

## **AXIS C8210 Network Audio Amplifier**

**Benutzerhandbuch**

# AXIS C8210 Network Audio Amplifier

## Lösungsübersicht

---

### Lösungsübersicht

Dieses Handbuch beschreibt, wie Sie das Gerät für Ihr Audiosystem zugänglich machen und wie Sie das Gerät direkt von der Benutzeroberfläche aus konfigurieren (z. B. wenn Sie das Gerät ohne Audio- oder Videoverwaltungssoftware verwenden).

Wenn Sie eine Audio- oder Video Management Software verwenden, können Sie das Gerät mit dieser Software konfigurieren. Für die Steuerung Ihres Audiosystems steht die folgende Management-Software zur Verfügung:

- **AXIS Audio Manager Edge** – Audio Management Software für kleine Systeme. Ist auf allen Audiogeräten mit der Firmware 10.0 oder höher vorinstalliert.
  - *AXIS Audio Manager Edge – Benutzerhandbuch*
- **AXIS Audio Manager Pro** – Fortgeschrittene Audioverwaltungs-Software für große Systeme.
  - *AXIS Audio Manager Pro – Benutzerhandbuch*
- **AXIS Camera Station** – Erweiterte Videoverwaltungs-Software für große Systeme.
  - *AXIS Camera Station – Benutzerhandbuch*
- **AXIS Companion** – Videoverwaltungs-Software für kleine Systeme.
  - *AXIS Companion – Benutzerhandbuch*

Weitere Informationen hierzu finden Sie unter *Audioverwaltungssoftware*.



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

[help.axis.com/?etpid=47555&section=solution-overview](http://help.axis.com/?etpid=47555&section=solution-overview)

*Eine Übersicht über die Funktionsweise von Netzwerk-Audio.*

# AXIS C8210 Network Audio Amplifier

## Installation

---

### Installation



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

*[help.axis.com/?&piid=47555&section=solution-overview](http://help.axis.com/?&piid=47555&section=solution-overview)*

*Installationsvideo für das Produkt.*

# AXIS C8210 Network Audio Amplifier

## 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](http://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*.

#### Auf das Gerät zugreifen

1. Öffnen Sie einen Browser, und geben Sie die IP-Adresse oder den Hostnamen des Axis Geräts in die Adresszeile des Browsers ein.
2. Den Benutzernamen und das Kennwort eingeben. Wenn dies der erste Zugriff auf das Gerät ist, muss zuerst das Root-Kennwort konfiguriert werden. Siehe *Ein neues Kennwort für das Root-Konto festlegen auf Seite 4*.

#### Ein neues Kennwort für das Root-Konto festlegen

##### Wichtig

Der voreingestellte Benutzernamen für das Administratorkonto lautet **root**. Bei Verlust des Kennworts für das Benutzerkonto Root muss das Gerät auf die Werkseinstellungen zurückgesetzt werden. Siehe *Zurücksetzen auf die Werkseinstellungen auf Seite 43*



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

[help.axis.com/?&pid=47555&section=set-a-new-password-for-the-root-account](http://help.axis.com/?&pid=47555&section=set-a-new-password-for-the-root-account)

*Support-Tipp: Überprüfung der Kennwortsicherheit*

# AXIS C8210 Network Audio Amplifier

## Erste Schritte

---

1. Geben Sie ein Kennwort ein. Befolgen Sie die Anweisungen zum Erstellen sicherer Kennwörter. Siehe *Sichere Kennwörter auf Seite 5*.
2. Geben Sie das Kennwort erneut ein, um die korrekte Zeichenfolge zu bestätigen.
3. Klicken Sie auf **Speichern**. Das Kennwort wurde konfiguriert.

### 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.

# AXIS C8210 Network Audio Amplifier

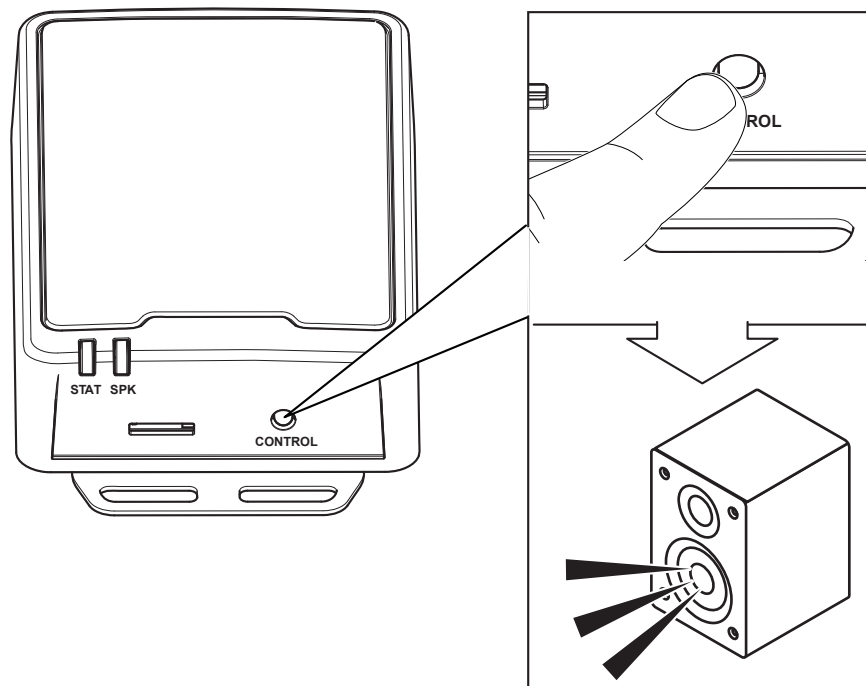
## Weitere Einstellungen

---

### Weitere Einstellungen

#### Testen Sie die Impedanz

Testen Sie die Impedanz, nachdem Sie den Lautsprecher angeschlossen haben und bevor Sie den Verstärker zum ersten Mal benutzen, oder wenn Sie die Einstellung des Lautsprechers geändert haben, der an den Verstärker angeschlossen ist. Die SPK-LED blinkt grün, wenn ein Impedanztest erforderlich ist. Führen Sie den Impedanztest durch, indem Sie den Steuerknopf drücken, bis Sie Töne aus dem Lautsprecher hören.



#### Direktes SIP (P2P) einrichten

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 zur Funktionsweise von P2P finden Sie unter *Peer-to-Peer SIP (P2PSIP)* auf Seite 11.

Weitere Informationen zu den Einstellungsoptionen finden Sie unter *SIP* auf Seite 33.

1. Wechseln Sie zu **System > SIP > SIP settings** (System > SIP > SIP-Einstellungen), und wählen Sie **Enable SIP** (SIP aktivieren).
2. Um die Annahme eingehender Anrufe durch das Gerät zu erlauben, wählen Sie die Option **Allow incoming calls** (Eingehende Anrufe erlauben) aus.
3. Legen Sie unter **Call handling** (Anrufbehandlung) die Zeitüberschreitung und Dauer des Anrufs fest.
4. Geben Sie unter **Ports** die Portnummern ein.
  - **SIP port** (SIP-Port) – Der für die SIP-Kommunikation genutzte Netzwerk-Port. Der Datenverkehr über diesen Port ist nicht verschlüsselt. Die Standardportnummer ist 5060. Bei Bedarf eine andere Portnummer eingeben.

# AXIS C8210 Network Audio Amplifier

## Weitere Einstellungen

---

- **TLS port (TLS-Port)** – Der für verschlüsselte SIP-Kommunikation genutzte Netzwerk-Port. Der Datenverkehr über diesen Port wird mittels Transport Layer Security (TLS) verschlüsselt. Die Standardportnummer ist 5061. Bei Bedarf eine andere Portnummer eingeben.
  - **RTP start port (RTP-Startport)** – Den Port für den ersten RTP-Mediastream eines SIP-Anrufs eingeben. Der Standardstartport für Medienübertragungen ist 4000. Möglicherweise blockieren einige Firewalls RTP-Datenverkehr an bestimmten Portnummern. Eine Portnummer muss zwischen 1024 und 65535 liegen.
5. Wählen Sie unter **NAT Traversal** die Protokolle, die für NAT Traversal aktiviert werden sollen.

### Hinweis

NAT Traversal verwenden, wenn das Axis Gerät über einen NAT-Router oder eine Firewall mit dem Netzwerk verbunden ist. Weitere Informationen finden Sie unter *NAT-Traversal auf Seite 12*.

6. Wählen Sie unter **Audio** mindestens einen Audiocodec mit der für SIP-Anrufe gewünschten Audioqualität. Ändern Sie die Prioritätsreihenfolge per Drag & Drop.
7. Wählen Sie unter **Additional (Erweitert)** weitere Optionen aus.
- **UDP-to-TCP switching (Zwischen UDP und TCP wechseln)** – 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.
  - **Allow via rewrite (Umschreiben erlauben)** – Wählen Sie diese Option, um die lokale IP-Adresse anstelle der öffentlichen IP-Adresse des Routers zu senden.
  - **Allow via rewrite (Umschreiben des Kontakts erlauben)** – Wählen Sie diese Option, um die lokale IP-Adresse anstelle der öffentlichen IP-Adresse des Routers zu senden.
  - **Register with server every (Häufigkeit der Registrierung am Server)** – Legen Sie fest, wie oft sich das Gerät beim SIP-Server für die vorhandenen SIP-Konten registrieren soll.
  - **DTMF payload type (DTMF-Nutzlasttyp)** – Ändert den Standard-Nutzlasttyp für DTMF.
8. Klicken Sie auf **Save (Speichern)**.

## SIP über einen Server (PBX) einrichten

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 zur Funktionsweise von P2P finden Sie unter *Private Branch Exchange (PBX) auf Seite 11*.

Weitere Informationen zu den SIP-Einstellungsoptionen finden Sie unter *SIP auf Seite 33*.

1. Fordern Sie folgende Informationen von Ihrem PBX-Anbieter an:
- Benutzer-ID
  - Domain
  - Kennwort
  - Authentifizierungs-ID
  - Caller-ID (Anrufer-ID)
  - Registrator
  - RTP-Startport
2. Um ein neues Konto hinzuzufügen, wechseln Sie zu **System > SIP > SIP accounts (SIP-Konten)** und klicken Sie auf **+ Account (+ Konto)**.

# AXIS C8210 Network Audio Amplifier

## Weitere Einstellungen

---

3. Geben Sie die von Ihrem PBX-Anbieter erhaltenen Informationen ein.
4. Wählen Sie **Registered (Registriert)** aus.
5. Transportmodus auswählen.
6. Klicken Sie auf **Save (Speichern)**.
7. Die SIP-Einstellungen auf die gleiche Weise wie für Peer-to-Peer einrichten. Weitere Informationen siehe *Direktes SIP (P2P) einrichten auf Seite 6*.

### Einrichten von Regeln für Ereignisse

Sie können Regeln erstellen, damit das Gerät beim Auftreten bestimmter Ereignisse Aktionen ausführt. Eine Regel besteht aus Bedingungen und Aktionen. Die Bedingungen können verwendet werden, um die Aktionen auszulösen. So kann das Gerät beispielsweise einen Audioclip nach einem Zeitplan oder bei Eingang eines Anrufs abspielen oder eine E-Mail senden, wenn das Gerät die IP-Adresse ändert.

Weitere Informationen finden Sie in unserer Anleitung *Erste Schritte mit Regeln für Ereignisse*.

### Wiedergabe von Audio, wenn eine Kamera eine Bewegung erkennt

Dieses Beispiel erläutert das Einrichten des Audiogeräts zum Wiedergeben eines Audioclips bei Bewegungserfassung durch eine Axis Netzwerk-Kamera.

#### Voraussetzungen

- Das Axis Audiogerät und die Axis Netzwerk-Kamera befinden sich im selben Netzwerk.
- Die Anwendung für die Bewegungserfassung ist konfiguriert und ist auf dem aktuellen Stand und wird auf der Kamera ausgeführt.

#### 1. Links zu Audioclips vorbereiten:

1.1 Rufen Sie **Audio > Audio clips** auf.

1.2 Klicken Sie auf  > **Create link (Link erstellen)**, um einen Link zu einem Audioclip zu erstellen.

1.3 Stellen Sie die Lautstärke und die Anzahl der Wiederholungen für den Clip ein.

1.4 Klicken Sie auf das Kopiersymbol, um den Link zu kopieren.

#### 2. Erstellen Sie eine Aktionsregel:

2.1 Wechseln Sie zu **System > Events (Ereignisse) > Recipients (Empfänger)**.

2.2 Klicken Sie auf **+ Add recipient (+ Empfänger hinzufügen)**.

2.3 Geben Sie einen Namen für den Empfänger ein, z. B. „Lautsprecher“.

2.4 **HTTP** aus dem Aufklappmenü **Typ** wählen.

2.5 Fügen Sie den konfigurierten Link aus dem Audiogerät in das Feld **URL** ein.

2.6 Geben Sie den Benutzernamen und das Kennwort des Audiogeräts ein.

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

2.8 Wechseln Sie zu **Rules (Regeln)**, und klicken Sie auf **+ Add a rule (+ Regel hinzufügen)**.

2.9 Geben Sie Namen für die Aktionsregel ein, z. B. „Clip wiedergeben“.



# AXIS C8210 Network Audio Amplifier

## Weitere Einstellungen

---

- 2.10 Aus der Liste **Condition (Bedingung)** eine alternative videobasierte Bewegungserkennung unter **Applications (Anwendungen)** auswählen.

### Hinweis

Wenn keine Optionen für die videobasierte Bewegungserkennung vorhanden sind, wechseln Sie zu **Apps**, klicken Sie auf **AXIS Video Motion Detection (AXIS Videobasierte Bewegungserkennung)** und aktivieren Sie die Bewegungserkennung.


- 2.11 Aus der Liste **Action (Aktion)** die Option **Send notification through HTTP (Benachrichtigung über HTTP senden)** auswählen.

2.12 Unter **Recipient (Empfänger)** den Empfänger auswählen.

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

## Audio mit DTMF anhalten

Dieses Beispiel erläutert, wie:

- DTMF auf einem Gerät konfiguriert werden kann.
  - Erstellen Sie ein Ereignis zur Unterbrechung der Audioübertragung, sobald ein DTMF-Befehl an das Gerät gesendet wird.
1. Wechseln Sie zu **System > SIP > SIP settings** (System > SIP > SIP-Einstellungen).
  2. Stellen Sie sicher, dass **Enable SIP (SIP aktivieren)** eingeschaltet ist.  
Wenn Sie dies aktivieren müssen, klicken Sie anschließend auf **Speichern**.
  3. Wechseln Sie zu **SIP accounts (SIP-Konten)**.
  4. Klicken Sie neben dem SIP-Konto auf  > **Edit (Bearbeiten)**.
  5. Klicken Sie unter **DTMF** auf **+ DTMF sequence (+ DTMF-Sequenz)**.
  6. Geben Sie unter **Sequence (Sequenz)** „1“ ein.
  7. Geben Sie unter **Description (Beschreibung)** „Audio anhalten“ ein.
  8. Klicken Sie auf **Save (Speichern)**.
  9. Wechseln Sie zu **System > Events (Ereignisse) > Rules (Regeln)** und klicken Sie auf **+ Add a rule (+ Regel hinzufügen)**.
  10. Geben Sie unter **Name** „DTMF – Audio anhalten“ ein.
  11. Wählen Sie unter **Condition (Bedingung)** die Option **DTMF**.
  12. Wählen Sie unter **DTMF Event ID (DTMF-Ereignis-ID)** die Option **stop audio (Audio anhalten)**.
  13. Wählen Sie unter **Action (Aktion)** die Option **Stop playing audio clip (Audioclip anhalten)**.
  14. Klicken Sie auf **Save (Speichern)**.

## Audio für eingehende SIP-Anrufe einrichten

Für eingehende SIP-Anrufe können Sie eine Regel erstellen, die einen bestimmten Audioclip abspielt.

Daneben können Sie zudem eine zusätzliche Regel zur automatischen Annahme des SIP-Anrufs nach Abspielen des Audioclips erstellen. Dies kann nützlich sein, um bei Bedarf andere Personen im Bereich eines Audiogeräts zu alarmieren und eine Kommunikationsverbindung zur Alarmzentrale herzustellen. Hierzu erfolgt ein SIP-Anruf an das jeweilige Audiogerät, das einen Audioclip abspielt, um die Personen seinem Einzugsbereich zu warnen. Nach Abspielen des Audioclips nimmt das Audiogerät


# AXIS C8210 Network Audio Amplifier

## Weitere Einstellungen

---

den SIP-Anruf automatisch an und stellt eine Kommunikationsverbindung zwischen der Alarmzentrale und den Personen im Einzugsbereich des Audiogeräts her.

SIP-Einstellungen aktivieren:

1. Rufen Sie die Geräteschnittstelle des Lautsprechers auf, indem Sie die entsprechende IP-Adresse in einem Webbrowser eingeben.
2. Wechseln Sie zu **System > SIP > SIP settings** (System > SIP > SIP-Einstellungen), und wählen Sie **Enable SIP (SIP aktivieren)**.
3. Um die Annahme eingehender Anrufe durch das Gerät zu erlauben, wählen Sie die Option **Allow incoming calls (Eingehende Anrufe erlauben)** aus.
4. Klicken Sie auf **Save (Speichern)**.
5. Wechseln Sie zu **SIP accounts (SIP-Konten)**.
6. Klicken Sie neben dem SIP-Konto auf  > **Edit (Bearbeiten)**.
7. Deaktivieren Sie die Option **Answer automatically (Automatische Annahme)**.

Audiowiedergabe bei eingehendem SIP-Anruf:

1. Wechseln Sie zu **Settings > System > Events > Rules** (Einstellungen > System > Ereignisse > Regeln), und fügen Sie eine Regel hinzu.
2. Geben Sie einen Namen für die Regel ein.
3. Wählen Sie in der Bedingungsliste die Option **State (Zustand)** aus.
4. Wählen Sie in der Zustandsliste die Option **Ringling (Klingelton)** aus.
5. Wählen Sie in der Aktionsliste die Option **Play audio clip (Audioclip wiedergeben)** aus.
6. Wählen Sie aus der Liste der Audioclips den Clip aus, den Sie abspielen möchten.
7. Wählen Sie aus, wie oft der Audioclip abgespielt werden soll. „0“ bedeutet „nur einmal“.
8. Klicken Sie auf **Save (Speichern)**.

SIP-Anruf nach Abspielen des Audioclips automatisch annehmen:

1. Wechseln Sie zu **Settings > System > Events > Rules** (Einstellungen > System > Ereignisse > Regeln), und fügen Sie eine Regel hinzu.
2. Geben Sie einen Namen für die Regel ein.
3. Wählen Sie in der Bedingungsliste die Option **Audio clip playing (Audioclip abspielen)** aus.
4. Aktivieren Sie die Option **Use this condition as a trigger (Diese Bedingung als Auslöser verwenden)**.
5. Aktivieren Sie die Option **Invert this condition (Diese Bedingung umkehren)**.
6. Klicken Sie auf **+ Add a condition (+ Bedingung hinzufügen)**, um dem Ereignis eine zweite Bedingung hinzuzufügen.
7. Wählen Sie in der Bedingungsliste die Option **State (Zustand)** aus.
8. Wählen Sie in der Zustandsliste die Option **Ringling (Klingelton)** aus.
9. Wählen Sie in der Aktionsliste die Option **Answer call (Anruf annehmen)** aus.
10. Klicken Sie auf **Save (Speichern)**.

# AXIS C8210 Network Audio Amplifier

## Mehr erfahren

---

### Mehr erfahren

#### Session Initiation Protocol (SIP)

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

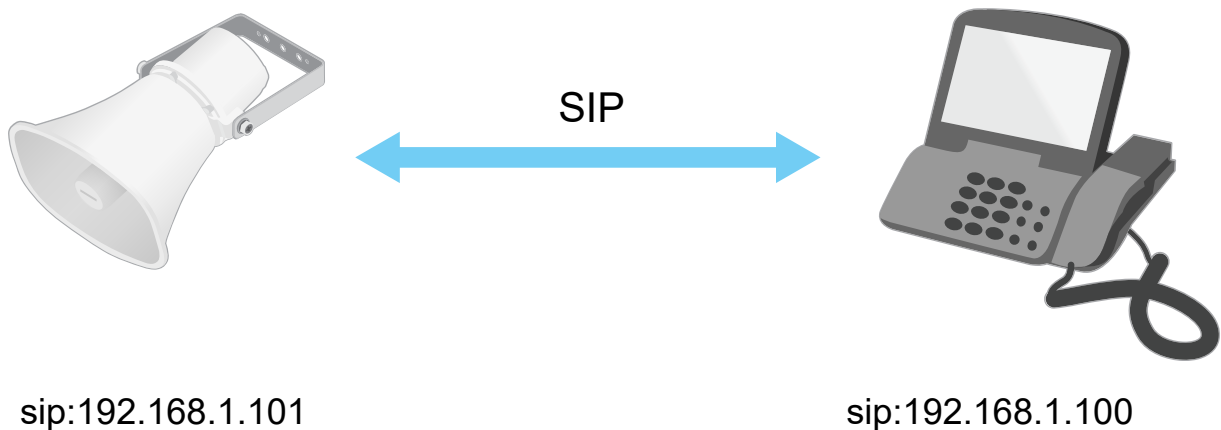
Die eigentlichen Audio- bzw. Videoübertragungen werden zwischen den SIP-Benutzeragenten mit einem Transportprotokoll, wie z. B. RTP (Real-Time Transport Protocol), ausgetauscht.

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

#### Peer-to-Peer SIP (P2PSIP)

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

Beispiel:



Sie können ein SIP-fähiges Telefon so einrichten, dass ein Audiogerät im selben Netzwerk über ein Peer-to-Peer-SIP-Setup angerufen wird.

#### 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.

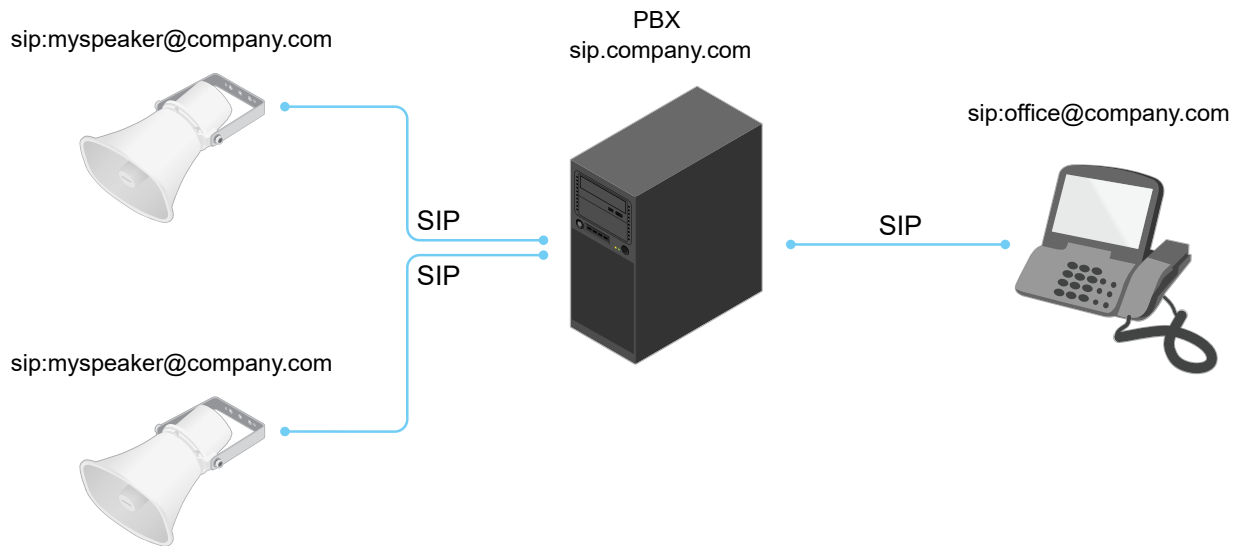
Der PBX-SIP-Server kann lokal oder extern eingerichtet werden. Er kann im Intranet oder durch einen Drittanbieter gehostet werden. Wenn Sie SIP-Anrufe zwischen Netzwerken tätigen, werden Anrufe über einen Satz von PBX-Anlagen weitergeleitet, die den Standort der zu erreichenden SIP-Adresse abfragen.

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.

# AXIS C8210 Network Audio Amplifier

## Mehr erfahren

Beispiel:



## NAT-Traversal

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

### Hinweis

Der Router muss NAT-Traversal und UPnP® unterstützen.

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

- **ICE** – Das Protokoll ICE (Interactive Connectivity Establishment) erhöht die Chancen, den effizientesten Kommunikationspfad zwischen gleichrangigen Geräten zu finden. Mit dem Aktivieren von STUN und TURN werden die Chancen des ICE-Protokolls nochmals verbessert.
- **STUN** – STUN (Session Traversal Utilities for NAT) ist ein Client-Server-Netzwerkprotokoll, an dem Axis Produkte erkennen, ob sie sich hinter einer NAT oder Firewall befinden. Zudem werden mit diesem Protokoll öffentlich zugewiesene IP-Adressen (NAT-Adressen) und Portnummern abgerufen, die von NAT für Verbindungen mit Remote-Hosts zugewiesen wurden. 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. Die TURN-Server-Adresse und die Anmeldedaten eingeben.

## 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](http://help.axis.com).



# AXIS C8210 Network Audio Amplifier


## Die Weboberfläche

### Die Weboberfläche

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

 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:

- 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:

- **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.

### Status

#### Audio system info (Informationen zum Audiosystem)

Diese Informationen werden nur für Geräte angezeigt, die zu einem AXIS Audio Manager Edge-Standort gehören.

**AXIS Audio Manager Edge**: AXIS Audio Manager Edge starten.

#### Locate device (Gerät lokalisieren)

Zeigt die Gerätelokalisierungsinformationen an, einschließlich Seriennummer und IP-Adresse.

**Locate device (Gerät lokalisieren)**: Spielt einen Ton ab, der Ihnen bei der Erkennung des Lautsprechers hilft. Bei einigen Produkten blinkt eine LED auf dem Gerät.

#### 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.

# AXIS C8210 Network Audio Amplifier

## Die Weboberfläche

---

### 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 (Härtungsleitfaden):** 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.

**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 **Aufzeichnungen auf Seite 16**.



Anzeige des Speicherorts der Aufzeichnung.

## Audio

### AXIS Audio Manager Edge

**AXIS Audio Manager Edge:** Starten Sie die Anwendung.

### Geräteinstellungen

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

**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.

# AXIS C8210 Network Audio Amplifier

## Die Weboberfläche

---

**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 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.

### 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.

# AXIS C8210 Network Audio Amplifier

## Die Weboberfläche

---

### Mithören und aufzeichnen



Klicken Sie darauf, um zu hören.



Startet eine ständige Aufzeichnung des Audiostreams. Klicken Sie erneut, um die Aufzeichnung anzuhalten. Wenn eine Aufzeichnung läuft, wird sie nach einem Neustart automatisch fortgesetzt.

#### Hinweis

Sie können nur zuhören und aufzeichnen, wenn der Eingang für das Gerät aktiviert ist. Wechseln Sie zu **Audio > Device settings (Audio > Geräteeinstellungen)**, um sicherzustellen, dass der Eingang aktiviert ist.



zeigt den konfigurierten Speicher für das Gerät an. Melden Sie sich als Administrator an, um den Speicher zu konfigurieren.

### Sicherheit des Audiostandorts

**CA-Zertifikat:** Wählen Sie das Zertifikat aus, das beim Hinzufügen von Geräten zum Audio-Standort verwendet werden soll. Sie müssen die TLS-Authentifizierung in AXIS Audio Manager Edge aktivieren.

**Save (Speichern):** Auswahl aktivieren und speichern.

### Aufzeichnungen



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.

**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.





# AXIS C8210 Network Audio Amplifier

## Die Weboberfläche


 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.

## 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.

# AXIS C8210 Network Audio Amplifier

## Die Weboberfläche

Falls Sie keinen Lizenzschlüssel besitzen, gehen Sie zu [axis.com/products/analytics](http://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.

**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.

# AXIS C8210 Network Audio Amplifier

## Die Weboberfläche

---

### 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.

### 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)

# AXIS C8210 Network Audio Amplifier

## Die Weboberfläche

---

**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

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](https://axis.com/end-to-end-solutions/hosted-services).

# AXIS C8210 Network Audio Amplifier

## Die Weboberfläche

### 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

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

**SNMP:** Wählen Sie die zu verwendende SNMP-Version.

- **v1 und v2c:**
  - **Lese-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.

# AXIS C8210 Network Audio Amplifier

## Die Weboberfläche

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.

- **Kenntwort 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.

## Sicherheit

### Zertifikate

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 Wählenden sicheren Schlüsselspeicher finden Sie unter [help.axis.com/en-us/axis-os#cryptographic-support](http://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)

# AXIS C8210 Network Audio Amplifier

## Die Weboberfläche

### 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:

- **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

# AXIS C8210 Network Audio Amplifier

## Die Weboberfläche

**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 Geräteebene 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 Ofestgelegt 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.

### Benutzerdefiniertes signiertes AXIS OS-Zertifikat



# AXIS C8210 Network Audio Amplifier

## Die Weboberfläche

---

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:** Darf keine Änderungen an den Einstellungen vornehmen.




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)

# AXIS C8210 Network Audio Amplifier

## Die Weboberfläche

---



**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.

### 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.

# AXIS C8210 Network Audio Amplifier

## Die Weboberfläche

**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 unter *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.

# AXIS C8210 Network Audio Amplifier

## Die Weboberfläche

**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*.

Ihr Produkt verfügt möglicherweise über einige der folgenden vorkonfigurierten Regeln:

**Front-facing LED Activation: LiveStream (Aktivierung der Front-LED: LiveStream):** Wenn das Mikrofon eingeschaltet ist und ein Live-Stream empfangen wird, wird die Front-LED des Audiogeräts grün.

**Front-facing LED Activation: Recording (Aktivierung der Front-LED: Aufzeichnung):** Wenn das Mikrofon eingeschaltet ist und eine Aufzeichnung läuft, wird die Front-LED des Audiogeräts grün.

**Front-facing LED Activation: SIP (Aktivierung der Front-LED: SIP):** Wenn das Mikrofon eingeschaltet ist und ein SIP-Anruf aktiv ist, ist die Front-LED des Audiogeräts grün. SIP muss auf dem Audiogerät aktiviert sein, bevor dieses Ereignis ausgelöst werden kann.

**Pre-announcement tone: Play tone on incoming call (Ton vor der Ansage: Ton bei eingehendem Anruf abspielen):** Wenn ein SIP-Anruf beim Audiogerät erfolgt, wird vom Gerät ein vordefinierter Audioclip abgespielt. SIP muss für das Audiogerät aktiviert sein. Damit der SIP-Anrufer einen Klingelton hört, während der Audioclip abgespielt wird, muss das SIP-Konto des Audiogeräts so konfiguriert werden, dass es den Anruf nicht automatisch beantwortet.

**Pre-announcement tone: Answer call after incoming call-tone (Ton vor der Ansage: Anruf nach dem Ton für eingehende Anrufe beantworten):** Nach dem Ende des Audioclips wird der eingehende SIP-Anruf beantwortet. SIP muss für das Audiogerät aktiviert sein.

**Loud ringer (Lauter Klingelton):** Wenn ein SIP-Anruf beim Audiogerät erfolgt, wird ein vordefinierter Audioclip abgespielt, solange die Regel aktiv ist. SIP muss für das Audiogerät aktiviert sein.

### Empfänger

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-Zielserver zum Öffnen der Datenverbindung auf. Normalerweise initiiert das Gerät die FTP-Steuerung und die Datenverbindungen zum Zielservers. Dies ist in der Regel erforderlich, wenn zwischen dem Gerät und dem FTP-Zielservers eine Firewall eingerichtet ist.
- **HTTP**

# AXIS C8210 Network Audio Amplifier

## Die Weboberfläche

- **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.
  - **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.

# AXIS C8210 Network Audio Amplifier

## Die Weboberfläche

- **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.

### 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.

# AXIS C8210 Network Audio Amplifier

## Die Weboberfläche

---

### 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 die 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.

#### Broker

**Host:** 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

# AXIS C8210 Network Audio Amplifier

## Die Weboberfläche

**Device topic prefix (Themenpräfix des Geräts):** Wird in den Standardwerten für das Thema in der Verbindungsnachricht und der LWT-Nachricht auf der Registerkarte **MQTT Client** und in den Veröffentlichungsbedingungen auf der Registerkarte **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 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-Namespaces 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 Meldungen werden als nicht beibehalten gesendet.
- **Property (Eigenschaft):** Es werden nur statusbehaftete Meldungen als beibehalten gesendet.
- **Alle:** Es werden nur statuslose Meldungen als beibehalten gesendet.



# AXIS C8210 Network Audio Amplifier

## Die Weboberfläche

---

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.

## SIP

### Settings (Einstellungen)

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

**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.

# AXIS C8210 Network Audio Amplifier

## Die Weboberfläche

- **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 Netzwerkumgebung richten.

- **ICE:** Das Protokoll ICE (Interactive Connectivity Establishment) erhöht die Chancen, den effizientesten Kommunikationspfad zwischen gleichrangigen Geräten zu finden. Mit dem Aktivieren von STUN und TURN werden die Chancen des ICE-Protokolls nochmals verbessert.
- **STUN:** STUN (Session Traversal Utilities for NAT) ist ein Client-Server-Netzwerkprotokoll, an dem 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

- **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.

### Zusätzliches

- **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)

# AXIS C8210 Network Audio Amplifier



## Die Weboberfläche

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.
- **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.

# AXIS C8210 Network Audio Amplifier

## Die Weboberfläche

- **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.

## Speicher

### Network storage (Netzwerk-Speicher)

**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](#).

# AXIS C8210 Network Audio Amplifier

## Die Weboberfläche

- **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.
- **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.

# AXIS C8210 Network Audio Amplifier

## Die Weboberfläche

- **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.

## 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](http://axis.com).



**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 ein.

**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.

# AXIS C8210 Network Audio Amplifier

## Die Weboberfläche



**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.

- **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.



# AXIS C8210 Network Audio Amplifier

## Die Weboberfläche

### Melder

#### 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.

### Zubehör



#### E/A-Ports



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.

#### Port

**Name:** 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



# AXIS C8210 Network Audio Amplifier

## Die Weboberfläche

### 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 Anmeldekennwort 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

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.

# AXIS C8210 Network Audio Amplifier

## Die Weboberfläche

---

### 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](http://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](http://axis.com/support) auf.

Bei der Aktualisierung können Sie zwischen drei Optionen wählen:

- **Standard upgrade (Standardaktualisierung):** Aktualisieren Sie auf die neue AXIS OS-Version.
- **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 C8210 Network Audio Amplifier

## Fehlerbehebung

---

### Fehlerbehebung

#### Zurücksetzen auf die Werkseinstellungen

##### Wichtig

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

Zurücksetzen des Produktes auf die werkseitigen Standardeinstellungen:

1. Trennen Sie das Produkt von der Stromversorgung.
2. Halten Sie die Steuertaste gedrückt und stellen Sie die Stromversorgung wieder her. Siehe *Produktübersicht auf Seite 46*.
3. Halten Sie die Steuertaste 10 Sekunden gedrückt, bis die Status-LED zum zweiten Mal gelb leuchtet.
4. Lassen Sie die Steuertaste los. Der Vorgang ist abgeschlossen, wenn die Status-LED grün leuchtet. Das Produkt wurde auf die Werkseinstellungen zurückgesetzt. Wenn kein DHCP-Server im Netzwerk verfügbar ist, lautet die Standard-IP-Adresse 192.168.0.90.
5. Mithilfe der Softwaretools für das Installieren und Verwalten, IP-Adressen zuweisen, das Kennwort festlegen und auf das Produkt zugreifen.

Die Parameter können auch über die Weboberfläche auf die Werkseinstellungen zurückgesetzt werden. **Wartung > Wartungsaktionen** aufrufen und auf **wiederherstellen** klicken, um auf die werkseitigen Standardwerte zurückzusetzen, aber die IP-Adresse beizubehalten, oder **Standard**, um alle Werte einschließlich der IP-Adresse zurücksetzen.

#### Die aktuelle Firmware überprüfen

Firmware ist die Software mit der die Funktionalität von Netzwerk-Geräten festgelegt wird. Eine der ersten Maßnahmen bei der Fehlerbehebung sollte das Prüfen der aktuellen Firmware-Version sein. Die aktuelle Version enthält möglicherweise eine Verbesserung, die das Problem behebt.

Um die aktuelle Firmware zu überprüfen:

1. Auf der Webseite des Geräts, **Übersicht** aufrufen.
2. Überprüfen Sie die **Firmware-Version**.

#### Die Firmware aktualisieren

##### Wichtig

Vorkonfigurierte und angepasste Einstellungen werden beim Aktualisieren der Firmware gespeichert (vorausgesetzt die Funktionen sind als Teil der neuen Firmware verfügbar). Dies wird von Axis Communications AB jedoch nicht garantiert.

##### Wichtig

Sicherstellen, dass das Gerät während der Aktualisierung an die Stromversorgung angeschlossen ist.

##### Hinweis

Beim Aktualisieren des Geräts mit der aktuellen Firmware wird dieses mit den neuesten Funktionsmerkmalen versehen. Vor der Aktualisierung der Firmware stets die entsprechenden Aktualisierungsanweisungen und Versionshinweise lesen. Die aktuelle Version der Firmware und die Versionshinweise stehen unter [axis.com/support/firmware](http://axis.com/support/firmware) bereit.

1. Die aktuelle Version der Firmware steht auf der Axis Website unter [www.axis.com/support/firmware](http://www.axis.com/support/firmware) zum kostenlosen Herunterladen bereit.
2. Melden Sie sich auf dem Gerät als Administrator an.

# AXIS C8210 Network Audio Amplifier

## Fehlerbehebung

---

3. Gehen Sie zu **System > Wartung > Firmwareaktualisierung** und befolgen Sie die Anweisungen auf der Seite. Nach der Aktualisierung wird das Gerät automatisch neu gestartet.

### Technische Probleme, Hinweise und Lösungen

Falls Sie hier nicht das Gesuchte finden, bitte den Bereich "Fehlerbehebung" unter [axis.com/support](http://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): |
|---|--|

- Wenn Folgendes angezeigt wird: `Reply from (Antwort von)<IP address>: bytes=32; time=10...` 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: `Request timed out` bedeutet, dass die IP-Adresse mit dem Axis Gerät verwendet werden kann. Prüfen Sie alle Kabel und installieren Sie das Gerät erneut.

|  |   |
|--|---|
| 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 werksseitigen Standardeinstellungen zurückgesetzt werden. Siehe *Zurücksetzen auf die Werkseinstellungen auf Seite 43*.

|  |  |
|--|--|
| Die IP-Adresse wurde von DHCP geändert | Von einem DHCP-Server zugewiesene 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 Camera Station Video Management Software: Kostenlose 30-Tage-Testversion, ideal für kleine bis mittelgroße Systeme.

Auf [axis.com/vms](http://axis.com/vms) finden Sie Anweisungen und die Download-Datei.

# AXIS C8210 Network Audio Amplifier

## Fehlerbehebung

---

### Probleme mit Sounddateien

---

Medienclip kann nicht hochgeladen werden

Folgende Audioclipformate werden unterstützt:

- au-Dateiformat, in  $\mu$ -law codiert und mit 8 oder 16 kHz abtastiert.
- wav-Dateiformat, in PCM-Audio codiert. Codierung als 8- oder 16-Bit-Mono oder Stereo und eine Abtastrate von 8 bis 48 kHz werden unterstützt.
- mp3-Dateiformat, mono oder stereo, mit einer Bitrate von 64 bis 320 kHz und einer Abtastrate von 8 bis 48 kHz.

Medienclips werden in unterschiedlicher Lautstärke abgespielt.

Eine Sounddatei wird mit einer bestimmten Verstärkung aufgezeichnet. Wenn bei der Erstellungen Ihrer Audioclips verschiedenen Verstärkungsarten eingestellt waren, werden sie in unterschiedlicher Lautstärke abgespielt. Stellen Sie sicher, dass Sie Clips mit derselben Verstärkung verwenden.

### Leistungsaspekte

Achten Sie beim Einrichten Ihres Systems unbedingt darauf, wie sich die verschiedenen Einstellungen und Situationen auf die erforderliche Menge der benötigten Bandbreite (die Bitrate) auswirken.

Die folgenden wichtigen Faktoren müssen beachtet werden:

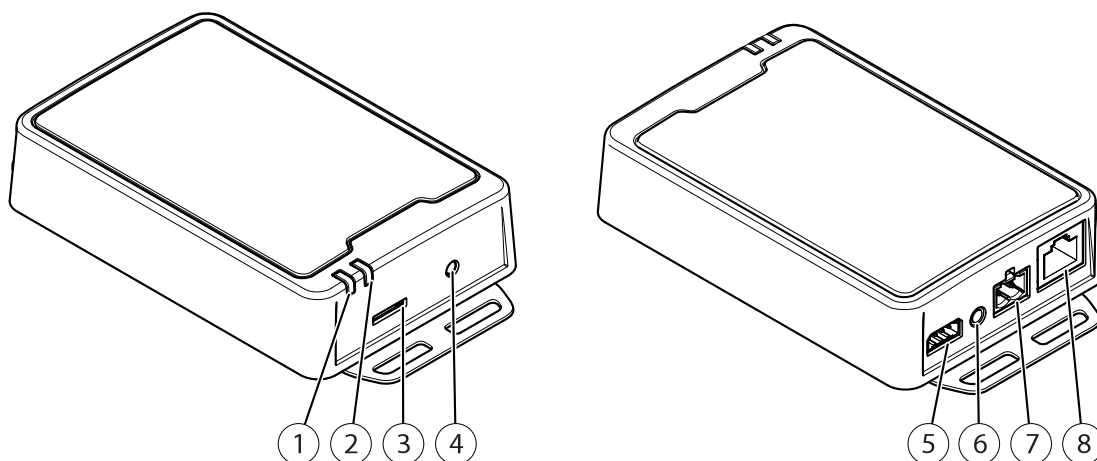
- Intensive Netzwerknutzung aufgrund mangelhafter Infrastruktur beeinflusst die Bandbreite.
- Mehrere gleichzeitig ausgeführte ACAP-Anwendungen (AXIS Camera Application Platform) können die allgemeine Leistung beeinflussen.

# AXIS C8210 Network Audio Amplifier

## Technische Daten

### Technische Daten

### Produktübersicht



- 1 Status-LED
- 2 Lautsprecher-LED
- 3 Einschub für SD-Speicherkarten
- 4 Steuertaste
- 5 E/A-Anschluss
- 6 Anschluss für Audioeingang
- 7 Lautsprecher-Anschluss
- 8 Netzwerk-Anschluss

### LEDs

| LED-Statusanzeige | Bedeutung   |
|-------------------|---|
| Leuchtet nicht    | Leuchtet im Normalbetrieb nicht                                   |
| Grün              | Leuchtet bei Normalbetrieb grün.                                  |
| Gelb              | Leuchtet beim Start und beim Wiederherstellen der Einstellungen.  |
| Rot               | Blinkt langsam bei einem Aktualisierungsfehler.                   |
| Rot/Grün          | Schneller Wechsel zwischen Rot und Grün – Wahl eines Audiogeräts. |

| SPK-LED | Bedeutung  |
|---------|--|
| Grün    | Leuchtet bei Normalbetrieb grün.<br>Blinkt (zwei Mal kurz in grün und ein Mal lange ohne Licht), wenn die Impedanz nicht kalibriert wurde. |
| Rot     | Blinkt rot, wenn der Überstromschutz ausgelöst wurde.  |

# AXIS C8210 Network Audio Amplifier

## Technische Daten

### 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.

Empfehlungen zu SD-Karten finden Sie auf [axis.com](http://axis.com).



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

### Tasten

#### Steuertaste

Drücken Sie die Steuertaste, um einen Impedanztest durchzuführen. Halten Sie die Steuertaste gedrückt, bis Sie die Töne des Lautsprechers hören. Weitere Informationen siehe *Testen Sie die Impedanz auf Seite 6*.

### Anschlüsse

#### Netzwerk-Anschluss

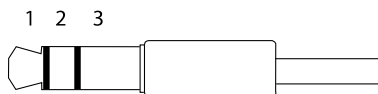
RJ45-Ethernetanschluss mit Power over Ethernet Plus (PoE+).

#### HINWEIS

Das Produkt muss mit einem geschirmten Netzwerk-Kabel (STP) angeschlossen werden. Alle Kabel, die das Produkt mit dem Netzwerk-Switch verbinden, müssen hierfür ausgelegt sein. Sicherstellen, dass die Netzwerk-Geräte gemäß den Anweisungen des Herstellers installiert werden. Informationen zu gesetzlichen Bestimmungen finden Sie im Installationshandbuch auf [www.axis.com](http://www.axis.com).

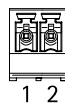
#### Audioanschluss

- Audioeingang – 3,5 mm, für ein Monomikrofon oder ein Monosignal (der linke Kanal wird von einem Stereosignal genutzt).



|              | 1 Spitze               | 2 Ring               | 3 Hülse |
|--------------|------------------------|----------------------|---------|
| Audioeingang | Eingang Mikrofon/Audio | Mikrofon-Vorspannung | Erdung  |

2-poliger Anschlussblock für Lautsprecherausgang.



# AXIS C8210 Network Audio Amplifier

## Technische Daten

| Funktion             | Kontakt | Hinweise |
|----------------------|---------|----------|
| Lautsprecher aus (-) | 1       |          |
| Lautsprecher aus (+) | 2       |          |

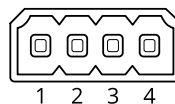
### E/A-Anschluss

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.

4-poliger Anschlussblock



| 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<br>Max. Stromstärke = 50 mA             |
| Konfigurierbar (Ein- oder Ausgang) | 3-4     | 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 |

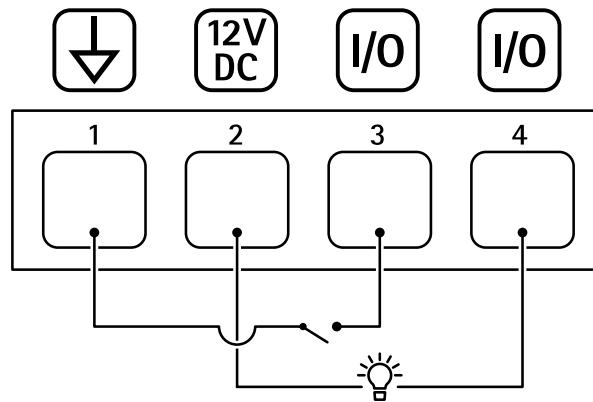
Beispiel:



# AXIS C8210 Network Audio Amplifier

## Technische Daten

---



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

# AXIS C8210 Network Audio Amplifier

## API-Befehle

---

### API-Befehle

VAPIX® ist die eigene offene API (Application Programming Interface) von Axis. Über VAPIX® können fast alle Funktionen, die in Axis Geräten zur Verfügung stehen, gesteuert werden. Um auf die gesamte VAPIX®-Dokumentation zugreifen zu können, treten Sie der *Axis Developer Community* unter [axis.com/developer-Community](http://axis.com/developer-Community) bei

Geben Sie die Befehle in einem Webbrowser ein und ersetzen Sie `<deviceIP>` durch die IP-Adresse oder den Host-Namen Ihres Geräts.

#### Wichtig

Die API-Befehle werden sofort ausgeführt. Wenn Sie das Gerät wiederherstellen oder zurücksetzen, gehen alle Einstellungen verloren. Zum Beispiel Aktionsregeln.

#### Beispiel:

Gerät neu starten

#### Anforderung

`http://<deviceIP>/axis-cgi/restart.cgi`

#### Beispiel:

Das Gerät zurücksetzen. Die Anforderung setzt die meisten Einstellungen auf die Standardwerte zurück, die IP-Nummer bleibt aber erhalten.

#### Anforderung

`http://<deviceIP>/axis-cgi/factorydefault.cgi`

#### Beispiel:

Das Gerät zurücksetzen. Die Anforderung setzt alle Einstellungen einschließlich der IP-Nummer auf die Standardwerte zurück.

#### Anforderung

`http://<deviceIP>/axis-cgi/hardfactorydefault.cgi`

#### Beispiel:

Siehe Liste aller Geräteparameter.

#### Anforderung

`http://<deviceIP>/axis-cgi/param.cgi?action=list`

#### Beispiel:

Debug-Archiv abrufen

#### Anforderung

`http://<deviceIP>/axis-cgi/debug/debug.tgz`

#### Beispiel:

Server-Bericht abrufen

#### Anforderung

`http://<deviceIP>/axis-cgi/serverreport.cgi`

#### Beispiel:

Netzwerk-Trace von 300 Sekunden aufnehmen

#### Anforderung

`http://<deviceIP>/axis-cgi/debug/debug.tgz?cmd=pcapdump&duration=300`

#### Beispiel:

FTP aktivieren

# AXIS C8210 Network Audio Amplifier

## API-Befehle

---

**Anforderung**

`http://<deviceIP>/axis-cgi/param.cgi?action=update&Network.FTP.Enabled=yes`

**Beispiel:**

FTP deaktivieren

**Anforderung**

`http://<deviceIP>/axis-cgi/param.cgi?action=update&Network.FTP.Enabled=no`

**Beispiel:**

SSH aktivieren

**Anforderung**

`http://<deviceIP>/axis-cgi/param.cgi?action=update&Network.SSH.Enabled=yes`

**Beispiel:**

SSH deaktivieren

**Anforderung**

`http://<deviceIP>/axis-cgi/param.cgi?action=update&Network.SSH.Enabled=no`

