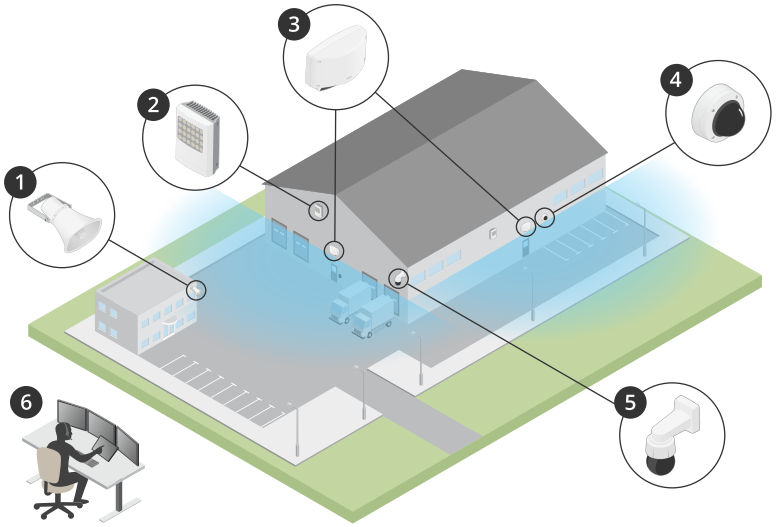
AXIS D2110-VE Security Radar

Manuale per l'utente

AXIS D2110-VE Security Radar

Sommario

Panoramica delle soluzioni



1 *Altoparlante a tromba C1310-E*
2 *Door controller*
3 *D2110–VE Security Radar*
4 *Telecamera a cupola fissa*
5 *Telecamera PTZ*
6 *Centro di sorveglianza*

Profili radar

Nota

Per utilizzare i profili radar sul dispositivo deve essere in esecuzione la versione firmware 10.11 o successiva. Visitare il sito per aggiornare il firmware.

Il manuale per l'utente consente di utilizzare il radar a seconda dell'operazione che si desidera effettuare. AXIS D2110-VE Security Radar ha due profili:

- **Profilo di monitoraggio dell'area** per rilevare gli oggetti grandi e piccoli che si muovono a velocità inferiori a 55 km/h
- **Profilo di monitoraggio della strada** per rilevare i veicoli che si muovono a velocità fino a 105 km/h

Tutte le informazioni contenute in questo manuale per l'utente che non rientrano nelle sezioni **Profilo di monitoraggio dell'area** o **Profilo di monitoraggio della strada** sono comuni ad entrambi i profili ed è possibile farvi riferimento indipendentemente dal profilo utilizzato.

Dove installare il dispositivo

- Il radar è destinato a controllare aree aperte. Gli oggetti solidi (ad esempio una parete, una recinzione, un albero o un cespuglio di grandi dimensioni) in quest'area di copertura creeranno un limite di utilizzo (ombra radar) nella parte posteriore.
- Installare il radar su un palo stabile o in un punto su un muro in cui non ci sono altri oggetti o installazioni accanto ad esso. Gli oggetti entro 1 m a sinistra e a destra del radar, che riflettono le onde radio, influiscono sulle prestazioni del radar.
- Gli oggetti metallici nel campo visivo causano riflessi che influiscono sulla capacità del radar di eseguire le classificazioni.

- Se vuoi eseguire l'installazione di più di due radar nella stessa zona di coesistenza, consultare *Installazione di più radar alla pagina 5*.

Area di copertura

Axis D2110–VE ha una copertura orizzontale di 180°. L'intervallo di rilevamento corrisponde a 5.600 m^2 per gli esseri umani e a 11.300 m^2 per i veicoli.

Nota

Una copertura ottimale dell'area si applica quando il radar è montato da 3,5 a 4 m. L'altezza di montaggio influisce sulle dimensioni del punto cieco sotto il radar.

Profilo di monitoraggio dell'area

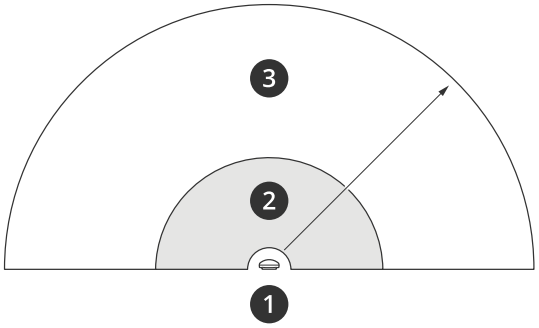
Il **profilo di monitoraggio dell'area** è ottimizzato per gli oggetti in movimento fino a una velocità di 55 km/h. Questo profilo consente di rilevare se un oggetto è un essere umano, un veicolo o un oggetto sconosciuto. È possibile impostare una regola o un'azione in modo da attivare un evento quando viene rilevato uno di questi oggetti. Per seguire i veicoli che si muovono a velocità superiori, utilizzare il *Profilo di monitoraggio della strada alla pagina 12*.

Installazione di più radar

Puoi eseguire l'installazione di molteplici radar per la copertura di aree come l'area circostante di un edificio o la zona di buffer fuori da una recinzione.

Coesistenza

Quando posizioni oltre due radar nella stessa zona di coesistenza, le onde radio che provengono dai radar nella zona possono causare interferenze e avere un influsso sulle prestazioni. Il raggio della zona di coesistenza corrisponde a 350 m.



1 Radar
2 Area di rilevamento
3 Zona di coesistenza

Nota

Le prestazioni del radar nella zona di coesistenza possono anche subire l'influenza dell'ambiente e/o della direzione del radar verso recinzioni, edifici o radar vicini.

Installa 2–3 radar nella stessa zona coesistenza

Quando posizioni due o tre radar nella stessa zona di coesistenza, devi definire il numero di radar vicini nell'interfaccia del dispositivo. Così puoi migliorare le prestazioni dei radar ed evitare interferenze.

1. Vai su **Radar > Settings > Coexistence (Radar > Impostazioni > Coesistenza)**.
2. Seleziona il numero di radar vicini.

Vedi *Esempi di installazione su un'area alla pagina 6* per leggere esempi di installazioni con molteplici radar.

Installa 4–6 radar nella stessa zona coesistenza

Nota

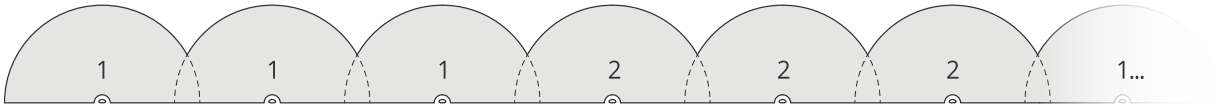
L'opzione di installare un massimo di sei radar nella stessa zona di coesistenza è disponibile dalla versione firmware 11.3.

Quando monti tra i quattro e i sei radar nella stessa zona di coesistenza, imposta per prima cosa il numero di radar vicini, poi aggiungi ciascun radar ad un gruppo. Inizia con il radar installato più lontano, ad es. il più lontano a sinistra. Aggiungi i radar in gruppi di tre e aggiungi i radar più vicini l'uno all'altro nello stesso gruppo.

Profilo di monitoraggio dell'area

I radar nel gruppo si sincronizzeranno tra loro per l'ottimizzazione delle prestazioni e al fine di evitare che interferiscano tra loro.

1. Vai su **Radar > Settings > Coexistence (Radar > Impostazioni > Coesistenza)**.
2. Imposta il numero di radar vicini come **3–5**.
3. Seleziona un gruppo per il tuo radar.



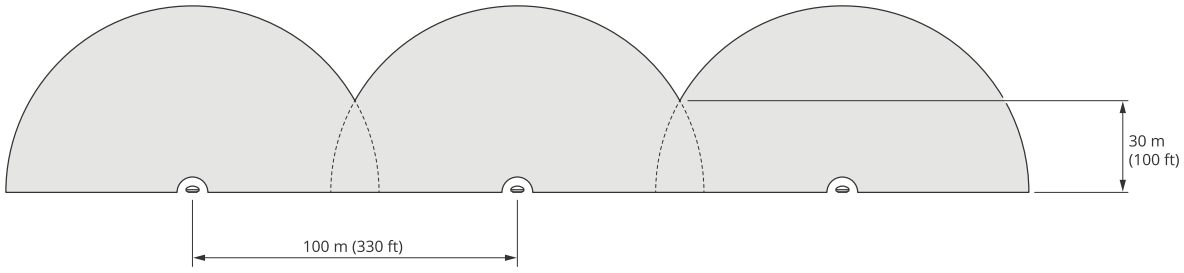
Questo esempio illustra come si raggruppano molteplici radar installati uno accanto all'altro nella stessa zona di coesistenza.

Vedi *Esempi di installazione su un'area alla pagina 6* per leggere ulteriori esempi di installazioni con molteplici radar.

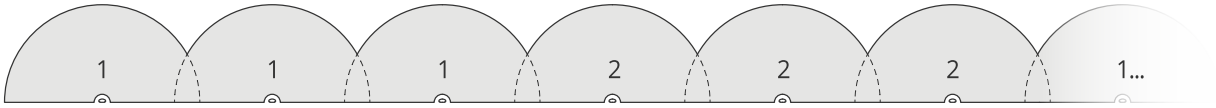
Esempi di installazione su un'area

Crea una recinzione virtuale con molteplici radar

Per eseguire la creazione di una recinzione virtuale, ad es. lungo o intorno un edificio, puoi posizionare molteplici radar uno accanto all'altro. Si consiglia di posizionarli distanziandoli di 100 m.

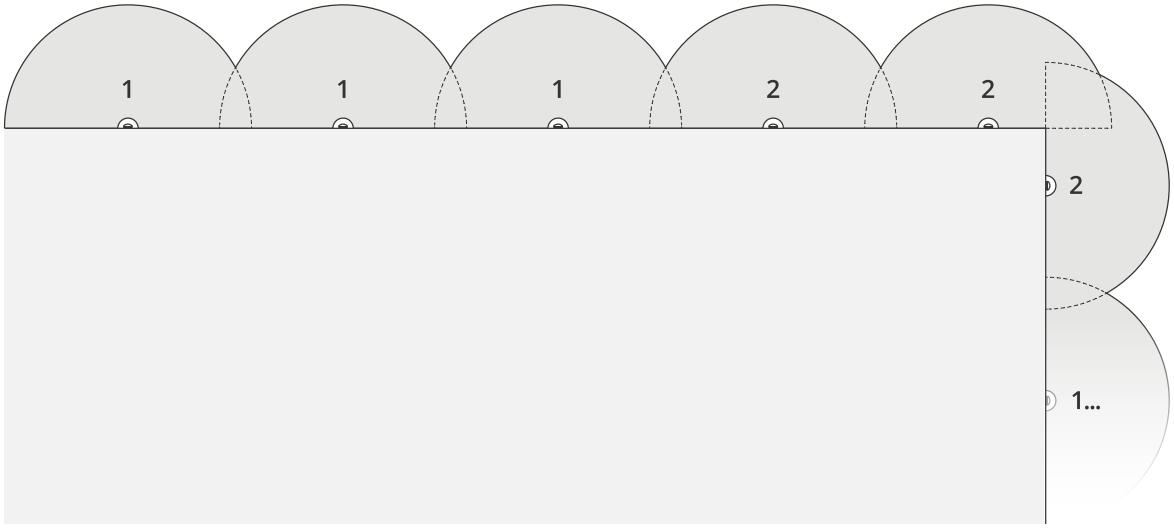


Per evitare interferenze quando monti più di due radar nella stessa zona di coesistenza, imposta il numero di radar vicini nell'interfaccia del dispositivo. In più, quando monti oltre tre radar, aggiungi ogni radar ad un gruppo.



Puoi eseguire la regolazione della recinzione virtuale per coprire anche gli angoli, come illustra questo esempio.

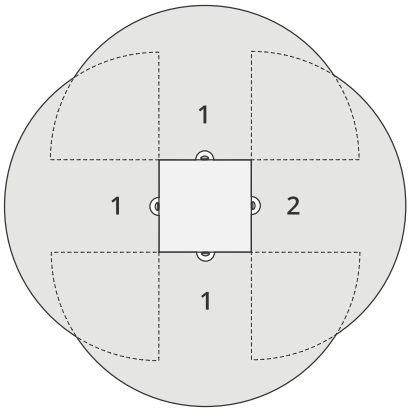
Profilo di monitoraggio dell'area



Vedi *Installazione di più radar alla pagina 5* per maggiori informazioni sui radar e sui gruppi vicini.

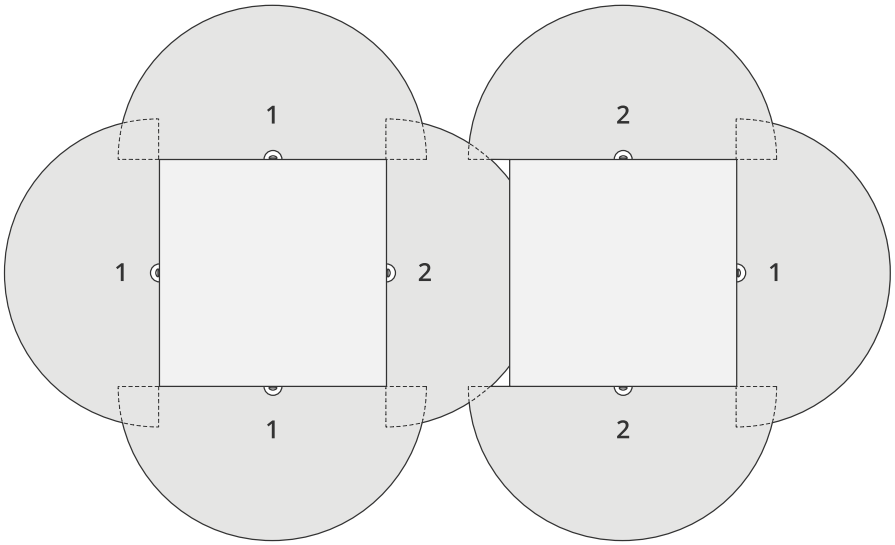
Coprire un'area intorno a un edificio

Per coprire l'area intorno a un edificio, posizionare i radar sulle pareti dell'edificio rivolti verso l'esterno. Se posizioni oltre tre radar nella stessa zona di coesistenza, imposta il numero di radar vicini nell'interfaccia dei dispositivi e aggiungi ogni radar ad un gruppo, come illustra questo esempio.



Puoi anche coprire l'area intorno a molteplici edifici.

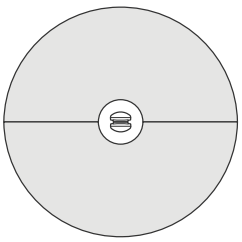
Profilo di monitoraggio dell'area

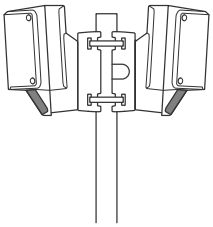


Vedi *Installazione di più radar alla pagina 5* per maggiori informazioni sui radar e sui gruppi vicini.

Coprire un'area aperta

Per coprire un'ampia area aperta, utilizzare due supporti per il montaggio su palo per posizionare due radar in modo che siano rivolti in direzioni opposte.





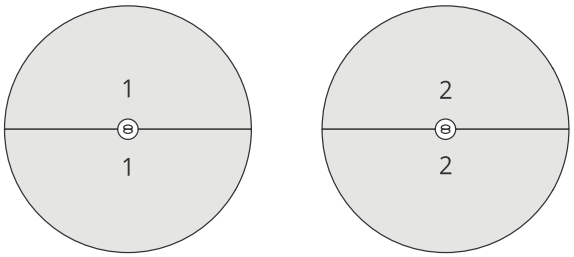
È possibile utilizzare l'uscita PoE da un radar per alimentare il secondo radar, ma non è possibile collegare un terzo radar in questo modo.

Nota

L'uscita PoE sul radar è abilitata quando il radar è alimentato da un midspan da 60 W.

Se servono molte installazioni back-to-back nella stessa zona di coesistenza, imposta il numero di radar vicini nell'interfaccia del dispositivo e aggiungi ogni radar ad un gruppo per evitare interferenze. Questo è un esempio di come si raggruppano i radar in un'installazione back-to-back.

Profilo di monitoraggio dell'area



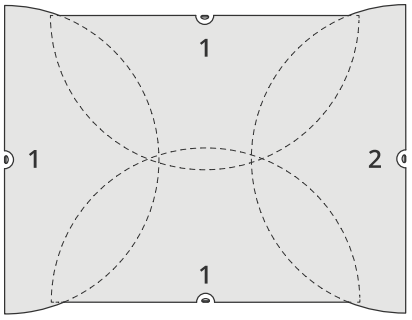
Vedi *Installazione di più radar alla pagina 5* per maggiori informazioni sui radar e sui gruppi vicini.

Installa molteplici radar l'uno di fronte all'altro

Generalmente sconsigliamo l'installazione di oltre tre radar l'uno di fronte all'altro, perché questo incrementa il rischio di interferenze tra i radar. Ciononostante, in certe aree specifiche può rendersi necessario. Ad esempio, se vuoi la copertura di un campo da calcio, non puoi posizionare i radar al centro del campo.

Se installi oltre tre radar l'uno di fronte all'altro, la distanza minima da un radar a un altro deve corrispondere a 40 metri. Per di più, è particolarmente importante l'impostazione del numero di radar vicini nell'interfaccia del dispositivo e l'aggiunta di ogni radar ad un gruppo. Ciò aiuta a migliorare le prestazioni dei radar.

Questo esempio illustra come si raggruppano quattro radar che coprono un campo.



Vedi *Installazione di più radar alla pagina 5* per maggiori informazioni sui radar e sui gruppi vicini.

Intervallo di rilevamento area

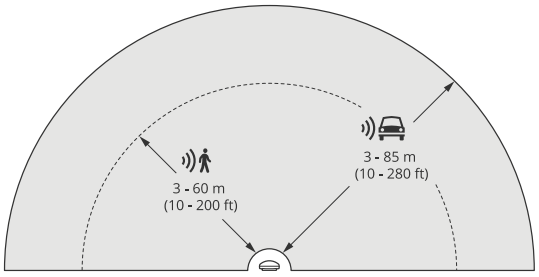
L'intervallo di rilevamento è la distanza entro la quale un oggetto può essere monitorato e può attivare un allarme. Viene misurato a partire da un **limite di rilevamento vicino** (quanto vicino al dispositivo è possibile eseguire un rilevamento) a un **limite di rilevamento lontano** (quanto lontano dal dispositivo è possibile eseguire un rilevamento).

Il **profilo di monitoraggio dell'area** è ottimizzato per il rilevamento di esseri umani, tuttavia, consentirà inoltre di rilevare veicoli e altri oggetti in movimento fino a 55 km/h con un'accuratezza di velocità di +/- 2 km/h (1.24 mph).

Se montato a un'altezza di installazione ottimale, gli intervalli di rilevamento sono:

- **3 – 60 m** per il rilevamento di un essere umano
- **3 – 85 m** per il rilevamento di un veicolo

Profilo di monitoraggio dell'area



Nota

- Se si installare il radar a un'altezza diversa, inserire l'altezza di montaggio effettiva nelle pagine Web del dispositivo quando di calibra il radar.
- L'intervallo di rilevamento è influenzato dalla scena.
- L'intervallo di rilevamento è influenzato dai radar vicini.
- L'intervallo di rilevamento è influenzato dal tipo di oggetto.

La portata di rilevamento è stata misurata in queste condizioni:

- La portata è stata misurata sul suolo.
- L'oggetto era una persona alta 170 cm.
- La persona stava camminando dritta davanti al radar.
- I valori vengono misurati quando la persona entra nella zona di rilevamento.
- La sensibilità del radar è impostata su **Medium (Media)**.

Altezza di montaggio	**Inclinazione 0°**	**Inclinazione 10°**	**Inclinazione 20°**
2,5 m	3–60 m	Non consigliate	Non consigliate
3,5 m	3–60 m	Non consigliate	Non consigliate
4,5 m	4–60 m	Non consigliate	Non consigliate
5,5 m	7,5–60 m	Non consigliate	Non consigliate
6,5 m	7,5–60 m	5,5–60 m	Non consigliate
8 m	Non consigliate	9–60 m	7,5–30 m
10 m	Non consigliate	15–60 m	9–35 m
12 m	Non consigliate	23–60 m	13–38 m
14 m	Non consigliate	27–60 m	17–35 m
16 m	Non consigliate	Non consigliate	25–50 m

Profilo di monitoraggio dell'area

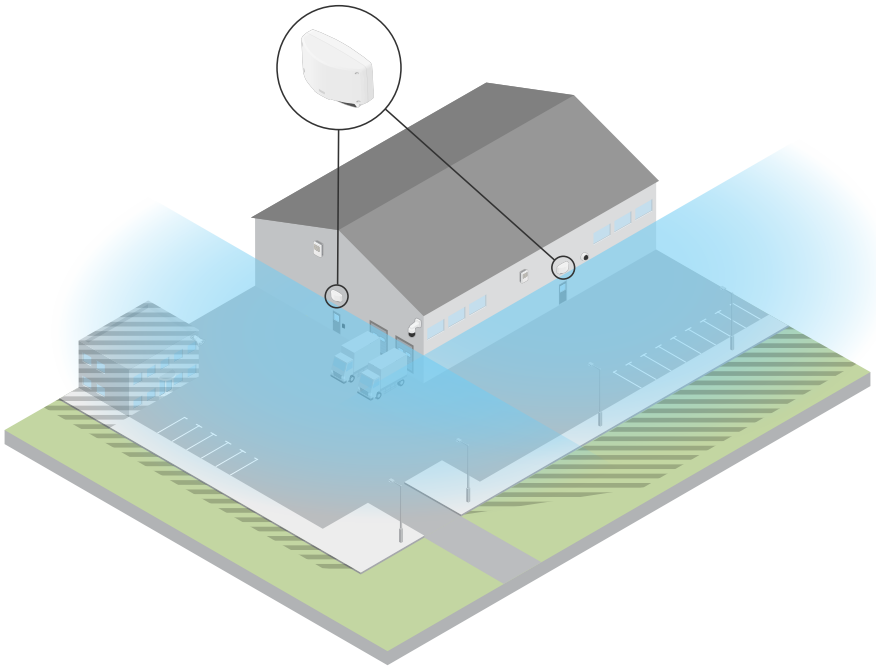
Casi d'uso per il monitoraggio dell'area

Copertura dell'area della piscina

Una piscina pubblica ha subito una serie di intrusioni dopo l'orario di chiusura. A causa della natura privata dell'attività, i proprietari non possono installare la videosorveglianza. Hanno scelto di installare un radar e di configurarlo in **Area monitoring profile (Profilo di monitoraggio dell'area)**. Il radar è montato sull'edificio e copre l'intera piscina e la maggior parte dell'area circostante. Attiva un avviso da un altoparlante quando viene rilevato un essere umano tra l'orario di chiusura alle 20:00 e l'orario di apertura alle 06:00.

Coprire il campo intorno a un edificio

Una fabbrica di sostanze chimiche aggiunge un altro livello di sicurezza al sistema utilizzando i radar per coprire l'area intorno a un edificio sensibile. Il sistema di sicurezza include già telecamere, telecamere termiche e door controller. I radar possono attivare eventi che causano il rilevamento dell'intruso, l'ingrandimento e la registrazione delle attività delle telecamere. I segnali lampeggianti, collegati alle telecamere termiche, vengono attivati per far comprendere all'intruso che l'area è protetta. I door controller possono limitare gli accessi. I radar aiutano il sistema di difesa a entrare in azione molto prima che l'intruso raggiunga l'edificio sensibile.



Coprire un'ampia area aperta

Il parcheggio di un piccolo centro commerciale ha fatto rilevare un maggior numero di effrazioni dopo l'orario di chiusura. C'è un solo vigilante in turno alla volta ma sentono di aver bisogno di ulteriore sicurezza durante la notte senza costi aggiuntivi e senza dover assumere altro personale. Hanno deciso di installare due radar di sicurezza, in **Area monitoring profile (Profilo di monitoraggio dell'area)**, montati back-to-back in modo da coprire l'intera area del parcheggio. I radar sono configurati per avvisare il vigilante in servizio riguardo comportamenti sospetti in modo che possa esaminare la scena. È anche possibile installare un altoparlante a tromba che viene attivato dai radar per riprodurre un allarme in grado di scoraggiare i ladri.

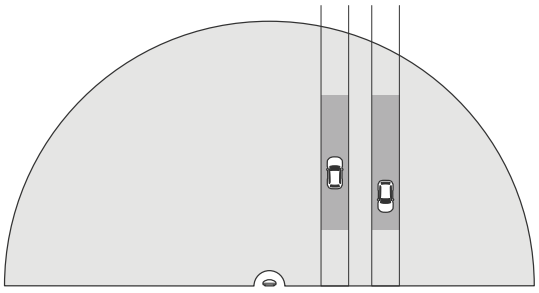
Profilo di monitoraggio della strada

L'opzione **Road monitoring profile (Profilo di monitoraggio della strada)** viene utilizzato al meglio per rilevare i veicoli che si muovono a una velocità massima di 105 km/h nelle aree urbane, nelle zone chiuse e nelle strade suburbane. Questa modalità non deve essere utilizzata per il rilevamento di esseri umani o altri tipi di oggetti. Per tenere traccia di oggetti diversi dai veicoli, utilizzare il radar in *Profilo di monitoraggio dell'area alla pagina 5*.

Esempi di installazione su strada

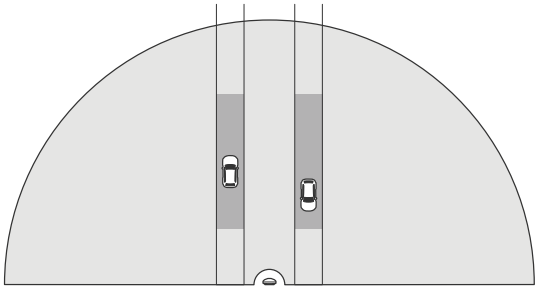
Montaggio laterale

Per monitorare i veicoli su strada è possibile montare il radar sul lato della strada. Il radar fornisce una distanza di copertura laterale di 10 m.



Montaggio al centro

Questa opzione di montaggio necessita di una posizione stabile. Il radar si può montare su un palo al centro della strada o su un ponte sopra la strada. Il radar fornirà poi una distanza di copertura laterale di 10 m su entrambi i lati del radar. Il radar copre una distanza laterale più ampia quando viene montato al centro.



Nota

Si consiglia di montare il radar a un'altezza compresa tra 3 e 8 m per **Road monitoring profile (Profilo di monitoraggio della strada)**.

Intervallo di rilevamento su strada

L'intervallo di rilevamento è la distanza entro la quale un oggetto può essere monitorato e può attivare un allarme. Viene misurato a partire da un **limite di rilevamento vicino** (quanto vicino al dispositivo è possibile eseguire un rilevamento) a un **limite di rilevamento lontano** (quanto lontano dal dispositivo è possibile eseguire un rilevamento).

Profilo di monitoraggio della strada

Questo profilo è ottimizzato per il rilevamento di veicoli e produrrà un'accuratezza di velocità di +/- 2 km/h durante il monitoraggio di veicoli in movimento fino a 105 km/h.

Intervallo di rilevamento quando il radar è montato a un'altezza di installazione ottimale:

- **da 25 a 70 m** per veicoli in movimento a 60 km/h.
- **da 30 a 60 m** per veicoli in movimento a 105 km/h.

Nota

Se il numero massimo di radar nella stessa zona di coesistenza supera due, è possibile che si verifichi una degradazione dell'intervallo di circa il 10% (da vicino) e il 20% (da lontano).

Casi d'uso per il monitoraggio della strada

Controllo della velocità dei veicoli in zone a bassa velocità

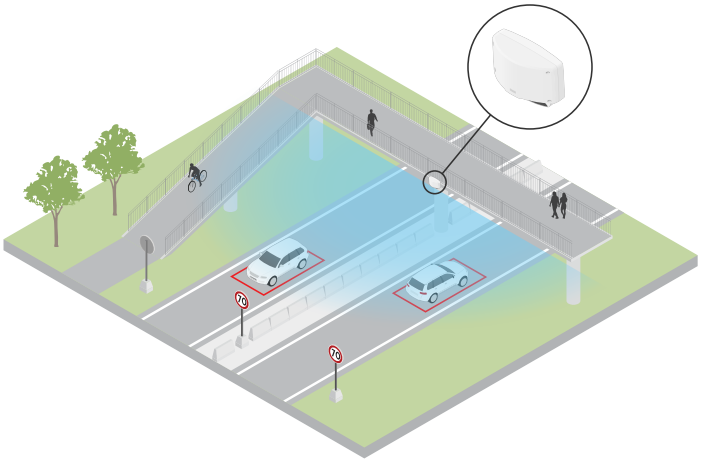
Un impianto industriale con una lunga strada tra due magazzini ha installato un radar per consentire di far rispettare il limite di velocità di 60 km/h. In **Road monitoring profile (Profilo di monitoraggio della strada)**, il radar è in grado di rilevare quando un veicolo nella specifica zona di rilevamento supera tale velocità. Attiva quindi un evento che invia notifiche e-mail ai conducenti e ai manager. Il promemoria consente di aumentare la conformità ai limiti di velocità.

Veicoli indesiderati su strada chiusa

Una piccola strada che porta a un vecchio quartiere è stata chiusa, tuttavia, le segnalazioni di veicoli sulla strada hanno comportato l'installazione di un radar di sicurezza in **Road monitoring profile (Profilo di monitoraggio della strada)**. Il radar è montato lungo la strada e copre l'intera larghezza della stessa. Ogni volta che un veicolo entra nello scenario, attiva un segnale lampeggiante che avverte i conducenti di cambiare strada. Invia, inoltre, un messaggio al personale addetto alla sicurezza in modo che possa eventualmente inviare un'unità.

Consapevolezza della velocità sulla strada

Una strada che passa attraverso un piccolo centro abitato ha fatto riscontrare alcuni incidenti per eccesso di velocità. Per far rispettare il limite di velocità di 70 km/h, il controllo del traffico ha installato un radar di sicurezza, **Road monitoring profile (Profilo di monitoraggio della strada)**, su un ponte che attraversa la strada. In questo modo è possibile rilevare la velocità dei veicoli in circolazione e monitorare quando è necessario inviare unità lungo la strada per controllare il traffico.

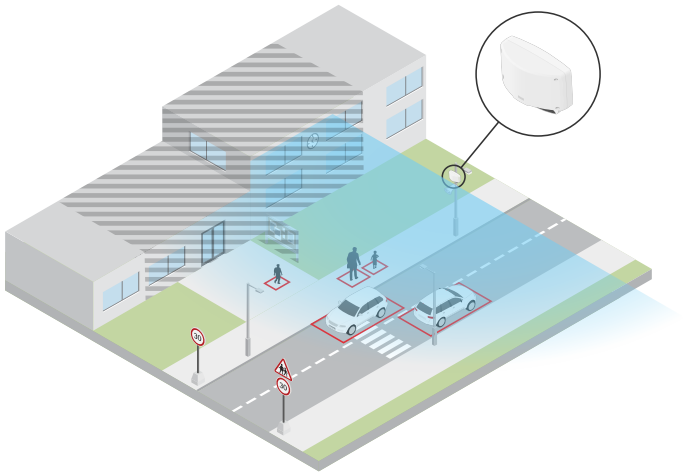


Sicurezza di esseri umani e veicoli

Il personale di una scuola ha identificato due problemi di sicurezza che desidera affrontare. Visitatori indesiderati sono entrati nella struttura durante in giornate scolastiche e alcuni veicoli hanno violato l'area con limite di velocità di 20 km/h all'esterno della scuola. Il radar è montato su un palo, accanto al percorso pedonale. È stato scelto *Profilo di monitoraggio dell'area alla pagina 5* perché

Profilo di monitoraggio della strada

rende il radar in grado di rilevare sia esseri umani che veicoli in movimento a velocità inferiori a 55 km/h. Questo consente al personale di tenere traccia dei visitatori che vanno e vengono durante l'orario scolastico pur essendo in grado di attivare un altoparlante per avvisare i pedoni quando un veicolo si sta avvicinando troppo velocemente.



Introduzione

Individuazione del dispositivo sulla rete

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

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

Supporto browser

Il dispositivo può essere utilizzato con i seguenti browser:

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

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

Aprire l'interfaccia web del dispositivo

1. Aprire un browser e digitare il nome di host o l'indirizzo IP del dispositivo Axis.

   Se non si conosce l'indirizzo IP, utilizzare AXIS IP Utility o AXIS Device Manager per individuare il dispositivo sulla rete.

2. Digitare il nome utente e password. Se si accede al dispositivo per la prima volta, è necessario creare un account amministratore. Vedere *Creare un account amministratore alla pagina 15*.

Creare 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 alla pagina 15*.
3. Reinserire la password.
4. Fare clic su **Add user (Aggiungi utente)**.

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 alla pagina 70*.

Password sicure

Importante

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

Introduzione

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

Per proteggere i tuoi dati ti consigliamo vivamente di:

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

Panoramica dell'interfaccia web

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

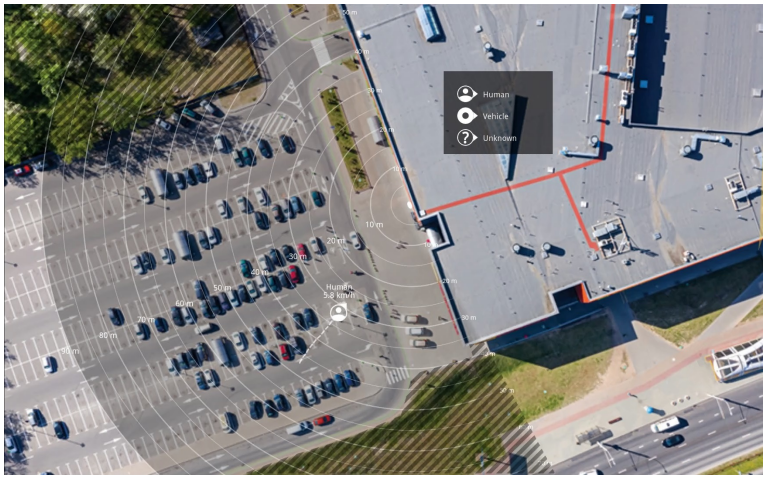
Interfaccia web dei dispositivi Axis

Configurare il dispositivo

Calibrazione del radar

Il radar è pronto ad essere utilizzato appena installato. La visualizzazione in diretta predefinita mostrerà la copertura radar con tutti i movimenti rilevati e sarà possibile aggiungere subito aree di rilevamento e regole.

Se il radar è montato a 3,5 m dal suolo, non è necessario fare altro. Se il radar è montato a un'altezza diversa, è necessario calibrare il radar in modo da compensare l'altezza di montaggio.



Per semplificare la visione degli oggetti in movimento, è possibile caricare una mappa di riferimento, ad esempio una pianta o una foto aerea, che mostra l'area coperta dal radar.

Requisiti dell'immagine:

- I formati dei file supportati sono jpeg e png.
- L'orientamento non è importante poiché l'area di copertura del radar si sposterà per adattarsi all'immagine durante la calibrazione.

Carica una mappa di riferimento

Carica la mappa di riferimento e calibrala in modo che la copertura radar effettiva si adatti alla posizione, alla direzione e alla scala della mappa.

1. Andare a **Radar > Map calibration (Radar > Calibrazione della mappa)**.
2. Carica la mappa di riferimento e segui l'assistente alla configurazione.

Imposta zone di rilevamento

Per determinare dove rilevare il movimento, è possibile aggiungere più zone. È possibile utilizzare diverse zone per attivare azioni diverse.

Esistono due tipi di aree:

- Uno **scenario** (precedentemente detto zona di inclusione) è un'area in cui gli oggetti in movimento attiveranno le regole. Lo scenario predefinito corrisponde all'intera area coperta dal radar.

- Una **exclude zone (zona di esclusione)** è un'area in cui gli oggetti in movimento verranno ignorati. Se all'interno di uno scenario sono presenti aree che attivano molti allarmi indesiderati, utilizzare le aree di esclusione.

Aggiungi scenari

Uno scenario (precedentemente detto zona di inclusione) è un'area in cui gli oggetti in movimento attiveranno le regole. Aggiungi scenari se vuoi la creazione di regole diverse per parti della scena diverse.

Aggiungere uno scenario:

1. Andare a **Radar > Scenarios (Radar > Scenari)**.
2. Fare clic su **Add scenario (Aggiungi scenario)**.
3. Inserire il nome dello scenario.
4. seleziona se vuoi che il trigger siano oggetti che si spostano in un'area o oggetti che attraversano una o due linee.

Attiva in caso di oggetti che si muovono in un'area:

1. Selezionare **Movement in area (Movimento nell'area)**.
2. Fare clic su **Next (Avanti)**.
3. Selezionare il tipo di zona da includere nello scenario.

   Utilizzare il mouse per spostare e dimensionare la zona in modo che copra la parte desiderata dell'immagine radar o della mappa di riferimento.
4. Fare clic su **Next (Avanti)**.
5. Aggiungi impostazioni rilevamento.

   5.1 Aggiungere secondi fino all'attivazione in **Ignore short-lived objects (Ignora oggetti di breve durata)**.

   5.2 Selezionare il tipo di oggetto da attivare in **Trigger on object type (Attiva su tipo di oggetto)**.

   5.3 Aggiungere un intervallo per il limite di velocità in **Speed limit (Limite di velocità)**.
6. Fare clic su **Next (Avanti)**.
7. Impostare la durata minima dell'allarme in **Minimum trigger duration (Durata attivazione minima)**.
8. Fare clic su **Save (Salva)**.

Attivazione causata da oggetti che attraversano una linea:

1. Selezionare **Line crossing (Attraversamento linea)**.
2. Fare clic su **Next (Avanti)**.
3. Posiziona la linea nella scena.

   Utilizzare il mouse per spostare e dare forma alla linea.
4. Per modificare la direzione di rilevamento, attiva **Change direction (Cambia direzione)**.
5. Fare clic su **Next (Avanti)**.
6. Aggiungi impostazioni rilevamento.

   6.1 Aggiungere secondi fino all'attivazione in **Ignore short-lived objects (Ignora oggetti di breve durata)**.

   6.2 Selezionare il tipo di oggetto da attivare in **Trigger on object type (Attiva su tipo di oggetto)**.

   6.3 Aggiungere un intervallo per il limite di velocità in **Speed limit (Limite di velocità)**.

7. Fare clic su **Next (Avanti)**.
8. Impostare la durata minima dell'allarme in **Minimum trigger duration (Durata attivazione minima)**.

   Il valore predefinito è impostato su 2 secondi. Se si desidera che lo scenario si attivi ogni volta che un oggetto attraversa la linea, ridurre la durata a 0 secondi.
9. Fare clic su **Save (Salva)**.

Attivazione causata da oggetti che attraversano due linee:

1. Selezionare **Line crossing (Attraversamento linea)**.
2. Fare clic su **Next (Avanti)**.
3. Per fare in modo che l'oggetto attraversi due linee in modo che l'allarme si accenda, attivare **Require crossing of two lines (Richiedi attraversamento di due linee)**.
4. Posiziona le linee nella scena.

   Utilizzare il mouse per spostare e dare forma alla linea.
5. Per modificare la direzione di rilevamento, attiva **Change direction (Cambia direzione)**.
6. Fare clic su **Next (Avanti)**.
7. Aggiungi impostazioni rilevamento.

   7.1 Impostare il limite di tempo tra l'attraversamento della prima e la seconda linea in **Max time between crossings (Tempo massimo tra gli attraversamenti)**.

   7.2 Selezionare il tipo di oggetto da attivare in **Trigger on object type (Attiva su tipo di oggetto)**.

   7.3 Aggiungere un intervallo per il limite di velocità in **Speed limit (Limite di velocità)**.
8. Fare clic su **Next (Avanti)**.
9. Impostare la durata minima dell'allarme in **Minimum trigger duration (Durata attivazione minima)**.

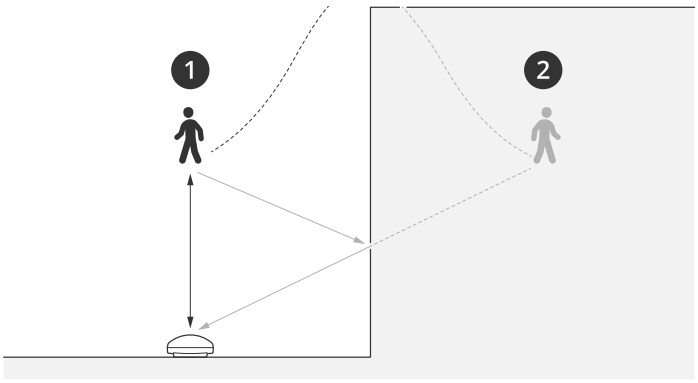
   Il valore predefinito è impostato su 2 secondi. Se si desidera che lo scenario si attivi ogni volta che un oggetto ha attraversato le due linee, ridurre la durata a 0 secondi.
10. Fare clic su **Save (Salva)**.

Aggiungi zone di esclusione

Le zone di esclusione sono aree in cui gli oggetti in movimento verranno ignorati. Aggiungi zone di esclusione per ignorare aree dove sono presenti oggetti in movimento in grado di causare falsi allarmi.

Esempio:

Gli oggetti in materiali radar-riflettenti, come i tetti in metallo, le recinzioni, i veicoli e persino i muri di mattoni, possono interferire con le prestazioni del radar. Possono creare riflessi o ghost track che causano apparenti rilevamenti che possono essere difficili da distinguere dai rilevamenti reali.



1 Rilevamento reale
2 Rilevamento da riflesso

Aggiungere una zona di esclusione:

1. Andare a **Radar > Exclude zones (Radar > Zone di esclusione)**.
2. Fai clic su **Add exclude zone (Aggiungi zona di esclusione)**.

   Utilizzare il mouse per spostare e dimensionare la zona in modo che copra la parte desiderata dell'immagine radar o della mappa di riferimento.

Nota

Dalla versione firmware 11.4, non ci sono più limiti sulla quantità di zone di esclusione.

Ridurre al minimo i falsi allarmi

Se si nota di ricevere troppi falsi allarmi, è possibile filtrare determinati tipi di movimento o oggetti, modificare la copertura oppure regolare la sensibilità di rilevamento. Verifica quali impostazioni sono le più adatte al tuo ambiente.

- Regola la sensibilità di rilevamento del radar:

  Andare a **Radar > Settings > Detection (Radar > Impostazioni > Rilevamento)** e selezionare una **Detection sensitivity (Sensibilità di rilevamento)** più bassa. Ciò diminuisce il rischio di falsi allarmi, ma fa anche sì che il radar possa perdere qualche movimento.

  L'impostazione della sensibilità influisce su tutte le zone.

  - **Low (Bassa)**: utilizzare questa sensibilità quando ci sono molti oggetti metallici o veicoli di grandi dimensioni nell'area. Il radar richiederà più tempo per tracciare e classificare gli oggetti. In questo modo è possibile ridurre l'intervallo di rilevamento, specialmente per gli oggetti in rapido movimento.
  - **Medium (Medio)**: Questa è l'impostazione predefinita.
  - **High (Alto)**: utilizzare questa sensibilità quando si ha un campo aperto senza oggetti metallici davanti al radar. Ciò aumenterà l'intervallo di rilevamento per gli esseri umani.

- Modifica gli scenari e le zone di esclusione:

  se uno scenario include superfici dure, ad esempio una parete metallica, potrebbero esserci riflessi che causano più rilevamenti per un singolo oggetto fisico. È possibile modificare la forma dello scenario o aggiungere una zona di esclusione che ignora alcune parti dello scenario. Per ulteriori informazioni, consultare *Aggiungi scenari alla pagina 18* e *Aggiungi zone di esclusione alla pagina 19*.

- Attivazione su oggetti che attraversano due linee anziché su una:

Se uno scenario che attraversa una linea include, oggetti ondulanti o animali che si muovono, esiste il rischio che un oggetto attraversi la linea e attivi un falso allarme. In questo caso, è possibile configurare lo scenario in modo da attivarsi solo quando un oggetto ha attraversato due linee. Per ulteriori informazioni, consultare *Aggiungi scenari alla pagina 18*.

- Filtro in movimento:
  - Andare in **Radar > Settings > Detection (Radar > Impostazioni > Rilevamento)** e selezionare **Ignore swaying objects (Ignora oggetti ondulanti)**. questa impostazione riduce al minimo i falsi allarmi causati da alberi, cespugli e pennoni nella zona di rilevamento.
  - Andare a **Radar > Settings > Detection (Radar > Impostazioni > Rilevamento)** e selezionare **Ignore small objects (Ignora oggetti piccoli)**. Questa impostazione è disponibile nel profilo di monitoraggio dell'area e riduce al minimo i falsi allarmi di piccoli oggetti presenti nella zona di rilevamento, ad esempio gatti e conigli.
- Filtrare in tempo:
  - Andare a **Radar > Scenarios (Radar > Scenari)**.
  - Selezionare uno scenario e fare clic su ⋮ per modificarne le impostazioni.
  - Selezionare un valore più elevato in **Seconds until trigger (Secondi fino all'attivazione)**. Questo è il periodo di ritardo da quando il radar avvia il rilevamento di un oggetto a quando può attivare un allarme. Il timer si avvia quando il radar rileva per la prima volta l'oggetto, non quando l'oggetto entra nella zona specificata nello scenario.
- Filtra per tipo di oggetto.
  - Andare a **Radar > Scenarios (Radar > Scenari)**.
  - Selezionare uno scenario e fare clic su ⋮ per modificarne le impostazioni.
  - Per evitare di attivarlo su tipi di oggetti specifici, deselezionare i tipi di oggetto che non possono attivare eventi nello scenario.

Visualizzare e registrare video

Questa sezione include istruzioni sulla configurazione del dispositivo. Per ulteriori informazioni sul funzionamento dello streaming e dello storage, vedere *Streaming e archiviazione alla pagina 62*.

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 **Radar > Stream (Radar > Flusso)**.
2. Nella visualizzazione in diretta, fare clic su ⚙.
3. Selezionare **Video format (formato video) H.264**.
4. Andare a **Radar > Stream > General (Radar > Flusso > Generale)** e aumentare la **Compression (Compressione)**.

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 la 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 **Add (Aggiungi)**.

Registrare e guardare video

Registrazione di video direttamente dalla radar

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

   Se non è stato impostato alcun dispositivo di archiviazione, fare clic su e . Per istruzioni sull'impostazione dell'archiviazione di rete, vedere *Configurazione dell'archiviazione di rete alla pagina 22*
3. Fare di nuovo clic su per arrestare la registrazione.

Visualizzazione del video

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

Imposta regole per eventi

Consulta la nostra guida *Introduzione alle regole per gli eventi* per ottenere maggiori informazioni.

Attivazione di un'azione

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

Nota

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

Attivazione di un allarme se qualcuno apre l'alloggiamento

In questo esempio viene spiegato come attivare un allarme se qualcuno apre l'alloggiamento.

Add a recipient (Aggiungi un destinatario):

1. Andare a **System > Events > Recipients (Sistema > Eventi > Destinatari)** e fare clic su **Add recipient (Aggiungi destinatari)**.
2. Immettere un nome per il destinatario.
3. Seleziona **Email**.
4. Immettere un indirizzo e-mail a cui inviare l'e-mail.
5. La telecamera non ha un proprio server e-mail, quindi dovrà accedere a un altro server e-mail per essere in grado di inviare e-mail. Compila il resto delle informazioni sulla base del tuo provider e-mail.
6. Fare clic su **Test (Test)** per inviare un'e-mail di prova.
7. Fare clic su **Save (Salva)**.

Creare una regola:

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

Registra dei video da una telecamera quando viene rilevato movimento

In questo esempio viene illustrato come configurare il radar e una telecamera in modo che questa inizi a registrare sulla scheda di memoria cinque secondi prima che il radar rilevi il movimento e si fermi dopo un minuto.

Collegare i dispositivi:

1. Collegare un cavo da un'uscita I/O sul radar a un ingresso I/O della telecamera.

Configurare la porta I/O del radar:

2. Andare a **System > Accessories > I/O ports (Sistema > Accessori > Porte I/O)** e configurare la porta I/O come output e selezionare lo stato normale.

Creare una regola nel radar:

3. Andare a **System > Events (Sistema > Eventi)** e aggiungere una regola.
4. Inserire un nome per la regola.
5. Dall'elenco delle condizioni, selezionare uno scenario in **Radar motion (Movimento radar)**.

Per l'impostazione di uno scenario, consultare *Aggiungi scenari alla pagina 18*.

6. Dall'elenco delle azioni, selezionare **Toggle I/O while the rule is active (Attiva/disattiva l'I/O mentre la regola è attiva)**, quindi selezionare la porta collegata alla telecamera.
7. Fare clic su **Save (Salva)**.

Configurare la porta I/O della telecamera:

8. Andare a **System > Accessories > I/O ports (Sistema > Accessori > Porte I/O)** e configurare la porta I/O come input e selezionare lo stato normale.

Creare una regola nella telecamera:

9. Andare a **System > Events (Sistema > Eventi)** e aggiungere una regola.
10. Inserire un nome per la regola.
11. Dall'elenco delle condizioni, selezionare **Digital input is active (Input digitale è attivo)**, quindi selezionare la porta che deve attivare la regola.
12. Dall'elenco delle azioni, selezionare **Record video (Registra video)**.
13. Selezionare **SD card (scheda di memoria)** dall'elenco delle opzioni di archiviazione.
14. Selezionare un profilo di streaming esistente o crearne uno nuovo.
15. Impostare il tempo pre-buffer su 5 secondi.
16. Imposta il post-buffer su 1 minuto.
17. Fare clic su **Save (Salva)**.

Attivare una luce quando viene rilevato movimento

Accendere una luce quando un intruso entra nella zona di rilevamento può avere un effetto dissuasivo e migliorerà anche la qualità di immagine di una telecamera visiva che registra l'intrusione.

In questo esempio viene illustrato come configurare il radar e un illuminatore in modo che l'illuminatore si accenda quando il radar rileva il movimento e si spegne dopo un minuto.

Collegare i dispositivi:

1. Collegare uno dei cavi dell'illuminatore all'alimentatore tramite la porta relè del radar. Collegare l'altro cavo direttamente tra l'alimentatore e l'illuminatore.

Configurare la porta relè del radar:

2. Andare a **System > Accessories > I/O ports (Sistema > Accessori > Porte I/O)** e selezionare **Open circuit (Circuito aperto)** come stato normale della porta relè.

Creare una regola nel radar:

3. Andare a **System > Events (Sistema > Eventi)** e aggiungere una regola.
4. Inserire un nome per la regola.
5. Dall'elenco delle condizioni, selezionare uno scenario in **Radar motion (Movimento radar)**.

   Per l'impostazione di uno scenario, consultare *Aggiungi scenari alla pagina 18*.
6. Dall'elenco delle azioni, selezionare **Toggle I/O once (Attiva/disattiva I/O una volta)** e quindi selezionare la porta relè.
7. Selezionare **Active (Attivo)**.

8. Impostare la **Duration (Durata)**.
9. Fare clic su **Save (Salva)**.

Controllo di una telecamera PTZ con il radar

È possibile utilizzare le informazioni relative alle posizioni degli oggetti dal radar per far sì che la telecamera PTZ tracci gli oggetti. Ci sono due modi per effettuare questa operazione:

- *Controlla una telecamera PTZ con il servizio di tracking automatico del radar integrato alla pagina 25*. L'opzione integrata è adatta quando si dispone di una telecamera PTZ e di un radar montati molto vicini tra loro.
- *Controlla una telecamera PTZ con AXIS Radar Autotracking for PTZ alla pagina 26*. L'applicazione Windows è adatta quando si desidera utilizzare più telecamere PTZ e radar per tracciare oggetti.

Nota

Usa un server NTP per la sincronizzazione dell'ora sulle telecamere, sui radar e sul computer Windows. Nel caso gli orologi non siano sincronizzati, potrebbero verificarsi ritardi nel tracking, oppure ghost tracking.

Controlla una telecamera PTZ con il servizio di tracking automatico del radar integrato

Il tracking automatico del radar integrato crea una soluzione edge-to-edge in cui il radar controlla direttamente la telecamera PTZ. Supporta tutte le telecamere PTZ Axis.

Queste istruzioni spiegano come associare una telecamera PTZ al radar, come calibrarle e come impostare il tracking degli oggetti.

Nota

È possibile utilizzare il servizio di tracking automatico del radar integrato per collegare un radar a una telecamera PTZ. Per una configurazione in cui desideri utilizzare più di un radar o telecamera PTZ, utilizza AXIS Radar Autotracking for PTZ. Per ulteriori informazioni, consultare *Controlla una telecamera PTZ con AXIS Radar Autotracking for PTZ alla pagina 26*.

Associare il radar alla telecamera PTZ:

1. Andare a **System > Edge-to-edge > PTZ Pairing (Sistema > Edge-to-edge > Associazione PTZ)**.
2. Inserire l'indirizzo IP, il nome utente e password della telecamera PTZ.
3. Fare clic su **Connect (Connetti)**.
4. Fai clic su **Configure Radar autotracking (Configura tracking automatico del radar)** o vai a **Radar > Autotracking (Radar > Tracking automatico)** per impostare il tracking automatico del radar.

Calibrare il radar e la telecamera PTZ:

5. Andare a **Radar > Autotracking (Radar > Tracking automatico)**.
6. Per impostare l'altezza di montaggio della telecamera, vai a **Camera mounting height (Altezza di montaggio della telecamera)**.
7. Per eseguire la panoramica della telecamera PTZ in modo che punti nella stessa direzione del radar, vai a **Pan alignment (Allineamento panoramica)**.
8. Se devi regolare l'inclinazione per compensare un terreno in pendenza, vai a **Ground incline offset (Offset inclinazione del terreno)** e aggiungi un offset in gradi.

Imposta il tracking PTZ:

9. Vai a **Track (Rilevamento)** per selezionare questa opzione per seguire persone, veicoli e/o oggetti sconosciuti.
10. Per avviare il rilevamento di oggetti con la telecamera PTZ, attivare l'opzione **Tracking (Rilevamento)**.

    Il rilevamento ingrandisce automaticamente un oggetto o un gruppo di oggetti al fine di mantenerli nella vista della telecamera.

11. Attiva **Object switching (Cambio oggetto)** se prevedi che più oggetti non si adattino alla visualizzazione della telecamera.

    Con questa impostazione il radar dà la priorità agli oggetti da rilevare.

12. Per determinare quanti secondi tenere traccia di ciascun oggetto, impostare **Object hold time (Tempo di attesa oggetto)**.

13. Per riportare la telecamera PTZ alla relativa posizione iniziale quando il radar non rileva più alcun oggetto, attivare **Return to home (Ritorna alla posizione iniziale**.

14. Per determinare quanto tempo la telecamera deve rimanere sull'ultima posizione nota degli oggetti rilevati prima di tornare alla posizione iniziale, impostare **Return to home timeout (Timeout ritorno alla posizione iniziale)**.

15. Per ottimizzare lo zoom della telecamera PTZ, regolarlo sul dispositivo di scorrimento.

Controlla una telecamera PTZ con AXIS Radar Autotracking for PTZ

AXIS Radar Autotracking for PTZ è una soluzione basata su server in grado di gestire diverse configurazioni durante il tracciamento degli oggetti:

- Controllo di più telecamere PTZ con un solo radar.
- Controllo di una telecamera PTZ con più radar.
- Controllo di più telecamere PTZ con più radar.
- Controllo di una telecamera PTZ con un radar quando sono montati in posizioni diverse che coprono la stessa area.

L'applicazione è compatibile con un set specifico di telecamere PTZ. Per ulteriori informazioni, vedere *axis.com/products/axis-radar-autotracking-for-ptz#compatible-products*.

Scarica l'applicazione e consulta il manuale dell'utente per informazioni su come configurare l'applicazione. Per ulteriori informazioni, vedere *axis.com/products/axis-radar-autotracking-for-ptz/support*.

Interfaccia web

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

Nota

Il supporto per le funzionalità e le impostazioni descritte in questa sezione varia da un dispositivo all'altro. Questa icona indica che la funzione o l'impostazione è disponibile solo in certi dispositivi.

Mostra o nascondi il menu principale.

Accedere alle note di rilascio.

Accedere alla guida dispositivo.

Modificare la lingua.

Imposta il tema chiaro o il tema scuro.

Il menu contestuale contiene:

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

Il menu contestuale contiene:

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

Stato

Stato sincronizzazione ora

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

NTP settings (Impostazioni NTP): visualizza e aggiorna le impostazioni NTP. Porta l'utente alla pagina **Date and time (Data e ora)** dove è possibile modificare le impostazioni NTP.

Registrazioni in corso

Mostra le registrazioni in corso e il relativo spazio di archiviazione designato.

Recordings (Registrazioni): Consente di visualizzare le registrazioni in corso e quelle filtrate oltre alla relativa origine. Per ulteriori informazioni, vedere *Registrazioni alla pagina 34*

Mostra lo spazio di archiviazione in cui è stata salvata la registrazione.

Informazioni dispositivo

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

Upgrade firmware (Aggiorna il firmware): aggiorna il firmware sul dispositivo. Porta l'utente sulla pagina Manutenzione dove è possibile aggiornare il firmware.

Connected clients (Client collegati)

Mostra il numero di connessioni e client connessi.

View details (Visualizza dettagli): Consente di visualizzare e aggiornare l'elenco dei client connessi. L'elenco mostra l'indirizzo IP, il protocollo, la porta e il PID/processo di ogni client.

Radar

Impostazioni

Generale

Radar transmission (Trasmissione radar): usa questa opzione per lo spegnimento completo del modulo del radar.

Channel (Canale) : se avvengono problemi con molteplici dispositivi che interferiscono l'uno con l'altro, seleziona lo stesso canale per un massimo di quattro dispositivi vicini l'uno all'altro. Per la maggior parte delle installazioni, seleziona **Auto (Automatico)** per permettere ai dispositivi di negoziare in automatico quale canale usare.

Mounting height (Altezza di montaggio): inserisci l'altezza di montaggio per il dispositivo.

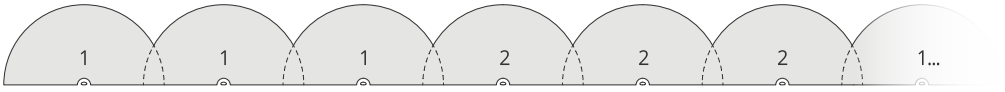
Nota

Nell'inserire l'altezza di montaggio, usa la massima specificità possibile. Ciò aiuta il dispositivo a visualizzare il rilevamento radar nella posizione giusta nell'immagine.

Coexistence (Coesistenza)

Number of neighboring radars (Numero di radar vicini): Seleziona il numero di radar vicini montati all'interno della stessa zona di coesistenza. Ciò contribuirà ad evitare le interferenze. Il raggio di coesistenza corrisponde a 350 m.

- **0–1**: Seleziona questa opzione se monti uno o due radar nella stessa zona di coesistenza.
- **2**: Seleziona questa opzione se monti tre radar nella stessa zona di coesistenza.
- **3–5**: Seleziona questa opzione se monti fra i quattro e i sei radar nella stessa zona di coesistenza.
  - **Groups (Gruppi)**: Seleziona un gruppo (**Group 1 (Gruppo 1)** o **Group 2 (Gruppo 2)**) per il tuo radar. Anche questo contribuirà ad evitare le interferenze. Consigliamo l'aggiunta di tre radar ad ogni gruppo e l'aggiunta dei radar più vicini l'uno all'altro allo stesso gruppo.



Per ulteriori informazioni, consultare *Installazione di più radar alla pagina 5* .

Rilevamento

Detection sensitivity (Sensibilità del rilevamento): seleziona quale dovrebbe essere il livello di sensibilità del radar. Un valore più elevato vuol dire che avrai un intervallo di rilevamento maggiore, ma c'è anche un rischio più elevato di falsi allarmi. Una sensibilità più bassa eliminerà i falsi allarmi, ma può rendere più breve l'intervallo di rilevamento.

Radar profile (Profilo radar): Selezionare un profilo più adatto all'area di interesse.

- **Area monitoring (Monitoraggio area)**: traccia gli oggetti grandi e piccoli che si muovono a velocità inferiori in aree aperte.
  - **Ignore swaying objects (Ignora oggetti ondulanti)**: attivare per ridurre al minimo i falsi allarmi provenienti da oggetti ondulanti, come alberi, cespugli o pennoni.
  - **Ignore small objects (Ignora oggetti piccoli):** attivare per ridurre al minimo i falsi allarmi provenienti da oggetti di piccole dimensioni, ad esempio gatti o conigli.
- **Road monitoring (Monitoraggio della strada)**: traccia i veicoli che si muovono a velocità maggiore nelle zone urbane e sulle strade sub-urbane
  - **Ignore swaying objects (Ignora oggetti ondulanti)**: attivare per ridurre al minimo i falsi allarmi provenienti da oggetti ondulanti, come alberi, cespugli o pennoni.

View (Vista)

Information legend (Legenda informazioni): Attivare per visualizzare una legenda contenente i tipi di oggetto che il radar può rilevare e seguire. Trascinare e rilasciare per spostare la legenda delle informazioni.

Zone opacity (Opacità zona): seleziona quanto la zona di copertura dovrebbe essere opaca o trasparente.

Grid opacity (Opacità griglia): seleziona quanto la griglia dovrebbe essere opaca o trasparente.

Color scheme (Schema colore): seleziona un tema per la visualizzazione radar.

Rotation (Rotazione) : Selezionare l'orientamento preferito dell'immagine del radar.

Visualizzazione oggetto

Trail lifetime (Durata traccia): Selezionare per quanto tempo la traccia di un oggetto tracciato è visibile nella vista radar.

Icon style (Stile icona): Selezionare lo stile dell'icona degli oggetti tracciati nella vista radar. Per un testo normale, selezionare **Triangle (Triangolo)**. Per simboli rappresentati, selezionare **Symbol (Simbolo)**. Le icone puntano nella direzione in cui si muovono gli oggetti tracciati, indipendentemente dal tipo di movimento.

Show information with icon (Mostra informazioni con icona): Selezionare le informazioni da mostrare accanto all'icona dell'oggetto tracciato:

- **Object type (Tipo di oggetto)**: Mostra il tipo di oggetto che il radar ha rilevato.
- **Classification probability (Probabilità di classificazione)**: Mostra quanto il radar è sicuro che la classificazione degli oggetti sia esatta.
- **Velocity (Velocità)**: Mostra la velocità con cui l'oggetto si muove.

Zone di esclusione

Un'**exclude zone (zona di esclusione)** è un'area in cui gli oggetti in movimento sono ignorati. Se all'interno di uno scenario sono presenti aree che attivano molti allarmi indesiderati, utilizzare le aree di esclusione.

+ : Fai clic per creare una nuova zona di esclusione.

Per la modifica di una zona di esclusione, selezionala nell'elenco.

Selezionare uno dei **Zone shape presets (Preset di forma zona)** per la zona di esclusione. **Cover everything (Copri tutto)** imposta come zona tutta l'area di copertura del radar. **Reset to box (Reimposta alla casella)** crea un rettangolo nel mezzo dell'area di copertura.

Per la modifica della zona, trascina e rilascia uno qualsiasi dei punti sulle linee. Per rimuovere un punto, fare clic con il pulsante destro del mouse su di esso.

Scenari

Uno scenario è una combinazione di condizioni trigger nonché di impostazioni di scena e di rilevamento.

+ : Fai clic per creare un nuovo scenario. È possibile creare fino a 20 scenari.

Triggering conditions (Condizioni trigger): Selezionare la condizione che attiva gli allarmi.

- **Movement in area (Movimento nell'area)**: seleziona se vuoi che lo scenario si attivi su oggetti che si spostano in un'area.
- **Attraversamento linea**: seleziona questa opzione se si desidera che lo scenario si attivi su oggetti che attraversano una o due linee.

Scene (Scena): definire l'area o le linee nello scenario in cui gli oggetti in movimento attiveranno gli allarmi.

- Per **Movement in area (Movimento nell'area)**, selezionare il preset di forma per modificare l'area.
- Per **Line crossing (attraversamento linea)**, trascinare e rilasciare la linea nella scena. Per la creazione di molteplici punti sulla linea, fare clic e trascina in una qualsiasi parte della linea. Per rimuovere un punto, fare clic con il pulsante destro del mouse su di esso.
  - **Require crossing of two lines (Richiedi attraversamento di due linee)**: Attivare se l'oggetto deve passare due linee prima che lo scenario accenda un allarme.
  - **Change direction (Cambia orientamento):** Attivare se si desidera che lo scenario attivi un allarme quando oggetti attraversano la linea nell'altra direzione.

Detection settings (Impostazioni rilevamento): Definisci i criteri di trigger per lo scenario.

- Per **Movement in area (Movimento in area)**:
  - **Ignore short-lived objects (Ignora movimenti di breve durata)**: Impostare l'intervallo di tempo in secondi da quando il radar rileva l'oggetto a quando lo scenario attiva un allarme. In questo modo è possibile ridurre i falsi allarmi.
  - **Trigger on object type (Attiva su tipo di oggetto)**: Selezionare il tipo di oggetti (umani, veicoli, sconosciuti) su cui si desidera attivare lo scenario.
  - **Speed limit (Limite velocità)**: Si attiva quando oggetti si muovono a velocità all'interno di un intervallo specifico.
  - **Invert (Inverti)**: Selezionare questa opzione se si desidera attivare velocità superiori e inferiori al limite di velocità impostato.
- Per **Line crossing (Attraversamento linea)**:
  - **Ignore short-lived objects (Ignora movimenti di breve durata)**: Impostare l'intervallo di tempo in secondi da quando il radar rileva l'oggetto a quando lo scenario attiva un'azione. In questo modo è possibile ridurre i falsi allarmi. Questa opzione non è disponibile per gli oggetti che attraversano due linee.
  - **Max time between crossings (Tempo massimo tra attraversamenti)**: Impostare il tempo massimo tra l'attraversamento della prima e la seconda linea. Questa opzione è disponibile solo per gli oggetti che attraversano due linee.
  - **Trigger on object type (Attiva su tipo di oggetto)**: Selezionare il tipo di oggetti (umani, veicoli, sconosciuti) su cui si desidera attivare lo scenario.
  - **Speed limit (Limite velocità)**: Si attiva quando oggetti si muovono a velocità all'interno di un intervallo specifico.
  - **Invert (Inverti)**: Selezionare questa opzione se si desidera attivare velocità superiori e inferiori al limite di velocità impostato.

Alarm settings (Impostazioni allarme): Definire i criteri per l'allarme.

- **Minimum trigger duration (Durata attivazione minima)**: Impostare la durata minima per l'allarme attivato.

Calibrazione mappa

Usa la calibrazione della mappa per il caricamento e la calibrazione di una mappa di riferimento. Ciò renderà più facile capire dove si muovono gli oggetti nell'area coperta dal radar.

Upload map (Carica mappa): seleziona la mappa di riferimento che vuoi caricare.

Set radar position on map (Imposta posizione radar sulla mappa): specifica la posizione del radar sulla mappa, aggiungi un punto di riferimento direttamente davanti al radar e digita la distanza tra il radar e il punto di riferimento. Fai clic su **Calibrate (Calibra)** per avviare la calibrazione.

Il risultato della calibrazione è una mappa di riferimento che mostra la copertura del radar nella scala appropriata.

Flusso

General (Caratteristiche generali)

Resolution (Risoluzione): Selezionare la risoluzione dell'immagine adatta per la scena di sorveglianza. Una risoluzione più elevata necessita di più larghezza di banda e spazio di archiviazione.

Frame rate (Velocità in fotogrammi): Per evitare problemi di larghezza di banda nella rete o ridurre le dimensioni di archiviazione, puoi limitare la velocità in fotogrammi a una quantità fissa di fotogrammi. Se la velocità in fotogrammi è zero, il valore viene impostato sul valore massimo possibile nelle condizioni correnti. Una velocità in fotogrammi più elevata necessita di larghezza di banda e spazio di archiviazione maggiori.

Compression (Compressione): Utilizzare il cursore per regolare la compressione d'immagine. Un'elevata compressione si traduce in velocità di trasmissione e qualità dell'immagine inferiori. Una compressione bassa migliora la qualità dell'immagine ma utilizza larghezza di banda e spazio di archiviazione maggiori durante la registrazione.

Signed video (Video firmato)  : Attivare per aggiungere la funzione video firmata al video. Il video firmato protegge il video dalle manomissioni aggiungendo firme crittografiche al video.

Zipstream

P-frames (P-frame): Un P-frame è un'immagine predetta che mostra solo le modifiche nell'immagine rispetto al fotogramma precedente. Immetti il numero desiderato di P-frame. Più è alto il numero, minore è la larghezza di banda necessaria. Tuttavia, se è presente una congestione di rete, potrebbe verificarsi un deterioramento della qualità video.

Bitrate control (Controllo velocità in bit)

- **Average (Media)**: Selezionare per la regolazione automatica della velocità in bit per un periodo di tempo più lungo e la migliore qualità di immagine possibile sulla base dell'archiviazione a disposizione.
  -  Fare clic per il calcolo della velocità in bit di destinazione sulla base dell'archiviazione disponibile, del tempo di conservazione e del limite della velocità in bit.
  - **Target bitrate (Velocità in bit di destinazione)**: Immetti la velocità in bit di destinazione voluta.
  - **Retention time (Tempo di conservazione)**: Immetti il numero di giorni per la conservazione delle registrazioni.
  - **Storage (Archiviazione)**: mostra lo spazio di archiviazione stimato che può essere utilizzato per il flusso.
  - **Maximum bitrate (Velocità di trasmissione massima)**: Attiva per l'impostazione di un limite di velocità in bit.
  - **Bitrate limit (Limite velocità in bit)**: Immettere un limite per la velocità in bit che sia maggiore rispetto alla velocità in bit di destinazione.
- **Maximum (Massimo)**: selezionare per impostare una velocità di trasmissione massima istantanea del flusso in base alla larghezza di banda di rete.
  - **Maximum (Massimo)**: Immetti la velocità in bit massima.
- **Variable (Variabile)**: Seleziona per permettere che la velocità in bit vari sulla base del livello di attività nella scena. Un'attività maggiore necessita di più larghezza di banda. Raccomandiamo questa opzione per la gran parte delle situazioni.

Sovrapposizioni

+ : Fare clic per aggiungere una sovrapposizione. Seleziona il tipo di sovrapposizione dall'elenco a discesa:

- **Text (Testo)**: Seleziona per mostrare un testo integrato nell'immagine della visualizzazione in diretta e visibile in tutte le viste, registrazioni ed istantanee. Puoi inserire un testo personalizzato e comprendere anche modificatori preconfigurati per mostrare in automatico, ad esempio, l'ora, la data e la velocità in fotogrammi.
  - : Fare clic per aggiungere il modificatore della data `%F` per visualizzare il formato aaaa-mm-gg.
  - : fare clic per aggiungere il campo di modifica dell'ora `%X` per visualizzare hh:mm:ss (formato 24 ore).
  - **Modifiers (Campi di modifica)**: Fare clic per selezionare qualsiasi campo di modifica presente nell'elenco per aggiungerlo alla casella di testo. Ad esempio, `%a` mostra il giorno della settimana.
  - **Size (Dimensioni)**: Selezionare le dimensioni font desiderate.
  - **Appearance (Aspetto)**: selezionare il colore del testo e di sfondo, ad esempio, testo bianco su sfondo nero (valore predefinito).
  - : selezionare la posizione di sovrapposizione nell'immagine.
- **Image (Immagine)**: Seleziona per mostrare un'immagine statica sovrimpressa sul flusso video. Puoi usare file .bmp, .png, .jpeg o .svg.
  Per caricare un'immagine, fare clic su **Images (Immagini)**. Prima del caricamento di un'immagine, puoi scegliere di:
  - **Scale with resolution (Scala con risoluzione)**: Seleziona per adattare automaticamente l'immagine grafica sovrapposta alla risoluzione video.
  - **Use transparency (Usa trasparenza)**: Seleziona e inserisci il valore esadecimale RGB per quel colore. Usa il formato RRGGBB. Esempi di valori esadecimali: FFFFFF per bianco, 000000 per nero, FF0000 per rosso, 6633FF per blu e 669900 per verde. Solo per immagini .bmp.
- **Scene annotation (Annotazioni scena)** : Selezionare tale opzione per mostrare una sovrapposizione di testo nel flusso video che rimanga nella stessa posizione, anche nel momento in cui la telecamera esegue la panoramica o l'inclinazione in una direzione diversa. Si può decidere di mostrare la sovrapposizione solo in certi livelli di zoom.
  - : Fare clic per aggiungere il modificatore della data `%F` per visualizzare aaaa-mm-gg.
  - : fare clic per aggiungere il campo di modifica dell'ora `%X` per visualizzare hh:mm:ss (formato 24 ore).
  - **Modifiers (Campi di modifica)**: Fare clic per selezionare qualsiasi campo di modifica presente nell'elenco per aggiungerlo alla casella di testo. Ad esempio, `%a` mostra il giorno della settimana.
  - **Size (Dimensioni)**: Selezionare le dimensioni font desiderate.
  - **Appearance (Aspetto)**: selezionare il colore del testo e di sfondo, ad esempio, testo bianco su sfondo nero (valore predefinito).
  - : selezionare la posizione di sovrapposizione nell'immagine. La sovrapposizione testo è salvata e resta nelle coordinate panoramica e inclinazione di tale ubicazione.
  - **Annotation between zoom levels (%) (Annotazione tra livelli di zoom (%))**: Impostare i livelli di zoom nei quali sarà mostrata la sovrapposizione testo.
  - **Annotation symbol (Simbolo annotazioni)**: Selezionare un simbolo che compare invece della sovrapposizione testo quando la telecamera non è nei livelli di zoom impostati.
- **Streaming indicator (Indicatore di streaming)** : Seleziona per mostrare un'animazione sovrimpressa sul flusso video. Questa animazione indica che il flusso video è in diretta anche se la scena non contiene nessun movimento.
  - **Appearance (Aspetto)**: selezionare il colore dell'animazione e di sfondo, ad esempio, animazione rossa su sfondo trasparente (valore predefinito).
  - **Size (Dimensioni)**: Selezionare le dimensioni font desiderate.
  - : selezionare la posizione di sovrapposizione nell'immagine.
- **Widget: Grafico a linee** : Mostrare un grafico che illustri in che modo un valore misurato cambia nel corso del tempo.
  - **Titolo**: Immettere un titolo per il widget.

  - **Campo di modifica sovrapposizione testo**: Selezionare un campo di modifica di sovrapposizione testo come sorgente dati. Se sono state create delle sovrapposizioni testo MQTT, si troveranno alla fine dell'elenco.
  -  : selezionare la posizione di sovrapposizione nell'immagine.
  - **Size (Dimensioni)**: Selezionare le dimensioni della sovrapposizione testo.
  - **Visibile su tutti i canali**: Disattivare perché appaia solo sul canale correntemente selezionato. Attivare perché appaia su tutti i canali attivi.
  - **Intervallo di aggiornamento**: Selezionare il periodo tra aggiornamenti di dati.
  - **Trasparenza**: Impostare la trasparenza di tutta la sovrapposizione testo.
  - **Trasparenza dello sfondo**: Impostare la trasparenza solamente dello sfondo della sovrapposizione testo.
  - **Punti**: Attivare per eseguire l'aggiunta di un punto alla linea del grafico quando i dati sono aggiornati.
  - **Asse x**
  - **Label (Etichetta)**: Inserire l'etichetta testo per l'asse x.
  - **Intervallo di tempo**: Inserire quanto a lungo i dati saranno visualizzati.
  - **Unità di tempo**: Inserire un'unità di tempo per l'asse x.
  - **Asse y**
  - **Label (Etichetta)**: Inserire l'etichetta testo per l'asse y.
  - **Scala dinamica**: Attivare questa opzione perché la scala si adatti in automatico ai valori dei dati. Disattivare questa opzione per inserire in modo manuale i valori per una scala fissa.
  - **Soglia allarme minima** e **Soglia allarme massima**: Tali valori aggiungeranno linee di riferimento orizzontali al grafico, facendo sì che si possa vedere più facilmente quando il valore dei dati diventa eccessivo o troppo basso.

- **Widget: Contatore**  : Mostrare un grafico a barre che illustra il valore dei dati misurati più di recente.
  - **Titolo**: Immettere un titolo per il widget.
  - **Campo di modifica sovrapposizione testo**: Selezionare un campo di modifica di sovrapposizione testo come sorgente dati. Se sono state create delle sovrapposizioni testo MQTT, si troveranno alla fine dell'elenco.
  -  : selezionare la posizione di sovrapposizione nell'immagine.
  - **Size (Dimensioni)**: Selezionare le dimensioni della sovrapposizione testo.
  - **Visibile su tutti i canali**: Disattivare perché appaia solo sul canale correntemente selezionato. Attivare perché appaia su tutti i canali attivi.
  - **Intervallo di aggiornamento**: Selezionare il periodo tra aggiornamenti di dati.
  - **Trasparenza**: Impostare la trasparenza di tutta la sovrapposizione testo.
  - **Trasparenza dello sfondo**: Impostare la trasparenza solamente dello sfondo della sovrapposizione testo.
  - **Punti**: Attivare per eseguire l'aggiunta di un punto alla linea del grafico quando i dati sono aggiornati.
  - **Asse y**
  - **Label (Etichetta)**: Inserire l'etichetta testo per l'asse y.
  - **Scala dinamica**: Attivare questa opzione perché la scala si adatti in automatico ai valori dei dati. Disattivare questa opzione per inserire in modo manuale i valori per una scala fissa.
  - **Soglia allarme minima** e **Soglia allarme massima**: Tali valori aggiungeranno linee di riferimento orizzontali al grafico a barre, facendo sì che si possa vedere più facilmente quando il valore dei dati diventa eccessivo o troppo basso.

Tracking automatico

Abbinare il radar a una telecamera PTZ per utilizzare il tracking automatico del radar. Per stabilire la connessione, andare a **System > edge-to-edge (Sistema > edge-to-edge)**.

Tracking automatico radar PTZ

Configurazione delle impostazioni generali:

Camera mounting height (Altezza di montaggio della telecamera): la distanza dal suolo all'altezza di montaggio della telecamera PTZ.

Pan alignment (Allineamento panoramica): eseguire un movimento panoramico della telecamera PTZ in modo che punti nella stessa direzione del radar. Fare click sull'indirizzo IP della telecamera PTZ per eseguire l'accesso.

Save pan offset (Salva offset panoramica): fare clic per salvare l'allineamento della panoramica.

Ground incline offset (Offset inclinazione rispetto al suolo): Utilizzare il valore dell'offset inclinazione rispetto al suolo per regolare l'inclinazione della telecamera. Se il terreno è inclinato, o se la telecamera non è montata orizzontalmente, la telecamera potrebbe essere orientata troppo in alto o troppo in basso durante il rilevamento di un oggetto.

Done (Fatto): fare clic per salvare le impostazioni e proseguire con la configurazione.

Configurazione del tracking automatico PTZ:

Track (Traccia): selezionare questa opzione per seguire persone, veicoli e/o oggetti sconosciuti.

Tracking (Rilevamento): attivare per avviare il rilevamento di oggetti con la telecamera PTZ. Il rilevamento ingrandisce automaticamente un oggetto o un gruppo di oggetti al fine di mantenerli nella vista della telecamera.

Object switching (Passaggio da un oggetto all'altro): se il radar rileva più oggetti che non rientreranno nella vista della telecamera PTZ, la telecamera PTZ traccia l'oggetto a cui il radar assegna la priorità più elevata e ignora gli altri oggetti.

Object hold time (Tempo attesa oggetto): determina per quanti secondi la telecamera PTZ deve tracciare ciascun oggetto.

Return to home (Torna alla posizione iniziale): attivare per riportare la telecamera PTZ alla relativa posizione iniziale quando il radar non rileva più alcun oggetto.

Return to home timeout (Timeout torna alla posizione iniziale): determina per quanto tempo la telecamera PTZ deve rimanere sull'ultima posizione nota degli oggetti rilevati prima di tornare alla posizione iniziale.

Zoom (Zoom): usare il cursore per regolare in modo accurato il livello di zoom della telecamera PTZ.

Reconfigure installation (Riconfigura l'installazione): fare clic per cancellare tutte le impostazioni e tornare alla configurazione iniziale.

Registrazioni

Registrazioni in corso: mostra tutte le registrazioni in corso sul dispositivo.

● Avvia una registrazione sul dispositivo.

Scegli il dispositivo di archiviazione in cui salvare.

● Arresta una registrazione sul dispositivo.

Le registrazioni attivate termineranno in caso di arresto manuale o in caso di spegnimento del dispositivo.

Le registrazioni continue continueranno fino all'arresto manuale. Anche se il dispositivo si arresta, la registrazione prosegue quando il dispositivo si avvia nuovamente.

Riproduci la registrazione.

Interrompi la riproduzione della registrazione.

Mostra o nascondi le informazioni e le opzioni sulla registrazione.

Set export range (Impostare l'intervallo di esportazione): Se vuoi esportare solo parte della registrazione, indica un intervallo di tempo.

Encrypt (Codifica): selezionare per impostare una password per le registrazioni esportate. Non è possibile aprire il file esportato senza la password.

Fare clic per eliminare una registrazione.

Export (Esporta): esporta l'intera registrazione o una sua parte.

Fare clic per filtrare le registrazioni.

From (Da): Mostra le registrazioni avvenute dopo un certo punto temporale.

To (A): Mostra le registrazioni fino a un certo punto temporale.

Source (Sorgente) : mostra le registrazioni sulla base della sorgente. La sorgente si riferisce al sensore.

Event (Evento): mostra le registrazioni sulla base degli eventi.

Storage (Archiviazione): mostra le registrazioni in base al tipo di dispositivo di archiviazione.

App

Add app (Aggiungi app): Installa una nuova app.

Find more apps (Trova altre app): Trova altre app da installare. Verrà visualizzata una pagina panoramica delle app Axis.

Allow unsigned apps (Consenti app non firmate): Attiva per permettere che siano installate app senza firma.

Allow root-privileged apps (Permetti app con privilegi root): Abilitare per consentire l'accesso completo al dispositivo alle app con privilegi root.

Visualizzare gli aggiornamenti sulla sicurezza nelle app AXIS OS e ACAP.

Nota

Eseguire più app allo stesso tempo può avere un impatto sulle prestazioni del dispositivo.

Usa l'interruttore vicino al nome dell'app per l'avvio o l'arresto dell'app.

Open (Apri): Accedi alle impostazioni dell'app. Le impostazioni disponibili dipendono dall'applicazione. Alcune applicazioni non sono dotate di impostazioni.

Il menu contestuale può contenere una o più delle seguenti opzioni:

- **Open-source license (Licenza open-source)**: Visualizza le informazioni relative alle licenze open source usate nell'app.
- **App log (Registro app)**: Visualizza un registro degli eventi relativi all'app. Il registro è utile quando si contatta l'assistenza.
- **Activate license with a key (Attiva licenza con una chiave)**: nel caso l'app necessiti di una licenza, devi attivarla. Se il dispositivo non ha accesso a Internet, usa questa opzione.
  Se non si dispone di una chiave di licenza, andare a *axis.com/products/analytics*. Per generare una chiave di licenza, sono necessari il codice di licenza e il numero di serie del dispositivo Axis.
- **Activate license automatically (Attiva automaticamente la licenza)**: Nel caso l'app necessiti di una licenza, devi attivarla. Se il dispositivo ha accesso a Internet, usa questa opzione. È necessario un codice di licenza per attivare la licenza.
- **Deactivate the license (Disattiva la licenza)**: Disattivare la licenza per sostituirla con un'altra licenza, ad esempio quando si passa da una licenza di prova a una licenza completa. Se si disattiva la licenza, verrà eliminata anche dal dispositivo.
- **Settings (Impostazioni)**: Configurare i parametri del dispositivo.
- **Delete (Elimina)**: Cancella permanentemente l'app dal dispositivo. La licenza resta attiva a meno che non la disattivi prima.

Sistema

Ora e ubicazione

Data e ora

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

Nota

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

Synchronization (Sincronizzazione): selezionare un'opzione per la sincronizzazione di data e ora del dispositivo.

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

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

Nota

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

Ubicazione dei dispositivi

Immettere la posizione del dispositivo. Il sistema di gestione video può utilizzare queste informazioni per posizionare il dispositivo su una mappa.

- **Latitude (Latitudine)**: i valori positivi puntano a nord dell'equatore.
- **Longitude (Longitudine)**: i valori positivi puntano a est del primo meridiano.
- **Heading (Intestazione)**: Inserire la direzione della bussola verso cui è diretto il dispositivo. 0 punta a nord.
- **Label (Etichetta)**: Inserire un nome descrittivo per il dispositivo.
- **Save (Salva)**: Fare clic per salvare la posizione del dispositivo.

Regional settings (Impostazioni nazionali)

Imposta il sistema di misura da utilizzare in tutte le impostazioni del sistema.

Sistema metrico (m, km/h): Selezionare affinché la distanza sia misurata in metri e la velocità sia misurata in chilometri orari.

U.S. customary (ft, mph) (Statunitense (piedi, mph)): seleziona affinché la distanza sia misurata in piedi e la velocità sia misurata in miglia orarie.

Rete

IPv4 (IPv4)

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

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

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

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

Fallback to static IP address if DHCP isn't available (Fallback all'indirizzo IP fisso se DHCP non è disponibile): selezionalo se vuoi aggiungere un indirizzo IP statico da usare come fallback se DHCP non è disponibile e non è possibile assegnare in automatico un indirizzo IP.

Nota

Se DHCP non è disponibile e il dispositivo utilizza un fallback dell'indirizzo statico, l'indirizzo statico viene configurato con un ambito limitato.

IPv6

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

Hostname (Nome host)

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

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

DNS servers (Server DNS)

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

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

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

HTTP and HTTPS (HTTP e HTTPS)

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

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

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

Nota

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

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

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

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

Protocolli di rilevamento della rete

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

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

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

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

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

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

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

Allow O3C (Consenti O3C):

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

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

Host: Inserire l'indirizzo del server del proxy.

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

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

Authentication method (Metodo di autenticazione):

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

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

SNMP (SNMP)

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

SNMP: Selezionare la versione di SNMP da utilizzare.

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

Nota

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

- **v3**: SNMP v3 è una versione più sicura che fornisce crittografia e password sicure. Per utilizzare SNMP v3, si consiglia di attivare HTTPS poiché la password verrà successivamente inviata via HTTPS. Ciò impedisce inoltre alle parti non autorizzate di accedere ai trap SNMP v1 e v2c non crittografati. Se si utilizza SNMP v3, è possibile impostare i trap tramite l'applicazione di gestione SNMP v3.
  - **Password for the account "initial" (Password per l'account "iniziale")**: Immettere la password SNMP per l'account denominato "iniziale". Sebbene la password possa essere inviata senza attivare HTTPS, non è consigliabile. La password SNMP v3 può essere impostare solo una volta e preferibilmente solo quando è attivato HTTPS. Una volta impostata la password, il relativo campo non verrà più visualizzato. Per impostare di nuovo la password, il dispositivo deve essere ripristinato alle impostazioni predefinite di fabbrica.

Sicurezza

Certificates (Certificati)

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

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

Questi formati sono supportati:

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

Importante

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

Filtra i certificati nell'elenco.

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

- **More... (Altro...)** : mostra altri campi da compilare o selezionare.
- **Secure keystore (Archivio chiavi sicuro)**: selezionare questa opzione per utilizzare **Secure Element (Elemento sicuro)** o **Trusted Platform Module 2.0** per archiviare in modo sicuro la chiave privata. Per ulteriori informazioni su quale keystore sicuro selezionare, andare a *help.axis.com/en-us/axis-os#cryptographic-support*.
- **Key type (Tipo chiave)**: selezionare l'algoritmo di crittografia predefinito o diverso dall'elenco a discesa per proteggere il certificato.

Il menu contestuale contiene:

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

Secure keystore (Archivio chiavi sicuro) :

- **Secure element (CC EAL6+) (Elemento sicuro)**: Selezionare questa opzione per utilizzare un elemento sicuro per l'archivio chiavi sicuro.
- **Trusted Platform Module 2.0 (CC EAL4+, FIPS 140-2 Level 2)** Selezionare questa opzione per utilizzare TPM 2.0 per il keystore sicuro.

IEEE 802.1x and IEEE 802.1AE MACsec (IEEE 802.1x e IEEE 802.1AE MACsec)

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

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

Certificates (Certificati)

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

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

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

Authentication method (Metodo di autenticazione): Selezionare un tipo EAP impiegato per l'autenticazione. L'opzione predefinita è **EAP-TLS**.

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

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

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

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

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

IEEE 802.1AE MACsec

IEEE 802.1AE MACsec rappresenta uno standard IEEE per la sicurezza MAC (Media Access Control) che definisce la riservatezza e l'integrità dati senza connessione per i protocolli indipendenti di accesso ai media.

Le impostazioni sono a disposizione solo in caso di uso di **EAP-TLS** in qualità di metodo di autenticazione.

Mode (Modalità)

- **Dynamic CAK / EAP-TLS**: L'opzione predefinita. In seguito ad una connessione protetta, il dispositivo verifica la presenza di MACsec sulla rete.
- **Chiave Static CAK / pre-shared (PSK)**: selezionare questa opzione per eseguire l'impostazione del nome e del valore della chiave per connettersi alla rete.

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

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

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

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

IP address filter (Filtro indirizzi IP)

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

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

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

Certificato firmware con firma personalizzata

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

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

Il menu contestuale contiene:

- **Delete certificate (Elimina certificato)**: Elimina il certificato.

Account

Account

Add account (Aggiungi account): Fare clic per aggiungere un nuovo account. Puoi aggiungere un massimo di 100 account.

Account: Inserire un nome account univoco.

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

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

Privileges (Privilegi):

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

Il menu contestuale contiene:

Update account (Aggiorna account): Modifica le proprietà dell'account.

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

Anonymous access (Accesso anonimo)

Allow anonymous viewing (Consenti visualizzazione anonima): attiva questa opzione per permettere a chiunque l'accesso al dispositivo in qualità di visualizzatore senza accedere con un account utente.

Allow anonymous PTZ operating (Consenti uso anonimo di PTZ): per permettere agli utenti anonimi di eseguire la panoramica, inclinazione e zoom dell'immagine, attiva questa opzione.

Account SSH

+ **Add SSH account (Aggiungi account SSH)**: Fare clic per aggiungere un nuovo account SSH.

- **Restrict root access (Limita accesso root)**: Attivare per limitare la funzionalità che richiede l'accesso root.
- **Abilita SSH**: Attivare per utilizzare il servizio SSH.

Account: Inserire un nome account univoco.

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

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

Commento: Inserire un commenti (facoltativo).

⋮ Il menu contestuale contiene:

Update SSH account (Aggiorna account SSH): Modifica le proprietà dell'account.

Delete SSH account (Elimina account SSH): Elimina l'account. Non puoi cancellare l'account root.

OpenID Configuration (Configurazione OpenID):

Importante

inserire i valori appropriati per assicurare che sia possibile accedere nuovamente al dispositivo.

Client ID (ID client): inserire il nome utente OpenID.

Outgoing Proxy (Proxy in uscita): inserire l'indirizzo proxy che può essere utilizzato dalla connessione OpenID.

Admin claim (Richiesta amministratore): inserire un valore per il ruolo di amministratore.

Provider URL (URL provider): inserire il collegamento web per l'autenticazione dell'endpoint API. Il formato deve https://[inserire URL]/.well-known/openid-configuration

Operator claim (Richiesta operatore): inserire un valore per il ruolo di operatore.

Require claim (Richiesta obbligatoria): inserire i dati che devono essere contenuti nel token.

Viewer claim (Richiesta visualizzatore): inserire il valore per il ruolo visualizzatore.

Remote user (Utente remoto): inserire un valore per identificare gli utenti remoti. In questo modo sarà possibile visualizzare l'utente corrente nell'interfaccia web del dispositivo.

Scopes (Ambiti): Ambiti opzionali che potrebbero far parte del token.

Client secret (Segreto client): inserire la password OpenID

Save (Salva): Fare clic per salvare i valori OpenID.

Enable OpenID (Abilita OpenID): attivare per chiudere la connessione corrente e consentire l'autenticazione del dispositivo dall'URL del provider.

Eventi

Regole

Una regola consente di definire le condizioni che attivano il prodotto per l'esecuzione di un'azione. L'elenco mostra tutte le regole correntemente configurate nel dispositivo.

Nota

Puoi creare un massimo di 256 regole di azione.

Add a rule (Aggiungi una regola): Creare una regola.

Name (Nome): Inserire un nome per la regola.

Wait between actions (Attesa tra le azioni): Inserisci il periodo di tempo minimo (hh:mm:ss) che deve trascorrere tra le attivazioni della regola. Risulta utile se la regola si attiva, ad esempio, nelle condizioni della modalità diurna/notturna, per evitare che piccole variazioni di luce durante l'alba e il tramonto attivino ripetutamente la regola.

Condition (Condizione): Selezionare una condizione dall'elenco. Una condizione che deve essere soddisfatta affinché il dispositivo esegua un'azione. Se vengono definite più condizioni, devono essere tutte soddisfatte per attivare l'azione. Vedere *Introduzione alle regole per gli eventi* per ottenere informazioni riguardo a condizioni specifiche.

Use this condition as a trigger (Utilizza questa condizione come trigger): Selezionare questa opzione affinché questa prima condizione operi solo in qualità di trigger di avvio. Vuol dire che una volta attivata la regola, essa rimane attiva purché tutte le altre condizioni siano soddisfatte, a prescindere dallo stato della prima condizione. Se non selezioni questa opzione, la regola sarà semplicemente attiva quando tutte le condizioni sono soddisfatte.

Invert this condition (Inverti questa condizione): Selezionala se desideri che la condizione sia l'opposto della tua selezione.

Add a condition (Aggiungi una condizione): fare clic per l'aggiunta di un'ulteriore condizione.

Action (Azione): seleziona un'azione dalla lista e inserisci le informazioni necessarie. Vedere *Introduzione alle regole per gli eventi* per ottenere informazioni riguardo ad azioni specifiche.

Destinatari

Hai la possibilità di configurare il dispositivo perché invii ai destinatari notifiche relative ad eventi o dei file. Nell'elenco vengono mostrati i destinatari configurati al momento nel dispositivo insieme alle varie informazioni sulla relativa configurazione.

Nota

È possibile creare fino a 20 destinatari.

Add a recipient (Aggiungi un destinatario): fare clic per aggiungere un destinatario.

Name (Nome): immettere un nome per il destinatario.

Type (Tipo): Seleziona dall'elenco:

- FTP
  - **Host**: Inserire l'indirizzo IP o il nome host del server. Se inserisci un nome host, accertati che sia specificato un server DNS in **System > Network > IPv4 and IPv6 (Sistema > Rete > IPv4 e IPv6)**.
  - **Port (Porta)**: Immettere il numero di porta utilizzata dal server FTP. Il valore predefinito è 21.
  - **Folder (Cartella)**: inserisci il percorso alla directory nella quale vuoi conservare i file. Se questa directory non esiste già sul server FTP, durante il caricamento dei file riceverai un messaggio di errore.
  - **Username (Nome utente)**: immettere il nome utente per l'accesso.
  - **Password**: immettere la password per l'accesso.
  - **Use temporary file name (Usa nome file temporaneo)**: seleziona questa opzione per il caricamento dei file con nomi file temporanei generati in automatico. Ai file sono assegnati i nomi desiderati quando viene completato il caricamento. Se il caricamento viene annullato/interrotto, non si avrà alcun file corrotto. Tuttavia, probabilmente avrai comunque i file temporanei. In questo modo è possibile sapere che tutti i file con il nome desiderato sono corretti.
  - **Use passive FTP (Usa FTP passivo)**: in circostanze normali il dispositivo richiede semplicemente il server FTP di destinazione per aprire la connessione dati. Il dispositivo inizializza attivamente il comando FTP e

le connessioni dati sul server di destinazione. Ciò è necessario generalmente se esiste un firewall tra il dispositivo e il server FTP di destinazione.

- **HTTP**
  - **URL**: Inserire l'indirizzo di rete sul server HTTP e lo script che gestirà la richiesta. Ad esempio, http://192.168.254.10/cgi-bin/notify.cgi.
  - **Username (Nome utente)**: immettere il nome utente per l'accesso.
  - **Password**: immettere la password per l'accesso.
  - **Proxy**: Attiva e inserisci le informazioni necessarie se si deve superare un server proxy per eseguire la connessione al server HTTP.
- **HTTPS**
  - **URL**: Inserire l'indirizzo di rete sul server HTTPS e lo script che gestirà la richiesta. Ad esempio, https://192.168.254.10/cgi-bin/notify.cgi.
  - **Validate server certificate (Convalida certificato server)**: Selezionare per convalidare il certificato creato dal server HTTPS.
  - **Username (Nome utente)**: immettere il nome utente per l'accesso.
  - **Password**: immettere la password per l'accesso.
  - **Proxy**: Attiva e inserisci le informazioni necessarie se si deve superare un server proxy per eseguire la connessione al server HTTPS.
- **Network storage (Archiviazione di rete)**
  Puoi aggiungere dispositivi di archiviazione di rete, ad esempio NAS (Network Attached Storage) e utilizzarli come destinatario per archiviare i file. I file vengono archiviati in formato Matroska (MKV).
  - **Host**: Immettere il nome host o l'indirizzo IP per il dispositivo di archiviazione di rete.
  - **Share (Condivisione)**: Immettere il nome della condivisione nell'host.
  - **Folder (Cartella)**: inserisci il percorso alla directory nella quale vuoi conservare i file.
  - **Username (Nome utente)**: immettere il nome utente per l'accesso.
  - **Password**: immettere la password per l'accesso.
- **SFTP**
  - **Host**: Inserire l'indirizzo IP o il nome host del server. Se inserisci un nome host, accertati che sia specificato un server DNS in **System > Network > IPv4 and IPv6 (Sistema > Rete > IPv4 e IPv6)**.
  - **Port (Porta)**: Immettere il numero della porta utilizzata dal server SFTP. Il valore predefinito è 22.
  - **Folder (Cartella)**: inserisci il percorso alla directory nella quale vuoi conservare i file. Se questa directory non esiste già sul server SFTP, durante il caricamento dei file riceverai un messaggio di errore.
  - **Username (Nome utente)**: immettere il nome utente per l'accesso.
  - **Password**: immettere la password per l'accesso.
  - **SSH host public key type (MD5) (Tipo di chiave pubblica host SSH (MD5))**: Immetti l'impronta digitale della chiave pubblica dell'host remoto (una stringa di 32 cifre esadecimali). Il client SFTP supporta i server SFTP mediante SSH-2 con tipi di chiavi host RSA, DSA, ECDSA e ED25519. RSA è il metodo preferito durante la negoziazione, seguito da ECDSA, ED25519 e DSA. Assicurarsi di inserire la chiave host MD5 esatta utilizzata dal server SFTP. Benché il dispositivo Axis supporti chiavi hash sia MD5 sia SHA-256, consigliamo l'uso di SHA-256 per una maggiore sicurezza rispetto a MD5. Per maggiori informazioni su come si configura un server SFTP con un dispositivo Axis, vai sul *Portale AXIS OS*.
  - **SSH host public key type (SHA256) (Tipo di chiave pubblica host SSH (SHA256))**: Immetti l'impronta digitale della chiave pubblica dell'host remoto (una stringa di 43 cifre con codifica Base64). Il client SFTP supporta i server SFTP mediante SSH-2 con tipi di chiavi host RSA, DSA, ECDSA e ED25519. RSA è il metodo preferito durante la negoziazione, seguito da ECDSA, ED25519 e DSA. Assicurarsi di inserire la chiave host MD5 esatta utilizzata dal server SFTP. Benché il dispositivo Axis supporti chiavi hash sia MD5 sia SHA-256, consigliamo l'uso di SHA-256 per una maggiore sicurezza rispetto a MD5. Per maggiori informazioni su come si configura un server SFTP con un dispositivo Axis, vai sul *Portale AXIS OS*.
  - **Use temporary file name (Usa nome file temporaneo)**: seleziona questa opzione per il caricamento dei file con nomi file temporanei generati in automatico. Ai file sono assegnati i nomi desiderati quando viene completato il caricamento. Se il caricamento viene annullato o interrotto, non si avrà alcun file corrotto. Tuttavia, probabilmente avrai comunque i file temporanei. In questo modo è possibile sapere che tutti i file con il nome desiderato sono corretti.
- **SIP or VMS (SIP o VMS)** :
  SIP: selezionare per eseguire una chiamata SIP.
  VMS: selezionare per eseguire una chiamata VMS.
  - **From SIP account (Dall'account SIP)**: Selezionare dall'elenco.
  - **To SIP address (All'indirizzo SIP)**: Immetti l'indirizzo SIP.
  - **Test (Verifica)**: fare clic per verificare che le impostazioni di chiamata funzionino.
- **Email (E-mail)**

- **Send email to (Invia e-mail a)**: Inserire l'indirizzo e-mail a cui inviare i messaggi e-mail. Per immettere più indirizzi, separarli utilizzando le virgole.
- **Send email from (Invia e-mail da)**: immettere l'indirizzo e-mail del server mittente.
- **Username (Nome utente)**: Immettere il nome utente per il server mail. Lasciare vuoto questo campo se il server mail non necessita di autenticazione.
- **Password**: Immettere la password per il server mail. Lasciare vuoto questo campo se il server mail non necessita di autenticazione.
- **Email server (SMTP) - Server e-mail (SMTP)**: inserire il nome del server SMTP, ad esempio, smtp.gmail.com, smtp.mail.yahoo.com.
- **Port (Porta)**: inserire il numero della porta per il server SMTP, utilizzando i valori nell'intervallo da 0 a 65535. Il valore predefinito è 587.
- **Encryption (Crittografia)**: Per usare la crittografia, seleziona SSL o TLS.
- **Validate server certificate (Convalida certificato server)**: Se usi la crittografia, seleziona questa opzione per convalidare l'identità del dispositivo. Il certificato può essere autofirmato o emesso da un'autorità di certificazione (CA).
- **POP authentication (Autenticazione POP)**: Attiva per inserire il nome del server POP, ad esempio pop.gmail.com.

Nota

Alcuni provider e-mail hanno filtri di sicurezza che impediscono agli utenti di ricevere o visualizzare allegati di grandi dimensioni, ad esempio e-mail pianificate e simili. Controllare i criteri di sicurezza del provider e-mail per evitare che l'account e-mail venga bloccato o perda i messaggi e-mail attendibili.

- **TCP**
  - **Host**: Inserire l'indirizzo IP o il nome host del server. Se inserisci un nome host, accertati che sia specificato un server DNS in **System > Network > IPv4 and IPv6 (Sistema > Rete > IPv4 e IPv6)**.
  - **Porta**: Immettere il numero della porta utilizzata per l'accesso al server.

Test (Verifica): Fare clic per testare l'impostazione.

⋮ Il menu contestuale contiene:

View recipient (Visualizza destinatario): fare clic per visualizzare tutti i dettagli del destinatario.

Copy recipient (Copia destinatario): Fare clic per copiare un destinatario. Quando copi, puoi modificare il nuovo destinatario.

Delete recipient (Elimina destinatario): Fare clic per l'eliminazione permanente del destinatario.

Pianificazioni

Le pianificazioni e gli impulsi possono essere utilizzati come condizioni nelle regole. Nell'elenco vengono mostrati le pianificazioni e gli impulsi configurati al momento nel dispositivo, insieme alle varie informazioni sulla relativa configurazione.

+ **Add schedule (Aggiungi pianificazione)**: Fare clic per la creazione di una pianificazione o un impulso.

Trigger manuali

È possibile utilizzare l'attivazione manuale per attivare manualmente una regola. L'attivazione manuale può, ad esempio, essere per convalidare le azioni durante l'installazione e la configurazione del dispositivo.

MQTT

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

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

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

ALPN (RETE ALPN)

ALPN è un'estensione TLS/SSL che consente la selezione di un protocollo applicativo durante la fase di handshake della connessione tra client e server. Viene utilizzato per abilitare il traffico MQTT sulla stessa porta utilizzata per altri protocolli, ad esempio HTTP. In alcuni casi, potrebbe non esserci una porta dedicata aperta per la comunicazione MQTT. Una soluzione in tali casi consiste nell'utilizzare ALPN per trattare l'uso di MQTT come protocollo applicativo su una porta standard, consentito dai firewall.

MQTT client (Client MQTT)

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

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

Broker

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

Protocol (Protocollo): Selezionare il protocollo da utilizzare.

Port (Porta): Immettere il numero di porta.

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

ALPN protocol (Protocollo ALPN): Inserire il nome del protocollo ALPN fornito dal provider MQTT. Ciò è applicabile solo con MQTT over SSL e MQTT over WebSocket Secure.

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

Password: immettere una password per il nome utente.

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

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

HTTP proxy (Proxy HTTP): Un URL dotato di una lunghezza non superiore a 255 byte. È possibile lasciare il campo vuoto se non si vuole usare un proxy HTTP.

HTTPS proxy (Proxy HTTPS): Un URL dotato di una lunghezza non superiore a 255 byte. È possibile lasciare il campo vuoto se non si vuole usare un proxy HTTPS.

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

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

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

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

Connect message (Messaggio connessione)

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

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

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

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

Payload: Immettere il contenuto per il messaggio predefinito.

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

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

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

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

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

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

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

Payload: Immettere il contenuto per il messaggio predefinito.

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

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

MQTT publication (Pubblicazione MQTT)

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

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

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

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

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

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

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

QoS: Seleziona il livello desiderato per la pubblicazione MQTT.

MQTT subscriptions (Sottoscrizioni MQTT)

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

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

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

Subscription type (Tipo di sottoscrizione):

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

QoS: Seleziona il livello desiderato per la sottoscrizione MQTT.

MQTT overlays (Sovrapposizioni testo MQTT)

Nota

Connetti a un broker MQTT prima dell'aggiunta dei campi di modifica di sovrapposizione testo MQTT.

+ Add overlay modifier (Aggiungi campo di modifica sovrapposizione testo): Fare clic per l'aggiunta di un nuovo campo di modifica di sovrapposizione testo.

Topic filter (Filtro argomenti): Aggiungi l'argomento MQTT contenente i dati che vuoi mostrare nella sovrapposizione testo.

Data field (Campo dati): Specifica la chiave per il payload del messaggio che vuoi visualizzare nella sovrapposizione testo, purché il messaggio sia in formato JSON.

Modifier (Campo di modifica): Usa il campo di modifica risultante quando crei la sovrapposizione testo.

- I campi di modifica che cominciano con **#XMP** mostrano tutti i dati ricevuti dall'argomento.
- I campi di modifica che cominciano con **#XMD** mostrano i dati specificati nel campo dati.

Archiviazione

Network storage (Archiviazione di rete)

Ignore (Ignora): Attiva per ignorare l'archiviazione di rete.

Add network storage (Aggiungi archiviazione di rete): fare clic su questa opzione per eseguire l'aggiunta di una condivisione di rete nella quale poter salvare le registrazioni.

- **Address (Indirizzo)**: Inserire l'indirizzo IP o il nome host del server host, generalmente NAS (Network Attached Storage). Si consiglia di configurare l'host per utilizzare un indirizzo IP fisso (non DHCP perché un indirizzo IP dinamico potrebbe cambiare) o di utilizzare DNS. I nomi Windows SMB/CIFS non sono supportati.
- **Network share (Condivisione di rete)**: Inserire il nome dell'ubicazione condivisa nel server host. Diversi dispositivi Axis possono utilizzare la stessa condivisione di rete dal momento che ogni dispositivo ha una propria cartella.
- **User (Utente)**: inserire il nome utente se serve eseguire il login per il server. Digita `DOMAIN\username` per accedere a un server di dominio specifico.
- **Password**: Immetti la password se serve eseguire il login per il server.
- **SMB version (Versione SMB)**: Seleziona la versione del protocollo di archiviazione SMB da collegare al NAS. Se selezioni **Auto (Automatico)**, il dispositivo cerca di negoziare una delle versioni sicure SMB: 3.02, 3.0, o 2.1. Seleziona 1.0 o 2.0 per la connessione a NAS meno recenti che non sono dotati di supporto per versioni superiori. Puoi leggere maggiori dettagli sul supporto SMB nei dispositivi Axis *qui*.

- **Add share without testing (Aggiungi condivisione senza test)**: seleziona questa opzione per eseguire l'aggiunta della condivisione di rete a prescindere dal rilevamento di un errore durante il test della connessione. Ad esempio, l'errore può consistere nel non aver inserito una password nonostante sia necessaria per il server.

Remove network storage (Rimuovi archiviazione di rete): Fare clic su questa opzione per smontare, disassociare ed eseguire la rimozione della connessione alla condivisione di rete. Ciò elimina ogni impostazione per la condivisione di rete.

Unbind (Disassocia): fare clic per disassociare e scollegare la condivisione di rete.
Bind (Associa): Fare clic per associare e connettere la condivisione di rete.

Unmount (Smonta): Fare clic per smontare la condivisione di rete.
Mount (Monta): Fare clic su questa opzione per montare la condivisione di rete.

Write protect (Proteggi da scrittura): attiva questa opzione per interrompere la scrittura nella condivisione di rete e proteggere le registrazioni dalla rimozione. Una condivisione di rete protetta da scrittura non può essere formattata.

Retention time (Tempo di conservazione): Selezionare il periodo di conservazione delle registrazioni in modo da porre un limite al numero di vecchie registrazioni od ottemperare alle normative in merito alla conservazione dei dati. Le registrazioni precedenti sono cancellate prima della scadenza del periodo selezionato se l'archiviazione di rete diventa piena.

Tools (Strumenti)

- **Test connection (Verifica connessione)**: Verifica la connessione alla condivisione di rete.
- **Format (Formatta)**: Formattare la condivisione di rete, ad esempio quando è necessario cancellare rapidamente tutti i dati. CIFS è l'opzione del file system disponibile.

Use tool (Utilizza strumento): Fare clic per attivare lo strumento selezionato.

Onboard storage (Archiviazione integrata)

Importante

Rischio di perdita di dati e danneggiamento delle registrazioni. Non rimuovere la scheda di memoria mentre il dispositivo è in funzione. Prima di rimuovere la scheda SD, smontala.

Unmount (Smonta): fare clic su questa opzione per eseguire la rimozione sicura della scheda di memoria.

Write protect (Proteggi da scrittura): attivare questa opzione per interrompere la scrittura nella scheda di memoria e proteggere le registrazioni dalla rimozione. Una scheda di memoria protetta da scrittura non può essere formattata.

Autoformat (Formattazione automatica): Attiva per la formattazione automatica di una scheda di memoria appena inserita. Formatta il file system in ext4.

Ignore (Ignora): attiva questa opzione per non archiviare più le registrazioni sulla scheda di memoria. Il dispositivo non riconosce più che la scheda di memoria esiste se la ignori. Solo gli amministratori hanno a disposizione questa impostazione.

Retention time (Tempo di conservazione): Selezionare il periodo di conservazione delle registrazioni in modo da porre un limite al numero di vecchie registrazioni od ottemperare alle normative in merito alla conservazione dei dati. Le registrazioni precedenti sono cancellate prima della scadenza del periodo selezionato se la scheda di memoria diventa piena.

Tools (Strumenti)

- **Check (Controlla)**: verificare la presenza di eventuali errori nella scheda di memoria. Questa opzione è valida solo per il file system ext4.
- **Repair (Ripara)**: corregge gli errori nel file system ext4. Per correggere gli errori in una scheda di memoria con file system VFAT, espellere la scheda di memoria, inserirla in un computer ed eseguire un riparazione degli errori del disco.
- **Format (Formatta)**: formatta la scheda di memoria, ad esempio quando necessario per modificare il file system o per cancellare rapidamente tutti i dati. VFAT e ext4 sono le due opzioni di file system disponibili. Il formato consigliato è ext4, grazie alla relativa resilienza rispetto alla perdita di dati se la scheda viene espulsa o in caso di drastica perdita di alimentazione. Tuttavia, avrai bisogno di un'applicazione o un driver ext4 di terze parti per accedere al file system da Windows®.
- **Encrypt (Codifica)**: Utilizza questo strumento per la formattazione della scheda di memoria e l'abilitazione della crittografia. **Encrypt (Codifica)** risulta nell'eliminazione di tutti i dati archiviati sulla scheda di memoria. Dopo aver usato **Encrypt (Codifica)**, i dati archiviati nella scheda di memoria saranno protetti da crittografia.

- **Decrypt (Decodifica)**: Usa questo strumento per la formattazione della scheda di memoria senza crittografia. **Decrypt (Decodifica)** risulta nell'eliminazione di tutti i dati archiviati sulla scheda di memoria. Dopo aver usato **Decrypt (Decodifica)**, i dati archiviati nella scheda di memoria non saranno protetti da crittografia.
- **Change password (Cambia password)**: modifica la password che serve per la crittografia della scheda di memoria.

Use tool (Utilizza strumento): Fare clic per attivare lo strumento selezionato.

Wear trigger (Trigger usura): Imposta un valore per il livello di usura della scheda di memoria in corrispondenza del quale desideri che sia attivata un'azione. Il livello di usura spazia da 0 a 200%. Una nuova scheda di memoria mai usata è dotata di un livello di usura pari allo 0%. Un livello di usura pari al 100% indica che la scheda di memoria è vicina alla fine del suo ciclo di vita previsto. Quando il livello di usura raggiunge il 200%, sussiste un rischio elevato di malfunzionamento della scheda di memoria. Consigliamo l'impostazione dell'intervallo del trigger di usura tra 80% e 90%. Così avrai il tempo di scaricare tutte le registrazioni e sostituire la scheda di memoria prima che si usuri del tutto. Il trigger di usura permette di impostare un evento e ricevere una notifica quando il livello di usura raggiunge il valore che hai impostato.

Profili di streaming

Un profilo di streaming è un gruppo di impostazioni che incidono sul flusso video. Puoi usare i profili di streaming in situazioni diverse, ad esempio quando crei eventi e usi regole per registrare.

+ **Add stream profile (Aggiungi profilo di streaming)**: Fare clic per creare un nuovo profilo di streaming.

Preview (Anteprima): Un'anteprima del flusso video con le impostazioni del profilo di streaming che selezioni. L'anteprima si aggiorna quando cambi le impostazioni nella pagina. Se il dispositivo ha aree di visione diverse, puoi cambiare l'area di visione nell'elenco a discesa nell'angolo in basso a sinistra dell'immagine.

Name (Nome): aggiungi un nome per il tuo profilo.

Description (Descrizione): aggiungi una descrizione del tuo profilo.

Video codec (Codec video): selezionare il codec video che va applicato al profilo.

Resolution (Risoluzione): Consulta per vedere una descrizione di questa impostazione.

Frame rate (Velocità in fotogrammi): Consulta per vedere una descrizione di questa impostazione.

Compression (Compressione): Consulta per vedere una descrizione di questa impostazione.

Zipstream : Consulta per vedere una descrizione di questa impostazione.

Optimize for storage (Ottimizza per archiviazione) : Consulta per vedere una descrizione di questa impostazione.

Dynamic FPS (FPS dinamico) : Consulta per vedere una descrizione di questa impostazione.

Dynamic GOP (Dynamic group of pictures) : Consulta per vedere una descrizione di questa impostazione.

Mirror (Specularità) : Consulta per vedere una descrizione di questa impostazione.

GOP length (Lunghezza GOP) : Consulta per vedere una descrizione di questa impostazione.

Bitrate control (Controllo velocità in bit): Consulta per vedere una descrizione di questa impostazione.

Include overlays (Includi sovrapposizioni testo): Selezionare il tipo di sovrapposizione da includere. Consulta *Sovrapposizioni alla pagina 32* per informazioni su come aggiungere sovrapposizioni.

Include audio (Includi audio)  : Consulta per vedere una descrizione di questa impostazione.

ONVIF

Account ONVIF

ONVIF (Open Network Video Interface Forum) è uno standard di interfaccia globale che rende più semplice a utenti finali, integratori, consulenti e produttori di avvalersi delle possibilità offerte dalla tecnologia video di rete. ONVIF consente interoperabilità tra dispositivi di fornitori differenti, massima flessibilità, costi ridotti e sistemi a prova di futuro.

Quando si crea un account ONVIF, la comunicazione ONVIF è abilitata automaticamente. Utilizzare il nome account e la password per tutte le comunicazioni ONVIF con il dispositivo. Per ulteriori informazioni, visitare l'Axis Developer Community sul sito web *axis.com*.

Add accounts (Aggiungi account) Per creare un nuovo account ONVIF.

Account: Inserire un nome account univoco.

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

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

Role (Ruolo):

- **Administrator (Amministratore)**: ha accesso completo a tutte le impostazioni. Gli amministratori possono anche aggiungere, aggiornare e rimuovere altri account.
- **Operator (Operatore)**: ha accesso a tutte le impostazioni ad eccezione di:
  - Tutte le impostazioni **System (Sistema)**.
  - L'aggiunta di app.
- **Media account (Account multimediale)**: Permette di accedere solo al flusso video.

Il menu contestuale contiene:

Update account (Aggiorna account): Modifica le proprietà dell'account.

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

Profili di supporti ONVIF

Un profilo di supporti ONVIF è costituito da una serie di configurazioni utilizzabili per modificare le impostazioni di flusso dei supporti. Puoi creare nuovi profili con il tuo set di configurazioni o utilizzare profili preconfigurati per una configurazione rapida.

Add media profile (Aggiungi profilo multimediale): Fare clic per aggiungere un nuovo profilo di supporti ONVIF.

Profile name (Nome profilo): Aggiungi un nome per il profilo multimediale.

Video source (Sorgente video): Seleziona la sorgente video per la tua configurazione.

- **Select configuration (Selezionare configurazione)**: Selezionare una configurazione definita dall'utente dall'elenco. Le configurazioni nell'elenco a discesa corrispondono ai canali video del dispositivo, comprese le multiview, le aree di visione e i canali virtuali.

Video encoder (Codificatore video): Selezionare il formato di codifica video per la tua configurazione.

- **Select configuration (Selezionare configurazione)**: Selezionare una configurazione definita dall'utente dall'elenco e regolare le impostazioni di codifica. Le configurazioni nell'elenco a discesa fungono da identificatori/nomi della

configurazione del video encoder. Selezionare l'utente da 0 a 15 per applicare le tue impostazioni oppure selezionare uno degli utenti predefiniti se si desidera utilizzare le impostazioni predefinite per un formato di codifica specifico.

Nota

Abilita l'audio nel dispositivo per avere la possibilità di selezionare una sorgente audio e la configurazione del codificatore audio.

Audio source (Sorgente audio) : Selezionare la sorgente di ingresso audio per la tua configurazione.

- **Select configuration (Selezionare configurazione)**: Selezionare una configurazione definita dall'utente dall'elenco e regolare le impostazioni audio. Le configurazioni nell'elenco a discesa corrispondono agli ingressi audio del dispositivo. Se il dispositivo ha un ingresso audio, è user0. Se il dispositivo dispone di più ingressi audio, nell'elenco saranno presenti altri utenti.

Audio encoder (Registratore audio) : Selezionare il formato di codifica audio per la tua configurazione.

- **Select configuration (Selezionare configurazione)**: Selezionare una configurazione definita dall'utente dall'elenco e regolare le impostazioni di codifica audio. Le configurazioni nell'elenco a discesa fungono da identificatori/nomi della configurazione dell'audio encoder.

Metadata: Selezionare i metadati da includere nella configurazione.

- **Select configuration (Selezionare configurazione)**: Selezionare una configurazione definita dall'utente dall'elenco e regolare le impostazioni dei metadati. Le configurazioni nell'elenco a discesa fungono da identificatori/nomi della configurazione dei metadati.

PTZ : Selezionare le impostazioni PTZ per la tua configurazione.

- **Select configuration (Selezionare configurazione)**: Selezionare una configurazione definita dall'utente dall'elenco e regolare le impostazioni PTZ. Le configurazioni nell'elenco a discesa corrispondono ai canali video del dispositivo con supporto PTZ.

Create (Crea): Fare clic per salvare le impostazioni e creare il profilo.

Cancel (Annulla): Fare clic per annullare la configurazione e cancellare tutte le impostazioni.

profile_x (profilo_x): Fare clic sul nome del profilo per aprire e modificare il profilo preconfigurato.

Rilevatori

Shock detection (Rilevamento urti)

Shock detector (Rilevatore urti): Attiva per generare un allarme se il dispositivo viene colpito da un oggetto o manomesso.

Sensitivity level (Livello di sensibilità): Sposta il cursore per regolare il livello di sensibilità in base al quale il dispositivo deve generare un allarme. Un valore basso indica che il dispositivo genera un allarme solo se l'urto è potente. Un valore elevato significa che il dispositivo genera un allarme anche solo con un urto di media entità.

Accessori

I/O ports (Porte I/O)

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

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

Port (Porta)

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

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

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

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

Nota

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

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

Edge-to-edge

Audio pairing (Associazione audio) consente di utilizzare un altoparlante di rete Axis compatibile come se fosse parte del dispositivo principale. Una volta associato, l'altoparlante di rete funge da dispositivo di uscita audio in cui è possibile riprodurre clip audio e trasmettere suoni.

Importante

Affinché funzioni con un software per la gestione video (VMS), è necessario prima associare il dispositivo all'altoparlante di rete, quindi aggiungere il dispositivo al VMS.

Impostare un limite "Attesa tra le azioni (hh:mm:ss)" nella regola di evento quando si utilizza un dispositivo audio associato di rete in una regola di evento con "Rilevamento di suoni" come condizione e "Riproduci clip audio" come azione. Questo consentirà di evitare il rilevamento di un loop se il microfono in uso rileva l'audio dall'altoparlante.

Associazione audio

Address (Indirizzo): inserire il nome host o l'indirizzo IP dell'altoparlante di rete.

Username (Nome utente): inserire il nome utente.

Password: inserire la password per l'utente.

Speaker pairing (Associazione altoparlanti): Selezionare per associare un altoparlante di rete.

Clear fields (Cancella campi): fare clic per cancellare il contenuto di tutti i campi.

Connect (Connetti): fare clic per stabilire la connessione all'altoparlante.

PTZ pairing (Associazione PTZ) consente di associare un radar a una telecamera PTZ per utilizzare il tracking automatico. Il tracking automatico fa sì che la telecamera PTZ monitori gli oggetti in base alle informazioni provenienti dal radar sulle posizioni degli oggetti.

PTZ pairing (Associazione PTZ)

Address (Indirizzo): Inserire il nome host o l'indirizzo IP della telecamera PTZ.

Username (Nome utente): inserire il nome utente della telecamera PTZ.

Password: inserire la password della telecamera PTZ.

Clear fields (Cancella campi): fare clic per cancellare il contenuto di tutti i campi.

Connect (Connetti): fare clic per stabilire la connessione alla telecamera PTZ.

Configure radar autotracking (Configurazione del tracking automatico del radar): fare clic per aprire e configurare il tracking automatico. È inoltre possibile andare a **Radar > Autotracking (Radar > Tracking automatico)** per eseguire la configurazione.

Registri

Report e registri

Reports (Report)

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

Logs (Registri)

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

Network trace (Analisi della rete)

Importante

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

Un file di analisi della rete può facilitare la risoluzione dei problemi registrando l'attività sulla rete.

Trace time (Tempo di analisi): Selezionare la durata dell'analisi in secondi o minuti e fare clic su **Download**.

Registro di sistema remoto

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

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

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

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

- Axis
- RFC 3164
- RFC 5424

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

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

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

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

Configurazione normale

La configurazione normale è per utenti avanzati con esperienza nella configurazione di dispositivi Axis. La maggior parte dei parametri può essere impostata e modificata da questa pagina.

Manutenzione

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

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

Importante

Dopo il ripristino, le uniche impostazioni salvate sono:

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

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

Nota

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

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

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

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

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

Convalida la tua installazione

Convalida l'installazione del radar

Nota

Questo test ti aiuta nella convalida dell'installazione nelle condizioni attuali. I cambiamenti nella scena possono influenzare le prestazioni quotidiane della tua installazione.

Il radar è pronto all'uso appena installato, ciononostante consigliamo l'esecuzione di una convalida prima di cominciare a usarlo. In questo modo è possibile aumentare la precisione del radar consentendo di identificare eventuali problemi durante l'installazione o gestire gli oggetti (come alberi e superfici riflettenti) nella scena.

Per prima cosa *Calibrazione del radar alla pagina 17* prima di tentare la convalida.

È bene eseguire la convalida ogni volta che:

- Sono presenti oggetti nella scena che vuoi escludere affinché nelle zone possano esserci determinati oggetti come vegetazione o superfici in metallo.
- Il radar viene associato a una telecamera PTZ e si desidera configurare **Radar autotracking (Tracking automatico radar)**.
- L'altezza di montaggio del radar è cambiata.

Convalida del radar

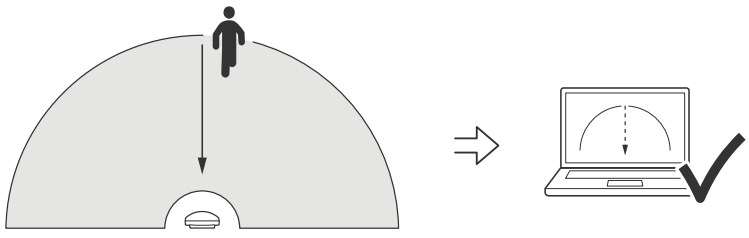
Check that there are no false detections (Controlla che non ci siano falsi rilevamenti)

1. Verifica che la zona di rilevamento sia sgombra di attività umana.
2. Attendi qualche minuto per accertarti che il radar non stia rilevando oggetti statici nella zona di rilevamento.
3. Nel caso non avvengano rilevamenti indesiderati, puoi saltare il passaggio 4.
4. In caso di rilevamenti indesiderati, scopri in che modo si filtrano certi tipi di movimento od oggetti, si modifica la copertura o si regola la sensibilità di rilevamento su *Ridurre al minimo i falsi allarmi alla pagina 20*.

Check for the correct symbol and direction of travel when the radar is approached from the front (Verifica che il simbolo e la direzione di viaggio siano esatti quando il radar viene avvicinato da davanti)

1. Accedi all'interfaccia web del radar e registra la sessione. Per ottenere aiuto in questo, vai a *Registrare e guardare video alla pagina 22*.
2. Comincia a 60 m davanti al radar e cammina direttamente verso il radar.
3. Controlla la sessione sull'interfaccia web del radar. Quando ti rileverà, dovrebbe apparire il simbolo di una classificazione umana.
4. Controlla che l'interfaccia web del radar mostri la direzione di viaggio esatta.

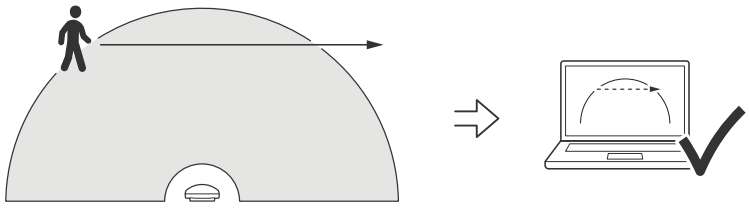
Convalida la tua installazione



Check for the correct symbol and direction of travel when the radar is approached from the front (Verifica che il simbolo e la direzione di viaggio siano esatti quando il radar viene avvicinato lateralmente)

1. Accedi all'interfaccia web del radar e registra la sessione. Per ottenere aiuto in questo, vai a *Registrare e guardare video alla pagina 22*.
2. Parti a 60 m dal radar e attraversa la sua area di copertura camminando dritto.
3. Verifica che l'interfaccia web del radar mostri il simbolo per una classificazione umana.
4. Controlla che l'interfaccia web del radar mostri la direzione di viaggio esatta.

Convalida la tua installazione



Crea una tabella simile a quella mostrata sotto per permettere la registrazione dei dati della tua convalida.

Testare	Superato/Fallito	Commento
1. Controlla che non avvengano rilevamenti indesiderati quando l'area è sgombra		
2a. Controlla che il rilevamento dell'oggetto avvenga con il simbolo corretto di "Umano" quando il radar viene avvicinato da davanti		

2b. Controlla che la direzione di viaggio sia esatta quando il radar viene avvicinato da davanti		
3a. Controlla che il rilevamento dell'oggetto avvenga con il simbolo corretto di "Umano" quando il radar viene avvicinato lateralmente		
3b. Controlla che la direzione di viaggio sia esatta quando il radar viene avvicinato lateralmente		

Completa la convalida

Quando avrai completato in modo esatto la prima parte della convalida, esegui le seguenti verifiche per il completamento del processo di convalida.

1. Accertati di aver eseguito la configurazione del tuo radar e aver seguito le istruzioni.
2. Per un'ulteriore convalida, aggiungi e calibra una mappa di riferimento.
3. Imposta lo scenario radar perché si attivi quando è rilevato un oggetto appropriato. Per impostazione predefinita, **seconds until trigger (secondi fino all'attivazione)** è impostato a due secondi, ma puoi modificare ciò nell'interfaccia web se serve.
4. Imposta il radar in modo che registri i dati quando è rilevato un oggetto appropriato.

   Per ottenere istruzioni, consultare *Registrare e guardare video alla pagina 22*.
5. Imposta la **trail lifetime (durata del percorso)** su un'ora affinché superi il tempo che ti serve per lasciare il tuo posto, camminare intorno all'area di sorveglianza e tornare al tuo posto. La **trail lifetime (durata del percorso)** terrà il tracciamento nella visualizzazione in diretta del radar per il tempo impostato e, una volta finita la convalida, potrai disabilitarla.
6. Cammina lungo il bordo dell'area di copertura del radar e accertati che il percorso sul sistema sia corrispondente a quello che hai percorso.
7. Se i risultati della convalida non ti soddisfano, calibra di nuovo la mappa di riferimento e ripeti la convalida.

Ulteriori informazioni

Streaming e archiviazione

Formati di compressione video

La scelta del metodo di compressione da utilizzare in base ai requisiti di visualizzazione e dalle proprietà della rete. Le opzioni disponibili sono:

Motion JPEG

Motion JPEG o MJPEG è una sequenza video digitale costituita da una serie di singole immagini JPEG. Queste immagini vengono successivamente visualizzate e aggiornate a una velocità sufficiente per creare un flusso che mostri il movimento costantemente aggiornato. Affinché il visualizzatore percepisca un video contenente movimento, la velocità deve essere di almeno 16 fotogrammi di immagini al secondo. Il video full motion viene percepito a 30 (NTSC) o 25 (PAL) fotogrammi al secondo.

Il flusso Motion JPEG utilizza quantità considerevoli di larghezza di banda, ma offre un'eccellente qualità di immagine e l'accesso a ogni immagine contenuta nel flusso.

H.264 o MPEG-4 Parte 10/AVC

Nota

H.264 è una tecnologia con licenza. Il dispositivo Axis include una licenza client per la visualizzazione H.264. L'installazione di copie aggiuntive senza licenza del client non è consentita. Per acquistare altre licenze, contattare il rivenditore Axis.

H.264 può, senza compromettere la qualità di immagine, ridurre le dimensioni di un file video digitale di più dell'80% rispetto al formato Motion JPEG e del 50% rispetto ai formati MPEG precedenti. Ciò significa che per un file video sono necessari meno larghezza di banda di rete e di spazio di archiviazione. In altre parole, è possibile ottenere una qualità video superiore per una determinata velocità in bit.

H.265 o MPEG-H Parte 2/HEVC

H.265 può, senza compromettere la qualità di immagine, ridurre le dimensioni di un file video digitale di più del 25% rispetto a H.264.

Nota

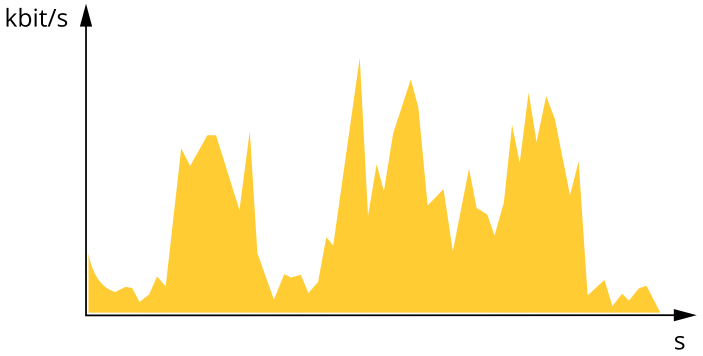
- H.265 è una tecnologia con licenza. Il dispositivo Axis include una licenza client per la visualizzazione H.265. L'installazione di copie aggiuntive senza licenza del client non è consentita. Per acquistare altre licenze, contattare il rivenditore Axis.
- La maggioranza dei browser non è dotata di supporto per la decodifica H.265 e per tale ragione l'interfaccia Web della telecamera non la supporta. Invece puoi utilizzare un'applicazione o un sistema di gestione video che supporta la codifica H.265.

Controllo velocità di trasmissione

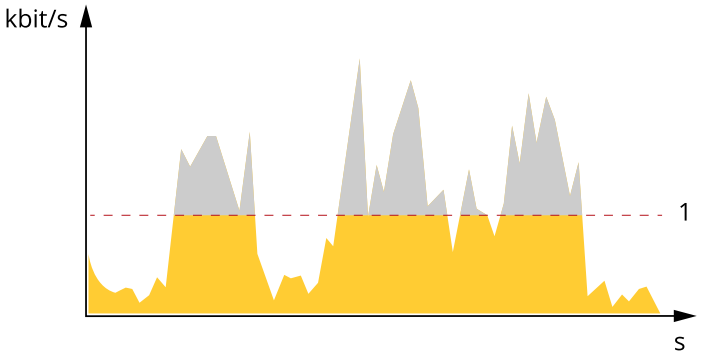
Il controllo della velocità di trasmissione aiuta a gestire il consumo di banda del flusso video.

Velocità di trasmissione variabile (VBR)
La velocità di trasmissione variabile consente al consumo di banda di variare in base al livello di attività nella scena. Più attività c'è, più larghezza di banda sarà necessaria. Con la velocità di trasmissione variabile sarà assicurata una qualità di immagine costante, ma devi accertarti di disporre di margini di archiviazione.

Ulteriori informazioni



Velocità di trasmissione massima (MBR)
La velocità di trasmissione massima ti permette di impostare una velocità di trasmissione di destinazione per gestire le limitazioni della velocità di trasmissione nel sistema. È possibile che si riduca la qualità d'immagine o la velocità in fotogrammi quando la velocità di trasmissione istantanea viene mantenuta sotto la velocità di trasmissione di destinazione specificata. È possibile scegliere di dare priorità alla qualità dell'immagine o alla velocità in fotogrammi. Si consiglia di configurare la velocità di trasmissione di destinazione a un valore superiore rispetto a quella prevista. Così avrai un margine in caso di elevato livello di attività nella scena.

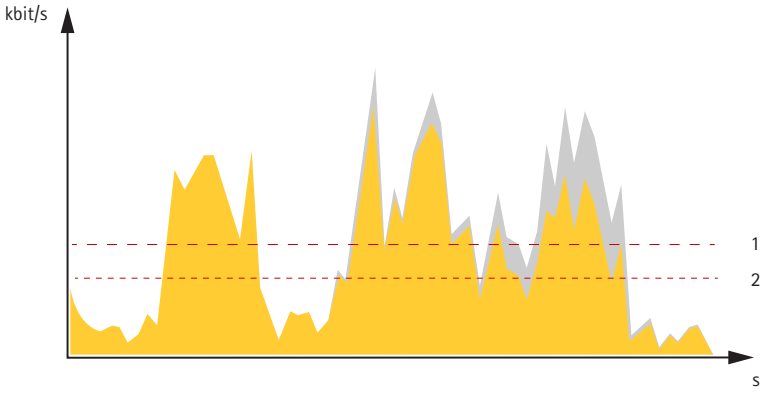


1 Velocità di trasmissione di destinazione

Velocità di trasmissione media (ABR)
Con velocità di trasmissione media, la velocità di trasmissione viene regolata automaticamente su un periodo di tempo più lungo. In questo modo è possibile soddisfare la destinazione specificata e fornire la qualità video migliore in base all'archiviazione disponibile. La velocità di trasmissione è maggiore in scene con molta attività, rispetto alle scene statiche. Hai più probabilità di ottenere una migliore qualità di immagine in scene con molta attività se usi l'opzione velocità di trasmissione media. È possibile definire l'archiviazione totale necessaria per archiviare il flusso video per un determinato periodo di tempo (tempo di conservazione) quando la qualità dell'immagine viene regolata in modo da soddisfare la velocità di trasmissione di destinazione specificata. Specificare le impostazioni della velocità di trasmissione medie in uno dei modi seguenti:

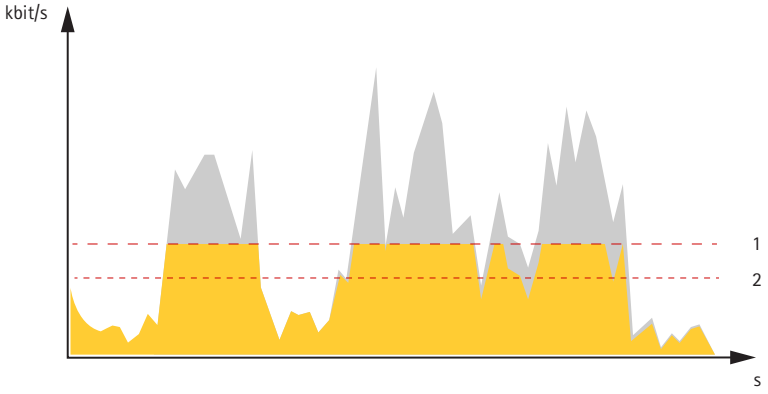
- Per calcolare la necessità di archiviazione stimata, impostare la velocità di trasmissione di destinazione e il tempo di conservazione.
- Per calcolare la velocità di trasmissione media in base allo spazio di archiviazione disponibile e al tempo di conservazione richiesto, utilizzare il calcolatore della velocità di trasmissione di destinazione.

Ulteriori informazioni



1 *Velocità di trasmissione di destinazione*
2 *Velocità di trasmissione media effettiva*

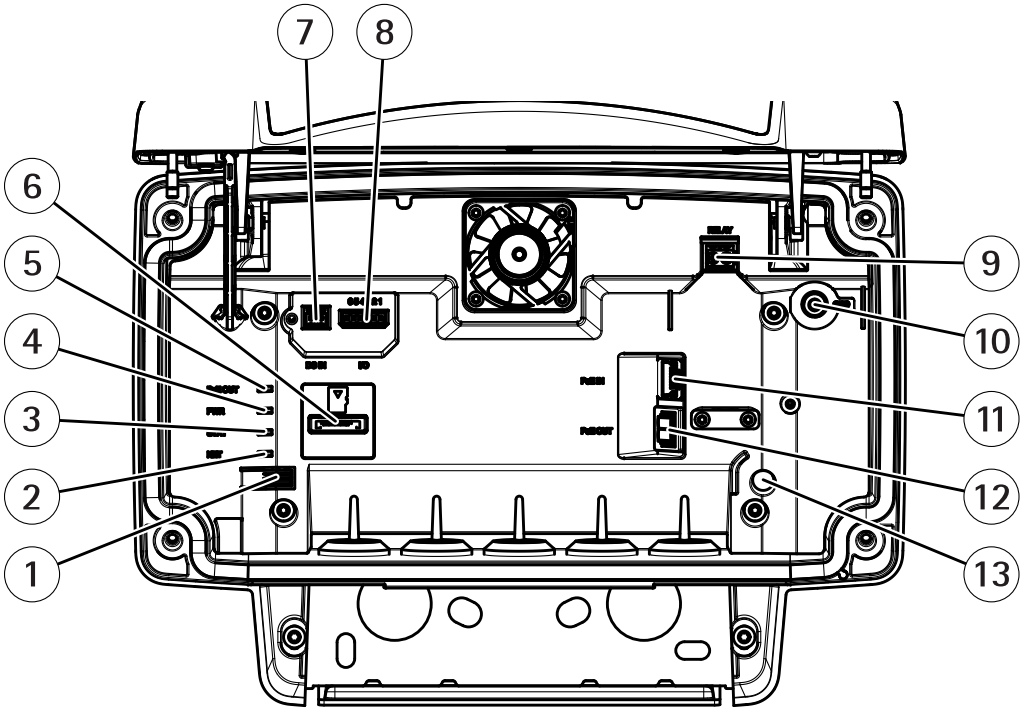
È inoltre possibile attivare la velocità di trasmissione massima e specificare una velocità di trasmissione di destinazione nell'opzione velocità di trasmissione media.



1 *Velocità di trasmissione di destinazione*
2 *Velocità di trasmissione media effettiva*

Specifiche

Panoramica del dispositivo



1 *Pulsante di comando*
2 *LED di rete*
3 *LED di stato*
4 *Power LED*
5 *LED uscita PoE*
6 *Slot per scheda microSD*
7 *Connettore di alimentazione (CC)*
8 *Connettore I/O*
9 *Connettore relè*
10 *Vite di messa a terra*
11 *Connettore di rete (PoE in)*
12 *Connettore di rete (PoE out)*
13 *Sensore allarme anti intrusione*

Per le specifiche tecniche, consultare *Specifiche alla pagina 65*.

Indicatori LED

LED di stato	Indicazione
Verde	Luce verde fissa: condizioni di normale utilizzo.

LED di rete	Indicazione
Verde	Luce fissa per connessione di rete a 100 Mbit/s. Luce lampeggiante: attività di rete.

Giallo	Luce fissa per connessione di rete a 10 Mbit/s. Luce lampeggiante: attività di rete.
Spento	Assenza di connessione.

LED di alimentazione	Indicazione
Verde	Funzionamento normale.

LED uscita PoE	Indicazione
Spento	Uscita PoE spenta
Verde	Uscita PoE accesa

Slot per schede di memoria

Questo dispositivo supporta schede microSD/microSDHC/microSDXC.

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

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

Pulsanti

Pulsante di comando

Per l'ubicazione del pulsante di comando, consultare *Panoramica del dispositivo alla pagina 65*.

Il pulsante di comando viene utilizzato per:

- Ripristinare le impostazioni predefinite di fabbrica del dispositivo. Consultare *pagina 70*.
- Collegarsi a un servizio AXIS Video Hosting System. Consultare . Per il collegamento, premere e tenere premuto il tasto per circa 3 secondi fino a quando il LED di stato lampeggia in verde.

Connettori

Connettore di rete

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

ATTENZIONE

Rischio di danni al dispositivo. Non alimentare il dispositivo sia con PoE che con CC.

Connettore di rete (PoE out)

Power over Ethernet IEEE 802.3at tipo 2, max 30 W

Utilizzare questo connettore per alimentare un altro dispositivo PoE, ad esempio una telecamera, un altoparlante a tromba o un secondo radar Axis.

Nota

L'uscita PoE è abilitata quando il radar è alimentato da un midspan 60 W (Power over Ethernet IEEE 802.3bt, tipo 3).

Specifiche

Nota

Se il radar è alimentato da un midspan 30 W o dall'alimentazione CC, l'uscita PoE è disattivata.

Nota

La lunghezza massima del cavo Ethernet è complessivamente pari a 100 m per l'uscita e l'ingresso PoE in combinazione. È possibile incrementarla con un amplificatore PoE.

Nota

Se il dispositivo PoE collegato richiede più di 30 W, è possibile aggiungere un midspan da 60 W tra la porta di uscita PoE sul radar e il dispositivo. Il midspan alimenterà il dispositivo mentre il radar di sicurezza fornirà la connessione Ethernet.

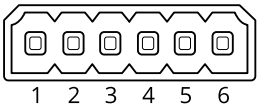
Connettore I/O

Utilizzare il connettore I/O con dispositivi esterni in combinazione con, ad esempio, attivazione di eventi e notifiche di allarme. Oltre al punto di riferimento 0 V CC e all'alimentazione (output 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 rilevatori di rottura.

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

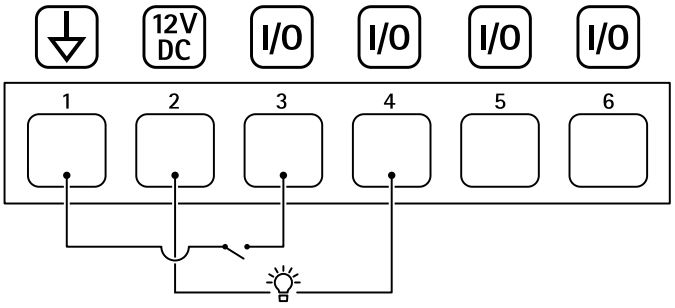
Morsettiera a 6 pin



Funzione	Pin	Note	Specifiche
Terra CC	1		0 V CC
Output CC	2	Può essere utilizzato per alimentare una periferica ausiliaria. Nota: questo pin può essere usato solo come uscita alimentazione.	12 V CC Carico massimo = 50 mA
Configurabile (input o output)	3–6	Ingresso digitale - collegare al pin 1 per l'attivazione oppure lasciare isolato (scollegato) per la disattivazione.	Da 0 a max 30 V CC
		Uscita digitale - collegato internamente al pin 1 (ground CC) quando attivo e isolato (scollegato) quando inattivo. Se utilizzata con un carico induttivo, ad esempio un relè, collegare un diodo in parallelo al carico per proteggere il dispositivo da sovratensioni.	Da 0 a max 30 V CC, open drain, 100 mA

Esempio:

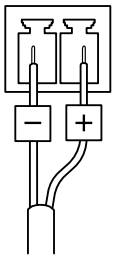
Specifiche



1 *Ground CC*
2 *Output CC 12 V, max 50 mA*
3 *I/O configurato come input*
4 *I/O configurato come output*
5 *I/O configurabile*
6 *I/O configurabile*

Connettore di alimentazione

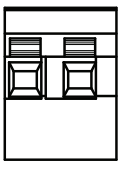
Morsettiera a 2 pin per ingresso alimentazione CC. Utilizzare una sorgente di alimentazione limitata (LPS) compatibile con una bassissima tensione di sicurezza (SELV) con una potenza di uscita nominale limitata a ≤100 W o una corrente nominale di uscita limitata a ≤5 A.



⚠ATTENZIONE

Rischio di danni al dispositivo. Non alimentare il dispositivo sia con PoE che con CC.

Connettore relè



⚠ATTENZIONE

Utilizzare cavi principali singoli per il connettore del relè.

Funzione	Specifiche
Tipo	Normalmente aperto
Classificazione	24 V CC/5 A
Isolamento da un altro circuito	2,5 kV

Consigli per la pulizia

Se il dispositivo si macchia di grasso o diventa molto sporco, è possibile pulirlo con sapone o detergente delicato e senza solventi.

AVVISO

Non utilizzare mai detergenti aggressivi, ad esempio benzina, benzene o acetone.

1. Utilizzare una bomboletta d'aria compressa per rimuovere polvere o sporcizia dal dispositivo.
2. Pulire il dispositivo con un panno morbido inumidito con un detergente delicato e acqua tiepida.
3. Strofinare accuratamente con un panno asciutto.

Nota

Evitare la pulizia alla luce diretta del sole o a temperature elevate, poiché ciò potrebbe causare macchie quando le goccioline d'acqua si asciugano.

Risoluzione di problemi

Ripristino delle impostazioni predefinite di fabbrica

Importante

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

Per ripristinare il dispositivo ai valori predefiniti di fabbrica:

1. Scollegare l'alimentazione dal dispositivo.
2. Tenere premuto il pulsante di comando quando si ricollega l'alimentazione. Consultare *Panoramica del dispositivo alla pagina 65*.
3. Tenere premuto il pulsante di comando per 15–30 secondi finché l'indicatore LED di stato non lampeggia in giallo.
4. Rilasciare il pulsante di comando. Il processo è completo quando l'indicatore del LED di stato diventerà verde. Il dispositivo è stato reimpostato alle impostazioni di fabbrica predefinite. Se nessun server DHCP è disponibile sulla rete, l'indirizzo IP predefinito è `192.168.0.90`.
5. Utilizzare gli strumenti per l'installazione e la gestione del software per assegnare un indirizzo IP, impostare la password e accedere al dispositivo.

   Gli strumenti per l'installazione e la gestione del software sono disponibili nelle pagine dedicate all'assistenza sul sito Web *axis.com/support*.

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

Controllo della versione firmware corrente

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

Per controllare il firmware corrente:

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

Aggiornamento del firmware

Importante

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

Nota

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

1. Scarica il file del firmware sul tuo computer, disponibile gratuitamente su *axis.com/support/device-software*.

2. Accedi al dispositivo come amministratore.
3. Andare a **Maintenance > Firmware upgrade (Manutenzione > Aggiornamento firmware)** e fare clic su **Upgrade (Aggiorna)**.

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

Problemi tecnici, indicazioni e soluzioni

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

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

Problemi durante l'impostazione dell'indirizzo IP	
Il dispositivo si trova su una subnet diversa	Se l'indirizzo IP destinato al dispositivo e l'indirizzo IP del computer utilizzato per accedere al dispositivo si trovano in subnet diverse, non è possibile impostare l'indirizzo IP. Contattare l'amministratore di rete per ottenere un indirizzo IP.
L'indirizzo IP è già utilizzato da un altro dispositivo	Scollegare il dispositivo Axis dalla rete. Eseguire il comando ping (in una finestra di comando/DOS digitare `ping` e l'indirizzo IP del dispositivo): • Se si riceve: `Reply from <IP address>: bytes=32; time=10...` significa che l'indirizzo IP potrebbe già essere utilizzato da un altro dispositivo nella rete. Contattare l'amministratore di rete per un nuovo indirizzo IP e reinstallare il dispositivo. • Se si riceve: `Request timed out` significa che l'indirizzo IP può essere utilizzato con il dispositivo Axis. Controllare tutti i cablaggi e reinstallare il dispositivo.
Possibile conflitto dell'indirizzo IP con un altro dispositivo nella stessa subnet	Prima che il server DHCP imposti un indirizzo dinamico viene utilizzato l'indirizzo IP statico del dispositivo Axis. Ciò significa che se lo stesso indirizzo IP statico viene utilizzato anche da un altro dispositivo, si potrebbero verificare dei problemi durante l'accesso al dispositivo.

Impossibile accedere al dispositivo da un browser	
Non è possibile eseguire l'accesso	Se HTTPS è abilitato, assicurarsi di utilizzare il protocollo corretto (HTTP o HTTPS) quando si tenta di eseguire l'accesso. Potrebbe essere necessario digitare manualmente `http` o `https` nel campo dell'indirizzo del browser. Se si dimentica la password per l'account root, il dispositivo deve essere ripristinato alle impostazioni predefinite di fabbrica. Vedere *Ripristino delle impostazioni predefinite di fabbrica alla pagina 70*.

L'indirizzo IP è stato modificato dal server DHCP	Gli indirizzi IP ottenuti da un server DHCP sono dinamici e potrebbero cambiare. Se l'indirizzo IP è stato modificato, utilizzare AXIS IP Utility o AXIS Device Manager per individuare il dispositivo sulla rete. Identificare il dispositivo utilizzando il relativo numero di serie o modello oppure il nome DNS (se è stato configurato). Se necessario, è possibile assegnare manualmente un indirizzo IP statico. Per istruzioni, vedere *axis.com/support*.
Errore del certificato durante l'utilizzo di IEEE 802.1X	Per un corretto funzionamento dell'autenticazione, le impostazioni della data e dell'ora nel dispositivo Axis devono essere sincronizzate con un server NTP. Andare a **System > Date and time (Sistema > Data e ora)**.

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

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

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

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

Impossibile collegarsi tramite la porta 8883 con MQTT su SSL

Il firewall blocca il traffico utilizzando la porta 8883 poiché è insicuri.	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 la rete ALPN, l'uso di MQTT può essere negoziato su una porta aperta, ad esempio 443. Controllare con il provider del server/broker se è supportato ALPN e quale protocollo e porta ALPN utilizzare.

Considerazioni sulle prestazioni

Durante la configurazione del sistema, è importante considerare come le varie impostazioni e situazioni influiscono sulla quantità di larghezza di banda (velocità di trasmissione) necessaria.

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

- Un utilizzo eccessivo della rete dovuto a una scarsa infrastruttura influisce sulla larghezza di banda.

Manuale per l'utente
AXIS D2110-VE Security Radar

Ver. M21.3
Data: Gennaio 2024
Codice art. T10145149