

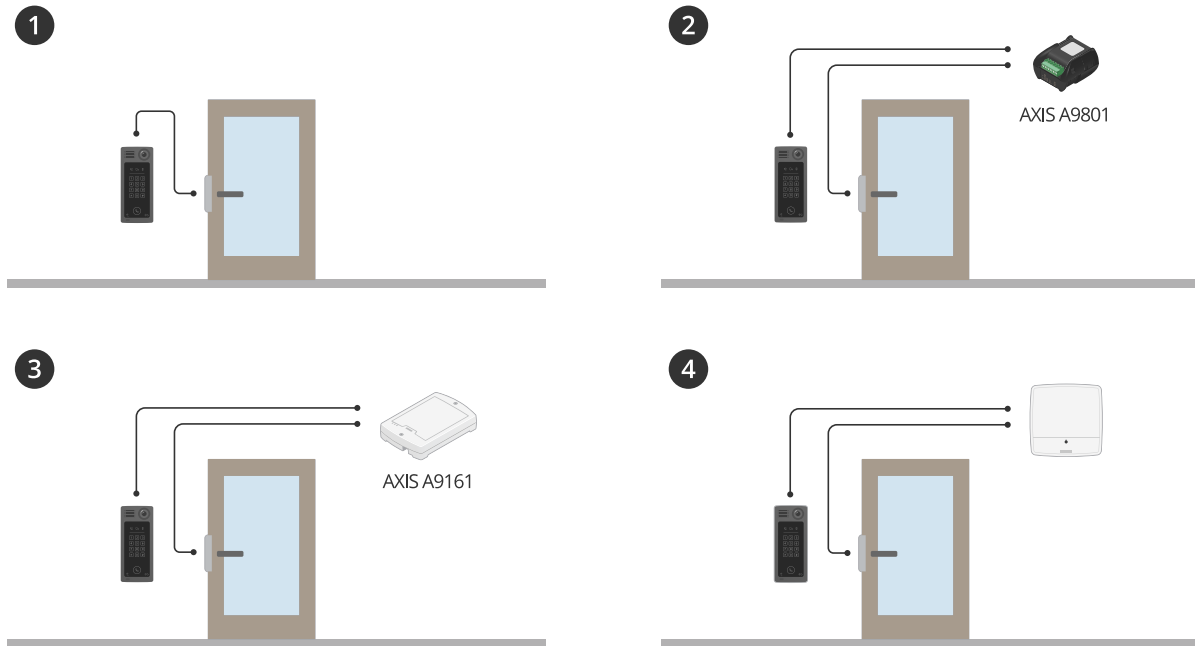
AXIS A8207-VE Mk II Network Video Door Station

Inhalt

Lösungsübersicht	4
Produktübersicht	5
Installation	7
Funktionsweise.....	8
Das Gerät im Netzwerk ermitteln	8
Unterstützte Browser.....	8
Weboberfläche des Geräts öffnen	8
Administratorkonto erstellen	8
Sichere Kennwörter	9
Stellen Sie sicher, dass keiner die Gerätesoftware manipuliert hat.	9
Übersicht über die Weboberfläche.....	9
Weitere Einstellungen	10
Das Root-Kennwort ändern	10
Remote-Lautsprechertests kalibrieren und ausführen	10
Direktes SIP (P2P) einrichten	10
SIP über einen Server (PBX) einrichten	11
Erstellen eines Kontakts	12
Konfigurieren der Anruftaste	12
Einrichtung als Kartenleser.....	12
Verwendung der Zugangsberechtigungsliste, um Eigentümern von Zugangsdaten den Zugang zu gewähren	13
Einrichtung als Kartenleser mithilfe einer Tür-Steuerung	14
Verwenden Sie geschützte Daten auf Karten, um die Sicherheit zu erhöhen.....	15
Verwenden Sie DTMF, um die Tür für einen Besucher zu entriegeln.	15
Live-Videoübertragung an einen Monitor.....	16
Weboberfläche	17
Mehr erfahren	18
Voice over IP (VoIP)	18
Session Initiation Protocol (SIP).....	18
Peer-to-Peer SIP (P2PSIP).....	18
Private Branch Exchange (PBX)	19
Einrichten von Regeln für Ereignisse.....	20
Analysefunktionen und Anwendungen.....	20
AXIS Client for Unified Communication Systems	20
Tägliche Nutzung.....	21
Verwenden des Tastenfelds.....	21
Fehlerbehebung	22
Zurücksetzen auf die Werkseinstellungen.....	22
Aktuelle AXIS OS-Version überprüfen	22
AXIS OS aktualisieren	22
Technische Probleme, Hinweise und Lösungen.....	23
Leistungsaspekte.....	24
Technische Daten.....	25
Anzeigen und Bedienelemente an der Vorderseite.....	25
Indikatorsymbole.....	25
Kartenleser-Markierungsstreifen	25
Ruftaste	25
LED-Anzeigen	25
Einschub für SD-Speicherkarte.....	25
Tasten.....	25
Steuertaste	25
Anschlüsse	26
HDMI-Anschluss.....	26

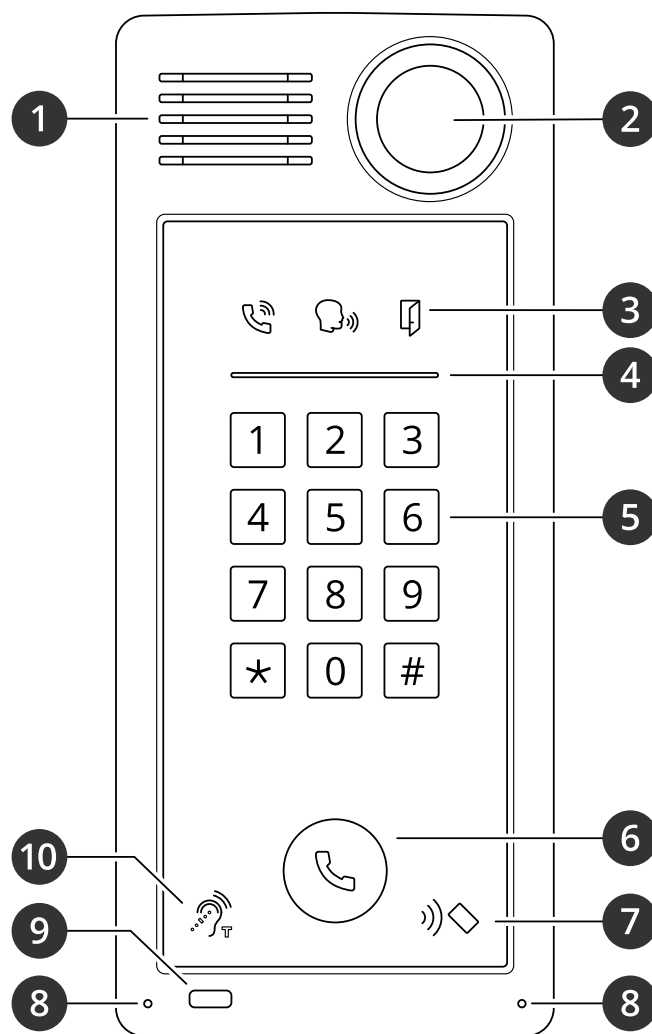
Netzwerk-Anschluss	26
Audioanschluss	26
Relaisanschluss	26
Lesegerätanschluss	27
E/A-Anschluss	27
Stromanschluss	28
Sicherheitsinformationen.....	30
Gefährdungstufen	30
Andere Meldeebenen	30
Cybersicherheit.....	31
Schwachstellen-Management	31
Sicherheitsbenachrichtigungen.....	31
Sicherer Produktlebenszyklus.....	31

Lösungsübersicht

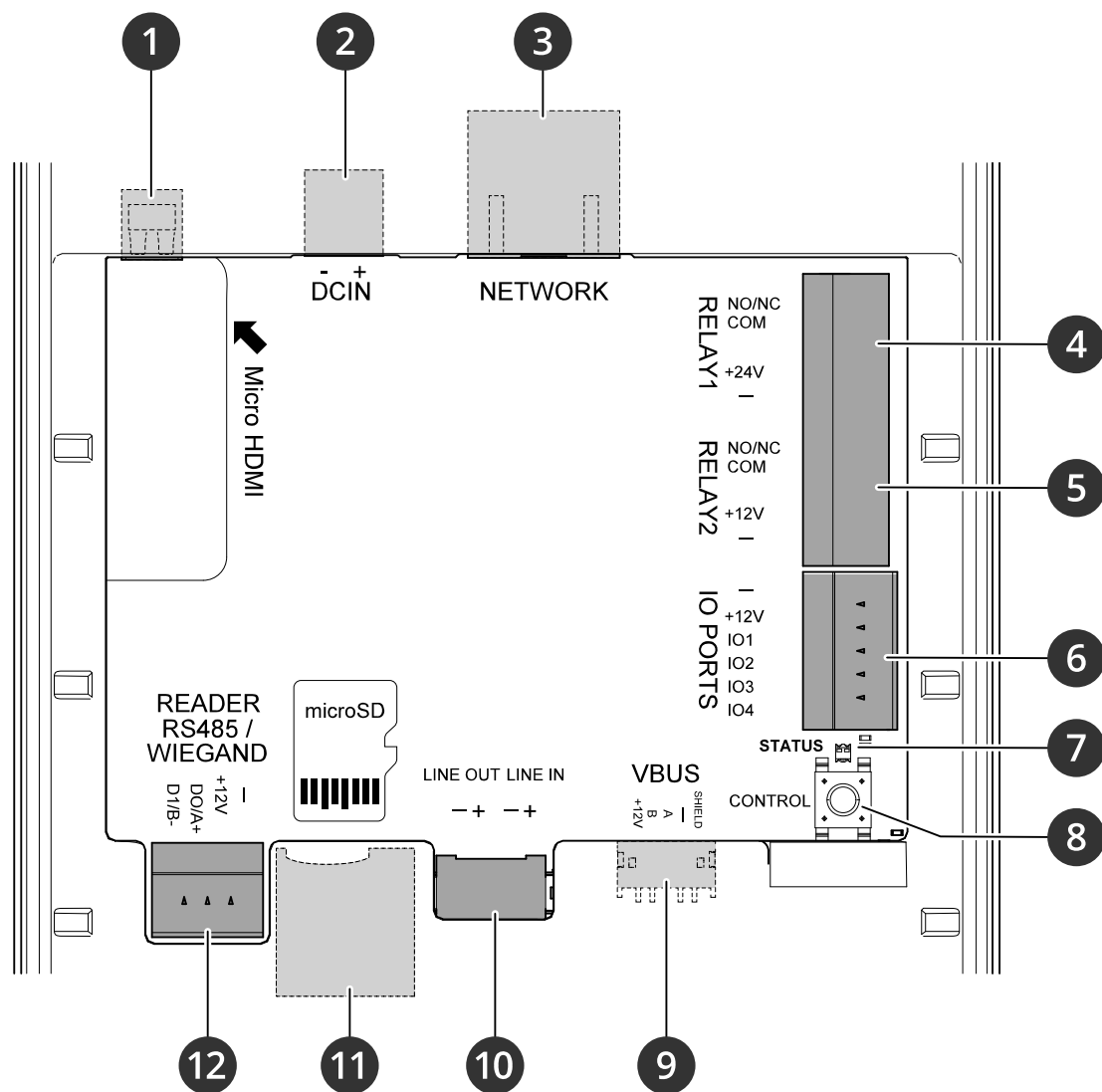


- 1 Türanlage
- 2 Türstation kombiniert mit AXIS A9801
- 3 Türstation kombiniert mit AXIS A9161
- 4 Türstation kombiniert mit einem Zutrittskontrollsystem, wie z. B. AXIS A1001 oder AXIS A1601

Produktübersicht



- 1 Lautsprecher
- 2 Kamera
- 3 Indikatorsymbole, on page 25
- 4 Kartenleser-Markierungsstreifen, on page 25
- 5 Funktionstastenfeld
- 6 Ruftaste, on page 25
- 7 Kartenleser-Symbol
- 8 Mikrofon
- 9 PIR-Sensor
- 10 T-Spule-Symbol



- 1 HDMI-Anschluss, on page 26 (microHDMI)
- 2 Stromanschluss, on page 28
- 3 Netzwerk-Anschluss, on page 26 (PoE+)
- 4 Relaisanschluss, on page 26
- 5 Relaisanschluss, on page 26
- 6 E/A-Anschluss, on page 27
- 7 Status-LED
- 8 Steuertaste, on page 25
- 9 2N-VBUS (nicht belegt)
- 10 Audioanschluss, on page 26
- 11 Einschub für SD-Speicherkarte, on page 25 (microSD/microSDHC/microSDXC)
- 12 Lesegerätanschluss, on page 27

Installation



Rufen Sie zur Wiedergabe dieses Videos die Webversion dieses Dokuments auf.

Installationsvideo für den Leser A8207-VE.



Rufen Sie zur Wiedergabe dieses Videos die Webversion dieses Dokuments auf.

Installationsvideo für das Relais A8207-VE.

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

*: Unterstützt mit Einschränkungen

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 kennen, 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 *Administratorkonto erstellen, on page 8*.

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

Administratorkonto erstellen

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

1. Einen Benutzernamen eingeben.
2. Geben Sie ein Passwort ein. Siehe *Sichere Kennwörter, on page 9*.
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 22*.

Sichere Kennwörter

Wichtig

Verwenden Sie HTTPS (standardmäßig aktiviert), um Ihr Kennwort oder andere sensible Konfigurationen über das Netzwerk einzustellen. HTTPS ermöglicht sichere und verschlüsselte Netzwerkverbindungen und schützt so sensible Daten wie 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 keiner die Gerätesoftware manipuliert hat.

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 22*. Nach dem Zurücksetzen gewährleistet Secure Boot den Status des Geräts.
2. Konfigurieren und installieren Sie das Gerät.

Übersicht über die Weboberfläche

In diesem Video erhalten Sie einen Überblick über die Weboberfläche des Geräts.



Weboberfläche des Axis Geräts

Weitere Einstellungen

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

Das Root-Kennwort ändern

1. Melden Sie sich in der Geräteschnittstelle an, und wechseln Sie zu **System > Benutzer**.
2. Klicken Sie für den Root-Benutzer auf  > **Update user (Benutzer aktualisieren)**.
3. Ein neues Kennwort eingeben und **Save (Speichern)** anklicken.

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 5 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 18.

Auf diesem Gerät wird VoIP über das SIP-Protokoll aktiviert. Weitere Informationen zu SIP finden Sie unter *Session Initiation Protocol (SIP)*, on page 18

Es gibt zwei Typen von Setups für SIP: Direkt oder Peer-to-Peer (P2P) ist einer von ihnen. Verwenden Sie Peer-to-Peer, wenn die Kommunikation zwischen wenigen Benutzern 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 18.

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, **Allow incoming calls (Eingehende Anrufe erlauben)** anklicken.

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 Standardstartport ist 4000. Möglicherweise blockieren einige Firewalls RTP-Datenverkehr an bestimmten Portnummern. 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 .

10. **Save (Speichern)** anklicken.

SIP über einen Server (PBX) einrichten

Bei VoIP (Voice over IP) handelt es sich um eine Technologiegruppe, die Sprachkommunikation und Multimediatelefonie über IP-Netzwerke ermöglicht. Weitere Informationen finden Sie unter *Voice over IP (VoIP)*, on page 18.

Auf diesem Gerät wird VoIP über das SIP-Protokoll aktiviert. Weitere Informationen zu SIP finden Sie unter *Session Initiation Protocol (SIP)*, on page 18

Es gibt zwei Typen von Setups für SIP: Einer davon ist ein PBX-Server. Verwenden Sie einen PBX-Server, wenn die Kommunikation zwischen einer unbegrenzten Anzahl von Benutzern 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 19.

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. **Save (Speichern)** anklicken.
8. Um die SIP-Einstellungen auf die gleiche Weise wie für Peer-to-Peer einzurichten, siehe *Direktes SIP (P2P) einrichten, on page 10* 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 18*.

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. **Save (Speichern)** anklicken.

Konfigurieren der Anruftaste

In der Standardeinstellung ist die Anruf-Schaltfläche so konfiguriert, dass VMS-Anrufe (Video Management Software) getätigt werden können. Wenn Sie diese Konfiguration beibehalten möchten, müssen Sie lediglich die Axis IP-Türsprechanlage zum VMS hinzufügen.

In diesem Beispiel wird erläutert, wie das System eingerichtet werden muss, um einen Kontakt in der Kontaktliste aufzurufen, wenn die Anruftaste gedrückt wird.

1. Rufen Sie **Communication > Calls > Call button (Kommunikation > Anrufe > Anruftaste)** auf.
2. Entfernen Sie unter **Recipients (Empfänger)** die Option **VMS**.
3. Wählen Sie unter **Recipients (Empfänger)** einen vorhandenen Kontakt aus oder erstellen Sie einen neuen.

Um die Anruftaste zu deaktivieren, deaktivieren Sie **Anruftaste aktivieren**.

Einrichtung als Kartenleser

Sie können Ihre Türstation als Kartenleser einrichten, damit Eigentümer von Zugangsdaten die Tür öffnen können.

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

Bei Verbindung der Türstation mit einer Tür-Steuerung kann die Türstation 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 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. **Save (Speichern)** anklicken.

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. **Save (Speichern)** anklicken.

Einrichtung als Kartenleser mithilfe einer Tür-Steuerung

Netzwerk-Verbindung

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 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 14*.

Einrichten der Türstation 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. **Save (Speichern)** anklicken.

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.

Bevor Sie beginnen:

- Schließen Sie die Türstation an die Türsteuerung an.
Siehe Schaltpläne, die auf axis.com/products/axis-a8207-ve-mk-ii/support zum Download stehen.
- Konfigurieren Sie die Hardware der Türsteuerung mit dem Wiegand-Protokoll für den Leser. Weitere Anweisungen finden Sie im Benutzerhandbuch der Türsteuerung.

Einrichten der Türstation 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. **Save (Speichern)** anklicken.

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**.

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. **Save (Speichern)** anklicken.

Verwenden Sie DTMF, um die Tür für einen Besucher zu entriegeln.

Wenn ein Besucher einen Anruf von der Türstation tätigt, kann die antwortende Person mithilfe des DTMF (Dual-Tone Multi-Frequency Signaling) des SIP-Geräts die Tür entriegeln. Die Türsteuerung entriegelt und verriegelt die Tür.

Dieses Beispiel erläutert, wie:

- Definieren des DTMF-Signals in der Türstation
- wie Sie die Türstation einrichten, um:
 - die Türsteuerung aufzufordern, die Tür zu entriegeln oder
 - die Tür mithilfe des internen Relais zu entriegeln.

Sie machen alle Einstellungen auf der Webseite der Türstation.

Bevor Sie beginnen:

- SIP-Anrufe vom Gerät zulassen und ein SIP-Konto erstellen. Siehe *Direktes SIP (P2P) einrichten, on page 10* und *SIP über einen Server (PBX) einrichten, on page 11*.

Definieren des DTMF-Signals in der Türstation

1. Gehen Sie zu **Communication (Kommunikation) > SIP > DTMF**.
2. Klicken Sie auf **+ Add sequence (+ Sequenz hinzufügen)**.
3. Geben Sie unter **Sequence (Sequenz)** **1** ein:
4. Geben Sie in **Description (Beschreibung)**, **Unlock door (Tür entriegeln)** ein.
5. Wählen Sie unter **Accounts (Konten)** das SIP-Konto aus.
6. **Save (Speichern)** anklicken.

Richten Sie die Türstation so ein, dass sie zum Entriegeln der Tür das interne Relais verwendet.

7. Gehen Sie auf **System > Events > Rules (System > Ereignisse > Regeln)** und fügen Sie eine Regel hinzu.
8. Geben Sie im Feld **Name** **DTMF unlock door (DTMF – Tür entriegeln)** ein.
9. Wählen Sie in der Liste der Bedingungen unter **Call (Anruf) DTMF** und **Unlock door (Tür entriegeln)** aus.
10. Wählen Sie in der Liste der Aktionen unter **E/A** die Option **Toggle I/O once (Einmal zwischen E/A umschalten)**.
11. Wählen Sie aus der Liste der Ports **Relay 1 (Relais 1)** aus.
12. Stellen Sie die **Duration (Dauer)** auf **00:00:07**, d. h. die Tür ist 7 Sekunden lang geöffnet.
13. **Save (Speichern)** anklicken.

Live-Videoübertragung an einen Monitor

Das Gerät kann einen Live-Videostream ohne Netzwerk-Verbindung an einen HDMI-Monitor übertragen. Verwenden Sie den Monitor, um zu sehen, wer an der Tür ist.

1. Schließen Sie einen externen Monitor über den HDMI-Anschluss an.
2. Passen Sie die HDMI-Einstellungen unter **System > Videoausgang** an.

Weboberfläche

Um sich über alle Funktionen und Einstellungen zu informieren, die in der Weboberfläche von Geräten mit AXIS OS verfügbar sind, rufen Sie die *Hilfe zur Weboberfläche von AXIS OS* auf.

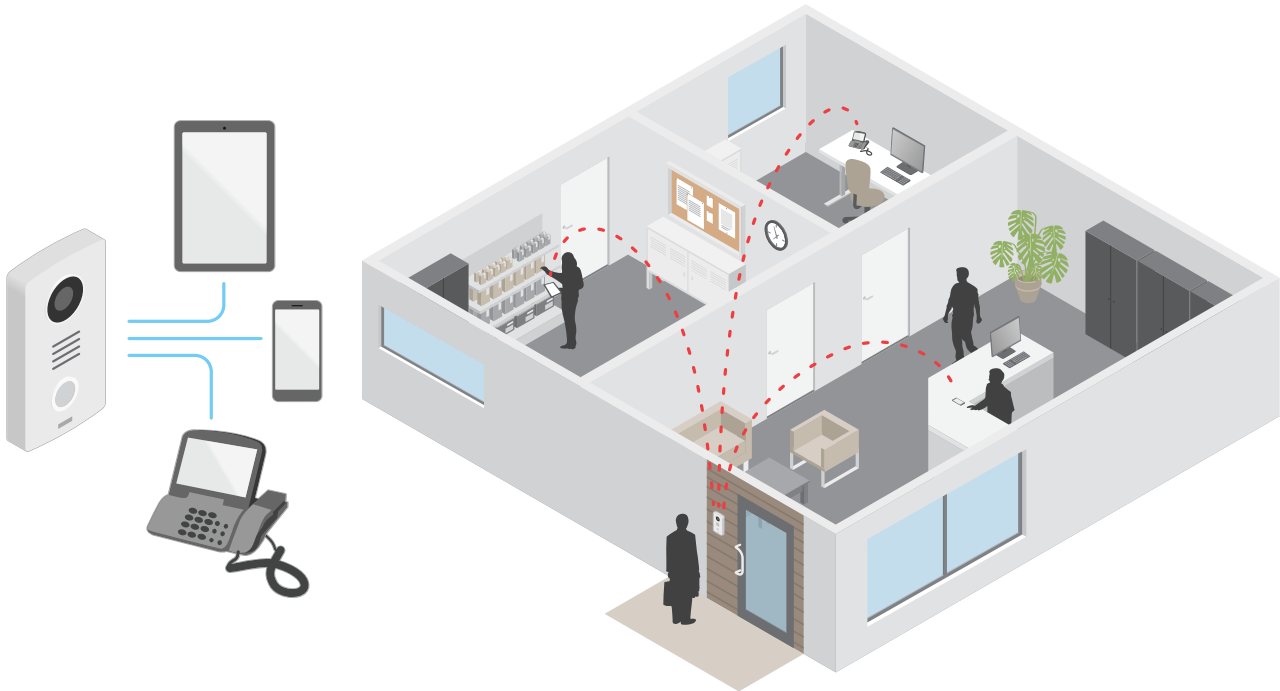
Mehr erfahren

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 Türstation 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.

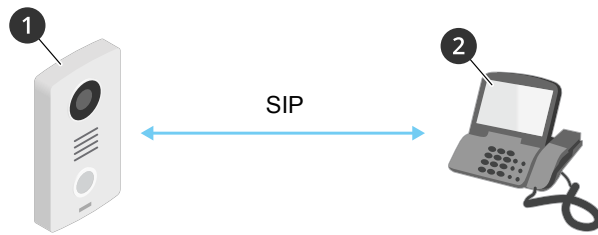
Die eigentlichen Audio- bzw. Videoübertragungen werden zwischen den SIP-Benutzeragenten mit einem Transportprotokoll, wie z. B. RTP (Real-Time Transport Protocol), ausgetauscht.

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. In diesem Fall ist eine typische SIP-Adresse `sip:<local-ip>`.

Beispiel:



- 1 Benutzeragent A-door Station. SIP-Adresse: sip:192.168.1.101
- 2 Benutzeragent B – SIP-fähiges Telefon. SIP-Adresse: sip:192.168.1.100

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

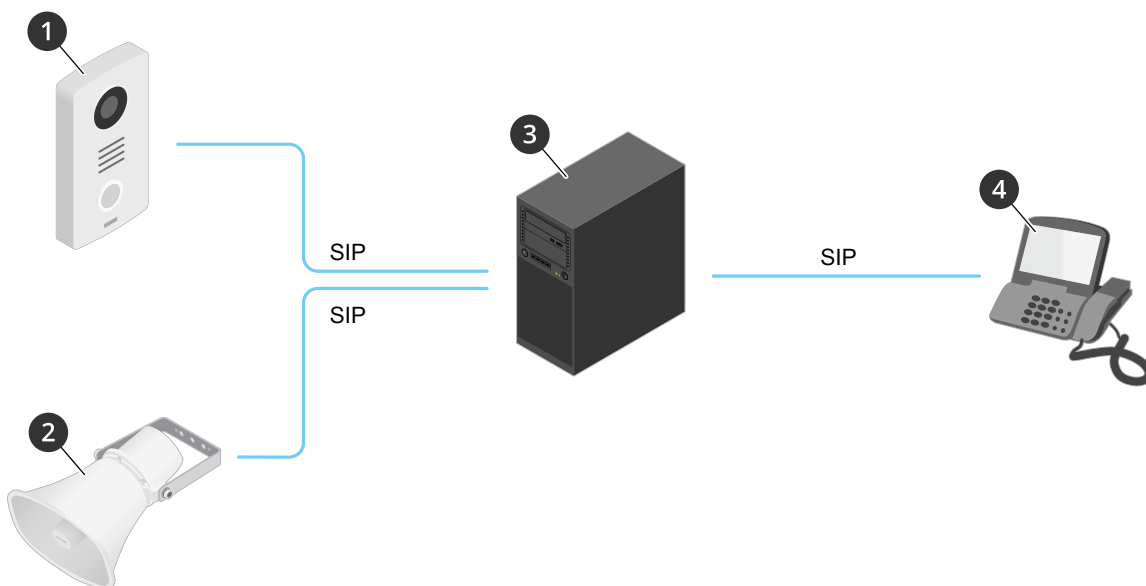
Private Branch Exchange (PBX)

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-Benutzer wird bei der Nebenstellenanlage registriert und kann dann die anderen über die entsprechende Durchwahl erreichen. In diesem Fall ist eine typische SIP-Adresse 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 Türstation drücken, wird der Anruf über eine oder mehrere PBX-Anlagen an eine SIP-Adresse entweder im lokalen IP-Netzwerk oder über das Internet weitergeleitet.

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*.

Tägliche Nutzung

Verwenden des Tastenfelds

Absicht	Aktion
Rufen Sie jemanden an, der mich in das Gebäude lassen kann.	Drücken Sie  .
Rufen Sie eine Person im Gebäude an.	Geben Sie die Kurzwahlnummer der Person ein und drücken Sie  .
Öffnen der Tür mit meiner Karte und PIN.	Tippen Sie auf die Karte und geben Sie die PIN ein.
Öffnen der Tür mit meinem PIN.	Geben Sie die PIN ein und drücken Sie #.
Öffnen der Tür mit meiner Karte.	Tippen Sie auf die Karte.

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 5*.
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 dem Gerät standardmäßig eine der folgenden IP-Adressen zugewiesen:
 - Geräte mit AXIS OS 12.0 oder höher: Zuweisung aus dem Subnetz der verbindungslokalen Adressen (169.254.0.0/16)
 - Geräte mit AXIS OS 11.11 oder niedriger: 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**.

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 Leitfaden zum Lebenszyklus: Upgrade-Pfad*.
- 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, Hinweise und Lösungen

Falls Sie hier nicht das Gesuchte finden, bitte den Bereich „Fehlerbehebung“ unter axis.com/support aufrufen.

Probleme beim Aktualisieren der Firmware	
Aktualisierung der Firmware fehlgeschlagen	Nach fehlgeschlagener Aktualisierung der Firmware lädt das Gerät erneut die Vorversion. Die häufigste Fehlerursache ist, wenn eine falsche Firmwaredatei hochgeladen wurde. Überprüfen, ob der Name der Firmwaredatei dem Gerät entspricht und erneut versuchen.

Probleme beim Einrichten der IP-Adresse

Das Gerät befindet sich in einem anderen Subnetz	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 von einem anderen Gerät verwendet	Trennen Sie das Axis Gerät vom Netzwerk. Führen Sie einen Ping-Befehl aus (geben Sie in einem Befehls-/DOS-Fenster <code>ping</code> und die IP-Adresse des Geräts ein): • Wenn Sie <code>Reply from <IP address>: bytes=32; time=10...</code> empfangen, bedeutet dies, 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. • Wenn Sie <code>Request timed out</code> empfangen, bedeutet dies, dass die IP-Adresse mit dem Axis Gerät verwendet werden kann. Prüfen Sie alle Kabel und installieren Sie das Gerät erneut.
Möglicher IP-Adressenkonflikt mit einem anderen Gerät im selben Subnetz.	Die statische IP-Adresse des Axis Geräts wird verwendet, bevor der DHCP-Server eine dynamische Adresse festlegt. Wenn daher ein anderes Gerät standardmäßig dieselbe statische IP-Adresse verwendet, treten beim Zugreifen auf das Gerät möglicherweise Probleme auf.

Vom Browser kein Zugriff auf das Gerät möglich

Anmelden nicht möglich	Stellen Sie bei aktiviertem HTTPS sicher, dass beim Anmelden das korrekte Protokoll (HTTP oder HTTPS) verwendet wird. Möglicherweise müssen Sie manuell <code>http</code> oder <code>https</code> in das Adressfeld des Browsers eingeben. Wenn das Kennwort für den Benutzer „root“ vergessen wurde, muss das Gerät auf die werksseitigen Standardeinstellungen zurückgesetzt werden. Siehe <i>Zurücksetzen auf die Werkseinstellungen</i>, on page 22.
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.

Auf das Gerät kann lokal, nicht jedoch extern zugegriffen werden

Für den externen Zugriff auf das Gerät wird empfohlen, eine der folgenden Anwendungen für Windows® zu verwenden:

- AXIS Companion: Kostenlos, ideal für kleine Systeme mit grundlegenden Überwachungsanforderungen.
- AXIS Camera Station: Kostenlose 30-Tage-Testversion, ideal für kleine bis mittelgroße Systeme.

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

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.

Technische Daten

Anzeigen und Bedienelemente an der Vorderseite

Wenn Sie das Gerät an die Stromversorgung anschließen, leuchten die Indikatoren auf der Vorderseite für einige Sekunden auf.

Indikatorsymbole

Symbol	Anzeige
	Leuchtet bei ausgehenden Anrufen blau. Blinkt blau, wenn ein Anruf gestartet wurde.
	Leuchtet bei laufendem Anruf gelb.
	Leuchtet grün, wenn die Tür geöffnet ist.

Kartenleser-Markierungsstreifen

Der Streifen gibt Leser-Feedback an.

Ruftaste

Sie können das integrierte Licht um die Anruftaste verwenden, um die Gesichter der Besucher auszuleuchten.

LED-Anzeigen

Status-LED	Anzeige
Grün	Leuchtet bei Normalbetrieb grün.

Einschub für SD-Speicherkarte

HINWEIS

- Gefahr von Schäden an der SD-Karte Benutzen Sie beim Einsetzen oder Entfernen der SD-Karte keine scharfen Werkzeuge oder Gegenstände aus Metall und wenden Sie keine übermäßige Kraft an. Setzen Sie die Karte per Hand ein. Das Gleiche gilt für das Entfernen.
- 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 22.*

Anschlüsse

HDMI-Anschluss

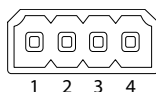
Über den microHDMI™-Anschluss werden Displays oder öffentliche Monitore angeschlossen.

Netzwerk-Anschluss

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

Audioanschluss

Vierpolige Klemmleiste für Audioeingang und -ausgang.

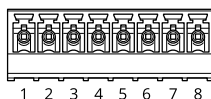


Funktion	Kontakt	Hinweise
Leitungseingang	1	Eingang (Mono)
GND	2	Audio-Masse
Line-Out	3	Line-Out
GND	4	Audio-Masse

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 350 mA ²

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.

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 Gleichstrom Maximalstrom 100 mA ³ Maximalstrom 700 mA ⁴
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: Ausgang DATA0 RS485: A+	
D1/B-	4	Wiegand: Ausgang DATA1 RS485: B-	

E/A-Anschluss

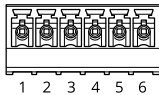
Über den E/A-Anschluss werden externe Geräte in Verbindung mit Manipulationsalarmen, Bewegungserkennung, Ereignisauslösung, Alarmbenachrichtigungen und anderen Funktionen angeschlossen. Zusätzlich zum Gleichstrombezugspunkt 0 V DC und der Stromversorgung (12-VDC-Ausgang) stellt der E/A-Anschluss folgende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

Digitaleingang – 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.

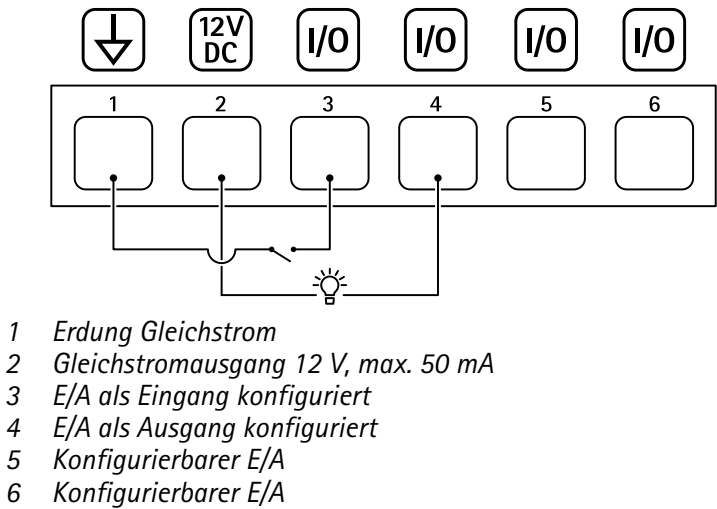
3. Bei Stromversorgung über Power over Ethernet IEEE 802.3af/802.3at Typ 1 Klasse 3.

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



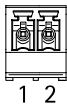
Funktion	Kon-takt	Hinweise	Technische Daten
Erdung Gleichstrom	1		0 V Gleichstrom
Gleichstrom-ausgang	2	 Kann für die Stromversorgung von Zusatzausrüstung verwendet werden. Hinweis: Dieser Kontakt kann nur als Stromausgang verwendet werden.	12 V Gleichstrom Max. Stromstärke = 50 mA
Konfigurierbar (Ein- 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:



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
Gleichstromein- gang	2	Stromversorgung der Steuerung bei Nichtverwendung von Power over Ethernet. Hinweis: Dieser Kontakt kann nur für den Stromeingang verwendet werden.	8 bis 28 V DC, max. 22 W Max. Last an Ausgängen 9 W

Sicherheitsinformationen

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.

Andere Meldeebenen

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 Dokumentationen zu unserem Ansatz im Bereich Cybersicherheit finden Sie unter axis.com/about-axis/cybersecurity. Befolgen Sie die nachstehenden Cybersicherheitsrichtlinien, um Produktsicherheitsbenachrichtigungen von Axis zu erhalten und Ihre Konfiguration für einen sicheren Lebenszyklus und eine sichere Außerbetriebnahme durchzuführen.

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

Abonnieren Sie die Sicherheits-E-Mails von Axis unter axis.com/security-notification-service. Wir senden Ihnen Informationen zu Sicherheitslücken, entsprechenden Sicherheitshinweisen und 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.

T10176599_de

2026-07 (M25.2)

© 2021 – 2026 Axis Communications AB