AXIS Optimizer

AXIS Optimizer per XProtect®.
AXIS Optimizer for Siemens Siveillance™

Manuale dell'utente

Indice

AXIS Optimizer 7
Uso previsto di AXIS Optimizer 7
Requisiti di sistema 7
Supporto per sistemi federati 7
Supporto per sistemi interconnessi 7
Note sul rilascio 7
Installazione o aggiornamento di AXIS Optimizer 8
Installazione di AXIS Optimizer 8
Quali versioni sono installate nel sistema? 8
Opzioni di installazione avanzate 8
Migrazione del sistema di gestione video (VMS) 9
Verificare l'integrità del programma di installazione 9
Aggiorna AXIS Optimizer 9
Aggiornamento manuale 10
Esegui in automatico l'aggiornamento del sistema 10
Attivazione dell'aggiornamento automatico 10
Disattivazione dell'aggiornamento automatico 11
Per saperne di più 11
Disinstallare AXIS Optimizer 11
Factory default (Valori predefiniti di fabbrica): 11
Messa fuori servizio sicura 11
Privilegi degli utenti 12
Impostazioni dispositivo accessi 13
Assistente dispositivo 13
Configurazione di un dispositivo Axis 13
Installazione di applicazioni in un dispositivo Axis 13
Configurazione delle applicazioni in un dispositivo Axis 13
Aggiornamento delle applicazioni su un dispositivo Axis 13
Riavvio di un dispositivo Axis 14
Copia dell'indirizzo IP di un dispositivo Axis 14
Esegui automazione 15
Creazione di azioni per i dispositivi Axis 15
Plugin server di eventi 15
Installazione del plugin del server di eventi 15
Asciugare più telecamere con un singolo clic 15
Attivazione della messa a fuoco per più telecamere con un clic 16
Attivare più sirene con un solo clic 17
Disattivazione delle privacy mask automaticamente su più telecamere 18
Attivazione di una sirena quando una videocamera rileva movimento 20
Riproduci clip audio su altoparlanti o in una zona altoparlante quando una telecamera rileva movimento 21
Risoluzione dei problemi di una regola 23
Gestione centralizzata degli elenchi delle targhe 23
Creazione di un elenco 23
Configurazione delle autorizzazioni per gli elenchi 24
Modifica di un elenco 24
Importazione di un elenco 24
Esportazione di un elenco 25
Ulteriori informazioni sugli elenchi 26
Rispondi agli eventi in diretta 27
Uso dei comandi del dispositivo 27
Comandi operatore 27
Accesso ai controlli operatore 27

Salvataggio di un'area di messa a fuoco per una telecamera PTZ 27
Esecuzione della messa a fuoco automatica di una telecamera 28
Attivazione di speed dry o del tergicristallo 28
Misura temperatura spot 29
Zoom in avanti e tracciamento automatico di un oggetto in movimento 29
Creazione di comandi operatore personalizzati 30
Configurazione degli accessi ai comandi dell'operatore 30
Interazione attraverso gli altoparlanti 30
Gestore altoparlante 30
Modalità 31
Modalità AXIS Audio Manager Pro 31
Modalità AXIS Audio Manager Edge 33
Modalità legacy 34
Riproduci audio sugli altoparlanti 35
Riproduci audio su altoparlanti nella vista della telecamera 35
Riprodurre l'audio dagli altoparlanti in allarme 36
Impostare il comportamento visivo per l'interazione con l'altoparlante 36
Segnalibri per clip audio nella vista della telecamera o degli allarmi 36
Gestione visitatori 37
Plugin dell'interfono 37
Impostazione di un interfono 37
Impostazione delle autorizzazioni per l'interfono 38
Chiamata di prova 39
Eliminazione dell'eco durante le chiamate 39
Controllo dell'interfono dalla visualizzazione in diretta 39
Risposta a una chiamata dalla visualizzazione in diretta 41
Visualizzazione di più telecamere nella finestra di chiamata 42
Azioni della finestra di chiamata 43
Visualizzare una pagina nella finestra di chiamata 43
Filtro dell'estensione di chiamata 44
Visualizzazione della cronologia di chiamata 44
Disattivazione del microfono in caso di mancanza di chiamate attive 45
Ricezione di un allarme in caso di apertura forzata di una porta 46
Ricezione di un allarme in caso di porta aperta troppo a lungo 46
Esclusione di un client dalla ricezione di chiamate 46
Visualizzazione dell'audio 46
Vista microfono 46
Configurazione di VMS per la vista microfono 47
Aggiunta della vista microfono a Smart Client 47
Usa vista microfono 47
Ascolto di molteplici microfoni in contemporanea 48
Rilevamento di incidenti con l'audio 48
Indaga gli incidenti dopo che sono accaduti 48
Ricerca forense 49
Ricerca forense 49
Prima di iniziare 49
Configurazione della ricerca forense 49
Esecuzione di una ricerca 50
Ottimizzazione di una ricerca 51
Limiti 51
Ricerca veicolo 52
Configurazione della ricerca di veicoli 54
Ricerca di un veicolo 54
Ottimizzazione di una ricerca 54
Ottimizzare la velocità di ricerca 55
Ricerca velocità zona 55

Configura ricerca velocità zona 55
Ricerca di eventi di velocità della zona 56
Ottimizzazione di una ricerca 56
Ricerca contenitore 57
Configurazione della ricerca del contenitore 57
Ricerca di un contenitore 57
Ottimizzazione di una ricerca 58
Creare un report PDF di alta qualità 58
Targhe Axis 58
Prima di iniziare 59
Configurazione delle targhe Axis 59
Ricerca di una targa 59
Ricerca di una targa in diretta 59
Ottimizzazione di una ricerca 60
Ottimizzare la velocità di ricerca 60
Esportare la ricerca di una targa come report PDF 60
Esportare la ricerca di una targa come report CSV 61
Informazioni Axis 61
Accedere ad Axis insights 61
Creare un nuovo dashboard 61
Configurare l'elenco a discesa della dashboard 62
Mostrare gli approfondimenti per una specifica vista della telecamera 62
Configurare Informazioni Axis 62
Risoluzione dei problemi per Axis insights 63
Dewarping video 64
Creazione di una vista con dewarping 64
Creazione di una vista con dewarping per telecamere panoramiche multisensore 65
Vista ampia 66
Impostazione di una posizione iniziale 66
Controllo e modifica delle viste con dewarping da parte degli operatori 67
Prestazioni e risoluzione dei problemi 67
Integrazione di dispositivi indossabili 69
Per saperne di più 69
Controllo accessi 70
Configurazione controllo degli accessi 70
Aggiunta di un door controller di rete Axis al sistema 70
Attivare le licenze per le porte 71
Configurazione del controllo degli accessi 71
Integrazione controllo degli accessi 72
Porte e zone 72
Esempio di porte e zone 73
Aggiunta di una porta 74
Impostazioni della porta 75
Livello di sicurezza porta 76
Opzioni relative all'orario 77
Aggiungi un monitor porta 78
Aggiungere una porta di monitoraggio 78
Aggiungi un lettore 79
Aggiungi un dispositivo REX 80
Aggiunta di una zona 80
Livello di sicurezza zona 81
Ingressi con supervisione 82
Azioni manuali 83
Formati tessera e PIN 83
Impostazioni formato tessera 85
Profili di identificazione 86

Comunicazione crittografata 88
Canale sicuro OSDP 88
Multi-server BETA 88
Flusso di lavoro 88
Genera il file di configurazione dal server secondario 89
Importa il file di configurazione sul server principale 89
Revoca un server secondario 89
Rimuovi un server secondario 89
Gestione degli accessi 89
Flusso di lavoro di gestione degli accessi 90
Aggiungi un titolare tessera 90
Aggiungi credenziali 91
Aggiungi un gruppo 93
Aggiungi una regola di accesso 94
Sbloccare in modo manuale porte e zone 94
Esportazione dei report sulla configurazione del sistema 94
Crea report sull'attività dei titolari di tessere 95
Impostazioni di gestione degli accessi 96
Importa ed esporta 96
Backup e ripristino 97
Gestione degli accessi in Smart Client 98
Impostazioni dei ruoli di AXIS Secure Entry 98
Gestione del sistema e controlli di sicurezza 99
Personalizzazione dell'accesso alle funzionalità per gli operatori 99
Impostazioni ruolo 99
Configura le impostazioni dei ruoli 99
Gestione dei dispositivi 100
AXIS Device Manager Extend 100
Installazione dell'host edge 100
Richiedi l'edge host e sincronizza i dispositivi 101
Usa AXIS Device Manager Extend per la configurazione dei dispositivi 102
Risoluzione dei problemi per aggiungere dispositivi all'host edge 102
Importazione AXIS Site Designer 102
Importazione del progetto 102
Impostazioni importate 103
Limiti 103
Gestione account 104
Connettiti ai dispositivi con l'account del servizio XProtect 104
Eventi Axis 104
Impostare un evento per molteplici dispositivi 105
Informazioni sugli eventi 105
Metadati e ricerca 105
Configurare le impostazioni di metadati 105
Configurare le categorie di ricerca Axis 106
Cyber security 107
Gestione delle vulnerabilità 107
Notifiche di sicurezza 107
Ciclo di vita sicuro del prodotto 107
Guida all'Hardening 107
Bisogno di assistenza? 108
FAQ 108
Risoluzione dei problemi 108
Contattare l'assistenza 108
Consigli e suggerimenti 109
Aggiunta di una pagina Web in una vista Smart Client 109
Esporta video con funzioni di ricerca integrate 109

Esportazione di video in formato XProtect 109
Sblocca le esportazioni sui computer di ricezione 109
Riproduzione della visualizzazione trasformata Axis esportata 109

AXIS Optimizer

AXIS Optimizer sblocca funzionalità Axis direttamente in XProtect o Siemens Siveillance Video. L'applicazione ottimizza le prestazioni dei dispositivi Axis in questi sistemi di gestione video, consentendo di risparmiare tempo e risorse durante la configurazione di un sistema o nell'ambito delle attività quotidiane. L'applicazione è gratuita.

Uso previsto di AXIS Optimizer

Questo prodotto è destinato all'uso da parte di professionisti che dispongono di una conoscenza approfondita del funzionamento di un Video Management System (VMS).

Requisiti di sistema

AXIS Optimizer è totalmente supportato sulle seguenti piattaforme:

- XProtect Essential+
- XProtect Express+
- XProtect Professional+
- XProtect Expert
- XProtect Corporate
- Siemens Siveillance Video Pro
- Siemens Siveillance Video Advanced
- Siemens Siveillance Video Core Plus
- Siemens Siveillance Video Core

Raccomandiamo di usare le versioni più recenti di Management Client e Smart Client. La versione più recente di AXIS Optimizer è sempre testata e compatibile con l'ultima versione del VMS. Per maggiori informazioni, leggere *Note sul rilascio, on page 7*.

Nota

Piattaforma minima supportata

- Versione VMS 2019 R3.

Quando si fa riferimento a Smart Client nella guida, si intende XProtect Smart Client e Video Client in un sistema Siemens.

Supporto per sistemi federati

AXIS Optimizer è totalmente supportato nei sistemi federati.

Supporto per sistemi interconnessi

AXIS Optimizer è totalmente supportato con i sistemi interconnessi.

Nota

Requisiti

- VMS versione 2022 R3 o successiva.

Note sul rilascio

Andare a *axis.com/ftp/pub_soft/cam_srv/optimizer_milestone/latest/relnote.txt* per leggere le note di rilascio più recenti.

Installazione o aggiornamento di AXIS Optimizer

Installazione di AXIS Optimizer



Nota

Per eseguire l'aggiornamento di AXIS Optimizer, è necessario disporre dei diritti di amministratore.

1. Assicurarsi di avere la versione client esatta del VMS.
2. Accedere all'account MyAxis.
3. Da *axis.com/products/axis-optimizer-for-milestone-xprotect*, scaricare AXIS Optimizer su ogni dispositivo che esegue Management Client o Smart Client.
4. Eseguire il file scaricato e seguire le istruzioni nella guida dettagliata.

Quali versioni sono installate nel sistema?

Nella **panoramica del sistema** è possibile controllare quali versioni di AXIS Optimizer e AXIS Optimizer Body Worn Extension sono installate in diversi server e client del tuo sistema.

Nota

Per visualizzare i client o i server del tuo sistema nella **panoramica del sistema**, i server devono avere AXIS Optimizer versione 3.7.17.0, AXIS Optimizer Body Worn Extension versione 1.1.11.0 o versioni successive.

Per vedere i server e i client attivi:

1. Su Management Client, andare a **Site Navigation > AXIS Optimizer > System overview (Navigazione sito > AXIS Optimizer > Panoramica di sistema)**.

Per eseguire l'aggiornamento a un determinato server o client:

1. andare a quel server o client specifico e aggiornarlo localmente.

Opzioni di installazione avanzate

Per eseguire l'installazione di AXIS Optimizer su molteplici dispositivi simultaneamente, senza interazione dell'utente:

1. Fare clic con il pulsante destro del mouse **Start**.
2. fare clic su **Esegui**;
3. Individuare il file di installazione scaricato e fare clic su **Open (Apri)**.
4. Aggiungere uno o molteplici parametri alla fine del percorso.

Parametro	Descrizione
`/SILENT`	Nel corso dell'installazione invisibile, la procedura passo dopo passo e la finestra di sfondo non sono visualizzate. Tuttavia, viene visualizzata la finestra di avanzamento dell'installazione.
`/VERYSILENT`	Durante l'installazione completamente invisibile, non sono mostrate né la procedura passo dopo passo né la finestra di avanzamento dell'installazione.

/FULL	Installare tutti i componenti, ad esempio il plugin opzionale del server eventi e il plugin Secure Entry. È utile combinarlo con /VERYSILENT.
/SUPPRESSMSGBOXES	Sopprimere tutte le finestre di messaggi. Generalmente si combina con /VERYSILENT.
/log=<filename>	Creare un file log.
/NORESTART	Impedire che il computer si riavvii nel corso dell'installazione.
/EVENTSERVERPLUGIN	Effettuare l'installazione del plugin del server evento se il computer di destinazione è il server evento.
/SECUREENTRY	Installare il servizio di controllo degli accessi Secure Entry se il computer di destinazione è il server evento.

5. Premere **Invio**.

Esempio:
Installazione molto invisibile, registrata su output.txt, senza riavvio del computer

```
.\AxisOptimizerXProtectSetup.exe /VERYSILENT /log=output.txt /NORESTART
```

Migrazione del sistema di gestione video (VMS)

AXIS Optimizer memorizza la maggior parte dei dati nel database del VMS e, per questo motivo, le informazioni vengono conservate quando si esegue la migrazione del VMS su un altro server.

Per migrare il VMS su un altro server, consultare *Come trasferire un'installazione/versione di XProtect VMS dai vecchi server ai nuovi*.

Verificare l'integrità del programma di installazione

Per verificare l'integrità del programma di installazione di AXIS Optimizer:

1. Fare clic con il tasto destro del mouse sul file di installazione e selezionare **Properties (Proprietà)**.
2. Andare a **Digital Signatures (Firme digitali)** e fare clic su **Details (Dettagli)**.
3. Verificare quanto segue:
   - Nella sezione **Digital Signature Information (Informazioni sulla firma digitale)** è indicato This digital signature is OK (Questa firma digitale è valida).
   - Nella sezione **Signer information (Informazioni sul firmatario)** > **Name (Nome)** è indicato Axis Communications AB.

Aggiorna AXIS Optimizer

Aggiorniamo regolarmente AXIS Optimizer con nuove funzionalità, miglioramenti e aggiornamenti di sicurezza. AXIS Optimizer offre un unico track di rilascio (l'ultimo e il migliore) ed è solo questa versione più recente ad essere disponibile per il download dal sito axis.com. Si consiglia di utilizzare sempre l'ultima versione di AXIS Optimizer.

AXIS Optimizer include anche una funzione che consente di aggiornare tutti i client presenti nel proprio VMS. Per ulteriori informazioni, consultare la sezione *Aggiornamento automatico del sistema*.

Nota

Per eseguire l'aggiornamento di AXIS Optimizer, è necessario disporre dei diritti di amministratore.

Notifiche di aggiornamento

AXIS Optimizer controlla regolarmente se sono disponibili nuove versioni e invia una notifica quando ci sono nuovi aggiornamenti. Se si dispone di una connessione di rete, si riceveranno notifiche di aggiornamento in Smart Client.

Per cambiare il tipo di notifiche ricevute:

1. In Smart Client, andare a **Settings** > **Axis general options** > **Notification preference** (Impostazioni > Opzioni generali Axis > Preferenze notifiche).
2. Selezionare **All (Tutte)**, **Major (Principali)** o **None (Nessuna)**.

Per effettuare la configurazione di queste notifiche per tutti i client del proprio VMS:

1. Andare a **Management Client (Gestione client)** > **Site Navigation (Navigazione sito)** > **AXIS Optimizer** > **System overview (Panoramica di sistema)**.
2. Fare clic su **System upgrade settings (Impostazioni di aggiornamento sistema)**.
3. Attivare o disattivare **Show upgrade notifications on all clients (Mostra notifiche di aggiornamento su tutti i client)**.

Aggiornamento manuale

È possibile eseguire l'aggiornamento manuale di AXIS Optimizer sia da Management Client che da Smart Client.

Nota

Per eseguire l'aggiornamento di AXIS Optimizer, è necessario disporre dei diritti di amministratore.

In Management Client

1. Andare a **Site Navigation > Basics > AXIS Optimizer (Navigazione sito > Operazioni di base > AXIS Optimizer)**.
2. Fare clic su **Update (Aggiorna)**.

In Smart Client

1. Andare a **Settings > Axis general options (Impostazioni > Opzioni generali di Axis)**.
2. Fare clic su **Update (Aggiorna)**.

Esegui in automatico l'aggiornamento del sistema

Dal server di gestione VMS, è possibile pubblicare una versione locale di AXIS Optimizer nel sistema. Una volta che avrai fatto ciò, AXIS Optimizer sarà aggiornato in automatico su tutti i computer client. L'aggiornamento automatico non interrompe mai il lavoro dell'operatore. Le installazioni invisibili sono eseguite nel corso del riavvio del computer o del client VMS. Anche quando il client non è connesso a Internet, l'aggiornamento automatico è supportato.

Nota

Il supporto per l'aggiornamento automatico è disponibile per i client che eseguono AXIS Optimizer 4.4 o versione successiva.

Attivazione dell'aggiornamento automatico



Nota

Requisiti

- Un sistema in cui il Management Client viene eseguito sullo stesso computer del server di gestione VMS.
- Diritti di amministratore del PC sul server di gestione VMS.

Per l'attivazione dell'aggiornamento automatico, devi pubblicare una versione specifica di AXIS Optimizer sul tuo sistema:

1. Nel server di gestione VMS, installare la versione di AXIS Optimizer che si desidera pubblicare nell'intero sistema.
2. Sul computer server di gestione VMS, aprire Management Client.
3. Andare a **Site Navigation > AXIS Optimizer > System overview (Navigazione sito > AXIS Optimizer > Panoramica di sistema)**.
4. Fare clic su **System upgrade settings (Impostazioni di aggiornamento sistema)**.
5. Verificare che **Local version (Versione locale)** sia corretta e fare clic su **Publish (Pubblica)**.
   Se esiste già una versione pubblicata di AXIS Optimizer, viene sostituita dalla nuova versione

Nota

I computer client con una versione di AXIS Optimizer precedente alla 4.4 vanno aggiornati in modo manuale.

Disattivazione dell'aggiornamento automatico

Per la disattivazione dell'aggiornamento automatico, devi ripristinare la versione pubblicata:

1. Sul computer server di gestione VMS, aprire Management Client.
2. Andare a **Site Navigation > AXIS Optimizer > System overview (Navigazione sito > AXIS Optimizer > Panoramica di sistema)**.
3. Fai clic su **System upgrade settings > Reset published version (Impostazioni aggiornamento sistema > Ripristina versione pubblicata)**.

Per saperne di più

- Gli Smart Client che non dispongono di AXIS Optimizer possono accedere al file del programma di installazione pubblicato dalla pagina Web del server di gestione (*http://[serveradress]/installation/*) anche se non sono connessi a Internet.
- Il pacchetto di installazione di AXIS Optimizer è disponibile e configurabile in Download Manager del VMS.
- Nei sistemi federati o interconnessi, è necessario pubblicare AXIS Optimizer su ciascun server di gestione.
- Dopo la pubblicazione di una nuova versione di AXIS Optimizer, puoi monitorare quali client hanno eseguito l'aggiornamento alla versione pubblicata. I computer nella pagina **System overview (Panoramica del sistema)** mostreranno una spunta verde quando eseguono la versione pubblicata.
- L'aggiornamento automatico è disattivato sui computer che eseguono un server di gestione VMS.

Disinstallare AXIS Optimizer

Factory default (Valori predefiniti di fabbrica):

Per ripristinare le impostazioni predefinite di AXIS Optimizer, disinstallarlo dal VMS e reinstallarlo.

Messa fuori servizio sicura

Per rimuovere completamente AXIS Optimizer e i dati memorizzati dal VMS, è necessario eseguire prima i seguenti passaggi, ove applicabili, prima della rimozione dal computer locale.

1. Per rimuovere gli elenchi delle targhe:
   – Aprire la Gestione Client e andare a **AXIS Optimizer** > **License plate lists (Elenchi targhe)**.

- Rimuovere tutti i siti dall'elenco.

2. Per scollegare il server AXIS Audio Manager Pro:
   - Aprire Gestione Client e andare a **AXIS Optimizer** > **Speaker manager (Gestione altoparlanti)**.
   - Fai clic su **Disconnect (Disconnetti)**.

Rimuovere AXIS Optimizer e i dati memorizzati localmente dal computer:

1. Fare clic sul **menu Start > Settings (Impostazioni)** > **App** > **Installed apps (App installate)**.
2. Andare alla scheda **AXIS Optimizer**.
3. Fare clic sul menu p,255mm,sfx)=″graphics:graphicE602A880D1B5621C58ABCAEDE29CCC0F″ e selezionare **Uninstall (Disinstalla)**.

Nota

Dopo aver disinstallato AXIS Optimizer, potrebbe essere necessario effettuare un riavvio di alcuni servizi VMS.

Privilegi degli utenti

AXIS Optimizer include un ruolo utente Axis Optimizer specifico. Lo scopo è rendere più semplice concedere i privilegi Smart Client necessari agli utenti per utilizzare le funzionalità AXIS Optimizer.

Se si esegue XProtect 2018 R3 o una versione precedente, questo ruolo è disponibile solo in XProtect Corporate.

Se si esegue XProtect 2019 R1 o versione successiva, questo ruolo è disponibile per le seguenti edizione XProtect:

- Corporate
- Expert
- Professional+
- Essential+
- Express+

Se si preferisce configurare manualmente i privilegi, utilizzare questa configurazione per consentire a un operatore Smart Client di utilizzare tutte le funzionalità incluse in AXIS Optimizer:

- Hardware: comandi driver
- Telecamere: comandi AUX

Nota

Per una gestione avanzata dei ruoli utente, vedere *Personalizzazione dell'accesso alle funzionalità per gli operatori, on page 99*.

Impostazioni dispositivo accessi

Assistente dispositivo

Usa Assistente dispositivo per dare un facile accesso a tutte le impostazioni dei dispositivi Axis direttamente in Management Client del sistema VMS. È possibile trovare e raggiungere facilmente la pagina Web del dispositivo Axis all'interno del VMS per modificare le diverse impostazioni del dispositivo. È inoltre possibile configurare le applicazioni installate sui dispositivi.

Importante

- Per usare Device assistant, è necessario che il dispositivo Axis sia connesso alla stessa rete di Management Client.
- Assistente dispositivo non è supportato sulle reti IPv6.

Configurazione di un dispositivo Axis

1. In Management Client, andare a **Site Navigation > AXIS Optimizer > Device assistant (Navigazione sito > AXIS Optimizer > Assistente dispositivo)**.
2. Selezionare un dispositivo e andare a **Device settings (Impostazioni dispositivo)**. Si apre la pagina web del dispositivo.
3. Configurare le impostazioni desiderate.

Installazione di applicazioni in un dispositivo Axis

1. In Management Client, andare a **Site Navigation > AXIS Optimizer > Device assistant (Navigazione sito > AXIS Optimizer > Assistente dispositivo)**.
2. Selezionare un dispositivo e andare a **Device settings (Impostazioni dispositivo)**. Si apre la pagina web del dispositivo.
3. Andare a **Apps (App)**. La posizione di **Apps (App)** dipende dalla versione del software del dispositivo. Per ulteriori informazioni, vedere la guida del dispositivo.
4. Installare le applicazioni desiderate.

Configurazione delle applicazioni in un dispositivo Axis

1. In Management Client, andare a **Site Navigation > AXIS Optimizer > Device assistant (Navigazione sito > AXIS Optimizer > Assistente dispositivo)**.
2. Selezionare un dispositivo e andare ad **Applications (Applicazioni)**. Se sul dispositivo sono installate applicazioni, verranno visualizzate qui.
3. Accedere all'applicazione pertinente, ad esempio AXIS Object Analytics.
4. Configurare l'applicazione in base alle proprie esigenze.

Aggiornamento delle applicazioni su un dispositivo Axis

1. In Management Client, andare a **Site Navigation > AXIS Optimizer > Device assistant (Navigazione sito > AXIS Optimizer > Assistente dispositivo)**.
2. Fare clic con il pulsante destro del mouse su un dispositivo e selezionare **Show updates (Mostra aggiornamenti)**. Se è possibile aggiornare tutte le applicazioni, verrà visualizzato un elenco degli aggiornamenti disponibili.
3. Scaricare il file di aggiornamento.
4. Fare clic su **How to update (Come eseguire l'aggiornamento)** e seguire le istruzioni.

Riavvio di un dispositivo Axis

1. In Management Client, andare a **Site Navigation > AXIS Optimizer > Device assistant (Navigazione sito > AXIS Optimizer > Assistente dispositivo)**.
2. Fare clic con il pulsante destro del mouse su un dispositivo e selezionare **Restart device (Riavvia dispositivo)**.

Copia dell'indirizzo IP di un dispositivo Axis

1. In Management Client, andare a **Site Navigation > AXIS Optimizer > Device assistant (Navigazione sito > AXIS Optimizer > Assistente dispositivo)**.
2. Fare clic con il pulsante destro del mouse su un dispositivo e selezionare **Copy device address (Copia indirizzo dispositivo)**.

Esegui automazione

Creazione di azioni per i dispositivi Axis

Plugin server di eventi

Il plugin del server di eventi AXIS Optimizer consente la creazione di azioni personalizzate per i dispositivi Axis. Quando si utilizza il motore delle regole XProtect e il plugin del server di eventi, è possibile ad esempio:

- Eseguire un'operazione personalizzata quando l'operatore fa clic su un pulsante in Smart Client. Per un esempio di impostazione, vedere *Asciugare più telecamere con un singolo clic, on page 15*.
- Eseguire azioni senza interazioni umane (automazione). Per un esempio di impostazione, vedere *Disattivazione delle privacy mask automaticamente su più telecamere, on page 18*.

Il plugin del server di eventi è composto da due parti:

- Un plugin separato che viene eseguito sul server di eventi. Ciò popola il motore delle regole con nuove azioni.
- Una pagina chiamata **Axis actions (Azioni Axis)** nel server di gestione in cui è possibile procedere alla creazione di nuove azioni preset.

Le azioni personalizzate per i dispositivi Axis sono: esegui controllo operatore, attiva/disattiva il radar, avvia la chiamata all'interfono e asciuga la telecamera (SpeedDry/tergicristallo).

Il plugin server di eventi è compreso in AXIS Optimizer. In un sistema a più PC, è possibile eseguire l'installazione di AXIS Optimizer sul computer Management Client e sul computer del server di eventi.

Installazione del plugin del server di eventi

Il plugin del server di eventi è un componente facoltativo compreso nel programma di installazione di AXIS Optimizer. È possibile eseguirne l'installazione solo su un server di eventi del video management system (VMS). Se i requisiti sono soddisfatti, l'installazione del plugin del server eventi verrà richiesta quando si esegue il programma di installazione di AXIS Optimizer.

Nota

Il server di eventi VMS necessiterà di un breve riavvio nel corso dell'installazione e a volte nell'ambito dell'aggiornamento di AXIS Optimizer. Verrà ricevuta una notifica in questo caso.

Asciugare più telecamere con un singolo clic

Con il plugin Server di eventi è possibile impostare regole personalizzate per agevolare gli operatori. Questo esempio mostra come si asciugano tutte le telecamere in un'area specifica con un clic su un pulsante di sovrapposizione testo.



Nota

Requisiti

- AXIS Optimizer versione 4.0 o successiva sul server di eventi e in Management Client
- Una o più telecamere che supportano la funzione SpeedDry o tergicristallo (ad esempio AXIS Q86, Q87 o Q61 Series).

1. Aggiungere un evento definito dall'utente:

1.1. Vai a **Site Navigation > Rules and Events (Navigazione sito > Regole ed eventi)** e fai clic con il pulsante destro del mouse su **User-defined Event (Evento definito dall'utente)**.

1.2. Selezionare **Add User-defined Event (Aggiungi evento definito dall'utente)** e immettere un nome, in questo esempio "Asciuga tutte le telecamere".

2. Creare una nuova regola:

2.1. Andare a **Site Navigation > Rules and Events (Navigazione sito > Regole ed eventi)** e fare clic con il pulsante destro del mouse su **Rules (Regole)**.

2.2. Selezionare **Add Rule (Aggiungi regola)** e immettere un nome, in questo esempio "Regola asciuga tutte le telecamere".

2.3. Selezionare **Perform an action on <event>(Esegui un azione legata all'evento)**.

2.4. Nel campo **Edit the rule description (Modifica la descrizione della regola)**, fare clic su **event (evento)**.

2.5. Andare a **Events > External Events > User-defined Events (Eventi > Eventi esterni > Eventi definiti dall'utente)** e selezionare **Dry all cameras (Asciuga tutte le telecamere)**.

2.6. Fare clic su **Next (Avanti)** finché non si arriva a **Step 3: Actions (Passaggio: 3 Azioni)**.

2.7. Selezionare l'azione: **Axis: Dry <camera>**.

2.8. Nel campo **Edit the rule description (Modifica la descrizione della regola)**, fare clic su **Axis: Dry camera**.

2.9. Nella finestra **Select Triggering Devices (Seleziona dispositivi di attivazione)**, scegliere **Select devices (Seleziona dispositivi)** e fare clic su **OK**.

2.10. Selezionare i dispositivi su cui si desidera attivare l'azione e fare clic su **OK**, quindi su **Finish (Fine)**.

3. In Smart Client, aggiungere l'evento definito dall'utente come pulsante di sovrapposizione su una mappa o vista video.

4. Fare clic sul pulsante di sovrapposizione testo e assicurarsi che la regola operi come desiderato.

Attivazione della messa a fuoco per più telecamere con un clic

Con il plugin Server di eventi è possibile impostare regole personalizzate per agevolare gli operatori. In questo esempio illustreremo come si attiva la messa a fuoco automatica per tutte le telecamere con un singolo clic.

Nota

Requisiti

- AXIS Optimizer versione 4.1 o versione successiva sul server di eventi e in Management Client
- Una o più telecamere che supportano la messa a fuoco automatica

1. Aggiungere un evento definito dall'utente:

1.1. Vai a **Site Navigation > Rules and Events (Navigazione sito > Regole ed eventi)** e fai clic con il pulsante destro del mouse su **User-defined Event (Evento definito dall'utente)**.

1.2. Selezionare **Add User-defined Event (Aggiungi evento definito dall'utente)** e immettere un nome, in questo esempio "Messa a fuoco automatica".

2. Creare una nuova regola:

2.1. Andare a **Site Navigation > Rules and Events (Navigazione sito > Regole ed eventi)** e fare clic con il pulsante destro del mouse su **Rules (Regole)**.

2.2. Selezionare **Add Rule (Aggiungi regola)** e immettere un nome, in questo esempio "Esegui messa a fuoco automatica".

2.3. Selezionare **Perform an action on <event>(Esegui un azione legata all'evento)**.

2.4. Nel campo **Edit the rule description (Modifica la descrizione della regola)**, fare clic su **event (evento)**.

2.5. Andare a **Events > External Events > User-defined Events (Eventi > Eventi esterni > Eventi definiti dall'utente)** e selezionare **Autofocus (Messa a fuoco automatica)**. Fare clic su **OK**.

2.6. Fare clic su **Next (Avanti)** finché non si arriva a **Step 3: Actions (Passaggio: 3 Azioni)**.

2.7. Selezionare l'azione **Axis: Run autofocus on <camera>(Esegui messa a fuoco automatica sulla telecamera)**.

2.8. Nel campo **Edit the rule description (Modifica la descrizione della regola)**, fare clic su **Axis: Run autofocus on camera (Esegui messa a fuoco automatica sulla telecamera)**.

2.9. Nella finestra **Select Triggering Devices (Seleziona dispositivi di attivazione)**, scegliere **Select devices (Seleziona dispositivi)** e fare clic su **OK**.

2.10. Selezionare i dispositivi su cui si desidera attivare l'azione e fare clic su **OK**, quindi su **Finish (Fine)**.

3. In Smart Client, aggiungere l'evento definito dall'utente "Messa a fuoco automatica" come pulsante di sovrapposizione su una mappa o una vista video.
4. Fare clic sul pulsante di sovrapposizione testo e assicurarsi che la regola operi come desiderato.

Attivare più sirene con un solo clic

Con il plugin Server di eventi è possibile impostare regole personalizzate per agevolare gli operatori. In questo esempio viene mostrato come attivare più sirene di protezione con un solo clic in Smart Client.

Nota

Requisiti

- AXIS Optimizer versione 4.4 o versione successiva sul server di eventi e in Management Client
- Una o più sirene Axis
- L'uscita 1 della sirena stroboscopica di Axis è stata abilitata e aggiunta ai dispositivi di uscita nel Management Client

1. Creare un evento definito dall'utente:
   1.1. Vai a **Site Navigation > Rules and Events (Navigazione sito > Regole ed eventi)** e fai clic con il pulsante destro del mouse su **User-defined Event (Evento definito dall'utente)**.
   1.2. Selezionare **Add User-defined Event (Aggiungi evento definito dall'utente)** e immettere un nome, ad esempio "Attiva tutte le sirene".
2. In Assistente dispositivo, creare profili della sirena:
   2.1. Vai in **Site Navigation > AXIS Optimizer > Device assistant (Site Navigation > AXIS Optimizer > Device assistant)**.
   2.2. Selezionare una sirena. Viene visualizzata la pagina Web della sirena.
   2.3. Vai su **Profiles (Profili)** e fai clic su **Add profile (Aggiungi profilo)**.
   2.4. Configurare l'operazione che si desidera eseguire quando l'operatore attiva le sirene in Smart Client
   2.5. Creare gli stessi profili sull'altra sirena. È necessario utilizzare lo stesso nome del profilo su tutti i dispositivi
3. Nelle azioni Axis, creare un preset di azione:
   3.1. Andare in **Site Navigation (Navigazione del sito) > Rules and Events (Regole ed eventi) > Axis actions (Azioni Axis)**.
   3.2. Fare clic su **Add new preset (Aggiungi nuovo preset)**.
   3.3. Vai in **Select strobe siren (Seleziona sirena)** e fai clic su **Strobe siren (Sirena)**.
   3.4. Selezionare le sirene che si desidera utilizzare e fare clic su **OK**.
   Viene visualizzato un elenco di profili delle sirene
   3.5. Selezionare il profilo sirena creato al passaggio precedente. L'azione preimpostata viene salvata automaticamente

3.6. Premere F5 per aggiornare la configurazione del server. Ora è possibile iniziare a utilizzare il nuovo preset azione creato.

4. Creare una regola:
   4.1. Andare a **Site Navigation > Rules and Events (Navigazione sito > Regole ed eventi)** e fare clic con il pulsante destro del mouse su **Rules (Regole)**.
   4.2. Selezionare **Add Rule (Aggiungi regola)** e immettere un nome, ad esempio "Attiva tutte le regole per tutte le sirene".
   4.3. Selezionare **Perform an action on <event>(Esegui un azione legata all'evento)**.
   4.4. Nel campo **Edit the rule description (Modifica la descrizione della regola)**, fare clic su **event (evento)**.
   4.5. Andare a **Events > External Events > User-defined Events (Eventi > Eventi esterni > Eventi definiti dall'utente)** e selezionare **Trigger all strobe sirens (Attiva tutte le sirene)**.
   4.6. Fare clic su **Next (Avanti** finché non si arriva a **Step 3: Actions (Passaggio 3: Azioni)**.
   4.7. Selezionare l'azione **Axis: Run a profile on a strobe siren: <preset>(avviare o arrestare un profilo su una sirena stroboscopica: evento**.
   4.8. Nel campo **Edit the rule description (Modifica la descrizione della regola)**, fare clic su **preset**.
   4.9. Selezionare quale preset che si desidera utilizzare.
   4.10. Fare clic su **Next (Avanti)** quindi su **Finish (Fine)**.
5. In Smart Client, aggiungere l'evento definito dall'utente come pulsante di sovrapposizione su una mappa o vista video.
6. Fare clic sul pulsante di sovrapposizione testo e assicurarsi che la regola operi come desiderato.

Disattivazione delle privacy mask automaticamente su più telecamere

Con il plugin del server di eventi è possibile rendere automatizzate determinate azioni. Questo esempio mostra come si disattivare in automatico le privacy mask su più telecamere quando si verifica un evento di analisi. Nell'esempio, l'evento è l'ingresso di persone o veicoli in un'area alla quale normalmente non dovrebbero accedere. Quando si ha una migliore vista di ciò che sta accadendo le privacy mask potranno essere disabilitate automaticamente.



Il flusso di lavoro è:

1. *Configurazione di uno scenario dell'analitica, on page 19* in AXIS Object Analytics (o altre applicazioni di analisi desiderate)
2. *Aggiunta dei comandi operatore alle telecamere pertinenti, on page 19*
3. *Creazione delle azioni preimpostate, on page 19*
4. *Creazione di una regola per la disattivazione delle privacy mask quando si verifica l'evento di analisi, on page 19*
5. *Creazione di una regola per riattivare le privacy mask, on page 20*
6. *Test della regola, on page 20* e verificare che tutto funzioni correttamente.

Nota

Requisiti

- AXIS Optimizer versione 4.0 o successiva sul server di eventi e in Management Client
- Telecamere dotate di AXIS OS 7.40 o versione successiva
- Telecamere capaci di generare eventi, in questo esempio una telecamera dotata di AXIS Object Analytics

Configurazione di uno scenario dell'analitica

1. Andare a **Site Navigation > AXIS Optimizer > Device assistant (Navigazione sito > AXIS Optimizer > Assistente dispositivo)** e cercare il dispositivo con le analisi desiderate.
2. Fare clic su **Applications (Applicazioni)** e creare uno scenario di analisi che attiverà l'azione.
3. Andare a **Devices > Cameras (Dispositivi > Telecamere)** e cercare la telecamera sulla quale è stato creato lo scenario di analisi.
4. Nella finestra **Properties (Proprietà)**, fare clic su **Events > Add (Eventi > Aggiungi)**.
5. Selezionare un evento driver, in questo esempio "Object Analytics: test evento salita" e fare clic su **OK**.
6. Fare clic su **Add (Aggiungi)** e selezionare l'evento driver "Object Analytics: test evento caduta." Quindi, fare clic su **OK**.
7. Fare clic su **Save (Salva)**.

Aggiunta dei comandi operatore alle telecamere pertinenti

1. Andare a **AXIS Optimizer > Operator controls (AXIS Optimizer > Comandi operatore)** e aprire la libreria Controlli.
2. Nella finestra **Configuration (Configurazione)**, selezionare la cartella pertinente e attivare **Turn off privacy mask (Disattiva privacy mask)** e **Turn on privacy mask (Attiva privacy mask)**.

Creazione delle azioni preimpostate

1. Andare a **Rules and Events > Axis actions (Regole ed eventi > Azioni Axis)** e fare clic su **Add new preset (Aggiungi nuovo preset)**.
2. Fare clic su **Cameras (Telecamere)** e selezionare le telecamere pertinenti. In questo esempio: AXIS P1375 e AXIS Q6075-E. Quindi, selezionare il comando **Turn on privacy mask (Attiva privacy mask)**.
3. Fare clic su **Add new preset > Cameras (Aggiungi nuovo preset > Telecamere)** e selezionare le telecamere pertinenti. In questo esempio: AXIS P1375 e AXIS Q6075-E. Quindi, selezionare il comando **Turn off privacy mask (Disattiva privacy mask)**.

Creazione di una regola per la disattivazione delle privacy mask quando si verifica l'evento di analisi

1. Andare a **Site Navigation > Rules and Events (Navigazione sito > Regole ed eventi)** e fare clic con il pulsante destro del mouse su **Rules (Regole)**.
2. Selezionare **Add Rule (Aggiungi regola)** e immettere un nome, in questo esempio "Disattiva privacy mask all'avvio dell'analisi".
3. Selezionare **Perform an action on <event>(Esegui un azione legata all'evento)**.
4. Nel campo **Edit the rule description (Modifica la descrizione della regola)**, fare clic su **event (evento)**. Andare in **Devices (Dispositivi) > Configurable Events (Eventi configurabili)** e selezionare **Object Analytics: Event test Rising (Analisi oggetti: test eventi ascendente)**.
5. Nel campo **Edit the rule description (Modifica la descrizione della regola)**, selezionare un dispositivo, in questo esempio AXIS P1375.
6. Fare clic su **Next (Avanti)** finché non si arriva a **Step 3: Actions (Passaggio: 3 Azioni)**.
7. Selezionare l'azione **Axis: Run operator control: (Esegui comando operatore) <preset>**.
8. Nel campo **Edit the rule description (Modifica la descrizione della regola)**, fare clic su **preset**. Aggiungere quindi l'obiettivo **Turn off privacy mask on 2 cameras (Disattiva privacy mask su 2 telecamere)** e fare clic su **OK**.

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

Creazione di una regola per riattivare le privacy mask

1. Selezionare **Add Rule (Aggiungi regola)** e immettere un nome, in questo esempio "Attiva privacy mask all'arresto dell'analisi".
2. Selezionare **Perform an action on <event>(Esegui un azione legata all'evento)**.
3. Nella sezione **Edit the rule description (Modifica la descrizione della regola)**, fare clic su **event (evento)**. Andare in **Devices (Dispositivi) > Configurable Events (Eventi configurabili)** e selezionare **Object Analytics: Event test Failing (Analisi oggetti: test eventi discendente)**.
4. Nella sezione **Edit the rule description (Modifica la descrizione della regola)**, selezionare un dispositivo, in questo esempio AXIS P1375.
5. Fare clic su **Next (Avanti)** finché non si arriva a **Step 3: Actions (Passaggio: 3 Azioni)**.
6. Selezionare l'azione **Axis: Run operator control: (Esegui comando operatore) <preset>**.
7. Nella sezione **Edit the rule description (Modifica la descrizione della regola)**, fare clic su **preset**. Aggiungere quindi l'obiettivo **Turn on privacy mask on 2 cameras (Attiva privacy mask su 2 telecamere)** e fare clic su **OK**.
8. Fare clic su **Finish (Fine)**.

Test della regola

1. Andare a **AXIS Optimizer > Device assistant (AXIS Optimizer > Assistente dispositivo)** e trovare il dispositivo con le analisi usate per la creazione dell'automazione. In questo esempio AXIS P1375.
2. Aprire lo scenario pertinente e fare clic su **Test alarm (Verifica allarme)**.

Attivazione di una sirena quando una videocamera rileva movimento

Con il plugin del server di eventi, hai la possibilità di impostare regole personalizzate per l'automatizzazione delle azioni. In questo esempio viene mostrato come attivare automaticamente le sirene quando una videocamera rileva movimento.

Nota

Requisiti

- AXIS Optimizer versione 4.4 o versione successiva sul server di eventi e in Management Client
- Una o più sirene Axis
- L'uscita 1 della sirena stroboscopica di Axis è stata abilitata e aggiunta ai dispositivi di uscita nel Management Client.
- Per una versione precedente rispetto alla versione VMS 2022 R2, le azioni Axis non sono disponibili come azioni di arresto. Per le versioni precedenti è necessario creare due regole separate per l'esecuzione e l'arresto della sirena stroboscopica.

1. Crea profili di sirena stroboscopica:
   1.1. Vai in **Site Navigation > AXIS Optimizer > Device assistant (Site Navigation > AXIS Optimizer > Device assistant)**.
   1.2. Vai su **Axis output devices (Dispositivi output Axis)** e seleziona una sirena stroboscopica. Viene visualizzata la pagina Web della sirena.
   1.3. Vai su **Profiles (Profili)** e fai clic su **Add profile (Aggiungi profilo)**.
   1.4. Assicurati di scegliere lo stesso nome di profilo per tutte le sirene.
   1.5. Configurare l'operazione che deve eseguire la sirena quando rileva movimento.
2. Crea preset di azione per l'avvio e l'arresto:
   2.1. Andare in **Site Navigation (Navigazione del sito) > Rules and Events (Regole ed eventi) > Axis actions (Azioni Axis)**.

2.2. Per creare un preset di avvio, vai su **Strobe siren (Sirena stroboscopica)** e fai clic su **Add new preset (Aggiungi nuovo preset)**.

2.3. Vai in **Select strobe siren (Seleziona sirena)** e fai clic su **Strobe siren (Sirena)**.

2.4. Seleziona una o più sirene stroboscopiche dall'elenco.

2.5. Seleziona dalla lista il profilo sirena che hai creato precedentemente. L'azione preimpostata viene salvata automaticamente

2.6. Per creare un preset di arresto, fai clic su **Add new preset (Aggiungi nuovo preset)**.

2.7. Vai in **Select strobe siren (Seleziona sirena)** e fai clic su **Strobe siren (Sirena)**.

2.8. Seleziona dall'elenco le stesse sirene stroboscopiche scelte per il preset di avvio.

2.9. Vai a **Select action (Seleziona azione)** e seleziona **Stop (Arresta)**.

2.10. Seleziona lo stesso profilo di sirena che è creato per l'azione di avvio. L'azione preimpostata viene salvata automaticamente

2.11. Fare clic su **per aggiornare** o premere F5 per aggiornare la configurazione del server.

3. Creare una regola:

3.1. Andare in **Site Navigation (Navigazione del sito) > Rules and Events (Regole ed eventi) > Rules (Regole)**.

3.2. Fare clic con il pulsante destro del mouse su **Rules (Regole)**, selezionare **Add Rule (Aggiungi regola)**, quindi inserire un nome.

3.3. In **Edit the rule description (Modifica descrizione regola)**, fare clic su **event (evento)**.

3.4. Andare in **Devices (Dispositivi) > Predefined Events (Eventi predefiniti)** e selezionare **Motion Started (Movimento avviato)**.

3.5. In **Edit the rule description (Modifica la descrizione della regola)**, fare clic su **devices/recording_server/management_server**.

3.6. Selezionare la videocamera che deve attivare le sirene stroboscopiche.

3.7. Fare clic su **Next (Avanti** finché non si arriva a **Step 3: Actions (Passaggio 3: Azioni)**.

3.8. Selezionare l'azione **Axis: avviare o arrestare un profilo su una sirena stroboscopica: <preset>**.

3.9. In **Edit the rule description (Modifica la descrizione della regola)**, fare clic su **preset**.

3.10. Seleziona il preset di avvio creato in precedenza.

3.11. Fare clic su **Next (Avanti)** e selezionare **Perform stop action on <event>(Esegui azione di arresto sull'evento)**.

3.12. Fare clic su **Next (Avanti)** e selezionare **Axis: Start or stop a profile on strobe siren: <evento> (Axis: Avviare o arrestare un profilo sulla sirena stroboscopica: evento)**.

3.13. In **Edit the rule description (Modifica la descrizione della regola)**, fare clic su **preset**.

3.14. Seleziona il preset di arresto creato in precedenza.

3.15. Selezionare **Finish (Fine)**.

4. Verifica che le sirene stroboscopiche funzionino correttamente quando la telecamera rileva movimento.

Riproduci clip audio su altoparlanti o in una zona altoparlante quando una telecamera rileva movimento



Con il plugin del server di eventi, hai la possibilità di impostare regole personalizzate per l'automatizzazione delle azioni, cosiddette preset di azione. In questo esempio, ti mostriamo come riprodurre una clip audio automaticamente su un altoparlante o in una zona altoparlante quando una telecamera rileva movimento.

Nota

Requisiti

- AXIS Optimizer versione 4.6 o versione successiva sul server di eventi e in Management Client.
- Uno o molteplici altoparlanti Axis dedicati o dispositivi Axis con altoparlanti integrati.
- Per riprodurre un clip audio in una zona altoparlante, è necessario un sistema AXIS Audio Manager Edge o AXIS Audio Manager Pro con una configurazione corretta. Per ulteriori informazioni su come configurare questi sistemi, consultare la sezione *Modalità di configurazione, on page 31*.

1. Per caricare una clip audio:
   1.1. Con modalità AXIS Audio Manager Edge o Legacy, posizionare la clip audio che si desidera caricare sugli altoparlanti nella cartella predefinita **C:\Users\Public\Documents\AXIS Optimizer for Milestone XProtect – Audio Clips**.
   Con la modalità AXIS Audio Manager Pro, è possibile caricare clip audio nell'interfaccia web di AXIS Audio Manager Pro.
   1.2. In Management Client (Gestione cliente), andare a **Site Navigation** > **AXIS Optimizer** > **Speaker manager** (Navigazione sito, AXIS Optimizer, Gestore altoparlante) e selezionare una destinazione o la zona.

   Nota

   Per ulteriori informazioni su come selezionare una modalità di gestione degli altoparlanti, consultare la sezione *Modalità di configurazione, on page 31*.

   1.3. Andare a **Audio clips (Clip audio)** e fare clic su **+** accanto alla clip audio che si desidera caricare.
   1.4. In modalità Legacy, ripetere i passaggi 1.2 - 1.3 per ciascun altoparlante su cui si desidera riprodurre la clip audio. Controllare di caricare lo stesso file audio su ogni altoparlante.
2. Per creare preset azione per la riproduzione di una clip audio su un altoparlante o in una zona altoparlante:
   2.1. Andare a **Site Navigation** > **Rules and Events** > **Axis actions** (Navigazione sito, Regole ed eventi, azioni Axis).
   2.2. Per creare un preset di avvio, andare a **Audio clips (Clip audio)** e fare clic su **Add new preset (Aggiungi nuovo preset)**.
   2.3. Con AXIS Audio Manager Edge o AXIS Audio Manager Pro, andare a **Select playback destination (Seleziona destinazione di riproduzione)**.
   In modalità Legacy, andare a **Select speaker (Seleziona altoparlante)**.
   2.4. Seleziona un altoparlante o una zona altoparlante.
   2.5. Dall'elenco, selezionare il file audio che è stato caricato al punto 1. L'azione preimpostata viene salvata automaticamente
   2.6. Con la modalità AXIS Audio Manager Pro, andare a **Select visual profile (Seleziona profilo visivo)** ed effettua la configurazione del profilo visivo e del testo.

   Nota

   Selezionare **Default (Predefinito)** nell'elenco dei profili visivi per utilizzare il comportamento predefinito del profilo visivo sul server AXIS Audio Manager Pro quando viene attivata l'azione relativa alla clip audio.

   2.7. Fare clic su **refresh (aggiorna)** o premere F5 per aggiornare la configurazione del server.
3. Per creare una regola:
   3.1. Andare a **Site Navigation** > **Rules and Events** > **Rules** (Navigazione sito, Regole ed eventi, Regole).
   3.2. Fare clic con il pulsante destro del mouse su **Rules (Regole)**, selezionare **Add Rule (Aggiungi regola)**, quindi inserire un nome.
   3.3. In **Edit the rule description (Modifica descrizione regola)**, fare clic su **event (evento)**.

3.4. Andare a **Devices (Dispositivi)** > **Predefined Events (Eventi predefiniti)** e selezionare **Motion Started (Movimento avviato)**.

3.5. In **Edit the rule description (Modifica la descrizione della regola)**, fare clic su **devices/recording_server/management_server**.

3.6. Seleziona la telecamera che deve attivare l'azione preset o la clip audio.

3.7. Fare clic su **Next (Avanti** finché non si arriva a **Step 3: Actions (Passaggio 3: Azioni)**.

3.8. Selezionare l'azione **Axis: Play audio clip: <preset> (Axis: riproduci clip audio: preset)**.

3.9. In **Edit the rule description (Modifica la descrizione della regola)**, fare clic su **preset**.

3.10. Seleziona il preset creato al passaggio precedente.

3.11. Selezionare **Finish (Fine)**.

4. Verifica che la clip audio sia riprodotta in modo esatto quando la telecamera rileva movimento.

Risoluzione dei problemi di una regola

Se una regola non funziona, controllare per prima cosa i messaggi del server di eventi per assicurarsi che il servizio eventi sia in esecuzione.

È possibile controllare inoltre i registri di AXIS Optimizer sul server di eventi. Se sono disponibili Management Client o Smart Client, usarli per abilitare e salvare i registri.

Gestione centralizzata degli elenchi delle targhe

Quando usi AXIS Optimizer List Manager è possibile gestire in modo centralizzato gli elenchi delle targhe per tutte le telecamere contemporaneamente. È possibile creare e gestire liste consentiti, bloccati e personalizzate direttamente da VMS. Il sistema supporta elenchi combinati. Ciò significa che è possibile avere un elenco complessivo che si applica a tutte le telecamere nel sistema e agli elenchi locali che si applicano a telecamere specifiche.

La gestione centralizzata dell'elenco è utile ad esempio quando si desidera automatizzare l'ingresso e l'uscita dai parcheggi o si desidera ricevere un allarme quando il sistema registra una determinata targa.

Per creare e modificare gli elenchi è necessario disporre dei privilegi di amministratore. È possibile concedere diritti di lettura e modifica ad altri ruoli, vedere la sezione *Configurazione delle autorizzazioni per gli elenchi, on page 24*.

Creazione di un elenco

Nota

Requisiti

- AXIS License Plate Verifier 1.8 o versione successiva in esecuzione sulle telecamere
- Se si desidera creare elenchi personalizzati, occorre AXIS License Plate Verifier 2.0

1. Su Management Client, vai su **Site Navigation > AXIS Optimizer > License plate lists (Navigazione sito > AXIS Optimizer > Liste targhe)**.
2. Seleziona le telecamere a cui vuoi inviare l'elenco consentiti, bloccati e personalizzato.
3. (Facoltativo) Aggiungere ruoli utente che possono visualizzare e modificare la lista consentiti, la lista bloccati e la lista personalizzata.
4. Aggiungi targhe all'elenco consentiti, bloccati e personalizzato.
   È inoltre possibile importare gli elenchi di targhe esistenti.
   Quando l'elenco è in stato **Synchronized (Sincronizzato)**, è stato inviato alle telecamere selezionate.

Configurazione delle autorizzazioni per gli elenchi

È possibile configurare i ruoli utente che possono modificare la lista consentiti, la lista bloccati e la lista personalizzata. Questa opzione è utile, ad esempio, quando l'amministratore ha configurato gli elenchi, ma si desidera che l'operatore aggiunga i visitatori in base alle esigenze giornaliere.

In Management Client

Tutte le autorizzazioni per la visualizzazione e la modifica degli elenchi per ogni elenco.

1. Andare a **Security > Roles (Sicurezza > Ruoli)** e selezionare un ruolo.
2. Vai alla scheda **AXIS Optimizer**.
3. Vai a **Role settings (Impostazioni ruolo)** > **AXIS Optimizer** > **License plate lists (Elenchi targhe)**
4. Selezionare **Read (Leggi)** nel campo **License plate lists (node) (Elenchi targhe (nodo))**.
5. Selezionare un elenco in **License plate lists (Elenchi targhe)** e selezionare **Edit license plates (Modifica targhe)**.
   - Per versioni precedenti rispetto a XProtect 2023 R2, vai a **MIP > AXIS Optimizer > AXIS Optimizer Security > License plate lists (MIP > AXIS Optimizer > AXIS Optimizer Security > Liste targhe)** e selezionare **Edit license plate lists (Modifica liste targhe)**.

Modifica di un elenco

In Management Client

1. Vai a **Site Navigation > AXIS Optimizer > License plate lists (Navigazione sito > AXIS Optimizer > Liste targhe)**.
2. Selezionare il sito che si desidera modificare.
3. Aggiornare **Cameras (Telecamere)** o **License plates (Targhe)** in base alle esigenze.
   Quando l'elenco passa allo stato **Synchronized (Sincronizzato)**, le modifiche verranno inoltrate alle telecamere selezionate.

In Smart Client

1. Vai alle *Targhe Axis, on page 58* e fai clic su **License plate lists (Elenchi targhe)**.
   Se la scheda non è visualizzata, vai su **Settings > Axis search options (Impostazioni > Opzioni di ricerca Axis)** e selezionare **Show license plate search tab (Mostra scheda ricerca targa)**.
2. Selezionare il sito che si desidera modificare.
3. Aggiungi targhe all'elenco consentiti, bloccati e personalizzato.
   È inoltre possibile importare gli elenchi delle targhe esistenti.
   Quando l'elenco è in stato **Synchronized (Sincronizzato)**, è stato inviato alle telecamere selezionate.

Importazione di un elenco

È possibile importare gli elenchi in diversi formati testo o CSV.

- Formato testo consentito: una targa per ciascuna riga
- Formati CSV consentiti:
  - una targa per ciascuna riga
  - Due campi: targa e data
  - Tre campi: targa, proprietario e commenti
  - Quattro campi: targa, proprietario, commenti e stringa "Attivo" o "Inattivo". Stesso formato applicato quando si esporta un elenco

In Management Client

1. Vai a **Site Navigation > AXIS Optimizer > License plate lists (Navigazione sito > AXIS Optimizer > Liste targhe)**.
2. Selezionare il sito che si desidera modificare.
3. Vai su **Allowed (Consentito)**, **Blocked (Bloccato)** o **Custom (Personalizzato)**.
4. Fare clic su ⋮ e selezionare **Import to allow list (Importa nell'elenco consentiti)**, **Import to block list (Importa nell'elenco bloccati)** o **Import to custom list (Importa nell'elenco personalizzato)**.
5. Nella finestra di dialogo **Reset list (Ripristina elenco)**:
   - Fare clic su **Yes (Sì)** per la rimozione di tutte le targhe esistenti ed eseguire l'aggiunta alla lista delle sole targhe appena importate.
   - Fare clic su **No** per eseguire la fusione delle targhe appena importate con quelle esistenti nella lista.

In Smart Client

1. Vai alle *Targhe Axis, on page 58* e fai clic su **License plate lists (Elenchi targhe)**.
   Se la scheda non è visualizzata, vai su **Settings > Axis search options (Impostazioni > Opzioni di ricerca Axis)** e selezionare **Show license plate search tab (Mostra scheda ricerca targa)**.
2. Selezionare il sito che si desidera modificare.
3. Vai su **Allowed (Consentito)**, **Blocked (Bloccato)** o **Custom (Personalizzato)**.
4. Fare clic su ⋮ e selezionare **Import to allow list (Importa nell'elenco consentiti)**, **Import to block list (Importa nell'elenco bloccati)** o **Import to custom list (Importa nell'elenco personalizzato)**.
5. Nella finestra di dialogo **Reset list (Ripristina elenco)**:
   - Fare clic su **Yes (Sì)** per la rimozione di tutte le targhe esistenti ed eseguire l'aggiunta alla lista delle sole targhe appena importate.
   - Fare clic su **No** per eseguire la fusione delle targhe appena importate con quelle esistenti nella lista.

Esportazione di un elenco

Nota

Per esportare gli elenchi delle targhe, è necessario disporre dei diritti di amministratore.

In Management Client

1. Vai a **Site Navigation > AXIS Optimizer > License plate lists (Navigazione sito > AXIS Optimizer > Liste targhe)**.
2. Selezionare il sito che si desidera modificare.
3. Vai su **Allowed (Consentito)**, **Blocked (Bloccato)** o **Custom (Personalizzato)**.
4. Fare clic su ⋮ e selezionare **Export allow list (Esporta elenco consentiti)**, **Export block list (Esporta elenco bloccati)** o **Export custom list (Esporta elenco personalizzato)**.
   L'elenco esportato sarà in formato CSV con quattro campi: targa, proprietario, commenti e stato Attivo o Inattivo.

In Smart Client

1. Vai alle *Targhe Axis, on page 58* e fai clic su **License plate lists (Elenchi targhe)**.
   Se la scheda non è visualizzata, vai su **Settings > Axis search options (Impostazioni > Opzioni di ricerca Axis)** e selezionare **Show license plate search tab (Mostra scheda ricerca targa)**.
2. Selezionare il sito che si desidera modificare.
3. Vai su **Allowed (Consentito)**, **Blocked (Bloccato)** o **Custom (Personalizzato)**.

4. Fare clic su ⋮ e selezionare **Export allow list (Esporta elenco consentiti)**, **Export block list (Esporta elenco bloccati)** o **Export custom list (Esporta elenco personalizzato)**.
L'elenco esportato sarà in formato CSV con quattro campi: targa, proprietario, commenti e stato Attivo o Inattivo.

Ulteriori informazioni sugli elenchi

- È possibile creare diversi siti.
- Ciascun sito è associato a una o più telecamere su cui è installato AXIS License Plate Verifier.
- Ciascun sito è associato a uno o più ruoli utente VMS. Il ruolo utente definisce chi dispone dell'autorizzazione di lettura e modifica degli elenchi delle targhe.
- Tutte le liste sono archiviate nel database VMS.
- Quando si aggiunge la telecamera a un sito, le targhe già esistenti sulla telecamera vengono sovrascritte.
- Se la stessa telecamera è presente in diversi siti, la telecamera riceverà la somma di tutti gli elenchi.
- Se la stessa targa è in molteplici liste, "bloccati" ha la priorità più elevata, "consentiti" ha priorità media e "personalizzato" ha la priorità più bassa.
- Per ciascuna targa, è possibile aggiungere informazioni sul proprietario del veicolo. Tuttavia, queste informazioni non vengono sincronizzate con le telecamere.

Rispondi agli eventi in diretta

Uso dei comandi del dispositivo

Comandi operatore

I controlli operatore consentono l'accesso alle funzionalità specifiche di una telecamera Axis direttamente da Smart Client. Le funzionalità alle quali è possibile avere accesso dipendono dalle telecamere nel sistema e dalle funzionalità di cui sono dotate. Oltre ai controlli operatore preinstallati, è possibile crearne di personalizzati. È inoltre possibile configurare i controlli ai quali un operatore ha accesso.

Alcuni esempi di controlli operatore:

- Attivare o disattivare il tergicristallo
- Attivare o disattivare il riscaldatore
- Attivare o disattivare l'IR
- Focus Recall
- Attivare o disattivare WDR
- Attivare o disattivare lo stabilizzatore elettronico dell'immagine (EIS)
- Attivare o disattivare privacy mask.

Per informazioni sui controlli dell'operatore specifici della telecamera, vedere la scheda tecnica.

Accesso ai controlli operatore

Nota

Requisiti

- Dispositivi Axis con AXIS OS 7.10, 7.40 o versione successiva. Le versioni 7.20 e 7.30 non supportano i controlli operatore.

1. In Smart Client, fare clic su **Live (Diretta)** e andare alla telecamera Axis.
2. Fare clic su e selezionare la funzione da usare.

Salvataggio di un'area di messa a fuoco per una telecamera PTZ

Il richiamo della messa a fuoco consente il salvataggio di aree di messa a fuoco alle quali la telecamera PTZ torna in automatico quando si sposta su tale area della scena. Risulta utile specialmente in condizioni di bassa luminosità in cui la telecamera avrebbe altrimenti difficoltà a trovare la messa a fuoco.



1. In Smart Client, spostare la telecamera sull'area sulla quale si desidera effettuare la messa a fuoco.

Nota

Le condizioni di luminosità devono essere ottimali quando si imposta l'area di messa a fuoco.

2. Mettere a fuoco la telecamera.
3. Selezionare **Add Focus Recall Zone (Aggiungi zona di richiamo messa a fuoco)**.

In seguito, quando si ruota o si inclina la telecamera e si sposta la vista su un'area, la telecamera richiama in automatico la messa a fuoco preimpostata per quella vista. Anche se si esegue lo zoom avanti o indietro, la telecamera preserverà la stessa posizione di messa a fuoco.

Se la zona è configurata in modo inesatto, selezionare **Remove Focus Recall Zone (Rimuovi zona di richiamo messa a fuoco)**.

Esecuzione della messa a fuoco automatica di una telecamera



Le telecamere con messa a fuoco automatica possono regolare l'obiettivo meccanicamente e automaticamente in modo che l'immagine rimanga a fuoco nell'area di interesse quando la vista cambia.

Messa a fuoco automatica su telecamere PTZ

1. In Smart Client, selezionare una vista della telecamera.
2. Fare clic su e andare in **Set Focus (Imposta messa a fuoco) > AF (Messa a fuoco automatica)**. **Focus Control (Controllo messa a fuoco)** consente di spostare il punto di messa a fuoco più vicino o più lontano:
   - Per un passo più ampio, fare clic sulla barra grande.
   - Per un passo più piccolo, fare clic sulla barra piccola.

Messa a fuoco automatica su telecamere fisse di tipo box e dome

1. In Smart Client, selezionare una vista della telecamera.
2. Fare clic su e andare in **Autofocus (Messa a fuoco automatica)**.

Attivazione di speed dry o del tergicristallo



La funzione speed dry consente alla cupola di scuotere via i liquidi quando si bagna. Quando la cupola vibra ad alta velocità, la tensione superficiale dell'acqua si spezza e le gocce vengono rimosse. Questo consente alla telecamera di produrre immagini nitide anche in caso di pioggia.

Per attivare la funzione speed dry

1. In Smart Client, selezionare una vista della telecamera.
2. Fare clic su e andare in **PTZ > Speed Dry**.

Importante

La funzione speed dry è disponibile solo nelle telecamere della serie AXIS Q61.

Per attivare la funzione tergicristallo

Il tergicristallo rimuove l'acqua e la pioggia in eccesso dall'obiettivo delle telecamere di posizionamento Axis.

1. In Smart Client, selezionare una vista della telecamera.
2. Fare clic su .

Importante

La funzione del tergicristallo è disponibile solo nelle telecamere della serie AXIS Q86.

Misura temperatura spot



Se hai nel tuo sistema una telecamera nella quale è integrata la lettura temperatura spot, è possibile misurare la temperatura direttamente nella vista della telecamera. Le telecamere AXIS con lettura temperatura spot sono AXIS Q1961-TE, AXIS Q2101-E e AXIS Q2901-E.

1. In Smart Client, apri una vista della telecamera in una telecamera integrata con la lettura temperatura spot.
2. Per misurare la temperatura spot, fare clic su e selezionare:
   - **Measure spot temperature (Misura la temperatura spot)** per AXIS Q2901-E.
   - **Enable temperature spot meter (Abilita il misuratore spot della temperatura)** per AXIS Q1961-TE e AXIS Q2101-E.
3. Fare clic su qualsiasi area nella vista e verrà visualizzata la temperatura spot corrente.
   Per Q1961-TE e AXIS Q2101-E, fare clic su **Done (Fatto)**.
4. Per AXIS Q1961-TE e AXIS Q2101-E, la temperatura spot resterà sull'immagine fino alla disabilitazione:
   - Selezionare > **Disable temperature spot meter (Disabilita misurazione temperatura spot)**.

Nota

Se si utilizza lo zoom digitale, le misurazioni della temperatura possono dare risultati non corretti.

Zoom in avanti e tracciamento automatico di un oggetto in movimento

Autotracking

Con il rilevamento automatico, la telecamera esegue automaticamente lo zoom in avanti e rintraccia gli oggetti in movimento, ad esempio un veicolo o una persona. È possibile selezionare manualmente un oggetto di cui tenere traccia o impostare le aree di attivazione e lasciare che la telecamera rilevi gli oggetti in movimento. Quando la telecamera non rileva un oggetto, ritorna alla posizione iniziale dopo 5 secondi.

- Configurare le aree di attivazione nell'interfaccia Web della telecamera PTZ.
- In Smart Client sarà possibile visualizzare:
  - Quadrato rosso: l'oggetto tracciato.
  - Aree blu: oggetti che non vengono tracciati, ma che possono esserlo se entrano in una zona di attivazione o se selezionati con il tasto destro del mouse.

Configurazione del tracking automatico

Nota

Requisiti

- AXIS OS 12.0
- Una o molteplici telecamere Axis con supporto per Tracking automatico 2, ad esempio, AXIS Q6075 PTZ Dome Network Camera

1. Assicurarsi che la telecamera e i dispositivi di metadati siano abilitati.
2. Selezionare Metadati 1 per la telecamera e fare clic su **Settings (Impostazioni)**.

3. Vai a **Metadata stream > Event data (Flusso metadati > Dati evento)** e seleziona **Yes (Sì)**.
4. Fare clic su **Save (Salva)**.
5. Configurare il tracking automatico nell'interfaccia Web della telecamera PTZ.

Attivazione o disattivazione del tracking automatico

1. In Smart Client, fare clic su .
2. Selezionare **Turn on autotracking (Attiva tracking automatico)** o **Turn off autotracking (Disattiva tracking automatico)**.

Nota

Se sono disponibili diverse opzioni per attivare/disattivare il tracciamento automatico, utilizzare l'ultima opzione nell'elenco.

Avvio manuale dell'autotracking

Al passaggio del mouse su un oggetto, verrà attivata la sovrapposizione testo. Facendo clic con il pulsante destro del mouse, un oggetto viene impostato come destinatario e la telecamera inizia a seguire l'oggetto da rilevare. La telecamera si ripristina dopo 5 secondi se l'oggetto non potrà più essere rilevato.

Facendo clic con il tasto destro fuori dai riquadri blu interrompe il tracciamento automatico.

Creazione di comandi operatore personalizzati

1. In Management Client, andare a **Site Navigation > AXIS Optimizer > Operator controls (Navigazione sito > AXIS Optimizer > Comandi operatore)**.
2. Selezionare un dispositivo o un gruppo di dispositivi.
3. Fare clic su **Add new control (Aggiungi nuovo comando)**.
4. immettere un **Nome** e una **Descrizione**.
5. Selezionare **Administrator (Amministratore)** se si desidera che il controllo dell'operatore sia disponibile solo per gli utenti con diritti di amministratore.
6. Aggiungere l'URL VAPIX per il controllo specifico.
   Esempio: Per aggiungere un comando operatore Defog on (Modalità sbrinamento attivata), immettere questo URL: `/axis-cgi/param.cgi?action=update&imageSource.IO.Sensor.Defog=on`.
   Per ulteriori informazioni sulle API dei dispositivi di rete Axis, vedere la .
7. Accedere a Smart Client e verificare che il comando operatore funzioni come previsto.

Configurazione degli accessi ai comandi dell'operatore

È possibile configurare a quali comandi ha accesso un operatore di Smart Client.

1. In Management Client, andare a **Site Navigation > AXIS Optimizer > Operator controls (Navigazione sito > AXIS Optimizer > Comandi operatore)**.
2. Selezionare un dispositivo o un gruppo di dispositivi.
3. Selezionare i controlli operatore a cui si desidera che gli operatori abbiano accesso in Smart Client.

Interazione attraverso gli altoparlanti

Gestore altoparlante

Gestore altoparlanti integra i dispositivi audio Axis nel VMS per darti massima funzionalità dei dispositivi Axis.

- Eseguire l'accesso agli altoparlanti correlati alla telecamera

Connettere le telecamere a un altoparlante o a un gruppo di altoparlanti ed eseguire l'accesso agli altoparlanti dalla visualizzazione in diretta. Non sarà più necessario cercare gli altoparlanti manualmente.

- Inviare audio a un gruppo di altoparlanti
  Inviare audio a più altoparlanti con un solo clic.
- Gestire le clip audio
  È possibile gestire facilmente i file audio.
- Intervenire immediatamente grazie agli altoparlanti
  Reagire in fretta ad un allarme senza uscire dalla Gestione allarmi.
- Sincronizzare l'audio tra gli altoparlanti
  Se si desidera usare il sistema audio per la musica di sottofondo, Gestore altoparlanti consente di impostare le zone per la sincronizzazione dell'audio tra gli altoparlanti (soltanto nelle modalità AXIS Audio Manager Pro ed Edge).

Modalità

Il Gestore altoparlante supporta tre diverse modalità per diversi tipi di impostazioni altoparlante.

- **Pro** per sistemi AXIS Audio Manager Pro
  Una soluzione software completa progettata per sistemi di avviso al pubblico su larga scala o di livello avanzato. Supporta oltre 5.000+ altoparlanti e oltre 500+ zone e offre opzioni flessibili per le licenze e l'installazione. È consigliato per sistemi di grandi dimensioni o per utenti con esigenze di pianificazione più complesse.
- **Edge** per sistemi AXIS Audio Manager Edge
  Una soluzione software snella per la gestione di un massimo di 200 altoparlanti distribuiti su 20 zone. È integrata direttamente negli altoparlanti di rete Axis e non richiede server né licenze aggiuntive. È consigliato per sistemi di piccole dimensioni che non presentano esigenze di pianificazione avanzate.
- **Versione precedente**
  La modalità legacy utilizza l'integrazione di altoparlanti nativi per trasmettere l'audio a un gruppo di altoparlanti o per attivare le clip audio. Non supporta la trasmissione sincronizzata. È consigliato per sistemi con altoparlanti singoli, che non richiedono una trasmissione sincronizzata.

Modalità di configurazione

La prima volta che si effettua l'accesso a questa pagina verrà chiesto di selezionare una modalità, ma è possibile modificare tale modalità in qualsiasi momento. La configurazione che si effettua in ciascuna modalità è separata, ma viene mantenuta quando si passa da una modalità all'altra.

1. Andare a **Site Navigation**> **AXIS Optimizer** > **Speaker manager** (Navigazione sito, AXIS Optimizer, Gestore altoparlante).
2. In **Mode** (Modalità), fare clic sulla modalità in cui ci si trova attualmente e selezionare quella desiderata nella finestra a comparsa.
3. Fare clic su **Switch mode** (Cambia modalità).

Modalità AXIS Audio Manager Pro

Per utilizzare questa modalità:

- Installare il software AXIS Audio Manager Pro su un computer server, ad esempio un server di registrazione.
- Attivare la licenza e effettuare la configurazione di AXIS Audio Manager Pro con accesso all'API.
- Facoltativo: impostare un certificato server per l'interfaccia Web vedere *Certificates (Certificati)*.
- Modificare il server AXIS Audio Manager Pro dalla porta 443 se è installato su un computer server VMS.

Questa modalità non richiede l'aggiunta o la registrazione della licenza di altoparlanti nel VMS, ma verrà automaticamente creato un dispositivo hardware per la connessione al server AXIS Audio Manager Pro (è necessaria una licenza per dispositivo VMS). Per maggiori informazioni su AXIS Audio Manager Pro, consultare il *manuale per l'utente di AXIS Audio Manager Pro*.

Nota

La modalità AXIS Audio Manager Pro è limitata al supporto di un unico sito locale. Le architetture multi-sito, federate e interconnesse esulano dall'ambito di questa integrazione.

Connettersi a un server AXIS Audio Manager Pro in modalità Pro

1. In Management Client, andare a **Site Navigation** > **AXIS Optimizer**> **Speaker manager** (Navigazione sito, AXIS Optimizer, Gestore altoparlante)
2. Fare clic su **Connetti**.
3. Nella finestra di dialogo:
   - Selezionare un server di registrazione a cui si desidera aggiungere l'hardware AXIS Audio Manager Pro .
   - Inserire l'indirizzo e la porta HTTPS del server AXIS Audio Manager Pro.
   - Inserire il nome utente e la password API (l'accesso all'API deve essere abilitato sul server AXIS Audio Manager Pro).
   - Fare clic su **Connetti**.

Sul lato sinistro è possibile visualizzare tutte le destinazioni e le zone disponibili in AXIS Audio Manager Pro. Facendo clic sul server di **AXIS Audio Manager Pro**, sul lato destro viene visualizzata l'interfaccia Web di AXIS Audio Manager Pro.

Nota

Per accedere all'interfaccia Web, è necessaria una connessione diretta tra il computer del Management Client e il server AXIS Audio Manager Pro.

Se si apportano modifiche alle zone, alle destinazioni, ai clip audio o ai profili visivi nell'interfaccia web di AXIS Audio Manager Pro:

- Andare a **Site Navigation** > **AXIS Optimizer** > **Speaker manager** (Navigazione sito, AXIS Optimizer, Gestore altoparlante).
- Fare clic su **Update** (Aggiorna)

Associazione di una telecamera a una destinazione o a una zona

È possibile associare una telecamera a una destinazione o a una zona specifica e utilizzarla direttamente nella vista telecamera di Smart Client.

1. In Management Client, andare a **Site Navigation** > **AXIS Optimizer** > **Speaker manager** (Navigazione sito, Gestore altoparlante, AXIS Optimizer) e selezionare una destinazione o la zona.
2. In **Associated camera(s)** (Telecamera(e) associata(e), fare clic su **Add cameras...** (Aggiungi telecamere) e selezionare la telecamera che si desidera associare alla destinazione o alla zona.

Quando una telecamera è associata a una destinazione o a una zona, la barra strumenti nella vista della telecamera su Smart Client mostra .

Creare profili visivi

- In Gestione Client, andare a **Site Navigation** > **AXIS Optimizer**> **Speaker manager** (Navigazione sito, AXIS Optimizer, Gestore altoparlante).
- Fare clic su **Audio Manager Pro server** per visualizzare l'interfaccia web.
- Fare clic su **Visual profiles (Profili visivi)** per creare o modificare i profili visivi.

Per ulteriori informazioni sui profili visivi, consultare *il manuale per l'utente di AXIS Audio Manager Pro*.

Modalità AXIS Audio Manager Edge

AXIS Audio Manager Edge è preinstallato sulla maggior parte degli altoparlanti Axis e verrà rilevato automaticamente quando si seleziona questa modalità. I siti leader, i dispositivi intermediari per la sorgente di paging e gli altoparlanti autonomi devono essere aggiunti al VMS perché la modalità AXIS Audio Manager Edge funzioni correttamente.

Nota

In modalità AXIS Audio Manager Edge, non si possono usare output audio integrati della telecamera e altri dispositivi audio incompatibili.

Per maggiori informazioni su AXIS Audio Manager Edge, consultare il *manuale per l'utente di AXIS Audio Manager Edge*.

Configura gli altoparlanti e le zone nella modalità AXIS Audio Manager Edge

Per la riproduzione di clip audio e per parlare in tempo reale, devi prima attivare il paging per le tue zone.

1. In Management Client, andare a **Site Navigation** > **Devices** > **Speakers** (Navigazione sito, Dispositivi, Altoparlanti) per aggiungere gruppi di dispositivi o aggiungere e rimuovere altoparlanti dai gruppi di dispositivi.
2. Andare a **Site Navigation** > **AXIS Optimizer** > **Speaker manager** (Navigazione sito, AXIS Optimizer, Gestore altoparlante) e, controllare che la modalità **Edge**sia selezionata.
   Gestione altoparlanti cercherà successivamente tutti gli altoparlanti nel sistema VMS e mostrerà tutti i siti AXIS Audio Manager Edge e le zone che si possono usare in Smart Client.
3. Nell'elenco dei siti, seleziona un'area con paging disattivato.
4. Seleziona **Turn on paging for the zone (Attiva paging per la zona)**.

Se si apportano modifiche alle zone o alle sorgenti di paging:

5. Andare a **Site Navigation** > **AXIS Optimizer** > **Speaker manager** (Navigazione sito, AXIS Optimizer, Gestore altoparlante).
6. Fare clic su **Update** (Aggiorna)

Nota

Se l'impostazione non riesce, controlla la configurazione AXIS Audio Manager Edge e riprova.



Associazione di una telecamera a un altoparlante o a una zona

Per usare un altoparlante specifico o una zona direttamente nella vista della telecamera di Smart Client, è possibile eseguirne l'associazione a una telecamera.

1. In Management Client, andare a **Site Navigation** > **AXIS Optimizer** > **Speaker manager** (Navigazione sito, Gestore altoparlante, AXIS Optimizer) e selezionare un altoparlante o la zona.
2. Nella finestra **Associated cameras (Telecamere associate)**, fare clic su **+ Add cameras (Aggiungi telecamere)** e selezionare le telecamere a cui si desidera associare l'altoparlante o la zona.

Quando una telecamera è associata a un altoparlante, a un gruppo di dispositivi o a una zona, la barra strumenti nella vista della telecamera su Smart Client mostra .

Caricamento di clip audio sugli altoparlanti

Per la riproduzione di clip audio in un altoparlante o zona da Smart Client, è necessario prima caricare le clip audio sugli altoparlanti in Management Client.

1. Posizionare le clip audio che si desidera caricare sugli altoparlanti nella cartella predefinita **C:\Users\Public\Documents\AXIS Optimizer for Milestone XProtect – Audio Clips**.
2. In Management Client, andare a **Site Navigation** > **AXIS Optimizer** > **Speaker manager** (Navigazione sito, Gestore altoparlante, AXIS Optimizer) e selezionare un altoparlante o la zona.
3. Vai a **Audio clips (Clip audio)** e fai clic su **+** davanti alle clip che desideri caricare negli altoparlanti.

Modalità legacy

La modalità Legacy amplia le funzionalità native degli altoparlanti Axis e degli altri dispositivi Axis dotati di funzionalità audio che sono stati aggiunti al VMS. A differenza delle altre modalità, la modalità Legacy non supporta la trasmissione sincronizzata su più altoparlanti.

Configurare gli altoparlanti in modalità legacy

1. In Management Client, andare a **Site Navigation** > **Devices** > **Speakers** (Navigazione sito, Dispositivi, Altoparlanti) per aggiungere gruppi di dispositivi o aggiungere e rimuovere altoparlanti dai gruppi di dispositivi.
2. Andare a **Site Navigation** > **AXIS Optimizer** > **Speaker manager** (Navigazione sito, AXIS Optimizer, Gestore altoparlante) e controllare che la modalità legacy sia selezionata.
3. Fare clic su
   3.1. Nella finestra **Manage Side Panel (Gestisci pannello laterale)**, selezionare gli altoparlanti che si desidera mostrare in Smart Client.
   3.2. Fare clic su **Add (Aggiungi)** quindi su **OK**.
   Gli altoparlanti nel pannello **Visible (Visibile)** sono ora visibili in Smart Client per tutti gli utenti che hanno accesso all'altoparlante.
4. Per rimuovere gli altoparlanti:
   4.1. Andare **Site Navigation** > **AXIS Optimizer** > **Speaker manager** (Navigazione sito, AXIS Optimizer, Gestore altoparlante) e fare clic su .
   4.2. Nella finestra **Manage Side Panel (Gestisci pannello laterale)**, selezionare gli altoparlanti che si desidera rimuovere.
   4.3. Fare clic su **Remove (Rimuovi)** quindi su **OK**.

Associare una telecamera a un altoparlante o a una gruppo di altoparlanti

È possibile associare una telecamera a una destinazione o a una zona specifica e utilizzarla direttamente nella vista telecamera di Smart Client.

1. In Management Client, andare a **Site Navigation** > **AXIS Optimizer** > **Speaker manager** (Navigazione sito, AXIS Optimizer, Gestore altoparlante) e selezionare un altoparlante o il gruppo di altoparlanti.
2. In **Associated camera(s)** (Telecamera(e) associata(e), fare clic su **Add cameras...** (Aggiungi telecamere) e selezionare la telecamera che si desidera associare all'altoparlante o al gruppo di altoparlanti.

Quando una telecamera è associata a un altoparlante, a un gruppo di altoparlanti, la barra strumenti nella vista della telecamera su Smart Client mostra .

Caricamento di clip audio sugli altoparlanti

Per la riproduzione di clip audio in un altoparlante o zona da Smart Client, è necessario prima caricare le clip audio sugli altoparlanti in Management Client.

1. Posizionare le clip audio che si desidera caricare sugli altoparlanti nella cartella predefinita **C:\Users\Public\Documents\AXIS Optimizer for Milestone XProtect - Audio Clips**.
2. In Management Client, andare a **Site Navigation** > **AXIS Optimizer** > **Speaker manager** (Navigazione sito, AXIS Optimizer, Gestore altoparlante) e selezionare un altoparlante o il gruppo di altoparlanti.
3. Vai a **Audio clips (Clip audio)** e fai clic su **+** davanti alle clip che desideri caricare negli altoparlanti.



Regolazione del volume

Per modificare il volume dei tuoi altoparlanti:

1. In Management Client, andare a **Site Navigation > Speaker manager** (Navigazione sito, Gestore altoparlante) e selezionare un altoparlante o il gruppo di altoparlanti.
2. Vai a **Volume** e imposta il volume desiderato.



Riproduci audio sugli altoparlanti

1. In Smart Client, andare a **Live** > **MIP plug-ins** > **Axis speaker control** (In tempo reale, Plug-in MIP, Controllo altoparlante Axis) e selezionare un altoparlante o una zona nell'elenco a discesa.
2. Fai sì che il microfono invii l'audio all'altoparlante:
   2.1. Tenere premuto mentre si parla.
   Assicurati che il misuratore del livello del microfono mostri attività vocale.
3. Riproduci una clip audio sull'altoparlante:
   3.1. Vai a **Media clip (Clip multimediale)** e seleziona una clip audio nell'elenco a discesa.
   3.2. Per iniziare a riprodurre la clip audio sull'altoparlante selezionato, fare clic su Riproduci.

Riproduci audio su altoparlanti nella vista della telecamera

1. In Smart Client, andare a una vista della telecamera.
2. Se sussiste un'associazione con un altoparlante, un gruppo di dispositivi o una zona, è visibile nella barra strumenti.
3. Fare clic per aprire la finestra **Axis speaker control (Controllo altoparlante Axis)**.
4. Fai sì che il microfono invii l'audio all'altoparlante:
   4.1. Tenere premuto mentre si parla.
   Assicurati che il misuratore del livello del microfono mostri attività vocale.
5. Riproduci una clip audio sull'altoparlante:
   5.1. Vai a **Media clip (Clip multimediale)** e seleziona una clip audio nell'elenco a discesa.

5.2. Per iniziare a riprodurre la clip audio sull'altoparlante selezionato, fare clic su Riproduci.

Riprodurre l'audio dagli altoparlanti in allarme

1. In Smart Client, andare a **Alarms** (Allarmi).
2. Selezionare un allarme che ha una telecamera come origine.
   Se è presente un'associazione con un altoparlante o una zona, saranno visibili i comandi dell'altoparlante.
3. Fai sì che il microfono invii l'audio all'altoparlante:
   - Tenere premuto mentre si parla.
     Assicurati che il misuratore del livello del microfono mostri attività vocale.
4. Riproduci una clip audio sull'altoparlante:
   - Vai a **Media clip (Clip multimediale)** e seleziona una clip audio nell'elenco a discesa.
   - Per iniziare a riprodurre la clip audio sull'altoparlante selezionato, fare clic su Riproduci.

Impostare il comportamento visivo per l'interazione con l'altoparlante

In Smart Client è possibile configurare il comportamento visivo del dispositivo tramite il controllo altoparlanti di Axis, direttamente nella vista della telecamera o tramite la Gestione degli allarmi.

Nota

I profili visivi sono supportati solo nella modalità AXIS Audio Manager Pro.

- Nel pannello laterale del **controllo altoparlanti di Axis**:
  - Fare clic su .
  - Selezionare un profilo visivo dall'elenco a discesa.
  - Se si desidera sovrascrivere i testi attualmente associati al profilo visivo selezionato, inserire il testo nella casella di testo.
- Nella vista della telecamera:
  - Andare a una vista telecamera specifica.
  - Se sussiste un'associazione con un altoparlante, un gruppo di dispositivi o una zona, è visibile nella barra strumenti.
  - Fare clic per aprire la finestra **Axis speaker control (Controllo altoparlante Axis)**.
  - Fare clic su .
- In **Gestione degli allarmi**:
  - Selezionare un evento, andare alla vista della telecamera e fare clic su .

Segnalibri per clip audio nella vista della telecamera o degli allarmi

Quando si riproduce una clip audio tramite i comandi dell'altoparlante in una vista della telecamera o in Alarms, (Allarmi) viene creato un segnalibro contenente le informazioni relative a chi e da quale dispositivo è stato riprodotta la clip audio.

Per cercare i segnalibri delle clip audio:

1. In Smart Client, andare a **Search (Cerca)**.
2. Selezionare un intervallo di tempo e una o più telecamere.
3. Fare cli su **Search for** (Ricerca) > **Bookmarks** (Segnalibri) > **New search** (Nuova ricerca).

Gestione visitatori

Plugin dell'interfono

Gli interfoni di rete Axis combinano comunicazione, videosorveglianza e controllo degli accessi remoto in un unico dispositivo. AXIS Optimizer rende più semplice la configurazione e l'uso di interfoni Axis insieme al VMS. È possibile ad esempio ricevere chiamate e aprire porte.

Impostazione di un interfono



Generalmente, la serratura va connessa al primo relè sull'interfono. AXIS Optimizer stabilisce quale porta di output usare in base alle informazioni di **Usage (Uso)**. Userà la prima porta con **Usage = Door (Uso = porta)** (RELAY1 per impostazione predefinita).

Nota

Requisiti

- Un interfono Axis
- Un microfono installato sul PC che riceve le chiamate
- Smart Client in funzione

Nota

Dalla versione 5.0.AXIS Optimizer configura gli interfono nella VMS utilizzando un metodo di configurazione diverso rispetto alle versioni precedenti. Il dispositivo per i metadati può essere utilizzato per il rilevamento delle chiamate al posto dell'Input 1. Il vecchio metodo di configurazione continua a essere supportato, ma per le nuove installazioni consigliamo quello nuovo.

1. Installare la versione più recente di AXIS Optimizer su ciascun client da cui si desidera ricevere chiamate e controllare la porta.
2. Eseguire l'accesso a Management Client.
3. Aggiungere l'interfono Axis al server di registrazione.
4. In Management Client, abilitare tutti i dispositivi necessari. Per ricevere chiamate in Smart Client è necessario disporre di:
   - Telecamera 1
   - Microfono
   - Altoparlante
   - Metadata
   - Input 2 (facoltativo se si dispone di un relè di sicurezza connesso all'interfono sulla porta 2)
   - Uscita collegata alla porta. Se si conosce l'uscita collegata alla porta, selezionarla. In caso contrario, selezionare tutte le uscite.
5. Andare a **Site Navigation > Devices > Metadata (Navigazione sito > Dispositivi > Metadati)** e selezionare il dispositivo Metadati per l'interfono in fase di installazione.
6. Fai clic su **Settings (Impostazioni)**.
7. Impostare **Event data (Dati evento)** su **Yes (Sì)**.
8. Fare clic su **Save (Salva)**.

9. Se è stato abilitato Input 2, è necessario configurare anch'esso.
   9.1. Andare a **Site Navigation > Devices > Input (Navigazione sito > Dispositivi > Input)** e selezionare Input 2.
   9.2. Fare clic su **Events (Eventi)**, quindi su **Add (Aggiungi)**.
   9.3. Selezionare **Input Falling event (Evento caduta input)** e aggiungerlo agli input abilitati. Ripetere per **Input Rising event (Evento salita input)**.
   9.4. Fare clic su **Save (Salva)**.
10. Per impostare permessi per ruoli specifici, consulta *Impostazione delle autorizzazioni per l'interfono, on page 38*.
11. *Chiamata di prova, on page 39*.

Impostazione delle autorizzazioni per l'interfono

Per gestire una chiamata, è necessario prima abilitare le autorizzazioni.

1. Vai su **Site Navigation > Security > Roles (Navigazione sito > Sicurezza > Ruoli)**.
2. Scegli un ruolo.
3. Vai a **Overall Security (Sicurezza generale)**.
4. Verifica che siano impostati i permessi necessari per ogni gruppo di sicurezza. Vai su **Hardware** e seleziona **Driver commands (Comandi driver)**.
5. Per impostare i permessi a livello di sistema, vai su **Overall Security (Sicurezza generale)**.
   Per impostare i permessi a livello di un dispositivo, vai a **Device (Dispositivo)**.
6. Impostare le autorizzazioni per i gruppi di sicurezza:
   6.1. Andare a **Cameras (Telecamere)**. Selezionare **Read (Lettura)** e **View live (Visualizzazione in diretta)**.
   6.2. Andare a **Microphones (Microfoni)**. Selezionare **Read (Lettura)** e **Listen (Ascolto)**.
   6.3. Per **Overall Security (Sicurezza generale)**, andare a **Speakers (Altoparlanti)**. Selezionare **Read (Lettura)** e **Speak (Parlare)**.
   Per **Device (Dispositivo)**, andare a **Speakers (Altoparlanti)** e selezionare **Read (Leggere)**. Quindi andare alla scheda **Speech (Parlato)** e selezionare **Speak (Parlare)**.
   6.4. Andare a **Metadata (Metadati)**. Selezionare **Read (Lettura)** e **Live (Dal vivo)**.
   6.5. Andare a **Input**. Selezionare **Read (Lettura)**.
   6.6. Andare a **Output**. Selezionare **Read (Lettura)** e **Activate (Attivare)**.

Per assegnare le autorizzazioni per controllare quali operatori gestiscono le chiamate da un determinato interfono:

1. Selezionare l'autorizzazione **Read (Lettura)** per il dispositivo metadati 1 dello specifico interfono.
2. Deselezionare questa autorizzazione per tutti gli altri ruoli. Gli utenti che non dispongono dell'autorizzazione non potranno ricevere chiamate.

Per visualizzare la cronologia delle chiamate, è necessario disporre di autorizzazioni aggiuntive.

1. Per impostare i permessi a livello di sistema, vai su **Overall Security (Sicurezza generale)**.
   Per impostare i permessi a livello di un dispositivo, vai a **Device (Dispositivo)**.
2. Selezionare queste autorizzazioni per i gruppi di sicurezza:
   2.1. Andare a **Cameras (Telecamere)**. Selezionare **Playback (Riproduzione)** e **Read sequences (Lettura sequenze)**.
   2.2. Andare a **Microphones (Microfoni)**. Selezionare **Playback (Riproduzione)** e **Read sequences (Lettura sequenze)**.
   2.3. Andare a **Speakers (Altoparlanti)**. Selezionare **Listen (Ascolto)**, **Playback (Riproduzione)** e **Read sequences (Lettura sequenze)**.

Chiamata di prova

1. In Smart Client, andare a **Settings > Axis intercom options (Impostazioni > Opzioni interfono Axis)**.
2. Fare clic su **Test call (Chiamata di test)**.
3. Selezionare un interfono e fare clic su **Make call (Effettua chiamata)**.

Eliminazione dell'eco durante le chiamate

Con la funzione push-to-talk si invia l'audio in una sola direzione alla volta attraverso l'interfono. È possibile attivare la funzione push-to-talk quando si sente l'eco in una chiamata.

Per attivare **Push-to-talk (Premi per parlare)**:

- In Smart Client, andare a **Settings** > **Axis intercom options (Impostazioni > Opzioni interfono Axis)**.
- Andare a **Call (Chiamata)** e selezionare **Push-to-talk (Premi per parlare)**.

Controllo dell'interfono dalla visualizzazione in diretta

Per ogni interfono e relativa vista, fare clic su



per controllare velocemente il dispositivo.

Modalità	Istruzioni	Commento
Apertura della serratura	Fare clic su  > **Access (Accesso)** o **Extended access (Accesso prolungato)**.	Quando la serratura è sbloccata, non è possibile fare clic su **Access (Accesso)** o **Extended access (Accesso esteso)**.
Sapere se una porta è bloccata o sbloccata	Fare clic su  e leggere lo stato nella parte inferiore del menu.	-

Modalità	Istruzioni	Commento
Conversazione con una persona di fronte all'interfono	Fare clic su  > **Start call (Avvia chiamata)**.	La finestra di chiamata si apre e avvia la comunicazione bidirezionale con l'interfono.
Informazioni su chi ha chiamato ieri	Fare clic su  > **Call history (Cronologia chiamate)**.	Verrà visualizzato un elenco delle chiamate effettuate con l'interfono corrente.

Risposta a una chiamata dalla visualizzazione in diretta

Quando un visitatore preme il pulsante di chiamata sul sistema interfono, viene visualizzata una finestra di chiamata su ogni Smart Client in esecuzione. La finestra di chiamata seleziona in automatico l'immagine della telecamera appropriata quando si ridimensiona la finestra, ad esempio la vista corridoio o orizzontale.

Modalità	Istruzioni	Commento
Rispondere alla chiamata	Fare clic su **Accept**	Si apre un canale audio bidirezionale tra l'operatore e la persona vicino all'interfono.
Inviare la chiamata a un altro operatore perché sono occupato	Chiudere la finestra facendo clic su **X**	Quando si ignora una chiamata, un altro operatore può rispondere su un altro client L'interfono continua a suonare e a lampeggiare finché qualcuno non risponde. Se nessuno risponde, alla chiamata viene assegnato lo stato persa nella cronologia delle chiamate.
Rifiutare la chiamata perché ho già aperto la porta sulla base della conferma visiva e non serve parlare con la persona	Fare clic su **Decline (Rifiuta)**	Quando si rifiuta una chiamata, le finestre di chiamata si chiudono automaticamente sugli altri client. Nessun altro operatore può accettare la chiamata.

Modalità	Istruzioni	Commento
Rifiutare la chiamata perché non voglio parlare con un visitatore indesiderato		L'interfono smette di suonare e lampeggiare, successivamente la finestra di chiamata si chiude. Alla chiamata viene assegnato lo stato con risposta nella cronologia delle chiamate.
Aprire la porta	Fare clic su **Access (Accesso)**	Il blocco interfono è aperto per 7 secondi. Per configurare il periodo di apertura della porta: 1. In Smart Client, andare a **Settings > Axis intercom options > Door access (Impostazioni > Opzioni interfono Axis > Accesso porta)**. 2. Modificare **Access time (Tempo di accesso)**.
Interrompere temporaneamente l'audio dall'operatore all'interfono.	Fare clic su **Mute (Disattiva audio)**	-
Parlare con il visitatore quando è abilitata la funzione push-to-talk.	Fare clic su **Talk (Parla)**	Rilasciare il pulsante Talk (Parla) per ascoltare il visitatore mentre parla.
Chiudere la chiamata.	Fare clic su **Hang up (Interrompi)**	L'impostazione di chiusura automatica predefinita indica che la finestra di chiamata si chiude quando si rifiuta o si interrompe una chiamata. Per modificare il comportamento predefinito della finestra di chiamata: 1. In Smart Client, andare a **Settings > Axis intercom options > Call (Impostazioni > Opzioni videocitofono Axis > Chiamata)**. 2. Deselezionare **Auto-close window (Chiusura automatica finestra)**.

Visualizzazione di più telecamere nella finestra di chiamata

Nella finestra di chiamata è possibile visualizzare un massimo di tre telecamere contemporaneamente. Ciò significa che è possibile visualizzare il flusso video dell'interfono e i flussi video di altre due telecamere nella stessa finestra di chiamata. È utile, ad esempio, quando si desidera visualizzare l'addetto alle consegne e l'area intorno alla porta di consegna contemporaneamente.

Per la configurazione di più telecamere nella finestra di chiamata:

1. In Smart Client, andare a **Settings > Axis intercom options (Impostazioni > Opzioni interfono Axis)**. Andare a **Call > Intercom settings (Chiama > Impostazioni interfono)**.

2. Andare a **Selected device (Dispositivo selezionato)** e selezionare il dispositivo da configurare.
3. Andare a **Multiple cameras (Telecamere multiple)**. Selezionare l'interfono da vedere come **camera 1 (telecamera 1)** nella finestra di chiamata.
4. Seleziona quali telecamere associate vuoi vedere come **camera 2 (telecamera 2)** e **camera 3 (telecamera 3)** nella finestra di chiamata quando l'interfono chiama.
5. Chiudere la finestra **Intercom settings (Impostazioni dell'interfono)**.

Azioni della finestra di chiamata

Con le azioni della finestra di chiamata è possibile impostare eventi definiti dall'utente legati alle regole nel motore delle regole di XProtect. Gli eventi che puoi impostare e utilizzare dipendono dal tuo ruolo.

Per impostare le azioni della finestra di chiamata:

1. In Smart Client, andare a **Settings > Axis intercom options (Impostazioni > Opzioni interfono Axis)**.
2. Andare a **Call > Intercom settings (Chiama > Impostazioni interfono)**.
3. Andare a **Selected device (Dispositivo selezionato)** e selezionare il dispositivo da configurare.
4. Andare a **Call window actions (Azioni finestra di chiamata)** per selezionare le azioni finestra di chiamata che da utilizzare.

Esistono due tipi di azioni della finestra di chiamata:

- **Access button action (Azione del pulsante di accesso)**: Quando si imposta un'azione del pulsante di accesso, l'azione predefinita del pulsante di **Access (Accesso)** viene sovrascritta. Ad esempio, è possibile impostare l'apertura di una serie di porte con il pulsante **Access (Accesso)**.
- **Custom action (Azione personalizzata)**: Quando viene impostata un'azione personalizzata, viene visualizzato un pulsante nella finestra di chiamata. È possibile attivare l'azione personalizzata facendo clic su questo pulsante. Un'azione personalizzata è un'azione che non è necessariamente correlata all'accesso alla porta, ad esempio l'invio di e-mail, l'attivazione di allarmi o l'avvio di registrazioni continue.

Visualizzare una pagina nella finestra di chiamata

È possibile visualizzare le pagine nella finestra di chiamata quando si utilizza l'intercom di rete AXIS I8307-VE. Ciò è utile per visualizzare informazioni, ad esempio una mappa o gli orari di apertura, alla persona che si trova davanti all'intercom.

In primo luogo, configurare queste pagine nell'interfaccia web dell'intercom, consultare *AXIS I8307-VE Network Intercom*.

Quando si riceve una chiamata dall'intercom:

1. Fare clic su **Show page** (Visualizza pagina) per visualizzare una finestra di dialogo con tutte le pagine configurate sul dispositivo.
2. Fare clic su **Load previews** (Carica anteprime) per visualizzare un'anteprima di tutte le pagine.
   Per visualizzare un'anteprima di una pagina configurata, spostare il cursore sulla pagina e fare clic su icona dell'immagine.
3. Fare clic su una pagina configurata per visualizzarla sull'intercom.

È possibile impostare la finestra di chiamata in modo da visualizzare sia l'immagine della telecamera dell'intercom che la pagina utilizzando varie telecamere associate, ovvero la telecamera 1 per l'immagine della telecamera e la telecamera 2 per la visualizzazione della pagina. Per ulteriori dettagli, vedere *Visualizzazione di più telecamere nella finestra di chiamata, on page 42*.

Notare che la pagina si chiude al termine della chiamata. Ripetere i passaggi sopra indicati per visualizzare una pagina relativa a una nuova chiamata.

Filtro dell'estensione di chiamata

Per impostazione predefinita, tutti i PC connessi all'interfono ricevono le chiamate. Aggiungendo le estensioni di chiamata e filtrandole in VMS, le chiamate possono essere instradate dagli interfoni a determinati Smart Client nel sistema VMS. È possibile impostare pianificazioni per l'instradamento delle chiamate e aggiungere contatti di fallback. Inoltre, le chiamate possono essere instradate a contatti basati su SIP, da aggiungere come contatti di fallback.

Nell'interfaccia web dell'interfono

1. Andare a **Communication (Comunicazione)** > **SIP**.
2. Selezionare **Enable SIP (Abilita SIP)**.
3. Fare clic su **Save (Salva)**.
4. Andare a **Communication** > **VMS Calls** (Comunicazione, Chiamate).
5. Assicurarsi che **Allow calls in the video management system (VMS) (Consenti chiamate nel sistema di gestione video (VMS))** sia attivato.
6. Andare a **Communication** > **Contact list** (Comunicazione, Lista dei contatti).
7. In **Recipients (Destinatari)**, fare clic su + per aggiungere un nuovo contatto. Inserire le informazioni per il nuovo contatto e fare clic su **Save (Salva)**. È possibile aggiungere diversi contatti.
   - In **SIP address (Indirizzo SIP)** inserire `VMS_CALL:<extension>`. Sostituire `<extension>` con il nome dell'estensione di chiamata, ad esempio `ReceptionA`.
   - Se si desidera impostare una pianificazione per il contatto, scegliere **Availability (Disponibilità)** per il contatto.
   - È possibile aggiungere un contatto di fallback che riceverà la chiamata in caso di mancata risposta dei contatti originali, ad esempio `ReceptionB`.
8. Andare a **Communication** > **Calls**. (Comunicazione, Chiamate).
9. Per i dispositivi con AXIS OS precedente alla versione 11.6, disattivare **Make calls in the video management system (VMS) (Effettuare chiamate nel sistema di gestione video (VMS))**.
10. In **Recipients (Destinatari)**, rimuovere il contatto **VMS** e aggiungere il nuovo contatto creato.

In Management Client

È consigliabile configurare gli interfoni nel VMS per utilizzare un dispositivo di metadati per il rilevamento delle chiamate. Vedere *Impostazione di un interfono, on page 37*.

In Smart Client

Impostare l'estensione di chiamata per ogni utente che deve ricevere le chiamate. L'impostazione è memorizzata a livello di utente. Questo significa che l'utente riceverà le chiamate indipendentemente dal PC utilizzato.

1. Accedere a Smart Client come utente destinatario delle chiamate.
2. Andare a **Settings > Axis intercom options (Impostazioni > Opzioni interfono di Axis)**.
3. In **Call > Call extension** (Chiamata, Estensione di chiamata), inserire il nome dell'estensione di chiamata del contatto, ad esempio `ReceptionA`. A questo punto l'utente riceverà le chiamate solo se l'estensione di chiamata corrisponde al valore del filtro.
   Se si desidera aggiungere diversi nomi di estensioni di chiamata, separarli con il punto e virgola, ad esempio `ReceptionA;ReceptionC`

Visualizzazione della cronologia di chiamata

Nella cronologia delle chiamate è possibile visualizzare le chiamate con risposta, quelle perse e se la porta è stata sbloccata. È possibile selezionare le chiamate e visualizzare il video corrispondente, se disponibile.

1. In Smart Client, andare alla vista dell'interfono.

2. Fare clic su  > **Call history (Cronologia chiamate)**.

Nota

La cronologia delle chiamate è limitata a 39 chiamate e 1.000 voci del registro degli accessi. Il numero limitato di chiamate può essere inferiore se la conversazione viene silenziata di frequente.

Per eseguire una registrazione quando una porta è stata sbloccata, è necessario impostare il tempo di conservazione (giorni) per l'interfono Axis:

1. In Management Client, andare a **Tools > Options > Alarm and Events > Event retention (Strumenti > Opzioni > Allarmi ed eventi > Conservazione degli eventi)**.
2. Impostare l'ora per **Output Activated (Output attivato)** e **Output Deactivated (Output disattivato)**.

Disattivazione del microfono in caso di mancanza di chiamate attive

È possibile disattivare il microfono quando non arrivano chiamate all'interfono Axis. Il microfono verrà acceso quando è in arrivo una chiamata attiva.

Nota

- Sono necessari i diritti di amministratore per spegnere il microfono.
- Questa funzione non è supportata nell'architettura federata né quando si utilizzano i contatti di riserva.

1. In Smart Client, andare a **Settings** > **Axis intercom options (Impostazioni > Opzioni interfono Axis)**.
2. Selezionare **Turn off intercom microphone when no active call (Disattiva microfono dell'interfono quando non ci sono chiamate attive)**.

Ricezione di un allarme in caso di apertura forzata di una porta

Se una porta è dotata di un relè di sicurezza (Ingresso 2), la sovrapposizione porta nella finestra di chiamata di Smart Client mostra quando la porta è aperta o chiusa. Ciò significa che se qualcuno apre la porta forzandola mentre è bloccata, è possibile ricevere un allarme.

Nota

Per ricevere un allarme, almeno uno Smart Client deve essere in esecuzione.

Per configurare l'allarme:

1. In Smart Client, andare a **Settings > Axis intercom options > Administrator options (Impostazioni > Opzioni videocitofono Axis > Opzioni amministratore)**.
2. Selezionare **Trigger an alarm when a door has been forced open (Attiva un allarme quando una porta è stata sottoposta ad apertura forzata)**.

Ricezione di un allarme in caso di porta aperta troppo a lungo

Se una porta è dotata di un relè di sicurezza (Ingresso 2), la sovrapposizione porta nella finestra di chiamata di Smart Client mostra quando la porta è aperta o chiusa. Ciò significa che se qualcuno apre la porta e la porta rimane aperta per troppo tempo, sarà possibile ricevere un allarme.

Nota

Per ricevere un allarme, almeno uno Smart Client deve essere in esecuzione.

Per configurare l'allarme:

1. In Smart Client, andare a **Settings > Axis intercom options > Administrator options (Impostazioni > Opzioni videocitofono Axis > Opzioni amministratore)**.
2. Selezionare **Trigger an alarm when a door has been open longer than (s) (Attiva un allarme quando una porta è stata aperta per oltre (s))**.
3. Inserire il valore di tempo per cui la porta può rimanere aperta prima della disattivazione dell'allarme.

Esclusione di un client dalla ricezione di chiamate

È possibile configurare un client in modo da non ricevere chiamate. Ciò significa che quando qualcuno avvia una chiamata, non verrà aperta alcuna finestra di chiamata nel client specifico.

1. In Smart Client, andare a **Settings > Axis intercom options > Call (Impostazioni > Opzioni videocitofono Axis > Chiamata)**.
2. Deselezionare **Receive calls on this client (Ricevi chiamate su questo client)**.

Visualizzazione dell'audio

Vista microfono

Puoi visualizzare l'audio nel sistema con l'aggiunta di una o più viste microfono a Smart Client. Poi potrai eseguire il monitoraggio dell'audio sia nella visualizzazione in diretta che nella riproduzione. Potrai vedere quando i livelli audio salgono al di sopra di un certo livello usando il rilevamento audio integrato sul dispositivo Axis. I casi d'uso tipici sono:

- *Ascolto di molteplici microfoni in contemporanea, on page 48*
- *Rilevamento di incidenti con l'audio, on page 48*
- *Indaga gli incidenti dopo che sono accaduti, on page 48*

Nota

Requisiti

- VMS Smart Client 2020 R2 o versione successiva.

Configurazione di VMS per la vista microfono

1. Impostazione dei livelli di rilevamento:
   1.1. Su Management Client, vai a **Site Navigation > AXIS Optimizer > Device assistant (Navigazione sito > AXIS Optimizer > Assistente dispositivo)** e seleziona il tuo dispositivo.
   1.2. Apri le impostazioni **Detectors (Rilevatori)**. Il modo in cui si aprono tali impostazioni dipende dalla versione del software del dispositivo.
   1.3. Vai su **Audio detection (Rilevamento di suoni)** e modifica **Input 1 sound level (Volume sonoro input 1)** in base alle tue necessità.
2. Portare eventi dalla telecamera al VMS:
   2.1. Su Management Client, vai a **Site Navigation > Devices > Microphones (Navigazione sito > Dispositivi > Microfoni)**.
   2.2. Fai clic sul microfono, poi su **Events (Eventi)**.
   2.3. Aggiungi gli eventi **Audio Falling (Calo audio)** e **Audio Rising (Salita audio)**.
3. Configura quanto a lungo il sistema conserva i metadati relativi all'audio rilevato:
   3.1. Vai su **Tools > Options > Alarm and Events > Device events (Strumenti > Opzioni > Allarmi ed eventi > Eventi del dispositivo)**.
   3.2. Trova **Audio Falling (Calo audio)** e imposta il tempo di conservazione.
   3.3. Trova **Audio Raising (Salita audio)** e imposta il tempo di conservazione.
4. Verifica di aver eseguito l'impostazione della registrazione audio. Ad esempio, puoi registrare l'audio sempre o procedere alla creazione di una regola di registrazione sulla base di eventi di salita o calo audio.
5. Per ciascun microfono che vuoi usare con la vista microfono, ripeti i passaggi precedenti.
6. Su Smart Client, vai su **Settings > Timeline > Additional data (Impostazioni > Sequenza > Dati aggiuntivi)** e seleziona **Show (Mostra)**.

Aggiunta della vista microfono a Smart Client

1. Apri Smart Client e fai clic su **Setup (Impostazione)**.
2. Vai a **Views (Viste)**.
3. Fare clic su **Create new view (Crea nuova vista)** e selezionare un formato.
4. Andare a **System overview > AXIS Optimizer (Panoramica di sistema > AXIS Optimizer)**.
5. Fai clic su **Microphone view (Vista microfono)** e trascinala nella vista.
6. Seleziona un microfono.
7. Fare clic su **Setup (Impostazione)**.

Usa vista microfono

- Visualizzazione in diretta
  - I livelli audio sono visualizzati come grafico a barre con il livello attuale a destra e la cronologia audio fino a 60 s che si muove verso sinistra.
  - Fai clic nella vista per ascoltare l'audio dal microfono.
  - In ogni vista microfono c'è un'icona cuffie. Fare clic sull'icona per disattivare o attivare l'audio di ogni vista senza dover selezionare la vista stessa. In questo modo è possibile ascoltare più microfoni contemporaneamente.
- Riproduzione
  - Un'icona evidenzia quando viene rilevato audio disponibile per il microfono.

- Le barre gialle indicano che è avvenuto un rilevamento di audio sulla base dei livelli di rilevamento che hai impostato sul dispositivo.
- Fai clic nella vista per ascoltare l'audio dal microfono.
- In ogni vista microfono c'è un'icona cuffie. Fare clic sull'icona per disattivare o attivare l'audio di ogni vista senza dover selezionare la vista stessa. In questo modo è possibile ascoltare più microfoni contemporaneamente.

Ascolto di molteplici microfoni in contemporanea

La vista microfono permette l'ascolto di molteplici microfoni in contemporanea, sia nella visualizzazione in diretta sia nella riproduzione.

1. *Configurazione di VMS per la vista microfono, on page 47*.
2. Apri Smart Client e fai clic su **Setup (Impostazione)**.
3. Vai a **Views (Viste)**.
4. Fai clic su **Create new view (Crea nuova vista)** e seleziona una suddivisione dell'immagine.
5. Andare a **System overview > AXIS Optimizer (Panoramica di sistema > AXIS Optimizer)**.
6. Per ogni microfono che vuoi ascoltare:
   6.1. Fai clic su **Microphone view (Vista microfono)** e trascinala nella vista.
   6.2. Seleziona un microfono.
7. Fare clic su **Setup (Impostazione)**.
8. Per ogni microfono, decidi se vuoi la disattivazione o l'attivazione dell'audio facendo clic sull'icona cuffie in ogni vista del microfono. Ora puoi ascoltare in contemporanea tutti i microfoni non silenziati.

Rilevamento di incidenti con l'audio

Potresti voler eseguire il monitoraggio delle azioni che avvengono in aree dove non è permessa l'installazione di telecamere, ad esempio i bagni. Nella vista microfono puoi vedere velocemente quando avviene un evento, ad esempio quando il volume sonoro supera i livelli di rilevamento.

1. *Configurazione di VMS per la vista microfono, on page 47*. Ricorda l'impostazione dei livelli di rilevamento per il dispositivo e per l'area che vuoi monitorare.
2. Aggiungere una vista microfono con il dispositivo alla visualizzazione in diretta su Smart Client, vedere *Aggiunta della vista microfono a Smart Client, on page 47*.

Indaga gli incidenti dopo che sono accaduti

Una volta accaduto un evento, puoi identificare velocemente i periodi nella sequenza temporale di riproduzione dove i tuoi microfoni hanno rilevato l'audio.

1. *Configurazione di VMS per la vista microfono, on page 47*.
2. Per eseguire l'aggiunta di una o più viste microfono con dispositivi pertinenti per la riproduzione in Smart Client, consultare *Aggiunta della vista microfono a Smart Client, on page 47*.

Ricerca forense

AXIS Optimizer offre quattro categorie di ricerca per i dispositivi Axis nella ricerca centralizzata:

- *Ricerca forense, on page 49* (ricerca di oggetti)
- *Ricerca veicolo, on page 52*
- *Ricerca velocità zona, on page 55*
- *Ricerca contenitore, on page 57*

È inoltre possibile aggiungere una scheda di ricerca delle targhe separata a Smart Client, vedere *Targhe Axis, on page 58*.

È possibile configurare queste categorie di ricerca in un pannello centralizzato, vedere *Configurare le categorie di ricerca Axis, on page 106*.

Ricerca forense

Le telecamere Axis dotate di firmware AXIS OS 9.50 o versione successiva generano metadati con la descrizione di ogni oggetto che si muove nel campo visivo di una telecamera. Il VMS può registrare tali dati insieme a relativi video e audio. La funzione di ricerca forense in AXIS Optimizer ti consente di eseguire l'analisi e l'esecuzione delle ricerche in tali dati. Usare la ricerca forense per ottenere una panoramica di tutte le attività nella scena o individuare velocemente un oggetto o un evento specifico di interesse.

Prima di iniziare

1. Verificare di disporre dell'ultima versione AXIS OS sulla telecamera.
2. Verificare che il proprio VMS sia dotato della versione corretta:
   - Corporate 2019 R3 o versione successiva o Expert 2019 R3 o versione successiva
   - Professional+ 2022 R3 o versione successiva o Express+ 2022 R3 o versione successiva
3. L'ora della telecamera deve essere sincronizzata con NTP.
4. Per filtrare per i tipi di oggetto **umano**, **veicolo**, **moto/bicicletta**, **autobus**, **auto** o **camion**:
   4.1. Usare un dispositivo Axis con supporto per AXIS Object Analytics. Vedi il filtro Analisi nel *Selettore prodotti*.
   4.2. Andare a **System > Analytics metadata (Sistema > Analisi metadati)** e abilitare **Analytics Scene Description (Descrizione scena analisi)** nella pagina Web della telecamera.
5. Per il filtraggio in base al **Vehicle** color (Colore del veicolo), **Upper body clothing color (Colore abbigliamento superiore)** o **Lower body clothing color (Colore abbigliamento inferiore)**:
   5.1. Usare un dispositivo Axis con supporto per AXIS Object Analytics. Vedi il filtro Analisi nel *Selettore prodotti*.
   5.2. Usa un dispositivo Axis con ARTPEC-8 o CV25. Vedere il filtro System-on-chip nel *Product selector (Selettore prodotti)*.

Configurazione della ricerca forense



1. In Management Client, verificare che il dispositivo di metadati sia abilitato per le telecamere.
2. Assicurarsi che il dispositivo dei metadati sia collegato alla telecamera:

- Andare a **Devices (Dispositivi)** > **Camera (Telecamera)** e selezionare il dispositivo.
- Accedere alla scheda **Client** e assicurarsi che il dispositivo dei metadati della telecamera sia selezionato in **Related metadata (Metadati correlati)**.

3. Vai a **Site Navigation > Devices > Metadata (Navigazione sito > Dispositivi > Metadati)**.
4. Selezionare il dispositivo e fare clic su **Record (Registra)**. Assicurarsi che **Recording (Registrazione)** sia abilitata.
   Per impostazione predefinita, i metadati vengono registrati solo quando il VMS rileva del movimento in una scena. Si consiglia pertanto la regolazione della soglia di movimento nell'ambiente per non perdere nessun movimento dell'oggetto.
5. Fare clic su **Settings (Impostazioni)** e assicurarsi che l'opzione **Analytics data (Dati di analisi)** sia abilitata.
6. Aprire la visualizzazione in diretta di Smart Client e assicurarsi di vedere dei riquadri delimitatori sugli oggetti e che i riquadri siano visualizzati correttamente.
   Potrebbe volerci del tempo prima che l'orologio si adatti all'ora NTP.
7. Attendere almeno 15 minuti per consentire al sistema di registrare video e metadati. Al termine sarà possibile avviare la ricerca, vedere *Esecuzione di una ricerca, on page 50*.
8. Attivare **Consolidated metadata (Metadati consolidati)** per il miglioramento della velocità di ricerca sui dispositivi che eseguono AXIS OS 11.10 o superiore. Vedere *Metadati e ricerca, on page 105*.

Esecuzione di una ricerca



Nota

Prima di poter utilizzare questa funzione di ricerca, è necessario configurarla in Management Client. Per scoprire come fare, vedere *Configurazione della ricerca forense, on page 49*.

1. In Smart Client, andare a **Search (Cerca)**.
2. Selezionare un intervallo di tempo e una o più telecamere.
3. Fare clic su **Search for > Forensic search > New search (Cerca > Ricerca forense > Nuova ricerca)**. Per ciascun risultato della ricerca, verrà visualizzato l'oggetto e la traiettoria dell'oggetto nella miniatura.
   - La miniatura mostra il fotogramma video quando l'oggetto è più visibile.
   - Il punto verde indica la posizione in cui la telecamera ha eseguito il rilevamento dell'oggetto per la prima volta.
   - Il punto rosso indica la posizione in cui la telecamera ha eseguito il rilevamento dell'oggetto per l'ultima volta.
   - Fare clic su **Play forward (Avanzamento riproduzione)** nel pannello di anteprima per la visualizzazione della sequenza video completa.
   - Per nascondere le sovrapposizioni grafiche, andare a **Bounding boxes (Riquadri delimitatori)** e selezionare **Hide (Nascondi)**.

   Nota

   Le applicazioni di analisi in esecuzione sulla telecamera, ad esempio AXIS Object Analytics e AXIS Loitering Guard, potrebbero imprimere sovrapposizioni nel video. Per la rimozione di tali sovrapposizioni, andare alla pagina di configurazione Web dell'applicazione.
4. Selezionare i filtri della ricerca per limitarne il numero di risultati.
   Per saperne di più sull'uso dei diversi filtri, vedere *Ottimizzazione di una ricerca, on page 51*.

5. Selezionare i risultati della ricerca che si desidera esaminare più attentamente. È possibile, ad esempio, creare un segnalibro o *Creare un report PDF di alta qualità, on page 58*.

Ottimizzazione di una ricerca

Per limitare i risultati della ricerca è possibile usare uno o più filtri della ricerca.

- **Region of interest (Regione di interesse)**
  Rilevare oggetti che sono stati spostati in un'area specifica.
- **Direzione dell'oggetto**
  Rilevare oggetti il cui spostamento è avvenuto lungo un percorso specifico in una scena: a sinistra, a destra, verso il basso o l'alto.
- **Tipo di oggetto**
  Rilevare oggetti di un tipo specifico: esseri umani, veicoli, biciclette, autobus, auto o camion.

Nota

- La velocità (km/h) e la targa sono supportate solo su telecamere AXIS Q1686–DLE Radar-Video Fusion Camera.
- Per poterli utilizzare, è necessario attivare la velocità (km/h o mph) e la targa. A tal fine, vedere *Configurare le categorie di ricerca Axis, on page 106*.
- **Speed (km/h or mph) (Velocità (km/h))**
  Rilevare i veicoli che si muovono entro una certa velocità.
- **Targa**
  Rilevare i veicoli che hanno una specifica targa. È possibile usarlo anche per cercare targhe che includono determinate lettere o numeri.
- **Colore veicolo**
  Rilevare i veicoli del colore scelto.
- **Colore abbigliamento superiore**
  Rilevare l'abbigliamento del colore scelto sulla parte superiore del corpo di un umano.
- **Colore abbigliamento inferiore**
  Rilevare l'abbigliamento del colore scelto sulla parte inferiore del corpo di un umano.
- **Time-of-day (Ora del giorno)**
  Rilevare oggetti il cui rilevamento è avvenuto nel corso di una specifica parte della giornata. Questo filtro risulta utile quando viene eseguita una ricerca su più giorni, ma è necessario trovare solo gli oggetti a un'ora specifica di ogni giorno, ad esempio durante il pomeriggio.
- **Tempo minimo nella scena (s)**
  Rilevare oggetti che sono stati rilevati e monitorati per un numero minimo di secondi. Questo filtro nasconde gli oggetti che non sono rilevanti per la ricerca, ad esempio oggetti lontani e oggetti fittizi (effetti di luce). Il valore predefinito è 1 s. Ciò significa che quando il filtro non è impostato, gli oggetti con una durata inferiore a 1 s vengono esclusi.
- **Oggetti ondulanti (% dell'immagine)**
  Escludere gli oggetti che si sono spostati solo in un'area limitata, ad esempio una bandiera o un albero mosso dal vento. Il valore predefinito è 5-100%. Ciò significa che quando il filtro non è impostato, gli oggetti che non si sono spostati per oltre il 5% dell'area dell'immagine vengono esclusi.

Limiti

- Per avere le riprese video corrette per i risultati di ricerca, è importante che la sincronizzazione dell'orologio sia esatta.
- I dati analizzati in Ricerca forense non tengono conto della prospettiva della scena. Perciò le dimensioni e la velocità di un oggetto differiscono in base a quanto è vicino alla telecamera.
- Le condizioni climatiche avverse, ad esempio pioggia o neve, possono influire sulla precisione del rilevamento.

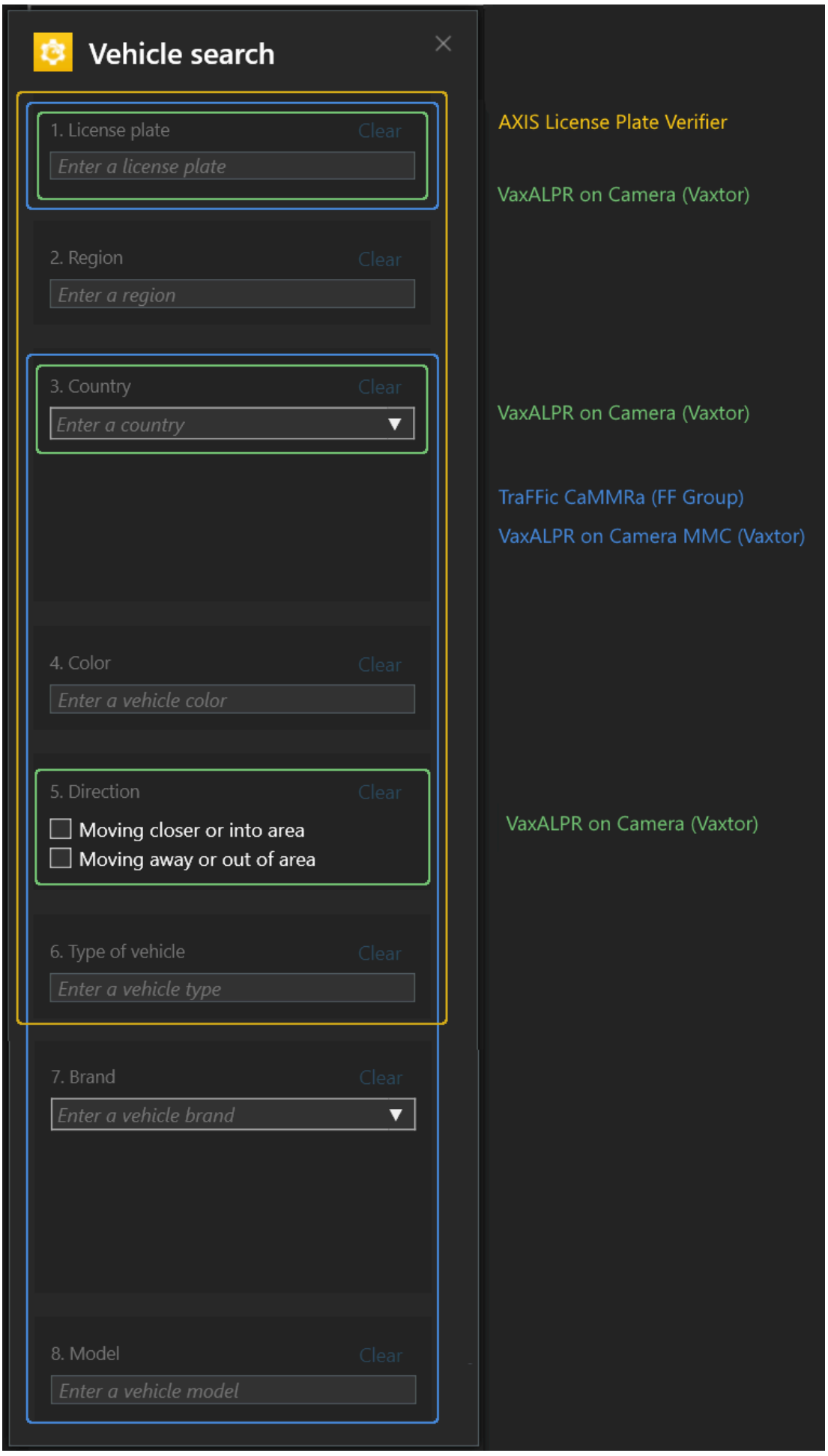
- L'analisi sarà più precisa se il contrasto dell'oggetto in scene a bassa luminosità è buono.
- Ci sono circostanze in cui un solo oggetto può generare più risultati. Ad esempio quando il rilevamento viene perso a causa dell'oscuramento temporaneo di un oggetto da parte di un altro.
- Le sovrapposizioni possono variare a seconda della versione di XProtect. Ad esempio puoi: le sovrapposizioni nell'anteprima video richiedono XProtect 2020 R3 e i colori della sovrapposizione richiedono XProtect 2020 R2.
- Affinché la Ricerca forense funzioni sui flussi video ruotati di 180 gradi, è necessario:
  - usare AXIS OS 10.6 o versione successiva sulle telecamere oppure
  - usare Device Pack 11.0 o versione successiva sul server di registrazione
- L'impostazione del bilanciamento del bianco sulla telecamera deve essere precisa per poter ottenere un buon rilevamento dei colori

Ricerca veicolo

Quando si utilizza AXIS Optimizer insieme ad alcune applicazioni installate sulla telecamera, è possibile cercare, identificare e condividere le prove video relative ai veicoli. La ricerca dei veicoli supporta i dati delle targhe da queste applicazioni:

- *AXIS License Plate Verifier* di Axis Communications
- *CAMMRA AI* di FF Group (è richiesta la versione 1.3 o superiore)
- *VaxALPR On Camera* di Vaxtor Recognition Technologies
- *VaxALPR On Camera MMC* di Vaxtor Recognition Technologies

I filtri della ricerca che è possibile utilizzare dipendono dall'applicazione installata sulle telecamere, vedere *Ottimizzazione di una ricerca, on page 54*


Vehicle search
1. License plate
Clear
Enter a license plate
2. Region
Clear
Enter a region
3. Country
Clear
Enter a country
4. Color
Clear
Enter a vehicle color
5. Direction
Clear
Moving closer or into area
Moving away or out of area
6. Type of vehicle
Clear
Enter a vehicle type
7. Brand
Clear
Enter a vehicle brand
8. Model
Clear
Enter a vehicle model
AXIS License Plate Verifier
VaxALPR on Camera (Vaxtor)
VaxALPR on Camera (Vaxtor)
TraFFic CaMMRa (FF Group)
VaxALPR on Camera MMC (Vaxtor)
VaxALPR on Camera (Vaxtor)

Configurazione della ricerca di veicoli

Nota

Requisiti

- Sistema VMS:
  - Corporate o Expert 2019 R3 o versione successiva
  - Professional+ o Express+ 2022 R3 o versione successiva
- Ora telecamera sincronizzata con NTP
- Una delle applicazioni elencate in

1. In Management Client, aggiungere la telecamera che esegue l'applicazione scelta.
2. Abilitare tutti i dispositivi necessari. Per poter utilizzare AXIS Licence Plate Verifier, sono necessari Camera 1 e Metadata 1
3. Assicurarsi che il dispositivo dei metadati sia collegato alla telecamera:
   - Andare a **Devices (Dispositivi)** > **Camera (Telecamera)** e selezionare il dispositivo.
   - Accedere alla scheda **Client** e assicurarsi che il dispositivo dei metadati della telecamera sia selezionato in **Related metadata (Metadati correlati)**.
4. Configurare i metadati:
   4.1. Andare a **Site Navigation > Recording Server (Navigazione sito > Server registrazione)** e individuare il dispositivo.
   4.2. Selezionare Metadati 1 e fare clic su **Settings (Impostazioni)**.
   4.3. Vai a **Metadata stream > Event data (Flusso metadati > Dati evento)** e seleziona **Yes (Sì)**.
5. Vai alla scheda **Record settings (Impostazioni di registrazione)** e controlla che la registrazione sia abilitata per i metadati.
6. Fare clic su **Save (Salva)**.
7. Configurare l'applicazione affinché funzioni per un utente standard:
   7.1. Aggiungere diritti di lettura e riproduzione per la telecamera e l'utente specifici.
   7.2. Aggiungere diritti di lettura e riproduzione sui metadati per la telecamera e l'utente specifici.

Ricerca di un veicolo

1. In Smart Client, andare a **Search (Cerca)**.
2. Selezionare un intervallo di tempo e una o più telecamere.
3. Fare clic su **Search for > Vehicle search > New search (Cerca > Ricerca veicolo > Nuova ricerca)**.
4. Selezionare i filtri della ricerca per limitarne il numero di risultati.
   Per saperne di più sui vari filtri, vedere *Ottimizzazione di una ricerca, on page 54*.
5. Selezionare i risultati della ricerca che si desidera esaminare più attentamente. È possibile, ad esempio, creare un segnalibro o *Creare un report PDF di alta qualità, on page 58*.

Ottimizzazione di una ricerca

Per limitare i risultati della ricerca è possibile usare uno o più filtri della ricerca. Le varie applicazioni offrono diverse opzioni di filtro.

- **Targa**
  Individuare un numero di targa specifico.
  Applicazione: AXIS License Plate Verifier, VaxALPR On Camera, CAMMRA AI oppure VaxALPR On Camera MMC.
- **Area**
  Consente di trovare veicoli in una determinata regione.

Applicazione: AXIS License Plate Verifier 2.9.19.

Nota

Impostare la posizione della telecamera nelle impostazioni di Axis License Plate Verifier per un riconoscimento ottimale della regione.

- **Paese**
  Consente di trovare veicoli in un determinato paese.
  Applicazione: Axis License Plate Verifier 2.9.19, VaxALPR On Camera, CAMMRA AI o VaxALPR On Camera MMC.
- **Colore**
  Consente di trovare veicoli di un colore specifico.
  Applicazione: Axis License Plate Verifier 2.9.19, CAMMRA AI o VaxALPR On Camera MMC.
- **Direction (Direzione)**
  Consente di trovare i veicoli in movimento in una specifica direzione.
  Applicazione: Axis License Plate Verifier 2.9.19, VaxALPR On Camera, CAMMRA AI o VaxALPR On Camera MMC.
- **Tipo di veicolo**
  Consente di trovare un tipo specifico di veicolo.
  Applicazione: Axis License Plate Verifier 2.9.19, CAMMRA AI o VaxALPR On Camera MMC.
- **Marchio**
  Consente di trovare un marchio specifico di veicolo.
  Applicazione: CAMMRA AI o VaxALPR On Camera MMC.
- **Modello**
  Consente di trovare un modello specifico di veicolo.
  Applicazione: CAMMRA AI o VaxALPR On Camera MMC.

Ottimizzare la velocità di ricerca

È possibile migliorare la velocità di ricerca controllando i dati che il sistema memorizza sul dispositivo dei metadati VMS.

- Disattivare i dati di analisi se non necessari.
  - Andare a **Devices (Dispositivi)** > **Metadata (Metadati)** e selezionare il dispositivo.
  - Fare clic su **Settings (Impostazioni)** e disattivare **Analytics data (Dati analitici)**.
- Se si ha bisogno di dati per l'analisi, si può ricorrere ai metadati consolidati se disponibili. Vedere *Metadati e ricerca, on page 105*.
- Disattivare gli eventi non necessari in AXIS License Plate Verifier. Per il corretto funzionamento di AXIS Optimizer è sufficiente l'evento **Lost (Perso)**. Vedere *AXIS License Plate Verifier*.
- Assicurarsi di utilizzare AXIS OS 12.8 o una versione successiva.

Ricerca velocità zona

In AXIS Optimizer, si può usare la ricerca velocità di zona per la ricerca di veicoli in eccesso di velocità rilevati quando entrano in una zona predeterminata nella vista di una telecamera. La ricerca velocità di zona funziona insieme all'applicazione *AXIS Speed Monitor* per la visualizzazione della velocità dei veicoli in una zona di rilevamento radar nella visualizzazione in diretta della telecamera. Con la ricerca velocità zona di AXIS, sei in grado di impostare filtri specifici per restringere la ricerca ed esportare e condividere le prove video nel corso delle indagini.

Configura ricerca velocità zona

Nota

Requisiti

- Sistema VMS:

  - Corporate o Expert 2019 R3 o versione successiva
  - Professional+ o Express+ 2022 R3 o versione successiva
- Ora telecamera sincronizzata con NTP

1. In Management Client, aggiungere la telecamera che esegue l'applicazione scelta.
2. Abilitare tutti i dispositivi necessari. Per poter usare la ricerca delle infrazioni di velocità in zona di AXIS, sono necessari Camera 1 e Metadata 1
3. Assicurarsi che il dispositivo dei metadati sia collegato alla telecamera:
   - Andare a **Devices (Dispositivi)** > **Camera (Telecamera)** e selezionare il dispositivo.
   - Accedere alla scheda **Client** e assicurarsi che il dispositivo dei metadati della telecamera sia selezionato in **Related metadata (Metadati correlati)**.
4. Per configurare i metadati:
   4.1. Andare a **Site Navigation > Recording Server (Navigazione sito > Server registrazione)** e individuare il dispositivo.
   4.2. Selezionare Metadati 1 e fare clic su **Settings (Impostazioni)**.
   4.3. Vai a **Metadata stream > Event data (Flusso metadati > Dati evento)** e seleziona **Yes (Sì)**.
5. Vai alla scheda **Record settings (Impostazioni di registrazione)** e controlla che la registrazione sia abilitata per i metadati.
6. Fare clic su **Save (Salva)**.
7. Per configurare l'applicazione affinché funzioni per un utente standard:
   7.1. Aggiungere diritti di lettura e riproduzione per la telecamera e l'utente specifici.
   7.2. Aggiungere diritti di lettura e riproduzione sui metadati per la telecamera e l'utente specifici.

Ricerca di eventi di velocità della zona



1. In Smart Client, andare a **Search (Cerca)**.
2. Selezionare un intervallo di tempo e una o più telecamere.
3. Fare clic su **Search for > Zone speed search > New search (Cerca > Ricerca velocità zona > Nuova ricerca)**.
4. Selezionare i filtri della ricerca per limitarne il numero di risultati.
   Per saperne di più sui vari filtri, vedere *Ottimizzazione di una ricerca, on page 56*.
5. Selezionare i risultati della ricerca che si desidera esaminare più attentamente. È possibile, ad esempio, creare un segnalibro o *Creare un report PDF di alta qualità, on page 58*.

Ottimizzazione di una ricerca

Per limitare i risultati della ricerca degli eventi di eccesso di velocità è possibile usare uno o più filtri della ricerca.

- **Max speed (Velocità massima)**
  Filtra la velocità massima di ogni oggetto nella zona per la durata dell'evento. Puoi impostare un limite inferiore e uno superiore per la velocità massima.
- **Tipo di oggetto**

Se è selezionato **Vehicle (Veicolo)**, la ricerca mostrerà solo gli eventi di eccesso di velocità in cui l'oggetto più veloce nella zona è stato classificato come veicolo.

- **Nome zona**
  Cerca e filtra le zone per nome.

Ricerca contenitore

Quando si utilizza AXIS Optimizer insieme a determinate applicazioni, è possibile cercare, identificare e condividere le prove video sui contenitori. La ricerca dei contenitori supporta i dati di questa applicazione:

- *Contenitori VaxOCR* di Vaxtor Recognition Technologies

Configurazione della ricerca del contenitore

Nota

Requisiti

- Sistema VMS:
  - Corporate o Expert 2019 R3 o versione successiva
  - Professional+ o Express+ 2022 R3 o versione successiva
- Ora telecamera sincronizzata con NTP
- L'applicazione elencata in

1. In Management Client, aggiungere la telecamera che esegue l'applicazione scelta.
2. Abilitare tutti i dispositivi necessari.
3. Assicurarsi che il dispositivo dei metadati sia collegato alla telecamera:
   - Andare a **Devices (Dispositivi)** > **Camera (Telecamera)** e selezionare il dispositivo.
   - Accedere alla scheda **Client** e assicurarsi che il dispositivo dei metadati della telecamera sia selezionato in **Related metadata (Metadati correlati)**.
4. Configurare i metadati:
   4.1. Andare a **Site Navigation > Recording Server (Navigazione sito > Server registrazione)** e individuare il dispositivo.
   4.2. Selezionare Metadati 1 e fare clic su **Settings (Impostazioni)**.
   4.3. Vai a **Metadata stream > Event data (Flusso metadati > Dati evento)** e seleziona **Yes (Sì)**.
5. Vai alla scheda **Record settings (Impostazioni di registrazione)** e controlla che la registrazione sia abilitata per i metadati.
6. Fare clic su **Save (Salva)**.
7. Configurare l'applicazione affinché funzioni per un utente standard:
   7.1. Aggiungere diritti di lettura e riproduzione per la telecamera e l'utente specifici.
   7.2. Aggiungere diritti di lettura e riproduzione sui metadati per la telecamera e l'utente specifici.

Ricerca di un contenitore

1. In Smart Client, andare a **Search (Cerca)**.
2. Selezionare un intervallo di tempo e una o più telecamere.
3. Fare clic su **Search for > Container search > New search (Cerca > Ricerca contenitore > Nuova ricerca)**.
4. Selezionare i filtri della ricerca per limitarne il numero di risultati.
   Per saperne di più sui vari filtri, vedere *Ottimizzazione di una ricerca, on page 58*.
5. Selezionare i risultati della ricerca che si desidera esaminare più attentamente. È possibile, ad esempio, creare un segnalibro o *Creare un report PDF di alta qualità, on page 58*.

Ottimizzazione di una ricerca

Per limitare i risultati della ricerca è possibile usare uno o più filtri della ricerca. Tutte le opzioni di filtro provengono dai contenitori VaxOCR dell'applicazione.

- **Codice container**
  Individuare un codice contenitore specifico.
- **Proprietario**
  Individuare i contenitori che appartengono a un determinato proprietario.
- **Codice proprietario**
  Individuare i contenitori che appartengono a un determinato proprietario.
- **Dimensioni**
  Individuare i contenitori di una certa dimensione e tipo.
- **Codice dimensione**
  Individuare i contenitori di una certa dimensione e tipo.
- **City or country (Città o paese)**
  Trova i contenitori di una determinata città o paese.
- **Convalida**
  Trova i contenitori che sono già stati convalidati tramite il codice proprietario o la cifra di controllo.

Creare un report PDF di alta qualità



Creare un report in base ai risultati della ricerca. È possibile utilizzare questa funzione per includere immagini ad alta risoluzione nei risultati.

1. Eseguire una ricerca in Smart Client.
2. Selezionare i risultati della ricerca da includere nel report.
3. Fare clic su p,255mm,sfx)=″graphics:graphicE602A880D1B5621C58ABCAEDE29CCC0F″ > **Create high quality PDF report (Crea report PDF di alta qualità)**.
4. (Facoltativo) Immettere **Report name (Nome report)**, **Report destination (Destinazione report)** e **Notes (Note)**.
5. Per ciascun risultato della ricerca, selezionare il fotogramma da includere nel report. Fare doppio clic per ingrandire un'immagine.
6. Fare clic su **Create (Crea)**. Quando il report è pronto verrà inviata una notifica.

Targhe Axis

È possibile aggiungere una scheda separata per la ricerca e la gestione delle targhe in Smart Client. Questa scheda centralizza tutte le attività dell'operatore relative alla gestione delle targhe, alla ricerca e all'esportazione in base alle informazioni fornite dalle telecamere Axis abilitate per LPR.



Prima di iniziare

- Verificare di avere la versione VMS 2018 R3 o successiva
- Assicurarsi di disporre di VMS Device Pack 10.1 o versione successiva
- L'ora della telecamera deve essere sincronizzata con NTP
- Usare una delle applicazioni elencate in

Configurazione delle targhe Axis

1. In Management Client, aggiungere la telecamera che esegue l'applicazione scelta.
2. Abilitare tutti i dispositivi necessari. Per poter utilizzare AXIS Licence Plate Verifier, sono necessari Camera 1 e Metadata 1
3. Assicurarsi che il dispositivo dei metadati sia collegato alla telecamera:
   - Andare a **Devices (Dispositivi)** > **Camera (Telecamera)** e selezionare il dispositivo.
   - Accedere alla scheda **Client** e assicurarsi che il dispositivo dei metadati della telecamera sia selezionato in **Related metadata (Metadati correlati)**.
4. Configurare i metadati:
   4.1. Andare a **Site Navigation > Recording Server (Navigazione sito > Server registrazione)** e individuare il dispositivo.
   4.2. Selezionare Metadati 1 e fare clic su **Settings (Impostazioni)**.
   4.3. Vai a **Metadata stream > Event data (Flusso metadati > Dati evento)** e seleziona **Yes (Sì)**.
5. Vai alla scheda **Record settings (Impostazioni di registrazione)** e controlla che la registrazione sia abilitata per i metadati.
6. Fare clic su **Save (Salva)**.

Ricerca di una targa

1. In Smart Client, vai su **Axis license plates (targhe Axis)**.
   Se la scheda non è visualizzata, vai su **Settings > Axis search options (Impostazioni > Opzioni di ricerca Axis)** e selezionare **Show license plate search tab (Mostra scheda ricerca targa)**.
2. Fare clic su **Add camera... (Aggiungi telecamera...)** e selezionare le telecamere pertinenti > Fare clic su **Close (Chiudi)**.
   Per aggiungere telecamere al sistema è necessario essere amministratori. Quando la telecamera rileva le targhe, queste appaiono dal vivo nell'elenco, comprese le immagini ritagliate delle targhe riprese dalla telecamera. Il risultato della ricerca non visualizza più di 5.000 risultati.
3. Immettere una targa e un **Time interval (Intervallo di tempo)** per filtrare i risultati della ricerca.
   - Immettere un **Time interval (Intervallo di tempo)** personalizzato tra due date specifiche, per filtrare i risultati della ricerca.

Ricerca di una targa in diretta

1. In Smart Client, vai su **Axis license plates (targhe Axis)**.
   Se la scheda non è visualizzata, vai su **Settings > Axis search options (Impostazioni > Opzioni di ricerca Axis)** e selezionare **Show license plate search tab (Mostra scheda ricerca targa)**.

2. Fare clic su **Add camera... (Aggiungi telecamera...)** e selezionare le telecamere pertinenti > Fare clic su **Close (Chiudi)**.
   Per aggiungere telecamere al sistema è necessario essere amministratori. Quando la telecamera rileva le targhe, queste appaiono dal vivo nell'elenco, comprese le immagini ritagliate delle targhe riprese dalla telecamera. Il risultato della ricerca non visualizza più di 5.000 risultati.
3. Immettere una targa e selezionare **Time interval (Intervallo di tempo)** > **Live (In tempo reale)** per filtrare i risultati della ricerca.

Ottimizzazione di una ricerca

Per limitare i risultati della ricerca è possibile usare uno o più filtri della ricerca.

- **Intervallo di tempo**
  Filtra in base ai riscontri della ricerca entro un periodo di tempo.
- **Targa**
  Filtra in base al testo della targa parziale o completo.
- **Telecamere**
  Filtra in base ai risultati di ricerca rilevati da telecamere specifiche.
- **Direction (Direzione)**
  Filtra in base ai veicoli in movimento in una determinata direzione.
- **Elenchi**
  Filtra in base ai risultati di ricerca in determinati siti e filtra in base ai risultati di ricerca consentiti, ai blocchi e agli elenchi personalizzati. Per ulteriori informazioni su come configurare gli elenchi, vedere *Gestione centralizzata degli elenchi delle targhe, on page 23*.

Ottimizzare la velocità di ricerca

È possibile migliorare la velocità di ricerca controllando i dati che il sistema memorizza sul dispositivo dei metadati VMS.

- Disattivare i dati di analisi se non necessari.
  - Andare a **Devices (Dispositivi)** > **Metadata (Metadati)** e selezionare il dispositivo.
  - Fare clic su **Settings (Impostazioni)** e disattivare **Analytics data (Dati analitici)**.
- Se si ha bisogno di dati per l'analisi, si può ricorrere ai metadati consolidati se disponibili. Vedere *Metadati e ricerca, on page 105*.
- Disattivare gli eventi non necessari in AXIS License Plate Verifier. Per il corretto funzionamento di AXIS Optimizer è sufficiente l'evento **Lost (Perso)**. Vedere *AXIS License Plate Verifier*.
- Assicurarsi di utilizzare AXIS OS 12.8 o una versione successiva.

Esportare la ricerca di una targa come report PDF

Utilizzare questa funzione per compilare i risultati della ricerca di interesse come report PDF con immagini di alta qualità.

1. Fare clic su **Export...(Esporta)**.
2. Selezionare **PDF...**.
3. (Facoltativo) Immettere **Report name (Nome report)**, **Report destination (Destinazione report)** e **Notes (Note)**.
4. Per ciascun risultato della ricerca, selezionare il fotogramma da includere nel report. Per ingrandire un'immagine, fare doppio clic.
5. Fare clic su **Create (Crea)**. Quando il report è pronto verrà inviata una notifica.

Esportare la ricerca di una targa come report CSV

Utilizzare questa funzione per compilare un numero elevato di risultati della ricerca in formato CSV.

1. Fare clic su **Export...(Esporta)**.
2. Selezionare **CSV...**.
3. Scegliere una destinazione per il file in cui eseguire l'esportazione.

Informazioni Axis

Informazioni Axis offre una panoramica dei dati dai dispositivi attraverso grafici e dashboard. Con questa opzione, è possibile visualizzare i metadati per tutti i dispositivi. È possibile visualizzare i dati relativi agli oggetti rilevati, ai veicoli identificati e agli allarmi. È inoltre possibile creare nuovi dashboard e condividerli con altri utenti.

Axis insights è disponibile nelle viste amministratore e operatore. La vista amministratore predefinita in Axis insights è disponibile solo per gli utenti con diritti di amministratore, mentre la vista operatore predefinita è disponibile per tutti gli operatori con le autorizzazioni appropriate. Vedere *Configura le impostazioni dei ruoli, on page 99* (Configura le impostazioni dei ruoli). La vista operatore fornisce dati specifici dalle viste delle telecamere selezionate e impostate, mentre la vista amministratore fornisce una panoramica dell'intero sistema.

Accedere ad Axis insights

- Accedere a **Smart Client** e fare clic su **Axis insights**.
- **Dashboard**: Selezionare una dashboard dall'elenco a discesa.
- **Camera view (Vista telecamera)**: Selezionare una vista specifica della telecamera per la panoramica dei dati.
- **Time range (Intervallo di tempo)**: Selezionare un intervallo di tempo specifico.
- **Auto-update (aggiornamento automatico)**: Attivare per aggiornare i dati in automatico.

••• Il menu contestuale contiene:

- **Edit dashboard (Modifica dashboard)**: Modificare, condividere o rimuovere il dashboard.
- **Add chart (Aggiungere grafico)**: Creare un nuovo grafico nel dashboard.
- **Informazioni su Axis insights**: Leggere informazioni su Axis insights.

••• Il menu contestuale di ciascun grafico contiene:

- **Maximize chart (Massimizza il grafico)**: Fare clic per ingrandire il grafico.
- **Copy as image (Copia come immagine)**: Fare clic per copiare il grafico negli appunti.
- **Export (Esporta)**: Fare clic per esportare il grafico in formato PNG o CSV.
- **Edit chart (Modifica grafico)**: Fare clic per modificare il grafico.
- **Remove chart (Rimuovere il grafico)**: Fare clic per rimuovere il grafico.

Nota

- In alcuni grafici è possibile fare clic sulla figura per visualizzare ulteriori informazioni.
-  : Mostra le selezioni specifiche applicabili a ciascun grafico nella dashboard.

Creare un nuovo dashboard

1. **Dashboard**: Selezionare **Add dashboard** (Aggiungi dashboard) dall'elenco a discesa.
2. Fare clic su **Empty (Vuoto)** per creare una nuova dashboard oppure fare clic su **From existing dashboard (Da una dashboard esistente)** per creare una dashboard simile a una già disponibile nel sistema.

3. **Nome**: Inserire un nome per il dashboard.
4. **Allow other users to view this dashboard** (Consenti ad altri utenti di visualizzare questo dashboard): Fare clic per condividere la dashboard con altri utenti in modalità di sola lettura.
5. fare clic su **Applica**;
6. **Add chart (Aggiungere grafico)**: Fare clic per aggiungere un nuovo grafico.
   - **Select chart type (Seleziona tipo di grafico)**: Selezionare il tipo di grafico desiderato e fare clic su **Next** (Avanti). È possibile cercare un tipo di grafico utilizzando i tag o i titoli dei grafici, come ad esempio analisi video, veicoli, grafici a linee e così via.
   - **Modify data selections (Modifica selezioni dati)**: Selezionare i filtri applicabili in ogni categoria.
   - **Adjust appearance (Regolare aspetto)**: Modifica i testi e seleziona le dimensioni grafico.

Configurare l'elenco a discesa della dashboard

Nota

- Per impostazione predefinita, è possibile visualizzare solo le dashboard create.

Per visualizzare le dashboard condivise da altri utenti nell'elenco a discesa **Dashboard**:

1. Andare a **Shared dashboards (Dashboard condivise)**.
2. Attivare l'interruttore relativo a ciascuna dashboard condivisa che si desidera aggiungere all'elenco a discesa.

Mostrare gli approfondimenti per una specifica vista della telecamera

Durante la visualizzazione in diretta o la riproduzione in una vista telecamera, è possibile aprire Axis Insights con la vista telecamera attiva già preselezionata.

Per aprire Informazioni Axis per una vista specifica della telecamera:

1. Andare a **Smart Client** e aprire una vista.
2. Fare clic su **Show insights (Mostra informazioni)**.

Configurare Informazioni Axis

1. Verificare che la telecamera supporti Axis Object Analytics. Vedere l'analisi in *Axis Product Selector*.
2. Verificare che la data e l'ora della telecamera siano impostate correttamente.
3. Verificare che il dispositivo di metadati sia abilitato per le telecamere in Management Client.
4. Assicurarsi che il dispositivo dei metadati sia collegato alla telecamera:
   - Andare a **Devices (Dispositivi)** > **Camera (Telecamera)** e selezionare il dispositivo.
   - Accedere alla scheda **Client** e assicurarsi che il dispositivo dei metadati della telecamera sia selezionato in **Related metadata (Metadati correlati)**.
5. Per visualizzare tutti i dati disponibili in Axis Insights, abilitare l'analisi scena sulla propria telecamera tramite *AXIS Scene Metadata*:
   5.1. Andare a **Devices (Dispositivi)** > **Metadata (Metadati)** e selezionare il dispositivo.
      - Fare clic su **Record (Registra)** e verificare che l'opzione **Recording (Registrazione)** sia abilitata.
      - Fare clic su **Settings (Impostazioni)** e assicurarsi che l'opzione **Analytics data (Dati di analisi)** sia abilitata.

   5.1. Abilitare **Consolidated metadata (Metadati consolidati)** per tempi di caricamento più rapidi, se disponibile. Vedere *Metadati e ricerca, on page 105*.

6. Per abilitare i dati per i tipi di grafici utilizzando *AXIS Object Analytics*, *AXIS Image Health Analytics*, oppure i *Sensori ambientali*:
   - Andare a **Devices (Dispositivi)** > **Metadata (Metadati)** e selezionare il dispositivo.
   - Fare clic su **Record (Registra)** e verificare che l'opzione **Recording (Registrazione)** sia abilitata.
   - Fare clic su **Settings (Impostazioni)** e assicurarsi che l'opzione **Event data (Dati evento)** sia abilitata.
   - Si consiglia di creare una regola nel VMS per registrare sempre i metadati da questo dispositivo.
7. Impostare le autorizzazioni per i gruppi di sicurezza:
   7.1. Andare a **Site Navigation (Navigazione sito)** > **Security (Sicurezza)** > **Roles (Ruoli)**.
   7.2. Seleziona un ruolo.
   7.3. Andare a **Cameras (Telecamere)**. Selezionare **Read (Lettura)**.
   7.4. Andare a **Metadata (Metadati)**. Selezionare **Read (Lettura)**, **Live (In diretta)** e **Playback (Riproduzione)**.
8. Per aggiungere i metadati delle targhe a Informazioni Axis, vedere *Configurazione delle targhe Axis, on page 59*

Risoluzione dei problemi per Axis insights

Problema	Soluzione
I grafici visualizzano "nessun dato".	È necessario configurare Informazioni Axis. Vedere *Configurare Informazioni Axis, on page 62*.
Il caricamento della vista operatore richiede molto tempo.	• Ridurre l'intervallo di tempo. • Creare e utilizzare una vista della telecamera con un minor numero di telecamere di analisi della scena. • Abilitare i metadati consolidati, vedere *Metadati e ricerca, on page 105*.

Dewarping video

Il dewarping appiattisce e corregge la prospettiva di un'immagine distorta geometricamente a causa di un grand'angolo o obiettivo fisheye. Il dewarping Axis nel VMS si può usare con qualsiasi telecamera panoramica Axis a 360°. Il dewarping avviene direttamente nella telecamera o in Smart Client.

Ulteriori dettagli sul dewarping:

- quando usi il dewarping lato client, otterrai un dewarping uniforme sia nei video in diretta che nelle registrazioni.
- Quando torni a una vista, passerai in automatico all'ultima posizione di dewarping.
- Il dewarping è incluso quando si esportano i video.
- È possibile salvare una posizione iniziale, vedere *Impostazione di una posizione iniziale, on page 66*.
- È possibile configurare se agli operatori è permesso controllare e modificare le viste sottoposte a dewarping, vedere *Controllo e modifica delle viste con dewarping da parte degli operatori, on page 67*.

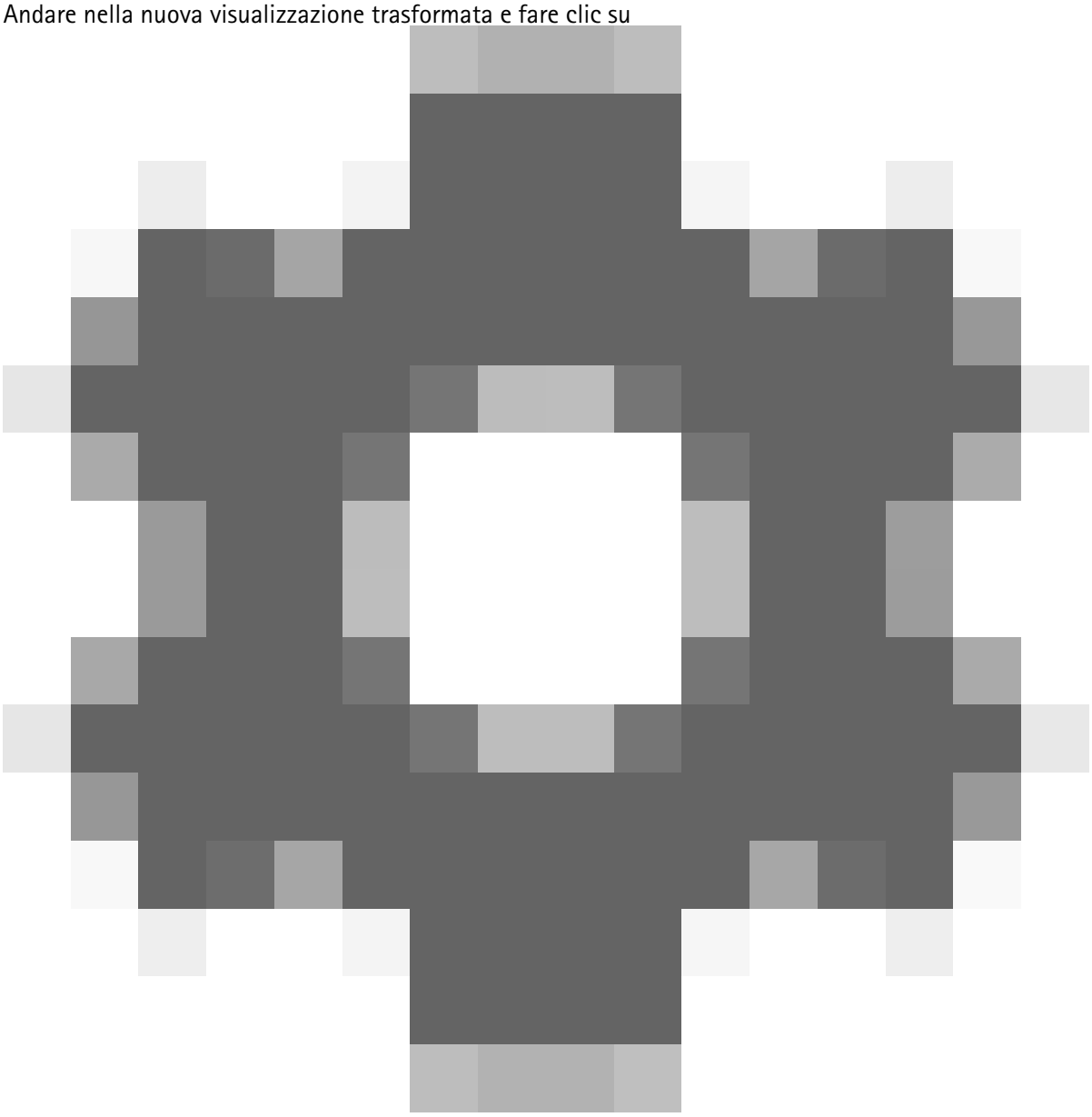
Creazione di una vista con dewarping



Nota

Per ottimizzare il flusso per il dewarping, selezionare la massima risoluzione disponibile per **Video stream 1 (Flusso video 1)** di **Camera 1 (Telecamera 1)** in Management Client. Per maggiori informazioni, vedere *Prestazioni e risoluzione dei problemi, on page 67*.

1. Apri Smart Client e fai clic su **Setup (Impostazione)**.
2. Vai a **Views (Viste)**.
3. Fare clic su **Create new view (Crea nuova vista)** e selezionare un formato.
4. Andare a **System overview > AXIS Optimizer (Panoramica di sistema > AXIS Optimizer)**.
5. Fare clic su **Dewarping view (vista sottoposta a dewarping)** e trascinarla nella vista.
6. Selezionare una telecamera e la posizione di montaggio corrente della telecamera.
7. Fare clic su **Setup (Impostazione)**.

8. Andare nella nuova visualizzazione trasformata e fare clic su 
.
9. Fare clic su **Set view type (Imposta tipo di vista)** e selezionare un'opzione. In base alla modalità di montaggio della telecamera, è possibile selezionare **Quad**, **Normal (Normale)**, **Normal with overview (Normale con panoramica)** o **Panorama (Panoramica)**.

Nota

Si consiglia di usare 100 % DPI. Se la risoluzione è diversa da 100%, il dewarping Axis sul secondo display potrebbe non essere completamente visibile.

Se si utilizzano altre impostazioni DPI, le finestre di distorsione potrebbero essere solo parzialmente visibili. Seguire le istruzioni in questi articoli esterni per risolvere questo problema:

- *Problemi con XProtect su schermi ad alta risoluzione (4K e versioni successive)*
- *Ridimensionamento interfaccia grafica utente client su schermi a DPI elevati*

Creazione di una vista con dewarping per telecamere panoramiche multisensore

È possibile usare le viste dewarping per le telecamere panoramiche multisensore, ad esempio AXIS P3807-PVE Network Camera e AXIS Q3819-PVE Panoramic Camera.

- Stitching lato client. Se la telecamera è impostata sulla modalità di acquisizione dewarp client, AXIS Optimizer esegue lo stitching delle quattro immagini in una panoramica continua (solo AXIS P3807-PVE).
- Regolazione orizzonte. È possibile regolare l'orizzonte della panoramica. Ciò può risultare utile se la telecamera è inclinata verso il suolo e l'orizzonte è curvo. Questa operazione renderà inoltre più intuitivi i comandi PTZ virtuali.
- Comandi PTZ. Consentono di ingrandire e spostarsi nell'immagine come in una telecamera PTZ.



Nota

Requisiti

- Utenti con uno dei seguenti diritti utente:
  - Ruolo ottimizzatore
  - Hardware > Comandi driver = Consenti
- Telecamera panoramica multisensore Axis

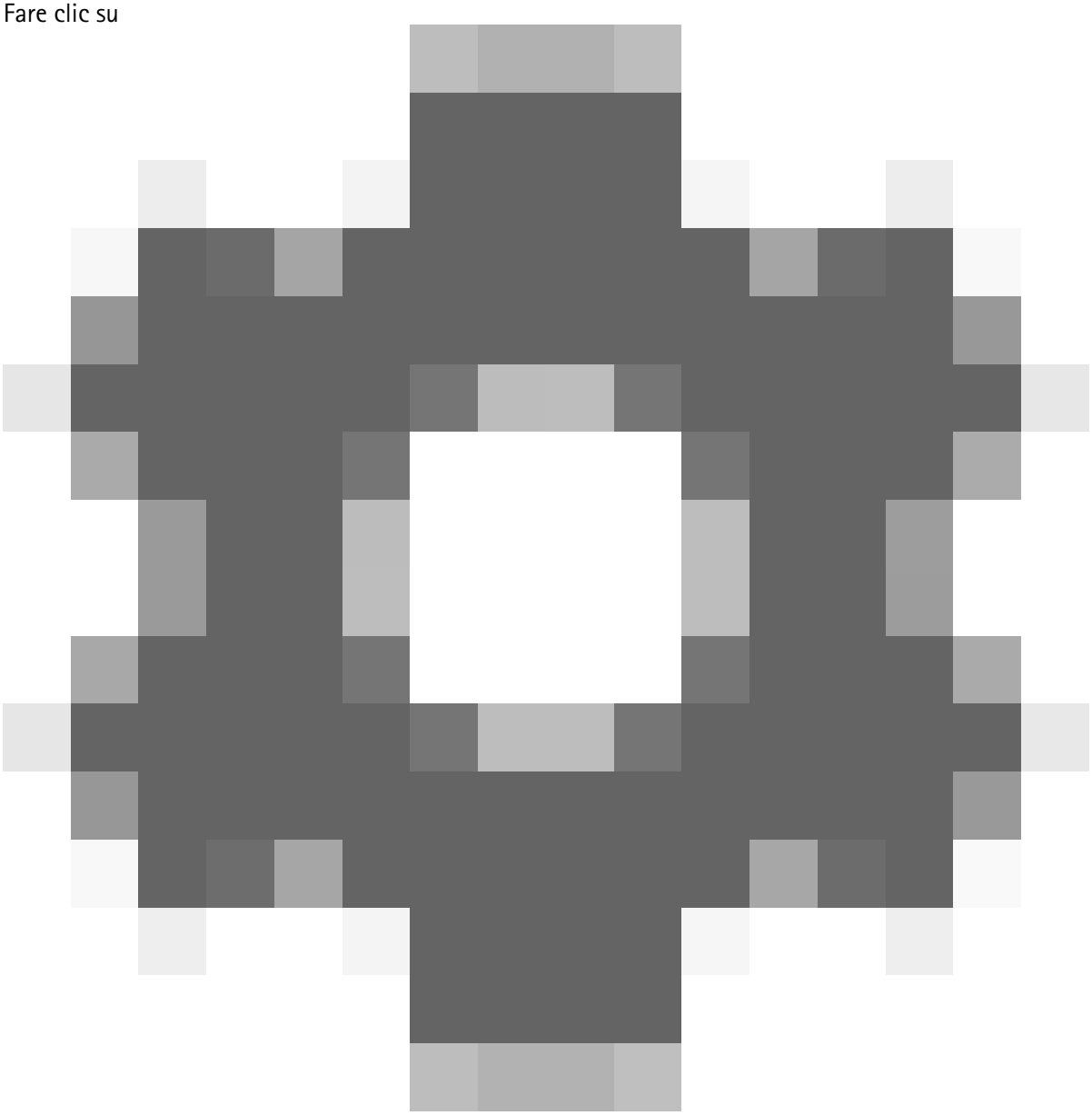
1. Se applicabile, impostare la modalità di acquisizione su **Client Dewarp (Dewarp client)** nel corso dell'impostazione iniziale del dispositivo.
2. Apri Smart Client e fai clic su **Setup (Impostazione)**.
3. Vai a **Views (Viste)**.
4. Fare clic su **Create new view (Crea nuova vista)** e selezionare un formato.
5. Andare a **System overview > AXIS Optimizer (Panoramica di sistema > AXIS Optimizer)**.
6. Fare clic su **Dewarping view (vista sottoposta a dewarping)** e trascinarla nella vista.
7. Selezionare una telecamera panoramica multisensore.
   La prima volta che si aggiunge la telecamera panoramica multisensore a una vista dewarping, sopra la vista sarà visualizzata una finestra di calibrazione dell'orizzonte.
8. Fare clic sulle frecce per allineare la linea rossa all'orizzonte.
9. Fare clic su **Done (Fatto)** per il salvataggio delle impostazioni ed uscire dalla modalità di calibrazione.

Vista ampia

La vista ampia è un tipo di visualizzazione per le telecamere panoramiche multisensore. Accendere **wide view (vista ampia)** se il normale campo visivo di 120° non è sufficiente. Con la vista ampia, l'immagine verrà sempre corretta. Spegnere **wide view (vista ampia)** per ottenere una transizione alla vista normale quando si esegue lo zoom completo.

Impostazione di una posizione iniziale

1. In Smart Client, aprire una vista sottoposta a dewarping.
2. Vai alla posizione che desideri salvare come posizione iniziale.

3. Fare clic su , quindi su **Set home position**.

Controllo e modifica delle viste con dewarping da parte degli operatori

È possibile configurare se agli operatori è consentito controllare e modificare le viste sottoposte a dewarping, vedere *Personalizzazione dell'accesso alle funzionalità per gli operatori, on page 99*.

Prestazioni e risoluzione dei problemi

Considerazioni sulle prestazioni

- Se possibile, il dewarping video di Axis viene eseguito nella GPU, ma verrà caricato anche sulla CPU.
- Per evitare che la velocità in fotogrammi porti a una vista di grandi dimensioni con molte viste sottoposte a dewarping, considerare quanto segue:
  - Risoluzione della telecamera. Un'elevata risoluzione della telecamera, ad esempio 2.880 x 2.880, consuma molta potenza del computer rispetto ad esempio alla risoluzione 1.920 x 1.920.
  - Velocità in fotogrammi della telecamera. Se non è necessaria un'elevata velocità in fotogrammi, una modifica a una velocità in fotogrammi più bassa può impedire la deframmentazione nella vista sottoposta a dewarping e in altre viste.

- Risoluzione del monitor. I monitor ad alta risoluzione, ad esempio 4K, richiedono molte risorse per visualizzare il video. Se non è necessaria la risoluzione più elevata, una risoluzione del monitor inferiore rende possibile eseguire più viste con dewarping senza scatti.

Risoluzione dinamica

- Il flusso video verrà automaticamente ridimensionato, se possibile, senza diminuire la qualità del video. In questo modo è possibile migliorare le prestazioni delle viste sottoposte a dewarping.
- In caso di luce lampeggiante quando si esegue lo zoom dalla panoramica, può essere utile disattivare la risoluzione dinamica.
- Per attivare o disattivare la risoluzione dinamica: in Smart Client, andare in **Settings (Impostazioni) > Axis dewarping options (Opzioni di dewarping Axis) > Rendering options (Opzioni di rendering)** e selezionare o cancellare **Dynamic resolution (Risoluzione dinamica)**.
- **Dynamic resolution (Risoluzione dinamica)** è abilitata per impostazione predefinita.

Rendering compatibilità

- Se si verificano errori visivi nell'immagine di dewarping, ad esempio un'immagine nera o se le prestazioni sembrano peggiori del previsto, abilitare il rendering di compatibilità. Le transizioni tra viste e ripulitura in riproduzione potrebbero essere soggette a sfarfallio, svantaggio del rendering di compatibilità.
- Per attivare o disattivare il rendering di compatibilità: aprire Smart Client e andare in **Settings (Impostazioni) > Axis dewarping options (Opzioni di dewarping Axis) > Rendering options (Opzioni di rendering)** e selezionare o cancellare **Use compatibility rendering (Usa rendering compatibilità)**.
- **Use compatibility rendering (Usa rendering compatibilità)** è abilitata per impostazione predefinita.

Cosa aspettarsi

In un sistema di riferimento con Intel i7 8700 NVIDIA Gefore 1050 GTX e tre monitor con risoluzione 1.920 x 1.080:

- 7 viste sottoposte a dewarping alla risoluzione 1.920 x 1.920 e 25fps possono essere eseguite senza perdite di fotogrammi oppure
- 4 viste sottoposte a dewarping in risoluzione 2.880 x 2.880 e 25 fps

Se uno dei tre schermi viene eseguito alla risoluzione 4K invece di 1.920 x 1.080:

- 5 viste sottoposte a dewarping in risoluzione 1.920 x 1.920 e 25fps possono essere eseguite senza perdite di fotogrammi oppure
- 3 viste sottoposte a dewarping in risoluzione 2.880 x 2.880 e 25 fps. Una vista sottoposta a dewarping su ciascun monitor.

Velocità in fotogrammi e risoluzione hanno scale lineari. Un computer in grado di eseguire 5 viste sottoposte a dewarping con 30 fps può eseguire 10 viste se si riduce la velocità in fotogrammi a 15 fps.

Integrazione di dispositivi indossabili

AXIS Optimizer Body Worn Extension consente agli utenti della telecamera di registrare, etichettare e condividere video con investigatori che possono cercare e gestire le prove video utilizzando il VMS. Il servizio consente la connessione e il trasferimento tra il sistema indossabile Axis e il VMS. AXIS Body Worn Extension è un servizio indipendente gratuito che è necessario installare sul server di registrazione.

Nota

Le versioni supportate sono:

- Versione VMS 2020 R1 Corporate o versioni più nuove
- Versione VMS 2020 R1 Professional+ o versioni più recenti
- Versione VMS 2020 R1 Expert o versioni più recenti

Utilizzare sempre i più recenti hotfix e programmi di installazione di patch cumulative per VMS.

Per saperne di più

- Per scaricare il servizio stesso o leggere la guida all'integrazione e la nota sulla soluzione, andare a *axis.com*.
- Per leggere il manuale per l'utente, andare a *axis.help.com*.

Controllo accessi

Il controllo degli accessi è una soluzione che combina il controllo fisico degli accessi con la videosorveglianza. Questa integrazione consente di configurare un sistema di controllo degli accessi Axis direttamente dal Management Client. Il sistema si integra perfettamente con XProtect, consentendo agli operatori di monitorare gli accessi ed eseguire azioni di controllo degli accessi nello Smart Client.

Nota

Requisiti

- VMS versione 2024 R1 o successiva.
- Licenze di accesso per XProtect, vedere *licenze di accesso*.
- Installare AXIS Optimizer sul server eventi e sul Management Client.

Le porte 53459 e 53461 si apriranno per il traffico in entrata (TCP) durante l'installazione di AXIS Optimizer tramite AXIS Secure Entry.

Per utilizzare le porte in AXIS Secure Entry, è necessario acquisire una licenza per ciascuna porta; vedere *Attivare le licenze per le porte, on page 71*.

Configurazione controllo degli accessi

Nota

Prima di iniziare, fare quanto segue:

- Aggiornare il software del door controller. Consultare la tabella che segue per conoscere la versione minima e consigliata di AXIS OS per la tua versione VMS.
- Assicurarsi che la data e l'ora siano corrette.

Versione AXIS Optimizer	Versione minima AXIS OS	Versione AXIS OS consigliata
6.0	12.6.94.1	12.10.73.4
5.8	12.6.94.1	12.8.55.1
5.6	12.6.94.1	12.6.94.1

Aggiunta di un door controller di rete Axis al sistema

1. Andare a **Site Navigation** > **AXIS Optimizer** > **Access control** (Navigazione sito, AXIS Optimizer, Controllo degli accessi).
2. In **Configuration** (Configurazione), selezionare **Devices** (Dispositivi).
3. Selezionare **Discovered devices** (Dispositivi rilevati) per visualizzare l'elenco delle unità che è possibile aggiungere al sistema.
4. Seleziona le unità che si desidera aggiungere.
5. Fare clic su **+ Add** (+ Aggiungi) nella finestra popup e fornire le credenziali per il controller.

Nota

- Nella scheda **Management** (Gestione) si dovrebbero vedere i controller aggiunti.
- Per aggiungere manualmente un controller al sistema, fare clic su **+ Add** (+ Aggiungi) nella scheda **Management** (Gestione).
- Per integrare l'aggiornamento nel VMS ogni volta che si aggiunge, rimuove o si modifica il nome di un door controller:
  - Andare a **Site Navigation** (navigazione sito) > **Access control** (controllo degli accessi) e fare clic su Access Control integration (Integrazione del controllo degli accessi).
  - Fare clic su **Refresh Configuration (Aggiorna configurazione)** nella scheda **General settings (Impostazioni generali)**.

Attivare le licenze per le porte

Prima di poter aggiungere delle porte, è necessario attivare le licenze presenti nel sistema.

1. In **Site Navigation (Navigazione sito)**, andare a **License Information (Informazioni licenza)**.
2. Fare clic su **Activate License Manually (Attiva licenza manualmente)** e scegliere tra **Online** o **Offline**.
3. Per attivare online le licenze per le porte:
   – Immettere il nome utente e la password.
4. Per attivare le licenze delle porte offline, vedere *activate licenses offline (attiva licenze offline)*.

Se è necessario modificare il numero di licenze per le porte da attivare:

1. Andare a **AXIS Optimizer** > **Access control** (AXIS Optimizer, Controllo degli accessi).
2. In **Configuration** (Configurazione), selezionare **Devices** (Dispositivi).
3. Andare a **Allocated door licenses (Licenze per porta assegnate)** > **Custom license allocation (Assegnazione personalizzata delle licenze)** e inserire il numero di licenze per porta che si desidera utilizzare.
4. fare clic su **Applica**;
5. Andare a pagina **License Information (Informazioni sulle licenze)** e riattivare le proprie licenze.

Configurazione del controllo degli accessi

1. Andare a **Site Navigation** > **AXIS Optimizer** > **Access control** (Navigazione sito, AXIS Optimizer, Controllo degli accessi).
2. Per modificare i profili di identificazione predefiniti o creare un nuovo profilo di identificazione, vedere *Profili di identificazione, on page 86*.
3. Per utilizzare un'impostazione personalizzata per i formati della tessera e la lunghezza del PIN, vedere *Formati tessera e PIN, on page 83*.
4. Aggiungere una porta e applicare un profilo di identificazione alla porta. Vedere *Aggiunta di una porta, on page 74*.
5. Aggiungere una zona e aggiungere porte alla zona. Vedere *Aggiunta di una zona, on page 80*.

Compatibilità del software del dispositivo per i door controller

Importante

Quando si aggiorna il sistema operativo AXIS OS sul door controller, tenere presente quanto segue:

- **Versioni AXIS OS supportate:** Le versioni del sistema operativo AXIS OS supportate, elencate in precedenza, sono valide solo in caso di aggiornamento dalla rispettiva versione VMS originale consigliata e quando il sistema è dotato di porta. Se il sistema non soddisfa queste condizioni, è necessario eseguire l'aggiornamento alla versione di AXIS OS consigliata per la versione VMS.
- **Versione AXIS OS minima supportata:** La versione di AXIS OS più vecchia installata nel sistema determina la versione minima supportata di AXIS OS, con un limite di due versioni precedenti. Supponiamo che si stia utilizzando AXIS Optimizer versione 6.0 e che si effettui l'aggiornamento di tutti i dispositivi alla versione consigliata di AXIS OS 12.10.73.4. D'ora in poi, la versione 12.6.94.1 di AXIS OS sarà la versione minima supportata per il proprio sistema.
- **Aggiornamento a una versione di AXIS OS superiore a quella consigliata:** supponiamo che si esegua l'aggiornamento a una versione di AXIS OS superiore a quella consigliata per una determinata versione di VMS. In tal caso, è sempre possibile eseguire il downgrade alla versione AXIS OS consigliata senza alcun problema, purché rientri nei limiti di supporto fissati per la versione di VMS.
- **Suggerimenti per AXIS OS futura:** Seguire sempre la versione AXIS OS consigliata per la rispettiva versione di VMS per garantire la stabilità del sistema e la piena compatibilità.

Integrazione controllo degli accessi

Per integrare il controllo degli accessi nel VMS:

1. Andare a **Site Navigation** > **Access Control** (Navigazione sito, Controllo degli accessi).
2. Fare clic con il pulsante destro del mouse su **Access Control** (Controllo degli accessi) e su **Create new...** (Crea nuovo).
3. Nella finestra di dialogo **Create Access Control System Integration** (Crea integrazione del sistemi di controllo degli accessi):
   - Immettere un nome per l'integrazione.
   - Selezionare **AXIS Secure Entry** dal menu a discesa in **Integration plug-in** (Plug-in di integrazione).
   - Fare clic su **Next** (Avanti) fino a quando non appare la finestra di dialogo **Associate cameras** (Associa telecamere).
     Per associare le telecamere agli access point delle porte:
     - Nel proprio dispositivo fare clic sulla voce **Cameras** (Telecamere) per visualizzare l'elenco delle telecamere configurate nel sistema XProtect.
     - Selezionare e trascinare una telecamera sull'access point a cui si desidera associarla.
     - Fare clic su **Close** (Chiudi) per chiudere la finestra di dialogo.

Nota

- Per ulteriori informazioni sull'integrazione del controllo degli accessi in XProtect, vedere *Utilizzo del controllo degli accessi in XProtect Smart Client*.
- Per ulteriori informazioni sulle proprietà del sistema di controllo degli accessi, quali le impostazioni generali, le porte e le telecamere associate, gli eventi di controllo degli accessi e così via, vedere *Proprietà del controllo degli accessi*.

Porte e zone

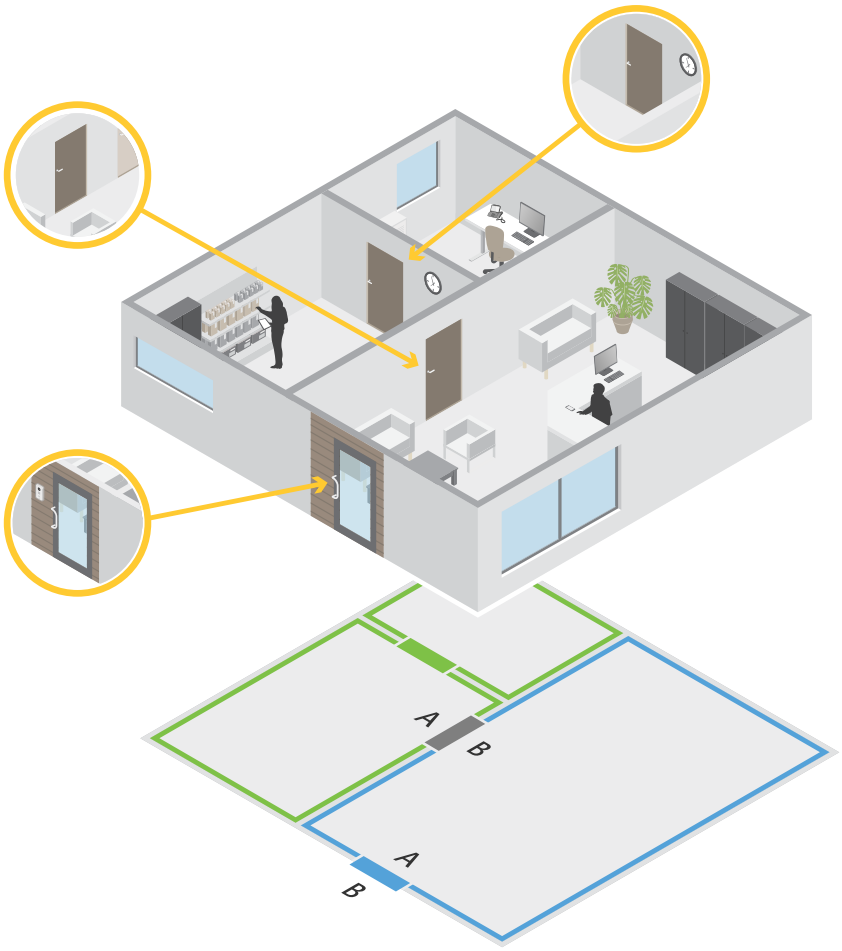
Andare a **Site Navigation** > **AXIS Optimizer** > **Access control** > **Doors and zones** (Navigazione sito, AXIS Optimizer, Controllo degli accessi, Porte e zone) per ottenere una panoramica ed eseguire la configurazione di porte e zone.

Schema dei PIN	Visualizzare lo schema dei pin del controller associato a una porta. Per stampare lo schema dei pin, fare clic su **Print (Stampa)**.
Profilo di identificazione	Cambiare il profilo di identificazione delle porte.
Canale sicuro	Disattivare o attivare OSDP Secure Channel per uno specifico lettore.

Porte	
Nome	Il nome della porta.
Door controller	Il door controller connesso alla porta.
Lato A	La zona in cui si trova il lato A della porta.
Lato B	La zona in cui si trova il lato B della porta.
Profilo di identificazione	Il profilo di identificazione applicato alla porta.
Formati tessera e PIN	Mostra il tipo di formato tessera o la lunghezza del PIN.

Stato	Lo stato della porta. • **Online:** La porta è online e funziona correttamente. • **Reader offline (Lettore offline):** Il lettore nella configurazione della porta è offline. • **Reader error (Errore lettore):** Il lettore nella configurazione della porta non supporta il canale sicuro oppure il canale sicuro non è attivato per il lettore.
Zone	
Nome	Il nome della zona.
Numero di porte	Numero di porte incluse nella zona.

Esempio di porte e zone



- Esistono due zone: zona verde e zona blu.
- Sono disponibili tre porte: porta verde, porta blu e porta marrone.
- La porta verde è una porta interna alla zona verde.
- La porta blu è una porta perimetrale solo per la zona blu.
- La porta a chiave è una porta perimetrale sia per la zona verde che per quella blu.

Aggiunta di una porta

Nota

- Si può configurare un door controller con una porta con due serrature o due porte con una serratura ciascuna.
- Se un door controller non ha porte e si sta utilizzando una nuova versione di AXIS Optimizer con software precedente sul door controller, il sistema impedirà di aggiungere una porta. Ciononostante, se c'è già una porta disponibile, il sistema consente nuove porte sui controller di sistema con software precedente.

Creare una nuova configurazione porta per aggiungere una porta:

1. Andare a **Site Navigation** > **AXIS Optimizer** > **Access control** > **Doors and zones** (Navigazione sito, AXIS Optimizer, Controllo degli accessi, Porte e zone).
2. Fare clic su **Add door (Aggiungi porta)**.
3. Immettere il nome della porta.
4. Nel menu a discesa **Controller (Dispositivo di controllo)**, selezionare un door controller. Il controller è disattivato (grigio) quando non si può aggiungere un'altra porta, quando è offline o HTTPS non è attivo.
5. Nel menu a discesa **Door type (Tipo di porta)**, selezionare il tipo di porta che si vuole creare.
6. Fare clic su **Next (Avanti)** per passare alla pagina di configurazione della porta.
7. Selezionare una porta relè dal menu a discesa **Primary lock (Blocco principale)**.
8. Per configurare due blocchi sulla porta, selezionare una porta relè dal menu a discesa **Secondary lock (Blocco secondario)**.
9. Selezionare un profilo di identificazione. Vedere *Profili di identificazione, on page 86*.
10. Configurare le impostazioni della porta. Vedere *Impostazioni della porta, on page 75*.
11. Impostare una porta di monitoraggio. Vedere *Aggiungere una porta di monitoraggio, on page 78*.
12. Fare clic su **Save (Salva)**.

Copiare una configurazione di porta esistente per aggiungere una porta:

1. Andare a **Site Navigation** > **AXIS Optimizer** > **Access control** > **Doors and zones** (Navigazione sito, AXIS Optimizer, Controllo degli accessi, Porte e zone).
2. Fare clic su **Add door (Aggiungi porta)**.
3. Immettere il nome della porta.
4. Nel menu a discesa **Controller (Dispositivo di controllo)**, selezionare un door controller.
5. Fare clic su **Next (Avanti)**.
6. Nel menu a discesa **Copy configuration (Copia configurazione)** selezionare una configurazione di porta esistente. Mostra le porte connesse mentre il controller risulta disattivato (grigio) se è stato configurato con due porte o una porta con due serrature.
7. Modificare le impostazioni se si desidera.
8. Fare clic su **Save (Salva)**.

Per modificare una porta:

1. Andare a **Site Navigation** > **AXIS Optimizer**> **Access control** > **Doors and zones** > **Doors** (Navigazione sito, AXIS Optimizer, Controllo degli accessi, Porte e zone, Porte).
2. Selezionare una porta dall'elenco.
3. Fare clic su **Edit (Modifica)**.
4. Modificare le impostazioni e fare clic su **Save (Salva)**.

Per rimuovere una porta:

1. Andare a **Site Navigation** > **AXIS Optimizer**> **Access control** > **Doors and zones** > **Doors** (Navigazione sito, AXIS Optimizer, Controllo degli accessi, Porte e zone, Porte).
2. Selezionare una porta dall'elenco.
3. Fare clic su **Remove (Rimuovi)**.
4. Fare clic su **Sì**.

Per integrare l'aggiornamento nel VMS ogni volta che si aggiunge, rimuove o si modifica il nome di una porta:

1. Andare a **Site Navigation** (navigazione sito) > **Access control** (controllo degli accessi) e fare clic su Access Control integration (Integrazione del controllo degli accessi).
2. Fare clic su **Refresh Configuration (Aggiorna configurazione)** nella scheda **General settings (Impostazioni generali)**.

Impostazioni della porta

1. Andare a **Site Navigation** > **AXIS Optimizer** > **Access control** > **Doors and zones** (Navigazione sito, AXIS Optimizer, Controllo degli accessi, Porte e zone).
2. Selezionare la porta che si desidera modificare.
3. Fare clic su **Edit (Modifica)**.

Tempo di accesso (sec)	Impostare il numero di secondi per cui la porta rimane sbloccata dopo aver consentito l'accesso. La porta rimane sbloccata fino all'apertura della porta o alla fine del tempo impostato. La porta si blocca quando si chiude anche se rimane del tempo di accesso a disposizione.
Open-too-long time (sec) (Tempo di apertura eccessivo (sec))	Valido solo se si è configurato un monitor porta. Impostare il numero di secondi durante i quali la porta resta aperta. Se la porta è aperta al termine del tempo impostato, si attiva l'allarme tempo di apertura eccessivo. Impostare una regola di azione per configurare l'azione che verrà attivata dall'evento porta aperta troppo a lungo.
Tempo di accesso lungo (sec)	Impostare il numero di secondi per cui la porta rimane sbloccata dopo aver consentito l'accesso. Il tempo di accesso lungo sovrascrive il tempo di accesso per i titolari della tessera che ha questa impostazione attivata.
Long open-too-long time (sec) (Tempo di apertura eccessivo lungo (sec))	Valido solo se si è configurato un monitor porta. Impostare il numero di secondi durante i quali la porta resta aperta. Se la porta è aperta al termine del tempo impostato, si attiva l'evento tempo di apertura eccessivo. Il tempo di apertura eccessivo lungo sovrascrive il tempo di apertura eccessivo già impostato per i titolari della tessera se si attiva l'impostazione **Long access time (Tempo di accesso lungo)**.

Ritardo ripetizione blocco (ms)	Impostare il tempo di sblocco della porta in millisecondi dopo l'apertura o la chiusura.
Ripetizione blocco	• **After opening (dopo apertura):** valido solo se è stato aggiunto un monitor porta. • **After closing (dopo chiusura):** valido solo se è stato aggiunto un monitor porta.

Livello di sicurezza porta

È possibile aggiungere le seguenti funzionalità di sicurezza alla porta:

Regola due persone – La regola per due persone richiede a due persone di utilizzare una credenziale valida per ottenere l'accesso.

Doppia passata – La doppia passata permette al titolare tessera di sovrascrivere lo stato corrente di una porta. Ad esempio, può usarla per il blocco o lo sblocco di una porta fuori della pianificazione normale, il che è più comodo che accedere al sistema per sbloccare la porta. Il doppio scorrimento non influisce su una pianificazione esistente. Ad esempio, se è pianificato il blocco di una porta all'ora di chiusura e un dipendente esce per la pausa pranzo, la porta si blocca comunque in base alla pianificazione.

È possibile configurare il livello di sicurezza quando si aggiunge una nuova porta o per una porta esistente.

Per aggiungere una **regola due persone** a una porta esistente:

1. Andare a **Site Navigation** > **AXIS Optimizer** > **Access control** > **Doors and zones** (Navigazione sito, AXIS Optimizer, Controllo degli accessi, Porte e zone).
2. Selezionare la porta per la quale si desidera configurare un livello di sicurezza.
3. Fare clic su **Edit (Modifica)**.
4. Fare clic su **Security level (Livello di sicurezza)**.
5. Attiva una **regola due persone**.
6. fare clic su **Applica**;

Regola due persone	
Side A (Lato A) e **Side B (Lato B)**	Selezionare i lati della porta su cui usare la regola.
Pianificazioni	Selezionare quando è attiva la regola.
Timeout (secondi)	Timeout è il tempo massimo consentito tra i passaggi di tessera o altri tipi di credenziali valide.

Per aggiungere una **Doppia passata** a una porta esistente:

1. Andare a **Site Navigation** > **AXIS Optimizer** > **Access control** > **Doors and zones** (Navigazione sito, AXIS Optimizer, Controllo degli accessi, Porte e zone).
2. Selezionare la porta per la quale si desidera configurare un livello di sicurezza.
3. Fare clic su **Edit (Modifica)**.
4. Fare clic su **Security level (Livello di sicurezza)**.
5. Attivare la **Doppia passata**.
6. fare clic su **Applica**;
7. Applicare la **Double-swipe (Doppia passata)** a un titolare della tessera.
   7.1. Andare in **Cardholder management (Gestione titolari tessere)**.
   7.2. Selezionare il titolare tessera da modificare e fare clic su **Edit (Modifica)**.

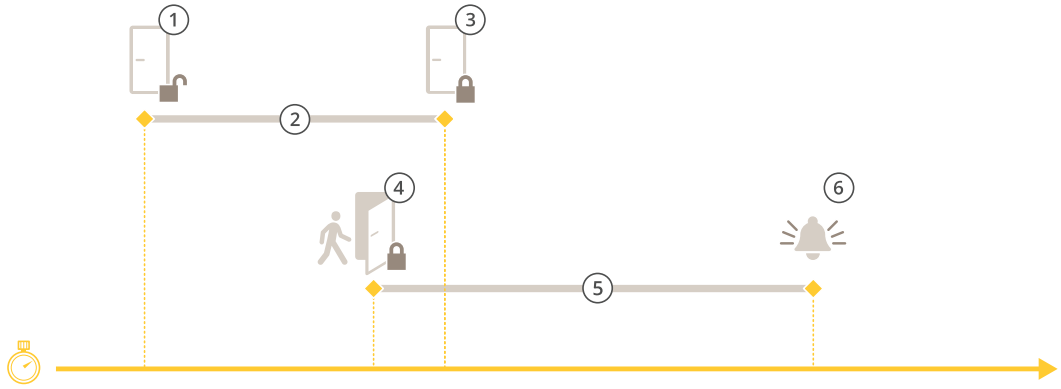
7.3. fare clic su **Avanzate**;

7.4. Selezionare **Allow double-swipe (Consenti doppia passata)**.

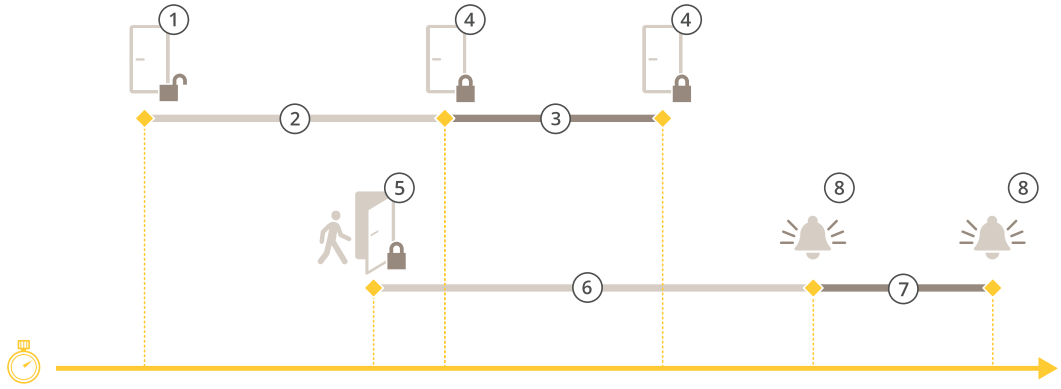
7.5. Fare clic su **Save (Salva)**.

Doppia passata	
Timeout (secondi)	Timeout è il tempo massimo consentito tra i passaggi di tessera o altri tipi di credenziali valide.

Opzioni relative all'orario



1 Accesso consentito: la serratura si sblocca
2 Tempo di accesso
3 Nessuna azione compiuta: la serratura si blocca
4 Azione compiuta (porta aperta): la serratura si blocca o rimane sbloccata finché non si chiude la porta
5 Tempo di apertura eccessivo
6 Scatta l'allarme tempo di apertura eccessivo



1 Accesso consentito: la serratura si sblocca
2 Tempo di accesso
3 2+3: Tempo di accesso lungo
4 Nessuna azione compiuta: la serratura si blocca
5 Azione compiuta (porta aperta): la serratura si blocca o rimane sbloccata finché non si chiude la porta
6 Tempo di apertura eccessivo
7 6+7: Tempo di apertura eccessivo lungo:
8 Scatta l'allarme tempo di apertura eccessivo

Aggiungi un monitor porta

Un monitor porta è uno switch di posizione della porta che controlla lo stato fisico di una porta. È possibile aggiungere un monitor porta alla porta e configurare la modalità di collegamento del monitor porta.

1. Andare alla pagina di configurazione della porta. Vedere *Aggiunta di una porta, on page 74*
2. In **Sensors (Sensori)**, fare clic su **Add (Aggiungi)**.
3. Selezionare **Door position sensor (Sensore posizione porta)**.
4. Selezionare la porta I/O a cui si desidera collegare il monitor porta.
5. In **Door open if (Porta aperta se)**, selezionare la modalità di collegamento dei circuiti del monitor della porta.
6. Per ignorare le modifiche di stato dell'input digitale prima che entri in un nuovo stato stabile, imposta un **Debounce time (Tempo debounce)**.
7. Per attivare un evento quando avviene un'interruzione della connessione tra il door controller e il monitor porta, attivare il **Supervised input (Input supervisionato)**. Vedere *Ingressi con supervisione, on page 82*.

Porta aperta se	
Circuito aperto	Il circuito del monitor porta è normalmente chiuso. Quando il circuito è aperto, il monitor porta invia un segnale di porta aperta. Quando il circuito è chiuso, il monitor porte invia un segnale di porta chiusa.
Circuito chiuso	Il circuito del monitor porta è normalmente aperto. Quando il circuito è chiuso, il monitor porta invia un segnale di porta aperta. Quando il circuito è aperto, il monitor porta invia un segnale di porta chiusa.

Aggiungere una porta di monitoraggio

Una porta di monitoraggio è un tipo di porta che può mostrare se è aperta o chiusa. Ad esempio, è possibile utilizzarla per una porta antincendio che non richiede una serratura, ma è necessario sapere se è aperta.

Una porta di monitoraggio è diversa da una porta normale dotata di monitor. Una porta normale con monitor supporta serrature e lettori, ma richiede un door controller. Una porta di monitoraggio supporta un sensore di posizione delle porte ma richiede solo un modulo relè I/O di rete collegato a un door controller. È possibile collegare fino a cinque sensori di posizione delle porte a un modulo relè I/O di rete.

Nota

Una porta di monitoraggio richiede un AXIS A9210 Network I/O Relay Module con il software più recente, inclusa l'applicazione AXIS Monitoring Door ACAP.

Per impostare una porta di monitoraggio:

1. Installare AXIS A9210 ed eseguire l'aggiornamento con l'ultima versione di AXIS OS.
2. Installare i sensori di posizione delle porte.
3. Nel VMS, andare a **Site Navigation** > **AXIS Optimizer** > **Access control** > **Doors and zones** (Navigazione sito, AXIS Optimizer, Controllo degli accessi, Porte e zone).
4. Fare clic su **Add door (Aggiungi porta)**.
5. Inserire un nome.
6. In **Type (Tipo)**, selezionare **Monitoring door (Porta di monitoraggio)**.
7. In **Device (Dispositivo)**, selezionare il modulo relè I/O di rete.
8. Fare clic su **Next (Avanti)**.

9. In **Sensors (Sensori)**, fare clic su **+ Add (+ Aggiungi)** e selezionare **Door position sensor (Sensore di posizione delle porte)**.
10. Selezionare la porta I/O connessa al sensore di posizione delle porte.
11. Fare clic su **Aggiungi**.

Aggiungi un lettore

Si può eseguire la configurazione di un door controller in modo da usare due lettori cablati. Scegliere di aggiungere un lettore su un lato o su entrambi i lati di una porta.

Se si applica un'impostazione personalizzata dei formati tessera o della lunghezza del PIN a un lettore, sarà visibile in **Card formats (Formati tessera)** in **Configuration > Access control > Doors and zones (Configurazione > Controllo degli accessi > Porte e zone)**. Vedere *Porte e zone, on page 72*.

1. Andare alla pagina di configurazione della porta. Vedere *Aggiunta di una porta, on page 74*.
2. Sotto un lato della porta, fare clic su **Add (Aggiungi)**.
3. Selezionare **Card reader (Lettore di schede)**.
4. Selezionare **Reader type (Tipo di lettore)**.
5. Per usare una configurazione personalizzata della lunghezza del PIN per questo lettore.
   5.1. fare clic su **Avanzate**;
   5.2. Attivare **Custom PIN length (Lunghezza PIN personalizzata)**.
   5.3. Imposta la **Min PIN length (Lunghezza PIN minima)**, **Max PIN length (Lunghezza PIN massima)** e **End of PIN character (Fine del carattere PIN)**.
6. Per usare un formato tessera personalizzato per questo lettore.
   6.1. fare clic su **Avanzate**;
   6.2. Attivare i **Custom card formats (Formati tessera personalizzati)**.
   6.3. Selezionare i formati tessera che si desidera utilizzare per il lettore. Se è già in uso un formato tessera con la stessa lunghezza in bit, è necessario disattivarlo prima. Un'icona di avviso appare nel client quando la configurazione del formato scheda differisce dall'impostazione del sistema configurata.
7. Fare clic su **Aggiungi**.
8. Per l'aggiunta di un lettore all'altro lato della porta, ripetere questa procedura.

Tipo di lettore	
OSDP RS485 half-duplex	Per i lettori RS485, selezionare **OSDP RS485 half-duplex** e una porta per il lettore.
Wiegand	Per i lettori che usano i protocolli Wiegand, selezionare **Wiegand** e una porta per il lettore.

Wiegand	
Comando LED	Selezionare **Single wire (Cavo singolo)** o **Dual wire (R/G) (Cavo doppio (R/G))**. I lettori con controllo LED doppio utilizzano cavi diversi per i LED rossi e verdi.
Avviso manomissione	Selezionare quando l'input manomissione del lettore è attivo. • **Open circuit (Circuito aperto)**: Il lettore invia il segnale di manomissione alla porta quando il circuito è aperto.

	• **Closed circuit (Circuito chiuso)**: Il lettore invia il segnale di manomissione alla porta quando il circuito è chiuso.
Tamper debounce time (Tempo debounce manomissione)	Per ignorare le variazioni di stato dell'input manomissione del lettore prima che entri in un nuovo stato stabile, impostare un **Tamper debounce time (Tempo debounce manomissione)**.
Input supervisionato	Attivare per il trigger di un evento quando c'è un'interruzione della connessione tra il door controller e il lettore. Vedere *Ingressi con supervisione, on page 82*.

Aggiungi un dispositivo REX

È possibile scegliere di aggiungere una richiesta per uscire da un dispositivo (REX) su un lato o su entrambi i lati della porta. Un dispositivo REX può essere un sensore PIR, un pulsante REX o un maniglione.

1. Andare alla pagina di configurazione della porta. Vedere *Aggiunta di una porta, on page 74*.
2. Sotto un lato della porta, fare clic su **Add (Aggiungi)**.
3. Selezionare **REX device (Dispositivo REX)**.
4. Selezionare la porta I/O a cui si desidera collegare il dispositivo REX. Se è disponibile una sola porta, verrà selezionata automaticamente.
5. Selezionare quale **Action (Azione)** attivare quando la porta riceve il segnale REX.
6. Selezionare la connessione circuiti del monitor della porta in **REX active (REX attivo)**.
7. Per ignorare le modifiche allo stato dell'ingresso digitale prima che entri in un nuovo stato stabile, configurare l'opzione **Debounce time (ms) (Tempo debounce (ms))**.
8. Per attivare un evento quando avviene un'interruzione della connessione tra il door controller e il dispositivo REX, attivare **Supervised input (Input supervisionato)**. Vedere *Ingressi con supervisione, on page 82*.

Azione	
Sblocca porta	Sceglierlo per sbloccare la porta nel momento in cui riceve il segnale REX.
Nessuna	Selezionare questa opzione se non si desidera attivare alcuna azione quando la porta riceve il segnale REX.

REX attivo	
Circuito aperto	Selezionare questa opzione se il circuito REX è normalmente chiuso. Il dispositivo REX invia il segnale quando il circuito è aperto.
Circuito chiuso	Selezionare questa opzione se il circuito REX è normalmente aperto. Il dispositivo REX invia il segnale quando il circuito è chiuso.

Aggiunta di una zona

Una zona è un'area fisica specifica con un gruppo di porte. È possibile creare zone e aggiungere porte alle zone. Esistono due tipi di porte:

- **Perimeter door (Porta perimetrale):** I titolari della tessera entrano nella zona o la abbandonano attraverso questa porta.
- **Internal door (Porta interna):** Una porta interna all'interno della zona.

Nota

Una porta perimetrale può appartenere a due zone. Una porta interna può appartenere a una sola zona.

1. Andare a **Site Navigation** > **AXIS Optimizer** > **Access control** > **Doors and zones** > **Zones** (Navigazione sito, AXIS Optimizer, Controllo degli accessi, Porte e zone, Zone).
2. Fare clic su **Add zone (Aggiungi zona)**.
3. Immettere il nome di una zona.
4. Fare clic su **Add door (Aggiungi porta)**.
5. Selezionare le porte che si vuole aggiungere alla zona e fare clic su **Add (Aggiungi)**.
6. La porta è impostata come porta perimetrale per impostazione predefinita. Per modificarla, selezionare **Internal door (Porta interna)** dal menu a discesa.
7. Per impostazione predefinita, una porta del perimetro impiega il lato della porta A come ingresso per la zona. Per modificare questa impostazione, selezionare **Leave (Abbandona)** dal menu a discesa.
8. Per rimuovere una porta dalla zona, selezionarla e fare clic su **Remove (Rimuovi)**.
9. Fare clic su **Save (Salva)**.

Per modificare una zona:

1. Andare a **Site Navigation** > **AXIS Optimizer** > **Access control** > **Doors and zones** > **Zones** (Navigazione sito, AXIS Optimizer, Controllo degli accessi, Porte e zone, Zone).
2. Selezionare una zona dall'elenco.
3. Fare clic su **Edit (Modifica)**.
4. Modificare le impostazioni e fare clic su **Save (Salva)**.

Per rimuovere una zona:

1. Andare a **Site Navigation** > **AXIS Optimizer** > **Access control** > **Doors and zones** > **Zones** (Navigazione sito, AXIS Optimizer, Controllo degli accessi, Porte e zone, Zone).
2. Selezionare una zona dall'elenco.
3. Fare clic su **Remove (Rimuovi)**.
4. Fare clic su **Sì**.

Livello di sicurezza zona

Si può aggiungere la funzionalità di sicurezza che segue ad una zona:

Anti-passback – Fa sì che le persone non possano impiegare le stesse credenziali di qualcuno entrato in un'area prima di loro. Impone l'uscita dall'area prima che si possano usare di nuovo le proprie credenziali.

Nota

- Con l'anti-passback, tutte le porte nella zona devono avere sensori di posizione della porta in modo che il sistema possa registrare che un utente ha aperto la porta dopo aver passato la carta.
- Se un door controller passa offline, l'anti-passback funziona finché tutte le porte nella zona appartengono allo stesso door controller. Tuttavia, se le porte nella zona appartengono a diversi door controller che passano offline, l'anti-passback smette di funzionare.

Si può eseguire la configurazione del livello di sicurezza quando si aggiunge una nuova area o si può fare in una zona esistente. Per eseguire l'aggiunta di un livello di sicurezza a una zona esistente:

1. Andare a **Site Navigation** > **AXIS Optimizer** > **Access control** > **Doors and zones** (Navigazione sito, AXIS Optimizer, Controllo degli accessi, Porte e zone).
2. Eseguire la selezione della zona per la quale si desidera configurare un livello di sicurezza.
3. Fare clic su **Edit (Modifica)**.
4. Fare clic su **Security level (Livello di sicurezza)**.
5. Eseguire l'attivazione delle funzioni di sicurezza che si vogliono aggiungere alla porta.
6. fare clic su **Applica**;

Anti-passback	
Log violation only (Soft) (Solo log violazione (tollerante))	Usare se si vuole permettere a una seconda persona di entrare dalla porta usando le stesse credenziali della prima persona. Questa opzione risulta unicamente in un allarme di sistema.
Deny access (Hard) (Nega accesso (rigido))	Da usare se si vuole evitare che il secondo utente entri dalla porta nel caso usi le stesse credenziali della prima persona. Anche questa opzione risulta in un allarme di sistema.
Timeout (secondi)	Il tempo che deve trascorrere prima che il sistema consenta all'utente di entrare di nuovo. Immettere 0 se non si vuole un timeout, il che significa che la zona ha l'anti-passback finché l'utente non lascia la zona. Usare unicamente il timeout **0** con **Deny access (Hard) (Nega accesso (rigido))** se tutte le porte nella zona hanno lettori su entrambi i lati.

Ingressi con supervisione

Gli ingressi supervisionati sono in grado di attivare un evento se si verifica un'interruzione della connessione a un door controller.

- Collegamento tra Door controller e Door monitor. Vedere *Aggiungi un monitor porta, on page 78*.
- Collegamento tra Door controller e lettore basato su protocolli Wiegand. Vedi *Aggiungi un lettore, on page 79*.
- Collegamento tra Door controller e dispositivo REX. Vedere *Aggiungi un dispositivo REX, on page 80*.

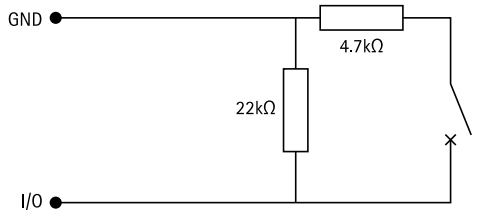
Per utilizzare gli input supervisionati:

1. Installare resistori terminali il più vicino possibile al dispositivo periferico secondo lo schema delle connessioni.
2. Andare alla pagina di configurazione di un lettore, di un monitor porta o di un dispositivo REX, attivare **Supervised input (Input supervisionato)**.
3. Se è stato seguito lo schema di prima connessione parallela, selezionare **Parallel first connection with a 22 KΩ parallel resistor and a 4.7 KΩ serial resistor (Prima connessione parallela con un resistore parallelo da 22 KΩ e un resistore seriale da 4,7 KΩ)**.
4. Se è stato seguito lo schema di prima connessione in serie, selezionare **Serial first connection (Prima connessione in serie)** e selezionare un valore dei resistori dal menu a discesa **Resistor values (Valori resistore)**.

Schemi delle connessioni

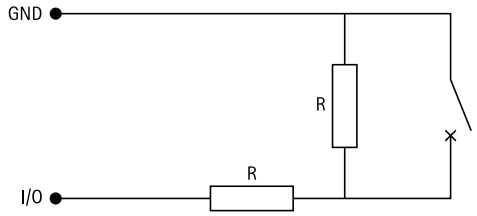
Prima connessione parallela

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



Prima connessione in serie

I valori dei resistori devono essere uguali nell'intervallo compreso tra 1 e 10 kΩ.



Azioni manuali

È possibile eseguire le seguenti azioni manuali su porte e zone:

Ripristina – Ritorna alle regole di sistema configurate.

Consenti accesso – Sblocca una porta o una zona per 7 secondi e poi la blocca di nuovo.

Sblocca – Mantiene la porta aperta fino al reset.

Blocco – Mantiene chiusa la porta finché il sistema non concede l'accesso a un titolare di tessera.

Chiusura totale – Nessuno può entrare o uscire finché non si resetta o si sblocca.

Per eseguire un'azione manuale:

1. Andare a **Site Navigation** > **AXIS Optimizer** > **Access control** > **Doors and zones** (Navigazione sito, AXIS Optimizer, Controllo degli accessi, Porte e zone).
2. Selezionare la porta o la zona su cui si desidera eseguire un'azione manuale.
3. Fare clic su una qualsiasi delle azioni manuali.

Nota

La porta rimarrà in modalità di funzionamento manuale, nota anche come modalità di comando manuale, fino a quando non verrà riportata alla sua pianificazione normale.

Formati tessera e PIN

Un formato tessera definisce la modalità in cui una tessera memorizza i dati. Si tratta di una tabella di conversione tra i dati in ingresso e i dati convalidati nel sistema. Ciascun formato di tessera dispone di un set di regole diverso riguardante il modo di organizzare le informazioni memorizzate. Definendo un formato tessera si indica al sistema come interpretare le informazioni che il dispositivo di controllo ottiene dal lettore di tessere.

Esistono formati di tessera comunemente usati predefiniti che è possibile utilizzare così come sono o modificare in base alle necessità. È possibile inoltre creare formati tessera personalizzati.

Andare a **Site Navigation** > **AXIS Optimizer** > **Access control** > **Card formats and PIN** (Navigazione sito, AXIS Optimizer, Controllo degli accessi, Formati tessera e PIN) per la creazione, la modifica o l'attivazione dei formati tessera. È inoltre possibile configurare il PIN.

I formati della tessera personalizzati possono contenere i seguenti campi dati utilizzati per la convalida delle credenziali.

Numero tessera – Un sottoinsieme dei dati binari delle credenziali codificati come numeri decimali o esadecimali. Usare il codice carta per identificare un titolare o una tessera specifica.

Codice struttura – Un sottoinsieme dei dati binari delle credenziali codificati come numeri decimali o esadecimali. Usare il codice struttura per identificare un sito o un cliente finale specifico.

Per creare un formato tessera:

1. Andare a **Site Navigation** > **AXIS Optimizer** > **Access control** > **Card formats and PIN** (Navigazione sito, AXIS Optimizer, Controllo degli accessi, Formati tessera e PIN).
2. Fare clic su **Add card format (Aggiungi formato scheda)**.
3. Inserire un nome per il formato tessera.
4. Digitare una lunghezza in bit tra 1 e 256 nel campo **Bit length (Lunghezza in bit)**.
5. Selezionare **Invert bit order (Inverti ordine dei bit)** se si desidera invertire l'ordine dei bit dei dati ricevuti dal lettore di tessere.
6. Selezionare **Invert byte order (Inverti ordine dei byte)** se si desidera invertire l'ordine dei byte dei dati ricevuti dal lettore di tessere. Questa opzione è disponibile solo quando si specifica una lunghezza in bit che si può dividere per otto.
7. Selezionare e configurare i campi dati in modo che siano attivi nel formato tessera. Il **Card number (Codice carta)** o il **Facility code (Codice struttura)**.
8. Fare clic su **OK**.
9. Per attivare il formato della tessera, selezionare la casella di controllo davanti al nome del formato della tessera.

Nota

- Non è possibile che due formati scheda con la stessa lunghezza in bit possano essere attivi contemporaneamente. Ad esempio, se sono stati definiti due formati di tessera a 32 bit, solo uno può essere attivo. Eseguire la disattivazione del formato tessera per attivare l'altro.
- È possibile attivare e disattivare i formati scheda solo se il door controller è stato configurato con almeno un lettore.

ⓘ	Fare clic su ⓘ per vedere un esempio di output dopo l'inversione dell'ordine dei bit.
Intervallo	Impostare l'intervallo bit dei dati per il campo dati. L'intervallo deve essere compreso tra i valori specificati per **Bit length (Lunghezza in bit)**.
Formato di output	Selezionare il formato di output dei dati per il campo dati. **Decimal (Decimale)**: noto anche come sistema numerico posizionale in base 10, è composto dai numeri compresi tra 0 e 9. **Hexadecimal (Esadecimale)**: noto anche come sistema numerico posizionale in base 16, consiste di 16 simboli unici: i numeri 0-9 e le lettere a-f.
Ordine bit di subrange	Selezionare l'ordine dei bit. **Little endian**: il primo bit è il più piccolo (meno significativo). **Big endian**: il primo bit è il più grande (più significativo).

Per modificare il formato di una tessera:

1. Andare a **Site Navigation** > **AXIS Optimizer** > **Access control** > **Card formats and PIN** (Navigazione sito, AXIS Optimizer, Controllo degli accessi, Formati tessera e PIN).
2. Selezionare un formato tessera e fare clic su .
3. Se cambia un formato tessera predefinito, si può modificare solo **Invert bit order (Inverti ordine dei bit)** e **Invert byte order (Inverti ordine dei byte)**.
4. Fare clic su **OK**.

È possibile rimuovere solo i formati tessera personalizzati. Per rimuovere un formato tessera personalizzato:

1. Andare a **Site Navigation** > **AXIS Optimizer** > **Access control** > **Card formats and PIN** (Navigazione sito, AXIS Optimizer, Controllo degli accessi, Formati tessera e PIN).
2. Selezionare un formato tessera personalizzato, fare clic su e **Yes (Sì)**.

Per il reset di un formato tessera predefinito:

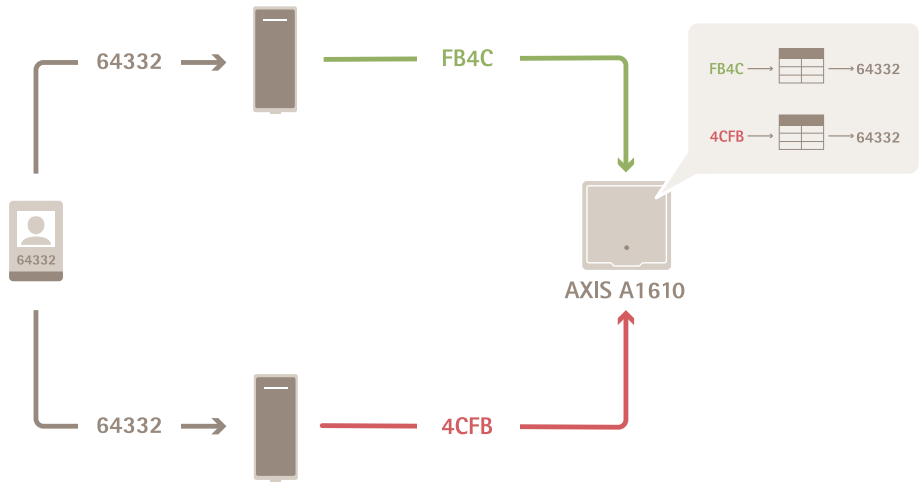
1. Andare a **Site Navigation** > **AXIS Optimizer** > **Access control** > **Card formats and PIN** (Navigazione sito, AXIS Optimizer, Controllo degli accessi, Formati tessera e PIN).
2. Fare clic su per ripristinare un formato tessera alla mappa dei campi predefinita.

Per configurare la lunghezza PIN:

1. Andare a **Site Navigation** > **AXIS Optimizer** > **Access control** > **Card formats and PIN** (Navigazione sito, AXIS Optimizer, Controllo degli accessi, Formati tessera e PIN).
2. In **PIN configuration (Configurazione PIN)** fare clic su .
3. Specificare **Min PIN length (Lunghezza PIN minima)**, **Max PIN length (Lunghezza PIN massima)** e **End of PIN character (Fine del carattere PIN)**.
4. Fare clic su **OK**.

Impostazioni formato tessera

Panoramica



- Il codice carta in decimale è `64332`.
- Un lettore trasferisce il codice carta al numero esadecimale `FB4C`. L'altro lettore la trasferisce al numero esadecimale `4CFB`.

- AXIS A1610 Network Door Controller riceve `FB4C` e lo trasferisce al numero decimale `64332` in base alle impostazioni del formato tessera nel lettore.
- AXIS A1610 Network Door Controller riceve `4CFB` e lo cambia in `FB4C` invertendo l'ordine dei byte e lo trasferisce al numero decimale `64332` in base alle impostazioni del formato tessera nel lettore.

Inverti ordine bit

Dopo aver capovolto l'ordine dei bit, i dati della scheda ricevuti dal lettore vengono letti da destra a sinistra bit per bit.



Inverti ordine byte

Un gruppo di otto bit è un byte. Dopo aver capovolto l'ordine dei byte, i dati della scheda ricevuti dal lettore vengono letti da destra a sinistra byte per byte.



Formato tessera Wiegand standard a 26 bit



1 *Parità principale*
2 *Codice struttura*
3 *Numero tessera*
4 *Parità finale*

Profili di identificazione

Un profilo di identificazione è una combinazione di tipi di identificazione e pianificazioni. Si può applicare un profilo di identificazione a una o molteplici porte per impostare come e quando un titolare tessera è in grado di accedere a una porta.

I tipi di identificazione sono vettori di credenziali necessarie per l'accesso a una porta. I tipi di identificazione più diffusi sono i token, i numeri di identificazione personale (PIN), le impronte digitali, le mappe facciali e i dispositivi REX. È possibile che un tipo di identificazione contenga uno o molteplici tipi di informazioni.

Le pianificazioni, note anche come **Profili temporali**, sono generate nel Management Client. Per impostare i profili temporali, consultare *Profili temporali (spiegazione)*.

Tipi di identificazione supportati: Tessera, PIN e REX.

Andare a **Site Navigation** > **AXIS Optimizer** > **Access control** > **Identification profiles** (Navigazione sito, AXIS Optimizer, Controllo degli accessi, Profili di identificazione).

Sono disponibili cinque profili di identificazione predefiniti da utilizzare così come sono o modificare secondo necessità.

Badge – I titolari della tessera devono strisciare la tessera per accedere alla porta.

Tessera e PIN – I titolari della tessera devono strisciare la tessera e inserire il PIN per accedere alla porta.

PIN – I titolari della tessera devono inserire il PIN per accedere alla porta.

Tessera o PIN – I titolari della tessera devono strisciare la tessera o inserire il PIN per accedere alla porta.

Targa – I titolari della tessera devono dirigersi verso la telecamera a bordo di un veicolo con targa omologata.

Per creare profilo di identificazione:

1. Andare a **Site Navigation** > **AXIS Optimizer** > **Access control** > **Identification profiles** (Navigazione sito, AXIS Optimizer, Controllo degli accessi, Profili di identificazione).
2. Fare clic su **Create identification profile (Creare profilo di identificazione)**.
3. Inserire un nome per il profilo di identificazione.
4. Selezionare **Include facility code for card validation (Includi codice struttura per convalida tessera)** per utilizzare il codice struttura come uno dei campi di convalida delle credenziali. Questo campo è disponibile solo se si attiva **Facility code (Codice struttura)** in **Access management > Settings (Gestione degli accessi > Impostazioni)**.
5. Eseguire la configurazione del profilo di identificazione per un lato della porta.
6. Sull'altro lato della porta, ripetere i passaggi precedenti.
7. Fare clic su **OK**.

Per modificare un profilo di identificazione:

1. Andare a **Site Navigation** > **AXIS Optimizer** > **Access control** > **Identification profiles** (Navigazione sito, AXIS Optimizer, Controllo degli accessi, Profili di identificazione).
2. Selezionare un profilo di identificazione e fare clic su .
3. Per cambiare il nome del profilo di identificazione, inserire un nuovo nome.
4. Eseguire le modifiche per il lato della porta.
5. Per modificare il profilo di identificazione dall'altro lato della porta, ripetere i passaggi precedenti.
6. Fare clic su **OK**.

Per rimuovere profilo di identificazione:

1. Andare a **Site Navigation** > **AXIS Optimizer** > **Access control** > **Identification profiles** (Navigazione sito, AXIS Optimizer, Controllo degli accessi, Profili di identificazione).
2. Selezionare un profilo di identificazione e fare clic su .
3. Se il profilo di identificazione è usato su una porta, selezionare un altro profilo di identificazione per la porta.
4. Fare clic su **OK**.

Modifica profilo di identificazione	
×	Per rimuovere un tipo di identificazione e la pianificazione correlata.
Tipo di identificazione	Per modificare un tipo di identificazione, selezionare uno o più tipi dal menu a discesa **Identification type (Tipo di identificazione)**.

Pianificazione	Per modificare una pianificazione, selezionare una o più pianificazioni dal menu a discesa **Schedule (Pianificazione)**.
+ **Aggiungi**	Aggiungere un tipo di identificazione e la pianificazione correlata, fare clic su **Add (Aggiungi)** e impostare i tipi di identificazione e le pianificazioni.

Comunicazione crittografata

Canale sicuro OSDP

Secure Entry supporta il canale sicuro OSDP (Open Supervised Device Protocol) per l'attivazione della crittografia della linea tra il dispositivo di controllo e i lettori Axis.

Per attivare il canale sicuro OSDP per un intero sistema:

1. Andare a **Site Navigation** > **AXIS Optimizer** > **Access control** > **Encrypted communication** (Navigazione sito, AXIS Optimizer, Controllo degli accessi, Comunicazione criptata).
2. Inserire la chiave di crittografia principale e fare clic su **OK**.
3. Attivare **OSDP Secure Channel (Canale sicuro OSDP)**. Solo dopo l'inserimento della chiave di crittografia principale questa opzione diventa disponibile.
4. Per impostazione predefinita, la chiave di crittografia principale genera una chiave del canale sicuro OSDP. Per impostare in modo manuale la chiave del canale sicuro OSDP:
   4.1. In **OSDP Secure Channel (Canale sicuro OSDP)** fare clic su .
   4.2. Deselezionare **Use main encryption key to generate OSDP Secure Channel key (Utilizzare la chiave di crittografia principale per generare la chiave del canale sicuro OSDP)**.
   4.3. Inserire la chiave del canale sicuro OSDP e fare clic su **OK**.

Per l'attivazione o la disattivazione del canale sicuro OSDP per un lettore specifico, vedere *Porte e zone*.

Multi-server BETA

I server secondari collegati possono, con multi server, usare i titolari di tessera e i gruppi di titolari di tessera globali dal server principale.

Nota

- Un sistema è un grado di supportare un massimo di 64 server secondari.
- Il server principale e i server secondari devono essere sulla stessa rete.
- Sui server principali e sui server secondari, assicurati di configurare Windows Firewall per permettere le connessioni TCP in entrata sulla porta Secure Entry. La porta predefinita è 53461.

Flusso di lavoro

1. Configura un server come server secondario e genera il file di configurazione. Vedere *Genera il file di configurazione dal server secondario, on page 89*.
2. Configura un server come server principale e importa il file di configurazione dei server secondari. Vedere *Importa il file di configurazione sul server principale, on page 89*.
3. Configura i titolari di tessera e i gruppi di titolari di tessera globali nel server principale. Vedere *Aggiungi un titolare tessera, on page 90* e *Aggiungi un gruppo, on page 93*.
4. Visualizza e monitora i titolari di tessera e i gruppi di titolari di tessera globali dal server secondario. Consultare *Gestione degli accessi, on page 89*.

Genera il file di configurazione dal server secondario

1. Dal server secondario, andare a **AXIS Optimizer** > **Access control** > **Multi server** (AXIS Optimizer, Controllo degli accessi, Multiserver).
2. Fai clic su **Sub server (Server secondario)**.
3. Fare clic su **Generate (Genera)**. Viene generato un file di configurazione in formato .json.
4. Fai clic su **Download** e scegli una posizione per salvare il file.

Importa il file di configurazione sul server principale

1. Dal server principale, andare a **AXIS Optimizer** > **Access control** > **Multi server** (AXIS Optimizer, Controllo degli accessi, Multiserver).
2. Fai clic su **Main server (Server principale)**.
3. Fare clic su + **Add (Aggiungi)** e andare al file di configurazione generato dal server secondario.
4. Inserisci il nome del server, l'indirizzo IP e il numero di porta del server secondario.
5. Fare clic su **Import (Importa)** per eseguire l'aggiunta del server secondario.
6. Lo stato del server secondario indicato è `Connected`.

Revoca un server secondario

Si può revocare un server secondario solo prima di importarne il file di configurazione su un server principale.

1. Dal server principale, andare a **AXIS Optimizer** > **Access control** > **Multi server** (AXIS Optimizer, Controllo degli accessi, Multiserver).
2. Fai clic su **Sub server (Server secondario)** e fai clic su **Revoke server (Revoca server)**.
   Ora puoi configurare questo server come server principale o secondario.

Rimuovi un server secondario

Dopo l'importazione del file di configurazione di un server secondario, connette il server secondario al server principale.

Per rimuovere un server secondario:

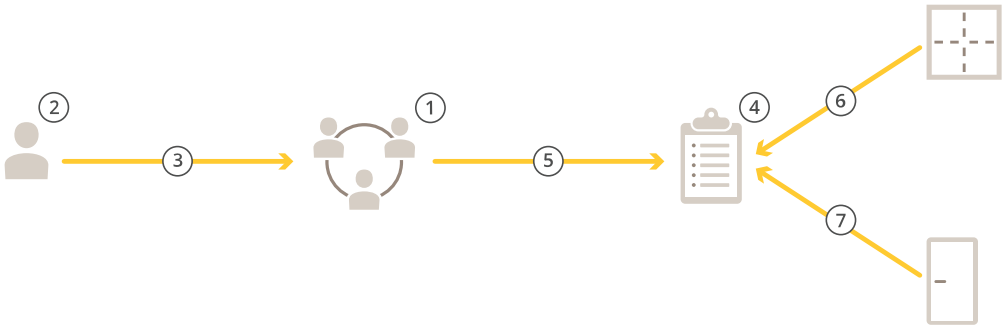
1. Dal server principale:
   1.1. Andare a **Access management** > **Dashboard** (Gestione degli accessi, Dashboard).
   1.2. Trasformare i titolari di tessera e i gruppi globali in titolari di tessera e gruppi locali.
   1.3. Andare a **AXIS Optimizer** > **Access control** > **Multi server** (AXIS Optimizer, Controllo degli accessi, Multiserver).
   1.4. Fare clic su **Main server (Server principale)** per mostrare l'elenco dei server secondari.
   1.5. Seleziona il server secondario e fai clic su **Delete (Elimina)**.
2. Dal server secondario:
   – Andare a **AXIS Optimizer** > **Access control** > **Multi server** (AXIS Optimizer, Controllo degli accessi, Multiserver).
   – Fare clic su **Sub server (Server secondario)** e su **Revoke server (Revoca server)**.

Gestione degli accessi

La scheda Access management (Gestione degli accessi) consente di configurare e gestire gli utenti, i titolari di tessere, i gruppi e le regole di accesso del sistema.

Flusso di lavoro di gestione degli accessi

La struttura di gestione degli accessi è flessibile. Questo consente all'utente di sviluppare un flusso di lavoro più adatto alle proprie esigenze. Di seguito è riportato un esempio di flusso di lavoro:



1. Aggiungi gruppi. Vedere *Aggiungi un gruppo, on page 93*.
2. Aggiungi titolari tessera. Vedere *Aggiungi un titolare tessera, on page 90*.
3. Aggiunta di titolari di tessera ai gruppi.
4. Aggiungi regole di accesso. Vedere *Aggiungi una regola di accesso, on page 94*.
5. Applicazione di gruppi alle regole di accesso.
6. Applicare le zone alle regole di accesso.
7. Applicare le porte alle regole di accesso.

Aggiungi un titolare tessera

Il titolare della tessera è una persona con un ID univoco registrato nel sistema. Eseguire la configurazione di un titolare della tessera con le credenziali che identificano la persona e il modo e il momento in cui lasciarla passare dalle porte.

1. Andare a **Site Navigation** > **AXIS Optimizer** > **Access control** > **Cardholder management** (Navigazione sito, AXIS Optimizer, Controllo degli accessi, Gestione titolare tessera).
2. Andare su **Cardholders (Titolari tessera)** e fare clic su **+ Add (+ Aggiungi)**.
3. Immettere il nome e il cognome del titolare di tessere e fare clic su **Next (Avanti)**.
4. Oppure, fare clic su **Advanced (Avenzate)** e selezionare le opzioni.
5. Aggiungere una credenziale al titolare di tessere. Vedere *Aggiungi credenziali, on page 91*
6. Fare clic su **Save (Salva)**.
7. Aggiunge il titolare di tessere a un gruppo.
   7.1. In **Groups (Gruppi)**, selezionare il gruppo a cui si vuole aggiungere il titolare di tessere e fare clic su **Edit (Modifica)**.
   7.2. Fare clic su **+Add (+Aggiungi)** e selezionare il titolare di tessere che si desidera aggiungere al gruppo. È possibile selezionare più titolari di tessere.
   7.3. Fare clic su **Aggiungi**.
   7.4. Fare clic su **Save (Salva)**.

Avanzata	
Tempo di accesso lungo	Selezionare per consentire al titolare della tessera un tempo di accesso lungo e un tempo di apertura eccessivo lungo quando c'è un monitor porta installato.
Sospendi titolare tessera	Selezionare per eseguire la sospensione del titolare tessera.
Allow double-swipe (Consenti doppia passata)	Selezionare per consentire a un titolare di tessere di ignorare lo stato corrente di una porta. Ad esempio, ha la possibilità di usarla per lo sblocco di una porta al di fuori della pianificazione normale.
Esente da blocco	Selezionare per permettere al titolare della tessera l'accesso durante il blocco.
Exempt from anti-passback (Esente da anti-passback)	Selezionare per dare al titolare della carta un'esenzione dalla regola anti-passback. L'anti-passback fa sì che le persone non possano impiegare le stesse credenziali di qualcuno entrato in un'area prima di loro. La prima persona deve uscire dall'area prima che le sue credenziali possano essere riutilizzate.
Titolare di tessera globale	Selezionare questa opzione per consentire la visualizzazione e il monitoraggio del titolare della tessera sui server secondari. Questa opzione è a disposizione solo per i titolari di tessere creati sul server principale. Vedere .

Aggiungi credenziali

È possibile aggiungere i seguenti tipi di credenziali al titolare della tessera:

- PIN
- Badge
- Targa
- Telefono cellulare

Per aggiungere una targa come credenziale di un titolare di tessere:

1. In **Credentials (Credenziali)**, fare clic su **+Add (+ Aggiungi)** e selezionare **License plate (Targa)**.
2. Inserire un nome credenziali che descriva il veicolo.
3. Inserisci il numero targa del veicolo.
4. Impostare la data di inizio e di fine delle credenziali.
5. Fare clic su **Aggiungi**.

Vedere l'esempio in *Usare il numero di targa come credenziale, on page 92*.

Per aggiungere un PIN come credenziale di un titolare di tessere:

1. In **Credentials (Credenziali)**, fare clic su **+Add (+ Aggiungi)** e selezionare **PIN**.
2. Immettere un PIN.
3. Per utilizzare un PIN di coercizione per attivare un allarme silenzioso, attivare **Duress PIN (PIN di coercizione)** e inserire un PIN di coercizione.
4. Fare clic su **Aggiungi**.

Le credenziali del PIN sono sempre valide. È inoltre possibile configurare un PIN di coercizione che apre la porta e attiva un allarme silenzioso nel sistema.

Per aggiungere un badge come credenziale di un titolare di tessere:

1. In **Credentials (Credenziali)**, fare clic su **+Add (+ Aggiungi)** e selezionare **Card (Badge)**.
2. Per immettere manualmente i dati della tessera: inserire il nome della tessera, il numero della tessera e la lunghezza dei bit.

Nota

La lunghezza dei bit è configurabile solo quando si crea un formato tessera con una specifica lunghezza di bit non presente nel sistema.

3. Per ottenere automaticamente i dati della tessera dell'ultima tessera letta:
   3.1. Selezionare una porta dal menu a discesa **Select reader (Seleziona lettore)**.
   3.2. Passare la tessera sul lettore connesso a tale porta.
   3.3. Fare clic su **Get last swiped card data from the door's reader(s) (Acquisisci i dati dell'ultima tessera strisciata dal lettore/dai lettori della porta)**.
4. Inserire un codice struttura. Questo campo è disponibile solo se il **Facility code (Codice struttura)** è stato abilitato in **Access management > Settings (Gestione degli accessi > Impostazioni)**.
5. Impostare la data di inizio e di fine delle credenziali.
6. Fare clic su **Aggiungi**.

Data di scadenza	
Valido da	Impostare una data e un'ora di validità delle credenziali.
Valido fino a	Selezionare un'opzione dal menu a discesa.

Valido fino a	
Nessuna data di fine	Le credenziali non hanno scadenza.
Data	Impostare una data e un'ora di scadenza delle credenziali.
Dal primo utilizzo	Selezionare l'intervallo di scadenza delle credenziali, a partire dal primo utilizzo. Selezionare giorni, mesi, anni o numero di volte dopo il primo utilizzo.
Dall'ultimo utilizzo	Selezionare il periodo di validità delle credenziali, a partire dall'ultimo utilizzo. Selezionare giorni, mesi o anni dopo l'ultimo utilizzo.

Usare il numero di targa come credenziale

Questo esempio illustra il modo di impiegare un door controller, una telecamera dotata di AXIS License Plate Verifier e il numero targa di un veicolo come credenziali per concedere l'accesso.

1. Aggiungere il door controller e la telecamera a AXIS Optimizer.
2. Impostare la data e l'ora per i nuovi dispositivi con **Synchronize with server computer time (Sincronizza con l'ora del computer server)**.
3. Aggiornare il software sui nuovi dispositivi alla versione più recente a disposizione.
4. Aggiungi una nuova porta connessa al tuo door controller. Vedere *Aggiunta di una porta, on page 74*.
   4.1. Aggiungere un lettore su **Lato A**. Vedere *Aggiungi un lettore, on page 79*.

4.2. In **Door settings (Impostazioni porta)**, seleziona **AXIS License Plate Verifier** come **Reader type (Tipo lettore)** e inserisci un nome per il lettore.

4.3. In via facoltativa, aggiungi un lettore o un dispositivo REX su **Side B (Lato B)**.

4.4. Fare clic su **Ok**.

5. Installare e attivare AXIS License Plate Verifier sulla tua telecamera. Vedi il manuale per l'utente *AXIS License Plate Verifier*.
6. Avvia AXIS License Plate Verifier.
7. Configura AXIS License Plate Verifier.
   7.1. Andare a **Configuration > Access control > Encrypted communication (Configurazione > Controllo degli accessi > Comunicazione crittografata)**.
   7.2. In **External Peripheral Authentication Key (Chiave di autenticazione dispositivo periferico esterno)**, fare clic su **Show authentication key (Mostra chiave di autenticazione)** e **Copy key (Copia chiave)**.
   7.3. Apri AXIS License Plate Verifier dall'interfaccia Web della telecamera.
   7.4. Non effettuare l'impostazione.
   7.5. Andare a **Settings (Impostazioni)**.
   7.6. In **Access control (Controllo degli accessi)**, seleziona **Secure Entry** come **Type (Tipo)**.
   7.7. In **IP address (Indirizzo IP)**, immetti l'indirizzo IP e le credenziali per il door controller.
   7.8. In **Authentication key (Chiave di autenticazione)**, incolla la chiave di autenticazione che hai copiato in precedenza.
   7.9. Fare clic su **Connetti**.
   7.10. In **Door controller name (Nome door controller)**, seleziona il door controller.
   7.11. In **Reader name (Nome lettore)**, seleziona il lettore che hai aggiunto in precedenza.
   7.12. Attiva l'integrazione.
8. Aggiungi il titolare tessera a cui vuoi concedere l'accesso. Vedere *Aggiungi un titolare tessera, on page 90*.
9. Eseguire l'aggiunta di credenziali targa al nuovo titolare tessera. Vedere *Aggiungi credenziali, on page 91*.
10. Aggiungi una regola di accesso. Vedere *Aggiungi una regola di accesso, on page 94*.
    10.1. Aggiungere una pianificazione.
    10.2. Aggiungi il titolare tessera a cui vuoi concedere l'accesso tramite targa.
    10.3. Aggiungi la porta con il lettore AXIS License Plate Verifier.

Aggiungi un gruppo

I gruppi consentono di gestire i titolari di tessera e le rispettive regole di accesso collettivamente e in modo efficiente.

1. Andare a **Site Navigation** > **AXIS Optimizer** > **Access control** > **Cardholder management** (Navigazione sito, AXIS Optimizer, Controllo degli accessi, Gestione titolare tessera).
2. Andare su **Groups (Gruppi)** e fare clic su **+ Add (+ Aggiungi)**.
3. Inserire un nome e, facoltativamente, le iniziali del gruppo.
4. Selezionare **Global group (Gruppo globale)** per rendere possibile visualizzare e monitorare il titolare della tessera sui server secondari. Questa opzione è a disposizione solo per i titolari di tessere creati sul server principale. Vedere *Multi-server BETA, on page 88*.
5. Aggiungere i titolari di tessere al gruppo:
   5.1. Fare clic su **+ Aggiungi**.

5.2. Selezionare i titolari di tessere che si desidera aggiungere e fare clic su **Add (Aggiungi)**.

6. Fare clic su **Save (Salva)**.

Aggiungi una regola di accesso

Una regola di accesso definisce le condizioni che devono essere soddisfatte per consentire l'accesso.

Una regola di accesso è composta da:

Titolari tessera e gruppi titolari tessere – a chi concedere l'accesso.

Porte e zone – dove si applica l'accesso.

Pianificazioni – quando concedere l'accesso.

Per aggiungere una regola di accesso:

1. Andare a **Access control** > **Cardholder management** (Controllo degli accessi, gestione titolare tessera).
2. In **Access rules (Regole di accesso)**, fare clic su **+ Add (+Aggiungi)**.
3. Immettere un nome per la regola di accesso e fare clic su **Next (Avanti)**.
4. Configurazione dei titolari e dei gruppi:
   4.1. In **Cardholders (Titolari di tessera)** o **Groups (Gruppi)**, fare clic su **+ Add (+Aggiungi)**.
   4.2. Selezionare i titolari di tessera o i gruppi e fare clic su **Add (Aggiungi)**.
5. Configurazione di porte e zone:
   5.1. In **Doors (Porte)** o **Zones (Zone)**, fare clic su **+ Add (+Aggiungi)**.
   5.2. Selezionare le porte o le zone e fare clic su **Add (Aggiungi)**.
6. Configurazione delle pianificazioni:
   6.1. In **Schedules (Programmi)**, fare clic su **+Add (+Aggiungi)**.
   6.2. Selezionare uno o più programmi e fare clic su **Add (Aggiungi)**.
7. Fare clic su **Save (Salva)**.

Una regola di accesso priva di uno o più dei componenti descritti sopra è incompleta. È possibile visualizzare tutte le regole di accesso incomplete nella scheda **Incomplete**.

Sbloccare in modo manuale porte e zone

Per informazioni sulle azioni manuali, come lo sblocco manuale di una porta, vedere *Azioni manuali, on page 83*.

Per informazioni sulle azioni manuali, come lo sblocco manuale di una zona, vedere *Azioni manuali, on page 83*.

Esportazione dei report sulla configurazione del sistema

È possibile esportare report contenenti diversi tipi di informazioni sul sistema. AXIS Optimizer esporta il report come file CSV (comma-separated value) e lo salva nella cartella di download predefinita. Per esportare un report:

1. Andare in **Reports** > **System configuration (Configurazione del sistema)**.
2. Selezionare i rapporti da esportare e fare clic su **Download**.

Dettagli del titolare tessera	Include informazioni sui titolari di tessera, sulle credenziali, sulla convalida della tessera e sull'ultima transazione.
Accesso titolari tessera	Include le informazioni relative al titolare di tessera e le informazioni su gruppi titolari di tessera, regole di accesso, porte e zone correlate al titolare di tessera.

Accesso gruppo titolari tessera	Include il nome del gruppo titolare di tessera e le informazioni su titolari di tessera, regole di accesso, porte e zone correlate al gruppo titolare di tessera.
Regola di accesso	comprende il nome della regola di accesso e informazioni su titolari di tessera, gruppi titolari di tessera, porte e zone correlate alla regola di accesso.
Accesso porta	comprende il nome della porta e informazioni su titolari di tessera, gruppi titolari di tessera, regole di accesso e zone correlate alla porta.
Accesso zona	comprende il nome della zona e informazioni su titolari di tessera, gruppi titolari di tessera, regole di accesso e porte correlate alla zona.

Crea report sull'attività dei titolari di tessere

Un report appelli elenca i titolari di tessere all'interno di una zona specifica, aiutando a identificare chi è presente in un determinato momento.

Un rapporto raduno elenca i titolari di carta all'interno di una zona specifica, aiutando a identificare chi è al sicuro e chi manca durante le emergenze. Assiste i responsabili degli edifici nella localizzazione del personale e dei visitatori dopo le evacuazioni. Un punto di raccolta è un lettore designato dove il personale si presenta durante le emergenze, generando un report delle persone presenti e non presenti sul sito. Il sistema segnala i titolari di tessera come dispersi finché non si presentano a un punto di raccolta o finché qualcuno non li segnala manualmente come al sicuro.

Sia i rapporti di appello che quelli di raduno richiedono che le zone tengano traccia dei titolari di tessera.

Per creare ed eseguire un report appello o raduno:

1. Andare in **Reports** > **Cardholder activity (Attività titolari tessera)**.
2. Fare clic su **+ Add (+Aggiungi)** e selezionare **Roll call / Mustering (Appello/Raduno)**.
3. Immettere un nome per il report.
4. Selezionare le zone da includere nel report.
5. Selezionare i gruppi che si desidera includere nel report.
6. Se si desidera un report di raduno, selezionare **Mustering point (Punto di raduno)** e un lettore per il punto di raduno.
7. Selezionare un intervallo temporale per il report.
8. Fare clic su **Save (Salva)**.
9. Selezionare il report e fare clic su **Run (Esegui)**.

Stato del report appello	Descrizione
Presente	Il titolare della tessera è entrato nella zona specificata e non è uscito prima della compilazione del report.
Non presente	Il titolare della tessera è uscita dalla zona specificata e non è rientrato prima della compilazione del report.

Stato del report raduno	Descrizione
Al sicuro	Il titolare ha strisciato il proprio badge presso il punto di raduno.
Mancante	Il titolare non ha strisciato il proprio badge presso il punto di raduno.

Impostazioni di gestione degli accessi

Per personalizzare i campi del titolare della tessera utilizzati nel dashboard di gestione degli accessi:

1. Nella scheda **Access management (Gestione accessi)**, fare clic su **Settings (Impostazioni)** > **Custom cardholder fields (Campi personalizzati titolari tessere)**.
2. Fare clic su **+ Add (+Aggiungi)** e immettere un nome. Si possono aggiungere fino a 6 campi personalizzati.
3. Fare clic su **Aggiungi**.

Per usare il codice struttura per verificare il sistema di controllo degli accessi:

1. Nella scheda **Access management (Gestione accessi)**, fare clic su **Settings (Impostazioni)** > **Facility code (Codice struttura)**.
2. Selezionare **Facility code on (Codice struttura attivo)**.

Nota

È anche necessario selezionare **Include facility code for card validation (Includi codice struttura per convalida tessera)** quando si configurano i profili di identificazione. Vedere .

Importa ed esporta

Importa titolari della tessera

Questa opzione importa i titolari di tessera, i gruppi di titolari, le credenziali e le foto dei titolari della tessera da un file CSV. Per importare le foto dei titolari della tessera, assicurarsi che il server abbia accesso alle foto.

Quando importi i titolari tessera, il sistema di gestione degli accessi salva in automatico la configurazione del sistema, inclusa tutta la configurazione hardware, ed elimina qualsiasi configurazione salvata in precedenza.

Opzione di importazione	
Nuovo	questa opzione rimuove i titolari di tessere esistenti e aggiunge nuovi titolari.
Aggiorna	questa opzione aggiorna i titolari di tessere esistenti e aggiunge nuovi titolari di tessere.
Aggiungi	questa opzione mantiene i titolari di tessere esistenti e aggiunge nuovi titolari. I codici carta e gli ID titolare tessera sono univoci e si possono usare una sola volta.

1. Nella scheda **Access management (Gestione accessi)**, fare clic su **Import and export (Importazione ed esportazione)**.
2. Fare clic su **Import cardholders (Importa titolari di tessera)**.
3. Seleziona **New (Nuovo)**, **Update (Aggiorna)** o **Add (Aggiungi)**.
4. Fare clic su **Next (Avanti)**.
5. Fare clic su **Choose a file (Scegli un file)** e andare al file CSV. Fare clic su **Open (Apri)**.

6. Immettere un delimitatore di colonna e selezionare un identificatore univoco, quindi fare clic su **Next (Avanti)**.
7. Assegnare un'intestazione a ogni colonna.
8. Fare clic su **Import (Importa)**.

Impostazioni importazione	
Prima riga è intestazione	Specificare se il file CSV contiene un'intestazione colonna.
Delimitatore colonna	Inserire una formattazione delimitatore di colonna per il file CSV.
Identificatore univoco	Il sistema usa **Cardholder ID (ID titolare tessera)** per riconoscere il titolare tessera per impostazione predefinita. Puoi anche usare il nome e il cognome o l'indirizzo e-mail. L'identificativo univoco impedisce l'importazione di registri del personale duplicati.
Formato numero di tessera	**Allow both hexadecimal and number (Consenti sia valori esadecimali che numeri)** è selezionata per impostazione predefinita.

Esporta titolari di tessera

Questa opzione esporta i dati di titolari di tessera nel sistema in un file CSV.

1. Nella scheda **Access management (Gestione accessi)**, fare clic su **Import and export (Importazione ed esportazione)**.
2. Fare clic su **Export cardholders (Esporta i titolari di tessera)**.
3. Scegliere una posizione per il download e fare clic su **Save (Salva)**.

AXIS Optimizer aggiorna le foto dei titolari di tessera in `C:\ProgramData\Axis Communications\AXIS Camera Station\Components\AXIS Secure Entry\Cardholder photos` ogni volta che si modifica la configurazione.

Undo import (Annulla importazione)

Il sistema salva in automatico la configurazione quando importi i titolari tessera. L'opzione **Undo import (Annulla importazione)** reimposta i dati dei titolari di tessera e di tutte le configurazioni hardware allo stato precedente all'ultima importazione dei titolari tessera.

1. Nella scheda **Access management (Gestione accessi)**, fare clic su **Import and export (Importazione ed esportazione)**.
2. Fare clic su **Undo import (Annulla importazione)**.
3. Fare clic su **Sì**.

Backup e ripristino

I backup automatici vengono eseguiti ogni notte. I tre file di backup più recenti sono archiviati in C:\ProgramData\Axis Communications\AXIS Optimizer Secure Entry\backup. Per ripristinare questi file:

1. Spostare il file di backup in C:\ProgramData\Axis Communications\AXIS Optimizer Secure Entry\restore.
2. Eseguire il riavvio di AXIS Secure Entry utilizzando uno dei seguenti metodi:
   - Avviare il programma MSC (Servizi), individuare "AXIS Optimizer Secure Entry Service" e procedere al riavvio.
   - Avviare il computer.

3. Eseguire nuovamente il programma di installazione di AXIS Optimizer sul computer che funge da server degli eventi.

Gestione degli accessi in Smart Client

Tramite Smart Client, gli operatori possono eseguire operazioni relative al vostro sistema di controllo degli accessi. La maggior parte delle funzioni relative al controllo degli accessi, come il comando manuale delle porte, è disponibile in Smart Client. Per ulteriori informazioni su queste funzionalità, consultare *Utilizzo del controllo degli accessi in Smart Client*.

È inoltre possibile gestire gli accessi direttamente in Smart Client. Le seguenti funzionalità presenti in Client di gestione sono disponibili anche in Smart Client:

- Gestione titolari di schede
- Impostazioni generali
- Campi del titolare di tessera personalizzati
- Codice struttura
- Modelli e-mail
- Modelli di badge BETA

Per visualizzare la scheda gestione accessi di Axis in Smart Client:

1. Installare AXIS Optimizer sul computer su cui è in esecuzione Smart Client.
2. Attivare la licenza per una porta, qualora non ne sia stata attivata nessuna. Per attivare una licenza per porta, consultare *Attivare le licenze per le porte, on page 71*.
3. Controllare che l'utente che ha effettuato l'accesso disponga delle autorizzazioni relative alla gestione degli accessi; per ulteriori informazioni, consultare *Impostazioni dei ruoli di AXIS Secure Entry, on page 98*.

Impostazioni dei ruoli di AXIS Secure Entry

1. In Management Client, andare a **Site Navigation** > **Security** > **Roles (Navigazione sito, Sicurezza, Ruoli)**.
2. Selezionare un ruolo specifico nel sistema.
3. Selezionare **AXIS Optimizer**.
4. Espandere l'elenco e fare clic su **Access control (Controllo degli accessi)**.
5. Selezionare **Read (Leggi)** per le impostazioni di sicurezza relative al controllo degli accessi.
6. Fare clic su quella funzionalità per la quale il ruolo deve disporre dell'autorizzazione e seleziona **Grant (Concedi)**.
   - **Access control configuration (Configurazione controllo degli accessi):** Conferisce al ruolo operatore l'autorizzazione a tutte le funzioni presenti nella scheda Configurazione.
   - **Access management (Gestione degli accessi):** Conferisce al ruolo operatore l'autorizzazione a tutte le funzioni presenti nella scheda Gestione degli accessi.

Gestione del sistema e controlli di sicurezza

Personalizzazione dell'accesso alle funzionalità per gli operatori

Impostazioni ruolo

Per impostazione predefinita, un operatore ha accesso a tutte le funzionalità di AXIS Optimizer in Smart Client se dispone dell'accesso al dispositivo in VMS. Tuttavia, in Management Client (Gestione Client), è possibile configurare le funzionalità a cui un operatore ha accesso tramite Role settings (Impostazioni ruolo).

Configura le impostazioni dei ruoli

Attivare **Role settings (Impostazioni ruolo)**:

1. In Management Client, andare a **Site Navigation > Security > AXIS Optimizer Security (Navigazione sito > Sicurezza > Sicurezza AXIS Optimizer)**.

Nota

Una volta attive le impostazioni dei ruoli, non è possibile disattivarle. L'impostazione è permanente.

2. Selezionare **Turn on role settings (Attiva impostazioni ruolo)**.
3. Riavviare Management Client.

Configurare **Role settings (Impostazioni ruolo)**:

1. In Management Client, andare a **Site Navigation > Security > Roles (Navigazione sito > Sicurezza > Ruoli)**.
2. Selezionare un ruolo e andare a **Overall security (Sicurezza generale)**.
3. Fai clic su **AXIS Optimizer Security**.
4. Selezionare le funzionalità a cui il ruolo deve avere accesso o meno.
   - **Full control (Controllo completo)**Fornisce al ruolo operatore l'accesso a tutte le funzionalità di AXIS Optimizer.
   - **Modifica (non applicabile)**Funzione VMS non applicabile alle impostazioni dei ruoli di AXIS Optimizer.
   - **Accedi a AXIS Optimizer in Management Client**L'operatore può utilizzare tutte le funzionalità di amministrazione di AXIS Optimizer in Management Client.
   - **Gestisci sicurezza di AXIS Optimizer**L'operatore può modificare le impostazioni in **Site Navigation > Security > AXIS Optimizer Security**.
   - **Controlli dell'operatore telecamera dinamico**L'operatore ha accesso a tutte le funzioni preinstallate che il sistema trova su un dispositivo.
   - **Controllo operatore messa a fuoco remota**L'operatore può impostare la messa a fuoco remota sulle telecamere dome fisse.
   - **Comandi operatore PTZ**Il ruolo operatore può ottenere accesso ai comandi PTZ dell'operatore specifico: controllo della messa a fuoco, preset PTZ, comandi operatore per rilevamento automatico 2, rondella e pulsante SpeedDry/tergiscristallo.
   - **Temperature spot measurement control**Il ruolo operatore può misurare la temperatura spot su AXIS Q2901-E.
   - **Controllo operatore altoparlante**L'operatore può accedere a tutte le funzionalità di gestione degli altoparlanti in Smart Client.
   - **Accedi a gestione visitatori**Il ruolo operatore può accedere a tutti gli elementi relativi alla gestione dei visitatori, ad esempio, rispondere a una chiamata e aprire una porta nella visualizzazione in diretta.

- **Accedi alla cronologia chiamate**Il ruolo operatore può accedere alla cronologia delle chiamate di un interfono. È necessario consentire ad **Access visitor management (Accedi a gestione visitatori)** di utilizzare questa impostazione.
- **Funzioni di ricerca avanzate**Se si seleziona **Deny**, la scheda AXIS License Plate Verifier viene nascosta in Smart Client. Inoltre, non è possibile utilizzare la ricerca di veicoli e contenitori nella ricerca centralizzata.
- **Controllo vista dewarping**L'operatore può spostarsi nelle viste con dewarping.
- **Modifica l'home di una vista dewarping**L'operatore può modificare la posizione iniziale di una telecamera.
- **Pagina web**L'operatore può creare una vista con un browser web.
- **Dashboard informazioni Axis**
  Il ruolo operatore ha accesso al dashboard informazioni Axis.

5. Fare clic su **Save (Salva)**.
6. Riavviare tutti gli Smart Client in esecuzione nel sistema.

Gestione dei dispositivi

AXIS Device Manager Extend

Su AXIS Optimizer, puoi usare AXIS Device Manager Extend per la gestione dei dispositivi da molteplici siti. Impostando gli host edge sui server di registrazione, AXIS Device Manager Extend può collegarsi ai tuoi dispositivi nel VMS. Rende facile rivedere le informazioni sulla garanzia ed eseguire aggiornamenti del software su molteplici dispositivi e siti da una sola interfaccia utente.

Per maggiori informazioni su AXIS Device Manager Extend, consulta il *manuale per l'utente*.

Nota

Requisiti

- Accedere ad un *account MyAxis*.
- I server di registrazione devono avere accesso a Internet.
- Supportato solo con dispositivi dotati di AXIS OS 6.50. Per sapere quali dispositivi sono supportati, consultare la sezione *FAQ* (Domande frequenti).

Installazione dell'host edge

L'host edge è un servizio di gestione locale che permette ad AXIS Device Manager Extend di comunicare con i dispositivi locali nel VMS.

L'host edge e il client desktop si devono installare per usare AXIS Device Manager Extend nel VMS. L'host edge e il client desktop sono inclusi nel programma di installazione di AXIS Device Manager Extend.

1. Scarica il *programma di installazione* di AXIS Device Manager Extend.
   L'host edge deve essere installato sui server di registrazione VMS.
2. Eseguire il programma di installazione nel server di registrazione e scegliere di installare solo l'host edge.

Consulta il *manuale per l'utente Axis Device Manager Extend* per maggiori informazioni sulle porte di rete aperte e altri requisiti.

Richiedi l'edge host e sincronizza i dispositivi



1. Apri Management Client.
2. Andare a **Site Navigation > AXIS Optimizer > System overview (Navigazione sito > AXIS Optimizer > Panoramica di sistema)**.
3. Selezionare ed eseguire l'accesso a MyAxis.
4. Fai clic su un riquadro del server di registrazione con un host edge installato pronto per essere richiesto.
5. Nella barra laterale, crea una nuova organizzazione o seleziona un'organizzazione creata precedentemente.
6. Fare clic su e richiedi l'host edge.
7. Attendi che la pagina sia stata ricaricata e fai clic su **Synchronize (Sincronizza)**.
   Tutti i dispositivi Axis sul server di registrazione vengono aggiunti all'host edge e appartengono all'organizzazione selezionata

Nota

AXIS Device Manager Extend deve poter accedere all'hardware Axis nel VMS. Per maggiori informazioni relativamente ai dispositivi supportati, vedere *Risoluzione dei problemi per aggiungere dispositivi all'host edge, on page 102*.

8. Se si aggiungono nuovi dispositivi a un server di registrazione o si modificano le informazioni di un qualsiasi dispositivo, è necessario ripetere il passaggio 7 per la sincronizzazione delle modifiche con il sistema AXIS Device Manager Extend.
9. Ripeti i passaggi da 4 a 7 per tutti i server di registrazione con dispositivi che vuoi aggiungere ad AXIS Device Manager Extend.

Stato host edge

In ogni server di registrazione in **System overview (Panoramica di sistema)** puoi vedere se l'host edge è stato installato o richiesto. È possibile attivare **Show machines that need edge host action (Mostra computer che necessitano di un'azione dell'host edge)** per filtrare la vista.

- – Nessun host edge è stato rilevato sul server di registrazione.
  - Se non è stato installato alcun host edge, scarica e installa l'host edge sul server di registrazione. Vedere *Installazione dell'host edge, on page 100*.
  - Se l'host edge è installato, significa che è necessario accedere all'account MyAxis per poter rilevare l'host edge.
- – L'host edge è installato ma non richiesto. Richiedi l'host edge creando una nuova organizzazione o selezionando un'organizzazione creata in precedenza. Vedere *Richiedi l'edge host e sincronizza i dispositivi, on page 101*.
- – L'host edge è installato e richiesto, ma non raggiungibile. Verificare se il server di registrazione ha accesso a Internet.
- : l'host edge è sincronizzato.

- : l'host edge deve essere sincronizzato. Potrebbero esserci nuovi dispositivi in VMS che è possibile aggiungere all'host edge o informazioni dispositivo aggiornate che necessitano di essere sincronizzate.

Usa AXIS Device Manager Extend per la configurazione dei dispositivi

Una volta avvenuta la sincronizzazione all'host edge, puoi configurare i dispositivi in AXIS Device Manager Extend. Puoi fare ciò da qualsiasi PC connesso a Internet.

Nota

Se si desidera anche gestire i dispositivi tramite una connessione remota, occorre attivare *remote access on each edge host (accesso remoto su ogni host edge).*

1. Installa e apri *l'applicazione desktop AXIS Device Manager Extend*.
2. Seleziona l'organizzazione usata per richiedere l'host edge.
3. I dispositivi sincronizzati possono essere trovati in un sito con lo stesso nome del server di registrazione VMS.

Risoluzione dei problemi per aggiungere dispositivi all'host edge

Se hai difficoltà ad aggiungere dispositivi all'host edge, assicurati di eseguire le operazioni seguenti:

- AXIS Optimizer aggiungerà unicamente hardware abilitato dal VMS.
- Verifica che la connessione con l'hardware non sia danneggiata nel VMS.
- Assicurati che il dispositivo sia dotato di AXIS OS 6.50 o superiore.
- Assicurati che il dispositivo sia impostato sull'autenticazione digest. Per impostazione predefinita, AXIS Device Management non supporta l'autenticazione di base.
- Prova ad aggiungere dispositivi direttamente dall'applicazione AXIS Device Manager Extend.
- Raccogli i registri da AXIS Device Manager Extend e contatta l'assistenza Axis.
  1. Sull'applicazione AXIS Device Manager Extend, vai al sito specifico sul server di registrazione dove è installata la telecamera.
  2. Vai a **Settings (Impostazioni)** e fai clic su **Download sitelog (Scarica sitelog)**.

Importazione AXIS Site Designer

In AXIS Optimizer, puoi importare il tuo AXIS Site Designer di progettazione e applicare la configurazione al tuo VMS con un semplice processo di importazione. Utilizzare *AXIS Site Designer* per progettare e configurare il sistema. Una volta completato il progetto, è possibile importare le impostazioni di tutte le telecamere e altri dispositivi da AXIS Site Designer al client di gestione utilizzando AXIS Optimizer.

Per ulteriori informazioni su AXIS Site Designer, consultare il *manuale per l'utente*.

Nota

Requisiti

- VMS versione 2020 R2 o successiva

Importazione del progetto



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

In AXIS Site Designer

1. Creare un progetto e configurare i dispositivi.
2. Al termine del progetto, generare un codice o scaricare il file delle impostazioni.

Nota

Se si apportano aggiornamenti al progetto, è necessario generare un nuovo codice o scaricare un nuovo file di impostazioni.

In Management Client

1. Assicurarsi che i dispositivi pertinenti siano aggiunti al VMS.
2. Andare a **Site Navigation > AXIS Optimizer > Import design project (Navigazione del sito > AXIS Optimizer > Importa progetto)**.
3. Si apre una guida passo dopo passo. Selezionare il progetto che si desidera importare inserendo il codice di accesso o selezionando il file delle impostazioni del progetto. Fare clic su **Next (Avanti)**.
4. In **Project overview (Panoramica del progetto)** è possibile vedere le informazioni su quanti dispositivi si trovano nel progetto AXIS Site Designer e quanti dispositivi si trovano nel VMS. Fare clic su **Next (Avanti)**.
5. Nel passaggio successivo, i dispositivi nel VMS vengono abbinati ai dispositivi nel progetto AXIS Site Designer. I dispositivi con una sola corrispondenza possibile vengono selezionati automaticamente. Vengono importati solo i dispositivi corrispondenti. Al termine dell'abbinamento, fare clic su **Next (Avanti)**.
6. Le impostazioni per tutti i dispositivi corrispondenti vengono importate e applicate al VMS. L'operazione può richiedere alcuni minuti a seconda delle dimensioni del progetto. Fare clic su **Next (Avanti)**.
7. In **Results of import (Risultati dell'importazione)** puoi trovare dettagli sui diversi passaggi del processo di importazione. Se non è stato possibile importare alcune impostazioni, risolvere i problemi ed eseguire nuovamente l'importazione. Fare clic su **Export... (Esporta...)** se si desidera salvare l'elenco dei risultati come file. Fare clic su **Done (Fatto)** per chiudere la guida dettagliata.

Impostazioni importate

Solo i dispositivi corrispondenti tra il VMS e il progetto di progettazione fanno parte dell'importazione. Le seguenti impostazioni vengono importate e applicate al VMS per tutti i tipi di dispositivo:

- Nome dispositivo utilizzato nel progetto
- Descrizione dispositivo utilizzato nel progetto
- Impostazioni di georilevazione, se il dispositivo è posizionato su una mappa

Se il dispositivo è abilitato al video, vengono applicate anche le seguenti impostazioni:

- Uno o due flussi video configurati nel VMS (risoluzione, velocità in fotogrammi, codec, compressione e impostazioni Zipstream)
  - Il flusso video 1 è configurato per il flusso video e la registrazione.
  - Il flusso video 2 viene configurato per la registrazione, se le impostazioni del flusso nel progetto di progettazione nella visualizzazione in diretta e nella registrazione sono diverse.
- Le regole per il rilevamento movimento o per la registrazione continua vengono impostate in base al progetto. Viene utilizzato il rilevamento movimento integrato del VMS, vengono creati profili di ora per le regole e profili di archiviazione per periodi di memorizzazione diversi sui server di registrazione.
- Il microfono viene acceso o spento in base alle impostazioni audio nel progetto.

Limiti

Ci sono limitazioni nel VMS quando si tratta di importare AXIS Site Designer progetti di design.

- La regola di registrazione del movimento predefinita nel VMS può sovrascrivere le regole di registrazione create dall'importazione. Disattivare tutte le regole in conflitto o escludere i dispositivi interessati dalle regole.
- Le stime della registrazione possono non essere accurate per le registrazioni attivate da movimento VMS.
- Le planimetrie dei piani non sono supportate nella versione corrente.
- Se nel progetto vengono configurate contemporaneamente registrazioni attivate da movimento e registrazioni continue, verranno utilizzate solo le impostazioni di streaming delle impostazioni di registrazione attivate da movimento.
- Non è possibile configurare la velocità in fotogrammi minima per Zipstream nel VMS.

Gestione account

La gestione account aiuta a gestire gli account e le password su tutti i dispositivi Axis utilizzati da XProtect.

Secondo le linee guida Axis, non dovresti utilizzare l'account root per connetterti ai dispositivi. Con Gestione account puoi creare un account di servizio XProtect. Per ciascun dispositivo vengono create password univoche di 16 caratteri. I dispositivi che dispongono già dell'account XProtect ricevono nuove password.

Connettiti ai dispositivi con l'account del servizio XProtect

1. Andare a **Site Navigation > AXIS Optimizer > Account management (Navigazione del sito > AXIS Optimizer > Gestione account)**.
   Il grafico mostra quanti dispositivi sono online, quanti di questi hanno l'account del servizio XProtect e quanti non hanno l'account del servizio XProtect.
2. Fare clic su **Show device details (Mostra i dettagli del dispositivo)** per visualizzare ulteriori informazioni sui dispositivi. I dispositivi online vengono visualizzati in cima all'elenco. È possibile selezionare dispositivi specifici per i quali generare password. Se non ne viene selezionato nessuno, tutti i dispositivi online riceveranno nuove password. Fare clic su **OK**.

Nota

Le password vengono inviate in chiaro tra il server di registrazione e il dispositivo di Axis se si seleziona HTTP nella configurazione hardware. Si consiglia di impostare HTTPS per proteggere la comunicazione tra VMS e dispositivo.

3. Fare clic su **Generate passwords (Genera password)**. La password generata include un testo casuale di 16 caratteri ASCII compreso tra 32 e 126.
   Fare clic su **Show device details (Mostra i dettagli del dispositivo)** per vedere gli aggiornamenti sullo stato in tempo reale del processo. Durante il processo, vedrai una breve interruzione delle visualizzazioni in diretta attive e delle registrazioni in sospeso.
4. I dispositivi online ricevono l'account del servizio XProtect e nuove password. I dispositivi online che dispongono già dell'account del servizio XProtect ricevono solo nuove password.

Eventi Axis

La funzione eventi Axis mette a disposizione una panoramica di eventi disponibili per dispositivi Axis nel VMS. Si possono testare gli eventi in un dispositivo specifico, vedere i dettagli relativi agli eventi e aggiungere eventi a molteplici dispositivi.

In **Site Navigation (Navigazione del sito)**, andare a **Rules and Events > Axis events (Regole ed eventi > Eventi Axis)**. Una lista di tutti gli eventi a disposizione è mostrata nella finestra **Configuration (Configurazione)**. Si può visualizzare quali eventi sono attivi e quali non attivi nel sistema.

Per ciascun evento si può vedere il nome del dispositivo a cui è aggiunto l'evento. Si può anche visualizzare il nome e lo stato dell'evento e l'ultima volta che è stato attivato.

Nota

Requisiti

- VMS versione 2023 R2 o successiva.

Impostare un evento per molteplici dispositivi

1. Andare a **Configuration (Configurazione)** e selezionare un evento.
2. Fare clic su **Aggiungi dispositivi** .
3. La finestra **Add devices (Aggiungi dispositivi)** mostra una lista di dispositivi a cui si può aggiungere l'evento. Selezionare uno o molteplici dispositivi e fare clic su **Add devices (Aggiungi dispositivi)**.

Per eseguire la rimozione di un evento da un dispositivo, fare clic su **Remove (Rimuovi)**.

Informazioni sugli eventi

Negli eventi Axis, si può visualizzare l'ultima occorrenza nota, lo stato degli eventi e gli aggiornamenti in tempo reale nell'interfaccia utente. Per farlo, serve impostare il tempo di conservazione nel client di gestione.

1. Andare su **Tools > Options > Alarm and Events > Event retention (Strumenti > Opzioni > Allarmi ed eventi > Conservazione degli eventi)**.
2. Impostare il tempo di conservazione per l'intero gruppo di eventi del dispositivo o eventi specifici nel gruppo.

Metadati e ricerca

Metadati e ricerca fornisce agli operatori una panoramica di tutti i dispositivi aggiunti al VMS, delle loro capacità di metadati e delle categorie di ricerca Axis.

In Metadati e ricerca è possibile di attivare funzionalità specifiche per questi dispositivi, ossia si ha la possibilità di attivare i dati evento, i dati di analisi e i dati consolidati per molteplici dispositivi e visualizzare le funzioni di analisi supportate dai dispositivi. Con le categorie di ricerca di Axis è possibile controllare le opzioni di ricerca per tutti gli operatori, in modo da riflettere le funzionalità di analisi disponibili nel VMS. Il supporto per le categorie di ricerca e i filtri varia a seconda dei modelli di telecamera e delle applicazioni di analisi installate.

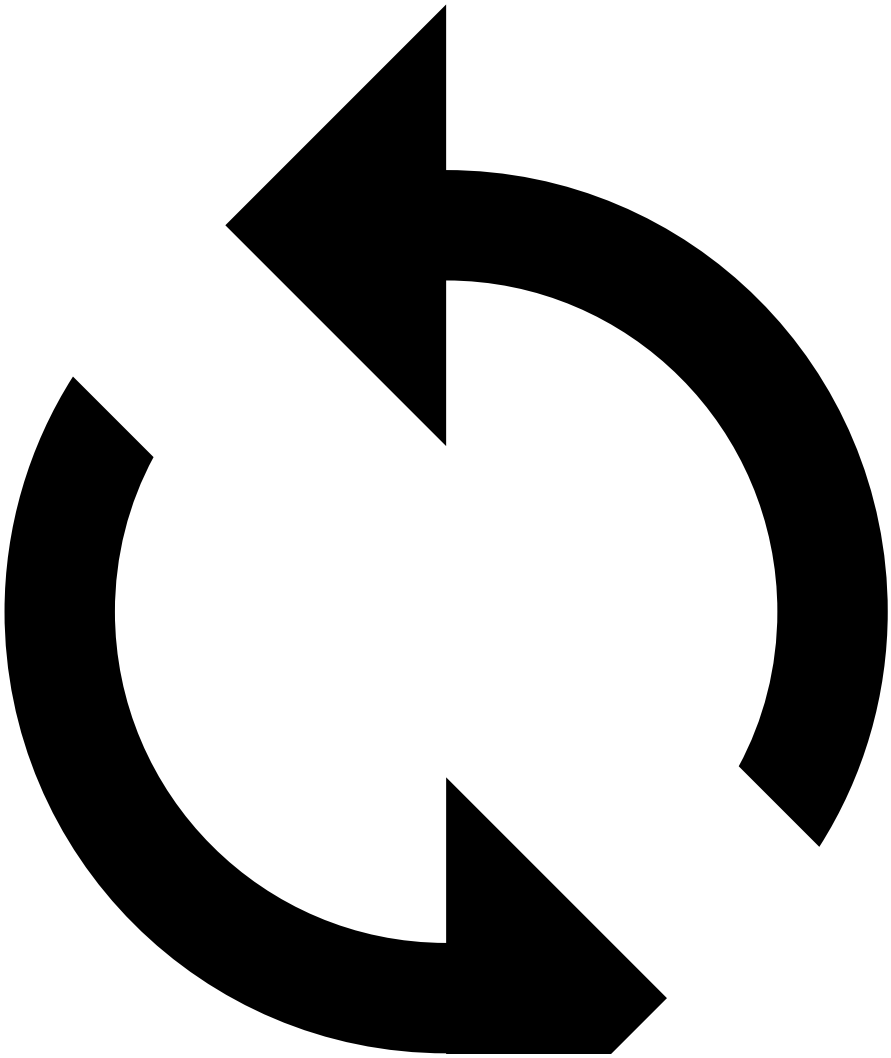
Configurare le impostazioni di metadati

1. Andare a **Management Client** > **Site Navigation (Navigazione sito)** > **AXIS Optimizer** > **Metadata and search (Metadati e ricerca)**.
   - **Dati eventi**: Attivare il VMS per il recupero dei dati evento dal dispositivo. Serve per varie funzionalità di AXIS Optimizer.
   - **Analytics data (Dati di analisi)**: Attivare l'opzione per usare la funzione di ricerca forense e mostrare i riquadri delimitatori del testo nella visualizzazione in diretta e durante la riproduzione.
   - **Analytics features (Caratteristiche di analisi)**: Visualizzare le funzioni di analisi video correntemente supportate dal dispositivo, ad esempio il tipo (umani, auto) e il colore dell'oggetto. Aggiornare il software del dispositivo può mettere a disposizione più funzionalità di analisi.
   - **Consolidated metadata (Metadati consolidati)**: Attivare questa opzione per una ricerca forense più rapida e tempi di caricamento più brevi delle informazioni Axis.

   Nota

   Requisiti di metadati consolidati
   - Dispositivi Axis dotati di AXIS OS 11.10 o versioni successive.

   Limitazioni metadati consolidati
   - I riquadri delimitatori del testo nella visualizzazione in diretta e nella registrazione e le opzioni di ricerca integrate nel VMS non sono a disposizione.

– 
: Fare clic per ricaricare le modifiche apportate alla configurazione del dispositivo.

Configurare le categorie di ricerca Axis

1. Andare a **Management Client** > **Site Navigation (Navigazione sito)** > **AXIS Optimizer** > **Metadata and search (Metadati e ricerca)**.
2. Attivare le categorie di ricerca che si desidera utilizzare nella finestra di dialogo **Axis search categories (Categorie di ricerca Axis)**:
   - Ricerca forense
   - Ricerca veicolo
   - Ricerca velocità zona
   - Ricerca contenitore
3. Selezionare i filtri applicabili in ogni categoria di ricerca.

Nota

Requisiti delle categorie di ricerca Axis

- AXIS Optimizer 5.3 o versione successiva su Smart Client.

Cyber security

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

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

Gestione delle vulnerabilità

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

Notifiche di sicurezza

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

Ciclo di vita sicuro del prodotto

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

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

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

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

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

Guida all'Hardening

In quanto parte integrante dell'infrastruttura VMS, AXIS Optimizer richiede configurazioni specifiche per garantire la sicurezza dell'ambiente. È fondamentale attenersi a queste impostazioni consigliate per salvaguardare le password dei dispositivi, proteggere le informazioni private e impedire l'accesso non autorizzato al proprio sistema.

- Utilizzare il protocollo HTTPS quando si aggiungono dispositivi Axis al VMS.
- Attivare la crittografia tra i client VMS e i server.
- Attivare l'archiviazione dei dati crittografati nel VMS.
- Esaminare tutti i ruoli del VMS e assicurarsi che non dispongano di autorizzazioni superiori al necessario.

Bisogno di assistenza?

FAQ

Domanda	Risposta
Come posso eseguire l'aggiornamento di AXIS Optimizer quando il PC client non ha accesso a Internet?	Pubblicare la nuova versione nel server di gestione VMS, vedere *Esegui in automatico l'aggiornamento del sistema, on page 10*.
Devo fare il backup delle impostazioni prima dell'aggiornamento a una nuova versione di AXIS Optimizer?	No, non è necessario. Non cambia niente quando si esegue l'aggiornamento alla nuova versione.
Se ho oltre 30 PC client con AXIS Optimizer, devo aggiornarli uno alla volta?	Puoi aggiornare i client individualmente. Si può anche inoltrare l'aggiornamento in automatico pubblicando una versione locale di AXIS Optimizer sul proprio sistema, vedere *Esegui in automatico l'aggiornamento del sistema, on page 10*.
Posso abilitare o disabilitare separatamente ciascun plugin in AXIS Optimizer?	No, ma non occuperanno nessuna risorsa se non le usi attivamente.
Quali porte usa AXIS Optimizer?	Le porte 80 e 443 sono entrambe necessarie per la comunicazione con axis.com, affinché il sistema sia in grado di ottenere informazioni sulle nuove versioni e scaricare gli aggiornamenti. Le porte 53459 e 53461 sono aperte per il traffico in entrata (TCP) durante l'installazione di AXIS Optimizer tramite AXIS Secure Entry.

Risoluzione dei problemi

In caso di problemi tecnici, attivare la registrazione debug, riprodurre il problema e condividere questi registri con l'assistenza Axis. È possibile attivare l'accesso al debug in Management Client o in Smart Client.

In Management Client:

1. Andare a **Site Navigation** > **Basics** > **AXIS Optimizer** (Navigazione sito > Operazioni di base > AXIS Optimizer).
2. Selezionare **Turn on debug logging** (Attiva registrazione debug).
3. Fare clic su **Save report** (Salva report) per salvare le registrazioni sul dispositivo.

In Smart Client:

1. Andare a **Settings** > **Axis general options** (Impostazioni, Opzioni generali di Axis).
2. Selezionare **Turn on debug logging** (Attiva registrazione debug).
3. Fare clic su **Save report** (Salva report) per salvare le registrazioni sul dispositivo.

Contattare l'assistenza

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

Consigli e suggerimenti

Aggiunta di una pagina Web in una vista Smart Client

AXIS Optimizer consente di visualizzare quasi tutte le pagine Web direttamente in Smart Client, non solo le pagine HTML. Questa visualizzazione Web è alimentata da un moderno motore del browser ed è compatibile con la maggior parte delle pagine Web. Questa opzione è utile, ad esempio, quando si desidera accedere ad AXIS Body Worn Manager da Smart Client o visualizzare un dashboard da AXIS Store Reporter accanto alle visualizzazioni in diretta.

1. In Smart Client, fare clic su **Setup (Impostazione)**.
2. Vai a **Views (Viste)**.
3. Creare una nuova vista o selezionarne una esistente.
4. Andare a **System overview > AXIS Optimizer (Panoramica di sistema > AXIS Optimizer)**.
5. Fare clic su **Web view (Visualizzazione web)** e trascinare l'opzione nella vista.
6. Immettere un indirizzo e fare clic su **OK**.
7. Fare clic su **Setup (Impostazione)**.

Esporta video con funzioni di ricerca integrate

Esportazione di video in formato XProtect

Per visualizzare video con funzioni di ricerca di AXIS Optimizer e/o funzionalità di distorsione Axis integrate, assicurarsi di esportare i video in formato XProtect. Ciò può essere utile, ad esempio, a fini dimostrativi.

Nota

Per AXIS Optimizer versione 5.3 o versioni successive Iniziare dal punto 3.

1. In Smart Client, andare a **Settings (Impostazioni)** > **Axis search options (Opzioni di ricerca Axis)**.
2. Attiva **Include search plugins in exports (Includi plugin di ricerca nelle esportazioni)**.
3. Seleziona **XProtect format (formato XProtect)** quando si crea l'esportazione in Smart Client.

Sblocca le esportazioni sui computer di ricezione

Per utilizzare correttamente l'esportazione su un altro computer assicurarsi di sbloccare l'archivio del file di esportazione.

1. Sul computer di ricezione, fare clic con il pulsante destro del mouse sul file di esportazione (zip) e selezionare **Properties (Proprietà)**.
2. Nella scheda **General (Generale)** fare clic su **Unblock (Sblocca)** > **OK**.
3. Estrarre l'esportazione e aprire il file "SmartClient-Player.exe".

Riproduzione della visualizzazione trasformata Axis esportata

1. Aprire il progetto esportato.
2. Selezionare la vista che include la visualizzazione trasformata Axis.

T10134385_it

2026-09 (M61.2)

© 2021 – 2026 Axis Communications AB