PRODUCT DOCUMENTATION

Version: 2.1.0

Source: docs.ultinous.com

Table of Contents

U-Alarm

Overview

version: 2.1.0 | Product Page

U-Alarm is an AI based actionable video intelligence software solution that runs on the Nvidia-based Edge platform. U-Alarm is designed to analyse any connected IP cameras and raise alarms based on the detections set, such as intrusion, unsafe amount of people, unauthorised access attempt, etc. The alarms can be managed on U-Alarm's user interface and/or sent to a third party dashboard, such as a Video Management System.

U-Alarm is supplied as a software only solution that supports multiple edge hardware devices.

Key features

- **Intrusion detection for fixed and PTZ cameras** including person and 5 vehicle classes
- **Multi Object Detection** including person and 8 vehicle classes
- **Multi Object Counting** including person and 8 vehicle classes
- **Crowd detection**
- **Milestone XProtect support**
- **Alarm notifications via e-mail**
- **Custom third-party software integration** for alarms and counters
- Genetec Security Center support (coming in 2022)

Release dates and change log.

Supported hardware models.

The General Terms and Conditions and the End User Licence Agreement of Ultinous.

This document shows you how to install, configure and use U-Alarm.

U-Alarm supports Milestone XProtect VMS integration. This step-by-step documentation will help you configure it to receive Alarms in Milestone XProtect triggered by U-Alarm.

U-Alarm allows you to send alarms via e-mail too. The service can be set up to be used either by human beings or automated systems.

This guide will also aid software developers who would like to interface U-Alarm Events to a custom third party component, like a Video Management System.

Troubleshooting

In case you encounter an error or have an enquiry about a particular segment of U-Alarm, consult one of the troubleshooting articles corresponding to your issue. If you have further questions, contact support@ultinous.com or create a ticket in our Support Center.

- Cameras
- Receiving Events
- Milestone XProtect Integration

U-Alarm release notes

Several additional utilities may be used in conjunction with U-Alarm. To find out which versions of them correspond to your U-Alarm, see the Additional Tools guide.

2.1.0

release date: 6th December 2021

Documentation of 2.1.0

Changes

- Thermal camera support for all use cases.
- New analytic models with improved accuracy.
- Adjustable detection size setting for custom scenes.
- Multi Object Counter improvements:
  - Binary Long range counting switch is replaced with adjustable detection size setting
  - More options are available in historical counter data export
- Integration improvements:
  - Camera snapshots for events are available via HTTP and e-mail. "End of event" notification is available via HTTP.
  - Multiple custom HTTP headers are now supported.
  - Custom detector sensitivity settings are available for each object type and use case.
- Detected object types are displayed in the video player.
- Unreachable cameras are now indicated via HTTP and SNMP (Monitoring).
- Grant SSH access with one click for remote support.
- Crowd Detection can be used with other use cases at the same time.
- PTZ / Thermal camera flag is now in the Cameras view.
- Minor usability improvements.

Compatibility

- Integration (HTTP): The metadata schema is extended with an end_of_event flag. Please read the corresponding documentation and update your event receiver service accordingly.
- Milestone XProtect Connector should be updated.

2.0.10

release date: 15th October 2021

Documentation of 2.0.10

Changes

- Startup time is increased after restart.

2.0.8

release date: 5th October 2021

Documentation of 2.0.8

Changes

- Increased the accuracy of Alarms and Counters.
- Counter API includes 'first' and 'min' values.
- Minor fixes and improvements in the user interface.

2.0.6

release date: 3rd September 2021

Documentation of 2.0.6

Changes

- Counter: Max/Average/Median calculation has been fixed.

2.0.4

release date: 26th August 2021

Documentation of 2.0.4

Changes

- Crowd detection range issue has been fixed.

2.0.2

release date: 18th August 2021

Documentation of 2.0.2

Changes

- Multi Object Counting maximum range has been increased by 60%.
- The most recent multi object counting has been visualised within the user interface.
- Historical counting data can be downloaded in .csv file.
- Multi Object Counting has been extended with *median* and *maximum* values.
- Bug fix: U-Alarm Network Discovery Tool did not recognize U-Alarm devices after changing device names.
- Minor bug fixes and improvements.

2.0.0

release date: 20th July 2021

Documentation of 2.0.0

Changes

- Vehicle detection added to Intrusion detection
- Person detection accuracy is further increased
- Person and vehicle amount counting
- Live and historical data access via API
- Simplified UI with improved layout
- HTTP status endpoint for monitoring

Compatibility

- Former alarm *Intrusion Detection (PTZ)* is merged to *Intrusion Detection*. PTZ camera support is now a parameter in this alarm.
- For Milestone XProtect integration, the U-Alarm / Milestone XProtect Connector should be updated.
- It is recommended to set all connected camera streams' framerate to 1 fps.
- Updating from a version older than 2.0.0 will **remove all existing events**!

1.2.2

release date: 31st May 2021

Documentation of 1.2.2

Changes

- U-Alarm can connect to a custom time synchronization server (NTP)
- RoI editor usability improvements
- U-Alarm software updater Service Pack 1

1.2.0

release date: 12th May 2021

Documentation of 1.2.0

Changes

- NVIDIA NX support: U-Alarm handles up to 10 cameras
- Software update (online & offline)
- Using RoI increases the detectors' performance
- Operators can receive alarm notifications via email
- Integration: alarm notification email attachment contains event metadata
- Test event sending option for integration via HTTP
- SSL support (HTTPS)
- Minor UX improvements
- Milestone XProtect integration documentation describes email notification settings.

1.1.0

release date: 29th March 2021

Documentation of 1.1.0

Changes

- Intrusion detection PTZ camera support
- Monitoring (SNMP)
- False alarm rate is further decreased
- Milestone XProtect connector: time offset setting
- Camera FPS can be set to a fraction number
- Minor improvements in user interface
- Camera thumbnail load issue has been solved
- U-Alarm Network discovery tool's crash issue has been solved

1.0.1

release date: 1st March 2021

Documentation of 1.0.1

Changes

- Added restart U-Alarm device from the User interface.
- Milestone XProtect connector has been upgraded to a Windows service (CGU-8800).
- CGU-8940: Timeout for camera connection issue is solved for Axis and Bosch cameras.
- CGU-8944: Licence handling issues have been solved.

- CGU-8864: Fixed the issue when the registration form did not appear after a factory reset.
- CGU-8886: Minor improvements in the video player and the user interface

1.0.0

release date: 10th February 2021

Documentation of 1.0.0

Key features

- Intrusion detection
- Crowd detection
- Milestone XProtect support
- Custom third-party software integration for alerting

Device Support

U-Alarm currently runs on Jetson TX2 and NX devices (U-Alarm boxes). Below you will find each tested model with their specifications.

Manufacturer	Model name (with specs link)	Generation	Extension
AAEON	BOXER-8253AI	NX	+ 500GB SSD
ADLINK	DLAP-201-JT2	TX2	+ 500GB SSD
ADLINK	DLAP-211-JNX*	NX	+500GB SSD

* Use the documentation provided for the DLAP-201-JT2 above.

IMPORTANT: In order to work with U-Alarm, all devices must have an 500 GB SSD storage which might be built-in or can be purchased separately.

Quick Start Guide

Follow these steps to have a working U-Alarm installation in roughly 5 minutes.

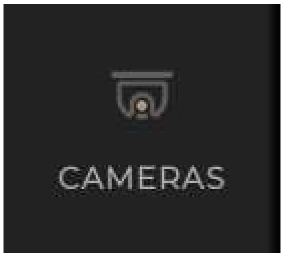
Before you start

Make sure that everything in the First Steps section is done.

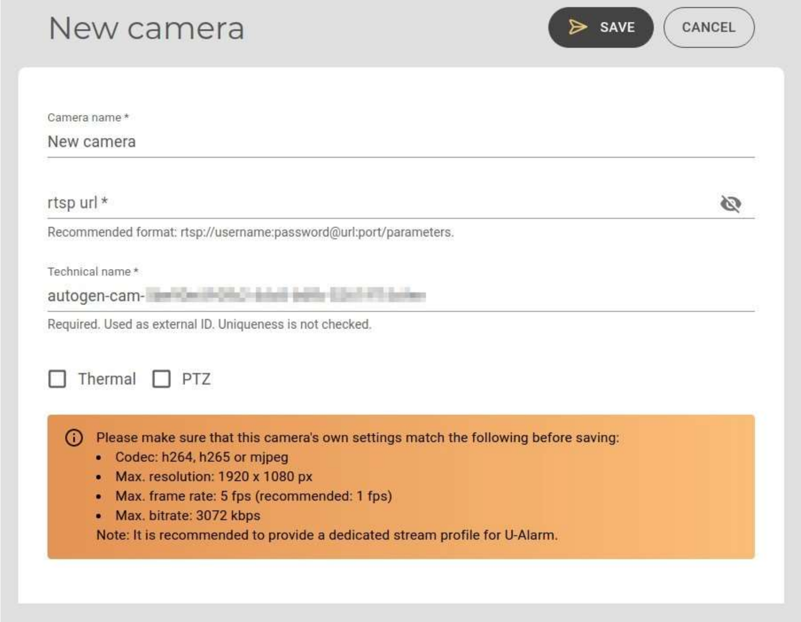
Step 1 - Add a camera

To do any video analysis we need a video stream. U-Alarm can read video streams via RTSP protocol. Follow these steps to add a new stream:

1. Click on the **Cameras** button in the left menu bar.



2. Click on the **New Camera** button.


New camera

SAVE CANCEL

Camera name *
New camera

rtsp url *
Recommended format: rtsp://username:password@url:port/parameters.

Technical name *
autogen-cam-[redacted]
Required. Used as external ID. Uniqueness is not checked.

□ Thermal □ PTZ

Please make sure that this camera's own settings match the following before saving:

- Codec: h264, h265 or mjpeg
- Max. resolution: 1920 x 1080 px
- Max. frame rate: 5 fps (recommended: 1 fps)
- Max. bitrate: 3072 kbps

Note: It is recommended to provide a dedicated stream profile for U-Alarm.

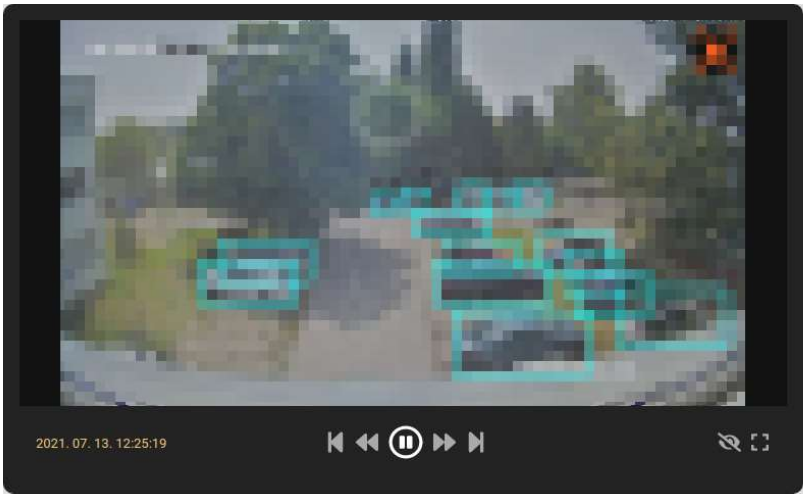
3. The **New camera** screen is where you need to enter basic information about the video stream. It is recommended to name the camera after the observed location (e.g.: Entrance). Make sure that the provided FPS, width and height information exactly matches the camera stream's (if not, set the appropriate values in your camera's own settings).

   Note: This version of U-Alarm supports up to 10 cameras with max. 1920 x 1080 resolution at 5 FPS on NX. TX2 is supported with up to 4 cameras.

4. Press **Save** when finished. If the new camera's name appears on the **Cameras** screen, you can proceed.

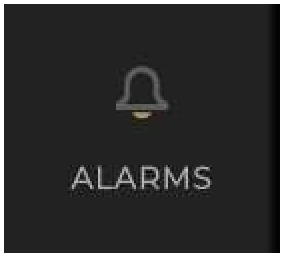
   The preview image will be loaded later automatically.

If the provided information was correct and U-Alarm can access the stream, you should see a live view like this:

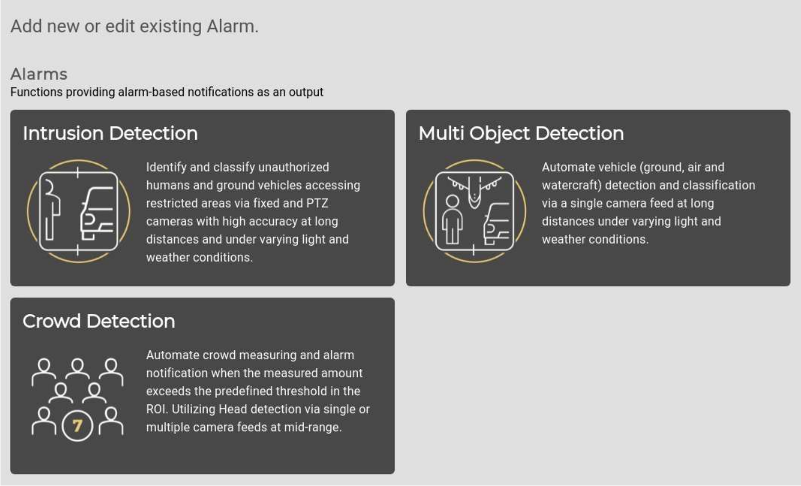


Step 2 - Configure an alarm

1. Click on **Alarms** on the left menu bar.



2. Click on the **New Alarm** button.



Add new or edit existing Alarm.

Alarms
Functions providing alarm-based notifications as an output

Intrusion Detection
Identify and classify unauthorized humans and ground vehicles accessing restricted areas via fixed and PTZ cameras with high accuracy at long distances and under varying light and weather conditions.

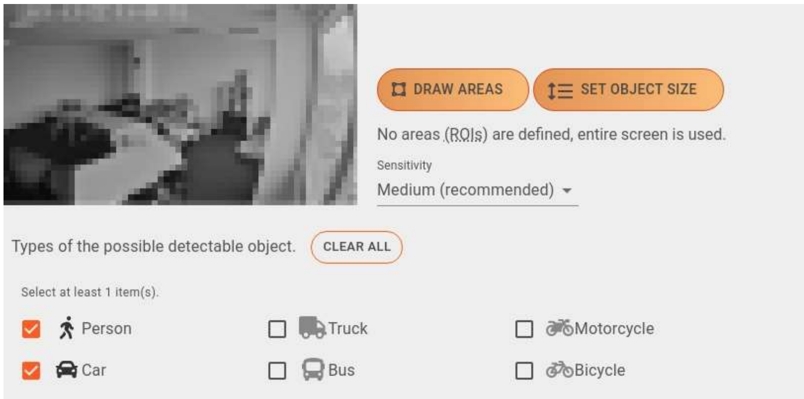
Multi Object Detection
Automate vehicle (ground, air and watercraft) detection and classification via a single camera feed at long distances under varying light and weather conditions.

Crowd Detection
Automate crowd measuring and alarm notification when the measured amount exceeds the predefined threshold in the ROI. Utilizing Head detection via single or multiple camera feeds at mid-range.

3. Click on the **Intrusion Detection** box.

4. Configure the Alarm. Set the **Name**.

5. Now select the previously registered camera. In this guide the entire video will be analysed.



No areas (ROIs) are defined, entire screen is used.

Sensitivity: Medium (recommended)

Types of the possible detectable object.

Select at least 1 item(s).

☑ Person □ Truck □ Motorcycle

☑ Car □ Bus □ Bicycle

6. Select any object type (at least one).
7. Leave all the other settings on their default value.
8. Click on the **Submit** button.

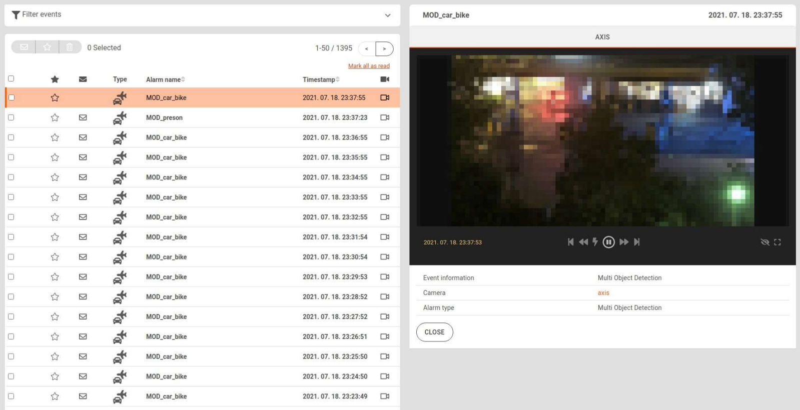
Step 3 - Handle events

At this moment, everything is set up and U-Alarm is operating. While U-Alarm is opened in your browser, you can see the following indications of a newly triggered Event:

- A *Bell icon* is displayed in the Live video player if the Cameras page is active.
- A red circle with an increasing number is displayed on the Events menu.
- A *notification bar* appears at the bottom of any page. The bar will not disappear until it is closed manually or the incident is investigated by clicking on the **More** link on it.
- A *Beeping sound* is played (unless the browser tab is muted).

  You can mute / unmute a browser tab by right-clicking on the tab and selecting the appropriate function.
- New *records* appear in the Events view.

By clicking on the **More** link on the notification or by clicking on the **Events** menu on the left side the corresponding page will appear. All events can be checked and replayed here one by one. Each camera's records can be replayed by selecting the camera at the top of the video player.



0 Selected

1-50 / 1395

□	★	✉	Type	Alarm name	Timestamp	
□	☆			MOD_car_bike	2021. 07. 18. 23:37:55	
□	☆	✉		MOD_preson	2021. 07. 18. 23:37:23	
□	☆	✉		MOD_car_bike	2021. 07. 18. 23:36:55	
□	☆	✉		MOD_car_bike	2021. 07. 18. 23:35:55	
□	☆	✉		MOD_car_bike	2021. 07. 18. 23:34:55	
□	☆	✉		MOD_car_bike	2021. 07. 18. 23:33:55	
□	☆	✉		MOD_car_bike	2021. 07. 18. 23:32:55	
□	☆	✉		MOD_car_bike	2021. 07. 18. 23:31:54	
□	☆	✉		MOD_car_bike	2021. 07. 18. 23:30:54	
□	☆	✉		MOD_car_bike	2021. 07. 18. 23:29:53	
□	☆	✉		MOD_car_bike	2021. 07. 18. 23:28:52	
□	☆	✉		MOD_car_bike	2021. 07. 18. 23:27:52	
□	☆	✉		MOD_car_bike	2021. 07. 18. 23:26:51	
□	☆	✉		MOD_car_bike	2021. 07. 18. 23:25:50	
□	☆	✉		MOD_car_bike	2021. 07. 18. 23:24:50	
□	☆	✉		MOD_car_bike	2021. 07. 18. 23:23:49	

MOD_car_bike 2021. 07. 18. 23:37:55

AXIS

2021. 07. 18. 23:37:53

Event information	Multi Object Detection
Camera	axis
Alarm type	Multi Object Detection

Further reading

All done. If you would like to learn more about U-Alarm please visit the User's guide.

U-Alarm User's Guide

For quickly checking U-Alarm's core features, see the quick start guide. Otherwise you can discover the full feature set by following these steps:

Take the **First steps** > Add **Cameras** > Set **Alarms** > Define a **Schedule** (optional) > Receive **Events**

Additional settings are available in the Control Panel.

This guide helps you setup your device in the fastest way possible (optional settings are skipped here).

Detailed installation guide for U-Alarm, hardware support, and software update process.

Assembly, account management and licence activation. Prerequisites to be met before configuring a U-Alarm device.

Add cameras to U-Alarm and watch their live feed.

Understand and configure alarm/counter logic in U-Alarm.

Determine operating hours for the alarms.

Details about the Operator's view.

Additional settings.

U-Alarm supports Milestone Xprotect VMS integration. This step-by-step documentation will help the configuration in order to receive Alarms in Milestone XProtect triggered by U-Alarm.

Installation

Before you start

Make sure you have the following devices and tools available:

- Linux Host PC Ubuntu (with 50 GB free space) with Internet connection.
- USB type A - micro USB cable (OTG cable).
- A supported Jetson device, see Prepare your device section below.
- An SSD of at least 500 GB in size in the Jetson device.
- A monitor attached to the HDMI port of the Jetson device. Optionally an USB keyboard as well.
- For some specific devices you might need SIM ejection pins (2 x SIM removal pin or paper clip as equivalent) for pressing the reset and recovery buttons at the same time, such as on ADLINK devices.

Prepare your device

Your device needs to be set to RECOVERY MODE.

Generation	Manufacturer	Model	Vendor supplied documentation
TX2	ADLINK	DLAP-201-	Link

		JT2	Section: 3.2 System Recovery
NX	ADLINK	DLAP-211-JNX	Link Section: 3.2 System Recovery
NX	AAEON	BOXER-8253AI	Link Section: 3.2 Connecting to PC / Force Recovery Mode

Excerpts

- ADLINK devices: **DLAP-201-JT2 (TX2)** and **DLAP-211-JNX (NX)**

    1. Connect the OTG cable to the USB 2.0 port.
    2. Press and hold the reset and recovery buttons at the same time.
    3. Press the power switch.
    4. Release the reset button.
    5. Release the recovery button.

- **AAEON BOXER-8253AI (NX)**

    1. Connect the OTG cable to the USB 2.0 port.
    2. Press and hold the recovery button.
    3. Press the power switch.
    4. Release the recovery button.

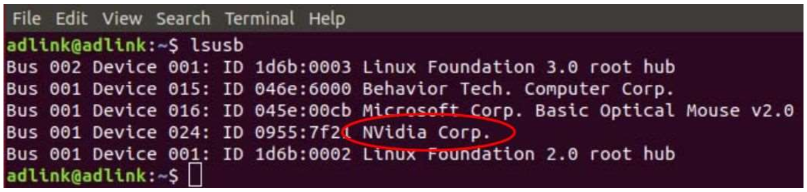
Host PC

1. Install Python 2.7, python-minimal (or equivalent packages) and qemu-user-static on the host PC.

2. Connect the host PC to the client via OTG cable.

3. Enter recovery mode, see above.

4. Open a terminal on the host PC and run the `lsusb` command.



```
adlink@adlink:~$ lsusb
Bus 002 Device 001: ID 1d6b:0003 Linux Foundation 3.0 root hub
Bus 001 Device 015: ID 046e:6000 Behavior Tech. Computer Corp.
Bus 001 Device 016: ID 045e:00cb Microsoft Corp. Basic Optical Mouse v2.0
Bus 001 Device 024: ID 0955:7f21 NVidia Corp.
Bus 001 Device 001: ID 1d6b:0002 Linux Foundation 2.0 root hub
adlink@adlink:~$ 
```

(Source: [ADLink TX2 documentation][Adlink-DLAP-201-JT2])

5. Look for `NVidia Corp.` in the output (an example is circled in red in the screenshot above). If found, the host PC recognises the client and you may proceed. If not, double-

check the OTG cable connection and perform troubleshooting as needed until the client is recognised.

6. Download the U-Alarm image and flasher using the link you have received from support via e-mail (support@ultinous.com).

```
root@host:~# wget "insert link here" -O ualarm_installer.tar.gz
```

7. Now run the following commands in the directory that contains your downloaded U-Alarm flasher file:

```
root@host:~# tar xzvf ualarm_installer.tar.gz

root@host:~# cd ualarm_installer_2_1_0  # or similar
```

8. Start flashing.

Before you start: Make sure that your default python interpreter is version 2.

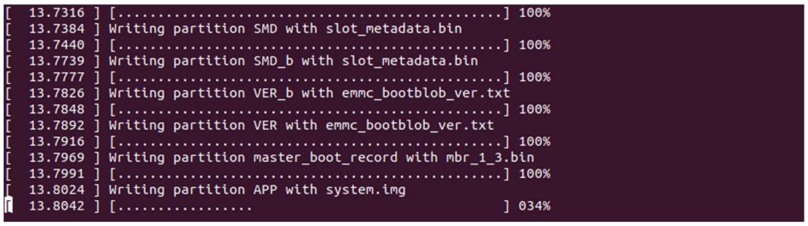
a. TX2 generation devices:

```
root@host:~/ualarm_installer_2_1_0# ./flash.sh -r jetson-tx2 mmcblk0p1
```

b. NX generation devices:

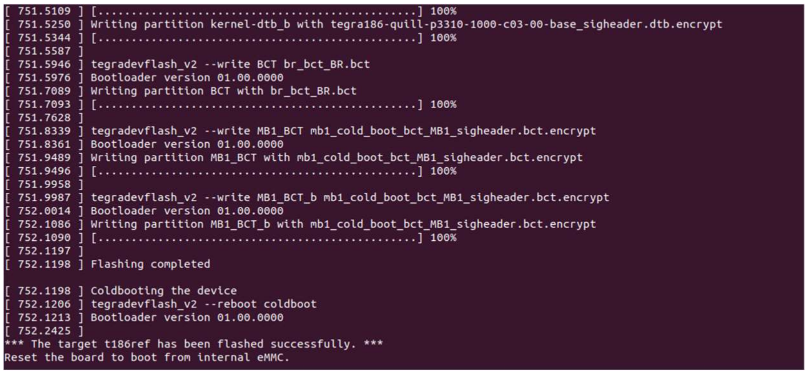
```
root@host:~/ualarm_installer_2_1_0# ./flash.sh -r jetson-xavier-nx-devkit-emmc mmcblk0p1
```

NOTE: Progress may take up to 15 minutes.



```
[   13.7316 ] [................................................] 100%
[   13.7384 ] Writing partition SMD with slot_metadata.bin
[   13.7440 ] [................................................] 100%
[   13.7739 ] Writing partition SMD_b with slot_metadata.bin
[   13.7777 ] [................................................] 100%
[   13.7826 ] Writing partition VER_b with emmc_bootblob_ver.txt
[   13.7848 ] [................................................] 100%
[   13.7892 ] Writing partition VER with emmc_bootblob_ver.txt
[   13.7916 ] [................................................] 100%
[   13.7969 ] Writing partition master_boot_record with mbr_1_3.bin
[   13.7991 ] [................................................] 100%
[   13.8024 ] Writing partition APP with system.img
[   13.8042 ] [.................                               ] 034%
```

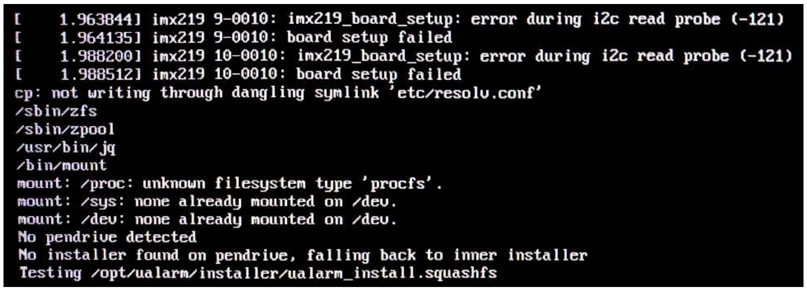
9. Allow the update to complete. If flashing was successful, the box will restart and the installation will begin automatically.



```
[ 751.5109 ] [................................................] 100%
[ 751.5250 ] Writing partition kernel-dtb_b with tegra186-quill-p3310-1000-c03-00-base_sigheader.dtb.encrypt
[ 751.5344 ] [................................................] 100%
[ 751.5587 ]
[ 751.5946 ] tegradevflash_v2 --write BCT br_bct_BR.bct
[ 751.5976 ] Bootloader version 01.00.0000
[ 751.7089 ] Writing partition BCT with br_bct_BR.bct
[ 751.7093 ] [................................................] 100%
[ 751.7628 ]
[ 751.8339 ] tegradevflash_v2 --write MB1_BCT mb1_cold_boot_bct_MB1_sigheader.bct.encrypt
[ 751.8361 ] Bootloader version 01.00.0000
[ 751.9489 ] Writing partition MB1_BCT with mb1_cold_boot_bct_MB1_sigheader.bct.encrypt
[ 751.9496 ] [................................................] 100%
[ 751.9958 ]
[ 751.9987 ] tegradevflash_v2 --write MB1_BCT_b mb1_cold_boot_bct_MB1_sigheader.bct.encrypt
[ 752.0014 ] Bootloader version 01.00.0000
[ 752.1086 ] Writing partition MB1_BCT_b with mb1_cold_boot_bct_MB1_sigheader.bct.encrypt
[ 752.1090 ] [................................................] 100%
[ 752.1197 ]
[ 752.1198 ] Flashing completed

[ 752.1198 ] Coldbooting the device
[ 752.1206 ] tegradevflash_v2 --reboot coldboot
[ 752.1213 ] Bootloader version 01.00.0000
[ 752.2425 ]
*** The target t186ref has been flashed successfully. ***
Reset the board to boot from internal eMMC.
```

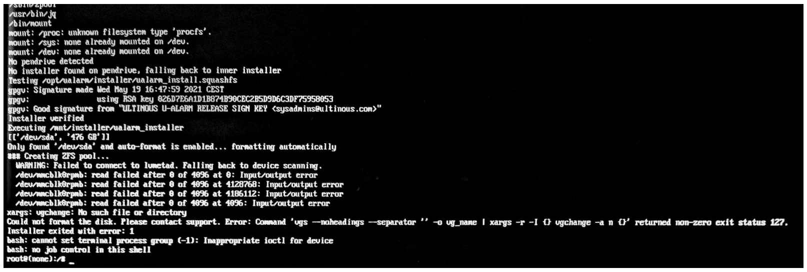
Installation

1. Wait for the installer to check its integrity.

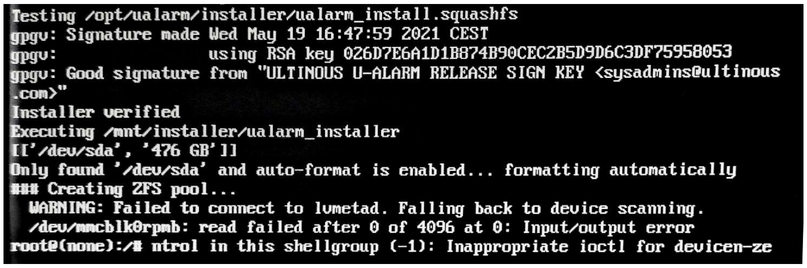


```
[    1.963844] imx219 9-0010: imx219_board_setup: error during i2c read probe (-121)
[    1.964135] imx219 9-0010: board setup failed
[    1.988200] imx219 10-0010: imx219_board_setup: error during i2c read probe (-121)
[    1.988512] imx219 10-0010: board setup failed
cp: not writing through dangling symlink 'etc/resolv.conf'
/sbin/zfs
/sbin/zpool
/usr/bin/jq
/bin/mount
mount: /proc: unknown filesystem type 'procfs'.
mount: /sys: none already mounted on /dev.
mount: /dev: none already mounted on /dev.
No pendrive detected
No installer found on pendrive, falling back to inner installer
Testing /opt/ualarm/installer/ualarm_install.squashfs
```

a. If you had previously installed and older version than 1.2.0 of U-Alarm on your machine, the installation might fail in one of two ways:



```
/sbin/zpool
/usr/bin/jq
/bin/mount
mount: /proc: unknown filesystem type 'procfs'.
mount: /sys: none already mounted on /dev.
mount: /dev: none already mounted on /dev.
No pendrive detected
No installer found on pendrive, falling back to inner installer
Testing /opt/ualarm/installer/ualarm_install.squashfs
gpgv: Signature made Wed May 19 16:47:59 2021 CEST
gpgv:                using RSA key 026D7E6A1D1B874B90CEC2B5D9D6C3DF75958053
gpgv: Good signature from "ULTINOUS U-ALARM RELEASE SIGN KEY <sysadmins@ultinous.com>"
Installer verified
Executing /mnt/installer/ualarm_installer
[['/dev/sda', '476 GB']]
Only found '/dev/sda' and auto-format is enabled... formatting automatically
### Creating ZFS pool...
  WARNING: Failed to connect to lvmetad. Falling back to device scanning.
  /dev/mmcblk0rpmb: read failed after 0 of 4096 at 0: Input/output error
  /dev/mmcblk0rpmb: read failed after 0 of 4096 at 4128768: Input/output error
  /dev/mmcblk0rpmb: read failed after 0 of 4096 at 4186112: Input/output error
  /dev/mmcblk0rpmb: read failed after 0 of 4096 at 4096: Input/output error
xargs: vgchange: No such file or directory
Could not format the disk. Please contact support. Error: Command 'vgs --noheadings --separator '' -o vg_name | xargs -r -I {} vgchange -a n {}' returned non-zero exit status 127.
Installer exited with error: 1
bash: cannot set terminal process group (-1): Inappropriate ioctl for device
bash: no job control in this shell
root@(none):/# _
```



```
Testing /opt/ualarm/installer/ualarm_install.squashfs
gpgv: Signature made Wed May 19 16:47:59 2021 CEST
gpgv:                using RSA key 026D7E6A1D1B874B90CEC2B5D9D6C3DF75958053
gpgv: Good signature from "ULTINOUS U-ALARM RELEASE SIGN KEY <sysadmins@ultinous
.com>"
Installer verified
Executing /mnt/installer/ualarm_installer
[['/dev/sda', '476 GB']]
Only found '/dev/sda' and auto-format is enabled... formatting automatically
### Creating ZFS pool...
  WARNING: Failed to connect to lvmetad. Falling back to device scanning.
  /dev/mmcblk0rpmb: read failed after 0 of 4096 at 0: Input/output error
root@(none):/# ntrol in this shellgroup (-1): Inappropriate ioctl for devicen-ze
```

b. To remedy this, the old partitioning will have to be cleared on the ssd.

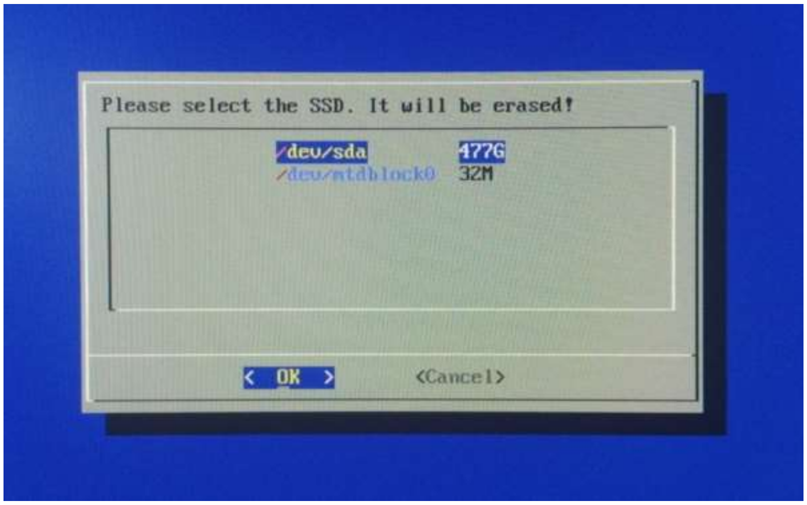
c. Note down your drive path from the line after `Executing /mnt/installer/ualarm_installer` (in the example image, it's `/dev/sda`).

d. Execute `wipefs -a <your drive path>` then `reboot -f`.

f. The system will reboot and the installation will resume from step 1. If the problem still persists, please contact our support (support@ultinous.com).

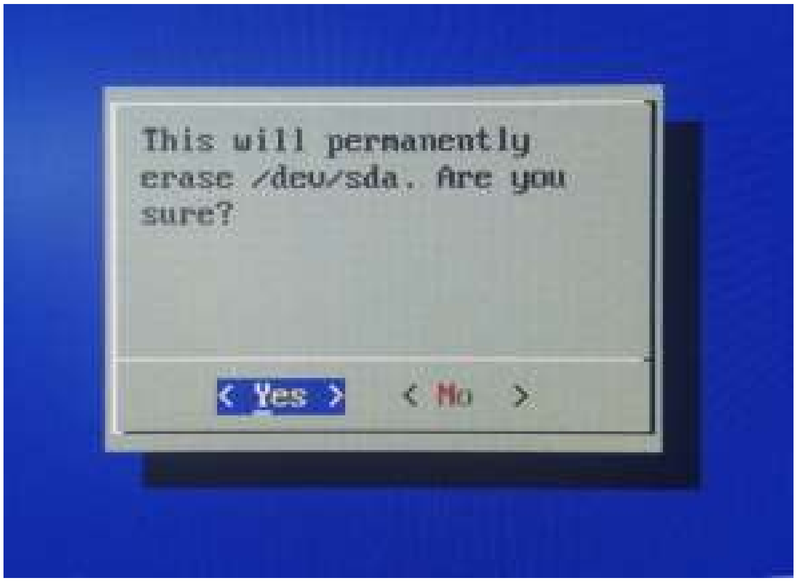
2. Select Target Medium (hardware dependent)

In case you have multiple drives suitable for installation, select the desired SSD drive for the installation (see the images below). If your hardware configuration includes only one such drive, this step will not appear.



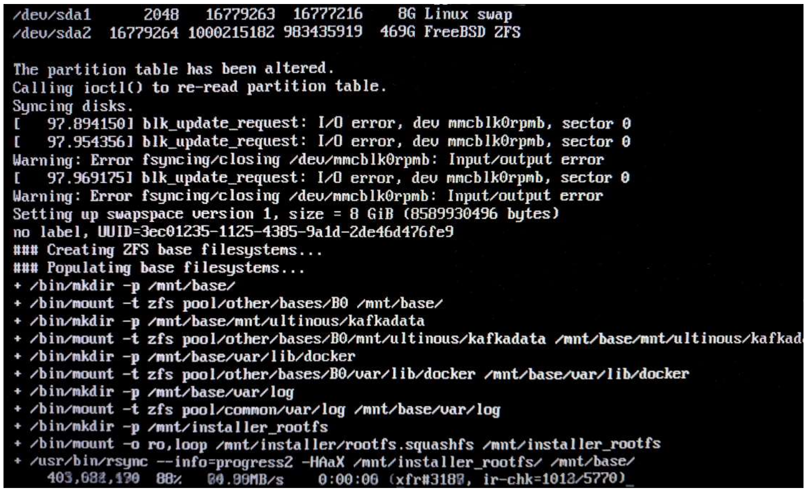
Please select the SSD. It will be erased!

```
/dev/sda         477G
/dev/mtdblock0   32M
```



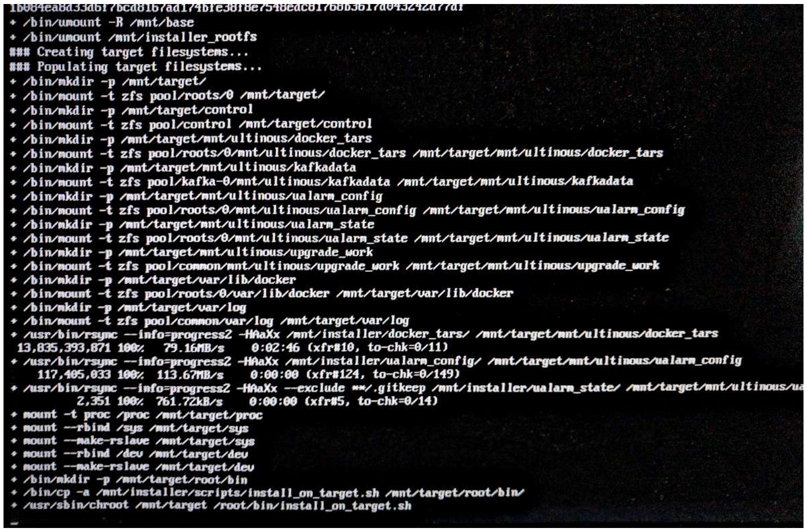
This will permanently erase /dev/sda. Are you sure?

3. Wait for the installer to copy the necessary files. This step can take up to 5 minutes.



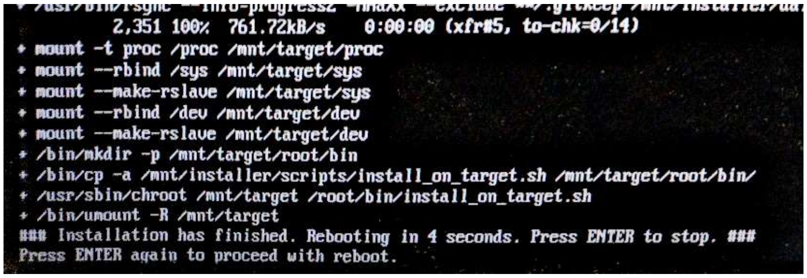
```
/dev/sda1      2048   16779263  16777216    8G Linux swap
/dev/sda2  16779264 1000215182 983435919  469G FreeBSD ZFS

The partition table has been altered.
Calling ioctl() to re-read partition table.
Syncing disks.
[   97.894150] blk_update_request: I/O error, dev mmcblk0rpmb, sector 0
[   97.954356] blk_update_request: I/O error, dev mmcblk0rpmb, sector 0
Warning: Error fsyncing/closing /dev/mmcblk0rpmb: Input/output error
[   97.969175] blk_update_request: I/O error, dev mmcblk0rpmb, sector 0
Warning: Error fsyncing/closing /dev/mmcblk0rpmb: Input/output error
Setting up swapspace version 1, size = 8 GiB (8589930496 bytes)
no label, UUID=3ec01235-1125-4385-9a1d-2de46d476fe9
### Creating ZFS base filesystems...
### Populating base filesystems...
+ /bin/mkdir -p /mnt/base/
+ /bin/mount -t zfs pool/other/bases/B0 /mnt/base/
+ /bin/mkdir -p /mnt/base/mnt/ultinous/kafkadata
+ /bin/mount -t zfs pool/other/bases/B0/mnt/ultinous/kafkadata /mnt/base/mnt/ultinous/kafkad
+ /bin/mkdir -p /mnt/base/var/lib/docker
+ /bin/mount -t zfs pool/other/bases/B0/var/lib/docker /mnt/base/var/lib/docker
+ /bin/mkdir -p /mnt/base/var/log
+ /bin/mount -t zfs pool/common/var/log /mnt/base/var/log
+ /bin/mkdir -p /mnt/installer_rootfs
+ /bin/mount -o ro,loop /mnt/installer/rootfs.squashfs /mnt/installer_rootfs
+ /usr/bin/rsync --info=progress2 -HAaX /mnt/installer_rootfs/ /mnt/base/
    403,682,170  88%   80.90MB/s    0:00:06 (xfr#3180, ir-chk=1013/5770)_
```

4. Wait for the installer to process the files. This step has no progress indication - it can take up to 5 minutes.



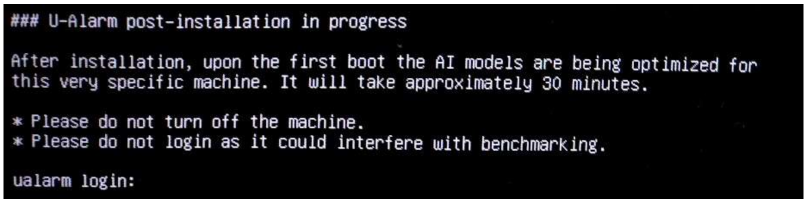
```
1b084ea8d33d6f7bcd8167ad174b1e38f8e7548edc81768b3617d0432422d77d1
+ /bin/umount -R /mnt/base
+ /bin/umount /mnt/installer_rootfs
### Creating target filesystems...
### Populating target filesystems...
+ /bin/mkdir -p /mnt/target/
+ /bin/mount -t zfs pool/roots/0 /mnt/target/
+ /bin/mkdir -p /mnt/target/control
+ /bin/mount -t zfs pool/control /mnt/target/control
+ /bin/mkdir -p /mnt/target/mnt/ultinous/docker_tars
+ /bin/mount -t zfs pool/roots/0/mnt/ultinous/docker_tars /mnt/target/mnt/ultinous/docker_tars
+ /bin/mkdir -p /mnt/target/mnt/ultinous/kafkadata
+ /bin/mount -t zfs pool/kafka-0/mnt/ultinous/kafkadata /mnt/target/mnt/ultinous/kafkadata
+ /bin/mkdir -p /mnt/target/mnt/ultinous/ualarm_config
+ /bin/mount -t zfs pool/roots/0/mnt/ultinous/ualarm_config /mnt/target/mnt/ultinous/ualarm_config
+ /bin/mkdir -p /mnt/target/mnt/ultinous/ualarm_state
+ /bin/mount -t zfs pool/roots/0/mnt/ultinous/ualarm_state /mnt/target/mnt/ultinous/ualarm_state
+ /bin/mkdir -p /mnt/target/mnt/ultinous/upgrade_work
+ /bin/mount -t zfs pool/common/mnt/ultinous/upgrade_work /mnt/target/mnt/ultinous/upgrade_work
+ /bin/mkdir -p /mnt/target/var/lib/docker
+ /bin/mount -t zfs pool/roots/0/var/lib/docker /mnt/target/var/lib/docker
+ /bin/mkdir -p /mnt/target/var/log
+ /bin/mount -t zfs pool/common/var/log /mnt/target/var/log
+ /usr/bin/rsync --info=progress2 -HAaXx /mnt/installer/docker_tars/ /mnt/target/mnt/ultinous/docker_tars
 13,835,393,871 100%   79.16MB/s    0:02:46 (xfr#10, to-chk=0/11)
+ /usr/bin/rsync --info=progress2 -HAaXx /mnt/installer/ualarm_config/ /mnt/target/mnt/ultinous/ualarm_config
    117,405,033 100%  113.67MB/s    0:00:00 (xfr#124, to-chk=0/149)
+ /usr/bin/rsync --info=progress2 -HAaXx --exclude **/.gitkeep /mnt/installer/ualarm_state/ /mnt/target/mnt/ultinous/ua
          2,351 100%  761.72kB/s    0:00:00 (xfr#5, to-chk=0/14)
+ mount -t proc /proc /mnt/target/proc
+ mount --rbind /sys /mnt/target/sys
+ mount --make-rslave /mnt/target/sys
+ mount --rbind /dev /mnt/target/dev
+ mount --make-rslave /mnt/target/dev
+ /bin/mkdir -p /mnt/target/root/bin
+ /bin/cp -a /mnt/installer/scripts/install_on_target.sh /mnt/target/root/bin/
+ /usr/sbin/chroot /mnt/target /root/bin/install_on_target.sh
_
```

5. Wait for the system to reboot. You can prevent rebooting and optionally do an inspection if you press ENTER once you see a countdown from 15 seconds.



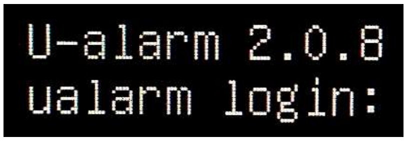
```
+ /usr/bin/rsync --info=progress2 -HAaXx --exclude **/.gitkeep /mnt/installer/ua
          2,351 100%  761.72kB/s    0:00:00 (xfr#5, to-chk=0/14)
+ mount -t proc /proc /mnt/target/proc
+ mount --rbind /sys /mnt/target/sys
+ mount --make-rslave /mnt/target/sys
+ mount --rbind /dev /mnt/target/dev
+ mount --make-rslave /mnt/target/dev
+ /bin/mkdir -p /mnt/target/root/bin
+ /bin/cp -a /mnt/installer/scripts/install_on_target.sh /mnt/target/root/bin/
+ /usr/sbin/chroot /mnt/target /root/bin/install_on_target.sh
+ /bin/umount -R /mnt/target
### Installation has finished. Rebooting in 4 seconds. Press ENTER to stop. ###
Press ENTER again to proceed with reboot.
```

6. Wait for the machine to optimise AI models for the specific machine. It will have no progress indication and can take up to 30 minutes.



```
### U-Alarm post-installation in progress

After installation, upon the first boot the AI models are being optimized for
this very specific machine. It will take approximately 30 minutes.

* Please do not turn off the machine.
* Please do not login as it could interfere with benchmarking.

ualarm login:
```

7. Installation is finished. The above notification is replaced with a standard login screen.



```
U-alarm 2.0.8
ualarm login:
```

The web user interface will take an additional 2 minutes to be available.

The installation is now complete. To shutdown the device, short press and release the power button - do not long press it - then wait for the system to shut down. Alternatively you can proceed with the configuration.

Next steps

To configure U-Alarm, follow the steps described in the User's guide.

First Steps

Before you start

Make sure you have all of the following components before you start the configuration process:

- A working computer with a browser (Google Chrome is recommended). It will be used to configure U-Alarm via its web interface. The supported Operating Systems are Windows, Linux and Mac OSX.
- (Optional) One or more additional tools, depending on your needs. See the Additional Tools guide for a complete list.
- LAN with DHCP service
- At least one working IP camera with a known RTSP URL.
- The Jetson box with U-Alarm installed (U-Alarm box).

  Contact sales@ultinous.com for help.
- A valid U-Alarm Licence Activation Key.

  Contact sales@ultinous.com for help.
- One free network port on the same subnet as the computer.
- One free 220 power supply socket.

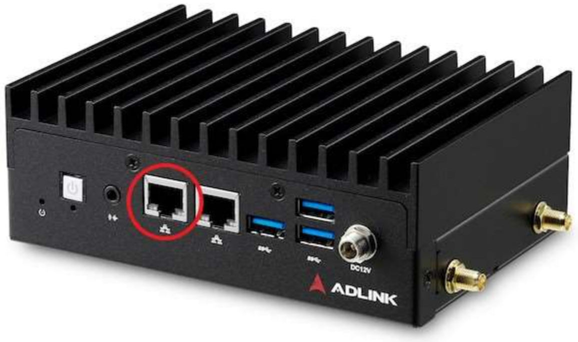
Power up the U-Alarm box

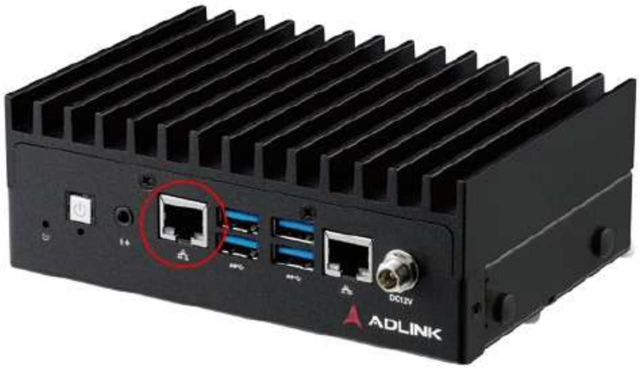
Connect the U-Alarm box to the 220 power supply.

Note: There are two similar silver sockets. Make sure to connect the power cable to the one with the DC label: it is on the same side of the box as the Ethernet port (see the image below).

Connect the U-Alarm box to the Ethernet network using the primary Ethernet port of the device.

Note: There could be more than one network port, depending on the device. Make sure to use the correct, primary Ethernet port of the device, and not, for instance, a PoE port. See the examples below.





There is no turn on/off button: a LED indicates if the box is properly connected to the power supply. Wait about one minute after you powered the U-Alarm box to let the Operating System and U-Alarm start.

Find out the IP address of the U-Alarm box

At this point the U-Alarm box is working, but you need to figure out its IP address to be able to log in to its web interface.

By default U-Alarm is configured to acquire IP address via DHCP. Later this can be changed to use a fixed IP address. There are multiple ways to find out its IP address:

1. In a corporate environment, ask the system administrators for help.
2. In a home environment, the IP address can be found on the router's web page (typically 192.168.0.1, look for a list of DHCP clients. The client name is 'ualarm' by default).
3. On Windows, use the provided U-Alarm IP discovery tool (it requires .NET 4.5 or higher. On Windows 10, it is installed by default).

The current version of the network discovery tool supports U-Alarm 2.0.2 and above.

Make sure the computer and the U-Alarm box are on the same sub-network. It automatically queries the network for available U-Alarm boxes, and displays their addresses in a table along with their configured hostnames and system uptime. The address can be copied to clipboard by double clicking on the row or by clicking the copy button.

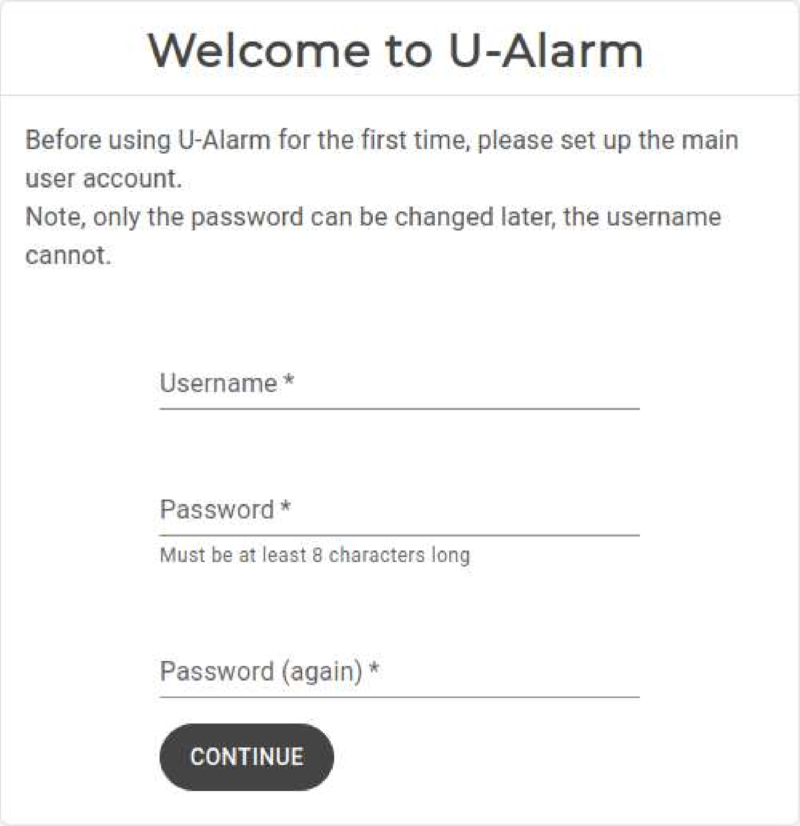
4. On Linux systems, use the provided Python script. The Python client has no dependencies other than a Python interpreter (version 3.6 or later). Ubuntu 18.04 and Debian 10 have them preinstalled. For other operating systems, please refer to their installation guide.

Open web interface

Copy the IP address of the box to a web browser and open it. You will see the user interface of U-Alarm. Here you can configure the system, check live streams with video analysis and manage alarms.

Setup your account

Create a user name and a password. Click the **Continue** button.



Welcome to U-Alarm

Before using U-Alarm for the first time, please set up the main user account.
Note, only the password can be changed later, the username cannot.

Username *

Password *

Must be at least 8 characters long

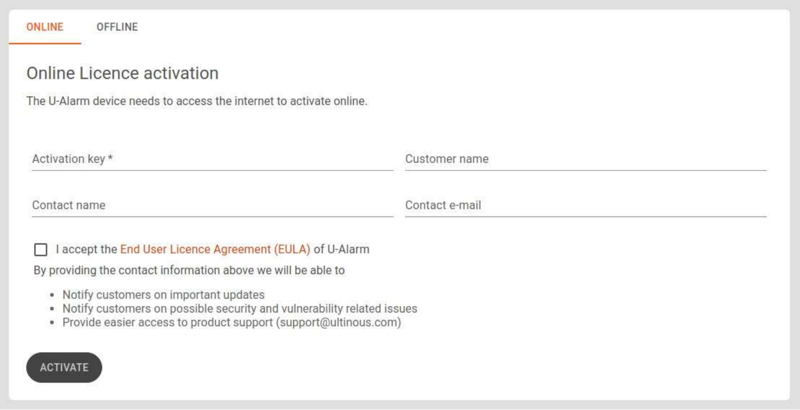
Password (again) *

Activate your licence

In this document it is assumed that you have a licence activation key for U-Alarm.

If your U-Alarm box has internet connection, you can activate your licence online, otherwise choose offline activation. You can set your licence later in the Control Panel but U-Alarm will work only after the licence is activated.

Option 1: Online licence activation



Online Licence activation

The U-Alarm device needs to access the internet to activate online.

Activation key *

Customer name

Contact name

Contact e-mail

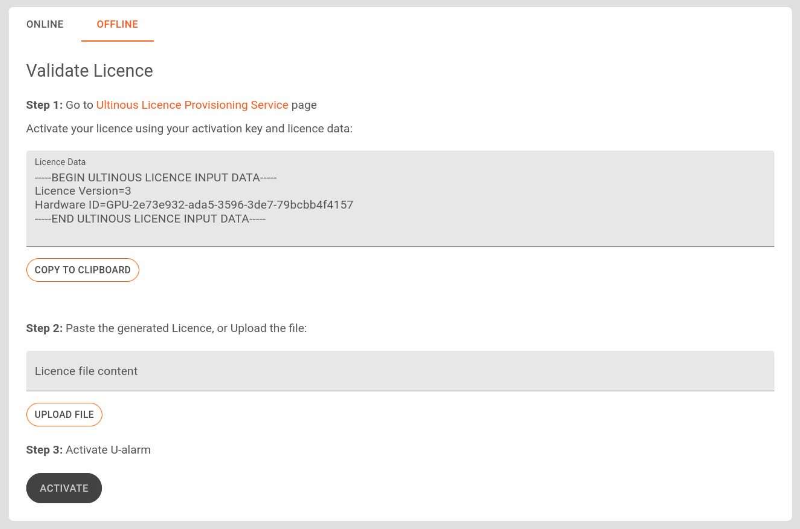
□ I accept the End User Licence Agreement (EULA) of U-Alarm

By providing the contact information above we will be able to

- Notify customers on important updates
- Notify customers on possible security and vulnerability related issues
- Provide easier access to product support (support@ultinous.com)

1. Copy your licence activation key to the Activation key field.
2. Fill in your name and contact information.
3. After you accept the Licence Agreement of U-Alarm, click the **Activate** button.

Option 2: Offline licence activation



Validate Licence

Step 1: Go to Ultinous Licence Provisioning Service page

Activate your licence using your activation key and licence data:

Licence Data

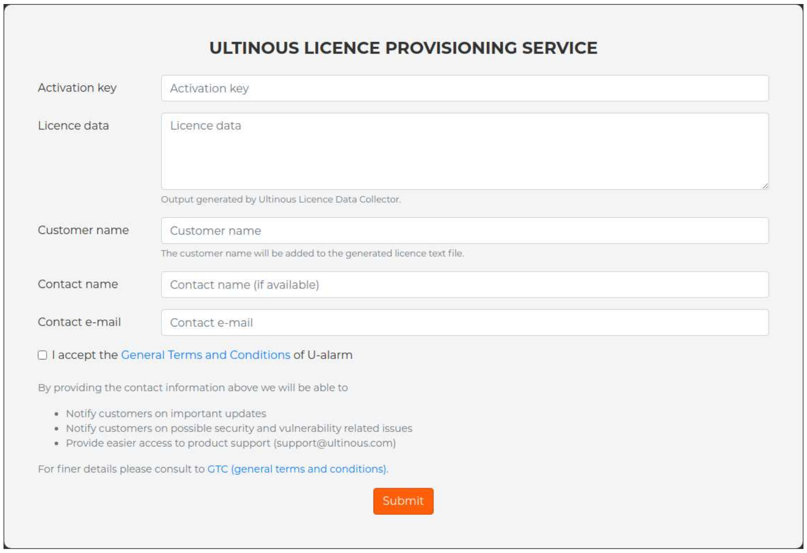
```
-----BEGIN ULTINOUS LICENCE INPUT DATA-----
Licence Version=3
Hardware ID=GPU-2e73e932-ada5-3596-3de7-79bcbb4f4157
-----END ULTINOUS LICENCE INPUT DATA-----
```

Step 2: Paste the generated Licence, or Upload the file:

Licence file content

Step 3: Activate U-alarm

1. Copy the entire content of the Licence data field to your clipboard.
2. Find a computer with internet access. Go to the Licence Provisioning Service web page at https://activation.ultinous.com/.
3. Type or paste your activation key and the licence data.
4. Fill in your name and contact information.
5. After you accept the GTC of U-Alarm, click the **Activate** button.
6. Press the **Submit** button.



ULTINOUS LICENCE PROVISIONING SERVICE

Activation key: Activation key

Licence data: Licence data

Output generated by Ultinous Licence Data Collector.

Customer name: Customer name

The customer name will be added to the generated licence text file.

Contact name: Contact name (if available)

Contact e-mail: Contact e-mail

□ I accept the General Terms and Conditions of U-alarm

By providing the contact information above we will be able to

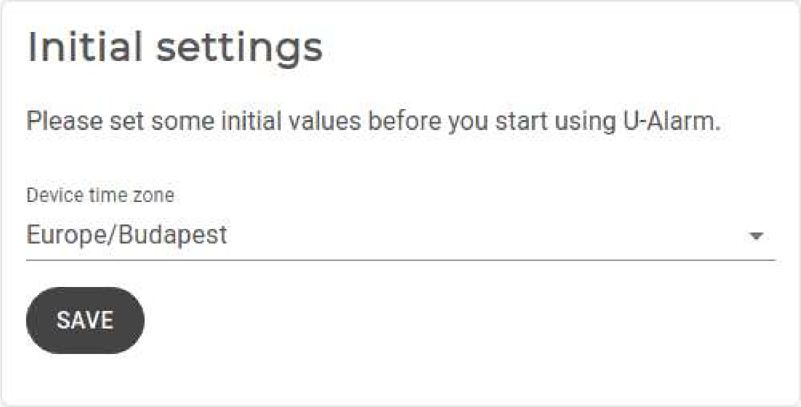
- Notify customers on important updates
- Notify customers on possible security and vulnerability related issues
- Provide easier access to product support (support@ultinous.com)

For finer details please consult to GTC (general terms and conditions).

7. Download the offline licence file.
8. Go back to U-Alarm and upload the offline licence file.
9. Click the Activate button.

Set Timezone

Once the web interface is loaded, U-Alarm asks you to set your Timezone. Setting it is mandatory but it can be modified later in the Control Panel.



Initial settings

Please set some initial values before you start using U-Alarm.

Device time zone: Europe/Budapest

Next steps

You can proceed with the Quick start guide or go to the detailed Camera settings help page.

Cameras

You can add your cameras to U-Alarm and watch their live play here.

Click the **Cameras** menu on the left sidebar for this view.

Before you start

Please make sure that everything described in the First Steps is done and you have all these information for each camera:

- The location / desired name of the camera
- Camera RTSP address (including username and password if the camera is protected)
- The current resolution and FPS setting.

Note: Make sure your camera's active infra range is aligned with the desired distance range.

Note: Make sure your camera's cover is clear. Dirt on it can heavily effect the night vision accuracy.

Understanding the detection range

The intrusion detection algorithm of U-Alarm can detect persons in a wide distance range but **the optimal person height range is between 30 and 1000 pixels**. Because the algorithm always works optimally in the this pixel range, **the effective person detection range depends on the camera resolution**. Detection range can vary from 1.4 meters to multiple hundreds of meters. U-Alarm has successfully demonstrated intrusion detection at 400 meters' range using high level of optical zoom.

Examples:

Vertical field of view (degrees)	Frame height (pixels)	max range (m)
100*	480*	11.7*
100	576	13.7
100	600	14.3
100	720	17.1
100	1080	25.7
75*	480*	18.2*
75	576	21.3
75	600	22.2
75	720	26.6
75	1080	39.9

40*	480*	38.5*
40	576	44.8
40	600	46.7
40	720	56
40	1080	84.1

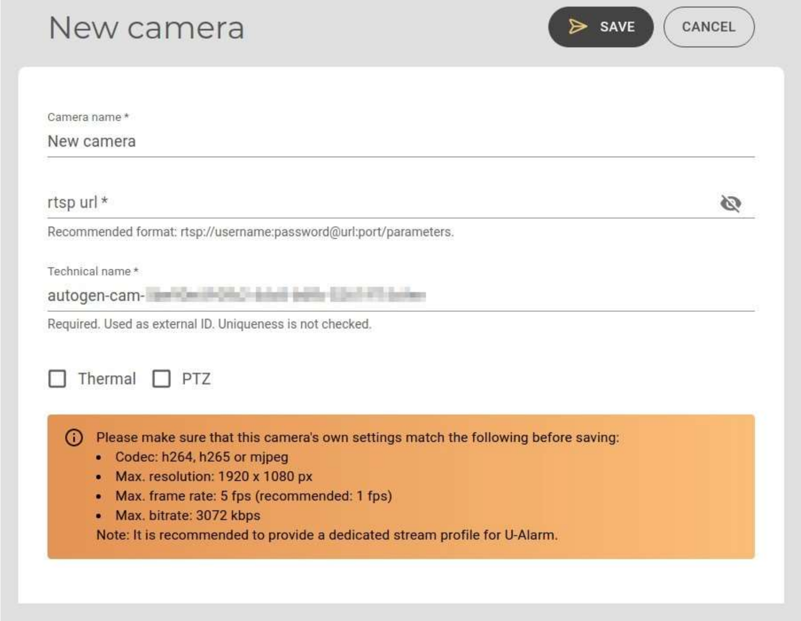
*Note: These lines refer to moving cameras. Range depends on the level of magnification.

Add a new camera

IMPORTANT: Make sure that this camera's *own settings* match the following before adding any cameras to U-Alarm:

- Codec: h264, h265 or mjpeg
- Maximum supported resolution is **1920 x 1080 px**.
- The recommended frame rate is **1 fps** (max. 5 fps).
- Max. bitrate **3072 kbps**.
- The keyframe interval (sometimes called "GOP length") is **3 or less**.

It is recommended to provide a dedicated stream profile for U-Alarm.



Camera name *
New camera

rtsp url *
Recommended format: rtsp://username:password@url:port/parameters.

Technical name *
autogen-cam-[redacted]
Required. Used as external ID. Uniqueness is not checked.

☐ Thermal ☐ PTZ

Please make sure that this camera's own settings match the following before saving:
- Codec: h264, h265 or mjpeg
- Max. resolution: 1920 x 1080 px
- Max. frame rate: 5 fps (recommended: 1 fps)
- Max. bitrate: 3072 kbps

Note: It is recommended to provide a dedicated stream profile for U-Alarm.

1. Click the **New Camera** button. Fill the form on the right side.
2. **Camera name**: This name should identify the camera for operator users (eg. Entrance 1).
3. **RTSP URL**: The location of the camera. The recommended format is *rtsp://username:password@url:port/parameters*.
4. **Technical name**: U-Alarm will automatically generate a technical name (denoted by the "autogen-" part): This will identify the camera in external services if the alarms are

sent to a third-party software according to the corresponding document. In such use cases, it is recommended to rename this to something unique and identifiable.

Make sure that the camera has the same *Technical name* in U-Alarm and *GUID* in Milestone XProtect - otherwise the camera will not be recognised! See the Milestone XProtect section of the guide for details.

5. **Thermal**: Tick this checkbox if the camera is a thermal one.

6. **PTZ**: Tick this checkbox if the camera is a PTZ one or is otherwise capable of movement or zooming.

7. Click the **Save** button to register the camera.

   After a few seconds, the new camera should appear in the **Cameras** list. The live view of the new camera is available after clicking on its name or preview image in this list.

   Warning: Do not modify the resolution or the framerate of a stream after it is connected to U-alarm. If the stream's settings are changed, U-Alarm will stop processing that stream and will be in unhealthy state in monitoring services used.

   If a stream's settings are changed anyway, and the new settings are still compatible with U-Alarm, the processing of the streams can be restarted by clicking on the **RELOAD ALL** button below the registered camera thumbnails.

   NOTE: It may take a while to load a preview image for your cameras. You can continue your work, the preview will appear automatically later.

   In rare cases U-Alarm can not determine your stream's FPS and asks for confirmation whether your framerate matches the requirements.

Edit an existing camera

1. In the **Cameras** list, click on the preview image of a camera.
2. Click the **Edit** button above the camera's live view.
3. Modify your settings. In this form everything is the same as when adding a new camera with the following exceptions:
   - **RTSP URL** should be filled only if the URL is changed. For security reasons, the current username and password is not visible in the URL.
   - **Deleting** a camera *deletes all alarms, events and incident records* which belong to this camera.
4. Click the **Save** button to apply the new settings or **Cancel** to discard your edits.

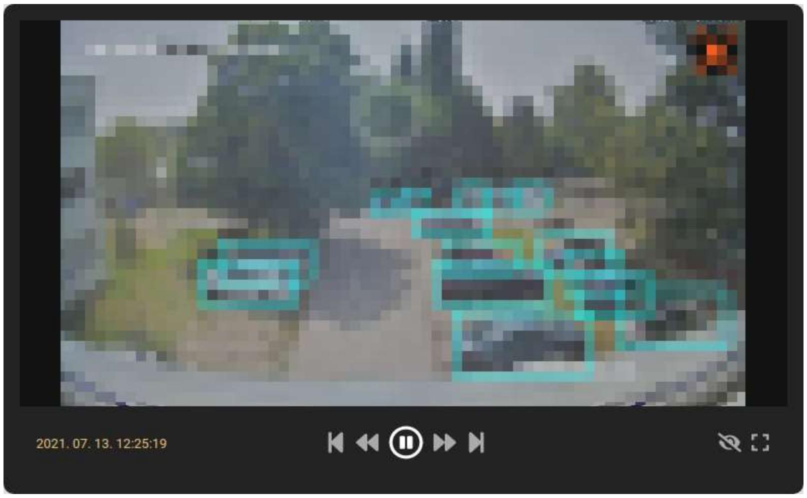
Delete an existing camera

NOTE: Deleting a camera **deletes all alarms, events and incident records** which belong to this camera.

1. In the **Cameras** list, click on the preview image of a camera.
2. Click the **Delete** button above the camera's live view.

Camera Live view

In the **Cameras** list, click on the preview image or the name of an existing camera. The live view will load in a few seconds.



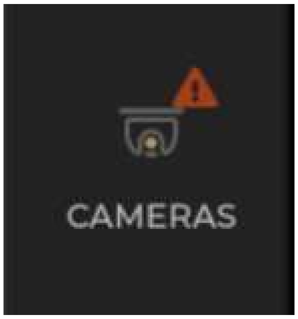
Display features

- If an Alarm with ROIs is associated with this camera, positive / negative ROIs are displayed as *green / red* polygons with a dashed line.
- Detections inside the ROI (or if there is no ROI) are solid *orange / aqua* polygons, depending on the detected object type. Their object type is denoted above the polygons. In the label next to it is the 'detection score' - the number that tells you the strength of the detection. This is influenced by the Sensitivity rating of the Camera associated with an Alarm. You can learn more about fine-tuning this in the Expert Settings part of the guide.
- If an Alarm is triggered, a *Bell* icon will appear in the top right corner of the player.
- The *timestamp* of the video is at the bottom left corner of the player (can be different from the one that comes from the camera) in the timezone of the device. The timezone can be modified in the Control Panel.

Controls

- **||** and **>** toggle between pause and play
- **|<** button rewinds to the earliest available video
- **>|** button jumps to live play
- **<<** button jumps backward ten seconds
- **>>** button jumps forward ten seconds
- The *Eye* button shows / hides annotations
- You can go to full screen play by clicking the *Rectangle* button in the lower right corner of the player

Troubleshooting



If something is wrong with the configuration of any of your cameras, U-Alarm has several indicators:

- A red "warning" badge on the Cameras button on the left-side panel
- A clickable red "Error" message on the malfunctioning camera
- A clickable notification bar will appear at the bottom right corner

Clicking the "Error" message or the notification bar will navigate you to the System Health page of the Control Panel, where information regarding the camera's health status will appear to help you investigate the issue.

Next steps

After the registration of your cameras, you may continue by setting up Alarms.

Alarms and Counters

Alarms are processes for detecting incidents.

Click the **Alarms** menu on the left sidebar for this view.

Before you start

Please make sure that all Cameras are registered and activated in U-Alarm.

When adding Alarms or Counters, make sure to take into account the Analysis Slots they would take up.

Supported Alarms

Intrusion Detection

An **Intrusion Detection alarm** is triggered whenever a person or ground vehicle is detected in a restricted area. It has high accuracy and low false alarm rate even at long range and with different light conditions.

- Core technology: full body and ground vehicle detection.

  Full body detection distance and accuracy is high, compared to head detection.

- Available classes: person, car, bus, truck, motorcycle, bicycle
- Compatible with *fixed*, *PTZ*, and *thermal* cameras.
- Areas of interest can be defined.
- Send alarm notifications to third-party software.

Multi Object Detection

A Multi Object Detection alarm is triggered whenever people or vehicles (ground, air and watercraft) are detected within a set time frame or location. It has high accuracy and low false alarm rate even at long range and with different light conditions. This method of detection is ideal for specialised use cases that require the detection, classification and filtering of objects, to determine if the following is true:

Person or Vehicle is:	Use case example
at the wrong place	Truck blocking an emergency exit
at the wrong time	A vehicle is detected at night in a daytime-only parking lot
of the wrong type	Motorcycle occupying a bicycle parking spot

- Core technology: full body and vehicle detection.
- Available classes: person, car, bus, truck, motorcycle, bicycle, *train, boat, airplane*
- Compatible with *fixed*, *PTZ*, and *thermal* cameras.
- Areas of interest can be defined.
- Send alarm notifications to third-party software.

Crowd Detection

A **Crowd Detection** alarm is triggered whenever the number of currently visible people reaches or exceeds a specific number. Multiple cameras can be associated with a single Crowd Detection, in which case the sum of the people triggers the alarm. This use case is ideal for detecting the extreme size of a queue or for detecting a potentially dangerous situation in a safety zone. Recommended for well lit areas.

- Core technology: head detection.
- Compatible with *fixed*, *PTZ*, and *thermal* cameras.
- Areas of interest can be defined.
- Send alarm notifications to third-party software.
- Multi-camera support.

Supported Counters

Counters are designed to be used with custom third party software. **See the Counter API section for detailed instructions.**

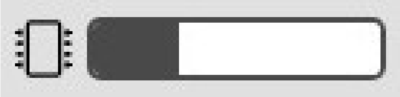
Multi Object Counter

Multi Object Counter is a tool for classifying and measuring the amount of the chosen type(s) of objects. Multiple cameras can be associated with a single Multi Object Counter - This enables the measurement of different object classes, as well as a single object type in two or more separate locations (such as counting the sum of cars in two parking lot areas) as well.

- Core technology: full body and vehicle detection.
- Compatible with *fixed*, *PTZ*, and *thermal* cameras.
- Areas of interest can be defined.
- Send data to third-party software.
- Multi-camera support.

The data produced by Multi Object Counters can be accessed by third-party tools - see the Counter API section for integration instructions - as well as in U-Alarm, in the Events screen.

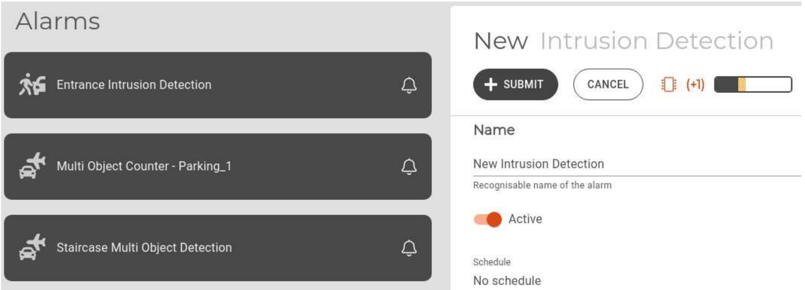
Analysis Slots



One camera stream is able to handle up to two types of detections (including Counters) - If you add an already associated Camera to a different type of Alarm or Counter too, it will fill up the stream's "quota".

A **dark grey** (so-called "Analysis Slots") indicator keeps track of this, in the upper right corner of the Alarms screen and on the New/Change Alarm screen. Click on the indicator to see how many free Slots you have.

NOTE: If the dark grey indicator fills up, you will have reached your limit and cannot add another Alarm or Counter.



Alarms

Entrance Intrusion Detection

Multi Object Counter - Parking_1

Staircase Multi Object Detection

New Intrusion Detection

Name

New Intrusion Detection

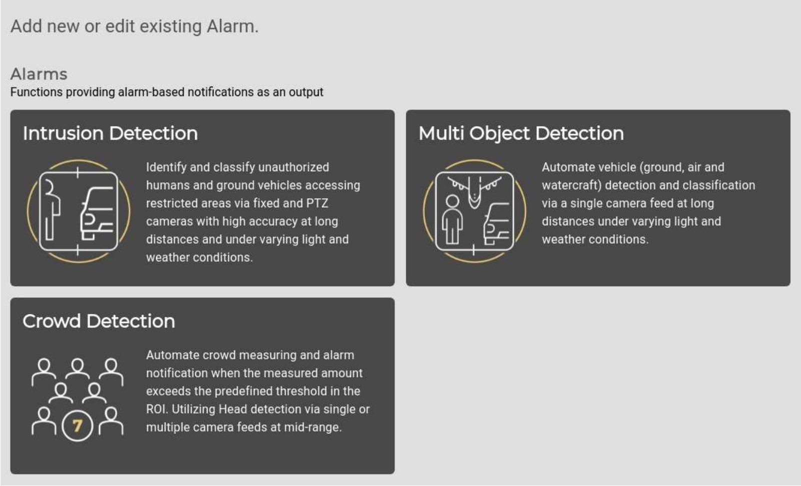
Recognisable name of the alarm

Active

Schedule

No schedule

Create a new alarm or counter



Add new or edit existing Alarm.

Alarms

Functions providing alarm-based notifications as an output

Intrusion Detection

Identify and classify unauthorized humans and ground vehicles accessing restricted areas via fixed and PTZ cameras with high accuracy at long distances and under varying light and weather conditions.

Multi Object Detection

Automate vehicle (ground, air and watercraft) detection and classification via a single camera feed at long distances under varying light and weather conditions.

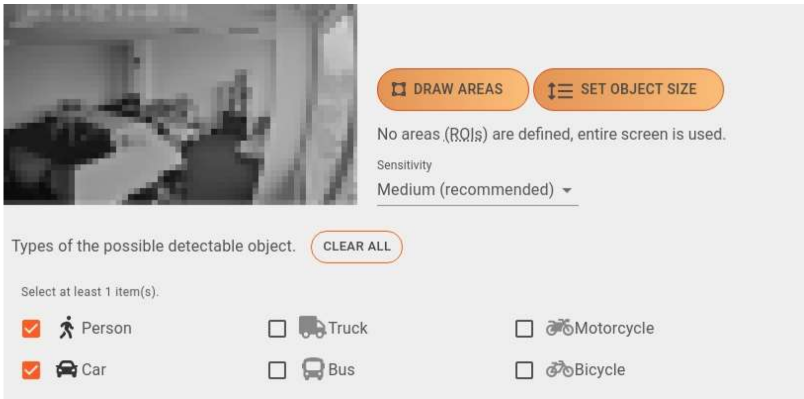
Crowd Detection

Automate crowd measuring and alarm notification when the measured amount exceeds the predefined threshold in the ROI. Utilizing Head detection via single or multiple camera feeds at mid-range.

Note: Currently, only one type of the alarm can be used at the same time per device.

New Intrusion Detection

1. Choose **Intrusion Detection** by clicking on its box. Fill in the form, as follows:
2. **Name**: A readable name of this alarm. This name will appear in the Events view and in all notifications.
3. **Armed**: The alarm can be deactivated here. Armed by default.
4. **Schedule** (optional): You can associate one of your previously defined Schedules with this alarm.
5. **Add Camera**: Select a camera from the list.



No areas (ROIs) are defined, entire screen is used.

Sensitivity

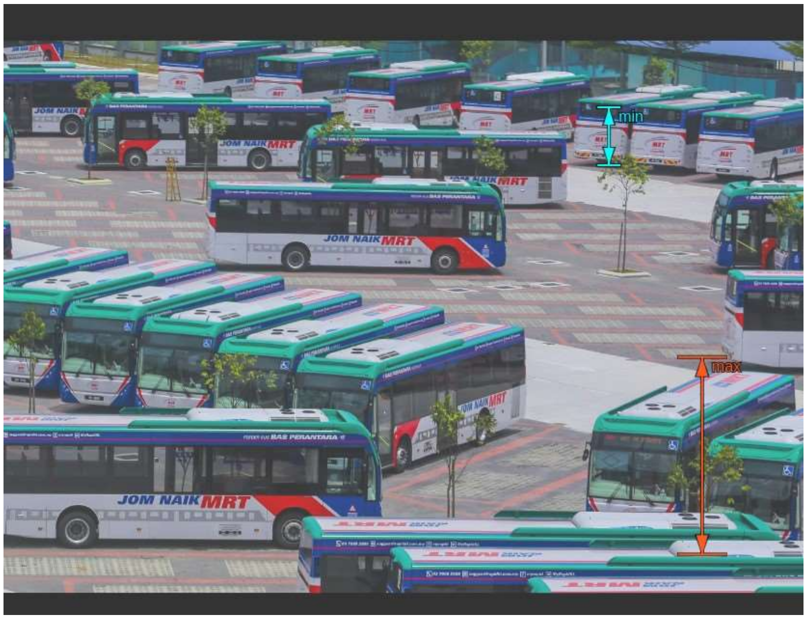
Medium (recommended)

Types of the possible detectable object.

Select at least 1 item(s).

☑ Person	□ Truck	□ Motorcycle
☑ Car	□ Bus	□ Bicycle

- **Draw Areas (ROIs)** (optional): Sometimes the alarm should be limited to a specific area of the video. If you would like to observe only a specific area, it can be determined here. Clicking this button makes the **Camera Editor** appear. Without ROIs, the entire area will be observed.



- **Set object size** (optional): If you have a good idea of what pixel range the detected objects would fall into, you can customise the minimum and maximum height size of detections, in pixels, here. This would ensure that only objects that fit into that range would get detected, resulting in a further decrease in the number of false alarms.

  Move the the arrows by clicking and dragging them to help you determine the optimal values. Adjust the slider's endpoints on the bottom part of the screen to set the minimum / maximum values. Click **Set sizes** to save your changes, or **Discard** to cancel them.

  NOTE: Take care that any object below or above the set range will NOT be detected, possibly resulting in missing incidents. It is good practice to set the minimum size slightly below, and the maximum size slightly above the desired amount.

  For example: If using U-Alarm with a combination of radar and PTZ cameras, setting custom object sizes would result in detections *only* if the radar have detected movement - since setting the proper minimum size would rule out random noise causing false detections.

- **Sensitivity**: The sensitivity of the detector can be fine tuned here. Lowering the sensitivity causes less false detections but decreases accuracy. Increasing it results in more alarms but may cause more false detections as well. The default sensitivity is *Medium*.

- **Object types**: Choose any number of object types from this list. Click *Clear all* to reset your selections. Please select at least 1 category.

6. **Cooldown**: After an alarm is triggered, it won't be triggered again for the specified duration.

7. **HTTP Client configuration (optional)**:

Use this feature to send triggered events to a third-party software with an optional snapshot image of the incident attached. It is also possible to include an *End of Event* timestamp, which triggers if 5 seconds have passed without incidents after the initial event that triggered the HTTP message. *End of Event* occurs once the incident is over.

The following information should be provided by the third-party software's administrator:

- **Enable HTTP client**: Enables / disables event sending.
- **Target URL**: The location of the API.
- **Header key and value**: Key and value of custom HTTP header. Click the **Add** button to add more Keys. To delete a Key, press the **Trash** icon next to it.
- **Trust all certificates**: If enabled, HTTPS certification errors will be ignored.

NOTE: Custom CA certificates can be uploaded in the Trusted Certificates setting.

- **Enable snapshot attach**: Off by default, only turn snapshot sending on if explicitly required. See the Snapshot part of the guide for its properties.
- **Send end of intrusion event**: Enables / disables *End of Event* sending. Note that the *Cooldown* setting of the Alarm has no effect on this.

End of Event records are sent as part of HTTP messages. They are not available in Milestone XProtect or in e-mail format.

Test Event: To test your integration, click the *Send Test Event* button **after the HTTP client settings are set.**

8. **Email notification configuration** (optional):

   This feature allows you to send alarms via e-mail to designated recipients.

   IMPORTANT: Make sure that sender e-mail settings are already set! See the Sender configuration section for instructions.

9. Click the **Submit** button to save your settings.

New Multi Object Detection

To add a **Multi Object Detection** alarm, follow the steps as laid out in New Intrusion Detection.

Compared to Intrusion Detection, you can detect 3 more types of objects (train, boat, airplane) with this feature.

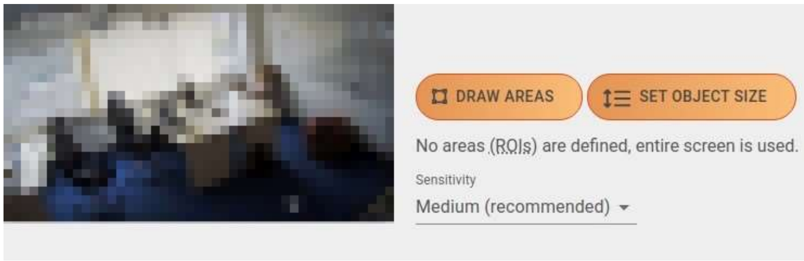
Before setting up HTTP / *End of event* message sending for Multi Object Detection alarms, consider reading the guide for third-party integration first.

New Crowd Detection

1. Choose **Crowd Detection** by clicking on its box. Fill the form, as follows:
2. **Name**: A readable name of this alarm. This name will appear in the Events view and in all notifications.
3. **Armed**: The alarm can be deactivated here. Armed by default.

4. **Schedule** (optional): You can associate one of your previously defined Schedules with this alarm.
5. **Critical number of people**: This alarm will be triggered if the sum of the people (considering all associated cameras) reaches or exceeds this number.
6. **Add Camera**: Select one or more cameras from the list.

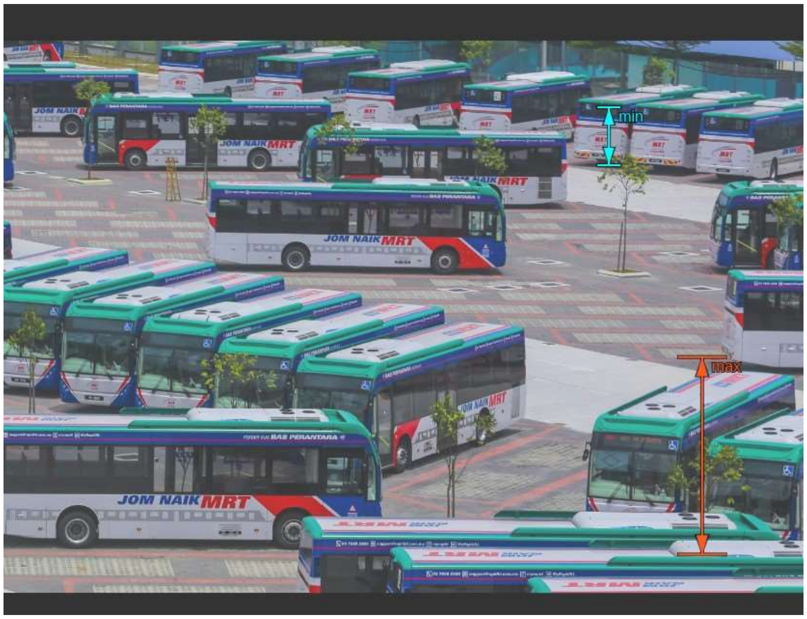
- You can add more than one camera for one Crowd Detection Alarm, since you may want to see an aggregated sum of all objects counted, spread across different cameras.
- You may also add the same camera multiple times, with different ROI and Sensitivity preferences.



No areas (ROIs) are defined, entire screen is used.

Sensitivity: Medium (recommended)

- **Draw Areas (ROIs)** (optional): Sometimes the alarm should be narrowed to a specific area of the video. If you would like to observe only a specific area, it can be determined here. Clicking this button makes the **Camera Editor** appear. Without ROIs, the entire area will be observed.



- **Set object size** (optional): If you have a good idea of what pixel range the detected objects would fall into, you can customise the minimum and maximum height size of detections, in pixels, here. This would ensure that only objects that fit into that range would get detected, resulting in a further decrease in the number of false alarms.

  Move the the arrows by clicking and dragging them to help you determine the optimal values. Adjust the slider's endpoints on the bottom part of the screen to set the minimum / maximum values. Click **Set sizes** to save your changes, or **Discard** to cancel them.

NOTE: Take care that any object below or above the set range will NOT be detected, possibly resulting in missing incidents. It is good practice to set the minimum size slightly below, and the maximum size slightly above the desired amount.

For example: If using U-Alarm with a combination of radar and PTZ cameras, setting custom object sizes would result in detections *only* if the radar have detected movement - since setting the proper minimum size would rule out random noise causing false detections.

- **Sensitivity**: The sensitivity of the detector can be fine tuned here. Lowering the sensitivity causes less false detections but decreases accuracy. Increasing it results in more alarms but may cause more false detections as well. The default sensitivity is *Medium*.

- Click **Change** to swap your previously selected camera for a different one. Click **Delete** to remove your previously selected camera.

7. **Cooldown**: After an alarm is triggered, it won't be triggered for the specified duration.

8. **HTTP Client configuration** (optional):

   Use this feature to send triggered events to a third-party software. The following information should be provided by the third-party software's administrator:

   - **Enable HTTP client**: Enables / disables event sending.
   - **Target url**: The location of the API.
   - **Header key and value**: Key and value of custom HTTP header. Click the **Add** button to add more Keys. To delete a Key, press the **Trash** icon next to it.
   - **Trust all certificates**: If enabled, HTTPS certification errors will be ignored.

NOTE: Custom CA certificates can be uploaded in the Trusted Certificates setting.

Test Event: To test your integration, click the *Send Test Event* button **after the HTTP client settings are set**.

9. **Email notification configuration** (optional):

   This feature allows you to send alarms via e-mail to designated recipients.

   IMPORTANT: Make sure that sender e-mail settings are already set! See the Sender configuration section for instructions.

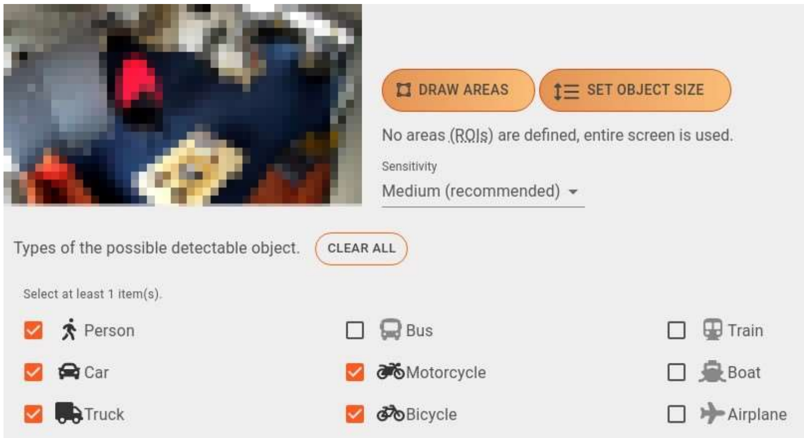
10. Click the **Submit** button to save your settings.

New Multi Object Counter

1. Scroll down to **Counters**, then choose **Multi Object Counter** by clicking on its box. Fill in the form, as follows:
2. **Name**: A readable name of the counter for easy identification in the U-alarm user interface.
3. **Armed**: The alarm can be deactivated here. Armed by default.

4. **Technical name**: A unique name that identifies your Counter in the API.
5. **Add Camera**: Select one or more cameras the counter should use from the list.

- You can add more than one camera for one counter, since you may want to see an aggregated sum of all objects counted, spread across different cameras.
- You may also add the same camera multiple times, with different ROI, Sensitivity and object type preferences.



No areas (ROIs) are defined, entire screen is used.

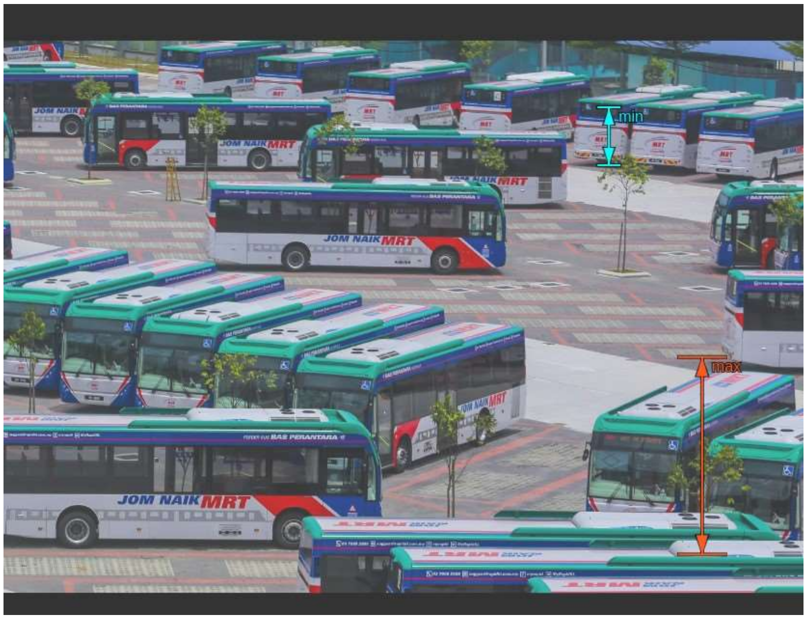
Sensitivity
Medium (recommended)

Types of the possible detectable object.

Select at least 1 item(s).

☑ Person
☑ Car
☑ Truck
☐ Bus
☑ Motorcycle
☑ Bicycle
☐ Train
☐ Boat
☐ Airplane

- **Draw Areas (ROIs)** (optional): Sometimes the counter should be limited to a specific area of the video. If you would like to observe only a specific area, it can be determined here. Clicking this button makes the **Camera Editor** appear. Without ROIs, the entire area will be observed.



- **Set object size** (optional): If you have a good idea of what pixel range the detected objects would fall into, you can customise the minimum and maximum height size of detections, in pixels, here. This would ensure that only objects that fit into that range would get detected.

Move the the arrows by clicking and dragging them to help you determine the optimal values. Adjust the slider's endpoints on the bottom part of the screen to set the minimum / maximum values. Click **Set sizes** to save your changes, or **Discard** to cancel them.

Setting the minimum size below 50 would correspond to turning the parameter known in releases older than 2.1.0 as "Long-range detections" on. Enabling this will increase the detection range but will lower the analysis period to 1/5 of a second and increase the Analysis Slot usage by one.

NOTE: Take care that any object below or above the set range will NOT be detected, possibly resulting in missing incidents. It is good practice to set the minimum size slightly below, and the maximum size slightly above the desired amount.

For example: If using U-Alarm with a combination of radar and PTZ cameras, setting custom object sizes would result in detections *only* if the radar have detected movement - since setting the proper minimum size would rule out random noise causing false detections.

- **Sensitivity**: The sensitivity of the detector can be fine tuned here. Lowering the sensitivity causes less false detections but decreases accuracy. Increasing it results in more alarms but may cause more false detections as well. The default sensitivity is *Medium*.
- **Object types**: Choose any number of object types from this list. Click *Clear all* to reset your selections. Please select at least 1 category.

6. To add the same camera to the counter, click **Clone** (optional). You may keep your settings as you set them previously, or modify the clone to your liking. Click **Change** to swap your previously selected camera for a different one. Click **Delete** to remove your previously selected camera.
7. **Aggregation frequency**: The interval between aggregating the counted objects. Default is 5 seconds.
8. Click the **Submit** button to save your camera and its clones if you added any.

To check the counter's detections inside U-Alarm, you can do so by opening the live view of the corresponding camera(s) in Cameras.

The data produced by Multi Object Counters can be accessed by third-party tools - see the Counter API section for integration instructions - as well as in U-Alarm, in the Events screen.

Edit an existing Alarm or Counter

1. On the left side of the interface, find and click the alarm or counter you would like to modify in the **Configured Alarms** list.
2. Edit your settings the same way this alarm or counter was created.
3. Click the **Save** button or press the **Revert** button to cancel your edits.

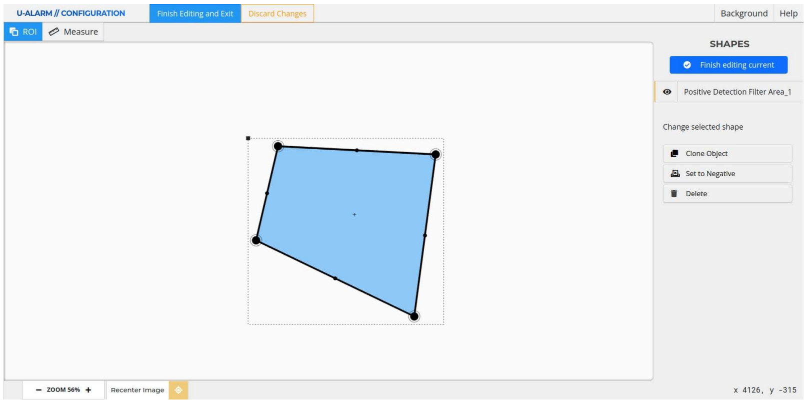
Delete an existing Alarm or Counter

1. On the left side of the interface, find and click the existing alarm or counter you would like to modify in the **Configured Alarms** list.

2. Click the **Delete** button.

Using the U-Alarm Camera Editor

(formerly the Stream Configurator)



Basic Navigation

The **scroll wheel** zooms in and out of the canvas.

Middle-mouse button + drag moves the canvas. To reset to the center of the canvas, click the **Go to Origin button.** ⌖

The following functions are available at the top of the screen:

- **Finish Editing and Exit** button to save all changes and return to the Alarm page in U-Alarm.

NOTE: This only saves the changes made in the Editor - do not forget to press **Save** at the top of the Alarm page to add your changes to the Alarm itself.

- **Discard Changes** button to cancel all changes.
- *Background*, *ROI* and *Measure* buttons to open their respective tools and windows.

Shapes panel

- The list of created Areas are available here.
- Editing options for the currently selected Area can also be found here.

Drawing a new ROI

1. Select the **ROI** tool from the top toolbar (selected by default).

2. Define an area by simply clicking on the canvas to create nodes.

   - Each step can be undone with a right-click.
   - Click on the starting point to finish drawing the area (or double-click the last point).

3. The new Positive ROI will appear in the **Shapes** list.

4. You can draw more Areas: a camera can have an unlimited number of them.

5. Click the **Finish editing current** button at the top of the Shapes panel. You can exit the Camera Editor by the **Finish Editing and Exit** button, or cancel all changes with the **Discard Changes** button.

NOTE: This only saves the changes made in the Editor - do not forget to press **Save** at the top of the Alarm page to add your changes to the Alarm itself.

Negative Areas (optional)

Negative Areas can be used when posters, billboards or other design elements contain people, causing false alarms. In a Negative Area all detections will be ignored.

1. Double click a ROI (or select it from the **Shapes** list).
2. Click the **Set to Negative** button. Clicking the button again will change the area back to positive.
3. Click the **Finish editing current** button at the top of the **Shapes** panel or click anywhere on the background to exit edit mode.
4. The Area will turn red, indicating that it is a Negative Area.

Edit an existing ROI

1. Double click a ROI (or select it from the **Shapes** list).
   - Each node of the Area can be moved by dragging them with the mouse on the canvas.
   - New nodes can be created by clicking on the mid-point of a section of the Area.
   - The entire Area can be moved by dragging the black square at the top-left corner of the bounding box.
2. Click the **Finish editing current** button at the top of the **Shapes** panel or click anywhere outside the bounds of the shape to exit the edit mode.

Delete an existing ROI

1. Double click a ROI (or select it from the **Elements** list).
2. Click the *Delete* button.

Additional Tools and Options

Background

By clicking the *Background* button, a detachable window will open, giving you the following options:

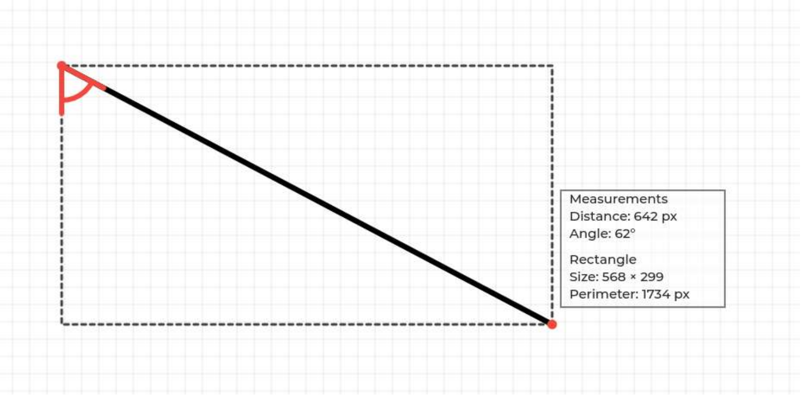
- The opacity of the background.
- Refresh the background image.
- Upload custom background image.

- Configure the background grid.

Measure

Measure

Enters into the Measuring mode. **Left click** sets the starting point and displays the distance between the starting point and the cursor location. It also calculates the size and perimeter of the rectangle where the ruler is the diagonal.


Measurements
Distance: 642 px
Angle: 62°

Rectangle
Size: 568 × 299
Perimeter: 1734 px

Next steps

You are most likely done with all mandatory settings. However, you can define Schedules for the alarms to only operate at specific times. Otherwise you can learn more about receiving Events.

Events

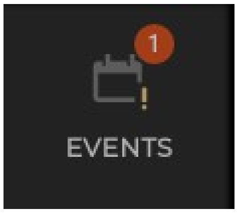
Events are incident notifications triggered by your alarms. A visualised output of your Counters can also be found here, see below for details.

Before you start

Once every Camera is registered and Alarms are created in U-Alarm (with or without a Schedule), everything is set for receiving Events.

Event notifications

U-Alarm



If U-Alarm is opened in your browser, you can see the following indications of a newly triggered Event:

- A notification badge will be displayed on the **Events** button at the left-side panel: it shows you the number of new detections since you last activated it. Clicking on it will take you to the list of recorded detections.
- A *notification bar* appears at the bottom centre of any page. The bar will not disappear until it is closed manually or the incident is investigated by clicking on the *More* link on it.
- A *Beeping sound* is played (unless the browser tab is muted).

  You can mute / unmute a browser tab by right-clicking on the tab and selecting the appropriate function.
- New detection Events are recorded in the **Events** view.

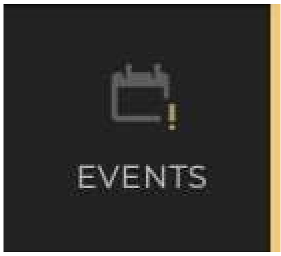
Integrated third-party software

U-Alarm Events can be sent to a third-party software where user notifications are defined by the respective software's custom implementation. Please contact the software provider to learn more about third-party notifications.

Events view

Past or recently reported incidents can be managed in the Events view.

Click the **Events** menu on the left sidebar for this view.

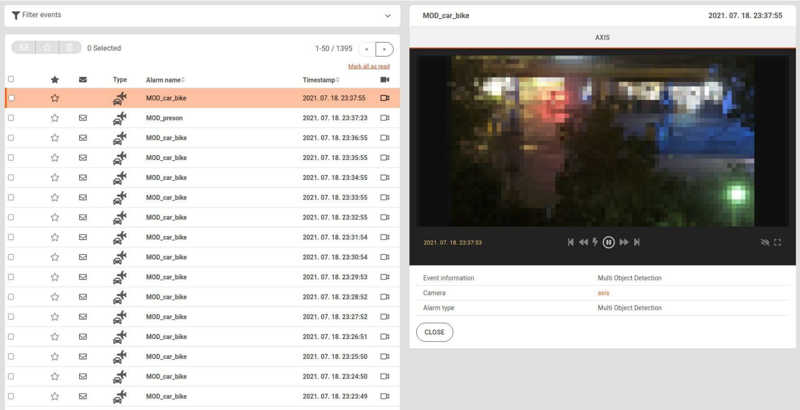


Event Replay

Triggered Events are listed in reversed time order by default. This can be changed by clicking on the respective column's header. The Alarm which triggered the event can be recognised by its name.

Click on a row in the table to replay the incident. The replay starts from a few seconds before the Event's timestamp.

The playback availability is denoted by the *Camera* icon on right side of the Event's row. If the icon is missing, the playback of that Event is still loading.



□	★	✉	Type	Alarm name	Timestamp	📹
□	☆			MOD_car_bike	2021. 07. 18. 23:37:55	📹
□	☆	✉		MOD_preson	2021. 07. 18. 23:37:23	📹
□	☆	✉		MOD_car_bike	2021. 07. 18. 23:36:55	📹
□	☆	✉		MOD_car_bike	2021. 07. 18. 23:35:55	📹
□	☆	✉		MOD_car_bike	2021. 07. 18. 23:34:55	📹
□	☆	✉		MOD_car_bike	2021. 07. 18. 23:33:55	📹
□	☆	✉		MOD_car_bike	2021. 07. 18. 23:32:55	📹
□	☆	✉		MOD_car_bike	2021. 07. 18. 23:31:54	📹
□	☆	✉		MOD_car_bike	2021. 07. 18. 23:30:54	📹
□	☆	✉		MOD_car_bike	2021. 07. 18. 23:29:53	📹
□	☆	✉		MOD_car_bike	2021. 07. 18. 23:28:52	📹
□	☆	✉		MOD_car_bike	2021. 07. 18. 23:27:52	📹
□	☆	✉		MOD_car_bike	2021. 07. 18. 23:26:51	📹
□	☆	✉		MOD_car_bike	2021. 07. 18. 23:25:50	📹
□	☆	✉		MOD_car_bike	2021. 07. 18. 23:24:50	📹
□	☆	✉		MOD_car_bike	2021. 07. 18. 23:23:49	📹

MOD_car_bike 2021. 07. 18. 23:37:55

2021. 07. 18. 23:37:53

Event information	Multi Object Detection
Camera	axis
Alarm type	Multi Object Detection

Display features

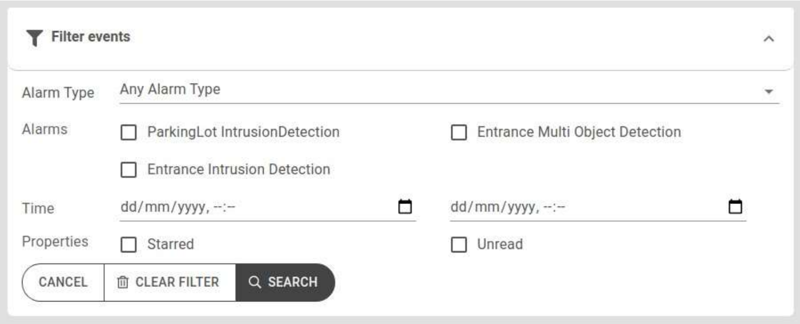
- If a ROI is associated with an alarm, the ROI is displayed as a dashed *green* polygon. Negative ROI are displayed as dashed *red* polygons.
- Detections are displayed as *orange* / *aqua* rectangles for people / vehicles, respectively.
- At the triggering moment, a *Bell* icon will appear in the top right corner of the player.
- The *timestamp* of the video is at the bottom left of the player (can be different from the one that comes from the camera) in the time zone of the device. The time zone can be modified in the Control Panel.

Note: If multiple cameras are linked to the triggering Alarm, there might be no activity in the record of some of these cameras. In this case, the Event was triggered by the activity of different cameras.

Controls

- || and > toggles between pause and play
- `Flash` button jumps to the triggering moment and pauses the player
- **|<** button rewinds to a few seconds before the Event
- **>|** button switches to live play
- **<<** button jumps backward ten seconds
- **>>** button jumps forward ten seconds
- The *Eye* button shows / hides annotations
- You can go to full screen play with the *Rectangle* button in the lower right corner of the player

Filter Events


Filter events

Alarm Type: Any Alarm Type

Alarms: □ ParkingLot IntrusionDetection □ Entrance Multi Object Detection □ Entrance Intrusion Detection

Time: dd/mm/yyyy, --:-- dd/mm/yyyy, --:--

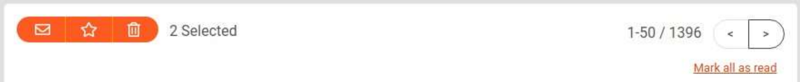
Properties: □ Starred □ Unread

You can filter what type of Events to display by clicking on the **Filter events** drop-down menu and ticking the respective checkbox. You can filter Events by:

- Detection type (Intrusion-, Multi Object- and Crowd Detection or 'Any' alarm type)
- Alarms, set up by the user, as described in Alarms
- The time frame the detections were triggered within
- Starred or Unread status

Note: You can also identify an Event's detection type by its icon in the Event list.

You can select and mark specific or all displayed Events as *Starred*, toggle their *Read/Unread* status, or delete them.



Tick the checkboxes of the respective Events, or tick the checkbox at the top left corner of the Event list to select or deselect all currently displayed Events. You may change their status by clicking the three orange icons (shown above). Alternatively, to mark an Event as *Starred* or toggle their *Read/Unread* status, click the corresponding icon on the Event's row.

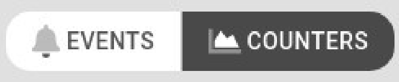
Counters

Counters are designed with third-party solutions in mind, however, their output can be accessed within U-Alarm as well, in the Events screen.

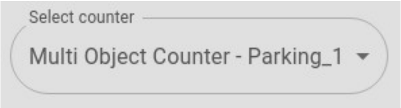
Before you start

Once every Camera is registered and Counters are created in U-Alarm, everything is set for viewing their output here.

- Click the **Events/Counters** button at the top right corner of the Events screen.



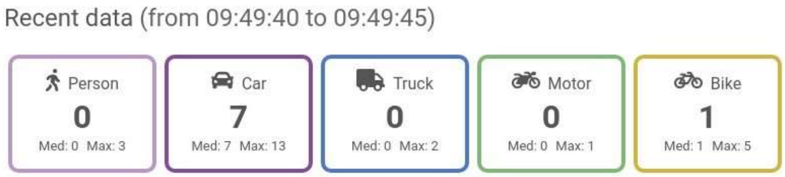
- Select the counter from the drop-down list on the upper left corner of the Events screen.



Select counter

Multi Object Counter - Parking_1

Recent data

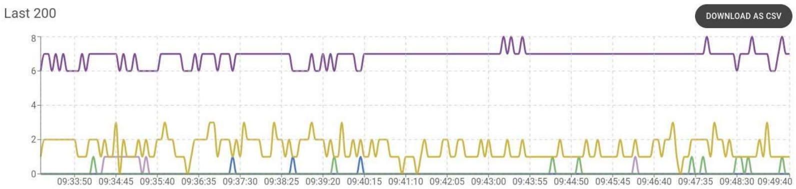


Recent data (from 09:49:40 to 09:49:45)

Person	Car	Truck	Motor	Bike
0	7	0	0	1
Med: 0 Max: 3	Med: 7 Max: 13	Med: 0 Max: 2	Med: 0 Max: 1	Med: 1 Max: 5

The rectangle(s) show you the last, median and maximum number of detections that occurred in the last aggregation interval, of each object type associated with the Counter. They are a good way to read the Counter's data at a glance.

Counter chart and table



Consulting the line chart gives you a bird's eye view of the observed area's detection trends for the last 200 observations.

Below, a table view is also available, showing the following data in an object-by-object basis: the first and last detections, as well as the median, average, minimum and maximum number of detections within each aggregation interval.

Aggregation frequency

The aggregation frequency for the Counter determines the time interval between each counting. It is 5 seconds by default, and can be adjusted in the Alarms screen. This setting applies to all three views as well as to the downloadable `.csv` file.

Note: The last 200 detections will be shown at all times, regardless of the time interval set between them - which means the time covered by the Recent data, chart and table can range from a few minutes to several hours, depending on the interval set.

You can download the Counter's data is `.csv` format, by clicking the **Download as csv** button in the top right of the chart. You can set a time interval here, for up to three days.

Troubleshooting

- I am not receiving any events from my Alarms.
  - Check your Alarm settings and try changing the Sensitivity of the detector to *Medium* or *High*.
- I am receiving false detections from my Alarms.

- Check your Alarm settings and try lowering the Sensitivity of the detector. You may also draw *Regions of Interest* to exclude areas/only include certain ones to run the detections on.

Control Panel

This is the place for under the hood settings in U-Alarm.

Click the **Control Panel** menu on the left sidebar for this view.

General

User

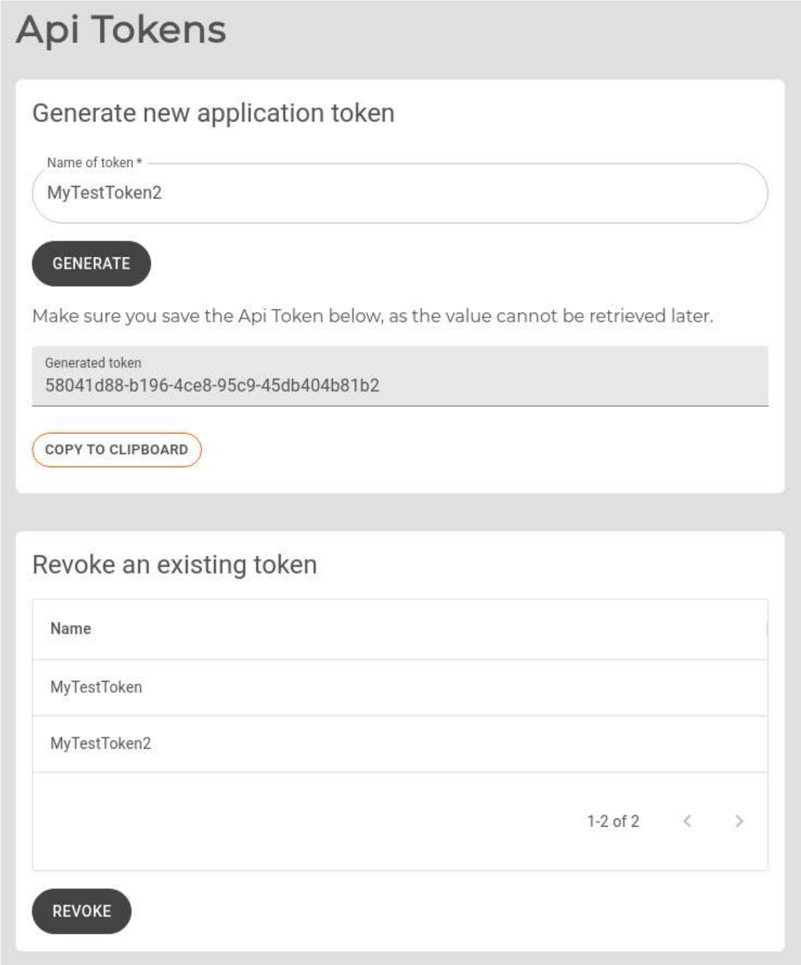
You can change your password here.

Licence

Online and offline licence activation and licence info.

API Tokens

Token-based authentication is possible to provide access to certain API-s, for third-party integration purposes. Tokens can be generated or revoked here.



Api Tokens

Generate new application token

Name of token *: MyTestToken2

Make sure you save the Api Token below, as the value cannot be retrieved later.

Generated token: 58041d88-b196-4ce8-95c9-45db404b81b2

Revoke an existing token

Name
MyTestToken
MyTestToken2

1-2 of 2

To create a new token, give it a name that is easily identify by, then press *Generate*. You may remove your tokens by selecting them from the list below, then pressing *Revoke*.

Make sure to save or copy your token immediately after generating it, as they cannot be retrieved after you navigate away from this page.

API tokens can be used for the following services:

- Status of U-Alarm
- Counter API

Schedule

Create and assign Schedules to your alarms to make them active only in a given time period.

System

Network

If there is a DHCP server in your network the IP of the U-Alarm device will be set automatically. However, it is possible to set the network properties manually here.

Grant SSH access

This feature allows Ultinous Support to access the U-Alarm box remotely, via **SSH**. It should only be used in the very rare case of an issue unsolvable by other means. Off by default, SSH access **must only be turned on when explicitly asked by Ultinous Support**.

E-mail

U-Alarm can be configured to send alarms via e-mail to multiple given recipients. See the Alarms via E-mail section for instructions.

SSL

U-Alarm supports SSL/TLS to protect data between your browser and the box itself. See the SSL Settings section for instructions.

SNMP

U-Alarm can be monitored by standard monitoring tools. See the SNMP Settings section for instructions.

U-Alarm is also capable of exposing certain metrics through its HTTP API.

Trusted certificates

Additional trusted CA certificates can be uploaded here. See the Trusted Certificates section for instructions.

Time

Schedules and timestamps on the video player are managed and displayed in this Time zone. This is a global setting for the entire system therefore it is recommended to set it to the physical location of the cameras.

For precise time synchronisation U-Alarm uses a remote default NTP server. If your U-Alarm device has no internet access it is recommended to set a custom NTP server available on the local network.

Maintenance

Reload & Restart

In case you would like to refresh your alarms and cameras - for troubleshooting purposes, for instance - it is possible to do that by pressing the **Reload** button.

To restart your device, press the **Restart** button. Take note that the device may need a few minutes to completely boot up again.

Backup & Restore

Once U-Alarm is fully configured, it is possible to *export this configuration*. If a U-Alarm device is replaced or its software is updated or reinstalled, the previously exported configuration file can be loaded, avoiding the need of a manual reconfiguration.

Factory reset is also available here. Please note that a full reboot process can take up to 3 minutes.

For troubleshooting purposes, a *status report* containing full diagnostic information about your system can be downloaded from here.

System Health

The data here provides you with information about your U-Alarm box's and your cameras' current working status.

System Update

U-Alarm firmware can be upgraded to a higher version. See the System Update section for instructions.

About

U-Alarm version information.

Expert Settings

Settings for advanced features that are hidden by default. To access them, click the **Expert Settings** button, then click "*I Accept*" on the pop-up.

NOTE: Make sure to have a clear understanding of the features here and their impact on your system before continuing! Consult support@ultinous.com, if necessary.

Sensitivity

Each Alarm's associated Camera can be customised to have a Sensitivity value from Very Low to Very High. The exact values of these Sensitivity parameters can be fine-tuned here.

The settings are in `.json` format, containing each object type's respective Sensitivity values (grouped by Alarm type, since each Alarm could have different Sensitivity thresholds for their objects), ranging from - from top to bottom - Very Low to Very High. Accepted values range from 0.1 to 1.

```
"INTRUSION_DETECTION": {
    "PERSON": [
      0.82,  "Very Low"
      0.685, "Low"
      0.56,  "Medium"
      0.51,  "High"
      0.48   "Very High"
    ]
```

Note that since these values represent the minimum threshold above which detections are accepted, **the higher the value, the fewer detections are observed and the fewer Events are generated**, and vica versa.

The settings are being validated as you type. To cancel editing, click **Undo changes**, or **Reset defaults**. Otherwise, press **Save** to commit your changes.

Online help

Links to external pages:

- Documentation
- Support
- General terms and Conditions
- U-Alarm webpage

Further reading

If you would like to learn more about U-Alarm, please visit the User's guide.

Schedule

Ideally, alarms should operate only in a specific period of the day. With this feature, you can add a weekly schedule for any alarm. You can also add exceptions for special occasions, like holidays.

Schedules may not be assigned to Counters.

Schedule settings are available in the Control Panel.

Before you start

Please make sure that :

- the Time zone is correctly configured in the Control Panel.
- the Alarms which require scheduling are created and active.

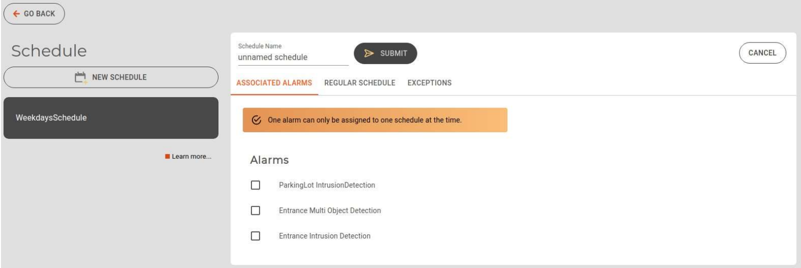
Create a new Schedule

1. In the Control Panel, click the **Schedule** button.

2. Click the **New Schedule** button.

3. Add a name to the new Schedule.

4. On the **Associated Alarms** tab select the Alarms which will be scheduled by this configuration. One alarm can only be assigned to one schedule at a time.



Schedule Name: unnamed schedule

One alarm can only be assigned to one schedule at the time.

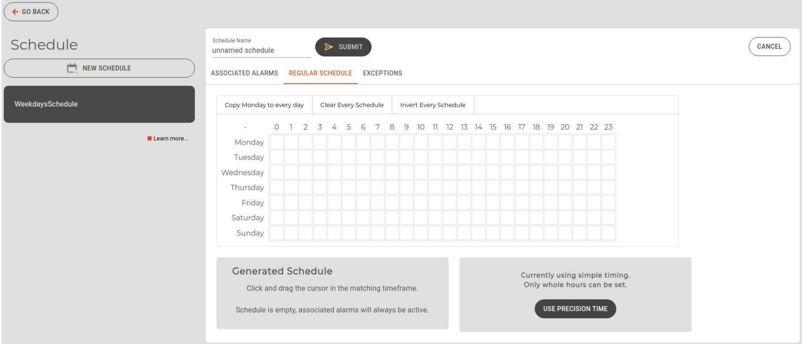
Alarms

☐ ParkingLot IntrusionDetection

☐ Entrance Multi Object Detection

☐ Entrance Intrusion Detection

5. Click the **Regular Schedule** tab.



Schedule Name: unnamed schedule

Generated Schedule

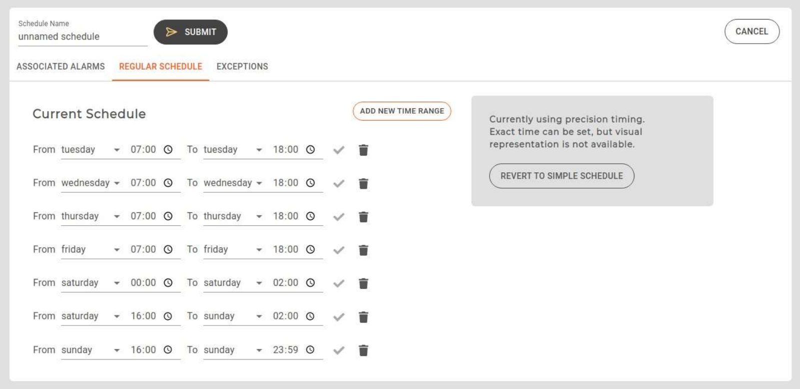
Click and drag the cursor in the matching timeframe.

Schedule is empty, associated alarms will always be active.

Currently using simple timing.
Only whole hours can be set.

6. Select the operation time of the associated Alarms with clicking and dragging the mouse cursor. Fine tune the selection with mouse clicks.

Optional: For precise time adjustment, click the **Use Precision Time** button.



Schedule Name
unnamed schedule

Current Schedule

From tuesday 07:00 To tuesday 18:00
From wednesday 07:00 To wednesday 18:00
From thursday 07:00 To thursday 18:00
From friday 07:00 To friday 18:00
From saturday 00:00 To saturday 02:00
From saturday 16:00 To sunday 02:00
From sunday 16:00 To sunday 23:59

Currently using precision timing. Exact time can be set, but visual representation is not available.

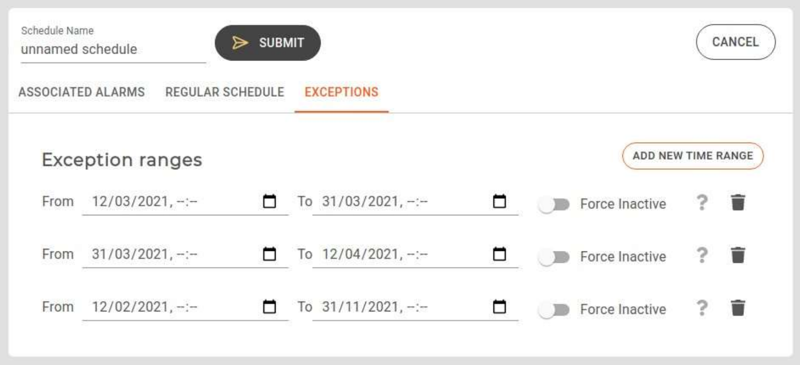
- Click the **Add New Time Range** button for a new period of time.
- Set the appropriate range.

Note: A Time Range's *From* value should not be later than the *To* value. An error symbol will indicate this problem.

- Delete a Time Range by clicking the *Trash* button.
- You can always go back to hourly precision by clicking the **Revert to Simple Schedule** button, however all Precision Time settings will be lost.

7. Optional: Add exceptions by clicking on the **Exceptions** tab.

   - Click the **Add New Time Range** button for a new exception.
   - Set the start and end dates. The start date should precede the end date. An error symbol will indicate this problem.
   - Set whether the Alarm should be forced to *Active* or *Inactive* regardless of the Regular Schedule. You cannot set *Active* and *Inactive* values for the same duration. An error symbol will indicate this problem.
   - Delete a Time Range by clicking the *Trash* button.



Schedule Name
unnamed schedule

Exception ranges

From 12/03/2021, --:-- To 31/03/2021, --:-- Force Inactive ?
From 31/03/2021, --:-- To 12/04/2021, --:-- Force Inactive ?
From 12/02/2021, --:-- To 31/11/2021, --:-- Force Inactive ?

8. Click the **Submit** button.

Edit an existing schedule

1. Select an existing **Schedule** by clicking its name from the **Schedules** list.

2. Make your modifications the same way as in Schedule creation.
3. Click the **Save** button.

Delete an existing schedule

1. Select an existing **Schedule** by clicking its name from the **Schedules** list.
2. Click the **Delete** button.

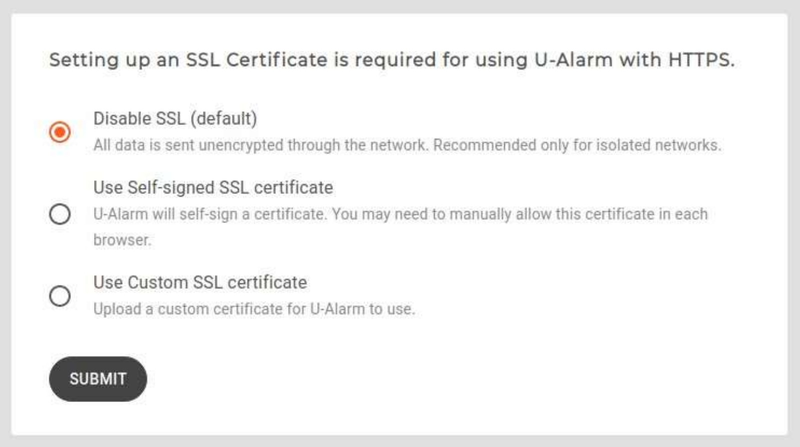
Next Steps

Everything is set and U-Alarm is ready to receive Events.

SSL settings

SSL Settings are available in the Control Panel.

U-Alarm supports SSL/TLS to protect data between your browser and the box itself. It is not enabled by default, but can be turned on here.



Setting up an SSL Certificate is required for using U-Alarm with HTTPS.

● Disable SSL (default)
All data is sent unencrypted through the network. Recommended only for isolated networks.

○ Use Self-signed SSL certificate
U-Alarm will self-sign a certificate. You may need to manually allow this certificate in each browser.

○ Use Custom SSL certificate
Upload a custom certificate for U-Alarm to use.

There are two options besides turning SSL off.

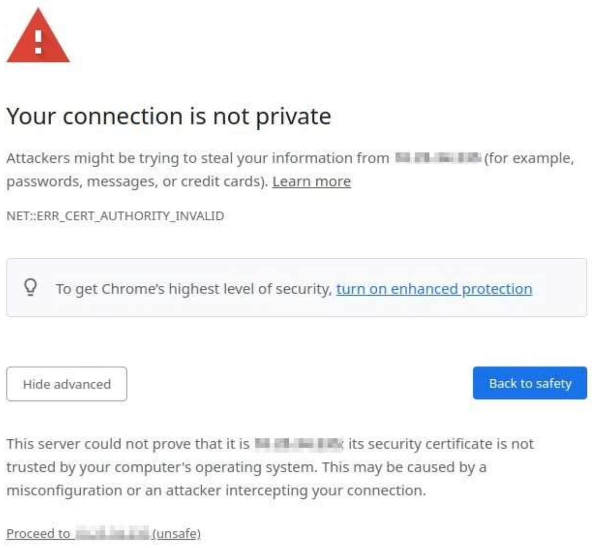
Self-signed SSL certificate

You can set a self-signed certificate in the matter of seconds:

Enter the name that should be in the certificate. In most cases, it is the same name you enter in the browser address bar (without the http:// prefix). IP address is allowed as well. The self-signed certificate will ensure that the data is transmitted between the browser and the U-Alarm box encrypted. However, it can not prevent all kinds of attacks (man-in-the-middle).

When a self-signed certificate is set, the browsers will show a warning that the certificate is not trusted as it was issued by the box itself, not a trusted 3rd party Certificate Authority - this can safely be ignored in this case.

Using Google Chrome, click **Proceed to...** on the bottom of the page:



Your connection is not private

Attackers might be trying to steal your information from [redacted] (for example, passwords, messages, or credit cards). Learn more

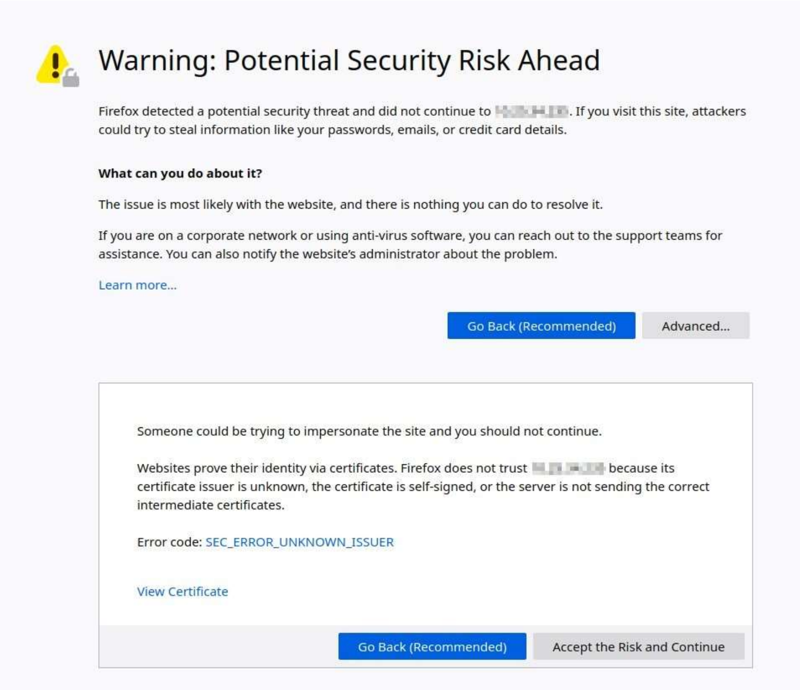
NET::ERR_CERT_AUTHORITY_INVALID

To get Chrome's highest level of security, turn on enhanced protection

This server could not prove that it is [redacted] its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection.

Proceed to [redacted] (unsafe)

On Firefox, click **Advanced**, then **Accept the Risk and Continue**:



Warning: Potential Security Risk Ahead

Firefox detected a potential security threat and did not continue to [redacted]. If you visit this site, attackers could try to steal information like your passwords, emails, or credit card details.

What can you do about it?

The issue is most likely with the website, and there is nothing you can do to resolve it.

If you are on a corporate network or using anti-virus software, you can reach out to the support teams for assistance. You can also notify the website's administrator about the problem.

Learn more...

Someone could be trying to impersonate the site and you should not continue.

Websites prove their identity via certificates. Firefox does not trust [redacted] because its certificate issuer is unknown, the certificate is self-signed, or the server is not sending the correct intermediate certificates.

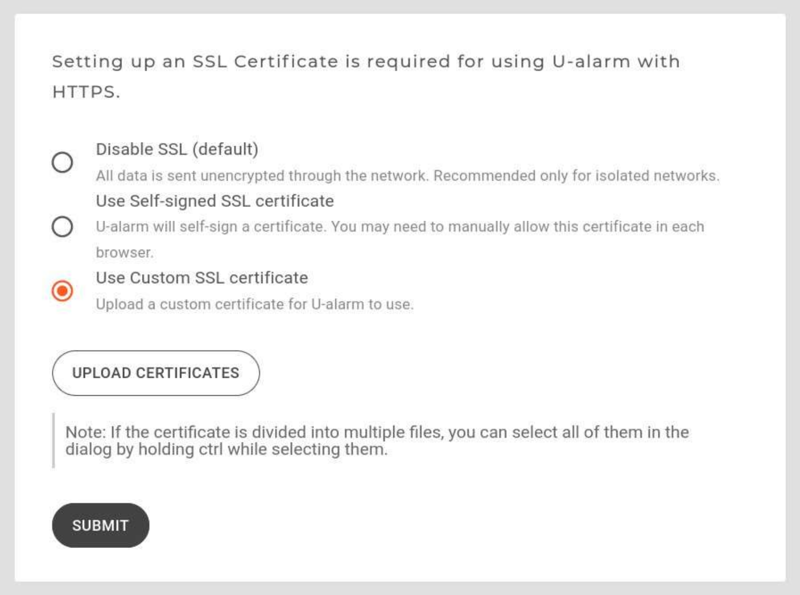
Error code: SEC_ERROR_UNKNOWN_ISSUER

View Certificate

Depending on the browser, the certificate can be added permanently, or temporarily for that session.

Custom SSL certificate

When a custom certificate is desired, you have the option to upload it along with the private key.



Setting up an SSL Certificate is required for using U-alarm with HTTPS.

○ Disable SSL (default)
All data is sent unencrypted through the network. Recommended only for isolated networks.

○ Use Self-signed SSL certificate
U-alarm will self-sign a certificate. You may need to manually allow this certificate in each browser.

● Use Custom SSL certificate
Upload a custom certificate for U-alarm to use.

Note: If the certificate is divided into multiple files, you can select all of them in the dialog by holding ctrl while selecting them.

A wide range of formats are supported - see the list below.

The workflow highly depends on your organization and your Certificate Authority (CA). The general steps are usually the following: you generate a keypair, a certificate request, you send your request to the CA of your choice, you prove the ownership of the domain name to the CA, the CA issues you a certificate that you can upload to the U-Alarm along with the generated key. Some enterprises have their CA in-house for their systems, others use trusted public CAs.

CAs generally have their own documentation on how to proceed, usually something like this (assuming U-Alarm is reached via U-Alarm.example.com and the openssl utility is available):

```
$ openssl req -new -newkey rsa:2048 -nodes -keyout U-Alarm.example.com.key -
out U-Alarm.example.com.csr
Generating a RSA private key
................................+++++
.............................................................................
+++++
writing new private key to 'U-Alarm.example.com.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
```

```
-----
Country Name (2 letter code) [AU]:HU
State or Province Name (full name) [Some-State]:Budapest
Locality Name (eg, city) []:Budapest
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Example company
Organizational Unit Name (eg, section) []:System administrators
Common Name (e.g. server FQDN or YOUR name) []:U-Alarm.example.com
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
```

The U-Alarm.example.com.csr file is then uploaded to the CA's website, after which they send a verification e-mail to admin@example.com. Finally the certificate will be sent. Some CA allows you to choose format, or destination system type - in this case it is recommended to choose PEM format, or choose Apache or Nginx webserver. Along with the certificate, they usually send the certification chain. You can upload the certificate chain either concatenated to your certificate or as a separate file(s).

PKCS12 formatted files (usually with the extensions of .pfx or p12; mostly used by Windows servers) are not supported. They can however be converted to separate cert and key files using the openssl utility.

On Linux, this can easily be done with:

```
openssl pkcs12 -in example.p12 -nokeys |   sed -ne '/-BEGIN CERTIFICATE-/,/-
END CERTIFICATE-/p' > example.cert.with.chain.pem
openssl pkcs12 -in example.p12 -nocerts -nodes | openssl pkcs8 -nocrypt -out
example.key.pem
```

- Accepted key types: RSA, ECC
- RSA keys can be either in PKCS1 or PKCS8 DER or PEM format
- ECC keys are only accepted in PKCS8 format

PEM files start with â€œ-----BEGIN PRIVATE KEY-----â€? or their binary DER equivalent. Legacy openssl format (â€œ-----BEGIN EC PRIVATE KEY-----)â€? is not supported.

To convert legacy openssl keys to pkcs8, use the following command:

```
$ openssl pkcs8 -in ec.openssl.key.pem -topk8 -nocrypt -out ec.pkcs8.key.pem
```

Supported curves are the SECG, NIST, X9.62 and RFC 5639 (brainpool) curves. Tested with prime192v1 (also known as, secp192r1 or P-192), secp384r1 (P-384), c2pnb163v1, brainpoolP512r1.

Certificates can be DER or PEM encoded (usually .crt, .cer or .pem), while the certificate chain can be concatenated to the certificate itself or as separate files. File and certificate order is not significant, the system will order it. Only one end certificate can be uploaded, the other certificates must be for the chain. The chain cannot contain missing links.

SNMP settings

SNMP Settings are available in the Control Panel.

Besides third-party tools, it is also possible to utilise U-Alarm's HTTP API functionality for monitoring. To learn more, see the Status via HTTP section of the documentation.

U-Alarm can be monitored by standard monitoring tools like Nagios, Zabbix, LibreNMS etc. using Simple Network Monitoring Protocol (SNMP). Only read only queries are supported via SNMPv1 or v2c.

Note: The **Allowed Networks** field only accepts IP addresses, for example:

192.168.0.1/24

The following subtrees are supported:

- SNMPv2-MIB::system (.1.3.6.1.2.1.1)
- SNMPv2-MIB::hrSystemUptime (.1.3.6.1.2.1.25.1)
- SNMPv2-MIB::hrStorage (.1.3.6.1.2.1.25.2)
- SNMPv2-MIB::hrProcessorTable (.1.3.6.1.2.1.25.3.3)
- UCD-SNMP-MIB::memory (.1.3.6.1.4.1.2021.4)
- UCD-SNMP-MIB::laTable (.1.3.6.1.4.1.2021.10)
- UCD-SNMP-MIB::systemStats (.1.3.6.1.4.1.2021.11)
- ULTI-UALARM-MIB (.1.3.6.1.4.1.57090.1.1)

With the exception of the last subtree, these are well supported by monitoring tools, often auto-discovered or templates are offered.

Currently, the following attributes are available from ULTI-UALARM-MIB (.1.3.6.1.4.1.57090.1.1):

Name	Type	Sub-oid
Overall healthiness of the software components	INTEGER enumeration (OK=1, ERROR=2)	1.1.0
Textual low level error message from the system	UTF-8 string	1.2.0
Avarage GPU usage	INTEGER	1.3.0
Video storage space, free space	INTEGER MIB	1.4.1.0
Video storage space, total size	INTEGER MIB	1.4.2.0
Video storage space, used percentage	INTEGER MIB	1.4.3.0
Number of configured cameras	INTEGER	1.5.0

Detailed camera info table (.1.3.6.1.4.1.57090.1.1.1.1000.1):

Name	Type	Sub-oid
Camera index	INTEGER	1.<CAMERA_INDEX>.1
Technical name of camera	UTF-8 string	1.<CAMERA_INDEX>.2
Display name of camera	UTF-8 string	1.<CAMERA_INDEX>.3
Problem description of camera	UTF-8 string	1.<CAMERA_INDEX>.4
Healthiness of camera	INTEGER enumeration (OK=1, ERROR=2)	1.<CAMERA_INDEX>.5

Assuming that there are at least 3 cameras, the 3rd camera's healthiness can be queried on the .1.3.6.1.4.1.57090.1.1.1.1000.1.1.3.5 oid. SNMP walk is supported, so monitoring tools can auto-generate their configuration dynamically.

Should your monitoring system require it, the MIB can be downloaded from:
https://assets.ultinous.com/u-alarm/support/UALARM-MIB.txt

A Zabbix template is available at: https://assets.ultinous.com/u-alarm/support/zbx_ultinous_ualarm_templates.xml

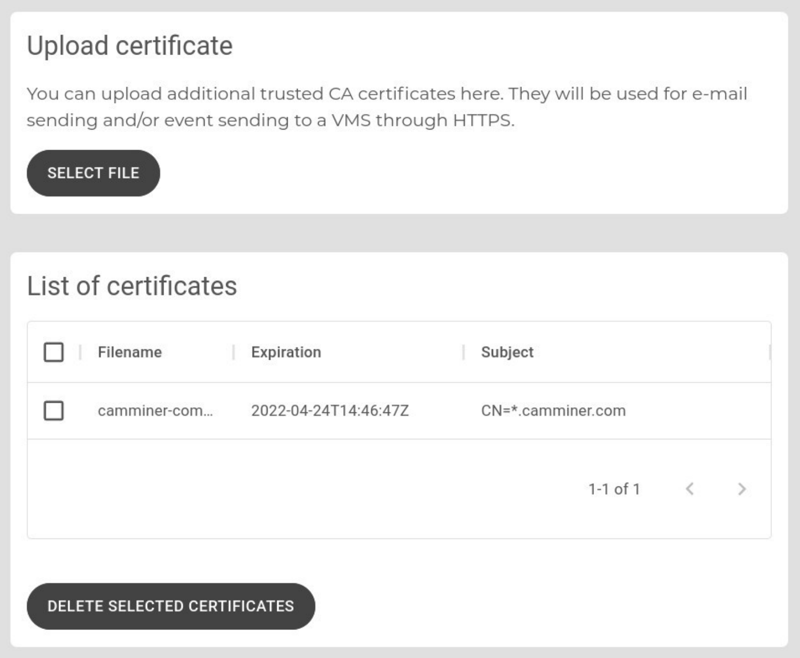
It is created and tested on Zabbix 5.0 and depends on the following external templates:
https://share.zabbix.com/network_devices/generic/ucd-snmp-mib-memory-monitoring
https://share.zabbix.com/network_devices/generic/ucd-snmp-mib-load-average-monitoring

For other monitoring systems, refer to their manual about adding custom oid.

Trusted Certificates

Trusted Certificates are available in the Control Panel.

Here you can upload additional trusted CA certificates that are needed in case you use your own PKI infrastructure. They are used to validate SMTP server certificates and alert notification hooks - should they use SSL.



Upload certificate

You can upload additional trusted CA certificates here. They will be used for e-mail sending and/or event sending to a VMS through HTTPS.

SELECT FILE

List of certificates

□	Filename	Expiration	Subject
□	camminer-com...	2022-04-24T14:46:47Z	CN=*.camminer.com

1-1 of 1 ‹ ›

DELETE SELECTED CERTIFICATES

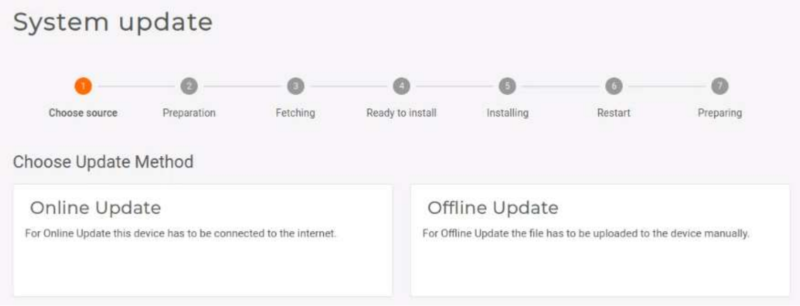
CA certificates in the Mozilla CA list (i.e Firefox) and Linux distributions' default trusted CA lists are trusted by default and are not listed here. Only CA certificates that have the Basic Constraint: ca = true flag set can be uploaded, therefore end certificates are not accepted, with the exception of self-signed certificates.

Required format is X.509 certificate in PEM or DER format. Usually they have the extension of .crt, .cert, .cer, .pem. The PEM encoded file starts with â€œ-----BEGIN CERTIFICATE-----â€?.

System Update

System Update is available in the Control Panel. Both Online and Offline updates are supported. Please choose the update source in the first step.

NOTE: If there was an update before, a Cleanup might be required to update U-Alarm again.



System update

Choose Update Method

Online Update

For Online Update this device has to be connected to the internet.

Offline Update

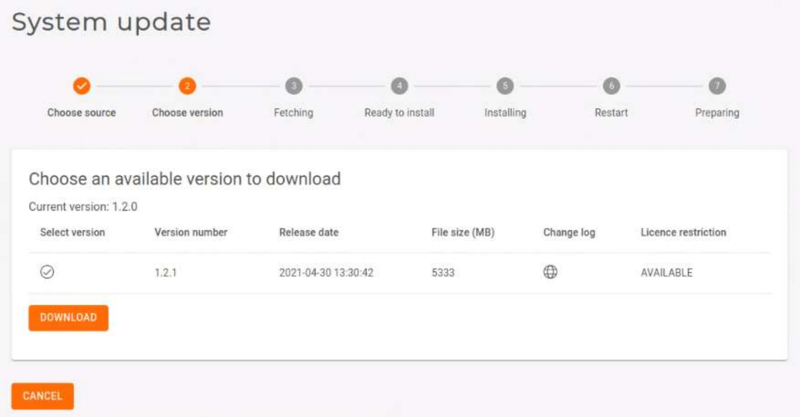
For Offline Update the file has to be uploaded to the device manually.

IMPORTANT: System Update is a long process depending on your bandwidth. Once the installation step is started, U-Alarm will not operate at all until the update is finished or aborted.

Online update

1. Make sure that the U-Alarm device has an internet connection. Select **Online Update**.

2. Select an available version by clicking its checkbox. Click the **Download** button.



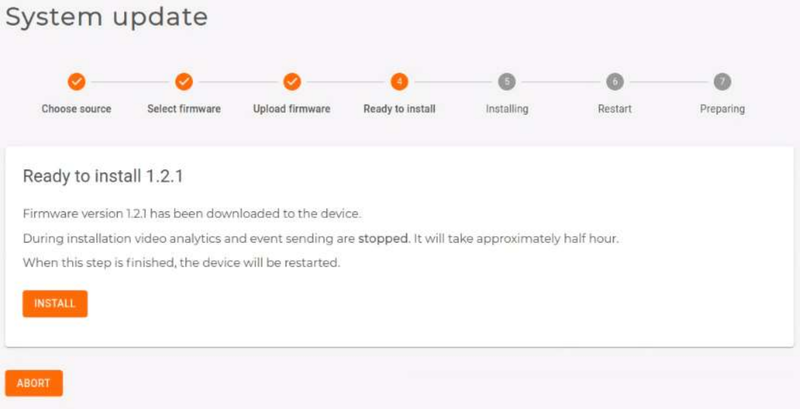
Choose an available version to download

Current version: 1.2.0

Select version	Version number	Release date	File size (MB)	Change log	Licence restriction
✓	1.2.1	2021-04-30 13:30:42	5333	🌐	AVAILABLE

3. Please wait until the download is finished.

4. Ready to Install. Press the **Install** button. From this point on, all U-Alarm services will be unavailable until the update is finished. Depending on your network speed, **this process can take up to 30 minutes**, meanwhile U-Alarm will go through the *Installing*, *Restart* and *Preparing* steps automatically during the installation.

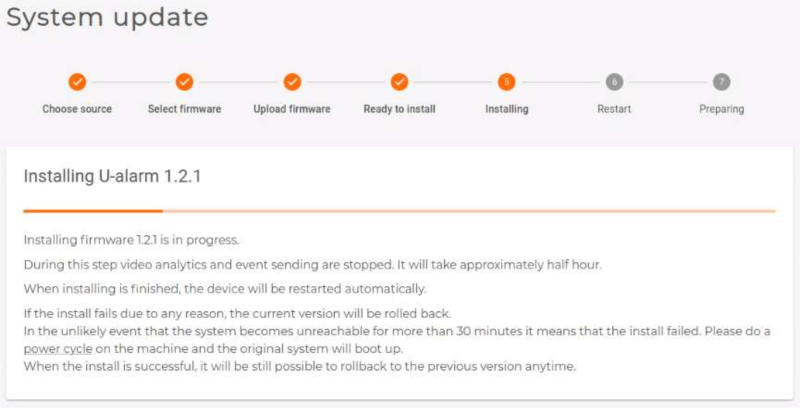


Ready to install 1.2.1

Firmware version 1.2.1 has been downloaded to the device.

During installation video analytics and event sending are **stopped**. It will take approximately half hour.

When this step is finished, the device will be restarted.



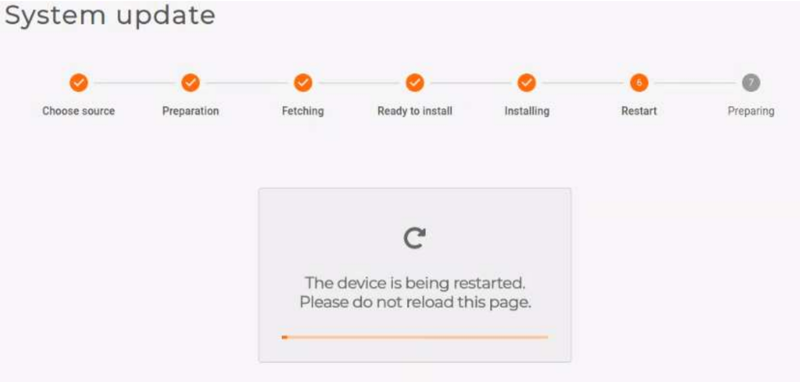
Installing U-alarm 1.2.1

Installing firmware 1.2.1 is in progress.

During this step video analytics and event sending are stopped. It will take approximately half hour.

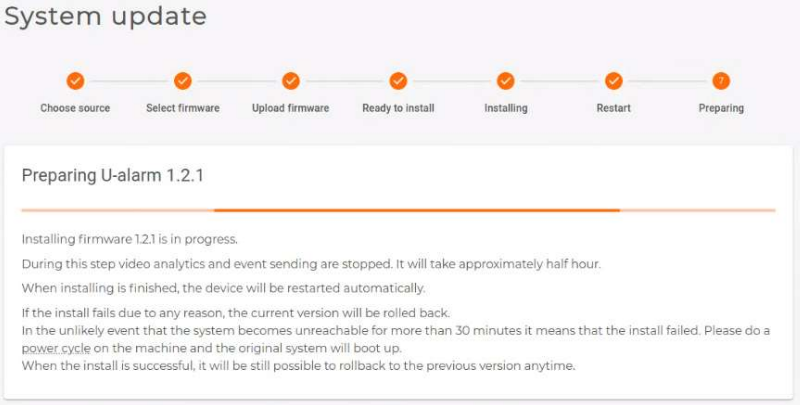
When installing is finished, the device will be restarted automatically.

If the install fails due to any reason, the current version will be rolled back.
In the unlikely event that the system becomes unreachable for more than 30 minutes it means that the install failed. Please do a power cycle on the machine and the original system will boot up.
When the install is successful, it will be still possible to rollback to the previous version anytime.



System update

The device is being restarted.
Please do not reload this page.



System update

Preparing U-alarm 1.2.1

Installing firmware 1.2.1 is in progress.

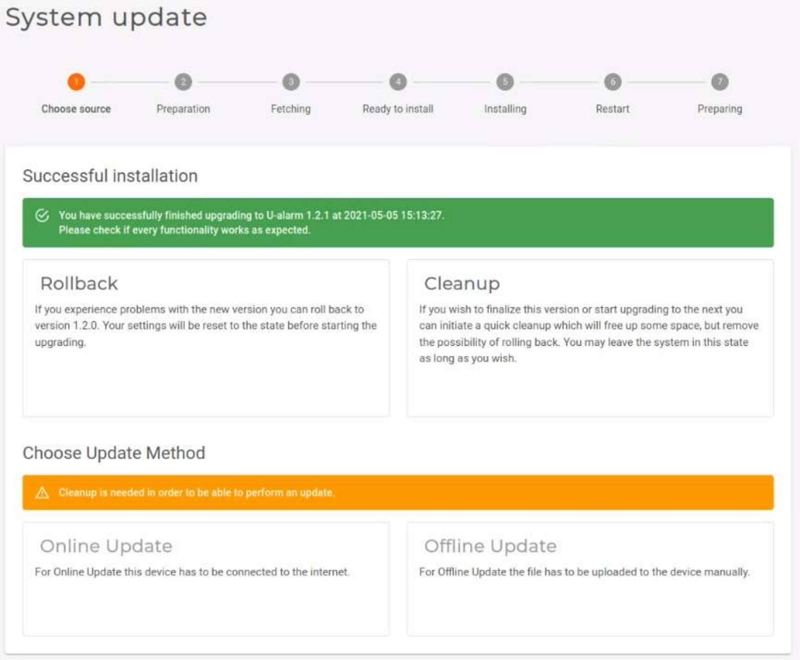
During this step video analytics and event sending are stopped. It will take approximately half hour.

When installing is finished, the device will be restarted automatically.

If the install fails due to any reason, the current version will be rolled back.
In the unlikely event that the system becomes unreachable for more than 30 minutes it means that the install failed. Please do a power cycle on the machine and the original system will boot up.
When the install is successful, it will be still possible to rollback to the previous version anytime.

5. All done. You can re-open U-Alarm and use the new version.

Before logging in after a completed update, it is recommended to hard refresh the U-Alarm login screen in your browser by pressing **Ctrl+Shift+R** or **Ctrl+F5**.



System update

Successful installation

You have successfully finished upgrading to U-alarm 1.2.1 at 2021-05-05 15:13:27.
Please check if every functionality works as expected.

Rollback

If you experience problems with the new version you can roll back to version 1.2.0. Your settings will be reset to the state before starting the upgrading.

Cleanup

If you wish to finalize this version or start upgrading to the next you can initiate a quick cleanup which will free up some space, but remove the possibility of rolling back. You may leave the system in this state as long as you wish.

Choose Update Method

Cleanup is needed in order to be able to perform an update.

Online Update

For Online Update this device has to be connected to the internet.

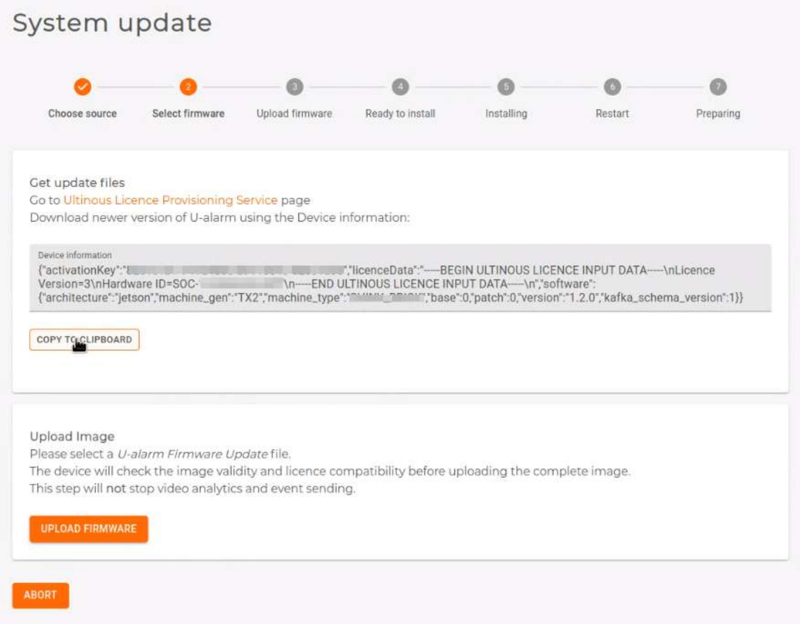
Offline Update

For Offline Update the file has to be uploaded to the device manually.

Offline update

1. Select **Offline Update**.

2. Press the **Copy to Clipboard** button to copy all *Device Information*.



Get update files

Go to Ultinous Licence Provisioning Service page

Download newer version of U-alarm using the Device information:

Device information

```
{"activationKey":"[redacted]","licenceData":"-----BEGIN ULTINOUS LICENCE INPUT DATA-----\nLicence
Version=3\nHardware ID=SOC-[redacted]\n-----END ULTINOUS LICENCE INPUT DATA-----\n","software":
{"architecture":"jetson","machine_gen":"TX2","machine_type":"[redacted]","base":0,"patch":0,"version":"1.2.0","kafka_schema_version":1}}
```

Upload Image

Please select a *U-alarm Firmware Update* file.

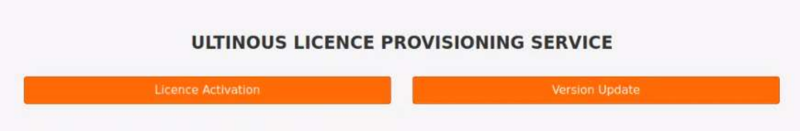
The device will check the image validity and licence compatibility before uploading the complete image.

This step will **not** stop video analytics and event sending.

3. Open a new browser tab and go to activation.ultinous.com.

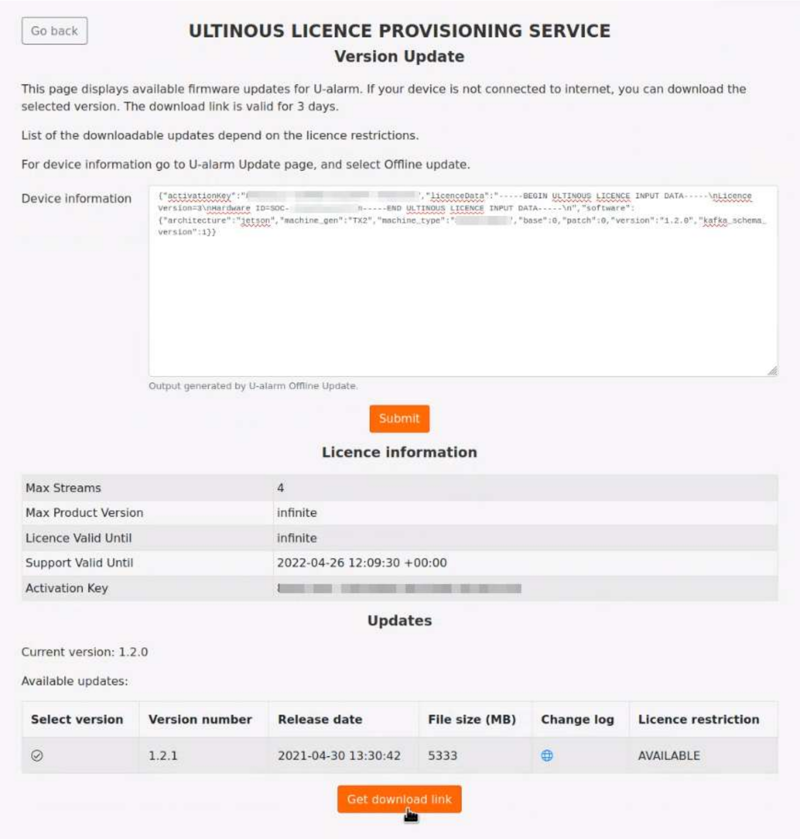
   NOTE: If you copied U-Alarm's *Device Information* from a different computer, please transfer the copied text to the computer with internet access.

4. Select **Version Update**.



5. Paste the previously copied *Device Information* into the textbox. Click **Submit**.

6. Your licence will be checked. Available updates are listed in the Updates section. Select an available version by clicking its checkbox. Click the **Get Download Link** button.



ULTINOUS LICENCE PROVISIONING SERVICE

Version Update

This page displays available firmware updates for U-alarm. If your device is not connected to internet, you can download the selected version. The download link is valid for 3 days.

List of the downloadable updates depend on the licence restrictions.

For device information go to U-alarm Update page, and select Offline update.

Device information

```
{"activationKey":"[redacted]","licenceData":"-----BEGIN ULTINOUS LICENCE INPUT DATA-----\nLicence
Version=3\nHardware ID=SOC-[redacted]n-----END ULTINOUS LICENCE INPUT DATA-----\n","software":
{"architecture":"jetson","machine_gen":"TX2","machine_type":"[redacted]","base":0,"patch":0,"version":"1.2.0","kafka_schema_
version":1}}
```

Output generated by U-alarm Offline Update.

Licence information

Max Streams	4
Max Product Version	infinite
Licence Valid Until	infinite
Support Valid Until	2022-04-26 12:09:30 +00:00
Activation Key	[redacted]

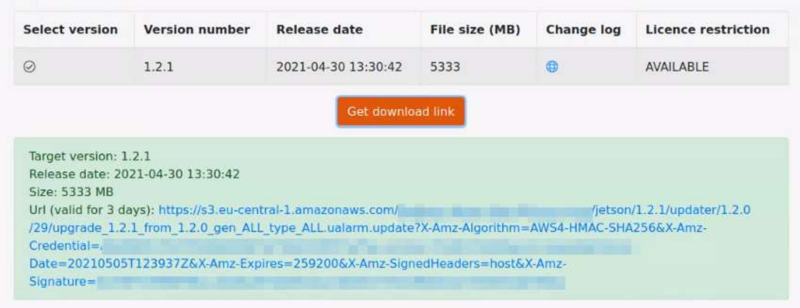
Updates

Current version: 1.2.0

Available updates:

Select version	Version number	Release date	File size (MB)	Change log	Licence restriction
✓	1.2.1	2021-04-30 13:30:42	5333	🌐	AVAILABLE

7. A download link is generated which is available for 3 days. Click the link and save the installer file to your computer. Please wait until the installer is fully downloaded.



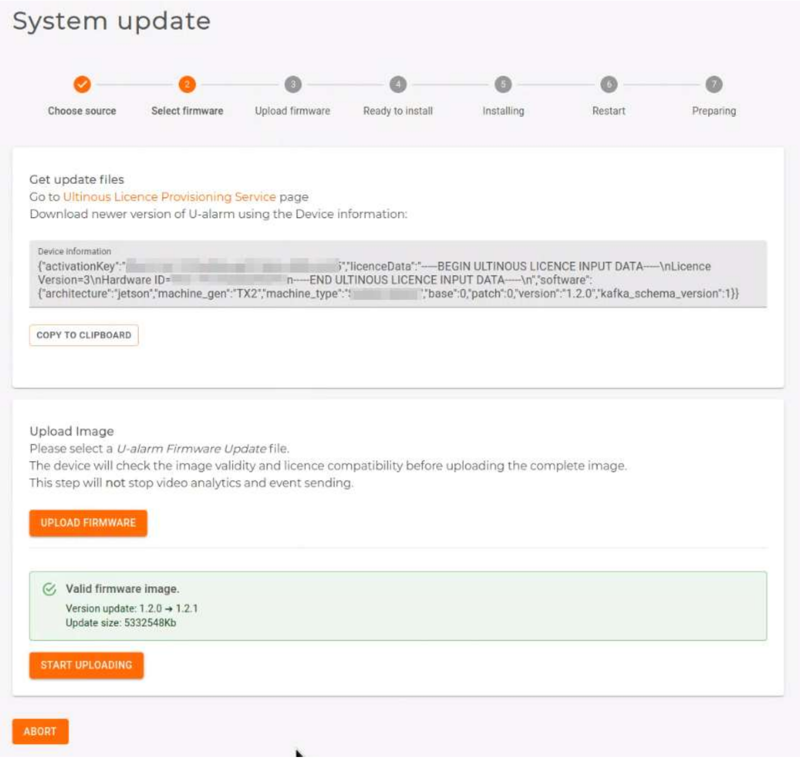
Select version	Version number	Release date	File size (MB)	Change log	Licence restriction
✓	1.2.1	2021-04-30 13:30:42	5333	🌐	AVAILABLE

Target version: 1.2.1
Release date: 2021-04-30 13:30:42
Size: 5333 MB
Url (valid for 3 days): https://s3.eu-central-1.amazonaws.com/[redacted]/jetson/1.2.1/updater/1.2.0/29/upgrade_1.2.1_from_1.2.0_gen_ALL_type_ALL.ualarm.update?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=[redacted]Date=20210505T123937Z&X-Amz-Expires=259200&X-Amz-SignedHeaders=host&X-Amz-Signature=[redacted]

8. **Go back to U-Alarm.**

   NOTE: If you used different computers for accessing U-Alarm and obtaining an installer file, please copy the installer file to the computer which has access to U-Alarm.

9. Click the **Upload Firmware** button. Select the downloaded installer in your computer's file system.



System update

Get update files

Go to Ultinous Licence Provisioning Service page

Download newer version of U-alarm using the Device information:

Device information

```
{"activationKey":"[redacted]","licenceData":"-----BEGIN ULTINOUS LICENCE INPUT DATA-----\nLicence
Version=3\nHardware ID=[redacted]n-----END ULTINOUS LICENCE INPUT DATA-----\n","software":
{"architecture":"jetson","machine_gen":"TX2","machine_type":"[redacted]","base":0,"patch":0,"version":"1.2.0","kafka_schema_version":1}}
```

Upload Image

Please select a *U-alarm Firmware Update* file.

The device will check the image validity and licence compatibility before uploading the complete image.

This step will **not** stop video analytics and event sending.

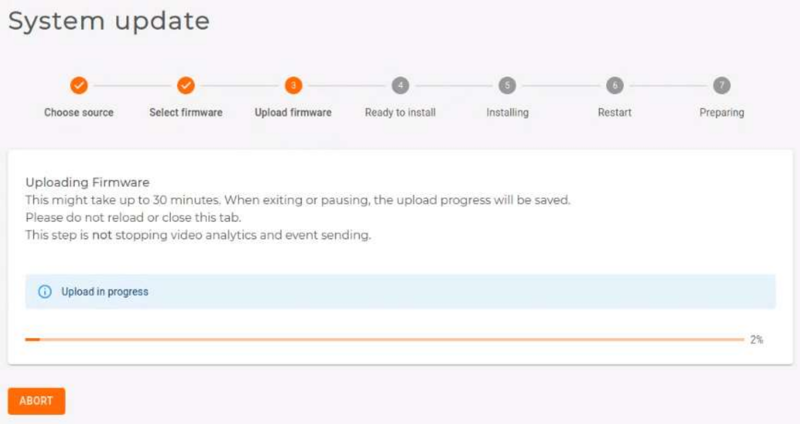
Valid firmware image.

Version update: 1.2.0 → 1.2.1

Update size: 5332548Kb

10. U-Alarm will quickly validate the installer.

11. Click the **Start Uploading** button. The upload process's duration depends on your bandwidth. Please wait until the upload is finished.



System update

Uploading Firmware

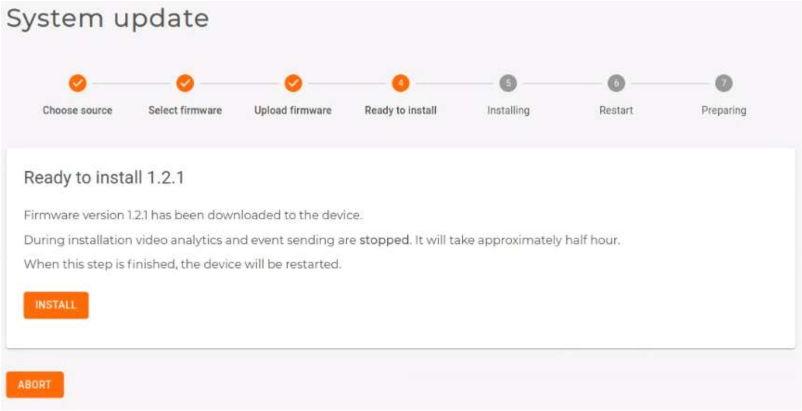
This might take up to 30 minutes. When exiting or pausing, the upload progress will be saved.

Please do not reload or close this tab.

This step is **not** stopping video analytics and event sending.

Upload in progress

12. Ready to Install. Press the **Install** button. From this point on, all U-Alarm services will be unavailable until the update is finished. This process can take up to 30 minutes as U-Alarm goes through the *Installing*, *Restart* and *Preparing* steps automatically during the installation.

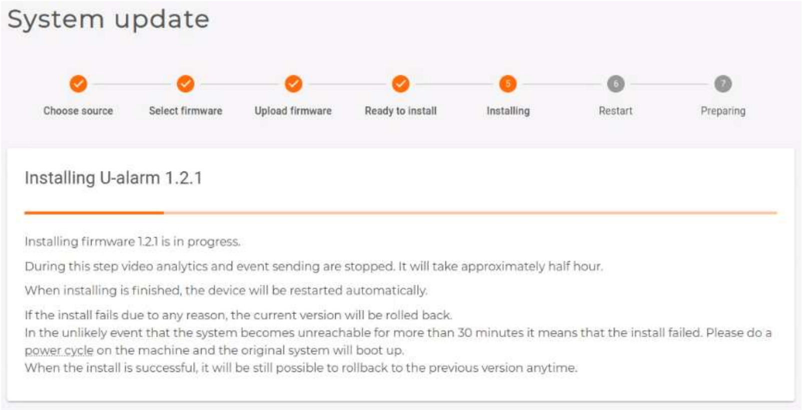


Ready to install 1.2.1

Firmware version 1.2.1 has been downloaded to the device.

During installation video analytics and event sending are **stopped**. It will take approximately half hour.

When this step is finished, the device will be restarted.



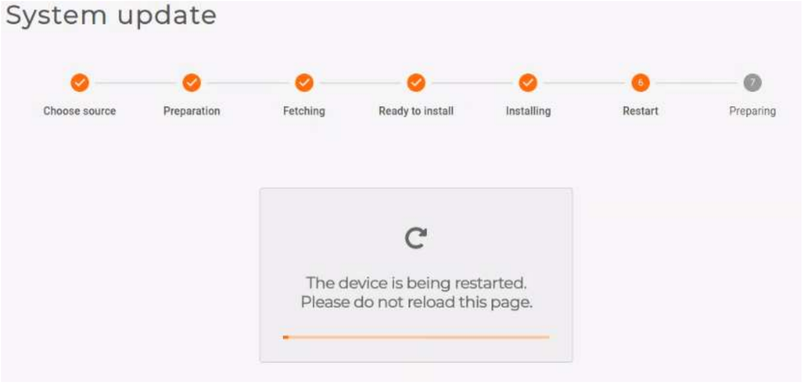
Installing U-alarm 1.2.1

Installing firmware 1.2.1 is in progress.

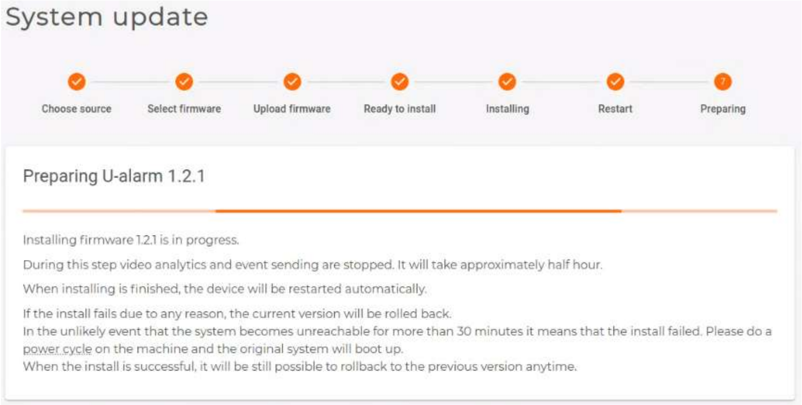
During this step video analytics and event sending are stopped. It will take approximately half hour.

When installing is finished, the device will be restarted automatically.

If the install fails due to any reason, the current version will be rolled back.
In the unlikely event that the system becomes unreachable for more than 30 minutes it means that the install failed. Please do a power cycle on the machine and the original system will boot up.
When the install is successful, it will be still possible to rollback to the previous version anytime.



The device is being restarted.
Please do not reload this page.



Preparing U-alarm 1.2.1

Installing firmware 1.2.1 is in progress.

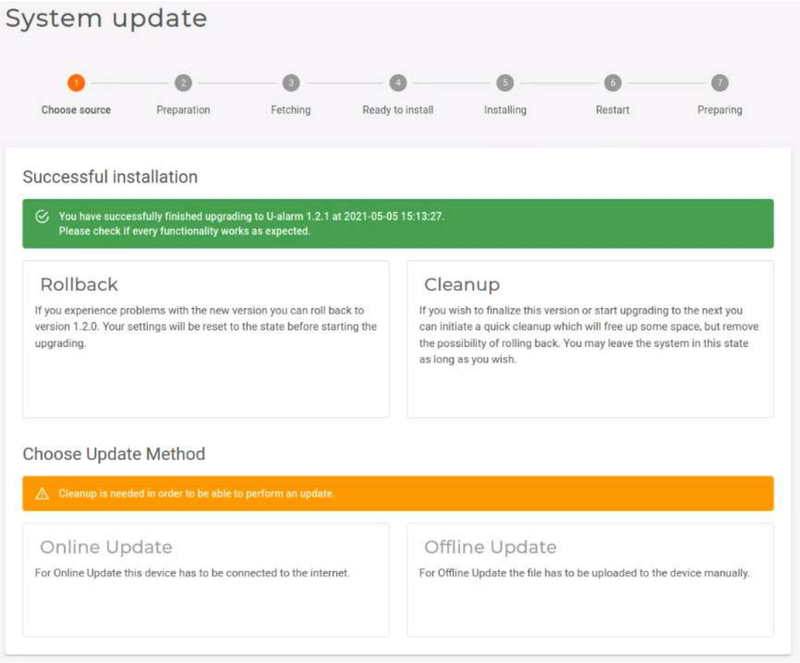
During this step video analytics and event sending are stopped. It will take approximately half hour.

When installing is finished, the device will be restarted automatically.

If the install fails due to any reason, the current version will be rolled back.
In the unlikely event that the system becomes unreachable for more than 30 minutes it means that the install failed. Please do a power cycle on the machine and the original system will boot up.
When the install is successful, it will be still possible to rollback to the previous version anytime.

13. All done. You can re-open U-Alarm and use the new version.

    Before logging in after a completed update, it is recommended to hard refresh the U-Alarm login screen in your browser by pressing **Ctrl + Shift + R**.



System update

Successful installation

You have successfully finished upgrading to U-alarm 1.2.1 at 2021-05-05 15:13:27.
Please check if every functionality works as expected.

Rollback

If you experience problems with the new version you can roll back to version 1.2.0. Your settings will be reset to the state before starting the upgrading.

Cleanup

If you wish to finalize this version or start upgrading to the next you can initiate a quick cleanup which will free up some space, but remove the possibility of rolling back. You may leave the system in this state as long as you wish.

Choose Update Method

Cleanup is needed in order to be able to perform an update.

Online Update

For Online Update this device has to be connected to the internet.

Offline Update

For Offline Update the file has to be uploaded to the device manually.

Cleanup

U-Alarm stores the previous version after an update has been installed. This provides a Rollback option to the previous version. However, no further update is possible until a **Cleanup** is done.

Click **Cleanup** to delete the previous version's archives and to prepare U-Alarm for another update.

NOTE: Rollback is not available after Cleanup.

Rollback

After an update has been completed, it is possible to roll back to the previous version. Click **Rollback** to restore the previous version of U-Alarm.

Before logging in after a completed rollback, it is recommended to hard refresh the U-Alarm login screen in your browser by pressing **Ctrl + Shift + R**.

NOTE: Rollback is not available after Cleanup.

Integration

U-Alarm is not only a stand-alone solution, but can be used in an integrated system as well. Each article contains valuable information about the required settings in U-Alarm, as well as in the corresponding third-party software.

General concept

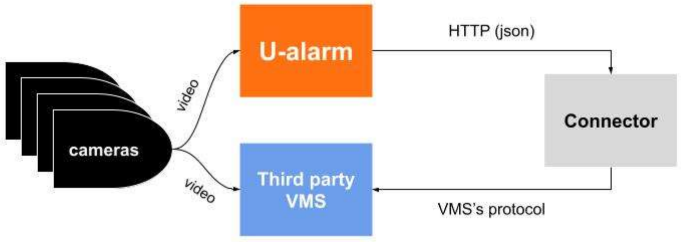
Components

The integration has 3 components:

- U-Alarm
- Third party application (preferably a VMS)
- a Connector

Note: In this document, the *Third party application* is often referred to as **VMS,** however it can be any software with similar capabilities.

Topology



U-Alarm

- Receives video streams from cameras.
- Detects incidents.
- Notifies the operator on its user interface.
- Sends Event messages with metadata to an external API via HTTP.

VMS

- Receives good quality video streams from cameras.
- Stores video/Provides user interface for operators including incident management.
- Has an interface to receive real time notifications (alarms/events) from external sources.

Connector

- Dedicated to a specific VMS.
- Usually running on the same machine as the VMS.
- Associates streams registered in U-Alarm with streams registered in the VMS (easier if the VMS provides a unique identifier for each camera).
- Receives Event messages or pulls count data from U-Alarm.
- Converts U-Alarm Events to a message which is readable by the VMS.

Capabilities

Capabilities are determined by both U-Alarm and the VMS. The following information is available in the U-Alarm Event's metadata:

- the incident's type (Intrusion and Crowd Detection, Multi Object Detection and Multi Object Counter)
- the timestamp of the incident
- camera identifier(s)
- the detections' coordinates in the camera frame
- confidence value - events with lower confidence can be filtered in order to decrease false positive alarms

(Learn more about the metadata for your Custom Integration...)

This information is translated by the Connector component. The capabilities of the VMS may limit the forwarded information and the overall end user experience.

Example scenario

Installation

- U-Alarm is installed on an NVidia Jetson NX box.
- The VMS is installed on a Windows server.
- The Connector is installed on the same machine.
- Both machines are on the same local network with fixed IP addresses.

Configuration

vms-1*VMS*

The VMS is configured according to its own documentation with the following requirements:

- Observed Cameras must be registered in both U-Alarm and in the VMS. The VMS may use the primary stream of the cameras with higher resolution and FPS compared to U-Alarm. A unique identifier should be memorized for each registered camera. The identifiers will be used in U-Alarm configuration.
- Access credentials for the connector.
- All other settings in order to receive external events.

connector-1*Connector*

Connector must have the following information:

- Access credentials for the VMS.
- An unused port for its service.
- The (network) location of the VMS interface.

u-alarm-1*U-Alarm*

U-Alarm is configured along its own documentation with the following exceptions:

- Observed Cameras must be registered in both U-Alarm and in the VMS. U-Alarm often uses a secondary stream of the same camera with lower resolution and FPS.
- Cameras' *Technical names* must be set. Each technical name should be unique and should match the unique identifier of the same camera in the VMS.
- The network address of the Connector (host, port) must be set in the Alarm configuration.

Workflow

In this example let's say we configured intrusion detection in U-Alarm.

1. The intruder enters an observed area.
2. The camera stream is sent to U-Alarm.
3. U-Alarm detects the intruder and immediately sends an Event to the Connector.
4. The Connector converts the incoming Event and sends it to the VMS.
5. The VMS triggers an alarm and notifies the operator.

Implementations

For alarms

Milestone XProtect is one of the most popular Video Management Systems. U-Alarm is able to send Alarms to this system so you can manage incidents in your well known platform.

U-Alarm can be configured to send alarms via e-mail. This enables you to use U-Alarm in conjunction with e-mail notifications, or omit the use of U-Alarm altogether. The service can be set up to be used by either human beings or automated systems.

This guide will aid developers in order to receive and process Alarms triggered U-Alarm in their custom solution.

For people and vehicle counting

U-Alarm's measurement-based counters are designed to be used with custom third party software. Read on to learn how the data created by the counters can be read from U-Alarm.

Monitoring

SNMP

SNMP settings are available in the Control Panel.

Status via HTTP API

You can progamatically acquire several metrics from the U-Alarm via its HTTP API.

The response contains a JSON object with the available metrics. Integrating applications should accept unkown keys in the response, as new metrics may be added in later versions.

The endpoint is authenticated via API token in the Authorization header, see here.

Standard HTTP response codes are used:

- 200 for successful response
- 401 for authentication failure
- >=500 if the API could not respond due to error

The following example uses curl to test if the U-Alarm API endpoint is reachable.

```
curl  -H 'Authorization: Bearer <API token>' -H 'Accept: application/json'
'http://<address-of-ualarm>/API/system/status'

or if HTTPS is configured

curl  -H 'Authorization: Bearer <API token>' -H 'Accept: application/json'
'https://<address-of-ualarm>/API/system/status'
```

Response body:

```
{

  "sysuptime": 78792, //< system uptime in seconds

  "avgcpu": 22, //< average CPU utilization

  "avggpu": 0,  //< average GPU utilization (used by video analitics)

  "ram_available_megabytes": 4900,    //< unused RAM
  "ram_used_megabytes": 7859,         //< RAM usage

  "ram_used_pcnt": 38,                //< RAM used percentage

  "ualarm": {

  "systemstatus": 1, //< 1=OK, 2=ERROR

  "videostorage_total_bytes": 491182010368,  //< storage assigned for Event
videos

  "videostorage_free_bytes": 401370316800,   //< storage free

  "videostorage_used_pcnt": 19,              //< storage used percentage

    "systemstatus_msg": " ",  //< if systemstatus is 2, a message describes
it.

    "cameras_statuses": [
      {
        "id": "cam5",
        "display_name": "display name of cam5",
        "technical_name": "technical name of cam5",
        "problems": []
      },
      {
        "id": "cam7",
        "display_name": "Garage",
        "technical_name": "garage cam",
        "problems": []
      }
    ]
  }
}
```

Milestone XProtect Integration

Milestone XProtect is one of the most popular Video Management Systems. U-Alarm is able to send alarms to this system so you can manage incidents in your well-known platform.

There are two ways of sending and managing alarms from U-Alarm: through the *Alarm Manager*, or alternatively, via e-mail, using the built-in e-mail notification feature of Milestone XProtect.

NOTE: As of now, the Alarm Manager is only available in editions Express+ and above. If using Essential+, the only way of receiving alarms in Milestone XProtect is via an E-mail notification.

Consult the following table for the different feature sets of Milestone XProtect editions:

XProtect Edition / Feature	Alarm manager	E-mail notification	Recording on Alarm
Corporate	âœ“	âœ“	âœ“
Expert	âœ“	âœ“	âœ“
Professional+	âœ“	âœ“	âœ“
Express+	âœ“	âœ“	âœ“
Essential+	-	âœ“	âœ“

**tested on XProtect version 2020 R3*

In order to integrate U-Alarm in your Milestone XProtect VMS you have to configure three components:

U-Alarm => Connector => Milestone XProtect

Alarm signals will flow in the order as described above. Configuration should be made in the reversed order:

1. Setup *Milestone XProtect*
2. Setup *U-Alarm / Milestone XProtect Connector*
3. Setup *U-Alarm*

Note: This guide has been tested on Milestone XProtect 2020 R1 and 2020 R3.

Before you start

In this guide it is assumed that Milestone XProtect is installed on a computer in your network and you know how to configure it when using it without U-Alarm. For further details, please visit the official site of Milestone.

Requirements:

- Cameras are reachable from both U-Alarm and Milestone XProtect, and U-Alarm is able to connect to Milestone XProtect.
- Please make sure that each camera is registered in Milestone XProtect which should use U-Alarm, as described in the Milestone documentation here.
- You have administrator privileges on the device running Milestone XProtect (both for Windows and within Milestone XProtect).

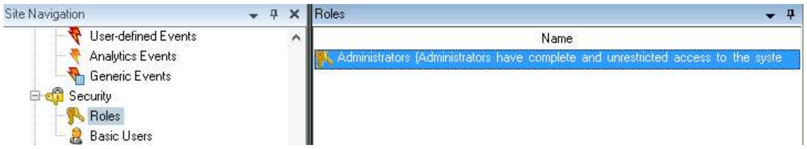
Milestone XProtect

User

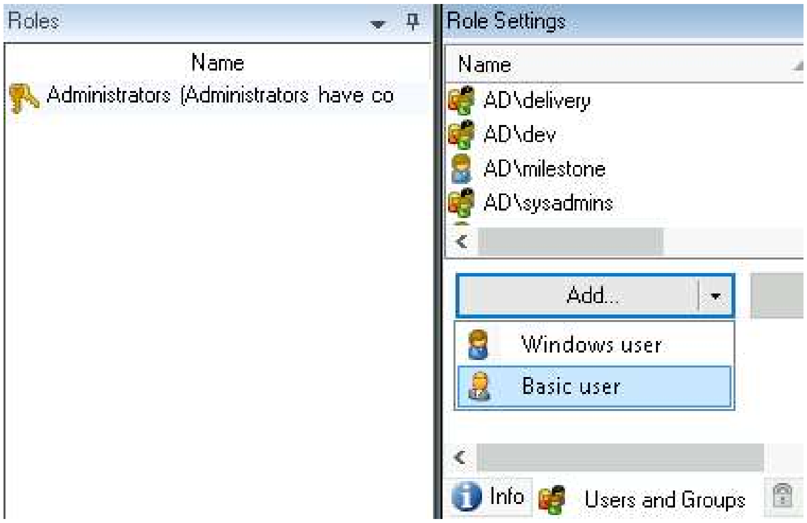
U-Alarm requires access to Milestone XProtect, therefore a new user should be created with administrator privileges.

1. In the *Milestone XProtect Management Client*, go to the *Site Navigation* panel => *Security* => *Roles*.

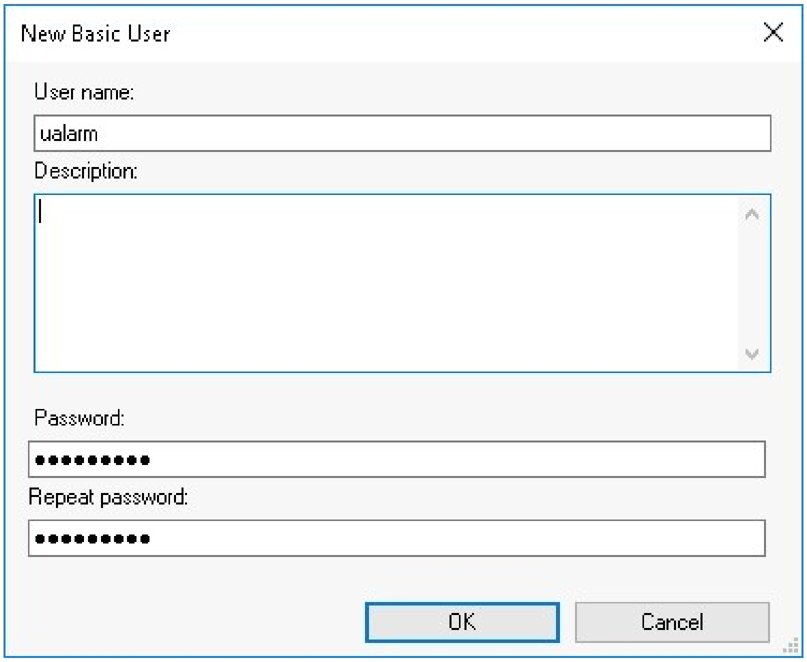
2. Click on *Administrators* in the *Roles* panel.



3. Find the *Users and Groups* tab at the bottom of the *Role Settings panel*. Click the *Add...* dropdown and select the *Basic user* option.



4. In the *Select Basic Users to add to Role* pop-up, click the *New* button.
5. A new pop-up appears. Fill in the form with new user credentials and click *OK*. Use a complex password with capital and small letters, numbers and special characters. Remember the password, because it will be used later in the Connector.



New Basic User

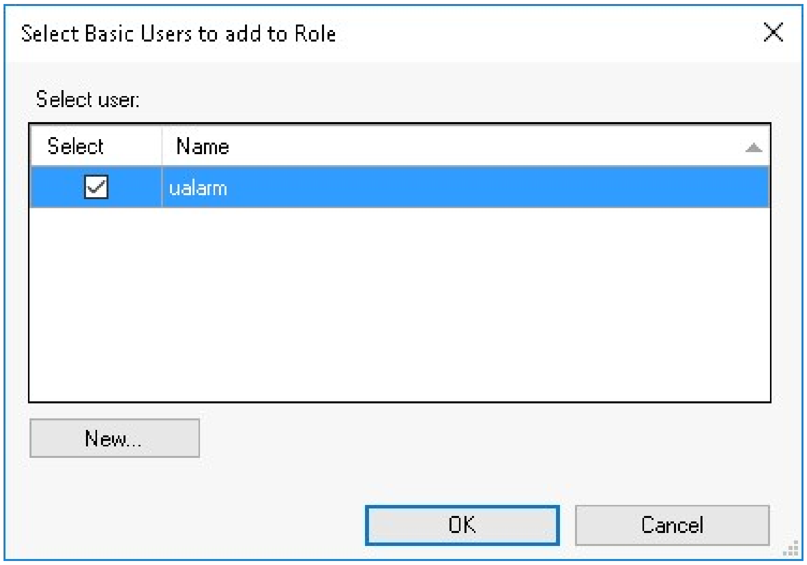
User name: ualarm

Description:

Password: ●●●●●●●●●●

Repeat password: ●●●●●●●●●●

6. Add this basic user to the Administrators by clicking *OK*.



Select Basic Users to add to Role

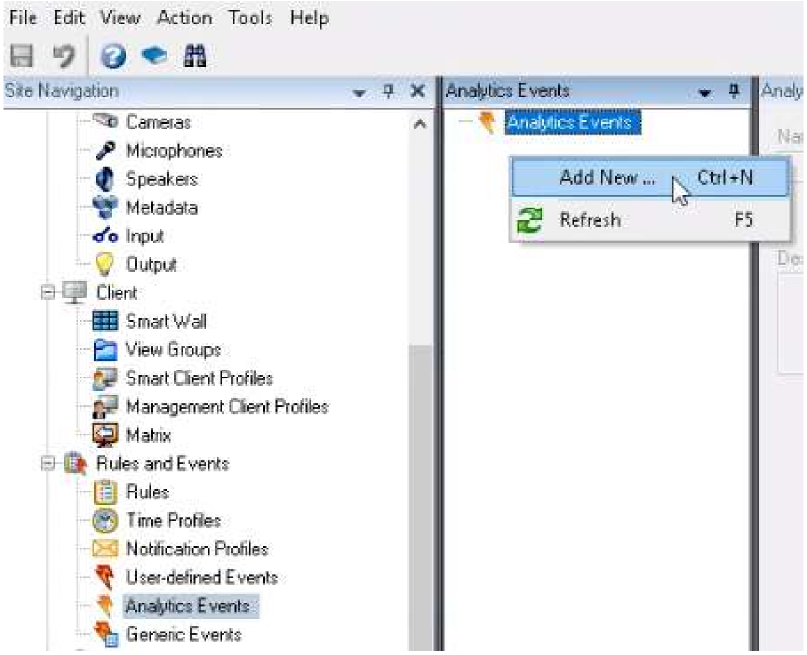
Select user:

Select	Name
☑	ualarm

Event

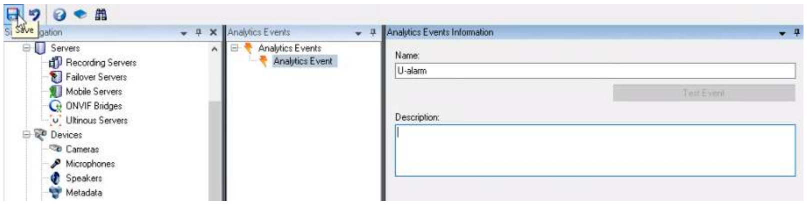
1. In the Milestone XProtect Management Client, go to the *Site Navigation* panel => *Rules and Events* => *Analytics Events*.

2. Right click on the *Analytics Events* panel => *Add new*.



4. The name should be **`U-Alarm`**.

   Note: It is very important to set this exact name without the dot or any white spaces.



Name: U-alarm

Description:

5. Click the *Save* button in the top left corner.

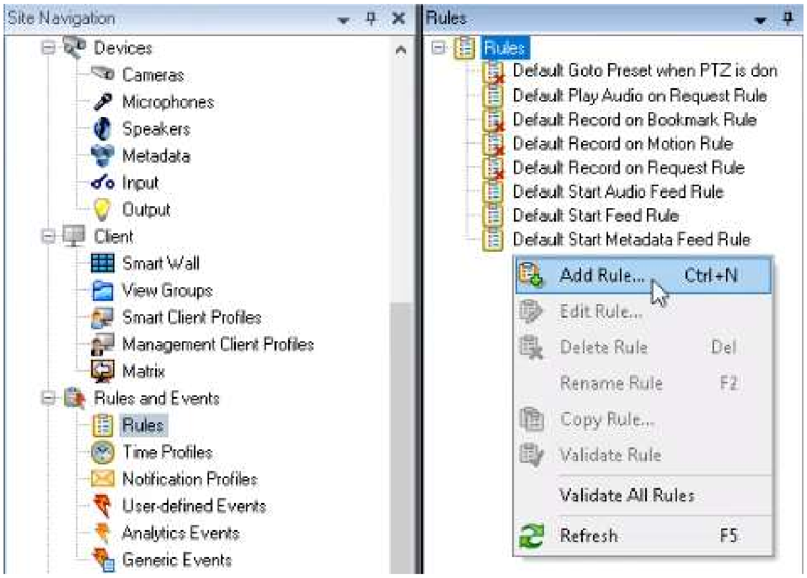
Recording Rule

If your system is not recording continuously, it is recommended to start recording on each triggered alarm. A Rule should be created for this purpose.

Tip: If your system has a custom recording logic, you can skip this step.

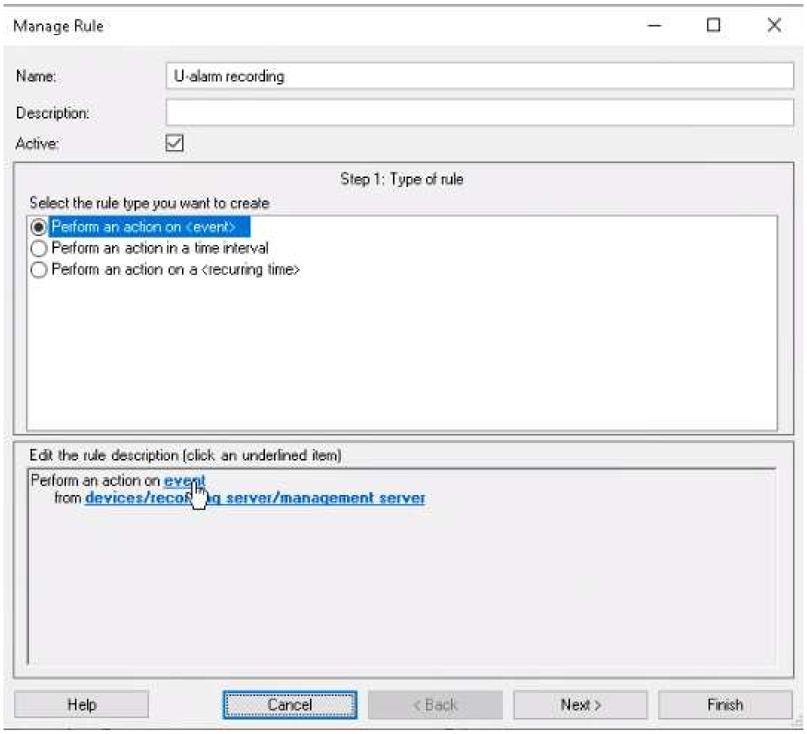
1. In the Milestone XProtect Management Client, go to the *Site Navigation* panel => *Rules and Events* => *Rules*.

2. Right-click on the *Rules* panel => *Add Rule*



3. Set any Name.

4. As the *Type of rule*, select *Perform action on event*. Click on the blue underlined "*event*" word in the lower panel.



Name: U-alarm recording

Description:

Active: ☑

Step 1: Type of rule

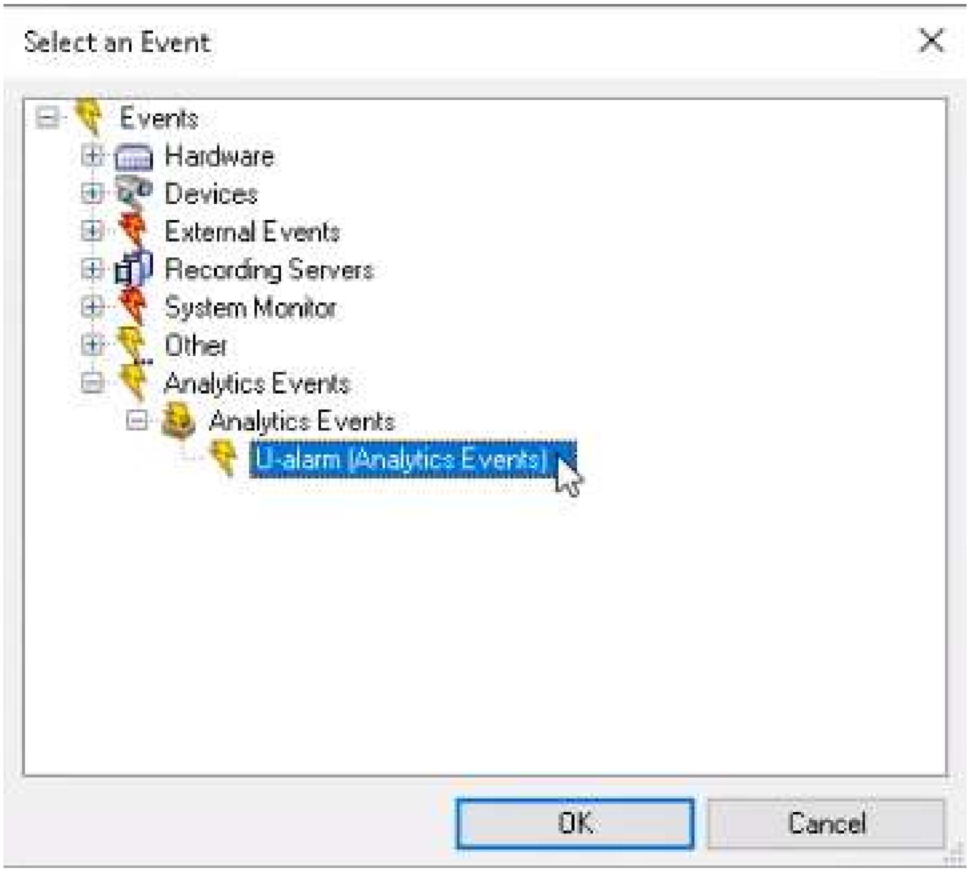
Select the rule type you want to create

● Perform an action on <event>
○ Perform an action in a time interval
○ Perform an action on a <recurring time>

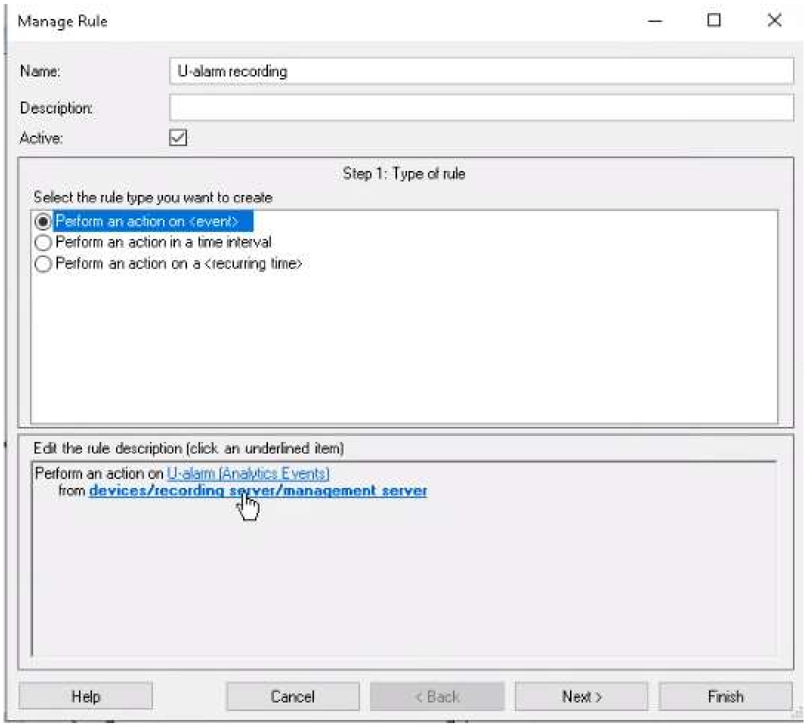
Edit the rule description (click an underlined item)

Perform an action on event
from devices/recording server/management server

5. In the pop-up select *Events* => *Analytics Events* => ... ***U-Alarm***. Click *OK*.



6. Click on the blue underlined "*devices/...*" line in the lower panel (after "*from*").



Name: U-alarm recording

Description:

Active: ☑

Step 1: Type of rule

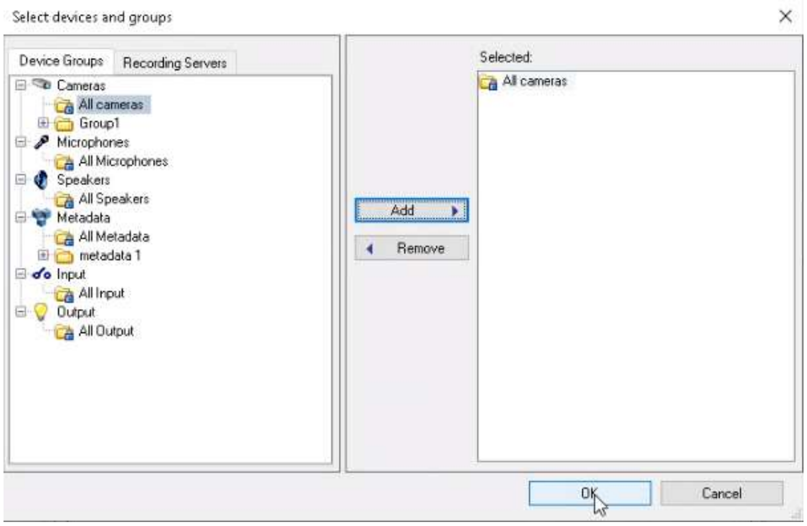
Select the rule type you want to create

● Perform an action on <event>
○ Perform an action in a time interval
○ Perform an action on a <recurring time>

Edit the rule description (click an underlined item)

Perform an action on U-alarm (Analytics Events)
from **devices/recording server/management server**

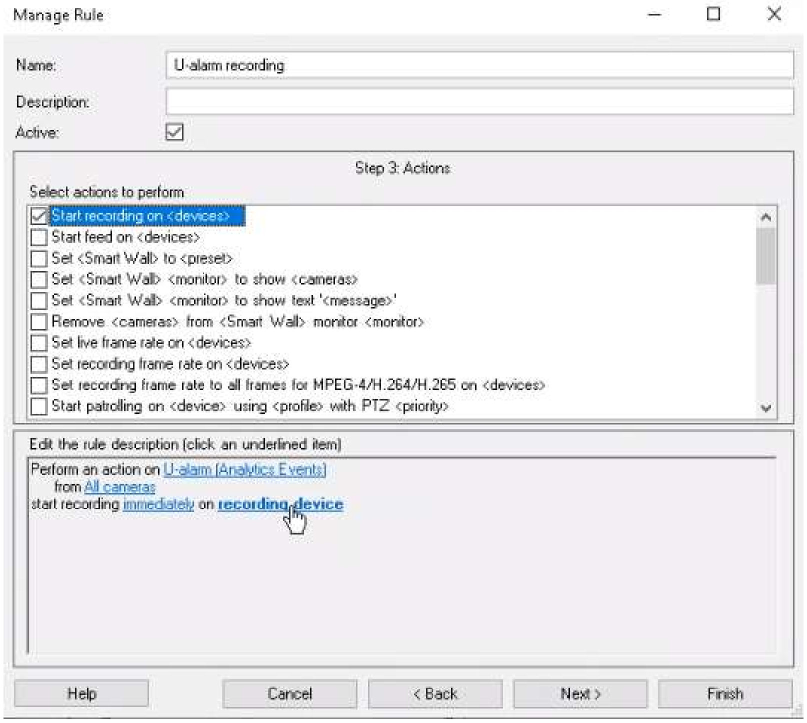
7. In the pop-up select *Cameras* => *All cameras*. Click the *Add* button. Click *OK*.



8. Click *Next*.

9. Skip the *Conditions Step* (2). Click *Next* again.

10. In the *Actions Step* (3) select *Start recording on devices*. Click on the blue underlined "*recording device*" words in the lower panel.



Name: U-alarm recording

Description:

Active: ☑

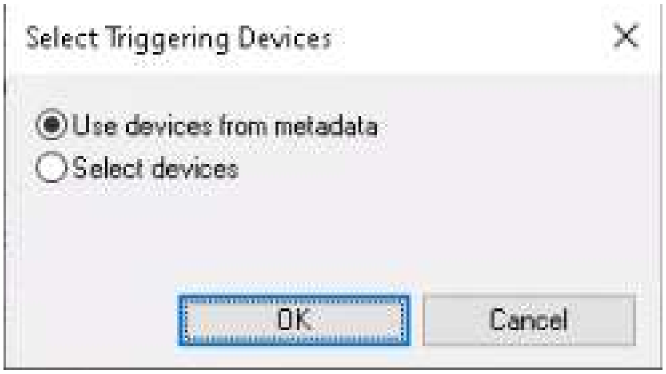
Select actions to perform

☑ Start recording on <devices>
☐ Start feed on <devices>
☐ Set <Smart Wall> to <preset>
☐ Set <Smart Wall> <monitor> to show <cameras>
☐ Set <Smart Wall> <monitor> to show text '<message>'
☐ Remove <cameras> from <Smart Wall> monitor <monitor>
☐ Set live frame rate on <devices>
☐ Set recording frame rate on <devices>
☐ Set recording frame rate to all frames for MPEG-4/H.264/H.265 on <devices>
☐ Start patrolling on <device> using <profile> with PTZ <priority>

Edit the rule description (click an underlined item)

Perform an action on U-alarm (Analytics Events)
from All cameras
start recording immediately on recording device

11. In the pop-up select *Use devices from metadata*. Click *OK*.



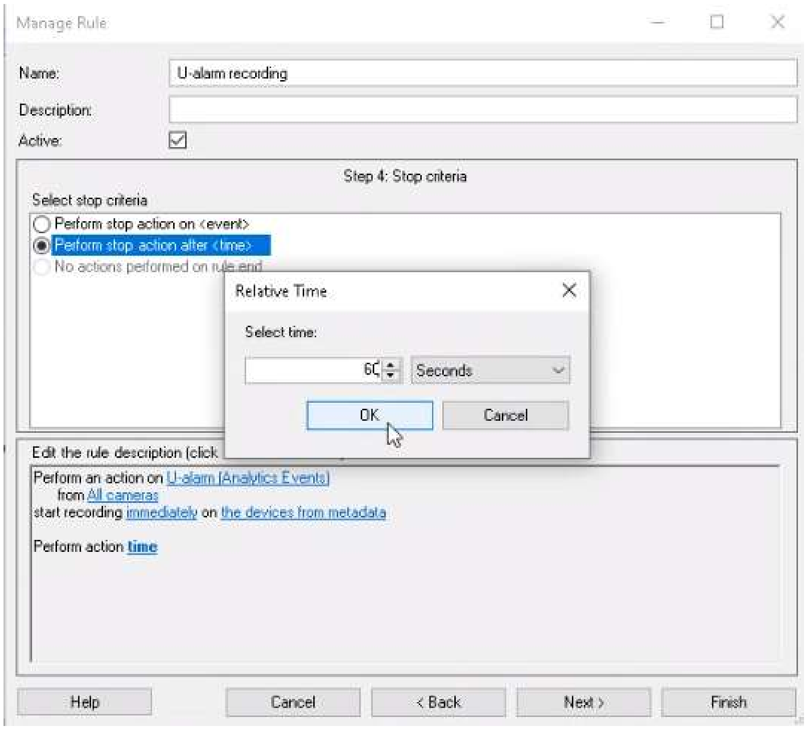
Select Triggering Devices

● Use devices from metadata
○ Select devices

12. The recording will start immediately on alarm. You can set other (even negative) values by clicking on the blue underlined "*immediately*" word in the lower panel.

13. Click the *Next* button.

14. In the *Stop Criteria* (4) step, select *Perform stop action after time*. Click the blue underlined "*time*" word in the lower panel and set the length of the recordings. Click *OK*.



Manage Rule

Name: U-alarm recording

Description:

Active: ☑

Step 4: Stop criteria

Select stop criteria

○ Perform stop action on <event>
● Perform stop action after <time>
○ No actions performed on rule end

Relative Time

Select time: 60 Seconds

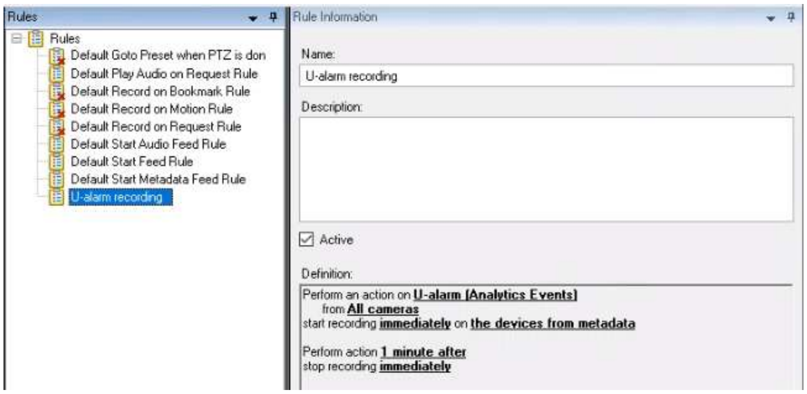
Edit the rule description (click

Perform an action on U-alarm (Analytics Events)
from All cameras
start recording immediately on the devices from metadata

Perform action time

15. Click *Next*.

16. Skip the "*Stop actions*" (5) step. Click *Finish*. The new rule is created.



Rules

Rules

- Default Goto Preset when PTZ is don
- Default Play Audio on Request Rule
- Default Record on Bookmark Rule
- Default Record on Motion Rule
- Default Record on Request Rule
- Default Start Audio Feed Rule
- Default Start Feed Rule
- Default Start Metadata Feed Rule
- U-alarm recording

Rule Information

Name: U-alarm recording

Description:

☑ Active

Definition:

Perform an action on U-alarm (Analytics Events)
from All cameras
start recording immediately on the devices from metadata

Perform action 1 minute after
stop recording immediately

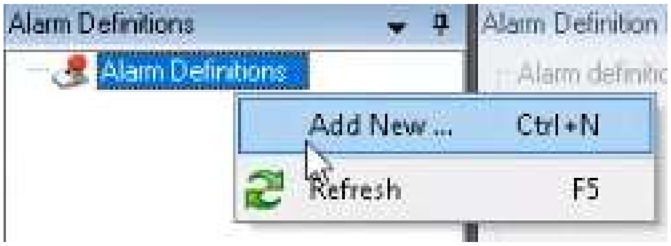
Alarm

Receiving alarms in the Alarm Manager

Now an Alarm has to be configured in Milestone XProtect.

1. In the *Milestone XProtect Management Client* go to the *Site Navigation* panel => *Alarms* => *Alarm Definitions*.

2. Right-click on the *Alarm Definitions* panel => *Add new*.



3. Fill the form. Make sure that the alarm is *Enabled*.

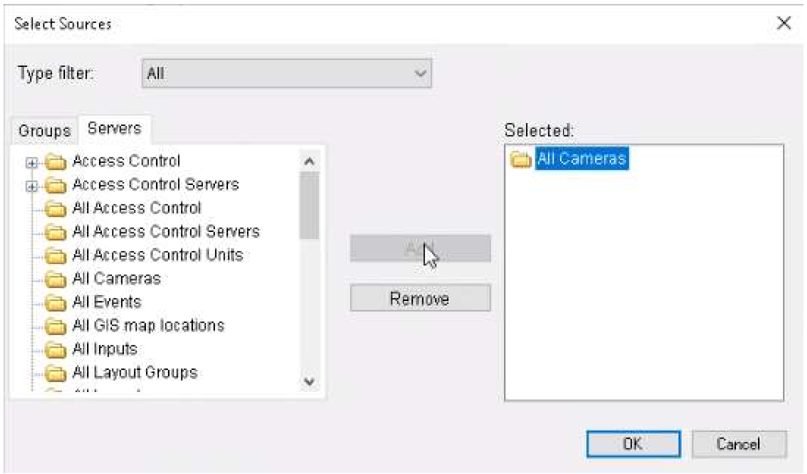
4. Set any *Name* for the alarm.

   This alarm will represent all notifications which come from U-Alarm.

5. Set the *Triggering event* to *Analytics Events*, then set ***U-Alarm*** in the drop-down list below.

6. At the *Sources* setting, click the *Select...* button. A pop-up will appear.

7. Click on the *Servers* tab. Select the ***All Cameras*** node and click the *Add* button. Click *OK*.

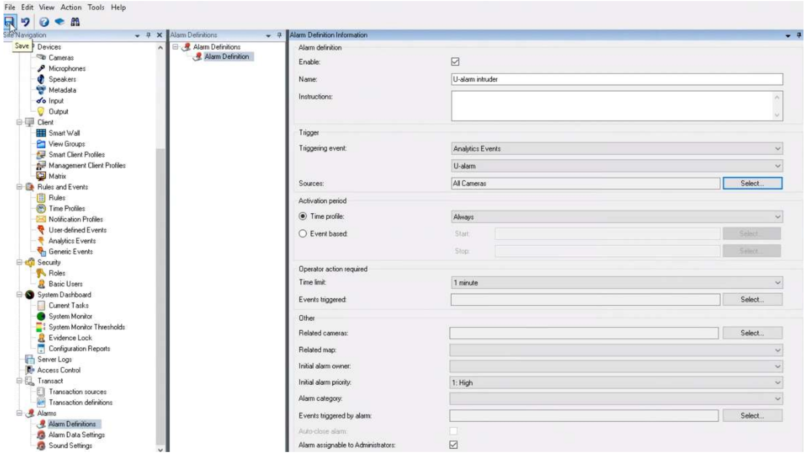


Select Sources

Type filter: All

Selected: All Cameras

8. If you are familiar with Milestone XProtect, you can configure the rest of the settings as you wish or you can leave them as they are.



Alarm Definition Information

Alarm definition

Enable: ☑

Name: U-alarm intruder

Instructions:

Trigger

Triggering event: Analytics Events

U-alarm

Sources: All Cameras

Activation period

● Time profile: Always

○ Event based

Start:

Stop:

Operator action required

Time limit: 1 minute

Events triggered:

Other

Related cameras:

Related map:

Initial alarm owner:

Initial alarm priority: 1: High

Alarm category:

Events triggered by alarm:

Auto-close alarm: □

Alarm assignable to Administrators: ☑

9. Click the *Save* button in the top left corner (once enabled).

All done. You will receive alarms in the Alarm Manager.

Receiving alarms by e-mail

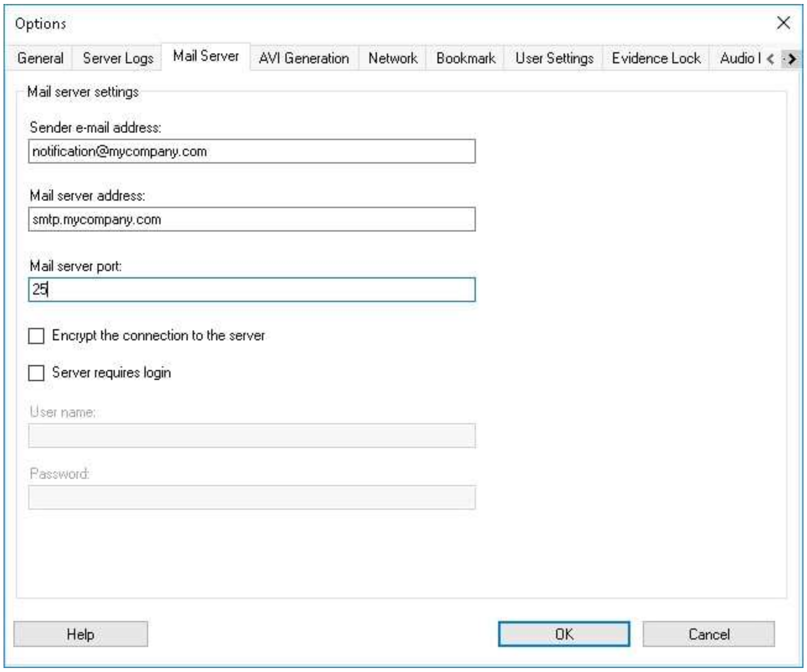
Besides the *Alarm Manager*, Milestone XProtect has an additional way of viewing received alarms: in e-mail format with optional image and/or video attachments.

If your copy of Milestone XProtect lacks the *Alarm Manager* feature (i.e.: your edition is the Essential+) - this is the only way of receiving alarms.

Follow the steps below to have a working e-mail notification setup.

mail-server*Mail server*

1. In the Milestone XProtect Management Client, go to the *Options* in the upper menu bar => *Mail Server*.



Mail server settings

Sender e-mail address: notification@mycompany.com

Mail server address: smtp.mycompany.com

Mail server port: 25

☐ Encrypt the connection to the server

☐ Server requires login

User name:

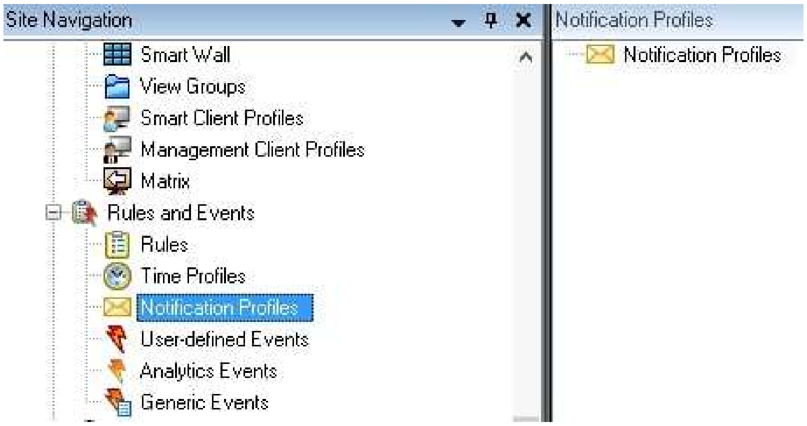
Password:

2. Type in the sender address.
3. Type in the smtp address of the sender in *Mail server address*.
4. Click *OK*.

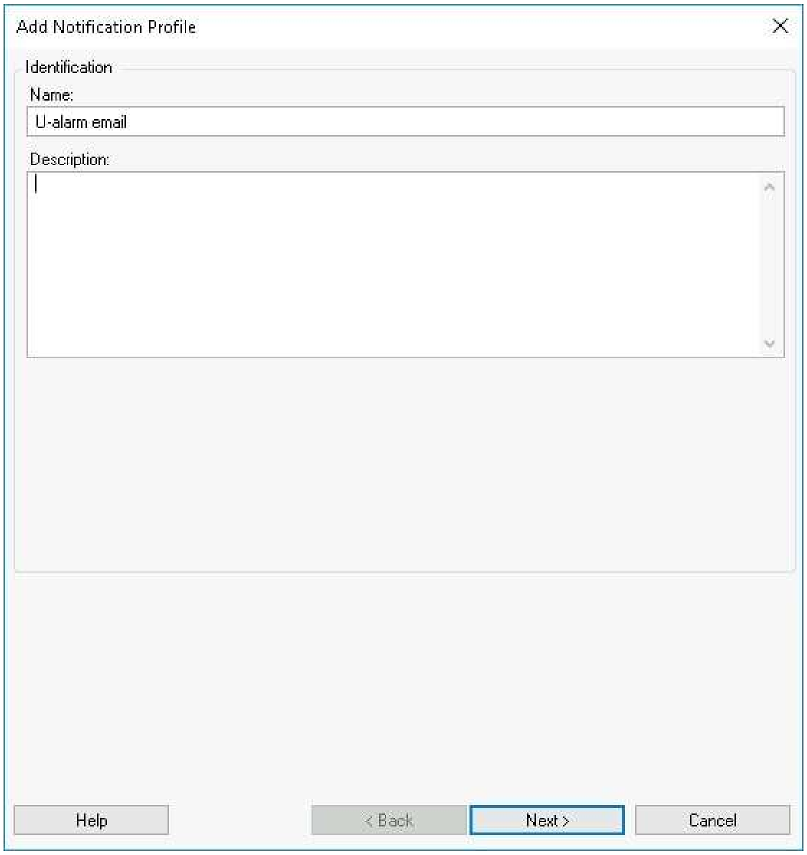
notification-profile*Notification Profile*

Now let us create a profile for sending the e-mail notifications.

1. In the *Milestone XProtect Management Client* go to the *Site Navigation* panel => *Rules and Events* => *Notification Profiles*.



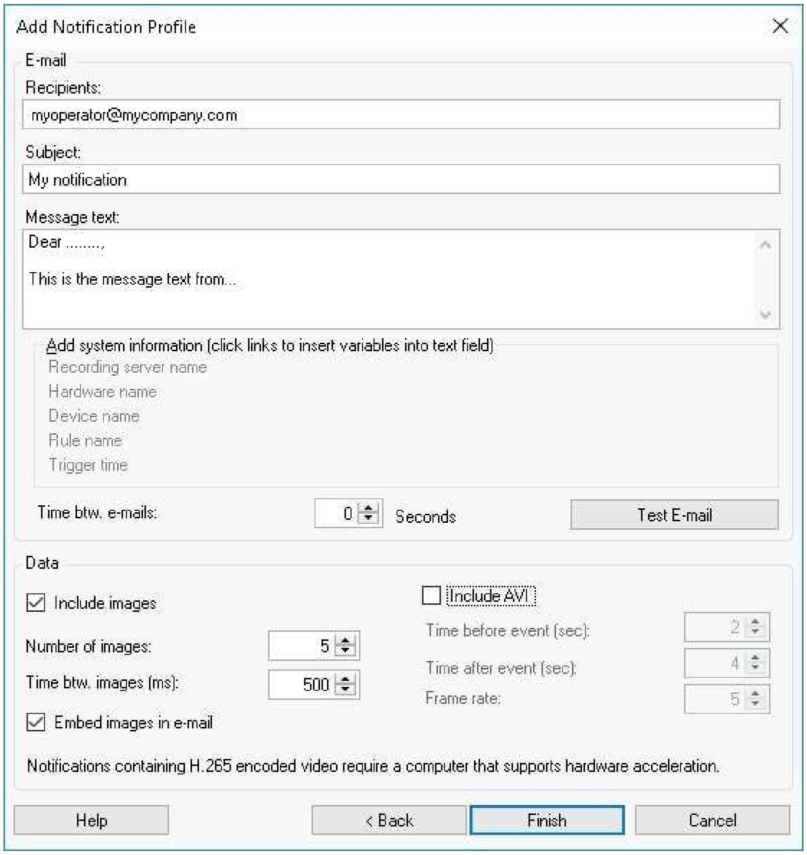
2. Right-click on the *Notification Profiles* icon in the right-side panel => *Add new*.
3. Set *U-Alarm email* as the *Name* of the profile. You may fill the *Description* field as well (optional).



Name:
U-alarm email

Description:

4. Click *Next*.



Add Notification Profile

E-mail

Recipients: myoperator@mycompany.com

Subject: My notification

Message text:
Dear ....,

This is the message text from...

Add system information (click links to insert variables into text field)
Recording server name
Hardware name
Device name
Rule name
Trigger time

Time btw. e-mails: 0 Seconds

Data

☑ Include images

Number of images: 5

Time btw. images (ms): 500

☑ Embed images in e-mail

□ Include AVI

Time before event (sec): 2

Time after event (sec): 4

Frame rate: 5

Notifications containing H.265 encoded video require a computer that supports hardware acceleration.

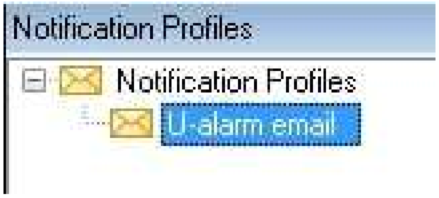
5. Fill in the *Recipients* field with the e-mail addresses of your recipients, separated by semi-colons.
6. Set any name for the e-mail *Subject*.
7. Type in any text for the e-mail.

Optional:

By clicking on any of the items under **Add system information**, the e-mail body will automatically include them as additional information. You may also set a minimum time interval between the e-mails sent, in seconds.

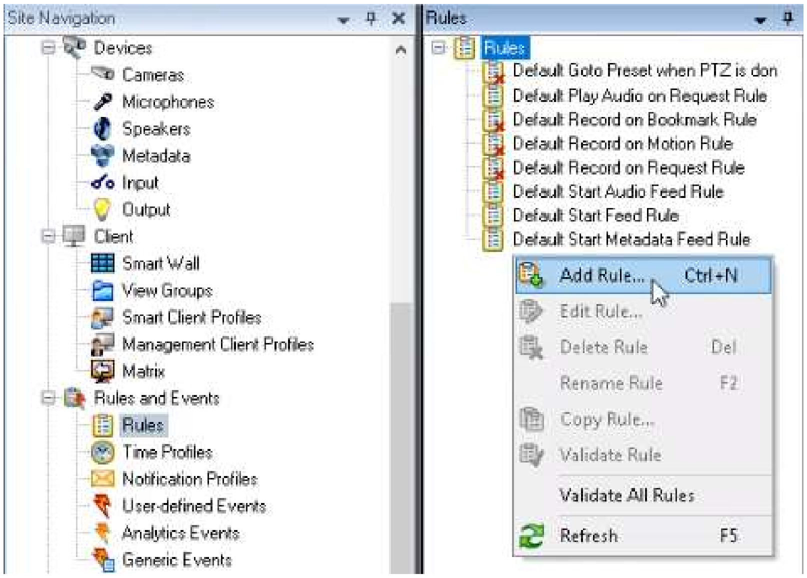
Under **Data**, you may add and configure images and videos (the latter in AVI format) of the alarms by ticking their respective boxes. You can include the images as attachment, or embedded in the e-mail by ticking the **Embed images in e-mail** box.

8. If you would like to test the settings you just configured, click *Test E-mail*.
9. Click *Finish* to save the profile, which will appear under *Notification Profiles* of the *Site Navigation Panel*.

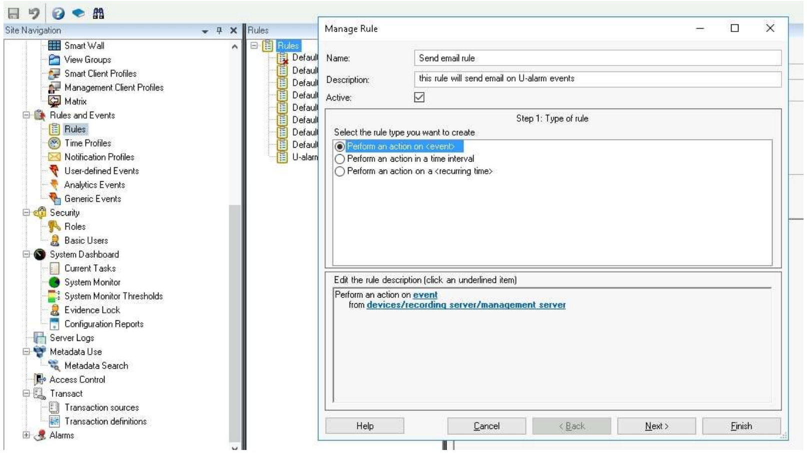


e-mail-rule*E-mail Rule*

1. In the Milestone XProtect Management Client, go to the *Site Navigation* panel => *Rules and Events* => *Rules*.
2. Right-click on the *Rules* panel => *Add Rule*



3. Set any *Name*.
4. In the *Type of rule Step (1)*, select *Perform action on event*. Click on the blue underlined "*event*" word in the lower panel.



Name: Send email rule

Description: this rule will send email on U-alarm events

Active: ☑

Step 1: Type of rule

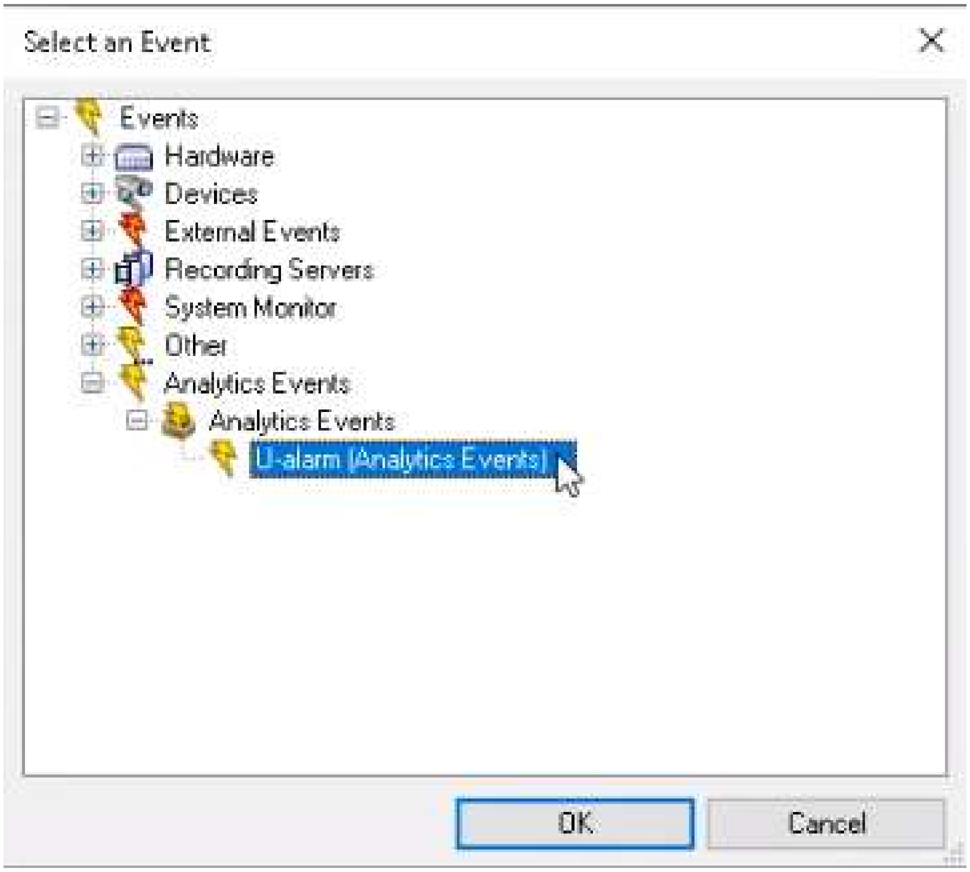
Select the rule type you want to create

● Perform an action on <event>
○ Perform an action in a time interval
○ Perform an action on a <recurring time>

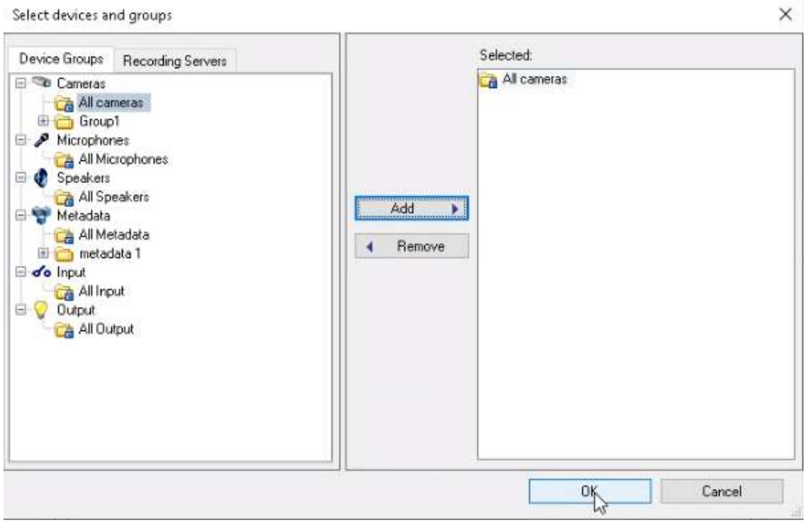
Edit the rule description (click an underlined item)

Perform an action on event
from devices/recording server/management server

5. In the pop-up, select *Events* => *Analytics Events* => ... ***U-Alarm***.

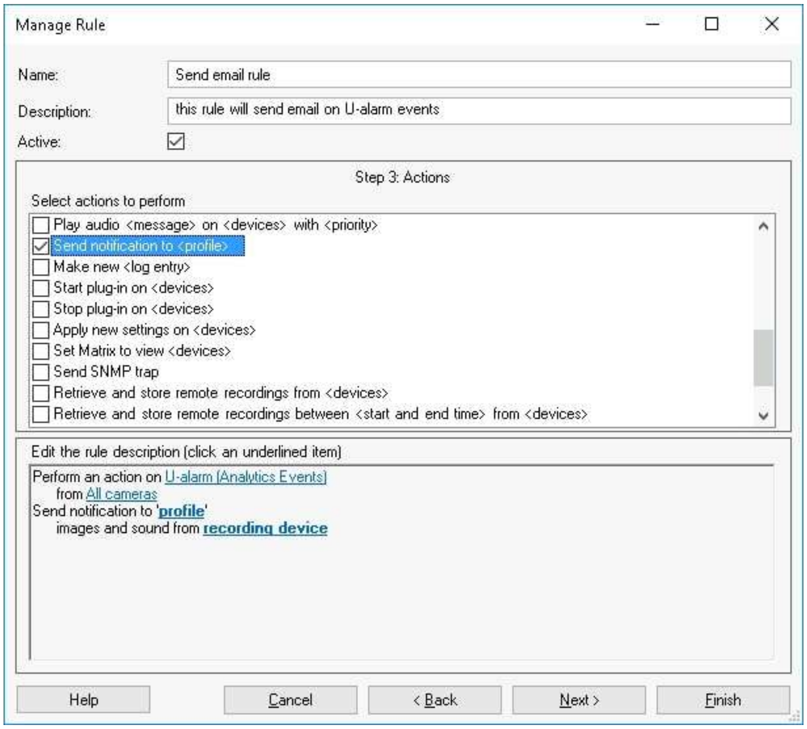


6. Click *OK*.
7. Click on the blue underlined "*devices/...*" line in the lower panel (after "*from*").
8. In the pop-up, select *Cameras* => *All cameras*. Click the *Add* button. Click *OK*.



8. Click *Next*.
9. Skip the *Conditions Step* (2). Click *Next* again.

10. In the *Actions Step* (3), select *Send notification to profile*. Click on the blue underlined "*profile*" word in the lower panel.



Manage Rule

Name: Send email rule

Description: this rule will send email on U-alarm events

Active: ☑

Step 3: Actions

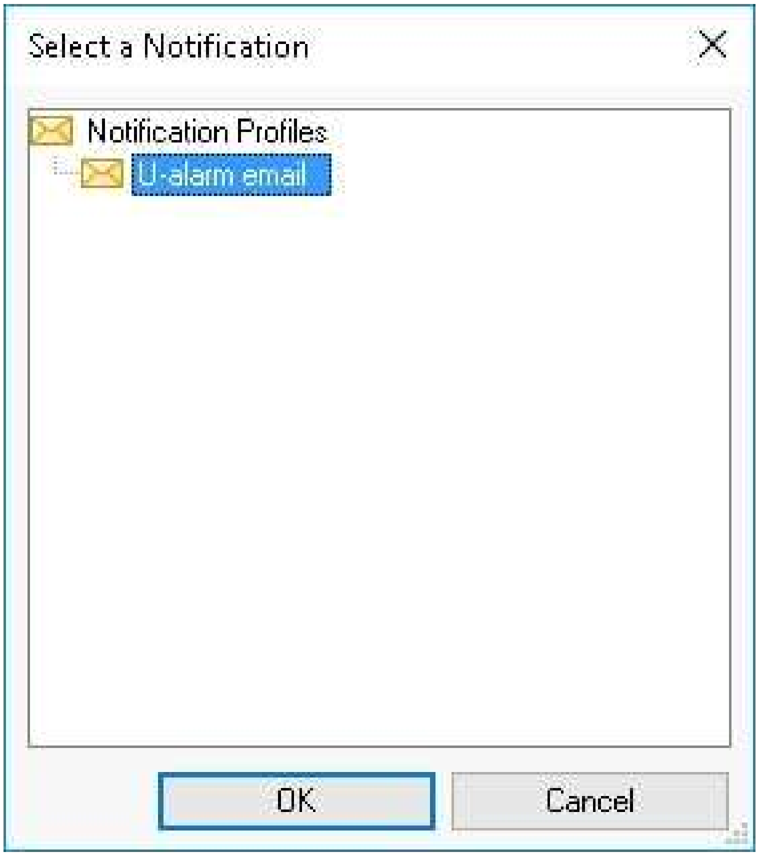
Select actions to perform

- ☐ Play audio <message> on <devices> with <priority>
- ☑ Send notification to <profile>
- ☐ Make new <log entry>
- ☐ Start plug-in on <devices>
- ☐ Stop plug-in on <devices>
- ☐ Apply new settings on <devices>
- ☐ Set Matrix to view <devices>
- ☐ Send SNMP trap
- ☐ Retrieve and store remote recordings from <devices>
- ☐ Retrieve and store remote recordings between <start and end time> from <devices>

Edit the rule description (click an underlined item)

Perform an action on U-alarm (Analytics Events)
from All cameras
Send notification to 'profile'
images and sound from recording device

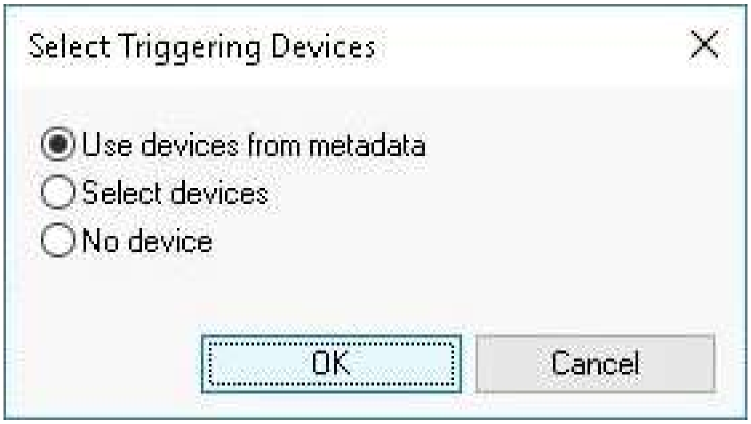
11. In the pop-up, select *U-Alarm email*, under *Notification Profiles*. Click *OK*.



Select a Notification

Notification Profiles
- U-alarm email

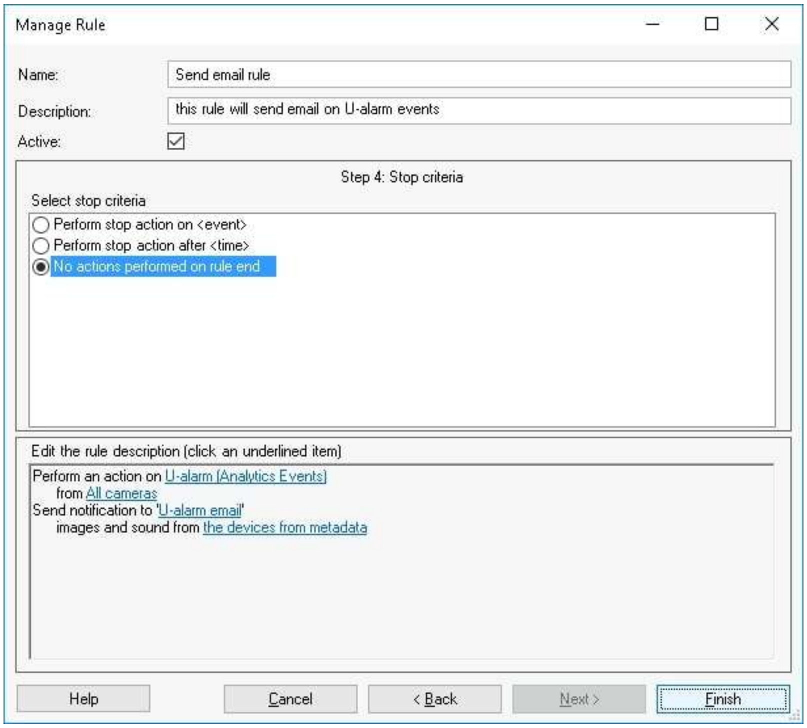
12. Click on the blue underlined "*recording device*" word in the lower panel.
13. In the pop-up, select *Use devices from metadata*. Click *OK*.



Select Triggering Devices

● Use devices from metadata
○ Select devices
○ No device

14. Click the *Next* button.
15. In the *Stop Criteria* (4) step, select *No actions performed on rule end*.



Name: Send email rule

Description: this rule will send email on U-alarm events

Active: ☑

Step 4: Stop criteria

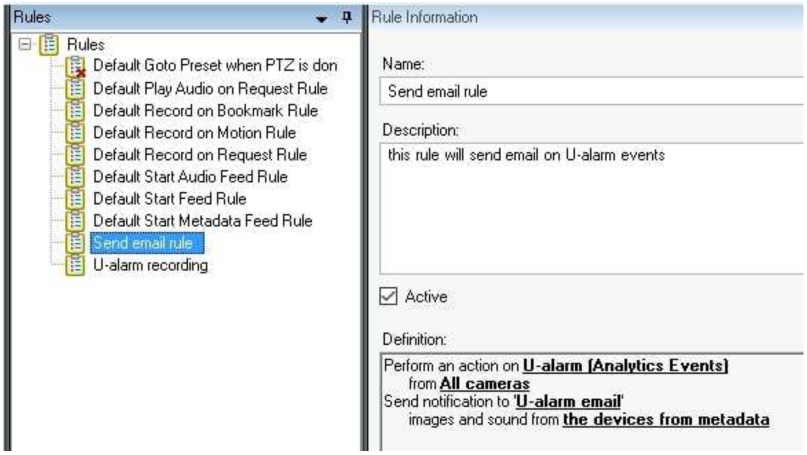
Select stop criteria

○ Perform stop action on <event>
○ Perform stop action after <time>
● No actions performed on rule end

Edit the rule description (click an underlined item)

Perform an action on U-alarm (Analytics Events)
from All cameras
Send notification to 'U-alarm email'
images and sound from the devices from metadata

16. Click *Finish*. The new rule is created and Milestone XProtect is ready to send alarms via e-mail from U-Alarm.



Rules
- Default Goto Preset when PTZ is don
- Default Play Audio on Request Rule
- Default Record on Bookmark Rule
- Default Record on Motion Rule
- Default Record on Request Rule
- Default Start Audio Feed Rule
- Default Start Feed Rule
- Default Start Metadata Feed Rule
- Send email rule
- U-alarm recording

Name: Send email rule

Description: this rule will send email on U-alarm events

☑ Active

Definition:

Perform an action on **U-alarm (Analytics Events)**
from **All cameras**
Send notification to '**U-alarm email**'
images and sound from **the devices from metadata**

All done. Recipients will receive emails upon a triggered alarm.

Connector

Compatibility

The latest version of Milestone XProtect Connector is backward compatible with U-Alarm releases older than 2.0.0 - it is therefore recommended to upgrade the Connector, as described below.

Upgrade Connector from 1.0.X to 3.0.0

1. Close the Connector 1.0.X.

2. Uninstall the Connector 1.0.X.

3. Proceed to the next section.

   NOTE: The Connector cannot use Windows credentials anymore, therefore you must create a Basic User in Milestone XProtect with Administrator privileges.

Install

1. Download U-Alarm - Milestone XProtect Connector installer.
2. Install it on the computer which runs Milestone XProtect.

Configure the Connector

1. Start the Connector service. Look for the Connector's *icon* on your system tray.

   The connector icon indicates the following states:

   - Running
   - Pending
   - Stopped

2. Double click its icon in the system tray to open the Connector's settings.

3. **Port**: The Connector uses port 10000 by default. Optionally you can set a different unused *Port* for the connector when the *Server status* is *Stopped*.:

   - Click the *Stop Server* button. This will enable the *Port* setting.

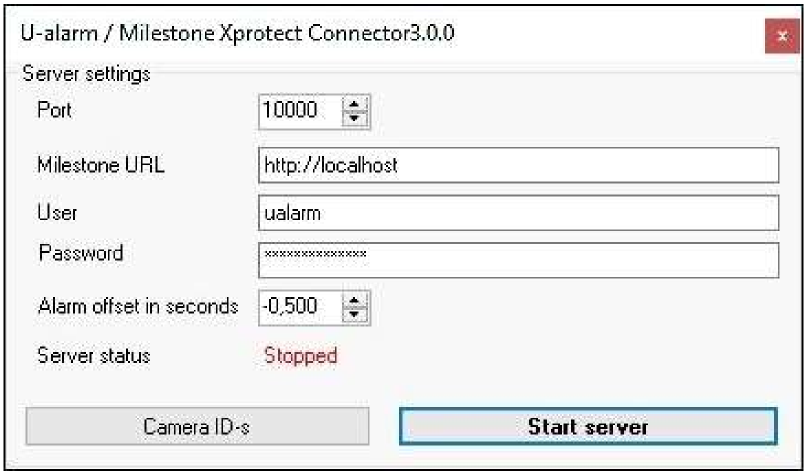
   - Set any other unused *Port* number.

NOTE: Please make sure your Windows Firewall on Connector's server is configured properly (enable communication through TCP 10000 port) or turned off.

NOTE: Remember the **static IP address** of this machine and the **port** you have set for it will be used in U-Alarm later.

4. **Milestone URL**: set the Milestone XProtect server's address.

5. **User** and **Password**: set the Milestone XProtect credentials you have created before.



U-alarm / Milestone Xprotect Connector3.0.0

Server settings

Port: 10000

Milestone URL: http://localhost

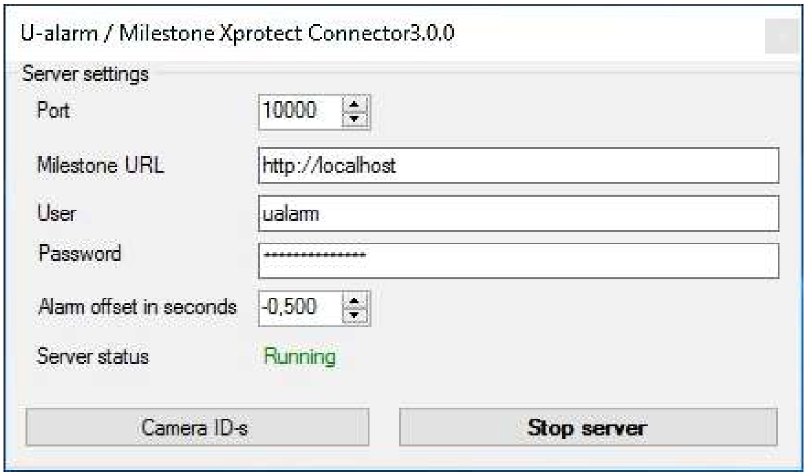
User: ualarm

Password: **************

Alarm offset in seconds: -0,500

Server status: Stopped

6. Click the *Start Server* button. The Server status will change to *Running*.



U-alarm / Milestone Xprotect Connector3.0.0

Server settings

Port: 10000

Milestone URL: http://localhost

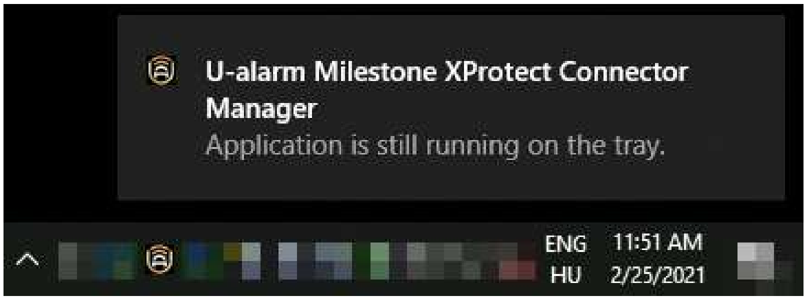
User: ualarm

Password: **************

Alarm offset in seconds: -0,500

Server status: Running

7. Everything is set. You can close the window - the service will continue running.



U-alarm Milestone XProtect Connector Manager

Application is still running on the tray.

Additional information:

- You can always stop or restart the service by right-clicking on the tray icon and selecting the Stop/Start server option.
- To re-open the settings view to modify the connection or credential settings double click the tray icon.
- On the settings view, you can always check the cameras registered to Milestone XProtect with their GUID. Click the *Camera ID-s* button for this list. Note that you must close and reopen the list dialog whenever you add (or remove) more cameras to Milestone XProtect.

- You can configure an alarm time offset in seconds. The default value is -0.5 seconds.

U-Alarm

Now U-Alarm can be configured as described in the User's guide, with a few extra steps. Please come back to this article after you have finished setting up U-Alarm.

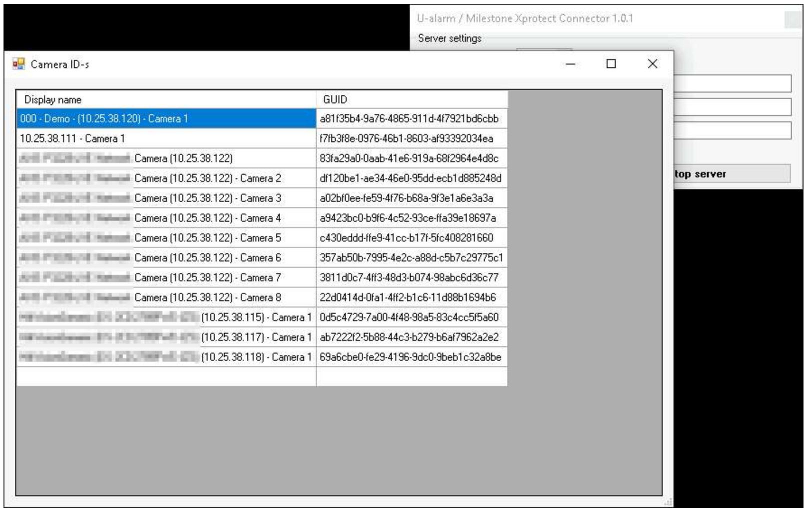
Cameras

Each camera's Technical name in U-Alarm should match its GUID in Milestone XProtect. Camera GUID's can be obtained from either the Connector or from Milestone XProtect.

How to get the GUID

option-1-get-the-guid-from-the-connector*Option 1: Get the GUID from the Connector*

1. Open the Connector.
2. Click on the *Camera ID-s* button.



Display name	GUID
000 - Demo - (10.25.38.120) - Camera 1	a81f35b4-9a76-4865-911d-4f7921bd6cbb
10.25.38.111 - Camera 1	f7fb3f8e-0976-46b1-8603-af93392034ea
[redacted] Camera (10.25.38.122)	83fa29a0-0aab-41e6-919a-68f2964e4d8c
[redacted] Camera (10.25.38.122) - Camera 2	df120be1-ae34-46e0-95dd-ecb1d885248d
[redacted] Camera (10.25.38.122) - Camera 3	a02bf0ee-fe59-4f76-b68a-9f3e1a6e3a3a
[redacted] Camera (10.25.38.122) - Camera 4	a9423bc0-b9f6-4c52-93ce-ffa39e18697a
[redacted] Camera (10.25.38.122) - Camera 5	c430eddd-ffe9-41cc-b17f-5fc408281660
[redacted] Camera (10.25.38.122) - Camera 6	357ab50b-7995-4e2c-a88d-c5b7c29775c1
[redacted] Camera (10.25.38.122) - Camera 7	3811d0c7-4ff3-48d3-b074-98abc6d36c77
[redacted] Camera (10.25.38.122) - Camera 8	22d0414d-0fa1-4ff2-b1c6-11d88b1694b6
[redacted] (10.25.38.115) - Camera 1	0d5c4729-7a00-4f48-98a5-83c4cc5f5a60
[redacted] (10.25.38.117) - Camera 1	ab7222f2-5b88-44c3-b279-b6af7962a2e2
[redacted] (10.25.38.118) - Camera 1	69a6cbe0-fe29-4196-9dc0-9beb1c32a8be

3. Copy the GUID of the respective camera.

Note: In this version, the camera list cannot be refreshed unless you close and reopen the list's window.

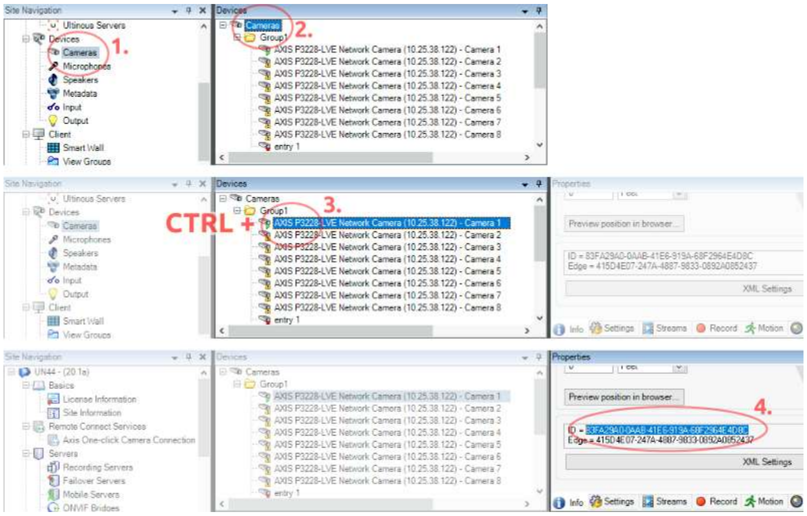
4. Paste it in U-Alarm as the Technical name. Please create or update each camera setting in U-Alarm accordingly.

option-2-get-the-guid-from-milestone-xprotect*Option 2: Get the GUID from Milestone XProtect*

1. In the *Milestone XProtect Management Client*, go to the *Site Navigation* panel => *Cameras*.

Note: This can be a little bit tricky so please follow this guide carefully.

2. In the *Devices* panel, find the *Cameras* root node and click on it.
3. Now (without clicking anywhere else) hold **CTRL** key and click on the **specific camera**.
4. In the *Properties* panel on the right, under the *Info* tab, you will find the *ID* (GUID).



- Ultinous Servers
- Devices
  - Cameras
  - Microphones
  - Speakers
  - Metadata
  - Input
  - Output
- Client
  - Smart Wall
  - View Groups

- UN44 - (20.1a)
  - Basics
    - License Information
    - Site Information
  - Remote Connect Services
    - Axis One-click Camera Connection
  - Servers
    - Recording Servers
    - Failover Servers
    - Mobile Servers
    - ONVIF Bridges

- Cameras
  - Group1
    - AXIS P3228-LVE Network Camera (10.25.38.122) - Camera 1
    - AXIS P3228-LVE Network Camera (10.25.38.122) - Camera 2
    - AXIS P3228-LVE Network Camera (10.25.38.122) - Camera 3
    - AXIS P3228-LVE Network Camera (10.25.38.122) - Camera 4
    - AXIS P3228-LVE Network Camera (10.25.38.122) - Camera 5
    - AXIS P3228-LVE Network Camera (10.25.38.122) - Camera 6
    - AXIS P3228-LVE Network Camera (10.25.38.122) - Camera 7
    - AXIS P3228-LVE Network Camera (10.25.38.122) - Camera 8
    - entry 1

ID = 83FA29A0-0AAB-41E6-919A-68F2964E4D8C
Edge = 415D4E07-247A-4887-9833-0892A0852437

3. Select the ID value and copy it to your clipboard.

Note: Make sure that you don't copy any leading or tailing spaces. It is recommended to create a note about these ID-s.

4. Paste it in U-Alarm as the Technical name. Please create or update each camera setting in U-Alarm accordingly.

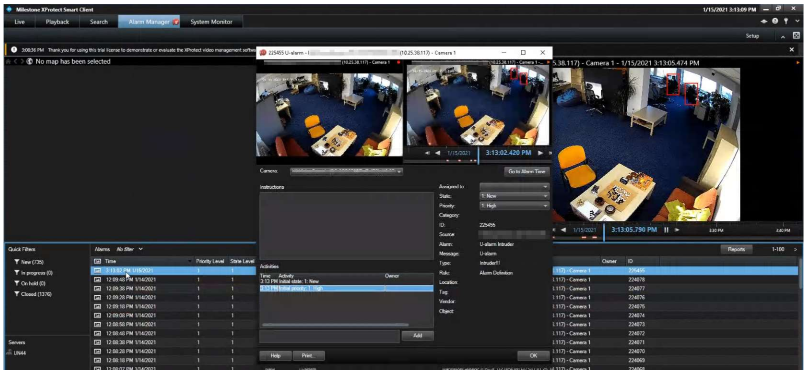
Alarms

1. Edit an existing Alarm or create a new one in U-Alarm.
2. Enable *HTTP client settings* in the form by clicking on the switch.
3. Set the *Target url* to the Connector's address using the location and the port you have memorized before, e.g. http://192.168.1.123:10000.
4. Submit your settings.

Receiving alarms in Milestone XProtect

Alarms through the Alarm Manager

Whenever an Alarm is triggered by U-Alarm, it should be visible in Milestone XProtect Smart Client under the *Alarm Manager* tab with annotations.



3:08:36 PM Thank you for using this trial license to demonstrate or evaluate the XProtect video management softwa

225455 U-alarm - [redacted] (10.25.38.117) - Camera 1

1/15/2021 3:13:02.420 PM

5.38.117) - Camera 1 - 1/15/2021 3:13:05.474 PM

1/15/2021 3:13:05.790 PM

Camera: [redacted]

Instructions

Assigned to:
State: 1: New
Priority: 1: High
Category:
ID: 225455
Source: [redacted]
Alarm: U-alarm Intruder
Message: U-alarm
Type: Intruder!!!
Rule: Alarm Definition
Location:
Tag:
Vendor:
Object:

Activities

Time	Activity	Owner
3:13 PM	Initial state: 1: New	
3:13 PM	Initial priority: 1: High	

Quick Filters
- New (735)
- In progress (0)
- On hold (0)
- Closed (1376)

Servers
- UN44

Alarms No filter

Time	Priority Level	State Level
3:13:02 PM 1/15/2021	1	1
12:09:48 PM 1/14/2021	1	1
12:09:38 PM 1/14/2021	1	1
12:09:28 PM 1/14/2021	1	1
12:09:18 PM 1/14/2021	1	1
12:09:08 PM 1/14/2021	1	1
12:08:58 PM 1/14/2021	1	1
12:08:48 PM 1/14/2021	1	1
12:08:38 PM 1/14/2021	1	1
12:08:28 PM 1/14/2021	1	1
12:08:18 PM 1/14/2021	1	1
12:08:07 PM 1/14/2021	1	1

Owner	ID
	225455
	224078
	224077
	224076
	224075
	224074
	224073
	224072
	224071
	224070
	224069

The metadata in the alarms:

- Name: The name of the alarm in *Milestone XProtect*.
- Message: U-Alarm (cannot be changed).
- Type: The name of the alarm in *U-Alarm.*

Alarms via E-mail

Recipients are receiving alarms according to the E-mail notification settings.

Troubleshooting

U-Alarm Connector can not be started

- Please make sure that the location of Milestone XProtect server is available
- Please make sure that the Milestone XProtect credentials are correct and the user has Administrator privileges in Milestone XProtect.

Milestone XProtect does not receive Alarms from U-Alarm

- Please double check all settings in Milestone XProtect.

Please check whether:

- The U-Alarm Connector is running
  - If not, please start the Connector and make sure that it is in *RUNNING* state.
- Milestone XProtect credentials are set well in the Connector.
  - Please update the credentials if needed.
- The window firewall is off or the communication is enabled so the location and the port is accessible for U-Alarm.
  - If these settings are fine, it means that U-Alarm Connector does not receive Alarms from U-Alarm. Please proceed to the next issue.

U-Alarm Connector does not receive Alarms from U-Alarm

- Please make sure that the network location of the connector is set well in U-Alarm's Alarm.
- Please double check that **your camera's Technical name in U-Alarm matches its GUID in Milestone XProtect**.
- Under Events in U-Alarm, please check whether U-Alarm detects incidents. If you can not find a recent record, it means U-Alarm does not trigger Alarms. In this case, please proceed to the next issue.

U-Alarm does not trigger Alarms

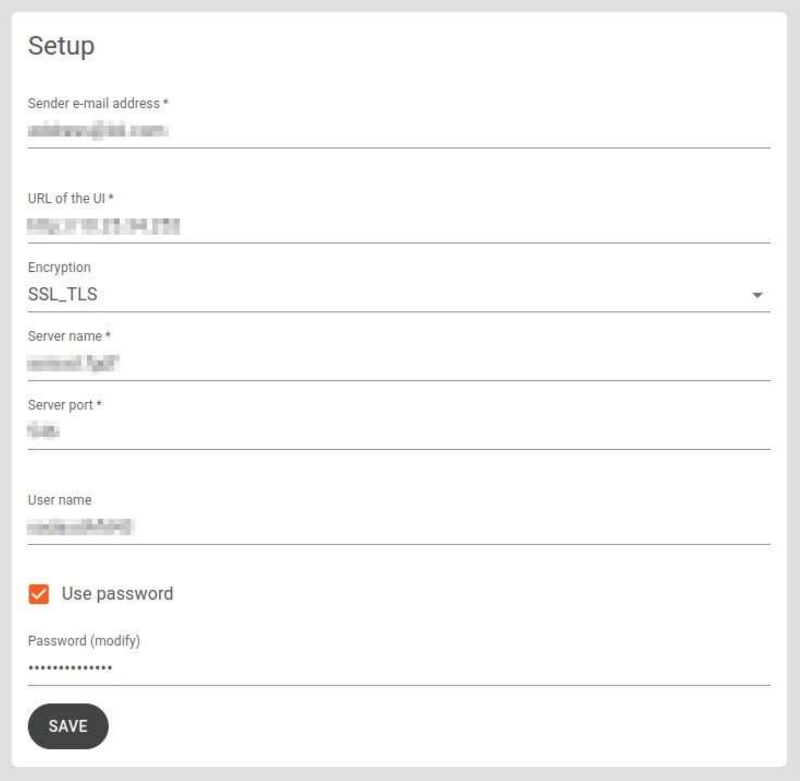
- Please double check the configuration of your Alarm in U-Alarm, especially the Sensitivity and the Filter Area (ROI) settings.

Alarms via E-mail

U-Alarm allows you to send alarms via e-mail. The service can be set up to be used by either human beings or automated systems.

The following section walks you through the steps needed to have a working setup.

Sender Configuration



Setup

Sender e-mail address *
[redacted]

URL of the UI *
[redacted]

Encryption
SSL_TLS

Server name *
[redacted]

Server port *
[redacted]

User name
[redacted]

☑ Use password

Password (modify)
••••••••••••••

1. In U-Alarm, navigate to the **System** section of the Control Panel, then click the **E-mail** box.

2. **Sender e-mail address**: Type the e-mail address you would like to send the alarms from.

3. **URL of the UI**: This is the URL of the U-Alarm platform that you are using at the moment of configuration. It is filled in for you by default.

   If the recipient(s) accesses U-Alarm from a different address than the sender (**Note**: this is and advanced, optional step - proceed only if you are confident), you may enter the URL of the U-Alarm the recipient is using.

4. **Encryption** (optional): Some e-mail providers require encryption. Two types can be set here: STARTTLS and SSL_TLS.

5. **Server name**: The name of the smtp server to send the alarms from. E.g. *smtp.gmail.com*.

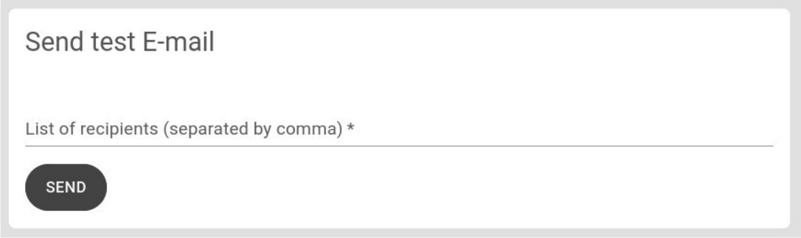
6. **Port name**: Enter the port of the smtp server used to send the alarms from.

7. **User name** and **Password** (optional): If your e-mail server requires user credentials to send e-mail, you can optionally set them here.

8. Click the **Save** button.

NOTE: Custom CA certificates can be uploaded in the Trusted Certificates setting.

Test email



Send test E-mail

List of recipients (separated by comma) *

Once you are finished with the configuration, you can test it here. Type in the list of recipients, separated by comma, then click the **Send** button. If configured properly, the recipients should receive a test alarm shortly.

Recipient configuration

Each alarm can be set up to have different sets of recipients. Therefore the configuration of recipients is done individually, on an alarm-by-alarm basis.

1. Open the **Alarms** panel of U-Alarm.

2. Click the alarm you would like to setup with recipients and scroll down to the bottom of the page.

3. Tick the **Enable email notification** button.

4. Type in a list of the desired recipients, separated by comma.

5. Click the **Save** button.

E-mail format

The e-mail provides information about the alarm in three ways: in the subject, in the e-mail body, and as an attachment, in .json format. This attachment can be used by automated systems - the schema is the same as described in Custom integration.

The structure of the e-mail body is as follows:

- Alarm name

- Timestamp
- **More info**: Includes a link to the respective event's screen in the U-Alarm web interface.

The subject is formatted according to the template: "[U-Alarm notification] <*Alarm name*> [<*timestamp*>]".

Custom Integration

U-Alarm is not only a standalone solution but can be used in an integrated system as well. All important information that belongs to an incident (eg. location, timestamp, detection coordinates, etc.) can be sent instantly to a third party software.

HTTP message

An external API endpoint can be set for each alarm. Whenever an alarm is triggered, a **POST** message will be sent to the API with metadata that belongs to the incident.

Message schema

The content type of messages is ***application/json***. The content is described in proto in this document.

```
message Event{
  enum Type
  {
    UNKNOWN = 0;
    CROWD_DETECTION = 1; ///< result of Crowd detection
    INTRUSION_DETECTION = 2; ///< result of Intrusion detection
    MULTI_OBJECT_DETECTION = 3; ///< result of Multi object detection
  }

  string id = 1; ///< Global unique id of current event
  uint64 timestamp = 2; ///< Timestamp of the last video frame in window
  string display_name = 3; ///< Human readable name of source alarm
configuration
  Type type = 4; ///< Type of source alarm configuration
  string config_id = 5; ///< id of source alarm configuration
  bool heartbeat = 6;

  oneof value
  {
    CrowdDetectionDetails crowd_detection_details = 7; ///< Only for
type=CROWD_DETECTION
    IntrusionDetectionDetails intrusion_detection_details = 8; ///< Only for
type=INTRUSION_DETECTION. Not set when heartbeat is true
```

```
    IntrusionDetectionDetails multi_object_detection_details = 9; ///< Only
for type=MULTI_OBJECT_DETECTION. Not set when heartbeat is true
  }
}

message CrowdDetectionDetails {
  int32 num_of_people = 1; ///< Number of detected people
  repeated CameraRecord sources = 2; ///< Detection details per camera
}

message IntrusionDetectionDetails {
  CameraRecord source = 1; ///< Detection detail from last frame
  bool end_of_event = 2; ///< If true, Intrusion is over
}

message CameraRecord {
  string camera_id = 1; ///< ID of current camera
  string camera_display_name = 2; ///< Display name of current camera
  string camera_technical_name = 3; ///< Technical name of current camera
  int32 width = 4; ///< Frame width of the video stream
  int32 height = 5; ///< Frame height of the video stream
  string source_topic = 6; ///< Source topic name of detection
  uint64 frame_timestamp = 7; ///< Timestamp of current video frame
  repeated Detection detections = 8; ///< Details of detections
}

message Detection {
  ObjectType type = 1; ///< Type of detected object.
  Rect bounding_box = 2; ///< Rectangular box containing the detection.
  float detection_confidence = 3; ///< Confidence of the detection. Range:
[0..1]
}

enum ObjectType
{
  PERSON_HEAD = 0; ///< Head detection result type. Supported event type
CROWD_DETECTION
  PERSON_FULL_BODY = 1; ///< Person detection result type. Supported event
type INTRUSION_DETECTION
  CAR = 2; ///< Car detection result type. Supported event type
INTRUSION_DETECTION
  BUS = 3; ///< Bus detection result type. Supported event type
INTRUSION_DETECTION
  BOAT = 4; ///< Boat detection result type. Supported event type
INTRUSION_DETECTION
  TRUCK = 5; ///< Truck detection result type. Supported event type
INTRUSION_DETECTION
  MOTORCYCLE = 6; ///< Motorcycle detection result type. Supported event type
INTRUSION_DETECTION
```

```
  BICYCLE = 7; ///< Bicycle detection result type. Supported event type
INTRUSION_DETECTION
  TRAIN = 8; ///< Train detection result type. Supported event type
INTRUSION_DETECTION
  AIRPLANE = 9; ///< Airplane detection result type. Supported event type
INTRUSION_DETECTION
}

/**  Rectangle
unit: pixels
*/
message Rect {
  int32 x = 1; ///< Horizontal coordinate of the upper left corner.
  int32 y = 2; ///< Vertical coordinate of the upper left corner.
  uint32 width = 3; // Rectangle width in pixels.
  uint32 height = 4; // Rectangle height in pixels.
}

/** Two dimensional point
range: [(0,0)..(width,height)); (0,0) is upper left corner
unit: pixels
*/
message Point {
  int32 x = 1; ///< Horizontal coordinate
  int32 y = 2; ///< Vertical coordinate
}
```

intrusion-detection-example*Intrusion detection example*

```
{
  "id": "1611842334668@mvp01.alert8.Event.json",
  "timestamp": 1611842334668,
  "display_name": "Test Intrusion Det.",
  "type": "INTRUSION_DETECTION",
  "config_id": "alert8",
  "heartbeat": false,
  "crowd_detection_details": null,
  "intrusion_detection_details": {
    "source": {
      "camera_id": "cam2",
      "camera_display_name": "cam2 (117)",
      "camera_technical_name": "cam2 tech. name",
      "width": 1920,
      "height": 1080,
      "source_topic":
"mvp01.cam2alert8DetFilterPort.ObjectDetectionRecord.json",
      "frame_timestamp": 1611842334668,
      "detections": [
        {
          "type": "PERSON_FULL_BODY",
          "bounding_box": {
```

```
      "x": 0,
      "y": 10,
      "width": 44,
      "height": 55
     },
     "detection_confidence": 0.9
    }, {
     "type": "BUS",
     "bounding_box": {
      "x": 28,
      "y": 32,
      "width": 54,
      "height": 45
     },
     "detection_confidence": 0.9
    }
   ]
  },
  "end_of_event": false
 },
 "multi_object_detection_details": null
}
```

multi-object-detection-example*Multi object detection example*

```
{
 "id": "1611842334668@mvp01.alert8.Event.json",
 "timestamp": 1611842334668,
 "display_name": "Test Intrusion Det.",
 "type": "MULTI_OBJECT_DETECTION",
 "config_id": "alert8",
 "heartbeat": false,
 "crowd_detection_details": null,
 "intrusion_detection_details": null,
 "multi_object_detection_details": {
  "source": {
   "camera_id": "cam2",
   "camera_display_name": "cam2 (117)",
   "camera_technical_name": "cam2 tech. name",
   "width": 1920,
   "height": 1080,
   "source_topic":
"mvp01.cam2alert8DetFilterPort.ObjectDetectionRecord.json",
   "frame_timestamp": 1611842334668,
   "detections": [
    {
     "type": "PERSON_FULL_BODY",
     "bounding_box": {
      "x": 0,
      "y": 10,
      "width": 44,
            "height": 55
          },
          "detection_confidence": 0.9
        }, {
          "type": "BUS",
          "bounding_box": {
            "x": 28,
            "y": 32,
            "width": 54,
            "height": 45
          },
          "detection_confidence": 0.9
        }
      ]
    },
    "end_of_event": false
  }
}
```

end-of-event*End of event*

It is possible to include an *End of Event* timestamp, which triggers if 5 seconds have passed without incidents after the initial event that triggered the HTTP message. *End of Event* occurs once the incident is over.

- End of intrusion detection:

```
{
  "id": "1611842334668@mvp01.alert8.Event.json",
  "timestamp": 1611842340668,
  "display_name": "Test Intrusion Det.",
  "type": "INTRUSION_DETECTION",
  "config_id": "alert8",
  "heartbeat": false,
  "crowd_detection_details": null,
  "intrusion_detection_details": {
    "source": {
      "camera_id": "cam2",
      "camera_display_name": "cam2 (117)",
      "camera_technical_name": "cam2 tech. name",
      "width": 1920,
      "height": 1080,
      "source_topic":
"mvp01.cam2alert8DetFilterPort.ObjectDetectionRecord.json",
      "frame_timestamp": 1611842334668,
      "detections": []
    },
    "end_of_event": true
  },
  "multi_object_detection_details": null
}
```

- End of multi object detection:

```
{
  "id": "1611842334668@mvp01.alert8.Event.json",
  "timestamp": 1611842334668,
  "display_name": "Test Intrusion Det.",
  "type": "MULTI_OBJECT_DETECTION",
  "config_id": "alert8",
  "heartbeat": false,
  "crowd_detection_details": null,
  "intrusion_detection_details": null,
  "multi_object_detection_details": {
    "source": {
      "camera_id": "cam2",
      "camera_display_name": "cam2 (117)",
      "camera_technical_name": "cam2 tech. name",
      "width": 1920,
      "height": 1080,
      "source_topic":
"mvp01.cam2alert8DetFilterPort.ObjectDetectionRecord.json",
      "frame_timestamp": 1611842334668,
      "detections": []
    },
    "end_of_event": true
  }
}
```

NOTE 1: `detections` is an empty array, and `end_of_event` is *true*.

NOTE 2: the `id` of this event is unique and it does **not** refer to any former event. This means that all events with this `display_name` and `type` are to be considered as having ended.

crowd-detection-example*Crowd detection example*

```
{
  "id": "1606727720510@mvp01.alert12.Event.json",
  "timestamp": 1606727720510,
  "display_name": "first alarm",
  "type": "CROWD_DETECTION",
  "config_id": "alert.12",
  "heartbeat": false,
  "crowd_detection_details": {
    "num_of_people": 1,
    "sources": [
      {
        "camera_id": "cam.1",
        "camera_display_name": "first cam",
        "camera_technical_name": "Outer_ID_01",
        "width": 1920,
        "height": 1080,
        "source_topic":
"mvp01.cam1alert12DetFilterPortObjectDetectionRecord.json",
        "frame_timestamp": 1606727720510,
        "detections": []
      }, {
        "camera_id": "cam.10",
        "camera_display_name": "second cam",
        "camera_technical_name": "Outer_ID_02",
        "width": 1920,
        "height": 1080,
        "source_topic":
"mvp01.cam10alert12DetFilterPortObjectDetectionRecord.json",
        "frame_timestamp": 1606727720478,
        "detections": [
          {
            "type": "PERSON_HEAD",
            "bounding_box": {
              "x": 1052,
              "y": 415,
              "width": 89,
              "height": 112
            },
            "detection_confidence": 0.99902487
          }
        ]
      }
    ]
  },
  "intrusion_detection_cascading_details": null,
  "multi_object_detection_details": null
}
```

Snapshot sending

If enabled, Snapshots are sent to the following endpoint:

[PUT] YOUR_URL/snapshot/{event_is}/{c_t_n}

Its properties are as follows:

- Content-Type: multipart/form-data
- image media type: image/jpeg

Setup message sending in U-Alarm

1. Give unique technical names to cameras. The technical name will appear in the metadata and will aid the identification of the camera.
2. Fill HTTP client settings for each alarm. Give the address, the security credentials in a custom message header (if any) and cert settings for the external API.

Counter API

U-Alarm's measurement-based counters are designed to be used with custom third party software. This guide will cover how the data created by the counters can be read from U-Alarm.

If you wish to double-check the data produced by your counters, they can be viewed inside U-Alarm as well, in a dedicated Counters interface.

Prerequisites

- Finished the Quick Start Guide and created a test Alarm to make sure that your camera is working and events are triggered. (This test Alarm can be deleted after testing.)
- Created an API Token so that the third party software has access to U-Alarm.
- Created a Multi Object Counter. Please note that the *technical name* value will be the identifier value for the API. This is a ***UUID*** by default, but can be renamed to any unique string.

Using the API

The output from each counter is a number indicating the number of detections in the union of all cameras' regions of interests (ROIs).

The API is read-only and has two main ways of accessing the counters:

- **Batch** mode, where past counter values are of interest.
- Live **Server Side Event** mode for real time processing of values.

Each **aggregation** contains:

- an `object_type` string, which is one of `PERSON_FULL_BODY, MOTORCYCLE, CAR, TRAIN, TRUCK, BUS, BICYCLE, BOAT, AIRPLANE`
- a `first` integer, the number of detections in the first frame of the aggregation period
- a `last` integer, the number of detections in the last frame of the aggregation period
- an `average` float, the average number of detections
- a `median` float, the median of detections in the whole aggregation period
- a `min` integer, the sum of detections on the last frame in the aggregation period
- and a `max` integer, the sum of detections on the first frame in the aggregation period

The two API endpoints have the following parameters:

Parameter	Used in /counter/?	Value	Example value
technical_name	/batch	Counter technical name	front-yard-counter
technical_names	/live	Array of technical names	first,second,third
from_timestamp	/batch	Unix timestamp (ms)	1625216205000
to_timestamp	/batch	Unix timestamp (ms)	1625216275000

		Maximum difference between to and from is 24 hours	
token	/batch and /live	API token from U-alarm UI	2eef33b9-a2ac-457b-a076-9b43a3ab6df6

Example

```
const url = "http://<address-of-ualarm>/API"; //< note the /API at the end.
```

Batch Mode

The following example is using `javascript` and its fetch function to show how these values can be read.

```
/**
 * maximum time interval is three days
 * @param technical_name: string ;  counter technical name
 * @param token  : A base64 token issued by U-Alarm
 * @param from_timestamp : unix timestamp;  Only show counter values from
given date
 * @param to_timestamp :   unix timestamp;  Show values until.
 */
const params = new URLSearchParams({
    'from_timestamp':'unix-timestamp',
    'to_timestamp':'unix-timestamp',
    'token':'api-token',
    'technical_name':'counter-technical-name'
});

fetch(`${url}/counter/batch${params.toString()}`)
    .then( value => console.log(value.json()))
```

Example response

```
[ //< Array of aggregation periods
    {
    "from_timestamp": 1625215860000,
    "to_timestamp": 1625215865000,
    //^ next aggregation periods from_timestamp is equal to this periods
to_timestamp
    "status": "ERROR", //< status is OK or ERROR.
    "aggregations": [
      {
       "object_type": "BOAT",
       //^ out of the 9 main object types, only those will be listed in the
aggregations array that are selected in the UI
       "first": 0,
        //^ first: integer, exact number of detections on the first frame in
the aggregation period
       "last": 0,
        //^ last: integer, exact number of detections on the last frame in
the aggregation period
       "median": 0.0,
        //^ median: float, median of detections in the whole aggregation
period
       "average": 0.0,
       //^ average: float, average number of detections in the whole
aggregation period
       "min": 0,
        //^ min: integer, exact sum of detections on the first frame in the
aggregation period
       "max": 0,
        //^ max: integer, exact sum of detections on the last frame in the
aggregation period
      },
      {"object_type": "PERSON_FULL_BODY","first": 0, "last": 0, "median":
0.0, "average": 0.2, "min": 0, "max": 0},
      {"object_type": "CAR",             "first": 0, "last": 0, "median":
0.0, "average": 0.0, "min": 0, "max": 0},
      {"object_type": "MOTORCYCLE",      "first": 0, "last": 0, "median":
0.0, "average": 0.1, "min": 0, "max": 0},
      {"object_type": "AIRPLANE",        "first": 0, "last": 0, "median":
0.0, "average": 0.2, "min": 0, "max": 0},
      {"object_type": "TRAIN",           "first": 0, "last": 0, "median":
0.0, "average": 0.2, "min": 0, "max": 0},
      {"object_type": "TRUCK",           "first": 0, "last": 0, "median":
0.0, "average": 0.0, "min": 0, "max": 0},
      {"object_type": "BICYCLE",         "first": 0, "last": 0, "median":
0.0, "average": 0.0, "min": 0, "max": 0},
      {"object_type": "BUS",             "first": 0, "last": 0, "median":
0.0, "average": 0.1, "min": 0, "max": 0}
    ],
    "cameras_with_error": [
    //^ If status is ERROR, cameras_with_error array will show the cameras
that are unreachable
        {"display_name": "Front Yard", "technical_name": "frontyard-hd"}
    ]
  },

]
```

Server Side Event Mode

This demo uses `javascripts's` EventSource API to read events.

Example Request

```
const params = new URLSearchParams({
    'token':'api-token',
    'technical_names':['name-1','name2'] //< Multiple technical_names can be
requested
});
const evtPath = `${url}/counter/live?${params.toString()}`
const evtSource = new EventSource(evtPath)
evtSource.onmessage = evt => console.log(evt.data)
```

Example response

```
[ //< Array of technical_names
 {
 "technical_name": "name-1",
 "record": { //< A record contains a single aggregation period
  "from_timestamp": 1625231670000,
  "to_timestamp": 1625231675000,
  "status": "ERROR",
  "aggregations": [
    {
     "object_type": "PERSON_FULL_BODY",
     "last": 0,
     "median": 0.0,
     "average": 0.0,
     "max": 0
    },
    /*... other detections*/
  ],
  "cameras_with_error": [{"display_name": "115", "technical_name": "115"}]
 }
}, {
  "technical_name" : "name-2",
  "record" : { /*... same as above*/ }
}
]
```

Troubleshooting

Error Status Codes

- **401 Unauthorized** - Wrong API Key. Make sure a valid key is set up.
- **404 Not Found** - The `technical_name(s)` parameter is invalid.
- **502 Bad Gateway** - U-Alarm API is not running. Please try logging in to the U-Alarm User Interface, or restart the physical device.