

AXIS A9210 Network I/O Relay Module

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 o 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 2*.

Per una descrizione di tutte le funzioni e impostazioni dell'interfaccia web dei dispositivi con AXIS OS, consultare *Guida per l'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 3*.
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 15*.

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 15*.
Dopo il ripristino, l'avvio sicuro garantisce lo stato del dispositivo.
2. Configurare e installare il dispositivo.

Panoramica dell'interfaccia Web

Questo video mette a disposizione una panoramica dell'interfaccia Web del dispositivo.



Interfaccia Web dei dispositivi Axis

Configurare il dispositivo

Configurazione di una porta I/O

1. Andare a Device > I/Os and relays > AXIS A9210 > I/Os (Dispositivo > I/O e relè > AXIS A9210 > I/O).
2. Fare clic su  per espandere le impostazioni della porta I/O.
3. Rinominare la porta.
4. Configurare lo stato normale. Fare clic su  per il circuito aperto o su  per il circuito chiuso.
5. Per configurare la porta I/O come input:
 - 5.1. In Direction (Direzione), fare clic su .
 - 5.2. Per monitorare lo stato dell'input, abilitare Supervised (Supervisionato). Vedere *Ingressi con supervisione, on page 14*.

Nota

Nelle API, le porte I/O supervisionate funzionano in modo diverso dalle porte di input supervisionate. Per ulteriori informazioni, andare alla *libreria VAPIX®*.

6. Per configurare la porta I/O come output:
 - 6.1. In Direction (Direzione), fare clic su .
 - 6.2. Per visualizzare gli URL per attivare e disattivare i dispositivi connessi, andare a Toggle port URL (Alterna URL porta).

Configurazione di un relè

1. Andare a Device > I/Os and relays > AXIS A9210 > Relays (Dispositivo > I/O e relè > AXIS A9210 > Relè).
2. Fare clic su  per espandere le impostazioni del relè.
3. Abilitare Relay (Relè).
4. Rinominare il relè.
5. Per visualizzare gli URL per attivare e disattivare il relè, andare a Toggle port URL (Alterna URL porta).

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.

Nota

- Se vengono apportate modifiche a una regola attiva, tale regola deve essere abilitata nuovamente per rendere valide le modifiche.

Interfaccia Web

Per informazioni su tutte le funzionalità e le impostazioni disponibili nell'interfaccia web dei dispositivi con AXIS OS, andare a *Guida per l'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 Door Monitoring

Questa applicazione effettua il monitoraggio dello stato della porta, indicando se è aperta o chiusa e se rimane aperta per un periodo eccessivo. Ad esempio, è possibile utilizzare l'applicazione su una porta antincendio che non richiede una serratura, ma di cui è necessario sapere se è aperta.

Una porta standard è dotata di un sensore di posizione della porta, REX, oltre a blocchi e lettori, che richiedono un door controller.

Una porta di monitoraggio richiede solo un sensore di posizione porta e REX e può essere monitorata utilizzando un modulo relè I/O di rete. Ogni modulo relè I/O di rete può collegare fino a cinque porte di monitoraggio.

Limiti

L'applicazione è disponibile solo su AXIS A9210. REX può essere collegato solo a I/O 1 e I/O 2, non è possibile configurare REX su I 3, I 4 o I 5.

Configurazione di AXIS Monitoring Door

Nome	Descrizione
Porta	Il numero della porta.
DPS input (Input DPS)	l'input DPS per la porta.
REX input	l'input REX per la porta.
Door open too long time (sec) (Porta aperta per troppo tempo (sec))	il numero di secondi per cui la porta può rimanere aperta.
Tempo di accesso (sec)	il numero di secondi per cui la porta può rimanere sbloccata dopo aver consentito l'accesso.
Stato	Lo stato della porta.

Cyber security

Per informazioni specifiche sulla cybersecurity (sicurezza informatica), consultare la scheda tecnica del dispositivo su axis.com.

Per informazioni approfondite sulla cybersecurity in AXIS OS, leggere la guida *AXIS OS Hardening*.

Axis Edge Vault

Axis Edge Vault è una piattaforma hardware di cybersecurity che protegge il dispositivo Axis. Offre funzionalità per garantire l'identità e l'integrità del dispositivo e per proteggere le informazioni sensibili da accessi non autorizzati. Si basa su solidi moduli di calcolo crittografico (Secure Element e TPM) e sicurezza del SoC (TEE e Secure Boot), combinati con le competenze di Axis nella sicurezza dei dispositivi edge.

SO firmato

Il SO firmato viene implementato dal fornitore del software che firma l'immagine di AXIS OS con una chiave privata. Quando la firma è allegata al sistema operativo, il dispositivo convalida il software prima di installarlo. Se il dispositivo rileva che l'integrità del software è compromessa, l'aggiornamento di AXIS OS verrà rifiutato.

Secure Boot

Secure Boot è un processo di avvio costituito da una catena ininterrotta di software crittograficamente convalidati eseguita da una memoria non modificabile (bootrom). Essendo basato sull'uso del SO firmato, l'avvio sicuro assicura che un dispositivo possa essere avviato solo con software autorizzato.

Archivio chiavi sicuro (keystore)

Un ambiente tutelato dalle manomissioni per la protezione delle chiavi private e l'esecuzione sicura di operazioni crittografiche. Impedisce l'accesso non autorizzato e l'estrazione dannosa in caso di violazione di sicurezza. A seconda dei requisiti di sicurezza, un dispositivo Axis può disporre di uno o più moduli di elaborazione crittografica, che forniscono un keystore sicuro protetto da hardware. In base ai requisiti di sicurezza, un dispositivo Axis può avere uno o più moduli di calcolo crittografici su base hardware, come un TPM 2.0 (Trusted Platform Module) o un secure element e/o un TEE (Trusted Execution Environment), che mettono a disposizione un archivio chiavi sicuro protetto dall'hardware. In più, dei dispositivi Axis selezionati dispongono di un archivio di chiavi sicuro con certificazione FIPS 140-2 Livello 2.

ID dispositivo Axis

poter verificare l'origine del dispositivo è fondamentale per stabilire che la sua identità è attendibile. Durante la produzione, ai dispositivi con Axis Edge Vault viene assegnato un certificato ID univoco e conforme a IEEE 802.1AR. È come avere un passaporto per dimostrare l'origine del dispositivo. L'ID del dispositivo viene archiviato in modo sicuro e permanente nell'archivio chiavi come certificato firmato dal certificato radice Axis. L'ID del dispositivo può essere sfruttato dall'infrastruttura IT del cliente per l'onboarding sicuro automatizzato di dispositivi e l'identificazione sicura dei dispositivi

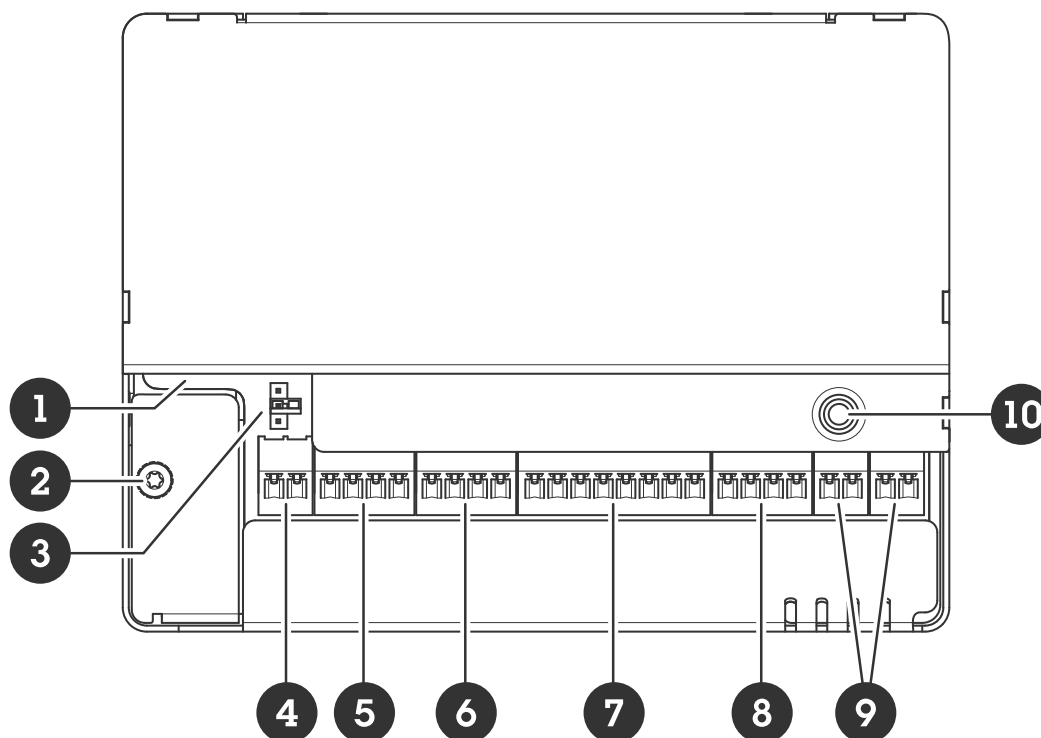
File system criptato

L'archivio chiavi sicuro impedisce l'esfiltrazione dannosa di informazioni e previene la manomissione della configurazione applicando una crittografia avanzata al file system. Così nessun dato memorizzato nel file system può essere estratto o manomesso quando non si usa il dispositivo, quando viene ottenuto l'accesso non autenticato al dispositivo e/o quando il dispositivo Axis viene rubato. Nel corso del processo di avvio sicuro, il file system lettura/scrittura è decrittografato ed è montabile e utilizzabile dal dispositivo Axis.

Per maggiori informazioni relativamente alle funzioni di cybersecurity nei dispositivi Axis, vai su axis.com/learning/white-papers e cerca cybersecurity.

Dati tecnici

Panoramica dei prodotti



- 1 Connettore di rete
- 2 Posizione di messa a terra
- 3 Ponticello relè
- 4 Connettore di alimentazione
- 5 Connettore relè
- 6 1 connettore di input
- 7 RS485 e connettore I/O
- 8 Connettore I/O
- 9 2 connettore di input
- 10 Pulsante di comando

Indicatori LED

LED	Colore	Significato
Stato	Verde	Luce verde fissa in condizioni di normale utilizzo.
	Giallo	Luce fissa durante l'avvio e quando si ripristinano le impostazioni.
	Rosso	Luce lampeggiante lenta per aggiornamento non riuscito.
Rete	Verde	Luce fissa per connessione di rete a 100 MBit/s. Lampeggiante per attività di rete.
	Giallo	Luce fissa per connessione di rete a 10 MBit/s. Lampeggiante per attività di rete.
	Spento	Assenza di collegamento di rete.

Alimentazione	Verde	Funzionamento normale.
	Giallo	Luce lampeggiante verde/gialla durante l'aggiornamento del firmware.
Relè	Verde	Relè attivo. ¹
	Spento	Relè inattivo.

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 15*.
- 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 con Power over Ethernet Plus (PoE +).

UL: Power over Ethernet (PoE) sarà tramite Ethernet IEEE 802.3af / 802.3at Tipo 1 Classe 3 o Power over Ethernet Plus (PoE +) IEEE 802.3at Tipo 2 Classe 4 iniettore limitato che fornisce 44-57 V DC, 15.4 W / 30 W. Power over Ethernet (PoE) è stato valutato da UL con AXIS T8133 Midspan 30 W 1-porta.

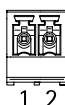
Priorità alimentazione

Questo dispositivo può essere alimentato tramite input PoE o CC. Vedere *Connettore di rete, on page 9* e *Connettore di alimentazione, on page 9*.

- Quando PoE e CC sono entrambi collegati prima dell'accensione del dispositivo, PoE viene utilizzato per l'alimentazione.
- PoE e CC sono entrambi collegati e PoE è attualmente in fase di alimentazione. Quando si perde l'alimentazione PoE, il dispositivo utilizza CC per l'alimentazione senza riavvio.
- PoE e CC sono entrambi collegati e CC è attualmente in fase di alimentazione. In caso di perdita di alimentazione CC, il dispositivo si riavvia e utilizza PoE per l'alimentazione.
- Quando CC viene utilizzato durante l'avvio e PoE viene collegato dopo l'avvio del dispositivo, viene utilizzato CC per l'alimentazione.
- Quando PoE viene utilizzato durante l'avvio e CC viene collegato dopo l'avvio del dispositivo, viene utilizzato PoE per l'alimentazione.

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.



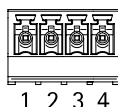
1. Il relè è attivo quando COM è connesso a NO.

Funzione	Pin	Note	Dati tecnici
Massa CC (GND)	1		0 V CC
Input CC	2	Per l'alimentazione del dispositivo quando non si utilizza Power over Ethernet. Nota: questo pin può essere usato solo come alimentazione.	12 V CC, max 36 W

UL: l'alimentazione CC deve essere fornita da un alimentatore conforme a UL 603, a seconda dell'applicazione, dotato delle classificazioni appropriate.

Connettore relè

Una morsettiera a 4 pin per relè a forma di C che possono essere utilizzati, ad esempio, per controllare un blocco o un'interfaccia di un cancello. Se utilizzata con un carico induttivo, ad esempio un blocco, collegare un diodo in parallelo al carico per proteggere il dispositivo da sovratensioni.



Funzione	Pin	Note	Dati tecnici
Massa CC (GND)	1		0 V CC
NO	2	Normalmente aperto. Per il collegamento di relè. Collegare un blocco di protezione intrinseca tra NO e massa CC. I due pin relè sono separati con isolamento galvanico dal resto dei circuiti se i ponticelli non vengono utilizzati.	Corrente massima = 2 A Tensione max. = 30 V CC
COM	3	Comune	
NC	4	Normalmente chiuso. Per il collegamento di relè. Collegare un blocco di sicurezza intrinseca tra NC e massa CC. I due pin relè sono separati con isolamento galvanico dal resto dei circuiti se i ponticelli non vengono utilizzati.	

Ponticello di alimentazione relè

Quando montato, il ponticello di alimentazione del relè si collega a 12 V CC o 24 V CC al pin COM del relè.

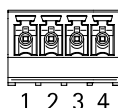
Può essere utilizzato per collegare un blocco tra i pin GND e NO o tra i pin GND e NC.

Sorgente di alimentazione	Potenza massima a 12 V CC	Potenza massima a 24 V CC
IN CC	2000 mA	1000 mA
PoE	350 mA	150 mA
PoE+	1100 mA	500 mA

1 connettore di input

Una morsettiera a 4 pin per input.

Supporta la supervisione con resistori di linea. Se il collegamento viene interrotto, viene attivato un allarme. Per utilizzare la supervisione ingressi, installare resistenze di fine linea. Per gli input supervisionati utilizzare lo schema delle connessioni. Vedere *Ingressi con supervisione, on page 14*.



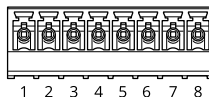
Funzione	Pin	Note	Dati tecnici
Terra CC	1, 3		0 V CC
Ingresso	2, 4	Ingresso digitale o ingresso supervisionato: collegarlo al pin 1 o 3 rispettivamente per attivarlo oppure lasciarlo isolato (scollegato) per disattivarlo.	Da 0 a max 30 V CC

Importante

La lunghezza certificata del cavo raggiunge il massimo di 200 m (656 piedi) se è soddisfatto il seguente requisito del cavo: AWG 24.

RS485 e connettore I/O

Una morsettiera a 8 pin con I/O a 4 pin e RS485 a 4 pin.



RS485

Funzione	Pin	Nota	Dati tecnici
Massa CC (GND)	1		0 V CC
Output CC (+12 V)	2	Fornisce alimentazione ai dispositivi ausiliari, ad esempio i sensori Modbus.	12 V CC, max 200 mA
A	3		
B	4		

I/O

Funzione	Pin	Nota	Dati tecnici
Uscita digitale	5	Se utilizzata con un carico induttivo, ad	Da 0 a max 30 V CC, open-drain, 100 mA

		esempio un relè, collegare un diodo in parallelo al carico per proteggere il dispositivo da sovratensioni.	
Uscita digitale	6	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
Ingresso	7	Input digitale o input supervisionato: collegarlo al pin 1 per attivarlo oppure lasciarlo isolato (scollegato) per disattivarlo.	Da 0 a max 30 V CC
Uscita digitale	8	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

Importante

- La lunghezza del cavo omologato per RS485 è fino a 1000 m (3281 ft) se sono soddisfatti i seguenti requisiti: 1 doppino intrecciato schermato, AWG 24, impedenza 120 ohm.
- La lunghezza del cavo omologato per I/O è fino a 200 m (656 ft).

Connettore I/O

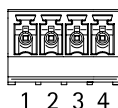
Utilizzare il connettore ausiliario con dispositivi esterni in combinazione con, ad esempio, rilevamento del movimento, attivazione di eventi e notifiche di allarme. Oltre al punto di riferimento 0 V CC e all'alimentazione (output CC), il connettore ausiliario fornisce l'interfaccia per:

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.

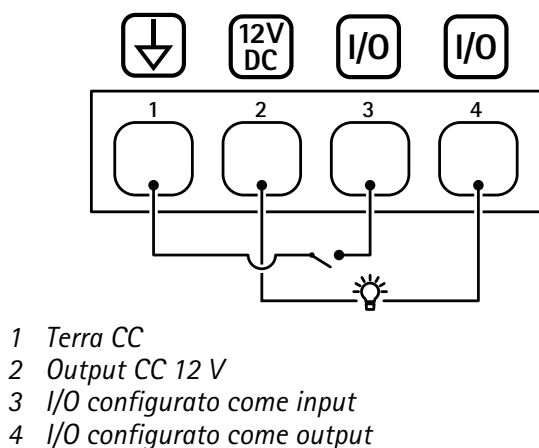
Uscita digitale – Per il collegamento di dispositivi esterni come relè e LED. I dispositivi collegati si possono attivare tramite l'API (interfaccia per la programmazione di applicazioni) del VAPIX® o dalla pagina web del prodotto.

Morsettiera a 4 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.	12 V CC

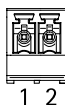
		Nota: questo pin può essere usato solo come uscita alimentazione.	Carico massimo = 50 mA in totale
Configurabile (ingresso o uscita)	3-4	Input digitale o input supervisionato - collegarlo al pin 1 per attivarlo oppure lasciarlo isolato (scollegato) per disattivarlo. Per utilizzare l'ingresso supervisionato, 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 si utilizza un carico induttivo, ad esempio un relè, collegare un diodo in parallelo al carico per proteggerlo da sovratensioni. Gli I/O sono in grado di pilotare un carico esterno da 12 V CC, 50 mA (massimo combinato), se si utilizza l'output interno da 12 V CC (PIN 2). In caso di utilizzo di connessioni di scarico aperte in combinazione con un alimentatore esterno, gli I/O possono gestire l'alimentazione CC di 0 - 30 V CC, 100 mA.	Da 0 a max 30 V CC, open-drain, 100 mA



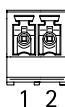
2 connettore di input

Due morsettiere a 2 pin per dispositivi esterni, ad esempio rottura vetri o rivelatori di incendio.

UL: il connettore non è stato valutato da UL per l'uso di antifurto o allarme antincendio.



Funzione	Pin	Note	Dati tecnici
Terra CC	1		0 V CC
Ingresso	2	Input digitale o input supervisionato - collegarlo al pin 1 per attivarlo oppure lasciarlo isolato (scollegato) per disattivarlo.	Da 0 a max 30 V CC



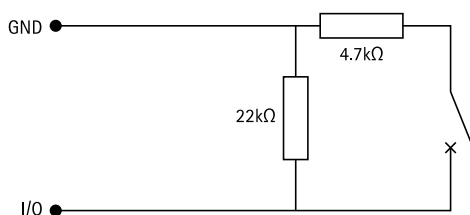
Funzione	Pin	Note	Dati tecnici
Terra CC	1		0 V CC
Ingresso	2	Input digitale o input supervisionato - collegarlo al pin 1 per attivarlo oppure lasciarlo isolato (scollegato) per disattivarlo.	Da 0 a max 30 V CC

Ingressi con supervisione

Per utilizzare gli input supervisionati, installare resistori terminali in base al diagramma di seguito riportato.

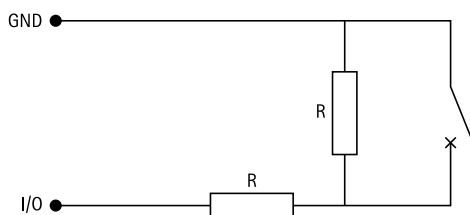
Prima connessione parallela

I valori dei resistori devono essere 4,7 k Ω e 22 k Ω .



Connessione prima in serie

I valori dei resistori devono essere gli stessi e i possibili valori sono 1 k Ω , 2,2 k Ω , 4,7 k Ω e 10 k Ω , 1%, standard 1/4 watt.



Nota

Si consiglia l'uso di cavi intrecciati e schermati. Connetti schermatura a 0 V CC.

Stato	Descrizione
Aperta	Lo switch supervisionato è in modalità aperta.
Chiusa	Lo switch supervisionato è in modalità chiusa.
Corto	Il cavo 1-5 I/O o di input è in corto circuito per messa a terra.
Interrotto	Il cavo 1-5 I/O o di input è interrotto e lasciato aperto senza percorso corrente per messa a terra.

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 8.
3. Tenere premuto il pulsante di comando per 25 secondi finché l'indicatore LED di stato non emette nuovamente una luce gialla.
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.

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 *Portale 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 15*.

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 2*.

Impossibile accedere al dispositivo dall'esterno

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

- 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.

Problemi con il funzionamento del dispositivo

Il riscaldatore anteriore e il tergicristallo non funzionano

Se il riscaldatore anteriore o il tergicristallo non si attivano, confermare che il coperchio superiore sia fissato correttamente alla parte inferiore dell'alloggiamento.

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.

Contattare l'assistenza

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

T10202445_it

2026-02 (M7.2)

© 2023 – 2026 Axis Communications AB