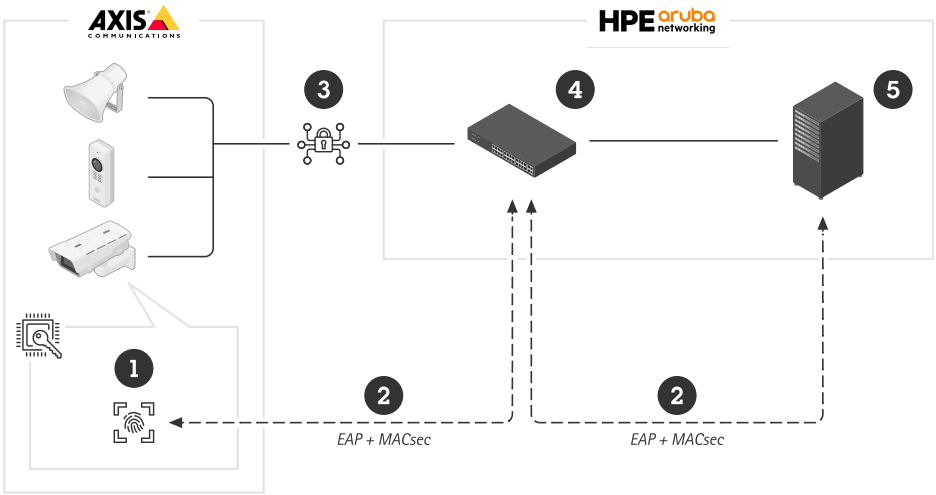
IEEE 802.1AE MACsec(Media Access Control Security)은 네트워크 계층 2의 지점 간 이더넷 링크를 암호화 방식으로 보호하는 잘 정의된 네트워크 프로토콜입니다. 이는 두 호스트 간의 데이터 전송의 기밀성과 무결성을 보장합니다.

IEEE 802.1AE MACsec 표준은 두 가지 작동 모드를 설명합니다.

- 수동으로 구성 가능한 사전 공유 키/정적 CAK 모드
- IEEE 802.1X EAP-TLS를 사용하는 자동 마스터 세션/동적 CAK 모드



AXIS OS 10.1(2020-09) 이상에서는 Axis 장치 ID와 호환되는 장치에 대해 IEEE 802.1X가 기본적으로 활성화됩니다. AXIS OS 11.8 이상에서는 기본적으로 활성화된 IEEE 802.1X EAP-TLS를 사용하여 자동 동적 모드로 MACsec을 지원합니다. 공장 출하 시 기본값의 Axis 장치를 연결하면 IEEE 802.1X 네트워크 인증이 수행되고, 성공하면 MACsec 동적 CAK 모드도 시도됩니다.



안전하게 저장된 Axis 장치 ID(1) – IEEE 802.1AR 호환 보안 장치 ID –는 IEEE 802.1X EAP-TLS 포트 기반 네트워크 액세스 제어(2)를 통해 네트워크에서 인증(4, 5)하는 데 사용됩니다. EAP-TLS 세션을 통

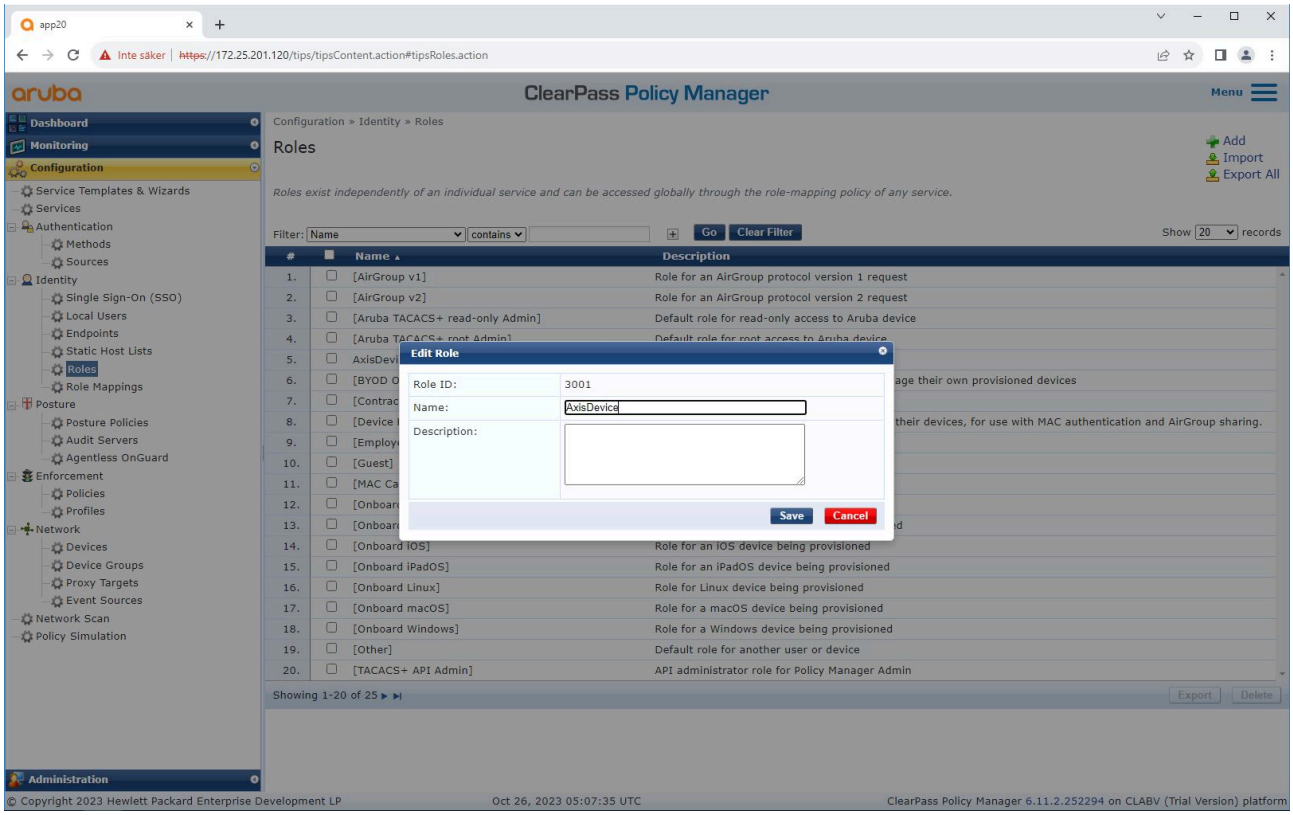
해 MACsec 키가 자동으로 교환되어 보안 링크(3)를 설정하여 Axis 장치에서 HPE Aruba Networking 액세스 스위치로의 모든 네트워크 트래픽을 보호합니다.

IEEE 802.1AE MACsec에는 HPE Aruba Networking 액세스 스위치와 ClearPass Policy Manager 구성 준비가 모두 필요합니다. EAP-TLS를 통한 IEEE 802.1AE MACsec 암호화 통신을 허용하기 위해 Axis 장치에 구성이 필요하지 않습니다.

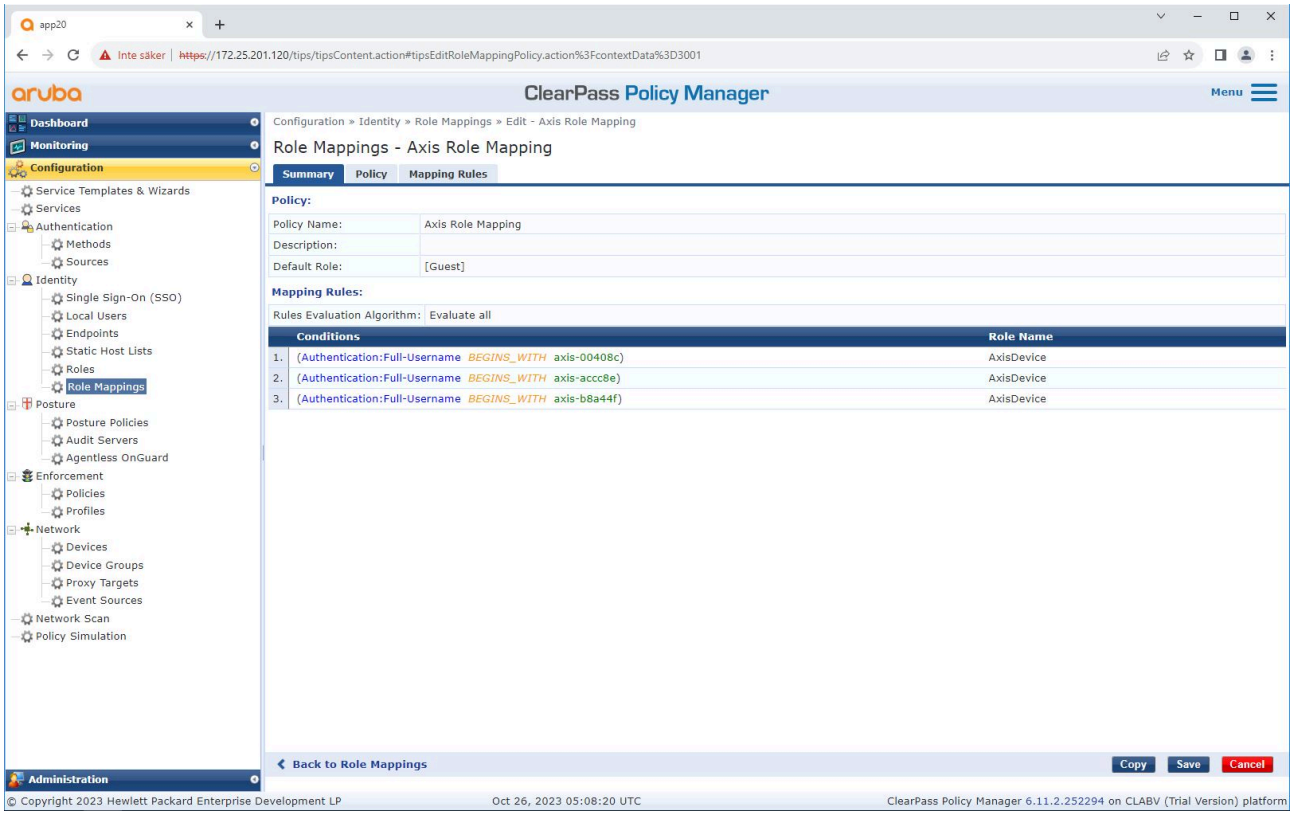
HPE Aruba Networking 액세스 스위치가 EAP-TLS를 사용하는 MACsec을 지원하지 않는 경우 사전 공유 키 모드를 사용하고 수동으로 구성할 수 있습니다.

HPE Aruba Networking ClearPass Policy Manager

역할 및 역할 매핑 정책



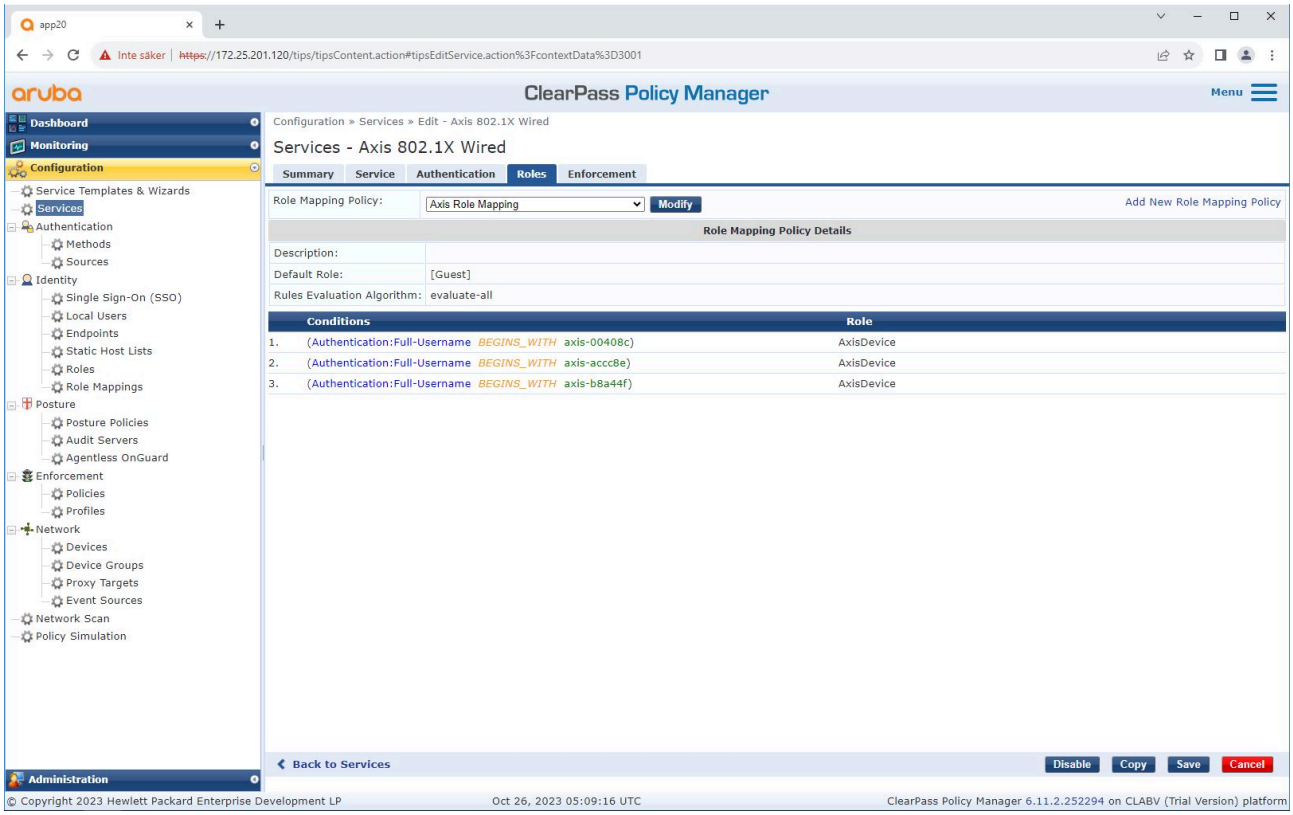
Axis 장치에 대한 역할 이름을 추가합니다. 이름은 액세스 스위치 구성의 포트 액세스 역할 이름입니다.



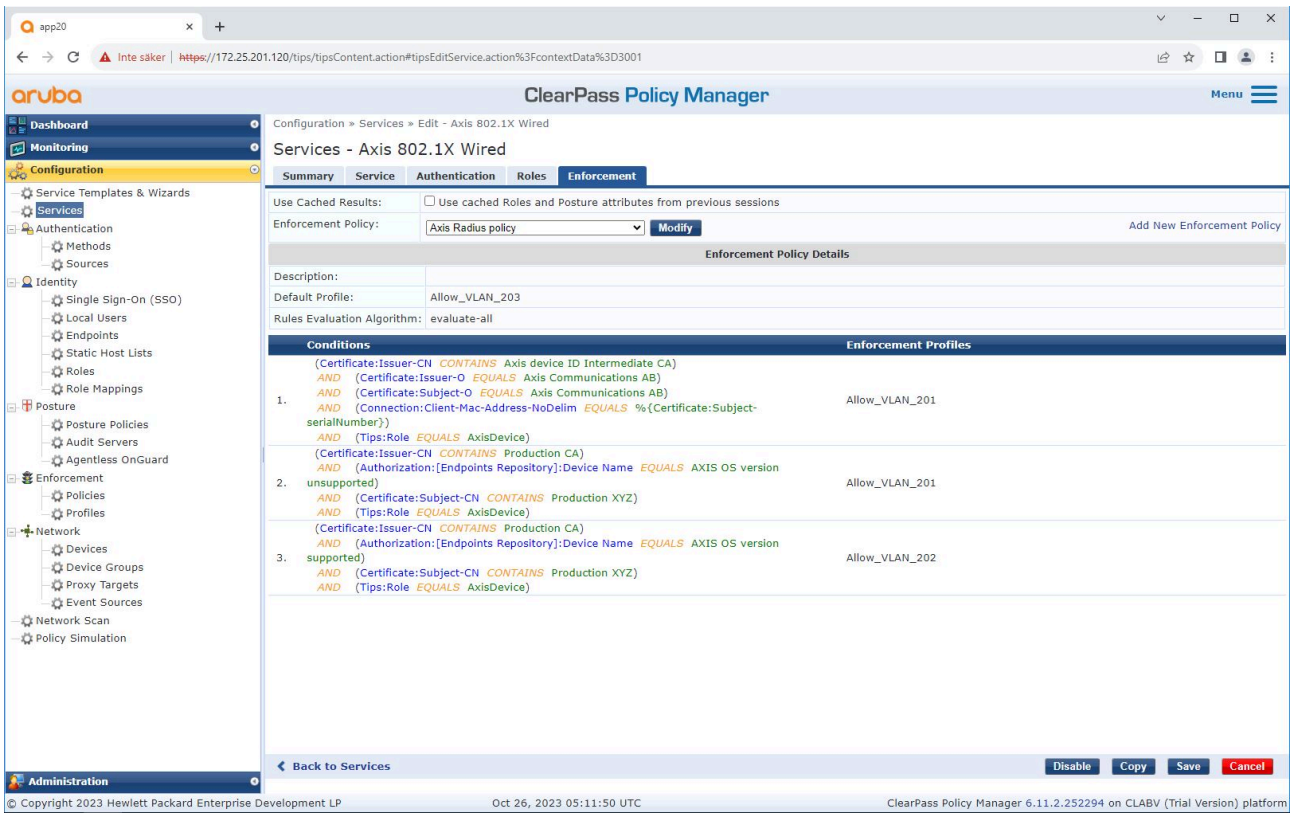
이전에 생성된 Axis 장치 역할에 대한 Axis 역할 매핑 정책을 추가합니다. 장치를 Axis 장치 역할에 매핑하려면 정의된 조건이 필요합니다. 조건이 충족되지 않으면 장치는 [Guest] 역할의 일부가 됩니다.

기본적으로 Axis 장치는 "axis-일련 번호" EAP ID 형식을 사용합니다. Axis 장치의 일련 번호는 MAC 주소입니다. 예를 들어 "axis-b8a44f45b4e6"입니다.

서비스 구성

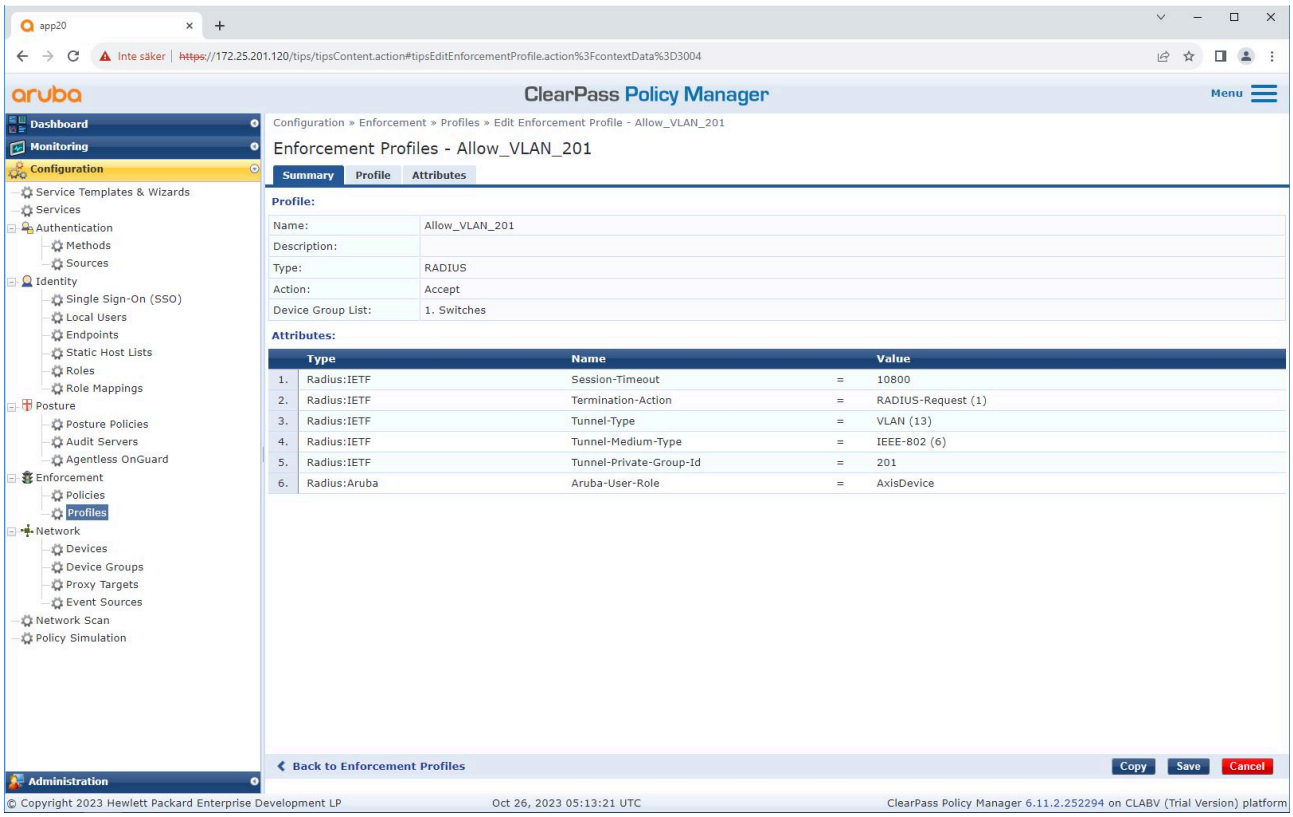


Axis 장치 온보딩을 위한 연결 방법으로 IEEE 802.1X를 정의하는 서비스에 이전에 생성된 Axis 역할 매핑 정책을 추가합니다.



기존 정책 정의에 Axis 역할 이름을 조건으로 추가합니다.

정책 적용 프로파일



IEEE 802.1X 온보딩 서비스에 할당된 정책 적용 프로파일에 Axis 역할 이름을 속성으로 추가합니다.

HPE Aruba Networking 액세스 스위치

*HPE Aruba Networking 액세스 스위치, on page 15*에 설명된 보안 온보딩 구성 외에도 IEEE 802.1AE MACsec을 구성하기 위한 HPE Aruba Networking 액세스 스위치의 예시 포트 구성은 아래를 참조하십시오.

```
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
```

인증서 관리 – Enrollment over Secure Transport(EST)

디지털 인증서는 장치와 네트워크를 보호하는 데 필수적이지만, 관리 작업이 복잡하고 시간이 많이 소요될 수 있습니다. 인증서는 만료되며 정기적으로 갱신해야 합니다. 자동화가 없으면 이 프로세스는 반복적인 수작업이 되며, 특히 대규모 구축 환경이나 다양한 장치 유형이 혼재된 환경에서는 관리 부담이 커집니다.

AXIS OS 12.9에는 Enrollment over Secure Transport(EST) 지원이 추가되었습니다. EST는 장치에 인증서를 안전하게 프로비저닝하기 위한 프로토콜입니다. RFC 7030에 정의된 EST는 인증서 수명 주기 전체를 단순화하고 자동화하도록 설계된 표준 기반 솔루션이며, 다음을 포함합니다.

- 등록 – 장치에 새 인증서를 안전하게 발급
- 갱신 – 만료가 임박한 인증서를 자동으로 교체
- 재등록 – IT 정책에 따라 인증서 업데이트

EST는 유효 기간, 키 유형(RSA/ECC), 키 길이 등 인증서 속성에 대한 IT 정의 정책을 지원하며, HTTPS만 사용합니다.

EST의 주요 이점

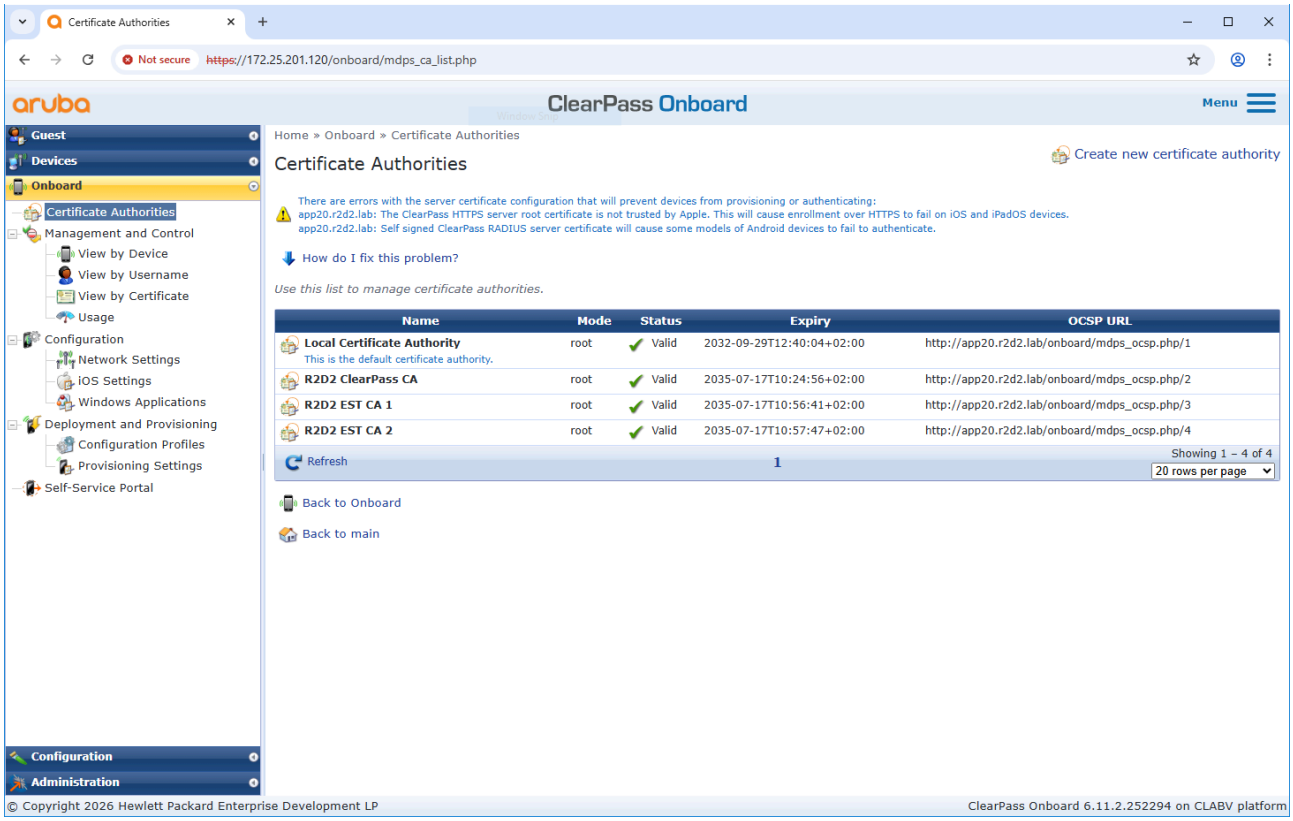
- IT 정책으로 관리되는 인증서 자동 등록/갱신/재등록을 통해, 시간이 많이 드는 수동 구성이 전혀 필요하지 않습니다.
- HTTPS 전용 TLS 1.2/1.3을 통해 최첨단 보안 통신을 제공합니다.
- IT 팀을 위한 중앙 집중식 가시성 및 모니터링을 제공합니다.
  표준 기반(RFC 7030)이며 IT 인프라와 통합됩니다.
- IoT, 엔터프라이즈 네트워크 및 장치 관리를 위한 확장 가능한 솔루션입니다.

EST 일반 문서는 *AXIS OS 지식 베이스*를 참조하십시오.

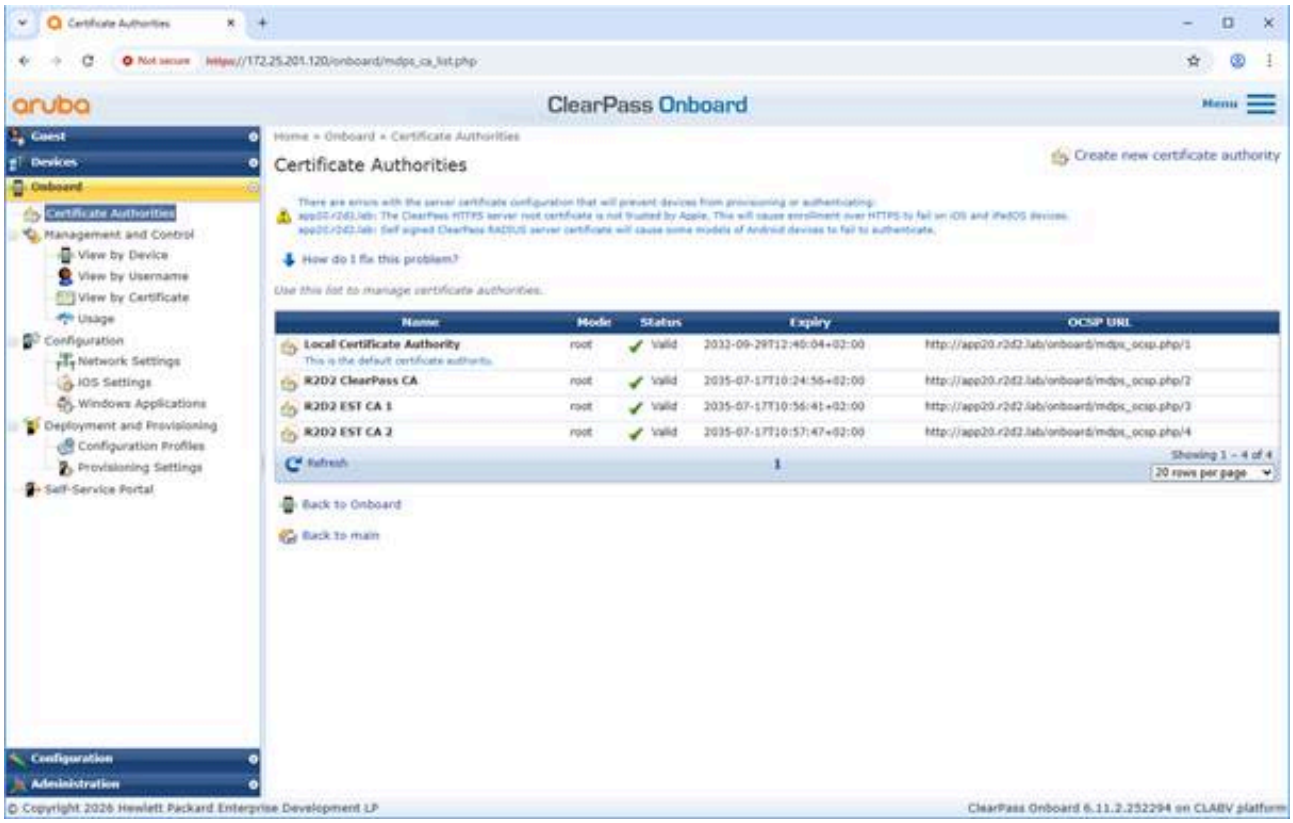
HPE Aruba ClearPass Onboard 구성

Aruba ClearPass Onboard는 EST와 통합되어 네트워크 액세스를 위한 장치 인증서를 안전하게 배포하고 관리합니다. EST를 사용하면 엔드포인트가 ClearPass에 인증한 후, 보안 TLS 채널을 통해 고유 인증서를 등록합니다. 이 인증서는 이후 802.1X 인증서 기반 인증 및 기타 서비스에 사용됩니다. 이는 장치 ID를 기반으로 보안 액세스 정책을 시행할 수 있는 표준 기반 자동화 및 패스워드리스(password-less) 방식을 제공합니다.

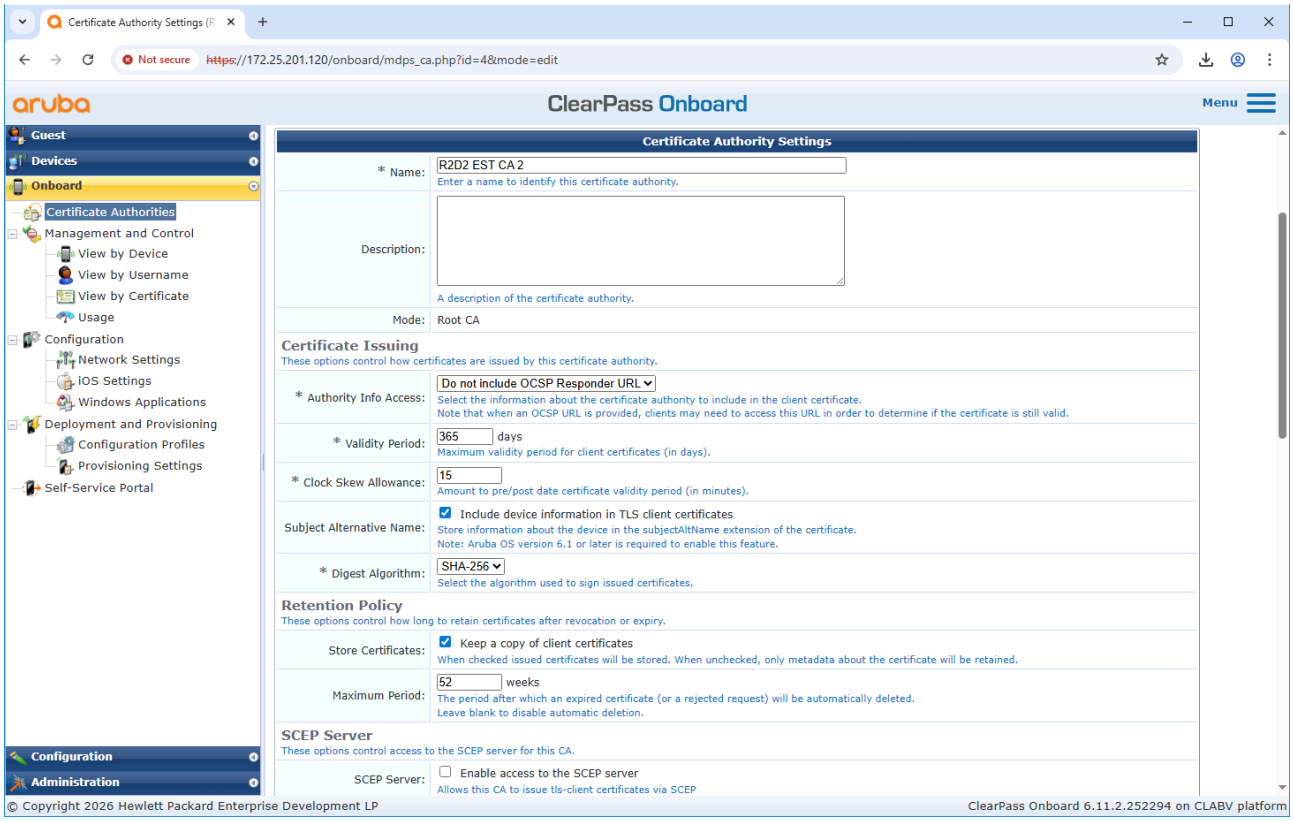
인증 기관(CA) 구성



ClearPass Onboard에서 새 인증 기관(CA)을 생성합니다.



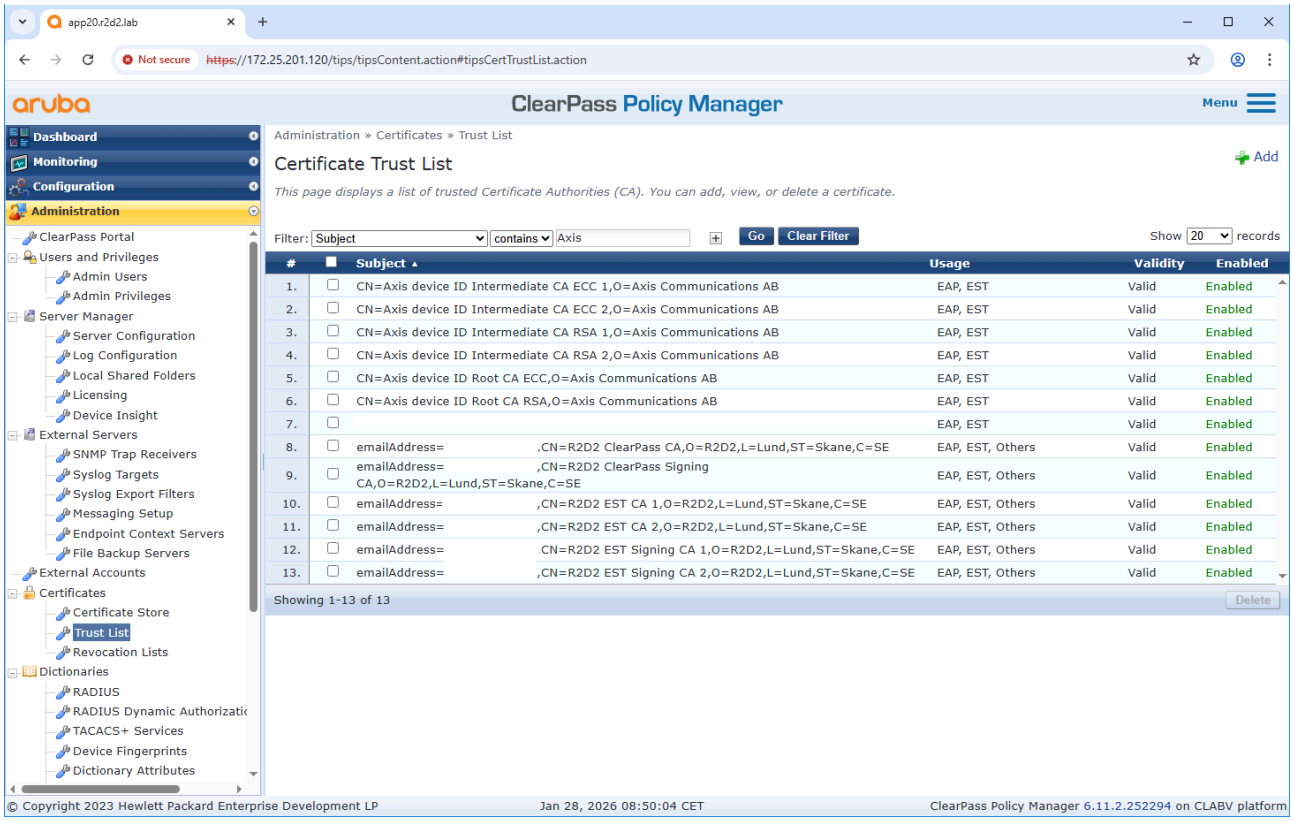
생성한 인증 기관에서 키 유형, 키 길이, 유효 기간 등 필요한 항목을 정의합니다.



생성한 인증 기관에 대해 EST Server 기능을 활성화합니다. EST Auth Method를 클라이언트 인증서 사용으로 구성합니다.

HPE Aruba ClearPass Policy Manager 구성

신뢰할 수 있는 인증서 저장소 구성

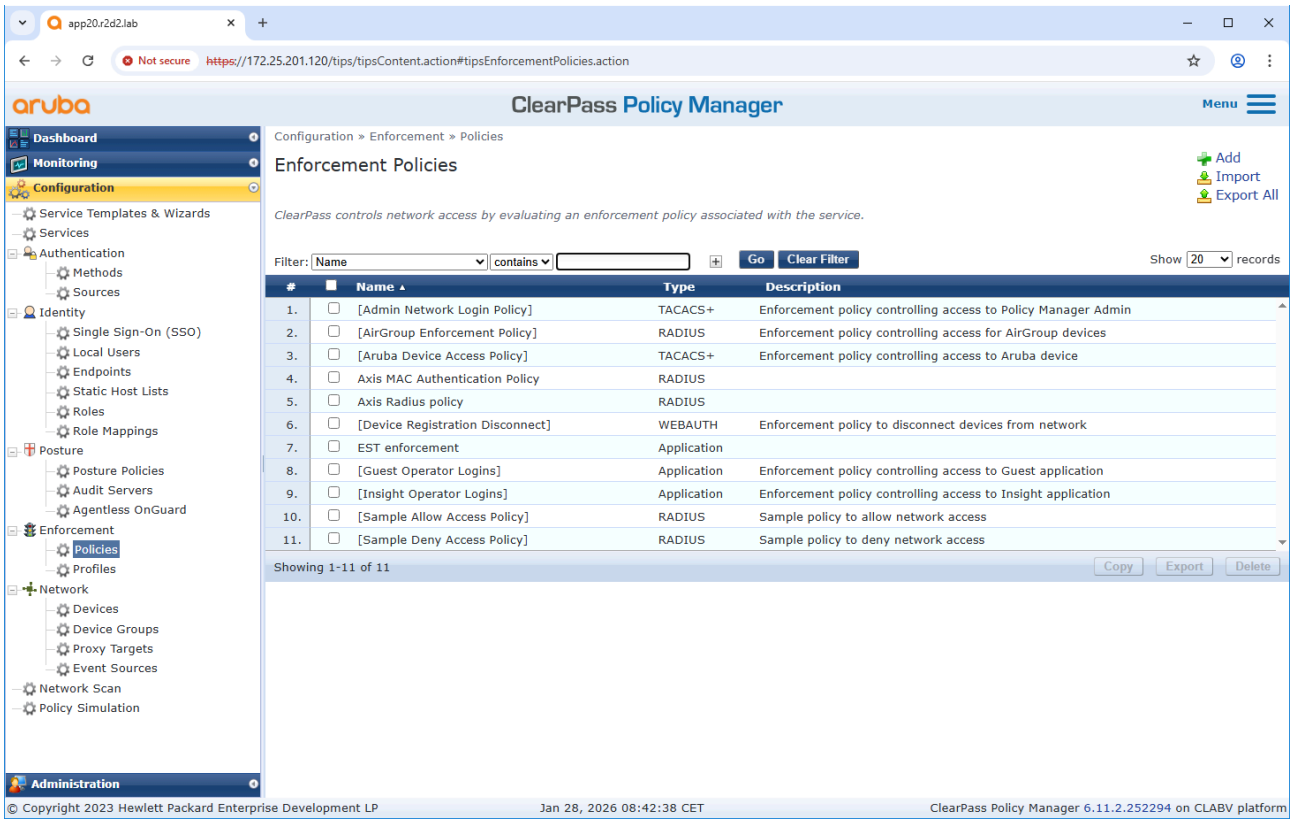


아직 수행하지 않았다면 ClearPass Policy Manager의 신뢰할 수 있는 인증서 저장소에 *Axis-specific IEEE 802.1AR certificates(Axis 전용 IEEE 802.1AR 인증서)*를 업로드합니다. EST 사용 항목이 추가되어

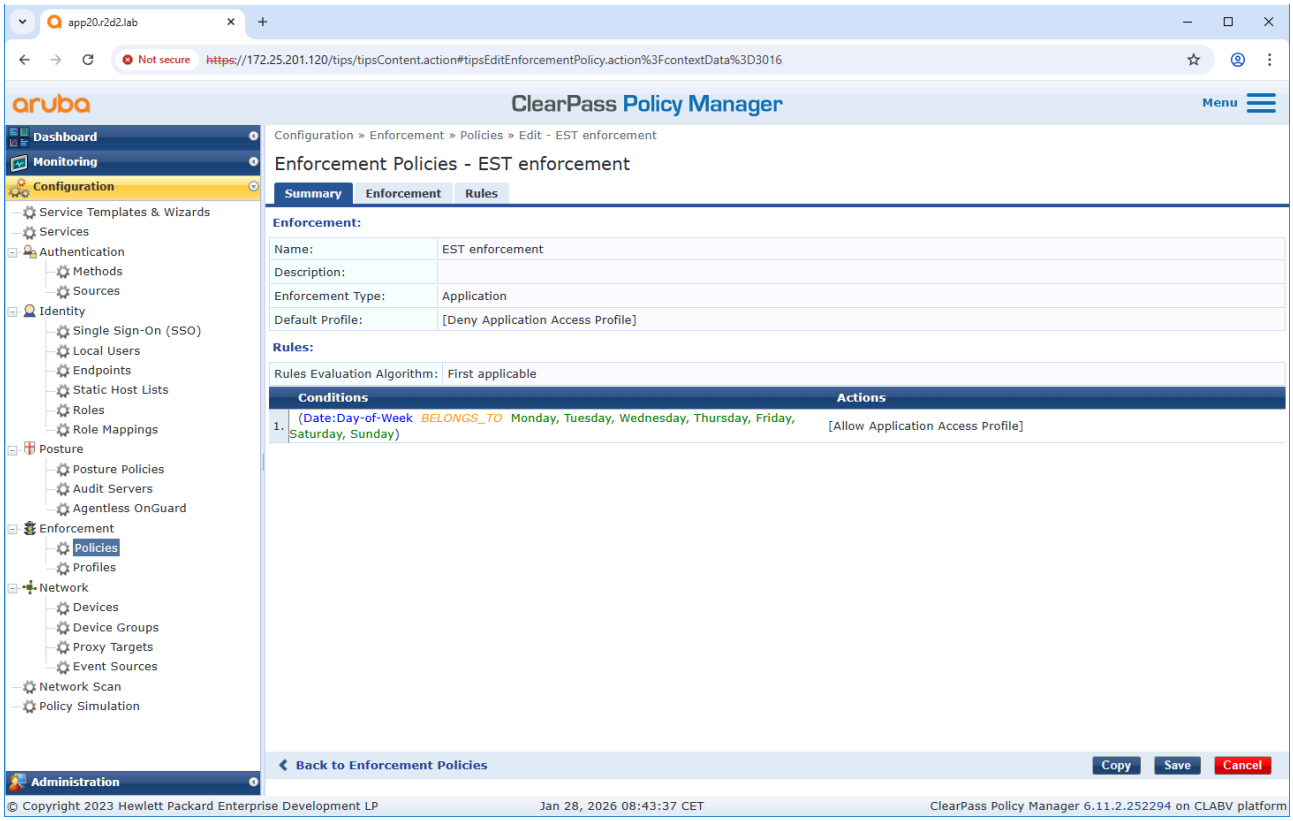
있는지 확인합니다. ClearPass Onboard에서 앞서 생성한 인증 기관에도 동일하게 적용되었는지 확인합니다.

정책 적용 정책 구성

Enforcement Profile(정책 적용 프로파일)을 사용하면 ClearPass Policy Manager가 EST 애플리케이션에 특정 정책 적용 규칙을 할당할 수 있습니다. 예를 들어, 새 인증서를 특정 엔드포인트에서만 등록하도록 하거나 특정 요일에만 등록되도록 제한할 수 있습니다.

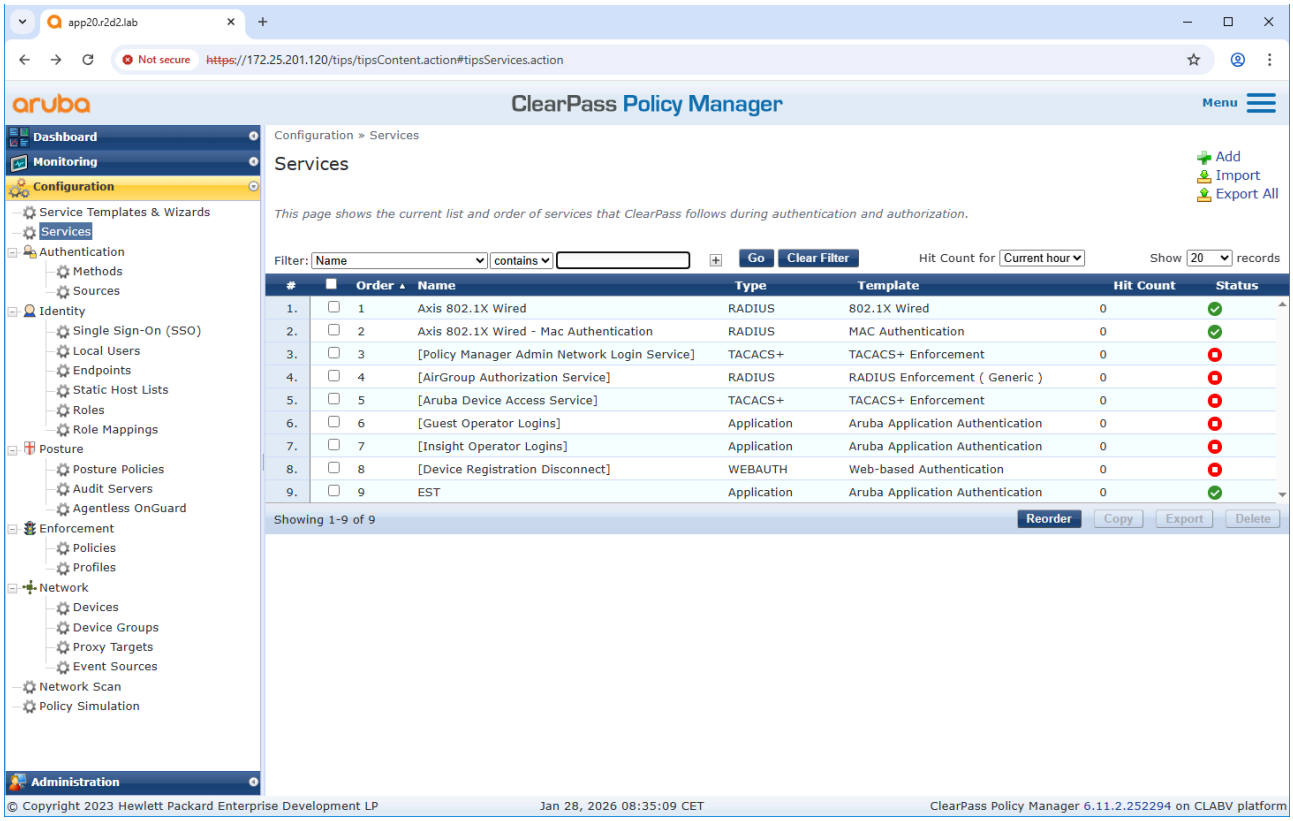


ClearPass Policy Manager의 정책 적용 정책 개요 화면입니다.

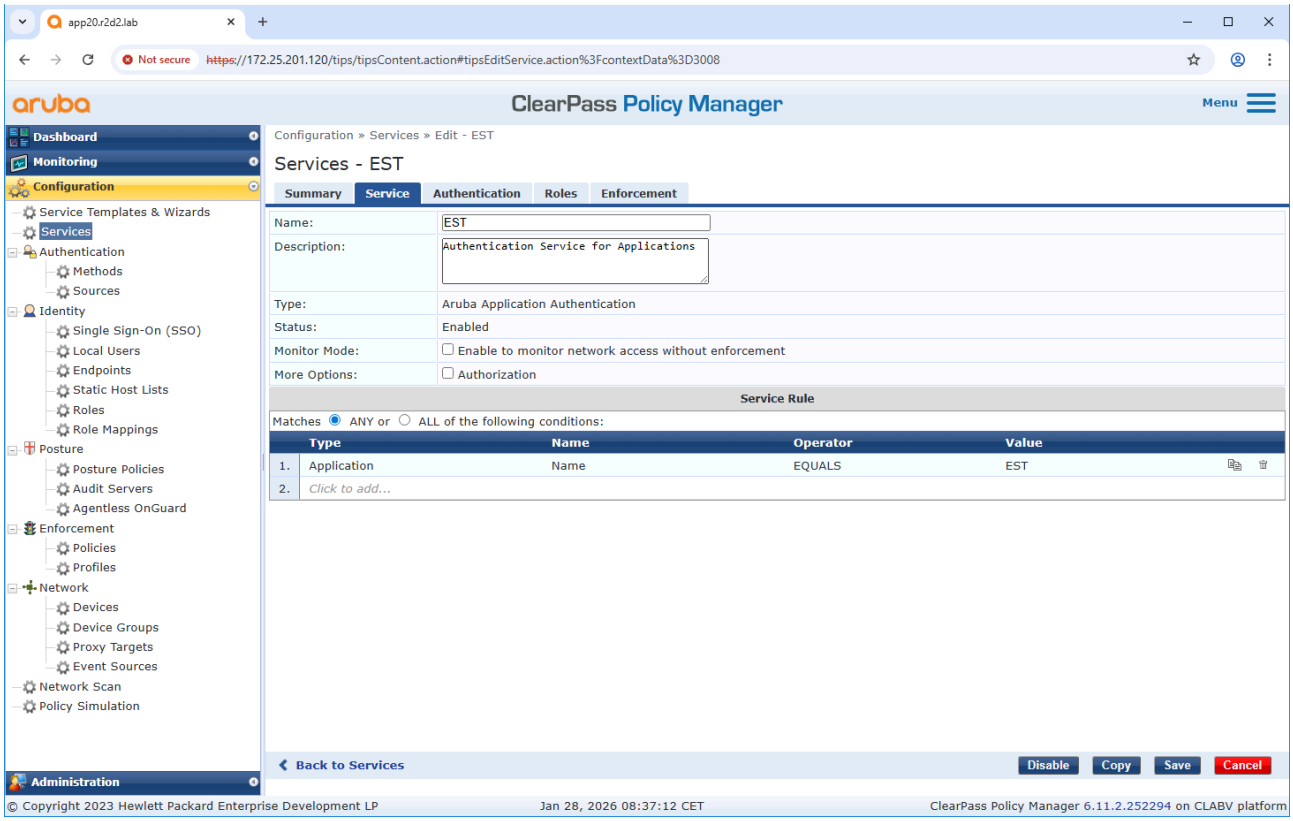


이 예시 정책에서는 EST 애플리케이션을 일주일 내내 허용합니다.

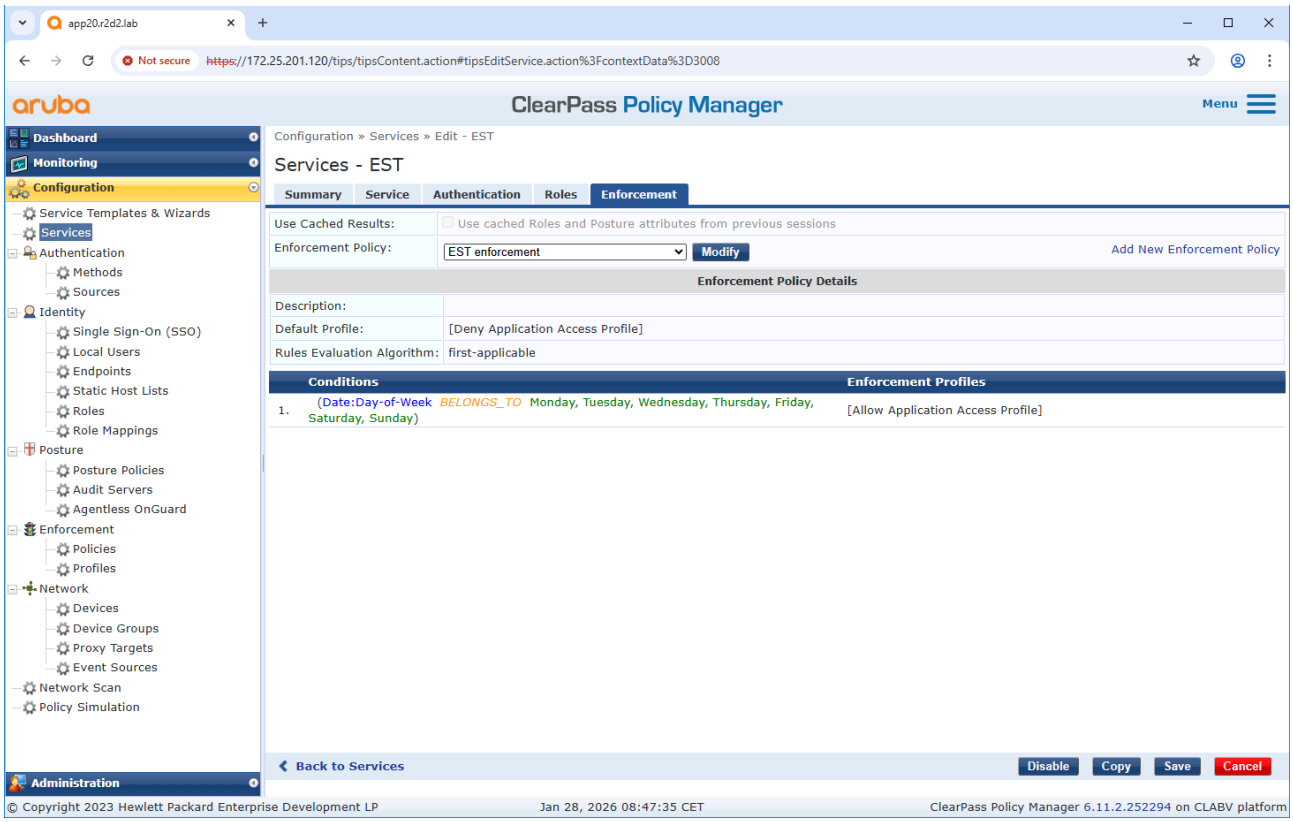
서비스 구성



전용 EST 서비스를 생성해야 합니다.



해당 서비스는 EST 애플리케이션에 맞게 구성해야 합니다.



앞서 생성한 EST 정책 적용 정책을 선택합니다.

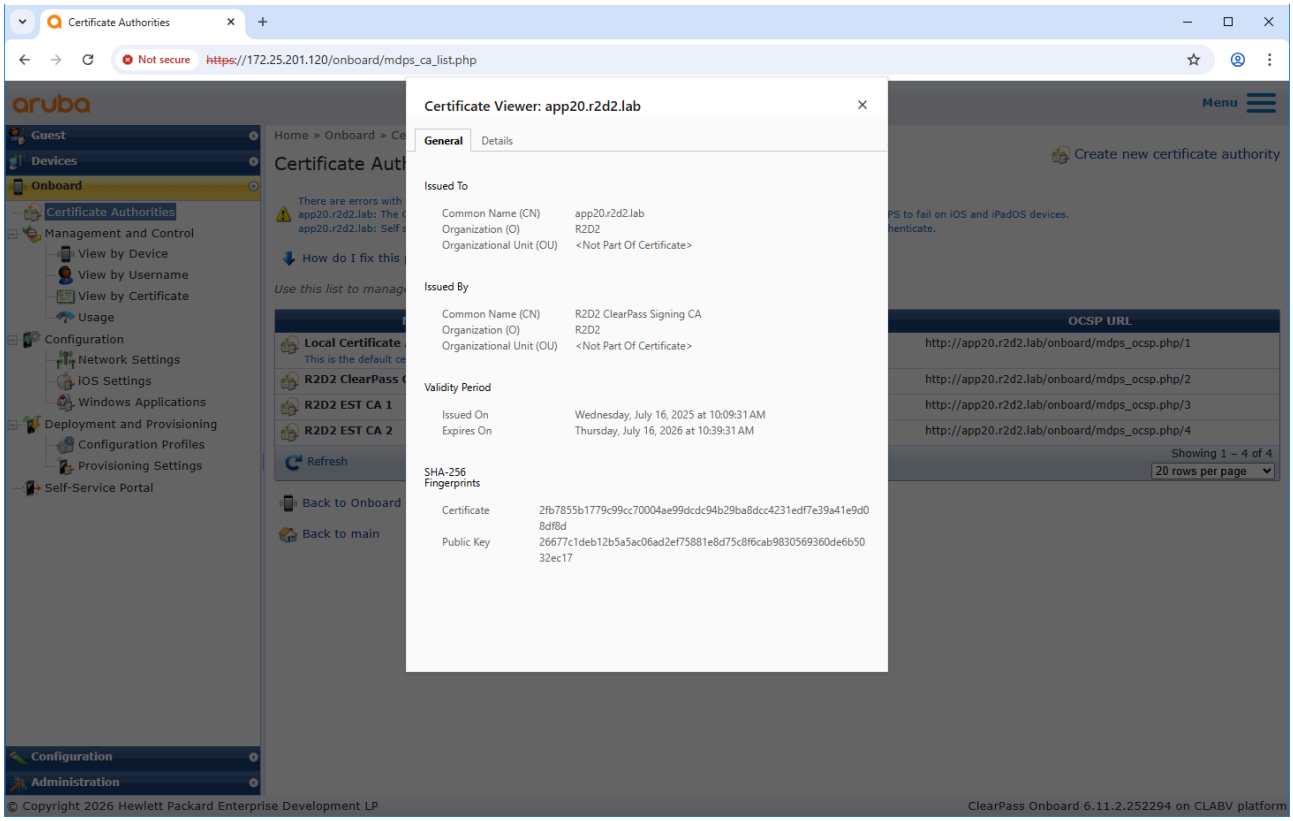
Axis 구성

Axis 장치의 구성은 두 단계로 진행됩니다.

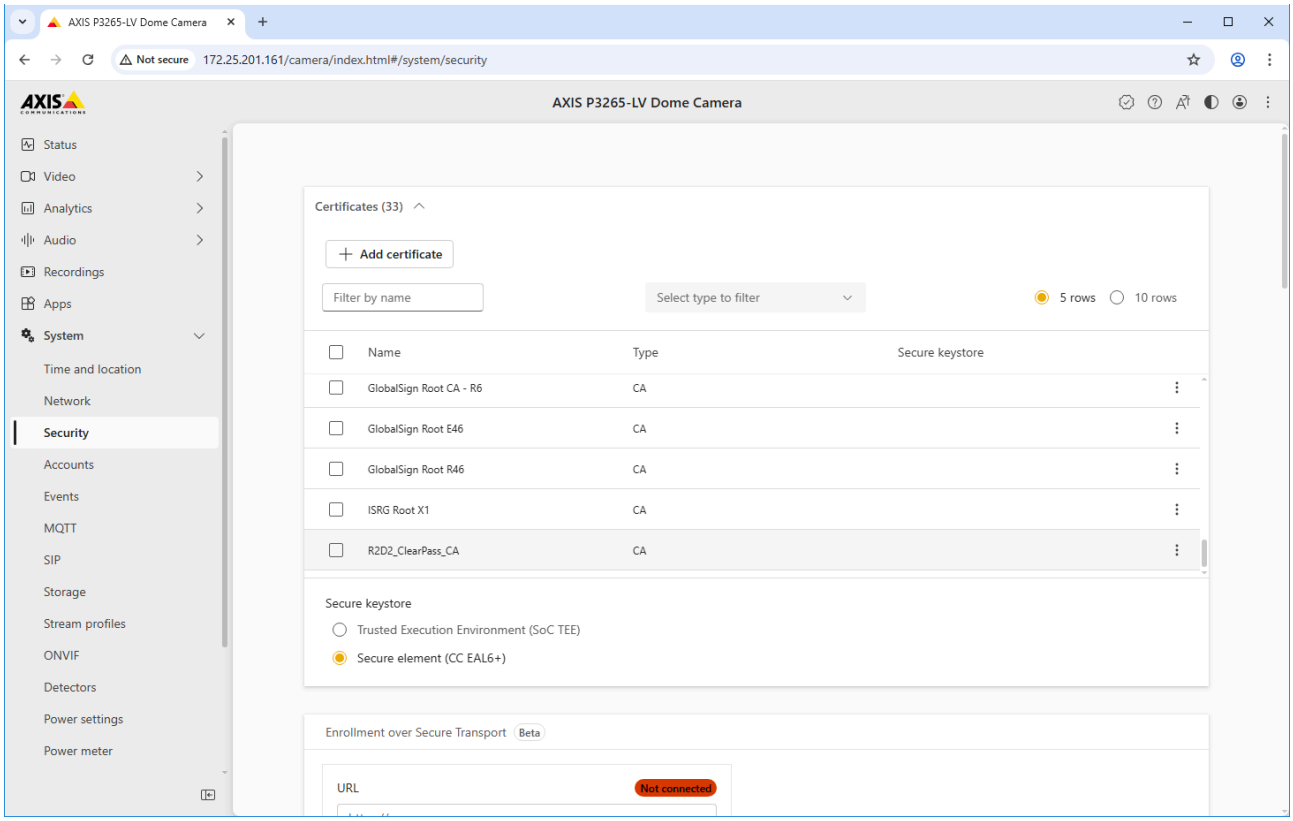
1. ClearPass Onboard HTTPS 엔드포인트와의 신뢰를 설정합니다.

2. Axis 장치에서 EST 클라이언트를 구성합니다.

신뢰할 수 있는 인증서 구성

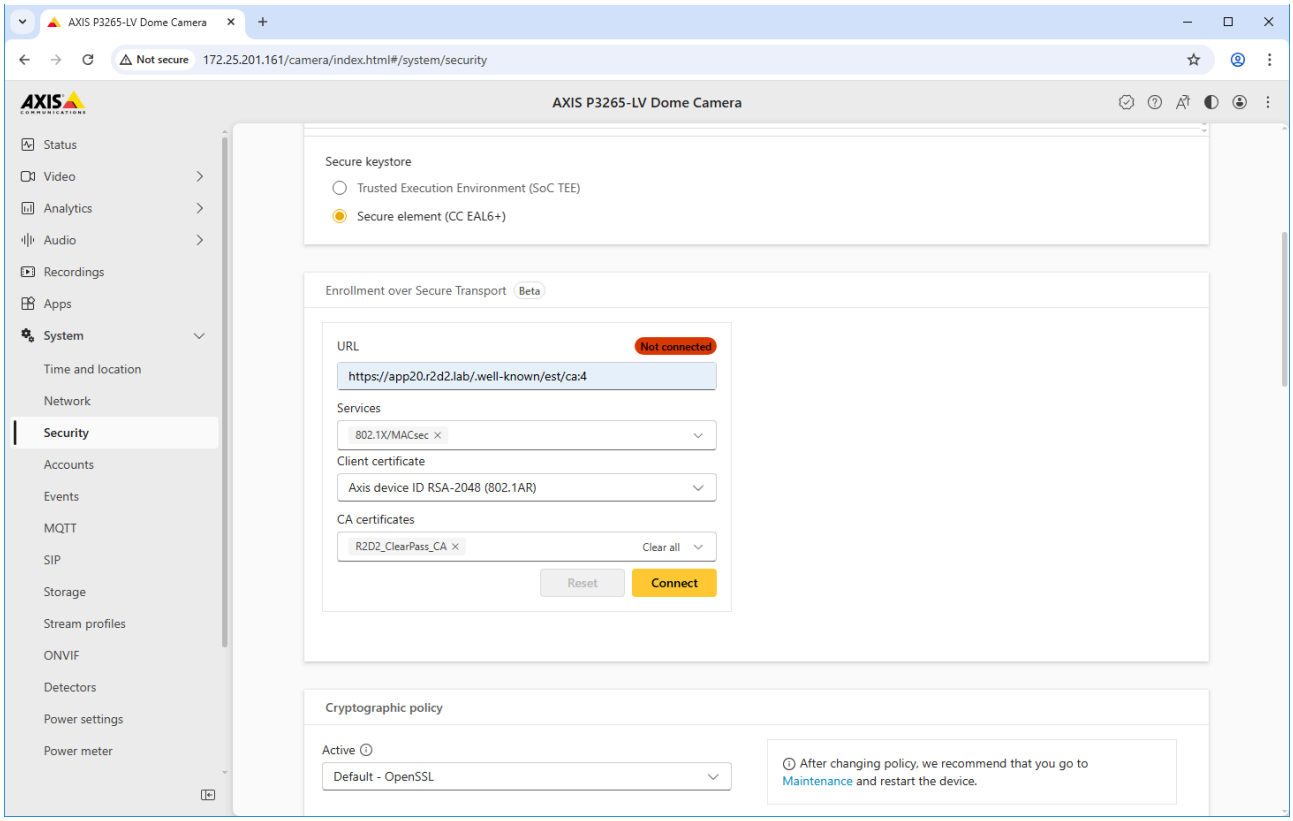


ClearPass Onboard HTTPS 엔드포인트의 인증서 체인을 확인합니다.

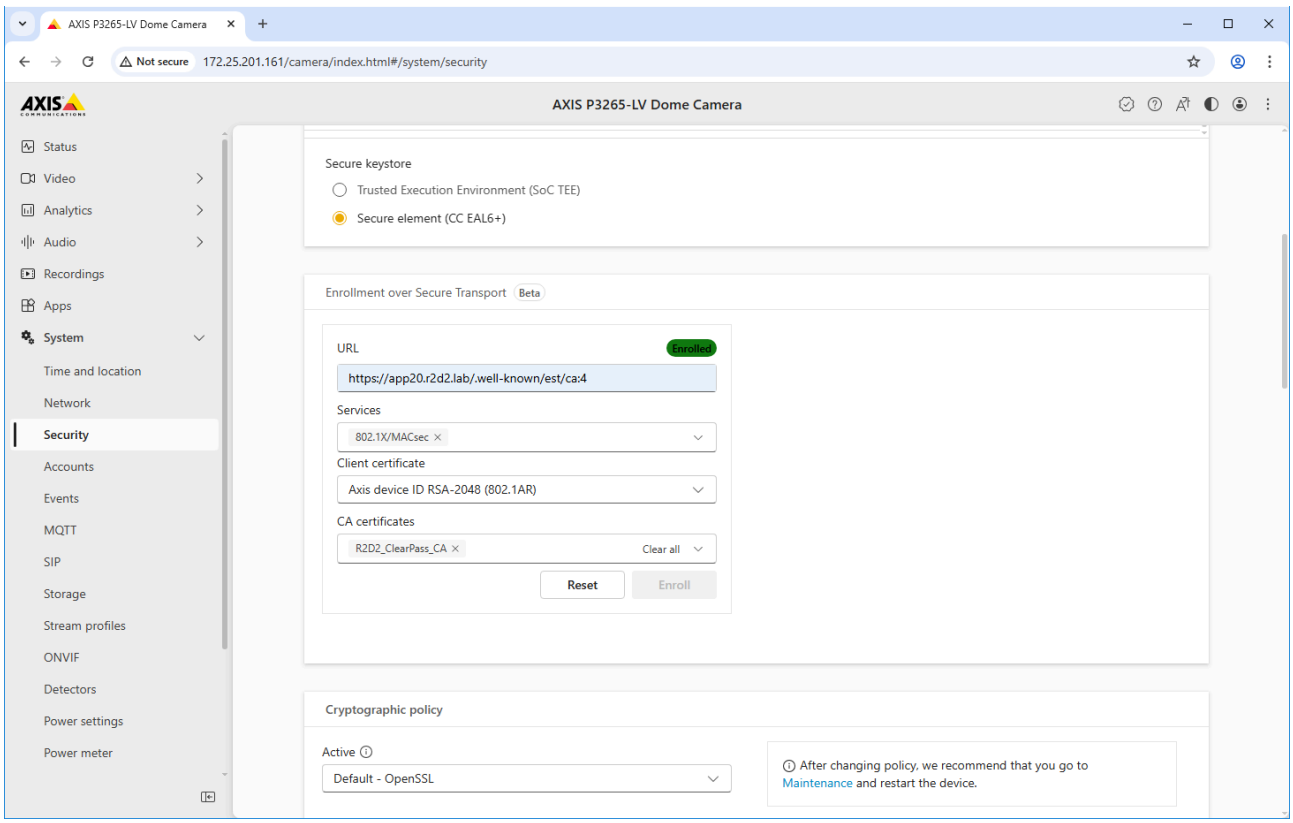


ClearPass Onboard HTTPS 엔드포인트의 CA 인증서를 Axis 장치에 업로드합니다.

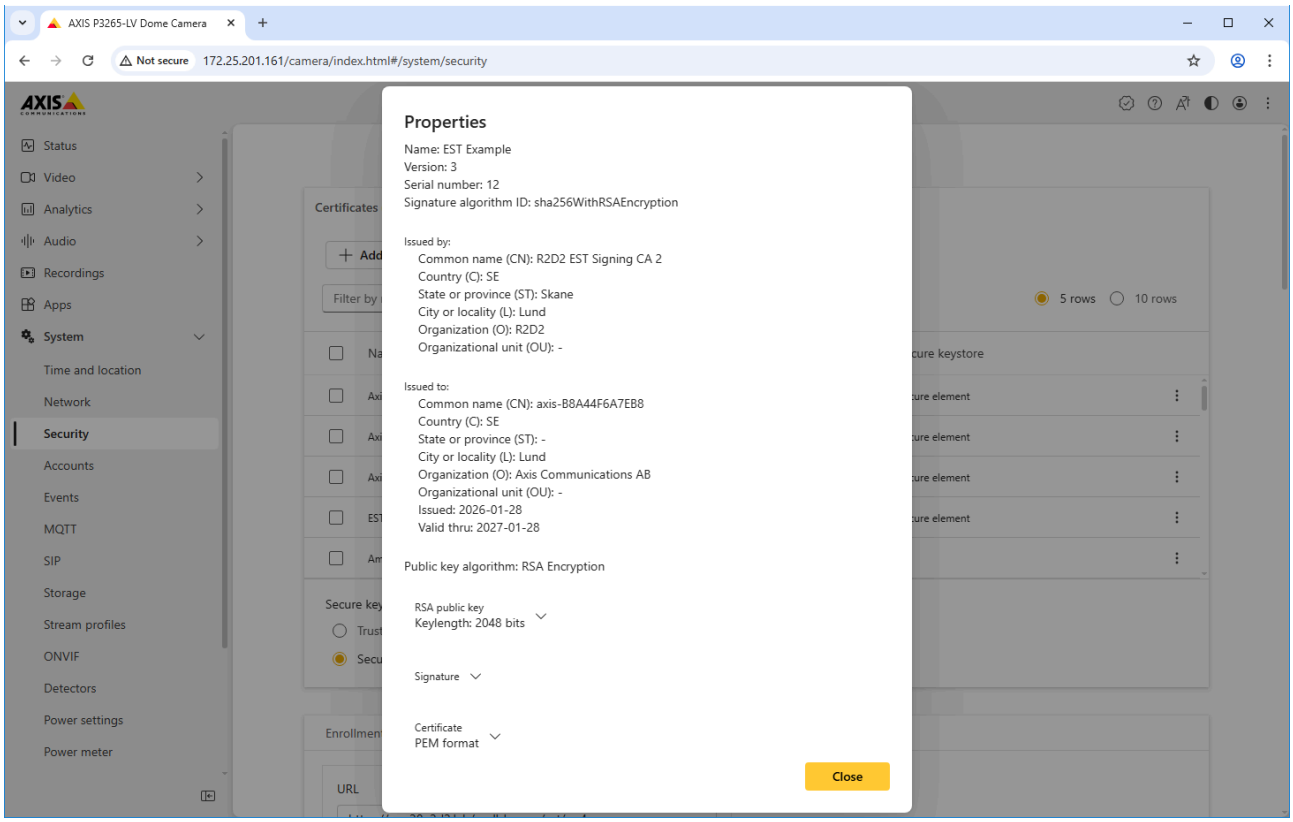
EST 클라이언트 구성



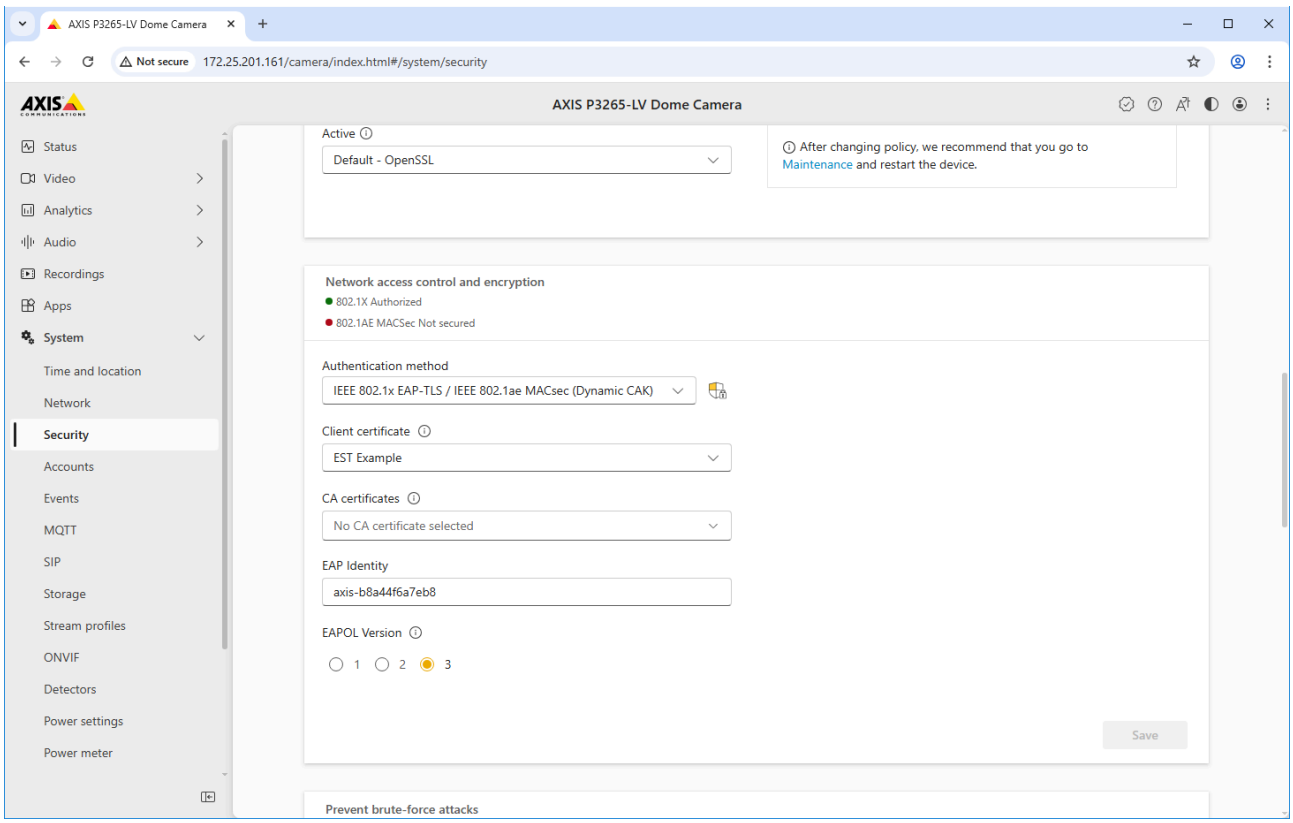
매개변수	값
URL	EST URL은 ClearPass Onboard에서 생성한 EST용 인증 기관에서 확인할 수 있습니다.
서비스	등록된 인증서로 자동 구성할 서비스를 선택합니다.
클라이언트 인증서	ClearPass Onboard EST 서버에 인증하기 위해 사용할 클라이언트 인증서를 선택합니다. ClearPass Policy Manager의 신뢰할 수 있는 인증서 저장소에 Axis 전용 IEEE 802.1AR 인증서 체인을 추가해 두었기 때문에, Axis Device ID가 있는 장치는 등록 시 자동으로 신뢰됩니다.
CA 인증서	Axis 장치가 해당 엔드포인트를 신뢰하도록 ClearPass Onboard HTTPS 엔드포인트의 CA 인증서를 선택합니다.



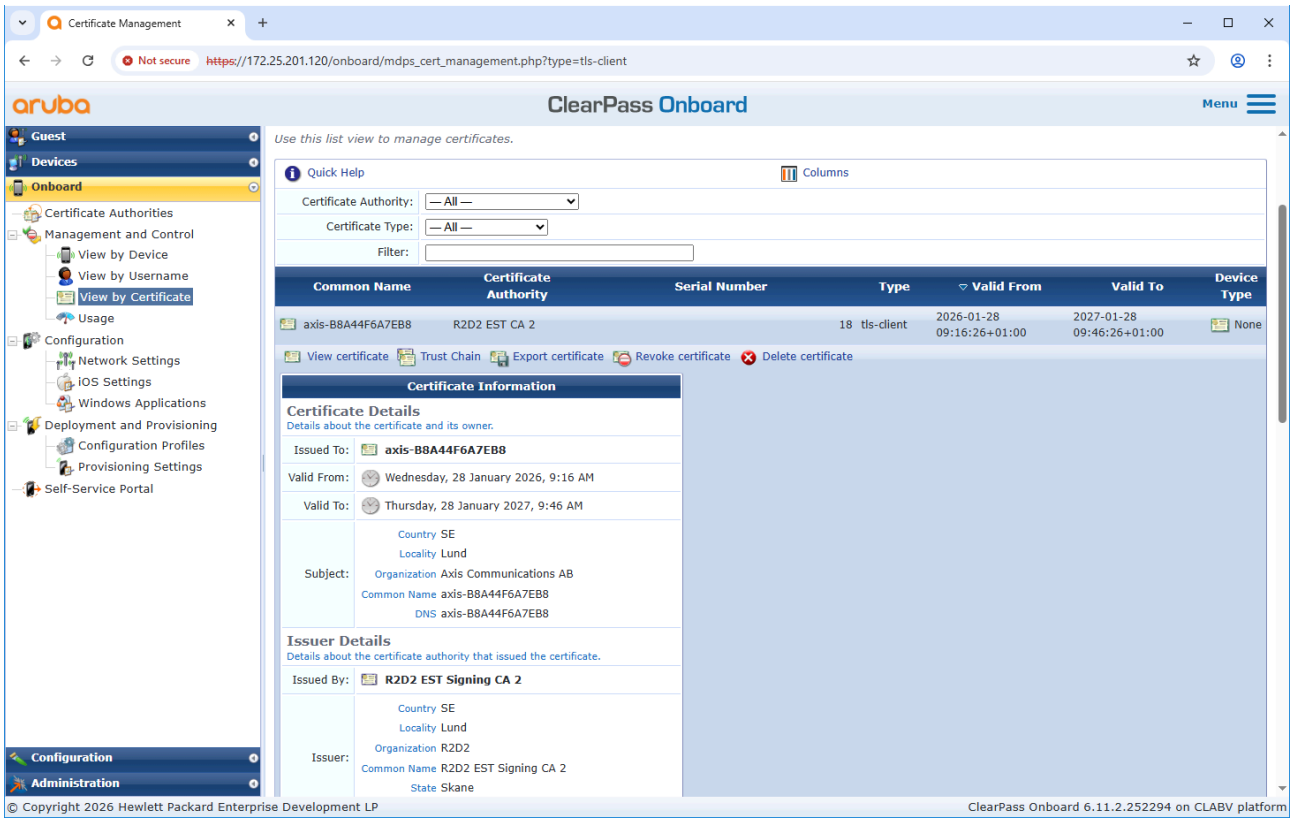
등록이 성공적으로 완료되었습니다.



Axis 장치에 EST로 등록된 인증서입니다.



등록된 인증서는 앞서 선택한 서비스에 자동으로 할당됩니다.



등록된 인증서는 ClearPass Onboard에서도 확인할 수 있습니다.

레거시 온보딩 - MAC 인증

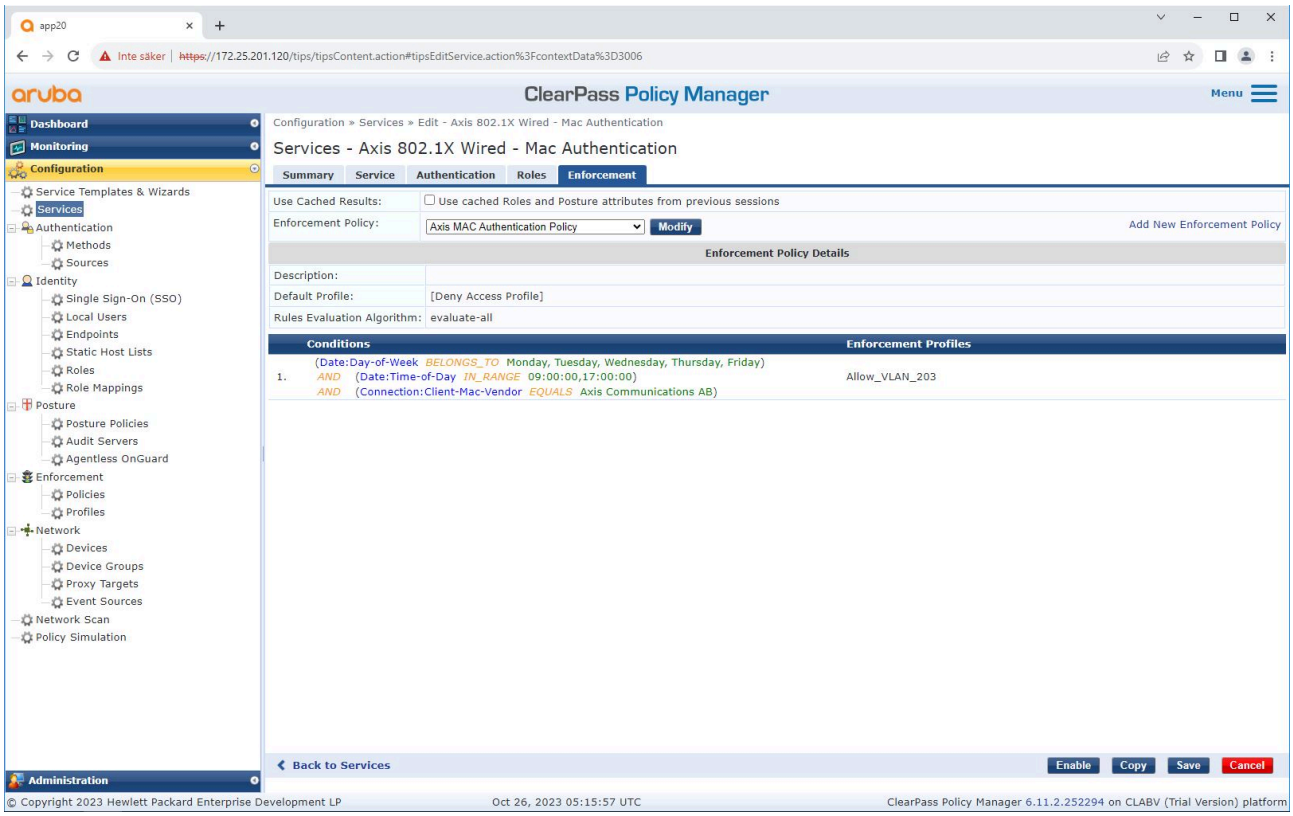
Axis 장치 ID 인증서 및 공장 기본 상태에서 활성화된 IEEE 802.1X를 사용한 IEEE 802.1AR 온보딩을 지원하지 않는 Axis 장치를 온보딩하기 위해 MAB(MAC Authentication Bypass)를 사용할 수 있습니다. 802.1X 온보딩이 실패하면 ClearPass Policy Manager는 Axis 장치의 MAC 주소를 확인하고 네트워크 액세스를 허용합니다.

MAB에는 액세스 스위치와 ClearPass Policy Manager 구성 준비가 모두 필요합니다. 온보딩을 위해 MAB를 허용하도록 Axis 장치에서 구성이 필요하지 않습니다.

HPE Aruba Networking ClearPass Policy Manager

정책 적용 정책

ClearPass Policy Manager의 정책 적용 정책 구성은 두 가지 정책 조건 예를 기반으로 Axis 장치에 HPE Aruba Networking 기반 네트워크에 대한 접근 권한을 부여할지 여부를 정의합니다.



네트워크 액세스를 거부

Axis 장치가 구성된 적용 정책을 충족하지 않으면 네트워크 액세스가 거부됩니다.

게스트 네트워크(VLAN 203)

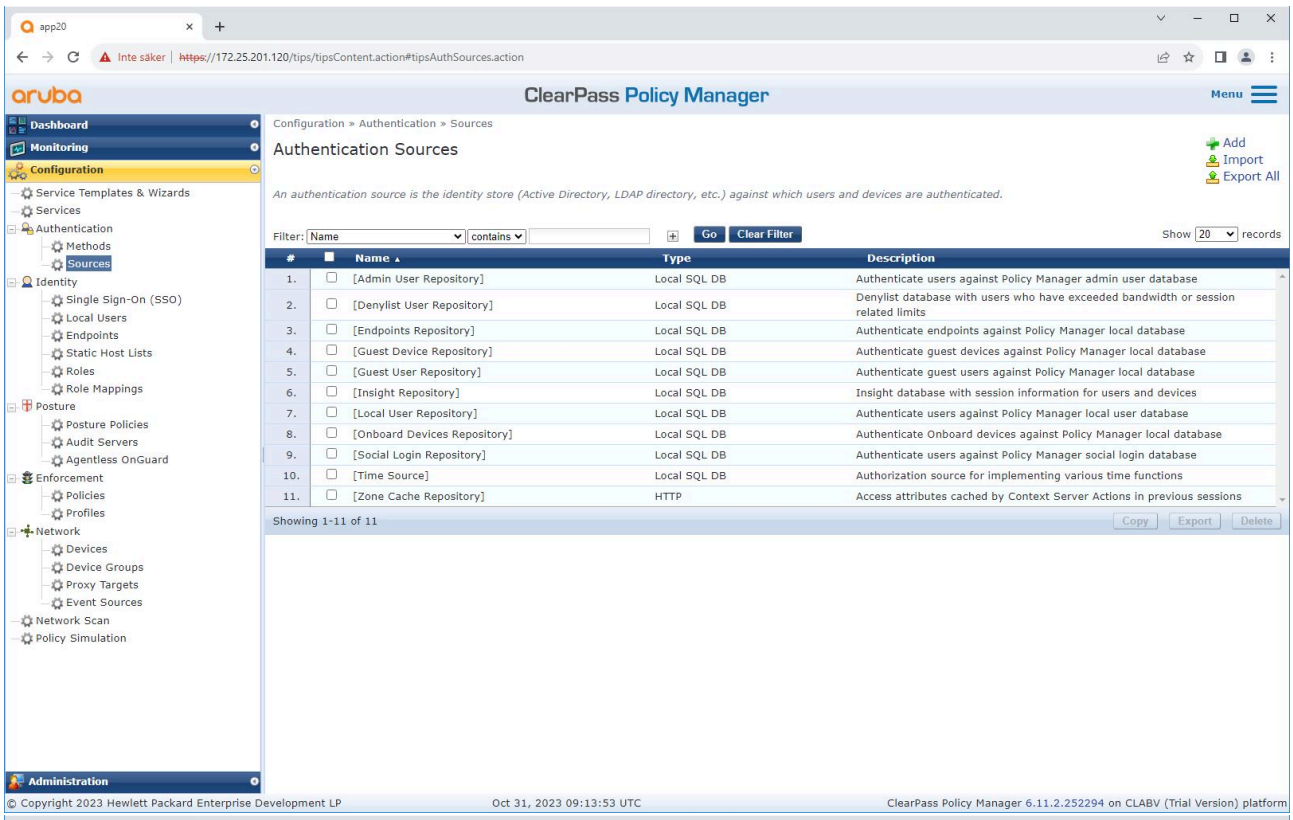
다음 조건이 충족되면 Axis 장치에는 제한적이고 격리된 네트워크에 대한 액세스 권한이 부여됩니다.

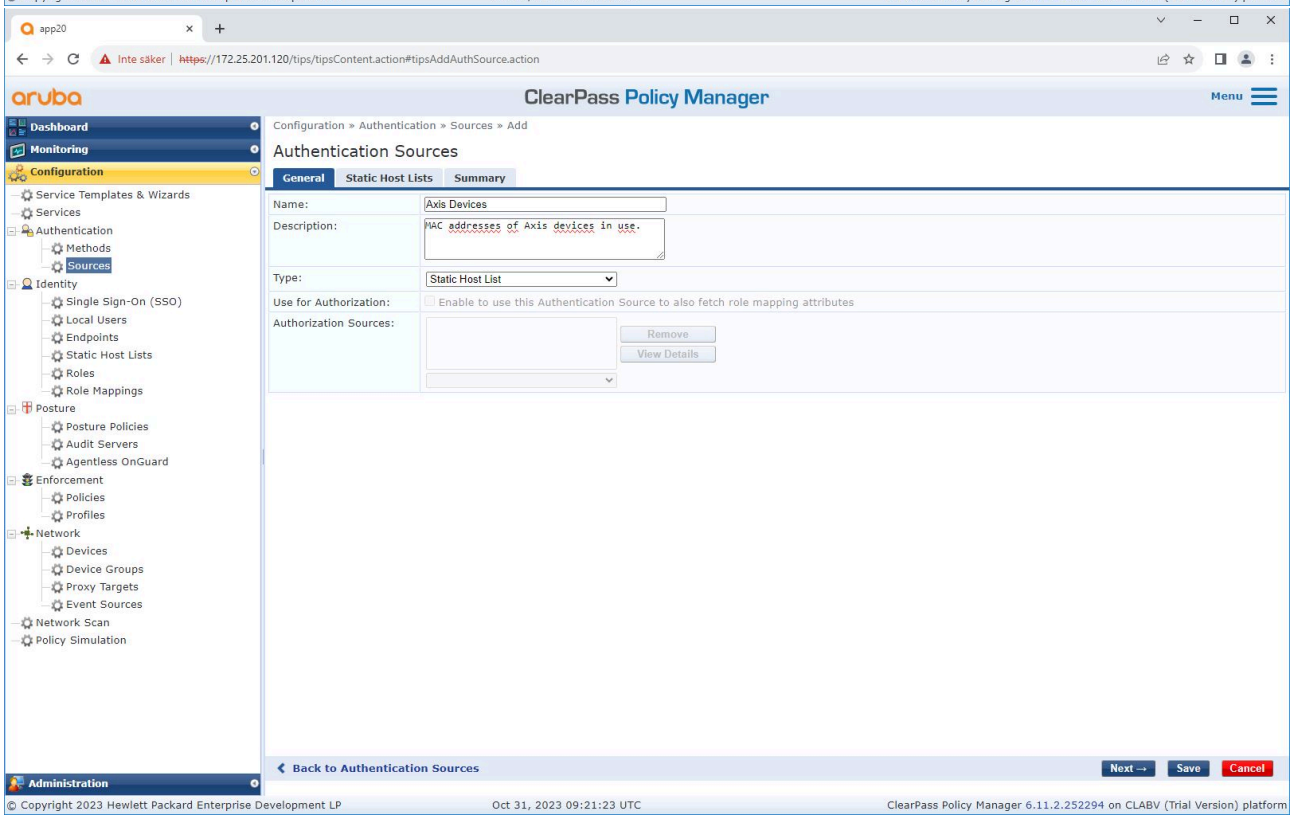
- 요일은 평일(월요일~금요일)입니다.
- 시간은 09:00에서 17:00 사이입니다.
- MAC 주소 공급업체가 Axis Communications와 일치합니다.

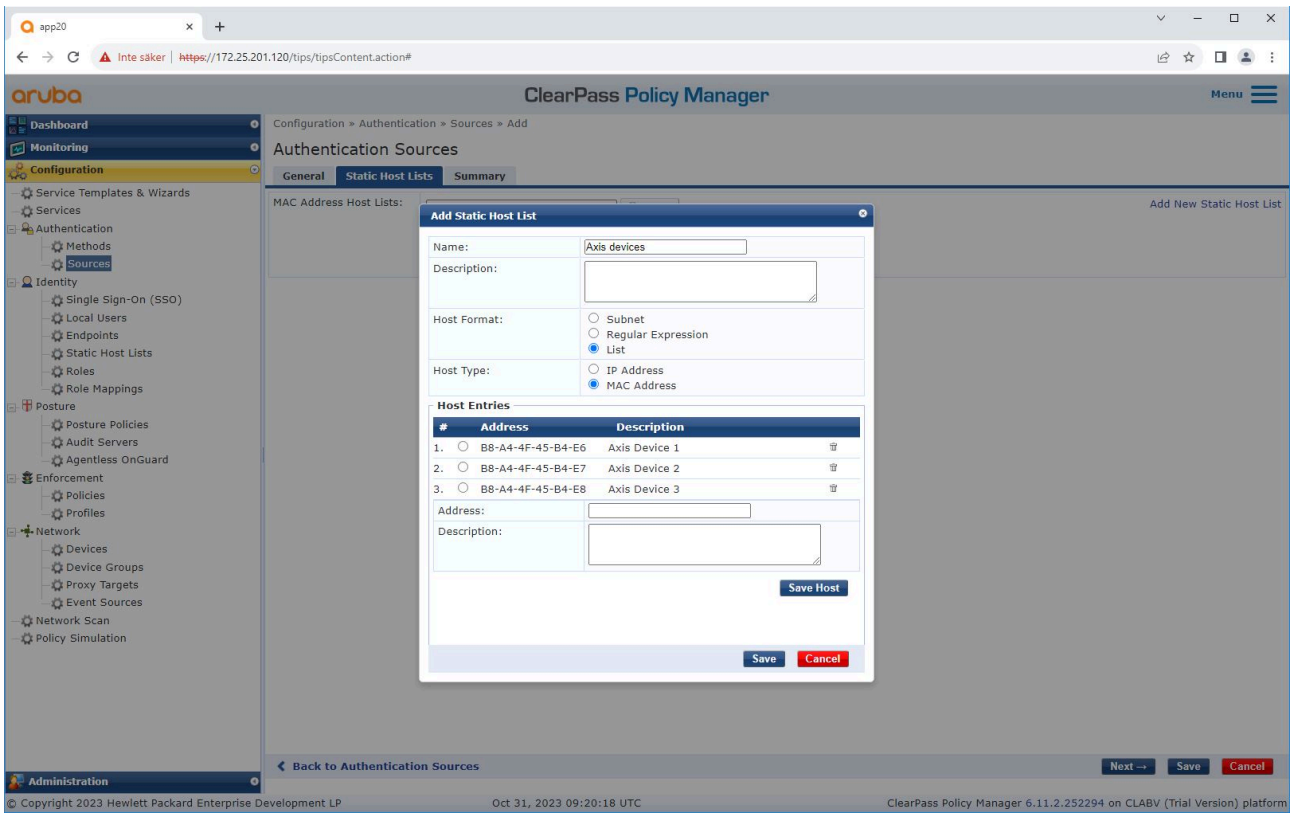
MAC 주소는 스푸핑이 가능하므로 일반 프로비저닝 네트워크에 대한 액세스는 허용되지 않습니다. 초기 온보딩에만 MAB를 사용한 다음 장치를 수동으로 추가 검사하는 것이 좋습니다.

소스 구성

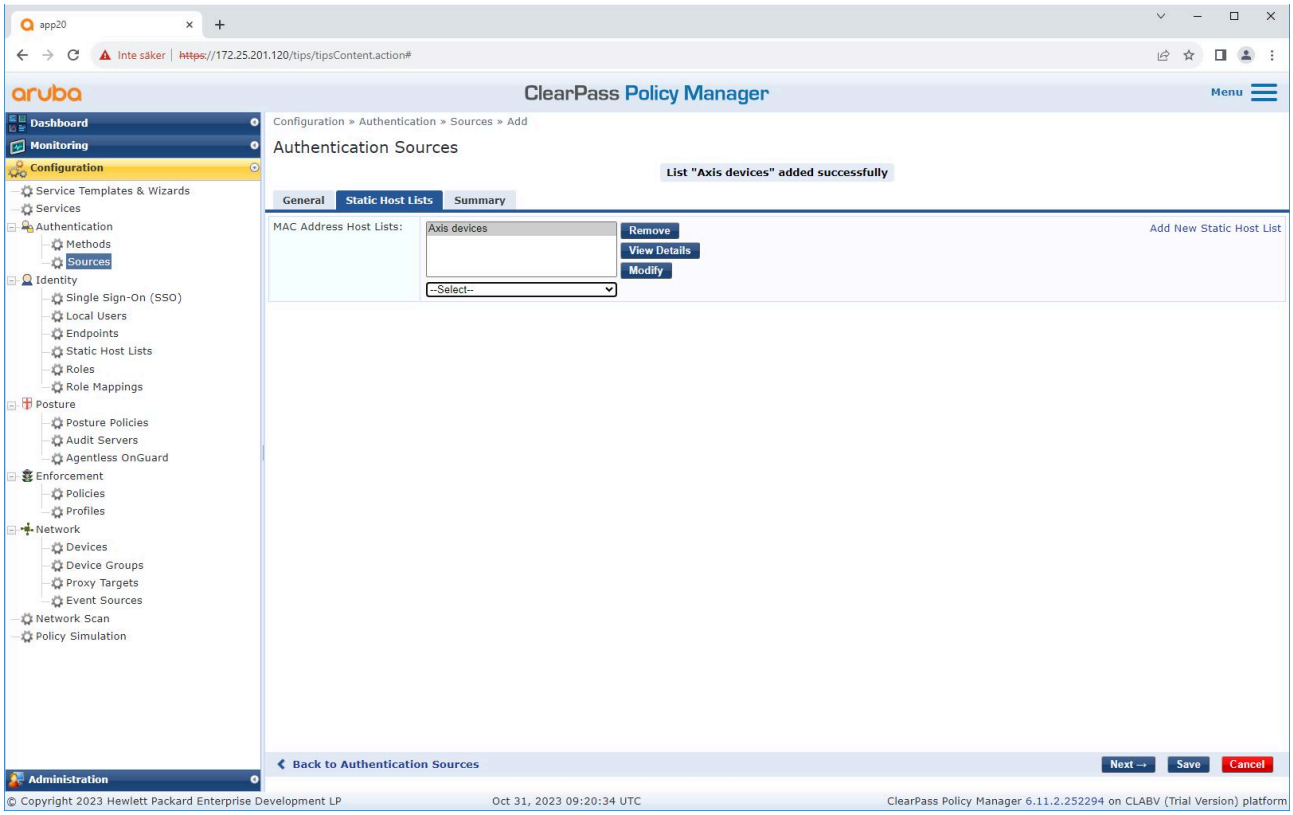
Sources(소스) 페이지에서는 수동으로 가져온 MAC 주소만 허용하는 새 인증 소스가 생성됩니다.


app20
Inte säker | https://172.25.201.120/tips/tipsContent.action#tipsAuthSources.action
aruba
ClearPass Policy Manager
Menu
Dashboard
Monitoring
Configuration
Service Templates & Wizards
Services
Authentication
Methods
Sources
Identity
Single Sign-On (SSO)
Local Users
Endpoints
Static Host Lists
Roles
Role Mappings
Posture
Posture Policies
Audit Servers
Agentless OnGuard
Enforcement
Policies
Profiles
Network
Devices
Device Groups
Proxy Targets
Event Sources
Network Scan
Policy Simulation
Administration
Configuration » Authentication » Sources
Authentication Sources
Add
Import
Export All
An authentication source is the identity store (Active Directory, LDAP directory, etc.) against which users and devices are authenticated.
Filter: Name contains Go Clear Filter
Show 20 records
Name Type Description
1. [Admin User Repository] Local SQL DB Authenticate users against Policy Manager admin user database
2. [Denylist User Repository] Local SQL DB Denylist database with users who have exceeded bandwidth or session related limits
3. [Endpoints Repository] Local SQL DB Authenticate endpoints against Policy Manager local database
4. [Guest Device Repository] Local SQL DB Authenticate guest devices against Policy Manager local database
5. [Guest User Repository] Local SQL DB Authenticate guest users against Policy Manager local database
6. [Insight Repository] Local SQL DB Insight database with session information for users and devices
7. [Local User Repository] Local SQL DB Authenticate users against Policy Manager local user database
8. [Onboard Devices Repository] Local SQL DB Authenticate Onboard devices against Policy Manager local database
9. [Social Login Repository] Local SQL DB Authenticate users against Policy Manager social login database
10. [Time Source] Local SQL DB Authorization source for implementing various time functions
11. [Zone Cache Repository] HTTP Access attributes cached by Context Server Actions in previous sessions
Showing 1-11 of 11
Copy Export Delete
© Copyright 2023 Hewlett Packard Enterprise Development LP
Oct 31, 2023 09:13:53 UTC
ClearPass Policy Manager 6.11.2.252294 on CLABV (Trial Version) platform


app20
Inte säker | https://172.25.201.120/tips/tipsContent.action#tipsAddAuthSource.action
aruba
ClearPass Policy Manager
Menu
Dashboard
Monitoring
Configuration
Service Templates & Wizards
Services
Authentication
Methods
Sources
Identity
Single Sign-On (SSO)
Local Users
Endpoints
Static Host Lists
Roles
Role Mappings
Posture
Posture Policies
Audit Servers
Agentless OnGuard
Enforcement
Policies
Profiles
Network
Devices
Device Groups
Proxy Targets
Event Sources
Network Scan
Policy Simulation
Administration
Configuration » Authentication » Sources » Add
Authentication Sources
General Static Host Lists Summary
Name: Axis Devices
Description: MAC addresses of Axis devices in use.
Type: Static Host List
Use for Authorization: Enable to use this Authentication Source to also fetch role mapping attributes
Authorization Sources:
Remove
View Details
Back to Authentication Sources
Next → Save Cancel
© Copyright 2023 Hewlett Packard Enterprise Development LP
Oct 31, 2023 09:21:23 UTC
ClearPass Policy Manager 6.11.2.252294 on CLABV (Trial Version) platform

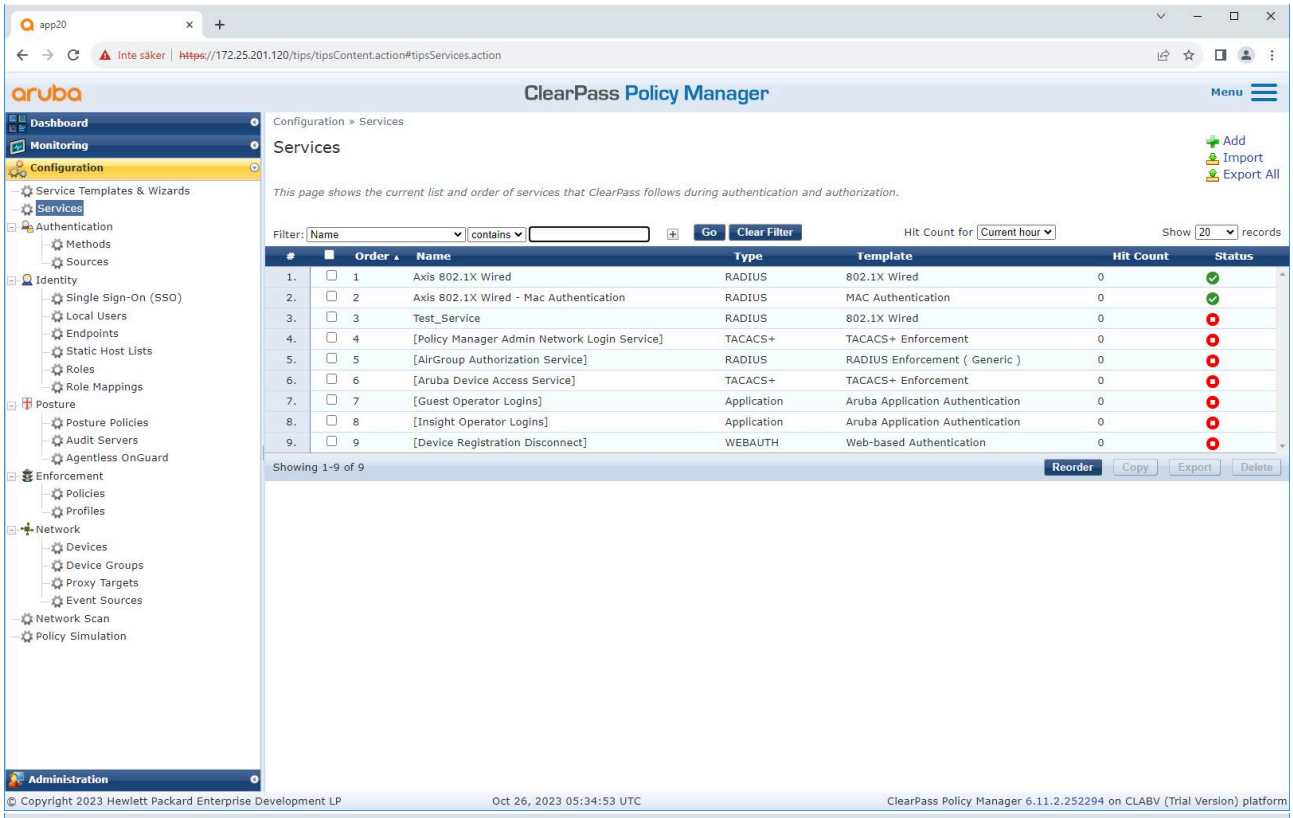


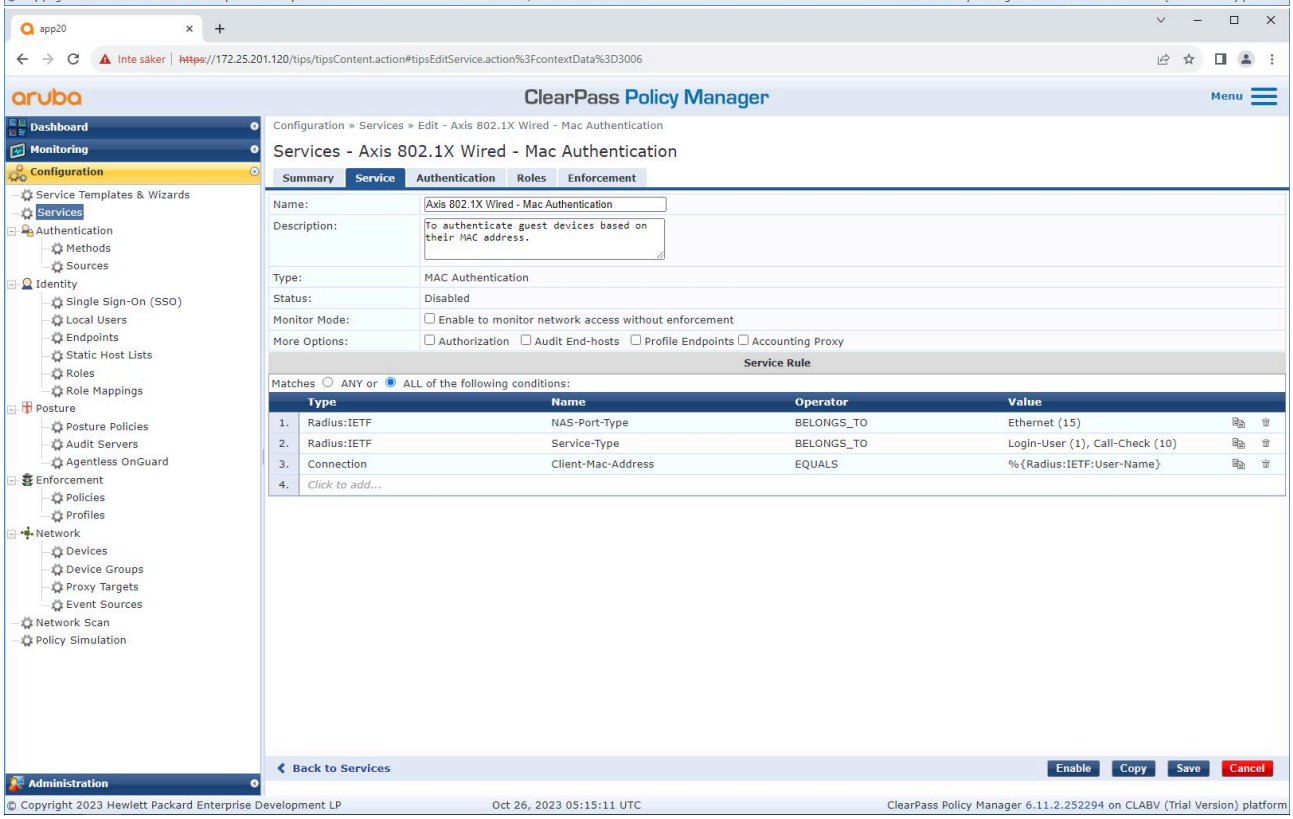
Axis MAC 주소를 포함하는 정적 호스트 목록이 생성됩니다.



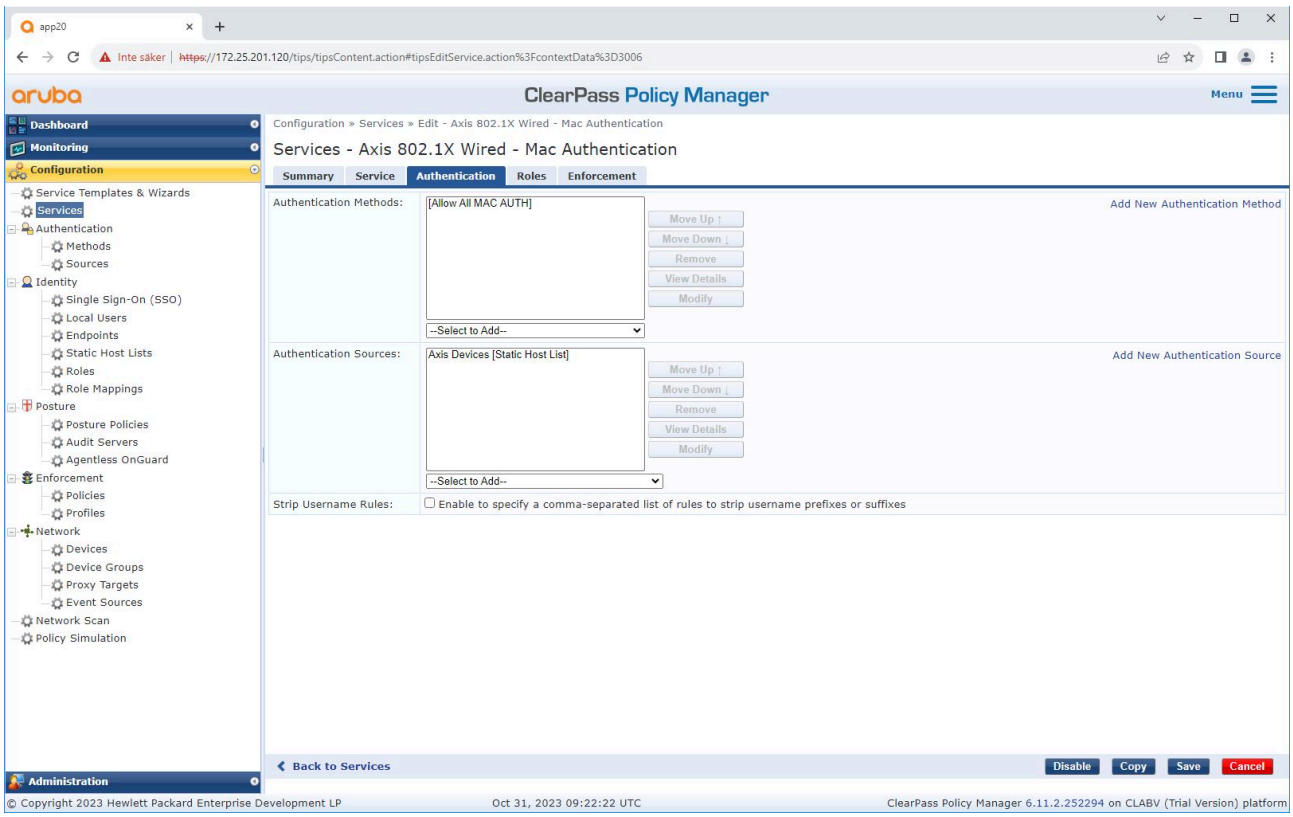
서비스 구성

Services(서비스) 페이지에서 구성 단계는 HPE Aruba Networking 네트워크에서 Axis 장치의 인증 및 권한 부여를 처리하는 단일 서비스로 결합됩니다.





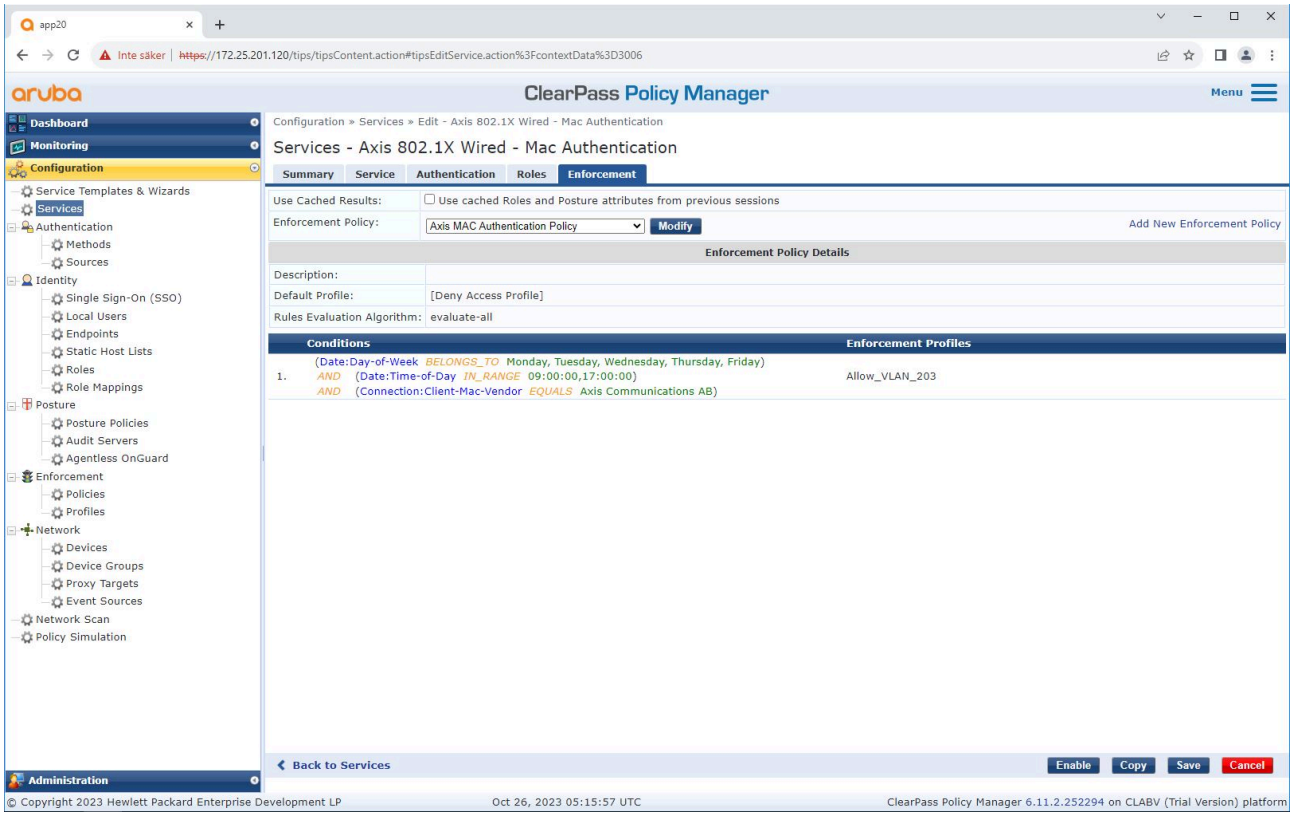
MAB를 연결 방법으로 정의하는 전용 Axis 서비스가 생성됩니다.



사전 구성된 MAC 인증 방법이 서비스에 대해 구성됩니다. 또한 Axis MAC 주소 목록을 포함하는 (이전에 생성된) 인증 소스가 선택됩니다.

Axis Communications는 다음 MAC 주소 OUI를 사용합니다.

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



마지막 단계에서 이전에 생성된 적용 정책이 서비스에 대해 구성됩니다.

HPE Aruba Networking 액세스 스위치

*HPE Aruba Networking 액세스 스위치, on page 15*에 설명된 보안 온보딩 구성 외에도 MAB를 허용하기 위한 HPE Aruba Networking 액세스 스위치의 예시 포트 구성은 아래를 참조하십시오.

```
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_ko

2026-02 (M8.3)