

AXIS D3110 Mk II Connectivity Hub

Panoramica delle soluzioni

Questo dispositivo consente l'integrazione di sensori e audio in sistemi video di rete che non dispongono di tali capacità o che hanno bisogno di ulteriori capacità sensore e audio. Ideale in una soluzione end-to-end Axis, ti aiuta ad avere un quadro più completo della scena senza compromettere la sicurezza della rete.

Se si utilizza un software per la gestione audio o video, è possibile utilizzare tale software per configurare il dispositivo. Il seguente software di gestione è disponibile per il controllo del sistema audio:

- **AXIS Audio Manager Edge:** software per la gestione audio per piccoli sistemi. Viene preinstallato su tutti i dispositivi audio con un firmware 10.0 o versione successiva.
 - *Manuale per l'utente di AXIS Audio Manager Edge*
- **AXIS Audio Manager Pro:** software di gestione dell'audio avanzato per sistemi di grandi dimensioni.
 - *Manuale per l'utente di AXIS Audio Manager Pro*
- **AXIS Audio Manager Center** – Servizio cloud per l'accesso e la gestione remota di sistemi multisito.
 - *Manuale per l'utente di AXIS Audio Manager Center*

Per ulteriori informazioni, consultare *Software per la gestione audio*.

Installazione



Per guardare questo video, andare alla versione web di questo documento.

Impostazioni preliminari

Individuazione del dispositivo sulla rete

Per trovare i dispositivi Axis sulla rete e assegnare loro un indirizzo IP in Windows®, utilizza AXIS IP Utility o AXIS Device Manager. Queste applicazioni sono entrambe gratuite e possono essere scaricate dal sito Web axis.com/support.

Per ulteriori informazioni su come trovare e assegnare indirizzi IP, andare alla sezione *Come assegnare un indirizzo IP e accedere al dispositivo*.

Supporto browser

Il dispositivo può essere utilizzato con i seguenti browser:

	Chrome™	Edge™	Firefox®	Safari®
Windows®	✓	✓	*	*
macOS®	✓	✓	*	*
Linux®	✓	✓	*	*
Altri sistemi operativi	*	*	*	*

✓: Consigliato

*: Supportato con limitazioni

Aprire l'interfaccia Web del dispositivo

1. Aprire un browser e digitare il nome di host o l'indirizzo IP del dispositivo Axis.
Se non si conosce l'indirizzo IP, utilizzare AXIS IP Utility oppure AXIS Device Manager per individuare il dispositivo sulla rete.
2. Digitare il nome utente e password. Se si accede al dispositivo per la prima volta, è necessario creare un account amministratore. Vedere *Crea un account amministratore, on page 4*.

Per le descrizioni di tutte le funzioni e impostazioni dell'interfaccia Web dei dispositivi con AXIS OS, consultare *Guida all'interfaccia Web di AXIS OS*.

Crea un account amministratore

La prima volta che si accede al dispositivo, è necessario creare un account amministratore.

1. Inserire un nome utente.
2. Inserire una password. Vedere *Password sicure, on page 5*.
3. Reinserire la password.
4. Accettare il contratto di licenza.
5. Fare clic su **Add account (Aggiungi account)**.

Importante

Il dispositivo non ha un account predefinito. In caso di smarrimento della password dell'account amministratore, è necessario reimpostare il dispositivo. Vedere *Ripristino delle impostazioni predefinite di fabbrica, on page 18*.

Password sicure

Importante

Utilizzare HTTPS (abilitato per impostazione predefinita) per impostare la password o altre configurazioni sensibili in rete. HTTPS consente connessioni di rete sicure e crittografate, proteggendo così i dati sensibili, come le password.

La password del dispositivo è il sistema di protezione principale dei dati e dei servizi. I dispositivi Axis non impongono criteri relativi alla password poiché i dispositivi potrebbero essere utilizzati in vari tipi di installazioni.

Per proteggere i dati consigliamo vivamente di:

- Utilizzare una password con almeno 8 caratteri, creata preferibilmente da un generatore di password.
- Non mostrare la password.
- Cambiare la password a intervalli regolari, almeno una volta all'anno.

Verificare che nessuno abbia alterato il software del dispositivo

Per verificare che il dispositivo disponga del firmware AXIS OS originale o per prendere il controllo completo del dispositivo dopo un attacco alla sicurezza:

1. Ripristinare le impostazioni predefinite di fabbrica. Vedere *Ripristino delle impostazioni predefinite di fabbrica, on page 18*.
Dopo il ripristino, l'avvio sicuro garantisce lo stato del dispositivo.
2. Configurare e installare il dispositivo.

Configurare il dispositivo

In questa sezione sono illustrate tutte le configurazioni importanti che un installatore deve eseguire per rendere il dispositivo operativo dopo aver completato l'installazione dell'hardware.

Imposta regole per eventi

Per ulteriori informazioni, consultare *Guida iniziale per le regole eventi*.

Attivazione di un'azione

1. Andare a **System > Events (Sistema > Eventi)** e aggiungere una regola. La regola consente di definire quando il dispositivo eseguirà determinate azioni. È possibile impostare regole pianificate, ricorrenti o attivate manualmente.
2. Immettere un **Name (Nome)**.
3. Selezionare la **Condition (Condizione)** che deve essere soddisfatta per attivare l'azione. Se si specifica più di una condizione per la regola, devono essere soddisfatte tutte le condizioni per attivare l'azione.
4. Selezionare quale **Action (Azione)** eseguire quando le condizioni sono soddisfatte.

Rilevamento manomissione con segnale di input

In questo esempio viene spiegato come inviare un e-mail in caso di interruzione o corto circuito del segnale di input. Per ulteriori informazioni sul connettore I/O, vedere *page 14*.

1. Andare in **System (Sistema) > Accessories (Accessori) > I/O ports (Porte I/O)** e attivare **Supervised (Supervisionato)** per una delle relative porte.

Aggiungere un destinatario e-mail:

1. Andare a **System > Events > Recipients (Sistema > Eventi > Destinatari)** e aggiungere un destinatario.
2. Immettere un nome per il destinatario.
3. Selezionare **Email (E-mail)** come tipo di notifica.
4. Digitare l'indirizzo e-mail del destinatario.
5. Digitare l'indirizzo e-mail da cui si desidera che la telecamera invii le notifiche.
6. Indicare i dati di accesso all'account dell'e-mail di invio, insieme al nome host e al numero di porta SMTP.
7. Per verificare la configurazione della posta elettronica, fare clic su **Test (Prova)**.
8. Fare clic su **Save (Salva)**.

Creare una regola:

1. Andare a **System > Events > Rules (Sistema > Eventi > Regole)** e aggiungere una regola.
2. Inserire un nome per la regola.
3. Nell'elenco delle condizioni, in **I/O**, selezionare **Supervised input tampering is active (Supervisione manomissione input attiva)**.
4. Selezionare la relativa porta.
5. Nell'elenco delle azioni, in **Notifications (Notifiche)**, selezionare **Send notification to email (Invia notifica all'indirizzo e-mail)**, quindi selezionare il destinatario dall'elenco.
6. Digitare un oggetto e il messaggio per l'e-mail.
7. Fare clic su **Save (Salva)**.

Attiva una lampada quando si apre la finestra

Questo esempio illustra il modo di connettere un contatto di una finestra a un hub di connettività e il modo di impostare un evento che attivi una lampada quando si apre una finestra con un contatto.

Prerequisiti

- Connetti un cavo con 2 fili (massa, I/O) al contatto della finestra e al connettore I/O sull'hub di connettività.
- Connetti la lampada all'alimentazione e al connettore relè sull'hub di connettività.

Configura le porte I/O nell'hub di connettività

1. Andare a **System > Accessories (Sistema > Accessori)**.
2. Immettere le seguenti informazioni in **Port 1 (Porta 1)**:
 - **Nome**: Sensore finestra
 - **Direction (Direzione)**: Ingresso
 - **Normal state (Stato normale)**: Circuito chiuso
3. Immettere le seguenti informazioni in **Port 2 (Porta 2)**:
 - **Nome**: Lampada
 - **Direction (Direzione)**: Uscita
 - **Normal state (Stato normale)**: Circuito aperto

Crea due regole nell'hub di connettività

1. Andare a **System > Events (Sistema > Eventi)** e aggiungere una regola.
2. Immettere le seguenti informazioni:
 - **Nome**: Sensore finestra
 - **Condition (Condizione)**: Ingresso digitale
Seleziona **Use this condition as a trigger (Utilizza questa condizione come trigger)**
 - **Porta**: Sensore finestra
 - **Action (Azione)**: Attiva/disattiva I/O mentre la regola è attiva
 - **Porta**: Lampada
 - **State (Stato)**: Attivo
3. Fare clic su **Save (Salva)**.

Attivazione dell'hub di connettività su MQTT quando la telecamera rileva movimento

Prerequisiti

- Configura un dispositivo per la porta I/O 1 nell'hub di connettività.
- Imposta un broker MQTT e ottieni l'indirizzo IP, il nome utente e la password del broker.
- Configurare AXIS Motion Guard nella telecamera.

Configura il client MQTT nella telecamera

1. Nell'interfaccia dispositivo della telecamera, vai su **System > MQTT > MQTT client > Broker (Sistema > MQTT > Client MQTT > Broker)** e immetti le seguenti informazioni:
 - **Host**: Indirizzo IP broker
 - **Client ID (ID client)**: Ad es., Telecamera 1
 - **Protocol (Protocollo)**: Il protocollo su cui è impostato il broker
 - **Porta**: Il numero di porta utilizzato dal broker
 - **Username (Nome utente)** e **Password** del broker
2. Fare clic su **Save (Salva)** e **Connect (Connetti)**.

Creazione di due regole nella telecamera per la pubblicazione MQTT

1. Andare a **System > Events > Rules (Sistema > Eventi > Regole)** e aggiungere una regola.
2. Immettere le seguenti informazioni:
 - **Nome**: Oggetti in movimento rilevati
 - **Condition (Condizione)**: **Applications > Motion alarm (Applicazioni > Allarme di movimento)**

- **Action (Azione):** MQTT > Send MQTT publish message (MQTT > Invia messaggio di pubblicazione MQTT)
 - **Topic (Argomento):** Movimento
 - **Payload:** On
 - **QoS:** 0, 1 o 2
3. Fare clic su **Save (Salva)**.
 4. Aggiungere un'altra regola con le seguenti informazioni:
 - **Nome:** Nessun movimento
 - **Condition (Condizione):** Applications > Motion alarm (Applicazioni > Allarme di movimento)
 - Seleziona **Invert this condition (Inverti questa condizione)**.
 - **Action (Azione):** MQTT > Send MQTT publish message (MQTT > Invia messaggio di pubblicazione MQTT)
 - **Topic (Argomento):** Movimento
 - **Payload:** Off
 - **QoS:** 0, 1 o 2
 5. Fare clic su **Save (Salva)**.

Imposta il client MQTT nell'hub di connettività

1. Nell'interfaccia dispositivo dell'hub di connettività, vai su **System > MQTT > MQTT client > Broker** (**Sistema > MQTT > Client MQTT > Broker**) e immetti le seguenti informazioni:
 - **Host:** Indirizzo IP broker
 - **Client ID (ID client):** Porta 1
 - **Protocol (Protocollo):** Il protocollo su cui è impostato il broker
 - **Porta:** Il numero di porta utilizzato dal broker
 - **Username (Nome utente) e Password**
2. Fare clic su **Save (Salva)** e **Connect (Connetti)**.
3. Vai su **MQTT subscriptions (Sottoscrizioni MQTT)** e aggiungi una sottoscrizione. Immettere le seguenti informazioni:
 - **Subscription filter (Filtro sottoscrizione):** Movimento
 - **Subscription type (Tipo di sottoscrizione):** Dotato di stato
 - **QoS:** 0, 1 o 2
4. Fare clic su **Save (Salva)**.

Creazione di una regola nell'hub di connettività per le sottoscrizioni MQTT

1. Andare a **System > Events > Rules** (**Sistema > Eventi > Regole**) e aggiungere una regola.
2. Immettere le seguenti informazioni:
 - **Nome:** Oggetti in movimento rilevati
 - **Condition (Condizione):** MQTT > Stateful (MQTT > Dotato di stato)
 - **Subscription filter (Filtro sottoscrizione):** Movimento
 - **Payload:** On
 - **Action (Azione):** I/O > Toggle I/O while the rule is active (**Attiva/disattiva l'I/O mentre la regola è attiva**)
 - **Port (Porta):** I/O 1.
3. Fare clic su **Save (Salva)**.

Apertura di una serratura quando si preme un pulsante

Questo esempio illustra in che modo si connette un relè all'hub di connettività e come si imposta un evento di apertura di una serratura quando qualcuno preme un pulsante collegato all'hub di connettività.

Prerequisiti

- Connetti un cavo con 2 fili (COM, NO) alla serratura e al connettore relè sull'hub di connettività.
- Connetti un cavo con 2 fili (massa, I/O) al pulsante e al connettore I/O sull'hub di connettività.

Configura le porte I/O nell'hub di connettività

1. Andare a **System > Accessories (Sistema > Accessori)**.
2. Immettere le seguenti informazioni in **Port 1 (Porta 1)**:
 - **Nome**: Pulsante
 - **Direction (Direzione)**: Ingresso
 - **Normal state (Stato normale)**: Circuito aperto
3. Immettere le seguenti informazioni in **Port 9 (Porta 9)**:
 - **Nome**: Serratura
 - **Normal state (Stato normale)**: Circuito aperto

Crea una regola nell'hub di connettività

1. Andare a **System > Events (Sistema > Eventi)** e aggiungere una regola.
2. Immettere le seguenti informazioni:
 - **Nome**: Apri serratura
 - **Condition (Condizione)**: I/O > Digital input is active (Input digitale attivo)
Seleziona Use this condition as a trigger (Utilizza questa condizione come trigger)
 - **Porta**: Pulsante
 - **Action (Azione)**: I/O > Toggle I/O once (Attiva/disattiva I/O una volta)
 - **Porta**: Serratura
 - **State (Stato)**: Attivo
 - **Duration (Durata)**: 10 s
3. Fare clic su **Save (Salva)**.

Audio

Registrazione audio nella scheda di memoria

Questo esempio illustra il modo di impostare la registrazione da due microfoni a una scheda di memoria.

Prima di iniziare

- Connetti due microfoni e inserisci una scheda microSD nell'hub di connettività.
1. Andare in **Audio > Device settings (Impostazioni dispositivo)** e attivare **Input 0: IN 1** e **Input 1: IN 2**.
 2. Seleziona **Input type (Tipo di ingresso)** e **Power type (Tipo di alimentazione)**.
 3. Se prevedi che i livelli sonori varino nella stanza, attiva **Automatic gain control (Controllo del guadagno automatico)**.
 4. Vai a **System > Storage > Onboard storage (Sistema > Archiviazione > Archiviazione integrata)** e imposta **Retention time (Tempo di conservazione)**.
 5. Vai a **Audio > Stream (Audio > Flusso)** e seleziona **Encoding (Codifica)**.

Nota

Per mantenere basso il carico della CPU quando esegui molteplici flussi (ad es. la registrazione e il flusso dal vivo dalla stessa sorgente), usa la stessa codifica per entrambi i flussi.

6. Andare in **Audio > Listen and record (Ascolta e registra)** e fare clic .
7. Fare clic su .

Interfaccia Web

Per informazioni su tutte le funzionalità e le impostazioni disponibili nell'interfaccia Web dei dispositivi con AXIS OS, andare a *Guida all'interfaccia Web di AXIS OS*.

Per saperne di più

Analisi e app

Le analisi e le app permettono di ottenere di più dal proprio dispositivo Axis. AXIS Camera Application Platform (ACAP) è una piattaforma aperta che permette a terze parti di sviluppare analisi e altre app per i dispositivi Axis. Le app possono essere preinstallate sul dispositivo oppure è possibile scaricarle gratuitamente o pagando una licenza.

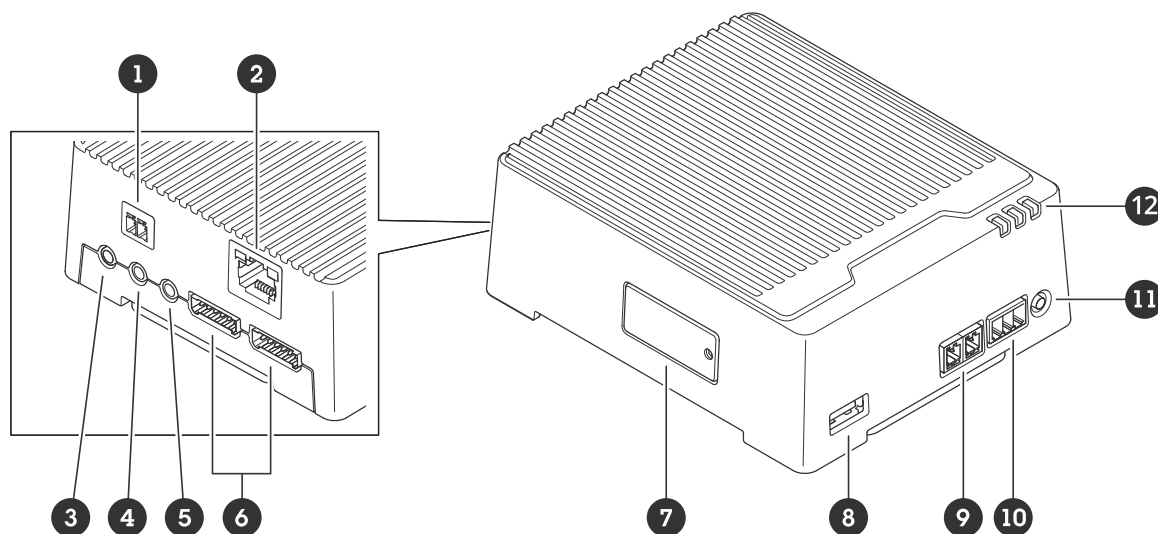
Per trovare i manuali per l'utente delle analisi e delle app Axis, visitare help.axis.com

AXIS Audio Analytics

AXIS Audio Analytics rileva aumenti improvvisi del volume sonoro e tipi specifici di suoni quali urla o grida entro la portata del dispositivo dov'è installato. Questi rilevamenti si possono configurare perché attivino una risposta, come registrare video, riprodurre un messaggio audio o inviare avvisi al personale di sicurezza. Per ulteriori informazioni su come funziona l'applicazione, consultare il *manuale per l'utente di AXIS Audio Analytics*.

Dati tecnici

Panoramica dei prodotti



- 1 Connettore di alimentazione
- 2 Connettore Ethernet RJ45
- 3 Porta microfono 2 (analogica)
- 4 Porta microfono 1 (digitale e analogica)
- 5 Uscita audio
- 6 2x connettori I/O (6 pin)
- 7 Slot per scheda MicroSD
- 8 Porta USB
- 9 Connettore RS485/RS422
- 10 Connettore relè
- 11 Pulsante di comando
- 12 LED di stato

Slot per scheda SD

Visitare axis.com per i consigli sulla scheda di memoria.



I loghi microSD, microSDHC e microSDXC sono tutti marchi registrati di SD-3C LLC. microSD, microSDHC, microSDXC sono marchi o marchi registrati di SD-3C, LLC negli Stati Uniti e/o in altri paesi.

Pulsanti

Pulsante di comando

Il pulsante di comando viene utilizzato per:

- Ripristino del dispositivo alle impostazioni predefinite di fabbrica. Vedere *Ripristino delle impostazioni predefinite di fabbrica, on page 18*.
- Connessione a servizio one-click cloud connection (O3C) su Internet. Per connettersi, premere e rilasciare il pulsante, quindi attendere che il LED di stato verde lampeggi tre volte.

Connettori

Connettore di rete

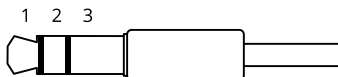
Connettore Ethernet RJ45.

Ingresso: Connettore Ethernet RJ45 con Power over Ethernet (PoE).

Documentazione prodotta: Connettore Ethernet RJ45 con Power over Ethernet (PoE).

Connettore audio

- **Audio in (Ingresso audio)** (microfono porta 1) - input da 3,5 mm per un microfono digitale, uno mono o un segnale mono line-in (il canale sinistro viene utilizzato da un segnale stereo).
- **Audio in (Ingresso audio)** (microfono porta 2) - input da 3,5 mm per un mono microfono analogico, o un segnale mono line-in (il canale sinistro viene utilizzato da un segnale stereo).
- **Uscita audio** - output da 3,5 mm per audio (line level) che è possibile collegare a un sistema di indirizzo pubblico (PA) o a un altoparlante attivo con amplificatore integrato. È possibile collegare anche delle cuffie. Per l'uscita audio è necessario utilizzare un connettore stereo.



Ingresso audio

1 Punta	2 Anello	3 Guaina
Microfono non bilanciato (con o senza alimentazione a elettrete) o ingresso linea	Alimentazione a elettrete se selezionata	Terra
Microfono bilanciato (con o senza alimentazione phantom) o ingresso linea, segnale "caldo"	Microfono bilanciato (con o senza alimentazione phantom) o ingresso linea, segnale "freddo"	Terra
Segnale digitale	Alimentazione anello se selezionata	Terra

Output audio

1 Punta	2 Anello	3 Guaina
Canale 1, linea non bilanciata, mono	Canale 1, linea non bilanciata, mono	Terra

Connettore I/O

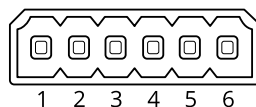
Utilizzare il connettore I/O con dispositivi esterni in combinazione con, ad esempio, rilevamento movimento, attivazione di eventi e notifiche di allarme. Oltre al punto di riferimento 0 V CC e all'alimentazione (output 12 V CC), il connettore I/O fornisce l'interfaccia per:

Ingresso digitale - Per il collegamento di dispositivi che possono passare da un circuito chiuso ad uno aperto, ad esempio i sensori PIR, i contatti porta/finestra e i rivelatori di rottura.

Input supervisionato - Consente di rilevare le manomissioni su un input digitale.

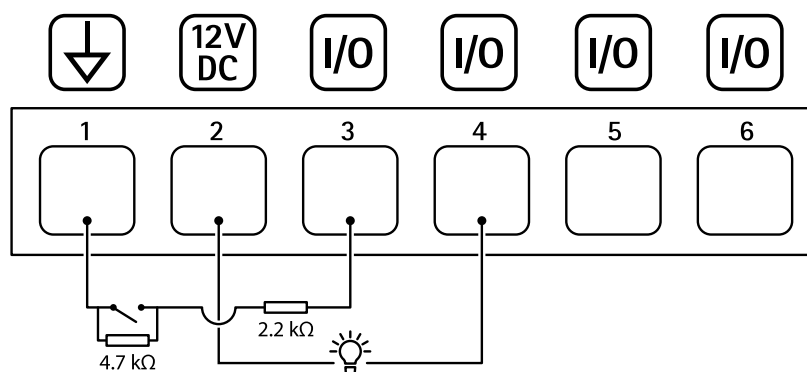
Uscita digitale - Per il collegamento di dispositivi esterni come relè e LED. I dispositivi collegati possono essere attivati tramite l'API (interfaccia per la programmazione di applicazioni) VAPIX® attraverso un evento oppure dall'interfaccia Web del dispositivo.

Morsettiera a 6 pin



Funzione	Pin	Note	Dati tecnici
Terra CC	1		0 V CC
Uscita CC	2	 Questo terminale può essere utilizzato anche per alimentare una periferica ausiliaria. Nota: questo pin può essere usato solo come uscita alimentazione.	12 V CC Carico massimo = 50 mA
Configurabile (ingresso o uscita)	3-6	Ingresso digitale o ingresso supervisionato - collegarlo al pin 1 per attivarlo oppure lasciarlo isolato (scollegato) per disattivarlo. Per utilizzare l'ingresso supervisionato, installare resistori terminali. Vedere il diagramma di connessione per informazioni su come collegare i resistori.	Da 0 a max 30 V CC
		Uscita digitale: collegato internamente al pin 1 (terra CC) quando attivo e isolato (scollegato) quando inattivo. Se utilizzata con un carico induttivo, ad esempio un relè, collegare un diodo in parallelo al carico per proteggere il dispositivo da sovratensioni.	Da 0 a max 30 V CC, open-drain, 100 mA

Esempio:



- 1 Terra CC
- 2 Output CC 12 V, max 50 mA
- 3 I/O configurato come ingresso supervisionato
- 4 I/O configurato come output
- 5 I/O configurabile
- 6 I/O configurabile

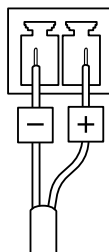
Specifiche di progettazione elettrica per I/O digitale

Parametro	Valore
Durata minima della tensione di input	-30 V CC
Durata massima della tensione di input	+30 V CC
Bassa tensione massima dell'input digitale	+0,50 V a 25 °C +0,40 V a 85 °C
Alta tensione minima dell'ingresso digitale	+1.5 V

Bassa tensione di uscita massima a 100 mA	+0.6 V
Bassa tensione di uscita massima a 10 mA	+0.06 V
Tempo di aumento massimo (compreso il ritardo dal GPIO) a 10 kHz	5 μ s
Tempo di diminuzione massimo (compreso il ritardo dal GPIO) a 10 kHz	5 μ s
Corrente di assorbimento in uscita massima	100 mA
Corrente di dispersione I/O massima	100 μ A a 12 V CC

Connettore di alimentazione

Morsettiera a 2 pin per ingresso alimentazione CC. Utilizzare una sorgente di alimentazione limitata (LPS) compatibile con una bassissima tensione di sicurezza (SELV) con una potenza di uscita nominale limitata a ≤ 100 W o una corrente nominale di uscita limitata a ≤ 5 A.

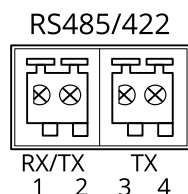


Connettore RS485/RS422

Due morsettiere a 2 pin per interfaccia seriale RS485/RS422.

La porta seriale può essere configurata per supportare:

- RS485 a due fili, half-duplex
- RS485 a quattro fili, full-duplex
- RS422 a due fili, simplex
- Comunicazione full-duplex punto a punto con RS422 a quattro fili



Funzione	Pin	Note
RS485/RS422 RX/TX A	1	(RX) Per RS485/RS422 full-duplex (RX/TX) per RS485 half-duplex
RS485/RS422 RX/TX B	2	
RS485/RS422 TX A	3	(TX) Per RS485/RS422 full-duplex
RS485/RS422 TX B	4	

Pulizia del dispositivo

È possibile pulire il dispositivo con acqua tiepida.

AVVISO

- Le sostanze chimiche possono danneggiare il dispositivo. Non utilizzare sostanze chimiche come detersivi per vetri o acetone per pulire il dispositivo.
 - Evitare la pulizia alla luce diretta del sole o a temperature elevate, poiché ciò può causare macchie.
1. Utilizzare una bomboletta d'aria compressa per rimuovere polvere e sporcizia dal dispositivo.
 2. Se necessario, pulire il dispositivo con un panno morbido in microfibra inumidito con acqua tiepida.
 3. Per evitare macchie, asciugare il dispositivo con un panno pulito e non abrasivo.

Per ulteriori informazioni sulla pulizia dei dispositivi Axis, consultare il documento tecnico *Resistenza chimica ai comuni prodotti per la pulizia*.

Risoluzione dei problemi

Ripristino delle impostazioni predefinite di fabbrica

Importante

Il ripristino dei valori predefiniti di fabbrica deve essere effettuato con cautela. Tale operazione consentirà di ripristinare i valori predefiniti di fabbrica per tutte le impostazioni, incluso l'indirizzo IP.

Per ripristinare il dispositivo alle impostazioni predefinite di fabbrica:

1. Scollegare l'alimentazione dal dispositivo.
2. Tenere premuto il pulsante di comando quando si ricollega l'alimentazione. Vedere *Panoramica dei prodotti*, on page 13.
3. Tenere premuto il pulsante di comando per circa 15-30 secondi fino a quando il LED di stato non lampeggia in giallo.
4. Rilasciare il pulsante di comando. La procedura è terminata quando il LED di stato diventa verde. Se nella rete non è disponibile un server DHCP, l'indirizzo IP del dispositivo sarà predefinito con uno dei seguenti:
 - **Dispositivi con AXIS OS 12.0 e successivo:** Ottenuto dal subnet dell'indirizzo di collegamento locale (169.254.0.0/16)
 - **Dispositivi con AXIS OS 11.11 e precedente:** 192.168.0.90/24
5. Utilizzare gli strumenti per l'installazione e la gestione del software per assegnare un indirizzo IP, impostare la password e accedere al dispositivo.
Gli strumenti per l'installazione e la gestione del software sono disponibili nelle pagine dedicate all'assistenza sul sito Web axis.com/support.

È inoltre possibile reimpostare i parametri ai valori predefiniti di fabbrica mediante l'interfaccia Web del dispositivo. Andare a **Maintenance (Manutenzione) > Factory default (Impostazione di fabbrica)** e fare clic su **Default (Predefinito)**.

Opzioni AXIS OS

Axis offre la gestione del software dei dispositivi in base alla traccia attiva o alle tracce di supporto a lungo termine (LTS). La traccia attiva consente di accedere continuamente a tutte le funzionalità più recenti del dispositivo, mentre le tracce LTS forniscono una piattaforma fissa con versioni periodiche incentrate principalmente sulle correzioni di bug e sugli aggiornamenti della sicurezza.

Si consiglia di utilizzare AXIS OS della traccia attiva se si desidera accedere alle funzionalità più recenti o se si utilizzano le offerte del sistema end-to-end Axis. Le tracce LTS sono consigliate se si utilizzano integrazioni di terze parti che non vengono convalidate continuamente a fronte della traccia attiva più recente. Con il supporto a lungo termine (LTS), i dispositivi possono mantenere la sicurezza informatica senza introdurre modifiche funzionali significative o compromettere eventuali integrazioni presenti. Per informazioni più dettagliate sulla strategia del software del dispositivo AXIS, visitare axis.com/support/device-software.

Controllo della versione corrente del AXIS OS

AXIS OS determina la funzionalità dei nostri dispositivi. Quando ti occupi della risoluzione di problemi, consigliamo di cominciare controllando la versione AXIS OS corrente. L'ultima versione potrebbe contenere una correzione che risolve il tuo particolare problema.

Per controllare la versione corrente di AXIS OS:

1. Andare all'interfaccia Web del dispositivo > **Status (Stato)**.
2. Vedere la versione AXIS OS in **Device info (Informazioni dispositivo)**.

Aggiornare AXIS OS

Importante

- Quando si esegue l'aggiornamento del software del dispositivo, le impostazioni preconfigurate e personalizzate vengono salvate. Axis Communications AB non può garantire il salvataggio delle impostazioni, anche se le funzionalità sono disponibili nella nuova versione del sistema operativo AXIS OS.
- A partire da AXIS OS 12.6, è necessario installare tutte le versioni LTS comprese tra la versione attuale del dispositivo e la versione di destinazione. Ad esempio, se la versione del software di installazione del dispositivo è AXIS OS 11.2, è necessario installare la versione LTS AXIS OS 11.11 prima di poter effettuare l'aggiornamento del dispositivo ad AXIS OS 12.6. Per ulteriori informazioni, consultare *Guida al ciclo di vita AXIS OS: Percorso di aggiornamento*.
- Assicurarsi che il dispositivo rimanga collegato alla fonte di alimentazione durante il processo di aggiornamento.

Nota

- Quando si aggiorna il dispositivo con la versione più recente di AXIS OS nella traccia attiva, il dispositivo riceve le ultime funzionalità disponibili. Leggere sempre le istruzioni di aggiornamento e le note di rilascio disponibili con ogni nuova versione prima dell'aggiornamento. Per la versione AXIS OS più aggiornata e le note sul rilascio, visitare il sito Web axis.com/support/device-software.
1. Scarica il file AXIS OS sul tuo computer, disponibile gratuitamente su axis.com/support/device-software.
 2. Accedi al dispositivo come amministratore
 3. Andare a **Maintenance > AXIS OS upgrade (Manutenzione > Aggiornamento AXIS OS)** e fare clic su **Upgrade (Aggiorna)**.

Al termine dell'operazione, il dispositivo viene riavviato automaticamente.

Problemi tecnici e possibili soluzioni

Problemi durante l'aggiornamento di AXIS OS

Aggiornamento di AXIS OS non riuscito

Se l'aggiornamento non riesce, il dispositivo ricarica la versione precedente. Il motivo più comune è il caricamento di un AXIS OS errato. Controllare che il nome del file di AXIS OS corrisponda al dispositivo e riprovare.

Problemi dopo l'aggiornamento di AXIS OS

Se si riscontrano problemi dopo l'aggiornamento, ripristinare la versione installata in precedenza dalla pagina **Maintenance (Manutenzione)**.

Problemi durante l'impostazione dell'indirizzo IP

Impossibile impostare l'indirizzo IP

- Se l'indirizzo IP destinato al dispositivo e l'indirizzo IP del computer utilizzato per accedere al dispositivo si trovano in subnet diverse, non è possibile impostare l'indirizzo IP. Contattare l'amministratore di rete per ottenere un indirizzo IP.
- L'indirizzo IP potrebbe già essere utilizzato da un altro dispositivo. Per verificare:
 1. Scollegare il dispositivo Axis dalla rete.
 2. In una finestra di comando/DOS digitare `ping` e l'indirizzo IP del dispositivo.
 3. Se la risposta ricevuta è `Reply from <IP address>: bytes=32; time=10...` significa che l'indirizzo IP potrebbe già essere utilizzato da un altro dispositivo nella rete. Contattare l'amministratore di rete per un nuovo indirizzo IP e reinstallare il dispositivo.
 4. Se si riceve: `Request timed out`, significa che l'indirizzo IP può essere utilizzato con il dispositivo Axis. Controllare tutti i cablaggi e reinstallare il dispositivo.
- Potrebbe verificarsi un conflitto di indirizzi IP con un altro dispositivo sulla stessa subnet. Prima che il server DHCP imposti un indirizzo dinamico viene utilizzato l'indirizzo IP statico del dispositivo Axis. Ciò significa che se lo stesso indirizzo IP statico viene utilizzato anche da un altro dispositivo, si potrebbero verificare dei problemi durante l'accesso al dispositivo.

Problemi di accesso al dispositivo

Impossibile effettuare l'accesso al dispositivo tramite un browser.

Quando HTTPS è abilitato, controllare di utilizzare il protocollo corretto (HTTP o HTTPS) durante il tentativo di accesso. Potrebbe essere necessario digitare manualmente `http` o `https` nel campo dell'indirizzo del browser.

Se si è smarrita la password per l'account root, è necessario ripristinare le impostazioni predefinite di fabbrica del dispositivo. Per le istruzioni, vedere *Ripristino delle impostazioni predefinite di fabbrica, on page 18*.

L'indirizzo IP è stato modificato dal server DHCP

Gli indirizzi IP ottenuti da un server DHCP sono dinamici e potrebbero cambiare. Se l'indirizzo IP è stato modificato, utilizzare AXIS IP Utility o AXIS Device Manager per individuare il dispositivo sulla rete. Identificare il dispositivo utilizzando il relativo numero di serie o modello oppure il nome DNS (se è stato configurato).

Se necessario, è possibile assegnare manualmente un indirizzo IP statico. Per istruzioni, vedere *axis.com/support*.

Errore del certificato durante l'utilizzo di IEEE 802.1X

Per un corretto funzionamento dell'autenticazione, le impostazioni della data e dell'ora nel dispositivo Axis devono essere sincronizzate con un server NTP. Andare a **System > Date and time (Sistema > Data e ora)**.

Il browser non è supportato

Per un elenco dei browser consigliati, consultare *Supporto browser, on page 4*.

Impossibile accedere al dispositivo dall'esterno

Per accedere al dispositivo esternamente, si consiglia di usare una delle seguenti applicazioni per Windows®:

- AXIS Camera Station Edge: gratuito, ideale per piccoli sistemi con esigenze di sorveglianza di base.
- AXIS Camera Station Pro: versione di prova di 90 giorni gratuita, ideale per sistemi di piccole e medie dimensioni.

Per istruzioni e download, visitare axis.com/vms.

Problemi con MQTT

Impossibile collegarsi tramite la porta 8883 con MQTT su SSL

Il firewall blocca il traffico che utilizza la porta 8883 poiché è considerato non sicuro.

In alcuni casi il server/broker potrebbe non fornire una porta specifica per la comunicazione MQTT. Potrebbe essere ancora possibile utilizzare MQTT su una porta normalmente utilizzata per il traffico HTTP/HTTPS.

- Se il server/broker supporta WebSocket/WebSocket Secure (WS/WSS), in genere sulla porta 443, utilizzare questo protocollo. Controllare con il provider del server/broker se è supportato WS/WSS e quale porta e base utilizzare.
- Se il server/broker supporta ALPN, l'uso di MQTT può essere negoziato su una porta aperta, come la 443. Verificate con il proprio server/broker provider se ALPN è supportato e quale protocollo e porta ALPN utilizzare.

Se non si riesce a trovare qui ciò che si sta cercando, provare ad accedere alla sezione relativa alla risoluzione dei problemi all'indirizzo axis.com/support.

Considerazioni sulle prestazioni

I fattori seguenti sono i più importanti di cui tener conto:

- Un utilizzo eccessivo della rete dovuto a una scarsa infrastruttura influisce sulla larghezza di banda.
- Eseguire molteplici attività simultaneamente può influire sulle prestazioni audio.

Contattare l'assistenza

Se serve ulteriore assistenza, andare su axis.com/support.

Cyber security

La sicurezza informatica sostiene un ciclo di vita del prodotto ottimale con rischi ridotti al minimo. È possibile trovare informazioni dettagliate e documentazione sul nostro approccio alla sicurezza informatica all'indirizzo axis.com/about-axis/cybersecurity. Seguire le linee guida sulla sicurezza informatica riportate di seguito per ricevere le notifiche di sicurezza sui prodotti da parte di Axis e per effettuare la configurazione del prodotto in modo da garantirne un ciclo di vita e una messa fuori servizio sicuri.

All'indirizzo *Axis Trust Center*, è possibile trovare informazioni su come Axis garantisce la conformità alle norme di sicurezza, la trasparenza, la protezione dei dati e la privacy.

Gestione delle vulnerabilità

Axis è una *Common Vulnerability and Exposures (CVE) Numbering Authority (CNA)*. Per ridurre al minimo il rischio di esposizione, seguiamo gli standard del settore nell'identificazione e nella risoluzione delle vulnerabilità presenti nei nostri dispositivi, software e servizi. Per informazioni sulla nostra politica di gestione delle vulnerabilità o per segnalare una vulnerabilità, fare riferimento a: axis.com/vulnerability-management.

Notifiche di sicurezza

Iscriversi alle e-mail di notifica sulla sicurezza di Axis all'indirizzo axis.com/security-notification-service. Verranno inviate informazioni relative alle vulnerabilità, alle relative avvertenze di sicurezza e ad altre questioni relative alla sicurezza del proprio prodotto Axis.

Ciclo di vita sicuro del prodotto

Axis riduce al minimo i rischi durante l'intero ciclo di vita dei propri prodotti grazie a una gestione sicura del ciclo di vita. Utilizzi le nostre guide al consolidamento disponibili su help.axis.com per configurare e utilizzare in modo più sicuro i prodotti Axis e per trovare informazioni su:

Primo utilizzo sicuro – I prodotti Axis sono pre-configurati con un elevato livello di protezione predefinito per garantire un'inizializzazione sicura e comunicazioni crittografate sin dall'inizio.

Uso previsto ed errori comuni di configurazione – Le nostre guide forniscono informazioni sull'uso previsto dei prodotti Axis, compresi gli errori di configurazione e gli usi impropri più comuni che possono compromettere la sicurezza e che è opportuno evitare.

Gestione delle vulnerabilità e trasparenza della catena di fornitura – Ad ogni rilascio del software viene pubblicata una distinta base dei componenti software (SBOM) su axis.com al fine di rendere note le vulnerabilità e migliorare la trasparenza della catena di fornitura.

Messa fuori servizio e cancellazione sicura dei dati – Per mettere fuori servizio in modo sicuro un prodotto quando raggiunge la fine del suo ciclo di vita, ripristinare le impostazioni predefinite di fabbrica. In questo modo le configurazioni, i dati salvati e le informazioni sensibili verranno cancellati.

T10208737_it

2026-07 (M7.2)

© 2025 – 2026 Axis Communications AB