AXIS Secure Entry for XProtect

사용자 설명서

목차

접근 제어

접근 제어는 물리적 접근 제어와 영상 감시를 결합한 솔루션입니다. 이 통합을 통해 Management Client에서 직접 Axis 접근 제어 시스템을 구성할 수 있습니다. 이 시스템은 XProtect와 매끄럽게 통합되어 운영자가 Smart Client에서 접근을 모니터링하고 접근 제어 작업을 수행할 수 있게 합니다.

비고

요구 사항

- VMS 버전 2024 R1 이상.
- XProtect Access 라이센스에 대한 자세한 내용은 *액세스 라이센스*를 참조하십시오.
- 이벤트 서버와 Management Client에 AXIS Optimizer를 설치합니다.

AXIS Secure Entry를 통해 AXIS Optimizer를 설치하면 인바운드 트래픽(TCP)용 53459 및 53461 포트가 열립니다.

접근 제어 구성

비고

시작하기 전에 다음을 수행합니다.

- 도어 컨트롤러 소프트웨어를 업그레이드합니다. 사용 중인 VMS 버전에 대한 최소 및 권장 AXIS OS 버전은 아래 표를 참조하십시오.
- 날짜와 시간이 올바른지 확인하십시오.

AXIS Optimizer 버전	최소 AXIS OS 버전	권장 AXIS OS 버전
5.6	12.6.94.1	12.6.94.1

시스템에 Axis 네트워크 도어 컨트롤러를 추가하는 방법:

1. **Site Navigation(사이트 탐색)** > **AXIS Optimizer** > **Access control(접근 제어)**로 이동합니다.
2. **Configuration(구성)**에서 **Devices(장치)**를 선택합니다.
3. **Discovered devices(검색된 장치)**를 선택하여 시스템에 추가할 수 있는 장치 목록을 확인합니다.
4. 추가할 장치를 선택합니다.
5. 팝업 창에서 **+ Add(+ 추가)**를 클릭하고 컨트롤러 자격 증명을 입력합니다.

비고

추가된 컨트롤러가 **Management(관리)** 탭에 표시됩니다.

컨트롤러를 수동으로 시스템에 추가하려면 **Management(관리)** 탭에서 **+ Add(+ 추가)**를 클릭합니다.

도어 컨트롤러 이름을 추가, 제거 또는 편집할 때마다 변경 사항을 VMS에 통합하는 방법:

- **Site Navigation(사이트 탐색)** > **Access control(접근 제어)**로 이동하여 Access Control integration(접근 제어 통합)을 클릭합니다.
- **General settings(일반 설정)** 탭에서 **Refresh Configuration(구성 새로 고침)**을 클릭합니다.

접근 제어를 구성하기 위한 워크플로

1. **Site Navigation(사이트 탐색)** > **AXIS Optimizer** > **Access control(접근 제어)**로 이동합니다.
2. 사전 정의된 식별 프로파일을 편집하거나 새 식별 프로파일을 만들려면 항목을 참조하십시오.
3. 카드 형식 및 PIN 길이의 사용자 지정 설정을 사용하려면 항목을 참조하십시오.
4. 도어에 특정 도어를 추가하고 식별 프로파일을 적용합니다. 을 참조하십시오.
5. 영역을 추가하고 해당 영역에 도어를 추가합니다. 을 참조하십시오.

도어 컨트롤러용 장치 소프트웨어 호환성

중요 사항

도어 컨트롤러에서 AXIS OS를 업그레이드할 때 다음 사항에 유의하십시오.

- **지원되는 AXIS OS 버전:** 위에 나열된 지원되는 AXIS OS 버전은 기존의 권장 VMS 버전에서 업그레이드하고 시스템에 도어가 있는 경우에만 적용됩니다. 시스템이 이 조건을 충족하지 않으면, 해당 VMS 버전에 권장되는 AXIS OS 버전으로 업그레이드해야 합니다.
- **지원되는 최소 AXIS OS 버전:** 시스템에 설치된 가장 오래된 AXIS OS 버전이 지원되는 최소 AXIS OS 버전을 결정하며, 최대 두 개의 이전 버전까지만 지원됩니다.
- **권장 AXIS OS 버전 이상으로 업그레이드:** 특정 VMS 버전에 권장되는 버전보다 높은 AXIS OS 버전으로 업그레이드하는 경우를 가정해 보십시오. VMS 버전에 설정된 지원 범위 내라면, 언제든지 문제 없이 권장 AXIS OS 버전으로 다시 다운그레이드할 수 있습니다.
- **향후 AXIS OS 권장 사항:** 시스템 안정성과 완벽한 호환성을 위해, 항상 해당 VMS 버전에 권장되는 AXIS OS 버전을 따르십시오.

접근 제어 통합

VMS에 접근 제어를 통합하는 방법:

1. **Site Navigation(사이트 탐색)** > **Access Control(접근 제어)**로 이동합니다.
2. **Access Control(접근 제어)**를 마우스 오른쪽 버튼으로 클릭하고 **Create new...(새로 만들기...)**를 클릭합니다.
3. **Create Access Control System Integration(접근 제어 시스템 통합 만들기)** 대화 상자에서:
   - 통합의 이름을 입력합니다.
   - **Integration plug-in(통합 플러그인)**에서 드롭다운 메뉴에서 **AXIS Secure Entry**를 선택합니다.
   - **Associate cameras(카메라 연결)** 대화 상자가 표시될 때까지 **Next(다음)**를 클릭합니다.
     도어 액세스 포인트에 카메라를 연결하는 방법:
     - **Cameras(카메라)**에서 장치를 클릭하여 XProtect 시스템에 구성된 카메라 목록을 확인합니다.
     - 카메라를 선택하여 연결하려는 출입 지점으로 드래그합니다.
     - **Close(닫기)**를 클릭하여 대화 상자를 닫습니다.

비고

- XProtect의 접근 제어 통합에 대한 자세한 내용은 *XProtect Smart Client에서 접근 제어 사용하기*를 참조하십시오.
- 일반 설정, 도어 및 연결 카메라, 접근 제어 이벤트 등 접근 제어 속성에 대한 자세한 내용은 *접근 제어 속성*을 참조하십시오.

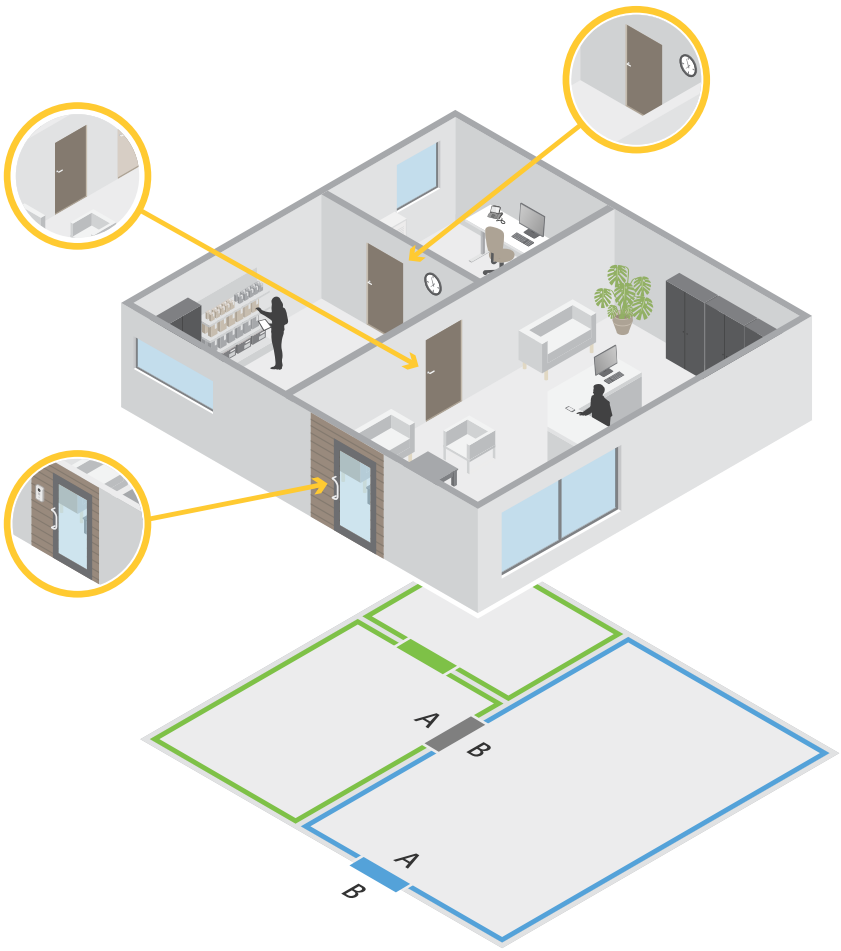
도어 및 영역

Site Navigation(사이트 탐색) > **Axis Optimizer** > **Access control(접근 제어)** > **Doors and zones (도어 및 구역)**로 이동하여 오버뷰를 확인하고 도어 및 구역을 구성합니다.

PIN 차트	도어와 관련된 컨트롤러 핀 차트를 봅니다. 핀 차트를 인쇄하려면 **Print(인쇄)**를 클릭합니다.
식별 프로파일	도어의 식별 프로파일을 변경합니다.
보안 채널	특정 리더에 대한 OSDP 보안 채널을 켜거나 끕니다.

도어	
이름	도어의 이름입니다.
도어 컨트롤러	도어에 연결된 도어 컨트롤러입니다.
A 사이드	도어의 측면 A가 속해 있는 영역입니다.
측면 B	도어의 측면 B가 속해 있는 영역입니다.
식별 프로파일	도어에 적용된 식별 프로파일입니다.
카드 형식 및 PIN	카드 형식 유형이나 핀 길이를 표시합니다.
상태	도어의 상태입니다. • **온라인:** 도어가 온라인 상태이며 올바르게 작동합니다. • **Reader offline(리더 오프라인):** 도어 구성의 리더가 오프라인 상태입니다. • **리더 오류:** 도어 구성의 리더가 보안 채널을 지원하지 않거나 리더에 대한 보안 채널이 꺼져 있습니다.
영역	
이름	영역의 이름입니다.
도어 수	영역에 포함된 도어의 수입니다.

도어 및 영역의 예



- 녹색 영역과 파란색 영역의 두 가지 영역이 있습니다.
- 녹색 도어, 파란색 도어, 갈색 도어 등 세 개의 도어가 있습니다.
- 녹색 도어는 녹색 영역의 내부 도어입니다.
- 파란색 도어는 파란색 영역 전용 경계구역 도어입니다.
- 갈색 도어는 녹색 영역 및 파란색 영역 양쪽의 경계구역 도어입니다.

도어 추가

비고

- 도어 하나에 잠금 두 개가 있는 도어 또는 도어 두 개에 각각 잠금이 하나씩 있는 도어 컨트롤러로 구성할 수 있습니다.
- 도어 컨트롤러에 도어가 없고 최신 AXIS Optimizer와 구형 도어 컨트롤러 소프트웨어를 함께 사용하는 경우 시스템은 도어 추가를 허용하지 않습니다. 다만, 기존 도어가 이미 있는 경우 구형 소프트웨어를 사용하는 시스템 컨트롤러에서 새 도어를 허용합니다.

새 도어 구성을 생성하여 도어를 추가합니다.

1. **Site Navigation(사이트 탐색)** > **AXIS Optimizer** > **Access control(접근 제어)** > **Doors and zones(도어 및 구역)**로 이동합니다.
2. + **Add door(도어 추가)**를 클릭합니다.
3. 도어 이름을 입력합니다.

4. **Controller(컨트롤러)** 드롭다운 메뉴에서 도어 컨트롤러를 선택합니다. 다른 도어를 추가할 수 없거나, 오프라인 상태이거나, HTTPS가 활성화되지 않은 경우 컨트롤러가 회색으로 표시됩니다.
5. **Door type(도어 유형)** 드롭다운 메뉴에서 생성하려는 도어 유형을 선택합니다.
6. **Next(다음)**를 클릭하여 도어 구성 페이지로 이동합니다.
7. **Primary lock(기본 잠금)** 드롭다운 메뉴에서 릴레이 포트를 선택합니다.
8. 도어에 잠금 두 개를 구성하려면 **Secondary lock(보조 잠금)** 드롭다운 메뉴에서 릴레이 포트 하나를 선택합니다.
9. 식별 프로파일을 선택합니다. 을 참조하십시오.
10. 도어 설정을 구성합니다. 을 참조하십시오.
11. 모니터링 도어를 설정합니다. 를 참조하십시오.
12. **Save(저장)**를 클릭합니다.

기존 도어 구성을 복사하여 도어를 추가합니다.

1. **Site Navigation(사이트 탐색)** > **AXIS Optimizer** > **Access control(접근 제어)** > **Doors and zones(도어 및 구역)**로 이동합니다.
2. **Add door(도어 추가)**를 클릭합니다.
3. 도어 이름을 입력합니다.
4. **Controller(컨트롤러)** 드롭다운 메뉴에서 도어 컨트롤러를 선택합니다.
5. **Next (다음)**를 클릭합니다.
6. **Copy configuration(구성 복사)** 드롭다운 메뉴에서 기존 도어 구성을 선택합니다. 연결된 도어가 표시되며, 도어가 두 개로 구성된 경우 컨트롤러가 회색으로 표시되고, 잠금 두 개가 있는 도어가 하나 있으면 컨트롤러가 회색으로 표시됩니다.
7. 원하는 경우 설정을 변경합니다.
8. **Save(저장)**를 클릭합니다.

도어를 편집하려면

1. **Site Navigation(사이트 탐색)** > **AXIS Optimizer** > **Access control(접근 제어)** > **Doors and zones(도어 및 구역)** > **Doors(도어)**로 이동합니다.
2. 목록에서 도어를 선택합니다.
3. **Edit(편집)**를 클릭합니다.
4. 설정을 변경하고 **Save(저장)**를 클릭합니다.

도어를 제거하려면

1. **Site Navigation(사이트 탐색)** > **AXIS Optimizer** > **Access control(접근 제어)** > **Doors and zones(도어 및 구역)** > **Doors(도어)**로 이동합니다.
2. 목록에서 도어를 선택합니다.
3. **Remove(제거)**를 클릭합니다.
4. **예**를 클릭합니다.

도어 이름을 추가, 제거 또는 편집할 때마다 변경 사항을 VMS에 통합하는 방법:

1. **Site Navigation(사이트 탐색)** > **Access control(접근 제어)**로 이동하여 Access Control integration(접근 제어 통합)을 클릭합니다.
2. **General settings(일반 설정)** 탭에서 **Refresh Configuration(구성 새로 고침)**을 클릭합니다.

도어 설정

1. **Site Navigation(사이트 탐색)** > **AXIS Optimizer** > **Access control(접근 제어)** > **Doors and zones(도어 및 구역)**로 이동합니다.
2. 편집할 도어를 선택합니다.
3. **Edit(편집)**를 클릭합니다.

접근 시간(초)	접근 권한이 부여된 후 도어가 잠금 해제된 상태로 유지되는 시간(초)을 설정합니다. 도어가 열릴 때까지 또는 설정된 시간이 끝날 때까지 도어의 잠금 해제 상태를 유지합니다. 접근 시간이 남아 있어도 도어가 닫히면 잠깁니다.
Open-too-long time (sec)(장시간 개방(초))	도어 모니터를 구성한 경우에만 유효합니다. 도어가 열려 있는 시간(초)을 설정합니다. 설정된 시간이 끝날 때 도어가 열려 있으면 도어가 장시간 개방되어 있다는 알람이 트리거됩니다. 액션 룰을 설정하여 장시간 개방 이벤트가 트리거하는 작업을 구성합니다.
긴 접근 시간(초)	접근 권한이 부여된 후 도어가 잠금 해제된 상태로 유지되는 시간(초)을 설정합니다. 긴 접근 시간은 이 설정이 켜진 상태인 카드 소지자의 접근 시간을 재정의합니다.
Long open-too-long time (sec)(긴 장시간 개방(초))	도어 모니터를 구성한 경우에만 유효합니다. 도어가 열려 있는 시간(초)을 설정합니다. 설정된 시간이 끝날 때 도어가 열려 있으면 도어가 장시간 개방되어 있다는 이벤트가 트리거됩니다. **Long access time(긴 접근 시간)** 설정을 켜면 너무 오래 열려 있는 경우 카드 소지자에 대해 이미 설정된 긴 장시간 개방을 재정의합니다.
다시 잠금 지연 시간(ms)	도어가 열리거나 닫힌 후 도어가 잠기지 않은 상태로 유지되는 시간(밀리초)을 설정합니다.
다시 잠그다	• **After opening(개방 후):** 도어 모니터를 추가한 경우에만 유효합니다. • **After closing(폐쇄 후):** 도어 모니터를 추가한 경우에만 유효합니다.

도어 보안 수준

도어에 다음 보안 기능을 추가할 수 있습니다.

2인 룰 - 2인 룰은 두 사람이 유효한 자격 증명을 사용하여 접근해야 합니다.

카드 두 번 대기 - 두 번 댄 카드 소지자는 도어의 현 상태를 무시할 수 있습니다. 예를 들어, 정규 시간 외에 도어를 잠금 또는 잠금 해제하는 데 사용할 수 있어 시스템으로 들어가서 도어를 잠금 해제하는 것보다 더 편리합니다. 카드 두 번 대기는 기존 일정에 영향을 주지 않습니다. 예를 들어, 도어가 닫히는 시간에 잠기도록 예약되어 있고 직원이 점심 시간에 퇴근하는 경우에도 도어는 일정에 따라 잠깁니다.

새 도어를 추가하는 동안 보안 수준을 구성하거나 기존 도어에서 보안 수준을 구성해도 됩니다.

기존 문에 **2인 룰**을 추가하려면 다음을 수행합니다.

1. **Site Navigation(사이트 탐색)** > **AXIS Optimizer** > **Access control(접근 제어)** > **Doors and zones(도어 및 구역)**로 이동합니다.

2. 보안 수준을 구성하려는 도어를 선택합니다.
3. **Edit(편집)**를 클릭합니다.
4. **Security level(보안 수준)**을 클릭합니다.
5. **Two-person rule(2인 룰)**을 켭니다.
6. **적용**을 클릭합니다.

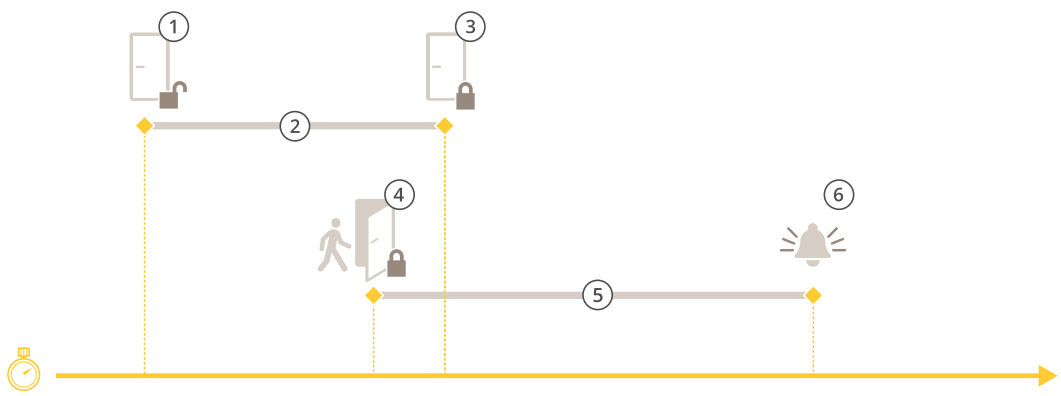
2인 룰	
Side A(측면 A) 및 **Side B(측면 B)**	룰을 사용할 도어의 측면을 선택합니다.
일정	룰이 활성화되는 시기를 선택합니다.
시간 초과(초)	시간 초과는 카드 긁기 또는 다른 유형의 유효한 자격 증명 사이에 허용되는 최대 시간입니다.

기존 도어에 **카드 두 번 대기**를 추가하려면 다음을 수행합니다.

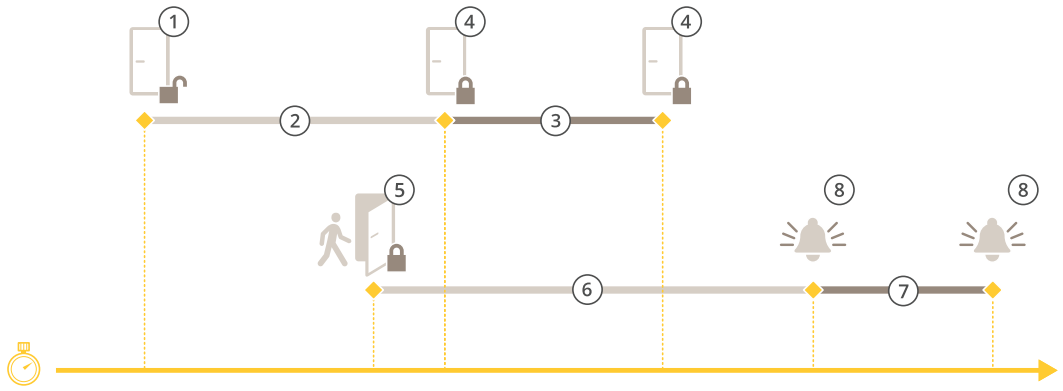
1. **Site Navigation(사이트 탐색)** > **AXIS Optimizer** > **Access control(접근 제어)** > **Doors and zones(도어 및 구역)**로 이동합니다.
2. 보안 수준을 구성하려는 도어를 선택합니다.
3. **Edit(편집)**를 클릭합니다.
4. **Security level(보안 수준)**을 클릭합니다.
5. **Double-swipe(카드 두 번 대기)**를 켭니다.
6. **적용**을 클릭합니다.
7. 카드 소지자에게 **Double-swipe(카드 두 번 대기)**를 적용합니다.
   7.1. **Cardholder management(카드 소지자 관리)**로 이동합니다.
   7.2. 편집할 카드 소지자의 ⋮ 을 클릭하고 **Edit(편집)**을 클릭합니다.
   7.3. **More(자세히)**를 클릭합니다.
   7.4. **Allow double-swipe(카드 두 번 대기 허용)**를 선택합니다.
   7.5. **적용**을 클릭합니다.

카드 두 번 대기	
시간 초과(초)	시간 초과는 카드 긁기 또는 다른 유형의 유효한 자격 증명 사이에 허용되는 최대 시간입니다.

시간 옵션



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



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

도어 모니터 추가

도어 모니터는 도어의 물리적 상태를 모니터링하는 도어 위치 스위치입니다. 사용자는 도어에 도어 모니터를 추가하고 도어 모니터 연결 방식을 구성할 수 있습니다.

1. 도어 구성 페이지로 이동합니다. 를 참조하십시오.
2. **Sensors(센서)**에서 **Add(추가)**를 클릭합니다.
3. **Door monitor sensor(도어 모니터 센서)**를 선택합니다.
4. 도어 모니터를 연결할 I/O 포트를 선택합니다.
5. **Door open if(도어가 열리면)**에서 도어 모니터 회로의 연결 방법을 선택합니다.
6. 새로운 안정 상태에 도달하기 전에 디지털 입력의 상태 변경을 무시하려면 **Debounce time (디바운스 시간)**을 설정하십시오.
7. 도어 컨트롤러 및 도어 모니터 간에 연결이 중단되었을 때 이벤트를 트리거하려면 **Supervised input(관리된 입력)**을 켭니다. 을 참조하십시오.

도어가 열리면	
회로가 개방되었습니다	도어 모니터 회로는 정상 폐쇄 상태입니다. 회로가 열리면 도어 모니터가 도어 개방 신호를 보냅니다. 회로가 닫히면 도어 모니터가 도어 폐쇄 신호를 보냅니다.
회로가 폐쇄되었습니다	도어 모니터 회로는 정상 개방 상태입니다. 회로가 닫히면 도어 모니터가 도어 개방 신호를 보냅니다. 회로가 열리면 도어 모니터가 도어 폐쇄 신호를 보냅니다.

모니터링 도어 추가

모니터링 도어는 도어가 열려 있는지 또는 닫혀 있는지 확인할 수 있는 도어 유형입니다. 예를 들어 잠금 장치가 필요하지 않지만 도어가 열려 있는지 확인해야 하는 방화문에 이 기능을 사용할 수 있습니다.

모니터링 도어는 도어 모니터가 있는 일반 도어와 다릅니다. 도어 모니터가 있는 일반 도어는 잠금 장치와 리더를 지원하지만 도어 컨트롤러가 필요합니다. 모니터링 도어는 하나의 도어 위치 센서를 지원하지만 도어 컨트롤러에 연결된 네트워크 I/O 릴레이 모듈만 있으면 됩니다. 하나의 네트워크 I/O 릴레이 모듈에 최대 5개의 도어 위치 센서를 연결할 수 있습니다.

비고

모니터링 도어에는 AXIS Monitoring Door ACAP 애플리케이션을 포함한 최신 소프트웨어가 설치된 AXIS A9210 Network I/O Relay Module이 필요합니다.

모니터링 도어를 설정하려면 다음을 수행합니다.

1. AXIS A9210을 설치하고 최신 버전의 AXIS OS로 업그레이드합니다.
2. 도어 위치 센서를 설치합니다.
3. VMS에서 **Site Navigation(사이트 탐색)** > **AXIS Optimizer** > **Access control(접근 제어)** > **Doors and zones(도어 및 구역)**로 이동합니다.
4. **Add door(도어 추가)**를 클릭합니다.
5. 이름을 입력합니다.
6. **Type(유형)**에서 **Monitoring door(모니터링 도어)**를 선택합니다.
7. **Device(장치)**에서 네트워크 I/O 릴레이 모듈을 선택합니다.
8. **Next (다음)**를 클릭합니다.
9. **Sensors(센서)**에서 **+ Add(+ 추가)**를 클릭하고 **Door position sensor(도어 위치 센서)**를 선택합니다.
10. 도어 위치 센서에 연결된 I/O를 선택합니다.
11. **추가**를 클릭합니다.

리더 추가

도어 컨트롤러가 두 개의 유선 리더를 사용하도록 구성할 수 있습니다. 사용자는 도어 한 측면이나 양면에 리더를 추가하려면 선택합니다.

리더에 **Card formats(카드 형식)** 또는 핀 길이의 사용자 지정 설정을 적용하는 경우 **Configuration > Access control > Doors and zones(구성 > 접근 제어 > 도어 및 영역)**의 카드 형식에서 확인할 수 있습니다. 을 참조하십시오.

1. 도어 구성 페이지로 이동합니다. 를 참조하십시오.
2. 도어의 한 측면에서 **Add(추가)**를 클릭합니다.
3. **Card reader(카드 리더)**를 선택합니다.
4. **Reader type(리더 유형)**을 선택합니다.
5. 이 리더에 사용자 지정 핀 길이 설정을 사용합니다.
   5.1. **고급**을 클릭합니다.
   5.2. **Custom PIN length(사용자 지정 핀 길이)**를 켭니다.
   5.3. **Min PIN length(최소 핀 길이)**, **Max PIN length(최대 핀 길이)** 및 **End of PIN character(핀 문자 끝)**를 설정합니다.
6. 이 리더에 사용자 지정 카드 형식을 사용합니다.
   6.1. **고급**을 클릭합니다.
   6.2. **Custom card formats(사용자 지정 카드 형식)**를 켭니다.

6.3. 리더에 사용하려는 카드 형식을 선택합니다. 비트 길이가 동일한 카드 형식을 이미 사용 중인 경우 먼저 이를 비활성화해야 합니다. 카드 형식 설정이 구성된 시스템 설정과 다르면 클라이언트에서 경고 아이콘이 표시됩니다.

7. **추가**를 클릭합니다.
8. 도어 반대편에 리더를 추가하려면 이 절차를 다시 반복합니다.

리더 유형	
OSDP RS485 half duplex(OSDP RS485 반이중)	RS485 리더의 경우 **OSDP RS485 half duplex (OSDP RS485 반이중)** 및 리더 포트를 선택합니다.
Wiegand	Wiegand 프로토콜을 사용하는 리더의 경우 **Wiegand** 및 리더 포트를 선택합니다.

Wiegand	
LED 제어	**Single wire(단일 와이어)** 또는 **Dual wire (R/G) (이중 와이어(R/G))**를 선택합니다. 이중 LED 컨트롤을 가진 리더는 빨간색 LED와 녹색 LED에 서로 다른 와이어를 사용합니다.
탬퍼 경보	리더 변조 입력이 활성화된 경우를 선택합니다. • **Open circuit(개방 회로)**: 회로가 개방되면 리더가 도어에 변조 신호를 보냅니다. • **Closed circuit(폐쇄 회로)**: 회로가 폐쇄되면 리더가 도어에 변조 신호를 보냅니다.
Tamper debounce time(탬퍼 디바운스 시간)	새로운 안정 상태에 도달하기 전에 리더 탬퍼 입력의 상태 변경을 무시하려면 **Tamper debounce time(탬퍼 디바운스 시간)**을 설정합니다.
관리된 입력	도어 컨트롤러 및 리더 간에 연결이 중단되었을 때 이벤트를 트리거하려면 켭니다. 을 참조하십시오.

REX 장치 추가

사용자는 도어 한쪽 면이나 양면에 퇴실 요청(REX) 장치 추가를 선택할 수 있습니다. REX 장치는 PIR 센서, REX 버튼 또는 푸시 바일 수 있습니다.

1. 도어 구성 페이지로 이동합니다. 를 참조하십시오.
2. 도어의 한 측면에서 **Add(추가)**를 클릭합니다.
3. **REX device(REX 장치)**를 선택합니다.
4. REX 장치를 연결하려는 I/O 포트를 선택합니다. 사용 가능한 포트가 하나뿐인 경우 이 포트가 자동으로 선택됩니다.
5. 도어가 REX 신호를 수신할 때 트리거할 **Action(액션)**을 선택합니다.
6. **REX active(REX 활성)**에서 도어 모니터 회로 연결을 선택합니다.
7. 새로운 안정 상태에 도달하기 전에 디지털 입력의 상태 변경을 무시하려면 **Debounce time (디바운스 시간(ms))**을 설정합니다.
8. 도어 컨트롤러와 REX 장치 간의 연결이 중단될 때 이벤트를 트리거하려면 **Supervised input (관리된 입력)**을 켭니다. 을 참조하십시오.

액션	
도어 잠금 해제	REX 신호가 수신되어 도어의 잠금을 해제하려면 선택합니다.
없음	도어가 REX 신호를 수신할 때 어떤 액션도 트리거하지 않으려면 선택합니다.

REX 활성화	
회로가 개방되었습니다	REX 회로가 정상 폐쇄된 경우에 선택합니다. REX 장치는 회로가 개방되었을 때 신호를 보냅니다.
회로가 폐쇄되었습니다	REX 회로가 정상 개방된 경우에 선택합니다. REX 장치는 회로가 폐쇄되었을 때 신호를 보냅니다.

영역 추가

영역은 도어 그룹이 속해 있는 특정한 물리적 영역입니다. 사용자는 영역을 생성하고 영역에 도어를 추가할 수 있습니다. 두 가지 유형의 도어가 있습니다.

- **Perimeter door:(경계구역 도어:)** 카드 소지자는 이 도어를 통해 영역을 출입합니다.
- **Internal door:(내부 도어:)** 영역 안의 내부 도어입니다.

비고

경계구역 도어는 두 영역에 속할 수 있습니다. 내부 도어는 한 영역에만 속할 수 있습니다.

1. **Site Navigation(사이트 탐색)** > **AXIS Optimizer** > **Access control(접근 제어)** > **Doors and zones(도어 및 구역)** > **Zones(구역)**로 이동합니다.
2. **Add zone(영역 추가)**을 클릭합니다.
3. 영역 이름을 입력합니다.
4. **Add door(도어 추가)**를 클릭합니다.
5. 영역에 추가할 도어를 선택하고 **Add(추가)**를 클릭합니다.
6. 도어는 기본적으로 경계구역 도어로 설정되어 있습니다. 이를 변경하려면 드롭다운 메뉴에서 **Internal door(내부 도어)**를 선택합니다.
7. 경계구역 도어는 기본적으로 도어 측면 A를 영역 입구로 사용합니다. 이를 변경하려면 드롭다운 메뉴에서 **Leave(나가기)**를 선택합니다.
8. 영역에서 도어를 제거하려면 도어를 선택하고 **Remove(제거)**를 클릭합니다.
9. **Save(저장)**를 클릭합니다.

영역을 편집하려면 다음을 수행합니다.

1. **Site Navigation(사이트 탐색)** > **AXIS Optimizer** > **Access control(접근 제어)** > **Doors and zones(도어 및 구역)** > **Zones(구역)**로 이동합니다.
2. 목록에서 영역을 선택합니다.
3. **Edit(편집)**를 클릭합니다.
4. 설정을 변경하고 **Save(저장)**를 클릭합니다.

영역을 제거하려면

1. **Site Navigation(사이트 탐색)** > **AXIS Optimizer** > **Access control(접근 제어)** > **Doors and zones(도어 및 구역)** > **Zones(구역)**로 이동합니다.

2. 목록에서 영역을 선택합니다.
3. **Remove(제거)**를 클릭합니다.
4. **예**를 클릭합니다.

영역 보안 수준

영역에 다음 보안 기능을 추가할 수 있습니다.

지정 통로 출입 방식 - 다른 사람들이 자신보다 먼저 구역에 입장한 사람과 동일한 자격 증명을 사용하는 것을 방지합니다. 자격 증명을 다시 사용하려면 먼저 해당 구역에서 나가야 합니다.

비고

- 지정 통로 출입 방식을 사용하면 해당 영역의 모든 도어에 도어 위치 센서가 있어야 사용자가 카드를 대고 도어를 열었다는 사실을 시스템에서 등록할 수 있습니다.
- 도어 컨트롤러가 오프라인 상태가 되면 해당 영역의 모든 도어가 동일한 도어 컨트롤러에 속해 있는 한 지정 통로 출입 방식이 작동합니다. 하지만 해당 영역의 도어가 서로 다른 도어 컨트롤러에 속해 오프라인 상태가 되면 지정 통로 출입 방식이 작동하지 않습니다.

새 영역을 추가하는 동안 보안 수준을 구성하거나 기존 영역에서 구성할 수 있습니다. 기존 영역에 보안 수준을 추가하려면 다음을 수행합니다.

1. **Site Navigation(사이트 탐색)** > **AXIS Optimizer** > **Access control(접근 제어)** > **Doors and zones(도어 및 구역)**로 이동합니다.
2. 보안 수준을 구성하려는 영역을 선택합니다.
3. **Edit(편집)**를 클릭합니다.
4. **Security level(보안 수준)**을 클릭합니다.
5. 도어에 추가하려는 보안 기능을 켭니다.
6. **적용**을 클릭합니다.

지정 통로 출입 방식	
Log violation only (Soft)(로그 위반만(소프트))	두 번째 사람이 첫 번째 사람과 동일한 자격 증명을 사용하여 도어에 들어갈 수 있도록 하려면 이 옵션을 사용합니다. 이 옵션은 시스템 알람만 발생시킵니다.
Deny access (Hard)(액세스 거부(하드))	두 번째 사용자가 첫 번째 사람과 동일한 자격 증명을 사용하는 경우 두 번째 사용자가 도어에 들어가는 것을 방지하려면 이 옵션을 사용합니다. 이 옵션도 시스템 알람을 발생시킵니다.
시간 초과(초)	시스템이 사용자의 재진입을 허용할 때까지의 시간입니다. 시간 초과를 원하지 않을 경우 0을 입력합니다. 이제, 사용자가 해당 영역을 떠날 때까지 해당 영역에 지정 통로 출입 방식이 적용됩니다. 해당 영역의 모든 도어 양쪽에 리더가 있는 경우 **Deny access (Hard)(액세스 거부(하드))**와 함께 **0** 타임아웃만 사용하십시오.

관리된 입력

관리된 입력은 도어 컨트롤러로의 연결이 중단될 때 이벤트를 트리거할 수 있습니다.

- 도어 컨트롤러와 도어 모니터 간의 연결. 를 참조하십시오.
- 도어 컨트롤러와 Wiegand 프로토콜을 사용하는 리더 간의 연결. 를 참조하십시오.
- 도어 컨트롤러와 REX 장치 간의 연결. 를 참조하십시오.

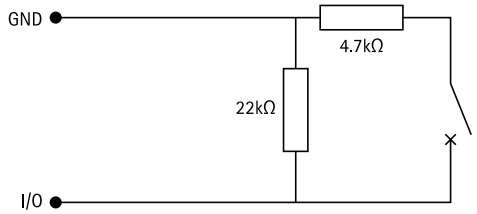
관리된 입력을 사용하려면

1. 연결 다이어그램에 따라 EOL 레지스터를 주변 장치에 최대한 가깝게 설치하십시오.
2. 리더, 도어 모니터 또는 REX 장치의 구성 페이지로 이동하여 **Supervised input(관리된 입력)**을 켭니다.
3. 병렬 우선 연결 다이어그램을 따른 경우 **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.
4. 직렬 우선 연결 다이어그램을 따른 경우 **Serial first connection(직렬 우선 연결)**을 선택하고 **Resistor values(저항 값)** 드롭다운 메뉴에서 저항 값을 선택합니다.

연결 다이어그램

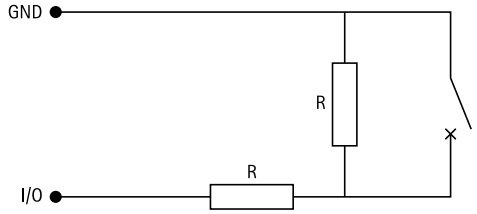
병렬 우선 연결

저항 값은 4.7kΩ 및 22kΩ이어야 합니다.



직렬 우선 연결

저항 값은 동일해야 하며 1-10 kΩ 범위 내에 있어야 합니다.



수동 액션

도어 및 영역에 대해 다음과 같은 수동 액션을 수행할 수 있습니다.

재설정 - 구성된 시스템 룰로 돌아갑니다.

액세스 권한 부여 - 7초 동안 도어 또는 영역의 잠금을 해제했다가 다시 잠급니다.

잠금 해제 - 재설정할 때까지 도어를 잠금 해제 상태로 유지합니다.

잠금 - 시스템에서 카드 소지자의 액세스를 허용할 때까지 도어를 잠금 상태로 유지합니다.

차단 - 재설정하거나 잠금을 해제할 때까지 아무도 출입할 수 없습니다.

수동 액션을 수행하려면 다음을 수행합니다.

1. **Site Navigation(사이트 탐색)** > **AXIS Optimizer** > **Access control(접근 제어)** > **Doors and zones(도어 및 구역)**로 이동합니다.
2. 수동 액션을 수행할 도어 또는 영역을 선택합니다.
3. 수동 액션을 클릭합니다.

카드 형식 및 PIN

카드 형식은 카드에 데이터가 저장되는 방식을 정의합니다. 이는 들어오는 데이터 및 시스템에서 유효성이 검사된 데이터 간의 변환 표입니다. 각 카드 형식에는 저장된 정보를 구성하는 방법에 대한 서

로 다른 룰이 있습니다. 카드 형식을 정의함으로써 컨트롤러가 카드 리더로부터 받는 정보를 어떻게 해석할지를 시스템에 알려줄 수 있습니다.

일반적으로 사용되는 카드 형식이 미리 정의되어 있어 그대로 사용하거나 필요에 따라 편집할 수 있습니다. 사용자 지정 카드 형식을 만들 수도 있습니다.

Site Navigation(사이트 탐색) > **AXIS Optimizer** > **Access control(접근 제어)** > **Card formats and PIN(카드 형식 및 PIN)**으로 이동하여 카드 형식을 생성, 편집 또는 활성화합니다. 또한, 핀을 구성할 수 있습니다.

사용자 지정 카드 형식에는 자격 증명 확인에 사용되는 다음 데이터 필드가 포함될 수 있습니다.

카드 번호 - 10진수 또는 16진수로 인코딩된 자격 증명 이진 데이터의 하위 집합입니다. 카드 번호로 특정 카드 또는 카드 소지자를 식별합니다.

시설 코드 - 10진수 또는 16진수로 인코딩된 자격 증명 이진 데이터의 하위 집합입니다. 시설 코드로 특정 최종 고객 또는 사이트를 식별합니다.

카드 형식을 만들려면

1. **Site Navigation(사이트 탐색)** > **AXIS Optimizer** > **Access control(접근 제어)** > **Card formats and PIN(카드 형식 및 PIN)**으로 이동합니다.
2. **Add card format(카드 형식 추가)**을 클릭합니다.
3. 카드 형식 이름을 입력합니다.
4. **Bit length(비트 길이)** 필드에서 1에서 256 사이의 비트 길이를 입력합니다.
5. 카드 리더로부터 수신한 데이터의 비트 순서를 역순으로 바꾸고자 하는 경우 **Invert bit order (비트 순서 반전)**를 선택합니다.
6. 카드 리더로부터 수신한 데이터의 바이트 순서를 역순으로 바꾸고자 하는 경우 **Invert byte order(바이트 순서 반전)**를 선택합니다. 이 옵션은 8로 나눌 수 있는 비트 길이를 지정하는 경우에만 사용할 수 있습니다.
7. 카드 형식에서 활성화할 데이터 필드를 선택하고 구성합니다. **Card number(카드 번호)** 또는 **Facility code(시설 코드)** 중 하나는 반드시 카드 형식으로 활성화되어야 합니다.
8. **OK(확인)**를 클릭합니다.
9. 카드 형식을 활성화하려면 카드 형식 이름 앞의 확인란을 선택합니다.

비고

- 비트 길이가 동일한 두 카드 형식을 동시에 활성화할 수 없습니다. 가령 32비트 카드 형식 두 개를 정의한 경우 이 중 하나만 활성화할 수 있습니다. 한 카드 형식을 비활성화하면 다른 형식을 활성화할 수 있습니다.
- 도어 컨트롤러에 하나 이상의 리더가 구성된 경우에만 카드 형식을 활성화 및 비활성화할 수 있습니다.

ⓘ	비트 순서를 반전한 후 출력의 예시를 보려면 ⓘ 을 클릭합니다.
범위	데이터 필드에 대한 데이터의 비트 범위를 설정합니다. 범위는 사용자가 **Bit length(비트 길이)**로 지정한 분량 이내여야 합니다.

출력 형식	데이터 필드에 대한 데이터의 출력 형식을 선택합니다. **Decimal(십진수)**: 기본 10진법이라고도 하며 숫자 0-9로 구성됩니다. **Hexadecimal(16진수)**: 16진수 체계라고도 하며, 숫자 0-9와 문자 a-f 등 16개의 고유 기호로 구성됩니다.
하위 범위의 비트 순서	비트 순서를 선택합니다. **Little-endian**: 첫 번째 비트는 가장 작은(최하위) 비트입니다. **Big-endian**: 첫 번째 비트가 가장 큰(최상위) 비트입니다.

카드 형식을 편집하려면

1. **Site Navigation(사이트 탐색)** > **AXIS Optimizer** > **Access control(접근 제어)** > **Card formats and PIN(카드 형식 및 PIN)**으로 이동합니다.
2. 카드 형식을 선택하고 을 클릭합니다.
3. 사전 정의된 카드 형식을 편집하면 **Invert bit order(비트 순서 반전)** 및 **Invert byte order(바이트 순서 반전)**만 편집할 수 있습니다.
4. **OK(확인)**를 클릭합니다.

사용자는 사용자 지정 카드 형식만 제거할 수 있습니다. 사용자 지정 카드 형식을 제거하려면 다음을 수행합니다.

1. **Site Navigation(사이트 탐색)** > **AXIS Optimizer** > **Access control(접근 제어)** > **Card formats and PIN(카드 형식 및 PIN)**으로 이동합니다.
2. 사용자 지정 카드 형식을 선택하고, 및 **Yes(예)**를 클릭합니다.

사전 정의된 카드 형식을 재설정하려면 다음을 수행합니다.

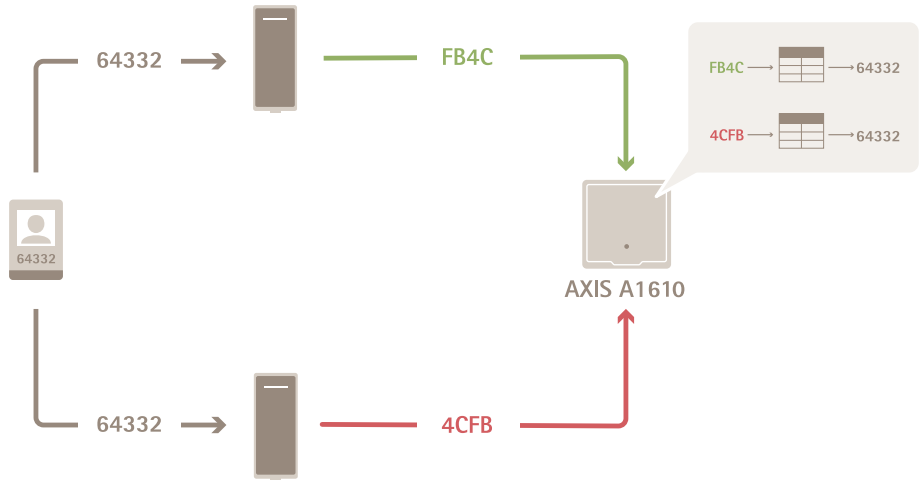
1. **Site Navigation(사이트 탐색)** > **AXIS Optimizer** > **Access control(접근 제어)** > **Card formats and PIN(카드 형식 및 PIN)**으로 이동합니다.
2. 카드 형식을 기본 필드 지도로 재설정하려면 을 클릭합니다.

핀 길이를 구성하려면 다음을 수행합니다.

1. **Site Navigation(사이트 탐색)** > **AXIS Optimizer** > **Access control(접근 제어)** > **Card formats and PIN(카드 형식 및 PIN)**으로 이동합니다.
2. **PIN configuration(PIN 구성)**에서 을 클릭합니다.
3. **Min PIN length(최소 PIN 길이)**, **Max PIN length(최대 PIN 길이)** 및 **End of PIN character (PIN 문자 끝)**를 지정합니다.
4. **OK(확인)**를 클릭합니다.

카드 형식 설정

개요



- 십진수로 표시된 카드 번호는 `64332`입니다.
- 어느 한 리더에 의해 카드 번호가 16진수 `FB4C`로 변환됩니다. 다른 한 리더는 이를 16진수 `4CFB`로 변환합니다.
- AXIS A1610 Network Door Controller는 `FB4C`를 수신하고 해당 리더의 카드 형식 설정에 따라 이를 십진수 `64332`로 변환합니다.
- AXIS A1610 Network Door Controller는 `4CFB`를 수신하고, 바이트 순서를 반전시켜 `FB4C`로 변경한 후, 리더의 카드 포맷 설정에 따라 이를 십진수 `64332`로 변환합니다.

비트 순서 반전

비트 순서를 반전한 후 해당 리더로부터 수신된 카드 데이터는 비트 단위로 오른쪽에서 왼쪽으로 판독됩니다.

바이트 순서 반전

8비트를 하나로 묶어서 바이트라고 합니다. 바이트 순서를 반전한 후 해당 리더로부터 수신된 카드 데이터는 바이트 단위로 오른쪽에서 왼쪽으로 판독됩니다.

26비트 표준 Wiegand 카드 형식

1 선행 패리티
2 시설 코드
3 카드 번호

4 후행 패리티

식별 프로파일

식별 프로파일은 식별 유형 및 스케줄의 조합입니다. 도어 하나 이상에 식별 프로파일을 적용하여 카드 소지자가 도어에 접근할 수 있는 방법과 시기를 설정할 수 있습니다.

식별 유형은 도어에 접근하는 데 필요한 자격 증명 정보의 전달자입니다. 일반적인 식별 유형으로는 토큰, 개인 식별 번호(핀), 지문, 안면 인식, REX 장치 등이 있습니다. 식별 유형에는 정보 유형이 하나 이상 포함될 수 있습니다.

Time profiles(시간 프로파일)라고도 하는 스케줄은 Management Client에서 생성됩니다. 시간 프로파일 설정 방법은 *시간 프로파일(설명)*을 참조하십시오.

지원되는 식별 유형: 카드, PIN 및 REX.

Site Navigation(사이트 탐색) > **AXIS Optimizer** > **Access control(접근 제어)** > **Identification profiles(식별 프로파일)**로 이동합니다.

사용자가 그대로 사용하거나 필요에 따라 편집할 수 있는 기본 식별 프로파일이 다섯 개 있습니다.

카드 - 카드 소지자가 도어에 접근하려면 카드를 대야 합니다.

카드 및 PIN - 카드 소지자는 도어에 접근하기 위해 카드를 대고 핀을 입력해야 합니다.

핀 - 카드 소지자는 도어에 접근하기 위해 핀을 입력해야 합니다.

카드 또는 핀 - 카드 소지자는 도어에 접근하기 위해 카드를 대거나 핀을 입력해야 합니다.

번호판 - 카드 소지자는 승인된 번호판을 부착한 차량으로 카메라를 향해 운전해야 합니다.

식별 프로파일을 생성하려면

1. **Site Navigation(사이트 탐색)** > **AXIS Optimizer** > **Access control(접근 제어)** > **Identification profiles(식별 프로파일)**로 이동합니다.
2. **Create identification profile(식별 프로파일 생성)**을 클릭합니다.
3. 식별 프로파일 이름을 입력합니다.
4. **Include facility code for card validation(카드 검증용 시설 코드 포함)**을 선택하여 시설 코드를 자격 증명 확인 필드 중 하나로 사용합니다. **Access management > Settings(접근 관리 > 설정)**에서 **Facility code(시설 코드)**를 켜는 경우에만 이 필드를 사용할 수 있습니다.
5. 도어의 한 측면에 대한 식별 프로파일을 구성합니다.
6. 도어 반대편에서 이전 단계를 다시 반복합니다.
7. **OK(확인)**를 클릭합니다.

식별 프로파일을 편집하려면

1. **Site Navigation(사이트 탐색)** > **AXIS Optimizer** > **Access control(접근 제어)** > **Identification profiles(식별 프로파일)**로 이동합니다.
2. 식별 프로파일을 선택하고 을 선택합니다.
3. 식별 프로파일 이름을 변경하려면 새 이름을 입력합니다.
4. 도어의 측면을 편집합니다.
5. 도어 반대편의 식별 프로파일을 편집하려면 이전 단계를 다시 반복합니다.
6. **OK(확인)**를 클릭합니다.

식별 프로파일을 제거하려면 다음을 수행합니다.

1. **Site Navigation(사이트 탐색)** > **AXIS Optimizer** > **Access control(접근 제어)** > **Identification profiles(식별 프로파일)**로 이동합니다.

2. 식별 프로파일을 선택하고 을 선택합니다.
3. 도어에 식별 프로파일이 적용된 경우 해당 도어의 다른 식별 프로파일을 선택합니다.
4. **OK(확인)**를 클릭합니다.

식별 프로파일 편집	
×	식별 유형 및 관련 일정을 제거합니다.
식별 유형	식별 유형을 변경하려면 **Identification type(식별 유형)** 드롭다운 메뉴에서 유형을 하나 이상 선택합니다.
Schedule	일정을 변경하려면 **Schedule(일정)** 드롭다운 메뉴에서 일정을 하나 이상 선택합니다.
+ **추가**	식별 유형 및 관련 일정을 추가하려면 **Add(추가)**를 클릭하고 식별 유형 및 일정을 설정합니다.

암호화된 통신

OSDP 보안 채널

Secure Entry는 OSDP(Open Supervised Device Protocol) Secure Channel을 지원하여 컨트롤러와 AXIS 리더 사이에 회선 암호화를 활성화합니다.

전체 시스템에 대해 OSDP 보안 채널을 켜려면 다음을 수행합니다.

1. **Site Navigation(사이트 탐색)** > **AXIS Optimizer** > **Access control(접근 제어)** > **Encrypted communication(암호화 통신)**으로 이동합니다.
2. 기본 암호화 키를 입력하고 **OK(확인)**를 클릭합니다.
3. **OSDP Secure Channel(OSDP 보안 채널)**을 켭니다. 기본 암호화 키를 입력한 후에만 이 옵션을 사용할 수 있습니다.
4. 기본적으로 기본 암호화 키는 OSDP 보안 채널 키를 생성합니다. 다음과 같이 OSDP 보안 채널 키를 수동으로 설정합니다.
   4.1. **OSDP Secure Channel(OSDP 보안 채널)**에서, 을 클릭합니다.
   4.2. **Use main encryption key to generate OSDP Secure Channel key(기본 암호화 키를 사용하여 OSDP 보안 채널 키 생성)**를 지웁니다.
   4.3. OSDP 보안 채널 키를 입력하고 **OK(확인)**를 클릭합니다.

특정 리더에 대해 OSDP Secure Channel을 켜거나 끄려면 *도어 및 영역*을 참조하십시오.

다중 서버 BETA

연결된 하위 서버는 다중 서버를 통해 기본 서버의 전역 카드 소지자 및 카드 소지자 그룹을 사용할 수 있습니다.

비고

- 한 시스템은 하위 서버를 최대 64개까지 지원할 수 있습니다.
- 주 서버와 하위 서버가 동일한 네트워크에 있어야 합니다.
- 주 서버 및 하위 서버에서 보안 항목 포트에서 들어오는 TCP 연결을 허용하도록 Windows 방화벽을 구성해야 합니다. 기본 포트는 53461입니다.

작업 흐름

1. 서버를 하위 서버로 구성하고 구성 파일을 생성합니다. 을 참조하십시오.

2. 서버를 주 서버로 설정하고 하위 서버의 설정 파일을 가져옵니다. 를 참조하십시오.
3. 주 서버에서 글로벌 카드 소지자 및 카드 소지자 그룹을 구성합니다. 및 를 참조하십시오.
4. 하위 서버에서 글로벌 카드 소지자 및 카드 소지자 그룹을 보고 모니터링합니다. 를 참조하십시오.

하위 서버에서 구성 파일 생성

1. 하위 서버에서 **AXIS Optimizer** > **Access control(접근 제어)** > **Multi server(다중 서버)**로 이동합니다.
2. **Sub server(하위 서버)**를 클릭합니다.
3. **Generate logs(생성)**를 클릭합니다. .json 형식의 구성 파일을 생성합니다.
4. **Download(다운로드)**를 클릭하고 파일을 저장할 위치를 선택합니다.

구성 파일을 주 서버로 가져오기

1. 주 서버에서 **AXIS Optimizer** > **Access control(접근 제어)** > **Multi server(다중 서버)**로 이동합니다.
2. **Main server(주 서버)**를 클릭합니다.
3. + **Add(추가)**를 클릭하고 하위 서버에서 생성된 구성 파일로 이동합니다.
4. 하위 서버의 서버 이름, IP 주소 및 포트 번호를 입력합니다.
5. **Import(가져오기)**를 클릭하여 하위 서버를 추가합니다.
6. 하위 서버의 상태가 `Connected`로 표시됩니다.

하위 서버 취소

기본 서버로 구성 파일을 가져오기 전에만 하위 서버를 취소할 수 있습니다.

1. 주 서버에서 **AXIS Optimizer** > **Access control(접근 제어)** > **Multi server(다중 서버)**로 이동합니다.
2. **Sub server(서브 서버)**를 클릭하고 **Revoke server(서버 취소)**를 클릭합니다.
   이제 이 서버를 주 서버 또는 하위 서버로 구성할 수 있습니다.

하위 서버 제거

하위 서버의 구성 파일을 가져오면 기본 서버에 하위 서버를 연결합니다.

하위 서버 제거를 제거하려면 다음을 수행합니다.

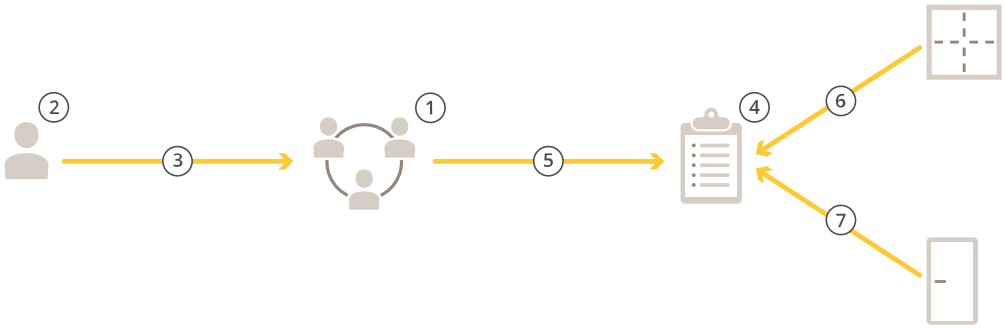
1. 주 서버에서:
   1.1. **Access management(접근 관리)** > **Dashboard(대시보드)**로 이동합니다.
   1.2. 전역 카드 소지자 및 그룹을 로컬 카드 소지자 및 그룹으로 변경합니다.
   1.3. **AXIS Optimizer** > **Access control(접근 제어)** > **Multi server(다중 서버)**로 이동합니다.
   1.4. **Main server(기본 서버)**를 클릭하여 하위 서버 목록을 표시합니다.
   1.5. 하위 서버를 선택하고 **Delete(삭제)**를 클릭합니다.
2. 기본 서버에서:
   - **AXIS Optimizer** > **Access control(접근 제어)** > **Multi server(다중 서버)**로 이동합니다.
   - **Sub server(하위 서버)**와 **Revoke server(서버 취소)**를 차례로 클릭합니다.

접근 관리

Access management(접근 관리) 탭에서는 시스템의 카드 소지자, 그룹 및 접근 룰을 구성 및 관리할 수 있습니다.

접근 관리의 작업 흐름

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



1. 그룹을 추가합니다. 을 참조하십시오.
2. 카드 소지자를 추가합니다. 을 참조하십시오.
3. 그룹에 카드 소지자를 추가합니다.
4. 접근 룰을 추가합니다. 을 참조하십시오.
5. 접근 룰에 그룹을 적용합니다.
6. 접근 룰에 영역을 적용합니다.
7. 접근 룰에 도어를 적용합니다.

카드 소지자 추가

카드 소지자는 시스템에 등록된 고유 ID를 지닌 사람입니다. 카드 소지자를 식별하는 자격 증명으로 카드 소지자를 구성하고 해당 사용자에게 도어에 대한 접근 권한을 부여하는 시기와 방법을 설정합니다.

1. **Site Navigation(사이트 탐색)** > **AXIS Optimizer** > **Access control(접근 제어)** > **Cardholder management(카드 소지자 관리)**로 이동합니다.
2. **Cardholders(카드 소지자)**로 이동하여 **+ Add(+ 추가)**를 클릭합니다.
3. 카드 소지자의 이름과 성을 입력하고 **Next(다음)**를 클릭합니다.
4. 원하는 경우 **Advanced(고급)**를 클릭하고 옵션을 선택합니다.
5. 카드 소지자에게 자격 증명을 추가합니다. 를 참조하십시오
6. **Save(저장)**를 클릭합니다.
7. 카드 소지자를 그룹에 추가합니다.
   7.1. **Groups(그룹)**에서 카드 소지자를 추가할 그룹을 선택하고 **Edit(편집)**을 클릭합니다.
   7.2. **+ Add(추가)**를 클릭하고 그룹에 추가할 카드 소지자를 선택합니다. 여러 카드 소지자를 선택할 수 있습니다.
   7.3. **추가**를 클릭합니다.
   7.4. **Save(저장)**를 클릭합니다.

고급 수준	
긴 접근 시간	도어 모니터가 설치된 경우 카드 소지자의 접근 시간과 장시간 개방이 길어지게 하려면 선택합니다.
카드 보유자 정지	카드 소지자를 정지하려면 선택합니다.
카드 두 번 대기	카드 소지자가 도어의 현재 상태를 재정의할 수 있도록 허용하려면 선택합니다. 예를 들어, 정규 일정 외의 시간에 도어를 여는 데 사용할 수 있습니다.
차단 면제	차단 기간에 카드 소지자가 접근할 수 있게 하려면 선택합니다.
Exempt from anti-passback(지정 통로 출입 방식 제외)	카드 소지자에게 지정 통로 출입 방식 룰의 면제를 제공하려면 선택합니다. 지정 통로 출입 방식은 다른 사람들이 자신보다 먼저 구역에 입장한 사람과 동일한 자격 증명을 사용하는 것을 방지합니다. 자격 증명을 다시 사용하려면 첫 번째 사용자가 먼저 해당 영역을 나가야 합니다.
전역 카드 소지자	하위 서버에서 카드 소지자를 보고 모니터링할 수 있게 하려면 선택합니다. 이 옵션은 주 서버에서 생성된 카드 소지자만 사용할 수 있습니다. 을 참조하십시오.

자격 증명 추가

카드 소지자에게 다음 유형의 자격 증명을 추가할 수 있습니다.

- 핀
- 카드
- 번호판
- 휴대폰

카드 소지자에게 번호판 자격 증명을 추가하려면 다음을 수행합니다.

1. **Credentials(자격 증명)**에서 **+ Add(추가)**를 클릭하고 **License plate(번호판)**를 선택합니다.
2. 차량을 설명하는 자격 증명 이름을 입력합니다.
3. 차량의 번호판 번호를 입력합니다.
4. 자격 증명의 시작 날짜와 종료 날짜를 설정합니다.
5. **추가**를 클릭합니다.

의 예시를 참조하십시오.

카드 소지자에게 PIN 자격 증명을 추가하려면 다음을 수행합니다.

1. **Credentials(자격 증명)**에서 **+ Add(추가)**를 클릭하고 **PIN**을 선택합니다.
2. 핀을 입력합니다.
3. 감금 핀을 사용하여 무음 알람을 트리거하려면 **Duress PIN(감금 핀)**을 켜고 감금 핀을 입력합니다.
4. **추가**를 클릭합니다.

핀 자격 증명은 항상 유효합니다. 또한 도어를 열고 시스템에서 무음 알람을 트리거하는 감금 핀을 구성할 수도 있습니다.

카드 소지자에게 카드 자격 증명을 추가하려면 다음을 수행합니다.

1. **Credentials(자격 증명)**에서 **+ Add(추가)**를 클릭하고 **Card(카드)**를 선택합니다.
2. 카드 데이터를 수동으로 입력하려면 카드 이름, 카드 번호 및 비트 길이를 입력합니다.

비고

비트 길이는 시스템에 없는 특정 비트 길이로 카드 형식을 생성할 때만 구성될 수 있습니다.

3. 마지막으로 긁은 카드의 카드 데이터를 자동으로 가져오려면 다음을 수행합니다.
   3.1. **Select reader(리더 선택)** 드롭다운 메뉴에서 도어를 선택합니다.
   3.2. 해당 도어에 연결된 리더에 카드를 댑니다.
   3.3. **Get last swiped card data from the door's reader(s)(도어의 리더에서 마지막으로 긁은 카드 데이터 가져오기)**를 클릭합니다.
4. 시설 코드를 입력합니다. 이 필드는 **Access management > Settings(접근 관리 > 설정)**에서 **Facility code(시설 코드)**를 활성화한 경우에만 사용될 수 있습니다.
5. 자격 증명의 시작 날짜와 종료 날짜를 설정합니다.
6. **추가**를 클릭합니다.

만료일	
유효 기간 시작:	자격 증명의 유효 기간을 날짜와 시간으로 설정합니다.
유효 기간 종료:	드롭다운 메뉴에서 옵션을 선택합니다.

유효 기간 종료:	
종료 날짜 없음	자격 증명은 만료되는 일이 없습니다.
날짜	자격 증명이 만료되는 날짜와 시간을 설정합니다.
최초 사용 이후	첫 번째 사용 후 자격 증명이 만료되는 기간을 선택합니다. 첫 사용 후 일수, 월수 또는 연수 또는 횟수를 선택합니다.
마지막 사용 이후	마지막 사용 후 자격 증명이 만료되는 기간을 선택합니다. 마지막 사용 후 일수, 월수 또는 연수를 선택합니다.

번호판 번호를 자격 증명으로 사용

이 예에서는 도어 컨트롤러, AXIS License Plate Verifier가 설치된 카메라, 번호판 번호를 자격 증명으로 사용하여 접근 권한을 부여하는 방법을 설명합니다.

1. AXIS Secure Entry for XProtect에 도어 컨트롤러 및 카메라를 추가합니다.
2. **Synchronize with server computer time(서버 컴퓨터 시간과 동기화)**을 사용하여 새 장치의 날짜와 시간을 설정합니다.
3. 사용 가능한 최신 버전으로 새 장치의 소프트웨어를 업그레이드합니다.
4. 도어 컨트롤러에 연결된 새 도어를 추가합니다. 을 참조하십시오.
   4.1. **Side A(A면)**에 리더를 추가합니다. 를 참조하십시오.
   4.2. **Door settings(도어 설정)**에서 **AXIS License Plate Verifier**를 **Reader type(리더 유형)**으로 선택하고 해당 리더의 이름을 입력합니다.
   4.3. 원하는 경우 **Side B(측면 B)**에 리더 또는 REX 장치를 추가합니다.
   4.4. **OK(확인)**를 클릭합니다.

5. 카메라에 AXIS License Plate Verifier를 설치하고 활성화합니다. *AXIS License Plate Verifier* 사용자 설명서를 참조하십시오.
6. AXIS License Plate Verifier를 시작합니다.
7. AXIS License Plate Verifier를 구성합니다.
   7.1. **Configuration > Access control > Encrypted communication(구성 > 접근 제어 > 암호화된 통신)**으로 이동합니다.
   7.2. **External Peripheral Authentication Key(외부 주변 장치 인증 키)**에서 **Show authentication key(인증 키 표시)** 및 **Copy key(키 복사)**를 클릭합니다.
   7.3. 카메라의 웹 인터페이스에서 AXIS License Plate Verifier를 엽니다.
   7.4. 설정하지 마십시오.
   7.5. **Settings(설정)**로 이동합니다.
   7.6. **Access control(접근 제어)**에서 **Secure Entry(보안 진입)**를 **Type(유형)**으로 선택합니다.
   7.7. **IP address(IP 주소)**에서 도어 컨트롤러의 IP 주소를 입력합니다.
   7.8. **Authentication key(인증 키)**에서 이전에 복사한 인증 키를 붙여넣습니다.
   7.9. **Connect(연결)**를 클릭합니다.
   7.10. **Door controller name(도어 컨트롤러 이름)**에서 도어 컨트롤러를 선택합니다.
   7.11. **Reader name(리더 이름)**에서 이전에 추가한 리더를 선택합니다.
   7.12. 통합을 켭니다.
8. 접근 권한을 부여받을 카드 소지자를 추가합니다. 을 참조하십시오.
9. 새 카드 소지자에게 번호판 자격 증명을 추가합니다. 을 참조하십시오.
10. 접근 룰을 추가합니다. 을 참조하십시오.
    10.1. 일정을 추가합니다.
    10.2. 번호판 접근 권한을 부여받을 카드 소지자를 추가합니다.
    10.3. AXIS License Plate Verifier 리더가 장착된 도어를 추가합니다.

그룹 추가

그룹을 사용하면 카드 소지자와 그의 접근 룰을 모두 함께 효율적으로 관리할 수 있습니다.

1. **Site Navigation(사이트 탐색)** > **AXIS Optimizer** > **Access control(접근 제어)** > **Cardholder management(카드 소지자 관리)**로 이동합니다.
2. **Groups(그룹)**로 이동하여 **+ Add(+ 추가)**를 클릭합니다.
3. 그룹의 이름을 입력하고 필요에 따라 이니셜을 선택적으로 입력합니다.
4. 하위 서버에서 카드 소지자 그룹을 보고 모니터링하기 위해 **Global group(글로벌 그룹)**을 선택합니다. 이 옵션은 주 서버에서 생성된 카드 소지자만 사용할 수 있습니다. 를 참조하십시오.
5. 그룹에 카드 소지자를 추가하려면 다음을 수행합니다.
   5.1. **+ 추가**를 클릭합니다.
   5.2. 추가할 카드 소지자를 선택하고 **Add(추가)**를 클릭합니다.
6. **Save(저장)**를 클릭합니다.

접근 룰 추가

접근 룰은 접근 권한 부여를 위해 충족되어야 하는 조건을 정의한 것입니다.

접근 룰은 다음으로 구성됩니다.

카드 소지자 및 카드 소지자 그룹 - 접근 권한을 부여할 대상입니다.

도어 및 영역 - 접근 권한이 적용되는 장소입니다.

일정 - 접근 권한을 부여하는 시간 계획입니다.

접근 룰을 추가하려면 다음을 수행합니다.

1. **Access control(접근 제어)** > **Cardholder management(카드 소지자 관리)**로 이동합니다.
2. **Access rules(접근 룰)**에서 **+ Add(추가)**를 클릭합니다.
3. 접근 룰의 이름을 입력하고 **Next(다음)**를 클릭합니다.
4. 카드 소지자와 그룹을 구성합니다.
   4.1. **Cardholders(카드 소지자)** 또는 **Groups(그룹)**에서 **+ Add(추가)**를 클릭합니다.
   4.2. 카드 소지자 또는 그룹을 선택하고 **Add(추가)**를 클릭합니다.
5. 도어 및 영역을 구성합니다.
   5.1. **Doors(도어)** 또는 **Zones(영역)**에서 **+ Add(추가)**를 클릭합니다.
   5.2. 도어 또는 영역을 선택하고 **Add(추가)**를 클릭합니다.
6. 일정을 구성합니다.
   6.1. **Schedules(스케줄)**에서 **+ Add(추가)**를 클릭합니다.
   6.2. 스케줄을 하나 이상 선택하고 **Add(추가)**를 클릭합니다.
7. **Save(저장)**를 클릭합니다.

위에서 설명한 구성 요소 중 하나 이상이 누락된 접근 룰은 불완전한 것입니다. **Incomplete(불완전)** 탭에서 모든 불완전한 접근 룰을 확인할 수 있습니다.

도어 및 구역 수동 잠금 해제

도어 수동 잠금 해제와 같은 수동 액션에 대한 자세한 내용은 을 참조하십시오.

구역 수동 잠금 해제와 같은 수동 액션에 대한 자세한 내용은 을 참조하십시오.

시스템 구성 보고서 내보내기

시스템에 대한 다양한 유형의 정보를 포함하는 보고서를 내보낼 수 있습니다. AXIS Secure Entry for XProtect은(는) 보고서를 쉼표로 구분된 값(CSV) 파일로 내보내고 기본 다운로드 폴더에 저장합니다. 보고서를 내보내려면 다음을 수행합니다.

1. **Reports(보고서)** > **System configuration(시스템 구성)**으로 이동합니다.
2. 내보낼 보고서를 선택한 후 **Download(다운로드)**를 클릭합니다.

카드 소지자 세부 정보	카드 소지자, 자격 증명, 카드 인증 및 마지막 트랜잭션에 대한 정보를 포함합니다.
카드 소지자 접근	카드 소지자 정보 및 카드 소지자 그룹, 접근 룰, 도어 및 카드 소지자와 관련된 영역에 대한 정보를 포함합니다.
카드 소지자 그룹 접근	카드 소지자 그룹 이름과 카드 소지자, 접근 룰, 도어 및 카드 소지자 그룹과 관련된 영역에 대한 정보를 포함합니다.
접근 룰	접근 룰 이름은 물론 접근 룰과 관련된 카드 소지자, 카드 소지자 그룹, 도어 및 영역에 대한 정보를 포함합니다.

도어 접근	도어 이름과 도어와 관련된 카드 소지자, 카드 소지자 그룹, 접근 룰 및 영역에 대한 정보를 포함합니다.
구역 접근	영역 이름은 물론 영역과 관련된 카드 소지자, 카드 소지자 그룹, 접근 룰 및 도어에 대한 정보를 포함합니다.

카드 소지자 활동 보고서 생성

점호 보고서는 지정된 영역 내의 카드 소지자를 나열하여 특정 시점에 누가 있는지 확인하는 데 도움을 줍니다.

소집 보고서는 지정된 영역 내의 카드 소지자를 나열하여 긴급 상황에서 누가 안전하며 누가 없는지 파악하는 데 도움이 됩니다. 건물 관리자가 대피 후 직원과 방문객의 위치를 파악하는 데 도움이 됩니다. 소집 지점은 긴급 상황 시 담당자가 보고하는 지정된 리더로, 사이트 안팎의 인원에 대한 보고서를 생성합니다. 시스템은 카드 소지자가 소집 지점에서 체크인하거나 누군가가 수동으로 안전하다고 표시할 때까지 카드 소지자를 부재중으로 표시합니다.

점호 보고서 및 소집 보고서 모두 카드 소지자를 추적하기 위한 영역이 필요합니다.

점호 보고서 또는 소집 보고서를 생성하고 실행하려면 다음을 수행합니다.

1. **Reports(보고서)** > **Cardholder activity(카드 소지자 활동)**로 이동합니다.
2. **+ Add(추가)**를 클릭하고 **Roll call / Mustering(점호 / 소집)**을 선택합니다.
3. 보고서의 이름을 입력합니다.
4. 보고서에 포함할 영역을 선택합니다.
5. 보고서에 포함할 그룹을 선택합니다.
6. 소집 보고서가 필요한 경우 **Mustering point(소집 지점)**와 소집 지점 리더를 선택합니다.
7. 보고서의 시간 프레임을 선택합니다.
8. **Save(저장)**를 클릭합니다.
9. 보고서를 선택하고 **Run(실행)**을 클릭합니다.

점호 보고서 상태	설명
있음	카드 소지자가 지정된 영역에 들어갔으며 보고서를 실행하기 전에 나오지 않았습니다.
없음	카드 소지자가 지정된 영역에서 나왔으며 보고서를 실행하기 전에 다시 들어가지 않았습니다.

소집 보고서 상태	설명
안전	카드 소지자가 소집 지점에서 카드를 댔습니다.
누락	카드 소지자가 소집 지점에서 카드를 대지 않았습니다.

액세스 관리 설정

액세스 관리 대시보드에서 사용되는 카드 소지자 필드를 사용자 지정하려면 다음을 수행합니다.

1. **Access management(접근 관리)** 탭에서 **Settings(설정)** > **Custom cardholder fields(사용자 지정 카드 소지자 필드)**를 클릭합니다.

2. **+ Add(추가)**를 클릭하고 이름을 입력합니다. 사용자 지정 필드를 최대 6개까지 추가할 수 있습니다.
3. **추가**를 클릭합니다.

시설 코드를 사용하여 접근 제어 시스템을 확인하려면 다음을 수행합니다.

1. **Access management(접근 관리)** 탭에서 **Settings(설정)** > **Facility code(시설 코드)**를 클릭합니다.
2. **Facility code on(시설 코드 켜짐)**을 선택합니다.

비고

또한 식별 프로파일을 구성할 때 **Include facility code for card validation(카드 검증용 시설 코드 포함)**도 선택해야 합니다. 을 참조하십시오.

가져오기 및 내보내기

카드 소지자 가져오기

이 옵션은 CSV 파일에서 카드 소지자, 카드 소지자 그룹 자격 증명 및 카드 소지자 사진을 가져옵니다. 카드 소지자 사진을 가져오려면 서버가 사진에 액세스할 수 있는지 확인하십시오.

카드 소지자를 가져올 때는 액세스 관리 시스템에서 자동으로 모든 하드웨어 구성을 포함한 시스템 구성을 저장하며 이전에 저장된 모든 구성을 삭제합니다.

가져오기 옵션	
새로 만들기	이 옵션은 기존 카드 소지자를 제거하고 새 카드 소지자를 추가합니다.
업데이트	이 옵션으로 기존 카드 소지자를 업데이트하고 새 카드 소지자를 추가합니다.
추가	이 옵션은 기존 카드 소지자를 유지하고 새 카드 소지자를 추가합니다. 카드 번호와 카드 소지자 ID는 고유하며 한 번만 사용할 수 있습니다.

1. **Access management(접근 관리)** 탭에서 **Import and export(가져오기 및 내보내기)**를 클릭합니다.
2. **Import cardholders(카드 소지자 가져오기)**를 클릭합니다.
3. **New(새로 만들기)**, **Update(업데이트)** 또는 **Add(추가)**를 선택합니다.
4. **Next (다음)**를 클릭합니다.
5. **Choose a file(파일 선택)**을 클릭하고 CSV 파일로 이동합니다. **열기**를 클릭합니다.
6. 열 구분자를 입력하고 고유 식별자를 선택한 후 **Next(다음)**를 클릭합니다.
7. 각 열에 방향을 할당합니다.
8. **Import(가져오기)**를 클릭합니다.

가져오기 설정	
첫 번째 행은 머리글입니다.	CSV 파일에 열 머리글이 포함되어 있으면 선택합니다.
열 구분자	CSV 파일의 열 구분자 형식을 입력합니다.

가져오기 설정	
고유 식별자	시스템은 기본적으로 **Cardholder ID(카드 소지자 ID)**를 사용하여 카드 소지자를 식별합니다. 또한, 성과 이름 또는 이메일 주소를 사용할 수 있습니다. 고유 식별자는 중복된 인사 기록의 가져오기를 방지합니다.
카드 번호 형식	**16진수와 숫자 모두 허용**이 기본으로 선택됩니다.

카드 보유자 내보내기

이 옵션은 시스템의 카드 소지자 데이터를 CSV 파일로 내보냅니다.

1. **Access management(접근 관리)** 탭에서 **Import and export(가져오기 및 내보내기)**를 클릭합니다.
2. **Export cardholders(카드 소지자 내보내기)**를 클릭합니다.
3. 다운로드 위치를 선택한 후 **Save(저장)**를 클릭합니다.

AXIS Secure Entry for XProtect은(는) 구성이 변경될 때마다 `C:\ProgramData\Axis Communications\AXIS Camera Station\Components\AXIS Secure Entry\Cardholder photos`에서 카드 소지자 사진을 업데이트합니다.

가져오기 실행 취소

카드 소지자 가져오기를 할 때 시스템에서 자동으로 해당 구성을 저장합니다. **Undo import(가져오기 실행 취소)** 옵션은 카드 소지자 데이터와 모든 하드웨어 구성을 마지막 카드 소지자 가져오기 이전 상태로 재설정합니다.

1. **Access management(접근 관리)** 탭에서 **Import and export(가져오기 및 내보내기)**를 클릭합니다.
2. **Undo import(가져오기 실행 취소)**를 클릭합니다.
3. **예**를 클릭합니다.

백업 및 복원

자동 백업은 매일 밤 수행됩니다. 최신 백업 파일 3개는 C:₩ProgramData₩Axis Communications₩AXIS Optimizer Secure Entry₩backup에 저장됩니다. 이 파일들을 복원하는 방법:

1. 백업 파일을 C:₩ProgramData₩Axis Communications₩AXIS Optimizer Secure Entry₩restore로 이동합니다.
2. 다음 방법 중 하나로 AXIS Secure Entry를 다시 시작합니다.
   - MSC(서비스) 프로그램을 시작하고 'AXIS Optimizer Secure Entry Service'를 찾아 재시작합니다.
   - 컴퓨터를 재시작합니다.

T10234037_ko

2025-10 (M3.2)