

Secure integration of Axis devices into Aruba networks

사용자 설명서

Secure integration of Axis devices into Aruba networks

목차

소개	3
보안 온보딩 - IEEE 802.1AR/802.1X	4
초기 인증	4
프로비저닝	4
생산 네트워크	4
구성 HPE Aruba	5
Axis 구성	16
안전한 네트워크 운영 - IEEE 802.1AE MACsec	19
Aruba ClearPass Policy Manager	19
Aruba 액세스 스위치	24
레거시 온보딩 - MAC 인증	25
Aruba ClearPass Policy Manager	25
Aruba 액세스 스위치	33

Secure integration of Axis devices into Aruba networks

소개

소개

이 통합 가이드의 목표는 Aruba 네트워크에서 Axis 장치를 온보딩하고 작동하는 방법에 대한 모범 사례 구성을 개략적으로 설명하는 것입니다. 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. Aruba 네트워크 장비 및 애플리케이션과 결합된 Axis 장치 관리 애플리케이션을 사용할 때 불필요한 시스템 복잡성을 제거할 수 있습니다. 다음은 Axis 장치 및 소프트웨어를 Aruba 네트워크 인프라와 결합할 때 얻을 수 있는 몇 가지 이점입니다.

- 장치 준비 네트워크를 제거하여 시스템 복잡성을 최소화할 수 있습니다.
- 자동화된 온보딩 프로세스와 장치 관리를 추가하여 비용을 절감할 수 있습니다.
- Axis 장치에서 제공하는 제로 터치 네트워크 보안 제어를 활용할 수 있습니다.
- Aruba와 Axis 전문 지식을 적용하여 전반적인 네트워크 보안을 강화할 수 있습니다.

구성을 시작하기 전에 Axis 장치의 무결성을 안전하게 확인할 수 있도록 네트워크 인프라를 준비해야 합니다. 이를 통해 온보딩 프로세스 전반에 걸쳐 논리 네트워크 간의 원활한 소프트웨어 정의 전환을 할 수 있습니다. 구성을 수행하기 전에 다음 영역에 대한 지식이 필요합니다.

- Aruba 액세스 스위치 및 Aruba ClearPass Policy Manager를 포함한 Aruba 엔터프라이즈 네트워크 IT 인프라 관리.
- 최신 네트워크 접근 제어 기술 및 네트워크 보안 정책에 대한 전문 지식.
- Axis 제품에 대한 기본 지식을 추천하지만, 가이드 전반에 걸쳐 제공합니다.

Secure integration of Axis devices into Aruba networks

보안 온보딩 - IEEE 802.1AR/802.1X

보안 온보딩 - IEEE 802.1AR/802.1X

초기 인증

Axis Edge Vault 지원 Axis 장치를 연결하여 Aruba 네트워크에 대해 장치를 인증합니다. 장치는 IEEE 802.1X 네트워크 접근 제어를 통해 IEEE 802.1AR Axis 장치 ID 인증서를 사용하여 자체 인증을 수행합니다.

네트워크에 대한 액세스 권한을 부여하기 위해 Aruba ClearPass 정책 관리자는 다른 장치별 지문과 함께 Axis 장치 ID를 확인합니다. MAC 주소 및 실행 중인 펌웨어와 같은 정보는 정책 기반 결정을 내리는 데 사용됩니다.

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

Axis 장치는 IEEE 802.1AR의 호환 Axis 장치 ID 인증서를 사용하여 Aruba 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 Aruba 네트워크는 Axis 장치를 Axis Device Manager가 설치된 프로비저닝 네트워크(VLAN201)로 이동합니다. Axis Device Manager를 통해 장치 구성, 보안 강화 및 펌웨어 업데이트를 수행할 수 있습니다. 장치 프로비저닝을 완료하기 위해 새로운 고객별 프로덕션 등급 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

생산 네트워크

새로운 IEEE 802.1X 인증서로 Axis 장치를 프로비저닝하면 새로운 인증 시도가 트리거됩니다. Aruba ClearPass 정책 관리자는 새 인증서를 확인하고 Axis 장치를 프로덕션 네트워크로 이동할지 여부를 결정합니다.

장치 구성 후 Axis 장치는 프로비저닝 네트워크를 떠나 Aruba 네트워크에 대해 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 프로덕션 네트워크(VLAN 202)로 이동됩니다. 해당 네트워크에서 VMS(영상 관리 시스템)가 Axis 장치에 연결되어 작동을 시작합니다.

Secure integration of Axis devices into Aruba networks

보안 온보딩 - IEEE 802.1AR/802.1X

Axis 장치에는 프로덕션 네트워크에 대한 액세스 권한이 부여됩니다.

- 1 액세스 스위치
- 2 생산 네트워크
- 3 ClearPass Policy Manager
- 4 영상 관리 시스템

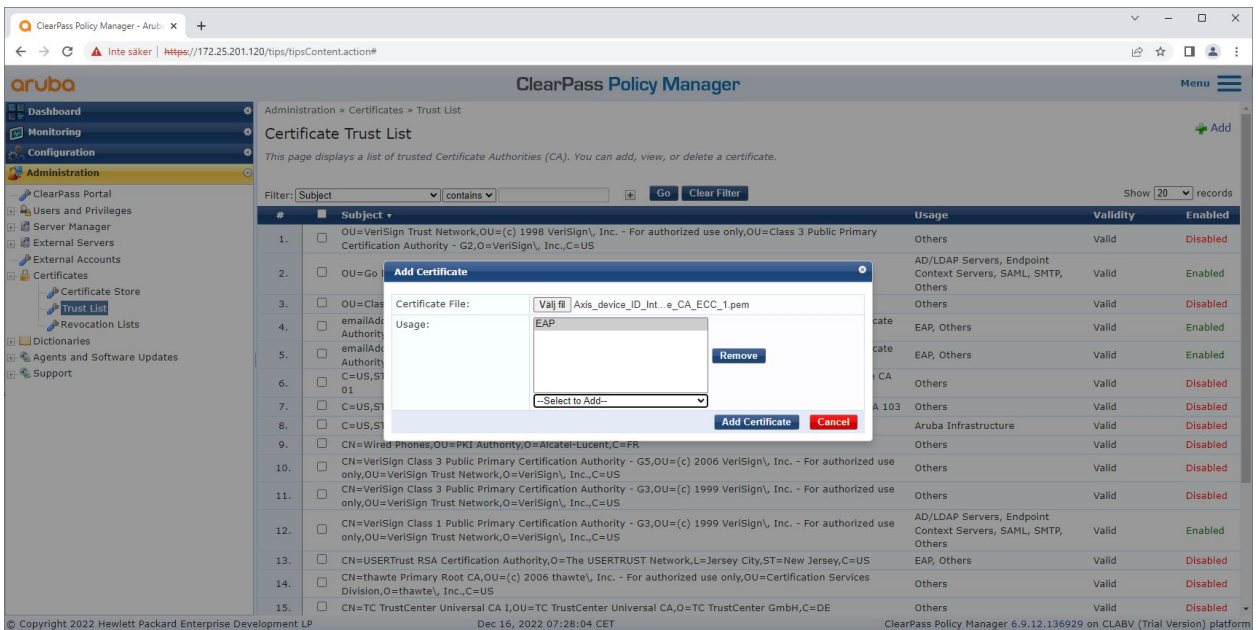
구성 HPE Aruba

Aruba ClearPass Policy Manager

Aruba의 ClearPass Policy Manager는 IoT, BYOD, 기업 장치, 직원, 계약자 및 게스트와 멀티벤더 유선, 무선 및 VPN 인프라에 대한 역할 및 장치 기반 보안 네트워크 접근 제어를 제공합니다.

신뢰할 수 있는 인증서 저장소 구성

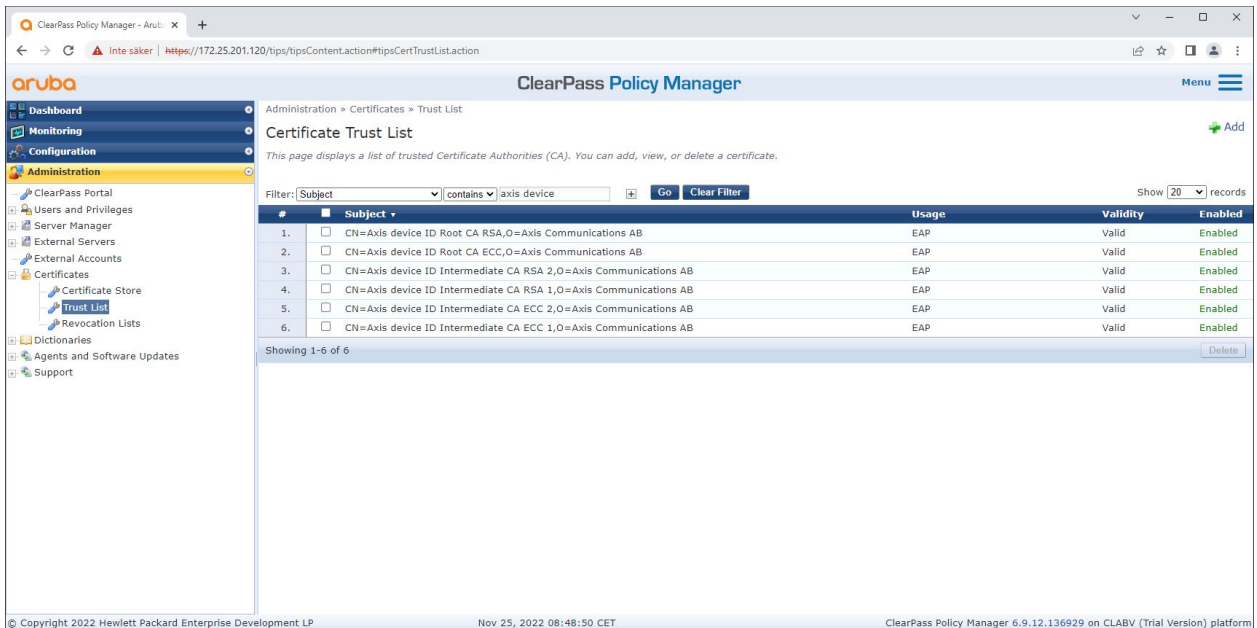
1. axis.com에서 Axis 관련 IEEE 802.1AR 인증서 체인을 다운로드하십시오.
2. Axis 특정 IEEE 802.1AR 루트 CA 및 중간 CA 인증서 체인을 신뢰할 수 있는 인증서 저장소에 업로드합니다.
3. Aruba ClearPass 정책 관리자를 활성화하여 IEEE 802.1X EAP-TLS를 통해 Axis 장치를 인증하십시오.
4. 사용량 필드에서 EAP를 선택합니다. 인증서는 IEEE 802.1X EAP-TLS 인증에 사용됩니다.



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

Secure integration of Axis devices into Aruba networks

보안 온보딩 - IEEE 802.1AR/802.1X



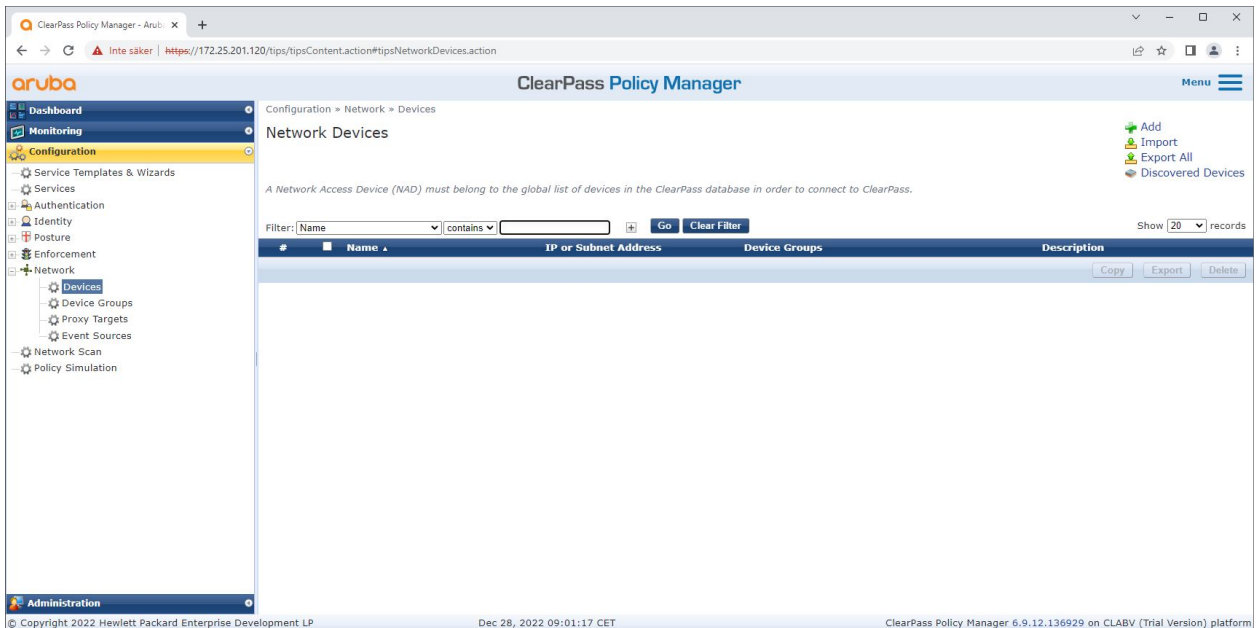
Axis 특정 IEEE 802.1AR 인증서 체인이 포함된 Aruba ClearPass Policy Manager의 신뢰할 수 있는 인증서 저장소입니다.

네트워크 장치/그룹 구성

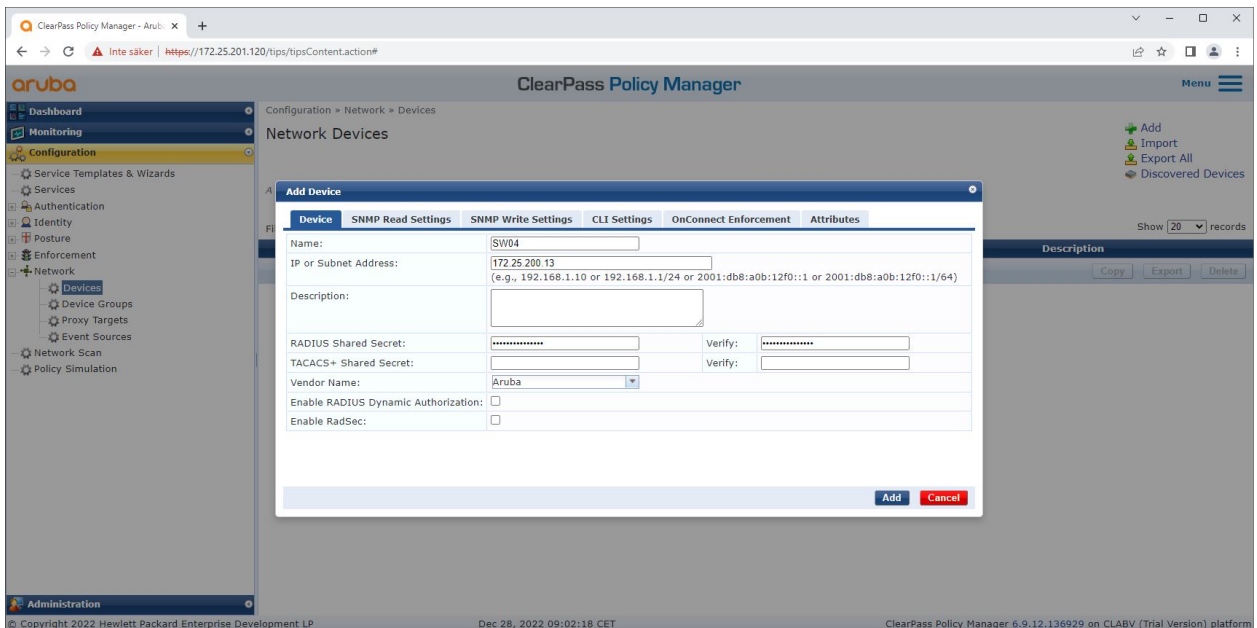
1. Aruba 액세스 스위치와 같은 신뢰할 수 있는 네트워크 액세스 장치를 ClearPass Policy Manager에 추가하십시오. ClearPass Policy Manager는 네트워크에서 IEEE 802.1X 통신에 사용될 Aruba 액세스 스위치를 알아야 합니다.
2. 네트워크 장치 그룹 구성을 사용하여 신뢰할 수 있는 여러 네트워크 액세스 장치를 그룹화합니다. 신뢰할 수 있는 네트워크 액세스 장치를 그룹화하면 정책 구성이 더 쉬워집니다.
3. RADIUS 공유 비밀은 특정 스위치 IEEE 802.1X 구성과 일치해야 합니다.

Secure integration of Axis devices into Aruba networks

보안 온보딩 - IEEE 802.1AR/802.1X



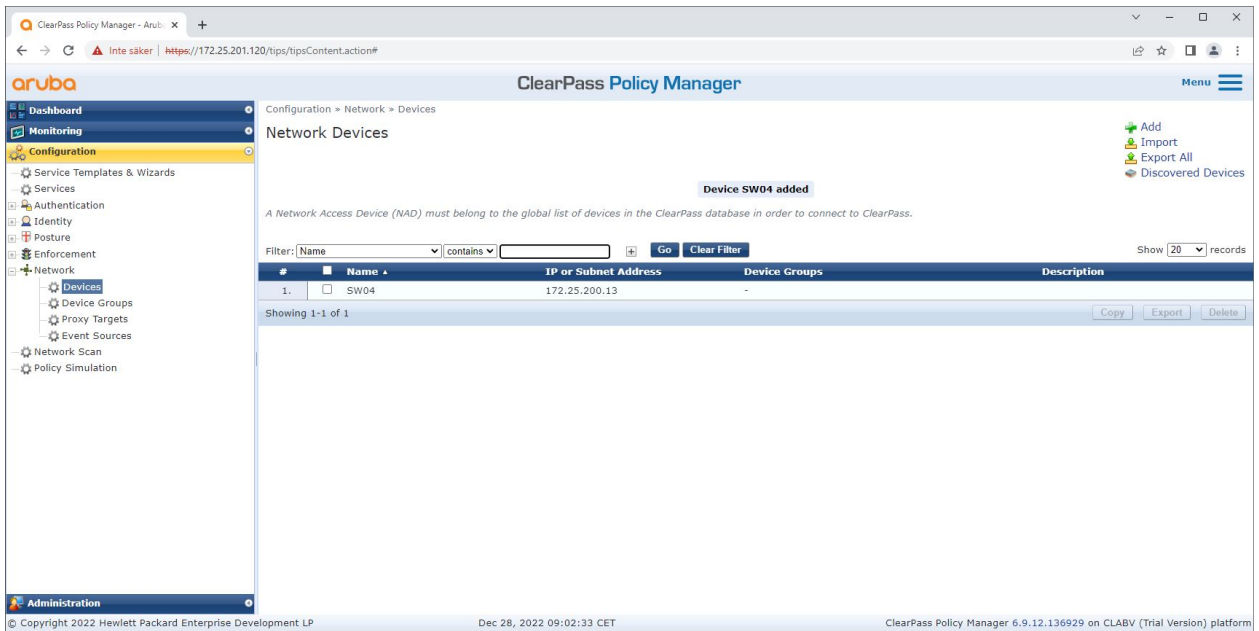
Aruba ClearPass Policy Manager의 신뢰할 수 있는 네트워크 장치 인터페이스입니다.



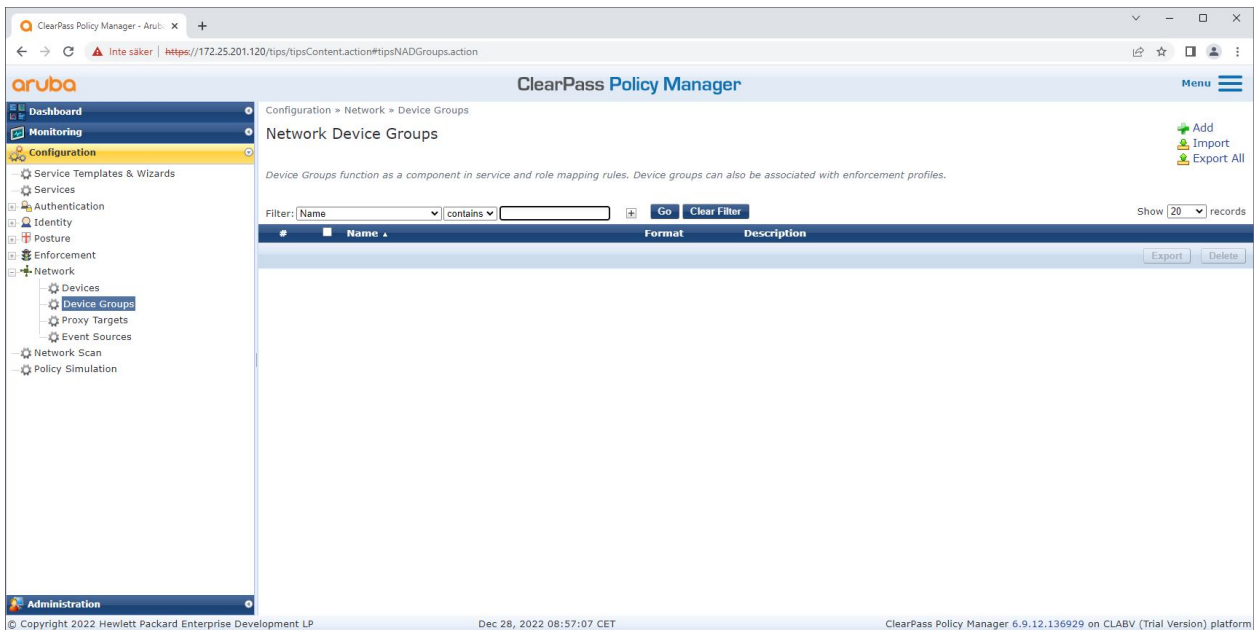
Aruba ClearPass Policy Manager에서 Aruba 액세스 스위치를 신뢰할 수 있는 네트워크 장치로 추가합니다. RADIUS 공유 비밀은 특정 스위치 IEEE 802.1X 구성과 일치해야 합니다.

Secure integration of Axis devices into Aruba networks

보안 온보딩 - IEEE 802.1AR/802.1X



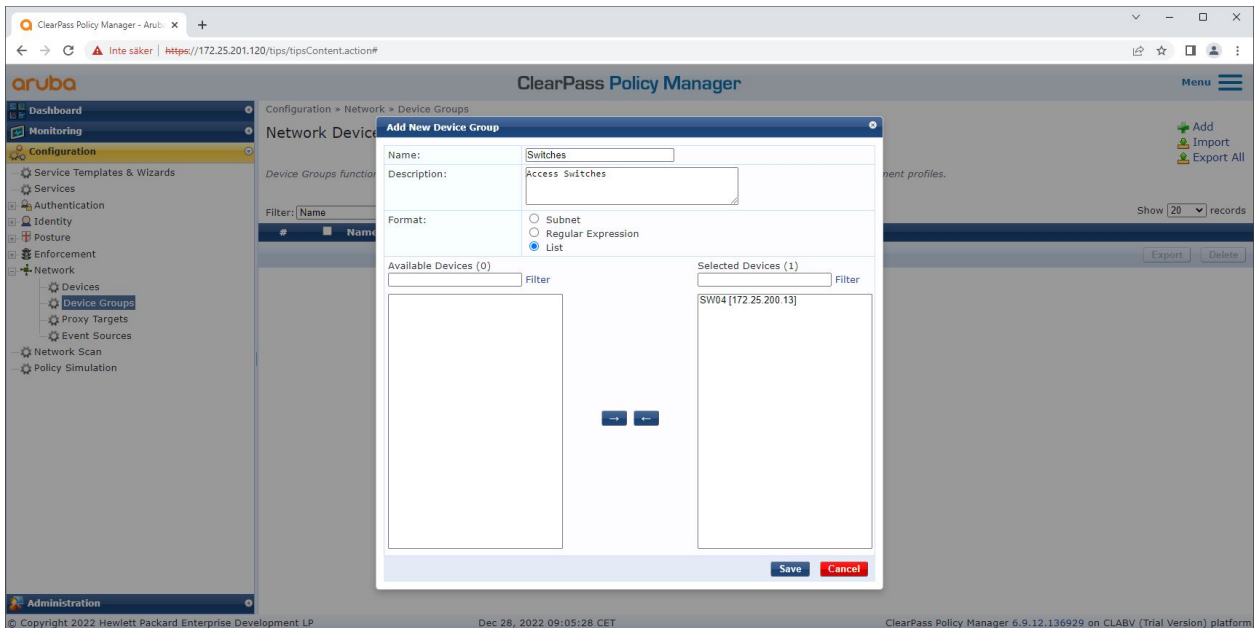
하나의 신뢰할 수 있는 네트워크 장치가 구성된 Aruba ClearPass Policy Manager.



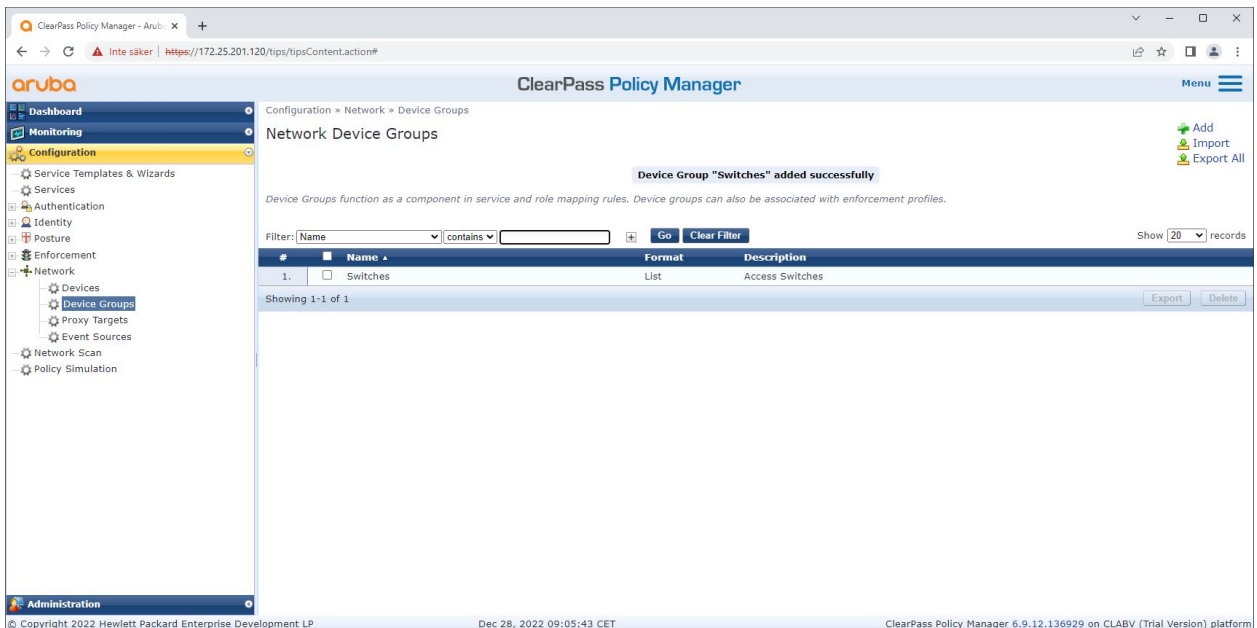
Aruba ClearPass Policy Manager의 신뢰할 수 있는 네트워크 장치 그룹 인터페이스입니다.

Secure integration of Axis devices into Aruba networks

보안 온보딩 - IEEE 802.1AR/802.1X



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



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

장치 지문 구성

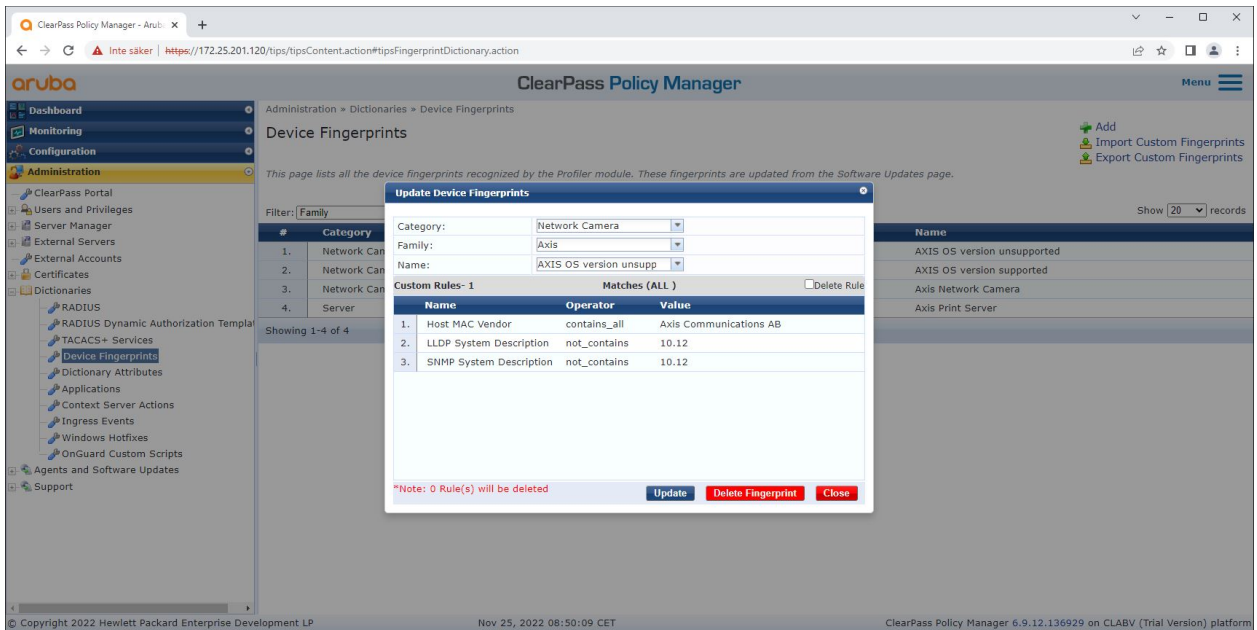
Axis 장치는 네트워크 검색을 통해 MAC 주소, 펌웨어 버전과 같은 장치별 정보를 배포할 수 있습니다. Aruba ClearPass Policy Manager의 장치 지문 인터페이스에서 장치 지문을 생성할 수 있습니다. 장치 지문을 업데이트하고 관리할 수 있습니다. 가능한 작업 중 하나는 AXIS OS 버전에 따라 액세스를 허용하거나 거부하는 것입니다.

장치 지문을 업데이트하고 관리할 수 있습니다. 가능한 작업 중 하나는 AXIS OS 버전에 따라 액세스를 허용하거나 거부하는 것입니다.

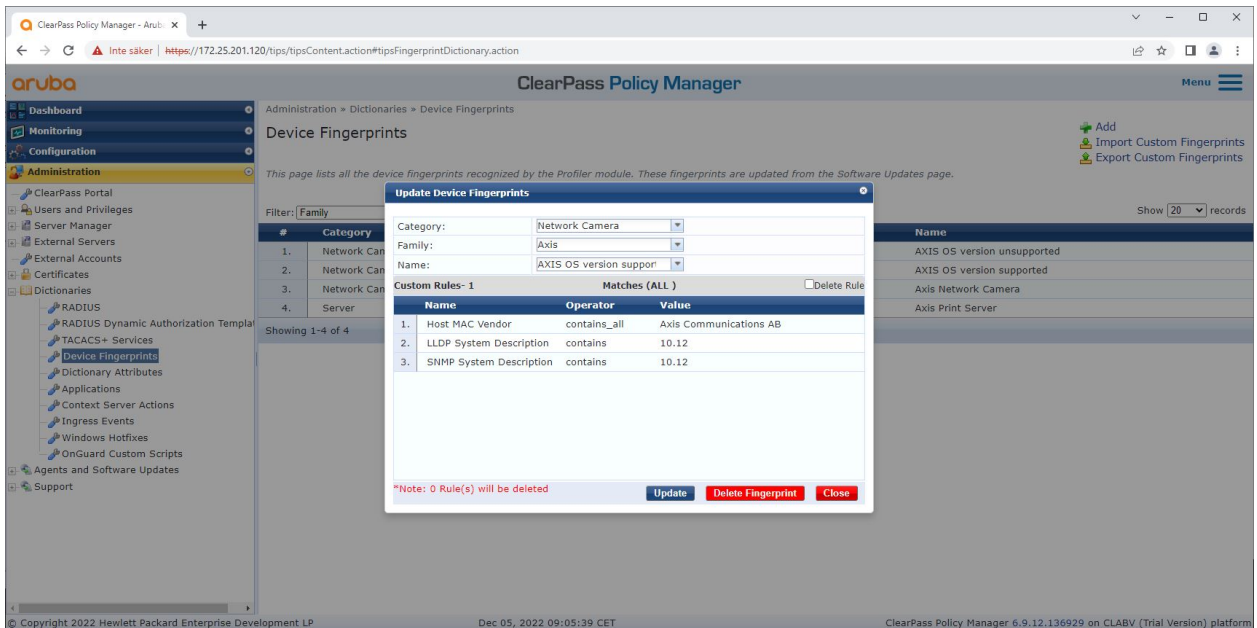
Secure integration of Axis devices into Aruba networks

보안 온보딩 - IEEE 802.1AR/802.1X

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



Aruba ClearPass Policy Manager의 장치 지문 구성입니다. 10.12 이외의 다른 펌웨어 버전을 실행하는 Axis 장치는 지원되지 않는 것으로 간주됩니다.



Aruba ClearPass Policy Manager의 장치 지문 구성입니다. 위 예에서는 펌웨어 10.12를 실행하는 Axis 장치가 지원되는 것으로 간주됩니다.

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

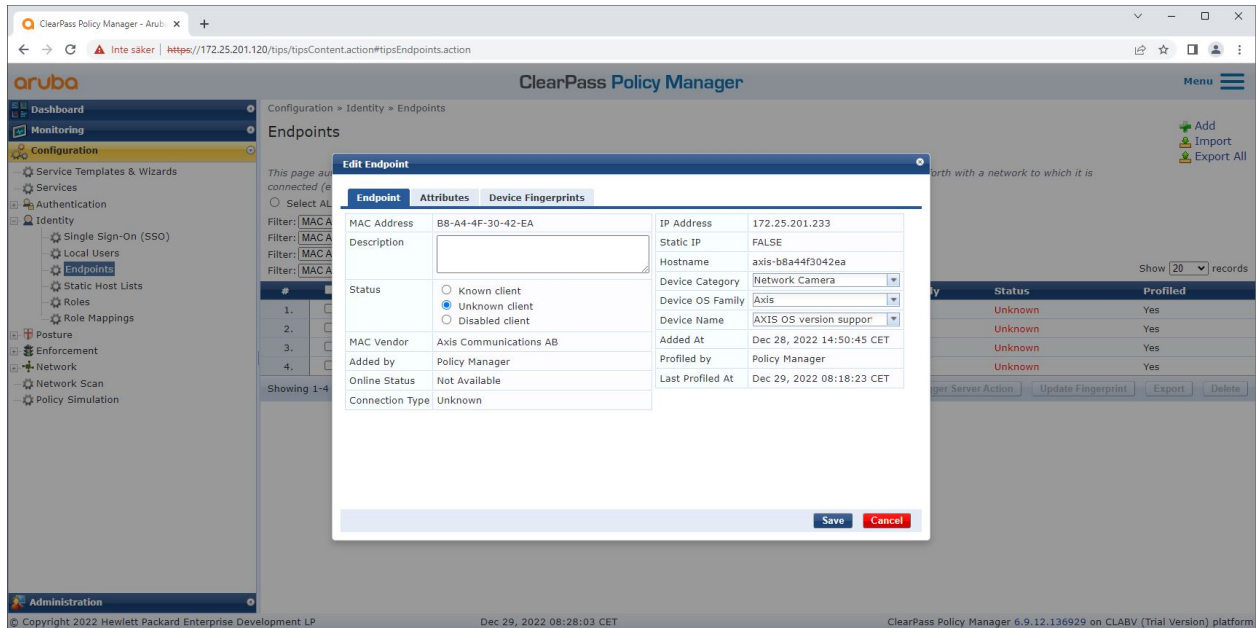
Secure integration of Axis devices into Aruba networks

보안 온보딩 - IEEE 802.1AR/802.1X

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

참고

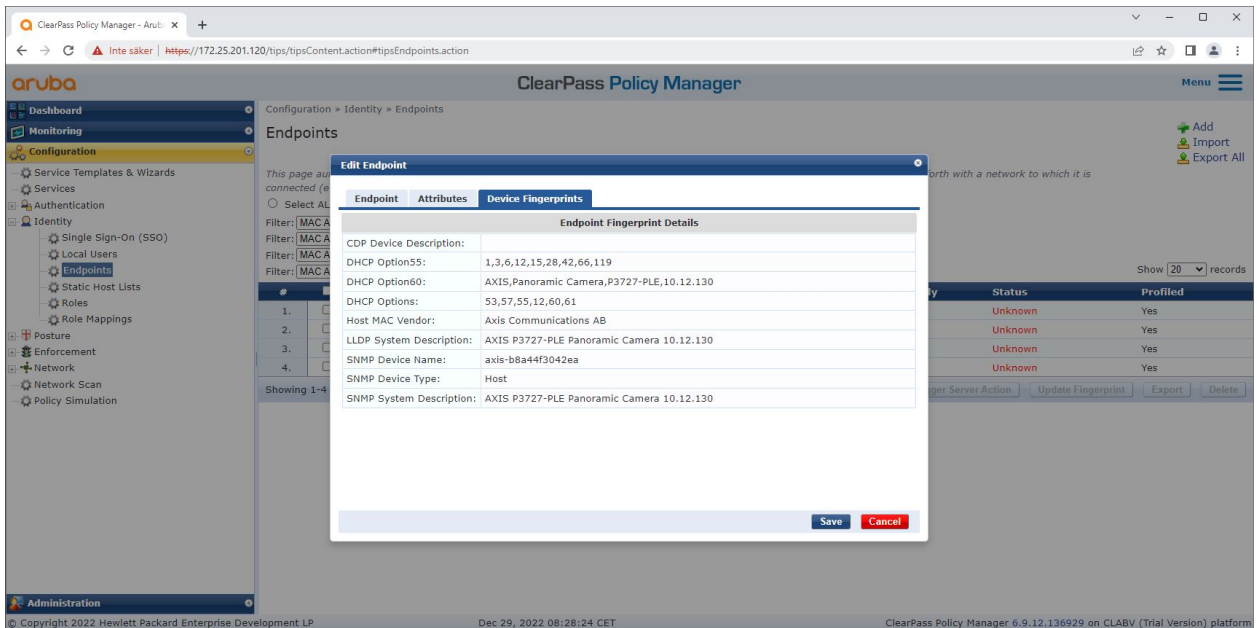
SNMP는 Axis 장치에서 기본적으로 비활성화되어 있으며 Aruba 액세스 스위치에서 수집됩니다.



Aruba ClearPass Policy Manager에 의해 프로파일링된 Axis 장치입니다.

Secure integration of Axis devices into Aruba networks

보안 온보딩 - IEEE 802.1AR/802.1X



프로파일링된 Axis 장치의 자세한 장치 지문입니다. Axis 장치에서는 SNMP가 기본적으로 비활성화되어 있습니다. LLDP, CDP 및 DHCP 관련 검색 정보는 공장 출하 시 기본 설정 상태에서 Axis 장치에 의해 공유되고 Aruba 액세스 스위치에 의해 ClearPass Policy Manager로 전달됩니다.

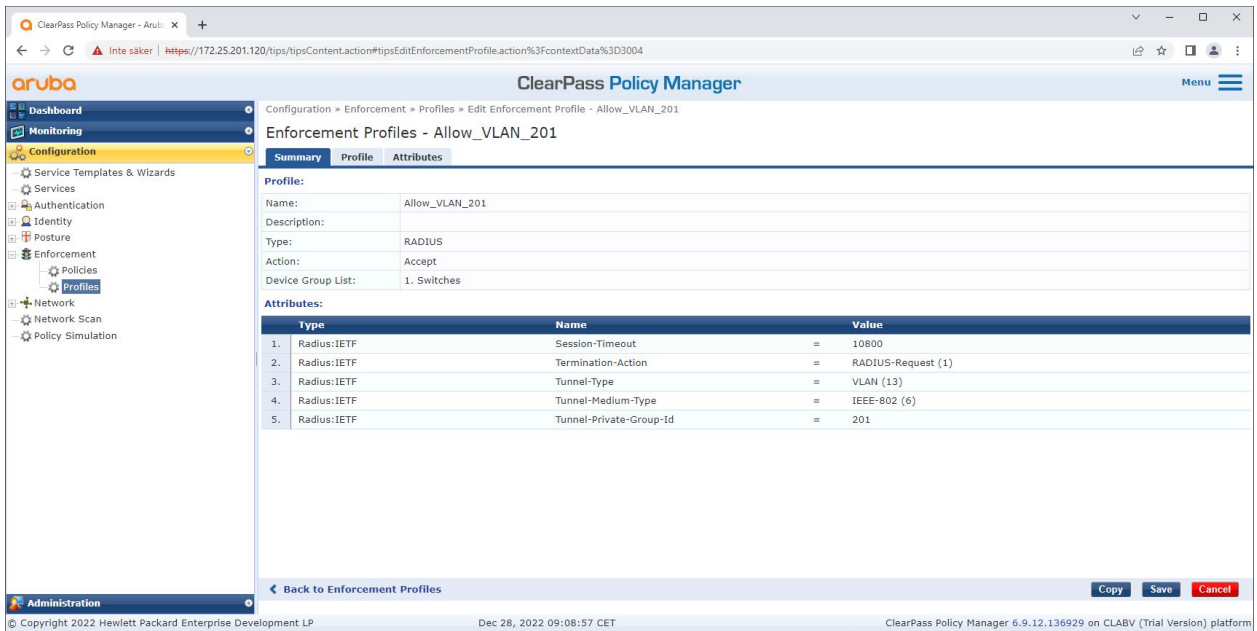
집행 프로파일 구성

집행 프로파일은 Aruba ClearPass Policy Manager가 스위치의 액세스 포트에 특정 VLAN ID를 할당할 수 있도록 하는 데 사용됩니다. 이는 장치 그룹 '스위치'의 네트워크 장치에 적용되는 정책 기반 결정입니다. 필요한 시행 프로파일 수는 사용될 VLAN 수에 따라 다릅니다. 우리 설정에는 3개의 시행 프로파일과 관련된 총 3개의 VLAN(VLAN 201, 202, 203)이 있습니다.

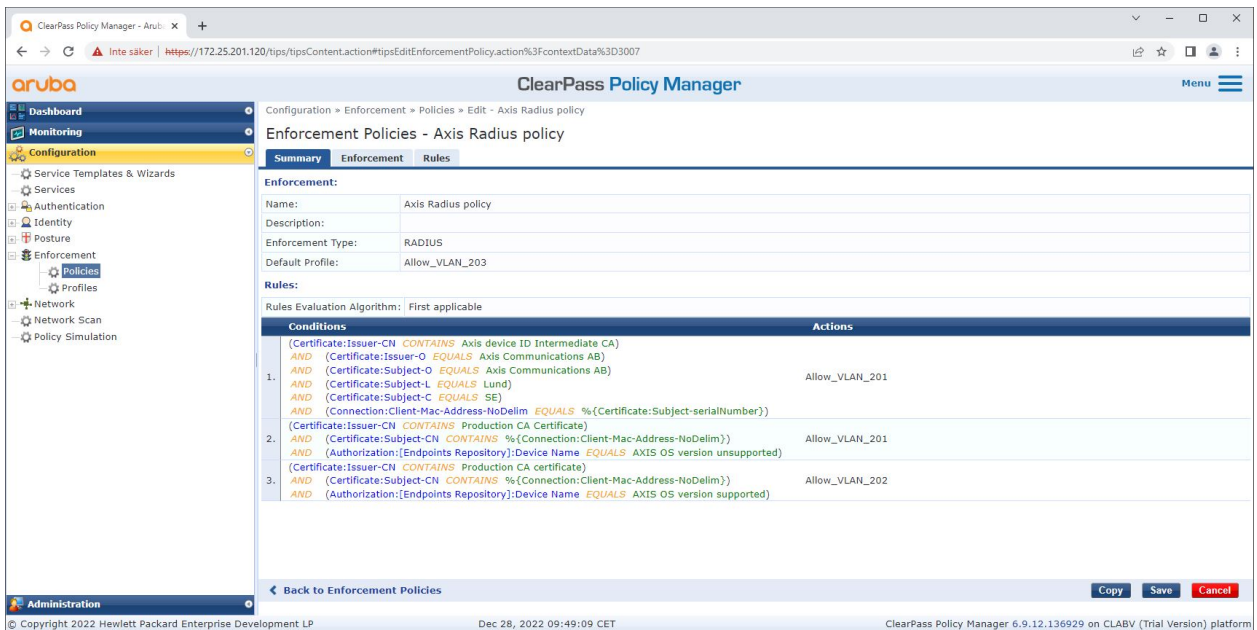
VLAN에 대한 시행 프로필을 구성한 후 실제 집행 정책을 구성할 수 있습니다. Aruba ClearPass Policy Manager의 시행 정책 구성은 네 가지 정책 프로파일 예시를 기반으로 Axis 장치에 Aruba 네트워크에 대한 액세스 권한을 부여할지 여부를 정의합니다.

Secure integration of Axis devices into Aruba networks

보안 온보딩 - IEEE 802.1AR/802.1X



VLAN 201에 대한 액세스를 허용하는 집행 프로파일의 예입니다.



Aruba ClearPass Policy Manager의 집행 정책 구성입니다.

네 가지 집행 정책과 해당 조치는 다음과 같습니다.

네트워크 액세스를 거부

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

게스트 네트워크(VLAN 203)

Secure integration of Axis devices into Aruba networks

보안 온보딩 - IEEE 802.1AR/802.1X

IEEE 802.1X 네트워크 접근 제어 인증이 실패하면 Axis 장치에는 제한되고 격리된 네트워크에 대한 액세스 권한이 부여됩니다. 적절한 조치를 취하려면 장치를 수동으로 검사해야 합니다.

네트워크 프로비저닝(VLAN 201)

Axis 장치에는 프로비저닝 네트워크에 대한 액세스 권한이 부여됩니다. 이는 *Axis Device Manager* 및 *Axis Device Manager Extend*를 통해 Axis 장치 관리 기능을 제공하기 위한 것입니다. 또한 펌웨어 업데이트, 생산 등급 인증서 및 기타 구성을 사용하여 Axis 장치를 구성할 수도 있습니다. Aruba ClearPass Policy Manager는 다음 조건을 확인합니다.

- Axis 장치의 펌웨어 버전입니다.
- 장치의 MAC 주소는 공급업체별 Axis MAC 주소 체계와 Axis 장치 ID 인증서의 일련 번호 특성과 일치합니다.
- Axis 장치 ID 인증서는 검증 가능하며 발급자, 조직, 위치, 국가 등 Axis 관련 속성과 일치합니다.

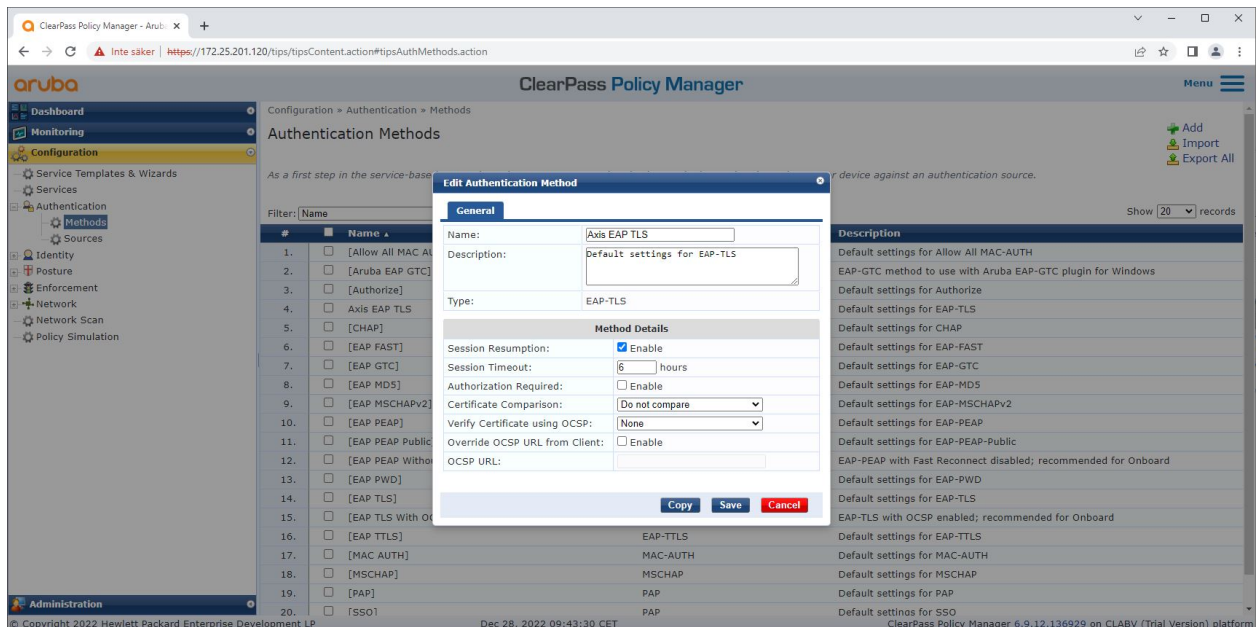
생산 네트워크(VLAN 202)

Axis 장치에는 Axis 장치가 작동할 프로덕션 네트워크에 대한 액세스 권한이 부여됩니다. 프로비저닝 네트워크(VLAN 201) 내에서 장치 프로비저닝이 완료된 후 액세스 권한이 부여됩니다. Aruba ClearPass Policy Manager는 다음 조건을 확인합니다.

- 장치의 MAC 주소는 공급업체별 Axis MAC 주소 체계와 Axis 장치 ID 인증서의 일련 번호 특성과 일치합니다.
- Axis 장치의 펌웨어 버전입니다.
- 프로덕션 등급 인증서는 신뢰할 수 있는 인증서 저장소에서 확인할 수 있습니다.

인증 방법 구성

인증 방법에서는 Axis 장치가 Aruba 네트워크에 대해 인증을 시도하는 방법이 정의됩니다. Axis Edge Vault를 지원하는 Axis 장치에는 기본적으로 IEEE 802.1X EAP-TLS가 활성화되어 있으므로 선호되는 인증 방법은 IEEE 802.1X EAP-TLS입니다.



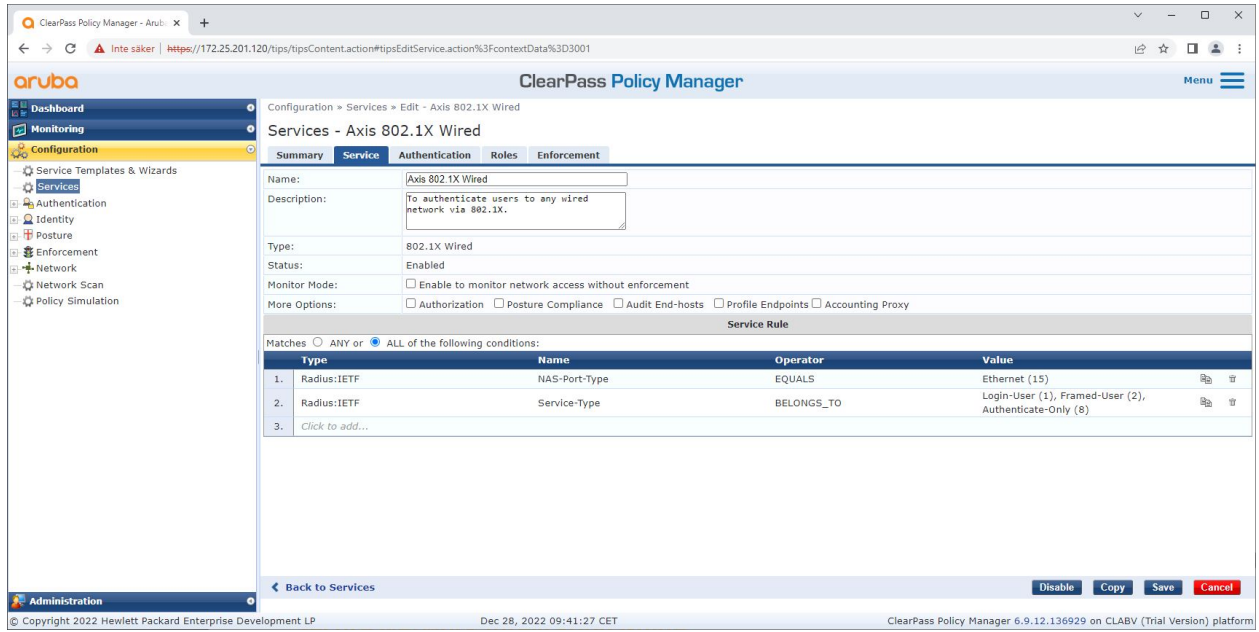
Axis 장치에 대한 EAP-TLS 인증 방법이 정의되는 Aruba ClearPass Policy Manager의 인증 방법 인터페이스입니다.

Secure integration of Axis devices into Aruba networks

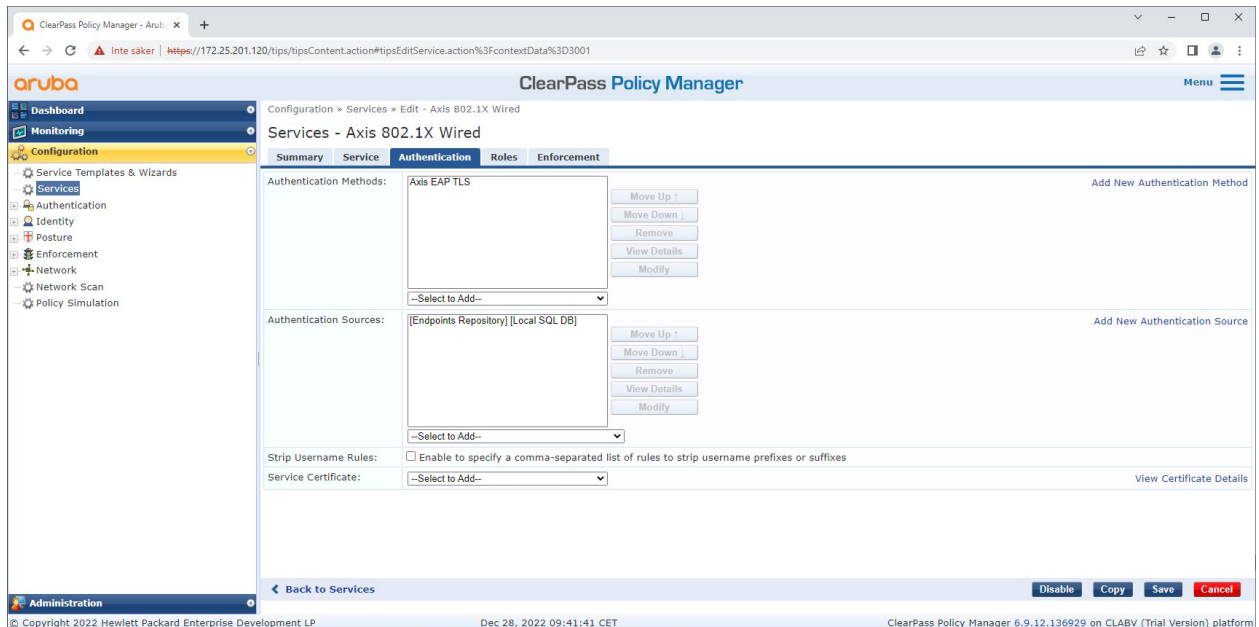
보안 온보딩 - IEEE 802.1AR/802.1X

서비스 구성

서비스 인터페이스에서 구성 단계는 Aruba 네트워크에서 Axis 장치의 인증 및 권한 부여를 처리하는 하나의 단일 서비스로 결합됩니다.



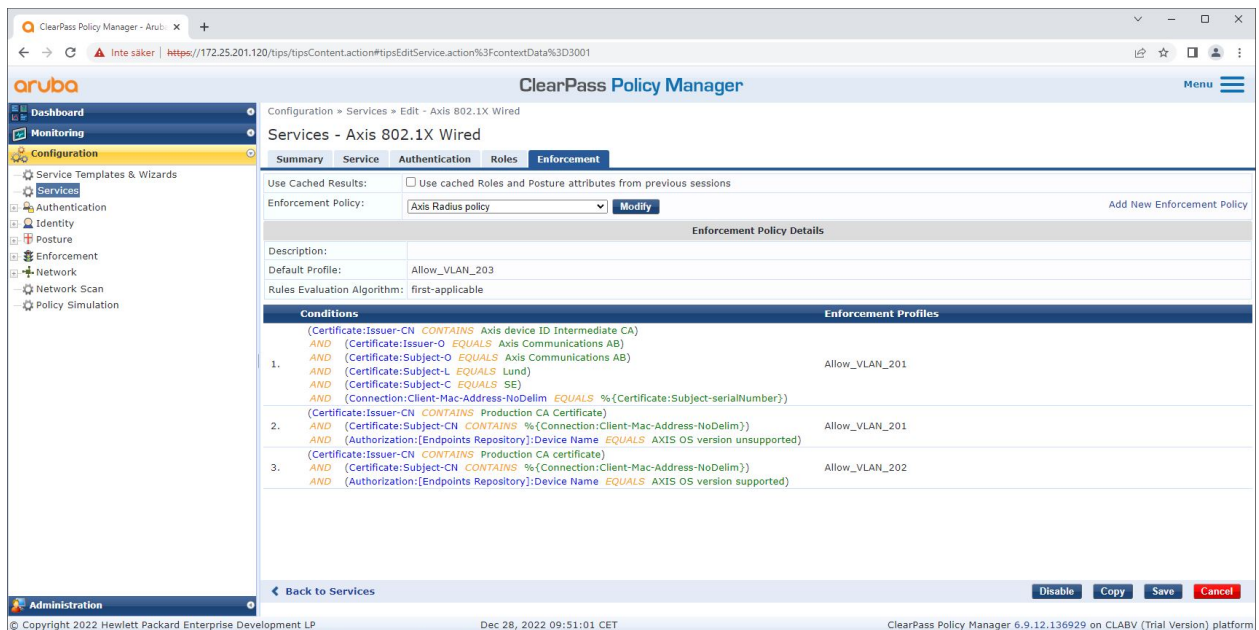
IEEE 802.1X를 연결 방법으로 정의하는 전용 Axis 서비스가 생성됩니다.



다음 단계에서는 이전에 생성된 EAP-TLS 인증 방법이 서비스에 구성됩니다.

Secure integration of Axis devices into Aruba networks

보안 온보딩 - IEEE 802.1AR/802.1X



마지막 단계에서는 이전에 생성된 시행 정책이 서비스에 구성됩니다.

Aruba 액세스 스위치

Axis 장치는 PoE 지원 Aruba 액세스 스위치에 직접 연결되거나 호환되는 Axis PoE 미드스팬을 통해 연결됩니다. Axis 장치를 Aruba 네트워크에 안전하게 온보딩하려면 IEEE 802.1X 통신용으로 액세스 스위치를 구성해야 합니다. Axis 장치는 RADIUS 서버 역할을 하는 Aruba ClearPass Policy Manager에 IEEE 802.1x EAP-TLS 통신을 중계합니다.

참고

전반적인 포트 액세스 보안을 강화하기 위해 Axis 장치에 대한 300초의 주기적인 재인증도 구성됩니다.

Aruba 액세스 스위치에 대한 아래의 전역 및 포트 구성 예시를 참조하십시오.

```
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
```

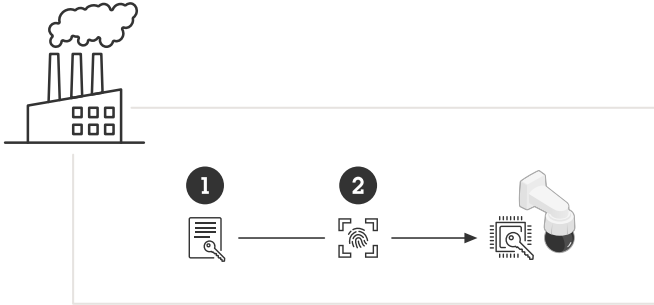
Axis 구성

Axis 네트워크 장치

Axis Edge Vault를 지원하는 Axis 장치는 Axis 장치 ID라고 하는 보안 장치 ID로 제조됩니다. Axis 장치 ID는 IEEE 802.1X를 통한 자동화된 보안 장치 식별 및 네트워크 온보딩 방법을 정의하는 국제 IEEE 802.1AR 표준을 기반으로 합니다.

Secure integration of Axis devices into Aruba networks

보안 온보딩 - IEEE 802.1AR/802.1X



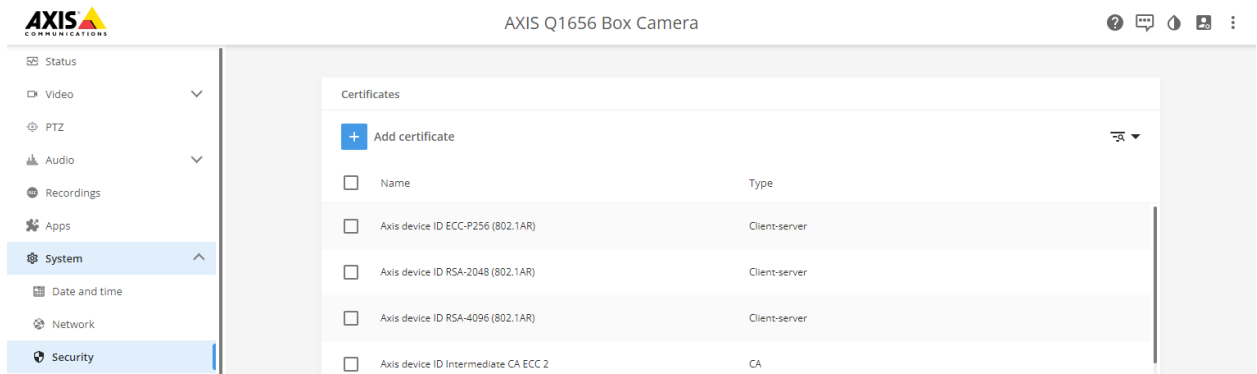
Axis 장치는 신뢰할 수 있는 장치 ID 서비스를 위해 IEEE 802.1AR 호환 Axis 장치 ID 인증서로 제조됩니다.

- 1 Axis 장치 ID 키 인프라(PKI)
- 2 Axis device ID

Axis 장치의 보안 요소에서 제공하는 하드웨어 보호 보안 키 저장소는 Axis 장치의 신뢰성을 전역적으로 증명할 수 있는 장치 고유 인증서 및 해당 키(Axis 장치 ID)와 함께 공장에서 프로비저닝됩니다. *Axis Product Selector*는 Axis Edge Vault 및 Axis 장치 ID를 지원하는 Axis 장치를 알아보는 데 사용할 수 있습니다.

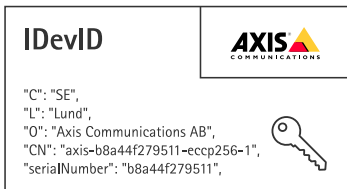
참고

Axis 장치의 일련 번호는 MAC 주소입니다.



Axis Device ID를 사용하여 공장 출하 시 기본값으로 설정된 Axis 장치의 인증서 저장소입니다.

IEEE 802.1AR 호환 Axis 장치 ID 인증서에는 일련 번호에 대한 정보와 기타 Axis 공급업체별 정보가 포함되어 있습니다. 이 정보는 Aruba ClearPass Policy Manager가 네트워크에 대한 액세스 권한을 부여하기 위한 분석 및 의사결정을 위해 사용됩니다. Axis 장치 ID 인증서에서 얻을 수 있는 아래 정보를 참조하십시오.



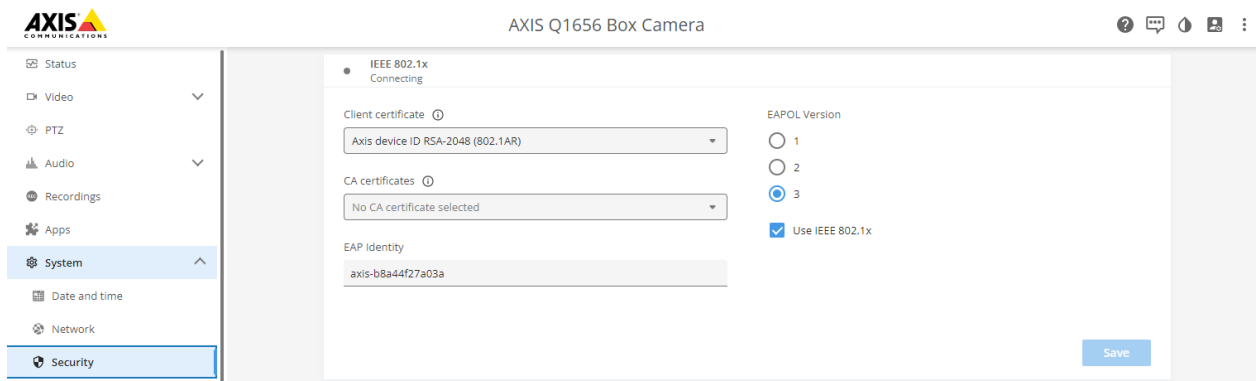
국가	SE
위치	룬드
발급자 조직	Axis Communications AB

Secure integration of Axis devices into Aruba networks

보안 온보딩 - IEEE 802.1AR/802.1X

발급자 일반 이름	Axis 장치 ID 중간
조직	Axis Communications AB
일반 이름	axis-b8a44f279511-eccp256-1
일련번호	b8a44f279511

일반 이름은 Axis 회사 이름, 장치의 일련 번호, 사용된 암호화 알고리즘(ECC P256, RSA 2048, RSA 4096)을 조합하여 구성됩니다. AXIS OS 10.1(2020-09)부터 IEEE 802.1X는 기본적으로 사전 구성된 Axis 장치 ID로 활성화됩니다. 이를 통해 Axis 장치는 IEEE 802.1X 지원 네트워크에서 자체 인증을 받을 수 있습니다.



IEEE 802.1X가 활성화되고 Axis 장치 ID 인증서가 미리 선택된 공장 출하 시 기본값 상태의 Axis 장치입니다.

Axis Device Manager

AXIS Device Manager 및 AXIS Device Manager Extend는 네트워크에서 여러 Axis 장치를 비용 효율적인 방식으로 구성하고 관리하는 데 사용할 수 있습니다. Axis Device Manager는 네트워크의 컴퓨터에 로컬로 설치할 수 있는 Microsoft Windows 기반 애플리케이션인 반면, Axis Device Manager Extend는 클라우드 인프라를 사용하여 다중 사이트 장치 관리를 수행합니다. 두 가지 모두 다음과 같은 Axis 장치에 대한 손쉬운 관리 및 구성 기능을 제공합니다.

- 펌웨어 업데이트 설치.
- HTTPS 및 IEEE 802.1X 인증서와 같은 사이버 보안 구성을 적용합니다.
- 이미지 설정 등 장치별 설정을 구성합니다.

Secure integration of Axis devices into Aruba networks

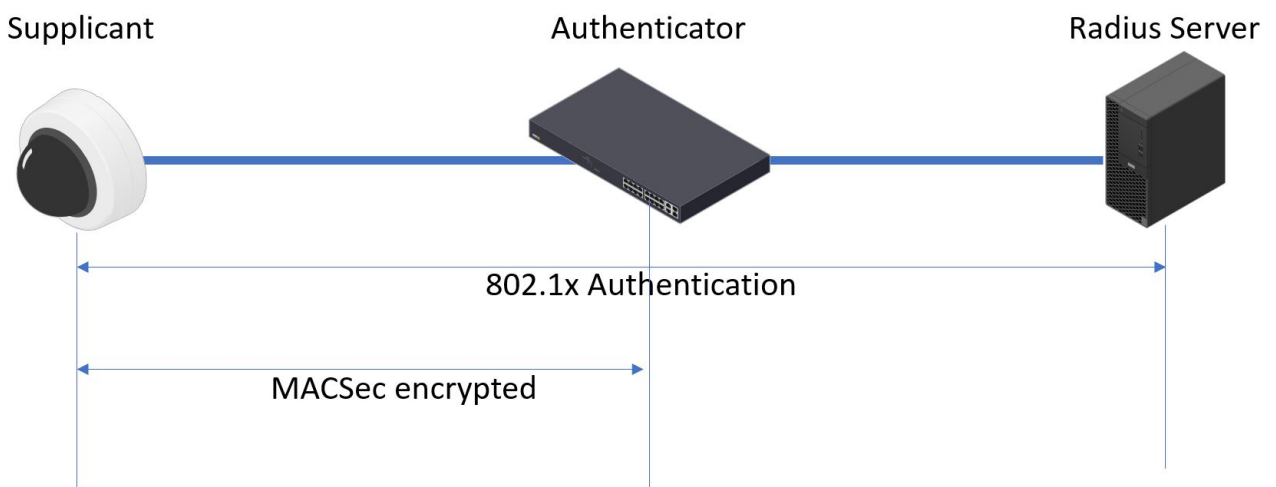
안전한 네트워크 운영 - IEEE 802.1AE MACsec

안전한 네트워크 운영 - IEEE 802.1AE MACsec

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) 이상에서 IEEE 802.1X는 Axis 장치 ID와 호환되는 장치에서는 기본적으로 활성화됩니다. AXIS OS 11.8 이상에서는 기본적으로 활성화되어 있는 IEEE 802.1X EAP-TLS를 사용하여 자동 동적 모드로 MACsec을 지원합니다. 공장 출하 시 기본 설정으로 Axis 장치를 연결하면 IEEE 802.1X 네트워크 인증이 수행되고, 성공하면 MACsec Dynamic CAK 모드도 시도됩니다.

안전하게 저장된 Axis 장치 ID(1), IEEE 802.1AR 규정을 준수하는 보안 장치 ID는 다음 IEEE 802.1X EAP-TLS 포트 기반 네트워크 접근 제어(2)를 통해 Aruba 네트워크(4, 5)에 인증하는 데 사용됩니다. EAP-TLS 세션을 통해 MACsec 키가 자동으로 교환되어 보안 링크(3)를 설정하여 Axis 장치에서 Aruba 스위치로의 모든 네트워크 트래픽을 보호합니다.

IEEE 802.1AE MACsec에는 Aruba 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.

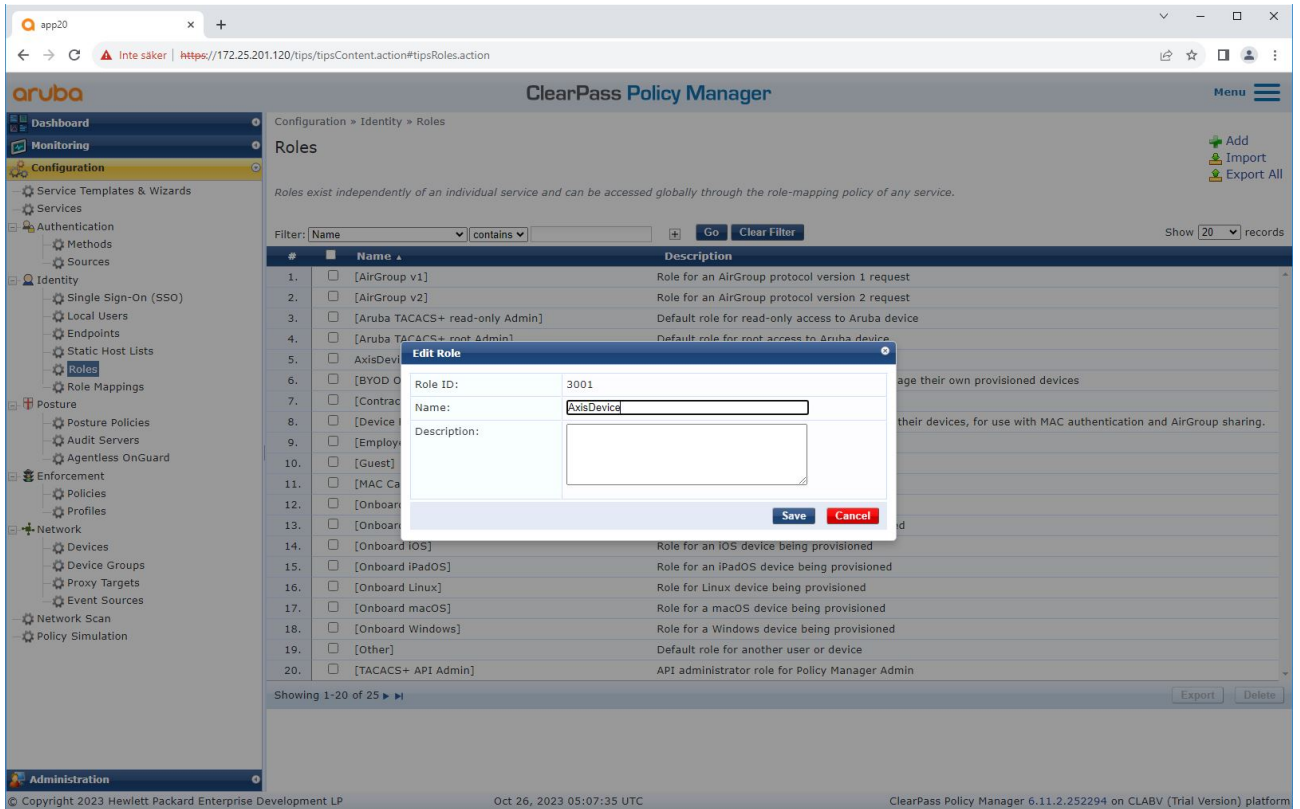
Aruba 액세스 스위치가 EAP-TLS를 사용하는 MACsec을 지원하지 않는 경우, 사전 공유 키 모드를 사용하고 수동으로 구성할 수 있습니다.

Secure integration of Axis devices into Aruba networks

안전한 네트워크 운영 - IEEE 802.1AE MACsec

Aruba ClearPass Policy Manager

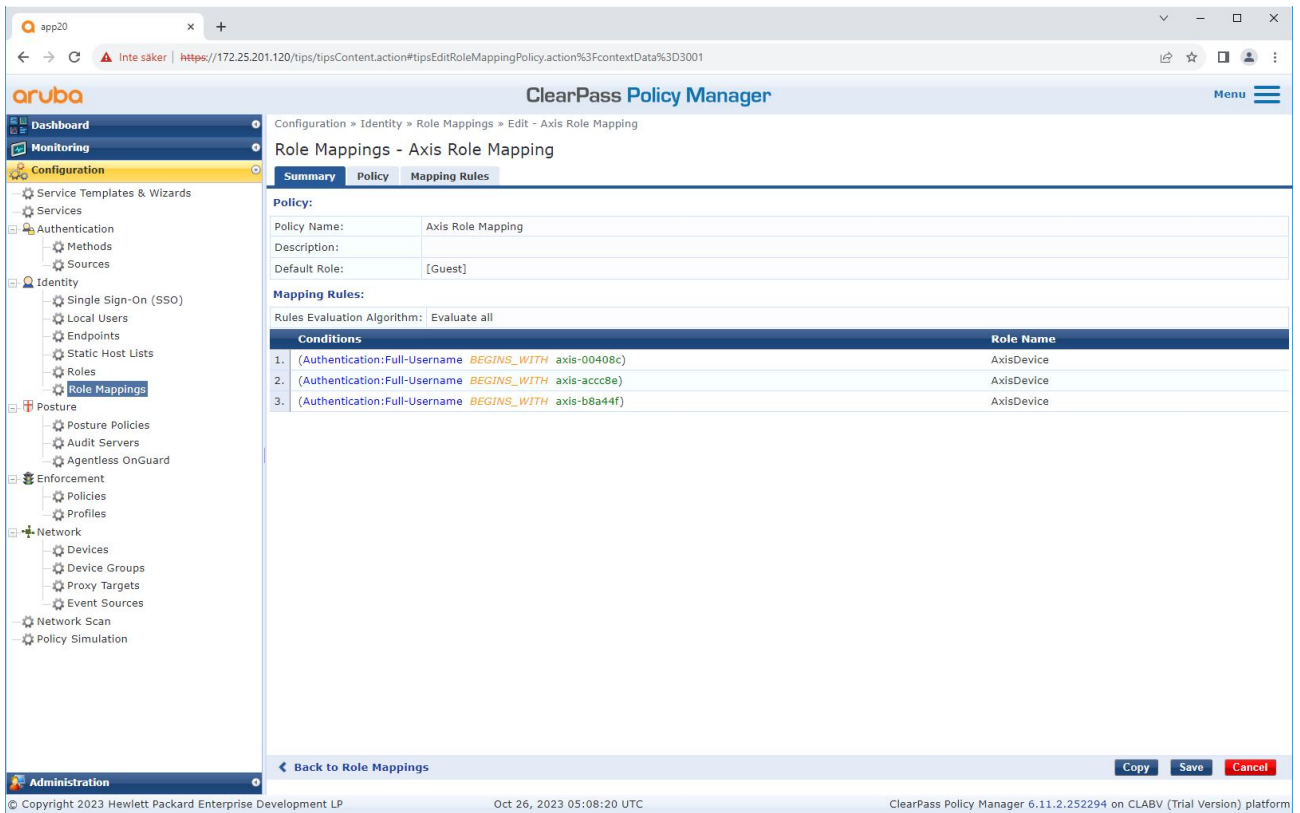
역할 및 역할 매핑 정책



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

Secure integration of Axis devices into Aruba networks

안전한 네트워크 운영 - IEEE 802.1AE MACsec



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

기본적으로 Axis 장치는 EAP ID 형식 'axis-serialnumber'를 사용합니다. Axis 장치의 일련 번호는 MAC 주소입니다. 예를 들어 'axis-b8a44f45b4e6'입니다.

Secure integration of Axis devices into Aruba networks

안전한 네트워크 운영 - IEEE 802.1AE MACsec

서비스 구성

The screenshot shows the Aruba ClearPass Policy Manager web interface. The left sidebar contains navigation menus for Dashboard, Monitoring, Configuration, and Administration. The main content area is titled 'Services - Axis 802.1X Wired' and has tabs for Summary, Service, Authentication, Roles, and Enforcement. The 'Roles' tab is active, displaying the 'Role Mapping Policy' configuration for 'Axis Role Mapping'. The 'Role Mapping Policy Details' section shows a description, default role of '[Guest]', and a rules evaluation algorithm of 'evaluate-all'. Below this is a table with columns 'Conditions' and 'Role'.

Conditions	Role
1. (Authentication:Full-Username BEGINS_WITH axis-00408c)	AxisDevice
2. (Authentication:Full-Username BEGINS_WITH axis-acc08e)	AxisDevice
3. (Authentication:Full-Username BEGINS_WITH axis-b8a44f)	AxisDevice

At the bottom of the interface, there are buttons for 'Back to Services', 'Disable', 'Copy', 'Save', and 'Cancel'. The footer shows copyright information for Hewlett Packard Enterprise Development LP and the version of ClearPass Policy Manager (6.11.2.252294).

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

Secure integration of Axis devices into Aruba networks

안전한 네트워크 운영 - IEEE 802.1AE MACsec

The screenshot shows the Aruba ClearPass Policy Manager interface. The left sidebar contains navigation menus for Dashboard, Monitoring, Configuration, and Administration. The main content area is titled 'Services - Axis 802.1X Wired' and has tabs for Summary, Service, Authentication, Roles, and Enforcement. The Enforcement tab is selected, showing a table of conditions and enforcement profiles.

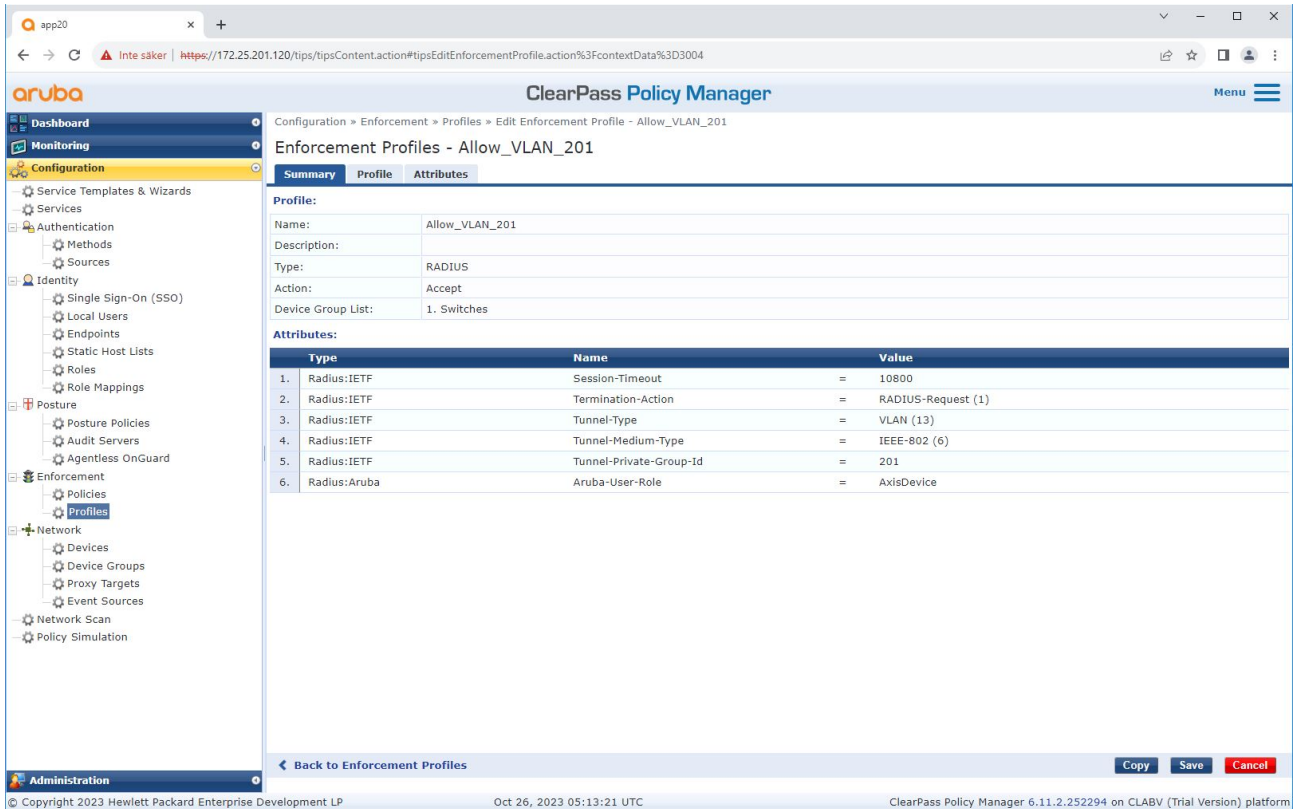
Conditions	Enforcement Profiles
1. (Certificate:Issuer-CN CONTAINS Axis device ID Intermediate CA) AND (Certificate:Issuer-O EQUALS Axis Communications AB) AND (Certificate:Subject-O EQUALS Axis Communications AB) AND (Connection:Client-Mac-Address-NoDelim EQUALS %(Certificate:Subject-serialNumber)) AND (Tips:Role EQUALS AxisDevice)	Allow_VLAN_201
2. unsupported) (Certificate:Issuer-CN CONTAINS Production CA) AND (Authorization:[Endpoints Repository]:Device Name EQUALS AXIS OS version AND (Certificate:Subject-CN CONTAINS Production XYZ) AND (Tips:Role EQUALS AxisDevice)	Allow_VLAN_201
3. supported) (Certificate:Issuer-CN CONTAINS Production CA) AND (Authorization:[Endpoints Repository]:Device Name EQUALS AXIS OS version AND (Certificate:Subject-CN CONTAINS Production XYZ) AND (Tips:Role EQUALS AxisDevice)	Allow_VLAN_202

기존 정책 정의에 Axis 역할 이름을 조건으로 추가합니다.

Secure integration of Axis devices into Aruba networks

안전한 네트워크 운영 - IEEE 802.1AE MACsec

집행 프로파일



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

Aruba 액세스 스위치

Aruba 액세스 스위치 페이지 16 항목에 설명된 보안 온보딩 구성 외에도, 하려면 IEEE 802.1AE MACsec을 구성하기 위해 Aruba 액세스 스위치를 위한 포트 구성 예시는 아래를 참조하십시오.

```
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  
mkacac-length 16  
enable
```


Secure integration of Axis devices into Aruba networks

레거시 온보딩 - MAC 인증

레거시 온보딩 - MAC 인증

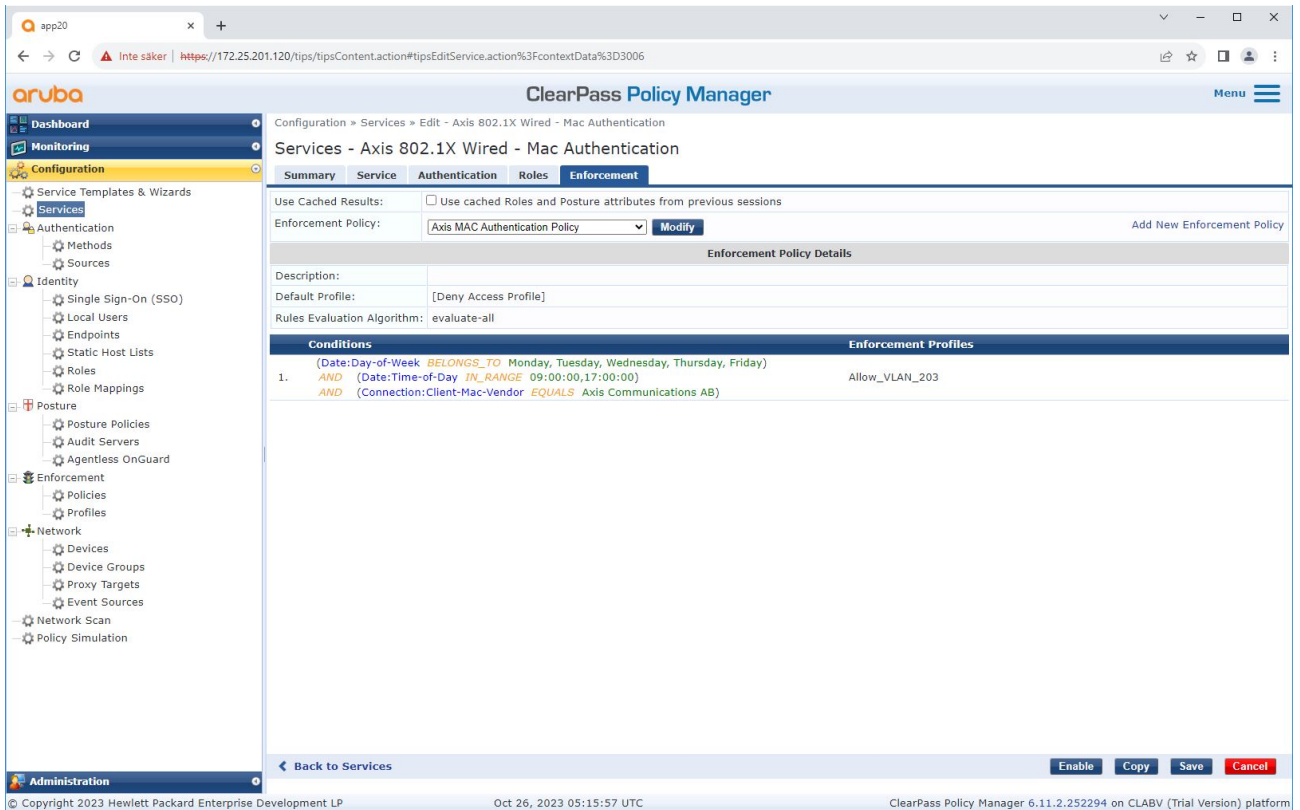
MAC Authentication Bypass(MAB)를 사용하여 장치 ID 인증으로 온보딩하는 IEEE 802.1X를 지원하지 않는 Axis 장치를 온보딩할 수 있으며 IEEE 802.1X가 공장 출하 시 기본 설정 상태가 됩니다. 802.1X 온보딩이 실패하면 Aruba ClearPass Policy Manager는 Axis 장치의 MAC 주소를 검증하고 네트워크에 대한 액세스 권한을 부여합니다.

MAB에는 Aruba 액세스 스위치와 ClearPass Policy Manager 구성 준비가 모두 필요합니다. Axis 장치에서는 온보딩을 위해 MAB를 허용하는 데 구성이 필요하지 않습니다.

Aruba ClearPass Policy Manager

집행 정책

Aruba ClearPass Policy Manager의 시행 정책 구성은 두 가지 정책 조건 프로파일 예시를 기반으로 Axis 장치에 Aruba 네트워크에 대한 액세스 권한을 부여할지 여부를 정의합니다.



네트워크 액세스를 거부

Axis 장치가 구성된 시행 정책을 충족하지 않으면 네트워크에 대한 액세스가 거부됩니다.

게스트 네트워크(VLAN 203)

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

- 월요일부터 금요일 사이의 평일
- 09:00~17:00 사이

Secure integration of Axis devices into Aruba networks

레거시 온보딩 - MAC 인증

- MAC 주소 벤더는 Axis Communications AB와 일치합니다.

MAC 주소는 스푸핑할 수 있으므로 일반 프로비저닝 네트워크에 대한 액세스는 허용되지 않습니다. 초기 온보딩에 만 MAB를 사용하고 장치를 추가로 수동으로 검사하는 것이 좋습니다.

소스 구성

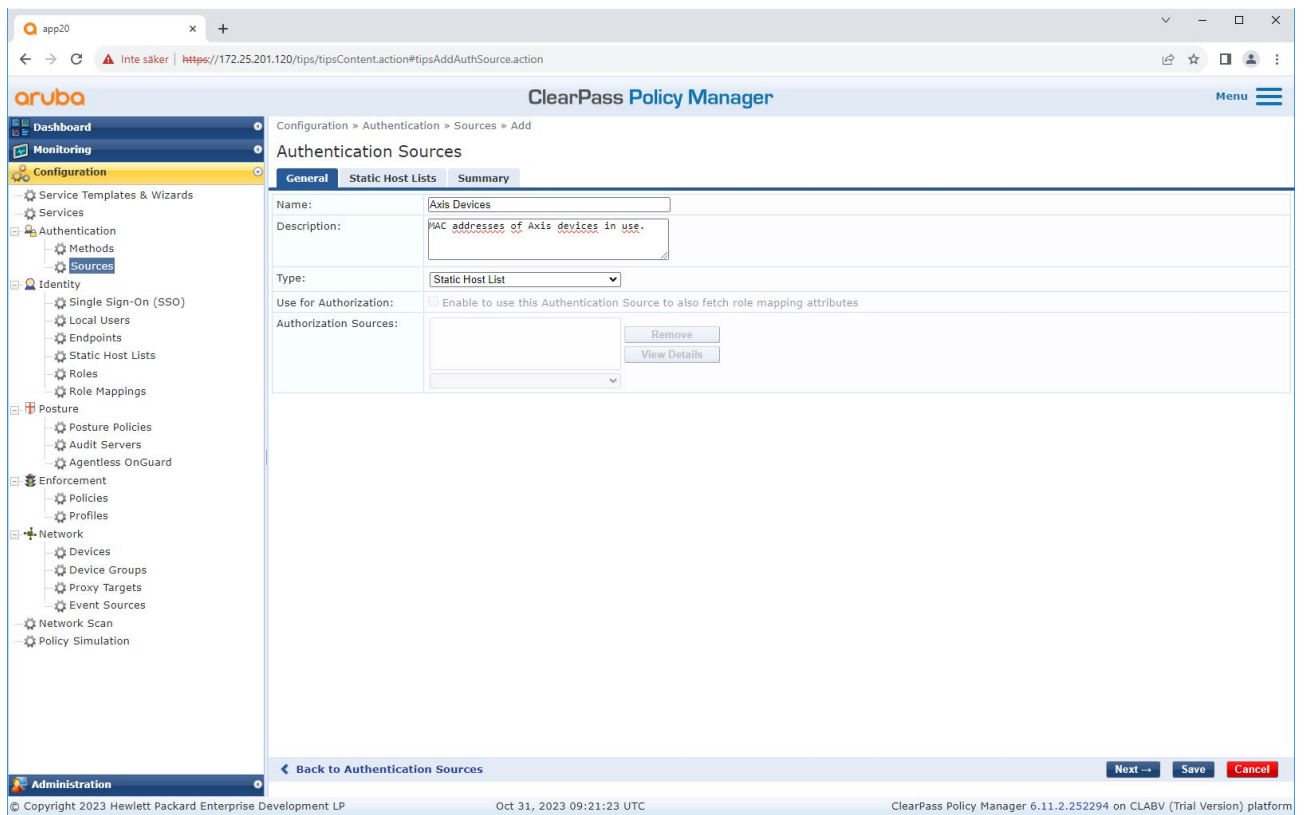
소스 인터페이스에서는 수동으로 가져온 MAC 주소만 허용하는 새로운 인증 소스가 생성됩니다.

The screenshot shows the Aruba ClearPass Policy Manager web interface. The left sidebar contains navigation menus for Dashboard, Monitoring, Configuration, Identity, Posture, Enforcement, and Network. The main content area is titled 'Authentication Sources' and includes a filter bar and a table of 11 authentication sources. The table has columns for '#', 'Name', 'Type', and 'Description'. Below the table are 'Copy', 'Export', and 'Delete' buttons. The footer shows copyright information for Hewlett Packard Enterprise Development LP and the version of the ClearPass Policy Manager.

#	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

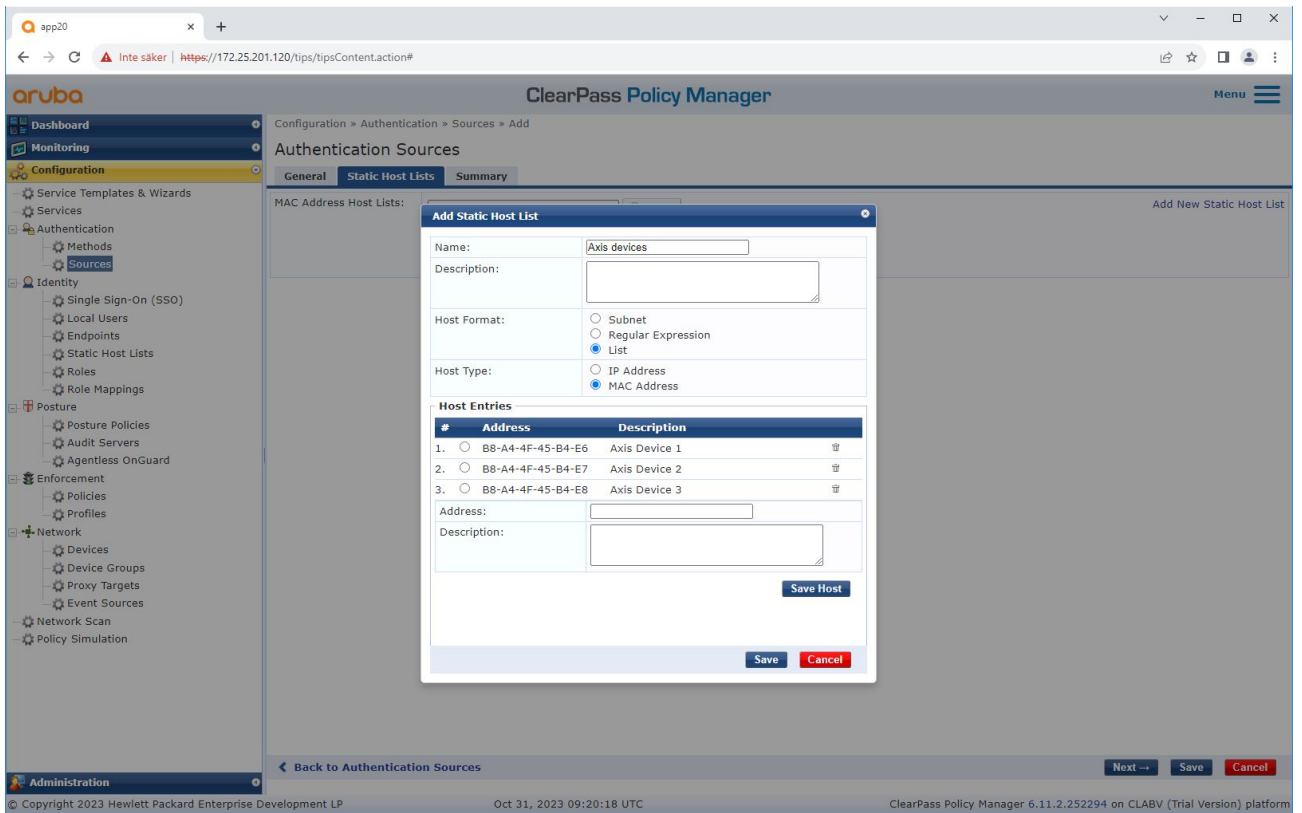
Secure integration of Axis devices into Aruba networks

레거시 온보딩 - MAC 인증



Secure integration of Axis devices into Aruba networks

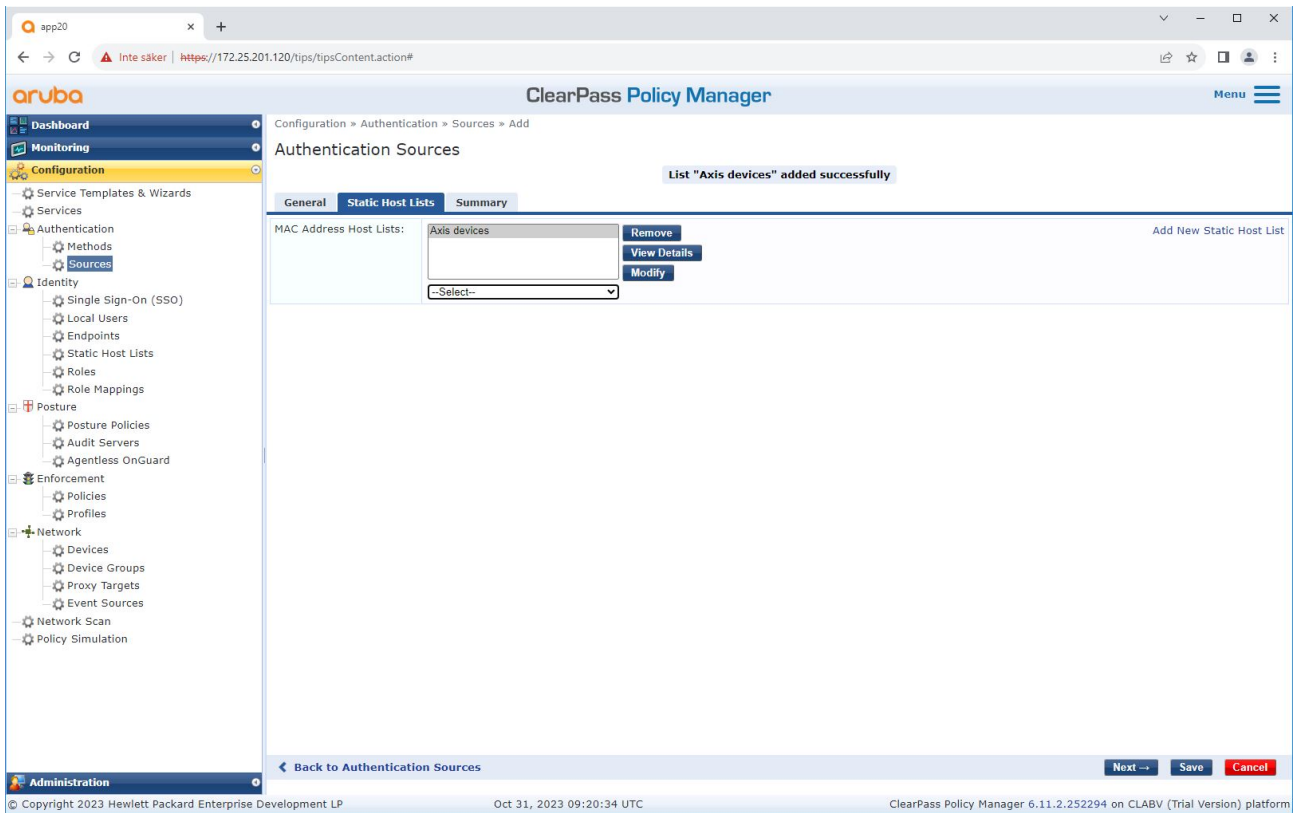
레거시 온보딩 - MAC 인증



Axis MAC 주소가 포함된 정적 호스트 목록이 생성됩니다.

Secure integration of Axis devices into Aruba networks

레거시 온보딩 - MAC 인증



서비스 구성

서비스 인터페이스에서, 구성 단계는 Aruba 네트워크에서 Axis 장치의 인증 및 권한 부여를 처리하는 하나의 단일 서비스로 결합됩니다.

Secure integration of Axis devices into Aruba networks

레거시 온보딩 - MAC 인증

The screenshot displays the Aruba ClearPass Policy Manager interface. The left sidebar shows the navigation menu with 'Configuration' selected. The main content area is titled 'Services' and contains a table of service configurations. The table has columns for '#', 'Order', 'Name', 'Type', 'Template', 'Hit Count', and 'Status'. The status column uses icons: a green checkmark for active services and a red circle for inactive ones. Below the table, there are buttons for 'Reorder', 'Copy', 'Export', and 'Delete'. The footer of the page shows the copyright information and the current date and time.

#	Order	Name	Type	Template	Hit Count	Status
1.	1	Axis 802.1X Wired	RADIUS	802.1X Wired	0	Active
2.	2	Axis 802.1X Wired - Mac Authentication	RADIUS	MAC Authentication	0	Active
3.	3	Test_Service	RADIUS	802.1X Wired	0	Inactive
4.	4	[Policy Manager Admin Network Login Service]	TACACS+	TACACS+ Enforcement	0	Inactive
5.	5	[AirGroup Authorization Service]	RADIUS	RADIUS Enforcement (Generic)	0	Inactive
6.	6	[Aruba Device Access Service]	TACACS+	TACACS+ Enforcement	0	Inactive
7.	7	[Guest Operator Logins]	Application	Aruba Application Authentication	0	Inactive
8.	8	[Insight Operator Logins]	Application	Aruba Application Authentication	0	Inactive
9.	9	[Device Registration Disconnect]	WEBAUTH	Web-based Authentication	0	Inactive

Secure integration of Axis devices into Aruba networks

레거시 온보딩 - MAC 인증

The screenshot shows the Aruba ClearPass Policy Manager web interface. The left sidebar contains navigation menus for Dashboard, Monitoring, Configuration, and Administration. The main content area is titled 'Services - Axis 802.1X Wired - Mac Authentication' and has tabs for Summary, Service, Authentication, Roles, and Enforcement. The 'Service' tab is active, displaying the following configuration details:

- Name: Axis 802.1X Wired - Mac Authentication
- Description: To authenticate guest devices based on their MAC address.
- Type: MAC Authentication
- Status: Disabled
- Monitor Mode: Enable to monitor network access without enforcement
- More Options: Authorization Audit End-hosts Profile Endpoints Accounting Proxy

Below the configuration fields is a 'Service Rule' section with a table of conditions:

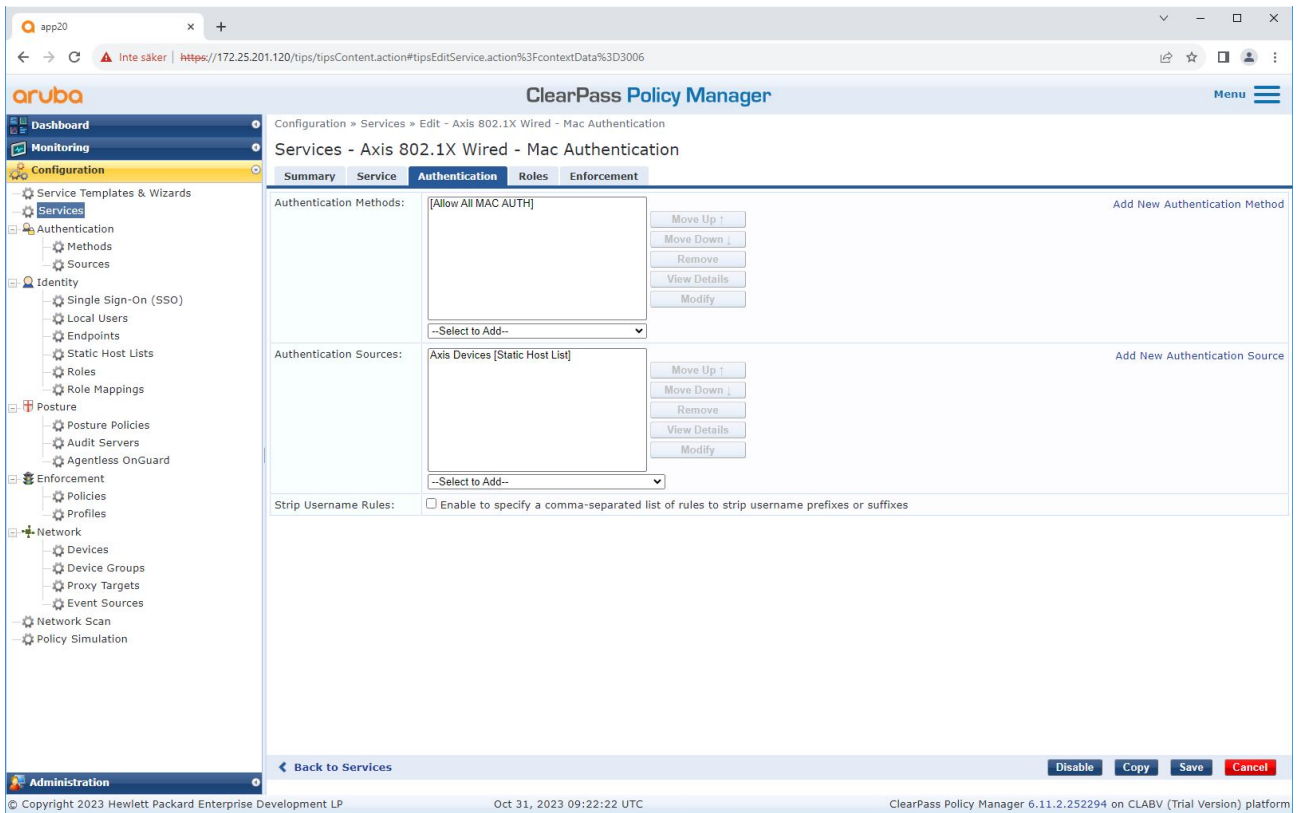
Type	Name	Operator	Value
1.	Radius:IETF	NAS-Port-Type	BELONGS_TO Ethernet (15)
2.	Radius:IETF	Service-Type	BELONGS_TO Login-User (1), Call-Check (10)
3.	Connection	Client-Mac-Address	EQUALS % {Radius:IETF:User-Name}
4.	Click to add...		

At the bottom of the configuration area, there are buttons for 'Enable', 'Copy', 'Save', and 'Cancel'. The footer of the interface shows copyright information for Hewlett Packard Enterprise Development LP and the version of the ClearPass Policy Manager (6.11.2.252294).

MAB를 연결 방법으로 정의하는 전용 Axis 서비스가 생성됩니다.

Secure integration of Axis devices into Aruba networks

레거시 온보딩 - MAC 인증



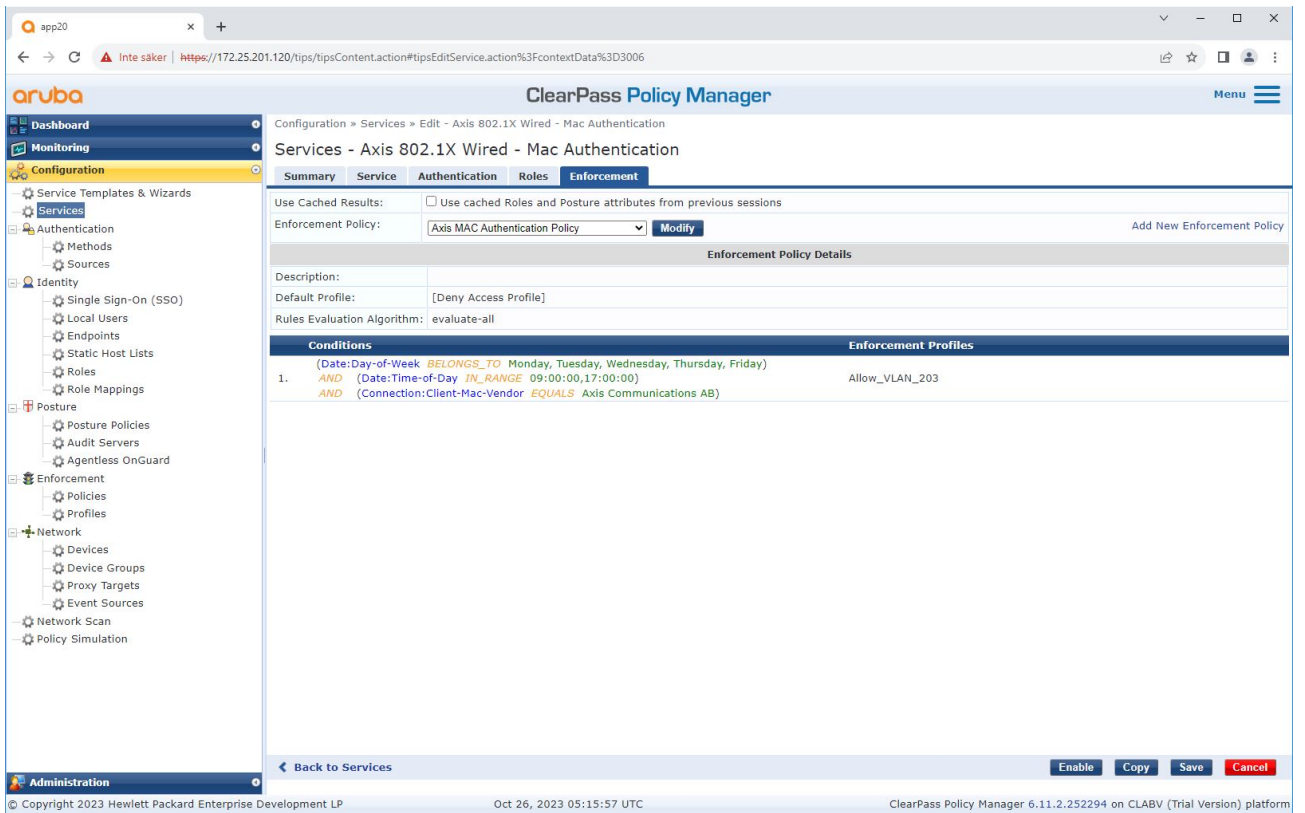
서비스에는 미리 구성된 MAC 인증 방법이 구성되어 있습니다. 또한 Axis MAC 주소 목록을 포함하는 이전에 생성된 인증 소스가 선택됩니다.

Axis Communications AB는 다음 MAC 주소 OUI를 사용:

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

Secure integration of Axis devices into Aruba networks

레거시 온보딩 - MAC 인증



마지막 단계에서는 이전의 생성된 집행 정책이 서비스에 구성됩니다.

Aruba 액세스 스위치

Aruba 액세스 스위치 페이지 16 항목에 설명된 보안 온보딩 구성 외에도, MAB를 허용하려면 Aruba 액세스 스위치에 대한 아래 예제 포트 구성을 참조하십시오.

```
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
```

