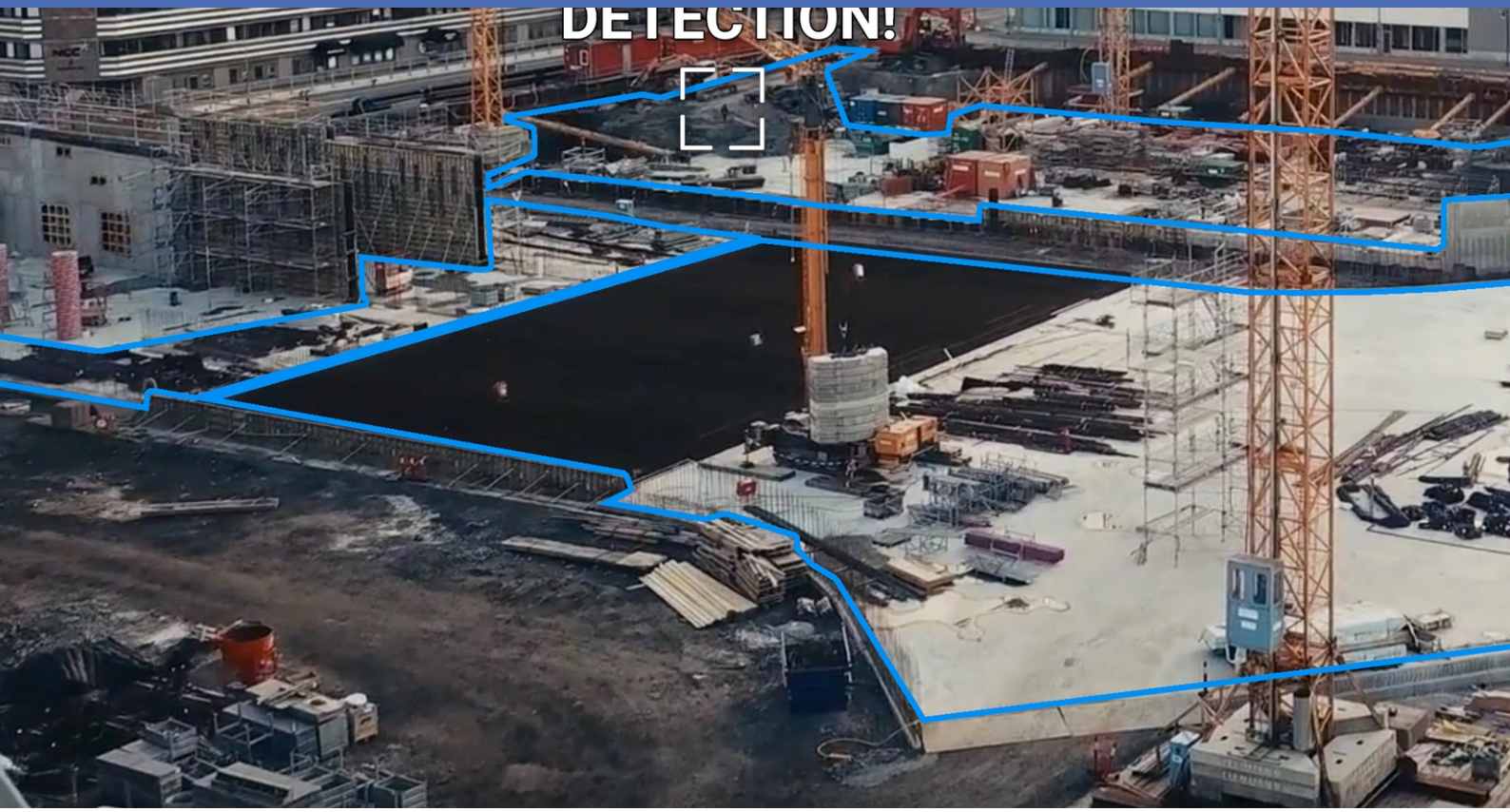
Guideline

Irisity IRIS AI Analytics - Intrusion Detection



BeyondHumanVision

MOBOTIX

V1.09_1/30/2023, Order Code: Mx-APP-IRIS-C-INT

Table of Contents

1

Before You Start

Support

If you need technical support, please contact your MOBOTIX dealer. If your dealer cannot help you, he will contact the support channel to get an answer for you as quickly as possible.

If you have internet access, you can open the MOBOTIX help desk to find additional information and software updates. Please visit:

www.mobotix.com > Support > Help Desk

Safety Notes

- This product must not be used in locations exposed to the dangers of explosion.
- Do not use this product in a dusty environment.
- Protect this product from moisture or water entering the housing.
- Install this product as outlined in this document. A faulty installation can damage the product!
- This equipment is not suitable for use in locations where children are likely to be present.
- When using a Class I adapter, the power cord shall be connected to a socket-outlet with proper ground connection.
- To comply with the requirements of EN 50130-4 regarding the power supply of alarm systems for 24/7 operation, it is highly recommended to use an uninterruptible power supply (UPS) for backing up the power supply of this product.
- This equipment is to be connected only to PoE networks without routing to other networks.

Legal Notes

Legal Aspects of Video and Sound Recording

You must comply with all data protection regulations for video and sound monitoring when using MOBOTIX AG products. Depending on national laws and the installation location of the cameras, the recording of video and sound data may be subject to special documentation or it may be prohibited. All users of MOBOTIX products are therefore required to familiarize themselves with all applicable regulations and to comply with these laws. MOBOTIX AG is not liable for any illegal use of its products.

Declaration of Conformity

The products of MOBOTIX AG are certified according to the applicable regulations of the EC and other countries. You can find the declarations of conformity for the products of MOBOTIX AG on www.mobotix.com under **Support > Download Center > Marketing & Documentation > Certificates & Declarations of Conformity**.

RoHS Declaration

The products of MOBOTIX AG are in full compliance with European Unions Restrictions of the Use of Certain Hazardous Substances in Electrical and Electronic Equipment (RoHS Directive 2011/65/EC) as far as they are subject to these regulations (for the RoHS Declaration of MOBOTIX, please see www.mobotix.com, **Support > Download Center > Marketing & Documentation > Brochures & Guides > Certificates**).

Disposal

Electrical and electronic products contain many valuable materials. For this reason, we recommend that you dispose of MOBOTIX products at the end of their service life in accordance with all legal requirements and regulations (or deposit these products at a municipal collection center). MOBOTIX products must not be disposed of in household waste! If the product contains a battery, please dispose of the battery separately (the corresponding product manuals contain specific directions if the product contains a battery).

Disclaimer

MOBOTIX AG does not assume any responsibility for damages, which are the result of improper use or failure to comply to the manuals or the applicable rules and regulations. Our General Terms and Conditions apply. You can download the current version of the **General Terms and Conditions** from our website at www.-mobotix.com by clicking on the corresponding link at the bottom of every page.

About Irisity IRIS AI Analytics - Intrusion Detection

Detect human activity in armed zones

Irisity IRIS AI Analytics - Intrusion Detection triggers alarms on trespassing in restricted areas. The algorithm offers accurate detections of human activity at long distances and across vast areas. The application has an accuracy of up to 99 %. The app can be tested free of charge for 30 days and can be activated for an unlimited period. Detections of human presence also includes vehicles such as bikes, cars, and trucks - even during bad weather conditions and under bad lighting.

- Detects the intrusion of objects of interest into user-defined detection zones / areas
- Designed for reliable detection of people and vehicles covering only small portions of the field of view
- Reduction of false alarms to a minimum by filtering out non-critical motion (e.g. trees, clouds, etc.)
- Simultaneous detection on one or more image sensors
- MOBOTIX events via MxMessageSystem
- Consolidated event search via MxManagementCenter Smart Data Interface and / or MOBOTIX HUB

CAUTION! ECO Thermal sensor modules are not supported by this app.

Smart Data Interface to MxManagementCenter

This app has a Smart Data interface to MxManagementCenter.

With the MOBOTIX Smart Data System, transaction data can be linked to the video recordings made at the time of the transactions. Smart Data source can be e.g. MOBOTIX Certified Apps (no license required) or general Smart Data sources (license required) like POS systems or license plate recognition systems.

The Smart Data System in MxManagementCenter enables you to quickly find and review any suspicious activities. The Smart Data Bar and the Smart Data View are available for searching and analyzing transactions. The Smart Data Bar provides a direct overview of the most recent transactions (from the last 24 hours) and for this reason it is convenient to use it for reviews and searches.

NOTE! For information on how to use the Smart Data System, see the corresponding online help of the camera software and MxManagementCenter.

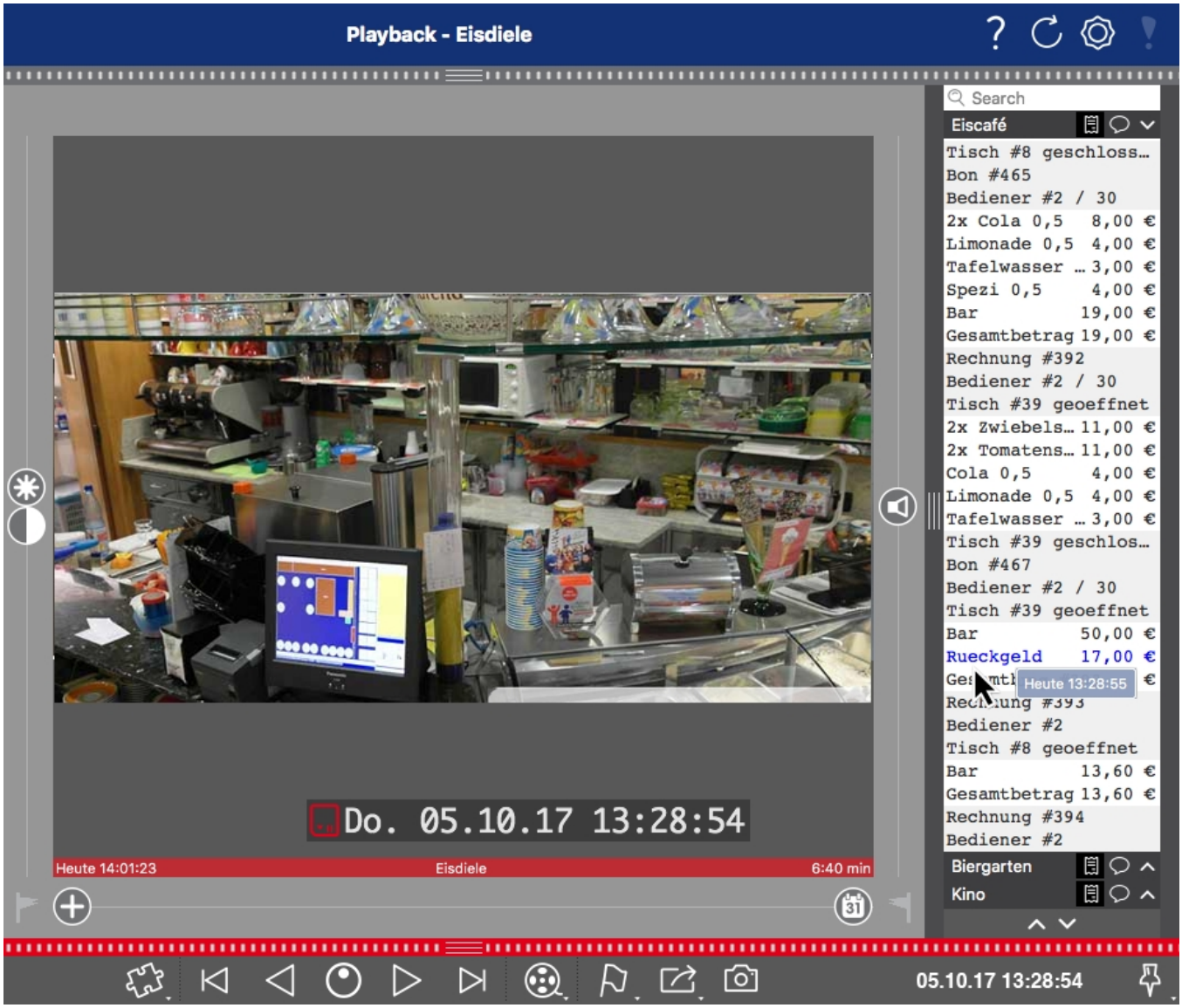


Fig. 1: : Smart Data Bar in MxManagementCenter (Example: POS System)

Technical Specifications

Product Information

Product Name	Irisity IRIS AI Analytics - Intrusion Detection
Order Code	Mx-APP-IRIS-C-INT
Supported MOBOTIX Cameras	Mx-M73A, Mx-S74A
Minimum Camera Firmware	V7.3.0.x
MxManagementCenter Integration	■ min. MxMC v2.5.3 ■ Configuration: Advanced Config license required ■ Research: Smart Data Interface license included

Product Features

App Features	■ Detects the intrusion of objects of interest into user-defined detection zones / areas ■ Designed for reliable detection of people and vehicles covering only small portions of the field of view ■ Reduction of false alarms to a minimum by filtering out non-critical motion (e.g. trees, clouds, etc.) ■ Simultaneous detection on one or more image sensors ■ MOBOTIX events via MxMessageSystem ■ Consolidated event search via MxManagementCenter Smart Data Interface and / or MOBOTIX HUB
Maximum number of recognition zones	20
Meta Data / Statistic formats	JSON
Trial License	30-day trial license pre-installed
MxMessageSystem supported	Yes
MOBOTIX Events	Yes
ONVIF Events	Yes (Generic Message event)

Scene Requirements

Minimum object height	20 px / ~6% of image height (analysis currently locked to 640 x 360 resolution)
Camera mounting height	min. 2m (considering scene requirements mostly 5 - 20m are optimal)
Maximum Vertical Angle	180°
Maximum Horizontal Angle	180°
Maximum Tilt Angle	Down tilt only: no limit

Technical App Specifications

Synchronous / Asynchronous App	Asynchronous
Accuracy	> 99% (considering scene requirements)
Processed number of frames per second	Typ. 10 fps
Detection time	~ 2 sec

Licensing Certified Apps

The following licenses are available for the Irisity IRIS AI Analytics - Intrusion Detection:

- **30-day test license** pre-installed
- **permanent commercial license**

The usage period begins with activation of the app interface (see)

NOTE! For buying or renewing a license, contact your MOBOTIX Partner.

NOTE! Apps are usually pre-installed with the firmware. In rare cases, apps must be downloaded from the website and installed. In this case see **www.mobotix.com > Support > Download Center > Marketing & Documentation**, download and install the app.

License Activation of Certified Apps in MxManagementCenter

After a test period commercial licenses must be activated for use with a valid license key.

Online-Activation

After receiving the activation IDs, activate them in MxMC as follows:

1. Select from the menu **Window > Camera App Licenses**.
2. Select the camera on which you want to license apps and click **Select**.

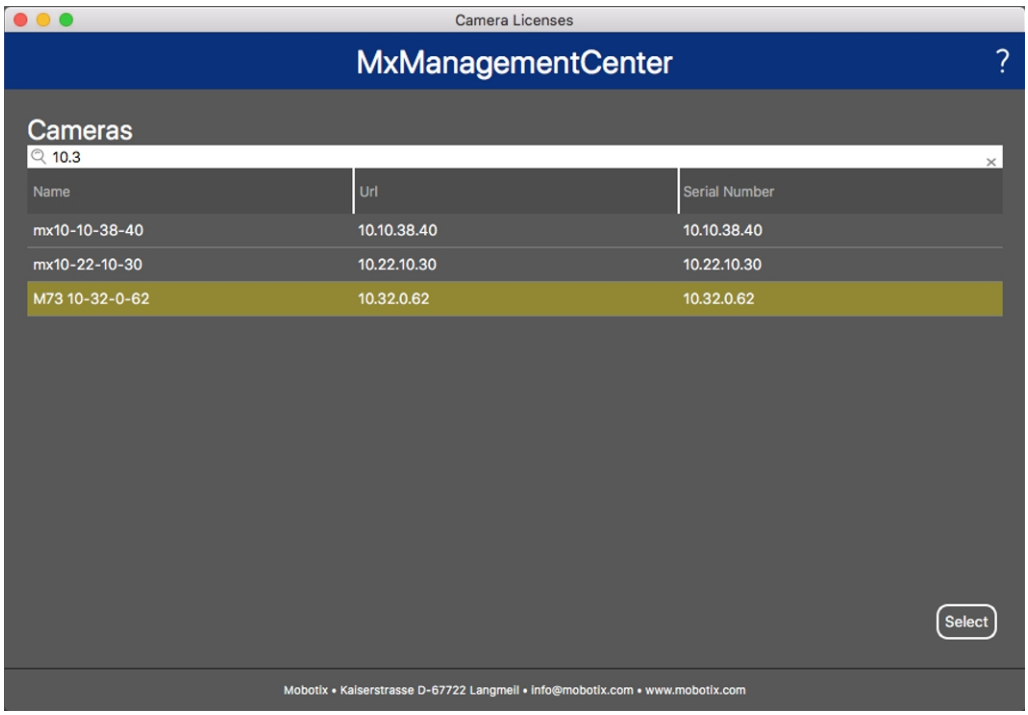


Fig. 2: Overview of Camera App Licenses in MxManagementCenter

NOTE! If necessary, correct the time set on the camera.

1. An overview of the licenses installed on the camera may be displayed. Click **Activate License**.

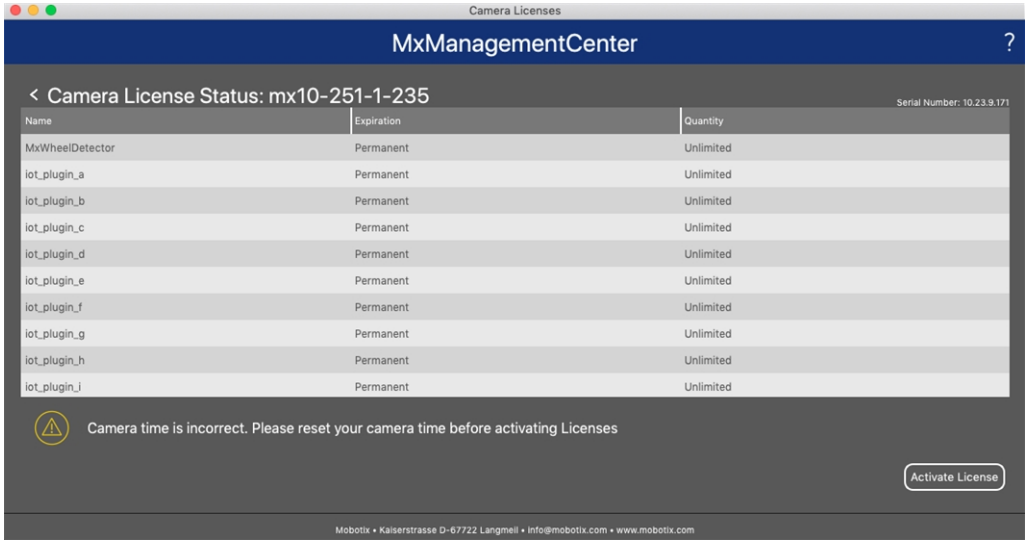


Fig. 3: Overview of the licenses installed on the camera

NOTE! If necessary, correct the time set on the camera.

2. Enter a valid Activation ID and specify the number of licenses to install on this computer.
3. If you want to license another product, click on . In the new row, enter the appropriate Activation ID and the number of licenses you want.
4. To remove a line click .

5. When you have entered all Activation IDs, click **Activate License Online**. During activation, **MxMC** connects to the license server. This requires an Internet connection.

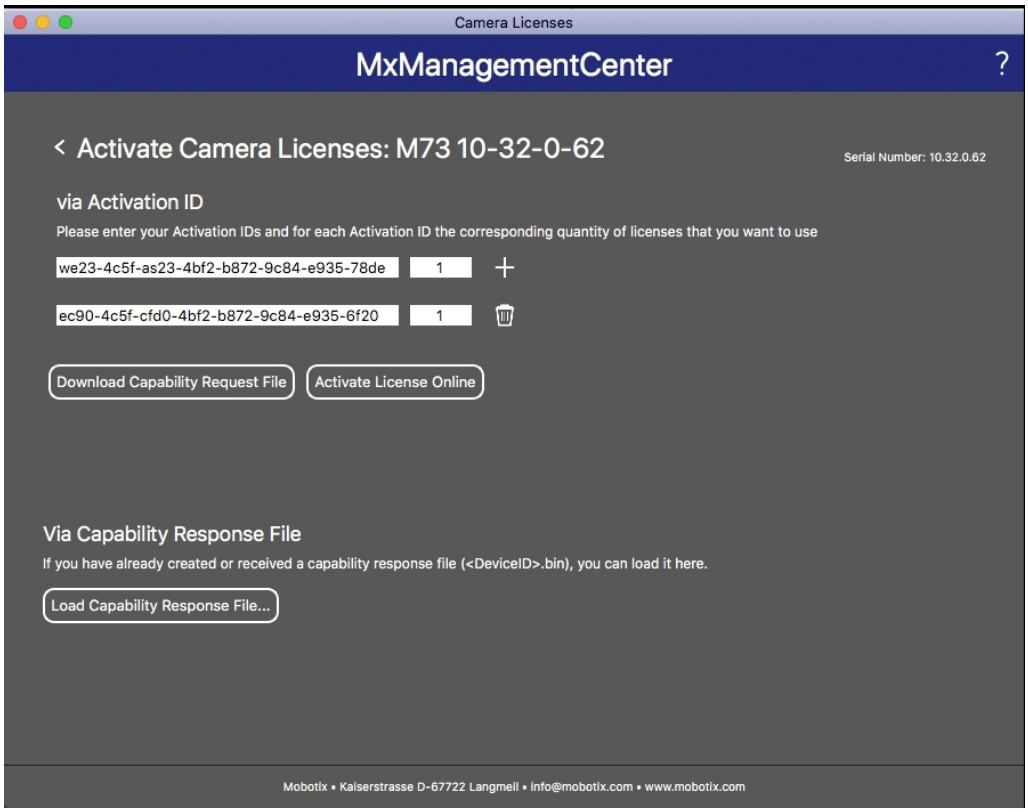


Fig. 4: Adding licenses

Successful activation

After successful activation, a new log in is required to apply the changes. Alternatively, you can return to license management.

Failed activation (missing internet connection)

If the license server cannot be reached, e.g. due to a missing internet connection, apps can also be activated offline. (see Offline Activation, p. 12).

Offline Activation

For offline activation, the partner/installer from whom you purchased the licenses can generate a capability response (.bin file) on the license server to activate their licenses.

1. Select from the menu **Window > Camera App Licenses**.
2. Select the camera on which you want to license apps and click **Select**.

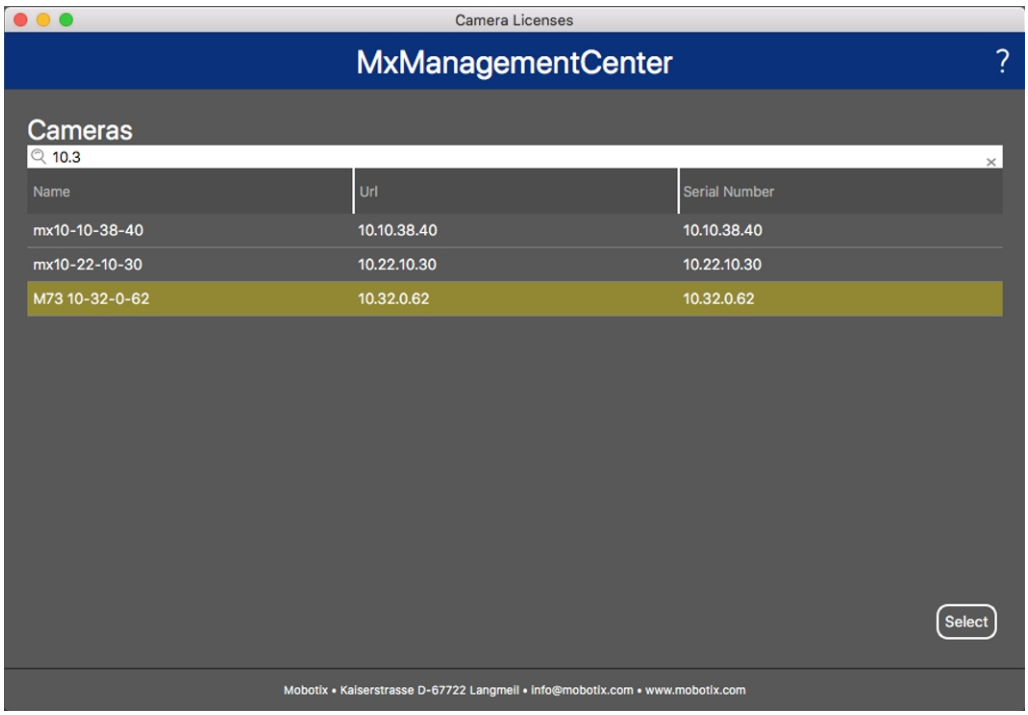


Fig. 5: Overview of Camera App Licenses in MxManagementCenter

NOTE! If necessary, correct the time set on the camera.

3. An overview of the licenses installed on the camera may be displayed. Click **Activate License**.

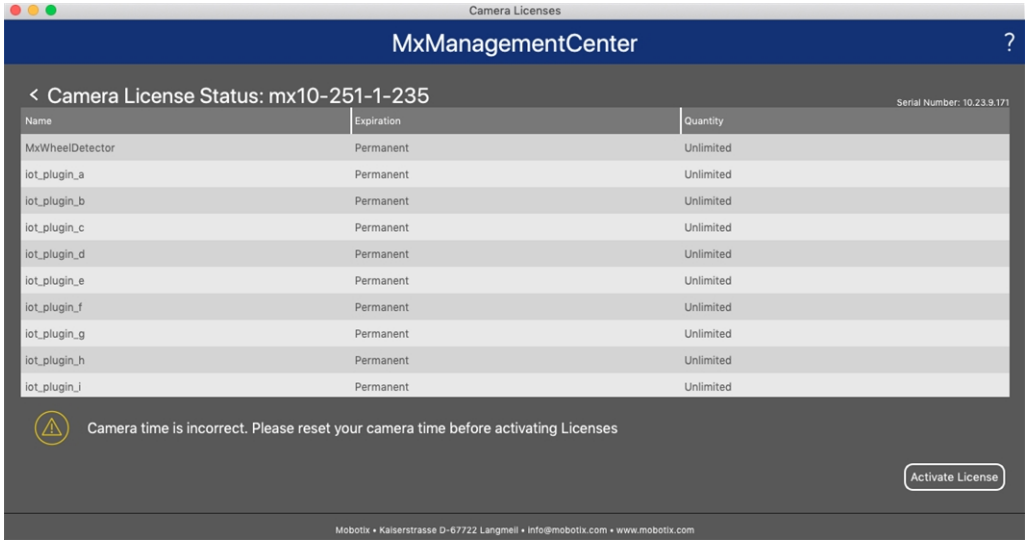


Fig. 6: Overview of the licenses installed on the camera

NOTE! If necessary, correct the time set on the camera.

4. Enter a valid Activation ID and specify the number of licenses to install on this computer.
5. If you want to license another product, click on . In the new row, enter the appropriate **Activation ID** and the number of licenses you want.

6. If necessary, click | to remove a line.
7. When you have entered all Activation IDs, click **Download Capability Request File (.lic)**. and send it to your partner/installer.

NOTE! This file allows the partner / installer from whom you purchased the licenses to generate a capability response file (.bin) on the license server.

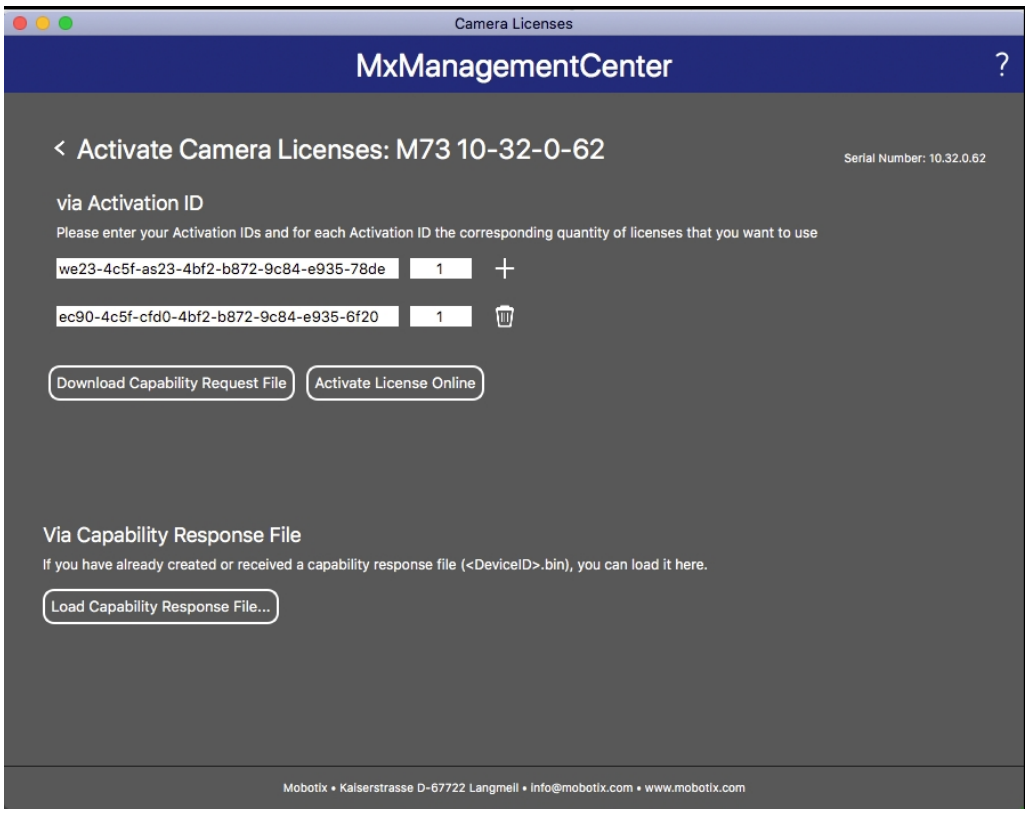


Fig. 7: Adding licenses

8. Click Load Capability Response File and follow the instructions.

Successful activation

After successful activation, a new log in is required to apply the changes. Alternatively, you can return to license management.

Managing Licenses in MxManagementCenter

In MxManagementCenter you can comfortably manage all licenses that have been activated for a camera.

1. Select from the menu **Window > Camera App Licenses**.
2. Select the camera on which you want to license apps and click **Select**.

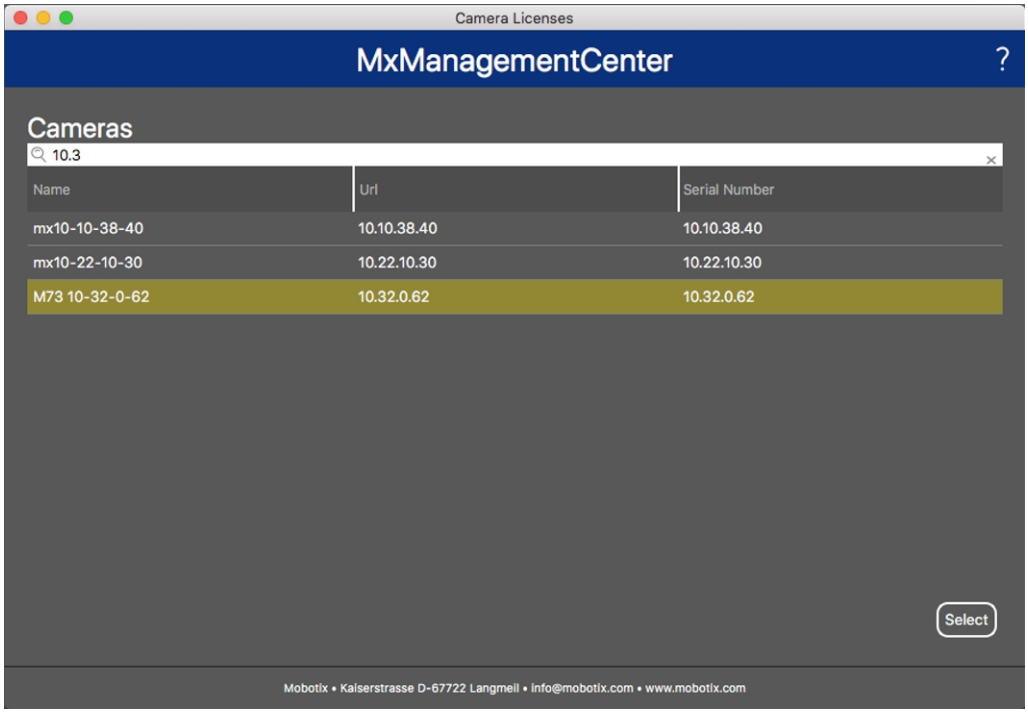


Fig. 8: Overview of Camera App Licenses in MxManagementCenter

An overview of the licenses installed on the camera may be displayed.

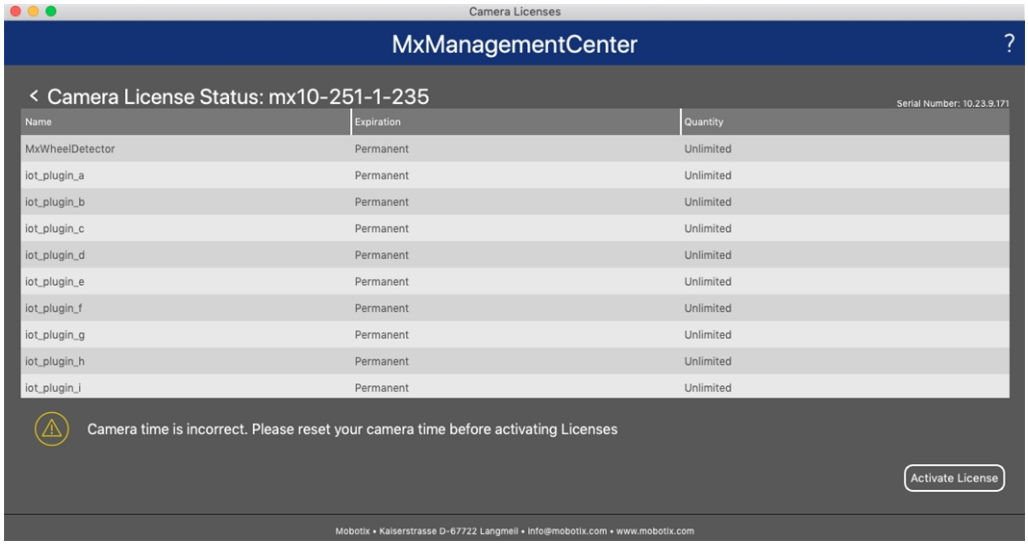


Fig. 9: Overview of the licenses installed on the camera

NOTE! If necessary, correct the time set on the camera.

Column	Explanation
Name	Name of the licensed app
Expiration	the time limit of the license
Quantity	Number of licenses purchased for a product.
Serial Number	Unique identification determined by MxMC for the device used. If problems occur during licensing, please have the device ID ready.

Synchronize licenses with server

When the program starts, there is no automatic comparison of the licenses between the computer and the license server. Therefore, click **Update** to reload the licenses from the server.

Update licenses

To update temporary licenses, click **Activate Licenses**. The dialog for updating/activating licenses opens.

NOTE! You need administrator rights to synchronize and update licenses.

Camera, image and scene requirements

The camera should be setup so that the combination of the distance, the lens's focal length and the camera's resolution provide an image that can be accurately analyzed. Therefore the following prerequisites must be fulfilled for the scene:

Highest possible mounting positions for best results

When planning your video surveillance system, prefer the highest possible camera positions in order to cover as much area as possible with each camera. Consider an installation height of at least 5 meters. An installation height of 10-25 meters usually leads to significantly better results.

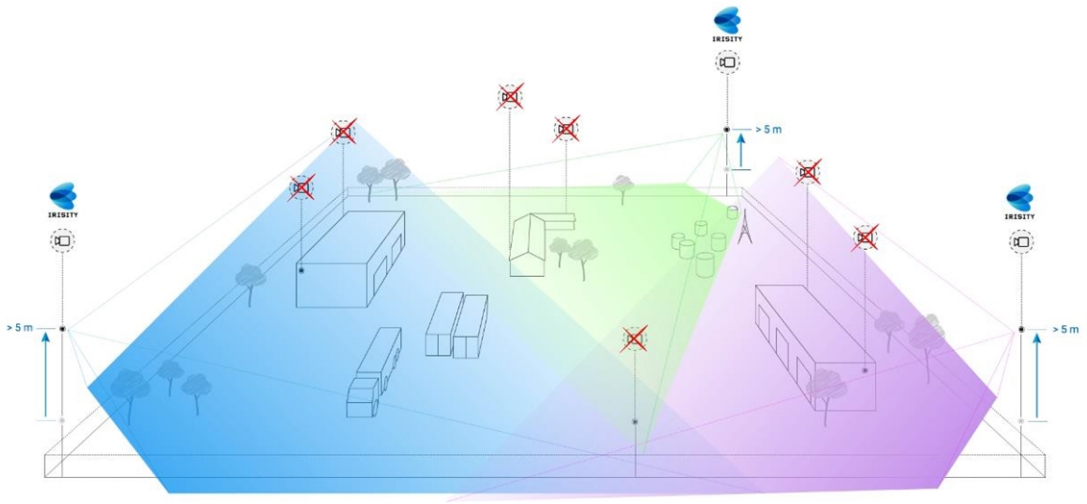


Fig. 10: Using high mounting positions can reduce the number of cameras in a classic CCTV installation.

Scene illumination

With optimal light sources (we recommend at least two light sources) can significantly improve the quality of video analysis and thus the security of your site.

- Illuminate the monitored area sufficiently.
- Ensure good contrast in the surveillance area.
- Do not over-light objects near the cameras to avoid blending and noise.

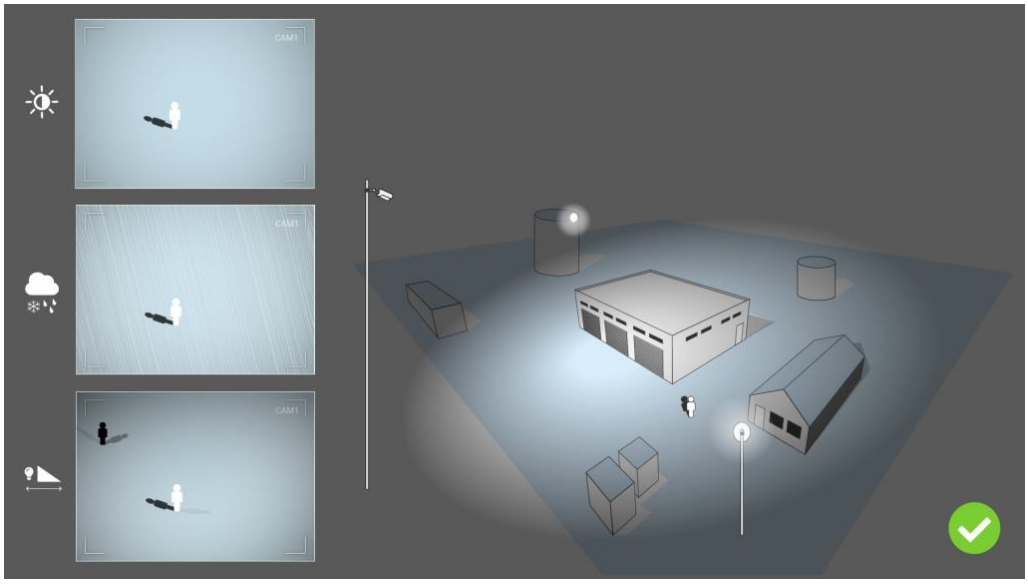


Fig. 11: Off-axis lighting improves visibility, contrast, and object detection significantly. It makes accurate detections possible in even the most challenging weather conditions.

Troubleshooting

Light design issues

By placing the light source near the camera and too far away from the guarded object, the emitted light may compromise surveillance by creating video issues. Possible issues are:

- Contrast in the video image may be too low (without shadows)
- Light source may create noise in picture by accentuating raindrops and snowflakes
- Light intensity may not be sufficient to light up the guarded object

While the camera's built-in lighting, or other on-axis lighting, is often convenient it often reduces the efficiency of the surveillance system. In challenging weather intruders might become almost invisible, hidden behind rain, snow or fog

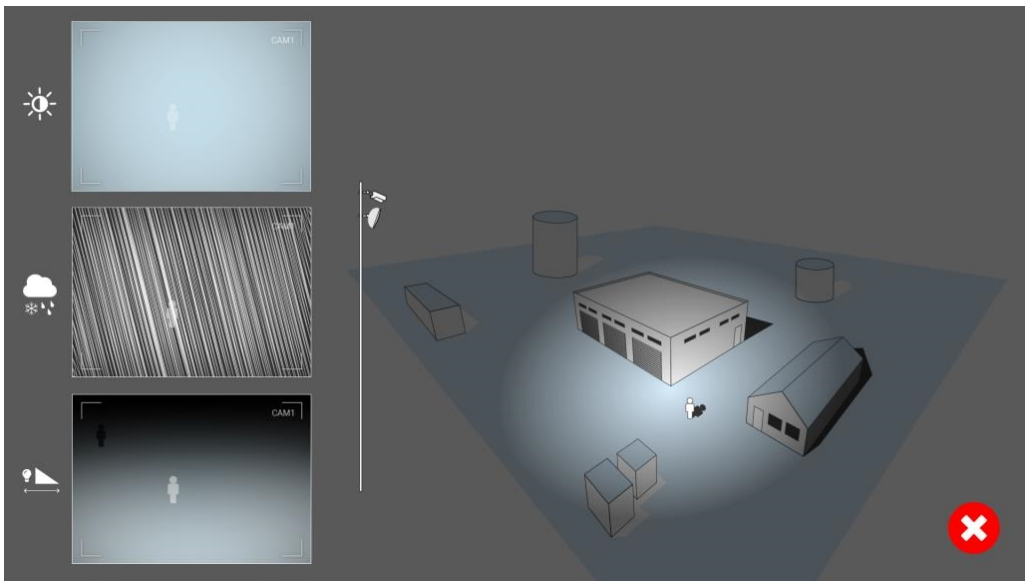


Fig. 12: In challenging weather intruders might become almost invisible, hidden behind rain, snow or fog

Activation of the Certified App Interface

CAUTION! The Irisity IRIS AI Analytics - Intrusion Detection does not consider obscure areas defined for the live image. Therefore there is no pixelation in obscure areas while configuring the app and during image analysis by the app.

NOTE! The user must have access to the setup menu (http(s)://<Camera IP address>/control). Therefore check the user rights of the camera.

1. In the camera web interface, open: **Setup Menu / Certified App Settings** (http(s)://<Camera IP address>/control/app_config).

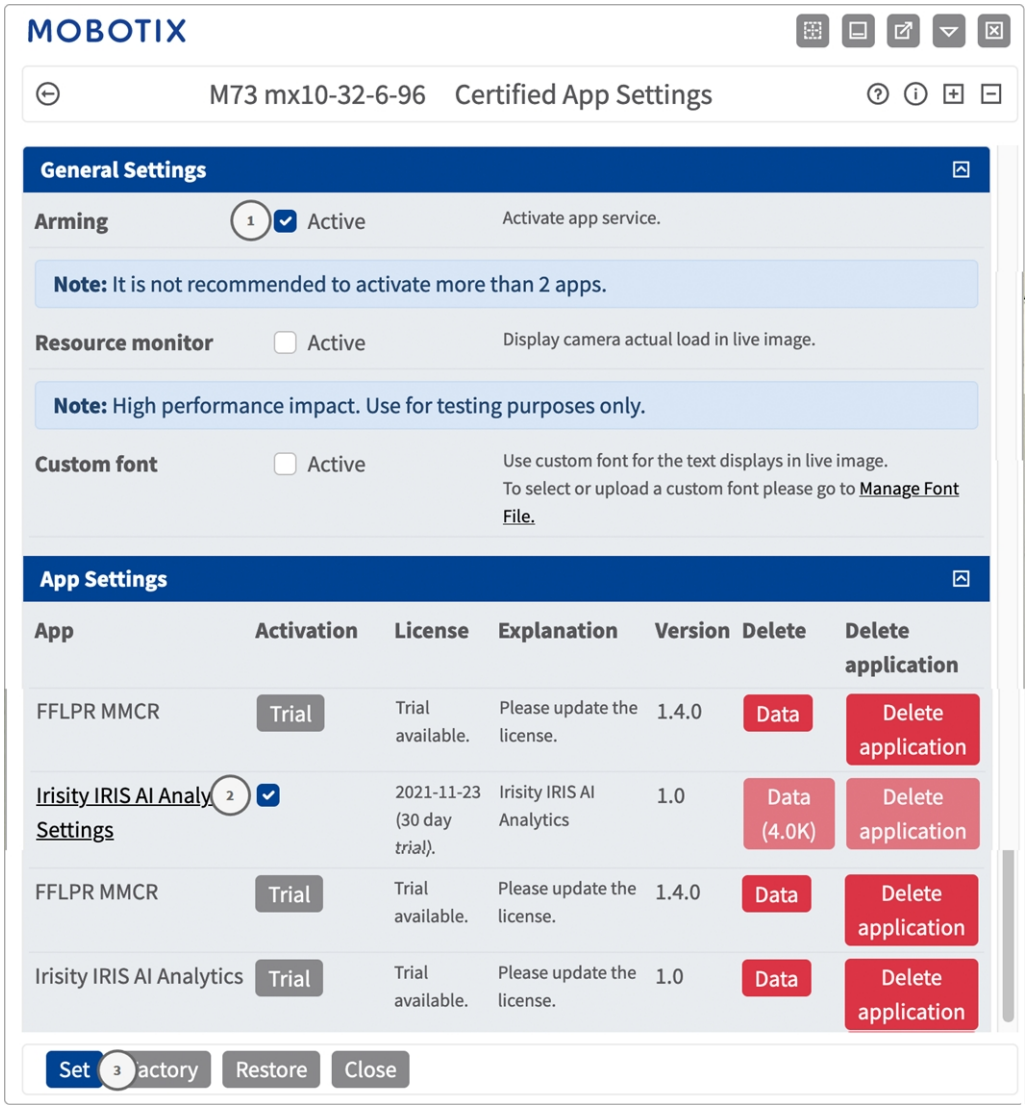


Fig. 13: Certified App: Settings

2. Under **General Settings** activate the **Arming** of the MOBOTIX app service ① .
3. Click Set ③ . The installed apps are now listed.
4. Under **App Settings** check the **Active** option of the of the relevant app.
5. Click on the name of the App ② to be configured to open the Apps user interface.
6. For configuration of the App see Configuration of Irisity IRIS AI Analytics - Intrusion Detection, p. 22

Configuration of Irisity IRIS AI Analytics - Intrusion Detection

CAUTION! The user must have access to the setup menu (http(s)://<Camera IP address>/control). Therefore check the user rights of the camera.

1. In the camera web interface, open: **Setup Menu / Certified App Settings** (http(s)://<Camera IP address>/control/app_config).
2. Click on the name of the **Irisity IRIS AI Analytics - Intrusion Detection**.

The configuration window of the app appears with the following options:

IRIS Intrusion detection

The following configurations should be taken into account:

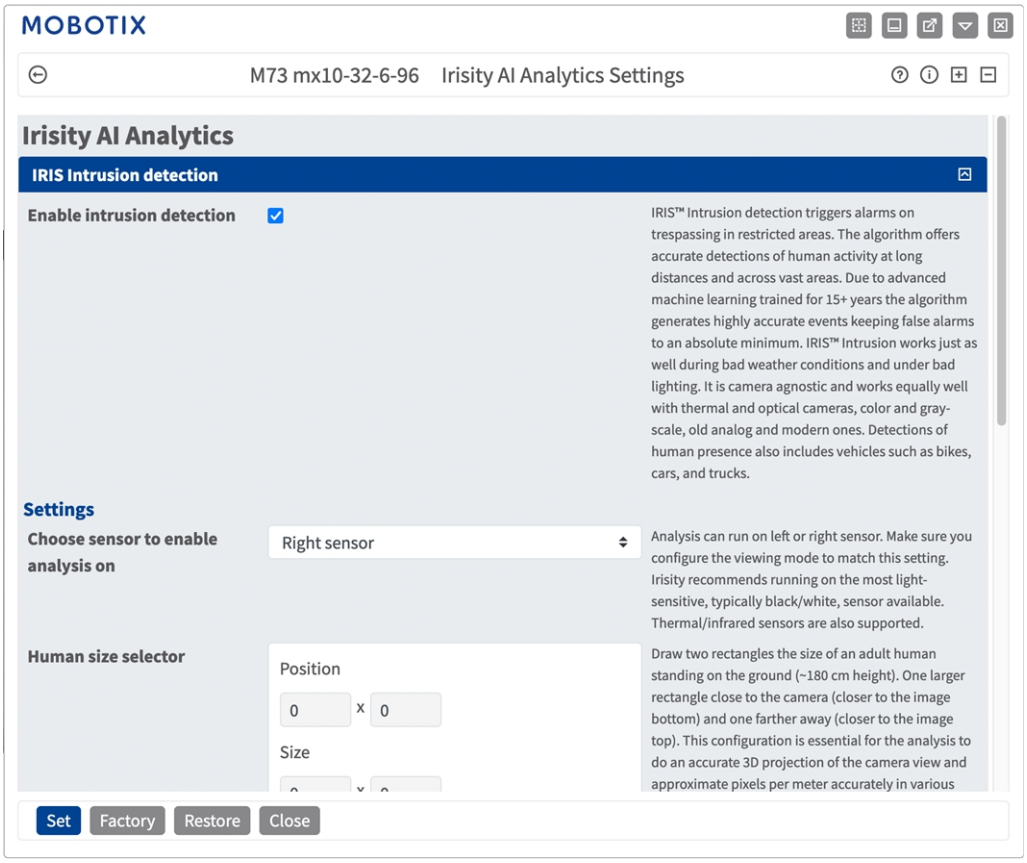


Fig. 14: Default operating mode: IRIS Intrusion detection

Enable intrusion detection: Check to activate the algorithm

Settings

- **Choose sensor to enable analysis on:** Select the sensor to be used for image analysis.
- **Human size selector:** 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 (see IRIS Tampering Detection, p. 23).
- **Alarm zones:** At least one alarm zone (detection area) needs to be defined in the live image (see Alarm Zones, p. 24).
- **Detect Object Type:** Select a filter to only trigger on humans or vehicles. Detections by default include all human-propelled motion such as pedestrians, bikes, cars and trucks.

Advanced Settings

- **Alarm zone cooldown:** Number of seconds an alarm zone will be deactivated after an alarm has been triggered.
- **Event cooldown:** Number of seconds an alarm will disable further detections from the same alarming object, including nearby objects.
- **Sensitivity:** Level of sensitivity for objects to be classified as human activity. Medium is recommended in most cases.

IRIS Tampering Detection

Here you can configure the tampering detection features .

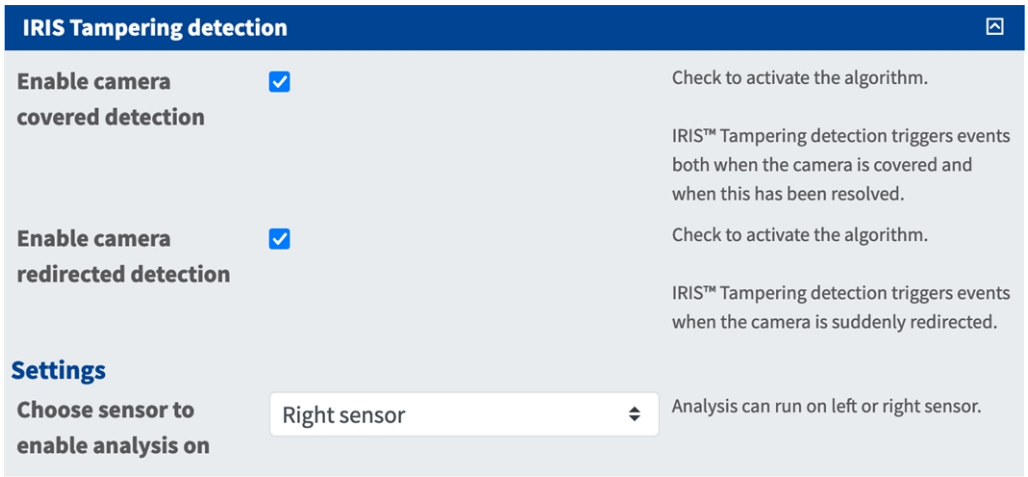


Fig. 15: IRIS Tampering Detection

Enable camera covered detection: Check to activate the algorithm.

NOTE! IRIS™ Tampering detection triggers events both when the camera is covered and when this has been resolved.

Enable camera redirected detection: Enable camera redirected detection.

NOTE! IRIS™ Tampering detection triggers events when the camera is suddenly redirected.

Choose sensor to enable analysis on: Select the sensor on which the analytics should run.

Drawing a Human Size Selector

1. In the live view simply click and drag a rectangular recognition area.
2. Drag the corner points to refine the recognition area.
3. In the top right corner of the live view click **Submit** to adopt the coordinates of the rectangle.

Alarm Zones

You can optionally set one or more Alarm Zones (detection areas). If left blank the entire image will be used for detections.

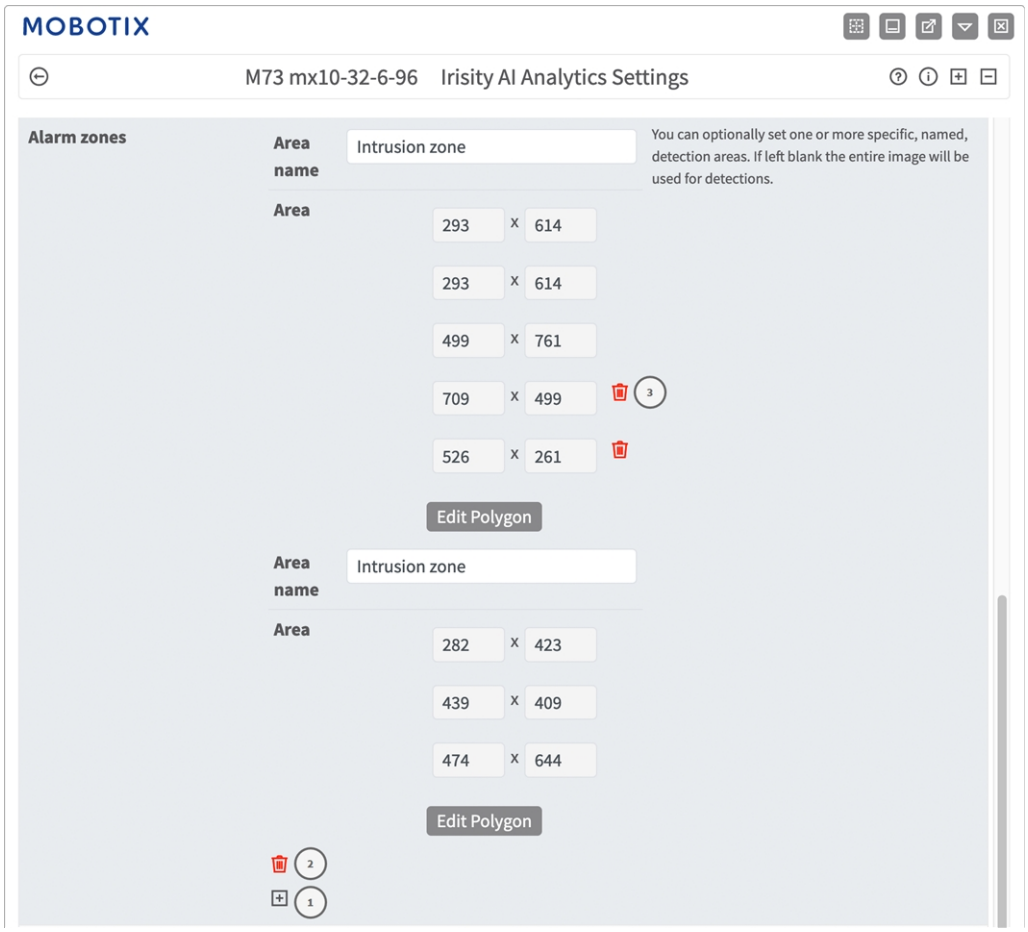


Fig. 16: Alarm Zones

Area Name Enter an unique name to identify the Alarm Zone

Area: The defined corner points of the Alarm Zone. Click **Edit Polygon** ① to draw the Detection Area in the Live View (see Drawing a Polygon Area in the Live View, p. 25

Add an Alarm Zone: Click the **plus** icon ② to define a new Alarm Zone.

Delete an Area: Click the **bin** icon ② to delete the recognition area.

Visual Overlays

Here you can select objects and data of IRIS Intrusion Detection to be displayed in the live image.

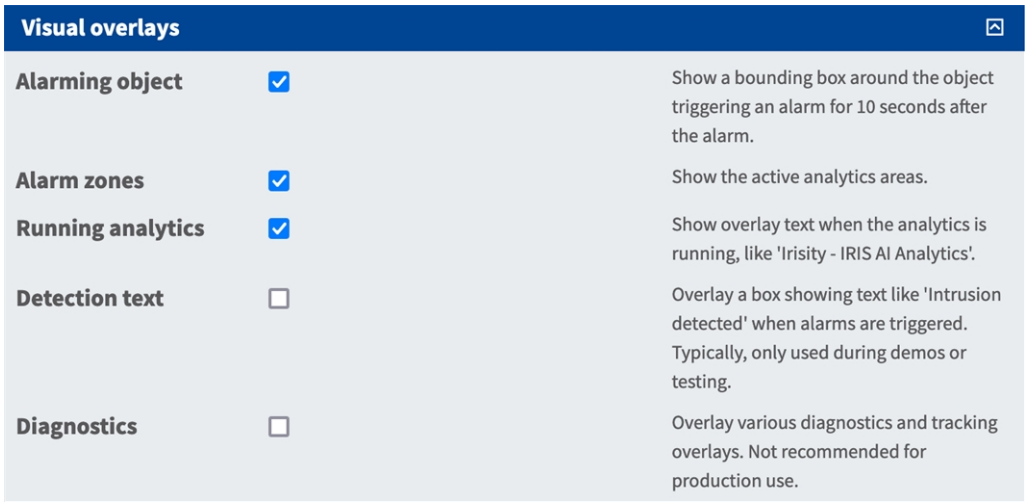


Fig. 17: Visual Overlays

Alarming object: Check to show a bounding box around the object triggering an alarm for 5 seconds after the alarm.

Alarm zones: Check to show the active analytics areas.

Running analytics: Check to overlay text of the analytics configured and running, e. g. "Irisity - IRIS Intrusion detection".

Detection text when alarm is triggered: Overlay a box showing text like 'Intrusion detected' when alarms are triggered.

Diagnostics: Check to overlay various diagnostics and tracking overlays e. g. for debugging.

Drawing a Polygon Area in the Live View

In Live View, there you can draw areas based on polygons depending on the App. These areas are e.g. Detection Areas, Excluded Areas, Reference Areas etc.

1. In the Live View simply click and drag a rectangular area.
2. Drag the corner points to the desired position.
3. To add another corner point, drag a smaller point between two corner points on the contour of the area.

4. In the top right corner of the live view click **Submit** to adopt the coordinates of the polygon.
5. Optionally click the **bin** icon to delete the recognition area.

Visual Overlays

Here you can select objects and data of IRIS Intrusion Detection to be displayed in the live image.

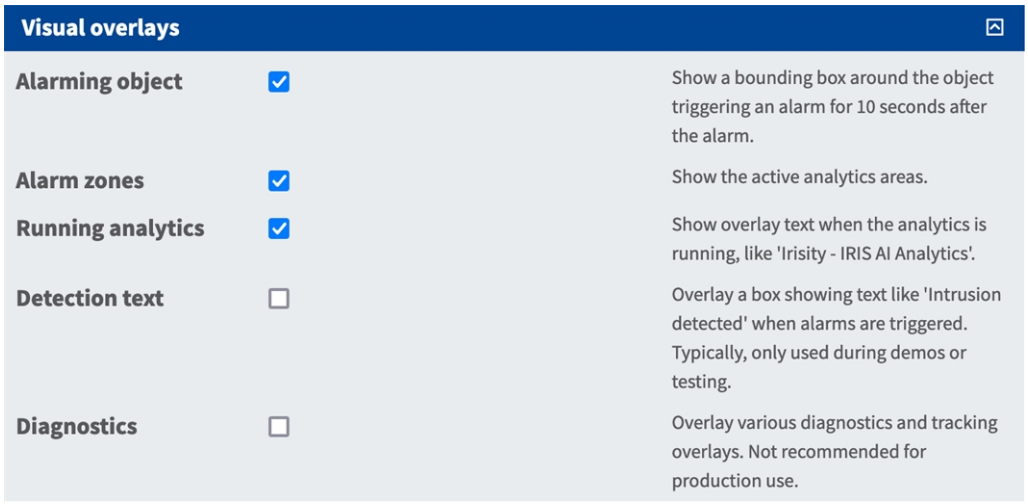


Fig. 18: Visual Overlays

Alarming object: Check to show a bounding box around the object triggering an alarm for 5 seconds after the alarm.

Alarm zones: Check to show the active analytics areas.

Running analytics: Check to overlay text of the analytics configured and running, e. g. "Irisity - IRIS Intrusion detection".

Detection text: Overlay a box showing text like 'Intrusion detected' when alarms are triggered.

Diagnostics: Check to overlay various diagnostics and tracking overlays e. g. for debugging.

Storing the Configuration

To store the configuration you have the following options:

Fig. 19: Storing the configuration

- Click on the **Set** button to activate your settings and to save them until the next reboot of the camera.
- Click on the **Factory** button to load the factory defaults for this dialog (this button may not be present in all dialogs).
- Click on the **Restore** button to undo your most recent changes that have not been stored in the camera permanently.
- Click on the **Close** button to close the dialog. While closing the dialog, the system checks the entire configuration for changes. If changes are detected, you will be asked if you would like to store the entire configuration permanently.

After successfully saving the configuration, the event and meta data are automatically sent to the camera in case of an event.

MxMessageSystem

What is MxMessageSystem?

MxMessageSystem is a communication system based on name oriented messages. This means that a message must have a unique name with a maximum length of 32 bytes.

Each participant can send and receive messages. MOBOTIX cameras can also forward messages within the local network. This way, MxMessages can be distributed over the entire local network (see Message Area: Global).

For example, a MOBOTIX 7 series camera can exchange a MxMessage generated by a camera app with an Mx6 camera that does not support certified MOBOTIX apps.

Facts about MxMessages

- 128-bit encryption ensures privacy and security of message content.
- MxMessages can be distributed from any camera of the Mx6 and 7 series.
- The message range can be defined individually for each MxMessage.
  - **Local:** Camera expects a MxMessage within its own camera system (e.g. through a Certified App).
  - **Global:** the camera expects a MxMessage that is distributed in the local network by another MxMessage device (e.g. another camera of the 7 series equipped with a certified MOBOTIX app).
- Actions that the recipients are to perform are configured individually for each participant of the MxMessageSystem.

MxMessageSystem: Processing the automatically generated app events

Checking automatically generated app events

NOTE! After successfully activating the app (see Activation of the Certified App Interface, p. 20), a generic message event for this specific app is automatically generated in the camera.

1. Go to **Setup-Menu / Event Control / Event Overview**. In section **Message Events** the automatically generated message event profile is named after the application (e. g. IRIS).

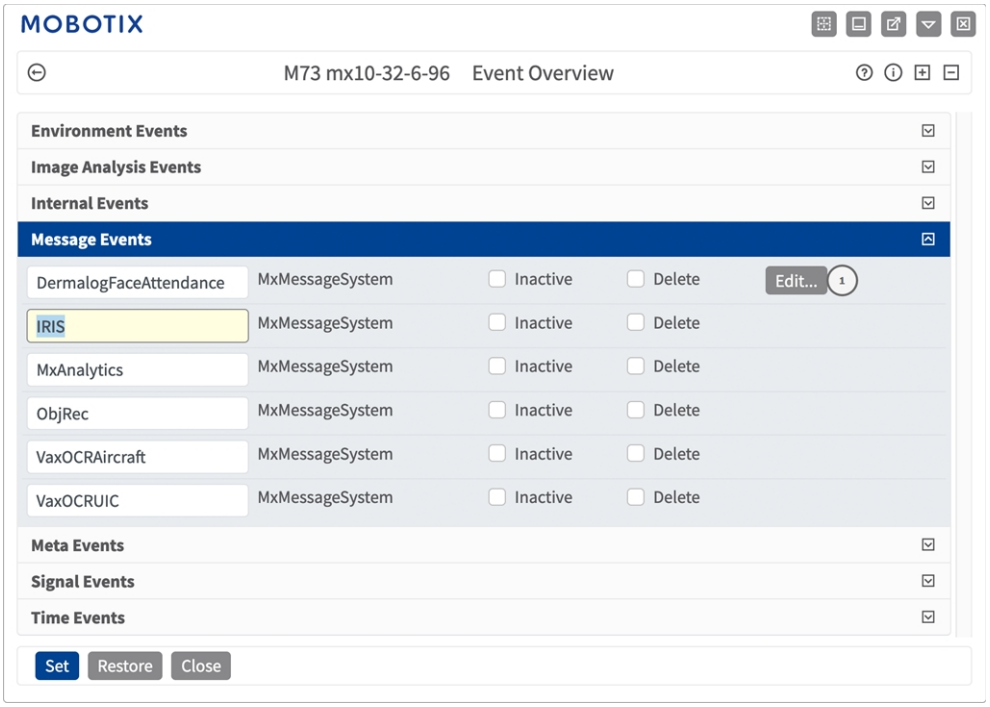


Fig. 20: Example: Generic message event from Irisity IRIS AI Analytics - Intrusion Detection

2. Click **Edit**① to display a selection of all configured message events.

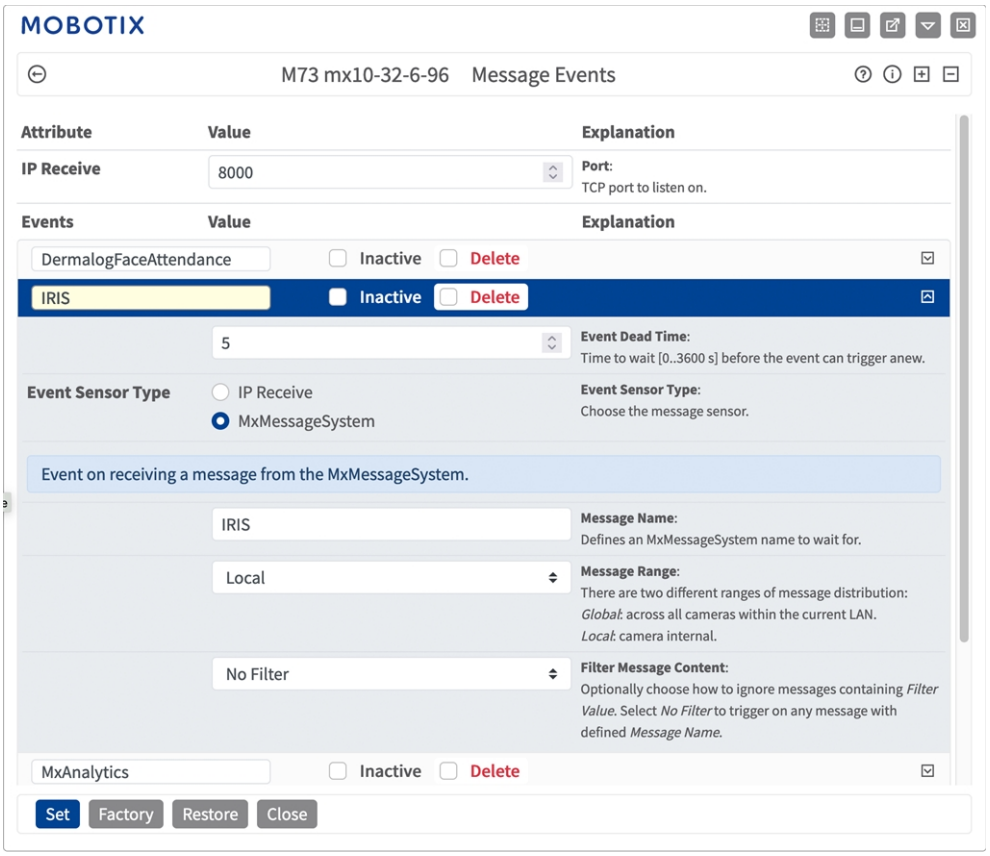


Fig. 21: Example: Generic message event details - no filter

Action handling - Configuration of an action group

CAUTION! To use events, trigger action groups or record images the general arming of the camera must be enabled (http(s)/<Camera IP address>/control/settings)

An action group defines which action(s) is (are) triggered by the Irisity IRIS AI Analytics - Intrusion Detection event.

1. In the camera web interface, open: **Setup Menu / Action Group Overview** (http(s)://<Camera IP address>/control/actions).

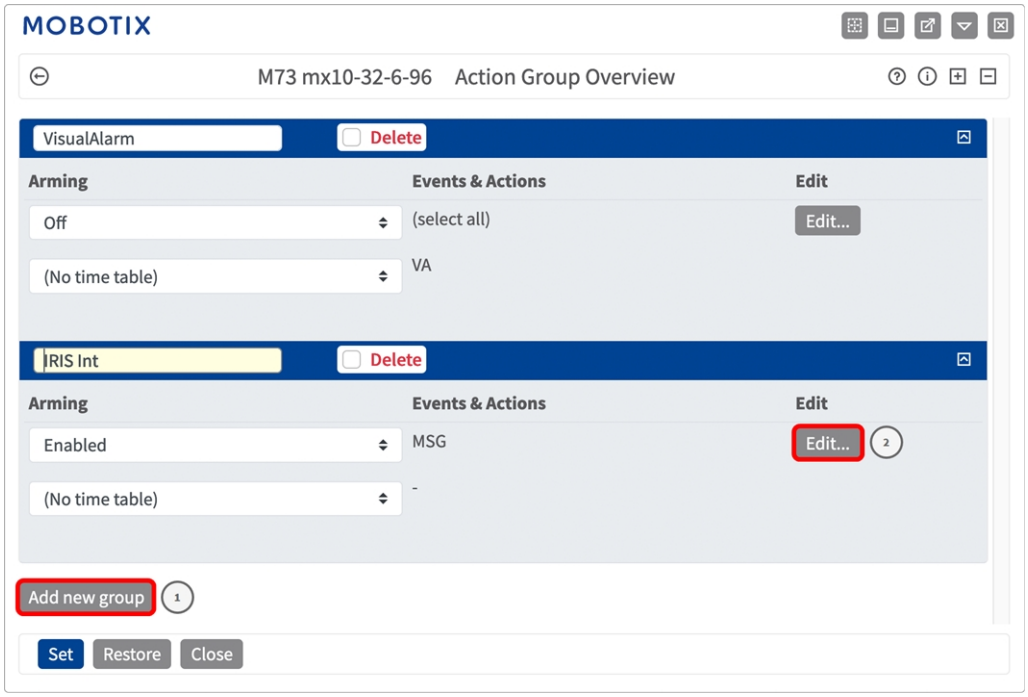


Fig. 22: Defining Action Groups

2. Click **Add new group**① and give a meaningful name.
3. Click **Edit**② , to configure the group.

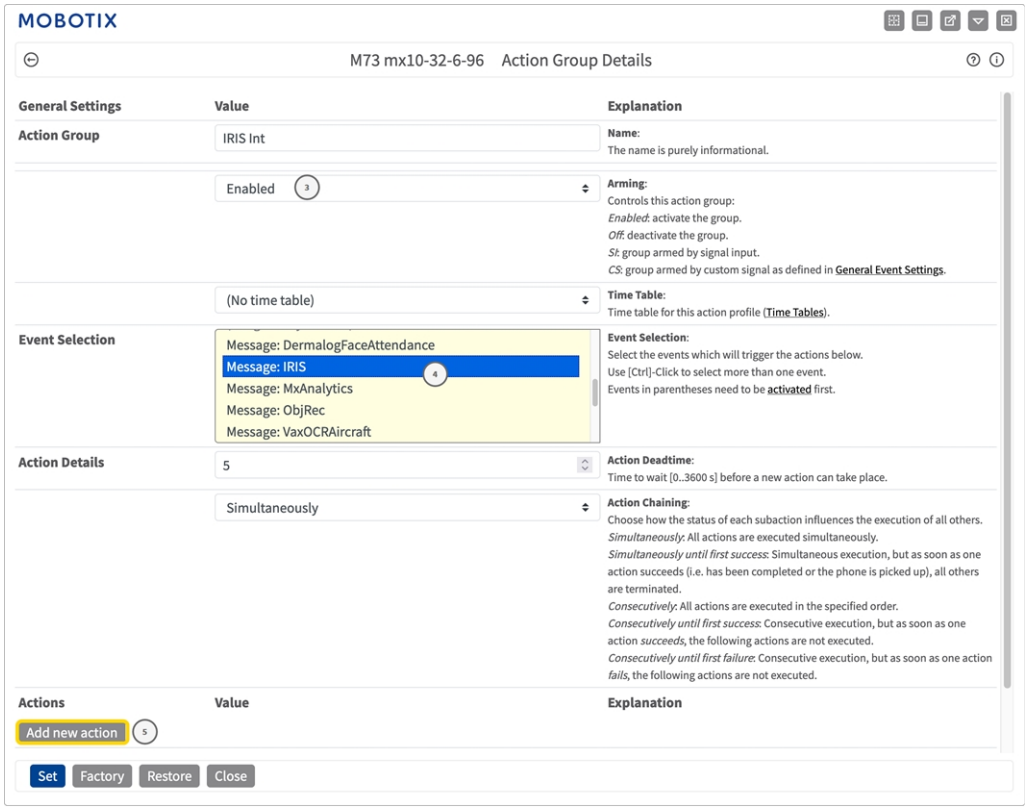


Fig. 23: Configuring an Action Group

4. Enable **Arming**③ of the Action Group.
5. Select your message event in the **Event selection** list ④ . To select multiple events, hold the shift key.
6. Click **Add new Action**⑤ .
7. Select a proper action from list **Action Type and Profile**⑥ .

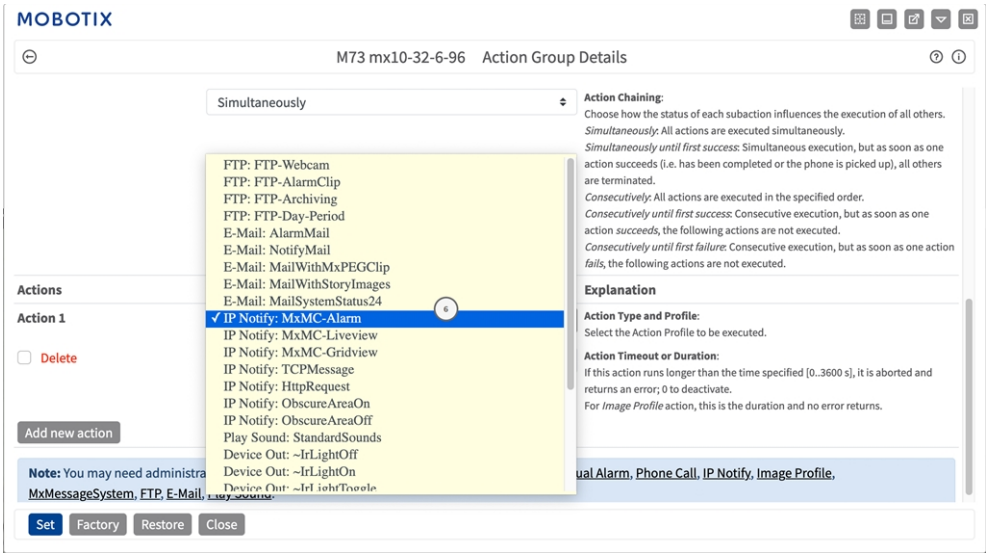


Fig. 24: Select Action Type- and Profile

NOTE! If the required action profile is not yet available, you can create a new profile in the Admin Menu sections "MxMessageSystem", "Transfer Profiles" and "Audio and VoIP Telephony".

If necessary, you can+ add further actions by clicking the button again. In this case, please make sure that the "action chaining" is configured correctly (e.g. at the same time).

8. Click on the **Set** button at the end of the dialog box to confirm the settings.

Action settings - Configuration of the camera recordings

1. In the camera web interface, open: **Setup Menu / Event Control / Recording**(http(s)/<Camera IP address>/control/recording).

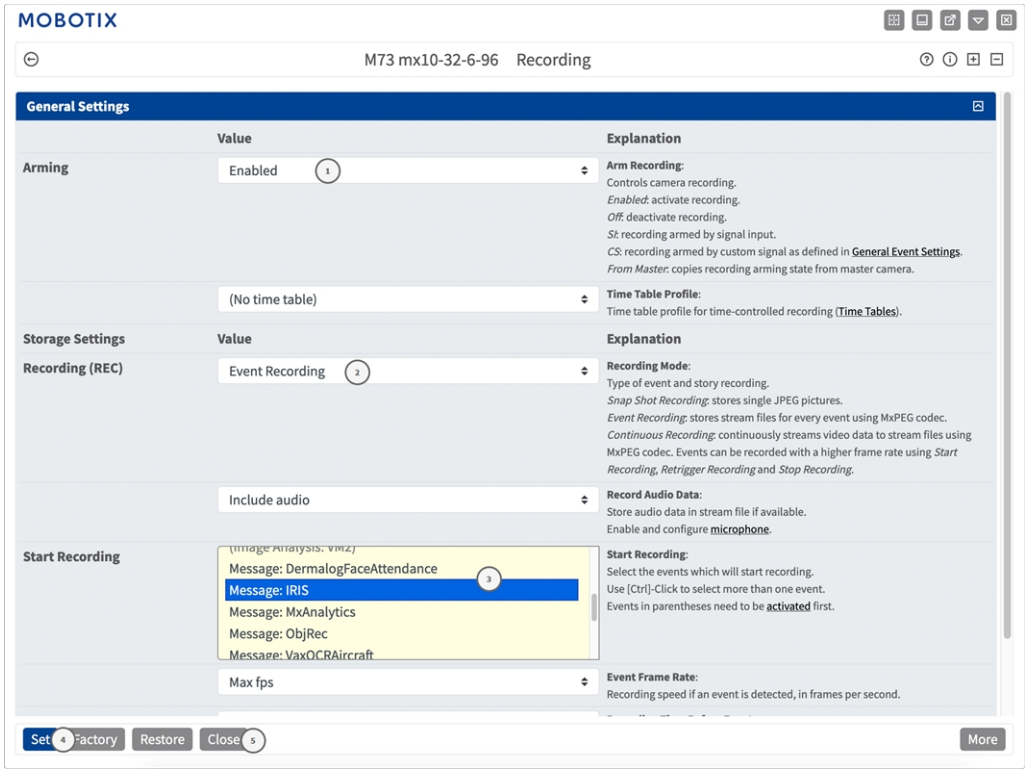


Fig. 25: Configuration of camera recording settings

2. Activate **Arm Recording** ① .
3. Under **Storage Settings** / **Recording (REC)** select a **Recording mode** ② . The following modes are available:
   - Snap Shot Recording
   - Event Recording
   - Continuous Recording
4. In list **Start recording** ③ select the message event just created.
5. Click on the **Set** ④ button at the end of the dialog box to confirm the settings.
6. Click on **Close** ⑤ to save your settings permanently.

NOTE! Alternatively, you can save your settings in the Admin menu under Configuration / Save current configuration to permanent memory.

MxMessageSystem: Processing the meta data transmitted by apps

Meta data transferred within the MxMessageSystem

For each event, the app also transfers meta data to the camera. This data is sent in the form of a JSON schema within a MxMessage.

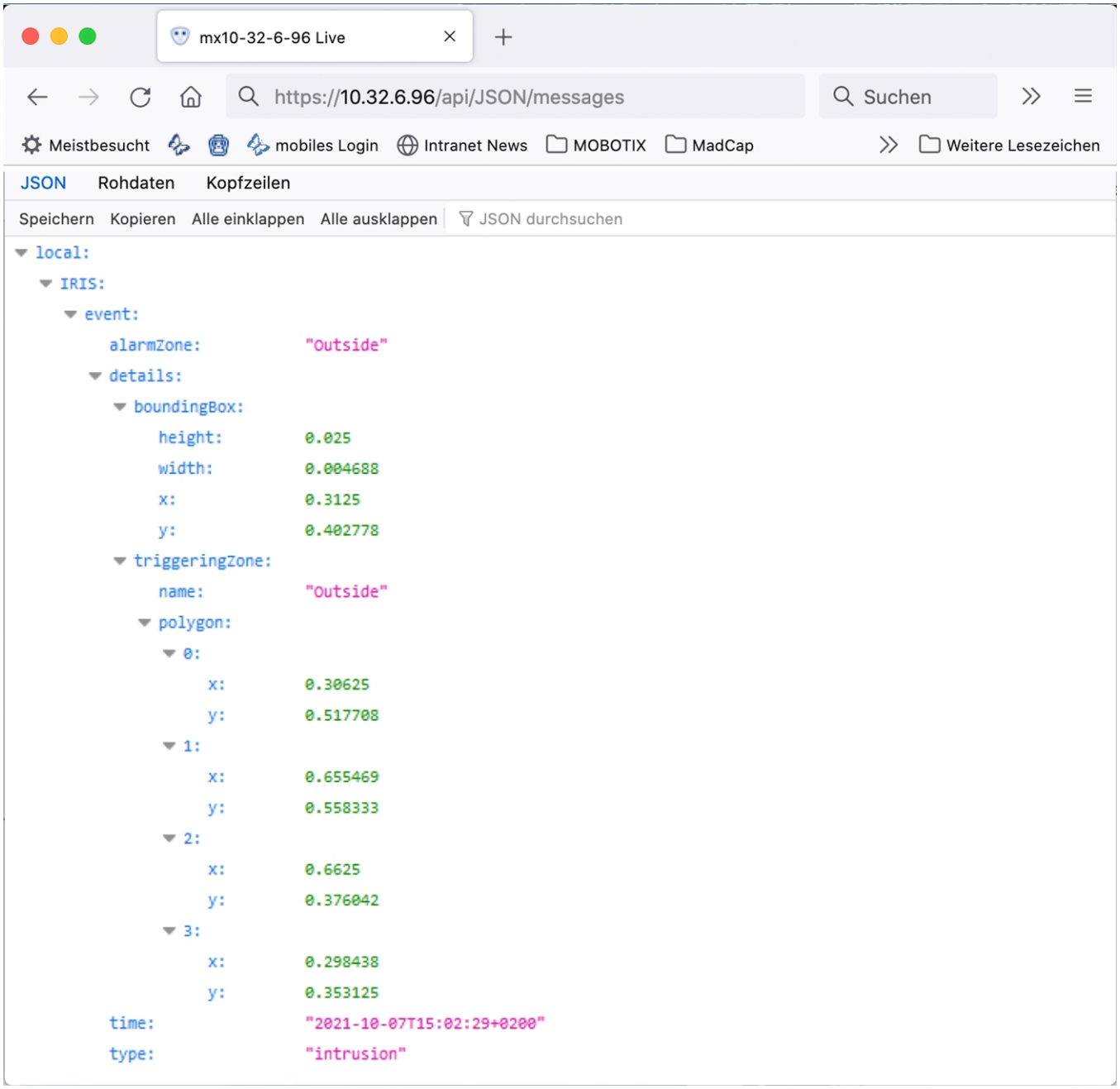


Fig. 26: Example: Meta data transmitted within a MxMessage of the Irisity IRIS AI Analytics - Intrusion Detection

NOTE! To view the meta data structure of the last App event, enter the following URL in the address bar of your browser: http(s)/IPAddresseOfYourCamera/api/json/messages

Creating a Custom Message Event

1. Go to **Setup-Menu / Event Control / Event Overview**. In section **Message Events** the automatically generated message event profile is named after the application (e. g. IRIS).

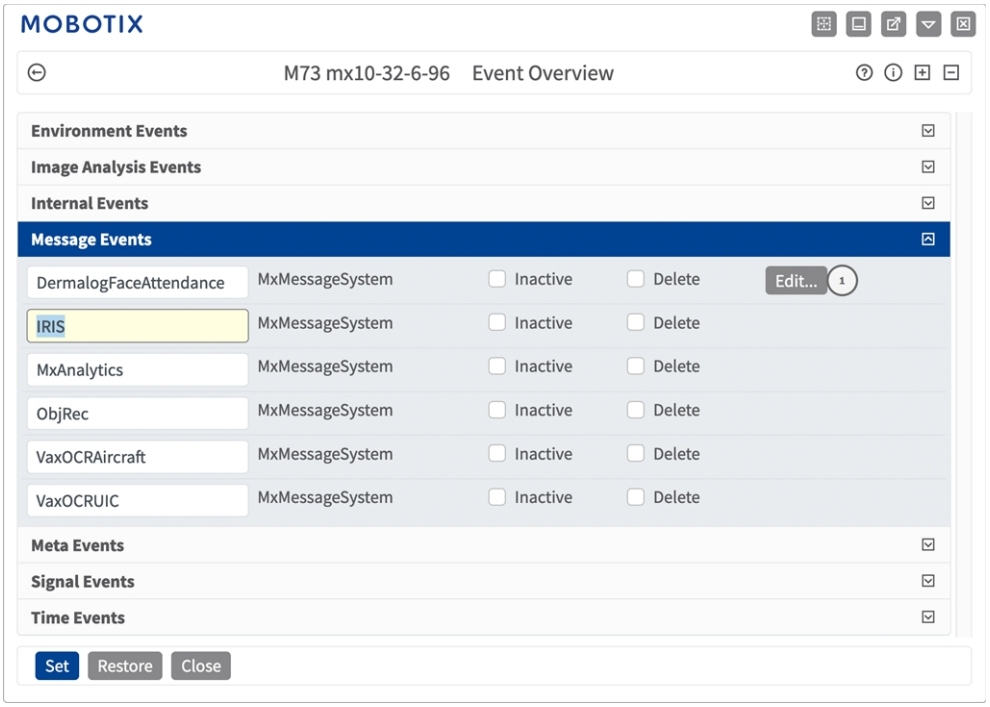


Fig. 27: Example: Generic message event from Irisity IRIS AI Analytics - Intrusion Detection

2. Click **Edit**① to display a selection of all configured message events.

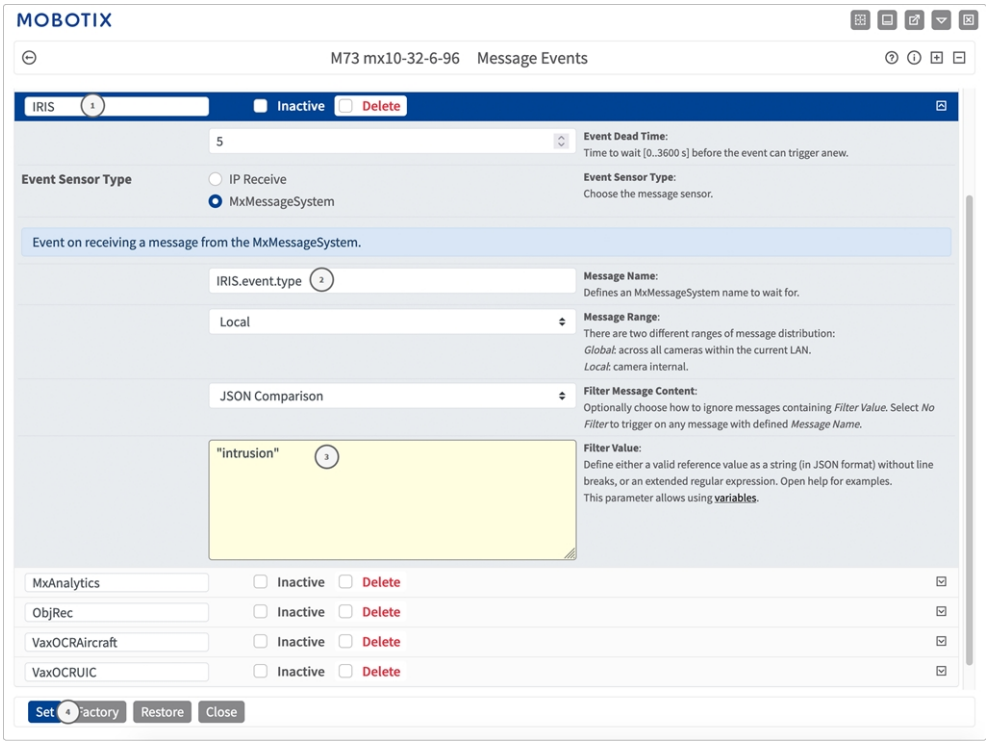


Fig. 28: Example: Intrusion message event

3. Click on the event (e. g. IRIS) ① to open the event settings.
4. Configure the parameters of the event profile as follows:

- **Message Name:** Enter the "Message Name" ② according to the event documentation of the corresponding app (see Examples for message names and filter values of the Irisity IRIS AI Analytics - Intrusion Detection, p. 38)
- **Message Range:**
  - **Local:** Default settings for the Irisity IRIS AI Analytics - Intrusion Detection
  - **Global:** (MxMessage is forwarded from another MOBOTIX camera in the local network.
- **Filter Message Content:**
  - **Generic Event:** “No Filter”
  - **Filtered Event:** “JSON Comparison”
- **Filter Value:** ③ see Examples for message names and filter values of the Irisity IRIS AI Analytics - Intrusion Detection, p. 38.

CAUTION! “Filter Value“ is used to differentiate the MxMessages of an app / bundle. Use this entry to benefit from individual event types of the apps (if available).

Choose “No Filter” if you want to use all incoming MxMessages as generic event of the related app.

2. Click on **Set**④ at the end of the dialog box to confirm the settings.

Examples for message names and filter values of the Irisity IRIS AI Analytics - Intrusion Detection

IRIS Intrusion Detection	MxMessage Name	Filter Value
Generic Event	IRIS	
Alarm zone event	IRIS.event.alarmZone	Name of alarm zone, e. g.: “Intrusion Zone 2”
Event type	IRIS.event.type	"intrusion"

MOBOTIX

BeyondHumanVision

EN_01/23
MOBOTIX AG • Kaiserstrasse • D-67722 Langmeil • Tel.: +49 6302 9816-103 • sales@mobotix.com • www.mobotix.com