

AXIS P3265-LVE-3 License Plate Verifier Kit

Indice

Impostazioni preliminari	4
Individuazione del dispositivo sulla rete	4
Supporto browser	4
Aprire l'interfaccia Web del dispositivo	4
Crea un account amministratore	4
Password sicure	5
Verificare che nessuno abbia alterato il software del dispositivo	5
Panoramica dell'interfaccia Web	5
Configurazione di base	6
Consigli sul montaggio della telecamera	6
Assistente alla configurazione	8
Libera circolazione	8
Controllo accessi	9
Accedi alle impostazioni dell'applicazione	10
Regolare l'area di interesse	10
Selezionare la regione	11
Regolare le impostazioni di acquisizione	11
Configurazione dell'archiviazione degli eventi	11
Installazione	13
Modalità anteprima	13
Configurare il dispositivo	14
Per gli utenti di AXIS Camera Station	14
Impostare AXIS License Plate Verifier	14
Impostazioni di base	14
Regolare l'immagine	14
Ridurre i tempi di elaborazione delle immagini con la modalità a bassa latenza	14
Selezione della modalità di esposizione	15
Compensazione dell'effetto barile	15
Verificare la risoluzione dei pixel	15
Visualizzare e registrare video	16
Ridurre la larghezza di banda e dello spazio di archiviazione	16
Configurazione dell'archiviazione di rete	17
Registrare e guardare video	17
Verifica che nessuno abbia alterato il video	17
Imposta regole per eventi	18
Registrare video quando la telecamera rileva una targa	18
Attivazione di una notifica in caso di manomissione dell'obiettivo della telecamera	18
Audio	19
Aggiunta di audio alla registrazione	19
Aggiungi funzionalità audio al dispositivo usando portcast	19
Gestione degli elenchi	20
Aggiunta all'elenco della targa rilevata	20
Aggiunta di descrizioni alle targhe	20
Personalizzazione dei nomi degli elenchi	21
Importazione di numeri di targhe consentite	22
Condividere elenchi delle targhe con altre telecamere	23
Elenchi di pianificazione	24
Impostazioni supplementari	25
Configurare sovrapposizione testo	25
Rileva targhe in condizioni di scarsa illuminazione	25
Consentire un minor numero di caratteri sulle targhe	25
Consenti solo corrispondenze esatte di targhe	25
Consentire più di una deviazione di carattere quando si confrontano le targhe	25

Accesso limitato agli operatori.....	26
Impostare una connessione sicura.....	26
Backup e ripristino delle impostazioni delle app.....	26
Cancellazione di tutti gli eventi	26
Usa porte virtuali per l'attivazione di azioni	26
Scenario di ingresso e uscita veicoli	28
Aprire una barriera per i veicoli noti utilizzando un modulo relè	28
Aprire una barriera per i veicoli noti utilizzando l'I/O della telecamera	29
Ricevi una notifica relativa a un veicolo non autorizzato	30
Scenario di controllo degli accessi dei veicoli	31
Connetti a un dispositivo di controllo porte.....	31
Connettere ad AXIS Secure Entry	33
Scenario con flusso libero con misurazione della velocità	35
Configurare lo scenario.....	35
Cercare eventi specifici.....	37
Esportare e condividere i risultati della ricerca.....	37
Integrazione.....	38
Utilizzare i profili per inviare gli eventi a più server.....	38
Inviare le informazioni relative agli eventi a software di terze parti	38
Invio a un server di immagini di targhe.....	39
Integrazione diretta con 2N.....	39
Integrazione con Genetec Security Center.....	40
Interfaccia Web	43
Per saperne di più	44
Tecnologia edge-to-edge	44
Abbinamento radar.....	44
Associazione altoparlante.....	44
Area di visualizzazione.....	44
AXIS Image Health Analytics.....	44
Dati tecnici	46
Panoramica dei prodotti.....	46
Indicatori LED	46
Slot per scheda SD	47
Pulsanti.....	47
Pulsante di comando.....	47
Connettori.....	47
Connettore di rete	47
Connettore audio.....	47
Connettore I/O	47
Risoluzione dei problemi.....	49
Ripristino delle impostazioni predefinite di fabbrica.....	49
Opzioni AXIS OS.....	49
Controllo della versione corrente del AXIS OS.....	49
Aggiornare AXIS OS.....	50
Problemi tecnici e possibili soluzioni	50
.....	53
Considerazioni sulle prestazioni	54
Contattare l'assistenza.....	54
Cyber security.....	55
Gestione delle vulnerabilità	55
Notifiche di sicurezza	55
Ciclo di vita sicuro del prodotto	55

Impostazioni preliminari

Individuazione del dispositivo sulla rete

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

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

Supporto browser

Il dispositivo può essere utilizzato con i seguenti browser:

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

✓: Consigliato

*: Supportato con limitazioni

Aprire l'interfaccia Web del dispositivo

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

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

Crea un account amministratore

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

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

Importante

Il dispositivo non ha un account predefinito. In caso di smarrimento della password dell'account amministratore, è necessario reimpostare il dispositivo. Vedere *Ripristino delle impostazioni predefinite di fabbrica, on page 49*.

Password sicure

Importante

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

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

Per proteggere i dati consigliamo vivamente di:

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

Verificare che nessuno abbia alterato il software del dispositivo

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

1. Ripristinare le impostazioni predefinite di fabbrica. Vedere *Ripristino delle impostazioni predefinite di fabbrica, on page 49*.
Dopo il ripristino, l'avvio sicuro garantisce lo stato del dispositivo.
2. Configurare e installare il dispositivo.

Panoramica dell'interfaccia Web

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



Interfaccia Web dei dispositivi Axis

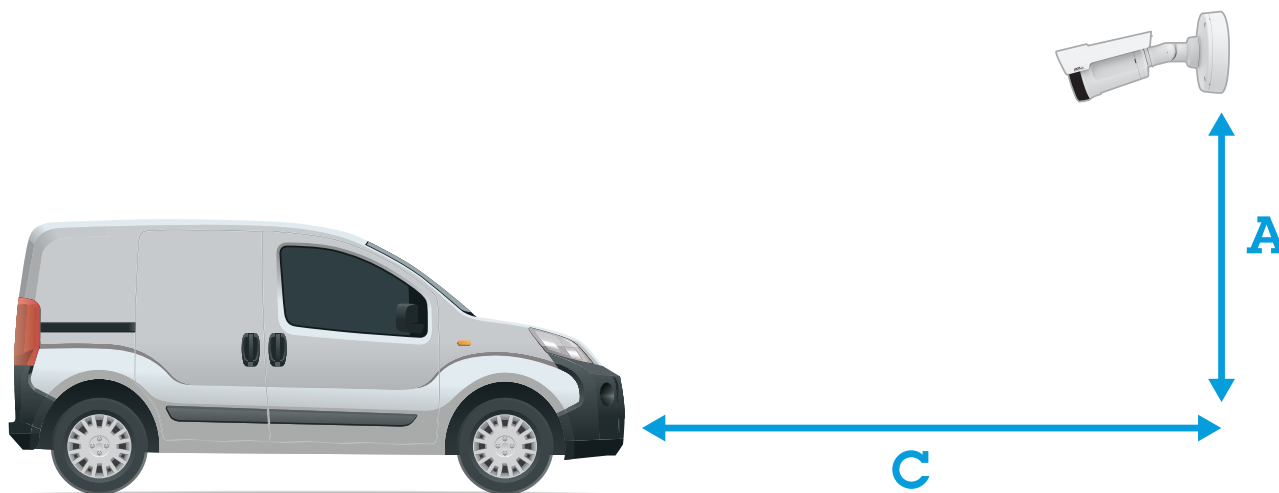
Configurazione di base

Queste istruzioni per la configurazione sono valide per tutti gli scenari:

- 1.
- 2.
3. *Regolare l'area di interesse, on page 10*
4. *Selezionare la regione, on page 11*
5. *Configurazione dell'archiviazione degli eventi, on page 11*

Consigli sul montaggio della telecamera

- Quando si seleziona la posizione di montaggio, ricordare che la luce solare diretta può distorcere l'immagine, ad esempio, durante l'alba e il tramonto.
- In uno scenario **Access control (Controllo degli accessi)**, è necessario che l'altezza di montaggio corrisponda alla metà della distanza che intercorre fra il veicolo e la telecamera.
- In uno scenario **Free flow (Libera circolazione)** (riconoscimento targhe nel traffico a bassa velocità) è necessario che l'altezza di montaggio per la telecamera sia minore rispetto alla distanza che intercorre fra il veicolo e la telecamera.



Distanza di acquisizione del sistema di **controllo degli accessi**: 2-7 m (6,6-23 ft). Questo è un esempio che si basa su AXIS P3265-LVE-3 License Plate Verifier kit.

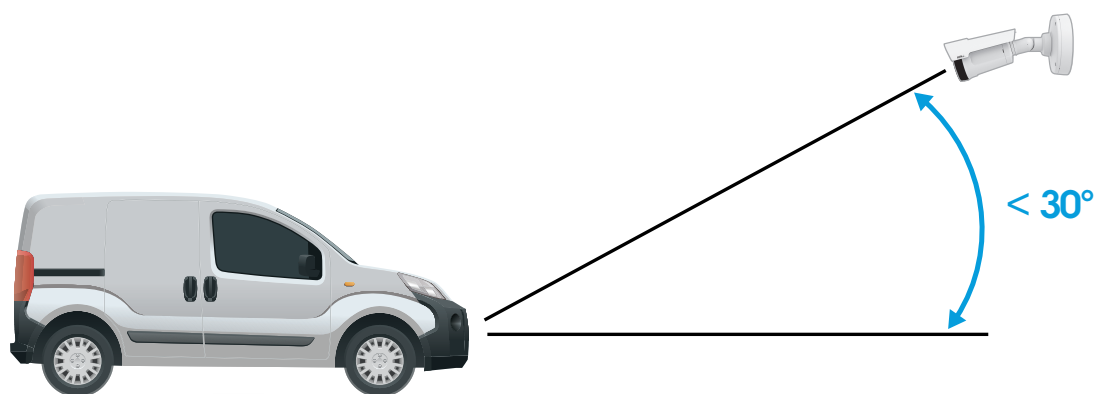
Distanza di rilevamento: (C)	Altezza di montaggio (A)
2 m (6,6 ft)	1,0 m (3,3 ft)
3 m (9,8 ft)	1,5 m (4,9 ft)
4 m (13 ft)	2 m (6,6 ft)
5 m (16 ft)	2,5 m (8,2 ft)
7 m (23 ft)	3,5 m (11 ft)

Distanza di acquisizione **flusso libero**: 7-20 m (23-65 ft). Questo è un esempio che si basa su AXIS P1465-LE-3 License Plate Verifier kit.

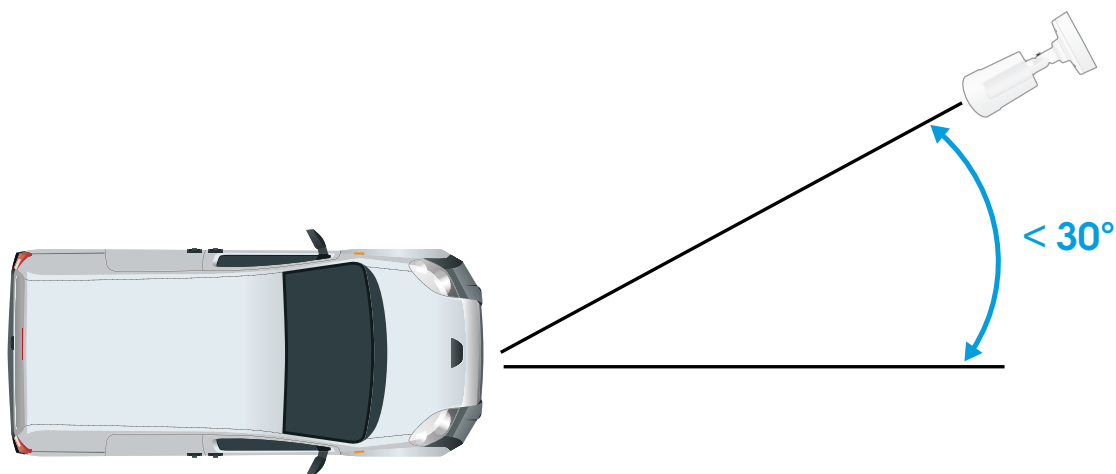
Distanza di rilevamento (C)	Altezza di montaggio (A)
7 m (23 ft)	3 m (9,8 ft)

10 m (33 ft)	4 m (13 ft)
15 m (49 ft)	6 m (19,5 ft)
20 m (65 ft)	10 m (33 ft)

- L'angolo di montaggio della telecamera non deve essere maggiore di 30° in alcuna direzione.

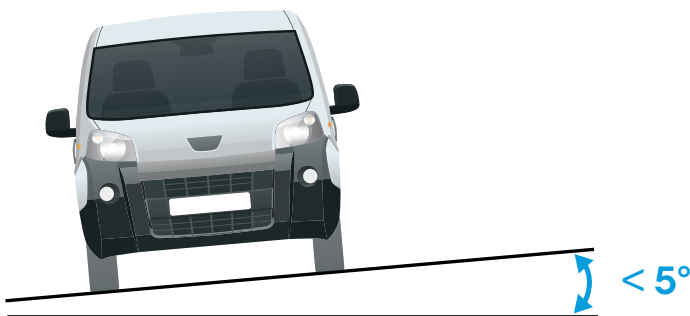


Angolo di montaggio visto di lato.



Angolo di montaggio visto da sopra.

- L'immagine della targa non deve avere un'inclinazione superiore a 5° in orizzontale. Se l'immagine è inclinata di oltre 5°, è consigliabile regolare la telecamera in modo che la targa venga visualizzata orizzontalmente nel flusso dal vivo.



Angolo di rotolamento.

Assistente alla configurazione

Imposta **Free flow (Libera circolazione)** o **Access control (Controllo degli accessi)** utilizzando l'assistente alla configurazione, quando esegui l'applicazione per la prima volta. Se si desidera apportare modifiche in un secondo momento, andare a **Settings > Maintenance** (Impostazioni, Manutenzione) e in **Setup assistant** (Assistente di configurazione) premere **Start** (Avvia).

Libera circolazione

In Libera circolazione, l'applicazione può effettuare il rilevamento e la lettura di targhe nel traffico a velocità bassa su strade d'accesso più ampie, centri città e in zone recintate quali campus universitari, porti o aeroporti. Ciò consente ricerche forensi di riconoscimento targhe ed eventi attivati dal riconoscimento targhe in un VMS.

1. Seleziona **Free flow (Libera circolazione)** e fai clic su **Next (Avanti)**.
2. Seleziona la rotazione d'immagine corrispondente al modo in cui la tua telecamera è montata.
3. Seleziona la quantità di aree di interesse. Tieni conto che una singola area è capace di rilevamento di targhe in entrambe le direzioni.
4. Seleziona la regione in cui la telecamera è ubicata.
5. Selezione del tipo di acquisizione.
 - **License plate crop (Ritaglia targa)** salva solo la targa.
 - **Vehicle crop (Ritaglia veicolo)** salva tutto il veicolo acquisito.
 - **Frame downsized 480x270 (Fotogramma ridimensionato 480x270)** salva l'intera immagine e riduce la risoluzione a 480x270.
 - **Full frame (Fotogramma completo)** salva l'intera immagine alla massima risoluzione.
6. Per regolare l'area di interesse, trascina i punti di ancoraggio. Vedere *Regolare l'area di interesse, on page 10*.
7. Regola la direzione dell'area di interesse. Fai clic sulla freccia e ruotala per determinare la direzione. Il modo in cui l'applicazione registra i veicoli in entrata o in uscita dall'area è determinato dalla direzione.
8. Fare clic su **Next (Avanti)**
9. Nell'elenco a discesa **Protocol (Protocollo)**, selezionare uno dei seguenti protocolli:
 - TCP
 - HTTP POST
10. Nel campo **Server URL (URL server)**, digitare l'indirizzo del server e la porta nel seguente formato:
127.0.0.1:8080

11. Nel campo **Device ID (ID dispositivo)**, digitare il nome del dispositivo o lasciarlo invariato.
12. In **Event types (Tipi di evento)**, selezionare una o più opzioni seguenti:
 - **New (Nuova)** indica il primo rilevamento di una targa.
 - **Update (Aggiornamento)** è una correzione di un carattere su una targa rilevata in precedenza o quando viene rilevata una direzione mentre la targa si sposta ed è tracciata nell'immagine.
 - **Lost (Persa)** è l'ultimo evento della targa rilevato prima della sua uscita dall'immagine. Contiene inoltre la direzione della targa.
13. Per attivare la funzione, selezionare **Send event data to server (Invia dati eventi al server)**.
14. Per ridurre la larghezza di banda quando si utilizza HTTP POST, è possibile selezionare **Do not to send images through HTTP POST (Non inviare immagini tramite HTTP POST)**.
15. Fare clic su **Next (Avanti)**.
16. Se hai già un elenco di targhe registrate a disposizione, scegli di importarlo in qualità di **blocklist (lista bloccati)** o di **allowlist (lista consentiti)**.
17. Fare clic su **Finish (Fine)**.

Controllo accessi

Per eseguire la configurazione in modo rapido e facile, serviti della procedura guidata. Per abbandonare la guida in qualsiasi momento, puoi selezionare **Skip (Salta)**.

1. Seleziona **Access control (Controllo degli accessi)** e fai clic su **Next (Avanti)**.
2. selezionare il tipo di controllo degli accessi da utilizzare:
 - **Internal I/O (I/O interno)** se vuoi mantenere la gestione degli elenchi nella telecamera. Vedere *Aprire una barriera per i veicoli noti utilizzando l'I/O della telecamera, on page 29*.
 - **Controller** se vuoi connettere un door controller. Vedere .
 - **Relay (Relè)** se vuoi effettuare il collegamento a un modulo relè. Vedere .
3. Nell'elenco a discesa **Barrier mode (Modalità barriera)**, in **Open from lists (Apri da elenchi)**, seleziona **Allowlist (Lista consentiti)**.
4. Nell'elenco a discesa **Vehicle direction (Direzione veicolo)**, selezionare **out (uscita)**.
5. Seleziona l'area di interesse che vuoi usare o se desideri impiegarle tutte nell'elenco a discesa **ROI**.
6. Fare clic su **Next (Avanti)**.

Nella pagina **Image settings (Impostazioni immagine)**:

1. Seleziona la quantità di aree di interesse.
2. Seleziona la regione in cui la telecamera è ubicata.
3. Selezione del tipo di acquisizione. Vedere *Regolare le impostazioni di acquisizione, on page 11*.
4. Per regolare l'area di interesse, trascina i punti di ancoraggio. Vedere *Regolare l'area di interesse, on page 10*.
5. Regola la direzione dell'area di interesse. Il modo in cui l'applicazione registra i veicoli in entrata o in uscita dall'area è determinato dalla direzione.
6. Fare clic su **Next (Avanti)**

Nella pagina **Event data (Dati evento)**:

Nota

Per impostazioni dettagliate, consultare: *Inviare le informazioni relative agli eventi a software di terze parti, on page 38*.

1. Nell'elenco a discesa **Protocol (Protocollo)**, selezionare uno dei seguenti protocolli:
 - TCP

- HTTP POST
- 2. Nel campo **Server URL (URL server)**, digitare l'indirizzo del server e la porta nel seguente formato:
127.0.0.1:8080.
- 3. Nel campo **Device ID (ID dispositivo)**, digitare il nome del dispositivo o lasciarlo invariato.
- 4. In **Event types (Tipi di evento)**, selezionare una o più opzioni seguenti:
 - **New (Nuova)** indica il primo rilevamento di una targa.
 - **Update (Aggiornamento)** è una correzione di un carattere su una targa rilevata in precedenza o quando viene rilevata una direzione mentre la targa si sposta ed è tracciata nell'immagine.
 - **Lost (Persa)** è l'ultimo evento della targa rilevato prima della sua uscita dall'immagine. Contiene inoltre la direzione della targa.
- 5. Per attivare la funzione, selezionare **Send event data to server (Invia dati eventi al server)**.
- 6. Per ridurre la larghezza di banda quando si utilizza HTTP POST, è possibile selezionare **Do not to send images through HTTP POST (Non inviare immagini tramite HTTP POST)**.
- 7. Fare clic su **Next (Avanti)**

Nella pagina **Import list from a .csv file (Importa elenco da un file .csv)**:

1. Se hai già un elenco di targhe registrate a disposizione, scegli di importarlo in qualità di **blocklist (lista bloccati)** o di **allowlist (lista consentiti)**.
2. Fare clic su **Finish (Fine)**.

Accedi alle impostazioni dell'applicazione

1. Nell'interfaccia web della videocamera, vai su **Apps (App)**, avvia l'applicazione e fai clic su **Open (Apri)**.

Regolare l'area di interesse

L'area di interesse è l'area nella visualizzazione in diretta in cui l'applicazione ricerca le targhe. Per prestazioni ottimali, mantenere l'area di interesse alle dimensioni minime. Per regolare l'area di interesse procedere nel modo seguente:

1. Andare a **Settings (Impostazioni)**.
2. Fare clic su **Image (Immagine)**.
3. Fare clic su 1:1 per ingrandire l'area in cui desidera monitorare il traffico o gestire il controllo degli accessi.
4. Per migliorare la verifica e le immagini acquisite, fare clic su **AF**.
5. Per consentire alla fotocamera di mettere a fuoco automaticamente i veicoli, fare clic su **AF**. Per impostare la messa a fuoco in modo manuale, regolarla utilizzando il cursore.
6. Fare clic su **Area of interest (Area di interesse)** per visualizzarla nell'area di visione.
7. Per spostare l'area di interesse, fare clic in un punto qualsiasi nell'area per selezionarla e trascinarla nel punto in cui sono più visibili le targhe. Assicurarsi che la regione di interesse rimanga in posizione dopo aver salvato le impostazioni.
8. Eseguire la regolazione dell'area di interesse facendo clic su qualsiasi punto nell'area per selezionarla e trascinare i punti di ancoraggio evidenziati in blu.
 - Per reimpostare l'area di interesse, fare clic su pulsante di ripristino nell'angolo in basso a sinistra accanto all'icona numerica.
 - Per aggiungere punti di ancoraggio, fare clic su uno dei punti di ancoraggio scuri. Il punto di ancoraggio si accende in giallo, mostrando che può essere manipolato. I nuovi punti scuri vengono aggiunti automaticamente accanto al punto di ancoraggio giallo. La quantità massima di punti di ancoraggio gialli è otto.
9. Fare clic in un punto qualsiasi all'esterno dell'area di interesse per salvare le modifiche.

10. Per ottenere il feedback corretto sulla direzione in **Event log (Registro eventi)**, è necessario rivolgere la freccia verso la direzione di guida.
 - 10.1. Fare clic sull'icona della freccia.
 - 10.2. Selezionare il punto di ancoraggio e ruotare la freccia in modo che sia allineata alla direzione di guida.
 - 10.3. Fare clic all'esterno dell'area di interesse per salvare le modifiche.

Tieni conto che una singola area è capace di rilevamento di targhe in entrambe le direzioni. Il feedback relativo alla direzione viene visualizzato nella colonna **Direction (Direzione)**.

11. Per verificare se l'area di interesse è sufficientemente grande da garantire risultati ottimali, si consiglia di utilizzare il contatore di pixel.
 - Per visualizzare il contatore di pixel, fare clic sull'icona della calcolatrice.
 - Per regolare l'area del contatore di pixel a dimensione intera, trascinare l'angolo inferiore destro dell'area evidenziata in giallo.
 - Per spostare l'area del contatore di pixel, fare clic su un punto qualsiasi dell'area e trascinarla nella posizione desiderata.
- Per aggiungere una seconda area di interesse, fare clic su **+** accanto a 1.
- Se si utilizza una telecamera stand-alone, è possibile impostare dall'app le impostazioni consigliate per il riconoscimento delle targhe.
 1. Fare clic sull'icona della bacchetta magica e le impostazioni saranno ottimizzate per il riconoscimento targhe.
 2. Fare clic su un pulsante del menu accanto alla bacchetta magica per visualizzare i valori impostati.

Selezionare la regione

1. Andare a **Settings > Recognition (Impostazioni, Riconoscimento)**.
2. Selezionare la regione nell'elenco a discesa **Region (Regione)**.

Regolare le impostazioni di acquisizione

1. Andare a **Settings (Impostazioni) > Image (Immagine)**.
2. Per modificare la risoluzione delle immagini acquisite, andare a **Image Resolution (Risoluzione immagine)**.
3. Per modificare la rotazione dell'immagine acquisita, andare a **Rotation (Rotazione)**.

Configurazione dell'archiviazione degli eventi

Un evento comprende immagine acquisita, targa, area di interesse, direzione del veicolo, accesso e data e ora.

Questo esempio di caso d'uso spiega come memorizzare eventi di numeri targhe consentite per 30 giorni.

Requisiti:

- Telecamera fisicamente installata e connessa alla rete.
 - AXIS License Plate Verifier in funzione sulla telecamera.
 - Spazio di archiviazione interno o scheda di memoria installata nella telecamera.
1. Andare a **Settings (Impostazioni) > Storage (Archiviazione)**.
 2. In **Retain events (Conserva eventi)**, selezionare **Allowlisted (Consentiti)**.
 3. In **Retention period (Periodo di conservazione)**, selezionare **30 days (30 giorni)**.
 4. Per modificare la modalità di salvataggio delle immagini acquisite, andare a **Save full frame (Salva fotogramma completo)**:
 - **License plate crop (Ritaglia targa)** salva solo la targa.

- **Vehicle crop (Ritaglia veicolo)** salva tutto il veicolo acquisito.
- **Frame downsized 480x270 (Fotogramma ridimensionato 480x270)** salva l'intera immagine e riduce la risoluzione a 480x270.
- **Full frame (Fotogramma completo)** salva l'intera immagine alla massima risoluzione.

Nota

Devi riavviare l'app affinché la scheda di memoria inserita sia rilevata durante il funzionamento dell'app. Nel caso nella telecamera sia installata una scheda di memoria, l'app la selezionerà automaticamente come spazio di archiviazione predefinito.

AXIS License Plate Verifier impiega la memoria interna della telecamera per salvare un massimo di 1.000 eventi, usando come fotogramma ritagli di targhe. Se usi fotogrammi più grandi, la quantità di eventi salvabili cambierà.

Una scheda di memoria è in grado di salvare un massimo di 100.000 eventi impiegando qualsiasi tipo di fotogramma.

Installazione

Modalità anteprima

La modalità anteprima è perfetta per gli installatori quando ottimizzano la vista della telecamera nel corso dell'installazione. Non è necessario fare login per ottenere l'accesso alla vista della telecamera in modalità anteprima. È a disposizione solo nello stato impostazione di fabbrica per un lasso di tempo limitato dal momento dell'accensione del dispositivo.



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

Questo video dimostra come usare la modalità anteprima.

Configurare il dispositivo

Per gli utenti di AXIS Camera Station

Impostare AXIS License Plate Verifier

Un dispositivo si considera un'origine dati esterna nel Video Management System quando è configurato con AXIS License Plate Verifier. Si può connettere una vista all'origine dati, cercare le targhe acquisite dal dispositivo e visualizzare la relativa immagine.

Nota

- Richiede AXIS Camera Station 5.38 o successivo.
 - AXIS License Plate Verifier necessita una licenza.
1. Scaricare e installare l'applicazione sul dispositivo.
 2. Configurare l'applicazione. Vedere il *manuale per l'utente AXIS License Plate Verifier*.
 3. Per un'installazione esistente di AXIS Camera Station, rinnovare il certificato server che è utilizzato per comunicare con il client. Vedere *Rinnovo dei certificati*.
 4. Attivare la sincronizzazione dell'ora per utilizzare il server AXIS Camera Station come server NTP. Vedere *Impostazioni server*.
 5. aggiungere il dispositivo ad AXIS Camera Station; Vedere *Aggiunta di dispositivi*.
 6. Viene aggiunta automaticamente un'origine dati in **Configuration > Devices > External data sources** (**Configurazione > Dispositivi > Origini di dati esterne**) quando viene ricevuto il primo evento.
 7. Connettere l'origine dati a una vista. Vedere *Origini di dati esterne*.
 8. Cercare targhe catturate dal dispositivo. Consultare *Ricerca di dati*.
 9. Per esportare i risultati della ricerca in un file .txt, fare clic su .

Impostazioni di base

Imposta la posizione di montaggio

1. Vai a **Video > Installation > Mounting position** (**Video > Installazione > Posizione di montaggio**).
2. Fare clic su **Change (Modifica)**.
3. Seleziona una posizione di montaggio e fai clic su **Save and restart** (**Salva e riavvia**).

Impostare la frequenza linea di alimentazione

1. Andare a **Video > Installation > Power line frequency** (**Video > Installazione > Frequenza linea di alimentazione**).
2. Seleziona la frequenza linea di alimentazione e fare clic su **Save and restart** (**Salva e riavvia**).

Regolare l'immagine

Questa sezione include istruzioni sulla configurazione del dispositivo.

Ridurre i tempi di elaborazione delle immagini con la modalità a bassa latenza

È possibile ottimizzare il tempo di elaborazione delle immagini del flusso dal vivo attivando la modalità a bassa latenza. La latenza nel flusso dal vivo è ridotta al minimo. Quando si utilizza la modalità a bassa latenza, la qualità di immagine è inferiore al solito.

1. Andare in **System > Plain config** (**Sistema > Configurazione normale**).
2. Selezionare **ImageSource** dall'elenco a discesa.

3. Passare alla **ImageSource/I0/Sensor > Low latency mode (ImageSource/I0/Sensore > Modalità a bassa latenza)** e selezionare **On (Attiva)**.
4. Fare clic su **Save (Salva)**.

Selezione della modalità di esposizione

Per il miglioramento della qualità di immagine per specifiche scene di sorveglianza, usa le modalità di esposizione. Le modalità di esposizione ti permettono il controllo dell'apertura, della velocità dell'otturatore e del guadagno. Andare a **Video > Image > Exposure (Video > Immagine > Esposizione)** e selezionare le seguenti modalità di esposizione:

- Per la maggior parte dei casi di utilizzo, selezionare l'esposizione **Automatic (Automatico)**.
- Per ambienti con determinate illuminazioni artificiali, ad esempio con luci fluorescenti, selezionare **Flicker-free (Privo di sfarfallio)**.
Selezionare la stessa frequenza di quella della linea di alimentazione.
- Per ambienti con determinate luci artificiali e luce intensa, ad esempio esterni con luci fluorescenti di notte e sole durante il giorno, selezionare **Flicker-free (Privo di sfarfallio)**.
Selezionare la stessa frequenza di quella della linea di alimentazione.
- Per bloccare le impostazioni di esposizione correnti, selezionare **Hold current (Mantieni opzioni correnti)**.

Compensazione dell'effetto barile

L'effetto barile è un fenomeno che fa sì che le linee rette appaiano sempre più inarcate quanto più ci si avvicina ai bordi del fotogramma. Un ampio campo visivo crea spesso un effetto barile in un'immagine. La correzione dell'effetto barile compensa questa distorsione.

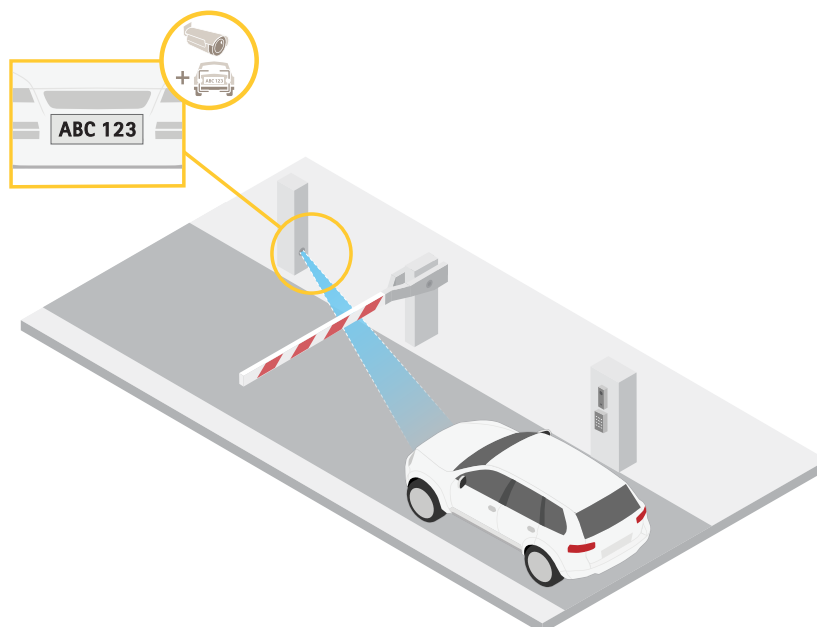
Nota

La correzione dell'effetto barile influisce sulla risoluzione e sul campo visivo dell'immagine.

1. Andare a **Video > Installation > Image correction (Video > Installazione > Correzione immagine)**.
2. Attivare **Barrel distortion correction (BDC) (Correzione dell'effetto barile (BDC))**.

Verificare la risoluzione dei pixel

Per verificare che una parte definita dell'immagine contenga pixel sufficienti, ad esempio per riconoscere le targhe, è possibile utilizzare il contatore di pixel.



1. Andare a **Video > Image (Video > Immagine)**.
2. Fare clic su .
3. Fare clic su  per **Pixel counter (Contatore di pixel)**.
4. Nella visualizzazione in diretta della telecamera, regolare le dimensioni e la posizione del rettangolo intorno all'area di interesse, ad esempio dove si prevede che vengano visualizzate le targhe.
5. È possibile visualizzare il numero di pixel per ciascuno dei lati del rettangolo e decidere se i valori sono sufficienti per le proprie esigenze.

Visualizzare e registrare video

Questa sezione include istruzioni sulla configurazione del dispositivo. Per ulteriori informazioni sul funzionamento dello streaming e dello storage, vedere .

Ridurre la larghezza di banda e dello spazio di archiviazione

Importante

Ridurre la larghezza di banda può causare la perdita di dettagli nell'immagine.

1. Andare a **Video > Stream (Video > Flusso)**.
2. Nella visualizzazione in diretta, fare clic su .
3. Seleziona **Video format (Formato video) AV1** se il tuo dispositivo lo supporta. Altrimenti seleziona **H.264**.
4. Andare a **Video > Stream > General (Video > Flusso > Generale)** e aumenta la **Compression (Compressione)**.
5. Andare a **Video > Stream > Zipstream (Video > Flusso > Zipstream)** e compi una o più delle operazioni seguenti:

Nota

Le impostazioni di **Zipstream** vengono utilizzate per tutti i codificatori video tranne MJPEG.

- Seleziona la **Strength (Intensità) Zipstream** che vuoi usare.
- Attivare **Optimize for storage (Optimize per l'archiviazione)**. Questa opzione può essere utilizzata solo se il software per la gestione video supporta B-frame.

- Attivare **Dynamic FPS (FPS dinamico)**.
- Attivare il **Dynamic GOP (GOP dinamico)** e impostare un elevato valore **Upper limit (Limite superiore)** per la lunghezza GOP.

Nota

La maggioranza dei browser non è dotata di supporto per la decodifica H.265 e per tale ragione l'interfaccia Web del dispositivo non la supporta. È invece possibile utilizzare un'applicazione o un sistema di gestione video che supporta la codifica H.265.

Configurazione dell'archiviazione di rete

Per archiviare le registrazioni in rete, è necessario configurare l'archiviazione di rete.

1. Andare a **System > Storage (Sistema > Archiviazione)**.
2. Fare clic su  **Add network storage (Aggiungi archiviazione di rete)** in **Network storage (Archiviazione di rete)**.
3. Digitare l'indirizzo IP del server host.
4. Digitare il nome dell'ubicazione condivisa nel server host in **Network share (Condivisione di rete)**.
5. Digitare il nome utente e password.
6. Selezionare la versione SMB o lasciare questa impostazione su **Auto (Automatico)**.
7. Selezionare **Add share without testing (Aggiungi condivisione senza test)** se si riscontrano problemi di connessione temporanei o se non è stata ancora eseguita la configurazione della condivisione di rete.
8. Fare clic su **Aggiungi**.

Registrazione e guardare video

Registrazione di video direttamente dalla telecamera

1. Andare a **Video > Stream (Video > Flusso)**.
2. Per avviare una registrazione, fare clic su .

Se non hai impostato alcun dispositivo di archiviazione, fare clic su  e . Per istruzioni sull'impostazione dell'archiviazione di rete, vedere *Configurazione dell'archiviazione di rete, on page 17*

3. Fare di nuovo clic su  per arrestare la registrazione.

Guarda il video

1. Andare a **Recordings (Registrazioni)**.
2. Fare clic su  per la tua registrazione nella lista.

Verifica che nessuno abbia alterato il video

Con un video firmato, sarai in grado di verificare che il video registrato dalla telecamera non abbia subito alcuna manomissione.

1. Vai su **Video > Stream > General (Video > Flusso > Generale)** e attiva **Signed video (Video firmato)**.
2. Registrare il video direttamente sul dispositivo oppure utilizzare AXIS Camera Station Pro o un altro software per la gestione video compatibile. Per istruzioni su AXIS Camera Station Pro consultare il *Manuale per l'utente di AXIS Camera Station Pro*.
3. Esporta il video registrato.
4. Utilizzare lo strumento di *verifica supporti multimediali firmati* di Axis, per verificare la registrazione.

Imposta regole per eventi

È possibile creare delle regole per fare sì che il dispositivo esegua un'azione quando si verificano determinati eventi. Una regola consiste in condizioni e azioni. Le condizioni possono essere utilizzate per attivare le azioni. Ad esempio, il dispositivo può avviare una registrazione o inviare un e-mail quando rileva un movimento oppure può mostrare un testo in sovrapposizione mentre il dispositivo registra.

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

Registrare video quando la telecamera rileva una targa

Questo esempio illustra in che modo si configura la telecamera perché inizi la registrazione sulla scheda di memoria quando la telecamera rileva un oggetto. La registrazione comprende cinque secondi prima del rilevamento e un minuto dopo la fine del rilevamento.

Operazioni preliminari:

- Assicurati di avere una scheda di memoria installata.

Verificare che AXIS Licence Plate Verifier sia in esecuzione:

1. Vai a **Apps > AXIS License Plate Verifier (Applicazioni > AXIS License Plate Verifier)**.
2. Avviare l'applicazione se non è già in esecuzione.
3. Assicurarsi di aver impostato l'applicazione in base alle proprie esigenze.

Creare una regola:

1. Andare a **System > Events (Sistema > Eventi)** e aggiungere una regola.
2. Inserire un nome per la regola.
3. Nell'elenco delle condizioni, in **Application (Applicazione)**, selezionare **ALPV.PlateInView**.
4. Nell'elenco delle azioni, in **Recordings (Registrazioni)**, selezionare **Record video while the rule is active (Registra video mentre la regola è attiva)**.
5. Selezionare **SD_DISK** dall'elenco delle opzioni di archiviazione.
6. Seleziona una telecamera e un profilo di streaming.
7. Impostare il tempo prebuffer su 5 secondi.
8. Imposta il tempo post buffer su 1 minuto.
9. Fare clic su **Save (Salva)**.

Attivazione di una notifica in caso di manomissione dell'obiettivo della telecamera

Questo esempio spiega come impostare una notifica via e-mail quando l'obiettivo della telecamera viene spruzzato, coperto o sfocato.

Attivare il rilevamento delle manomissioni:

1. Andare a **System > Detectors > Camera tampering (Sistema > Rilevatori > Manomissione telecamera)**.
2. Impostare un valore per **Trigger delay (Ritardo attivazione)**. Il valore indica il tempo che deve passare prima dell'invio di un'e-mail.
3. Attivare **Trigger on dark images (Trigger sulle immagini scure)** per rilevare se gli obiettivi sono stati spruzzati, coperti o gravemente alterati e sfocati.

Aggiungere un destinatario e-mail:

4. Andare a **System > Events > Recipients (Sistema > Eventi > Destinatari)** e aggiungere un destinatario.
5. Immettere un nome per il destinatario.
6. Selezionare **Email (E-mail)** come tipo di notifica.
7. Digitare l'indirizzo e-mail del destinatario.
8. Digitare l'indirizzo e-mail da cui si desidera che la telecamera invii le notifiche.

9. Indicare i dati di accesso all'account dell'e-mail di invio, insieme al nome host e al numero di porta SMTP.
10. Per verificare la configurazione della posta elettronica, fare clic su **Test (Prova)**.
11. Fare clic su **Save (Salva)**.

Creare una regola:

12. Andare a **System > Events > Rules (Sistema > Eventi > Regole)** e aggiungere una regola.
13. Inserire un nome per la regola.
14. Nell'elenco delle condizioni, in **Video**, selezionare **Tampering (Manomissione)**.
15. Nell'elenco delle azioni, in **Notifications (Notifiche)**, selezionare **Send notification to email (Invia notifica all'indirizzo e-mail)**, quindi selezionare il destinatario dall'elenco.
16. Digitare un oggetto e il messaggio per l'e-mail.
17. Fare clic su **Save (Salva)**.

Audio

Aggiunta di audio alla registrazione

Attivare l'audio:

1. Andare a **Video > Stream > Audio (Video > Flusso > Audio)** e includere l'audio.
2. Se il dispositivo ha più sorgenti di ingresso, selezionare quella corretta in **Source (Sorgente)**.
3. Andare a **Audio > Device settings (Audio > Impostazioni dispositivo)** e attivare la sorgente di ingresso corretta.

Modificare il profilo di streaming utilizzato per la registrazione:

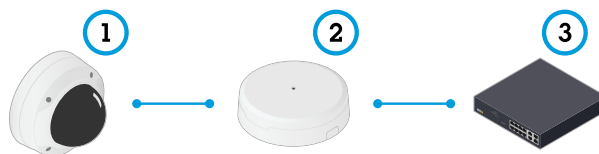
4. Andare a **System > Stream profiles (Sistema > Profili di streaming)** e seleziona il profilo di streaming.
5. Selezionare **Include audio (Includi audio)** e attivare questa opzione.
6. Fare clic su **Save (Salva)**.

Aggiungi funzionalità audio al dispositivo usando portcast

Servendoti della tecnologia portcast, puoi aggiungere funzionalità audio al tuo dispositivo. Permette la comunicazione audio e I/O in modo digitale attraverso il cavo di rete tra la telecamera e l'interfaccia.

Per aggiungere funzionalità audio al dispositivo con tecnologia video di rete Axis, collegare il dispositivo audio ed interfaccia I/O Axis compatibile con il portcast tra il tuo dispositivo e lo switch PoE che fornisce alimentazione.

1. Collega il dispositivo video di rete Axis (1) e il dispositivo portcast Axis (2) con un cavo PoE.
2. Collega il dispositivo portcast Axis (2) e lo switch PoE (3) con un cavo PoE.



- 1 Dispositivo con tecnologia video di rete Axis
- 2 Dispositivo portcast Axis
- 3 Switch

Una volta che i dispositivi sono collegati, una scheda audio diventa visibile nelle impostazioni del dispositivo con tecnologia video di rete Axis. Vai alla scheda **Audio** e attiva l'opzione **Allow audio (Consenti audio)**.

Consulta il manuale per l'utente del tuo dispositivo portcast Axis.

Gestione degli elenchi

Aggiunta all'elenco della targa rilevata

È possibile aggiungere direttamente una targa rilevata dall'applicazione a un elenco.

1. Fare clic su **Home** (pagina principale).
2. Andare a **Live** (In diretta).
3. Fare clic sull'icona a forma di freccia sulla targa registrata nell'elenco.
4. Fare clic su **Append plate to list** (Aggiungi targa all'elenco).
5. Nella finestra di dialogo, scegliere a quale elenco aggiungere la targa.
6. Fai clic su **Append** (Aggiungi).

Nota

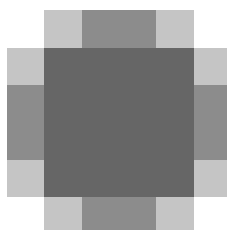
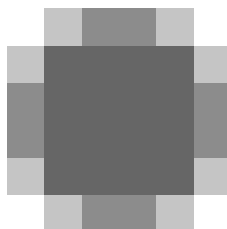
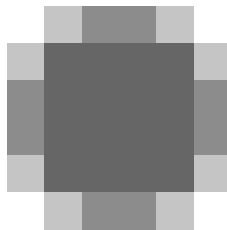
Assicurarsi che i simboli <, > e & non siano utilizzati né nella targa né nella descrizione.

Aggiunta di descrizioni alle targhe

Per aggiungere una descrizione a una targa nell'elenco:

- Andare a **List management** (Gestione elenchi).

- Selezionare la targa e fare clic su



quindi selezionare **Edit** (Modifica) nel menu a discesa.

- Digitare le informazioni pertinenti nel campo **Description** (Descrizione).
- Fare clic su **Save** (Salva).

Nota

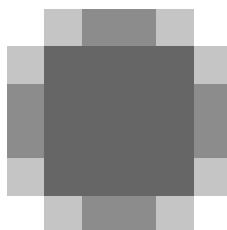
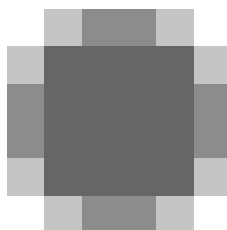
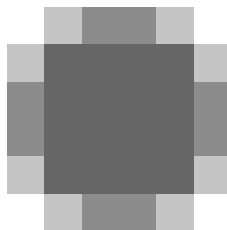
Assicurarsi che i simboli <, > e & non siano utilizzati né nelle targhe né nelle descrizioni.

Personalizzazione dei nomi degli elenchi

Il nome di qualsiasi elenco può essere cambiato a seconda del caso d'uso specifico.

1. Andare a **List management** (Gestione elenchi).

2. Fare clic su



accanto all'elenco che si desidera modificare.

3. Selezionare **Edit** (Modifica).
4. Inserisci il nome dell'elenco.
5. Fare clic su **Submit**.

Il nome nuovo dell'elenco sarà aggiornato in ogni configurazione esistente.

Importazione di numeri di targhe consentite

È possibile importare i numeri delle targhe autorizzate da un file .csv nel computer. Oltre al numero di targa stesso, è possibile aggiungere commenti per ogni numero di targa nel file .csv.

La struttura del file .csv deve avere l'aspetto seguente: `license plate,date,description`

Esempio:

Solo targa: `AXIS123`

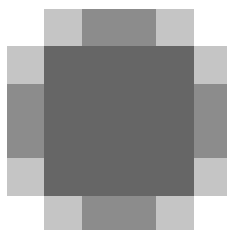
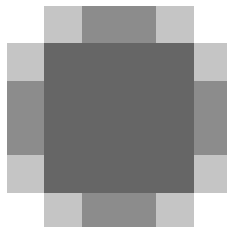
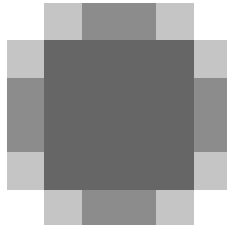
Targa + descrizione: `AXIS123, , John Smith`

Targa + data + descrizione: `AXIS123,2022-06-08, John Smith`

Nota

Assicurarsi che i simboli <, > e & non siano utilizzati né nelle targhe né nelle descrizioni.

1. Andare a **List management (Gestione elenchi)**
2. Fare clic su



accanto a **Allowlist (Consentiti)** e selezionare **Import (Importa)** nel menu a discesa.

3. Accedere al percorso di un file .csv nel computer.
4. Fare clic su **OK**.
5. Controllare che i numeri di targhe importate siano visualizzati in **Allowlist (Lista consentiti)**.

Condividere elenchi delle targhe con altre telecamere

È possibile condividere gli elenchi delle targhe con altre telecamere nella rete. La sincronizzazione sovrascriverà tutti gli elenchi delle targhe correnti nelle altre telecamere.

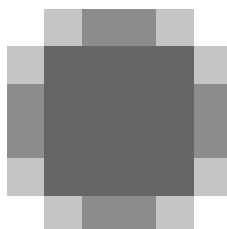
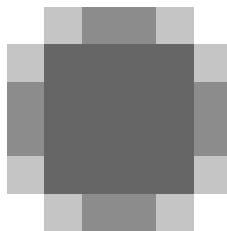
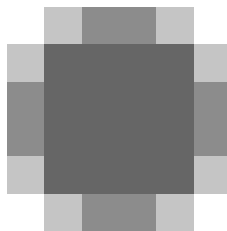
1. Andare a **List management > List synchronization (Gestione elenchi, Sincronizzazione elenco)**.
2. In **Remote connected devices (Dispositivi collegati da remoto)**, digitare indirizzo IP, nome utente e password.
3. Fare clic su **Aggiungi**.

4. Fare clic su **Synchronize list** (Sincronizza elenco).
5. Controllare che la data e l'ora in **Last sync** (Ultima sincronizzazione) si aggiornino di conseguenza.

Elenchi di pianificazione

Gli elenchi possono essere pianificati per essere attivi solo in determinati orari durante giorni della settimana specifici. Per pianificare un elenco:

- Andare a **List management** (Gestione elenchi).
- Fare clic su



accanto all'elenco che si desidera modificare.

- Selezionare **Schedule** (Pianifica) dal menu a discesa.
- Selezionare l'ora di inizio e di fine e il giorno in cui l'elenco deve essere attivo.
- Fare clic sul pulsante accanto a **Enabled** (Abilitato).
- Fare clic su **Save** (Salva).

Impostazioni supplementari

Configurare sovrapposizione testo

Una sovrapposizione testo mostra le seguenti informazioni sull'evento nella visualizzazione in diretta: `weekday, month, time, year, license plate number`.

1. Andare a **Settings (Impostazioni) > Image (Immagine)**.
2. Attiva **Text overlay (Sovrapposizione del testo)**.
3. Selezionare una delle seguenti opzioni: **Timestamp e license plate (Timbro orario e targa)** oppure **License plate only (Solo targa)**.
4. Imposta **Overlay duration (Durata sovrapposizione)** su un valore compreso tra 1 e 9 secondi.
5. Controllare che la sovrapposizione sia visualizzata nella visualizzazione in diretta.

Rileva targhe in condizioni di scarsa illuminazione

Ogni rilevamento ottiene un punteggio dall'algoritmo, questo punteggio è detto soglia di affidabilità. I rilevamenti con un punteggio inferiore al livello selezionato non verranno visualizzati nell'elenco degli eventi.

Per scene con bassa luminosità, è possibile impostare una soglia di affidabilità più bassa, che consentirà il rilevamento di un numero maggiore di targhe.

1. Andare a **Settings > Recognition (Impostazioni, Riconoscimento)**.
2. Regolare il cursore in **Confidence threshold (Soglia di affidabilità)**.
3. Verificare che l'algoritmo rilevi le targhe come previsto.

Consentire un minor numero di caratteri sulle targhe

Nell'applicazione è impostato un numero minimo predefinito di caratteri per la rilevazione di una targa. Il numero minimo predefinito di caratteri è cinque. È possibile configurare l'applicazione perché rilevi targhe con meno caratteri.

1. Andare a **Settings > Recognition (Impostazioni, Riconoscimento)**.
2. In **Number of characters (Numero di caratteri)**, regolare il cursore per impostare il numero minimo di caratteri che si desidera consentire.
3. Verificare che l'applicazione rilevi le targhe come previsto.

Consenti solo corrispondenze esatte di targhe

L'algoritmo di corrispondenza consente automaticamente una deviazione di un carattere quando si confronta la targa rilevata con la lista consentiti o bloccati. Tuttavia, alcuni scenari richiedono una corrispondenza esatta di tutti i caratteri della targa.

1. Andare a **List management (Gestione elenchi)**.
2. Fai clic per l'attivazione di **Strict matching (Corrispondenza rigida)**.
3. Verificare che l'applicazione corrisponda alle targhe come previsto.

Consentire più di una deviazione di carattere quando si confrontano le targhe

L'algoritmo di corrispondenza consente automaticamente una deviazione di un carattere quando si confronta la targa rilevata con la lista consentiti o bloccati. Tuttavia, è possibile consentire più di una deviazione di carattere.

1. Andare a **Settings > Recognition (Impostazioni, Riconoscimento)**.
2. Seleziona il numero di caratteri che possono essere diversi in **Allowed character deviation (Deviazione di carattere consentita)**.

3. Verificare che l'applicazione corrisponda alle targhe come previsto.

Accesso limitato agli operatori

Agli operatori può essere concesso un accesso limitato all'applicazione tramite un URL. In questo modo hanno accesso solo a Event log (Registro eventi) e List management (Gestione liste). L'URL si trova in Settings > User rights (Impostazioni > Diritti utente).

Impostare una connessione sicura

Per proteggere la comunicazione e i dati tra i dispositivi, ad esempio tra la telecamera e il controller della porta, impostare una connessione sicura con HTTPS usando certificati.

1. Andare a Settings (Impostazioni) > Security (Sicurezza).
2. In HTTPS, selezionare Self-signed (Autofirmato) oppure CA-signed (Firmato da CA).

Nota

Per ulteriori informazioni sull'HTTPS e su come si usa vedere .

Backup e ripristino delle impostazioni delle app

È possibile eseguire il backup e ripristinare le impostazioni effettuate nell'app relative all'acquisizione di immagini, alla sicurezza, al rilevamento e all'integrazione. In caso di problemi, è possibile ripristinare le impostazioni di cui è stato eseguito il backup.

Per eseguire il backup delle impostazioni dell'app:

- Andare a Settings > Maintenance (Impostazioni > Manutenzione).
- Fare clic su Download backup configuration (Scarica configurazione di backup).

Un file JSON verrà scaricato nella cartella dei download.

Per ripristinare le impostazioni dell'app:

- Andare a Settings > Maintenance (Impostazioni > Manutenzione).
- Fare clic su Restore configuration (Ripristina configurazione).

Selezionare il file JSON contenente il backup.

L'impostazione viene ripristinata automaticamente.

Cancellazione di tutti gli eventi

Dopo aver impostato l'app, può essere una buona idea cancellare le registrazioni di tutte le immagini o delle targhe acquisite dal processo di impostazione.

Per cancellare tutte le immagini e le targhe dal database:

Andare a Settings > Maintenance (Impostazioni > Manutenzione).

- Fare clic su Clear all recognition results (Cancella tutti i risultati del riconoscimento).
- Fare clic su Sì.

Usa porte virtuali per l'attivazione di azioni

Le porte virtuali si possono usare insieme al controllo degli accessi per l'attivazione di qualsiasi tipo di azione. Questo esempio spiega come configurare AXIS License Plate Verifier insieme alla porta I/O della telecamera per mostrare una sovrapposizione testo usando una porta virtuale.

Requisiti:

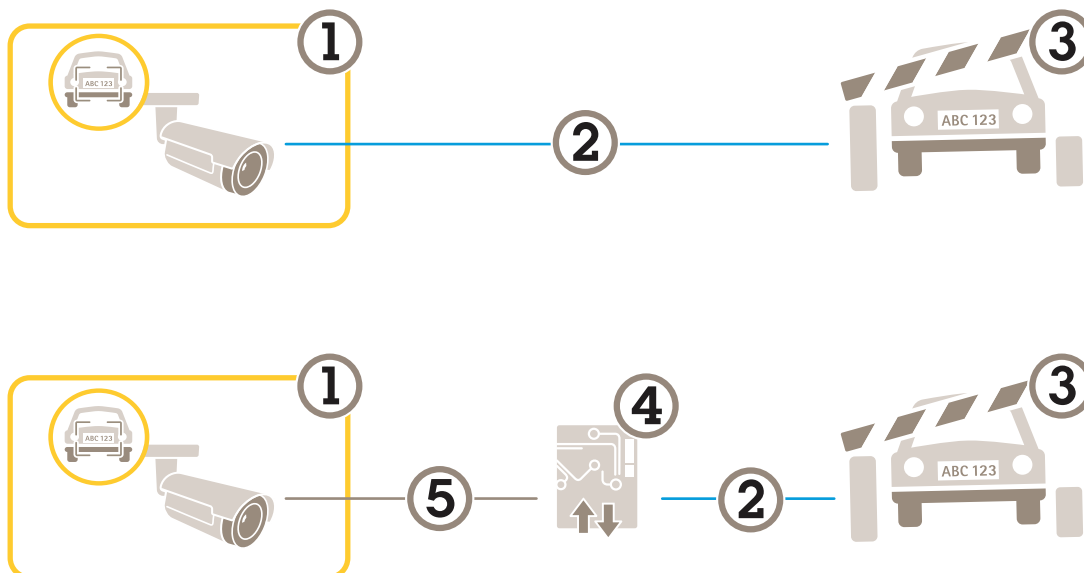
- Telecamera fisicamente installata e connessa alla rete.
- AXIS License Plate Verifier in funzione sulla telecamera.
- Cavi collegati alla barriera e alla porta I/O della telecamera.

- Configurazione di base effettuata. Vedere .
- 1. Andare alla pagina Web dell'applicazione e selezionare la scheda **Settings (Impostazioni)**.
- 2. Vai ad **Access control (Controllo degli accessi)**.
- 3. In **Access control** (controllo degli accessi), selezionare **Internal I/O (I/O interno)**.
- 4. Seleziona **I/O output # (Uscita I/O #)**.
- 5. Seleziona una porta dall'elenco a discesa **Virtual port (Porta virtuale)**.
- 6. In **Barrier mode** (Modalità barriera), selezionare **Open to all (Apri a tutti)**.
- 7. In **Vehicle direction** (Direzione veicolo), selezionare **Any (Qualsiasi)**.
- 8. Selezionare l'**Area of interest** (area di interesse) che si desidera utilizzare.
- 9. Nella pagina Web della telecamera, vai a **System > Events (Sistema > Eventi)**.
- 10. Fare clic su **Add rule (Aggiungi regola)**.
- 11. In **Condition (Condizione)** seleziona **Virtual input is active (L'input virtuale è attivo)** e il numero di porta che hai selezionato.
- 12. In **Action (Azione)**, seleziona **Use overlay text (Usa sovrapposizione testo)**.
- 13. Selezionare **Video channels (Canali video)**.
- 14. Digita il testo che vuoi sia visualizzato.
- 15. Aggiungi la durata del testo.
- 16. Fare clic su **Save (Salva)**.
- 17. Andare a **Video > Overlays (Video > Sovrapposizioni)**.
- 18. Vai a **Overlays (Sovrapposizioni testo)**.
- 19. Seleziona **Text (Testo)** nel menu a discesa e fai clic su **+**.
- 20. Digitare #D o selezionare il campo di modifica nell'elenco a discesa **Modifiers (Campi di modifica)**.
- 21. Verifica che la sovrapposizione testo sia visualizzata quando un veicolo entra nella regione di interesse nella visualizzazione in diretta.

Scenario di ingresso e uscita veicoli

Nello scenario per l'ingresso e l'uscita di veicoli, l'applicazione legge la targa del veicolo acquisita dalla telecamera e ne verifica la presenza su un elenco di targhe autorizzate o non autorizzate archiviate nella telecamera.

Questo scenario richiede l'applicazione incorporata in una telecamera con supporto I/O o un modulo relè I/O collegato per aprire e chiudere la barriera.



Due possibili impostazioni per lo scenario di ingresso e uscita di veicoli.

- 1 Telecamera Axis con AXIS License Plate Verifier
- 2 Comunicazione I/O
- 3 Barriera
- 4 Modulo relè I/O Axis
- 5 Comunicazione IP

Aprire una barriera per i veicoli noti utilizzando un modulo relè

In questo esempio viene illustrato come configurare AXIS License Plate Verifier insieme a un modulo relè per aprire una barriera per un veicolo conosciuto che attraversa una specifica regione di interesse (ROI) per raggiungere, ad esempio, un'area di parcheggio.

Requisiti:

- Telecamera fisicamente installata e connessa alla rete.
 - AXIS License Plate Verifier in funzione sulla telecamera.
 - Cavi collegati tra la barriera e il modulo relè.
 - Configurazione di base effettuata. Vedere *Configurazione di base, on page 6*.
1. Andare alla pagina Web della telecamera, selezionare **Settings (Impostazioni)** e aprire **AXIS License Plate Verifier**.
 2. Accedere alla pagina Web del modulo relè e verificare che la porta relè sia collegata alla porta I/O della telecamera.
 3. Copiare l'indirizzo IP del modulo relè.
 4. Torna ad **AXIS License Plate Verifier**.
 5. Andare in **Settings (Impostazioni) > Access control (Controllo degli accessi)**.
 6. Andare a **Type (Tipo)** e selezionare **Relay (Relè)** nell'elenco a discesa.
 7. Nell'elenco a discesa **I/O output (Output I/O)**, selezionare la porta I/O collegata alla barriera.

8. Nell'elenco a discesa **Barrier mode (Modalità barriera)**, selezionare **Open from lists (Apri da elenchi)** e poi **Allowlist (Lista consentiti)**.
9. Nell'elenco a discesa **Vehicle direction (Direzione veicolo)**, selezionare **in (entrata)**.
10. Nell'elenco a discesa **ROI**, selezionare l'area di interesse che copre la corsia del traffico.
11. Immettere le seguenti informazioni:
 - l'indirizzo IP per il modulo relè in formato 192.168.0.0
 - il nome utente per il modulo relè
 - la password per il modulo relè
12. Per assicurarsi che il collegamento funzioni, fare clic su **Connect (Collega)**.
13. Per attivare la connessione, fare clic su **Turn on integration (Attiva integrazione)**.
14. Andare alla scheda **List management (Gestione elenchi)**.
15. Immettere il numero di targa nel campo **Allowlist (Lista consentiti)**.

Nota

Le porte fisiche di input da 1 a 8 sul modulo relè corrispondono alle porte da 1 a 8 nell'elenco a discesa. Tuttavia, le porte relè da 1 a 8 sul modulo relè corrispondono alle porte da 9 a 16 nell'elenco a discesa. Questo vale anche se il modulo relè ha solo 8 porte.

16. Controllare che l'applicazione verifichi il numero di targa nella lista consentiti e lo identifichi come veicolo noto, quindi accertarsi che la barriera sia apra come previsto.

Aprire una barriera per i veicoli noti utilizzando l'I/O della telecamera

Questo esempio spiega come impostare AXIS License Plate Verifier insieme alla porta I/O della telecamera per aprire una barriera per un veicolo noto che entra, ad esempio, in un'area di parcheggio.

Requisiti:

- Telecamera fisicamente installata e connessa alla rete.
 - AXIS License Plate Verifier in funzione sulla telecamera.
 - Cavi collegati alla barriera e alla porta I/O della telecamera.
 - Configurazione di base effettuata. Vedere .
1. Vai alla pagina web dell'applicazione, e accedere alla **Home (Pagina principale)** e aggiungi a un elenco le targhe rilevate. Vedere *Aggiunta all'elenco della targa rilevata, on page 20*
 2. Andare a **List management (Gestione elenchi)** per modificare direttamente gli elenchi.
 3. Inserire i numeri delle targhe autorizzate nel campo **Allowlist (Lista consentiti)**.
 4. Andare a **Settings (Impostazioni)**.
 5. In **Access control (controllo degli accessi)**, selezionare **Internal I/O (I/O interno)**.
 6. Seleziona **I/O output # (Uscita I/O #)**.
 7. In **Barrier mode (Modalità barriera)**, selezionare **Open from lists (Apri da elenchi)** e contrassegnare **Allowlist (Consentiti)**.
 8. Nell'elenco a discesa **Vehicle direction (Direzione veicolo)**, selezionare **in (entrata)**.
 9. In **Area of interest (Area di interesse)** selezionare l'area di interesse da usare o se si desidera usarle tutte.
 10. Controllare che l'applicazione verifichi il numero di targa nella lista consentiti e lo identifichi come veicolo noto, quindi accertarsi che la barriera sia apra come previsto.

Nota

Il nome di qualsiasi elenco può essere cambiato a seconda del caso d'uso specifico.

Ricevi una notifica relativa a un veicolo non autorizzato

Questo esempio spiega come impostare l'applicazione in modo che un evento che attiva una notifica possa essere creato nella telecamera.

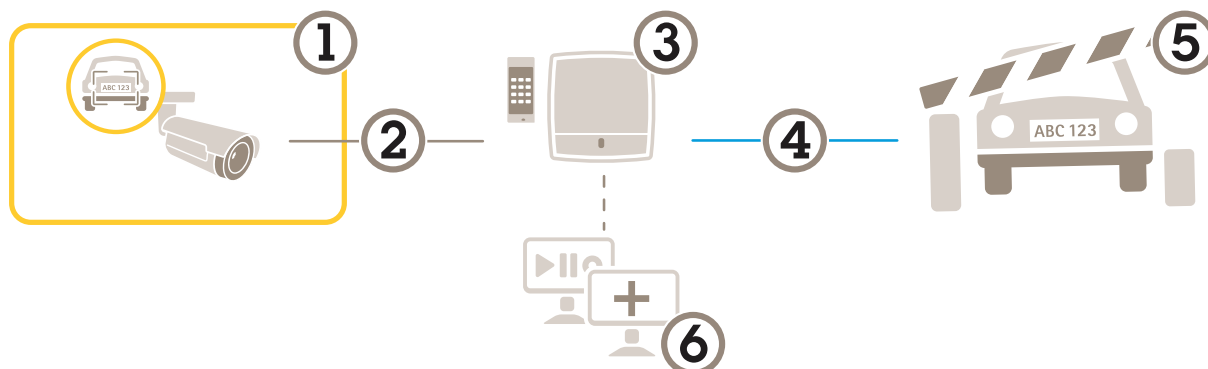
Requisiti:

- Configurazione di base effettuata. Consulta *Configurazione di base, on page 6*.
- 1. Andare a **List management (Gestione elenchi)**.
- 2. Immettere il numero di targa nel campo **Blocklist (Lista bloccati)**.
- 3. Accedere alla pagina Web della telecamera.
- 4. Andare a **Settings (Impostazioni) > Events (Eventi)** e impostare una regola di azione con l'applicazione come condizione e con una notifica come azione.
- 5. Controllare che l'applicazione identifichi il numero di targa aggiunto come veicolo non autorizzato e che la regola di azione venga eseguita come previsto.

Scenario di controllo degli accessi dei veicoli

Nello scenario per il controllo degli accessi dei veicoli, l'applicazione può essere connessa a un dispositivo di controllo delle porte di rete Axis per configurare le regole di accesso, creare pianificazioni per gli orari di accesso e gestire l'accesso dei veicoli non solo dei dipendenti, ma anche, ad esempio, dei visitatori e dei fornitori.

Per il backup, utilizzare un sistema di accesso che implica la presenza di un dispositivo di controllo delle porte e un lettore di schede. Per impostare il dispositivo di controllo delle porte e il lettore di schede, vedere la documentazione per l'utente sul sito Web axis.com



- 1 Telecamera Axis con AXIS License Plate Verifier
- 2 Comunicazione IP
- 3 Dispositivo di controllo per porte di rete con lettore di schede Axis
- 4 Comunicazione I/O
- 5 Barriera
- 6 Software di terze parti facoltativo

Connetti a un dispositivo di controllo porte

In questo esempio la telecamera viene collegata a un dispositivo di controllo delle porte di rete, che le consente di funzionare come un sensore. La telecamera inoltra le informazioni al dispositivo di controllo, che a sua volta analizza le informazioni e attiva gli eventi.

Nota

Quando si passa da AXIS License Plate Verifier a AXIS Entry Manager e viceversa, assicurarsi di aggiornare le pagine Web per ottenere l'accesso a tutti i parametri.

Requisiti:

- Telecamera e dispositivo di controllo delle porte fisicamente installato e connesso alla rete.
- AXIS License Plate Verifier in funzione sulla telecamera.
- Configurazione di base effettuata. Vedere *Configurazione di base*, on page 6.



Come mantenere l'applicazione in esecuzione con AXIS A1001 Door Controller.

Configurazione dell'hardware in AXIS Entry Manager

1. Andare a AXIS Entry Manager e avviare una nuova configurazione hardware in **Setup (Impostazione)**.
2. Nell'area di configurazione dell'hardware, rinominare il dispositivo di controllo delle porte di rete in "Dispositivo di controllo cancello".
3. Fare clic su **Next (Avanti)**.

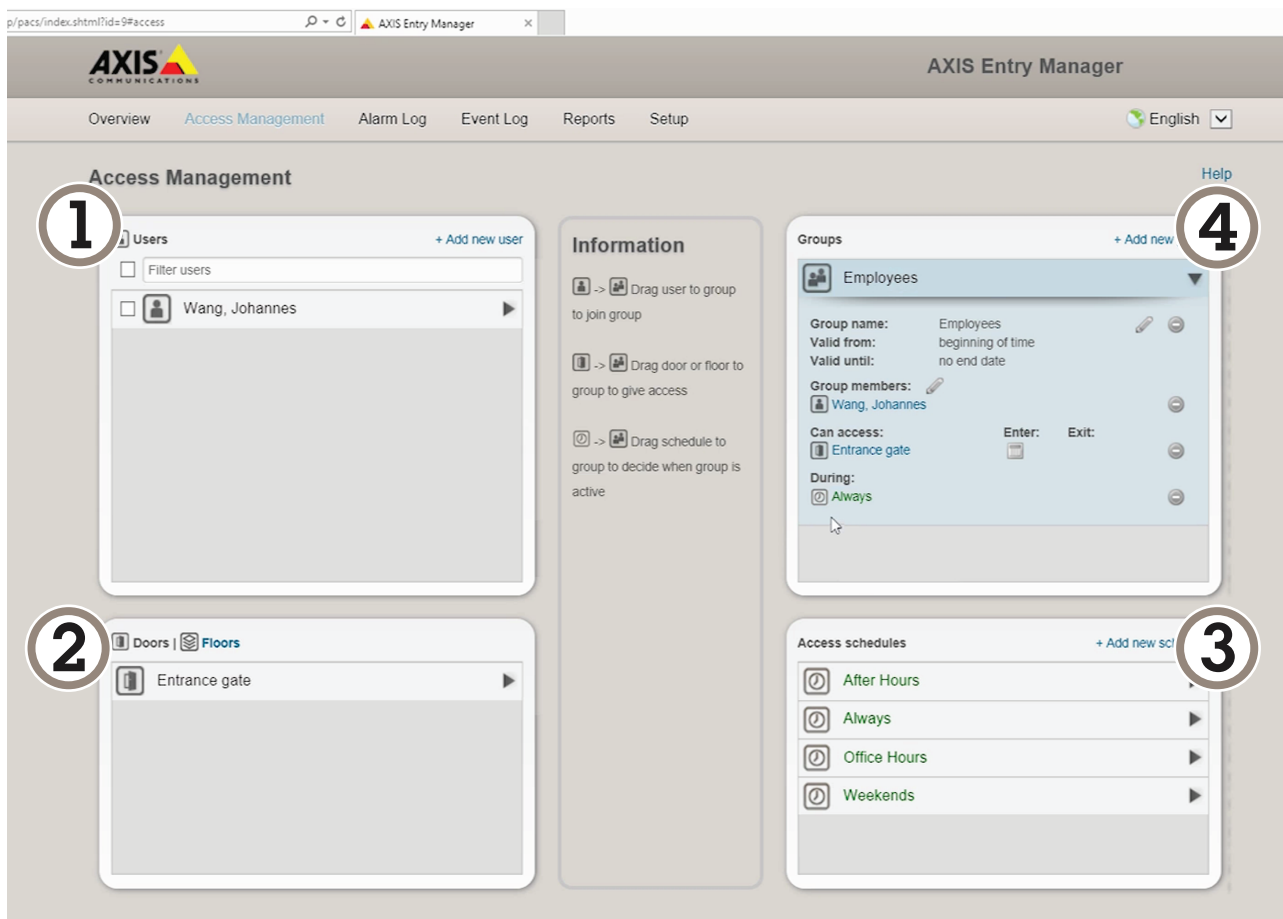
4. In **Configure locks connected to this controller** (Configura blocchi collegati al controller), deselezionare l'opzione **Door monitor** (Monitoraggio porte).
5. Fare clic su **Next** (Avanti).
6. In **Configure readers connected to this controller** (Configura lettori collegati al controller), deselezionare l'opzione **Exit reader** (Lettore di uscita).
7. Fare clic su **Finish** (Fine).

Configurazione in AXIS License Plate Verifier

1. Andare alla pagina Web **AXIS License Plate Verifier**.
2. Andare in **Settings (Impostazioni) > Access control (Controllo degli accessi)**.
3. Andare a **Type (Tipo)** e selezionare **Controller (Dispositivo di controllo)** nell'elenco a discesa.
4. Immettere le seguenti informazioni:
 - l'indirizzo IP per il dispositivo di controllo in formato 192.168.0.0
 - il nome utente per il dispositivo di controllo
 - la password per il dispositivo di controllo
5. Fare clic su **Connetti**.
6. Se la connessione ha esito positivo, viene visualizzato "Gatecontroller" nell'elenco a discesa **Network Door Controller name (Nome dispositivo di controllo porta di rete)**. Selezionare "Gatecontroller".
7. Nell'elenco a discesa **Reader name (Nome lettore)** selezionare il lettore collegato al "Gatecontroller" della porta, ad esempio "Lettore entrata". Questi nomi si possono modificare in **AXIS Entry Manager**.
8. Per attivare la connessione, selezionare **Turn on integration (Attiva integrazione)**.
9. Inserire un numero di targa dell'utente oppure utilizzare il numero predefinito, nel campo di prova e fare clic su **Test integration (Testare l'integrazione)**. Verificare la riuscita del test.

Configurare utenti, gruppi, porte e pianificazioni in AXIS Entry Manager

1. Andare a **AXIS Entry Manager**.
2. Andare ad **Access Management (Gestione degli accessi)**.
3. Andare a **Doors > Add identification type (Porte > Aggiungi tipo di identificazione)**.
4. Nell'elenco a discesa **Credentials needed (Credenziali necessarie)** selezionare **License plate only (Solo targa)**.
5. Per impostare i limiti per l'utilizzo del tipo di identificazione, trascinare e rilasciare una **Schedule (Pianificazione)** sulla porta.
6. Aggiungere utenti e, per ogni utente, aggiungere le credenziali **License plate (Targa)**.
7. Fare nuovamente clic su **Add credential (Aggiungi credenziali)** e inserire le informazioni sulla targa.
8. Fare clic su **Add new group (Aggiungi nuovo gruppo)** e inserire le informazioni.
9. Per aggiungere utenti a un gruppo, trascinare e rilasciare **Users (Utenti)** sul gruppo di utenti.
10. Per consentire l'accesso agli utenti, trascinare e rilasciare la **Door (Porta)** sul gruppo degli utenti.
11. Per limitare il tempo di accesso, trascinare e rilasciare una **pianificazione** sul gruppo degli utenti.



Panoramica dell'interfaccia utente di AXIS Entry Manager.

- 1 Utenti
- 2 Porte
- 3 Pianificazioni
- 4 Gruppi di utenti

Connettere ad AXIS Secure Entry

Questo esempio illustra la connessione di un door controller Axis in AXIS Camera Station e AXIS Secure Entry con AXIS Licence Plate Verifier.

Requisiti:

- Telecamera e dispositivo di controllo delle porte fisicamente installato e connesso alla rete.
- AXIS License Plate Verifier in funzione sulla telecamera.
- Client AXIS Camera Station versione 5.49.449 e successiva.
- Configurazione di base effettuata. Vedere *Configurazione di base, on page 6*.

In AXIS Camera Station, consulta *Aggiungere un lettore*.

Nell'app AXIS License Plate Verifier:

1. Nella scheda **Settings (Impostazioni)**, vai su **Configuration wizard (Procedura guidata di configurazione guidata)** e fai clic su **Start (Inizio)**.
2. Seleziona **Access Control (Controllo degli accessi)**.
3. Seleziona **Secure Entry** e fai clic su **Next (Avanti)**.

In AXIS Camera Station:

4. Digita l'indirizzo IP del door controller, disponibile nell'elenco dei dispositivi in **AXIS Camera Station>Configuration>Other Devices (AXIS Camera Station>Configurazione>Altri dispositivi)**.

5. Per l'aggiunta di una chiave di autenticazione, vai su **AXIS Camera Station>Configuration>Encrypted communication** (**AXIS Camera Station>Configurazione>Comunicazione crittografata**).
6. Vai a **External Peripheral Authentication Key** (**Chiave di autenticazione dispositivo periferico esterno**) e fai clic su **Show authentication key** (**Mostra chiave di autenticazione**).
7. Fai clic su **Copy key** (**Copia chiave**).

Nell'app **AXIS License Plate Verifier**:

8. Vai su **Authentication key** (**Chiave di autenticazione**) nella procedura guidata di configurazione e incolla la chiave.
9. Fare clic su **Connetti**.
10. Seleziona il **Door controller name** (**Nome del door controller**) nel menu a discesa.
11. Seleziona **Reader name** (**Nome lettore**) nel menu a discesa.
12. Controlla **Turn on integration** (**Attiva l'integrazione**).
13. Fare clic su **Next** (**Avanti**).
14. Regola l'area di interesse. Vedi *Regolare l'area di interesse, on page 10*.
15. Fare clic su **Next** (**Avanti**) due volte quindi su **Finish** (**Fine**).

Scenario con flusso libero con misurazione della velocità

In uno scenario a flusso libero con misurazione della velocità, la telecamera è abbinata a un radar Axis tramite la tecnologia edge-to-edge. La telecamera copre due corsie e legge le targhe dei veicoli di passaggio e il radar accoppiato copre le stesse due corsie per misurare la velocità dei veicoli. Inoltre, l'applicazione *AXIS Speed Monitor* può visualizzare la velocità massima in ogni corsia tramite sovrapposizioni nella visualizzazione in diretta della telecamera.

Per ulteriori informazioni su edge-to-edge, vedere *Tecnologia edge-to-edge, on page 44*.

Requisiti:

- Un kit telecamera AXIS License Plate Verifier e *AXIS D2210-VE Radar* installati e collegati alla rete

Configurare lo scenario

L'impostazione dello scenario avviene in quattro fasi: prima si configura la telecamera, poi si associa e si configura il radar e infine si utilizza *AXIS Speed Monitor* per aggiungere sovrapposizioni.

Operazioni preliminari:

- Assicurarsi che la telecamera e il radar siano diretti verso la stessa area di interesse.
- Assicurarsi che la telecamera e il radar siano sincronizzati. Per controllare lo stato, andare a **Installation > Time sync status (Installazione > Stato sincronizzazione ora)** in ogni dispositivo.
- Assicurarsi che la seconda area di visione della telecamera (**View area 2 (area di visione 2)**) non sia utilizzata, poiché il radar la utilizzerà dopo l'accoppiamento.

Configurare la telecamera:

1. Configurare la telecamera in base alle istruzioni fornite in *Configurazione di base, on page 6*.
2. Assicurarsi di selezionare il flusso libero quando si segue l'Assistente di configurazione. Per ulteriori informazioni, vedere *Libera circolazione, on page 8*.

Associare la telecamera a un radar:

1. Nell'interfaccia Web della telecamera, andare a **System > Edge-to-edge > Radar pairing (Sistema > Edge-to-edge > abbinamento radar)**.
2. Immettere il nome host, il nome utente e la password del radar.
3. Fare clic su **Connect (Connetti)** per associare i dispositivi.
Una volta stabilita la connessione, le impostazioni del radar saranno disponibili nell'interfaccia Web della telecamera.

Nota

La risoluzione predefinita del radar associato è 1280x720. Mantenere la risoluzione predefinita del radar nell'interfaccia Web della telecamera e se la si aggiunge a un VMS.

Configure the radar (Configurare il radar):

1. Nell'interfaccia web della telecamera, andare a **Radar > Scenarios (Radar > Scenari)**.
2. Aggiungere uno scenario radar che copre una corsia e un altro scenario radar che copre l'altra corsia.
3. Per entrambi gli scenari, selezionare **Movement in area (Movimento nell'area)**, attivare su **Vehicles (Veicoli)** e impostare un **Speed limit (Limite di velocità)**.
Per ulteriori informazioni, andare ad *Add scenarios (Aggiungi scenari)* nel manuale per l'utente del radar *AXIS D2210-VE*.

Nota

Se si desidera aggiungere sovrapposizioni contenenti informazioni sulle targhe tramite *AXIS License Plate Verifier*, assicurarsi di aggiungerle prima di aggiungere le sovrapposizioni in *AXIS Speed Monitor*.

Utilizzare *AXIS Speed Monitor* per aggiungere sovrapposizioni di velocità:

1. Scaricare e installare *AXIS Speed Monitor* sulla telecamera.
2. Aggiungere una sovrapposizione testo per ogni testo che mostrerà la velocità massima nella visualizzazione in diretta della telecamera.

Per le istruzioni di installazione e configurazione, andare al manuale per l'utente di *AXIS Speed Monitor*.

Cercare eventi specifici

Utilizzare la funzione di ricerca per cercare eventi utilizzando diversi criteri.

1. Andare alla pagina Web dell'applicazione e selezionare la pagina **Search (Cerca)**.
2. Selezionare la data nei menu del calendario **From (Da)** e **To (A)**.
3. Fare clic sul menu a discesa **AOI** per selezionare l'area di interesse da includere nella ricerca.
4. Selezionare **Direction (Direzione)** per filtrare per ingresso o uscita.
5. Inserire la targa nel campo **Plate (Targa)**, se si desidera cercare una targa.
6. Per individuare le targhe appartenenti a un determinato paese, selezionare un paese nell'elenco a discesa **Country (Paese)**.
7. Per filtrare le immagini in base alla vista del veicolo, selezionare **Front (Anteriore)** oppure **Rear (Posteriore)** nell'elenco del menu a discesa **Vehicle view (Vista veicolo)**.
8. Per filtrare i risultati della ricerca in base a marca, modello, tipo o colore del veicolo, selezionare le opzioni desiderate nei menu a discesa **Vehicle details (Dettagli del veicolo)**.
9. Fare clic su **Apply filters (Applica filtri)** per visualizzare i risultati della ricerca.

Esportare e condividere i risultati della ricerca

Per esportare i risultati della ricerca come file CSV con le statistiche di quel momento, fare clic su **Export (Esporta)** per salvare i risultati come file CSV

Per copiare l'API come collegamento che può essere utilizzato per esportare i dati in sistemi di terze parti, fare clic su **Copy search link (Copia ricerca collegamento)**.

Integrazione

Utilizzare i profili per inviare gli eventi a più server

Con i profili, è possibile inviare un evento a diversi server utilizzando diversi protocolli contemporaneamente. Per utilizzare i profili:

1. Andare a **Integration** (Integrazione) e alla pagina **Push events** (Invia eventi).
2. Selezionare **Profile 1** (Profilo 1).
3. Configurare la regola. Vedere *Inviare le informazioni relative agli eventi a software di terze parti, on page 38*.
4. Test della regola.
5. Selezionare una nuova scheda profilo per configurare una nuova regola.

Inviare le informazioni relative agli eventi a software di terze parti

Nota

L'applicazione invia le informazioni relative agli eventi in formato JSON. *Accedi tramite il tuo account MyAxis*, vai su *AXIS VAPIX Library* e seleziona *AXIS License Plate Verifier* per ottenere maggiori informazioni.

Con questa funzione è possibile integrare software di terze parti inviando i dati relativi agli eventi tramite TCP o HTTP POST.

Operazioni preliminari:

- La telecamera deve essere fisicamente installata e connessa alla rete.
 - AXIS License Plate Verifier deve essere in esecuzione sulla telecamera.
1. Vai su **Integration** (Integrazione) > **Push events** (Invia eventi).
 2. Selezionare un profilo vuoto
 3. Nell'elenco a discesa **Protocol** (Protocollo) selezionare **HTTP POST**.
 4. Nel campo **Server URL** (URL server), digitare l'indirizzo del server e la porta nel seguente formato:
127.0.0.1:8080
 5. Digitare il nome utente e la password.
 6. Se si sta utilizzando un proxy, attivarlo e inserire il nome host, nome utente e password.
 7. Nel campo **Device ID** (ID dispositivo), digitare il nome del dispositivo o lasciarlo invariato.
 8. Selezionare la direzione in cui attivare gli eventi push in **Push conditions** (Condizioni di push).
 9. In **LPR Event types** (Tipi di evento LPR), selezionare una o più opzioni seguenti:
 - **New** (Nuova) indica il primo rilevamento di una targa.
 - **Update** (Aggiornamento) è una correzione di un carattere su una targa rilevata in precedenza o quando viene rilevata una direzione mentre la targa si sposta ed è tracciata nell'immagine.
 - **Lost** (Persa) è l'ultimo evento della targa rilevato prima della sua uscita dall'immagine. Contiene inoltre la direzione della targa.
 - **Conditional** (Condizionale) invia un evento per un oggetto quando le condizioni sono soddisfatte.
 10. Per ridurre la larghezza di banda quando si utilizza HTTP POST, è possibile selezionare **Do not to send images** (Non inviare immagini).
 11. Abilitare **Event buffer** (Buffer evento) per memorizzare gli eventi nel buffer in caso di interruzione del server e inviarli quando il server torna disponibile.
 12. Per includere il ritaglio della targa oltre all'immagine, se è stata scelta l'opzione in **Retention settings** (Impostazioni di conservazione) selezionare **Send two images** (Invia due immagini).
 13. Per inviare gli eventi in formato multipart anziché base64, selezionare **Multipart**.

14. Fare clic su **Test (Prova)** per verificare l'integrazione con una targa virtuale.
15. Per attivare la funzione, selezionare **Activate (Attiva)**.

Nota

Per inviare gli eventi tramite HTTP POST, è possibile utilizzare un'intestazione di autorizzazione anziché un nome utente e una password, andare a **Auth-Header (Autore-Intestazione)** e aggiungere un percorso a un'API di autenticazione.

Invio a un server di immagini di targhe

Questa funzione ti consentirà l'invio delle immagini delle targhe a un server tramite FTP.

Operazioni preliminari:

- La telecamera deve essere fisicamente installata e connessa alla rete.
 - AXIS License Plate Verifier deve essere in esecuzione sulla telecamera.
1. Vai su **Integration (Integrazione) > Push events (Invia eventi)**.
 2. Nell'elenco a discesa **Protocol (Protocollo)** seleziona **FTP**.
 3. Nel campo **Server URL (URL server)**, digitare l'indirizzo del server nel seguente formato: `ftp://10.21.65.77/LPR`.
 4. Inserisci il nome utente e la password per il server FTP.
 5. Selezionare i campi di modifica del percorso e del nome per i nomi dei file.
 6. Nel campo **Device ID (ID dispositivo)**, digitare il nome del dispositivo. Una cartella con questo nome sarà creata per le immagini. Le immagini vengono create utilizzando il seguente formato: `timestamp_area di interesse_direzione_ID auto_testo targa_paese.jpg`.
 7. Selezionare la direzione in cui attivare gli eventi push in **Push conditions (Condizioni di push)**.
 8. In **Event types (Tipi di evento)**, selezionare una o più opzioni seguenti:
 - **New (Nuova)** indica il primo rilevamento di una targa.
 - **Update (Aggiornamento)** è una correzione di un carattere su una targa rilevata in precedenza o quando viene rilevata una direzione mentre la targa si sposta ed è tracciata nell'immagine.
 - **Lost (Persa)** è l'ultimo evento della targa rilevato prima della sua uscita dall'immagine. Contiene inoltre la direzione della targa.
 - **Conditional (Condizionale)** invia un evento per un oggetto quando le condizioni sono soddisfatte.

Nota

La direzione è compresa nel nome del file solo quando si seleziona **Lost (Persa)** o **Update (Aggiorna)**.

9. Fare clic su **Test (Prova)** per verificare l'integrazione con una targa virtuale.
10. Per attivare la funzione, fare clic su **Activate (Attiva)**.

Nota

Notare che l'immagine subisce variazioni a seconda del tipo di modalità di acquisizione selezionata, consultare *Regolare le impostazioni di acquisizione, on page 11*.

Nota

Se gli eventi push falliscono, l'applicazione invia nuovamente al server fino ai primi 100 eventi falliti. Quando si usa l'FTP negli eventi push su un server Windows, non usare %c per denominare le immagini che forniscono data e ora. Questo perché Windows non accetta la denominazione impostata dalla funzione %c per la data e l'ora. Questo problema non si presenta se si utilizza un server Linux.

Integrazione diretta con 2N

Questo esempio illustra l'integrazione diretta con un dispositivo IP 2N.

Configurazione di un account nel dispositivo 2N:

1. Vai su 2N IP Verso.
2. Andare a **Services (Servizi) > HTTP API (API HTTP)> Account 1**.
3. Seleziona **Enable account (Abilita account)**.
4. Seleziona **Camera access (Accesso alla telecamera)**.
5. Seleziona **License plate recognition (Riconoscimento targhe)**.
6. Copia l'indirizzo IP.

Nell'app AXIS License Plate Verifier:

1. Andare a **Integration (Integrazione) > Direct integration (Integrazione diretta)**.
2. Selezionare **2N IP Device (Dispositivo IP 2N)**.
3. Aggiungi al dispositivo 2N l'indirizzo IP o l'URL.
4. Immetti il nome utente e la password.
5. Seleziona **Connection type (Tipo di connessione)**.
6. Seleziona un uso per la barriera con l'apposita opzione **Barrier is used for (La barriera è usata per)**.
7. Fare clic su **Enable integration (Abilita integrazione)**.
8. Selezionare la direzione dei veicoli.
9. Per attivare la funzione, selezionare **Activate (Attiva)**.

Per verificare il funzionamento dell'integrazione:

1. Vai su 2N IP Verso.
2. Andare a **Status (Stato) > Events (Eventi)**.

Integrazione con Genetec Security Center

Questo esempio descrive come impostare un'integrazione diretta con Genetec Security Center.

In Genetec Security Center:

1. Andare a **Overview (Panoramica)**.
2. Assicurati che **Database, Directory e License (Licenza)** siano online. Se non lo sono, esegui tutti i servizi Genetec e SQLEXPRESS in Windows.
3. Vai su **Genetec Config Tool > Plugins (Genetec Config Tool > Plugin)**.
4. Fai clic su **Add an entity (Aggiungi un'entità)**.
5. Vai su **Plugin** e seleziona **LPR plugin (Plugin LPR)**.
6. Fare clic su **Next (Avanti)**.
7. Fare clic su **Next (Avanti)**.
8. Fare clic su **Next (Avanti)**.
9. Seleziona il plugin LPR che hai aggiunto e vai su **Data sources (Sorgenti dati)**.

In **ALPR reads API (API letture ALPR)**:

10. Seleziona **Enabled (Abilitato)**.
11. In **Name (Nome)**, digita: **Plugin REST API**.
12. In **API path prefix (Prefisso percorso API)**, digitare: **lpr**.
13. In **REST port (Porta REST)**, seleziona **443**.
14. In **WebSDK host (Host WebSDK)**, digitare: **localhost**.
15. In **WebSDK port, (Porta WebSDK)** seleziona **443**.
16. Seleziona **Allow self signed certificates (Consenti certificati autofirmati)**.

In Security Center events data source (Sorgente dati eventi Security Center):

17. Seleziona **Enabled (Abilitato)**.
18. In **Name (Nome)**, digita eventi Lpr Security Center.
19. In **Processing frequency (Frequenza di elaborazione)**, seleziona 5 sec nel menu a discesa.
20. Vai alla scheda **Data sinks (Sink di dati)**.
21. Fare clic su **+**.
22. In **Type (Tipo)**, seleziona **Database**.
23. Seleziona e configura il database:
 - Seleziona **Enabled (Abilitato)**.
 - In **Source (Sorgente)**, seleziona **Plugin REST API e Native ALPR Events (Eventi nativi ALPR)**.
 - In **Name (Nome)**, digita **Reads DB (Database letture)**.
 - In **Include (Includi)**, seleziona **Reads (Letture)**, **Hits (Riscontri)** e **Images (Immagini)**.
 - Vai alla scheda **Resources (Risorse)**.
 - Fai clic su **Delete the database (Elimina il database)** e poi su **Create a database (Crea un database)**.

Create an API user: (Crea un utente API)

24. Vai su **Config Tool > User Management (Strumento configurazione > Gestione utente)**.
25. Fai clic su **Add an entity (Aggiungi un'entità)**.
26. Seleziona **User (Utente)**.
27. Digitare un nome utente e una password. Lascia invariati gli altri campi.
28. Seleziona l'utente aggiunto e vai alla scheda **Privileges (Privilegi)**.
29. Seleziona per permettere tutto in **Application privileges (Privilegi applicazione)**.
30. Seleziona per permettere **Third-party ALPR reads API (API letture ALPR di terze parti)**.
31. fare clic su **Applica**;

Nell'app **AXIS License Plate Verifier**:

1. Andare a **Integration (Integrazione) > Direct integration (Integrazione diretta)**.
2. Selezionare **Genetec Security Center**.
3. In **URL/IP**, digitare il proprio indirizzo in base a questo modello: `https://server-address/api/V1/lpr/lpringestion/reads`.
4. Digita il tuo nome utente e la password Genetec.
5. Seleziona **Connection type (Tipo di connessione)**.
6. Per attivare la funzione, selezionare **Activate (Attiva)**.
7. Fare clic su **Test (Prova)** per verificare l'integrazione con una targa virtuale.
8. Se si è scelto **HTTPS**, andare alla scheda **Settings (Impostazioni)**.
9. In **Security > HTTPS (Sicurezza > HTTPS)**.
10. Seleziona **Self-signed (Autofirmato)** o **CA-signed (Con firma CA)** in base alle impostazioni in Genetec Security Center.

In Genetec Security Center:

1. Vai a **Genetec Security desk**.
2. In **Investigation (Indagine)**, fai clic **Reads (Letture)**.
3. Vai alla scheda **Reads (Letture)**.
4. Filtra il risultato in base alle tue esigenze.

5. Fare clic su **Genera report**.

Nota

Puoi anche leggere la documentazione di Genetec relativa all'integrazione di plugin ALPR di terzi. *Puoi farlo qui (registrazione necessaria).*

Interfaccia Web

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

Per saperne di più

Tecnologia edge-to-edge

Edge-to-edge è una tecnologia che consente ai dispositivi IP di comunicare direttamente tra loro. Offre la funzionalità di accoppiamento intelligente, ad esempio, tra le telecamere Axis e i prodotti audio o radar Axis.

Nota

Verificare che i dispositivi associati utilizzino la stessa versione di AXIS OS.

Per ulteriori informazioni, consultare il documento tecnico "Tecnologia edge-to-edge" all'indirizzo [whitepapers.axis.com/edge-to-edge-technology](https://axis.com/edge-to-edge-technology).

Abbinamento radar

Grazie all'abbinamento radar edge-to-edge è possibile collegare la telecamera a un radar Axis compatibile e trarre vantaggio dalle funzionalità radar integrate, come il rilevamento della velocità.

L'abbinamento radar è una configurazione unidirezionale in cui una telecamera viene abbinata a un radar e utilizzata per configurare e mantenere entrambi i dispositivi. Se abbinato, è possibile accedere alle impostazioni del radar e creare regole per eventi specifici del radar direttamente nell'interfaccia Web della telecamera. La telecamera si identificherà anche con un VMS come una telecamera con funzionalità radar integrata.

In più, il flusso radar è visualizzato nella seconda area di visione della telecamera, detta **area di visione 2**. I metadati prodotti dal radar sono disponibili tramite il secondo canale di produttore di metadati della telecamera denominato **channel 2 (canale 2)**.

Associazione altoparlante

L'associazione altoparlante edge-to-edge consente di utilizzare un altoparlante di rete Axis compatibile come se fosse parte della telecamera. Una volta associate, le caratteristiche dell'altoparlante sono integrate nell'interfaccia Web della telecamera e l'altoparlante di rete agisce come un dispositivo di uscita audio in cui è possibile riprodurre clip audio e trasmettere l'audio attraverso la telecamera.

La telecamera si identificherà al VMS come una telecamera con uscita audio integrata e reindirizza l'audio riprodotto all'altoparlante.

Area di visualizzazione

Un'area di visione è una parte ritagliata della vista completa. È possibile eseguire lo streaming e l'archiviazione di aree di visione invece della vista completa per ridurre al minimo le esigenze di larghezza di banda e spazio di archiviazione. Se si abilita PTZ per un'area di visione, è possibile eseguire la rotazione, l'inclinazione e lo zoom all'interno dell'area in questione. Utilizzando le aree di visione, è possibile rimuovere parti della vista completa, ad esempio il cielo.

Quando si configura un'area di visione, si consiglia di impostare la risoluzione del flusso video sullo stesso formato o un formato inferiore rispetto alla dimensione dell'area di visione. Se si imposta una risoluzione del flusso video maggiore della dimensione dell'area di visione, il video viene scalato digitalmente dopo l'acquisizione del sensore richiedendo una maggiore larghezza di banda senza aggiungere informazioni sull'immagine.

Nota

Se la telecamera viene abbinata a un radar tramite edge-to-edge, il flusso radar viene visualizzato nella seconda area di visione della telecamera.

AXIS Image Health Analytics

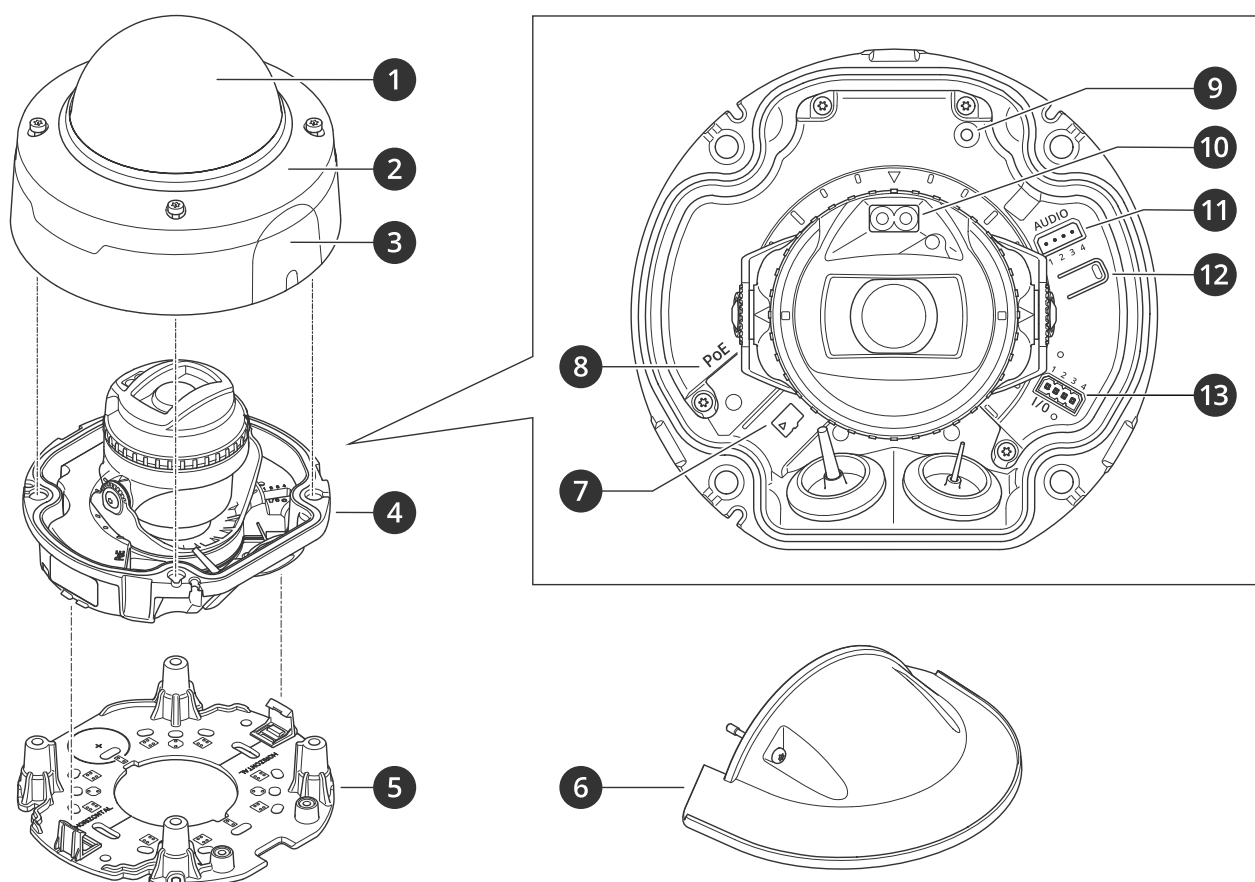
AXIS Image Health Analytics è un'applicazione basata sull'intelligenza artificiale che può essere impiegata per rilevare la degradazione delle immagini o i tentativi di manomissione. L'applicazione analizza e apprende il comportamento della scena per rilevare sfocature o sottoesposizioni nell'immagine, oppure per rilevare una vista

ostruita o reindirizzata. È possibile impostare l'applicazione in modo che invii eventi per uno qualsiasi dei rilevamenti e che attivi azioni attraverso il sistema di eventi della telecamera o un software di terze parti.

Per ulteriori informazioni su come funziona l'applicazione, consultare il *manuale per l'utente di AXIS Image Health*.

Dati tecnici

Panoramica dei prodotti



- 1 Dome
- 2 Copertura della cupola
- 3 Coperchio
- 4 Unità telecamera
- 5 Staffa di montaggio
- 6 Schermo di protezione
- 7 Slot per scheda di memoria SD
- 8 Connettore di rete (PoE)
- 9 Indicatore LED di stato
- 10 LED a infrarossi
- 11 Connettore audio
- 12 Pulsante di comando
- 13 Connettore I/O

Indicatori LED

LED di stato	Significato
Spento	Connessione e funzionamento normale.
Verde	Una luce verde fissa per 10 secondi indica il normale funzionamento una volta completato l'avvio.
Giallo	Luce fissa durante l'avvio. Lampeggia durante l'aggiornamento del software del dispositivo o il ripristino delle impostazioni predefinite.
Giallo/rosso	Lampeggia in giallo/rosso se il Collegamento di rete non è disponibile o è stato perso.

Slot per scheda SD

AVVISO

- Rischio di danneggiamento della scheda di memoria. Non utilizzare strumenti appuntiti oppure oggetti metallici e non esercitare eccessiva forza durante l'inserimento o la rimozione della scheda di memoria. Utilizzare le dita per inserire e rimuovere la scheda.
- Rischio di perdita di dati e danneggiamento delle registrazioni. Smontare la scheda di memoria dall'interfaccia Web del dispositivo prima di rimuoverla. Non rimuovere la scheda di memoria mentre il dispositivo è in funzione.

Questo dispositivo supporta schede microSD/microSDHC/microSDXC.

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



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

Pulsanti

Pulsante di comando

Il pulsante di comando viene utilizzato per:

- Ripristino del dispositivo alle impostazioni predefinite di fabbrica. Vedere *Ripristino delle impostazioni predefinite di fabbrica, on page 49*.

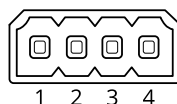
Connettori

Connettore di rete

Connettore Ethernet RJ45 con Power over Ethernet (PoE).

Connettore audio

Morsettiera a 4 pin per ingresso e uscita audio.



Funzione	Pin	Note
TERRA	1	Terra
Alimentazione ad anello	2	12 V per sorgente esterna
Ingresso microfono/linea	3	Microfono (analogico o digitale) o ingresso linea (mono). La polarizzazione del microfono può essere impostata sul valore 5 V.
Uscita linea	4	Uscita audio linea (mono). Può essere connessa a un impianto di diffusione sonora (PA) oppure a un altoparlante con amplificatore integrato.

Connettore I/O

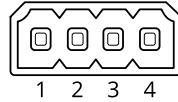
Utilizzare il connettore I/O con dispositivi esterni in combinazione con, ad esempio, rilevamento movimento, attivazione di eventi e notifiche di allarme. Oltre al punto di riferimento 0 V CC e all'alimentazione (output 12 V CC), il connettore I/O fornisce l'interfaccia per:

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

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

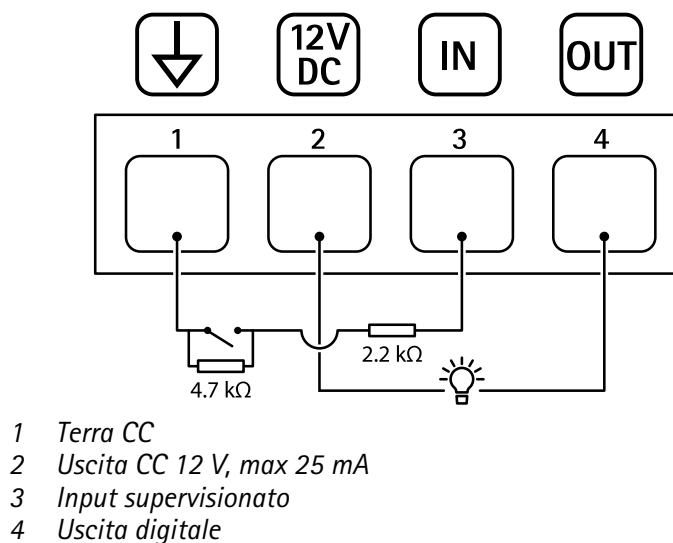
Uscita digitale – Per il collegamento di dispositivi esterni come relè e LED. I dispositivi collegati possono essere attivati tramite l'API (interfaccia per la programmazione di applicazioni) VAPIX® attraverso un evento oppure dall'interfaccia Web del dispositivo.

Morsettiera a 4 pin



Funzione	Pin	Note	Dati tecnici
Terra CC	1		0 V CC
Uscita CC	2	 Questo terminale può essere utilizzato anche per alimentare una periferica ausiliaria. Nota: questo pin può essere usato solo come uscita alimentazione.	12 V CC Carico massimo = 25 mA
Ingresso digitale o ingresso supervisionato	3	Collegarlo al pin 1 per attivarlo oppure lasciarlo isolato (scollegato) per disattivarlo. Per utilizzare l'ingresso supervisionato, installare resistori terminali. Vedere il diagramma di connessione per informazioni su come collegare i resistori.	Da 0 a max 30 V CC
Uscita digitale	4	Collegato internamente al pin 1 (terra CC) quando attivo e isolato (scollegato) quando inattivo. Se utilizzata con un carico induttivo, ad esempio un relè, collegare un diodo in parallelo al carico per proteggere il dispositivo da sovratensioni.	Da 0 a max 30 V CC, open-drain, 100 mA

Esempio:



Risoluzione dei problemi

Ripristino delle impostazioni predefinite di fabbrica

▲ AVVISO

⚠ Questo dispositivo emette radiazioni ottiche pericolose. Potrebbe essere dannoso per gli occhi. Non fissare la lampada accesa.

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.

Nota

La telecamera è stata preconfigurata con AXIS License Plate Verifier. In caso di ripristino dei valori predefiniti di fabbrica, sarà necessario reinstallare la chiave di licenza. Non sarà necessario reinstallare l'applicazione dopo un ripristino di fabbrica.

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 46.
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. 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.
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 la pagina Web del dispositivo. Andare a **Maintenance (Manutenzione) > Factory default (Impostazione di fabbrica)** e fare clic su **Default (Predefinito)**.

Opzioni AXIS OS

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

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

Controllo della versione corrente del AXIS OS

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

Per controllare la versione corrente di AXIS OS:

1. Andare all'interfaccia Web del dispositivo > **Status (Stato)**.

2. Vedere la versione AXIS OS in **Device info (Informazioni dispositivo)**.

Aggiornare AXIS OS

Importante

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

Nota

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

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

Puoi usare AXIS Device Manager per l'aggiornamento di più dispositivi allo stesso tempo. Maggiori informazioni sono disponibili sul sito Web axis.com/products/axis-device-manager.

Problemi tecnici e possibili soluzioni

Problemi durante l'aggiornamento di AXIS OS

Aggiornamento di AXIS OS non riuscito

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

Problemi dopo l'aggiornamento di AXIS OS

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

Problemi durante l'impostazione dell'indirizzo IP

Impossibile impostare l'indirizzo IP

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

Problemi di accesso al dispositivo

Impossibile effettuare l'accesso al dispositivo tramite un browser.

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

Se si è smarrita la password per l'account root, è necessario ripristinare le impostazioni predefinite di fabbrica del dispositivo. Per le istruzioni, vedere *Ripristino delle impostazioni predefinite di fabbrica, on page 49*.

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 durante lo streaming

Multicast H.264 accessibile solo dai client locali

Verificare se il router supporta il multicasting o se è necessario configurare le impostazioni del router tra il client e il dispositivo. Potrebbe essere necessario aumentare il valore TTL (Time To Live).

Nessun multicast H.264 visualizzato nel client

Verificare con l'amministratore di rete che gli indirizzi multicast utilizzati dal dispositivo Axis siano validi per la rete.

Verificare con l'amministratore di rete se è disponibile un firewall che impedisce la visualizzazione.

Rendering scarso delle immagini H.264

Assicurarsi che la scheda video utilizzi il driver più recente. Puoi generalmente scaricare i driver più recenti dal sito Web del produttore.

La saturazione del colore è diversa in H.264 e Motion JPEG

Modificare le impostazioni per l'adattatore della scheda video. Per ulteriori informazioni controllare la documentazione dell'adattatore.

Velocità in fotogrammi inferiore al previsto

- Vedere *Considerazioni sulle prestazioni, on page 54*.
- Ridurre il numero di applicazioni in esecuzione nel computer client.
- Limitare il numero di visualizzatori simultanei.
- Controllare con l'amministratore di rete che sia disponibile una larghezza di banda sufficiente.
- Ridurre la risoluzione dell'immagine.
- Accedere all'interfaccia Web del dispositivo e impostare una modalità di acquisizione che dia priorità alla velocità in fotogrammi. Se si modifica la modalità di acquisizione in modo da dare priorità alla velocità in fotogrammi, si potrebbe ridurre la risoluzione massima a seconda del dispositivo utilizzato e delle modalità di acquisizione disponibili.

Impossibile selezionare la codifica H.265 nella visualizzazione in diretta

I browser Web non supportano la codifica H.265. Utilizzare un'applicazione o un sistema di gestione video che supporta la codifica H.265.

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. Verificare con il proprio server/broker provider se ALPN è supportato e quale protocollo e porta ALPN utilizzare.

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

I veicoli sconosciuti sono contrassegnati come accettati

Se l'applicazione consente ai veicoli con targhe non incluse nella lista consentiti, un motivo probabile è che il confronto consenta una deviazione di un carattere.

Ad esempio, se **AXI S1234** è nella lista consentiti, l'applicazione accetta **AXI SI234**.

Allo stesso modo, se **AXIS 1234** è nella lista consentiti, l'applicazione accetta **AXI 1234**.

Vai a *Impostazioni supplementari*, on page 25 per impostare i caratteri permessi.

La connessione tra l'applicazione e il dispositivo di controllo o un modulo relè non funziona

Assicurarsi che il dispositivo di controllo, o il modulo relè, consenta il traffico di dati tramite HTTP. Per sapere come modificare questa impostazione, consultare il manuale per l'utente del dispositivo corrispondente.

Problemi con l'abbinamento radar

Impossibile associare la telecamera al radar	Assicurarsi che la seconda area di visione della telecamera (View area 2 (Area di visione 2)) non sia utilizzata poiché il radar verrà assegnato automaticamente. Se viene utilizzata la seconda area di visione, andare su Video > View areas (Video > Aree di visione) per rimuoverla, quindi riprovare ad associare i dispositivi.
I veicoli in movimento nella vista della telecamera non sono sincronizzati con le sovrapposizioni di velocità o con le tracce nella vista radar	Assicurarsi che la telecamera e il radar siano sincronizzati. Per controllare lo stato, andare a Status > Time sync status (Stato > stato di sincronizzazione dell'ora) nell'interfaccia Web di ogni dispositivo. Se lo stato mostra Synchronized: No (Sincronizzato: no), fare clic su NTP settings (Impostazioni NTP) e selezionare una sorgente di tempo per la sincronizzazione del dispositivo. Assicurarsi di utilizzare la stessa origine ora per entrambi i dispositivi.
La seconda area di visione della telecamera non mostra correttamente il flusso radar	La risoluzione predefinita del radar dopo l'associazione edge-to-edge è 1280x720, sia nell'interfaccia Web della telecamera che in un VMS. Se si seleziona un'altra risoluzione, il flusso radar verrà visualizzato in modo errato. Per regolare la risoluzione del radar, andare a Video > Stream > General (Video > Flusso > Generale) nell'interfaccia Web della telecamera e selezionare View area 2 (Area di visione 2).

Problemi con le sovrapposizioni	
Le sovrapposizioni testo aggiunte tramite l'interfaccia Web della telecamera scompaiono dopo l'accoppiamento radar	Se sono state aggiunte più aree di visione nella telecamera, tutte le sovrapposizioni testo aggiunte in precedenza scompariranno dall'interfaccia Web della telecamera. Poiché il radar occupa la seconda area di visione dopo l'accoppiamento radar, tutte le sovrapposizioni presenti nell'interfaccia Web della telecamera scompariranno. Le sovrapposizioni testo scompariranno solo dall'interfaccia Web. È comunque possibile richiedere un flusso contenente le sovrapposizioni, ad esempio in un VMS.
Le sovrapposizioni delle targhe aggiunte in AXIS License Plate Verifier non vengono visualizzate	Se sono state aggiunte delle sovrapposizioni che mostrano la velocità del veicolo in AXIS Speed Monitor e quindi si attivano le sovrapposizioni delle targhe in AXIS License Plate Verifier, le sovrapposizioni delle targhe non verranno visualizzate. Assicurarsi di attivare le sovrapposizioni in AXIS License Plate Verifier prima di aggiungere eventuali sovrapposizioni di velocità tramite AXIS Speed Monitor.

Considerazioni sulle prestazioni

Quando s'imposta il sistema, è importante considerare come le diverse impostazioni e situazioni influiscono sulle prestazioni. Alcuni fattori influiscono sulla larghezza di banda (velocità in bit), altri sulla velocità in fotogrammi e altri ancora influenzano entrambi.

I fattori più importanti da considerare:

- Una risoluzione elevata dell'immagine o livelli di compressione inferiori generano immagini con più dati che, a loro volta, influiscono sulla larghezza di banda.
- La rotazione dell'immagine nell'interfaccia grafica utente (GUI) può aumentare il carico della CPU del dispositivo.
- L'accesso da parte di numerosi client Motion JPEG o unicast H.264/H.265/AV1 influisce sulla larghezza di banda.
- La vista simultanea di flussi differenti (risoluzione, compressione) di client diversi influisce sia sulla velocità in fotogrammi che sulla larghezza di banda. Utilizzare flussi identici quando possibile per mantenere un frame rate elevato. Per garantire che i flussi siano identici, è possibile utilizzare i profili di streaming.
- L'accesso simultaneo a flussi video con codec differenti influisce sulla velocità in fotogrammi e sulla larghezza di banda. Per ottenere prestazioni ottimali, impiegare flussi con lo stesso codec.
- L'uso eccessivo di impostazioni evento influisce sul carico CPU del dispositivo che, a sua volta, influisce sul frame rate.
- L'uso di HTTPS può ridurre il frame rate, in particolare se streaming Motion JPEG.
- Un utilizzo eccessivo della rete dovuto a una scarsa infrastruttura influisce sulla larghezza di banda.
- La visualizzazione in client computer con prestazioni scarse abbassa la qualità delle prestazioni percepite e influisce sul frame rate.
- L'esecuzione simultanea di più applicazioni di Piattaforma applicativa per telecamere AXIS (ACAP) può influire sulla velocità in fotogrammi e sulle prestazioni generali.

Contattare l'assistenza

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

Cyber security

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

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

Gestione delle vulnerabilità

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

Notifiche di sicurezza

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

Ciclo di vita sicuro del prodotto

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

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

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

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

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

T10191705_it

2026-07 (M16.2)

© 2023 – 2026 Axis Communications AB