



Next-generation video analytics

Edge-based Ai engine Rules and Analytics User Manual



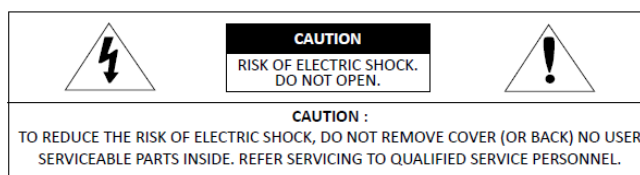
Read this first

Read through this Installation Guide carefully before installing the product. Keep the Installation Guide for future reference. See the complete user manual for more information on the product's proper installation, use and care.

These instructions ensure users can use the product correctly to avoid danger or property loss. The precaution measure is divided into "Warnings" and "Cautions":

Warnings: Serious injury or death may occur if any warnings are neglected.

Cautions: Injury or equipment damage may occur if any cautions are neglected.



This symbol indicates that a dangerous voltage, a risk of electric shock, is present within this unit.



This exclamation point symbol is intended to alert the user to important operating and maintenance (servicing) instructions in the literature included with the appliance.

WARNING

1. You must strictly comply with your nation's and region's electrical safety regulations when using the product. The device shall be firmly fixed when the product is mounted on a wall or ceiling.
2. Be sure to use only the standard adapter specified in the specification sheet. Using any other adapter could cause fire, electrical shock, or damage to the product.
3. Make sure the power supply voltage is correct before using the camera.
4. Incorrectly connecting the power supply or replacing the battery may cause an explosion, fire, electric shock, or damage to the product.
5. Do not connect multiple cameras to a single adapter. Exceeding the capacity may cause excessive heat generation or fire.
6. Securely plug the power cord into the power source. An insecure connection may cause a fire.
7. When installing the camera, fasten it securely and firmly. A falling camera may cause personal injury.
8. Do not install in a location subject to elevated temperature, low temperature, or high humidity. Doing so may cause fire or electric shock.
9. Do not place conductive objects (e.g., screwdrivers, coins, metal items, etc.) or containers filled with water on top of the camera. Doing so may cause personal injury due to fire, electric shock, or falling objects.
10. Do not install the unit in humid, dusty, or sooty locations. Doing so may cause fire or electric shock.
11. Do not install near any heat sources, such as radiators, heat registers, or other products (including amplifiers) that produce heat.
12. Keep out of direct sunlight and heat radiation sources. It may cause a fire.
13. Stop using the product immediately if any unusual smells or smoke come from the unit. Immediately disconnect the power source and contact the service center. Continued use in such a condition may cause fire or electric shock.
14. If this product does not operate normally, contact the nearest service center. Never disassemble or change this product in any way.
15. When cleaning the product, do not spray water directly onto parts of the product. Doing so may cause fire or electric shock.

CAUTION

1. Use proper safety gear when installing and wiring the product.
2. Do not drop objects on the product or apply strong shock to it. Keep away from a location subject to excessive vibration or magnetic interference.
3. Do not use this product near water.
4. The product shall not be exposed to dripping or splashing, and no objects filled with liquids, such as vases, shall be placed on the product.
5. Avoid aiming the camera directly toward highly bright objects, such as the sun, as this may damage the image sensor.
6. The main plug is a disconnect device and shall always remain readily operable.
7. Remove the power adapter from the outlet when there is lightning. Neglecting to do so may cause fire or damage to the product.
8. Do not block any ventilation openings. Install following the manufacturer's instructions.



9. A polarized or grounding-type plug is recommended for this product. A polarized plug has two blades, one wider than the other. A grounding-type plug has two blades and a third grounding prong. If the provided plug does not fit your outlet, consult an electrician for replacement.
10. Protect the power cord from being walked on or pinched, particularly at plugs, convenience receptacles, and where they exit from the product.
11. If any laser equipment is used near the product, ensure the sensor's surface is not exposed to the laser beam, which may damage the sensor module.
12. If you want to move the installed product, turn off the power and then move or reinstall it.
13. The installer and/or end-user must properly configure all passwords and other security settings.
14. If cleaning is necessary, please use a clean cloth to wipe it gently. If the device will not be used for a long time, please cover the lens cap to protect the device from dirt.
15. Do not touch the camera's lens or sensor module with your fingers. If cleaning is necessary, please use a clean cloth to wipe it gently. If the device will not be used for a long time, please cover the lens cap to protect the device from dirt.
16. Use only attachments/accessories specified by the manufacturer.
17. Always use hardware (e.g., screws, anchors, bolts, locking nuts, etc.) compatible with the mounting surface and of sufficient length and construction to ensure a secure mount.
18. Use only with a cart, stand, tripod, bracket, or table specified by the manufacturer or sold with the product.
19. Unplug this product when a cart is used. Use caution when moving the cart/product combination to avoid injury from tip-over.
20. Refer all servicing to qualified service personnel. Servicing is needed when the product has been damaged in any way, such as a power supply cord or plug is damaged, liquid has been spilled, objects have fallen into the product, the product has been exposed to rain or moisture, does not operate normally, or has been dropped.



Copyright © Digital Watchdog 2022. All rights reserved. Specifications and pricing are subject to change without notice.

Legal considerations

Video 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. Digital Watchdog cannot be held responsible for technical or typographical errors and reserves the right to change the product and manuals without notice.

Digital Watchdog makes no warranty regarding the material contained within this document. Digital Watchdog shall neither be liable nor responsible for incidental or consequential damages concerning this material's furnishing, performance, or use. This product is only to be used for its intended purpose.

Equipment modifications

This equipment must be installed and used strictly per the instructions given in the user documentation. Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to use the equipment.

Trademark acknowledgments

Digital Watchdog, DW, DW Spectrum, MEGApix and Star-Light are registered trademarks or trademark applications of Digital Watchdog in various jurisdictions.

Regulatory Information

USA

This device complies with part 15 of the FCC Rules, subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.



This equipment has been tested and found to comply with the limits for a Class B digital device, according to part 15 of the FCC Rules. These limits are designed to protect reasonably against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used following the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. Suppose this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on. In that case, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and the receiver.
- Connect the equipment to an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Canada

This digital apparatus complies with CAN ICES-3 (Class B). The product shall be connected using a shielded network cable (STP) that is properly grounded. Cet appareil numérique est conforme à la norme CAN NMB-3 (classe B). Le produit doit être connecté à l'aide d'un câble réseau blindé (STP) qui est correctement mis à la terre.

Disposal and recycling

Digital Watchdog cares for the environment at all product manufacturing stages and is taking measures to provide customers with more environmentally friendly products. When this product has reached the end of its useful life, dispose of it according to local laws and regulations. For information about your nearest designated collection point, contact the local authority responsible for waste disposal. Following local legislation, penalties may be applicable for the incorrect disposal of this waste.

Warranty information

For information about Digital Watchdog's product warranty and related information, go to <https://digital-watchdog.com/page/rma-landing-page/>

Regular part replacement: a few parts (e.g., electrolytic capacitor) of the equipment shall be replaced regularly according to their average endurance time. The average time varies because of differences between the operating environment and the user's history, so regular checking is recommended for all users. Please contact your dealer for more details.

Support

Contact your Digital Watchdog installer or reseller for any questions, help and troubleshooting. If your questions are not answered immediately, your installer will forward them to ensure a rapid response. If you are connected to the Internet, you can:

- Download user documentation and software updates from Digital Watchdog's website.
- Find answers to resolved problems in the FAQ database
- Visit Digital Watchdog's Support at <https://digital-watchdog.com/DW-Tech-Support/>

Learn more!

Visit Digital Watchdog's learning center <https://digital-watchdog.com/page/dw-university/> for valuable training, webinars, tutorials and guides.



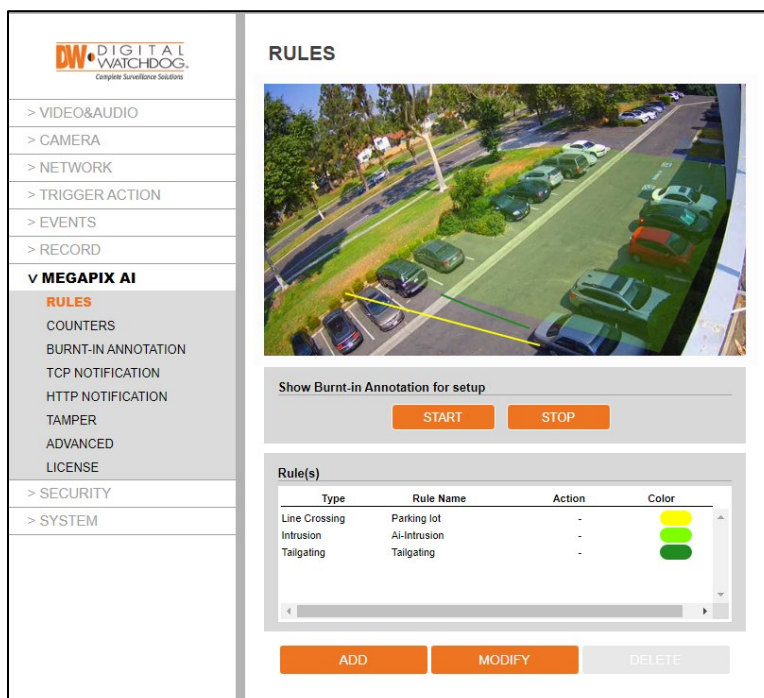
Table of Contents

Rules.....	6
Rules and Definitions.....	8
Intrusion.....	9
Line Crossing.....	10
Enter.....	11
Exit.....	12
Appear.....	13
Disappear.....	14
Stopped.....	15
Dwell.....	16
Direction.....	17
Tailgating.....	18
Counting Line.....	19
Logical Rule.....	20
Non-Detection Zone.....	22
Counters.....	23
Burnt-in Annotation.....	26
TCP Notification.....	27
HTTP Notification.....	29
Tamper.....	31
Advanced.....	32
License.....	33
Activate License.....	33
Activated License(s).....	33
Assign.....	33
How to apply a Token.....	34
How to Delete License(s).....	34
Tokens.....	35

Rules

Rules are used to react to events within a scene and trigger actions. To manage the rules active on the camera, open the camera's "SETUP" and go to MEGApix Ai > RULES.

Note: Chrome browser is recommended for Ai configuration.



The rules feature displays a live view from the camera and allows you to add, modify or delete rules.

Show Burnt-in annotation for setup:

Enable or disable the active rules display on the camera's preview screen. This is for the setup only. To enable the burnt-in annotation on the camera's live and recorded view, go to MEGApix Ai> Burnt-In annotation on the left navigation bar.

Note: Burnt-in annotation to be enabled on the left navigation bar to be enabled here.

Rules:

The table shows the current rules set up for the camera.

Add, Modify, Delete:

When selected, the drop-down menu will display all available rules to add to the camera.

How to Add a Rule:

1. Click 'Add' to display the available rules in the drop-down window, and select a rule to add.



2. Adjust the rule settings accordingly.
3. Click on 'Save' to save the rule.

How to Modify a Rule:

1. Select a rule from the table.
2. Click on 'Modify' to open the settings for the rule and modify them accordingly.
3. Click on 'Save' to save the rule.

How to Delete a Rule:

1. Select a rule from the table.
2. Click on 'Delete' to delete the rule from the list.

Note: Rules cannot be deleted if linked to an action or counter. Remove any links before deleting a rule.

Rules and Definitions

The table will show the rules defined for the camera. **Add** can be used to add additional rules. **Modify** is used to change the settings on a selected rule, and **Delete** will remove the selected rule.

Note: Rules cannot be deleted if linked to an action or counter. Remove these links before attempting to delete them.

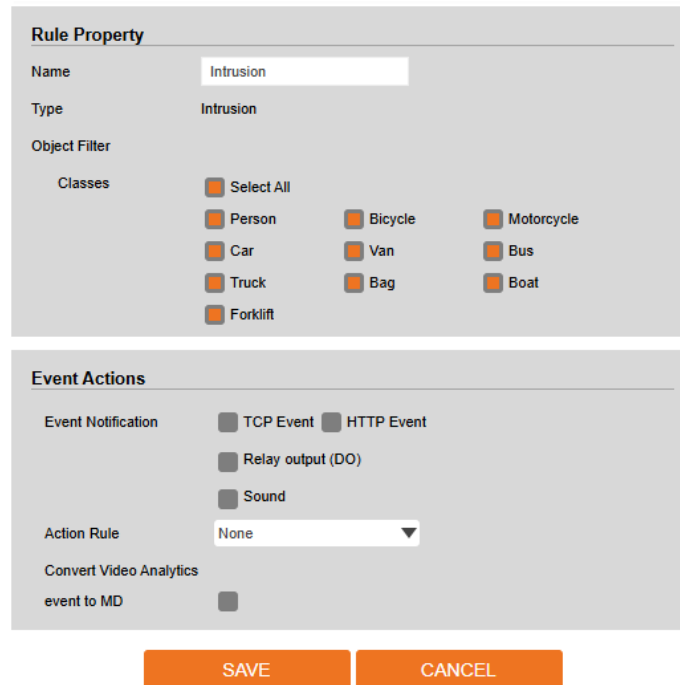
Types of Rules Available

- **Intrusion:** When people or objects are first detected inside the detection zone, they trigger an alarm. The people or objects keep being tracked while in the detection zone.
- **Line Crossing:** When people or objects cross the detection line in any direction, they trigger an alarm. The people or objects are tracked only once when they cross the detection line.
- **Enter:** An alarm is triggered when people or objects overlap with the detection zone's border.
- **Exit:** An alarm is triggered when people or objects leave the detection zone.
- **Appear:** An alarm will be triggered when the camera tracks people or objects inside the detection zone. The rule detects people or objects being tracked from within the detection zone.
- **Disappear:** An alarm will be triggered when the camera stops tracking people or objects inside the detection zone. The rule detects people or objects that stop being tracked from within the detection zone.
- **Stopped:** An alarm will be triggered when people or objects cross into a detection zone and remain past the set dwell time. The people or objects must remain stopped. Use the dwell rule for alarm triggers when an object remains moving in the zone.
- **Dwell:** An alarm will be triggered when people or objects cross into a detection zone and remain past the set dwell time. The people or objects must stay moving. Use the Stopped rule for alarm triggers when an object remains stopped in the zone.
- **Direction:** When people or objects cross the direct line from the set direction and angle, they will trigger an alarm.
- **Tailgating:** Detect a person or object crossing the detection line within a set period from the previous people or objects that have passed through the detection zone.
- **Counting Line:** When a person or object crosses the detection line in the set "forward" direction, the count adds 1. When a person or object crosses the detection line, the count decreases by 1. The counting can be added as a text overlay on the camera's view.
- **Logical Rules:** The logical rules option combines rules to form a complex filter for events to check against, which can help reduce false alerts.
- **Non-Detect Zone:** The non-detect zone option can be used to exclude areas of the scene from being processed through the analytics engine. This can reduce false triggers caused by moving foliage or busy scenes.
- **Camera Tampering:** An alarm is triggered when the camera detects the camera's bagging, defocusing, and general movement. (Please note the camera tampering setup is completed under MEGApix Ai> TAMPER.)

Intrusion

The Intrusion rule triggers an event when an object is first detected in the detection zone.

Note: The Intrusion rule will trigger in the same circumstances as the Enter and Appear rules. The choice of which rule is most appropriate will depend on the scenario and the camera's FOV.



The screenshot shows a configuration window for the 'Intrusion' rule. It is divided into two main sections: 'Rule Property' and 'Event Actions'.

Rule Property:

- Name:** A text field containing 'Intrusion'.
- Type:** A dropdown menu set to 'Intrusion'.
- Object Filter:** A section titled 'Classes' containing a grid of checkboxes for object types:
 - ☒ Select All
 - ☐ Person
 - ☐ Car
 - ☐ Truck
 - ☐ Forklift
 - ☐ Bicycle
 - ☐ Van
 - ☐ Bag
 - ☐ Motorcycle
 - ☐ Bus
 - ☐ Boat

Event Actions:

- Event Notification:** A section with checkboxes for:
 - ☐ TCP Event
 - ☐ HTTP Event
 - ☐ Relay output (DO)
 - ☐ Sound
- Action Rule:** A dropdown menu set to 'None'.
- Convert Video Analytics event to MD:** A checkbox that is currently unchecked.

At the bottom of the window are two orange buttons: 'SAVE' and 'CANCEL'.

The rule will create an overlay detection zone on the live view.

Click and drag any corners to adjust the zone's size and position.

Click on a gray node to split the segment and create a more complex shape. Select the minus red sign next to a node to remove a segment.

1. **Name:** Name the rule.
2. **Object Filter:** Allow the rule to trigger based on the classification of an object (e.g., person, vehicle). Any combination of the available options is possible.
3. **Event Actions:** Define the action to occur when an event is triggered. Any combination of the available options is possible.
 - a. TCP Event: Enable/disable TCP notification when an event occurs.
 - b. HTTP Event: Enable/disable HTTP notification when an event occurs.

Note: TCP/HTTP notification actions must be configured separately under the left navigation bar.

4. **Action Rule:** Send an image of the camera's view to an FTP/SMTP server when an event occurs.
Note: FTP and/or SMTP servers must be added, and IMAGE TRANSFER must be set in the left navigation bar.
5. **Convert Video Analytics:** Pass an Ai event to the camera's event engine, which is compatible with ONVIF.
6. Click 'Save' to save all settings.
 Click 'Cancel' to return to the previous setting.

Line Crossing

The line-crossing rule triggers an event when an object is first detected crossing the rule line.

Note: The line-crossing rule will activate in the same circumstances as the direction and counting line rules. The choice of which rule is most appropriate will depend on the scenario and the camera's FOV.

The screenshot shows a configuration window with two main sections: 'Rule Property' and 'Event Actions'.

Rule Property:

- Name:** Line Crossing
- Type:** Line Crossing
- Object Filter:**
 - Classes:**
 - ☒ Select All
 - ☒ Person
 - ☒ Car
 - ☒ Truck
 - ☒ Forklift
 - ☒ Bicycle
 - ☒ Van
 - ☒ Bag
 - ☒ Motorcycle
 - ☒ Bus
 - ☒ Boat

Event Actions:

- Event Notification:**
 - ☐ TCP Event
 - ☐ HTTP Event
 - ☐ Sound
- Action Rule:** None (dropdown menu)
- Convert Video Analytics event to MD:** ☐

At the bottom are two orange buttons: **SAVE** and **CANCEL**.

The rule will create a line and overlay it on the live view.

The line's orientation and length can be reshaped by selecting the color nodes at the edge of the lines.

Click on a gray node to split the segment and create a more complex shape.

Select the minus red sign next to a node to remove a segment.

1. **Name:** Name the rule.
2. **Object Filter:** Allow the rule to trigger based on the classification of an object (e.g., person, vehicle). Any combination of the available options is possible.
3. **Event Actions:** Define the action to occur when an event is triggered. Any combination of the available options is possible.
 - a. TCP Event: Enable/disable TCP notification when an event occurs.
 - b. HTTP Event: Enable/disable HTTP notification when an event occurs.

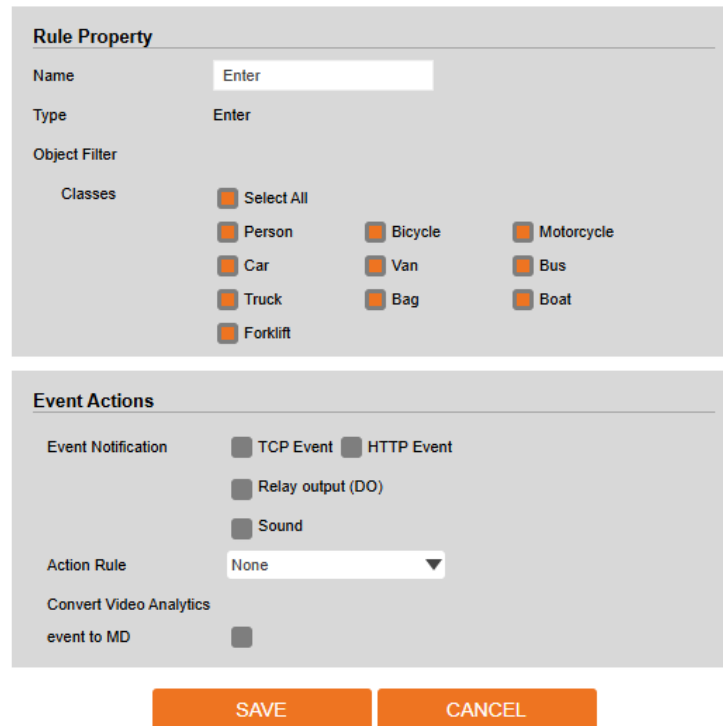
Note: TCP/HTTP notification actions must be configured separately under the left navigation bar.

4. **Action Rule:** Send an image of the camera's view to an FTP/SMTP server when an event occurs.
Note: FTP and/or SMTP servers must be added, and IMAGE TRANSFER must be set in the left navigation bar.
5. **Convert Video Analytics:** Pass an Ai event to the camera's event engine, which is compatible with ONVIF.
6. Click 'Save' to save all settings.
 Click 'Cancel' to return to the previous setting.

Enter

The enter rule triggers an event when an object crosses from outside to inside a zone.

Note: The enter rule detects already-tracked objects crossing the zone border from outside to inside.



The screenshot shows a configuration window with two main sections: 'Rule Property' and 'Event Actions'.

Rule Property:

- Name:** Enter
- Type:** Enter
- Object Filter:**
 - Classes:**
 - ☒ Select All
 - ☒ Person
 - ☒ Bicycle
 - ☒ Motorcycle
 - ☒ Car
 - ☒ Van
 - ☒ Bus
 - ☒ Truck
 - ☒ Bag
 - ☒ Boat
 - ☒ Forklift

Event Actions:

- Event Notification:**
 - ☐ TCP Event
 - ☐ HTTP Event
 - ☐ Relay output (DO)
 - ☐ Sound
- Action Rule:** None (dropdown menu)
- Convert Video Analytics event to MD:** ☐

At the bottom, there are two orange buttons: 'SAVE' and 'CANCEL'.

The rule will create an overlay detection zone on the live view.

Click and drag any corners to adjust the zone's size and position.

Click on a gray node to split the segment and create a more complex shape. Select the minus red sign next to a node to remove a segment.

1. **Name:** Name the rule.
2. **Object Filter:** Allow the rule to trigger based on the classification of an object (e.g., person, vehicle). Any combination of the available options is possible.
3. **Event Actions:** Define the action to occur when an event is triggered. Any combination of the available options is possible.
 - a. TCP Event: Enable/disable TCP notification when an event occurs.
 - b. HTTP Event: Enable/disable HTTP notification when an event occurs.

Note: TCP/HTTP notification actions must be configured separately under the left navigation bar.

4. **Action Rule:** Send an image of the camera's view to an FTP/SMTP server when an event occurs.
Note: FTP and/or SMTP servers must be added, and IMAGE TRANSFER must be set in the left navigation bar.
5. **Convert Video Analytics:** Pass an Ai event to the camera's event engine, which is compatible with ONVIF.
6. Click 'Save' to save all settings.
 Click 'Cancel' to return to the previous setting.

Exit

The exit rule triggers an event when an object crosses from inside to outside a zone.

Note: The exit rule detects already-tracked objects crossing the zone border from inside to outside.

Rule Property

Name: Exit

Type: Exit

Object Filter

Classes

- ☐ Select All
- ☐ Person
- ☐ Bicycle
- ☐ Motorcycle
- ☐ Car
- ☐ Van
- ☐ Bus
- ☐ Truck
- ☐ Bag
- ☐ Boat
- ☐ Forklift

Event Actions

Event Notification

- ☐ TCP Event
- ☐ HTTP Event
- ☐ Relay output (DO)
- ☐ Sound

Action Rule: None

Convert Video Analytics event to MD: ☐

SAVE CANCEL

The rule will create an overlay detection zone on the live view.

Click and drag any corners to adjust the zone's size and position.

Click on a gray node to split the segment and create a more complex shape. Select the minus red sign next to a node to remove a segment.

1. **Name:** Name the rule.
2. **Object Filter:** Allow the rule to trigger based on the classification of an object (e.g., person, vehicle). Any combination of the available options is possible.
3. **Event Actions:** Define the action to occur when an event is triggered. Any combination of the available options is possible.
 - a. TCP Event: Enable/disable TCP notification when an event occurs.
 - b. HTTP Event: Enable/disable HTTP notification when an event occurs.

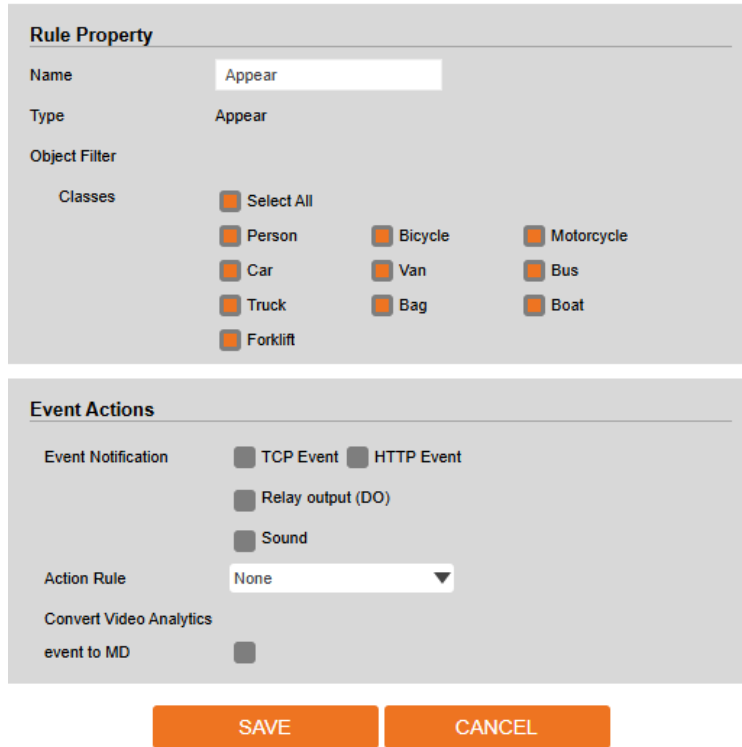
Note: TCP/HTTP notification actions must be configured separately under the left navigation bar.

4. **Action Rule:** Send an image of the camera's view to an FTP/SMTP server when an event occurs.
Note: FTP and/or SMTP servers must be added, and IMAGE TRANSFER must be set in the left navigation bar.
5. **Convert Video Analytics:** Pass an Ai event to the camera's event engine, which is compatible with ONVIF.
6. Click 'Save' to save all settings.
 Click 'Cancel' to return to the previous setting.

Appear

The appear rule triggers an event when an object starts to be tracked from within a zone.

Note: The appear rule detects objects being tracked from within a zone.



The rule will create an overlay detection zone on the live view.

Click and drag any corners to adjust the zone's size and position.

Click on a gray node to split the segment and create a more complex shape. Select the minus red sign next to a node to remove a segment.

1. **Name:** Name the rule.
2. **Object Filter:** Allow the rule to trigger based on the classification of an object (e.g., person, vehicle). Any combination of the available options is possible.
3. **Event Actions:** Define the action to occur when an event is triggered. Any combination of the available options is possible.
 - a. TCP Event: Enable/disable TCP notification when an event occurs.
 - b. HTTP Event: Enable/disable HTTP notification when an event occurs.

Note: TCP/HTTP notification actions must be configured separately under the left navigation bar.

4. **Action Rule:** Send an image of the camera's view to an FTP/SMTP server when an event occurs.
Note: FTP and/or SMTP servers must be added, and IMAGE TRANSFER must be set in the left navigation bar.
5. **Convert Video Analytics:** Pass an Ai event to the camera's event engine, which is compatible with ONVIF.
6. Click 'Save' to save all settings.
 Click 'Cancel' to return to the previous setting.

Disappear

The disappear rule triggers an event when an object stops being tracked from within a zone.

Note: The disappear rule detects objects that stop being tracked from within a zone.

Rule Property

Name: Disappear

Type: Disappear

Event Actions

Event Notification: ☐ TCP Event ☐ HTTP Event

☐ Relay output (DO)

☐ Sound

Action Rule: None

Convert Video Analytics event to MD: ☐

SAVE CANCEL

The rule will create an overlay detection zone on the live view.

Click and drag any corners to adjust the zone's size and position.

Click on a gray node to split the segment and create a more complex shape. Select the minus red sign next to a node to remove a segment.

1. **Name:** Name the rule.
2. **Object Filter:** Allow the rule to trigger based on the classification of an object (e.g., person, vehicle). Any combination of the available options is possible.
3. **Event Actions:** Define the action to occur when an event is triggered. Any combination of the available options is possible.
 - a. TCP Event: Enable/disable TCP notification when an event occurs.
 - b. HTTP Event: Enable/disable HTTP notification when an event occurs.

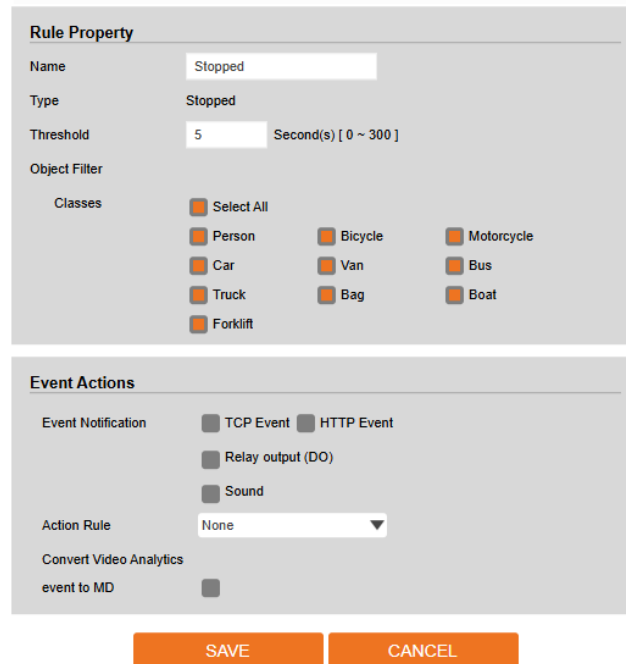
Note: TCP/HTTP notification actions must be configured separately under the left navigation bar.

4. **Action Rule:** Send an image of the camera's view to an FTP/SMTP server when an event occurs.
Note: FTP and/or SMTP servers must be added, and IMAGE TRANSFER must be set in the left navigation bar.
5. **Convert Video Analytics:** Pass an Ai event to the camera's event engine, which is compatible with ONVIF.
6. Click 'Save' to save all settings.
 Click 'Cancel' to return to the previous setting.

Stopped

The stopped rule detects objects stationary inside a detection zone for longer than the specified threshold.

Note: The stopped rule does not detect abandoned objects. It detects objects that are moving and then becomes stationary.



The screenshot shows a configuration window for a 'Stopped' rule. It is divided into two main sections: 'Rule Property' and 'Event Actions'.

Rule Property:

- Name:** Stopped
- Type:** Stopped
- Threshold:** 5 Second(s) [0 ~ 300]
- Object Filter:**
 - Classes:**
 - ☒ Select All
 - ☒ Person
 - ☒ Car
 - ☒ Truck
 - ☒ Forklift
 - ☒ Bicycle
 - ☒ Van
 - ☒ Bag
 - ☒ Motorcycle
 - ☒ Bus
 - ☒ Boat

Event Actions:

- Event Notification:**
 - ☐ TCP Event
 - ☐ HTTP Event
 - ☐ Relay output (DO)
 - ☐ Sound
- Action Rule:** None (dropdown menu)
- Convert Video Analytics event to MD:** ☐

At the bottom of the window are two orange buttons: 'SAVE' and 'CANCEL'.

The rule will create an overlay detection zone on the live view.

Click and drag any corners to adjust the zone's size and position.

Click on a gray node to split the segment and create a more complex shape. Select the minus red sign next to a node to remove a segment.

1. **Name:** Name the rule.
2. **Threshold:** Define, in seconds, the time an object must be stopped before triggering an event.
3. **Object Filter:** Allow the rule to trigger based on the classification of an object (e.g., person, vehicle). Any combination of the available options is possible.
4. **Event Actions:** Define the action to occur when an event is triggered. Any combination of the available options is possible.

a. TCP Event: Enable/disable TCP notification when an event occurs.

b. HTTP Event: Enable/disable HTTP notification when an event occurs.

Note: TCP/HTTP notification actions must be configured separately under the left navigation bar.

5. **Action Rule:** Send an image of the camera's view to an FTP/SMTP server when an event occurs.

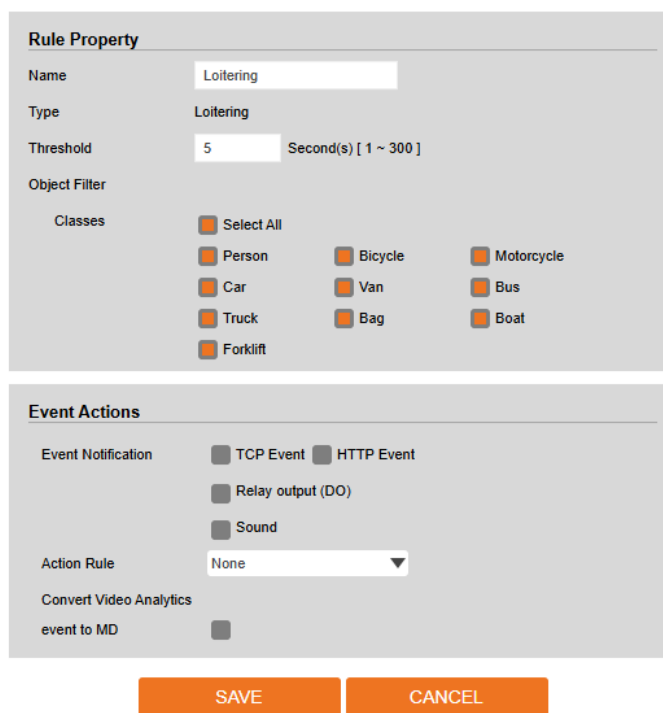
Note: FTP and/or SMTP servers must be added, and IMAGE TRANSFER must be set in the left navigation bar.

6. **Convert Video Analytics:** Pass an Ai event to the camera's event engine, which is compatible with ONVIF.

7. Click 'Save' to save all settings.
Click 'Cancel' to return to the previous setting.

Dwell

The Dwell rule triggers an event when a person is in a detection zone for a set threshold.



The rule will create an overlay detection zone on the live view.

Click and drag any corners to adjust the zone's size and position.

Click on a gray node to split the segment and create a more complex shape. Select the minus red sign next to a node to remove a segment.

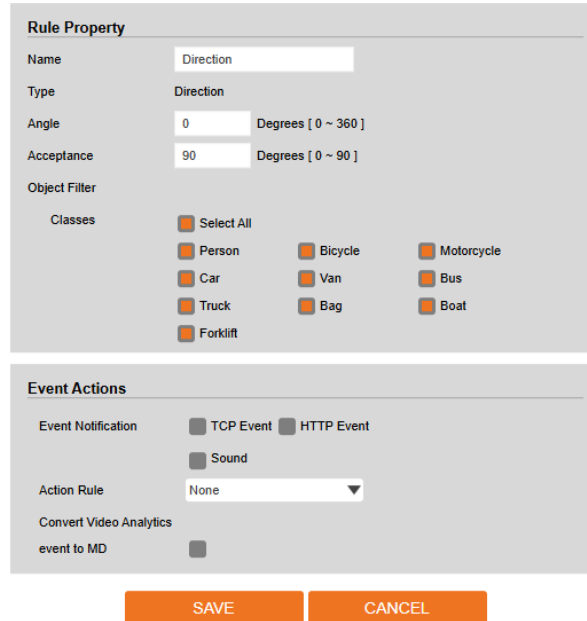
1. **Name:** Name the rule.
2. **Threshold:** Define, in seconds, the time an object must be stopped before triggering an event.
3. **Object Filter:** Allow the rule to trigger based on the classification of an object (e.g., person, vehicle). Any combination of the available options is possible.
4. **Event Actions:** Define the action to occur when an event is triggered. Any combination of the available options is possible.
 - a. TCP Event: Enable/disable TCP notification when an event occurs.
 - b. HTTP Event: Enable/disable HTTP notification when an event occurs.

Note: TCP/HTTP notification actions must be configured separately under the left navigation bar.

5. **Action Rule:** Send an image of the camera's view to an FTP/SMTP server when an event occurs.
Note: FTP and/or SMTP servers must be added, and IMAGE TRANSFER must be set in the left navigation bar.
6. **Convert Video Analytics:** Pass an Ai event to the camera's event engine, which is compatible with ONVIF.
7. Click 'Save' to save all settings.
Click 'Cancel' to return to the previous setting.

Direction

The direction rule triggers an event when an object crosses the detection line in a particular direction and within acceptable parameters.



The screenshot shows a configuration window with two main sections: 'Rule Property' and 'Event Actions'.

Rule Property:

- Name:** Direction
- Type:** Direction
- Angle:** 0 Degrees [0 ~ 360]
- Acceptance:** 90 Degrees [0 ~ 90]
- Object Filter:**
 - Classes:**
 - ☒ Select All
 - ☒ Person
 - ☒ Car
 - ☒ Truck
 - ☒ Forklift
 - ☒ Bicycle
 - ☒ Van
 - ☒ Bag
 - ☒ Motorcycle
 - ☒ Bus
 - ☒ Boat

Event Actions:

- Event Notification:**
 - ☐ TCP Event
 - ☐ HTTP Event
 - ☐ Sound
- Action Rule:** None
- Convert Video Analytics event to MD:** ☐

At the bottom, there are two orange buttons: 'SAVE' and 'CANCEL'.

The rule will create a line and overlay it on the live view.

The line's orientation and length can be reshaped by selecting the color nodes at the edge of the lines.

Click on a gray node to split the segment and create a more complex shape.

Select the minus red sign next to a node to remove a segment.

1. **Name:** Name the rule.
2. **Angle:** Define the direction in which the objects move to trigger an event.
3. **Acceptance:** Define the allowed variance on the direction side that will still trigger an event.
4. **Object Filter:** Allow the rule to trigger based on the classification of an object (e.g., person, vehicle). Any combination of the available options is possible.
5. **Event Actions:** Define the action to occur when an event is triggered. Any combination of the available options is possible.
 - a. TCP Event: Enable/disable TCP notification when an event occurs.
 - b. HTTP Event: Enable/disable HTTP notification when an event occurs.

Note: TCP/HTTP notification actions must be configured separately under the left navigation bar.

6. **Action Rule:** Send an image of the camera's view to an FTP/SMTP server when an event occurs.

Note: FTP and/or SMTP servers must be added, and IMAGE TRANSFER must be set in the left navigation bar.

7. **Convert Video Analytics:** Pass an Ai event to the camera's event engine, which is compatible with ONVIF.
8. Click 'Save' to save all settings.
Click 'Cancel' to return to the previous setting.

Tailgating

The tailgating rule triggers an event when objects cross a detection line within quick succession of each other in a set time.

Rule Property

Name: Tailgating

Type: Tailgating

Threshold: 1 Second(s) [1 ~ 300]

Object Filter

Classes

☒ Select All

☐ Person ☐ Bicycle ☐ Motorcycle

☐ Car ☐ Van ☐ Bus

☐ Truck ☐ Bag ☐ Boat

☐ Forklift

Event Actions

Event Notification ☐ TCP Event ☐ HTTP Event

☐ Sound

Action Rule: None

Convert Video Analytics

event to MD ☐

SAVE CANCEL

The rule will create a line and overlay it on the live view.

The line's orientation and length can be reshaped by selecting the color nodes at the edge of the lines.

Click on a gray node to split the segment and create a more complex shape.

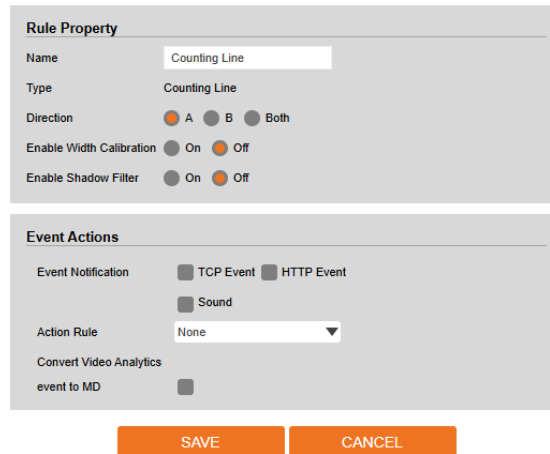
Select the minus red sign next to a node to remove a segment.

1. **Name:** Name the rule.
 2. **Threshold:** Define, in seconds, the time an object must be stopped before triggering an event.
 3. **Object Filter:** Allow the rule to trigger based on the classification of an object (e.g., person, vehicle). Any combination of the available options is possible.
 4. **Event Actions:** Define the action to occur when an event is triggered. Any combination of the available options is possible.
 - a. TCP Event: Enable/disable TCP notification when an event occurs.
 - b. HTTP Event: Enable/disable HTTP notification when an event occurs.
- Note:** TCP/HTTP notification actions must be configured separately under the left navigation bar.
5. **Action Rule:** Send an image of the camera's view to an FTP/SMTP server when an event occurs.
Note: FTP and/or SMTP servers must be added, and IMAGE TRANSFER must be set in the left navigation bar.
 6. **Convert Video Analytics:** Pass an Ai event to the camera's event engine, which is compatible with ONVIF.
 7. Click 'Save' to save all settings.
Click 'Cancel' to return to the previous setting.

Counting Line

The counting line rule triggers an event when an object crosses the line in the direction indicated.

Note: The counting line differs from the direction rule. Each segment of the line can have a different direction defined.



The screenshot shows two configuration panels. The top panel, titled 'Rule Property', contains the following settings: Name (Counting Line), Type (Counting Line), Direction (radio buttons for A, B, and Both, with A selected), Enable Width Calibration (radio buttons for On and Off, with Off selected), and Enable Shadow Filter (radio buttons for On and Off, with Off selected). The bottom panel, titled 'Event Actions', contains: Event Notification (checkboxes for TCP Event and HTTP Event, both unchecked), Sound (checkbox, unchecked), Action Rule (dropdown menu set to None), Convert Video Analytics (checkbox, unchecked), and event to MD (checkbox, unchecked). At the bottom of the form are two orange buttons: 'SAVE' and 'CANCEL'.

The rule will create a line and overlay it on the live view.

The line's orientation and length can be reshaped by selecting the color nodes at the edge of the lines.

Click on a gray node to split the segment and create a more complex shape.

Select the minus red sign next to a node to remove a segment.

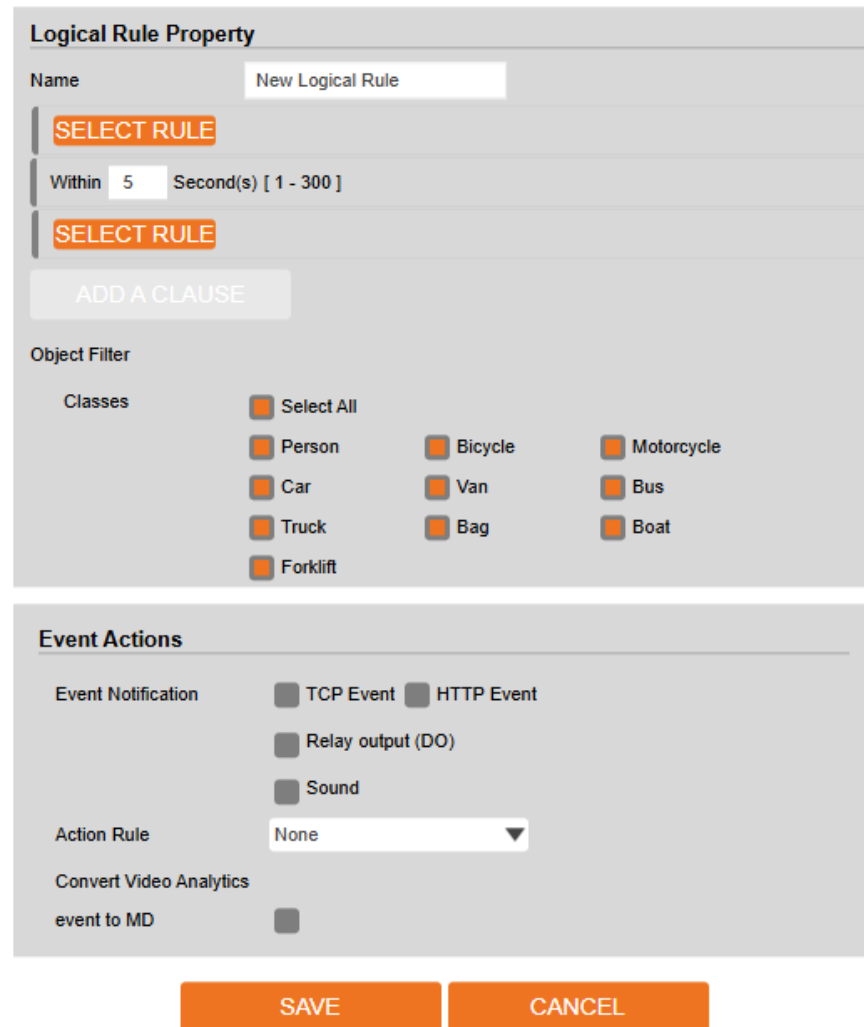
1. **Name:** Name the rule.
2. **Direction:** Define the direction that will be monitored.
 - a. A: Define the direction monitored.
 - b. B: Define the opposite direction from A to be monitored.
 - c. Both: Both directions across the counting line are monitored
3. **Enable Width Calibration:** If enabled, define the width value for the counting line to count an object.
4. **Enable Shadow Filter:** The camera can analyze the image to prevent counting shadows.
5. **Event Actions:** Define the action to occur when an event is triggered. Any combination of the available options is possible.
 - a. TCP Event: Enable/disable TCP notification when an event occurs.
 - b. HTTP Event: Enable/disable HTTP notification when an event occurs.

Note: TCP/HTTP notification actions must be configured separately under the left navigation bar.

6. **Action Rule:** Send an image of the camera's view to an FTP/SMTP server when an event occurs.
Note: FTP and/or SMTP servers must be added, and IMAGE TRANSFER must be set in the left navigation bar.
7. **Convert Video Analytics:** Pass an Ai event to the camera's event engine, which is compatible with ONVIF.
8. Click 'Save' to save all settings.
 Click 'Cancel' to return to the previous setting.

Logical Rule

Combine various rules and inputs using logical expressions to reduce false events.



The screenshot shows a 'Logical Rule Property' dialog box. It has a 'Name' field with the text 'New Logical Rule'. Below it are two 'SELECT RULE' buttons. Between them is a 'Within' field with the value '5' and a range '[1 - 300]' with the unit 'Second(s)'. Below that is another 'SELECT RULE' button and an 'ADD A CLAUSE' button. The 'Object Filter' section contains a 'Classes' label and a grid of checkboxes for various object types: Select All, Person, Car, Truck, Forklift, Bicycle, Van, Bag, Motorcycle, Bus, and Boat. The 'Event Actions' section includes checkboxes for 'Event Notification' (TCP Event, HTTP Event, Relay output (DO), Sound), a dropdown for 'Action Rule' (set to 'None'), and checkboxes for 'Convert Video Analytics' and 'event to MD'. At the bottom are 'SAVE' and 'CANCEL' buttons.

The rule allows you to combine other rules into a logical expression using the AND operator and can be used to filter and reduce false events.

1. **Name:** Name the rule.
2. **Within xx seconds:** add the maximum time (in seconds) between two rules.
3. **Add a Clause:** add more rules to the logic rule.
4. **Object Filter:** Allow the rule to trigger based on the classification of an object (e.g., person, vehicle). Any combination of the available options is possible.
5. **Event Actions:** Define the action to occur when an event is triggered. Any combination of the available options is possible.
 - a. TCP Event: Enable/disable TCP notification when an event occurs.

- b. HTTP Event: Enable/disable HTTP notification when an event occurs.

Note: TCP/HTTP notification actions must be configured separately under the left navigation bar.

6. **Action Rule:** Send an image of the camera's view to an FTP/SMTP server when an event occurs.
Note: FTP and/or SMTP servers must be added, and IMAGE TRANSFER must be set in the left navigation bar.
7. **Convert Video Analytics:** Pass an Ai event to the camera's event engine, which is compatible with ONVIF.
8. Click 'Save' to save all settings.
Click 'Cancel' to return to the previous setting.

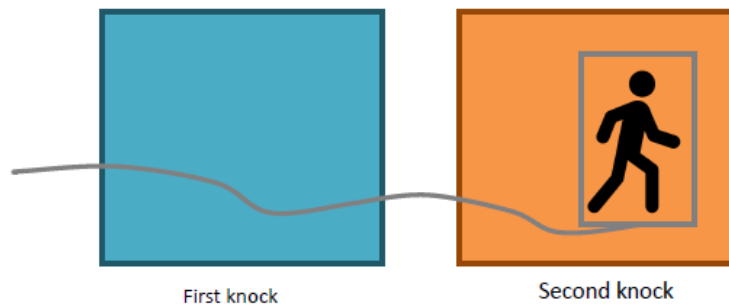
Using logical rules:

Logical rules can combine multiple rules into a single condition. Objects are checked against all combined rules before they become an event and trigger an action.

Example of a double-knock rule:

The double-knock rule is one of the most common scenarios used in video analytics. It uses two or more rules together to reduce false events. An object must trigger both rules before becoming an event and triggering an action.

If the zones used in rules for a double-knock scenario are in different locations, you can set an object's time threshold before triggering the following rule to become an event.

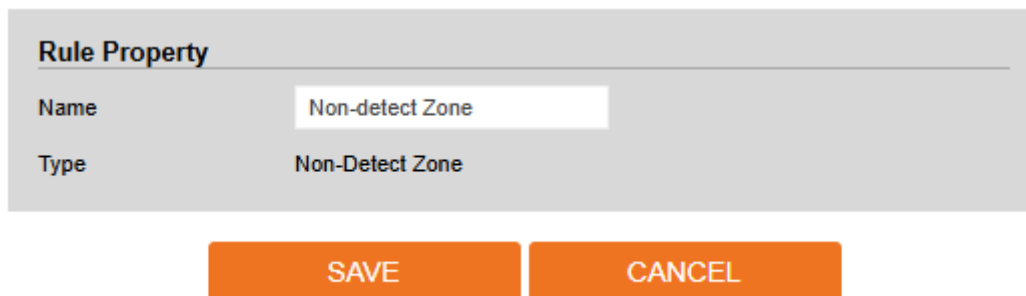


How to create a logical rule:

1. Select the two rules to be used in the double-knock logical rule.
2. Add a new logical rule.
3. Define a name for the rule.
4. Define the combination of rules and logical conditions that objects will be checked against.
5. Enable the check box in front of 'Within ____ seconds then.' Define the number of seconds an object must pass from one zone to the other to cause an event.
6. Define the action that will occur when the object triggers an event.
7. Click 'Save' to save all settings.
8. Click 'Cancel' to return to the previous setting.

Non-Detection Zone

The non-detection rule creates a zone that will not be processed through the analytics engine.



The screenshot shows a 'Rule Property' dialog box with a light gray background. It contains two rows of properties: 'Name' with the value 'Non-detect Zone' and 'Type' with the value 'Non-Detect Zone'. Below the properties are two orange buttons labeled 'SAVE' and 'CANCEL'.

Rule Property	
Name	Non-detect Zone
Type	Non-Detect Zone

SAVE CANCEL

The rule will create an overlay detection zone on the live view.

Click and drag any corners to adjust the zone's size and position.

Click on a gray node to split the segment and create a more complex shape. Select the minus red sign next to a node to remove a segment.

1. **Name:** Name the rule.
2. Click 'Save' to save all settings.
Click 'Cancel' to return to the previous setting.

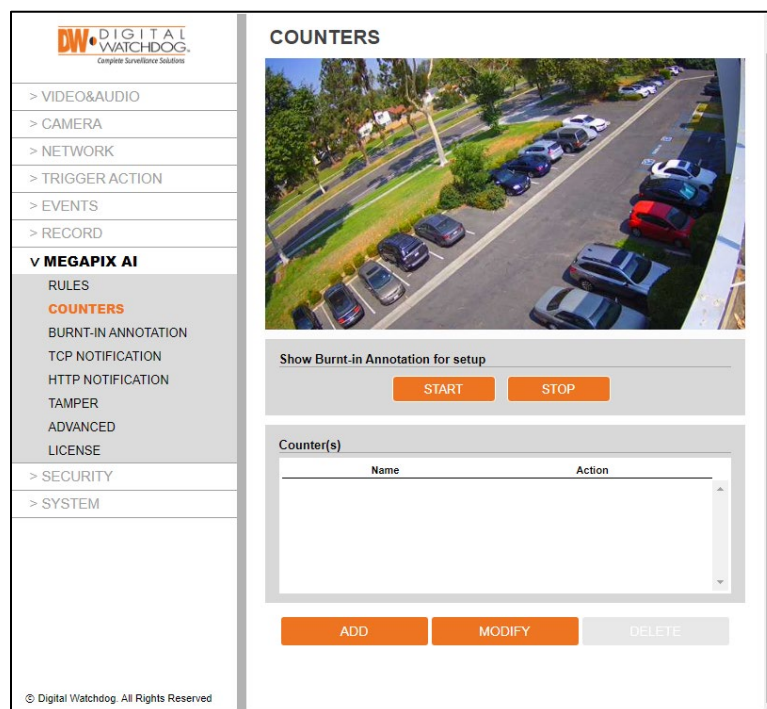


Counters

Counters can be configured to count the number of times a rule is triggered. The counter rule can count the following:

- **Increment:** The counter value increases with each trigger of an event.
- **Decrement:** The counter value decreases with each trigger of an event.
- **Occupancy:** The counter reflects the number of objects triggering the attached rule(s). It is available for a rule that links to a detection zone.

More than one rule can be assigned to any counter's three inputs. This allows, for example, the occupancy of two rules to be reflected in a single counter. Multiple counters can also be created.



The counters page displays a live view from the camera and allows you to add, modify or delete counters.

Show Burnt-in Annotation for Setup

Use this option to show analytic data on the camera view, select **Start** to show the data and **Stop** to hide the data.

Note: The burnt-in annotation feature must be enabled for this option to work. This does not affect the camera's analytical processing, but it may require additional resources from the camera and therefore is not enabled by default.

Counter(s)

The table will show the counters that have been defined for the camera. **Add** can be used to add a counter. **Modify** is used to change the settings on a selected counter, and **Delete** will remove the selected counter.

Counter

Counter Property

Name
Counter

Increment
ADD INPUT

Decrement
ADD INPUT

Occupancy
ADD INPUT

Trigger Condition
Counter Value Is
changed
0

RESET COUNTER

Event Actions

Event Notification
☐ TCP Event
☐ HTTP Event

Action Rule
None

Convert IVA To MD
☐

SAVE

CANCEL

More than one counting line rule can be assigned to a counter input. This allows, for example, the occupancy of two counting lines to be reflected in a single counter or more than one entrance/exit gate to be assigned to a counter.

Note: counters should not simultaneously be used for occupancy and increment/decrement.

1. **Name:** Name the counter.
2. **Increment:** Select the rule from the available list that will add to the counter when triggered.
3. **Decrement:** Select the rule from the available list that will subtract from the counter when triggered.
4. **Occupancy:** Set the counter rule from the available list, which, when triggered, will add to the counter.
5. **Trigger Condition:** Define the counter threshold that will cause an event to be triggered.

Counter Value Is

changed

changed
greater than or equal
greater than
equal
less than or equal
less than

6. **Reset Counter:** Remove all current settings from the selected counter.
Note: Clicking the Reset Counter button will return the counter tally to zero.
7. **Event Actions:** Define the action to occur when an event is triggered. Any combination of the available options is possible.
 - a. TCP Event: Enable/disable TCP notification when an event occurs.
 - b. HTTP Event: Enable/disable HTTP notification when an event occurs.

Note: TCP/HTTP notification actions must be configured separately under the left navigation bar.



8. **Action Rule:** Send an image of the camera's view to an FTP/SMTP server when an event occurs.
Note: FTP and/or SMTP servers must be added, and IMAGE TRANSFER must be set in the left navigation bar.
9. **Convert IVA to MD:** Pass an Ai event to the camera's event engine, which is compatible with ONVIF.
10. **Click 'Save' to save all settings.**
Click 'Cancel' to return to the previous setting.

How to create a Counter:

1. Select 'Add' to add a new counter and display the available options.
2. Move the counter by clicking and dragging the block to the desired position on the screen.
3. Enter a name for the counter.
4. Select 'Add Input' next to the desired action (increment, decrement, occupancy). Select a rule to link to the counter.
5. Define the action to trigger when counter values change.
6. Select 'Save' to save the rule.

How to modify a Counter:

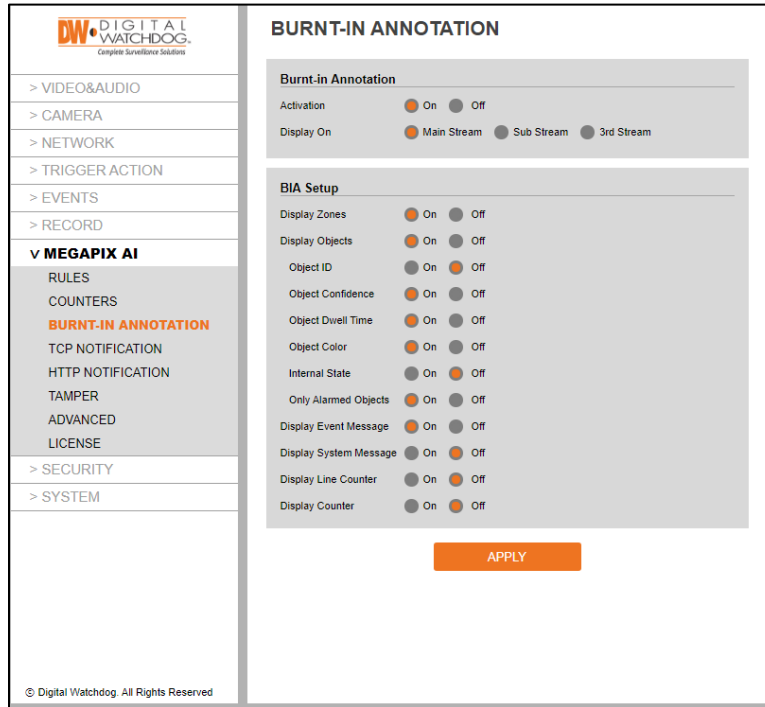
1. Highlight the counter and press 'Modify' to open the settings for the counter.
2. Modify the counter accordingly.
3. Select 'Save' to save the counter.

How to Delete a Counter:

1. Highlight the counter to be deleted.
2. Select 'Delete' to delete the counter from the list.

Burnt-in Annotation

The Burnt-In Annotation feature overlaps analytical data on the raw video stream. Annotations can include tracked objects, counters and system messages.



BURNT-IN ANNOTATION

Burnt-in Annotation

Activation ☒ On ☐ Off

Display On ☒ Main Stream ☐ Sub Stream ☐ 3rd Stream

BIA Setup

Display Zones ☒ On ☐ Off

Display Objects ☒ On ☐ Off

Object ID ☐ On ☒ Off

Object Confidence ☒ On ☐ Off

Object Dwell Time ☒ On ☐ Off

Object Color ☒ On ☐ Off

Internal State ☐ On ☒ Off

Only Alarmed Objects ☒ On ☐ Off

Display Event Message ☒ On ☐ Off

Display System Message ☐ On ☒ Off

Display Line Counter ☐ On ☒ Off

Display Counter ☐ On ☒ Off

APPLY

© Digital Watchdog. All Rights Reserved

1. **Activation:** Turn on burnt-in annotation.
2. **Display on:** Select to display the burnt-in annotation on the camera's first, second or third streams.
Note: Burnt-in annotation is unavailable if the stream is set to a higher resolution than 2.1MP/1080p.
 - a. **Main Stream:** Display the burnt-in annotation on the mainstream.
 - b. **Sub Stream:** Display the burnt-in annotation on the sub-stream.
 - c. **3rd Stream:** Display the burnt-in annotation on the 3rd stream.
3. **BIA Setup:** Select which annotations to display.
4. Select 'Apply' to save all changes.



TCP Notification

The TCP notification sends data to a remote TCP server when an event triggers a TCP notification. The format is configurable with a mixture of plain text and tokens. Tokens represent the event's metadata and will be included when a rule is triggered.

General Setting:

- **ON/OFF:** Enable or disable TCP notifications.

Note: Disabling TCP notifications will impact the rules' ability to send notifications through this action. Rules can still show a link to this action, but the action will not occur when the rule is triggered.

TCP Settings:

- **Host URL:** Enter the IP address or hostname of the remote TCP server receiving the event data.
- **Port:** Enter the port information associated with the TCP server.

Message:

- **Rule:** Enter a custom message for the TCP notification when linked to rules. You can include tokens from the available list. Token values will be replaced with the event metadata when triggered.
Note: Select the available tokens in the drop-down menu below the message window.
- **Counter:** Enter a custom message for the TCP notification when linked to counters. You can include Tokens from the available list. Token values will be replaced with the event metadata when triggered.
Note: Select the available tokens in the drop-down menu below the message window.
- **Tamper:** Enter a custom message for the TCP notification when linked to the camera tamper. You can include tokens from the list available. Token values will be replaced with the event metadata when triggered.

Note: Select the available tokens in the drop-down menu below the message window.

- Select 'Apply' to save your changes.

Note: See the tokens page for a complete list of the token system and example templates.



HTTP Notification

When an event is triggered, the HTTP notification sends a text/plain HTTP request to a remote endpoint. The format is configurable with a mixture of plain text and tokens. Tokens represent the event's metadata and will be included when a rule is triggered.

HTTP NOTIFICATION

General Setting
● On ● Off

HTTP Settings
Send To: Custom
URL: http://
Method: GET
User ID:
Password:

Query
Rule: ?p={ip}&uname={host}&date={datetime}&ts={time}&type=vca&id={id}&type=event&ev={id}&ts={value}, &p={type}, &v={zone}, &rt={ruleid}, &q=0 &id={id}, &v={value}, &st={time}&event={time}&id={ruleid}&vca={vca}&id={id}&uname={mac}
Counter: Select a token to add
Tamper: Select a token to add

APPLY

© Digital Watchdog. All Rights Reserved

General Setting:

ON/OFF: Enable or disable HTTP notifications.

Note: Disabling HTTP notifications will impact the rules' ability to send notifications through this action. Rules can still show a link to this action, but the action will not occur when the rule is triggered.

HTTP Settings:

- **URL:** Enter the IP address or hostname of the remote server receiving the event data.
- **Method:** Select the HTTP request method. Select from GET (default), POST, or Milestone.
- **User ID:** Enter the username used to send the notification.
- **Password:** Enter the username's password used to send the notification.

Query:

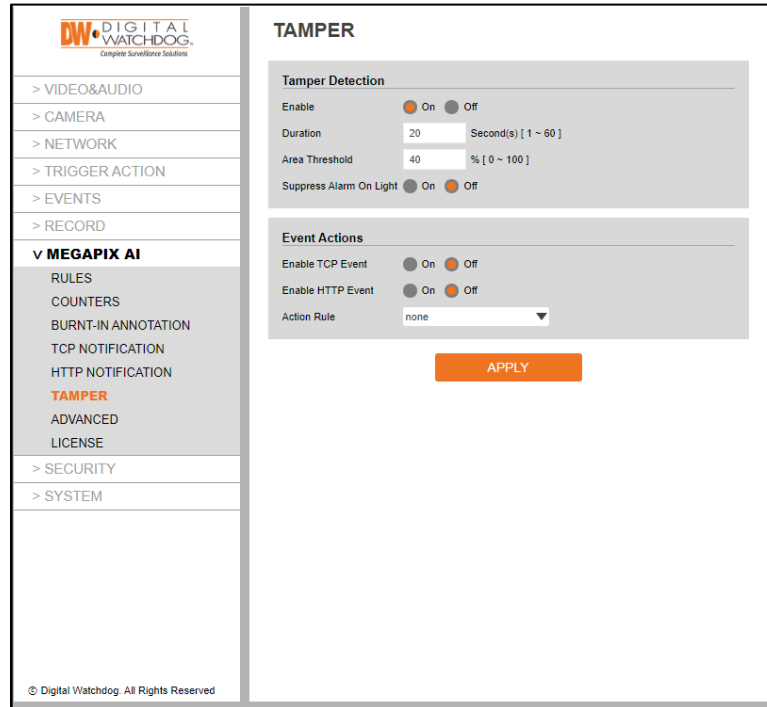
- **Rule:** Enter a custom message for the HTTP notification when linked to rules. You can include tokens from the list available. Token values will be replaced with the event metadata when triggered.
Note: Select the available tokens in the drop-down menu below the message window.
- **Counter:** Enter a custom message for the HTTP notification when linked to counters. You can include tokens from the list available. Token values will be replaced with the event metadata when triggered.
Note: Select the available tokens in the drop-down menu below the message window.

- **Tamper:** Enter a custom message for the HTTP notification when linked to the camera tamper. You can include tokens from the list available. Token values will be replaced with the event metadata when triggered.
Note: Select the available tokens in the drop-down menu below the message window.
- **Enable URL encoding:** Select whether to use URL encoding for the notification.
- Select 'Apply' to save your changes.

Note: See the tokens page for a complete list of the token system and example templates.

Tamper

The Tamper feature detects camera tampering events such as bagging, defocus and general camera movement. This is achieved by detecting significant persistent changes in the pixels in the image.



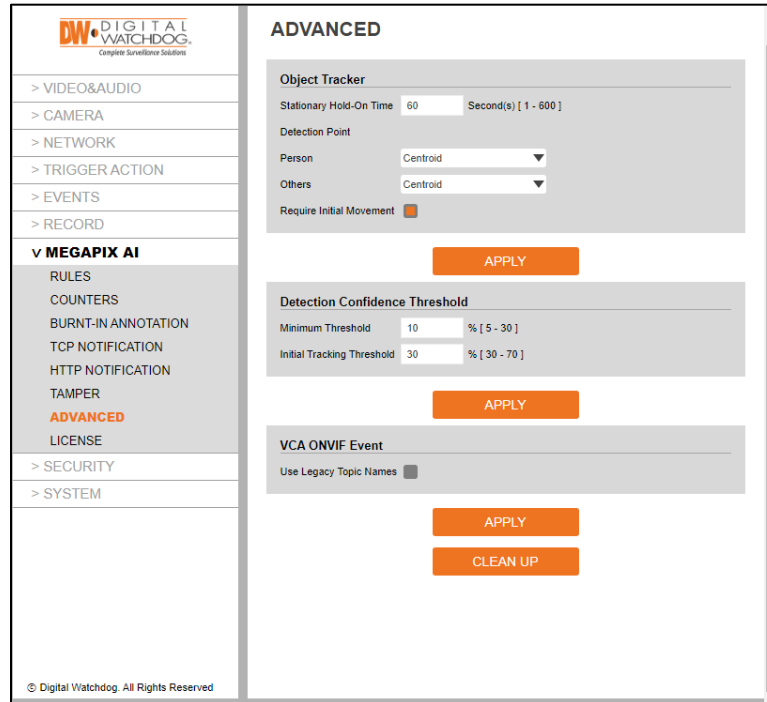
1. **Tamper Detection:**
 - a. **Enable:** Choose to turn the tamper detection feature on or off.
 - b. **Duration:** Set the duration (in seconds) the image must be changed before triggering the alarm.
 - c. **Area Threshold:** Set, as a percentage, the area of the image that must change before triggering the alarm.
 - d. **Suppress Alarm on Light:** Compensates for scenarios where sudden changes in light (such as lights being switched on/off) can cause false tamper events.
Note: The option will reduce sensitivity to genuine alarms and should be used cautiously.
2. **Event Actions:** Define the action to occur when an event is triggered. Any combination of the available options is possible.
 1. TCP Event: Enable/disable TCP notification when an event occurs.
 2. HTTP Event: Enable/disable HTTP notification when an event occurs.
Note: TCP/HTTP notification actions must be configured separately under the left navigation bar.
3. Select 'Apply' to save all changes.

Advanced

The advanced menu includes settings relating to how the analytics engine tracks objects.

Note: In most installations, the default configuration will apply.

Note: Supported settings are different depending on the tracker engine.



1. **Stationary Hold-on Time:** Defines how long an object will continue to be tracked and classified once it becomes stationary.
2. **Detection Point:** Defines the tracking point that will be used to evaluate objects against rules.
3. **Person:**
 - a. **Centroid:** The detection point for each person is located in the middle of the bounding box.
 - b. **Mid-bottom:** The detection point for each person is located along the bottom line of the bounding box in the center.
4. **Others:**
 - a. **Centroid:** The detection point for each object is located in the middle of the bounding box.
 - b. **Mid-bottom:** The detection point for each object is located along the bottom line of the bounding box in the center.
 - c. **Detection Confidence Threshold**
5. **Minimum threshold:** Defines the confidence (as a percentage) required to start tracking the object.
6. **Initial Tracking Threshold:** Defines the tracking (as a percentage) required to trigger an event.
7. Click **Apply** to save the current settings.
8. Click **Clean up** to perform a clean-up process.



License

A license is required to take advantage of the MEGApix Ai video analytic features. DW's MEGApix Ai cameras come with the Ai license preloaded and activated at no extra cost.

In some cases, activation may be necessary to enable additional functionality.

An **activation code** is linked to the camera's hardware configuration and is not transferable.

To manage activation codes, navigate to the license menu from the MEGApix Ai setup category.

Activate License

Activation Type: Defines the method that will be used for your activation request.

- **Token:** Allows the activation token to be entered to apply for further licenses.
- **Pre-activation:** Defines that software has been pre-licensed and no further action is required.
- **Activation code:** Provides the HW GUID to apply for further licenses.
 - **HW GUID:** The unique hardware code for this device. This is required to generate an activation code.
 - **Activation code:** This is where you enter activation codes to apply for licenses and enable features of the MEGApix Ai plug-in.
Note: Please refer to your license distributor for additional licenses.

Activated License(s)

This provides a list of the installed licenses with the option of deleting highlighted licenses.

Note: Multiple licenses can be applied to a camera, but only one can be active at a given time.

Assign

Assign the selected license for use with analytics.



Note: The system will reload to reflect any changes the license has applied. This may result in features not being available.

How to apply a Token

- Request an activation token from your DW distributor.
If needed, send your DW distributor your camera's **HWCODE**.
- Click **Assign** and type or paste the activation token. Select **Activate**.
- Verify the license has been applied by confirming it is valid in the activated license(s) section.

How to Delete License(s)

- Highlight the license you would like to delete.
- Select **Delete** and confirm the action to delete the license.

Note: deleting the active license from the camera will remove all analytic features. Any configured rules will be available when a new valid license is applied.



Tokens

Tokens are used with event actions such as TCP and HTTP notifications. They are automatically filled in with the metadata for the event. This allows the event's details to be specified in the message, such as the location of the object, type of event, etc.

List of tokens: Below is a list of the available tokens and a description of the data they provide.

{{name}} – The name of the event.

{{id}} – The unique ID of the event.

{{type}} – The type of event. This is usually the type of rule that triggered the event.

{{status}} – The status of the event.

{{iso8601}} – The event time in ISO 8601 format. For example:

Start time (ISO 8601 format): {{iso8601}} Start time (ISO 8601 format): 2017-04-21T10:09:42+00:00

{{time}} – The event time in Unix timestamp format. For example: time: {{time}} time: 1582308244.376

{{ip}} – The IP address of the device.

{{host}} – The hostname of the device.

{{datetime}} – The event time in the format DD MM D HH:MM:SS YYYY 'Tue Jan 1 12:00:00 2019'. for example: time: {{datetime}} time: Tue Jan 1 12:00:00 2019

{{zoneid}} – The zone ID of the event.

{{ruleid}} – The rule ID of the event.

{{bb}} – The bounding box of the object.

{{objectclass}} – The object class of the object triggering the rule.

{{mac}} – The MAC address of the device.

An example of using multiple tokens for notifications:

Event #{{id}}: {{name}} Event Actions: {{type}} Start time (ISO 8601 format): {{iso8601}} time: {{time}}
Device: {{host}}: {{ip}}: {{mac}} Object bounding box: {{bb}} Classification: {{objclass}}

This would produce the following text:

Event #350: My event name Event Actions: presence Start time (ISO 8601 format): 2017-04-21T10:09:42+00:00
time: 1492769382 Device: Camera: 10.0.5.2: AB:CD:EF:GH:01:02 Object bounding box:
[45251:12069:14004:8563] Classification: Vehicle