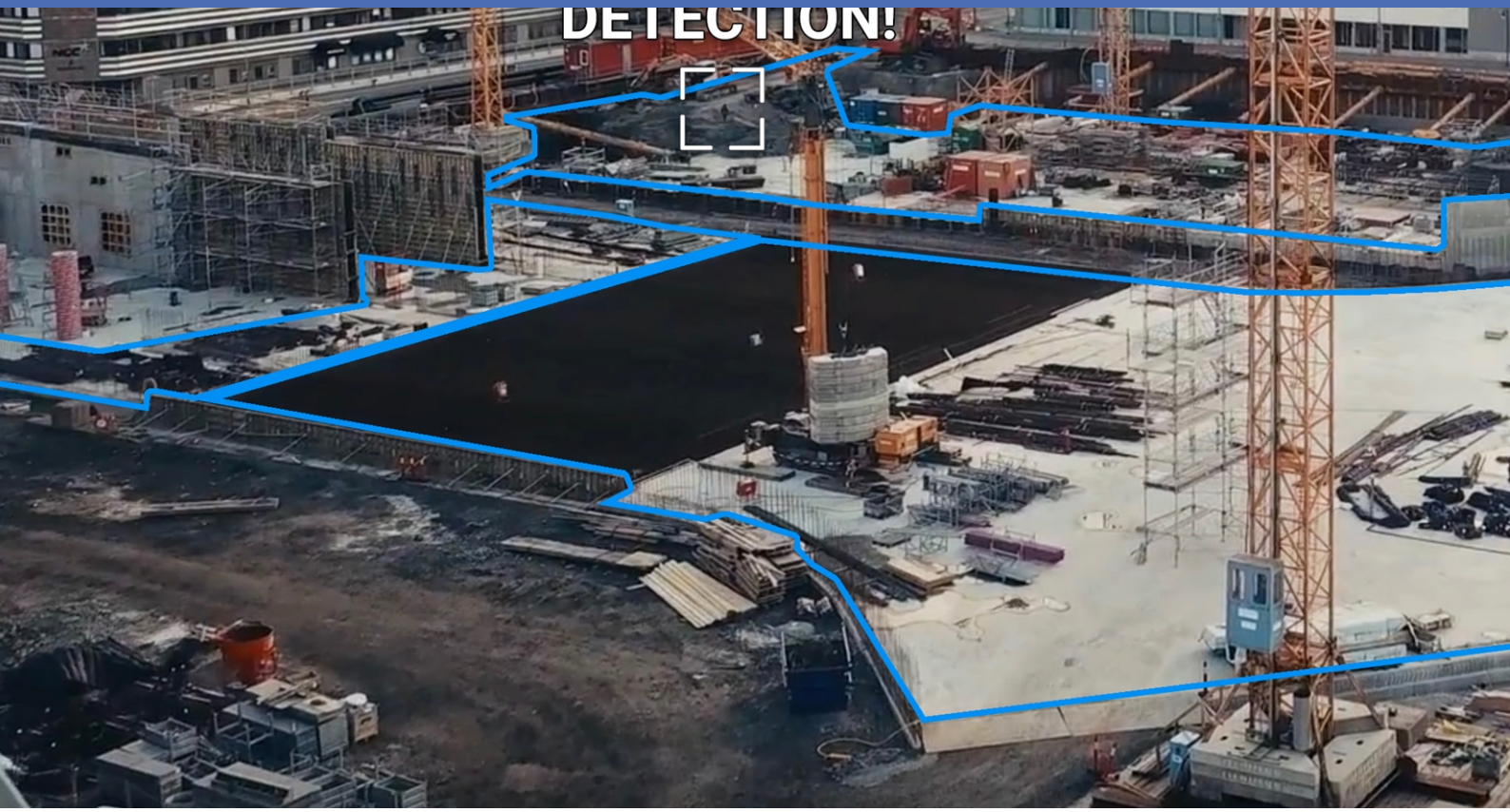
Leitfaden

Irisity IRIS AI Analytics - Intrusion Detection



BeyondHumanVision

MOBOTIX

V1.09_16.03.2023, Bestellcode: Mx-APP-IRIS-C-INT

Inhaltsverzeichnis

1

Bevor Sie beginnen

Support

Sollten Sie technische Unterstützung benötigen, wenden Sie sich bitte an Ihren MOBOTIX-Händler. Wenn Ihre Fragen nicht sofort beantwortet werden können, wird Ihr Vertriebspartner Ihre Anfragen über die entsprechenden Kanäle weiterleiten, um eine schnelle Antwort zu gewährleisten.

Ist ein Internetzugang vorhanden, können Sie im MOBOTIX-Helpdesk zusätzliche Dokumentation und Software-Updates herunterladen. Besuchen Sie dazu:

www.mobotix.com > Support > Help Desk

Sicherheitshinweise

- Die Verwendung dieses Produkts in explosionsgefährdeten Bereichen ist nicht zulässig.
- Verwenden Sie dieses Produkt keinesfalls in staubigen Umgebungen.
- Schützen Sie dieses Produkt vor Feuchtigkeit und vor Eindringen von Wasser.
- Installieren Sie dieses Produkt gemäß der vorliegenden Dokumentation. Fehlerhafte Montage kann Schäden am Produkt verursachen!
- Dieses Gerät darf nicht für Kinder zugänglich sein.
- Das Anschlusskabel für das Netzteil darf nur an eine Steckdose mit Erdkontakt angeschlossen werden.
- Um die Anforderungen der EN 50130-4 (Stromversorgung von Alarmsystemen für unterbrechungsfreien Betrieb) zu erfüllen, wird dringend empfohlen, die Spannungsversorgung dieses Produkts mit einer unterbrechungsfreien Stromversorgung (USV) abzusichern.
- Dieses Gerät darf nur in PoE-Netzwerken angeschlossen werden, und es darf nicht außerhalb des Netzwerks geroutet werden.

Rechtliche Hinweise

Rechtliche Aspekte der Video- und Audioaufzeichnung

Beim Einsatz von MOBOTIX AG Produkten sind die Datenschutzbestimmungen für Video- und Audioaufzeichnungen zu beachten. Je nach Landesgesetz und Aufstellungsort der Kameras kann die Aufzeichnung von Video- und Audiodaten besonderen Auflagen unterliegen oder untersagt sein. Alle Anwender von MOBOTIX Produkten sind daher aufgefordert, sich über die aktuell gültigen Bestimmungen zu informieren und diese zu befolgen. Die MOBOTIX AG übernimmt keine Verantwortung für einen nicht legalitätskonformen Produktgebrauch.

Konformitätserklärung

Die Produkte der MOBOTIX AG werden nach den anwendbaren Richtlinien der EU sowie weiterer Länder zertifiziert. Die Konformitätserklärungen für die Produkte von MOBOTIX AG finden Sie auf www.mobotix.com unter **Support > Download Center > Marketing & Documentation (Marketing & Dokumentation) > Certificates & Declarations of Conformity (Zertifikate & Konformitätserklärungen)**.

RoHS-Erklärung

Die Produkte von MOBOTIX AG sind konform mit den Anforderungen, die sich aus §5 ElektroG bzw. der RoHS-Richtlinie 2011/65/EU ergeben, soweit sie in den Anwendungsbereich dieser Regelungen fallen (die RoHS-Erklärung von MOBOTIXfinden Sie unter www.mobotix.com unter **Support > Download Center > Marketing & Documentation (Marketing & Dokumentation) > Brochures & Guides (Broschüren & Anleitungen) > Certificates (Zertifikate)**).

Entsorgung

Elektrische und elektronische Produkte enthalten viele Wertstoffe. Entsorgen Sie deshalb die Produkte von MOBOTIX am Ende ihrer Lebensdauer gemäß den geltenden gesetzlichen Bestimmungen und Vorschriften (beispielsweise bei einer kommunalen Sammelstelle abgeben). Produkte von MOBOTIX dürfen nicht in den Hausmüll gegeben werden! Entsorgen Sie einen im Produkt evtl. vorhandenen Akku getrennt vom Produkt (die jeweiligen Produkthandbücher enthalten einen entsprechenden Hinweis, wenn das Produkt einen Akku enthält).

Haftungsausschluss

Die MOBOTIX AG haftet nicht für Schäden, die durch unsachgemäße Handhabung seiner Produkte, dem Nichtbeachten der Bedienungsanleitungen sowie der relevanten Vorschriften entstehen. Es gelten die Allgemeinen Geschäftsbedingungen. Sie finden die jeweils gültige Fassung der **Allgemeinen Geschäftsbedingungen** auf www.mobotix.com, indem Sie auf den entsprechenden Link unten auf jeder Seite klicken.

Informationen zu Irisity IRIS AI Analytics - Intrusion Detection

Menschliche Aktivität in Alarmzonen erkennen

Irisity IRIS AI Analytics - Intrusion Detection löst Alarme bei unbefugtem Zutritt gesperrter Bereiche aus. Der Algorithmus ermöglicht eine präzise Erkennung menschlicher Aktivität auf großen Entfernungen und über weite Bereiche hinweg. Die Anwendung hat eine Genauigkeit von bis zu 99 %. Die App kann 30 Tage lang kostenlos getestet dann für unbegrenzte Zeit aktiviert werden. Es werden auch Fahrzeuge wie Fahrräder, Autos und Lastwagen erkannt – selbst bei schlechten Witterungsbedingungen und Lichtverhältnissen.

- Erkennt das Eindringen von relevanten Objekten in benutzerdefinierte Meldezonen/-bereiche
- Entwickelt für die zuverlässige Erkennung von Personen und Fahrzeugen, die nur kleine Bereiche des Sichtfeldes abdecken
- Reduziert Fehlalarme auf ein Minimum, indem nicht kritische Bewegungen ausgefiltert werden (z. B. Bäume, Wolken usw.)
- Gleichzeitige Erkennung auf einem oder mehreren Bildsensoren
- MOBOTIX-Ereignisse über MxMessageSystem
- Konsolidierte Ereignissuche über MxManagementCenter Smart Data Interface und/oder MOBOTIX HUB

VORSICHT! ECO-Thermalsensormodule werden von dieser App nicht unterstützt.

Smart Data-Schnittstelle zu MxManagementCenter

Diese App verfügt über eine Smart Data-Schnittstelle zu MxManagementCenter.

Mit dem MOBOTIX Smart Data-System können Transaktionsdaten mit der Videoaufzeichnung zum Zeitpunkt der jeweiligen Transaktion verknüpft werden. Als Smart Data-Quellen dienen z. B. MOBOTIX Certified Apps (keine Lizenz erforderlich) oder allgemeine Smart Data-Quellen (Lizenz erforderlich), mit denen Sie z. B. Kassensysteme oder Systeme zur Kennzeichenerkennung auswerten können.

Durch das Smart Data-System in MxManagementCenter können auffällige Aktivitäten schnell aufgefunden und überprüft werden. Zur Suche und zur Analyse der Transaktionen stehen die Smart Data-Leiste und die Smart Data-Ansicht zur Verfügung. Die Smart Data-Leiste gibt einen direkten Überblick über die letzten Transaktionen (der letzten 24 Stunden) und kann deshalb gut zur Kontrolle und zur schnellen Suche eingesetzt werden.

HINWEIS! Informationen zur Verwendung des Smart Data-Systems finden Sie in der entsprechenden Online-Hilfe zu Kamerasoftware und zu MxManagementCenter.

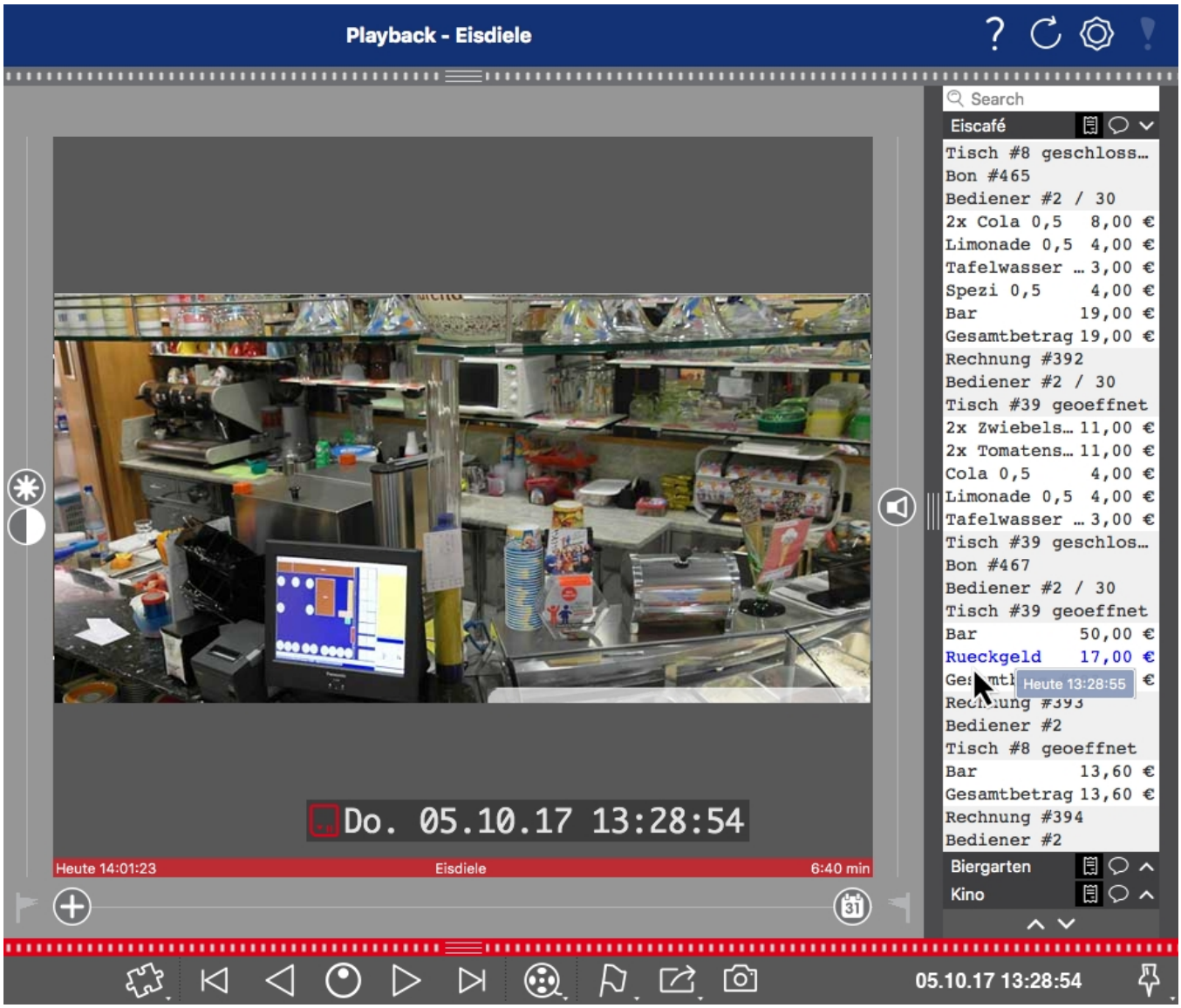


Abb. 1: : Smart Data-Leiste in MxManagementCenter (Beispiel: POS-System)

Technische Daten

Produktinformationen

Produktname	Irisity IRIS AI Analytics - Intrusion Detection
Bestellnummer	Mx-APP-IRIS-C-INT
Unterstützt MOBOTIX-Kameras	Mx-M73A, Mx-S74A
Erforderliche Kamera-Firmwareversion	V7.3.0.x
MxManagementCenter -Integration	■ Min. MxMC v2.5.3 ■ Konfiguration: Advanced Config-Lizenz erforderlich ■ Recherche: Smart Data-Schnittstellen-Lizenz im Lieferumfang enthalten

Produktfunktionen

App-Funktionen	■ Erkennt das Eindringen von relevanten Objekten in benutzerdefinierte Meldezonen/-bereiche ■ Entwickelt für die zuverlässige Erkennung von Personen und Fahrzeugen, die nur kleine Bereiche des Sichtfeldes abdecken ■ Reduziert Fehlalarme auf ein Minimum, indem nicht kritische Bewegungen ausgefiltert werden (z. B. Bäume, Wolken usw.) ■ Gleichzeitige Erkennung auf einem oder mehreren Bildsensoren ■ MOBOTIX-Ereignisse über MxMessageSystem ■ Konsolidierte Ereignissuche über MxManagementCenter Smart Data Interface und/oder MOBOTIX HUB
Maximale Anzahl an Erkennungszonen	20
Metadaten-/Statistikformate	JSON
Testlizenz	30-Tage-Testlizenz vorinstalliert
MxMessageSystem unterstützt	Ja

MOBOTIX-Ereignisse	Ja
ONVIF-Ereignisse	Ja (generisches Nachrichtenereignis)

Szenenanforderungen

Minimale Objekthöhe	20 px / ~6 % der Bildhöhe (Analyse derzeit auf eine Auflösung von 640 x 360 festgelegt)
Montagehöhe der Kamera	Min. 2 m (unter Berücksichtigung der Szenenanforderungen sind meist 5–20 m optimal)
Maximaler vertikaler Winkel	180°
Maximaler horizontaler Winkel	180°
Maximaler Neigungswinkel	Nur Neigung nach unten: keine Begrenzung

Technische App-Spezifikationen

Synchrone/ asynchrone App	Asynchron
Genauigkeit	>99 % (unter Berücksichtigung der Szenenanforderungen)
Verarbeitete Anzahl von Einzelbildern pro Sekunde	Typisch: 10 fps
Erkennungszeit	~ 2 Sek.

Lizenzierung der Certified Apps

Die folgenden Lizenzen sind verfügbar für Irisity IRIS AI Analytics - Intrusion Detection:

- **30-Tage-Testlizenz** vorinstalliert
- **Dauerhafte kommerzielle Lizenz**

Die Nutzungsdauer beginnt mit der Aktivierung der App-Schnittstelle (siehe Aktivierung der Certified App-Schnittstelle)

HINWEIS! Wenden Sie sich an Ihren MOBOTIX-Partner, wenn Sie eine Lizenz erwerben oder verlängern möchten.

HINWEIS! Apps werden in der Regel mit der Firmware vorinstalliert. In seltenen Fällen müssen Apps von der Website heruntergeladen und installiert werden. Lesen Sie in diesem Fall **www.mobotix.com > Support > Download Center > Marketing & Dokumentation**, um die App herunterzuladen und zu installieren.

Lizenzaktivierung zertifizierter Apps in MxManagementCenter

Nach Ablauf eines Testzeitraums müssen kommerzielle Lizenzen für die Verwendung mit einem gültigen Lizenzschlüssel aktiviert werden.

Online-Aktivierung

Aktivieren Sie die Apps in MxMC nach Erhalt der Aktivierungs-IDs wie folgt:

1. Wählen Sie im Menü **Fenster > Kamera-App-Lizenzen** aus.
2. Wählen Sie die Kamera aus, auf der Sie Apps lizenzieren möchten, und klicken Sie auf **Auswählen**.

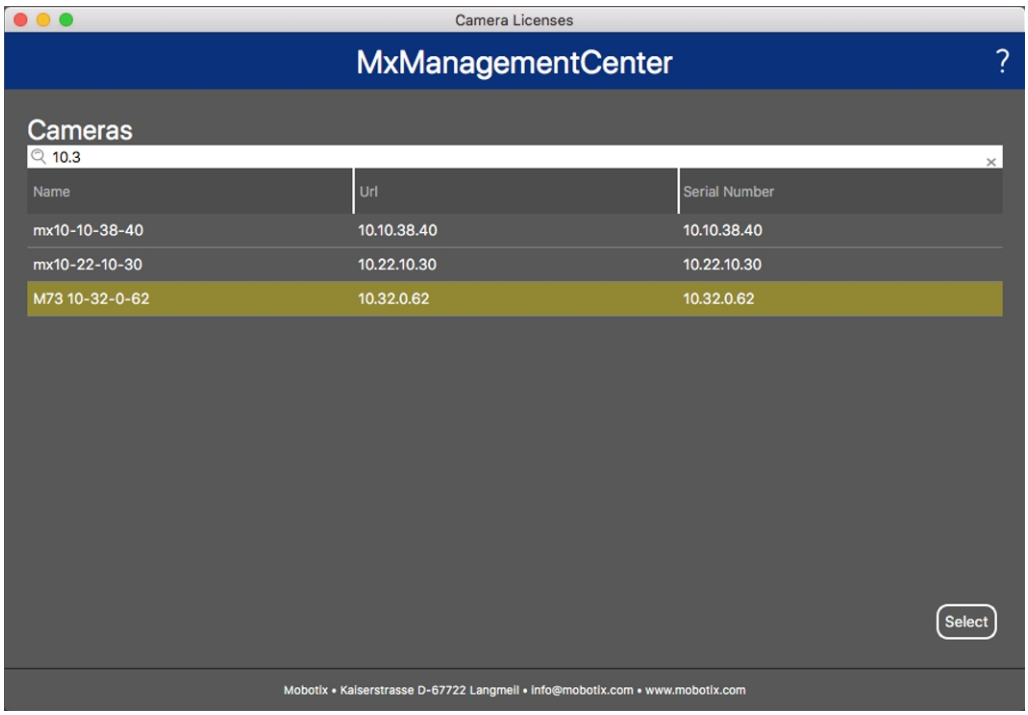


Abb. 2: Überblick über die Kamera-App-Lizenzen in MxManagementCenter

HINWEIS! Korrigieren Sie bei Bedarf die auf der Kamera eingestellte Uhrzeit.

1. Eine Übersicht der auf der Kamera installierten Lizenzen wird möglicherweise angezeigt. Klicken Sie auf **Lizenz aktivieren**.

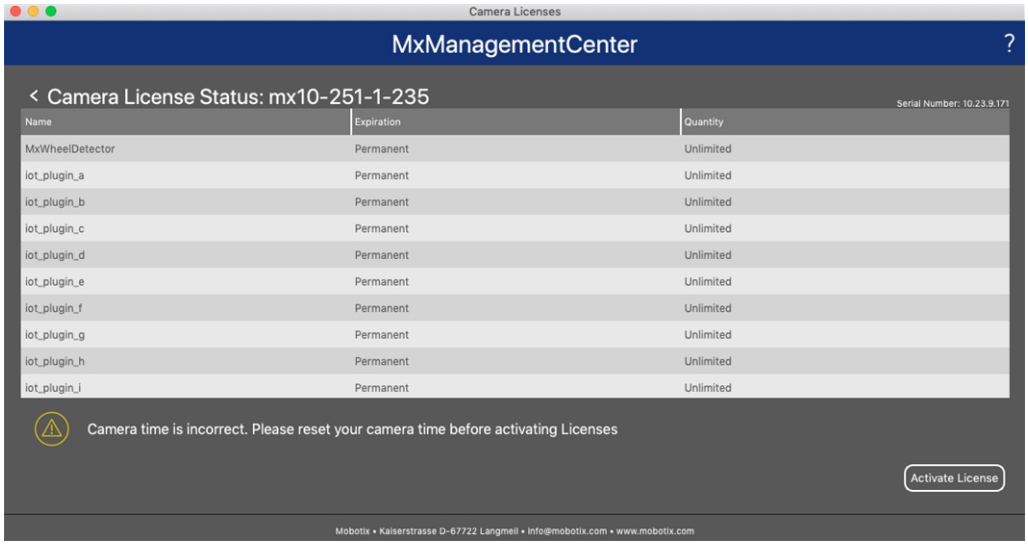


Abb. 3: Übersicht über die auf der Kamera installierten Lizenzen

HINWEIS! Korrigieren Sie bei Bedarf die auf der Kamera eingestellte Uhrzeit.

2. Geben Sie eine gültige Aktivierungs-ID ein und geben Sie die Anzahl der Lizenzen an, die auf diesem Computer installiert werden sollen.

3. Wenn Sie ein anderes Produkt lizenzieren möchten, klicken Sie auf . Geben Sie in der neuen Zeile die entsprechende Aktivierungs-ID und die Anzahl der gewünschten Lizenzen ein.
4. Um eine Zeile zu entfernen, klicken Sie auf .
5. Wenn Sie alle Aktivierungs-IDs eingegeben haben, klicken Sie auf **Lizenz online aktivieren**. Während der Aktivierung stellt **MxMC** eine Verbindung zum Lizenzserver her. Hierfür ist eine Internetverbindung erforderlich.

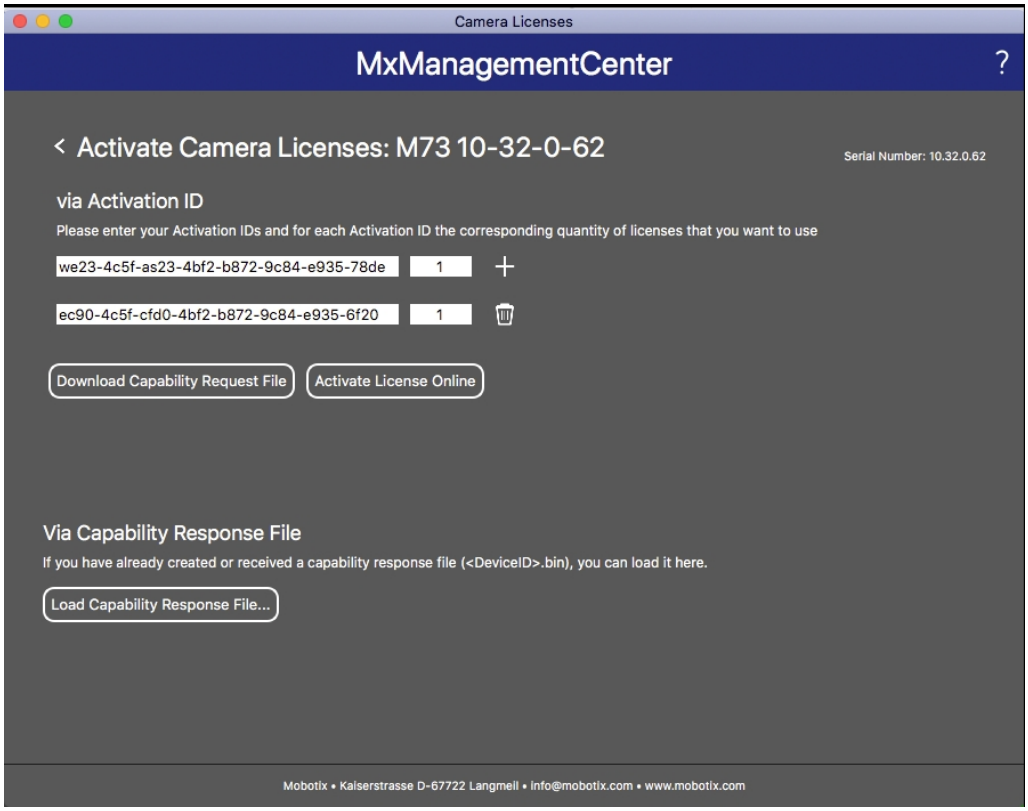


Abb. 4: Hinzufügen von Lizenzen

Aktivierung erfolgreich

Nach der erfolgreichen Aktivierung ist eine neue Anmeldung erforderlich, um die Änderungen zu übernehmen. Alternativ können Sie zur Lizenzverwaltung zurückkehren.

Aktivierung fehlgeschlagen (fehlende Internetverbindung)

Ist der Lizenzserver z. B. aufgrund einer fehlenden Internetverbindung nicht erreichbar, können Apps auch offline aktiviert werden. (Siehe Offline-Aktivierung, p. 12.)

Offline-Aktivierung

Für die Offline-Aktivierung kann der Partner/Techniker, von dem Sie die Lizenzen erworben haben, eine Funktionsantwort (.bin-Datei) auf dem Lizenzserver generieren, um die Lizenzen zu aktivieren.

1. Wählen Sie im Menü **Fenster > Kamera-App-Lizenzen** aus.
2. Wählen Sie die Kamera aus, auf der Sie Apps lizenzieren möchten, und klicken Sie auf **Auswählen**.

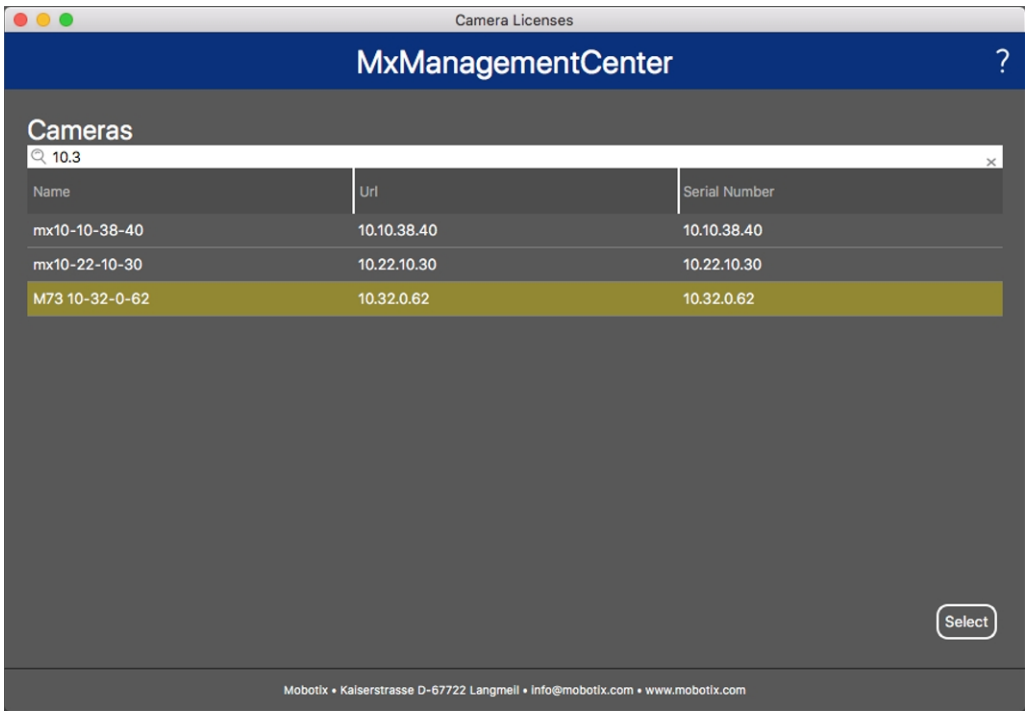


Abb. 5: Überblick über die Kamera-App-Lizenzen in MxManagementCenter

HINWEIS! Korrigieren Sie bei Bedarf die auf der Kamera eingestellte Uhrzeit.

3. Eine Übersicht der auf der Kamera installierten Lizenzen wird möglicherweise angezeigt. Klicken Sie auf **Lizenz aktivieren**.

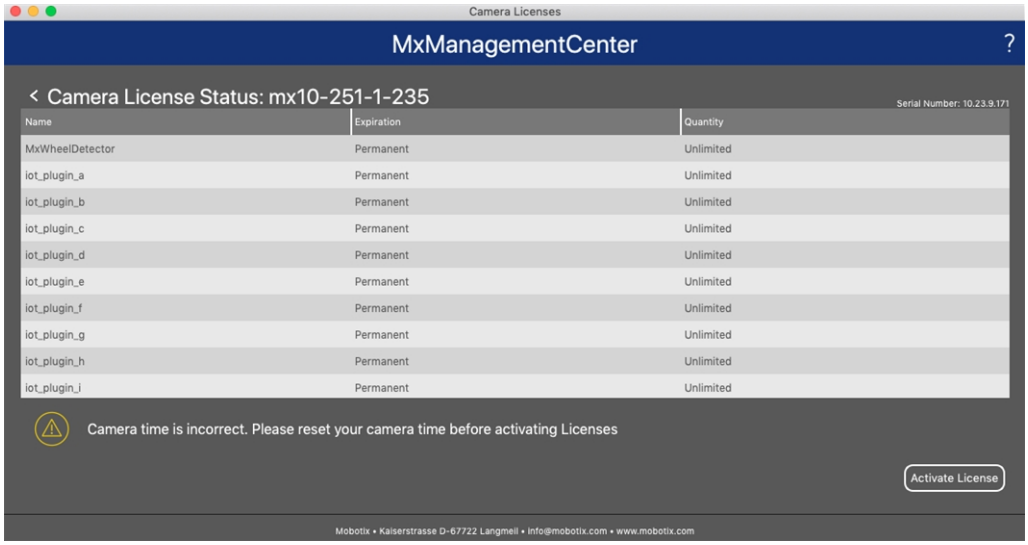


Abb. 6: Übersicht über die auf der Kamera installierten Lizenzen

HINWEIS! Korrigieren Sie bei Bedarf die auf der Kamera eingestellte Uhrzeit.

4. Geben Sie eine gültige Aktivierungs-ID ein und geben Sie die Anzahl der Lizenzen an, die auf diesem Computer installiert werden sollen.

5. Wenn Sie ein anderes Produkt lizenzieren möchten, klicken Sie auf |. Geben Sie in der neuen Zeile die entsprechende **Aktivierungs-ID** und die Anzahl der gewünschten Lizenzen ein.
6. Klicken Sie ggf. auf |, um eine Zeile zu entfernen.
7. Wenn Sie alle Aktivierungs-IDs eingegeben haben, klicken Sie auf **Funktionalitätsanforderungsdatei (.lic) herunterladen** und senden Sie diese an Ihren Partner/Techniker.

HINWEIS! Mit dieser Datei kann der Partner/Techniker, von dem Sie die Lizenzen erworben haben, eine Funktionalitätsantwortdatei (.bin) auf dem Lizenzserver generieren.

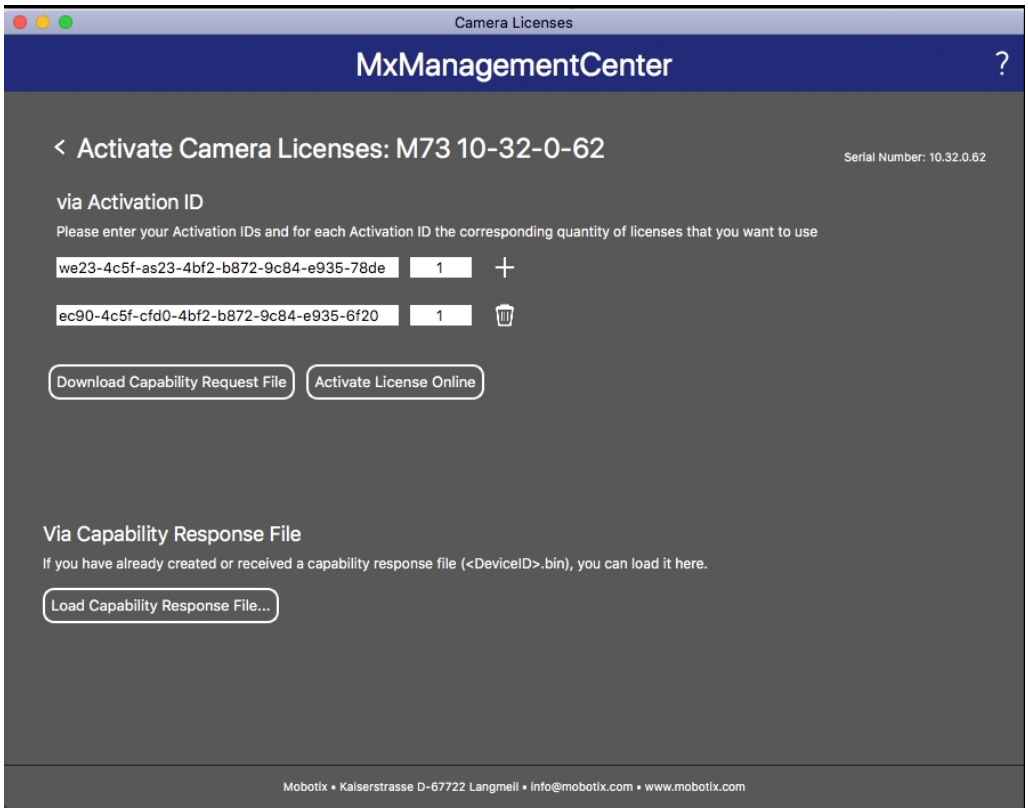


Abb. 7: Hinzufügen von Lizenzen

8. Klicken Sie auf „Funktionalitätsantwort-Datei laden“ und folgen Sie den Anweisungen.

Aktivierung erfolgreich

Nach der erfolgreichen Aktivierung ist eine neue Anmeldung erforderlich, um die Änderungen zu übernehmen. Alternativ können Sie zur Lizenzverwaltung zurückkehren.

Verwalten von Lizenzen in MxManagementCenter

In MxManagementCenter können Sie bequem alle Lizenzen verwalten, die für eine Kamera aktiviert wurden.

1. Wählen Sie im Menü **Fenster > Kamera-App-Lizenzen** aus.
2. Wählen Sie die Kamera aus, auf der Sie Apps lizenzieren möchten, und klicken Sie auf **Auswählen**.

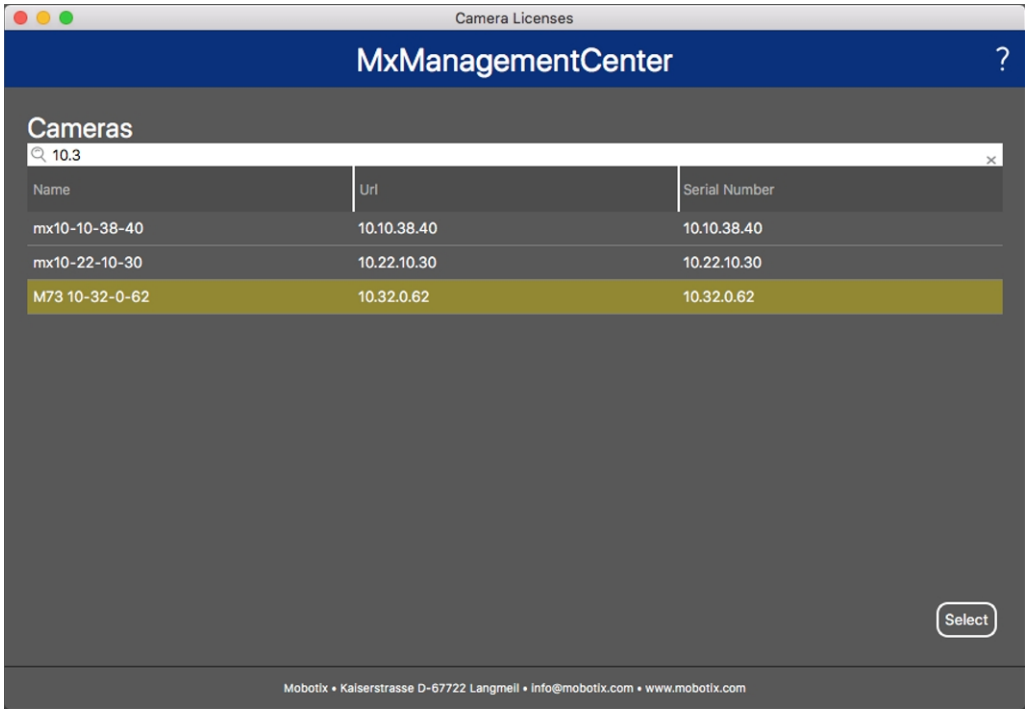


Abb. 8: Überblick über die Kamera-App-Lizenzen in MxManagementCenter

Eine Übersicht der auf der Kamera installierten Lizenzen wird möglicherweise angezeigt.

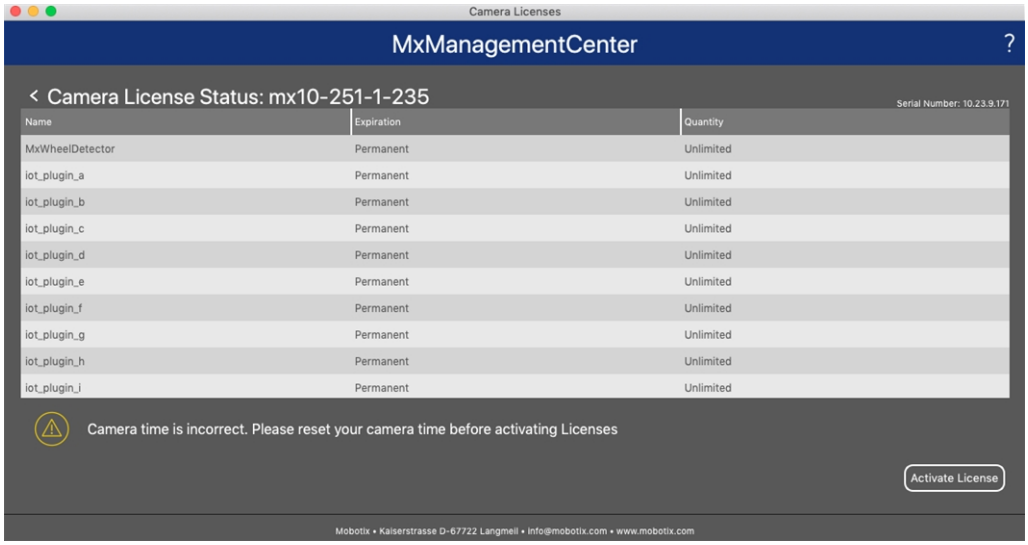


Abb. 9: Übersicht über die auf der Kamera installierten Lizenzen

HINWEIS! Korrigieren Sie bei Bedarf die auf der Kamera eingestellte Uhrzeit.

Spalte	Erläuterung
Name	Name der lizenzierten App
Ablaufdatum	Zeitlimit der Lizenz
Menge	Anzahl der für ein Produkt erworbenen Lizenzen.
Seriennummer	Eindeutige Kennung, die von MxMC für das verwendete Gerät bestimmt wird. Wenn während der Lizenzierung Probleme auftreten, halten Sie die Geräte-ID bereit.

Lizenzen mit dem Server synchronisieren

Wenn das Programm gestartet wird, findet kein automatischer Vergleich der Lizenzen zwischen dem Computer und dem Lizenzserver statt. Klicken Sie daher auf **Aktualisieren**, um die Lizenzen vom Server neu zu laden.

Lizenzen aktualisieren

Um temporäre Lizenzen zu aktualisieren, klicken Sie auf **Lizenzen aktivieren**. Das Dialogfeld zum Aktualisieren/Aktivieren von Lizenzen wird geöffnet.

HINWEIS! Sie benötigen Administratorrechte zum Synchronisieren und Aktualisieren von Lizenzen.

Kamera-, Bild- und Szenenanforderungen

Die Kamera sollte so eingerichtet werden, dass die Kombination aus Abstand, Brennweite des Objektivs und Auflösung der Kamera ein Bild liefert, das genau analysiert werden kann. Daher müssen die folgenden Voraussetzungen für die Szene erfüllt sein:

Höchstmögliche Montagepositionen für beste Ergebnisse

Bei der Planung Ihres Videoüberwachungssystems sollten Sie die höchstmöglichen Kamerapositionen bevorzugen, um mit jeder Kamera eine möglichst große Fläche abzudecken. Ziehen Sie eine Montagehöhe von mindestens 5 Metern in Betracht. Eine Montagehöhe von 10 bis 25 Metern führt in der Regel zu deutlich besseren Ergebnissen.

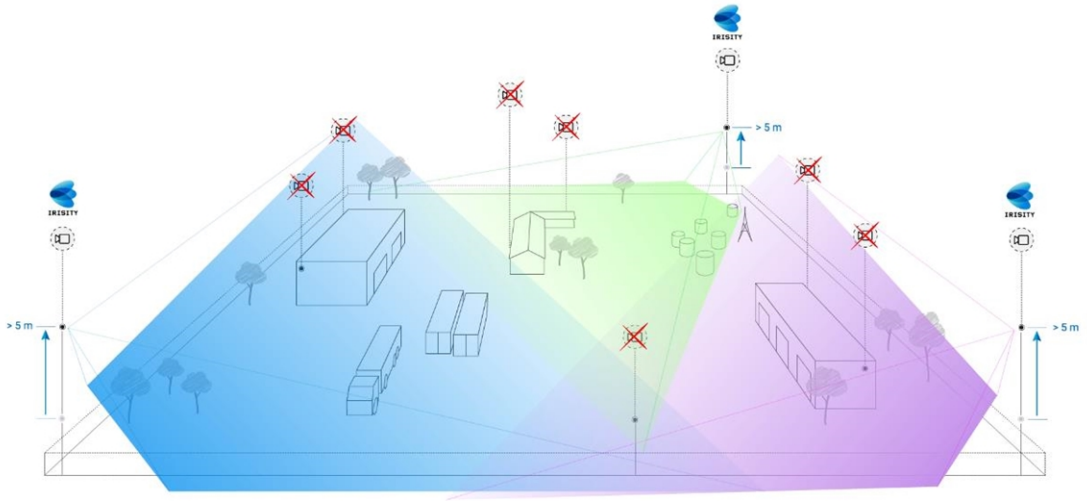


Abb. 10: Durch die Verwendung hoher Montagepositionen kann die Anzahl der Kameras in einer klassischen CCTV-Installation reduziert werden.

Szenenbeleuchtung

Mit optimalen Lichtquellen (wir empfehlen mindestens zwei Lichtquellen) lässt sich die Qualität der Videoanalyse und damit die Sicherheit Ihres Standorts deutlich verbessern.

- Beleuchten Sie den überwachten Bereich ausreichend.
- Sorgen Sie für einen guten Kontrast im Überwachungsbereich.
- Beleuchten Sie Objekte in der Nähe der Kameras nicht zu stark, um Überblendungen und Bildrauschen zu vermeiden.

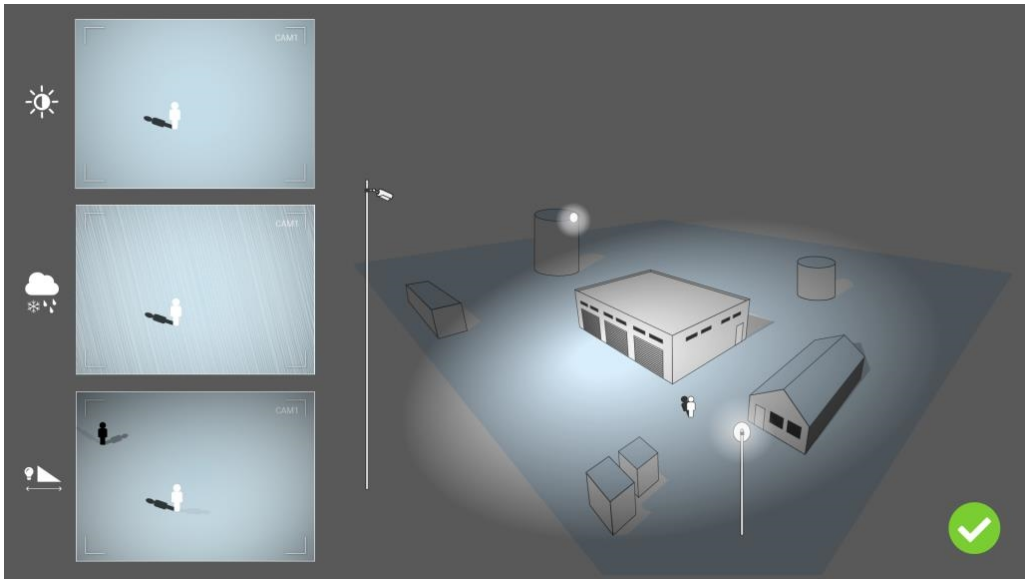


Abb. 11: Eine seitliche Beleuchtung verbessert die Sichtbarkeit, den Kontrast und die Objekterkennung erheblich. Sie ermöglicht präzise Erkennungen auch bei schwierigen Witterungsbedingungen.

Fehlerbehebung

Probleme beim Lichtdesign

Wenn die Lichtquelle in der Nähe der Kamera und zu weit vom geschützten Objekt entfernt platziert wird, kann das ausgestrahlte Licht Videoprobleme verursachen und so die Überwachung beeinträchtigen. Mögliche Probleme:

- Kontrast im Videobild zu niedrig (keine Schatten)
- Lichtquelle erzeugt Rauschen im Bild, indem sie Regentropfen und Schneeflocken betont
- Lichtintensität reicht nicht aus, um das bewachte Objekt zu beleuchten

Obwohl die integrierte Beleuchtung der Kamera oder andere direkte Beleuchtungen praktisch ist, verringert sie oft die Effizienz des Überwachungssystems. Bei schwierigen Witterungsbedingungen können Eindringlinge fast unsichtbar werden und sich hinter Regen, Schnee oder Nebel verstecken.

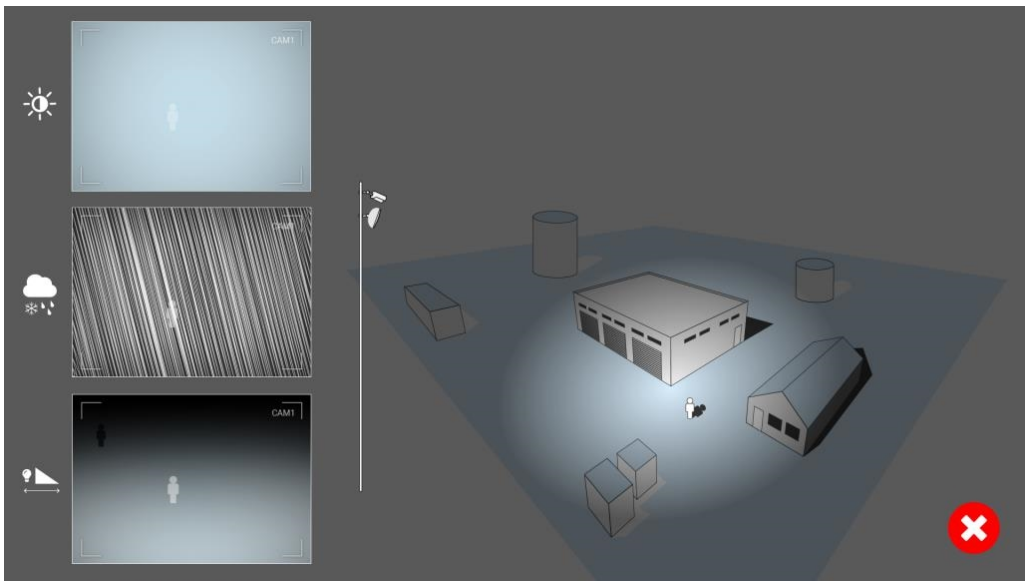


Abb. 12: Bei schwierigen Witterungsbedingungen können Eindringlinge fast unsichtbar werden und sich hinter Regen, Schnee oder Nebel verstecken.

Aktivierung der Certified App-Schnittstelle

VORSICHT! Irisity IRIS AI Analytics - Intrusion Detection lässt für das Live-Bild definierte verdeckte Bereiche außer Acht. Daher kommt es bei der Konfiguration der App und bei der Bildanalyse durch die App zu keiner Artefaktbildung in verdeckten Bereichen.

HINWEIS! Der Benutzer muss Zugriff auf das Setup-Menü haben (http(s)://<Kamera-IP-Adresse>/control). Überprüfen Sie daher die Benutzerberechtigungen der Kamera.

1. Öffnen Sie in der Webschnittstelle der Kamera: **Setup Menu / Certified App Settings** (Setup-Menü/Zertifizierte App-Einstellungen) (http(s)://<Camera IP address>/control/app_config).

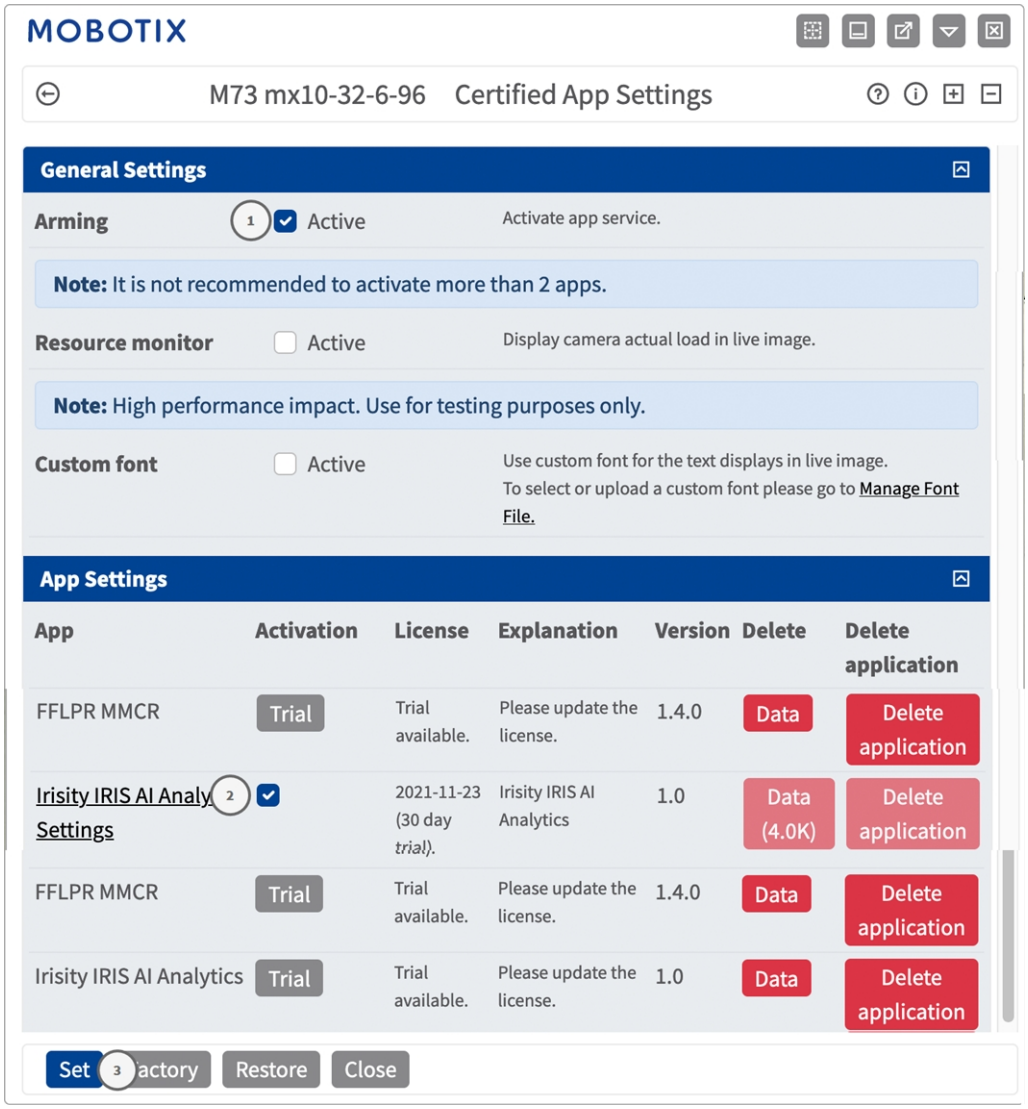


Abb. 13: Certified App: Einstellungen

2. Aktivieren Sie unter **General Settings** (Allgemeine Einstellungen) die Option **Arming** (Aktivierung) des MOBOTIX App-Dienstes ① .
3. Klicken Sie auf „Festlegen“ ③ . Die installierten Apps werden jetzt aufgelistet.
4. Aktivieren Sie unter **App Settings** (App-Einstellungen) die Option **Active** (Aktiv) für die entsprechende App.
5. Klicken Sie auf den Namen der App ② , die konfiguriert werden soll, um die App-Benutzeroberfläche zu öffnen.
6. Informationen zur Konfiguration der App finden Sie unter Konfiguration von Irisity IRIS AI Analytics - Intrusion Detection, p. 22.

Konfiguration von Irisity IRIS AI Analytics - Intrusion Detection

VORSICHT! Der Benutzer muss Zugriff auf das Setup-Menü haben (http(s)://<Kamera-IP-Adresse>/control). Überprüfen Sie daher die Benutzerberechtigungen der Kamera.

1. Öffnen Sie in der Webschnittstelle der Kamera: **Setup Menu / Certified App Settings** (Setup-Menü/Zertifizierte App-Einstellungen) (http(s)://<Camera IP address>/control/app_config).
2. Klicken Sie auf den Namen des **Irisity IRIS AI Analytics - Intrusion Detection**.

Das Konfigurationsfenster der App wird mit den folgenden Optionen angezeigt:

IRIS-Eindringungserkennung

Die folgenden Konfigurationen sollten berücksichtigt werden:

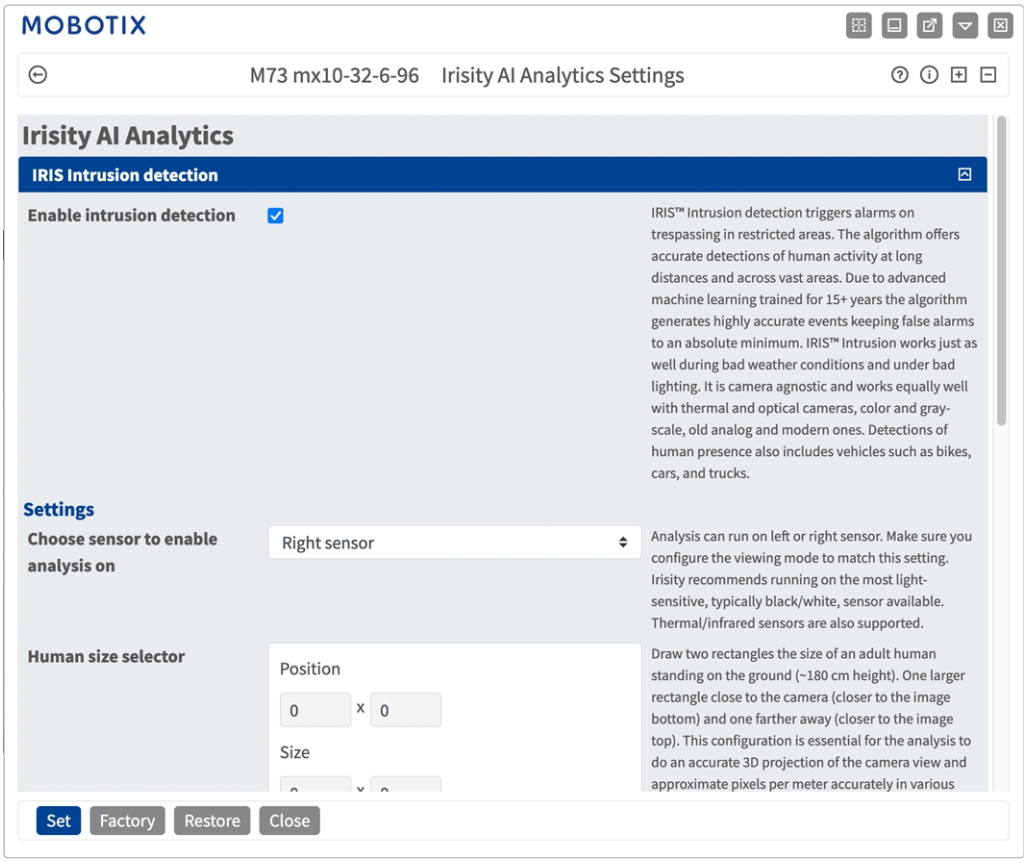


Abb. 14: Standardbetriebsmodus: IRIS-Eindringungserkennung

Enable intrusion detection (Eindringungserkennung aktivieren): Aktivieren Sie diese Option, um den Algorithmus zu aktivieren.

Einstellungen

- **Choose sensor to enable analysis on (Wählen Sie den Sensor, für den Sie die Analyse aktivieren möchten):** Wählen Sie den Sensor aus, der für die Bildanalyse verwendet werden soll.
- **Menschgrößenauswahl:** Diese Konfiguration ist für die Analyse unerlässlich, um eine genaue 3D-Projektion des Kamerabildes zu erstellen und die Pixel pro Meter in verschiedenen Teilen des Bildes genau zu bestimmen (siehe IRIS-Manipulationserkennung, p. 23).
- **Alarm zones (Alarmzonen):** Im Live-Bild muss mindestens eine Alarmzone (Erkennungsbereich) definiert sein (siehe Alarmzonen, p. 24).
- **Objekttyp erkennen:** Wählen Sie einen Filter aus, der nur bei Menschen oder Fahrzeugen ausgelöst werden soll. Die Erkennung umfasst standardmäßig alle von Menschen angetriebenen Bewegungen wie Fußgänger, Fahrräder, Autos und Lastkraftwagen.

Erweiterte Einstellungen

- **Alarmzonen-Abklingzeit:** Anzahl der Sekunden nach Auslösung eines Alarms, nach der die Alarmzone deaktiviert wird.
- **Ereignis-Abklingzeit:** Anzahl der Sekunden, nach denen ein Alarm weitere Erkennungen desselben alarmierenden Objekts, einschließlich nahegelegener Objekte, deaktiviert.
- **Empfindlichkeit:** Empfindlichkeitsgrad für Objekte, die als menschliche Aktivität einzustufen sind. In den meisten Fällen wird „Mittel“ empfohlen.

IRIS-Manipulationserkennung

Hier können Sie die Funktionen der Manipulationserkennung konfigurieren.

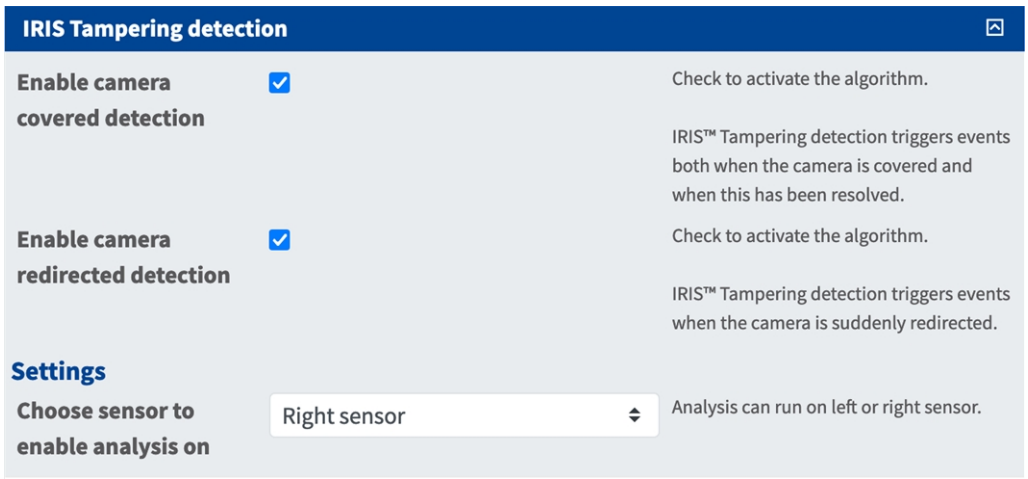


Abb. 15: IRIS-Manipulationserkennung

Erkennung verdeckter Kameras aktivieren: Aktivieren Sie diese Option, um den Algorithmus zu aktivieren.

HINWEIS! Die IRIS™-Manipulationserkennung löst Ereignisse aus, sowohl wenn die Kamera verdeckt wird als auch wenn das Problem behoben wurde.

Erkennung verstellter Kameras aktivieren: Aktivieren Sie die Erkennung verstellter Kameras.

HINWEIS! Die IRIS™-Manipulationserkennung löst Ereignisse aus, wenn die Kamera plötzlich verstellt wird.

Choose sensor to enable analysis on (Wählen Sie den Sensor, für den Sie die Analyse aktivieren möchten): Wählen Sie den Sensor aus, auf dem die Analyse ausgeführt werden soll.

Menschgrößenauswahl zeichnen

1. Klicken Sie einfach in die Live-Ansicht und ziehen Sie einen rechteckigen Erkennungsbereich.
2. Ziehen Sie die Eckpunkte, um den Erkennungsbereich genau einzustellen.
3. Klicken Sie oben rechts in der Live-Ansicht auf **Senden**, um die Koordinaten des Rechtecks zu übernehmen.

Alarmzonen

Sie können optional eine oder mehrere Alarmzonen (Erkennungsbereiche) festlegen. Wenn das Feld leer bleibt, wird das gesamte Bild für die Erkennung verwendet.

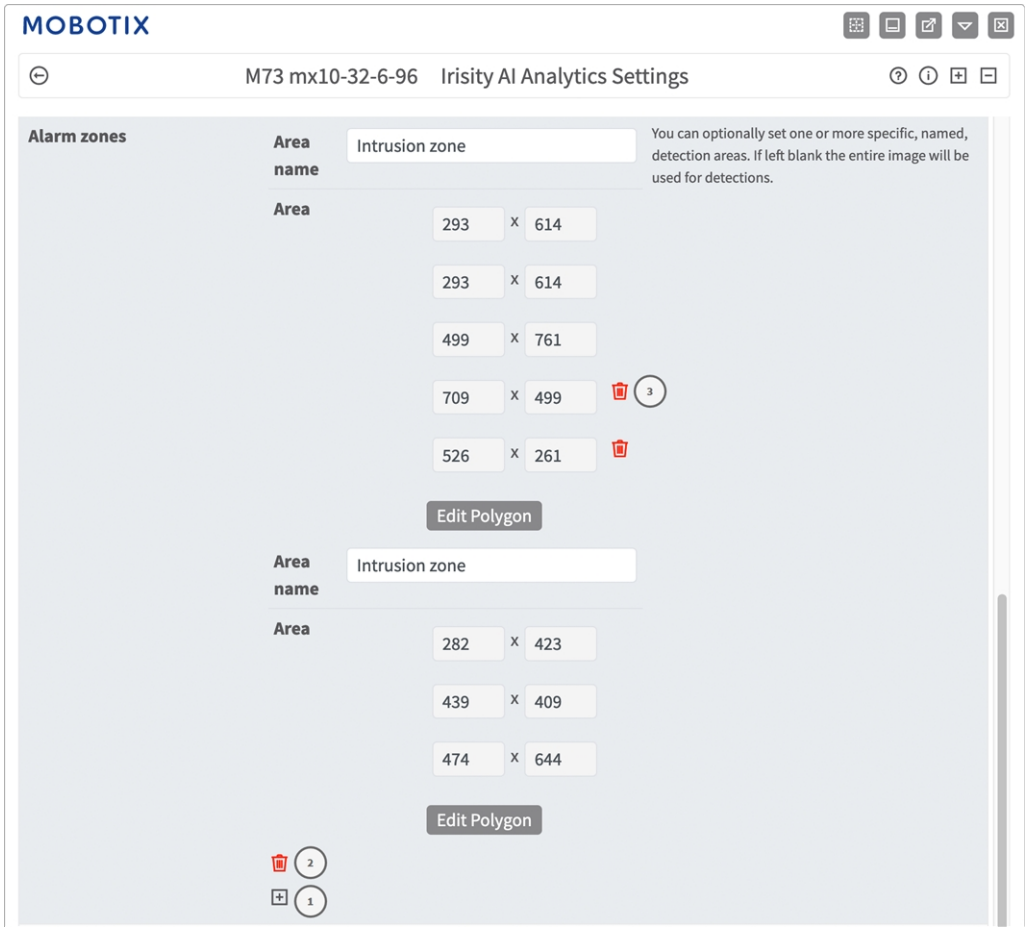


Abb. 16: Alarmzonen

Bereichsname: Geben Sie einen eindeutigen Namen ein, um die Alarmzone zu identifizieren.
Bereich: Die definierten Eckpunkte der Alarmzone. Klicken Sie auf **Polygon bearbeiten** ① , um den Erkennungsbereich in der Live-Ansicht zu zeichnen (siehe Polygonbereich in der Live-Ansicht zeichnen, p. 26).
Alarmzone hinzufügen: Klicken Sie auf das **Plussymbol**② , um eine neue Alarmzone zu definieren.
Bereich löschen: Klicken Sie auf das **Papierkorbsymbol** ② , um den Erkennungsbereich zu löschen.

Visual Overlays (Visuelle Überlagerungen)

Hier können Sie Objekte und Daten der IRIS-Eindringungserkennung auswählen, die im Live-Bild angezeigt werden sollen.

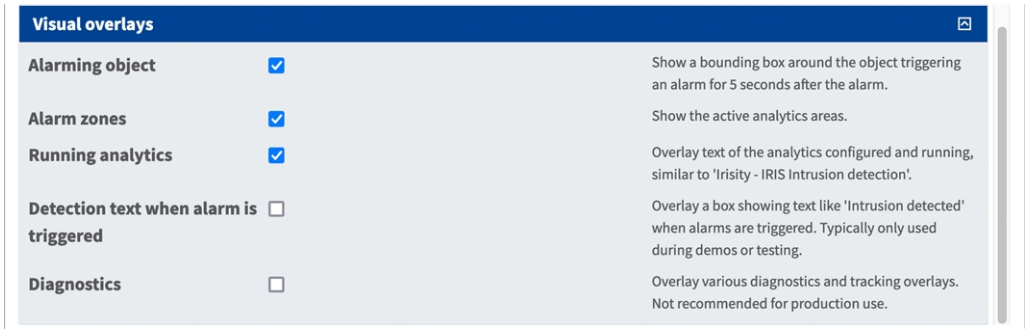


Abb. 17: Visual Overlays (Visuelle Überlagerungen)

Alarming object (Alarmierendes Objekt): Aktivieren Sie diese Option, um für 5 Sekunden nach dem Alarm einen Begrenzungsrahmen um das Objekt anzuzeigen, das einen Alarm ausgelöst hat.

Alarm zones (Alarmzonen): Aktivieren Sie diese Option, um die aktiven Analysebereiche anzuzeigen.

Running analytics (Aktive Analysen): Aktivieren Sie diese Option, um Text der konfigurierten und ausgeführten Analyse einzublenden, z. B. „Irisity – IRIS-Eindringungserkennung“.

Detection text when alarm is triggered (Erkennungstext bei Auslösen des Alarms): Blenden Sie ein Feld mit Text wie „Eindringen erkannt“ ein, wenn Alarme ausgelöst werden.

Diagnostics (Diagnose): Aktivieren Sie diese Option, um verschiedene Diagnose- und Tracking-Überlagerungen einzublenden, z. B. für das Debugging.

Polygonbereich in der Live-Ansicht zeichnen

In der Live-Ansicht können Sie je nach App Bereiche basierend auf Polygonen zeichnen. Diese Bereiche sind z. B. Erkennungsbereiche, ausgeschlossene Bereiche, Referenzbereiche usw.

1. Klicken Sie einfach in die Live-Ansicht, und ziehen Sie einen rechteckigen Bereich auf.
2. Ziehen Sie die Eckpunkte in die gewünschte Position.
3. Um einen weiteren Eckpunkt hinzuzufügen, ziehen Sie einen kleineren Punkt zwischen zwei Eckpunkten auf der Kontur des Bereichs.
4. Klicken Sie oben rechts in der Live-Ansicht auf **Senden**, um die Koordinaten des Polygons zu übernehmen.
5. Optional können Sie auf das **Papierkorb**-Symbol klicken, um den Erkennungsbereich zu löschen.

Visual Overlays (Visuelle Überlagerungen)

Hier können Sie Objekte und Daten der IRIS-Eindringungserkennung auswählen, die im Live-Bild angezeigt werden sollen.

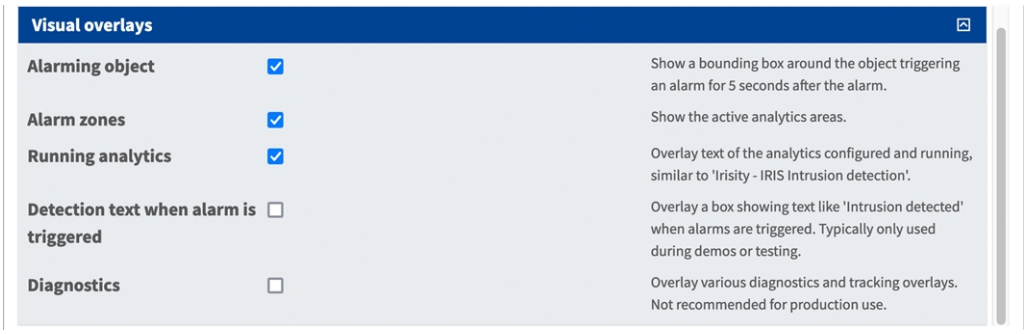


Abb. 18: Visual Overlays (Visuelle Überlagerungen)

Alarming object (Alarmierendes Objekt): Aktivieren Sie diese Option, um für 5 Sekunden nach dem Alarm einen Begrenzungsrahmen um das Objekt anzuzeigen, das einen Alarm ausgelöst hat.

Alarm zones (Alarmzonen): Aktivieren Sie diese Option, um die aktiven Analysebereiche anzuzeigen.

Running analytics (Aktive Analysen): Aktivieren Sie diese Option, um Text der konfigurierten und ausgeführten Analyse einzublenden, z. B. „Irisity – IRIS-Eindringungserkennung“.

Erkennungstext: Blenden Sie ein Feld mit Text wie „Eindringen erkannt“ ein, wenn Alarme ausgelöst werden.

Diagnostics (Diagnose): Aktivieren Sie diese Option, um verschiedene Diagnose- und Tracking-Überlagerungen einzublenden, z. B. für das Debugging.

Speichern der Konfiguration

Zum Speichern der Konfiguration stehen folgende Optionen zur Verfügung:

Abb. 19: Speichern der Konfiguration

- Klicken Sie auf die Schaltfläche **Set** (Festlegen), um Ihre Einstellungen zu aktivieren und bis zum nächsten Neustart der Kamera zu speichern.
- Klicken Sie auf die Schaltfläche **Factory** (Werkseinstellungen), um die Werkseinstellungen für dieses Dialogfeld zu laden (diese Schaltfläche ist möglicherweise nicht in allen Dialogfeldern vorhanden).
- Klicken Sie auf die Schaltfläche **Restore** (Wiederherstellen), um die letzten Änderungen rückgängig zu machen, die nicht dauerhaft in der Kamera gespeichert wurden.
- Klicken Sie auf die Schaltfläche **Close** (Schließen), um das Dialogfeld zu schließen. Beim Schließen des Dialogfelds prüft das System die gesamte Konfiguration auf Änderungen. Wenn Änderungen erkannt werden, werden Sie gefragt, ob Sie die gesamte Konfiguration dauerhaft speichern möchten.

Nach dem erfolgreichen Speichern der Konfiguration werden die Ereignis- und Metadaten im Falle eines Ereignisses automatisch an die Kamera gesendet.

MxMessageSystem

Was ist MxMessageSystem?

MxMessageSystem ist ein Kommunikationssystem, das auf namensorientierten Nachrichten basiert. Dies bedeutet, dass eine Nachricht einen eindeutigen Namen mit einer maximalen Länge von 32 Bytes haben muss.

Jeder Teilnehmer kann Nachrichten senden und empfangen. MOBOTIX-Kameras können auch Nachrichten innerhalb des lokalen Netzwerks weiterleiten. Auf diese Weise können MxMessages über das gesamte lokale Netzwerk verteilt werden (siehe Nachrichtenbereich: Global).

Eine MOBOTIX-Kamera der Serie 7 kann beispielsweise eine von einer Kamera-App generierte MxMessage mit einer Mx6-Kamera austauschen, die keine zertifizierten MOBOTIX-Apps unterstützt.

Fakten zu MxMessages

- 128-Bit-Verschlüsselung gewährleistet den Schutz und die Sicherheit von Nachrichteninhalten.
- MxMessages können von jeder Kamera der Mx6- und 7-Serie aus verteilt werden.
- Der Nachrichtenbereich kann für jede MxMessage einzeln definiert werden.
  - **Lokal:** Die Kamera erwartet eine MxMessage in ihrem eigenen Kamerasystem (z. B. über eine Certified App).
  - **Global:** Die Kamera erwartet eine MxMessage, die im lokalen Netzwerk von einem anderen MxMessage-Gerät (z. B. einer anderen Kamera der Serie 7 mit einer MOBOTIX Certified App) verteilt wird.
- Aktionen, die die Empfänger ausführen sollen, werden für jeden MxMessageSystem-Teilnehmer individuell konfiguriert.

MxMessageSystem: Verarbeiten der automatisch generierten App-Ereignisse

Überprüfen automatisch generierter App-Ereignisse

HINWEIS! Nach erfolgreicher Aktivierung der App (siehe Aktivierung der Certified App-Schnittstelle, p. 20) wird automatisch ein generisches Nachrichtenereignis für diese spezifische App in der Kamera generiert.

1. Wechseln Sie zu **Setup-Menu / Event Control / Event Overview** (Setup-Menü/Ereignissteuerung/Ereignisübersicht). Im Abschnitt **Message Events** (Nachrichtenereignisse) wird das automatisch generierte Nachrichtenereignisprofil nach der Anwendung benannt (z. B. IRIS).

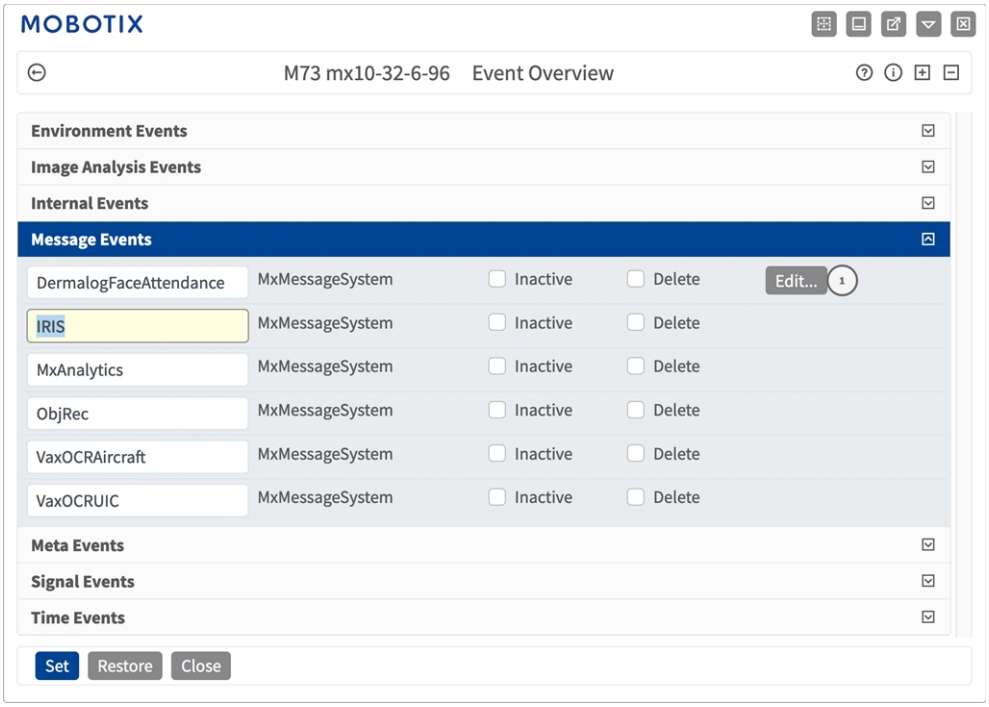


Abb. 20: Beispiel: Generisches Nachrichtenereignis von Irisity IRIS AI Analytics - Intrusion Detection

2. Klicken Sie auf **Edit** ⓘ (Bearbeiten), um eine Auswahl aller konfigurierten Nachrichtenereignisse anzuzeigen.

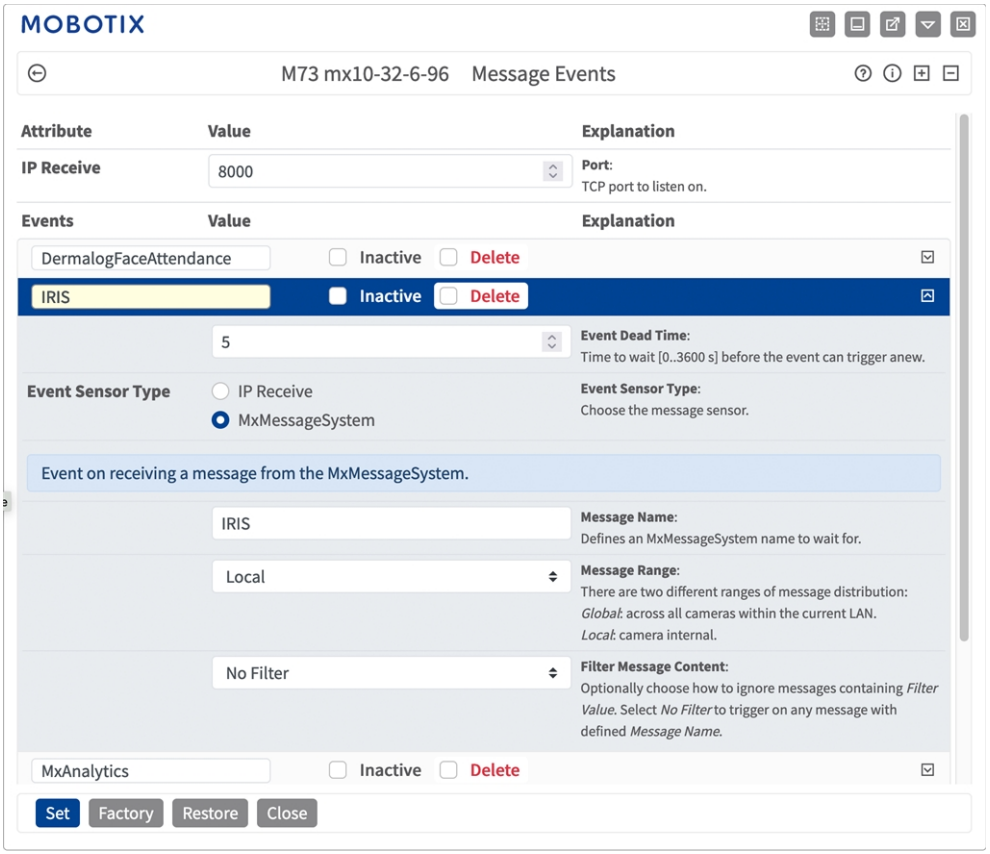


Abb. 21: Beispiel: Allgemeine Nachrichtenereignisdetails – kein Filter

Aktionsabwicklung – Konfiguration einer Aktionsgruppe

VORSICHT! Um Ereignisse zu verwenden, Aktionsgruppen auszulösen oder Bilder aufzuzeichnen, muss die allgemeine Aktivierung der Kamera aktiviert sein (http(s)/<Kamera-IP-Adresse>/Steuerung/Einstellungen).

Eine Aktionsgruppe definiert, welche Aktionen vom Irisity IRIS AI Analytics - Intrusion Detection-Ereignis ausgelöst werden.

1. Öffnen Sie in der Webschnittstelle der Kamera: **Setup Menu / Action Group Overview** (Setup-Menü/Aktionsgruppenübersicht) (http(s)://<Camera IP address>/control/actions).

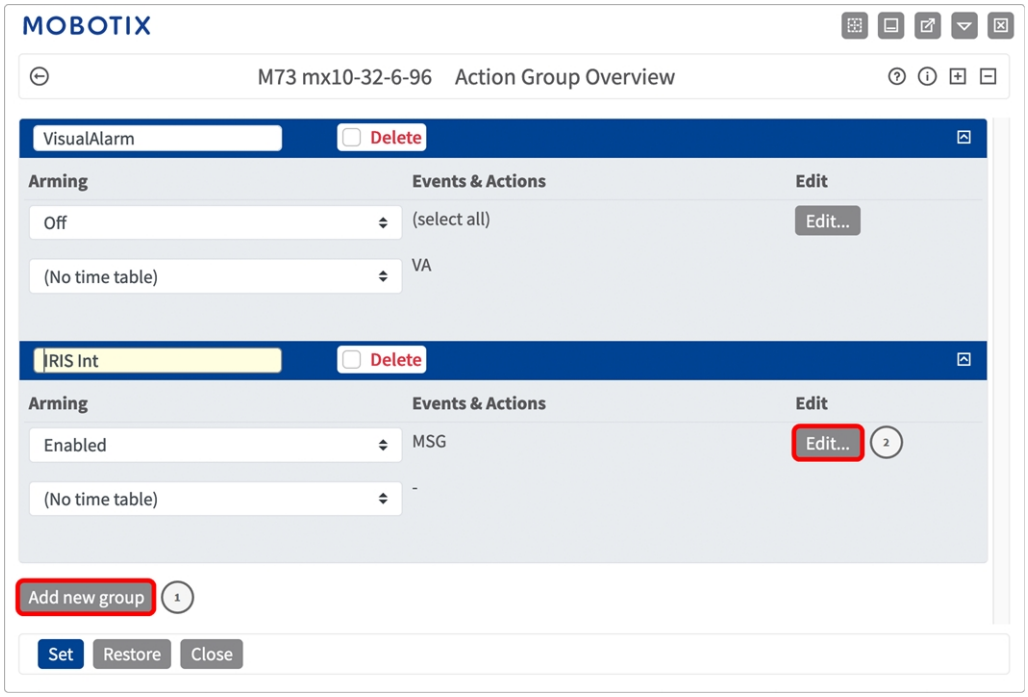


Abb. 22: Definieren von Aktionsgruppen

2. Klicken Sie auf **Add new group**① (Neue Gruppe hinzufügen) und geben Sie einen aussagekräftigen Namen ein.
3. Klicken Sie auf **Edit**② (Bearbeiten), um die Gruppe zu konfigurieren.

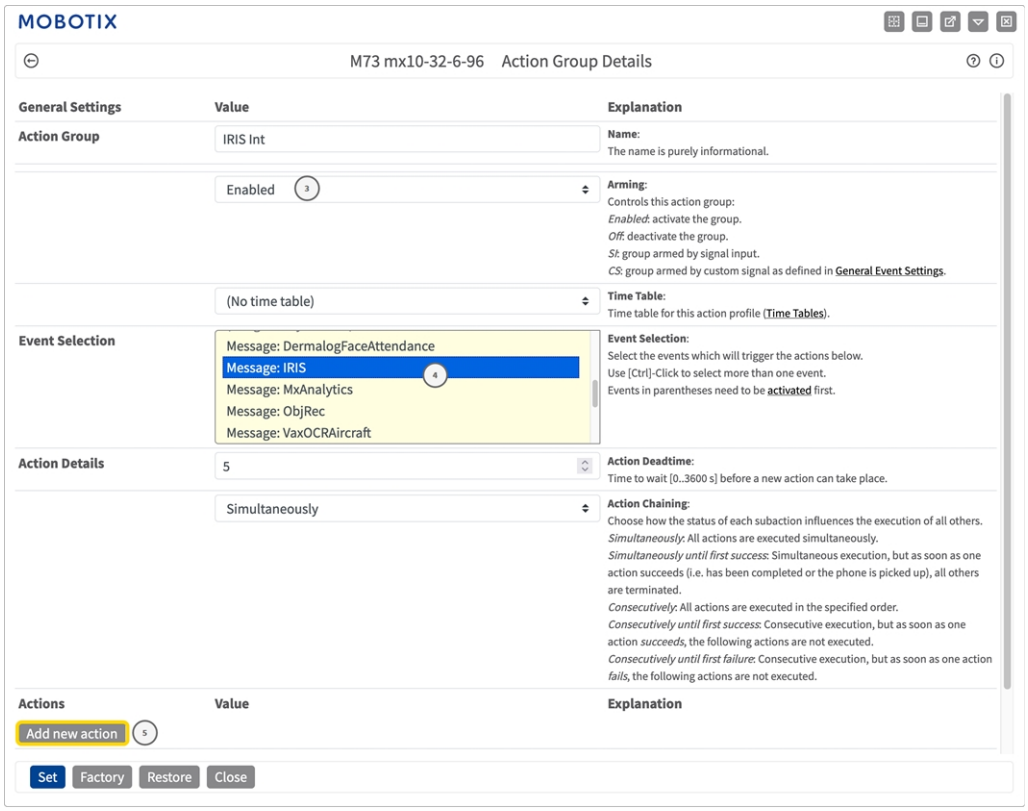


Abb. 23: Konfigurieren einer Aktionsgruppe

4. Aktivieren Sie **Arming**③ (Aktivierung) der Aktionsgruppe.
5. Wählen Sie das Nachrichtenereignis in der Liste **Event selection** ④ (Ereignisauswahl) aus. Um mehrere Ereignisse auszuwählen, halten Sie die Umschalttaste gedrückt.
6. Klicken Sie auf **Add new action**⑤ (Neue Aktion hinzufügen).
7. Wählen Sie eine geeignete Aktion aus der Liste **Action Type and Profile**⑥ (Aktionstyp und Profil) aus.

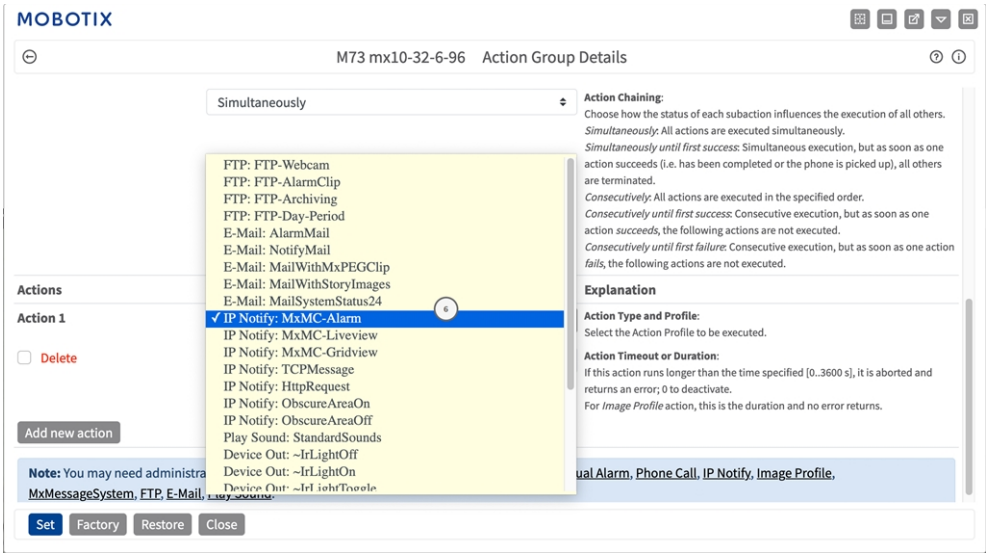


Abb. 24: Aktionstyp und Profil auswählen

HINWEIS! Wenn das erforderliche Aktionsprofil noch nicht verfügbar ist, können Sie in den Abschnitten „MxMessageSystem“, „Übertragungsprofile“ und „Audio- und VoIP-Telefonie“ im Admin-Menü ein neues Profil erstellen.

Bei Bedarf können Sie weitere Aktionen hinzufügen, indem Sie erneut auf die Schaltfläche klicken. Stellen Sie in diesem Fall sicher, dass die „action chaining“ (Aktionsverkettung) korrekt konfiguriert ist (z. B. gleichzeitig).

8. Klicken Sie am Ende des Dialogfelds auf die Schaltfläche **„Set“ (Festlegen)**, um die Einstellungen zu bestätigen.

Aktionseinstellungen – Konfiguration der Kameraaufzeichnungen

1. Öffnen Sie in der Webschnittstelle der Kamera: **„Setup Menu / Event Control / Recording“ (Setup-Menü/Ereignissteuerung/Aufzeichnung)**http(s)/<Kamera-IP-Adresse>/control/recording).

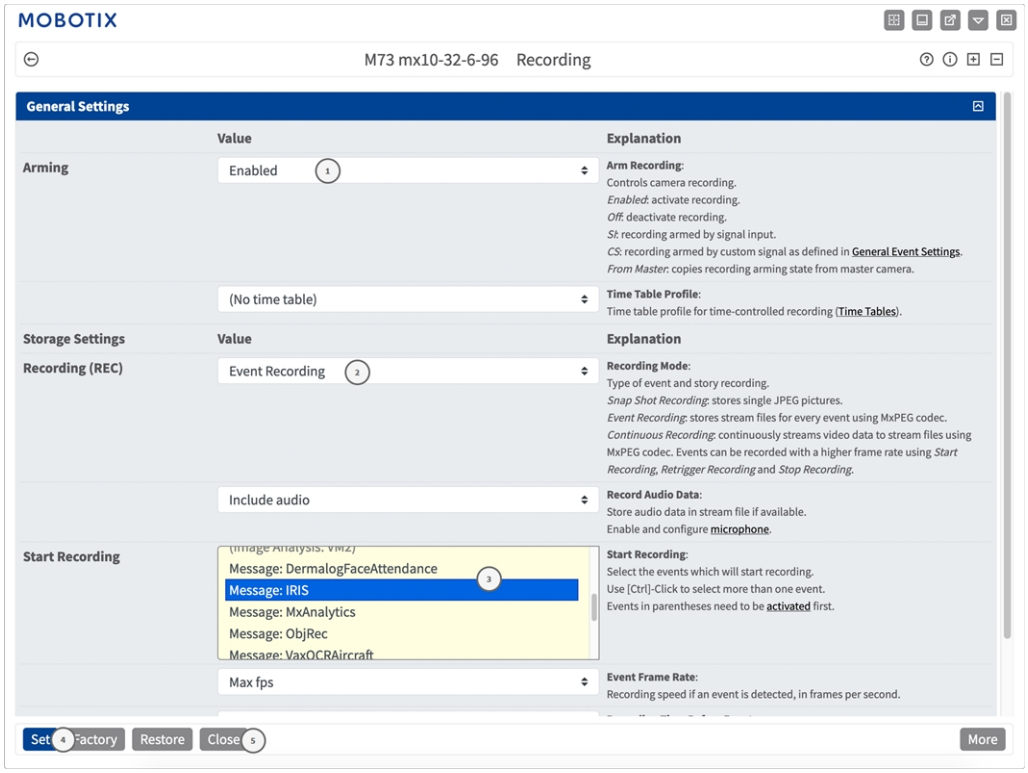


Abb. 25: Konfiguration der Aufnahmeeinstellungen der Kamera

2. Aktivieren Sie **Arm Recording** ① (Aufzeichnung aktivieren).
3. Wählen Sie unter **Storage Settings** (Speichereinstellungen)/**Recording (REC)** (Aufzeichnung) einen **Recording mode** ② (Aufnahmemodus) aus. Die folgenden Modi sind verfügbar:
   - Einzelbildaufzeichnung
   - Ereignisaufzeichnung
   - Kontinuierliche Aufzeichnung
4. Wählen Sie in der Liste **Start recording** ③ (Aufzeichnung starten) das soeben erstellte Nachrichtenereignis aus.
5. Klicken Sie am Ende des Dialogfelds auf die Schaltfläche **Set** ④ (Festlegen), um die Einstellungen zu bestätigen.
6. Klicken Sie auf **Close** ⑤ (Schließen), um Ihre Einstellungen dauerhaft zu speichern.

HINWEIS! Alternativ können Sie Ihre Einstellungen im Admin-Menü unter „Configuration / Save current configuration to permanent memory“ (Konfiguration/Aktuelle Konfiguration dauerhaft speichern) speichern.

MxMessageSystem: Verarbeiten der von Apps übertragenen Metadaten

Metadaten werden innerhalb des MxMessageSystem übertragen.

Für jedes Ereignis überträgt die App auch Metadaten an die Kamera. Diese Daten werden in Form eines JSON-Schemas innerhalb einer MxMessage gesendet.

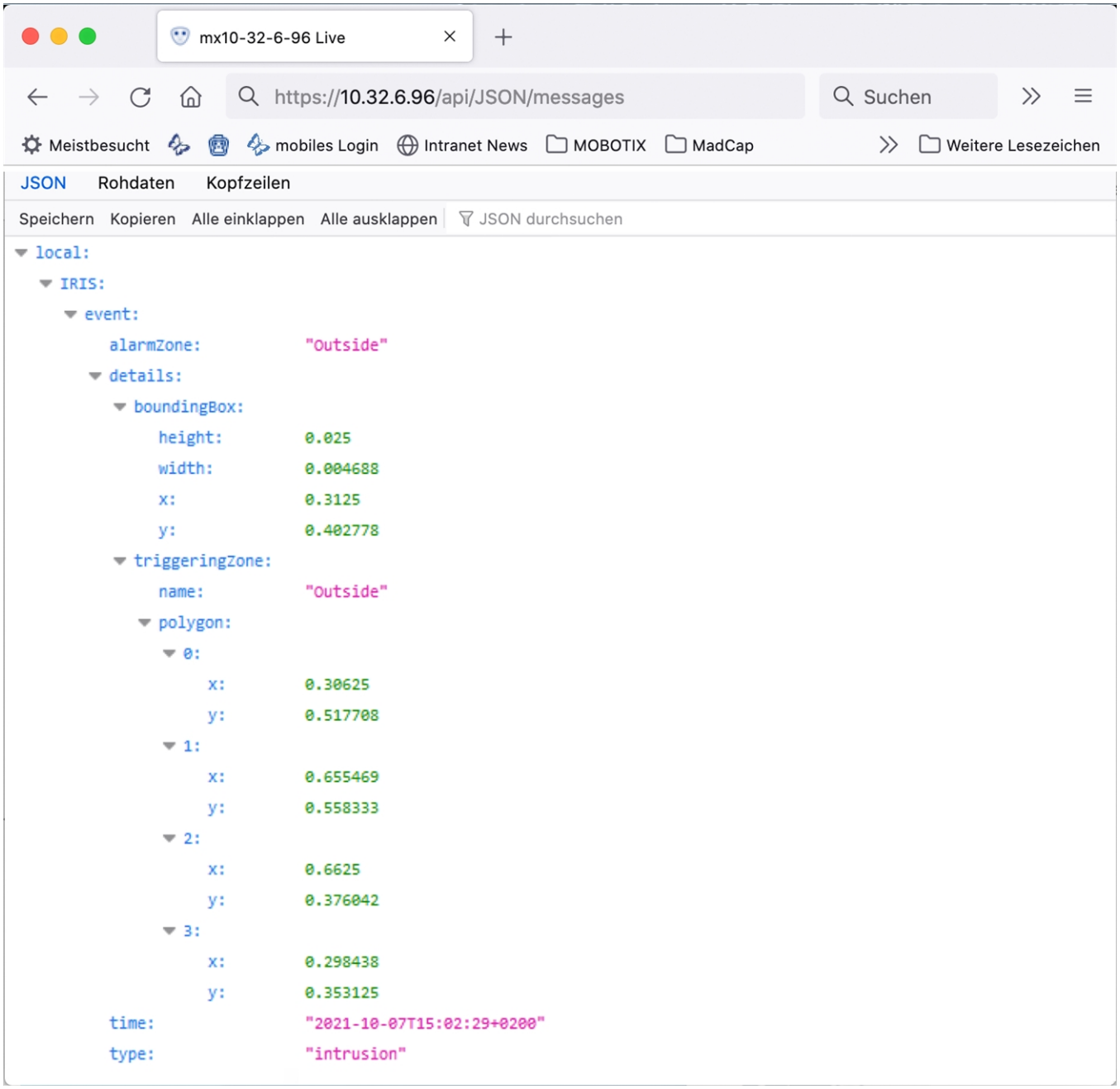


Abb. 26: Beispiel: Metadaten, die innerhalb einer MxMessage von Irisity IRIS AI Analytics - Intrusion Detection übertragen werden

HINWEIS! Um die Metadatenstruktur des letzten App-Ereignisses anzuzeigen, geben Sie die folgende URL in die Adresszeile Ihres Browsers ein: http(s)/IP-Adresse_Ihrer_Kamera/API/json/messages

Erstellen eines benutzerdefinierten Nachrichtenereignisses

1. Wechseln Sie zu **Setup-Menu / Event Control / Event Overview** (Setup-Menü/Ereignissteuerung/Ereignisübersicht). Im Abschnitt **Message Events** (Nachrichtenereignisse) wird das automatisch generierte Nachrichtenereignisprofil nach der Anwendung benannt (z. B. IRIS).

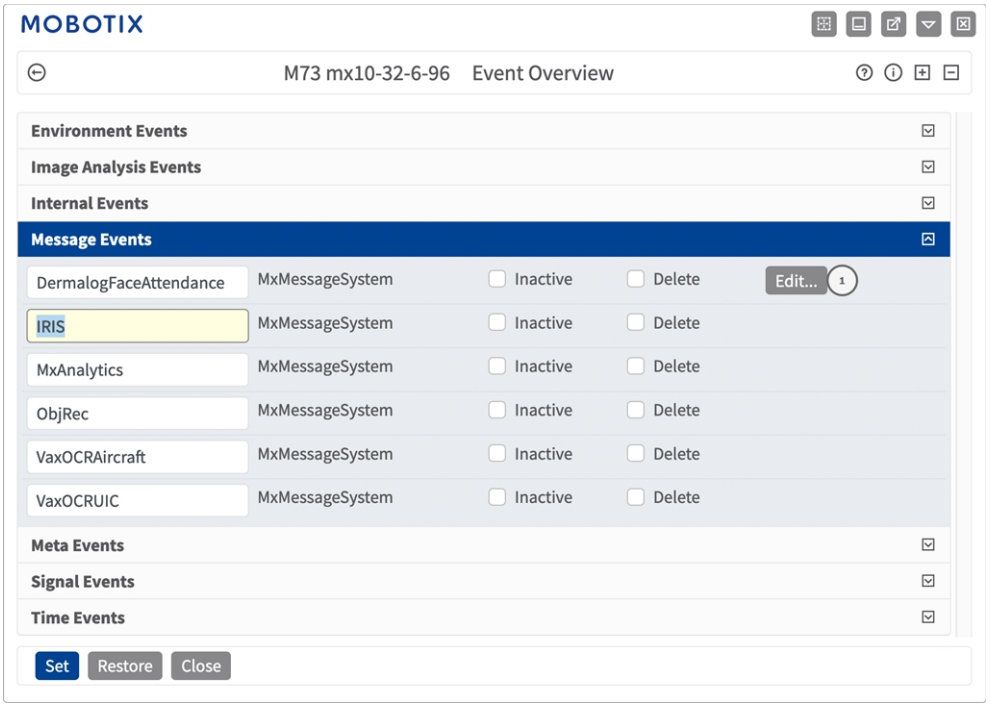


Abb. 27: Beispiel: Generisches Nachrichtenereignis von Irisity IRIS AI Analytics - Intrusion Detection

2. Klicken Sie auf **Edit** ① (Bearbeiten), um eine Auswahl aller konfigurierten Nachrichtenereignisse anzuzeigen.

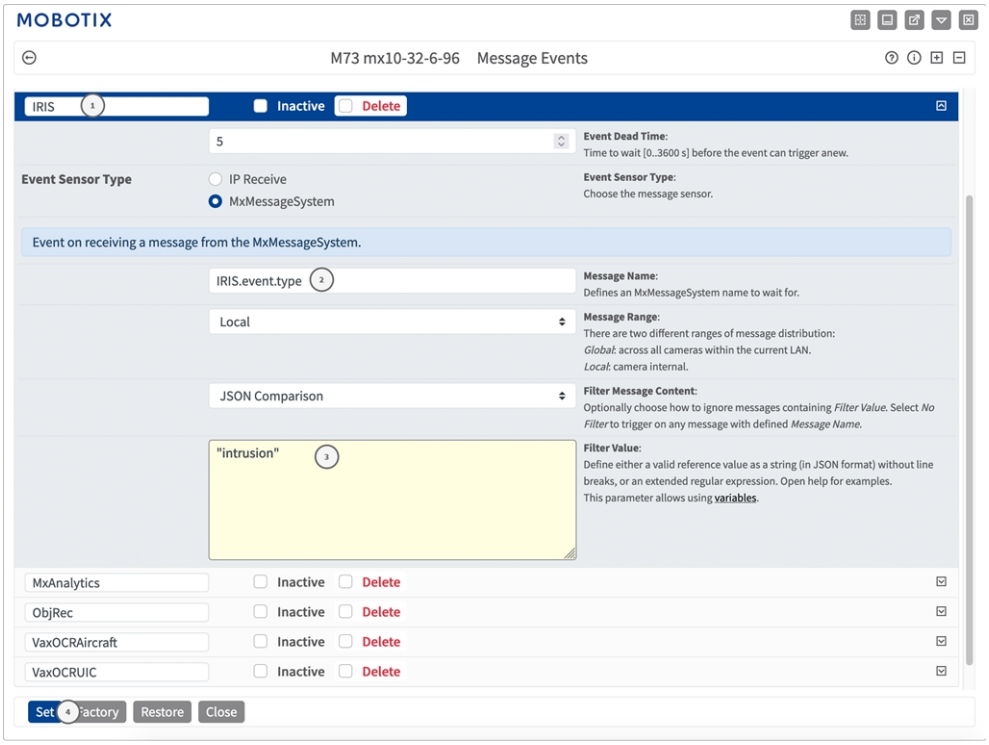


Abb. 28: Beispiel: Ereignis für Eindringungsnachricht

3. Klicken Sie auf das Ereignis (z. B. IRIS) ① , um die Ereigniseinstellungen zu öffnen.
4. Konfigurieren Sie die Parameter des Ereignisprofils wie folgt:

- **„Message Name“ (Nachrichtenname):** Geben Sie den „Nachrichtennamen“ ② gemäß der Ereignisdokumentation der entsprechenden App ein (siehe Beispiele für Nachrichtennamen und Filterwerte von Irisity IRIS AI Analytics - Intrusion Detection, p. 38).
- **„Message Range“ (Meldungsbereich):**
  - **Lokal:** Standardeinstellungen für Irisity IRIS AI Analytics - Intrusion Detection
  - **Global:** (MxMessage wird von einer anderen MOBOTIX-Kamera im lokalen Netzwerk weitergeleitet.)
- **Nachrichteninhalt filtern:**
  - **Generisches Ereignis:** „No Filter“ (Kein Filter)
  - **Gefiltertes Ereignis:** „JSON-Vergleich“
- **Filterwert:** ③ Siehe Beispiele für Nachrichtennamen und Filterwerte von Irisity IRIS AI Analytics - Intrusion Detection, p. 38.

VORSICHT! „Filter Value“ (Filterwert) wird verwendet, um die MxMessages einer App/eines Pakets zu unterscheiden. Verwenden Sie diesen Eintrag, um die einzelnen Ereignistypen der Apps zu nutzen (sofern verfügbar).

Wählen Sie „No Filter“ (Kein Filter), wenn Sie alle eingehenden MxMessages als generisches Ereignis der zugehörigen App nutzen möchten.

2. Klicken Sie auf die Schaltfläche **Set** ④ (Festlegen) am Ende des Dialogfelds, um die Einstellungen zu bestätigen.

Beispiele für Nachrichtennamen und Filterwerte von Irisity IRIS AI Analytics - Intrusion Detection

IRIS-Eindringungserkennung	MxMessage-Name	Filterwert
Generisches Ereignis	IRIS	
Alarmzonenereignis	IRIS.event.alarmZone	Name der Alarmzone, z. B.: „Eindringzone 2“
Ereignistyp	IRIS.event.type	„Eindringung“

MOBOTIX

BeyondHumanVision

DE_03.23
MOBOTIX AG • Kaiserstrasse • D-67722 Langmeil • Tel.: +49 6302 9816-103 • sales@mobotix.com • www.mobotix.com