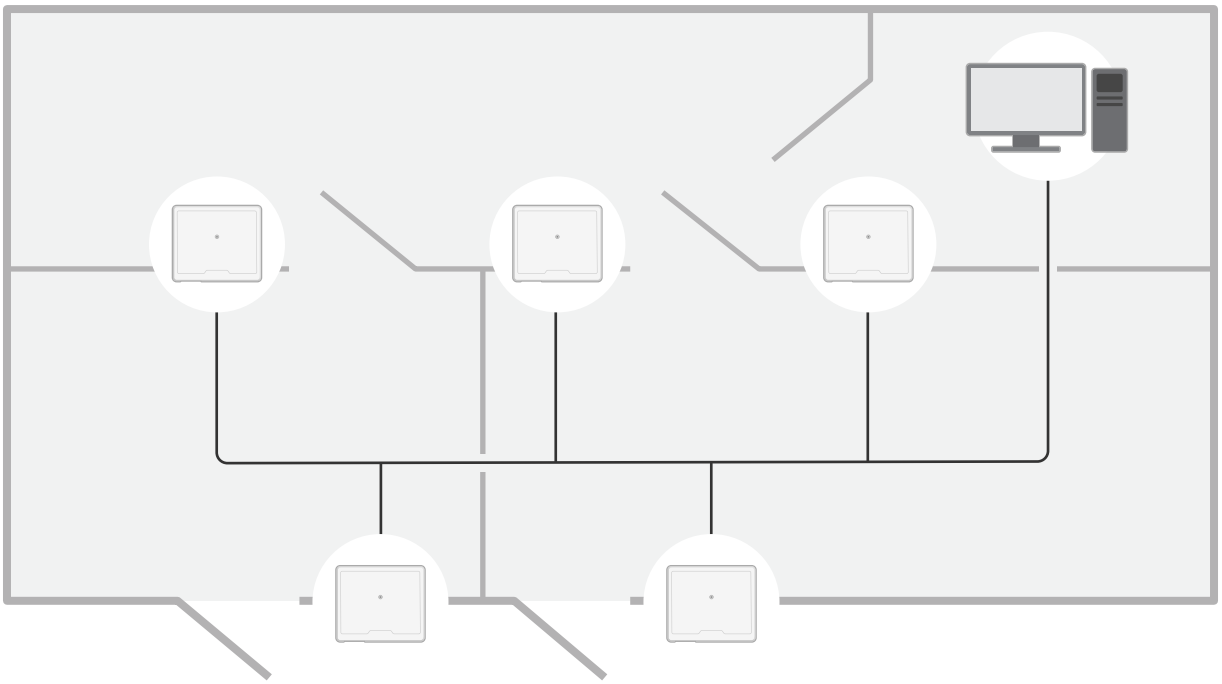
AXIS A1210 Network Door Controller

AXIS A1210-B Network Door Controller

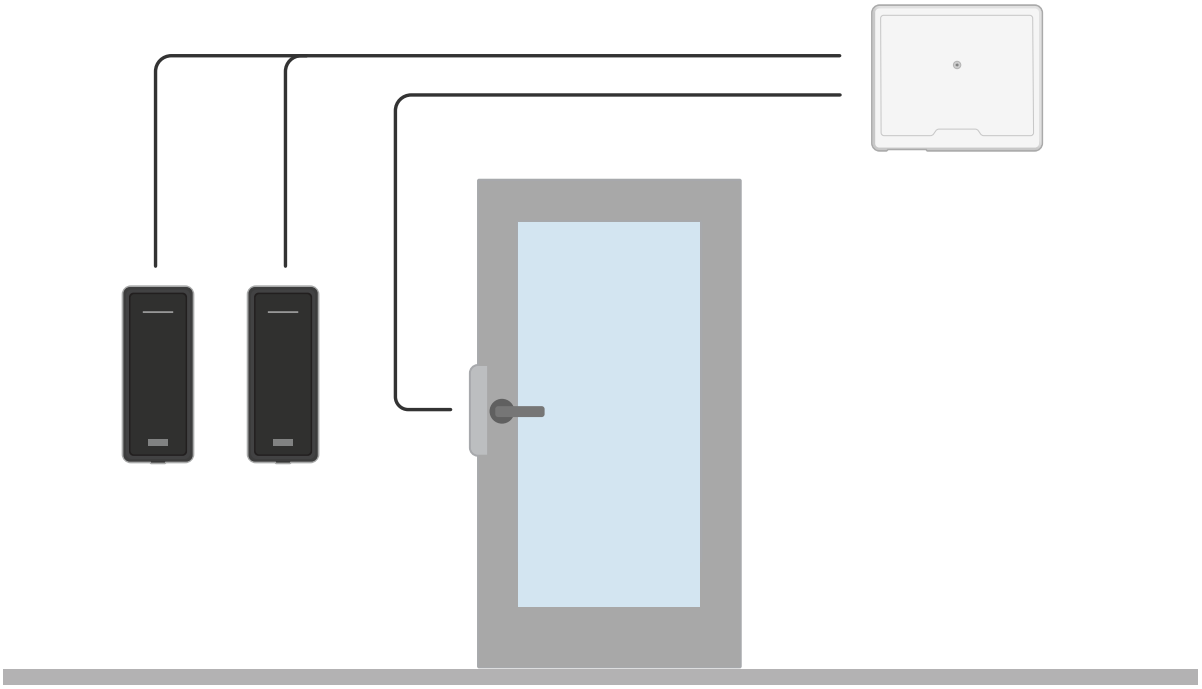
Manuale per l'utente

Sommario

Panoramica delle soluzioni



Il door controller di rete può essere facilmente collegato a e alimentato dalla rete IP esistente senza bisogno di cablaggi speciali.



Ciascun dispositivo di controllo delle porte di rete è un dispositivo intelligente che può essere facilmente montato vicino a una porta. È in grado di alimentare e controllare fino a due lettori.

Introduzione

Individuazione del dispositivo sulla rete

Per trovare i dispositivi Axis sulla rete e assegnare loro un indirizzo IP in Windows®, utilizzare 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™	Firefox®	Edge™	Safari®
Windows®	consigliato	consigliato	✓	
macOS®	consigliato	consigliato	✓	✓
Linux®	consigliato	consigliato	✓	
Altri sistemi operativi	✓	✓	✓	✓*

Per usare l'interfaccia web di AXIS OS con iOS 15 o iPadOS 15, vai a **Impostazioni > Safari > Avanzate > Funzioni sperimentali e disabilita NSURLSession Websocket.*

Per ulteriori informazioni sui browser consigliati, andare al *Portale AXIS OS*.

Aprire la pagina Web del dispositivo

1. Apri un browser e digita 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 la password. Se si accede al dispositivo per la prima volta, è necessario impostare la password root. Vedere *Impostazione di una nuova password per l'account root alla pagina 5*.

Impostazione di una nuova password per l'account root

Il nome utente predefinito dell'amministratore è `root`. Non c'è alcuna password predefinita per l'account root. La prima volta che si esegue l'accesso al dispositivo, impostare la password.

1. Digitare una password. Attenersi alle istruzioni sulle password sicure. Vedere *Password sicure alla pagina 5*.
2. Ridigitare la password per confermarne la correttezza.
3. Fare clic su **Add user (Aggiungi utente)**.

Importante

In caso di smarrimento della password per l'account root, andare a *Ripristino delle impostazioni predefinite di fabbrica alla pagina 32* e seguire le istruzioni.

Password sicure

Importante

I dispositivi Axis inviano la password inizialmente impostata in chiaro tramite la rete. Per proteggere il dispositivo dopo il primo accesso, impostare una connessione HTTPS sicura e crittografata, quindi cambiare la password.

La password del dispositivo è il sistema di protezione principale dei dati e dei servizi. I dispositivi Axis non impongono un criterio password in quanto potrebbero essere utilizzati in vari tipi di installazioni.

Per proteggere i tuoi dati ti consigliamo vivamente di:

- Utilizzare una password con almeno 8 caratteri, preferibilmente creata 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 firmware

Per verificare che il dispositivo disponga del firmware Axis 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 alla pagina 32*.

   Dopo il ripristino, l'avvio sicuro garantisce lo stato del dispositivo.

2. Configurare e installare il dispositivo.

Panoramica della pagina Web

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

Interfaccia Web dei dispositivi Axis

Installazione

Per guardare questo video, visitare la versione Web di questo documento.

help.axis.com/?&piaId=74266&section=solution-overview

Configurare il dispositivo

Per sapere in che modo si configura il dispositivo, consulta il *manuale per l'utente AXIS Camera Station* o soluzioni di terze parti.

L'interfaccia dispositivo

Per raggiungere l'interfaccia dispositivo, digita l'indirizzo IP del dispositivo in un browser web.

Nota

Il supporto per le funzionalità e le impostazioni descritte in questa sezione varia da un dispositivo all'altro.

Mostra o nascondi il menu principale.

Accedere alla guida dispositivo.

Modificare la lingua.

Imposta il tema chiaro o il tema scuro.

Il menu contestuale contiene:

- Informazioni relative all'utente che ha eseguito l'accesso.
- **Change user (Cambia utente)**: Disconnettersi dall'utente corrente e accedere a un nuovo utente.
- **Log out (Disconnetti)**: Disconnettere l'utente corrente.

Il menu contestuale contiene:

- **Analytics data (Dati di analisi)**: acconsenti alla condivisione dei dati non personali del browser.
- **Feedback**: condividi qualsiasi feedback per contribuire a rendere migliore la tua esperienza utente.
- **Legal (Informazioni legali)**: visualizzare informazioni sui cookie e le licenze.
- **About (Informazioni)**: visualizza le informazioni relative al dispositivo, compresa la versione del firmware e il numero di serie.
- **Legacy device interface (Interfaccia dispositivo legacy)**: Passa dall'interfaccia dispositivo all'interfaccia dispositivo precedente.

Stato

Sincronizzazione NTP

Mostra le informazioni di sincronizzazione NTP, inclusa l'eventuale sincronizzazione del dispositivo con un server NTP e il tempo che rimane fino alla sincronizzazione successiva.

NTP settings (Impostazioni NTP): Fare clic per andare sulla pagina Data e ora, dove è possibile modificare le impostazioni NTP.

Informazioni dispositivo

mostra le informazioni relative al dispositivo, compresa la versione del firmware e il numero di serie.

Upgrade firmware (Aggiorna il firmware): fare clic su questa opzione per andare alla pagina Manutenzione, dove puoi aggiornare il firmware.

Controllo degli accessi

Allarmi

Device motion (Movimento dispositivo): È attivato per impostazione predefinita per attivare un allarme nel tuo sistema quando avviene la rilevazione di movimento dispositivo del door controller.

Casing open (Apertura alloggiamento): È attivato per impostazione predefinita per attivare un allarme nel tuo sistema quando avviene la rilevazione di apertura alloggiamento del door controller.

External tamper (Manomissione esterna): Non è abilitato per impostazione predefinita. Accendi per attivare un allarme nel sistema quando viene rilevata una manomissione esterna. Ad esempio, quando l'armadietto esterno è aperto o chiuso.

- **Supervised input (Input supervisionato)**: Attivare per il monitoraggio dello stato di input e la configurazione dei resistori end-of-line.
  - Per utilizzare la prima connessione parallela, selezionare **Parallel first connection with a 22 KΩ parallel resistor and a 4.7 KΩ serial resistor (Prima connessione parallela con un resistore parallelo da 22 KΩ E un resistore seriale da 4,7 KΩ)**.
  - Per utilizzare la prima connessione in serie, selezionare **Serial first connection (Prima connessione in serie)** e selezionare un valore dei resistori dall'elenco a discesa **Resistor values (Valori resistore)**.

Periferiche

Upgrade readers (Aggiorna lettori): fai clic su questa opzione per eseguire l'aggiornamento dei lettori a una nuova versione del firmware. Solo i lettori supportati si possono aggiornare quando sono online.

Sistema

Data e ora

Le impostazioni della lingua del browser Web influenzano il formato dell'ora.

Nota

Ti consigliamo di eseguire la sincronizzazione di data e ora del dispositivo usando un server NTP.

Synchronization (Sincronizzazione): seleziona un'opzione per la sincronizzazione della data e dell'ora del dispositivo.

- **Automatic date and time (manual NTS KE servers) (Data e ora automatiche (server NTS KE manuali))**: esegui la sincronizzazione con i server NTP key establishment sicuri connessi al server DHCP.
  - **Manual NTS KE servers (Server NTS KE manuali)**: inserisci l'indirizzo IP di uno o due server NTP. Quando usi due server NTP, l'ora del dispositivo viene sincronizzata e adattata sulla base dell'input di entrambi.
- **Automatic date and time (NTP servers using DHCP) (Data e ora automatiche (server NTP tramite DHCP))**: esegui la sincronizzazione con i server NTP connessi al server DHCP.
  - **Fallback NTP servers (Server NTP di fallback)**: inserisci l'indirizzo IP di uno o due server fallback.
- **Automatic date and time (manual NTP servers) (Data e ora automatiche (server NTP manuali))**: esegui la sincronizzazione con i server NTP scelti.
  - **Manual NTP servers (Server NTP manuali)**: inserisci l'indirizzo IP di uno o due server NTP. Quando usi due server NTP, l'ora del dispositivo viene sincronizzata e adattata sulla base dell'input di entrambi.
- **Custom date and time (Data e ora personalizzate)**: impostare manualmente la data e l'ora. Per recuperare una volta dal computer o dal dispositivo mobile le impostazioni di data e ora, fare clic su **Get from system (Ottieni dal sistema)**.

Time zone (Fuso orario): selezionare il fuso orario da utilizzare. L'ora legale e l'ora solare si alterneranno automaticamente.

Nota

Il sistema utilizza le impostazioni di data e ora in tutte le registrazioni, i registri e le impostazioni di sistema.

Rete

IPv4 (IPv4)

Assign IPv4 automatically (Assegna automaticamente IPv4): Selezionare questa opzione per consentire al router di rete di assegnare automaticamente un indirizzo IP al dispositivo. Si consiglia l'IP automatico (DHCP) per la maggior parte delle reti.

IP address (Indirizzo IP): Inserire un indirizzo IP univoco per il dispositivo. Gli indirizzi IP fissi possono essere assegnati casualmente in reti isolate, a condizione che ogni indirizzo sia univoco. Per evitare conflitti, si consiglia di contattare l'amministratore di rete prima di assegnare un indirizzo IP statico.

Subnet mask: Immetti la subnet mask per definire quali indirizzi sono all'interno della rete locale. Qualsiasi indirizzo fuori dalla rete locale passa attraverso il router.

Router: Inserire l'indirizzo IP del router predefinito (gateway) utilizzato per connettere i dispositivi collegati a reti diverse e a segmenti di rete.

IPv6 (IPv6)

Assign IPv6 automatically (Assegna automaticamente IPv6): Selezionare questa opzione per attivare IPv6 e consentire al router di rete di assegnare automaticamente un indirizzo IP al dispositivo.

Hostname (Nome host)

Assign hostname automatically (Assegna automaticamente il nome host): Selezionare questa opzione per consentire al router di rete di assegnare automaticamente un nome host al dispositivo.

Hostname (Nome host): Immetti manualmente il nome host da usare come metodo alternativo per accedere al dispositivo. Il nome host viene utilizzato nel report del server e nel registro di sistema. I caratteri consentiti sono A–Z, a–z, 0–9 e -.

DNS servers (Server DNS)

Assign DNS automatically (Assegna automaticamente DNS): Selezionare questa opzione per consentire al router di rete di assegnare automaticamente i domini di ricerca e gli indirizzi del server DNS al dispositivo. Si consiglia il DNS automatico (DHCP) per la maggior parte delle reti.

Search domains (Domini di ricerca): Quando si utilizza un nome host non completo, fare clic su **Add search domain (Aggiungi dominio di ricerca)** e immettere un dominio in cui cercare il nome host utilizzato dal dispositivo.

DNS servers (Server DNS): Fare clic su **Add DNS server (Aggiungi server DNS)** e inserire l'indirizzo IP del server DNS. Offre la conversione dei nomi host in indirizzi IP nella rete.

HTTP and HTTPS (HTTP e HTTPS)

Allow access through (Consenti l'accesso tramite): Selezionare questa opzione se a un utente è consentito connettersi al dispositivo tramite **HTTP**, **HTTPS** o entrambi i protocolli **HTTP e HTTPS**.

HTTPS è un protocollo che fornisce la crittografia per le richieste di pagine da parte di utenti e per le pagine restituite dal server Web. Lo scambio di informazioni crittografate è regolato dall'utilizzo di un certificato HTTPS, che garantisce l'autenticità del server.

Per utilizzare HTTPS nel dispositivo, è necessario installare un certificato HTTPS. Andare a **System > Security (Sistema > Sicurezza)** per creare e installare i certificati.

Nota

Se si visualizzano pagine Web crittografate tramite HTTPS, è possibile che si verifichi un calo delle prestazioni, soprattutto quando si richiede una pagina per la prima volta.

HTTP port (Porta HTTP): immettere la porta HTTP da utilizzare. Sono consentite la porta 80 o qualsiasi porta nell'intervallo 1024-65535. Se è stato eseguito l'accesso come amministratore, è possibile immettere qualsiasi porta nell'intervallo da 1 a 1023. Se si utilizza una porta in questo intervallo, viene visualizzato un avviso.

HTTPS port (Porta HTTPS): immettere la porta HTTPS da utilizzare. Sono consentite la porta 443 o qualsiasi porta nell'intervallo 1024-65535. Se è stato eseguito l'accesso come amministratore, è possibile immettere qualsiasi porta nell'intervallo da 1 a 1023. Se si utilizza una porta in questo intervallo, viene visualizzato un avviso.

Certificate (Certificato): selezionare un certificato per abilitare HTTPS per il dispositivo.

Protocolli di rilevamento della rete

Bonjour®: attivare per consentire il rilevamento automatico sulla rete.

Bonjour name (Nome Bonjour): Inserire un nome descrittivo che deve essere visibile sulla rete. Il nome predefinito è il nome del dispositivo e l'indirizzo MAC.

UPnP®: attivare per consentire il rilevamento automatico sulla rete.

UPnP name (Nome UPnP): Inserire un nome descrittivo che deve essere visibile sulla rete. Il nome predefinito è il nome del dispositivo e l'indirizzo MAC.

WS-Discovery: attivare per consentire il rilevamento automatico sulla rete.

One-click cloud connection (Connessione a cloud con un clic)

One-Click Cloud Connect (O3C), utilizzato in combinazione con un servizio O3C, offre un accesso Internet facile e sicuro a video in diretta e registrati, accessibili da qualsiasi ubicazione. Per ulteriori informazioni, vedere *axis.com/end-to-end-solutions/hosted-services*.

Allow O3C (Consenti O3C):

- **One-click**: L'impostazione predefinita. Tenere premuto il pulsante di comando sul dispositivo per collegarsi a un servizio O3C via Internet. È necessario registrare il dispositivo con il servizio O3C entro 24 ore dopo aver premuto il pulsante di comando. In caso contrario, il dispositivo si disconnette dal servizio O3C. Una volta registrato il dispositivo, viene abilitata l'opzione **Always (Sempre)** e il dispositivo rimane collegato al servizio O3C.
- **Always (Sempre)**: il dispositivo Axis tenta costantemente di collegarsi a un servizio O3C via Internet. Una volta registrato, il dispositivo rimane collegato al servizio O3C. Utilizzare questa opzione se il pulsante di comando del dispositivo non è disponibile.
- **No**: disabilita il servizio O3C.

Proxy settings (Impostazioni proxy): Se necessario, immettere le impostazioni proxy per collegarsi al server proxy.

Host: Immettere l'indirizzo del server del proxy.

Port (Porta): immettere il numero della porta utilizzata per l'accesso.

Login (Accesso) e **Password**: se necessario, immettere un nome utente e una password per il server proxy.

Authentication method (Metodo di autenticazione):

- **Basic (Base)**: questo metodo è lo schema di autenticazione maggiormente compatibile per HTTP. È meno sicuro del metodo **Digest** perché invia il nome utente e la password non crittografati al server.
- **Digest**: questo metodo è più sicuro perché la password viene sempre trasferita crittografata nella rete.
- **Auto (Automatica)**: questa opzione consente al dispositivo Axis di selezionare il metodo di autenticazione a seconda dei metodi supportati, dando priorità a **Digest** rispetto al metodo **Basic (Base)**.

Owner authentication key (OAK) (Chiave di autenticazione proprietario (OAK)): Fare clic su **Get key (Ottieni chiave)** per recuperare la chiave di autenticazione proprietario. Questo è possibile solo se il dispositivo è connesso a Internet senza un firewall o un proxy.

SNMP (SNMP)

SNMP (Simple Network Management Protocol) consente il monitoraggio e la gestione in remoto dei dispositivi di rete.

SNMP: Selezionare la versione di SNMP da utilizzare.

- **v1 and v2c (v1 e v2c)**:
  - **Read community (Comunità con privilegi in lettura)**: Inserire il nome della comunità che dispone solo dell'accesso in lettura a tutti gli oggetti SNMP supportati. Il valore predefinito è **public (pubblico)**.
  - **Write community (Comunità con privilegi in scrittura)**: Specificare il nome della comunità che dispone di accesso in lettura e scrittura a tutti gli oggetti SNMP supportati (ad eccezione degli oggetti in sola lettura). Il valore predefinito è **write (scrittura)**.
  - **Activate traps (Attiva trap)**: Attivare la segnalazione di trap. Il dispositivo utilizza i trap per inviare messaggi per eventi importanti o cambi di stato a un sistema di gestione. Nell'interfaccia del dispositivo, è possibile impostare trap per SNMP v1 e v2c. I trap vengono disattivati automaticamente se si cambia in SNMP v3 o si disattiva SNMP. Se si utilizza SNMP v3, è possibile impostare i trap tramite l'applicazione di gestione SNMP v3.
  - **Trap address (Indirizzo trap)**: immettere l'indirizzo IP o il nome host del server di gestione.
  - **Trap community (Comunità trap)**: Immettere la comunità da utilizzare quando il dispositivo invia un messaggio trap al sistema di gestione.
  - **Traps (Trap)**:
  - **Cold start (Avvio a freddo)**: Invia un messaggio di trap all'avvio del dispositivo.
  - **Warm start (Avvio a caldo)**: Invia un messaggio trap quando si modifica un'impostazione SNMP.
  - **Link up**: invia un messaggio trap quando un collegamento cambia dal basso verso l'alto.
  - **Authentication fareled (Autenticazione non riuscita)**: invia un messaggio trap quando un tentativo di autenticazione non riesce.

Nota

Tutti i trap Axis Video MIB vengono abilitati quando si attivano i trap SNMP v1 e v2c. Per ulteriori informazioni, vedere *AXIS OS Portal > SNMP (Poortale sistema operativo AXIS > SNMP)*.

- **v3**: SNMP v3 è una versione più sicura che fornisce crittografia e password sicure. Per utilizzare SNMP v3, si consiglia di attivare HTTPS poiché la password verrà successivamente inviata via HTTPS. Ciò impedisce inoltre alle parti non autorizzate di accedere ai trap v1 e v2 non crittografati. Se si utilizza SNMP v3, è possibile impostare i trap tramite l'applicazione di gestione SNMP v3.
  - **Password for the account "initial" (Password per l'account "iniziale")**: Immettere la password SNMP per l'account denominato "iniziale". Sebbene la password possa essere inviata senza attivare HTTPS, non è consigliabile. La password SNMP v3 può essere impostare solo una volta e preferibilmente solo quando è attivato HTTPS. Una volta impostata la password, il relativo campo non verrà più visualizzato. Per impostare di nuovo la password, il dispositivo deve essere ripristinato alle impostazioni predefinite di fabbrica.

Connected clients (Client collegati)

L'elenco mostra tutti i client connessi al dispositivo.

Update (Aggiorna): Fare clic per aggiornare l'elenco.

Sicurezza

Certificates (Certificati)

I certificati sono utilizzati per autenticare i dispositivi in una rete. I tipi di certificati supportati da questo dispositivo sono due:

- **Client/server certificates (Certificati client/server)**
  Un certificato client/server convalida l'identità del dispositivo e può essere autofirmato o emesso da un'autorità di certificazione (CA). Un certificato autofirmato offre una protezione limitata e può essere utilizzato prima che sia stato ottenuto un certificato emesso da un'autorità di certificazione.
- **Certificati CA**
  È possibile utilizzare un certificato CA per autenticare un certificato peer, ad esempio per convalidare l'identità di un server di autenticazione nel caso in cui il dispositivo venga collegato a una rete protetta da IEEE 802.1X. Il dispositivo dispone di diversi certificati CA preinstallati.

Questi formati sono supportati:

- Formati dei certificati: .PEM, .CER e .PFX
- Formati delle chiavi private: PKCS#1 e PKCS#12

Importante

Se il dispositivo viene ripristinato alle impostazione di fabbrica, tutti i certificati vengono eliminati. Qualsiasi certificato CA preinstallato viene reinstallato.

Filtra i certificati nell'elenco.

Add certificate (Aggiungi certificato): fare clic sull'opzione per aggiungere un certificato.

Il menu contestuale contiene:

- **Certificate information (Informazioni certificato)**: visualizza le proprietà di un certificato installato.
- **Delete certificate (Elimina certificato)**: Elimina il certificato.
- **Create certificate signing request (Crea richiesta di firma certificato)**: Per fare richiesta di un certificato di identità digitale, crea una richiesta di firma del certificato da mandare a un'autorità di registrazione.

IEEE 802.1x

IEEE 802.1x è uno standard IEEE per il controllo di ammissione alla rete in base alla porta che fornisce un'autenticazione sicura di dispositivi di rete cablati e wireless. IEEE 802.1x è basato su EAP (Extensible Authentication Protocol).

Per accedere a una rete protetta da IEEE 802.1x, i dispositivi di rete devono autenticarsi. L'autenticazione viene eseguita da un server di autenticazione, generalmente un server RADIUS (ad esempio FreeRADIUS e Microsoft Internet Authentication Server).

Certificates (Certificati)

Se configurato senza un certificato CA, la convalida del certificato del server verrà disabilitata e il dispositivo cercherà in questo caso di autenticarsi a prescindere dalla rete a cui è connesso.

Nell'implementazione di Axis, quando si utilizza un certificato, il dispositivo e il server di autenticazione si autenticano con certificati digitali mediante EAP-TLS (Extensible Authentication Protocol - Transport Layer Security).

Per consentire al dispositivo di accedere a una rete protetta tramite certificati, è necessario installare un certificato client firmato nel dispositivo.

Client Certificate (Certificato client): Selezionare un certificato client per utilizzare IEEE 802.1x. Il server di autenticazione utilizza il certificato per convalidare l'identità del client.

CA Certificate (Certificato CA): Selezionare un certificato CA per convalidare l'identità del server di autenticazione. Quando non ne viene selezionato nessun certificato, il dispositivo tenterà di autenticarsi a prescindere dalla rete a cui è connesso.

EAP identity (Identità EAP): Immettere l'identità utente associata al certificato del client.

EAPOL version (Versione EAPOL): selezionare la versione EAPOL utilizzata nello switch di rete.

Use IEEE 802.1x (Usa IEEE 802.1x): Selezionare questa opzione per utilizzare il protocollo IEEE 802.1x.

Prevent brute-force attacks (Prevenire gli attacchi di forza bruta)

Blocking (Blocco): Attiva per bloccare gli attacchi di forza bruta. Un attacco di forza bruta usa tentativi ed errori per indovinare le informazioni di accesso o le chiavi di crittografia.

Blocking period (Periodo di blocco): Immettere il numero di secondi per cui si blocca un attacco di forza bruta.

Blocking conditions (Condizioni di blocco): Immettere il numero di errori di autenticazione consentiti al secondo prima dell'inizio del blocco. È possibile impostare il numero di errori consentiti a livello di pagina e di dispositivo.

IP address filter (Filtro indirizzi IP)

Use filter (Usa filtro): Selezionare questa opzione per filtrare gli indirizzi IP a cui è consentito accedere al dispositivo.

Policy (Criteri) Scegliere se **Allow (Consentire)** o **Deny (Negare)** l'accesso per determinati indirizzi IP.

Addresses (Indirizzi): Immettere i numeri IP a cui è consentito o negato l'accesso al dispositivo. È inoltre possibile utilizzare il formato CIDR.

Custom-signed firmware certificate (Certificato firmware con firma personalizzata)

Serve un certificato firmware con firma personalizzata per l'installazione di firmware di prova o firmware personalizzato di altro tipo di Axis sul dispositivo. Il certificato verifica che il firmware è stato approvato sia dal proprietario del dispositivo che da Axis. È possibile eseguire il firmware unicamente su uno specifico dispositivo identificabile tramite il suo numero di serie univoco e l'ID del chip. I certificati firmware con firma personalizzata possono essere creati solo da Axis, poiché Axis detiene la chiave per firmarli.

Fare clic su **Install (Installa)** per eseguire l'installazione del certificato. Il certificato deve essere installato prima del firmware.

Utenti

+ **Add user (Aggiunta di un utente)**: per creare un nuovo utente, fare clic su questa opzione. Puoi aggiungere un massimo di 100 utenti.

Username (Nome utente): inserire un nome utente univoco.

New password (Nuova password): immettere una password dell'utente. La lunghezza delle password deve essere compresa tra 1 e 64 caratteri. La password può contenere solo caratteri ASCII stampabili (codice da 32 a 126), quali lettere, numeri, segni di punteggiatura e alcuni simboli.

Repeat password (Ripeti password): immettere di nuovo la stessa password.

Role (Ruolo):

- **Administrator (Amministratore)**: ha accesso completo a tutte le impostazioni. Gli amministratori possono anche aggiungere, aggiornare e rimuovere altri utenti.
- **Operator (Operatore)**: ha accesso a tutte le impostazioni ad eccezione di:
  - Tutte le impostazioni **System (Sistema)**.
  - L'aggiunta di app.
- **Viewer (Visualizzatore)**: non ha l'accesso alla modifica di alcuna impostazioni.

⋮ Il menu contestuale contiene:

Update user (Aggiorna utente): Modifica le proprietà dell'utente.

Delete user (Elimina utente): Elimina l'utente. Non puoi cancellare l'utente root.

MQTT

MQTT (Message Queuing Telemetry Transport) è un protocollo di messaggistica standard per l'Internet of Things (IoT). È stato progettato per un'integrazione IoT semplificata ed è utilizzato in una vasta gamma di settori per collegare dispositivi remoti con un'impronta di codice ridotta e una larghezza di banda di rete minima. Il client MQTT nel firmware del dispositivo Axis può semplificare l'integrazione di dati ed eventi prodotti nel dispositivo con sistemi che non sono Video Management System (VMS).

Configurare il dispositivo come client MQTT. La comunicazione MQTT si basa su due entità, i client e il broker. I client possono inviare e ricevere messaggi. Il broker è responsabile del routing dei messaggi tra i client.

Potrai trovare maggiori informazioni relative a MQTT consultando l'*AXIS OS Portal*.

MQTT client (Client MQTT)

Connect (Connetti): Attivare o disattivare il client MQTT.

Status (Stato): Visualizza lo stato corrente del client MQTT.

Broker

Host: immettere il nome host o l'indirizzo IP del server MQTT.

Protocol (Protocollo): Selezionare il protocollo da utilizzare.

Port (Porta): Immettere il numero di porta.

- 1883 è il valore predefinito per **MQTT su TCP**
- 8883 è il valore predefinito per **MQTT su SSL**
- 80 è il valore predefinito per **MQTT su WebSocket**
- 443 è il valore predefinito per **MQTT su WebSocket Secure**

Username (Nome utente): immettere il nome utente che il client utilizzerà per accedere al server.

Password: immettere una password per il nome utente.

Client ID (ID client): Immettere un ID client. L'identificatore del client viene inviato al server al momento della connessione del client.

Clean session (Sessione pulita): Controlla il comportamento al momento della connessione e della disconnessione. Se selezionate, le informazioni sullo stato vengono ignorate al momento della connessione e della disconnessione.

Keep alive interval (Intervallo keep alive): L'intervallo keep alive consente al client di rilevare quando il server non è più disponibile senza dover attendere il lungo tempo di timeout TCP/IP.

Timeout: L'intervallo di tempo in secondi per consentire il completamento di una connessione. Valore predefinito: 60

Device topic prefix (Prefisso argomento dispositivo): utilizzato nei valori predefiniti per l'argomento nel messaggio di connessione e nel messaggio Ultime volontà e testamento nella scheda **MQTT client (Client MQTT)** e nelle condizioni di pubblicazione nella scheda **MQTT publication (Pubblicazione MQTT)**.

Reconnect automatically (Riconnetti automaticamente): specifica se il client deve riconnettersi automaticamente dopo una disconnessione.

Connect message (Messaggio connessione)

Specifica se un messaggio deve essere inviato quando viene stabilita una connessione.

Send message (Invia messaggio): Attivare per inviare messaggi.

Use default (Usa predefinito): Disattivare per immettere un messaggio predefinito.

Topic (Argomento): Immettere l'argomento per il messaggio predefinito.

Payload: Immettere il contenuto per il messaggio predefinito.

Retain (Conserva): Selezionare questa opzione per mantenere lo stato del client su questo **Topic (Argomento)**

QoS: Cambiare il livello QoS per il flusso di pacchetti.

Last Will and Testament message (Messaggio di ultime volontà e testamento)

Ultime volontà e testamento consente a un client di fornire un testamento insieme alle proprie credenziali quando si collega al broker. Se il client si disconnette in modo anomalo in un secondo momento (forse perché la sua sorgente di alimentazione non funziona), può lasciare che il broker recapiti un messaggio ad altri client. Questo messaggio Ultime volontà e testamento ha lo stesso formato di un messaggio ordinario e viene instradato tramite la stessa meccanica.

Send message (Invia messaggio): Attivare per inviare messaggi.

Use default (Usa predefinito): Disattivare per immettere un messaggio predefinito.

Topic (Argomento): Immettere l'argomento per il messaggio predefinito.

Payload: Immettere il contenuto per il messaggio predefinito.

Retain (Conserva): Selezionare questa opzione per mantenere lo stato del client su questo **Topic (Argomento)**

QoS: Cambiare il livello QoS per il flusso di pacchetti.

MQTT publication (Pubblicazione MQTT)

Use default topic prefix (Usa prefisso di argomento predefinito): Selezionare questa opzione per usare il prefisso dell'argomento predefinito, definito nel prefisso argomento dispositivo nella scheda **MQTT client (Client MQTT)**.

Include topic name (Includi nome argomento): selezionare questa opzione per l'inclusione dell'argomento che illustra la condizione nell'argomento MQTT.

Include topic namespaces (Includi spazi dei nomi degli argomenti): Selezionare questa opzione per includere gli spazi dei nomi degli argomenti di ONVIF nell'argomento MQTT.

Include serial number (Includi numero di serie): selezionare questa opzione per comprendere il numero di serie del dispositivo nel payload MQTT.

+ **Add condition (Aggiungi condizione)**: fare clic sull'opzione per aggiungere una condizione.

Retain (Conserva): definire quali messaggi MQTT sono inviati come conservati.

- **None (Nessuno)**: inviare tutti i messaggi come non conservati.
- **Property (Proprietà)**: inviare solo messaggi con stato conservati.
- **All (Tutto)**: Invia messaggi sia con che senza stato come conservati.

QoS: Seleziona il livello desiderato per la pubblicazione MQTT.

MQTT subscriptions (Sottoscrizioni MQTT)

+ **Add subscription (Aggiungi sottoscrizione)**. Fai clic per aggiungere una nuova sottoscrizione MQTT.

Subscription filter (Filtro sottoscrizione): Inserisci l'argomento MQTT per il quale desideri eseguire la sottoscrizione.

Use device topic prefix (Usa prefisso argomento dispositivo): Aggiungi il filtro sottoscrizione come prefisso all'argomento MQTT.

Subscription type (Tipo di sottoscrizione):

- **Stateless (Privo di stato)**: Seleziona per convertire i messaggi MQTT in messaggi senza stato.
- **Stateful (Dotato di stato)**: Seleziona per convertire i messaggi MQTT in una condizione. Il payload è usato come stato.

QoS: Seleziona il livello desiderato per la sottoscrizione MQTT.

Accessori

I/O ports (Porte I/O)

Utilizzare l'input digitale per collegare i dispositivi esterni che possono passare da un circuito aperto a un circuito chiuso, ad esempio i sensori PIR, i contatti porta o finestra e i rilevatori di rottura del vetro.

Utilizzare l'uscita digitale per collegare dispositivi esterni come relè e LED. È possibile attivare i dispositivi collegati tramite l'API VAPIX® o nell'interfaccia del dispositivo.

Port (Porta)

Name (Nome): modificare il testo per rinominare la porta.

Direction (Direzione):  indica che la porta è una porta di input.  indica che si tratta di una porta di output. Se la porta è configurabile, è possibile fare clic sulle icone per passare dall'input all'output.

Normal state (Stato normale): fare clic su  per il circuito aperto e su per il circuito chiuso.

Current state (Stato corrente): indica lo stato attuale della porta. L'input e l'output vengono attivati quando lo stato corrente è diverso dallo stato normale. Un input sul dispositivo ha un circuito aperto se disconnesso o in caso di tensione superiore a 1 V CC.

Nota

Durante il riavvio, il circuito di output è aperto. Al completamento del riavvio, il circuito torna alla posizione normale. Se si modificano le impostazioni in questa pagina, i circuiti di output tornano alle relative posizioni normali, indipendentemente dai trigger attivi.

Supervised (Supervisionato)  : Attivare per rendere possibile il rilevamento e l'attivazione di azioni se qualcuno manomette la connessione ai dispositivi I/O digitali. Oltre a rilevare se un ingresso è aperto o chiuso, è anche possibile rilevare se qualcuno l'ha manomesso (ovvero se è stato tagliato o corto). Per supervisionare la connessione è necessario un ulteriore hardware (resistori terminali) nel loop I/O esterno.

Registri

Report e registri

Reports (Report)

- **View the device server report (Visualizza il report del server del dispositivo)**: Fare clic su questa opzione per mostrare informazioni sullo stato del dispositivo in una finestra pop-up. Il registro degli accessi viene automaticamente incluso nel report del server.
- **Download the device server report (Scarica il report del server del dispositivo)**: Fare clic per scaricare il report del server. Crea un file .zip che contiene un file di testo del report del server completo in formato UTF-8 e un'istantanea dell'immagine corrente della visualizzazione in diretta. Includere sempre il file .zip del report del server quando si contatta l'assistenza.
- **Download the crash report (Scarica il report dell'arresto anomalo)**: Fare clic per scaricare un archivio con le informazioni dettagliate sullo stato del server. Il report di arresto anomalo contiene le informazioni presenti nel report del server e le informazioni dettagliate sul debug. Questo report potrebbe contenere informazioni riservate, ad esempio l'analisi della rete. Possono volerci alcuni minuti per generare il report.

Logs (Registri)

- **View the system log (Visualizza il registro di sistema)**: Fare clic per visualizzare le informazioni sugli eventi di sistema come l'avvio del dispositivo, gli avvisi e i messaggi critici.
- **View the access log (Visualizza il registro degli accessi)**: Fare clic per mostrare tutti i tentativi non riusciti di accedere al dispositivo, ad esempio quando si utilizza una password di accesso errata.

Network trace (Analisi della rete)

Importante

È possibile che un file di analisi della rete contenga informazioni riservate, ad esempio certificati o password.

Un file di analisi della rete può facilitare la risoluzione dei problemi registrando l'attività sulla rete. Selezionare la durata dell'analisi in secondi o minuti e fare clic su **Download**.

Registro di sistema remoto

Syslog è uno standard per la registrazione dei messaggi. Consente di separare il software che genera messaggi, il sistema che li archivia e il software che li riporta e li analizza. Ogni messaggio è contrassegnato con un codice struttura che indica il tipo di software che genera il messaggio. Inoltre viene assegnato un livello di gravità a tutti i messaggi.

+ **Server**: Fare clic per aggiungere un nuovo server.

Host: immettere il nome host o l'indirizzo IP del server proxy.

Format (Formato): selezionare il formato del messaggio syslog da utilizzare.

- RFC 3164
- RFC 5424

Protocol (Protocollo): selezionare il protocollo e la porta da utilizzare:

- UDP (la porta predefinita è 514)
- TCP (la porta predefinita è 601)
- TLS (la porta predefinita è 6514)

Severity (Gravità): Seleziona quali messaggi inviare al momento dell'attivazione.

CA certificate set (Certificato CA impostato): Visualizza le impostazioni correnti o aggiungi un certificato.

Manutenzione

Restart (Riavvia): Riavviare il dispositivo. Non avrà effetti su nessuna delle impostazioni correnti. Le applicazioni in esecuzione verranno riavviate automaticamente.

Restore (Ripristina): Riporta la *maggior parte* delle impostazioni ai valori predefiniti di fabbrica. In seguito dovrai riconfigurare il dispositivo e le app, reinstallare tutte le app non preinstallate e ricreare eventuali eventi e preset PTZ.

Importante

Dopo il ripristino, le uniche impostazioni salvate sono:

- Protocollo di avvio (DHCP o statico)
- Indirizzo IP statico
- Router predefinito
- Subnet mask
- Impostazioni 802.1X
- Impostazioni O3C

Factory default (Valori predefiniti di fabbrica): Riporta *tutte* le impostazioni ai valori predefiniti di fabbrica. Dopo, per rendere accessibile il dispositivo, devi reimpostare l'indirizzo IP.

Nota

Tutti i firmware per dispositivi Axis sono firmati digitalmente per assicurare di installare solo firmware verificato sul dispositivo. Ciò aumenta ulteriormente il livello di sicurezza informatica minimo globale dei dispositivi Axis. Vedere il white paper "Firmware firmato, avvio sicuro e sicurezza delle chiavi private" presso l'indirizzo *axis.com* per maggiori informazioni.

Firmware upgrade (Aggiornamento del firmware): aggiorna a una versione nuova del firmware. Le nuove versioni di firmware possono contenere funzionalità migliorate, correzioni di bug e funzionalità completamente nuove. Si consiglia di utilizzare sempre l'ultima versione. Per scaricare l'ultima versione, andare a *axis.com/support*.

Quando conduci l'aggiornamento, puoi scegliere fra tre opzioni:

- **Standard upgrade (Aggiornamento standard)**: Aggiorna a una nuova versione del firmware.
- **Factory default (Valori predefiniti di fabbrica)**: Aggiorna e riporta tutte le impostazioni ai valori predefiniti di fabbrica. Se selezioni questa opzione, dopo l'aggiornamento non puoi eseguire il ripristino della versione precedente del firmware.
- **Autorollback (Rollback automatico)**: Aggiorna e conferma l'aggiornamento entro il tempo impostato. Se non dai la conferma, il dispositivo tornerà alla precedente versione del firmware.

Firmware rollback (Rollback del firmware): eseguire il ripristino alla versione del firmware installata precedentemente.

Ulteriori informazioni

Sicurezza

Firmware firmato

Il firmware firmato viene implementato dal fornitore del software che firma l'immagine del firmware con una chiave privata. Quando questa firma è collegata a un firmware, un dispositivo convaliderà il firmware prima di accettare di installarlo. Se il dispositivo rileva che l'integrità del firmware è compromessa, l'aggiornamento del firmware verrà rifiutato.

Avvio sicuro

L'avvio sicuro 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 firmware firmato, l'avvio sicuro assicura che un dispositivo possa essere avviato solo con firmware autorizzato.

Axis Edge Vault

Axis Edge Vault è un modulo di calcolo crittografico sicuro che si può usare per operazioni di crittografia su certificati archiviati in modo sicuro. Edge Vault permette l'archiviazione protetta dalle manomissioni, permettendo a ogni dispositivo la tutela dei propri segreti. Getta le basi per un'implementazione sicura di funzionalità di sicurezza più avanzate.

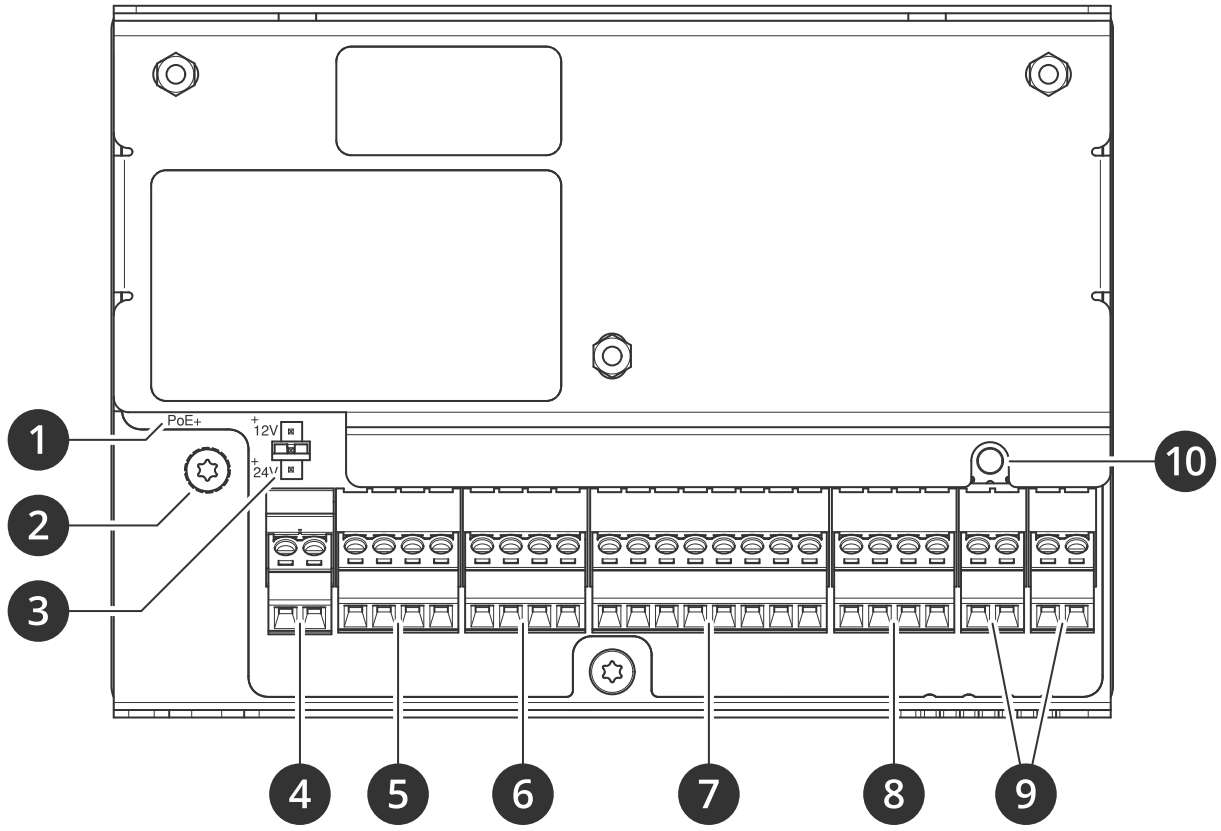
ID dispositivo Axis

L'ID dispositivo Axis funge da passaporto digitale, è unico per ogni unità dispositivo. Viene archiviato in maniera sicura e permanente su Edge Vault come certificato firmato dal certificato root Axis. L'ID dispositivo Axis è pensato per dimostrare l'origine del dispositivo, permettendo un nuovo livello di attendibilità del dispositivo in tutto il suo ciclo di vita.

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

Specifiche

Panoramica del dispositivo



1 *Connettore di rete*
2 *Posizione di messa a terra*
3 *Ponticello relè*
4 *Connettore di alimentazione*
5 *Connettore relè*
6 *Connettore porta*
7 *Connettore lettore*
8 *Connettore ausiliario*
9 *Connettori esterni*
10 *Pulsante di comando*

Il testo contrassegnato con **UL** è valido solo per le installazioni UL 294.

Requisiti di conformità con UL 294

In questa sezione vengono illustrate le informazioni e le istruzioni richieste per la conformità UL. Per assicurare la conformità UL dell'installazione, attenersi alle istruzioni riportate di seguito oltre che alle informazioni e istruzioni di carattere generale fornite all'interno dell'intero documento. Nei casi in cui le informazioni si contraddicano, i requisiti per la conformità UL sono sempre prioritari rispetto alle informazioni e istruzioni di carattere generale.

Livelli di prestazioni per il controllo degli accessi

In questa sezione vengono illustrate le informazioni del livello di prestazioni richieste per la conformità UL 294.

Funzione	Livello
Test attacco distruttivo	I
Sicurezza	I
Durata	IV - Video Intelligente
Alimentazione standby	I

Lettori supportati

- Per UL 294, la compatibilità con i seguenti lettori 485 è stata verificata da UL: AXIS A4020-E, AXIS A4120–E e HID Signo 20.

Istruzioni di sicurezza

- Deve essere installato conformemente all'articolo 725.121 del National Electrical Code, ANSI/NFPA 70.
- L'installazione e la manutenzione del dispositivo Axis devono essere effettuate da un professionista qualificato specializzato.
- Il dispositivo Axis deve essere installato all'interno degli ambienti sottoposti a protezione (area protetta).
- Il dispositivo Axis deve essere installato in ambienti chiusi. L'uso esterno non è stato valutato o approvato da UL.
- Tutti i dispositivi di interconnessione devono essere classificati UL listed e avere potenza limitata a basso voltaggio di Classe 2.
- Tutte le uscita di alimentazione sono uscite di Classe 2.
- Tutti i metodi di cablaggio devono essere eseguiti in conformità con ANSI/NFPA70, i codici e le autorità competenti locali.
- Consigliamo di usare un cavo di messa a terra riconosciuto UL, di dimensioni 14-16 AWG, colore giallo/verde. Crimpa il cavo al terminale ad occhiello da cavo non isolato che è messo a disposizione come pezzo di ricambio del prodotto. È importante servirsi di tecniche e strumenti di crimpaggio adeguati per assicurare la sicurezza di prodotto e utente.
- Quando il dispositivo Axis ha raggiunto la fine della sua vita utile, smaltirlo secondo le leggi e le normative locali. Il dispositivo non deve essere smaltito insieme ai normali rifiuti domestici o commerciali.
- Non connettere il dispositivo Axis a una presa controllata da un interruttore.
- Batteria
    - La batteria al litio da 3,0 V utilizzata nel dispositivo Axis è un componente riconosciuto UL. (Tipo: BR2032, diametro: 20 mm, produttori: Power Glory (Omnergy)). Anche il seguente tipo di batteria è un componente riconosciuto UL: Tipo CR2032.
    - Gli utenti non possono sostituire la batteria. Se la batteria si deve sostituire, l'operazione va effettuata unicamente da un tecnico qualificato.
    - Le batterie usate devono essere smaltite secondo le leggi e i regolamenti locali, che possono variare da stato a stato. Le celle al litio BR/CR non sono né elencate né omesse nelle norme USEPA per i rifiuti pericolosi. Le batterie al litio possono essere considerate rifiuti pericolosi reattivi se la quantità di litio non reagito o non consumato rimanente è considerevole. Per informazioni sullo smaltimento delle batterie al litio utilizzate, contattare l'autorità locale competente per lo smaltimento dei rifiuti.

Specifiche

- Condizioni di funzionamento

Uso normale (non valutato da UL)	Da -40 °C a 55 °C Umidità relativa compresa tra 20% e 85% (senza condensa)
UL 294	Da 0 °C a 55 °C, umidità massima 85%. Pensato per l'uso in alloggiamento classificato "UL listed" con interruttore anti-manomissione.

- Requisiti di cablaggio
  - Devono essere utilizzati cavi UL Listed o R/C AWM con un intervallo del calibro conduttore di AWG 22–14.
  - Il calibro di conduttore minimo per il collegamento tra l'apparecchiatura di alimentazione (PSE) o l'iniettore di alimentazione e il dispositivo alimentato (PD) è 26 AWG.
  - Richiesto per PoE come minimo PoE categoria 5e, cavo schermato.
  - Il dispositivo non è destinato al cablaggio in ambiente esterno, come stabilito dall'Articolo 800 del codice NFPA 70.
- Connettori
  - Connettore di alimentazione: per le applicazioni in ambito di sicurezza UL, l'alimentazione del dispositivo deve essere fornita da un alimentatore a bassa tensione SELV e alimentazione limitata di Classe 2 classificato UL 294 o UL 603.
  - Alimentazione esterna ai relè: se i relè sono connessi a una fonte di alimentazione esterna, deve essere un alimentatore a bassa tensione SELV e alimentazione limitata di Classe 2 classificato come "UL 294 listed".
  - Connettore di rete: cablaggio Ethernet standard. Valutato da UL quando alimentato da AXIS T8133 Midspan 30 W 1-port in modalità PoE B (alternativa A).
  - L'input batteria è destinato alla connessione a un gruppo di continuità in elenco e non è stato valutato da UL secondo UL 294.
  - Gli input supervisionati non sono stati valutati da UL per l'uso antifurto.
- Considerazioni di sistema
  - Il software di monitoraggio non è stato valutato da UL ed è destinato ad uso supplementare.
- Istruzioni di manutenzione
  - Per istruzioni di manutenzione e informazioni su come si configura il dispositivo Axis, consulta il Manuale per l'utente.
- Ulteriori Informazioni
  - Formati tessera verificati da UL: ISO Cards Mifare 1K, 32 bit.
- Alimentazione
  - **Alimentazione in entrata**: Da 10,5 a 28 V CC, max 36 W, max 2,4 A a 10,5 V, max 0,9 A a 28 V. Power over Ethernet (PoE) IEEE 802.3at Tipo 2 Classe 4, max 340 mA. Batteria da 12 V di backup.
  - **Relè**: 2 relè NO/NC, max 2 A CC
  - **Blocco alimentazione in uscita**: 2x 12/24 V CC,
con PoE+: a 12 V, 11 W, a 24 V, 10 W
Con ingresso CC: a 12 V, 22,5 W, a 24 V, 18 W
  - **Alimentazione in uscita lettore**: 12 V CC, max 6 W
  - **Output CC ausiliario**: 1x 12 V CC output, max 200 mA

  - **Power budget complessivo per dispositivi periferici (blocchi, lettori e così via)**: 2.100 mA a 12 V in caso di alimentazione CC, 1.300 mA a 12 V se alimentato da Classe PoE 4

- Interfaccia I/O – Funzionalità I/O
  - **I/O lettore**: output CC: 2 uscite da 12 V CC, max 486 mA; 2 x 2 ingressi/uscite configurabili supervisionati, (input digitale: da 0 a massimo 30 V CC, uscita digitale: da 0 a massimo 30 V CC, open-drain massimo 100 mA)
  - **Dati lettore**: OSDP/RS485 half-duplex, Wiegand
  - **Ausiliaria**: output CC: 1 uscita da 12 V CC, max 200 mA; 4 ingressi/uscite configurabili, (input digitale: da 0 a massimo 30 V CC, uscita digitale: da 0 a massimo 30 V CC, open-drain massimo 100 mA)
  - **Connessioni porte**: 2 x 2 ingressi supervisionati per monitor porte e REX (input digitale: da 0 a max 30 V CC)
  - **Esterno**: 2 ingressi/uscite configurabili per periferiche ausiliarie (input digitale: da 0 a massimo 30 V CC, uscita digitale: da 0 a massimo 30 V CC, open-drain massimo 100 mA)
- Requisiti del cavo
  - **Dimensioni dei cavi per i connettori**: CSA: AWG 28–16, CUL/UL: AWG 30-14
  - **Alimentazione CC e relè**: AWG 18-16
  - **Ethernet e PoE**: STP CAT 5e o superiore
  - **Dati lettore (RS485)**: 1 doppino con schermo, qualificato per un massimo di 1.000 m
  - **Dati lettore (Wiegand)**: qualificato per fino a 150 m
  - **Lettore alimentato dal dispositivo di controllo (RS485)**: AWG 20-16, qualificato fino a 200 m (656 ft) *(a seconda della tensione del lettore e dell'intervallo di ingresso corrente. Valutato con A4020-E e A4120-E.)*
  - **Lettore alimentato dal dispositivo di controllo (Wiegand)**: AWG 20-16, qualificato fino a 150 m (500 ft) *(a seconda della tensione del lettore e dell'intervallo di ingresso corrente.)*
  - **I/O come output**: qualificato per fino a 200 m

Indicatori LED

LED	Colore	Indicazione
Rete	Verde	Luce fissa per connessione di rete a 100 MBit/s. Luce lampeggiante: attività di rete.
	Giallo	Luce fissa per connessione di rete a 10 MBit/s. Luce lampeggiante: attività di rete.
	Spento	Assenza di connessione.
Stato	Verde	Luce verde fissa: condizioni di normale utilizzo.
	Giallo	Fissa durante l'avvio e quando si ripristinano le impostazioni.
	Rosso	Luce lampeggiante lenta: aggiornamento non riuscito.
Alimentazione	Verde	Funzionamento normale.
	Giallo	Luce lampeggiante verde/gialla durante l'aggiornamento del firmware.
Relè	Verde	Relè attivo. [1]
	Spento	Relè inattivo.

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

Pulsanti

Pulsante di comando

Il pulsante di comando viene utilizzato per:

- Ripristino del dispositivo alle impostazioni predefinite di fabbrica. Consultare *Ripristino delle impostazioni predefinite di fabbrica alla pagina 32*.

Connettori

Connettore di rete

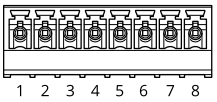
Connettore Ethernet RJ45 con Power over Ethernet Plus (PoE +).

UL: Power over Ethernet (PoE) deve essere fornito da un UL 294 elencato Power over 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-port.

Connettore lettore

Una morsettiera a 8 pin che supporta i protocolli OSDP e Wiegand per la comunicazione con il lettore.

È in grado di connettere un massimo di due lettori OSDP (multi-drop) o un lettore Wiegand. 500 mA a 12 V CC è riservata a tutti i lettori collegati al door controller.



Configurato per un lettore OSDP

Funzione	Pin	Nota	Specifiche
Terra CC (GND)	1		0 V CC
Output CC (+12 V)	2	Fornisce alimentazione al lettore.	12 V CC, max 500 mA
A	3	Half-duplex	
B	4	Half-duplex	

Configurato per due lettori OSDP (multi-drop)

Funzione	Pin	Nota	Specifiche
Terra CC (GND)	1		0 V CC
Output CC (+12 V)	2	Fornisce alimentazione ad entrambi i lettori.	12 V CC, Max 500 mA combinata per entrambi i lettori
A	3	Half-duplex	
B	4	Half-duplex	

Importante

- Quando il lettore è alimentato dal controller, la lunghezza del cavo certificata raggiunge il massimo di 200 m (656 piedi). Verificato unicamente per i lettori Axis.
- Quando il lettore non è alimentato dal controller, la lunghezza del cavo certificata per i dati del lettore raggiunge il massimo di 1000 m (3280,8 piedi) se sono soddisfatti i seguenti requisiti del cavo: 1 doppino con schermatura, AWG 24, impedenza 120 ohm. Verificato unicamente per i lettori Axis.

Configurato per un lettore Wiegand

Funzione	Pin	Nota	Specifiche
Terra CC (GND)	1		0 V CC
Output CC (+12 V)	2	Fornisce alimentazione al lettore.	12 V CC, max 500 mA
D0	3		
D1	4		
LED 1	5	LED rosso	
LED 2	6	LED verde	
MANOMISSIONE	7	Ingresso digitale: collegare al pin 1 per attivarlo oppure lasciarlo isolato (scollegato) per disattivarlo.	Da 0 a max 30 V CC
SEGNALE ACUSTICO	8	Output digitale: se utilizzato 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

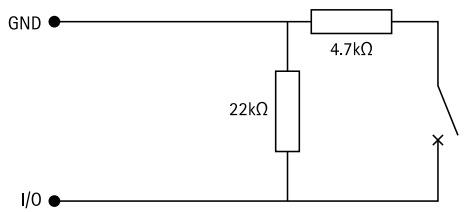
- Quando il lettore è alimentato dal controller, la lunghezza del cavo certificata raggiunge il massimo di 150 m (500 piedi).
- Quando il lettore non è alimentato dal controller, la lunghezza del cavo certificata per i dati del lettore raggiunge il massimo di 150 m (500 piedi) se è soddisfatto il seguente requisito del cavo: AWG 22.

Ingressi supervisionati

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

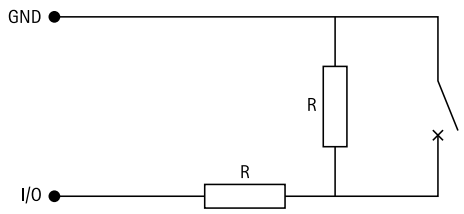
Prima connessione parallela

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



Serial first connection (Prima connessione in serie)

I valori dei resistori devono essere gli stessi e i possibili valori sono 1 kΩ, 2,2 kΩ, 4,7 kΩ e 10 kΩ.



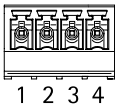
Nota

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

Connettore porta

Una morsettiera a 4 pin utilizzata per i monitor porte (input digitale).

Solo il monitor porte supporta la supervisione con resistori terminali. Se il collegamento viene interrotto, viene attivato un allarme. Per utilizzare input supervisionati, installare resistori terminali. Per gli input supervisionati utilizzare lo schema delle connessioni. Vedere .



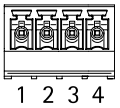
Funzione	Pin	Note	Specifiche
Terra CC	1, 3		0 V CC
Input	2, 4	Per comunicare con il monitor porte. Input digitale o input supervisionato: collegare al pin 1 o 3 rispettivamente per attivarlo oppure lasciarlo isolato (scollegato) per disattivarlo.	Da 0 a max 30 V CC

Importante

La lunghezza certificata del cavo raggiunge il massimo di 30 m (98,4 piedi) se è soddisfatto il seguente requisito del cavo: AWG 24.

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.



Funzione	Pin	Note	Specifiche
Terra CC (GND)	1		0 V CC

NO	2	Normalmente aperto. Per il collegamento di relè. Collegare un blocco di protezione intrinseca tra NO e messa a terra CC. I due pin dei relè sono isolati galvanicamente dal resto dei circuiti se i ponticelli non vengono utilizzati.	Corrente max = 2 A Tensione max = 30 V CC
COM	3	Comuni	
NC	4	Normalmente chiuso. Per il collegamento di relè. Collegare un blocco di protezione intrinseca tra NC e messa a terra CC. I due pin dei relè sono isolati galvanicamente 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	1.600 mA	800 mA
PoE	1200 mA	600 mA

AVVISO

Se il blocco non è polarizzato, si consiglia di aggiungere un diodo di ritorno esterno.

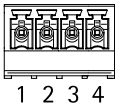
Connettore ausiliario

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:

Input digitale – Per il collegamento di dispositivi che possono passare dal circuito chiuso al circuito aperto, ad esempio i sensori PIR, i contatti porta/finestra e i rilevatori di rottura.

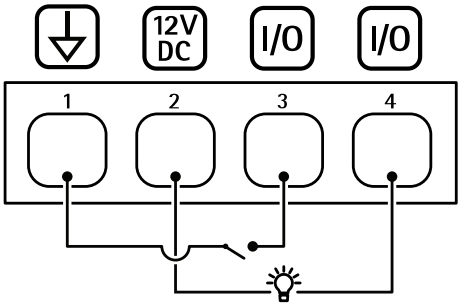
Uscita digitale – Per il collegamento di dispositivi esterni come relè e LED. I dispositivi collegati possono essere attivati tramite l'API (interfaccia per la programmazione di applicazioni) VAPIX® oppure dalla pagina Web del dispositivo.

Morsettiera a 4 pin



Funzione	Pin	Note	Specifiche
Terra CC	1		0 V CC

Output CC	2	Può essere utilizzato per alimentare una periferica ausiliaria. Nota: questo pin può essere usato solo come uscita alimentazione.	12 V CC Carico massimo = 50 mA in totale
Configurabile (input o output)	3–4	Ingresso digitale - collegare al pin 1 per l'attivazione oppure lasciare isolato (scollegato) per la disattivazione.	Da 0 a max 30 V CC
		Uscita digitale - collegato internamente al pin 1 (ground 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. Ogni I/O è in grado di guidare 12 V CC, 50 mA (max) carico esterno, se si utilizza l'uscita interna 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



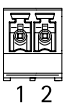
1 *DC ground*
2 *Output CC 12 V*
3 *I/O configurato come input*
4 *I/O configurato come output*

Connettore esterno

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	Specifiche
Terra CC	1		0 V CC
MANOMISSIONE	2	Ingresso digitale - collegare al pin 1 per l'attivazione oppure lasciare isolato (scollegato) per la disattivazione.	Da 0 a max 30 V CC



Funzione	Pin	Note	Specifiche
Terra CC	1		0 V CC
ALLARME	2	Ingresso digitale - collegare al pin 1 per l'attivazione oppure lasciare isolato (scollegato) per la disattivazione.	Da 0 a max 30 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 output nominale limitata a ≤100 W o una corrente nominale di output limitata a ≤5 A.

Funzione	Pin	Nota	Specifiche
Terra CC (GND)	1		0 V CC
Input CC	2	Per l'alimentazione del controller 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 294 o UL 603, a seconda dell'applicazione, dotato delle classificazioni appropriate.

Risoluzione di 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 ai valori predefiniti di fabbrica:

1. Scollegare l'alimentazione dal dispositivo.
2. Tenere premuto il pulsante di comando quando si ricollega l'alimentazione. Consultare *Panoramica del dispositivo alla pagina 22*.
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. Il processo è completo quando il LED di stato diventerà verde. Il dispositivo è stato reimpostato alle impostazioni di fabbrica predefinite. Se nessun server DHCP è disponibile sulla rete, l'indirizzo IP predefinito è `192.168.0.90`.
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 la pagina Web del dispositivo. Andare a **Maintenance (Manutenzione)** > **Factory default (Impostazione di fabbrica)** e fare clic su **Default (Predefinito)**.

Opzioni firmware

Axis offre la gestione del firmware 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 il firmware 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 di firmware del dispositivo AXIS, visitare *axis.com/support/firmware*.

Controllo della versione firmware corrente

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

Per controllare il firmware corrente:

1. Vai all'interfaccia del dispositivo > **Status (Stato)**.
2. Vedere la versione firmware in **Device info (Informazioni dispositivo)**.

Aggiornamento del firmware

Importante

- Le impostazioni preconfigurate e personalizzate vengono salvate quando aggiorni il firmware (a condizione che le funzioni siano disponibili nel nuovo firmware), sebbene ciò non sia garantito da Axis Communications AB.
- Assicurarsi che il dispositivo rimanga collegato alla fonte di alimentazione durante il processo di aggiornamento.

Nota

Quando si aggiorna il dispositivo con il firmware più recente 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 di aggiornare il firmware. Per il firmware più aggiornato e le note sul rilascio, visitare il sito Web *axis.com/support/firmware*.

Nota

Dal momento che il database di utenti, gruppi, credenziali e altri dati viene aggiornato dopo un aggiornamento firmware, il completamento del primo avvio potrebbe richiedere alcuni minuti. Il tempo richiesto dipende dalla quantità di dati.

1. Scarica il file del firmware sul tuo computer, disponibile gratuitamente su *axis.com/support/firmware*.
2. Accedi al dispositivo come amministratore.
3. Andare a **Maintenance > Firmware upgrade (Manutenzione > Aggiornamento firmware)** e fare clic su **Upgrade (Aggiorna)**.

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

4. Una volta riavviato il dispositivo, cancellare la cache del browser Web.

Problemi tecnici, indicazioni e soluzioni

Se non si riesce a individuare qui ciò che si sta cercando, provare a vedere la sezione relativa alla risoluzione dei problemi all'indirizzo *axis.com/support*.

Problemi durante l'aggiornamento del firmware	
Errore durante l'aggiornamento del firmware	Se l'aggiornamento del firmware non riesce, il dispositivo ricarica il firmware precedente. Il motivo più comune è il caricamento di un firmware errato. Controllare che il nome del file del firmware corrisponda al dispositivo e riprovare.
Problemi dopo l'aggiornamento del firmware	Se si riscontrano problemi dopo l'aggiornamento del firmware, ripristinare la versione installata in precedenza dalla pagina **Maintenance (Manutenzione)**.

Problemi durante l'impostazione dell'indirizzo IP	
Il dispositivo si trova su una subnet diversa	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 è già utilizzato da un altro dispositivo	Scollegare il dispositivo Axis dalla rete. Eseguire il comando ping (in una finestra di comando/DOS digitare `ping` e l'indirizzo IP del dispositivo): • Se si riceve: `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. • 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.
Possibile conflitto dell'indirizzo IP con un altro dispositivo nella 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.

Impossibile accedere al dispositivo da un browser

Non è possibile eseguire l'accesso	Se HTTPS è abilitato, assicurarsi di utilizzare il protocollo corretto (HTTP o HTTPS) quando si tenta di eseguire l'accesso. Potrebbe essere necessario digitare manualmente `http` o `https` nel campo dell'indirizzo del browser. Se si dimentica la password per l'utente root, il dispositivo deve essere ripristinato alle impostazioni predefinite di fabbrica. Vedere *Ripristino delle impostazioni predefinite di fabbrica alla pagina 32*.
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)**.

L'accesso al dispositivo può essere eseguito in locale ma non esternamente

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

- AXIS Companion: gratuito, ideale per piccoli sistemi con esigenze di sorveglianza di base.
- AXIS Camera Station: versione di prova di 30 giorni gratuita, ideale per sistemi di piccole e medie dimensioni.

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

Contattare l'assistenza

Contatta l'assistenza all'indirizzo *axis.com/support*.

Manuale per l'utente

Ver. M2.2
Data: Marzo 2023
Codice T10181041