AXIS I8307-VE Network Intercom

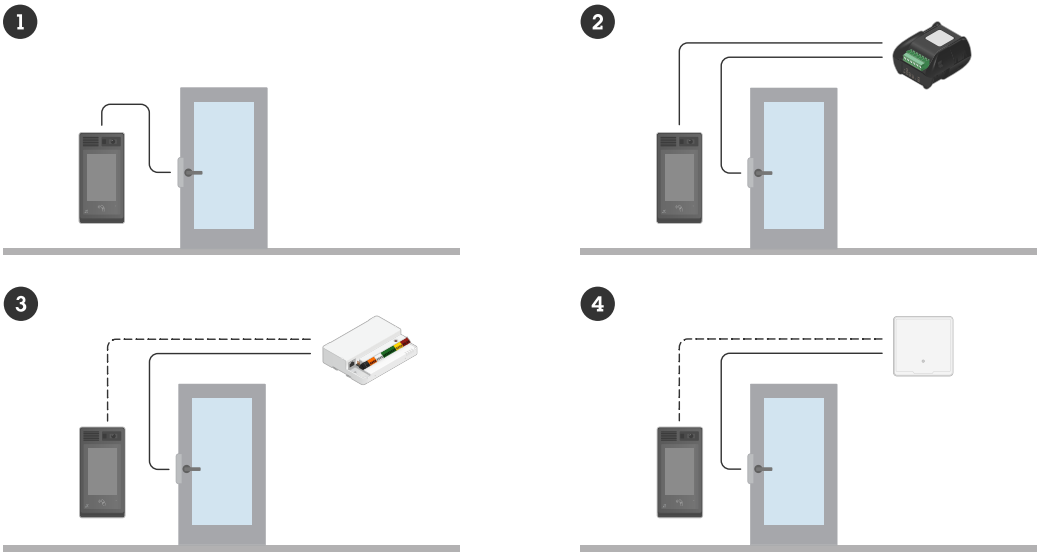
Benutzerhandbuch

Inhalt

Lösungsübersicht 4
Installation 5
Vorschaumodus 5
Funktionsweise 6
Das Gerät im Netzwerk ermitteln 6
Unterstützte Browser 6
Weboberfläche des Geräts öffnen 6
Erstellen Sie ein Administratorenkonto 6
Sichere Kennwörter 7
Stellen Sie sicher, dass die Gerätesoftware nicht manipuliert wurde 7
Ihr Gerät konfigurieren 8
Remote-Lautsprechertests kalibrieren und ausführen 8
Direktes SIP (P2P) einrichten 8
SIP über einen Server (PBX) einrichten 9
Erstellen eines Kontakts 10
Hinzufügen einer Ruftaste auf dem Bildschirm 10
Einrichtung als Kartenleser 10
Verwendung der Zugangsberechtigungsliste, um Eigentümern von Zugangsdaten den Zugang zu gewähren 11
Einrichtung als Kartenleser mithilfe einer Tür-Steuerung 12
Verwenden Sie geschützte Daten auf Karten, um die Sicherheit zu erhöhen 13
Verwenden Sie DTMF, um einen Lageplan auf dem Bildschirm anzuzeigen. 13
Weboberfläche 15
Mehr erfahren 16
Voice over IP (VoIP) 16
Session Initiation Protocol (SIP) 16
Peer-to-Peer SIP (P2PSIP) 16
Private Branch Exchange (PBX) 17
NAT-Traversal 18
Einrichten von Regeln für Ereignisse 18
Analysefunktionen und Anwendungen 18
AXIS Client for Unified Communication Systems 18
Technische Daten 19
Produktübersicht 19
LED-Anzeigen 20
Einschub für SD-Speicherkarte 20
Tasten 21
Steuertaste 21
Anschlüsse 21
Netzwerk-Steckverbinder 21
Audioanschluss 21
Relaisanschluss 21
Lesegerätanschluss 22
E/A-Anschluss 23
Stromanschluss 24
Geräte anschließen 25
Ein über PoE (12 V) gespeistes Relais 25
Zwei über PoE (12 V) gespeiste Relais 25
Ein über PoE (12 V) gespeistes Relais + ein über eine externe Stromversorgung gespeistes Relais 26
Ein über PoE (12 V) gespeistes Relais + ein potentialfreier Relaiskontakt 26
Ausfallsicheres Schloss (12 V) mit PoE+ Stromversorgung über IP-Türsprechanlage 27
Ausfallsicheres Schloss mit Stromversorgung über ein externes Netzteil 27
Ein über PoE (24 V) gespeistes Relais + ein potentialfreier Relaiskontakt 28

Kartenleser verbunden mit Tür-Controller über OSDP 28
Kartenleser verbunden mit Tür-Controller über Wiegand 29
Kartenleser an Axis Tür-Controller mit VAPIX Kartenleser angeschlossen 29
Fehlerbehebung 30
Zurücksetzen auf die Werkseinstellungen 30
Optionen für AXIS OS 30
Aktuelle AXIS OS-Version überprüfen 30
AXIS OS aktualisieren 31
Technische Probleme und mögliche Lösungen 31
Leistungsaspekte 33
Support 34
Sicherheitshinweise 35
Gefährdungsstufen 35
Weitere Hinweise 35
Cybersicherheit 36
Schwachstellen-Management 36
Sicherheitsbenachrichtigungen 36
Sicherer Produktlebenszyklus 36

Lösungsübersicht



1 *IP-Türsprechanlage*
2 *IP-Türsprechanlage in Kombination mit AXIS A9801*
3 *IP-Türsprechanlage in Kombination mit AXIS A9210*
4 *IP-Türsprechanlage kombiniert mit einem Zutrittssystem*

Installation



Vorschaumodus

Der Vorschaumodus eignet sich optimal für Monteure für die Feinjustierung der Kameraansicht während der Installation. Für den Zugriff auf die Kameraansicht im Vorschaumodus ist keine Anmeldung erforderlich. Sie ist ab dem Einschalten des Geräts nur für eine begrenzte Zeit in der Werkseinstellung verfügbar.



Dieses Video zeigt, wie der Vorschaumodus verwendet wird.

Funktionsweise

Das Gerät im Netzwerk ermitteln

Mit AXIS IP Utility und AXIS Device Manager die Axis Geräte im Netzwerk ermitteln und ihnen unter Windows® IP-Adressen zuweisen. Beide Anwendungen sind kostenlos und können von *axis.com/support* heruntergeladen werden.

Weitere Informationen zum Zuweisen von IP-Adressen finden Sie unter *Zuweisen von IP-Adressen und Zugreifen auf das Gerät*.

Unterstützte Browser

Das Gerät kann mit den folgenden Browsern verwendet werden:

	Chrome™	Edge™	Firefox®	Safari®
Windows®	✓	✓	*	*
macOS®	✓	✓	*	*
Linux®	✓	✓	*	*
Andere Betriebssysteme	*	*	*	*

✓: Empfohlen

*: Wird mit Einschränkungen unterstützt

Weboberfläche des Geräts öffnen

1. Öffnen Sie einen Browser, und geben Sie die IP-Adresse oder den Host-Namen des Axis Geräts in die Adresszeile des Browsers ein.
   Wenn Sie die IP-Adresse nicht gehen, ermitteln Sie das Gerät im Netzwerk mithilfe von AXIS IP Utility oder AXIS Device.
2. Geben Sie den Benutzernamen und das Kennwort ein. Wenn Sie zum ersten Mal auf das Gerät zugreifen, müssen Sie ein Administratorkonto erstellen. Siehe *Erstellen Sie ein Administratorenkonto, on page 6*.

Eine Beschreibung aller Funktionen und Einstellungen in der Weboberfläche von Geräten mit AXIS OS finden Sie in der *Hilfe zur AXIS OS-Weboberfläche*.

Erstellen Sie ein Administratorenkonto

Beim ersten Anmelden an Ihrem Gerät muss ein Administratorkonto erstellt werden.

1. Geben Sie einen Kontonamen ein.
2. Geben Sie ein Passwort ein. Siehe *Sichere Kennwörter, on page 7*.
3. Geben Sie das Kennwort erneut ein.
4. Stimmen Sie der Lizenzvereinbarung zu.
5. Klicken Sie auf **Konto hinzufügen**.

Wichtig

Das Gerät verfügt über kein Standardkonto. Wenn Sie das Kennwort für Ihr Administratorkonto verloren haben, müssen Sie das Gerät zurücksetzen. Siehe *Zurücksetzen auf die Werkseinstellungen, on page 30*.

Sichere Kennwörter

Wichtig

Verwenden Sie HTTPS (das standardmäßig aktiviert ist), um Ihr Kennwort oder andere sensible Einstellungen über das Netzwerk festzulegen. HTTPS ermöglicht sichere und verschlüsselte Netzwerkverbindungen und schützt so sensible Daten wie beispielsweise Kennwörter.

Das Gerätekennwort ist der Hauptschutz für Ihre Daten und Dienste. Produkte von Axis geben keine Kennwortrichtlinien vor, da die Produkte unter den verschiedensten Bedingungen eingesetzt werden.

Doch zum Schutz Ihrer Daten empfehlen wir dringend:

- Ein Kennwort zu verwenden, das aus mindestens acht Zeichen besteht, und das bevorzugt von einem Kennwortgenerator erzeugt wurde.
- Das Kennwort geheimzuhalten.
- Ändern Sie das Kennwort regelmäßig und mindestens einmal jährlich.

Stellen Sie sicher, dass die Gerätesoftware nicht manipuliert wurde.

So stellen Sie sicher, dass das Gerät über seine ursprüngliche AXIS OS-Version verfügt, bzw. übernehmen nach einem Sicherheitsangriff die volle Kontrolle über das Gerät:

1. Zurücksetzen auf die Werkseinstellungen. Siehe *Zurücksetzen auf die Werkseinstellungen, on page 30*. Nach dem Zurücksetzen gewährleistet Secure Boot den Status des Geräts.
2. Konfigurieren und installieren Sie das Gerät.

Ihr Gerät konfigurieren

In diesem Abschnitt werden alle wichtigen Konfigurationen behandelt, die ein Installationstechniker ausführen muss, um das Produkt nach Abschluss der Hardwareinstallation in Betrieb zu nehmen.

Remote-Lautsprechertests kalibrieren und ausführen

Mit dem Lautsprechertest kann von einem entfernten Standort aus überprüft werden, ob ein Lautsprecher wie vorgesehen funktioniert. Der Lautsprecher führt den Test durch, indem er eine Reihe von Testsignalen abspielt, die vom eingebauten Mikrofon registriert werden. Bei jeder Durchführung des Tests werden die registrierten Werte mit den Werten verglichen, die während der Kalibrierung registriert wurden.

Hinweis

Der Test muss in der montierten Position am Aufstellungsort kalibriert werden. Wenn der Lautsprecher bewegt wird oder sich die lokale Umgebung verändert (eine Wand wird gebaut/entfernt), muss der Lautsprecher erneut kalibriert werden

Es wird empfohlen, dass sich während der Kalibrierung eine Person am Standort befindet, um zu überprüfen, dass die Testtöne nicht gedämpft klingen und sich keine Hindernisse im Klangradius des Lautsprechers befinden.

1. Wechseln Sie zu Geräteschnittstelle > **Audio > Speaker test (Audio > Lautsprechertest)**.
2. Klicken Sie zum Kalibrieren des Audio-Geräts auf **Calibrate (Kalibrieren)**.

Hinweis

Sobald das Axis Produkt kalibriert ist, kann der Lautsprechertest jederzeit durchgeführt werden.

3. Zum Starten des Lautsprechertests klicken Sie auf **Run the test (Test ausführen)**.

Hinweis

Die Kalibrierung kann auch durch Drücken der Steuertaste auf dem physikalischen Gerät ausgeführt werden. Unter *Produktübersicht, on page 19* können Sie die Steuertaste identifizieren.

Direktes SIP (P2P) einrichten

Bei VoIP (Voice over IP) handelt es sich um eine Technologiegruppe, die Sprachkommunikation und Multimediakommunikation über IP-Netzwerke ermöglicht. Weitere Informationen finden Sie unter *Voice over IP (VoIP), on page 16*.

Auf diesem Gerät wird VoIP über das SIP-Protokoll aktiviert. Weitere Informationen zu SIP finden Sie unter *Session Initiation Protocol (SIP), on page 16*

SIP verfügt über zwei Einstellungstypen. Eine davon ist direkt oder Peer-to-Peer (P2P). Verwenden Sie Peer-to-Peer, wenn die Kommunikation zwischen wenigen Benutzeragenten innerhalb desselben IP-Netzwerks erfolgt und keine zusätzlichen Funktionen erforderlich sind, die von einem PBX-Server bereitgestellt werden können. Weitere Informationen zum Einrichten finden Sie unter *Peer-to-Peer SIP (P2PSIP), on page 16*.

1. Rufen Sie **Communication > SIP > Settings (Kommunikation > SIP > Einstellungen)** auf und wählen Sie **Enable SIP (SIP aktivieren)** aus.
2. Um auf dem Axis Gerät eingehende Anrufe zu erlauben, wählen Sie **Allow incoming calls (Eingehende Anrufe erlauben)** aus.

HINWEIS

Wenn Sie eingehende Anrufe zulassen, nimmt das Gerät Anrufe von allen Geräten an, die mit dem Netzwerk verbunden sind. Wenn auf das Gerät über ein öffentliches Netzwerk oder das Internet zugegriffen werden kann, wird empfohlen, eingehende Anrufe zu deaktivieren.

3. Klicken Sie auf **Call handling (Anrufbehandlung)**.
4. Unter **Calling timeout (Zeitüberschreitung bei Anruf)** die Sekundenanzahl eingeben, nach denen der Anruf ohne Antwort beendet wird.

5. Wenn Sie eingehende Anrufe zugelassen haben, legen Sie in **Incoming call Timeout (Zeitüberschreitung bei eingehenden Anrufen)** die Anzahl der Sekunden fest.
6. Klicken Sie auf **Ports**.
7. Geben Sie die Nummer für den **SIP port (SIP-Port)** und **TLS port (TLS-Port)** ein.

Hinweis

- **SIP-Port** – für SIP-Sitzungen. Der Datenverkehr über diesen Port ist nicht verschlüsselt. Der Standardport ist 5060.
- **TLS port (TLS-Port)** – für SIPs und TLS-gesicherte SIP-Sitzungen. Der Datenverkehr über diesen Port wird mittels Transport Layer Security (TLS) verschlüsselt. Der Standardport ist 5061.
- **RTP start port** – der Port für den ersten RTP-Mediastream eines SIP-Anrufs. Der Standard-Startport ist 4000. Einige Firewalls können den RTP-Datenaustausch über bestimmte Ports blockieren. Die Portnummer muss zwischen 1024 und 65535 liegen.

8. Klicken Sie auf **NAT Traversal**.
9. Wählen Sie die Protokolle, die für NAT-Traversal aktiviert werden sollen.

Hinweis

NAT Traversal verwenden, wenn das Axis Gerät über einen NAT-Router oder eine Firewall mit dem Netzwerk verbunden ist. Weitere Informationen finden Sie unter *NAT-Traversal, on page 18*.

10. Klicken Sie auf **Save (Speichern)**.

SIP über einen Server (PBX) einrichten

Bei VoIP (Voice over IP) handelt es sich um eine Technologiegruppe, die Sprachkommunikation und Multimediakommunikation über IP-Netzwerke ermöglicht. Weitere Informationen finden Sie unter *Voice over IP (VoIP), on page 16*.

Auf diesem Gerät wird VoIP über das SIP-Protokoll aktiviert. Weitere Informationen zu SIP finden Sie unter *Session Initiation Protocol (SIP), on page 16*

SIP verfügt über zwei Einstellungstypen. Ein PBX-Server ist einer davon. Verwenden Sie einen PBX-Server, wenn die Kommunikation zwischen einer unbegrenzten Anzahl von Benutzeragenten innerhalb und außerhalb des IP-Netzwerks erfolgen soll. Je nach PBX-Anbieter können dem Setup zusätzliche Funktionen hinzugefügt werden. Weitere Informationen finden Sie unter *Private Branch Exchange (PBX), on page 17*.

1. Fordern Sie folgende Informationen von Ihrem PBX-Anbieter an:
   - Benutzer-ID
   - Domäne
   - Kennwort
   - Authentifizierungs-ID
   - Anrufer-ID
   - Registrator
   - RTP-Startport
2. Rufen Sie **Communication > SIP > Accounts (Kommunikation > SIP > Konten)** auf, und klicken Sie auf **+ Add account (+ Konto hinzufügen)**.
3. Einen **Namen** für das Konto eingeben.
4. Wählen Sie **Registered (Registriert)** aus.
5. Transportmodus auswählen.
6. Die Kontoinformationen des PBX-Anbieters hinzufügen.
7. Klicken Sie auf **Save (Speichern)**.

8. Um die SIP-Einstellungen auf die gleiche Weise wie für Peer-to-Peer einzurichten, siehe *Direktes SIP (P2P) einrichten, on page 8*. Verwenden Sie den RTP-Startport des PBX-Anbieters.

Erstellen eines Kontakts

In diesem Beispiel wird das Erstellen eines neuen Kontakts in der Kontaktliste erläutert. Aktivieren Sie vor dem Start SIP unter **Communication > SIP (System > SIP)**.

So erstellen Sie einen neuen Kontakt:

1. Rufen Sie **Communication > Contact list (Kommunikation > Kontaktliste)** auf.
2. Klicken Sie auf **+ Add contact (+ Kontakt hinzufügen)**.
3. Geben Sie den Vor- und Nachnamen des Kontakts ein.
4. Geben Sie die SIP-Adresse des Kontakts ein.

Hinweis

Weitere Informationen zu SIP-Adressen finden Sie unter *Session Initiation Protocol (SIP), on page 16*.

5. Wählen Sie das SIP-Konto aus, aus dem der Aufruf erfolgen soll.

Hinweis

Verfügbarkeitsoptionen werden unter **System** > **Events (Ereignisse)** > **Schedules (Zeitpläne)** definiert.

6. Wählen Sie die **Availability (Verfügbarkeit)** des Kontakts. Wenn ein Anruf erfolgt, obwohl der Kontakt nicht verfügbar ist, wird der Anruf abgebrochen, es sei denn, es gibt einen Fallback-Kontakt.

Hinweis

Bei einem Fallback-Kontakt handelt es sich um einen Kontakt, an den der Anruf weitergeleitet wird, wenn der ursprüngliche Kontakt nicht antwortet oder nicht verfügbar ist.

7. Wählen Sie unter **Fallback**Keine**.**
8. Klicken Sie auf **Save (Speichern)**.

Hinzufügen einer Ruftaste auf dem Bildschirm

In diesem Beispiel wird erläutert, wie Sie die Anzeige so konfigurieren, dass eine Schaltfläche angezeigt wird, über die Besucher die Rezeption anrufen können.

Vorbereitungen

- Erstellen Sie den Rezeptionskontakt. Anweisungen finden Sie unter *Erstellen eines Kontakts, on page 10*.

1. Gehen Sie zu **Display (Bildschirm) > Pages (Seiten)**.
2. Klicken Sie in **Default Homepage (Standard-Homepage)** auf die Option ⋮ und wählen Sie **Edit (Bearbeiten)**.
3. **+ hinzufügen** anklicken.
4. Wählen Sie in der Liste **Type (Typ)** die Option **Button (Schaltfläche)** aus.
5. Wählen Sie in der Liste der Kontakte die Rezeption aus.
6. Wählen Sie eine Schaltflächengröße.
7. Um die Schaltfläche zu speichern, klicken Sie auf **Save (Speichern)**.
8. Um die Standard-Homepage zu speichern, klicken Sie auf **Save (Speichern)**.

Einrichtung als Kartenleser

Sie können Ihre IP-Türsprechanlage als Kartenleser einrichten, damit Eigentümer von Zugangsdaten die Tür öffnen können.

Mithilfe der Zugangsberechtigungsliste speichert die IP-Türsprechanlage die Zugangsdaten lokal und kann als eigenständiger Kartenleser für bis zu fünfzig Eigentümer von Zugangsdaten fungieren.

Bei Verbindung der IP-Türsprechanlage mit einer Tür-Steuerung kann die IP-Türsprechanlage weiterhin bis zu fünfzig Zugangsdatensätze speichern und die Verwaltung der Zugangsberechtigungen übernehmen, wenn sie die Zugangsdaten bei einer Zutrittsanfrage in der Zugangsberechtigungsliste findet. Wenn die Zugangsdaten zu einer Zutrittsanfrage nicht in der Zugangsberechtigungsliste gefunden werden und die Option **Use connected door controller (Verbundene Tür–Steuerung verwenden)** aktiviert ist, wird die Anfrage an die Tür-Steuerung weitergeleitet, die dann die Verwaltung der Zugangsberechtigungen übernimmt.

Verwendung der Zugangsberechtigungsliste, um Eigentümern von Zugangsdaten den Zugang zu gewähren

Mit der Zugangsberechtigungsliste können Eigentümer von Zugangsdaten Aktionen wie das Öffnen einer Tür über ihre Zugangsdaten auslösen. In diesem Beispiel wird erläutert, wie Sie einen Eigentümer von Zugangsdaten hinzufügen, der mit seiner Karte zehnmal die Tür öffnen kann.

Voraussetzungen

- Stellen Sie sicher, dass unter **Reader > Chip types (Leser > Chiptypen)** der richtige Chiptyp aktiviert ist.

Aktivieren Sie die Zugangsberechtigungsliste, und fügen Sie einen Eigentümer von Zugangsdaten hinzu:

1. Gehen Sie zu **Reader > Entry list (Leser > Zugangsberechtigungsliste)**.
2. Aktivieren Sie **Use Entry list (Zugangsberechtigungsliste verwenden)**.
3. Klicken Sie auf **+ Add credential holder (+ Eigentümer von Zugangsdaten hinzufügen)**.
4. Geben Sie den Vor- und Nachnamen des Eigentümers der Anmeldedaten ein. Der Vorname der Wiedergabeliste muss eindeutig sein.
5. Wählen Sie **Card (Karte)** aus.
6. Ziehen Sie die Karte des Eigentümers von Zugangsdaten auf dem Gerät durch, und klicken Sie auf **Get latest (Neueste abrufen)**.
7. Behalten Sie **Access granted (Zugang gewährt)** als Ereignisbedingung bei.
8. Wählen Sie unter **Valid to (Gültig bis)** die Option **Number of times (Anzahl)** aus.
9. Geben Sie unter **Number of times (Anzahl)** 10 ein:
10. Klicken Sie auf **Save (Speichern)**.

Eine Regel erstellen:

1. Gehen Sie auf **System > Ereignisse**.
2. Klicken Sie unter **Rules (Regeln)** auf **+ Add a rule (+ Regel hinzufügen)**.
3. Geben Sie in **Name** Unlock door (Tür entriegeln) ein.
4. Wählen Sie in der Liste der Bedingungen **Entry list > Access granted (Zugangsberechtigungsliste > Zugang gewährt)** aus.
5. Wählen Sie in der Liste der Aktionen **I/O > Toggle I/O once (E/A > E/A einmalig umschalten)** aus.
6. Wählen Sie in der Liste der Ports **Door (Tür)** aus.
7. Wählen Sie unter **State (Status)** die Option **Active (Aktiv)** aus.
8. Legen Sie die Dauer auf 00:00:07 fest:
9. Klicken Sie auf **Save (Speichern)**.

Einrichtung als Kartenleser mithilfe einer Tür-Steuerung

Netzwerk-Verbindung

Um die IP-Türsprechanlage als Kartenleser zu verwenden, kann sie mit einer Türsteuerung verbunden werden. Die Türsteuerung speichert alle Zugangsdaten und überwacht, wer durch die Tür gehen darf. In diesem Beispiel werden die Geräte über das Netzwerk angeschlossen. Wir ändern auch die zulässigen Kartentypen.

Wichtig

Die Netzwerk-Verbindung funktioniert nur mit Axis Türsteuerungen. Um eine Verbindung zu einer Nicht-Axis-Türsteuerung herzustellen, müssen die Geräte physisch mit Kabeln verbunden werden. Siehe *Drahtverbindung, on page 12*.

Einrichten der IP-Türsprechanlage als Kartenleser

1. Rufen Sie **Reader > Connection (Kartenleser > Verbindung)** auf.
2. Wählen Sie den **Protokolltyp des VAPIX-Lesers**.
3. Wählen Sie das Protokoll für die Kommunikation mit der Türsteuerung.

Hinweis

Bei Verwendung von **HTTPS** empfehlen wir Ihnen, **Zertifikat überprüfen** zu aktivieren.

4. Geben Sie die IP-Adresse für die Türsteuerung ein.
5. Geben Sie die Zugangsdaten für die Türsteuerung ein.
6. **Connect (Verbinden)** anklicken.
7. Wählen Sie den Eingangsleser für die entsprechende Tür.
8. Klicken Sie auf **Save (Speichern)**.

Drahtverbindung

Um die Türstation als Kartenleser zu verwenden, kann sie mit einer Türsteuerung verbunden werden. Die Türsteuerung speichert alle Zugangsdaten und überwacht, wer durch die Tür gehen darf. In diesem Beispiel verbinden wir die Geräte mit Kabeln, verwenden das Wiegand-Protokoll, aktivieren den Summer und verwenden einen E/A-Port für die LED. Wir ändern auch die zulässigen Kartentypen.

Wichtig

Verwenden Sie E/A-Ports, die noch nicht verwendet werden. Wenn E/A-Ports bereits verwendet werden, funktionieren für diese Ports erstellte Ereignisse nicht mehr.

Vorbereitungen

- Schließen Sie die IP-Türsprechanlage an die Türsteuerung an.
  Siehe Schaltpläne, die in *Geräte anschließen, on page 25* zu finden sind.
- Konfigurieren Sie die Hardware der Türsteuerung mit dem Wiegand-Protokoll für den Leser. Weitere Anweisungen finden Sie im Benutzerhandbuch der Türsteuerung.

Einrichten der IP-Türsprechanlage als Kartenleser

1. Rufen Sie **Reader > Connection (Kartenleser > Verbindung)** auf.
2. Wählen Sie als Protokolltyp **Wiegand** aus.
3. Aktivieren Sie den **Summer**.
4. Wählen Sie unter **Eingang für Summer** die Option **I3**.
5. Wählen Sie unter **Input used for LED control (Eingang für die LED-Steuerung)** die Option **1** aus.
6. Wählen Sie unter **Eingang für LED1**die Option **I1**.
7. Wählen Sie die für die einzelnen Zustände zu verwendenden Farben aus.
8. Wählen Sie unter **Tastendruckformat** die Option **FourBit**.
9. Klicken Sie auf **Save (Speichern)**.

10. Wechseln Sie zu **Reader > Chip types (Leser > Chiparten)** und aktivieren Sie die Chiparten, die Sie verwenden möchten.

Hinweis

Sie können die standardmäßig vorgegebenen Chiparten beibehalten. Wir empfehlen jedoch, die Liste ihren besonderen Anforderungen entsprechend zu ändern.

11. Klicken Sie auf **Datensatz hinzufügen**, um die Datensätze für die verschiedenen Chiparten anzugeben.
12. Klicken Sie auf **Save (Speichern)**.

Verwenden Sie geschützte Daten auf Karten, um die Sicherheit zu erhöhen

Für mehr Sicherheit in Ihrem Zutrittssystem können Sie sichere Kartendaten verwenden, die auf bestimmten Kartentypen gespeichert sind. Die Daten werden mit einem sicheren Schlüssel geschützt. Zum Auslesen der Kartendaten müssen der verborgene Schlüssel und weitere Informationen zur Karte auf dem Gerät gespeichert werden.

1. Wechseln Sie zu **Reader > Chip types (Leser > Chiparten)**.
2. Wählen Sie unter **Data sets (Datensätze)** die zu bearbeitenden Chipart und klicken Sie auf **Add data set (Datensatz hinzufügen)** .
3. Geben Sie Informationen zu den Kartendaten ein. Welche Informationen sie eingeben müssen, hängt vom Kartentyp und von der Art der Anmeldung ab.
4. Wenn Sie die Protokolle OSDP oder Wiegand verwenden, wählen Sie **Use as UID (Als UID verwenden)** aus, um die sicheren Daten als UID/CSN anstelle der normalen UID/CSN der Karte zu senden.
5. Damit nur Karten, die den angegebenen Kartendaten entsprechen, an den Zugangscontroller gesendet werden können, wählen Sie die Option **Erforderliche Daten**. Karten, die nicht den Anforderungen entsprechen, werden vom Leser ignoriert.
6. Klicken Sie auf **Save (Speichern)**.

Verwenden Sie DTMF, um einen Lageplan auf dem Bildschirm anzuzeigen.

Wenn ein Besucher über die IP-Türsprechanlage anruft und Hilfe benötigt, kann die Person, die den Anruf entgegennimmt, per DTMF-Signalisierung (Dual-Tone Multi-Frequency) einen Lageplan auf dem Bildschirm der IP-Türsprechanlage anzeigen.

Dieses Beispiel erläutert:

- Laden Sie ein Lageplanbild auf die IP-Türsprechanlage hoch.
- Erstellen Sie eine Seite, die das Lageplanbild in der IP-Türsprechanlage enthält.
- Definieren der DTMF-Sequenz in der IP-Türsprechanlage.
- Richten Sie die IP-Türsprechanlage so ein, dass die Lageplanseite 30 Sekunden lang als Antwort auf die DTMF-Sequenz angezeigt wird.

Vorbereitungen

- SIP-Anrufe vom Gerät zulassen und ein SIP-Konto erstellen. Weitere Anweisungen finden Sie unter *Direktes SIP (P2P) einrichten, on page 8* und *SIP über einen Server (PBX) einrichten, on page 9*.

Lageplanbild hochladen

1. Gehen Sie auf **Media (Medien)**.
2. **+ hinzufügen** anklicken.
3. Ziehen Sie per Drag and Drop ein Bild, das einen Lageplan des Gebäudes zeigt. Die empfohlene Bildauflösung ist 480x800 Pixel, die maximale Auflösung beträgt 2048x2048 Pixel.
4. Klicken Sie auf **Save (Speichern)**.

Erstellen Sie eine Lageplanseite für den Bildschirm.

5. Gehen Sie zu **Display (Bildschirm) > Pages (Seiten)**.

6. **+ hinzufügen** anklicken.
7. Geben Sie einen Namen für die Seite ein, zum Beispiel Lageplanseite.
8. **+ hinzufügen** anklicken.
9. Wählen Sie in der Liste der Typen **Image (Bild)**.
10. Geben Sie einen Namen für das Bild ein, zum Beispiel Lageplanbild.
11. Wählen Sie in der Liste der Lagepläne das Lageplanbild aus.
12. Klicken Sie auf **Save (Speichern)**.
13. Klicken Sie erneut auf **Save (Speichern)**.

Definieren der DTMF-Sequenz

14. Gehen Sie zu **Communication (Kommunikation) > SIP > DTMF**.
15. Klicken Sie auf **+ Add sequence (+ Sequenz hinzufügen)**.
16. Geben Sie in **Sequence (Sequenz)** 9 ein.
17. Geben Sie in **Description (Beschreibung)** Lageplan anzeigen ein.
18. Wählen Sie ein Konto.
19. Klicken Sie auf **Save (Speichern)**.

Eine Regel erstellen

20. Gehen Sie auf **System > Events (Ereignisse) > Rules (Regeln)** und fügen Sie eine Regel hinzu.
21. Geben Sie einen Namen für die Regel ein, z. B. DTMF verwenden, um Lagepläne anzuzeigen.
22. Wählen Sie aus der Liste der Bedingungen **Call (Anruf) > DTMF**.
23. Wählen Sie in der Liste der DTMF-Ereignis-IDs **Show map (Lagepläne anzeigen)**.
24. Wählen Sie in der Liste der Aktionen **Display (Bildschirm) > Show page (Seite anzeigen)**.
25. Wählen Sie in der Liste der Lagepläne **Map page (Lageplanseite)**.
26. Geben Sie in **Duration (Dauer)**, 00:00:30 ein, um den Lageplan 30 Sekunden lang anzuzeigen.
27. Klicken Sie auf **Save (Speichern)**.

Weboberfläche

Informationen zu allen Funktionen und Einstellungen, die in der Weboberfläche von Geräten mit AXIS OS verfügbar sind, finden Sie in der *Hilfe zur AXIS OS-Weboberfläche*.

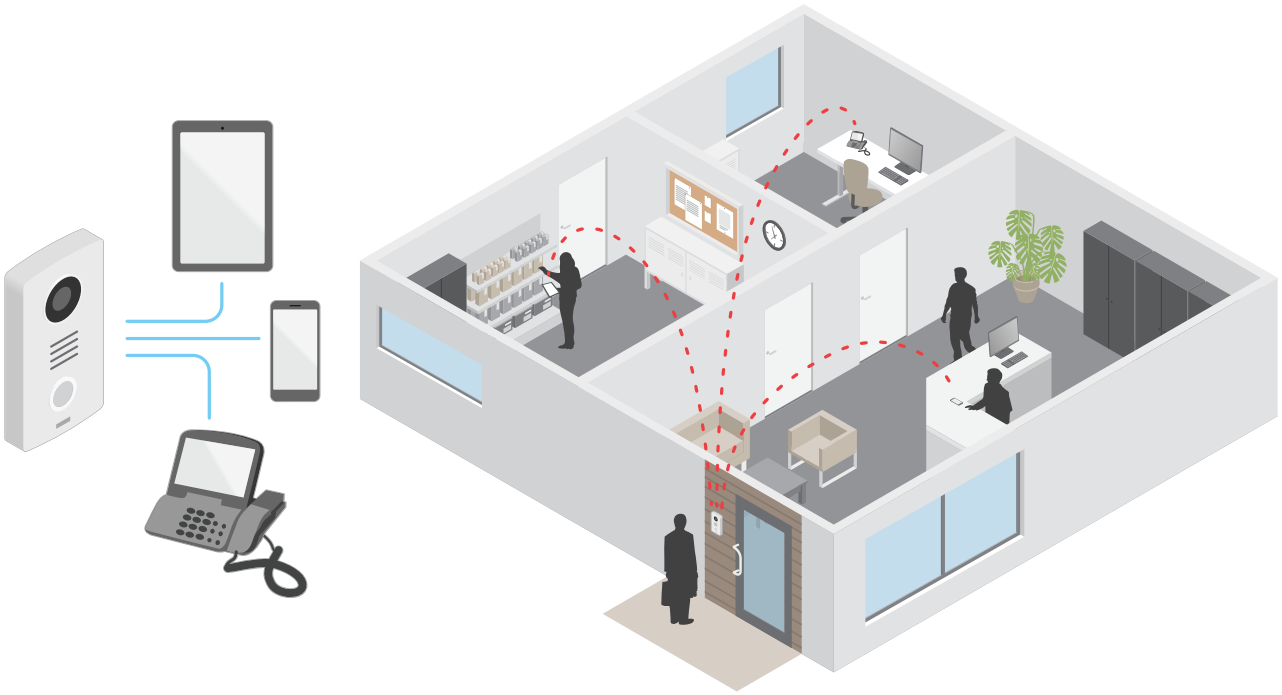
Mehr erfahren

Voice over IP (VoIP)

Bei Voice over IP (VoIP) handelt es sich um eine Technologiegruppe, die Sprachkommunikation und Multimedia-Sitzungen über IP-Netzwerke ermöglicht, z. B. das Internet. Bei herkömmlichen Telefongesprächen werden analoge Signale über einen Übertragungsschaltkreis über das öffentliche Telefonnetz (Public Switched Telephone Network - PSTN) gesendet. Bei einem VoIP-Anruf werden analoge Signale in digitale Signale umgewandelt, um sie über lokale IP-Netzwerke oder das Internet in Datenpaketen zu senden.

Im Axis Produkt wird VoIP durch das Session Initiation Protocol (SIP) und die Signalgebung Dual-Tone Multi-Frequency (DTMF) ermöglicht.

Beispiel:



Wenn Sie die Anruftaste einer Axis IP-Türsprechanlage drücken, wird ein Anruf für einen oder mehrere vordefinierte Empfänger initiiert. Wenn ein Empfänger antwortet, wird ein Anruf eingerichtet. Die Sprach- und Videoübertragung erfolgt über VoIP-Technologien.

Session Initiation Protocol (SIP)

Das SIP (Session Initiation Protocol) wird zum Einrichten, Warten und Beenden von VoIP-Anrufen verwendet. Sie können Anrufe zwischen zwei oder mehreren Teilnehmern, sogenannten SIP-Benutzeragenten, tätigen. Um einen SIP-Anruf zu tätigen, können Sie z. B. SIP-Telefone, Softphones oder SIP-fähige Axis Geräte verwenden.

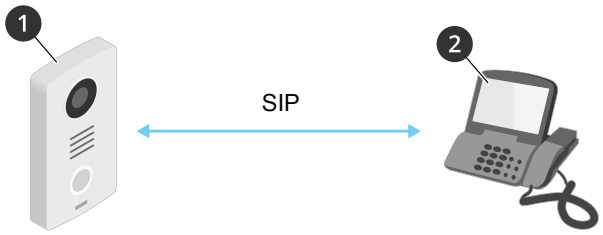
Die eigentlichen Audio- bzw. Videoübertragungen werden zwischen den SIP-Benutzeragenten mit einem Transportprotokoll, wie z. B. RTP (Real-Time Transport Protocol), ausgetauscht.

Sie können Anrufe in lokalen Netzwerken über ein Peer-to-Peer-Setup, oder netzwerkübergreifend mit einer PBX-Anlage tätigen.

Peer-to-Peer SIP (P2PSIP)

Die einfachste Art der SIP-Kommunikation findet direkt zwischen zwei oder mehr SIP-Benutzeragenten statt. Dies wird als Peer-to-Peer-SIP (P2PSIP) bezeichnet. Wenn dies in einem lokalen Netzwerk stattfindet, sind nur die SIP-Adressen der Benutzeragenten erforderlich. Eine typische SIP-Adresse wäre in diesem Fall `sip:<local-ip>`.

Beispiel:



1 *Benutzeragent A – Gegensprechanlage. SIP-Adresse: Schluck: 192.168.1.101*
2 *Benutzeragent B – SIP-fähiges Telefon. SIP-Adresse: Schluck: 192.168.1.100*

Sie können die Axis IP-Türsprechanlage so einrichten, dass sie beispielsweise ein SIP-fähiges Telefon im selben Netzwerk mit einem Peer-to-Peer-SIP-Setup anruft.

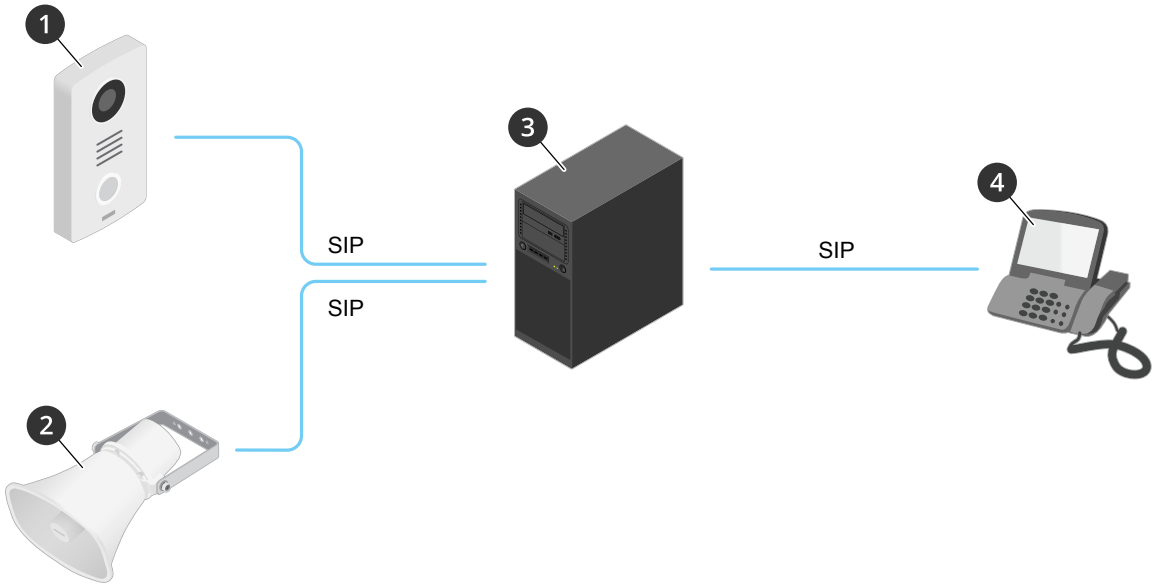
Private Branch Exchange (PBX)

Wenn Sie SIP-Anrufe außerhalb Ihres lokalen IP-Netzwerks tätigen, kann eine PBX (Private Branch Exchange) als zentraler Hub fungieren. Die Hauptkomponente einer PBX ist ein SIP-Server, der auch als SIP-Proxy oder Registrar bezeichnet wird. Eine PBX funktioniert wie eine herkömmliche Telefonzentrale, die den aktuellen Status des Clients anzeigt und beispielsweise Rufweiterleitungen, Voicemail und Weiterleitungen zulässt.

Der PBX-SIP-Server kann lokal oder extern eingerichtet werden. Er kann im Intranet oder durch einen Drittanbieter gehostet werden. Wenn Sie SIP-Anrufe zwischen Netzwerken tätigen, werden Anrufe über einen Satz von PBX-Anlagen weitergeleitet, die den Standort der zu erreichenden SIP-Adresse abfragen.

Jeder SIP-Benutzeragent wird bei der Nebenstellenanlage registriert und kann dann die anderen über die entsprechende Durchwahl erreichen. Eine typische SIP-Adresse wäre in diesem Fall `sip:<user>@<domain>` oder `sip:<user>@<registrar-ip>`. Die SIP-Adresse ist unabhängig von der jeweiligen IP-Adresse, und die PBX ermöglicht den Zugriff auf das Gerät, solange es für die PBX registriert ist.

Beispiel:



1 *sip:mydoor@company.com*
2 *sip:myspeaker@company.com*
3 ***PBX** sip.company.com*
4 *sip:office@company.com*

Wenn Sie die Anruftaste einer Axis IP-Türsprechanlage drücken, wird der Anruf über eine oder mehrere PBX-Anlagen an eine SIP-Adresse entweder im lokalen IP-Netzwerk oder über das Internet weitergeleitet.

NAT-Traversal

NAT-Traversal (Network Address Translation) verwenden, wenn sich das Axis Gerät in einem privaten Netzwerk befindet und auch von außerhalb verfügbar sein soll.

Hinweis

Der Router muss NAT-Traversal und UPnP® unterstützen.

Die Protokolle von NAT Traversal können einzeln oder in verschiedenen Kombinationen verwendet werden, die sich nach der Netzwerkumgebung richten.

- **ICE:** Das Protokoll ICE (Interactive Connectivity Establishment) erhöht die Chancen, den effizientesten Kommunikationspfad zwischen gleichrangigen Geräten zu finden. Mit dem Aktivieren von STUN und TURN werden die Chancen des ICE-Protokolls nochmals verbessert.
- **STUN:** STUN (Session Traversal Utilities for NAT) ist ein Client-Server-Netzwerkprotokoll, an dem Axis Produkte erkennen, ob sie sich hinter einer NAT oder Firewall befinden. Zudem werden mit diesem Protokoll öffentlich zugewiesene IP-Adressen (NAT-Adressen) und Portnummern abgerufen, die von NAT für Verbindungen mit Remote-Hosts zugewiesen wurden. Geben Sie die STUN-Server-Adresse ein, z. B. eine IP-Adresse.
- **TURN** — TURN (Traversal Using Relays around NAT) ist ein Protokoll, mit dem Geräte hinter einem NAT-Router oder einer Firewall über TCP oder UDP Daten von anderen Hosts empfangen können. Die TURN-Server-Adresse und die Anmeldedaten eingeben.

Einrichten von Regeln für Ereignisse

Es können Regeln erstellt werden, damit das Gerät beim Auftreten bestimmter Ereignisse eine Aktion ausführt. Eine Regel besteht aus Bedingungen und Aktionen. Die Bedingungen können verwendet werden, um die Aktionen auszulösen. Beispielsweise kann das Gerät beim Erfassen einer Bewegung eine Aufzeichnung starten, eine E-Mail senden oder während der Aufzeichnung einen Overlay-Text anzeigen.

Weitere Informationen finden Sie unter *Erste Schritte mit Regeln für Ereignisse*.

Analysefunktionen und Anwendungen

Mit den Analysefunktionen und Anwendungen können Sie den Funktionsumfang Ihres Axis Geräts erweitern. Die AXIS Camera Application Platform (ACAP) ist eine offene Plattform, die es anderen Anbietern ermöglicht, Analysefunktionen und andere Anwendungen für Axis Geräte zu entwickeln. Anwendungen können auf dem Gerät vorinstalliert und kostenlos oder für eine Lizenzgebühr heruntergeladen werden.

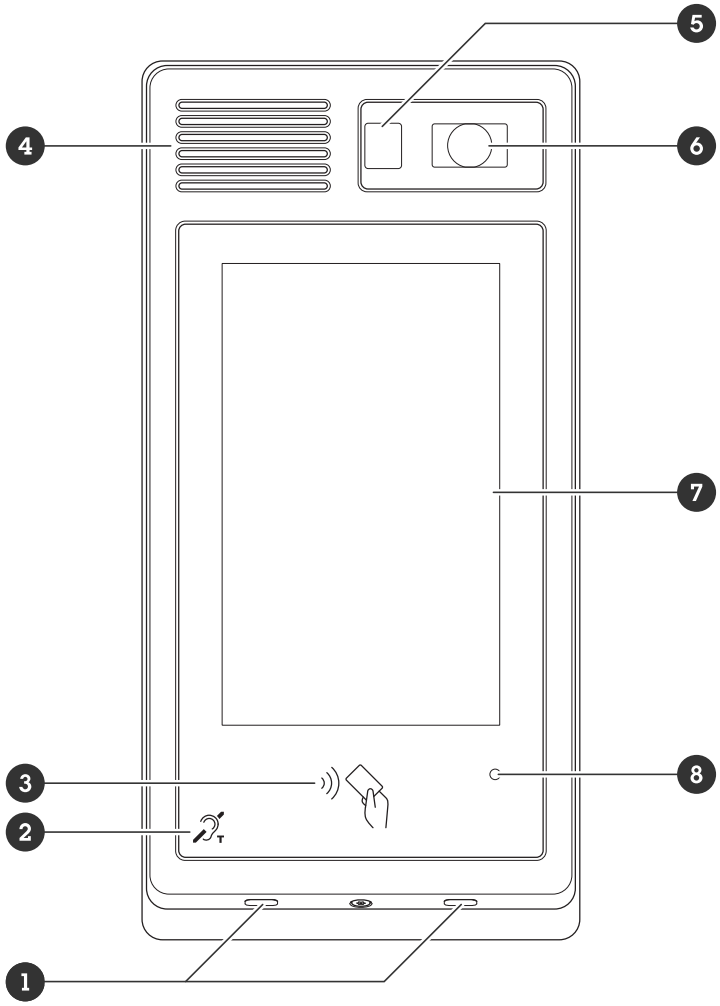
Benutzerhandbücher zu Axis Analysefunktionen und Anwendungen finden Sie auf *help.axis.com*.

AXIS Client for Unified Communication Systems

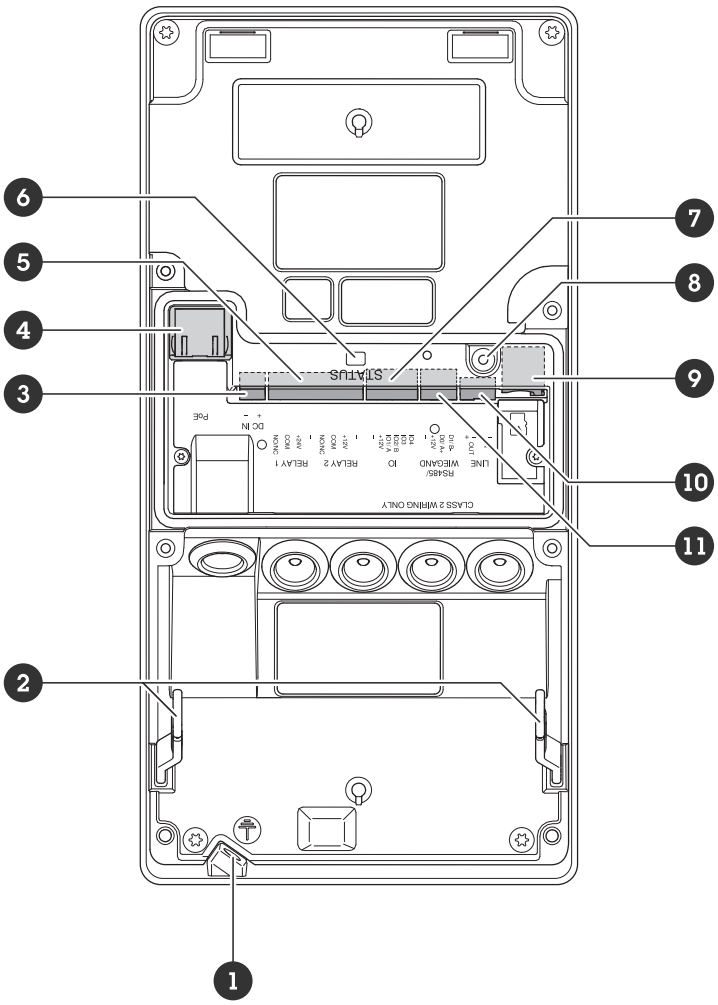
Mit dieser Anwendung können Sie Anrufe zwischen SIP-fähigen Axis Geräten und gekoppelten Microsoft® Teams-Konten tätigen. Weitere Informationen finden Sie im *Benutzerhandbuch zu AXIS Client for Unified Communication Systems*.

Technische Daten

Produktübersicht



1 *Mikrophone (x2)*
2 *T-Spule*
3 *RFID-Lesegerät*
4 *Lautsprecher*
5 *PIR-Sensor*
6 *Kamera*
7 *Anzeige*
8 *Lichtsensor*



1 *Erdungsschraube*
2 *Scharniere für die Installation*
3 *Stromanschluss*
4 *Netzwerk-Steckverbinder*
5 *Relaisanschluss (x2)*
6 *Status-LED*
7 *E/A-Anschluss*
8 *Steuertaste*
9 *Einschub für SD-Karte (MicroSD)*
10 *Audioanschluss*
11 *Lesegerätanschluss*

LED-Anzeigen

Status-LED	Anzeige
Grün	Leuchtet bei Normalbetrieb grün.

Einschub für SD-Speicherkarte

HINWEIS

- Gefahr der Beschädigung der SD-Karte. Verwenden Sie zum Einsetzen oder Entfernen der SD-Karte keine

scharfen Werkzeuge, Metallobjekte oder übermäßige Kraft. Setzen Sie die Karte mit den Fingern ein und entfernen Sie sie ebenfalls mit den Fingern.

- Gefahr von Datenverlust und beschädigten Aufzeichnungen. Entfernen Sie vor dem Herausnehmen die SD-Karte von der Weboberfläche des Geräts. Die SD-Karte darf nicht entfernt werden, während das Produkt in Betrieb ist.

Dieses Gerät unterstützt Karten des Typs microSD/microSDHC/microSDXC.

Für Empfehlungen zu SD-Karten siehe *axis.com*.

Die Logos microSD, microSDHC und microSDXC sind Marken von SD-3C, LLC. microSD, microSDHC und microSDXC sind in den USA und/oder anderen Ländern Marken oder eingetragene Marken von SD-3C, LLC.

Tasten

Steuertaste

Die Steuertaste hat folgende Funktionen:

- Zurücksetzen des Produkts auf die Werkseinstellungen. Siehe *Zurücksetzen auf die Werkseinstellungen, on page 30*.

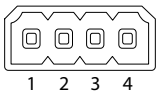
Anschlüsse

Netzwerk-Steckverbinder

RJ45-Ethernetanschluss mit Power over Ethernet Plus (PoE+).

Audioanschluss

Vierpolige Klemmleiste für Audioeingang und -ausgang.

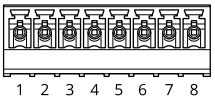


Funktion	Kontakt	Hinweise
Leitungseingang	1	Eingang (Mono)
GND	2	Audio-Masse
Line-Out	3	Line-Out
GND	4	Audio-Masse

Relaisanschluss

8-polige Klemmleiste für Solid State-Relais, der auf folgende Arten eingesetzt werden kann:

- Als Standardrelais, das zum Öffnen und Schließen von Zusatzstromkreisen verwendet wird.
- Zur direkten Steuerung einer Verriegelung.
- Zur Steuerung einer Verriegelung durch ein Sicherheitsrelais. Die Verwendung eines Sicherheitsrelais an der sicheren Seite der Tür verhindert ein Erwärmen der Drähte.



Funktion	Kontakt	Hinweise	Technische Daten
NO/NC	1	Normalerweise geöffnet/normalerweise geschlossen Zum Anschluss von Relaisgeräten. Die beiden Relaisanschlüsse sind galvanisch von den anderen Schaltkreisen getrennt.	Maximalstrom 1 A Max. Spannung 30 V DC
COM	2	Gemeinsam	
24 V Gleichstrom	3	Zur Stromversorgung von Zusatzgeräten. Hinweis: Dieser Kontakt kann nur als Stromausgang verwendet werden.	Ausgangsspannung 24 V Gleichstrom Maximalstrom 50 mA[1] Maximalstrom 300 mA[2]
Erdung Gleichstrom	4		0 V Gleichstrom
NO/NC	5	Normalerweise geöffnet/normalerweise geschlossen Zum Anschluss von Relaisgeräten. Die beiden Relaisanschlüsse sind galvanisch von den anderen Schaltkreisen getrennt.	Maximalstrom 1 A Max. Spannung 30 V DC
COM	6	Gemeinsam	
12 V Gleichstrom	7	Zur Stromversorgung von Zusatzgeräten. Hinweis: Dieser Kontakt kann nur als Stromausgang verwendet werden.	Ausgangsspannung 12 V DC Maximalstrom 100 mA[1] Maximalstrom 600 mA[2]
Erdung Gleichstrom	8		0 V Gleichstrom

Lesegerätanschluss

4-polige Klemmleiste für den Anschluss externer Leser.

Funktion	Kontakt	Hinweise	Technische Daten
Erdung Gleichstrom	1		0 V Gleichstrom
12 V Gleichstrom	2	Zur Stromversorgung von Zusatzgeräten. Hinweis: Dieser Kontakt kann nur als Stromausgang verwendet werden.	Ausgangsspannung 12 V Gleichstrom
D0/A+	3	Wiegand: DATA0-Ausgang RS485: A+	
D1/B-	4	Wiegand: DATA1-Ausgang RS485: B-	

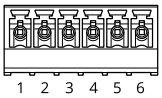
1. *Bei Stromversorgung über Power over Ethernet IEEE 802.3af/802.3at Typ 1 Klasse 3.*
2. *Bei Stromversorgung über Power over Ethernet Plus (PoE+) IEEE 802.3at Typ 2 Klasse 4 oder DC-Stromeingang.*

E/A-Anschluss

Über den E/A-Anschluss werden externe Geräte in Verbindung mit Manipulationsalarmen, Bewegungserkennung, Ereignisauslösung, Alarmbenachrichtigungen und anderen Funktionen angeschlossen. Zusätzlich zum Gleichstrombezugspunkt 0 V DC und der Stromversorgung (12-VDC-Ausgang) stellt der E/A-Anschluss folgende Schnittstellen bereit:

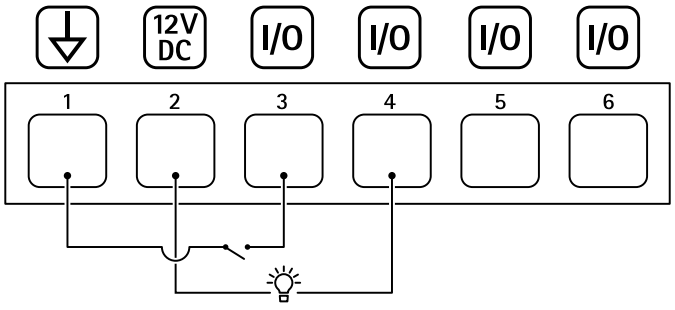
Digitaler Eingang – Zum Anschließen von Geräten, die zwischen geöffnetem und geschlossenem Schaltkreis wechseln können wie etwa PIR-Sensoren, Tür- und Fensterkontakte sowie Glasbruchmelder.

Digitalausgang – Zum Anschluss externer Geräte wie Relais und LEDs. Die angeschlossenen Geräte können über das VAPIX® Application Programming Interface, über ein Ereignis oder über die Weboberfläche des Geräts aktiviert werden.



Funktion	Kontakt	Hinweise	Technische Daten
Erdung Gleichstrom	1		0 V Gleichstrom
Gleichstromausgang	2	⚠ Kann für die Stromversorgung von Zusatzausrüstung verwendet werden. Hinweis: Dieser Kontakt kann nur als Stromausgang verwendet werden.	12 V Gleichstrom Max. Stromstärke = 50 mA
Konfigurierbar (Ein- oder Ausgang)	3–6	Digitaleingang – Zum Aktivieren an Kontakt 1 anschließen, zum Deaktivieren nicht anschließen.	0 bis max. 30 V Gleichstrom
		Digitaler Ausgang – Interne Verbindung mit Kontakt 1 (Erdschluss Gleichstrom), wenn aktiviert; unverbunden, wenn deaktiviert. Bei Verwendung mit einer induktiven Last wie etwa einem Relais muss zum Schutz vor Spannungssprüngen eine Diode parallel zur Last geschaltet werden.	0 bis max. 30 V Gleichstrom, Open-Drain, 100 mA

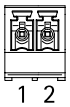
Beispiel:



1 *Erdung Gleichstrom*
2 *Gleichstromausgang 12 V, max. 50 mA*
3 *E/A als Eingang konfiguriert*
4 *E/A als Ausgang konfiguriert*
5 *Konfigurierbarer E/A*
6 *Konfigurierbarer E/A*

Stromanschluss

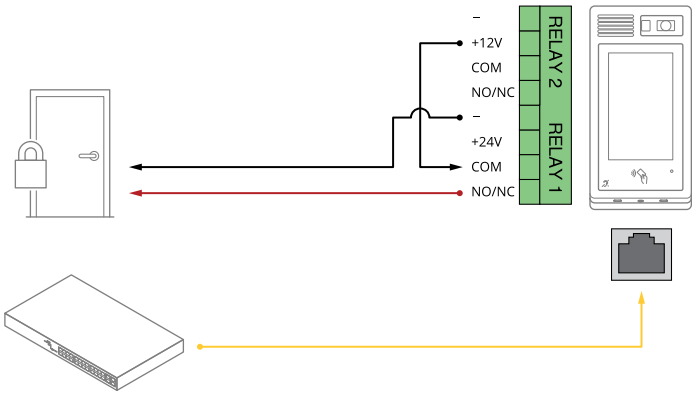
2-poliger Anschlussblock für die Gleichstromversorgung. Eine den Anforderungen für Schutzkleinspannung (SELV) entsprechende Stromquelle mit begrenzter Leistung (LPS) verwenden. Die Nennausgangsleistung muss dabei auf ≤100 W begrenzt sein oder der Nennausgangsstrom auf ≤5 A.



Funktion	Kontakt	Hinweise	Technische Daten
Erdung Gleichstrom	1		0 V Gleichstrom
Gleichstromeingang	2	Stromversorgung der Steuerung bei Nichtverwendung von Power over Ethernet. Hinweis: Dieser Kontakt kann nur für den Stromeingang verwendet werden.	18 bis 28 V DC, max. 22 W Max. Last an Ausgängen 9 W

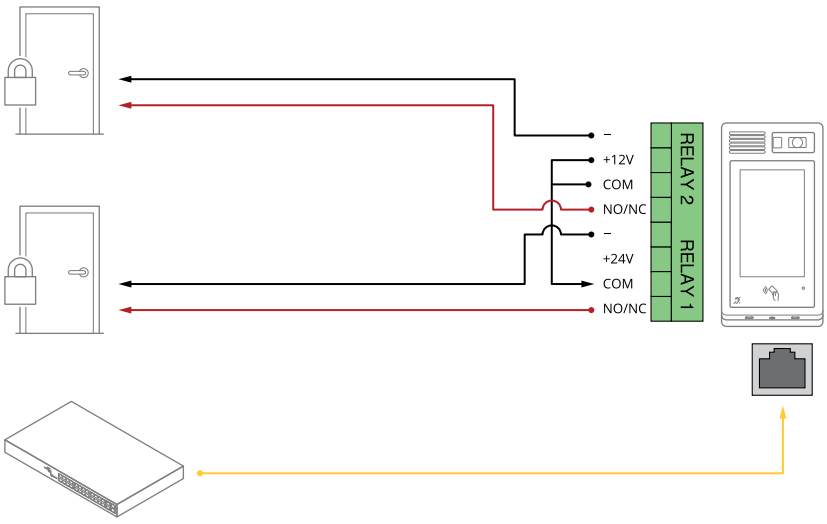
Geräte anschließen

Ein über PoE (12 V) gespeistes Relais



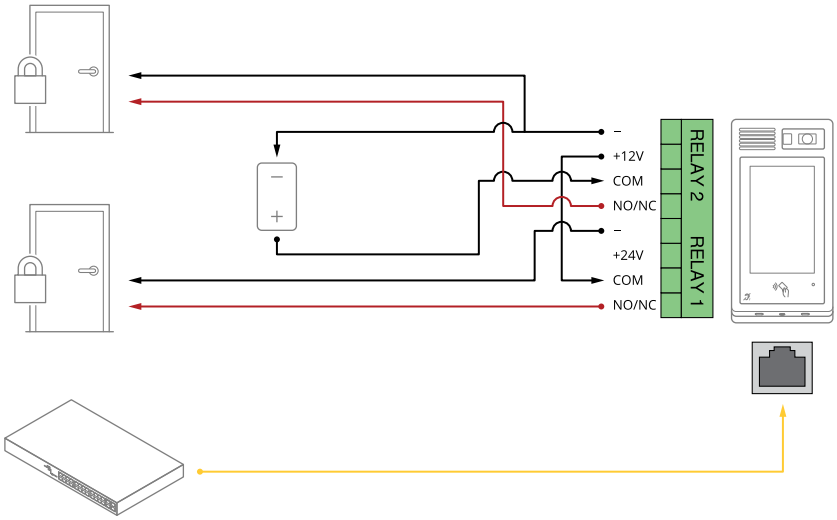
1. Um den Relaisstatus zu überprüfen, wechseln Sie zu **System > Accessories (System > Zubehör)** suchen Sie den Relaisport.
2. Stellen Sie den **Normal state (den Normalzustand)** auf:
   - für eine ausfallsichere Verriegelung.
   - für eine ausfallsichere Verriegelung.

Zwei über PoE (12 V) gespeiste Relais



1. Um den Relaisstatus zu überprüfen, wechseln Sie zu **System > Accessories (System > Zubehör)** suchen Sie den Relaisport.
2. Stellen Sie den **Normal state (den Normalzustand)** auf:
   - für eine ausfallsichere Verriegelung.
   - für eine ausfallsichere Verriegelung.

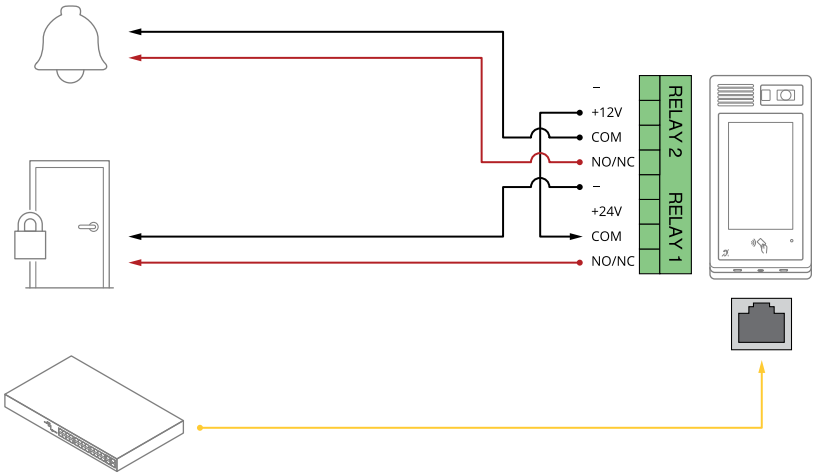
Ein über PoE (12 V) gespeistes Relais + ein über eine externe Stromversorgung gespeistes Relais



1. Um den Relaisstatus zu überprüfen, wechseln Sie zu **System > Accessories (System > Zubehör)** suchen Sie den Relaisport.
2. Stellen Sie den **Normal state (den Normalzustand)** auf:
   -  für eine ausfallsichere Verriegelung.
   -  für eine ausfallsichere Verriegelung.

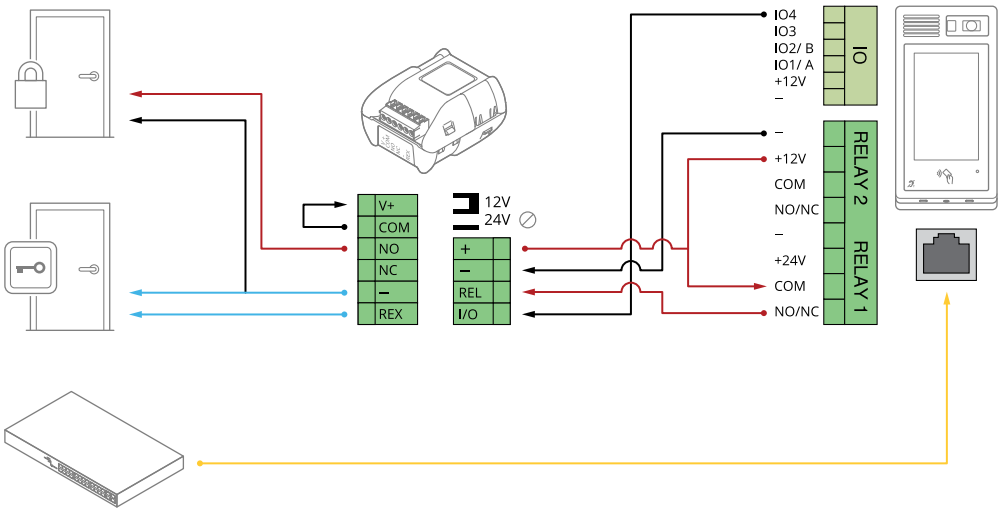
Ein über PoE (12 V) gespeistes Relais + ein potentialfreier Relaiskontakt

Der potenzialfreie Kontakt kann z. B. eine Türglocke sein.



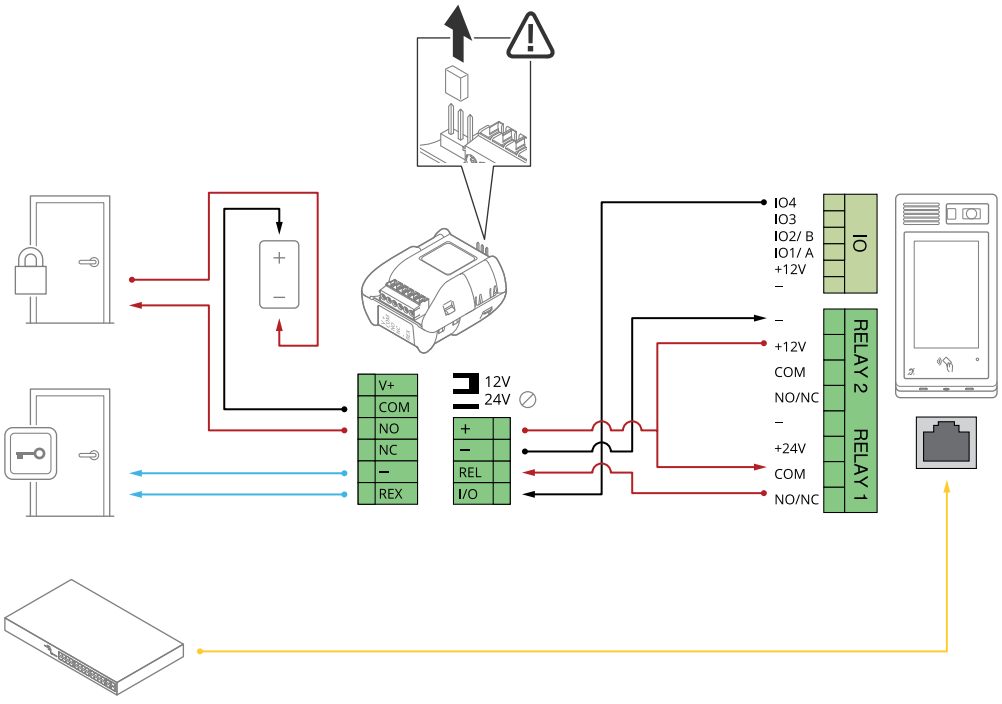
1. Um den Relaisstatus zu überprüfen, wechseln Sie zu **System > Accessories (System > Zubehör)** suchen Sie den Relaisport.
2. Stellen Sie den **Normal state (den Normalzustand)** auf:
   -  für eine ausfallsichere Verriegelung.
   -  für eine ausfallsichere Verriegelung.

Ausfallsicheres Schloss (12 V) mit PoE+ Stromversorgung über IP-Türsprechanlage



1. Um den Relaisstatus zu überprüfen, wechseln Sie zu **System > Accessories (System > Zubehör)** suchen Sie den Relaisport.
2. Stellen Sie den **Normal state (den Normalzustand)** auf:
   - für eine ausfallsichere Verriegelung.
   - für eine ausfallsichere Verriegelung.

Ausfallsicheres Schloss mit Stromversorgung über ein externes Netzteil

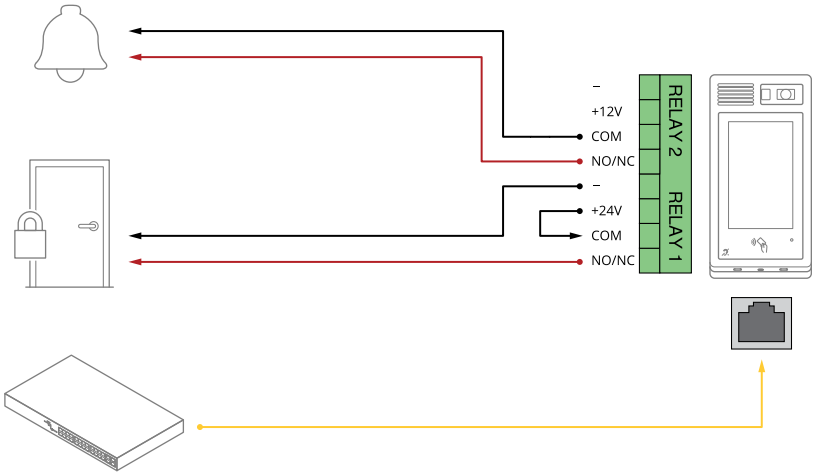


1. Um den Relaisstatus zu überprüfen, wechseln Sie zu **System > Accessories (System > Zubehör)** suchen Sie den Relaisport.
2. Stellen Sie den **Normal state (den Normalzustand)** auf:
   - für eine ausfallsichere Verriegelung.

–  für eine ausfallsichere Verriegelung.

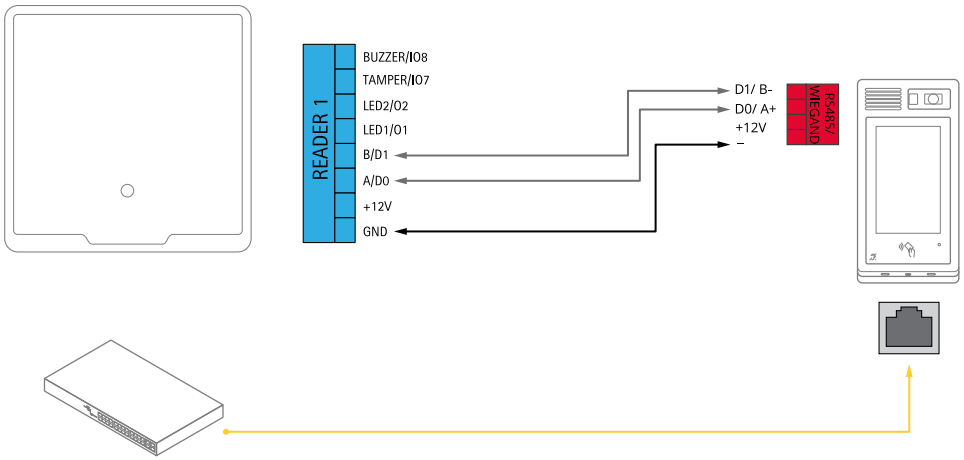
Ein über PoE (24 V) gespeistes Relais + ein potentialfreier Relaiskontakt

Der potenzialfreie Kontakt kann z. B. eine Türglocke sein.



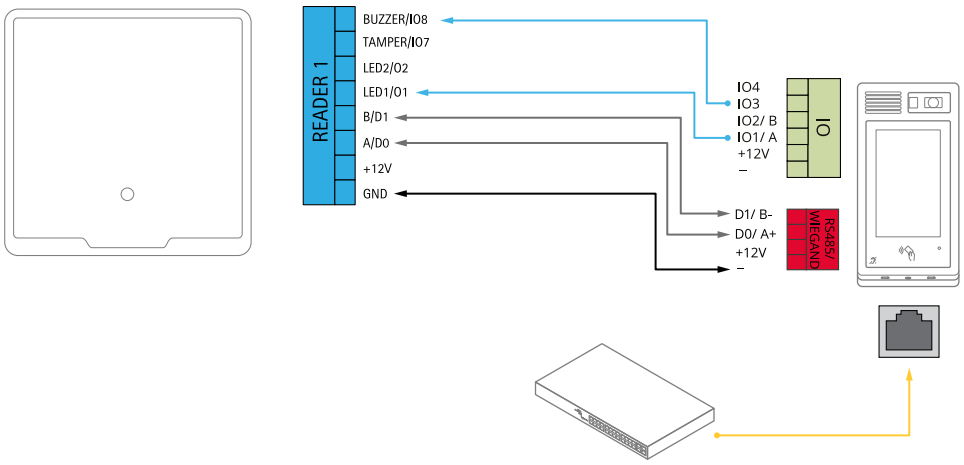
1. Um den Relaisstatus zu überprüfen, wechseln Sie zu **System > Accessories (System > Zubehör)** suchen Sie den Relaisport.
2. Stellen Sie den **Normal state (den Normalzustand)** auf:
   –  für eine ausfallsichere Verriegelung.
   –  für eine ausfallsichere Verriegelung.

Kartenleser verbunden mit Tür-Controller über OSDP



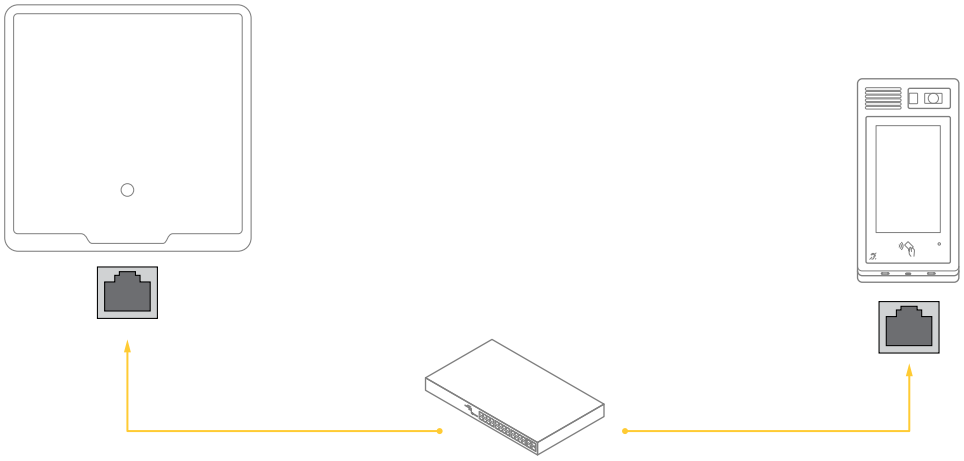
1. Gehen Sie zu **Reader (Kartenleser) > Connection (Verbindung) > Reader protocol (Kartenleserprotokoll)**.
2. Stellen Sie den **Reader protocol type (Protokolltyp des Kartenlesers)** auf **OSDP** und klicken Sie auf **Save (Speichern)**.

Kartenleser verbunden mit Tür-Controller über Wiegand



1. Gehen Sie zu **Reader (Kartenleser) > Connection (Verbindung) > Reader protocol (Kartenleserprotokoll)**.
2. Stellen Sie den **Reader protocol type (Protokolltyp des Kartenlesers)** auf **Wiegand** ein.
3. Aktivieren Sie den **Summer**.
4. Wählen Sie unter **Input for beeper (Eingang für Summer)** die Option **I3**.
5. Wählen Sie unter **Input used for LED control (Eingang für die LED-Steuerung)** die Option **1** aus.
6. Wählen Sie unter **Input for LED1 (Eingang für LED1)** die Option **I1**.
7. Nehmen Sie weitere Einstellungen vor und klicken Sie auf **Save (Speichern)**.

Kartenleser an Axis Tür-Controller mit VAPIX Kartenleser angeschlossen



1. Gehen Sie zu **Reader (Kartenleser) > Connection (Verbindung) > Reader protocol (Kartenleserprotokoll)**.
2. Stellen Sie den **Reader protocol type (Protokolltyp des Kartenlesers)** auf **VAPIX reader (VAPIX Kartenleser)** ein.
3. Verbinden Sie sich mit einem Axis Tür-Controller.

Fehlerbehebung

Zurücksetzen auf die Werkseinstellungen

Wichtig

Das Zurücksetzen auf die Werkseinstellungen muss mit Umsicht geschehen. Beim Zurücksetzen auf die Werkseinstellungen werden alle Einstellungen einschließlich der IP-Adresse zurückgesetzt.

Um das Produkt auf die Werkseinstellungen zurückzusetzen:

1. Trennen Sie das Gerät von der Stromversorgung.
2. Halten Sie die Steuertaste gedrückt und stellen Sie die Stromversorgung wieder her. Siehe *Produktübersicht, on page 19*.
3. Halten Sie die Steuertaste etwa 15–30 Sekunden gedrückt, bis die Status-LED gelb blinkt.
4. Lassen Sie die Steuertaste los. Der Vorgang ist abgeschlossen, wenn die LED-Statusanzeige grün wird. Wenn im Netzwerk kein DHCP-Server verfügbar ist, wird die IP-Adresse des Geräts standardmäßig auf eine der folgenden Adressen eingestellt:
   - **Geräte mit AXIS OS 12.0 und höher:** Beziehen sich auf das Subnetz der Adressen lokaler Links (169.254.0.0/16)
   - **Geräte bis AXIS OS 11.11:** 192.168.0.90/24
5. Verwenden Sie Installations- und Verwaltungstools, um IP-Adressen zuzuweisen, das Kennwort festzulegen und auf das Gerät zuzugreifen.
   Die Softwaretools für die Installation und Verwaltung stehen auf den Supportseiten unter *axis.com/support* zur Verfügung.

Die Parameter können auch über die Weboberfläche des Geräts auf die Werkseinstellungen zurückgesetzt werden. Gehen Sie auf **Wartung** > **Werkseinstellungen** und klicken Sie auf **Standardeinstellungen**.

Optionen für AXIS OS

Axis bietet eine Softwareverwaltung für Geräte entweder gemäß des aktiven Tracks oder gemäß Tracks für Langzeitunterstützung (LTS). Beim aktiven Track erhalten Sie einen kontinuierlichen Zugriff auf alle aktuellen Funktionen des Produkts. Die LTS-Tracks bieten eine feste Plattform, die regelmäßig Veröffentlichungen mit Schwerpunkt auf Bugfixes und Sicherheitsaktualisierungen bereitstellt.

Es wird empfohlen, AXIS OS vom aktiven Track zu verwenden, wenn Sie auf die neuesten Funktionen zugreifen möchten oder Axis End-to-End-Systemangebote nutzen. Die LTS-Tracks werden empfohlen, wenn Sie Integrationen von Drittanbietern verwenden, die nicht kontinuierlich auf den neuesten aktiven Track überprüft werden. Mit LTS kann die Cybersicherheit der Produkte gewährleistet werden, ohne dass signifikante Funktionsänderungen neu eingeführt oder vorhandene Integrationen beeinträchtigt werden. Ausführliche Informationen zur Vorgehensweise von Axis in Bezug auf Gerätesoftware finden Sie unter *axis.com/support/device-software*.

Aktuelle AXIS OS-Version überprüfen

AXIS OS bestimmt die Funktionalität unserer Geräte. Wir empfehlen Ihnen, vor jeder Problembehebung zunächst die aktuelle AXIS OS-Version zu überprüfen. Die aktuelle Version enthält möglicherweise eine Verbesserung, die das Problem behebt.

So überprüfen Sie die aktuelle AXIS OS-Version:

1. Rufen Sie die Weboberfläche des Geräts > **Status** auf.
2. Die AXIS OS-Version ist unter **Device info (Geräteinformationen)** angegeben.

AXIS OS aktualisieren

Wichtig

- Bei der Aktualisierung der Gerätesoftware werden Ihre vorkonfigurierten und benutzerdefinierten Einstellungen gespeichert. Axis Communications AB kann nicht garantieren, dass die Einstellungen gespeichert werden, selbst wenn die Funktionen in der neuen AXIS OS-Version verfügbar sind.
- Ab AXIS OS 12.6 müssen Sie jede einzelne LTS-Version zwischen der aktuellen Version Ihres Geräts und der Zielversion installieren. Wenn beispielsweise die derzeit installierte Gerätesoftwareversion AXIS OS 11.2 ist, müssen Sie die LTS-Version AXIS OS 11.11 installieren, bevor Sie das Gerät auf AXIS OS 12.6 aktualisieren können. Weitere Informationen finden Sie unter *AXIS OS Lifecycle guide: Upgrade path* (AXIS OS Lebenszyklus-Leitfaden: Aktualisierungspfad).
- Stellen Sie sicher, dass das Gerät während der Aktualisierung an die Stromversorgung angeschlossen ist.

Hinweis

- Beim Aktualisieren mit der aktuellen AXIS OS-Version im aktiven Track werden auf dem Gerät die neuesten verfügbaren Funktionen bereitgestellt. Lesen Sie vor der Aktualisierung stets die entsprechenden Aktualisierungsanweisungen und Versionshinweise. Die aktuelle AXIS OS-Version und die Versionshinweise finden Sie unter *axis.com/support/device-software*.

1. Die AXIS OS-Datei können Sie von *axis.com/support/device-software* kostenlos auf Ihren Computer herunterladen.
2. Melden Sie sich auf dem Gerät als Administrator an.
3. Rufen Sie **Maintenance (Wartung) > AXIS OS upgrade (AXIS OS-Aktualisierung)** auf und klicken Sie **Upgrade (Aktualisieren)** an.

Nach der Aktualisierung wird das Produkt automatisch neu gestartet.

Technische Probleme und mögliche Lösungen

Probleme beim Aktualisieren von AXIS OS

Aktualisierung von AXIS OS fehlgeschlagen

Nach fehlgeschlagener Aktualisierung lädt das Gerät erneut die Vorversion. Die häufigste Fehlerursache ist, wenn eine falsche AXIS OS-Datei hochgeladen wurde. Überprüfen, ob der Name der AXIS OS-Datei dem Gerät entspricht und erneut versuchen.

Probleme nach der AXIS OS-Aktualisierung

Bei nach dem Aktualisieren auftretenden Problemen die Installation über die **Wartungsseite** auf die Vorversion zurücksetzen.

Probleme beim Einrichten der IP-Adresse

IP-Adresse kann nicht eingestellt werden

- Wenn sich die IP-Adresse des Geräts und die IP-Adresse des zum Zugriff auf das Gerät verwendeten Computers in unterschiedlichen Subnetzen befinden, kann die IP-Adresse nicht eingestellt werden. Wenden Sie sich an Ihren Netzwerkadministrator, um eine IP-Adresse zu erhalten.
- Die IP-Adresse wird unter Umständen von einem anderen Gerät verwendet. Zur Überprüfung:
  1. Trennen Sie das Axis Gerät vom Netzwerk.
  2. Geben Sie in einem Befehls-/DOS-Fenster `ping` und die IP-Adresse des Geräts ein.
  3. Erscheint daraufhin `Reply from <IP address>: bytes=32; time=10...`, heißt das, dass die IP-Adresse möglicherweise bereits von einem anderen Gerät im Netzwerk verwendet wird. Bitten Sie den Netzwerkadministrator um eine neue IP-Adresse, und installieren Sie das Gerät erneut.
  4. `Request timed out` bedeutet, dass die IP-Adresse mit dem Axis Gerät verwendet werden kann. Prüfen Sie alle Kabel und installieren Sie das Gerät erneut.
- Es besteht unter Umständen ein Konflikt mit der IP-Adresse eines anderen Geräts im selben Subnetz. Die statische IP-Adresse des Axis Geräts wird verwendet, bevor der DHCP-Server eine dynamische Adresse festlegt. Verwendet also ein anderes Gerät standardmäßig dieselbe statische IP-Adresse, treten beim Zugreifen auf das Gerät möglicherweise Probleme auf.

Probleme beim Zugriff auf das Gerät

Anmeldung bei Gerätezugriff über einen Browser nicht möglich

Stellen Sie bei aktiviertem HTTPS sicher, dass Sie das richtige Protokoll (HTTP oder HTTPS) bei der Anmeldung verwenden. Gegebenenfalls müssen Sie manuell `http` oder `https` in das Adressfeld des Browsers eingeben.

Bei Verlust des Kennworts für das Haupt-Konto müssen Sie das Gerät auf die Werkseinstellungen zurücksetzen. Anweisungen finden Sie unter *Zurücksetzen auf die Werkseinstellungen, on page 30*.

Die IP-Adresse wurde von DHCP geändert

Von einem DHCP-Server zugeteilte IP-Adressen sind dynamisch und können sich ändern. Wenn die IP-Adresse geändert wurde, das Gerät mit AXIS IP Utility oder AXIS Camera Management im Netzwerk zu ermitteln. Das Gerät anhand seiner Modellnummer, Seriennummer oder anhand des DNS-Namens (sofern der Name konfiguriert wurde) ermitteln.

Bei Bedarf können Sie manuell eine statische IP-Adresse zuweisen. Anweisungen dazu finden Sie auf *axis.com/support*.

Zertifikatfehler beim Verwenden von IEEE 802.1X

Damit die Authentifizierung ordnungsgemäß funktioniert, müssen die Datums- und Uhrzeiteinstellungen des Axis Geräts mit einem NTP-Server synchronisiert werden. Gehen Sie auf **System > Date and time (System > Datum und Uhrzeit)**.

Der Browser wird nicht unterstützt.

Eine Liste der empfohlenen Browser finden Sie unter *Unterstützte Browser, on page 6*.

Externer Zugriff auf das Gerät ist nicht möglich

Für den externen Zugriff auf das Gerät wird die Verwendung einer der folgenden Anwendungen für Windows® empfohlen:

- AXIS Camera Station Edge: Kostenlos, ideal für kleine Systeme mit grundlegenden Überwachungsanforderungen.
- AXIS Camera Station Pro: Kostenlose 90-Tage-Testversion, ideal für kleine bis mittelgroße Systeme.

Auf *axis.com/vms* finden Sie Anweisungen und die Download-Datei.

Probleme mit MQTT

Verbindung über Port 8883 mit MQTT über SSL kann nicht hergestellt werden

Die Firewall blockiert den Datenaustausch über Port 8883, da dieser als unsicher gilt.

In einigen Fällen stellt der Server/Broker möglicherweise keinen bestimmten Port für die MQTT-Kommunikation bereit. Möglicherweise kann MQTT über einen Port verwendet werden, der normalerweise für HTTP/HTTPS-Datenverkehr verwendet wird.

- Wenn der Server/Broker WebSocket/WebSocket Secure (WS/WSS) unterstützt (in der Regel auf Port 443, verwenden Sie stattdessen dieses Protokoll. Prüfen Sie mit dem Betreiber des Servers/Brokers, ob WS/WSS unterstützt wird und welcher Port und welcher Basispfad verwendet werden soll.
- Wenn der Server/Broker ALPN unterstützt, kann die Verwendung von MQTT über einen offenen Port, z. B. 443, ausgehandelt werden. Erkundigen Sie sich bei Ihrem Server-/Brokeranbieter, ob ALPN unterstützt wird und welches ALPN-Protokoll und welchen Port Sie verwenden müssen.

Falls Sie hier nicht das Gesuchte finden, prüfen Sie den Bereich „Fehlerbehebung" auf *axis.com/support*.

Leistungsaspekte

Achten Sie bei der Einrichtung Ihres Systems unbedingt darauf, wie sich die verschiedenen Einstellungen und Situationen auf die Leistung auswirken. Einige Faktoren beeinflussen die Bandbreite (Bitrate), andere die Bildrate und wieder andere beides.

Die wichtigsten Umstände, die Sie berücksichtigen müssen, sind die folgenden:

- Hohe Bildauflösung und geringe Komprimierung führen zu Bildern mit mehr Daten, die wiederum mehr Bandbreite erfordern.
- Der Zugriff von vielen Clients des Typs Motion JPEG oder Unicast H.264/H.265/AV1 beeinflusst die Bandbreite.
- Die gleichzeitige Wiedergabe verschiedener Videostreams (Auflösung, Komprimierung) durch mehrere Clients beeinflusst sowohl die Bildrate als auch die Bandbreite.
  Wo immer möglich, identisch konfigurierte Videostreams verwenden, um eine hohe Bildrate zu erhalten. Videostreamprofile werden verwendet, um identische Videostreams sicherzustellen.
- Der gleichzeitige Zugriff auf Video-Streams mit unterschiedlichen Codecs wirkt sich sowohl auf die Bildrate als auch auf die Bandbreite aus. Für eine optimale Leistung sollten Sie Video-Streams mit demselben Codec verwenden.
- Die intensive Verwendung von Ereignissen beeinflusst die CPU-Auslastung, die sich wiederum auf die Bildrate auswirkt.
- Die Verwendung von HTTPS kann, besonders beim Streaming im Format Motion JPEG, die Bildrate reduzieren.
- Intensive Netzwerknutzung aufgrund mangelhafter Infrastruktur beeinflusst die Bandbreite.

- Die Wiedergabe auf schlecht arbeitenden Clientcomputern verringert die wahrgenommene Leistung und beeinflusst die Bildrate.
- Mehrere gleichzeitig ausgeführte ACAP-Anwendungen (AXIS Camera Application Platform) können die Bildrate und die allgemeine Leistung beeinflussen.

Support

Weitere Hilfe erhalten Sie hier: *axis.com/support*.

Sicherheitshinweise

Gefährdungsstufen

⚠ GEFAHR

Weist auf eine gefährliche Situation hin, welche, falls nicht verhindert, zu Tod oder schweren Verletzungen führen kann.

⚠ WARNUNG

Weist auf eine gefährliche Situation hin, welche, falls nicht verhindert, zu Tod oder schweren Verletzungen führen kann.

⚠ VORSICHT

Weist auf eine gefährliche Situation hin, welche, falls nicht verhindert, zu geringfügiger oder mäßiger Verletzung führen kann.

HINWEIS

Weist auf eine gefährliche Situation hin, welche, falls nicht verhindert, zu Sachschäden führen kann.

Weitere Hinweise

Wichtig

Weist auf wichtige Informationen hin, die den richtigen Betrieb des Produkts gewährleisten.

Hinweis

Weist auf nützliche Informationen hin, die die optimale Verwendung des Produkts unterstützen.

Cybersicherheit

Cybersicherheit trägt zu einem erfolgreichen Produktlebenszyklus bei, bei dem Risiken auf ein Minimum reduziert werden. Ausführliche Informationen und Dokumente zu unserer Cybersicherheitsstrategie finden Sie auf *axis.com/about-axis/cybersecurity*. Befolgen Sie die nachstehenden Richtlinien zur Cybersicherheit, um Sicherheitsbenachrichtigungen von Axis zu erhalten und Ihr Produkt für eine sichere Benutzung und Außerbetriebnahme zu konfigurieren.

Unter *Axis Trust Center* finden Sie Informationen darüber, wie Axis die Einhaltung von Sicherheitsvorschriften, Transparenz, Datenschutz und den Schutz der Privatsphäre implementiert.

Schwachstellen-Management

Axis ist eine *Common Vulnerability and Exposures (CVE) Numbering Authority (CNA)*. Um das Risiko einer Gefährdung für Sie so gering wie möglich zu halten, halten wir uns bei der Erkennung und Behebung von Sicherheitslücken in unseren Geräten, unserer Software und unseren Diensten an die Branchenstandards. Weitere Informationen zu unseren Richtlinien zur Verwaltung von Sicherheitslücken oder zur Meldung einer Schwachstelle finden Sie unter *axis.com/vulnerability-management*.

Sicherheitsbenachrichtigungen

Sicherheitsbenachrichtigungs-E-Mails von Axis können Sie auf *axis.com/security-notification-service* abonnieren. Wir informieren Sie über Schwachstellen, geben entsprechende Sicherheitshinweise und benachrichtigen Sie zu anderen sicherheitsrelevanten Themen für Ihr Axis Produkt.

Sicherer Produktlebenszyklus

Axis minimiert Risiken über die gesamte Lebensdauer unserer Produkte hinweg durch eine sichere Verwaltung des Lebenszyklus. Nutzen Sie unsere Sicherheitsrichtlinien unter *help.axis.com*, um Ihre Axis Produkte sicherer zu konfigurieren und zum Betrieb zu nutzen und um Informationen zu folgenden Themen zu erhalten:

Sichere Erstnutzung – Axis Produkte sind standardmäßig mit einem hohen Sicherheitsniveau in der Konfiguration vorkonfiguriert, um von Anfang an eine sichere Inbetriebnahme und verschlüsselte Kommunikation zu gewährleisten.

Bestimmungsgemäßer Gebrauch und häufige Fehler bei der Konfiguration – Unsere Anleitungen enthalten Informationen zur bestimmungsgemäßen Verwendung von Axis Produkten, einschließlich häufiger sicherheitsrelevanter Fehlbedienungen und Fehler bei der Konfiguration, die vermieden werden sollten.

Sicherheitslücken und Transparenz in der Lieferkette verwalten – Mit jeder Softwareversion wird auf *axis.com* eine Software-Bestellliste (SBOM) veröffentlicht, um Sicherheitslücken offenzulegen und die Transparenz in der Lieferkette zu verbessern.

Stilllegung und die sichere Löschung von Daten – Um ein Produkt am Ende seines Lebenszyklus sicher außer Betrieb zu nehmen, setzen Sie es auf die Werkseinstellungen zurück. Dadurch werden Ihre Konfigurationen, gespeicherten Daten und vertraulichen Informationen gelöscht.

T10213214_de

2026-10 (M12.2)

© 2025 – 2026 Axis Communications AB