AXIS Perimeter Defender

User Manual

About this Document

This manual is intended for administrators and users of AXIS Perimeter Defender. It includes instructions for using and managing the product on your network. Previous experience of networking will be of use when using this product. Some knowledge of UNIX or Linux-based systems may also be useful when developing shell scripts and applications. Later versions of this document will be posted at *www.axis.com*. See also the product's online help, available through the web-based interface.

Legal Considerations

Video and audio surveillance can be regulated by laws that vary from country to country. Check the laws in your local region before using this product for surveillance purposes.

Liability

Every care has been taken in the preparation of this document. Please inform your local Axis office of any inaccuracies or omissions. Axis Communications AB cannot be held responsible for any technical or typographical errors and reserves the right to make changes to the product and manuals without prior notice. Axis Communications AB makes no warranty of any kind with regard to the material contained within this document, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Axis Communications AB 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.

Intellectual Property Rights

Axis AB has intellectual property rights relating to technology embodied in the product described in this document. In particular, and without limitation, these intellectual property rights may include one or more of the patents listed at *www.axis.com/patent.htm* and one or more additional patents or pending patent applications in the US and other countries.

Trademark Acknowledgments

AXIS COMMUNICATIONS, AXIS, ETRAX, ARTPEC and VAPIX 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.

Microsoft, Windows, Windows Vista, WWW, Internet Explorer, DirectX, Intel, Intel Core, Pentium and Xeon are registered trademarks of the respective holders.

Genetec is a trademark and Milestone XProtect is a registered trademark of respective holders.

Support

Should you require any technical assistance, please contact your Axis 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 connected to the Internet, you can:

- download user documentation and software updates
- find answers to resolved problems in the FAQ database. Search by product, category, or phrase
- report problems to Axis support staff by logging in to your private support area
- chat with Axis support staff
- visit Axis Support at *www.axis.com/techsup/*

Learn More!

Visit Axis learning center *www.axis.com/academy/* for useful trainings, webinars, tutorials and guides.

Table of Contents

About

AXIS Perimeter Defender is a scalable and flexible video analytic application for perimeter surveillance and protection. This application is ideal for high-security perimeter protection scenarios such as power plants, chemical plants and other demanding installations where there is a need to reinforce the physical access control system with reliable intrusion detection.

AXIS Perimeter Defender offers four types of scenario to detect the situations as follow:

- Intrusion: an alarm is triggered when a person and/or a vehicle enters a zone defined on the ground (from any direction and with any trajectory).
- Loitering: an alarm is triggered when a person and/or a vehicle remains in a zone defined on the ground greater than a predefined number of seconds.
- Zone-Crossing: an alarm is triggered when a person and/or a vehicle passes through two or more zones defined on the ground in a given sequence.
- Conditional: an alarm is triggered when a person and/or a vehicle enters a zone defined on the ground but did not first pass through one or more zones defined on the ground.

Installation Considerations

AXIS Perimeter Defender is primarily designed for sterile zone protection, for example, along a fence marking a boundary. The term 'sterile zone' refers to an area where the presence of people could signify intent to intrude. It is used to:

- Detect moving humans in an indoor or outdoor environment.

Note

AXIS Perimeter Defender has been optimized for outdoor detection. It will also work for indoor use as long as prerequisites are met. If the camera is too low or there are too many objects in the field of view, performance will be degraded.

- Detect moving vehicles (without discriminating between vehicle types) in indoor or outdoor environments.

AXIS Perimeter Defender normal behavior:

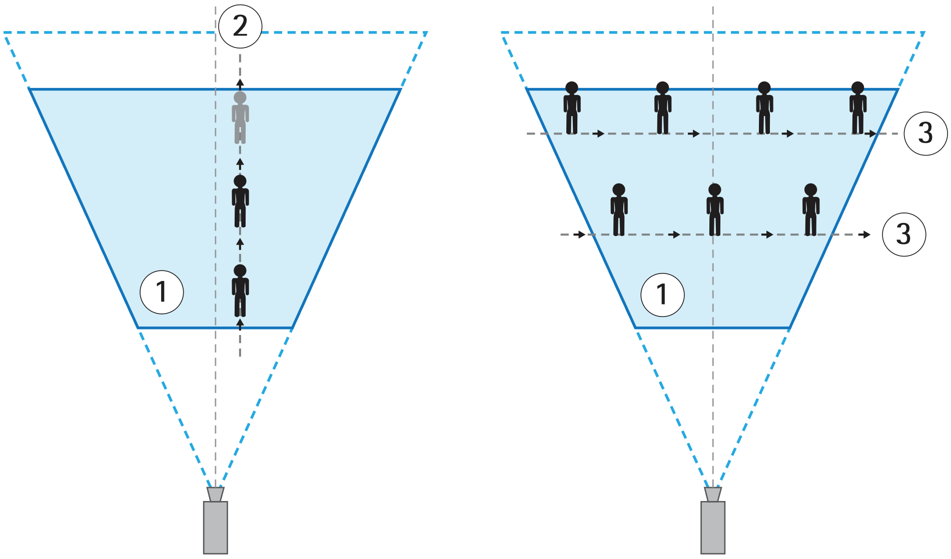
- A person or vehicle must be entirely visible in the detection zone for it to be detected initially. However, once they have been detected, AXIS Perimeter Defender carries on tracking a person or vehicle even if partially hidden (e.g. when the body of a person is hidden behind a car and only the person's head is visible).

Note

If a human/vehicle is too small or big in the field of view, it will not be correctly detected. This should not happen if you follow the requirements for camera installation.

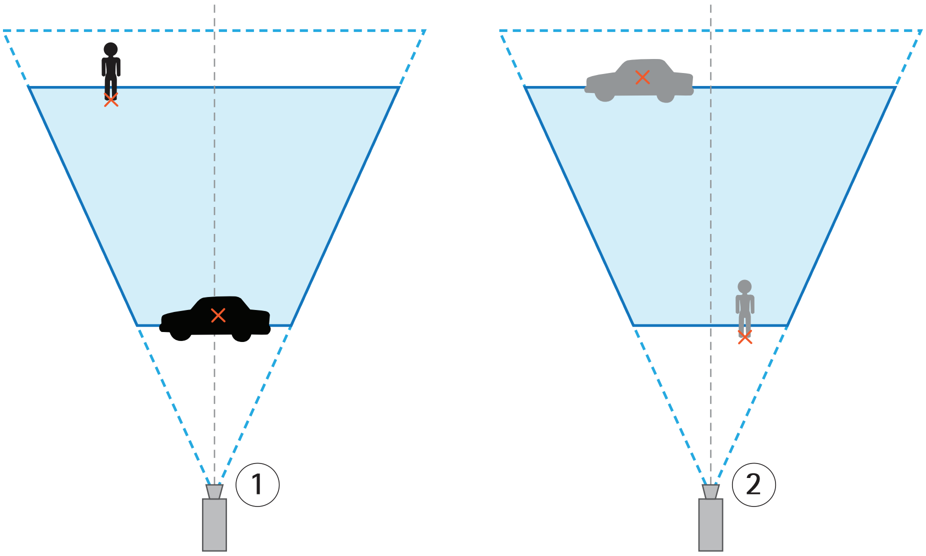
- After a few seconds of immobility, people and vehicles are no longer detected. If they start walking again after less than 15 seconds, they will be picked again by the system. If the person was in a zone-crossing zone, there is no guarantee that the scenario will correctly trigger.
- In order to be correctly detected, a vehicle must stay in the field of view of the cameras for a minimum amount of time.

About



1 Detection zone
2 A human walks away from the camera
3 A human walks perpendicular to the camera's field of view

- People or vehicles are only detected if visibly moving as seen from the camera. This means detection of a human approaching or walking away from the camera in a straight line will be decreased, compared to if the human walks perpendicular to the camera's field of view.



1 Point of detection inside the detection zone
2 Point of detection outside the detection zone

- People and vehicles will only trigger an alarm if the point of detection is inside the detection zone. On a vehicle the point of detection is in the center of the vehicle and on a human at its feet.

About

In certain environments the detection performance may be reduced. The following situations may provoke delayed or missed detections:

- Foggy conditions (detection may be improved with the use of thermal cameras).
- Direct light shining on the camera.
- Inadequate lighting level

Note

We do not recommend using AXIS Perimeter Defender in an area where there is human-presence-triggered automatic lighting.

- Overly noisy image.
- Under certain conditions (strong lights or sun casting shadows on ground), shadows can interfere with the detection process, and both misdetections and false alarms might happen.
- AXIS Perimeter Defender automatically learns the difference between “day” and “night” and uses this information to fine-tune the detection algorithms in order to optimize the detection performances. In order to learn the difference between “day” and “night”, AXIS Perimeter Defender needs to run for 24 hours, so optimal detection is achieved (both during day and night) after at least 24 hours of running.

The following situations may trigger false alarms:

- Partially hidden people or vehicles, e.g. a small van appearing from behind a wall will resemble a person since the visible part is high and narrow.
- Insects on the camera lens (Day-night cameras incorporating infrared spots attract spiders).
- A combination of car headlights and heavy rain.
- In certain conditions, large animals (similar to human size) – especially when crouch/crawl and log roll additional approach types are selected in the scenarios section of AXIS Perimeter Defender Setup interface.

Get Started

To get your site up and running, follow the steps below:

1. Place the camera, see chapter *Place the Camera on page 8* .
2. Install the software – To be able to access the AXIS Perimeter Defender Setup Interface you need to have administrator privileges, download and install the application on your PC or laptop. For system recommendations see *www.axis.com/global/en/products/axis-perimeter-defender/download*.
3. Connect to your devices and login with the root login, see *Add Devices on page 11* .
4. Install AXIS Perimeter Defender on each device – After you have installed the software on the computer you also have to install it on the camera, see *Installation on page 18*.
5. Calibrate – For AXIS Perimeter Defender to be able to interpret the scene the camera must be calibrated accurately, see *Calibration on page 20*.
6. Add scenarios – Allows the installer to define the rules for what should trigger the alarm, see *Scenarios on page 31*.
7. Integrate AXIS Perimeter Defender with Video Management Systems (VMS) – Allows the operator to get immediate and informative feedback on potential security incidents, see chapter *VMS Integration on page 40*.

Place the Camera

The maximum detection distance depends on:

- Camera type
- The Axis camera lens. A higher focal range will allow a longer detection distance.
- The minimum pixel size a human must cover the image to be detected. The pixel height of a standing person must be at least 10% of the image height and 7% on thermal cameras.
- Weather
- Lightning
- Camera load

Design Tool for AXIS Perimeter Defender

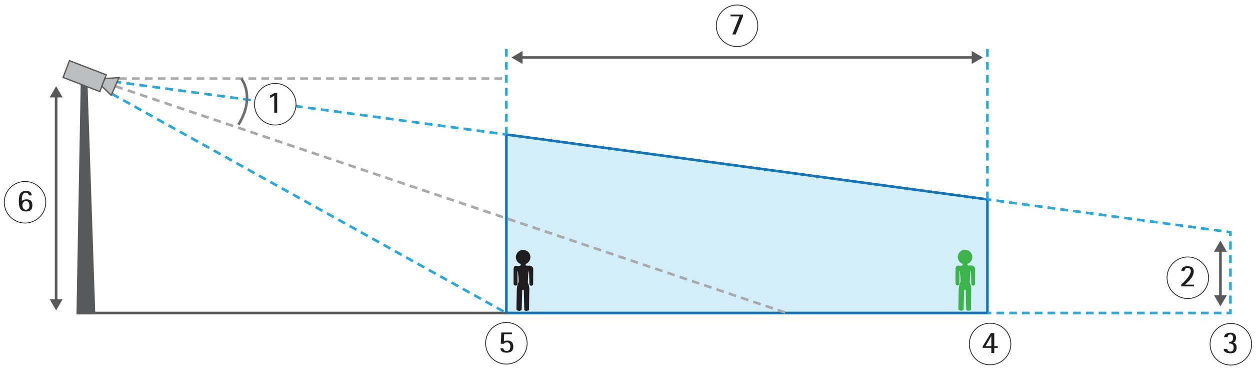
To be able to place the cameras in an effective manner, use the design tool for AXIS Perimeter Defender.

The design tool can be used to decide:

- Minimum detection distance
- Maximum detection distance
- Tilt angle
- Camera height

Recommended Camera Height and Orientation

The following drawing and notes indicates the appropriate camera orientation:

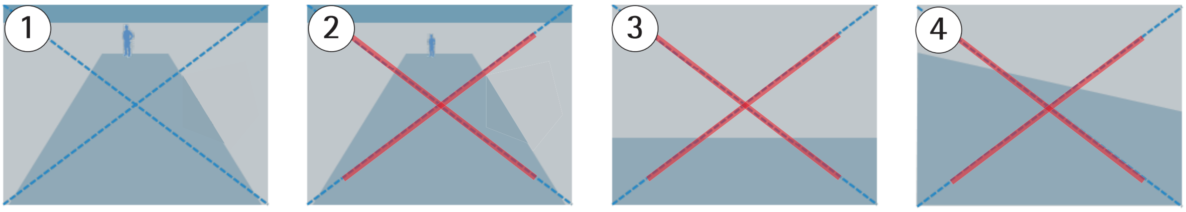


1	*Tilt*
2	*Field of view*
3	*Distance*
4	*Max detection distance*
5	*Min detection distance*
6	*Camera height*
7	*Detection zone*

- Object height: the pixel height of a standing person must be at least 10% (7% if it is a thermal camera) of the image height at the maximum detection distance (e.g. if the height of the visualized image is 576 pixels, the height of a person standing at the end of the detection zone must be above 58 pixels). The maximum height of a standing person must be 60% of the image height at the minimum detection distance.

- Tilt angle: the camera must be sufficiently oriented towards the ground so that the center of the image is under the horizon line. The side view of a person to be detected must be sufficient: Min Detection distance > Camera height / 2.

- Roll angle: The roll angle of the camera must be nearly equal to zero.



1 Object height tilt angle and roll angle are suitable.
2 The human height <10% (7% if it is a thermal camera) of the image height.
3 The center of the image is above the horizon line.
4 The roll angle of the camera is too significant.

Prerequisites for Effective Implementation

The following prerequisites are needed for AXIS Perimeter Defender to perform most effectively:

- Humans or vehicles to be detected are fully visible (from feet to head) in the image during at least 3 seconds and are not obscured by other fixed or moving objects.

- Humans or vehicles to be detected are moving on an horizontal plane or a slight slope.

- The field of view of the camera is fixed.

- The level of illumination and camera settings should be sufficient to provide enough contrast between humans or vehicles and the background. We recommend at least 50 lux in the whole detection area when using an AXIS day & night camera with artificial lighting. The Maximum Detection Distance recommended when using external IR spots is 80m and the IR spot should have a maximum distance > 2x Maximum Detection Distance. When a built-in IR lighting is used, the Maximum Detection Distance is limited to maximum 20m depending on the camera and the environment.

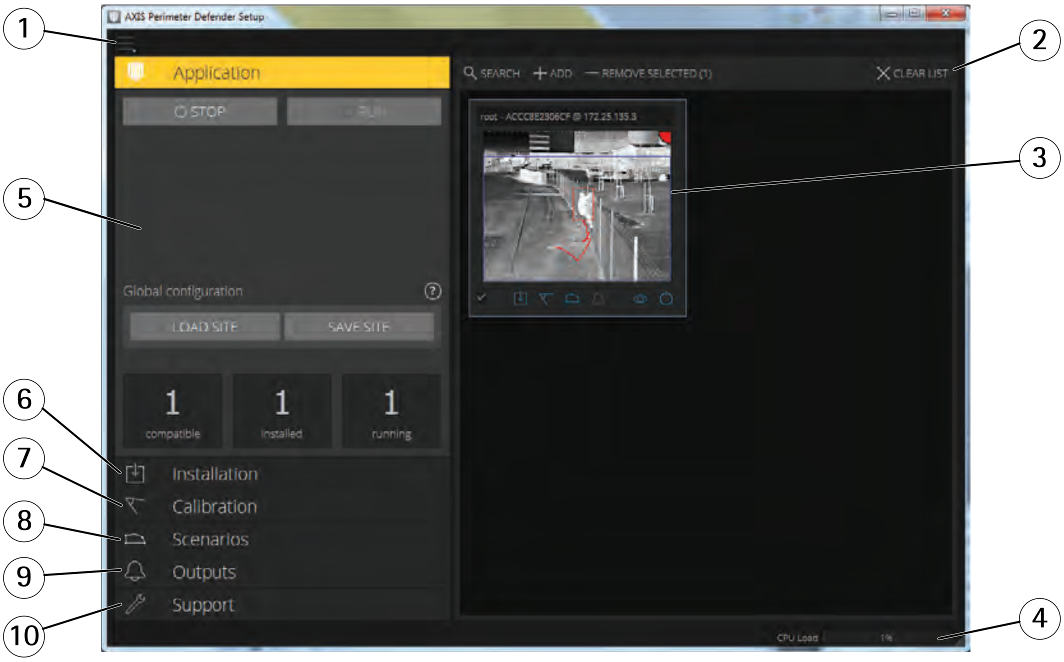
- Small camera vibrations are tolerated but maximum performances are reached for cameras which are not subject to vibrations.

- We recommend to use the AXIS Perimeter Defender Camera Design Tool to specify how the cameras must be installed on site. This tool takes into account both AXIS cameras and AXIS Perimeter Defender requirements.

AXIS Perimeter Defender Setup Interface

The setup interface offers access to the calibration and scenario definition functions – including the setup of multiple devices. Remote setup allows for configuration from wherever there is a network connection.

Overview



1. Settings for the interface, see chapter *Interface Settings on page 11*
2. Device addition tab which lets user:
   - Search for devices connected on the network, see chapter *Automatically Adding Devices – Search Function on page 11*
   - Manually add devices, see chapter *Manually Adding Devices*
   - Remove selected devices
   - Clear the list of devices, effectively disconnecting from all devices
3. Live view, fills up with live views when devices are added , see chapter *Live View on page 15*
4. The CPU load indicator indicates in real-time current computer CPU load. Too high CPU load could result in unresponsive computer/application. Make sure you close other applications when using AXIS Perimeter Defender Setup to maximize your CPU allocation. If your CPU is too high and you want to add a device, the system will issue a warning.
5. Application tab, see chapter *Application on page 17*
6. Installation tab, see chapter *Installation on page 18*
7. Calibration tab, see chapter *Calibration on page 20*
8. Scenarios tab, see chapter *Scenarios on page 31*

9. Outputs tab, see chapter *Outputs on page 34*

10. Support tab, see chapter *Support on page 34*

Interface Settings

Press the settings button to open the settings menu with the following actions available:

- Folder settings – opens a dialog where the user can decide where:
  - Device temporary files and calibration video should be stored ("Device configuration path").
  - Device configuration files from load paths should be stored ("Site configuration path").
- Camera passwords – lets the user visualize passwords already used (since the launch of the Setup interface) and add new ones.

Note

Passwords are not stored once user exits the Setup interface.

- Enable full frame rate mode – switches the frame rate in the live view from 1 fps (default) to 8 fps.
- About - Get information about the AXIS Perimeter Defender Setup interface version being used.

Add Devices

There are three different ways to add devices:

- Automatically - through a network scan.
- Manually - by specifying connection settings.
- Automatically - by loading saved site configurations.

After adding all the devices you wish to connect, it is recommended to save your site (pressing the SAVE SITE button). This is to avoid that you have to reconnect to all devices again if you have to turn off your computer before finishing setup of all devices.

Note

Your current session devices are automatically saved. You will be asked to restore them next time AXIS Perimeter Defender setup is started.

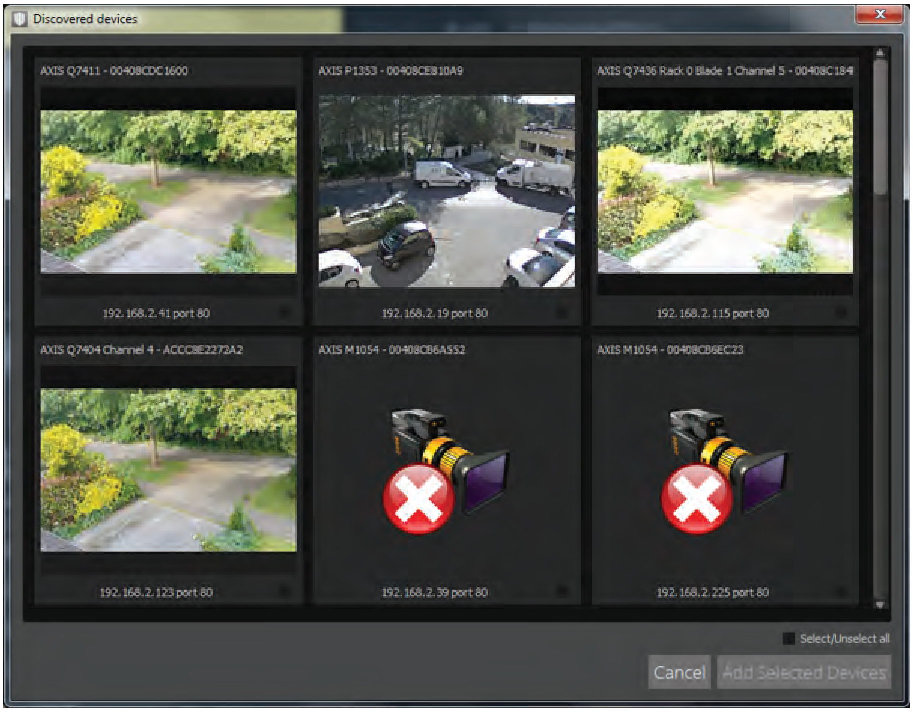
Important

Devices configured to only accept HTTPS connections cannot be connected if security certificate is not installed on the current machine. This is especially true for self-signed certificates. Certificates can be obtained by visiting the device web interface with a web browser and installing certificate. Refer to your web browser help on how to do this (if not done automatically).

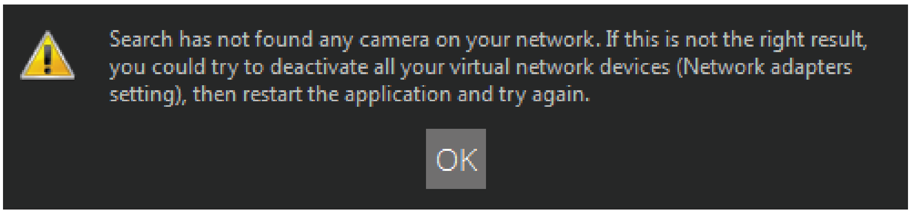
Automatically Adding Devices – Search Function

Click **SEARCH** to scan the surrounding network for devices to be connected and used. A background search of the network will start to discover potential compatible devices:

- Click **SEARCH**, when doing this for the first time and no password is available a password dialog opens, otherwise the available password are used to connect to the device.
- The scan is performed once a password is available.
- The following dialog shows devices that were found during the scan. If the password is correct a static image is captured to help you select the devices to configure. Add devices by clicking on each device or click the select all check box and press "Add Selected Devices" button to add them in the interface



- The device addition process tries to add devices one at a time. If the computer CPU load is too high a warning will be shown proposing to stop adding devices, a high CPU usage may cause the application to not work properly.
- If no cameras have been found after a time–out of 20 seconds, the following warning dialog is displayed. Virtual network adapters (like those created by Virtual Machine Software like VirtualBox) sometimes interfere with the detection process and must be disabled before performing the search.


Search has not found any camera on your network. If this is not the right result, you could try to deactivate all your virtual network devices (Network adapters setting), then restart the application and try again.

Important

The search functionality does not work across networks, i.e. AXIS Perimeter Defender Setup can only find the devices that are connected to the same sub-network of the client running the software. If you need to add devices connected to a different sub-network, use the manual addition procedure. The search functionality may also fail if the network routers/switches are configured to filter multicast.

Manually Adding Devices

Click on the ADD button. This pops-up a dialog, the user is then asked to enter the connection settings to the targeted device:

- Device IP address or hostname.

Note

If it doesn't work to add a camera by hostname, verify the network and DNS settings or add camera using its IP address.

- Device 'root' password as AXIS Perimeter Defender requires root access to be configured.

- HTTP port used to connect – default is 80.
- User can give an optional name to the device for easier recognition.
- User can also indicate that device is on a remote network for which connection may be slow. Slow connections which not are configured as remote can lead to non-working or bad calibrations. Proxy settings may also be entered. Proxy address, port and credentials have to be provided for such connections.

Note

For such connections to be acceptable it is mandatory that the user is able to connect to the device through HTTP connection. Make sure to setup the HTTP port correctly. Remote configuration can fail when the connection doesn't have sufficient or stable bandwidth.

- Press the OK button to validate the dialog and to try to connect with provided settings, Cancel aborts addition.

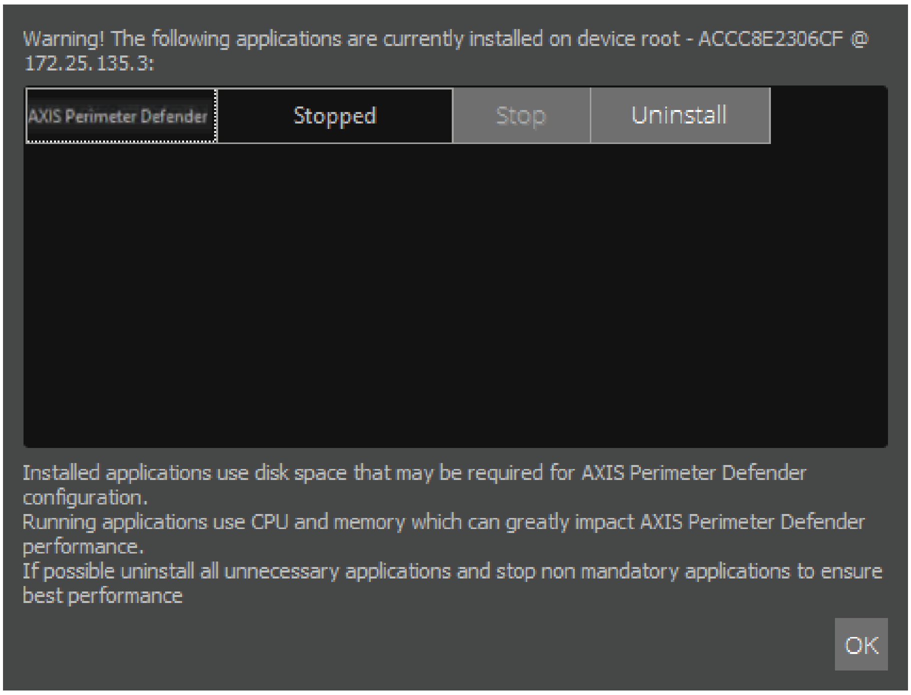
If connection information is available (i.e. an "ADD device" was performed previously) these fields are pre-filled with previous values to simplify connection to devices in the same IP range and with similar passwords.

Automatically Adding Devices – Load Saved Configurations

A site configuration is made from the different cameras that are connected. Saving a site configuration is useful to avoid having to manually reconnect to multiple devices each time. Pressing the LOAD SITE button under the application tab opens a browse dialog inviting the user to select a site file. Once selected this site file will be used to connect to the different devices that were connected when the site was saved. Connection settings are automatically restored from this site file.

Checking for Other Installed Applications on Camera

After adding a device, the setup interface automatically checks if other applications already are installed on the camera as they might impact on the detection performance and may prevent correct installation if using too much disk size. If another applications already are installed on the camera, the dialog displays the list of applications installed and their status (running or not). From this dialog the user can stop and/or uninstall these applications. We recommend you to stop any non-essential or redundant (other video analytic) applications as they use camera CPU resources, this impacts the AXIS Perimeter Defender detection performance.



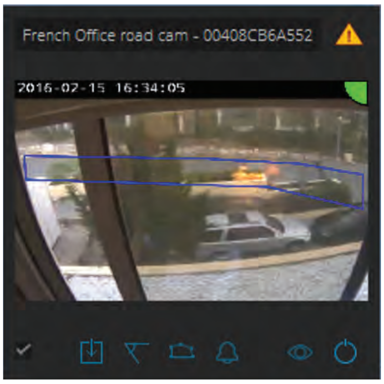
Warning! The following applications are currently installed on device root - ACCC8E2306CF @ 172.25.135.3:

AXIS Perimeter Defender	Stopped	Stop	Uninstall

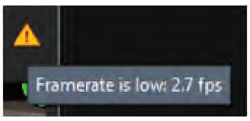
Installed applications use disk space that may be required for AXIS Perimeter Defender configuration.
Running applications use CPU and memory which can greatly impact AXIS Perimeter Defender performance.
If possible uninstall all unnecessary applications and stop non mandatory applications to ensure best performance

AXIS Perimeter Defender Setup Interface

If the camera don't have enough CPU resource AXIS Perimeter Defender will lower the frame rate. If the frame rate is running too low (below 5 frames per second) a yellow warning triangle is displayed in the upper right corner of the camera tile:



By hovering the mouse cursor over the icon, a detailed information about the actual frame rate is displayed:


Framerate is low: 2.7 fps

Note

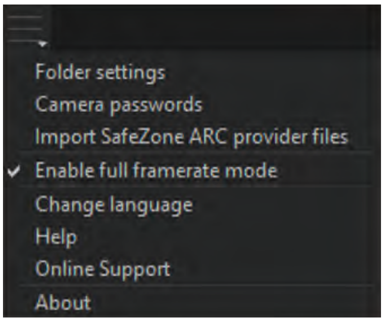
A low frame rate (below 5 fps) can significantly decrease the video analytic performances, leading to both false alarms and misdetections.

Performance Notes

Added devices take up CPU resources from the host computer to decode video streams from the camera and displays them. To limit this impact on the host computer, video stream from added devices is displayed at reduced frame rate (~1 fps) by default. Normal frame rate (~8 fps) is restored when streams are displayed maximized or during the calibration acquisition process.

Note

The "Enable full frame rate mode" option can be selected in the interface settings menu. Note that this issue should only be selected when a limited number of cameras are added and/or when the host computer has sufficient resources to support it.



Important

The "Enable full frame rate mode" mode may lead to an unresponsive interface if it is used when connecting to a too large amount of cameras and/or when using a low power computer.

AXIS Perimeter Defender Setup Interface

Problem	Possible reason	Solution
The application will not run even though the configuration is good.	The firmware of the camera is not up to date.	Make sure you have the latest firmware for the camera.
	The firmware has recently been updated	Re-install package on device and restart camera if problem persists.

Actions that can be performed on multiple devices

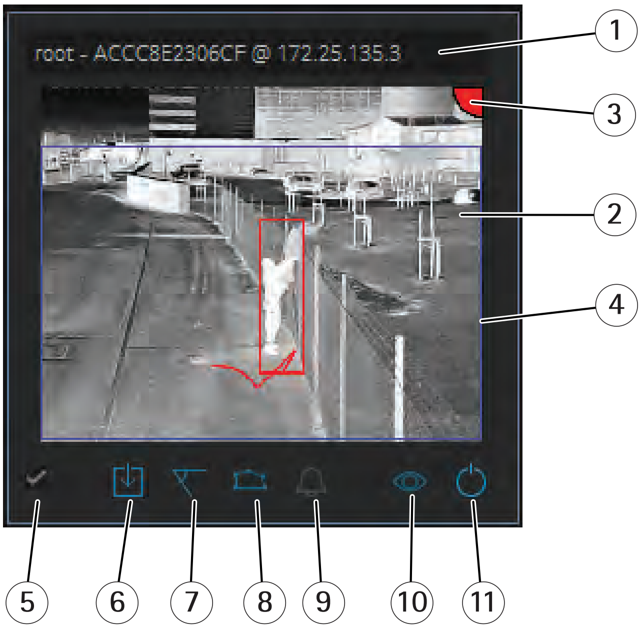
As shown in some of the previous sections, some actions can be performed on multiple cameras. These actions are limited to:

- Installation of AXIS Perimeter Defender
- Installation of license
- Uninstallation *
- Running *
- Stopping AXIS Perimeter Defender*
- Calibration
- Backing-up / restoring / clearing configurations

*If selected cameras do not have the same status only the logical action will be performed. For example if 3 cameras are selected and 2 of them have AXIS Perimeter Defender running, clicking "Run" will only start AXIS Perimeter Defender on the camera where AXIS Perimeter Defender is not already running.

Scenarios and Output tabs are disabled when multiple devices are selected. Clicking on one of the quick access buttons in the device live view will nevertheless open the related tab for the clicked device.

Live View



1 Current device name
2 Live image
3 Alarm status

4 *Detection areas*
5 *Selection check box*
6 *Installation status / quick access button*
7 *Calibration status / quick access button*
8 *Scenarios status / quick access button*
9 *Outputs status / quick access button*
10 *Overlay status / quick activation button*
11 *Running status / quick activation button*

Each connected device is displayed as shown in the figure. It provides status of the device and quick access to the main functions.

- Current device name – Can be edited by the user to give a friendlier name. The name will always contain, besides the "friendlier" part, the camera IP address and MAC number.

Note

Hover the mouse over a device name to display the aspect ratio used for analysis which provides maximum field of view coverage. It will also indicate if the device is on a remote connection.

- Live image from the connected camera. In the overview mode the frame rate is 1fps and when the live view is maximized it is 8 fps.
- Alarm status – Only visible if overlay is active and AXIS Perimeter Defender is installed, configured and running. The color displays the alarm status:
  - Grey = Not active – Loading configuration settings
  - Green = Active
  - Red = Alarm triggered
- Detection areas - Only visible if the overlay is active and AXIS Perimeter Defender is installed, configured and running
- Selection check box – Indicates if a device is selected or not. Click to select a device.
- Installation status / quick access button – Click to open the installation tab for the device. The color displays current installation status:
  - Grey = Not installed
  - Orange = Installed but not licensed
  - Blue = Installed and licensed

Hover with the mouse cursor over this button to display the version of the AXIS Perimeter Defender installed on the camera. The icon may also be shown as 🔄 when a more recent version is available for installation.

- Calibration status / quick access button – Click to open the calibration tab. The Color indicates calibration status (grey = not calibrated / blue = calibrated).
- Scenarios status / quick access button – Click to open the scenarios tab. The color indicates scenarios status (grey = no scenario defined / blue = at least one scenario defined).
- Outputs status / quick access button – Click to open the output tab. The color indicates outputs status (grey = no outputs configured / blue = at least one output configured).
- Overlay status / quick activation button – Displays overlay status (grey = inactive, blue = activated). Click to activate/deactivate overlay. Overlay is shown as a bounding-box around detected objects as well as a "snail-trail" displaying trajectory of objects.

Note

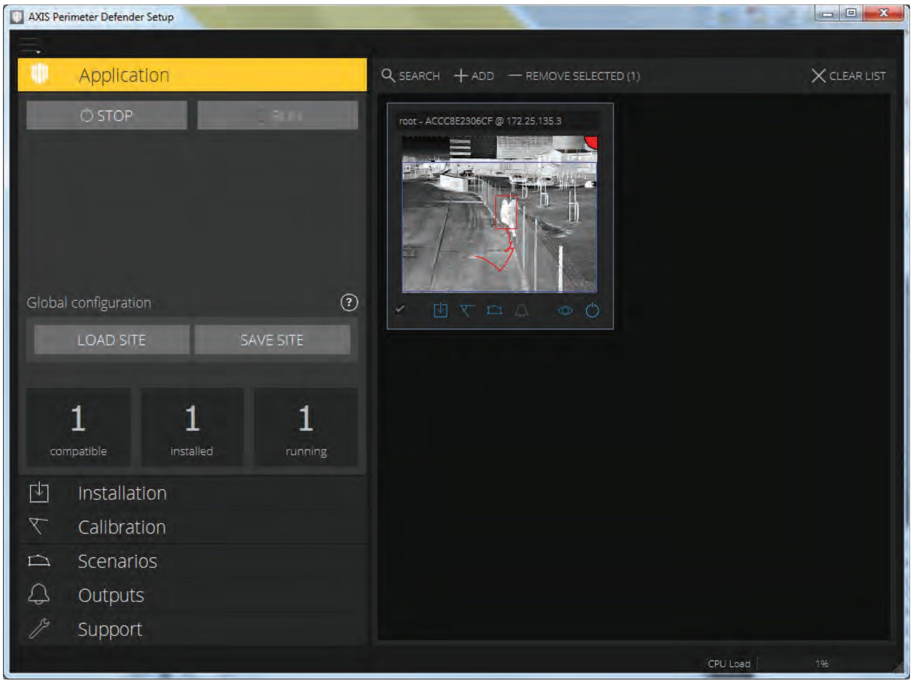
Overlay is only available if direct connection from the camera to the user's computer is available (i.e. if no firewalls or similar devices prevent connection to overlay port on device).

- Running status / quick activation button – Displays current running status (grey = inactive, blue = activated). Click to run/stop AXIS Perimeter Defender.

Note

Double click on live view image to maximize it.

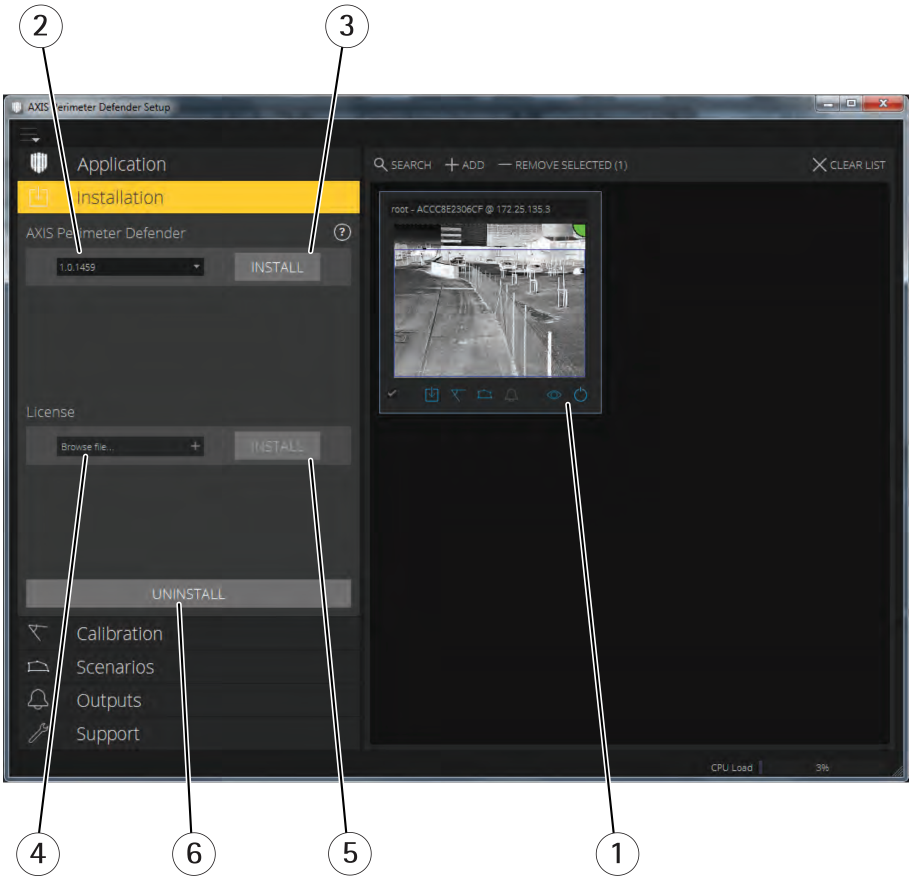
Application



- **Run** – Start the analytics on the selected device(s).
- **Stop** – Stop the analytics on the selected device(s).
- **Load Site** – Load a previously saved site (devices and their configuration files)
- **Save Site** – Save the current site (i.e. save all the device information as well as their respective configurations files)

You can also see the number of compatible devices added, the total number of devices with AXIS Perimeter Defender installed and the number of devices on which analytics is running.

Installation



1. On a device where AXIS Perimeter Defender never has been installed the display should have all icons greyed out. This is also shown after uninstalling the program from a device.

2. Available AXIS Perimeter Defender versions – These versions are automatically found in AXIS Perimeter Defender Setup interface installation directory. The latest version is always presented first. The user can select which version to install or browse for another version (that may have been provided as an update for example). It is recommended to use the latest available version.

3. **INSTALL** – Press the button to install the selected version on the selected device(s).

4. License file/folder – Press the "+" icon to open a browse dialog inviting the user to:

   - Select the license file corresponding to the selected device if only one device is selected.

   - Select a folder where license files are stored in case multiple devices were selected.

5. **INSTALL** – Press the button to install the license on selected devices. Error message will be shown if no license is found for selected device(s).

6. **UNINSTALL** button – Removes AXIS Perimeter Defender and its license and configuration from the selected device(s).

Tip: If AXIS Perimeter Defender is already installed on the camera, it is possible to know exactly the installed version by selecting the camera and hovering the cursor on the "Installation status" button on the live view.

AXIS Perimeter Defender Setup Interface

Fresh Installation

A fresh installation is performed on devices where AXIS Perimeter Defender has never been installed or uninstalled:

1. Select version to install and press install.
2. After a short moment a success notification is shown.
3. Browse for a license then press install.
4. Once again after a short moment a success notification is shown.

AXIS Perimeter Defender is now installed on the selected device(s) and will start automatically.

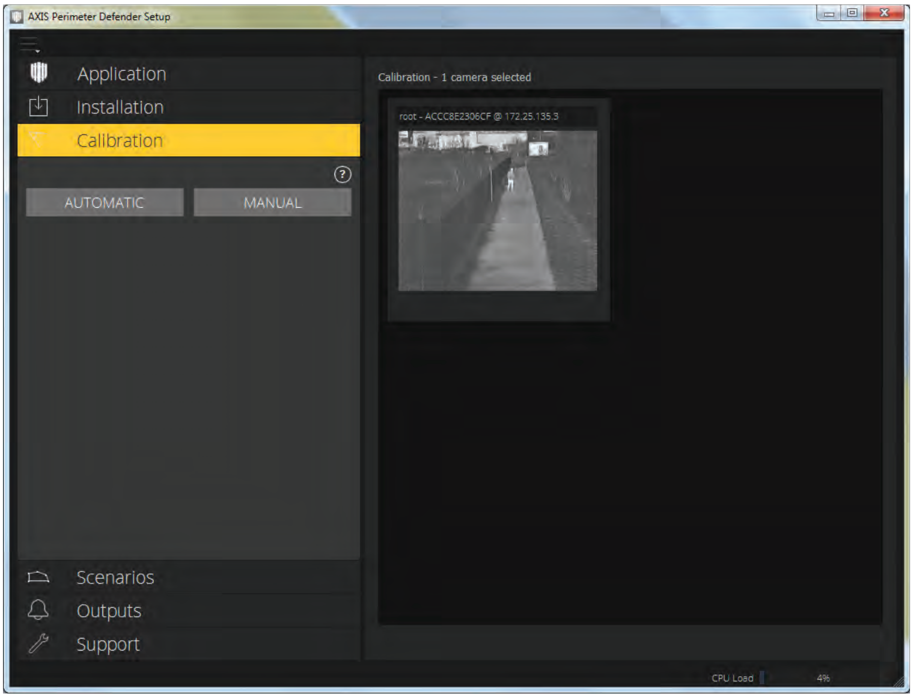
Update Version

It is possible (and recommended) to update an existing version of AXIS Perimeter Defender to take advantage of latest improvements without having to re-calibrate and redefine scenarios. To update an installation:

1. Download and install the latest version of the AXIS Perimeter Defender.
2. Select version to install. A warning will be displayed if the version is older or already installed.
3. Press **INSTALL**. AXIS Perimeter Defender Setup will perform the following steps:
   - Back-up the existing calibration, scenarios, parameters and license.
   - Install new version.
   - Restore license.
   - Restore calibration and scenarios.
   - Restore parameters.
   - If an application was running it is started.

A success notification is shown. The selected device are now updated.

Calibration


AXIS Perimeter Defender Setup
Application
Installation
Calibration
AUTOMATIC
MANUAL
Calibration - 1 camera selected
root - ACCC8E2306CF @ 172.25.135.3
Scenarios
Outputs
Support
CPU Load
4%

For the AXIS Perimeter Defender engine to correctly interpret the scene under surveillance, the camera must first be calibrated accurately. The auto-calibration function is used to simplify this step. A manual calibration mode is also available for when auto-calibration is infeasible, or for fine tuning.

All cameras and encoders needs to be calibrated. There are two steps to calibration. The first is to introduce points of reference that provide depth and height information for the processor and the second is to define the broad zone of interest that will be monitored.

The first step can be completed with either the auto-calibration function or the manual calibration mode. The installer first has to select a device(s) to be calibrated in the device browser on the right. To start the calibration process, click the **Calibration** tab in the navigation pane on the left and select a calibration approach.

Note

Before a camera can be calibrated, the application and a valid license must be installed on the camera.

Auto-calibration

This mode allows an installer to calibrate one or more camera(s) by undertaking a simple walk through the scene under surveillance. The camera will automatically capture the information required to calibrate itself.

1. Select the device(s) to be calibrated in the device browser on the right and ensure that the AXIS Perimeter Defender application and a valid license have been installed – Signalled by this blue icon on the device thumbnail.
2. Click the **Calibration** tab in the navigation pane or the calibration icon on the device thumbnail (this will perform calibration for this particular device only).
3. Select **AUTOMATIC** in the Calibration tab.
4. Set the recording start time and duration (leaving enough time for the installer to walk into and then out of the scene), enter the installers height (in cm) and click **CAPTURE** or click **USE PREVIOUS CAPTURE** to reuse a previously captured video.

5. The installer should then walk through the scene, following a zigzag path covering as much as possible the field of view of the camera. See the following picture for an example of correct walk. The capture should start at least 10 seconds before the installer expects to enter the field of view. During the walk, ensure that the installer:

   - Walks in a path that covers as much as possible of the detection zone from front to back of the scene (a V-shaped path across the field of view will typically suffice).

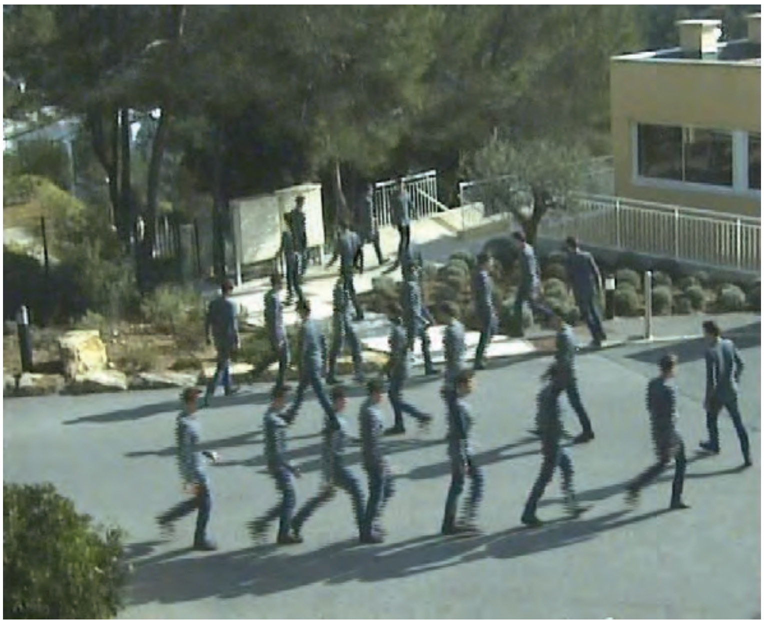
   - Remains almost always fully visible (from head to feet) in the field of view.

   - Walks slowly in straight lines.

   - Keeps an upright posture while walking (avoid bending postures when changing direction. Making a little stop of 1-2 seconds before changing direction helps).

   Note

   Auto-calibration for remote camera not connected as remote only works if the installer walks several minutes (around 5) in front of the camera to make sure a sufficient number of images are captured. The frame rate is usually lower for devices on remote networks.



6. Limit the duration of the video to the minimum required to cover the area, since the length of the video affects the subsequent calibration computation.

Note

The recorded walk sequence will also be used to verify that the scene has been correctly calibrated.

7. When the installer returns to the setup interface, he is required to verify that auto-calibration has been successful by confirming that the installer is detected accurately on screen as they move through the scene in the walkthrough footage, see *Verifying the Calibration* .

8. If the calibration was successful click **ACCEPT**. If the auto-calibration has failed for any reason, click **NEW** to repeat the auto-calibration or **MANUAL** to switch to manual calibration.

9. If the auto-calibration is accepted, the installer is presented with a view of the maximum detection area, which can be adjusted if required. This zone will cover the maximum extent of the area to be monitored – and is the default intrusion detection zone. The initial zone represents the maximal detection zone. Outside of this zone, intruders might be detected but it is not guaranteed.

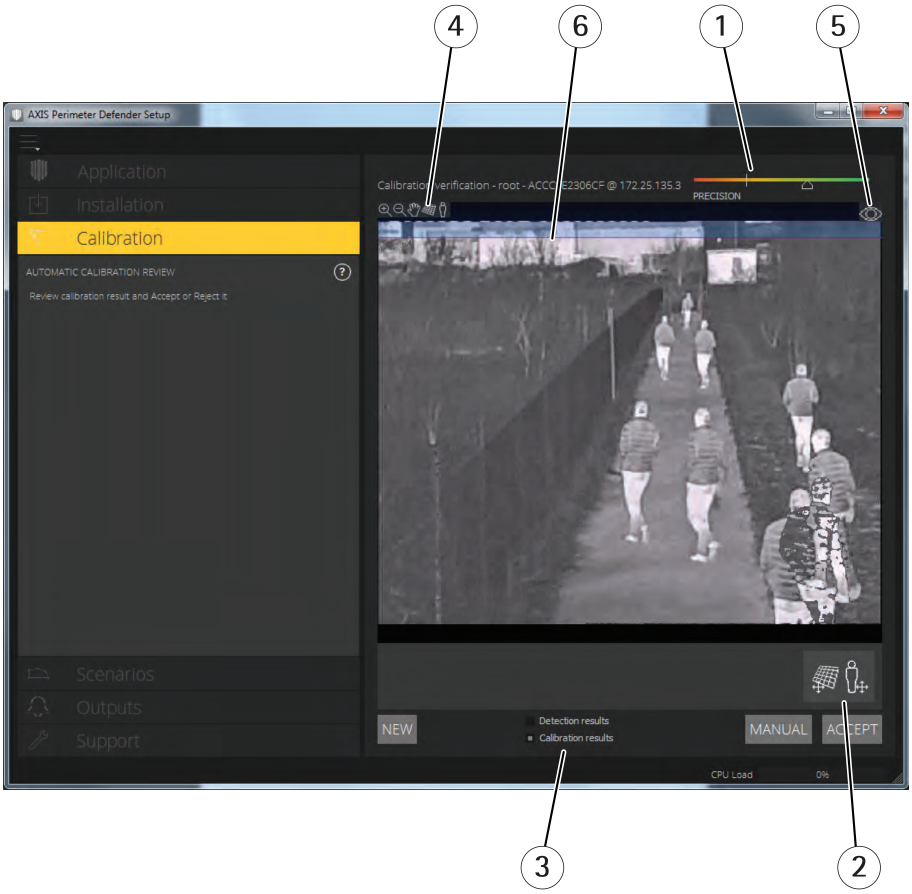
Note

For a successful automatic calibration, follow these guidelines:

- Avoid automatically calibrating when there are a lot of people in the camera field of view.
- Avoid automatically calibrating when there are a lot of vehicles passing in the camera field of view.
- Avoid automatically calibrating when there are moving trees (e.g. because of wind) in the camera field of view.
- Do not attempt to calibrate camera installed not parallel to the ground (i.e. having a roll) as it will not work..
- If it is not possible to cover the whole field of view from front to back because of a physical limitation (e.g. something that prevents the installer to go all the way back), then it is better to switch to manual calibration.

Verifying the Calibration

There are several ways you can verify the quality of your calibration. Once the automatic calibration has finished, you will be presented with a preview pane.



AUTOMATIC CALIBRATION REVIEW

Review calibration result and Accept or Reject it

1 *Calibration precision*
2 *Manipulators*
3 *Static/dynamic view*
4 *View modifiers*
5 *Toggle display between calibration (merged) image and live view.*
6 *Horizon line*

The image shown in the preview pane will show selected positions of the installer during the walk through the scene under surveillance. If no person is visible, the automatic calibration has failed.

The precision indicator reflects an automatically computed precision level that measures how well the installer covered the scene and how well they were detected. If the precision indicator is in the red zone the calibration has failed and you are not able to click **ACCEPT** , see *After a Failed Automatic Calibration on page 25*.

The horizon line represents the visible end of the scene ground plane (if nothing is blocking the view). When defining scenarios, it is not possible to place scenario zones in the blue area above the horizon as this is above the ground and scenario zones are – by definition – on the ground.

Grid

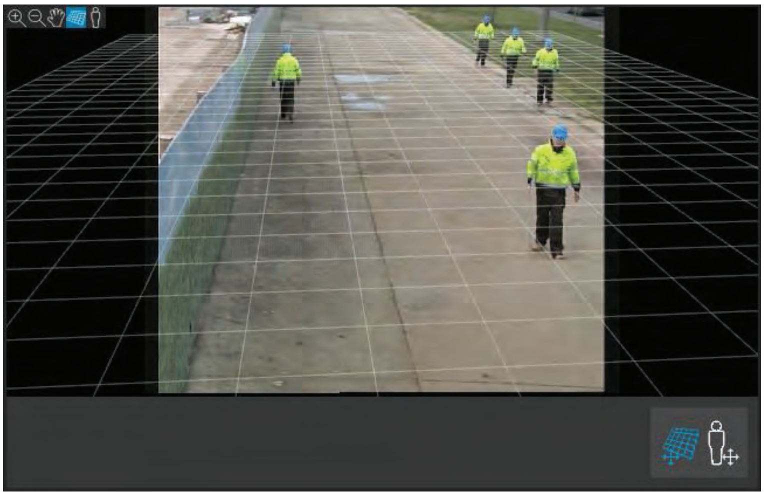
The manipulators allow you to place a grid or an avatar on top of the image. The grid should correspond to a square grid on the ground. You can toggle the display of the grid by clicking the grid view modifier icon.

Important

The grid will not affect the calibration, it is a tool to see if the calibration is correct.

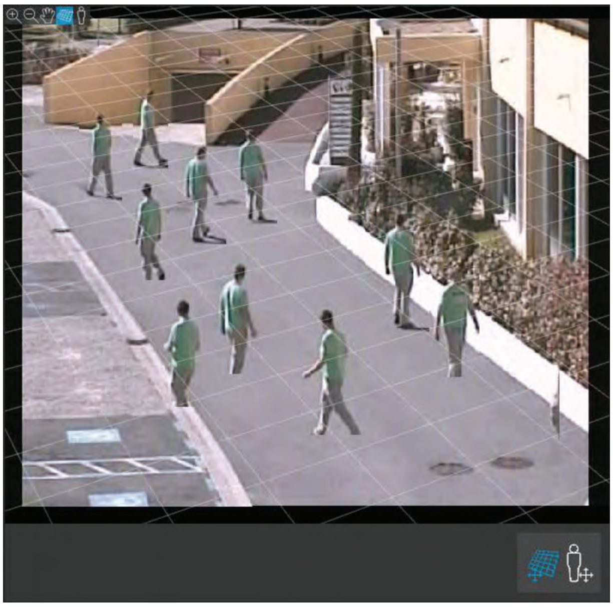
When the grid manipulator is active, you can turn the grid by dragging it in the preview pane. Try to align it with some structure in the scene to see if the result seems reasonable (see figures below):

- If the grid is parallel to the ground (it does not have a weird slope) and, after having applied the necessary rotation to the grid, it is parallel to man-made artefacts that are parallel in the real world, then the calibration is good.



Grid correctly aligned with road shoulders means that the calibration is correct.

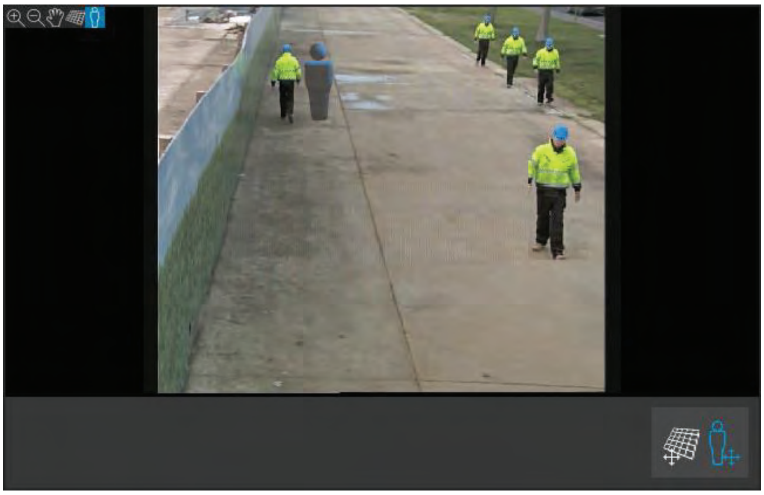
- Otherwise, the calibration is probably bad.



The grid does not align correctly with the road shoulders, meaning that the calibration can be improved.

Avatar

The avatar manipulator allows you to place a 3D person avatar of average height in the scene. You can toggle the display of the avatar by clicking the avatar view modifier icon.



Its size in the view pane will correspond to the size we expect an average person to be at that point according to the current calibration. By moving the avatar around you can make sure its size is reasonable in relation to any object or people visible. For example, for the same person you must expect the avatar to have the same height (the person height) in the front of the scene, where it is nearest to the camera, and on the back. You should check the avatar at different positions as the avatar may have good size at a specific position but incorrect size elsewhere in the image.

Detection Results

Finally you can check how AXIS Perimeter Defender would "see" your captured installer walkthrough video by switching the preview pane to **Detection results**, paragraph 3 in *Verifying the Calibration* . This will display a video player, showing how AXIS Perimeter

Defender would perform with the current calibration if it received the video footage of the installers walk as a live stream. After a short initialization phase (a few seconds), people or vehicles entering the scene under surveillance should be marked with a rectangle (Reviewing calibration may not work on remotely connected cameras because the capture can have a too low frame rate. It does not mean that the configuration has failed, Use the avatar and the grid to verify calibration). Most of the time people should be marked with red rectangles and vehicles with blue rectangles. If this is the case, the calibration is fine. However, if too often people or vehicles are not marked, the automatic calibration has most likely failed.

Note

If the installer is too far away, he might not be marked. A minimum size is necessary for the detection to work.

A red zone (displayed in the following image) shows the detection limit zone according to the computed calibration, i.e. the zone where the prerequisites on the human height in the image are not respected, i.e. the zone where the detection might fail because of the target size.

Note

If computed calibration is wrong, the red zone will be wrong as well.

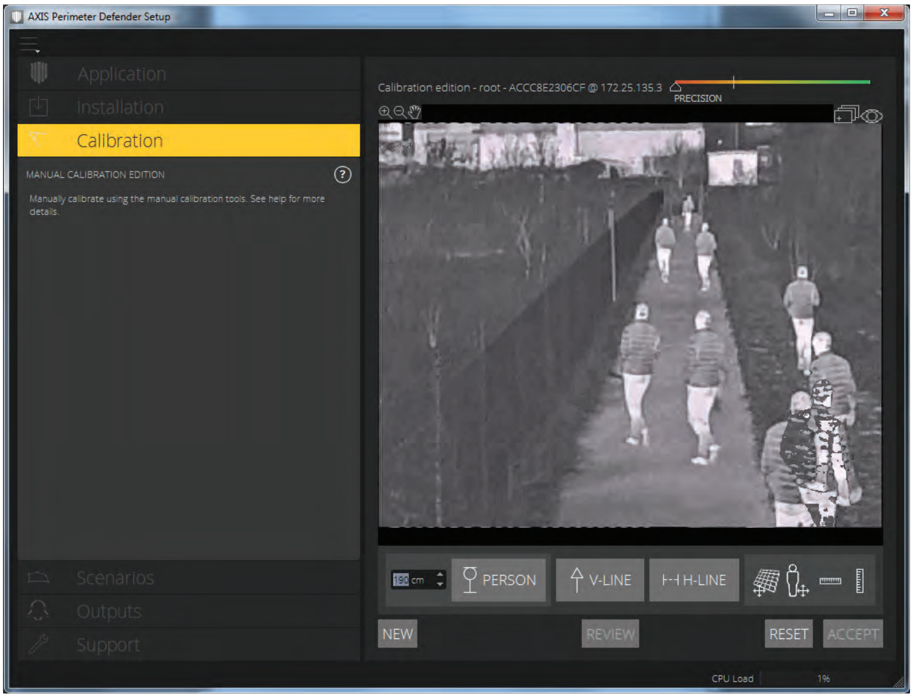
Once satisfied with the calibration quality, click **ACCEPT**. This will bring you to scenario definition step. If the automatic calibration has failed, click **NEW** to retry or click **MANUAL** to go to manual calibration.

Manual Calibration

This mode is provided in the event that auto-calibration fails on a particular camera – or for installers that prefer to revert to a more conventional approach to camera calibration. For example, this mode is ideal when it would be impractical to conduct an installer walkthrough and in situations where objects of known height are in the scene. An obvious example of this would be a remote perimeter with a fence line consisting of a number of evenly spaced fence posts of a consistent height. Whilst it requires more effort than automated modes, manual calibration is designed to be simple to perform.

After a Failed Automatic Calibration

This section describes the procedure for manual calibration after automatic calibration has been attempted and has failed. This means that at some point during the review process, the installer clicked the **MANUAL** button. The editor pane will be displayed as seen in figure below.



AXIS Perimeter Defender Setup

Calibration edition - root - ACCC8E2306CF @ 172.25.135.3

MANUAL CALIBRATION EDITION

Manually calibrate using the manual calibration tools. See help for more details.

190 cm

Manual calibration - Editor Pane

Several of the elements from the Preview Pane are also found in the Editor Pane. The calibration engine calibrates by estimating:

- The horizon.
- The way vertical lines spread out (or fan out) in the image.
- The scale of the scene.

Manual calibration is carried out by manually providing this information about the scene – calibration elements – to the calibration engine. These calibration elements can take three forms:

- **Person sticks** – These are used to mark the known height of an average person at various positions in the scene. If you have already attempted an automatic calibration, it is very likely that the image displayed in the Editor Pane shows several instances of the same person as in the picture. Person sticks are placed from the ground up to mark the height and direction of the person at one or more positions. A person stick must start on the ground and should be vertical in the real world. The length of a person stick in the real world must correspond to the height indicated next to the **PERSON** button in the Editor Pane. Person sticks are marked with a semi-transparent light blue symbol.

  How to best place a person stick:

  - Ideally, you should place the stick on a person having their feet close together.
  - If you place a stick on a person with their feet apart (but on the ground), you should place the lower point on the ground halfway between the heels of the person.
  - The stick should be aligned with the person's torso. However, if they are leaning in some direction - typically forwards while walking - you should try to compensate the leaning by placing the stick more upright. Use any clues in the scene to guide you (e.g. trees, fences, lamp posts, ...)
  - For the scale of the scene, at least one person stick with the corresponding person height is needed. If however no person is visible in the scene, you may "cheat" by placing a person stick on some other vertical object of known height (e.g. a 3m fence post) and setting the person height to the height of the object.

- **Parallel horizontal lines (or H-lines)** – These are used to mark known horizontal and parallel lines in the scene. These lines can be on the ground or on a wall or both, but they must all be parallel. If you place H-lines, you need to place two or more. You could place them on the sides or the markings on a straight road, on a set of straight railroad tracks, on some visible structure on a wall (e.g. rows of windows), on the tops and bottoms of a row of fence posts, etc. H-lines are marked in light blue.

- **Vertical lines (or V-lines)** – These are used to mark known vertical lines in the scene. A V-line should mark some vertical structure in the real world. This could be a fence post, the corner of a building, a sign etc. A V-line need not start on the ground. V-lines are marked in dark blue. Note that V-Lines are very sensitive as a small change of orientation may dramatically modify calibration. As a rule of thumb, V-Lines should lean right on the right side of image (and left on the left side).

Generally, when you draw lines in the scene - person sticks, H-lines and V-lines - the more the better. The calibration engine can calibrate with very few lines, but typically, the calibration quality will be better if you draw more than the minimum number of lines and sticks. When you place person sticks, ideally you would place some both near and far and both left and right.

According to *Recommended Camera Height and Orientation on page 8* , all camera devices must point slightly downwards. As a result all vertical structures in the real world will seem to fan out like a peacock-tail in the image. This means that all person sticks and V-lines should tilt towards the edge of the image. A stick on the right half of the image should tilt to the right and a stick on the left should tilt to the left. At least one of the placed person sticks or V-lines must be “correctly tilting” for the calibration to work.

A precision indicator (located at the top right of the calibration editor window) provides visual feedback on the level and quality of detail that has been added to the scene. For successful manual calibrations, mark-ups should cover the scene from front to back and from left to right. This will be reflected in a green precision indicator.

The quality of the calibration can be checked with the grid or avatar manipulators as described in the section *Verifying the Calibration on page 22*. Alternatively, you may click **REVIEW**. This will show you the result of running AXIS Perimeter Defender on the captured video using the current manual calibration

Direct Manual Calibration

Direct manual calibration functions mostly like described in *After a Failed Automatic Calibration on page 25*, except that you must first capture a short video and create a composite image as a support for the placement calibration elements.

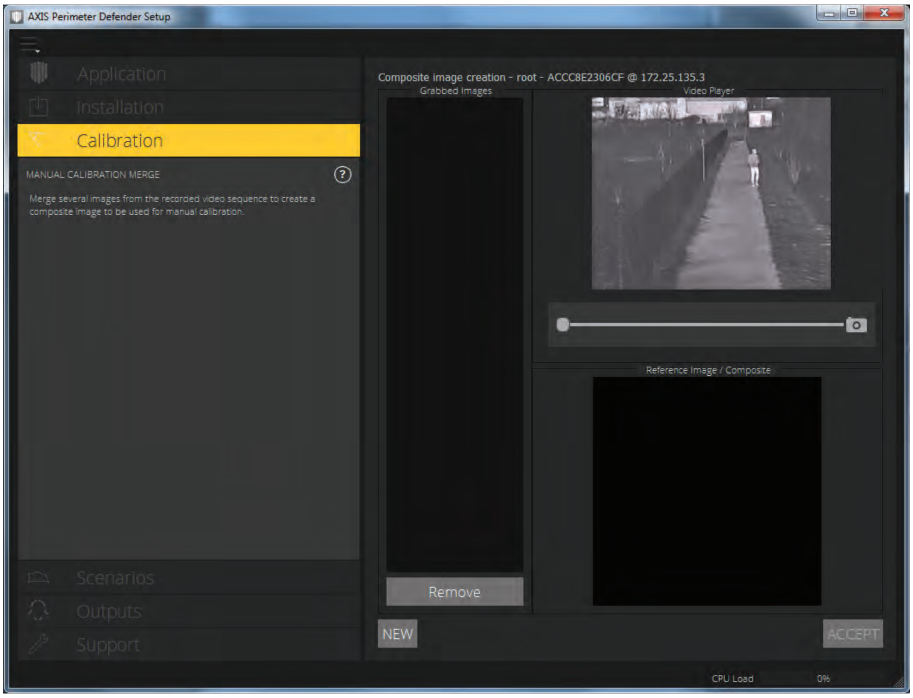
1. Select the device to calibrate in the device browser and ensure that the application and a valid license have been installed, see *Installation on page 18*.

2. Click the **Calibration** tab in the navigation pane or the calibration icon on the device thumbnail.

3. Click **MANUAL** in the Calibration tab, see picture on page *page 20* .

4. If you have already attempted to calibrate (manually or automatically), you may re-use the video footage recorded for that purpose by clicking **USE PREVIOUS CAPTURE**. Otherwise you need to capture a short video before moving on to the next step: Set the recording start time and duration and click **CAPTURE**. When you are satisfied with the recording, click **STOP**.

5. You should now see the Composite image creation pane as shown in the picture below.



Composite image creation - root - ACCC8E2306CF @ 172.25.135.3

MANUAL CALIBRATION MERGE

Merge several images from the recorded video sequence to create a composite image to be used for manual calibration.

6. Now build up a composite image using snapshots of the recorded video. Navigate in the video clip by moving the slider. At key positions you can add images to the composite by clicking the camera icon below the image. The current snapshot of the video will be added to the list in the middle and the composite image below the video slider will be updated. Images may be removed from the composite by selecting them in the list and click **Remove**. The objective is to build up a composite image that reflects the full cross-section of the scene, front, back, left and right.

7. Once satisfied with the composite image, click **ACCEPT** to proceed with manual calibration as described in the previous section, see *After a Failed Automatic Calibration*.

Multi-Camera Calibration

Note

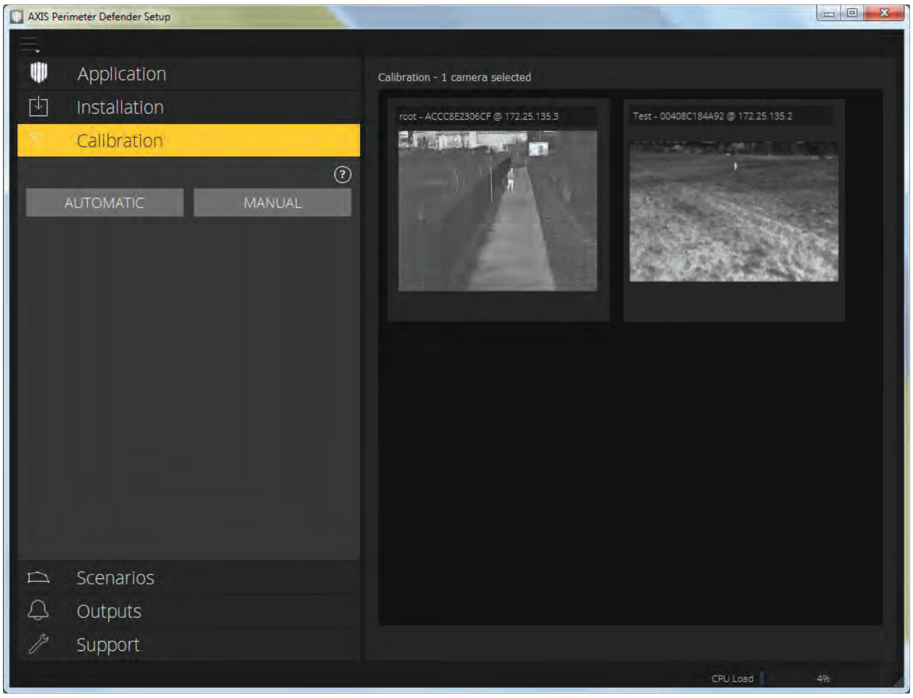
The maximum number of cameras you can install and configure simultaneously depends on the CPU power and the memory available on your computer. Too many cameras in the AXIS Perimeter Defender Setup interface can cause crashes. When the CPU overload warning appears, please install and configure a subset of the cameras using the Save Site feature.

Calibration can be performed on multiple devices simultaneously in order to make configuration of a multi-camera site easier. Multi-camera calibration can be done in manual or automatic mode just as single camera calibration. To perform multi-camera calibration:

1. Select the device to be calibrated in the device browser and ensure that the application and a valid license have been installed, see *Installation on page 18*.

2. Click the **Calibration** tab in the navigation pane on. Do not use the calibration icon under devices as it will start calibration for that particular device. You should see the calibration mode selection window with selected devices visible.

AXIS Perimeter Defender Setup Interface


AXIS Perimeter Defender Setup
Application
Installation
Calibration
?
AUTOMATIC
MANUAL
Scenarios
Outputs
Support
Calibration - 1 camera selected
root - ACCC8E2306CF @ 172.25.135.3
Test - 00408C184A92 @ 172.25.135.2
CPU Load
4%

3. Select the preferred calibration mode.

Note

Automatic calibration on multiple devices requires more CPU resources than for a single device and requires more RAM. On low-spec systems this might make computer unresponsive for some time or lead to an application crash. In the latter case, videos captured are still available to be used afterwards for single camera calibration.

4. Once mode is selected, press **CAPTURE** and perform the installer walk described previously in the field of view of each camera to be calibrated. Press **STOP** once done or wait for capture to finish.

5. For each device, automatic calibration process can be stopped at any moment by clicking on the **MANUAL** button. You will then be shown the composite image creation window for this particular device. Then perform the manual calibration as detailed previously.

6. If no interruption was performed (by clicking the **MANUAL** button), the first successful automatic calibration will be presented as shown in *Verifying the Calibration on page 22*. From then on you can verify the automatically computed calibration as detailed previously.

7. Whatever the calibration mode selected, you can check another device calibration by pressing **CANCEL** to be brought back to the calibrated devices selection window.

8. Accepting a calibration will also bring you back to the calibrated devices selection window. Devices for which calibration has been accepted are shown with a green tick.

9. Once all cameras have been calibrated press **EXIT** to be brought back to the device browser. If some devices still don't have an accepted calibration a warning message will pop-up.

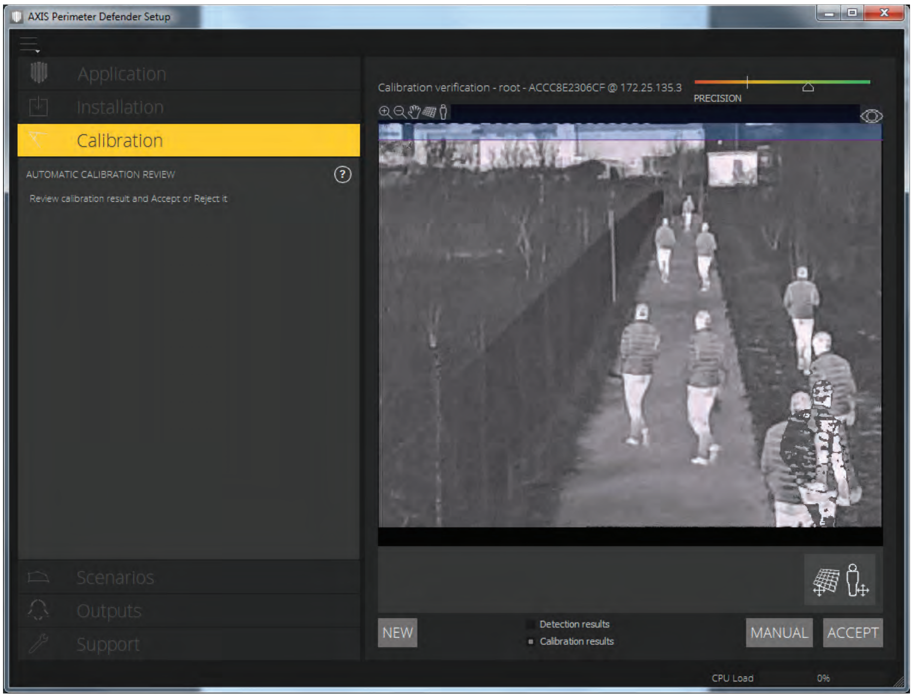
Note

Devices with a previous calibration can be recalibrated using multi-camera calibration but as long as the new calibration has not been accepted no changes are made on the device. Furthermore, if a previous calibration exists for a device, pressing **EXIT** will NOT pop-up a warning as it is considered that you changed your mind and don't want to change calibration.

Editing / Reviewing an Existing Calibration

Calibration from an already calibrated camera can always be reviewed or edited from the main window. Select camera and click **Calibration**, depending on the type of calibration that was performed the interface may vary.

Reviewing Automatic Calibrations



AUTOMATIC CALIBRATION REVIEW

Review calibration result and Accept or Reject it

Calibration verification - root - ACCC8E2306CF @ 172.25.135.3

When opening a previous automatic calibration the interface shown in the picture. From this interface you can:

- To perform a new calibration, click **NEW**.
- Review results.
- Click **MANUAL** to perform a manual calibration using the computed composite image computed by auto-calibration.

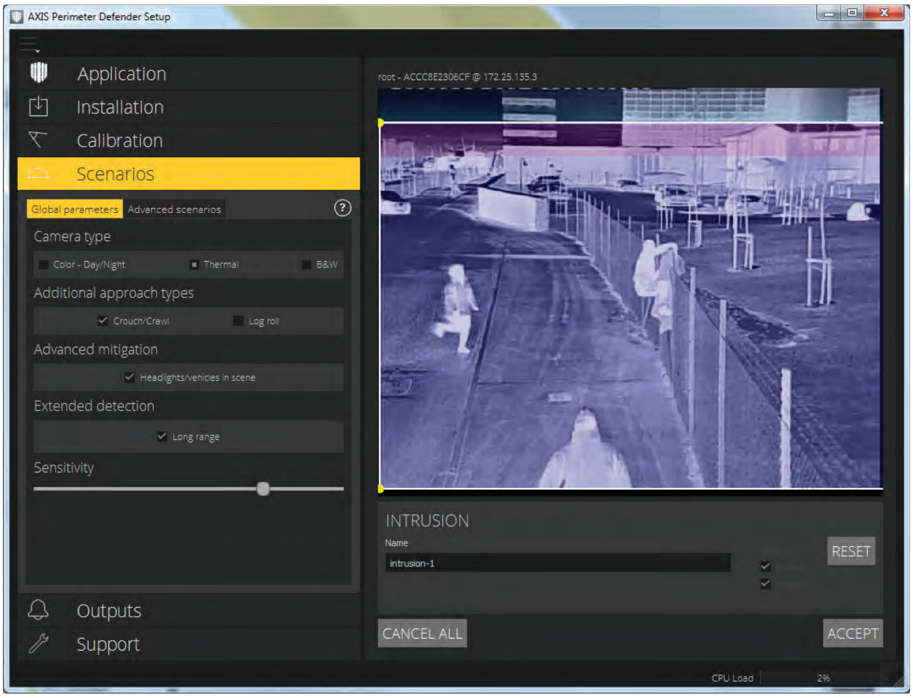
Reviewing / Modifying Manual Calibrations

Editing an existing manual calibration will display the same interface shown in *After a Failed Automatic Calibration on page 25*. User can then modify person sticks, V-lines and H-lines, change person height, review results

Important Calibration Notes

- AXIS Perimeter Defender supports different image aspect ratios according to the maximum field-of-view resolution provided by the camera. As a result, all previous calibrations should be redone to fit with the new field of view. Changing stream resolution in Axis web interface no longer requires recalibration as a result of this change.
- Users are advised to use the same image aspect ratio as AXIS Perimeter Defender (accessible by hovering mouse over camera name in main interface) in their VMS so that displayed information fits image content.
- If a camera moves after calibration the calibration has to be performed again otherwise analytic results can be incorrect.

Scenarios



Camera type

□ Color - Day/Night ■ Thermal □ B&W

Additional approach types

☑ Crouch/Crawl □ Log roll

Advanced mitigation

☑ Headlights/vehicles in scene

Extended detection

☑ Long range

Sensitivity

INTRUSION

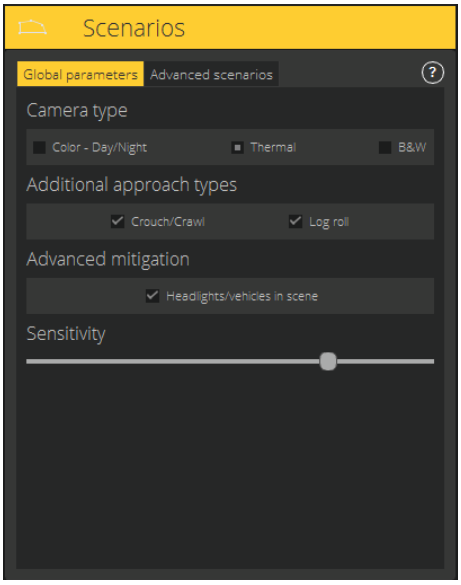
Name: intrusion-1

AXIS Perimeter Defender incorporates common sterile zone monitoring scenarios that can be configured to secure and monitor sensitive areas. The calibration step includes definition of a minimum detection zone to provide a default scenario. The Scenarios tab allows an installer to define more sophisticated scenarios.

AXIS Perimeter Defender is able to detect and distinguish people and vehicles (with a maximum length of 12m) in one of four security scenarios: intrusion, loitering, zone-crossing and conditional.

Global Parameters

These parameters apply to all scenarios.



Camera type

□ Color - Day/Night ▣ Thermal □ B&W

Additional approach types

☑ Crouch/Crawl ☑ Log roll

Advanced mitigation

☑ Headlights/vehicles in scene

Sensitivity

- Choose camera type. If the camera is a color one, choose **Color – Day/Night**. For thermal cameras, the camera type is automatically detected and set as thermal.

- Choose the additional approach types you want to cover with your intrusion scenario. Be aware that adding crouch/crawl and log roll approach types might generate false alarms (e.g. caused by animals).

- If the field of view can contain vehicles, headlights or headlights effects such as reflections, you can choose to activate the advanced mitigation related to headlights. Be aware that adding headlights mitigation can sometimes reduce performance in normal conditions. By default all scenarios are supposed to contain vehicles and thus headlights. Disabling vehicle detection in a scenario will prompt user about the presence of headlights in the scene, answering No will automatically deselect headlights.

Note

If another scenario has vehicle selected, headlights mitigation will be performed anyway.

- Sensitivity slider: Increase the sensitivity of the system by sliding the cursor to the right. Decrease it by sliding to the left. More sensitivity means lower risk of missed detections but greater risk of false alarms, whilst less sensitivity means fewer false alarms but greater risk of missed detections.

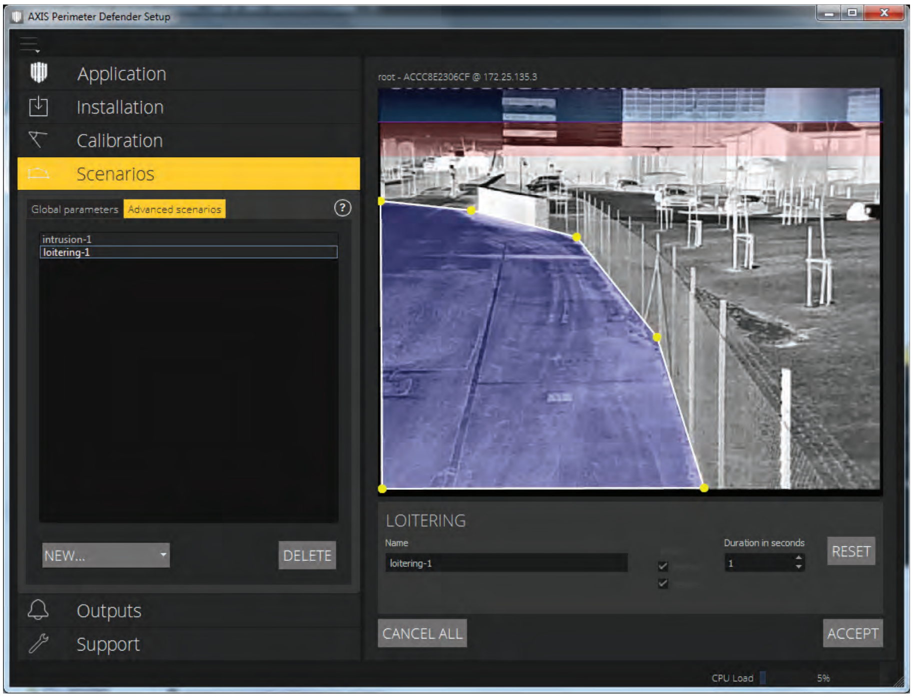
Standard Security Scenario: Intrusion

This is the default security scenario and raises an alarm when a subject enters a zone. If intrusion detection is wanted on the maximum detection zone, nothing more needs to be done. The scenario is uploaded to the camera the moment the installer accepts the calibration. The default parameters can, however, be modified under Global parameters on the Scenarios tab and the default detection zone can be modified on the right. Existing points may be moved by dragging them with the mouse and additional points may be created by clicking on any of the existing segments. Click **ACCEPT** to upload the modifications to the camera and switch back to the main view.

If a "!" symbol appears near the scenario name the scenario is not completely defined (very often its zone has not yet been defined). This is true for any scenario type, not only for intrusion.

AXIS Perimeter Defender Setup Interface

Advanced Security Scenario: Loitering



Name: loitering-1

Duration in seconds: 1

This scenario is designed to output an alarm when a subject is loitering in a zone for longer than the time that has been predefined by an installer. To create this scenario from within the scenario editor, switch to **Advanced scenarios** on the Scenarios tab. Then select **LOITERING** from the **NEW** dropdown menu, add a zone and adjust the settings in the pane on the right:

- Detect: list the targets which can be detected by AXIS Perimeter Defender. Choose Person and/or Vehicle.
- Duration in seconds [1s - 120s]: set the presence duration of target in the loitering zone before triggering an alarm.

The zone is added by simply clicking in the image field. Click the right mouse button to finish the zone.

Click **ACCEPT** to upload the modifications to the camera and switch back to the main view.

Advanced Security Scenario: Zone-Crossing

This scenario is designed to output an alarm when a subject passes through two zones in a given sequence. To create this scenario from within the scenario editor:

1. Switch to **Advanced scenarios** in the Scenarios tab.
2. Select **ZONE-CROSSING** from the **NEW** dropdown menu, see picture in chapter *Advanced Security Scenario: Loitering on page 33*
3. Add two zones (separated by at least a meter) and adjust the settings in the pane on the right. Zones are added by simply clicking in the image field. Click the right mouse button to finish a zone.
4. Click **SELECT ORIGIN** and then click one of the zones to specify the forbidden crossing direction
5. Click **ACCEPT** to upload the modifications to the camera and switch back to the main view.

Important

The Zone-Crossing scenario has the following limitation: if the person triggering the scenario stops moving for a few seconds in the first zone before passing to the second one, the scenario will not trigger.

Advanced Security Scenario: Conditional

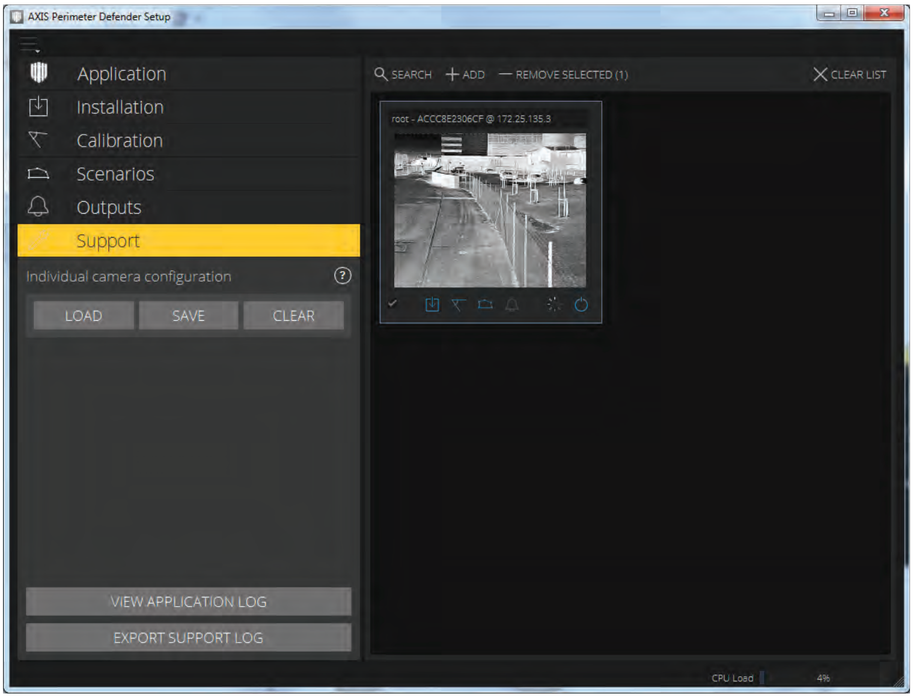
This scenario is designed to output an alarm when a subject enters a certain zone without passing through others. To create this scenario from within the scenario editor:

1. Switch to **Advanced scenarios** in the Scenarios tab.
2. Select **CONDITIONAL** from the **NEW** dropdown menu, see picture in chapter *Advanced Security Scenario: Loitering*,
3. Add two or more zones (separated by at least one meter) and adjust the settings in the pane on the right. Zones are added by simply clicking in the image field. Click the right mouse button to finish a zone.
4. Click **SELECT INTRUSION ZONE** and then click one of the zones to specify the allowed crossing direction(s).
5. Click **ACCEPT** to upload the modifications to the camera and switch back to the main view.

Outputs

See *VMS Integration on page 40.*

Support



The Support tab interface is shown in the figure for a single device selection. This tab offers 4 functionalities, 3 of them are related to device configuration management and can be activated for multiple devices. The last action focuses on exporting support log from a single device.

1. **LOAD** – Loads backed-up configuration for selected devices. This is especially useful to restore rapidly after a device failure or accidental uninstallation. Configuration contains:
   - License
   - Parameters

  - Calibration and scenarios
  - Calibration video

2. **SAVE** – Creates a backup of the selected devices configurations (as above).
3. **CLEAR** – Erases calibration and scenarios from the selected device. This is useful if the cameras have moved as calibration and detection areas are no longer valid.
4. **VIEW APPLICATION LOG** – Opens a window displaying the AXIS Perimeter Defender internal log.
5. **EXPORT SUPPORT LOG** – Generates a support file that contains detailed information necessary for problems resolution from Axis support. This should be passed along any support request.

Upgrade Camera Firmware

Before upgrading the camera firmware, save all AXIS Perimeter Defender settings. Upgrading the firmware removes the application and its settings from the camera. If settings are saved, they can be restored using AXIS Perimeter Defender Setup.

To upgrade camera firmware, follow these steps:

1. Use AXIS Perimeter Defender Setup to save the site configuration.
2. Upgrade the camera firmware. For instructions, see the camera's User Manual.
3. Start AXIS Perimeter Defender Setup.
4. Use the load site option to automatically load the saved site configuration for each upgraded camera.

Troubleshooting

In order to have all the functionalities working as expected, it is mandatory to configure correctly the following Axis parameters:

- Network / TCP-IP / Basic / Default router
- Network / TCP-IP / Advanced / Domain name
- Network / TCP-IP / Primary DNS Server
- Network / TCP-IP / Secondary DNS Server
- Network / TCP-IP / NTP server address
- Network / TCP-IP / SMTP (email)
- System Options/ Date & Time / Time Zone
- System Options/ Date & Time / Synchronize with NTP server

Installation of the Setup Interface

Problem	Possible reason	Solution
There is a windows message saying it is impossible to install the software.	The operating system on the laptop or PC is not compatible.	Verify the Windows operating system matches that specified in the requirements.
There is a windows message saying the installation was incorrect.	Windows Compatibility Assistant has detected a possible problem with the installation.	Confirm that the installation is correct anyway and proceed.

AXIS Perimeter Defender Setup Interface

Problem	Possible reason	Solution
Installation fails during installation of XVID.	Installation of XVID fails because of old partial installation of XVID present on computer.	Delete the XVID folder in C:\Program Files (x86) and try installing again.
The installer package suddenly crashes after the EULA display. There is a Windows error message telling that the application exited in an unusual way. It is impossible to close the installer.	A known problem in the installers leads to an application crash under some circumstances.	Open task manager and kill all "msiexec.exe" processes. Then kill the installer process and restart the installer.

Configuration Troubleshooting

Problem	Possible reason	Solution
Problem opening AXIS Perimeter Defender.	You do not have sufficient windows user rights.	Make sure you have administrator rights.
The "Search" functionality does not find my cameras.	Firewall	Firewalls and antivirus software can sometimes block camera discovery. If required, configure the firewall to allow network traffic to and from the Setup Interface. If this does not solve the problem, configure the firewall to allow the following ports: UDP port 5353 and TCP port 80.
	IP address problems	Any device in a network must have a unique IP address to be able to communicate with other devices. When using AXIS Perimeter Defender, it is recommended to use fixed IP addresses for the cameras. Make sure that every IP device on the network has its own IP address and does not reuse an already taken IP address.
	The camera is not available from the user computer.	Use a web browser to browser to the IP address of the camera to confirm whether it is available. If you cannot see it then the camera has not been correctly installed on the network, or the computer does not have access to the camera.
It is not possible to add a camera.	Camera connection parameters e.g. IP address, password or HTTP port are incorrect.	Verify the parameters entered are correct and repeat.
	The camera cannot be seen from the user's computer.	Use a web browser to browse to the IP address of the camera, to confirm whether it is available. If you cannot see it then the camera has not been correctly installed on the network, or the computer does not have access to the network which the camera is on.
Loss of video streams in the AXIS Perimeter Defender Setup.	Video Source is no longer available.	The video source has been interrupted and has not refreshed on the display.
	Use a web browser to check if the camera is available.	Click on the tile where the stream should be and resize the interface and the stream should come back.

AXIS Perimeter Defender Setup Interface

Problem	Possible reason	Solution
The automatic calibration does not work or yields bad results.	Pre-requisites are not met.	Make sure the AXIS Perimeter Defender requirements are met, see *Place the Camera*
	The camera has a roll.	It is not possible to calibrate camera having a roll.
	Slow connection to camera not configured as remote.	Connect camera as remote device to lower bandwidth requirements.
	There are other moving objects in the scene used for the automatic calibration such as cars, trees or other persons.	Repeat the auto-calibration, or perform the calibration using the "Manual" method.
	The field of view is cluttered making the person walking in front of the camera partially hidden a lot of the time.	Perform the calibration using the "Manual" method.
	The field of view is small like indoor corridors, rooms or outdoor entrances.	Perform the calibration using the "Manual" method.
	The capture video was not properly recorded because of insufficient disk space.	Check that there is adequate disk space and that the application has permission to save the video recording on the computer where the AXIS Perimeter Defender interface is running.

Operation Troubleshooting

Problem	Possible reason	Solution
The application will not run even though the configuration is good.	The firmware of the camera is not up to date.	Make sure you have the latest firmware for the camera.
The overlay is not displayed in AXIS Perimeter Defender Setup even though the analysis is running.	The application is blocked after a start/stop operation or an upgrade of the AXIS Perimeter Defender package``.	Restart the camera.
	A firewall is blocking the connection to the camera metadata listening port.	Configure the firewall in order to allow the configuration interface to connect to the metadata listening port on the camera.
	An anti-virus program is blocking the reception of the overlay.	Configure the anti-virus in order to allow the overlay to be received.
No alarms are triggered in the AXIS Perimeter Defender setup on the configuration computer even though the analysis is running and the overlay is visible.	Although the target is in the scene it not matching a conditional scenario e.g. not moving from one zone to another in the zone crossing scenario.	Make sure the scenario is correctly specified, including conditions.
	Poor detection.	Make sure the AXIS Perimeter Defender requirements are met (see *Place the Camera*), that the calibration is precise enough, that sensitivity is high enough.

Performance

Problem	Possible reason	Solution
OSD and analysis keeps switching on and off.	CPU charge on the camera is too high.	Possible solutions: -Make sure the stream of the camera is not visualized in unnecessary places because every visualization of the camera stream increase CPU load. -If recording on in-built motion detection is activated try to decrease the quality of the recording to free up CPU. -Deactivate recording on in-built motion detection and make sure in-built motion detection is deactivated.
A target enters the sterile zone and causes multiple alerts to be raised.	The duration of the Post-alarm time is too short.	Adjust the Post-alarm time in the "Outputs" section. Please refer to the Setup Guide.
A potential target enters the sterile zone but does not raise an alert – missed detection.	Contrast of the object against the background in the scene is too low.	Make sure the AXIS Perimeter Defender requirements are met, see *Place the Camera*
	There is inadequate lighting in the scene or the low light performance of the camera is insufficient.	Make sure the AXIS Perimeter Defender requirements are met, see *Place the Camera*
	AXIS Perimeter Defender has the sensitivity set too low.	Increase the sensitivity in the global scenario parameters.
	Camera has moved rendering the calibration incorrect.	Redo the calibration.
	The calibration is not precise enough.	Verify the calibration of the camera. Please refer to the Setup Guide.
	Although the target is in the scene it is not matching a conditional scenario e.g. not moving from one zone to another in the zone crossing scenario.	Make sure the scenario is correctly specified, including conditions.
The target is detected but is incorrectly classified (person as vehicle or vehicle as person).	The camera height, positioning or orientation is incorrect.	Make sure the AXIS Perimeter Defender requirements are met , see *Place the Camera.*
	The camera is too far away from the zone.	Make sure the AXIS Perimeter Defender requirements are met, see *Place the Camera*
	Calibration is not precise enough.	Verify the calibration of the camera. Please refer to the Setup Guide.
AXIS Perimeter Defender generates an alarm when there is not an intrusion into the sterile zone.	Sensitivity of analysis is too high.	Decrease the sensitivity. Please refer to the Setup Guide.
	Calibration is not precise enough.	Verify the calibration of the camera. Please refer to the Setup Guide.
	Camera has moved rendering the calibration incorrect.	Redo the calibration.
	Wrong camera height, positioning or orientation.	Make sure the AXIS Perimeter Defender requirements are met, see *Place the Camera*
	Camera is moving e.g. swaying, vibrating.	Install the camera in a more stable environment.

AXIS Perimeter Defender Setup Interface

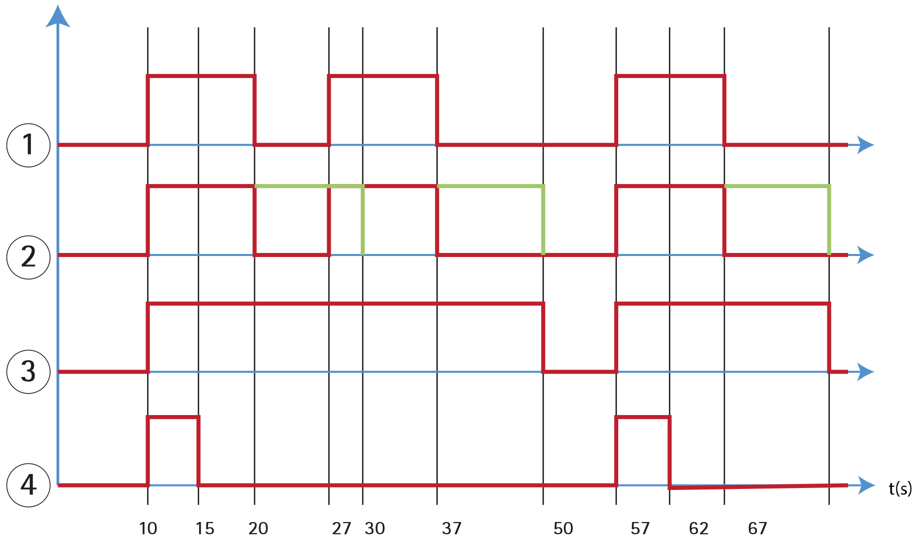
Problem	Possible reason	Solution
	Vegetation or other moving objects (e.g. flags) close to the camera.	Remove the offending items from the camera field of view (note objects that are constantly in the scene but are not close to the camera will be ignored by AXIS Perimeter Defender).
	Insects are crawling on or near the camera lens.	Deter insects where possible from encroaching on or near the camera lens.

VMS Integration

An automated intrusion detection system is designed to trigger alarms and provide information that helps inform the security intervention. This may include providing a prompt to a mobile device or displaying the alarm event within a VMS perhaps with the subject that created the alarm event highlighted on screen.

Configuring Alarm Output

AXIS Perimeter Defender implement the notion of "post-alarm time". This is defined as the time interval, after the real stop of the alarm, during which, if another alarm is triggered, both alarms are merged together in a unique one, as following:



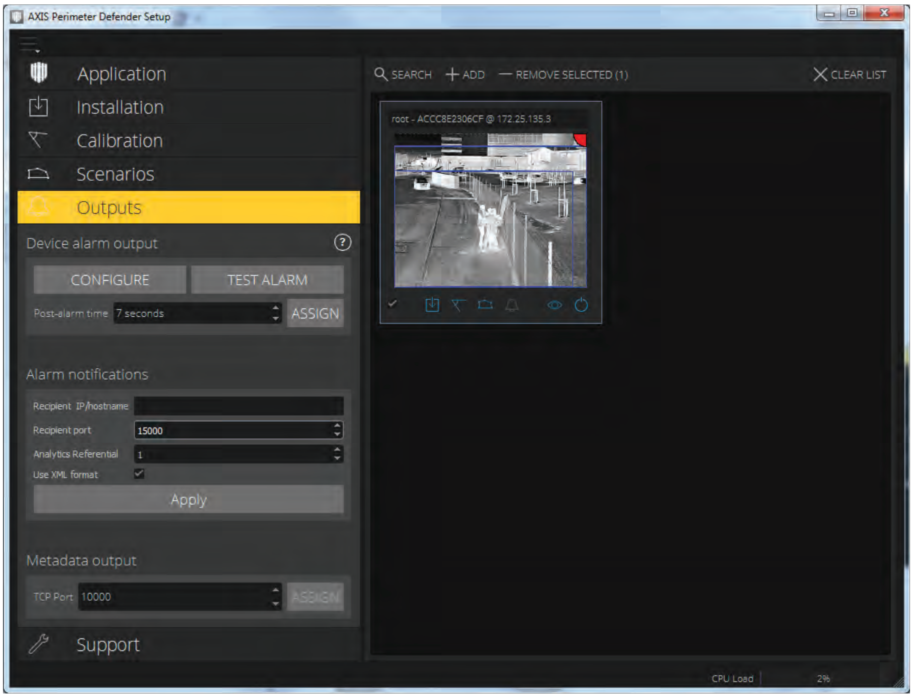
1 *Three alarms triggered by AXIS Perimeter Defender, at time 10, 27 and 57. Each alarm has a real duration of 10 seconds, i.e. an intruder has taken 10 seconds to cross the intrusion zone.*
2 *A post-alarm time of 10 seconds is added*
3 *Alarms using XML notifications and XML metadata*
4 *Alarms using email notifications, ftp image upload, electrical contacts and basic TCP/IP notifications*

Notice how a post-alarm time of 10 seconds increases (in green) the duration of each alarm, thus leading to the fusion (merge) of two alarms that are separated by 10 seconds or less.

You can see the resulting alarm number and duration as raised by AXIS Perimeter Defender through XML notifications and XML metadata. The post-alarm time can be used for obtaining fewer longer alarms instead of several, shorter and consecutive ones.

It is important to note that for email notifications, ftp image upload, electrical contacts and basic TCP/IP notifications the behaviour resulting from a post-alarm time different from zero is slightly different. These notifications consider the alarm start event only and neglect the alarm stop. Thus, there is no notion of "alarm duration" when using these notifications, and, as consequence, the post-alarm time does not change the duration of the notification itself (that is always fixed to the value chosen by the user when configuring the notification). However, given that AXIS Perimeter Defender might merge consecutive alarms because of the post-alarm time, these notifications will "miss" the merged alarm and no notification will be generated for those ones. This situation is depicted by graph 4: AXIS Perimeter Defender will merge two of the three alarms together, thus suppressing one of them. Therefore, email notifications, ftp image upload, electrical contacts and basic TCP/IP notifications will notify only two of them. Graph 4 shows a fixed duration of 5 seconds for these notifications.

To configure the post-alarm time, follow these steps:



Device alarm output

Post-alarm time: 7 seconds

Alarm notifications

Recipient IP/hostname:

Recipient port: 15000

Analytics Referential: 1

Use XML format: ☑

Metadata output

TCP Port: 10000

1. Open the AXIS Perimeter Defender Setup interface.
2. Click on the **Outputs** tab.
3. Modify the **Post-alarm time** setting (the default value is 7 seconds).
4. Click **ASSIGN**.

Standard Event Integration

AXIS Perimeter Defender leverages and extends the native ACAP interfaces and capabilities for sending alarms and supplementary information to external devices or VMS. Events output by AXIS Perimeter Defender can be translated into messages to the VMS, by connecting action rules to them.

The following alarm channels from the camera to the VMS are available:

- Basic free text notifications for alarms (TCP/IP)
- Electrical outputs (dry or wet contacts)
- E-mail notifications
- Ftp upload of alarm images

These integrations can be configured on the camera using the following procedure:

1. Open the **Outputs** menu.
2. Click **Configure**.
3. The Axis web interface opens the cameras "Action Rules" page.

For information on how to continue the configuration in the camera, see the camera manual.

XML/text Alarm Notification

This interface allows a TCP/IP recipient to receive a more complete and descriptive XML or text message for each alarm. With respect to the free-text interface, the XML/text interface offers the following advantages:

- A notification is sent at the beginning of the alarm, at the end of the alarm and every 10 seconds during the alarm duration.
- Timestamp: the start-of-alarm and end-of-alarm notifications contain a timestamp (synchronized with the camera clock) giving the exact date and time of these two events.
- Alarm type: AXIS Perimeter Defender supports several alarm types, see *Scenarios on page 31*. The XML/text notifications contain the information of which type of alarm has been triggered. Pay attention: the "zone crossing" scenario has type "passage" and the loitering scenario has type "presence"
- Zone(s) involved in the alarm generation; where each AXIS Perimeter Defender scenario is associated to one or more zones, the XML/text notifications include which zone is associated to the alarm (i.e., for an intrusion alarm, the intrusion zone in which a person has been detected)

With respect to the free-text interface, the XML/text interface has the following limitations:

- The message text is fixed, and there are no free-text fields.
- Only one recipient is supported per camera at a time.

The recipient of the XML/text notifications receives four types of messages:

- AXIS Perimeter Defender sends a CONNECTION_TEST message when the XML notification is configured in order to verify that the communication with the recipient works as expected.
- When AXIS Perimeter Defender triggers an alarm, it sends an ALARM_START message.
- During the alarm duration, AXIS Perimeter Defender sends several "alarm in progress" messages, one every 10 seconds. All these messages have the same GUID tag, identical to that of the ALARM_START message and ALARM_STOP messages related to the same alarm
- At the end of the alarm, AXIS Perimeter Defender sends an ALARM_STOP alarm.

The format of these messages, both in XML and text format, is explained in the following section.

XML and Text Formats

The XML format is the default format for the TCP/IP notifications. Nevertheless, if the notification size is important, a text format, generating shorter messages, can be used. In order to select the text format, the "Do not use XML for alarms" parameter must be ticked in the AXIS Perimeter Defender configuration page (see section "Configuration" here below).

A CONNECTION_TEST message in XML format looks like this example:

```
<?xml version="1.0"?>
<KEENEO_MESSAGE xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
         xmlns:xsd="http://www.w3.org/2001/XMLSchema"
         VERSION="5.0.0"
         ID="1"
         TYPE="CONNECTION_TEST"
         SENDER_IP="192.168.1.40"
         SENDER_PORT="0">
  <REFERENTIAL>45</REFERENTIAL>
</KEENEO_MESSAGE>
```

- VERSION is the internal version of the XML syntax and protocol.
- ID is a numeric identity for the message. ID's are not guaranteed to be unique nor progressive.
- TYPE is the type of the message, here "CONNECTION_TEST". The message type determines the sub-tags of the message (none for messages of type "CONNECTION_TEST").

- SENDER_IP is the ip address of the Axis camera sending the XML notification.
- SENDER_PORT is always zero; the camera cannot receive incoming messages.
- REFERENTIAL is the numeric ID associated to the camera (see the Configuration section at page 13)

If the text format is chosen, the notification messages contain 7 fields each, separated by the "pipe" character "|". If a field can't be specified (for example, it does not make sense for that message type), it is replaced by "-".

The seven fields are, from the first to the last (in parenthesis, the corresponding XML field when the format is XML):

1. The message numeric ID ("ID" attribute of the XML "KEENEO_MESSAGE" header).
2. The IPv4 address of the camera ("SENDER_IP" attribute of the XML "KEENEO_MESSAGE" header).
3. The referential number associated to the AXIS Perimeter Defender instance ("REFERENTIAL" tag).
4. The message type ("TYPE" attribute of the XML "KEENEO_MESSAGE" header).
5. The alarm type ("TYPE" tag).
6. The name of the scenario that has triggered the alarm ("SCENARIO_NAME" tag).
7. The timestamp ("TIMESTAMP" tag). The timestamp format is the same as for the XML format.

The previous CONNECTION_TEST message in TEXT format is:

```
1|192.168.1.40|45|CONNECTION_TEST|-|-|-
```

An ALARM_START message in XML format looks like this example:

```
<?xml version="1.0"?>
<KEENEO_MESSAGE xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
         xmlns:xsd="http://www.w3.org/2001/XMLSchema"
         VERSION="5.0.0"
         ID="9999"
         TYPE="ALARM_START"
         SENDER_IP="192.168.1.40"
         SENDER_PORT="0">
  <REFERENTIAL>0</REFERENTIAL>
  <TYPE>INTRUSION</TYPE>
  <SCENARIO_NAME>Intrusion-0</SCENARIO_NAME>
  <EXTRA_DATA>zone=testzone</EXTRA_DATA>
  <TIMESTAMP>2014-03-01T21:24:12.114</TIMESTAMP>
  <GUID>77acddf9-e0d4-402e-a497-231aeee22788</GUID>
</KEENEO_MESSAGE>
```

- The message header is the same as the "CONNECTION_TEST" message.
- The message type is "ALARM_START", and has a set of sub-tags.
  - REFERENTIAL is the numeric ID associated to the camera (see the Configuration section at page 13).
  - TYPE is the type of the alarm triggered by AXIS Perimeter Defender, "INTRUSION" in this example. Other possible types are "PRESENCE", "PASSAGE" and "CONDITIONAL".
  - SCENARIO_NAME is the name of the scenario that triggered the alarm, as defined in the configuration interface, see *Standard Security Scenario: Intrusion on page 32*
  - EXTRA_DATA carries the zone name (or list of zone names) involved with the alarm, like the intrusion zone.
  - TIMESTAMP is the date and time of the alarm start, in the format YYYY-MM-DDTHH:mm:ss.zzz, where:

    – YYYY is the year on 4 digits, like 2014.

– MM is the month number on 2 digits, like 01 for January.

– DD is the day number on 2 digits, like 03 for the 3rd.

– 'T' is a fixed letter

– HH is the hour in 24-hour format, from 00 to 23

– mm are the minutes on 2 digits, from 00 to 59

– ss are the seconds on 2 digits, from 00 to 59

– zzz are the milliseconds on 3 digits, from 000 to 999.

AXIS Perimeter Defender uses the camera internal date and time for generating the alarm timestamp, thus it is important to synchronize the camera with some kind of external clock.

- GUID is a unique identifier that is constant for all messages related to the same alarm (so ALARM_START, ALARM_IN_PROGRESS and ALARM_STOP)

This is the equivalent, in text format, of the ALARM_START message:

```
9999|192.168.1.40|0|ALARM_START|INTRUSION|Intrusion-0|2014-03-01T21:24:12.114
```

An ALARM_IN_PROGRESS message in XML format looks like this example:

```
<?xml version="1.0"?>
<KEENEO_MESSAGE xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
         xmlns:xsd="http://www.w3.org/2001/XMLSchema"
         VERSION="5.0.0"
         ID="9999"
         TYPE="ALARM_IN_PROGRESS"
         SENDER_IP="192.168.1.40"
         SENDER_PORT="0">
  <REFERENTIAL>0</REFERENTIAL>
  <TYPE>INTRUSION</TYPE>
  <SCENARIO_NAME>Intrusion-0</SCENARIO_NAME>
  <GUID>77acddf9-e0d4-402e-a497-231aeee22788</GUID>
</KEENEO_MESSAGE>
```

- The message header is the same as the "CONNECTION_TEST" and "ALARM_START" message.
- The message type is "ALARM_IN_PROGRESS", and has a set of sub-tags.
  - REFERENTIAL is the numeric ID associated to the camera (see the Configuration section at page 13).
  - TYPE is the type of the alarm triggered by AXIS Perimeter Defender the same of the corresponding ALARM_START.
  - SCENARIO_NAME is the name of the scenario that triggered the alarm, the same of the corresponding ALARM_START.
  - The GUID is the same of the corresponding ALARM_START.

The corresponding ALARM_IN_PROGRESS message in TEXT format:

```
9999|192.168.1.40|0|ALARM_IN_PROGRESS|INTRUSION|Intrusion-0|-
```

An ALARM_STOP message in XML format looks like this example:

```
<?xml version="1.0"?>
<KEENEO_MESSAGE xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
         xmlns:xsd="http://www.w3.org/2001/XMLSchema"
         VERSION="5.0.0"
         ID="9999"
         TYPE="ALARM_STOP"
```

```
        SENDER_IP="192.168.1.40"
        SENDER_PORT="0">
  <REFERENTIAL>0</REFERENTIAL>
  <TYPE>INTRUSION</TYPE>
  <SCENARIO_NAME>Intrusion-0</SCENARIO_NAME>
  <EXTRA_DATA>zone=testzone</EXTRA_DATA>
  <TIMESTAMP>2014-03-01T21:24:26.304</TIMESTAMP>
  <GUID>77acddf9-e0d4-402e-a497-231aeee22788</GUID>
</KEENEO_MESSAGE>
```

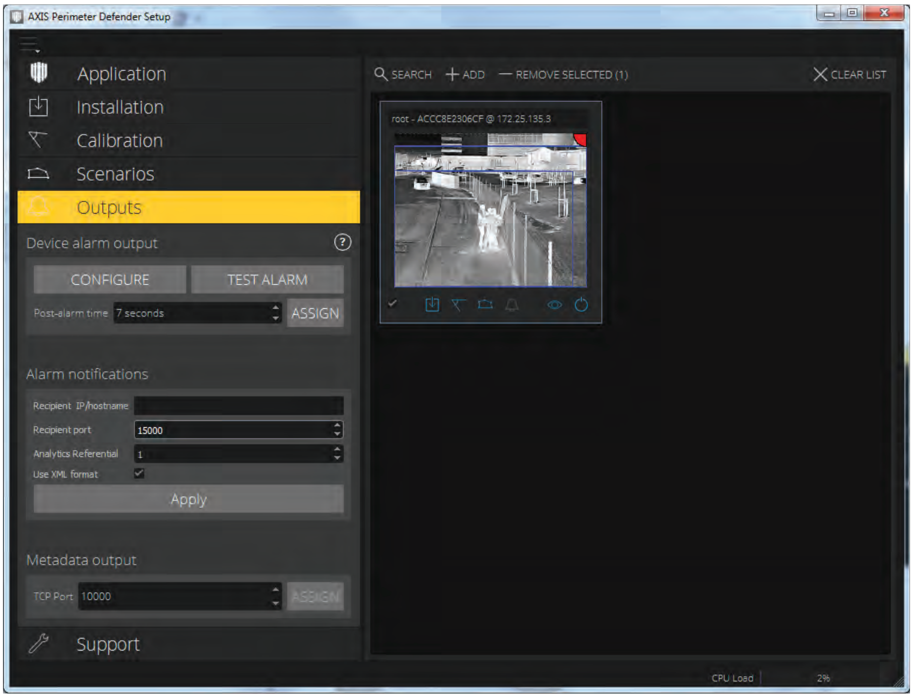
- The message header is the same as the previous messages.
- The message type is "ALARM_STOP", and has the same set of subtypes of the ALARM_START message.

The corresponding ALARM_IN_PROGRESS message in TEXT format:

```
9999|192.168.1.40|0|ALARM_STOP|INTRUSION|Intrusion-0|2014-03-01T21:24:26.304
```

The TCP/IP connection is always closed after each message. Therefore, the recipient has to keep the listening socket always open for being able to receive further notifications.

Configuration



Post-alarm time 7 seconds

Recipient IP/hostname

Recipient port 15000

Analytics Referential 1

Use XML format ☑

TCP Port 10000

Configure the XML/TEXT alarm interface by following the steps below:

1. Open the **Outputs** menu.
2. Click **Configure**.
3. The Axis web interface opens the cameras "Action Rules" page. For configurations in the camera, see the camera manual.

Communication Errors

If the remote recipient of XML notifications is not reachable anymore (for example, because of a network disconnection), AXIS Perimeter Defender starts buffering the non-delivered alarms internally, and periodically (every 10 seconds or more frequently) tries to deliver them again. After a consecutive number of failures in delivering new messages (failures while trying to delivery again a message from the buffer does not account for that) AXIS Perimeter Defender declares the recipient as "permanently off-line" and ceases sending XML notifications to it. The number of consecutive failures is fixed to 20, roughly corresponding to 4 or 5 intrusion alarms of an average duration of 40 seconds each. AXIS Perimeter Defender will start sending notifications to this same recipient again if one of the following events occurs:

- AXIS Perimeter Defender is restarted.
- The same value of the parameter "Alarm streaming url" is saved again.

VMS Bridges

For the following VMS, Axis provides pre developed integration modules, referred to as "bridges":

- Milestone XProtect® 2014 and 2016 Corporate and Expert. Enterprise editions only work with Axis notifications (only alarms , no metadata)
- Genetec™ Service Center 5.3

The bridges provide two integrations:

- Creating custom alarm events in the VMS matching the events output by AXIS Perimeter Defender.
- Displaying alarm overlays – "bounding boxes" – on top of live and recorded video material from.

The VMS bridges are downloaded and installed as separate applications. For more information on how to install and configure these bridges, see the user manual for the specific bridge.

User Manual
AXIS Perimeter Defender
© Axis Communications AB, 2016

Ver. M2.2
Date: April 2016
Part No. 1587516