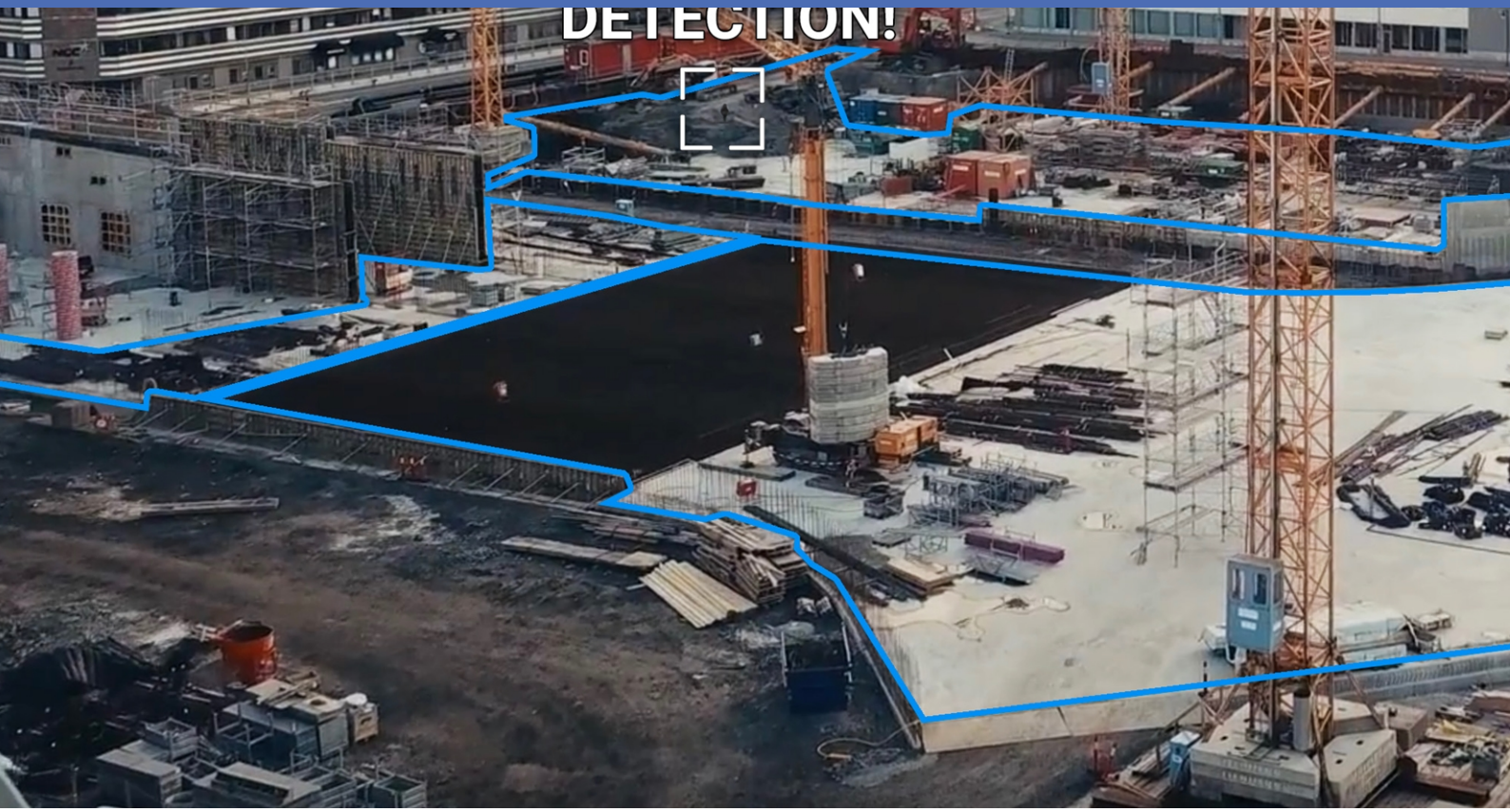
Guida

Irisity IRIS AI Analytics - Intrusion Detection



BeyondHumanVision

MOBOTIX

V1.09_16/03/2023, Codice ordine: Mx-APP-IRIS-C-INT

Sommario

1

Prima di iniziare

Supporto

Per assistenza tecnica, contattare il rivenditore MOBOTIX. Se il rivenditore non è in grado di fornire assistenza, contatterà a sua volta il canale di supporto per fornire una risposta il prima possibile.

Se si dispone dell'accesso a Internet, è possibile aprire l'help desk MOBOTIX per trovare ulteriori informazioni e aggiornamenti software. Visitare:

www.mobotix.com > Supporto > Assistenza

Note sulla sicurezza

- Questo prodotto non deve essere utilizzato in luoghi esposti a pericoli di esplosione.
- Non utilizzare il prodotto in ambienti polverosi.
- Proteggere il prodotto dall'ingresso di umidità o acqua nell'alloggiamento.
- Installare questo prodotto come descritto nel presente documento. Un'installazione non corretta può danneggiare il prodotto!
- Questa apparecchiatura non è adatta per l'uso in luoghi in cui è probabile che siano presenti bambini.
- Se si utilizza un adattatore di Classe I, il cavo di alimentazione deve essere collegato a una presa con un collegamento a massa adeguato.
- Per garantire la conformità ai requisiti della norma EN 50130-4 in materia di alimentazione dei sistemi di allarme per il funzionamento 24 ore su 24, 7 giorni su 7, si consiglia vivamente di utilizzare un gruppo di continuità (UPS) per il backup dell'alimentazione del prodotto.
- Questa apparecchiatura deve essere collegata solo a reti PoE senza routing ad altre reti.

Note legali

Aspetti legali della registrazione video e audio

Quando si utilizzano prodotti MOBOTIX AG, è necessario rispettare tutte le normative sulla protezione dei dati per il monitoraggio audio e video. In base alle leggi nazionali e alla posizione di installazione delle videocamere, la registrazione dei dati video e audio può essere soggetta a documentazione speciale o può essere vietata. Tutti gli utenti di prodotti MOBOTIX sono pertanto tenuti a conoscere tutte le normative applicabili e a rispettare tali leggi. MOBOTIX AG non è responsabile per qualsiasi uso illegale dei suoi prodotti.

Dichiarazione di conformità

I prodotti MOBOTIX AG sono certificati in conformità alle normative vigenti nella CE e in altri paesi. Le dichiarazioni di conformità per i prodotti di MOBOTIX AG sono disponibili su www.mobotix.com in **Supporto > Centro Download > Marketing & Documentazione > Certificati & Dichiarazioni di conformità**.

Dichiarazione RoHS

I prodotti di MOBOTIX AG sono pienamente conformi alle limitazioni imposte dall'Unione Europea relativamente all'uso di determinate sostanze pericolose nelle apparecchiature elettriche ed elettroniche (Direttiva RoHS 2011/65/CE) nella misura in cui sono soggetti a queste normative (per la Dichiarazione RoHS di MOBOTIX, vedere www.mobotix.com, **Supporto > Centro Download > Marketing & Documentazione > Opuscoli e Istruzioni > Certificati**).

Smaltimento

I prodotti elettrici ed elettronici contengono molti materiali preziosi. Per questo motivo, si consiglia di smaltire i prodotti MOBOTIX al termine della relativa vita utile in modo conforme a tutti i requisiti e le normative legali (o di depositare questi prodotti presso un centro di raccolta comunale). I prodotti MOBOTIX non devono essere smaltiti insieme ai rifiuti domestici! Se il prodotto contiene una batteria, smaltirla separatamente (i manuali del prodotto forniscono istruzioni specifiche se il prodotto contiene una batteria).

Esclusione di responsabilità

MOBOTIX AG non si assume alcuna responsabilità per danni derivanti da un uso improprio o dalla mancata conformità ai manuali o alle norme e alle normative applicabili. Vengono applicati i nostri Termini e condizioni generali. È possibile scaricare la versione corrente dei **Termini e condizioni generali** dal nostro sito Web www.mobotix.com facendo clic sul collegamento corrispondente nella parte inferiore di ogni pagina.

Informazioni su Irisity IRIS AI Analytics - Intrusion Detection

Rileva l'attività umana nelle aree blindate

Irisity IRIS AI Analytics - Intrusion Detection attiva gli allarmi al superamento in aree ristrette. L'algoritmo offre rilevamenti accurati dell'attività umana a lunghe distanze e su vaste aree. L'applicazione ha una precisione fino al 99%. L'applicazione può essere testata gratuitamente per 30 giorni e viene attivata per un periodo di tempo illimitato. I rilevamenti della presenza umana includono anche veicoli come biciclette, automobili e camion, anche in condizioni meteorologiche avverse e con scarsa illuminazione.

- Rileva l'intrusione di oggetti di interesse nelle zone/aree di rilevamento definite dall'utente
- Progettato per il rilevamento affidabile di persone e veicoli che occupano solo piccole porzioni del campo visivo
- Riduce al minimo i falsi allarmi filtrando i movimenti non critici (ad es. alberi, nuvole, ecc.)
- Rilevamento simultaneo su uno o più sensori di immagine
- Eventi MOBOTIX tramite MxMessageSystem
- Ricerca di eventi consolidata tramite MxManagementCenter Smart Data Interface e/o MOBOTIX HUB

ATTENZIONE! Questa app non supporta i moduli sensore termico ECO.

Interfaccia Smart Data a MxManagementCenter

Questa applicazione è dotata di un'interfaccia Smart Data a MxManagementCenter.

Con il sistema MOBOTIX Smart Data, i dati di transazione possono essere collegati alle registrazioni video effettuate al momento delle transazioni. Le fonti di Smart Data possono essere ad esempio MOBOTIX Applicazioni certificate (non è richiesta alcuna licenza) o fonti Smart Data generali (è richiesta la licenza), come sistemi di punti vendita o sistemi di riconoscimento delle targhe.

Il sistema Smart Data in MxManagementCenter consente di individuare e rivedere rapidamente qualsiasi attività sospetta. La barra e la visualizzazione Smart Data sono disponibili per la ricerca e l'analisi delle transazioni. La barra Smart Data offre una panoramica diretta delle transazioni più recenti (dalle ultime 24 ore) e, per questo motivo, è comoda da usare per revisioni e ricerche.

AVISSO! Per informazioni sull'utilizzo del sistema Smart Data, consultare la guida online corrispondente del software della telecamera e MxManagementCenter.

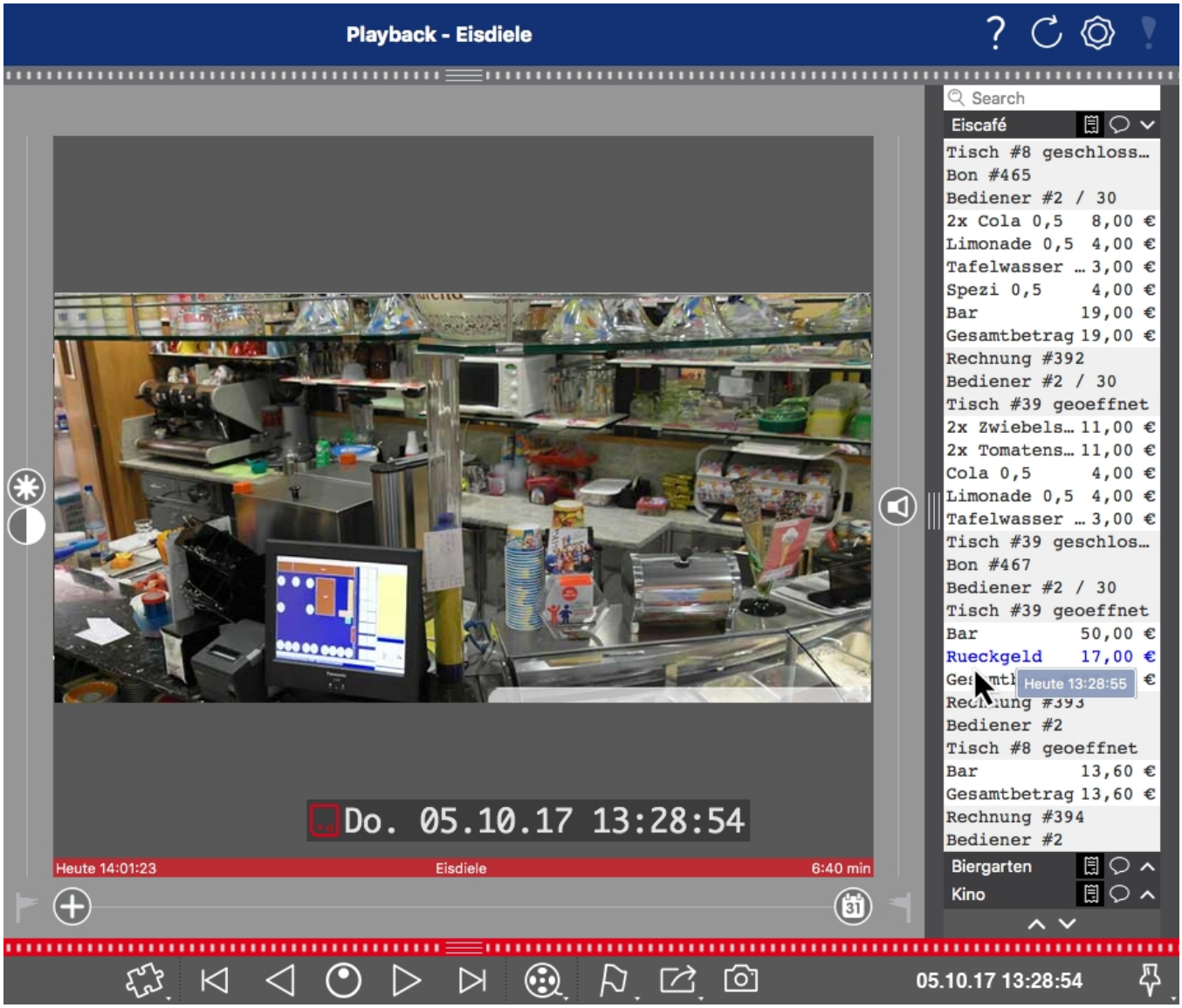


Fig. 1: : Barra Smart Data in MxManagementCenter (esempio: sistema di punti vendita)

Specifiche tecniche

Informazioni sul prodotto

Nome prodotto	Irisity IRIS AI Analytics - Intrusion Detection
Codice ordine	Mx-APP-IRIS-C-INT
Supportati Videocamere MOBOTIX	Mx-M73A, Mx-S74A
Firmware minimo della tele-camera	V7.3.0.x
MxManagementCenter Integrazione	■ min. MxMC v2.5.3 ■ Configurazione: Necessaria licenza di configurazione Advanced ■ Ricerca: Licenza Interfaccia Smart Data inclusa

Caratteristiche del prodotto

Caratteristiche dell'applicazione	■ Rileva l'intrusione di oggetti di interesse nelle zone/aree di rilevamento definite dall'utente ■ Progettato per il rilevamento affidabile di persone e veicoli che occu-pano solo piccole porzioni del campo visivo ■ Riduce al minimo i falsi allarmi filtrando i movimenti non critici (ad es. alberi, nuvole, ecc.) ■ Rilevamento simultaneo su uno o più sensori di immagine ■ Eventi MOBOTIX tramite MxMessageSystem ■ Ricerca di eventi consolidata tramite MxManagementCenter Smart Data Interface e/o MOBOTIX HUB
Numero massimo di zone di riconoscimento	20
Formati meta-dati/statistiche	JSON
Licenza di prova	Licenza di prova di 30 giorni preinstallata
MxMessageSystem supportato	Sì

Eventi MOBOTIX	Sì
Eventi ONVIF	Sì (evento messaggio generico)

Requisiti della scena

Altezza minima degli oggetti	20 px / ~6% dell'altezza dell'immagine (analisi attualmente bloccata sulla risoluzione 640 x 360)
Altezza di montaggio della videocamera	min. 2 m (tenendo conto dei requisiti della scena, l'ideale è tra 5 e 20 m)
Angolo verticale massimo	Emisferica
Angolo orizzontale massimo	Emisferica
Angolo di inclinazione massimo	Solo inclinazione verso il basso: nessun limite

Specifiche tecniche dell'applicazione

Applicazione sincrona / asincrona	Asincrona
Precisione	> 99% (tenendo conto dei requisiti della scena)
Numero di frame al secondo elaborati	Tipo 10 fps
Tempo di rilevamento	~ 2 s

Licenze per applicazioni certificate

Per l'applicazione Irisity IRIS AI Analytics - Intrusion Detection sono disponibili le seguenti licenze:

- **Licenza di prova di 30 giorni** preinstallata
- **licenza commerciale permanente**

Il periodo di utilizzo inizia con l'attivazione dell'interfaccia app (vedere)

AVISSO! Per acquistare o rinnovare una licenza, contattare il proprio partner MOBOTIX.

AVISSO! Le applicazioni vengono generalmente preinstallate con il firmware. Capita raramente che debbano essere scaricate dal sito Web e installate. In tal caso, vedere **www.mobotix.com > Supporto > Centro Download > Marketing & Documentazione** e scaricare e installare l'applicazione.

Attivazione della licenza delle applicazioni certificate in MxManagementCenter

Dopo un periodo di prova, le licenze commerciali devono essere attivate per l'uso con una chiave di licenza valida.

Attivazione online

Dopo aver ricevuto gli ID di attivazione, attivarli in MxMC come segue:

1. Selezionare dal menu **Window > Camera App Licenses (Finestra > Licenze applicazioni telecamera)**.
2. Selezionare la telecamera su cui si desidera attivare le licenze delle applicazioni e fare clic su **Select (Seleziona)**.

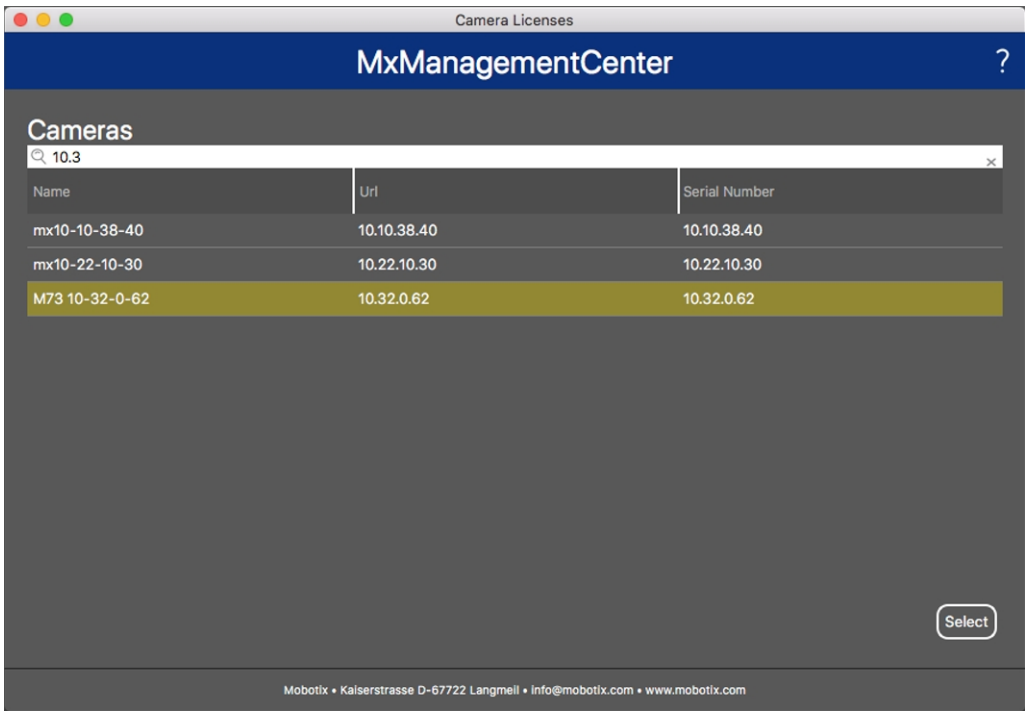


Fig. 2: Panoramica delle licenze applicazioni telecamera in MxManagementCenter

AVISSO! Se necessario, correggere l'ora impostata sulla telecamera.

1. È possibile visualizzare una panoramica delle licenze installate sulla telecamera. Fare clic su **Activate License (Attiva licenza)**.

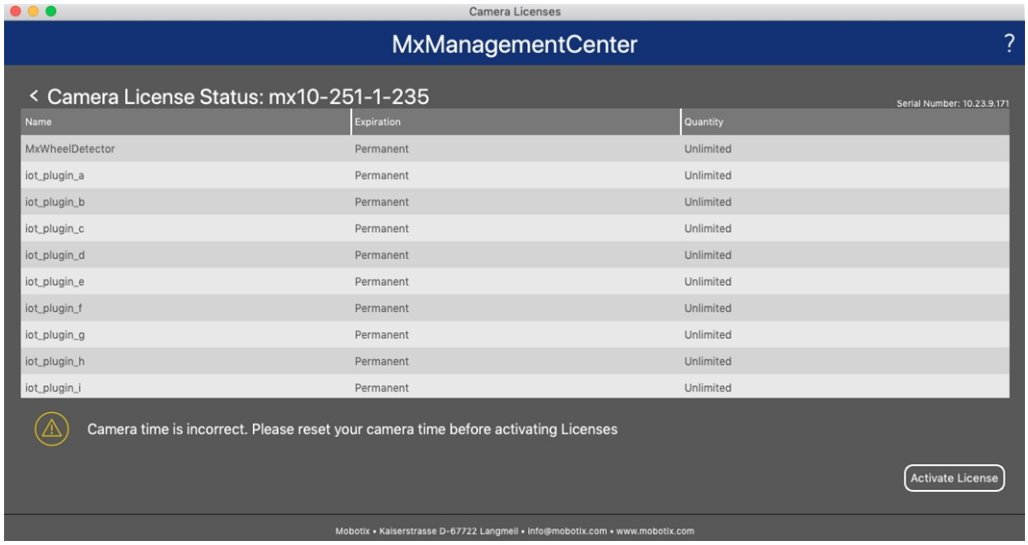


Fig. 3: Panoramica delle licenze installate sulla telecamera

AVISSO! Se necessario, correggere l'ora impostata sulla telecamera.

2. Inserire un ID di attivazione valido e specificare il numero di licenze da installare sul computer in uso.
3. Se si desidera attivare la licenza di un altro prodotto, fare clic su . Nella nuova riga, inserire l'ID di attivazione appropriato e il numero di licenze desiderate.

4. Per rimuovere una riga, fare clic su .
5. Una volta inseriti tutti gli ID di attivazione, fare clic su **Activate License Online Attiva licenza online)**. Durante l'attivazione, **MxMC** si collega al server delle licenze. Ciò richiede una connessione a Internet.

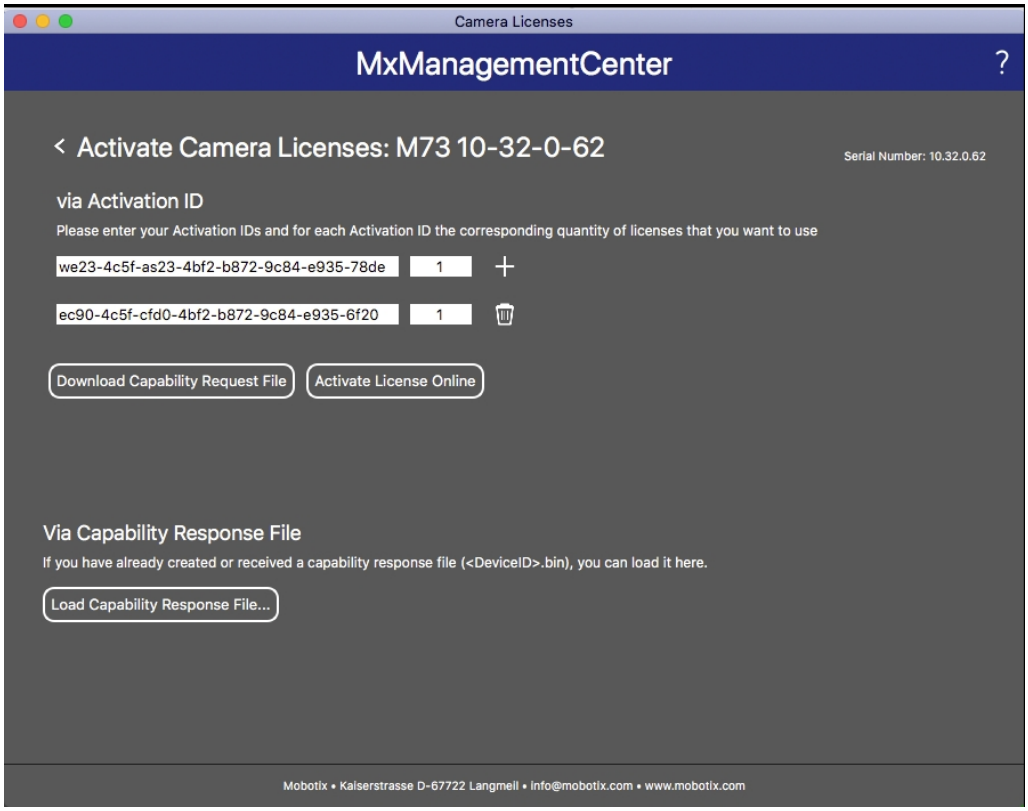


Fig. 4: Aggiunta di licenze

Attivazione riuscita

Una volta completata l'attivazione, è necessario effettuare un nuovo accesso per applicare le modifiche. In alternativa, è possibile tornare alla gestione delle licenze.

Attivazione non riuscita (connessione a Internet mancante)

Qualora non sia possibile raggiungere il server delle licenze, ad esempio a causa della mancanza di una connessione a Internet, è possibile attivare le applicazioni anche offline (vedere Attivazione offline, p. 12).

Attivazione offline

Per l'attivazione offline, il partner/installatore da cui sono state acquistate le licenze può generare una risposta di capacità (file .bin) sul server delle licenze per attivare le relative licenze.

1. Selezionare dal menu **Window > Camera App Licenses (Finestra > Licenze applicazioni telecamera)**.
2. Selezionare la telecamera su cui si desidera attivare le licenze delle applicazioni e fare clic su **Select (Seleziona)**.

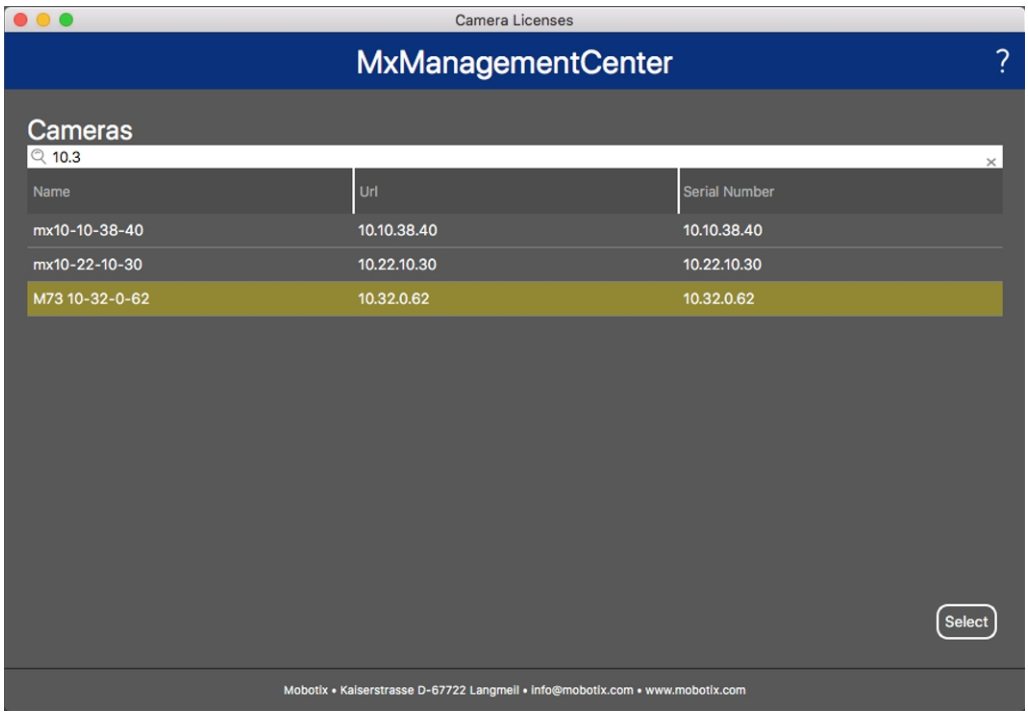


Fig. 5: Panoramica delle licenze applicazioni telecamera in MxManagementCenter

AVISSO! Se necessario, correggere l'ora impostata sulla telecamera.

3. È possibile visualizzare una panoramica delle licenze installate sulla telecamera. Fare clic su **Activate License (Attiva licenza)**.

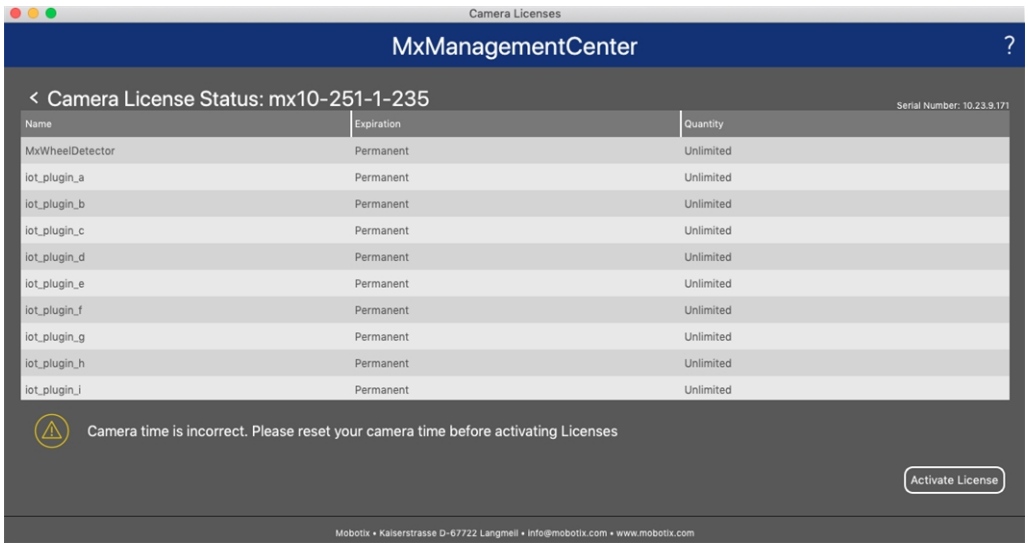


Fig. 6: Panoramica delle licenze installate sulla telecamera

AVISSO! Se necessario, correggere l'ora impostata sulla telecamera.

4. Inserire un ID di attivazione valido e specificare il numero di licenze da installare sul computer in uso.
5. Se si desidera attivare la licenza di un altro prodotto, fare clic su . Nella nuova riga, inserire l'**ID di attivazione** appropriato e il numero di licenze desiderate.
6. Se necessario, fare clic su per rimuovere una riga.
7. Una volta inseriti tutti gli ID di attivazione, fare clic su **Download Capability Request File (.lic) (Scarica file richiesta capacità (.lic)** e inviare il file scaricato al proprio partner/installatore.

AVISSO! Questo file consente al partner/installatore da cui sono state acquistate le licenze di generare un file di risposta di capacità (file .bin) sul server delle licenze.

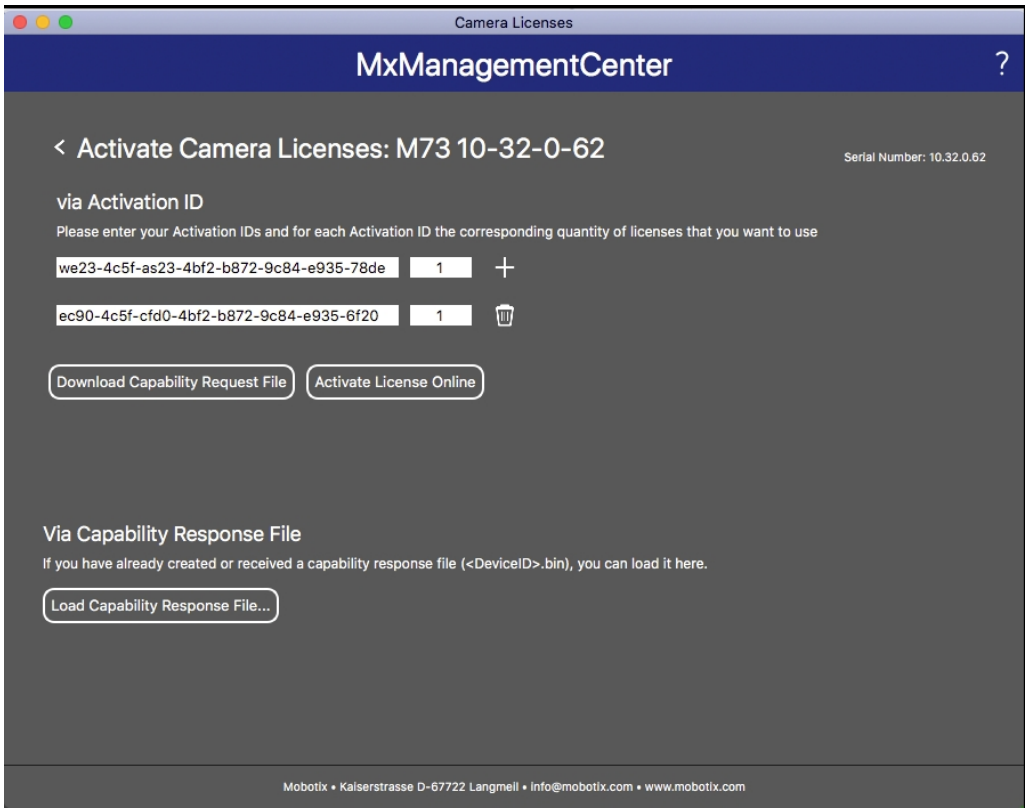


Fig. 7: Aggiunta di licenze

8. Fare clic su Load Capability Response File (Carica file risposta capacità) e seguire le istruzioni.

Attivazione riuscita

Una volta completata l'attivazione, è necessario effettuare un nuovo accesso per applicare le modifiche. In alternativa, è possibile tornare alla gestione delle licenze.

Gestione delle licenze in MxManagementCenter

In MxManagementCenter è possibile gestire comodamente tutte le licenze che sono state attivate per una telecamera.

1. Selezionare dal menu **Window > Camera App Licenses (Finestra > Licenze applicazioni telecamera)**.
2. Selezionare la telecamera su cui si desidera attivare le licenze delle applicazioni e fare clic su **Select (Seleziona)**.

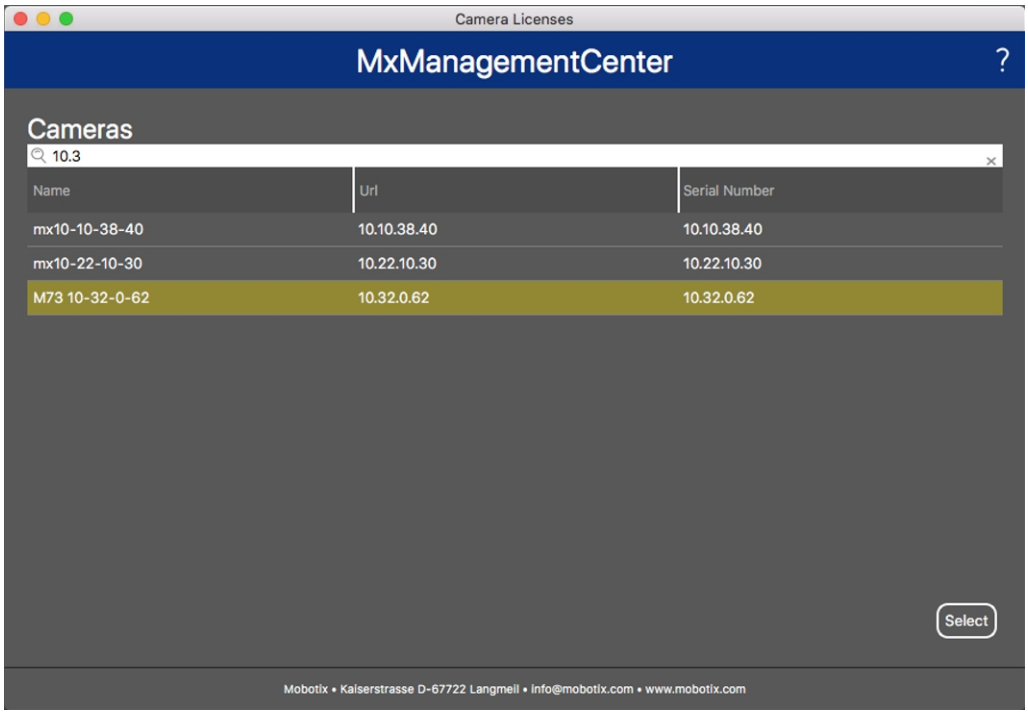


Fig. 8: Panoramica delle licenze applicazioni telecamera in MxManagementCenter

È possibile visualizzare una panoramica delle licenze installate sulla telecamera.

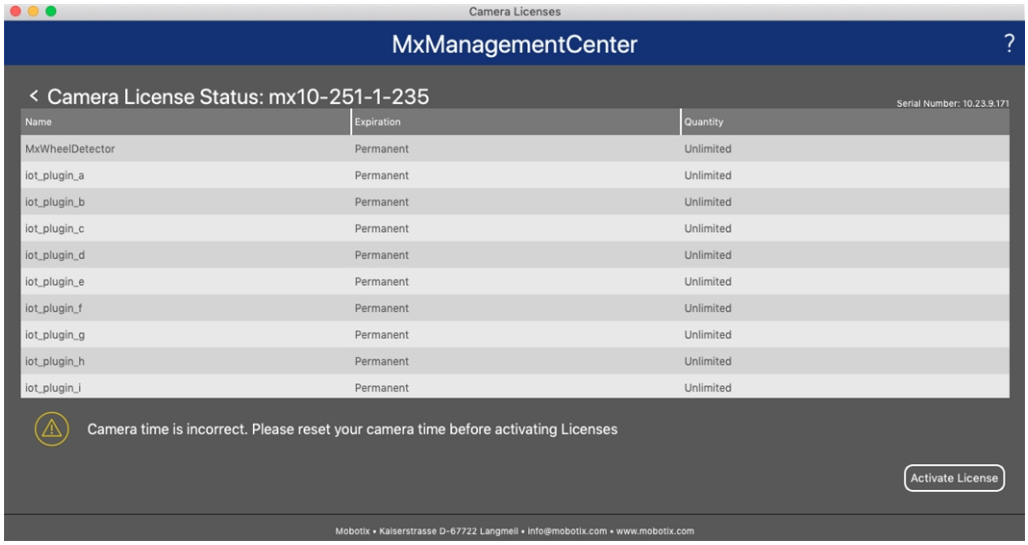


Fig. 9: Panoramica delle licenze installate sulla telecamera

AVISSO! Se necessario, correggere l'ora impostata sulla telecamera.

Colonna	Spiegazione
Nome	Nome dell'applicazione ottenuta in licenza
Scadenza	Durata temporale della licenza
Quantità	Numero di licenze acquistate per un prodotto.
Numero di serie	Numero di identificazione univoco stabilito da MxMC per il dispositivo utilizzato. Se durante il periodo di licenza si verificano dei problemi, tenere a portata di mano l'ID del dispositivo.

Sincronizzazione delle licenze con il server

All'avvio del programma, non viene effettuato alcun confronto automatico delle licenze tra il computer e il server delle licenze. Pertanto fare clic su **Update (Aggiorna)** per ricaricare le licenze dal server.

Aggiornamento delle licenze

Per aggiornare le licenze temporanee, fare clic su **Activate Licenses (Attiva licenze)**. Verrà visualizzata la finestra di dialogo per l'aggiornamento/attivazione delle licenze.

AVISSO! Per sincronizzare e aggiornare le licenze, è necessario disporre dei diritti di amministratore.

Requisiti relativi a videocamera, immagine e scena

La telecamera deve essere configurata in modo che la combinazione della distanza, della lunghezza focale dell'obiettivo e della risoluzione della telecamera fornisca un'immagine che possa essere analizzata con precisione. Rispetto alla scena, devono essere pertanto soddisfatti i prerequisiti riportati di seguito.

Posizioni di montaggio più alte possibili per risultati ottimali

Durante la pianificazione del sistema di videosorveglianza, è consigliabile posizionare la videocamera più in alto per coprire l'area più ampia possibile con ciascuna videocamera. Considerare un'altezza di installazione di almeno 5 metri. Solitamente un'altezza di installazione di 10-25 metri permette di ottenere risultati significativamente migliori.

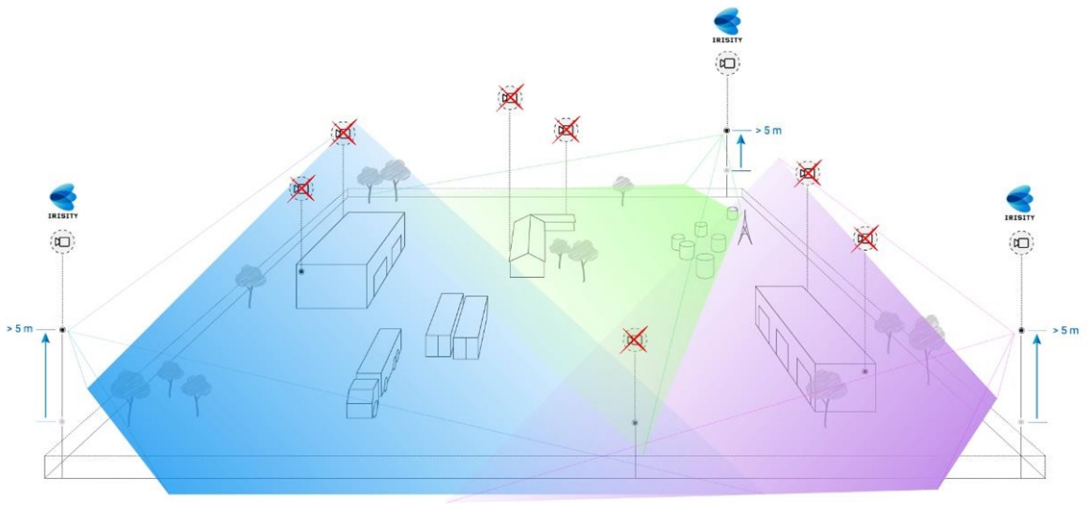


Fig. 10: L'utilizzo di posizioni di montaggio elevate può ridurre il numero di telecamere in un'installazione CCTV classica.

Illuminazione della scena

Con sorgenti luminose ottimali (si consigliano almeno due sorgenti luminose), è possibile migliorare significativamente la qualità dell'analisi video e quindi la sicurezza del sito.

- Illuminare a sufficienza l'area monitorata.
- Garantire un buon contrasto nell'area di sorveglianza.
- Non illuminare in modo eccessivo oggetti vicino alla fotocamera per evitare interferenze e rumori.

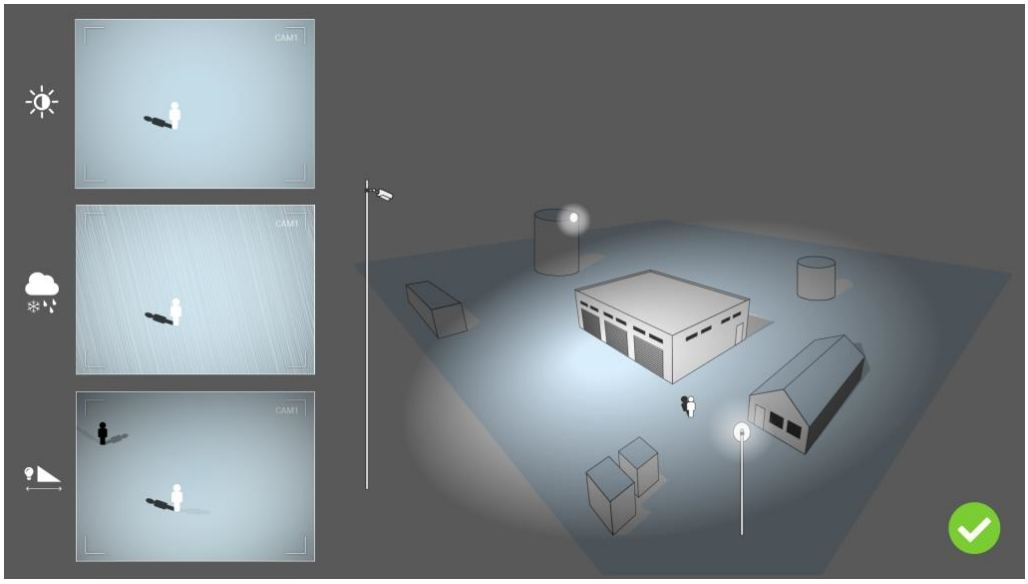


Fig. 11: L'illuminazione fuori asse migliora significativamente la visibilità, il contrasto e il rilevamento degli oggetti. In questo modo è possibile eseguire rilevamenti precisi anche nelle condizioni climatiche più difficili.

Risoluzione dei problemi

Problemi di progettazione della luce

Se si posiziona la sorgente luminosa vicino alla videocamera e troppo lontano dall'oggetto controllato, la luce emessa potrebbe compromettere la sorveglianza creando problemi video. I possibili problemi sono:

- Il contrasto nell'immagine video può essere troppo basso (senza ombre)
- La sorgente luminosa può creare rumore nell'immagine accentuando le gocce di pioggia e i fiocchi di neve
- L'intensità luminosa può non essere sufficiente a illuminare l'oggetto controllato

Anche se può essere comodo avere la luce integrata della telecamera, o altre luci in asse, spesso ciò riduce l'efficienza del sistema di sorveglianza. In condizioni climatiche avverse, gli intrusi potrebbero diventare quasi invisibili, coperti da pioggia, neve o nebbia

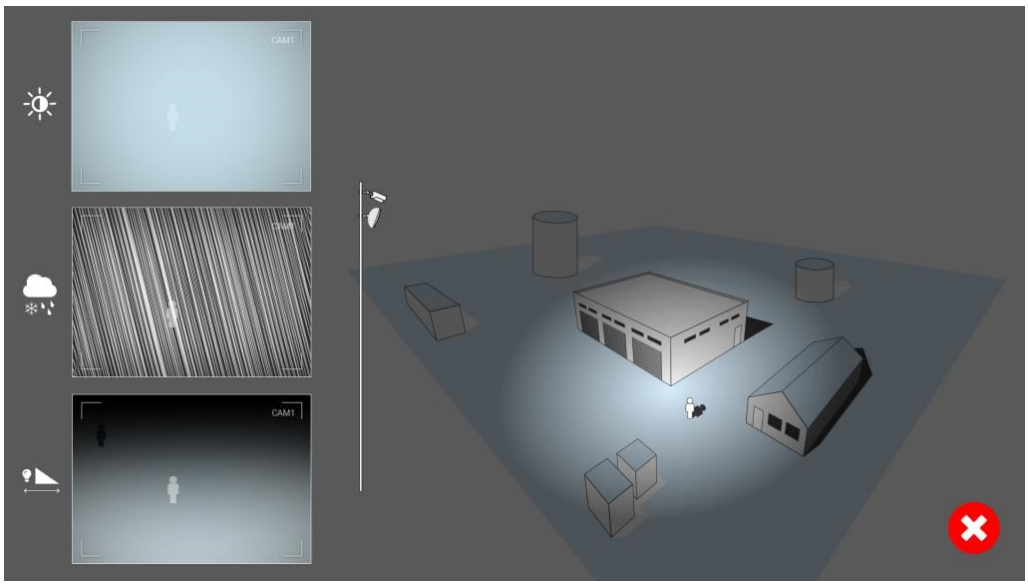


Fig. 12: In condizioni climatiche avverse, gli intrusi potrebbero diventare quasi invisibili, coperti da pioggia, neve o nebbia

Attivazione dell'interfaccia dell'applicazione certificata

ATTENZIONE! L'applicazione Irisity IRIS AI Analytics - Intrusion Detection non considera le aree oscure definite per l'immagine live. Pertanto, durante la configurazione dell'applicazione e l'analisi dell'immagine da parte dell'applicazione, non vi è alcuna pixelizzazione nelle aree oscure.

AVISSO! L'utente deve avere accesso al menu di configurazione (http(s)://<Camera IP address>/control). Verificare pertanto i diritti dell'utente della telecamera.

1. Nell'interfaccia Web della telecamera, aprire: **Setup Menu / Certified App Settings (Menu Setup / Impostazioni applicazioni certificate)** (http(s)://<Camera IP address>/control/app_config).

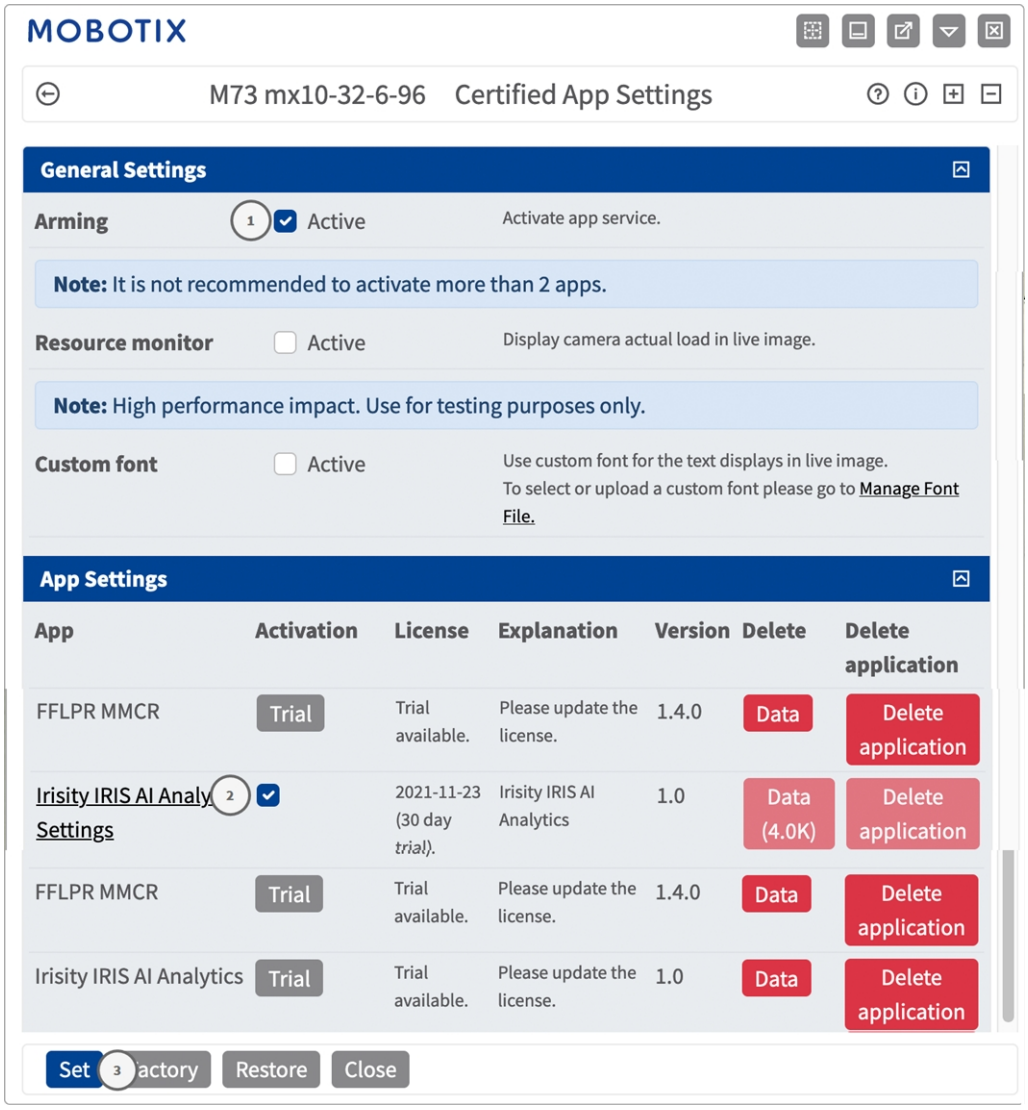


Fig. 13: Applicazione certificata: Impostazioni

2. In **Impostazioni generali**, spuntare l'opzione **Attivazione** del MOBOTIXservizio dell'app① .
3. Fare clic su Imposta ③ . Le app installate ora sono in elenco.
4. In **Impostazioni app**, selezionare l'opzione **Attiva** dell'app pertinente.
5. Fare clic sul nome dell'applicazione ② da configurare per aprire l'interfaccia utente delle applicazioni.
6. Per la configurazione dell'applicazione, vedere Configurazione dell'applicazione Irisity IRIS AI Analytics - Intrusion Detection, p. 22

Configurazione dell'applicazione Irisity IRIS AI Analytics - Intrusion Detection

ATTENZIONE! L'utente deve avere accesso al menu di configurazione (http(s)://<Camera IP address>/control). Verificare pertanto i diritti dell'utente della telecamera.

1. Nell'interfaccia Web della telecamera, aprire: **Setup Menu / Certified App Settings (Menu Setup / Impostazioni applicazioni certificate)** (http(s)://<Camera IP address>/control/app_config).
2. Fare clic sul nome dell'applicazione **Irisity IRIS AI Analytics - Intrusion Detection**.

Verrà visualizzata la finestra di configurazione dell'applicazione con le opzioni riportate di seguito.

Rilevamento intrusioni IRIS

Considerare le seguenti configurazioni:

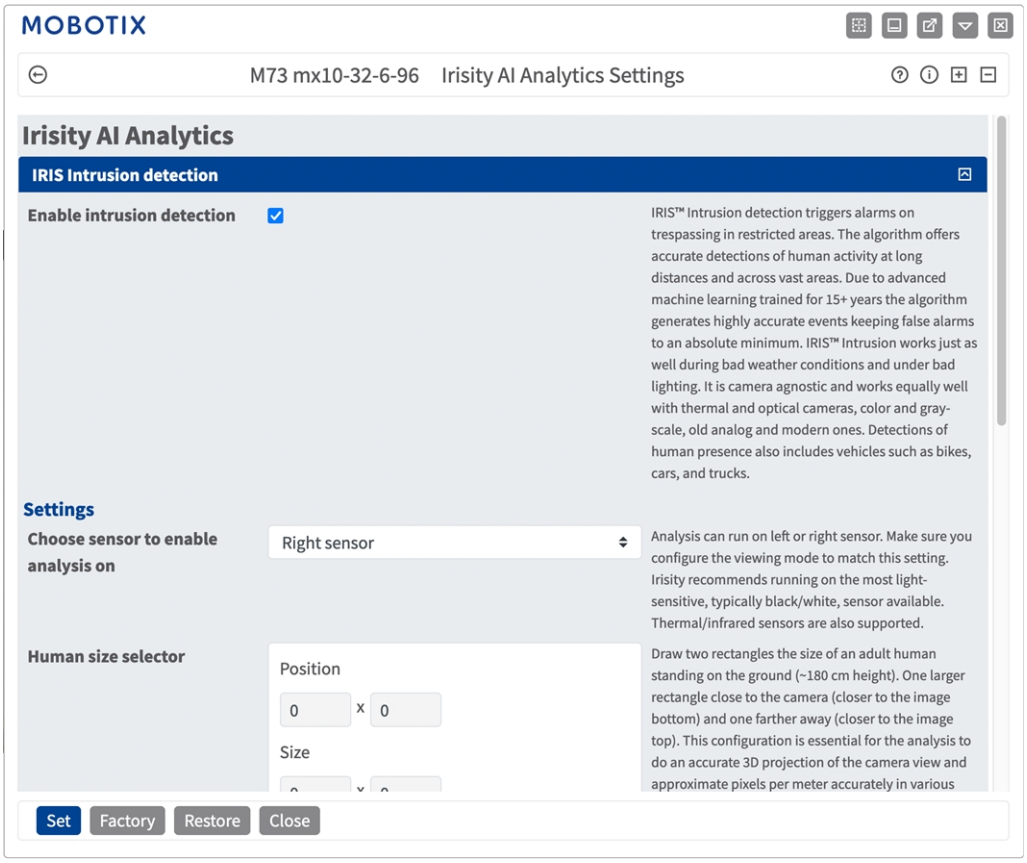


Fig. 14: Default operating mode (modalità di funzionamento predefinita): Rilevamento intrusioni IRIS

Enable intrusion detection (Attiva la rilevazione intrusioni): Selezionare per attivare l'algoritmo

Impostazioni

- **Scegliere il sensore per abilitare l'analisi su:** Selezionare il sensore da utilizzare per l'analisi delle immagini.
- **Selettore grandezza naturale:** questa configurazione è essenziale affinché l'analisi esegua una proiezione 3D accurata della vista della videocamera e approssimi i pixel per metro con precisione in varie parti dell'immagine (vedere Rilevamento manomissione IRIS, p. 23).
- **Zone di allarme:** è necessario definire almeno una zona di allarme (area di rilevamento) nell'immagine live (vedere Zone di allarme, p. 24).
- **Rileva tipo di oggetto:** selezionare un filtro per attivare solo su esseri umani o veicoli. Per impostazione predefinita, i rilevamenti includono tutti i movimenti a propulsione umana come pedoni, biciclette, auto e camion.

Impostazioni avanzate

- **Tempo di recupero zona allarme:** numero di secondi in cui una zona di allarme viene disattivata dopo l'attivazione di un allarme.
- **Tempo di recupero evento:** numero di secondi in cui un allarme disattiva ulteriori rilevamenti dallo stesso oggetto in allarme, compresi gli oggetti vicini.
- **Sensibilità:** livello di sensibilità per gli oggetti da classificare come attività umana. Il livello medio è consigliato nella maggior parte dei casi.

Rilevamento manomissione IRIS

Qui è possibile configurare le funzioni di rilevamento delle manomissioni.

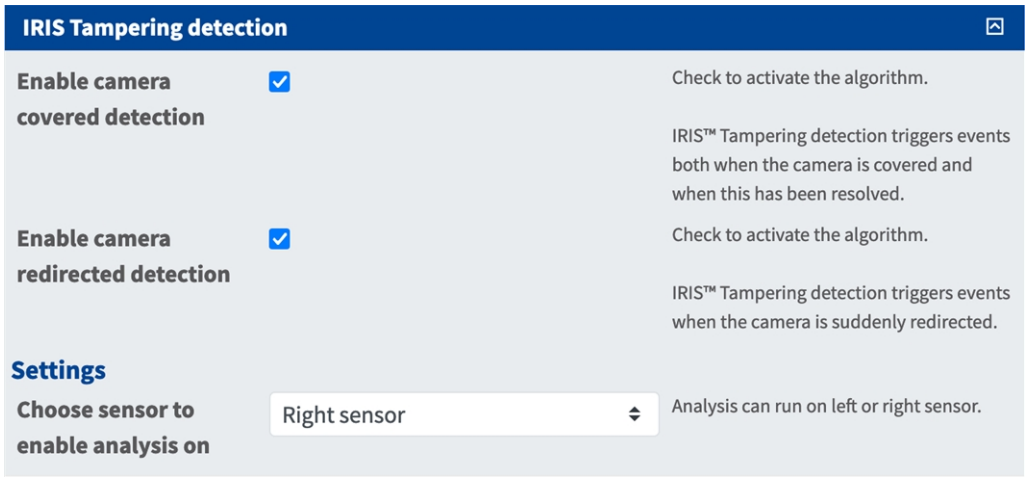


Fig. 15: Rilevamento manomissione IRIS

Abilita rilevamento copertura videocamera: selezionare per attivare l'algoritmo.

AVISSO! Il rilevamento della manomissione IRIS™ attiva gli eventi sia quando la videocamera è coperta sia quando questo problema è stato risolto.

Abilita rilevamento riorientamento videocamera: abilita il rilevamento del riorientamento della videocamera.

AVISSO! Il rilevamento della manomissione IRIS™ attiva gli eventi quando la videocamera viene improvvisamente riorientata.

Scegliere il sensore per abilitare l'analisi su: selezionare il sensore su cui eseguire l'analisi.

Disegnare un selettore grandezza naturale

1. Nella vista live, è sufficiente fare clic e trascinare un'area di riconoscimento rettangolare.
2. Trascinare i punti d'angolo per perfezionare l'area di riconoscimento.
3. Nell'angolo in alto a destra della vista live, fare clic su **Invia** per adottare le coordinate del rettangolo.

Zone di allarme

È possibile impostare una o più zone di allarme (aree di rilevamento). Se lasciate vuote, l'intera immagine verrà utilizzata per i rilevamenti.

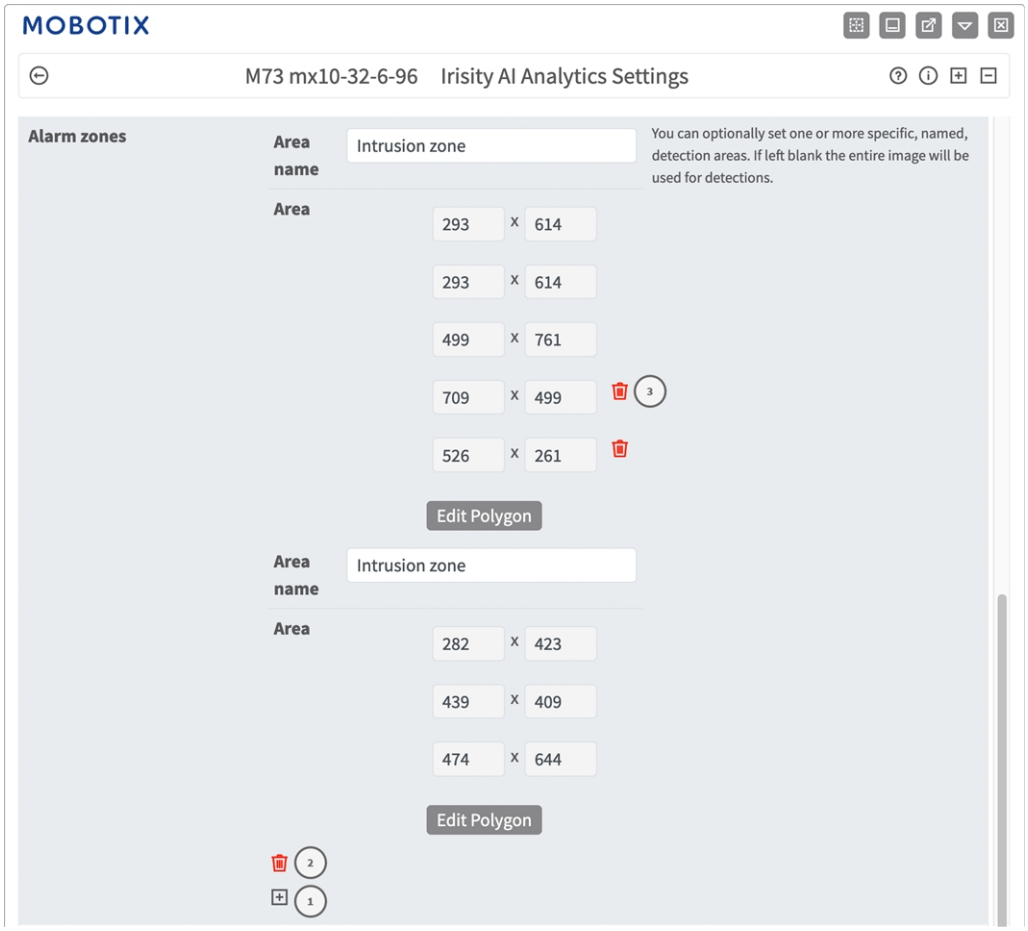


Fig. 16: Zone di allarme

Nome area: immettere un nome univoco per identificare la zona di allarme.

Area: i punti d'angolo definiti della zona di allarme. Fare clic su **Modifica poligono** ① per disegnare l'area di rilevamento nella vista live (vedere Come disegnare un'area a forma di poligono nella vista live, p. 26

Aggiungi una zona di allarme: fare clic sull'icona **più** ② per definire una nuova zona di allarme.

Eliminare un'area: Se lo si desidera, fare clic sull'icona del **cestino** ② per eliminare l'area di riconoscimento.

Sovrapposizioni visuali

Qui è possibile selezionare oggetti e dati del rilevamento intrusioni IRIS da visualizzare nell'immagine live.

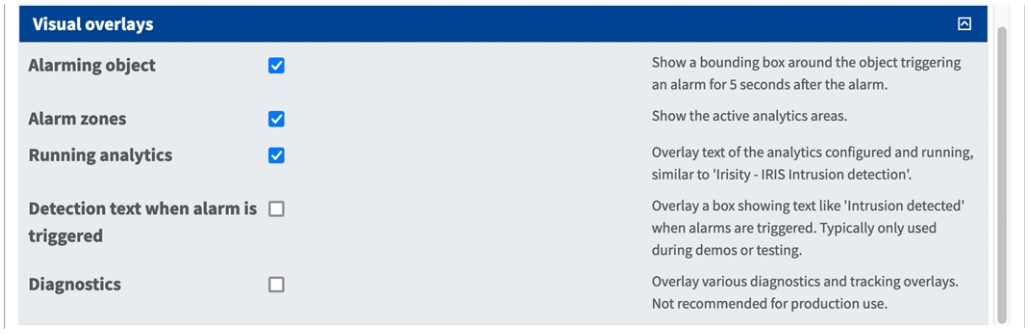


Fig. 17: Sovrapposizioni visuali

Oggetto che attiva l'allarme: Selezionare per mostrare un rettangolo di selezione intorno all'oggetto che attiva un allarme per 5 secondi dopo l'allarme.

Zone di allarme: Selezionare per mostrare le aree di analisi attive.

Analisi in esecuzione: Selezionare per sovrapporre il testo dell'analisi configurata e in esecuzione, ad es. "Irisity - rilevamento intrusioni IRIS".

Testo di rilevamento all'attivazione dell'allarme: Sovrapporre una casella di testo come "intrusione rilevata" quando gli allarmi vengono attivati.

Diagnostica: Selezionare per sovrapporre diverse diagnostiche e tracciamenti, ad es. per il debug.

Come disegnare un'area a forma di poligono nella vista live

Nella vista live è possibile disegnare aree in base ai poligoni, a seconda dell'applicazione. Queste aree sono ad esempio aree di rilevamento, aree escluse, aree di riferimento, ecc.

1. Nella vista live, è sufficiente fare clic e trascinare un'area rettangolare.
2. Trascinare i punti d'angolo nella posizione desiderata.
3. Per aggiungere un altro punto d'angolo, trascinare un punto più piccolo tra due punti d'angolo sul contorno dell'area.
4. Nell'angolo in alto a destra della vista live, fare clic su **Invia** per adottare le coordinate del poligono.
5. Se lo si desidera, fare clic sull'icona del **cestino** per eliminare l'area di riconoscimento.

Sovrapposizioni visuali

Qui è possibile selezionare oggetti e dati del rilevamento intrusioni IRIS da visualizzare nell'immagine live.

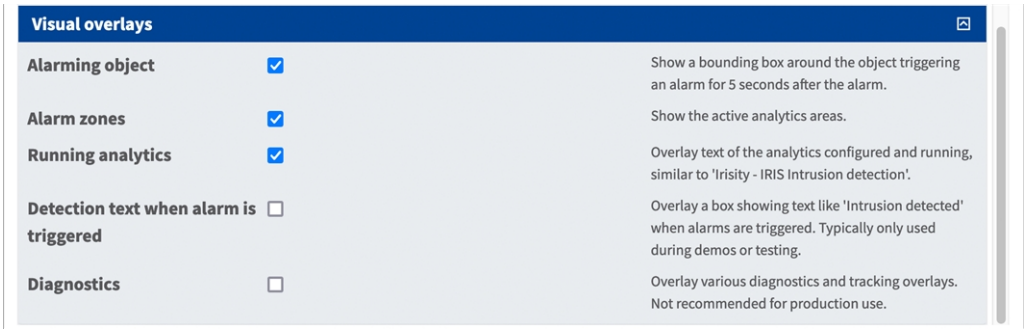


Fig. 18: Sovrapposizioni visuali

Oggetto che attiva l'allarme: Selezionare per mostrare un rettangolo di selezione intorno all'oggetto che attiva un allarme per 5 secondi dopo l'allarme.

Zone di allarme: Selezionare per mostrare le aree di analisi attive.

Analisi in esecuzione: Selezionare per sovrapporre il testo dell'analisi configurata e in esecuzione, ad es. "Irisity - rilevamento intrusioni IRIS".

Testo di rilevamento: Sovrapporre una casella di testo come "intrusione rilevata" quando gli allarmi vengono attivati.

Diagnostica: Selezionare per sovrapporre diverse diagnostiche e tracciamenti, ad es. per il debug.

Come memorizzare la configurazione

Per memorizzare la configurazione sono disponibili le seguenti opzioni:

Fig. 19: Come memorizzare la configurazione

- Fare clic sul pulsante **Set (Imposta)** per attivare le impostazioni inserite e salvarle fino al successivo riavvio della telecamera.
- Fare clic sul pulsante **Factory (Fabbrica)** per caricare le impostazioni predefinite in fabbrica per la finestra di dialogo in questione (questo pulsante potrebbe non essere presente in tutte le finestre di dialogo).
- Fare clic sul pulsante **Restore (Ripristina)** per annullare le modifiche più recenti effettuate che non sono state memorizzate nella telecamera in modo permanente.
- Fare clic sul pulsante **Close (Chiudi)** per chiudere la finestra di dialogo. Durante la chiusura della finestra di dialogo, il sistema verifica l'eventuale presenza di modifiche nell'intera configurazione. Se vengono rilevate delle modifiche, viene richiesto se si desidera memorizzare l'intera configurazione in modo permanente.

Una volta che la configurazione è stata correttamente salvata, l'evento e i metadati vengono automaticamente inviati alla telecamera nel caso di un evento.

MxMessageSystem

Che cos'è MxMessageSystem?

MxMessageSystem è un sistema di comunicazione basato su messaggi orientati al nome. Ciò significa che un messaggio deve avere un nome univoco con una lunghezza massima di 32 byte.

Ogni partecipante può inviare e ricevere messaggi. Le telecamere MOBOTIX sono anche in grado di inoltrare messaggi all'interno della rete locale. In questo modo, gli MxMessage possono essere distribuiti all'interno dell'intera rete locale (vedere Area messaggi: Globale).

Ad esempio, una videocamera MOBOTIX della serie 7 può scambiare un MxMessage generato da un'applicazione videocamera con una videocameraMx6 che non supporta le applicazioni MOBOTIX certificate.

Informazioni sugli MxMessage

- La crittografia a 128 bit garantisce la privacy e la sicurezza del contenuto dei messaggi.
- Gli MxMessage possono essere distribuiti da qualsiasi telecamera della serie Mx6 e 7.
- Il raggio di distribuzione del messaggio può essere definito singolarmente per ciascun MxMessage.
  - **Locale:** la videocamera prevede un MxMessage distribuito all'interno del proprio sistema di videocamere (ad esempio tramite un'applicazione certificata).
  - **Globale:** la videocamera prevede un MxMessage distribuito all'interno della rete locale da un altro dispositivo MxMessage (ad esempio, un'altra videocamera della serie 7 dotata di un'applicazione MOBOTIX certificata).
- Le azioni che i destinatari devono eseguire vengono configurate singolarmente per ciascun partecipante del sistema MxMessageSystem.

MxMessageSystem: elaborazione degli eventi dell'applicazione generati automaticamente

Controllo degli eventi dell'applicazione generati automaticamente

AVISSO! Dopo la corretta attivazione dell'applicazione (vedere Attivazione dell'interfaccia dell'applicazione certificata, p. 20), nella telecamera viene generato automaticamente un evento messaggio generico relativamente a tale applicazione specifica.

1. Accedere a **Setup Menu / Event Control / Event Overview** (Menu Setup / Controllo eventi / Panoramica eventi). Nella sezione **Eventi messaggio**, il profilo dell'evento messaggio generato automaticamente viene denominato come l'applicazione (ad es. IRIS).

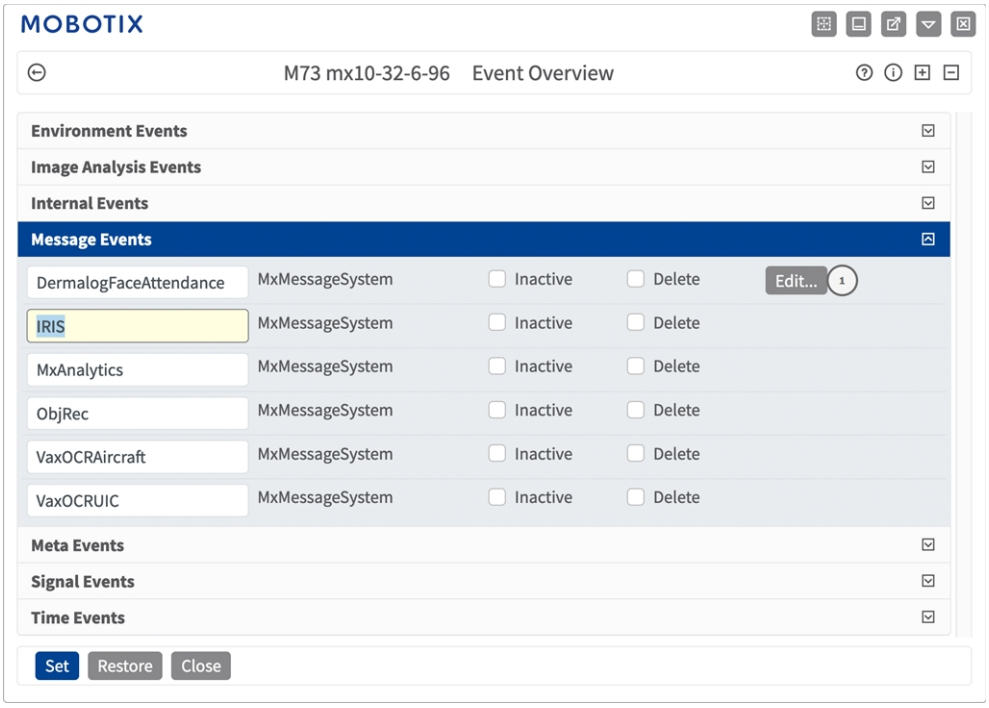


Fig. 20: Esempio: evento messaggio generico da Irisity IRIS AI Analytics - Intrusion Detection

2. Fare clic su **Edit** (Modifica)① per visualizzare una selezione di tutti gli eventi messaggio configurati.

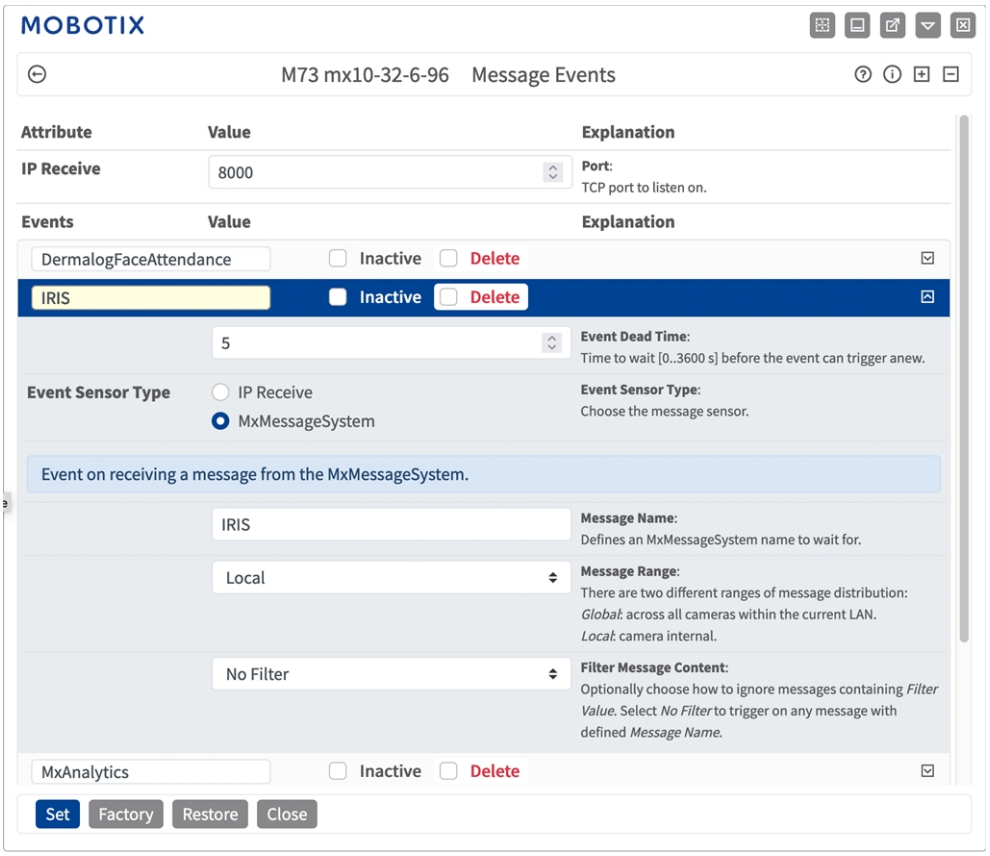


Fig. 21: Esempio: Dettagli evento messaggio generico - senza filtro

Gestione delle azioni - Configurazione di un gruppo di azioni

ATTENZIONE! Per utilizzare eventi, attivare gruppi di azioni o registrare immagini, è necessario abilitare l'attivazione generale della telecamera (http(s)/<Indirizzo IP telecamera>/control/settings)

Un gruppo di azioni definisce quali azioni vengono attivate dall'evento Irisity IRIS AI Analytics - Intrusion Detection.

1. Nell'interfaccia Web della telecamera, aprire: **Setup Menu / Action Group Overview (Menu Setup / Panoramica gruppo azioni)** (http(s)://<Camera IP address>/control/actions).

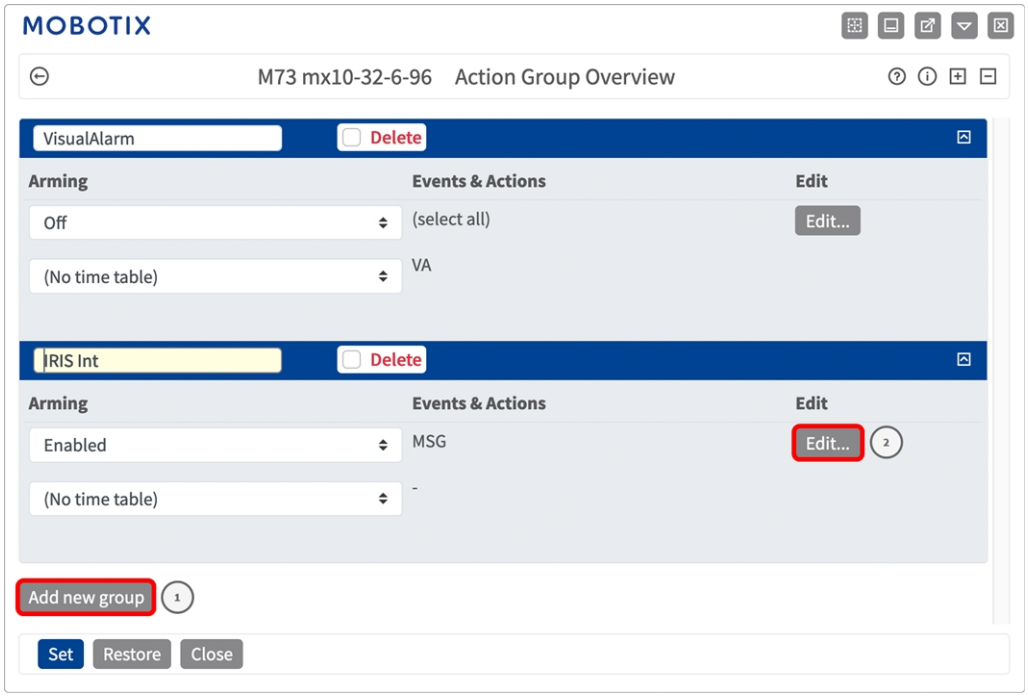


Fig. 22: Definizione dei gruppi di azioni

2. Fare clic su **Add new group**① (Aggiungi nuovo gruppo) e assegnare un nome significativo.
3. Fare clic su **Modifica**② per configurare il gruppo.

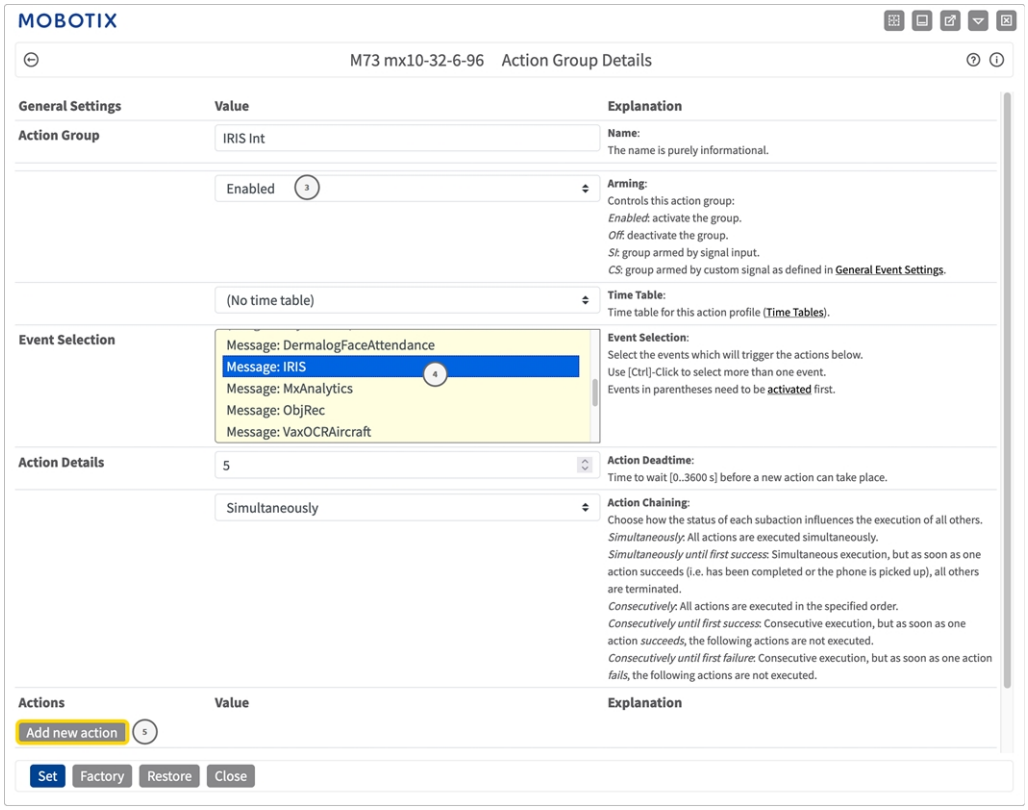


Fig. 23: Configurazione di un gruppo di azioni

4. Abilitare l'opzione **Arming (Attivazione)**③ del gruppo di azioni.
5. Selezionare l'evento messaggio desiderato nell'elenco **Event Selection** (Selezione eventi) ④ . Per selezionare più eventi, tenere premuto il tasto Maiusc.
6. Fare clic su **Add new Action** (**Aggiungi nuova azione)**⑤ .
7. Selezionare un'azione appropriata dall'elenco **Action Type and Profile** (**Tipo e profilo azione)**⑥ .

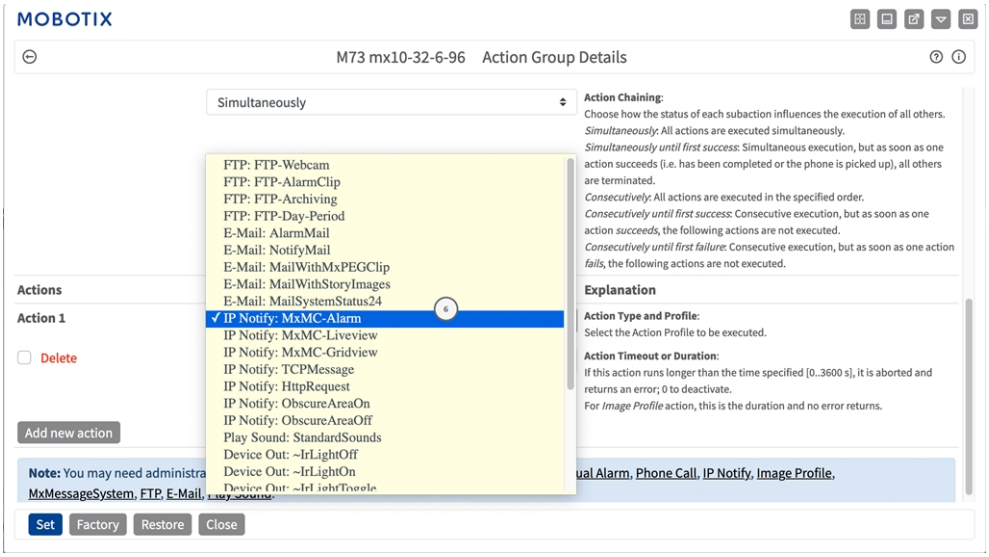


Fig. 24: Selezione del tipo e del profilo dell'azione

AVISSO! Se il profilo dell'azione richiesto non è ancora disponibile, è possibile creare un nuovo profilo nelle sezioni dell'Admin Menu (Menu Amministrazione) "MxMessageSystem", "Transfer Profiles" (Profili di trasferimento) e "Audio and VoIP Telephony" (Audio e telefonia VoIP).

Se necessario, è possibile aggiungere ulteriori azioni, facendo nuovamente clic sul pulsante. In tal caso, assicurarsi che la "concatenazione delle azioni" sia configurata correttamente (es. azioni contemporanee).

8. Fare clic sul pulsante **Imposta** in fondo alla finestra di dialogo per confermare le impostazioni.

Impostazioni delle azioni - Configurazione delle registrazioni della telecamera

1. Nell'interfaccia Web della telecamera, aprire: **Setup Menu / Event Control / Recording (Menu Setup / Controllo eventi / Registrazione)**(http(s)/<Camera IP address>/control/recording).

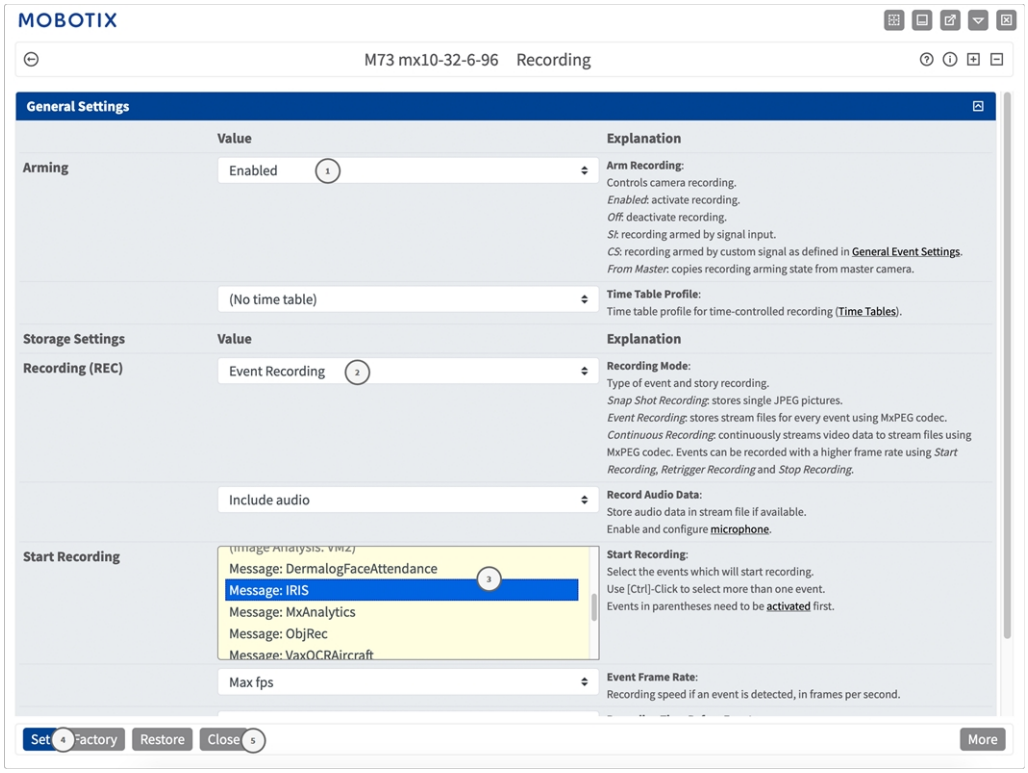


Fig. 25: Configurazione delle impostazioni di registrazione della telecamera

2. Attivare l'opzione **Arm Recording (Attiva registrazione)**① .
3. In **Impostazioni di archiviazione/Registrazione (REC)** selezionare una **Modalità di registrazione** ② .
   Sono disponibili le seguenti modalità:
   - Registrazione istantanea
   - Registrazione eventi
   - Registrazione continua
4. Nell'elenco **Start Recording** (**Avvia registrazione**)③ , selezionare l'evento messaggio appena creato.
5. Fare clic sul pulsante **Set (Imposta)**④ in fondo alla finestra di dialogo per confermare le impostazioni.
6. Fare clic su **Close (Chiudi)**⑤ per salvare le impostazioni in modo permanente.

AVISSO! In alternativa, è possibile salvare le impostazioni dal menu Amministrazione in Configurazione/Salva configurazione corrente nella memoria permanente.

MxMessageSystem: elaborazione dei metadati trasmessi dalle applicazioni

Metadati trasferiti all'interno del sistema MxMessageSystem

Per ogni evento, l'applicazione trasferisce alla telecamera anche dei metadati. Tali dati vengono inviati sotto forma di uno schema JSON all'interno di un MxMessage.

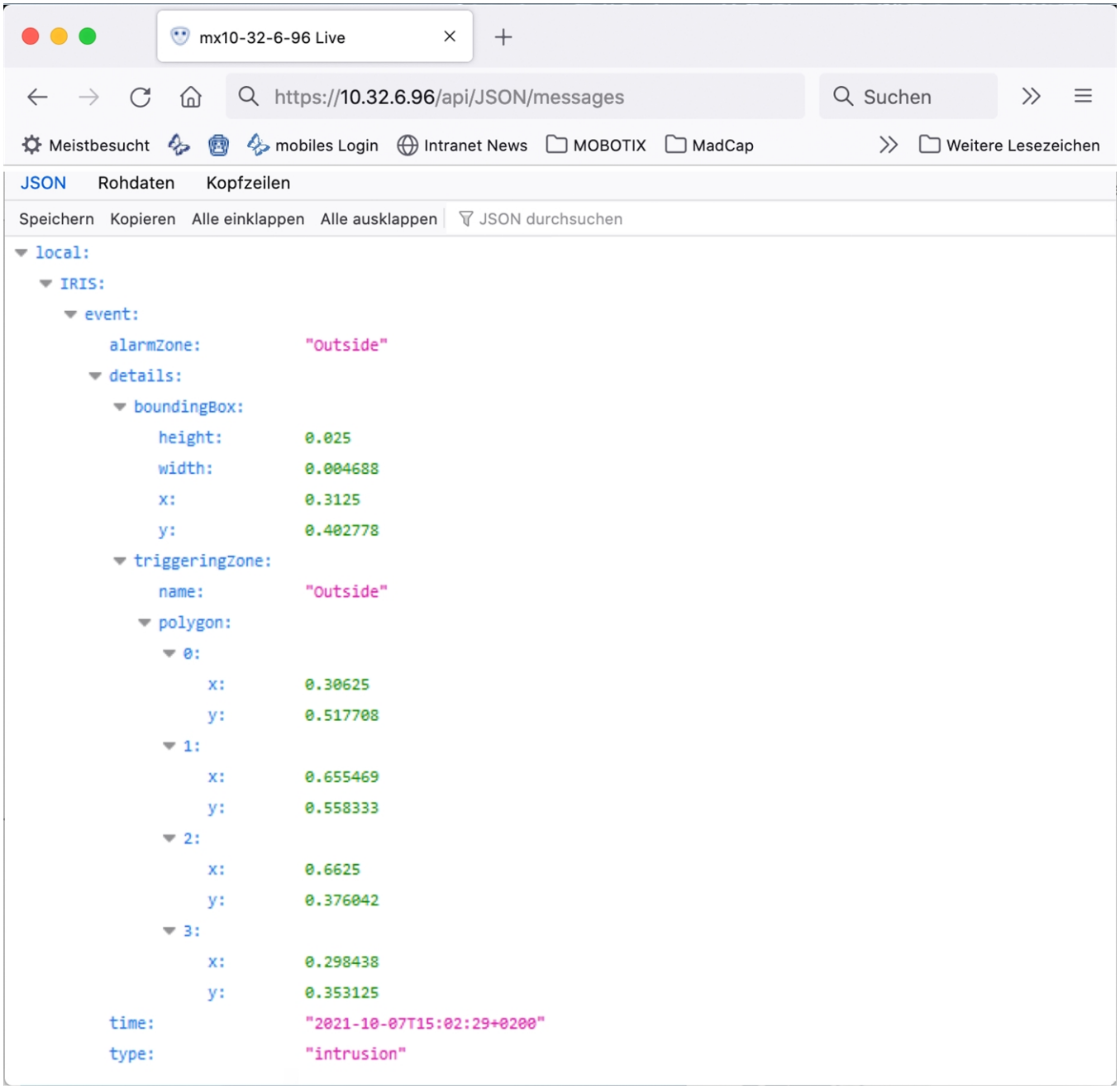


Fig. 26: Esempio: metadati trasmessi all'interno di un MxMessage di Irisity IRIS AI Analytics - Intrusion Detection

AVISSO! Per visualizzare la struttura dei metadati dell'ultimo evento dell'applicazione, inserire il seguente URL nella barra degli indirizzi del browser: http(s)/IndirizzoIPDellaTelecamera/api/json/messages

Creazione di un evento messaggio personalizzato

1. Accedere a **Setup Menu / Event Control / Event Overview** (Menu Setup / Controllo eventi / Panoramica eventi). Nella sezione **Eventi messaggio**, il profilo dell'evento messaggio generato automaticamente viene denominato come l'applicazione (ad es. IRIS).

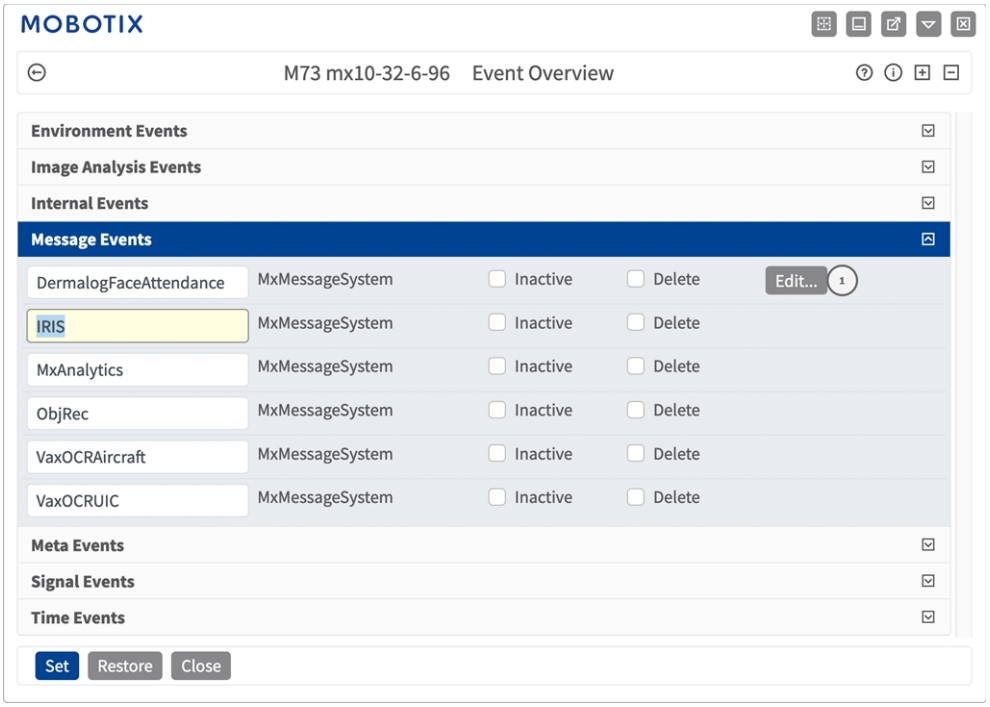


Fig. 27: Esempio: Evento messaggio generico da Irisity IRIS AI Analytics - Intrusion Detection

2. Fare clic su **Edit** (Modifica)① per visualizzare una selezione di tutti gli eventi messaggio configurati.

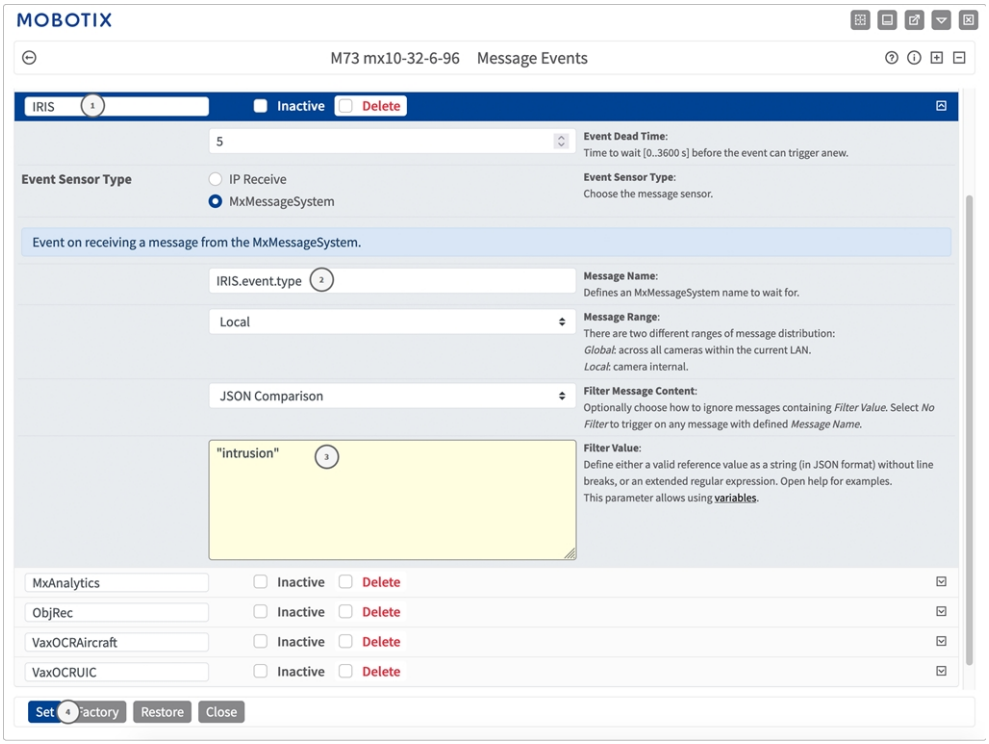


Fig. 28: Esempio: Evento messaggio intrusione

3. Fare clic sull'evento (ad es. IRIS) ① per aprire le impostazioni evento.
4. Configurare i parametri del profilo dell'evento come segue:

- **Message Name (Nome messaggio):** Inserire il nome messaggio ② in base alla documentazione dell'evento dell'applicazione corrispondente (vedere Esempi di nomi di messaggi e valori di filtro dell'applicazione Irisity IRIS AI Analytics - Intrusion Detection, p. 38)
- **Message Range (Raggio di distribuzione messaggio):**
  - **Locale:** impostazioni predefinite per l'applicazione Irisity IRIS AI Analytics - Intrusion Detection
  - **Global (Globale):** l'MxMessage viene inoltrato nella rete locale da un'altra telecamera MOBOTIX
- **Filter Message Content (Filtra contenuto messaggi):**
  - **Evento generico:** "No Filter" (Nessun filtro)
  - **Evento filtrato:** "Confronto JSON"
- **Filter Value (Valore di filtro):** ③ vedere Esempi di nomi di messaggi e valori di filtro dell'applicazione Irisity IRIS AI Analytics - Intrusion Detection, p. 38.

ATTENZIONE! L'opzione "Filter Value" (Valore di filtro) viene utilizzata per differenziare gli MxMessage di un'applicazione/bundle. Utilizzare questa opzione per beneficiare dei singoli tipi di eventi delle applicazioni (se disponibili).

Selezionare "No Filter" (Nessun filtro) se si desidera utilizzare tutti gli MxMessage in entrata come evento generico dell'applicazione correlata.

2. Fare clic sul pulsante **Imposta**④ in fondo alla finestra di dialogo per confermare le impostazioni.

Esempi di nomi di messaggi e valori di filtro dell'applicazione Irisity IRIS AI Analytics - Intrusion Detection

IRIS Intrusion Detection (Rilevamento intrusioni)	Nome MxMessage	Valore di filtro
Evento generico	IRIS	
Evento zona allarme	IRIS.event.alarmZone	Nome della zona di allarme, ad es.: "Zona di intrusione 2"
Tipo di evento	IRIS.event.type	"intrusione"

MOBOTIX

BeyondHumanVision

IT_03/23

MOBOTIX AG • Kaiserstrasse • D-67722 Langmeil • Tel.: +49 6302 9816-103 • sales@mobotix.com • www.mobotix.com