

AXIS A4611 Network Reader

목차

설치	3
.....	3
시작하기	4
네트워크에서 장치 찾기	4
브라우저 지원	4
장치의 웹 인터페이스 열기	4
장치 구성	5
IP 주소 구성	5
장치 소프트웨어 업그레이드	5
CA 및 사용자 인증서 업로드	5
웹 인터페이스	7
.....	7
대시보드	7
.....	7
모듈	7
터치 키패드	8
13.56MHz 카드 리더	8
I/O	8
활성 출력	8
릴레이	8
사용자 설정	8
시스템	9
시스템 대시보드	9
네트워크 연결	9
날짜 및 시간	10
인증서	11
진단	11
유지보수	13
사양	14
제품 오버뷰	14
신호 LED	14
버튼	15
제어 버튼	15
케이블	15
외부 전원	15
네트워크 커넥터	15
전원 우선 순위	15
활성 출력	16
릴레이 케이블	16
입력 케이블	16
장치 세척	17
문제 해결	18
공장 초기화 설정으로 재설정	18
현재 소프트웨어 버전 확인	18
소프트웨어 업그레이드	18
기술적 문제 및 가능한 해결책	19
성능 고려 사항	19
지원 센터 문의	19

설치

다음 영상은 AXIS A46 Network Reader Series를 설치하는 방법의 예를 보여줍니다.

모든 설치 시나리오에 대한 완전한 지침과 중요한 안전 정보는 다음의 설치 가이드를 참조하십시오.

- AXIS A4610: axis.com/products/axis-a4610/support
- AXIS A4611: axis.com/products/axis-a4611/support
- AXIS A4612: axis.com/products/axis-a4612/support



이 비디오를 시청하려면 이 문서의 웹 버전으로 이동하십시오.

시작하기

네트워크에서 장치 찾기

네트워크에서 Axis 장치를 찾고 Windows®에서 해당 장치에 IP 주소를 할당하려면 AXIS IP Utility를 사용합니다. 애플리케이션은 axis.com/support에서 무료로 다운로드할 수 있습니다.

비고

AXIS IP Utility를 실행하는 컴퓨터는 Axis 장치와 동일한 네트워크 세그먼트(물리적 서브넷)에 있어야 합니다.

1. Axis 장치에 전원과 네트워크를 연결합니다.
2. AXIS IP Utility를 시작합니다. 네트워크에서 사용 가능한 모든 장치가 자동으로 목록에 표시됩니다.
3. 브라우저에서 장치에 액세스하려면 목록에서 이름을 두 번 클릭합니다.

브라우저 지원

다음 브라우저에서 장치를 사용할 수 있습니다.

	Chrome™	Firefox®	Edge™	Safari®
Windows®	✓	✓	✓	
macOS®	✓	✓	✓	✓
Linux®	✓	✓	✓	
기타 운영 체제	✓	✓	✓	

✓: 권장

*: 제한을 두고 지원

장치의 웹 인터페이스 열기

1. 브라우저를 열고 Axis 장치의 IP 주소 또는 호스트 이름을 입력합니다.
IP 주소를 모르는 경우에는 AXIS IP Utility를 사용하여 네트워크에서 장치를 찾습니다.
2. 기본 사용자 이름 `root` 및 비밀번호 `pass`를 입력합니다. 장치에 처음 액세스하면 비밀번호와 장치 이름을 변경하라는 메시지가 표시됩니다. *웹 인터페이스, on page 7*를 참조합니다.

장치의 웹 인터페이스에서 볼 수 있는 모든 컨트롤과 옵션에 대한 설명은 *웹 인터페이스, on page 7* 참조합니다.

장치 구성

이 장치는 설치 후 즉시 표준 리더로 작동합니다. 이 섹션에서는 하드웨어 설치 완료 후 제품을 정상적으로 가동하기 위해 설치자가 수행해야 하는 모든 주요 구성 단계를 설명합니다.

IP 주소 구성

장치가 LAN에 연결되어 있으며 유효한 IP 주소를 할당받거나 LAN DHCP 서버에서 IP 주소를 가져와야 합니다. 웹 인터페이스에서 IP 주소와 DHCP를 구성합니다.

IP 주소를 수동으로 구성하는 방법:

1. **System(시스템) > Network connection(네트워크 연결) > Basic configuration(기본 구성)**으로 이동합니다.
2. **IP address settings(IP 주소 설정)**에서 **Use DHCP Server(DHCP 서버 사용)**을 켜서 LAN DHCP 서버에서 IP 주소를 자동으로 가져옵니다.
3. **IP 주소, 네트워크 마스크 및 기본 게이트웨이**를 입력합니다.
4. 수동 DNS 설정을 사용하려면 **Always use manual DNS settings(항상 수동 DNS 설정 사용)**을 켭니다.
5. **기본 DNS 및 보조 DNS**를 입력합니다.
6. 장치를 식별할 수 있도록 **호스트 이름** 및 **공급업체 클래스 식별자**를 입력합니다.
7. **Required port mode(필수 포트 모드)** 옵션을 선택합니다.

현재 IP 주소를 찾는 방법:

비고

- 장치를 재시작해도 구성이 동일하게 유지됩니다.
1. 장치를 열고 후면 LED 표시등이 빨간색과 녹색으로 동시에 켜지고 짧은 신호음이 한 번 들릴 때까지 컨트롤 버튼을 약 15초 동안 누릅니다.
 2. 제어 버튼에서 손을 떼면 장치가 스피커를 통해 현재 IP 주소를 알려줍니다.

장치 소프트웨어 업그레이드

장치에 처음 로그인할 때 장치 소프트웨어를 업그레이드할 것을 권장합니다. axis.com/support에서 장치에 맞는 최신 버전을 다운로드합니다. 새 버전 업로드 방법:

1. **System(시스템) > Maintenance(유지보수)**로 이동합니다.
2. **Firmware upload(펌웨어 업로드)**를 클릭하고 다운로드한 소프트웨어 버전을 선택합니다.
3. **Upload(업로드)**를 클릭합니다.

비고

업로드 후 장치가 재시작되어 업그레이드가 완료됩니다.

CA 및 사용자 인증서 업로드

비고

- 인증서 ID는 40자를 넘지 않아야 하며 소문자와 대문자, 숫자, _, - 만 포함해야 합니다.
- 2048비트보다 긴 개인 RSA 키가 있는 인증서가 거부되면 다음 메시지가 표시됩니다.
- 타원 곡선을 기반으로 하는 인증서의 경우, secp256r1(prime256v1 및 NIST P-256이라고도 함) 및 secp384r1(NIST P-384라고도 함) 곡선만 사용합니다.

CA 인증서 업로드 방법:

1. **System(시스템) > Certificates(인증서) > CA Certificates(CA 인증서)**로 이동합니다.

2.  **Upload(업로드)**를 클릭합니다.
3. **인증서 ID**를 입력합니다.
4. **Select file(파일 선택)**을 클릭하여 CA 인증서를 업로드합니다.
5. **Upload(업로드)**를 클릭합니다.

사용자 인증서 업로드 방법:

1. **System(시스템) > Certificates(인증서) > User Certificates(사용자 인증서)**로 이동합니다.
2. 인증서 또는 개인 키를 업로드하려면  **Upload(업로드)**를 클릭합니다.
3. **인증서 ID**를 입력합니다.
4. **Select file(파일 선택)**을 클릭하여 사용자 인증서와 개인 키를 업로드합니다.
5. 개인 키를 업로드하는 경우 **기본 키 패스워드**가 있으면 이를 입력합니다.
6. **Upload(업로드)**를 클릭합니다.

비고

도어 컨트롤러의 웹 인터페이스에서 리더를 연결해야 합니다. 도어 컨트롤러의 사용자 설명서를 참조하십시오.

웹 인터페이스

비고

이 섹션에서 설명하는 기능 및 설정에 대한 지원은 장치마다 다릅니다. 이 아이콘  은 일부 장치에서만 기능이나 설정을 사용할 수 있음을 나타냅니다.



장치의 새 알림에 액세스합니다.



사용자 메뉴에는 다음이 포함됩니다.

- **Device time(장치 시간):** 장치의 현재 시간.
- **언어 변경:** 언어를 변경합니다.
- **Change password(패스워드 변경):** 장치에 로그인하는 데 필요한 패스워드를 변경합니다.
- **Help(도움말):** 제품 도움말에 액세스합니다.
- **About(정보):** 펌웨어 버전 및 일련번호를 포함한 제품 정보를 봅니다.
-  **Log out(로그아웃):** 현재 계정에서 로그아웃합니다.

대시보드



상황에 맞는 메뉴에는 다음이 포함됩니다.

- **장치 이름 변경:** 장치 이름을 변경합니다.

Locate(찾기): 리더를 식별하는 데 도움이 되는 소리를 재생합니다.

Serial number(일련 번호): 장치 일련 번호

Firmware version(펌웨어 버전): 현재 장치에서 실행 중인 소프트웨어 버전입니다.

MAC 주소: 장치의 고유 식별자 번호입니다.

가동 시간: 장치가 작동한 시간을 표시합니다.

하드웨어 버전: 현재 장치에서 실행 중인 하드웨어 버전입니다.

전원: 현재 전원입니다.

Modules(모듈): 카드 및 리더의 모듈 정보를 확인하고 업데이트하려면 →을 클릭합니다.

모듈



상황에 맞는 메뉴에는 다음이 포함됩니다.

- **Module details(모듈 세부 정보):** 카드 리더 이름, 모듈 유형, 보드 유형, 어셈블리 버전, 애플리케이션 버전 및 부트로더 버전을 표시합니다.
- **Locate(찾기):** 연결된 모듈을 검색하려면 클릭합니다.

터치 키패드

모듈 이름: 장치 키패드용 모듈 이름을 입력합니다.

버튼을 눌렀을 때 플래시: 누군가 키패드를 누를 때 옵션을 선택합니다.

- **아니요:** 키패드의 조명이 꺼진 상태로 유지됩니다.
- **예:** 누군가 버튼을 누르면 키패드의 조명이 깜박입니다.

13.56MHz 카드 리더

모듈 이름: 입력 및 출력 사양의 모듈 이름을 입력합니다.

허용되는 카드 유형: 카드 리더기가 인식해야 할 카드 유형을 드롭다운 목록에서 선택하십시오.

I/O

활성 출력

논리적 상태: 도어의 상태를 표시합니다. 시스템이 도어를 열라는 요청을 받지 못하면 논리적 상태가 꺼지고, 문을 열라는 요청을 받으면 논리적 상태가 켜집니다.

출력 상태: 물리적 출력의 실제 상태를 표시합니다. 출력 상태는 정상 모드에서 논리적 상태에 해당합니다. 반전 및 보안 모드에서는 논리 상태와 출력 상태가 반전됩니다.

Mode(모드): 드롭다운 메뉴에서 모드를 선택합니다.

- **Normal(정상):** 출력은 항상 꺼져 있지만, 도어 열기 요청이 있을 때 활성화됩니다.
- **Security(보안):** 출력은 보안 릴레이와 연결되는 모드입니다. 이 모드에서는 출력이 항상 켜져 있으며, 도어 열림이 요청되면 출력선을 통해 보안 릴레이로 코드가 전송됩니다. 릴레이는 코드가 올바른지 확인합니다.
- **반전:** 출력은 항상 켜져 있지만, 도어 열기 요청이 있을 때 비활성화됩니다.

Test(테스트): I/O의 활성 출력이 작동하는지 확인하려면 클릭하세요.

릴레이

릴레이 상태: 물리적 릴레이 상태를 표시합니다.

Test(테스트): 릴레이가 작동하는지 확인하려면 클릭하세요.

사용자 설정

시그널링 볼륨

시그널링 볼륨은 접근 제어 시스템 내에서 통신이 이루어질 때 장치에서 발생하는 사운드의 레벨입니다(예: 장치가 카드를 읽거나 접근을 허용할 때 내는 신호음).

키 신호음 볼륨: 음량을 설정합니다.

경고음 볼륨: 예를 들어 전원 커짐에서 케이블 연결로 장치 작동 상태가 전환될 때 경고 및 신호의 볼륨을 설정할 수 있습니다.

역광

신호 LED 강도: LED 밝기를 설정합니다.

Backlight enabled(백라이트 활성화됨)  : 백라이트를 활성화하려면 켵니다.

강도: 백라이트 밝기 레벨을 설정합니다.

시스템

시스템 대시보드

Download diagnostic package(진단 패키지 다운로드) : 진단 패키지를 파일로 다운로드하려면 클릭합니다.

Network connection(네트워크 연결) : 네트워크 설정을 편집하려면 →을 클릭합니다.

- **Network overview(네트워크 오버뷰)**: 장치에 현재 구성된 네트워크 설정을 표시합니다.

날짜 및 시간: 장치의 현재 날짜와 시간을 표시합니다. 날짜 및 시간을 편집하려면 →을 클릭합니다.

Maintenance(유지 관리): 장치의 현재 소프트웨어 버전을 표시합니다. 유지 관리 웹 페이지로 이동하려면 →을 클릭합니다.

- **Download backup(백업 다운로드)**: 클릭하여 컴퓨터에 장치 구성 파일을 다운로드합니다.
- **Restore configuration(구성 복구)**: 클릭하여 구성 파일을 업로드하고 대화 상자에서 가져오기 설정을 선택합니다.

네트워크 연결

로컬 네트워크

장치는 이더넷 케이블을 사용하여 LAN에 연결할 수 있습니다.

IP 주소 설정

DHCP 서버 사용: LAN DHCP 서버에서 IP 주소를 자동으로 가져오려면 켵니다. 대부분의 네트워크에 대해 자동 DNS(DHCP)를 권장합니다.

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.

네트워크 마스크: 네트워크 마스크를 입력하여 LAN(Local Area Network) 내부에 있는 주소를 정의합니다.

기본 게이트웨이: off-LAN 장비와의 통신을 제공하는 기본 게이트웨이의 주소를 입력합니다.

현재 IP 주소 설정: 장치에 현재 있는 IP 주소 설정을 표시합니다.

DNS 설정

항상 수동 DNS 설정 사용: DNS 설정을 수동으로 설정하려면 켵니다.

기본 DNS: 도메인 이름을 IP 주소로 변환하기 위한 기본 DNS 서버 주소를 입력합니다. 공장 재설정 후 기본 DNS 값은 8.8.8.8입니다.

보조 DNS: 기본 DNS에 액세스할 수 없는 경우 대안으로 보조 DNS 서버 주소를 입력합니다. 공장 재설정 후 보조 DNS 값은 8.8.4.4입니다.

현재 DNS 설정: 장치에 현재 있는 DNS 설정을 표시합니다.

고급 구성

호스트 이름: IP 네트워크 ID를 입력합니다. 허용되는 문자는 A~Z, a~z, 0~9, -입니다.

공급업체 클래스 식별자: DHCP Option 60용 공급업체 클래스 식별자를 문자열로 입력합니다.

필수 포트 모드: 선호하는 네트워크 인터페이스 포트 모드를 선택합니다. 자동 또는 반이중 - 10mbps. 사용 중인 네트워크 케이블이 100Mbps 트래픽용으로 안정적이지 않은 경우 10Mbps의 낮은 비트 레이트가 필요할 수 있습니다.

현재 포트 상태: 현재 네트워크 인터페이스 포트 상태(반이중 또는 전이중 - 10mbps 또는 100mbps)를 표시합니다.

웹 서버

통합 웹 서버에 액세스하여 표준 웹 브라우저에서 장치를 구성할 수 있습니다. HTTPS 프로토콜은 장치와 웹 브라우저 간의 보안 통신을 활성화합니다.

HTTP port(HTTP 포트): 사용할 HTTP 포트를 입력합니다.

HTTPS port(HTTPS 포트): 사용할 HTTPS 포트를 입력합니다.

최소 허용 TLS 버전: 장치에 연결할 가장 낮은 TLS 버전을 선택합니다.

HTTPS 사용자 인증서: HTTP 서버용 사용자 인증서와 개인 키를 선택합니다. 선택이 없는 경우 장치는 자체 서명된 인증서를 사용합니다.

원격 액세스 활성화: off-LAN IP 주소에서 인터콤 웹 서버에 대한 원격 액세스를 활성화하려면 켵니다.

방화벽

방화벽은 장치를 보호하며 권한이 있는 사용자만 네트워크에 액세스할 수 있도록 보장합니다.

비활성화: 토글을 사용하여 방화벽을 활성화하거나 비활성화합니다.

날짜 및 시간

비고

장치의 날짜와 시간을 NTP 서버와 동기화하는 것이 좋습니다.

시간 동기화 설정

Automatic time from NTP or internet(NTP 또는 인터넷을 통한 자동 시간 설정): 토글을 사용하여 NTP 서버 또는 인터넷과의 시간 동기화를 활성화하거나 비활성화합니다.

NTP 서버 주소: 동기화를 위한 NTP 서버 주소를 입력합니다.

Synchronize with browser(브라우저와 동기화): 장치의 시간을 컴퓨터의 시간과 동기화하려면 클릭합니다.

시간대:

수동 선택: 장치의 표준 시간대를 선택합니다.

사용자 지정 룰: 시간대를 수동으로 입력합니다.

인증서

인증서는 네트워크상의 장치를 인증하는 데 사용됩니다. 장치는 다음 인증서 및 개인 키 형식을 지원합니다.

- PEM
- CER
- PFX
- DER

CA 인증서: CA 인증서를 사용하여 피어 인증서를 인증할 수 있습니다. 장치가 네트워크에 연결될 때 인증 서버의 ID 확인합니다.

중요 사항

장치를 공장 출하 시 기본값으로 재설정하면 모든 인증서가 삭제됩니다.

CA 인증서: 장치 ID 확인을 위한 인증서를 선택합니다.



Upload(업로드): CA 인증서를 업로드하고 인증서 ID를 입력하려면 클릭합니다.

Search(검색): 인증서 ID를 입력하여 CA 인증서 목록에서 찾습니다.



: 장치에서 인증서를 삭제하려면 클릭합니다.



: 인증서 정보를 보려면 클릭합니다.

사용자 인증서: 사용자 인증서는 사용자의 신원을 확인합니다. 이는 CA(인증 기관)이 자체 서명하거나 발행할 수 있습니다. 자체 서명 인증서는 CA 발급 인증서를 받기 전에 사용할 수 있는 제한된 보호를 제공합니다.

사용자 인증서: 신원 확인에 사용할 인증서와 개인 키를 선택합니다.



Upload(업로드): 사용자 인증서와 개인 키를 업로드하고 키 패스워드가 있는 경우 입력하려면 클릭합니다.

Search(검색): 인증서 ID를 입력하여 사용자 인증서 목록에서 찾습니다.



: 장치에서 인증서를 삭제하려면 클릭합니다.



: 인증서 정보를 보려면 클릭합니다.

진단

진단 로그는 보고된 문제를 식별하고 해결하는 데 도움이 됩니다. 진단을 사용하여 추후 다운로드 및 기술 지원을 위해 진단 로그를 캡처할 수 있습니다.

Ping: IP 주소로 테스트 데이터를 보내는 방법:

- **Ping**을 클릭합니다.
- IP 주소 또는 URL을 입력합니다.
- **Ping**을 클릭합니다.

Close(닫기): 대화 상자를 닫으려면 클릭합니다.

진단 패키지

진단 패키지는 네트워크 패킷과 syslog 메시지가 포함된 ZIP 파일입니다. 여기에는 장치에 대한 정보, 구성, 네트워크 트래픽, 충돌 로그 및 메모리 통계가 포함되어 있습니다. 또한 장치가 캡처한 네트워크 패킷 수와 syslog 메시지의 크기도 표시됩니다.

Restart capture(캡처 재시작): 패킷 캡처를 재시작하려면 클릭합니다.

Download(다운로드): 진단 패키지를 파일로 다운로드하려면 클릭합니다.

온-디바이스 네트워크 패킷 캡처

Download(다운로드): 캡처한 네트워크 패킷을 다운로드하려면 클릭합니다.

시작: 네트워크에서 수신 및 발신 패킷 캡처를 시작하려면 클릭합니다.

비고

시작을 클릭하면 이전에 캡처한 패킷이 삭제됩니다.

Stop(중지): 네트워크에서 수신 및 발신 패킷 캡처를 중지하려면 클릭합니다.

Syslog 캡처: 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.

⋮ 상황에 맞는 메뉴에는 다음이 포함됩니다.

- **Delete captured messages(캡처한 메시지 삭제):** syslog 메시지를 삭제하려면 클릭합니다.

Download(다운로드): syslog 메시지를 다운로드하려면 클릭합니다.

시작: 데이터 캡처를 시작하려면 클릭합니다.

Stop(중지): 데이터 캡처를 중지하려면 클릭합니다.

네트워크 패킷 캡처 다운로드

이를 통해 장치 네트워크 인터페이스에서 수신 및 발신 패킷을 캡처하여 컴퓨터로 다운로드할 수 있습니다.

시작: 데이터 캡처를 시작하려면 클릭합니다.

Time to capture(캡처할 시간): 캡처를 위한 기간을 설정합니다.

Stop(중지): 데이터 캡처를 중지하려면 클릭합니다.

원격 서버로 syslog 보내기: 토글을 사용하여 syslog를 활성화/비활성화할 수 있습니다. 이를 통해 기록 보관 및 추가 장치 분석을 위해 syslog 메시지를 syslog 서버로 전송할 수 있습니다.

Server address(서버 주소): syslog 애플리케이션이 실행 중인 서버의 IP 또는 MAC 주소를 입력합니다.

Severity level(심각도 수준): 트리거될 때 보낼 메시지의 심각도를 선택합니다.

유지보수

Reset to default(기본값으로 재설정): 장치를 공장 출하 시 기본 구성으로 초기화하려면 클릭합니다.

- 네트워크 및 인증서에 대해 구성된 설정을 유지하려면 **Keep network settings and certificates(네트워크 설정 및 인증서 유지)**를 선택합니다.
- 모든 장치 설정을 재설정하려면 **Reset everything(모두 재설정)**을 선택합니다.
- **Reset(재설정):** 재설정하려면 클릭합니다.

장치 재시작: 장치를 재시작하려면 클릭합니다.

Download backup(백업 다운로드): 클릭하여 컴퓨터에 장치 구성 파일을 다운로드합니다.

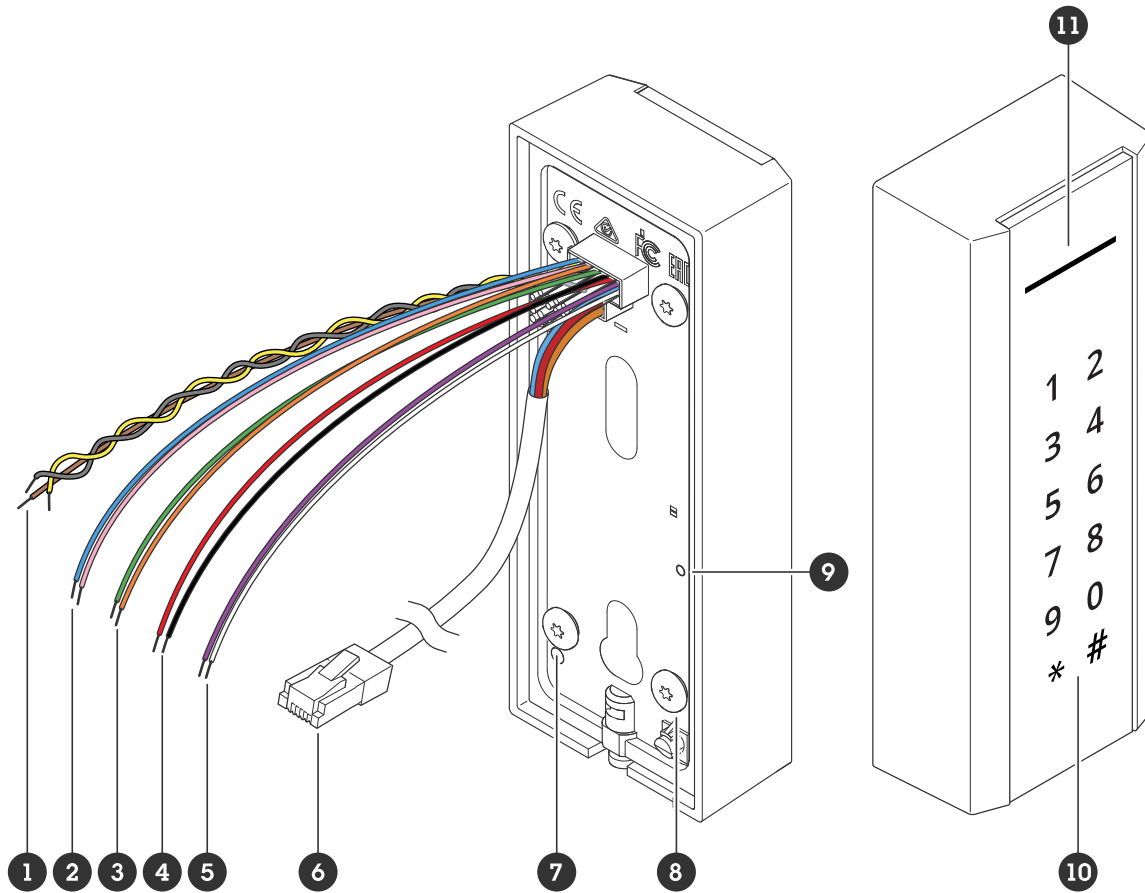
Restore configuration(구성 복구): 클릭하여 구성 파일을 업로드하고 대화 상자에서 가져오기 설정을 선택합니다.

펌웨어: 현재 장치에서 실행 중인 소프트웨어 버전, 장치에서 사용할 수 있는 최소 소프트웨어 버전, 부트로더 버전, 소프트웨어 빌드 유형, 날짜 및 시간에 대한 오버뷰를 표시합니다.

Firmware upload(펌웨어 업로드): 소프트웨어 파일을 업로드하고 장치 소프트웨어를 업그레이드하려면 클릭합니다.

사양

제품 오버뷰



- 1 릴레이 케이블
- 2 입력 케이블 1
- 3 입력 케이블 2
- 4 외부 전원
- 5 활성 출력
- 6 네트워크 커넥터(PoE)
- 7 제어 버튼
- 8 탬퍼 스위치
- 9 후면 LED 표시등
- 10 키패드
- 11 전면 리더 표시기 스트라이프

신호 LED

상태 LED	표시
화이트	장치를 찾습니다.
녹색	인증이 유효합니다.
빨간색	카드 대기 중에 계속 켜져 있습니다. 인증이 유효하지 않을 때 깜박입니다.

비고

백라이트 및 밝기 수준을 설정하려면 *사용자 설정, on page 8*을 참조하십시오.

버튼

제어 버튼

제어 버튼의 용도는 다음과 같습니다.

- 현재 IP 주소를 찾습니다. 후면 LED 표시등이 빨간색과 녹색으로 동시에 켜지고 짧은 신호음이 한 번 들릴 때까지 버튼을 약 15초 동안 누릅니다.
- 제품을 공장 초기화 설정으로 재설정합니다. *공장 초기화 설정으로 재설정, on page 18*을 참조하십시오.
- 장치를 재시작합니다. 버튼을 1초 이내로 눌러 장치를 재시작합니다.
- 고정 IP 주소(192.168.1.100)로 전환하기:
 - 장치 뒷면의 LED 표시등이 빨간색과 녹색으로 동시에 켜지고 신호음이 들릴 때까지 버튼을 약 15초 동안 길게 누릅니다.
 - 빨간색 LED가 꺼지고 신호음이 두 번 울린 후 버튼을 놓습니다.
- DHCP 서버로 전환하기:
 - 후면 LED 표시등이 빨간색과 녹색으로 동시에 켜지고 신호음이 들릴 때까지 버튼을 15초 동안 길게 누릅니다.
 - 빨간색 LED가 꺼지고 신호음이 두 번 울리는 동안 버튼을 3초간 누릅니다.
 - 녹색 LED가 꺼진 후 버튼을 놓으면 빨간색 LED가 다시 켜지고 신호음이 세 번 울립니다.

케이블

외부 전원

장치에는 외부 전원 공급에 연결할 수 있는 케이블이 있습니다.

기능	색상	사양
DC +	빨간색	12V DC, 최대 12.0W 케이블 길이: 350mm
DC -	블랙	

네트워크 커넥터

기능	색상	사양
이더넷 및 PoE	블랙	RJ45 케이블 길이: 2,900mm

전원 우선 순위

이 장치는 PoE 또는 DC 입력으로 전원을 공급받을 수 있습니다. *네트워크 커넥터, on page 15*를 참조하십시오.

- PoE와 DC가 모두 연결된 경우 DC가 전원 공급에 사용됩니다.
- PoE와 DC가 모두 연결되어 있고, 현재 PoE에 전원이 공급되고 있습니다. DC가 끊기면 장치가 PoE를 사용하여 전원을 공급합니다.
- 시동 중에 PoE를 이용하고 장치를 시동한 후 DC를 연결하면 전원 공급에 DC를 사용합니다.

활성 출력

활성 출력 케이블은 보안 릴레이 또는 전기 잠금 장치에 연결하는 데 사용됩니다.

비고

보안을 강화하려면 리더와 잠금 장치 사이에 2N Security Relay를 추가합니다.

기능	색상	사양
DC +	화이트	전원 공급 장치에 따라 9.8~13.8V DC, 최대 600mA. PoE: 11.6V DC: 소스 전압 -0.4V 케이블 길이: 350mm
DC -	바이올렛	

릴레이 케이블

액세스 잠금장치 및 센서를 관리하기 위한 릴레이 케이블입니다.

기능	색상	비고	사양
NO	노란색	폐일 시큐어 잠금을 위한 정상 개방	Max 1 A 30 V DC 케이블 길이: 350mm
COM	회색	공통	
NC	갈색	폐일 세이프 잠금을 위한 정상 폐쇄	

입력 케이블

입력 케이블은 외부 입력 장치에 연결하는 동시에 장치 제어판과 입력 장치 간의 원활한 통신을 활성화하는 데 사용됩니다. 장치에는 도어 위치 센서와 REX 버튼을 연결하는 데 사용할 수 있는 입력 커넥터 2개, 입력 1 및 입력 2가 있습니다.

케이블	색상	사양
입력 1+	분홍색	0~30V DC
입력 1-	청색	
입력 2+	주황색	
입력 2-	녹색	

장치 세척

비고

- 자극적인 화학 물질로 인해 장치가 손상될 수 있습니다. 창문 세정제나 아세톤과 같은 화학 물질을 사용하여 장치를 세척하지 마십시오.
 - 직사광선이나 고온에서 세척하면 얼룩이 생길 수 있으므로 주의해서 피해야 합니다.
1. 압축된 공기통을 사용하여 장치에서 먼지와 느슨한 오물을 제거하십시오.
 2. 필요한 경우 미지근한 물에 적신 부드러운 극세사 천으로 장치를 닦으십시오.
 3. 얼룩이 생기지 않도록 깨끗한 비마모성 천으로 장치를 건조시키십시오.

문제 해결

공장 초기화 설정으로 재설정

비고

- 공장 출하 시 기본값으로 재설정하면 모든 설정이 공장 출하 시 기본값으로 변경됩니다.

1. 장치를 엽니다.
2. 후면 LED 표시등이 빨간색, 녹색으로 변했다가 꺼질 때까지 버튼을 약 24초 동안 길게 누릅니다.

비고

신호음이 한 번, 두 번, 세 번, 네 번 다른 간격으로 울립니다.

3. 네 번째 신호음이 울린 후 제어 버튼에서 손을 땁니다. 프로세스가 완료되고 제품이 공장 출하 시 기본 설정으로 재설정되었습니다.
4. 설치 및 관리 소프트웨어 도구를 사용하여 패스워드를 설정하고 제품에 액세스합니다.
설치 및 관리 소프트웨어 도구는 axis.com/support의 지원 페이지에서 제공됩니다.

또한 장치의 웹 인터페이스를 통해 매개변수를 공장 출하 시 기본값으로 재설정할 수 있습니다.

System(시스템) > Maintenance(유지 관리) > Reset to default(기본값으로 재설정)로 이동합니다.

현재 소프트웨어 버전 확인

장치 소프트웨어가 장치의 기능을 결정합니다. 문제를 해결할 때는 현재 소프트웨어 버전을 먼저 확인하는 것이 좋습니다. 최신 버전에 특정 문제를 해결하는 수정 사항이 포함되어 있을 수 있습니다.

현재 소프트웨어 버전은 두 가지 방법으로 확인할 수 있습니다.

- 장치의 웹 인터페이스로 이동합니다:
 - **Dashboard(대시보드)**로 이동합니다.
 - **Firmware(펌웨어)**로 이동하거나 *유지보수, on page 13*를 참조합니다.

소프트웨어 업그레이드

중요 사항

- Axis Communications AB가 이를 보장하지는 않지만(새 펌웨어 버전에서 기능을 사용할 수 있는 경우) 장치 소프트웨어를 업그레이드할 때 사전 구성되고 사용자 정의된 설정이 저장됩니다.
- 업그레이드 프로세스 중에 장치가 전원에 연결되어 있는지 확인합니다.

비고

장치를 최신 소프트웨어 버전으로 업그레이드하면 제품에서 최신 기능을 사용할 수 있습니다. 업그레이드하기 전에 항상 새 릴리스마다 제공되는 릴리즈 정보와 업그레이드 지침을 참조하십시오. 최신 소프트웨어 버전 및 릴리스 노트를 확인하려면 axis.com/support/device-software로 이동합니다.

1. axis.com/support/device-software에서 무료로 제공되는 소프트웨어 파일을 컴퓨터에 다운로드합니다.
2. 장치 페이지에 로그인합니다.
3. **System(시스템) > Maintenance(유지보수)**로 이동하여 **Firmware upload(펌웨어 업로드)**를 클릭합니다.
4. 소프트웨어 파일을 선택하고 **Upload(업로드)**를 클릭합니다.

업그레이드가 완료되면 제품이 자동으로 재시작됩니다.

기술적 문제 및 가능한 해결책

IP 주소 설정 문제

- 장치에 해당하는 IP 주소와 장치 액세스에 사용된 컴퓨터의 IP 주소가 다른 서브넷에 있는 경우에는 IP 주소를 설정할 수 없습니다. 네트워크 관리자에게 문의하여 IP 주소를 받으십시오.
- IP 주소를 다른 장치에서 사용 중인 경우:
 1. 네트워크에서 Axis 장치를 분리합니다.
 2. Command/DOS 창에서, ping을 입력한 후 장치의 IP 주소를 입력합니다.
 3. Reply from <IP address>: bytes=32; time=10...이라는 응답을 받는 경우, 이는 해당 IP 주소가 이미 네트워크의 다른 장치에서 사용 중일 수 있음을 의미합니다. 네트워크 관리자에게 새 IP 주소를 받아 장치를 다시 설치하십시오.
 4. Request timed out을 수신하는 경우 이는 Axis 장치에 IP 주소를 사용할 수 있음을 의미합니다. 모든 케이블 배선을 확인하고 장치를 다시 설치하십시오.

장치 액세스 관련 문제

로그인할 수 없음

HTTPS가 활성화된 경우 로그인을 시도할 때 올바른 프로토콜(HTTP 또는 HTTPS)이 사용되는지 확인하십시오. 브라우저의 주소 필드에 http 또는 https를 수동으로 입력해야 할 수도 있습니다.

계정 패스워드를 분실한 경우 장치를 공장 출하 시 기본값으로 재설정해야 합니다. 공장 초기화 설정으로 재설정, on page 18을 참조하십시오.

IP 주소가 DHCP에 의해 변경됨

DHCP서버에서 획득한 IP 주소는 동적이며 변경될 수 있습니다. IP 주소가 변경된 경우에는 AXIS IP Utility를 사용하여 네트워크에서 장치를 찾습니다. 해당 모델이나 일련 번호 또는 DNS 이름을 이용하여 장치를 식별합니다(이름이 구성된 경우).

인증서 경고 NET::ERR_CERT_AUTHORITY_INVALID

인증서 경고는 OS 장치용 표준 절차입니다. **Advanced(고급)**을 클릭한 후 **Proceed to *IP address*(**IP 주소**로 진행)(안전하지 않음)**을 클릭하여 장치 로그인 웹페이지에 액세스합니다. 옵션이 거의 없음:

- 다른 브라우저 또는 장치를 사용합니다.
- 인증서 경고 페이지의 아무 곳이나 클릭하고 **thisisunsafe**를 입력합니다.

웹페이지에 도착하면 **System(시스템) > Maintenance(유지보수) > Firmware upload(펌웨어 업로드)**로 이동하여 최신 장치 소프트웨어로 업데이트합니다.

찾는 내용이 여기에 없는 경우에는 axis.com/support에서 장애 처리 섹션을 확인해 보십시오.

성능 고려 사항

고려해야 할 가장 중요한 요소:

- 좋지 않은 인프라로 인해 네트워크 점유율이 과중되면 대역폭에 영향을 줍니다.

지원 센터 문의

추가 도움이 필요하면 axis.com/support로 이동하십시오.

T10237046_ko

2026-07 (M2.3)

© 2026 Axis Communications AB