

## AXIS Device Manager Extend

사용자 설명서

# AXIS Device Manager Extend

## 목차

정보	3
솔루션 오버뷰	4
제한 조건	7
시작하기	9
My Axis 계정 등록	9
클라이언트를 설치하고 계정 활성화	9
에지 호스트 설치	10
에지 호스트 요청	10
장치 관리	11
에지 호스트에 검색된 장치 추가	11
장비 제거	12
장치에 로그인	12
구성	13
원격 액세스 활성화	13
사이트 제거	13
조직에 사용자 추가	13
사용자 역할 승격	13
사용자 제거	14
펌웨어 관리	15
기기 모델에 따른 펌웨어 관리	15
에지 호스트에서 장치 펌웨어를 관리합니다.	15
진행 중인 중이거나 완료된 펌웨어 업그레이드 보기	15
Policies(정책)	16
보안 정책 생성 및 적용	16
보안 정책 생성 및 적용	16
정책 편집	17
정책 삭제	17
장애 처리	18
방화벽 설정을 구성하는 방법	18

# AXIS Device Manager Extend

## 정보

---

### 정보

AXIS Device Manager Extend 솔루션은 시스템 관리자에게 조직의 네트워크에서 Axis 장치를 검색, 구성 및 작동할 수 있는 인터페이스를 제공합니다.

#### **AXIS Device Manager Extend 데스크톱 앱**

데스크탑 앱은 주문형 또는 시스템 관리를 위해 항상 사용 가능한 사용자 인터페이스로 사용할 수 있는 소프트웨어 유틸리티 프로그램입니다. 로컬에 설치된 에지 호스트와 함께 전용 시스템에서 실행하거나 원격으로 연결된 노트북의 에지 호스트와 별도로 실행할 수 있습니다. 클라이언트는 시스템의 전체 상태와 즉시 사용 가능한 관리 작업을 사용자에게 제공합니다.

#### **에지 호스트**

AXIS Device Manager Extend에서 에지 호스트 구성 요소는 카메라와 같은 로컬 장치를 유지 관리하는 항상 사용 가능한 온 프레미스 관리 서비스입니다. AXIS Device Manager Extend 에지 호스트는 Axis 원격 관리 서비스에 대한 링크 역할도 합니다. 여기서 동일한 API 기능은 Axis 서비스 플랫폼을 통해 사이트의 원격 관리를 지원합니다.

# AXIS Device Manager Extend

## 솔루션 오버뷰

### 솔루션 오버뷰

로컬 및 원격 액세스로 AXIS Device Manager Extend

- 1 Axis를 선택합니다.
- 2 IAM(My Axis)
- 3 조직 데이터
- 4 로컬 클라이언트
- 5 에지 호스트
- 6 장치
- 7 VMS
- 8 TURN
- 9 시그널링
- 10 원격 클라이언트
- 11 원격 액세스 WebRTC 서버
- 12 사이트 1

Con- nec- tion(연 결)	URL 및 IP	포트	프로토콜	설명
A	prod.adm.con- nect.axis.com(52.224.128.152 or 40.127.155.231)	443	HTTPS	필수
B	HTTP 검색(클라이언트에서 에지 호스 트로) 데이터 전송(클라이언트와 에지 호스 트 간) 멀티캐스트 검색(클라이언트에서 에지 호스트로) 멀티캐스트 검색(에지 호스트에서 클 라이언트로)	37080 37443 6801 6801	HTTP HTTPS UDP UDP	사이트를 프로비저닝하 는 데 필요합니다. 제 공 후 선택 사항입니다.
C	데이터 전송(에지 호스트와 장치 간) 유니캐스트 검색 멀티캐스트 검색 HTTP 검색	80/사용자 정의 포트, 443 1900 1900, 5353 80,443	HTTP, HTTPS SSDP, Bonjour	필수
D	signaling.prod.webrtc.connect.axis.com *.turn.prod.webrtc.connect.axis.com	443 443, 5349	HTTPS HTTPS, DTLS(UDP 및 TCP)	WebRTC 표준 기반 선택 사항이며 기본적 으로 꺼짐으로 설정됩 니다
E	피어 투 피어(P2P)	49152-6553 5	DTLS (UDP 및 TCP)	

로컬 및 원격 액세스를 사용하여 다중 사이트 설정을 갖춘 AXIS Device Manager Extend

- 1 Axis를 선택합니다.
- 2 IAM(My Axis)
- 3 조직 데이터
- 4 로컬 클라이언트
- 5 에지 호스트
- 6 장치

# AXIS Device Manager Extend

## 솔루션 오버뷰

- 7 VMS
- 8 TURN
- 9 시그널링
- 10 원격 클라이언트
- 11 원격 액세스 WebCRT 서버
- 12 사이트 1
- 13 사이트 2
- 14 사이트 3

Con- nec- tion(연 결)	URL 및 IP	포트	프로토콜	설명
A	prod.adm.con- nect.axis.com(52.224.128.152 or 40.127.155.231)	443	HTTPS	필수
B	HTTP 검색(클라이언트에서 에지 호스 트로) 데이터 전송(클라이언트와 에지 호스 트 간) 멀티캐스트 검색(클라이언트에서 에지 호스트로) 멀티캐스트 검색(에지 호스트에서 클 라이언트로)	37080 37443 6801 6801	HTTP HTTPS UDP UDP	사이트를 프로비저닝하 는 데 필요합니다. 제 공 후 선택 사항입니다.
C	데이터 전송(에지 호스트와 장치 간) 유니캐스트 검색 멀티캐스트 검색 HTTP 검색	80/사용자 정의 포트, 443 1900 1900, 5353 80,443	HTTP, HTTPS SSDP, Bonjour	필수
D	signaling.prod.webrtc.connect.axis.com *.turn.prod.webrtc.connect.axis.com	443 443, 5349	HTTPS HTTPS, DTLS(UDP 및 TCP)	WebRTC 표준 기반 선택 사항이며 기본적 으로 꺼짐으로 설정됩 니다
E	피어 투 피어(P2P)	49152-6553 5	DTLS (UDP 및 TCP)	

VPN 연결을 사용하여 로컬 액세스 및 원격 액세스를 갖춘 AXIS Device Manager Extend

- 1 Axis를 선택합니다.
- 2 IAM(My Axis)
- 3 조직 데이터
- 4 로컬 클라이언트
- 5 에지 호스트
- 6 장치
- 7 VMS
- 8 TURN
- 9 시그널링
- 10 원격 클라이언트
- 11 원격 액세스 WebCRT 서버
- 12 사이트 1
- 13 사이트 2
- 14 사이트 3

# AXIS Device Manager Extend

## 솔루션 오버뷰

Con- nec- tion(연 결)	URL 및 IP	포트	프로토콜	설명
A	prod.adm.con- nect.axis.com(52.224.128.152 or 40.127.155.231)	443	HTTPS	필수
B	HTTP 검색(클라이언트에서 에지 호스 트로) 데이터 전송(클라이언트와 에지 호스 트 간) 멀티캐스트 검색(클라이언트에서 에지 호스트로) 멀티캐스트 검색(에지 호스트에서 클 라이언트로)	37080 37443 6801 6801	HTTP HTTPS UDP UDP	사이트를 프로비저닝하 는 데 필요합니다. 제 공 후 선택 사항입니다.
C	데이터 전송(에지 호스트와 장치 간) 유니캐스트 검색 멀티캐스트 검색 HTTP 검색	80/사용자 정의 포트, 443 1900 1900, 5353 80,443	HTTP, HTTPS SSDP, Bonjour	필수
D	signaling.prod.webrtc.connect.axis.com *.turn.prod.webrtc.connect.axis.com	443 443, 5349	HTTPS HTTPS, DTLS(UDP 및 TCP)	WebRTC 표준 기반 선택 사항이며 기본적 으로 꺼짐으로 설정됩 니다
E	피어 투 피어(P2P)	49152-6553 5	DTLS (UDP 및 TCP)	

- 추가 요구 사항은 Google DNS와 같은 퍼블릭 DNS입니다. 8.8.8.8/8.8.4.4 또는 Cloudflare DNS: 1.1.1.1
- AXIS Device Manager Extend 시스템의 전체 기능을 지원하려면 A 및 C 연결이 모두 필요합니다.
- 현재 애플리케이션을 개발 중이므로 AXIS Device Manager Extend 데스크톱 앱 및 모든 에지 호스트에 대해 발신 네트워크 연결에 대한 방화벽 액세스를 허용하는 것이 좋습니다.

# AXIS Device Manager Extend

## 전제 조건

---

### 전제 조건

#### 호환되는 운영 체제

- Windows 10 Pro 및 Enterprise
- Windows 11 Pro 및 Enterprise
- Windows Server 2016, 2019 및 2022 (x64 기반 시스템)
- 설치 및 구성 변경에 필요한 시스템 관리자 권한.

#### 최소 시스템 권장 사항:

- CPU: Intel Core i5
- RAM: 4GB
- 네트워크: 100Mbps

#### 인터넷 연결.

##### 참고

AXIS Device Manager Extend 애플리케이션을 사용하려면 설치에 사용된 My Axis 계정과 연결된 조직에 속하는 것으로 식별되는 인증서로 인터넷 연결을 프로비저닝해야 합니다. 그러나 보증 정보 및 다중 사이트 지원과 같은 특정 기능을 이용하려면 인터넷 연결이 필요합니다. 또한 클라이언트 및/또는 사이트 컨트롤러는 온라인 모드에서만 자동으로 업데이트됩니다.

#### 동기화된 시간 및 날짜

##### 참고

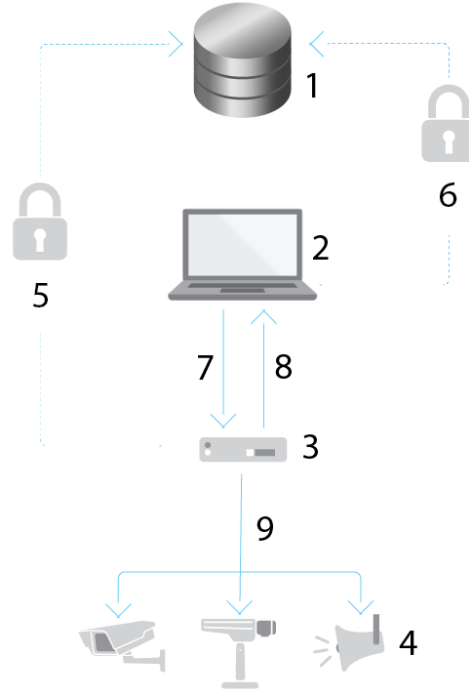
모든 시스템 구성 요소가 동기화되었는지 확인하십시오. 그렇지 않으면 에지 호스트와 클라이언트 또는 백 엔드 간의 인증서 인증이 실패할 수 있습니다. 잠재적인 문제를 방지하기 위해 모든 호스트 시스템을 공통 네트워크 시간 서버에 동기화하는 것이 좋습니다.

#### 개방형 네트워크 포트:

AXIS Device Manager Extend 데스크톱 앱에서 에지 호스트, 에지 호스트 검색 및 Axis 원격 서비스로의 보안 연결용.

# AXIS Device Manager Extend

## 전제 조건



- 1 Axis 서비스 플랫폼
- 2 AXIS Device Manager Extend 데스크톱 앱
- 3 에지 호스트
- 4 장치
- 5 HTTPS(포트 443)
- 6 HTTPS(포트 443)
- 7 HTTPS(포트 37443), UDP 멀티캐스트 검색(포트 6801), HTTP 검색(포트 37080)
- 8 UDP 멀티캐스트 검색(포트 6801)
- 9 HTTPS 및 HTTP (포트 443 및 80), 멀티캐스트 검색 —SSDP (포트 1900) — Bonjour(포트 5353), 유니캐스트 검색(포트 1900), HTTP 검색(포트 80 및 443)

### 발신 네트워크 액세스

현재 애플리케이션을 개발 중이므로 AXIS Device Manager Extend 데스크톱 앱 및 모든 에지 호스트에 대해 발신 네트워크 연결에 대한 방화벽 액세스를 허용하는 것이 좋습니다.



# AXIS Device Manager Extend

## 시작하기

### 시작하기



이 비디오를 시청하려면 이 문서의 웹 버전으로 이동하십시오.

[help.axis.com/?&piaId=63389&section=get-started](https://help.axis.com/?&piaId=63389&section=get-started)


소프트웨어 설치, 조직 생성 및 장치 추가

### My Axis 계정 등록

My Axis 계정을 [axis.com/my-axis/login](https://axis.com/my-axis/login)에서 등록하십시오.

다단계 인증(MFA)을 활성화하여 My Axis 계정을 보다 안전하게 만들 수 있습니다. 다단계 인증(MFA)은 사용자의 신원을 확인하기 위해 또 다른 확인 계층을 추가하는 보안 시스템입니다.

다단계 인증(MFA) 활성화:

1. **My Axis** 자격 증명으로 로그인합니다.
2.  으로 이동하고 **Account settings(계정 설정)**를 선택합니다.
3. **Security settings(보안 설정)**를 클릭합니다.
4. **2-Step verification(2단계 검증)**을 켭니다.

로그인 페이지로 리디렉션됩니다.

5. **My Axis** 자격 증명으로 로그인합니다.

다단계 인증(MFA)이 지금 활성화됩니다.

MFA가 활성 상태일 때 로그인:

1. **My Axis** 계정에 로그인합니다.

이메일이 발송됩니다.

2. 이메일을 열고 **Authenticate(인증)**를 클릭합니다.

이메일을 받지 못했다면 스팸 폴더에 있는지 확인하십시오. 없는 경우 IT 지원에 문의하십시오.

### 클라이언트를 설치하고 계정 활성화

[axis.com](https://axis.com)의 제품 페이지로 이동하여 **AXIS Device Manager Extend 데스크톱 앱 설치 프로그램**을 다운로드하십시오.

1. 애플리케이션을 다운로드한 위치를 찾아 클릭하여 설치합니다.
2. **client(클라이언트)**를 선택하고 **Install(설치)**을 클릭합니다.

# AXIS Device Manager Extend

## 시작하기

---

3. My Axis 계정에 로그인하십시오.
4. 활성화를 완료하려면 이메일 주소를 확인하십시오.
5. 기존 조직을 생성하거나 가입합니다.

### 에지 호스트 설치

에지 호스트와 데스크톱 클라이언트 둘다 AXIS Device Manager Extend 설치 프로그램에 포함되어 있습니다. 가능한 한 장치에 가까운 서버에 사이트 컨트롤러를 설치하는 것이 좋습니다.

1. 에지 호스트를 설치할 서버를 선택
2. 서버에서 설치 프로그램을 실행하고 에지 호스트만 설치하도록 선택하십시오.

### 에지 호스트 요청

AXIS Device Manager Extend 데스크톱 앱에서 장치에 대한 보안 연결을 생성하려면 먼저 에지 호스트를 조직에 요청해야 합니다.

1. 상태가 **Unclaimed(청구되지 않음)**인 에지 호스트를 클릭합니다.
  - 1.1 목록에 에지 호스트가 없으면 **Add new edge host(새 에지 호스트 추가)**를 클릭합니다.
  - 1.2 에지 호스트가 있는 IP 주소를 입력하십시오.
2. 에지 호스트의 이름을 입력
3. 선택적 설명 추가(권장)
4. **Claim edge host(에지 호스트 클레임)**을 클릭합니다.

### 장치 관리

#### 에지 호스트에 검색된 장치 추가

1. **Edge hosts**(에지 호스트)로 이동합니다.
2. 장치를 추가하려는 목록에서 청구된 에지 호스트를 선택합니다.
3. **Devices > Discovered**(장치 > 검색됨)로 이동합니다.
4. 추가할 장치를 선택하거나 선택 열 상단의 상자를 선택하여 모든 장치를 선택합니다.
5. **Add devices to edge host**(에지 호스트에 장치 추가)를 클릭합니다.

이제 장치가 **Managed**(관리됨) 탭에 나열되며 해당 상태는 **Edge host overview**(에지 호스트 오버뷰)에서 검토할 수 있습니다.

#### IP 주소로부터 장치 추가

서브넷, 개별 IP 주소 또는 IP 범위에서 자동으로 검색되지 않는 장치를 추가합니다.

#### IP 범위에서 장치 추가

1. 조직에서 요청한 에지 호스트로 이동합니다.
2. **Settings > Device discovery**(설정 > 장치 검색)로 이동합니다.
3. **Add by IP**(IP로 추가)를 클릭합니다.
4. **Manual entry**(수동 입력)를 선택합니다.
5. IP 범위를 입력
6. **Add IP addresses**(IP 주소 추가)를 클릭
7. **Devices > Discovered**(장치 > 검색됨)로 이동합니다.
8. 추가할 장치를 선택하거나 선택 열 상단의 상자를 선택하여 모든 장치를 선택합니다.
9. **Add devices**(장치 추가)를 클릭합니다.

#### 파일에서 장치 추가

1. 조직에서 요청한 에지 호스트로 이동합니다.
2. **Settings > Device discovery**(설정 > 장치 검색)로 이동합니다.
3. **Add by IP**(IP로 추가)를 클릭합니다.
4. **Import from file**(파일에서 가져오기)를 선택합니다.
5. IP 주소가 있는 쉼표로 구분된(.CSV) 파일을 선택하십시오.
6. **Import**(가져오기)를 클릭합니다.
7. **Devices > Discovered devices**(장치 > 검색된 장치)로 이동합니다.
8. 추가할 장치를 선택하거나 선택 열 상단의 상자를 선택하여 모든 장치를 선택합니다.
9. **Add devices**(장치 추가)를 클릭합니다.

# AXIS Device Manager Extend

## 장치 관리

### 참고

파일에는 다음이 포함되어야 합니다.  
IP 주소 열의 헤더입니다.  
단일 열.  
최대 25,600개의 IP 주소.

## 장비 제거



에지 호스트에서 장치 제거

1. **Edge host(에지 호스트)**를 클릭합니다.
2. 에지 호스트를 선택합니다.
3. **Devices(장치)**로 이동
4. 제거하려는 장치를 선택하거나 선택 열 상단의 확인란을 선택하여 모든 장치를 선택합니다.
5. 작업 메뉴의 **Remove devices from edge host(에지 호스트에서 기기 제거)** 아이콘을 클릭합니다.
6. **Remove(제거)**를 클릭합니다.

제거된 장치는 **Devices > Discovered(장치 > 검색됨)**에서 찾을 수 있습니다.

## 장치에 로그인

1. **Edge hosts(에지 호스트)**를 클릭합니다.
2. 에지 호스트를 선택합니다.
3. **Devices > Managed(장치 > 관리됨)**로 이동합니다
4. 액세스하려는 장치를 선택하거나 선택 열 상단의 확인란을 선택하여 모든 장치를 선택합니다.
5. 여러 장치에 자동으로 로그인하려면 **Log in(로그인)**을 클릭합니다.
6. 사용자 이름과 패스워드를 입력합니다.
7. **Log in(로그인)**을 클릭합니다.

### 참고

사용자 이름 및 패스워드가 정확하면 **Status(상태)**에 **Reachable(접근 가능)**이 표시됩니다.

# AXIS Device Manager Extend

## 구성

### 구성

#### 원격 액세스 활성화

방화벽 설정이 아웃바운드 연결을 차단하는 경우 사이트에 원격으로 액세스하려면 프록시 연결을 입력해야 할 수 있습니다.

1. 원격 액세스를 활성화할 에지 호스트를 선택하십시오.
2. **Settings > Edge hosts connections(설정 > Edge 호스트 연결)**으로 이동합니다.
3. **Allow remote access to edge host(에지 호스트에 대한 원격 액세스 허용)**를 활성화하십시오.
4. 인터넷에 액세스하기 위해 프록시 주소를 입력해야 하는 경우 **프록시 주소** 아래에 주소를 입력합니다.

연결이 활성화되면 알림을 받게 됩니다.

#### 참고

다른 네트워크의 에지 호스트에 대한 연결을 지원하려면 회사 네트워크 방화벽의 '허용 목록'에 다음 구성을 추가해야 할 수 있습니다. 엔드 포인트 포트 프로토콜 신호.prod.webrtc.connect.axis.com 443 HTTPS \*.turn.prod.webrtc.connect.axis.com 443 HTTPS webRTC (Turn 및 P2P) 5349, 49152-65535 DTLS (UDP 및 TCP)

#### 사이트 제거

조직에서 에지 호스트를 제거하기 전에 에지 호스트에 속한 *장비 제거 페이지 12*를 수행해야 합니다. 장치는 **Devices > Discovered(장치 > 검색됨)**에서 찾을 수 있습니다.

1. **Edge hosts(에지 호스트)**를 클릭합니다.
2. 화살표 키로 에지 호스트를 선택하거나 마우스 포인터로 해당 에지 호스트를 가리킵니다.
3. ... 을 클릭하고 드롭다운 메뉴에서 **Remove edge host(에지 호스트 제거)**를 선택합니다.
4. **I'm aware of the risks.(위험을 알고 있습니다.)**를 확인
5. **Remove(제거)**를 클릭합니다.

#### 조직에 사용자 추가

1. 사용자 설정을 구성할 조직을 선택하십시오.
2. **Users(사용자)**로 이동합니다.
3. **Invite to organization(조직에 초대)**를 클릭합니다.
4. 조직에 초대할 사용자의 이메일 주소를 입력합니다.
5. **Send invite(초대 전송)**를 클릭합니다.

#### 참고

사용자는 AXIS Device Manager Extend에 로그인하는 데 사용할 수 있는 초대 이메일을 받게 됩니다. 기본 사용자 역할은 **Viewer(뷰어)**입니다. My Axis 계정이 없는 경우 조직에 액세스하려면 해당 이메일을 사용하여 가입해야 합니다. 수락을 보류하는 동안 초대를 취소할 수 있습니다.

#### 사용자 역할 승격

1. 사용자 설정을 구성할 조직을 선택하십시오.

# AXIS Device Manager Extend

## 구성

---

2. **Users(사용자)**로 이동합니다.
3. 승격하려는 사용자의 **Role(역할)**로 이동합니다.
4. 드롭다운 메뉴를 클릭하여 새 역할을 선택합니다.

### 참고

역할은 선택되면 즉시 변경됩니다. 보안상의 이유로 초대는 뷰어 역할로 제한됩니다.

## 사용자 제거

1. 사용자 설정을 구성할 조직을 선택하십시오.
2. **Users(사용자)**로 이동합니다.
3. 새 옵션 메뉴를 표시하려면 제거하려는 사용자의 사용자 위로 마우스 포인터를 가져갑니다. ...
4. ...을 클릭하고 드롭다운 메뉴에서 **Remove user(사용자 제거)**를 선택합니다.

# AXIS Device Manager Extend

## 펌웨어 관리

---

### 펌웨어 관리

AXIS Device Manager Extend를 사용하면 각 조직에서 여러 장치의 펌웨어를 관리할 수 있습니다.

모델별로 그룹화된 조직의 모든 장치에 사용할 수 있는 펌웨어 업데이트 목록을 보려면 **Home>Firmware inventory(홈>펌웨어 인벤토리)**로 이동합니다. 특정 에지 호스트에서 사용할 수 있는 펌웨어 업데이트 목록을 보려면 에지 호스트를 선택하고 **Firmware inventory(펌웨어 인벤토리)**로 이동합니다.

### 기기 모델에 따른 펌웨어 관리

조직 전체에서 장치 모델별로 펌웨어를 관리하려면:

1. **Home > Firmware inventory(홈 > 펌웨어 인벤토리)**로 이동합니다.
2. 관리할 모델을 확인합니다.
3. **Upgrade to(다음으로 업그레이드)** 드롭다운 메뉴를 클릭하여 사용 가능한 항목을 확인하십시오. 최신 펌웨어가 미리 선택됩니다.
4. **Upgrade(업그레이드)**를 클릭합니다.

### 에지 호스트에서 장치 펌웨어를 관리합니다.

에지 호스트에 있는 일부 또는 모든 장치의 펌웨어를 관리하려면:

1. **Edge hosts(에지 호스트)**로 이동합니다.
2. 액세스하려는 에지 호스트를 클릭합니다.
3. **Devices(장치)**로 이동
4. 관리하려는 모든 기기 또는 기기만 선택합니다.
5. 작업 메뉴의 **Firmware(펌웨어)** 아이콘을 클릭
6. 목록에서 전체 또는 일부 모델을 확인하십시오.
7. 선택한 펌웨어를 변경하려면 제안된 펌웨어를 클릭하여 각 장치에서 사용할 수 있는 펌웨어를 확인하십시오. 최신 펌웨어가 미리 선택됩니다.
8. **Upgrade(업그레이드)**를 클릭합니다.

### 진행 중이거나 완료된 펌웨어 업그레이드 보기

완료된 펌웨어 업그레이드를 보려면:

1. **Sites(사이트)**로 이동합니다.
2. 액세스하려는 사이트를 클릭합니다.
3. **Tasks(작업)**으로 이동

진행 중인 펌웨어 업그레이드를 보려면:

4. **Sites(사이트)**로 이동합니다.
5. 액세스하려는 사이트를 클릭합니다.
6. **Tasks>Ongoing tasks(작업>진행 중인 작업)**으로 이동

# AXIS Device Manager Extend

## Policies(정책)

---

### Policies(정책)

정책은 장치를 자동으로 관리합니다. 사이트 전체에서 사이버 보안을 유지하기 위한 정책을 생성합니다. 장치에 앱을 자동으로 설치하고 업데이트하도록 정책을 설정할 수도 있습니다.

### 보안 정책 생성 및 적용

이 예의 사용 사례에서는 에지 호스트에 연결된 선택된 수의 장치에 기본 보안 정책을 생성하고 적용합니다. 기본 보안 정책을 생성합니다.

1. **Edge hosts(에지 호스트)**로 이동합니다.
2. 액세스하려는 에지 호스트를 클릭합니다.
3. **Devices(장치)**로 이동
4. **Policies(정책)** 옆에 있는 + 아이콘을 클릭합니다.
5. **Basic security(기본 보안)**을 선택하고 **Continue(계속)**을 클릭
6. 정책 이름 지정
7. 보안 요구 사항에 맞는 설정을 선택합니다. 권장 보안 수준의 경우 기본 설정을 유지합니다.
  - 선택한 장치의 루트 패스워드를 변경하려면 **Device root password(장치 루트 패스워드)**를 클릭하고 새 루트 패스워드를 입력합니다.
8. **Create(생성)**를 클릭합니다.

정책을 적용합니다.

1. 정책을 적용할 장치를 선택합니다.
2. 작업 메뉴의 **Policy options(정책 옵션)** 아이콘을 클릭합니다.
3. 보안 정책을 선택하고 **Save(저장)**를 클릭합니다.

### 앱 정책 생성 및 적용

이 예의 사용 사례에서는 에지 호스트에 연결된 선택된 수의 장치에 앱 정책을 생성하고 적용합니다.

1. **Edge hosts(에지 호스트)**로 이동합니다.
2. 액세스하려는 에지 호스트를 클릭합니다.
3. **Devices(장치)**로 이동
4. **Policies(정책)** 옆에 있는 + 아이콘을 클릭합니다.
5. **Apps(앱)**을 선택하고 **Continue(계속)**를 클릭
6. 정책 이름 지정
7. 장치에 설치 및 업데이트하려는 앱을 선택합니다.
8. 드롭다운 메뉴에서 업데이트 창을 선택합니다.
9. **Create(생성)**를 클릭합니다.

정책을 적용합니다.



# AXIS Device Manager Extend

## Policies(정책)

---

1. 정책을 적용할 장치를 선택합니다.
2. 작업 메뉴의 **Policy options(정책 옵션)** 아이콘을 클릭합니다.
3. 적용할 앱 정책을 선택합니다.
4. **Save(저장)**를 클릭합니다.

### 참고

선택한 앱이 제거되면 자동으로 다시 설치됩니다.

## 정책 편집

기존 정책을 편집하려면:

1. **Edge hosts(에지 호스트)**로 이동합니다.
2. 액세스하려는 에지 호스트를 클릭합니다.
3. **Devices(장치)**로 이동
4. 수정하려는 정책 옆에 있는 ...을 클릭하고 드롭다운 메뉴에서 **Edit policy(정책 편집)**를 선택합니다..
5. 필요에 맞게 정책 설정을 편집합니다.
6. **Save(저장)**를 클릭합니다.

## 정책 삭제

기존 정책을 삭제하려면:

- **Edge hosts(에지 호스트)**로 이동합니다.
- 액세스하려는 에지 호스트를 클릭합니다.
- **Devices(장치)**로 이동
- 편집하려는 정책 옆에 있는 ...을 클릭하고 드롭다운 메뉴에서 **Delete policy(정책 삭제)**를 선택합니다..
- **Delete(삭제)**를 클릭

### 참고

해당 정책이 적용된 모든 장치는 정책 설정을 유지하지만 설정은 더 이상 지속되지 않습니다.

# AXIS Device Manager Extend

## 장애 처리

---

### 장애 처리

#### 방화벽 설정을 구성하는 방법

AXIS Device Manager Extend 클라이언트는 axis.com 도메인 및 모든 하위 도메인에 대한 액세스 권한이 필요합니다.

AXIS Device Manager Extend 에지 호스트가 Axis 서비스와 통신하려면 다음 IP 주소 및 포트를 조직 방화벽의 허용 목록에 추가해야 합니다.

- 40.127.155.231(EU), 포트 443
- 52.224.128.152 및 40.127.155.231(미국), 포트 443
- 공용 DNS 서버 IP, 포트 53

또는 방화벽 설정에서 도메인 prod.adm.connect.axis.com(위의 IP 주소를 가리키는 DNS A 레코드)를 사용할 수 있습니다.

AXIS Device Manager Extend 에지 호스트는 모든 아웃바운드 요청에 prod.adm.connect.axis.com 도메인 이름을 사용합니다.

이것이 작동하려면 네트워크에서 공용 DNS 서버를 사용해야 하며 DNS 서버 IP 주소(및 기본 포트 53)로의 트래픽 아웃을 허용해야 합니다.

