AXIS TP3604-E Cellular Back Box

Manuale dell'utente

Indice

Installazione....3
Impostazioni preliminari....4
Individuazione del dispositivo sulla rete....4
Supporto browser....4
Aprire l'interfaccia Web del dispositivo....4
Creare un account amministratore....4
Password sicure....4
Accertarsi che nessuno abbia manomesso il software del dispositivo....5
Configurare il dispositivo....6
Gestione SIM....6
Impostare un APN....6
Verificare la potenza del segnale e l'indirizzo IP....6
Controllare la connettività....6
Verificare le porte di gestione....6
Attivare l'inoltro alla telecamera....7
Configurare la proprietà dell'indirizzo IP della telecamera....7
Modalità locale....8
Modalità passante....8
Imposta regole per eventi....9
Attivazione di un'azione....9
Attivare una notifica all'apertura dell'involucro....9
Interfaccia Web....10
Dati tecnici....11
Panoramica dei prodotti....11
Indicatori LED....11
Pulsanti....12
Pulsante di comando....12
Connettori....12
Connettore di input PoE (PoE in)....12
Connettore di rete (PoE OUT)....12
Connettore di alimentazione....12
Pulizia del dispositivo....13
Risoluzione dei problemi....14
Ripristinare le impostazioni predefinite di fabbrica....14
Opzioni AXIS OS....14
Controllo della versione corrente del AXIS OS....14
Aggiornare AXIS OS....15
Problemi tecnici e possibili soluzioni....15
Contattare l'assistenza....17
Cyber security....18
Gestione delle vulnerabilità....18
Notifiche di sicurezza....18
Ciclo di vita sicuro del prodotto....18

Installazione



Il video illustra come installare AXIS TP3604-E Cellular Back Box con le telecamere a cupola fissa della serie AXIS P32 Dome Camera e in formato bullet della serie AXIS P14 Bullet Camera.

Per istruzioni che riguardano tutti gli scenari di installazione e le informazioni di sicurezza, consultare la guida all'installazione.

Impostazioni preliminari

Individuazione del dispositivo sulla rete

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. Digitare il nome utente e password. Se si accede al dispositivo per la prima volta, è necessario creare un account amministratore. Vedere *Creare un account amministratore, on page 4*.

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

Creare un account amministratore

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

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

Password sicure

Importante

Utilizza il protocollo HTTPS (abilitato per impostazione predefinita) per configurare la password o altre configurazioni sensibili tramite la rete. Il protocollo HTTPS abilita collegamenti di rete sicuri e crittografati, garantendo così la protezione dei 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.

Accertarsi che nessuno abbia manomesso 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. Configurare e installare il dispositivo.

Configurare il dispositivo

Per configurare il dispositivo, effettuare i seguenti passaggi:

1. *Gestione SIM, on page 6*
2. Se la rete richiede un nome access point (APN) esplicito, *Impostare un APN, on page 6*
3. *Verificare la potenza del segnale e l'indirizzo IP, on page 6*
4. *Controllare la connettività, on page 6*
5. *Verificare le porte di gestione, on page 6*
6. *Attivare l'inoltro alla telecamera, on page 7*

Gestione SIM

La gestione della SIM è obbligatoria quando il PIN della SIM è abilitato. Se il PIN della SIM è disabilitato, si può saltare questo passaggio.

1. Inserire la scheda SIM. Andare a **Modem > SIM management > SIM status (Modem > Gestione SIM > Stato SIM)** per verificare il rilevamento del modem/della SIM.
2. Se il PIN della SIM è bloccato, andare a **Modem > SIM management > SIM PIN > Unlock (Modem > Gestione SIM > PIN SIM > Sblocca)** per sbloccarlo inserendo il PIN corretto.

Impostare un APN

Nota

È necessario eseguire questo passaggio solo se la propria rete richiede un APN (Access Point Name) esplicito.

Per impostare un APN esplicito, andare a **Modem > Cellular network > APN (Modem > Rete cellulare > APN)**.

Verificare la potenza del segnale e l'indirizzo IP

Nota

Questo passaggio richiede l'accesso alla rete cellulare.

1. Verificare la potenza del segnale in **System > Modem > Cellular network > Radio parameters > Signal strength index (Sistema > Modem > Rete cellulare > Parametri radio > Indice di intensità del segnale)**. Tre o quattro tacche indicano una buona qualità del segnale.
2. In **System > Modem > Cellular network > User equipment IP address (Sistema > Modem > Rete cellulare > Indirizzo IP dell'apparecchiatura utente)**, verificare che sia stato ricevuto un indirizzo IP della rete cellulare.

Controllare la connettività

Nota

Questo passaggio richiede l'accesso alla rete cellulare.

1. Andare a **System > Modem > Cellular network > Test cellular connection (Sistema, Modem, Rete cellulare, Test connessione cellulare)**. Inserire un nome host o un indirizzo IP.
2. Verificare che il test di connessione abbia esito positivo.

Verificare le porte di gestione

Prima di attivare la modalità di instradamento finale, verificare le porte di gestione della back box.

1. Andare a **Cellular routing > Back box management ports (Routing cellulare, porte di gesionte back box)**.
2. Modificare le porte se i valori predefiniti non sono supportati dalla rete.

Attivare l'inoltro alla telecamera

L'ultimo passaggio consiste nell'attivare l'inoltro alla telecamera.

1. Andare a **routing > Main mode (Routing cellulare, Modalità principale)** e fare clic su **Enable forwarding to connected device (Abilita inoltro al dispositivo connesso)**.

Una volta abilitato l'inoltro, le porte di servizio standard vengono reindirizzate alla telecamera, mentre la gestione del backbox rimane disponibile tramite le porte di gestione riservate.

2. Verificare l'accesso alla telecamera: In un browser Web, inserire l'indirizzo IP del cellulare seguito dal numero di porta 80, `http://<cellular-ip-address>:80`.
3. Verificare l'accesso al back box: In un browser Web, inserire l'indirizzo IP del dispositivo cellulare seguito dal numero di porta 11080 (la porta predefinita per la gestione del back box tramite HTTP), `http://<cellular-ip-address>:11080`.

Configurare la proprietà dell'indirizzo IP della telecamera

Nota

Questo passaggio è facoltativo ed è necessario solo se si desidera effettuare una modifica del comportamento predefinito della subnet o per ottimizzarlo.

Una rete cellulare assegna un solo indirizzo IP, che è legato all'identità della scheda SIM. Un'installazione standard prevede una back boc e una telecamera connessa. La modalità DHCP determina quale IP viene assegnato alla telecamera come "proprio". Questa è la decisione fondamentale alla base della scelta della modalità di un server DHCP.

Per impostazione predefinita (modalità locale), l'indirizzo IP del dispositivo cellulare rimane associato alla back box e alla telecamera viene assegnato un indirizzo IP privato dalla rete locale della back box. La telecamera è ancora completamente accessibile dalla rete cellulare. Nella maggior parte dei casi, questo è tutto ciò che serve e garantisce che la telecamera rimanga isolata in modo sicuro su una rete privata.

La differenza diventa evidente quando uno strumento analizza l'IP dal punto di vista della telecamera stessa. Se un VMS rileva l'indirizzo IP segnalato dalla telecamera, oppure se la telecamera è configurata in modo da inserire il proprio indirizzo IP in una sovrapposizione testo del video, tale indirizzo IP corrisponderà all'indirizzo IP privato della LAN della telecamera, non all'indirizzo IP pubblico del cellulare che il mondo esterno utilizza per raggiungerla. I due indirizzi non corrispondono, perché l'IP del cellulare appartiene all'identità della scheda SIM presente nella back box, non alla telecamera.

La modalità passante risolve questo problema prendendo il singolo indirizzo IP che la rete cellulare assegna alla back box e inoltrandolo alla telecamera. Con la funzione passante abilitata, la telecamera possiede esattamente lo stesso indirizzo IP della rete cellulare, quindi l'indirizzo che la telecamera comunica (e mostra in una sovrapposizione testo del video) è lo stesso indirizzo utilizzato per raggiungerla da remoto. Poiché la telecamera ora dispone dell'identità cellulare, questa scelta modifica anche il modo in cui essa può comunicare con altri dispositivi degli utenti (UE) sulla rete cellulare.

Il resto di questa sezione descrive in dettaglio ciascuna modalità.

È possibile accedere alla telecamera collegata alla back box tramite IP cellulare sulle porte standard (`80/443/554/22`) ed è comunque possibile accedere alla back box tramite le porte di gestione riservate (ad esempio`11080/11443/11554/11022`).

La differenza tra la modalità Locale e la modalità Passante:

Modalità locale

- Alla telecamera viene assegnata una subnet locale privata.
- L'indirizzo IP interno della telecamera è diverso dall'indirizzo IP raggiungibile tramite cellulare.
- In caso di dubbio, utilizzare la modalità DHCP locale.

Modalità passante

- Alla telecamera viene assegnato l'indirizzo IP del cellulare.

Modalità locale

Attivare la modalità locale

1. In **Cellular routing > Advanced DHCP configuration > DHCP server mode (Routing cellulare, Configurazione DHCP avanzata, Modalità server DHCP)**, selezionare **Local (Locale)**.
2. Verificare che l'indirizzo IP locale della telecamera non sia in conflitto con nessun altro indirizzo IP raggiungibile nella rete: **Cellular routing > Advanced DHCP configuration > Local private network configuration (Routing cellulare, Configurazione DHCP avanzata, Configurazione della rete privata locale)**
3. Se necessario, modificare l'indirizzo IP in **Cellular routing > Advanced DHCP configuration > Local private network configuration (Routing cellulare, Configurazione DHCP avanzata, Configurazione rete privata locale)**. Impostare lo stesso valore sia per **Starting IP address (Indirizzo IP iniziale)** che per **Ending IP address (Indirizzo IP finale)**.
4. Fare clic su **Save (Salva)**.

Modalità passante

Se gli UE (User Equipment, equipaggiamenti utente, ovvero le telecamere) non comunicano tra loro e il traffico proviene sempre da un'altra LAN del VMS verso gli UE, non esiste un percorso da UE a UE per l'IP shadowing. In tal caso, la modalità passante è considerata sicuro dal punto di vista dello shadowing IP.

In linea di massima, ciò significa che la rete cellulare viene ampliata lato telecamera. Ciò è utile quando la telecamera deve essere visibile direttamente all'indirizzo IP associato alla rete cellulare.

Rischio importante: Shadowing IP in modalità passante

Questa descrizione dei rischi si applica alle configurazioni con una sola telecamera. Anche con una sola telecamera, la modalità passante richiede comunque due indirizzi IP sulla subnet lato LAN:

- Un indirizzo IP per la telecamera.
- Un indirizzo IP per il server DHCP della back box lato Ethernet.

Scenario 1: Subnet minima per UE `(/30)`

In questo modello, ogni UE dispone di una piccola subnet indipendente.

- Un `(/30)` fornisce due indirizzi IP host utilizzabili.
- La telecamera utilizza un indirizzo IP.

L'indirizzo IP di riserva viene utilizzato internamente dal server DHCP della back box.

Raccomandazione per lo scenario 1:

- Mantenere separate le singole subnet UE.
- Controllare che ogni subnet UE sia univoca. Evitare che le subnet si sovrappongano tra i dispositivi UE.

Scenario 2: Subnet condivisa più ampia con numerosi UE

In alcune implementazioni viene utilizzata un'unica subnet più ampia, condivisa da più UE. Il rischio di shadowing si verifica se la telecamera tenta di connettersi a un altro UE che utilizza lo stesso IP del server DHCP della back box. In tal caso, il traffico potrebbe essere indirizzato all'indirizzo locale della back box anziché all'UE remoto di destinazione.

Raccomandazione per lo scenario 2:

- Controllare l'indirizzo IP del server DHCP indicato sul retro del dispositivo nelle impostazioni della modalità passante.
- Controllare che tale indirizzo IP non sia assegnato a nessun altro UE.
- Controllare che tale indirizzo IP non sia assegnato a nessuna SIM nel portale dei servizi di rete.

Attivare la modalità passante

Nota

È indispensabile l'accesso alla rete cellulare.

1. In **Cellular routing > Advanced DHCP configuration > DHCP server mode (Routing cellulare, Configurazione DHCP avanzata, Modalità server DHCP)** selezionare **Passthrough (Passante)**.
2. In **Cellular routing > Advanced DHCP configuration > Local private network configuration > Server IP and prefix length (Routing cellulare, Configurazione DHCP avanzata, Configurazione rete privata locale, IP e lunghezza prefisso server**, verificare che l'IP e la lunghezza del prefisso di subnet del server selezionati automaticamente non siano in conflitto con altri indirizzi IP raggiungibili.
3. Fare clic su **Save (Salva)**.

Imposta regole per eventi

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

Attivazione di un'azione

1. Andare a **System (Sistema)** > **Events (Eventi)** e fare clic su **+ Add a rule (Aggiungi 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)** deve eseguire il dispositivo quando le condizioni sono soddisfatte.

Attivare una notifica all'apertura dell'involucro

Questo esempio spiega come impostare una notifica via e-mail quando la custodia o l'involucro del dispositivo viene aperto.

Aggiungere un destinatario e-mail:

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

Creare una regola:

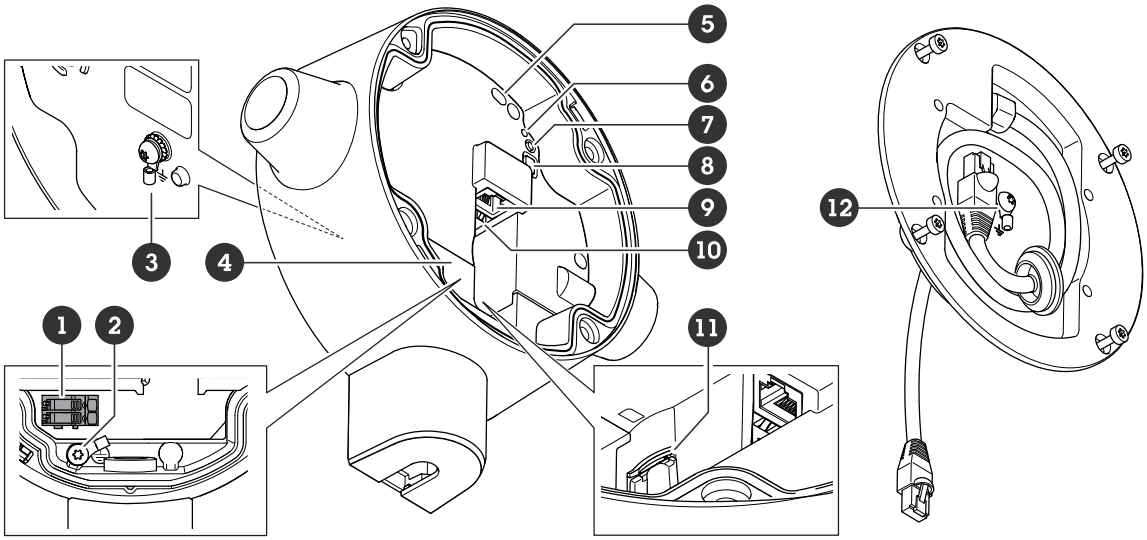
9. Andare a **System > Events > Rules (Sistema > Eventi > Regole)** e fare clic su **Add a rule (Aggiungi una regola)**.
10. Inserire un nome per la regola.
11. Nell'elenco delle condizioni, selezionare **Casing open (Alloggiamento aperto)**.
12. Dall'elenco delle azioni, selezionare **Send notification to email (Invia notifica via email)**.
13. Selezionare un destinatario dall'elenco.
14. Digitare un oggetto e il messaggio per l'e-mail.
15. Fare clic su **Save (Salva)**.

Interfaccia Web

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

Dati tecnici

Panoramica dei prodotti



1 *Connettore CA*
2 *Massa di protezione*
3 *Vite di terra*
4 *Copertura di protezione (AC)*
5 *Rilevatore apertura alloggiamento*
6 *Pulsante di ripristino*
7 *LED di stato*
8 *Pulsante di comando*
9 *Uscita PoE (dati)*
10 *Ingresso PoE*
11 *Alloggiamento scheda SIM*
12 *Vite di massa (telecamera)*

Indicatori LED

LED di stato in modalità impostazione

LED di stato	Significato
Spento	Il sensore IR di rilevamento alloggiamento è coperto.
Verde	Funzionamento normale, l'interfaccia Ethernet è pronta.
Giallo	Luce fissa durante l'avvio. Lampeggia durante l'aggiornamento del software del dispositivo o il ripristino delle impostazioni predefinite.
Giallo/rosso	Non è presente alcuna connessione Ethernet e il modem viene configurato all'avvio.
Rosso	Errore durante l'aggiornamento del software del dispositivo.

LED di stato in modalità connessa

LED di stato	Significato
Spento	Il sensore IR di rilevamento alloggiamento è coperto.
Verde	Il modem non è collegato alla rete.
Giallo	Luce fissa durante l'avvio. Lampeggia durante l'aggiornamento del software del dispositivo o il ripristino delle impostazioni predefinite.

Giallo/rosso	Il modem viene configurato durante l'avvio.
Rosso	Errore durante l'aggiornamento del software del dispositivo.

Pulsanti

Pulsante di comando

Il pulsante di comando viene utilizzato per:

- Ripristino del dispositivo alle impostazioni predefinite di fabbrica. Vedere *Ripristinare le impostazioni predefinite di fabbrica, on page 14*.
- 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 input PoE (PoE in)

Connettore RJ45 Ethernet con Power over Ethernet (PoE) IEEE 802.3af/802.3at/802.3bt Tipo 3 Classe 5.

Nota

Questo connettore è utilizzato esclusivamente per l'input di alimentazione; non è disponibile alcun collegamento di rete.

Nota

- È necessario un input CA per l'output PoE IEEE 802.3at Tipo 2 Classe 4.
- Per un output PoE IEEE 802.3at Tipo 1 Classe 3, è richiesto IEEE 802.3at Tipo 2 Classe 4 o superiore.
- Per l'input PoE IEEE 802.3af Tipo 1 Classe 3, il dispositivo è operativo ma non eroga potenza.

Nota

La lunghezza massima del cavo Ethernet è di 20 m.

Connettore di rete (PoE OUT)

Connettore Ethernet RJ45.

Nota

- È necessario un input CA per l'output PoE IEEE 802.3at Tipo 2 Classe 4.
- Per un output PoE IEEE 802.3at Tipo 1 Classe 3, è richiesto IEEE 802.3at Tipo 2 Classe 4 o superiore.
- Per l'input PoE IEEE 802.3af Tipo 1 Classe 3, il dispositivo è operativo ma non eroga potenza.

Nota

La lunghezza massima del cavo Ethernet è di 20 m.

Connettore di alimentazione

Morsettiera per il collegamento all'alimentazione CA.

Nota

È necessario un input CA per l'output PoE IEEE 802.3at Tipo 2 Classe 4.

Pulizia del dispositivo

È possibile pulire il dispositivo con acqua tiepida e sapone delicato, non abrasivo.

AVVISO

- Le sostanze chimiche possono danneggiare il dispositivo. Non utilizzare sostanze chimiche come detergenti per vetri o acetone per pulire il dispositivo.
- Evitare la pulizia alla luce diretta del sole o a temperature elevate, poiché ciò può causare macchie.

1. Utilizzare una bomboletta d'aria compressa per rimuovere polvere e sporcizia dal dispositivo.
2. Se necessario, pulire il dispositivo con un panno morbido in microfibra inumidito con acqua tiepida e sapone delicato, non abrasivo.
3. Per rimuovere eventuali prodotti per la pulizia, pulire il dispositivo con un panno morbido in microfibra inumidito con acqua tiepida.
4. Per evitare macchie, asciugare il dispositivo con un panno pulito e non abrasivo.

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

Risoluzione dei problemi

Ripristinare le 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 11*.
3. Tenere premuto il pulsante di comando per circa 15-30 secondi fino a quando il LED di stato non lampeggia in giallo.
4. Rilasciare il pulsante di comando. La procedura è terminata quando il LED di stato diventa verde. Se nella rete non è disponibile un server DHCP, l'indirizzo IP del dispositivo sarà predefinito con uno dei seguenti valori:
   - **Dispositivi con AXIS OS 12.0 e versioni successive:** ottenuti dalla subnet degli indirizzi di collegamento locale (169.254.0.0/16)
   - **Dispositivi con AXIS OS 11.11 e precedenti:** 192.168.0.90/24
5. Utilizzare gli strumenti per l'installazione e la gestione del software per assegnare un indirizzo IP, impostare la password e accedere al dispositivo.
   Gli strumenti per l'installazione e la gestione del software sono disponibili nelle pagine dedicate all'assistenza sul sito Web *axis.com/support*.

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

Opzioni AXIS OS

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

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

Controllo della versione corrente del AXIS OS

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

Per controllare la versione corrente di AXIS OS:

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

Aggiornare AXIS OS

Importante

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

Nota

- Quando si aggiorna il dispositivo con la versione più recente di AXIS OS nella traccia attiva, il dispositivo riceve le ultime funzionalità disponibili. Leggere sempre le istruzioni di aggiornamento e le note di rilascio disponibili con ogni nuova versione prima dell'aggiornamento. Per la versione AXIS OS più aggiornata e le note sul rilascio, visitare il sito Web *axis.com/support/device-software*.

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

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

Problemi tecnici e possibili soluzioni

Problemi durante l'aggiornamento di AXIS OS

Aggiornamento di AXIS OS non riuscito

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

Problemi dopo l'aggiornamento di AXIS OS

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

Problemi durante l'impostazione dell'indirizzo IP

Impossibile impostare l'indirizzo IP

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

Problemi di accesso al dispositivo

Impossibile effettuare l'accesso al dispositivo tramite un browser.

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

Se si è smarrita la password per l'account root, è necessario ripristinare le impostazioni predefinite di fabbrica del dispositivo. Per le istruzioni, vedere *Ripristinare le impostazioni predefinite di fabbrica, on page 14*.

L'indirizzo IP è stato modificato dal server DHCP

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

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

Errore del certificato durante l'utilizzo di IEEE 802.1X

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

Il browser non è supportato

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

Impossibile accedere al dispositivo dall'esterno

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

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

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

Problemi con MQTT

Impossibile collegarsi tramite la porta 8883 con MQTT su SSL

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

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

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

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

Contattare l'assistenza

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

Cyber security

La sicurezza informatica sostiene un ciclo di vita del prodotto ottimale con rischi ridotti al minimo. È possibile trovare informazioni approfondite e documentazione sul nostro approccio alla sicurezza informatica all'indirizzo *axis.com/about-axis/cybersecurity*. Segui le linee guida sulla sicurezza informatica riportate di seguito per ricevere le notifiche di sicurezza relative al prodotto da parte di Axis e per configurare il prodotto per garantirne un ciclo di vita e una dismissione sicuri.

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

Gestione delle vulnerabilità

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

Notifiche di sicurezza

Iscriversi alle e-mail di notifica sulla sicurezza di Axis all'indirizzo *axis.com/security-notification-service*. Ti invieremo informazioni relative alle vulnerabilità, alle relative note di sicurezza e ad altre questioni relative alla sicurezza del tuo prodotto Axis.

Ciclo di vita sicuro del prodotto

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

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

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

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

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

T10233346_it

2026-10 (M2.2)

© 2026 Axis Communications AB