ARAANI® Tamper Guard

V4.03.05

USER- & INSTALLATION MANUAL

Copyright Notice

This document is copyright protected and is the property of Araani NV and may not be copied, reproduced, or distributed in any way without the prior written consent of Araani NV.
©2021 Araani NV. Araani is a registered trademark of Araani NV. All other company names and products are trademarks or registered trademarks of their respective companies. We reserve the right to introduce modifications without notice.

Table of Contents

Safety and regulatory information 5

Introduction 6

About this manual 6

Product overview 6

Overview 6

Functionality description 6

How to install Araani Tamper Guard 8

System requirements 8

Camera requirements 8

AXIS streaming limitations 8

Araani Tamper Guard installation 10

Camera firmware 10

Installing the Araani Tamper Guard ACAP 11

Activating the Araani Tamper Guard license 12

Activate a trial license for Araani Tamper Guard 14

How to use Araani Tamper Guard 15

Starting / stopping Araani Tamper Guard 15

Starting Araani Tamper Guard 15

Start-up behaviour 15

Stopping Araani Tamper Guard 15

Configuring Araani Tamper Guard 16

Accessing Araani Tamper Guard configuration 16

Basic configuration of Araani Tamper Guard 17

Advanced configuration of Araani Tamper Guard 18

Working with PTZ cameras 20

Working with multi-sensor cameras 21

Configuring display options 22

View Araani Tamper Guard status 22

Maintenance and troubleshooting 24

Retrieving diagnostics information 24

Using Araani Tamper Guard with Axis Live Privacy Shield (ALPS) 25

Integration of Araani Tamper Guard with VMS systems 26

Integration with Milestone XProtect 26

Integration with Genetec Security Center 29

Integration with Axis Camera Station 32
Other VMS systems 37
Technical specification 38
Functional specification 38
System requirements 38
Addendum: Araani Application EULA 39

Safety and regulatory information

Definition of symbols

Hazard statements

Danger:	Indicates a hazardous situation which, if not avoided, *will* result in serious injury or death.
Warning:	Indicates a hazardous situation which, if not avoided, *could* result in serious injury or death.
Caution:	Indicates a hazardous situation which, if not avoided, *might* result in moderate or minor injury.
Notice:	Indicates a situation which, if not avoided, might result in property damage or in an undesirable result or state.

Others

Information:	Indicates a shortcut or any other useful indication.
Attention:	Indicates an element which requires extra attention, not necessarily a hazard

Safety information

Attention:
Please read this document carefully before installing or using Araani Tamper Guard.
This document must be kept for future reference.

Liability

Every care has been taken in the preparation of this document. Please inform Araani NV of any inaccuracies or omissions. Araani NV cannot be held responsible for damage caused by technical or typographical errors and reserves the right to make changes to the product and manuals without prior notice. Araani NV makes no warranty of any kind regarding the material contained within this document, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Araani NV shall not be liable nor responsible for incidental or consequential damages in connection with the furnishing, performance or use of this material. This product is only to be used for its intended purpose.

Trademark acknowledgements

AXIS COMMUNICATIONS and AXIS are registered trademarks or trademark applications of Axis AB in various jurisdictions. All other company names and products are trademarks or registered trademarks of their respective companies. Ethernet, Torx, Microsoft, Milestone, Genetec and WWW are registered trademarks of the respective holders.

Contact and support

Should you require any technical assistance, please contact your Araani reseller. If your questions cannot be answered immediately, your reseller will forward your queries through the appropriate channels to ensure a rapid response.
If you are a reseller, please contact your direct contact person, or contact our support staff via support@araani.com.

Araani NV; Luipaardstraat 12; 8500 Kortrijk (Belgium)		
info@araani.com	http://www.araani.com	Tel. : +32 (0)56 49 93 94

Introduction

About this manual

This manual describes the installation and usage of Araani Tamper Guard software.
Please read this document carefully before installing, using, or interacting with the Araani Tamper Guard software or products running this software.
The manual expects the reader to have some basic knowledge about video surveillance and the use of cameras.
Please refer to the camera documentation for any information that is related to the use, installation, or restrictions of the camera on which this software is or will be installed.

Information: Illustrations of Axis camera interface throughout this manual are taken from the new web interface. Your camera interface may have a slightly different layout or may be using the legacy interface. Still, all indicated functions will be valid; the interface does not affect the functionality.

Product overview

Overview

Araani Tamper Guard is an edge-based video analytics software that runs on an Axis® camera, that will trigger an alarm if it sees one of following disturbances in the video image, related to the visual quality:

- Tampering:
  - Blocked / blurred alarm: blocked or blurred image.
  - Exposure alarm: too bright or too dark scene.
  - Camera redirected alarm: sudden change of field of view.
- Image quality:
  - Image quality alarm: an alarm will be raised if the image quality is constantly low, under a certain threshold.
  - Image quality warning: if the image quality is approaching the Image quality alarm threshold during a certain minimum time interval.

Functionality description

Functionality		Description	Event type
Tampering	BLOCKING-BLURRING	Detection of: • Blurred image (out of focus, rain/snow/large dirt stains on lens, etc.). • Blocking of image by object or spray. This alarm remains active as long as the alarm condition is present. As soon as the image quality is restored, the alarm will automatically switch off.	"Blocked or Blurred Alarm"
	EXPOSURE	As soon as the mean brightness is below the minimum or above the maximum threshold, an alarm will be raised. This alarm remains active as long as the alarm condition is present. As soon as the image quality is restored, the alarm will automatically switch off.	"Exposure Alarm"

	CAMERA REDIRECTION	An event is reported when the field of view changed abruptly. The functionality is based on a sudden loss of the current background image and will react on any type of different background. The new field of view will be learned as new background, so after a few seconds the event is switched off.	"Camera Redirected Alarm"
IMAGE QUALITY	IMAGE QUALITY ALARM	Detection of image degradation: • Dirty camera lens. • Lens (slowly) out of focus. This alarm remains active as long as the alarm condition is present. As soon as the quality is restored, the alarm will automatically switch off.	"ImageQuality Degradation Alarm"
	IMAGE QUALITY WARNING	Optional feature to receive a warning before the image quality alarm is raised, to allow maintenance actions.	"ImageQuality Degradation Warning"
OPERATION	OPERATIONAL	Araani Tamper Guard algorithm active and running.	"Operational Signal"
	RECALIBRATING	Araani Tamper Guard algorithm is learning background. This occurs when the algorithm is starting up or when the algorithm is re-initializing after an alarm condition or PTZ movement	"Recalibrating"
	STOPPED	Araani Tamper Guard algorithm stopped. This occurs when a PTZ camera is out of preset or in an unknown preset position. This also occurs when the video stream is lost, e.g. because of processor overload.	"Stopped"

How to install Araani Tamper Guard

System requirements

CAMERA REQUIREMENTS

The Araani Tamper Guard software is compatible with a broad range of Axis® cameras. The camera needs to comply with the following characteristics:

- **Brand**: Axis® (https://www.axis.com/).
- **Model**: Verify the online compatibility list https://www.araani.com/en/solutions/surveillance/araani-fire-guard/fire-guard-camera-compatibility/
- **Chipset**: ARTPEC-6, ARTPEC-7, ARTPEC-8 or Ambarella S-8. (*)
- **Firmware**: Latest qualified Axis® LTS (= long-term support) firmware >= version 10.12.x!
  Attention: Araani Tamper Guard V4.03.05 does NOT work with Axis OS releases <=10.8.
  Firmware can be downloaded at https://www.axis.com/support/firmware.
  Refer to your camera manual on how to install firmware on the device or follow the steps under camera firmware.
- **Resolution**: 1920 x 1080 or higher.
- **Aspect ratio**: 16:9, 4:3 or 10:6 or rotated version of these. (**)

Notice: Check the Araani Tamper Guard release notes to verify what Axis software versions are compatible with your Araani Tamper Guard software version. Using an incompatible or untested version may result in malfunction, errors or performance issues.

(*) **Information:** Araani Tamper Guard is available in 4 versions: signed_TamperGuard_Vx.xx.xx_artpec6.eap, signed_TamperGuard_Vx.xx.xx_artpec7.eap, signed_TamperGuard_Vx.xx.xx_artpec8.eap and signed_TamperGuard_Vx.xx.xx_Ambarella_aarch64.eap. Verify what ARTPEC chipset your camera has and select the correct Araani Tamper Guard software.

(**) **Attention:** After changing the aspect ratio, a restart of the Araani Tamper Guard software is required.

AXIS STREAMING LIMITATIONS

In setting up your system, pay attention to the fact that total streaming video capacity of an Axis® camera may be limited. For Araani analytics to work properly, the camera should be capable of delivering an application-specific video stream. In combination with other video streams for recording, visualization, etc., the total computational capacity of the camera could be exceeded which will result in failure of the analytics.
The amount and complexity of video streams that can be delivered simultaneously by an Axis camera is limited by the performance of the processor. The computational load of a stream is expressed in megapixels per second (mps) and is calculated using the following formula:

P_{stream} = horizontal resolution (pixels) x vertical resolution (pixels) x frame rate (fps = frames per second) /1.000.000

The total streaming capacity is obtained by adding the load of all unique streams. Only unique streams are counted for as requesting twice the same video stream (same resolution, frame rate, encoding type, compression, etc.) from a camera does not require separate encoding and as such does not increase the computational requirements.

$P_{CPU} = \Sigma$ unique P_{stream}

Araani analytics requests a video stream that depends on the aspect ratio of the maximum resolution of the camera at 12 frames per second:

Aspect ratio	Analytics stream resolution	P_{Araani}
16:9	1280 x 720 @ 12 fps	11 mps
16:10	1280 x 800 @ 12 fps	12,3 mps
4:3	1280 x 960 @ 12 fps	14,8 mps

This stream should be considered when calculating the total load.
The streaming load is practically independent of the encoding type (H264 versus H265).
The maximum capacity for a camera depends on the type of processor. Currently, two generations of processor are common in the Axis offering, named ARTPEC-6 and ARTPEC-7. These are the limits for both processor types:

- ARTPEC-6 maximum total streaming capacity = approximately 310 mps.
- ARTPEC-7 maximum total streaming capacity = approximately 367 mps.
- ARTPEC-8 maximum total streaming capacity = approximately 498 mps.

In case of doubt, contact your supplier to know what processor type is used in your cameras.
As video stream compression is occurring in a dedicated part of the CPU, these limits are practically independent of other processor activities such as image optimization, mirroring or ACAP-based analytics.
For proper functioning of Araani analytics, make sure the total stream demand - including the required analytics stream - does not exceed this limit and preferably add some margin. If that limit is exceeded, the camera will lower the frame rate on ALL streams and as a result, Araani analytics will no longer work.
Example: A 4K CCTV system requires one high resolution stream for visualization and one HD resolution stream for recording. (3840 / 2160 = 16:9 aspect ratio)

Stream role	Resolution	P_{stream}
Visualization	3840 x 2160 @ 25 fps	207,4 mps
Recording	1920 x 1080 @ 25 fps	51,8 mps
Araani analytics	1280 x 720 @ 12 fps	11 mps
Total		270,2 mps

The total load in this example is well below the limit of both processor types, so this will work fine. Adding another HD recording stream with different settings for example would exceed the maximum performance of an ARTPEC-6 based camera and analytics will fail to run on such combination.

Notice: For performance reasons:

- Do not exceed streaming limits of the processor!

This can lead to malfunction of the algorithm.

Araani Tamper Guard will automatically try to re-establish a video stream connection when it is lost.
Araani Tamper Guard will generate STOPPED status when the video stream is lost and reconnection fails a number of times.

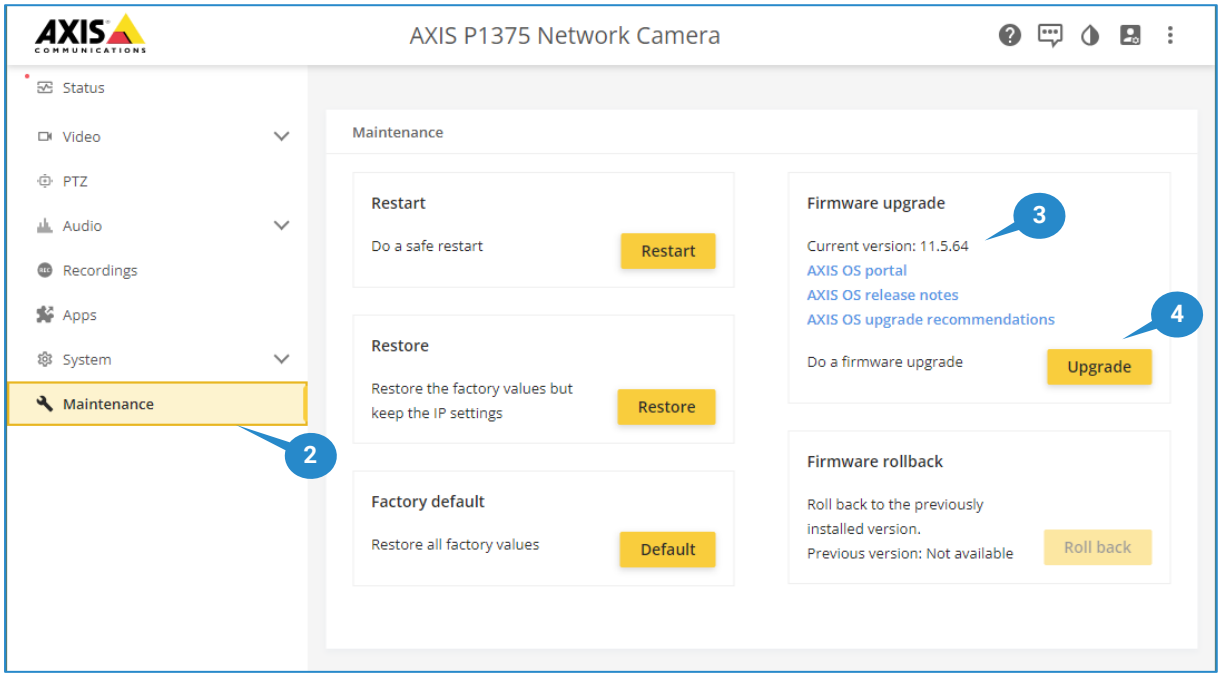
Araani Tamper Guard installation

The Araani Tamper Guard software comes as an ACAP (Axis® Camera Application Platform) compatible package. The ACAP platform allows Axis® Development Partners (ADP) to build smart applications that run on a wide range of Axis® cameras. Multiple applications can be installed and running on a camera simultaneously.
An ACAP application software package comes in the form of a single file with .eap extension. Installing the software on an Axis® camera involves uploading the file to the camera, activating the appropriate license, and potentially configuring the application parameters.

CAMERA FIRMWARE

Before installing Araani Tamper Guard software, verify if your camera has the required firmware (see: Camera requirements).
To verify the firmware version of your camera, perform the following steps:

1. Connect with a laptop, tablet, or smart phone to your camera, using your internet browser software and login to the camera webpage. Refer to the camera user manual on how to do this.
2. Select "Maintenance" from the menu pane.
3. The current firmware version is displayed in the Firmware upgrade section of the maintenance screen, as indicated in the screenshot below.



If the version is not compliant to the camera requirements for Araani Tamper Guard, you can download the required firmware from https://www.axis.com/support/firmware.
Proceed in the maintenance interface to upgrade the firmware version of your camera:

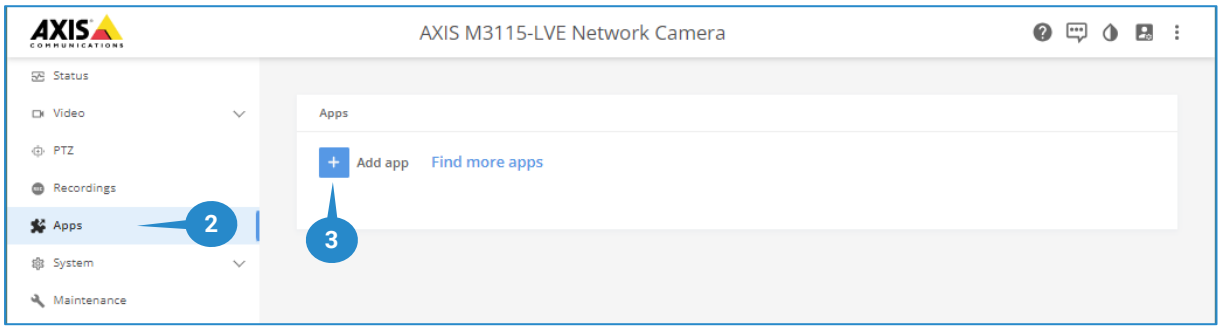
4. Select "Upgrade" and follow on-screen instructions.
5. Verify if the camera is properly upgraded by checking the version again in the maintenance menu.

Notice: In case the new (qualified LTS) firmware is a lower revision than the one that was installed, it is required to perform a factory restore (keeping IP-address/network information) after firmware downgrade to make sure that all settings are configured in a valid way.

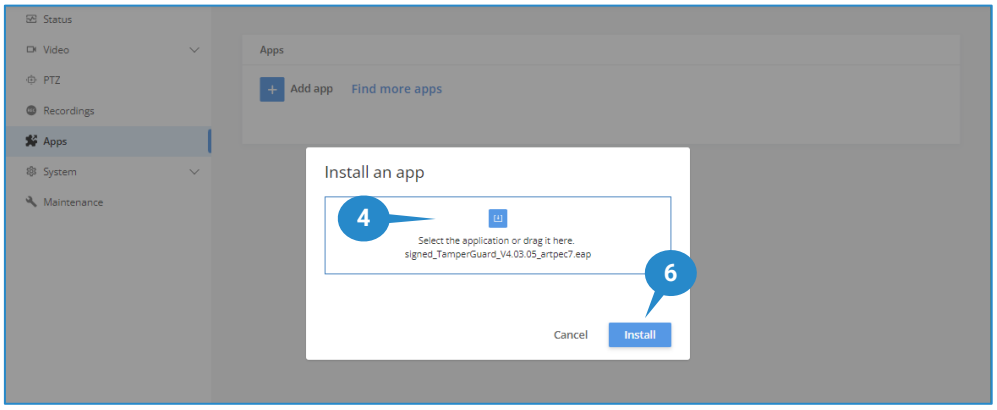
INSTALLING THE ARAANI TAMPER GUARD ACAP

To install the Araani Tamper Guard, perform the following steps:

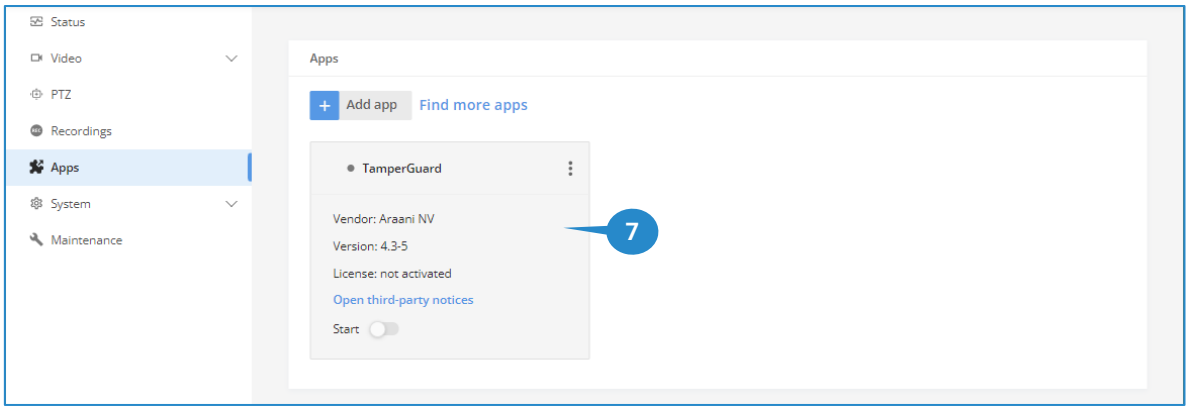
1. Connect with a laptop, tablet, or smart phone to your camera, using your internet browser software and login to the camera webpage. Refer to the camera user manual on how to do this.
2. Select “Apps” from the menu pane.
3. Select “Add App”.



4. Select the upload button to browse your local storage for the ACAP file.
5. Select Signed_TamperGuard_*Vx.xx.xx*_artpec*x*.eap.
6. Select Install.



7. The application will start installing. This may take a few minutes. After successful installation, the Araani Tamper Guard application should be visible in the “Apps” tab.



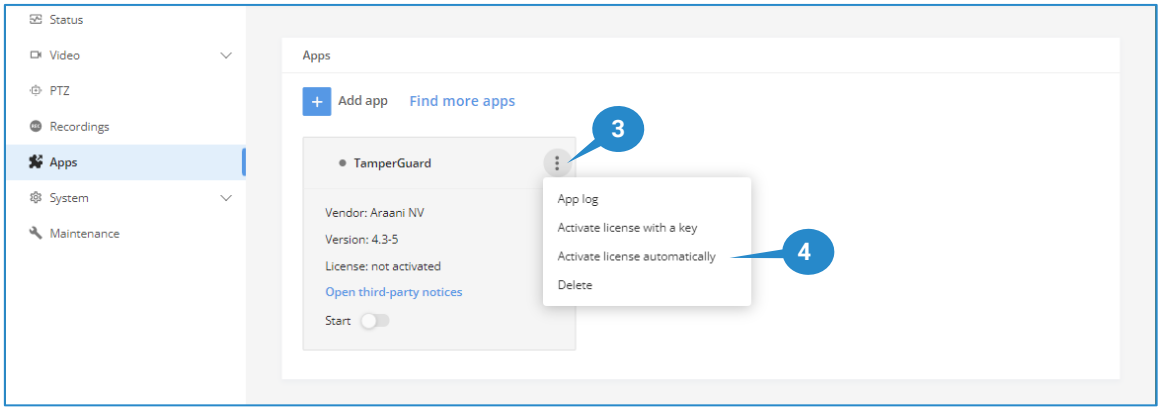
ACTIVATING THE ARAANI TAMPER GUARD LICENSE

With the purchase of Araani Tamper Guard, a **license activation code** is provided. This code is valid for a number of Araani Tamper Guard installations, as purchased.

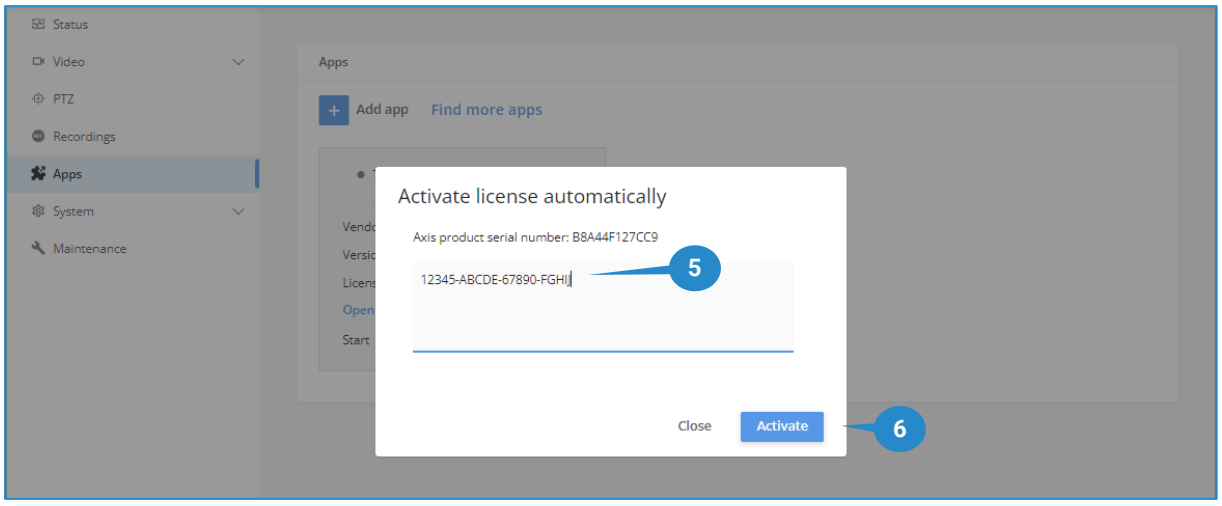
Case 1: the camera is connected to the internet

Perform the steps below to activate the Araani Tamper Guard app directly on the camera.

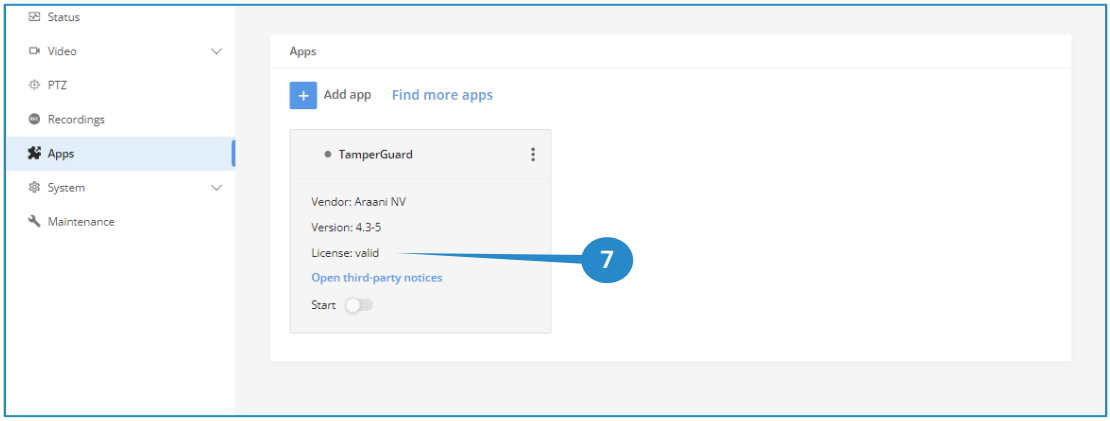
1. Connect to your camera, using your internet browser software and login to the camera webpage. Refer to the camera user manual on how to do this.
2. Select "Apps" from the menu pane.
3. Select the Araani Tamper Guard app menu button.
4. Select "Activate license automatically"



5. The license activation code can be directly entered in "Automatic license" field.
6. Select "Activate"
   The camera will connect to the Axis® licensing system. A license for this camera will be created and automatically installed on the device. The camera will be registered in the Axis® licensing system as being licensed, and the license will be linked to your license activation code and your camera.



7. When installed correctly with a valid license key, following screen should re-appear with Araani Tamper Guard License 'valid'.

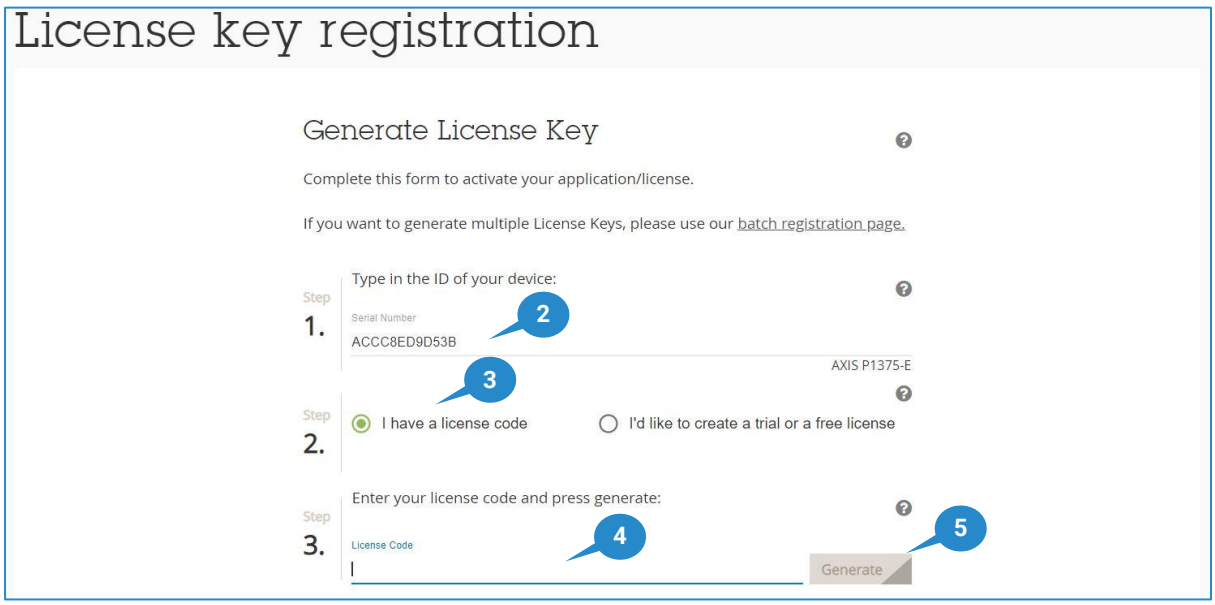


Case 2: the camera has no internet connectivity

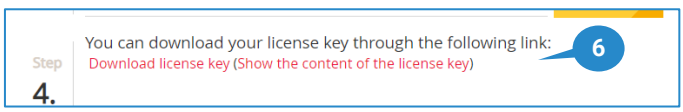
When the camera on which the Araani Tamper Guard application is installed has no direct internet connection, a license key must be generated upfront on a computer with internet connection.

To create the license key, perform the steps below.

1. Using your internet browser, connect to https://www.axis.com/products/camera-applications/license-key-registration#/registration.
2. Fill in the serial number of your camera. The serial number can be found on a sticker on your camera housing, indicated by "S/N".
3. Select "I have a license code".
4. Fill in the license activation code, received with your purchase.
5. Click "Generate".

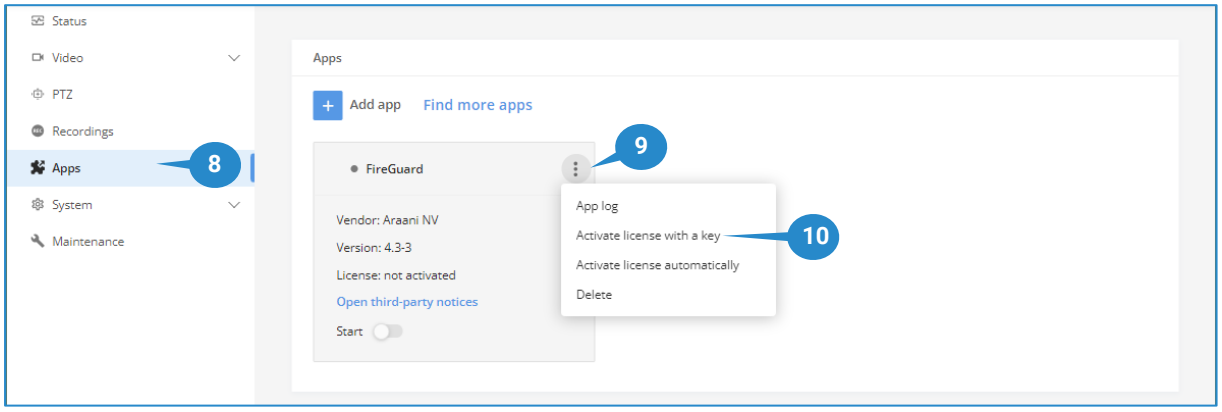


6. A message will appear from which you can download the license key to your local storage.

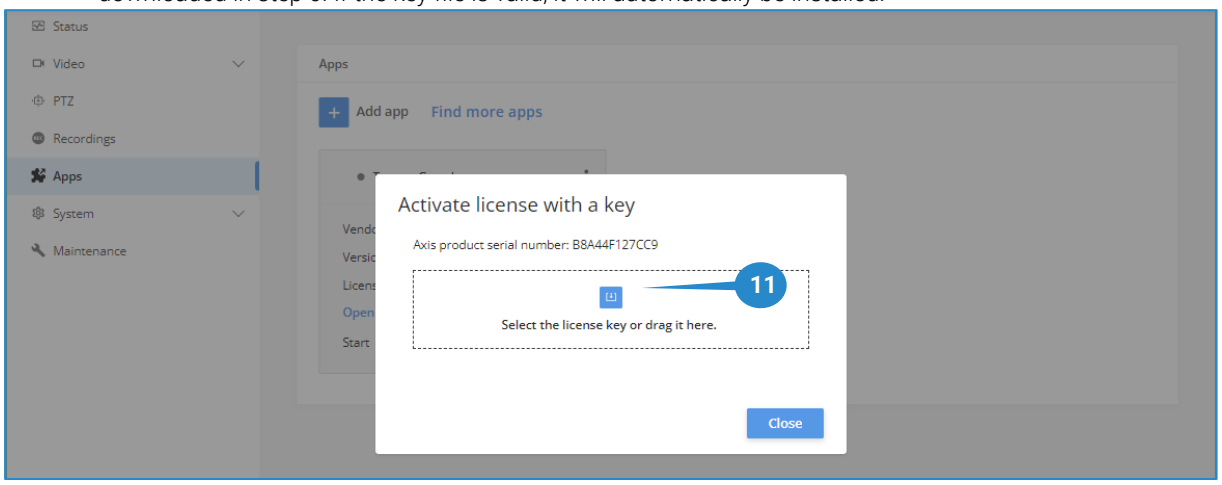


The license key, created in previous steps can now be uploaded and installed on the camera to activate the Araani Tamper Guard app. Follow steps below to activate the app:

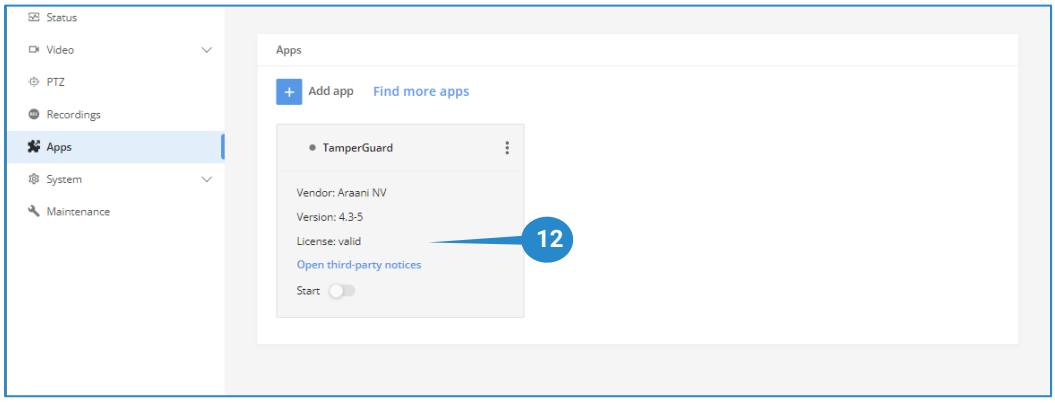
7. Connect to your camera, using your internet browser software and login to the camera webpage. Refer to the camera user manual on how to do this.
8. Select “Apps” from the menu pane.
9. Select the Araani Tamper Guard app menu button.
10. Select “Activate license with a key”



11. Select the upload button to browse your local storage for the *serialnumber*-TamperGuard.key file as downloaded in step 6. If the key file is valid, it will automatically be installed.



12. When installed correctly with a valid license key, following screen should appear:



ACTIVATE A TRIAL LICENSE FOR ARAANI TAMPER GUARD

If you prefer to try out Araani Tamper Guard before purchasing, follow the same steps as in Activating the Araani Tamper Guard license case 2. In step 3, select “I’d like to create a trial or a free license”. Provide a valid e-mail address if requested. Proceed with the rest of the procedure.

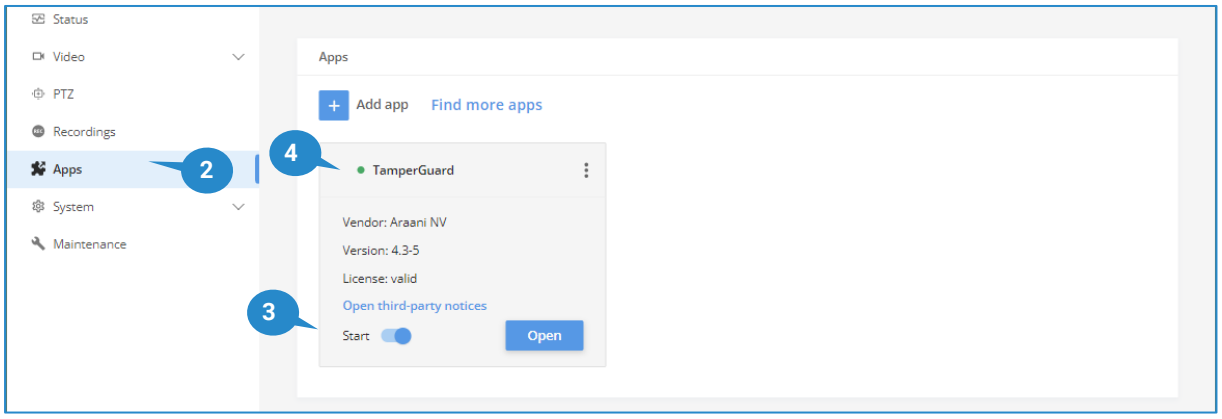
How to use Araani Tamper Guard

Starting / stopping Araani Tamper Guard

STARTING ARAANI TAMPER GUARD

After installation, Araani Tamper Guard needs to be started manually. To do so, follow the steps below.

1. Connect to your camera, using your internet browser software and login to the camera webpage. Refer to the camera user manual on how to do this.
2. Select “Apps” from the menu pane.
3. Select the Araani Tamper Guard app Start switch button.
4. The Araani Tamper Guard app button should change state and the status indicator should turn green.



START-UP BEHAVIOUR

At start-up, Araani Tamper Guard needs to learn the background of the scene. This takes a few minutes. During this period, Araani Tamper Guard is not fully operational yet. The default start-up state is “Recalibrating”. Within a maximum of 1 minute, Araani Tamper Guard will either move into "Operational" state, or go to some alarm state if the image is not ok.

STOPPING ARAANI TAMPER GUARD

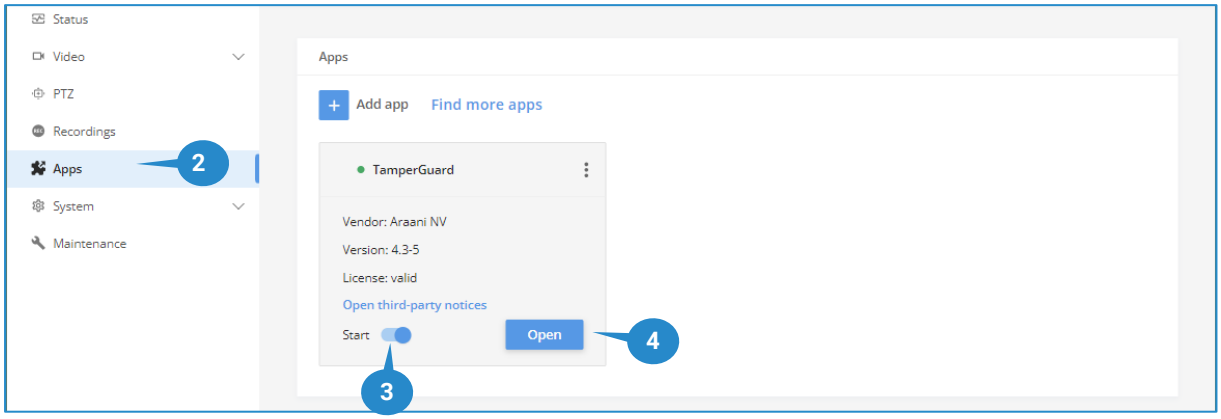
To stop the Araani Tamper Guard app, perform the same steps as Starting the Araani Tamper Guard app. When clicking the switch in step 3, the application will be stopped.

Configuring Araani Tamper Guard

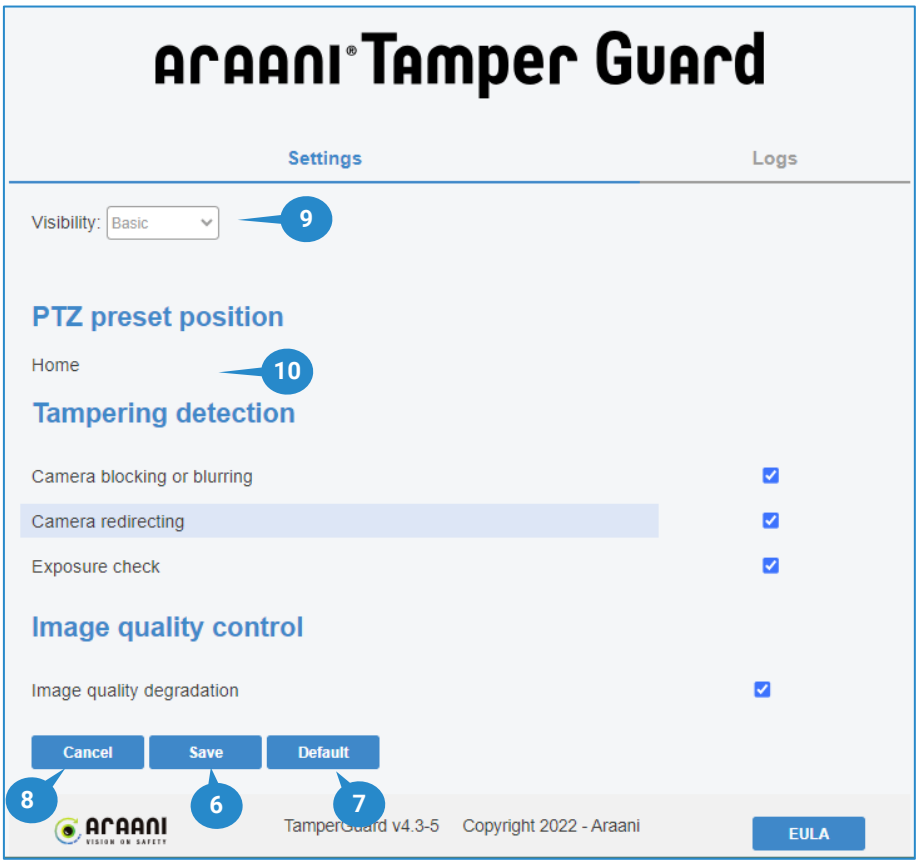
ACCESSING ARAANI TAMPER GUARD CONFIGURATION

To access the settings of Araani Tamper Guard on the camera, proceed with steps below.

1. Connect to your camera, using your internet browser software and login to the camera webpage. Refer to the camera user manual on how to do this.
2. Select “Apps” from the menu pane.
3. Make sure the application is running, otherwise start Araani Tamper Guard.
4. Select the Araani Tamper Guard app Open button.



5. A new browser window will appear that contains the basic settings to configure Araani Tamper Guard.



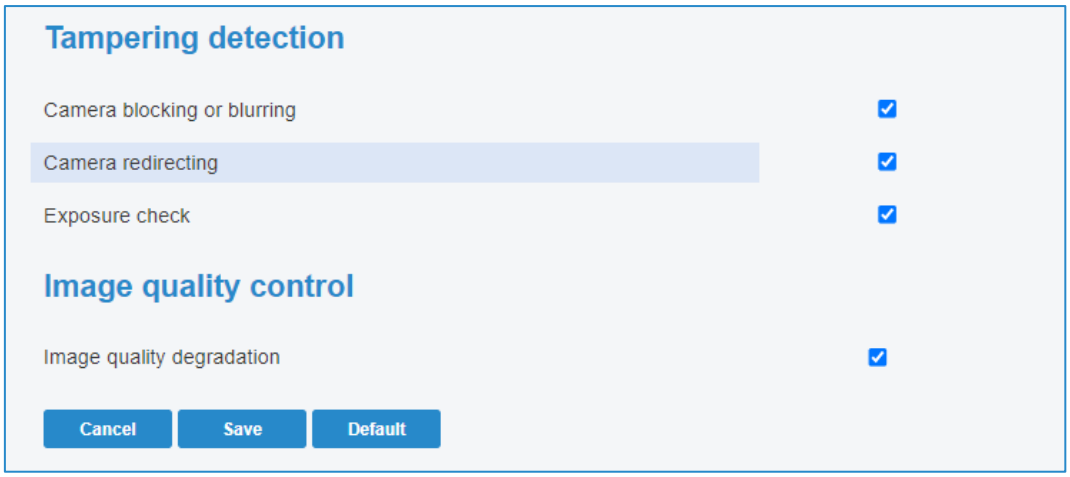
Refer to Araani Tamper Guard settings for detailed information on all available settings.

6. Select “Save” to register the new settings in the app.

7. “Default” can be used to return all settings to default.
8. “Cancel” can be used when changes to the settings have been done (but not saved) and one wants to return to the setting as is in the camera.
9. The visibility selector allows to select between "Basic" and "Advanced" settings. The "Advanced" setting allows to finetune the detection when basic settings are not satisfactory.
10. The label under "PTZ preset position" returns the value of the preset of a PTZ camera. See working with PTZ for more information.

Basic configuration of Araani Tamper Guard

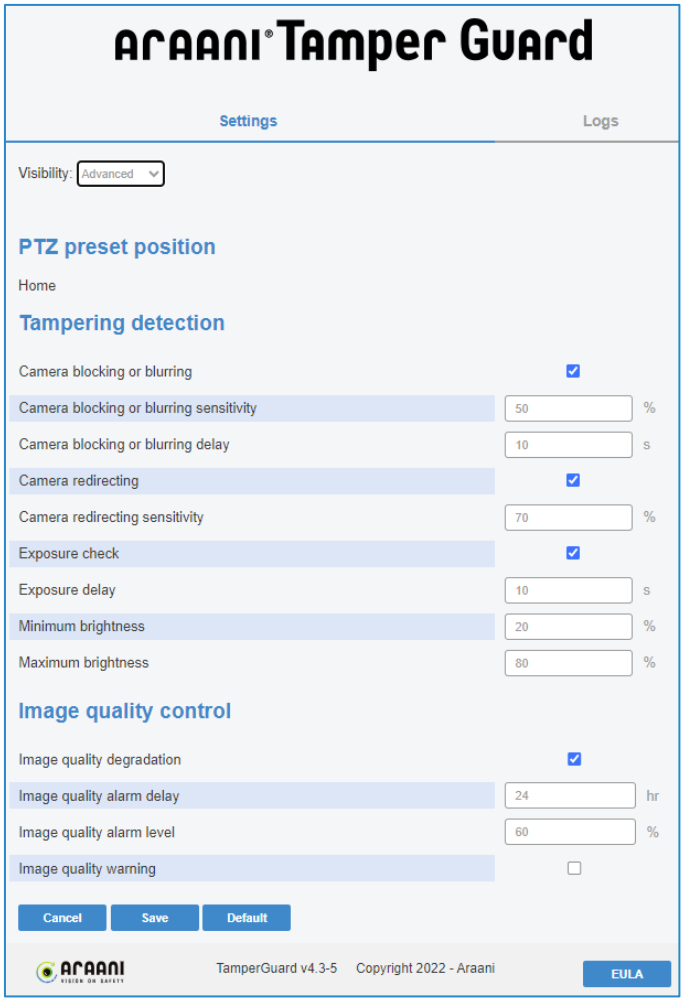
Following settings are available in basic configuration mode. These settings allow to enable or disable the individual sub algorithms.



Name	Range	Unit	Default value	Meaning
Camera blocking or blurring	on - off	-	on	This algorithm will trigger an alarm when the camera view is blocked or blurred.
Camera redirecting	on - off	-	on	This algorithm will trigger an alarm on a sudden change of the camera position.
Exposure check	on - off	-	on	This algorithm will trigger an alarm on under- or over-exposure of the image.
Image quality degradation *	on - off	-	on	This algorithm will trigger an alarm when the image quality degrades over time.

Advanced configuration of Araani Tamper Guard

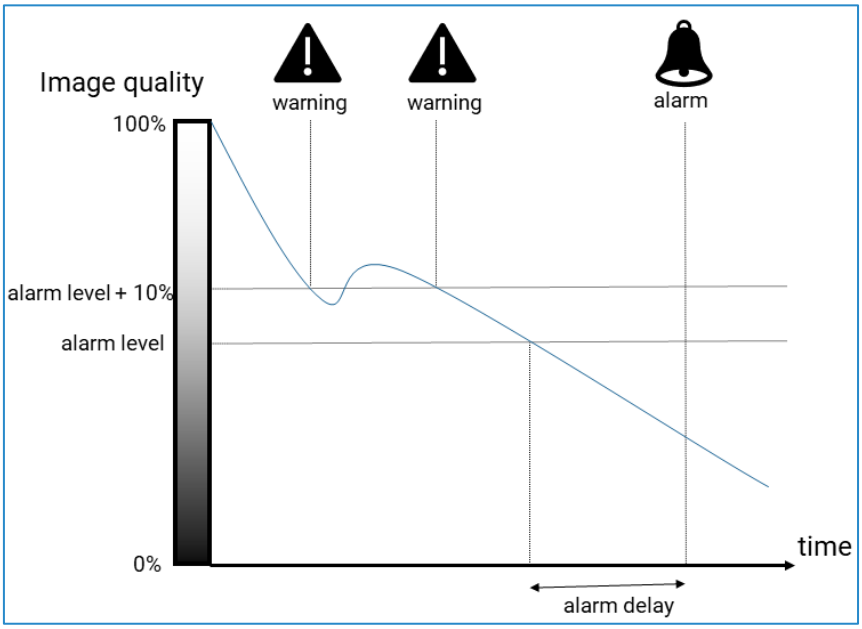
Advanced configuration mode makes a few extra parameters accessible. These additional parameters allow to fine-tune the behaviour of the algorithm and to change alarm threshold values.



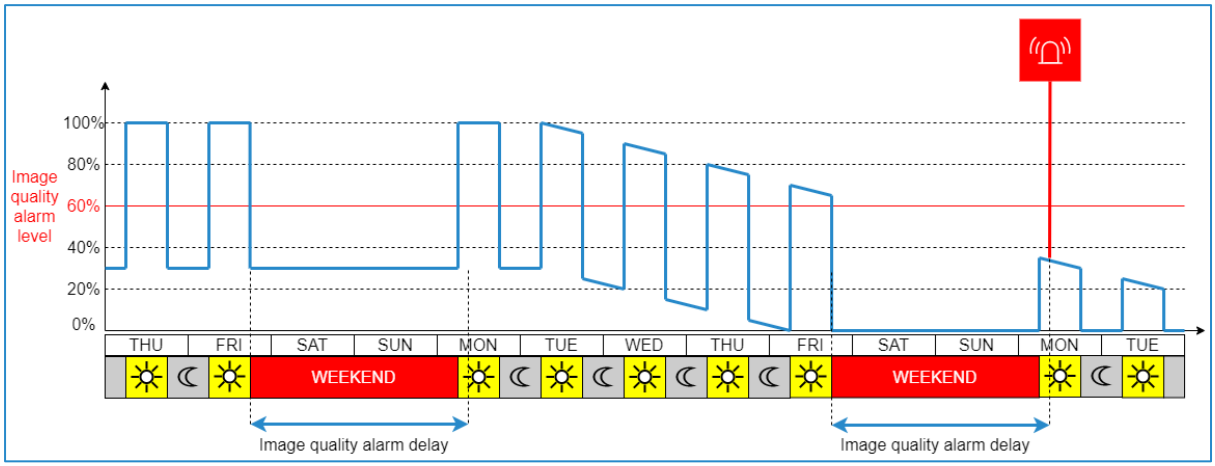
Name	Range	Unit	Default value	Meaning
Camera blocking or blurring sensitivity	20 - 90	%	50	A higher value results in a higher sensitivity and vice versa. The higher this value, the faster the event will be triggered.
Camera blocking or blurring delay	3 - 60	sec	10	Minimum duration of the blocking and blurring before the event is triggered.
Camera redirecting sensitivity	10 - 90	%	70	A higher value results in a higher sensitivity and vice versa. The higher this value, the faster the event will be triggered.
Exposure delay	3 - 60	sec	10	Minimum duration of over- or under-exposure before the event is triggered.

Minimum brightness	0 - 50	%	20	If the average brightness, calculated over the whole field of view is lower than this level, an exposure alarm is triggered. Minimum brightness = all black = 0%. Maximum brightness = all saturated white = 100%.
Maximum brightness	50 - 100	%	80	If the average brightness, calculated over the whole field of view is higher than this level, an exposure alarm is triggered. Minimum brightness = all black = 0%. Maximum brightness = all saturated white = 100%.
Image quality alarm delay	1 - 72	hours	24	An alarm will be raised when the image quality remains lower than the "Image quality alarm level" for the duration of "Image quality alarm delay" time. This setting allows to skip the alarm if the environment is intentionally unlit over a long period of time (e.g. holiday or weekend).
Image quality alarm level	30 - 80	%	60	A higher value results in a higher sensitivity and vice versa. The higher this value, the faster the event will be triggered.
Image quality warning	on - off		off	Generates a warning when the image quality is less than 10% above the "Image quality alarm level" during the "Image quality alarm delay". This warning can be used e.g. to initiate maintenance.

Alarm warning is optional and can be used as a signal for preventive cleaning. A warning will be generated when the image quality is approaching the alarm level by 10%.



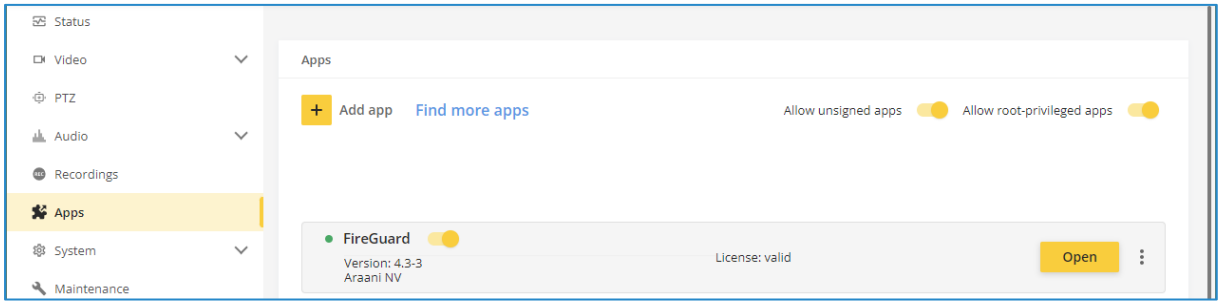
The image quality alarm will only trigger if quality has been below image quality alarm level for a configured amount of time. The image quality alarm delay time allows to skip alarms when companies close (and lights go out) in the nights and/or over weekends.



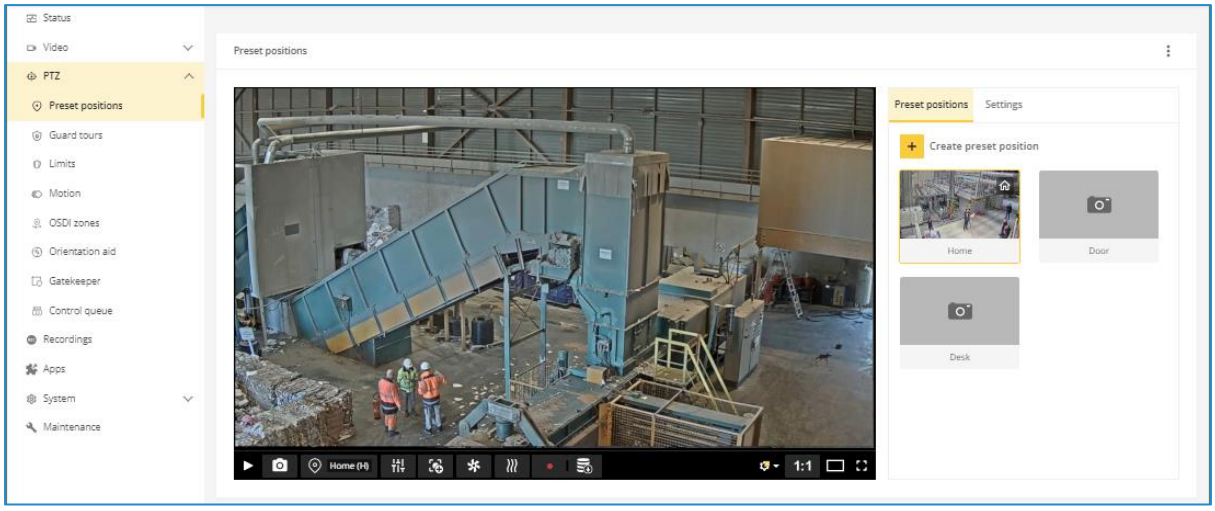
Working with PTZ cameras

Araani Tamper Guard is capable of working on pan tilt zoom cameras. This includes cameras with motorized lenses that only allow changes in zooming.

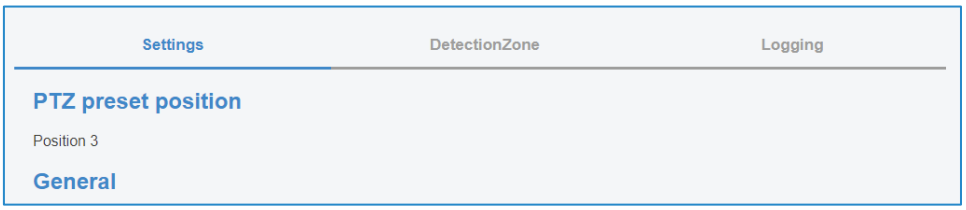
Attention: On cameras with Axis OS firmware >= 11.5, 'Allow root-privileged apps' must be enabled to allow Araani Tamper Guard to work in PTZ mode. This can be verified in the Apps setup page:



For each of the configured preset positions, a separate configuration is created. Up to 10 preset positions (and related settings) are supported. These individual configurations include all configuration settings.
While moving or when the camera is positioned out of any preset position, Araani Tamper Guard is stopped (status 'STOPPED'). When the camera is returned to one of the named preset positions, the algorithm recognizes that position, automatically loads the correct configuration and starts learning the background again (status 'RECALIBRATING') before returning to 'OPERATIONAL' mode.
The camera presets and associated names are configured in the camera setup interface as illustrated below. Refer to your camera manual for details on PTZ preset configuration.



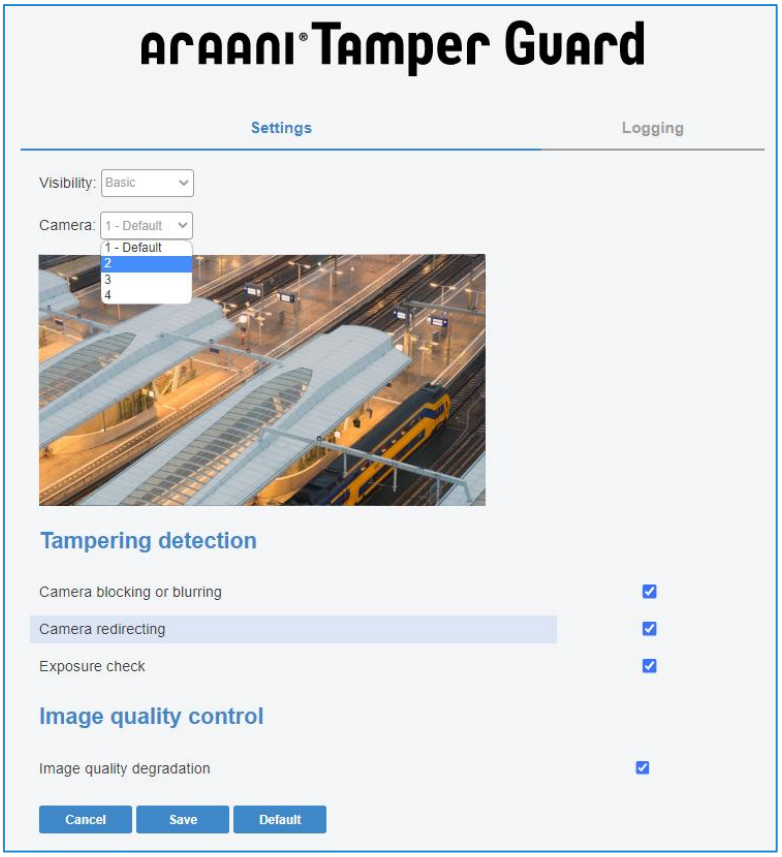
After moving to any of the configured presets, the associated configuration is loaded and the preset name is shown in the Araani Tamper Guard settings interface in the 'PTZ preset position' section as illustrated below.



Notice: Make sure all relevant PTZ positions are properly configured and named. Even for a camera with motorized lens that remains in fixed position after initial configuration, this position should be named (e.g. 'home'). Unnamed positions will not be identified, and the algorithm will not start.

Working with multi-sensor cameras

On cameras with multiple sensors, the configuration interface looks slightly different: it allows to select the sensor on which Araani Tamper Guard will be active and shows a preview of that monitored stream. Configuration can be different for each stream and is saved as such, similar to working with PTZ cameras. When switching the active stream, Araani Tamper Guard is stopped and restarted with the applicable configuration. This switching may take a few seconds and the background will be re-learned.



Configuring display options

To visualize Araani Tamper Guard events inside the video stream, text overlay that displays the Araani Tamper Guard status can be activated.

VIEW ARAANI TAMPER GUARD STATUS

The Araani Tamper Guard app status is one of following:

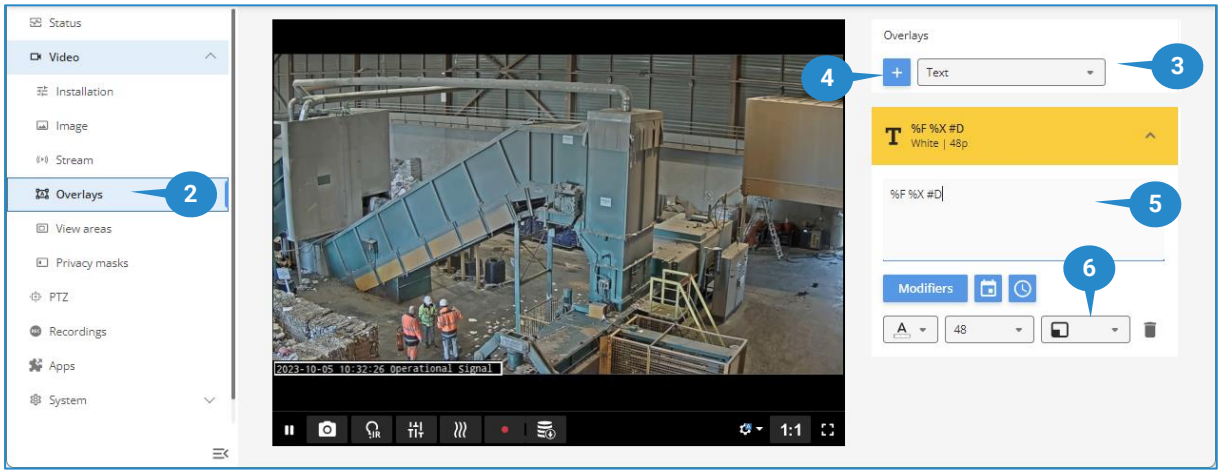
- OPERATIONAL SIGNAL: the app is running; no incident is seen, and conditions are ok.
- BLOCKED OR BLURRED ALARM: camera view is blocked or blurred.
- EXPOSURE ALARM: image too bright or too dark.
- CAMERA REDIRECTED ALARM: sudden change of field of view.
- IMAGE QUALITY ALARM: low image quality.
- IMAGE QUALITY WARNING: approaching low image quality threshold.
- RECALIBRATING: the app is (re-)learning the background (after a reset or position change of a PTZ camera).
- STOPPED: the app stopped monitoring. This occurs while a PTZ camera is changing position or when the new position is not recognized as a preset position. This also occurs when the video stream is lost, e.g. because of processor overload.

The Araani Tamper Guard status can be visualized in the video stream by using the Axis® camera overlay capabilities. To visualize the Araani Tamper Guard events on screen, follow these steps:

1. Connect to your camera, using your internet browser software and login to the camera webpage. Refer to the camera user manual on how to do this.
2. Select “Overlays” from the menu pane.

3. Select “Text”.
4. Select The “+” button to create a new overlay.
5. In text box that appears, one can create a custom overlay text by using codes. The available Araani Tamper Guard status codes are dependent on your Axis OS version:
    a. For Axis OS firmware < 11.2.16
        i. Add #D to the overlay definition to add the Araani Tamper Guard status.
    b. For Axis OS firmware >= 11.2.16
        i. Add #D1 to the overlay definition to add the Araani Tamper Guard status.

    This can be combined with other custom fields such as date (%F) and time (%X) in the example below. Refer to your camera manual for all available options.
6. In the dropdown box, select the location where you want the overlay to appear in the image. This should always be bottom left or bottom right, to not influence the detection. Font, colour and size are customizable.
7. Leaving the menu item will automatically save the overlay and create it.



8. An overlay text bar will now appear in the video with the selected options, including the Araani Tamper Guard events.

Note that only one status can be shown at any time. If multiple alarms or statuses occur at any time, following hierarchy is applied:

Stopped > Recalibrating > Blocked or blurred > Camera redirected > Exposure > Image quality alarm > Image quality warning > Operational

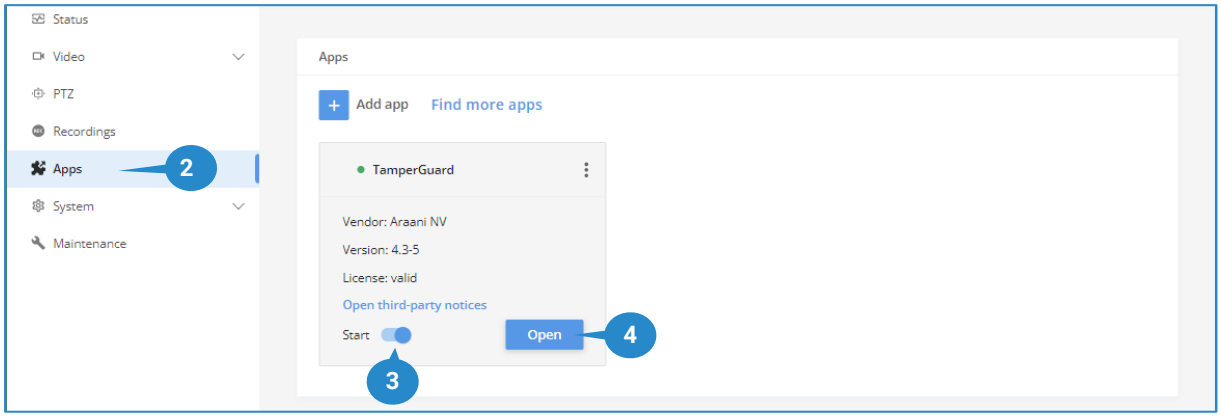
Only the highest-in-rank status will be displayed.

Maintenance and troubleshooting

Retrieving diagnostics information

In case of problems with the Araani Tamper Guard, your support contact may request you to retrieve the logging information from the app. When contacting support services, it is advised to include this information by default in the problem report. Follow steps below to retrieve this diagnostics information.

1. Connect to your camera, using your internet browser software and login to the camera webpage.
   Refer to the camera user manual on how to do this.
2. Select “Apps” from the menu pane.
3. Make sure the application is running, otherwise start Araani Tamper Guard.
4. Select the Araani Tamper Guard app “Open” button.

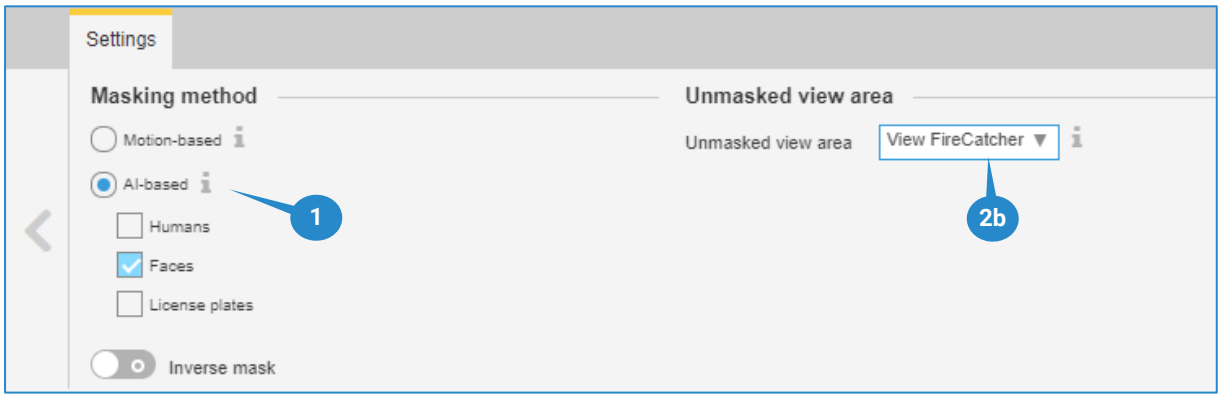


5. Select the “Logs” tab.
6. To view the log information of the application, select “View”.
7. To download the logging information of the application, select “Download”.
   A text file will be created with extension ‘.log’ that contains all available logging information. This file can be sent to your support contact for diagnosis and troubleshooting.

Using Araani Tamper Guard with Axis Live Privacy Shield (ALPS)

Axis Live Privacy Shield is an ACAP application that adds AI-based dynamic masking of moving and still objects such as humans, license plates, or backgrounds to the streaming video in order to safeguard privacy. Araani Tamper Guard can operate in combination with ALPS, subject to following conditions.

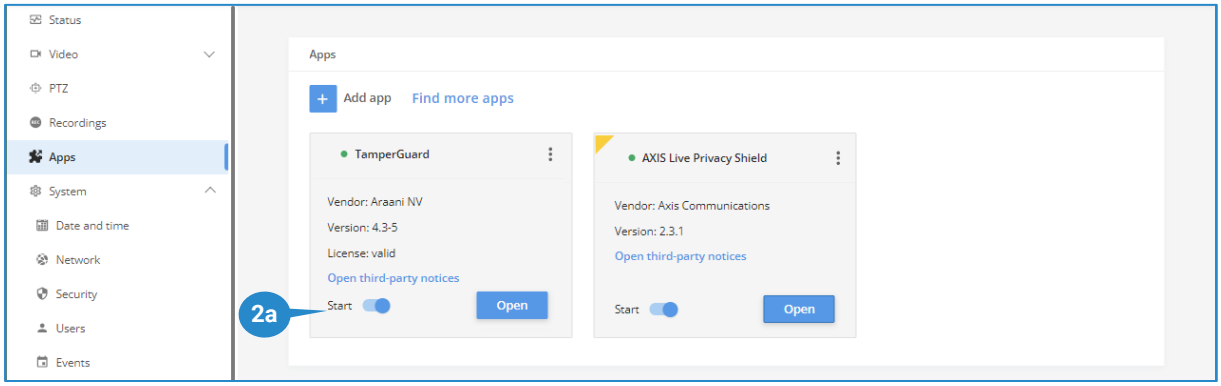
1. The camera has a deep learning processing unit (DLPU) and the ALPS application is assigned to run on it. This is done by selecting the AI-based version of ALPS as shown below. If the ALPS application does not show the AI-based option, then your camera has no DLPU and the ALPS applications must not be used. The motion-based option is executed on the main CPU of a camera and due to its heavy computing load will interfere with the Araani Tamper Guard operation.



2. Araani Tamper Guard needs access to an unmasked version of the video. This is realized through the use of a dedicated view area, called “View Araani Tamper Guard ”. This view is created automatically by the Araani Tamper Guard application at startup but it is not assigned automatically as the unmasked view area. For correct configuration, follow these steps:

    a. If ALPS was installed after Araani Tamper Guard, stop and restart the Araani Tamper Guard application. This will make sure the “View Araani Tamper Guard” is created.

    b. Select the “View Araani Tamper Guard” as the unmasked view area in the ALPS configuration interface.



Integration of Araani Tamper Guard with VMS systems

Araani Tamper Guard can be easily integrated with many video management systems (VMS), allowing to view alarms in the alarm interface of the VMS. Depending on the type of VMS, all kinds of actions can then be associated with the alarm such as messaging, recording, activating scenarios, etc.
To make integration of alarms possible, Araani Tamper Guard sends out alarm and status messages, using the Axis dynamic events scheme. This method is recognized by most VMS systems that allow for integration with Axis cameras and Axis video analytics capabilities.
For integration with other VMS systems than the ones stated below, please contact your supplier.

Attention: The following instructions assume that you are familiar with the video management software and have already installed and configured the cameras that are running Araani Tamper Guard analytics. For instructions on how to accomplish this, please refer to the VMS documentation.

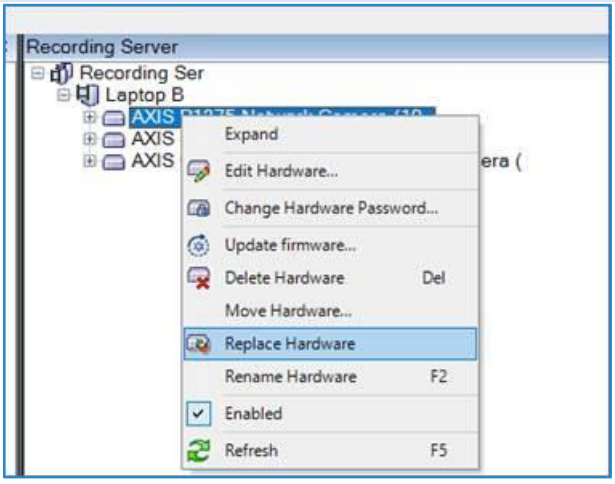
Integration with Milestone XProtect

Araani Tamper Guard is compatible with Milestone Xprotect Express+, Professional+, Expert and Corporate. Araani Tamper Guard is tested with Milestone XProtect Express+ version 2021R2.
Enabling alarm notifications from Araani Tamper Guard involves 2 steps:

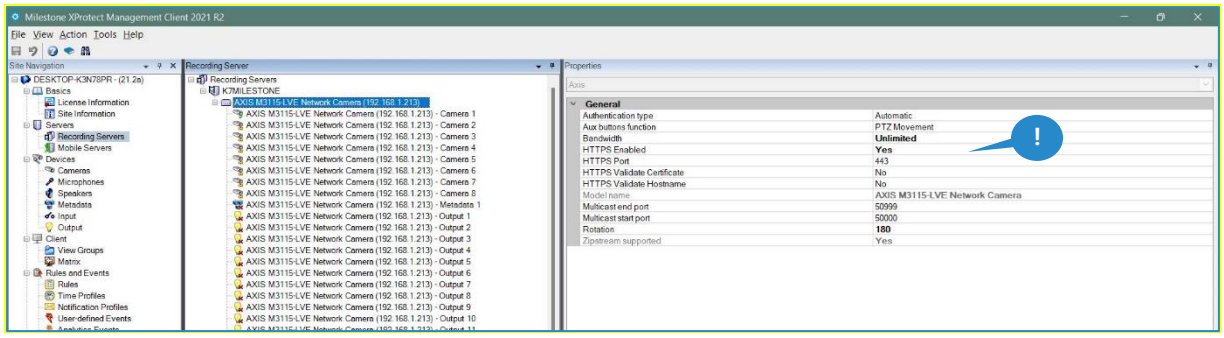
- Enable the device events in the device configuration on the recording server.
- Define the alarms, associated with these events.

Attention: When Araani Tamper Guard was installed after the camera installation in Milestone VMS, or the application is replacing another, or an upgrade has occurred with new features, it may be required to reinitialize the hardware in the Milestone XProtect Management Client. This is done by right clicking the camera under the selected recording server and choosing "Replace hardware". Follow the instructions to perform a reinitialization. At this time, the capabilities of the camera are re-read.

Information: If your camera has been configured for https communication only w.r.t. cybersecurity, it may be needed to temporarily enable http communication in the camera system security setup to be able to perform this action.



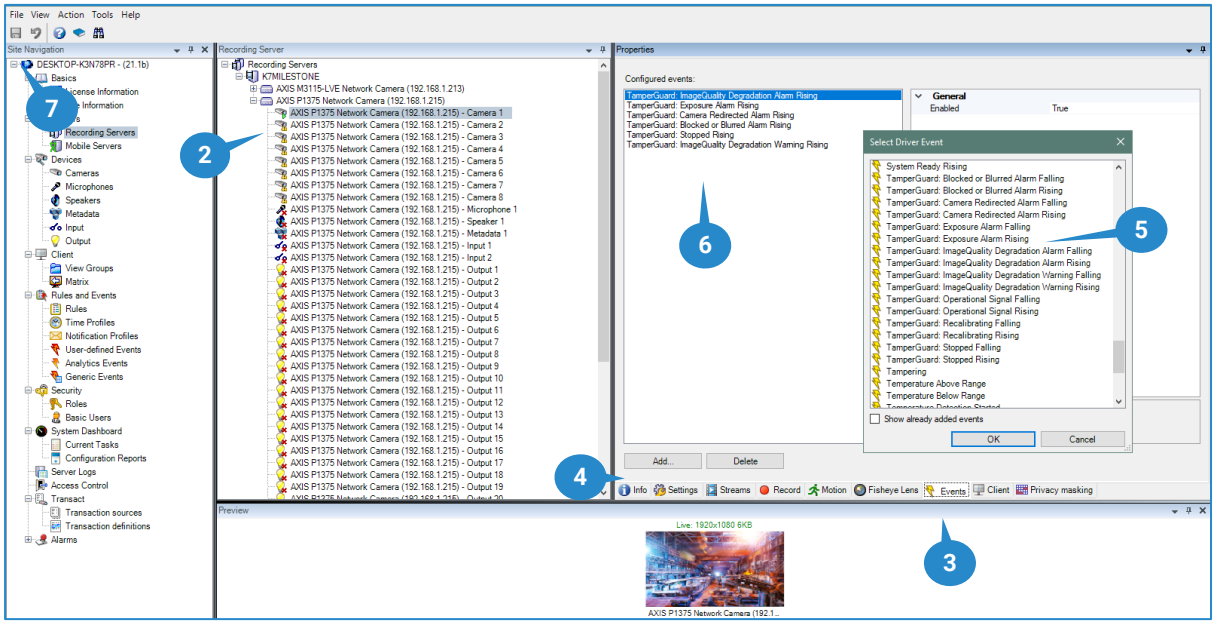
Attention: Araani Tamper Guard release 4.00.03 and higher may be using secure https for communications. In such case, https needs to be enabled on camera level in the Milestone XProtect Management Client:



To enable the events for each camera in Milestone VMS, follow these steps:

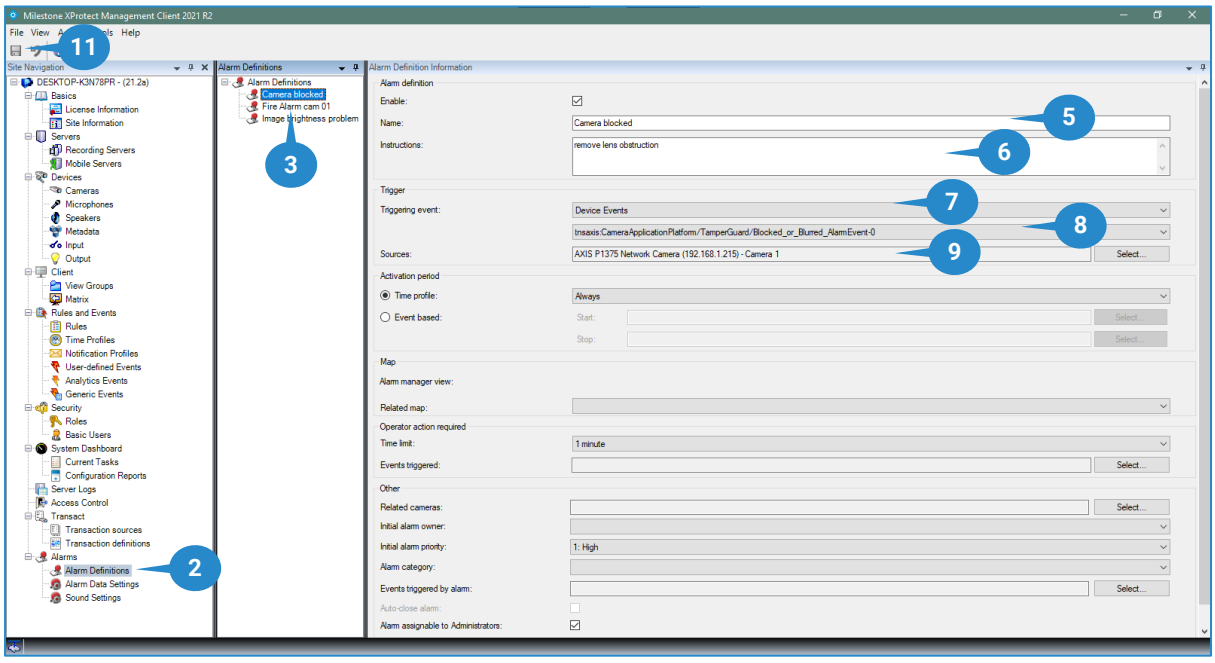
1. Open Milestone XProtect Management Client.
2. Find the camera under the corresponding recording server on which Araani Tamper Guard is running and for which you want to enable Araani Tamper Guard alarm notifications.
3. Select the Events tab.
4. Select "Add"; a popup box "Select Driver Event" appears.
5. Add the event for which you want to raise an alarm. All events start with the application name, followed by the event name and either "Falling" or "Rising" option. "Rising" refers to the beginning of the event, so only select the "Rising" version of the event. Following events are available:
    a. Blocked or Blurred Alarm
    b. Camera Redirected Alarm
    c. Exposure Alarm
    d. ImageQuality Degradation Alarm
    e. ImageQuality Degradation Warning
    f. Operational Signal
    g. Recalibrating
    h. Stopped

    Refer to View Araani Tamper Guard status for the meaning of these events.
6. Repeat steps 4-5 for each event that you want to be notified of in the VMS client.
7. Save the configuration by selecting the save button or confirm saving when asked.
8. Repeat steps 2-7 for each camera with Araani Tamper Guard installed.

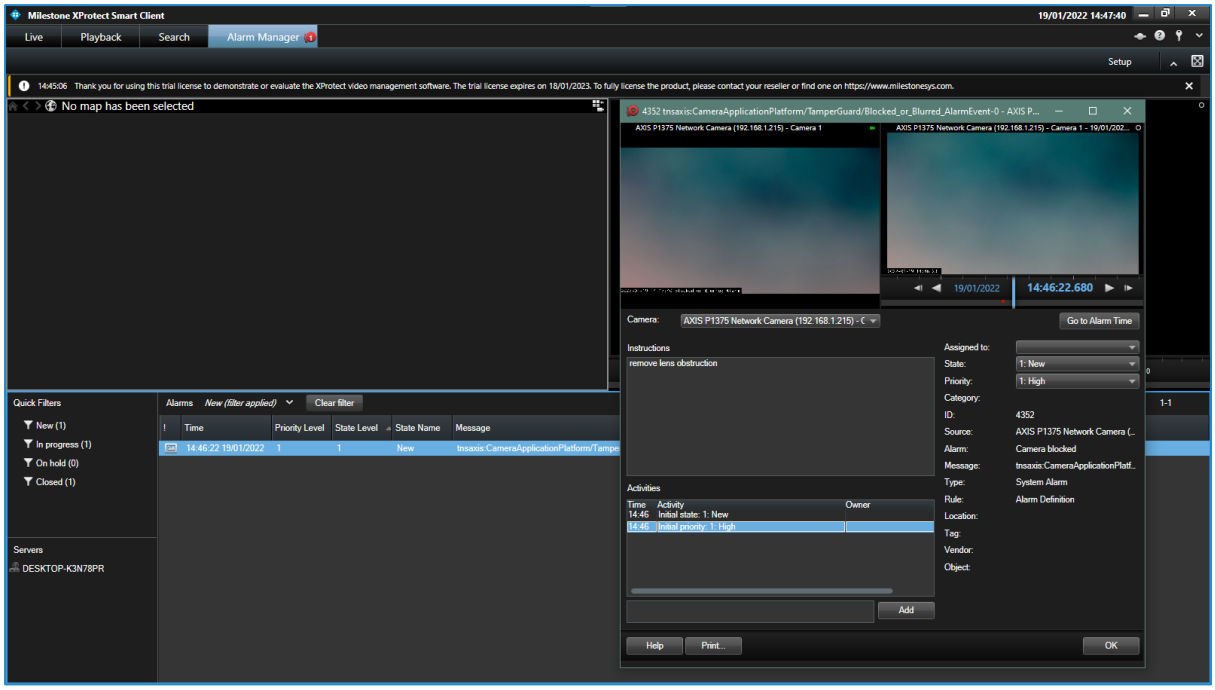


To define the alarms associated with the events as configured above, follow these steps:

1. Open Milestone XProtect Management Client.
2. Select "Alarm Definitions".
3. Right-click on the Alarm Definitions field and select "Add New" or press Ctrl+N.
4. A form appears to configure the new alarm.
5. Provide a meaningful name for the alarm that is easily recognized by the operator.
6. Add instructions for the operator if needed.
7. Under Triggering Event, select "Device Events" from the dropdown.
8. In the following field, scroll down and find the appropriate event in the dropdown list.
   This will be in the format "tnsaxis :CameraApplicationPlatform/TamperGuard/*eventname-x*" where eventname is similar to the event list as seen at the device event configuration and x is either 0 or 1. For the "Rising" events configured in first step, select the "0" event here.
   E.g. for the Blocked / Blurred event, select
   " tnsaxis :CameraApplicationPlatform/TamperGuard/Blocked_or_Blurred_AlarmEvent-0"
9. In the source field, select the camera device for which you want to set the alarm.
10. Other fields are optional, depending on your local preferences. Refer to the Milestone documentation for further information on these fields.
11. Save the configuration by selecting the save button or confirm when asked.
12. Repeat steps 2-11 for each event that you want to raise an alarm for.
13. Repeat steps 2-12 for each camera device for which you want to raise alarms.



When both the event is defined for a camera device and a corresponding alarm definition is created that is associated with the event, alarms will appear in the Milestone Xprotect Smart Client alarm window as illustrated below. Clicking the alarm will cause a replay in the replay window. Double clicking the alarm will show details about the alarm. Refer to the Milestone documentation on how to process alarms.



Integration with Genetec Security Center

Araani Tamper Guard is compatible with Genetec Security Center. Araani Tamper Guard is tested with Security Center version 5.10.

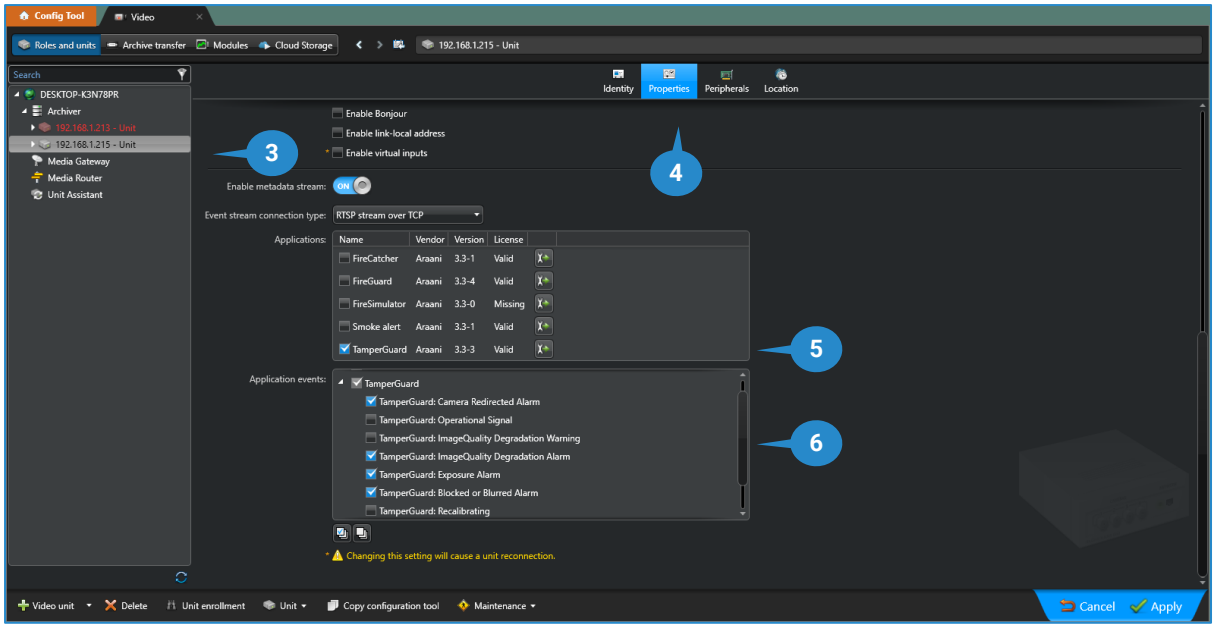
Attention: Araani Tamper Guard release 4.00.03 and higher may be using secure https for communications. In such case, https needs to be enabled on camera level in the Genetec Security Center.

Enabling alarm notifications from Araani Tamper Guard involves 3 steps:

- Enable the device events in the device configuration.
- Define an alarm.
- Create an action rule to generate the alarm.

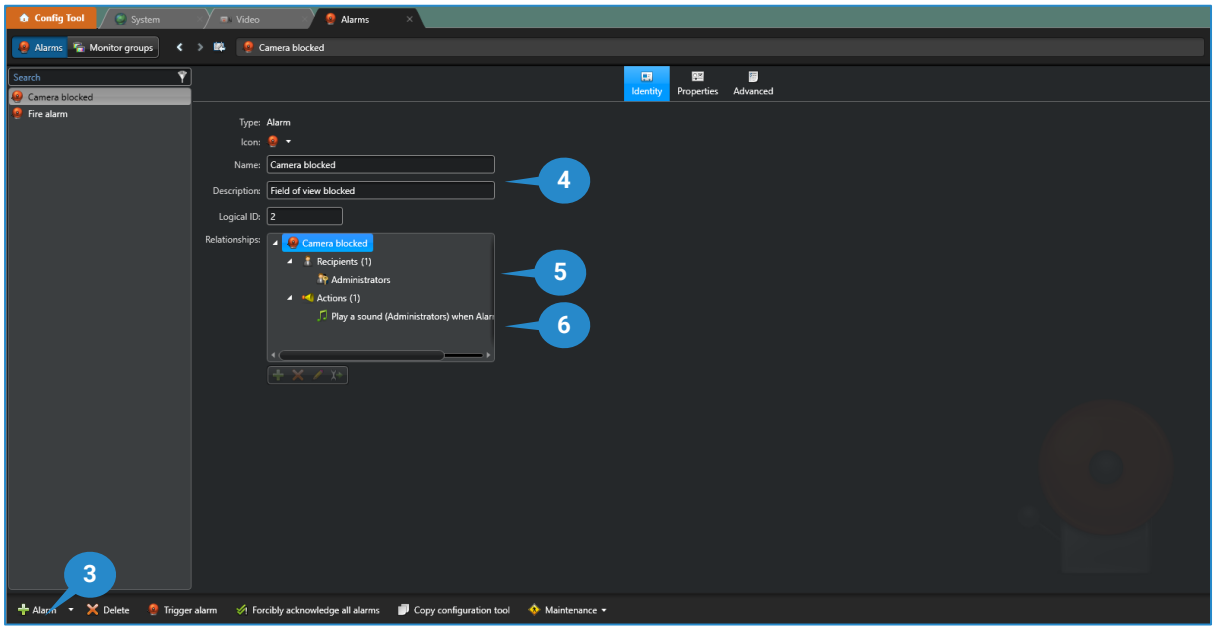
To enable the Araani Tamper Guard events, follow these steps:

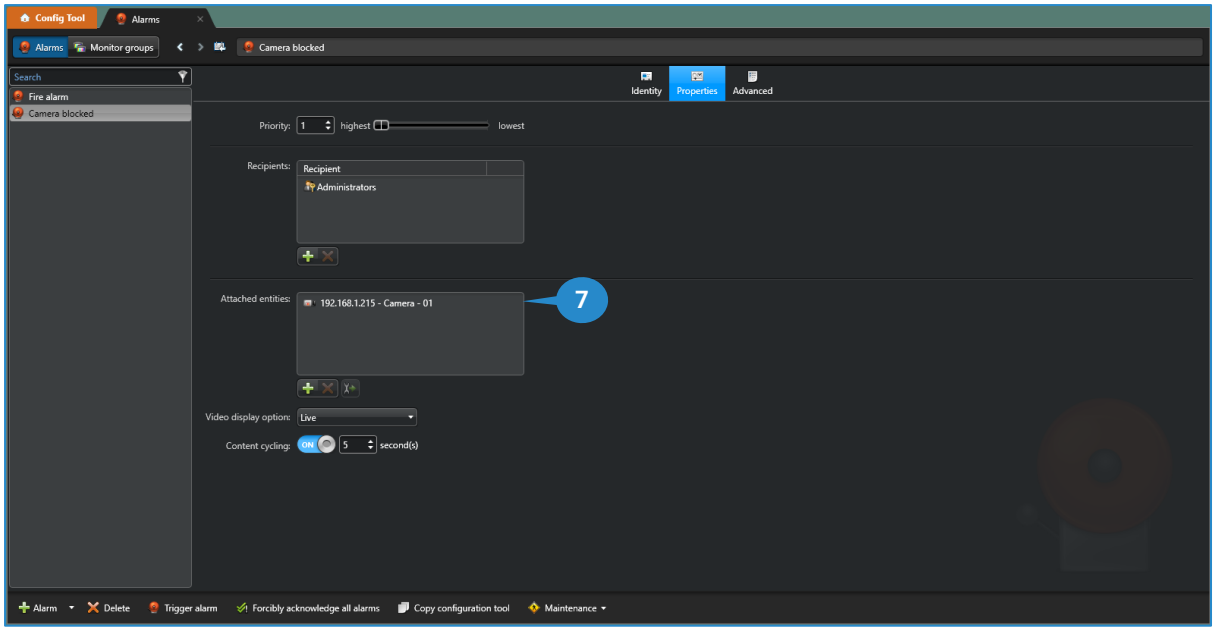
1. Open the Genetec Config Tool.
2. Open the "Video" configuration task.
3. Select the camera unit for which you want to enable the Araani Tamper Guard alarms. Select the unit level, not the lower stream level.
4. Choose "properties".
5. Under "Applications", enable the Araani Tamper Guard entry. Click "Apply".
6. Under Application events for Araani Tamper Guard, select the events for which you want to raise an alarm and click "Apply".



Define an alarm by following these steps:

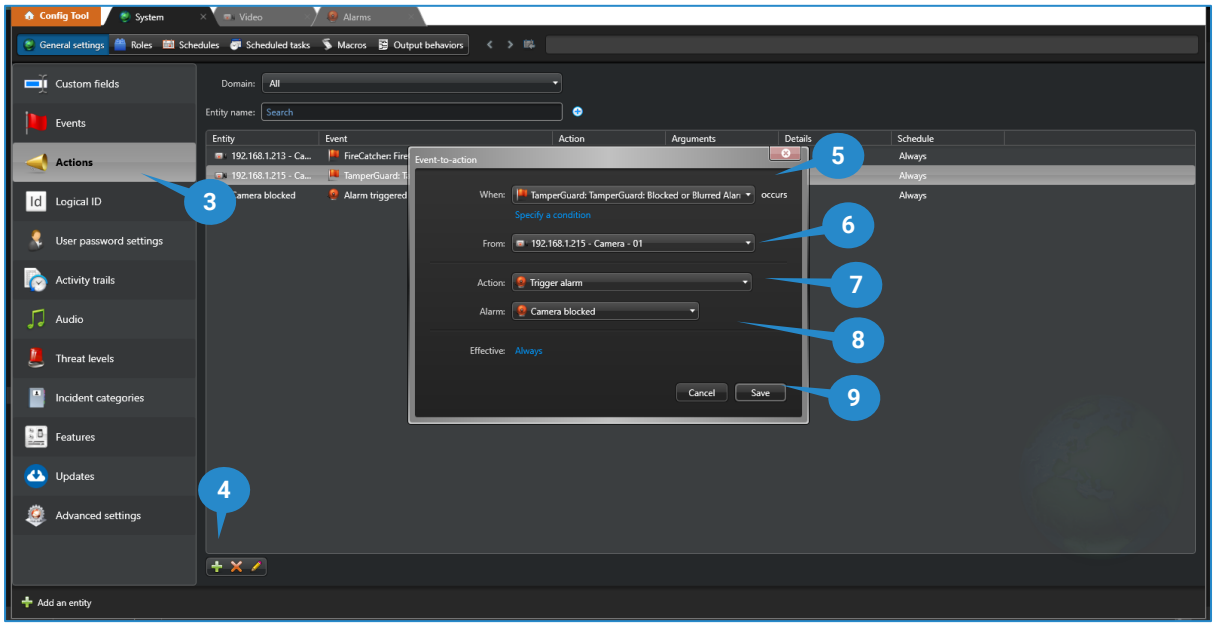
1. Open the Genetec Config Tool.
2. Open the "Alarms" configuration task.
3. Add a new alarm by clicking the "+ Alarm" button.
4. Provide a meaningful name and description for the alarm.
5. If not present, add the operator accounts for which you want to raise this type of alarm under "Recipients"
6. Under "Actions", you can define all kind of actions when the "Alarm triggered" occurs, e.g. playing a sound, starting a recording, etc.
7. In the 'Properties' tab, add the cameras for which you want to raise the alarm under “Attached entities”.



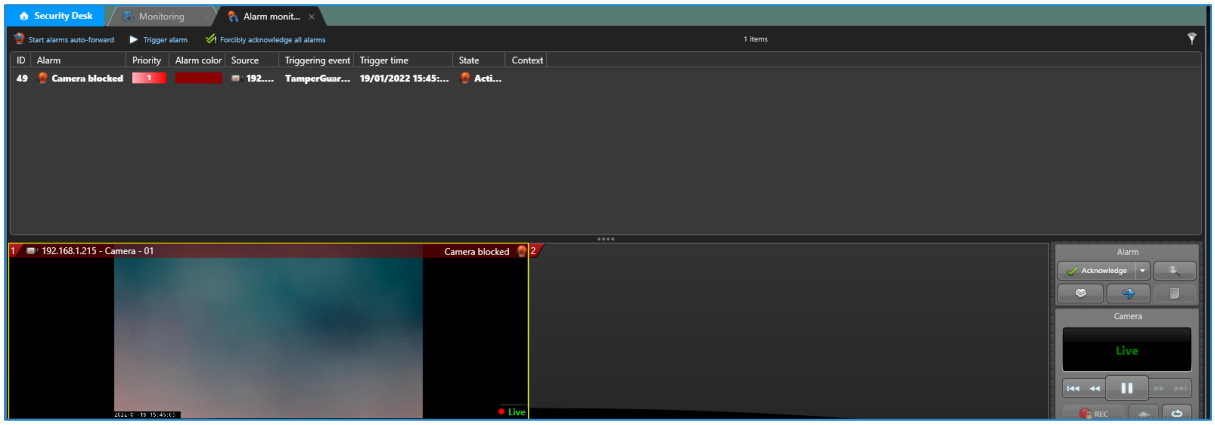


Finally, create a rule to trigger the alarm when a Araani Tamper Guard event occurs by following these steps:

1. Open the Genetec Config Tool.
2. Open the "General Settings" task under "System".
3. Select "Actions".
4. Add a new action by clicking the "+" button.
5. In the "When:" dropdown, select the Araani Tamper Guard for which you want the alarm to occur. Choose the "ON" option to select the beginning of the event e.g., "TamperGuard: Blocked or Blurred Alarm ON".
6. In the "From:" field, select the camera for which you want to enable the alarm. Note that here, the stream level is selected.
7. As "Action:", select "Trigger Alarm".
8. In the "Alarm:" field, select the alarm that you defined in previous step.
9. Select "Save"



When properly configured, the selected Araani Tamper Guard events will cause an alarm to be generated and displayed in the Security desk monitor panel as illustrated below.

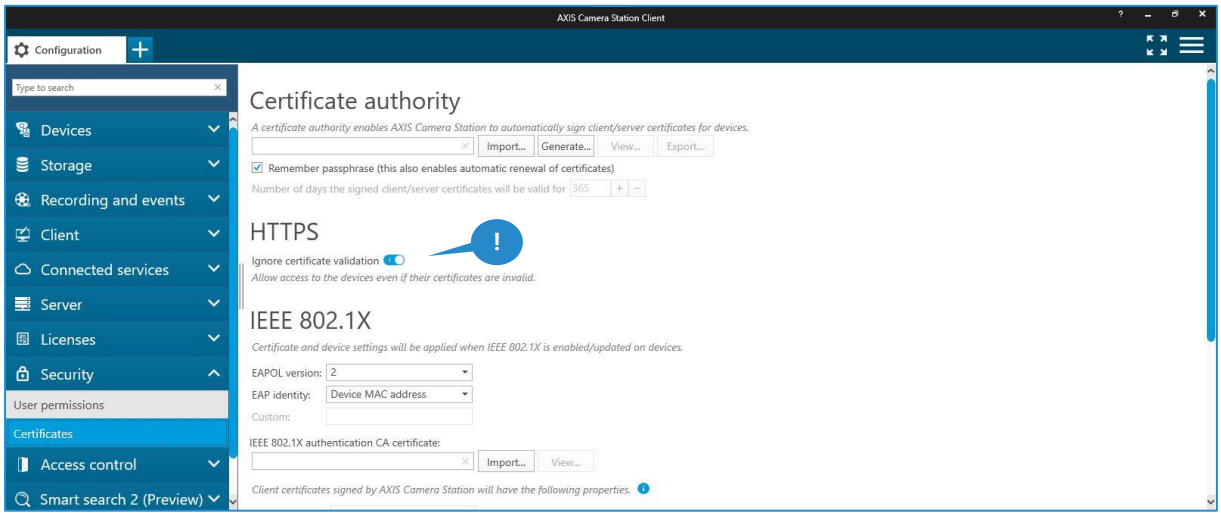


For more information on how to configure alarms and all the possible options, please refer to the Genetec Security Center documentation.

Integration with Axis Camera Station

Araani Tamper Guard is compatible with Axis Camera Station (ACS). Araani Tamper Guard is tested with ACS version 5.40.

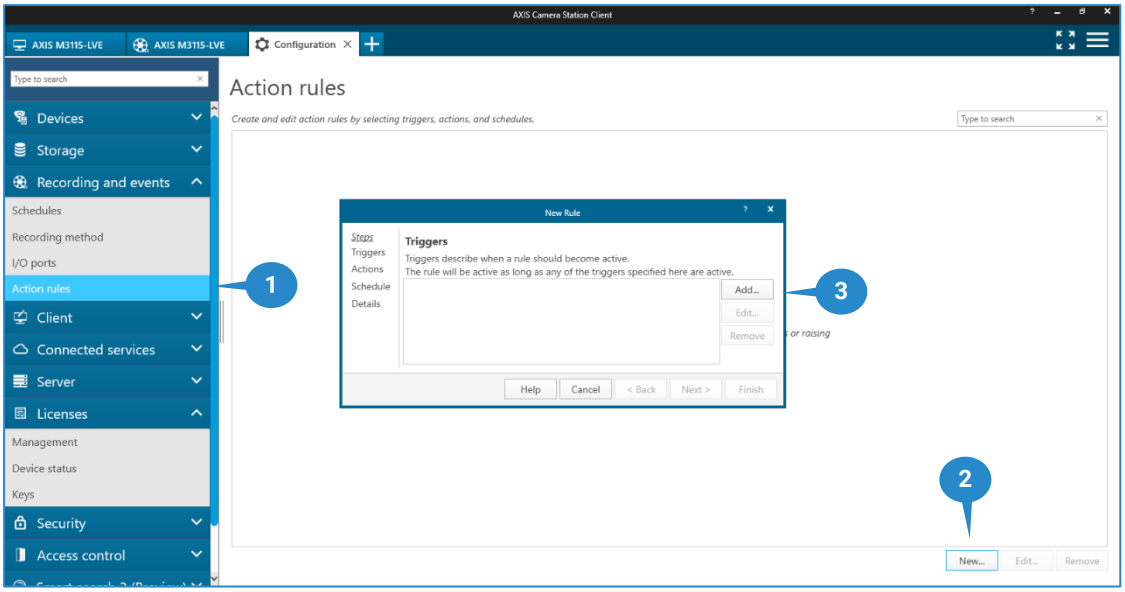
Attention: Araani Tamper Guard release 4.00.03 and higher may be using secure https only for communications. By default, Axis cameras use a self-signed certificate. In such case, https certificate validation needs to be disabled in Axis Camera Station. This can be found under security settings:



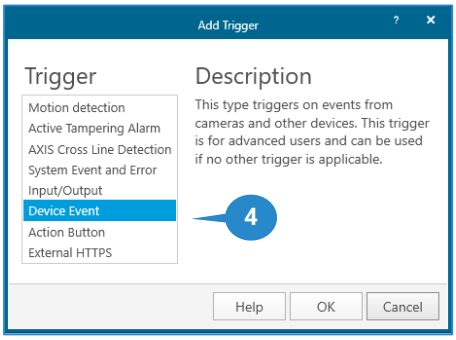
Enabling Araani Tamper Guard alarm notifications is done by creating a new action rule for each event that you want to be notified off and for each camera that has Araani Tamper Guard installed.
To enable Araani Tamper Guard alarm notification, follow these steps:

1. In ACS Client, select "Action rules" under "Recording and events" on the "Configuration" tab.
2. Select "New". A popup window appears to configure a new rule.

3. In the "Triggers" dialog, select "Add". A new popup window appears to select the type of trigger.

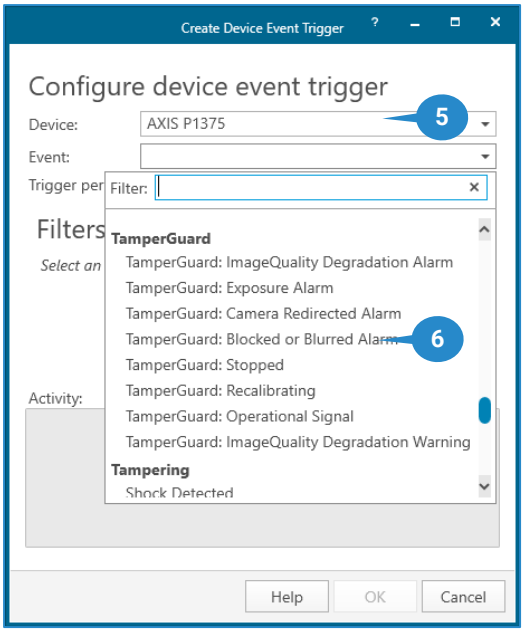


4. Select "Device Events" and "OK". A device event trigger configuration dialog window appears.

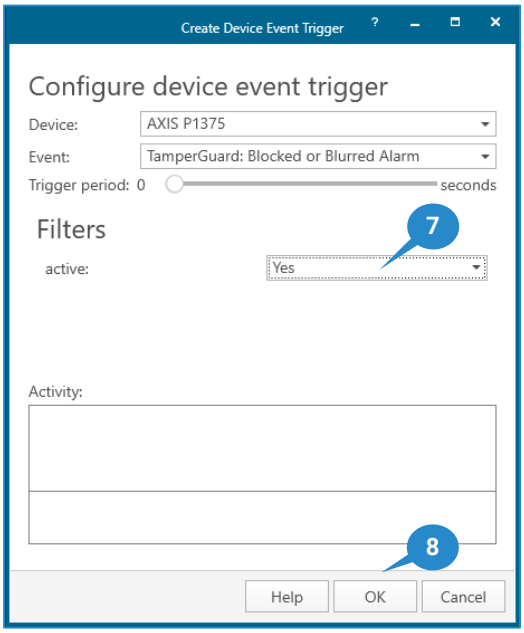


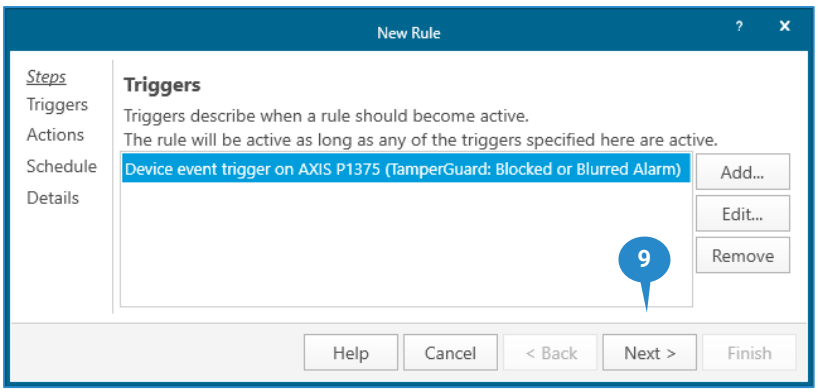
5. In the device dropdown, select the camera for which you want to enable the alarm.
6. In the Event dropdown, select the event for which you want an alarm notification. Following events are available:
    a. Blocked or Blurred Alarm
    b. Camera Redirected Alarm
    c. Exposure Alarm
    d. ImageQuality Degradation Alarm
    e. ImageQuality Degradation Warning
    f. Operational Signal
    g. Recalibrating
    h. Stopped

Refer to View Araani Tamper Guard Status for the meaning of these events.



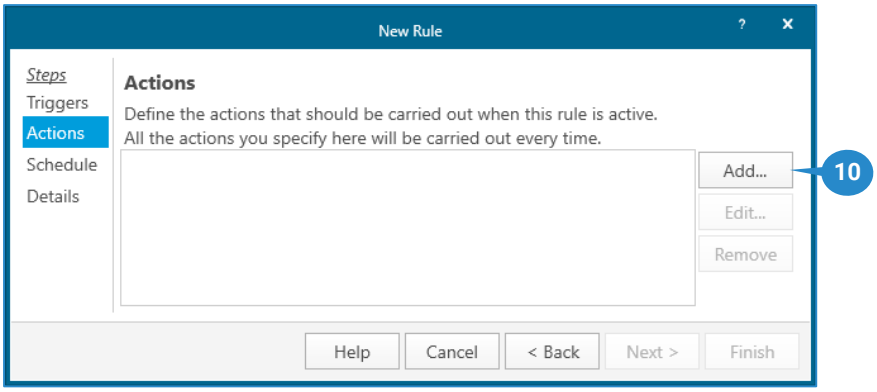
7. Make sure you select "YES" under "Filters", next to active. This will make sure only one alarm notification is generated at the beginning of the Araani Tamper Guard event.



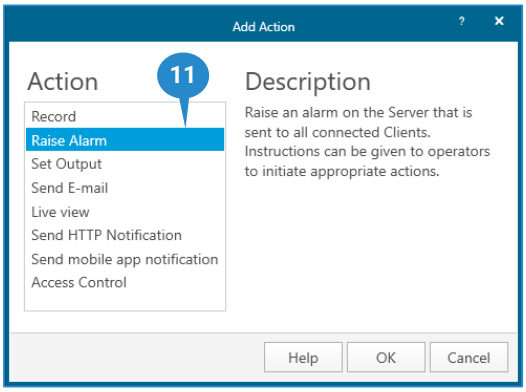
8. 

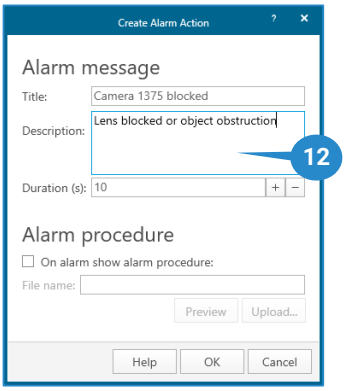
Select "OK" to save.

9. Select "Next" to proceed to the action configuration step.
10. In the Actions dialog window, select "Add" to configure the required alarm notification. A new popup window appears to select the type of action.

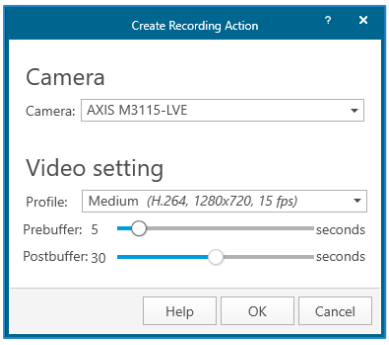


11. Select "Raise Alarm". A new popup window appears to configure the alarm notification.



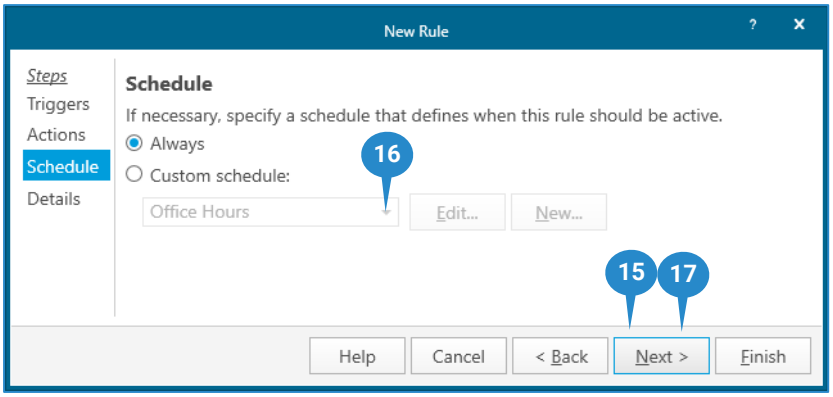


12. Enter a meaningful title and description as needed. This information will appear in the alarm list of the ACS client interface when the event occurs.
13. Select "OK" to save.
14. Other actions may be added e.g. to create a recording when the event occurs.

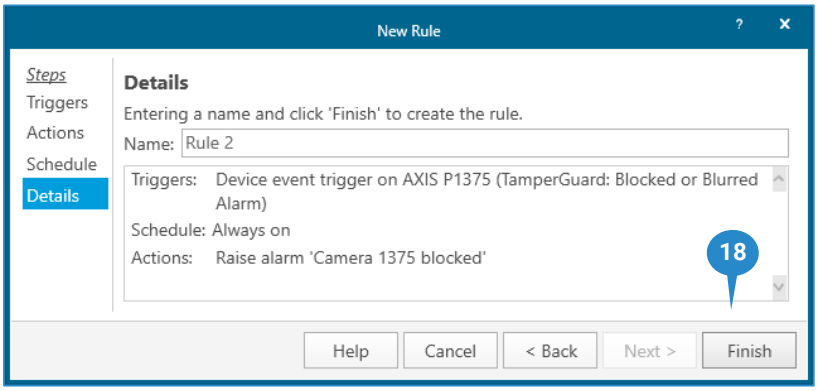


15. Select "Next" to proceed to the scheduling step.

16. A schedule can be entered if the alarm notification is needed only during certain hours. E.g. during hours when no operator is not present, you may prefer a different action.

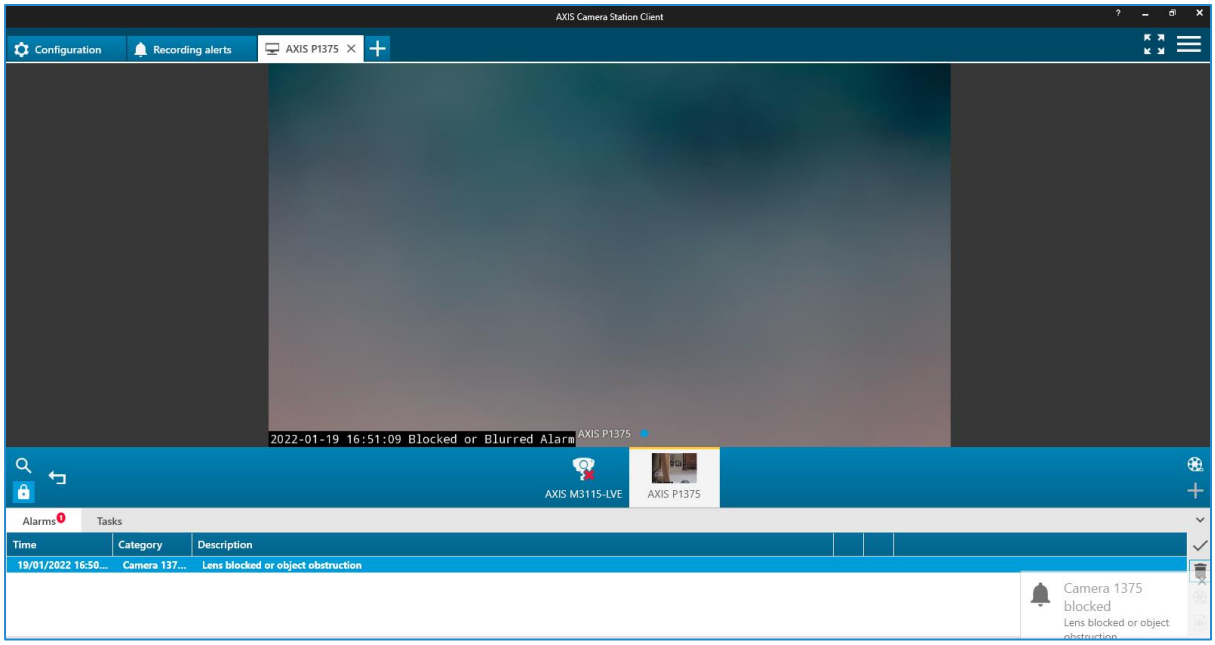


17. Select "Next" to proceed to the next step.
18. An overview of the configured event and associated actions appears. Select Finish to save this rule.



19. The complete rule now appears in the Action rule overview.
20. Repeat steps 3 - 18 for each event that you want to be notified of in the VMS client.
21. Repeat steps 3 - 20 for each camera with Araani Tamper Guard installed.

When the action rule is defined for a camera device, alarms will appear in the ACS client interface as illustrated below. Clicking the alarm will open the recording if configured as such.



Other VMS systems

Araani Tamper Guard supports the UltraView Security Center from Carrier through the use of a custom bridge software that translates Araani event communication towards the VMS protocol.
Other VMS software can potentially be integrated through custom solutions, using the Araani protocol.
For any of these cases, contact your supplier for more information.

Technical specification

Functional specification

Type:	Araani Tamper Guard is an intelligent video surveillance solution that will detect tampering events and reduced image quality.
Event types:	Araani Tamper Geard can generate following mutual exclusive events:
TAMPERING	• Blocked / blurred alarm: Detection of: o Blurred image (out of focus, rain/snow/large dirt stains on lens...). o Blocking of image by object or spray. This alarm remains active as long as the alarm condition is present. As soon as the image is restored, the alarm will automatically switch off. • Exposure alarm: As soon as the mean brightness is below the minimum or above the maximum threshold, an alarm will be raised. This alarm remains active as long as the alarm condition is present. As soon as the image quality is restored, the alarm will automatically switch off. • Camera redirected alarm An event is reported when the field of view changed abruptly. The functionality is based on a loss of background image and will react on any type of different background. The new field of view will be learned as new background, so after a few seconds the event is switched off.
IMAGE QUALITY	• Image quality alarm Detection of image degradation: o Dirty cameras. o Lens (slowly) out of focus. This alarm remains active as long as the alarm condition is present. As soon as the image quality is restored, the alarm will automatically switch off. • Image quality warning Optional feature to receive a warning before the maintenance alarm is raised, in order to take preventive maintenance actions or schedule camera maintenance.
Easy set of parameters:	• Tampering: o Sensitivity level. • Image quality: o Sensitivity level. o Delay.

System requirements

Camera compatibility:	Araani Tamper Guard is only compatible with Axis® cameras: • ARTPEC-6, ARTPEC-7, ARTPEC-8 or Ambarella S8 chipset. • Aspect ratio 16:9, 4:3 or 10:6 or rotated version of these.

Addendum: Araani Application EULA

This End User License Agreement ("**EULA**") between you, the End User (as defined below), and Araani NV, a registered company with company number 0505.774.826 and registered office at Luipaardstraat 12, 8500 Kortrijk in Belgium ("**Araani**"), sets forth the terms and conditions under which Araani shall provide the End User with a license to the Application (as defined below), as well as the manner in which the End User should (not) use the Application.

Please note that this EULA may be updated from time to time. The latest version shall always be available on Araani's Website and on the Application. Araani shall send the End User a notification in the Application when an update of the EULA is available. The new version enters into effect when the End-User receives the notification.

1. DEFINITIONS

Application	Araani Tamper Guard, including any updates, upgrades, enhancements, modifications or new versions made available by Araani to (the) End User(s).
Application Documentation	All written materials, binders, user manuals and other documentation/materials supplied by Araani and related to use of the Application.
Araani Tamper Guard	Araani Tamper Guard is an edge-based video analytics software that runs on an Axis® camera, that will trigger an alarm if it sees one of following disturbances in the video image, related to the visual quality.
EULA	This End User License Agreement which includes **(i)** the conditions under which the End User shall obtain a license to the Application; and **(ii)** the manner in which said license/Application should or should not be used by the End User.
End User	The person or legal entity that installs and uses the Application, including its employees or any authorized person acting on its behalf.
External Services	Third party software or hardware to which the Application may have access or with which it may communicate.
Intellectual Property Rights	Any and all of Araani's rights to patents, design, utility models, trademarks, trade names, know-how, trade secrets, copyrights, photography rights and other industrial and intellectual property rights relating to the Application, whether registered or not.
License Fee	Amounts due by the End User for obtaining and using a license to the Application.
Privacy Legislation	**(i)** the General Data Protection Regulation of 27 April 2016 ("the Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC"), including all future changes and amendments thereof; and/or **(ii)** all similar national data protection laws that are applicable to the processing of personal data within the scope of this EULA.
Supplier(s)	Araani authorized vendor(s) of the Application or of a hardware device equipped with the Application.
Trial license	The temporary installation and use of the Application in order to evaluate the performance, quality and suitability of the Application.
Website	Araani's official website: https://www.araani.com.

2. SCOPE OF LICENSE

2.1 Standard license to Application

2.1.1 Subject to approval to and compliance with this EULA, Araani grants, for the duration of this EULA (*cfr.* **Article 3**), the End User a limited, personal, non-commercial and non-transferable license to **(i)** use the Application and/or **(ii)**, install this Application on a hardware device that it owns or controls (where applicable).

2.1.2 The number of allowed installations and uses depends on the type of license:

- ✓ A **single instance license** allows the End User to use and/or install the Application on one (1) hardware device.
- ✓ A **bulk license** allows the End User to use/and or install the Application on the number of hardware devices as described in the order.

2.1.3 The terms of this EULA shall govern the Application as well as any standard upgrades, updates, enhancements or other modifications to the Application provided by Araani, unless such upgrade, update, enhancement or other modification is accompanied by a new or customized End User License Agreement.

2.2 Trial license

2.2.1 Trial licenses are available to the End User for the Application with a limited activation period. Continued use of the Application beyond said activation period requires the purchase of a standard license to the Application.

2.2.2 The terms described in this EULA apply both to standard and to Trial licenses.

2.2.3 By installing the Application with Trial license, the End User automatically acknowledges the Intellectual Property Rights of Araani (*cfr.* **Article 6**).

2.3 Non-transferable

2.3.1 The End User acknowledges that both the standard license (*cfr*. **Article 2.1**) and the Trial license (*cfr.* **Article 2.2**) are non-transferrable. This means that the End User may not / cannot:

- ✓ transfer such licenses to any third parties, including its affiliates. Accordingly, any third party / parties requiring the Application must request their own copy of the license;
- ✓ move licenses to other hardware devices. An activated license is linked to the unique serial number of a specific hardware device and therefore cannot be installed again on other pieces of (a) hardware device(s). Such action requires the purchase of a new license or is subject to a service contract, e.g. in case of hardware failure (provided that this hardware is (still) covered by the warranty);
- ✓ distribute or make the Application available over a network where it could be accessed or downloaded by third parties.

3. DURATION

3.1 This EULA applies for the duration of the use of the Application by the End User, unless terminated in accordance with **Article 9**, and takes effect from the moment that the Application is used on the intended hardware device.

4. CONDITIONS OF USE

4.1 Acceptable use of the Application

4.1.1 The End User hereby agrees to use the Application in accordance with certain restrictions and conditions. In particular, the End User shall not use the Application in a manner that Araani believes:

- ✓ copies (part of) the Application in any way shape or form (except as permitted by this EULA);
- ✓ reverse-engineers, disassembles or otherwise attempts to derive the source code of the Application;
- ✓ modifies, alters, tempers with, or otherwise creates derivative works of the Application;
- ✓ transfers the license to the Application to a third party in violation with **Article 2.3** of this EULA;
- ✓ violates Privacy Legislation;
- ✓ violates or otherwise encroaches on the rights of Araani or others, including, but not limited to, infringing or misappropriating any privacy, human, intellectual property, proprietary right;
- ✓ advocates or induces illegal activity;
- ✓ interferes with or adversely affects the Application or use of the Application by other End Users;
- ✓ is in general to be considered abnormal use of the Application.

4.1.2 The End User commits itself to:

- ✓ apply all reasonable techniques, practices and/or technology (e.g. use of strong passwords that are regularly changed) to prevent unauthorized use of the Application by a third party;
- ✓ always use the latest, updated version of the Application as (and if) made available by Araani (*cfr*. **Article 7.1**);
- ✓ notify any malfunction or disruption (due to, for example, bugs or malicious code) of the Application to the Supplier of which the End User bought the license).

4.2 Legal disclaimer

4.2.1 The Application should in all cases be used by the End User only for the purpose for which it is intended, taking into account the specifications indicated above.

4.2.2 In no event can Araani or its affiliates be held accountable for any – direct or indirect – damages for loss or damage of property, death or personal injury to any person.

5. DATA PROTECTION

5.1 In principle, access to / the use of the Application by the End User does not automatically result in the processing by Araani of personal data. However, Araani may receive and process the personal data of an End User in the event it is requested by a Supplier to provide second line support;

5.2 In such case, Araani shall process such personal data of the End User in accordance with Privacy Legislation and with the Araani privacy policy as published on the Website: https://www.araani.com/en/standalone-pages/privacy-policy/.

6. INTELLECTUAL PROPERTY RIGHTS

6.1 The End User acknowledges that Araani is and remains the sole owner of all Intellectual Property Rights related to the Application, developed by Araani itself (or by a third party for the benefit of Araani). Nothing in this EULA shall be construed as to limit Araani's right, title and interest in the Application.

6.2 Araani warrants that the Application does not infringe upon the intellectual property rights of any third parties. If a third party (successfully) claims that the Application infringes upon its intellectual property rights, Araani shall obtain the right to use the third-party software or will amend or replace it so as to allow the End User to lawfully use it.

7. WARRANTY

7.1 Compatibility

7.1.1 Araani warrants for one (1) year that the Application shall run on compatible hardware devices and that the Application shall perform substantially as described in the Application Documentation.

7.2 Software maintenance and updates

7.2.1 During the first year of the license, Araani shall (proactively) take all commercially and technically reasonable measures to ensure that the Application is error/defect-free and free of malicious code. To that effect, Araani shall to its best abilities make sure that the Application is regularly updated and shall perform software maintenances if required. Beyond said first year, Araani shall only be required to proactively update the Application to fix severe bugs or other malicious code that make it impossible or seriously prevent the use of the Application (in general or by a specific End User).

7.2.2 The End User acknowledges that the aforementioned is subject to its own efforts to:

- ✓ notify any bugs of or other errors in the Application to the Supplier; and
- ✓ use, at all times, the latest (updated) version(s) of the Applications, if made available to the End User.

7.3 Exemptions

7.3.1 Araani shall not warrant:

- ✓ that the Application shall work on every hardware device and on future versions and upgrades of such hardware device, given the ever evolving and changing nature of technology;
- ✓ that all defects in the Application shall be corrected;
- ✓ the compensation for damage caused by an alteration or a modification made by the End User or another non-authorized person, or the correction or reparation of any malfunction caused by such alteration/modification;
- ✓ the correction or reparation of a malfunction caused by (non-limited) **(i)** the improper use or installation of the Application in violation with **Article 4.1.1**; (ii) negligence of the End User or any other breach of its commitments under **Article 4.1.2**; or **(iii)** a power surge or failure at the End User's location.

7.3.2 Araani is not responsible for examining or maintaining the compliance of external hardware devices, in which the Application is installed and shall not warrant the compensation of any

damage or the correction of any malfunction of the Application caused by such external hardware device.

7.3.3 If national law applicable to the use of the Application provide that certain warranties cannot be excluded or can only be excluded to a limited extent, this EULA shall be interpreted in accordance with such national law provisions.

8. LIMITATION OF LIABILITY

8.1 Araani's liability

8.1.1 Araani's total liability to the End User for all claims relating to this EULA or the use of the Application shall not exceed the License Fee.

8.2 Exemption for indirect damages

8.2.1 Araani shall not be liable for any incidental, special, indirect, or consequential damages whatsoever, such as, but not limited to: damages for loss of property, loss of profits, loss of revenue, loss of data, business interruption, reputational damage, (legal) advisory fees, etc.

8.3 Wilful misconduct, gross negligence, personal injury or death

8.3.1 The limitations of liability set forth in this **Article 8** shall not apply to damages caused by wilful misconduct or gross negligence, personal injury or death attributable to Araani or the Application.

9. TERMINATION

9.1 Breach of any of the terms of this EULA by the End User shall result in the immediate revocation of the standard or Trial license. In such case, the End User shall not be entitled to a refund of the License Fee.

9.2 Upon termination (for whatsoever reason), the End User is obliged to destroy all copies of the Application and associated license files, including backup or archival copies on external storage, and uninstall the Application from all hardware devices it owns or controls.

10. EXTERNAL SERVICES

10.1 The End User agrees to use External Services at its sole risk. Araani is not responsible for examining or evaluating the content or accuracy of any External Services, and shall not be liable for any such External Services.

10.2 The End User shall not use the External Services in any manner that is inconsistent with the terms of this EULA or that infringes the Intellectual Property Rights of Araani or any third party.

10.3 External Services may not be available in the End User's languages and may not be appropriate or available for use in any particular location. To the extent the End User chooses to use such External Services, it is solely responsible for compliance with any applicable laws.

10.4 Araani reserves the right to change, suspend, remove, disable or impose access restrictions or limits on any External Services at any time, in which case it shall reasonably notify the End User thereof.

11. MISCELLANEOUS

11.1 End User acknowledges that it has fully read and understood all terms within this EULA.

11.2 This EULA supersedes any other agreement (oral or written) between Araani and the End User with the same scope. The aforementioned does not apply to customized End User License Agreement between the End User and Araani.

11.3 No deviation from this EULA shall be accepted, without prior consent of Araani.

12. GOVERNING LAW AND DISPUTE RESOLUTION

12.1 This EULA and all relations, disputes, claims and other matters arising hereunder (including non-contractual disputes or claims) shall be governed exclusively by, and construed exclusively in accordance with, the laws of Belgium, without regard to conflicts of law provisions.

12.2 The competent courts located in Kortrijk, Belgium shall have exclusive jurisdiction to adjudicate any dispute or claim arising out of or relating to this EULA (including non-contractual disputes or claims).