# AXIS A1001 & AXIS Entry Manager

## 사용자 설명서

## 목차

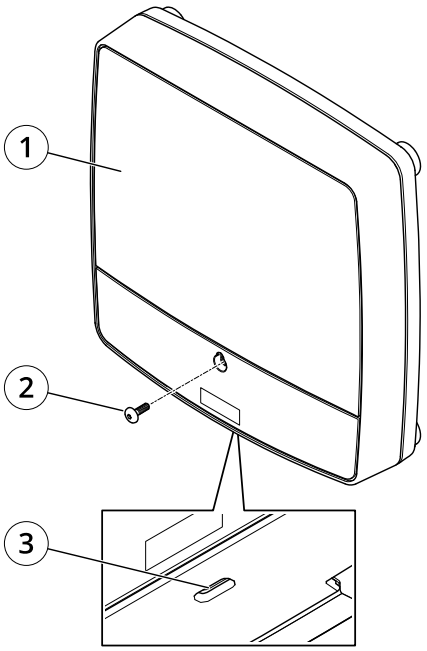
**제품 개요** ..... 4
LED 표시기 ..... 6
커넥터 및 버튼 ..... 7
**설치** ..... 9
**제품에 액세스하는 방법** ..... 10
장치 액세스 ..... 10
모바일 랜딩 페이지 정보 ..... 10
인터넷에서 제품에 액세스하는 방법 ..... 10
root 패스워드를 설정하는 방법 ..... 10
개요 페이지 ..... 11
**시스템 구성** ..... 12
구성 - 단계별 ..... 12
언어 선택 ..... 12
날짜 및 시간 설정 ..... 12
네트워크 설정 구성 ..... 14
하드웨어 구성 ..... 14
하드웨어 연결 확인 ..... 21
카드 및 형식 구성 ..... 22
서비스 구성 ..... 24
네트워크 도어 컨트롤러 관리 ..... 27
구성 모드 ..... 30
유지보수 지침 ..... 30
**접근 관리** ..... 32
사용자에 대한 정보 ..... 32
접근 관리 페이지 ..... 32
차량 종류 선택 ..... 32
접근 일정 생성 및 편집 ..... 33
그룹 생성 및 편집 ..... 35
도어 관리 ..... 35
플로어 관리 ..... 38
사용자 생성 및 편집 ..... 41
접근 일정 조합의 예 ..... 43
**알람 및 이벤트 구성** ..... 45
이벤트 로그 보기 ..... 45
알람 로그 보기 ..... 46
이벤트 및 알람 로그 구성 ..... 46
액션 룰을 설정하는 방법 ..... 47
리더 피드백 ..... 52
**보고서** ..... 53
보고서 보기, 인쇄 및 내보내기 ..... 53
**시스템 옵션** ..... 54
보안 ..... 54
날짜 및 시간 ..... 56
네트워크 ..... 56
포트 및 장치 ..... 62
유지보수 ..... 62
애플리케이션 데이터 백업 ..... 62
지원 ..... 63
고급 ..... 63
공장 출하 시 기본 설정으로 재설정 ..... 64
**장애 처리** ..... 65
현재 펌웨어를 확인하는 방법 ..... 65
펌웨어를 업그레이드하는 방법 ..... 65
긴급 복구 절차 ..... 65
증상, 가능한 원인 및 수정 조치 ..... 66
**사양** ..... 68
커넥터 ..... 68
연결 다이어그램 ..... 72

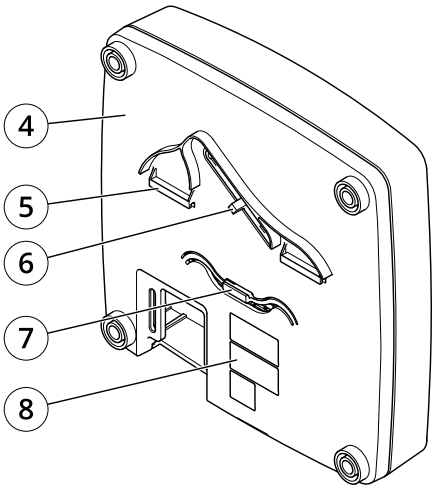
## 목차

**안전 정보** ..... 74
위험 레벨 ..... 74
기타 메시지 레벨 ..... 74

## 제품 개요

### 제품 개요

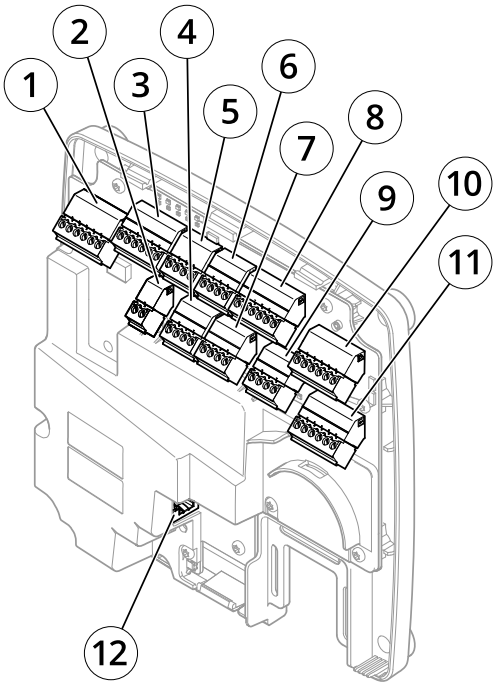



**전면/후면:**

*1 커버*
*2 커버 나사*
*3 커버 탈착 슬롯*
*4 베이스*
*5 DIN 클립 - 상부*
*6 탬퍼링 알람 스위치 - 후면*
*7 DIN 클립 - 하부*
*8 부품 번호(P/N) 및 일련 번호(S/N)*

## 제품 개요

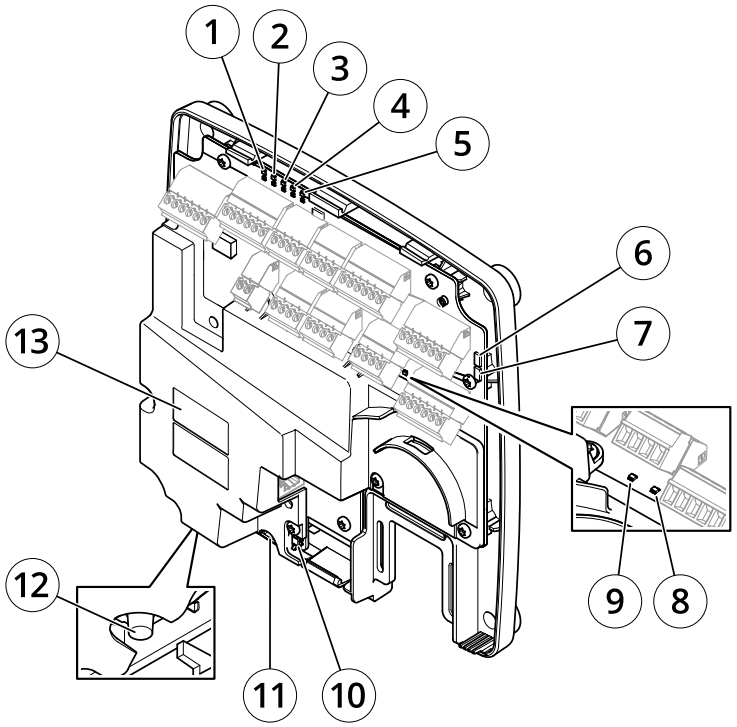



**I/O 인터페이스:**
*1 리더 데이터 커넥터(READER DATA 1)*
*10 리더 데이터 커넥터(READER DATA 2)*
*3 리더 I/O 커넥터(READER I/O 1)*
*8 리더 I/O 커넥터(READER I/O 2)*
*4 도어 커넥터(DOOR IN 1)*
*7 도어 커넥터(DOOR IN 2)*
*6 보조 커넥터(AUX)*
*5 오디오 커넥터(AUDIO)(사용되지 않음)*

**외부 전원 입력:**
*2 전원 커넥터(DC IN)*
*12 네트워크 커넥터(PoE)*

**전원 출력:**
*9 전원 잠금 커넥터(LOCK)*
*11 전원 및 릴레이 커넥터(PWR, RELAY)*

## 제품 개요




**LED 표시기, 버튼 및 기타 하드웨어:**

*1 전원 LED 표시기*
*2 상태 LED 표시기*
*3 네트워크 LED 표시기*
*4 리더 2 LED 표시기(사용되지 않음)*
*5 리더 1 LED 표시기(사용되지 않음)*
*6 탬퍼링 알람 핀 헤더 - 전면(TF)*
*7 탬퍼링 알람 핀 헤더 - 후면(TB)*
*8 잠금 LED 표시기*
*9 잠금 LED 표시기*
*10 탬퍼링 알람 센서 - 전면*
*11 SD 카드 슬롯(microSDHC)(사용되지 않음)*
*12 제어 버튼*
*13 부품 번호(P/N) 및 일련 번호(S/N)*

## LED 표시기

| LED | 컬러 | 표시 |
|---|---|---|
| 네트워크 | 녹색 | 100Mbit/s 네트워크에 연결된 경우 켜져 있습니다. 네트워크 작업 시 깜박입니다. |
| | 주황색 | 10Mbit/s 네트워크에 연결된 경우 켜져 있습니다. 네트워크 작업 시 깜박입니다. |
| | 켜져 있지 않음 | 네트워크 연결이 없습니다. |
| 상태 | 녹색 | 정상 작동 시 녹색이 계속 표시됩니다. |
| | 주황색 | 시작 시 및 설정값 복원 시 계속 표시됩니다. |
| | 빨간색 | 업그레이드에 실패한 경우 느리게 깜박입니다. |

| | | |
|---|---|---|
| 전원 | 녹색 | 정상 작동 중입니다. |
| | 주황색 | 펌웨어 업그레이드 중에는 녹색/주황색으로 깜박입니다. |
| 잠금 | 녹색 | 무전압 상태인 경우 켜져 있습니다. |
| | 빨간색 | 전압 상태인 경우 켜져 있습니다. |
| | 켜져 있지 않음 | 부동 상태입니다. |

참고

- 이벤트가 활성 상태인 동안에는 상태 LED가 깜박이도록 구성할 수 있습니다.
- 유닛 식별용으로 상태 LED가 깜박이도록 구성할 수 있습니다. **Setup > Additional Controller Configuration > System Options > Maintenance(설정 > 추가 컨트롤러 구성 > 시스템 옵션 > 유지보수)**로 이동합니다.

## 커넥터 및 버튼

### I/O 인터페이스

리더 데이터 커넥터
리더와 통신하기 위해 RS485 및 Wiegand 프로토콜을 지원하는 2개의 6핀 터미널 블록입니다. 사양은 *페이지 68* 항목을 참조하십시오.

리더 I/O 커넥터
리더 입력 및 출력용 2개의 6핀 터미널 블록입니다. 리더 I/O 커넥터는 0V DC 참조점 및 전원(DC 출력) 이외에 다음에 대한 인터페이스도 제공합니다.

- 디지털 입력 - 예를 들어, 리더 탬퍼링 알람 연결에 사용됩니다.
- 디지털 출력 - 예를 들어, 리더 호출기 및 리더 LED 연결에 사용됩니다.

사양은 *페이지 68* 항목을 참조하십시오.

도어 커넥터
도어 모니터링 장치 및 REX(종료 요청) 장치를 연결하는 2개의 4핀 터미널 블록입니다. 사양은 *페이지 69* 항목을 참조하십시오.

보조 커넥터
구성 가능한 4핀 I/O 터미널 블록입니다. 탬퍼링 알람, 이벤트 트리거링, 알람 알림 등과 함께 외부 장치에 사용합니다. 보조 커넥터는 0V DC 참조점 및 전원(DC 출력) 이외에 다음에 대한 인터페이스도 제공합니다.

- 디지털 입력 - PIR 센서 또는 유리 파손 감지기 등의 개방 회로와 폐쇄 회로 사이를 전환할 수 있는 장치를 연결하는 알람 입력입니다.
- 디지털 출력 - 절도범 알람, 사이렌 또는 조명 등의 외부 장치와 연결하는 데 사용합니다. 연결된 장치는 VAPIX® 애플리케이션 프로그래밍 인터페이스 또는 액션 룰을 통해 활성화될 수 있습니다.

사양은 *페이지 70* 항목을 참조하십시오.

### 외부 전원 입력

***통지***

차폐 네트워크 케이블(STP)을 사용하여 제품을 연결해야 합니다. 제품을 네트워크에 연결하는 모든 케이블은 특정 용도를 위한 케이블입니다. 네트워크 장치가 제조사의 지침에 따라 설치되었는지 확인하십시오. 규정 요건에 대한 자세한 내용은 항목을 참조하십시오.

전원 커넥터
DC 전원 입력용 2핀 터미널 블록입니다. 정격 출력 전력이 100W 이하로 제한되거나 정격 출력 전류가 5A 이하로 제한된 SELV(Safety Extra Low Voltage) 준수 LPS(제한된 전원)를 사용하십시오. 사양은 *페이지 70* 항목을 참조하십시오.

## 제품 개요

네트워크 커넥터
RJ45 이더넷 커넥터입니다. PoE(Power over Ethernet)를 지원합니다. 사양은 *페이지 71* 항목을 참조하십시오.

### 전원 출력

전원 잠금 커넥터

1개 또는 2개의 잠금 장치를 연결하는 4핀 터미널 블록입니다. 잠금 커넥터는 외부 장치에 전원을 공급하는 데에도 사용할 수 있습니다. 사양은 *페이지 71* 항목을 참조하십시오.

전원 및 릴레이 커넥터

전원 및 도어 컨트롤러의 릴레이를 잠금 장치 및 센서와 같은 외부 장치에 연결하는 6핀 터미널 블록입니다. 사양은 *페이지 71* 항목을 참조하십시오.

### 버튼 및 기타 하드웨어

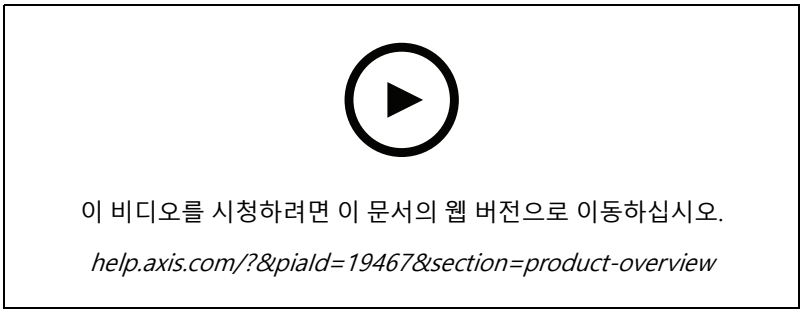
탬퍼링 알람 핀 헤더
전면 및 후면 탬퍼링 알람을 분리하는 2핀 헤더 두 개입니다. 사양은 *페이지 72* 항목을 참조하십시오.

제어 버튼
제어 버튼의 용도는 다음과 같습니다.

- 제품을 공장 출하 시 기본 설정으로 재설정합니다. *페이지 64* 항목을 참조하십시오.
- AXIS Video Hosting System 서비스에 연결합니다. *페이지 58* 항목을 참조하십시오. 연결하려면 상태 LED 가 녹색으로 깜박일 때까지 약 1초 동안 이 버튼을 누릅니다.
- AXIS Internet Dynamic DNS 서비스에 연결합니다. *페이지 58* 항목을 참조하십시오. 연결하려면 약 3 초 동안 이 버튼을 누릅니다.

## 설치

### 설치




*제품 설치 비디오*

# 제품에 액세스하는 방법

## 제품에 액세스하는 방법

Axis 제품을 설치하려면 제품과 함께 제공되는 설치 가이드를 참조하십시오.

### 장치 액세스

1. 브라우저를 열고 Axis 장치의 IP 주소 또는 호스트 이름을 입력합니다.

   IP 주소를 모르는 경우에는 AXIS IP Utility 또는 AXIS Device Manager를 사용하여 네트워크에서 장치를 찾습니다.

2. 사용자 이름과 패스워드를 입력합니다. 처음으로 장치에 액세스하는 경우 root 패스워드를 설정해야 합니다. 항목을 참조하십시오.

3. AXIS Entry Manager가 브라우저에서 열립니다. 컴퓨터를 사용하는 경우 오버뷰 페이지가 열립니다. 모바일 장치를 사용하는 경우 모바일 랜딩 페이지가 열립니다.

### 모바일 랜딩 페이지 정보

모바일 랜딩 페이지에는 도어 컨트롤러에 연결된 잠금 장치와 도어의 상태가 표시됩니다. 잠금과 잠금 해제를 테스트할 수 있습니다. 결과를 보려면 페이지를 새로 고치십시오.

링크를 클릭하면 Axis Entry Manager로 연결됩니다.

참고

- Axis Entry Manager는 모바일 장치를 지원하지 않습니다.
- 계속해서 Axis Entry Manager로 이동하면 모바일 랜딩 페이지로 돌아가는 링크가 없어집니다.

### 인터넷에서 제품에 액세스하는 방법

네트워크 라우터를 사용하면 사설 네트워크(LAN)의 제품이 인터넷 단일 연결을 공유할 수 있습니다. 이렇게 하려면 사설 네트워크에서 인터넷으로 네트워크 트래픽을 전달하면 됩니다.

대부분의 라우터는 공용 네트워크(인터넷)에서 LAN(사설 네트워크)에 액세스하는 시도를 중지하도록 사전 구성되어 있습니다.

Axis 제품이 인트라넷(LAN)에 있으며 NAT(Network Address Translator) 라우터의 다른 (WAN) 쪽에서 사용할 수 있게 하려면 **NAT 통과**를 설정합니다. NAT 통과가 적절하게 구성되면 NAT 라우터의 외부 HTTP 포트에 대한 모든 HTTP 트래픽이 제품에 전달됩니다.

**NAT 통과 기능을 설정하는 방법**

- **Setup > Additional Controller Configuration > System Options > Network > TCP/IP > Advanced(설정 > 추가 컨트롤러 구성 > 시스템 옵션 > 네트워크 > TCP/IP > 고급)**으로 이동합니다.
- **Enable(활성화)**을 클릭합니다.
- 인터넷에서 액세스를 허용하도록 NAT 라우터를 수동으로 구성합니다.

또한 *www.axiscam.net*의 AXIS Internet Dynamic DNS 서비스를 참조하십시오.

참고

- 이 문맥에서 "라우터"는 NAT 라우터, 네트워크 라우터, 인터넷 게이트웨이, 브로드밴드 라우터, 브로드밴드 공유 장치와 같은 네트워크 라우팅 장치 또는 방화벽과 같은 소프트웨어를 나타냅니다.
- NAT 통과가 작동하려면 라우터에서 NAT 통과를 지원해야 합니다. 또한 라우터가 UPnP®를 지원해야 합니다.

# 제품에 액세스하는 방법

## root 패스워드를 설정하는 방법

Axis 제품에 액세스하려면 기본 관리자 사용자 **root**에 대한 패스워드를 설정해야 합니다. 이 작업은 제품에 처음 액세스할 때 열리는 **Configure Root Password(Root 패스워드 구성)** 대화 상자에서 수행됩니다.

네트워크 도청을 방지하기 위해 암호화된 HTTPS 연결을 통해 root 패스워드를 설정할 수 있습니다. 이러한 연결에는 HTTPS 인증서가 필요합니다. HTTPS(Hypertext Transfer Protocol over SSL)는 웹 브라우저와 서버 간의 트래픽을 암호화할 때 사용되는 프로토콜입니다. HTTPS 인증서는 암호화된 정보 교환을 보장합니다. *HTTPS 페이지 54* 항목을 참조하십시오.

기본 관리자 사용자 이름 **root**는 영구적이며 삭제할 수 없습니다. root에 대한 패스워드가 기억나지 않으면 제품을 공장 출하 시 기본 설정으로 재설정해야 합니다. *공장 출하 시 기본 설정으로 재설정 페이지 64* 항목을 참조하십시오.

패스워드를 설정하려면 대화 상자에 직접 패스워드를 입력합니다.

## 개요 페이지

AXIS Entry Manager의 개요 페이지에는 도어 컨트롤러의 이름, MAC 주소, IP 주소 및 펌웨어 버전에 대한 정보가 표시됩니다. 이 페이지에서 네트워크 또는 시스템의 도어 컨트롤러를 식별할 수도 있습니다.

Axis 제품에 처음 액세스하면 개요 페이지에 하드웨어를 구성하고, 날짜 및 시간을 설정하고, 네트워크 설정을 구성하고, 도어 컨트롤러를 시스템의 일부 또는 독립 실행형 장치로 구성하라는 메시지가 나타납니다. 시스템 구성에 대한 자세한 내용은 *구성 - 단계별 페이지 12* 항목을 참조하십시오.

제품의 다른 웹 페이지에서 개요 페이지로 돌아가려면 메뉴 모음에서 **Overview(개요)**를 클릭합니다.

## 시스템 구성

제품 설정 페이지를 열려면 개요 페이지 오른쪽 위 모서리에서 **Setup(설정)**을 클릭하십시오.

Axis 제품은 관리자가 구성할 수 있습니다. 사용자 및 관리자에 대한 자세한 내용은 *페이지 32*, *페이지 41* 및 *페이지 54* 항목을 참조하십시오.

### 구성 - 단계별

접근 제어 시스템을 사용하기 전에 다음 설정 단계를 완료해야 합니다.

1. 영어가 모국어가 아닌 경우 AXIS Entry Manager에 다른 언어를 사용할 수 있습니다. *언어 선택 페이지 12* 항목을 참조하십시오.
2. 날짜 및 시간을 설정합니다. *페이지 12* 항목을 참조하십시오.
3. 네트워크 설정을 구성합니다. *페이지 14* 항목을 참조하십시오.
4. 도어 컨트롤러와 리더, 잠금 장치, 종료 요청(REX) 장치 등 연결된 장치를 구성합니다. *하드웨어 구성 페이지 14* 항목을 참조하십시오.
5. 하드웨어 연결을 확인합니다. *페이지 21* 항목을 참조하십시오.
6. 카드 및 형식을 구성합니다. *페이지 22* 항목을 참조하십시오.
7. 도어 컨트롤러 시스템을 구성합니다. *네트워크 도어 컨트롤러 관리 페이지 27* 항목을 참조하십시오.

시스템의 도어, 일정, 사용자 및 그룹을 구성하고 관리하는 방법에 대한 자세한 내용은 *접근 관리 페이지 32* 항목을 참조하십시오.

유지보수 권장 사항에 대한 자세한 내용은 *유지보수 지침 페이지 30* 항목을 참조하십시오.

참고

도어 컨트롤러를 추가 또는 제거하거나 사용자를 추가, 제거 또는 편집하거나 하드웨어를 구성하려면 시스템의 도어 컨트롤러 중 반 이상이 **온라인** 상태여야 합니다. 도어 컨트롤러 상태를 확인하려면 **Setup > Manage Network Door Controllers in System(설정 > 시스템의 네트워크 도어 컨트롤러 관리)**으로 이동합니다.

### 언어 선택

AXIS Entry Manager의 기본 언어는 영어이지만 제품의 펌웨어에 포함된 다른 언어로 전환할 수 있습니다. 사용 가능한 최신 펌웨어에 대한 정보는 *www.axis.com*을 참조하십시오.

제품 웹 페이지에서 언어를 전환할 수 있습니다.

언어를 전환하려면 언어 드롭다운 목록  을 클릭하고 언어를 선택합니다. 모든 제품의 웹 페이지와 도움말 페이지가 선택된 언어로 표시됩니다.

참고

- 언어를 전환하면 날짜 형식도 선택한 언어에서 일반적으로 사용되는 형식으로 변경됩니다. 올바른 형식이 데이터 필드에 표시됩니다.
- 제품을 공장 출하 시 기본값으로 재설정하면 AXIS Entry Manager가 다시 영어로 전환됩니다.
- 제품을 복구하는 경우 AXIS Entry Manager에서는 선택된 언어가 계속 사용됩니다.
- 제품을 재시작하는 경우 AXIS Entry Manager에서는 선택된 언어가 계속 사용됩니다.
- 펌웨어를 업그레이드하는 경우 AXIS Entry Manager에서는 선택된 언어가 계속 사용됩니다.

## 날짜 및 시간 설정

도어 컨트롤러가 시스템의 일부일 경우 날짜 및 시간 설정이 모든 도어 컨트롤러에 배포됩니다. 즉, NTP 서버와 동기화하는지, 날짜 및 시간을 수동으로 설정하는지 또는 컴퓨터의 날짜 및 시간을 가져오는지에 관계없이 설정이 시스템의 다른 컨트롤러에 푸시됩니다. 변경 내용이 보이지 않으면 브라우저에서 페이지를 새로 고쳐 보십시오. 도어 컨트롤러 시스템 관리에 대한 자세한 내용은 *네트워크 도어 컨트롤러 관리 페이지 27* 항목을 참조하십시오.

Axis 제품의 날짜 및 시간을 설정하려면 **Setup > Date & Time(설정 > 날짜 및 시간)**으로 이동합니다.

다음 방법으로 날짜 및 시간을 설정할 수 있습니다.

- NTP(Network Time Protocol) 서버에서 날짜와 시간을 가져옵니다. *페이지 13* 항목을 참조하십시오.
- 수동으로 날짜 및 시간을 설정합니다. *페이지 13* 항목을 참조하십시오.
- 컴퓨터에서 날짜 및 시간을 가져옵니다. *페이지 13* 항목을 참조하십시오.

**Current controller time(현재 컨트롤러 시간)**은 도어 컨트롤러의 현재 날짜와 시간(24시간제)을 표시합니다.

날짜 및 시간의 동일한 옵션을 시스템 옵션 페이지에서도 사용할 수 있습니다. **설정 > 추가 컨트롤러 구성 > 시스템 옵션 > 날짜 및 시간**으로 이동합니다.

### NTP(Network Time Protocol) 서버에서 날짜 및 시간 가져오기

1. **Setup > Date & Time(설정 > 날짜 및 시간)**으로 이동합니다.
2. 드롭다운 목록에서 **Timezone(시간대)**을 선택합니다.
3. 해당 지역에서 일광 절약 시간제를 사용하는 경우 **Adjust for daylight saving(일광 절약 시간 조정)**을 선택합니다.
4. **Synchronize with NTP(NTP와 동기화)**를 선택합니다.
5. 기본 DHCP 주소를 선택하거나 NTP 서버 주소를 입력합니다.
6. **Save(저장)**를 클릭합니다.

NTP 서버와 동기화할 때는 NTP 서버에서 데이터가 푸시되므로 날짜와 시간이 계속 업데이트됩니다. NTP 설정에 대한 자세한 내용은 *NTP 구성 페이지 59* 항목을 참조하십시오.

NTP 서버에 호스트 이름을 사용할 경우 DNS 서버를 구성해야 합니다. *DNS 구성 페이지 58* 항목을 참조하십시오.

### 수동으로 날짜 및 시간 설정

1. **Setup > Date & Time(설정 > 날짜 및 시간)**으로 이동합니다.
2. 해당 지역에서 일광 절약 시간제를 사용하는 경우 **Adjust for daylight saving(일광 절약 시간 조정)**을 선택합니다.
3. **Set date & time manually(수동으로 날짜 및 시간 설정)**를 선택합니다.
4. 원하는 날짜와 시간을 입력합니다.
5. **Save(저장)**를 클릭합니다.

수동으로 날짜와 시간을 설정하는 경우 날짜와 시간이 한 번 설정되고 자동으로 업데이트되지 않습니다. 즉, 날짜 또는 시간을 업데이트해야 하는 경우 외부 NTP 서버에 연결되어 있지 않으므로 수동으로 변경해야 합니다.

### 컴퓨터에서 날짜 및 시간 가져오기

1. **Setup > Date & Time(설정 > 날짜 및 시간)**으로 이동합니다.
2. 해당 지역에서 일광 절약 시간제를 사용하는 경우 **Adjust for daylight saving(일광 절약 시간 조정)**을 선택합니다.

3. **Set date & time manually(수동으로 날짜 및 시간 설정)**를 선택합니다.
4. **Sync now and save(지금 동기화 및 저장)**를 클릭합니다.

컴퓨터 시간을 사용할 때는 날짜와 시간이 컴퓨터 시간과 한 번 동기화되고 자동으로 업데이트되지 않습니다. 즉, 시스템 관리에 사용하는 컴퓨터에서 날짜나 시간을 변경하면 다시 동기화해야 합니다.

## 네트워크 설정 구성

기본 네트워크 설정을 구성하려면 **Setup > Network Settings(설정 > 네트워크 설정)** 또는 **Setup > Additional Controller Configuration > System Options > Network > TCP/IP > Basic(설정 > 추가 컨트롤러 구성 > 시스템 옵션 > 네트워크 > TCP/IP > 기본)**으로 이동합니다.

네트워크 설정에 대한 자세한 내용은 *네트워크 페이지 56* 항목을 참조하십시오.

## 하드웨어 구성

도어 및 바닥을 관리하기 전에 하드웨어 구성 페이지에서 하드웨어를 구성해야 합니다.

하드웨어 구성을 완료하기 전에도 리더, 잠금 장치 및 기타 장치를 Axis 제품에 연결할 수 있습니다. 그러나 하드웨어 구성을 먼저 완료하면 장치에 더 쉽게 연결할 수 있습니다. 왜냐하면 구성을 완료했을 때 하드웨어 핀 차트를 사용할 수 있기 때문입니다. 하드웨어 핀 차트는 장치를 핀에 연결하는 방법을 알려주며, 유지보수를 위한 참조 시트로 사용할 수 있습니다. 유지보수 지침은 *페이지 30* 항목을 참조하십시오.

처음으로 하드웨어를 구성하는 경우 다음 방법 중 하나를 선택합니다.

- 하드웨어 구성 파일을 가져옵니다. *페이지 14* 항목을 참조하십시오.
- 새 하드웨어 구성을 만듭니다. *페이지 15* 항목을 참조하십시오.

참고

이전에 제품의 하드웨어를 구성하지 않았거나 삭제한 경우 **Hardware Configuration(하드웨어 구성)**은 개요 페이지의 알림 패널에서 사용할 수 있습니다.

### 하드웨어 구성 파일을 가져오는 방법

하드웨어 구성 파일을 가져오면 Axis 제품의 하드웨어 구성을 더 빠르게 완료할 수 있습니다.

한 제품에서 파일을 내보내고 다른 제품으로 파일을 가져오면 동일한 단계를 여러 번 반복하지 않고 동일한 하드웨어 설정의 여러 복사본을 만들 수 있습니다. 또한 내보낸 파일을 백업으로 저장할 수 있으며, 해당 파일을 사용하여 이전 하드웨어 구성을 복구할 수 있습니다. 자세한 내용은 *하드웨어 구성 파일을 내보내는 방법 페이지 14* 항목을 참조하십시오.

하드웨어 구성 파일을 가져오려면

1. **Setup > Hardware Configuration(설정 > 하드웨어 구성)**으로 이동합니다.
2. **Import hardware configuration(하드웨어 구성 가져오기)**을 클릭하거나 하드웨어 구성이 이미 있는 경우 **Reset and import hardware configuration(하드웨어 구성 재설정 및 가져오기)**을 클릭합니다.
3. 표시되는 파일 브라우저 대화 상자에서 컴퓨터의 하드웨어 구성 파일(*.json)을 찾아 선택합니다.
4. **OK(확인)**를 클릭합니다.

### 하드웨어 구성 파일을 내보내는 방법

Axis 제품의 하드웨어 구성을 내보내 같은 하드웨어 설정의 여러 복사본을 만들 수 있습니다. 또한 내보낸 파일을 백업으로 저장할 수 있으며, 해당 파일을 사용하여 이전 하드웨어 구성을 복구할 수 있습니다.

참고

플로어의 하드웨어 구성은 내보낼 수 없습니다.

무선 잠금 설정은 하드웨어 구성 내보내기에 포함되지 않습니다.

하드웨어 구성 파일을 내보내려면

1. **Setup > Hardware Configuration(설정 > 하드웨어 구성)**으로 이동합니다.
2. **Export hardware configuration(하드웨어 구성 내보내기)**을 클릭합니다.
3. 브라우저에 따라 대화 상자에서 내보내기를 완료해야 할 수도 있습니다.

   별도로 지정하지 않는 한 내보낸 파일(*.json)이 기본 다운로드 폴더에 저장됩니다. 웹 브라우저 사용자 설정에서 다운로드 폴더를 선택할 수 있습니다.

## 새 하드웨어 구성 만들기

요구 사항에 대한 지침을 따르십시오.

- *주변 장치가 없는 새 하드웨어 구성을 만드는 방법 페이지 15*
- *무선 잠금 장치에 대한 새 하드웨어 구성을 만드는 방법 페이지 19*
- *엘리베이터 제어를 통해 새 하드웨어 구성을 만드는 방법(AXIS A9188) 페이지 19*

## 주변 장치가 없는 새 하드웨어 구성을 만드는 방법

1. **Setup > Hardware Configuration(설정 > 하드웨어 구성)**으로 이동하고 **Start new hardware configuration(새 하드웨어 구성 시작)**을 클릭합니다.
2. Axis 제품의 이름을 입력합니다.
3. 연결된 도어의 수를 선택하고 **Next(다음)**를 클릭합니다.
4. 요구 사항에 따라 도어 모니터(도어 위치 센서) 및 잠금 장치를 구성하고 **Next(다음)**를 클릭합니다. 사용 가능한 옵션에 대한 자세한 내용은 *도어 모니터 및 잠금을 구성하는 방법 페이지 15* 항목을 참조하십시오.
5. 사용할 리더 및 REX 장치를 구성하고 **Finish(마침)**를 클릭합니다. 사용 가능한 옵션에 대한 자세한 내용은 *리더 및 REX 장치 구성 방법 페이지 18* 항목을 참조하십시오.
6. **Close(닫기)**를 클릭하거나 링크를 클릭하여 하드웨어 핀 차트를 봅니다.

### 도어 모니터 및 잠금을 구성하는 방법

새 하드웨어 구성에서 도어 옵션을 선택한 경우 도어 모니터 및 잠금을 구성할 수 있습니다.

1. 도어 모니터를 사용할 경우 **Door monitor(도어 모니터)**를 선택한 다음 도어 모니터 회로 연결 방법과 일치하는 옵션을 선택합니다.
2. 도어가 열리는 즉시 도어 잠금이 잠겨야 할 경우 **Cancel access time once door is opened(도어가 열리면 접근 시간 취소)**를 선택합니다.

   다시 잠금을 지연하려면 **Relock time(다시 잠금 시간)**에서 지연 시간을 밀리초 단위로 설정합니다.
3. 도어 모니터 시간 옵션을 지정하거나 도어 모니터를 사용하지 않을 경우 잠금 시간 옵션을 지정합니다.
4. 잠금 회로가 연결되는 방법과 일치하는 옵션을 선택합니다.
5. 잠금 모니터를 사용할 경우 **Lock monitor(잠금 모니터)**를 선택한 다음 잠금 모니터 회로 연결 방법과 일치하는 옵션을 선택합니다.

6. 리더, REX 장치 및 도어 모니터의 입력 연결을 관리해야 할 경우 **Enable supervised inputs(관리된 입력 활성화)**를 선택합니다.

   자세한 내용은 *관리된 입력을 사용하는 방법 페이지 18* 항목을 참조하십시오.

참고

- 대부분의 잠금, 도어 모니터 및 리더 옵션은 새 하드웨어 구성을 재설정 및 시작하지 않고 변경할 수 있습니다. **Setup > Hardware Reconfiguration(설정 > 하드웨어 재구성)**으로 이동합니다.
- 도어 컨트롤러당 하나의 잠금 모니터를 연결할 수 있습니다. 따라서 이중 잠금 도어를 사용하는 경우 잠금 중 하나에만 잠금 모니터가 있습니다. 동일한 컨트롤러에 두 개의 도어가 연결된 경우 잠금 모니터를 사용할 수 없습니다.
- 전동 잠금은 보조 잠금으로 구성해야 합니다.

**도어 모니터 및 시간 옵션 정보**

다음과 같은 도어 모니터 옵션을 사용할 수 있습니다.

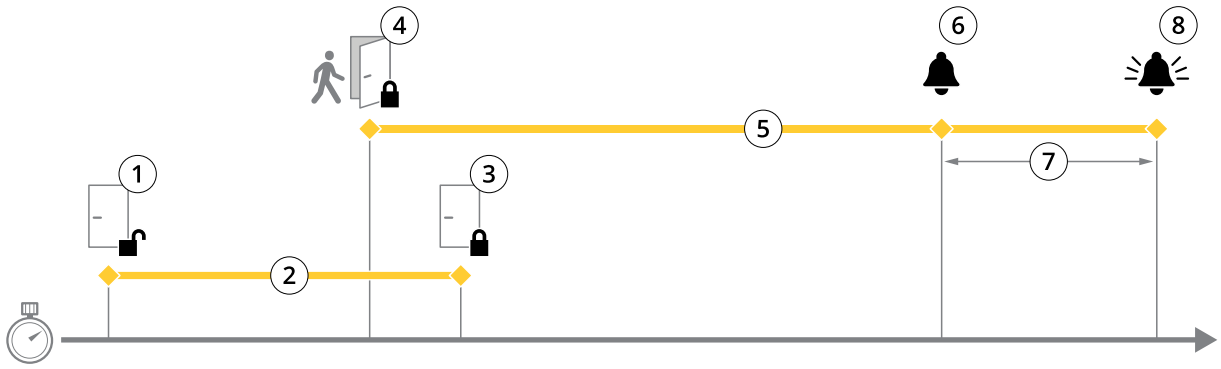
- **Door monitor(도어 모니터)** - 기본적으로 선택됩니다. 도어마다 자체 도어 모니터가 있어서 도어가 강제로 열렸거나 너무 오래 열려 있으면 신호를 보내는 등의 역할을 합니다. 도어 모니터를 사용하지 않으려면 선택을 취소하십시오.
  - **Open circuit = Closed door(개방 회로 = 폐쇄 도어)** - 도어 모니터 회로가 정상 개방된 경우 선택합니다. 회로가 닫히면 도어 모니터가 도어 개방 신호를 제공합니다. 회로가 열리면 도어 모니터가 도어 폐쇄 신호를 제공합니다.
  - **Open circuit = Open door(개방 회로 = 개방 도어)** - 도어 모니터 회로가 정상 폐쇄된 경우 선택됩니다. 회로가 열리면 도어 모니터가 도어 개방 신호를 제공합니다. 회로가 닫히면 도어 모니터가 도어 폐쇄 신호를 제공합니다.
- **Cancel access time once door is opened(도어가 열리면 접근 시간 취소)** - 다른 사람을 뒤따라 들어가는 행동을 방지하려면 선택합니다. 도어 모니터에서 도어가 열렸음을 나타내는 즉시 잠금 장치가 잠깁니다.

다음과 같은 도어 시간 옵션을 항상 사용할 수 있습니다.

- **Access time(접근 시간)** - 접근이 허용된 후 도어 잠금이 해제된 상태로 유지될 시간(초)을 설정합니다. 도어가 열릴 때까지 또는 설정 시간에 도달할 때까지 도어가 잠금 해제 상태로 유지됩니다. 접근 시간이 만료되었는지 여부에 관계없이 도어가 닫히면 도어가 잠깁니다.
- **Long access time(긴 접근 시간)** - 접근이 허용된 후 도어 잠금이 해제된 상태로 유지될 시간(초)을 설정합니다. 긴 접근 시간은 이미 설정된 접근 시간보다 우선하며 긴 접근 시간이 선택된 사용자에게 적용됩니다. *사용자 자격 증명 페이지 41* 항목을 참조하십시오.

다음과 같은 도어 시간 옵션을 사용할 수 있게 하려면 **Door monitor(도어 모니터)**를 선택하십시오.

- **Open too long time(장시간 개방)** - 도어를 열어 놓을 수 있는 시간(초)을 설정합니다. 설정된 시간에 도달했을 때 도어가 여전히 열려 있으면 도어 장시간 개방 알람이 트리거됩니다. 장시간 개방 이벤트가 트리거되는 액션을 구성하려면 액션 룰을 설정합니다.
- **Pre-alarm time(사전 알람 시간)** - 사전 알람은 장시간 개방에 도달하기 전에 트리거되는 경고 신호입니다. 관리자에게 알리고, 액션 룰이 설정된 방법에 따라 도어 출입자에게 도어 장시간 개방 알람이 울리지 않게 하려면 도어를 닫아야 한다는 사실을 경고합니다. 도어 장시간 개방 알람이 트리거되기 전에 시스템에서 사전 알람 경고 신호를 보낼 시간(초)을 설정합니다. 사전 알람을 비활성화하려면 사전 알람 시간을 0으로 설정하십시오.




1 *접근 권한 부여됨 - 잠금 장치 잠금 해제*
2 *접근 시간*
3 *취한 액션 없음 - 잠금 장치 잠금*
4 *취한 액션(도어 열림) - 도어가 닫힐 때까지 잠금 장치 잠금 또는 잠금 해제 유지*
5 *장시간 개방*
6 *사전 알람 해제*
7 *사전 알람 시간*
8 *장시간 개방 알람 해제*

액션 룰을 설정하는 방법에 대한 자세한 내용은 *액션 룰을 설정하는 방법 페이지 47* 항목을 참조하십시오.

**잠금 옵션에 대한 정보**

다음과 같은 잠금 회로 옵션을 사용할 수 있습니다.

- **12V**
  - **Fail-secure(페일 시큐어)** - 정전 중에 잠금 상태를 유지하려는 경우에 선택합니다. 전류를 공급하면 잠금이 해제됩니다.
  - **Fail-safe(페일 세이프)** - 정전 중에 잠금을 해제하려는 경우에 선택합니다. 전류를 공급하면 잠깁니다.
- **Relay(릴레이)** - 도어 컨트롤러당 하나의 잠금 장치에만 사용할 수 있습니다. 두 개의 도어가 도어 컨트롤러에 연결된 경우 두 번째 도어의 잠금 장치에만 릴레이를 사용할 수 있습니다.
  - **Relay open = Locked(릴레이 개방 = 잠금)** - 릴레이가 개방될 때 잠금 상태를 유지하려는 경우에 선택합니다(페일 시큐어). 릴레이가 닫히면 잠금 해제됩니다.
  - **Relay open = Unlocked(릴레이 개방 = 잠금 해제)** - 정전 중에 잠금을 해제하려는 경우에 선택합니다(페일 세이프). 릴레이가 닫히면 잠깁니다.
- **None(없음)** - 잠금 장치 2에만 사용할 수 있습니다. 잠금 장치를 하나만 사용할 경우에 선택합니다.

단일 도어 구성에서는 다음과 같은 잠금 모니터 옵션을 사용할 수 있습니다.

- **Lock monitor(잠금 모니터)** - 잠금 모니터 제어를 사용하려면 선택합니다. 그런 다음 모니터링할 잠금 장치를 선택합니다. 잠금 모니터는 이중 잠금 도어에만 사용할 수 있으며 도어 컨트롤러에 두 개의 도어가 연결된 경우에는 사용할 수 없습니다.
  - **Open circuit = Locked(개방 회로 = 잠금)** - 잠금 모니터 회로가 정상적으로 닫히는 경우에 선택합니다. 잠금 모니터는 회로가 닫히면 도어 잠금 해제 신호를 제공합니다. 잠금 모니터는 회로가 열리면 도어 잠금 신호를 제공합니다.
  - **Open circuit = Unlocked(개방 회로 = 잠금 해제)** - 잠금 모니터 회로가 정상적으로 열리는 경우에 선택합니다. 잠금 모니터는 회로가 열리면 도어 잠금 해제 신호를 제공합니다. 잠금 모니터는 회로가 닫히면 도어 잠금 신호를 제공합니다.

## 시스템 구성

### 리더 및 REX 장치 구성 방법

새로운 하드웨어 구성에서 도어 모니터와 잠금 장치를 구성한 경우 리더와 REX(종료 요청) 장치를 구성할 수 있습니다.

1. 리더를 사용하려면 확인란을 선택한 후 리더의 통신 프로토콜에 맞는 옵션을 선택합니다.
2. 버튼, 센서, 푸시 바 등의 REX 장치를 사용하려면 확인란을 선택한 후 REX 장치의 회로가 연결되는 방법에 맞는 옵션을 선택합니다.

   REX 신호가 도어 개방에 영향을 주지 않을 경우(예: 기계식 손잡이나 푸시 바가 있는 도어) **REX does not unlock door(REX가 도어 잠금을 해제하지 않음)**를 선택합니다.
3. 둘 이상의 리더나 REX 장치를 도어 컨트롤러에 연결하는 경우 각 리더나 REX 장치의 설정이 올바르게 될 때까지 앞의 두 단계를 다시 수행합니다.

### 리더 및 REX 장치 옵션에 대한 정보

다음과 같은 리더 옵션을 사용할 수 있습니다.

- **Wiegand** - Wiegand 프로토콜을 사용하는 리더에 대해 선택합니다. 그런 다음 리더에서 지원되는 LED 컨트롤을 선택합니다. 단일 LED 컨트롤을 가진 리더는 일반적으로 빨간색과 녹색 사이에서 전환됩니다. 이중 LED 컨트롤을 가진 리더는 빨간색 LED와 녹색 LED에 서로 다른 와이어를 사용합니다. 즉, LED가 서로 독립적으로 제어됩니다. 두 LED가 모두 켜질 경우 표시등이 주황색으로 보입니다. 리더에서 지원하는 LED 컨트롤은 제조업체의 정보를 참조하십시오.
- **OSDP, RS485 반이중** - 반이중을 지원하는 RS485 리더에 대해 선택합니다. 리더에서 지원하는 프로토콜은 제조업체의 정보를 참조하십시오.

다음 REX 장치 옵션을 사용할 수 있습니다.

- **Active low(액티브 로우)** - REX 장치를 활성화하면 회로가 폐쇄되는 경우에 선택합니다.
- **Active high(액티브 하이)** - REX 장치를 활성화하면 회로가 개방되는 경우에 선택합니다.
- **REX does not unlock door(REX가 도어 잠금을 해제하지 않음)** - REX 신호가 도어 개방에 영향을 주지 않을 경우(예: 기계식 손잡이나 푸시 바가 있는 도어)에 선택합니다. 사용자가 접근 시간 내에 도어를 여는 경우에는 도어 강제 열림 알람이 트리거되지 않습니다. 사용자가 REX 장치를 활성화하면 도어 잠금을 자동으로 해제해야 하는 경우에는 선택 취소하십시오.

참고

대부분의 잠금, 도어 모니터 및 리더 옵션은 새 하드웨어 구성을 재설정 및 시작하지 않고 변경할 수 있습니다. **Setup > Hardware Reconfiguration(설정 >하드웨어 재구성)**으로 이동합니다.

### 관리된 입력을 사용하는 방법

관리된 입력은 도어 컨트롤러와 리더, REX 장치, 도어 모니터 간의 연결 상태를 보고합니다. 연결이 중단되면 이벤트가 활성화됩니다.

관리된 입력을 사용하려면

1. 사용되는 모든 관리된 입력에 EOL 레지스터를 설치합니다. *페이지 73*에서 연결 다이어그램을 참조하십시오.
2. **Setup > Hardware Reconfiguration(설정 > 하드웨어 재구성)**으로 이동하여 **Enable supervised inputs(관리된 입력 활성화)**를 선택합니다. 하드웨어 구성 중에 관리된 입력을 활성화할 수도 있습니다.

### 관리된 입력 호환성에 대한 정보

다음 커넥터는 관리된 입력을 지원합니다.

- 리더 I/O 커넥터 - 탬퍼링 신호. *페이지 68* 항목을 참조하십시오.
- 도어 커넥터. *페이지 69* 항목을 참조하십시오.

관리된 입력과 함께 사용할 수 있는 리더와 스위치는 다음과 같습니다.

- 내부 1kΩ 풀업 ~ 5V를 사용하는 리더 및 스위치
- 내부 풀업을 사용하지 않는 리더 및 스위치

### 무선 잠금 장치에 대한 새 하드웨어 구성을 만드는 방법

1. **Setup > Hardware Configuration(설정 > 하드웨어 구성)**으로 이동하고 **Start new hardware configuration(새 하드웨어 구성 시작)**을 클릭합니다.
2. Axis 제품의 이름을 입력합니다.
3. 주변 장치 목록에서 무선 게이트웨이의 제조업체를 선택합니다.
4. 유선 도어를 연결하려면 **1 Door(도어 1)** 확인란을 선택하고 **Next(다음)**를 클릭합니다. 도어가 포함되지 않으면 **Finish(마침)**를 클릭합니다.
5. 사용하는 잠금 장치 제조업체를 기준으로 다음 글머리 기호 목록 중 하나에 따라 진행합니다.
   - **ASSA Aperio**: 하드웨어 핀 차트를 보려면 링크를 클릭하고, 구성을 완료하려면 **Close(닫기)**를 클릭하고 **Setup > Hardware Reconfiguration(설정 > 하드웨어 재구성)**으로 이동합니다. *Assa Aperio™ 도어 및 장치 추가 페이지 19* 항목을 참조하십시오.
   - **SmartIntego**: 하드웨어 핀 차트를 보려면 링크를 클릭하고, 구성을 완료하려면 **Click here to select wireless gateway and configure doors(무선 게이트웨이를 선택하고 도어를 구성하려면 여기를 클릭)**를 클릭합니다. *SmartIntego를 구성하는 방법 페이지 27* 항목을 참조하십시오.

#### Assa Aperio™ 도어 및 장치 추가

시스템에 무선 도어를 추가하기 전에 Aperio PAP(Aperio 프로그래밍 애플리케이션 도구)를 사용하여 연결된 Assa Aperio 커뮤니케이션 허브와 결합해야 합니다.

무선 도어를 추가하려면

1. **Setup(설정)** > **Hardware Reconfiguration(하드웨어 재구성)**으로 이동합니다.
2. 무선 도어 및 장치에서 **Add door(도어 추가)**를 클릭합니다.
3. **Door name(도어 이름)** 필드에 설명이 포함된 이름을 입력합니다.
4. **Lock(잠금)**의 **ID** 필드에 추가하려는 장치의 6자리 주소를 입력합니다. 장치 주소는 제품 라벨에 인쇄되어 있습니다.
5. 원하는 경우 **Door position sensor(도어 위치 센서)**에서 **Built in door position sensor(내장 도어 위치 센서)** 또는 **External door position sensor(외부 도어 위치 센서)**를 선택합니다.

참고

외부 DPS(도어 위치 센서)를 사용하는 경우 이를 구성하기 전에 Aperio 잠금 장치가 도어 핸들 상태 감지를 지원하는지 확인하십시오.

6. 선택 사항으로 **Door position sensor(도어 위치 센서)**의 **ID** 필드에 추가하려는 장치의 6자리 주소를 입력합니다. 장치 주소는 제품 라벨에 인쇄되어 있습니다.
7. **Add(추가)**를 클릭합니다.

### 엘리베이터 제어를 통해 새 하드웨어 구성을 만드는 방법(AXIS A9188)

중요 사항

HW 구성을 생성하기 전에 AXIS A9188 Network I/O Relay Module에서 사용자를 추가해야 합니다. A9188 웹 인터페이스 > **Preferences > Additional device configuration > Basic setup > Users > Add > User setup(기본 설정 > 추가 장치 구성 > 기본 설정 > 사용자 > 추가 > 사용자 설정)**으로 이동합니다.

참고

각 Axis 네트워크 도어 컨트롤러를 통해 최대 2개의 AXIS 9188 Network I/O Relay Module을 구성할 수 있습니다.

1. A1001에서 **Setup > Hardware Configuration(설정 > 하드웨어 구성)**으로 이동하고 **Start new hardware configuration(새 하드웨어 구성 시작)**을 클릭합니다.
2. Axis 제품의 이름을 입력합니다.
3. 주변 장치 목록에서 **Elevator control(엘리베이터 제어)**을 선택하여 AXIS A9188 Network I/O Relay Module을 포함하고 **Next(다음)**를 클릭합니다.
4. 연결된 리더 이름을 입력합니다.
5. 사용할 리더 프로토콜을 선택하고 **Finish(마침)**를 클릭합니다.
6. 구성을 완료하려면 **Network Peripherals(네트워크 주변 장치)**를 클릭하고(*네트워크 주변 장치를 추가하고 설정하는 방법 페이지 20* 참조), 하드웨어 핀 차트로 이동하려면 링크를 클릭합니다.

## 네트워크 주변 장치를 추가하고 설정하는 방법

중요 사항

- 네트워크 주변 장치를 설정하기 전에 AXIS A9188 Network I/O Relay Module에서 사용자를 추가해야 합니다. AXIS A9188 웹 인터페이스 > **Preferences > Additional device configuration > Basic setup > Users > Add > User setup(기본 설정 > 추가 장치 구성 > 기본 설정 > 사용자 > 추가 > 사용자 설정)**으로 이동합니다.
- 다른 AXIS A1001 Network Door Controller를 네트워크 주변 장치로 추가하지 마십시오.

1. **Setup > Network Periphals(설정 > 네트워크 주변 장치)**로 이동하여 장치를 추가합니다.
2. **Discovered devices(검색된 장치)**에서 장치를 찾습니다.
3. **Add this device(이 장치 추가)**를 클릭합니다.
4. 장치의 이름을 입력합니다.
5. AXIS A9188 사용자 이름과 패스워드를 입력합니다.
6. **Add(추가)**를 클릭합니다.

참고

**Manually add device(수동으로 장치 추가)** 대화 상자에서 MAC 주소 또는 IP 주소를 입력하여 수동으로 네트워크 주변 장치를 추가할 수 있습니다.

중요 사항

스케줄을 삭제하려면 먼저 네트워크 I/O 릴레이 모듈에서 스케줄을 사용하지 않는지 확인하십시오.

### 네트워크 주변 장치에서 I/O 및 릴레이를 설정하는 방법

중요 사항

네트워크 주변 장치를 설정하기 전에 AXIS A9188 Network I/O Relay Module에서 사용자를 추가해야 합니다. AXIS A9188 웹 인터페이스 > **Preferences > Additional device configuration > Basic setup > Users > Add > User setup(기본 설정 > 추가 장치 구성 > 기본 설정 > 사용자 > 추가 > 사용자 설정)**으로 이동합니다.

1. **Setup > Network Periphals(설정 > 네트워크 주변 장치)**로 이동하고 **Added devices(추가된 장치)** 행을 클릭합니다.
2. 플로어로 설정할 I/O 및 릴레이를 선택합니다.
3. **Set as floor(플로어로 설정)**를 클릭하고 이름을 입력합니다.

4. **Add(추가)**를 클릭합니다.

이제 **Access Management(접근 관리)** 아래의 **Floor(플로어)** 탭에 해당 플로어가 표시됩니다.

참고

AXIS Entry Manager에서 최대 16개 플로어를 추가할 수 있습니다.

## 하드웨어 연결 확인

하드웨어 설치 및 구성이 완료되고 도어 컨트롤러 수명 중 언제든지 연결된 도어 모니터, 네트워크 I/O 릴레이 모듈, 잠금 장치 및 리더의 기능을 확인할 수 있습니다.

구성을 확인하고 확인 컨트롤에 액세스하려면 **Setup > Hardware Connection Verification(설정 > 하드웨어 연결 확인)**으로 이동합니다.

### 컨트롤 도어 확인

- **Door state(도어 상태)** - 도어 모니터, 도어 알람 및 잠금 장치의 현재 상태를 확인합니다. **Get current state(현재 상태 가져오기)**를 클릭합니다.
- **Lock(잠금)** - 수동으로 잠금을 트리거합니다. 기본 잠금과 보조 잠금(있을 경우)에 모두 적용됩니다. **Lock(잠금)** 또는 **Unlock(잠금 해제)**을 클릭합니다.
- **Lock(잠금)** - 접근할 수 있도록 잠금을 수동으로 트리거합니다. 기본 잠금에만 적용됩니다. **Access(접근)**를 클릭합니다.
- **Reader: Feedback(리더: 피드백)** - 리더 피드백(예: 다양한 명령을 나타내는 사운드 및 LED 신호)을 확인합니다. 명령을 선택하고 **Test(테스트)**를 클릭합니다. 사용할 수 있는 피드백 유형은 리더에 따라 달라집니다. 자세한 내용은 *리더 피드백 페이지 52* 항목을 참조하십시오. 또한 제조업체 지침을 참조하십시오.
- **Reader: Tampering(리더: 탬퍼링)** - 마지막 탬퍼링 시도에 대한 정보를 가져옵니다. 리더가 설치되면 첫 번째 탬퍼링 시도가 등록됩니다. **Get last tampering(마지막 탬퍼링 가져오기)**을 클릭합니다.
- **Reader: Card swipe(리더: 카드 긁기)** - 마지막에 긁은 카드 또는 리더에서 수락한 다른 유형의 사용자 토큰에 대한 정보를 가져옵니다. **Get last credential(마지막 자격 증명 가져오기)**을 클릭합니다.
- **REX** - 장치 종료 요청(REX)이 마지막으로 제기된 시간에 대한 정보를 가져옵니다. **Get last REX(마지막 REX 가져오기)**를 클릭합니다.

### 컨트롤 플로어 확인

- **Floor state(플로어 상태)** - 플로어 접근의 현재 상태를 확인합니다. **Get current state(현재 상태 가져오기)**를 클릭합니다.
- **Floor lock & unlock(플로어 잠금 및 잠금 해제)** - 플로어 접근을 수동으로 트리거합니다. 기본 잠금과 보조 잠금(있을 경우)에 모두 적용됩니다. **Lock(잠금)** 또는 **Unlock(잠금 해제)**을 클릭합니다.
- **Floor access(플로어 접근)** - 수동으로 임시 접근 권한을 플로어에 부여합니다. 기본 잠금에만 적용됩니다. **Access(접근)**를 클릭합니다.
- **Elevator Reader: Feedback(엘리베이터 리더: 피드백)** - 리더 피드백(예: 다양한 명령을 나타내는 사운드 및 LED 신호)을 확인합니다. 명령을 선택하고 **Test(테스트)**를 클릭합니다. 사용할 수 있는 피드백 유형은 리더에 따라 달라집니다. 자세한 내용은 *리더 피드백 페이지 52* 항목을 참조하십시오. 또한 제조업체 지침을 참조하십시오.
- **Elevator Reader: Tampering(엘리베이터 리더: 탬퍼링)** - 마지막 탬퍼링 시도에 대한 정보를 가져옵니다. 리더가 설치되면 첫 번째 탬퍼링 시도가 등록됩니다. **Get last tampering(마지막 탬퍼링 가져오기)**을 클릭합니다.

- **Elevator Reader: Card swipe(엘리베이터 리더: 카드 긁기)** - 마지막에 긁은 카드 또는 리더에서 수락한 다른 유형의 사용자 토큰에 대한 정보를 가져옵니다. **Get last credential(마지막 자격 증명 가져오기)**을 클릭합니다.
- **REX** - 장치 종료 요청(REX)이 마지막으로 제기된 시간에 대한 정보를 가져옵니다. **Get last REX(마지막 REX 가져오기)**를 클릭합니다.

## 카드 및 형식 구성

도어 컨트롤러에는 몇 가지 사전 정의된 일반적으로 사용되는 카드 형식이 있습니다. 이러한 형식을 그대로 사용하거나 필요에 따라 수정할 수 있습니다. 사용자 정의 카드 형식을 만들 수도 있습니다. 각 카드 형식에는 카드에 저장된 정보가 어떻게 구성되는지를 제어하는 다양한 룰 세트와 필드 맵이 있습니다. 카드 형식을 정의하여 컨트롤러가 리더로부터 받는 정보를 어떻게 해석할지를 시스템에 알려줄 수 있습니다. 리더가 지원하는 카드 형식에 대한 자세한 내용은 제조업체의 지침을 참조하십시오.

카드 형식을 활성화하려면

1. **Setup > Configure cards and formats(설정 > 카드 및 형식 구성)**로 이동합니다.
2. 연결된 리더에서 사용하는 카드 형식과 일치하는 하나 이상의 카드 형식을 선택합니다.

새 카드 형식을 만들려면

1. **Setup > Configure cards and formats(설정 > 카드 및 형식 구성)**로 이동합니다.
2. **Add card format(카드 형식 추가)**을 클릭합니다.
3. **Add card format(카드 형식 추가)** 대화 상자에서 카드 형식의 이름, 설명 및 비트 길이를 입력합니다. *카드 형식 설명 페이지 22* 항목을 참조하십시오.
4. **Add field map(필드 맵 추가)**을 클릭하고 필드에 필요한 정보를 입력합니다. *필드 맵 페이지 23* 항목을 참조하십시오.
5. 여러 필드 맵을 추가하려면 이전 단계를 반복합니다.

**Card formats(카드 형식)** 목록의 항목을 확장하여 카드 형식 설명과 필드 맵을 보려면 을 클릭합니다.

카드 형식을 편집하려면 을 클릭하고 필요에 따라 카드 형식 설명 및 필드 맵을 변경합니다. 그런 다음 **Save(저장)**를 클릭합니다.

필드 맵을 삭제하려면 **Edit card format(카드 형식 편집)** 또는 **Add card format(카드 형식 추가)** 대화 상자에서 을 클릭합니다.

카드 형식을 삭제하려면 을 클릭합니다.

중요 사항

- 카드 형식에 대한 모든 변경 사항은 도어 컨트롤러 전체 시스템에 적용됩니다.
- 시스템에 있는 하나 이상의 도어 컨트롤러에 하나 이상의 리더가 구성되어 있는 경우에만 카드 형식을 활성화 및 비활성화할 수 있습니다. *하드웨어 구성 페이지 14* 및 *리더 및 REX 장치 구성 방법 페이지 18* 항목을 참조하십시오.
- 비트 길이가 동일한 두 카드 형식을 동시에 활성화할 수 없습니다. 예를 들어, "형식 A"와 "형식 B"라는 두 개의 32비트 카드 형식을 정의했으며 "형식 A"를 활성화한 경우 "형식 B"를 활성화하려면 먼저 "형식 A"를 비활성화해야 합니다.
- 활성화된 카드 형식이 없는 경우 **Card raw only(카드 로우만)** 및 **Card raw and PIN(카드 로우와 PIN)** 식별 유형을 사용하여 카드를 식별하고 사용자에게 접근 권한을 부여할 수 있습니다. 그러나 리더 제조업체와 리더 설정이 다르면 서로 다른 카드 로우 데이터가 생성될 수 있으므로 이 방법은 사용하지 않는 것이 좋습니다.

### 카드 형식 설명

- **Name(이름)**(필수) - 설명이 포함된 이름을 입력합니다.

- **Description(설명)** - 원하는 경우 추가 정보를 입력합니다. 이 정보는 **Edit card format(카드 형식 편집)** 및 **Add card format(카드 형식 추가)** 대화 상자에만 표시됩니다.
- **Bit length(비트 길이)**(필수) - 카드 형식의 비트 길이를 입력합니다. 1에서 1,000,000,000 사이의 숫자여야 합니다.

### 필드 맵

- **Name(이름)**(필수) - 공백 없이 필드 맵 이름을 입력합니다(예: `OddParity`).

  일반적인 필드 맵의 예는 다음과 같습니다.

  - 패리티 - 오류 감지에 패리티 비트가 사용됩니다. 일반적으로 패리티 비트는 이진 코드 문자열 처음이나 끝에 추가되며 비트 수가 짝수인지 홀수인지를 나타냅니다.
  - 짝수 패리티 - 짝수 패리티 비트는 문자열에 짝수 비트를 포함하게 합니다. 값이 1인 비트가 계산됩니다. 개수가 이미 짝수이면 패리티 비트 값이 0으로 설정됩니다. 개수가 홀수이면 짝수 패리티 비트 값이 1로 설정되어 총 개수가 짝수가 되게 합니다.
  - 홀수 패리티 - 홀수 패리티 비트는 문자열에 홀수 비트를 포함하게 합니다. 값이 1인 비트가 계산됩니다. 개수가 이미 홀수이면 홀수 패리티 비트 값이 0으로 설정됩니다. 개수가 짝수이면 패리티 비트 값이 1로 설정되어 총 개수가 홀수가 되게 합니다.
  - 시설 코드 - 토큰이 정렬된 최종 사용자 자격 증명 배치와 일치하는지 확인하기 위해 가끔 시설 코드가 사용됩니다. 기존 접근 제어 시스템에서는 등급이 낮은 확인에 시설 코드가 사용되어 일치하는 사이트 코드로 인코딩된 자격 증명 배치의 모든 직원에게 출입을 허용합니다. 제품이 시설 코드를 확인하기 위해서는 대소문자를 구분하는 이 필드 맵 이름이 필요합니다.
  - 카드 번호 - 카드 번호나 사용자 ID는 접근 제어 시스템에서 가장 일반적으로 확인됩니다. 제품이 카드 번호를 확인하기 위해서는 대소문자를 구분하는 이 필드 맵 이름이 필요합니다.
  - `CardNrHex` - 카드 번호 이진 데이터가 제품에서 16진수 소문자로 인코딩됩니다. 리더에서 필요한 카드 번호를 가져올 수 없는 이유를 해결하기 위해 주로 사용됩니다.
- **Range(범위)**(필수) - 필드 맵의 비트 범위를 입력합니다(예: 1, 2-17, 18-33 및 34).
- **Encoding(인코딩)**(필수) - 각 필드 맵의 인코딩 유형을 선택합니다.
  - **BinLE2Int** - 이진 데이터가 little endian 비트 순서의 정수로 인코딩됩니다. 정수는 소수가 아니라 실수가 되어야 한다는 의미입니다. little endian 비트 순서는 첫 번째 비트가 가장 작아야 한다는(최하위) 의미입니다.
  - **BinBE2Int** - 이진 데이터가 big endian 비트 순서의 정수로 인코딩됩니다. 정수는 소수가 아니라 실수가 되어야 한다는 의미입니다. big endian 비트 순서는 첫 번째 비트가 가장 커야 한다는(최상위) 의미입니다.
  - **BinLE2Hex** - 이진 데이터가 little endian 비트 순서의 16진수 소문자로 인코딩됩니다. 기본 16자 시스템으로 알려진 16진수 시스템은 고유한 기호 16개(숫자 0~9 및 문자 a~f)로 이루어집니다. little endian 비트 순서는 첫 번째 비트가 가장 작아야 한다는(최하위) 의미입니다.
  - **BinBE2Hex** - 이진 데이터가 big endian 비트 순서의 16진수 소문자로 인코딩됩니다. 기본 16자 시스템으로 알려진 16진수 시스템은 고유한 기호 16개(숫자 0~9 및 문자 a~f)로 이루어집니다. big endian 비트 순서는 첫 번째 비트가 가장 커야 한다는(최상위) 의미입니다.
  - **BinLEIBO2Int** - 이진 데이터가 BinLE2Int와 같은 방식으로 인코딩되지만 인코딩을 위해 필드 맵을 가져오기 전에 카드 원시 데이터가 다중 바이트 시퀀스의 변환된 바이트 순서로 읽힙니다.
  - **BinBEIBO2Int** - 이진 데이터가 BinBE2Int와 같이 인코딩되지만 인코딩을 위해 필드 맵을 가져오기 전에 카드 원시 데이터가 다중 바이트 시퀀스의 변환된 바이트 순서로 읽힙니다.

카드 형식에 사용되는 필드 맵에 대한 자세한 내용은 제조업체의 지침을 참조하십시오.

### 사전 설정 시설 코드

토큰이 시설의 접근 제어 시스템에 맞는지 확인하기 위해 때때로 시설 코드가 사용됩니다. 종종 한 시설에 대해 발행된 모든 토큰의 시설 코드가 동일합니다. 카드 배치를 더 쉽게 수동으로 등록할 수 있게 하려면 프리셋 시설 코드를 입력하십시오. 사용자를 추가할 때 사전 설정 시설 코드가 자동으로 입력됩니다. *사용자 자격 증명 페이지 41* 항목을 참조하십시오.

사전 설정 시설 코드를 설정하려면

1. **Setup > Configure cards and formats(설정 > 카드 및 형식 구성)**로 이동합니다.
2. **Preset facility code(사전 설정 시설 코드)**에서 시설 코드를 입력합니다.
3. **Set facility code(시설 코드 설정)**를 클릭합니다.

## 서비스 구성

설정 페이지의 서비스 구성은 도어 컨트롤러와 함께 사용할 수 있는 외부 서비스에 대한 설정에 액세스하는 데 사용됩니다.

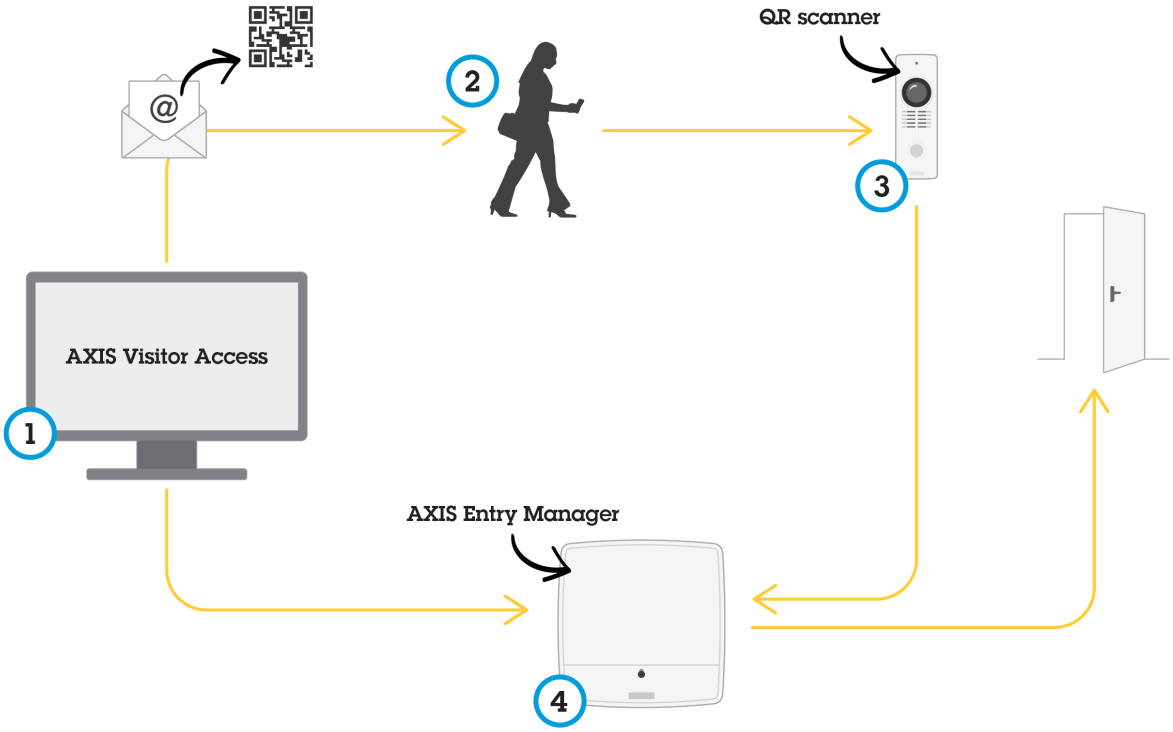
### AXIS Visitor Access

AXIS Visitor Access를 사용하면 QR 코드 형태로 임시 자격 증명을 생성할 수 있습니다. 접근 제어 시스템에 연결된 Axis 네트워크 카메라나 도어 스테이션이 OR 코드를 스캔합니다.

서비스는 다음과 같이 구성됩니다.

- AXIS Entry Manager와 펌웨어 버전 1.65.2 이상이 설치된 Axis 도어 컨트롤러
- OR 스캐너 애플리케이션이 설치된 도어 스테이션 또는 Axis 네트워크 카메라
- AXIS Visitor Access 애플리케이션이 설치된 Windows® PC

## 시스템 구성




*AXIS Visitor Access 서비스 사용*

사용자가 AXIS Visitor Access(1)에서 초대장을 만들어 방문객 이메일 주소로 보냅니다. 동시에 도어 잠금을 해제하기 위한 자격 증명이 생성되어 연결된 Axis 도어 컨트롤러(4)에 저장됩니다. 방문객이 네트워크 카메라나 도어 스테이션(3)에서 초대장에 포함된 QR 코드를 보여 줍니다. 이때 방문객을 위해 도어 잠금을 해제하도록 도어 컨트롤러(4)에 요청합니다.

*QR 코드는 Denso Wave, inc.의 등록 상표입니다.*

**전제 조건 AXIS Visitor Access**

AXIS Visitor Access 서비스를 사용하려면 먼저 다음 사항이 필요합니다.

- 도어 컨트롤러 하드웨어 구성
- 도어 컨트롤러와 같이 동일한 네트워크에 연결되고 도어 근처 방문객이 접근할 수 있는 곳에 놓인 Axis 네트워크 카메라 또는 도어 스테이션
- AXIS Visitor Access 설치 패키지. *axis.com*에서 찾을 수 있습니다.
- AXIS Visitor Access 서비스에만 사용할 추가 사용자 계정 2개(도어 컨트롤러). 하나는 AXIS Visitor Access 애플리케이션용이고, 다른 하나는 QR 스캐너 애플리케이션용입니다. 사용자 계정 생성 방법을 알아보려면 *사용자 페이지 54* 항목을 참조하십시오.

# 시스템 구성

중요 사항

- 전체 시스템에서 도어 컨트롤러 하나에만 AXIS Visitor Access 서비스를 연결할 수 있습니다.
- AXIS Visitor Access 서비스를 사용하면 연결된 도어 컨트롤러로 제어되는 도어만 접속할 수 있습니다. 시스템의 다른 도어에는 접속할 수 없습니다.
- AXIS Visitor Access 애플리케이션을 사용하여 방문객을 수정하고 삭제합니다. AXIS Entry Manager를 사용하지 마십시오.
- AXIS Visitor Access에 사용되는 사용자 계정의 패스워드를 변경할 경우 AXIS Visitor Access에서도 패스워드를 업데이트해야 합니다.
- QR 스캐너 애플리케이션에 사용되는 사용자 계정의 패스워드를 변경할 경우 QR 스캐너를 다시 설정해야 합니다.

### AXIS Visitor Access 설정


AXIS Visitor Access 서비스를 설정할 때 Axis 네트워크 카메라나 도어 스테이션에 QR 스캐너 애플리케이션을 설치합니다. 별도의 설치는 전혀 필요 없습니다.

1. 도어 컨트롤러 웹 페이지에서 **Setup > Configure Services > Settings(설정 > 서비스 구성 > 설정)**로 이동합니다.
2. **Start a new setup(새 설정 시작)**을 클릭합니다.
3. 지침에 따라 설정을 마칩니다.

중요 사항

HTTPS를 사용하게 하려면 도어 컨트롤러가 HTTPS를 통해 통신해야 합니다. 그렇지 않으면 애플리케이션이 도어 컨트롤러와 통신할 수 없습니다.

4. 임시 자격 증명 생성에 사용할 컴퓨터에서 AXIS Visitor Access 애플리케이션을 설치 및 설정합니다.

## SmartIntego

SmartIntego는 도어 컨트롤러에서 더 많은 도어를 처리할 수 있도록 해주는 무선 솔루션입니다.

### SmartIntego 전제 조건

SmartIntego 구성을 진행하기 전에 다음 전제 조건을 충족해야 합니다.

- csv 파일을 생성해야 합니다. csv 파일에는 SmartIntego 솔루션에 사용되는 GatewayNode 및 도어에 대한 정보가 포함되어 있습니다. 이 파일은 SimonsVoss 파트너가 제공하는 독립형 소프트웨어로 생성됩니다.
- SmartIntego 하드웨어 구성을 완료합니다. *무선 잠금 장치에 대한 새 하드웨어 구성을 만드는 방법 페이지 19* 항목을 참조하십시오.

참고

- SmartIntego 구성 도구는 버전 2.1.6452.23485, 빌드 2.1.6452.23485(8/31/2017 1:02:50 PM) 이상이어야 합니다.
- AES(Advanced Encryption Standard)는 SmartIntego에서 지원되지 않으므로 SmartIntego 구성 도구에서 비활성화되어야 합니다.

**SmartIntego를 구성하는 방법**

참고

- 나열된 전제 조건이 충족되었는지 확인하십시오.
- 배터리 상태의 가시성을 향상시키려면 **Setup(설정)** > **Configure event and alarms logs(이벤트 및 알람 로그 구성)**로 이동하고 **Door - Battery alarm(도어 - 배터리 알람)** 또는 **IdPoint - Battery alarm(IdPoint - 배터리 알람)**을 알람으로 추가합니다.
- 도어 모니터 설정은 가져온 CSV 파일에 있습니다. 일반 설치의 경우 이 설정을 변경할 필요가 없습니다.

1. **Browse...(찾아보기...)**를 클릭하고 csv 파일을 선택한 다음 **Upload file(파일 업로드)**을 클릭합니다.
2. GatewayNode를 선택하고 **Next(다음)**를 클릭합니다.
3. 새 구성의 미리 보기가 표시됩니다. 필요한 경우 도어 모니터를 비활성화합니다.
4. **Configure(구성)**를 클릭합니다.
5. 구성에 포함된 도어의 개요가 표시됩니다. **Settings(설정)**를 클릭하여 각 도어를 개별적으로 구성합니다.

**SmartIntego를 재구성하는 방법**

1. 최상위 메뉴에서 **Setup(설정)**을 클릭합니다.
2. **Configure Services(서비스 구성)** > **Settings(설정)**로 이동합니다.
3. **Re-configure(재구성)**를 클릭합니다.
4. **Browse...(찾아보기...)**를 클릭하고 csv 파일을 선택한 다음 **Upload file(파일 업로드)**을 클릭합니다.
5. GatewayNode를 선택하고 **Next(다음)**를 클릭합니다.
6. 새 구성의 미리 보기가 표시됩니다. 필요한 경우 도어 모니터를 비활성화합니다.

참고

도어 모니터 설정은 가져온 CSV 파일에 있습니다. 일반 설치의 경우 이 설정을 변경할 필요가 없습니다.

7. **Configure(구성)**를 클릭합니다.
8. 구성에 포함된 도어의 개요가 표시됩니다. **Settings(설정)**를 클릭하여 각 도어를 개별적으로 구성합니다.

## 네트워크 도어 컨트롤러 관리

Manage Network Door Controllers in System(시스템의 네트워크 도어 컨트롤러 관리) 페이지에는 도어 컨트롤러, 시스템 상태, 시스템에 포함된 다른 도어 컨트롤러 등에 대한 정보가 있습니다. 관리자가 이 페이지에서 도어 컨트롤러를 추가 및 제거하여 시스템을 변경할 수도 있습니다.

중요 사항

시스템의 모든 도어 컨트롤러가 같은 네트워크에 연결되고 단일 사이트에서 사용하도록 설정되어 있어야 합니다.

도어 컨트롤러를 관리하려면 **Setup > Manage Network Door Controllers in System(설정 > 시스템의 네트워크 도어 컨트롤러 관리)**으로 이동합니다.

# 시스템 구성

시스템의 네트워크 도어 컨트롤러 관리 페이지에는 다음과 같은 패널이 있습니다.

- **System status of this controller(이 컨트롤러의 시스템 상태)** - 도어 컨트롤러 시스템 상태가 표시되고 시스템 모드와 독립 실행형 모드 간 전환을 가능하게 합니다. 자세한 내용은 *도어 컨트롤러 시스템 상태 페이지 28* 항목을 참조하십시오.
- **Network door controllers in system(시스템의 네트워크 도어 컨트롤러)** - 시스템의 도어 컨트롤러에 대한 정보가 표시되고 시스템에서 컨트롤러를 추가 및 제거할 수 있는 컨트롤이 있습니다. 자세한 내용은 *시스템의 연결된 도어 컨트롤러 페이지 28* 항목을 참조하십시오.

## 도어 컨트롤러 시스템 상태

도어 컨트롤러가 도어 컨트롤러 시스템의 일부가 될 수 있는지는 시스템 상태에 따라 달라집니다. 도어 컨트롤러의 시스템 상태는 **System status for this controller(이 컨트롤러의 시스템 상태)** 패널에 표시됩니다.

도어 컨트롤러가 독립 실행형 모드가 아니며 도어 컨트롤러를 시스템에 추가할 수 없도록 하려면 **Activate standalone mode(독립 실행형 모드 활성화)**를 클릭하여 독립 실행형 모드로 전환합니다.

도어 컨트롤러가 독립 실행형 모드이지만 도어 컨트롤러를 시스템에 추가하려는 경우 **Deactivate standalone mode(독립 실행형 모드 비활성화)**를 클릭하여 독립 실행형 모드에서 나갑니다.

### 시스템 모드

- **This controller is not part of a system and not in standalone mode(이 컨트롤러는 시스템의 일부가 아니며 독립 실행형 모드가 아닙니다)** - 도어 컨트롤러가 시스템의 일부로 구성되어 있지 않으며 독립 실행형 모드가 아닙니다. 즉, 도어 컨트롤러가 열려 있고 동일한 네트워크에 있는 다른 도어 컨트롤러에 의해 시스템에 추가될 수 있습니다. 도어 컨트롤러가 시스템에 추가되지 않도록 하려면 독립 실행형 모드를 활성화하십시오.
- **This controller is set to standalone mode(이 컨트롤러는 독립 실행형 모드로 설정되어 있습니다)** - 도어 컨트롤러가 시스템의 일부가 아닙니다. 네트워크에 있는 다른 도어 컨트롤러에 의해 시스템에 추가될 수 없으며 다른 도어 컨트롤러를 추가할 수도 없습니다. 독립 실행형 모드는 일반적으로 도어 컨트롤러 하나와 둘 이상의 도어가 있는 소규모 설정에서 사용됩니다. 도어 컨트롤러를 시스템에 추가할 수 있도록 하려면 독립 실행형 모드를 비활성화하십시오.
- **This controller is part of a system(컨트롤러는 시스템의 일부입니다)** - 도어 컨트롤러가 분산 시스템의 일부입니다. 분산 시스템에서는 연결된 컨트롤러 간에 사용자, 그룹 및 일정이 공유됩니다.

## 시스템의 연결된 도어 컨트롤러

**Network door controllers in system(시스템의 네트워크 도어 컨트롤러)** 패널에는 다음과 같이 시스템을 변경할 수 있는 컨트롤이 있습니다.

- 시스템에 도어 컨트롤러를 추가합니다. *시스템에 도어 컨트롤러 추가 페이지 29* 항목을 참조하십시오.
- 시스템에서 도어 커트롤러를 제거합니다. *시스템에서 도어 컨트롤러 제거 페이지 29* 항목을 참조하십시오.

### 연결된 도어 컨트롤러 목록

**Network door controllers in system(시스템의 네트워크 도어 컨트롤러)** 패널에는 시스템의 연결된 도어 컨트롤러에 대한 다음과 같은 ID와 상태 정보를 보여주는 목록도 있습니다.

- **Name(이름)** - 사용자가 정의한 도어 컨트롤러 이름입니다. 관리자가 하드웨어를 구성할 때 이름을 설정하지 않은 경우 기본 이름이 표시됩니다.
- **IP address(IP 주소)**
- **MAC address(MAC 주소)**
- **Status(상태)** - 시스템에 액세스하는 도어 컨트롤러가 **This controller(이 컨트롤러)** 상태를 표시합니다. 시스템의 다른 도어 컨트롤러는 **Online(온라인)** 상태를 표시합니다.

- **Firmware version(펌웨어 버전)**

다른 도어 컨트롤러의 웹 페이지를 열려면 컨트롤러의 IP 주소를 클릭하십시오.

목록을 업데이트하려면 **Refresh the list of controllers(컨트롤러 목록 새로 고침)**를 클릭합니다.

참고

시스템에 있는 모든 컨트롤러의 펌웨어 버전은 항상 동일해야 합니다. Axis Device Manager를 사용하여 전체 시스템의 모든 컨트롤러에서 펌웨어 업그레이드를 동시에 진행할 수 있습니다.

#### 시스템에 도어 컨트롤러 추가

중요 사항

도어 컨트롤러를 페어링할 때 추가된 도어 컨트롤러의 모든 접근 관리 설정이 삭제되며 시스템의 접근 관리 설정이 이 설정을 덮어씁니다.

도어 컨트롤러 목록에서 시스템에 도어 컨트롤러를 추가하려면

1. **Setup > Manage Network Door Controllers in System(설정 > 시스템의 네트워크 도어 컨트롤러 관리)**으로 이동합니다.
2. **Add controllers to system from list(목록에서 시스템에 컨트롤러 추가)**를 클릭합니다.
3. 추가할 도어 컨트롤러를 선택합니다.
4. **Add(추가)**를 클릭합니다.
5. 도어 컨트롤러를 더 추가하려면 위의 단계를 반복합니다.

알려진 IP 주소나 MAC 주소로 시스템에 도어 컨트롤러를 추가하려면

1. **Manage Devices(장치 관리)**로 이동합니다.
2. **Add controller to system by IP or MAC address(IP 또는 MAC 주소로 시스템에 컨트롤러 추가)**를 클릭합니다.
3. IP 주소나 MAC 주소를 입력합니다.
4. **Add(추가)**를 클릭합니다.
5. 도어 컨트롤러를 더 추가하려면 위의 단계를 반복합니다.

페어링이 완료되면 모든 사용자, 도어, 일정 및 그룹이 시스템의 모든 도어 컨트롤러에 공유됩니다.

목록을 업데이트하려면 **Refresh list of controllers(컨트롤러 목록 새로 고침)**를 클릭합니다.

#### 시스템에서 도어 컨트롤러 제거

중요 사항

- 시스템에서 도어 컨트롤러를 재거하기 전에 하드웨어 구성을 재설정하십시오. 이 단계를 건너뛰면 제거된 도어 컨트롤러에 관련된 모든 도어가 시스템에 남아 있고 삭제할 수 없습니다.
- 2개의 컨트롤러 시스템에서 도어 컨트롤러를 제거할 때는 두 도어 컨트롤러 모두 독립 실행형 모드로 자동 전환됩니다.

시스템에서 도어 컨트롤러를 제거하려면

1. 제거할 도어 컨트롤러를 통해 시스템에 액세스하고 **Setup > Hardware Configuration(설정 > 하드웨어 구성)**으로 이동합니다.
2. **Reset hardware configuration(하드웨어 구성 재설정)**을 클릭합니다.

3. 하드웨어 구성이 재설정되면 **Setup > Manage Network Door Controllers in System(설정 > 시스템의 네트워크 도어 컨트롤러 관리)**으로 이동합니다.
4. **Network door controllers in system(시스템의 네트워크 도어 컨트롤러)** 목록에서 제거할 도어 컨트롤러를 찾아 **Remove from system(시스템에서 제거)**을 클릭합니다.
5. 도어 컨트롤러의 하드웨어 구성을 재설정하라고 알리는 대화 상자가 열립니다. **Remove controller(컨트롤러 제거)**를 클릭하여 확인합니다.
6. 도어 컨트롤러를 제거할 것인지 확인하는 내용의 대화 상자가 열립니다. **OK(확인)**를 클릭하여 확인합니다. 제거된 도어 컨트롤러는 이제 독립 실행형 모드입니다.

참고

- 시스템에서 도어 컨트롤러가 제거되면 모든 접근 관리 설정이 삭제됩니다.
- 온라인 상태인 도어 컨트롤러만 제거할 수 있습니다.

## 구성 모드

구성 모드는 처음 장치에 액세스할 때의 표준 모드입니다. 구성 모드가 비활성화되면 장치의 대부분의 구성 기능이 숨겨집니다.

중요 사항

구성 모드를 비활성화하려는 경우 구성 모드를 보안 기능으로 사용해서는 안됩니다. 구성 모드는 구성 실수를 방지하기 위한 용도이지 악의적 사용자가 중요한 설정을 변경하는 것을 막지는 못합니다.

### 구성 모드를 비활성화하는 방법

1. **Setup(설정)** > **Disable Configuration Mode(구성 모드 비활성화)**로 이동합니다.
2. PIN을 입력하고 **OK(확인)**를 선택합니다.

참고

PIN은 필수가 아닙니다.

### 구성 모드를 활성화하는 방법

1. **Setup(설정)** > **Enable Configuration Mode(구성 모드 활성화)**로 이동합니다.
2. PIN을 입력하고 **OK(확인)**를 선택합니다.

참고

PIN을 저장하지 않으려면 `http://[IP-address]/webapp/pacs/index.shtml#resetConfigurationMode`를 입력하여 구성 모드를 활성화할 수 있습니다.

## 유지보수 지침

접근 제어 시스템이 원활하게 실행되도록 유지하려면 도어 컨트롤러 및 연결된 장치를 비롯하여 접근 제어 시스템을 정기적으로 유지보수하는 것이 좋습니다.

일년에 한 번 이상 유지보수를 실행하십시오. 제안된 유지보수 절차에는 다음 단계가 포함됩니다(이에 국한되지 않음).

- 도어 컨트롤러와 외부 장치 간의 모든 연결이 고정되어 있는지 확인합니다.
- 모든 하드웨어 연결을 확인합니다. *컨트롤 도어 확인 페이지 21* 항목을 참조하십시오.
- 연결된 외부 장치를 비롯하여 시스템이 올바르게 작동하는지 확인합니다.
  - 카드를 긁고 리더, 도어 및 잠금 장치를 테스트합니다.

- 시스템에 REX 장치, 센서 또는 기타 장치가 포함되어 있는 경우 해당 장치도 테스트합니다.
- 활성화된 경우 탬퍼링 알람을 테스트합니다.

위 단계의 결과가 결함이나 예상치 못한 동작을 나타내는 경우 다음을 수행하십시오.

- 적절한 장비를 사용하여 와이어의 신호를 테스트하고 와이어 또는 케이블이 어떤 식으로든 손상되었는지 확인합니다.
- 손상되거나 결함이 있는 케이블 및 와이어를 모두 교체합니다.
- 케이블과 와이어를 교체하면 모든 하드웨어 연결을 다시 확인합니다. *컨트롤 도어 확인 페이지 21* 항목을 참조하십시오.

- 모든 접근 일정, 도어, 그룹 및 사용자가 최신 상태인지 확인합니다.
- 도어 컨트롤러가 예상한 대로 작동하지 않는 경우 이에 대한 자세한 내용은 *장애 처리 페이지 65* 및 *유지 보수 페이지 62* 항목을 참조하십시오.

## 접근 관리

### 사용자에 대한 정보

AXIS Entry Manager에서 사용자는 하나 이상의 토큰(식별 유형)에 대한 소유자로 등록된 사람입니다. 개인마다 접근 제어 시스템의 도어에 접근할 수 있도록 고유한 사용자 프로파일이 있어야 합니다. 사용자 프로파일은 사용자가 누구이며 도어에 언제 어떻게 접근할 수 있는지 시스템에 알려주는 자격 증명으로 구성됩니다. 자세한 내용은 *사용자 생성 및 편집 페이지 41* 항목을 참조하십시오.

이 경우의 사용자를 관리자와 혼동해서는 안 됩니다. 관리자는 모든 설정에 무제한 액세스할 수 있습니다. 접근 제어 시스템 관리의 측면에서 제품 웹 페이지(AXIS Entry Manager)에서는 관리자를 사용자라고도 합니다. 자세한 내용은 *사용자 페이지 54* 항목을 참조하십시오.

### 접근 관리 페이지

접근 관리 페이지에서는 시스템의 사용자, 그룹, 도어 및 일정을 구성하고 관리할 수 있습니다. 접근 관리 페이지를 열려면 **Access Management(접근 관리)**를 클릭합니다.

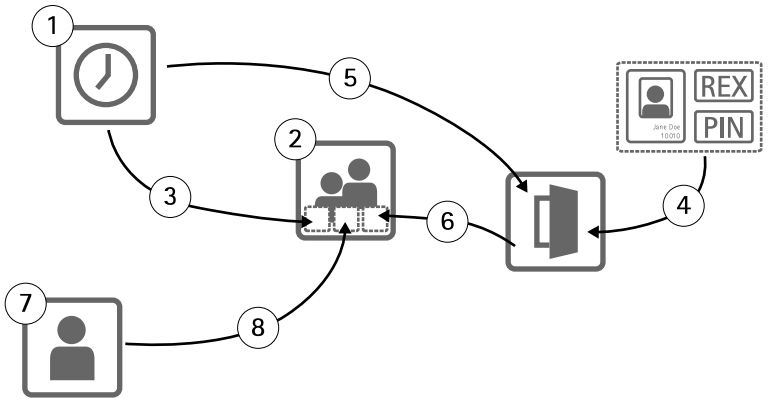
그룹에 사용자를 추가하고 접근 일정 및 도어를 적용하려면 **Groups(그룹)** 및 **Doors(도어)** 목록에서 해당 대상으로 항목을 끌어 놓습니다.

참고

액션이 필요한 메시지는 빨간 텍스트로 표시됩니다.

### 작업 흐름 선택

접근 관리 구조가 유연하여 필요에 따라 적합한 작업 흐름을 개발할 수 있습니다. 다음은 작업 흐름의 예입니다.




1. 접근 일정을 생성합니다. *페이지 33* 항목을 참조하십시오.
2. 그룹을 만듭니다. *페이지 35* 항목을 참조하십시오.
3. 접근 일정을 그룹에 적용합니다.
4. 식별 유형을 도어 또는 플로어에 추가합니다. *페이지 35* 및 *페이지 36* 항목을 참조하십시오.
5. 접근 일정을 각 식별 유형에 적용합니다.
6. 도어 또는 플로어를 그룹에 적용합니다.
7. 사용자를 만듭니다. *페이지 41* 항목을 참조하십시오.

8. 사용자를 그룹에 추가합니다.

이 작업 흐름이 적용된 예는 *접근 일정 조합의 예 페이지 43* 항목을 참조하십시오.

## 접근 일정 생성 및 편집

접근 일정은 도어에 접근할 수 있는 시간과 없는 시간에 대한 일반적인 룰을 정의하는 데 사용됩니다. 그룹이 시스템의 도어에 접근할 수 있는 시간과 없는 시간에 대한 룰을 정의할 때도 사용됩니다. 자세한 내용은 *접근 일정 유형 페이지 33* 항목을 참조하십시오.

새 접근 일정을 만들려면

1. **Access Management(접근 관리)**로 이동합니다.
2. **Access Schedules(접근 일정)** 탭에서 **Add new schedule(새 일정 추가)**을 클릭합니다.
3. **Add access schedule(접근 일정 추가)** 대화 상자에서 일정 이름을 입력합니다.
4. 정기적인 접근 일정을 만들려면 **Addition Schedule(추가 일정)**을 선택합니다.

   또는 삭제 일정을 생성하려면 **Subtraction Schedule(삭제 일정)**을 선택합니다.

   자세한 내용은 *접근 일정 유형 페이지 33* 항목을 참조하십시오.
5. **Save(저장)**를 클릭합니다.

**Access Schedules(접근 일정)** 목록의 항목을 확장하려면 을 클릭합니다. 추가 일정은 녹색 텍스트로 표시되고 삭제 일정은 추가 일정은 진한 빨간색 텍스트로 표시됩니다.

접근 일정의 달력을 보려면 을 클릭합니다.

접근 일정 이름이나 일정 항목을 편집하려면 을 클릭하고 변경합니다. 그런 다음 **Save(저장)**를 클릭합니다.

접근 일정을 삭제하려면 을 클릭합니다.

참고

도어 컨트롤러에는 사전 정의되고 공통적으로 사용되며 예로 사용되거나 필요에 따라 수정할 수 있는 접근 일정이 몇 가지 있습니다. 하지만 사전 정의된 접근 일정 **Always(항상)**는 수정하거나 삭제할 수 없습니다.

### 접근 일정 유형

두 가지 유형의 접근 일정이 있습니다.

- **Addition schedule(추가 일정)** - 도어에 접근할 수 있는 시간을 정의하는 정기적인 접근 일정입니다. 일반적인 추가 일정은 근무 시간, 영업 시간, 근무 시간 후 또는 야간 시간입니다.
- **Subtraction schedule(삭제 일정)** - 정기적인 접근 일정의 예외입니다. 일반적으로 정기적인 일정(추가 일정)기간에 발생하는 특정 기간의 접근을 제한하기 위해 사용됩니다. 예를 들어 주중의 공휴일에 사용자의 건물 접근을 거부하기 위해 삭제 일정을 사용할 수 있습니다.

두 유형의 접근 일정 모두 두 가지 수준에서 사용할 수 있습니다.

- **Identification type schedules(식별 유형 일정)** - 리더가 사용자의 도어 접근을 허용하는 시간과 방법을 결정합니다. 특정한 식별 유형으로 사용자의 접근을 허용하는 시간을 시스템에 알리는 접근 일정에 각 식별 유형이 연결되어 있어야 합니다. 식별 유형마다 여러 추가 일정과 삭제 일정을 추가할 수 있습니다. 식별 유형에 대한 자세한 내용은 *페이지 36* 항목을 참조하십시오.
- **Group schedules(그룹 일정)** - 그룹 멤버가 도어에 접근할 수 있는 시간(방법이 아니라)을 결정합니다. 멤버에게 접근을 허용하는 시간을 시스템에 알리는 하나 이상의 접근 일정에 각 그룹에 연결되어 있어야 합니다. 그룹마다 여러 추가 일정과 삭제 일정을 추가할 수 있습니다. 그룹에 대한 자세한 내용은 *페이지 35* 항목을 참조하십시오.

그룹 일정은 출입 권한을 제한할 수 있지만 식별 유형 일정이 허용하는 이상으로 출입을 확대하거나 접근 권한을 종료할 수는 없습니다. 즉, 식별 유형 일정이 특정 시간에 출입 접근을 제한할 경우 그룹 일정은 해당 식별 유형 일정을 무시할 수 없습니다. 하지만 그룹 일정이 식별 유형 일정보다 접근에 대해 제한적일 경우 그룹 일정이 식별 유형 일정을 무시합니다.

여러 가지 방식으로 식별 유형과 그룹 일정을 조합하여 다양한 결과를 얻을 수 있습니다. 접근 일정 조합의 예는 *페이지 43* 항목을 참조하십시오.

### 스케줄 항목 추가

추가 스케줄과 삭제 스케줄은 일회성(단일) 이벤트이거나 반복 이벤트일 수 있습니다.

접근 스케줄에 스케줄 항목을 추가하려면

1. **Access Schedules(접근 스케줄)** 목록에서 접근 일정을 확장합니다.
2. **Add schedule item(스케줄 항목 추가)**을 클릭합니다.
3. 예약된 항목의 이름을 입력합니다.
4. **One time(한 번)** 또는 **Recurrence(반복)**를 선택합니다.
5. 시간 필드에서 기간을 설정합니다. *시간 옵션 페이지 34* 항목을 참조하십시오.
6. 반복 스케줄 이벤트의 경우 **Recurrence pattern(반복 패턴)** 및 **Range of recurrence(반복 범위)** 매개변수를 선택합니다. *반복 패턴 옵션 페이지 34* 및 *반복 범위 옵션 페이지 34* 항목을 참조하십시오.
7. **Save(저장)**를 클릭합니다.

#### 시간 옵션

다음과 같은 시간 옵션을 사용할 수 있습니다.

- **All day(하루 종일)** - 24시간 동안 종일 지속되는 이벤트에 대해 선택합니다. 그런 다음 원하는 **Start(시작)** 날짜를 입력합니다.
- **Start(시작)** - 시간 필드를 클릭하고 원하는 시간을 선택합니다. 필요한 경우 날짜 필드를 클릭하고 원하는 월, 일, 연도를 선택합니다. 필드에 날짜를 직접 입력할 수도 있습니다.
- **End(종료)** - 시간 필드를 클릭하고 원하는 시간을 선택합니다. 필요한 경우 날짜 필드를 클릭하고 원하는 월, 일, 연도를 선택합니다. 필드에 날짜를 직접 입력할 수도 있습니다.

#### 반복 패턴 옵션

다음과 같은 반복 패턴 옵션을 사용할 수 있습니다.

- **Yearly(매년)** - 매년 반복하려면 선택합니다.
- **Weekly(매주)** - 매주 반복하려면 선택합니다.
- 매주 **Monday(월요일)**, **Tuesday(화요일)**, **Wednesday(수요일)**, **Thursday(목요일)**, **Friday(금요일)**, **Saturday(토요일)**, **Sunday(일요일)**에 반복 - 반복할 요일을 선택합니다.

#### 반복 범위 옵션

다음과 같은 반복 범위 옵션을 사용할 수 있습니다.

- **First occurrence(첫 번째 발생)** - 날짜 필드를 클릭하고 원하는 월, 일, 연도를 선택합니다. 필드에 날짜를 직접 입력할 수도 있습니다.
- **No end date(종료 날짜 없음)** - 발생을 무기한 반복하려면 선택합니다.

- **End by(종료 기한)** - 날짜 필드를 클릭하고 원하는 월, 일, 연도를 선택합니다. 필드에 날짜를 직접 입력할 수도 있습니다.

## 그룹 생성 및 편집

그룹을 사용하면 사용자와 사용자의 접근 권한을 모두 함께 효율적으로 관리할 수 있습니다. 그룹은 그룹을 구성하는 사용자, 그룹 구성원에게 도어에 대한 접근 권한이 부여되는 시기 및 방법에 대해 시스템에 알려주는 자격 증명으로 구성됩니다.

각 사용자는 하나 이상의 그룹에 속해야 합니다. 사용자를 그룹에 추가하려면 해당 사용자를 **Groups(그룹)** 목록의 원하는 그룹으로 끌어서 놓습니다. 자세한 내용은 *사용자 생성 및 편집 페이지 41* 항목을 참조하십시오.

새 그룹을 생성하려면

1. **Access Management(접근 관리)**로 이동합니다.
2. **Groups(그룹)** 탭에서 **Add new group(새 그룹 추가)**을 클릭합니다.
3. **Add Group(그룹 추가)** 대화 상자에 그룹의 자격 증명을 입력합니다. *그룹 자격 증명 페이지 35* 항목을 참조하십시오.
4. **Save(저장)**를 클릭합니다.

**Groups(그룹)** 목록의 항목을 확장하여 해당 구성원, 도어 접근 권한 및 스케줄을 보려면 을 클릭합니다.

그룹의 이름이나 유효 날짜를 편집하려면 을 클릭하고 변경합니다. 그런 다음 **Save(저장)**를 클릭합니다.

그룹이 특정 도어에 접근할 수 있는 시기와 방법을 확인하려면 을 클릭합니다.

그룹이나 그룹 구성원, 도어 또는 스케줄을 그룹에서 삭제하려면 을 클릭합니다.

### 그룹 자격 증명

그룹에 다음과 같은 자격 증명을 사용할 수 있습니다.

- **Name(이름)**(필수)
- **Valid from(유효 기간 시작)** 및 **Valid to(유효 기간 만료)** 그룹의 자격 증명이 유효한 기간(날짜)을 입력합니다. 날짜 필드를 클릭하고 원하는 월, 일, 연도를 선택합니다. 필드에 날짜를 직접 입력할 수도 있습니다.
- **Whitelist(화이트 리스트)** - 네트워크 또는 전원 장애가 발생해도 화이트 리스트 그룹의 사용자는 항상 그룹에 있는 도어에 접근할 수 있습니다. 그룹의 사용자는 항상 도어에 접근할 수 있으므로 일정이나 유효 기간 시작 및 유효 기간 만료가 적용되지 않습니다. 화이트 리스트 그룹의 도어를 여는 사용자에게는 긴 접근 시간이 지원되지 않습니다. 화이트 리스트 기능을 지원하며 무선 잠금 기능을 갖춘 도어만 그룹에 추가할 수 있습니다.

참고

- 그룹을 저장하려면 그룹 **Name(이름)**을 입력해야 합니다.
- 사용자를 화이트 리스트 그룹에 추가할 때는 사용자의 유효 기간 만료 및 유효 기간 시작이 적용되지 않습니다.
- 화이트 리스트에 있는 자격 증명을 무선 잠금과 동기화하려면 시간이 좀 걸리고 이 동기화 작업이 정상 도어 개방 절차에 간섭합니다. 사용량이 많은 시간에는 시스템에서 많은 자격 증명을 추가하거나 제거하지 마십시오. 업데이트된 자격 증명을 잠금에 동기화할 때는 잠금에 대해 이벤트 로그에 `SyncOngoing: false`가 표시됩니다.

## 도어 관리

각 도어에 대한 일반 룰은 **Doors(도어)** 탭에서 관리됩니다. 룰에는 사용자에게 도어에 대한 접근 권한이 부여되는 방법을 결정하는 식별 유형과 각 식별 유형이 유효한 때를 결정하는 접근 스케줄이 포함됩니다. 자세한 내용은 *식별 유형 페이지 36* 및 *접근 일정 생성 및 편집 페이지 33* 항목을 참조하십시오.

도어를 관리하려면 먼저 하드웨어 구성을 완료하여 도어를 접근 제어 시스템에 추가해야 합니다. *하드웨어 구성 페이지 14* 항목을 참조하십시오.

도어를 관리하려면

1. **Access Management(접근 관리)**로 이동하여 **Doors(도어)** 탭을 선택합니다.
2. **Doors(도어)** 목록에서 편집할 도어 옆의 ▶ 을 클릭합니다.
3. 도어를 하나 이상의 그룹으로 끕니다. **Groups(그룹)** 목록이 비어 있으면 새 그룹을 생성합니다. *그룹 생성 및 편집 페이지 35* 항목을 참조하십시오.
4. **Add identification type(식별 유형 추가)**을 클릭하고 도어에 대한 접근 권한을 부여받기 위해 사용자가 리더에 제공해야 할 자격 증명을 선택합니다. *식별 유형 페이지 36* 항목을 참조하십시오.

   각 도어에 하나 이상의 식별 유형을 추가합니다.
5. 여러 식별 유형을 추가하려면 이전 단계를 반복합니다.

   **Card number only(카드 번호만)**와 **PIN only(PIN만)** 두 식별 유형을 모두 추가한 경우 사용자는 카드를 긁거나 핀을 입력하는 두 가지 방법 중 하나로 도어에 접근할 수 있습니다. 그러나 **Card number and PIN(카드 번호 및 PIN)** 식별 유형만 추가한 경우에는 사용자가 카드를 긁고 PIN을 입력하는 두 가지 작업을 모두 수행해야 도어에 접근할 수 있습니다.
6. 자격 증명의 유효 기간을 정의하려면 스케줄을 각 식별 유형으로 끕니다.

수동으로 도어의 잠금을 해제하거나 잠그거나 임시 접근 권한을 부여하려면 필요에 따라 수동 도어 액션 중 하나를 클릭합니다. *수동 도어 액션 사용 페이지 37* 항목을 참조하십시오.

참고

무선 도어/장치에 대해서는 수동으로 도어의 잠금을 해제하거나 잠그거나 임시 접근 권한을 부여하는 컨트롤을 사용할 수 없습니다.

**Doors(도어)** 목록의 항목을 확장하려면 ▶ 을 클릭합니다.

도어 또는 리더 이름을 편집하려면 ✎ 을 클릭하고 변경합니다. 그런 다음 **Save(저장)**를 클릭합니다.

리더, 식별 유형 및 접근 스케줄 조합을 확인하려면  을 클릭합니다.

도어에 연결된 잠금 장치의 기능을 확인하려면 확인 컨트롤을 클릭합니다. *컨트롤 도어 확인 페이지 21* 항목을 참조하십시오.

식별 유형 또는 접근 스케줄을 삭제하려면 ⊖ 을 클릭합니다.

### 식별 유형

식별 유형은 이동식 자격 증명 스토리지 장치, 기억된 정보 또는 사용자가 도어에 접근하도록 허용하는 방법을 결정하는 다양한 조합입니다. 공통적인 식별 유형에는 카드나 전자 열쇠와 같은 토큰, PIN(개인 식별 번호), REX(종료 요청) 장치 등이 있습니다.

자격 증명에 대한 자세한 내용은 *사용자 자격 증명 페이지 41* 항목을 참조하십시오.

다음과 같은 식별 유형을 사용할 수 있습니다.

- **Facility code only(시설 코드만)** - 사용자가 카드 또는 리더에서 수락한 시설 코드가 있는 그 밖의 토큰을 사용하여 도어에 접근할 수 있습니다.
- **Card number only(카드 번호만)** - 사용자가 카드 또는 리더에서 수락한 그 밖의 토큰만 사용하여 도어에 접근할 수 있습니다. 카드 번호는 대개 카드에 찍힌 고유 번호입니다. 카드 번호 위치는 카드 제조업체의 정보를 참조하십시오. 시스템에서 카드 번호를 검색할 수도 있습니다. 연결된 리더에 카드를 긁고 목록에서 리드를 선택한 후 **Retrieve(검색)**를 클릭합니다.
- **Card raw only(카드 로우만)** - 사용자가 카드 또는 리더에서 수락한 그 밖의 토큰만 사용하여 도어에 접근할 수 있습니다. 정보가 원시 데이터로 카드에 저장됩니다. 시스템에서 카드 원시 데이터를 검색할 수 있습니다. 연결된 리더에 카드를 긁고 목록에서 리드를 선택한 후 **Retrieve(검색)**를 클릭합니다. 카드 번호를 찾을 수 없으면 이 식별 유형만 사용하십시오.
- **PIN only(PIN만)** - 사용자가 4자리 PIN(개인 식별 번호)만 사용하여 도어에 접근할 수 있습니다.
- **Facility code and PIN(시설 코드 및 PIN)** - 사용자가 카드 또는 리더에서 수락한 시설 코드를 가진 그 밖의 토큰 및 PIN을 둘 다 사용하여 도어에 접근해야 합니다. 사용자는 지정된 순서로(카드, PIN 순서로) 자격 증명을 제공해야 합니다.
- **Card number and PIN(카드 번호 및 PIN)** - 사용자는 카드 또는 리더에서 수락한 그 밖의 토큰과 PIN을 둘 다 사용하여 도어에 접근해야 합니다. 사용자는 지정된 순서로(카드, PIN 순서로) 자격 증명을 제공해야 합니다.
- **Card raw and PIN(카드 로우 및 PIN)** - 사용자는 카드 또는 리더에서 수락한 그 밖의 토큰과 PIN을 둘 다 사용하여 도어에 접근해야 합니다. 카드 번호를 찾을 수 없으면 이 식별 유형만 사용하십시오. 사용자는 지정된 순서로(카드, PIN 순서로) 자격 증명을 제공해야 합니다.
- **REX** - 사용자는 버튼, 센서, 푸시 바 등의 REX(종료 요청) 장치를 활성화하여 도어에 접근할 수 있습니다.
- **License plate only(번호판만)** - 사용자는 차량 번호판의 번호만 사용하여 도어에 접근할 수 있습니다.

### 예약된 잠금 해제 상태 추가

특정 기간에 자동으로 도어를 잠금 해제 상태로 유지하려면 **Scheduled unlock(예약된 잠금 해제)** 상태를 도어에 추가하고 접근 일정을 적용하면 됩니다.

예를 들어 근무 시간에 도어를 잠금 해제 상태로 유지하려면

1. **Access Management(접근 관리)**로 이동하여 **Doors(도어)** 탭을 선택합니다.
2. 편집할 **Doors(도어)** 목록 항목 옆의 ▶ 을 클릭합니다.
3. **Add scheduled unlock(예약된 잠금 해제 추가)**을 클릭합니다.
4. 도어에 잠금 장치가 1개인지 2개인지에 따라 **Unlock state(잠금 해제 상태)**(**unlocked(잠금 해제됨)** 또는 **unlock both locks(잠금 장치 둘 다 잠금 해제)**)를 선택합니다.
5. **OK(확인)**를 클릭합니다.
6. 사전 정의된 **Office hours(근무 시간)** 접근 일정을 **Scheduled unlock(예약된 잠금 해제)** 상태에 적용합니다.

도어 잠금이 해제될 때 확인하려면 을 클릭합니다.

예약된 잠금 해제 상태나 접근 일정을 삭제하려면 을 클릭합니다.

### 수동 도어 액션 사용

**Manual door actions(수동 도어 액션)**를 통해 **Doors(도어)** 탭에서 도어를 잠금 해제하거나 잠그고 임시 접근을 허용할 수 있습니다. 특정 도어에 대해 사용할 수 있는 수동 도어 액션은 도어를 구성한 방법에 따라 다릅니다.

수동 도어 액션을 사용하려면

1. **Access Management(접근 관리)**로 이동하여 **Doors(도어)** 탭을 선택합니다.

2. **Doors(도어)** 목록에서 제어할 도어 옆의 ▶ 을 클릭합니다.
3. 필요한 도어 액션을 클릭합니다. *수동 도어 액션 페이지 38* 항목을 참조하십시오.

참고

수동 도어 액션을 사용하려면 해당 도어가 연결되는 도어 컨트롤러를 통해 접근 관리 페이지를 열어야 합니다. 다른 도어 컨트롤러를 통해 접근 관리 페이지를 열면 수동 도어 액션 대신 해당 도어가 연결된 도어 컨트롤러의 개요 페이지로 연결하는 링크가 있습니다. 링크를 클릭하고 **Access Management(접근 관리)**로 이동하여 **Doors(도어)** 탭을 선택합니다.

**수동 도어 액션**

다음과 같은 수동 도어 액션을 사용할 수 있습니다.

- **Get door status(도어 상태 가져오기)** - 도어 모니터, 도어 알람 및 잠금 장치의 현재 상태를 확인합니다.
- **Access(접근)** - 사용자의 도어 접근을 허용합니다. 주어진 접근 시간이 적용됩니다. *도어 모니터 및 잠금을 구성하는 방법 페이지 15* 항목을 참조하십시오.
- **Unlock(잠금 해제)**(잠금 장치 1개) 또는 **Unlock both locks(잠금 장치 둘 다 잠금 해제)**(잠금 장치 2개) - 도어 잠금을 해제합니다. **Lock(잠금)** 또는 **Lock both locks(잠금 장치 둘 다 잠금 해제)**를 누르거나, 예약된 도어 상태가 활성화되거나, 도어 컨트롤러가 다시 시작될 때까지 도어는 잠금 해제된 상태로 유지됩니다.
- **Lock(잠금)**(잠금 장치 1개) 또는 **Lock both locks(잠금 장치 둘 다 잠금)**(잠금 장치 2개) - 도어를 잠급니다.
- **Unlock second lock and lock primary(두 번째 잠금 장치 잠금 해제, 기본 잠금 장치 잠금)** - 이 옵션은 도어가 보조 잠금 장치로 구성된 경우에만 사용할 수 있습니다. 도어를 잠금 해제합니다. **Double lock(이중 잠금)**을 누르거나 예약된 도어 상태가 활성화될 때까지 보조 잠금 장치는 잠금 해제된 상태로 유지됩니다.

## 플로어 관리

시스템에 AXIS 9188 Network I/O Relay Module을 설치한 경우 도어 관리와 비슷한 방법으로 플로어를 관리할 수 있습니다.

참고

전역 이벤트가 활성화된 클러스터 모드에서 A1001을 사용하는 경우 각 플로어에 대한 설명이 포함된 고유한 이름을 사용해야 합니다. 예: *"Elevator A, Floor 1"*

참고

각 A1001 Network Door Controller를 통해 최대 2개의 AXIS 9188 Network I/O Relay Module을 구성할 수 있습니다.

각 플로어에 대한 일반 룰은 **Floors(플로어)** 탭에서 관리됩니다. 룰에는 사용자에게 플로어에 대한 접근 권한이 부여되는 방법을 결정하는 식별 유형과 각 식별 유형이 유효한 때를 결정하는 접근 일정이 포함됩니다. 자세한 내용은 *식별 유형 플로어 페이지 39* 및 *접근 일정 생성 및 편집 페이지 33* 항목을 참조하십시오.

플로어를 관리하려면 먼저 하드웨어 구성을 완료하여 플러어를 접근 제어 시스템에 추가해야 합니다. *하드웨어 구성 페이지 14* 항목을 참조하십시오.

플로어를 관리하려면

1. **Access Management(접근 관리)**로 이동하여 **Floors(플로어)** 탭을 선택합니다.
2. **Floors(플로어)** 목록에서 편집할 플로어 옆의 ▶ 을 클릭합니다.
3. 플로어를 하나 이상의 그룹으로 끕니다. **Groups(그룹)** 목록이 비어 있으면 새 그룹을 생성합니다. *그룹 생성 및 편집 페이지 35* 항목을 참조하십시오.

4. **Add identification type(식별 유형 추가)**을 클릭하고 플로어에 대한 접근 권한을 부여받기 위해 사용자가 리더에 제공해야 할 자격 증명을 선택합니다. *식별 유형 플로어 페이지 39* 항목을 참조하십시오.

   각 플로어에 하나 이상의 식별 유형을 추가합니다.

5. 여러 식별 유형을 추가하려면 이전 단계를 반복합니다.

   **Card number only(카드 번호만)**와 **PIN only(PIN만)** 두 식별 유형을 모두 추가한 경우 사용자는 카드를 긁거나 핀을 입력하는 두 가지 방법 중 하나로 도어에 접근할 수 있습니다. 그러나 **Card number and PIN(카드 번호 및 PIN)** 식별 유형만 추가한 경우에는 사용자가 카드를 긁고 PIN을 입력하는 두 가지 작업을 모두 수행해야 도어에 접근할 수 있습니다.

6. 자격 증명의 유효 기간을 정의하려면 일정을 각 식별 유형으로 끕니다.

수동으로 플로어의 잠금을 해제하거나 잠그거나 임시 접근 권한을 부여하려면 필요에 따라 수동 도어 액션 중 하나를 클릭합니다. *수동 플로어 액션 사용 페이지 40* 항목을 참조하십시오.

참고

무선 도어/장치에 대해서는 수동으로 플로어의 잠금을 해제하거나 잠그거나 임시 접근 권한을 부여하는 컨트롤을 사용할 수 없습니다.

**Floors(플로어)** 목록의 항목을 확장하려면 을 클릭합니다.

플로어 또는 리더 이름을 편집하려면 을 클릭하고 변경합니다. 그런 다음 **Save(저장)**를 클릭합니다.

리더, 식별 유형 및 접근 일정 조합을 확인하려면 을 클릭합니다.

플로어에 연결된 잠금 장치의 기능을 확인하려면 확인 컨트롤을 클릭합니다. *컨트롤 플로어 확인 페이지 21* 항목을 참조하십시오.

식별 유형 또는 접근 일정을 삭제하려면 을 클릭합니다.

### 식별 유형 플로어

식별 유형은 이동식 자격 증명 저장 장치, 기억된 정보 또는 사용자가 플로어에 접근하도록 허용하는 방법을 결정하는 다양한 조합입니다. 공통적인 식별 유형에는 카드나 전자 열쇠와 같은 토큰, PIN(개인 식별 번호), REX(종료 요청) 장치 등이 있습니다.

자격 증명에 대한 자세한 내용은 *사용자 자격 증명 페이지 41* 항목을 참조하십시오.

다음과 같은 식별 유형을 사용할 수 있습니다.

- **Facility code only(시설 코드만)** - 사용자가 카드 또는 리더에서 수락한 시설 코드가 있는 그 밖의 토큰을 사용하여 플로어에 접근할 수 있습니다.
- **Card number only(카드 번호만)** - 사용자가 카드 또는 리더에서 수락한 그 밖의 토큰만 사용하여 플로어에 접근할 수 있습니다. 카드 번호는 대개 카드에 찍힌 고유 번호입니다. 카드 번호 위치는 카드 제조업체의 정보를 참조하십시오. 시스템에서 카드 번호를 검색할 수도 있습니다. 연결된 리더에 카드를 긁고 목록에서 리더를 선택한 후 **Retrieve(검색)**를 클릭합니다.
- **Card raw only(카드 로우만)** - 사용자가 카드 또는 리더에서 수락한 그 밖의 토큰만 사용하여 플로어에 접근할 수 있습니다. 정보가 원시 데이터로 카드에 저장됩니다. 시스템에서 카드 원시 데이터를 검색할 수 있습니다. 연결된 리더에 카드를 긁고 목록에서 리드를 선택한 후 **Retrieve(검색)**를 클릭합니다. 카드 번호를 찾을 수 없으면 이 식별 유형만 사용하십시오.
- **PIN only(PIN만)** - 사용자가 4자리 PIN(개인 식별 번호)만 사용하여 플로어에 접근할 수 있습니다.
- **Facility code and PIN(시설 코드 및 PIN)** - 사용자가 카드 또는 리더에서 수락한 시설 코드를 가진 그 밖의 토큰 및 PIN을 둘 다 사용하여 플로어에 접근해야 합니다. 사용자는 지정된 순서로(카드, PIN 순서로) 자격 증명을 제공해야 합니다.

- **Card number and PIN(카드 번호 및 PIN)** - 사용자는 카드 또는 리더에서 수락한 그 밖의 토큰과 PIN을 둘 다 사용하여 플로어에 접근해야 합니다. 사용자는 지정된 순서로(카드, PIN 순서로) 자격 증명을 제공해야 합니다.
- **Card raw and PIN(카드 로우 및 PIN)** - 사용자는 카드 또는 리더에서 수락한 그 밖의 토큰과 PIN을 둘 다 사용하여 플로어에 접근해야 합니다. 카드 번호를 찾을 수 없으면 이 식별 유형만 사용하십시오. 사용자는 지정된 순서로(카드, PIN 순서로) 자격 증명을 제공해야 합니다.
- **REX** - 사용자는 버튼, 센서, 푸시 바 등의 REX(종료 요청) 장치를 활성화하여 플로어에 접근할 수 있습니다.

### 예약된 잠금 해제 상태 추가

자동으로 일정한 기간에 누구나 플로어에 접근할 수 있게 하려면 **Scheduled unlock(예약된 잠금 해제)** 상태를 플로어에 추가하고 접근 일정을 적용할 수 있습니다.

예를 들어 근무 시간에 누구나 플로어에 접근할 수 있게 하려면

1. **Access Management(접근 관리)**로 이동하여 **Floors(플로어)** 탭을 선택합니다.
2. 편집할 **Floors(플로어)** 목록 항목 옆의 ▶ 을 클릭합니다.
3. **Add scheduled unlock(예약된 잠금 해제 추가)**을 클릭합니다.
4. 플로어에 잠금 장치가 1개인지 2개인지에 따라 **Unlock state(잠금 해제 상태)**(**unlocked(잠금 해제됨)** 또는 **unlock both locks(잠금 장치 둘 다 잠금 해제)**)를 선택합니다.
5. **OK(확인)**를 클릭합니다.
6. 사전 정의된 **Office hours(근무 시간)** 접근 일정을 **Scheduled unlock(예약된 잠금 해제)** 상태에 적용합니다.

플로어에 접근할 수 있는 시간을 확인하려면  을 클릭합니다.

예약된 잠금 해제 상태나 접근 일정을 삭제하려면 ⊖ 을 클릭합니다.

### 수동 플로어 액션 사용

플로어의 접근 가능성이 각기 다르거나 모두에게 제한적이거나 모두가 접근할 수 있습니다. **Manual floor actions(수동 플로어 액션)**를 통해 **Floors(플로어)** 탭에서 임시 접근 권한을 부여할 수 있습니다. 특정 플로어에 사용할 수 있는 수동 플로어 액션은 플로어를 구성한 방법에 따라 다릅니다.

수동 플로어 액션을 사용하려면

1. **Access Management(접근 관리)**로 이동하여 **Floors(플로어)** 탭을 선택합니다.
2. **Floors(플로어)** 목록에서 제어할 플로어 옆의 ▶ 을 클릭합니다.
3. 필요한 플로어 액션을 클릭합니다. *수동 플로어 액션 페이지 40* 항목을 참조하십시오.

참고

수동 플로어 액션을 사용하려면 해당 도어가 연결되는 플로어 컨트롤러를 통해 접근 관리 페이지를 열어야 합니다. 다른 플로어 컨트롤러를 통해 접근 관리 페이지를 열면 수동 플로어 액션 대신 해당 플로어가 연결된 플로어 컨트롤러의 개요 페이지로 연결하는 링크가 있습니다. 링크를 클릭하고 **Access Management(접근 관리)**로 이동하여 **Floors(플로어)** 탭을 선택합니다.

#### 수동 플로어 액션

다음과 같은 수동 플로어 액션을 사용할 수 있습니다.

- **Get floor status(플로어 상태 가져오기)** - 플로어에 연결된 릴레이의 현재 상태를 확인합니다.

- **Access(접근)** - 사용자에게 도어 접근을 허용합니다. 주어진 접근 시간이 적용됩니다. *도어 모니터 및 잠금을 구성하는 방법 페이지 15* 항목을 참조하십시오.
- **Unlock(잠금 해제)** - **Lock(잠금)**을 누르거나 예약된 플로어 상태가 활성화되거나 도어 컨트롤러가 다시 시작될 때까지 모든 사람이 플로어에 완전히 접근할 수 있습니다.
- **Lock(잠금)** - **Unlock(잠금 해제)**을 누르거나 예약된 플로어 상태가 활성화되거나 도어 컨트롤러가 다시 시작될 때까지 모든 사람이 플로어에 액세스할 수 없습니다.

## 사용자 생성 및 편집

개인마다 접근 제어 시스템의 도어에 접근할 수 있도록 고유한 사용자 프로파일이 있어야 합니다. 사용자 프로파일은 사용자가 누구이며 도어에 언제 어떻게 접근할 수 있는지 시스템에 알려주는 자격 증명으로 구성됩니다.

사용자 접근 권한을 효율적으로 관리하려면 각 사용자가 하나 이상의 그룹에 속해 있어야 합니다. 자세한 내용은 *그룹 생성 및 편집* 항목을 참조하십시오.

새 사용자 프로파일을 생성하려면

1. **Access Management(접근 관리)**로 이동합니다.
2. **Users(사용자)** 탭을 선택하고 **Add new user(새 사용자 추가)**를 클릭합니다.
3. **Add User(사용자 추가)** 대화 상자에 사용자의 자격 증명을 입력합니다. *사용자 자격 증명 페이지 41* 항목을 참조하십시오.
4. **Save(저장)**를 클릭합니다.
5. **Groups(그룹)** 목록에 있는 하나 이상의 그룹으로 사용자를 끌어 놓습니다. **Groups(그룹)** 목록이 비어 있으면 새 그룹을 생성합니다. *그룹 생성 및 편집 페이지 35* 항목을 참조하십시오.

**Users(사용자)** 목록에 있는 항목을 확장하여 사용자의 자격 증명을 보려면  을 클릭합니다.

특정 사용자를 찾으려면 필터 사용자 필드에 필터를 입력합니다. 정확하게 일치하는 항목을 찾으려면 큰따옴표로 필터 텍스트를 묶으십시오(예: "John" 또는 "potter, virginia").

사용자 자격 증명을 편집하려면  을 클릭하고 필요에 따라 자격 증명을 변경합니다. 그런 다음 **Save(저장)**를 클릭합니다.

사용자를 삭제하려면  을 클릭합니다.

중요 사항

AXIS Visitor Manager를 통해 사용자가 생성된 경우 AXIS Entry Manager에서 편집하거나 삭제하지 마십시오. AXIS Visitor Manager 및 QR 코드 리더 서비스에 대한 자세한 내용은 *AXIS Visitor Access 페이지 24* 항목을 참조하십시오.

### 사용자 자격 증명

사용자에 대해 다음과 같은 자격 증명을 사용할 수 있습니다.

- **First name(이름)**(필수)
- **Last name(성)**
- **Valid from(유효 기간 시작)** 및 **Valid until(유효 기간 만료)** - 사용자 자격 증명이 유효한 날짜를 입력합니다. 날짜 필드를 클릭하고 원하는 월, 일, 연도를 선택합니다. 필드에 날짜를 직접 입력할 수도 있습니다.
- **Suspend credential(자격 증명 일시 중단)** - 자격 증명을 일시 중단하려면 선택합니다. 일시 중단된 경우 사용자는 시스템에서 이 자격 증명을 통해 도어에 접근할 수 없습니다. 사용자 접근 권한을 다시 부여하려면 선택 취소하십시오. 일시 중단은 일시적인 조치입니다. 사용자의 접근을 영구히 거부하려면 사용자 프로파일을 삭제하는 것이 좋습니다.

- **PIN**(카드 번호 또는 카드 로우가 없는 경우에 필요) - 사용자가 선택하거나 사용자에게 할당된 4자리 PIN(개인 식별 번호)을 입력합니다.
- **Facility code(시설 코드)** - 시설의 접근 제어 시스템을 확인하기 위한 코드를 입력합니다. 프리셋 시설 코드를 입력한 경우 이 필드가 자동으로 채워집니다. 자세한 내용은 *사전 설정 시설 코드 페이지 24* 항목을 참조하십시오.
- **Card number(카드 번호)**(PIN 또는 카드 로우가 없는 경우에 필요) - 카드 번호를 입력합니다. 카드 번호 위치는 카드 제조업체의 정보를 참조하십시오. 시스템에서 카드 번호를 검색할 수도 있습니다. 연결된 리더에 카드를 긁고 목록에서 리더를 선택한 후 **Retrieve(검색)**를 클릭합니다.
- **Card raw(카드 로우)**(PIN 또는 카드 번호가 없는 경우에 필요) - 카드 원시 데이터를 입력합니다. 시스템에서 데이터를 검색할 수 있습니다. 연결된 리더에 카드를 긁고 목록에서 리더를 선택한 후 **Retrieve(검색)**를 클릭합니다. 카드 번호를 찾을 수 없으면 이 식별 유형만 사용하십시오.
- **Long access time(긴 접근 시간)** - 기존 접근 시간을 무시하고 사용자가 긴 접근 시간 동안 도어를 열 수 있도록 허용하려면 선택합니다. 자세한 내용은 *도어 모니터 및 시간 옵션 정보 페이지 16* 항목을 참조하십시오.
- **License plate(번호판)**(기본 도어 컨트롤러 설치에는 이 자격 증명을 사용할 수 없음) - 파트너 소프트웨어에서 이 자격 증명을 활성화한 경우 사용자 차량의 번호판 번호를 입력합니다.
  이 자격 증명은 Axis 파트너 소프트웨어 및 번호판 인식 소프트웨어가 있는 카메라와 함께 사용해야 합니다. 자세한 내용은 Axis 파트너 또는 현지 Axis 영업 담당자에게 문의하십시오.

참고

**Retrieve(검색)** 버튼은 하드웨어 구성을 완료하고 하나 이상의 리더를 컨트롤러에 연결한 경우에만 사용할 수 있습니다.

### 사용자 가져오기

쉼표로 구분된 값(CSV) 형식으로 텍스트 파일을 가져와서 사용자를 시스템에 추가할 수 있습니다. 한 번에 많은 사용자를 추가해야 하는 경우 사용자를 가져오는 것이 좋습니다.

사용자를 가져오려면 파일(*.csv 또는 *.txt)을 만든 후 올바른 CSV 형식으로 저장해야 합니다. 값을 공백 없이 쉼표로 구분하고 각 사용자를 줄 바꿈으로 구분합니다.

**예시**

```
jane,doe,1234,12345678,abc123
john,doe,5435,87654321,cde321
```

사용자를 가져오려면

1. **Setup > Import Users(설정 > 사용자 가져오기)**로 이동합니다.
2. 사용자 목록이 보관된 *.csv 또는 *.txt 파일을 찾아서 선택합니다.
3. 각 열에 대해 올바른 자격 증명 옵션을 선택합니다.
4. 사용자를 시스템으로 가져오려면 **Import users(사용자 가져오기)**를 클릭합니다.
5. 각 열에 올바른 유형의 자격 증명이 포함되어 있는지 확인합니다.
6. 열이 올바른 경우 **Start importing users(사용자 가져오기 시작)**를 클릭합니다. 열이 잘못된 경우 **Cancel(취소)**을 클릭하고 다시 시작합니다.
7. 가져오기를 완료한 후 **OK(확인)**를 클릭합니다.

다음 자격 증명 옵션을 사용할 수 있습니다.

- **First name(이름)**
- **Last name(성)**
- **PIN code(PIN 코드)**

- **Card number(카드 번호)**
- **License plate(번호판)**
- **Unassigned(할당되지 않음)** - 가져오지 않을 값입니다. 특정 열을 건너뛰려면 이 옵션을 선택합니다.

자격 증명에 대한 자세한 내용은 *사용자 생성 및 편집* 항목을 참조하십시오.

### 사용자 내보내기

내보내기 페이지에는 시스템에 있는 모든 사용자의 쉼표로 구분된 값(CSV) 목록이 표시됩니다. 이 목록을 사용하여 사용자를 다른 시스템으로 가져올 수 있습니다.

사용자 목록을 내보내려면

1. 일반 텍스트 편집기를 열고 새 문서를 만듭니다.
2. **Setup > Export Users(설정 > 사용자 내보내기)**로 이동합니다.
3. 페이지에 있는 모든 값을 선택하고 복사합니다.
4. 값을 텍스트 문서에 붙여넣습니다.
5. 문서를 쉼표로 구분된 값 파일(*csv) 또는 텍스트(*.txt) 파일로 저장합니다.

## 접근 일정 조합의 예

여러 가지 방식으로 식별 유형과 그룹 일정을 조합하여 다양한 결과를 얻을 수 있습니다. 아래의 예는 *페이지 32*에서 설명하는 작업 흐름을 따릅니다.

**예시**

다음과 같은 일정 조합을 만들려면

- 항상 경비원이 도어에 접근할 수 있게 합니다.
  - 주간 교대 근무 시간(월요일 ~ 금요일 오전 6시 ~ 오후 4시) 중에 경비원이 카드를 사용합니다.
  - 주간 교대 근무 시간 전후에 카드와 PIN을 사용합니다.
- 주간 교대 근무자가 같은 도어에 접근할 수 있게 합니다.
  - 주간 교대 근무 시간 중에만 카드를 사용합니다.

1. **Day shift hours(주간 교대 근무 시간)**라는 **Addition schedule(추가 일정)**을 만듭니다. *페이지 33* 항목을 참조하십시오.
2. 월요일 ~ 금요일, 06:00 ~ 16:00로 반복되는 주간 교대 근무 시간 **Schedule item(일정 항목)**을 만듭니다.
3. 한 **Group(그룹)**은 **Guards(경비원)**이고 한 **Group(그룹)**은 **Day shift personnel(주간 교대 근무자)**인 두 그룹을 만듭니다. *페이지 35* 항목을 참조하십시오.
4. 사전 정의된 **Always(항상)** 접근 일정을 **Guards(경비원)** 그룹으로 끌어 놓습니다.
5. **Day shift hours(주간 교대 근무 시간)** 접근 일정을 **Day shift personnel(주간 교대 근무자)** 그룹으로 끌어 놓습니다.
6. **Card number and PIN(카드 번호 및 PIN)** 및 **Card number only(카드 번호만)** 식별 유형을 도어 리더에 추가합니다.
7. 사전 정의된 **Always(항상)** 접근 일정을 **Card number and PIN(카드 번호 및 PIN)** 식별 유형으로 끌어 놓습니다.

8. **Day shift hours(주간 교대 근무 시간)** 접근 일정을 **Card number only(카드 번호만)** 식별 유형으로 끌어 놓습니다.
9. 도어를 두 그룹으로 끌어 놓습니다. 그런 다음 필요에 따라 그룹에 사용자를 추가합니다. *페이지 41* 항목을 참조하십시오.

**예시**

다음과 같은 일정 조합을 만들려면

- 항상 경비원이 도어에 접근할 수 있게 합니다.
  - 주간 교대 근무 시간(월요일 ~ 금요일 오전 6시 ~ 오후 4시) 중에 경비원이 카드를 사용합니다.
  - 주간 교대 근무 시간 전후에 카드와 PIN을 사용합니다.
- 매일 오전 6시 ~ 오후 4시에 주간 교대 근무자가 같은 도어에 접근할 수 있게 합니다.,
  - 주간 교대 근무 시간 중에 카드를 사용합니다.
  - 야간 및 주말에 카드와 PIN을 사용합니다.

1. **Day shift hours(주간 교대 근무 시간)**라는 **Addition schedule(추가 일정)**을 만듭니다. *페이지 33* 항목을 참조하십시오.
2. 월요일 ~ 금요일, 06:00 ~ 16:00로 반복되는 주간 교대 근무 시간 **Schedule item(일정 항목)**을 만듭니다.
3. **Nights & weekends(야간 및 주말)**라는 **Subtraction schedule(삭제 일정)**을 만듭니다.
4. 일요일 ~ 토요일, 16:00 ~ 06:00에 반복되는 야간 및 주말 **Schedule item(일정 항목)**을 만듭니다.
5. 사전 정의된 **Always(항상)** 일정과 **Nights & weekends(야간 및 주말)** 접근 일정을 **Day shift personnel(주간 교대 근무자)** 그룹으로 끌어 놓습니다.
6. 한 **Group(그룹)**은 **Guards(경비원)**이고 한 **Group(그룹)**은 **Day shift personnel(주간 교대 근무자)**인 두 그룹을 만듭니다. *페이지 35* 항목을 참조하십시오.
7. 사전 정의된 **Always(항상)** 접근 일정을 **Guards(경비원)** 그룹과 **Day shift personnel(주간 교대 근무자)** 그룹으로 끌어 놓습니다.
8. **Nights & weekends(야간 및 주말)** 접근 일정을 **Day shift personnel(주간 교대 근무자)** 그룹으로 끌어 놓습니다.
9. **Card number and PIN(카드 번호 및 PIN)** 및 **Card number only(카드 번호만)** 식별 유형을 도어 리더에 추가합니다.
10. 사전 정의된 **Always(항상)** 접근 일정을 **Card number and PIN(카드 번호 및 PIN)** 식별 유형으로 끌어 놓습니다.
11. **Day shift hours(주간 교대 근무 시간)** 접근 일정을 **Card number only(카드 번호만)** 식별 유형으로 끌어 놓습니다.
12. 도어를 두 그룹으로 끌어 놓습니다. 그런 다음 필요에 따라 그룹에 사용자를 추가합니다. *페이지 41* 항목을 참조하십시오.

# 알람 및 이벤트 구성

시스템에서 발생하는 이벤트(예: 사용자가 카드를 밀거나 REX 장치가 활성화된 경우)는 이벤트 로그에 기록됩니다. 기록된 이벤트가 알람을 트리거하도록 구성할 수 있으며 해당 알람은 알람 로그에 기록됩니다.

- 이벤트 로그를 봅니다. *페이지 45* 항목을 참조하십시오.
- 이벤트 로그를 내보냅니다. *페이지 45* 항목을 참조하십시오.
- 알람 로그를 봅니다. *페이지 46* 항목을 참조하십시오.
- 이벤트 및 알람 로그를 구성합니다. *페이지 46* 항목을 참조하십시오.

이메일 알림과 같은 액션을 트리거하도록 알람을 구성할 수도 있습니다. 자세한 내용은 *액션 룰을 설정하는 방법 페이지 47* 항목을 참조하십시오.

## 이벤트 로그 보기

기록된 이벤트를 보려면 **Event Log(이벤트 로그)**로 이동합니다.

글로벌 이벤트가 활성화된 경우 시스템의 도어 컨트롤러에서 이벤트 로그를 열 수 있습니다. 글로벌 이벤트에 대한 자세한 내용은 *이벤트 및 알람 로그 구성 페이지 46* 항목을 참조하십시오.

이벤트 로그의 항목을 확장하고 이벤트 세부 정보를 보려면 ▶ 을 클릭하십시오.

이벤트 로그에 필터를 적용하면 특정 이벤트를 더 쉽게 찾을 수 있습니다. 목록을 필터링하려면 하나 이상의 이벤트 로그 필터를 선택하고 **Apply filters(필터 적용)**를 클릭합니다. 자세한 내용은 *이벤트 로그 필터 페이지 45* 항목을 참조하십시오.

관리자는 다른 이벤트보다 일부 이벤트에 더 관심이 있을 수 있습니다. 따라서 기록할 이벤트와 이벤트를 기록할 대상 컨트롤러를 선택할 수 있습니다. 자세한 내용은 *이벤트 로그 옵션 페이지 46* 항목을 참조하십시오.

### 이벤트 로그 필터

다음 필터 중 하나 이상을 선택하여 이벤트 로그의 범위를 좁힐 수 있습니다.

- 사용자 - 선택한 사용자와 관련된 이벤트를 필터링합니다.
- 도어 및 플로어 - 특정 도어 또는 플로어와 관련된 이벤트를 필터링합니다.
- 주제 - 이벤트 유형을 필터링합니다.
- 소스 - 선택한 컨트롤러에서 이벤트를 필터링합니다. 글로벌 이벤트가 활성화된 경우에 컨트롤러 클러스터에서만 사용할 수 있습니다.
- 날짜 및 시간 - 날짜 및 시간 범위로 이벤트 로그를 필터링합니다.

### 이벤트 로그 내보내기

기록된 이벤트를 내보내려면 **Event Log(이벤트 로그)**로 이동합니다.

1. ⬇ 을 클릭합니다.
2. 팝업 메뉴에서 내보내기 형식을 선택하여 내보내기를 시작합니다.

참고

CSV 형식은 모든 브라우저에서 지원되고, XLSX 형식은 Chrome™ 및 Internet Explorer®에서 지원됩니다.

참고

내보내기가 완료되면 내보내기 버튼이  에서  으로 변경됩니다. 다른 내보내기를 시작하려면 웹 페이지를 새로 고칩니다. 내보내기 버튼이 다시  으로 변경됩니다.

## 알람 로그 보기

트리거된 알람을 보려면 **Alarm Log(알람 로그)**로 이동합니다. 글로벌 이벤트가 활성화된 경우 시스템의 도어 컨트롤러에서 알람 로그를 열 수 있습니다. 글로벌 이벤트에 대한 자세한 내용은 *이벤트 및 알람 로그 구성 페이지 46* 항목을 참조하십시오.

알람 로그의 항목을 확장하고 알람 세부 정보(예: 도어 ID 및 상태)를 보려면  을 클릭합니다.

알람의 원인을 확인한 후 목록에서 알람을 제거하려면 **Acknowledge(승인)**를 클릭합니다. 모든 알람을 제거하려면 **Acknowledge all alarms(모든 알람 승인)**를 클릭합니다.

관리자는 알람을 트리거하는 일부 이벤트가 필요할 수 있습니다. 따라서 알람을 트리거할 이벤트와 해당 컨트롤러를 선택할 수 있습니다. 자세한 내용은 *알람 로그 옵션 페이지 47* 항목을 참조하십시오.

## 이벤트 및 알람 로그 구성

이벤트 및 알람 로그 구성 페이지에서 기록되고 알람을 트리거할 이벤트를 정의할 수 있습니다.

모든 연결된 컨트롤러 간에 이벤트 및 알람을 공유하려면 **Global events(글로벌 이벤트)**를 선택합니다. 글로벌 이벤트를 활성화한 경우 이벤트 로그 페이지와 알람 로그 페이지를 하나씩만 열어서 시스템의 모든 도어 컨트롤러에 대한 이벤트와 알람을 동시에 관리해야 합니다. 글로벌 이벤트는 기본적으로 활성화됩니다.

글로벌 이벤트를 비활성화할 경우 개별 도어 컨트롤러에 대해 이벤트 로그 페이지와 알람 로그 페이지를 하나씩 열고 해당 이벤트와 알람을 별도로 관리해야 합니다.

중요 사항

글로벌 이벤트를 활성화하거나 비활성화할 때마다 이벤트 로그가 지워집니다. 즉, 해당 시점 이전의 모든 이벤트가 제거되고 이벤트 로그가 다시 시작됩니다.

이메일 알림과 같은 액션을 트리거하도록 알람을 구성할 수도 있습니다. 자세한 내용은 *액션 룰을 설정하는 방법 페이지 47* 항목을 참조하십시오.

### 이벤트 로그 옵션

이벤트 로그에 포함될 이벤트를 정의하려면 **Setup > Configure Event and Alarm Logs(설정 > 이벤트 및 알람 로그 구성)**으로 이동합니다.

다음과 같은 이벤트 로깅 옵션을 사용할 수 있습니다.

- **No logging(로깅 안 함)** - 이벤트 로깅을 비활성화합니다. 이벤트가 등록되지 않거나 이벤트 로그에 포함되지 않습니다.
- **Log for all sources(모든 소스의 로그)** - 모든 도어 컨트롤러에서 이벤트 로깅을 활성화합니다. 이벤트가 모든 컨트롤러에 대해 등록되고 이벤트 로그에 포함됩니다.
- **Log for selected sources(선택한 소스의 로그)** - 선택한 도어 컨트롤러에서 이벤트 로깅을 활성화합니다. 이벤트가 모든 선택된 컨트롤러에 대해 등록되고 이벤트 로그에 포함됩니다. 알람 로그 옵션 **No alarms(알람 없음)** 또는 **Log alarm for selected controllers(선택한 컨트롤러의 알람 로그)**와 결합될 이벤트에 대해 이 옵션을 선택합니다.

  **Configure event logging(이벤트 로깅 구성)** 목록에서 활성화하려는 이벤트 로그 항목 아래에 있는 **Select controllers(컨트롤러 선택)**를 클릭합니다. **Device Specific Event Logging(장치별 이벤트 로깅)** 대화 상자가 열립니다. **Log event(로그 이벤트)**에서 알람 로깅을 활성화할 컨트롤러를 선택하고 **Save(저장)**를 클릭합니다.

### 알람 로그 옵션

알람을 트리거할 이벤트를 정의하려면 **Setup > Configure Event and Alarm Logs(설정 > 이벤트 및 알람 로그 구성)**로 이동합니다.

다음과 같은 알람 트리거 및 로깅 옵션을 사용할 수 있습니다.

- **No alarms(알람 없음)** - 알람 로깅을 비활성화합니다. 이벤트가 알람을 트리거하지 않거나 알람 로그에 포함되지 않습니다.
- **Log alarm for all sources(모든 소스에 대한 알람 로그)** - 모든 도어 컨트롤의 알람 로깅을 활성화합니다. 이벤트가 알람을 트리거하고 알람 로그에 포함됩니다.
- **Log alarm for selected sources(선택한 소스에 대한 알람 로그)** - 선택한 도어 컨트롤러의 알람 로깅을 활성화합니다. 이벤트가 알람을 트리거하고 알람 로그에 포함됩니다.

  **Configure alarm logging(알람 로깅 구성)** 목록에서 활성화할 알람 로그 항목 아래의 **Select sources(소스 선택)**를 클릭합니다. **Device Specific Alarm Triggering(장치별 알람 트리거링)** 대화 상자가 열립니다. **Trigger alarm(알람 트리거)**에서 알람 로깅을 활성화할 도어 컨트롤러를 선택하고 **Save(저장)**를 클릭합니다.

## 액션 룰을 설정하는 방법

이벤트 페이지에서는 다양한 이벤트가 발생할 때 액션을 수행하도록 Axis 제품을 구성할 수 있습니다. 예를 들어, 알람이 트리거되면 제품에서 전자 메일 알림을 보내거나 출력 포트를 활성화하도록 구성할 수 있습니다. 액션이 트리거되는 방법 및 시기를 정의하는 조건 세트를 액션 룰이라고 합니다. 여러 조건이 정의된 경우 액션을 트리거하려면 모든 조건이 충족되어야 합니다.

사용 가능한 트리거 및 액션에 대한 자세한 내용은 *트리거 페이지 48* 및 *액션 페이지 50* 항목을 참조하십시오.

이 예에서는 알람이 트리거되면 이메일 알림을 전송하는 액션 룰을 설정하는 방법을 설명합니다.

1. 알람을 구성합니다. *이벤트 및 알람 로그 구성 페이지 46* 항목을 참조하십시오.
2. **Setup > Additional Controller Configuration > Events > Action Rules(설정 > 추가 컨트롤러 구성 > 이벤트 > 액션 룰)**로 이동하고 **Add(추가)**를 클릭합니다.
3. **Enable rule(룰 활성화)**을 선택하고 룰에 대한 설명이 포함된 이름을 입력합니다.
4. **Trigger(트리거)** 드롭다운 목록에서 **Event Logger(이벤트 로거)**를 선택합니다.
5. 선택 사항으로 **Schedule(스케줄)** 및 **Additional conditions(추가 조건)**를 선택합니다. 아래 내용을 참조하십시오.
6. **Actions(액션)**에서 **Type(유형)** 드롭다운 목록의 **Send Notification(알림 전송)**을 선택합니다.
7. 드롭다운 목록에서 이메일 수신자를 선택합니다. *수신자를 추가하는 방법 페이지 50* 항목을 참조하십시오.

이 예에서는 도어가 강제로 열릴 때 출력 포트를 활성화하는 액션 룰을 설정하는 방법을 설명합니다.

1. **Setup > Additional Controller Configuration > System Options > Ports & Devices > I/O Ports(설정 > 추가 컨트롤러 구성 > 시스템 옵션 > 포트 및 장치 > I/O 포트)**로 이동합니다.
2. 원하는 **I/O Port Type(I/O 포트 유형)** 드롭다운 목록에서 **Output(출력)**을 선택하고 **Name(이름)**을 입력합니다.
3. I/O 포트의 **Normal state(정상 상태)**를 선택하고 **Save(저장)**를 클릭합니다.
4. **Events > Action Rules(이벤트 > 액션 룰)**로 이동하여 **Add(추가)**를 클릭합니다.
5. **Trigger(트리거)** 드롭다운 목록에서 **Door(도어)**를 선택합니다.
6. 드롭다운 목록에서 **Door Alarm(도어 알람)**을 선택합니다.
7. 드롭다운 목록에서 원하는 도어를 선택합니다.

8. 드롭다운 목록에서 **DoorForcedOpen(도어 강제 열림)**을 선택합니다.
9. 선택 사항으로 **Schedule(스케줄)** 및 **Additional conditions(추가 조건)**를 선택합니다. 아래 내용을 참조하십시오.
10. **Actions(액션)**에서 **Type(유형)** 드롭다운 목록의 **Output Port(출력 포트)**를 선택합니다.
11. **Port(포트)** 드롭다운 목록에서 원하는 출력 포트를 선택합니다.
12. 상태를 **Active(활성)**로 설정합니다.
13. **Duration(기간)** 및 **Go to opposite state after(이후 반대 상태로 이동)**를 선택합니다. 그런 다음 원하는 액션 기간을 입력합니다.
14. **OK(확인)**를 클릭합니다.

액션 룰에 둘 이상의 트리거를 사용하려면 **Additional conditions(추가 조건)**를 선택하고 **Add(추가)**를 클릭하여 추가 트리거를 추가합니다. 추가 조건을 사용하는 경우 액션을 트리거하려면 모든 조건이 충족되어야 합니다.

액션이 반복적으로 트리거되지 않도록 **Wait at least(최소 대기 시간)** 시간을 설정할 수 있습니다. 액션 룰이 다시 활성화되기 전까지 트리거가 무시되어야 하는 시간(시간, 분, 초)을 입력합니다.

자세한 내용은 제품의 기본 도움말을 참조하십시오.

### 트리거

사용 가능한 **트리거** 및 **조건** 액션 룰은 다음과 같습니다.

- **Access Point(접근 포인트)**
  - **Access Point Enabled(접근 포인트 활성화)** - 하드웨어 구성이 완료되었거나 식별 유형이 추가된 것과 같이 리더나 REX 장치 등 접근 포인트 장치가 구성되었을 때 액션 룰을 트리거합니다.
- **Configuration(구성)**
  - **Access Point Changed(접근 포인트 변경)** - 하드웨어가 구성되었거나 식별 유형 편집, 도어를 접근할 수 있는 방식 변경과 같이 리더나 REX 장치 등 접근 포인트 장치 구성이 변경되었을 때 액션 룰을 트리거합니다.
  - **Access Point Removed(접근 포인트 제거)** - 리더나 REX 장치 등 접근 포인트 장치의 하드웨어 구성이 재설정되었을 때 액션 룰을 트리거합니다.
  - **Area Changed(영역 변경)** - 이 버전의 AXIS Entry Manager가 지원하지 않습니다. 이 기능을 지원하고 필요한 신호를 제공할 수 있는 장치를 사용하는 VAPIX® 애플리케이션 프로그래밍 인터페이스를 통해 액세스 관리 시스템 같은 클라이언트가 구성해야 합니다. 액세스 영역이 변경되면 액션 룰을 트리거합니다.
  - **Area Removed(영역 제거)** - 이 버전의 AXIS Entry Manager가 지원하지 않습니다. 이 기능을 지원하고 필요한 신호를 제공할 수 있는 장치를 사용하는 VAPIX® 애플리케이션 프로그래밍 인터페이스를 통해 액세스 관리 시스템 같은 클라이언트가 구성해야 합니다. 접근 영역이 시스템에서 제거되면 액션 룰을 트리거합니다.
  - **Door Changed(도어 변경)** - 도어 이름과 같은 도어 구성 설정이 변경되거나 시스템에 도어가 추가될 때 액션 룰을 트리거합니다. 예를 들어 도어가 설치되고 구성되었을 때 알림을 보내는 데 사용할 수 있습니다.
  - **Door Removed(도어 제거)** - 시스템에서 도어가 제거되면 액션 룰을 트리거합니다. 예를 들어 시스템에서 도어가 제거되었을 때 알림을 보내기 위해 사용될 수 있습니다.
- **Door(도어)**
  - **Battery Alarm(배터리 알람)** - 무선 도어 배터리 전력이 부족하거나 다 떨어졌을 때 액션 룰을 트리거합니다.

- **Door Alarm(도어 알람)** - 도어가 강제로 열리거나, 도어가 너무 오래 열려 있거나, 도어에 어떤 결함을 발생한 것을 도어 모니터가 표시했을 때 액션 룰을 트리거합니다. 예를 들어 누군가 강제로 들어올 때 알림을 보내기 위해 사용될 수 있습니다.
- **Door Double-Lock Monitor(도어 이중 잠금 모니터)** - 보조 잠금 상태가 잠김 또는 잠김 해제됨으로 변경되었을 때 액션 룰을 트리거합니다.
- **Door Lock Monitor(도어 잠금 모니터)** - 일반 잠금 상태가 잠김 또는 잠김 해제됨으로 변경되었을 때 액션 룰을 트리거합니다. 예를 들어, 도어 모니터가 잠김 상태임에도 불구하고 도어가 열린 경우를 발견했을 때 결함이 트리거됩니다.
- **Door Mode(도어 모드)** - 도어를 접근했거나 차단했을 때, 도어가 차단 모드인 경우와 같이 도어 상태가 변경되었을 때 액션 룰을 트리거합니다. 이런 모드에 대한 자세한 설명은 온라인 도움말을 참조하십시오.
- **Door Monitor(도어 모니터)** - 도어 모니터 상태가 변경되면 액션 룰을 트리거합니다. 예를 들어 도어가 열렸거나 닫힌 것을 도어 모니터가 표시할 때 알림을 보내기 위해 사용될 수 있습니다.
- **Door Tamper(도어 탬퍼)** - 누군가 도어 모니터 배선을 절단한 것과 같이 연결이 차단된 것을 도어 모니터가 표시했을 때 액션 룰을 트리거합니다. 이 트리거를 사용하려면 **Enable supervised inputs(관리된 입력 활성화)**가 선택되었고 라인 저항기 끝이 관련 도어 커넥터 입력 포트에 설치되었는지 확인합니다. 자세한 내용은 *관리된 입력을 사용하는 방법 페이지 18* 항목을 참조하십시오.
- **Door Warning(도어 경고)** - 도어가 너무 오래 열려 있다는 알람이 표시되기 전에 액션 룰을 트리거합니다. 예를 들어, 도어가 너무 오래 열려 있음을 판단하도록 지정한 시간 내에 도어가 닫히지 않은 경우 도어 컨트롤러가 실제 알람을 보내도록 경고 신호를 보내기 위해 사용될 수 있습니다. 도어가 너무 오래 열려 있음에 대한 자세한 내용은 *도어 모니터 및 잠금을 구성하는 방법 페이지 15* 항목을 참조하십시오.
- **Lock Jammed(잠금 재밍)** - 무선 도어 잠금이 물리적으로 차단되었을 때 액션 룰을 트리거합니다.

- **Event Logger(이벤트 로거)** - 사용자가 카드를 밀거나 도어를 연 것과 같은 도어 컨트롤러의 모든 이벤트를 추적합니다. **Global events(글로벌 이벤트)**가 활성화된 경우 이벤트 로거는 시스템에서 모든 컨트롤러의 이벤트 전체를 추적합니다. 액션 룰을 트리거할 수 있는 알람과 이벤트를 설정하려면 **Setup > Configure Event and Alarm Logs(설정 > 이벤트 및 알람 로그 구성)**로 이동합니다. 이벤트 로거는 시스템이 공유하고 30,000개의 이벤트까지 저장할 수 있습니다. 한계에 도달하면 이벤트 로거는 선입선출(First In First Out, FIFO) 룰을 사용합니다. 이는 첫 번째 이벤트를 처음으로 덮어쓴다는 것을 의미합니다.
  - **Alarm(알람)** - 지정된 알람 중 하나가 트리거되었을 때 액션 룰을 트리거합니다. 시스템 관리자는 다른 것에 비해 어떤 이벤트가 더 중요하고 특정 이벤트에 대한 알람 트리거 여부를 구성할 수 있습니다.
  - **Dropped Alarms(손실된 알람)** - 새 알람 레코드를 알람 로그에 쓸 수 없을 때 액션 룰을 트리거합니다. 예를 들어 이벤트 로거가 추적할 수 없을 정도로 동시에 알람이 너무 많이 발생하는 경우가 있습니다. 알람이 손실되면 운영자에게 알림이 전송될 수 있습니다.
  - **Dropped Events(손실된 이벤트)** - 새 이벤트 레코드를 이벤트 로그에 쓸 수 없을 때 액션 룰을 트리거합니다. 예를 들어 이벤트 로거가 추적할 수 없을 정도로 동시에 이벤트가 너무 많이 발생하는 경우가 있습니다. 이벤트가 손실되면 운영자에게 알림이 전송될 수 있습니다.
- **Hardware(하드웨어)**
  - **Network(네트워크)** - 네트워크 연결이 끊어졌을 때 액션 룰을 트리거합니다. 네트워크 연결이 끊어졌을 때 액션 룰을 트리거하려면 **Yes(예)**를 선택합니다. 네트워크 연결이 복구되었을 때 액션 룰을 트리거하려면 **No(아니요)**를 선택합니다. IP 주소가 변경될 때 액션을 트리거하려면 **IPv4/v6 address removed(IPv4/v6 주소 제거됨)** 또는 **New IPv4/v6 address(새 IPv4/v6 주소)**를 선택합니다.
  - **Peer Connection(피어 연결)** - Axis 제품이 다른 도어 컨트롤러와 연결되었거나, 장치 간의 네트워크 연결이 끊어졌거나, 도어 컨트롤러 연결에 실패한 경우 액션 룰을 트리거합니다. 예를 들어 도어 컨트롤러의 네트워크 연결이 끊어졌다는 알림을 보내기 위해 사용할 수 있습니다.
- **Input Signal(입력 신호)**

- **Digital Input Port(디지털 입력 포트)** - I/O 포트가 연결된 장치로부터 신호를 수신하면 액션 룰을 트리거합니다. *I/O 포트 페이지 62* 항목을 참조하십시오.
- **Manual Trigger(수동 트리거)** - 수동 트리거가 활성화될 때 액션 룰을 트리거합니다. 액션 룰을 수동으로 시작하거나 중지하도록 VAPIX® 애플리케이션 프로그래밍 인터페이스를 통해 접근 관리 시스템 같은 클라이언트가 사용할 수 있습니다.
- **Virtual Inputs(가상 입력)** - 가상 입력 중 하나가 상태를 변경하면 액션 룰을 트리거합니다. 액션을 트리거하도록 VAPIX® 애플리케이션 프로그래밍 인터페이스를 통해 접근 관리 시스템 같은 클라이언트가 사용할 수 있습니다. 예를 들어 가상 입력은 관리 시스템의 사용자 시스템에 있는 버튼에 연결될 수 있습니다.

• **Schedule(일정)**

- **Interval(간격)** - 일정의 시작 시간에 액션 룰을 트리거하고 일정의 종료 시간에 도달할 때까지 활성 상태를 유지합니다.
- **Pulse(펄스)** - 이벤트가 한 번 발생하면 액션 룰을 트리거합니다. 즉, 특정 시간에 발생하고 기간이 없는 이벤트입니다.

• **System(시스템)**

- **System Ready(시스템 준비 완료)** - 시스템이 준비 완료 상태일 때 액션 룰을 트리거합니다. 예를 들어, Axis 제품이 시스템 상태를 감지한 후 시스템이 가동될 때 알림을 보냅니다.

  제품이 준비 완료 상태일 때 액션 룰을 트리거하려면 **Yes(예)**를 선택합니다. 참고로 룰은 이벤트 시스템과 같이 필요한 모든 서비스가 시작되었을 때에만 트리거됩니다.

• **Time(시간)**

- **Recurrence(반복)** - 생성된 반복을 모니터링하여 액션 룰을 트리거합니다. 이 트리거를 사용하여 매 시간 알림 보내기 등과 같은 반복 액션을 시작할 수 있습니다. 반복 패턴을 선택하거나 새 패턴을 만듭니다. 반복 패턴 설정에 대한 자세한 내용은 *반복을 설정하는 방법 페이지 52* 항목을 참조하십시오.
- **Use Schedule(스케줄 사용)** - 선택된 일정에 따라 액션 룰을 트리거합니다. *스케줄을 생성하는 방법 페이지 51* 항목을 참조하십시오.

### 액션

몇 가지 액션을 구성할 수 있습니다.

- **Output Port(출력 포트)** - I/O 포트를 활성화하여 외부 장치를 제어합니다.
- **Send Notification(알림 전송)** - 수신자에게 알림 메시지를 전송합니다.
- **Status LED(상태 LED)** - 상태 LED를 액션 룰 기간 동안이나 설정된 시간(초) 동안 깜박이도록 설정할 수 있습니다. 설치 및 구성 중에 상태 LED를 사용하여 도어가 너무 오래 열려 있음 트리거와 같은 트리거 설정이 제대로 작동하는지 시각적으로 확인할 수 있습니다. 상태 LED가 깜박일 컬러를 설정하려면 드롭다운 목록에서 **LED Color(LED 컬러)**를 선택합니다.

## 수신자를 추가하는 방법

본 제품은 수신자에게 이벤트 및 알람에 대해 알리는 메시지를 보낼 수 있습니다. 하지만 제품에서 알림 메시지를 보내려면 먼저 한 명 이상의 수신자를 정의해야 합니다. 사용 가능한 옵션에 대한 자세한 내용은 *수신자 유형 페이지 51* 항목을 참조하십시오.

수신자를 추가하려면

1. **Setup > Additional Controller Configuration > Events > Recipients(설정 > 추가 컨트롤러 구성 > 이벤트 > 수신자)**로 이동하고 **Add(추가)**를 클릭합니다.
2. 설명이 포함된 이름을 입력합니다.

3. 수신자 **Type(유형)**을 선택합니다.
4. 수신자 유형에 필요한 정보를 입력합니다.
5. **Test(테스트)**를 클릭하여 수신자에 대한 연결을 테스트합니다.
6. **OK(확인)**를 클릭합니다.

**수신자 유형**

다음과 같은 수신자 유형을 사용할 수 있습니다.

**HTTP**

**HTTPS**

**이메일**

**TCP**

**이메일 수신자를 설정하는 방법**

나열된 이메일 공급자 중 하나를 선택하거나 회사 이메일 서버 등에 사용되는 SMTP 서버, 포트 및 인증을 지정하여 이메일 수신자를 구성할 수 있습니다.

참고

일부 이메일 공급자는 예약된 이메일과 그와 유사한 형태를 수신하면서 사용자가 큰 첨부 파일을 받거나 보는 것을 제한하기 위해 보안 필터를 사용합니다. 배달 문제 및 이메일 계정 잠김을 방지하려면 이메일 공급자의 보안 정책을 확인하십시오.

나열된 공급자 중 하나를 사용하여 이메일 수신자를 설정하려면

1. **Events > Recipients(이벤트 > 수신자)**로 이동하고 **Add(추가)**를 클릭합니다.
2. **Name(이름)**을 입력하고 **Type(유형)** 목록에서 **Email(이메일)**을 선택합니다.
3. **To(받는 사람)** 필드에 이메일을 받을 주소를 입력합니다. 쉼표를 사용하여 여러 주소를 구분하십시오.
4. **Provider(공급자)** 목록에서 이메일 공급자를 선택합니다.
5. 이메일 계정의 사용자 ID와 패스워드를 입력합니다.
6. **Test(테스트)**를 클릭하여 테스트 이메일을 보냅니다.

예를 들어 회사 이메일 서버를 사용하여 이메일 수신자를 설정하려면 위의 지침을 따르되 **User defined(사용자 정의)**를 **Provider(공급자)**로 선택합니다. **From(보낸 사람)** 필드에 보낸 사람으로 표시할 이메일 주소를 입력합니다. **Advanced settings(고급 설정)**를 선택하고 SMTP 서버 주소, 포트 및 인증 방법을 지정합니다. 선택적으로 암호화된 연결을 통해 이메일을 보내려면 **Use encryption(암호화 사용)**을 선택합니다. Axis 제품에서 사용 가능한 인증서를 사용하여 서버 인증서를 검증할 수 있습니다. 인증서를 업로드하는 방법에 대한 자세한 내용은 *인증서 페이지 55* 항목을 참조하십시오.

## 스케줄을 생성하는 방법

스케줄은 액션 룰 트리거로 사용되거나 추가 조건으로 사용될 수 있습니다. 사전 정의된 스케줄 중 하나를 사용하거나 아래에 설명된 대로 새 스케줄을 생성합니다.

새 스케줄을 생성하려면

1. **Setup > Additional Controller Configuration > Events > Schedules(설정 > 추가 컨트롤러 구성 > 이벤트 > 스케줄)**로 이동하여 **Add(추가)**를 클릭합니다.
2. 일별, 주별, 월별 또는 연간 스케줄에 필요한 정보 및 설명이 포함된 이름을 입력합니다.

3. **OK(확인)**를 클릭합니다.

액션 룰에 스케줄을 사용하려면 액션 룰 설정 페이지의 **Schedule(스케줄)** 드롭다운 목록에서 스케줄을 선택합니다.

### 반복을 설정하는 방법

반복은 액션 룰을 반복적으로(예: 5분마다 또는 매시간) 트리거하는 데 사용됩니다.

반복을 설정하려면

1. **Setup > Additonal Controller Configuration > Events > Recurrences(설정 > 추가 컨트롤러 구성 > 이벤트 > 반복)**로 이동하여 **Add(추가)**를 클릭합니다.
2. 설명이 포함된 이름과 반복 패턴을 입력합니다.
3. **OK(확인)**를 클릭합니다.

액션 룰에서 반복을 사용하려면 먼저 액션 룰 설정 페이지의 **Trigger(트리거)** 드롭다운 목록에서 **Time(시간)**을 선택하고 두 번째 드롭다운 목록에서 반복을 선택합니다.

반복을 수정하거나 제거하려면 **Recurrences List(반복 목록)**에서 **Modify(수정)** 또는 **Remove(제거)**를 클릭합니다.

## 리더 피드백

리더는 LED와 알람음을 사용하여 사용자(도어에 접근하고 있거나 접근을 시도하는 사람)에게 피드백 메시지를 보냅니다. 도어 컨트롤러는 수많은 피드백 메시지를 트리거할 수 있으며 그 중 일부는 도어 컨트롤러에 사정 구성되어 대부분의 리더에서 지원됩니다.

리더의 LED 동작은 다양하지만, 일반적으로 빨간색/녹색/주황색의 계속 표시됨/깜박거림의 다양한 시퀀스로 구성됩니다.

또한 리더는 한 가지 톤의 짧고 긴 알람음 신호의 다양한 시퀀스를 사용하여 메시지를 보냅니다.

아래 표에는 리더 피드백을 트리거하기 위해 도어 컨트롤러에 사전 구성되어 있는 이벤트와 해당하는 리더 피드백 신호가 나와 있습니다. AXIS 리더의 피드백 신호는 AXIS 리더와 함께 제공된 설치 가이드에 나와 있습니다.

| 이벤트 | Wiegand 이중 LED | Wiegand 단일 LED | OSDP | 알람음 패턴 | 상태 |
|---|---|---|---|---|---|
| Idle[1] | 꺼짐 | 빨간색 | 빨간색 | 무음 | 정상 |
| RequirePIN | 빨간색/녹색 깜박임 | 빨간색/녹색 깜박임 | 빨간색/녹색 깜박임 | 두 번의 짧은 알람음 | PIN 필요 |
| AccessGranted | 녹색 | 녹색 | 녹색 | 알람음 | 접근 권한 부여됨 |
| AccessDenied | 빨간색 | 빨간색 | 빨간색 | 알람음 | 접근 권한 거부됨 |

1. 도어가 닫히고 잠금이 잠기면 유휴 상태로 들어갑니다.

위에 나온 피드백 메시지 외의 피드백 메시지는 이 기능을 지원하고 필요한 신호를 제공할 수 있는 리더를 사용하는 VAPIX® 애플리케이션 프로그래밍 인터페이스를 통해 접근 관리 시스템 같은 클라이언트에서 구성해야 합니다. 자세한 내용은 접근 관리 시스템 개발자 및 리더 제조업체가 제공한 사용자 정보를 참조하십시오.

# 보고서

## 보고서

보고서 페이지에서 시스템에 대한 여러 유형의 정보가 포함된 보고서를 보고 인쇄하고 내보낼 수 있습니다. 사용할 수 있는 보고서에 대한 자세한 내용은 *보고서 유형 페이지 53* 항목을 참조하십시오.

### 보고서 보기, 인쇄 및 내보내기

보고서 페이지를 열려면 **Reports(보고서)**를 클릭합니다.

보고서를 보려면 **View and print(보기 및 인쇄)**를 클릭합니다.

보고서를 인쇄하려면

1. **View and print(보기 및 인쇄)**를 클릭합니다.
2. 보고서에 포함할 열을 선택합니다. 기본적으로 모든 열이 선택됩니다.
3. 보고서의 범위를 좁히려면 관련 필터 필드에 필터를 입력합니다. 예를 들어 속한 그룹으로 사용자를 필터링하거나 일정에 따라 도어를 필터링하거나 접근할 수 있는 도어에 따라 그룹을 필터링할 수 있습니다.

   정확하게 일치하는 항목을 찾으려면 큰따옴표로 필터 텍스트를 묶으십시오(예: "John").
4. 보고서 항목을 다른 순서로 정렬하려면 해당 열에서 을 클릭합니다. 표준 순서와 역순 중에서 변경하려면 정렬 버튼을 토글합니다.

   ▲ 표준 순서(오름차순)로 항목을 표시합니다.

   ▼ 역순(내림차순)으로 항목을 표시합니다.
5. **Print selected columns(선택한 열 인쇄)**를 클릭합니다.

보고서를 내보내려면 **Export CSV file(CSV 파일 내보내기)**을 클릭합니다.

보고서는 쉼표로 구분된 값(CSV) 파일로 내보내지고 보고서 유형에 사용할 수 있는 모든 열과 항목을 포함합니다. 별도로 지정하지 않는 한 내보낸 파일(*.csv)이 기본 다운로드 폴더에 저장됩니다. 웹 브라우저 사용자 설정에서 다운로드 폴더를 선택할 수 있습니다.

참고

자격 증명을 가진 사용자만 보고서에 표시됩니다.

#### 보고서 유형

다음과 같은 보고서 유형을 사용할 수 있습니다.

- 접근 일정. 접근 일정 유형 및 옵션에 대한 자세한 내용은 *페이지 33* 및 *페이지 34* 항목을 참조하십시오.
- 그룹. 그룹 자격 증명에 대한 자세한 내용은 *페이지 35* 항목을 참조하십시오.
- 도어. 도어 및 식별 유형에 대한 자세한 내용은 *페이지 35* 및 *페이지 36* 항목을 참조하십시오.
- 사용자. 사용자에 대한 자세한 내용은 *페이지 41* 항목을 참조하십시오.
- 도어 컨트롤러. 연결된 컨트롤러 및 해당 ID 유형에 대한 자세한 내용은 *페이지 28* 항목을 참조하십시오. 도어 모니터 시간 및 옵션에 대한 자세한 내용은 *페이지 17* 항목을 참조하십시오.

## 시스템 옵션

# 보안

### 사용자

사용자 액세스 제어는 기본적으로 활성화되며 **Setup > Additional Controller Configuration > System Options > Security > Users(설정 > 추가 컨트롤러 구성 > 시스템 옵션 > 보안 > 사용자)**에서 구성할 수 있습니다. 관리자는 사용자 이름과 패스워드를 제공하여 다른 사용자를 설정할 수 있습니다.

사용자 목록에는 권한이 있는 사용자 및 사용자 그룹(접근 레벨)이 표시됩니다.

- **Administrators(관리자)**는 모든 설정에 무제한 액세스할 수 있습니다. 관리자는 다른 사용자를 추가, 수정 및 제거할 수 있습니다.

참고

**Encrypted & unencrypted(암호화 및 암호화되지 않은 경우)**를 선택하면 웹 서버가 패스워드를 암호화합니다. 새 장치 또는 공장 출하 시 기본 설정으로 재설정된 장치의 경우 이것이 기본 옵션입니다.

**HTTP/RTSP Password Settings(HTTP/RTSP 패스워드 설정)**에서 허용할 패스워드 유형을 선택합니다. 암호화를 지원하지 않는 보기 클라이언트가 있거나 펌웨어를 업그레이드하여 기존 클라이언트가 암호화를 지원하지만 이 기능을 사용하려면 다시 로그인하여 기능을 구성해야 하는 경우 암호화되지 않은 패스워드를 허용해야 합니다.

### ONVIF

ONVIF는 IP 기반 물리적 보안 제품의 효과적인 상호운용성을 위해 표준화된 인터페이스를 제공하고 촉진하는 개방형 업계 포럼입니다.

사용자를 생성하면 ONVIF 통신이 자동으로 활성화됩니다. 제품과의 모든 ONVIF 통신에는 사용자 이름과 패스워드를 사용합니다. 자세한 내용은 *www.onvif.org*를 참조하십시오.

### IP 주소 필터

IP 주소 필터링은 **Setup > Additional Controller Configuration > System Options > Security > IP Address Filter(설정 > 추가 컨트롤러 구성 > 시스템 옵션 > 보안 > IP 주소 필터)** 페이지에서 활성화합니다. 활성화되면 나열된 IP 주소의 Axis 제품에 대한 액세스가 허용되거나 거부됩니다. IP 주소 필터링을 활성화하려면 목록에서 **Allow(허용)** 또는 **Deny(거부)**를 선택하고 **Apply(적용)**를 클릭합니다.

관리자는 최대 256개의 IP 주소 항목을 목록에 추가할 수 있습니다. 단일 항목이 여러 IP 주소를 포함할 수 있습니다.

### HTTPS

HTTPS(HyperText Transfer Protocol over Secure Socket Layer 또는 HTTP over SSL)는 암호화된 브라우징을 제공하는 웹 프로토콜입니다. 사용자와 클라이언트가 HTTPS를 사용하여 올바른 장치에 액세스하고 있는지 확인할 수도 있습니다. HTTPS에서 제공하는 보안 수준은 대부분의 상거래에 적합하다고 간주됩니다.

관리자가 로그인할 때 HTTPS를 요구하도록 Axis 제품을 구성할 수 있습니다.

HTTPS를 사용하려면 먼저 HTTPS 인증서를 설치해야 합니다. 인증서를 설치하고 관리하려면 **Setup > Additional Controller Configuration > System Options >; Security > Certificates(설정 > 추가 컨트롤러 구성 > 시스템 옵션 > 보안 > 인증서)**로 이동합니다. *인증서 페이지 55* 항목을 참조하십시오.

Axis 제품에서 HTTPS를 활성화하려면

1. **Setup > Additional Controller Configuration > System Options > Security > HTTPS(설정 > 추가 컨트롤러 구성 > 시스템 옵션 > 보안 > HTTPS)**로 이동합니다.
2. 설치된 인증서 목록에서 HTTPS 인증서를 선택합니다.

3. **Ciphers(암호)**를 클릭하고 SSL에 사용할 암호화 알고리즘을 선택합니다(선택 사항).
4. 여러 사용자 그룹의 **HTTPS Connection Policy(HTTPS 연결 정책)**를 설정합니다.
5. 설정을 활성화하려면 **Save(저장)**를 클릭합니다.

원하는 프로토콜을 통해 Axis 제품에 액세스하려면 HTTPS 프로토콜로 `https://`를 입력하고 HTTP 프로토콜로 `http://`를 입력합니다.

**System Options > Network > TCP/IP > Advanced(시스템 옵션 > 네트워크 > TCP/IP > 고급)** 페이지에서 HTTPS 포트를 변경할 수 있습니다.

### IEEE 802.1X

IEEE 802.1X는 유선 및 무선 네트워크 장치의 보안 인증을 제공하는 포트 기반 NAC(Network Admission Control)를 위한 표준입니다. IEEE 802.1X는 EAP(Extensible Authentication Protocol)를 기준으로 합니다.

IEEE 802.1X로 보호되는 네트워크에 액세스하려면 장치가 인증되어야 합니다. 대개 **RADIUS 서버**인 인증 서버에서 인증을 수행하며 FreeRADIUS 및 Microsoft 인터넷 인증 서비스 등이 있습니다.

Axis 구현 시 Axis 제품 및 인증 서버는 EAP-TLS(확장 가능 인증 프로토콜 - 전송 계층 보안)를 사용하여 디지털 인증서로 자체적으로 식별합니다. **CA**(Certification Authority)에서 인증서를 제공합니다. 다음 항목이 필요합니다.

- 인증 서버를 인증할 CA 인증서
- Axis 제품을 인증할 CA 서명 클라이언트 인증서

인증서를 만들고 설치하려면 **Setup > Additional Controller Configuration > System Options > Security > Certificates(설정 > 추가 컨트롤러 구성 > 시스템 옵션 > 보안 > 인증서)**로 이동합니다. *인증서 페이지 55* 항목을 참조하십시오.

IEEE 802.1X로 보호되는 네트워크에 제품이 액세스하도록 허용하려면

1. **Setup > Additional Controller Configuration > System Options > Security > IEEE 802.1X(설정 > 추가 컨트롤러 구성 > 시스템 옵션 > 보안 > IEEE 802.1X)**로 이동합니다.
2. 설치된 인증서 목록에서 **CA Certificate(CA 인증서)** 및 **Client Certificate(클라이언트 인증서)**를 선택합니다.
3. **Settings(설정)**에서 EAPOL 버전을 선택하고 클라이언트 인증서와 연결된 EAP ID를 제공합니다.
4. IEEE 802.1X 활성화 확인란을 선택하고 **Save(저장)**를 클릭합니다.

참고

인증이 제대로 작동하려면 Axis 제품의 날짜 및 시간이 NTP 서버와 동기화되어야 합니다. *날짜 및 시간 페이지 56* 항목을 참조하십시오.

### 인증서

인증서는 네트워크에서 장치를 인증하는 데 사용됩니다. 일반 애플리케이션에는 암호화된 웹 검색(HTTPS), IEEE 802.1X를 통한 네트워크 보호, 이메일 등을 통한 알림 메시지가 포함됩니다. Axis 제품에는 두 가지 유형의 인증서를 사용할 수 있습니다.

**서버/클라이언트 인증서 -** Axis 제품을 인증하려면 **Server/Client(서버/클라이언트)** 인증서는 CA(Certificate Authority)에서 자체 서명하거나 발행할 수 있습니다. 자체 서명 인증서는 제한된 보호를 제공하며 CA 발행 인증서를 얻기 전까지 사용할 수 있습니다.

**CA 인증서 -** Axis 제품이 IEEE 802.1X 보호 네트워크에 연결된 경우 인증 서버의 인증서와 같은 피어 인증서를 인증합니다. Axis 제품은 여러 CA 인증서가 사전 설치되어 배송됩니다.

참고

- 제품을 공장 출하 시 기본값으로 재설정하면 사전 설치된 CA 인증서를 제외한 모든 인증서가 삭제됩니다.
- 제품을 공장 출하 시 기본값으로 재설정하면 삭제되었던 모든 사전 설치된 CA 인증서가 다시 설치됩니다.

**자체 서명된 인증서를 만드는 방법**

1. **Setup > Additional Controller Configuration > System Options > Security > Certificates(설정 > 추가 컨트롤러 구성 > 시스템 옵션 > 보안 > 인증서)**로 이동합니다.
2. **Create self-signed certificate(자체 서명된 인증서 만들기)**를 클릭하고 필수 정보를 제공합니다.

**CA 서명 인증서를 생성하고 설치하는 방법**

1. 자체 서명 인증서를 생성합니다. 항목을 참조하십시오.
2. **Setup > Additional Controller Configuration > System Options > Security > Certificates(설정 > 추가 컨트롤러 구성 > 시스템 옵션 > 보안 > 인증서)**로 이동합니다.
3. **Create certificate signing request(인증서 서명 요청 만들기)**를 클릭하고 요청된 정보를 제공합니다.
4. PEM 형식의 요청을 복사하고 원하는 CA로 보냅니다.
5. 서명된 인증서가 반환되면 **Install certificate(인증서 설치)**를 클릭하고 인증서를 업로드합니다.

**추가 CA 인증서를 설치하는 방법**

1. **Setup > Additional Controller Configuration > System Options > Security > Certificates(설정 > 추가 컨트롤러 구성 > 시스템 옵션 > 보안 > 인증서)**로 이동합니다.
2. **Install certificate(인증서 설치)**를 클릭하고 인증서를 업로드합니다.

## 날짜 및 시간

Axis 제품의 날짜 및 시간 설정은 **Setup > Additional Controller Configuration > System Options > Date & Time(설정 > 추가 컨트롤러 구성 > 시스템 옵션 > 날짜 및 시간)**에서 구성합니다.

**Current Server Time(현재 서버 시간)**은 현재 날짜와 시간(24시간제)을 표시합니다.

날짜 및 시간 설정을 변경하려면 **New Server Time(새 서버 시간)**에서 원하는 **Time mode(시간 모드)**를 선택합니다.

- **Synchronize with computer time(컴퓨터 시간과 동기화)** - 컴퓨터의 시계에 따라 날짜와 시간을 설정합니다. 이 옵션을 사용하면 날짜와 시간이 한 번만 설정되며 자동으로 업데이트되지 않습니다.
- **Synchronize with NTP Server(NTP 서버와 동기화)** - NTP 서버에서 날짜와 시간을 가져옵니다. 이 옵션을 사용하면 날짜 및 시간 설정이 지속적으로 업데이트됩니다. NTP 설정에 대한 자세한 내용은 *NTP 구성 페이지 59* 항목을 참조하십시오.

  NTP 서버에 대해 호스트 이름을 사용할 경우 DNS 서버를 구성해야 합니다. *DNS 구성 페이지 58* 항목을 참조하십시오.
- **Set manually(수동 설정)** - 날짜와 시간을 수동으로 설정할 수 있습니다.

NTP 서버를 사용할 경우 드롭다운 목록에서 **Time zone(시간대)**을 선택합니다. 필요한 경우 **Automatically adjust for daylight saving time changes(일광 절약 시간 변경에 맞게 자동으로 조정)**를 선택합니다.

## 네트워크

### 기본 TCP/IP 설정

Axis 제품은 IP 버전 4(IPv4)를 지원합니다.

Axis 제품은 다음과 같은 방법으로 IPv4 주소를 가져올 수 있습니다.

- **Dynamic IP address(동적 IP 주소)** - **Obtain IP address via DHCP(DHCP를 통해 IP 주소 가져오기)**가 기본적으로 선택됩니다. 즉, Axis 제품이 DHCP(Dynamic Host Configuration Protocol)를 통해 IP 주소를 자동으로 가져오도록 설정됩니다.

  DHCP를 사용하면 네트워크 관리자가 IP 주소 할당을 중앙에서 관리하고 자동화할 수 있습니다.

- **Static IP address(고정 IP 주소)** - 고정 IP 주소를 사용하려면 **Use the following IP address(다음 IP 주소 사용)**을 선택하고 IP 주소, 서브넷 마스크 및 기본 라우터를 지정합니다. 그런 다음 **Save(저장)**를 클릭합니다.

동적 IP 주소 알림을 사용하거나, DHCP가 이름(호스트 이름)으로 Axis 제품에 액세스할 수 있도록 해주는 DNS 서버를 업데이트할 수 있는 경우에만 DHCP를 활성화해야 합니다.

DHCP가 활성화되고 제품에 액세스할 수 없는 경우 AXIS IP Utility를 실행하여 연결된Axis 제품의 네트워크를 검색하거나 제품을 공장 출하 시 기본 설정으로 재설정한 후 다시 설치하십시오. 공장 출하 시 기본값으로 재설정하는 방법에 대한 자세한 내용은 *페이지 64* 항목을 참조하십시오.

### ARP/Ping

ARP 및 Ping을 사용하여 제품의 IP 주소를 할당할 수 있습니다. 자세한 내용은 *ARP/Ping을 사용하여 IP 주소 할당 페이지 57* 항목을 참조하십시오.

ARP/Ping 서비스는 기본적으로 활성화되지만 제품이 시작되고 2분이 지나고 또는 IP 주소가 할당되자 마자 자동으로 비활성화됩니다. ARP/Ping을 사용하여 IP 주소를 다시 할당하려면 다시 2분간 ARP/Ping이 활성하되도록 제품을 다시 시작해야 합니다.

서비스를 비활성화하려면 **Setup > Additional Controller Configuration > System Options > Network > TCP/IP > Basic(설정 > 추가 컨트롤러 구성 > 시스템 옵션 > 네트워크 > TCP/IP > 기본)**으로 이동하여 **Enable ARP/Ping setting of IP address(IP 주소의 ARP/Ping 설정 활성화)** 옵션 선택을 취소하십시오.

서비스가 비활성화되어 있어도 제품을 계속 ping할 수 있습니다.

### ARP/Ping을 사용하여 IP 주소 할당

ARP/Ping을 사용하여 장치의 IP 주소를 할당할 수 있습니다. 전원을 연결하고 2분 내에 명령을 실행해야 합니다.

1. 컴퓨터와 동일한 네트워크 세그먼트에서 사용되지 않는 고정 IP 주소를 구합니다.
2. 장치 라벨에서 일련 번호(S/N)를 찾습니다.
3. 명령 프롬프트를 열고 다음 명령을 입력합니다.

   **Linux/Unix 구문**

   ```
   arp -s <IP address> <serial number> temp
   ping -s 408 <IP address>
   ```

   **Linux/Unix 예**

   ```
   arp -s 192.168.0.125 00:40:8c:18:10:00 temp
   ping -s 408 192.168.0.125
   ```

   **Windows 구문**(이 구문에서는 관리자로 명령 프롬프트를 실행해야 할 수도 있음)

   ```
   arp -s <IP address> <serial number>
   ping -l 408 -t <IP address>
   ```

   **Windows 예**(이 구문에서는 관리자로 명령 프롬프트를 실행해야 할 수도 있음)

   ```
   arp -s 192.168.0.125 00-40-8c-18-10-00
   ping -l 408 -t 192.168.0.125
   ```

4. 네트워크 커넥터를 분리했다 다시 연결하여 장치를 재시작합니다.
5. 장치에 `Reply from 192.168.0.125:...` 또는 이와 유사한 응답이 나타나면 명령 프롬프트를 닫습니다.

6. 브라우저를 열고 주소 필드에 `http://<IP address>`를 입력합니다.

IP 주소를 할당하는 다른 방법은 *www.axis.com/support*의 *IP 주소를 할당하고 장치에 액세스하는 방법* 문서를 참조하십시오.

참고

- Windows에서 명령 프롬프트를 열려면 **Start(시작)** 메뉴를 열고 `cmd`를 검색하십시오.
- Windows 8/Windows 7/Windows Vista에서 ARP 명령을 사용하려면 명령 프롬프트 아이콘을 마우스 오른쪽 버튼으로 클릭한 다음 **Run as administrator(관리자로 실행)**를 선택하십시오.
- Mac OS X에서 명령 프롬프트를 열려면 **Application > Utilities(애플리케이션 > 유틸리티)**에서 **Terminal utility(터미널 유틸리티)**를 엽니다.

#### AVHS(AXIS Video Hosting System)

AVHS 서비스와 함께 AVHS를 사용하면 어느 곳에서든 컨트롤러 관리 및 로그에 쉽고 안전하게 액세스할 수 있습니다. 로컬 AVHS 서비스 공급자를 찾기 위한 자세한 내용은 www.axis.com/hosting을 참조하십시오.

**Setup > Additional Controller Configuration > System Options > Network > TCP IP > Basic(설정 > 추가 컨트롤러 구성 > 시스템 옵션 > 네트워크 > TCP IP > 기본)**에서 AVHS 설정을 구성합니다. 기본적으로 AVHS 연결할 수 있습니다. 연결을 비활성화하려면 **Enable AVHS(AVHS 활성화)** 상자의 선택을 취소하십시오.

**One-click enabled(원클릭 활성화)** - 제품의 제어 버튼을 3초 정도 눌러(*제품 개요 페이지 4* 참조) 인터넷으로 AVHS 서비스에 연결합니다. 등록되면 **Always(항상)**가 활성화되고 Axis 제품이 계속 AVHS 서비스와 연결되어 있습니다. 버튼을 눌렀을 때 24시간 안에 제품이 등록되지 않으면 제품과 AVHS 서비스의 연결이 끊어집니다.

**Always(항상)** - Axis 제품이 인터넷을 통해 AVHS 서비스에 대한 연결을 지속적으로 시도합니다. 등록되면 제품이 AVHS 서비스에 계속 연결되어 있습니다. 제품이 이미 설치되어 있고 원클릭 설치를 사용하기가 불편하거나 불가능할 때 이 옵션을 사용할 수 있습니다.

참고

서비스 공급자의 구독 여부에 따라 AVHS 지원이 결정됩니다.

#### AXIS Internet Dynamic DNS 서비스

AXIS Internet Dynamic DNS 서비스는 제품에 쉽게 액세스할 수 있도록 호스트 이름을 할당합니다. 자세한 내용은 *www.axiscam.net*을 참조하십시오.

AXIS Internet Dynamic DNS 서비스에 Axis 제품을 등록하려면 **Setup > Additional Controller Configuration > System Options > Network > TCP/IP > Basic(설정 > 추가 컨트롤러 구성 > 시스템 옵션 > 네트워크 > TCP/IP > 기본)**으로 이동합니다. **Services(서비스)**에서 AXIS Internet Dynamic DNS 서비스 **Settings(설정)** 버튼을 클릭합니다(인터넷에 액세스해야 함). AXIS Internet Dynamic DNS 서비스에 현재 등록된 도메인 이름을 언제든지 제거할 수 있습니다.

참고

AXIS Internet Dynamic DNS 서비스를 이용하려면 IPv4가 필요합니다.

### 고급 TCP/IP 설정

#### DNS 구성

DNS(Domain Name Service)는 호스트 이름을 IP 주소로 변환합니다. DNS 설정은 **Setup > Additional Controller Configuration > System Options > Network > TCP/IP > Advanced(설정 > 추가 컨트롤러 구성 > 시스템 옵션 > 네트워크 > TCP/IP > 고급)**에서 구성됩니다.

DHCP 서버에서 제공하는 DNS 설정을 사용하려면 **Obtain DNS server address via DHCP(DHCP를 통해 DNS 서버 주소 가져오기)**를 선택하십시오.

수동으로 설정하려면 **Use the following DNS server address(다음 DNS 서버 주소 사용)**를 선택하고 다음을 지정합니다.

## 시스템 옵션

**도메인 이름 -** 도메인을 입력하여 Axis 제품에 사용되는 호스트 이름을 검색합니다. 도메인이 여러 개일 경우 세미콜론으로 구분할 수 있습니다. 호스트 이름은 항상 정규화된 도메인 이름의 첫 번째 부분입니다. 예를 들어 `myserver`는 정규화된 도메인 이름 `myserver.mycompany.com`의 호스트 이름입니다. 여기서 `mycompany.com`은 도메인 이름입니다.

**기본/보조 DNS 서버 -** 기본 및 보조 DNS 서버의 IP 주소를 입력하십시오. 보조 DNS 서버는 선택 사항이며 기본 DNS를 사용할 수 없는 경우 사용됩니다.

#### NTP 구성

NTP(Network Time Protocol)는 네트워크에 있는 장치의 시계 시간을 동기화하는 데 사용됩니다. NTP 설정은 **Setup > Additional Controller Configuration > System Options > Network > TCP/IP > Advanced(설정 > 추가 컨트롤러 구성 > 시스템 옵션 > 네트워크 > TCP/IP > 고급)**에서 구성됩니다.

DHCP 서버에서 제공하는 NTP 설정을 사용하려면 **Obtain NTP server address via DHCP(DHCP를 통해 NTP 서버 주소 가져오기)**를 선택하십시오.

수동으로 설정하려면 **Use the following NTP server address(다음 NTP 서버 주소 사용)**를 선택하고 NTP 서버의 호스트 이름 또는 IP 주소를 입력하십시오.

#### 호스트 이름 구성

IP 주소 대신 호스트 이름을 사용하여 Axis 제품에 액세스할 수 있습니다. 호스트 이름은 보통 DNS 이름과 같습니다. 호스트 이름은 **Setup > Additional Controller Configuration > System Options > Network > TCP/IP > Advanced(설정 > 추가 컨트롤러 구성 > 시스템 옵션 > 네트워크 > TCP/IP > 고급)**에서 구성됩니다.

IPv4에서 실행 중인 DHCP 서버에서 제공하는 호스트 이름을 사용하려면 **Obtain host name via IPv4 DHCP(IPv4 DHCP를 통해 호스트 이름 가져오기)**를 선택합니다.

호스트 이름을 수동으로 설정하려면 **Use the host name(호스트 이름 사용)**을 선택합니다.

Axis 제품의 IP 주소가 변경될 때마다 로컬 DNS 서버를 동적으로 업데이트하려면 **Enable dynamic DNS updates(동적 DNS 업데이트 활성화)**를 선택합니다. 자세한 내용은 온라인 도움말을 참조하십시오.

#### 링크 로컬 IPv4 주소

**Link-Local Address(링크 로컬 주소)**는 기본적으로 활성화되며 로컬 네트워크의 동일한 세그먼트에 있는 다른 호스트에서 제품에 액세스하기 위해 사용할 수 있는 추가 IP 주소를 Axis 제품에 할당합니다. 본 제품은 로컬 링크 IP 주소와 고정 또는 DHCP 제공 IP 주소를 동시에 가질 수 있습니다.

**Setup > Additional Controller Configuration > System Options > Network > TCP/IP > Advanced(설정 > 추가 컨트롤러 구성 > 시스템 옵션 > 네트워크 > TCP/IP > 고급)**에서 이 기능을 비활성화할 수 있습니다.

#### HTTP

**Setup > Additional Controller Configuration > System Options > Network > TCP/IP > Advanced(설정 > 추가 컨트롤러 구성 > 시스템 옵션 > 네트워크 > TCP/IP > 고급)**에서 Axis 제품에 사용되는 HTTP 포트를 변경할 수 있습니다. 기본 설정인 80 외에 1024 ~ 65535 범위의 어느 포트라도 사용할 수 있습니다.

#### HTTPS

Axis 제품에서 사용하는 HTTP 포트는 **Setup > Additional Controller Configuration > System Options > Network > TCP/IP > Advanced(설정 > 추가 컨트롤러 구성 > 시스템 옵션 > 네트워크 > TCP/IP > 고급)**에서 변경할 수 있습니다. 기본 설정인 443 외에 1024 ~ 65535 범위의 어느 포트라도 사용할 수 있습니다.

HTTPS를 활성화하려면 **Setup > Additional Controller Configuration > System Options > Security > HTTPS(설정 > 추가 컨트롤러 구성 > 시스템 옵션 > 보안 > HTTPS)**로 이동합니다. 자세한 내용은 *HTTPS 페이지 54* 항목을 참조하십시오.

**IPv4에 대한 NAT 통과(포트 매핑)**

네트워크 라우터를 사용하면 사설 네트워크(LAN)의 장치가 인터넷에 대한 단일 연결을 공유할 수 있습니다. 이렇게 하려면 사설 네트워크에서 "외부", 즉 인터넷으로 네트워크 트래픽을 전달하면 됩니다. 대부분의 라우터는 공용 네트워크(인터넷)에서 사설 네트워크(LAN)에 액세스하려는 시도를 중지하도록 사전 구성되어 있으므로 사설 네트워크(LAN)의 보안이 증대됩니다.

Axis 제품이 인트라넷(LAN)에 있을 때 NAT 라우트 다른 쪽(WAN)에서 이 제품을 사용할 수 있게 하려면 **NAT 통과**를 사용하십시오. NAT 통과가 적절하게 구성되면 NAT 라우터의 외부 HTTP 포트에 대한 모든 HTTP 트래픽이 제품에 전달됩니다.

NAT 통과는 **Setup > Additional Controller Configuration > System Options > Network > TCP/IP > Advanced(설정 > 추가 컨트롤러 구성 > 시스템 옵션 > 네트워크 > TCP/IP > 고급)**에서 구성됩니다.

참고

- NAT 통과가 작동하려면 라우터에서 이 기능을 지원해야 합니다. 또한 라우터가 UPnP®를 지원해야 합니다.
- 여기서 라우터는 NAT 라우터, 네트워크 라우터, 인터넷 게이트웨이, 브로드밴드 라우터, 브로드밴드 공유 장치와 같은 네트워크 라우팅 장치 또는 방화벽과 같은 소프트웨어를 나타냅니다.

**활성화/비활성화** - 활성화할 경우 Axis 제품은 UPnP를 사용하여 네트워크의 NAT 라우터에서 포트 매핑을 구성하려고 시도합니다. 제품에 UPnP가 활성화되어 있어야 합니다(**Setup > Additional Controller Configuration > System Options > Network > UPnP(설정 > 고급 컨트롤러 구성 > 시스템 옵션 > 네트워크 > UPnP)** 참조).

**수동으로 선택한 NAT 라우터 사용** - NAT 라우터를 수동으로 선택하려면 이 옵션을 선택하고 필드에 라우터의 IP 주소를 입력하십시오. 라우터를 지정하지 않으면 제품이 자동으로 네트워크에서 NAT 라우터를 검색합니다. 라우터가 하나 이상 발견되면 기본 라우터가 선택됩니다.

**대체 HTTP 포트** - 외부 HTTP 포트를 수동으로 정의하려면 이 옵션을 선택하십시오. 1024 ~ 65535 범위의 포트를 입력합니다. 포트 필드가 비어 있거나 기본 설정(0)이 있으면 NAT 통과를 활성화할 경우 포트 번호가 자동으로 선택됩니다.

참고

- NAT 통과가 비활성화되어 있어도 대체 HTTP 포트를 사용하거나 활성화할 수 있습니다. NAT 라우터가 UPnP를 지원하지 않고 NAT 라우터에서 포트 포워딩을 수동으로 구성해야 할 경우 이 기능이 유용합니다.
- 이미 사용 중인 포트를 수동으로 입력하려고 하면 사용 가능한 다른 포트가 자동으로 선택됩니다.
- 포트가 자동으로 선택되면 이 필드에 표시됩니다. 이 설정을 변경하려면 새 포트 번호를 입력하고 **Save(저장)**를 클릭합니다.

**FTP**

Axis 제품에서 실행되는 FTP 서버는 새 펌웨어, 사용자 애플리케이션 등을 업로드할 수 있도록 합니다. **Setup > Additional Controller Configuration > System Options > Network > TCP/IP > Advanced(설정 > 추가 컨트롤러 구성 > 시스템 옵션 > 네트워크 > TCP/IP > 고급)**에서 FTP 서버를 비활성화할 수 있습니다.

**RTSP**

Axis 제품에서 실행되는 RTSP 서버는 연결 클라이언트가 이벤트 스트림을 시작할 수 있게 허용합니다. **Setup > Additional Controller Configuration > System Options > Network > TCP/IP > Advanced(설정 > 추가 컨트롤러 구성 > 시스템 옵션 > 네트워크 > TCP/IP > 고급)**에서 RTSP 포트 번호를 변경할 수 있습니다. 기본 포트는 554입니다.

참고

RTSP 서버가 비활성화되면 이벤트 스트림을 사용할 수 없습니다.

## SOCKS

SOCKS는 네트워킹 프록시 프로토콜입니다. SOCKS 서버를 사용하여 방화벽이나 프록시 서버 반대편에 있는 네트워크에 도달하도록 Axis 제품을 구성할 수 있습니다. Axis 제품이 방화벽 뒤 로컬 네트워크에 있고 알림, 업로드, 알람 등을 로컬 네트워크 밖에 있는 대상(예: 인터넷)으로 전송해야 할 경우 이 기능이 유용합니다.

**Setup > Additional Controller Configuration > System Options > Network > SOCKS(설정 > 추가 컨트롤러 구성 > 시스템 옵션 > 네트워크 > SOCKS)**에서 SOCKS를 구성합니다. 자세한 내용은 온라인 도움말을 참조하십시오.

### QoS(Quality of Service)

QoS(Quality of Service)는 네트워크의 선택된 트래픽에 일정 수준의 지정된 리소스를 보장합니다. QoS 인식 네트워크는 네트워크 트래픽의 우선 순위를 정하고, 애플리케이션에 사용되는 대역폭의 양을 제어하여 네트워크 신뢰성을 강화합니다.

**Setup > Additional Controller Configuration > System Options > Network > QoS(설정 > 추가 컨트롤러 구성 > 시스템 옵션 > 네트워크 > QoS)**에서 QoS 설정을 구성합니다. Axis 제품은 DSCP(Differentiated Services Codepoint) 값을 사용하여 이벤트/알람 트래픽과 관리 트래픽을 표시할 수 있습니다.

### SNMP

SNMP(Simple Network Management Protocol)를 이용하여 네트워크 장치를 원격으로 관리할 수 있습니다. SNMP 커뮤니티는 장치 그룹이며 SNMP를 실행하는 관리 스테이션입니다. 커뮤니티 이름은 그룹을 식별하는 데 사용됩니다.

Axis 제품에서 SNMP를 활성화하고 구성하려면 **Setup > Additional Controller Configuration > System Options > Network > SNMP(설정 > 추가 컨트롤러 구성 > 시스템 옵션 > 네트워크 > SNMP)** 페이지로 이동하십시오.

필요한 보안 수준에 따라 사용할 SNMP의 버전을 선택하십시오.

중요한 이벤트 및 상태 변화에 대해 관리 시스템에 메시지를 전송하기 위해 Axis 제품에 트랩이 사용됩니다. **Enable traps(트랩 활성화)**를 선택하고 트랩 메시지를 보낼 IP 주소와 메시지를 수신할 **Trap community(트랩 커뮤니티)**를 입력하십시오.

참고

HTTPS가 활성화되면 SNMP v1과 SNMP v2c를 비활성화해야 합니다.

중요한 이벤트 및 상태 변화에 대해 관리 시스템에 메시지를 전송하기 위해 Axis 제품에 **Traps for SNMP v1/v2(SNMP v1/v2용 트랩)**가 사용됩니다. **Enable traps(트랩 활성화)**를 선택하고 트랩 메시지를 보낼 IP 주소와 메시지를 수신할 **Trap community(트랩 커뮤니티)**를 입력하십시오.

다음과 같은 트랩을 사용할 수 있습니다.

- 콜드 부팅
- 웜 부팅
- 링크 업
- 인증 실패

**SNMP v3**는 암호화 및 보안 패스워드를 제공합니다. SNMP v3와 함께 트랩을 사용하려면 SNMP v3 관리 애플리케이션이 필요합니다.

SNMP v3를 사용하려면 HTTPS가 활성화되어야 합니다. *HTTPS 페이지 54* 항목을 참조하십시오. SNMP v3를 활성화하려면 상자를 선택하고 초기 사용자 패스워드를 제공하십시오.

참고

초기 패스워드는 한 번만 설정할 수 있습니다. 패스워드를 분실한 경우 Axis 제품을 공장 출하 시 기본값으로 재설정해야 합니다. *공장 출하 시 기본 설정으로 재설정 페이지 64* 항목을 참조하십시오.

### UPnP

Axis 제품에는 UPnP®에 대한 지원이 포함되어 있습니다. UPnP는 기본적으로 활성화되며 이 프로토콜을 지원하는 운영 체제와 클라이언트에서 제품을 자동으로 감지합니다.

**Setup > Additional Controller Configuration > System Options > Network > UPnP(설정 > 추가 컨트롤러 구성 > 시스템 옵션 > 네트워크 > UPnP)**에서 UPnP를 비활성화할 수 있습니다.

### Bonjour

Axis 제품에는 Bonjour에 대한 지원이 포함되어 있습니다. Bonjour는 기본적으로 활성화되며 이 프로토콜을 지원하는 운영 체제와 클라이언트에서 제품을 자동으로 감지합니다.

**Setup > Additional Controller Configuration > System Options > Network > Bonjour(설정 > 추가 컨트롤러 구성 > 시스템 옵션 > 네트워크 > Bonjour)**에서 Bonjour를 비활성화할 수 있습니다.

## 포트 및 장치

### I/O 포트

Axis 제품의 보조 커넥터는 외부 장치 연결을 위한 2개의 구성 가능한 입력 및 출력 포트를 제공합니다. 외부 장치를 연결하는 방법에 대한 자세한 내용은 *www.axis.com*을 참조하십시오.

I/O 포트는 **Setup > Additional Controller Configuration > System Options > Ports & Devices > I/O Ports(설정 > 추가 컨트롤러 구성 > 시스템 옵션 > 포트 및 장치 > I/O 포트)**에서 구성합니다. 포트 방향(**Input(입력)** 또는 **Output(출력)**)을 선택합니다. 포트에 설명이 포함된 이름을 지정하고 **Normal states(정상 상태)**를 **Open circuit(개방 회로)** 또는 **Grounded circuit(접지 회로)**으로 구성할 수 있습니다.

### 포트 상태

**System Options > Ports & Devices > Port Status(시스템 옵션 > 포트 및 장치 > 포트 상태)** 페이지에는 제품의 입력 및 출력 포트의 상태가 표시됩니다.

## 유지보수

Axis 제품은 다양한 유지보수 기능을 제공합니다. **Setup > Additional Controller Configuration > System Options > Maintenance(설정 > 추가 컨트롤러 구성 > 시스템 옵션 > 유지보수)**에서 이러한 기능을 사용할 수 있습니다.

Axis 제품이 원하는 대로 작동하지 않을 경우 올바르게 다시 시작하려면 **Restart(재시작)**를 클릭합니다. 이는 현재 설정에 영향을 주지 않습니다.

참고

재시작하면 서버 리포트의 모든 항목이 지워집니다.

대부분의 설정을 공장 출하 시 기본값으로 재설정하려면 **Restore(복구)**를 클릭합니다. 다음 설정은 영향을 받지 않습니다.

- 부팅 프로토콜(DHCP 또는 고정)
- 고정 IP 주소
- 기본 라우터
- 서브넷 마스크
- 시스템 시간
- IEEE 802.1X 설정

IP 주소를 비롯한 모든 설정을 공장 출하 시 기본값으로 재설정하려면 **Default(기본값)**를 클릭합니다. 이 버튼은 주의해서 사용해야 합니다. 제어 버튼을 사용하여 Axis 제품을 공장 출하 시 기본값으로 재설정할 수도 있습니다. 자세한 내용은 *공장 출하 시 기본 설정으로 재설정 페이지 64* 항목을 참조하십시오.

펌웨어 업그레이드에 대한 자세한 내용은 *펌웨어를 업그레이드하는 방법 페이지 65* 항목을 참조하십시오.

## 애플리케이션 데이터 백업

**Setup > Create a backup(설정 > 백업 생성)**으로 이동하여 애플리케이션 데이터의 백업을 생성합니다. 백업된 데이터에는 사용자, 자격 증명, 그룹 및 일정이 포함됩니다. 백업을 생성하면 데이터가 포함된 파일이 컴퓨터에 로컬로 저장됩니다.

**Setup > Upload a backup(설정 > 백업 업로드)**로 이동해 이전에 생성된 백업 파일을 사용하여 애플리케이션 데이터를 복원합니다. 백업 파일을 업로드하려면 먼저 장치를 공장 출하 시 기본 설정으로 재설정해야 합니다. 자세한 내용은 *공장 출하 시 기본 설정으로 재설정 페이지 64* 항목을 참조하십시오.

## 지원

### 지원 개요

**Setup > Additional Controller Configuration > System Options > Support > Support Overview(설정 > 추가 컨트롤러 구성 > 시스템 옵션 > 지원 > 지원 개요)** 페이지에 장애 처리에 대한 정보와 기술 지원 요청에 필요한 연락처 정보가 나와 있습니다.

또한 *장애 처리 페이지 65* 항목을 참조하십시오.

### 시스템 개요

Axis 제품의 상태 및 설정에 대한 개요를 보려면 **Setup > Additional Controller Configuration > System Options > Support > System Overview(설정 > 추가 컨트롤러 구성 > 시스템 옵션 > 지원 > 시스템 개요)**로 이동합니다. 여기에서 펌웨어 버전, IP 주소, 네트워크 및 보안 설정, 이벤트 설정, 최근 로그 항목과 같은 정보를 확인할 수 있습니다.

### 로그 및 보고서

**Setup > Additional Controller Configuration > System Options > Support > Logs & Reports(설정 > 추가 컨트롤러 구성 > 시스템 옵션 > 지원 > 로그 및 보고서)** 페이지에서는 시스템을 분석하고 문제를 해결하는 데 유용한 로그 및 보고서를 생성합니다. Axis 지원 서비스에 연락할 경우 질의와 함께 서버 리포트를 제공해 주십시오.

**시스템 로그** - 시스템 이벤트에 대한 정보를 제공합니다.

**액세스 로그** - 실패한 제품 액세스 시도를 모두 나열합니다. 제품에 대한 연결을 모두 나열하도록 액세스 로그를 구성할 수도 있습니다(아래 참조).

**서버 리포트 보기** - 팝업 창에 제품 상태에 대한 정보를 제공합니다. 액세스 로그는 자동으로 서버 리포트에 포함됩니다.

**서버 리포트 다운로드** - 전체 서버 리포트 텍스트 파일이 UTF-8 형식으로 포함된 .zip 파일을 생성합니다. 제품 실시간 보기의 스냅샷을 포함하려면 **Include snapshot from Live View(실시간 보기의 스냅샷 포함)** 옵션을 선택합니다. 지원 부서에 연락할 때는 항상 .zip 파일을 포함해야 합니다.

**매개변수 목록** - 제품의 매개변수와 현재 설정을 표시합니다. 그러면 문제를 해결하거나 Axis 지원 서비스에 연락할 때 유용합니다.

**연결 목록** - 미디어 스트림에 현재 액세스 중인 모든 클라이언트를 나열합니다.

**충돌 보고서** - 디버깅 정보가 포함된 아카이브를 생성합니다. 보고서를 생성하는 데 몇 분 정도 소요됩니다.

시스템 및 액세스 로그의 로그 레벨은 **Setup > Additional Controller Configuration > System Options > Support > Logs & Reports > Configuration(설정 > 추가 컨트롤러 구성 > 시스템 옵션 > 지원 > 로그 및 보고서 > 구성)**에서 설정합니다. 제품에 대한 모든 연결을 나열하도록 액세스 로그를 구성할 수 있습니다(위험, 경고 및 정보 선택).

## 고급

### 스크립팅

스크립팅을 통해 숙련된 사용자가 자신의 스크립트를 사용자 정의하고 사용할 수 있습니다.

***통지***

잘못 사용하면 예기치 않은 동작이 생기고 Axis 제품과의 접촉이 끊어질 수 있습니다.

결과를 잘 모르면 이 기능을 사용하지 마십시오. Axis 지원 부서에서는 사용자 정의 스크립트로 인한 문제에 지원을 제공하지 않습니다.

스크립트 편집기를 열려면 **Setup > Additional Controller Configuration > System Options > Advanced > Scripting(설정> 추가 컨트롤러 구성 > 시스템 옵션 > 고급 > 스크립팅)**으로 이동하십시오. 스크립트로 인해 문제가 생기면 제품을 공장 출하 시 기본 설정으로 재설정하고*페이지 64* 항목을 참조하십시오.

자세한 내용은 *www.axis.com/developer*를 참조하십시오.

### 파일 업로드

웹 페이지 및 이미지와 같은 파일을 Axis 제품에 업로드하여 사용자 정의 설정으로 사용할 수 있습니다. 파일을 업로드하려면 **설정 > 추가 컨트롤러 구성 > 시스템 옵션 > 고급 > 파일 업로드**로 이동합니다.

업로드한 파일은 `http://<ip address>/local/<user>/<file name>` 전체에서 액세스할 수 있습니다. 여기서 `<user>`는 업로드한 파일에 대해 선택한 사용자 그룹(관리자)입니다.

## 공장 출하 시 기본 설정으로 재설정

중요 사항

공장 출하 시 기본값으로 재설정은 주의해서 사용해야 합니다. 공장 출하 시 기본값으로 재설정하면 IP 주소를 비롯한 모든 설정이 공장 출하 시 기본값으로 재설정됩니다.

제품을 공장 출하 시 기본 설정으로 재설정하려면 다음을 수행하십시오.

1. 제품의 전원을 끊습니다.
2. 제어 버튼을 누른 상태에서 전원을 다시 연결합니다. *제품 개요 페이지 4* 항목을 참조하십시오.
3. 상태 LED 표시기가 다시 주황색으로 바뀔 때까지 25초 동안 제어 버튼을 누르고 있습니다.
4. 제어 버튼을 놓습니다. 상태 LED 표시기가 녹색으로 바뀌면 프로세스가 완료됩니다. 제품이 공장 출하 시 기본 설정으로 재설정되었습니다. 네트워크에서 사용할 수 있는 DHCP 서버가 없는 경우 기본 IP 주소는 `192.168.0.90`입니다.
5. 설치 및 관리 소프트웨어 도구를 사용하여 IP 주소를 할당하고, 패스워드를 설정하고, 제품에 액세스합니다.

또한 웹 인터페이스를 통해 매개변수를 공장 출하 시 기본값으로 재설정할 수 있습니다. **Setup > Additional Controller Configuration > Setup > System Options > Maintenance(설정 > 추가 컨트롤러 구성 > 설정 > 시스템 옵션 > 유지보수)**로 이동하고 **Default(기본값)**를 클릭합니다.

## 장애 처리

### 현재 펌웨어를 확인하는 방법

펌웨어는 네트워크 장치의 기능을 결정하는 소프트웨어입니다. 장애를 처리하는 경우 첫 번째로 취해야 할 동작 중 하나는 현재 펌웨어 버전을 확인하는 것입니다. 최신 버전에 특정 문제를 해결하는 수정 사항이 포함되어 있을 수 있습니다.

Axis 제품의 현재 펌웨어 버전이 개요 페이지에 표시됩니다.

### 펌웨어를 업그레이드하는 방법

중요 사항

- 판매자는 사용자의 결합 업그레이드로 인해 발생하는 모든 수리에 대해 비용을 청구할 권리가 있습니다.
- 펌웨어가 업그레이드되면 사전 구성된 사용자 정의 설정이 저장되며(새 펌웨어에서 기능을 사용할 수 있는 경우) Axis Communications AB에서 이를 보장하지는 않습니다.
- 이전 펌웨어 버전을 설치할 경우 나중에 제품을 공장 출하 시 기본 설정으로 복구해야 합니다.

참고

- 업그레이드 프로세스가 완료되면 제품이 자동으로 다시 시작됩니다. 업그레이드 후 수동으로 제품을 다시 시작할 경우 업그레이드가 실패한 것 같더라도 5분간 기다려 주십시오.
- 사용자, 그룹, 자격 증명 및 기타 데이터의 데이터베이스가 펌웨어 업그레이드 이후에 업데이트되었기 때문에 처음 시작 시 완료하는 데 몇 분 정도 소요될 수 있습니다. 소요되는 시간은 데이터 양에 따라 달라집니다.
- Axis 제품을 최신 펌웨어로 업그레이드하면 제품에 사용할 수 있는 최신 기능이 업데이트됩니다. 펌웨어를 업그레이드하기 전에 항상 각각의 새로운 릴리스에서 사용할 수 있는 릴리스 정보와 업그레이드 지침을 참조하십시오.

**독립형 도어 컨트롤러:**

1. *www.axis.com/support*에서 무료로 제공되는 최신 펌웨어 파일을 컴퓨터에 다운로드합니다.
2. 제품 웹 페이지에서 **Setup > Additional Controller Configuration > System Options > Maintenance(설정 > 추가 컨트롤러 구성 > 시스템 옵션 > 유지보수)**로 이동합니다.
3. **Upgrade Server(서버 업그레이드)**에서 **Choose file(파일 선택)**을 선택하고 컴퓨터에서 파일을 찾습니다.
4. 업그레이드 후 제품을 공장 출하 시 기본 설정으로 자동 복구하려면 **Default(기본값)** 확인란을 선택합니다.
5. **Upgrade(업그레이드)**를 클릭합니다.
6. 제품을 업그레이드하고 다시 시작하는 동안 5분 가량 기다립니다. 그런 다음 웹 브라우저의 캐시를 지웁니다.
7. 제품에 액세스합니다.

**시스템의 도어 컨트롤러:**

AXIS Device Manager 또는 AXIS Camera Station을 사용하여 시스템의 모든 도어 컨트롤러를 업그레이드할 수 있습니다. 자세한 내용은 *www.axis.com*을 참조하십시오.

중요 사항

- 순차적 업그레이드를 선택하지 마십시오.

참고

- 시스템의 모든 컨트롤러가 항상 같은 펌웨어 버전에 있어야 합니다.
- AXIS Device Manager 또는 AXIS Camera Station의 병렬 옵션을 사용하여 시스템의 모든 컨트롤러를 동시에 업그레이드합니다.

## 긴급 복구 절차

업그레이드 중에 전원 또는 네트워크 연결이 끊어지면 프로세스가 실패하고 제품이 응답하지 않을 수 있습니다. 상태 표시기가 빨간색으로 깜박이면 업그레이드 실패를 나타냅니다. 제품을 복구하려면 아래 단계를 따르십시오. 일련번호는 제품 라벨에 있습니다.

1. **UNIX/Linux**에서는 명령줄에 다음과 같이 입력하십시오.

   ```
   arp -s <IP address> <serial number> temp
   ping -l 408 <IP address>
   ```

   **Windows**에서는 명령/DOS 프롬프트에 다음과 같이 입력하십시오. 이때 관리자 권한으로 명령 프롬프트를 실행해야 할 수도 있습니다.

   ```
   arp -s <IP address> <serial number>
   ping -l 408 -t <IP address>
   ```

2. 제품이 30초 이내에 응답하지 않으면 제품을 다시 시작하고 응답할 때까지 기다립니다. 키보드에서 CTRL+C를 눌러 Ping을 중지합니다.
3. 브라우저를 열고 제품의 IP 주소를 입력합니다. 페이지가 열리면 **Browse(찾아보기)** 버튼을 사용하여 사용할 업그레이드 파일을 선택합니다. 그런 다음 **Load(업로드)**를 클릭하여 업그레이드 프로세스를 다시 시작합니다.
4. 업그레이드가 완료되면(1~10분) 제품이 자동으로 다시 시작되고 상태 표시기가 녹색으로 켜집니다.
5. 설치 가이드를 참조하여 제품을 다시 설치합니다.

긴급 복구 절차를 수행해도 제품이 다시 실행되지 않을 경우 *www.axis.com/support*의 Axis 지원 부서에 문의하십시오.

## 증상, 가능한 원인 및 수정 조치

| **펌웨어 업그레이드 문제** | |
|---|---|
| 펌웨어 업그레이드 실패 | 펌웨어 업그레이드에 실패하면 제품이 이전 펌웨어를 다시 로드합니다. 펌웨어 파일을 확인하고 다시 시도하십시오. |

| **IP 주소 설정 문제** | |
|---|---|
| ARP/Ping을 사용하는 경우 | 다시 설치해 보십시오. IP 주소는 제품에 전원이 공급된 후 2분 이내에 설정해야 합니다. Ping 길이를 408로 설정해야 합니다. 자세한 내용은 *axis.com*의 제품 페이지에서 설치 가이드를 참조하십시오. |
| 제품이 다른 서브넷에 있습니다. | 제품에 해당하는 IP 주소와 제품 액세스에 사용된 컴퓨터의 IP 주소가 다른 서브넷에 있는 경우에는 IP 주소를 설정할 수 없습니다. 네트워크 관리자에게 문의하여 IP 주소를 받으십시오. |
| IP 주소가 다른 장치에서 사용 중입니다. | 네트워크에서 Axis 제품을 분리합니다. Ping 명령을 실행합니다(명령/DOS 윈도우에서 제품의 IP 주소 및 `ping`을 입력하십시오).<br>• 다음과 같이 `Reply from <IP address>: bytes=32; time=10...`이라는 메시지를 받는 경우 이는 IP 주소가 이미 네트워크의 다른 장치에서 사용 중 일 수 있음을 의미합니다. 네트워크 관리자에게 새 IP 주소를 받아 제품을 다시 설치하십시오.<br>• 다음과 같이 `Request timed out`이라는 메시지를 받는 경우 이는 Axis 제품에 IP 주소를 사용할 수 있음을 의미합니다. 모든 케이블 배선을 확인하고 제품을 다시 설치하십시오. |
| 동일한 서브넷의 다른 장치와 충돌하는 가용 IP 주소 | DHCP 서버에서 다이내믹 주소를 설정하기 전에 Axis 제품의 고정 IP 주소가 사용되었습니다. 이는 동일한 기본 고정 IP 주소가 다른 장치에서도 사용되는 경우 제품 액세스에 문제가 발생했을 수 있음을 의미합니다. |

# 장애 처리

**제품을 브라우저에서 액세스할 수 없음**

| | |
|---|---|
| 로그인할 수 없음 | HTTPS가 활성화 되면, 로그인을 시도할 때 올바른 프로토콜(HTTP 또는 HTTPS)이 사용되는지 확인하십시오. 브라우저의 주소 입력란에 `http` 또는 `https`를 수동으로 입력해야 할 수도 있습니다.<br><br>사용자 root의 비밀번호를 분실한 경우에는 제품을 공장 기본 설정값으로 재설정해야 합니다. *공장 출하 시 기본 설정으로 재설정 페이지 64* 항목을 참조하십시오. |
| IP 주소가 DHCP에 의해 변경됨 | DHCP서버에서 획득한 IP 주소는 동적이며 변경될 수 있습니다. IP 주소가 변경된 경우에는 AXIS IP Utility 또는 AXIS Device Manager를 사용하여 네트워크에서 제품을 찾습니다. 해당 모델이나 일련 번호 또는 DNS 이름을 이용하여 제품을 식별합니다(이름이 구성된 경우).<br><br>필요한 경우 고정 IP 주소를 수동으로 할당할 수 있습니다. 자세한 내용은 *axis.com*의 제품 페이지에서 *IP 주소를 할당하고 장치에 액세스하는 방법* 문서를 참조하십시오. |
| IEEE 802.1X를 사용하는 동안 발생하는 인증 오류 | 인증이 제대로 작동하려면 Axis 제품의 날짜 및 시간이 NTP 서버와 동기화되어야 합니다. *날짜 및 시간 페이지 56* 항목을 참조하십시오. |

**제품에 로컬 액세스를 할 수 있지만 외부에서 액세스할 수 없음**

| | |
|---|---|
| 라우터 구성 | Axis 제품에 데이터 트래픽 수신을 허용하도록 라우터를 구성하려면 Axis 제품에 대한 액세스를 허용하도록 라우터를 자동으로 구성하려고 시도하는 NAT 통과 기능을 활성화하십시오. 자세한 내용은 *IPv4에 대한 NAT 통과(포트 매핑) 페이지 60* 항목을 참조하십시오. 라우터가 UPnP®를 지원해야 합니다. |
| 방화벽 보호 | 네트워크 관리자를 통해 인터넷 방화벽을 확인하십시오. |
| 기본 라우터 필요 | **Setup > Network Settings(설정 > 네트워크 설정)** 또는 **Setup > Additional Controller Configuration > System Options > Network > TCP/IP > Basic(설정 > 추가 컨트롤러 구성 > 시스템 옵션 > 네트워크 > TCP/IP > 기본)**에서 라우터 설정을 구성해야 하는지 확인합니다. |

**상태 및 네트워크 표시기 LED가 빨간색으로 빠르게 깜박임**

| | |
|---|---|
| 하드웨어 오류 | Axis 리셀러에게 문의하십시오. |

**제품이 시작되지 않음**

| | |
|---|---|
| 제품이 시작되지 않음 | 제품이 시작되지 않는 경우 네트워크 케이블을 연결된 상태로 유지하고 전원 케이블을 미드스팬에 다시 연결합니다. |

# 사양

## 사양

### 커넥터

커넥터 위치에 대한 자세한 내용은 항목을 참조하십시오.

하드웨어 구성을 통해 생성된 하드웨어 핀 차트에 대한 정보 및 연결 다이어그램은 *연결 다이어그램 페이지 72* 및 *하드웨어 구성 페이지 14* 항목을 참조하십시오.

다음 섹션에서는 커넥터의 기술 사양에 대해 설명합니다.

#### 리더 데이터 커넥터

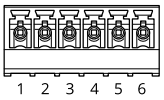
리더와 통신하도록 RS485 및 Wiegand 프로토콜을 지원하는 6핀 터미널 블록입니다.

RS485 포트 지원:

- 2개 와이어 RS485 반이중
- 4개 와이어 RS485 전이중

Wiegand 포트 지원:

- 2개 와이어 Wiegand




| 기능 | | 핀 | 참고 |
|---|---|---|---|
| RS485 | A- | 1 | 전이중 RS485에 사용됨<br>반이중 RS485에 사용됨 |
| | B+ | 2 | |
| RS485 | A- | 3 | 전이중 RS485에 사용됨<br>반이중 RS485에 사용됨 |
| | B+ | 4 | |
| Wiegand | D0(Data 0) | 5 | Wiegand에 사용됨 |
| | D1(Data 1) | 6 | |

중요 사항

RS485 포트의 고정 보드 속도는 9600Bit/s입니다.

중요 사항

최대 권장 케이블 길이는 30m(98.4ft)입니다.

중요 사항

이 섹션의 출력 회로는 Class 2 전류로 제한되어 있습니다.

#### 리더 I/O 커넥터

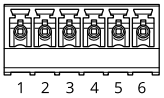
다음 용도의 6핀 터미널 블록입니다.

- 보조 전원(DC 출력)

## 사양

- 디지털 입력
- 디지털 출력
- 0V DC(-)

리더 I/O 커넥터의 3번 핀은 관리될 수 있습니다. 연결이 중단되면 이벤트가 활성화됩니다. 관리된 입력을 사용하려면 EOL 레지스터를 설치하십시오. 관리된 입력에 대한 연결 다이어그램을 사용합니다. *페이지 73* 항목을 참조하십시오.




| 기능 | 핀 | 참고 | 사양 |
|---|---|---|---|
| 0V DC(-) | 1 | | 0V DC |
| DC 출력 | 2 | 보조 장비에 전원을 공급하는 데 사용됩니다. 참고: 이 핀은 정전된 경우에만 사용할 수 있습니다. | 12V DC<br>최대 부하 = 300mA |
| 구성 가능(입력 또는 출력) | 3–6 | 디지털 입력 - 활성화하려면 핀 1에 연결하고 비활성화하려면 부동 상태(연결되지 않음)로 둡니다. | 0 ~ 최대 40V DC |
| | | 디지털 출력 - 활성화하려면 핀 1에 연결하고 비활성화하려면 부동 상태(연결되지 않음)로 둡니다. 릴레이와 같은 유도 부하와 함께 사용할 경우 다이오드는 전압 과도 현상을 방지하도록 부하와 병렬로 연결해야 합니다. | 0 ~ 최대 40V DC, 개방 드레인, 100mA |

중요 사항

최대 권장 케이블 길이는 30m(98.4ft)입니다.

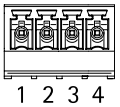
중요 사항

이 섹션의 출력 회로는 Class 2 전류로 제한되어 있습니다.

### 도어 커넥터

도어 모니터링 장치용 2개의 4핀 터미널 블록입니다(디지털 입력).

모든 도어 입력 핀을 관리할 수 있습니다. 연결이 중단되면 알람이 트리거됩니다. 관리된 입력을 사용하려면 EOL 레지스터를 설치하십시오. 관리된 입력에 대한 연결 다이어그램을 사용합니다. *페이지 73* 항목을 참조하십시오.




| 기능 | 핀 | 참고 | 사양 |
|---|---|---|---|
| 0V DC(-) | 1, 3 | | 0V DC |
| 입력 | 2, 4 | 도어 모니터와 통신하는 데 사용됩니다.<br>디지털 입력 - 활성화하려면 핀 1 또는 3에 각각 연결하고, 비활성화하려면 부동 상태(연결되지 않음)로 둡니다.<br>참고: 이 핀은 입력에만 사용할 수 있습니다. | 0 ~ 최대 40V DC |

## 사양

중요 사항

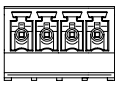
최대 권장 케이블 길이는 30m(98.4ft)입니다.

### 보조 커넥터

다음 용도의 구성 가능한 4핀 I/O 터미널 블록입니다.

- 보조 전원(DC 출력)
- 디지털 입력
- 디지털 출력
- 0V DC(-)

연결 다이어그램 예는 *연결 다이어그램 페이지 72* 항목을 참조하십시오.




| 기능 | 핀 | 참고 | 사양 |
|---|---|---|---|
| 0V DC(-) | 1 | | 0V DC |
| DC 출력 | 2 | 보조 장비에 전원을 공급하기 위해 사용합니다. 참고: 이 핀은 정전된 경우에만 사용할 수 있습니다. | 3.3V DC<br>최대 부하 = 100mA |
| 구성 가능(입력 또는 출력) | 3–4 | 디지털 입력 - 활성화하려면 핀 1에 연결하고 비활성화하려면 부동 상태(연결되지 않음)로 둡니다. | 0 ~ 최대 40V DC |
| | | 디지털 출력 - 활성화하려면 핀 1에 연결하고 비활성화하려면 부동 상태(연결되지 않음)로 둡니다. 릴레이와 같은 유도 부하와 함께 사용할 경우 다이오드는 전압 과도 현상을 방지하도록 부하와 병렬로 연결해야 합니다. | 0 ~ 최대 40V DC, 개방 드레인, 100mA |

중요 사항

최대 권장 케이블 길이는 30m(98.4ft)입니다.

중요 사항

이 섹션의 출력 회로는 Class 2 전류로 제한되어 있습니다.

### 전원 커넥터

DC 전원 입력용 2핀 터미널 블록입니다. 정격 출력 전력이 100W 이하로 제한되거나 정격 출력 전류가 5A 이하로 제한된 SELV(Safety Extra Low Voltage) 준수 LPS(제한된 전원)를 사용하십시오.

## 사양

| 기능 | 핀 | 참고 | 사양 |
|---|---|---|---|
| 0V DC(-) | 1 | | 0V DC |
| DC 입력 | 2 | PoE(Power over Ethernet) 미사용 시 컨트롤러에 전원을 공급하는 데 사용됩니다.<br>참고: 이 핀은 전원이 공급된 경우에만 사용할 수 있습니다. | 10 ~ 28V DC, 최대 36W<br>출력의 최대 부하 = 14W |

### 네트워크 커넥터

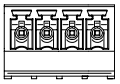
RJ45 이더넷 커넥터입니다. Category 5e 케이블 이상을 사용합니다.

| 기능 | 사양 |
|---|---|
| PoE(Power over Ethernet) | PoE(Power over Ethernet) IEEE 802.3af/802.3at Type 1 Class 3, 44 ~ 57V DC<br><br>출력의 최대 부하 = 7.5W |

### 전원 잠금 커넥터

1개 또는 2개의 잠금 장치에 전원을 공급하는 4핀 터미널 블록입니다(DC 출력). 잠금 커넥터는 외부 장치에 전원을 공급하는 데에도 사용할 수 있습니다.

하드웨어 구성을 통해 생성된 하드웨어 핀 차트에 따라 잠금 장치 및 부하 장치를 핀에 연결합니다.




| 기능 | 핀 | 참고 | 사양 |
|---|---|---|---|
| 0V DC(-) | 1, 3 | | 0V DC |
| 0V DC, 부동 또는 12V DC | 2, 4 | 최대 2개의 12V 잠금 장치를 제어하는 데 사용됩니다. 하드웨어 핀 차트를 사용합니다. *하드웨어 구성 페이지 14* 항목을 참조하십시오. | 12V DC<br>최대 부하 합계 = 500mA |

***통지***

잠금 장치가 극성이 없는 경우 외부 플라이백 다이오드를 추가하는 것이 좋습니다.

중요 사항

이 섹션의 출력 회로는 Class 2 전류로 제한되어 있습니다.

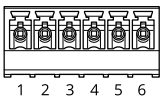
### 전원 및 릴레이 커넥터

다음 용도의 내장 릴레이가 있는 6핀 터미널 블록

- 외부 장치
- 보조 전원(DC 출력)
- 0V DC(-)

하드웨어 구성을 통해 생성된 하드웨어 핀 차트에 따라 잠금 장치 및 부하 장치를 핀에 연결합니다.

## 사양




| 기능 | 핀 | 참고 | 사양 |
|---|---|---|---|
| 0V DC(-) | 1, 4 | | 0V DC |
| 릴레이 | 2–3 | 릴레이 장치 연결에 사용됩니다. 하드웨어 핀 차트를 사용합니다. *하드웨어 구성 페이지 14* 항목을 참조하십시오.<br>두 개의 릴레이 핀은 나머지 회로와 전기적으로 분리되어 있습니다. | 최대 전류 = 700mA<br>최대 전압 = +30V DC |
| 12V DC | 5 | 보조 장비에 전원을 공급하는 데 사용됩니다.<br>참고: 이 핀은 정전된 경우에만 사용할 수 있습니다. | 최대 전압 = +12V DC<br>최대 부하 = 500mA |
| 24V DC | 6 | 사용되지 않음 | |

***통지***

잠금 장치가 극성이 없는 경우 외부 플라이백 다이오드를 추가하는 것이 좋습니다.

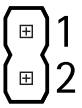
중요 사항

이 섹션의 출력 회로는 Class 2 전류로 제한되어 있습니다.

### 탬퍼링 알람 핀 헤더

다음을 우회하는 2개의 2핀 헤더입니다.

- 후면 탬퍼링 알람(TB)
- 전면 탬퍼링 알람(TF)




| 기능 | 핀 | 참고 |
|---|---|---|
| 후면 탬퍼링 알람 | 1–2 | 전면 및 후면 탬퍼링 알람을 동시에 우회하려면 TB 1, TB 2 및 TF 1, TF 2 간에 점퍼를 각각 연결하십시오. 탬퍼링 알람을 우회한다는 것은 시스템이 탬퍼링 시도를 식별하지 못한다는 의미입니다. |
| 전면 탬퍼링 알람 | 1–2 | |

참고

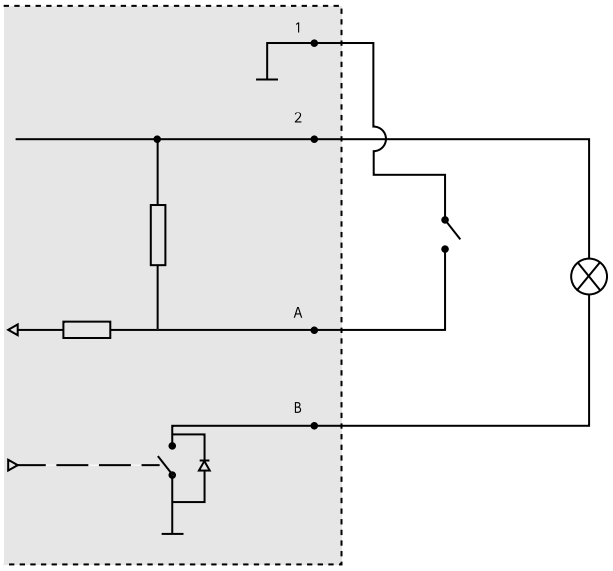
전면 및 후면 탬퍼링 알람은 모두 기본적으로 연결되어 있습니다. 도어 컨트롤러가 열려 있거나 도어 컨트롤러가 벽이나 천장에서 분리되는 경우 액션을 수행하도록 케이스 열림 트리거를 구성할 수 있습니다. 알람 및 이벤트를 구성하는 방법에 대한 자세한 내용은 *알람 및 이벤트 구성 페이지 45* 항목을 참조하십시오.

## 연결 다이어그램

하드웨어 구성을 통해 생성된 하드웨어 핀 차트에 따라 장치를 연결합니다. 하드웨어 구성 및 하드웨어 핀 차트에 대한 자세한 내용은 *하드웨어 구성 페이지 14* 항목을 참조하십시오.

## 사양

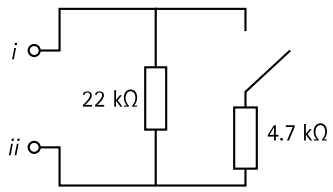
### 보조 커넥터




*1 0V DC(-)*
*2 DC 출력: 3.3V, 최대 100mA*
*A I/O가 입력으로 구성됨*
*B I/O가 출력으로 구성됨*

### 관리된 입력

관리된 입력을 사용하려면 아래의 다이어그램에 따라 EOL 레지스터를 설치하십시오.




*i 입력*
*ii 0V DC(-)*

참고

트위스트 및 차폐 케이블을 사용하는 것이 좋습니다. 차폐물을 0V DC에 연결하십시오.

# 안전 정보

## 위험 레벨

**⚠위험**

피하지 못한 경우 사망이나 심각한 부상이 발생하는 위험한 상황을 나타냅니다.

**⚠경고**

피하지 못한 경우 사망이나 심각한 부상이 발생할 수 있는 위험한 상황을 나타냅니다.

**⚠주의**

피하지 못한 경우 경미하거나 심하지 않은 부상이 발생할 수 있는 위험한 상황을 나타냅니다.

***통지***

피하지 못한 경우 재산상 손해가 발생할 수 있는 상황을 나타냅니다.

## 기타 메시지 레벨

중요 사항

제품이 올바르게 작동하는 데 필수적인 중요 정보를 나타냅니다.

참고

제품을 최대한으로 활용하는 데 도움이 되는 유용한 정보를 나타냅니다.

사용자 설명서
AXIS A1001 & AXIS Entry Manager

Ver. M25.2
날짜: 12월 2023
부품 번호 T10010336