AXIS Perimeter Defender

AXIS Perimeter Defender
AXIS Perimeter Defender PTZ Autotracking

Manuale dell'utente

Indice

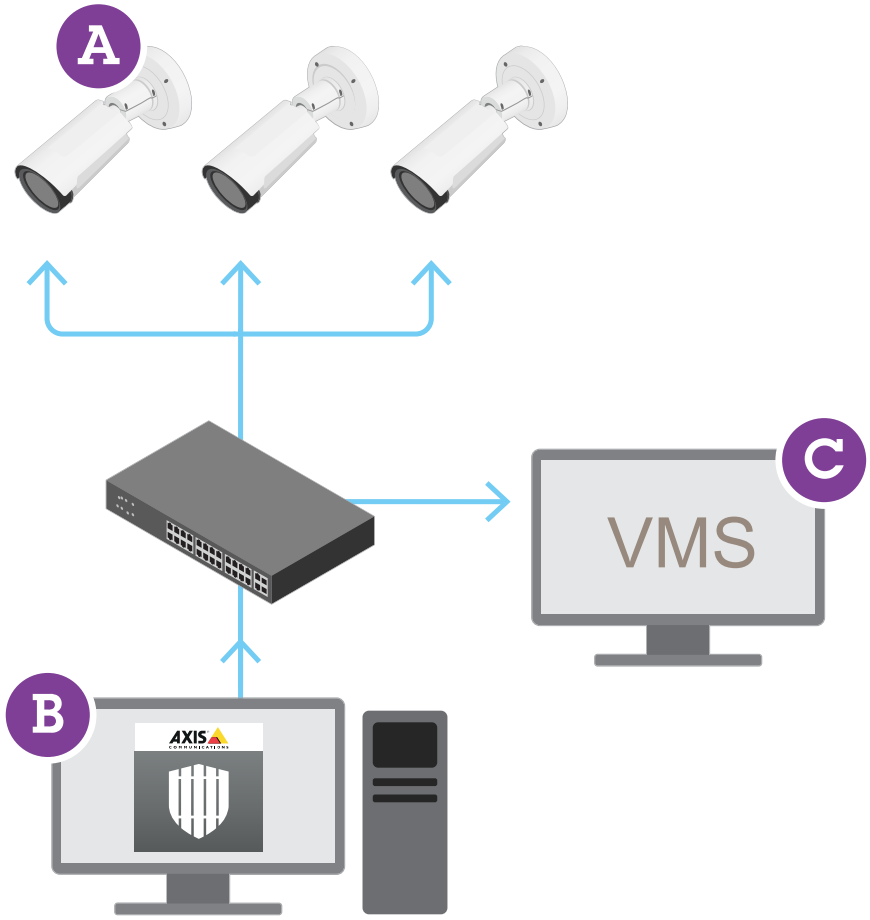
AXIS Perimeter Defender

AXIS Perimeter Defender è un'applicazione per la sorveglianza perimetrale e la protezione. È ideale per la protezione perimetrale ad alta sicurezza in cui è necessario rafforzare il sistema di controllo degli accessi fisico con un rilevamento affidabile delle intrusioni.

AXIS Perimeter Defender è progettato principalmente per la protezione della cosiddetta zona sterile, ad esempio lungo una recinzione che contrassegna un confine. Il termine zona sterile si riferisce a un'area in cui non dovrebbero esserci le persone.

Utilizzare AXIS Perimeter Defender in un ambiente esterno per:

- rilevare le persone in movimento.
- rilevare i veicoli in movimento, senza discriminare tra i tipi di veicoli.



Questa telecamera è in grado di eseguire l'applicazione in modalità calibrazione, AI o in entrambe combinate. Se si sceglie di eseguirla solo in modalità IA, il montaggio della telecamera è più flessibile e non è necessario calibrare le telecamere.

AXIS Perimeter Defender è costituito da un'interfaccia desktop (B), da cui si installa e si configura l'applicazione sulle telecamere (A). È quindi possibile configurare il sistema per l'invio di allarmi al software di gestione video (C).

AXIS Perimeter Defender PTZ Autotracking è un plugin per l'applicazione AXIS Perimeter Defender che utilizza la stessa interfaccia desktop. Con il plugin, si accoppia una telecamera visiva fissa o termica con una telecamera Axis Q-line PTZ. È quindi possibile mantenere la copertura di rilevamento continuo di una scena con la

telecamera fissa, mentre la telecamera PTZ traccia automaticamente e fornisce una visione più ravvicinata degli oggetti rilevati.

Importante

AXIS Perimeter Defender PTZ Autotracking richiede la calibrazione di entrambe le telecamere fisse e PTZ.

AXIS Perimeter Defender offre i seguenti tipi di scenari di rilevamento:

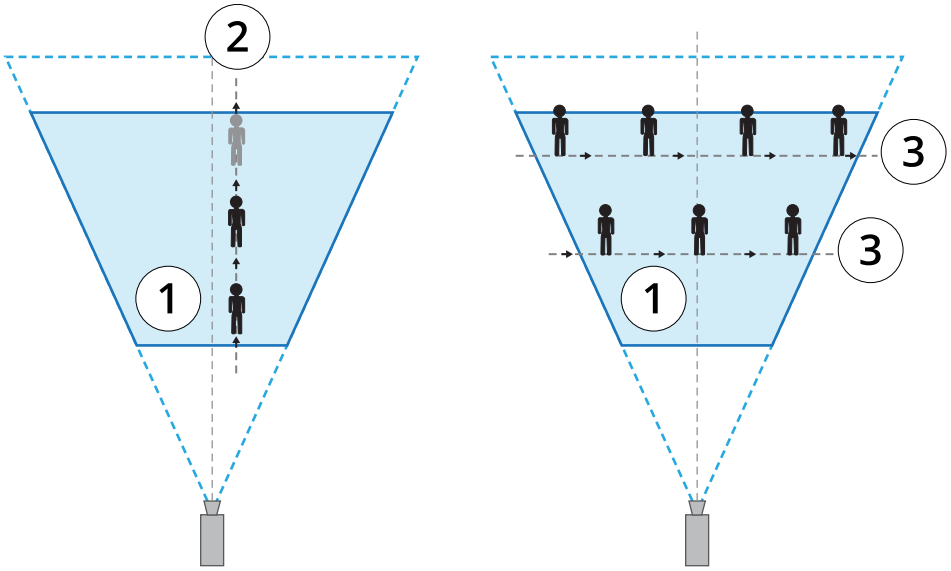
- **Intrusione**: attiva un allarme quando una persona o un veicolo entra in una zona definita a terra (da qualsiasi direzione e con qualsiasi traiettoria).
- **Movimenti sospetti**: attiva un allarme quando una persona o un veicolo rimane in una zona definita a terra per un numero di secondi più elevato rispetto a quello predefinito.
- **Attraversamento zone**: attiva un allarme quando una persona o un veicolo passa attraverso due o più zone definite a terra in una determinata sequenza.
- **Condizionale**: attiva un allarme quando una persona o un veicolo entra in una zona definita a terra senza prima passare attraverso un'altra zona o zone definite a terra.

Come funziona?

Rilevamento di oggetti

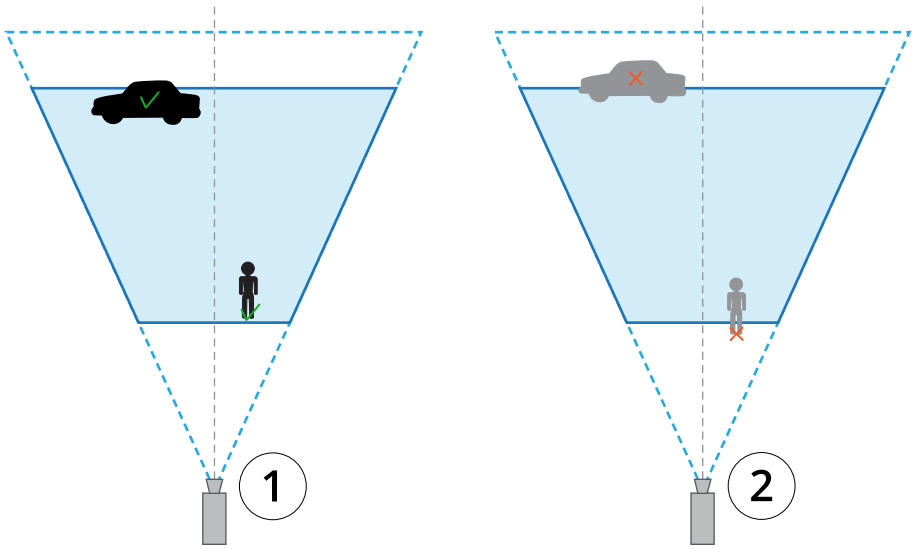
AXIS Perimeter Defender è in grado di rilevare persone o veicoli in movimento. Da rilevare:

- Una persona o un veicolo deve essere completamente visibile nella zona di rilevamento per almeno tre secondi.
- Un veicolo può essere lungo fino a 12 metri (39,4 piedi). (Con la modalità IA non c'è una lunghezza massima)
- Persone o veicoli devono essere visibilmente in movimento nel campo visivo della telecamera. Questo significa che l'area di rilevamento di una persona che si avvicina o si allontana dalla telecamera in linea retta è inferiore rispetto a una persona che cammina perpendicolarmente al campo visivo della telecamera.



1 *Zona di rilevamento*
2 *Persona che si allontana dalla telecamera*
3 *Persone che camminano perpendicolarmente al campo visivo della telecamera*

- Il punto di rilevamento deve trovarsi all'interno della zona di rilevamento. Il punto di rilevamento si trova ai piedi di una persona o al centro di un veicolo.



1 Punto di rilevamento all'interno della zona di rilevamento
2 Punto di rilevamento fuori dalla zona di rilevamento

Dopo il rilevamento, AXIS Perimeter Defender continua a seguire la persona o il veicolo anche se è parzialmente nascosta/o, ad esempio nel caso in cui il corpo di una persona sia nascosto dietro un'auto, ma la testa sia ancora visibile.

Se una persona o un veicolo rilevata/o smette di muoversi per alcuni secondi, AXIS Perimeter Defender smette di tracciarlo. Se ricominciano a muoversi dopo meno di 15 secondi, l'applicazione continua a monitorarli. Se la persona si trovava in una zona di attraversamento, non vi è alcuna garanzia che lo scenario si attivi correttamente.

Come funziona PTZ Autotracking?

In AXIS Perimeter Defender PTZ Autotracking, una telecamera fissa e una telecamera PTZ lavorano insieme. Quando la telecamera fissa rileva le persone o i veicoli in movimento, invia i dati di posizione degli oggetti alla telecamera PTZ associata. Finché gli oggetti rimangono all'interno del campo visivo della telecamera fissa, la telecamera PTZ è in grado di seguirli automaticamente e di regolare il livello di zoom per mantenerli nella visuale.

Condizioni in cui i rilevamenti possono essere ritardati o persi

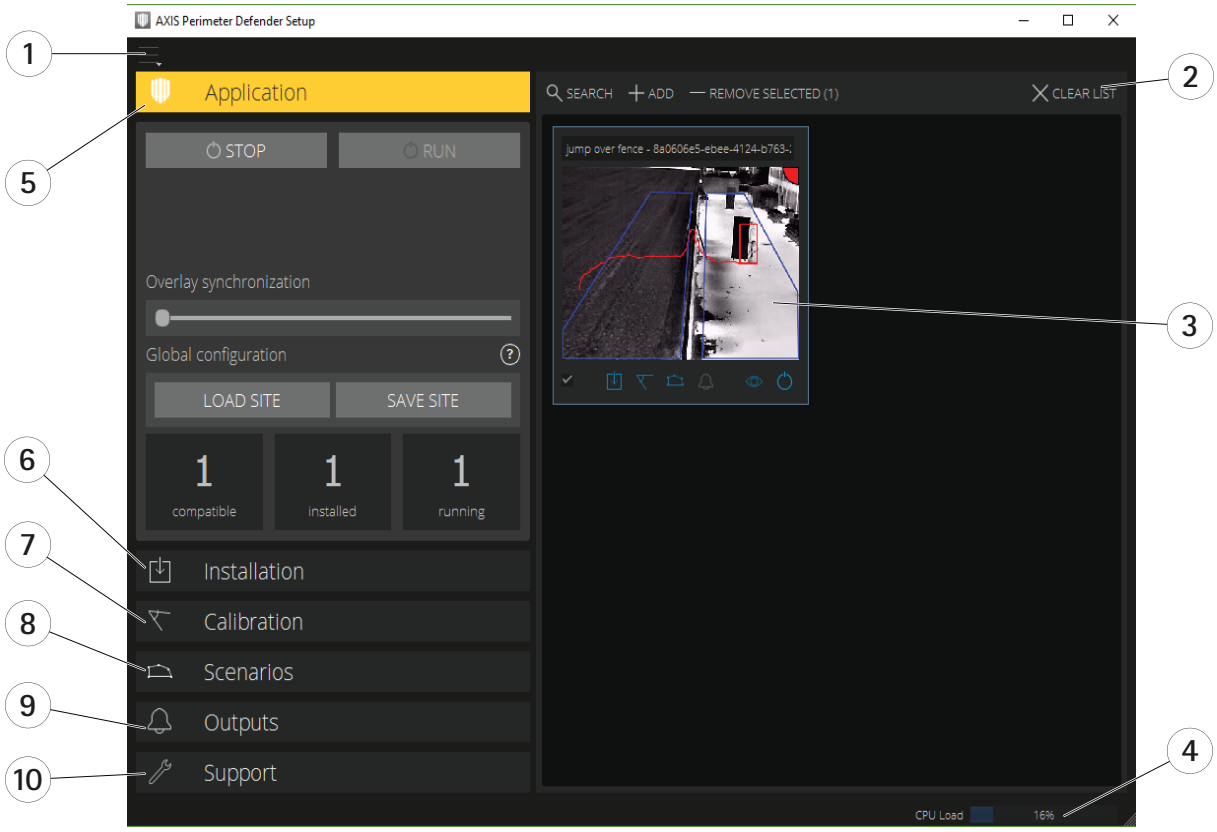
- Nebbia
- Luce che colpisce direttamente la telecamera
- Luce inadeguata
- Immagine troppo disturbata

Situazioni che possono attivare falsi allarmi

- Persone o veicoli parzialmente nascosti. Ad esempio, un piccolo furgone che appare da dietro un muro può apparire come una persona poiché la parte visibile è alta e stretta.
- Insetti sull'obiettivo della telecamera. Si ricorda che le telecamere per le riprese diurne e notturne con luci a infrarossi attirano insetti e ragni.
- Una combinazione di fari d'auto e pioggia battente.
- Animali di stazza grande simile a quella umana, soprattutto se sono stati selezionati i tipi di approccio aggiuntivi "persone accovacciate o che strisciano" o se è stato selezionato il rotolamento nella scheda **Scenarios (Scenari)** .
- Luce intensa che causa ombre.

L'interfaccia utente

L'interfaccia di AXIS Perimeter Defender consente, ad esempio, di calibrare i dispositivi, configurare scenari ed eseguire azioni per più dispositivi. La configurazione remota è possibile ovunque sia disponibile un collegamento di rete.



1 *Impostazioni dell'interfaccia, on page 7*
2 *Gestire i dispositivi. Vedere Aggiunta di dispositivi, on page 17.*
3 *Visualizzazione in diretta, on page 8*
4 *Indicatore di carico della CPU. Vedere Carico CPU, on page 11.*
5 *Scheda applicazioni, on page 9*
6 *Scheda installazione, on page 10*
7 *Scheda di calibrazione, on page 10*
8 *Scheda scenari, on page 10*
9 *Scheda output, on page 11*
10 *Scheda assistenza, on page 11*

Impostazioni dell'interfaccia

Il menu delle impostazioni dell'interfaccia contiene:

Impostazioni cartella –

Percorso di configurazione del dispositivo: Selezionare la posizione in cui memorizzare i file temporanei e il video di calibrazione.

Percorso di configurazione del sito: selezionare la posizione in cui archiviare i file di configurazione dai percorsi di caricamento.

Password per la videocamera – Visualizza le password in uso e ne aggiunge di nuove. Le password non vengono memorizzate una volta che l'utente esce dall'applicazione.

Gestire i pacchetti di clip di dimostrazione – Importare o rimuovere le clip di dimostrazione.

Abilitare la modalità velocità in fotogrammi completa – Modificare la velocità in fotogrammi nella vista in tempo reale. Vedere *Carico CPU, on page 11*.

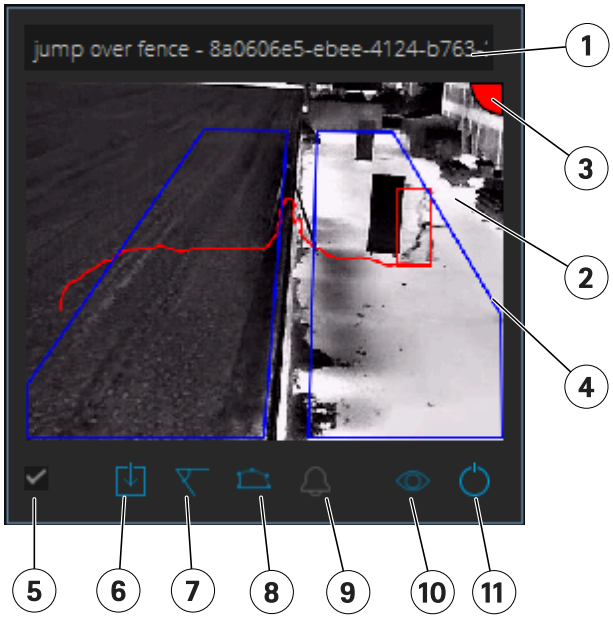
Piedi e pollici del display – Modificare le unità in unità metriche e imperiali.

Cambia lingua – Modificare la lingua nell'applicazione.

Informazioni su – Visualizzare la versione di AXIS Perimeter Defender Setup.

Visualizzazione in diretta

Ciascun dispositivo collegato ottiene una vista in tempo reale nell'interfaccia principale. La vista in tempo reale fornisce lo stato del dispositivo e rapido accesso alle principali funzioni.



1. Nome del dispositivo – Fare clic per modificare il nome del dispositivo. Include sempre l'indirizzo IP e il numero MAC del dispositivo. Passare il cursore del mouse sul nome per visualizzare le proporzioni utilizzate per l'analisi, che forniscono il campo visivo di copertura massimo e per vedere se il dispositivo usa una connessione remota.

2. Immagine in diretta – In modalità panoramica, la velocità in fotogrammi è di 1 fps. Fare doppio clic per ingrandire l'immagine e aumentare la velocità in fotogrammi a 8 fps.

3. Stato di allarme – Lo stato di allarme è visibile solo se la sovrapposizione è attiva e AXIS Perimeter Defender è installato, configurato e in esecuzione. Grigio significa che la funzionalità di allarme non è attiva o che le impostazioni di configurazione sono in caricamento. Verde significa che la funzionalità di allarme è attiva. Rosso significa che è stato attivato un allarme.

4. Zone di rilevamento – Le zone di rilevamento sono visibili solo se la sovrapposizione è attiva e AXIS Perimeter Defender è installato, configurato e in esecuzione.

5. Casella di controllo per la selezione – Per poter selezionare più dispositivi, utilizzare questa casella di controllo.

6. Stato dell'installazione e pulsante di accesso rapido – Passare il cursore del mouse per visualizzare la versione di AXIS Perimeter Defender installata sul dispositivo. Se l'icona viene sostituita da , significa che è disponibile una versione più recente. Fare clic per aprire la scheda Installazione per il dispositivo. Grigio indica che il dispositivo non è installato. Arancione indica che il dispositivo è installato ma non dispone di una licenza valida. Blu indica che il dispositivo è installato con una licenza valida.

7. Stato della calibrazione e pulsante di accesso rapido – Fare clic per aprire la scheda Calibrazione per il dispositivo. Grigio indica che il dispositivo non è calibrato. Blu indica che il dispositivo è calibrato.

8. Stato degli scenari e pulsante di accesso rapido – Fare clic per aprire la scheda Scenari per il dispositivo. Grigio indica che non è stato definito uno scenario. Blu indica che è stato definito almeno uno scenario.

9. Stato delle uscite e pulsante di accesso rapido – Fare clic per aprire la scheda Output per il dispositivo. Grigio indica che non sono configurate uscite. Blu indica che è stata configurata almeno un'uscita.

10. Stato sovrapposizione e pulsante di attivazione/disattivazione – Fare clic per attivare e disattivare la sovrapposizione. Grigio indica che la sovrapposizione è inattiva. Blu indica che la sovrapposizione è attiva. La sovrapposizione viene visualizzata come un riquadro attorno agli oggetti rilevati e una "sbavatura di lumaca" per la visualizzazione della traiettoria degli oggetti.

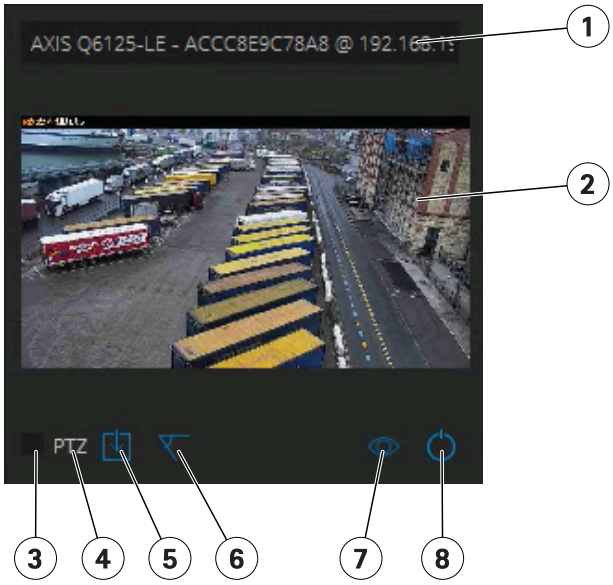
11. Stato dell'esecuzione e pulsante di attivazione/disattivazione – Fare clic per eseguire/arrestare l'applicazione sul dispositivo. Grigio indica che l'applicazione è stata arrestata. Blu indica che è in esecuzione.

Nota

La sovrapposizione è disponibile solo se è disponibile una connessione diretta dal dispositivo al computer dell'utente ovvero se non sono presenti firewall o simili che impediscono la connessione alla porta di sovrapposizione sul dispositivo.

Vista in tempo reale – PTZ Autotracking

La vista in tempo reale dei dispositivi con AXIS Perimeter Defender PTZ Autotracking è leggermente diversa dalla normale vista in tempo reale.



1 *Nome del dispositivo*
2 *Immagine in diretta*
3 *Casella di controllo per la selezione*
4 *Indica che il dispositivo utilizza AXIS Perimeter Defender PTZ Autotracking.*
5 *Stato dell'installazione e pulsante di accesso rapido*
6 *Stato della calibrazione e pulsante di accesso rapido*
7 *Stato sovrapposizione e pulsante di attivazione/disattivazione*
8 *Stato dell'esecuzione e pulsante di attivazione/disattivazione*

Scheda applicazioni

- **Run** (Esegui) - Avvia le analisi sui dispositivi selezionati.
- **Stop** (Arresta) - Arresta le analisi sui dispositivi selezionati.
- **Load Site (Carica sito)**: consente di caricare un sito salvato in precedenza, ovvero i dispositivi e i rispettivi file di configurazione
- **Save Site (Salvare sito)**: consente di salvare il sito corrente, cioè salvare tutte le informazioni sul dispositivo e i rispettivi file di configurazione

- **Overlay synchronization (Sincronizzazione sovrapposizione)** - controllo sulla sincronizzazione della sovrapposizione dei metadati di AXIS Perimeter Defender. Questo cursore controlla il ritardo tra la sovrapposizione dei metadati e le immagini ricevute per compensare lo streaming delle immagini più lento rispetto ai metadati. Il valore del cursore indica il ritardo impostato per la telecamera selezionata al momento. Se sono collegate più telecamere, il valore indicato è quello della prima telecamera selezionata. La modifica del valore del cursore cambia il ritardo per tutte le telecamere selezionate.

È inoltre possibile visualizzare il numero di dispositivi compatibili aggiunti, il numero totale di dispositivi con AXIS Perimeter Defender installato e il numero di dispositivi su cui è in esecuzione l'analisi.

Scheda installazione

- **Application: Install (Applicazione: installa)**: consente di installare l'applicazione sui dispositivi selezionati.
- **Application: Uninstall (Applicazione: disinstalla)**: consente di disinstallare l'applicazione sui dispositivi selezionati.
- **Licence: Install (Licenza: installa)**: consente di installare la licenza sui dispositivi selezionati.

Scheda di calibrazione

- **Automatic (Automatica)**: consente di eseguire una calibrazione automatica dei dispositivi selezionati.
- **Manual (Manuale)**: consente di eseguire una calibrazione manuale dei dispositivi selezionati.

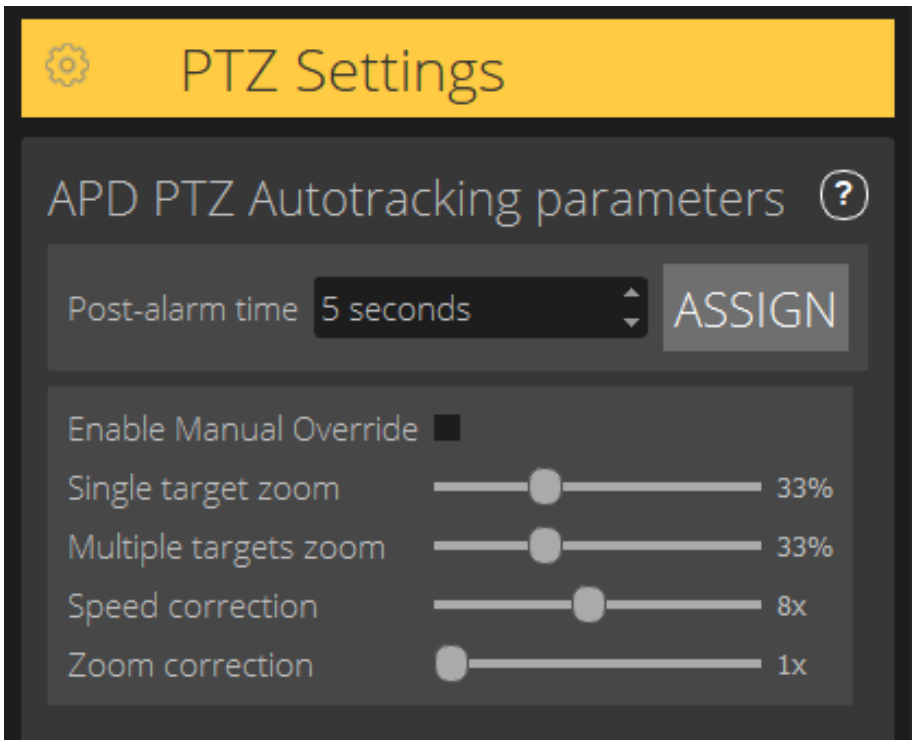
Scheda scenari

- **Global parameters (Parametri globali)**: si applicano a tutti gli scenari.
- **Advanced scenarios (Scenari avanzati)**: consente di creare scenari condizionali, di intrusioni, circolazione sospetta e attraversamento di zone.

Scheda impostazioni PTZ

Nota

Questa scheda viene visualizzata solo se si dispone del plug-in AXIS Perimeter Defender PTZ Autotracking.



- **Post-alarm time (Periodo post-allarme)**: definisce il tempo che deve passare perché la telecamera PTZ ritorni alla posizione iniziale, una volta che l'oggetto tracciato è scomparso dalla vista.
- **Enable manual override (Abilita sovrascrizione manuale)**: se è selezionata, l'operatore può assumere il controllo della telecamera PTZ con un joystick, nella VMS o nella pagina web della telecamera.
- **Single target zoom (Zoom su soggetto singolo)**: consente di regolare il livello di zoom per monitorare un singolo soggetto. Un valore più alto offre migliori possibilità di identificazione, ma aumenta anche il rischio di perdere oggetti in rapido movimento.
- **Multiple targets zoom (Zoom su soggetti multipli)**: consente di regolare il livello di zoom per il rilevamento di più soggetti.
- **Speed correction (Correzione della velocità)**: regolare la velocità di tracciamento per mantenere gli oggetti in rapido movimento centrati nell'immagine della telecamera PTZ. Si noti che un valore elevato può causare instabilità nel monitoraggio.
- **Zoom correction (Correzione dello zoom)**: un valore più alto aumenta lo zoom all'indietro per gli oggetti che si trovano vicino al bordo del campo visivo della telecamera PTZ.

Scheda output

- **Configure (Configura)**: consente di aprire la pagina web del dispositivo per creare e configurare gli allarmi.
- **Test alarm (Testare allarme)**: provare l'allarme configurato per il dispositivo.
- **Post-alarm time: Assign (durata post-allarme: assegna)** - Impostare il periodo di post-allarme.

Scheda assistenza

- **Load (Carica)**: consente di caricare la configurazione di backup per i dispositivi selezionati. Ciò è particolarmente utile per un ripristino rapido dopo un guasto del dispositivo o disinstallazione accidentale. Questa configurazione include:

– Licenza

– Parametri

– Calibrazione e scenari

– Video di calibrazione

- **Save (Salva)**: consente di creare un backup della configurazione dei dispositivi selezionati.
- **Clear (Cancella)**: consente di cancellare la calibrazione e gli scenari dai dispositivi selezionati. Ciò è utile se le telecamere si sono spostate, poiché le zone di calibrazione e rilevamento non sono più valide.
- **View application log (Visualizza registro applicazione)**: consente di visualizzare il registro interno di AXIS Perimeter Defender.
- **Export support log (Esportare registro di assistenza)**: consente di generare un file di supporto contenente informazioni dettagliate. Includere sempre questo file con una richiesta di assistenza.

Carico CPU

L'indicatore di carico della CPU indica il carico attuale della CPU in tempo reale. Un carico eccessivo della CPU potrebbe risultare in un computer o un'applicazione che non risponde. Assicurarsi di chiudere altre applicazioni quando si utilizza AXIS Perimeter Defender Setup, per ottimizzare l'allocazione della CPU. Se il carico della CPU è troppo elevato e si tenta di aggiungere un dispositivo, il sistema emette un avviso.

Ogni dispositivo aggiunto occupa risorse della CPU del computer host durante la decodifica e la visualizzazione del flusso video. Per limitare l'impatto sul computer host, i flussi video da dispositivi aggiunti vengono visualizzati a una velocità in fotogrammi ridotta (circa 1 fps) per impostazione predefinita. La velocità in fotogrammi normale (circa 8 fps) viene ripristinata quando i flussi vengono massimizzati o durante il processo di calibrazione.

Importante

Enable full frame rate mode (Abilita modalità massima velocità in fotogrammi) può causare la mancata risposta dell'interfaccia se si effettua la connessione a un numero elevato di telecamere o quando si utilizza un computer con bassa potenza.

Mostrare una dimostrazione di AXIS Perimeter Defender

A scopo dimostrativo, AXIS Perimeter Defender e AXIS Perimeter Defender PTZ Autotracking comprendono alcune clip di dimostrazione preinstallate che possono essere utilizzate per illustrare le analisi senza la necessità di un programma attivo installato sulla telecamera. Le clip di dimostrazione mostrano il tipo di rilevamento e i risultati di rilevamento automatico che possono previsti in diversi ambienti.

1. Andare su **Application > Add > Demo Clips (Applicazione > Aggiungere > Clip di dimostrazione)** e condurre una o più delle seguenti operazioni:
   - Filtrare le clip di dimostrazione in base al tipo.
   - Selezionare almeno una clip di dimostrazione.
2. Per aggiungere le clip di dimostrazione, fare clic su **Add Selected Demo Clips (Aggiungi clip di dimostrazione selezionate)**.

Una volta aggiunte, le clip di dimostrazione vengono visualizzate come flussi video standard nell'interfaccia. La calibrazione è disponibile e le analisi già attivate in modo che l'utente veda immediatamente i risultati dell'analisi e del rilevamento automatico nel flusso video. L'analisi e il rilevamento automatico possono essere interrotti o avviati facendo clic sullo stato in esecuzione nella visualizzazione in diretta sui pulsanti **Run (Esegui)** o **Stop (Arresta)** nel riquadro di sinistra.

La calibrazione e l'abbinamento possono essere modificati e ripetuti. Allo stesso modo, gli scenari di rilevamento possono essere aggiunti, rimossi e modificati.

La scheda **Support (Supporto)** nel riquadro sinistro dispone di un pulsante **Clear (Cancella)** che consente di ripristinare la calibrazione e gli scenari ai valori originali. Non è possibile rimuovere completamente la calibrazione.

Impostazioni preliminari

Il processo di installazione per AXIS Perimeter Defender differisce leggermente da quello per AXIS Perimeter Defender PTZ Autotracking.

Introduzione ad AXIS Perimeter Defender

È necessario seguire i seguenti passaggi per mettere in funzione il sistema con AXIS Perimeter Defender:

1. Montare la telecamera. Vedere *Montare la telecamera, on page 13*.
2. Scaricare e installare il software sul computer. Vedere *Installare il software sul computer, on page 16*.
3. Collegare ai dispositivi. Vedere *Aggiunta di dispositivi, on page 17*.
4. Installare AXIS Perimeter Defender su ogni dispositivo. Vedere *Installare il software sui dispositivi, on page 18*.

Nota

Non è necessario calibrare i dispositivi che vengono eseguiti esclusivamente in modalità IA. Per far funzionare contemporaneamente i dispositivi in modalità di calibrazione e IA, è necessario calibrarli.

5. Calibrare i dispositivi. Vedere *Calibrare - AXIS Perimeter Defender, on page 19*.
6. Definire le regole per l'attivazione degli allarmi aggiungendo scenari. Vedere *Definire gli scenari, on page 26*.
7. Impostare gli allarmi da inviare. Vedere *Definire gli output, on page 30*.

Introduzione ad AXIS Perimeter Defender PTZ Autotracking

È necessario seguire i seguenti passaggi per mettere in funzione il sistema con AXIS Perimeter Defender PTZ Autotracking:

1. Montare le telecamere: Vedere *Montare la telecamera, on page 13* e *Montare la telecamera PTZ, on page 16*.
2. Scaricare e installare il software sul computer. Vedere *Installare il software sul computer, on page 16*.
3. Collegare ai dispositivi. Vedere *Aggiunta di dispositivi, on page 17*.
4. Installare AXIS Perimeter Defender versione 2.5.0 o successiva sulla telecamera fissa e AXIS Perimeter Defender PTZ Autotracking sulla telecamera PTZ. Vedere *Installare il software sui dispositivi, on page 18*.
5. Calibrare i dispositivi e impostare gli scenari. Vedere *Calibrazione - PTZ Autotracking, on page 26*.
6. Associare i dispositivi. Vedere *Associare le telecamere - PTZ Autotracking, on page 29*.
7. Impostare gli allarmi da inviare. Vedere *Definire gli output, on page 30*.

Montare la telecamera

Informazioni sullo strumento di progettazione

Per specificare il posizionamento della telecamera nel sito, si consiglia di utilizzare lo strumento di progettazione per AXIS Perimeter Defender. Prende in considerazione sia i requisiti delle telecamere Axis che quelli di AXIS Perimeter Defender. Inoltre, è possibile utilizzarlo nelle installazioni doppie, cioè per l'utilizzo combinato di due telecamere. Lo strumento aiuta a decidere:

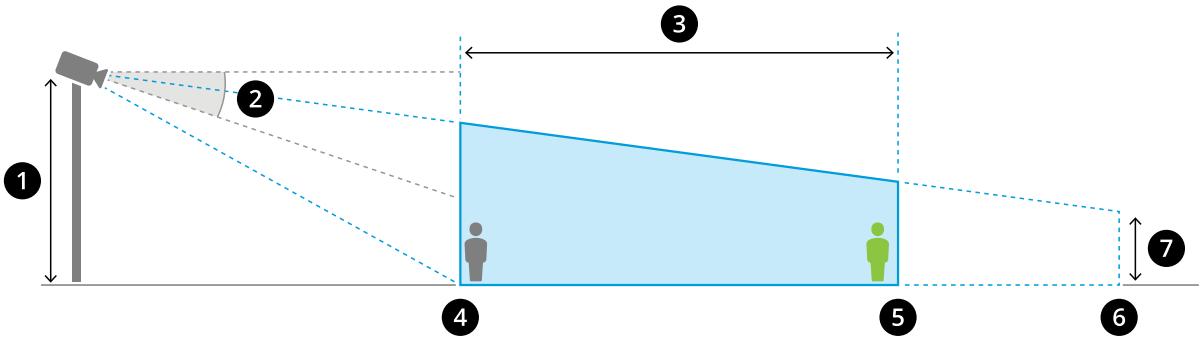
- Altezza di montaggio della telecamera
- Angolo di inclinazione
- Distanza di rilevamento minima
- Distanza massima di rilevamento

Per scaricare lo strumento, visitare la pagina *axis.com/products/axis-perimeter-defender*

Raccomandazioni per il montaggio della telecamera

Nota

Sono disponibili i consigli di montaggio nell'applicazione per le telecamere che vengono eseguite solo in modalità IA.



Una telecamera montata in modo appropriato.

1 *Altezza di montaggio*
2 *Inclinazione*
3 *Zona di rilevamento*
4 *Distanza di rilevamento minima*
5 *Distanza massima di rilevamento*
6 *Distanza dal campo visivo*
7 *Elevazione campo visivo*

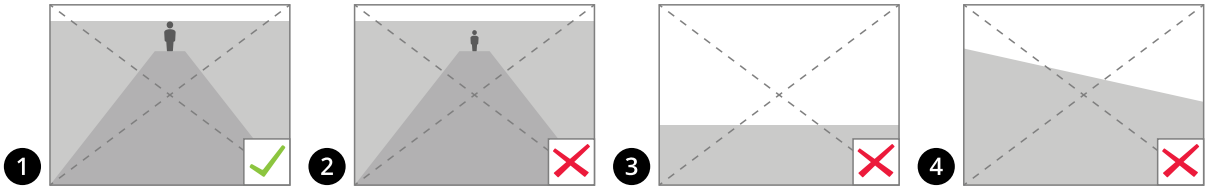
Altezza dell'oggetto alla distanza di rilevamento massima – Affinché una persona in piedi venga rilevata alla distanza massima di rilevamento, l'altezza in pixel deve essere almeno il 5% dell'altezza totale dell'immagine (3,5% per le telecamere termiche). Ad esempio, se l'altezza dell'immagine visualizzata è di 576 pixel, l'altezza di una persona in piedi alla fine della zona di rilevamento deve essere di almeno 28 pixel (20 pixel per termico).

Altezza dell'oggetto alla distanza di rilevamento minima – Affinché una persona in piedi venga rilevata alla distanza minima di rilevamento, l'altezza in pixel deve essere almeno il 60% dell'altezza totale dell'immagine.

Altezza dell'oggetto in modalità IA – Quando si esegue l'applicazione in modalità IA, gli oggetti devono essere della stessa dimensione o più grandi dell'avatar da rilevare.

Angolo di inclinazione – La telecamera deve essere orientata verso il suolo in modo che il centro dell'immagine si trovi sotto la linea dell'orizzonte. Montare la telecamera in modo che la distanza minima di rilevamento sia più lunga della metà dell'altezza di montaggio della telecamera (distanza minima di rilevamento > altezza di montaggio della telecamera, diviso 2).

Angolo di rotolamento – L'angolo di rotolamento della telecamera deve essere circa pari a zero.



1 *L'altezza dell'oggetto, l'angolo di inclinazione e l'angolo di rotazione sono adatti.*
2 *L'altezza dell'oggetto alla distanza massima di rilevamento è inferiore al 5% dell'altezza dell'immagine (3,5% per le telecamere termiche).*
3 *Il centro dell'immagine è sopra la linea dell'orizzonte.*
4 *L'angolo di rotazione della telecamera non è quasi uguale a zero.*

La distanza massima di rilevamento dipende da:

- Tipo e modello di telecamera
- Obiettivo della telecamera. Un raggio focale più elevato consente una distanza di rilevamento più ampia.

- Le dimensioni in pixel minime che una persona deve coprire nell'immagine da rilevare. L'altezza in pixel di una persona in piedi deve essere almeno il 5% dell'altezza dell'immagine per le telecamere visive e il 3,5% per le telecamere termiche.
- Clima
- Illuminazione
- Carico della telecamera

Quando si monta la telecamera, ricordare quanto segue:

- L'applicazione tollera lievi vibrazioni della telecamera, ma le migliori prestazioni si ottengono quando la telecamera non è soggetta a vibrazioni.
- è necessario fissare il campo visivo della telecamera.

Altezza di montaggio

Per raggiungere una determinata distanza di rilevamento, oltre alla dimensione minima dei pixel richiesta, la telecamera deve essere posizionata a un'altezza minima. Non c'è nessuna altezza massima di montaggio purché gli altri requisiti, soprattutto l'angolo di inclinazione, siano soddisfatti.

Distanza di rilevamento richiesta	Altezza di montaggio minima della telecamera:
20 m	2,5 m (8 ft) (altezza minima consentita)
100 m (330 ft)	3m (10 ft)
200 m (650 ft)	4 m (13 ft)
300 m (1000 ft)	5 m
500 m (1600 ft)	6 m

Requisiti della scena

Nota

Sono disponibili i consigli di scena nell'applicazione per le telecamere che vengono eseguite solo in modalità IA.

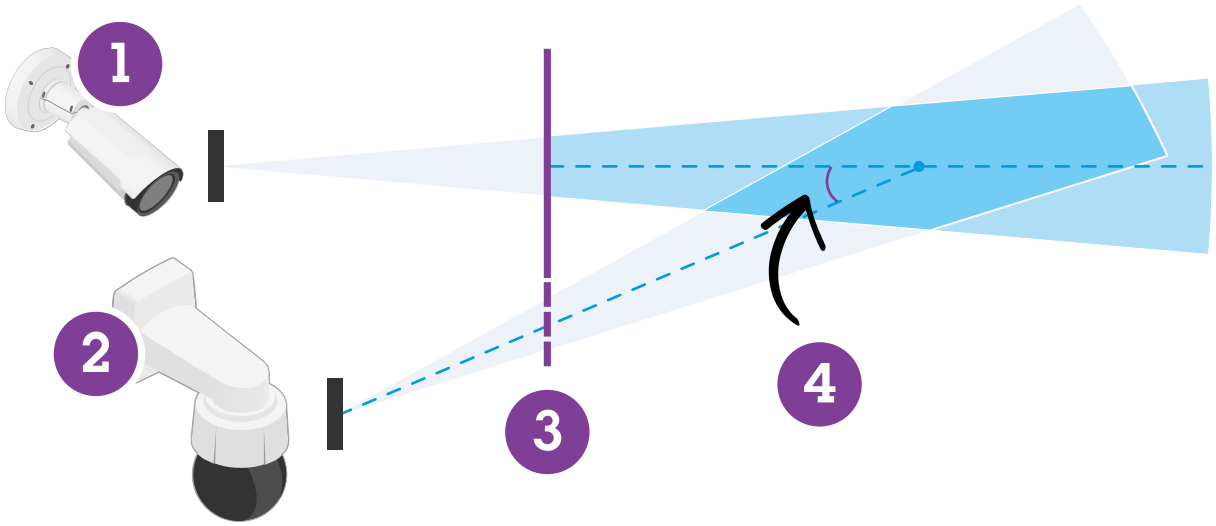
La zona di rilevamento deve fornire le seguenti condizioni:

- Vista nitida
- Il terreno deve essere piatto o con solo una leggera pendenza
- La luce non viene attivata dal movimento
- Vista nitida
- Per le telecamere ottiche, il livello di illuminazione e le impostazioni delle immagini devono fornire un contrasto sufficiente tra umani e veicoli e lo sfondo.
  - Quando si utilizza una telecamera per riprese diurne/notturne di Axis con l'illuminazione artificiale, si consigliano almeno 50 lux nell'intera zona di rilevamento.
  - Quando si utilizzano punti IR esterni, si consiglia una distanza massima di rilevamento di 80 m e che la portata dei punti IR sia superiore al doppio della distanza massima di rilevamento.
  - Quando si utilizza l'illuminazione IR integrata, la distanza massima di rilevamento è limitata a circa 20 m, a seconda della telecamera e dell'ambiente.
- Per le telecamere termiche, ci deve essere un elevato contrasto tra sfondo e primo piano

Per ottimizzare le prestazioni di rilevamento, AXIS Perimeter Defender apprende automaticamente la differenza tra il giorno e la notte e utilizza queste informazioni per ottimizzare gli algoritmi di rilevamento. L'ottimizzazione richiede circa 24 ore, il che significa che il rilevamento ottimale sia durante il giorno che durante la notte viene raggiunto dopo l'esecuzione dell'applicazione per quel periodo.

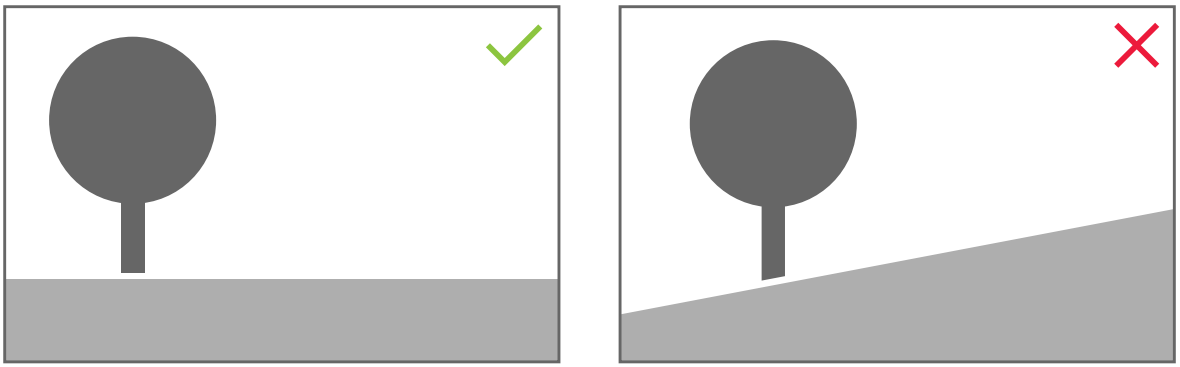
Montare la telecamera PTZ

Questo capitolo descrive come montare la telecamera PTZ in relazione alla telecamera fissa. Per istruzioni su come montare la telecamera fissa, vedere *Montare la telecamera, on page 13*.



1 *Telecamera di rete fissa*
2 *Telecamera di rete PTZ*
3 *Distanza di rilevamento minima*
4 *Angolo tra le telecamere*

- La posizione preimpostata iniziale della telecamera PTZ deve coprire più del 60% della zona di rilevamento della telecamera fissa.
- Per essere monitorata dalla telecamera PTZ, una persona in piedi deve coprire più del 4% dell'altezza dell'immagine della telecamera PTZ.
- La telecamera PTZ deve essere posizionata prima della distanza minima di rilevamento della telecamera fissa (C).
- L'angolo tra la telecamera fissa e la telecamera PTZ deve essere inferiore a 30 (D).



- Il terreno deve essere piatto.

Installare il software sul computer

Le telecamere con AXIS Perimeter Defender installato devono essere raggiungibili tramite HTTP dal computer che esegue l'interfaccia di impostazione di AXIS Perimeter Defender.

L'interfaccia di impostazione di AXIS Perimeter Defender (necessaria solo durante la fase di impostazione) richiede:

- Processore Intel® Core™ 2 Duo o superiore
- Supporto per Open GL
- Almeno 16 GB di RAM
- Windows® 10, Windows® 11 o Win Server 2022
- Risoluzione dello schermo almeno 1024 x 768

Si ricorda che esistono limiti al numero di telecamere che possono essere gestite da un singolo computer. Ad esempio, in una macchina con processore Intel® Core™ i5-1135G7 di 11a generazione a 2,40GHz si consiglia di aggiungere un massimo di 10 telecamere e di eseguire una calibrazione automatica simultanea su un massimo di 5 telecamere.

Nota

L'esecuzione dell'interfaccia di impostazione di AXIS Perimeter Defender su una macchina virtuale non è supportata.

1. Scaricare il software AXIS Perimeter Defender *axis.com/products/axis-perimeter-defender*
2. Installare il software sul computer.

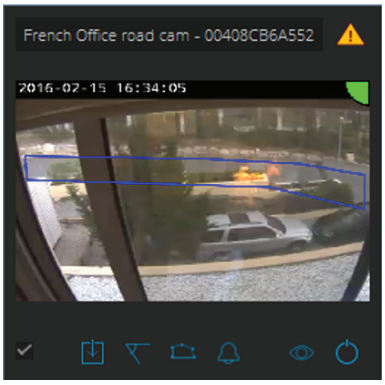
Aggiunta di dispositivi

È possibile aggiungere dispositivi all'applicazione AXIS Perimeter Defender in tre modi diversi:

- Automaticamente attraverso una scansione di rete. Vedere *Aggiunta automatica di dispositivi, on page 18*.
- Manualmente specificando le impostazioni di connessione. Vedere *Aggiunta manuale di dispositivi, on page 18*.
- Automaticamente caricando un sito salvato in precedenza. Vedere *Caricamento di un sito esistente, on page 18*.

Una volta aggiunto un dispositivo, viene visualizzato un elenco di tutte le altre applicazioni installate sul dispositivo. Si consiglia di arrestare tutte le applicazioni non essenziali, poiché utilizzano le risorse CPU della telecamera, influendo sulle prestazioni di AXIS Perimeter Defender e potrebbero impedire la corretta installazione.

Se un dispositivo non dispone di risorse CPU sufficienti, ad esempio perché altre applicazioni sono in esecuzione, AXIS Perimeter Defender riduce la velocità in fotogrammi. Se la velocità in fotogrammi è inferiore 5 fotogrammi al secondo, viene visualizzato un triangolo giallo di avvertimento accanto al nome del dispositivo nella visualizzazione in diretta. Quando si passa il cursore sul triangolo, viene visualizzata la velocità in fotogrammi corrente.



Nota

Una velocità in fotogrammi inferiore a 5 fps può ridurre significativamente le prestazioni di analisi video. Ciò può risultare sia in rilevazioni mancate che in false rilevazioni.

Per ulteriori informazioni, vedere *Carico CPU, on page 11*.

Aggiunta automatica di dispositivi

Importante

La funzionalità di ricerca non funziona su più reti, ovvero AXIS Perimeter Defender Setup è in grado di rilevare solo i dispositivi connessi alla stessa sottorete del client che esegue il software. Se si desidera aggiungere dispositivi connessi a un'altra sottorete, aggiungerli manualmente. La funzionalità di ricerca potrebbe non funzionare anche se i router o gli switch di rete sono configurati per filtrare il multicast.

1. Per eseguire la scansione della rete circostante e cercare i dispositivi, andare su **Application (Applicazione)** e fare clic su **Search (Cerca)**.
   Quando si esegue una ricerca per la prima volta e non sono disponibili password, si apre una finestra di dialogo delle password. In caso contrario, la password disponibile viene utilizzata per connettersi ai dispositivi.
2. Selezionare i dispositivi e fare clic su **Add selected devices (Aggiungi dispositivi selezionati)**.
   Se la password è corretta, viene visualizzata un'immagine statica per guidare l'utente nella selezione dei dispositivi.

Aggiunta manuale di dispositivi

1. Andare su **Application (Applicazione)** e fare clic su **Add (Aggiungi)**.
2. Immettere quanto segue:

- L'indirizzo IP o il nome host del dispositivo.
- La password root del dispositivo, poiché AXIS Perimeter Defender richiede accesso root.
- La porta HTTP utilizzata per la connessione. La porta predefinita è 80.
- Un nome facoltativo per il dispositivo per un riconoscimento più semplice.
- Se il dispositivo è connesso tramite rete remota la cui connessione potrebbe essere lenta, selezionare **Device on remote network (Dispositivo su rete remota)**. Le connessioni lente non configurate come remote possono portare a calibrazioni errate o non funzionanti.

Nota

Per le connessioni remote, l'utente deve potersi collegare al dispositivo tramite HTTP. Assicurarsi di impostare correttamente la porta HTTP. La configurazione remota può non riuscire quando la connessione non dispone di larghezza di banda sufficiente o stabile.

3. Fare clic su **OK**.

Nota

Se non funziona per aggiungere una telecamera per nome host, verificare le impostazioni di rete e DNS o aggiungere il dispositivo utilizzando il relativo indirizzo IP.

Caricamento di un sito esistente

Per caricare una configurazione del sito salvata in precedenza:

1. Andare su **Application (Applicazione)** e fare clic su **Load site (Carica sito)**.
2. Cercare il file di configurazione del sito da selezionare e fare clic su **Open (Apri)**. La vista in tempo reale viene visualizzata automaticamente.

Installare il software sui dispositivi

È necessario installare AXIS Perimeter Defender su ogni dispositivo.

Se si desidera verificare quale versione di AXIS Perimeter Defender è installata su un dispositivo, è possibile passare il cursore su **Installation status (Stato dell'installazione)** nella vista in tempo reale.

Se AXIS Perimeter Defender non è stato installato su un dispositivo, tutte le icone nella vista in tempo reale sono grigie.

Installare il software su un dispositivo

1. Andare su **Installation (Installazione)**.
2. Selezionare i dispositivi in cui si desidera installare l'applicazione.
3. Selezionare l'ultima versione disponibile di AXIS Perimeter Defender e fare clic su **Install (Installa)**. AXIS Perimeter Defender è ora installato sui dispositivi selezionati e viene avviato automaticamente.
4. Cercare una licenza ed eseguire una delle operazioni seguenti:

– Se si installa su un singolo dispositivo: selezionare il file di licenza per il dispositivo.

– Se si installa su più dispositivi: selezionare la cartella in cui sono archiviati i file di licenza.

5. Fare clic su **Installa**.

Calibrare - AXIS Perimeter Defender

Calibrazione

Nota

Non è necessario calibrare i dispositivi che vengono eseguiti esclusivamente in modalità IA. Per far funzionare contemporaneamente i dispositivi in modalità di calibrazione e IA, è necessario calibrarli.

Affinché AXIS Perimeter Defender interpreti correttamente la scena, è necessario calibrare tutti i dispositivi. Durante la calibrazione, si introducono punti di riferimento che forniscono al processore informazioni sulla profondità e l'altezza. È inoltre possibile definire la zona di interesse.

La calibrazione è costituita da due attività:

1. Eseguire una calibrazione:
   - automatica: consigliato nella maggior parte dei casi. Vedere *Eseguire una calibrazione automatica, on page 20*.
   - manuale: consigliato se la calibrazione automatica non riesce su una telecamera, per l'ottimizzazione o quando sarebbe poco pratico condurre un attraversamento della scena e vi sono presenti oggetti di altezza nota. Un esempio è un perimetro remoto con una linea di recinzione costituita da un numero di pali uniformemente distanziati e di un'altezza costante. Vedere *Eseguire una calibrazione manuale, on page 24*.
2. Verificare i risultati della calibrazione. Vedere *Verificare la qualità della calibrazione , on page 21*.

Per velocizzare la configurazione di un sito di grandi dimensioni, è possibile calibrare più dispositivi contemporaneamente. È possibile eseguire la calibrazione automaticamente o manualmente, proprio come per una singola telecamera. Prima di calibrare più dispositivi contemporaneamente, tenere presente quanto segue:

- il numero massimo di dispositivi che è possibile installare e configurare contemporaneamente dipende dalla potenza della CPU e dalla memoria disponibile nel computer. Troppi dispositivi in AXIS Perimeter Defender Setup possono causare arresti anomali. Quando viene visualizzato l'avviso di sovraccarico della CPU, installare e configurare un sottoinsieme dei dispositivi utilizzando la funzionalità salva sito.
- La calibrazione automatica di più dispositivi richiede più risorse della CPU e RAM rispetto a quella di un singolo dispositivo. Nei sistemi con specifiche basse, questo potrebbe far sì che il computer non risponde per qualche tempo o portare a un arresto anomalo dell'applicazione. In caso di arresto anomalo, i video acquisiti sono ancora disponibili per essere utilizzati in seguito per la calibrazione a telecamera singola.

Nota

- AXIS Perimeter Defender supporta proporzioni diverse dell'immagine in base alla risoluzione massima fornita dalla telecamera. Di conseguenza, è necessario rieseguire tutte le calibrazioni precedenti se si modifica la risoluzione. Tuttavia, se si modifica la risoluzione del flusso nella pagina web della telecamera, non è necessario ricalibrare nuovamente.
- È consigliabile usare le stesse proporzioni dell'immagine in AXIS Perimeter Defender e in VMS, per

assicurarsi che le informazioni visualizzate siano in linea con il contenuto dell'immagine. Per scoprire le proporzioni, passare il cursore sul nome della telecamera nella vista in tempo reale.

- Se una telecamera si sposta dopo la calibrazione, è necessario ricalibrare perché i risultati analitici siano corretti.

Eseguire una calibrazione automatica

Con la calibrazione automatica, è possibile calibrare una o più telecamere lasciando che una persona attraversi la scena di sorveglianza. La telecamera raccoglie automaticamente le informazioni necessarie per calibrare se stessa.

Per una calibrazione automatica con esito positivo:

- Non calibrare quando ci sono molte persone nel campo visivo.
- Non calibrare quando molti veicoli attraversano il campo visivo.
- Non calibrare quando ci sono altri oggetti che si muovono nel campo visivo. Ad esempio alberi o bandiere che si muovono nel vento.
- Non calibrare una telecamera che non è stata installata parallelamente al suolo.
- La persona che attraversa la scena deve essere in grado di coprire l'intero campo visivo da davanti a dietro. Se ciò non è possibile, è meglio passare alla calibrazione manuale.
- Se la telecamera si trova su una rete remota ma non è collegata come remota, la persona che attraversa la scena deve camminare per circa 5 minuti per assicurarsi che vengano acquisite abbastanza immagini. La ragione è che la velocità in fotogrammi è in genere inferiore per i dispositivi su reti remote.

1. Andare su **Calibration (Calibrazione)**.
2. Selezionare i dispositivi che si desidera calibrare.
3. Fare clic su **Automatic (Automatica)**.
4. Impostare l'ora di inizio della registrazione. La cattura deve iniziare almeno 10 secondi prima che la persona che attraversa la scena entri nel campo visivo.
5. Impostare la durata della registrazione. Si consideri che:
   - Deve esserci abbastanza tempo perché la persona cammini avanti e indietro attraverso l'intera scena.
   - La lunghezza del video influisce sul calcolo della calibrazione.
6. Immettere l'altezza (cm) della persona che attraversa la scena e fare clic su **Capture (Acquisisci)**.
   Per riutilizzare un video acquisito in precedenza, fare clic su **Use previous capture (Usa acquisizione precedente)**.
7. Lasciare che la persona cammini attraverso la scena secondo le seguenti istruzioni:
   - Camminare in un percorso a zig-zag che copra il più possibile la zona di rilevamento da davanti a dietro la scena. Si consiglia un percorso a forma di V attraverso il campo visivo.
   - Rimanere quasi sempre completamente visibile dalla testa ai piedi nel campo visivo.
   - Camminare lentamente in linea retta.
   - Mantenere una postura eretta per tutto il tempo.
   - Fermarsi per 1-2 secondi prima di cambiare direzione.

Esempio di una sequenza di camminata.

8. Verificare che la calibrazione automatica sia stata eseguita correttamente confermando che la persona venga rilevata con precisione. Vedere *Verificare la qualità della calibrazione , on page 21*.
9. Per salvare la calibrazione, fare clic su **Accept (Accetta)**.
   Per eseguire una nuova calibrazione, fare clic su **New (Nuovo)**.
   Per eseguire una calibrazione manuale, fare clic su **Manual (Manuale)**.

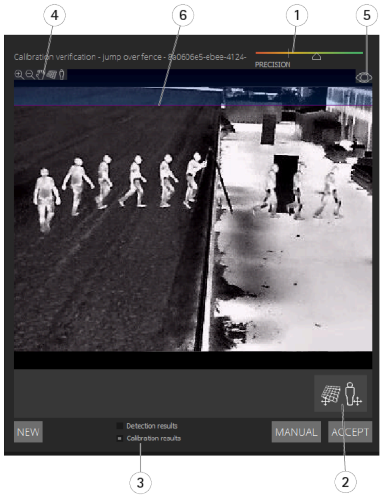
Una volta accettata la calibrazione, i bordi blu indicano la zona di rilevamento massima. La zona di rilevamento massima è l'area più grande che può essere monitorata. Al di fuori di quest'area, gli intrusi potrebbero essere rilevati, ma non è garantito.

Verificare la qualità della calibrazione

Dopo una calibrazione, dovrebbe essere possibile vedere la persona che ha camminato attraverso la scena in diversi luoghi. Se la persona non è affatto visibile, la calibrazione automatica non è riuscita e deve essere ripetuta.

Esistono diversi modi per verificare la qualità della calibrazione:

- Controllare l'indicatore di precisione della calibrazione. Riflette un livello di precisione calcolato automaticamente che misura come la persona ha coperto la scena e in che misura lui o lei è stato rilevato. Se l'indicatore di precisione si trova nella zona rossa, la calibrazione non è riuscita e non è possibile fare clic su **Accept (Accetta)**. Vedere *Eseguire una calibrazione manuale, on page 24*.
- È possibile utilizzare lo strumento griglia. Vedere *Utilizzare la griglia per verificare la calibrazione, on page 22*.
- È possibile utilizzare lo strumento avatar. Vedere *Utilizzare l'avatar per verificare la calibrazione, on page 23*.
- È possibile controllare i risultati del rilevamento. Vedere *Utilizzare i risultati del rilevamento per verificare la calibrazione, on page 23*.



1 *Indicatore di precisione della calibrazione*
2 *Strumenti quali griglia e avatar*
3 *Visualizzazione dinamica o statica*
4 *Modificatori di vista*
5 *Passare dall'immagine di calibrazione alla visualizzazione dal vivo e viceversa*
6 *Linea dell'orizzonte*

La linea dell'orizzonte rappresenta l'estremità visibile del terreno nella scena. Quando si definiscono gli scenari, non è possibile posizionare le zone dello scenario nell'area blu sopra la linea dell'orizzonte, poiché si trova sopra il suolo e le zone dello scenario sono per definizione sul terreno.

Utilizzare la griglia per verificare la calibrazione

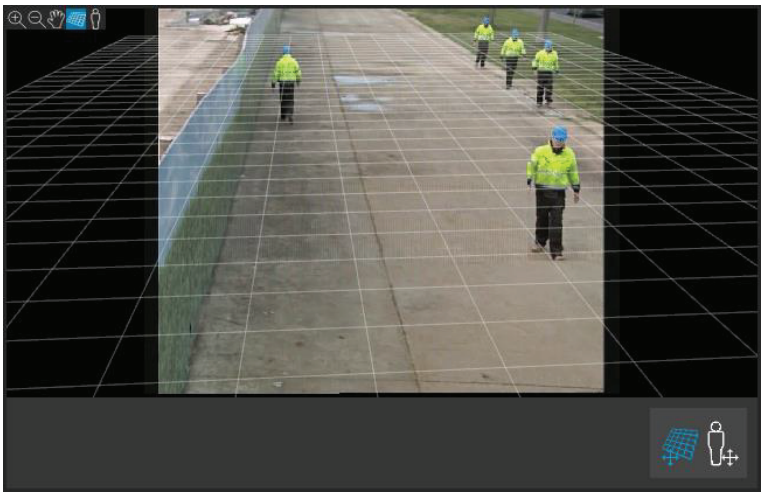
La griglia deve corrispondere a una griglia quadrata sul terreno. È possibile attivare o disattivare la visualizzazione della griglia facendo clic sull'icona del modificatore della visualizzazione griglia.

Importante

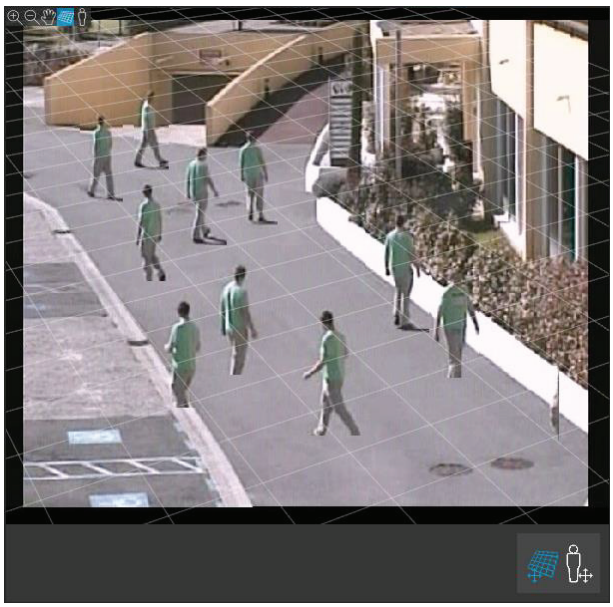
La griglia non influisce sulla calibrazione, è uno strumento per assicurarsi che la calibrazione sia corretta.

È possibile ruotare la griglia trascinandola nel riquadro di anteprima. Provare ad allinearla con qualche struttura nella scena per vedere se il risultato sembra ragionevole.

Se la griglia è parallela al suolo, non ha una strana pendenza e, dopo aver applicato la rotazione necessaria alla griglia, è parallela a manufatti creati dall'uomo che sono paralleli nel mondo reale, allora la calibrazione è buona.



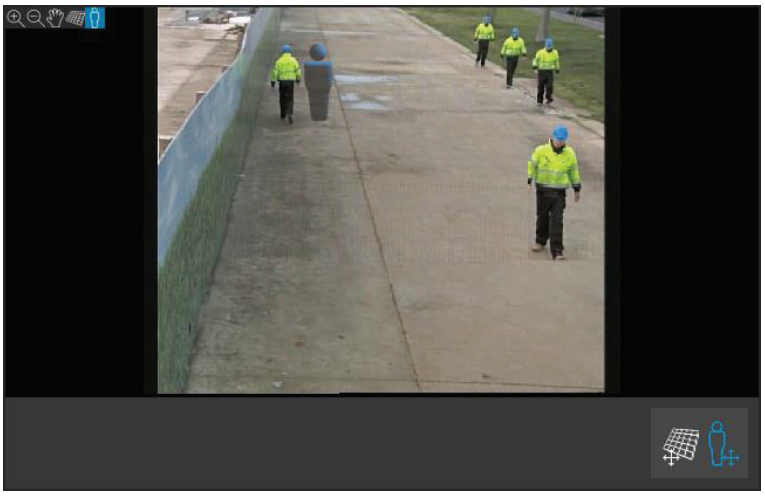
Esempio in cui la griglia è allineata correttamente con le banchine stradali.



Esempio in cui la griglia non è allineata correttamente con le banchine stradali.

Utilizzare l'avatar per verificare la calibrazione

L'avatar consente di posizionare nella scena l'avatar 3D di una persona di altezza media. È possibile attivare o disattivare la visualizzazione dell'avatar facendo clic sull'icona del modificatore della visualizzazione dell'avatar.



Le dimensioni nel riquadro di visualizzazione corrispondono alle dimensioni di una persona media in quella posizione in base alla calibrazione corrente. Spostando l'avatar, è possibile assicurarsi che le sue dimensioni siano ragionevoli in relazione ad altri oggetti o persone nella scena. Si dovrebbe controllare l'avatar in posizioni diverse, dal momento che l'avatar potrebbe avere le dimensioni corrette in una posizione, ma errate altrove nell'immagine.

Utilizzare i risultati del rilevamento per verificare la calibrazione

È possibile utilizzare i risultati del rilevamento per verificare quali sarebbero le prestazioni di AXIS Perimeter Defender con la calibrazione corrente se ricevesse il video della persona che cammina come flusso dal vivo.

1. Passare da **Calibration results (Risultati della calibrazione)** a **Detection results (Risultati del rilevamento)**.
2. Controllare i rilevamenti delle persone o dei veicoli che entrano nella scena di sorveglianza:
   - Se la calibrazione va bene, le persone sono contrassegnate con rettangoli rossi e i veicoli con rettangoli blu.
   - Se le persone o i veicoli spesso non sono contrassegnati, molto probabilmente la calibrazione automatica non è riuscita.

– Una zona rossa mostra la zona del limite di rilevamento in base alla calibrazione calcolata, ovvero la zona in cui i prerequisiti sull'altezza umana nell'immagine non vengono rispettati. In questa zona il rilevamento potrebbe non riuscire a causa della dimensione di destinazione.

Nota

- Se la calibrazione calcolata è errata, anche la zona rossa è errata.
- Se la persona è troppo lontana, potrebbe non essere contrassegnata. Per il funzionamento del rilevamento è necessaria una dimensione minima. Per ulteriori informazioni, vedere *Montare la telecamera, on page 13*.
- La revisione dei risultati del rilevamento potrebbe non funzionare su telecamere collegate in remoto, perché l'acquisizione può avere una frequenza fotogrammi troppo bassa. Ciò non significa che la configurazione non sia riuscita. Utilizzare invece l'avatar e la griglia per verificare la calibrazione.

Eseguire una calibrazione manuale

Se non è stata tentata una calibrazione automatica, è necessario acquisire un breve video e creare un'immagine composita prima di poter eseguire una calibrazione manuale. Seguire la stessa procedura descritta per una calibrazione automatica (*Eseguire una calibrazione automatica, on page 20*), ma selezionare **Manual (Manuale)** invece di **Automatic (Automatica)** nella scheda **Calibration (Calibrazione)**. Per creare l'immagine composita dopo aver acquisito un video:

- Spostare il cursore per spostarsi nel video clip
- Nelle posizioni chiave, fare clic sull'icona della telecamera per aggiungere immagini al composito

Assicurarsi che l'immagine composita rifletta l'intera sezione trasversale della scena: davanti, dietro, a destra e a sinistra.

Quando si dispone di un'immagine composita, creata manualmente o automaticamente, è possibile continuare la calibrazione manuale.

Il motore di calibrazione calibra stimando:

- L'orizzonte
- Il modo in cui le linee verticali si diffondono o si aprono a ventaglio nell'immagine
- La scala della scena

Quando si esegue una calibrazione manuale, è necessario fornire queste informazioni al motore di calibrazione tramite elementi di calibrazione. Esistono tre tipi di elementi di calibrazione:

- Le **asticelle per persone** sono utilizzate per contrassegnare l'altezza nota di una persona media in varie posizioni nella scena. Se è già stata tentata una calibrazione automatica, è molto probabile che l'immagine visualizzata nel riquadro dell'editor mostri la stessa persona più volte. Posizionare un'asticella per persone partendo da terra per contrassegnare l'altezza e la direzione della persona in una o più posizioni. Un'asticella per persone deve iniziare da terra e dovrebbe essere verticale nel mondo reale. La lunghezza di un'asticella per persone nel mondo reale deve corrispondere all'altezza indicata accanto al pulsante **Person (Persona)** nel riquadro dell'editor. Le asticelle per persone sono contrassegnate da un simbolo azzurro semitrasparente.
  Come posizionare al meglio un'asticella per persone

– Si consiglia di posizionare l'asticella su una persona che tiene i piedi vicini.

– Se si posiziona un'asticella su una persona in piedi con i piedi divaricati, posizionare il punto inferiore a terra a metà strada tra i talloni della persona.

– Allineare l'asticella con il busto della persona. Tuttavia, se lui o lei è inclinato in qualche direzione, in genere in avanti mentre cammina, cercare di compensare l'inclinazione mettendo l'asticella in posizione più dritta. Farsi guidare da qualsiasi indizio nella scena, ad esempio alberi, recinzioni o lampioni.

– Per la scala della scena, è necessaria almeno un'asticella per persone con l'altezza della persona corrispondente. Se non c'è nessuna persona visibile nella scena, è possibile aggiungere un'asticella per persone su qualche altro oggetto verticale di altezza nota, ad esempio un palo di recinzione di 3 m, e impostare l'altezza della persona sull'altezza dell'oggetto.

- **Le linee orizzontali parallele (linee H)** vengono utilizzate per contrassegnare linee orizzontali e parallele note nella scena. Queste linee possono essere a terra o su un muro o entrambi, ma devono essere tutte parallele. Se si aggiungono linee H, è necessario aggiungerne almeno due. È possibile posizionarle sui lati o sulle marcature su una strada dritta, su una serie di binari ferroviari dritti, su qualche struttura visibile su una parete, o sulla parte superiore e inferiore di una fila di pali di recinzione. Le linee H sono contrassegnate in azzurro.
- **Le linee verticali (linee V)** vengono utilizzate per contrassegnare le linee verticali note nella scena. Una linea V dovrebbe contrassegnare una struttura verticale nel mondo reale. Può trattarsi ad esempio di un palo di recinzione, l'angolo di un edificio o un cartello. Una linea V non deve necessariamente partire da terra. Le linee V sono contrassegnate in blu scuro. Si noti che le linee V sono molto sensibili, in quanto un piccolo cambiamento di orientamento può cambiare drasticamente la calibrazione. Come regola generale, le linee V dovrebbero pendere a destra sul lato destro dell'immagine e a sinistra sul lato sinistro.

1 *Asticelle per persone*
2 *Linee verticali (linee V)*
3 *Linee parallele orizzontali (linee H)*
4 *Strumenti quali griglia e avatar*

Numero di elementi di calibrazione

Generalmente, quando si aggiungono asticelle per persone, linee H e linee V nella scena, più sono meglio è. Il motore di calibrazione può calibrare con pochissime linee, ma in genere più linee e asticelle si disegnano, più migliora la qualità della calibrazione. Quando si aggiungono asticelle per persone, si consiglia di posizionarle sia vicino che lontano, a sinistra e a destra.

Strutture verticali nell'immagine

Secondo *Raccomandazioni per il montaggio della telecamera, on page 14*, tutte le telecamere devono puntare leggermente verso il basso. Di conseguenza, tutte le strutture verticali nel mondo reale sembrano aprirsi come una coda di pavone nell'immagine. Ciò significa che tutte le asticelle per persone e le linee V dovrebbero essere inclinate verso il bordo dell'immagine. Un'asticella sulla metà destra dell'immagine dovrebbe essere inclinata a destra e un'asticella a sinistra dovrebbe essere inclinata a sinistra. Almeno una delle asticelle per persone o linee V posizionate deve essere "inclinata correttamente" affinché la calibrazione funzioni.

L'indicatore di precisione fornisce un feedback ottico sul livello e sulla qualità dei dettagli aggiunti alla scena. Perché le calibrazioni manuali abbiano esito positivo, i contrassegni devono coprire la scena da davanti a dietro e da sinistra a destra. Ciò è indicato da un indicatore di precisione verde.

Qualità di calibrazione

La qualità della calibrazione può essere controllata con i manipolatori a griglia o avatar. Vedere *Verificare la qualità della calibrazione , on page 21*. In alternativa, fare clic su **Review (Revisione)**. Questo mostra il risultato dell'esecuzione di AXIS Perimeter Defender sul video acquisito utilizzando la calibrazione manuale corrente.

Calibrazione - PTZ Autotracking

Importante

Per ottenere buoni risultati, la calibrazione deve essere di alta qualità. Seguire attentamente le linee guida e le istruzioni.

Nota

È possibile calibrare entrambe le telecamere contemporaneamente o una alla volta.

1. Selezionare sia la telecamera fissa che la telecamera PTZ.
2. Andare su **Calibration (Calibrazione)** e fare clic su **Setup PTZ position (Posizione configurazione PTZ)**. Viene visualizzato un pop-up con la vista dalla telecamera fissa.
   All'avvio dell'applicazione, la telecamera PTZ eseguirà le funzioni pan, tilt e zoom per un breve periodo di tempo.
3. Verificare che le viste delle due telecamere siano allineate l'una con l'altra.
   In caso contrario, fare clic sull'immagine con visualizzazione diretta per regolare la visualizzazione della telecamera PTZ fino a quando non corrisponde alla visualizzazione della telecamera fissa. Assicurarsi che la telecamera non stia eseguendo una rotazione.
4. Fare clic su **Setup PTZ position (Imposta posizione PTZ)**.
   Se il pulsante non è visibile, spostare il popup con la vista dalla telecamera fissa.
5. Fare clic su **Automatic (Automatica)**.
6. Eseguire una calibrazione automatica secondo le istruzioni in *Eseguire una calibrazione automatica, on page 20*.
7. Utilizzare l'avatar per verificare la qualità della calibrazione per la telecamera fissa. Vedere *Utilizzare l'avatar per verificare la calibrazione, on page 23*.
   Se la qualità è sufficiente, fare clic su **Accept (Accetta)**.
   Se la qualità non è sufficiente, utilizzare il video della calibrazione automatica per effettuare una calibrazione manuale. Fare clic su **Manual (Manuale)** e seguire le istruzioni in *Eseguire una calibrazione manuale, on page 24*.
8. Definire le regole riguardanti cosa dovrebbe attivare un allarme su **Scenarios (Scenari)**. Vedere *Definire gli scenari, on page 26*.
9. In **Calibration (Calibrazione)**, fare clic su **Review (Verifica)** nella vista in diretta della telecamera PTZ.
10. Utilizzare l'avatar per verificare la qualità della calibrazione per la telecamera PTZ. Vedere *Utilizzare l'avatar per verificare la calibrazione, on page 23*.
    Se la qualità è sufficiente, fare clic su **Accept (Accetta)**.
    Se la qualità non è sufficiente, utilizzare il video della calibrazione automatica per effettuare una calibrazione manuale. Fare clic su **Manual (Manuale)** e seguire le istruzioni in *Eseguire una calibrazione manuale, on page 24*.
11. Associare le telecamere. Vedere *Associare le telecamere - PTZ Autotracking, on page 29*.

Definire gli scenari

Scenari

AXIS Perimeter Defender include scenari di zone sterili comuni che è possibile configurare per proteggere e monitorare le aree sensibili. Nella fase di calibrazione, l'area di rilevamento massima è stata creata per fornire uno scenario predefinito di tipo intrusione/movimenti sospetti. In questa fase, è possibile definire scenari di rilevamento più sofisticati di tre tipi diversi:

Nota

Se si è utenti di AXIS Perimeter Defender 4.0, ora è possibile configurare gli scenari senza ricorrere all'applicazione desktop. Le modifiche verranno trasferite all'applicazione desktop. Per ulteriori informazioni, andare alla *Interfaccia Web, on page 39*.

- intrusione/movimenti sospetti. Vedere *Impostare lo scenario di intrusione/circolazione sospetta, on page 27*

- attraversamento zona. Vedere *Impostare lo scenario di attraversamento della zona, on page 28*
- condizionale. Vedere *Impostare lo scenario condizionale, on page 28*

Se il simbolo **!** appare vicino al nome di uno scenario, significa che l'impostazione dello scenario non è completa. Il problema più comune è che la relativa zona di rilevamento non è ancora stata definita.

Parametri globali

I parametri globali impostati nell'interfaccia utente si applicano a tutti gli scenari.

Tipo di telecamera – Per le telecamere ottiche, selezionare **Color – Day-Night (Colore – Giorno-Notte)**. Per le telecamere termiche, il tipo di telecamera viene impostato automaticamente su termica.

Nota

- I tipi di approccio aggiuntivi possono aumentare il rischio di falsi allarmi, provocati ad esempio da animali.
- Altri tipi di approccio non sono supportati per i dispositivi che vengono eseguiti solo in modalità IA.

Altri tipi di approccio – Selezionare quelli che si desidera coprire con lo scenario di rilevamento.

Mitigazione avanzata – Per i dispositivi con modalità IA, selezionare **IA** per attivarla. Puoi usare **Headlights/vehicles in scene (Fari/veicoli nella scena)** se la scena contiene veicoli, fari o effetti faro come i riflessi. Se si utilizza questa impostazione, le prestazioni a volte possono essere ridotte in condizioni normali. Per impostazione predefinita, tutti gli scenari devono contenere veicoli e quindi fari. È possibile utilizzare **Insects/droplets on lens (Insetti/goccioline sull'obiettivo)** per ignorare i trigger dalle gocce di pioggia o dagli insetti e ridurre i falsi allarmi.

Sensibilità – Per aumentare la sensibilità del sistema, spostare il cursore verso destra. Una maggiore sensibilità riduce il rischio di rilevamenti mancati, ma aumenta il rischio di falsi allarmi.

Filtro dimensione destinazione – Per i dispositivi con modalità IA, è possibile filtrare gli oggetti più piccoli rispetto alla dimensione target.

Parametri di durata

Per ogni scenario creato, è possibile impostare i parametri di durata.

Presenza minima nella zona – Impostare per quanto tempo un oggetto deve rimanere in una zona affinché essa venga attivata.

Restringi zona – Se la zona è stretta e può essere attraversata in 1-2 secondi, sussiste il rischio di allarmi mancati. È possibile attenuare questa funzionalità con **Narrow zone (Restringi zona)**. Si noti che non può essere combinata **Min presence in zone (Presenza min. in zona)**.

Impostare lo scenario di intrusione/circolazione sospetta

Lo scenario di intrusione/circolazione sospetta è progettato per attivare un allarme quando un oggetto entra in una determinata zona e rimane nella zona per un periodo di tempo superiore a quello predefinito.

Lo scenario predefinito creato nella fase di calibrazione è del tipo intrusione/circolazione sospetta e utilizza la zona di rilevamento massima. Per utilizzare questo scenario così com'è, fare clic su **Accept (Accetta)** nella scheda **Scenarios (Scenari)**.

Per modificare lo scenario predefinito:

1. Andare su **Scenarios > Advanced scenarios (Scenari > Scenari avanzati)**.
2. Modificare la zona di rilevamento predefinita:
   - Per spostare i punti esistenti nella zona di rilevamento, fare clic su di essi e trascinarli con il mouse.
   - Per creare punti aggiuntivi, fare clic su uno dei segmenti esistenti e trascinare con il mouse.

3. In **Detect (Rileva)**, selezionare il tipo di oggetti da rilevare.
4. In **Duration parameters (Parametri di durata)**, se non si desidera che un oggetto attivi un allarme non appena entra nella zona, impostare il tempo di circolazione sospetta in **Min presence in zona (Presenza min, nella zona)**.
5. Se la zona è stretta e può essere attraversata in 1-2 secondi e si desidera ancora attivare allarmi, selezionare **Narrow zone (Restringi zona)**. Questa impostazione non può essere combinata con **Min presence in zone (Presenza min. in zona)**. Per ulteriori informazioni, vedere *Parametri di durata, on page 27*.
6. Per caricare le modifiche alla telecamera e tornare alla vista principale, fare clic su **Accept (Accetta)**.

Impostare lo scenario di attraversamento della zona

Lo scenario di attraversamento della zona è progettato per attivare un allarme quando un oggetto passa attraverso due zone di rilevamento in una determinata sequenza.

Importante

Lo scenario di attraversamento della zona presenta i limiti seguenti: se l'oggetto che attiva lo scenario smette di muoversi per alcuni secondi nella zona di origine prima di passare alla zona finale, lo scenario non viene attivato.

In **Duration parameters (Parametri di durata)**, è possibile definire un tempo di presenza minimo per ognuna delle zone dello scenario. Se T_A è il tempo minimo nella zona di origine e T_B nella zona finale, l'allarme si attiva solo se l'oggetto rimane più a lungo di T_A nella zona di origine e poi più a lungo di T_B nella zona finale.

1. Andare su **Scenarios > Advanced scenarios (Scenari > Scenari avanzati)**.
2. Fare clic su **New (Nuovo)** e selezionare **Zone-crossing (Attraversamento zona)**.
3. Creare due zone di rilevamento separate da almeno un metro (3 piedi, 3 3/8 pollici):
   - Per creare una zona di rilevamento, fare clic più volte nell'immagine.
   - Per completare la zona, fare clic con il pulsante destro del mouse sull'immagine.
4. Per specificare la direzione di attraversamento proibita, fare clic su **Select origin (Selezionare origine)** e fare clic su una delle zone.
5. In **Detect (Rileva)**, selezionare il tipo di oggetti da rilevare.
6. In **Duration parameters (Parametri di durata)**, se non si desidera attivare una zona non appena un oggetto entra, impostare la **Min presence in (Presenza min. in)** per una o entrambe le zone.
7. Se la zona è stretta e può essere attraversata in 1-2 secondi e si desidera ancora attivare allarmi, selezionare **Narrow zone (Restringi zona)**. Questa impostazione non può essere combinata con **Min presence in zone (Presenza min. in zona)**. Per ulteriori informazioni, vedere *Parametri di durata, on page 27*.
8. Per caricare le modifiche alla telecamera e tornare alla vista principale, fare clic su **Accept (Accetta)**.

Impostare lo scenario condizionale

Lo scenario condizionale è progettato per attivare un allarme quando un oggetto entra in una determinata zona senza prima passare attraverso altre.

In **Duration parameters (Parametri di durata)**, è possibile definire un tempo di presenza minimo per ognuna delle zone dello scenario. Se T_A è il tempo minimo nella zona autorizzata e T_B nella zona d'intrusione, l'allarme si attiva solo se l'oggetto:

- rimane più a lungo di T_B nella zona d'intrusione senza essere entrato prima nella zona autorizzata.
- rimane più a lungo di T_A nella zona autorizzata, poi entra e rimane più a lungo di T_B nella zona d'intrusione.

Nessun allarme si attiva se l'oggetto:

- non entra o rimane più a lungo di T_B nella zona d'intrusione.

- rimane più a lungo di T_A nella zona autorizzata, poi entra nella zona d'intrusione (indipendentemente dalla durata della permanenza dell'oggetto).

1. Andare su **Scenarios > Advanced scenarios (Scenari > Scenari avanzati)**.
2. Fare clic su **New (Nuovo)** e selezionare **Conditional (Condizionale)**.
3. Creare due o più zone di rilevamento separate da almeno un metro (3 piedi, 3 3/8 pollici):
   - Per creare una zona di rilevamento, fare clic più volte nell'immagine.
   - Per completare la zona, fare clic con il pulsante destro del mouse sull'immagine.
4. Per specificare la direzione di attraversamento consentita, fare clic su **Select intrusion zone (Selezionare zona di intrusione)**, quindi fare clic su una delle zone.
5. In **Detect (Rileva)**, selezionare il tipo di oggetti da rilevare.
6. In **Duration parameters (Parametri di durata)**, se non si desidera attivare una zona non appena un oggetto entra, impostare la **Min presence in (Presenza min. in)** per una o entrambe le zone.
7. Se la zona è stretta e può essere attraversata in 1-2 secondi e si desidera ancora attivare allarmi, selezionare **Narrow zone (Restringi zona)**. Questa impostazione non può essere combinata con **Min presence in zone (Presenza min. in zona)**. Per ulteriori informazioni, vedere *Parametri di durata, on page 27*.
8. Per caricare le modifiche alla telecamera e tornare alla vista principale, fare clic su **Accept (Accetta)**.

Associare le telecamere - PTZ Autotracking

Nella configurazione di AXIS Perimeter Defender PTZ Autotracking, è necessario associare la telecamera fissa e la telecamera PTZ per assicurarsi che un oggetto in movimento venga tracciato in modo efficiente dalla telecamera PTZ.

Se è stata eseguita una calibrazione automatica, si può *Eseguire un accoppiamento automatico, on page 29* delle due telecamere. In caso contrario, è necessario *Eseguire un'associazione manuale, on page 30*.

Eseguire un accoppiamento automatico

Nel video di associazione, le linee rosse rappresentano la persona e il riquadro delimitatore arancione rappresenta l'immagine ingrandita della telecamera PTZ.

1. **Calibration > PTZ Pairing review (Calibrazione > Verifica collegamento PTZ)**, verificare i video di abbinamento delle due telecamere:
   - Verificare che le linee rosse nelle due immagini siano allineate in tutto il video
   - Controllare che le linee rosse vadano sempre dai piedi alla testa della persona
   - Verificare che la persona sia sempre centrata all'interno del riquadro delimitatore arancione nel video della telecamera PTZ
2. Se le condizioni nel passaggio 1 sono soddisfatte, selezionare **Interactive pairing review (Revisione associazione interattiva)**.
   Se le condizioni non sono soddisfatte, fare clic su **Manual (Manuale)** e seguire in passaggi in *Eseguire un'associazione manuale, on page 30*.
3. spostare il cursore per spostarsi nel video clip. Verificare che:
   - le linee blu nelle due immagini sono allineate in tutto il video
   - la persona sia sempre centrata all'interno del riquadro delimitatore arancione nel video della telecamera PTZ
4. Se sono presenti scene in cui manca il riquadro delimitatore arancione:
   4.1. Attivare l'avatar nell'immagine della telecamera fissa.
   4.2. Utilizzare il cursore per spostarsi avanti e indietro nel video. Posizionare l'avatar in corrispondenza della persona nella vista fissa della telecamera e verificare che il punto rosso si trovi ai piedi della persona nell'immagine dalla telecamera PTZ.

5. Se sono presenti scene in cui l'associazione automatica non ha aggiunto linee blu, fare clic su **Manual (Manuale)** e aggiungere manualmente le linee rosse alla persona. Consultare le istruzioni dettagliate riportate di seguito. *Eseguire un'associazione manuale, on page 30*
6. Fare clic su **Accept (Accettare)**e **Exit (Uscita)**.

Eseguire un'associazione manuale

Quando si esegue un'associazione manuale, si aggiungono linee rosse verticali dai piedi alla testa della persona che ha attraversato la scena di sorveglianza nella fase di calibrazione. È necessario aggiungere linee in tutto il video, per coprire l'intera scena.

Se è già stato eseguita un'associazione automatica, il video contiene già linee blu.

Rimuovere le linee blu e rosse che:

- non iniziano dai piedi della persona
- non arrivano fino alla testa della persona
- non hanno una linea corrispondente nell'immagine della telecamera PTZ

Per rimuovere una linea, fare clic su di essa e premere Delete (elimina).

1. Spostare il cursore per passare a un'immagine in cui la persona è visibile nel video clip.
2. Aggiungere una linea rossa sulla persona nell'immagine della telecamera fissa. La linea deve cominciare dai piedi della persona. Alla linea viene assegnato un numero ID.
3. Aggiungete una linea rossa corrispondente sullo stesso oggetto nell'immagine della telecamera PTZ. Verificare che il numero ID corrisponda a quello nell'immagine della telecamera fissa.
4. Ripetere i passaggi da 1 a 3 fino a coprire l'intera scena.
   Quando il video clip contiene un numero sufficiente di linee per un'associazione valida:
   - il pulsante **Accept (Accetta)** diventa attivo
   - un riquadro delimitatore arancione viene visualizzato nell'immagine della telecamera PTZ
5. Verificare che la persona sia sempre centrata all'interno del riquadro delimitatore arancione. Se ci sono scene in cui non lo è, aggiungere altre linee rosse.
6. Attivare l'avatar nell'immagine della telecamera fissa.
7. spostare il cursore per spostarsi nel video clip. Usare l'avatar per verificare che:
   - nell'immagine della telecamera fissa, la dimensione dell'avatar corrisponda alle dimensioni della persona, in diverse posizioni
   - nell'immagine della telecamera PTZ, il punto rosso sia ai piedi della persona
   - nell'immagine della telecamera PTZ, la persona sia sempre centrata all'interno del riquadro delimitatore arancione
8. Fare clic su **Accept (Accetta)**. Se il pulsante è inattivo, è necessario aggiungere prima altre linee rosse.
9. Fare clic su **Exit (Esci)**.

Definire gli output

Perché AXIS Perimeter Defender mandi un allarme quando rileva un'intrusione, è necessario definire delle regole. Il sistema può inviare allarmi, ad esempio, a un VMS.

AXIS Perimeter Defender può inviare allarmi attraverso diverse interfacce.

Dall'applicazione stessa:

- notifiche degli allarmi in XML o in formato di testo normale tramite TCP/IP
- flussi di metadati XML tramite multipart HTTP

Dal dispositivo:

- semplici notifiche su SMS gratis per allarmi tramite TCP/IP
- output elettrici (contatti asciutti o bagnati)
- notifiche tramite e-mail
- caricamento delle immagini di allarme tramite FTP

È possibile attivare più interfacce contemporaneamente.

Per informazioni più approfondite, vedere *Uscite, on page 32*.

Per definire le regole per l'invio di allarmi dal dispositivo:

1. Andare su **Outputs (Output)** e fare clic su **Configure (Configurare)**. La pagina web del dispositivo si apre nel browser.
2. Creazione di una nuova regola di azione.
3. Nell'elenco dei trigger, selezionare **Applications (Applicazioni)**, poi **AXISPerimeterDefender** e lo scenario per attivare l'azione.

Nota

Per attivare la stessa azione per tutti gli scenari definiti, selezionare **ALL_SCENARIOS (tutti gli scenari)**.

4. Dall'elenco di azioni, selezionare l'azione da eseguire quando viene soddisfatta la condizione.
5. Fare clic su **OK**.

Per informazioni più dettagliate su come creare regole di azione, consultare il manuale dell'utente del dispositivo.

Configurazione avanzata

Uscite

Notifiche degli allarmi XML/testo

Questa interfaccia consente a un destinatario TCP/IP di ricevere un messaggio XML o di testo più completo e descrittivo per ogni allarme. Per quanto riguarda l'interfaccia a testo libero, l'interfaccia XML/testo offre i seguenti vantaggi:

- una notifica viene inviata all'inizio dell'allarme, alla fine dell'allarme e ogni 10 secondi durante l'allarme.
- Timestamp: le notifiche di inizio allarme e fine dell'allarme contengono un'indicazione temporale che è sincronizzata con l'orologio della telecamera e fornisce la data e l'ora esatte degli eventi.
- Tipo di allarme: AXIS Perimeter Defender supporta diversi tipi di allarme, vedere *Definire gli scenari, on page 26*. Le notifiche XML/testo contengono le informazioni relative al tipo di allarme che è scattato. Fare attenzione: lo scenario "attraversamento della zona" è di tipo "passage" (passaggio) e lo scenario circolazione sospetta è di tipo "presence" (presenza)
- Zone coinvolte nella generazione dell'allarme; in cui ogni scenario AXIS Perimeter Defender è associato a una o più zone, le notifiche XML/testo includono la zona associata all'allarme (ad esempio, per un allarme di intrusione, la zona di intrusione in cui una persona è stata rilevata)

Per quanto riguarda l'interfaccia a testo libero, l'interfaccia XML/testo ha i seguenti limiti:

- il testo del messaggio è fisso e non sono presenti campi a testo libero.
- È supportato un solo destinatario per telecamera alla volta.

Il destinatario delle notifiche XML/testo riceve quattro tipi di messaggi:

- AXIS Perimeter Defender invia un messaggio CONNECTION_TEST quando la notifica XML è configurata per verificare che la comunicazione con il destinatario funzioni come previsto.
- Quando AXIS Perimeter Defender attiva un allarme, invia un messaggio ALARM_START.
- Per la durata dell'allarme, AXIS Perimeter Defender invia diversi messaggi di "alarm in progress", uno ogni 10 secondi. Tutti questi messaggi hanno lo stesso tag GUID, identico a quello dei messaggi ALARM_START e ALARM_STOP relativi allo stesso allarme
- Alla fine dell'allarme, AXIS Perimeter Defender invia un allarme ALARM_STOP.

Per la spiegazione del formato di questi messaggi, sia in formato testo che XML, vedere *Esempi di formato XML e testo, on page 32*.

Esempi di formato XML e testo

Il formato XML è quello predefinito per le notifiche TCP/IP. Tuttavia, se le dimensioni della notifica sono notevoli, è possibile utilizzare un formato testo, generando messaggi più brevi. Per selezionare il formato testo, il parametro **Do not use XML for alarms (Non utilizzare XML per gli allarmi)** deve essere selezionato nella pagina di configurazione AXIS Perimeter Defender.

Esempio:
Un messaggio CONNECTION_TEST in formato XML è simile all'esempio seguente:

```
<?xml version="1.0"?><KEENEO_MESSAGE xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance"          xmlns:xsd="http://www.w3.org/2001/XMLSchema"          VERSION=
"5.0.0"         ID="1"          TYPE="CONNECTION_TEST"          SENDER_IP=
"192.168.1.40"          SENDER_PORT="0">  <REFERENTIAL>45</REFERENTIAL></KEENEO_MESSAGE>
```

- VERSION è la versione interna della sintassi e del protocollo XML.
- L'ID è un'identità numerica per il messaggio. Non viene garantito che gli ID siano univoci o progressivi.
- TYPE (tipo) è il tipo di messaggio, qui "CONNECTION_TEST" (test di connessione). Il tipo di messaggio determina i tag secondari del messaggio (nessuno per i messaggi di tipo "CONNECTION_TEST").
- SENDER_IP è l'indirizzo IP della telecamera Axis che invia la notifica XML.

- SENDER_PORT è sempre zero; la telecamera non può ricevere i messaggi in arrivo.
- REFERENTIAL è l'ID numerico associato alla telecamera

Se si sceglie il formato testo, i messaggi di notifica contengono 7 campi ciascuno, separati dal carattere "pipe" "|". Se non è possibile specificare un campo (ad esempio, perché non ha senso per quel tipo di messaggio), viene sostituito da "-".

I sette campi sono, dal primo all'ultimo (tra parentesi il campo XML corrispondente quando il formato è XML):

1. ID numerico del messaggio ("ID" dell'intestazione XML "KEENEO_MESSAGE").
2. L'indirizzo IPv4 della telecamera ("SENDER_IP" dell'intestazione XML "KEENEO_MESSAGE").
3. Numero referenziale associato all'istanza AXIS Perimeter Defender (tag "REFERENTIAL").
4. Il tipo di messaggio ("TYPE" dell'intestazione XML "KEENEO_MESSAGE").
5. Il tipo di allarme (tag "TYPE").
6. Il nome dello scenario che ha attivato l'allarme (tag "SCENARIO_NAME").
7. Il timestamp (tag "TIMESTAMP"). Il formato dello timestamp è lo stesso del formato XML.

Il precedente messaggio CONNECTION_TEST in formato TESTO è:

```
1|192.168.1.40|45|CONNECTION_TEST|-|-|-
```

Esempio:
Un messaggio ALARM_START in formato XML è simile all'esempio seguente:

```
<?xml version="1.0"?><KEENEO_MESSAGE xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance"         xmlns:xsd="http://www.w3.org/2001/XMLSchema"         VERSION=
"5.0.0"         ID="9999"         TYPE="ALARM_START"         SENDER_IP=
"192.168.1.40"         SENDER_PORT="0">  <REFERENTIAL>0</REFERENTIAL>  <TYPE>INTRUSION</
TYPE>  <SCENARIO_NAME>Intrusion-0</SCENARIO_NAME>  <EXTRA_DATA>zone=testzone</EXTRA_
DATA>  <TIMESTAMP>2014-03-01T21:24:12.114</TIMESTAMP>  <GUID>77acddf9-e0d4-402e-a497-
231aeee22788</GUID></KEENEO_MESSAGE>
```

- L'intestazione del messaggio è uguale al messaggio "CONNECTION_TEST".
- Il tipo di messaggio è "ALARM_START" e dispone di un set di sottotag.

– REFERENTIAL è l'ID numerico associato alla telecamera.

– TYPE è il tipo di allarme attivato da AXIS Perimeter Defender, "INTRUSION" in questo esempio. Altri tipi possibili sono "PRESENCE", "PASSAGE" e "CONDITIONAL".

– SCENARIO_NAME è il nome dello scenario che ha attivato l'allarme, come definito nell'interfaccia di configurazione. Vedere *Impostare lo scenario di intrusione/circolazione sospetta, on page 27*

– EXTRA_DATA porta il nome della zona (o l'elenco dei nomi di zona) coinvolti nell'allarme, come la zona di intrusione.

– TIMESTAMP è la data e l'ora di inizio dell'allarme, nel formato YYYY-MM-DDTHH:mm:ss.zzz, dove:
  – YYYY è l'anno in 4 cifre, come 2014.
  – MM è il numero del mese a 2 cifre, ad esempio 01 per gennaio.
  – DD è il numero del giorno su 2 cifre, come 03 per il 3.
  – 'T' è una lettera fissa
  – HH è l'ora nel formato 24 ore, da 00 a 23
  – mm sono i minuti in 2 cifre, da 00 a 59
  – ss sono i secondi in 2 cifre, da 00 a 59
  – zzz sono i millisecondi in 3 cifre, da 000 a 999.
  AXIS Perimeter Defender utilizza la data e l'ora interne della telecamera per generare il timestamp dell'allarme, quindi è importante sincronizzare la telecamera con un qualche tipo di orologio esterno.

– GUID è un identificatore univoco costante per tutti i messaggi correlati allo stesso allarme (quindi ALARM_START, ALARM_IN_PROGRESS e ALARM_STOP)

Questo è l'equivalente, in formato testo, del messaggio ALARM_START:

```
9999|192.168.1.40|0|ALARM_START|INTRUSION|Intrusion-0|2014-03-01T21:24:12.114
```

Esempio:
Un messaggio ALARM_IN_PROGRESS in formato XML è simile all'esempio seguente:

```
<?xml version="1.0"?><KEENEO_MESSAGE xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance"         xmlns:xsd="http://www.w3.org/2001/XMLSchema"         VERSION=
"5.0.0"         ID="9999"         TYPE="ALARM_IN_PROGRESS"         SENDER_IP=
"192.168.1.40"         SENDER_PORT="0">  <REFERENTIAL>0</REFERENTIAL>  <TYPE>INTRUSION</
TYPE>  <SCENARIO_NAME>Intrusion-0</SCENARIO_NAME>  <GUID>77acddf9-e0d4-402e-a497-
231aeee22788</GUID></KEENEO_MESSAGE>
```

- L'intestazione del messaggio è uguale ai messaggi "CONNECTION_TEST" e "ALARM_START".
- Il tipo di messaggio è "ALARM_IN_PROGRESS" e dispone di un set di sottotag.

– REFERENTIAL è l'ID numerico associato alla telecamera.

– TYPE è il tipo di allarme attivato da AXIS Perimeter Defender, lo stesso del corrispondente ALARM_START.

– SCENARIO_NAME è il nome dello scenario che ha attivato l'allarme, lo stesso del corrispondente ALARM_START.

– Il GUID è lo stesso del corrispondente ALARM_START.

Il messaggio ALARM_IN_PROGRESS corrispondente in formato TESTO:

```
9999|192.168.1.40|0|ALARM_IN_PROGRESS|INTRUSION|Intrusion-0|-
```

Esempio:
Un messaggio ALARM_STOP in formato XML è simile all'esempio seguente:

```
<?xml version="1.0"?><KEENEO_MESSAGE xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance"         xmlns:xsd="http://www.w3.org/2001/XMLSchema"         VERSION=
"5.0.0"         ID="9999"         TYPE="ALARM_STOP"         SENDER_IP=
"192.168.1.40"         SENDER_PORT="0">  <REFERENTIAL>0</REFERENTIAL>  <TYPE>INTRUSION</
TYPE>  <SCENARIO_NAME>Intrusion-0</SCENARIO_NAME>  <EXTRA_DATA>zone=testzone</EXTRA_
DATA>  <TIMESTAMP>2014-03-01T21:24:26.304</TIMESTAMP>  <GUID>77acddf9-e0d4-402e-a497-
231aeee22788</GUID></KEENEO_MESSAGE>
```

- L'intestazione del messaggio è la stessa dei messaggi precedenti.
- Il tipo di messaggio è "ALARM_STOP" e ha lo stesso set di sottotipi del messaggio ALARM_START.

Il messaggio ALARM_IN_PROGRESS corrispondente in formato TESTO:

```
9999|192.168.1.40|0|ALARM_STOP|INTRUSION|Intrusion-0|2014-03-01T21:24:26.304
```

La connessione TCP/IP viene sempre chiusa dopo ogni messaggio. Pertanto, il destinatario deve mantenere il socket di ascolto sempre aperto per essere in grado di ricevere ulteriori notifiche.

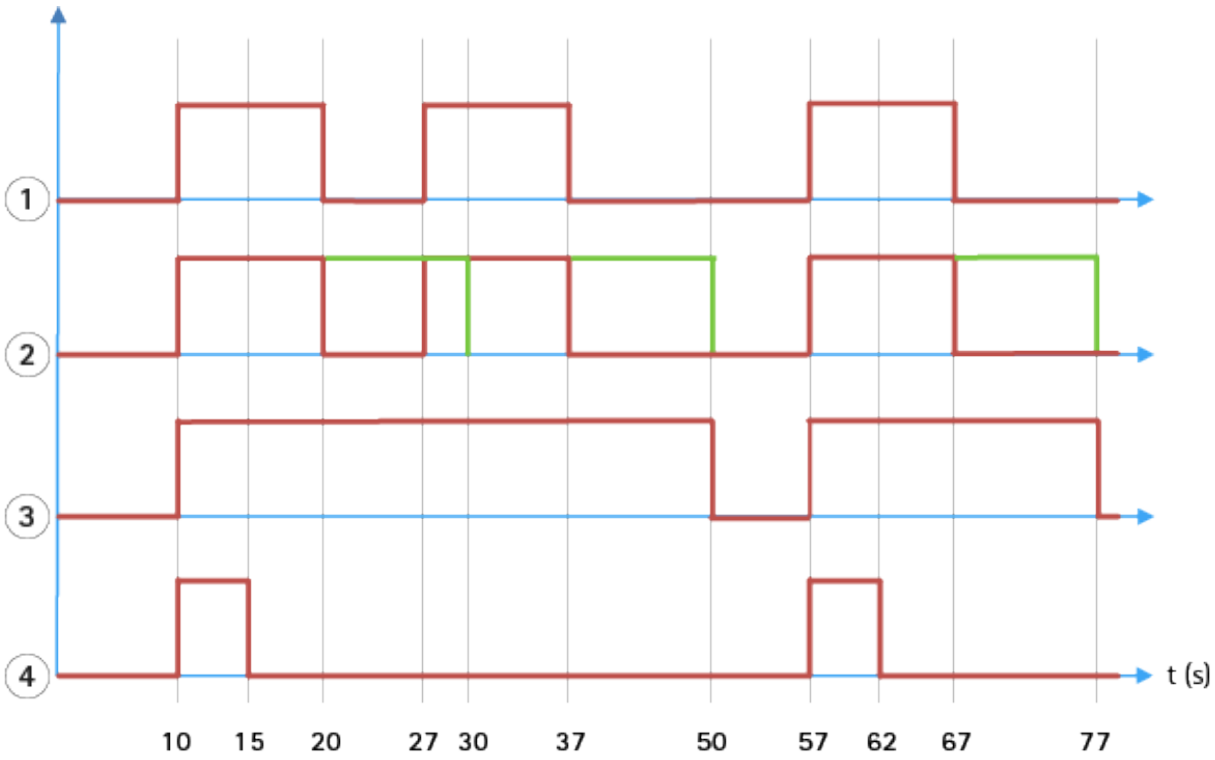
Errori di comunicazione:

Se il destinatario remoto delle notifiche XML non è raggiungibile, ad esempio a causa di una disconnessione di rete, AXIS Perimeter Defender avvia il buffering degli allarmi non recapitati internamente e tenta di reinviarli periodicamente (almeno ogni 10 secondi). Dopo un numero consecutivo di errori nella consegna di nuovi messaggi (i tentativi ripetuti di recapito di un messaggio dal buffer non contano), AXIS Perimeter Defender dichiara il destinatario "permanente offline" e smette di inviare notifiche XML al destinatario. Il numero di errori consecutivi è fissato a 20, approssimativamente corrispondente a 4 o 5 allarmi di intrusione di una durata media di 40 secondi ciascuno. AXIS Perimeter Defender ricomincia ad inviare notifiche allo stesso destinatario se si verifica uno degli eventi seguenti:

- AXIS Perimeter Defender viene riavviato.
- Lo stesso valore del parametro "Alarm streaming url" viene salvato nuovamente.

Tempo post-allarme

AXIS Perimeter Defender implementa l'idea di un "periodo post-allarme". Esso è definito come l'intervallo di tempo dopo l'arresto di un allarme, durante il quale, se viene attivato un altro allarme, entrambi gli allarmi vengono uniti in uno solo.



1 Tre allarmi attivati da AXIS Perimeter Defender nei momenti 10, 27 e 57. Ogni allarme ha una durata di 10 secondi, ad esempio un intruso ha impiegato 10 secondi per attraversare la zona di intrusione.
2 Viene aggiunto un periodo di post-allarme di 10 secondi.
3 Allarmi tramite notifiche XML e metadati XML.
4 Allarmi tramite notifiche e-mail, caricamento dell'immagine su FTP, contatti elettrici e notifiche TCP/IP di base.

(2) Notare come un periodo di post-allarme di 10 secondi (in verde) aumenta la durata di ogni allarme, portando così alla fusione (merge) di due allarmi separati da 10 secondi o meno.

(3) È possibile vedere il numero di allarme e la durata generati da AXIS Perimeter Defender tramite notifiche XML e metadati XML. Il periodo di post-allarme può essere utilizzato per ottenere allarmi meno frequenti e più lunghi invece di molti allarmi più brevi e consecutivi.

(4) Per le notifiche e-mail, il caricamento dell'immagine tramite FTP, i contatti elettrici e le notifiche TCP/IP di base, il risultato dell'utilizzo di un periodo di post-allarme di 10 secondi è diverso. Queste notifiche considerano solo l'avvio dell'allarme e trascurano l'arresto dell'allarme. Pertanto, non vi è alcuna idea di "durata dell'allarme" quando si utilizzano queste notifiche e, di conseguenza, il periodo post-allarme non modifica la durata della notifica stessa. È sempre fissato sul valore scelto dall'utente durante la configurazione della notifica. Pertanto, quando gli allarmi consecutivi vengono uniti in uno a causa del periodo di post-allarme, viene inviata una sola notifica. È possibile vedere che AXIS Perimeter Defender unisce i primi due allarmi, inviando così una sola notifica. Pertanto, le notifiche e-mail, il caricamento delle immagini tramite ftp, i contatti elettrici e le notifiche TCP/IP di base notificano solo due di essi. Il grafico mostra una durata fissa di 5 secondi per queste notifiche.

Come configurare il periodo di post-allarme

1. Aprire AXIS Perimeter Defender Setup.
2. Andare su **Outputs (output)**.
3. Modificare l'impostazione **Post-alarm time (Periodo post-allarme)**. Il valore predefinito è 7 secondi.
4. Fare clic su **Assign (Assegna)**.

Metadati

Sovrimpressione di metadati

La sovrimpressione dei metadati è una funzionalità che può tracciare rilevamenti analitici su determinati flussi in diretta direttamente sulla telecamera. I rilevamenti sono sovrapposizioni grafiche sotto forma di riquadri delimitatori e linee di traiettoria. I flussi vengono selezionati in base alla loro risoluzione e, se il dispositivo dispone del supporto per le aree di visione, a un'area di visione. I metadati sovrimpressi vengono visualizzati sia nella visualizzazione in diretta che durante la riproduzione del materiale registrato.

Sovrimpressioni di metadati sui flussi selezionati

Ad esempio, è possibile impostare l'applicazione in modo che aggiunga sovrapposizioni a tutti i flussi con risoluzione 640x480. In questo caso, solo i flussi con questa risoluzione avranno la sovrapposizione, mentre gli altri rimarranno immutati.

Sovrimpressione di metadati nelle aree di visione selezionate

Se supportata, è anche possibile indicare un'area di visione insieme alla risoluzione. Ad esempio, si può scegliere di avere sovrapposizioni sui flussi recuperati dall'area di visione numero 3 alla risoluzione 1280x720. In questo caso, solo i flussi che corrispondono a questa configurazione avranno le sovrapposizioni, mentre gli altri rimarranno immutati, compresi quelli recuperati dall'area di visione 3, ma a una risoluzione diversa, e quelli recuperati a 1280x720, ma non appartenenti all'area di visione 3.

Aggiungere metadati sovrimpressi al flusso video

Nota

Questa funzione è disponibile solo su dispositivi con software 7.30 o versioni successive.

Questo esempio spiega come attivare le sovrapposizioni di metadati su tutti i flussi video con risoluzione 640x480. I flussi video con qualsiasi altra risoluzione rimangono inalterati.

1. Selezionare la telecamera nel pannello con le viste in tempo reale.
2. Passare a **Outputs > Burnt-in Metadata Overlay (Output > Sovrimpressione metadati)**.
3. Selezionare **Enabled (Abilitata)**.
4. Selezionare la risoluzione 640x480 dall'elenco a discesa.
5. Fare clic su **Applica**.
6. Assicurarsi che i metadati vengano visualizzati nella vista in tempo reale per tale risoluzione.

Integrazione del VMS

AXIS Perimeter Defender si integra perfettamente con i seguenti sistemi di gestione video (VMS):

- Security Center di Genetec™
- XProtect® di Milestone

Per informazioni sulle versioni di VMS supportate, vedere *axis.com/products/axis-perimeter-defender/support-and-documentation*

Gli allarmi attivati da AXIS Perimeter Defender vengono automaticamente convertiti in eventi nel VMS, che a sua volta può attivare un'ampia serie di azioni e sfruttare tutta la potenza del VMS. Contemporaneamente, i metadati in tempo reale generati da AXIS Perimeter Defender vengono inviati al VMS per la visualizzazione e la registrazione in tempo reale. Pertanto, i metadati sono disponibili anche durante la riproduzione delle sequenze video registrate in modalità di riproduzione.

Un sistema di rilevamento delle intrusioni automatizzato è progettato per attivare allarmi e fornire informazioni che consentono di preparare l'intervento di sicurezza. Ciò può includere l'invio di un prompt a un dispositivo mobile o la visualizzazione dell'evento di allarme all'interno di un VMS, magari con il soggetto che ha creato l'evento di allarme evidenziato sullo schermo.

Integrazione di eventi standard

AXIS Perimeter Defender sfrutta ed estende le interfacce e le funzionalità ACAP native per l'invio di allarmi e informazioni supplementari a dispositivi esterni o VMS. Gli eventi emessi da AXIS Perimeter Defender possono essere tradotti in messaggi al VMS, collegandovi regole di azione.

Sono disponibili i seguenti canali di allarme dalla telecamera al VMS:

- semplici notifiche su SMS gratis per allarmi (TCP/IP)
- output elettrici (contatti asciutti o bagnati)
- Notifiche e-mail
- caricamento delle immagini di allarme tramite ftp

Queste integrazioni possono essere configurate sulla telecamera. Vedere *Tempo post-allarme, on page 34*.

Ponti VMS

Per i seguenti sistemi di gestione video, forniamo moduli di integrazione presviluppati, denominati "ponti":

- Milestone XProtect® 2014 e 2016 Corporate/Expert/Enterprise/Professional/Express. Le edizioni Enterprise/Professional/Express non supportano i metadati (non è possibile visualizzare i metadati in diretta o riprodurli)
- Genetec™ Service Center 5,3 e 5,4 Pro/Enterprise/SV32/SV16

I ponti forniscono due integrazioni:

- Creazione di eventi di allarme personalizzati nel VMS, abbinamento dell'output degli eventi di AXIS Perimeter Defender.
- Visualizzazione di sovrapposizioni di allarme o riquadri delimitatori sopra al materiale video in diretta e registrato (tranne che sulle edizioni Enterprise/Professional/Express di Milestone XProtect®).

È necessario scaricare e installare i ponti VMS come applicazioni separate. Per ulteriori informazioni su come installare e configurare questi ponti, consultare il manuale per l'utente per il ponte specifico.

Creare una regola in AXIS Camera Station

Questa sezione indica come integrare AXIS Perimeter Defender con il sistema di eventi AXIS Camera Station. In questa sezione viene descritto come:

- Configurare una regola di AXIS Camera Station da attivare quando si verifica un'intrusione.
- Verificare che la configurazione sia eseguita correttamente.

1. Configurare e calibrare AXIS Perimeter Defender nel software di configurazione AXIS Perimeter Defender. Per assistenza con l'installazione e la calibrazione di AXIS Perimeter Defender, fare riferimento al manuale utente di AXIS Perimeter Defender oppure *o alla pagina del dispositivo*.
2. Aggiungere la telecamera ad AXIS Camera Station seguendo la procedura **Aggiungi telecamera**.
3. Configurare un trigger eventi dispositivo:
   3.1. Andare a **Configurazione** > **Registrazione ed eventi** e aprire la scheda **Regole avanzate**.
   3.2. Creare una nuova regola e selezionare il trigger **Evento dispositivo**.
   3.3. Selezionare la telecamera in cui è installato AXIS Perimeter Defender.
   3.4. Nell'elenco **Evento**, selezionare **AXISPerimeterDefender**.
   3.5. Nell'elenco **Funzione**, selezionare il nome dell'intrusione configurata (in questo caso "Intrusione-1"). Se si desidera attivare la regola per tutti gli scenari configurati, selezionare **ALL_SCENARIOS**.

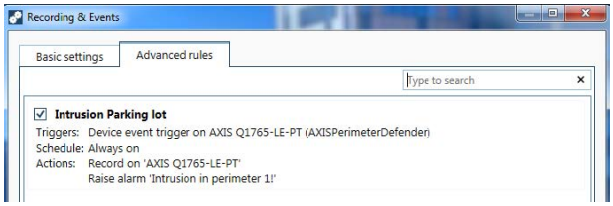
3.6. Selezionare **Sì** se il trigger deve essere attivato quando non si verifica un'intrusione. Quando viene rilevata un'intrusione, la finestra Attività mostrerà una modifica di stato che consente di verificare se la configurazione è corretta.

3.7. Fare clic su **OK** e **Avanti** per configurare le azioni.

3.8. Nella finestra di dialogo **Aggiungi azione**, è possibile aggiungere una o più azioni per la regola.

In questo esempio aggiungiamo un'azione di registrazione e un'azione di allarme.

3.9. Fare clic su **Finish** (Fine).



L'esempio mostra una regola che attiva due azioni quando si verifica un'intrusione.

4. Verificare che la configurazione funzioni come desiderato simulando un'intrusione, ad esempio immettendo fisicamente un'area monitorata.

Interfaccia Web

A partire da AXIS Perimeter Defender 4.0, è ora possibile accedere a un'interfaccia web che consente la configurazione degli scenari senza aver installato l'applicazione desktop.

Per accedere all'interfaccia web:

- Aprire un browser Web.
- Digitare l'indirizzo IP del dispositivo
- Andare a Apps (App)
- Andare a **AXIS Perimeter Defender** nell'elenco e fare clic su **Open** (Apri).

Nota

La calibrazione non è ancora disponibile nell'interfaccia web. Per calibrare la telecamera, utilizzare l'applicazione desktop. Per ulteriori informazioni, andare a *Calibrare - AXIS Perimeter Defender, on page 19*

Scenari

Creare uno scenario di intrusione

Lo scenario di intrusione è progettato per attivare un allarme quando un oggetto entra in una zona definita e rimane nella zona per un periodo di tempo superiore a quello impostato.

Per creare uno scenario di intrusione:

1. Andare alla sezione **Scenarios** (Scenari) nell'interfaccia web.
2. Fare clic su **+ Create** (+ Crea).
3. Selezionare **Intrusion** (Intrusione).
4. Fare clic su **Select this template** (Seleziona questo modello).
5. Impostare un nome descrittivo personalizzato per lo scenario
6. Selezionare il tipo di oggetti che dovrebbero attivare l'allarme.
7. Per ridefinire la zona di rilevamento, trascinare i punti di ancoraggio in qualsiasi direzione. Una volta spostato un punto di ancoraggio, verranno creati nuovi punti di ancoraggio per personalizzare ulteriormente la forma.
8. In **Intrusion Zone** (Zona di intrusione), se non si desidera che un oggetto attivi un allarme non appena entra nella zona, impostare il tempo di **Minimum presence in zone** (Presenza minima nella zona).
9. Se la zona è stretta e può essere attraversata in 1-2 secondi e si desidera ancora attivare allarmi, selezionare **Narrow zone (Restringi zona)**. Per ulteriori informazioni, vedere *Parametri di durata, on page 27*.
10. Fare clic su **Save (Salva)**.

Creare uno scenario di attraversamento zona

Lo scenario di attraversamento zona è progettato per attivare un allarme quando un oggetto si sposta da una zona predefinita a una zona limitata.

Per creare uno scenario di attraversamento zona:

1. Andare alla sezione **Scenarios** (Scenari) nell'interfaccia web.
2. Fare clic su **+ Create** (+ Crea).
3. Selezionare **Zone crossing** (Attraversamento zona).
4. Fare clic su **Select this template** (Seleziona questo modello).
5. Impostare un nome descrittivo personalizzato per lo scenario

6. Selezionare il tipo di oggetti che dovrebbero attivare l'allarme.
7. Per ridefinire le zone predefinite, trascinare i punti di ancoraggio in qualsiasi direzione. Una volta spostato un punto di ancoraggio, verranno creati nuovi punti di ancoraggio per personalizzare ulteriormente la forma.
8. In **Zone 1** (Zona 1), se non si desidera che un oggetto attivi un allarme non appena entra nella zona, impostare il tempo di **Minimum presence in zone** (Presenza minima nella zona).
9. Se la zona è stretta e può essere attraversata in 1-2 secondi e si desidera ancora attivare allarmi, selezionare **Narrow zone (Restringi zona)**. Per ulteriori informazioni, vedere *Parametri di durata, on page 27*.
10. Per decidere quale zona debba essere soggetta a limitazioni, fare clic su una freccia direzionale accanto a **Restricted zone entry** (Accesso zona limitato). Per impostazione predefinita, **Zone 2** (Zona 2) è la zona soggetta a limitazioni.
11. Impostare i parametri per la **Zone 2** (Zona 2).
12. Fare clic su **Save (Salva)**.

Creare uno scenario condizionale

Lo scenario condizionale consente di definire le condizioni per l'attivazione degli allarmi in una scena.

Per creare uno scenario condizionale:

1. Andare alla sezione **Scenarios** (Scenari) nell'interfaccia web.
2. Fare clic su **+ Create** (+ Crea).
3. Selezionare **Conditional** (Condizionale).
4. Fare clic su **Select this template** (Seleziona questo modello).
5. Impostare un nome descrittivo personalizzato per lo scenario
6. Selezionare il tipo di oggetti che dovrebbero attivare l'allarme.
7. Se ha bisogno di più zone rispetto a quelle predefinite, fare clic su **+ Add zone** (+Aggiungi zona)
8. Scegliere la zona corrispondente alla zona di intrusione dal menu a discesa alla voce **Intrusione Zone** (Zona di intrusione). Le frecce indicano la posizione delle diverse zone rispetto alla zona di intrusione scelta.
9. Per ridefinire le zone predefinite, trascinare i punti di ancoraggio in qualsiasi direzione. Una volta spostato un punto di ancoraggio, verranno creati nuovi punti di ancoraggio per personalizzare ulteriormente la forma.
10. Se non si desidera che un oggetto attivi un allarme non appena entra nella zona, impostare il tempo di **Minimum presence in zone** (Presenza minima nella zona).
11. Se la zona è stretta e può essere attraversata in 1-2 secondi e si desidera ancora attivare allarmi, selezionare **Narrow zone (Restringi zona)**. Per ulteriori informazioni, vedere *Parametri di durata, on page 27*.
12. Fare clic su **Save (Salva)**.

Modifica scenari

Per modificare uno scenario creato nell'interfaccia web o nell'app desktop:

1. Andare alla sezione **Scenarios** (Scenari) nell'interfaccia web.
2. Fare clic su **Edit** (Modifica) per lo scenario che si desidera modificare.
3. Fare clic su **Save** (Salva) al termine dell'operazione.

Rinominare gli scenari

Per modificare il nome di più scenari contemporaneamente:

1. Selezionare gli scenari che si desidera rinominare.
2. Fare clic su **Rename** (Rinomina), ora disponibile nel menu.
3. Modificare i nomi a proprio piacimento.
4. Fare clic su **Save (Salva)**.

Eliminare gli scenari

Per eliminare più scenari contemporaneamente:

1. Selezionare gli scenari che si desidera eliminare
2. Fare clic su **Delete** (Elimina), ora disponibile nel menu.
3. Per confermare, fare clic su **Delete** (Elimina).

Impostazioni

L'interfaccia web dispone di un pannello di guida integrata che fornisce informazioni sulle varie impostazioni presenti in ogni pagina. Fare clic sull'icona di aiuto (?) per accedere al pannello.

Risoluzione dei problemi

Affinché tutte le funzionalità funzionino come previsto, è obbligatorio configurare i seguenti parametri Axis:

- Rete / TCP-IP / Base / Router predefinito
- Rete / TCP-IP / Avanzate / Nome di dominio
- Rete / TCP-IP / Server DNS primario
- Rete / TCP-IP / Server DNS secondario
- Rete / TCP-IP / Indirizzo server NTP
- Rete / TCP-IP / SMTP (e-mail)
- Opzioni di sistema / Data e ora / Fuso orario
- Opzioni di sistema / Data e ora / Sincronizza con il server NTP

Aggiornare alla versione più recente

Per sfruttare i miglioramenti più recenti senza dover ricalibrare e ridefinire gli scenari, si consiglia di eseguire l'aggiornamento alla versione più recente di AXIS Perimeter Defender.

1. Scaricare e installare l'ultima versione di AXIS Perimeter Defender.
2. Fare clic su **Installa**. AXIS Perimeter Defender Setup esegue automaticamente i passaggi necessari per completare l'installazione:

– Eseguire il backup della calibrazione, degli scenari, dei parametri e della licenza correnti.

– Installare la nuova versione.

– Ripristinare la licenza.

– Ripristinare la calibrazione e gli scenari.

– Ripristinare i parametri.

– Se un'applicazione era in esecuzione viene riavviata.

Aggiornamento del software della telecamera

Nota

Prima di aggiornare il software della telecamera, salvare tutte le impostazioni di AXIS Perimeter Defender. L'aggiornamento del software rimuove l'applicazione e le relative impostazioni dalla telecamera. Se le impostazioni vengono salvate, possono essere ripristinate utilizzando AXIS Perimeter Defender Setup.

1. Utilizzare AXIS Perimeter Defender Setup per salvare la configurazione del sito.
2. Aggiornamento del software della telecamera. Per istruzioni, consultare il Manuale per l'utente della telecamera.
3. Avviare AXIS Perimeter Defender Setup.
4. Utilizzare l'opzione carica sito per caricare automaticamente la configurazione del sito salvata per ogni telecamera aggiornata.

Risoluzione di problemi relativi all'installazione

Problema	Possibile motivo	Soluzione
C'è un messaggio di Windows® che riporta l'impossibilità di installare il software.	Il sistema operativo del computer portatile o del PC non è compatibile.	Verificare che il sistema operativo Windows® corrisponda a quello specificato nei requisiti.
Viene visualizzato un messaggio di Windows® che indica che l'installazione non è avvenuta correttamente.	Windows® Compatibility Assistant ha rilevato un possibile problema con l'installazione.	Confermare che l'installazione sia comunque corretta e procedere.
L'installazione non riesce durante l'installazione di XVID.	L'installazione di XVID fallisce a causa della vecchia installazione parziale di XVID presente sul computer.	Eliminare la cartella XVID in C:\Programmi (x86) e tentare di nuovo l'installazione.
Il pacchetto di installazione si blocca improvvisamente dopo la visualizzazione della schermata EULA. È presente un messaggio di errore di Windows® che indica che l'applicazione è stata chiusa in modo insolito. È impossibile chiudere il programma di installazione.	Un problema noto nei programmi di installazione porta a un arresto anomalo dell'applicazione in alcune circostanze.	Aprire Gestione attività e terminare tutti i processi "msiexec.exe". Quindi terminare il processo di installazione e riavviare il programma di installazione.

Risoluzione dei problemi di configurazione

Problema	Possibile motivo	Soluzione
Problemi con l'apertura di AXIS Perimeter Defender.	Non si dispone di sufficienti diritti utente di Windows®.	Assicurarsi di disporre dei diritti di amministratore.
La funzionalità di ricerca non trova le mie telecamere.	Firewall	Talvolta, firewall e software antivirus possono bloccare l'individuazione della telecamera. Se necessario, configurare il firewall in modo da consentire il traffico di rete in entrata e in uscita da AXIS Perimeter Defender. Se il problema non dovesse risolversi, configurare il firewall in modo da abilitare il traffico attraverso le seguenti porte: UDP: porta 5353 e TCP: porta 80.
	Problemi con l'indirizzo IP	Tutti i dispositivi in una rete devono avere un indirizzo IP univoco, in modo da poter comunicare con altri dispositivi. Quando si utilizza AXIS Perimeter Defender, si consiglia di utilizzare indirizzi IP fissi per le telecamere. Assicurarsi che ogni dispositivo IP sulla rete abbia un proprio indirizzo IP e non riutilizzi un indirizzo IP già preso.

Problema	Possibile motivo	Soluzione
	La telecamera non è disponibile dal computer dell'utente.	In un browser, accedere all'indirizzo IP della telecamera per verificare se è disponibile o meno. Se non è possibile raggiungerlo, la telecamera non è stata installata correttamente sulla rete o il computer non ha accesso alla telecamera.
Non è possibile aggiungere una telecamera.	I parametri di connessione della telecamera, ad esempio l'indirizzo IP, la password o la porta HTTP, non sono corretti.	Verificare che i parametri immessi siano corretti e ripetere l'operazione.
	La telecamera non può essere visualizzata dal computer dell'utente.	In un browser, accedere all'indirizzo IP della telecamera per verificare se è disponibile o meno. Se non si riesce a raggiungerlo, la telecamera non è stata installata correttamente sulla rete o il computer non ha accesso alla rete su cui si trova la telecamera.
Perdita di flussi video in AXIS Perimeter Defender Setup.	Sorgente video non più disponibile.	La sorgente video è stata interrotta e non è stata aggiornata sul display.
	Utilizzare un browser per verificare se la telecamera è disponibile.	Fare clic sul riquadro in cui deve trovarsi il flusso e ridimensionare l'interfaccia, così il flusso dovrebbe tornare.
La calibrazione automatica non funziona o produce risultati negativi.	I prerequisiti non sono soddisfatti.	Assicurarsi che i requisiti di montaggio siano soddisfatti. Vedere *Montare la telecamera, on page 13*.
	La telecamera presenta una rotazione.	Non è possibile calibrare la telecamera che presenta una rotazione.
	Connessione lenta alla telecamera non configurata come remota.	Collegare la telecamera come dispositivo remoto per ridurre i requisiti di larghezza di banda.
	Ci sono altri oggetti in movimento nella scena utilizzata per la calibrazione automatica, come automobili, alberi o altre persone.	Ripetere la calibrazione automatica o calibrare il dispositivo manualmente.
	Il campo visivo non è sgombro e pulito, rendendo la persona che cammina davanti alla telecamera parzialmente nascosta per molto tempo.	Calibrare il dispositivo manualmente.
	Il campo visivo è piccolo come gli ingressi.	Calibrare il dispositivo manualmente.

Problema	Possibile motivo	Soluzione
	Il video di acquisizione non è stato registrato correttamente a causa dello spazio su disco insufficiente.	Verificare che lo spazio su disco sia sufficiente e che l'applicazione disponga dell'autorizzazione per salvare la registrazione video nel computer in cui è in esecuzione l'interfaccia AXIS Perimeter Defender.

Risoluzione dei problemi relativi alle operazioni

Problema	Possibile motivo	Soluzione
L'applicazione non viene eseguita anche se la configurazione è corretta.	Il software della telecamera non è aggiornato.	Assicurarsi di disporre del software più recente per la telecamera.
La sovrapposizione non viene visualizzata in AXIS Perimeter Defender Setup, anche se l'analisi è in esecuzione.	L'applicazione viene bloccata dopo un'operazione di avvio o arresto o un aggiornamento del pacchetto AXIS Perimeter Defender.	Riavviare la telecamera.
	Un firewall sta bloccando la connessione alla porta di ascolto dei metadati della telecamera.	Configurare il firewall per consentire all'interfaccia di configurazione di connettersi alla porta di ascolto dei metadati sulla telecamera.
	Un programma antivirus sta bloccando la ricezione della sovrapposizione.	Configurare l'antivirus per consentire la ricezione della sovrapposizione.
Nessun allarme viene attivato nel setup di AXIS Perimeter Defender sul computer di configurazione, anche se l'analisi è in esecuzione e la sovrapposizione è visibile.	Anche se l'obiettivo è nella scena, non corrisponde a uno scenario condizionale, ad esempio non si sposta da una zona all'altra nello scenario di attraversamento della zona.	Assicurarsi che lo scenario sia specificato correttamente, incluse le condizioni.
	Scarsa rilevazione.	Assicurarsi che i requisiti di montaggio siano soddisfatti. Vedere *Montare la telecamera, on page 13*. Assicurarsi inoltre che la calibrazione sia sufficientemente precisa e che la sensibilità sia sufficientemente elevata.

Risoluzione dei problemi relativi alle prestazioni

Problema	Possibile motivo	Soluzione
OSD e analisi continuano ad accendersi e spegnersi.	Il carico della CPU nella telecamera è eccessivo.	Soluzioni possibili: • Assicurarsi che i flussi della telecamera non vengano visualizzati inutilmente, poiché ogni istanza aumenta il carico sulla CPU. • Se è attivata la registrazione sul rilevamento movimento incorporato, provare a diminuire la qualità della registrazione per liberare spazio nella CPU. • Disattivare la registrazione del rilevamento del movimento e assicurarsi che il rilevamento del movimento sia disattivato.
La velocità in fotogrammi del video visualizzato è molto bassa.	Troppe visualizzazioni del flusso video possono far scendere la velocità in fotogrammi al di sotto degli 8 fps predefiniti.	Assicurarsi che i flussi della telecamera non vengano visualizzati inutilmente, poiché ogni istanza aumenta il carico sulla CPU.
Un obiettivo entra nella zona sterile e fa scattare diversi avvisi.	La durata del post-allarme è troppo breve.	Regolare la durata del post-allarme. Andare su AXIS Perimeter Defender Setup > **Outputs (output)**.
Un potenziale obiettivo entra nella zona sterile ma non fa scattare un avviso, fallendo il rilevamento.	Il contrasto dell'oggetto contro lo sfondo è troppo basso.	Assicurarsi che i requisiti di montaggio siano soddisfatti. Vedere *Montare la telecamera, on page 13*.
	L'illuminazione della scena è inadeguata o le prestazioni della telecamera con bassa luminosità sono insufficienti.	Assicurarsi che i requisiti di montaggio siano soddisfatti. Vedere *Montare la telecamera, on page 13*.
	AXIS Perimeter Defender ha la sensibilità troppo bassa.	Aumentare la sensibilità nei parametri di scenario globali.
	La telecamera è stata spostata rendendo la calibrazione inesatta.	Ripetere la calibrazione.
	La calibrazione non è sufficientemente precisa.	Verificare la calibrazione della telecamera. Passare a AXIS Perimeter Defender Setup.
	Anche se l'obiettivo si trova nella scena, non corrisponde a uno scenario condizionale. Ad esempio, nello scenario di attraversamento	Controllare che lo scenario sia specificato correttamente, incluse le rispettive condizioni.

Problema	Possibile motivo	Soluzione
	delle zone, l'oggetto non si sposta da una zona all'altra.	
L'obiettivo viene rilevato ma è classificato in modo errato (persona come veicolo o veicolo come persona).	L'altezza, il posizionamento o l'orientamento della telecamera non sono corretti.	Assicurarsi che i requisiti di montaggio siano soddisfatti. Vedere *Montare la telecamera, on page 13*.
	La telecamera è troppo lontana dalla zona.	Assicurarsi che i requisiti di montaggio siano soddisfatti. Vedere *Montare la telecamera, on page 13*.
	Calibrazione non sufficientemente precisa.	Verificare la calibrazione della telecamera. Passare a AXIS Perimeter Defender Setup.
AXIS Perimeter Defender genera un allarme quando non c'è un'intrusione nella zona sterile.	La sensibilità dell'analisi è troppo alta.	Diminuire la sensibilità. Passare a AXIS Perimeter Defender Setup.
	La calibrazione non è sufficientemente precisa.	Verificare la calibrazione della telecamera. Passare a AXIS Perimeter Defender Setup.
	La telecamera è stata spostata rendendo la calibrazione inesatta.	Ripetere la calibrazione.
	Altezza, posizionamento o orientamento errato della telecamera.	Assicurarsi che i requisiti di montaggio siano soddisfatti. Vedere *Montare la telecamera, on page 13*.
	La telecamera si muove, ondeggia o vibra.	Rendere più stabile l'installazione della telecamera.
	Vegetazione, bandiere o altri oggetti in movimento vicino alla telecamera.	Rimuovere gli elementi di disturbo dal campo visivo della telecamera. Gli oggetti che sono costantemente nella scena ma non vicino alla telecamera sono ignorati da AXIS Perimeter Defender.
	Insetti sopra o vicino all'obiettivo della telecamera.	Impedire il più possibile l'ingresso o l'avvicinamento di insetti all'obiettivo della telecamera.

Informazioni su questo manuale

Questo manuale è destinato agli amministratori e agli utenti di AXIS Perimeter Defender. Include le istruzioni per l'uso e la gestione del dispositivo nella rete. È utile avere dell'esperienza precedente di collegamento in rete quando si utilizza questo dispositivo.

Marchi di fabbrica

T10068952_it

2026-03 (M17.3)