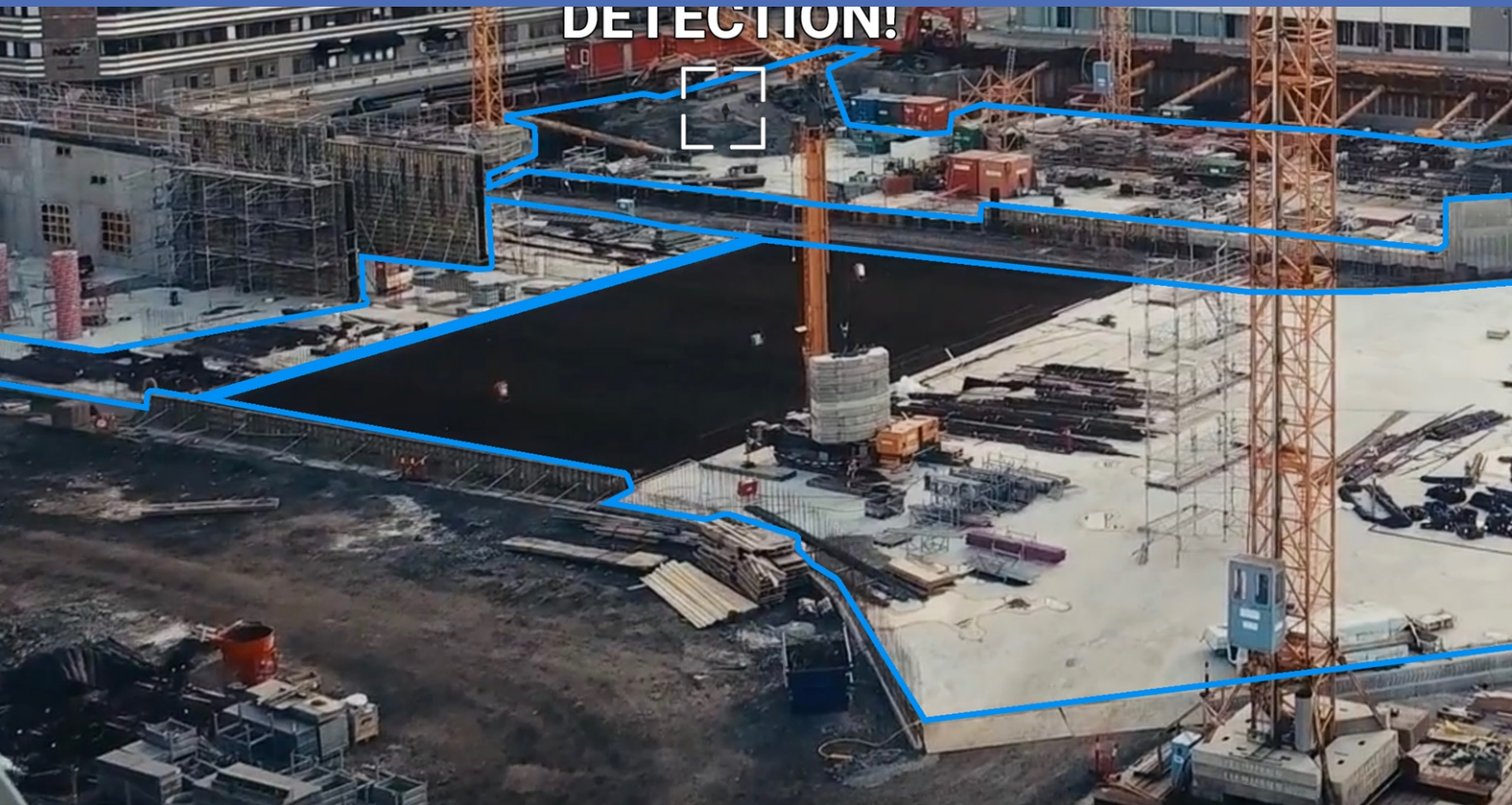




# Leitfaden

## Irisity IRIS Core Intrusion App

© 2024 MOBOTIX AG



BeyondHumanVision

MOBOTIX

# Inhaltsverzeichnis

---

<b>Inhaltsverzeichnis</b> .....	<b>2</b>
<b>Bevor Sie beginnen</b> .....	<b>5</b>
Support .....	6
MOBOTIX Support .....	6
MOBOTIX eCampus .....	6
MOBOTIX Community .....	6
Sicherheitshinweise .....	7
Rechtliche Hinweise .....	7
<b>Informationen zu Irisity IRIS Core Intrusion App</b> .....	<b>9</b>
Smart Data-Schnittstelle zu MxManagementCenter .....	9
<b>Technische Daten</b> .....	<b>11</b>
<b>Lizenzierung der Certified Apps</b> .....	<b>13</b>
Lizenzaktivierung zertifizierter Apps in MxManagementCenter .....	13
Verwalten von Lizenzen in MxManagementCenter .....	18
<b>Kamera-, Bild- und Szenenanforderungen</b> .....	<b>20</b>
Fehlerbehebung .....	21
<b>Aktivierung der Certified App-Schnittstelle</b> .....	<b>23</b>
<b>Konfiguration von Irisity IRIS Core Intrusion App</b> .....	<b>25</b>
IRIS-Eindringungserkennung .....	25
Einstellungen .....	26
Erweiterte Einstellungen .....	28

---

IRIS-Manipulationserkennung .....	28
Visual Overlays (Visuelle Überlagerungen) .....	29
Speichern der Konfiguration .....	30
<b>MxMessageSystem .....</b>	<b>31</b>
Was ist MxMessageSystem? .....	31
Fakten zu MxMessages .....	31
<b>MxMessageSystem: Verarbeiten der automatisch generierten App-Ereignisse .....</b>	<b>32</b>
Überprüfen automatisch generierter App-Ereignisse .....	32
Aktionsabwicklung – Konfiguration einer Aktionsgruppe .....	33
Aktionseinstellungen – Konfiguration der Kameraaufzeichnungen .....	35
<b>MxMessageSystem: Verarbeiten der von Apps übertragenen Metadaten .....</b>	<b>37</b>
Metadaten werden innerhalb des MxMessageSystem übertragen. ....	37
Erstellen eines benutzerdefinierten Nachrichteneignisses .....	38
Beispiele für Nachrichtennamen und Filterwerte von Irisity IRIS Core Intrusion App .....	40



## Bevor Sie beginnen

<b>Support</b> .....	<b>6</b>
<b>Sicherheitshinweise</b> .....	<b>7</b>
<b>Rechtliche Hinweise</b> .....	<b>7</b>

# Support

## MOBOTIX 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](http://www.mobotix.com) > **Support** > **Help Desk**.



## MOBOTIX eCampus

Der MOBOTIX eCampus ist eine Rundum-Plattform für das E-Learning. Sie können damit entscheiden, wann und wo Sie die Inhalte Ihrer Schulungsseminare durchsehen und bearbeiten möchten. Öffnen Sie einfach die Website in Ihrem Browser und wählen Sie das gewünschte Schulungsseminar aus.

Besuchen Sie dazu <https://www.mobotix.com/de/ecampus-mobotix>.



## MOBOTIX Community

Die MOBOTIX Community ist ebenfalls eine nützliche Informationsquelle. Die Mitarbeiter von MOBOTIX und andere Benutzer teilen dort ihr Wissen miteinander. Auch Sie haben diese Möglichkeit.

Besuchen Sie dazu [community.mobotix.com](http://community.mobotix.com).



## Sicherheitshinweise

- Diese Kamera muss von qualifiziertem Personal installiert werden, und die Installation muss allen örtlichen Vorschriften entsprechen.
- 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.
- Die Installation dieses Produkts muss gemäß der vorliegenden Dokumentation erfolgen. Fehlerhafte Montage kann Schäden am Produkt verursachen!
- Ersetzen Sie keinesfalls die Batterien des Kamera. Wenn eine Batterie durch einen falschen Batterietyp ersetzt wird, kann die Batterie explodieren.
- Externe Netzteile müssen den LPS-Anforderungen (Limited Power Source, begrenzte Stromquelle) entsprechen und die gleichen Leistungsdaten wie die Kamera aufweisen.
- 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.

## 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](http://www.mobotix.com) unter **Support > Download-Center > Marketing & Dokumentation > 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 MOBOTIX finden Sie unter [www.mobotix.com](http://www.mobotix.com) unter **Support > Download Center > Marketing & Dokumentation > Broschüren & Anleitungen > 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](http://www.mobotix.com), indem Sie auf den entsprechenden Link unten auf jeder Seite klicken.

Der Benutzer ist dafür verantwortlich, dass er im Zusammenhang mit der Nutzung der Software und des Produkts alle geltenden lokalen, staatlichen, nationalen und ausländischen Gesetze, Vorschriften, Verträge und Bestimmungen einhält, einschließlich derjenigen, die sich auf den Datenschutz, den Health Insurance Portability and Accountability Act von 1996 (HIPPA), die internationale Kommunikation und die Übertragung technischer oder personenbezogener Daten beziehen.



# Informationen zu Irisity IRIS Core Intrusion App

## Menschliche Aktivität in Alarmzonen erkennen

Irisity IRIS Core Intrusion App 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.)
- 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.

# Technische Daten

## Produktinformationen

Produktname	Irisity IRIS Core Intrusion App
Bestellnummer	Mx-APP-IRIS-C-INT
Unterstützt MOBOTIX-Kameras	D71, M73, S74, p71, v71
Erforderliche Kamera-Firm- wareversion	V7.3.0.x
MxManagementCenter -Integration	<ul style="list-style-type: none"><li>▪ Min. MxMC v2.5.3</li><li>▪ Konfiguration: Advanced Config-Lizenz erforderlich</li><li>▪ Recherche: Smart Data-Schnittstellen-Lizenz im Lieferumfang enthalten</li></ul>

## Produktfunktionen

App-Funktionen	<ul style="list-style-type: none"><li>▪ Erkennt menschliche Aktivität in benutzerdefinierten Detektionszonen in weiten Bereichen (Einbrucherkennung)</li><li>▪ Die KI-Objektklassifizierung ermöglicht gezielte Alarmierung von Personen und/oder Fahrzeugen (Autos, Fahrräder, LKWs), die nur kleine Teile des Sichtfeldes abdecken</li><li>▪ Reduziert Fehlalarme auf ein Minimum, indem nicht kritische Bewegungen ausgefiltert werden (z. B. Tiere, Bäume, Wolken usw.)</li><li>▪ Manipulationserkennung bei verdeckter oder bewegter Kamera</li><li>▪ Geeignet für optische und Wärmebildkameras</li><li>▪ MOBOTIX und ONVIF Veranstaltungen über MxMessageSystem</li><li>▪ Smart Data Interface und/oder MOBOTIX HUB</li></ul>
Maximale Anzahl an Erkennungszonen	20
Metadaten-/Sta- tistikformate	JSON
Testlizenz	30-Tage-Testlizenz vorinstalliert

## Technische Daten

### Smart Data-Schnittstelle zu MxManagementCenter

---

MxMessageSystem unterstützt	Ja
MOBOTIX-Ereignisse	Ja
ONVIF-Ereignisse	Ja (generisches Nachrichtenergebnis)

---

## Szenenanforderungen

Minimale Objekthöhe	20 Pixel
Typ. Maximaler Erkennungsabstand	<a href="https://community.mobotix.com/t/irisity-iris-core-ai-lens-distance-over-view/4728">https://community.mobotix.com/t/irisity-iris-core-ai-lens-distance-over-view/4728</a>
Montagehöhe der Kamera	5 - 25 m
Maximaler Neigungswinkel	Nur Neigung nach unten: keine Begrenzung

---

## Technische App-Spezifikationen

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

---

### HINWEIS!

- Die Erkennungsgenauigkeit kann nur erreicht werden, wenn in der App-Konfiguration die richtigen „Personengrößenindikatoren“ eingestellt sind.
- Ziele, die weitgehend durch andere Objekte oder Vegetation verdeckt sind, können von der App nicht zuverlässig erkannt werden. Dies ist bei der Planung und Installation der Kameras zu berücksichtigen.
- Speziell für den Einsatz von Wärmebildkameras: Eine korrekte Erkennung kann nur erreicht werden, wenn die Temperatur der umgebenden Oberflächen, wie sie vom Thermosensor wahrgenommen wird, von der des Zielobjekts abweicht.

# Lizenzierung der Certified Apps

Die folgenden Lizenzen sind verfügbar für Irisity IRIS Core Intrusion App:

- **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](http://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**.

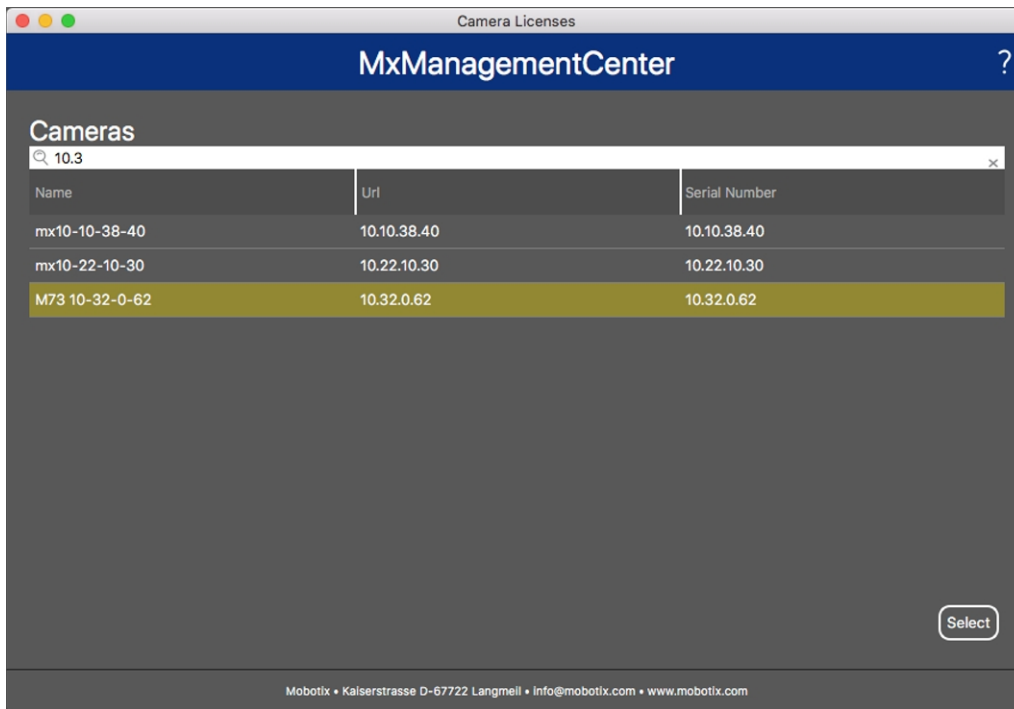


Abb. 1: Überblick über die Kamera-App-Lizenzen in MxManagementCenter

**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**.

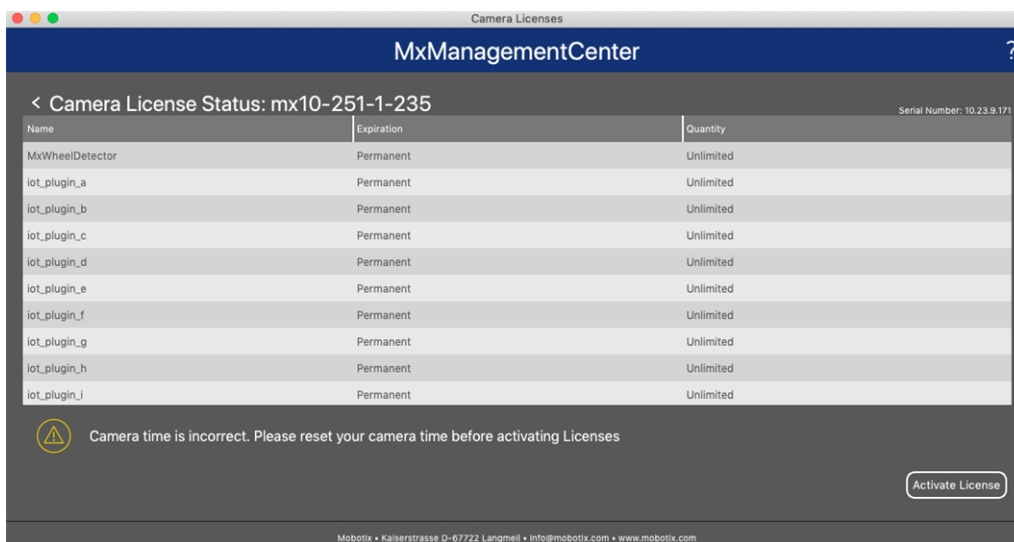




Abb. 2: Übersicht über die auf der Kamera installierten Lizenzen

**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.

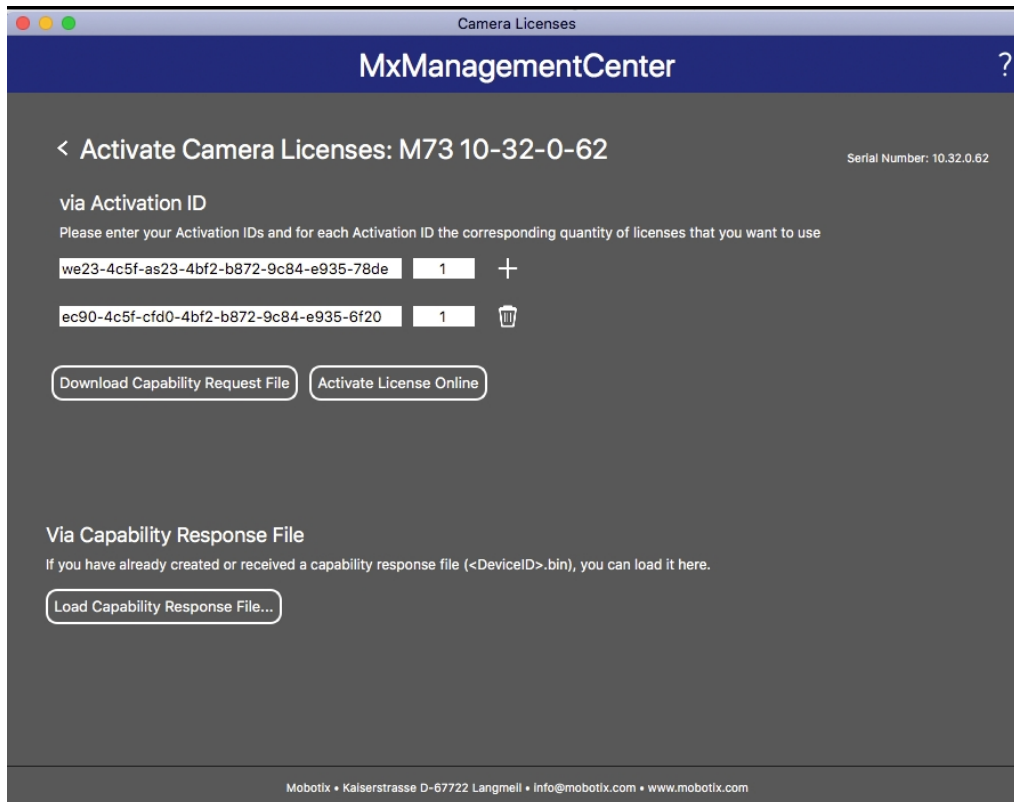


Abb. 3: Hinzufügen von Lizenzen

### 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. 15.)

## 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**.

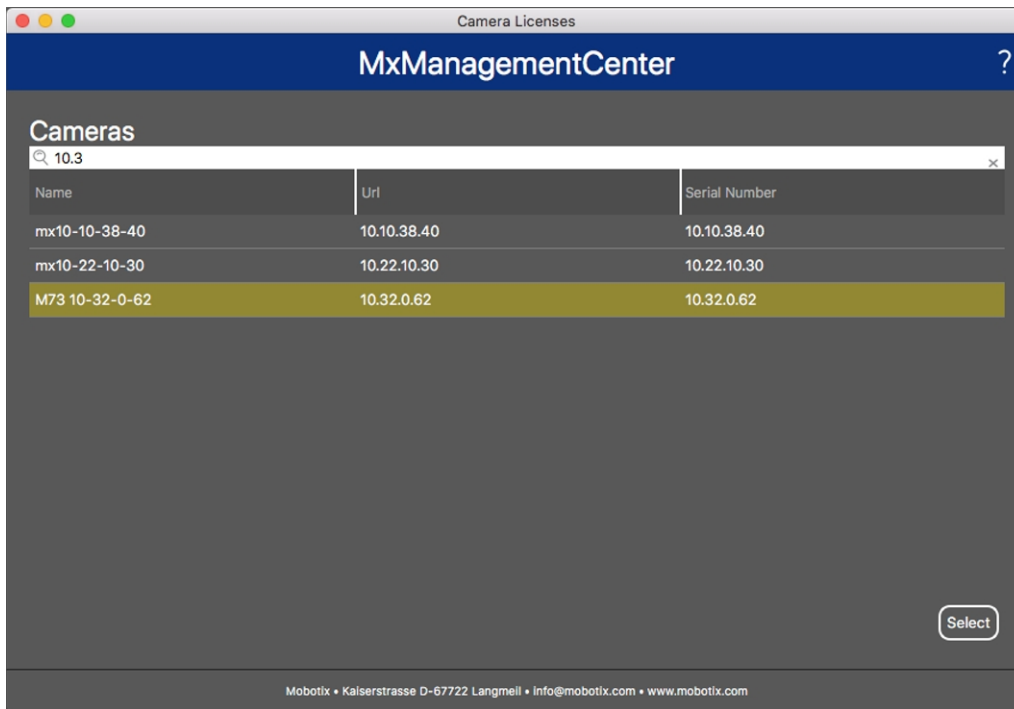


Abb. 4: Überblick über die Kamera-App-Lizenzen in MxManagementCenter

**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**.

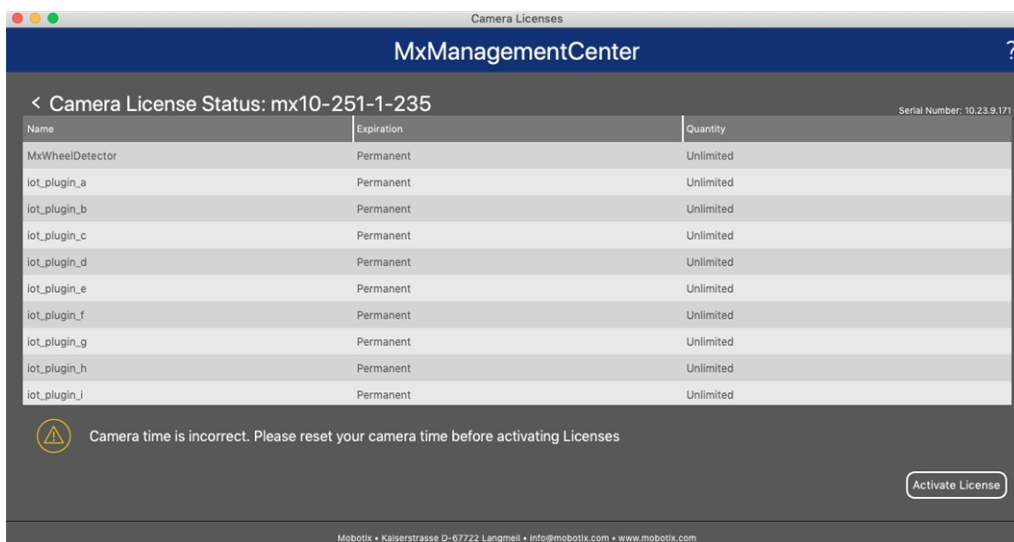




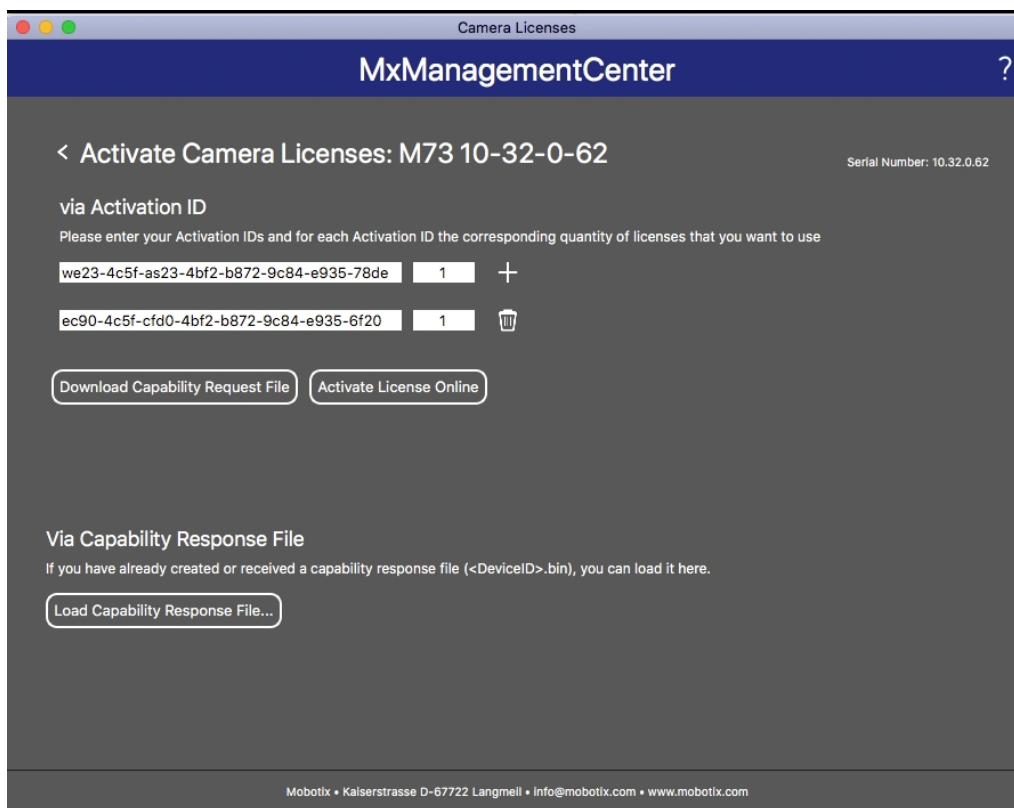
Abb. 5: Übersicht über die auf der Kamera installierten Lizenzen

**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. 6: 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**.

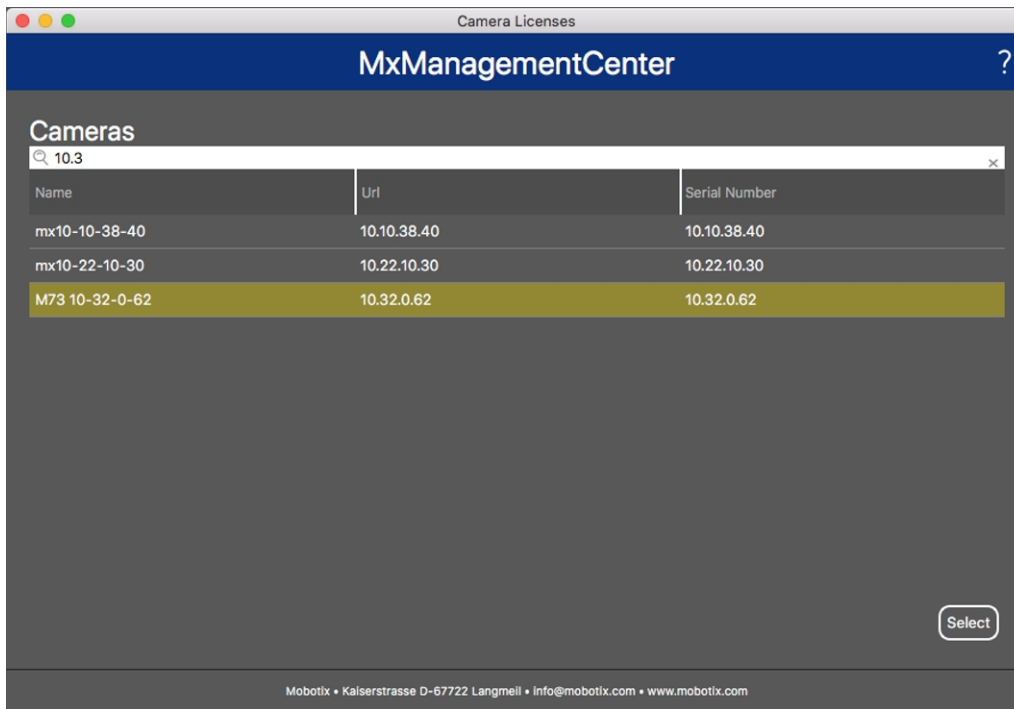


Abb. 7: Überblick über die Kamera-App-Lizenzen in MxManagementCenter

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



Abb. 8: Übersicht über die auf der Kamera installierten Lizenzen

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

<b>Spalte</b>	<b>Erläuterung</b>
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.

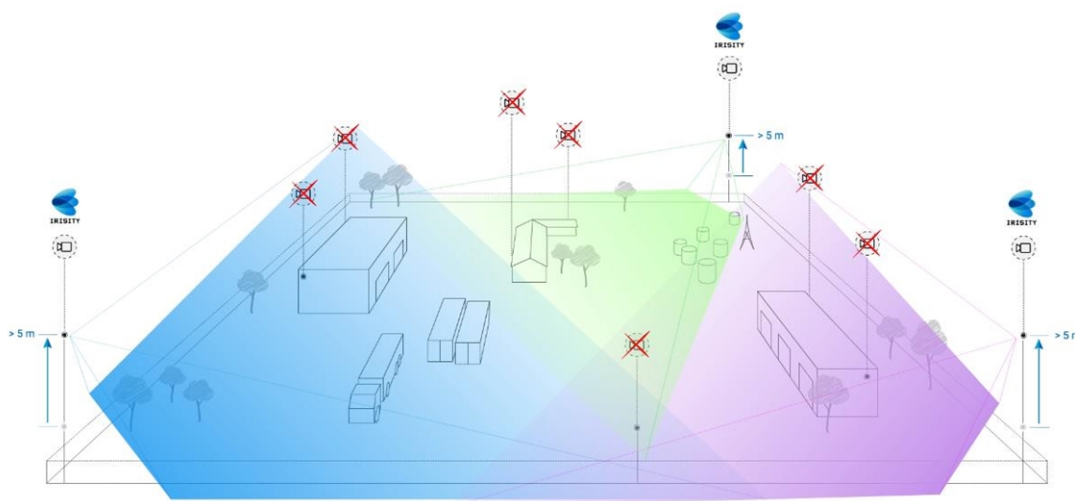
**HINWEIS!** Sie benötigen Administratorrechte zum Synchronisieren und Aktualisieren von Lizenzen.

# 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

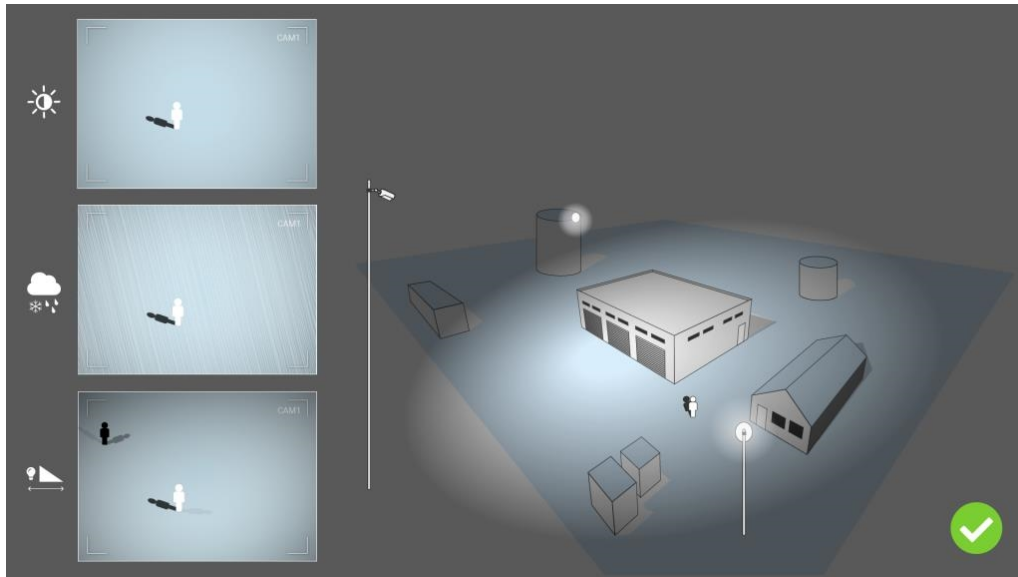
Bei der Planung Ihres Videoüberwachungssystems sollten Sie die höchstmöglichen Kamerapositionen bevorzugen, um mit jeder Kamera eine möglichst große Fläche abzudecken. Ziehen Sie eine Montagehöhe von mindestens 5 Metern in Betracht. Eine Montagehöhe von 10 bis 25 Metern führt in der Regel zu deutlich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



## 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.



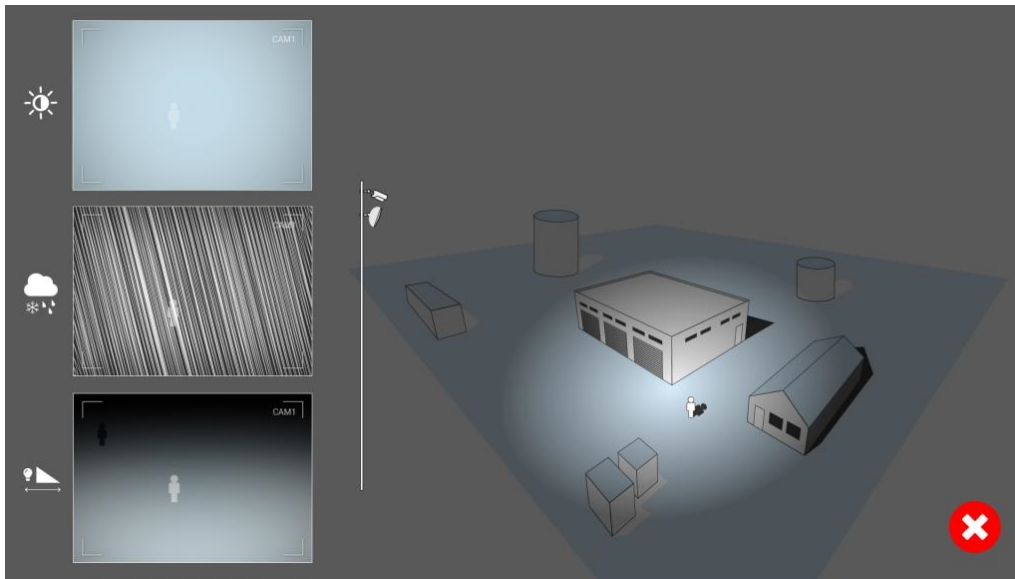
## Fehlerbehebung

### 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.



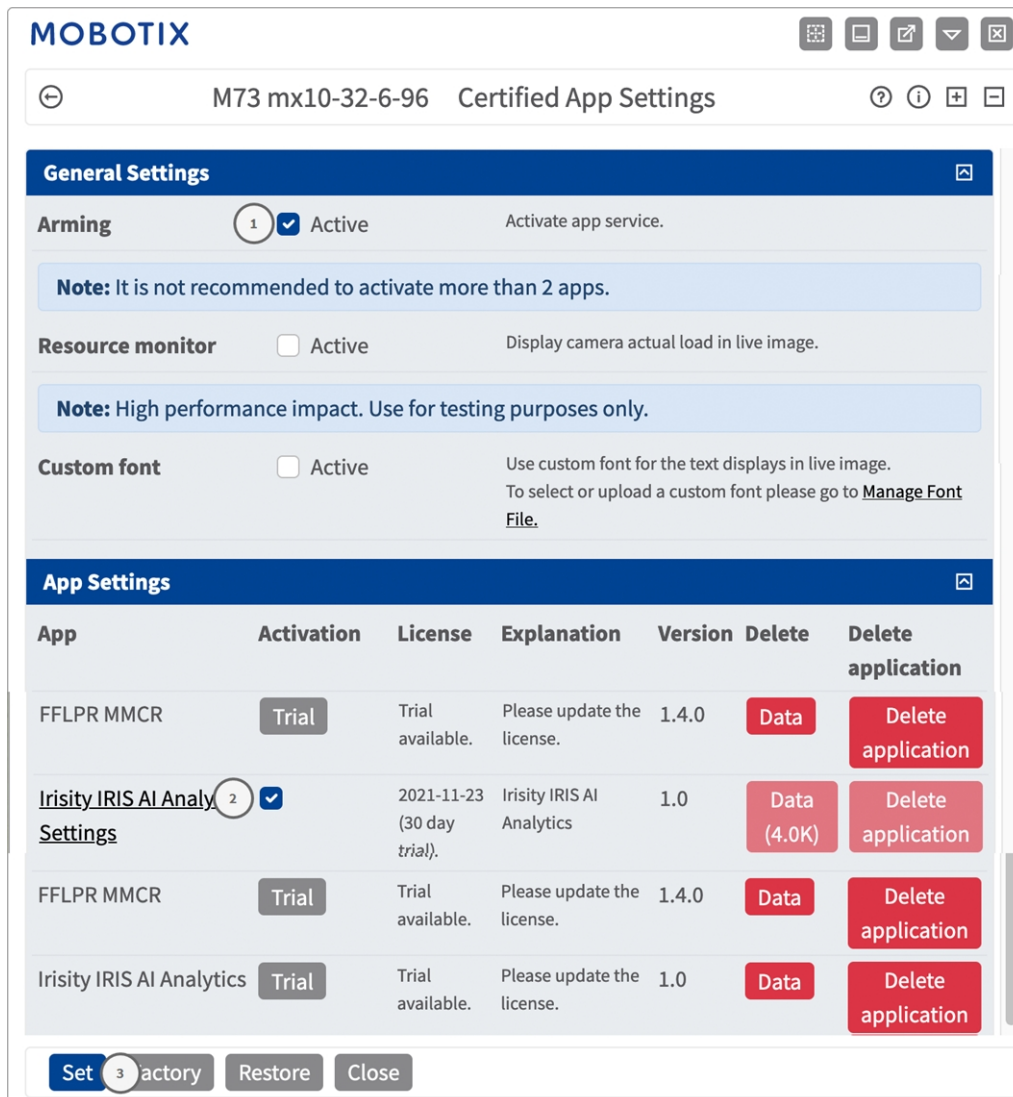
**Abb. 9:** Bei schwierigen Witterungsbedingungen können Eindringlinge fast unsichtbar werden und sich hinter Regen, Schnee oder Nebel verstecken.

# Aktivierung der Certified App-Schnittstelle

**VORSICHT!** Irisity IRIS Core Intrusion App 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\(s\)://<IP-Adresse der Kamera>/control](http(s)://<IP-Adresse der Kamera>/control)). Überprüfen Sie daher die Benutzerberechtigungen der Kamera.

1. Öffnen Sie in der Webschnittstelle der Kamera: **Setup-Menü > Zertifizierte App-Einstellungen** ([http\(s\)://<IP-Adresse der Kamera>/control/app\\_config](http(s)://<IP-Adresse der Kamera>/control/app_config)).



The screenshot shows the MOBOTIX Certified App Settings interface. The browser address bar displays 'M73 mx10-32-6-96 Certified App Settings'. The 'General Settings' section includes:

- Arming:** Checked (1) with a blue checkmark and the text 'Active Activate app service.'
- Resource monitor:** Unchecked with the text 'Active Display camera actual load in live image.'
- Custom font:** Unchecked with the text 'Active Use custom font for the text displays in live image. To select or upload a custom font please go to [Manage Font File](#).'

The 'App Settings' section contains a table with the following data:

App	Activation	License	Explanation	Version	Delete	Delete application
FFLPR MMCR	Trial	Trial available.	Please update the license.	1.4.0	Data	Delete application
<a href="#">Irisity IRIS AI Analytics Settings</a>	Checked (2)	2021-11-23 (30 day trial).	Irisity IRIS AI Analytics	1.0	Data (4.0K)	Delete application
FFLPR MMCR	Trial	Trial available.	Please update the license.	1.4.0	Data	Delete application
Irisity IRIS AI Analytics	Trial	Trial available.	Please update the license.	1.0	Data	Delete application

At the bottom, there are buttons for 'Set factory' (3), 'Restore', and 'Close'.

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 Core Intrusion App, p. 25](#).



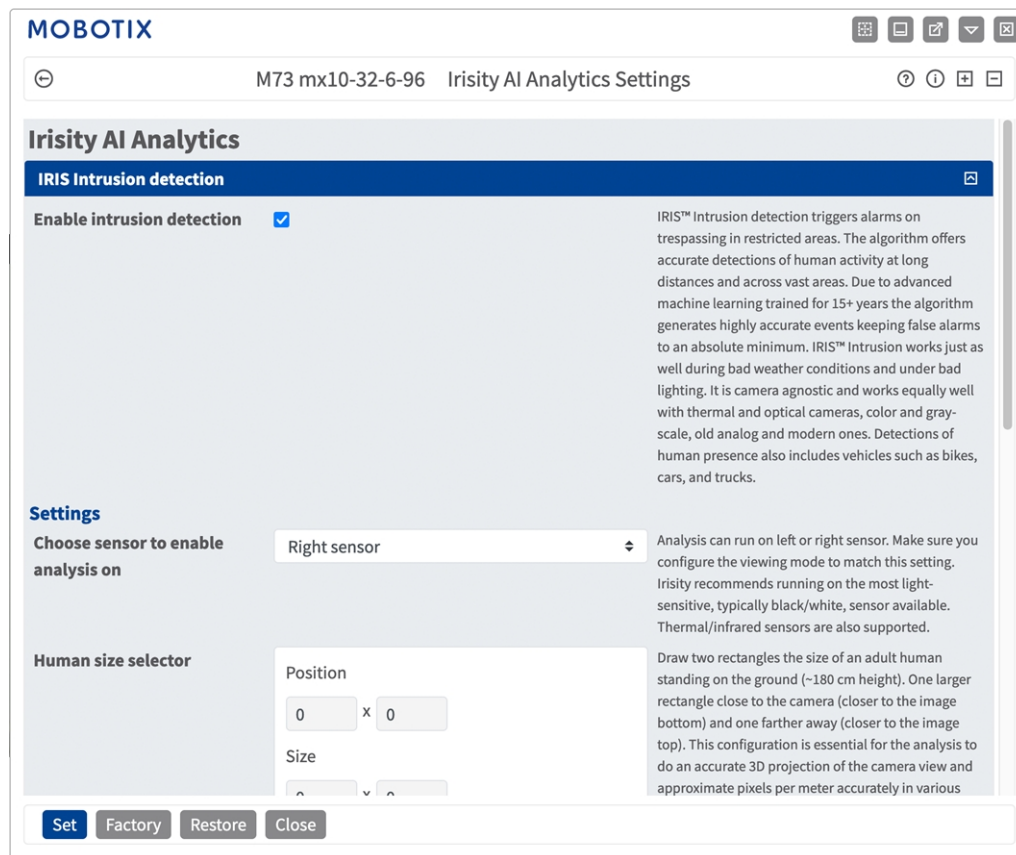
# Konfiguration von Irisity IRIS Core Intrusion App

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

1. Öffnen Sie in der Webschnittstelle der Kamera: **Setup-Menü > Zertifizierte App-Einstellungen** ([http\(s\)://<IP-Adresse der Kamera>/control/app\\_config](http(s)://<IP-Adresse der Kamera>/control/app_config)).
2. Klicken Sie auf den Namen des **Irisity IRIS Core Intrusion App**.

Das Konfigurationsfenster der App wird mit den folgenden Optionen angezeigt:

## IRIS-Eindringungserkennung



The screenshot displays the 'Irisity AI Analytics' configuration page. The 'IRIS Intrusion detection' section is highlighted in blue. Under 'Enable intrusion detection', there is a checked checkbox. To the right, a text block explains that the algorithm triggers alarms on trespassing in restricted areas and is highly accurate due to 15+ years of machine learning training. The 'Settings' section includes a dropdown for 'Choose sensor to enable analysis on' set to 'Right sensor', and a 'Human size selector' with 'Position' set to '0 x 0'. At the bottom, there are buttons for 'Set', 'Factory', 'Restore', and 'Close'.

**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:** Für die perspektivische Korrektur sind zwei Rechtecke erforderlich, die die Größe eines erwachsenen Menschen darstellen, der auf dem Boden steht (~180 cm Höhe) (siehe [Human Size Selector \(Menschgrößenauswahl\)](#), p. 26).
- **Alarm zones (Alarmzonen):** Im Live-Bild muss mindestens eine Alarmzone (Erkennungsbereich) definiert sein (siehe [Alarmzonen](#), p. 27).
- **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.

### Human Size Selector (Menschgrößenauswahl)

Die Konfiguration einer Menschgrößenauswahl 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.

Human size selector	Human size	Position	Size	
		264 x 1		Draw two rectangles the size of an adult human standing on the ground (~180 cm height). One larger rectangle close to the camera (closer to the image bottom) and one farther away (closer to the image top). This configuration is essential for the analysis to do an accurate 3D projection of the camera view and approximate pixels per meter accurately in various parts of the image.
		209 x 486		
		<a href="#">Edit Rectangle</a>		
	Human size	939 x 384		Draw each rectangle with the bottom side touching the ground in the position where you set the size of a human.
		92 x 320		
		<a href="#">Edit Rectangle</a>		

Zeichnen Sie daher ein größeres Rechteck in der Nähe der Kamera (näher am unteren Bildrand) und ein weiter entferntes Rechteck (näher am oberen Bildrand).

**HINWEIS!** Zeichnen Sie jedes Rechteck so, dass die Unterseite den Boden berührt, und zwar an der Stelle, an der Sie die Größe eines Menschen festlegen. (Siehe [Menschgrößenauswahl zeichnen.](#))

## Rechteckigen Bereich in der Live-Ansicht zeichnen

In der Live-Ansicht können Sie einen rechteckigen Bereich zeichnen. Je nach App sind diese Bereiche z. B. Erkennungsbereiche, ausgeschlossene Bereiche, Referenzbereiche, Menschrößenauswahl 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. Klicken Sie oben rechts in der Live-Ansicht auf **Senden**, um die Koordinaten des Polygons zu übernehmen.
4. Optional können Sie auf das **Papierkorb**-Symbol klicken, um den Erkennungsbereich zu löschen.

## Alarmzonen

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

**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. 28).

**Alarmzone hinzufügen:** Klicken Sie auf das **Plus**-Symbol ② .

**Bereich löschen:** Klicken Sie auf das **Papierkorb**-Symbol ③ .

**Eckpunkt löschen:** Klicken Sie auf das **Papierkorb**-Symbol ④ .

### 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.

## 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.

IRIS Tampering detection		
<b>Enable camera covered detection</b>	<input checked="" type="checkbox"/>	Check to activate the algorithm.  IRIS™ Tampering detection triggers events both when the camera is covered and when this has been resolved.
<b>Enable camera redirected detection</b>	<input checked="" type="checkbox"/>	Check to activate the algorithm.  IRIS™ Tampering detection triggers events when the camera is suddenly redirected.
<b>Settings</b>		
<b>Choose sensor to enable analysis on</b>	Right sensor	Analysis can run on left or right sensor.

**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 diese Option, um den Algorithmus zu aktivieren.

**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.

## Visual Overlays (Visuelle Überlagerungen)

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

Visual overlays		
<b>Alarming object</b>	<input checked="" type="checkbox"/>	Show a bounding box around the object triggering an alarm for 10 seconds after the alarm.
<b>Alarm zones</b>	<input checked="" type="checkbox"/>	Show the active analytics areas.
<b>Running analytics</b>	<input checked="" type="checkbox"/>	Show overlay text when the analytics is running, like 'Irisity - IRIS AI Analytics'.
<b>Detection text</b>	<input type="checkbox"/>	Overlay a box showing text like 'Intrusion detected' when alarms are triggered. Typically, only used during demos or testing.
<b>Diagnostics</b>	<input type="checkbox"/>	Overlay various diagnostics and tracking overlays. Not recommended for production use.

**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:** Aktivieren Sie diese Option, um ein Feld mit Text wie „Eindringen erkannt“ einzublenden, 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:



- Klicken Sie auf **Festlegen**, um Ihre Einstellungen zu aktivieren und bis zum nächsten Neustart der Kamera zu speichern.
- Klicken Sie auf **Werkseinstellungen**, um die Werkseinstellungen für dieses Dialogfeld zu laden (diese Schaltfläche ist möglicherweise nicht in allen Dialogfeldern vorhanden).
- Klicken Sie auf **Wiederherstellen**, um alle Änderungen seit dem letzten permanenten Speichern der Konfiguration zu verwerfen.
- Klicken Sie auf **Schließen**, um den Dialog zu beenden. Hierbei wird geprüft, ob Änderungen der Gesamtkonfiguration vorliegen. Ist dies der Fall, werden Sie gefragt, ob die Gesamtkonfiguration dauerhaft gesichert werden soll.

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

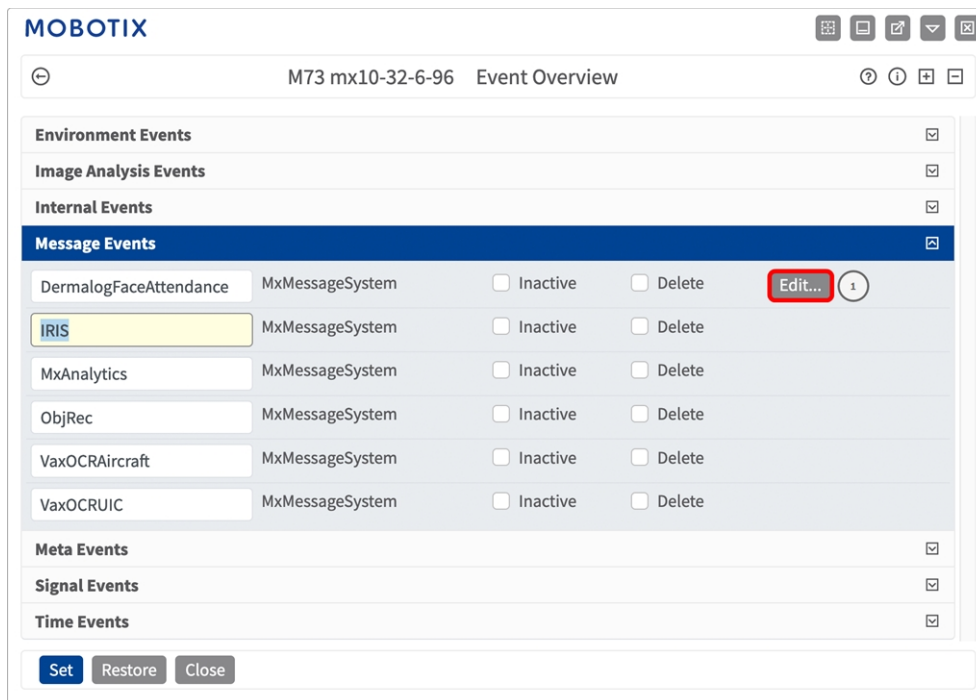
- 128-Bit-Verschlüsselung gewährleistet den Schutz und die Sicherheit von Nachrichteninhalten.
- MxMessages können von jeder Kamera der Mx6- und 7-Serie aus verteilt werden.
- Der Nachrichtenbereich kann für jede MxMessage einzeln definiert werden.
  - **Lokal:** Die Kamera erwartet eine MxMessage in 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. 23](#)) wird automatisch ein generisches Nachrichtenereignis für diese spezifische App in der Kamera generiert.

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





2. Klicken Sie auf **Bearbeiten** ⓘ , um die Ereigniseigenschaften im Detail anzuzeigen und zu konfigurieren.

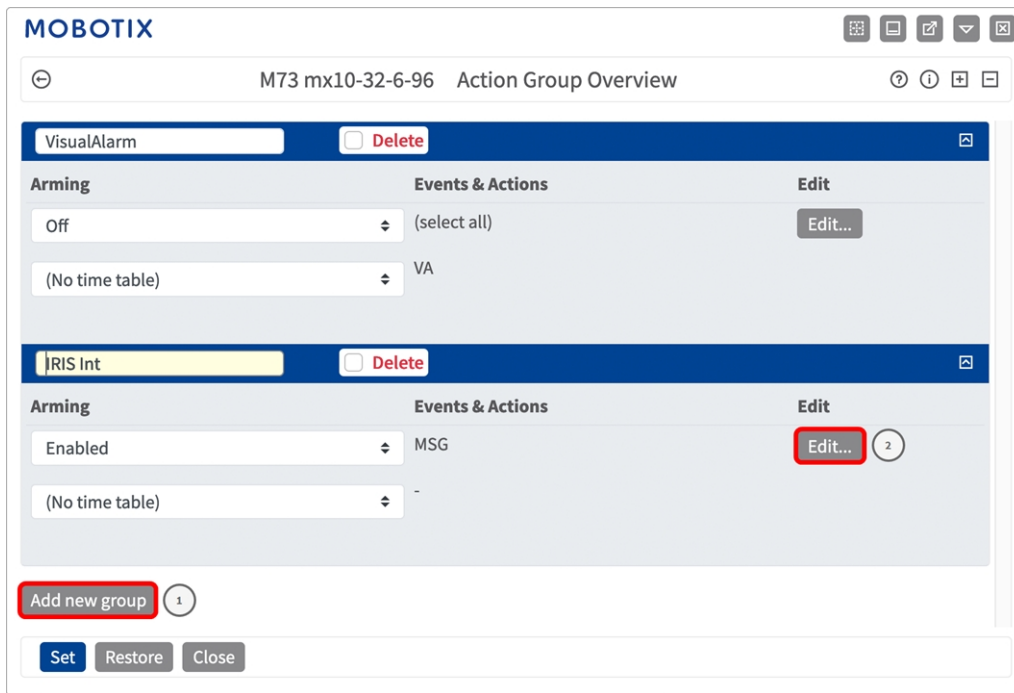
The screenshot shows the MOBOTIX configuration interface for Message Events. The interface is titled "M73 mx10-32-6-96 Message Events". It features a table with columns for Attribute, Value, and Explanation. The "IRIS" event is selected and highlighted in blue. Below the table, the configuration details for the selected event are shown, including Event Dead Time (5), Event Sensor Type (MxMessageSystem), Message Name (IRIS), Message Range (Local), and Filter Message Content (No Filter). The interface also includes buttons for Set, Factory, Restore, and Close.

## Aktionsabwicklung – Konfiguration einer Aktionsgruppe

**VORSICHT!** Um Ereignisse zu verwenden, Aktionsgruppen auszulösen oder Bilder aufzuzeichnen, muss die allgemeine Aktivierung der Kamera aktiviert sein ([http\(s\):/<IP-Adresse der Kamera>/control/settings](http(s):/<IP-Adresse der Kamera>/control/settings)).

Eine Aktionsgruppe definiert, welche Aktionen vom Irisity IRIS Core Intrusion App-Ereignis ausgelöst werden.

1. Öffnen Sie in der Webschnittstelle der Kamera: **Setup-Menü > Aktionsgruppenübersicht** ([http\(s\):/<IP-Adresse der Kamera>/control/actions](http(s):/<IP-Adresse der Kamera>/control/actions)).



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.

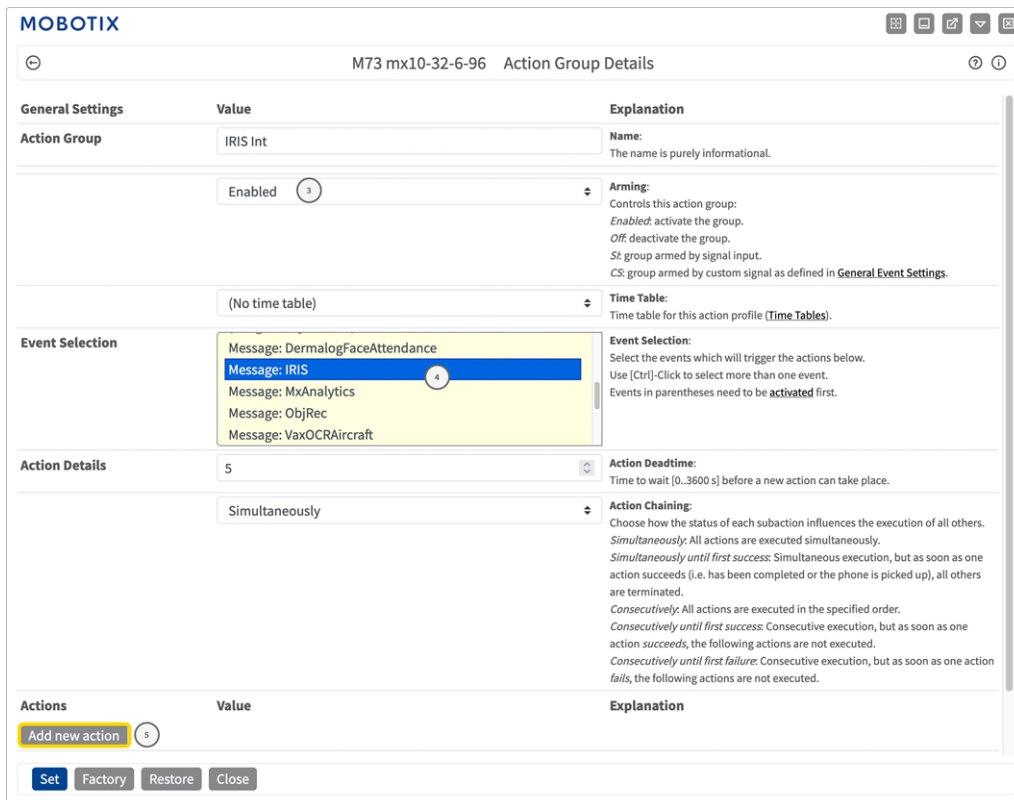
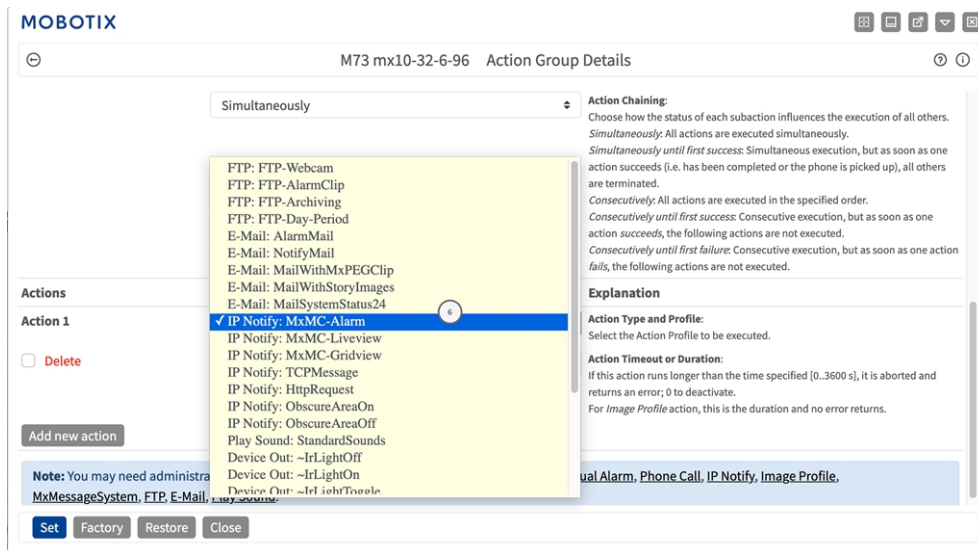


Abb. 10: Konfigurieren einer Aktionsgruppe

4. Aktivieren Sie **Arming** ③ (Aktivierung) der Aktionsgruppe.
5. Wählen Sie das Nachrichtenergebnis 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.



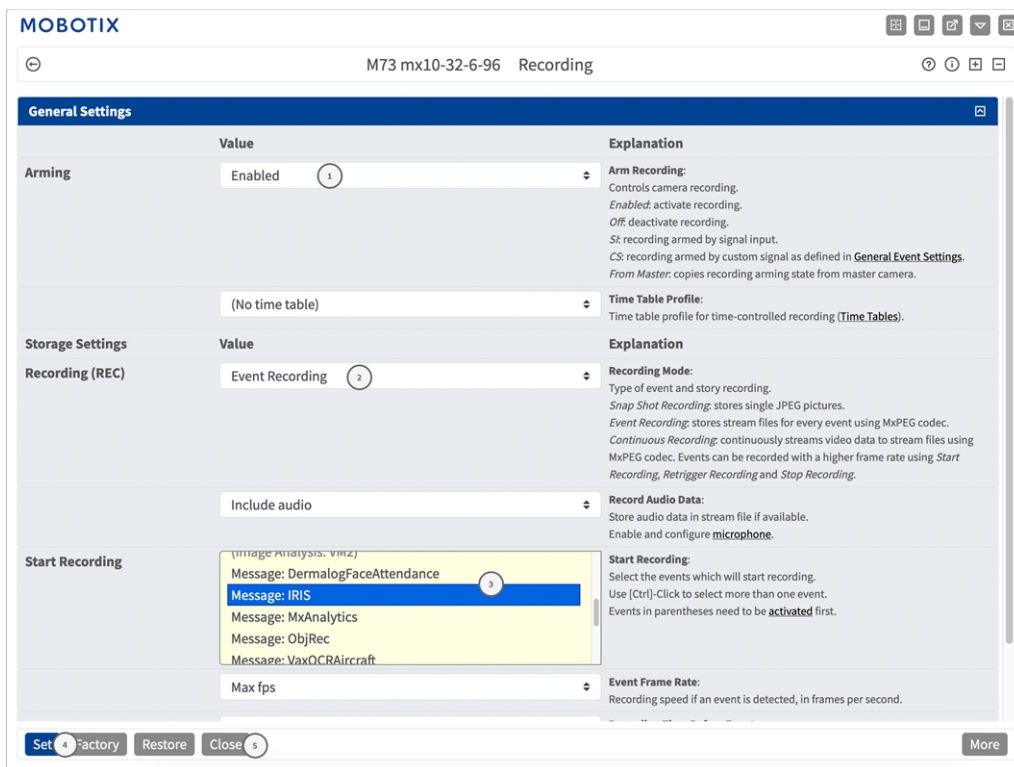
**HINWEIS!** Wenn das erforderliche Aktionsprofil noch nicht verfügbar ist, können Sie in den Abschnitten "MxMessageSystem", "Übertragungsprofile" und "Audio- und VoIP-Telefonie" im Admin-Menü ein neues Profil erstellen.

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-Menü > Ereignissteuerung > Aufzeichnung** ([http\(s\)/<IP-Adresse der Kamera>/control/recording](http(s)/<IP-Adresse der Kamera>/control/recording)).



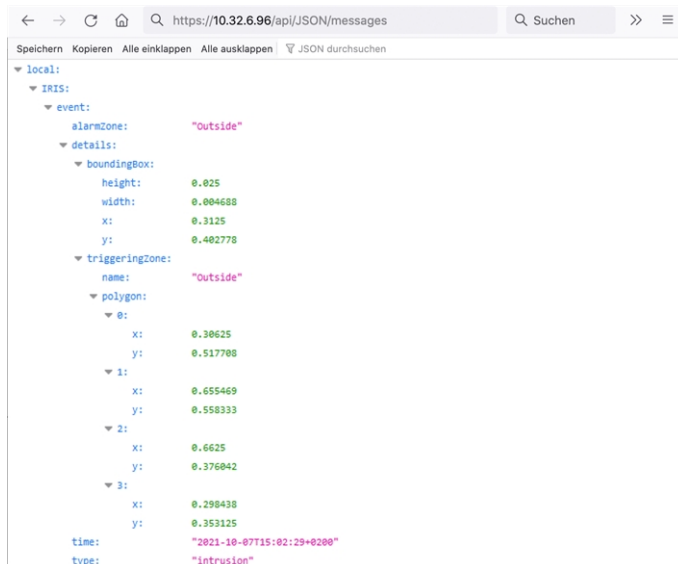
2. Aktivieren Sie **Arm Recording** ① (Aufzeichnung aktivieren).
3. Wählen Sie unter **Speichereinstellungen > Aufzeichnung** einen **Aufnahmemodus** ② aus. Die folgenden Modi sind verfügbar:
  - Einzelbildaufzeichnung
  - Ereignisaufzeichnung
  - Kontinuierliche Aufzeichnung
4. Wählen Sie in der Liste **Start recording** ③ (Aufzeichnung starten) das soeben erstellte Nachrichtenergebnis 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.



```
https://10.32.6.96/api/JSON/messages
Suchen
Speichern Kopieren Alle einklappen Alle ausklappen JSON durchsuchen
local:
  IRIS:
    event:
      alarmZone: "outside"
    details:
      boundingBox:
        height: 0.025
        width: 0.004688
        x: 0.3125
        y: 0.402778
      triggeringZone:
        name: "outside"
        polygon:
          0:
            x: 0.30625
            y: 0.517708
          1:
            x: 0.655469
            y: 0.558333
          2:
            x: 0.6625
            y: 0.376042
          3:
            x: 0.298438
            y: 0.353125
      time: "2021-10-07T15:02:29+0200"
      type: "intrusion"
```

**HINWEIS!** Um die Metadatenstruktur des letzten App-Ereignisses anzuzeigen, geben Sie die folgende URL in die Adresszeile Ihres Browsers ein: [http\(s\)://IPAdresseOfYourCamera/api/json/messages](http(s)://IPAdresseOfYourCamera/api/json/messages)

# Erstellen eines benutzerdefinierten Nachrichteneignisses

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

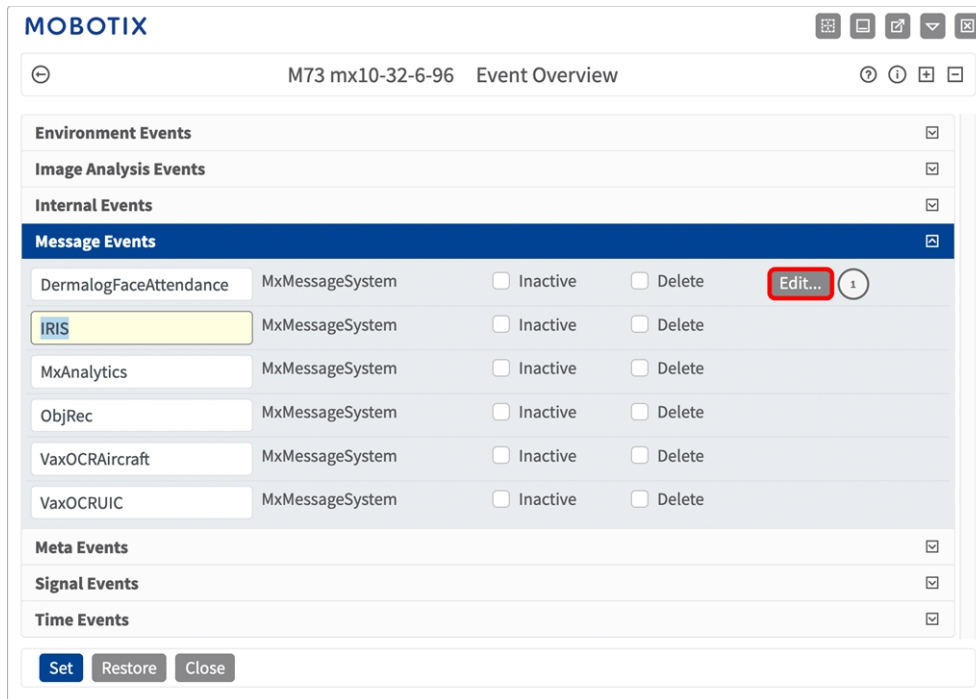


Abb. 11: Beispiel: Generisches Nachrichteneignis von Irisity IRIS Core Intrusion App

2. Klicken Sie auf **Bearbeiten** ① , um die Ereignisseigenschaften im Detail anzuzeigen und zu konfigurieren.

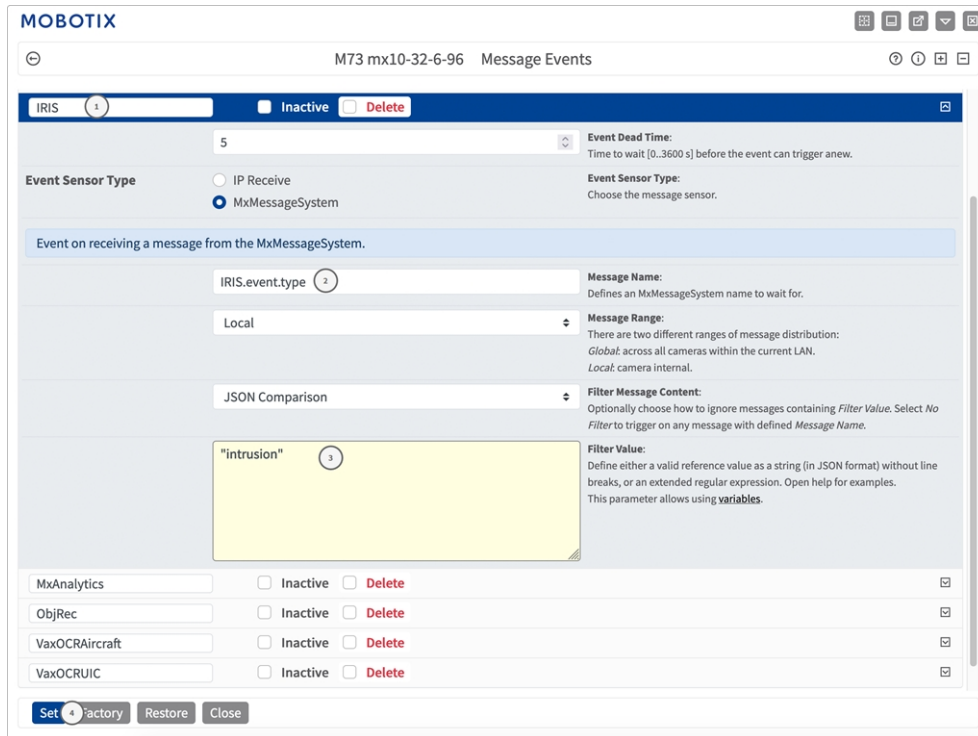


Abb. 12: Beispiel: Ereignis für Eindringungsnachricht

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“ (Nachrichtennamen):** Geben Sie den „Nachrichtennamen“ ② gemäß der Ereignisdokumentation der entsprechenden App ein (siehe [Beispiele für Nachrichtennamen und Filterwerte von Irisity IRIS Core Intrusion App](#), p. 40).
  - **„Message Range“ (Meldungsbereich):**
    - **Lokal:** Standardeinstellungen für Irisity IRIS Core Intrusion App
    - **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 Core Intrusion App](#), p. 40

**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 Core Intrusion App

IRIS Eindringungserkennung	MxMessage-Name	Filterwert
Generisches Ereignis	IRIS	
Alarmzonenergebnis	IRIS.event.alarmZone	Name der Alarmzone, z. B.: „Eindringzone 2“
Details des Begrenzungsrahmens	IRIS.event.details.boundingBox	Koordinaten der Eckpunkte des Begrenzungsrahmens, z. B.: „Höhe“: 00,5, „Breite“: 0,0256, „x“: 0,05, „y“: 0,4658)
Details zur auslösenden Zone	IRIS.event.details.triggeringZone.polygone	Koordinaten der Eckpunkte der auslösenden Zone, z. B.: [{ „x“: 0,456, „y“: 0,3569}, { „x“: 0,568, „y“: 0,5 } , ...]
Ereignistyp	IRIS.event.type	„Eindringen“ oder „Manipulation“



<b>IRIS Eindringungserkennung</b>	<b>MxMessage-Name</b>	<b>Filterwert</b>
Ereignisuntertyp	IRIS.event.subType	Untertypen des Ereignisses. Mögliche Untertypen für ein Manipulationsereignis sind z. B. „abgedeckt“ oder „verstellt“
Ereignisstatus	IRIS.event.state	Statusdefinition, z. B.: „gelöst“, „pointInTime“ usw.
Ereigniszeit	IRIS.event.time	Datumszeichenfolge, z. B.: „2023-06-19T09:40:47+0200“

---

# MOBOTIX

BeyondHumanVision

DE\_07.24

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

MOBOTIX ist eine Marke der MOBOTIX AG, die in der Europäischen Union, in den USA und in anderen Ländern eingetragen ist. Änderungen vorbehalten. MOBOTIX übernimmt keine Haftung für technische oder redaktionelle Fehler oder Auslassungen in diesem Dokument. Alle Rechte vorbehalten. © MOBOTIX AG 2021