

AXIS A8207-VE Mk II Network Video Door Station

Benutzerhandbuch

AXIS A8207-VE Mk II Network Video Door Station

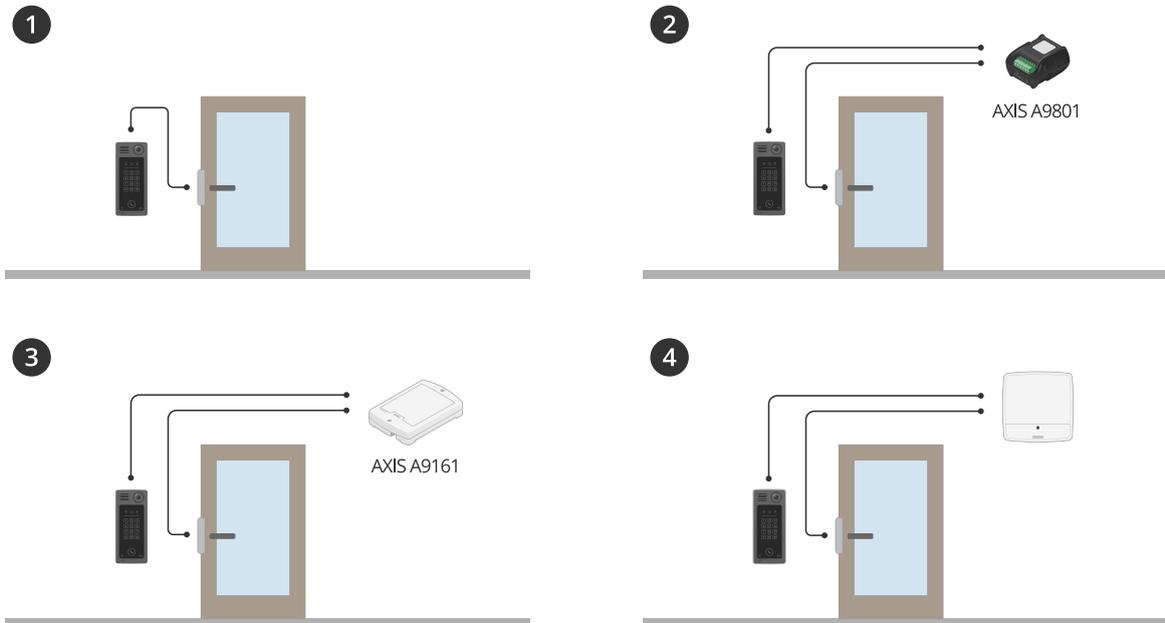
Inhalt

Lösungsübersicht	3
Produktübersicht	4
Installation	6
Erste Schritte	7
Das Gerät im Netzwerk ermitteln	7
Weboberfläche des Geräts öffnen	7
Erstellen Sie ein Administratorenkonto	7
Sichere Kennwörter	7
Stellen Sie sicher, dass keiner die Gerätesoftware manipuliert hat.	8
Übersicht über die Weboberfläche	8
Weitere Einstellungen	9
Das Root-Kennwort ändern	9
Direktes SIP (P2P) einrichten	9
SIP über einen Server (PBX) einrichten	10
Erstellen eines Kontakts	10
Konfigurieren der Anruftaste	11
Einrichten als Kartenleser – Netzwerk-Verbindung	11
Einrichten als Kartenleser – kabelgebundene Verbindung	12
Verwenden Sie geschützte Daten auf Karten, um die Sicherheit zu erhöhen .	12
Verwenden Sie DTMF, um die Tür für einen Besucher zu entriegeln.	13
Live-Videoübertragung an einen Monitor	14
Zulassen, dass der Eigentümer der Zugangsdaten die Tür öffnet	14
Die Weboberfläche	16
Status	16
Kommunikation	17
Video	22
Leser	31
Audio	33
Aufzeichnungen	34
Apps	35
System	35
Wartung	54
Mehr erfahren	56
Voice over IP (VoIP)	56
Einrichten von Regeln für Ereignisse	58
Anwendungen	58
Tägliche Nutzung	59
Verwenden des Tastenfelds	59
Fehlerbehebung	60
Zurücksetzen auf die Werkseinstellungen	60
Aktuelle AXIS OS-Version überprüfen	60
AXIS OS aktualisieren	60
Technische Probleme, Hinweise und Lösungen	61
Leistungsaspekte	62
Technische Daten	63
Anzeigen und Bedienelemente an der Vorderseite	63
LED-Anzeigen	63
Einschub für SD-Speicherkarte	63
Tasten	63
Anschlüsse	64
Sicherheitsinformationen	67
Gefährdungsstufen	67
Andere Meldeebenen	67

AXIS A8207-VE Mk II Network Video Door Station

Lösungsübersicht

Lösungsübersicht

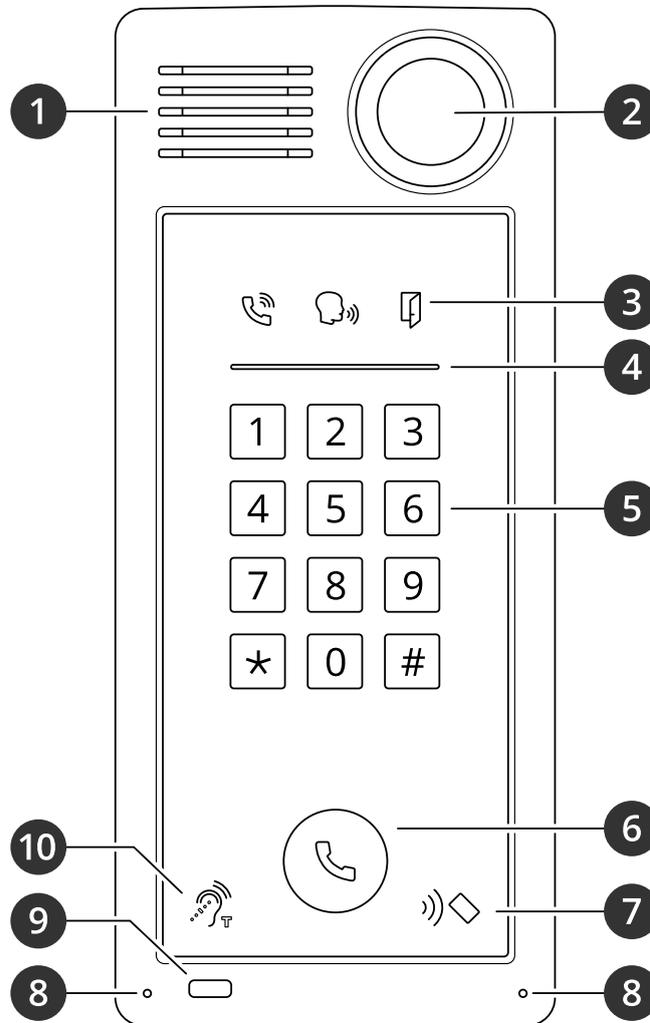


- 1 Türanlage
- 2 Türstation kombiniert mit AXIS A9801
- 3 Türstation kombiniert mit AXIS A9161
- 4 Türstation kombiniert mit einem Zutrittskontrollsystem, wie z. B. AXIS A1001 oder AXIS A1601

AXIS A8207-VE Mk II Network Video Door Station

Produktübersicht

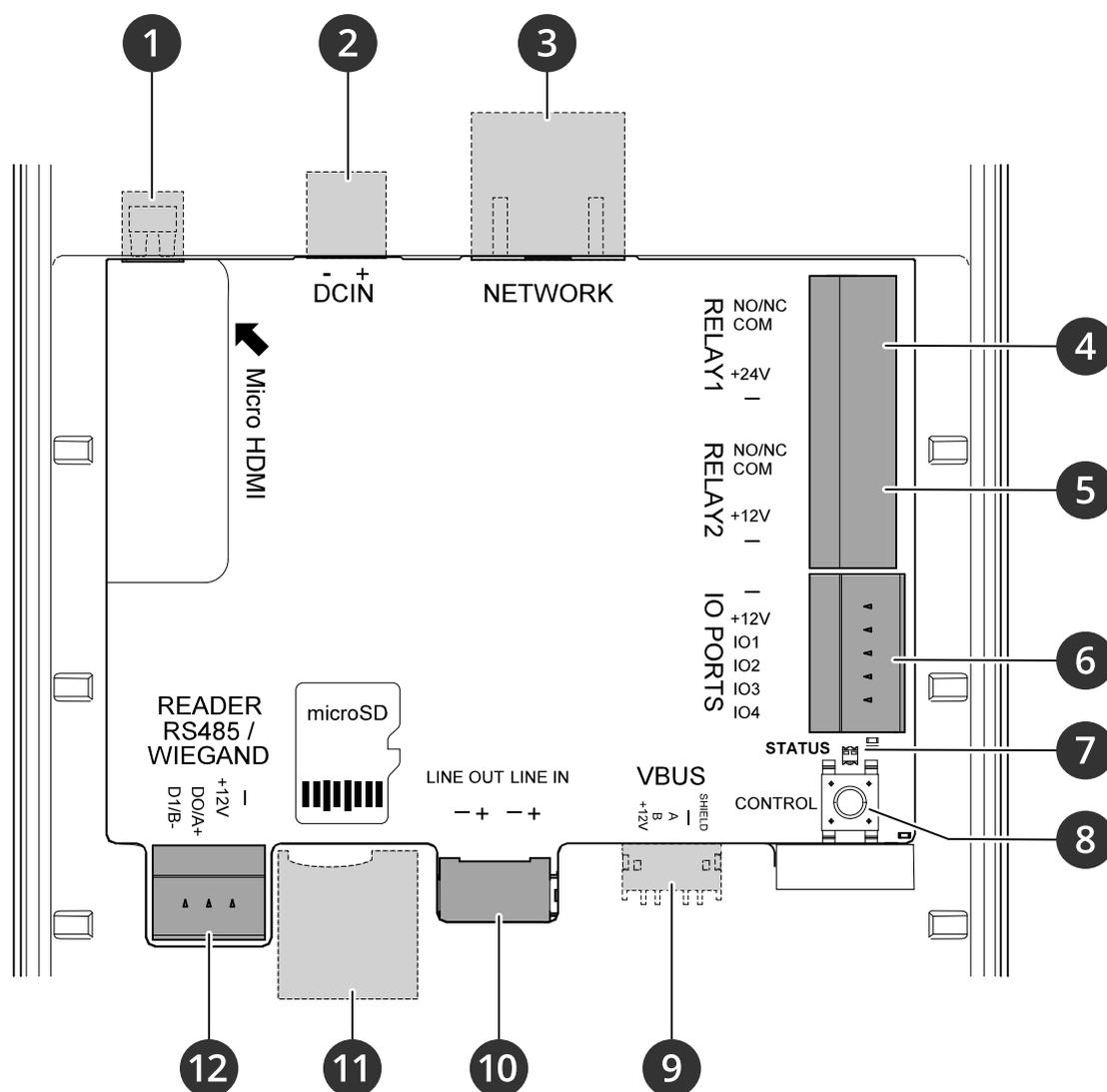
Produktübersicht



- 1 Lautsprecher
- 2 Kamera
- 3
- 4
- 5 Tastenfeld
- 6
- 7 Kartenleser-Symbol
- 8 Mikrofon
- 9 PIR-Sensor
- 10 T-Spule-Symbol

AXIS A8207-VE Mk II Network Video Door Station

Produktübersicht



- 1 (microHDMI)
- 2
- 3 (PoE+)
- 4
- 5
- 6
- 7 Status-LED
- 8
- 9 2N-VBUS (nicht belegt)
- 10
- 11 (microSD/microSDHC/microSDXC)
- 12

AXIS A8207-VE Mk II Network Video Door Station

Installation

Installation



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

help.axis.com/?Etpiald=62351&tsection=solution-overview

Installationsvideo für den Leser A8207-VE.



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

help.axis.com/?Etpiald=62351&tsection=solution-overview

Installationsvideo für das Relais A8207-VE.

AXIS A8207-VE Mk II Network Video Door Station

Erste Schritte

Erste Schritte

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

Um die Weboberfläche von AXIS OS mit iOS 15 oder iPadOS 15 zu verwenden, deaktivieren Sie unter **Settings (Einstellungen) > Safari > Advanced (Erweitert) > Experimental Features (Experimentelle Funktionen) die Option **NSURLSession Websocket**.*

Weitere Informationen zu empfohlenen Browsern finden Sie im *AXIS OS Portal*.

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 .

Eine Beschreibung aller Steuerelemente und Optionen auf der Weboberfläche des Geräts finden Sie unter .

Erstellen Sie ein Administratorkonto

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

1. Einen Benutzernamen eingeben.
2. Ein Kennwort eingeben. Siehe .
3. Geben Sie das Kennwort erneut ein.
4. Stimmen Sie der Lizenzvereinbarung zu.
5. Klicken Sie auf **Add account (Konto hinzufügen)**.

Wichtig

Das Gerät verfügt über kein Standardkonto. Wenn Sie das Kennwort für Ihr Administratorkonto verloren haben, müssen Sie das Gerät zurücksetzen. Siehe .

AXIS A8207-VE Mk II Network Video Door Station

Erste Schritte

Sichere Kennwörter

Wichtig

Das voreingestellte Kennwort wird vom Axis Gerät unverschlüsselt über das Netz gesendet. Um das Gerät zu schützen, nach dem ersten Anmelden eine sichere und verschlüsselte HTTPS-Verbindung einrichten und dann das Kennwort ändern.

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.
- Das Kennwort regelmäßig und mindestens jährlich zu ändern.

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 .
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.



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

help.axis.com/?&piald=62351§ion=web-interface-overview

Weboberfläche des Axis Geräts

AXIS A8207-VE Mk II Network Video Door Station

Weitere Einstellungen

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  **> Benutzer aktualisieren**.
3. Geben Sie ein neues Kennwort ein und klicken Sie auf „Save“ (Speichern).

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 .

Auf diesem Gerät wird VoIP über das SIP-Protokoll aktiviert. Weitere Informationen zu SIP finden Sie unter .

SIP verfügt über zwei Einstellungstypen. Eine davon ist direkt oder Peer-to-Peer (P2P). 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 .

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 (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.

AXIS A8207-VE Mk II Network Video Door Station

Weitere Einstellungen

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. 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 .

Auf diesem Gerät wird VoIP über das SIP-Protokoll aktiviert. Weitere Informationen zu SIP finden Sie unter .

SIP verfügt über zwei Einstellungstypen. Ein PBX-Server ist einer davon. 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 .

1. Fordern Sie folgende Informationen von Ihrem PBX-Anbieter an:
 - Benutzer-ID
 - Domain
 - Kennwort
 - Authentifizierungs-ID
 - Anrufer-ID
 - Registrierungsstelle
 - 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 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.

AXIS A8207-VE Mk II Network Video Door Station

Weitere Einstellungen

4. Geben Sie die SIP-Adresse des Kontakts ein.

Hinweis

Weitere Informationen zu SIP-Adressen finden Sie unter .

5. Wählen Sie das SIP-Konto aus, von dem aus 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** die Option **None (Keiner)** aus.
8. Klicken Sie auf **Save (Speichern)**.

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 Sprechanlage 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.

Einrichten als Kartenleser – Netzwerk-Verbindung

Um die Türstation als Kartenleser zu verwenden, muss sie an eine Türsteuerung angeschlossen 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 .

Bevor Sie beginnen:

Konfigurieren Sie die Hardware der Türsteuerung mit dem Wiegand-Protokoll für den Leser. Weitere Anweisungen finden Sie im Benutzerhandbuch der Türsteuerung.

Türstation als Kartenleser einrichten

1. Wechseln Sie zu **Reader > Reader protocol (Leser > Leserprotokoll)**.
2. Wählen Sie den **Protokolltyp des VAPIX-Lesers**.
3. Wählen Sie das Protokoll für die Kommunikation mit der Türsteuerung.

AXIS A8207-VE Mk II Network Video Door Station

Weitere Einstellungen

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. Klicken Sie auf **Connect (Verbinden)**.
7. Wählen Sie den Eingangsleser für die entsprechende Tür.
8. Klicken Sie auf **Save (Speichern)**.

Einrichten als Kartenleser – kabelgebundene Verbindung

Um die Türstation als Kartenleser zu verwenden, muss sie an eine Türsteuerung angeschlossen 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.
Sehen Sie sich die Schaltpläne an, die Sie von axis.com/products/axis-a8207-ve-mk-ii/support herunterladen können.
- Konfigurieren Sie die Hardware der Türsteuerung mit dem Wiegand-Protokoll für den Leser. Weitere Anweisungen finden Sie im Benutzerhandbuch der Türsteuerung.

Türstation als Kartenleser einrichten

1. Wechseln Sie zu **Reader > Reader protocol (Leser > Leserprotokoll)**.
2. Wählen Sie **Wiegand**.
3. Aktivieren Sie den **Summer**.
4. Wählen Sie unter **Eingang für Summer** die Option I3.
5. Wählen Sie unter **Eingänge für die LED-Steuerung** die Option 1.
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)**.

AXIS A8207-VE Mk II Network Video Door Station

Weitere Einstellungen

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 **Datensätze für aktive Chiparten** die zu bearbeitenden Chipart und klicken Sie auf **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 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 Sie das DTMF-Signal in der Türstation definieren
- wie Sie die Türstation einrichten, um:
 - die Türsteuerung aufzufordern, die Tür zu entriegeln oder
 - die Tür mithilfe des internen Relais zu entriegeln.

Sie nehmen alle Einstellungen auf der Webseite der Türstation vor.

Bevor Sie beginnen

- SIP-Anrufe vom Gerät zulassen und ein SIP-Konto erstellen. Siehe und .

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)** Folgendes ein: 1.
4. Geben Sie unter **Description (Beschreibung)** Folgendes ein: **Tür entsperren**.
5. Wählen Sie unter **Accounts (Konten)** das SIP-Konto aus.
6. Klicken Sie auf **Save (Speichern)**.

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

7. Wechseln Sie zu **System > Events > Rules (System > Ereignisse > Regeln)**, und fügen Sie eine Regel hinzu.
8. Geben Sie im Feld **Name** Folgendes ein: **DTMF – Tür entriegeln**.
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)**.

AXIS A8207-VE Mk II Network Video Door Station

Weitere Einstellungen

11. Wählen Sie aus der Liste der Ports **Relay 1 (Relais 1)** aus.
12. Ändern Sie **Duration (Dauer)** in **00:00:07**, d. h. die Tür ist 7 Sekunden lang geöffnet.
13. Klicken Sie auf **Save (Speichern)**.

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

Zulassen, dass der Eigentümer der Zugangsdaten die Tür öffnet

Mit der Zugangsberechtigungsliste können Eigentümer von Zugangsdaten Aktionen wie das Öffnen einer Tür über ihre Karte oder PIN 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 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)** Folgendes ein: **10**.
10. Klicken Sie auf **Save (Speichern)**.

Eine Regel erstellen:

1. Gehen Sie zu **System > Events (System > Ereignisse)**.
2. Klicken Sie unter **Rules (Regeln)** auf **+ Add a rule (+ Regel hinzufügen)**.
3. Geben Sie unter **Name** Folgendes ein: **Tür öffnen**.
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.

AXIS A8207-VE Mk II Network Video Door Station

Weitere Einstellungen

8. Legen Sie folgende Dauer fest: 00:00:07.
9. Klicken Sie auf Save (Speichern).

AXIS A8207-VE Mk II Network Video Door Station

Die Weboberfläche

Die Weboberfläche

Um die Weboberfläche des Geräts aufzurufen, müssen Sie die IP-Adresse des Geräts in einen Webbrowser eingeben.

Hinweis

Die in diesem Abschnitt beschriebenen Funktionen und Einstellungen werden von Gerät zu Gerät unterschiedlich unterstützt.

Dieses Symbol  zeigt an, dass die Funktion oder Einstellung nur für einige Geräte verfügbar ist.

	Hauptmenü anzeigen oder ausblenden.		Zugriff auf die Versionshinweise.		Auf die Hilfe zum Produkt zugreifen.		
	Die Sprache ändern.		Helles oder dunkles Design einstellen.				Das Benutzermenü enthält:
							<ul style="list-style-type: none">• Informationen zum angemeldeten Benutzer.•  Change account (Konto wechseln): Melden Sie sich vom aktuellen Konto ab und melden Sie sich bei einem neuen Konto an.•  Log out (Abmelden): Melden Sie sich vom aktuellen Konto ab.
	Das Kontextmenü enthält:						
							<ul style="list-style-type: none">• Analytics data (Analysedaten): Stimmen Sie der Teilung nicht personenbezogener Browserdaten zu.• Feedback: Teilen Sie Feedback, um Ihr Benutzererlebnis zu verbessern.• Rechtliches: Lassen Sie sich Informationen zu Cookies und Lizenzen anzeigen.• About (Info): Lassen Sie sich Geräteinformationen, einschließlich AXIS OS-Version und Seriennummer anzeigen.• Legacy device interface (Frühere Benutzeroberfläche): Wechseln Sie zur früheren Weboberfläche des Geräts.

Status

Geräteinformationen

Zeigt die Geräteinformationen an, einschließlich AXIS OS-Version und Seriennummer.

Upgrade AXIS OS (AXIS OS aktualisieren): Aktualisieren Sie die Software auf Ihrem Gerät. Klicken Sie darauf, um zur Wartungsseite zu gehen, auf der Sie die Aktualisierung durchführen können.

Zeitsynchronisierungsstatus

Zeigt Informationen zur NTP-Synchronisierung an, z. B. ob das Gerät mit einem NTP-Server synchronisiert ist und wie lange es noch bis zur nächsten Synchronisierung dauert.

NTP settings (NTP-Einstellungen): Anzeigen und Aktualisieren der NTP-Einstellungen. Klicken Sie darauf, um zur Seite **Date and time (Datum und Uhrzeit)** zu wechseln, auf der Sie die NTP-Einstellungen ändern können.

Sicherheit

Zeigt an, welche Art von Zugriff auf das Gerät aktiv ist, welche Verschlüsselungsprotokolle verwendet werden und unsignierte Apps zulässig sind. Empfehlungen zu den Einstellungen finden Sie im **AXIS OS Härtingsleitfaden**.

Hardening guide (Härtingsleitfaden): Hier gelangen Sie zum **AXIS OS Härtingsleitfaden**, in dem Sie mehr über Best Practices für die Cybersicherheit auf Axis Geräten erfahren.

Connected clients (Verbundene Clients)

Zeigt die Anzahl der Verbindungen und der verbundenen Clients an.

AXIS A8207-VE Mk II Network Video Door Station

Die Weboberfläche

View details (Details anzeigen): Anzeigen und Aktualisieren der Liste der verbundenen Clients. Die Liste zeigt IP-Adresse, Protokoll, Port, Zustand und PID/Process für jede Verbindung an.

Ongoing recordings (Laufende Aufzeichnungen)

Zeigt laufende Aufzeichnungen und den dafür vorgesehenen Speicherplatz an.

Aufzeichnungen: Aktuelle und gefilterte Aufzeichnungen und deren Quelle anzeigen. Weitere Informationen finden Sie unter



Anzeige des Speicherorts der Aufzeichnung.

Kommunikation

Kontaktliste

Kontakte



Klicken Sie hier, um die Kontaktliste als JSON-Datei herunterzuladen.



Klicken Sie hier, um eine Kontaktliste (json) zu

importieren.



Add contact (Kontakt hinzufügen): Klicken Sie, um der Kontaktliste einen neuen Kontakt hinzuzufügen.**First name (Vorname):** Geben Sie den Vornamen des Kontakts ein.**Last name (Nachname):** Geben Sie den Nachnamen des Kontakts

ein.**Speed dial (Schnellwahl)**  : Geben Sie eine verfügbare Schnellwahlnummer für den Kontakt ein. Diese Nummer wird verwendet, um den Kontakt vom Gerät aus anrufen.**SIP address (SIP-Adresse):** Geben Sie die IP-Adresse oder Durchwahl des

Kontakts ein, falls Sie SIP verwenden.  : Klicken Sie hier, um einen Testanruf zu tätigen. Der Anruf wird nach der Annahme automatisch beendet.**SIP account (SIP-Konto):** Wählen Sie das SIP-Konto für den Anruf vom Gerät zum Kontakt aus, falls Sie SIP verwenden.**Availability (Verfügbarkeit):** Wählen Sie den Verfügbarkeitszeitplan des Kontakts aus. Wenn ein Anruf versucht wird, obwohl der Kontakt nicht verfügbar ist, wird der Anruf abgebrochen, es sei denn, es gibt einen Ersatzkontakt.**Fallback**

(Ausweichoption): Wählen Sie bei Bedarf einen Ersatzkontakt aus der Liste aus.  Das Kontextmenü enthält:**Edit contact (Kontakt bearbeiten):** Eigenschaften des Kontakts bearbeiten.**Delete contact (Kontakt löschen):** Den Kontakt löschen.

Gruppen



Klicken Sie hier, um die Kontaktliste als JSON-Datei herunterzuladen.



Klicken Sie hier, um eine Kontaktliste (json)

zu importieren.



Add group (Gruppe hinzufügen): Klicken Sie hier, um eine neue Gruppe aus bestehenden Kontakten zu erstellen.**Name:** Geben Sie einen Namen für die Gruppe ein.**Use for group calls only (Nur für Gruppenanrufe verwenden):**

Einschalten, um die Gruppe nur für Gruppenanrufe zu verwenden. Ausschalten, wenn Sie einzelne Kontakte zu einer Gruppe hinzufügen möchten, diese jedoch nicht für Gruppenanrufe verwenden möchten.**Speed dial (Schnellwahl):** Geben Sie eine verfügbare Schnellwahlnummer für die Gruppe ein. Diese Nummer wird verwendet, um die Gruppe vom Gerät aus anrufen. Nur für Gruppenanrufgruppen.**Recipients (Empfänger):** Wählen Sie die Kontakte aus, die in die Gruppe aufgenommen werden sollen. Anrufe gehen gleichzeitig an alle Empfänger. Die maximale Anzahl der Empfänger ist sechs.**Fallback (Ausweichoption):** Wählen

Sie bei Bedarf einen Ersatzkontakt aus der Liste aus. Nur für Gruppenanrufgruppen.  Das Kontextmenü enthält:**Edit group (Gruppe bearbeiten):** Bearbeiten der Gruppeneigenschaften.**Delete group (Gruppe löschen):** Löscht die Gruppe.

SIP

Settings (Einstellungen)

Das Session Initiation Protocol (SIP) wird für die Kommunikation zwischen Benutzern verwendet. Die Sitzungen können Audio- und Videoelemente enthalten.

AXIS A8207-VE Mk II Network Video Door Station

Die Weboberfläche

SIP-Einrichtungsassistent: Klicken Sie hier, um SIP schrittweise einzurichten und zu konfigurieren.**SIP aktivieren:** Markieren Sie diese Option, um SIP-Anrufe zu starten und zu empfangen.**Eingehende Anrufe zulassen:** Wählen Sie diese Option, um eingehende Anrufe von anderen SIP-Geräten zuzulassen.

Call handling (Anrufbearbeitung)

- **Calling timeout (Zeitüberschreitung bei Anruf):** Legen Sie die maximale Dauer eines Anrufversuchs fest, wenn niemand antwortet.
- **Incoming call duration (Dauer des eingehenden Anrufs):** Legen Sie die maximale Dauer für einen eingehenden Anruf (maximal 10 Minuten) fest.
- **End calls after (Anrufe beenden nach):** Legen Sie die maximale Anrufdauer (maximal 60 Minuten) fest. Wählen Sie **Infinite call duration (Unendliche Anrufdauer)**, wenn Sie die Dauer eines Anrufs nicht begrenzen möchten.

Ports

Eine Portnummer muss zwischen 1024 und 65535 liegen.

- **SIP-Port:** Der für die SIP-Kommunikation genutzte Netzwerkport. Der Datenverkehr über diesen Port ist nicht verschlüsselt. Die Standardportnummer ist 5060. Bei Bedarf eine andere Portnummer eingeben.
- **TLS_Port:** Der für verschlüsselte SIP-Kommunikation genutzte Netzwerkport. Der Datenverkehr über diesen Port wird mittels Transport Layer Security (TLS) verschlüsselt. Die Standardportnummer ist 5061. Bei Bedarf eine andere Portnummer eingeben.
- **RTP-Startport:** Der Netzwerkport, der für den ersten RTP-Medienstream in einem SIP-Anruf verwendet wird. Der Standardstartport ist 4000. Möglicherweise blockieren einige Firewalls RTP-Datenverkehr an bestimmten Portnummern.

NAT-Traversal

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

Hinweis

NAT-Traversal muss vom Router unterstützt werden. Der Router muss außerdem UPnP® unterstützen.

Die Protokolle von NAT Traversal können einzeln oder in verschiedenen Kombinationen verwendet werden, die sich nach der Netzwerkkumgebung 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 das Gerät erkennt, ob sie sich hinter einer NAT oder Firewall befinden. Zudem werden mit diesem Protokoll öffentlich verortete IP-Adressen (NAT-Adressen) und Portnummern abgerufen, die von NAT für Verbindungen mit Remote-Hosts zugewiesen wurden. Die STUN-Server-Adresse eingeben, zum Beispiel 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. Geben Sie die TURN-Server-Adresse und die Anmeldedaten ein.

Audio und Video

- **Audio-Codec-Priorität:** Wählen Sie mindestens einen Audiocodec, um SIP-Anrufe in der gewünschten Audioqualität zu ermöglichen. Ändern Sie die Prioritätsreihenfolge per Drag & Drop.

Hinweis

Die gewählten Codecs müssen mit dem Codec des Anrufempfängers übereinstimmen, da dieser für den Anruf entscheidend ist.

- **Audioausrichtung:** Wählen Sie zulässige Audiorichtungen.
- **H.264-Paketierungsmodus:** Wählen Sie den zu verwendenden Paketierungsmodus aus.
 - **Auto:** (Empfohlen) Das Gerät entscheidet, welcher Paketierungsmodus verwendet wird.
 - **Keinen:** Es wird kein Paketierungsmodus festgelegt. Dieser Modus wird häufig als Modus 0 bezeichnet.
 - **0:** Nicht-verschachtelter Modus.
 - **1:** Modus für eine einzelne NAL-Einheit.
- **Videoausrichtung:** Wählen Sie zulässige Videorichtungen.

Zusätzliches

AXIS A8207-VE Mk II Network Video Door Station

Die Weboberfläche

- **Wechsel von UDP zu TCP:** Wählen Sie diese Option, um vorübergehend vom Übertragungsprotokoll (User Datagram Protocol) auf das Protokoll TCP (Transmission Control Protocol) zu wechseln. Mit einem Wechsel wird Fragmentierung vermieden und der Wechsel kann stattfinden sofern eine Anfrage innerhalb von 200 Bytes der maximalen Übertragungseinheit (MTU) liegt oder größer als 1300 Byte ist.
- **Über Umschreiben zulassen:** Wählen Sie diese Option, um die lokale IP-Adresse anstelle der öffentlichen IP-Adresse des Routers zu senden.
- **Kontakt umschreiben zulassen:** Wählen Sie diese Option, um die lokale IP-Adresse anstelle der öffentlichen IP-Adresse des Routers zu senden.
- **Alle ... am Server registrieren:** Legen Sie fest, wie oft sich das Gerät am SIP-Server für SIP-Konten registrieren soll.
- **DTMF-Nutzlasttyp:** Ändert den Standard-Nutzlasttyp für DTMF.
- **Max retransmissions (Max. erneute Übertragungen):** Legen Sie fest, wie oft das Gerät maximal versuchen soll, eine Verbindung zum SIP-Server herzustellen.
- **Seconds until failback (Sekunden bis zum Ausfall):** Legen Sie die Anzahl der Sekunden fest, die das Gerät nach einem Failover auf einen sekundären SIP-Server warten soll, bis es erneut versucht, eine Verbindung zum primären SIP-Server herzustellen.

Accounts (Konten)

Alle aktuellen SIP-Konten sind unter **SIP accounts (SIP-Konten)** aufgeführt. Der farbige Kreis zeigt den Status von registrierten Konten an.



Das Konto wurde erfolgreich beim SIP-Server registriert.



Es liegt bei diesem Konto ein Problem vor. Mögliche Gründe: Autorisierungsfehler, falsche Kontendaten oder der SIP-Server kann das Konto nicht ermitteln.

Ein **Peer-to-peer (Standard)** Konto ist ein automatisch erstelltes Konto. Sobald mindestens ein weiteres Konto erstellt ist, kann das automatisch erstellte Konto gelöscht werden und das neu eingerichtete Konto als Standardkonto gewählt werden. Das Standardkonto wird immer für Anrufe über die programmierbare Schnittstelle VAPIX® Application Programming Interface (API) verwendet, wenn kein SIP-Senderkonto angegeben ist.



Add account (Konto hinzufügen): Klicken Sie darauf, um ein neues SIP-Konto zu erstellen.

- **Active (Aktiv):** Wählen Sie diese Option, um das Konto nutzen zu können.
- **Als Standard setzen:** Mit dieser Option dieses Konto als Standardkonto verwenden. Es muss ein und nur ein Standardkonto vorhanden sein.
- **Answer automatically (Automatisch annehmen):** Einen eingehenden Anruf automatisch annehmen.
- **Prioritize IPv6 over IPv4 (IPv6 über IPv4 bevorzugen)**  : Wählen Sie diese Option aus, um IPv6-Adressen gegenüber IPv4-Adressen zu bevorzugen. Dies ist nützlich, wenn Verbindungen zu Peer-to-Peer-Konten oder Domännennamen hergestellt werden, die sowohl in IPv4- als auch in IPv6-Adressen auflösen. IPv6 kann nur für Domännennamen priorisiert werden, die IPv6-Adressen zugeordnet sind.
- **Name:** Geben Sie einen beschreibenden Namen ein. Das kann zum Beispiel ein Vor- und Nachname, eine Funktion oder ein Standort sein. Der Name muss nicht eindeutig sein.
- **Benutzer-ID:** Geben Sie die dem Axis Gerät zugeordnete eindeutige Telefonnummer oder Durchwahl an.
- **Peer-to-Peer:** Für Direktanrufe an ein anderes SIP-Gerät im lokalen Netzwerk.
- **Registriert:** Für Anrufe an SIP-Geräte außerhalb des lokalen Netzwerks über einen SIP-Server.
- **Domain:** Sofern verfügbar, geben Sie den Domainnamen ein. Dieser wird bei Anrufen bei anderen Konten als Teil der SIP-Adresse angezeigt.
- **Kennwort:** Geben Sie zum Authentifizieren am SIP-Server das dem SIP-Konto zugeordnete Kennwort ein.
- **Authentifizierungs-ID:** Geben Sie die Authentifizierungs-ID für den SIP-Server ein. Wenn diese mit der Benutzer-ID identisch ist, muss sie nicht gesondert eingegeben werden.
- **Anrufer-ID:** Der dem Empfänger der von diesem Gerät aus getätigten Anrufe angezeigte Name.
- **Registrierungsstelle:** Geben Sie die IP-Adresse der Registrierungsstelle ein.
- **Übertragungsmodus:** Den SIP-Übertragungsmodus für das Konto wählen: UPD, TCP oder TLS.
- **TLS version (nur mit Übertragungsmodus TLS):** Wählen Sie die zu verwendende TLS-Version. Die Versionen v1.2 und v1.3 sind die sichersten. **Automatic (Automatisch)** wählt die sicherste Version aus, die das System verarbeiten kann.
- **Media encryption (Medienverschlüsselung)** (nur mit Übertragungsmodus TLS): Die Art der Verschlüsselung für Medien (Audio und Video) für SIP-Anrufe wählen.

AXIS A8207-VE Mk II Network Video Door Station

Die Weboberfläche

- **Zertifikat** (nur mit Übertragungsmodus TLS): Ein Zertifikat wählen.
- **Server-Zertifikat überprüfen** (nur mit Übertragungsmodus TLS): Markieren Sie diese Option, um das Server-Zertifikat zu überprüfen.
- **Sekundärer SIP-Server**: Aktivieren Sie diese Option, damit bei fehlgeschlagener Registrierung am primären SIP-Server das Gerät versucht, sich am sekundären SIP-Server zu registrieren.
- **SIP secure (SIP-Secure)**: Diese Option zum Verwenden von Secure Session Initiation Protocol (SIPS) wählen. SIPS verwendet zum Verschlüsseln den Übertragungsmodus TLS.
- **Proxys**
 - **+** **Proxy**: Klicken Sie darauf, um einen Proxy hinzuzufügen.
 - **Priorisieren**: Klicken Sie darauf, um Proxys zu priorisieren, wenn Sie zwei oder mehrere davon haben.
 - **Server-Adresse**: Geben Sie die IP-Adresse des primären SIP-Servers ein.
 - **Username (Benutzername)**: Falls verlangt, einen Benutzernamen für den SIP-Proxyserver eingeben.
 - **Kennwort**: Geben Sie das Kennwort für den SIP-Proxyserver ein, falls erforderlich.
- **Video** ⓘ
 - **Sichtbereich**: Wählen Sie den für Videoanrufe zu verwendenden Sichtbereich. Ohne Auswahl wird die Standardansicht verwendet.
 - **Auflösung**: Wählen Sie die für Videoanrufe zu verwendende Auflösung. Die Auflösung wirkt sich auf die erforderliche Bandbreite aus.
 - **Bildrate**: Wählen Sie die Bildrate für Videoanrufe auf. Die Bildrate wirkt sich auf die erforderliche Bandbreite aus.
 - **H.264 profile (Profil H.264)**: Wählen Sie das Profil aus, das für Videoanrufe verwendet werden soll.

DTMF

- **+** **Add sequence (Sequenz hinzufügen)**: Klicken Sie hier, um eine neue DTMF-Sequenz (Dual-Tone Multifrequency) zu erstellen. Um eine Regel zu erstellen, die mit dem Ton aktiviert wird, wechseln Sie zu **Events > Rules (Ereignisse > Regeln)**. **Sequence (Sequenz)**: Geben Sie zum Aktivieren der Regel zu verwendenden Zeichen ein. Zulässige Zeichen: 0-9, A-D, #, und *. **Description (Beschreibung)**: Geben Sie eine Beschreibung der durch die Sequenz auszulösenden Aktion ein. **Accounts (Konten)**: Wählen Sie die Konten aus, die die DTMF-Sequenz verwenden sollen. Wenn Sie sich für **peer-to-peer (Peer-to-Peer)** entscheiden, teilen alle Peer-to-Peer-Konten dieselbe DTMF-Sequenz.

Protocols (Protokolle): Wählen Sie die Protokolle für die einzelnen Konten aus. Alle Peer-to-Peer-Konten teilen die gleichen Protokolleinstellungen. **Use RTP (RFC2833) (RTP (RFC2833) verwenden)**: Wählen Sie diese Option, um die Mehrfrequenzwahl, weitere Tonsignale und Telefonie-Ereignisse in RTP-Paketen zuzulassen. **Use SIP INFO (RFC2976) (SIP INFO (RFC2976) verwenden)**: Diese Option verwenden, um die Methode INFO in das SIP-Protokoll aufzunehmen. Mit der Methode INFO werden optionale, in der Regel auf die Sitzung bezogene, Anwendungsschichten aufgenommen.

Test call (Testanruf)

SIP account (SIP-Konto): Wählen Sie das Konto, von dem aus der Testanruf durchgeführt werden soll. **SIP-Adresse**: Geben Sie eine SIP-Adresse ein und klicken Sie auf , um einen Testanruf zu tätigen und sicherzustellen, dass das Konto funktioniert.

Access list (Zugangsliste)

Use access list (Zugangsliste verwenden): Aktivieren Sie dies, um die Zahl der Anrufer auf das Gerät begrenzen. **Policy (Richtlinie)**:

- **Allow (Zulassen)**: Wählen Sie diese Option aus, um eingehende Anrufe nur von den Quellen in der Zugangsliste zu erlauben.
- **Block (Blockieren)**: Wählen Sie diese Option aus, um eingehende Anrufe von den Quellen in der Zugangsliste zu blockieren.

- **+** **Add source (Quelle hinzufügen)**: Klicken Sie hier, um einen neuen Eintrag in der Zugangsliste zu erstellen. **SIP source (SIP-Quelle)**: Geben Sie die Anrufer-ID oder die SIP-Server-Adresse der Quelle ein.

Multicast controller (Multicast-Controller)

AXIS A8207-VE Mk II Network Video Door Station

Die Weboberfläche

User multicast controller (Benutzer Multicast-Controller): Aktivieren Sie den Multicast-Controller. Audio codec (Audio-Codec):

Wählen Sie einen Audio-Codec aus.



Source (Quelle): Neue Quelle für Multicast-Controller hinzufügen.

- Label (Bezeichnung): Geben Sie den Namen einer Bezeichnung ein, die noch nicht von einer Quelle verwendet wird.
- Source (Quelle): Geben Sie eine Quelle ein.
- Port: Geben Sie einen Port ein.
- Priority (Priorität): Wählen Sie eine Priorität aus.
- Profile (Profil): Ein Profil auswählen.
- SRTP key (SRTP-Schlüssel): Geben Sie einen SRTP-Schlüssel ein.



Das Kontextmenü enthält: Edit (Bearbeiten): Quelle für den Multicast-Controller bearbeiten. Delete (Löschen): Löschen Sie die Quelle des Multicast-Controllers.

Anrufe

Ruftaste

Enable call button (Ruftaste aktivieren): Aktivieren Sie diese Option, um die Ruftaste zu verwenden. Standby light (Standby-Licht): Wählen Sie eine Option für die integrierte Anruftasten-Beleuchtung aus.

- Auto  : Das Gerät schaltet die integrierte Leuchte auf Grundlage des Umgebungslichts ein und aus.
- On (Ein): Die integrierte Leuchte wird immer eingeschaltet, wenn sich das Gerät im Stand-by-Modus befindet.
- Off (Aus): Die integrierte Leuchte wird immer ausgeschaltet, wenn sich das Gerät im Stand-by-Modus befindet.

Recipients (Empfänger): Wählen oder erstellen Sie einen oder mehrere Anrufkontakte, wenn die Anruftaste gedrückt wird. Wenn Sie mehr als einen Empfänger hinzufügen, werden alle Empfänger gleichzeitig angerufen. Die maximale Anzahl der SIP-Anrufempfänger beträgt sechs, die Anzahl der möglichen VMS-Anrufempfänger ist dagegen unbegrenzt. Fallback (Ausweichoption): Fügen Sie einen Ersatzkontakt aus der Liste hinzu, falls keiner der Empfänger antwortet.

Allgemein

Audio

Hinweis

- Der ausgewählte Audioclip wird nur bei einem Anruf abgespielt.
- Bei Änderung des Audioclips oder der Lautstärke während eines laufenden Anrufs wird die Änderung erst beim nächsten Anruf wirksam.

Ringtone (Klingelton): Wählen Sie den Audioclip aus, der bei einem eingehenden Anruf auf dem Gerät abgespielt werden soll. Stellen Sie die Lautstärke mithilfe des Schiebereglers ein. Ringback tone (Freizeichen): Wählen Sie den Audioclip aus, der bei einem ausgehenden Anruf auf dem Gerät abgespielt werden soll. Stellen Sie die Lautstärke mithilfe des Schiebereglers ein.

VMS-Anrufe

VMS-Anrufe

Allow calls in the video management software (VMS) (Anrufe im Video Management System (VMS) zulassen): Wählen Sie diese Option, um Anrufe vom Gerät an das VMS zuzulassen. VMS-Anrufe sind auch bei deaktivierter SIP-Funktion möglich. Zeitüberschreitung bei Anruf: Legen Sie die maximale Dauer eines Anrufversuchs fest, wenn niemand antwortet.

AXIS A8207-VE Mk II Network Video Door Station

Die Weboberfläche

Video

 Klicken Sie darauf, um den Live-Videostream wiederzugeben.  Klicken Sie darauf, um den Live-Videostream einzufrieren.  Klicken Sie darauf, um vom Live-Videostream eine Momentaufnahme anzufertigen. Die Datei wird im Ordner Downloads des Rechners gespeichert. Die Bilddatei trägt den Namen [snapshot_JJJJ_MM_TT_HH_MM_SS.jpg]. Die tatsächliche Größe des Schnappschusses hängt von der Komprimierung ab, die von der Engine des jeweiligen Browsers angewendet wird, auf dem der Schnappschuss empfangen wird. Daher kann die Größe des Schnappschusses von der eigentlichen Komprimierungseinstellung abweichen, die im Axis Gerät konfiguriert ist.   Klicken Sie darauf, um sich die E/A-Ausgangspoints anzeigen zu lassen. Verwenden Sie den Schalter, um den Schaltkreis eines Ports zu öffnen oder zu schließen, z. B. um Zusatzausrüstung zu testen.   Klicken Sie darauf, um die IR-Beleuchtung manuell ein- oder auszuschalten.   Klicken Sie darauf, um das sichtbare Weißlicht manuell ein- oder auszuschalten.  Klicken Sie darauf, um auf die Steuerelemente auf dem Bildschirm zuzugreifen:

- **Voreingestellte Steuerelemente:** Aktivieren Sie diese Option, um die auf dem Bildschirm verfügbaren Steuerelemente zu verwenden.
- **Benutzerdefinierte Steuerelemente:** Klicken Sie auf  **Benutzerdefinierte Steuerelemente** hinzufügen, um dem Bildschirm Steuerelemente hinzuzufügen.

  Startet die Waschanlage. Zu Beginn der Abfolge wird die Kamera in die Waschposition gefahren. Nach Abschluss der Abfolge wird die Kamera in ihre vorherige Position zurückgefahren. Dieses Symbol wird nur angezeigt, wenn die Waschanlage angeschlossen und konfiguriert ist.   Startet den Wischer.   Klicken Sie und wählen Sie eine vordefinierte Position aus, um zu dieser vordefinierten Position in der Live-Ansicht zu wechseln. Oder klicken Sie auf **Setup**, um zur Seite mit der vordefinierten Position zu wechseln.    Fügt einen Fokusabrufbereich hinzu oder entfernt diesen. Bei Hinzufügen eines Fokusabrufbereichs speichert die Kamera die Fokuseinstellungen des spezifischen Schwenk-/Neigungsbereichs. Wenn die Kamera sich in der Live-Ansicht in einen als Fokusabrufbereich definierten Bereich begibt, dann ruft die Kamera die gespeicherten Fokusdaten ab. Es muss lediglich die Hälfte des Bereichs abgedeckt werden, um die Fokusdaten abzurufen.   Klicken Sie, um eine Guard-Tour auszuwählen, und klicken Sie dann auf **Start**, um die Guard-Tour wiederzugeben. Oder klicken Sie auf **Setup**, um zur Seite mit der Guard-Tour Position zu wechseln.   Klicken Sie darauf, um für einen ausgewählten Zeitraum die Heizung manuell einzuschalten.  Klicken Sie darauf, um die ständige Aufzeichnung eines Live-Videostreams zu starten. Klicken Sie erneut, um die Aufzeichnung anzuhalten. Wenn eine Aufzeichnung läuft, wird sie nach einem Neustart automatisch fortgesetzt.  Klicken Sie darauf, um sich den für das Gerät konfigurierten Speicher anzeigen zu lassen. Melden Sie sich als Administrator an, um den Speicher zu konfigurieren.  Klicken Sie darauf, um auf weitere Einstellungen zuzugreifen:

- **Video format (Videoformat):** Wählen Sie das Codierungsformat aus, das in der Live-Ansicht verwendet werden soll.
-  **Autoplay:** Aktivieren Sie diese Option, um einen stummgeschalteten Videostream automatisch wieder wiederzugeben, wenn Sie das Gerät in einer neuen Sitzung öffnen.
- **Client stream information (Informationen über den Client-Stream):** Aktivieren Sie diese Option, um dynamische Informationen über den vom Browser zur Anzeige der Live-Ansicht verwendeten Videostream anzuzeigen. Die Bitrate-Informationen unterscheiden sich aufgrund unterschiedlicher Informationsquellen von den in einem Text-Overlay angezeigten Informationen. Die Bitrate in den Informationen zum Clientstream ist die Bitrate der letzten Sekunde und stammt vom Codierungstreiber des Geräts. Die Bitrate im Overlay ist die durchschnittliche Bitrate der letzten 5 Sekunden und stammt vom Browser. Beide Werte decken nur den Rohvideostream ab und nicht die zusätzliche Bandbreite, die bei der Übertragung über das Netzwerk via UDP/TCP/HTTP erzeugt wird.
- **Adaptiver Videostream:** Aktivieren Sie diese Option, um die Bildauflösung zur Erhöhung der Benutzerfreundlichkeit an die tatsächliche Bildschirmauflösung des Clients anzupassen und eine mögliche Überlastung der Client-Hardware zu vermeiden. Der adaptive Videostream wird nur eingesetzt, wenn die Wiedergabe des Live-Videostreams über die

AXIS A8207-VE Mk II Network Video Door Station

Die Weboberfläche

Weboberfläche in einem Browser erfolgt. Wenn adaptiver Videostream aktiviert ist, beträgt die maximale Bildrate 30 Bilder pro Sekunde. Wenn Sie bei aktiviertem adaptivem Stream eine Momentaufnahme erstellen, wird die vom adaptiven Videostream ausgewählte Bildauflösung verwendet.

- **Nivellieraster:** Klicken Sie auf , um sich das Nivellieraster anzeigen zu lassen. Mithilfe des Rasters können Sie entscheiden, ob das Bild horizontal ausgerichtet ist. Klicken Sie auf , um es auszublenden.
- **Pixel counter (Pixelzähler):** Klicken Sie auf , um den Pixelzähler anzuzeigen. Das Feld auf den ausgewählten Bereich platzieren und die Größe durch Ziehen anpassen. Die Größe des Felds in Pixeln lässt sich auch über die Felder **Width (Breite)** und **Height (Höhe)** definieren.
- **Refresh (Aktualisieren):** Klicken Sie auf , um das Standbild der Live-Ansicht zu aktualisieren.
- **PTZ-Steuerelemente**  : Aktivieren Sie diese Ansicht, um die PTZ-Steuerelemente in der Live-Ansicht anzuzeigen.

1:1

Klicken Sie darauf, um sich die Live-Ansicht mit voller Auflösung anzeigen zu lassen. Wenn die volle Auflösung größer als die Bildschirmgröße ist, navigieren Sie unter Verwendung des kleineren Bilds im Bild.  Klicken Sie darauf, um sich den Live-Videostream im Vollbildmodus anzeigen zu lassen. Drücken Sie DIE ABBRUCHTASTE, um den Vollbildmodus zu verlassen.

Installation

Capture mode (Aufnahmemodus)  : Ein Aufnahmemodus ist eine voreinstellte Konfiguration, um festzulegen, wie die Kamera Bilder aufnehmen soll. Eine Änderung des Aufnahmemodus kann sich auf viele anderen Einstellungen, wie Sichtbereiche und Privatzonenmasken, auswirken. **Mounting position (Montageposition)**  : Die Bildausrichtung kann sich je nach Installation der Kamera ändern. **Power line frequency (Netzfrequenz):** Wählen Sie die in Ihrer Region verwendete Frequenz aus, um Bildflimmern zu minimieren. In Amerika wird in der Regel eine Frequenz von 60 Hz verwendet. Auf allen anderen Kontinenten wird in der Regel eine Frequenz von 50 Hz verwendet. Wenden Sie sich bei Fragen zur Netzfrequenz an Ihr Stromversorgungsunternehmen.

Bild

Darstellung

Szeneprofil  : Wählen Sie ein Szeneprofil für Ihr Überwachungsszenario aus. Ein Szene-Profil optimiert die Bildeinstellungen einschließlich Farbstufe, Helligkeit, Schärfe, Kontrast und lokaler Kontrast für eine bestimmte Umgebung oder zu einem bestimmten Zweck.

- **Forensisch:** Zu Überwachungszwecken geeignet.
- **Innenbereich**  : Für den Innenbereich geeignet.
- **Außenbereich**  : Für den Außenbereich geeignet.
- **Vivid (Anschaulich)**  : Zu Demonstrationszwecken nützlich.
- **Traffic overview (Verkehrsübersicht)**  : Für die Überwachung des Fahrzeugverkehrs geeignet.

Saturation (Sättigung): Stellen Sie mithilfe des Schiebereglers die Farbintensität ein. Sie können z. B. ein Bild in Graustufen erstellen.

AXIS A8207-VE Mk II Network Video Door Station

Die Weboberfläche



Contrast (Kontrast): Passen Sie mithilfe des Schiebereglers den Unterschied zwischen hell und dunkel an.



Helligkeit: Stellen Sie mithilfe des Schiebereglers die Lichtstärke ein. Dadurch lassen sich Objekte leichter erkennen. Helligkeit wird nach der Bildaufnahme angewendet und hat keine Auswirkungen auf die Bilddaten. Um mehr Details aus dunklen Bereichen zu erhalten, ist es normalerweise besser, die Verstärkung oder die Belichtungszeit zu erhöhen.



Schärfe: Stellen mithilfe des Schiebereglers den Randkontrast ein, um Objekte in einem Bild schärfer darzustellen. Wenn Sie die Schärfe erhöhen, kann dies zu einer höheren Bitrate und einem höheren Bedarf an Speicherplatz führen.



Großer Dynamikbereich

WDR ⓘ : Aktivieren Sie diese Option, um sowohl helle als auch dunkle Bereiche im Bild darzustellen. **Lokaler Kontrast** ⓘ : Stellen Sie mithilfe des Schiebereglers den Kontrast des Bildes ein. Bei einem höheren Wert wird der Kontrast zwischen dunklen und hellen Bereichen größer. **Farbtonzuordnung** ⓘ : Passen Sie mithilfe des Schiebereglers das auf das Bild angewendete Tone-Mapping an. Bei einem Korrekturwert von „0“ erfolgt lediglich eine normale Gammakorrektur, ein größerer Wert erhöht dagegen die Sichtbarkeit der dunkelsten und hellsten Bildbereiche.

Weißabgleich

Wenn die Kamera die Farbtemperatur der Lichtquelle erfasst, kann sie das Bild so anpassen, dass die Farben natürlicher dargestellt werden. Sollte dies nicht ausreichen, können Sie eine geeignete Lichtquelle aus der Liste wählen.

Die Einstellung Automatischer Weißabgleich verringert durch allmähliches Anpassen das Risiko von Farbflimmern. Wenn die Beleuchtung geändert oder die Kamera das erste Mal hochgefahren wird, kann die Anpassung an die veränderten Lichtverhältnisse bis zu 30 Sekunden dauern. Befindet sich in einer Szene mehr als eine Art von Lichtquelle, also wenn sie sich in ihrer Farbtemperatur

AXIS A8207-VE Mk II Network Video Door Station

Die Weboberfläche

unterscheiden, dann wird die stärkere Lichtquelle als Bezugswert für den Algorithmus zum Ermitteln des Weißabgleichs verwendet. Dieses Verhalten kann übersteuert werden. Dazu wird ein fester Weißabgleichswert gewählt, welcher der als Bezugswert bevorzugten Lichtquelle entspricht.

Lichtverhältnisse:

- **Automatisch:** Automatisches Identifizieren und Ausgleichen der Lichtquellenfarbe. Dies ist die empfohlene Einstellung, die für die meisten Situationen verwendet werden kann.
- **Automatisch – Außenbereiche**  : Automatisches Identifizieren und Ausgleichen der Lichtquellenfarbe. Dies ist die empfohlene Einstellung, die für die meisten Situationen im Außenbereich verwendet werden kann.
- **Benutzerdefiniert – Innenbereiche**  : Fester Farbausgleichswert für Innenräume mit Kunstlichtquelle, ausgenommen fluoreszierendes Licht, und geeignet für normale Farbtemperaturen von etwa 2800 K.
- **Benutzerdefiniert – Außenbereiche**  : Fester Farbausgleichswert für sonniges Wetter und eine Farbtemperatur von etwa 5.500 K.
- **Fest – Fluoreszierend 1:** Fester Farbausgleichswert für fluoreszierendes Licht und eine Farbtemperatur von etwa 4000 K.
- **Fest – Fluoreszierend 2:** Fester Farbausgleichswert für fluoreszierendes Licht mit einer Farbtemperatur von etwa 3.000 K.
- **Fest – Innenbereich:** Fester Farbausgleichswert für Innenräume mit Kunstlichtquelle, ausgenommen fluoreszierendes Licht, und geeignet für normale Farbtemperaturen von etwa 2800 K.
- **Fest – Außenbereich 1:** Fester Farbausgleichswert für sonniges Wetter und eine Farbtemperatur von etwa 5.500 K.
- **Fest – Außenbereich 2:** Fester Farbausgleichswert für bewölktetes Wetter und eine Farbtemperatur von etwa 6.500 K.
- **Street light – mercury (Straßenbeleuchtung – Quecksilber)**  : Fester Farbausgleichswert zur Kompensation des ultravioletten Anteil von häufig als Straßenbeleuchtung eingesetzten Quecksilberdampfleuchten.
- **Street light – sodium (Straßenbeleuchtung – Natriumdampflampen)**  : Fester Farbausgleichswert, der den Gelb-Gelbanteil von häufig als Straßenbeleuchtung eingesetzten Natriumdampfleuchten ausgleicht.
- **Aktuelle Einstellung beibehalten:** Behält die aktuelle Einstellung bei und nimmt keinen Lichtausgleich vor.
- **Manuell**  : Legen Sie den Weißabgleich mit Hilfe eines weißen Objekts fest. Ziehen Sie dazu einem Kreis zu einem Objekt, das von der Kamera als weiß interpretiert werden soll (zum Beispiel ein weißes Blatt Papier) in die Mitte des Live-Bildes. Stellen Sie mit den Schieberegler für **Rotabgleich** und **Blauabgleich** den Weißabgleich manuell ein.

Exposure (Belichtung)

Wählen Sie einen Belichtungsmodus, sich rasch verändernde unregelmäßige Bildeffekte zu verringern, zum Beispiel durch unterschiedliche Lichtquellen verursachtes Flimmern. Wir empfehlen dem automatischen Belichtungsmodus oder dieselbe Frequenz wie Ihr Stromnetz.

Exposure mode (Belichtungsmodus):

- **Automatic (Automatisch):** Die Kamera stellt Blende, Verstärkung und Verschlusszeit selbsttätig ein.
- **Automatic aperture (Automatische Blendeneinstellung)**  : Die Kamera stellt Blende und Verstärkung selbsttätig ein. Die Verschlusszeit ist vorgegeben.
- **Automatische Verschlusseinstellung**  : Die Kamera stellt die Verschlusszeit und die Verstärkung automatisch ein. Die Blende ist vorgegeben.
- **Aktuelle Einstellung beibehalten:** Behält die aktuellen Belichtungseinstellungen bei.
- **Flimmerfrei**  : Die Kamera stellt unter Verwendung folgender Verschlusszeiten Blende und Verstärkung automatisch ein: 1/50 s (50 Hz) und 1/60 s (60 Hz).
- **Flimmerfrei 50 Hz**  : Die Kamera stellt unter Verwendung einer Verschlusszeit ist mit 1/50 s der Blende und Verstärkung selbsttätig ein.

AXIS A8207-VE Mk II Network Video Door Station

Die Weboberfläche

- **Flimmerfrei 60 Hz**  : Die Kamera stellt unter Verwendung einer Verschlusszeit ist mit 1/60 s der Blende und Verstärkung selbsttätig ein.
- **Flimmerreduziert**  : Wie flimmerfrei, allerdings kann die Kamera bei stärker ausgeleuchteten Szenen beliebige Verschlusszeiten von kürzer als 1/100 Sekunden (50 Hz) und 1/120 Sekunden (60 Hz) einsetzen.
- **Flimmerreduziert 50 Hz**  : Wie flimmerfrei, allerdings kann die Kamera bei stärker ausgeleuchteten Szenen beliebige Verschlusszeiten von kürzer als 1/100 Sekunden einsetzen.
- **Flimmerreduziert 60 Hz**  : Wie flimmerfrei, allerdings kann die Kamera bei stärker ausgeleuchteten Szenen beliebige Verschlusszeiten von kürzer als 1/120 Sekunden einsetzen.
- **Manuell**  : Die Blendenöffnung, Verstärkung und Verschlusszeit sind vorgegeben.

Exposure zone (Belichtungsbereich)  : Verwenden Sie Belichtungsbereiche, um die Belichtung in einem ausgewählten Teil der Szene zu optimieren, z. B. dem Bereich vor einer Eingangstür.

Hinweis

Die Belichtungsbereiche beziehen sich auf das Originalbild (nicht gedreht); die Bereichsnamen gelten für das Originalbild. Wenn zum Beispiel der Videostream um 90° gedreht wird, dann wird der **Obere** Bereich zum **Unteren** Bereich des Streams und der **linke** Bereich zum **rechten** Bereich.

- **Automatisch**: Für die meisten Situationen geeignet.
- **Mitte**: Damit wird anhand eines einen fest definierten Bereichs in der Bildmitte die Belichtung berechnet. Dieser Bereich hat in der Live-Ansicht eine feste Größe und Position.
- **Full (Gesamt)**  : Damit wird anhand der kompletten Live-Ansicht die Belichtung berechnet.
- **Upper (Oben)**  : Damit wird anhand eines festgelegten Bereichs im oberen Teil des Bildes die Belichtung berechnet.
- **Lower (Unten)**  : Damit wird anhand eines festgelegten Bereichs im unteren Teil des Bildes die Belichtung berechnet.
- **Left (Links)**  : Damit wird anhand eines festgelegten Bereichs im linken Teil des Bildes die Belichtung berechnet.
- **Right (Rechts)**  : Damit wird anhand eines festgelegten Bereichs im rechten Teil des Bildes die Belichtung berechnet.
- **Genau**: Damit wird anhand eines Bereichs mit festgelegter Größe und Position die Belichtung berechnet.
- **Benutzerdefiniert**: Damit wird anhand eines Ausschnitts der Live-Ansicht die Belichtung berechnet. Sie können Größe und Position des Bereichs anpassen.

Maximale Verschlusszeit: Wählen Sie die Verschlusszeit für beste Bildqualität. Zu lange Verschlusszeiten (längere Belichtung) können Bewegungsunschärfe erzeugen, wobei zu kurze Verschlusszeiten die Bildqualität beeinträchtigen können. Die maximale Verschlusszeit verbessert das Bild mittels maximaler Verstärkung. **Maximale Verstärkung**: Wählen Sie die passende maximale Verstärkung aus. Wenn Sie die maximale Verstärkung erhöhen, wird die Detailschärfe dunkler Bilder verbessert, jedoch auch den Rauschpegel erhöht. Mehr Rauschen kann einem erhöhten Bedarf an Bandbreite und Speicherplatz zur Folge haben. Bei Einstellung einer hohen maximalen Verstärkung kann die Bildqualität bei extrem unterschiedlichen Lichtverhältnissen (Tag/und Nacht) sehr unterschiedlich ausfallen. Die maximierte Verstärkung verbessert das Bild mittels maximierter Verschlusszeit. **Motion-adaptive**

exposure (Bewegungsadaptive Belichtung)  : Wählen Sie diese Option, um die Bewegungsunschärfe bei schlechten Lichtverhältnissen zu verringern. **Balance zwischen Bewegungsunschärfe und Rauschen**: Passen Sie mithilfe des Schiebereglers an, ob Bewegungsschärfe oder geringes Rauschen Vorrang hat. Um geringere Bandbreite und geringes Rauschen auf Kosten den Bewegungsschärfe zu bevorzugen, schieben Sie den Schieberegler in Richtung **Geringes Rauschen**. Um Bewegungsschärfe auf Kosten geringer Bandbreite und geringen Rauschens zu bevorzugen, schieben den Schieberegler in Richtung **Geringe Bewegungsunschärfe**.

AXIS A8207-VE Mk II Network Video Door Station

Die Weboberfläche

Hinweis

Sie können die Belichtung entweder durch Einstellen der Belichtungszeit oder der Verstärkung verändern. Die Erhöhung der Belichtungszeit führt dies zu mehr Bewegungsunschärfe und die Erhöhung der Verstärkung zu mehr Rauschen. Wenn Sie **Blur-noise trade-off (Kompromiss zwischen Unschärfe und Rauschen)** in Richtung **Low noise (Geringes Rauschen)** einstellen, wird die automatische Belichtung bei erhöhter Belichtung eher längeren Belichtungszeiten Vorrang geben und umgekehrt, wenn Sie den Kompromiss in Richtung **Low motion blur (Geringe Bewegungsunschärfe)** anpassen. Bei schwachem Licht erreichen sowohl die Verstärkung und die Belichtungszeit letztendlich ihren jeweiligen Maximalwert und es wird keiner der beiden mehr bevorzugt.

Blendenöffnung arretieren  : Aktivieren Sie diese Option, um die mithilfe des Schiebereglers der **Blendenöffnung** eingestellte Blendenöffnung zu halten. Aktivieren Sie diese Option, um der Kamera zu erlauben, den Bildfokus automatisch an die Blendenöffnung anzupassen. Sie können z. B. die Öffnung für Szenen mit konstanten Lichtverhältnissen feststellen.**Blendenöffnung**

 : Passen Sie mithilfe des Schiebereglers die Blendenöffnung an, d. h. wie viel Licht durch das Objektiv gelassen wird. Bewegen Sie den Schieberegler in Richtung **Öffnen**, damit mehr Licht in den Sensor gelangen kann, um bei schwachen Lichtverhältnissen ein helleres Bild zu erzeugen. Eine große Blendenöffnung reduziert auch die Schärfentiefe, d.h. dass sich nahe der Kamera oder weit von ihr entfernt befindliche Objekte nur unscharf erfasst werden. Bewegen Sie den Schieberegler in Richtung **Geschlossen**, damit ein das Bild stärker fokussiert werden kann.**Belichtungsgrad**: Stellen Sie mithilfe des Schiebereglers die

Bildbelichtung ein.Defog (Entnebelung)  : Aktivieren Sie diese Option, damit Nebelwetter erkannt wird und zur Erzeugung eines deutlicheren Bilds Nebel effekte erfasst und entfernt wird.

Hinweis

Wir raten Ihnen davon ab, bei Szenen mit geringem Kontrast, großen Unterschieden in den Lichtverhältnissen oder bei leicht unscharfem Autofokus **Entnebelung** zu aktivieren. Dies kann die Bildqualität beispielsweise durch erhöhten Kontrast beeinflussen. Bei aktivierter Entnebelung kann sich außerdem zu große Helligkeit negativ auf die Bildqualität auswirken.

Videostream

Allgemein

Auflösung: Wählen Sie eine für die zu überwachende Szene geeignete Bildauflösung. Eine höhere Auflösung erfordert mehr Bandbreite und Speicherplatz.**Bildrate**: Um Bandbreitenprobleme im Netzwerk zu vermeiden oder den Speicherbedarf zu reduzieren, kann die Bildrate auf eine feste Größe begrenzt werden. Wird die Bildrate bei Null belassen, wird die unter den aktuellen Bedingungen höchstmögliche Bildrate zugelassen. Höhere Bildraten erfordern mehr Bandbreite und Speicherkapazität.**P-frames (P-Frames)**: Ein P-Frame ist ein vorhersagbares Einzelbild, das nur die Bildänderungen gegenüber dem vorangehenden Einzelbild anzeigt. Geben Sie die gewünschte Anzahl von P-Frames ein. Je höher die Anzahl, desto weniger Bandbreite ist erforderlich. Tritt aber im Netzwerk ein Datenstau auf, könnte es zu einer merklichen Verschlechterung der Videoqualität kommen.**Compression (Komprimierung)**: Stellen Sie mithilfe des Schiebereglers die Bildkomprimierung ein. Höhere Komprimierung hat eine niedrigere Bitrate und eine geringere Bildqualität zur Folge. Eine niedrigere Komprimierung verbessert die Bildqualität, benötigt jedoch

beim Aufzeichnen eine höhere Bandbreite und mehr Speicher.**Signiertes Video**  : Aktivieren Sie diese Option, um Videos die Funktion Signiertes Video hinzuzufügen. Signiertes Video schützt durch das Hinzufügen von kryptografischen Signaturen das Video vor Manipulation.

Zipstream

Zipstream ist eine Technologie zur Bitratenreduzierung, um die Videoüberwachung zu optimieren. Sie reduziert in Echtzeit die durchschnittliche Bitrate eines H.264- oder H.265-Streams. Bei Szenen mit mehreren Interessensbereichen wendet Axis Zipstream eine hohe Bitrate an, z.B. bei Szenen mit sich bewegenden Objekten. Ist die überwachte Szene eher statisch, wendet Zipstream eine niedrigere Bitrate an und reduziert so den Bedarf an Speicherplatz. Weitere Informationen finden Sie unter *Reduzierung der Bitrate mit Axis Zipstream*

AXIS A8207-VE Mk II Network Video Door Station

Die Weboberfläche

Strength (Stärke) der Bitrate-Verringerung wählen:

- **Off (Aus):** Keine Reduzierung der Bitrate.
- **Low (Niedrig):** Bei den meisten Szenen keine sichtbaren Qualitätseinbußen. Dies ist die Standardoption, die bei allen Szenentypen zur Reduzierung der Bitrate verwendet werden kann.
- **Mittel:** Sichtbare Auswirkungen in einigen Szenen, mit weniger Rauschen und leicht verringerte Detailschärfe in Bereichen von untergeordnetem Interesse (zum Beispiel Bereichen ohne Bewegungsaufkommen).
- **High (Hoch):** Sichtbare Auswirkungen in einigen Szenen, mit weniger Rauschen und verringerte Detailschärfe in Bereichen von untergeordnetem Interesse (zum Beispiel Bereichen ohne Bewegungsaufkommen). Diese Stufe wird für mit der Cloud verbundene Geräte und Geräte empfohlen, die auf lokalen Speicher zurückgreifen.
- **Höher:** Sichtbare Auswirkungen in einigen Szenen, mit weniger Rauschen und verringerte Detailschärfe in Bereichen von untergeordnetem Interesse (zum Beispiel Bereichen ohne Bewegungsaufkommen).
- **Extreme (Extrem):** Sichtbarer Effekt in den meisten Szenen: Die Bitrate wird für den kleinsten Speicher optimiert.

Optimize for storage (Für Speicherung optimieren): Aktivieren Sie dies, um die Bitrate zu minimieren und dabei die Qualität zu erhalten. Die Optimierung wird nicht auf den im Webclient angezeigten Videostream angewendet. Dies kann nur verwendet werden, wenn Ihr VMS B-Rahmen unterstützt. Durch Aktivieren von **Optimize for storage** (Speicheroptimierung) wird auch **Dynamic GOP** aktiviert.**Dynamische FPS** (Bilder pro Sekunde): Aktivieren Sie diese Option, damit sich die Bandbreite je nach Aktivitätsniveau der Szene ändern kann. Mehr Aktivität erfordert mehr Bandbreite.**Unterer Grenzwert:** Geben Sie einen Wert ein, um je nach Bewegung in der Szene die Bildrate zwischen der Mindestanzahl an Bildern pro Sekunde und den Standardanzahl an Bilder pro Sekunde anzupassen. Wir empfehlen, bei Szenen mit sehr geringer Bewegung, bei denen die Anzahl an Bilder pro Sekunde auf 1 oder niedriger fallen können, einen unteren Grenzwert anzugeben.**Dynamic GOP** (Group of Pictures): Aktivieren Sie diese Option, um das Intervall zwischen I-Frames anhand des Aktivitätsniveaus der Szene dynamisch anzupassen.**Oberer Grenzwert:** Geben Sie eine maximale GOP-Länge ein, das heißt die maximale Anzahl von P-Frames zwischen zwei I-Frames. Ein I-Frame ist ein Einzelbild, das unabhängig von anderen Einzelbildern dekodierbar ist.

Bitrate control (Bitratensteuerung)

- **Average (Durchschnitt):** Wählen Sie diese Option, um die Bitrate automatisch über einen längeren Zeitraum anzupassen und je nach verfügbarem Speicher die bestmögliche Bildqualität zu liefern.
 -  Klicken Sie darauf, um die Zielbitrate anhand des verfügbaren Speichers, der Aufbewahrungszeit und des Bitratenlimits zu berechnen.
 - **Zielbitrate:** Geben Sie die gewünschte Zielbitrate ein.
 - **Aufbewahrungszeit:** Geben Sie die Aufbewahrungszeit für Aufzeichnungen in Tagen ein.
 - **Speicher:** Zeigt den für den Videostream nutzbaren geschätzten Speicherplatz an.
 - **Maximale Bitrate:** Aktivieren Sie diese Option, um eine Bitratengrenze festzulegen.
 - **Bitratengrenze:** Geben Sie eine Bitratengrenze ein, die über der Zielbitrate liegt.
- **Maximum:** Wählen Sie diese Option, um die maximale Sofort-Bitrate des Videostreams auf Grundlage der Netzwerkbandbreite festzulegen.
 - **Maximum:** Geben Sie die maximale Bitrate ein.
- **Variable:** Wählen Sie diese Option, damit sich die Bitrate je nach Aktivitätsniveau der Szene anpasst. Mehr Aktivität erfordert mehr Bandbreite. Diese Option wird für die meisten Situationen empfohlen.

Ausrichtung

Spiegelung: Aktivieren Sie diese Option, um das Bild zu spiegeln.

Audio

Einschließen: Aktivieren Sie diese Option, um Audio im Videostream zu verwenden.**Source (Quelle)**  : Wählen die zu verwendende Audioquelle.**Stereo**  : Aktivieren Sie diese Option, um sowohl integriertes Audio als auch Audio von einem externen Mikrofon zu verwenden.

AXIS A8207-VE Mk II Network Video Door Station

Die Weboberfläche

Overlays



- : Klicken Sie darauf, um ein Overlay hinzuzufügen. Wählen Sie in der Auswahlliste den Typ des Overlays aus:
- **Text:** Wählen Sie diese Option, um einen Text anzeigen zu lassen, der in das Live-Ansichtsbild integriert und in allen Ansichten, Aufzeichnungen und Schnappschüssen sichtbar ist. Sie können einen eigenen Text eingeben und Sie können auch vorkonfigurierte Modifikatoren verwenden, um z. B. Uhrzeit, Datum und Bildrate automatisch anzeigen zu lassen.
 -  : Klicken Sie darauf, um den Datumsmodifikator %F hinzuzufügen und das Format JJJJ-MM-TT anzuzeigen.
 -  : Klicken Sie darauf, um den Uhrzeitmodifikator %X hinzuzufügen und das Format hh:mm:ss (24-Stunden) anzeigen zu lassen.
 - **Modifikatoren:** Klicken Sie darauf, um beliebige der in der Liste angezeigten Modifikatoren auszuwählen und sie dem Textfeld hinzuzufügen. So zeigt zum Beispiel %a den Wochentag an.
 - **Größe:** Wählen Sie die gewünschte Schriftgröße.
 - **Darstellung:** Wählen Sie die Textfarbe und den Hintergrund, zum Beispiel weißer Text auf schwarzem Hintergrund (Standardeinstellung).
 -  : Wählen Sie die Position des Overlays im Bild.
 - **Bild:** Wählen Sie diese Option, um ein statisches Bild über dem Videostream zu zeigen. Sie können .bmp-, .png-, .jpeg- oder .s jpeg-Dateien verwenden.

Um ein Bild hochzuladen, klicken Sie auf **Bilder**. Bevor Sie ein Bild hochladen, können Sie folgende Optionen festlegen:

 - **An Auflösung anpassen:** Wählen Sie diese Option, um das Overlay-Bild automatisch an die Videoauflösung anzupassen.
 - **Transparenz verwenden:** Wählen Sie den Hexadezimal-RGB-Wert für diese Farbe und geben Sie diesen ein. Verwenden Sie das Format RRGGBB. Beispiele für Hexadezimalwerte: FFFFFFF für Weiß, 000000 für Schwarz, FF0000 für Rot, 6633FF für Blau und 669900 für Grün. Nur bei .bmp-Bildern.
 - **Scene annotation (Szenenkennzeichnung)**  : Wählen Sie diese Option aus, um im Videostream ein Text-Overlay anzuzeigen, das an derselben Position bleibt, auch wenn die Kamera in eine andere Richtung schwenkt oder neigt. Sie können festlegen, dass das Overlay nur innerhalb bestimmter Zoomstufen angezeigt wird.
 -  : Klicken Sie darauf, um den Datumsmodifikator %F hinzuzufügen und das Format JJJJ-MM-TT anzuzeigen.
 -  : Klicken Sie darauf, um den Uhrzeitmodifikator %X hinzuzufügen und das Format hh:mm:ss (24-Stunden) anzeigen zu lassen.
 - **Modifikatoren:** Klicken Sie darauf, um beliebige der in der Liste angezeigten Modifikatoren auszuwählen und sie dem Textfeld hinzuzufügen. So zeigt zum Beispiel %a den Wochentag an.
 - **Größe:** Wählen Sie die gewünschte Schriftgröße.
 - **Darstellung:** Wählen Sie die Textfarbe und den Hintergrund, zum Beispiel weißer Text auf schwarzem Hintergrund (Standardeinstellung).
 -  : Wählen Sie die Position des Overlays im Bild. Das Overlay wird gespeichert und verbleibt in den Schwenk- und Neigekoordinaten dieser Position.
 - **Annotation between zoom levels (%) (Kennzeichnung zwischen diesen Zoomstufen (%)):** Legen Sie die Zoomstufen fest, innerhalb derer das Overlay angezeigt wird.
 - **Annotation symbol (Kennzeichnungssymbol):** Wählen Sie ein Symbol aus, das anstelle des Overlays angezeigt wird, wenn sich die Kamera nicht innerhalb der eingestellten Zoomstufen befindet.
 - **Streaming indicator (Streaming-Indikator)**  : Wählen Sie diese Option, um eine Animation über dem Videostream zu einzublenden. Die Animation zeigt an, dass der Videostream live ist, selbst wenn die Szene aktuell bewegungsfrei ist.
 - **Darstellung:** Wählen Sie die Farbe der Animation und des Hintergrunds, zum Beispiel rote Animation auf durchsichtigem Hintergrund (Standardeinstellung).
 - **Größe:** Wählen Sie die gewünschte Schriftgröße.
 -  : Wählen Sie die Position des Overlays im Bild.

AXIS A8207-VE Mk II Network Video Door Station

Die Weboberfläche

- **Widget: Liniendiagramm**  : Zeigt ein Diagramm an, das verdeutlicht, wie sich ein Messwert im Laufe der Zeit ändert.
 - **Title (Titel):** Einen Titel für das Widget eingeben.
 - **Overlay modifier (Overlay-Modifikator):** Wählen Sie einen Overlay-Modifikator als Datenquelle aus. Wenn Sie MQTT-Overlays erstellt haben, werden diese am Ende der Liste angezeigt.
 -  : Wählen Sie die Position des Overlays im Bild.
 - **Size (Größe):** Die Größe des Overlays auswählen.
 - **Auf allen Kanälen sichtbar:** Deaktivieren Sie die Option, um nur auf Ihrem aktuell ausgewählten Kanal anzuzeigen. Schalten Sie diese Option ein, um auf allen aktiven Kanälen anzuzeigen.
 - **Aktualisierungsintervall:** Wählen Sie die Zeit zwischen Datenaktualisierungen.
 - **Transparenz:** Legen Sie die Transparenz des gesamten Overlays fest.
 - **Hintergrundtransparenz:** Stellen Sie die Transparenz nur für den Hintergrund des Overlays ein.
 - **Punkte:** Schalten Sie diese Option ein, um der Diagrammlinie einen Punkt hinzuzufügen, wenn Daten aktualisiert werden.
 - **X-Achse**
 - **Bezeichnung:** Geben Sie die Textbeschriftung für die x-Achse ein.
 - **Zeitfenster:** Geben Sie ein, wie lange die Daten visualisiert werden sollen.
 - **Zeiteinheit:** Geben Sie eine Zeiteinheit für die x-Achse ein.
 - **Y-Achse**
 - **Bezeichnung:** Geben Sie die Textbeschriftung für die y-Achse ein.
 - **Dynamische Skala:** Schalten Sie diese Option ein, damit sich die Skala automatisch an die Datenwerte anpasst. Schalten Sie diese Option aus, um Werte für eine feste Skala manuell einzugeben.
 - **Min. Alarmschwelle und Max. Alarmschwelle:** Diese Werte fügen dem Diagramm horizontale Referenzlinien hinzu, sodass Sie leichter erkennen können, wann der Datenwert zu hoch oder zu niedrig wird.
- **Widget: Messen**  : Zeigen Sie ein Balkendiagramm an, das den zuletzt gemessenen Datenwert anzeigt.
 - **Title (Titel):** Einen Titel für das Widget eingeben.
 - **Overlay modifier (Overlay-Modifikator):** Wählen Sie einen Overlay-Modifikator als Datenquelle aus. Wenn Sie MQTT-Overlays erstellt haben, werden diese am Ende der Liste angezeigt.
 -  : Wählen Sie die Position des Overlays im Bild.
 - **Size (Größe):** Die Größe des Overlays auswählen.
 - **Auf allen Kanälen sichtbar:** Deaktivieren Sie die Option, um nur auf Ihrem aktuell ausgewählten Kanal anzuzeigen. Schalten Sie diese Option ein, um auf allen aktiven Kanälen anzuzeigen.
 - **Aktualisierungsintervall:** Wählen Sie die Zeit zwischen Datenaktualisierungen.
 - **Transparenz:** Legen Sie die Transparenz des gesamten Overlays fest.
 - **Hintergrundtransparenz:** Stellen Sie die Transparenz nur für den Hintergrund des Overlays ein.
 - **Punkte:** Schalten Sie diese Option ein, um der Diagrammlinie einen Punkt hinzuzufügen, wenn Daten aktualisiert werden.
 - **Y-Achse**
 - **Bezeichnung:** Geben Sie die Textbeschriftung für die y-Achse ein.
 - **Dynamische Skala:** Schalten Sie diese Option ein, damit sich die Skala automatisch an die Datenwerte anpasst. Schalten Sie diese Option aus, um Werte für eine feste Skala manuell einzugeben.
 - **Min. Alarmschwelle und Max. Alarmschwelle:** Diese Werte fügen dem Balkendiagramm horizontale Referenzlinien hinzu, sodass Sie leichter erkennen können, wann der Datenwert zu hoch oder zu niedrig wird.

Privatzonenmasken



: Klicken Sie darauf, um eine neue Privatzonenmaske zu erstellen. **Privacy masks (Privatzonenmasken):** Klicken Sie darauf, um die Farbe aller Privatzonenmasken zu ändern oder um alle Privatzonenmasken dauerhaft zu löschen.  **Maske x:** Klicken Sie darauf, um die Maske umzubenennen, zu deaktivieren oder dauerhaft zu löschen.

AXIS A8207-VE Mk II Network Video Door Station

Die Weboberfläche

Leser

Verbindung

Protokoll des Lesegeräts

Protokolltyp des Lesegeräts: Wählen Sie das Protokoll für die Leser-Funktionalität aus.

- **VAPIX-Leser:** Kann nur mit einer Axis Tür-Steuerung verwendet werden.
 - **Protokoll:** Wählen Sie HTTPS oder HTTP aus.
 - **Adresse der Türsteuerung:** Geben Sie die IP-Adresse für die Türsteuerung ein.
 - **Username (Benutzername):** Geben Sie den Benutzernamen der Tür-Steuerung ein.
 - **Kennwort:** Geben Sie das Kennwort der Tür-Steuerung ein.
 - **Connect (Verbinden):** Klicken Sie, um eine Verbindung mit der Tür-Steuerung herzustellen.
 - **Leser auswählen:** Wählen Sie den Eingangsleser für die entsprechende Tür.
- **OSDP:**
 - **OSDP-Adresse:** Geben Sie die OSDP-Lesegerätadresse ein. 0 ist der Standardwert und die gebräuchlichste Adresse für einzelne Leser.
- **Wiegand ** :
 - **Signaltongeber:** Anschalten, um den Tonsignaleingang zu aktivieren.
 - **Eingang für Summer:** Wählen Sie den für den Summer verwendeten E/A-Port aus.
 - **Eingang für die LED-Steuerung:** Wählen Sie aus, wie viele E/A-Ports für die Steuerung des LED-Feedbacks auf dem Gerät verwendet werden soll.
 - **Input for LED1/LED2 (Eingang für LED1/LED2):** Wählen Sie aus, welche E/A-Ports für den LED-Eingang verwendet werden sollen.
 - **Idle color (Farbe Leerbetrieb):** Wenn zur Steuerung der LED kein I/O-Port verwendet wird, können Sie eine statische Farbe wählen, die auf dem Kartenleser-Markierungsstreifen angezeigt werden soll.
 - **Farbe für den Status Niedrig/Hoch:** Wenn für die LED-Steuerung ein I/O-Port verwendet wird, wählen Sie die Farbe aus, die für den Status niedrig bzw. den Status hoch angezeigt werden soll.
 - **Farbe für Leerbetrieb/LED1-Farbe/LED2-Farbe/LED1 + LED2-Farbe:** Wenn für die LED-Steuerung zwei I/O-Ports verwendet werden, wählen Sie die Farben für Leerbetrieb, LED1, LED2 bzw. LED1 + LED2.
 - **Drucktastenformat:** Wählen Sie aus, wie die PIN formatiert wird, wenn sie an die Zugangskontrolleinheit gesendet wird.
 - **FourBit:** PIN 1234 wird codiert und als 0x1 0x2 0x3 0x4 gesendet. Dies ist das am häufigsten verbreitete Standardverhalten.
 - **EightBitZeroPadded:** PIN 1234 wird codiert und als 0x01 0x02 0x03 0x04 gesendet.
 - **EightBitInvertPadded:** PIN 1234 wird codiert und als 0xE1 0xD2 0xC3 0xB4 gesendet.
 - **Wiegand26:** Die PIN ist im Wiegand26-Format mit einem 8-Bit-Gebäude-Zugangscod und einer 16-Bit-ID codiert.
 - **Wiegand34:** Die PIN ist im Wiegand34-Format mit einem 16-Bit-Gebäude-Zugangscod und einer 16-Bit-ID codiert.
 - **Wiegand37:** Die PIN ist im Wiegand37-Format (H10302) mit einer 35-Bit-ID codiert.
 - **Wiegand37FacilityCode:** Die PIN ist im Wiegand37-Format (H10304) mit einem 16-Bit-Gebäude-Zugangscod und einer 19-Bit-ID codiert.
 - **Facility code (Gebäude-Zugangscod):** Geben Sie den Gebäude-Zugangscod ein, der gesendet werden soll. Diese Option ist nur für einige Tastendruckformate verfügbar.

Ausgabeformat

Datenformat auswählen: Wählen Sie aus, in welchem Format Kartendaten an die Zugangskontrolleinheit gesendet werden.

- **Raw:** Überträgt die Kartendaten so, wie sie sind.
- **Wiegand26:** Kodiert die Kartendaten im Wiegand26-Format mit einem facility code für 8 Bit und einer 16-Bit-ID.
- **Wiegand34:** Kodiert die Kartendaten im Wiegand34-Format mit einem facility code für 16 Bit und einer 16-Bit-ID.
- **Wiegand37:** Kodiert die Kartendaten im Wiegand37-Format (H10302) mit einer 35-Bit-ID.
- **Wiegand37FacilityCode:** Kodiert die Kartendaten im Wiegand37-Format (H10304) mit einem Gebäude-Zugangscod für 16 Bit und einer 19-Bit-ID.
- **Benutzerdefiniert:** Legen Sie Ihre eigene Formatierung fest.

Überschreibungsmodus für Gebäude-Zugangscod: Wählen Sie eine Option aus, um den Gebäude-Zugangscod zu überschreiben.

AXIS A8207-VE Mk II Network Video Door Station

Die Weboberfläche

- **Auto:** Überschreibt den Gebäude-Zugangscod nicht und erstellt aus der automatischen Erfassung von Eingangsdaten einen Gebäude-Zugangscod. Verwendet entweder den ursprünglichen Gebäude-Zugangscod der Karte oder fälscht ihn aus überschüssigen Bits einer Kartennummer.
- **Optional:** Verwendet den Gebäude-Zugangscod aus den Eingangsdaten oder überschreibt ihn mit einem konfigurierten optionalen Wert.
- **Überschreiben:** Überschreibt stets mit einem bestimmten Gebäude-Zugangscod.

Chiptypen

Chiptypen

Activate chip type (Chiptyp aktivieren): Wählen Sie einen Chiptyp aus der Liste aus, um diesen zu aktivieren. **Activate chip types (Chiptypen aktivieren)** zeigt eine Liste aller aktiven Chiptypen an und gibt an, ob diese Standard- oder benutzerdefinierte Daten

verwenden.  Das Kontextmenü enthält:

- **Deaktivieren:** Klicken Sie hier, um den Chiptyp aus der Liste aktiver Chiptypen zu entfernen.

Datensätze für aktive Chiptypen

Invert byte order for all chip types using the full card serial number (CSN) (Byte-Reihenfolge für alle Chiptypen anhand der vollständigen Karten-Seriennummer (CSN) invertieren): Aktivieren Sie diese Option, um die Byte-Reihenfolge der Karten-Seriennummer zu invertieren. Die Seriennummer der Karte ist standardmäßig voreingestellt. **Invert byte order for all chip types using secure card data** (Byte-Reihenfolge für alle Chiptypen anhand sicherer Kartendaten invertieren): Aktivieren Sie diese Option, um die Byte-Reihenfolge der sicheren Kartendaten für Chiptypen zu invertieren, die einen benutzerdefinierten Datensatz verwenden. **Add data set (Datensatz hinzufügen):** Wählen Sie einen Chiptyp aus, und klicken Sie auf diese Option, um einen Datensatz hinzuzufügen. Für benutzerdefinierte Daten.

- **Name of data set (Datensatzname):** Benennen Sie den Datensatz zur leichteren Datenzuordnung um. Der Name muss eindeutig sein. Er übernimmt die Funktion einer ID, z. B. in der API.
- **Enabled (Aktiviert):** Deaktivieren Sie diese Option, um die Verwendung des Datensatzes zu beenden, ohne ihn zu löschen.
- **Required data (Erforderliche Daten):** Bei Aktivierung dieser Einstellung sendet das Gerät keine Daten an die Türsteuerung, falls aus irgendeinem Grund nicht auf sichere Kartendaten zugegriffen werden kann. Deaktivieren Sie diese Option, um die Karten-Seriennummer (CSN) an die Türsteuerung zu senden, falls keine sicheren Kartendaten zur Verfügung stehen.
- **Use as authenticator (Als Authentifikator verwenden):** Deaktivieren Sie diese Option, falls Sie keine sicheren Kartendaten für die Authentifizierung verwenden und diese nur als gültige Metadaten für das VAPIX-Protokoll übertragen möchten.
- **Offset (bits) (Offset in Bits):** Geben Sie die Startposition der Daten ein. „0“ bedeutet, dass die Startposition das erste Bit ist.
- **Length (bits) (Bitlänge):** Geben Sie Länge der Daten ein. „0“ bedeutet, dass eine beliebige Datenlänge ausgelesen wird.
- **Use data on card (Daten auf Karte verwenden):** Aktivieren Sie diese Option, um sichere Kartendaten zu verwenden. Deaktivieren Sie diese Option, um anstelle sicherer Kartendaten die Karten-Seriennummer (CSN) zu verwenden.

Die übrigen Einstellungen sind chiptyp-spezifisch und legen fest, wie die sicheren Kartendaten ausgelesen werden sollen.

PIN

Die PIN-Einstellungen müssen mit denen übereinstimmen, die in der Zugangskontrolleinheit konfiguriert wurden.

Length (0–32) (Länge (0–32)): Geben Sie die Anzahl der Stellen in der PIN ein. Wenn Benutzer beim Verwenden des Readers keine PIN verwenden müssen, legen Sie die Länge auf 0 fest. **Timeout (seconds, 3–50) (Zeitüberschreitung (3 bis 50 Sekunden)):** Geben Sie die Anzahl der Sekunden ein, die vergehen müssen, bis das Gerät in den Stromsparmmodus zurückkehrt, wenn keine PIN empfangen wird.

Zugangsberechtigungsliste

Mit der Zugangsberechtigungsliste können Sie das Gerät so einrichten, dass Eigentümer von Zugangsdaten ihre Karte oder PIN verwenden können, um verschiedene Aktionen wie etwa das Öffnen einer Tür durchzuführen. Die Zugangsdaten werden lokal im Gerät gespeichert. Diese Funktion kann auch mit einer externen Tür-Steuerung kombiniert werden.

AXIS A8207-VE Mk II Network Video Door Station

Die Weboberfläche

Use Entry list (Zugangsberechtigungsliste verwenden): Aktivieren Sie die Funktion, um die Zugangsberechtigungsliste zu verwenden.**Use connected door controller (Verbundene Tür-Steuerung verwenden):** Aktivieren Sie diese Funktion, wenn das Gerät bereits mit einer Tür-Steuerung verbunden ist. Wenn eine Person Zugangsdaten angibt, die nicht in der Zugangsberechtigungsliste aufgeführt sind, senden wir die Anfrage an die verbundene Tür-Steuerung. Wir senden keine Zugangsdaten, die in der Zugangsberechtigungsliste verfügbar sind.**Add credential holder (Eigentümer der Anmeldedaten hinzufügen):** Klicken Sie hier, um einen neuen Eigentümer der Anmeldedaten hinzuzufügen.**First name (Vorname):** Geben Sie einen Vornamen ein.**Last name (Nachname):** Geben Sie einen Nachnamen ein.**Credential type (Art der Zugangsdaten):**

- **PIN:**
 - **PIN:** Geben Sie eine eindeutige PIN ein, oder klicken Sie auf **Generate (Generieren)**, um automatisch eine erstellen zu lassen.
- **Card (Karte):**
 - **UID:** Geben Sie die UID und die Bitlänge der Karte ein, oder klicken Sie auf **Get latest (Neueste abrufen)**, um die Daten des letzten Durchziehens einer Karte abzurufen.

Event condition (Ereignisbedingung): Wählen Sie eine oder mehrere Bedingungen aus, die ausgelöst werden, wenn der Eigentümer der Zugangsdaten seine Zugangsdaten verwendet. Um die daraus resultierende Aktion einzurichten, gehen Sie zu **System > Events (System > Ereignisse)**, und erstellen Sie eine Regel mit der Bedingung, die Sie hier ausgewählt haben.**Valid from (Gültig ab):** Wählen Sie **Current device time (Aktuelle Gerätezeit)** aus, um die Zugangsdaten sofort zu aktivieren. Hier können Sie angeben, wann die Zugangsdaten aktiviert werden sollen.**Valid to (Gültig bis):**

- **No end date (Kein Enddatum):** Die Zugangsdaten sind unbegrenzt gültig.
- **End date (Enddatum):** Geben Sie das Datum und die Uhrzeit des Zeitpunkts an, zu dem die Zugangsdaten ungültig werden.
- **Number of times (Anzahl):** Geben Sie an, wie oft der Eigentümer der Zugangsdaten die Zugangsdaten verwenden kann. Der Wert im Feld verringert sich, wenn die Zugangsdaten verwendet werden, und zeigt die verbleibende Anzahl von Verwendungen an.

Hinweise: Geben Sie optionale Informationen ein.**Suspend (Aussetzen):** Wählen Sie diese Option aus, um die Zugangsdaten vorübergehend ungültig zu machen.

Audio

Geräteinstellungen

Input (Eingang): Audioeingang ein- oder ausschalten. Zeigt die Eingangsart an.

Noise cancellation (Geräuschreduktion): Aktivieren Sie dies, um die Audioqualität durch Entfernen von Hintergrundgeräuschen zu verbessern.**Input type (Eingangsart)**  : Wählen Sie die Art des Eingangs aus, z. B. interner Mikrofon- oder Line-Eingang.**Power type (Spannungsart)**  : Wählen Sie die Art der Eingangsstromversorgung aus.**Apply changes (Änderungen übernehmen)**  : Wenden Sie Ihre Auswahl an.**Echo cancellation (Echounterdrückung)**  : Schalten Sie diese Option ein, um Echos während der Zwei-Wege-Kommunikation zu entfernen.**Separate gain controls (Separate Verstärkungsregler)**  : Schalten Sie diese Option ein, um die Verstärkung für die verschiedenen Eingangsarten separat einzustellen.**Automatic gain control (Automatische Verstärkungsregelung)**  : Aktivieren Sie dieses Option, damit die Verstärkung dynamisch an Klangänderungen angepasst wird.**Verstärkung:** Ändern Sie mithilfe des Schiebereglers die Verstärkung. Klicken Sie zum Stummschalten oder Aufheben der Verstärkung. Klicken Sie zum Stummschalten oder Aufheben der Stummschaltung auf das Mikrofonsymbol.

Ausgang: Zeigt die Ausgangsart an.

Verstärkung: Ändern Sie mithilfe des Schiebereglers die Verstärkung. Klicken Sie zum Stummschalten oder Aufheben der Stummschaltung auf das Lautsprechersymbol.

AXIS A8207-VE Mk II Network Video Door Station

Die Weboberfläche

Videostream

Encoding (Codierung): Wählen Sie die Codierung für das Streaming der Eingangsquelle aus. Diese Kodierung steht nur bei aktiviertem Audioeingang zur Auswahl. Klicken Sie auf **Enable audio input (Audioeingang aktivieren)**, falls der Audioeingang deaktiviert ist.

Echounterdrückung: Aktivieren Sie diese Option, um Echos während der Zwei-Wege-Kommunikation zu entfernen.

Audioclips

+ Add clip (Clip hinzufügen): Fügen Sie einen neuen Audioclip hinzu. Sie können Dateien wie .au, .mp3, .opus, .vorbis, .wav verwenden.  Audio-Clip abspielen.  Audio-Clip anhalten.  Das Kontextmenü enthält:

- **Rename (Umbenennen):** Namen des Audio-Clip ändern.
- **Create link (Link erstellen):** Erstellen Sie eine URL, über die der Audioclip auf dem Gerät abgespielt wird. Legen Sie für den Clip die Lautstärke und die Anzahl der Wiederholungen fest.
- **Herunterladen:** Laden Sie den Audioclip auf Ihren Computer herunter.
- **Löschen:** Entfernen Sie den Audioclip vom Gerät.

Aufzeichnungen

Ongoing recordings (Laufende Aufzeichnungen): Anzeige aller laufenden Aufzeichnungen des Geräts.  Starten einer Aufzeichnung des Geräts.  Wählen Sie das Speichermedium, auf dem die Aufzeichnung gespeichert werden soll. Beenden einer Aufzeichnung des Geräts. **Ausgelöste Aufzeichnungen** können entweder manuell gestoppt oder durch Ausschalten des Geräts beendet werden. **Fortlaufende Aufzeichnungen** laufen so lange weiter, bis sie manuell gestoppt werden. Bei Ausschalten des Geräts wird die Aufzeichnung nach dem Wiedereinschalten fortgesetzt.

 Die Aufzeichnung wiedergeben.  Abspielen der Aufzeichnung anhalten.   Informationen und Aufzeichnungsoptionen anzeigen oder verbergen. **Set export range (Exportbereich festlegen):** Geben Sie den Zeitraum ein, wenn Sie nur einen Teil der Aufzeichnung exportieren möchten. Beachten Sie, dass die Zeitspanne auf der Zeitzone des Geräts basiert, wenn Sie in einer anderen Zeitzone als der am Standort des Geräts arbeiten. **Encrypt (Verschlüsseln):** Legen Sie mit dieser Option ein Kennwort für exportierte Aufzeichnungen fest. Die exportierte Datei kann ohne das Kennwort nicht geöffnet werden. Klicken Sie auf , um eine Aufzeichnung zu löschen. **Export (Exportieren):** Exportieren der ganzen Aufzeichnung oder eines Teils davon.

 Klicken Sie darauf, um die Aufzeichnungen zu filtern. **Von:** Zeigt Aufzeichnungen, die nach einem bestimmten Zeitpunkt gemacht wurden. **Bis:** Zeigt Aufzeichnungen, die bis zu einem bestimmten Zeitpunkt gemacht wurden. **Source (Quelle) ** : Zeigt Aufzeichnungen auf Grundlage der Quelle. Die Quelle bezieht sich auf den Sensor. **Event (Ereignis):** Zeigt Aufzeichnungen auf Grundlage von Ereignissen. **Storage (Speicher):** Zeigt Aufzeichnungen nach Speichertyp.

AXIS A8207-VE Mk II Network Video Door Station

Die Weboberfläche

Apps

+ **Add app (App hinzufügen)**: Installieren einer neuen App. **Find more apps (Weitere Apps finden)**: Finden weiterer zu installierender Apps. Sie werden zu einer Übersichtsseite der Axis Apps weitergeleitet. **Allow unsigned apps (Unsignierte Apps erlauben)**  : Schalten Sie diese Option ein, um die Installation unsignierter Apps zu ermöglichen. **Allow root-privileged apps (Apps mit Root-Berechtigungen zulassen)**  : Schalten Sie diese Option ein, um Apps mit Root-Berechtigungen uneingeschränkter Zugriff auf das Gerät zu ermöglichen.  Sehen Sie sich die Sicherheitsupdates in den AXIS OS und ACAP-Apps an.

Hinweis

Bei gleichzeitiger Ausführung mehrerer Apps kann die Leistung des Geräts beeinträchtigt werden.

Verwenden Sie den Schalter neben dem App-Namen, um diese zu starten oder anzuhalten. **Open (Öffnen)**: Auf die Anwendungseinstellungen zugreifen. Die verfügbaren Einstellungen sind anwendungsabhängig. Für einige Anwendungen stehen keine Einstellmöglichkeiten zur Verfügung.  Das Kontextmenü kann je nachdem die folgenden Optionen enthalten:

- **Open-source license (Open-Source-Lizenz)**: Anzeigen von Informationen über die in der App genutzten Open-Source-Lizenzen.
- **App log (App-Protokoll)**: Ereignisprotokoll der App anzeigen. Das Protokoll ist hilfreich, wenn Sie sich an den Support wenden müssen.
- **Lizenz mit Schlüssel aktivieren**: Wenn für die App eine Lizenz erforderlich ist, muss sie aktiviert werden. Verwenden Sie diese Option, wenn Ihr Gerät keinen Internetzugang besitzt. Falls Sie keinen Lizenzschlüssel besitzen, gehen Sie zu axis.com/products/analytics. Um einen Lizenzschlüssel zu erzeugen, benötigen Sie einen Lizenzcode und die Seriennummer Ihres Axis Produkts,
- **Lizenz automatisch aktivieren**: Wenn für die App eine Lizenz erforderlich ist, muss sie aktiviert werden. Gehen Sie über diese Option, wenn Ihr Gerät über einen Internetzugang verfügt. Sie benötigen einen Lizenzschlüssel, um die Lizenz zu aktivieren.
- **Deactivate the license (Lizenz deaktivieren)**: Deaktivieren Sie die Lizenz, um sie durch eine andere Lizenz zu ersetzen, z. B. wenn Sie von einer Testlizenz zu einer vollständigen Lizenz wechseln. Wenn Sie die Lizenz deaktivieren, wird sie damit auch vom Gerät entfernt.
- **Settings (Einstellungen)**: Darüber werden die Parameter konfiguriert.
- **Delete (Löschen)**: Darüber löschen Sie die App dauerhaft vom Gerät. Die Lizenz muss zuerst deaktiviert werden, da sie andernfalls weiterhin aktiv ist.

System

Uhrzeit und Standort

Datum und Uhrzeit

Das Zeitformat hängt von den Spracheinstellungen des Webbrowsers ab.

Hinweis

Wir empfehlen Ihnen, Datum und Uhrzeit des Geräts mit einem NTP-Server zu synchronisieren.

AXIS A8207-VE Mk II Network Video Door Station

Die Weboberfläche

Synchronization (Synchronisierung): Wählen Sie eine Option zur Synchronisierung von Datum und Uhrzeit des Geräts aus.

- **Automatic date and time (manual NTS KE servers) (Datum und Uhrzeit automatisch (manuelle NTS-KE-Server)):** Diese Option führt eine Synchronisierung mit den sicheren NTP-Schlüssel-Servern durch, die mit dem DHCP-Server verbunden sind.
 - **Manual NTS KE servers (Manuelle NTS-KE-Server):** Geben Sie die IP-Adresse eines oder zweier NTP-Server ein. Wenn Sie zwei NTP-Server verwenden, synchronisiert und passt das Gerät die Uhrzeit anhand der Eingangsdaten beider Geräte an.
 - **Max NTP poll time (Max. NTP-Abfragezeit):** Wählen Sie die maximale Zeitspanne aus, die das Gerät warten soll, bis es den NTP-Server abfragt, um eine aktualisierte Zeit zu erhalten.
 - **Min NTP poll time (Min. NTP-Abfragezeit):** Wählen Sie die minimale Zeitspanne aus, die das Gerät warten soll, bis es den NTP-Server abfragt, um eine aktualisierte Zeit zu erhalten.
- **Automatic date and time (NTP servers using DHCP) (Datum und Uhrzeit automatisch (NTP-Server mit DHCP)):** Synchronisieren Sie das Gerät mit den NTP-Servern, die mit dem DHCP-Server verbunden sind.
 - **Fallback NTP servers (NTP-Reserve-Server):** Geben Sie die IP-Adresse eines oder zweier Reserve-Server ein.
 - **Max NTP poll time (Max. NTP-Abfragezeit):** Wählen Sie die maximale Zeitspanne aus, die das Gerät warten soll, bis es den NTP-Server abfragt, um eine aktualisierte Zeit zu erhalten.
 - **Min NTP poll time (Min. NTP-Abfragezeit):** Wählen Sie die minimale Zeitspanne aus, die das Gerät warten soll, bis es den NTP-Server abfragt, um eine aktualisierte Zeit zu erhalten.
- **Automatic date and time (manual NTP servers) (Datum und Uhrzeit automatisch (manuelle NTP-Server)):** Führen Sie eine Synchronisierung mit NTP-Servern Ihrer Wahl durch.
 - **Manual NTP servers (Manuelle NTP-Server):** Geben Sie die IP-Adresse eines oder zweier NTP-Server ein. Wenn Sie zwei NTP-Server verwenden, synchronisiert und passt das Gerät die Uhrzeit anhand der Eingangsdaten beider Geräte an.
 - **Max NTP poll time (Max. NTP-Abfragezeit):** Wählen Sie die maximale Zeitspanne aus, die das Gerät warten soll, bis es den NTP-Server abfragt, um eine aktualisierte Zeit zu erhalten.
 - **Min NTP poll time (Min. NTP-Abfragezeit):** Wählen Sie die minimale Zeitspanne aus, die das Gerät warten soll, bis es den NTP-Server abfragt, um eine aktualisierte Zeit zu erhalten.
- **Custom date and time (Datum und Uhrzeit benutzerdefiniert):** Stellen Sie Datum und Uhrzeit manuell ein. Klicken Sie **Get from system (Vom System abrufen)** an, um die Datums- und Uhrzeiteinstellungen einmalig von Ihrem Computer oder Mobilgerät abzurufen.

Time zone (Zeitzone): Wählen Sie die zu verwendende Zeitzone aus. Die Zeit wird automatisch bei Sommer- und Standardzeit angepasst.

- **DHCP:** Übernimmt die Zeitzone des DHCP-Servers. Bevor Sie diese Option auswählen können, muss das Gerät mit einem DHCP-Server verbunden werden.
- **Manuell:** Wählen Sie in der Drop-Down-Liste eine Zeitzone aus.

Hinweis

Die Einstellungen für Datum und Uhrzeit werden vom System für alle Aufzeichnungen, Protokolle und Systemeinstellungen verwendet.

Gerätestandort

Den Gerätestandort eingeben. Das Videoverwaltungssystem kann mit dieser Information das Gerät auf eine Karte setzen.

- **Latitude (Breite):** Positive Werte bezeichnen Standorte nördlich des Äquators.
- **Longitude (Länge):** Positive Werte bezeichnen Standorte östlich des Referenzmeridians.
- **Heading (Ausrichtung):** Die Ausrichtung des Geräts laut Kompass eingeben. Der Wert 0 steht für: genau nach Norden.
- **Label (Bezeichnung):** Eine aussagekräftige Bezeichnung für das Gerät eingeben.
- **Save (Speichern):** Klicken Sie hier, um den Gerätestandort zu speichern.

AXIS A8207-VE Mk II Network Video Door Station

Die Weboberfläche

Konfigurationsprüfung

Interactive device image (Interaktives Gerätebild): Klicken Sie auf die Schaltflächen im Bild, um die Tastenbedienung zu simulieren. Auf diese Weise können Sie Konfigurationen ausprobieren oder eine Fehlerbehebung für die Hardware durchführen, ohne physischen Zugriff auf das Gerät zu haben.

Latest credentials (Letzte Zugangsdaten)  : Zeigt Informationen zu den zuletzt registrierten Zugangsdaten an.   Die aktuellen Zugangsdaten anzeigen.   Das Kontextmenü enthält:

- **Reverse UID (UID umkehren):** Die Byte-Reihenfolge der UID umdrehen.
- **Revert UID (UID wiederherstellen):** Die Byte-Reihenfolge der UID zurück in die ursprüngliche Reihenfolge bringen.
- **Copy to clipboard (In die Zwischenablage kopieren):** Kopieren Sie die UID.

Check credentials (Zugangsdaten überprüfen)  : Geben Sie eine UID oder eine PIN ein und senden Sie, um die Zugangsdaten zu überprüfen. Das System antwortet auf die gleiche Weise, als hätten Sie Zugangsdaten für das Gerät verwendet. Wenn sowohl UID als auch PIN erforderlich sind, geben Sie zunächst die UID ein.

Netzwerk

IPv4

Assign IPv4 automatically (IPv4 automatisch zuweisen): Wählen Sie diese Option, damit der Netzwerkrouter dem Gerät automatisch eine IP-Adresse zuweisen kann. Für die meisten Netzwerke empfehlen wir eine automatische Zuweisung der IP-Adresse (DHCP).

IP address (IP-Adresse): Geben Sie für das Gerät eine eindeutige IP-Adresse ein. Statische IP-Adressen können innerhalb von isolierten Netzwerken zufällig zugewiesen werden, sofern jede Adresse eindeutig ist. Zur Vermeidung von Konflikten empfehlen wir Ihnen, sich vor dem Zuweisen einer statischen IP-Adresse an den Netzwerkadministrator zu wenden.

Subnet mask (Subnetzmaske): Geben Sie die Subnetzmaske ein, um festzulegen, welche Adressen sich im lokalen Netzwerk befinden. Jede Adresse außerhalb des lokalen Netzwerks wird über den Router geleitet.

Router: Geben Sie die IP-Adresse des Standardrouters (Gateway) ein, um Geräten zu verbinden, die in verschiedenen Netzwerken und Netzwerk-Segmenten verwendet werden.

Fallback to static IP address if DHCP isn't available (Fallback zu statischer IP-Adresse, wenn DHCP nicht verfügbar): Wählen Sie aus, ob Sie eine statische IP-Adresse hinzufügen möchten, die als Reserve verwendet werden soll, wenn DHCP nicht verfügbar ist und keine IP-Adresse automatisch zugewiesen werden kann.

Hinweis

Wenn DHCP nicht verfügbar ist und das Gerät eine statische Fallback-Adresse verwendet, wird die statische Adresse mit einem begrenzten Bereich konfiguriert.

IPv6

IPv6 automatisch zuweisen: Wählen Sie diese Option, um IPv6 einzuschalten und damit der Netzwerk-Router dem Gerät automatisch eine IP-Adresse zuweisen kann.

Host-Name

Assign hostname automatically (Host-Namen automatisch zuweisen): Wählen Sie diese Option aus, damit der Netzwerkrouter dem Gerät automatisch einen Host-Namen zuweisen kann.

Host-Name: Geben Sie den Host-Namen manuell ein, um ihn als alternative Möglichkeit für den Zugriff auf das Gerät zu verwenden. Der Server-Bericht und das Systemprotokoll verwenden den Host-Namen. Zugelassene Zeichen sind A-Z, a-z, 0-9 und -.

DNS servers (DNS-Server)

Assign DNS automatically (DNS automatisch zuweisen): Wählen Sie diese Option, damit der DHCP-Server dem Gerät automatisch Domains für die Suche und DNS-Server-Adressen zuweisen kann. Für die meisten Netzwerke empfehlen wir eine automatische Zuweisung der DNS-Server-Adresse (DHCP).

Search domains (Suchdomains): Wenn Sie einen Host-Namen verwenden, der nicht vollständig qualifiziert ist, klicken Sie auf **Add search domain (Suchdomain hinzufügen)** und geben Sie eine Domain ein, in der nach dem vom Gerät verwendeten Host-Namen gesucht werden soll.

DNS servers (DNS-Server): Klicken Sie auf **Add DNS server (DNS-Server hinzufügen)** und geben Sie die IP-Adresse des DNS-Servers ein. Dadurch werden in Ihrem Netzwerk Host-Namen in IP-Adressen übersetzt.

HTTP und HTTPS

AXIS A8207-VE Mk II Network Video Door Station

Die Weboberfläche

HTTPS ist ein Protokoll, das Verschlüsselung für Seitenanforderungen von Benutzern und für die vom Webserver zurückgegebenen Seiten bereitstellt. Der verschlüsselte Austausch von Informationen wird durch die Verwendung eines HTTPS-Zertifikats geregelt, das die Authentizität des Servers gewährleistet.

Um HTTPS auf dem Gerät verwenden zu können, muss ein HTTPS-Zertifikat installiert werden. Gehen Sie für die Erstellung und Installation von Zertifikaten zu **System > Security (System > Sicherheit)**.

Zugriff zulassen über: Wählen Sie aus, ob Sie einem Benutzer erlauben wollen, eine Verbindung mit dem Gerät über die Protokolle HTTP, HTTPS oder HTTP and HTTPS (HTTP und HTTPS) herzustellen.

Hinweis

Wenn Sie auf verschlüsselte Internetseiten über HTTPS gehen, kann es zu Beeinträchtigungen der Leistung kommen, insbesondere wenn Sie eine Seite zum ersten Mal aufrufen.

HTTP port (HTTP-Port): Geben Sie den zu verwendenden HTTP-Port ein. Das Gerät lässt Port 80 oder jeden Port im Bereich 1024-65535 zu. Wenn Sie als Administrator angemeldet sind, können Sie auch einen beliebigen Port im Bereich 1-1023 eingeben. Wenn Sie einen Port in diesem Bereich verwenden, erhalten Sie eine Warnung.**HTTPS port (HTTPS-Port):** Geben Sie den zu verwendenden HTTPS-Port ein. Das Gerät lässt Port 443 oder jeden Port im Bereich 1024-65535 zu. Wenn Sie als Administrator angemeldet sind, können Sie auch einen beliebigen Port im Bereich 1-1023 eingeben. Wenn Sie einen Port in diesem Bereich verwenden, erhalten Sie eine Warnung.**Zertifikat:** Wählen Sie ein Zertifikat, um HTTPS für das Gerät zu aktivieren.

Protokolle zur Netzwerkerkennung

Bonjour®: Aktivieren Sie diese Option, um die automatische Erkennung im Netzwerk bei Aktivierung zuzulassen.**Bonjour-Name:** Geben Sie den im Netzwerk anzuzeigenden Namen an. Der Standardname setzt sich aus dem Namen des Geräts und seiner MAC Adresse zusammen.**UPnP®:** Aktivieren Sie diese Option, um die automatische Erkennung im Netzwerk bei Aktivierung zuzulassen.**UPnP-Name:** Geben Sie den im Netzwerk anzuzeigenden Namen an. Der Standardname setzt sich aus dem Namen des Geräts und seiner MAC Adresse zusammen.**WS-Erkennung:** Aktivieren Sie diese Option, um die automatische Erkennung im Netzwerk bei Aktivierung zuzulassen.**LLDP und CDP:** Aktivieren Sie diese Option, um die automatische Erkennung im Netzwerk bei Aktivierung zuzulassen. Das Deaktivieren von LLDP und CDP kann sich auf das PoE-Leistungsmanagement auswirken. Konfigurieren Sie den PoE-Switch nur für das Hardware-PoE-Leistungsmanagement, um Probleme mit dem PoE-Leistungsmanagement zu beheben.

Cloud-Anbindung mit einem Mausklick

One-Click Cloud Connect (O3C) stellt in Verbindung mit einem O3C-Dienst einen einfachen und sicheren Internetzugang zu Live-Video und aufgezeichneten Videos von jedem Standort aus bereit. Weitere Informationen finden Sie unter axis.com/end-to-end-solutions/hosted-services.

Allow O3C (O3C zulassen):

- **One-click:** Dies ist die Standardeinstellung. Halten Sie die Steuertaste am Gerät gedrückt, um über das Internet eine Verbindung mit einem O3C-Dienst herzustellen. Sie müssen das Gerät innerhalb von 24 Stunden nach dem Drücken der Steuertaste beim O3C-Dienst registrieren. Andernfalls wird sich das Gerät vom O3C-Dienst getrennt. Nach der Registrierung des Geräts ist **Always (Immer)** aktiviert und das Gerät bleibt mit dem O3C-Dienst verbunden.
- **Immer:** Das Gerät versucht ständig, über das Internet eine Verbindung mit einem O3C-Dienst herzustellen. Nach der Registrierung bleibt das Gerät mit dem O3C-Dienst verbunden. Verwenden Sie diese Option, wenn die Steuertaste am Gerät außer Reichweite ist.
- **Nein:** Deaktiviert den O3C-Dienst.

Proxy settings (Proxy-Einstellungen): Geben Sie falls erforderlich die Proxyeinstellungen ein, um eine Verbindung zum Proxy-Server herzustellen.

Host: Geben Sie die Adresse des Proxy-Servers ein.**Port:** Geben Sie die Nummer der für den Zugriff verwendeten Ports an.**Anmeldung und Kennwort:** Geben Sie falls erforderlich einen Benutzernamen und ein Kennwort für den Proxyserver ein.**Authentication method (Authentifizierungsmethode):**

- **Basic (Einfach):** Diese Methode ist das am besten geeignete Authentifizierungsschema für HTTP. Sie ist nicht so sicher wie die Digest-Methode, da sie den Benutzernamen und das Kennwort unverschlüsselt an den Server sendet.
- **Digest:** Diese Methode ist sicherer, da das Kennwort hier stets verschlüsselt im Netzwerk übermittelt wird.
- **Auto:** Bei dieser Option kann das Gerät die Authentifizierungsmethode automatisch je nach unterstützten Methoden auswählen. Die Methode Digest wird gegenüber der Methode Einfach bevorzugt.

Besitzerauthentifizierungsschlüssel (OAK): Klicken Sie auf **Schlüssel abrufen**, um den Besitzerauthentifizierungsschlüssel abzurufen. Dies ist nur dann möglich, wenn das Gerät ohne Firewall oder Proxy mit dem Internet verbunden ist.

SNMP

AXIS A8207-VE Mk II Network Video Door Station

Die Weboberfläche

Simple Network Management Protocol (SNMP) ermöglicht die Remoteverwaltung von Netzwerk-Geräten.

SNMP: Wählen Sie die zu verwendende SNMP-Version.

- **v1 und v2c:**
 - **Lesen-Community:** Geben Sie den Namen der Community mit ausschließlich Lesezugriff auf alle unterstützten SNMP-Objekte an. Der Standardwert ist **public (öffentlich)**.
 - **Write community (Schreib-Community):** Geben Sie den Namen der Community mit Lese- oder Schreibzugriff auf alle unterstützten SNMP-Objekte (außer schreibgeschützte Objekte) an. Der Standardwert ist **schreiben**.
 - **Traps aktivieren:** Aktivieren Sie die Option, um Trap-Berichte zu erhalten. Traps werden vom Gerät bei wichtigen Ereignissen und Statusänderungen zum Versenden von Meldungen verwendet. In der Weboberfläche können Sie Traps für SNMP v1 und v2c einrichten. Traps werden automatisch deaktiviert, wenn Sie zu SNMP v3 wechseln oder SNMP deaktivieren. Wenn Sie SNMP v3 verwenden, können Sie Traps über die Verwaltungsanwendung für SNMP v3 einrichten.
 - **Trap-Adresse:** Geben Sie die IP-Adresse oder den Host-Namen des Verwaltungsservers ein.
 - **Trap-Community:** Geben Sie die Trap-Community ein, die das Gerät zum Versenden einer Trap-Meldung an das Verwaltungssystem verwenden soll.
 - **Traps:**
 - **Kaltstart:** Versendet eine Trap-Nachricht, wenn das Gerät hochgefahren wird.
 - **Warmstart:** Versendet eine Trap-Nachricht, wenn Sie eine SNMP-Einstellung ändern.
 - **Verbindungsaufbau:** Versendet eine Trap-Meldung, wenn der Status eines Links von Down zu Up wechselt.
 - **Authentifizierung fehlgeschlagen:** Versendet eine Trap-Meldung, wenn ein Authentifizierungsversuch fehlschlägt.

Hinweis

Alle Axis Video MIB-Traps sind aktiviert, wenn Sie SNMP v1- und v2c-Traps aktivieren. Weitere Informationen dazu finden Sie unter *AXIS OS Portal > SNMP*.

- **v3:** SNMP v3 ist eine Version mit höherer Sicherheit, die Verschlüsselung und sichere Kennwörter bereitstellt. Beim Verwenden von SNMP v3 empfehlen wir Ihnen, HTTPS zu aktivieren, da Kennwörter dann über HTTPS gesendet werden. Dadurch wird auch verhindert, dass Unbefugte auf unverschlüsselte Traps des Typs SNMP v1 und v2c zugreifen können. Wenn Sie SNMP v3 verwenden, können Sie Traps über die Verwaltungsanwendung für SNMP v3 einrichten.
 - **Kennwort für das Konto "initial":** Geben Sie das SNMP-Kennwort für das Konto mit dem Namen "initial" ein. Obwohl das Kennwort ohne Aktivierung von HTTPS gesendet werden kann, empfehlen wir es nicht. Das Kennwort für SNMP v3 kann nur einmal und vorzugsweise dann bei aktiviertem HTTPS festgelegt werden. Nach dem Einrichten des Kennworts wird das Kennwortfeld nicht mehr angezeigt. Wenn ein neues Kennwort eingerichtet werden soll, muss das Gerät auf die Werkseinstellungen zurückgesetzt werden.

Connected clients (Verbundene Clients)

Zeigt die Anzahl der Verbindungen und der verbundenen Clients an.

View details (Details anzeigen): Anzeigen und Aktualisieren der Liste der verbundenen Clients. Die Liste zeigt IP-Adresse, Protokoll, Port, Zustand und PID/Process für jede Verbindung an.

Sicherheit

Zertifikate

AXIS A8207-VE Mk II Network Video Door Station

Die Weboberfläche

Zertifikate werden in Netzwerken zum Authentifizieren von Geräten verwendet. Das Gerät unterstützt zwei Zertifikattypen:

- **Client-/Serverzertifikate**
Ein Client-/Serverzertifikat identifiziert das Axis Produkt und kann selbstsigniert oder von einer Zertifizierungsstelle (Certificate Authority, CA) ausgegeben worden sein. Ein selbstsigniertes Zertifikat bietet begrenzten Schutz und kann vor Erhalt eines CA-Zertifikats verwendet werden.
- **CA-Zertifikate**
CA-Zertifikate werden zum Authentifizieren von Peer-Zertifikaten verwendet, um zum Beispiel die Identität eines Authentifizierungsservers zu überprüfen, wenn das Gerät mit einem durch IEEE 802.1X geschützten Netzwerk verbunden ist. Auf dem Gerät sind mehrere CA-Zertifikate vorinstalliert.

Folgende Formate werden unterstützt:

- Zertifikatsformate: .PEM, .CER und .PFX
- Formate von privaten Schlüssel: PKCS#1 und PKCS#12

Wichtig

Wenn Sie das Gerät auf die Werkseinstellungen zurücksetzen, werden alle Zertifikate gelöscht. Vorinstallierte CA-Zertifikate werden neu installiert.



Zertifikat hinzufügen : Klicken Sie auf diese Option, um ein Zertifikat hinzuzufügen.

- **More (Mehr)**  : Anzeige weiterer Ausfüll- oder Auswahlfelder.
- **Secure keystore (Sicherer Schlüsselspeicher)**: Wählen Sie **Secure element (Sicheres Element)** oder **Trusted Platform Module 2.0** zum sicheren Speichern des privaten Schlüssels aus. Weitere Informationen zum zu wählenden sicheren Schlüsselspeicher finden Sie unter help.axis.com/en-us/axis-os#cryptographic-support.
- **Key type (Schlüsseltyp)**: Wählen Sie in der Dropdown-Liste zum Schutz des Zertifikats den Standard- oder einen anderen Verschlüsselungsalgorithmus aus.



Das Kontextmenü enthält:

- **Certificate information (Zertifikatsinformationen)**: Lassen Sie sich die Eigenschaften eines installierten Zertifikats anzeigen.
- **Zertifikat löschen**: Löschen Sie das Zertifikat.
- **Signierungsanforderung erstellen**: Erstellen Sie eine Anforderung zur Zertifikatsignierung, um sie an eine Registrierungsstelle zu senden und ein digitales Zertifikat zu erhalten.

Secure keystore (Sicherer Schlüsselspeicher)  :

- **Secure element (CC EAL6+)**: Wählen Sie diese Option aus, um sicheres Element für sicheren Schlüsselspeicher zu verwenden.
- **Trusted Platform Module 2.0 (CC EAL4+, FIPS 140-2 Level 2)**: Wählen Sie diese Option aus, um TPM 2.0 für sicheren Schlüsselspeicher zu verwenden.

Network access control and encryption (Netzwerkzugangskontrolle und Verschlüsselung)

IEEE 802.1x IEEE 802.1x ist ein IEEE-Standard für portbasierte Netzwerk-Zugriffskontrolle, die eine sichere Authentifizierung für drahtgebundene und drahtlose Netzwerk-Geräte bereitstellt. IEEE 802.1x basiert auf EAP (Extensible Authentication Protocol). Zum Zugriff auf ein mit IEEE 802.1x geschütztes Netzwerk müssen sich die Netzwerk-Geräte authentifizieren. Die Authentifizierung erfolgt durch einen Authentifizierungsserver, üblicherweise ein RADIUS-Server (zum Beispiel FreeRADIUS und Microsoft Internet Authentication Server). **IEEE 802.1AE MACsec** IEEE 802.1AE MACsec ist ein IEEE-Standard für MAC-Sicherheit (Media Access Control), der die Vertraulichkeit und Integrität verbindungsloser Daten für medienzugriffsunabhängige Protokolle definiert. **Zertifikate** Wenn die Konfiguration ohne CA-Zertifikat erfolgt, ist die Validierung des Serverzertifikats deaktiviert und das Gerät versucht, sich selbst zu authentifizieren, unabhängig vom aktuellen Netzwerk. Bei Verwendung eines Zertifikats bei der Implementierung von Axis authentifizieren sich das Gerät und der Authentifizierungsserver mithilfe von digitalen Zertifikaten über EAP-TLS (Extensible Authentication Protocol – Transport Layer Security). Damit das Gerät auf ein netzwerkgeschütztes Netzwerk zugreifen darf, müssen Sie ein signiertes Clientzertifikat auf dem Gerät installieren. **Authentication method (Authentifizierungsmethode)**: Wählen Sie einen EAP-Typ aus, der für die Authentifizierung verwendet wird. **Client certificate (Client-Zertifikat)**: Wählen Sie ein Client-Zertifikat aus, um IEEE 802.1x zu verwenden. Der Authentifizierungsserver verwendet das Zertifikat zur Validierung der Identität des Clients. **CA certificates (CA-Zertifikate)**: Wählen Sie CA-Zertifikate zur Validierung der Identität des Authentifizierungsservers. Wenn kein Zertifikat ausgewählt sind, versucht das Gerät, sich selbst zu authentifizieren, unabhängig vom Netzwerk, mit dem es verbunden ist. **EAP-Identität**: Geben Sie die mit dem Clientzertifikat verknüpfte Identität des Benutzers ein. **EAPOL-Version**: Wählen Sie die in dem Netzwerk-Switch verwendete EAPOL-Version. **Use IEEE 802.1x (IEEE 802.1x verwenden)**: Wählen Sie diese Option aus, um das IEEE 802.1x-Protokoll zu verwenden. Diese Einstellungen stehen nur zur Verfügung, wenn Sie IEEE 802.1x PEAP-MSCHAPv2 als Authentifizierungsmethode verwenden:

AXIS A8207-VE Mk II Network Video Door Station

Die Weboberfläche

- **Password (Kennwort):** Geben Sie das Password (Kennwort) für die Benutzeridentität ein.
- **Peap version (Peap-Version):** Wählen Sie die in dem Netzwerk-Switch verwendete Peap-Version aus.
- **Label (Bezeichnung):** Wählen Sie 1 aus, um die EAP-Verschlüsselung des Client zu verwenden. Wählen Sie 2 aus, um die PEAP-Verschlüsselung des Client zu verwenden. Wählen Sie die Bezeichnung aus, das der Netzwerk-Switch bei Verwendung von Peap-Version 1 verwendet.

Diese Einstellungen stehen nur zur Verfügung, wenn Sie IEEE 802.1ae MAGCsec (Static CAK/Pre-Shared Key) als Authentifizierungsmethode verwenden:

- **Key agreement connectivity association key name (Schlüsselname der Key Agreement Connectivity Association):** Geben Sie den Namen der Connectivity Association (CKN) ein. Der Name muss aus 2 bis 64 (durch 2 teilbare) Hexadezimalzeichen bestehen. Der CKN muss manuell in der Connectivity Association konfiguriert werden und auf beiden Seiten der Verbindung gleich sein, um MACsec zu initialisieren.
- **Key agreement connectivity association key (Schlüssel der Key Agreement Connectivity Association):** Geben Sie den Schlüssel der Connectivity Association (CAK) ein. Der Schlüssellänge sollte entweder 32 oder 64 Hexadezimalzeichen betragen. Der CAK muss manuell in der Connectivity Association konfiguriert werden und auf beiden Seiten der Verbindung gleich sein, um MACsec zu initialisieren.

Brute-Force-Angriffe verhindern

Blocken: Aktivieren Sie diese Option, um Brute-Force-Angriffe zu blockieren. Ein Brute-Force-Angriff versucht über Trial-and-Error, Zugangsdaten oder Verschlüsselungsschlüssel zu erraten.**Blockierdauer:** Geben Sie ein, wie viele Sekunden ein Brute-Force-Angriff blockiert werden soll.**Blockierbedingungen:** Geben Sie die Anzahl der pro Sekunde zulässigen Authentifizierungsfehler ein, bevor blockiert wird. Sie können die Anzahl der zulässigen Fehler sowohl auf Seiten- als auch auf Geräteebeine festlegen.

Firewall

Activate (Aktivieren): Schalten Sie die Firewall ein.

Default Policy (Standardrichtlinie): Wählen Sie den Standardstatus für die Firewall aus.

- **Allow: (Zulassen:)** Ermöglicht alle Verbindungen mit dem Gerät. Diese Option ist in der Standardeinstellung festgelegt.
- **Deny: (Verweigern:)** Verhindert alle Verbindungen mit dem Gerät.

Für Ausnahmen von der Standardrichtlinie können Sie Regeln erstellen, die über bestimmte Adressen, Protokolle und Ports Verbindungen zum Gerät zulassen oder verweigern.

- **Adresse:** Geben Sie eine Adresse im IPv4-/IPv6- oder im CIDR-Format ein, für die Sie den Zugriff zulassen oder verweigern möchten.
- **Protokoll:** Wählen Sie ein Protokoll aus, für das Sie den Zugriff zulassen oder verweigern möchten.
- **Anschluss:** Geben Sie eine Portnummer ein, für die Sie den Zugriff zulassen oder verweigern möchten. Sie können eine Portnummer zwischen 1 und 65535 hinzufügen.
- **Richtlinie:** Wählen Sie die Richtlinien der Regel aus.



: Klicken Sie darauf, um eine weitere Regel zu erstellen.

Add rules: (Regeln hinzufügen): Klicken Sie hier, um die von Ihnen definierten Regeln hinzuzufügen.

- **Time in seconds: (Zeit in Sekunden:)** Legen Sie für das Testen der Regeln ein Zeitlimit fest. Das Standardzeitlimit ist 300 Sekunden. Legen Sie die Zeit fest, um die Regeln sofort zu aktivieren 0 Sekunden.
- **Confirm rules: (Regeln bestätigen:)** Bestätigen Sie die Regeln und deren Zeitlimit. Wenn Sie eine Zeitbegrenzung von mehr als einer Sekunde festgelegt haben, sind die Regeln in dieser Zeit aktiv. Wenn Sie die Zeit auf 0 festgelegt haben, sind die Regeln sofort aktiv.

Pending rules (Ausstehende Regeln): Eine Übersicht über die kürzlich getesteten, noch zu bestätigenden Regeln.

Hinweis

Die Regeln mit einer Zeitgrenze werden unter **Active rules (Aktive Regeln)** angezeigt, bis der angezeigte Timer abläuft oder Sie die Regeln bestätigen. Wenn Sie die Regeln nicht bestätigen, werden sie unter **Pending rules (Ausstehende Regeln)** angezeigt, bis der Timer abläuft, und die Firewall wird auf die zuvor festgelegten Einstellungen zurückgesetzt. Wenn Sie diese bestätigen, werden die aktuellen aktiven Regeln ersetzt.

Confirm rules (Regeln bestätigen): Klicken Sie hier, um die anstehenden Regeln zu aktivieren.**Active rules (Aktive Regeln):** Eine

Übersicht über die Regeln, die momentan auf dem Gerät ausgeführt werden.  : Klicken Sie hier, um eine aktive Regel zu

löschen.  : Klicken Sie hier, um alle Regeln zu löschen, sowohl anstehend als auch aktiv.

AXIS A8207-VE Mk II Network Video Door Station

Die Weboberfläche

Benutzerdefiniertes signiertes AXIS OS-Zertifikat

Zum Installieren von Testsoftware oder anderer benutzerdefinierter Software von Axis auf dem Gerät benötigen Sie ein benutzerdefiniertes signiertes AXIS OS-Zertifikat. Das Zertifikat prüft, ob die Software sowohl vom Geräteeigentümer als auch von Axis genehmigt wurde. Die Software kann nur auf einem bestimmten Gerät ausgeführt werden, das anhand seiner eindeutigen Seriennummer und Chip-ID identifiziert wird. Spezifisch signierte AXIS OS-Zertifikate können nur von Axis erstellt werden, da Axis den Schlüssel zum Signieren besitzt.

Install (Installieren): Klicken Sie, um das Zertifikat zu installieren. Sie müssen das Zertifikat installieren, bevor Sie die Software installieren.  Das Kontextmenü enthält:

- **Delete certificate (Zertifikat löschen):** Löschen Sie das Zertifikat.

Konten

Accounts (Konten)



Add account (Konto hinzufügen): Klicken Sie, um ein neues Konto hinzuzufügen. Es können bis zu 100 Konten hinzugefügt werden.**Account (Konto):** Geben Sie einen eindeutigen Kontonamen ein.**New password (Neues Kennwort):** Geben Sie ein Kennwort für den Kontonamen ein. Kennwörter müssen aus 1 bis 64 Zeichen bestehen. Für das Kennwort sind nur die druckbaren Zeichen des ASCII-Codes (Code 32 bis 126), also Buchstaben, Ziffern, Satzzeichen sowie einige Sonderzeichen zulässig.**Repeat password (Kennwort wiederholen):** Geben Sie das gleiche Kennwort erneut ein.**Privileges (Rechte):**

- **Administrator:** Hat uneingeschränkten Zugriff auf alle Einstellungen. Administratoren können auch Konten hinzufügen, aktualisieren, bearbeiten und entfernen.
- **Operator (Bediener):** Hat Zugriff auf alle Einstellungen, außer:
 - Alle Systemeinstellungen.
 - Apps werden hinzugefügt.
- **Betrachter:** Hat Zugriff auf:
 - Videostreams ansehen und Momentaufnahmen erstellen.
 - Aufzeichnungen ansehen und exportieren.
 - Schwenken, Neigen und Zoomen; mit PTZ-Benutzerzugriff.



Das Kontextmenü enthält:**Update account (Konto aktualisieren):** Bearbeiten Sie die Eigenschaften des Kontos.**Delete account (Konto löschen):** Das Konto löschen. Das Root-Konto kann nicht gelöscht werden.

Anonymous access (Anonymer Zugriff)

Allow anonymous viewing (Anonymes Betrachten zulassen): Schalten Sie diese Option ein, damit Personen als Betrachter auf das Gerät zugreifen können, ohne sich mit einem Benutzerkonto anmelden zu müssen.**Allow anonymous PTZ operating (Anonyme**

PTZ-Benutzung zulassen)  : Schalten Sie diese Option ein, damit anonyme Benutzer das Bild schwenken, neigen und zoomen können.

SSH accounts (SSH-Konten)



Add SSH account (SSH-Konto hinzufügen): Klicken Sie, um ein neues SSH-Konto hinzuzufügen.

- **Restrict root access (Root-Zugriff beschränken):** Aktivieren, um die Funktion einzuschränken, die einen Root-Zugriff erfordert.
- **Enable SSH (SSH aktivieren):** Den SSH-Dienst aktivieren.

Account (Konto): Geben Sie einen eindeutigen Kontonamen ein.**Neues Kennwort:** Geben Sie ein Kennwort für das Konto ein. Kennwörter müssen aus 1 bis 64 Zeichen bestehen. Für das Kennwort sind nur die druckbaren Zeichen des ASCII-Codes (Code 32 bis 126), also Buchstaben, Ziffern, Satzzeichen sowie einige Sonderzeichen zulässig.**Repeat password (Kennwort wiederholen):**

Geben Sie das gleiche Kennwort erneut ein.**Comment (Anmerkung):** Geben Sie eine Anmerkung ein (optional).  Das Kontextmenü enthält:**Update SSH account (SSH-Konto aktualisieren):** Bearbeiten Sie die Eigenschaften des Kontos.**Delete SSH account (SSH-Konto löschen):** Das Konto löschen. Das Root-Konto kann nicht gelöscht werden.

AXIS A8207-VE Mk II Network Video Door Station

Die Weboberfläche

Virtual host (Virtueller Host)

+ **Add virtual host (Virtuellen Host hinzufügen):** Klicken Sie hier, um einen neuen virtuellen Host hinzuzufügen. **Enabled (Aktiviert):** Wählen Sie diese Option aus, um diesen virtuellen Host zu verwenden. **Server name (Servername):** Geben Sie den Namen des Servers ein. Verwenden Sie nur die Zahlen 0 bis 9, die Buchstaben A bis Z und den Bindestrich (-). **Port:** Geben Sie den Port ein, mit dem der Server verbunden ist. **Type (Typ):** Wählen Sie den Typ der Authentifizierung aus. Sie haben die Wahl zwischen Basic, Digest und Open ID. **Das Kontextmenü enthält:**

- **Update (Aktualisieren):** Aktualisieren Sie den virtuellen Host.
- **Delete (Löschen):** Löschen Sie den virtuellen Host.

Disabled (Deaktiviert): Der Server ist deaktiviert.

OpenID Configuration (OpenID-Konfiguration)

Wichtig

Wenn Sie sich nicht mit OpenID anmelden können, verwenden Sie die Digest- oder Basic-Anmeldeinformationen, die Sie bei der Konfiguration von OpenID für die Anmeldung verwendet haben.

Client ID (Client-ID): Geben Sie den OpenID-Benutzernamen ein. **Outgoing Proxy (Ausgehender Proxy):** Geben Sie die Proxyadresse für die OpenID-Verbindung ein, um einen Proxyserver zu verwenden. **Admin claim (Administratorenforderung):** Geben Sie einen Wert für die Administratorrolle ein. **Provider URL (Provider-URL):** Geben Sie den Weblink für die API-Endpunkt-Authentifizierung ein. Das Format muss `https://[insert URL]/well-known/openid-configuration` sein. **Operator claim (Bedienerforderung):** Geben Sie einen Wert für die Bedienerrolle ein. **Require claim (Anspruchanforderung):** Geben Sie die Daten ein, die im Token enthalten sein sollen. **Viewer claim (Betrachterforderung):** Geben Sie den Wert für die Betrachterrolle ein. **Remote user (Remote-Benutzer):** Geben Sie einen Wert zur Identifizierung von Remote-Benutzern ein. Dadurch wird der aktuelle Benutzer auf der Weboberfläche des Geräts angezeigt. **Scopes (Bereiche):** Optionale Bereiche, die Teil des Tokens sein können. **Client secret (Kundengeheimnis):** Geben Sie das OpenID-Kennwort ein. **Save (Speichern):** Klicken Sie hier, um die OpenID-Werte zu speichern. **Enable OpenID (OpenID aktivieren):** Die aktuelle Verbindung aktivieren und die Geräteauthentifizierung über die Provider-URL zulassen.

Ereignisse

Regeln

Eine Aktionsregel definiert die Bedingungen, die dazu führen, dass das Produkt eine Aktion ausführt. Die Liste zeigt alle derzeit konfigurierten Regeln für das Produkt.

Hinweis

Es können bis zu 256 Aktionsregeln erstellt werden.

+ **Add a rule (Regel hinzufügen):** Eine Regel erstellen. **Name:** Geben Sie einen Namen für die Regel ein. **Wait between actions (Wartezeit zwischen den Aktionen):** Geben Sie die an (hh:mm:ss), wie viel Zeit mindestens zwischen Regelaktivierungen vergehen muss. Es ist sinnvoll, wenn die Regel beispielsweise durch Tag-Nacht-Bedingungen aktiviert wird, damit nicht aufgrund kleiner Änderungen der Lichtverhältnisse bei Sonnenaufgang und -untergang die Regel wiederholt aktiviert wird. **Bedingung:** Wählen Sie eine Bedingung aus der Liste aus. Eine Bedingung muss erfüllt sein, damit das Gerät eine Aktion ausführen kann. Wenn mehrere Bedingungen festgelegt wurden, müssen zum Auslösen der Aktion alle dieser Bedingungen erfüllt sein. Informationen zu bestimmten Bedingungen finden Sie unterunter *Erste Schritte mit Regeln für Ereignisse*. **Die Bedingung als Auslöser verwenden:** Wählen Sie diese Option aus, damit diese erste Bedingung nur als Startauslöser funktioniert. Damit bleibt die Regel nach Aktivierung so lange aktiv, wie alle anderen Bedingungen erfüllt sind, unabhängig vom Status der ersten Bedingung. Wenn diese Option nicht ausgewählt ist, ist die Regel nur aktiv, wenn alle Bedingungen erfüllt sind. **Bedingungen umkehren:** Wählen Sie diese Option, wenn die Bedingung im Gegensatz zu Ihrer Auswahl stehen soll. **+** **Bedingung hinzufügen:** Klicken Sie darauf, um eine zusätzliche Bedingung hinzuzufügen. **Aktion:** Wählen Sie eine Aktion aus der Liste aus und geben Sie die erforderlichen Informationen ein. Informationen zu bestimmten Aktionen finden Sie unter *Erste Schritte mit Regeln für Ereignisse*.

Empfänger

AXIS A8207-VE Mk II Network Video Door Station

Die Weboberfläche

Sie können Ihr Gerät so einrichten, dass Empfänger über Ereignisse benachrichtigt oder Dateien gesendet werden. Die nachfolgende Liste führt alle aktuell im Produkt konfigurierten Empfänger sowie Informationen zur Konfigurierung aus.

Hinweis

Sie können bis zu 20 Empfänger erstellen.



Einen Empfänger hinzufügen: Klicken Sie darauf, um einen Empfänger hinzuzufügen. **Name:** Geben Sie den Name des Empfängers ein. **Typ:** Aus der Liste auswählen:

- **FTP** 
 - **Host:** Geben Sie die IP-Adresse oder den Host-Namen des Servers ein. Stellen Sie bei der Eingabe eines Host-Namen sicher, dass unter **System > Network > IPv4 und IPv6** ein DNS-Server angegeben ist.
 - **Port:** Geben Sie die vom FTP-Server verwendete Portnummer ein. Der Standardport ist 21.
 - **Ordner:** Geben Sie den Pfad zum Verzeichnis ein, in dem Sie die Dateien speichern möchten. Wenn dieses Verzeichnis noch nicht auf dem FTP-Server eingerichtet ist, erhalten Sie beim Hochladen eine Fehlermeldung.
 - **Benutzername:** Geben Sie den Benutzernamen für die Anmeldung ein.
 - **Kennwort:** Geben Sie das Kennwort für die Anmeldung ein.
 - **Temporären Dateinamen verwenden:** Wählen Sie diese Option zum Hochladen von Dateien mit temporären, automatisch generierten Dateinamen. Die Dateien werden nach abgeschlossenem Hochladen in die gewünschten Namen umbenannt. Wenn das Hochladen abgebrochen oder unterbrochen wird, werden keine beschädigten Dateien eingestellt. Jedoch werden möglicherweise die temporären Dateien eingestellt. So wissen Sie, dass alle Dateien mit dem gewünschten Namen in Ordnung sind.
 - **Use passive FTP (Passives FTP verwenden):** Normalerweise fordert das Produkt den FTP-Zielsever zum Öffnen der Datenverbindung auf. Normalerweise initiiert das Gerät die FTP-Steuerung und die Datenverbindungen zum Zielsever. Dies ist in der Regel erforderlich, wenn zwischen dem Gerät und dem FTP-Zielsever eine Firewall eingerichtet ist.
- **HTTP**
 - **URL:** Geben Sie die Netzwerkadresse des HTTP-Servers und das Skript, das die Anforderung bearbeiten wird, ein. Beispielsweise `http://192.168.254.10/cgi-bin/notify.cgi`.
 - **Username (Benutzername):** Geben Sie den Benutzernamen für die Anmeldung ein.
 - **Kennwort:** Geben Sie das Kennwort für die Anmeldung ein.
 - **Proxy:** Aktivieren Sie diese Option und geben Sie die erforderlichen Informationen ein, wenn für die Verbindung mit dem HTTP-Server ein Proxyserver erforderlich ist.
- **HTTPS**
 - **URL:** Geben Sie die Netzwerkadresse des HTTPS-Servers und das Skript, das die Anforderung bearbeiten wird, ein. Beispielsweise `https://192.168.254.10/cgi-bin/notify.cgi`.
 - **Validate server certificate (Server-Zertifikat validieren):** Wählen Sie diese Option, um zu überprüfen, ob das Zertifikat von HTTPS-Server erstellt wurde.
 - **Benutzername:** Geben Sie den Benutzernamen für die Anmeldung ein.
 - **Kennwort:** Geben Sie das Kennwort für die Anmeldung ein.
 - **Proxy:** Schalten Sie diese Option ein und geben Sie die erforderlichen Informationen ein, wenn für die Verbindung mit dem HTTPS-Server ein Proxyserver erforderlich ist.
- **Network storage (Netzwerk-Speicher)** 

Darüber können Sie einen Netzwerk-Speicher wie NAS (Network Attached Storage) hinzufügen und als Empfänger für zu speichernde Dateien verwenden. Die Dateien werden im Format Matroska (MKV) gespeichert.

 - **Host:** Geben Sie die IP-Adresse oder den Host-Namen der Netzwerk-Speicher ein.
 - **Freigabe:** Geben Sie den Namen der Freigabe auf dem Host ein.
 - **Ordner:** Geben Sie den Pfad zum Verzeichnis ein, in dem Sie die Dateien speichern möchten.
 - **Benutzername:** Geben Sie den Benutzernamen für die Anmeldung ein.
 - **Kennwort:** Geben Sie das Kennwort für die Anmeldung ein.
- **SFTP** 
 - **Host:** Geben Sie die IP-Adresse oder den Host-Namen des Servers ein. Stellen Sie bei der Eingabe eines Host-Namen sicher, dass unter **System > Network > IPv4 und IPv6** ein DNS-Server angegeben ist.
 - **Port:** Geben Sie die vom SFTP-Server verwendete Portnummer ein. Der Standardport ist 22.
 - **Ordner:** Geben Sie den Pfad zum Verzeichnis ein, in dem Sie die Dateien speichern möchten. Wenn dieses Verzeichnis noch nicht auf dem SFTP-Server eingerichtet ist, erhalten Sie beim Hochladen eine Fehlermeldung.
 - **Benutzername:** Geben Sie den Benutzernamen für die Anmeldung ein.

AXIS A8207-VE Mk II Network Video Door Station

Die Weboberfläche

- **Kennwort:** Geben Sie das Kennwort für die Anmeldung ein.
 - **Öffentlicher SSH-Host-Schlüsseltyp (MD5):** Geben Sie der Fingerabdruck des öffentlichen Schlüssels des Zielrechners (eine hexadezimale Zeichenfolge mit 32 Stellen) ein. Der SFTP-Client unterstützt SFTP-Server, die SSH-2 mit RSA-, DSA-, ECDSA- und ED25519-Schlüsseltypen verwenden. RSA ist die bevorzugte Methode während der Aushandlung, gefolgt von ECDSA, ED25519 und DSA. Stellen Sie sicher, dass Sie den richtigen MD5-Hostschlüssel eingeben, der von Ihrem SFTP-Server verwendet wird. Das Axis Gerät unterstützt zwar sowohl MD5- als auch SHA-256-Hash-Schlüssel, wir empfehlen jedoch die Verwendung von SHA-256, da es sicherer ist als MD5. Weitere Informationen zur Konfiguration eines SFTP-Servers mit einem Axis Gerät finden Sie im *AXIS OS-Portal*.
 - **Öffentlicher SSH-Host-Schlüsseltyp (SHA256):** Geben Sie der Fingerabdruck des öffentlichen Schlüssels des Zielrechners (eine Base64-kodierte Zeichenfolge mit 43 Stellen) ein. Der SFTP-Client unterstützt SFTP-Server, die SSH-2 mit RSA-, DSA-, ECDSA- und ED25519-Schlüsseltypen verwenden. RSA ist die bevorzugte Methode während der Aushandlung, gefolgt von ECDSA, ED25519 und DSA. Stellen Sie sicher, dass Sie den richtigen MD5-Hostschlüssel eingeben, der von Ihrem SFTP-Server verwendet wird. Das Axis Gerät unterstützt zwar sowohl MD5- als auch SHA-256-Hash-Schlüssel, wir empfehlen jedoch die Verwendung von SHA-256, da es sicherer ist als MD5. Weitere Informationen zur Konfiguration eines SFTP-Servers mit einem Axis Gerät finden Sie im *AXIS OS-Portal*.
 - **Temporären Dateinamen verwenden:** Wählen Sie diese Option zum Hochladen von Dateien mit temporären, automatisch generierten Dateinamen. Die Dateien werden nach abgeschlossenem Hochladen in die gewünschten Namen umbenannt. Wenn das Hochladen abgebrochen oder unterbrochen wird, werden keine beschädigten Dateien eingestellt. Jedoch werden möglicherweise die temporären Dateien eingestellt. So wissen Sie, dass alle Dateien mit dem gewünschten Namen in Ordnung sind.
-  :
- **SIP or VMS (SIP oder VMS)**
 - SIP: Wählen Sie diese Option, um einen SIP-Anruf zu starten.
 - VMS: Wählen Sie diese Option, um einen VMS-Anruf zu starten.
 - **From SIP account (Von SIP-Konto):** Wählen Sie die entsprechende Option aus der Liste aus.
 - **To SIP address (An SIP-Adresse):** Geben Sie die entsprechende SIP-Adresse ein.
 - **Test:** Klicken Sie hier, um die Anrufeinstellungen auf einwandfreie Funktion zu überprüfen.
 - **E-Mail**
 - **Send email to (E-Mail senden an):** Geben Sie die gewünschte(n) E-Mail-Versandadresse(n) ein. Trennen Sie mehrere Adressen jeweils mit einem Komma.
 - **E-Mail senden von:** Geben Sie die als Absender anzuzeigende E-Mail-Adresse ein.
 - **Benutzername:** Geben Sie den Benutzernamen für den Mailserver ein. Lassen dieses Feld frei, wenn der Mailserver keine Authentifizierung erfordert.
 - **Kennwort:** Geben Sie das Kennwort für den Mailserver ein. Lassen dieses Feld frei, wenn der Mailserver keine Authentifizierung erfordert.
 - **Email server (SMTP) (E-Mail-Server (SMTP)):** Geben Sie den Namen des SMTP-Servers ein. Zum Beispiel smtp.gmail.com, smtp.mail.yahoo.com.
 - **Port:** Geben Sie die Portnummer des SMTP-Servers ein. Zulässig sind Werte zwischen 0 und 65535. Der Standardport ist 587.
 - **Verschlüsselung:** Um die Verschlüsselung zu verwenden, wählen Sie SSL bzw. TLS.
 - **Server-Zertifikate validieren:** Wenn Sie eine Verschlüsselung verwenden, wählen Sie diese Option zur Überprüfung der Identität des Geräts. Das Zertifikat kann ein eigensigniertes oder ein von einer Zertifizierungsstelle (Certificate Authority, CA) ausgestelltes Zertifikat sein.
 - **POP authentication (POP-Authentifizierung):** Schalten Sie diese Option ein, um den Namen des POP-Servers einzugeben, z.B. pop.gmail.com.

Hinweis

Einige E-Mail-Dienste verwenden Sicherheitsfilter, die verhindern, dass Benutzer eine große Anzahl von Anhängen erhalten oder anzeigen, geplante E-Mails erhalten usw. Prüfen Sie die Sicherheitsrichtlinien des E-Mail-Anbieters, damit Ihr E-Mail-Konto nicht gesperrt wird oder die erwarteten E-Mails nicht verloren gehen.

- **TCP**
 - **Host:** Geben Sie die IP-Adresse oder den Host-Namen des Servers ein. Stellen Sie bei der Eingabe eines Host-Namen sicher, dass unter **System > Network > IPv4 und IPv6** ein DNS-Server angegeben ist.
 - **Port:** Geben Sie die Nummer des für den Zugriff auf den Server verwendeten Ports ein.

Test: Klicken auf dieses Feld, um die Einrichtung zu überprüfen.  Das Kontextmenü enthält:**Empfänger anzeigen:** Klicken Sie darauf, um die Details zu den Empfängern zu sehen.**Empfänger kopieren:** Klicken Sie darauf, um einen Empfänger zu kopieren. Beim Kopieren können Sie Änderungen am neuen Empfänger vornehmen.**Empfänger löschen:** Klicken Sie darauf, um den Empfänger dauerhaft zu löschen.

AXIS A8207-VE Mk II Network Video Door Station

Die Weboberfläche

Zeitpläne

Zeitpläne und Impulse können als Bedingungen in Regeln verwendet werden. Die nachfolgende Liste führt alle aktuell im Produkt konfigurierten Zeitpläne und Impulse sowie Informationen zur Konfigurierung auf.  Zeitplan hinzufügen: Klicken Sie hier, um einen Zeitplan oder Impuls zu erstellen.

Manuelle Auslöser

Mithilfe des manuellen Auslösers können Sie eine Regel manuell auslösen. Der manuelle Auslöser kann beispielsweise zum Validieren von Aktionen beim Installieren und Konfigurieren des Produkts verwendet werden.

MQTT

MQTT (Message Queuing Telemetry Transport) ist ein Standardprotokoll für das Internet der Dinge (IoT). Es wurde für eine vereinfachte IoT-Integration entwickelt und wird in einer Vielzahl von Branchen zum Anschließen von Remote-Geräten mit kleinem Code-Footprint und minimaler Netzwerkbandbreite verwendet. Der MQTT-Client in der Axis Gerätesoftware kann die Integration der im Gerät erzeugten Daten und Ereignisse in Systeme vereinfachen, bei denen es sich nicht um Video Management Software (VMS) handelt. Richten Sie das Gerät als MQTT-Client ein. Die MQTT-Kommunikation basiert auf zwei Entitäten, den Clients und dem Broker. Die Clients können Nachrichten senden und empfangen. Der Broker ist für das Routing von Nachrichten zwischen den Clients zuständig. Weitere Informationen zu MQTT finden Sie im *AXIS OS Portal*.

ALPN

Bei ALPN handelt es sich um eine TLS/SSL-Erweiterung, mit der während der Handshake-Phase der Verbindung zwischen Client und Server ein Anwendungsprotokoll ausgewählt werden kann. Auf diese Weise können Sie den MQTT-Datenverkehr über denselben Port zulassen, der für andere Protokolle wie HTTP verwendet wird. In einigen Fällen ist möglicherweise kein dedizierter Port für die MQTT-Kommunikation vorhanden. Eine Lösung besteht in diesem Fall in der Verwendung von ALPN, um die von den Firewalls erlaubte Verwendung von MQTT als Anwendungsprotokoll auf einem Standardport zu nutzen.

MQTT-Client

Verbinden: Aktivieren oder deaktivieren Sie den MQTT-Client. **Status:** Zeigt den aktuellen Status des MQTT-Clients an. **BrokerHost:** Geben Sie den Host-Namen oder die Adresse des MQTT-Servers ein. **Protokoll:** Wählen Sie das zu verwendende Protokoll aus. **Port:** Geben Sie die Portnummer ein.

- 1883 ist der Standardwert für MQTT über TCP
- 8883 ist der Standardwert für MQTT über SSL
- 80 ist der Standardwert für MQTT über WebSocket
- 443 ist der Standardwert für MQTT über WebSocket Secure

ALPN protocol (ALPN-Protokoll): Geben Sie den Namen des ALPN-Protokolls ein, den Sie vom Anbieter Ihres MQTT-Brokers erhalten haben. Dies gilt nur für MQTT über SSL und MQTT über WebSocket Secure. **Username (Benutzername):** Geben Sie den Benutzernamen ein, den der Client für den Zugriff auf den Server verwenden soll. **Kennwort:** Geben Sie ein Kennwort für den Benutzernamen ein. **Client-ID:** Geben Sie eine Client-ID ein. Die Client-ID wird an den Server gesendet, wenn der Client eine Verbindung herstellt. **Sitzung bereinigen:** Steuert das Verhalten bei Verbindung und Trennungszeit. Wenn diese Option ausgewählt ist, werden die Statusinformationen beim Verbinden und Trennen verworfen. **HTTP proxy (HTTP-Proxy):** eine URL mit einer maximalen Länge von 255 Byte. Sie können das Feld leer lassen, wenn Sie keinen HTTP-Proxy verwenden möchten. **HTTPS proxy (HTTPS-Proxy):** eine URL mit einer maximalen Länge von 255 Byte. Sie können das Feld leer lassen, wenn Sie keinen HTTPS-Proxy verwenden möchten. **Keep alive interval (Keep-Alive-Intervall):** Hiermit kann der Client erkennen, wann der Server nicht mehr verfügbar ist, ohne auf das lange TCP/IP-Timeout warten zu müssen. **Timeout (Zeitüberschreitung):** Das Zeitintervall in Sekunden, in dem eine Verbindung hergestellt werden kann. Standardwert: 60 **Device topic prefix (Themenpräfix des Geräts):** Wird in den Standardwerten für das Thema in der Verbindungsnachricht und der LWT-Nachricht auf der Registrierkarte MQTT Client und in den Veröffentlichungsbedingungen auf der Registrierkarte MQTT-Veröffentlichung verwendet. **Reconnect automatically (Automatisch wiederverbinden):** Gibt an, ob der Client nach einer Trennung der Verbindung die Verbindung automatisch wiederherstellen soll. **Nachricht zum Verbindungsaufbau:** Gibt an, ob eine Nachricht gesendet werden soll, wenn eine Verbindung hergestellt wird. **Nachricht senden:** Aktivieren Sie diese Option, damit Nachrichten versendet werden. **Standardeinstellung verwenden:** Deaktivieren Sie diese Option, um Ihre eigene Standardnachricht eingeben zu können. **Thema:** Geben Sie das Thema der Standardnachricht ein. **Nutzlast:** Geben Sie den Inhalt der Standardnachricht ein. **Beibehalten:** Wählen Sie diese Option, um den Status des Clients bei diesem Thema beizubehalten. **QoS:** Ändern Sie die QoS-Ebene für den Paketfluss. **Nachricht zum letzten**

AXIS A8207-VE Mk II Network Video Door Station

Die Weboberfläche

Willen und Testament Mit Letzter Wille und Testament (LWT) kann ein Client bei der Verbindung mit dem Broker ein Testament zusammen mit seinen Zugangsdaten bereitstellen. Wenn der Kunde die Verbindung irgendwann später auf nicht ordnungsgemäße Weise abbricht (vielleicht weil seine Stromquelle deaktiviert ist), kann er den Broker eine Nachricht an andere Kunden übermitteln lassen. Diese LWT-Nachricht hat dieselbe Form wie eine normale Nachricht und wird über die gleiche Mechanik geroutet.
Nachricht senden: Aktivieren Sie diese Option, damit Nachrichten versendet werden.
Standardeinstellung verwenden: Deaktivieren Sie diese Option, um Ihre eigene Standardnachricht eingeben zu können.
Thema: Geben Sie das Thema der Standardnachricht ein.
Nutzlast: Geben Sie den Inhalt der Standardnachricht ein.
Beibehalten: Wählen Sie diese Option, um den Status des Clients bei diesem Thema beizubehalten.
QoS: Ändern Sie die QoS-Ebene für den Paketfluss.

MQTT publication (MQTT-Veröffentlichung)

Use default topic prefix (Standard-Themenpräfix verwenden): Wählen Sie diese Option aus, um das Standard-Themenpräfix zu verwenden, das im Gerätethemenpräfix auf der Registerkarte **MQTT client (MQTT-Client)** definiert ist.
Include topic name (Themanamen einschließen): Wählen Sie diese Option aus, um das Thema einzufügen, das die Bedingung des MQTT-Themas beschreibt.
Include topic namespaces (Themen-Namespace einschließen): Wählen Sie diese Option aus, um Namespaces des ONVIF-Themas im MQTT-Thema einzuschließen.
Include serial number (Seriennummer hinzufügen): Wählen Sie diese Option, um die Seriennummer des Geräts in die MQTT-Nutzlast einzuschließen.
+ Bedingung hinzufügen: Klicken Sie darauf, um eine Bedingung hinzuzufügen.
Retain (Beibehalten): Definiert, welche MQTT-Meldungen als beibehalten gesendet werden.

- **None (Keine):** Alle Melden werden als nicht beibehalten gesendet.
- **Property (Eigenschaft):** Es werden nur statusbehaftete Meldungen als beibehalten gesendet.
- **Alle:** Es werden nur statuslose Meldungen als beibehalten gesendet.

QoS: Wählen Sie die gewünschte Stufe für die MQTT-Veröffentlichung.

MQTT-Abonnements

+ Abonnement hinzufügen: Klicken Sie darauf, um ein neues MQTT-Abonnement hinzuzufügen.
Abonnementfilter: Geben Sie das MQTT-Thema ein, das Sie abonnieren möchten.
Themenpräfix des Geräts verwenden: Fügen Sie den Abonnementfilter als Präfix zum MQTT-Thema hinzu.
Abonnementart:

- **Statuslos:** Wählen Sie diese Option, um MQTT-Meldungen in statuslose Meldungen zu konvertieren.
- **Statusbehaftet:** Wählen Sie diese Option, um MQTT-Meldungen in Bedingungen zu konvertieren. Als Status wird der Nutzlast verwendet.

QoS: Wählen Sie die gewünschte Stufe für das MQTT-Abonnement.

MQTT-Overlays

Hinweis

Stellen Sie eine Verbindung mit einem MQTT-Broker her, bevor Sie MQTT-Overlay-Modifikatoren hinzufügen.

+ Overlay-Modifikator hinzufügen: Klicken Sie hier, um einen neuen Overlay-Modifikator hinzuzufügen.
Themenfilter: Fügen Sie das MQTT-Thema hinzu, das die Daten enthält, die im Overlay angezeigt werden sollen.
Datenfeld: Geben Sie den Schlüssel für die Nutzdaten der Nachricht an, die Sie im Overlay anzeigen möchten, vorausgesetzt, die Nachricht ist im JSON-Format.
Modifikator: Verwenden Sie beim Erstellen des Overlays den resultierenden Modifikator.

- Modifikatoren, die mit **#XMP** beginnen, zeigen alle vom Thema empfangenen Daten an.
- Modifikatoren, die mit **#XMD** beginnen, zeigen die im Datenfeld angegebenen Daten an.

Speicher

Network storage (Netzwerk-Speicher)

AXIS A8207-VE Mk II Network Video Door Station

Die Weboberfläche

Ignore (Ignorieren): Schalten Sie diese Option ein, um den Netzwerk-Speicher zu ignorieren. **Add network storage (Netzwerk-Speicher hinzufügen):** Klicken Sie auf diese Option zum Hinzufügen einer Netzwerk-Freigabe, auf der Sie Aufzeichnungen speichern können.

- **Adresse:** Geben Sie die IP-Adresse des Host-Servers, in der Regel ein NAS (Network Attached Storage), ein. Wir empfehlen Ihnen, den Host für eine statische IP-Adresse zu konfigurieren (nicht DHCP, da sich eine dynamische IP-Adresse ändern kann) oder DNS zu verwenden. Namen des Typs Windows SMB/CIFS werden nicht unterstützt.
- **Netzwerk-Freigabe:** Geben Sie den Namen des freigegebenen Speicherorts auf dem Host-Server ein. Mehrere Axis Geräte können dieselbe Netzwerk-Freigabe verwenden, da jedes Gerät einen eigenen Ordner erhält.
- **User (Benutzer):** Wenn der Server eine Anmeldung erfordert, geben Sie den Benutzernamen ein. Zur Anmeldung an einem bestimmten Domainserver geben Sie `DOMAIN\Benutzername` ein.
- **Kennwort:** Wenn der Server eine Anmeldung erfordert, geben Sie das Kennwort ein.
- **SMB-Version:** Wählen Sie die SMB-Speicherprotokollversion für die Verbindung mit dem NAS. Wenn Sie **Auto** wählen, versucht das Gerät, eine der sicheren Versionen SMB zu installieren: 3.02, 3.0 oder 2.1. Wählen Sie 1.0 oder 2.0 zur Herstellung einer Verbindung zu älteren NAS, die höhere Versionen nicht unterstützen. Weitere Informationen zur SMB-Unterstützung in Axis Geräten finden Sie *hier*.
- **Add share without testing (Freigabe ohne Test hinzufügen):** Wählen Sie diese Option, um die Netzwerk-Freigabe hinzuzufügen, auch wenn während des Verbindungstests ein Fehler erkannt wurde. Bei dem Fehler kann es beispielsweise sein, dass Sie kein Kennwort eingegeben haben, obwohl für den Server ein Kennwort erforderlich ist.

Remove network storage (Netzwerk-Speicher entfernen): Klicken Sie hier, um die Verbindung zur Netzwerk-Freigabe zu trennen, zu lösen oder zu entfernen. Dadurch werden alle Einstellungen für die Netzwerk-Freigabe entfernt. **Unbind (Lösen):** Klicken Sie hier, um die Netzwerk-Freigabe zu lösen und zu trennen.

Bind (Zuweisen): Klicken Sie hier, um die Netzwerk-Freigabe zuzuweisen und zu verbinden. **Unmount (Trennen):** Klicken Sie hier, um die Netzwerk-Freigabe zu trennen.

Mount (Einbinden): Klicken Sie hier, um die Netzwerk-Freigabe einzubinden. **Write protect (Schreibschutz):** Schalten Sie diese Option ein, damit nicht mehr auf die Netzwerk-Freigabe geschrieben werden kann und bestehende Aufzeichnungen nicht entfernt werden können. Eine schreibgeschützte Netzwerk-Freigabe kann nicht formatiert werden. **Retention time (Aufbewahrungszeit):** Wählen Sie, wie lange die Aufzeichnungen gespeichert werden, um die Datenmenge alter Aufzeichnungen zu begrenzen oder die Bestimmungen zur Datenspeicherung einzuhalten. Wenn der Netzwerk-Speicher voll ist, werden alte Aufzeichnungen gelöscht, bevor der ausgewählte Zeitraum verstrichen ist. **Tools (Werkzeuge)**

- **Test connection (Verbindung testen):** Prüfen Sie die Verbindung zur Netzwerk-Freigabe.
- **Format (Formatieren):** Formatieren Sie die Netzwerk-Freigabe, wenn zum Beispiel schnell alle Daten gelöscht werden müssen. CIFS ist die verfügbare Dateisystemoption.

Use tool (Werkzeug verwenden): Klicken Sie hier, um das ausgewählte Werkzeug zu aktivieren.

Integrierter Speicher

Wichtig

Gefahr von Datenverlust und Beschädigung von Aufzeichnungen. Die SD-Karte darf nicht entfernt werden, während das Gerät in Betrieb ist. Trennen Sie die SD-Karte, bevor Sie sie entfernen.

Trennen: Klicken Sie hier, um die SD-Karte sicher zu entfernen. **Schreibschutz:** Aktivieren Sie diese Option, damit nicht mehr auf die SD-Karte geschrieben werden kann und bestehende Aufzeichnungen nicht entfernt werden können. Eine schreibgeschützte SD-Karte kann nicht formatiert werden. **Automatisch formatieren:** Aktivieren Sie diese Option, um eine neu eingesetzte SD-Karte automatisch zu formatieren. Sie wird als Dateisystem ext4 formatiert. **Ignorieren:** Aktivieren Sie diese Option, um die Speicherung der Aufzeichnungen auf der SD-Karte zu beenden. Wenn Sie die SD-Karte ignorieren, erkennt das Gerät nicht mehr, dass die Karte vorhanden ist. Diese Einstellung steht nur Administratoren zur Verfügung. **Aufbewahrungszeit:** Wählen Sie, wie lange die Aufzeichnungen gespeichert werden, um die Datenmenge alter Aufzeichnungen zu begrenzen oder die Bestimmungen zur Datenspeicherung einzuhalten. Wenn die SD-Karte voll ist, werden alte Aufzeichnungen gelöscht, bevor der ausgewählte Zeitraum verstrichen ist. **Werkzeuge**

- **Überprüfen:** Überprüfen Sie die SD-Speicherkarte auf Fehler. Diese Funktion steht nur für das Dateisystem ext4 zur Verfügung.
- **Reparieren:** Beheben Sie Fehler im Dateisystem ext4. Um eine SD-Karte mit dem Dateisystem VFAT zu reparieren, werfen Sie die SD-Karte aus und setzen Sie sie einem Computer ein, bevor Sie die Festplattenreparatur durchführen.
- **Format (Formatieren):** Formatieren Sie die SD-Karte zum Beispiel, wenn das Dateisystem geändert oder alle Daten schnell gelöscht werden sollen. Die beiden verfügbaren Dateisysteme sind VFAT und ext4. Das Format ext4 wird wegen des Schutzes vor Datenverlust beim Auswerfen der Karte oder bei plötzlichem Stromausfall empfohlen. Sie benötigen jedoch einen externen ext4-Treiber oder eine Anwendung, um unter Windows® auf das Dateisystem zuzugreifen.

AXIS A8207-VE Mk II Network Video Door Station

Die Weboberfläche

- **Encrypt (Verschlüsseln):** Verwenden Sie dieses Tool, um die SD-Karte zu formatieren und die Verschlüsselung zu aktivieren. **Encrypt (Verschlüsseln)** löscht alle auf der SD-Karte gespeicherten Daten. Nach der Verschlüsselung mit **Encrypt** sind alle auf der SD-Karte gespeicherten Daten mittels Verschlüsselung geschützt.
 - **Decrypt (Entschlüsseln):** Verwenden Sie dieses Tool, um die SD-Karte ohne Verschlüsselung zu formatieren. **Decrypt (Entschlüsseln)** löscht alle auf der SD-Karte gespeicherten Daten. Nach der Entschlüsselung mit **Decrypt** sind die auf der SD-Karte gespeicherten Daten nicht mehr mittels Verschlüsselung geschützt.
 - **Change password (Kennwort ändern):** Ändern Sie das zum Verschlüsseln der SD-Karte erforderliche Kennwort.
- Use tool (Werkzeug verwenden): Klicken Sie hier, um das ausgewählte Werkzeug zu aktivieren.

Wear trigger (Auslöser für Abnutzung): Legen Sie einen Wert für die Abnutzung der SD-Speicherkarte fest, bei dem eine Aktion ausgelöst werden soll. Der Abnutzungsgrad reicht von 0 bis 200 %. Eine neue SD-Karte, die noch nie verwendet wurde, hat einen Abnutzungsgrad von 0 %. Ein Abnutzungsgrad von 100 % gibt an, dass die zu erwartende Lebensdauer der SD-Karte bald abläuft. Wenn der Abnutzungsgrad 200% erreicht, besteht ein hohes Risiko einer Fehlfunktion der SD-Karte. Wir empfehlen Ihnen, den Auslöser für Abnutzung auf 80 bis 90 % einzustellen. Dadurch haben Sie Zeit, Aufzeichnungen herunterzuladen und die SD-Karte zu ersetzen, bevor sie möglicherweise abgenutzt ist. Mit dem Auslöser für Abnutzung können Sie ein Ereignis einrichten und sich eine Benachrichtigung senden lassen, wenn der Abnutzungsgrad den von Ihnen festgelegten Wert erreicht.

Videostreamprofile

Ein Videostreamprofil besteht aus einer Gruppe von Einstellungen, die sich auf den Videostream auswirken. Videostreamprofile können in verschiedenen Situationen verwendet werden, z. B. bei der Erstellung von Ereignissen und der Verwendung von Aufzeichnungsregeln.

+ **Add stream profile (Videostreamprofil hinzufügen):** Klicken Sie, um ein neues Videostreamprofil zu erstellen. **Preview (Vorschau):** Vorschau des Videostreams mit den ausgewählten Einstellungen des Videostreamprofils. Die Vorschau wird aktualisiert, wenn Sie die Einstellungen auf der Seite ändern. Wenn Ihr Gerät unterschiedliche Sichtbereiche hat, können Sie den Sichtbereich in der Dropdown-Ansicht in der unteren linken Ecke des Bildes ändern. **Name:** Fügen Sie einen Namen für Ihr Profil hinzu. **Description (Beschreibung):** Fügen Sie eine Profilbeschreibung hinzu. **Video codec (Video-Codec):** Wählen Sie den Video-Codec aus, der für das Profil verwendet werden soll. **Resolution (Auflösung):** Siehe für eine Beschreibung dieser Einstellung. **Frame rate (Bildrate):** Siehe für eine Beschreibung dieser Einstellung. **Compression (Komprimierung):** Siehe für eine Beschreibung dieser Einstellung. **Zipstream** ⓘ : Siehe für eine Beschreibung dieser Einstellung. **Optimize for storage (Für Speicherung optimieren)** ⓘ : Siehe für eine Beschreibung dieser Einstellung. **Dynamic FPS (Dynamische Bilder pro Sekunde)** ⓘ : Siehe für eine Beschreibung dieser Einstellung. **Dynamic GOP (Dynamic Group of Pictures)** ⓘ : Siehe für eine Beschreibung dieser Einstellung. **Mirror (Spiegelung)** ⓘ : Siehe für eine Beschreibung dieser Einstellung. **GOP length (GOP-Länge)** ⓘ : Siehe für eine Beschreibung dieser Einstellung. **Bitrate control (Bitratensteuerung):** Siehe für eine Beschreibung dieser Einstellung. **Include overlays (Overlays einbeziehen)** ⓘ : Wählen Sie den Typ der einzubeziehenden Overlays aus. Weitere Informationen zum Hinzufügen von Overlays finden Sie unter **.Include audio (Audio einbeziehen)** ⓘ : Siehe für eine Beschreibung dieser Einstellung.

ONVIF

ONVIF-Konten

ONVIF (Open Network Video Interface Forum) ist ein globaler Schnittstellenstandard, der Endbenutzern, Integratoren, Beratern und Herstellern die Nutzung der Vorteile von Netzwerk-Videotechnologie erleichtert. ONVIF sorgt für die Kompatibilität zwischen Produkten unterschiedlicher Hersteller, erhöhte Flexibilität, verringerte Kosten und zukunftssichere Systeme.

Beim Erstellen eines ONVIF-Kontos wird automatisch die ONVIF-Kommunikation aktiviert. Verwenden Sie den Kontonamen und das Kennwort für sämtliche ONVIF-Kommunikation mit dem Gerät. Weitere Informationen finden Sie auf den Seiten für die Axis Developer Community auf axis.com.

AXIS A8207-VE Mk II Network Video Door Station

Die Weboberfläche

+ **Add accounts (Konten hinzufügen):** Klicken Sie darauf, um ein neues ONVIF-Konto hinzuzufügen. **Account (Konto):** Geben Sie einen eindeutigen Kontonamen ein. **Neues Kennwort:** Geben Sie ein Kennwort für das Konto ein. Kennwörter müssen aus 1 bis 64 Zeichen bestehen. Für das Kennwort sind nur die druckbaren Zeichen des ASCII-Codes (Code 32 bis 126), also Buchstaben, Ziffern, Satzzeichen sowie einige Sonderzeichen zulässig. **Repeat password (Kennwort wiederholen):** Geben Sie das gleiche Kennwort erneut eingeben. **Rolle:**

- **Administrator:** Hat uneingeschränkten Zugriff auf alle Einstellungen. Administratoren können auch Konten hinzufügen, aktualisieren, bearbeiten und entfernen.
- **Operator (Bediener):** Hat Zugriff auf alle Einstellungen, außer:
 - Alle Systemeinstellungen.
 - Apps werden hinzugefügt.
- **Media account (Medienkonto):** Erlaubt nur Zugriff auf den Videostream.

⋮ Das Kontextmenü enthält: **Update account (Konto aktualisieren):** Bearbeiten Sie die Eigenschaften des Kontos. **Delete account (Konto löschen):** Das Konto löschen. Das Root-Konto kann nicht gelöscht werden.

ONVIF-Medienprofile

Ein ONVIF-Medienprofil besteht aus einem Satz von Konfigurationen, mit deren Hilfe Sie die Medienstream-Einstellungen ändern können. Sie können neue Profile mit Ihren eigenen Konfigurationen erstellen oder vorkonfigurierte Profile für eine schnelle Einrichtung verwenden.

+ **Add media profile (Medienprofil hinzufügen):** Klicken Sie darauf, um ein neues ONVIF-Medienprofil hinzuzufügen. **Profile name (Profilname):** Fügen Sie einen Namen für das Medienprofil hinzu. **Video source (Videoquelle):** Wählen Sie die Videoquelle für Ihre Konfiguration aus.

- **Select configuration (Konfiguration wählen):** Wählen Sie eine benutzerdefinierte Konfiguration aus der Liste. Die Konfigurationen in der Dropdown-Liste entsprechen den Videokanälen des Geräts, einschließlich Multiviews, Sichtbereichen und virtuellen Kanälen.

Video encoder (Video-Encoder): Wählen Sie das Videokodierungsformat für Ihre Konfiguration aus.

- **Select configuration (Konfiguration wählen):** Wählen Sie eine benutzerdefinierte Konfiguration aus der Liste aus und passen Sie die Kodierungseinstellungen an. Die Konfigurationen in der Dropdown-Liste dienen als Kennungen/Namen der Konfiguration des Video-Encoders. Wählen Sie Benutzer 0 bis 15 aus, um Ihre eigenen Einstellungen anzuwenden, oder wählen Sie einen der Standardbenutzer aus, wenn Sie vordefinierte Einstellungen für ein bestimmtes Codierungsformat verwenden möchten.

Hinweis

Aktivieren Sie Audio im Gerät, um die Option zur Auswahl einer Audioquelle und Audio-Encoder-Konfiguration zu erhalten.

Audio source (Audioquelle)  : Wählen Sie die Audioeingangsquelle für Ihre Konfiguration aus.

- **Select configuration (Konfiguration wählen):** Wählen Sie eine benutzerdefinierte Konfiguration aus der Liste aus und passen Sie die Audioeinstellungen an. Die Konfigurationen in der Dropdown-Liste entsprechen den Audioeingängen des Geräts. Wenn das Gerät über einen Audioeingang verfügt, ist es user0. Wenn das Gerät über mehrere Audioeingänge verfügt, werden weitere Benutzer in der Liste angezeigt.

Audio encoder (Audio-Encoder)  : Wählen Sie das Audiokodierungsformat für Ihre Konfiguration aus.

- **Select configuration (Konfiguration wählen):** Wählen Sie eine benutzerdefinierte Konfiguration aus der Liste aus und passen Sie die Audio-Kodierungseinstellungen an. Die Konfigurationen in der Dropdown-Liste dienen als Kennungen/Namen der Konfiguration des Audio-Encoders.

Audio decoder (Audiodecoder)  : Wählen Sie das Audiodekodierungsformat für Ihre Konfiguration aus.

- **Select configuration (Konfiguration wählen):** Wählen Sie eine benutzerdefinierte Konfiguration aus der Liste aus und passen Sie die Einstellungen an. Die Konfigurationen in der Dropdown-Liste dienen als Kennungen/Namen der Konfiguration.

Audio output (Audioausgang)  : Wählen Sie das Audioausgangsformat für Ihre Konfiguration aus.

AXIS A8207-VE Mk II Network Video Door Station

Die Weboberfläche

- **Select configuration (Konfiguration wählen):** Wählen Sie eine benutzerdefinierte Konfiguration aus der Liste aus und passen Sie die Einstellungen an. Die Konfigurationen in der Dropdown-Liste dienen als Kennungen/Namen der Konfiguration.
- Metadata (Metadaten):** Wählen Sie die Metadaten aus, die in Ihre Konfiguration einbezogen werden sollen.
- **Select configuration (Konfiguration wählen):** Wählen Sie eine benutzerdefinierte Konfiguration aus der Liste aus und passen Sie die Metadaten-Einstellungen an. Die Konfigurationen in der Dropdown-Liste dienen als Kennungen/Namen der Konfiguration der Metadaten.
- PTZ**  : Wählen Sie die PTZ-Einstellungen für Ihre Konfiguration aus.
- **Select configuration (Konfiguration wählen):** Wählen Sie eine benutzerdefinierte Konfiguration aus der Liste aus und passen Sie die PTZ-Einstellungen an. Die Konfigurationen in der Dropdown-Liste entsprechen den Videokanälen des Geräts mit PTZ-Unterstützung.
- Create (Erstellen):** Klicken Sie hier, um Ihre Einstellungen zu speichern und das Profil zu erstellen. **Cancel (Abbrechen):** Klicken Sie hier, um die Konfiguration abzubrechen und alle Einstellungen zu löschen. **profile_x:** Klicken Sie auf den Profilnamen, um das vorkonfigurierte Profil zu öffnen und zu bearbeiten.

Analytische Metadaten

Metadatenproduzenten

Listet die Apps auf, die Metadaten streamen, sowie die Kanäle, die sie verwenden.

Producer (Produzent): Die App, die Metadaten erzeugt. Unterhalb der App befindet sich eine Liste der Metadatenarten, die die App vom Gerät streamt. **Kanal:** Der Kanal, den die App verwendet. Wählen Sie diese Option, um den Metadatenstream zu aktivieren. Schalten Sie diese Option aus aus Gründen der Kompatibilität oder Ressourcenverwaltung.

Melder

Kameramanipulation

Der Manipulationsmelder der Kamera generiert einen Alarm, wenn sich die Szene ändert, beispielsweise wenn das Objektiv abgedeckt, besprüht oder stark defokussiert ist, und die in **Trigger delay (Verzögerung beim Auslösen)** festgelegte Zeit verstrichen ist. Der Manipulationsmelder wird nur aktiviert, wenn die Kamera mindestens 10 Sekunden lang nicht bewegt wurde. In dieser Zeit richtet der Melder ein Szenemodell ein, um durch einen Vergleich Manipulationen in aktuellen Bildern zu erkennen. Stellen Sie zur ordnungsgemäßen Einrichtung des Szenemodells sicher, dass die Kamera fokussiert ist, die Lichtbedingungen stimmen und die Kamera nicht auf eine konturlose Szene wie etwa eine leere Wand gerichtet ist. Die Funktion Kamera-Manipulation kann auch als Bedingung für das Auslösen von Aktionsregeln verwendet werden.

Verzögerung beim Auslösen: Geben Sie ein, wie lange die Manipulationsbedingungen gegeben sein müssen, bevor der Alarm ausgelöst wird. So können falsche Alarmer bei bekannten Bedingungen, die das Bild beeinträchtigen, verhindert werden. **Auslösen bei dunklem Bild:** Es ist schwer möglich einen Alarm zu generieren, wenn das Kameraobjektiv besprüht wird, denn dieses Ereignis ist unmöglich von anderen Situationen zu unterscheiden, in denen der gleiche Effekt auftritt, also wenn sich etwa die Lichtverhältnisse ändern. Aktivieren Sie diese Einstellung, um in allen Fällen, in denen sich das Bild verdunkelt, Alarmer zu erzeugen. Wenn das Gerät ausgeschaltet ist, erzeugt es keinen Alarm, wenn sich das Bild verdunkelt.

Hinweis

Zur Erfassung von Manipulationsversuchen in statischen und nicht überfüllten Szenen.

Audioerkennung

Diese Einstellungen sind für jeden Audioeingang verfügbar. **Lautstärke:** Die Lautstärke kann auf einen Wert von 0 bis 100 festgelegt werden, wobei 0 die empfindlichste und 100 die unempfindlichste Einstellung ist. Richten Sie die Lautstärke mithilfe der Aktivitätsanzeige als Richtwert ein. Beim Erstellen von Ereignissen kann der Schallpegel als Bedingung verwendet werden. Sie können wählen, ob eine Aktion ausgelöst werden soll, wenn der Schallpegel den eingestellten Wert übersteigt, unter- oder überschreitet.

Stoßerkennung

AXIS A8207-VE Mk II Network Video Door Station

Die Weboberfläche

Stoßmelder: Aktivieren Sie diese Option, damit ein Alarm erzeugt wird wenn das Gerät von einem Objekt getroffen oder manipuliert wird. **Empfindlichkeitsstufe:** Bewegen Sie den Schieberegler, um die Empfindlichkeitsstufe einzustellen, bei der das Gerät einen Alarm erzeugen soll. Bei einem niedrigen Wert erzeugt das Gerät nur bei starkem Schlag einen Alarm. Bei einem hohen Wert erzeugt das Gerät schon bei leichter Manipulation einen Alarm.

Videoausgang

HDMI

Über ein HDMI-Kabel kann ein externer Monitor an das Gerät angeschlossen werden. **Single source (Einzelquelle)** Auf dem externen Monitor wird ein Videostream einer einzelnen Kamera angezeigt.

- **Source (Quelle):** Wählen Sie nur eine Kamera aus.
- **Rotate image 180° (Bild um 180° drehen):** Klicken Sie hier, um das Bild zu drehen.
- **Mirror image (Bild spiegeln):** Klicken Sie hier, um das Bild zu spiegeln.

- **Dynamic overlays (Dynamische Overlays)**  : Klicken Sie hier für ein Overlay.

Quad view (Vierfachansicht)  Zeigen Sie Streams von vier separaten Kameras gleichzeitig auf dem externen Monitor an.

- **Sources (Quellen):** Wählen Sie in jedem der vier Aufklappmenüs eine andere Kamera aus. Das Bild neben der Quelle zeigt, wo das Video von dieser Kamera auf dem Bildschirm angezeigt wird.
- **Rotate image 180° (Bild um 180° drehen):** Klicken Sie hier, um alle Bilder zu drehen.

Playlist (Wiedergabeliste)  Einzelne Streams von mehreren Kameras wechseln sich auf dem externen Monitor ab.

- **Rotate image 180° (Bild um 180° drehen):** Klicken Sie hier, um das Bild aus allen Quellen zu drehen.
- **+** : Klicken Sie hier, um eine Kamera zur Wiedergabeliste hinzuzufügen.
- **Source (Quelle):** Wählen Sie die gewünschte Kamera aus.
- **Duration (Dauer):** Legen Sie fest, wie lange (in mm:ss) die Wiedergabeliste bei jeder Drehung von dieser Kamera gestreamt wird.
- **Mirror image (Bild spiegeln):** Klicken Sie hier, um das Bild zu spiegeln.
- **Create (Erstellen):** Zum Speichern hier klicken.

Picture-in-picture (Bild-in-Bild)  Auf dem externen Monitor werden gleichzeitig zwei Streams angezeigt. Ein Stream füllt den Bildschirm vollständig aus, während der andere in einem kleineren Bild angezeigt wird. Die Einstellungen für **Position**, **Picture size (Bildgröße)** und **Borders (Ränder)** können angepasst werden.

- **Picture-in-picture (Bild-in-Bild)**
 - **Source (Quelle):** Wählen Sie die Kamera aus, die als kleineres Bild gestreamt werden soll.
 - **Rotate image 180° (Bild um 180° drehen):** Klicken Sie hier, um das Bild zu drehen.
 - **Mirror image (Bild spiegeln):** Klicken Sie hier, um das Bild zu spiegeln.
 - **Position:** Wählen Sie die Stelle aus, an der das Bild am Bildschirm angezeigt werden soll.
 - **Picture size (Bildgröße):** Legen Sie mit dem Schieberegler die Bildgröße (in % des Bildschirms) fest.
 - **Border (Rahmen):** Klicken Sie auf diese Schaltfläche, um Rahmen für das Bild ein- oder auszuschalten.
 -  : Ziehen Sie den Schieberegler, um die Dicke des gesamten Rahmens zu ändern.
 -  : Ziehen Sie den Schieberegler, um die Dicke des oberen Rands des Rahmens zu ändern.
 -  : Ziehen Sie den Schieberegler, um die Dicke des rechten Rands des Rahmens zu ändern.
 -  : Ziehen Sie den Schieberegler, um die Dicke des unteren Rands des Rahmens zu ändern.
 -  : Ziehen Sie den Schieberegler, um die Dicke des linken Rands des Rahmens zu ändern.
 - **Border color (Rahmenfarbe):** Wählen Sie eine Farbe für den Rahmen aus.
- **Main view (Hauptansicht)**
 - **Source (Quelle):** Wählen Sie die Kamera aus, die auf dem gesamten Bildschirm gestreamt werden soll.
 - **Rotate image 180° (Bild um 180° drehen):** Klicken Sie hier, um das Bild zu drehen.
 - **Mirror image (Bild spiegeln):** Klicken Sie hier, um das Bild zu spiegeln.

Zubehör

E/A-Ports

AXIS A8207-VE Mk II Network Video Door Station

Die Weboberfläche

Schließen Sie externe Geräte über digitale Eingänge an, die zwischen geöffnetem und geschlossenem Schaltkreis wechseln können, wie etwa PIR-Sensoren, Tür- oder Fensterkontakte und Glasbruchmelder.

Schließen Sie externe Geräte wie Relais und LEDs über digitale Ausgänge an. Sie können verbundene Geräte über die VAPIX® Application Programming Interface oder über die Weboberfläche aktivieren.

PortName: Bearbeiten Sie den Text, um den Port umzubenennen. **Direction (Richtung):**  gibt an, dass es sich bei dem Port um einen Eingangsanschluss handelt.  gibt an, dass es sich um einen Ausgangsanschluss handelt. Wenn der Port konfigurierbar ist, können Sie auf die Symbole klicken, um zwischen Eingang und Ausgang zu wechseln. **Normal state (Normalzustand):** Klicken

Sie auf  für einen geöffneten Schaltkreis" und auf  für einen geschlossenen Schaltkreis. **Current state (Aktueller Status):** Zeigt den aktuellen Status der Ports an. Der Ein- oder Ausgang wird aktiviert, wenn der aktuelle Zustand vom Normalzustand abweicht. Ein Eingang am Gerät ist offen, wenn er getrennt ist oder eine Spannung von mehr als 1 V Gleichstrom anliegt.

Hinweis

Der Schaltkreis des Ausgangs ist während eines Neustarts offen. Nach abgeschlossenem Neustart nimmt der Schaltkreis wieder die normale Position an. Wenn die Einstellungen auf dieser Seite geändert werden, nehmen die Schaltkreise der Ausgänge wieder ihre jeweiligen normalen Positionen an, wobei es unerheblich ist, ob aktive Auslöser vorliegen.

Supervised (Überwacht)  : Aktivieren Sie diese Option, um Aktionen zu erkennen und auszulösen, wenn jemand die Verbindung zu digitalen E/A-Geräten manipuliert. Sie können nicht nur erkennen, ob ein Eingang geöffnet oder geschlossen ist, sondern auch, ob jemand diesen manipuliert hat (d. h. abgeschnitten oder gekürzt). Zur Überwachung der Verbindung ist im externen E/A-Kreis zusätzliche Hardware (Abschlusswiderstände) erforderlich.

Protokolle

Protokolle und Berichte

Berichte

- **View the device server report (Geräteserver-Bericht anzeigen):** Zeigt Informationen zum Produktstatus in einem Popup-Fenster bereit. Das Zugangsprotokoll wird automatisch dem Server-Bericht angefügt.
- **Download the device server report (Bericht zum Geräteserver herunterladen):** Dabei wird eine .zip-Datei mit dem vollständigen Server-Bericht als Textdatei im Format UTF-8 sowie einem Momentaufnahme der aktuellen Live-Ansicht erstellt. Schließen Sie beim Kontakt mit dem Support stets die ZIP-Datei des Server-Berichts ein.
- **Download the crash report (Absturzbericht herunterladen):** So wird ein Archiv mit ausführlichen Informationen zum Produktstatus heruntergeladen. Der Absturzbericht enthält die im Server-Bericht enthaltenen Informationen sowie ausführliche Debug-Informationen. Dieser Bericht enthält möglicherweise vertrauliche Daten wie z. B. Netzwerk-Traces. Es kann einige Minuten dauern, bis der Bericht generiert wird.

Protokolle

- **Systemprotokoll sehen:** Klicken Sie, um Informationen zu Systemereignissen, wie z. B. Gerätestart, Warnungen und wichtige Meldungen, zu sehen.
- **View the access log (Zugangsprotokoll anzeigen):** Klicken Sie darauf, um alle fehlgeschlagenen Zugriffsversuche auf das Gerät zu sehen, bei denen z. B. ein falsches Anmeldekenntwort verwendet wurde.

Netzwerk-Trace

Wichtig

Eine Datei zum Netzwerk-Trace enthält möglicherweise vertrauliche Informationen wie Zertifikate oder Kennwörter.

Netzwerkablaufsverfolgungsdateien zeichnen Netzwerkaktivitäten auf und helfen so bei der Fehlersuche und -behebung. **Trace time (Verfolgungsdauer):** Geben Sie die Verfolgungsdauer in Sekunden oder Minuten an, und klicken Sie auf **Download (Herunterladen)**.

Remote-Systemprotokoll

AXIS A8207-VE Mk II Network Video Door Station

Die Weboberfläche

Syslog ist ein Standard für die Nachrichtenprotokollierung. Dadurch können die Software, die Nachrichten generiert, das System, in dem sie gespeichert sind, und die Software, die sie meldet und analysiert voneinander getrennt werden. Jede Nachricht ist mit einem Einrichtungscode versehen, der den Softwaretyp, der die Nachricht generiert, angibt, und einem Schweregrad zugewiesen.



Server: Klicken Sie, um einen neuen Server hinzuzufügen.**Host:** Geben Sie den Host-Namen oder die IP-Adresse des Servers ein.**Format:** Wählen Sie das zu verwendende syslog-Nachrichtenformat aus.

- Axis
- RFC 3164
- RFC 5424

Protocol (Protokoll): Wählen Sie das gewünschte Protokoll aus:

- UDP (Standardport ist 514)
- TCP (Standardport ist 601)
- TLS (Standardport ist 6514)

Port: Bearbeiten Sie die Port-Nummer, um einen anderen Port zu verwenden.**Severity (Schweregrad):** Wählen Sie aus, welche Meldungen bei Auslösung gesendet werden sollen.**CA-Zertifikat einrichten:** Sehen Sie sich die aktuellen Einstellungen an oder fügen Sie ein Zertifikat hinzu.

Direktkonfiguration

Direktkonfiguration ist für fortgeschrittene Benutzer mit Erfahrung bei der Konfiguration von Axis Geräten vorgesehen. Die meisten Parameter können auf dieser Seite eingestellt und bearbeitet werden.

Wartung

Neustart: Starten Sie das Gerät neu. Dies hat keine Auswirkungen auf aktuelle Einstellungen. Aktive Anwendungen werden automatisch neu gestartet.**Wiederherstellen:** Setzen Sie die *meisten Einstellungen* auf die Werkseinstellungen zurück. Anschließend müssen Sie Gerät und Apps neu konfigurieren, nicht vorinstallierte Apps neu installieren sowie Ereignisse und Voreinstellungen neu erstellen.

Wichtig

Die einzigen nach der Wiederherstellung weiterhin gespeicherten Einstellungen sind:

- Boot-Protokoll (DHCP oder statisch)
- Statische IP-Adresse
- Standardrouter
- Subnetzmaske
- Einstellungen für 802.1X
- Einstellungen für O3C
- DNS-Server IP-Adresse

Werkseinstellungen: Setzen Sie *alle* Einstellungen werden auf die Werkseinstellungen zurück. Anschließend müssen Sie die IP-Adresse zurücksetzen, um auf das Gerät zugreifen zu können.

Hinweis

Sämtliche Software des Axis Geräts ist digital signiert, um sicherzustellen, dass Sie nur die verifizierte Software auf Ihrem Gerät installieren. Diese Maßnahme erhöht das allgemeine Mindestniveau der Cybersicherheit für die Geräte von Axis. Weitere Informationen finden Sie im Whitepaper „Axis Edge Vault“ unter axis.com.

AXIS OS upgrade (AXIS OS-Aktualisierung): Aktualisieren Sie auf eine neue AXIS OS-Version. Neue Versionen können verbesserte Funktionen, Fehlerkorrekturen und vollständig neue Merkmale beinhalten. Wir empfehlen Ihnen, stets die aktuellste AXIS OS-Version zu verwenden. Um die neueste Version herunterzuladen, rufen Sie axis.com/support auf.

Bei der Aktualisierung können Sie zwischen drei Optionen wählen:

- **Standard upgrade (Standardaktualisierung):** Aktualisieren Sie auf die neue AXIS OS-Version.

AXIS A8207-VE Mk II Network Video Door Station

Die Weboberfläche

- **Factory default (Werkseinstellungen):** Führen Sie die Aktualisierung durch und alle Einstellungen werden auf die Werkseinstellungen zurückgesetzt. Wenn Sie diese Option wählen, können Sie nach der Aktualisierung nicht mehr zur vorherigen AXIS OS-Version zurückkehren.
 - **Autorollback (Automatisches Zurücksetzen):** Aktualisieren Sie und bestätigen Sie die Aktualisierung innerhalb der festgelegten Zeit. Wenn Sie diese nicht bestätigen, wird das Gerät auf die vorherige AXIS OS-Version zurückgesetzt.
- AXIS OS rollback (AXIS OS zurücksetzen):** Setzen Sie die Version auf die vorherige AXIS OS-Version zurück.

AXIS A8207-VE Mk II Network Video Door Station

Mehr erfahren

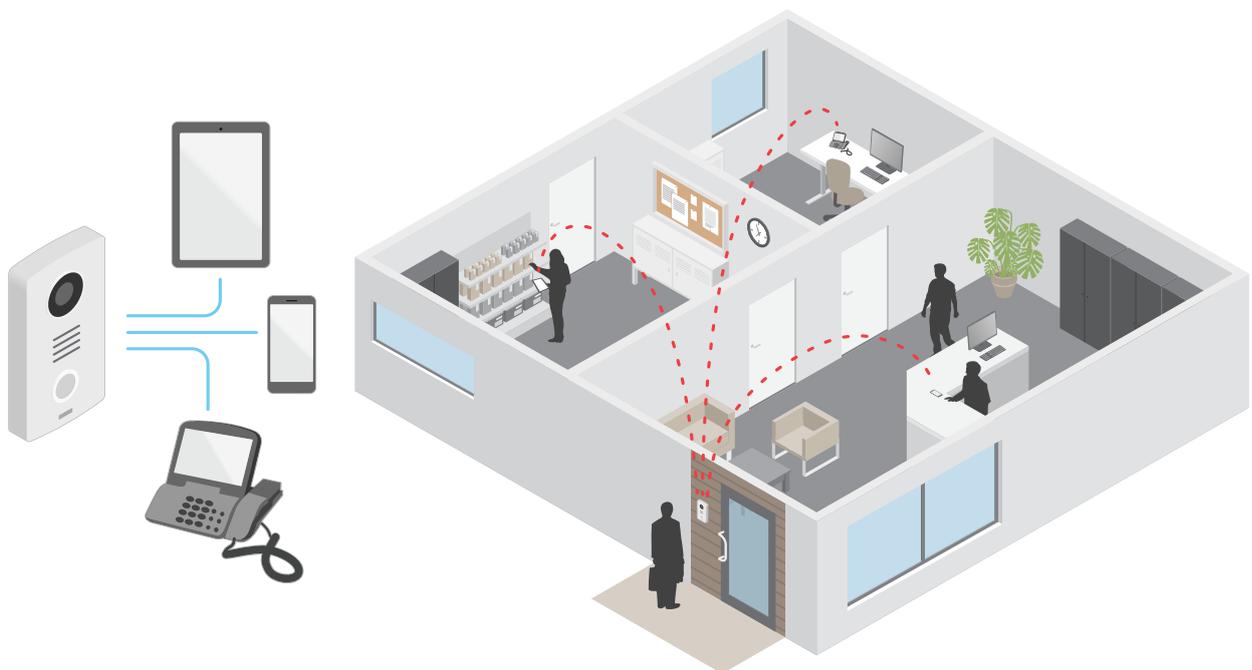
Mehr erfahren

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.

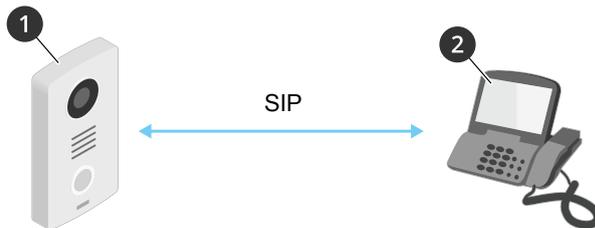
AXIS A8207-VE Mk II Network Video Door Station

Mehr erfahren

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 in diesem Fall ist `sip:<local-ip>`.

Beispiel:



- 1 Benutzeragent A – Türstation. 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.

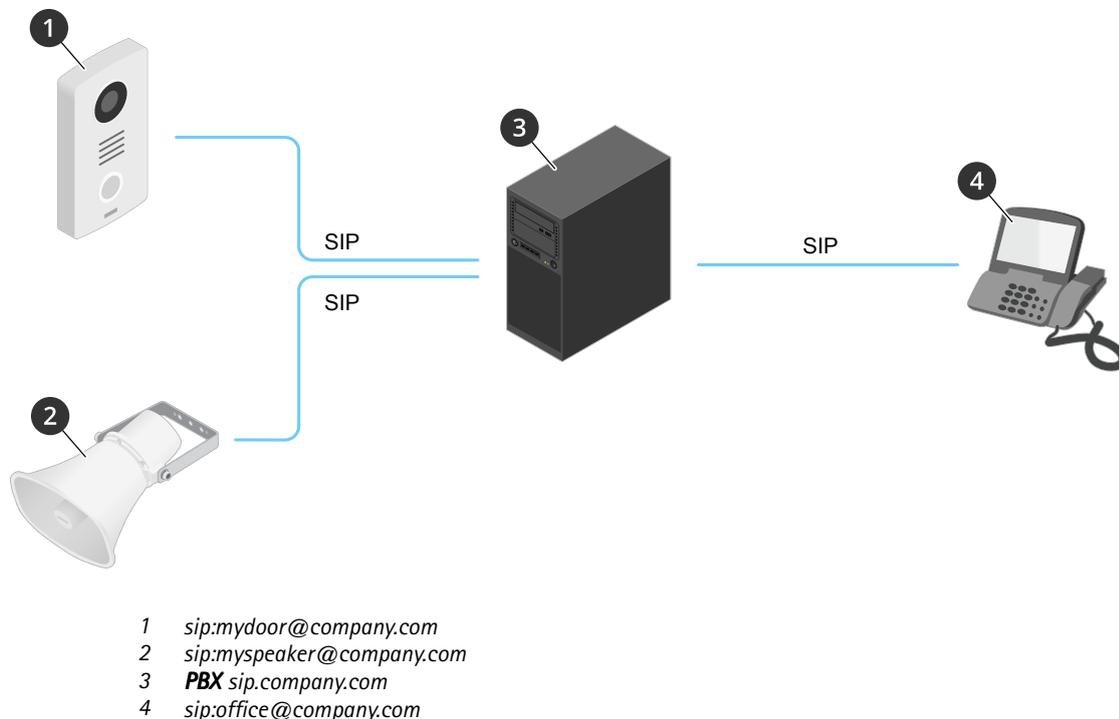
Der PBX-SIP-Server kann lokal oder extern eingerichtet werden. Er kann im Intranet oder durch einen Drittanbieter gehostet werden. Wenn Sie SIP-Anrufe zwischen Netzwerken tätigen, werden Anrufe über einen Satz von PBX-Anlagen weitergeleitet, die den Standort der zu erreichenden SIP-Adresse abfragen.

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:

AXIS A8207-VE Mk II Network Video Door Station

Mehr erfahren



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 in unserer Anleitung *Erste Schritte mit Regeln für Ereignisse*.

Anwendungen

Mit Anwendungen erhalten Sie mehr aus Ihrem Axis Gerät. Die AXIS Camera Application Platform (ACAP) ist eine offene Plattform, die es für andere Anbietern möglich macht, Analysefunktionen und andere Anwendungen für Axis Geräte zu entwickeln. Anwendungen können auf dem Gerät vorinstalliert werden und kostenlos oder für eine Lizenzgebühr heruntergeladen werden.

Benutzerhandbücher zu Axis Anwendungen finden Sie auf help.axis.com.

AXIS A8207-VE Mk II Network Video Door Station

Tägliche Nutzung

Tägliche Nutzung

Verwenden des Tastenfelds

Ich möchte...	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.

AXIS A8207-VE Mk II Network Video Door Station

Fehlerbehebung

Fehlerbehebung

Zurücksetzen auf die Werkseinstellungen

Wichtig

Das Zurücksetzen auf die Werkseinstellungen sollte mit Vorsicht erfolgen. Beim Zurücksetzen auf die Werkseinstellungen werden alle Einstellungen einschließlich der IP-Adresse zurückgesetzt.

So wird das Produkt auf die werksseitigen Standardeinstellungen zurückgesetzt:

1. Trennen Sie das Produkt von der Stromversorgung.
2. Halten Sie die Steuertaste gedrückt und stellen Sie die Stromversorgung wieder her. Siehe .
3. Halten Sie die Steuertaste etwa 15 bis 30 Sekunden gedrückt, bis die Status-LED gelb blinkt.
4. Lassen Sie die Steuertaste los. Der Vorgang ist abgeschlossen, wenn die Status-LED grün leuchtet. Das Produkt wurde auf die Werkseinstellungen zurückgesetzt. Wenn im Netzwerk kein DHCP-Server verfügbar ist, lautet die Standard-IP-Adresse 192.168.0.90.
5. Verwenden Sie Installations- und Verwaltungstools, um IP-Adressen zuzuweisen, das Kennwort festzulegen und auf das Gerät zuzugreifen.

Die Installations- und Verwaltungstools finden auf den Supportseiten unter axis.com/support.

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

Aktuelle AXIS OS-Version überprüfen

AXIS OS bestimmt die Funktionalität unserer Geräte. Wir empfehlen Ihnen, vor jeder Problembeseitigung 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

- Vorkonfigurierte und angepasste Einstellungen werden beim Aktualisieren der Gerätesoftware gespeichert (sofern die Funktionen als Teil der neuen AXIS OS-Version verfügbar sind). Es besteht diesbezüglich jedoch keine Gewährleistung seitens Axis Communications AB.
- 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.

AXIS A8207-VE Mk II Network Video Door Station

Fehlerbehebung

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 Einstellen 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): <ul style="list-style-type: none">• Wenn Folgendes angezeigt wird: <code>Reply from (Antwort von)<IP address>: bytes=32; time=10...</code> dies bedeutet, 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 Folgendes angezeigt wird: <code>Request timed out</code> bedeutet, 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	Wenn HTTPS aktiviert ist, stellen Sie sicher, dass beim Anmelden das korrekte Protokoll (HTTP oder HTTPS) verwendet wird. Möglicherweise müssen Sie manuell <code>http</code> oder <code>https</code> in die Adressleiste des Browsers eingeben. Wenn das Kennwort für den Benutzer „root“ vergessen wurde, muss das Gerät auf die werkseitigen Standardeinstellungen zurückgesetzt werden. Siehe .
------------------------	---

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

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

AXIS A8207-VE Mk II Network Video Door Station

Fehlerbehebung

Leistungsaspekte

Achten Sie beim Einrichten Ihres Systems unbedingt darauf, wie sich die verschiedenen Einstellungen und Situationen auf die Leistung auswirken. Einige Faktoren wirken sich auf die erforderliche Bandbreite (die Bitrate) aus, andere auf die Bildrate und einige sowohl auf die Bandbreite als auch die Bildrate. Wenn die CPU-Auslastung ihre Grenze erreicht, wirkt sich dies ebenfalls auf die Bildrate aus.

Die folgenden wichtigen Faktoren müssen beachtet werden:

- 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 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 Videostreams des Typs Motion JPEG und H.264 beeinflusst sowohl die Bildrate als auch die Bandbreite.
- 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.

AXIS A8207-VE Mk II Network Video Door Station

Technische Daten

Technische Daten

Anzeigen und Bedienelemente an der Vorderseite

Wenn Sie das Produkt an die Stromversorgung anschließen, leuchten die Indikatorsymbole und die Anzeigeleiste ein paar Sekunden lang auf.

Indikatorsymbole

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

Kartenleser-Markierungstreifen

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 mit den Fingern ein und entnehmen Sie diese auf die gleiche Weise.
- 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.

Empfehlungen zu SD-Karten finden Sie auf 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.

AXIS A8207-VE Mk II Network Video Door Station

Technische Daten

Tasten

Steuertaste

Die Steuertaste hat folgende Funktionen:

- Zurücksetzen des Produkts auf die Werkseinstellungen. Siehe .

Anschlüsse

HDMI-Anschluss

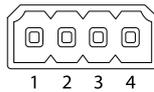
Über den microHDMI™-Anschluss werden Displays oder öffentliche Monitore angeschlossen.

Netzwerk-Anschluss

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

Audioanschluss

4-polige Klemmleiste für Audioein- und -ausgang.

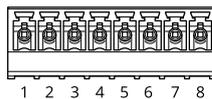


Funktion	Kontakt	Hinweise
Leitungseingang	1	Eingang (Mono)
Erde (GND)	2	Audio-Masse
Ausgang	3	Ausgang
Masse (GND)	4	Audio-Masse

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	Schließer-/Öffner-Kontakt Für den Anschluss von Relais-Geräten. Die beiden Relaisanschlüsse sind galvanisch von den anderen Schaltkreisen getrennt.	Max. Stromstärke 1 A Max. Spannung 30 V Gleichstrom

AXIS A8207-VE Mk II Network Video Door Station

Technische Daten

COM	2	Gemeinsam	
24 V Gleichstrom	3	Zur Stromversorgung von Zusatzgeräten. Hinweis: Dieser Kontakt darf nur für den Stromausgang verwendet werden.	Ausgangsspannung 24 V Gleichstrom Max. Strom 50 mA ¹ Max. Strom 350 mA ²
Erdung Gleichstrom	4		0 V Gleichstrom
NO/NC	5	Schließer-/Öffner-Kontakt Für den Anschluss von Relais-Geräten. Die beiden Relaisanschlüsse sind galvanisch von den anderen Schaltkreisen getrennt.	Max. Stromstärke 1 A Max. Spannung 30 V Gleichstrom
COM	6	Gemeinsam	
12 V Gleichstrom	7	Zur Stromversorgung von Zusatzgeräten. Hinweis: Dieser Kontakt darf nur für den Stromausgang verwendet werden.	Ausgangsspannung 12 V Gleichstrom Max. Stromstärke 100 mA ³ Max. Stromstärke 700 mA ⁴
Erdung Gleichstrom	8		0 V Gleichstrom

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 Gleichstromversorgung.
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 Gleichstrom-Stromzufuhr.

Lesegerätanschluss

4-polige Klemmleiste für den Anschluss externer Leser.

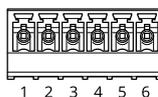
Funktion	Kontakt	Hinweise	Technische Daten
Erdung Gleichstrom	1		0 V Gleichstrom
12 V Gleichstrom	2	Zur Stromversorgung von Zusatzgeräten. Hinweis: Dieser Kontakt darf nur für den Stromausgang verwendet werden.	Ausgangsspannung 12 V Gleichstrom
D0/A+	3	Wiegand: DATA0-Ausgang RS485: A+	
D1/B-	4	Wiegand: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

E/A-Anschluss

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

Digitaleingang – Zum Anschluss 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.

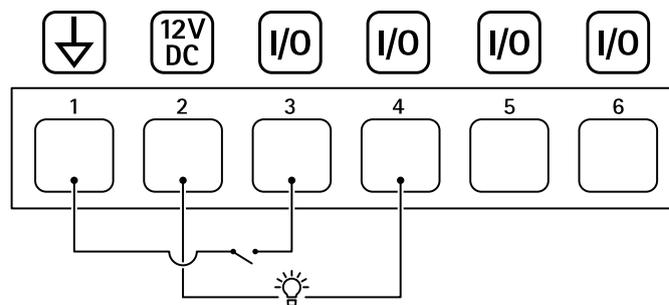


AXIS A8207-VE Mk II Network Video Door Station

Technische Daten

Funktion	Kontakt	Hinweise	Technische Angaben
Erdung Gleichstrom	1		0 V Gleichstrom
Gleichstromausgang	2	Darf für die Stromversorgung von Zusatzgeräten verwendet werden. Hinweis: Dieser Kontakt darf nur für den Stromausgang verwendet werden.	12 V DC 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 (Gleichstrom Erdschluss), 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

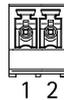
Beispiel:



- 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. Verwenden Sie eine mit den Anforderungen für Schutzkleinspannung (SELV) kompatible Stromquelle mit begrenzter Leistung (LPS) mit einer Nennausgangsleistung von ≤ 100 W oder einem dauerhaft auf ≤ 5 A begrenzten Nennausgangsstrom.



Funktion	Kontakt	Hinweise	Technische Daten
Erdung Gleichstrom	1		0 V Gleichstrom
Wechselstromeingang	2	Stromversorgung der Steuerung bei Nichtverwendung von Power over Ethernet. Hinweis: Dieser Kontakt kann nur für den Stromeingang verwendet werden.	8–28 V Gleichstrom, max. 22 W Max. Last an den Ausgängen 9 W

AXIS A8207-VE Mk II Network Video Door Station

Sicherheitsinformationen

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.

