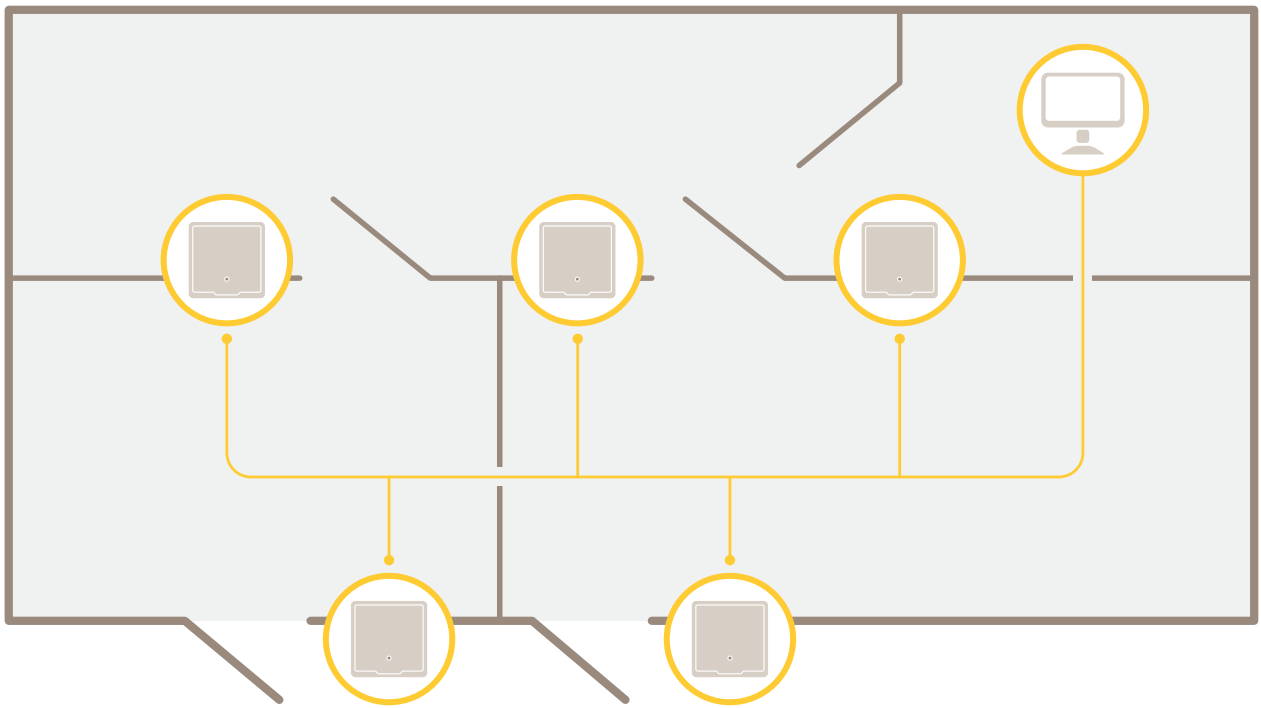
AXIS A1601 Network Door Controller

사용자 설명서

목차

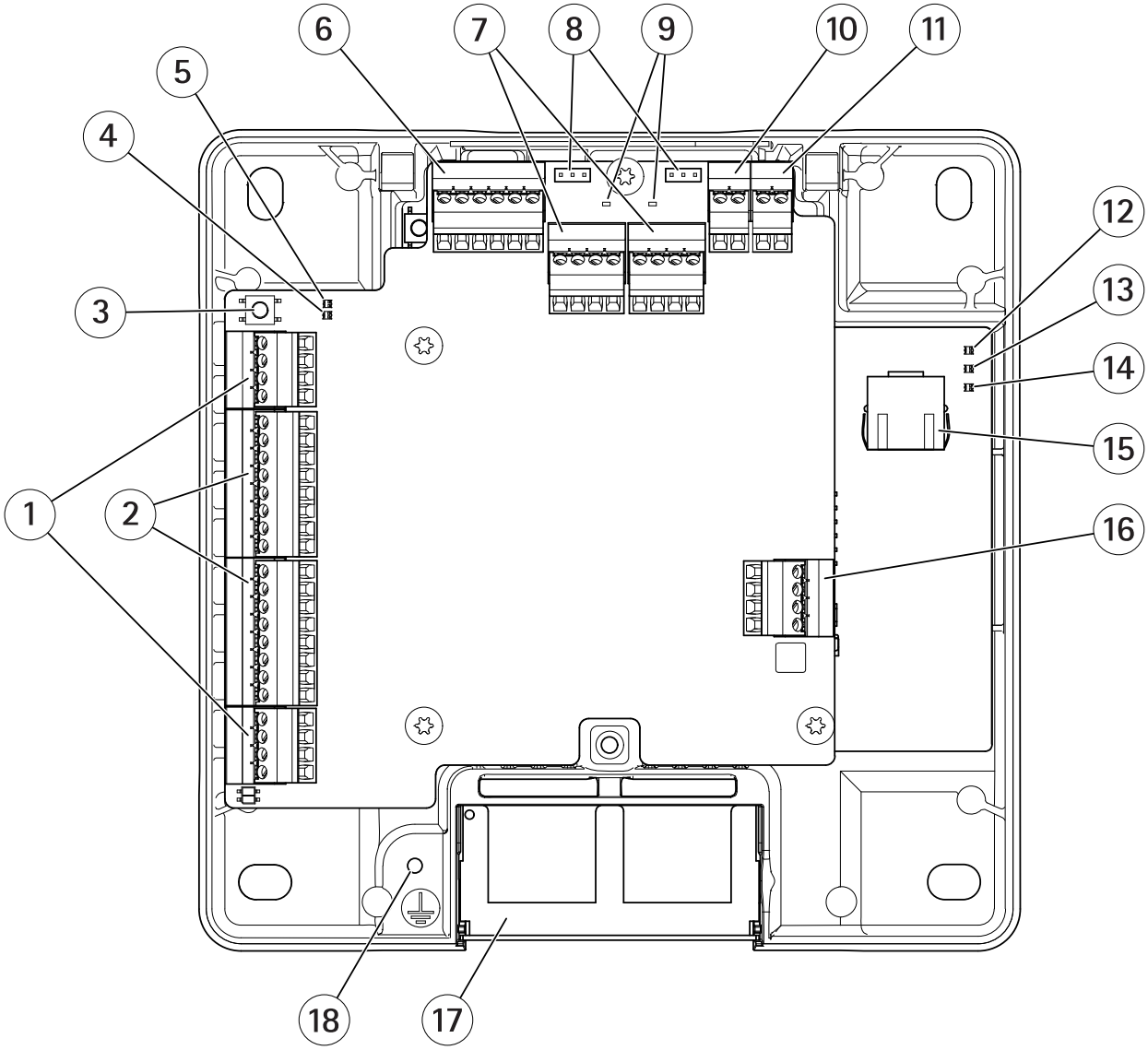
솔루션 개요



특별한 배선 없이 네트워크 도어 컨트롤러에 쉽게 연결하고 기존의 IP 네트워크로 전원을 공급할 수 있습니다.

각 네트워크 도어 컨트롤러는 도어 근처에 쉽게 장착할 수 있는 지능형 장치입니다. 최대 네 개의 리더에 전원을 공급하고 제어할 수 있습니다.

제품 개요



1 (2개)
2 (2개)
3
4 리더 과전류 LED
5 릴레이 과전류 LED
6
7 (2개)
8 릴레이 점퍼(2개)
9 릴레이 LED(2개)
10
11
12 전원 LED
13 상태 LED
14 네트워크 LED
15
16
17 양면 케이블 커버
18 접지 위치

네트워크에서 장치 찾기

네트워크에서 Axis 장치를 찾고 Windows®에서 해당 장치에 IP 주소를 할당하려면 AXIS IP Utility 또는 AXIS Device Manager를 사용합니다. 두 애플리케이션은 *axis.com/support*에서 무료로 다운로드할 수 있습니다.

*IP 주소를 할당하고 장치에 액세스하는 방법*으로 이동하여 어떻게 IP 주소를 찾아 할당하는지 자세히 알아보십시오.

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. 을 참조하십시오.
3. 브라우저에서 장치의 웹 페이지가 열립니다. 시작 페이지를 개요 페이지라고 합니다.

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

비고

- 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.

안전한 패스워드

중요 사항

네트워크를 통해 패스워드 또는 기타 민감한 구성을 설정하려면 HTTPS(기본적으로 활성화됨)를 사용하십시오. HTTPS는 보안 및 암호화된 네트워크 연결을 활성화하여 패스워드와 같은 민감한 데이터를 보호합니다.

장치 패스워드는 데이터 및 서비스에 대한 기본 보호입니다. Axis 장치는 다양한 설치 유형에 사용될 수 있으므로 해당 장치에는 패스워드 정책을 적용하지 않습니다.

데이터 보호를 위해 적극 권장되는 작업은 다음과 같습니다.

- 최소 8자 이상의 패스워드를 사용합니다. 패스워드 생성기로 패스워드를 생성하는 것이 더 좋습니다.
- 패스워드를 노출하지 않습니다.

- 최소 일 년에 한 번 이상 반복되는 간격으로 패스워드를 변경합니다.

root 패스워드를 설정하는 방법

엑시스 제품에 액세스하려면 기본 관리자 사용자 **Root(루트)**에 대한 비밀번호를 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 암호화를 통해 정보를 교환할 수 있도록 해줍니다. 을 참조하십시오.

기본 관리자 사용자 이름 **Root(루트)**는 영구적이며 삭제할 수 없습니다. Root(루트)의 비밀번호를 분실한 경우 제품을 공장 기본 설정값으로 재설정해야 합니다. 을 참조하십시오.

패스워드를 설정하려면 대화 상자에 직접 패스워드를 입력합니다.

개요 페이지

제품 웹 페이지의 개요 페이지에는 도어 컨트롤러의 이름, MAC 주소, IP 주소 및 펌웨어 버전에 대한 정보가 표시됩니다. 이 페이지에서 네트워크의 도어 컨트롤러를 식별할 수도 있습니다.

Axis 제품에 처음 액세스하면 개요 페이지에 하드웨어를 구성하고, 날짜 및 시간을 설정하고, 네트워크 설정을 구성하라는 메시지가 나타납니다. 시스템 구성에 대한 자세한 내용은 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 항목을 참조하십시오.

구성 - 단계별

접근 제어 시스템을 사용하기 전에 다음 설정 단계를 완료해야 합니다.

1. 영어가 모국어가 아닌 경우 제품 웹 페이지에서 다른 언어를 사용할 수 있습니다. 을 참조하십시오.
2. 날짜 및 시간을 설정합니다. 을 참조하십시오.
3. 네트워크 설정을 구성합니다. 을 참조하십시오.
4. 도어 컨트롤러와 리더, 잠금장치, 종료 요청(REX) 장치 등 연결된 장치를 구성합니다. 을 참조하십시오.
5. 하드웨어 연결을 확인합니다. 을 참조하십시오.
6. 카드 및 형식을 구성합니다. 을 참조하십시오.

유지보수 권장 사항에 대한 자세한 내용은 항목을 참조하십시오.

언어 선택

제품 웹 페이지의 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.

비고

- 언어를 전환하면 날짜 형식도 선택한 언어에서 일반적으로 사용되는 형식으로 변경됩니다. 올바른 형식이 데이터 필드에 표시됩니다.
- 제품을 공장 출하 시 기본값으로 재설정하면 제품 웹 페이지가 다시 영어로 전환됩니다.
- 제품을 복구 또는 재시작하거나 펌웨어를 업그레이드할 경우 제품 웹 페이지에서는 선택된 언어가 계속 사용됩니다.

날짜 및 시간 설정

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. 을 참조하십시오.
- 수동으로 날짜 및 시간을 설정합니다. 을 참조하십시오.
- 컴퓨터에서 날짜 및 시간을 가져옵니다. 을 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. **Setup(설정) > Additional Controller Configuration(추가 컨트롤러 구성) > System Options(시스템 옵션) > Date & Time(날짜 및 시간)**로 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 항목을 참조하십시오.
NTP 서버에 호스트 이름을 사용할 경우 DNS 서버를 구성해야 합니다. 을 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 항목을 참조하십시오.

하드웨어 구성

하드웨어 구성을 완료하기 전에도 리더, 잠금장치 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 항목을 참조하십시오.

처음으로 하드웨어를 구성하는 경우 다음 방법 중 하나를 선택합니다.
- 하드웨어 구성 파일을 가져옵니다. 을 참조하십시오.

- 새 하드웨어 구성을 만듭니다. 을 참조하십시오.

비고

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 를 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.

비고

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

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 잠금장치를 구성하고 **Next(다음)**를 클릭합니다. 사용 가능한 옵션에 대한 자세한 내용은 항목을 참조하십시오.
5. 사용할 리더 및 REX 장치를 구성하고 **Finish(마침)**를 클릭합니다. 사용 가능한 옵션에 대한 자세한 내용은 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 를 참조하십시오.

비고

- 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.

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 잠금장치가 잠깁니다.

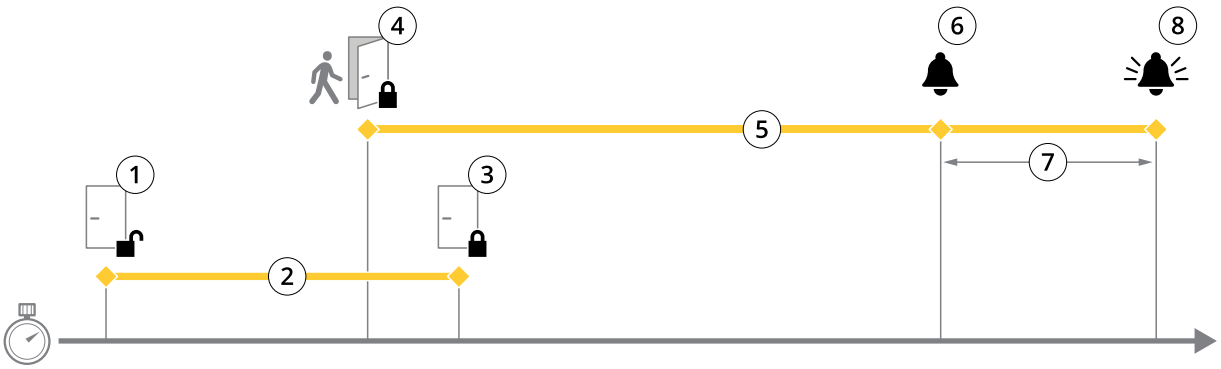
다음과 같은 도어 시간 옵션을 항상 사용할 수 있습니다.

- **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.

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 - 잠금장치 잠금 해제
2 접근 시간
3 취한 액션 없음 - 잠금장치 잠금
4 취한 액션(도어 열림) - 도어가 닫힐 때까지 잠금장치 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 항목을 참조하십시오.

잠금 옵션에 대한 정보

다음과 같은 잠금 회로 옵션을 사용할 수 있습니다.

- **Relay(릴레이)** - 도어 컨트롤러당 하나의 잠금장치에만 사용할 수 있습니다. 두 개의 도어가 도어 컨트롤러에 연결된 경우 두 번째 도어의 잠금장치에만 릴레이를 사용할 수 있습니다.
- **None(없음)** - 잠금장치 2에만 사용할 수 있습니다. 잠금장치를 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 잠금장치를 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.

리더 및 REX 장치 구성 방법

새로운 하드웨어 구성에서 도어 모니터와 잠금장치를 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 제어 기능이 있는 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.

비고

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 도어 모니터 간의 연결 상태를 보고합니다. 연결이 중단되면 이벤트가 활성화됩니다.

관리된 입력을 사용하려면

1. 사용되는 모든 관리된 입력에 EOL 레지스터를 설치합니다. 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 기능은 관리된 입력을 지원합니다.

- 도어 모니터. 을 참조하십시오.

무선 잠금장치에 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 잠금장치 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. 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. 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.

비고

외부 DPS(도어 위치 센서)를 사용하는 경우 이를 구성하기 전에 Aperio 잠금장치가 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. **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.

비고

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

1. 도어 컨트롤러의 웹 페이지에서 **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(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. **추가**를 클릭합니다.

비고

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. **추가**를 클릭합니다.

하드웨어 연결 확인

하드웨어 설치 및 구성이 완료되고 도어 컨트롤러 수명 중 언제든지 연결된 도어 모니터, 네트워크 I/O 릴레이 모듈, 잠금장치 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 잠금장치의 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(액세스)**를 클릭합니다.

- **Reader: Feedback(리더: 피드백)** – 다양한 명령에 대한 리더 피드백(예: 소리 및 LED 신호)을 확인합니다. 명령을 선택하고 **Test(테스트)**를 클릭합니다. 사용할 수 있는 피드백 유형은 리더에 따라 달라집니다. 자세한 내용은 를 참조하십시오. 또한 제조업체 지침을 참조하십시오.
- **Reader: Tampering(리더: 탬퍼링)** – 마지막 탬퍼링 시도에 대한 정보를 확인합니다. 리더가 설치되면 첫 번째 탬퍼링 시도가 등록됩니다. **Get last tampering(마지막 탬퍼링 가져오기)**을 클릭합니다.
- **Reader: Card swipe(리더: 카드 태그)** – 마지막에 태그한 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(액세스)**를 클릭합니다.
- **Elevator Reader: Feedback(엘리베이터 리더: 피드백)** – 다양한 명령에 대한 리더 피드백(예: 소리 및 LED 신호)을 확인합니다. 명령을 선택하고 **Test(테스트)**를 클릭합니다. 사용할 수 있는 피드백 유형은 리더에 따라 달라집니다. 자세한 내용은 를 참조하십시오. 또한 제조업체 지침을 참조하십시오.
- **Elevator Reader: Tampering(엘리베이터 리더: 탬퍼링)** – 마지막 탬퍼링 시도에 대한 정보를 확인합니다. 리더가 설치되면 첫 번째 탬퍼링 시도가 등록됩니다. **Get last tampering(마지막 탬퍼링 가져오기)**을 클릭합니다.
- **Elevator Reader: Card swipe(엘리베이터 리더: 카드 태그)** – 마지막에 태그한 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 지정 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. 을 참조하십시오.
4. **Add field map(필드 맵 추가)**을 클릭하고 필드에 필요한 정보를 입력합니다. 을 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 ,255mm,sfx)="graphics:graphic9888EC0F1598FFE8AD18417EB19F3348"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 ,255mm,sfx)="graphics:graphicE2E4BFB630DBE68A0DD8F8511E2830AE"을 클릭합니다.

카드 형식을 삭제하려면 ,255mm,sfx)="graphics:graphicE2E4BFB630DBE68A0DD8F8511E2830AE"을 클릭합니다.

중요 사항

- 도어 컨트롤러에 하나 이상의 리더가 구성된 경우에만 카드 형식을 활성화 및 비활성화할 수 있습니다. 자세한 내용은 및 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.
  - `Parity` - 오류 감지에 패리티 비트가 사용됩니다. 일반적으로 패리티 비트는 이진 코드 문자열 처음이나 끝에 추가되며 비트 수가 짝수인지 홀수인지를 나타냅니다.
  - `EvenParity` – 짝수 패리티 비트는 문자열의 비트 수가 짝수가 되도록 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.
  - `OddParity` – 홀수 패리티 비트는 문자열의 비트 수가 홀수가 되도록 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.
  - `FacilityCode` – 토큰이 주문된 최종 사용자 자격 증명 배치와 일치하는지 확인하기 위해 시설 코드가 사용되는 경우가 있습니다. 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.
  - `CardNr` – 접근 제어 시스템에서 가장 일반적으로 검증하는 항목은 카드 번호 또는 사용자 ID입니다. 제품이 카드 번호를 확인하기 위해서는 대소문자를 구분하는 이 필드 맵 이름이 필요합니다.
  - `CardNrHex` – 카드 번호의 이진 데이터는 제품에서 소문자 16진수 숫자로 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. 16진수 체계는 기수 16 진법이라고도 하며, 숫자 0~9와 문자 a~f의 16개 고유 기호로 구성됩니다. Little endian 비트 순서는 첫 번째 비트가 가장 작은(최하위) 비트임을 의미합니다.
  - **BinBE2Hex** - 이진 데이터가 big endian 비트 순서의 16진수 소문자로 인코딩됩니다. 16진수 체계는 기수 16 진법이라고도 하며, 숫자 0~9와 문자 a~f의 16개 고유 기호로 구성됩니다. Big endian 비트 순서는 첫 번째 비트가 가장 큰(최상위) 비트임을 의미합니다.
  - **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.

서비스 구성

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

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. 항목을 참조하십시오.

비고

- 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

비고

- 나열된 전제 조건이 충족되었는지 확인하십시오.
- 배터리 상태의 가시성을 향상시키려면 **Setup(설정)** > **Configure event and alarms logs(이**

벤트 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.

비고

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.

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. 을 참조하십시오.
- 연결된 외부 장치를 비롯하여 시스템이 올바르게 작동하는지 확인합니다.

– 카드를 긁고 리더, 도어 및 잠금장치를 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. 을 참조하십시오.

- 도어 컨트롤러가 예상한 대로 작동하지 않는 경우 이에 대한 자세한 내용은 및 항목을 참조하십시오.

이벤트 설정

시스템에서 발생하는 이벤트(예: 사용자가 카드를 밀거나 REX 장치가 활성화된 경우)는 이벤트 로그에 기록됩니다.

- 이벤트 로그를 봅니다. 을 참조하십시오.
- 이벤트 로그를 내보냅니다. 을 참조하십시오.
- 이벤트 로그를 구성합니다. 을 참조하십시오.

이벤트 로그 보기

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

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 를 참조하십시오.

관리자는 다른 이벤트보다 일부 이벤트에 더 관심이 있을 수 있습니다. 따라서 기록할 이벤트를 선택할 수 있습니다. 자세한 내용은 를 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.
- 날짜 및 시간 - 날짜 및 시간 범위로 이벤트 로그를 필터링합니다.

이벤트 로그 구성

이벤트 로그 구성 페이지에서 기록할 이벤트를 정의할 수 있습니다.

이벤트 로그 옵션

이벤트 로그에 포함될 이벤트를 정의하려면 **Setup > Configure Event Logs(설정 > 이벤트 로그 구성)**로 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)** - 이벤트 로깅을 활성화합니다. 이벤트가 등록되고 이벤트 로그에 포함됩니다.

액션 룰을 설정하는 방법

이벤트 페이지에서는 다양한 이벤트가 발생할 때 액션을 수행하도록 Axis 제품을 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 제품의 기본 도움말을 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.

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 항목을 참조하십시오.

수신자를 추가하려면 다음을 수행합니다.

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 수신자와의 연결을 테스트합니다.
6. **OK(확인)**를 클릭합니다.

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.

비고

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 지정)**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 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 스케불을 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
유휴[1]	꺼짐	빨간색	빨간색	무음	일반
RequirePIN	빨간색/녹색 깜박임	빨간색/녹색 깜박임	빨간색/녹색 깜박임	두 번의 짧은 알람음	핀 필요
AccessGrant-ed	녹색	녹색	녹색	신호음	접근 권한 부여됨
AccessDenied	빨간색	빨간색	빨간색	신호음	액세스 거부됨

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.

1. 도어가 닫히고 잠금장치가 잠기면 유휴 상태로 전환됩니다.

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.

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

비고

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(설정) > Additional Controller Configuration(추가 컨트롤러 구성) > System Options(시스템 옵션) > Security(보안) > IP Address Filter(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 (설정) > Additional Controller Configuration(추가 컨트롤러 구성) > System Options(시스템 옵션) > Security(보안) > Certificates(인증서)**로 이동합니다. 을 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. **Save(저장)**를 클릭하여 설정을 활성화합니다.

원하는 프로토콜을 통해 Axis 제품에 액세스하려면 브라우저 주소 필드에 HTTPS 프로토콜의 경우 `https://`를, HTTP 프로토콜의 경우 `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(확장 가능 인증 프로토콜)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. 적합한 소프트웨어

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

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

비고

인증이 제대로 작동하려면 Axis 제품의 날짜 및 시간이 NTP 서버와 동기화되어야 합니다. 을 참조하십시오.

인증서

인증서는 네트워크상의 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.

비고

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

네트워크

기본 TCP/IP 설정

Axis 제품은 IP 버전 4(IPv4)와 IP 버전 6(IPv6)을 지원합니다.

Axis 제품은 다음과 같은 방법으로 IP 주소를 가져올 수 있습니다.

- **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 항목을 참조하십시오.

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(설정) > Additional Controller Configuration(추가 컨트롤러 구성) > System Options(시스템 옵션) > Network(네트워크) > TCP IP > Basic(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(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.

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.

비고

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*를 참조하십시오.

AXIS Internet Dynamic DNS 서비스에 Axis 제품을 등록하려면 **Setup(설정) > Additional Controller Configuration(추가 컨트롤러 구성) > System Options(시스템 옵션) > Network(네트워크) > TCP/IP > Basic(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.

비고

AXIS Internet Dynamic DNS 서비스를 이용하려면 IPv4가 필요합니다.

고급 TCP/IP 설정

DNS 구성

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

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.

도메인 이름 - 도메인을 입력하여 Axis 제품에 사용되는 호스트 이름을 검색합니다. 도메인이 여러 개일 경우 세미콜론으로 구분할 수 있습니다. 호스트 이름은 항상 정규화된 도메인 이름(FQDN)의 첫 번째 부분입니다. 예를 들어, `myserver`는 정규화된 도메인 이름 `myserver.mycompany.com`의 호스트 이름이며, 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. **Setup(설정) > Additional Controller Configuration(추가 컨트롤러 구성) > System Options(시스템 옵션) > Network(네트워크) > TCP/IP > Advanced(고급)**에서 NTP 설정을 구성합니다.

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 일반적으로 할당된 DNS 이름과 동일합니다. **Setup(설정) > Additional Controller Configuration(추가 컨트롤러 구성) > System Options(시스템 옵션) > Network(네트워크) > TCP/IP > Advanced(고급)**에서 호스트 이름을 구성합니다.

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

HTTP

Setup(설정) > Additional Controller Configuration(추가 컨트롤러 구성) > System Options(시스템 옵션) > Network(네트워크) > TCP/IP > Advanced(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 을 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.

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

비고

- 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(설정) > Additional Controller Configuration(추가 컨트롤러 구성) > System Options(시스템 옵션) > Network(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.

비고

- 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 실행 중인 FTP 서버는 새로운 펌웨어, 사용자 애플리케이션 등을 업로드할 수 있도록 지원합니다. **Setup(설정) > Additional Controller Configuration(추가 컨트롤러 구성) > System Options(시스템 옵션) > Network(네트워크) > TCP/IP > Advanced(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.

비고

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

QoS(서비스 품질)

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(설정) > Additional Controller Configuration(추가 컨트롤러 구성) > System Options(시스템 옵션) > Network(네트워크) > SNMP** 페이지로 이동합니다.

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.

비고

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 스타트
- 웜 스타트
- 링크 업
- 인증 실패

SNMP v3는 암호화 및 보안 패스워드를 제공합니다. SNMP v3와 함께 트랩을 사용하려면 SNMP v3 관리 애플리케이션이 필요합니다.

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

비고

초기 패스워드는 한 번만 설정할 수 있습니다. 패스워드를 분실한 경우 Axis 제품을 공장 출하 시 기본값으로 재설정해야 합니다. 항목을 참조하십시오.

UPnP

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

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

포트 및 장치

I/O 포트

외부 장치 연결을 위해 보조 커넥터가 구성 가능한 입력 및 출력 포트 4개를 제공합니다.

외부 커넥터는 외부 장치 연결을 위해 구성 가능한 입력 및 출력 포트 2개를 제공합니다.

Setup > Additional Controller Configuration > System Options > Ports & Devices > I/O Ports (설정 > 추가 컨트롤러 구성 > 시스템 옵션 > 포트 및 장치 > I/O 포트)에서 I/O 포트를 구성할 수 있습니다. 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(설정) > Additional Controller Configuration(추가 컨트롤러 구성) > System Options(시스템 옵션) > Maintenance(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.

비고

재시작하면 서버 보고서의 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 항목을 참조하십시오.

펌웨어 업그레이드에 대한 자세한 내용은 항목을 참조하십시오.

지원(Support)

지원 개요

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

항목을 참고하십시오.

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(설정) > Additional Controller Configuration(추가 컨트롤러 구성) > System Options(시스템 옵션) > Support(지원) > Logs & Reports(로그 및 보고서) 페이지에서는 시스템을 분석하고 문제를 해결하는 데 유용한 로그 및 보고서를 생성합니다. Axis 지원 서비스에 연락할 경우 질의와 함께 서버 보고서를 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 보고서 보기 - 팝업 창에 제품 상태에 대한 정보를 제공합니다. 액세스 로그는 자동으로 서버 보고서에 포함됩니다.

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

고급 수준

스크립팅

스크립팅을 통해 숙련된 사용자가 자신의 스크립트를 사용자 지정하고 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 지정 스크립트로 인한 문제에 지원을 제공하지 않습니다.

스크립트 편집기를 열려면 **Setup(설정) > Additional Controller Configuration(추가 컨트롤러 구성) > System Options(시스템 옵션) > Advanced(고급) > Scripting(스크립팅)**으로 이동합니다. 스크립트로 인해 문제가 생기면 제품을 공장 출하 시 기본 설정으로 재설정하고 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 **Setup(설정) > Additional Controller Configuration(추가 컨트롤러 구성) > System Options(시스템 옵션) > Advanced(고급) > File Upload(파일 업로드)**로 이동합니다.

업로드한 파일은 `http://<ip address>/local/<user>/<file name>`를 통해 액세스할 수 있으며, 여기서 `<user>`는 업로드된 파일에 대해 선택된 사용자 그룹(관리자)입니다.

문제 해결

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. 을 참조하십시오.
3. 상태 LED 표시기가 다시 주황색으로 바뀔 때까지 25초 동안 제어 버튼을 누르고 있습니다.
4. 제어 버튼을 놓습니다. 상태 LED 표시등이 녹색으로 바뀌면 과정이 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(설정) > Additional Controller Configuration(추가 컨트롤러 구성) > Setup(설정) > System Options(시스템 옵션) > Maintenance(유지관리)**로 이동한 후 **Default(기본값)**를 클릭합니다.

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 지정 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.

비고

- 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.

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. **업그레이드**를 클릭합니다.
6. 제품을 업그레이드하고 다시 시작하는 동안 5분 가량 기다립니다. 그런 다음 웹 브라우저의 캐시를 지웁니다.
7. 제품에 액세스합니다.

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 길이가 408로 설정되어 있는지 확인합니다. 설명은 *axis.com*의 제품 페이지에 있는 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 (Command/DOS 창에서 `ping`과 제품의 IP 주소 입력): • `Reply from <IP address>: bytes=32; time=10...`을 수신하는 경우 이는 IP 주소가 이미 네트워크의 다른 장치에서 사용 중 일 수 있음을 의미합니다. 네트워크 관리자에게 새 IP 주소를 받아 제품을 다시 설치하십시오. • `Request timed out` 메시지를 수신하면, 해당 IP 주소를 Axis 제품에서 사용할 수 있다는 의미입니다. 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.

제품을 브라우저에서 액세스할 수 없음

로그인할 수 없음	HTTPS가 활성화된 경우 로그인을 시도할 때 올바른 프로토콜(HTTP 또는 HTTPS)이 사용되는지 확인하십시오. 브라우저의 주소 필드에 `http` 또는 `https`를 수동으로 입력해야 할 수도 있습니다. 사용자 root의 비밀번호를 분실한 경우에는 제품을 공장 기본 설정값으로 재설정해야 합니다. 을 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). 필요한 경우 고정 IP 주소를 수동으로 할당할 수 있습니다. 자세한 내용은 axis.com의 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. 을 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 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.

사양

UL 표시가 있는 텍스트는 UL 293 또는 UL 294 설치에만 유효합니다.

LED 표시

LED	색상	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 켜져 있습니다.
	빨간색	업그레이드 실패하면 느리게 깜박입니다.
전원	녹색	정상 작동 중입니다.
	주황색	펌웨어 업그레이드 중에는 녹색/주황색으로 깜박입니다.
릴레이 과전류	빨간색	회로가 단락되거나 과전류가 감지되면 켜집니다.
	켜져 있지 않음	정상 작동 중입니다.
리더 과전류	빨간색	회로가 단락되거나 과전류가 감지되면 켜집니다.
	켜져 있지 않음	정상 작동 중입니다.
릴레이	녹색	릴레이 활성화.[2]
	켜져 있지 않음	릴레이가 비활성화되었습니다.

비고

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

버튼

제어 버튼

제어 버튼의 용도는 다음과 같습니다.

- 제품을 공장 출하 시 기본 설정으로 재설정합니다. 을 참조하십시오.

커넥터

네트워크 커넥터

PoE+(Power over Ethernet Plus)를 지원하는 RJ45 이더넷 커넥터

2. *COM*이 *NO*에 연결되면 릴레이가 활성화됩니다.

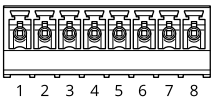
UL: PoE(Power over Ethernet)에 UL 294 등재 PoE(Power over Ethernet) IEEE 802.3af/802.3at Type 1 Class 3 또는 PoE+(Power over Ethernet Plus) IEEE 802.3at Type 2 Class 4 전력 제한 인젝터(44 ~ 57V DC, 15.4W/30W 제공)로 전원을 공급해야 합니다. PoE(Power over Ethernet)는 AXIS T8133 Midspan 30 W 1-port를 사용하여 UL에 의해 평가되었습니다.

리더 커넥터

리더와 통신하도록 RS485 및 Wiegand 프로토콜을 둘 다 지원하는 2개의 8핀 터미널 블록입니다.

지정된 전원 출력 값이 두 리더 포트에 공유됩니다. 즉, 도어 컨트롤러에 연결된 모든 리더에 12V DC에서 486mA가 예약됩니다.

제품의 웹 페이지에서 사용할 프로토콜을 선택합니다.



RS485용으로 구성

기능	핀	비고	사양
DC 접지(GND)	1		0V DC
DC 출력(+12V)	2	리더에 전원을 공급합니다.	12V DC, 최대 486mA가 두 리더에 대해 결합
RX/TX	3–4	전이중: RX. 반이중: RX/TX.	
TX	5–6	전이중: TX.	
구성 가능(입력 또는 출력)	7–8	디지털 입력 - 활성화하려면 핀 1에 연결하고 비활성화하려면 부동 상태(연결되지 않음)로 둡니다.	0 ~ 최대 30V DC
		디지털 출력 - 릴레이와 같은 유도 부하와 함께 사용할 경우 전압 과도 현상을 방지하도록 다이오드를 부하와 병렬로 연결해야 합니다.	0 ~ 최대 30V DC, 개방 드레인, 100mA

중요 사항

- 판독기에 컨트롤러에 의해 전원이 공급되는 경우, 적격 케이블 길이는 최대 200m(656피트)입니다.
- 컨트롤러가 리더에 전원을 공급하지 않는 경우, 케이블 요구 사항(차폐 포함, AWG24, 120옴 임피던스 적용 트위스트 페어 1개)이 충족되는 경우 리더 데이터에 대한 적격 케이블 길이는 최대 1000m(3280.8ft)입니다.

Wiegand용으로 구성

기능	핀	비고	사양
DC 접지(GND)	1		0V DC
DC 출력(+12V)	2	리더에 전원을 공급합니다.	12V DC, 최대 486mA가 두 리더에 대해 결합
D0	3		

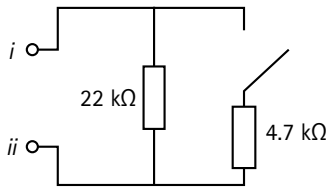
D1	4		
O	5–6	디지털 출력, 개방 드레인	
구성 가능(입력 또는 출력)	7–8	디지털 입력 - 활성화하려면 핀 1에 연결하고 비활성화하려면 부동 상태(연결되지 않음)로 둡니다.	0 ~ 최대 30V DC
		디지털 출력 - 릴레이와 같은 유도 부하와 함께 사용할 경우 전압 과도 현상을 방지하도록 다이오드를 부하와 병렬로 연결해야 합니다.	0 ~ 최대 30V DC, 개방 드레인, 100mA

중요 사항

- 판독기에 컨트롤러에 의해 전원이 공급되는 경우, 적격 케이블 길이는 최대 150m(500피트)입니다.
- 컨트롤러가 리더에 전원을 공급하지 않는 경우, 케이블 요구 사항(AWG22)이 충족되는 경우 리더 데이터에 대한 적격 케이블 길이는 최대 150m(500ft)입니다.

관리된 입력

관리된 입력을 사용하려면 아래의 다이어그램에 따라 EOL 레지스터를 설치하십시오.



i 입력

ii 0V DC(-)

UL: 관리된 입력을 UL에서 절도용으로 평가하지 않았습니다. 도어 모니터 및 REX에서만 EOL 레지스터를 통한 관리를 지원합니다.

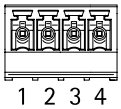
비고

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

도어 커넥터

도어 모니터링 장치용 2개의 4핀 터미널 블록입니다(디지털 입력).

도어 모니터는 EOL 레지스터를 통한 관리를 지원합니다. 연결이 중단되면 알람이 트리거됩니다. 관리된 입력을 사용하려면 EOL 레지스터를 설치하십시오. 관리된 입력에 대한 연결 다이어그램을 사용합니다. 을 참조하십시오.



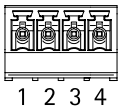
기능	핀	비고	사양
DC 접지	1, 3		0V DC
입력	2, 4	도어 모니터와 통신하는 데 사용됩니다. 디지털 입력 또는 관리된 입력 - 활성화하려면 각각 핀 1 또는 3에 연결하고 비활성화하려면 부동 상태(연결되지 않음)로 둡니다.	0 ~ 최대 30V DC

중요 사항

다음 케이블 요구 사항 AWG 24가 충족되는 경우 적격 케이블 길이는 최대 200m(656ft)입니다.

릴레이 커넥터

예를 들어 잠금장치 또는 게이트에 대한 인터페이스를 제어하는 데 사용할 수 있는 C형 릴레이를 위한 2개의 4핀 터미널 블록입니다.



기능	핀	비고	사양
DC 접지(GND)	1		0V DC
NO	2	정상 개방. 릴레이 장치 연결에 사용됩니다. NO와 DC 접지 사이에 페일 시큐어 잠금장치를 연결합니다. 점퍼를 사용하지 않더라도, 릴레이 핀 2개는 나머지 회로와 전기적으로 분리됩니다.	릴레이당 최대 전류 = 2A 최대 전압 = 30V DC
COM	3	공통	
NC	4	정상 폐쇄 릴레이 장치 연결에 사용됩니다. NC와 DC 접지 사이에 페일 세이프 잠금장치를 연결합니다. 점퍼를 사용하지 않더라도, 릴레이 핀 2개는 나머지 회로와 전기적으로 분리됩니다.	

릴레이 전원 점퍼

릴레이 전원 점퍼를 장착한 경우 12V DC 또는 24V DC를 릴레이 COM 핀에 연결합니다.

GND와 NO 핀 또는 GND와 NC 핀 사이에 잠금장치를 연결하는 데 사용할 수 있습니다.

전원	12V DC에서의 최대 전력[3]	24V DC에서의 최대 전력[3]
DC IN	1,600mA	800mA
PoE	800mA	400mA

통지

잠금장치가 극성이 없는 경우 외부 플라이백 다이오드를 추가하는 것이 좋습니다.

3. 전원은 2개의 릴레이와 AUX I/O 12V DC 간에 공유됩니다.

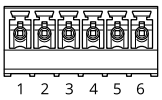
보조 커넥터

모션 디텍션, 이벤트 트리거, 알람 알림 등과 함께 외부 장치에 보조 커넥터를 사용합니다. 보조 커넥터는 0V DC 참조점 및 전원(DC 출력) 이외에 다음에 대한 인터페이스도 제공합니다.

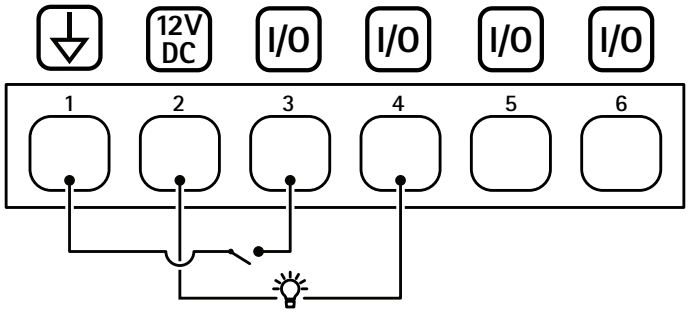
디지털 입력 - PIR 센서, 도어/윈도우 감지기, 유리 파손 감지기 등의 개방 회로와 폐쇄 회로 사이를 전환할 수 있는 장치를 연결하는 데 사용합니다.

디지털 출력 - 릴레이 및 LED와 같은 외부 장치 연결용. 연결된 장치는 VAPIX® Application Programming Interface 또는 제품 웹페이지에서 활성화할 수 있습니다.

6핀 단자대입니다.



기능	핀	비고	사양
DC 접지	1		0V DC
DC 출력	2	보조 장비에 전원을 공급할 때 사용 가능합니다. 참고: 이 핀은 정전된 경우에만 사용할 수 있습니다.	12 V DC 각 I/O의 최대 부하 = 50mA
구성 가능(입력 또는 출력)	3–6	디지털 입력 - 활성화하려면 핀 1에 연결하고 비활성화하려면 부동 상태(연결되지 않음)로 둡니다.	0 ~ 최대 30V DC
		디지털 출력 - 활성화된 경우 핀 1에 연결되며(DC 접지) 비활성화된 경우 부동 상태(연결되지 않음)입니다. 릴레이와 같은 유도 부하와 함께 사용할 경우 전압 과도 현상을 방지하도록 다이오드를 부하와 병렬로 연결해야 합니다. 내부 12V DC 출력(핀 2)이 사용될 경우 각 I/O는 12V DC, 50mA(최대) 외부 부하를 유도합니다. 외부 전원 공급 장치와 함께 개방 드레인 연결을 사용하는 경우 I/O가 DC 공급 0 ~ 30V DC, 100mA를 관리할 수 있습니다.	0 ~ 최대 30V DC, 개방 드레인, 100mA

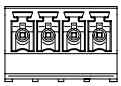


1 DC 접지
2 DC 출력 12V
3 I/O가 입력으로 구성됨
4 I/O가 출력으로 구성됨
5 구성 가능한 I/O
6 구성 가능한 I/O

외부 커넥터

유리 파손 감지기 또는 화재 감지기와 같은 외부 장치용 4핀 블록 터미널

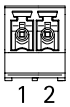
UL: 절도범/화재 알람용 UL에 의해 커넥터가 평가되지 않았습니다.



기능	핀	비고	사양
DC 접지	1, 3		0V DC
구성 가능(입력 또는 출력)	2, 4	디지털 입력 – 활성화하려면 핀 1 또는 3에 연결하고 비활성화하려면 부동 상태(연결되지 않음)로 둡니다.	0 ~ 최대 30V DC
		디지털 출력 - 활성화하려면 핀 1 또는 3에 연결하고 비활성화하려면 부동 상태(연결되지 않음)로 둡니다. 릴레이와 같은 유도 부하와 함께 사용할 경우 전압 과도 현상을 방지하도록 다이오드를 부하와 병렬로 연결해야 합니다.	0 ~ 최대 30V DC, 개방 드레인, 100mA

전원 커넥터

DC 전원 입력용 2핀 단자대입니다. 정격 출력 전력이 ≤100W로 제한되거나 정격 출력 전류가 ≤5A로 제한되는 SELV(Safety Extra Low Voltage) 준수 LPS(제한된 전원)를 사용하십시오.



기능	핀	비고	사양
0V DC(-)	1		0V DC
DC 입력	2	PoE(Power over Ethernet) 미사용 시 컨트롤러에 전원을 공급하는 데 사용됩니다. 참고: 이 핀은 전원이 공급된 경우에만 사용할 수 있습니다.	10.5 ~ 28V DC, 최대 36W

UL: 적용 분야에 따라 UL 294, UL 293 또는 UL 603 등재 전원 공급 장치에 적절한 정격의 DC 전원이 공급됩니다.

백업 배터리 입력 커넥터

충전기가 내장된 배터리를 사용하는 백업 솔루션에 사용됩니다. 12V DC 입력.

UL: UL에 의해 커넥터가 평가되지 않았습니다.

중요 사항

배터리 입력을 사용할 때는 외부 3A 저속 블로어 퓨즈를 직렬로 연결해야 합니다.

기능	핀	비고	사양
0V DC(-)	1		0V DC
배터리 입력	2	다른 전원을 사용할 수 없을 때 도어 컨트롤러에 전원을 공급합니다. 참고: 이 핀은 배터리 전원이 공급되는 경우에만 사용할 수 있습니다. UPS 연결 전용.	11 ~ 13.7V DC, 최대 36W

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.

비고
제품을 최대한으로 활용하는 데 도움이 되는 유용한 정보를 나타냅니다.

웹 인터페이스

장치의 웹 인터페이스에 접근하려면 웹 브라우저에 장치의 IP 주소를 입력하십시오.

비고

이 섹션은 AXIS Camera Station Secure Entry 펌웨어가 있는AXIS A1601 Network Door Controller에만 유효합니다.

기본 메뉴를 표시하거나 숨깁니다.

릴리스 정보에 액세스합니다.

제품 도움말에 액세스합니다.

언어를 변경합니다.

밝은 테마 또는 어두운 테마를 설정합니다.

사용자 메뉴에는 다음이 포함됩니다.

- 로그인한 사용자에 대한 정보.
- **Change account(계정 변경)**: 현재 계정에서 로그아웃하고 새 계정에 로그인합니다.
- **Log out(로그아웃)**: 현재 계정에서 로그아웃합니다.

상황에 맞는 메뉴에는 다음이 포함됩니다.

- **분석 데이터**: 개인용이 아닌 브라우저 데이터를 공유하려면 수락하십시오.
- **Feedback(피드백)**: 사용자 경험을 개선하는 데 도움이 되는 피드백을 공유하십시오.
- **Legal(법률)**: 쿠키 및 라이센스에 대한 정보를 봅니다.
- **About(정보)**: AXIS OS 버전 및 일련 번호를 포함한 장치 정보를 봅니다.

상태

시간 동기화 상태

장치가 NTP 서버와 동기화되었는지 여부 및 다음 동기화까지 남은 시간을 포함하여 NTP 동기화 정보를 표시합니다.

NTP settings(NTP 설정): NTP 설정을 보고 업데이트합니다. NTP 설정을 변경할 수 있는 **Time and location(시간 및 위치)** 페이지로 이동합니다.

장치 정보

AXIS OS 버전 및 일련 번호를 포함한 장치 정보를 표시합니다.

Upgrade AXIS OS(AXIS OS 업그레이드): 장치의 소프트웨어를 업그레이드합니다. 업그레이드를 수행할 수 있는 유지보수 페이지로 이동합니다.

장치

알람

Device motion(장치 모션): 장치의 움직임이 감지될 때 시스템에서 알람을 트리거하려면 켭니다.

Casing open(케이스 열림) : 도어 컨트롤러의 케이스 열림을 감지하면 시스템에서 알람을 트리거하기 위해 켜십시오. barebone 도어 컨트롤러에 대해 이 설정을 끕니다.

External tamper(외부 변조) : 외부 변조가 감지될 때 시스템에서 알람을 트리거하려면 켭니다. 예를 들어 누군가 외부 캐비닛을 열거나 닫을 때가 해당됩니다.

- **Supervised input(관리형 입력)** : 입력 상태를 모니터링하고 EOL 저항기를 구성하려면 켭니다.
  - 병렬 우선 연결을 사용하려면 **Parallel first connection with a 22 KΩ parallel resistor and a 4.7 KΩ serial resistor(22KΩ 병렬 저항 및 4.7KΩ 직렬 저항으로 병렬 우선 연결)**를 선택합니다.
  - 직렬 우선 연결을 사용하려면 **Serial first connection(직렬 우선 연결)**을 선택하고 **Resistor values(저항 값)** 드롭다운 목록에서 저항 값을 선택합니다.

주변장치

리더

Add reader(리더 추가): 리더를 추가하려면 클릭합니다.

AXIS A4612: 컨트롤러에 최대 16개의 블루투스 리더를 라이센스 없이 추가할 수 있습니다.
- **이름**: 리더 이름을 입력합니다.
- **리더**: 드롭다운 목록에서 리더를 선택합니다.
- **IP 주소**: 리더의 IP 주소를 직접 입력합니다.
- **Username(사용자 이름)**: 리더의 사용자 이름을 입력합니다.
- **패스워드**: 리더의 패스워드를 입력합니다.
- **Ignore server certificate verification(서버 인증서 확인 무시)**: 인증을 무시하려면 켭니다.
- **I/O ports and relays(I/O 포트 및 릴레이)**: I/O 포트 및 릴레이를 구성하려면 확장합니다.
  - **Port(포트)**: 포트의 이름을 표시합니다.
  - **방향**: 입력 포트 또는 출력 포트임을 나타냅니다.
  - **Normal state(정상 상태)**: 개회로의 경우  을 클릭하고 폐회로의 경우  을 클릭합니다.

AXIS License Plate Verifier(AXIS Camera Station에서 재구성 필요)
- **이름**: 리더 이름을 입력합니다.
- **API-key(API 키)**: API 키를 입력합니다.
- **Generate(생성)**: API 키를 생성하려면 클릭합니다.
- **Copy API-key(API 키 복사)**: API 키를 안전한 곳에 저장하려면 클릭하여 복사합니다.

AXIS Barcode Reader(AXIS Camera Station에서 재구성 필요)
- **이름**: 리더 이름을 입력합니다.
- **API-key(API 키)**: API 키를 입력합니다.
- **Generate(생성)**: API 키를 생성하려면 클릭합니다.
- **Copy API-key(API 키 복사)**: API 키를 안전한 곳에 저장하려면 클릭하여 복사합니다.

Axis 인터콤 리더(AXIS Camera Station에서 재구성 필요)
- **이름**: 리더 이름을 입력합니다.
- **리더**: 드롭다운 목록에서 리더를 선택합니다.
- **IP 주소**: 리더의 IP 주소를 직접 입력합니다.
- **Username(사용자 이름)**: 리더의 사용자 이름을 입력합니다.
- **패스워드**: 리더의 패스워드를 입력합니다.
- **Ignore server certificate verification(서버 인증서 확인 무시)**: 인증을 무시하려면 켭니다.

Edit(편집): 리더를 선택한 후 **Edit(편집)**를 클릭하여 선택한 리더를 변경합니다.

삭제: 리더들을 선택한 후 **Delete(삭제)**를 클릭하여 선택한 리더를 삭제합니다.

무선 잠금장치

AH30 Communication Hub를 사용하여 최대 16개의 ASSA ABLOY Aperio 무선 잠금장치를 연결할 수 있습니다. 무선 잠금장치를 사용하려면 라이센스가 필요합니다.

비고

AH30 Communication Hub를 보안 측에 설치해야 합니다.

Connect communication hub(통신 허브 연결): 무선 잠금을 연결하려면 클릭합니다.

업그레이드

리더 업그레이드: 리더의 소프트웨어를 업그레이드하려면 클릭합니다. 지원되는 리더가 온라인 상태일 때만 업그레이드할 수 있습니다.

Upgrade converters(컨버터 업그레이드): 컨버터의 소프트웨어를 업그레이드하려면 클릭합니다. 지원되는 컨버터가 온라인 상태일 때만 업그레이드할 수 있습니다.

시스템

시간과 장소

날짜 및 시간

시간 형식은 웹 브라우저의 언어 설정에 따라 다릅니다.

비고

장치의 날짜와 시간을 NTP 서버와 동기화하는 것이 좋습니다.

Synchronization(동기화): 장치의 날짜 및 시간 동기화 옵션을 선택합니다.

- **Automatic date and time (PTP)(자동 날짜 및 시간(PTP))**: 정밀 시간 프로토콜을 사용하여 동기화합니다.
- **Automatic date and time (manual NTS KE servers)(자동 날짜 및 시간(수동 NTS KE 서버))**: DHCP 서버에 연결된 보안 NTP 키 설정 서버와 동기화합니다.
  - **수동 NTS KE 서버**: 하나 또는 두 개의 NTP 서버의 IP 주소를 입력합니다. 두 개의 NTP 서버를 사용하는 경우 장치는 두 서버에 입력된 내용을 기반으로 시간을 동기화하고 조정합니다.
  - **Trusted NTS KE CA certificates(신뢰할 수 있는 NTS KE CA 인증서)**: 보안 NTS KE 시간 동기화에 사용할 신뢰할 수 있는 CA 인증서를 선택하거나 선택하지 않은 상태로 둡니다.
  - **Max NTP poll time(최대 NTP 폴링 시간)**: 업데이트된 시간을 얻기 위해 NTP 서버를 폴링할 때까지 장치가 기다려야 하는 최대 시간을 선택합니다.
  - **Min NTP poll time(최소 NTP 폴링 시간)**: 업데이트된 시간을 얻기 위해 NTP 서버를 폴링할 때까지 장치가 기다려야 하는 최소 시간을 선택합니다.
- **Automatic date and time (NTP server using DHCP)(자동 날짜 및 시간(DHCP를 사용하는 NTP 서버))**: DHCP 서버에 연결된 NTP 서버와 동기화합니다.
  - **Fallback NTP servers(대체 NTP 서버)**: 하나 또는 두 개의 대체 서버의 IP 주소를 입력합니다.
  - **Max NTP poll time(최대 NTP 폴링 시간)**: 업데이트된 시간을 얻기 위해 NTP 서버를 폴링할 때까지 장치가 기다려야 하는 최대 시간을 선택합니다.
  - **Min NTP poll time(최소 NTP 폴링 시간)**: 업데이트된 시간을 얻기 위해 NTP 서버를 폴링할 때까지 장치가 기다려야 하는 최소 시간을 선택합니다.
- **Automatic date and time (manual NTP server)(자동 날짜 및 시간(수동 NTP 서버))**: 선택한 NTP 서버와 동기화합니다.
  - **수동 NTP 서버**: 하나 또는 두 개의 NTP 서버의 IP 주소를 입력합니다. 두 개의 NTP 서버를 사용하는 경우 장치는 두 서버에 입력된 내용을 기반으로 시간을 동기화하고 조정합니다.
  - **Max NTP poll time(최대 NTP 폴링 시간)**: 업데이트된 시간을 얻기 위해 NTP 서버를 폴링할 때까지 장치가 기다려야 하는 최대 시간을 선택합니다.
  - **Min NTP poll time(최소 NTP 폴링 시간)**: 업데이트된 시간을 얻기 위해 NTP 서버를 폴링할 때까지 장치가 기다려야 하는 최소 시간을 선택합니다.
- **Custom date and time(사용자 지정 날짜 및 시간)**: 수동으로 날짜 및 시간을 설정합니다. **Get from system(시스템에서 가져오기)**을 클릭하여 컴퓨터 또는 모바일 장치에서 날짜 및 시간 설정을 한 차례 가져옵니다.

시간대: 사용할 시간대를 선택합니다. 일광 절약 시간 및 표준 시간에 맞춰 시간이 자동으로 조정됩니다.

- **DHCP**: DHCP 서버의 시간대를 채택합니다. 이 옵션을 선택하려면 먼저 장치가 DHCP 서버에 연결되어 있어야 합니다.
- **Manual(수동)**: 드롭다운 목록에서 시간대를 선택합니다.

비고

시스템에서는 모든 녹화, 로그 및 시스템 설정에 날짜 및 시간 설정이 사용됩니다.

네트워크

IPv4

Assign IPv4 automatically(IPv4 자동 할당): 수동 구성 없이 네트워크에서 IP 주소, 서브넷 마스크, 라우터를 자동으로 할당하도록 하려면 IPv4 자동 IP(DHCP)를 선택합니다. 대부분의 네트워크에서는 자동 IP 할당(DHCP)을 사용하는 것이 좋습니다.

IP 주소: 장치의 고유한 IP 주소를 입력하십시오. 고정 IP 주소는 각 주소가 고유한 경우 격리된 네트워크 내에서 무작위로 할당될 수 있습니다. 충돌을 방지하려면 고정 IP 주소를 할당하기 전에 네트워크 관리자에게 문의하는 것이 좋습니다.

서브넷 마스크: 서브넷 마스크를 입력하여 LAN(Local Area Network) 내부에 있는 주소를 정의합니다. LAN 외부의 모든 주소는 라우터를 통과합니다.

Router(라우터): 다른 네트워크 및 네트워크 세그먼트에 연결된 장치를 연결하는 데 사용되는 기본 라우터(게이트웨이)의 IP 주소를 입력합니다.

Fallback to static IP address if DHCP isn't available(DHCP를 사용할 수 없는 경우 고정 IP 주소로 폴백): DHCP를 사용할 수 없고 IP 주소를 자동으로 할당할 수 없는 경우 대체로 사용할 고정 IP 주소를 추가하려면 선택합니다.

비고

DHCP를 사용할 수 없고 장치가 고정 주소 대체를 사용하는 경우, 고정 주소는 제한된 범위로 구성됩니다.

IPv6

Assign IPv6 automatically(IPv6 자동 할당): IPv6을 켜고 네트워크 라우터가 장치에 IP 주소를 자동으로 할당하도록 하려면 선택합니다.

호스트 이름

호스트 이름을 자동으로 할당: 네트워크 라우터가 장치에 호스트 이름을 IP 주소를 자동으로 할당하도록 하려면 선택합니다.

호스트 이름: 장치에 액세스하는 다른 방법으로 사용하려면 호스트 이름을 수동으로 입력합니다. 서버 보고서 및 시스템 로그는 호스트 이름을 사용합니다. 허용되는 문자는 A~Z, a~z, 0~9, -입니다.

동적 DNS 업데이트 활성화: IP 주소가 변경될 때마다 장치에서 도메인 네임 서버 녹화를 자동으로 업데이트하도록 허용합니다.

DNS 이름 등록: 장치의 IP 주소를 가리키는 고유한 도메인 이름을 입력합니다. 허용되는 문자는 A~Z, a~z, 0~9, -입니다.

TTL: TTL(Time to Live)은 DNS 레코드가 업데이트되어야 할 때까지 유효하게 유지되는 기간을 설정합니다.

DNS 서버

Assign DNS automatically(DNA 자동 할당): DHCP 서버가 검색 도메인 및 DNS 서버 주소를 장치에 자동으로 할당하게 하려면 선택합니다. 대부분의 네트워크에 대해 자동 DNS(DHCP)를 권장합니다.

Search domains(도메인 검색): 정규화되지 않은 호스트 이름을 사용하는 경우 **Add search domain(검색 도메인 추가)**을 클릭하고 장치가 사용하는 호스트 이름을 검색할 도메인을 입력합니다.

DNS servers(DNS 서버): **Add DNS server(DNS 서버 추가)**를 클릭하고 DNS 서버의 IP 주소를 입력합니다. 이 서버는 네트워크에서 호스트 이름을 IP 주소로 변환하여 제공합니다.

비고

DHCP를 비활성화하면 호스트 이름, DNS 서버, NTP 등 자동 네트워크 구성에 의존하는 기능이 작동하지 않을 수 있습니다.

HTTP 및 HTTPS

HTTPS는 사용자의 페이지 요청 및 웹 서버에서 반환된 페이지에 대한 암호화를 제공하는 프로토콜입니다. 암호화된 정보 교환은 서버의 신뢰성을 보장하는 HTTPS 인증서를 사용하여 관리됩니다.

장치에서 HTTPS를 사용하려면 HTTPS 인증서를 설치해야 합니다. 인증서를 생성하고 설치하려면 **System > Security(시스템 > 보안)**로 이동합니다.

Allow access through(액세스 허용): 사용자가 **HTTP**, **HTTPS** 또는 **HTTP and HTTPS(HTTP 및 HTTPS)** 프로토콜 둘 다를 통해 장치에 연결하도록 허용할지 선택합니다.

비고

HTTPS를 통해 암호화된 웹 페이지를 보는 경우 특히 페이지를 처음 요청할 때 성능이 저하될 수 있습니다.

HTTP port(HTTP 포트): 사용할 HTTP 포트를 입력합니다. 장치는 포트 80 또는 1024-65535 범위의 모든 포트를 허용합니다. 관리자로 로그인한 경우 1-1023 범위의 포트를 입력할 수도 있습니다. 이 범위의 포트를 사용하면 경고가 표시됩니다.

HTTPS port(HTTPS 포트): 사용할 HTTPS 포트를 입력합니다. 장치는 포트 443 또는 1024-65535 범위의 모든 포트를 허용합니다. 관리자로 로그인한 경우 1-1023 범위의 포트를 입력할 수도 있습니다. 이 범위의 포트를 사용하면 경고가 표시됩니다.

Certificate(인증서): 장치에 HTTPS를 활성화하려면 인증서를 선택합니다.

네트워크 검색 프로토콜

Bonjour®: 네트워크에서 자동 검색을 허용하려면 이 옵션을 켭니다.

Bonjour 이름: 네트워크에 표시할 이름을 입력합니다. 기본 이름은 장치 이름과 MAC 주소입니다.

UPnP®: 네트워크에서 자동 검색을 허용하려면 이 옵션을 켭니다.

UPnP 이름: 네트워크에 표시할 이름을 입력합니다. 기본 이름은 장치 이름과 MAC 주소입니다.

WS-검색: 네트워크에서 자동 검색을 허용하려면 이 옵션을 켭니다.

LLDP 및 CDP: 네트워크에서 자동 검색을 허용하려면 이 옵션을 켭니다. LLDP 및 CDP를 끄면 PoE 전원 협상에 지장이 생길 수 있습니다. PoE 전원 협상과 관련한 문제를 해결하려면 하드웨어 PoE 전원 협상 전용으로 PoE 스위치를 구성합니다.

One-Click Cloud Connection

One-click cloud connection(O3C)과 O3C 서비스는 어느 위치에서나 실시간 및 녹화 영상에 쉽고 안전한 인터넷 액세스를 제공합니다. 자세한 내용은 *axis.com/end-to-end-solutions/hosted-services*를 참조하십시오.

Allow O3C(O3C 허용):

- **One-click(원클릭)**: 기본 옵션입니다. O3C에 연결하려면 장치의 제어 버튼을 누릅니다. 장치 모델에 따라 상태 LED가 깜박일 때까지 버튼을 눌렀다 놓거나, 길게 누릅니다. **Always(항상)**를 활성화하고 연결 상태를 유지하려면 24시간 이내에 장치를 O3C 서비스에 등록합니다. 등록하지 않으면 장치의 O3C 연결이 끊어집니다.
- **항상**: 장치가 인터넷을 통해 O3C 서비스에 대한 연결을 지속적으로 시도합니다. 장치를 등록하면 연결 상태가 유지됩니다. 제어 버튼에 손이 닿지 않는 경우 이 옵션을 사용하십시오.
- **No(아니요)**: O3C 서비스를 연결 해제합니다.

Proxy settings (프록시 설정): 필요한 경우 프록시 설정을 입력하여 프록시 서버에 연결합니다.

호스트: 프록시 서버의 주소를 입력합니다.

Port(포트): 액세스에 사용되는 포트 번호를 입력하십시오.

로그인 및 **패스워드**: 필요한 경우 프록시 서버에 대한 사용자 이름 및 패스워드를 입력합니다.

Authentication method(인증 방법):

- **기본**: 이 방법은 HTTP에 대해 가장 호환성이 뛰어난 인증 체계입니다. 암호화되지 않은 사용자 이름과 패스워드를 서버로 전송하기 때문에 **Digest(다이제스트)** 방법보다 안전하지 않습니다.
- **다이제스트**: 이 방법은 항상 네트워크를 통해 암호화된 패스워드를 전송하기 때문에 더 안전합니다.
- **자동**: 이 옵션을 사용하면 지원되는 방법에 따라 장치가 인증 방법을 선택할 수 있습니다. 우선순위는 **다이제스트** 방법, **기본** 방법 순서로 설정합니다.

소유자 인증 키(OAK): 소유자 인증 키를 가져오려면 **Get key(키 가져 오기)**를 클릭합니다. 이것은 장치가 방화벽이나 프록시없이 인터넷에 연결된 경우에만 가능합니다.

SNMP

SNMP(Simple Network Management Protocol)를 이용하여 네트워크 장치를 원격으로 관리할 수 있습니다.

SNMP: 사용할 SNMP 버전을 선택합니다.

- **v1 및 v2c**:
  - **Read community(읽기 커뮤니티)**: 지원되는 모든 SNMP 객체에 대해 읽기 전용 권한이 있는 커뮤니티 이름을 입력합니다. 기본값은 **공개**입니다.
  - **Write community(쓰기 커뮤니티)**: 지원되는 모든 SNMP 객체에 대해 읽기 또는 쓰기 권한이 있는 커뮤니티 이름을 입력합니다(읽기 전용 객체 제외). 기본값은 **쓰기**입니다.
  - **Activate traps(트랩 활성화)**: 트랩보고를 활성화하려면 켜십시오. 장치는 트랩을 사용하여 중요한 이벤트 또는 상태 변경에 대한 메시지를 관리 시스템에 보냅니다. 웹 인터페이스에서 SNMP v1 및 v2c에 대한 트랩을 설정할 수 있습니다. SNMP v3으로 변경하거나 SNMP를 끄면 트랩이 자동으로 꺼집니다. SNMP v3를 사용하는 경우 SNMP v3 관리 애플리케이션을 통해 트랩을 설정할 수 있습니다.
  - **Trap address(트랩 주소)**: 관리 서버의 IP 주소 또는 호스트 이름을 입력하십시오.
  - **Trap community(트랩 커뮤니티)**: 장치가 관리 시스템에 트랩 메시지를 보낼 때 사용할 커뮤니티를 입력합니다.
  - **Traps(트랩)**:
    - **Cold start(콜드 부팅)**: 장치가 시작될 때 트랩 메시지를 보냅니다.
    - **Link up(링크 업)**: 링크가 다운에서 업으로 변경된 경우 트랩 메시지를 보냅니다.
    - **Link down(링크 다운)**: 링크가 업에서 다운으로 변경된 경우 트랩 메시지를 보냅니다.
    - **Authentication failed(인증 실패)**: 인증 시도가 실패하면 트랩 메시지를 보냅니다.

비고

SNMP v1 및 v2c 트랩을 켜면 모든 Axis 비디오 MIB 트랩이 활성화됩니다. 자세한 내용은 *AXIS OS Portal> SNMP*를 참조하세요.

- **v3**: SNMP v3는 암호화 및 보안 암호를 제공하는 보다 안전한 버전입니다. SNMP v3를 사용하려면 암호가 HTTPS를 통해 전송되므로 HTTPS를 활성화하는 것이 좋습니다. 또한 권한이 없는 당사자가 암호화되지 않은 SNMP v1 및 v2c 트랩에 액세스하는 것을 방지합니다. SNMP v3를 사용하는 경우 SNMP v3 관리 애플리케이션을 통해 트랩을 설정할 수 있습니다.
  - **Password for the account "initial"('초기' 계정의 패스워드)**: 이름이 'initial'인 계정의 SNMP 패스워드를 입력합니다. HTTPS를 활성화하지 않고도 패스워드를 전송할 수 있지만 권장하지 않습니다. SNMP v3 패스워드는 한 번만 설정할 수 있고 HTTPS가 활성화된 경우에만 설정하는 것이 좋습니다. 패스워드를 설정하면 패스워드 필드가 더 이상 표시되지 않습니다. 패스워드를 다시 설정하려면 장치를 공장 기본 설정으로 재설정해야 합니다.

연결된 클라이언트

연결 및 연결된 클라이언트 수를 표시합니다.

View details(세부 사항 보기): 연결된 클라이언트 목록을 보고 업데이트합니다. 목록에는 각 연결의 IP 주소, 프로토콜, 포트, 상태 및 PID/프로세스가 표시됩니다.

보안

인증서

인증서는 네트워크상의 장치를 인증하는 데 사용됩니다. 이 장치는 두 가지 유형의 인증서를 지원합니다.

- **Client/server certificates(클라이언트/서버 인증서)**
  클라이언트/서버 인증서는 장치의 ID를 검증하며 자체 서명할 수 있으며 CA(인증 기관)에서 발급할 수 있습니다. 자체 서명 인증서는 제한된 보호를 제공하며 CA 발행 인증서를 얻기 전까지 사용할 수 있습니다.
- **CA 인증서**
  CA 인증서를 사용하여 피어 인증서를 인증합니다. 예를 들어, 장치가 IEEE 802.1X로 보호되는 네트워크에 연결된 경우 인증 서버의 ID를 검증합니다. 장치에는 여러 개의 사전 설치된 CA 인증서가 있습니다.

지원되는 형식은 다음과 같습니다.

- 인증서 형식: .PEM, .CER, .PFX
- 개인 키 형식: PKCS#1 및 PKCS#12

중요 사항

장치를 공장 출하 시 기본값으로 재설정하면 모든 인증서가 삭제됩니다. 사전 설치된 CA 인증서가 다시 설치됩니다.

Add certificate(인증서 추가) : 인증서를 추가하려면 클릭합니다. 단계별 가이드가 열립니다.

- **More(더 보기)** : 작성하거나 선택할 추가 필드를 표시합니다.
- **Secure keystore(보안 키 저장소)**: 개인 키를 안전하게 저장하려면 **Trusted Execution Environment (SoC TEE)**, **Secure element(보안 요소)** 또는 **Trusted Platform Module 2.0** 을 선택합니다. 선택할 보안 키 저장소에 대한 자세한 내용을 보려면 *help.axis.com/axis-os#cryptographic-support*를 참조하십시오.
- **Key type(키 유형)**: 인증서를 보호하려면 드롭다운 목록에서 기본 암호화 알고리즘이나 다른 암호화 알고리즘을 선택합니다.

상황에 맞는 메뉴에는 다음이 포함됩니다.

- **Certificate information(인증서 정보)**: 설치된 인증서의 속성을 봅니다.
- **Delete certificate(인증서 삭제)**: 인증서를 삭제하십시오.
- **Create certificate signing request(인증서 서명 요청 생성)**: 디지털 ID 인증서를 신청하기 위해 등록 기관에 보낼 인증서 서명 요청을 생성합니다.

Secure keystore(보안 키 저장소):

- **Trusted Execution Environment (SoC TEE)**: 보안 키 저장소로 SoC TEE를 사용하려면 선택합니다.
- **Secure element(보안 요소)(CC EAL6+, FIPS 140-3 Level 3)**: 보안 키 저장소에 보안 요소를 사용하려면 선택합니다.
- **Trusted Platform Module 2.0(CC EAL4+, FIPS 140-2 레벨 2)**: 보안 키 저장소에 TPM 2.0을 사용하려면 선택합니다.

네트워크 접근 제어 및 암호화

IEEE 802.1x

IEEE 802.1x는 유선 및 무선 네트워크 장치의 보안 인증을 제공하는 포트 기반 네트워크 승인 제어를 위한 IEEE 표준입니다. IEEE 802.1x는 EAP(Extensible Authentication Protocol)를 기준으로 합니다.

IEEE 802.1X로 보호되는 네트워크에 액세스하려면 네트워크 장치가 자체적으로 인증되어야 합니다. 인증은 인증 서버에서 수행되며, 일반적으로 RADIUS 서버(예: FreeRADIUS 및 Microsoft Internet Authentication Server)입니다.

IEEE 802.1AE MACsec

IEEE 802.1AE MACsec은 미디어 액세스 독립 프로토콜을 위한 비연결형 데이터 기밀성 및 무결성을 정의하는 IEEE의 MAC(미디어 액세스 컨트롤) 보안 표준입니다.

인증서

CA 인증서 없이 구성하면 서버 인증서 유효성 검사가 비활성화되고 장치는 연결된 네트워크에 관계없이 자체 인증을 시도합니다.

인증서를 사용할 때 Axis 구현 시 기기 및 인증 서버는 EAP-TLS(확장 가능 인증 프로토콜 - 전송 계층 보안)를 사용하여 디지털 인증서로 자체적으로 인증합니다.

장치가 인증서를 통해 보호되는 네트워크에 액세스할 수 있도록 하려면 서명된 클라이언트 인증서를 장치에 설치해야 합니다.

Authentication method(인증 방법): 인증에 사용되는 EAP 유형을 선택합니다.

Client Certificate(클라이언트 인증서): IEEE 802.1x를 사용할 클라이언트 인증서를 선택합니다. 인증 서버는 인증서를 사용하여 클라이언트의 ID를 확인합니다.

CA 인증서: CA 인증서를 선택하여 인증 서버의 ID를 확인합니다. 인증서를 선택하지 않으면 장치는 연결된 네트워크에 관계없이 자체 인증을 시도합니다.

EAP identity(EAP ID): 클라이언트 인증서와 연관된 사용자 ID를 입력하십시오.

EAPOL version(EAPOL 버전): 네트워크 스위치에서 사용되는 EAPOL 버전을 선택합니다.

Use IEEE 802.1x(IEEE 802.1x 사용): IEEE 802.1x 프로토콜을 사용하려면 선택합니다.

인증 방법으로 **IEEE 802.1x PEAP-MSCHAPv2**를 사용하는 경우에만 이러한 설정을 이용할 수 있습니다.

- **패스워드**: 해당 사용자 ID의 패스워드를 입력합니다.
- **Peap version(Peap 버전)**: 네트워크 스위치에서 사용되는 Peap 버전을 선택합니다.
- **Label(라벨)**: 클라이언트 EAP 암호화를 사용하려면 1을 선택하고, 클라이언트 PEAP 암호화를 사용하려면 2를 선택합니다. Peap 버전 1을 사용하는 경우 네트워크 스위치가 사용하는 라벨을 선택합니다.

IEEE 802.1ae MACsec(정적 CAK/사전 공유 키)를 인증 방법으로 사용하는 경우에만 이러한 설정을 이용할 수 있습니다.

- **키 일치 연결 관련 키 이름**: 연결 관련 이름(CKN)을 입력합니다. 2 ~ 64자(2로 분할 가능) 16진수여야 합니다. CKN은 연결 관련에서 수동으로 구성해야 하며, 처음에 MACsec을 활성화하려면 링크의 양쪽 끝에서 일치해야 합니다.
- **키 일치 연결 관련 키**: 연결 관련 키(CAK)를 입력합니다. 32자 또는 64자의 16진수여야 합니다. CAK는 연결 관련에서 수동으로 구성해야 하며, 처음에 MACsec을 활성화하려면 링크의 양쪽 끝에서 일치해야 합니다.

무차별 대입 공격 방지

Blocking(차단 중): 무차별 대입 공격을 차단하려면 켜십시오. 무차별 대입 공격은 시행 착오를 통해 로그인 정보 또는 암호화 키를 추측합니다.

차단 기간: 무차별 대입 공격을 차단할 시간(초)을 입력합니다.

차단 조건: 블록이 시작되기 전에 허용되는 초당 인증 실패 횟수를 입력합니다. 페이지 수준과 장치 수준 모두에서 허용되는 실패 수를 설정할 수 있습니다.

방화벽

Firewall(방화벽): 방화벽을 활성화하려면 켭니다.

Default Policy(기본 정책): 룰에서 다루지 않는 연결 요청을 방화벽이 어떻게 처리할지 선택합니다.

- **ACCEPT(수락):** 장치에 대한 모든 연결을 허용합니다. 이 옵션은 기본 설정되어 있습니다.
- **DROP(거부):** 장치에 대한 모든 연결을 차단합니다.

기본 정책에 예외를 적용하려면 특정 주소, 프로토콜 및 포트에서 장치에 대한 연결을 허용하거나 차단하는 룰을 생성할 수 있습니다.

+ New rule(새 룰 추가): 룰을 생성하려면 클릭합니다.

Rule type(룰 유형):

- **FILTER(필터)**: 룰에 정의된 기준과 일치하는 장치의 연결을 허용하거나 차단하도록 선택합니다.
  - **정책**: 방화벽 룰에 대해 **Accept(수락)** 또는 **Drop(거부)**을 선택합니다.
  - **IP range(IP 범위)**: 허용하거나 차단할 주소 범위를 지정하도록 선택합니다. **Start(시작)** 및 **End(끝)**에서 IPv4/IPv6를 사용합니다.
  - **IP 주소**: 허용하거나 차단하려는 주소를 입력합니다. IPv4/IPv6 또는 CIDR 형식을 사용합니다.
  - **Protocol(프로토콜)**: 허용하거나 차단할 네트워크 프로토콜(TCP, UDP 또는 둘 다)을 선택합니다. 프로토콜을 선택하는 경우, 포트도 지정해야 합니다.
  - **MAC**: 허용하거나 차단하려는 장치의 MAC 주소를 입력합니다.
  - **Port range(포트 범위)**: 허용하거나 차단할 포트 범위를 지정하도록 선택합니다. **Start(시작)** 및 **End(끝)**에 추가합니다.
  - **Port(포트)**: 허용하거나 차단하려는 포트 번호를 입력합니다. 포트 번호는 1에서 65535 사이여야 합니다.
  - **Traffic type(트래픽 유형)**: 허용하거나 차단하려는 트래픽 유형을 선택합니다.
    - **UNICAST(유니캐스트)**: 단일 발신자가 단일 수신자에게 보내는 트래픽입니다.
    - **BROADCAST(브로드캐스트)**: 단일 발신자가 네트워크의 모든 장치로 보내는 트래픽입니다.
    - **MULTICAST(멀티캐스트)**: 하나 이상의 발신자가 하나 이상의 수신자에게 보내는 트래픽입니다.
- **LIMIT(제한)**: 룰에 정의된 기준과 일치하는 장치의 연결을 수락하지만 과도한 트래픽을 줄이기 위해 제한을 적용하려면 선택합니다.
  - **IP range(IP 범위)**: 허용하거나 차단할 주소 범위를 지정하도록 선택합니다. **Start(시작)** 및 **End(끝)**에서 IPv4/IPv6를 사용합니다.
  - **IP 주소**: 허용하거나 차단하려는 주소를 입력합니다. IPv4/IPv6 또는 CIDR 형식을 사용합니다.
  - **Protocol(프로토콜)**: 허용하거나 차단할 네트워크 프로토콜(TCP, UDP 또는 둘 다)을 선택합니다. 프로토콜을 선택하는 경우, 포트도 지정해야 합니다.
  - **MAC**: 허용하거나 차단하려는 장치의 MAC 주소를 입력합니다.
  - **Port range(포트 범위)**: 허용하거나 차단할 포트 범위를 지정하도록 선택합니다. **Start(시작)** 및 **End(끝)**에 추가합니다.
  - **Port(포트)**: 허용하거나 차단하려는 포트 번호를 입력합니다. 포트 번호는 1에서 65535 사이여야 합니다.
  - **Unit(단위)**: 허용하거나 차단할 연결의 유형을 선택합니다.
  - **Period(기간)**: **Amount(횟수)**와 관련된 시간 기간을 선택합니다.
  - **Amount(횟수)**: 설정된 **Period(기간)** 내에 장치가 연결할 수 있는 최대 횟수를 설정합니다. 최대 값은 65535입니다.

- **Burst(버스트)**: 설정된 **Period(기간)** 동안 한 번 설정된 **Amount(횟수)**를 초과할 수 있는 연결 횟수를 입력합니다. 설정된 횟수에 도달하면, 이후에는 설정된 기간 동안 설정된 횟수만 허용됩니다.
- **Traffic type(트래픽 유형)**: 허용하거나 차단하려는 트래픽 유형을 선택합니다.
  - **UNICAST(유니캐스트)**: 단일 발신자가 단일 수신자에게 보내는 트래픽입니다.
  - **BROADCAST(브로드캐스트)**: 단일 발신자가 네트워크의 모든 장치로 보내는 트래픽입니다.
  - **MULTICAST(멀티캐스트)**: 하나 이상의 발신자가 하나 이상의 수신자에게 보내는 트래픽입니다.

Test rules(룰 테스트): 정의한 룰을 테스트하려면 클릭합니다.

- **Test time in seconds(초 단위 테스트 시간)**: 룰 테스트에 대한 시간 제한을 설정합니다.
- **Roll back(롤백)**: 룰을 테스트하기 전의 이전 상태로 방화벽을 롤백하려면 클릭합니다.
- **Apply rules(룰 적용)**: 테스트하지 않고 룰을 활성화하려면 클릭합니다. 이렇게 하는 것은 권장하지 않습니다.

사용자 지정 서명된 AXIS OS 인증서

장치에 Axis의 테스트 소프트웨어 또는 기타 사용자 지정 소프트웨어를 설치하려면 사용자 지정 서명된 AXIS OS 인증서가 필요합니다. 인증서는 소프트웨어가 장치 소유자와 Axis 모두에 의해 승인되었는지 확인합니다. 소프트웨어는 고유한 일련 번호와 칩 ID로 식별되는 특정 장치에서만 실행할 수 있습니다. Axis가 서명을 위한 키를 보유하고 있으므로 Axis만이 사용자 지정 서명된 AXIS OS 인증서를 생성할 수 있습니다.

Install(설치): 인증서를 설치하려면 클릭합니다. 소프트웨어를 설치하기 전에 인증서를 설치해야 합니다.

⋮ 상황에 맞는 메뉴에는 다음이 포함됩니다.

- **Delete certificate(인증서 삭제)**: 인증서를 삭제하십시오.

계정

계정

Add account(계정 추가): 새 계정을 추가하려면 클릭합니다. 최대 100개의 계정을 추가할 수 있습니다.

Account(계정): 고유한 계정 이름을 입력합니다.

New password(새 패스워드): 계정의 패스워드를 입력합니다. 패스워드는 1~64자 길이여야 합니다. 문자, 숫자, 구두점, 일부 기호 등 인쇄 가능한 ASCII 문자(코드 32~126)만 패스워드에 사용할 수 있습니다.

Repeat password(패스워드 반복): 동일한 패스워드를 다시 입력하십시오.

Privileges(권한):

- **Administrator(관리자)**: 모든 설정에 완전히 액세스합니다. 관리자는 다른 계정을 추가, 업데이트 및 제거할 수 있습니다.
- **Operator(운영자)**: 다음을 제외한 모든 설정에 액세스할 수 있습니다.
  - 모든 **System(시스템)** 설정
- **Viewer(뷰어)**: 설정을 변경할 수 있는 권한이 없습니다.

상황에 맞는 메뉴에는 다음이 포함됩니다.

Update account(계정 업데이트): 계정 속성을 편집합니다.

Delete account(계정 삭제): 계정을 삭제합니다. root 계정은 삭제할 수 없습니다.

MQTT

MQTT(Message Queuing Telemetry Transport)는 사물 인터넷(IoT)을 위한 표준 메시징 프로토콜입니다. 단순화된 IoT 통합을 위해 설계되었으며 작은 코드 공간(small code footprint)과 최소 네트워크 대역폭으로 원격 장치를 연결하기 위해 다양한 산업에서 사용됩니다. Axis 장치 소프트웨어의 MQTT 클라이언트를 통해 장치에서 생성된 데이터 및 이벤트를 영상 관리 소프트웨어(VMS)가 아닌 시스템에 간편하게 통합할 수 있습니다.

기기를 MQTT 클라이언트로 설정합니다. MQTT 통신은 클라이언트와 브로커라는 두 엔터티를 기반으로 합니다. 클라이언트는 메시지를 보내고 받을 수 있습니다. 브로커는 클라이언트 간의 메시지 라우팅을 담당합니다.

*AXIS OS 지식 베이스*에서 MQTT에 대해 자세히 알아볼 수 있습니다.

ALPN

ALPN은 클라이언트 및 서버 간 연결의 핸드셰이크 단계에서 애플리케이션 프로토콜을 선택할 수 있게 하는 TLS/SSL 확장입니다. 이는 HTTP와 같이 다른 프로토콜에 사용되는 동일한 포트를 통해 MQTT 트래픽을 활성화하는 데 사용됩니다. 경우에 따라 MQTT 통신 전용으로 개방된 포트가 없을 수도 있습니다. 그러한 경우의 해결책은 ALPN을 사용해서 방화벽에서 허용되는 표준 포트에서 MQTT를 애플리케이션 프로토콜로 사용할지를 결정하는 것입니다.

MQTT 클라이언트

Connect(연결): MQTT 클라이언트를 켜거나 끕니다.

Status(상태): MQTT 클라이언트의 현재 상태를 표시합니다.

브로커

호스트: MQTT 서버의 호스트 이름 또는 IP 주소를 입력하십시오.

Protocol(프로토콜): 사용할 프로토콜을 선택합니다.

Port(포트): 포트 번호를 입력합니다.

- 1883은 **MQTT over TCP(TCP를 통한 MQTT)**의 기본값입니다.
- 8883은 **SSL를 통한 MQTT**의 기본값입니다.
- 80은 **웹 소켓을 통한 MQTT**의 기본값입니다.
- 443은 **웹 소켓 보안을 통한 MQTT**의 기본값입니다.

ALPN protocol(ALPN 프로토콜): MQTT 브로커 공급자가 제공한 ALPN 프로토콜 이름을 입력합니다. 이는 SSL을 통한 MQTT 및 웹 소켓 보안을 통한 MQTT에만 적용됩니다.

Username(사용자 이름): 클라이언트에서 서버에 액세스하기 위해 사용할 사용자 이름을 입력합니다.

패스워드: 사용자 이름의 패스워드를 입력합니다.

Client ID(클라이언트 ID): 클라이언트 ID를 입력하십시오. 클라이언트 식별자는 클라이언트가 서버에 연결할 때 서버로 전송됩니다.

Clean session(클린 세션): 연결 및 연결 해제 시의 동작을 제어합니다. 선택하면 연결 및 연결 해제 시 상태 정보가 삭제됩니다.

HTTP proxy(HTTP 프록시): 최대 길이가 255바이트인 URL입니다. HTTP 프록시를 사용하지 않으려면 필드를 비워 둘 수 있습니다.

HTTPS proxy(HTTPS 프록시): 최대 길이가 255바이트인 URL입니다. HTTPS 프록시를 사용하지 않으려면 필드를 비워 둘 수 있습니다.

Keep alive interval(간격 유지): 클라이언트가 긴 TCP/IP 시간 제한를 기다릴 필요 없이 서버를 더 이상 사용할 수 없는 시점을 감지할 수 있습니다.

Timeout(시간 제한): 연결이 완료되는 시간 간격(초)입니다. 기본값: 60

장치 항목 접두사: **MQTT 클라이언트** 탭의 연결 메시지 및 LWT 메시지의 주제에 대한 기본값과 **MQTT 발행** 탭의 게시 조건에서 사용됩니다.

Reconnect automatically(자동으로 재연결): 연결 해제 후 클라이언트가 자동으로 다시 연결해야 하는지 여부를 지정합니다.

메시지 연결

연결이 설정될 때 메시지를 보낼지 여부를 지정합니다.

Send message(메시지 전송): 메시지를 보내려면 사용 설정하세요.

Use default(기본값 사용): 자신의 기본 메시지를 입력하려면 끄십시오.

Topic(주제): 기본 메시지의 주제를 입력합니다.

Payload(페이로드): 기본 메시지의 내용을 입력합니다.

Retain(유지): 이 **Topic(주제)**에서 클라이언트 상태를 유지하려면 선택합니다.

QoS: 패킷 흐름에 대한 QoS 계층을 변경합니다.

마지막 유언 메시지

마지막 유언(LWT)을 사용하면 클라이언트가 브로커에 연결될 때 자격 증명과 함께 유언을 제공할 수 있습니다. 클라이언트가 나중에 어느 시점에서 비정상적으로 연결이 끊어지면(전원이 끊어졌기 때문일 수 있음) 브로커가 다른 클라이언트에 메시지를 전달할 수 있습니다. 이 LWT 메시지는 일반 메시지와 동일한 형식이며 동일한 메커니즘을 통해 라우팅됩니다.

Send message(메시지 전송): 메시지를 보내려면 사용 설정하세요.

Use default(기본값 사용): 자신의 기본 메시지를 입력하려면 끄십시오.

Topic(주제): 기본 메시지의 주제를 입력합니다.

Payload(페이로드): 기본 메시지의 내용을 입력합니다.

Retain(유지): 이 **Topic(주제)**에서 클라이언트 상태를 유지하려면 선택합니다.

QoS: 패킷 흐름에 대한 QoS 계층을 변경합니다.

MQTT 발행

기본 주제 접두사 사용: **MQTT client(MQTT 클라이언트)** 탭에서 장치 주제 접두사에 정의된 기본 주제 접두사를 사용하려면 선택합니다.

Include condition(조건 포함): MQTT 주제에서 조건을 설명하는 주제를 포함하려면 선택합니다.

Include namespaces(네임스페이스 포함): MQTT 주제에 ONVIF 주제 네임스페이스를 포함하려면 선택합니다.

일련 번호 포함: MQTT 페이로드에 장치의 일련 번호를 포함하려면 선택합니다.

Add condition(조건 추가): 조건을 추가하려면 클릭합니다.

Retain(유지): 어떤 MQTT 메시지가 보유로 전송되는지 정의합니다.

- **None(없음)**: 모든 메시지가 비유지 상태로 전송합니다.
- **Property(속성)**: 상태 추적 가능 메시지만 보관된 상태로 보냅니다.
- **All(모두)**: 상태 추적 가능 및 상태를 추적할 수 없음 메시지를 모두 보관된 상태로 보냅니다.

QoS: MQTT 발행에 대해 원하는 레벨을 선택합니다.

MQTT 구독

Add subscription(구독 추가): 새 MQTT 구독을 추가하려면 클릭합니다.

Subscription filter(구독 필터): 구독하려는 MQTT 주제를 입력하십시오.

Use device topic prefix(장치 항목 접두사 사용): 구독 필터를 MQTT 주제에 접두사로 추가합니다.

Subscription type(구독 유형):

- **Stateless(상태 추적 불가능)**: MQTT 메시지를 상태 추적 불가능 메시지로 변환하려면 선택합니다.
- **Stateful(상태 추적 가능)**: MQTT 메시지를 조건으로 변환하려면 선택합니다. 페이로드는 상태로 사용됩니다.

QoS: MQTT 구독에 대해 원하는 레벨을 선택합니다.

액세서리

I/O 포트

디지털 입력을 사용하여 개방 및 폐쇄 회로 사이를 전환할 수 있는 외부 장치(예: PIR 센서, 도어 또는 창 접점, 유리 파손 감지기)를 연결하십시오.

디지털 출력을 사용하여 릴레이 및 LED 등의 외부 장치와 연결합니다. VAPIX® 애플리케이션 프로그래밍 인터페이스 또는 웹 인터페이스를 통해 연결된 장치를 활성화할 수 있습니다.

포트

이름: 포트 이름을 바꾸려면 텍스트를 편집합니다.

Direction(방향):  은 포트가 입력 포트임을 나타냅니다.  은 포트가 출력 포트임을 나타냅니다. 포트를 구성할 수 있는 경우 아이콘을 클릭하여 입력과 출력 간에 변경할 수 있습니다.

Normal state(정상 상태): 개회로의 경우  을 클릭하고 폐회로의 경우  을 클릭합니다.

Current state(현재 상태): 포트의 현재 상태를 표시합니다. 현재 상태가 정상 상태와 같지 않을 때 입력 또는 출력이 활성화됩니다. 장치의 입력은 연결이 끊어지거나 1V VDC 이상의 전압이 있을 때 개방 회로가 됩니다.

비고

재시작하는 동안 출력 회로가 개방됩니다. 재시작이 완료되면 회로가 정상 위치로 돌아갑니다. 이 페이지에서 설정을 변경하면 출력 회로는 활성 트리거에 관계없이 원래 위치로 돌아갑니다.

Supervised(관리형)  : 누군가가 디지털 I/O 장치에 대한 연결을 변경하는 경우 작업을 감지하고 트리거할 수 있도록 하려면 켜십시오. 입력이 열렸는지 닫혔는지 감지하는 것 외에도 누군가가 입력을 변조했는지(즉, 잘리거나 단락되었는지) 감지할 수 있습니다. 연결을 감시하려면 외부 I/O 루프에 추가 하드웨어(EOL 레지스터)가 필요합니다.

로그

보고서 및 로그

보고서

- **View the device server report(장치 서버 보고서 보기)**: 팝업 창에서 제품 상태에 대한 정보를 봅니다. 액세스 로그는 자동으로 서버 보고서에 포함됩니다.
- **Download the device server report(장치 서버 보고서 다운로드)**: 현재 실시간 보기 이미지의 스냅샷뿐 아니라 UTF-8 형식의 전체 서버 보고서 텍스트 파일이 포함된 .zip 파일이 생성됩니다. 지원 서비스에 문의할 때 항상 서버 보고서 .zip 파일을 포함하십시오.
- **Download the crash report(충돌 보고서 다운로드)**: 서버 상태에 대한 자세한 정보가 있는 아카이브를 다운로드합니다. 충돌 보고서에는 자세한 디버그 정보와 서버 보고서에 있는 정보가 포함됩니다. 이 보고서에는 네트워크 추적과 같은 민감한 정보가 있을 수 있습니다. 보고서를 생성하는 데 몇 분 정도 소요될 수 있습니다.

로그

- **View the system log(시스템 로그 보기)**: 장치 시작, 경고 및 중요한 메시지와 같은 시스템 이벤트에 대한 정보를 표시하려면 클릭합니다.
- **View the access log(액세스 로그 보기)**: 잘못된 로그인 패스워드를 사용한 경우 등 실패한 장치 액세스 시도를 모두 표시하려면 클릭합니다.
- **View the audit log(감사 로그 보기)**: 클릭하면 성공 또는 실패한 인증 및 구성과 같은 사용자 및 시스템 활동에 대한 정보가 표시됩니다.

네트워크 추적

중요 사항

네트워크 추적 파일에는 인증서 또는 패스워드와 같은 민감한 정보가 포함될 수 있습니다.

네트워크 추적 파일은 네트워크 활동을 기록하여 문제를 해결하는 데 도움을 줄 수 있습니다.

Trace time(추적 시간): 추적 기간(초 또는 분)을 선택하고 **Download(다운로드)**를 클릭합니다.

원격 시스템 로그

Syslog는 메시지 로깅의 표준입니다. Syslog에서는 메시지를 생성하는 소프트웨어, 메시지를 저장하는 시스템, 메시지를 보고 및 분석하는 소프트웨어를 분리할 수 있습니다. 각 메시지별로 그 메시지를 생성하는 소프트웨어 유형을 나타내는 시설 코드가 표시되고 심각도 수준이 할당됩니다.

Server(서버): 새 서버를 추가하려면 클릭합니다.

호스트: 서버의 호스트 이름 또는 IP 주소를 입력합니다.

Format(포맷): 사용할 syslog 메시지 포맷을 선택합니다.

- Axis
- RFC 3164
- RFC 5424

Protocol(프로토콜): 사용할 프로토콜 선택:

- UDP(기본 설정 포트: 514)
- TCP(기본 설정 포트: 601)
- TLS(기본 설정 포트: 6514)

Port(포트): 다른 포트를 사용하려면 포트 번호를 편집합니다.

Severity(심각도): 트리거될 때 전송할 메시지를 선택합니다.

Type(유형): 전송하려는 로그 유형을 선택합니다.

Test server setup(서버 설정 테스트): 설정을 저장하기 전에 모든 서버에 테스트 메시지를 보냅니다.

CA certificate set(CA 인증서 설정): 현재의 설정을 확인하거나 인증서를 추가합니다.

유지보수

Restart(재시작): 장치를 재시작합니다. 이는 현재 설정에 영향을 주지 않습니다. 실행 중인 애플리케이션이 자동으로 재시작됩니다.

Restore(복구): 대부분의 설정을 공장 출하 시 기본값으로 되돌리십시오. 나중에 장치와 앱을 다시 구성하고 사전 설치되지 않은 모든 앱을 다시 설치하고 이벤트 및 프리셋을 다시 만들어야 합니다.

중요 사항

복원 후 저장되는 유일한 설정은 다음과 같습니다.

- 부팅 프로토콜(DHCP 또는 고정)
- 고정 IP 주소
- 기본 라우터
- 서브넷 마스크
- 802.1X 설정
- O3C 설정
- DNS 서버 IP 주소

Factory default(공장 출하 시 기본값): 모든 설정을 공장 출하 시 기본값으로 되돌리십시오. 그런 후에 장치에 액세스할 수 있도록 IP 주소를 재설정해야 합니다.

비고

모든 Axis 장치 소프트웨어는 디지털 서명되어 장치에 검증된 소프트웨어만 설치할 수 있습니다. 이렇게 하면 Axis 장치의 전반적인 최소 사이버 보안 수준을 더욱 높일 수 있습니다. 자세한 내용은 *axis.com*에서 백서 "Axis Edge Vault"를 참조하십시오.

AXIS OS upgrade(AXIS OS 업그레이드): 새 AXIS OS 버전으로 업그레이드합니다. 새 릴리스에는 향상된 기능, 버그 수정 및 완전히 새로운 기능이 포함됩니다. 항상 최신 AXIS OS 릴리즈를 사용하는 것이 좋습니다. 최신 릴리즈를 다운로드하려면 *axis.com/support*로 이동합니다.

업그레이드할 때 다음 세 가지 옵션 중에서 선택할 수 있습니다.

- **Standard upgrade(표준 업그레이드)**: 새 AXIS OS 버전으로 업그레이드합니다.
- **Factory default(공장 출하 시 기본값)**: 업그레이드하고 모든 설정을 공장 출하 시 기본값으로 되돌리십시오. 이 옵션을 선택하면 업그레이드 후에 이전 AXIS OS 버전으로 되돌릴 수 없습니다.
- **Automatic rollback(자동 롤백)**: 설정된 시간 내에 업그레이드하고 업그레이드를 확인하십시오. 확인하지 않으면 장치가 이전 AXIS OS 버전으로 되돌아갑니다.

AXIS OS rollback(AXIS OS 롤백): 이전에 설치된 AXIS OS 버전으로 되돌립니다.

T10125657_ko

2025-11 (M14.3)