

Oncam C-SERIES

Installation and User Manual



C-SERIES OUTDOOR

C-SERIES INDOOR

INSTRUCTION MANUAL - C-SERIES - 006-0064-0538 - Rev 7

Contents

1. Legal and Warnings.....	3
1.1 Legal Considerations.....	3
2. Introduction.....	9
3. Camera Installation	10
3.1 Camera Configuration & Pre-Configuration.....	10
3.2 Placement and Orientation	10
3.3 Connection	12
3.4 Indoor Camera.....	12
3.5 Outdoor Plus Camera.....	36
3.6 SD Card Support.....	75
3.7 Uninstalling and Returns.....	76
4. Camera Access.....	79
4.1 First Time Access - Discovery.....	79
4.2 First Time Access - Set Primary Administrator Username and Password	81
5. Camera Configuration	86
5.1 Dashboard – Camera Web Interface	86
5.2 Network	89
5.3 Video/Audio Streaming	95
5.4 Recording.....	152
5.5 Events.....	161
5.6 Motion / Analytics.....	172
5.7 Users.....	183
5.8 Device.....	187
5.9 Peripherals.....	209
6. Technical Support	216
Appendix A	217
Appendix B.....	218
Appendix C.....	223

1. Legal and Warnings



Read through the Quick Start Guide carefully before installing the product. Keep this guide for future reference. If you need further support during installation, please visit:

<https://www.oncamgrandeye.com/>

This camera should be installed by a qualified service personnel and the installation should conform to local and national regulations.

1.1 Legal Considerations

The use of video surveillance may be regulated by local laws that vary from country to country. Please check the laws in your local region before using this product for surveillance purposes.

1.1.1 Intellectual Property Rights

Oncam has intellectual property rights relating to the technology embodied in the product described in this document. These intellectual property rights may include one or more of the Oncam patents or pending patent applications in the US and other countries. This product contains licensed third-party software. See the menu item “Attributions” in the product’s user interface for more details.

1.1.2 Product Modifications

This product must be installed and used in accordance with the instructions provided in the user documentation. Any modifications will invalidate all applicable product warranties, regulatory certifications and approvals. Please note this product does not contain any parts which are user serviceable.

1.1.3 Liability Notice

Every care has been taken in the preparation of this and the accompanying installation documentation.

©Oncam Global Group AG, 2013 - 2020. All rights reserved. No part of this manual may be reproduced except for your express personal use. Oncam and their affiliate’s further reserve the right to alter, amend or revise this document and any product specifications without any obligation to provide notice of such changes. Oncam and its affiliates make no guarantee, representation, or warranty, either expressed or implied, regarding the accuracy of the information contained in this manual. Furthermore, Oncam and its affiliates assume no responsibility or any potential liability for any errors that may appear in this manual.

For product and service liabilities please refer to our standard terms and conditions.

<https://www.oncamgrandeye.com/terms-and-conditions/>

1.1.4 Trademarks and Third-Party Trademarks

“ONCAM” and the “ONCAM logo” are trademarks, and in some cases registered or protected trademarks, of Oncam Global Limited and/or Oncam Global, Inc. (subsidiary companies to Oncam Global Group AG), including under registration in the UK, India and in the U.S. Patent and Trademark Office, and also protected in the following countries through designations under an International Registration: Australia, China, the EU, Philippines, Singapore and Switzerland. The names of other companies, organizations, products or services mentioned in this manual are the trademarks of their respective owners.

1.1.5 Copyright

© Copyright 2020 ONVU Technologies AG. All rights reserved. Oncam is a trading name of ONVU Technologies AG.

1.1.6 Regulatory Information

1.1.6.1 Europe



This product complies with the applicable CE marking directives and harmonized standards:

- Electromagnetic Compatibility (EMC) Directive 2014/30/EU.
- Restrictions of Hazardous Substances (RoHS) Directive (EU) 2015/863, amending Annex II to Directive 2011/65/EU.

1.1.6.2 Electromagnetic Compatibility (EMC)

This equipment has been designed and tested to applicable standards for:

- Radio frequency emission when installed according to the instructions and used in its intended environment.
- Immunity to electrical and electromagnetic phenomena when installed according to the instructions and used in its intended environment.
- This digital equipment fulfils the requirements for RF emission according to the Class B limit of EN 55032. The product shall be connected using a shielded network cable (STP) that is properly grounded.

1.1.6.3 USA

This device complies with part 15 of the FCC Rules. Operation is 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 to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC rules.

These limits provide adequate protection against harmful interference when the equipment is operated in a commercial environment. This equipment creates, uses, and can radiate radio frequency energy and therefore if not installed and used as directed in the documentation, may cause harmful interference to radio communications.

1.1.6.4 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.

1.1.6.5 Australia / New Zealand

This digital equipment fulfils the requirements for RF emission according to the Class B limit of AS/NZS CISPR 32. The product shall be connected using a shielded network cable (STP) that is properly grounded.

1.1.7 Product Safety

This product complies with IEC/EN/UL 62368-1, safety of audio/video and IT equipment, and IEC/EN/UL 60950-22, Safety of Information Technology Equipment. The product shall be grounded either through a shielded network cable (STP) or other appropriate method. When used with Power over Ethernet (PoE), the Power Sourcing Equipment (PSE) shall comply with IEEE 802.3af and Limited Power Source (LPS) according to clause 2.5 of IEC/EN/UL 60950-1 or annex Q of IEC/EN/UL 62368-1.

1.1.8 Disposal and Recycling

When this product has reached the end of its useful life, dispose of it according to local laws and regulations.

Europe



This symbol means that the product shall not be disposed of together with household or commercial waste. Directive 2012/19/EU on waste electrical and electronic equipment (WEEE) is applicable in the European Union member states. To prevent potential harm to human health and the environment, the product must be disposed of in an approved and environmentally safe recycling process. For information about your nearest designated collection point, contact your local authority responsible for waste disposal. Businesses should contact the product supplier for information about how to dispose of this product correctly.

This product complies with the requirements of Directive (EU) 2015/863 on the restriction of the use of certain hazardous substances in electrical and electronic equipment (RoHS).

1.1.9 Contact Information

For our contact details please go to: <https://www.oncamgrandeye.com/contact-us/>

1.1.10 Warranty Information

All Oncam camera products are covered by a 3-year limited manufacturer's warranty. It is required to speak to a local technical support representative before initiating a product return. In many cases, issues can be resolved over the phone or via remote diagnostic tools.

1.1.11 Support

If you require any technical assistance, please contact your Oncam 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 go to:

<https://support.oncamgrandeye.com/>

Here you can:

- Download user documentation and software updates.
- Find answers to resolved problems in the FAQ database, search by product, category, or phrase.

To contact us via email, please use support@oncamgrandeye.com.

Include the following in your email:

- A detailed description of the problem

- Camera model numbers
- Relevant configuration information

1.1.12 Open Ports

For reference, the camera has the following open port pre-configuration.

Port	Service
TCP - 554	RTSP Server
TCP – 80	HTTP Server
TCP - 443	HTTP Server
UDP – 3702	Web Service Dynamic Discovery (Multicast)
UDP – 12345 UDP - 12346	Oncam Probe

Table 1 Port Pre - Configuration

1.1.13 Safety Information

1.1.13.1 Hazard Levels



CAUTION

Indicates a hazardous situation which, if not avoided, could result in minor or moderate injury or property damage.



RISK OF EXPLOSION

If components are replaced incorrectly.



SHARP

Indicates cautionary warning of sharp edge or object.

1.1.13.2 Iconography



Note: Indicates important information.



Tip: Recommendation or time saving idea.

1.1.14 Important Safety Instructions

1.1.14.1 Installation

- Heed all warnings.
- Follow all instructions.
- Do not immerse in water. Protect the connectors from moisture.
- Do not block any ventilation openings, install in accordance with the manufacturer's instructions.
- Do not install near any heat sources such as radiators, heat registers, stoves or other.
- Avoid exposing the product to shocks or heavy pressure.
- Please ensure you have the correct mounting accessories and fittings before proceeding with your installation.
- Only use attachments / accessories specified by the manufacturer.
- Do not install the product on unstable poles, brackets, surfaces, or walls.
- Use only applicable tools when installing the product. Using excessive force with power tools could cause damage to the product.
- Incorrect installation can compromise the IP rating, follow user guide for correct installation.
- Safe handling required during installation of external input/output devices, audio, and DC power supply to the Plus board on the camera, follow user manual instructions.
- The polarity of any connector attached to the product should be verified before connection.
- Protect all cables from being crushed or pinched particularly at plugs, convenience receptacles, and the point where they exit from the apparatus.
- Direct DC Input. Use only a UL/CSA-approved LPS or NEC Class 8-28 VDC, 15W LPS, power supply (not supplied). The power source must be connected with the correct polarity.



Do not use an excess of 28 VDC from an external power supply. Doing so may damage the camera and void the warranty.

1.1.14.2 Storage

Store the product in a dry and ventilated environment.

1.1.14.3 Transportation

When transporting one of our products, use the original packaging or equivalent to prevent damage to the product.

1.1.14.4 Maintenance

- This product may get hot during operation. Please allow to cool down before handling the camera module.
- Do not attempt to repair the product yourself.
- Unplug or appropriately protect this apparatus during lighting storms or when unused for long periods of time.
- Refer all servicing to qualified service personnel. Servicing is required when the apparatus has been damaged in any way, such as power-supply cord or plug is damaged, liquid has been spilled or objects have fallen into the apparatus, the apparatus has been exposed to rain or moisture, does not operate normally, or has been dropped.
- Use only spare parts provided by or recommended by Oncam.



Risk of Explosion if replacing a battery with an incorrect battery type. Battery not user replaceable.

1.1.14.5 Dome Maintenance

- Be careful not to scratch, damage or leave fingerprints on the dome cover because this could decrease image quality. If possible, keep the protective plastic on the dome cover until the installation is complete.
- Care to be taken with camera dome and lens, during camera installation and routine maintenance, particularly when attaching the camera front enclosure to rear enclosure using the lanyard.

1.1.14.6 Dome Handling and Cleaning

- The standard dome is made of a polycarbonate (PC) polymer. Take care when handling or cleaning the dome to avoid scratching the surface.
- Always handle the dome by the outside edge of the flange or trim ring assembly.
- Avoid contacting inside surface of the dome.
- Remove dust or other surface contaminants from the dome's interior with clean, dry air pressure (compressed air cans).
- Remove heavy residue (spots, streaks, stains) or other contaminants from the dome surface with a solution of isopropyl alcohol and water.
- Only use lint free soft paper towels or a microfiber cloth. After cleaning the dome apply clean, dry air to complete drying and leave no dust.

2. Introduction

The Oncam C-Series are the most powerful compact cameras from Oncam. Capable of streaming at High Frame Rates, the 12MP C-12 camera streams 55 fps at full resolution, significantly outperforming other 360-degree cameras in the market today, whilst the C-08, 8MP camera can achieve 60fps at full resolution. This performance capability enables you to maintain your chosen frame rate up to 30 fps on the primary stream even with up to 3 other streams running. Users can now experience the benefits of full frame rate video without sacrificing the flexibility for secondary streams.

The benefits of a high performance, powerful camera can only be achieved when users are equipped with the right tools to harness them and this is where the C-Series really comes into its own. Thanks to a wide range of onboard technologies developed by the Oncam team, combined with an intuitive user interface and seamless ONVIF implementation, users have the freedom to configure and tailor the camera to best serve their installation environment.

For example, via ONVIF commands from a VMS or the attractive Camera Web Interface, the user has quick and easy access to Camera Modes, media streaming profiles, StreamLite compression, TrueDetail HDR and Advanced Light Management settings. This ensures the delivered stream has the desired image quality level, resolution, frame rate and bandwidth.

The Oncam Camera Configuration Tool uses the same sleek user interface and enables advanced management of the C-Series cameras, enabling you to discover, update, configure and control single or multiple cameras simultaneously with ease, saving time and resource.

In this guide we will take you through how to install, set up and get the most out of the C-Series Camera.

The camera can be configured using a compatible ONVIF-conformant VMS within ONVIF profile settings, or via the Camera's built in ONVIF based Web Interface and Camera Configuration Tool. In this guide we will primarily reference the Camera Web Interface and Camera Configuration Tool controls. Any changes made using the Web Interface and Configuration Tool will be reflected in the compatible VMS and vice versa.



The features and functionality in this guide are based on V2.0.x firmware and above. If you are using a firmware prior to this release, not all functionality described in this guide will be available. The Camera Web Interface images referenced in this guide are also taken from V2.0.x firmware.

C-08 Camera is only supported from Version 2.1.5 Firmware onwards, this is a common firmware for the C-Series and therefore supports the C-12 and C-08.

3. Camera Installation

3.1 Camera Configuration & Pre-Configuration

For access to full configuration functionality, it is recommended to install the camera module in the correct final housing (Indoor or outdoor) prior to configuring the camera.



V2.0.x firmware or above required to access this feature.

From Firmware V2.0.6 onwards several key features can be pre-configured on the camera module prior to being placed in the final housing, these are:

- User Settings - User Credentials (e.g., Username and Password)
- Network Settings and Network configuration (e.g., Static IP)
- Device maintenance settings (e.g., Date and Time)
- SD card Recording configurations.
- Motion / Analytics (e.g., created rules)
- Image settings
- Camera mode preferences
 - o Image output (e.g., Fisheye only, Panoramic+ only, Multi-Mode)
 - o Performance (e.g., High Speed or Multiple streaming)
- OSD/masks saved by Image output mode – (e.g., Fisheye, Panoramic+ and Multi-Mode).

The following settings need to be configured when the camera module is in the correct final housing:

- Media profiles
- Metadata settings
- Events

The Camera module will need to be in outdoor housing for Plus feature recognition and configuration of the following settings:

- Actions/ Triggers
- H/W Input / Output
- Audio



For settings that require the camera to be in the correct housing, once a camera is configured the configuration can be saved and applied to other similar type cameras (Indoor or outdoor) simultaneously using the Camera Configuration Tool. Please see C-Series Camera Configuration Tool User manual section 8.

<https://www.oncamgrandeye.com/resources/c-series-camera-config-tool/>

3.2 Placement and Orientation

Camera placement is an important factor when planning your deployment. The Oncam C-Series camera has an exceptionally wide viewing angle. Consider the camera location for providing

comprehensive coverage of a wide area. Mount the camera with an unobstructed view and consider scene optimization when one portion of the scene is bright and another dark. The camera supports three different mounting orientations, Ceiling, Wall and Table.



Each of these mounting options require correct orientation settings selected from the Camera Web Interface. These camera settings ensure the use of correct dewarping algorithm when connecting to a compatible VMS or NVR system. To set the correct option via the Camera Web Interface go to: **Video/Audio > Image Settings > Camera Mount Position**.

3.2.1 Ceiling Mount

Ceiling mounting is preferred when most of the action is occurring below the camera in a horizontal plane. When a person is directly below the camera, captured is the top-of head view. When the person moves away from the camera, more of their face and body becomes visible. Hats extend that top-of-head zone to some degree. Consider the viewing angle when requiring people identification or recognition.

Depending on the use case, use a single camera to cover a small to medium sized space. Mounting a camera high gives great situational awareness throughout a large space. When planning coverage ensure there are no obstructions. Examples of obstructions include pillars, high-sided furniture, and any hanging objects near the camera such as signage.

3.2.2 Wall Mount

Wall mounting the camera can give a complete 180-degree side on view of an area. Use this view where ceiling mounting is not possible or if you need to capture a higher level of detail for objects closer to the camera (such as people's faces as they walk past the camera).

3.2.3 Table Mount

Mount the Table Mount camera on a flat surface looking up. While this mount is for demonstration or testing purposes, you could use this mount in a system. Use the Table Mount for inspecting systems or viewing under vehicles.

3.2.4 Coverage Area

The Oncam C-Series cameras provide coverage for open areas where situational awareness of people and objects are required. The higher camera placement provides a larger coverage area. However, with higher camera placement a reduction in the pixel density is expected. Height impacts the image quality; therefore, ensure you consider image quality versus the mounting height.

Perform tests to ensure that the camera meets the system operational requirements, and the required detail level is available.



Use a minimum height of 2 m (6.5 ft.) when ceiling mounting a camera for best results. For multiple camera layouts, ensure the camera areas overlap for full coverage.

3.2.5 Lighting

Avoid bright light sources pointing towards the camera lens. Always face lighting away from the camera or above the camera installation line (if ceiling mounted).

For low light conditions consider adjusting the Exposure Priority in the camera from the Web Interface. By default, this is set to **Low Noise** which optimizes the image by increasing exposure time in lower light levels. It's important to note that the maximum frame rate is reduced as exposure time increases. The image remains in full color until below one Lux, after which it transitions to black and white for better contrast. Exposure priority is accessible from the Camera Web Interface; **Video/Audio > Image Settings > Exposure Priority**.

Consider where the sun might rise and set, this may interfere with the image over time.

3.3 Connection

3.3.1 Power requirements

The Indoor C-Series is powered by Power over Ethernet (PoE). Connect power and data using an Ethernet cable plugged into the camera Ethernet port. The PoE supply equipment must be compliant with IEEE 802.3AF.

The C-Series Outdoor Plus can be powered in two ways using either Power over Ethernet (PoE) or Direct DC Input.

For PoE, connect power and data using an Ethernet cable plugged into the camera Ethernet port. The PoE supply equipment must be compliant with IEEE 802.3AF.

For direct DC Input use only a UL/CSA-approved LPS or NEC Class 8-28 VDC, 15W LPS, power supply (not supplied). The power source must be connected with the correct polarity. Do not use an excess of 28 VDC from an external power supply. Doing so may damage the camera and void the warranty.

3.3.2 RJ45 and Punch Down

For increased flexibility during camera installation, two methods of connection to the Oncam C-Series camera are available - RJ45 and Punch Down (or IDC).

As part of the installation, if a network installer is bringing ethernet to every camera position then you can plug the cable straight into the camera. If you are running your own infrastructure and are terminating the cable, then you can either use punch down or add RJ45 connector on the end.

3.4 Indoor Camera

3.4.1 Surface Mounting

Using a spirit level to make sure it is straight, affix the drilling template to the wall by removing the self-adhesive backing.



If you are concerned about the adhesive on a delicate surface, put the drilling template on work trousers or other cloth to make it less sticky.

Identify if you are going to install using the punch down or RJ45 connector, using a bradawl or sharp point mark the two holes for the screws and the one hole for the ethernet cable.

Remove the drilling template carefully from the wall.

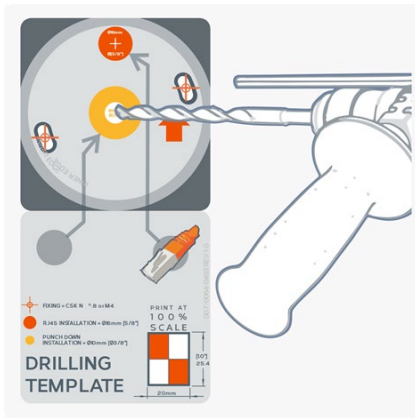
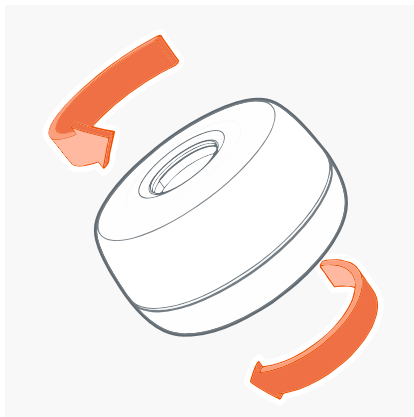


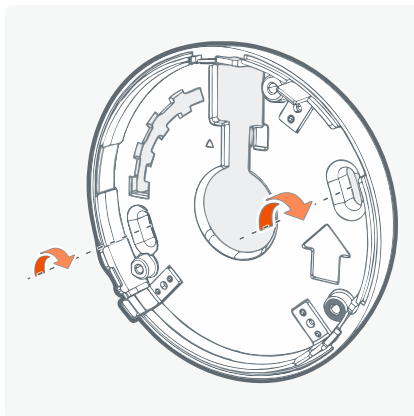
Figure 1 Drilling Template

Using the appropriate size of drill bit, drill the mounting holes and the hole for the ethernet cable.



Open camera enclosure.

Figure 2 Opening of Camera Enclosure



Mount the rear of the camera enclosure to the wall with the screws (not provided with the product).

Figure 3 Mounting of Camera Enclosure



The camera has been designed to be mounted with #8 or 4mm countersunk screws, however the length and fixing support material (plugs etc.) need to be specified by the installer on a case by case basis.

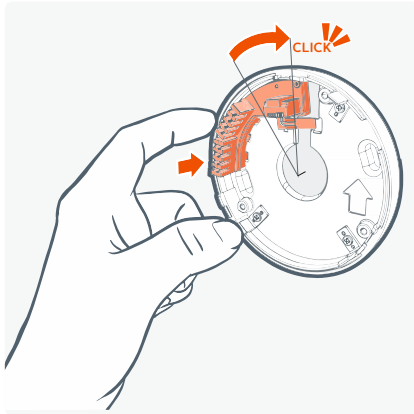


Figure 4 Punch down Adapter

If you prefer to use the punch down, you need to add the punch down adapter here (accessory located in the box packaging). Following the guide, punch down the ethernet cable.

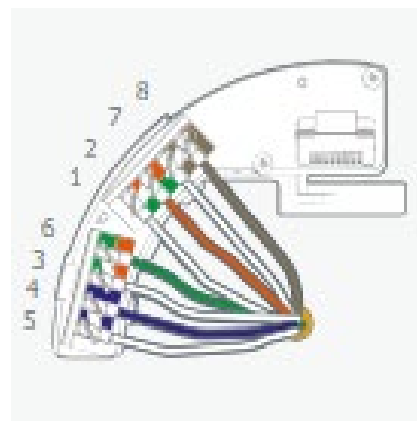
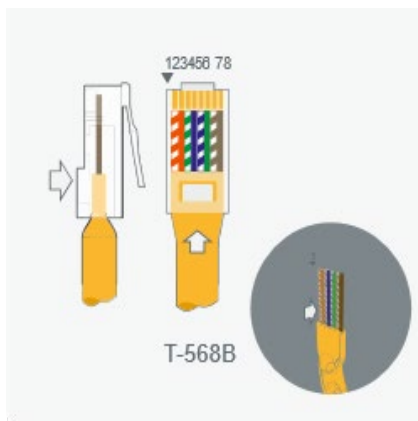
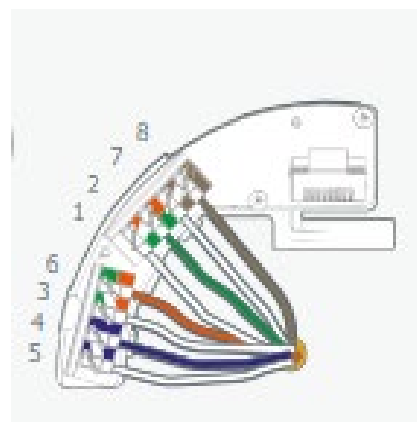
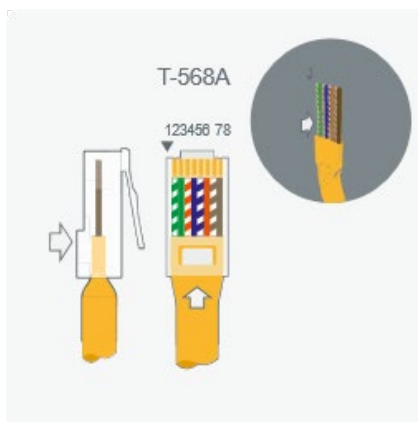


Figure 5 Identify Wiring Type for Punch Down



Strip sheath to approximately 7cm [2 3/4"]. So, you have enough wires to punch down, excess wire can be cut after punching down.

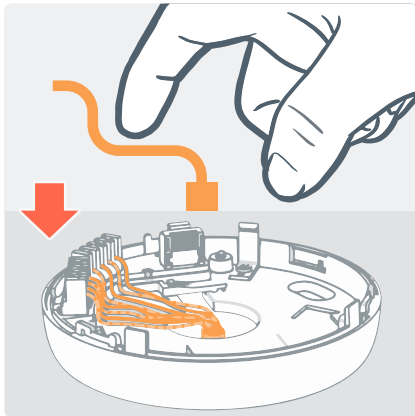


Figure 6 Punch Down Wires

If using punch down press the wires down to ensure they do not obstruct the camera module.



After wires are punched down, cut off any excess wires.



Figure 7 Protective Cover Removal

Remove and recycle the protective cover from the rear of the camera module.

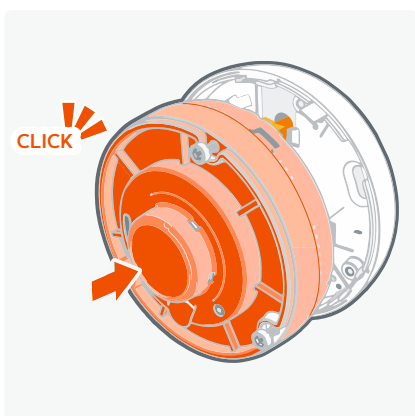


Figure 8 Connecting of Camera Module

Connect the camera module, the clips will hold the camera in place.

For RJ45 simply plug the camera module in, for the punch down simply connect the camera.

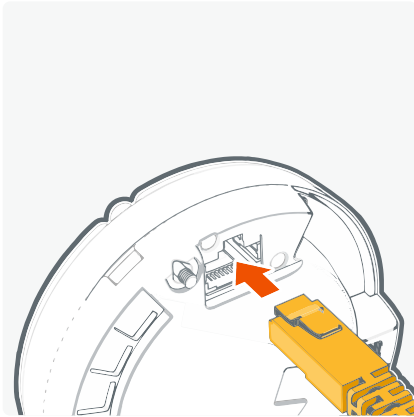
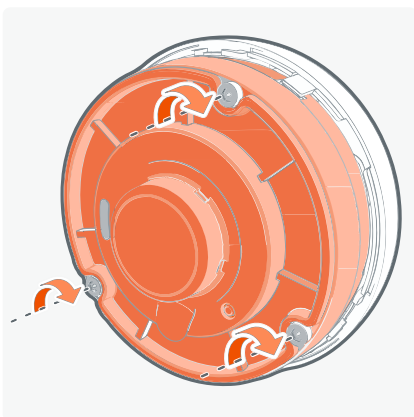
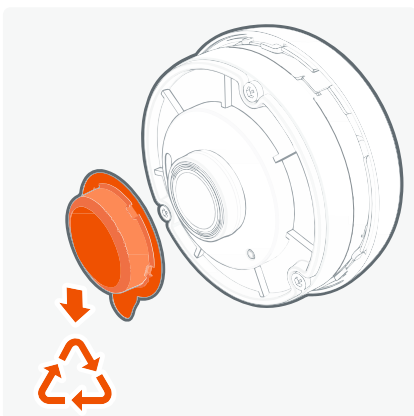


Figure 9 Connecting of Ethernet Cable



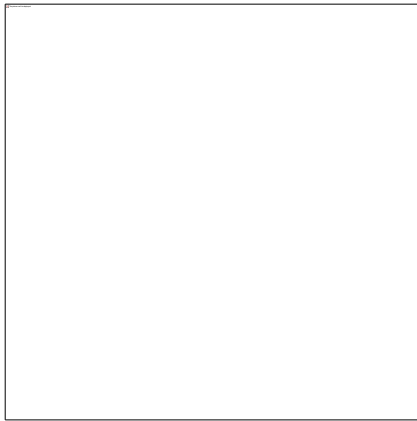
Using the security hex tool, tighten the 3 captive screws.

Figure 10 Securing the Camera Module



Remove and recycle the protective lens cover.

Figure 11 Protective Lens Cover Removal



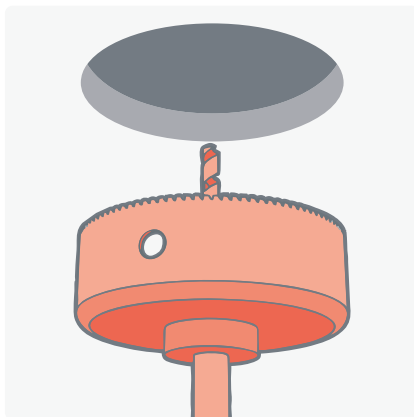
Using the alignment feature as a guide, push on the cover twist to lock in place.

Figure 12 Cover Twist

3.4.2 Recessed Mounting

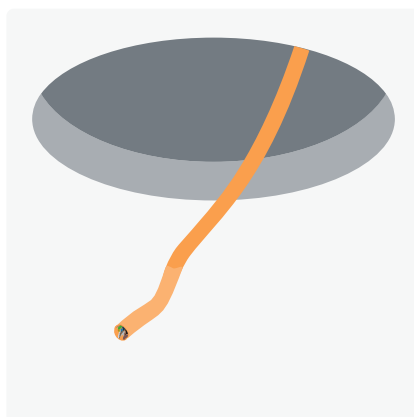
This camera is designed to work with sheet material such as plasterboard. There is no minimum sheet thickness, only it requires flat material, however the spring retaining strength will be weaker the thinner the material is.

The springs will retain the camera material up to a maximum 25mm [1"] thick.



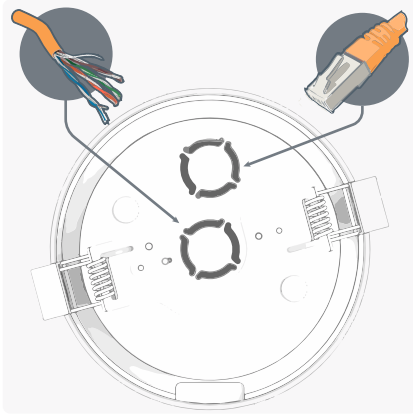
After selecting a suitable position, drill a $\varnothing 100\text{mm}$ ($\varnothing 4''$) hole.

Figure 13 Drilling Hole



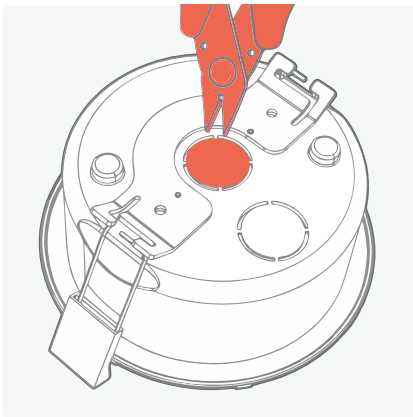
Feed a suitable ethernet cable to the hole.

Figure 14 Feeding Ethernet cable to the hole



Identify which type of connection you want to use; RJ45 or punch down, remove the outer plug for RJ45 and the center plug for punch down.

Figure 15 Connecting of RJ45 / Punch down



Using wire cutters carefully snip two of the support tabs.

Figure 16 Snipping of Support tabs for Punch down

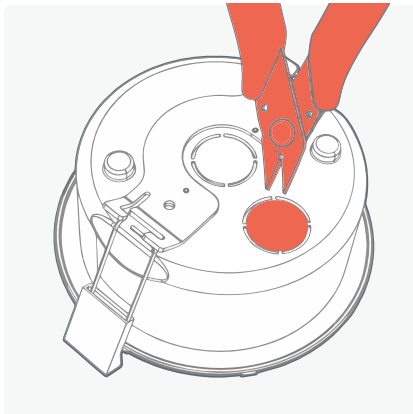


Figure 17 Snipping of Support tab for Ethernet Cable



Sharp Edges

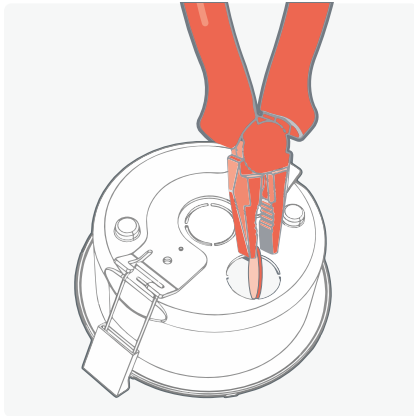


Figure 18 Removal of Plug using Pliers

Use pliers to twist and remove the plug.



Sharp Edges

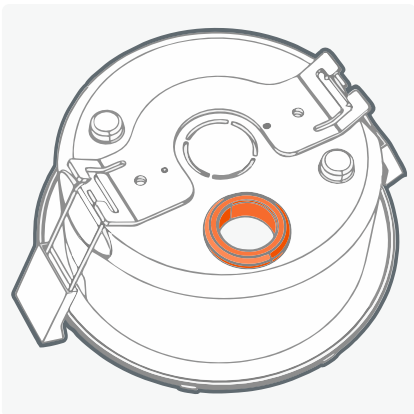


Figure 19 Inserting of Grommet

Being careful; watching for sharp edges insert the grommet to protect the wire and to make cut edges safe.

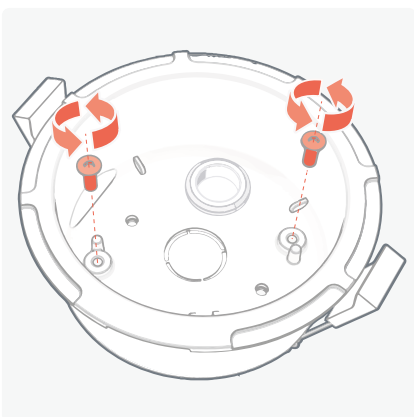
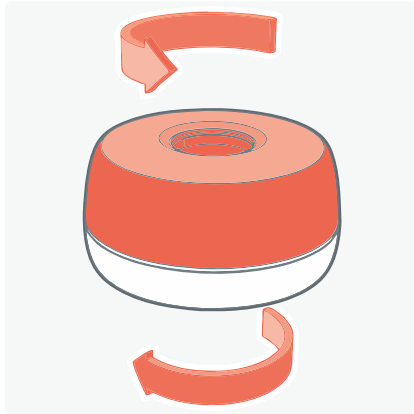


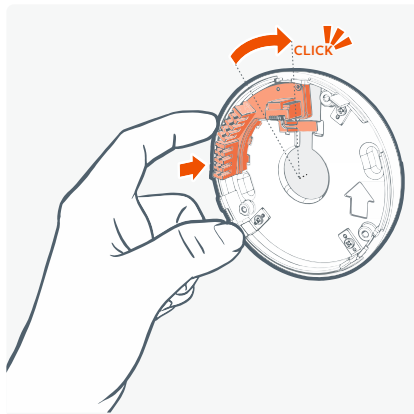
Figure 20 Mount Screws Removal

Remove the two mount screws, put to one side. These will be used later to mount the rear camera enclosure.



Open the indoor enclosure, dispose of and recycle the plastic front cover.

Figure 21 Indoor Enclosure Opening



Punch down only: insert the punch down adaptor (accessory located in the box packaging) and punch down the ethernet cable using the guide.

Figure 22 Inserting Punch down adaptor



Figure 23 Punch down Ethernet cable

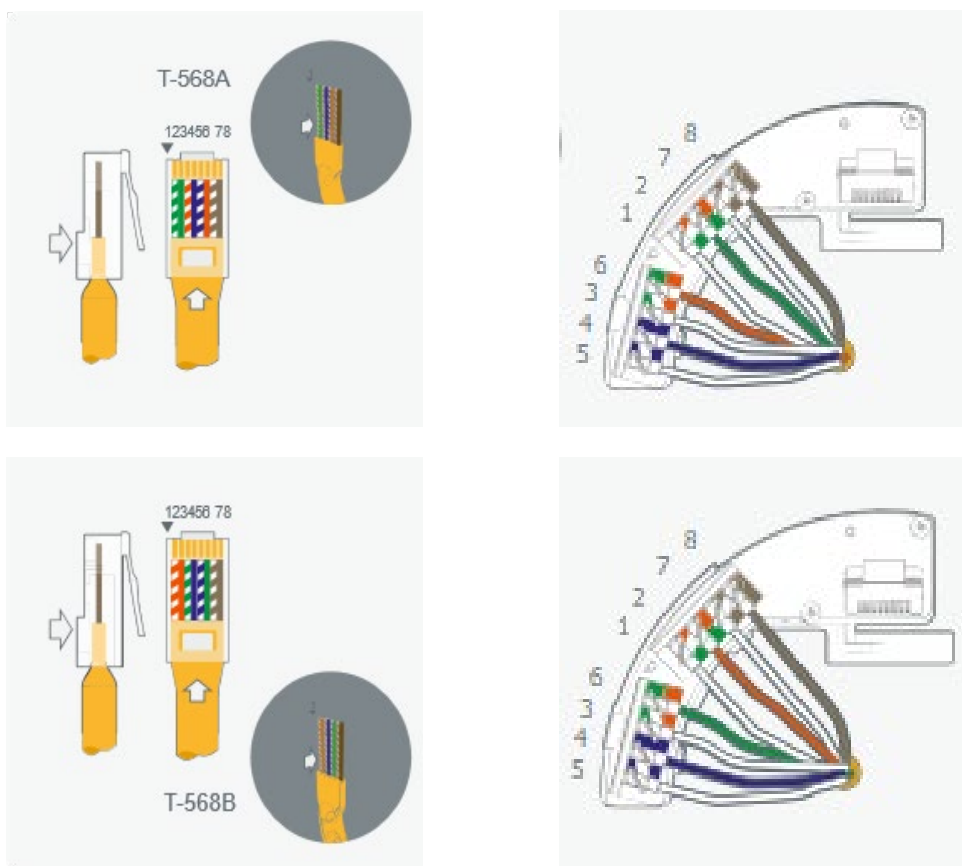


Figure 24 Identify Wiring Type for Punch Down



Strip sheath to approximately 7cm [2 3/4"]. So, you have enough wires to punch down, excess wire can be cut after punching down.

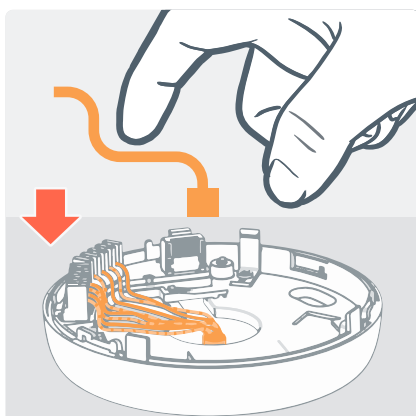
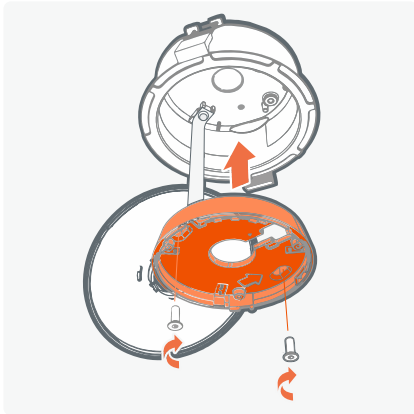


Figure 25 Punch Down Wires

If using punch down press the wires down to ensure they do not obstruct the camera module.



After wires are punched down, cut off any excess wires.



Insert the rear of the enclosure into the recessed mount and screw it down with the two mount screws removed earlier.

Figure 26 Inserting Rear Enclosure into Recessed Mount



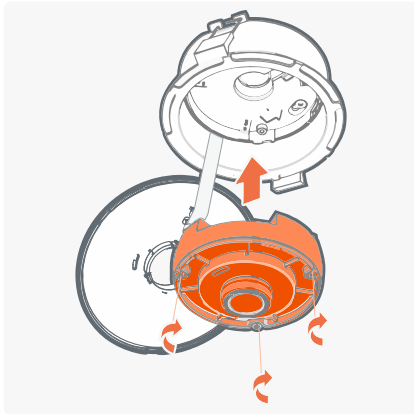
Remove and recycle the protective cover from the rear of the camera module.

Figure 27 Protective Cover Removal



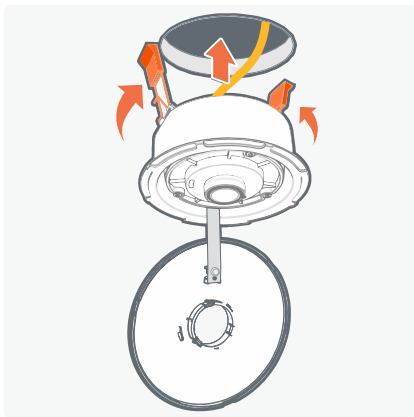
RJ45 Only. If the RJ45 cable is to be used, plug it in now.

Figure 28 Plug in RJ45 Cable



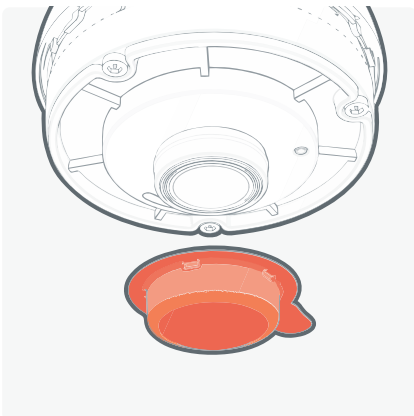
Plug the camera module into the recessed enclosure, tighten the 3 captive security screws to hold it in place. There are arrows that aid alignment.

Figure 29 Plugin of Camera Module into the Recessed Enclosure



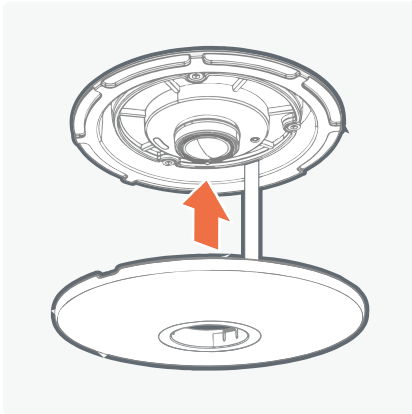
Taking the two retaining springs in each hand open them backwards and gently push into the hole drilled earlier. This will then pull the recessed enclosure into the hole. The camera can be aligned for the correct view if required.

Figure 30 Securing of Recessed Enclosure into the Ceiling



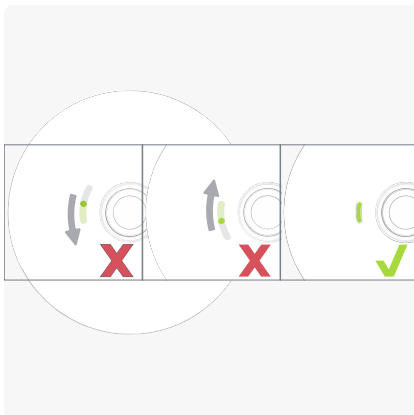
Remove and recycle the protective lens cover.

Figure 31 Protective Lens Cover Removal



Clip the front cover onto the camera module lens surround, make sure the tether is folded in out of the way.

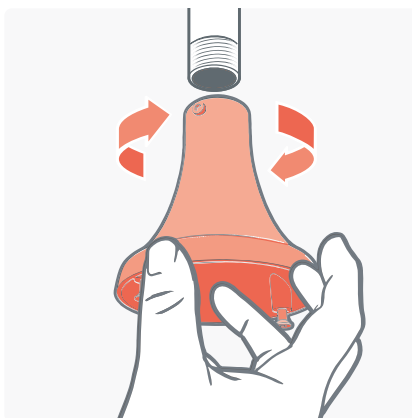
Figure 32 Clipping of Front Cover



Align the slot with the Status LED for the best view.

Figure 33 Slot Alignment with LED

3.4.3 Pendant Mounting



Run a drop conduit using external (male) thread M20 or 3/4" NPT conduit. The pendant mount will screw directly onto the conduit.

Figure 34 Pendant Mount



The two thread sizes use the same hole.



If you have not done, run the ethernet cable through the conduit and through the pendant mount.

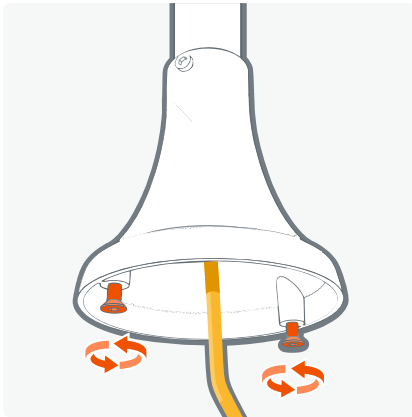


Figure 35 Mounting Screws Removal

Remove and retain the two mounting screws. These will be used later to mount the rear camera enclosure.



Figure 36 Opening of Camera Enclosure

Open the camera enclosure.

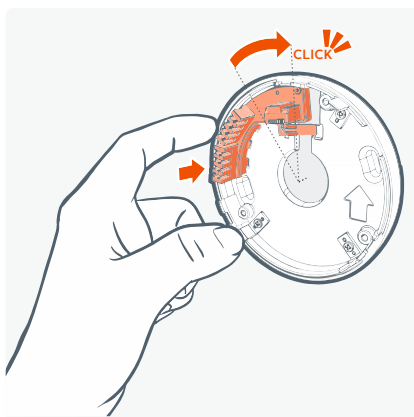


Figure 37 Punch Down Adaptor

Punch down only: insert the punch down adaptor (accessory located in the box packaging).



Punch down the ethernet cable using the guide.

Figure 38 Punch Down Ethernet Cable

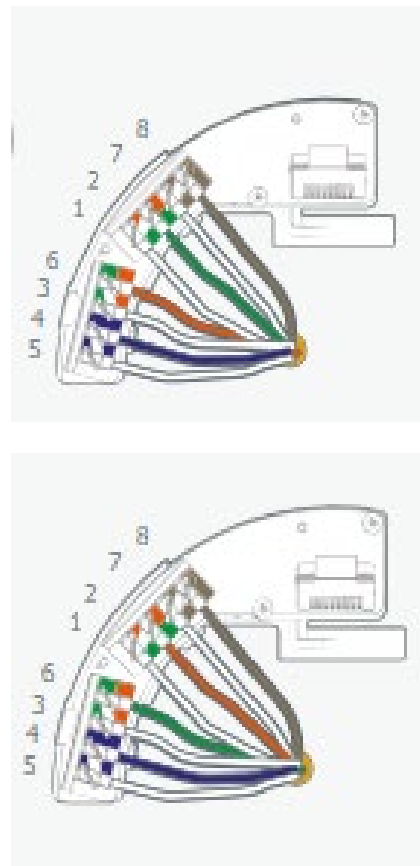
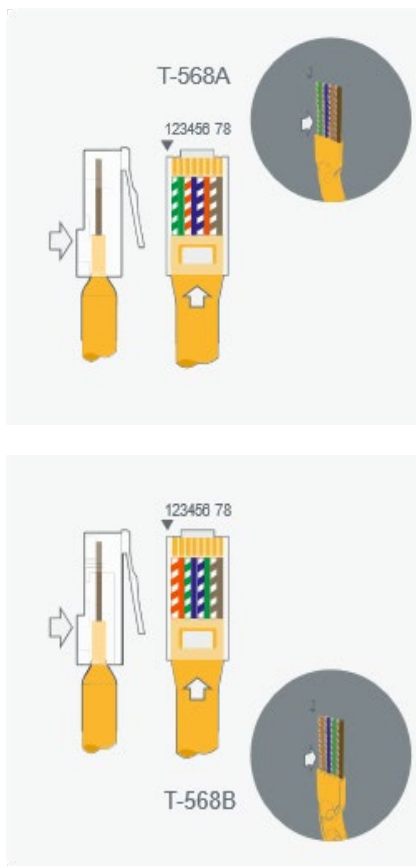


Figure 39 Identify Wiring Type for Punch Down



Strip sheath to approximately 7cm [2 3/4"] so you have enough wires to punch down. Excess wire can be trimmed after punching down.

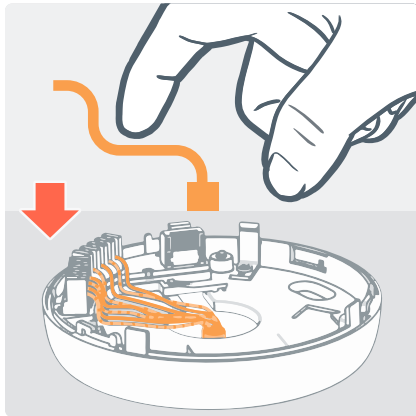


Figure 40 Punch Down Wires

If using punch down press the wires down to ensure they do not obstruct the camera module.



After wires are punched down, cut off any excess wires.

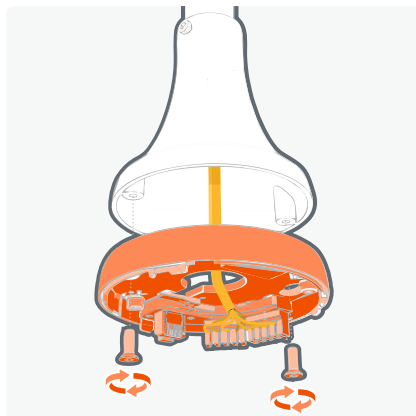


Figure 41 Secure Camera Enclosure onto the Pendant Mount

Screw the rear of the camera enclosure to the pendant mount using the two mounting screws. Make sure the ethernet cable pulls through the mounted rear of the camera enclosure.

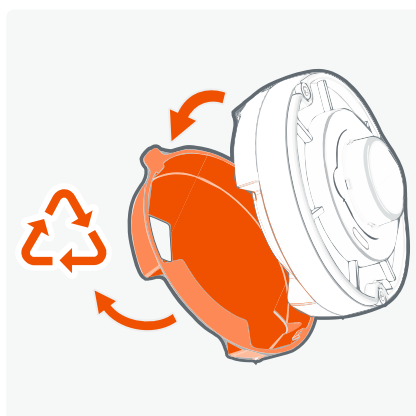


Figure 42 Protective Cover Removal

Remove and recycle the protective cover from the rear of the camera module.

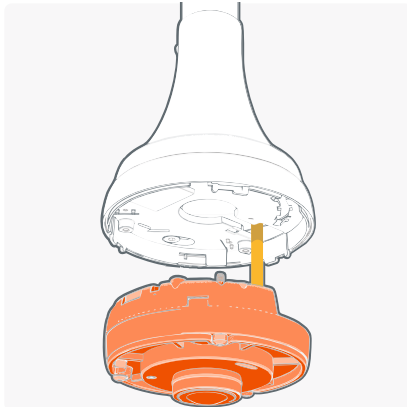


Figure 43 Connecting Camera Using RJ5 / Punch Down

For RJ45 simply plug the camera module in.
For the punch down simply connect the camera.

Connect the camera module, the clips will hold the camera in place. Ensure all three clips are fully engaged.

Tighten the 3 captive security screws to fix the camera module securely in place.

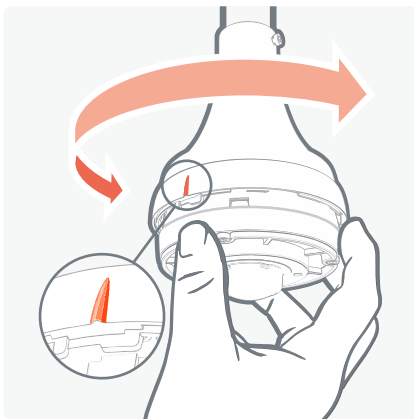


Figure 44 Camera Image Alignment

Using the marker on the rear of the camera housing as a reference align the pendant mount for the desired image orientation.



There is a "top" to the camera image represented by this marker, it is recommended that this directional top is used to orientate the camera image as required.



Care must be taken as over-adjusting the angle may unscrew the camera.

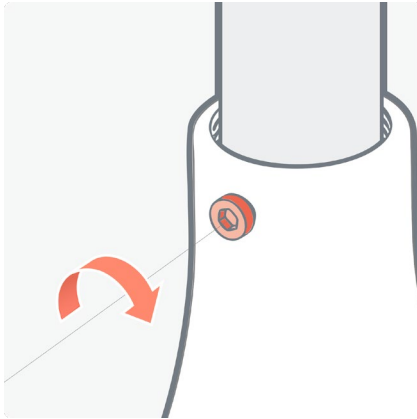


Figure 45 Locking Screw

Using the locking screw, fix the camera in place. This will stop rotation on the conduit screw thread and hold the camera onto the conduit screw thread.

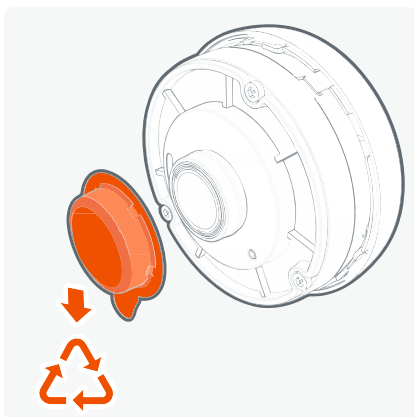


Figure 46 Protective Lens Cover Removal

Returning to the camera module, remove and recycle the protective lens cover.

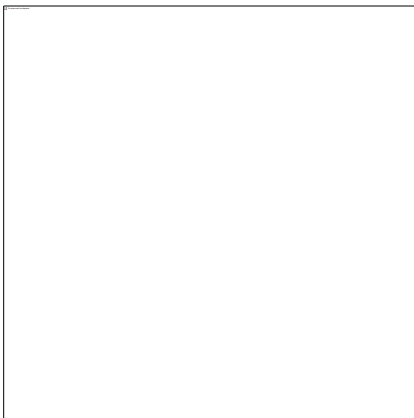


Figure 47 Align and close the Camera Enclosure Front Cover

Using the alignment marker push the camera enclosure cover over the camera module and twist to lock in place.

3.4.4 Panoramic+ Tilt Mount -Surface Mounting

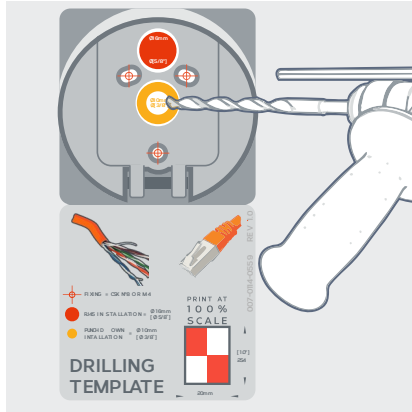
Using a spirit level to make sure it is straight, affix the drilling template to the wall by removing the self-adhesive backing.



If you are concerned about the adhesive on a delicate surface, put the drilling template on work trousers or other cloth to make it less sticky.

Identify if you are going to install using the punch down or RJ45 connector, using a bradawl or sharp point mark the two holes for the screws and the one hole for the ethernet cable.

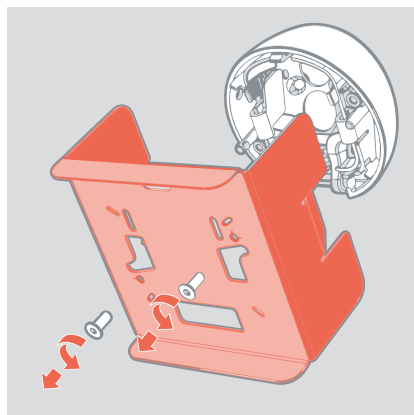
Remove the drilling template carefully from the wall.



Using the appropriate size of drill bit, drill the mounting holes and the hole for the ethernet cable.

Remove the drilling template once drilled.

Figure 48 Drilling Template

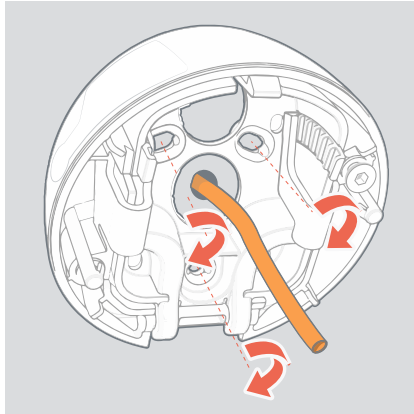


Unscrew the two mount screws and retain to mount the camera. Recycle the card insert.

Figure 49 Remove Card Insert



The camera has been designed to be mounted with #8 or 4mm countersunk screws, however the length and fixing support material (plugs etc.) need to be specified by the installer on a case-by-case basis.



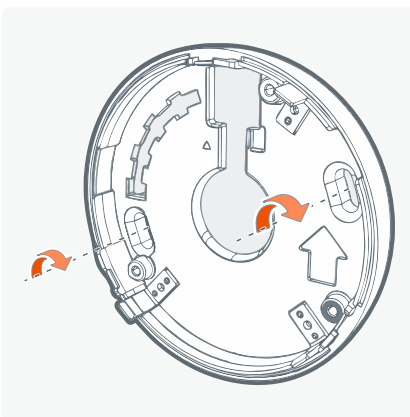
Using 3 off. Screws mount the bracket to the wall using the holes drilled previously.

Figure 50 Mount to wall



Open camera enclosure.

Figure 51 Opening of Camera Enclosure



Mount the rear of the camera enclosure to the bracket with the screws retained above.

Figure 52 Mounting of Camera Enclosure

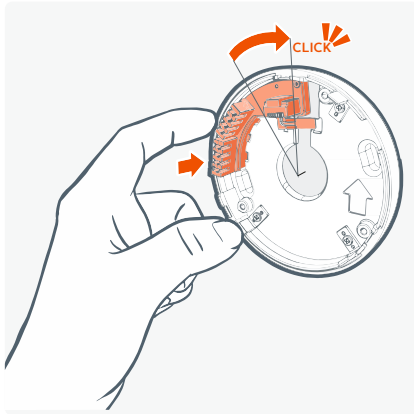


Figure 53 Punch down Adapter

If you prefer to use the punch down, you need to add the punch down adapter here (accessory located in the box packaging). Following the guide, punch down the ethernet cable.

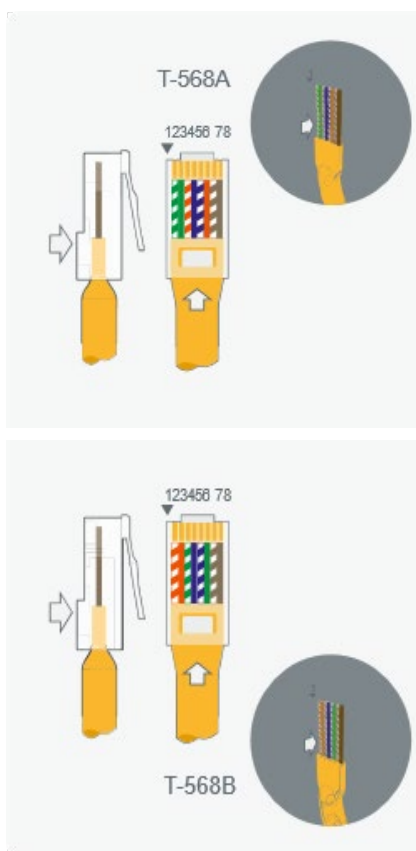
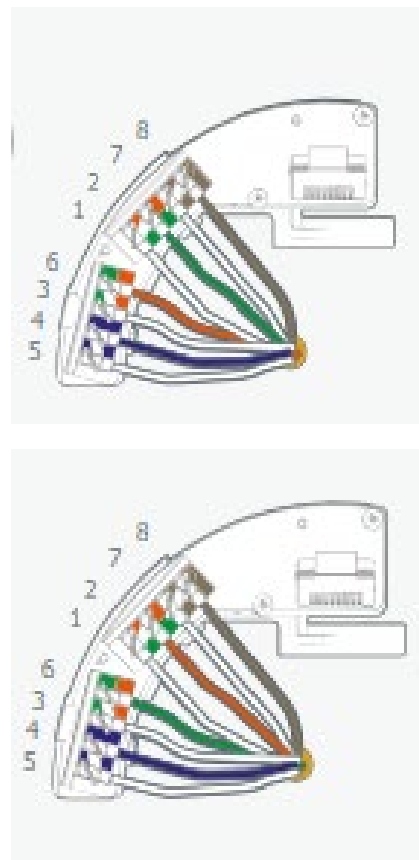


Figure 54 Identify Wiring Type for Punch Down



Strip sheath to approximately 7cm [2 3/4"]. So, you have enough wires to punch down, excess wire can be cut after punching down.

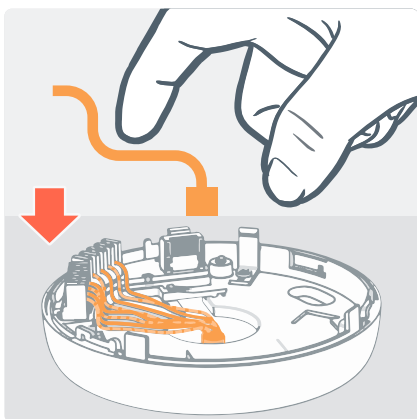


Figure 55 Punch Down Wires

If using punch down press the wires down to ensure they do not obstruct the camera module.



After wires are punched down, cut off any excess wires.



Figure 56 Protective Cover Removal

Remove and recycle the protective cover from the rear of the camera module.

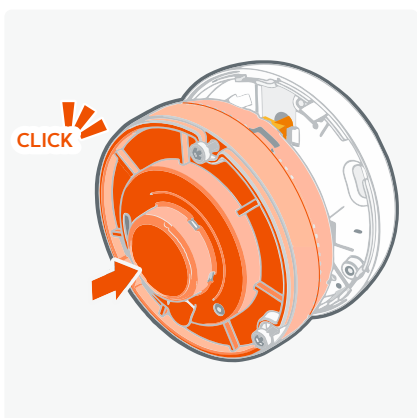


Figure 57 Connecting of Camera Module

Connect the camera module, the clips will hold the camera in place.

For RJ45 simply plug the camera module in, for the punch down simply connect the camera.

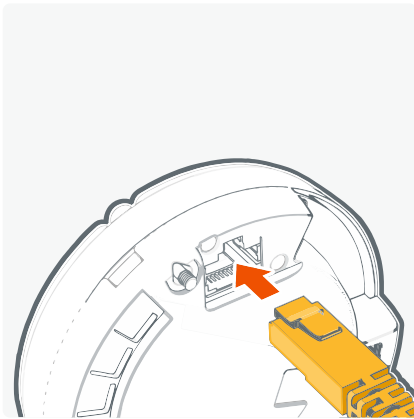


Figure 58 Connecting of Ethernet Cable

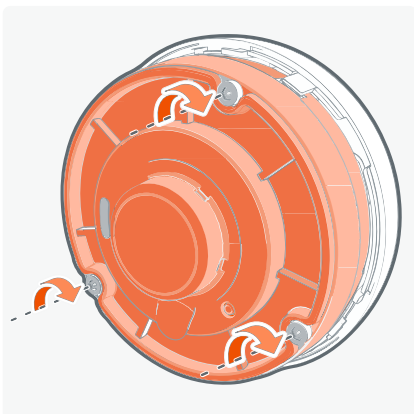


Figure 59 Securing the Camera Module

Using the security hex tool, tighten the 3 captive screws.

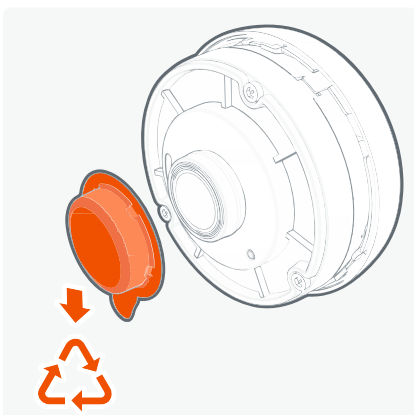


Figure 60 Protective Lens Cover Removal

Remove and recycle the protective lens cover.

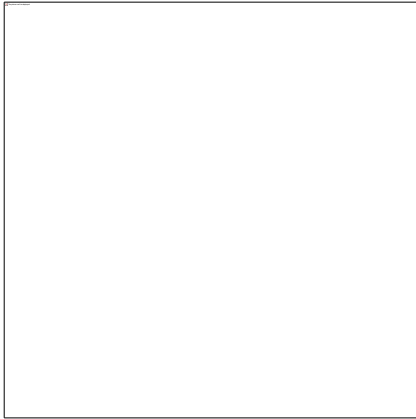


Figure 61 Cover Twist

Using the alignment feature as a guide, push on the cover twist to lock in place.

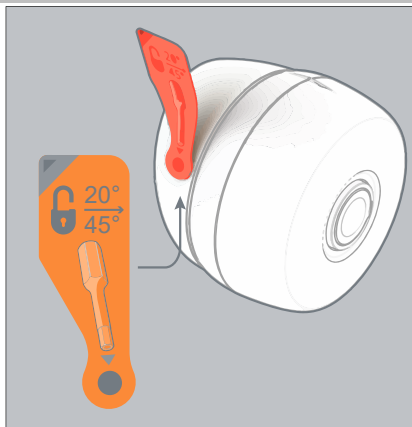


Figure 62 - Remove Label

Remove the label from the side of the angle mount, exposing the security hole to allow the angle to be set.

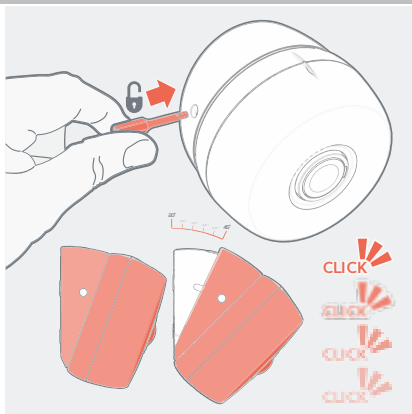


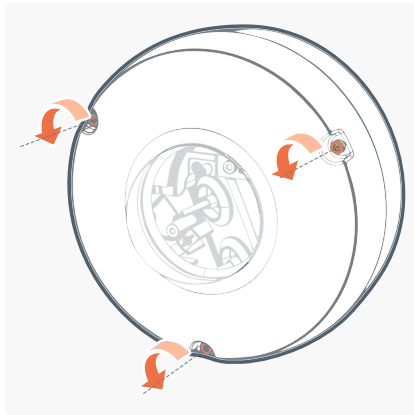
Figure 63 – Hex Tool Unlocks

Using the hex tool used for mounting the camera screws, push it in the hole on the side. This will unlock the catch on the inside of the mount and allow the camera angle to be carefully adjusted.

There are physical and audible “clicks” at each 5-degree set angle.

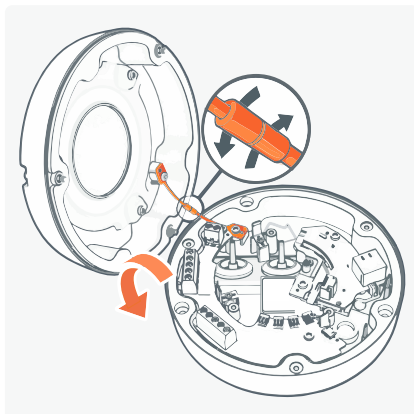
3.5 Outdoor Plus Camera

3.5.1 Surface Mounting



The camera comes assembled, using the security hex bit, loosen the three captive screws.

Figure 64 Loosen Captive Screws



Once the front is loose, open the camera enclosure and undo the retaining tether. Put the front enclosure back in the box for safe keeping.

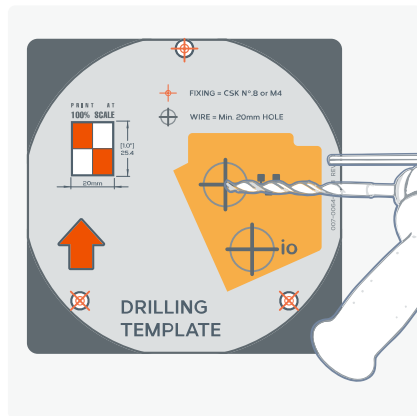
Figure 65 Front Camera Enclosure removal

Using a spirit level to make sure it is straight, affix the drilling template to the wall by removing the self-adhesive backing.



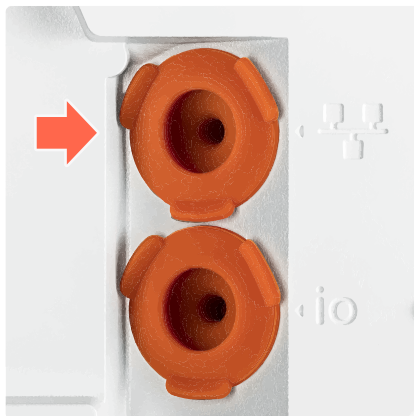
If you are concerned about the adhesive on a delicate surface put the drilling template on work trousers or other cloth to make it less sticky.

Using a bradawl or sharp point, mark the three holes for the screws and the one hole for the ethernet cable.



Drill the 3 holes suitable for these fixings and the larger hole for the ethernet cable, then carefully remove the drilling template from the wall.

Figure 66 Drilling Template



Remove the gland from the rear enclosure (the two glands are highlighted with icons to denote which one should be used; This is the one for the ethernet cable).

Figure 67 Gland Identification

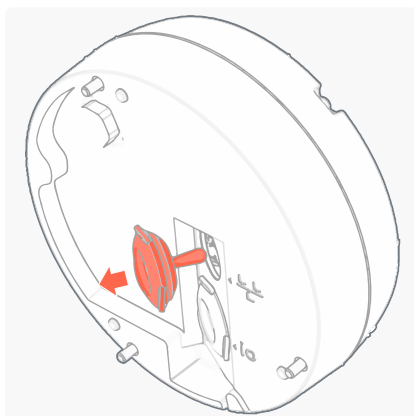


Figure 68 Removal of Gland

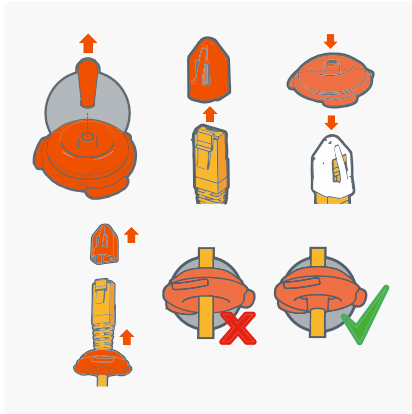


Figure 69 Sealing of Cable

Remove the tip from the gland, push the ethernet cable through the gland.

For a cable with a terminated RJ45 connector, use the RJ45 cap to protect the gland from damage and pull through 12cm [4 3/4"] of cable. Remove the cap.

For Punch down pull through 6cm [2 1/2"].

Pull the cable backwards to flip the seal inside out to ensure the seal is at its best.

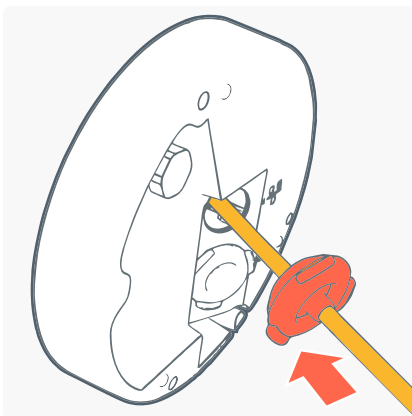


Figure 70 Gland into Rear Enclosure

Push the gland back into the rear enclosure, ensure it is bedded back into place.

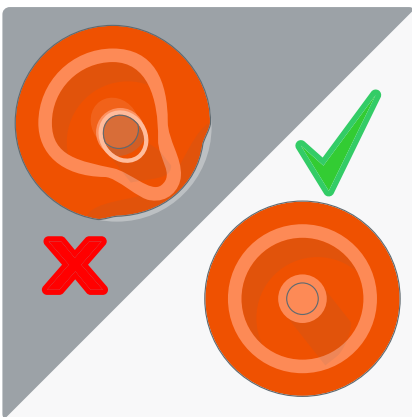


Figure 71 Check positioning

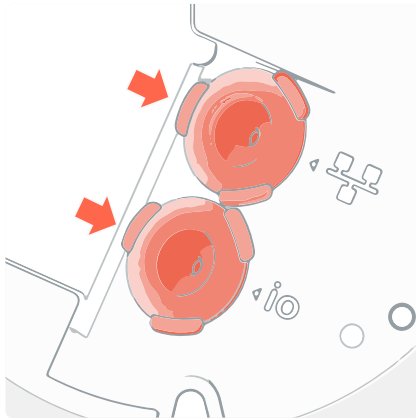


Figure 72 Gland Alignment

Ensure the tabs of the gland are aligned as shown.

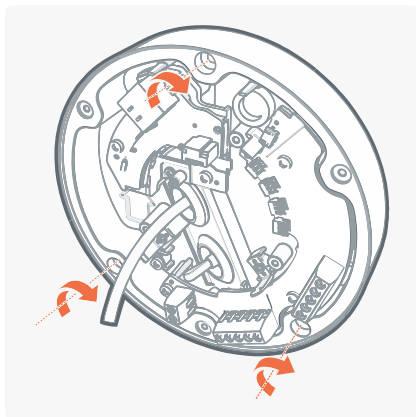


Figure 73 Rear Enclosure

Using appropriate fixings for the surface mount, the rear enclosure to the wall.

The camera has been designed to be mounted with #8 or 4mm countersunk screws, however the length and fixing support material (plugs etc.) need to be specified by the installer on a case by case basis.

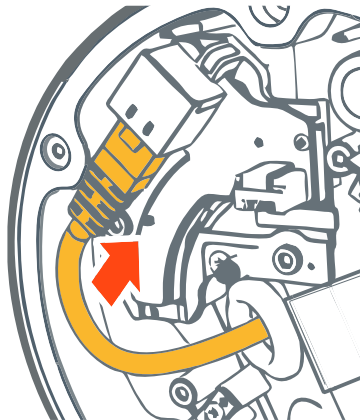


Figure 74 Plugging RJ45 Connector to RJ45 Socket

If a cable terminated with a RJ45 connector is used, then plug it into to RJ45 socket.

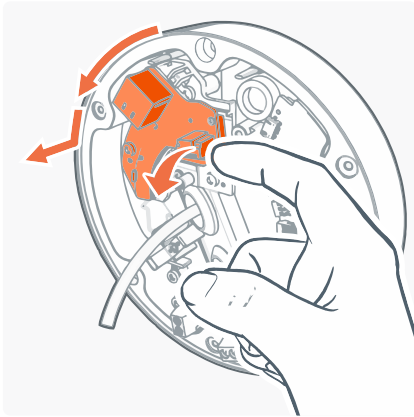


Figure 75 Removal of RJ45 Board

If using the punch down remove the RJ45 board and replace it with the punch down board (accessory located in the box packaging).

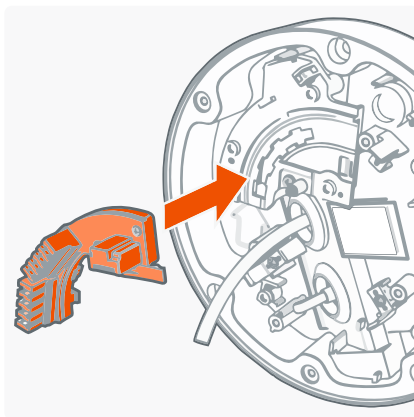


Figure 76 Insert Punch Down Board

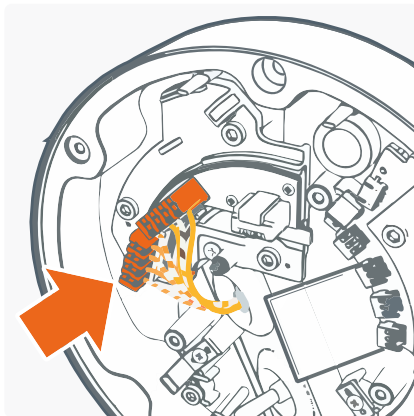


Figure 77 Punch Down Ethernet Cable

Strip and punch down the ethernet cable.

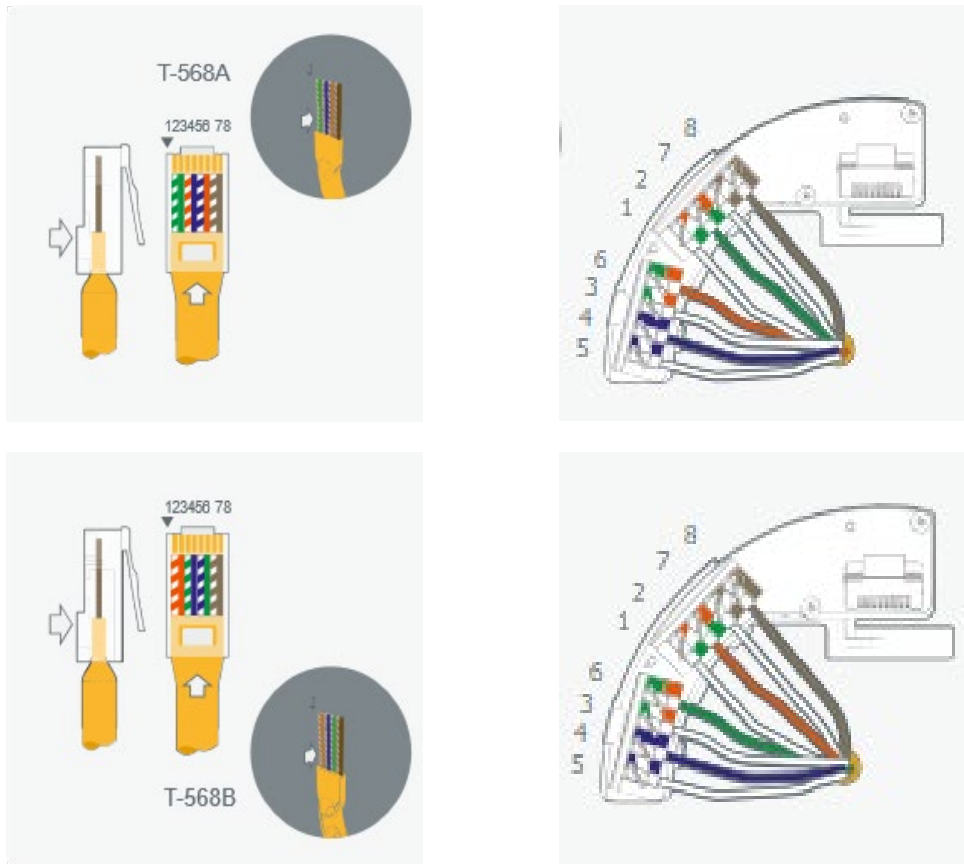


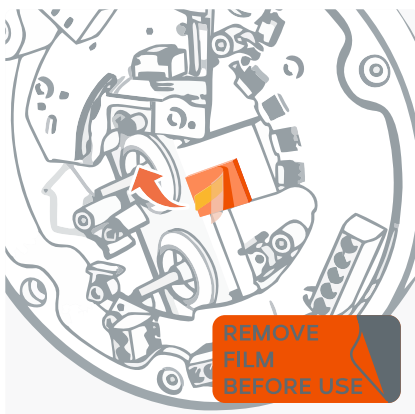
Figure 78 Identify Wiring Type for Punch Down



Strip sheath to approximately 6cm [2 1/2"] so you have enough wires to punch down. Excess wire can be trimmed after punching down.

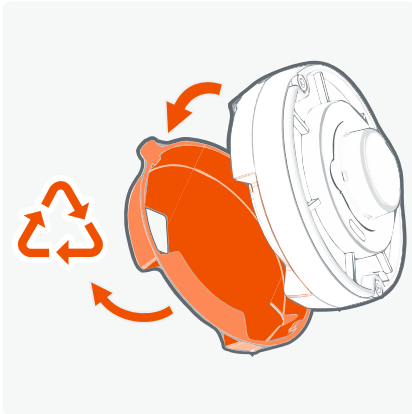


After wires are punched down, cut off any excess wires.



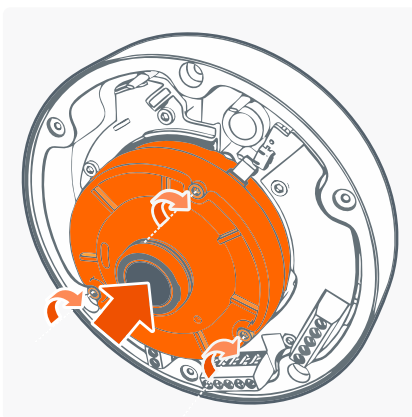
Remove and recycle the protective film from the thermal pad.

Figure 79 Protective Film Removal



Remove and recycle the protective cover from the rear of the camera module.

Figure 80 Protective Cover Removal



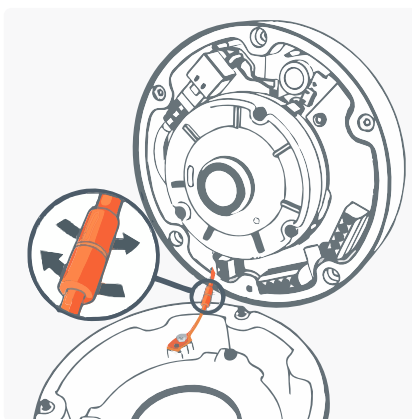
Connect the camera module, the clips will help to hold the camera in place.

Tighten the 3 captive screws using the hex tool.

Figure 81 Camera Module Connection

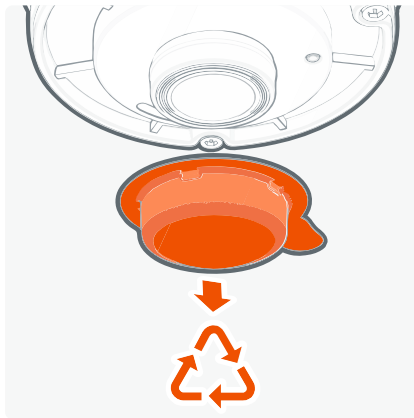


Ensure all three clips are correctly engaged.



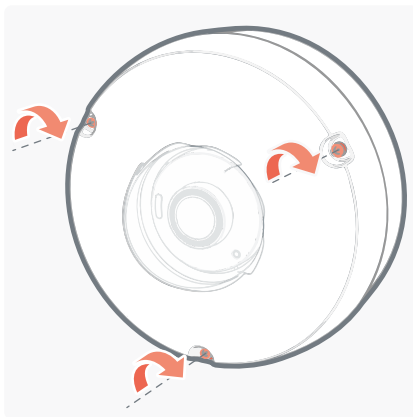
Taking the front of the enclosure, which was set aside; reattach the retaining tether.

Figure 82 Reattach Front Cover



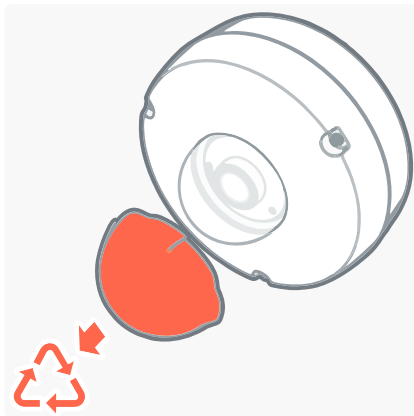
Remove and recycle the protective lens cover.

Figure 83 Protective Cover Removal



With care, place the front of the camera enclosure onto the rear of the enclosure and tighten the 3 captive security screws using the hex tool.

Figure 84 Secure the Front Cover

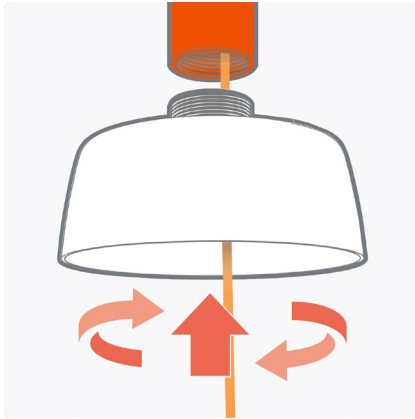


Remove and recycle the protective film from dome.

Figure 85 Protective Cover Removal

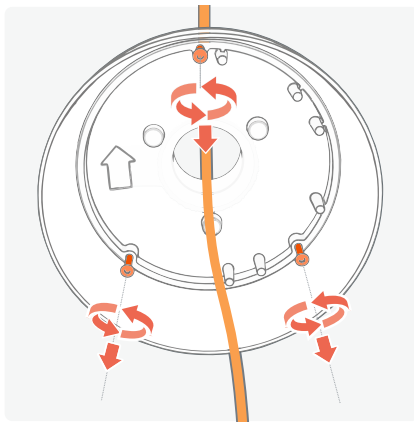
3.5.2 Pendant Mount Kit (Including Sunshield)

Run a drop conduit or pendant arm with an internal (female) 1 ½ " NPT thread. Run the ethernet cable through the conduit.



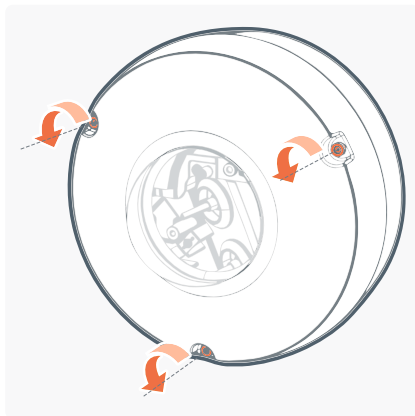
Push the ethernet cable through the central hole on the pendant mount, screw the pendant mount to the 1 ½ " NPT thread.

Figure 86 Ethernet Cable onto the Pendant Mount



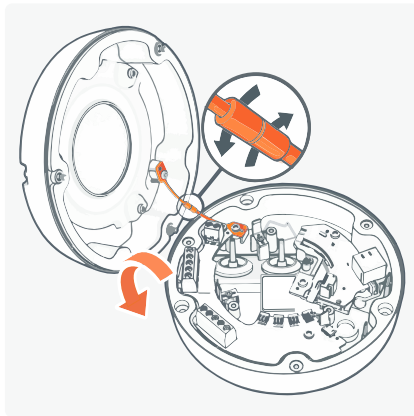
Remove the 3 mounting screws and put to one side. These will be used later to mount the rear camera enclosure.

Figure 87 Removal of Mounting Screws



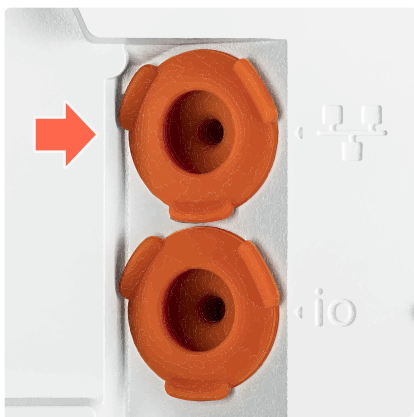
The camera comes assembled, using the security hex bit, loosen the 3 captive screws.

Figure 88 Loosen Captive Screws



Once the front is loose, open the camera enclosure and undo the retaining tether. Put the front enclosure back in the box for safe keeping.

Figure 89 Opening of Camera Enclosure



Remove the gland from the rear enclosure (the two glands are highlighted with icons to denote which one should be used; this is the one for the ethernet cable).

Figure 90 Gland Identification

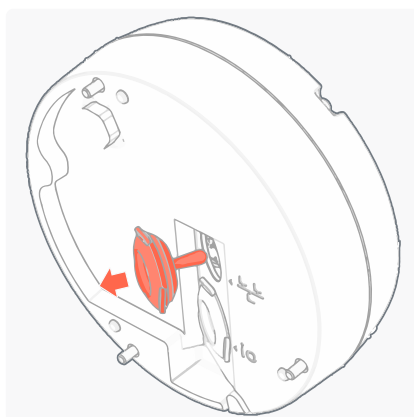


Figure 91 Removal of Gland

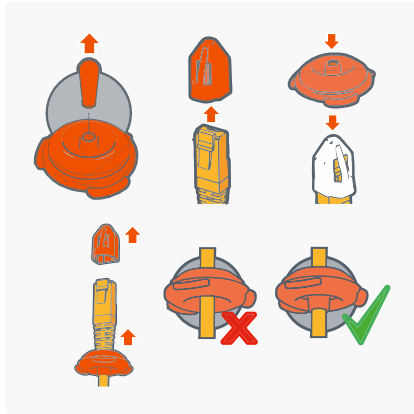


Figure 92 Sealing of Cable

Remove the tip from the gland, push the ethernet cable through the gland.

For a cable with a terminated RJ45 connector, use the RJ45 cap to protect the gland from damage and pull through 12cm [4 3/4"] of cable. Remove the cap.

For Punch down pull through 6cm [2 1/2"].

Pull the cable backwards to flip the seal inside out to ensure the seal is at its best.

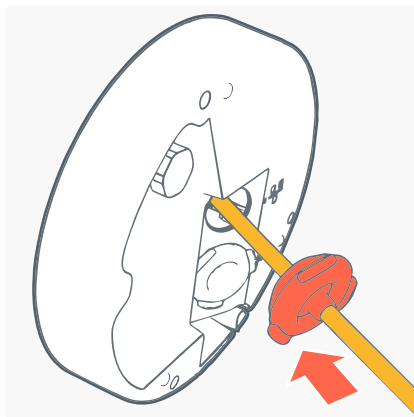


Figure 93 Gland into Rear Enclosure

Push the gland back into the rear enclosure ensure it is bedded back into place.

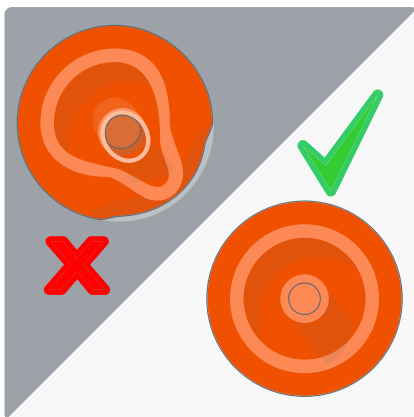
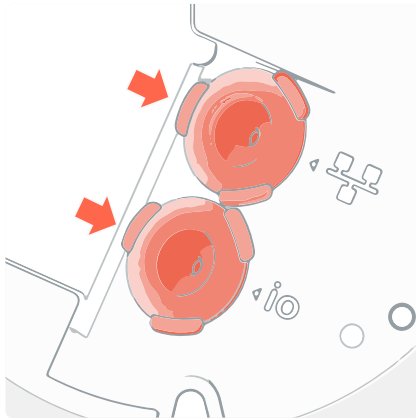
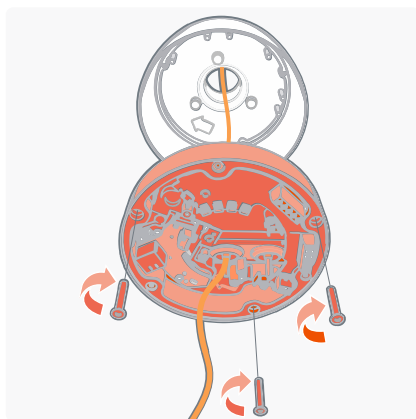


Figure 94 Check Positioning



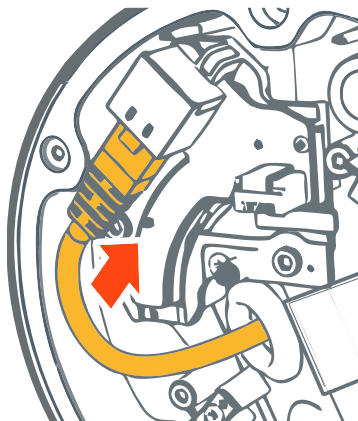
Ensure the tabs of the gland are aligned as shown.

Figure 95 Gland Alignment



Screw the rear enclosure to the pendant mount using the 3 screws removed from the pendant mount previously.

Figure 96 Secure Rear Enclosure to the Pendant Mount



If using a cable terminated with RJ45 connector, plug it into to RJ45 socket.

Figure 97 RJ45 Connector into RJ45 Socket

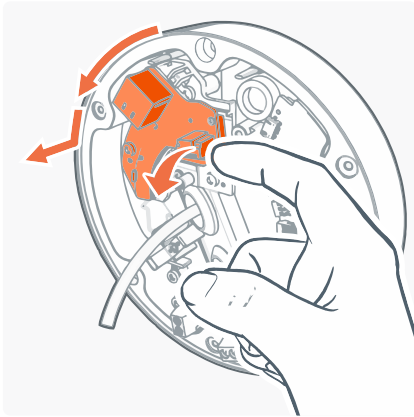


Figure 98 Removal of RJ45 Board

If using the punch down, remove the RJ45 board and replace it with the punch down board (accessory located in the box packaging).

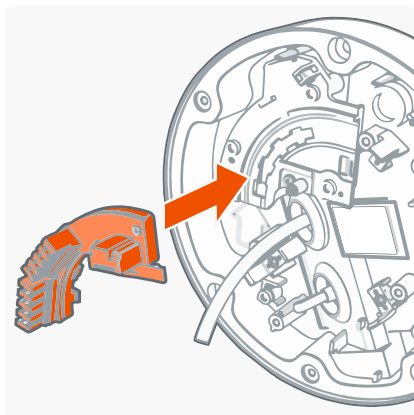


Figure 99 Insert Punch Down Board

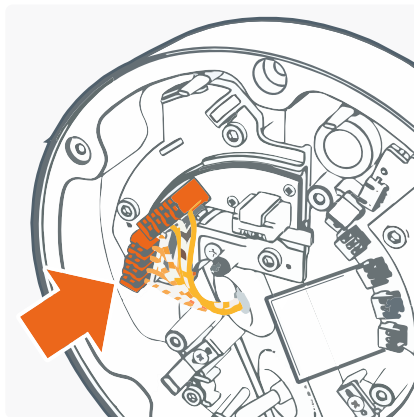


Figure 100 Punch Down of Ethernet Cable

Strip and punch down the ethernet cable using the guide.

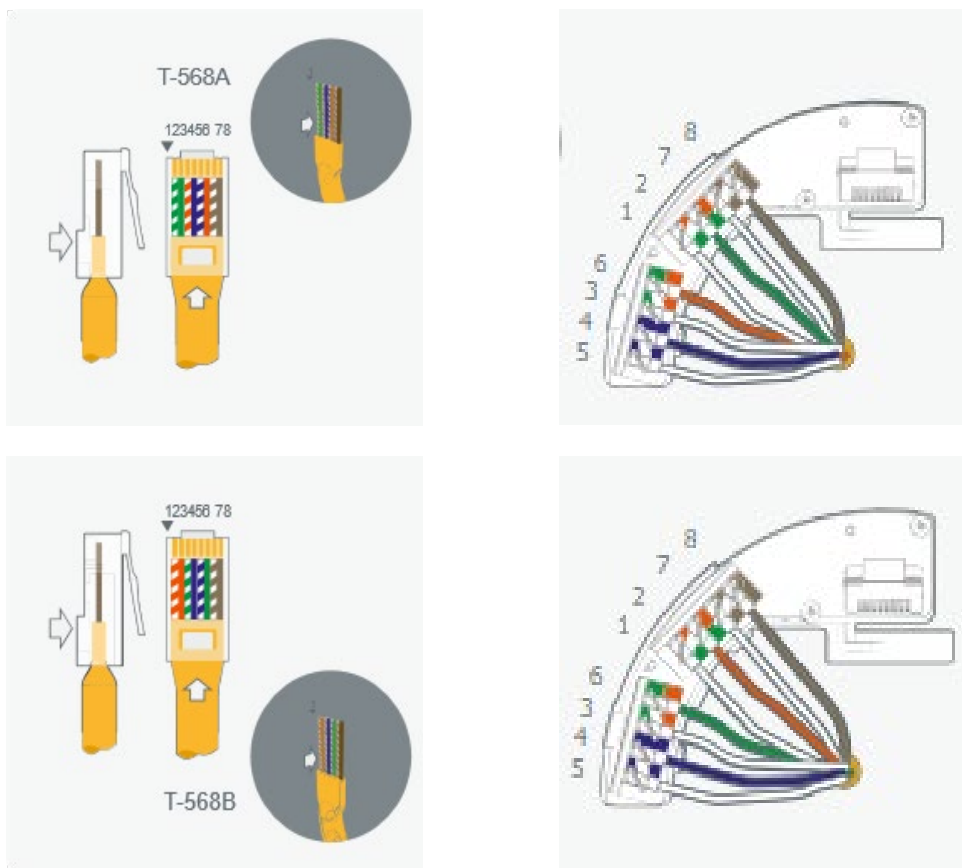


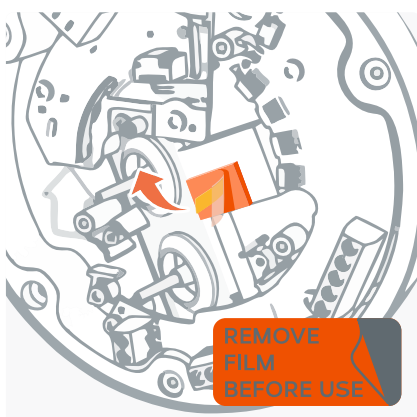
Figure 101 Identify Wiring Type for Punch Down



Strip sheath to approximately 6cm [2 1/2"] so you have enough wires to punch down. Excess wire can be trimmed after punching down.

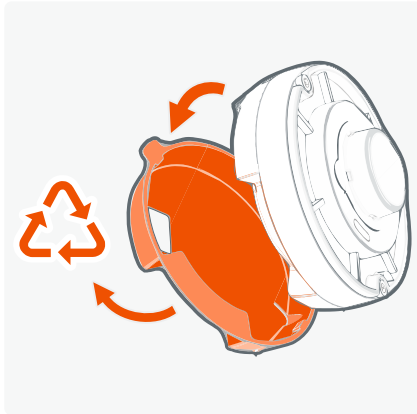


After wires are punched down, cut off any excess wires.



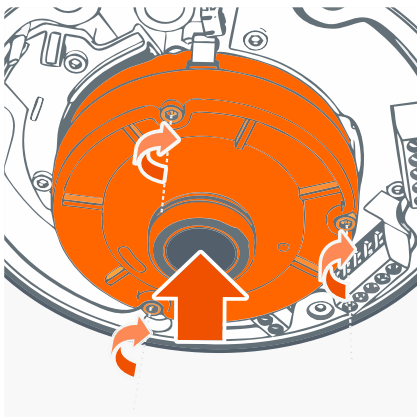
Remove and recycle the protective film from the thermal pad.

Figure 102 Protective Film Removal



Remove and recycle the protective cover from the rear of the camera module.

Figure 103 Protective Cover Removal



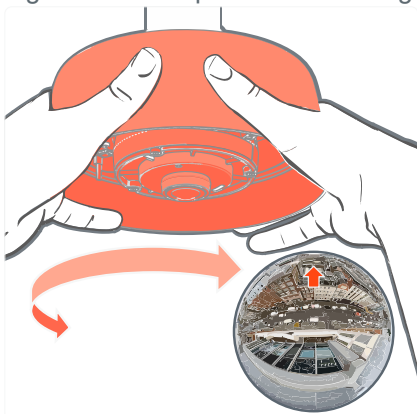
Connect the camera module, the clips can help hold the camera in place.

Figure 104 Camera Module



Ensure all three clips are correctly engaged.

Tighten the 3 captive screws using the hex tool.



Using the arrow on the camera module as a reference align the pendant mount for the desired image orientation.

Figure 105 Camera Module Alignment



There is a "top" to the camera image represented by direction of this arrow, it is recommended that this directional top is used to orientate the camera image as required.



Care must be taken as over-adjusting the angle may unscrew the camera.

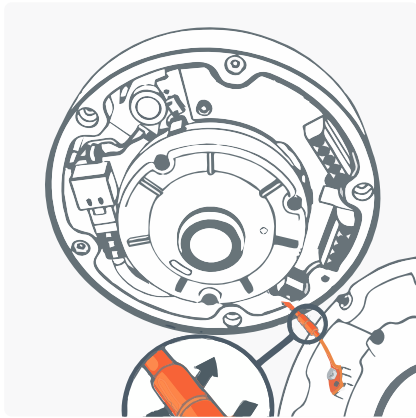


Figure 106 Reattach the front cover

Taking the front of the enclosure, which was set aside; reattach the retaining tether.

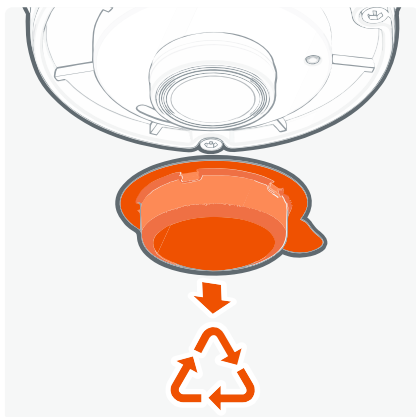


Figure 107 Protective Lens Cover

Remove and recycle the protective lens cover.

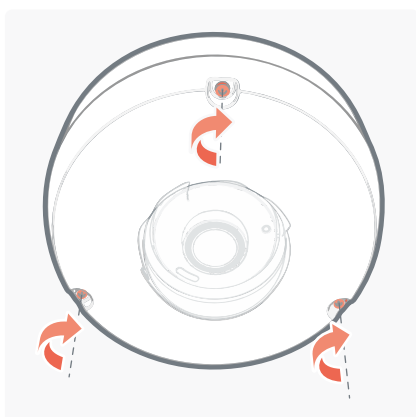
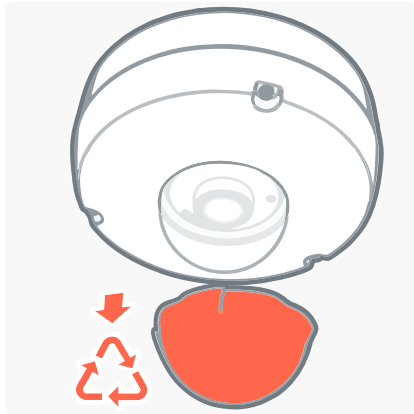


Figure 108 Secure Front Enclosure

With care, place the front of the camera enclosure onto the rear of the enclosure and tighten the 3 captive security screws using the hex tool.



Remove and recycle the protective film from dome.

Figure 109 Protective Film



Completed installation.

Figure 110 Camera after installation

3.5.3 Panoramic+ Tilt Adaptor - Pendant drop

Having found a suitable pendant arm with a 1½" NPT female thread. Mount it in a suitable position for the Panoramic+ camera.



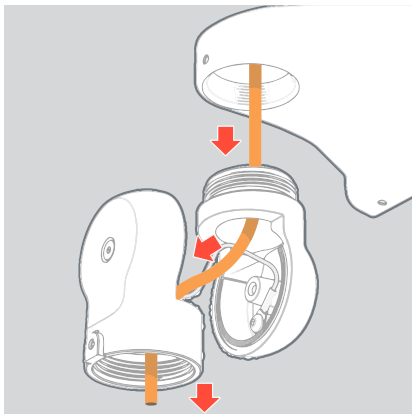
Using the hex bit included in the box, unscrew the locking screw. The screw is captive and therefore will not fall out.

Figure 111 Undo The Locking Screw



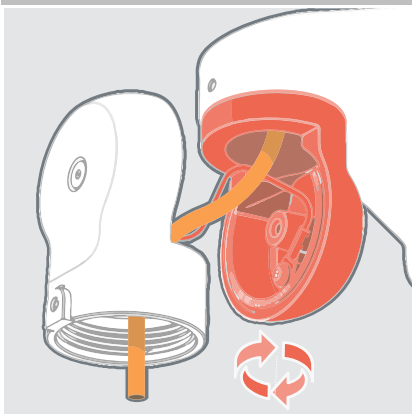
During the installation, it is important not to allow the ethernet cable to twist.

Therefore, it's important to take the tilt adaptor apart.



With the two halves apart, run the ethernet cable through the center of the tilt adaptor.

Figure 112 Run Ethernet Cable



Whilst still apart, screw the tilt adaptor into the pendant mount.

Figure 113 Screw To Pendant

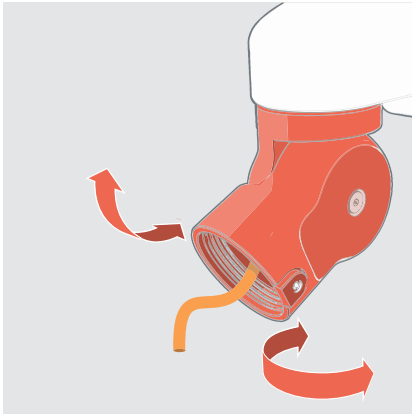


Figure 114 Adjust The Angle

Adjust the angle to point the camera towards the area of interest.

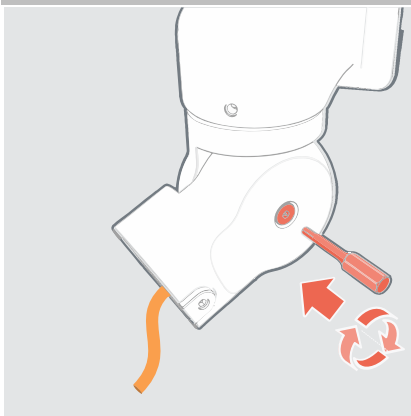


Figure 115 Tighten The Locking Screw

Using the hex tool, tighten the locking screw until it just nips it in place to hold at the approximate angle.

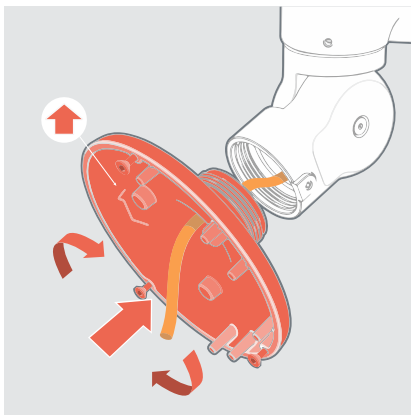


Figure 116 – Screw On Pendant Mount

Taking the CA-OPM1-O Outdoor Pendant Mount (required) screw the mount to the tilt adaptor.

Note the arrow points “up” with regard the Panoramic+ image.

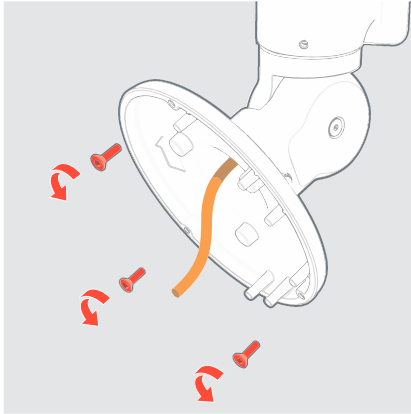


Figure 117 – Mounting Screws

Remove the 3 mounting screws and retain for mounting the camera enclosure

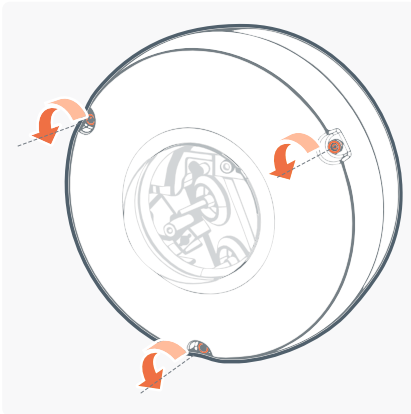


Figure 118 Loosen Captive Screws

The outdoor camera (required) comes assembled, using the security hex bit, loosen the 3 captive screws.

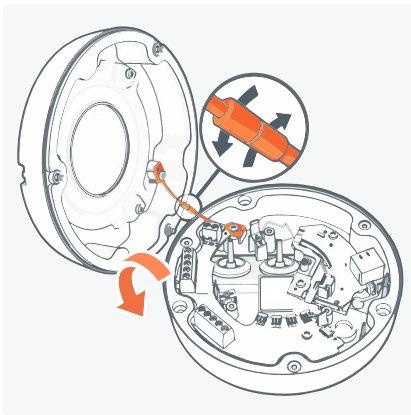


Figure 119 Opening of Camera Enclosure

Once the front is loose, open the camera enclosure and undo the retaining tether. Put the front enclosure back in the box for safe keeping.

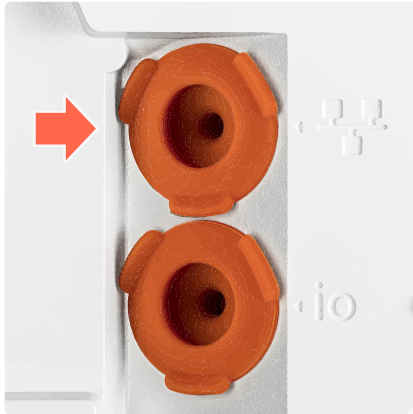


Figure 120 Gland Identification

Remove the gland from the rear enclosure (the two glands are highlighted with icons to denote which one should be used; this is the one for the ethernet cable).

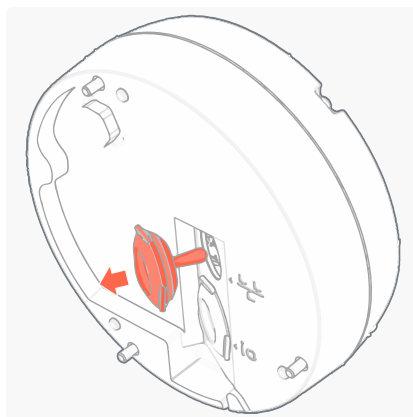


Figure 121 Removal of Gland

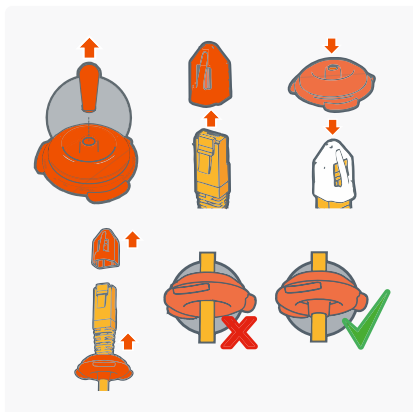


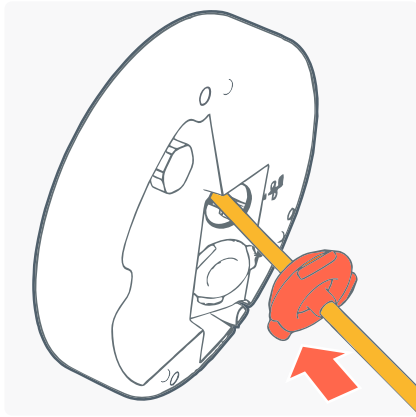
Figure 122 Sealing of Cable

Remove the tip from the gland, push the ethernet cable through the gland.

For a cable with a terminated RJ45 connector, use the RJ45 cap to protect the gland from damage and pull through 12cm [4 3/4"] of cable. Remove the cap.

For Punch down pull through 6cm [2 1/2"].

Pull the cable backwards to flip the seal inside out to ensure the seal is at its best.



Push the gland back into the rear enclosure ensure it is bedded back into place.

Figure 123 Gland into Rear Enclosure

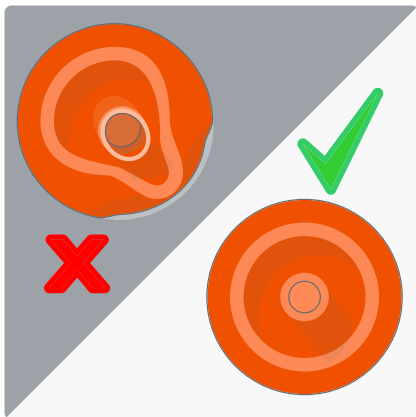
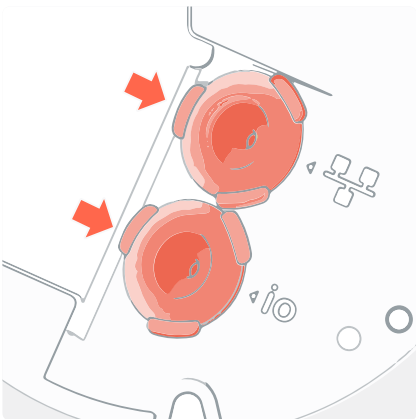


Figure 124 Check Positioning



Ensure the tabs of the gland are aligned as shown.

Figure 125 Gland Alignment

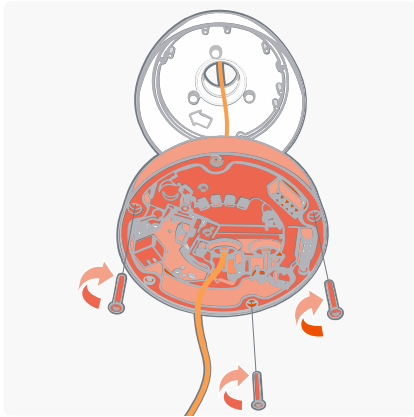


Figure 126 Secure Rear Enclosure to the Pendant Mount

Screw the rear enclosure to the pendant mount using the 3 screws removed from the pendant mount previously.

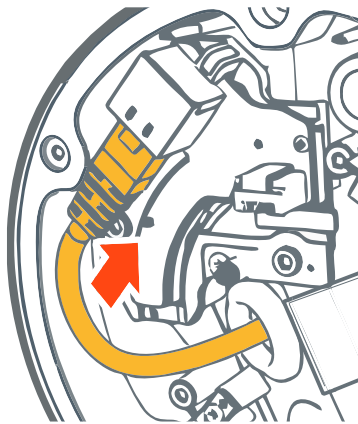


Figure 127 RJ45 Connector into RJ45 Socket

If using a cable terminated with RJ45 connector, plug it into to RJ45 socket.

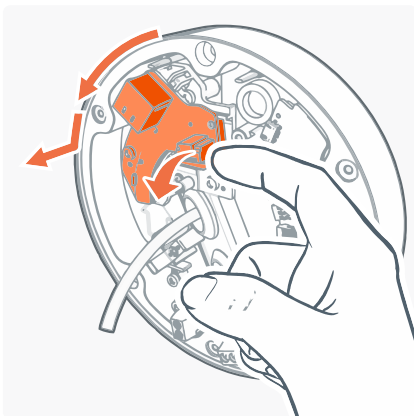


Figure 128 Removal of RJ45 Board

If using the punch down, remove the RJ45 board and replace it with the punch down board (accessory located in the box packaging).

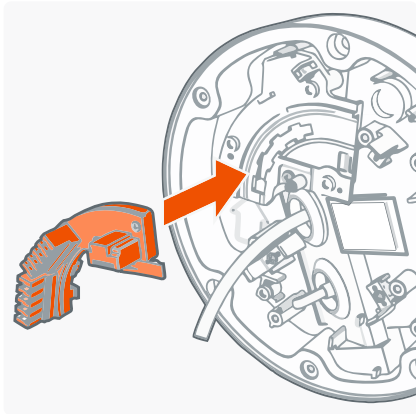


Figure 129 Insert Punch Down Board

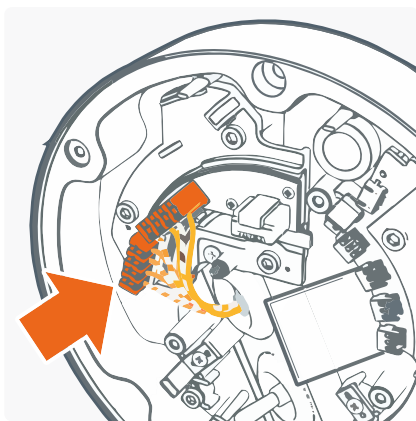
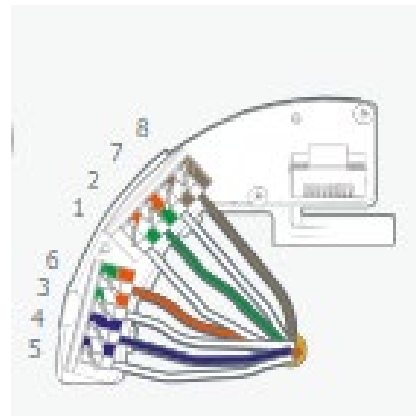
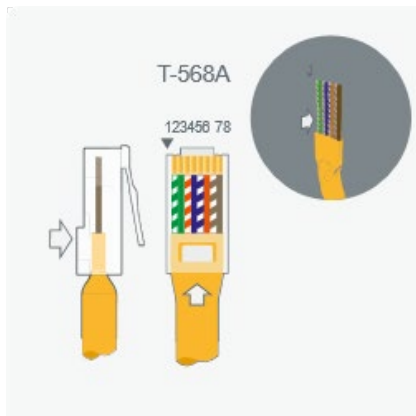


Figure 130 Punch Down of Ethernet Cable

Strip and punch down the ethernet cable using the guide.



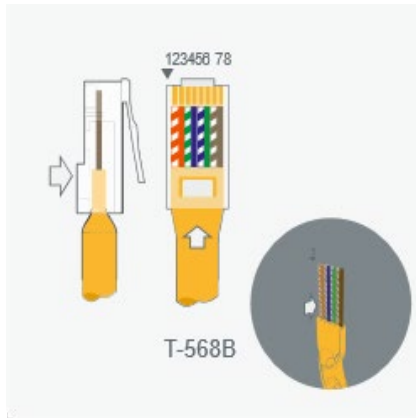
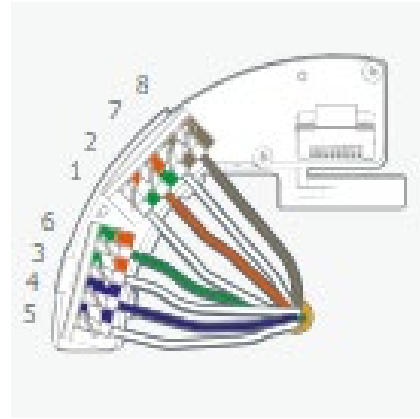


Figure 131 Identify Wiring Type for Punch Down



Strip sheath to approximately 6cm [2 1/2"] so you have enough wires to punch down. Excess wire can be trimmed after punching down.



After wires are punched down, cut off any excess wires.

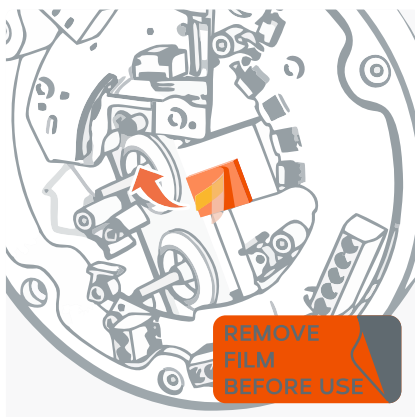


Figure 132 Protective Film Removal

Remove and recycle the protective film from the thermal pad.



Figure 133 Protective Cover Removal

Remove and recycle the protective cover from the rear of the camera module.

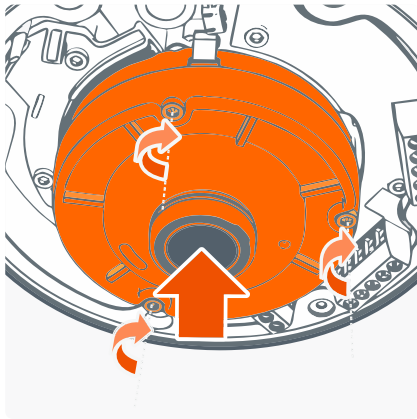


Figure 134 Camera Module

Connect the camera module, the clips can help hold the camera in place. Using the hex tool, tighten the 3 mounting screws.



Ensure all three clips are correctly engaged.

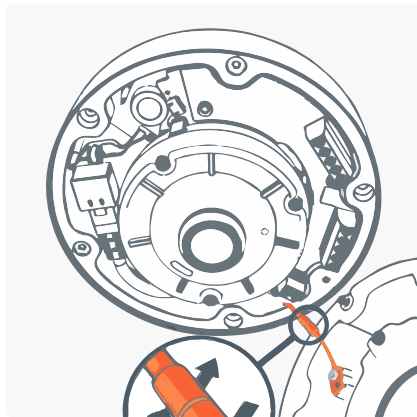


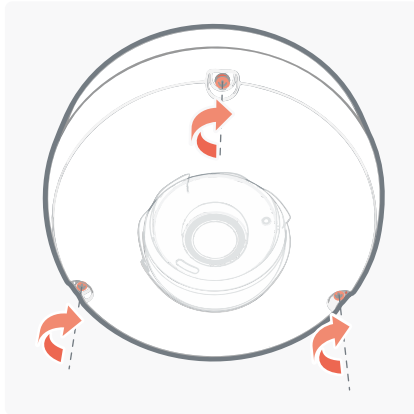
Figure 135 Reattach the front cover

Taking the front of the enclosure, which was set aside; reattach the retaining tether.



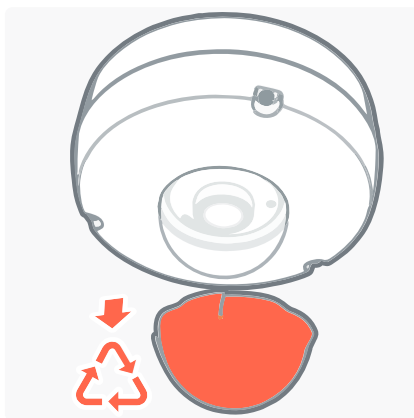
Figure 136 Protective Lens Cover

Remove and recycle the protective lens cover.



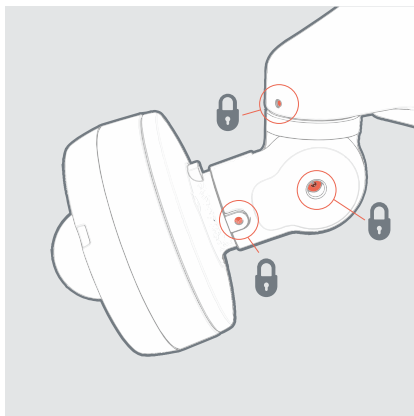
With care, place the front of the camera enclosure onto the rear of the enclosure and tighten the 3 captive security screws using the hex tool.

Figure 137 Secure Front Enclosure



Remove and recycle the protective film from dome.

Figure 138 Protective Film

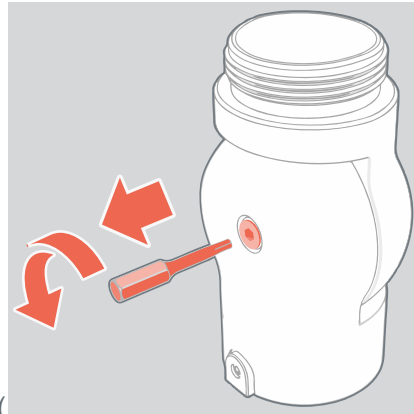


Having fitted the camera and confirmed the perfect angle – tighten the locking screws.

Figure 139 Lock Angles

3.5.4 Rain Guard

3.5.4.1 Pendant drop



Having installed the Tilt bracket and pendant Mount (

Figure 111 to Figure 117).

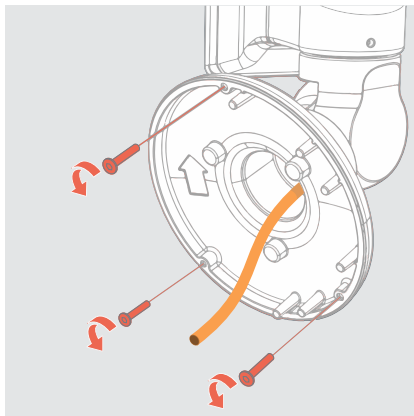


Figure 140 Remove mounting screws

Using the hex bit tool included in the box, remove the 3 mounting screws and retain them for mounting the camera enclosure

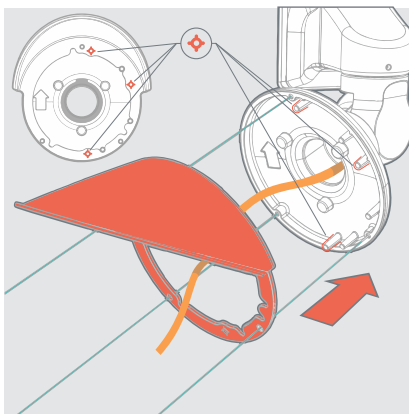
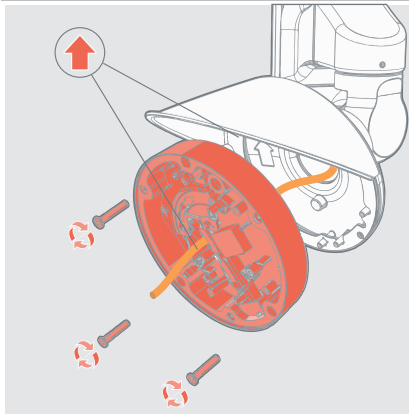


Figure 141 Align Rain Guard

Align the rain guard with the pendant mount using the 3 location pins ensuring the captive mounting holes are clear

Firmly push the rain guard onto the pendant mount, the rain guard has retaining features built in to hold it in place.



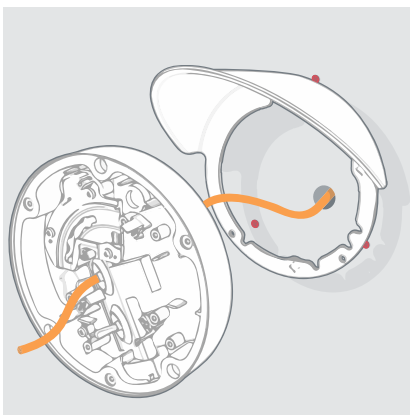
Mount the rear enclosure to the pendant mount using the 3 screws removed from the pendant mount earlier.

Figure 142 Screw rear enclosure To Pendant mount

Continue installing the camera from *Figure 127* to complete installation

3.5.4.2 Surface Mounting

Having used the drilling template to mark and drill the holes in the surface (steps: *Figure 66* to *Figure 72*)



Feed the ethernet cable through the middle of the rain guard and into the camera enclosure.

Figure 143 Align Rain Guard

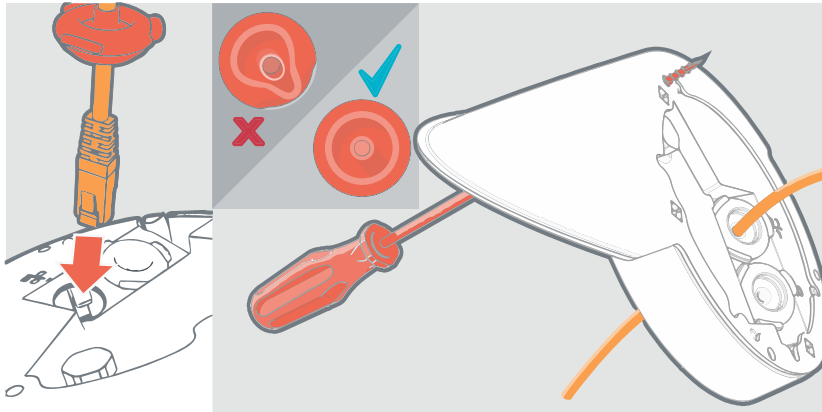


Figure 144 – Insert Gland, install to surface

Using one of the appropriate screws to mount the camera housing to the surface, hold the 2 parts (RainGaurd and rear enclosure) together. Offer up the parts to the hole you have made and screw it in a little.

Now screw the remaining screws in place.

Finish by tightening all three screws.

Continue installing the camera from **Figure 74** onwards.

3.5.5 Plus Board

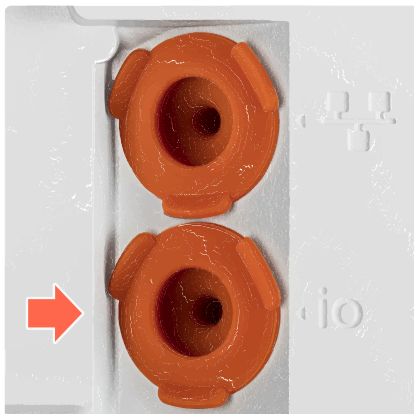


Figure 145 IO Entry Gland

There is a second gland entry point provided for the input / output devices. This is marked with an IO.

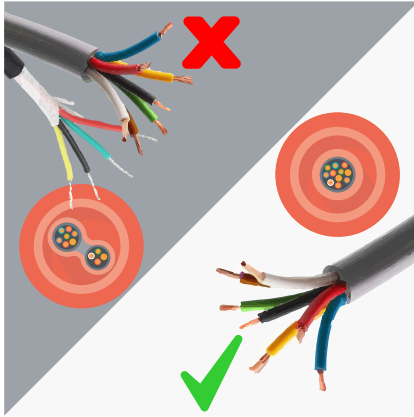


Figure 146 Multi - Core Cable

There are several cables available with multiple cores, you should use one multi-core cable and not multiple cables through the gland.

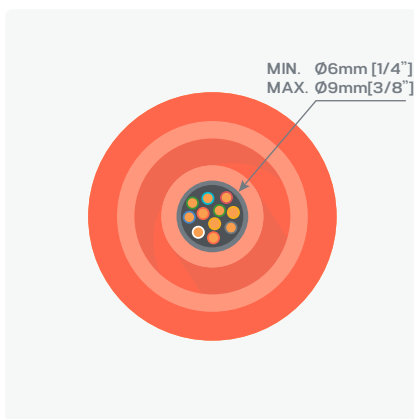


Figure 147 Sealing the Cable Sheath

For sealing the cable sheath outer diameter needs to be cylindrical and minimum of 6mm diameter and maximum of 9mm diameter.



The cable needs to be sealed at both ends, the camera will seal one end.



If the other end of the cable is left open, moisture can wick down the cable and enter the camera.

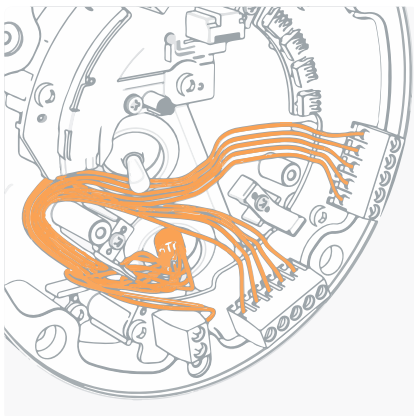


Figure 148 Cable through Screw Terminals

Run the cable downwards, and up to the screw terminals along the path shown in **Figure 148** and **Figure 149**, keeping clear of the camera.

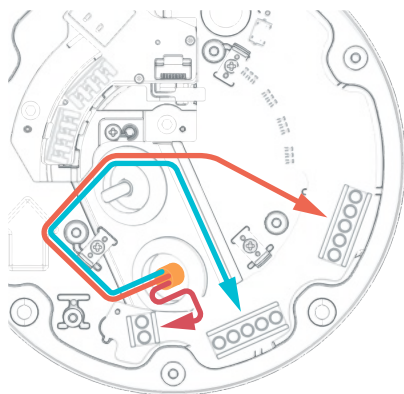


Figure 149 Cable Path to Screw Terminals

3.5.5.1 Input / Output

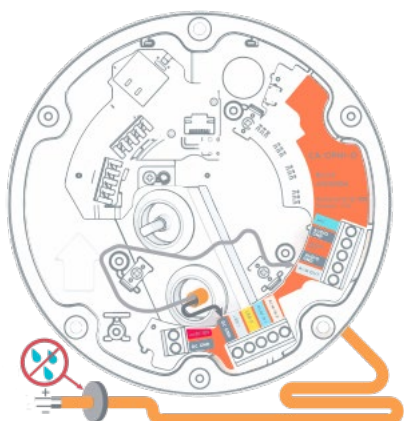


Figure 150 Alarm Output Signal

Alarm output is provided by the screw terminal on the plus board. When an event occurs triggering an external alarm on the camera, the ALM OUT pin outputs a GND signal (Low). Use this signal to drive the external alarm circuit (known as sinking). The output can sink current at 15 mA (max). By default, the output is normally open (NO), but can be switched to normally closed (NC) in the camera settings.

LED1 and LED2 outputs are located on the lower screw terminal block and provide logic level outputs, allowing camera alarms to operate external equipment with a logic level control input.

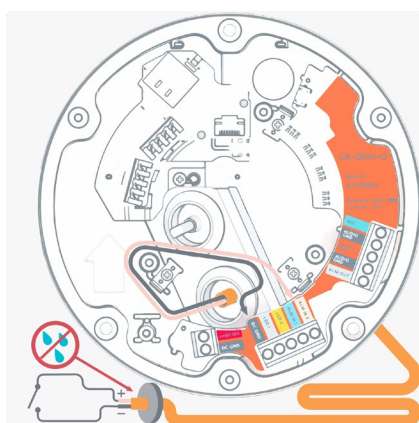


Figure 151 Alarm Input Signal

ALM IN 1 is Alarm in: 1 which provides external control input to the user.

ALM IN 2 is Alarm in: 2 which provides external control input to the user.

ALM OUT enables the camera to output a signal to control an external device.

When connecting alarm inputs/output, use the DC GND connection next to the ALM IN/ALM OUT (not the DC GND next to DC 12V).

3.5.5.2 Audio Microphone

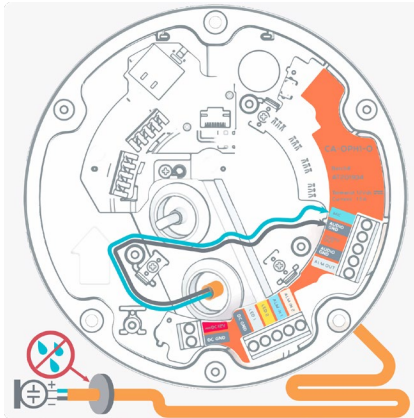


Figure 152 Audio Microphone

The electret microphone and the connecting cable should be electrically floating to minimize noise and hum from ground loops. Coaxial cable is best for noise immunity, but if twisted pair cable must be used, make sure to use two wires from the same pair for the microphone.



The microphone end must be IP66 to maintain the camera seal - moisture can wick up into the camera.

3.5.5.3 Audio – Speaker

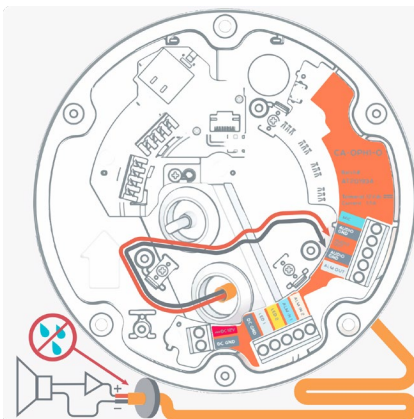


Figure 153 Audio Speaker

There is an audio out provided on the camera, these two screw terminals provide an unamplified output.

It is expected that a speaker with a built-in amplifier will be used, the negative should be connected to the nearest ground terminal and the positive should be connected to the audio out connection.

3.5.5.4 DC Power

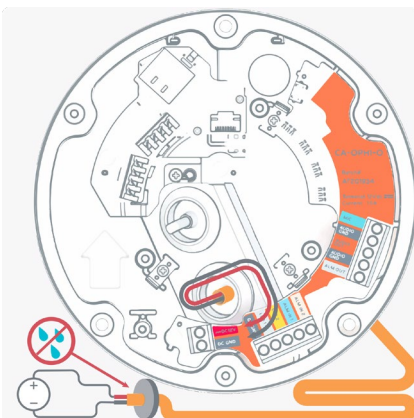


Figure 154 DC Power

The cable type required depends on the distance from the power supply to the camera placement - if in doubt consult a qualified person.

Direct DC Input. Use only a UL/CSA-approved LPS or NEC Class 8-28 VDC, 15W LPS, power supply (not supplied). The power source must be connected with the correct polarity.



Do not use an excess of 28 VDC from an external power supply. Doing so may damage the camera and void the warranty.

Do not connect the 12v power supply to the mains before wiring up the camera. Run the wires away from the camera placement and connect the power to the screw down terminals; Black is neutral, and Red is positive.

3.5.6 Heater Module



Figure 155 Camera Module Removal

Remove the camera module from its packaging.



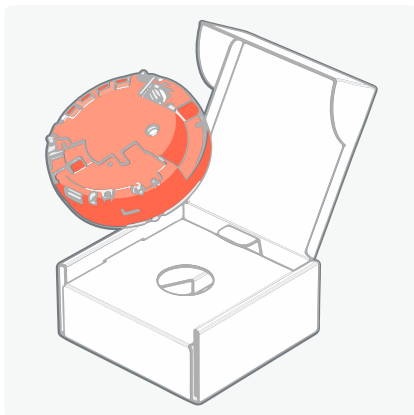
Figure 156 Camera Module Box

Fold the camera module box back up - we will use the box to support the camera module and protect the lens during installation of the heater module.



Remove and recycle the protective cover from the rear of the camera module.

Figure 157 Protective Cover Removal



Place the camera module back into the box with the lens facing down.

Figure 158 Camera Module Box

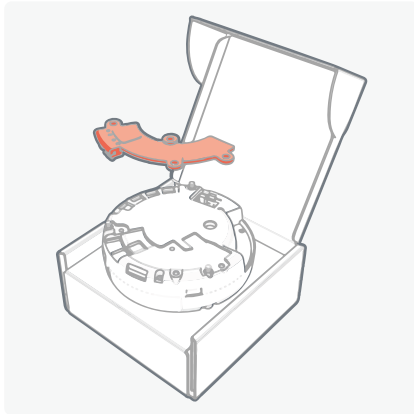


Ensure the protective lens cap is in place.



Take the heating module, remove and recycle the film that protects the thermal pad.

Figure 159 Remove Protective Film



Flip the heater module the other way up and align it to the 4 holes on the back of the camera.

Figure 160 Align Heater Module



Care should be taken as the pins are fragile.



Tighten the 4 screws using the hex tool.

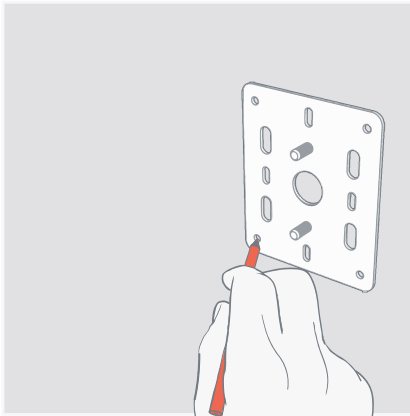
Figure 161 Secure the Heater Module



Place the camera module back into the box for protection until required for installation.

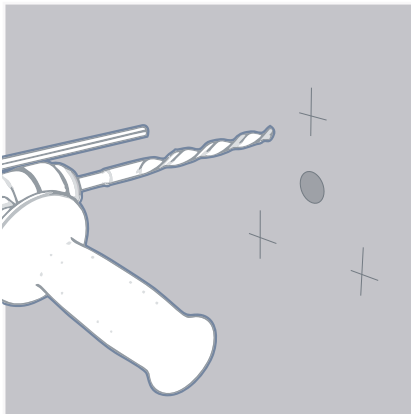
Figure 162 Camera Module Box

3.5.7 Outdoor Pendant Wall Mount Bracket



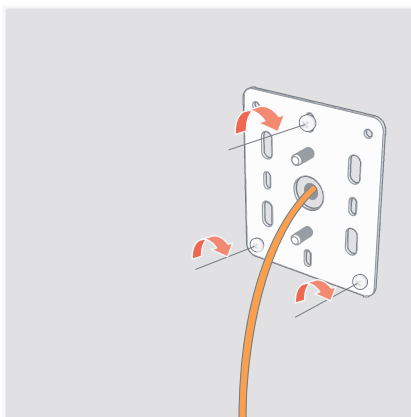
Using the wall mount plate, mark the holes on the wall.

Figure 163 Step 1 - Wall Mount Plate



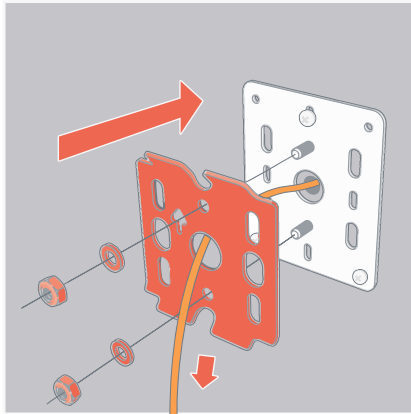
Drill the 3 mounting holes and hole for the ethernet cable.

Figure 164 Step 2 - Mounting Holes



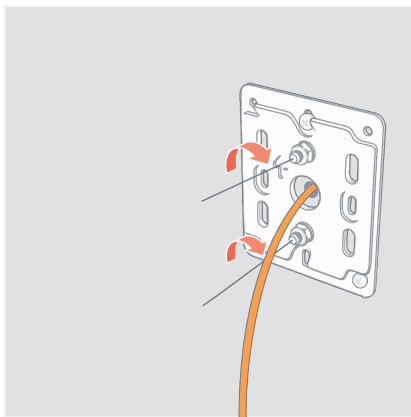
Using a 4.5mm or #9 pan head screw, fix the wall mount plate to the wall.

Figure 165 Step 3 - Fixing Wall Mount into the Wall



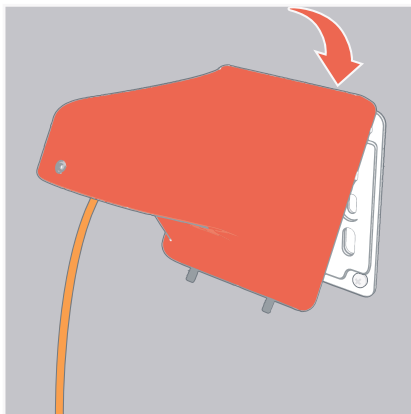
Feed the ethernet cable through the hole in the centre of the hook plate, push the hook plate onto the studs on the wall mount plate.

Figure 166 Step 4 - Feeding Ethernet Cable through the Hook Plate



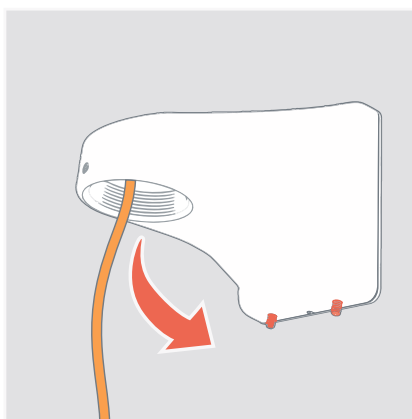
Use the provided nuts and washers to screw the hook plate in place.

Figure 167 Step 5 - Hook Plate Placement



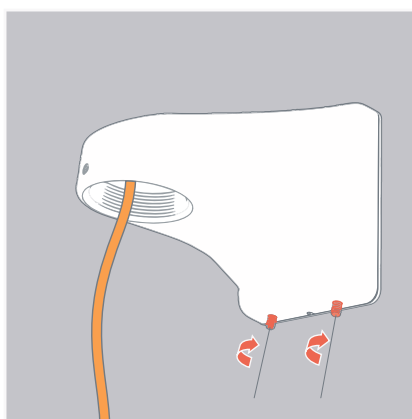
Taking the arm body feed the ethernet cable through the center, hook it onto the hook plate.

Figure 168 Step 6 - Arm Body



Pull the arm down so that the arm is at a right angle to the wall.

Figure 169 Step 7 - Arm at Right Angle



Screw in the two grub screws to secure the pendant arm.

Figure 170 Step 8 - Pendant Arm

Mount the camera using the 1 ½" thread adapter. Outdoor Pendant Mount Kit required.

3.5.8 Outdoor Pendant Corner Wall Mount Bracket

Assess an appropriate corner position for the mount, a corner of a building or wall is ideal.

Using appropriate fixings, mount the bracket to the wall.

Mount the wall plate to the corner bracket.

This bracket gives a suitable mount for the wall mount, then follow steps 4 - 8 above from section 3.4.5 (Outdoor Pendant Wall Mount Bracket).

3.5.9 Outdoor Pendant Pole Mount Bracket

Assess an appropriate pole to mount the bracket (it should not have an excessive taper for example).

Using the long hose clips around the pole, mount the bracket.

Mount the wall plate to the pole mount bracket.

This bracket gives a suitable mount for the wall mount, then follow steps 4 - 8 above from section 3.4.5 (Outdoor Pendant Wall Mount Bracket).

3.6 SD Card Support

3.6.1 Installation

Adding an SD card to the camera module is a simple and convenient way of adding local storage to your camera.

This can be done as part of the install or afterwards.

You will require a microSD card (max 512GB). It needs to be a minimum speed of class 10 (v10).



Due to the nature of video recording, a brand name microSD card is recommended.

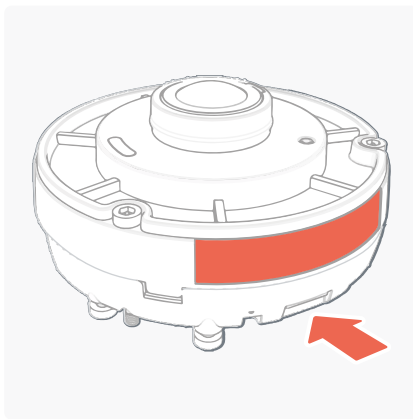


Figure 171 microSD Card Slot

On the side of the camera, below the MAC address and serial number is a small slot, this is for the SD card.

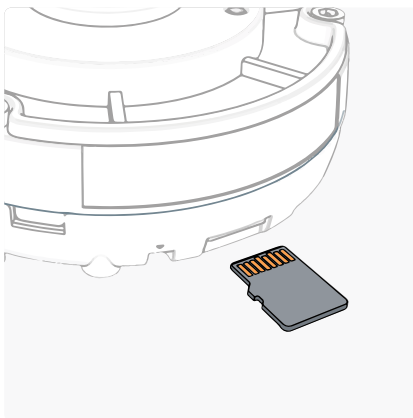
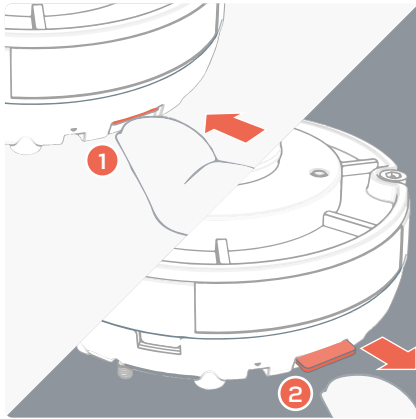


Figure 172 Inserting microSD Card

The SD card should be inserted with the gold contacts face up - towards the lens.



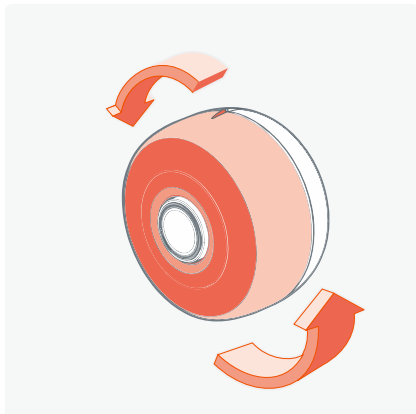
Push the card in, it will lock in place - to remove it, push again and it will spring eject.

Figure 173 microSD Card Insertion / Ejection

3.7 Uninstalling and Returns

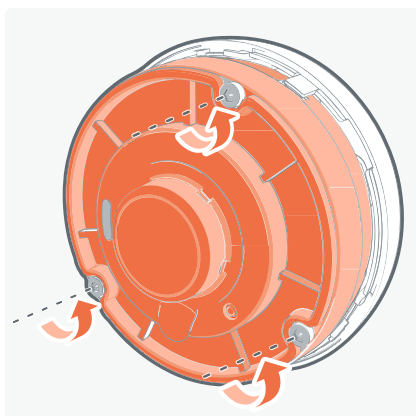
3.7.1 Indoor Camera Removal

The camera has been designed in a modular form. This should allow for simple replacement in case of an RMA. Only when advised, return the camera module rather than the whole enclosure. It is not necessary to remove the whole camera, just the camera module.



Remove the front cover.

Figure 174 Camera Front Cover

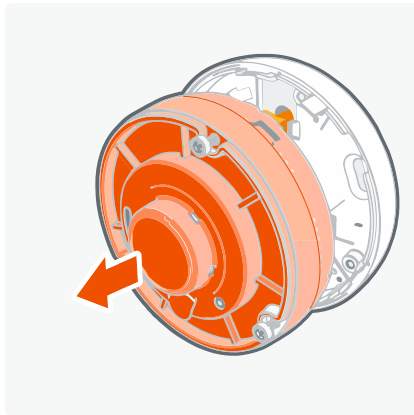


Undo the 3 retaining front screws with a security hex tool. Ensure the screws are fully disengaged.

Figure 175 Retaining Front Screws using Hex Tool



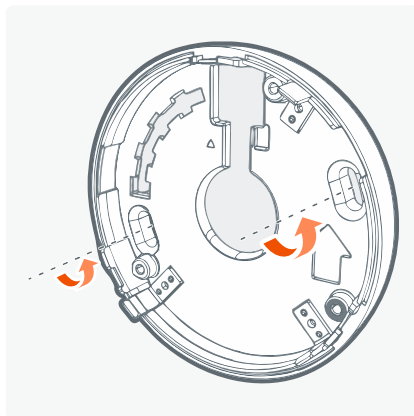
Care should be taken to support the camera.



Pull the camera module off the rear enclosure.

Figure 176 Camera Module off the Rear

Remove the ethernet cable by unplugging the RJ45 or unclip the punch down board.



To remove the rear enclosure, undo the two wall mount fixings.

Figure 177 Undo Wall Mount Fix

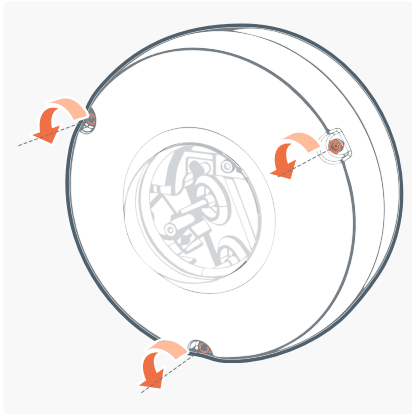
The punch down board will go through the holes in the rear enclosure.

The punch down board is easily cut off if required.

The camera rear is aluminum, the front cover is a polymer and the camera module are electrical device enclosed in aluminum. These parts are widely recycled.

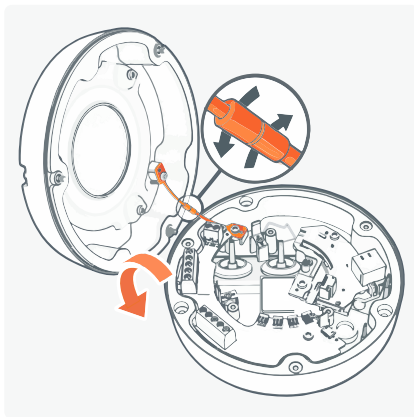
3.7.2 Outdoor Plus Camera Removal

The camera has been designed in a modular form. This should allow for simple replacement in case of RMA. Only when advised, simply return the camera module rather than the whole enclosure. It is not necessary to remove the whole camera, just the camera module.



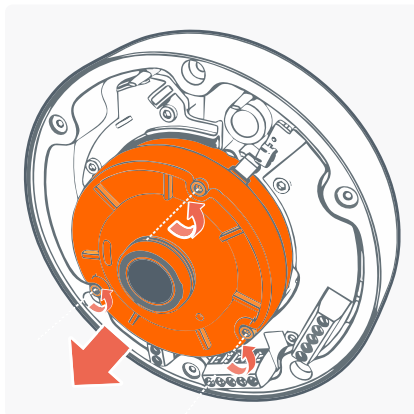
Undo the 3 retaining front screws with a security hex tool.

Figure 178 Retaining Front Screws using Hex Tool



Remove the front cover, undo the retaining tether.

Figure 179 Undo Retaining Tether



Undo the 3 retaining camera module screws with a security hex tool.

Figure 180 Remove camera module Screws using Hex Tool



Care should be taken to support the camera.

Pull the camera module off the rear.
Remove the ethernet cable by unplugging the RJ45 or unclip the punch down board.



Figure 181 Undo Wall Mounting

To remove the rear enclosure, undo the three wall mount fixings.

Remove the rear enclosure from the wall.

Pull the ethernet cable, gland and, if attached, the punch down board through the ethernet hole.

The gland and Punch down are easily cut off if required.

The camera rear is aluminum, the front cover is a polymer and the camera module are an electrical device enclosed in aluminum. These parts are widely recycled.

4. Camera Access

4.1 First Time Access – Discovery

4.1.1 Camera Discovery

To access the camera for the first time, you will need to discover the IP address of the camera.

This can be discovered using your ONVIF compatible VMS (for a list of supported VMS partners please go to <https://www.oncamgrandeye.com>), the Oncam C-Series Camera Configuration Tool (download from <https://www.oncamgrandeye.com/resources/c-series-camera-config-tool/>) or an IP Address scanning tool.

4.1.1.1 IP Address

The IP Address can be assigned to the camera in three different ways as described in the sections below. When the camera is configured with DHCP it responds using the DHCP provided address; if configured with a Static IP address, it responds with the static address, and it responds with its Link Local address if DHCP is not reachable or the Static IP address is in a different subnet to the discovering device.

4.1.1.1.1 DHCP

The factory default configuration of the camera is DHCP.

If a DHCP server is present, the camera will be allocated an IP Address, a Gateway address and DNS addresses, if these are available for discovery and connected to the camera.



When on DHCP, the camera also self-allocates a Link Local address - see Link Local.

4.1.1.1.2 Link Local

When a DHCP server is not found and the camera does not yet have a static IP address, after a period (up to 60 seconds) the camera will self-allocate a random Link Local address. This address can be used to communicate with the camera over HTTP / HTTPS and RTSP. The Link Local address is also used by the camera to respond if the Static IP address configured does not match the current network. If this is the case, the camera responds over Link Local.

To communicate with a camera on a Link Local address the PC must also have a Link Local address allocated. This can be done manually if needed in all PC operating systems. This can also be done within the Oncam Camera Configuration Tool by clicking on the Link Local toggle switch to turn the feature on.



The Link Local address is always accessible over HTTP / HTTPS and RTSP, and a previously assigned address is reused on the camera where possible. However, during boot up if the previous Link Local address is detected to be in use by another device, the camera will select the next available random Link Local address.

4.1.1.1.3 Static IP

The camera can be configured with a manual Static IP Address. This will also require the Gateway to be set to allow communication with the outside network, and DNS addresses to resolve DNS names if required. On first time setup, the camera will need to be discovered using DHCP or Link Local as described above. The Primary Administrator will need to create login credentials, log-into the camera and set up the Static IP Address. This can be configured in the Camera Web Interface; **Network > Network Configuration**.



If the camera is configured with a Static IP Address on a different subnet than the local network, either use the camera's Link Local address, which will be provided in discovery, or simply force a Physical Reset to Factory Defaults. See *Section 5.8.3.3 Reset to Factory Defaults*

4.1.1.2 Camera Configuration Tool (CCT)

4.1.1.2.1 Download

To discover the camera's IP Address, download the C- Series Camera Configuration Tool from <https://www.oncamgrandeye.com/resources/c-series-camera-config-tool/>





Please ensure you meet the minimum system requirements and have the latest Edge Browser (90 or above) installed.

4.1.1.2.2 Installation

Follow the on-screen instructions to install the application.

4.1.1.2.3 Discovery

Open the Camera Configuration Tool on a PC that is on the same network as the cameras. As soon as the App is initiated it will discover the Oncam C-Series cameras on your network and display key information including the Friendly name, Model number, MAC Address and most importantly the IP Address of the camera. If no C-Series cameras populate in the discovery

pane, left click the Link Local toggle switch  to turn on Link Local discovery. The switch should change from light grey to orange when Link Local discovery is enabled. To update the list, select **Refresh Discovery icon**  in the top right-hand corner.



The discovered camera list is displayed on initiation of the Camera Configuration Tool, and then only when the Refresh discovery icon is manually selected.

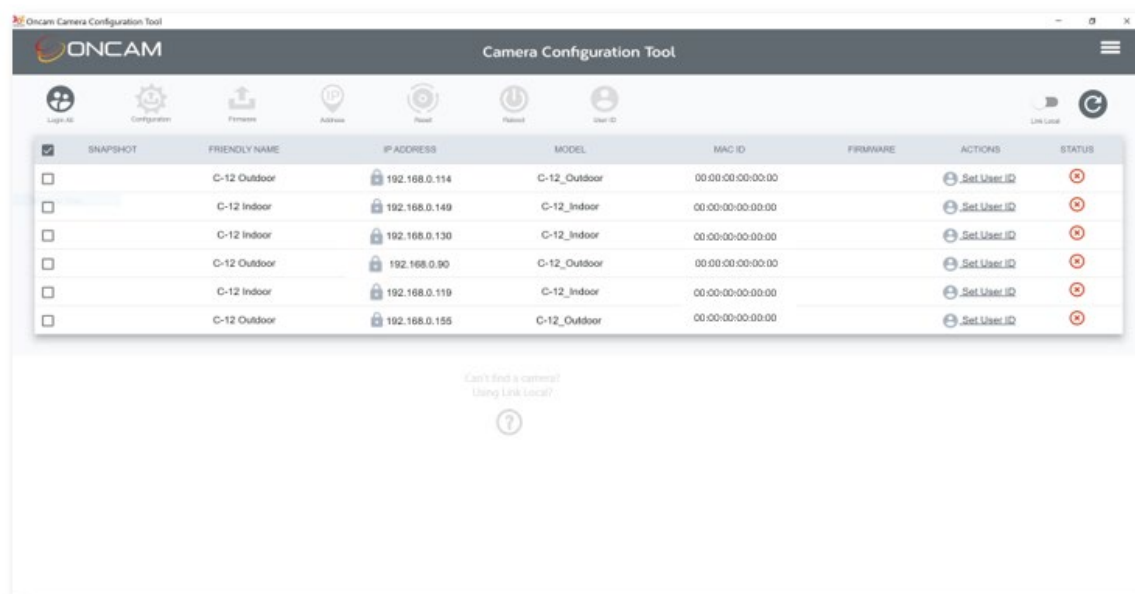


Figure 182 CCT Discovery

4.1.1.3 Video Management Systems (VMS)

4.1.1.3.1 Discovery

The camera's IP Address can be discovered by an ONVIF compatible VMS (for a list of supported VMS partners please visit <https://www.oncamgrandeye.com/>), however, before the VMS can communicate with the camera, the username and password for the Primary Administrator will need to be set via the Camera Web Interface or the C-Series Camera Configuration Tool.

4.2 First Time Access - Set Primary Administrator Username and Password

4.2.1.1 Camera Web Interface

4.2.1.1.1 Connecting to the Camera

Once you have discovered the IP Address of the camera, you will need to set the Primary Administrator Username and Password before you can access the camera. This can be done via the Camera Web Interface.

Connect to the camera on your network by entering the camera IP address (for example, <http://192.168.0.114>) into the address bar of a compatible web browser running on a PC on the same network. Supported browsers are Chrome, Firefox, Edge or Safari. Please check datasheet for latest supported minimum versions.

The first response from the camera will be an authentication screen requesting the Primary Administrator to set up a Username and Password. For enhanced security, default usernames and passwords are not supported, users will be required to set a secure password, which will need to meet the minimum requirement stated below. Please follow the steps below to set up your login credentials.

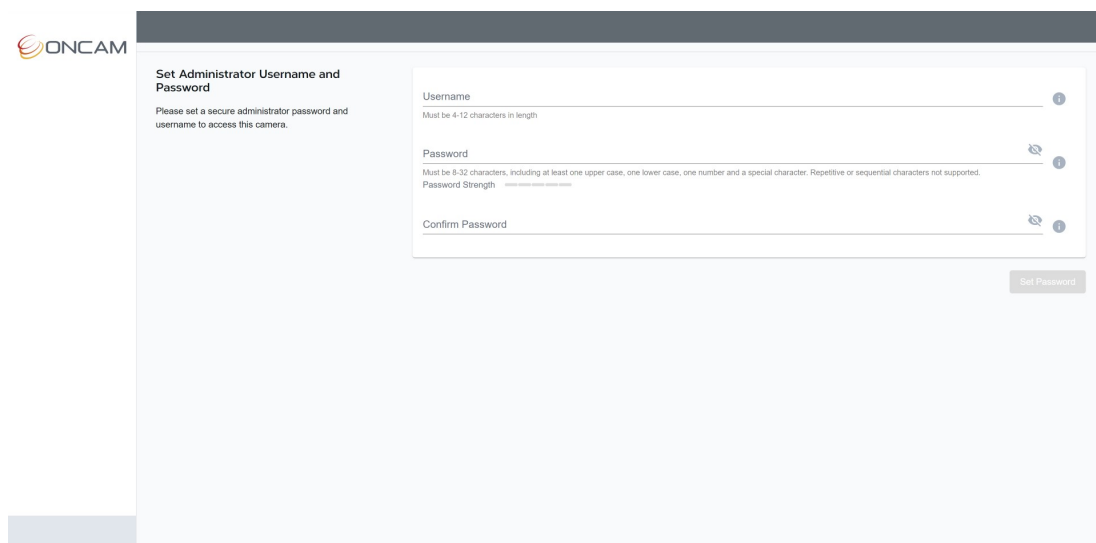
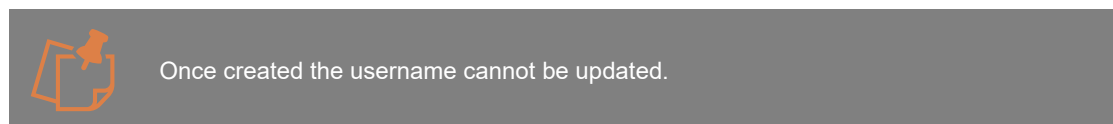


Figure 183 Camera Web Interface, Set Password

4.2.1.1.2 Username

Set an easily identifiable and memorable username for the Primary Administrator. The name must be a between 4-12 characters in length. The username can consist of uppercase letters (A-Z), lowercase letters (a-z) and numbers (0-9). Special characters are not supported.




4.2.1.1.3 Password

It is important to always set and use a secure password to access the camera, therefore the camera enforces strong password criteria for all user accounts as specified below:

- Minimum of 8 characters and a maximum of 32.
- The password requires at least one uppercase letter (A-Z), one lowercase letter (a-z), one number (0-9) and one special character. The following special characters are supported (~!@#\$%^&* -+=`|(){}[]:;'.?/).



For enhanced security repetitive or sequential characters (e.g. 'aaa', '123', 'abc' or '321') are no longer supported when creating a new password. V2.0.x firmware or above required to access this feature. For existing installations where repetitive or sequential characters have been setup using Firmware prior to V2.x, these will still be supported, however any new users created will need to follow the new security criteria for password setting.

If you would like to check the Password you have entered and it is safe to do so, select the view icon  and the password will be displayed. Select it again and the password will be hidden.

4.2.1.1.4 Strength Indicator

For guidance, the strength of the password combination is displayed below the password. Use the combination of upper and lower case alphabetic, numeric and special characters until the password strength is strong enough.

4.2.1.1.5 Confirm Password

Please retype your password to confirm it has been correctly entered, if the passwords do not match a notification will appear.



The Primary Administrator account is considered the root account for the camera and therefore cannot be deleted. To remove this account and replace it with a Primary Administrator with a different name, the camera must be **Reset to Factory Defaults (All Settings or User Accounts Only)**, accessible via **Device > Maintenance/Support**.

4.2.1.2 Camera Configuration Tool (CCT)

4.2.1.2.1 Single or multiple Cameras

The Camera Configuration Tool can be used to create the Primary Administrator username and password for first time use of the camera. Using this powerful tool, the same login details can be created for multiple cameras at the same time, saving valuable time and resource during installation.

4.2.1.2.2 Setting username and password

After the C-Series cameras have been discovered, any cameras that require login credentials to be created will display **Set User ID** under the **ACTIONS** column. Click the check box next to each camera you want create credentials for and select the **User ID** option from the top menu. For enhanced security, default username and passwords are not supported. Users will be required to set a secure password, which will need to meet the minimum requirement below. Please follow these steps to set up your login credentials.

Figure 184 CCT, Set Password

4.2.1.2.3 Username

Set an easily identifiable and memorable username for the Primary Administrator. The name must be a between 4-12 characters in length. The username can consist of uppercase letters (A-Z), lowercase letters (a-z) and numbers (0-9). Special characters are not supported.

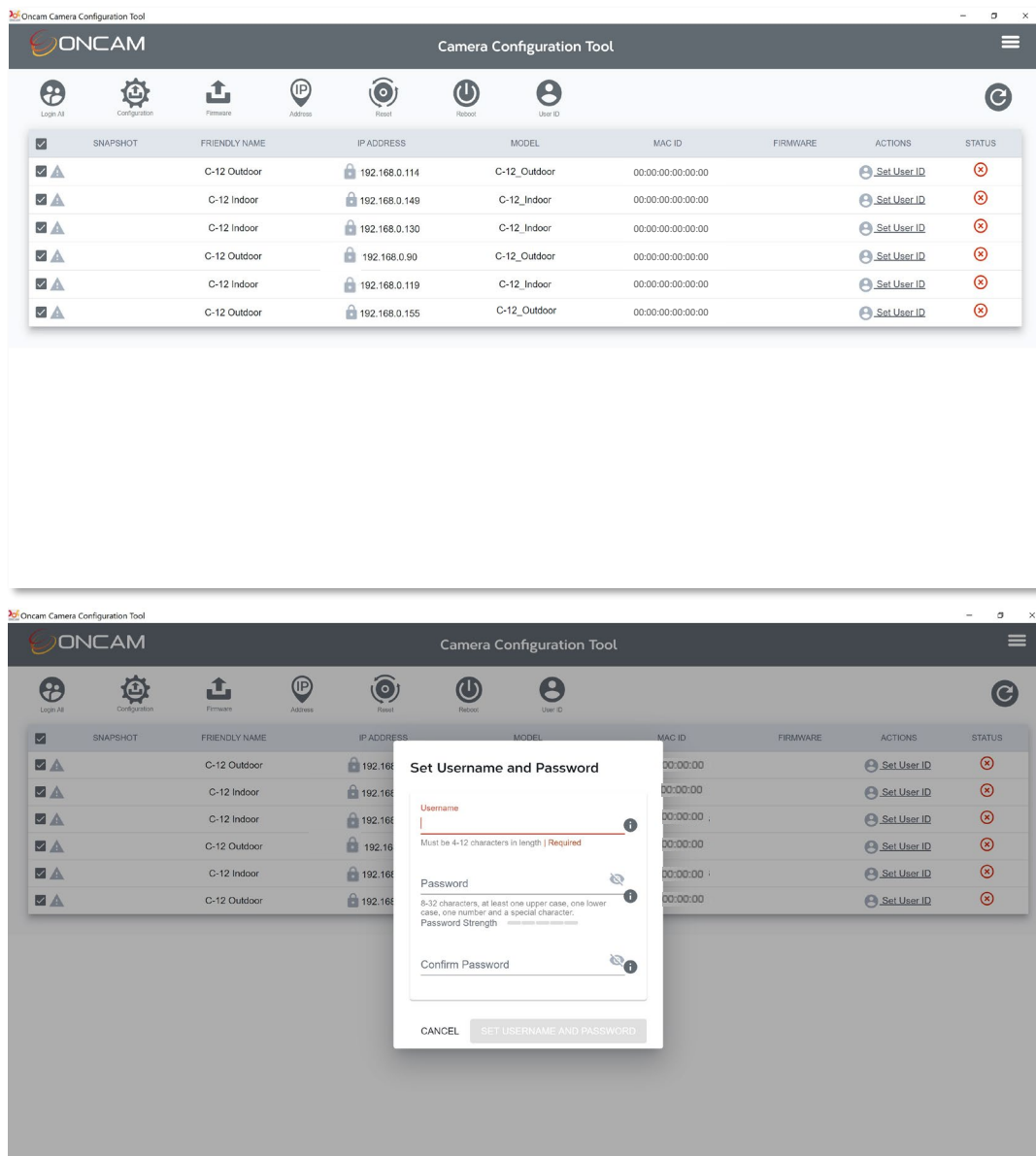


Figure 185 CCT Username and Password Setting



Once created the username cannot be updated.

4.2.1.2.4 Password

It is important to always set and use a secure password to access the camera, therefore the camera enforces strong password criteria for all user accounts as specified below:

- Minimum of 8 characters and a maximum of 32.
- The password requires at least one uppercase letter (A-Z), one lowercase letter (a-z), one number (0-9) and one special character. The following special characters are supported (~!@#\$%^&* -+=`|(){}[]:;'.?/).



For enhanced security repetitive or sequential characters (e.g. 'aaa', '123', 'abc' or '321') are no longer supported when creating a new password. V2.0.x firmware or above required to access this feature. For existing installations where repetitive or sequential characters have been setup using Firmware prior to V2.x, these will still be supported, however any new users created will need to follow the new security criteria for password setting.

4.2.1.2.5 Strength Indicator

For guidance, the strength of the password combination is displayed below the password. Use the combination of upper and lower case alphabetic, numeric, and special characters until the password strength is strong enough.

4.2.1.2.6 Confirm Password

Please retype your password to confirm it has been correctly entered, if the passwords do not match a notification will appear.

4.2.1.2.7 Set Password Confirmation

Click **Set Username and Password**, the credentials will be saved, and you will be taken back to the main Camera Configuration Tool discovery page. The **Logout** option will now be displayed under the ACTIONS column for the selected cameras

SNAPSHOT	FRIENDLY NAME	IP ADDRESS	MODEL	MAC ID	FIRMWARE	ACTIONS	STATUS
	C-12 Outdoor	192.168.0.114	C-12_Outdoor	00:00:00:00:00:00	C-12_1.1.0		
	C-12 Indoor	192.168.0.149	C-12_Indoor	00:00:00:00:00:00	C-12_1.1.0		
	C-12 Indoor	192.168.0.130	C-12_Indoor	00:00:00:00:00:00	C-12_1.1.0		
	C-12 Outdoor	192.168.0.90	C-12_Outdoor	00:00:00:00:00:00	C-12_1.1.0		
	C-12 Indoor	192.168.0.119	C-12_Indoor	00:00:00:00:00:00	C-12_1.1.0		
	C-12 Outdoor	192.168.0.155	C-12_Outdoor	00:00:00:00:00:00	C-12_1.1.0		

Figure 186 CCT Password Confirmation



Set Username & Password can only be set from the CCT as part of first-time camera access. If you wish to update user credentials, select the configure option under the ACTIONS column for the camera and update the password in the user section of the Camera Web Interface. Usernames cannot be updated.

4.2.1.3 Accessing the Camera

Using the login credentials created, the camera is now ready to be configured using your compatible VMS, the Camera Web Interface or the C-Series Camera Configuration tool.

5. Camera Configuration

5.1 Dashboard – Camera Web Interface

5.1.1 Overview

Once you have created your Primary Administrator username and password, you can use these credentials to set up and configure the camera in one of the following ways:

1. ONVIF commands using your compatible VMS
2. The Camera Web Interface
3. The Camera Configuration Tool (opens Camera Web Interface within the tool)

To access the Camera Web Interface, type the IP address of the camera into a compatible web browser. Supported browsers are Chrome, Firefox, Edge or Safari. Please check datasheet for latest supported minimum versions. Enter your username and password.



The Camera Web interface can also be accessed via the Camera Configuration Tool. Once you have logged into your camera click configure under ACTIONS next to the camera and this will open up the Camera Web Interface from within the configuration tool.

You will be presented with the main camera dashboard. From this page you can access all camera configuration settings, test the live stream, and set up the camera based on your requirements.



Only Administrator level users will have access to camera settings, users with operator and user level privileges will only be able to view the dashboard page and the live stream.

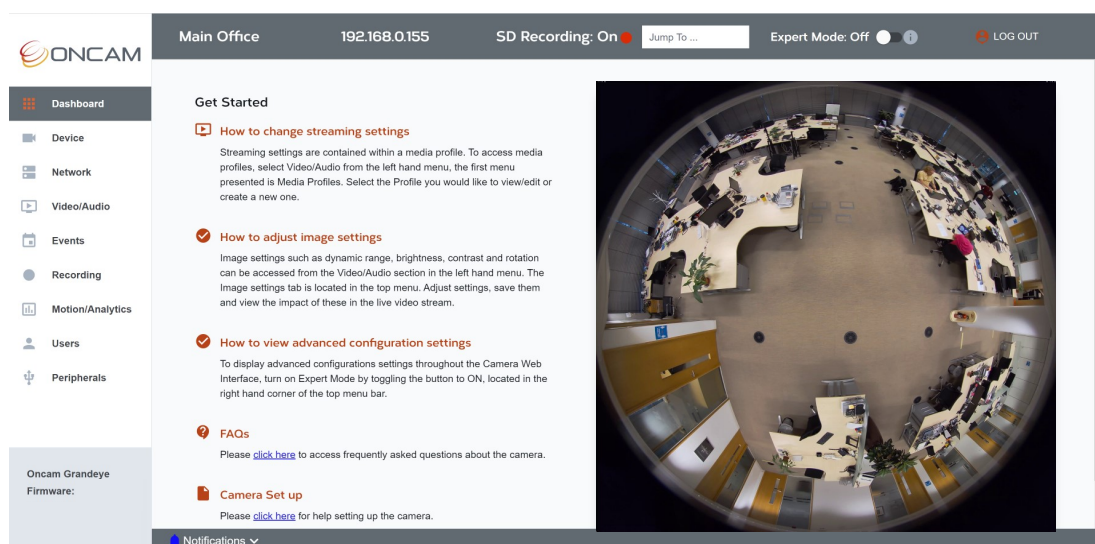



Figure 187 Dashboard Overview

5.1.1.1 Test the Live Stream

A snapshot of the camera image will be displayed on the right-hand side of the screen. To view the live stream, click the play button located on the center of the image. The video can be maximized by selecting the icon  in the bottom right hand corner of the image to fill the

screen. To minimize the live video and return to the dashboard. Press **Escape** on your keyboard or move your mouse towards the top of the screen at the center and click the X icon that appears.



This stream is designed for test and configuration purposes only and therefore will display a low-resolution image of 512 x 512.




Figure 188 Dashboard Overview Fullscreen

5.1.1.2 Connecting Directly to Camera Streams

Another way to test the camera stream is to connect directly to camera streams (MJPEG, H.264 & H.265) using your media player. For this you will require your camera's IP address and the appropriate URL detailed in **Appendix A**

5.1.1.3 Getting Started

To help easily navigate around the user interface, several tool bars and quick access links are available. You will also notice that many of the settings have helpful hints displayed, with more

detailed information about the settings available if you hover over the information  icon. The get started section in the dashboard briefly describes where to go to access important features such as creating and editing streaming settings, adjusting image settings, and view advanced configuration settings by enabling the Expert Mode. There are also links to the Camera FAQ's and Set up instructions.

5.1.1.4 Camera Configuration Access

The Camera Web Interface is designed to be intuitive and easy to use. The left-hand navigational bar has been created to provide quick access to all the main camera settings as described below:

Device - Identification, Date & Time, Support, Firmware update, Security and Licensing

Network - Standard and Advanced network set up

Video/Audio – Camera Modes and Media Profiles for Streaming Video, Audio and Metadata, Image settings, Overlays, Global Compression and Audio

Events - Alarm rule creation based on event triggers

Recording - Create, manage and search continuous and event recordings on the SD card

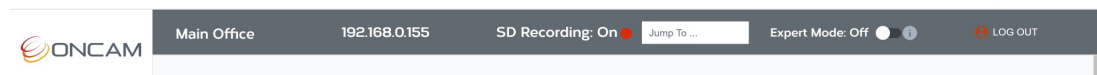
Motion / Analytics - Create and configure analytic rules to run on the camera

Users - User access control

Peripherals - Input and output connections management on the camera (Plus version of camera required)

5.1.1.5 Camera Information Bar

The top bar of the dashboard displays key camera information in the form of, the camera-friendly name, its IP Address and SD recording status. The following three functions are also displayed on this bar:



5.1.1.5.1 Jump To

If you know the specific area of the web interface you want to go to, then simply type in the beginning of it (e.g. Device) in the **Jump to** search bar, and all the related options in the Camera Web Interface will be displayed, click the area you want to go to and you will be taken directly to that section.

5.1.1.5.2 Expert Mode

The Camera Web Interface is very comprehensive to enable full camera control. As some of the features are only required by advanced users, the interface is designed to hide the advanced settings tabs by default. When required these can be easily unhidden from the dashboard by an Admin user by enabling the **Expert Mode** toggle button in the top menu bar to **On**. This can be accessed from anywhere in the Interface, however whenever the status is changed (enabled/disabled) it will return to the dashboard screen.

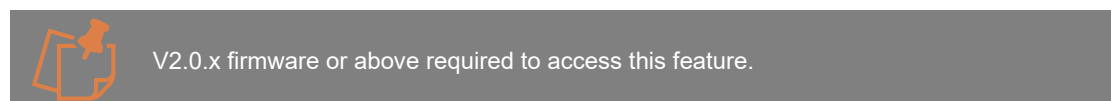
When this feature is off the following tabs are hidden:

Device - Security and Licenses

Network - Advanced Network Configuration

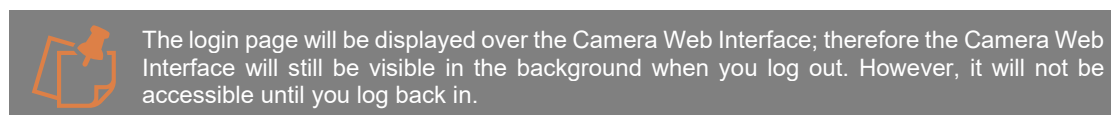
Video/Audio - Global StreamLite Compression – tab is visible, but sections are rolled up.

Motion / Analytics – Global Settings



5.1.1.5.3 Logout

The Camera Web Interface will automatically log you out after 15 minutes of inactivity. When you have completed your changes, it is recommended to log out using the button in the top right-hand corner on the information bar. Click it once and you will be logged out.



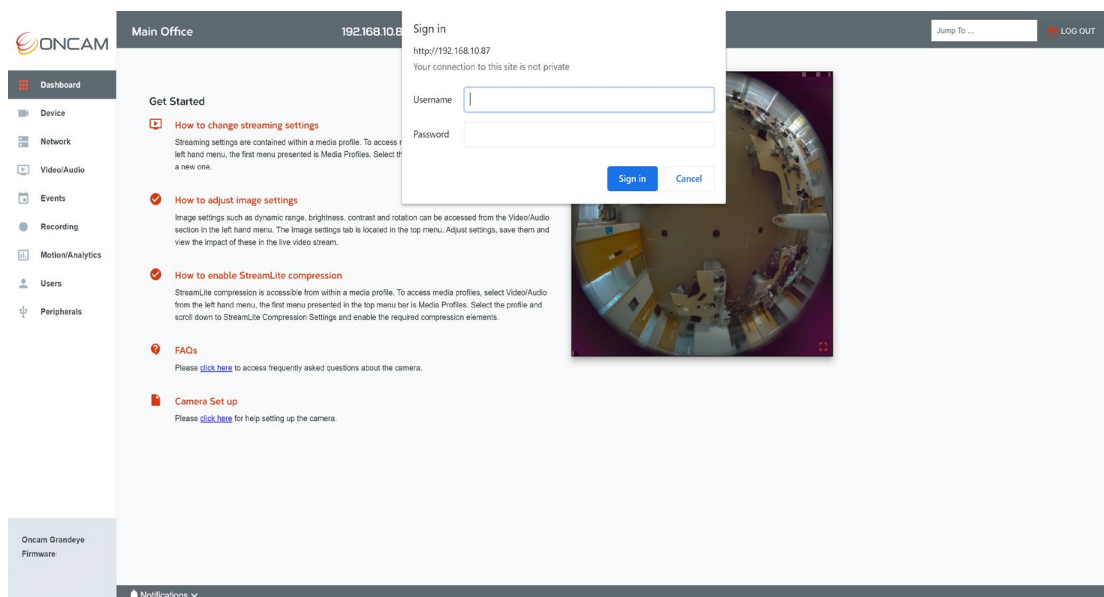


Figure 189 Dashboard Logout

5.1.1.6 Notifications Bar

The notification bar is located at the bottom of the screen and displays events, and the API status of commands to the camera. The notification bar's bell icon is displayed in red in case of events or API error and for successful event notifications the color will be blue. Click the notification bar to open an in-browser window to display the notification messages for more information of the event. Once a message has been read it will turn grey.

5.2 Network

5.2.1 Network Configuration

5.2.1.1 Network Settings

Configure essential camera network settings such as IP address, DNS, Gateway and NTP.

The following settings are accessible:

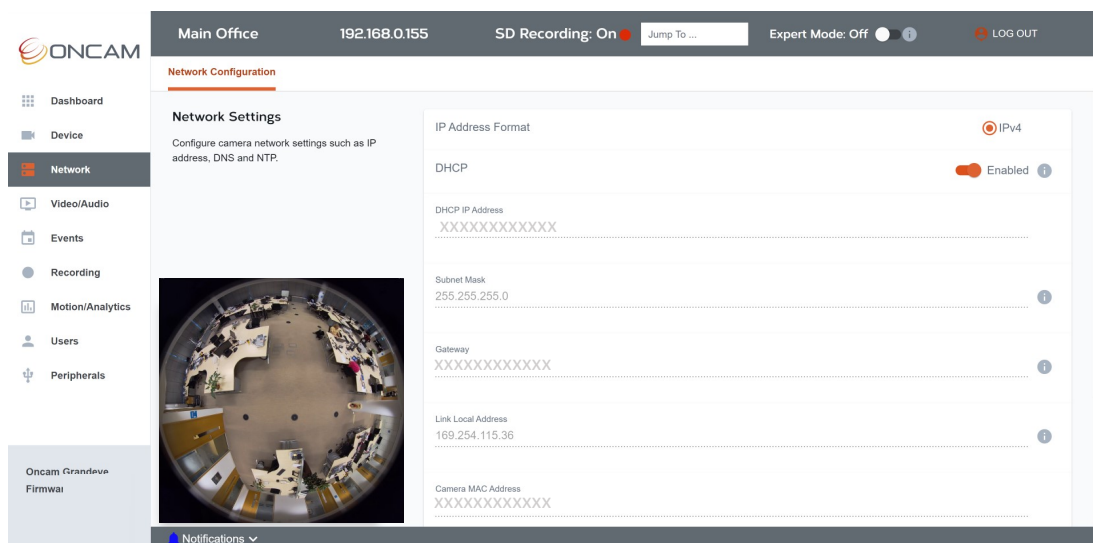


Figure 190 Network Configuration

5.2.1.2 IP Address Format

The supported IP address format is IPv4 only.

5.2.1.3 DHCP

Allows IP address assignment by an external DHCP server. Switching this off means that the static IP address will have to be assigned instead. Default is ON.

5.2.1.3.1 DHCP IP Address

If DHCP is enabled, the **DHCP IP Address** field displays the IP address that has been obtained by the DHCP server and assigned to the network interface of the camera.

5.2.1.3.2 Static IP Address

If DHCP is disabled, enter the fixed IP address for the camera to use on the network.



Ensure another device is not already using this IP Address.

5.2.1.3.3 Subnet Mask

Defines the range of IP addresses available within the network and must match the settings of the current network.

This is set to the value received from the DHCP server if the DHCP is enabled.

If DHCP is disabled, please manually enter the required range.

5.2.1.3.4 Gateway

The default gateway for network traffic to devices that are not on the local network.

This is automatically set if DHCP is enabled. The value assigned from the DHCP server will overwrite any previous value that was set manually.

If DHCP is disabled, set the Gateway manually for Static IP.

5.2.1.4 Link Local address

This is a unique address self-allocated by the camera as a fallback address to allow communication with other devices on the local network.

When a DHCP server is not found and the camera does not yet have a static IP address, after a period (up to 60 seconds) the camera will self-allocate a random Link Local address. In the absence of a DHCP server, this is the only means to communicate with the camera. The Link Local address is used by the camera to respond if the Static IP address configured does not match the current network.

To communicate with a camera on a Link Local address the PC must also have a Link Local address configured. This can be done manually if needed in all PC operating systems.

5.2.1.5 DNS

Select Auto to make the camera find the DNS server on the network automatically via DHCP or select manual to enter a specific IP address for the DNS server to be used. If DNS is set to manual but the IP address is retrieved via DHCP, the camera will reassign the address based on the settings received from the DHCP server.

5.2.1.6 NTP Server

Enables the camera to communicate with an NTP server to synchronize the camera clock time to the global network time. Default is disabled, (to enable via the camera interface, go to Device > Date/Time > NTP). The NTP server is configured by default to 0.beevik-ntp.pool.ntp.org.

NTP will update the cameras clock on reboot and henceforth every 12 hours if the camera time differs by more than 1 minute. Any running camera streams will be restarted to sync the stream to the correct NTP time.

5.2.1.6.1 Manual

Enter the domain name or IP address of the NTP server.

5.2.1.6.2 Auto

This feature does not currently function correctly. Please enter the NTP address manually as described above.

5.2.2 Advanced Network Configuration

5.2.2.1 Advanced Network Settings

Configure advanced camera network settings such as TCP Ports.

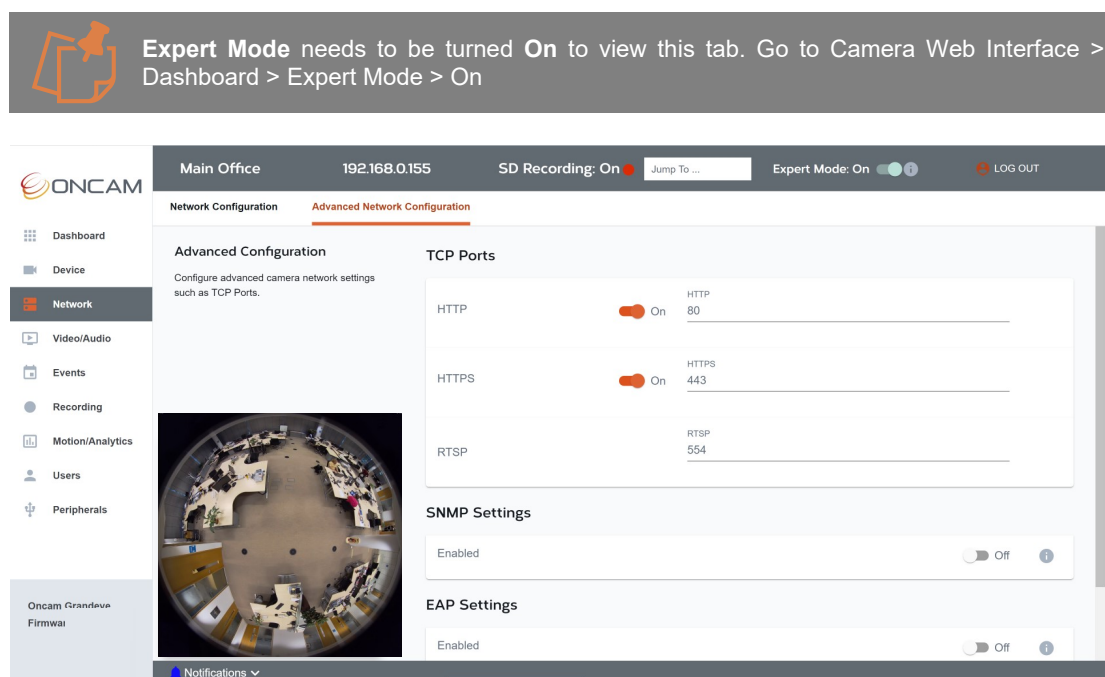


Figure 191 Advanced Network Configuration

5.2.2.2 TCP Ports

Define the inbound ports used by the camera for its essential communications.

5.2.2.2.1 HTTP

Defines the port used for HTTP traffic to the camera. HTTP is used to access the Camera Web Interface and settings, and HTTP is the default protocol for communications to the camera via ONVIF. Instead of the standard port, an alternate port number can be used if required. Default is 80. Any user defined port needs to be in the range of 1024 – 65535.

Can be disabled if not required to tighten network security on the camera but cannot be disabled at the same time as HTTPS.

5.2.2.2.2 HTTPS

Defines the port used for HTTPS traffic to the camera. HTTPS is used to securely access the Camera Web Interface and settings over TLS. Instead of standard port, an alternate port number can be used if required. Default is 443.

Can be disabled if not required but cannot be disabled at the same time as HTTP. The mode for maximum security is HTTPS enabled and HTTP disabled.

5.2.2.2.3 RTSP

Defines the port used for Real Time Streaming Protocol (RTSP), which is the protocol used by the camera for streaming video, audio and metadata. Instead of standard port, an alternate port number can be used if required. Default is 554.

5.2.2.2.4 SNMP Settings - v2c or v3

Streaming Simple Network Management Protocol (SNMP) is an application-layer protocol used to manage and monitor network devices and their functions. SNMP version 2c or version 3 is supported by the camera.

The following SNMP settings can be configured here.

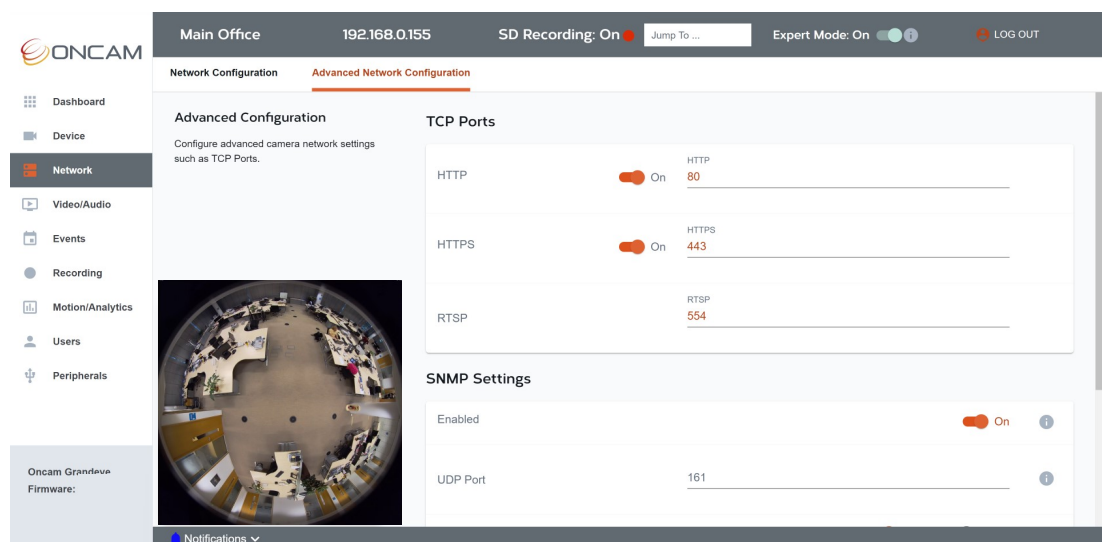


Figure 192 Advanced Network SNMP

5.2.2.2.4.1 Enable SNMP

Enable SNMP by toggling to **On**

5.2.2.2.4.2 UDP Port

Select your UDP port number, the available range is 1024 -65535. Default is 161.

5.2.2.2.4.3 SNMP Version

Select the version of SNMP between v2c or v3


If you select v3 you will be requested to set up a username and password.

5.2.2.2.4.4 Username

The username can be a maximum of 32 characters.

5.2.2.2.4.5 Password

- Minimum of 8 characters and a maximum of 32.

If you would like to check the Password you have entered and it is safe to do so, select the view icon  and the password will be displayed. Select it again and the password will be hidden.

5.2.2.2.4.6 Save Changes

Save your changes to apply them

5.2.2.2.4.7 SNMP-V2c Connection Example:

Activate SNMP V2 via Camera Web Interface as above.

Use MIB Browser tool, Load ONCAM-MIB module provided in the firmware package, complete connection settings, Enter Camera IP, Port 161, Read Community "public" and Write community "private"

You can browse the ONCAM-MIB module by running various types of GET commands

5.2.2.2.4.8 SNMP-V3 Connection Example :

Activate SNMP V3 via Camera Web Interface as above.

Use MIB Browser tool, Load ONCAM-MIB module provided in the firmware package, complete connection settings, Enter Camera IP, Port 161, Username, Security Level "AuthNoPriv", Auth Protocol "MD5" Auth Password

You can browse the ONCAM-MIB module by running various types of GET commands

5.2.2.2.5 EAP Settings - 802.1x EAP-MD5 / EAP-TLS / EAP-PEAP

802.1x authentication standard is used for passing Extensible Authentication Protocol (EAP) over Local Area Networks (LAN). It provides an encrypted EAP tunnel that prevents outside users from intercepting information. The camera supports the MD5, TLS and PEAP authentication types.

The following EAP settings can be configured here.

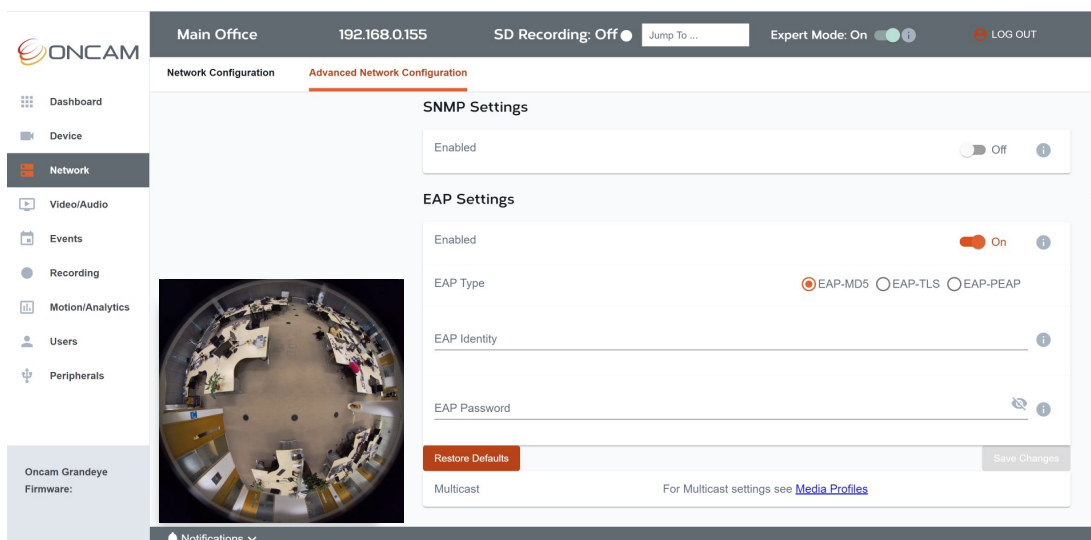


Figure 193 Advanced Network EAP

5.2.2.2.5.1 Enable EAP

Enable EAP by toggling to **On**

5.2.2.2.5.2 EAP Type


Select the EAP type. Choose from MD5, TLS or PEAP.

5.2.2.2.5.3 EAP Identity

The name can be a maximum of 32 characters.

5.2.2.2.5.4 EAP Password


Minimum of 8 characters and a maximum of 32.

If you would like to check the Password you have entered and it is safe to do so, select the view icon  and the password will be displayed. Select it again and the password will be hidden

5.2.2.2.5.5 For EAP- TLS or PEAP the following options will need to be set.

5.2.2.2.5.6 Client Key.

Upload Client Key Certificate file
Minimum of 8 characters and a maximum of 32.

If you would like to check the Password you have entered and it is safe to do so, select the view icon  and the password will be displayed. Select it again and the password will be hidden

5.2.2.2.5.7 Anonymous Identity.

Enter the anonymous identity for EAP so that the authenticator can choose the correct authentication server to process the credentials. 8-32 characters in length.

5.2.2.2.5.8 Certificate Authority Certificate.

Upload the Digital Security Certificate Authority file.

5.2.2.2.5.9 Client Certificate.

Upload the Client-Side Certificate file

5.3 Video/Audio Streaming

5.3.1 Media Profiles

5.3.1.1 Overview

The C-Series camera can output a 360-degree Fisheye and/or onboard dewarped views dependent on the use case.



V2.0.x firmware or above required to access this feature.

Supported dewarped views are: Panoramic+, Corridor+, T Corridor+ and VCams, explained in more detail below.

During initial configuration decide on how to set up the camera using Camera Modes.

Camera Modes are accessible via the Camera Web Interface > Video/Audio > Media Profiles > Camera Modes.

5.3.1.2 Camera Modes

Camera Modes control which types of stream the camera can produce simultaneously.



V2.0.x firmware or above required to access this feature.

Performance Mode enables selection between a High Speed single stream, at up to 60 fps, or Multiple Streams (max four), at up to 30 fps.

Image Output Modes offer the choice of Fisheye only, Panoramic+ only, or Multi-Mode where combinations of these views and various other dewarped views are possible.

The modes chosen determines which media profiles are available, and the view type, frame rate and resolution options within them.

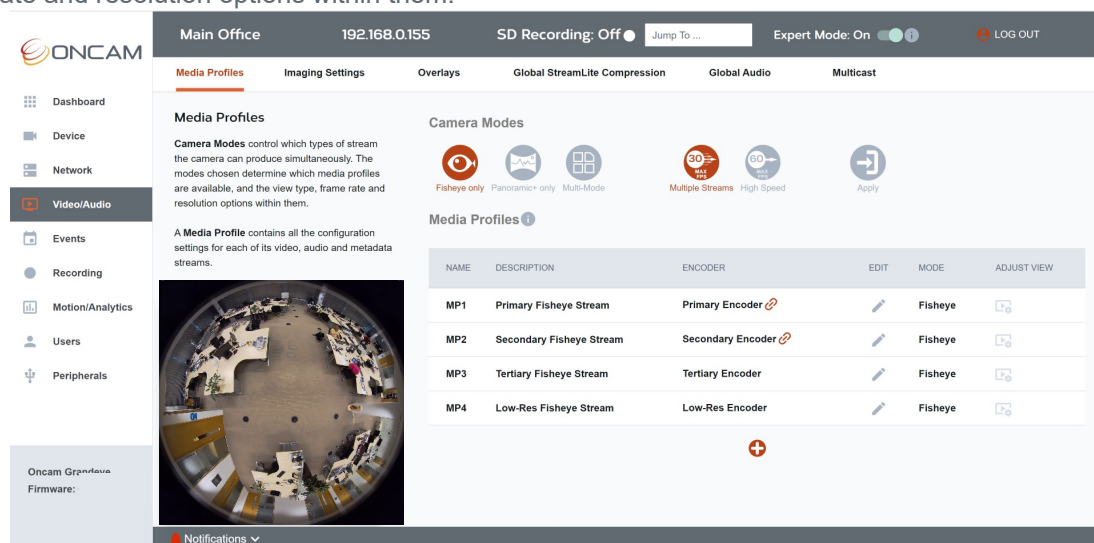


Figure 194 Media Profile Overview

5.3.1.2.1 Performance Mode

Select the Performance Mode of the camera. This will impact the number of available streams, resolutions, and speed.

High Speed - A single stream only is available and can achieve up to 60 fps dependent on selected resolution.



In High Speed Mode when a stream above 30fps is selected, TrueDetail HDR (5.3.2.3) is automatically disabled.

Multiple Streams – A maximum of four streams are supported simultaneously at up to 30 fps, the fps varies by encoder see: 5.3.1.6.3.

Hovering over each option will provide a pop-up with further information about the option.

Default is **Multiple Streams**. If a different Performance Mode is selected, the **Apply** button will change color. Select it to apply the change. A pop-up warning message will be displayed, select **Confirm** to apply the change.

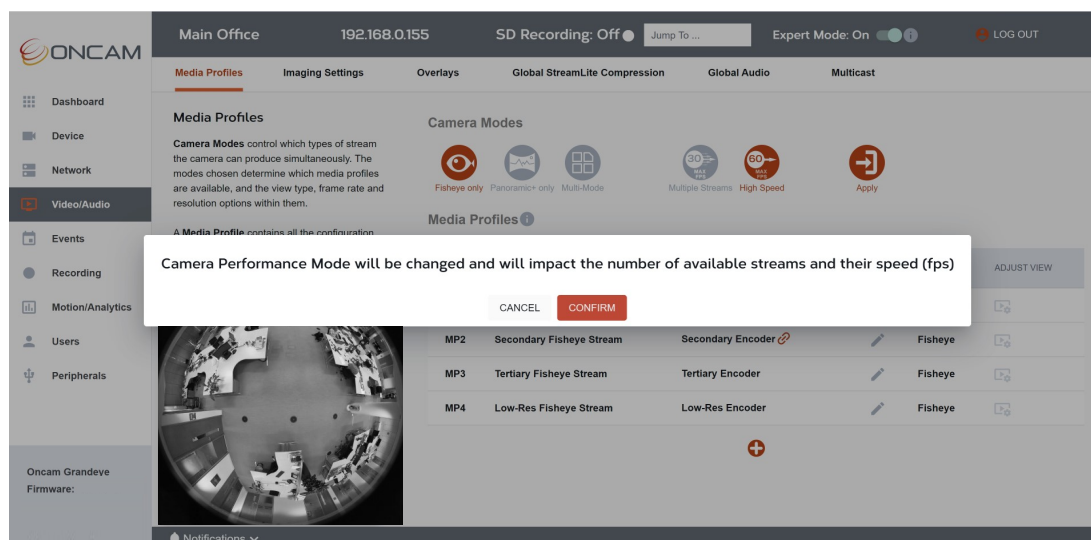


Figure 195 Media Profiles, Camera Mode Change Request

A countdown will be displayed while the change is being applied to the camera, once complete the web page will automatically refresh and the Dashboard displayed. Navigate to Video/Audio using the left-hand menu. The selected Performance Mode and associated media profiles will be displayed, in the example below, Fisheye only, High Speed.

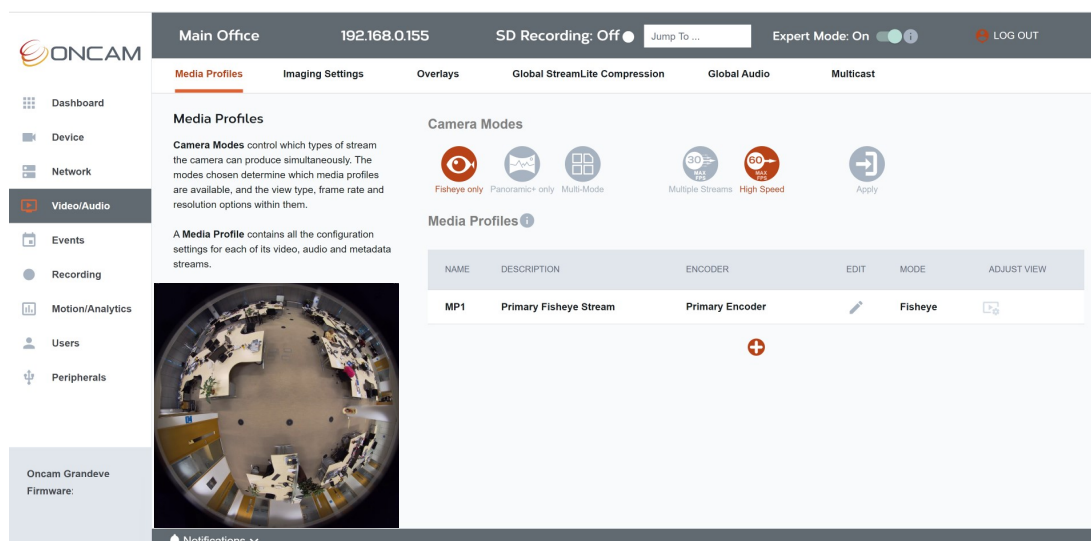


Figure 196 Media Profiles, Camera Mode Changed

5.3.1.2.2 Image Output Mode

Select the most appropriate Image Output mode (Video Source Mode) of the camera, from the following options:

Fisheye only camera – All streams will be 360° Fisheye.

Panoramic+ only camera – All streams will be 180° Panoramic+.

Multi-Mode camera – All streams can display a different view, up to 4 different streams can be supported simultaneously.

**Multi-Mode example:**

Primary Stream: 180° Panoramic+ view for easier viewing on a screen for live monitoring.

Secondary Stream: 360° Fisheye view for recording and retrospective review.

Tertiary Stream: VCam focused on a particular area of interest in the scene.



In Multi-Mode up to 4 different views, for four different streams are supported. If TrueDetail HDR is enabled a maximum of 3 different views are supported as the Primary and secondary encoders are linked and so share the same Video Source.

Hovering over each option will provide a pop-up with further information about the option.

Default is **Fisheye Only**. If a different Image Output Mode is selected, the **Apply** button will change color. Select it to apply the change. A pop-up warning message will be displayed, select **Confirm** to apply the change.

A countdown will be displayed while the change is being applied to the camera, once complete the web page will automatically refresh and the Dashboard displayed. Navigate to Video/Audio using the left-hand menu. The selected Image Output Mode and associated media profiles will be displayed.

Select the appropriate Performance Mode and Image Output Mode for the camera based on the use case.

5.3.1.3 Media Profiles Overview

A Media Profile contains all the configuration settings for each of its video, audio and metadata streams.

5.3.1.4 Default Media Profiles and Video Encoders

The Oncam C-Series camera supports up to four hardware video encoders which capture, compress, and convert video data into a format suitable for streaming and/or recording.

Four default Media Profiles (MP1 - MP4 when in Multiple Streams Mode) have been created to represent each video encoder.

New profiles can be created by reusing one of the camera's four video encoders. This allows multiple combinations of video, audio and metadata. A total of 6 new Media Profiles can be created in addition to the default 4 that are always present (in Multiple Streams Mode).

See *Figure 194 Media Profile Overview*



Any changes made to the video settings in a profile will change the configuration of that encoder and therefore effect all Media Profiles using that video encoder including the default Media Profiles.


In High Speed Mode only one encoder is supported, hence one default Media Profile (MP1) is available.

See *Figure 196 Media Profiles, Camera Mode Changed*

Default and user created Media Profiles can be edited. User created Media Profiles (for example MPUxx) can be deleted, however default Media Profiles (MP1 - MP4) cannot be deleted. This is to ensure all the four hardware video encoders are always accessible and are easily identifiable for profile creation and modification.

Create, edit and delete a Media Profile using an ONVIF Profile S or Profile T Conformant VMS within ONVIF profile settings, or via the Camera's built-in ONVIF based Web Interface, under Video/Audio > Media Profiles. Changes made in the VMS will be reflected in the Camera Web Interface.

5.3.1.5 How to edit a Media Profile

To edit a Media Profile via the camera interface, go to **Video/Audio > Media Profiles**, from the table select the icon  under the Edit column next to the Media Profile that requires editing.

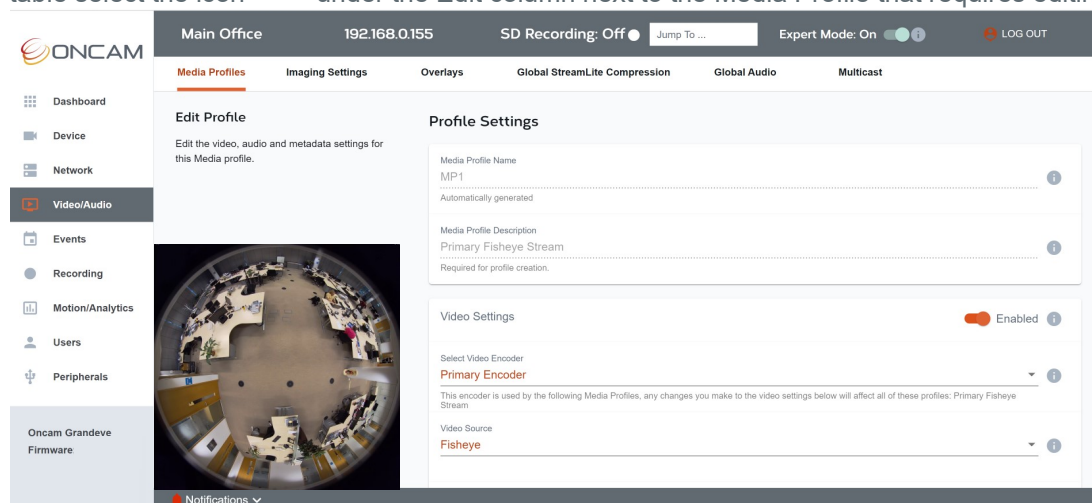


Figure 197 Media Profile Edit

5.3.1.6 How to Create a New Media Profile

To create a Media Profile via the Camera Web Interface, go to **Video/Audio > Media Profiles**, select icon  located under the Media Profile summary table.

The following Media Profile settings can be selected and edited.

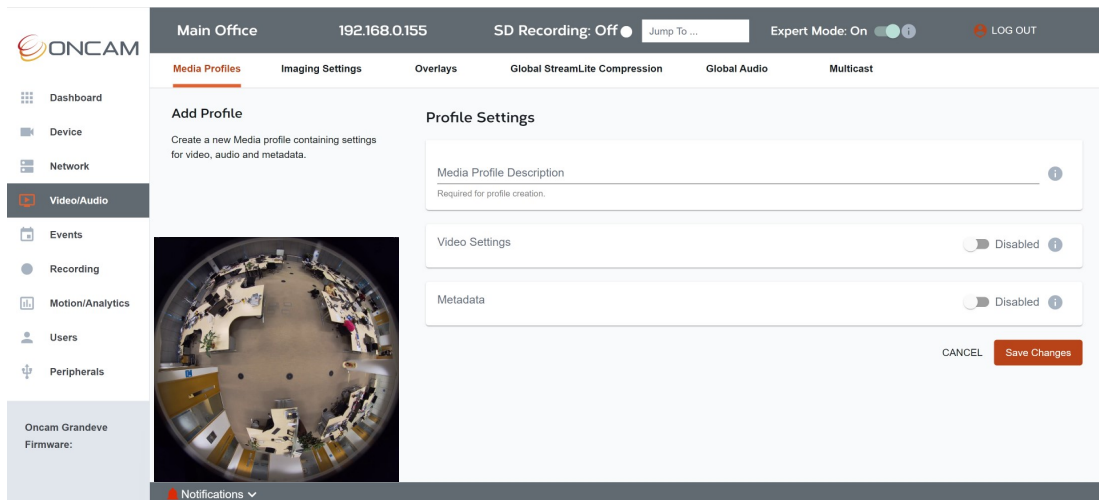


Figure 198 Media Profile, New Profile Creation

5.3.1.6.1 Media Profile Description

The Media Profile name such as MP1 (default), MPU1 (user created) are tokens automatically allocated by the camera. For easier recognition, a Media Profile description needs to be created for the profile.



Choose a name that will easily help in identify this profile. e.g. Remote Monitoring.



Once created this description cannot be edited.

5.3.1.6.2 Video

Enable **Video Settings** to allow video streaming in the profile, in the Camera Web Interface toggle this feature to enable it and display further video settings of the camera. In a VMS, adding a video encoder to the media profile enables this section.

5.3.1.6.3 Select a Video Encoder

Select a video encoder to use for this profile from one of the four available (Multiple Streams Mode). In High Speed Mode only encoder 1 will be available. Any changes made to the video settings will affect any other profiles that use this encoder. The list of associated profiles will be displayed once an encoder is selected.

The four encoders have different characteristics and capabilities:

Encoder Name	Maximum Resolution (Fisheye)	Maximum Frame Rate	Max Bit Rate
Primary Encoder	2992 x 2992 (C-12) 2160 x 2160 (C-08)	Up to 60 fps (60Hz) / 50fps(50Hz)	Up to 40Mbps
Secondary Encoder	2992 x 2992 (C-12) 2160 x 2160 (C-08)	Up to 15 fps (60 & 50Hz)	Up to 20Mbps
Tertiary Encoder	1920 x 1920 (C-12) 1440 x 1440 (C-08)	30 fps (60Hz) / 25 fps (50Hz)	Up to 10Mbps

Low – Res Encoder	512 x 512 (C-12 & C-08)	10 fps (60 & 50Hz)	Up to 5Mbps
-------------------	----------------------------	--------------------	-------------

Table 2 Characteristics and Capabilities of Encoders

5.3.1.6.4 Video Source

Select the Video Source. Depending on the Image Output Mode selected different options will be presented.

In **Fisheye Only Mode**, Fisheye is the only option available.

In **Panoramic+ Only Mode**, Panoramic+ is the only option available

In **Multi-Mode** both Fisheye and Dewarped views (e.g. Panoramic+, Corridor+ etc) are supported and available to choose from, per stream.



V2.0.x firmware or above required to access this feature.

5.3.1.6.4.1 Video Source Views - Onboard Dewarping

In addition to a 360° fisheye, the C-Series Camera also supports Onboard Dewarped views.



V2.0.x firmware or above required to access this feature.

The following views are supported:

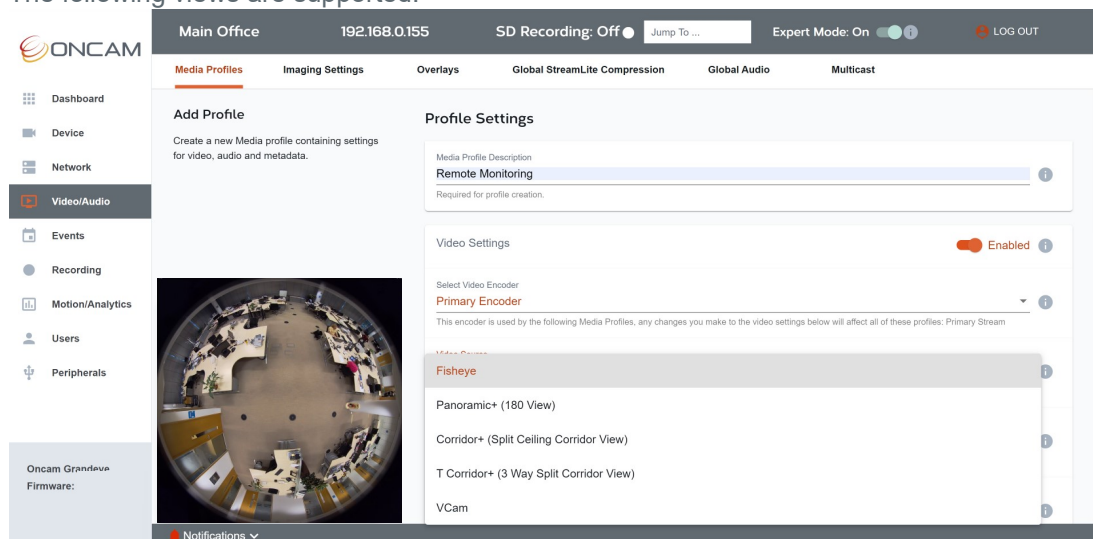


Figure 199 Media Profile, Video Source Selection

Fisheye: (360° View)

The standard non-dewarped 360-degree fisheye view, ideal for total situational awareness. Available in Fisheye Only Mode and Multi-Mode



Panoramic+ (180° View)

A 5:2 pre-dewarped panoramic view ideal for wall-mounted cameras, that uses the center of the fisheye sensor to generate a true 180-degree image. When installed at an angle, tools like Angle Compensation Technology (ATC) and Scene Offset (See 5.3.1.12.1) allow the image to be optimized to provide an even more natural representation of the scene. Available in Panoramic+ Only Mode and Multi-Mode.



Corridor+ (Ceiling Split Corridor View)

A 2-way split corridor view, that's gives perfect coverage of a corridor from a ceiling mounted camera. Corridor+ allows you to watch both directions of a 360-image at the same time, with no blind spots even when objects move from one view to the other. Available in Multi-Mode.



T Corridor+ (3 Way Split Corridor View)

A 3-way corridor view, that perfectly covers three corridors from a ceiling mounted camera. T Corridor+ allows you to see in all three directions at the same time, with no blind spots even when objects move from one view to the other. Ideal for areas like a Lift Lobby with a corridor. Available in Multi-Mode.



VCam

A user defined dewarped view of a specific portion of the fisheye image, where users can decide which specific area(s) of the scene are of interest and focus on them. Up to four separate VCams can be supported at any one time, one for each encoder. Available in Multi-Mode.



VCam1

VCam2

When selecting VCam as the **Video Source**, an additional setting will be presented **PTZ Preset**. This enables you select the VCam PTZ for this profile between VCam1, 2,3 & 4. The coordinates for the view you then set for this VCam in the **View Adjust** page will be saved for this Preset (see 5.3.1.12.4). As four encoders are available, a maximum of four VCam's can be set and streamed at any one time.

Select the **Video Source** if the source is changed a pop-up will be shown requesting confirmation. Select **Confirm** to apply. Once confirmed the video source for the encoder and all associated profiles will automatically be changed and saved even if the profile is not saved.

Available resolutions will be automatically updated based on the **Video Source** chosen. For the stream to work an expected the associated correct resolution will need to be selected and saved as part of the profile changes.

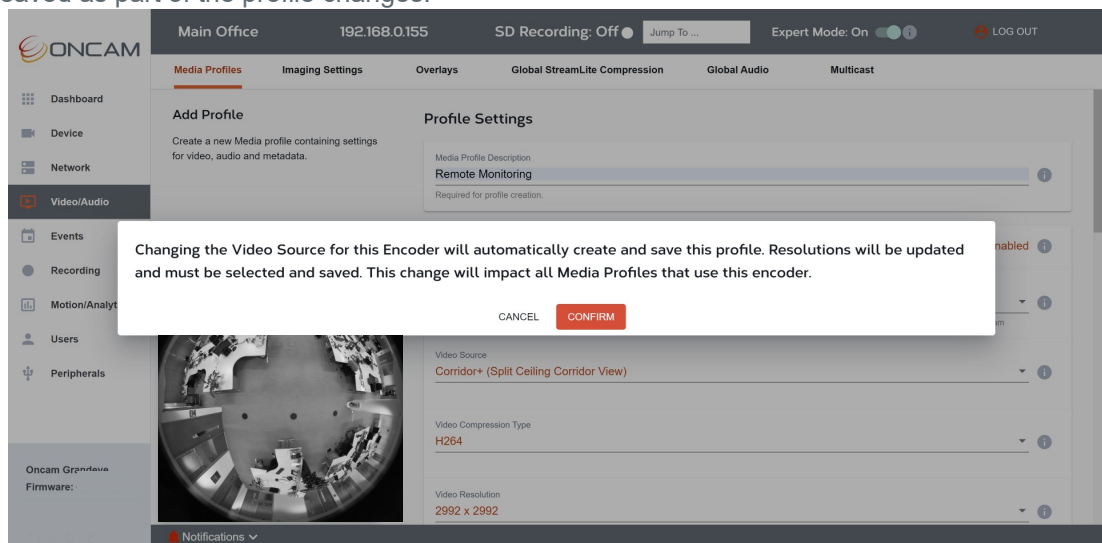



Figure 200 Media Profile, Video Source Change Confirmation



Multi-Mode can be used in conjunction with High Speed mode to deliver a dewarped single stream up to 60fps.

If selecting a dewarped view, after saving this profile you will be taken to the Media Profile overview page which includes a summary table where you can set and edit this image view by clicking the adjust view icon  next to this profile. (See 5.3.1.12)

5.3.1.6.5 Video Compression type

Select a video compression method, the following options are available:

H.264

H.264 also known as MPEG – 4 Part 10 or Advanced Video Coding (MPEG-4 AVC) is a well-known industry standard for video compression. It converts digital video into a format that takes up less capacity when it is stored or transmitted. The four default media profiles (MP1-MP4) are set to H.264 by default.

H.265

H.265 High Efficiency Video Encoding (HEVC) offers almost double the compression of H.264 using advanced algorithms that encode video at the lowest possible bit rate whilst maintaining a high image quality level.

JPEG - Motion JPEG (MJPEG)

MJPEG is a compilation of separately compressed individual JPEGs in a digital video sequence that are displayed and updated at a frequency sufficient to create a stream that shows constantly updated motion. This option supports a maximum resolution of 512 x 512 and a maximum frame rate of 10 fps and maximum bit rate of 5000 kbps.

5.3.1.6.6 Video Resolution

Select the Video Resolution for the stream. The resolutions available vary by Encoder and Video Source:

Fisheye Resolutions	Panoramic+ Resolutions	Corridor+ Resolutions	T Corridor+ Resolutions	VCam Resolutions
C-12				
PRIMARY ENCODER (MP1)				
2992 x 2992 (9.0MP) 2800 x 2800 (7.8 MP) 2304 x 2304 (5.3 MP) 1920 x 1920 (3.7 MP) 1440 x 1440 (2.1 MP) 992 x 992 (0.98 MP) 512 x 512 (0.26 MP)	3040 x 1216 (3.7MP) 2400 x 960 (2.3 MP) 1920 x 768 (1.5 MP) 1440 x 576 (0.83 MP) 960 x 384 (0.37 MP) 800 x 320 (0.26 MP)	2432 x 1520 (3.7 MP) 1920 x 1200 (2.3MP) 1536 x 960 (1.5 MP) 1152 x 720 (0.83 MP) 768 x 480 (0.37 MP) 640 x 400 (0.26MP)	3456 x 1440 (5.0MP) 2880 x 1200 (3.5 MP) 2304 x 960 (2.2 MP) 1728 x 720 (1.2 MP) 1152 x 480 (0.6 MP) 768 x 320 (0.25 MP)	1280 x 720 (0.9MP) 640 x 480 (0.3 MP) 576 x 432 (0.25 MP)
SECONDARY ENCODER (MP2)				
2992 x 2992 (9.0MP) 2800 x 2800 (7.8 MP) 2304 x 2304 (5.3 MP) 1920 x 1920 (3.7 MP) 1440 x 1440 (2.1 MP) 992 x 992 (0.98 MP) 512 x 512 (0.26 MP)	3040 x 1216 (3.7MP) 2400 x 960 (2.3 MP) 1920 x 768 (1.5 MP) 1440 x 576 (0.83 MP) 960 x 384 (0.37 MP) 800 x 320 (0.26 MP)	2432 x 1520 (3.7 MP) 1920 x 1200 (2.3MP) 1536 x 960 (1.5 MP) 1152 x 720 (0.83 MP) 768 x 480 (0.37 MP) 640 x 400 (0.26MP)	3456 x 1440 (5.0MP) 2880 x 1200 (3.5 MP) 2304 x 960 (2.2 MP) 1728 x 720 (1.2 MP) 1152 x 480 (0.6 MP) 768 x 320 (0.25 MP)	1280 x 720 (0.9MP) 640 x 480 (0.3 MP) 576 x 432 (0.25 MP)
TERTIARY ENCODER (MP3)				
1920 x 1920 (3.7 MP) 1440 x 1440 (2.1 MP) 992 x 992 (0.98 MP) 512 x 512 (0.26 MP)	3040 x 1216 (3.7MP) 2400 x 960 (2.3 MP) 1920 x 768 (1.5 MP) 1440 x 576 (0.83 MP) 960 x 384 (0.37 MP) 800 x 320 (0.26 MP)	2432 x 1520 (3.7 MP) 1920 x 1200 (2.3MP) 1536 x 960 (1.5 MP) 1152 x 720 (0.83 MP) 768 x 480 (0.37 MP) 640 x 400 (0.26MP)	3456 x 1440 (5.0MP) 2880 x 1200 (3.5 MP) 2304 x 960 (2.2 MP) 1728 x 720 (1.2 MP) 1152 x 480 (0.6 MP) 768 x 320 (0.25 MP)	1280 x 720 (0.9MP) 640 x 480 (0.3 MP) 576 x 432 (0.25 MP)
LOW-RES ENCODER (MP4)				
512 x 512 (0.26 MP)	800 x 320 (0.26 MP)	640 x 400 (0.26MP)	768 x 320 (0.25 MP)	576 x 432 (0.25 MP)

Table 3 C-12 Video Resolutions Supported by Encoder and Video Source

Fisheye Resolutions	Panoramic+ Resolutions	Corridor+ Resolutions	T Corridor+ Resolutions	VCam Resolutions
C-08				
PRIMARY ENCODER (MP1)				
2160 x 2160 (4.7MP) 1920 x 1920 (3.7 MP) 1440 x 1440 (2.1 MP) 992 x 992 (0.98 MP) 512 x 512 (0.26 MP)	2160 x 864 (1.9MP) 1920 x 768 (1.5 MP) 1440 x 576 (0.83 MP) 960 x 384 (0.37 MP) 800 x 320 (0.26 MP)	1728 x 1080 (1.9MP) 1536 x 960 (1.5 MP) 1152 x 720 (0.83 MP) 768 x 480 (0.37 MP) 640 x 400 (0.26MP)	2592 x 1080 (2.8 MP) 2304 x 960 (2.2 MP) 1728 x 720 (1.2 MP) 1152 x 480 (0.6 MP) 768 x 320 (0.25 MP)	1280 x 720 (0.9MP) 640 x 480 (0.3 MP) 576 x 432 (0.25 MP)

SECONDARY ENCODER (MP2)				
2160 x 2160 (4.7MP) 1920 x 1920 (3.7 MP) 1440 x 1440 (2.1 MP) 992 x 992 (0.98 MP) 512 x 512 (0.26 MP)	2160 x 864 (1.9MP) 1920 x 768 (1.5 MP) 1440 x 576 (0.83 MP) 960 x 384 (0.37 MP) 800 x 320 (0.26 MP)	1728 x 1080 (1.9MP) 1536 x 960 (1.5 MP) 1152 x 720 (0.83 MP) 768 x 480 (0.37 MP) 640 x 400 (0.26MP)	2592 x 1080 (2.8 MP) 2304 x 960 (2.2 MP) 1728 x 720 (1.2 MP) 1152 x 480 (0.6 MP) 768 x 320 (0.25 MP)	1280 x 720 (0.9MP) 640 x 480 (0.3 MP) 576 x 432 (0.25 MP)
TERTIARY ENCODER (MP3)				
1440 x 1440 (2.1 MP) 992 x 992 (0.98 MP) 512 x 512 (0.26 MP)	1440 x 576 (0.83 MP) 960 x 384 (0.37 MP) 800 x 320 (0.26 MP)	1152 x 720 (0.83 MP) 768 x 480 (0.37 MP) 640 x 400 (0.26MP)	1152 x 480 (0.6 MP) 768 x 320 (0.25 MP)	640 x 480 (0.3 MP) 576 x 432 (0.25 MP)
LOW-RES ENCODER (MP4)				
512 x 512 (0.26 MP)	800 x 320 (0.26 MP)	640 x 400 (0.26MP)	768 x 320 (0.25 MP)	576 x 432 (0.25 MP)

Table 4 C-08 Video Resolutions Supported by Encoder and Video Source



V2.0.x firmware or above required to access the dewarped resolutions.

5.3.1.6.6.1 Video Resolutions and Video Sources Supported in TrueDetail HDR

Two image sensor modes are supported by the camera - **Normal** (single exposure per frame) and **TrueDetail HDR** (dual exposures per frame) for improved detail in light and dark areas of the image in challenging scenes (5.3.2.3)


TrueDetail HDR is the default image sensor mode of the camera, to activate Normal Mode via the Camera Web Interface go to **Video/Audio > Image Settings > TrueDetail HDR**. Disable this feature and click **Save Changes** and **Reboot** the camera to apply this change.

The image sensor mode selected will have an impact on resolution and frame rates available.

The Resolutions and Video Source in the Tables 3 & 4 above are applicable per encoder to Normal mode streaming only. In TrueDetail HDR mode, due to capacity, the primary and secondary encoders must share the same Resolution and Video Source, so changes made to one will be applied to the other.

For instance, if the Primary Encoder Video Source is changed to Corridor+ and the Resolution set to 1536 x 960, then when TrueDetail HDR is enabled, the same settings will be applied the Secondary Encoder, as shown below.

The frame rate and other settings however can be different.

To show that TrueDetail HDR is enabled and that the two encoders are linked the following symbol  is shown next to each media profile, if you hover above the symbol a pop-up will be displayed to explain this linkage between the two encoders.

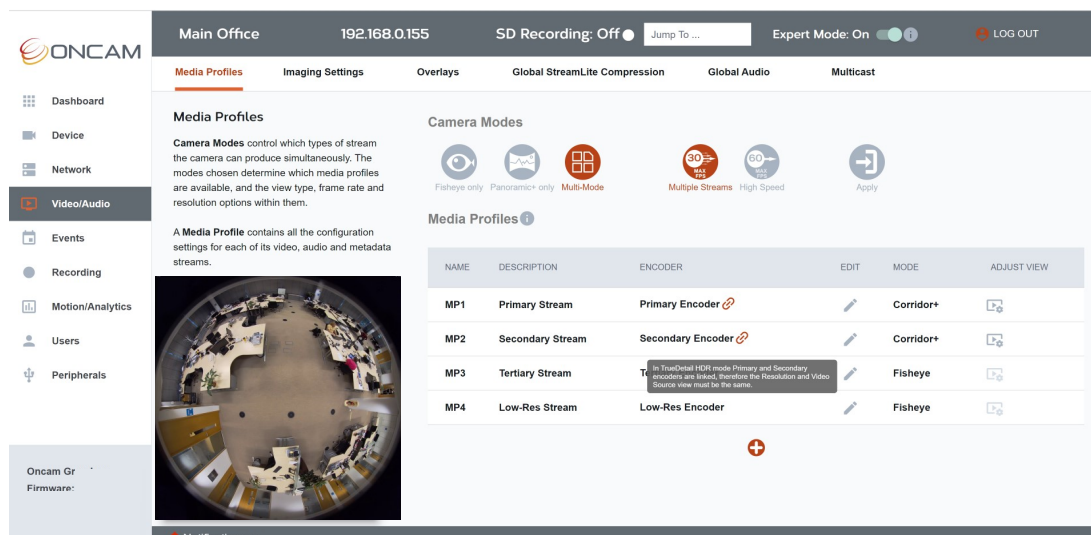
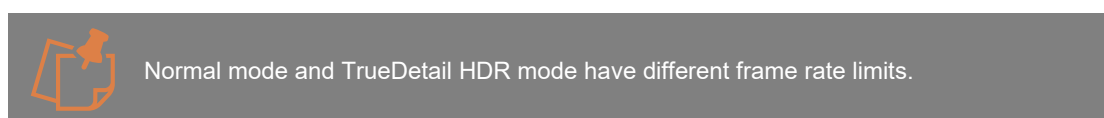


Figure 201 Media Profile, TrueDetail HDR Impact

5.3.1.6.7 Frame Rate

Select the desired frames per second for the stream.



The following frame rates are supported by the camera, the available rates will be determined by the Performance Mode of the Camera selected:

60Hz mode:

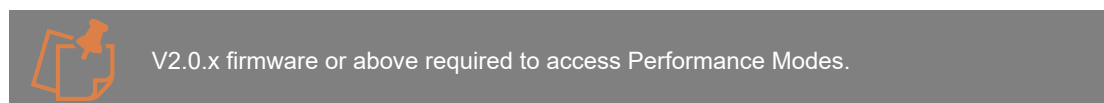
Multiple Streams Mode: 1 – 30 fps in increments of 1

High Speed Mode: 1 – 30 fps in increments of 1 & 60 fps

50Hz mode:

Multiple Streams Mode: 1 – 25 fps in increments of 1

High Speed Mode: 1 – 25 fps in increments of 1 & 50 fps



The maximum frame rates available for each encoder in Normal Image sensor mode are:

High Speed Mode:

Primary Encoder (MP1)

up to 60 fps (60Hz)

up to 50 fps (50Hz)

Multiple Streams Mode:

Primary Encoder (MP1)

up to 30 fps (60Hz)

up to 25 fps (50Hz)

Secondary Encoder (MP2)

up to 15 fps (60Hz)

up to 15 fps (50Hz)

Tertiary Encoder (MP3)

up to 30 fps (60Hz)

up to 25 fps (50Hz)

Low - Res Encoder (MP4)

up to 10 fps (60Hz)

up to 10 fps (50Hz)

5.3.1.6.8 Frames Per Second (fps) Supported in TrueDetail HDR

The maximum frame rates available in each encoder in TrueDetail HDR mode are:

High Speed Mode:

Primary Encoder (MP1)

up to 60 fps (60Hz)

up to 50 fps (50Hz)

If frame rate above 25 / 30 fps is selected, TrueDetail HDR is automatically disabled.

Multiple Streams Mode:

Primary Encoder (MP1)

C-12

up to 25 fps (60Hz), possible to Select 30 fps but 25 fps will be delivered.

up to 25 fps (50Hz)

C-08

up to 30 fps (60Hz)

up to 25 fps (50Hz)

Secondary Encoder (MP2)

C-12 & C-08

up to 15 fps(60Hz)

up to 15 fps (50Hz)



Will be same Resolution and Video Source as MP1.

Tertiary Encoder (MP3)

C-12

up to 25 fps (60Hz), possible to Select 30 fps but 25 fps will be delivered.

up to 25 fps (50Hz)

C-08

up to 30 fps (60Hz)

up to 25 fps (50Hz)

Low - Res Encoder (MP4)

C-12 & C-08

up to 10 fps (60Hz)

up to 10 fps (50Hz)

5.3.1.6.8.1 Recommended Frame Rate

For optimum performance and smooth streaming, it is recommended to use a frame rate that is wholly divisible into the Power Line Frequency configured in **Video/Audio > Imaging Settings**.



In TrueDetail HDR it is recommended to use 30 fps (60Hz) or 25 fps (50Hz).
In Normal Mode for 60Hz, the recommendation is to use 60,30,20,15,12,10,6,5,4,3,2 or 1 fps and in 50Hz to use 50,25,10,5,2, or 1 fps.

5.3.1.6.8.2 High Speed - Maximum Frame Rate

For the **C-12** at a maximum resolution of **2992 x 2992** (Fisheye), **55 fps** is supported by the primary encoder running a single stream in **Normal mode**.

For the **C-08** at a maximum resolution of **2160 x 2160** (Fisheye), **60 fps** is supported by the primary encoder running a single stream in **Normal mode**.



V2.0.x firmware or above required to use the steps below to access this feature.

To access this feature, go to **Video/Audio > Media Profiles > Camera Modes** and select **High Speed Mode**. Select the required **Image Output Mode** (Fisheye Only, Panoramic+ or Multi-Mode based on whether a Fisheye or Dewarped image is required). The **Apply** button will change color. Select it to apply the change. A pop-up warning message will be displayed, select **Confirm** to apply the change.

A countdown will be displayed while the change is being applied to the camera, once complete the web page will automatically refresh and the Dashboard displayed. Navigate to Video/Audio using the left-hand menu. The selected Image Output Mode and High Speed Mode will be displayed.

Select the **Edit** icon  next to the Primary Fisheye Stream profile in the summary table, select the required **Video Source** view and confirm. Select the required **Resolution**, and 60 fps under Frames Per second, scroll to the bottom and click **Save**.

To maintain this frame rate even in low light, set the **Exposure Priority to Frame Rate**, accessible via **Video/Audio > Imaging Settings > Low Light Technology**. The camera also needs to be in 60Hz Power Line Frequency Mode, accessible via **Video/Audio > Image Settings**.

You can switch the image sensor mode to Normal mode on the camera by **disabling TrueDetail HDR** mode: Go to **Video/Audio > Image Settings > TrueDetail HDR**, disable this feature and click **Save Changes** and reboot the camera to apply this change. However even if you do not change this, TrueDetail HDR will be disabled automatically if you request 60 fps.



Requesting more than one stream from the camera (Multiple Stream Mode) will reduce this frame rate to 30 fps.

For the C-12 if 60 fps is required from the camera the maximum supported resolution is 2800 x 2800.

At a maximum resolution of **2992 x 2992, 25 fps (C-12) or 2160 x 2160, 30 fps (C-08)**, is supported by the primary encoder running in **TrueDetail HDR** mode. This image sensor mode is on by default. Go to **Video/Audio > Media Profiles**, select **Edit** next to the **Primary Fisheye Stream** profile in the summary table, and **select 30 fps** under Frames Per Second, scroll to the bottom and click **Save**. To maintain this rate even in low light, set the **Exposure Priority to Frame Rate**, accessible via **Video/Audio > Imaging Settings > Low Light Technology**. The camera also needs to be in 60Hz Power Line Frequency Mode, accessible via **Video/Audio > Image Settings**. TrueDetail HDR will be disabled automatically if you request 60 fps.



TrueDetail HDR is unnecessary in low light because there are smaller variations in brightness. It is automatically switched off in these conditions to maximize exposure time and get the best image quality. There is a small visual switchover when TrueDetail HDR switches Off or On.
Frame rate will be reduced in low light if Exposure Priority is set to Low Noise.

5.3.1.6.8.3 Maintain Frame Rate when Multiple Streaming

Four streams can be requested and run concurrently (e.g. MP1,2,3,4). In this scenario, the primary encoder (MP1) can maintain a frame rate of 30 fps in **Normal mode**.



V2.0.x firmware or above required to use the steps below to access this feature.

To access this feature, go to **Video/Audio > Media Profiles > Camera Modes** and select **Multiple Streams Mode** (default). Select the required Image Output Mode (**Fisheye Only**, **Panoramic+** or **Multi-Mode** based on whether a Fisheye only, Panoramic+ only or a mix of views are required per stream). The **Apply** button will change color. Select it to apply the change. A pop-up warning message will be displayed, select **Confirm** to apply the change.

A countdown will be displayed while the change is being applied to the camera, once complete the web page will automatically refresh and the Dashboard displayed. Navigate to Video/Audio using the left-hand menu. The selected Image Output Mode and Multiple Streams Mode will be displayed.

To support four different views, enable **Normal mode** on the camera by disabling **TrueDetail HDR** mode: Go to **Video/Audio > Image Settings > TrueDetail HDR**, disable this feature and click **Save Changes** to apply this change. If TrueDetail HDR is enabled a maximum of three views are supported as Primary and Secondary Encoders are linked and therefore must have the same **Video Source** and **Resolution**.

Go to **Video/Audio > Media Profiles** select **Edit** next to the Primary Fisheye Stream profile in the summary table, and Select and save the Video source. Select the Resolution and select 30 fps under **Frames Per Second**, scroll to the bottom and click **Save**. To maintain this rate even in low light, set the **Exposure Priority to Frame Rate**, accessible via **Video/Audio > Imaging Settings > Low Light Technology**. The camera also needs to be in 60Hz Power Line Frequency Mode, accessible via **Video/Audio > Image Settings**.



When maintaining 30 fps on the primary stream, the fps can fluctuate $\pm 5\%$. 25 fps in TrueDetail HDR Mode is supported at 60Hz for the C-12 and 30 fps for the C-08.

5.3.1.6.9 Bit Rate Control

The amount of network bandwidth used by the camera is controlled by the bit rate control mechanism.

The bit rate of the stream is affected by several factors including resolution, frame rate, image quality level and the amount of activity and detail in the scene. It is important to consider these elements when selecting an appropriate bit rate for the stream and setting the bit rate level.

Two bit rate control options are supported, Constant Bit Rate (CBR) and Fixed Quality (Capped Bit rate).

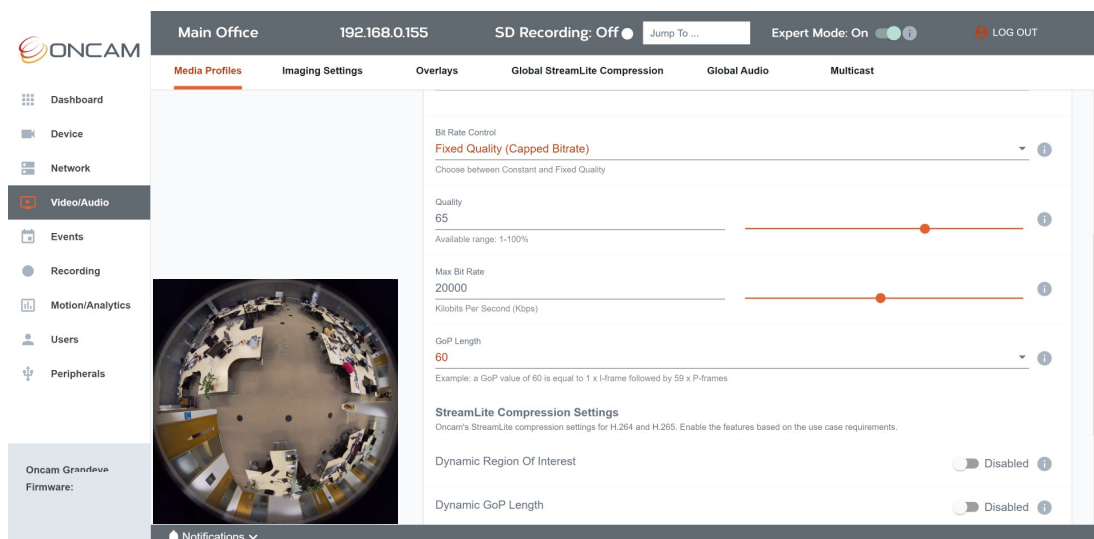


Figure 202 Media Profile Bit Rate Control

5.3.1.6.9.1 Constant Bit Rate

Maintains the bit rate at a consistent level (+/- 10%) irrespective of image quality, therefore image quality may be decreased during periods of high motion. To enable Constant Bit Rate, select it from the drop-down menu under Bit Rate Control.



Constant Bit Rate does not support StreamLite compression, Fixed Quality will need to be selected to use StreamLite compression.

Set the preferred **Constant Bit Rate** level. The camera will stay at this rate +/- 10%. The maximum bit rates available vary by encoder:

Encoder	Max Bit Rate	Default Rate
Primary Encoder (MP1)	Up to 40,000 Kbps (40Mbps)	20,000 Kbps (20Mbps)
Secondary Encoder (MP2)	Up to 20,000 Kbps (20Mbps)	10,000 Kbps (10Mbps)
Tertiary Encoder (MP3)	Up to 10,000 Kbps (10Mbps)	5,000 Kbps (5 Mbps)
Low – Res Encoder (MP4)	Up to 5,000 Kbps (5Mbps)	1,000 Kbps (1Mbps)

Table 5 Encoder Bit Rate Level

5.3.1.6.9.2 Fixed Quality (Capped Bit Rate)

Prioritizes and maintains the image quality level (user selectable) allowing the bit rate to vary to deliver the desired quality. A cap or limit on the bit rate is applied using the **Max Bit Rate** setting (user settable) to ensure the stream does not use excessive bandwidth. This is designed to prevent extreme or prolonged excessive bit rates, but momentary bit rate levels above the cap are permitted to avoid interfering with image quality where possible. If tighter control is essential, use Constant Bit Rate, or set a lower **Max Bit Rate**.

To enable this option, select it from the drop-down menu under **Bit Rate Control**. This is the default bit rate control mechanism.



Fixed Quality is required to support the StreamLite compression feature.

5.3.1.6.9.3 Quality

Set the preferred image quality level for the stream from 1-100%. The higher the percentage the better the image quality. However, this will increase the bit rate of the stream and a higher maximum bit rate will be required to maintain the quality level. The default setting is 65%.

5.3.1.6.10 Max Bit Rate

Set the maximum bit rate level for Fixed Quality (Capped Bit Rate). This level will reduce the quality of the image when required to keep the bit rate in and around this cap. The priority in this mode is to maintain a good quality image, therefore small excesses over the cap for a short period of time are allowed. However large excesses will be reduced immediately.

Set this cap based on your network requirements but also considering the resolution, frame rate, quality level selected and expected level of activity and detail in the scene to ensure sufficient bandwidth is available to achieve this in most scenarios.



As an example, if the Primary Encoder (MP1) is set to maximum resolution of 2992 x 2992 and a **Quality** level of 65%, a Max Bit Rate of 20,000 Kbps (20Mbps) may be appropriate dependent on the expected level of motion in the scene.

The maximum bit rates for each encoder are as follows:

Encoder	Max Bit Rate	Default Rate
Primary Encoder (MP1)	Up to 40,000 Kbps (40Mbps)	20,000 Kbps (20Mbps)
Secondary Encoder (MP2)	Up to 20,000 Kbps (20Mbps)	10,000 Kbps (10Mbps)
Tertiary Encoder (MP3)	Up to 10,000 Kbps (10Mbps)	5,000 Kbps (5 Mbps)
Low – Res Encoder (MP4)	Up to 5,000 Kbps (5Mbps)	1,000 Kbps (1Mbps)

Table 6 Encoder Bit Rate Level

5.3.1.6.11 GOP Length

The video stream (H.264 & H.265) consists of I-frames and P-frames. I-frames are large self-contained frames that contain all image data, while P-frames are smaller in size as they only contain motion information that has changed from previous I- or P-frames.

A Group of Pictures (GoP) is a complete set of images including one I-frame and all the following P-frames. **GoP Length** is the total number of frames in this group. Increasing the gap between I-frames reduces the overall bandwidth and storage requirements because more of the smaller sized P-frames are used in the stream.

The GoP length can be set from 1-1800, for the default Media Profiles (MP1-4) this is set to double the default frame rate, for instance for MP1 it is 60, which would mean 1 I-frame followed by 59 P-Frames. In this scenario if the stream is set to 30 fps, an I-frame will be provided every 2 seconds.



Increasing the **GoP Length** means full frame detail is sent less frequently which can cause an issue if the stream is corrupted or temporarily drops. This feature can also affect video playback as it may require playback to start earlier than required because video playback must always start from an I-frame.

5.3.1.6.12 StreamLite Compression

StreamLite is Oncam's advanced real time adaptive video encoder enhancement technology that is applied to industry compression standards like H.264 & H.265. It uses smart dynamic object & motion-based algorithms, to analyze the video stream on the fly and identify what's really important. The desired level of quality is then applied to the areas that matter whilst less important areas can be compressed to deliver significant bandwidth savings. StreamLite also offers advanced users an industry leading level of control to tune the compression and analytics it uses for their specific environment.

StreamLite uses smart dynamic object & motion-based algorithms to analyze the scene in real time and provide data to the compression engine. The compression engine then uses 3 key techniques: Dynamic Regions of Interest (ROI), Dynamic Group of Pictures (GoP) and Dynamic Frames Per Second (FPS) to determine the quality to apply to each area of the scene, which type of frame to create and how many to send per second. This ensures significantly less data is transmitted and stored without losing the important details when you need them.

To enable StreamLite select your preferred compression algorithms to apply to the stream from Dynamic ROI, GoP and FPS.

Advanced settings and configuration for this feature are available via **Video/Audio > Global StreamLite Compression**.

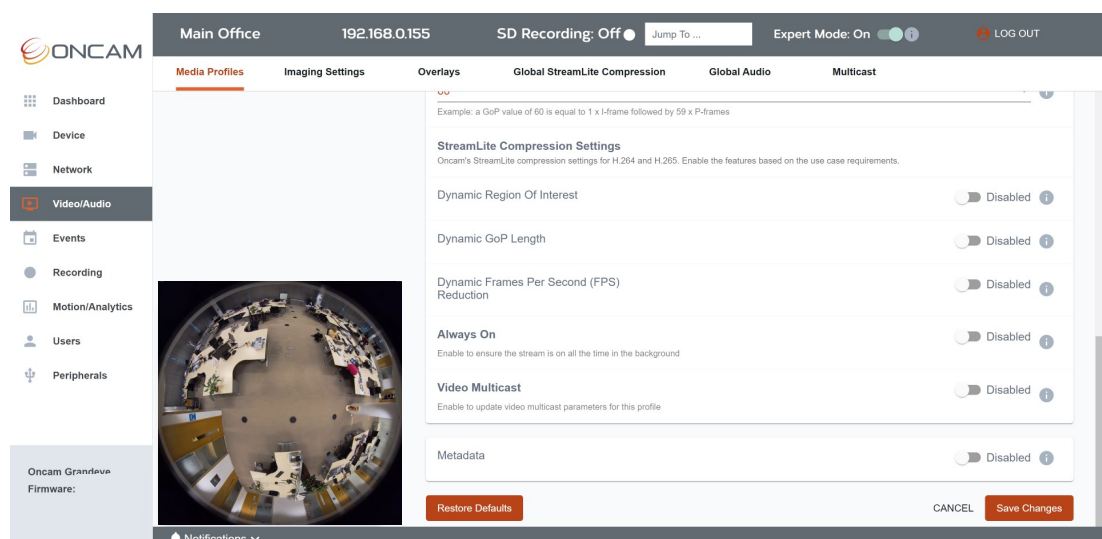


Figure 203 Media Profile StreamLite Compression

5.3.1.6.12.1 Dynamic Regions of Interest (ROI)

Dynamic Regions of Interest compression uses the analytics engine to identify the important areas in the scene and encodes these areas at higher quality than the background. The higher quality level applied is determined by the % value set under **Fixed Quality** bit rate control in the Media Profile, accessible via **Video/Audio > Media Profile > Fixed Quality > Quality**. Use the toggle to enable Dynamic ROI and then select your compression level.

Advanced settings and configuration for this feature are available via **Video/Audio > Global StreamLite Compression**.

5.3.1.6.12.2 Compression Level (ROI)

Three Dynamic ROI compression levels are available:

- Low: maintains the best image quality with some reduction in bandwidth.
- Balanced: delivers an impressive image with increased bandwidth savings, this is the default setting.
- Best: provides good image quality with significant bandwidth savings.

In all modes the Regions of Interest remain unaffected by the compression.

5.3.1.6.12.3 Dynamic GOP Length

Dynamic GoP Length extends the gap between each beginning I-frame of a group of pictures in the video stream when there is little or no motion in the scene, achieving good bit rate reduction. It will send I-frames less frequently (up to a user defined limit) when there is no motion in the scene, as videos with limited motion require fewer detail intensive I-frames, but it will automatically revert to the original GoP length when motion is detected to ensure no loss of detail.

Use the toggle to apply Dynamic GoP and select your GoP Maximum length.

Advanced settings and configuration for this feature are available via **Video/Audio > Global StreamLite Compression**.



Increasing the **GoP Length** means full frame detail is sent less frequently which can cause an issue if the stream is corrupted or temporarily drops. This feature can also affect video playback as it may require playback to start earlier than required because video playback must always start from an I-frame.

5.3.1.6.12.4 Maximum GOP Length

The Maximum GoP length can be set from 1-1800, the default value is 300, which results in 1 I-frame followed by 299 P-frames. In this scenario if the stream is using 30 fps, an I-frame will be sent every 10 seconds when there is little or no motion in the scene.

This value should be set to an acceptable Maximum GoP length. The value should be higher than the standard GoP length. This is the highest level the Dynamic GoP feature will use when saving video bitrate.

5.3.1.6.12.5 Dynamic Frames Per Second (FPS) Reduction

Dynamic Frames Per Second (FPS) reduces the frames per second of your video stream when there is little or no motion in the scene with potentially very large bitrate savings as in this scenario, streaming and storing data at full frame rate adds little value. The frame rate is reduced to a user defined minimum when there is little or no activity, to minimize the amount of data encoded and transmitted.

The video stream is captured at full frame rate, analyzed frame by frame, and the unnecessary frames removed from the transmitted stream. This adaptive algorithm varies the FPS based on the amount of motion in the scene and immediately reverts to the original frame rate settings upon detecting motion, to ensure no loss of activity.

Use the toggle to apply Dynamic FPS and select your minimum FPS length.

Advanced settings and configuration for this feature are available via **Video/Audio > Global StreamLite Compression**.

5.3.1.6.12.6 Minimum FPS

The Minimum FPS length can be set from 1-30 fps. The recommended default value for Dynamic FPS is 1, so 1 frame will be sent every second when there is little or no motion in the scene.

This value should be set to an acceptable Minimum frame rate and should be lower than the standard frame rate for the stream. This is the lowest FPS the Dynamic FPS feature will use when saving video bitrate.



StreamLite is enabled at a profile level, however some settings are applied at a global level. These are accessible via **Video/Audio > Global StreamLite Compression**.

5.3.1.6.13 Always On

Enable this feature to ensure the encoder is on all the time in the background. This will ensure that when the stream is called it will be immediately available and its initialization will not disrupt any other streams. However, activating this feature uses more camera resources in the background.



V2.0.x firmware or above required to access this feature.

5.3.1.6.14 Multicast

Multicast Video, Audio and Metadata streaming is supported. Using multicast, a single stream is sent to a multicast address, which can then be distributed to a group of recipients.

5.3.1.6.14.1 Video Multicast

Use the toggle to enable Video Multicast and configure the settings for this profile. Set up the multicast address to store the multicast stream using the parameters below:

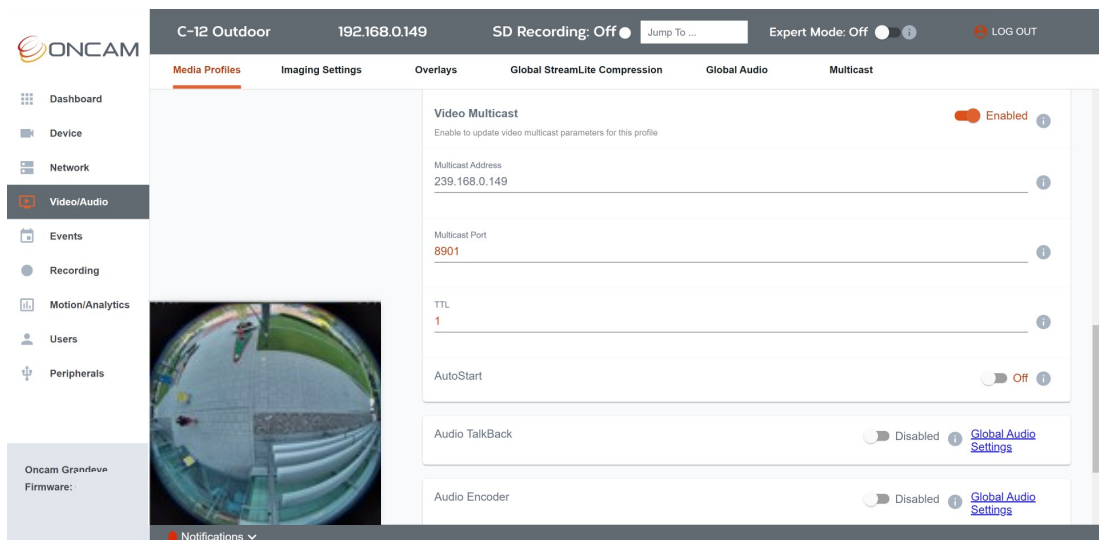


Figure 204 Media Profile Video Multicast

5.3.1.6.14.2 Multicast Address

Set the IP Address of the multicast group for receiving RTP streaming. The multicast clients need this address value as well as the multicast RTP port to receive the video. This is prepopulated starting “239.” followed by the IP address of the camera.

5.3.1.6.14.3 Multicast Port

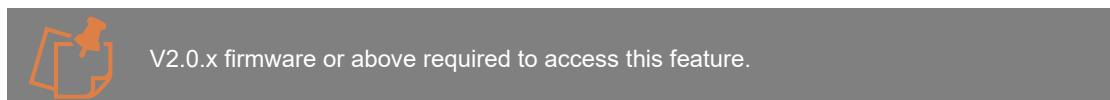
RTP port for receiving the multicast video. The clients that receive the video use the Multicast RTP Port and Multicast Address values to receive the video. This is prepopulated 890x

5.3.1.6.14.4 Time to Live (TTL)

Sets the Time to Live value in the multicast IP packets. The default is set to 1.

5.3.1.6.14.5 AutoStart

Enable to automatically restart Video Multicast after the camera reboots



5.3.1.6.14.6 Accessing the multicast stream

Once the above parameters are set and saved, stream directly via RTSP using your preferred VMS.

Invoke the GetStreamURI with multicast option via your VMS, the response will create a RTSP stream and then multicast traffic is exchanged between the clients. In this scenario RTSP will be communicated on the unicast address and RTP packet goes over the configured multicast address.

Alternatively, to stream via RTP, configure your settings and save this Media Profile. Then go to **Video/Audio > Multicast** tab and use the start / stop control next to this profile. This will

invoke the StartMulticastAPI, the client will then directly use RTP with the Multicast address and port.



Refer to your VMS documentation for any additional steps to enable streaming using Multicast.

5.3.1.7 Audio Settings

The audio is included in stream if the **Audio Encoder** is enabled in the media profile and the Audio input source is configured in **Global Audio settings** tab. During the RTSP connection to the camera, if audio is enabled, an additional mono audio channel is streamed to the player. Enable **Audio Encoder** to add audio streaming to the profile. Configure the **Audio Input settings** in the **Global Audio Settings** using the link provided or go to: **Video/Audio > Global Audio > Audio Input Settings**.

Global Audio Multicast settings are also configured in **Global Audio** and are applied to all profiles with the Audio Encoder enabled.

An external audio input stream is supported. This input is designed to work with an ordinary Electret microphone in close proximity to the enclosure. The camera mic input is provided from the 12-pin I/O connector located on the Plus board.



A **Plus** version of the camera is required to support this functionality, therefore the Outdoor Plus version of the camera is required to support this feature.
Audio is enabled at a profile level; however, audio settings are applied at a global level. These are accessible via **Video/Audio > Global Audio**.

Audio **TalkBack** enables remote 2-way communication if an external speaker is connected to the camera. Toggle to enable the TalkBack feature for the profile and then configure the Audio decoder in the Global Audio settings tab using the link provided or go to: **Video/Audio > Global Audio > External Audio Output Settings**. Then follow your VMS instructions to enable and use this feature.



V2.0.x firmware or above required to access this feature.

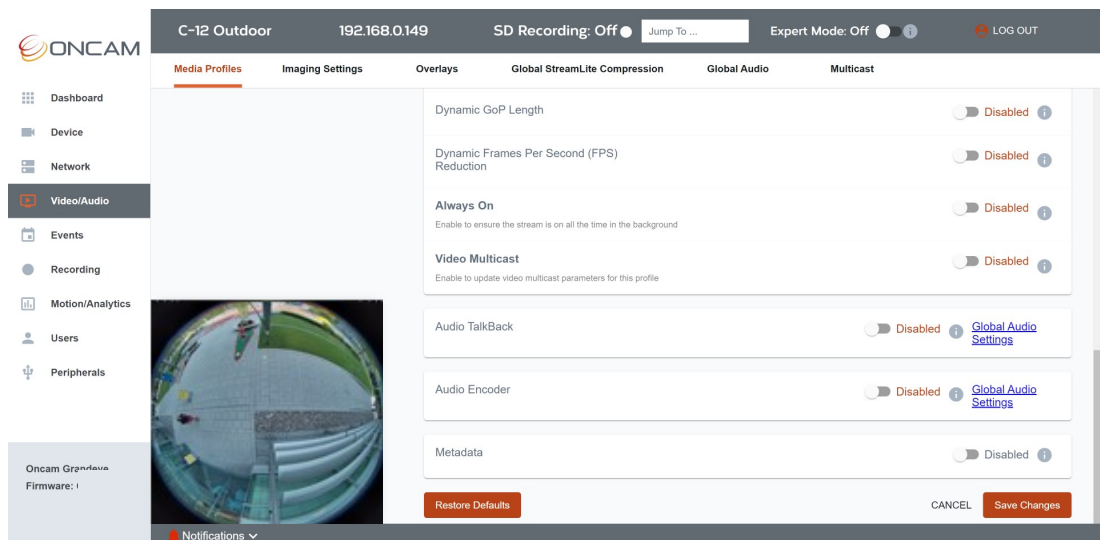


Figure 205 Media Profile Audio

5.3.1.8 Metadata Settings

5.3.1.8.1 Streamed Metadata

Metadata includes changes related to a video stream and camera event data, and is sent over the stream alongside the video and audio streams. Metadata provides context to events in the digital video stream, allowing the video to be organized, searched, and retrieved easily. Metadata offers three important functions to a VMS - search, alert/alarm and reporting.

Metadata topics are mainly used to send camera or video events to the NVR/VMS. Analytics rules created in **Motion/Analytics > Rules** can be added to a metadata stream.

Enable to add Metadata streaming to the Media Profile and configure it using the parameters below.

Metadata can be analyzed by external systems, such as certain ONVIF NVR/VMS systems.

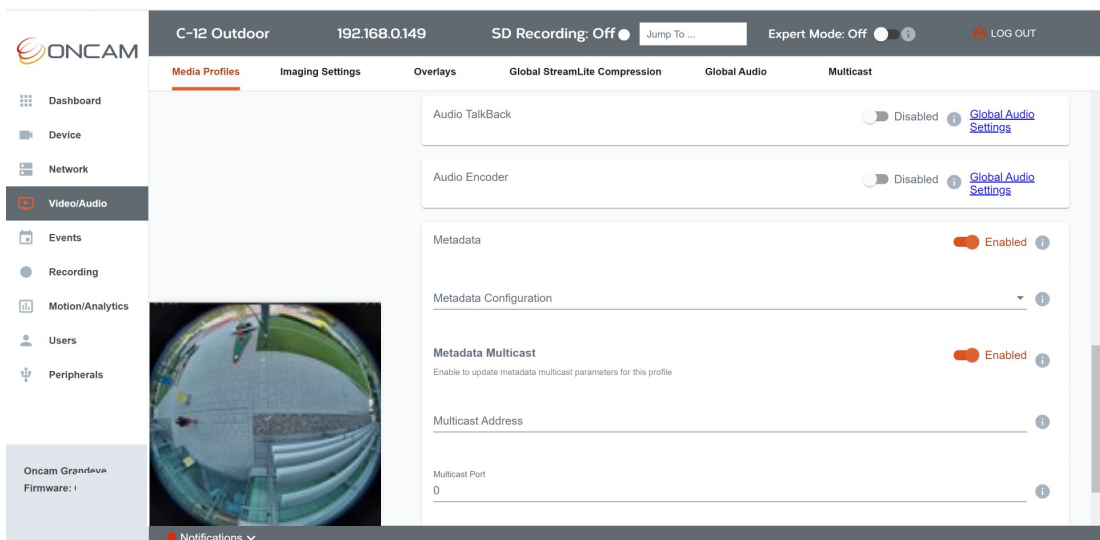


Figure 206 Media Profile Metadata

5.3.1.8.2 Metadata Configuration

Two metadata streams are created by default on the camera, select a metadata configuration from the two options available to add the metadata configuration for this media profile.

5.3.1.8.3 Topic List

Select the topics to be sent in the metadata stream. Multiple selection is possible. Any changes made to this configuration will also be applied to other media profiles that use the same metadata configuration. To use Analytics topic, a corresponding rule has to be created in the Analytics section.

5.3.1.8.4 Metadata Multicast

Use the toggle to enable Metadata Multicast and configure the settings for this profile. Set up the multicast address to store the multicast stream using the parameters below:



V2.0.x firmware or above required to access this feature.

5.3.1.8.4.1 Multicast Address

Set the IP Address of the multicast group for receiving RTP streaming. The multicast clients need this address value as well as the multicast RTP port to receive the metadata.

5.3.1.8.4.2 Multicast Port

RTP port for receiving the multicast metadata. The clients that receive the metadata use the Multicast RTP Port and Multicast Address values to receive the metadata.

5.3.1.8.4.3 Time to Live (TTL)

Sets the Time to Live value in the multicast IP packets.

5.3.1.8.4.4 AutoStart

Enable to automatically restart Metadata Multicast after the camera reboots.

5.3.1.8.4.5 Accessing the multicast stream

Once the above parameters are set and saved, stream directly via RTSP using your preferred VMS.

Invoke the GetStreamURI with multicast option via your VMS, the response will create a RTSP stream and then multicast traffic is exchanged between the clients. In this scenario RTSP will be communicated on the unicast address and RTP packet goes over the configured multicast address.

Alternatively, to stream via RTP, configure your settings and save this Media Profile. Then go to **Video/Audio > Multicast** tab and use the start / stop control next to this profile. This will invoke the StartMulticastAPI, the client will then directly use RTP with the Multicast address and port.



Refer to your VMS documentation for any additional steps to enable streaming using Multicast.

5.3.1.9 Save Media Profile

Once all Media Profile changes have been made, you will need to **Save Changes** them to apply them. If you would rather not save the changes you can select **Cancel**, this will cancel the changes except if the Video Source has been changed as this change is automatically applied.

5.3.1.10 Restore Defaults

Select **Restore Defaults** if you want to return to the pre-set defaults of the page. You can also select **Restore Defaults** if you would like to change the settings back to default settings before any changes were made.

5.3.1.11 Media Profiles Overview

Once you have saved changes to the media Profile you will be taken back to the Media Profiles summary page. The Media Profiles Table will have been updated with any significant changes, for instance, new profiles added will be shown here, and changes to existing profiles like description will be reflected in this table.

If you have changed the Video source from Fisheye to a dewarped view, this will be shown in under Mode, next to this profile the **Adjust View** icon  will be highlighted in grey. For Fisheye view this icon is not selectable.

5.3.1.12 Adjust Dewarped View

From the summary table select the **Adjust View** icon next to the media Profile view you would like to review



V2.0.x firmware or above required to access this feature.

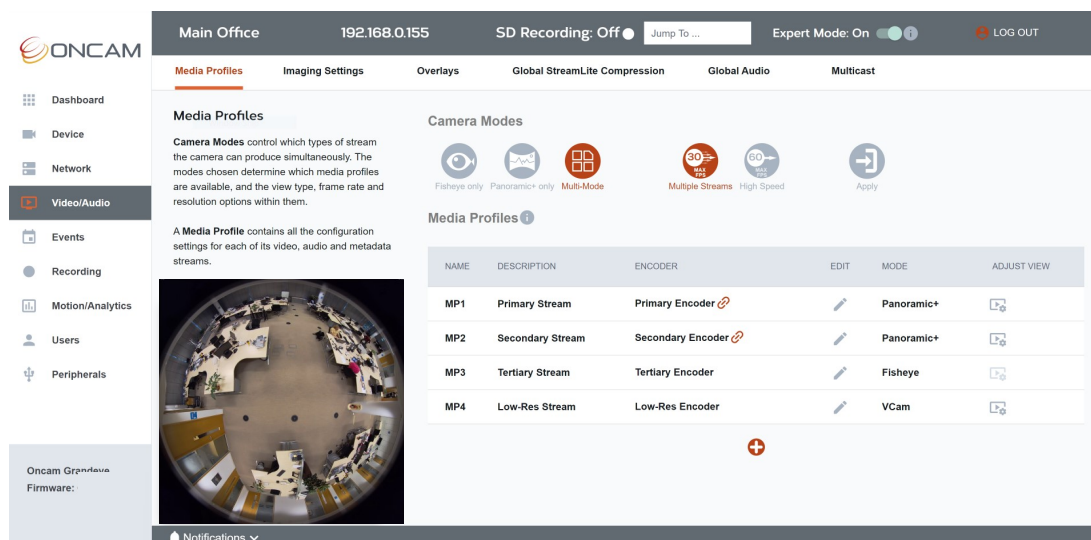


Figure 207 Media Profile Adjust Dewarped View

On selection the following page will be displayed dependent on the dewarped view

Simple easy to use mouse controls are provided in the **Adjust View** page to adjust the dewarped image to produce the best possible view for the use case.

5.3.1.12.1 Panoramic+

A 5:2 pre-dewarped panoramic view uses the center of the fisheye sensor to generate a true 180-degree image.

The camera needs to be installed on a wall and the mount position should be set to wall. Go to **Camera Web Interface > Video / Audio > Image Settings > Camera Mount Position > Wall**

The camera automatically produces a panoramic view that is a dewarped 180-degree image.

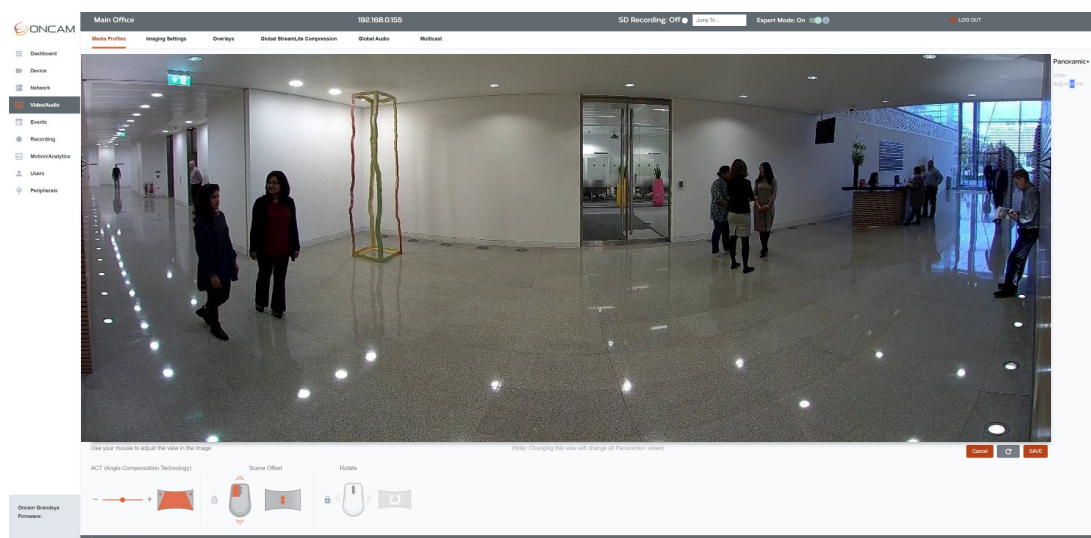


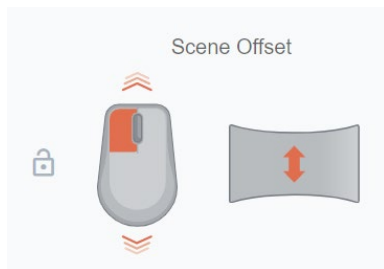
Figure 208 Media Profile Adjust Panoramic+ View

If installed flat on a wall at the correct height the image will require little adjustment.

Flat wall-mounting at a low height is ideal for capturing people's activity and faces, but depending on the usage environment, consideration should be given to the risk of people interfering with a camera that is within an easy reach.

Similar scenes may still be achieved at higher mounting heights using the Scene Offset Angle control to lower the view produced by the panorama.


In the example above the camera is mounted flat to the wall at a height of 1.7 m (5 ft 7 in), and a Scene Offset Angle of approximately -15° is used to show more of the floor area instead of less relevant ceiling.



When using this feature, it's advisable to lock the Rotate feature. To adjust the **Scene Offset**, in the image click and hold the left mouse button, then drag the mouse up and down to the desired view. Click on the lock icon to lock this setting.

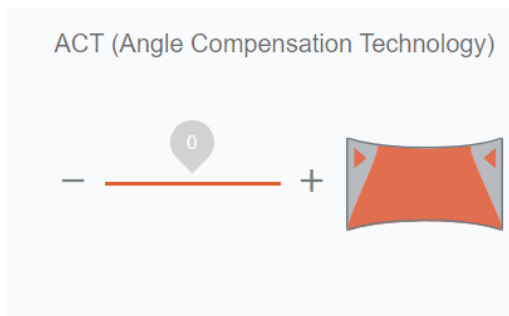
Once all view changes are made click the **SAVE** button and the view will be saved and you will be returned to the Media Profiles overview page.

CANCEL will not save your changes and return to the Media Profiles overview page.

The Reset Icon  will set the image back to default Panoramic+ settings.

Wall-mounting the Camera using a Mounting Bracket (Indoor Panoramic+ Tilt Mount or Outdoor Panoramic+ Adapter required) allows a similar area to be captured to flat wall-mounting, but from a higher vantage point. This helps keep the camera out of reach while still producing a complete 180-degree view of a large area. With ordinary panoramic cameras, mounting at an angle in this way causes a bending effect to the image, making vertical objects tilt outwards towards the sides, but with Oncam Angle Compensation Technology, they are perfectly parallel.

The purpose of the **Angle Compensation Technology** is to correct the image so that all vertical lines in the scene (such as door or window frames, pillars, lamp posts etc.) are shown vertical and parallel. When the camera is tilted downwards without this compensation, vertical objects towards the side appear to point outwards. The wall mount angle corrects this when set to the angle the camera is mounted. For example, if the camera is tilted down by 20° , the settings should be -20 . If the camera angle is unknown, the correct value can be found easily by trial and error using these simple steps:



Default is set to zero. Available Range is -45 to $+45$ degrees.




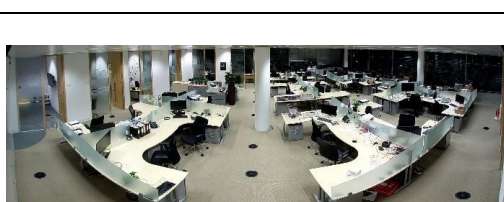
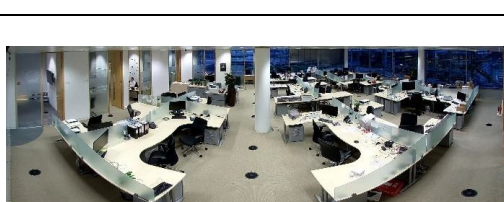
Take a guess at the angle, hover over the cursor on the slider and the current value in degrees will be shown above the cursor, click and hold the left mouse button and then drag to the desired value. For smaller increments of 1 degree click the $-$ or $+$ icons. Review the panoramic image produced by the camera. (Remember that if the camera is pointing downwards, the Mount Angle is a negative number.)

If vertical lines in the scene are leaning outwards from the middle of the image, the angle should be made more negative.

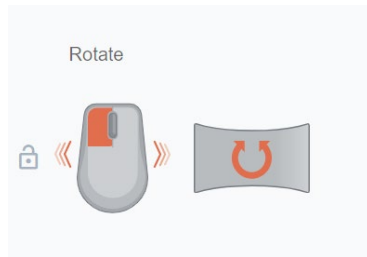
If vertical lines are leaning inwards towards the middle of the image, the angle should be made more positive.

Keep refining your guess at the angle using this simple guide until you settle on the best number.

Below is a worked example to help you:

	<p>This is the initial image with ACT set to zero. We need a negative setting because the vertical lines are leaning outwards from the middle of the image. (This camera is installed tilted downwards.)</p>
	<p>We guess the angle it's mounted at is -22° and enter that setting: A setting of -22° gives us a better result, but the vertical lines of the doorways are still leaning outwards, so we need to make it more negative.</p>
	<p>Now we guess it's -34°: A setting of -34° gives an image where the vertical lines are now leaning inwards. We've gone too far and need a setting somewhere in between -34° and -22°.</p>
	<p>This time we guess it's -25°: A setting of -25° is almost right, but the door frames near the sides of the image are still leaning outwards slightly and looking at the wall on either side of the camera, it also points outwards. We need a slightly more negative setting.</p>
	<p>This time we guess it is -27°: Perfect. All the vertical lines are nicely vertical, and the wall the camera is mounted on, can be seen on either side running parallel with the edge of the image. Now we know the camera is at an angle of -27°.</p>

The final adjustment setting for the Panoramic+ image is rotate, this is locked by default.



Click the lock icon to unlock it and it will turn orange. When using this feature, it's advisable to lock the Scene Offset. In the image, click and hold the left mouse button and move your mouse left or right and the image will rotate around the center.

5.3.1.12.2 Corridor +

A split 2-way corridor view from a ceiling mounted camera, Corridor+ allows you to watch both directions of a 360-image at the same time, with no blind spots, so that objects can move seamlessly from one view to the other.

The camera needs to be installed on a Ceiling and the mount position should be set to Ceiling. Go to **Camera Web interface > Video / Audio > Image Settings > Camera Mount Position > Ceiling**

The camera automatically produces a dewarped Corridor+ View.

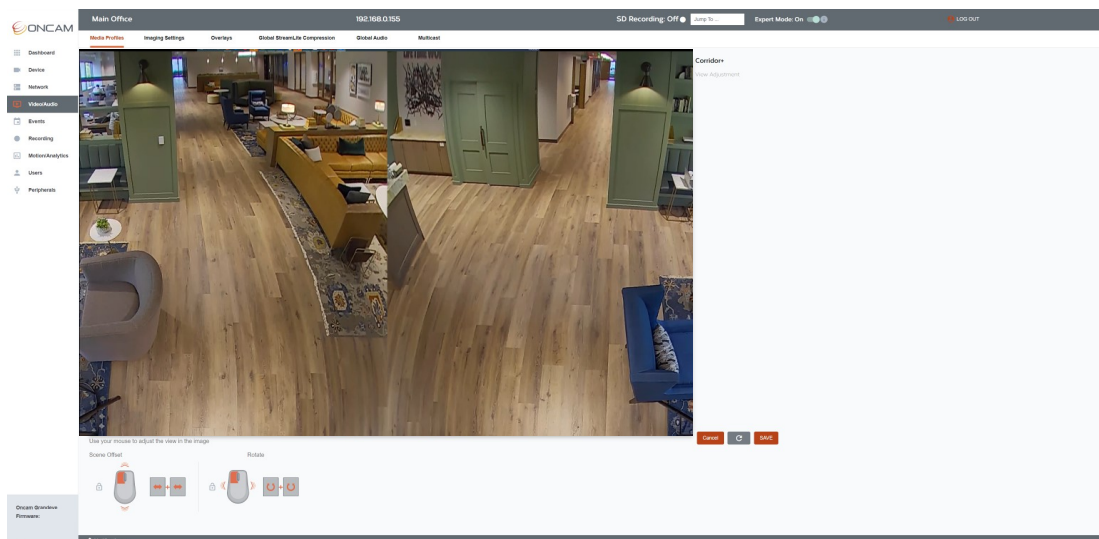


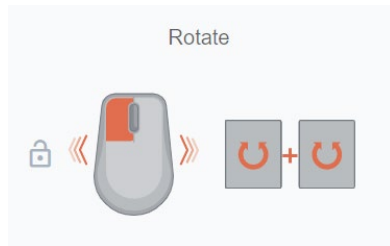
Figure 209 Media Profile Adjust Corridor+ View

Two image adjustment controls are available for this dewarped view, Scene Offset and Rotate.



Scene off set will adjust both split views left to right at the same time so you can ensue the full width of the corridor is captured. When using this feature, it's advisable to lock the Rotate feature.

To adjust the **Scene Offset**, in the image click and hold the left mouse button, then drag the mouse up and down to the desired view. Click on the lock icon to lock this setting.



When using this feature, it's advisable to lock the **Scene Offset**. In the image, click and hold the left mouse button and move your mouse left or right and both views of the image will rotate around the center.

Once all view changes are made click the **SAVE** button and the view will be saved and you will be returned to the Media Profiles overview page.

CANCEL will not save your changes and return to the Media Profiles overview page.

The Reset Icon  will set the image back to default Corridor+ settings.

5.3.1.12.3 T Corridor +

A 3-way junction view from a ceiling mounted camera, T Corridor+ allows you to see in all three directions at the same time, with no blind spots even when objects move from one view to the other

The camera needs to be installed on a Ceiling and the mount position should be set to Ceiling. Go to **Camera Web interface > Video / Audio > Image Settings > Camera Mount Position > Ceiling**

The camera automatically produces a dewarped T Corridor+ View.

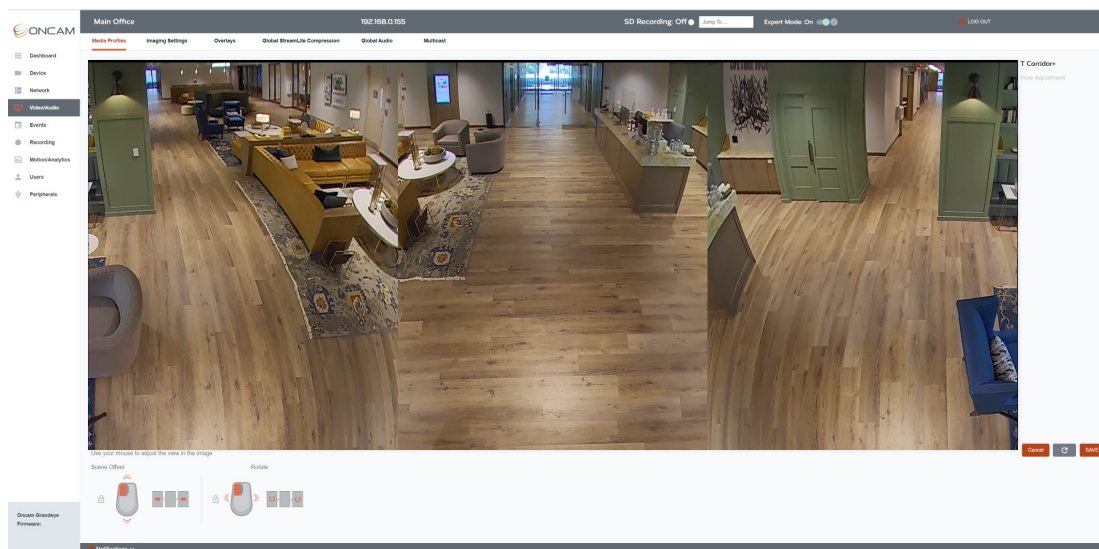


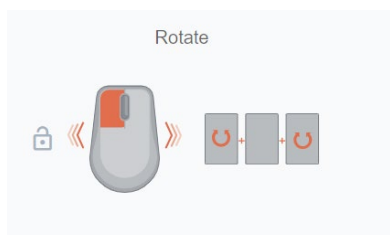
Figure 210 Media Profile Adjust T Corridor+ View

Two image adjustment controls are available for this dewarped view, Scene Offset and Rotate.



Scene Offset will adjust the left and right split views (not the one in the center) directionally moving the views from left to right at the same time so you can ensure the full width of the corridor is captured. When using this feature, it's advisable to lock the **Rotate** feature.

To adjust the **Scene Offset**, in the image click and hold the left mouse button, then drag the mouse up and down to the desired view. Click on the lock icon to lock this setting.



When using this feature, it's advisable to lock the **Scene Offset**. In the image, click and hold the left mouse button and move your mouse left or right and all three views of the image will rotate around the center.

Once all view changes are made click the **SAVE** button and the view will be saved and you will be returned to the Media Profiles overview page.

CANCEL will not save your changes and return to the Media Profiles overview page

The Reset Icon  will set the image back to default T Corridor+ settings.

5.3.1.12.4 VCam

A user defined dewarped view of a specific portion of the fisheye image, where users can decide which specific area(s) of the scene are of interest and focus on them. Up to four separate VCam's can be supported at any one time

The camera settings need to reflect the correct mount position for the dewarping to work as expected. Go to **Camera Web Interface > Video / Audio > Image Settings > Camera Mount Position >** and select Wall or Ceiling based on installation.

The camera will initially show a fisheye view that can be dewarped into the desired VCam view.

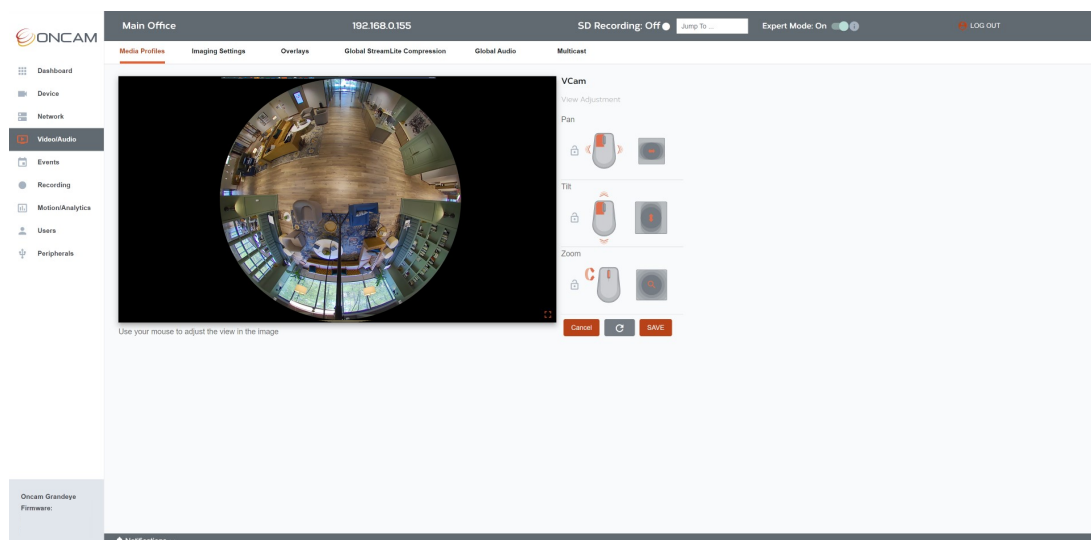
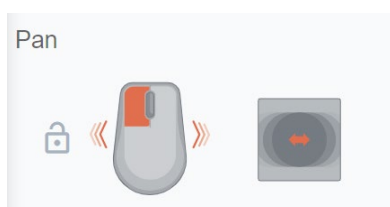


Figure 211 Media Profile Adjust VCam View

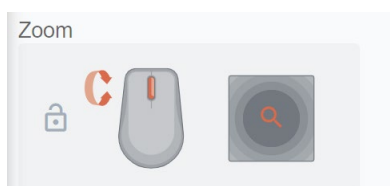
Three image adjustment controls are available to create this dewarped view, Pan, Tilt and Zoom.



Pan enables navigation around the fisheye from left to right. To adjust the **Pan**, in the image click and hold the left mouse button, then drag the mouse left and right to the desired view. Click on the lock icon to lock this setting.



Tilt enables navigation around the fisheye up and down. To adjust the **Tilt**, in the image click and hold the left mouse button, then drag the mouse up and down to the desired view. Click on the lock icon to lock this setting.



Zoom enables navigation in and out of the fisheye to get a closer look at a particular area of interest. To adjust the **Zoom**, in the image scroll the mouse wheel forwards and backwards to zoom in and out of the image. Click on the lock icon to lock this setting.

Use a combination these three settings to get the desired VCam view, as the example below shows.

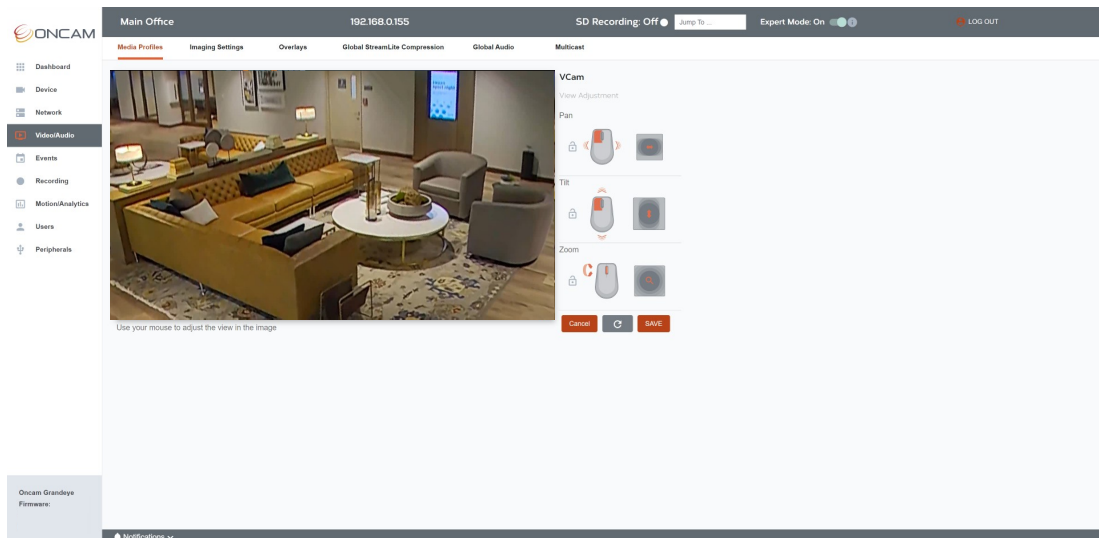


Figure 212 Media Profile Adjusted VCam View

Once all view changes are made click the **SAVE** button and the view will be saved and you will be returned to the Media Profiles overview page.

CANCEL will not save your changes and return to the Media Profiles overview page

The Reset Icon  will set the image back to default VCam settings of a Fisheye image.

5.3.2 Image Settings

5.3.2.1 Image Settings Controls

Oncam cameras are designed to adapt to the current lighting and scene conditions to produce optimal images at all times with default settings. Configure settings for any flicker-inducing, infra-red, or high dynamic range lighting conditions. Occasionally, user preferences, unusual conditions or areas of interest in the scene can require other special adjustments. Remember that manual settings that look nice in one lighting or scene condition may not work well in other conditions, so be sure to check your settings under a range of conditions before settling on them.



Settings are applied only when they are saved using the button at the bottom of the page. A few of the changes require the camera to be rebooted.

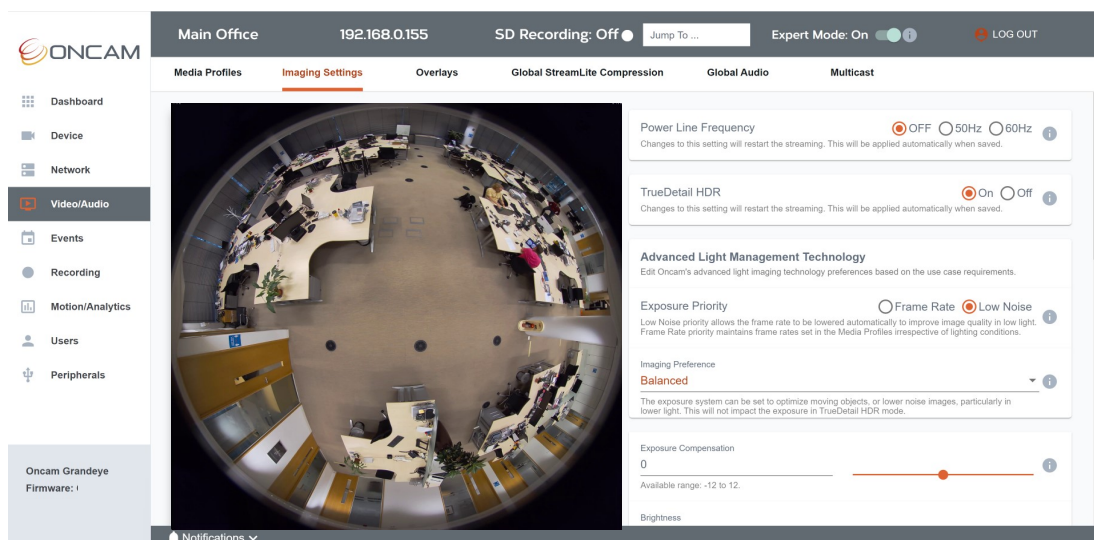


Figure 213 Image Setting Overview

5.3.2.2 Power Line Frequency

Certain types of mains-powered lighting (e.g. some LED or fluorescent lights) can induce flicker in video images because the brightness oscillates with the local electrical supply frequency. In this case, select the frequency of the local electricity supply to allow the camera to compensate for the flickering. The default is set to OFF.



V2.0.x firmware or above required to access the "OFF" feature.



Changes to this setting affect the available frame rates and so require the camera to be rebooted. Video Management Systems using ONVIF may need to be reconnected to the camera to update the list of frame rates, so it may help to make this change before adding the camera to such systems.

5.3.2.3 TrueDetail HDR

Photographers know that bright and dark areas are difficult to capture properly in a single shot. Dark areas need a longer exposure and therefore more light onto the film or sensor than the bright areas, so when both exist in the same scene, one of them loses out and detail is lost. TrueDetail HDR allows the camera to capture these "High Dynamic Range" scenes properly, by taking both a long and a short exposure and seamlessly blending them together, carefully selecting the better exposure for each area. With TrueDetail HDR, bright and dark areas can be captured together perfectly without compromise and the whole process is done tightly in a single frame to minimize any blurring or distortion of moving objects.

Two exposures are needed for each image, so the camera's maximum frame rate is 25 fps at both 50 Hz and 60 Hz in TrueDetail HDR for the C-12 and 30 fps for the C-08.



The list of available frame rates remains the same, but the rate will not exceed these limits if a higher frame rate is selected. **TrueDetail HDR is enabled by default.**

In High Speed Mode, TrueDetail HDR will not be applied to the image if the selected frame rate is above 30 fps even if it is shown as enabled in the Camera Web Interface.



TrueDetail HDR is unnecessary in low light because there are smaller variations in brightness. It is automatically switched off in these conditions to maximize exposure time and get the best image quality. There may be a brief interruption to the video when the switch occurs. The threshold for the switch is automatic and not user controllable.

5.3.2.4 Advanced Light Management Technology

Oncam's Advanced Light Management Technology dynamically manages the available light to achieve the best results in every corner of every 360-degree scene. Whether it be extreme low light or a complex mixed lighting environment, it automatically optimizes image quality whatever light available to produce clearer, full-color, lower noise surveillance videos, while maintaining the sharpness of static or moving objects even in very low light conditions. In low light, longer exposures are needed to keep the image bright and minimize noise, but some applications favor emphasis on higher frame rates or shorter exposures. You can adjust these settings to allow adjustment to cater for such requirements, go to **Video/Audio > Image settings > Low Light Technology** and adjust the settings below:

5.3.2.4.1 Exposure Priority

By default, in low light the camera can reduce the frame rate to allow longer exposures, in order to maintain image detail and color and minimize noise. To maintain the frame rate at the expense of image quality, the Exposure Priority should be changed from Low Noise to Frame Rate. When set to Low Noise, the minimum frame rate is determined by the Imaging Preference setting.

5.3.2.4.2 Imaging Preference

In low light conditions, longer exposures result in brighter images with less noise and more accurate color, but they can also result in blurring of moving objects and reduced frame rates. In brighter conditions, very short exposures can be a little noisier and less detailed, in exchange for sharply capturing fast moving objects. The Imaging Preference setting has three options to direct the camera in managing this trade-off:

Motion - Has faster shutter speeds and should be selected where capturing moving objects is most important. In this mode, the frame rate will not be reduced below 15fps in low light and moving objects will be captured with the maximum fidelity.

Balanced - Has moderate shutter speeds, aimed for optimum image quality in good light and good quality images in low light. Moving objects in lower light will exhibit some motion blur. The frame rate will not be reduced to below 4 fps in low light.

Low Light - Has slightly more generous shutter speeds in all but the brightest of conditions, maximizing image detail and reducing noise in exchange for slightly more motion blur in some conditions. Frame rate may be reduced to as low as 2 fps for optimum images in low light.



Default is set to Balanced.

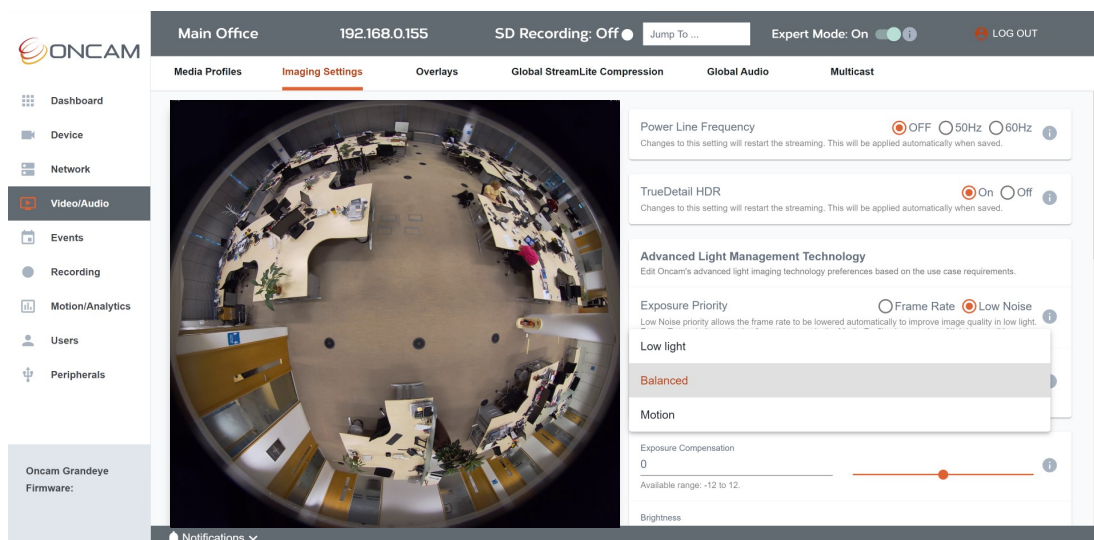


Figure 214 Image Preference

5.3.2.5 Exposure Compensation

The camera measures brightness across the whole scene to determine the best exposure for everything in the image. The aim is to capture all areas properly, assuming all of them to be equally important. Reducing Exposure Compensation favors brighter areas and increasing Exposure Compensation favors darker areas. This is useful when bright or dark areas of the scene are regarded as unimportant, for example when nearby lighting is visible from the camera. The bright light would normally cause the exposure to be reduced, making other areas darker and the Exposure Compensation could be increased to brighten the more important areas.



TrueDetail HDR may be able to achieve proper exposure of all areas without the need for Exposure Compensation but may result in an overall reduced contrast in the image.



Range is -12 to +12. Default is 0.

5.3.2.6 Brightness

Brightness increases or decreases the brightness level of the whole image evenly. Use this control to compensate for display systems with darker images.



Extreme settings can lead to clipping (bright or dark areas becoming completely white or black, resulting in loss of shading detail).



Range is 1 to 64. Default is 16.

5.3.2.7 Contrast

Contrast increases or decreases the contrast level of the whole image. Use this control to compensate for very evenly lit scenes where there will be no extremes of bright or dark.



High settings can lead to clipping (bright or dark areas becoming completely white or black, resulting in loss of shading detail).



Range is 1 to 11. Default is 6.

5.3.2.8 Sharpness

Sharpness increases or decreases the accent on edges between colors and brightness's. Increasing sharpness brings out detail and makes objects stand out, but it can also make noise more visible and increase the amount of storage required for the images.



Range is 0 to 12. Default is 2.

5.3.2.9 Saturation

Saturation controls the amount of color in the image. The default setting is calibrated to look as lifelike as possible on color-calibrated displays. Use this control to adjust the appearance of the scene on your display systems as preferred. Saturation may also be decreased to minimize color noise, for example in low-light scenes. A setting of 0 will result in completely monochrome images.



Range is 0 to 10. Default is 6.

5.3.2.10 Wide Dynamic Range

The Wide Dynamic Range control is used to increase or decrease the shading detail of bright regions in the scene. Increasing the setting reveals more shading detail in bright areas. Reducing it suppresses this detail in favor of more detail in the middle range of brightness.



This control has no effect on exposure, so if the scene is over- or under-exposed, the Exposure Compensation or TrueDetail HDR features should be used to address this, but the WDR control may be used in conjunction with those if required. Default is off.

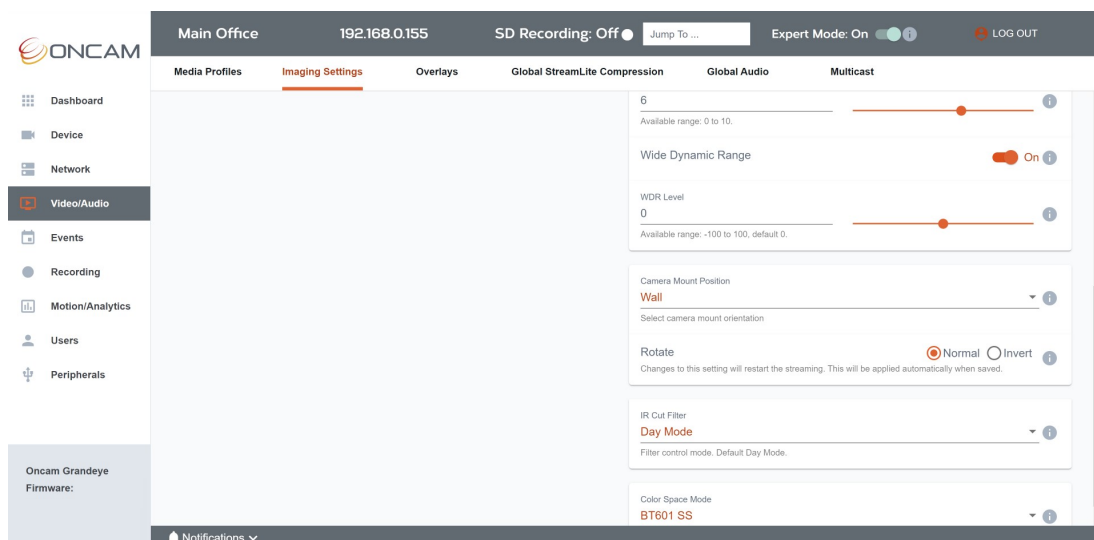


Figure 215 WDR Image Setting

5.3.2.10.1 WDR Level

The WDR level controls the degree of emphasis given to shading of brighter areas. For scenes with bright areas that feature important detail, a low WDR setting may be used to enhance the shading in those areas, increasing the difference between different shades and exposing more bright detail. For scenes that do not feature bright areas or where the bright areas are unimportant (e.g. clouds), a higher WDR setting will improve the contrast of the scene, giving more shading detail to less bright areas. A setting of 0 is the same as the Wide Dynamic Range being turned off.



This control has no effect on exposure, so if the scene is over- or under-exposed, the Exposure Compensation or TrueDetail HDR features should be used to address this, but the WDR control may be used in conjunction with those if also required.



Range is -100 to +100. Default is 0.

5.3.2.11 Camera Mount Position

This control lets any Oncam-enabled dewarping systems know in which orientation the camera is installed, so the dewarping systems can make sure the VCam images stay the right way up and move naturally. The setting can be overridden by settings in the dewarping systems but configuring them correctly in each camera means the dewarping systems can just be left in their default settings.

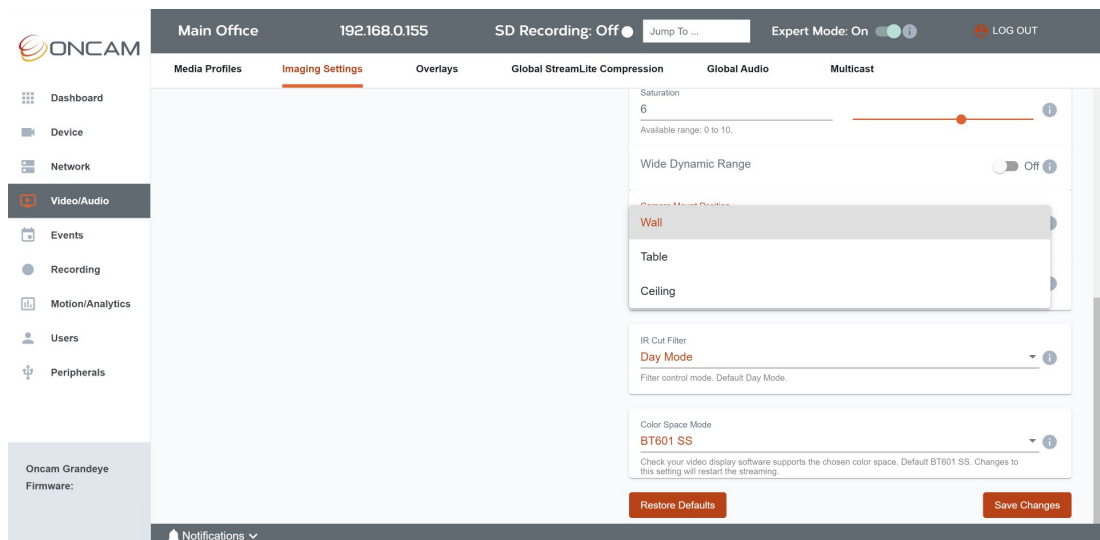


Figure 216 Camera Mounting

5.3.2.12 Rotate

This control inverts the original camera fisheye image by rotating it 180°. This allows the camera to be wall-mounted upside-down (for cable access reasons etc.) and to keep the image the right way up. It is less important for ceiling-mounted cameras but may still be used to keep all camera images in an installation pointing the same way to avoid confusion.



The invert feature is currently not working as expected on the C-08 and therefore currently not supported.

5.3.2.13 IR-Cut Filter mode

The camera has a removable IR-cut filter which is necessary for sharp color images in visible light. When insufficient visible light is present, the camera's internal mechanism can remove this filter, allowing infra-red light to be used instead. When the filter is removed, an audible click may be heard, and the filter is replaced by a glass element that allows in infra-red light. The IR-cut filter is focused for visible light and the infra-red element is focused for infra-red light. Removing the IR-cut filter with visible light present can reduce image sharpness because the glass element is optimized to focus infra-red light. Control of this switching has three modes.

Day Mode: IR-cut filter is always in place. ONVIF equivalent is "ON". Unless infra-red light is present, removing the filter provides no benefit and can cause visible light images to be less sharp, so the camera should be in "Day" mode at all times unless IR light is present.

Automatic: IR-cut filter is automatically removed when the light level in the scene falls below a pre-set threshold. The filter is switched back in once visible light returns to a level sufficiently above that threshold. The light level used for switching is determined by the user settings below.

Night Mode: When the camera is in an area with permanent infra-red illumination, the IR-cut filter mode may be set to "Night". However, any visible light also present will soften the images because it is focused differently. To avoid this, use Auto mode to switch to visible light when there is enough illumination.



Default is Day Mode.



The camera does not provide IR light itself, so an external source of IR light must be provided.

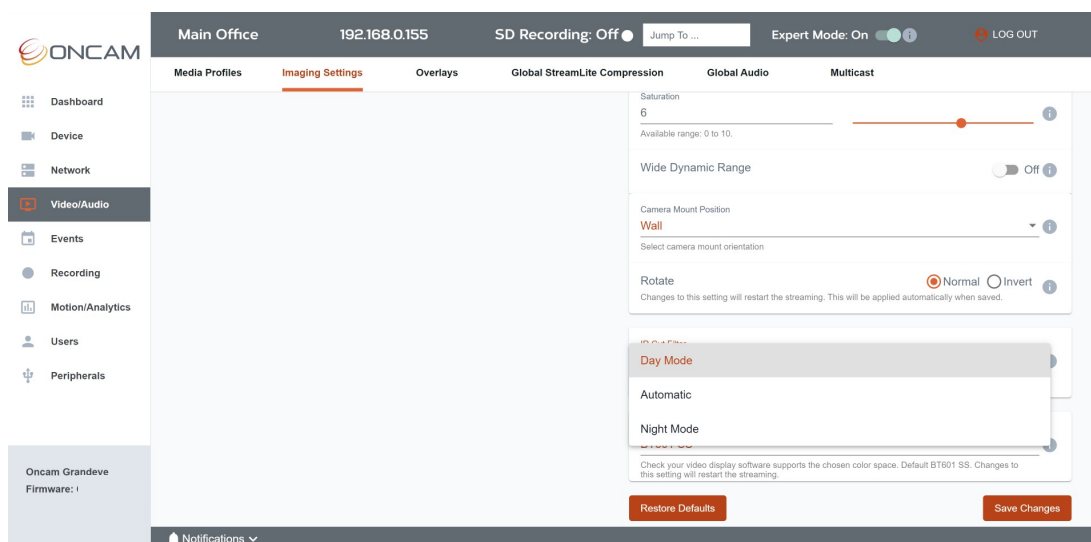


Figure 217 IR Cut Filter Mode

5.3.2.13.1 Day Mode Switch Delay Time

Set the period of time the visible light level must remain above the required threshold before switching back to Day Mode. Use this setting to prevent temporary lighting changes such as passing headlights etc. from causing the camera to switch to Day Mode unnecessarily.



Range is 5 to 20 seconds. Default is 5 seconds.

5.3.2.13.2 Switch to Night Mode Below

Set the light level below which the camera should switch to Night Mode (remove the IR-cut filter). This value is an approximate average Lux level over the whole scene. Once in Night mode, the camera only switches back to Day mode once the visible light has returned to a level sufficiently above this threshold. The light level must remain constantly beyond the respective threshold for the time set by the Night Mode/Day Mode Switch Delay Time to trigger the change in either direction.



Range is approximately 0 to 500 lux. Default is 140.

5.3.2.13.3 Night Mode Switch Delay Time

Set the period of time the visible light level must remain below the threshold set by Switch to Night Mode Below before switching to Night Mode. Use this setting to prevent temporary lighting

changes such as objects shading the camera etc. from causing the camera to switch to Night Mode unnecessarily.



Range is 5 to 20 seconds. Default is 5 seconds.

5.3.2.14 Color Space Modes

The camera supports several color space modes to suit different Video Management Systems and provide optimum performance on display systems. The camera provides the appropriate flags in the RTSP connection, to set the video stream to signal which color space mode is used and the display system should read the flags and use the appropriate color space for display. Unfortunately, many display systems do not pay attention to these flags and may display the video with incorrect colors if the camera is not set to their default mode. In this case, to avoid incorrect colors, select the mode required by the display system. If you are not sure, use BT.601 Studio Swing. If incorrect, it will have the least harmful effect on the image. In Oncam's tests, most display systems were found to use BT.601 SS regardless of the flags and so that is the default setting.

Options are:

- BT.601 Full Swing
- BT.601 Studio Swing
- BT.709 Full Swing



Default is BT.601 Studio Swing.

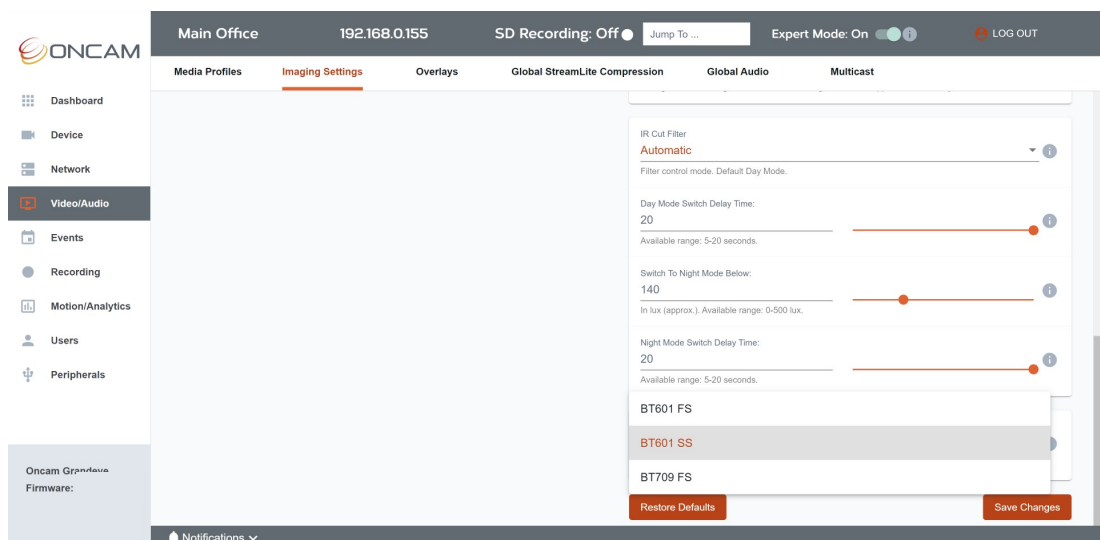


Figure 218 Color Space Mode

5.3.2.15 Save

Select **Save Changes** to apply changes made on the page. Some changes may need a page refresh to be viewed, others like TrueDetail HDR and Frequency will require a reboot to be correctly applied.

5.3.2.16 Restore Defaults

Select **Restore Defaults** if you want to return to the pre-set defaults of the page.

5.3.3 Overlays

5.3.3.1 Overlays Overview

Important information can be applied on top of the video stream in the form of Overlays. Two types of overlays are supported, On Screen Captions and Privacy Regions.



Overlays are "burned into the image", meaning that once applied they cannot be removed, therefore please ensure they do not obscure any region that could be required for evidence. Privacy Regions will be applied to the live and recorded stream, the analytics stream and motion detection regions. Analytic tracking and motion identification will not be possible in these areas.

A maximum of 3 On Screen Caption and 5 Privacy Region overlays are supported by the camera at any time.

In TrueDetail HDR mode a maximum of 2 Overlays can be supported across both categories. In this mode supporting more than 1 Overlay will reduce the maximum fps of the stream.

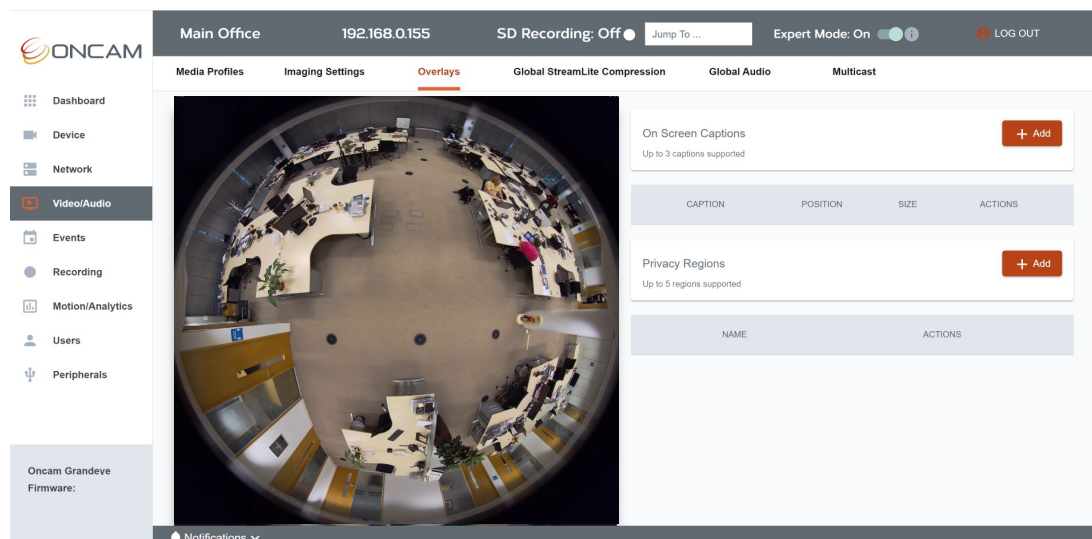


Figure 219 Overlays Overview

5.3.3.2 On Screen Captions

On Screen Captions provide extra information during the live stream and playback and can be overlaid onto the image, it is recommended to set them outside of the fisheye circle so as not to obscure the video.

Timestamp and plain text captions are supported. Up to a maximum of 3 overlays can be created.

5.3.3.3 How to create an On-Screen Caption

To create a On Screen Caption via the Camera Interface, go to **Video/Audio > Overlays > On Screen Captions** and select the **+ Add** button located in the top right-hand corner.

5.3.3.4 Configure on Screen Caption Settings

The following On Screen Caption settings can be selected and edited.

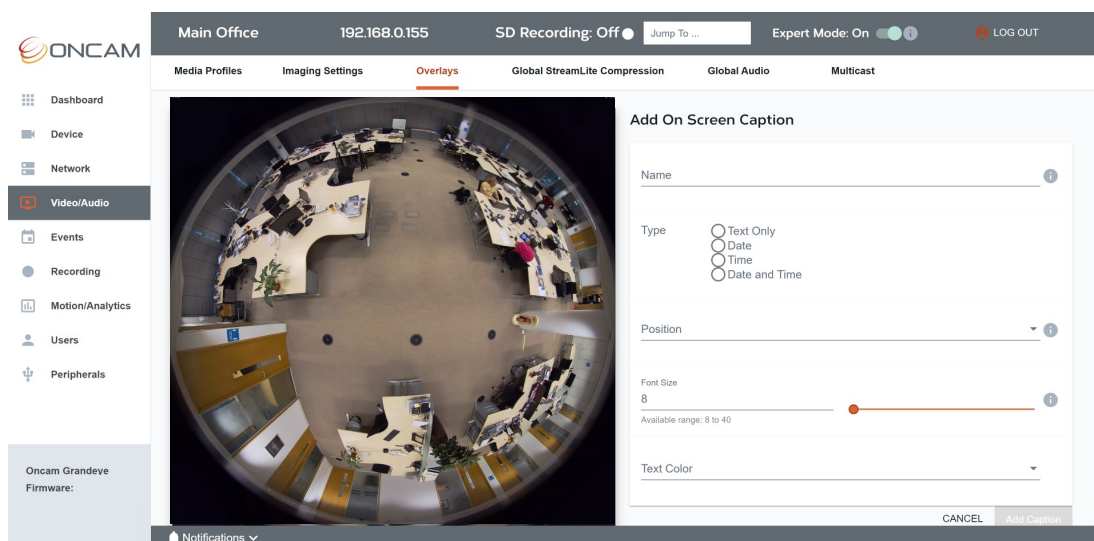


Figure 220 Overlay on Screen Caption

5.3.3.4.1 Name

Set an easily identifiable on-screen caption name.

5.3.3.4.2 Type

Select the type of caption you want to create; 4 options are available:

- Text Only
- Date
- Time
- Date and Time

If **Text Only** is selected a blank text box will be shown to enter the text.

If **Date**, **Time** or **Date & Time** is selected, you will need to choose the preferred display format from the options available.

5.3.3.4.3 Position

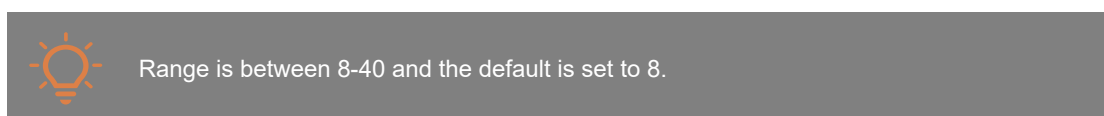
Select the positioning of the overlay, 5 options are available:

- Upper Left
- Upper Right
- Lower Left
- Lower Right
- Center

Please note the "Center" option will display the text over the middle of the image, the other options will display the text outside the fisheye image depending on size and length of text.

5.3.3.4.4 Font Size

Choose the size of the text font.



5.3.3.4.5 Text Color

Select the color of the text to be displayed. Several colors are available to choose from.

5.3.3.5 Edit on Screen Captions

To edit an On-Screen Caption via the Camera Web Interface, go to **Video/Audio > Overlays**. From the table underneath the area titled **On Screen Caption** select **Edit** next to the caption that requires editing.

Make the changes required and save them. Check the relevant fields in the table are updated and that the live stream reflects these changes.

5.3.3.6 Delete on Screen Captions

To delete an On-Screen Caption via the Camera Web Interface, go to **Video/Audio > Overlays**. From the table underneath On-Screen Caption select **Delete** next to the caption that requires removing. You will be asked to confirm this request.

5.3.3.7 Privacy Regions

Privacy Regions enable you to define and obscure specific sensitive areas on the live and recorded stream. Privacy regions use a video-embedded mask to prevent the viewing of this area for all video streams. Up to 5 regions can be created.

5.3.3.8 How to create a Privacy Region

To create a Privacy Region via the Camera Web Interface, go to **Video/Audio > Overlays > Privacy Regions** and select the **+ Add** button located in the opposite right-hand corner.

5.3.3.9 Configure Privacy Region Settings

The following Privacy Region settings can be selected and edited.

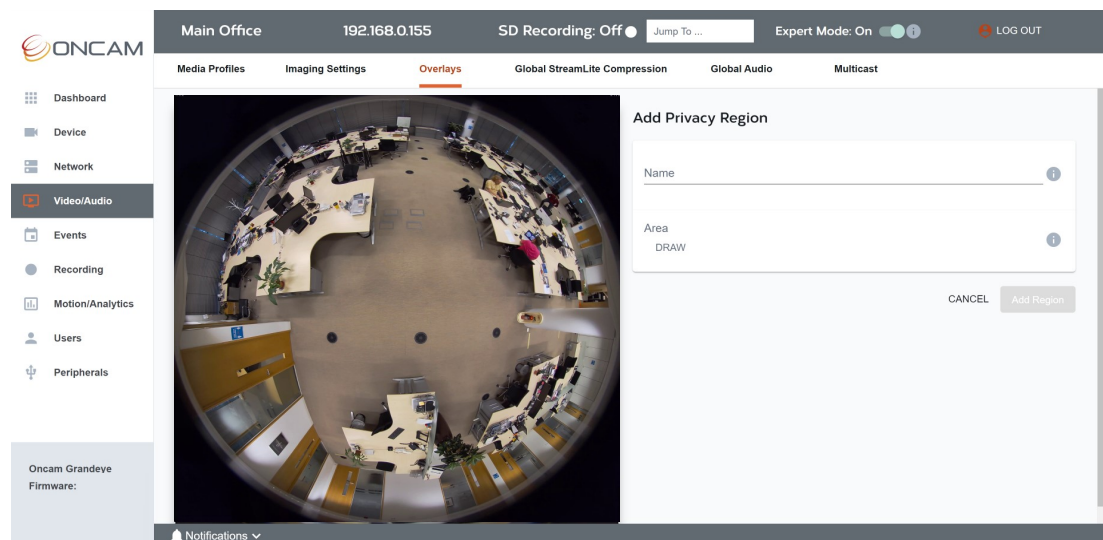


Figure 221 Overlays Privacy Region

5.3.3.9.1 Name

Set an easily identifiable Privacy Region name.

5.3.3.9.2 Draw Region

- Click **Draw** and move the mouse cursor over the image to begin creating a polygonal privacy region.
- Every left mouse click creates a point in the region. A minimum of three points is required to create a region. The name of the region will be displayed inside the region for easier recognition when you are using multiple regions.

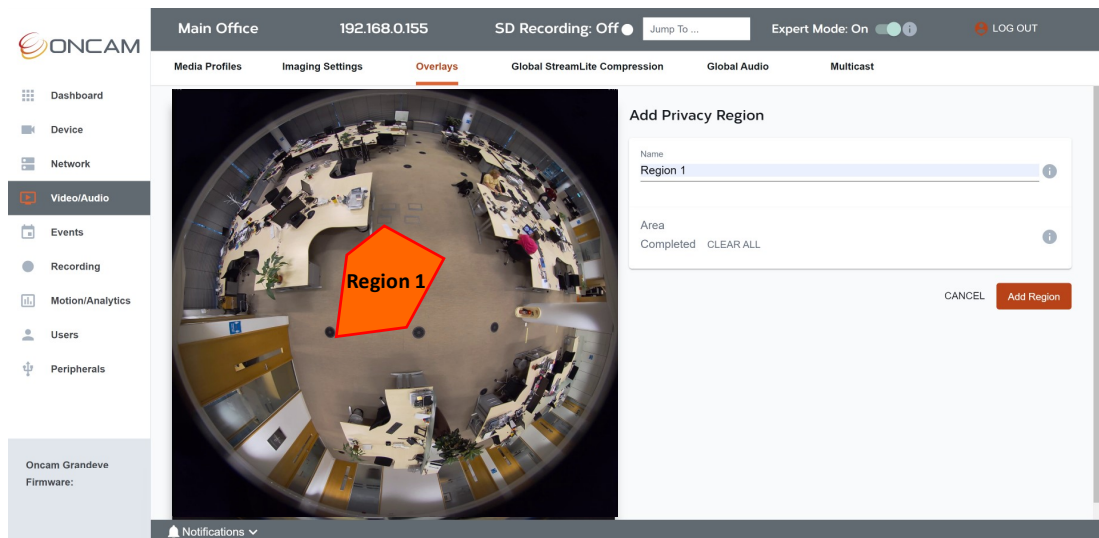


Figure 222 Video / Audio Overlays Privacy Region

Once you have finished drawing your region, move the mouse to the right, away from the image in one swift motion.

- To make any changes before saving the region, the available edit options are 'undo last point', 'clear all' and 'cancel' to start again.
- Click **Save Area** to save the region.
- Click **Add Region** to apply the region to the stream. You will be redirected to the main overlay page where the newly created Region will be displayed in the Privacy Regions table.

The region will also be displayed in video stream in the Overlay page, it will be red in color and contain the name of the region for easy identification.

When you return to the main dashboard or view the live stream via your VMS, the region will be displayed in blue, protecting the area required.

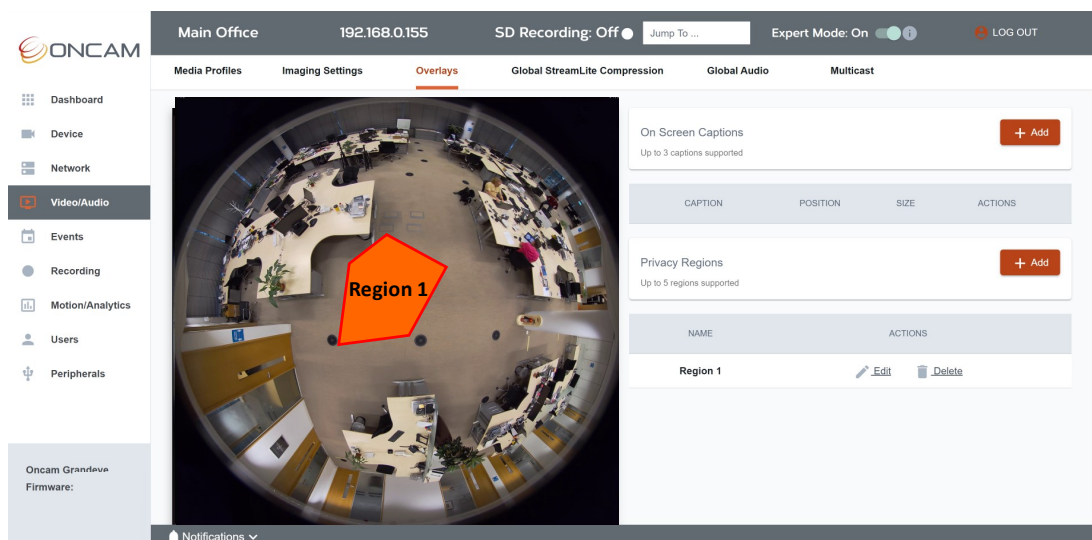


Figure 223 Video / Audio Overlays Privacy Region Overview

5.3.3.10 Edit Privacy Region

To edit a Privacy Region via the camera interface, go to **Video/Audio > Overlays**. From the table underneath the area titled **Privacy Region**, select **Edit** next to the region that requires editing.

Make the changes required and save them. Check the relevant fields in the table are updated and that the live stream reflects these changes.

5.3.3.11 Delete Privacy Regions

To delete a Privacy Region via the camera interface, go to **Video/Audio > Overlays**, from the table underneath Privacy Region select **Delete** next to the region that requires removing. You will be asked to confirm this request.

5.3.4 Global StreamLite Compression

5.3.4.1 StreamLite Compression – Global Settings Controls

StreamLite is Oncam's advanced real time adaptive video encoder enhancement technology that is applied to industry compression standards like H.264 & H.265. It uses smart dynamic object & motion-based algorithms, to analyze the video stream on the fly and identify what's really important. The desired level of quality is then applied to the areas that matter whilst less important areas can be compressed to deliver significant bandwidth savings.

StreamLite uses smart dynamic object & motion-based algorithms, namely, Dynamic Regions of Interest (ROI), Dynamic Group of Pictures (GoP) and Dynamic Frames per Second (FPS) to analyze the image in real time to determine the level of quality to apply to each element of the scene, which type of frame to create and how many to send per second in order to ensure significantly less data is transmitted and stored without losing the important details.

StreamLite control is per media profile, to enable each of the features go to: **Video/Audio > Media Profile > StreamLite Compression Settings**. For each media profile it's possible to select your preferred compression strength for Dynamic ROI, your minimum GoP and minimum FPS.

Access to global settings can be accessed via **Video/Audio > Global StreamLite Compression**.



Expert Mode needs to be turned **On** to see all the settings in this tab otherwise they will be rolled up. They can be accessed by clicking on the three dots next to each section or by turning Expert Mode On. Go to Camera Web Interface > Dashboard > Expert Mode > On

This section provides the global settings which allow the advanced user to configure and change the behavior of the compression engine to suite their use case.

This section is also where ColorMap Compression is activated globally for all streams enabling StreamLite+ and offering an additional 20% bitrate saving.

5.3.4.2 ColorMap Compression

ColorMap is Oncam's advanced color compression technology. By acting only on unperceivable colors in the scene, it can lead to an additional 20% bandwidth saving on top of traditional compression technologies. Shrink bandwidth and storage even further, without compromising image quality and level of details.

When enabled, ColorMap applies to all video streams and requires a compatible VMS integration to decode the Color Compression - Look for **StreamLite+** or **ColorMap Support**.



If your image seems dull or lacking in color when you enable ColorMap, the decode is not operating correctly.

Use the toggle to enable ColorMap Compression.

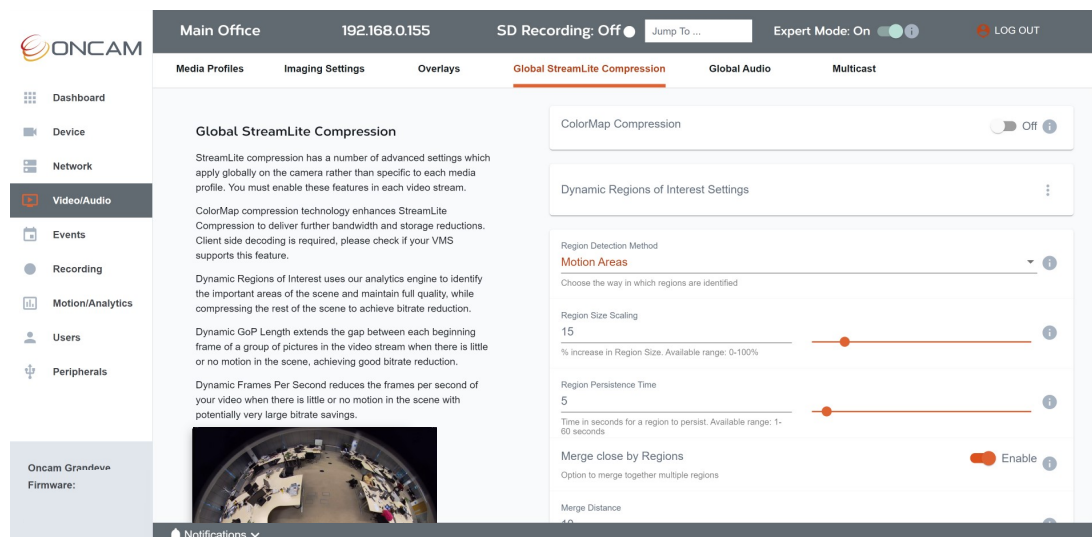


Figure 224 Global StreamLite Setting ColorMap and Dynamic ROI

5.3.4.3 Dynamic Regions of Interest Settings

See: 5.3.1.6.12.1 Video/Audio > Media Profile > Dynamic Regions of Interest.

Certain global settings for Dynamic ROI are available in this section. Advanced users can choose and configure the behavior of analytics and the compression engine to best suit their particular use case.

These advanced settings are recommended for tuning the compression to a particular scene when experience is showing some changes are needed to increase compression to better ensure all details are captured.

5.3.4.3.1 Region Detection Method

Dynamic Regions of Interest compression uses the analytics engine to identify the important areas in the scene and encodes these areas at higher quality than the background. There are two different analytics algorithms for identifying those regions.

The first and default is **Motion Areas** which looks for important movement, (to the best of its ability, disregards shadows and repetitive motion such as wind effect) and creates rectangles around the areas of movement which become the Regions of Interest.

The second is the more advanced Scene Content Analysis method **Object Tracking** which identifies trackable objects as they are moving through the scene. This method is more accurate at identifying people and moving vehicles and is more reliable in terms of avoiding irrelevant movement. To use this method the camera must be calibrated for the scene, setting the **Camera Height** correctly and the object size thresholds. Object tracking also continues to track objects even when they stop moving. It is the recommended option once calibration has been completed.

There is a third option combines the results of these two algorithms (**Motion Areas and Tracked Objects**). This option is the safest to make sure all motion and objects are identified as regions.

Calibration Settings are changed in the Camera Web Interface via **Motion/Analytics > Global Settings**.

5.3.4.3.2 Region Size Scaling

To ensure the whole area of interest is captured, a scaling factor can be applied to the region to enlarge the areas encoded at full quality around each region of interest.

Enter a percentage to increase the size of the region. The larger the region the less efficient the compression. If you are expecting fast moving objects, a larger region ensures the area in front of the object is encoded at full quality.

5.3.4.3.3 Region Persistence Time

This option allows for the Region of Interest to persist even after the analytics engine no longer considers it ended. This setting can be used to ensure the area where a person or vehicle has been, remains in high quality for a short time afterwards.

This setting is in seconds.

5.3.4.3.4 Merge Close by Regions

As two objects interact it can be beneficial in certain scenes to combine those regions into a large one to ensure the details are captured of the whole interaction.

If this option is enabled regions will grow considerably when objects interact, and thus particular attention should be paid to Region Size Scaling.



The larger the regions the less efficient the encoding.

5.3.4.3.5 Merge Distance

When 'Merge Close by Regions' is enabled it is possible to configure the range at which regions are combined. The advanced user can use the settings to tune the compression to their needs.

5.3.4.4 Dynamic GoP Length Settings

See: 5.3.1.6.12.3 Video/Audio > Media Profile > Dynamic GoP Length.

Certain global settings for Dynamic GoP are available in this section. Advanced users can choose and configure the behavior of analytics and GoP controller.

These advanced settings are recommended for tuning the compression to a particular scene when experience is showing some changes are needed to the way Dynamic GoP is triggered and how it returns to normal.

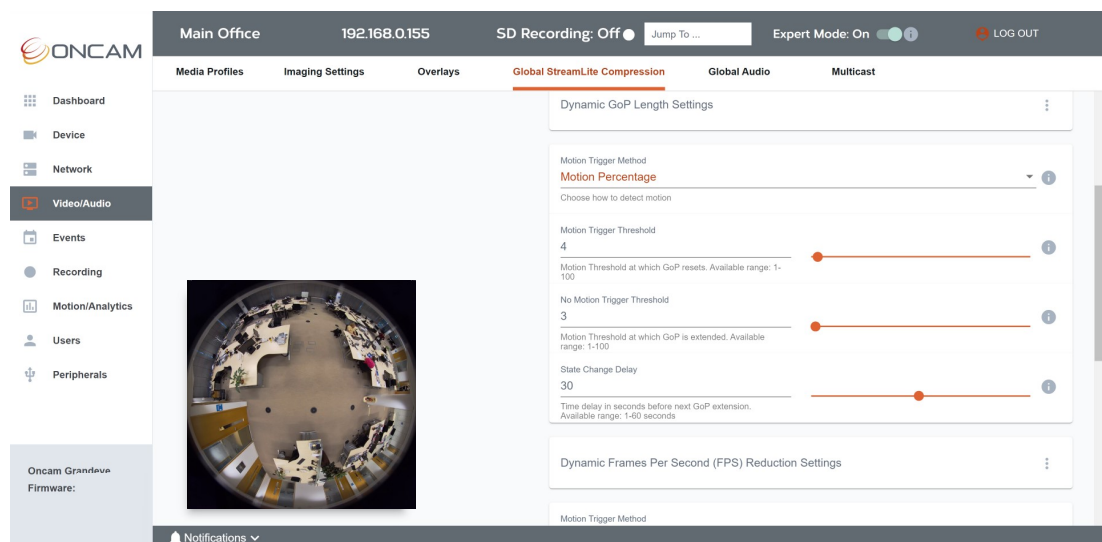


Figure 225 Global StreamLite Dynamic GoP Length Setting

5.3.4.4.1 Motion Trigger Method

There are three different analytics algorithms which can be used to trigger the Dynamic GoP feature.

The simplest and default is **Motion Percentage** which looks at the percentage of the scene which is determined to be legitimate motion.

The second is **Motion Areas**, which is the size of the largest assessed area of motion in the scene, this option might be used when a certain minimum size of motion region is desired before motion is triggered.

The third is **Tracked Objects** which triggers based on the number of tracked objects in the scene. To use this method the camera must be calibrated for the scene, setting the **Camera Height** correctly and the object size thresholds. Object tracking also continues to track objects even when they stop moving. It is the recommended option once calibration has been completed. Tracked objects is the best choice when the user only wants to return to standard GoP when a confirmed object is in the scene.

5.3.4.4.2 Motion Trigger Threshold

The motion trigger threshold is the point at which the camera considers motion to have occurred.

Depending on which Motion Trigger method is selected, the percentage trigger value is calculated slightly differently.

For Motion Percentage: 100% on the trigger threshold setting equates to 2% of the full 360-degree fisheye image moving. So, 10% equates to 0.2% of the scene.

For Motion Areas: 100% on the trigger threshold setting equates to a rectangle surrounding the area of motion being 25% of the scene, so 10% would equate to an area 2.5% of the scene.

For Tracked Objects: 100% on the trigger threshold setting equates to 10 Objects being in the scene, 10% would equate to 1 object being in the scene.

5.3.4.4.3 No Motion Trigger Threshold

The No Motion Trigger Threshold works the same way as the **Motion Trigger Threshold**, but it is the point when no motion is detected and thus the camera will switch into Dynamic GoP Length mode. No Motion Trigger should always be set the same or lower than Motion Trigger Threshold.

5.3.4.4.4 State Change Delay

Whenever motion is detected the Dynamic GoP setting will immediately return to normal mode. However, there is then a minimum time before Dynamic mode will again be triggered. This delay is controlled by this setting. It is measured in seconds. So, if this setting is at 30s, the camera will always remain in normal operation for at least 30 seconds after each motion event.

5.3.4.5 Dynamic Frame Rate Seconds (FPS) Reduction Settings

See: 5.3.1.6.12.5 Video/Audio > Media Profile > Dynamic FPS Reduction.

Certain global settings for Dynamic FPS are available in this section. Advanced users can choose and configure the behavior of analytics and Dynamic FPS controller.

These advanced settings are recommended for tuning the compression to a particular scene when experience is showing some changes are needed to the way Dynamic FPS is triggered and how it returns to normal.

The screenshot shows the Oncam web interface. The top navigation bar includes 'Main Office', '192.168.0.155', 'SD Recording: Off', 'Jump To ...', 'Expert Mode: On', and 'LOG OUT'. The sidebar on the left lists various settings categories: Dashboard, Device, Network, Video/Audio (selected), Events, Recording, Motion/Analytics, Users, and Peripherals. The main content area is titled 'Global StreamLife Compression' and contains 'Dynamic Frames Per Second (FPS) Reduction Settings'. This section includes a dropdown for 'Motion Trigger Method' set to 'Motion Percentage', a 'Choose how to detect motion' option, and three sliders: 'Motion Trigger Threshold' (value 4), 'No Motion Trigger Threshold' (value 3), and 'State Change Delay' (value 30). A live video feed of a large indoor space is displayed on the left side of the settings panel.

Figure 226 Global StreamLite Dynamic FPS Reduction Setting

5.3.4.5.1 Motion Trigger Method

There are three different analytics algorithms which can be used to trigger the Dynamic FPS feature.

The simplest and default is **Motion Percentage** which looks at the percentage of the scene which is determined to be legitimate motion.

The second is **Motion Areas**, which is the Size of the largest assessed area of motion in the scene, this option might be used when a certain minimum size of motion region is desired before motion is triggered.

The third is **Tracked Objects** which triggers based on the number of tracked objects in the scene. To use this method the camera must be calibrated for the scene setting the **Camera Height** correctly and the object size thresholds. Object tracking also continues to track objects even when they stop moving, it is the recommended option once calibration has been completed. Tracked objects is the best choice when the user only wants to return to standard FPS when a confirmed object is in the scene.

Calibration Settings are changed in the Camera Web Interface via **Motion/Analytics > Global Settings**.

5.3.4.5.2 Motion Trigger Threshold

The motion trigger threshold is the point at which the camera considers motion to have occurred.

Depending on which **Motion Trigger** method has been selected, the percentage trigger value is calculated slightly differently.

For Motion Percentage: 100% on the trigger threshold setting equates to 2% of the full 360-degree fisheye image moving. So, 10% equates to 0.2% of the scene.

For Motion Areas: 100% on the trigger threshold setting equates to a rectangle surrounding the area of motion being 25% of the scene, so 10% would equate to an area 2.5% of the scene.

For Tracked Objects: 100% on the trigger threshold setting equates to 10 Objects being in the scene, 10% would equate to 1 object being in the scene.

5.3.4.5.3 No Motion Trigger Threshold

The No Motion Trigger Threshold works the same way as the **Motion Trigger Threshold**, but it is the point when no motion is detected and thus the camera will switch into Dynamic FPS mode. No Motion Trigger should always be set the same or lower than Motion Trigger Threshold.

5.3.4.5.4 State Change Delay

Whenever motion is detected the Dynamic FPS setting will immediately return to normal mode. However, there is then a minimum time before Dynamic mode will again be triggered. This delay is controlled by this setting. It is measured in seconds. So, if this setting is at 30s, the camera will always remain in normal operation for at least 30 seconds after each motion event.

5.3.4.6 Motion Settings

This section allows you to configure the motion analytic algorithms used by StreamLite Compression.

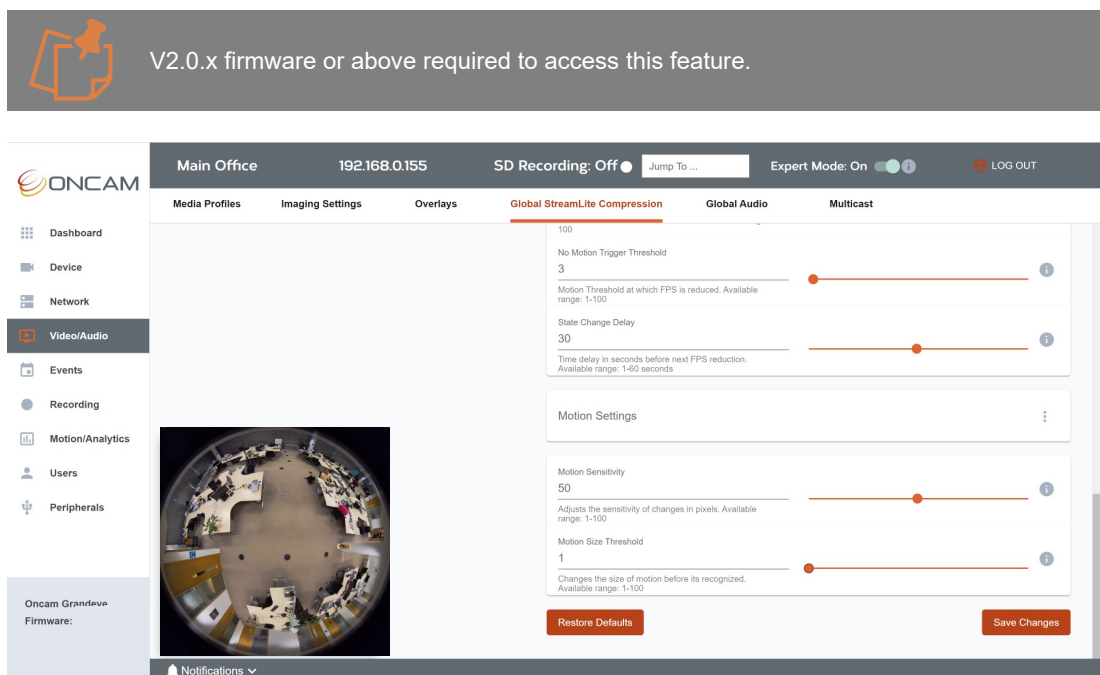


Figure 227 Global StreamLite Motion Setting

5.3.4.6.1 Motion Sensitivity

It is a scale of how sensitive the threshold is on each pixel to determine if it has changed and thus there is motion. Default Settings should work for most scenes.

5.3.4.6.2 Motion Threshold

It is a scale of how large a group of changing pixels is before it is determined as a motion area for investigation by the analytics engine. Default Settings should work for most scenes.

5.3.4.7 Save

Select **Save Changes** to apply changes made on the page.

5.3.4.8 Restore Defaults

Select **Restore Defaults** if you want to return to the pre-set defaults of the page.

5.3.5 Audio Settings – Global Audio

5.3.5.1 Global Audio settings controls

Settings on this page affect all audio streams in or out of the camera. The settings only appear when audio hardware is detected on the camera via the Plus board.

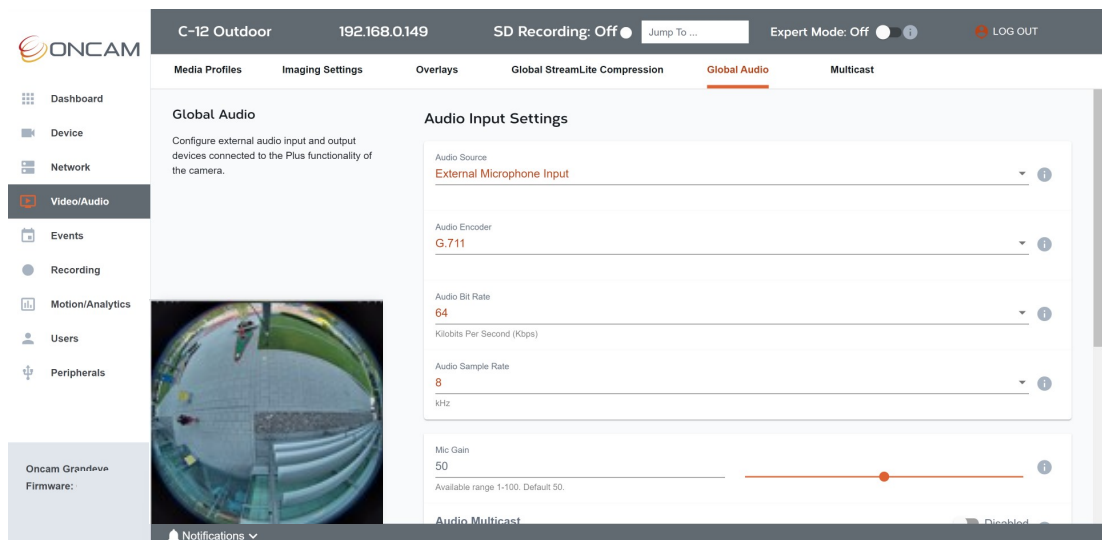


Figure 228 Global Audio Settings

Otherwise the following message will be displayed:

"This camera configuration does not support Audio. A "Plus" version of the camera is required to support audio functionality, please upgrade to the Outdoor Plus camera for audio support."

5.3.5.2 Audio not supported on Indoor Camera

A "Plus" version of the camera is required to support audio functionality.

The audio input and output hardware to support the camera's audio functions is provided on a "Plus" module. This module is fitted to only certain camera housings, such as the Outdoor Plus housing.

The Indoor version of the camera for example does not support audio because this module is not present.

If you have an Outdoor Plus camera, the audio settings can only be accessed when the required "Plus" module is present, and the camera module is mounted within the Outdoor housing. Otherwise the camera will be detected as an Indoor model.

If your camera is mounted in the Outdoor housing and the audio settings are not accessible, make sure the module is properly located and screwed down so that the correct connections are made.

5.3.5.3 Audio Input Settings

These settings control the audio input system, including the type and data rate of encoding, and input audio level.

5.3.5.3.1 Audio Source

Select the audio input to be used as the source for the camera's audio streams. The options available will depend on the specific hardware configuration. External microphone input is primary supported option.

5.3.5.3.2 Audio Encoder

Select the audio encoding standard to be used for the input audio stream. Options include G.711 and AAC.



Make sure you choose an option supported by any client systems that will stream audio from the camera.

5.3.5.3.3 Audio Bit Rate

Select the bit rate required for the audio encoder. As with video, higher bit rate requires more storage, but can offer a better-quality signal. For G.711 64 Kbps is supported.

5.3.5.3.4 Audio Sample Rate

Select the required sample rate for the audio encoder. For AAC 48kHz is supported, which provides a high-quality audio. For G.711 8kHz sampling frequency is supported.

5.3.5.3.5 MIC gain

The input level of the Plus board's "MIC" terminal is controlled by the MIC gain. Adjust this setting for optimum volume of the incoming audio without distortion.

5.3.5.3.6 Audio Multicast

Configure Audio Multicast settings for all Profiles. Enabling this option will update audio multicast parameters for all profiles. This will only be applied to profiles where the **Audio Encoder** is enabled. Go to **Video/Audio > Media Profiles** and scroll down to **Audio Encoder** and enable.



V2.0.x firmware or above required to access this feature.

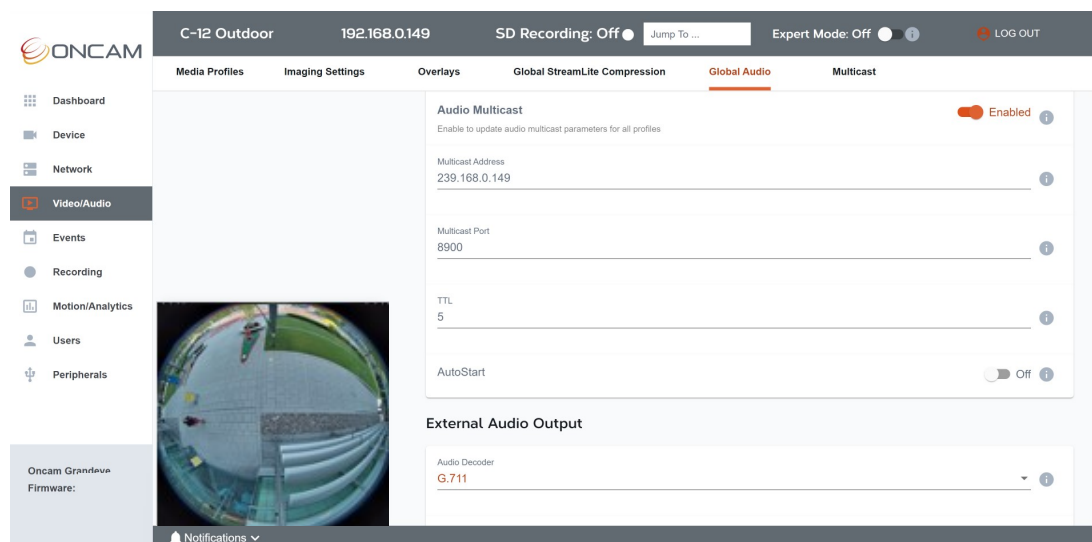


Figure 229 Global Audio Settings, Audio Multicast

5.3.5.3.6.1 Multicast Address

Set the IP Address of the multicast group for receiving RTP streaming. The multicast clients need this address value as well as the multicast RTP port to receive the audio. This is prepopulated starting "239." followed by the IP address of the camera.

5.3.5.3.6.2 Multicast Port

RTP port for receiving the multicast audio. The clients that receive the audio use the Multicast RTP Port and Multicast Address values to receive the audio.

This is prepopulated 890x

5.3.5.3.6.3 Time to Live (TTL)

Sets the Time to Live value in the multicast IP packets.

The default is set to 5.

5.3.5.3.6.4 AutoStart

Enable to automatically restart audio Multicast after the camera reboots

5.3.5.3.6.5 Accessing the multicast stream

Once the above parameters are set and saved, stream directly via RTSP using your preferred VMS.

Invoke the GetStreamURI with multicast option via your VMS, the response will create a RTSP stream and then multicast traffic is exchanged between the clients. In this scenario RTSP will be communicated on the unicast address and RTP packet goes over the configured multicast address.

Alternatively, to stream via RTP, configure your settings and save this Media Profile. Then go to **Video/Audio > Multicast** tab and use the start / stop control next to this profile. This will invoke the StartMulticastAPI, the client will then directly use RTP with the Multicast address and port.

5.3.5.4 External Audio Output

The camera's audio system will support "Talkback" features (please see note below) via ONVIF-conformant Video Management Systems. Audio signals sent to the camera from a VMS are available at the "AUDIO OUT" terminal on the Plus Board. These global settings can be used to control the audio output levels according to the connected device.

The Talkback feature is enabled at a profile level, go to **Video /Audio >Media Profiles**. Select your profile, scroll down to Audio talkback and toggle the button to enable it. Global settings for this output are configured here.



V2.0.x firmware or above required to access this feature.

5.3.5.4.1 Audio Decoder

Select the audio decoding standard to be used for the output audio stream. Options include G.711 and AAC.

5.3.5.4.2 Mute

The audio output is muted by switching on the Mute setting. No audio signals will be sent to the "AUDIO OUT" terminal while this setting is On.

5.3.5.4.3 Volume

The output level of the "AUDIO OUT" terminal is controlled by the Volume setting. Adjust the setting to achieve the output level appropriate to the connected device.

5.3.5.5 Save


Select **Save Changes** to apply changes made on the page.

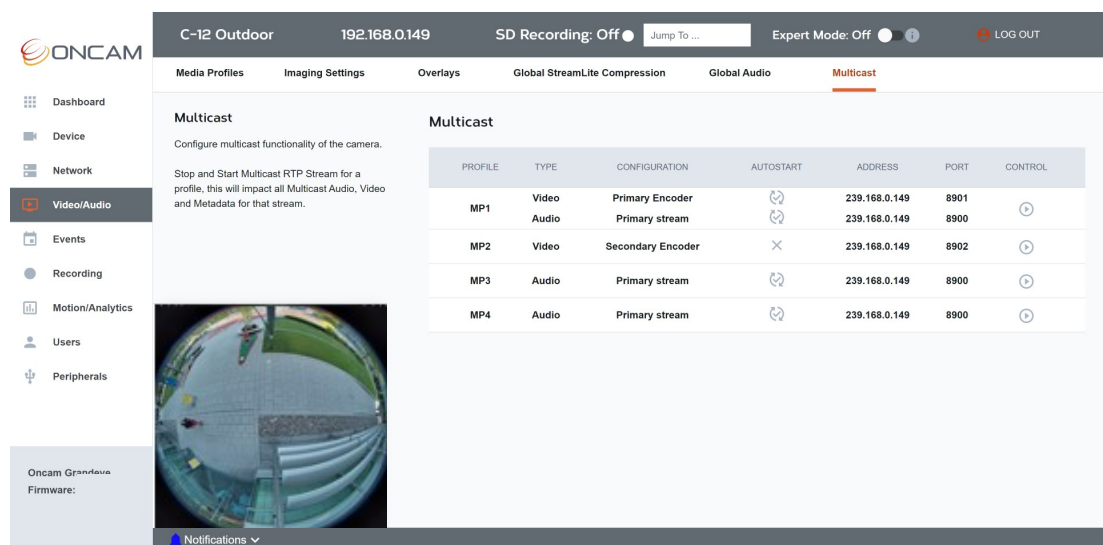
5.3.5.6 Restore Defaults

Select **Restore Defaults** if you want to return to the pre-set defaults of the page.

5.3.6 Multicast - Summary Table

As Multicast settings are configured within a Media Profile the **Multicast** Tab provides a summary table for easy viewing of all Multicast settings for the Camera. Any Multicast changes made in a Media profile will be reflected in this table.

 V2.0.x firmware or above required to access this feature.












PROFILE	TYPE	CONFIGURATION	AUTOSTART	ADDRESS	PORT	CONTROL
MP1	Video	Primary Encoder		239.168.0.149	8901	
	Audio	Primary stream		239.168.0.149	8900	
MP2	Video	Secondary Encoder		239.168.0.149	8902	
MP3	Audio	Primary stream		239.168.0.149	8900	
MP4	Audio	Primary stream		239.168.0.149	8900	

Figure 230 Multicast Summary Table

5.3.6.1 Multicast Summary Table

The summary table will display the Profile Name (e.g. MP1), Type of Multicast enabled (Video, Audio or Metadata) the encoder it is related to (Primary, secondary etc), if AutoStart is enabled, the associated address and port.

5.3.6.2 Multicast via RTP

To stream via RTP use the start / stop control next to this profile. This will invoke the StartMulticastAPI, the client will then directly use RTP with the Multicast address and port.

5.4 Recording

5.4.1 Storage Devices

5.4.1.1 Recording Overview

Where recording is referred to in the Camera Web Interface, it refers to recording directly onto the camera's SD card, also known as Local Recording or Edge Recording.

Up to 2 media profile streams can be recorded at once. The recording is dependent on the configuration of the media profile. Recording can include video, audio (Plus version of camera required) or metadata streams.

Recordings and the related configuration are created and stored on the SD card as a pair. Deleting a Recording Configuration also deletes the associated recorded video files.

The camera supports a microSD card, minimum Class 10 up to 512GB.

The card will need to be formatted to FAT32 before it can be used. To format the card using the Camera Web Interface, go to **Recording > Storage Devices**

Once the MicroSD card is inserted, it will be shown as below under the name column and inform you that the card is detected but requires formatting. Select the **Format microSD** card button on the right.

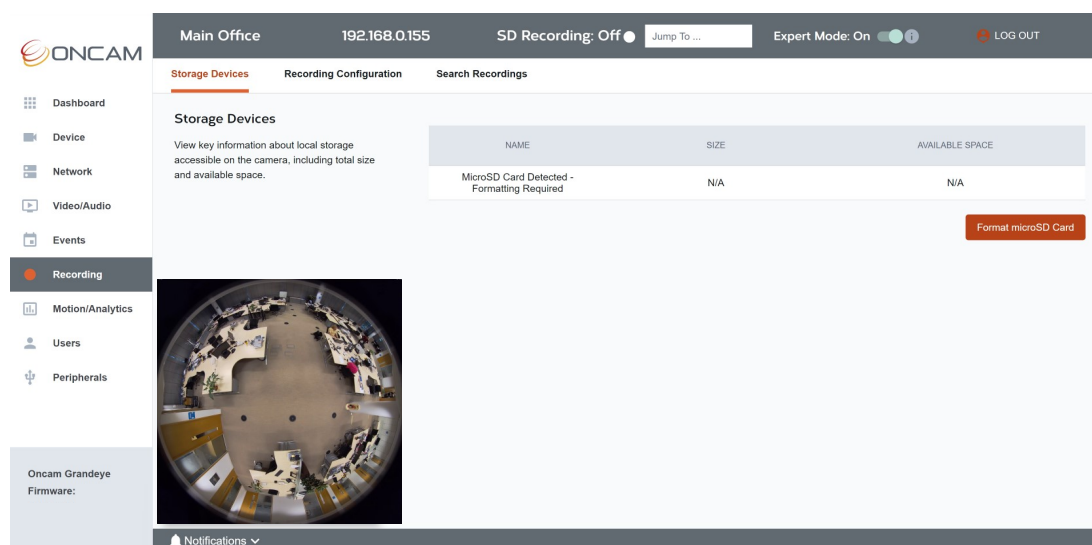


Figure 231 Recording Format microSD card

The following warning pop up message will be displayed, if you are happy to proceed select **Apply**

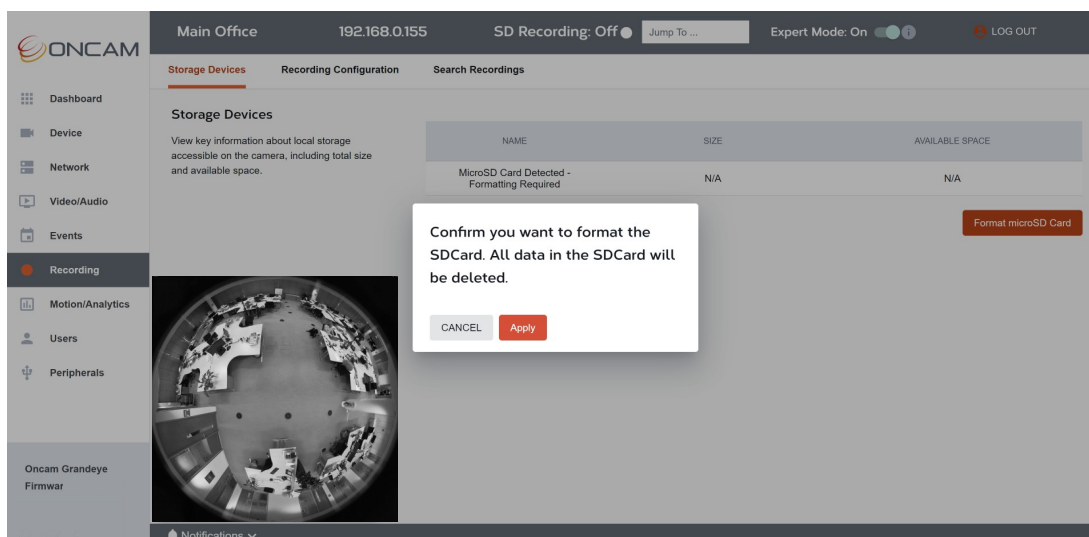


Figure 232 Recording Formatting Warning

A notification message will be displayed in the bottom left-hand corner confirming the card is being formatted.

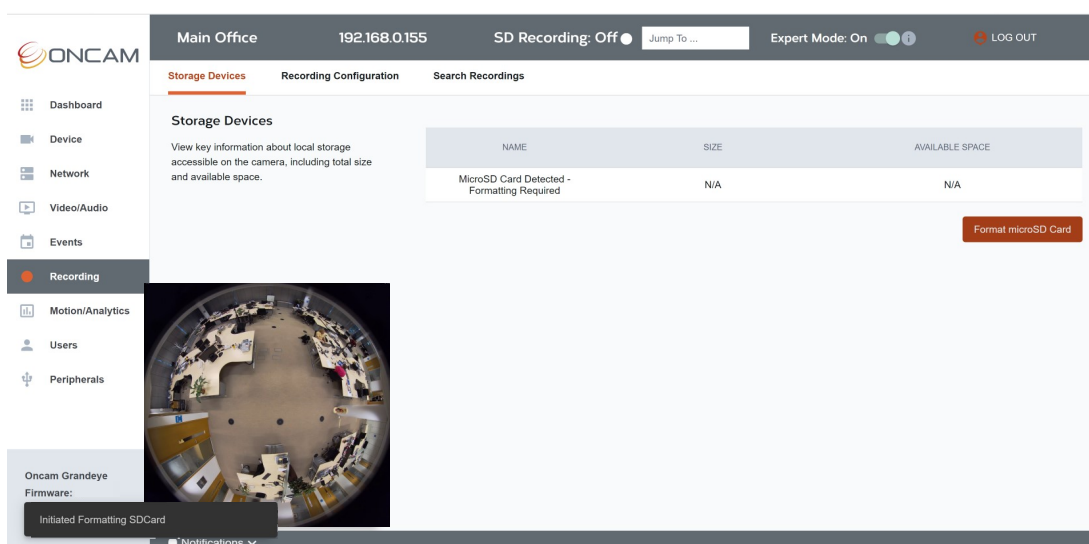


Figure 233 Recording Formatting in progress

Once successfully formatted the available space on the SD card will be displayed. You may need to refresh the page to see this update. Key information about the capacity of the card will be displayed in the table under storage devices, accessible via Recording > Storage Devices, this includes total capacity and available space. This information is updated when the web page is refreshed.

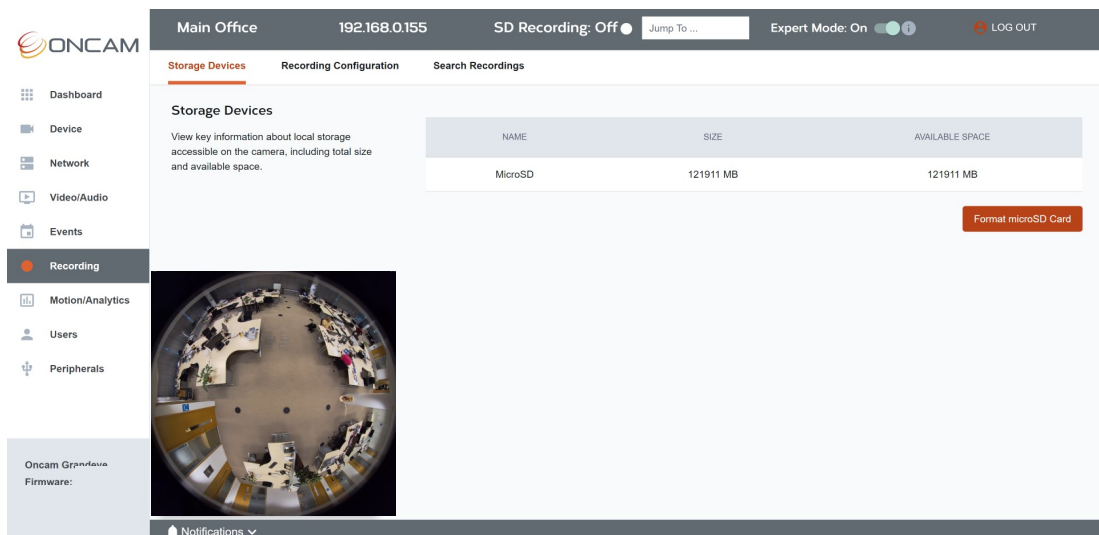


Figure 234 Recording Formatting complete

For guidance on how to insert the card into the camera module see 3.6.1 SD card Installation.

5.4.2 Recording Configuration

To instigate a recording, create a recording configuration. Two types of recordings are supported; continuous for recording all the time and event based for recordings based on a trigger such as a motion alarm.



A maximum of two recording configurations can be created and used at any one time. Only H.264 codec streams can be recorded. The output format available for download will be H.264.

The configuration overview table is accessible via **Recording > Recording Configuration** and provides an overview of the key characteristics of each configuration and controls to edit and delete them.

5.4.2.1 Create a Recording Configuration

To create a recording configuration via the Camera Web Interface, go to **Recording > Recording Configuration**, and select **+ Create Recording** button located in the top right-hand corner.

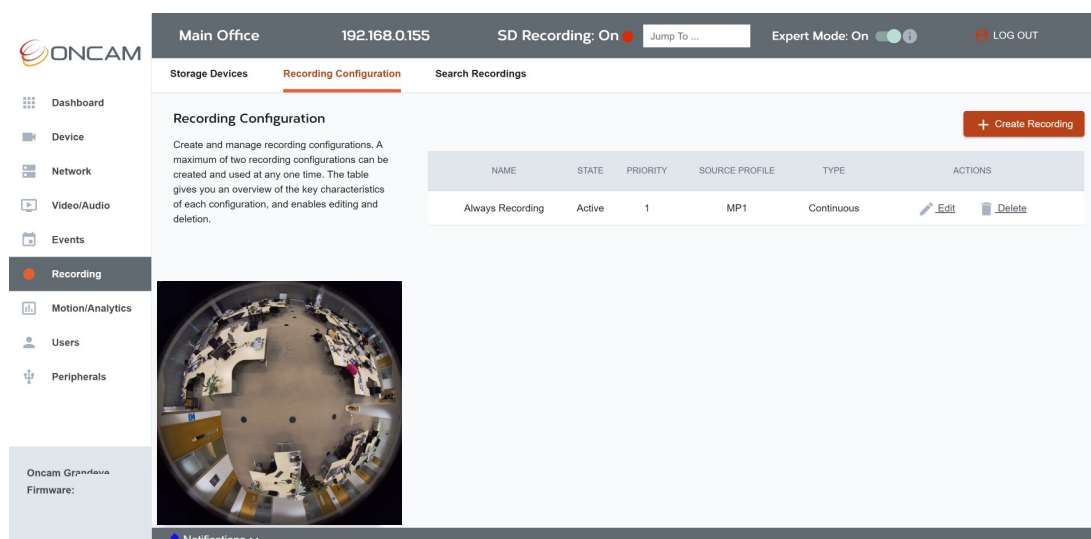


Figure 235 Recording Configuration Overview

The following recording settings can be selected and configured.

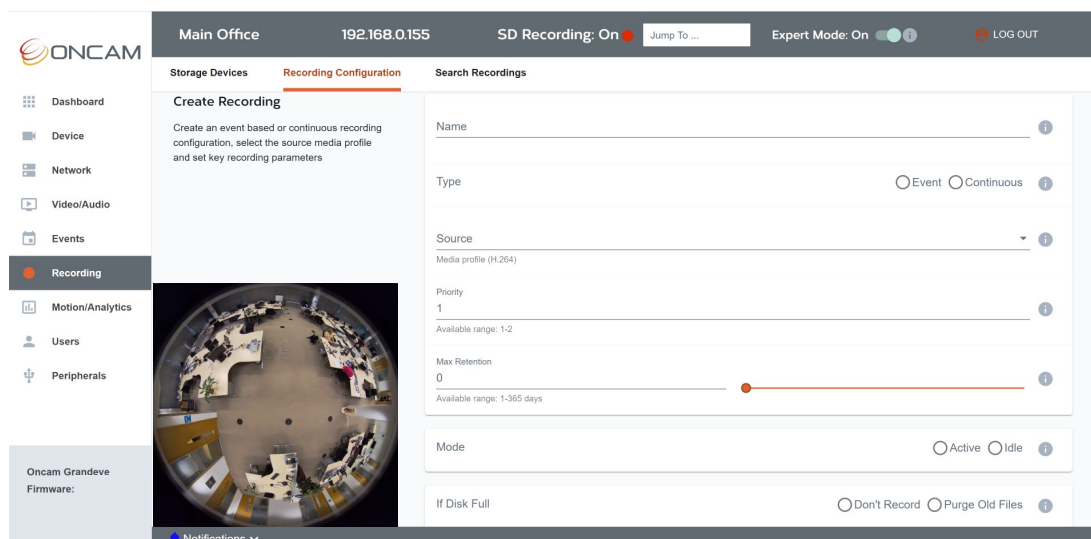
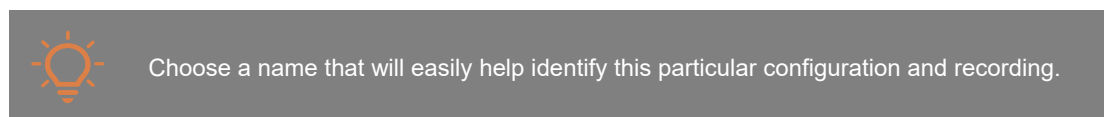


Figure 236 Recording Create a Configuration

5.4.2.1.1 Name

Set an easily identifiable recording configuration name. This is a mandatory field.



5.4.2.1.2 Type

Choose the type of recording to create; either record the stream continuously or only when it is triggered by an event.

Consider the impact on storage requirements and the storage capacity of the microSD Card. The table below provides some guidance on the amount of potential storage space required at particular bit rates.



These are estimations only and will vary significantly based on a number of factors as highlighted below.

Bitrate (Mbps)	24HR = GB*
40	432
30	324
20	216
10	108
5	54
4	43.2
3	32.4
2	21.6
1	10.8

Table 7 Storage Requirements Estimation

* Estimation only, assuming a constant bit rate and a stable level of motion in the scene. Bit Rate will vary depending on several factors, including Bit Rate control method: Constant (+/- 10%) or Fixed Quality (dependent on Quality level, Max Bit Rate level and the amount of activity and detail in the scene). Bit rate is also influenced by resolution and frame rate. If StreamLite compression is applied to the stream this will significantly impact the size of the stream being transmitted and stored. The reduction achieved will be dependent on the level and type of compression applied.

5.4.2.1.3 Source

Select the Media Profile you want to record.



Ensure the chosen profile is set to H.264 and that a Time and Date Overlay is enabled using Onscreen Captions to provide a time stamp if required.

5.4.2.1.4 Priority

Recording configurations can be given a priority level to ensure preference is given to the most important recording configuration. Set the priority level of the recording where 1 is the most important and 2 is the least.



Setting both configurations to the same level will give neither configuration priority.

5.4.2.1.5 Max Retention

Set the maximum number of days you want the camera to retain recorded footage on the SD card. Assuming there is sufficient space, once this limit is reached, the earliest recording will be overwritten.

The available range to select from is 0-365 days.

If the Maximum Retention period is set to 0 days, the camera will carry on recording until the storage is full.



This setting is dependent on the availability of sufficient storage space. If the microSD card runs out of space before the max retention period, the camera's behavior depends on the **Disk Full** setting below (5.4.2.1.7 If Disk Full).

5.4.2.1.6 Mode

Set the status of the recording. 'Active' will initiate the configuration to record. 'Idle' will place the recording on hold, which is useful if you want to stop a recording for a period of time, but plan to initiate it again in the future.



If a recording configuration is placed into Idle, it is still considered as part of the two permitted configurations, therefore a third configuration cannot be created. One of the existing configurations will need to be deleted before another one can be created and saved.

5.4.2.1.7 If Disk Full

When the storage is full, select how you want the camera to behave from the two options available.

1. **Do not Record** will stop the recording and alert you in the following ways:
 - The SD card recording message displayed in the top bar of the Camera Web Interface will switch to **off**.
 - An alert notification will be shown in the notification bar at the bottom of the Camera Web Interface.
 - A notification will also be sent to your VMS (recording job status changed to idle).
 - The Status LED on the camera will turn and remain solid red.
2. **Purge Old Files** instructs the camera to carry on recording and overwrite the oldest footage first.

5.4.2.1.8 Additional options for Event based Recording:

When selecting **Event** as the recording type the additional options below will also need to be configured.

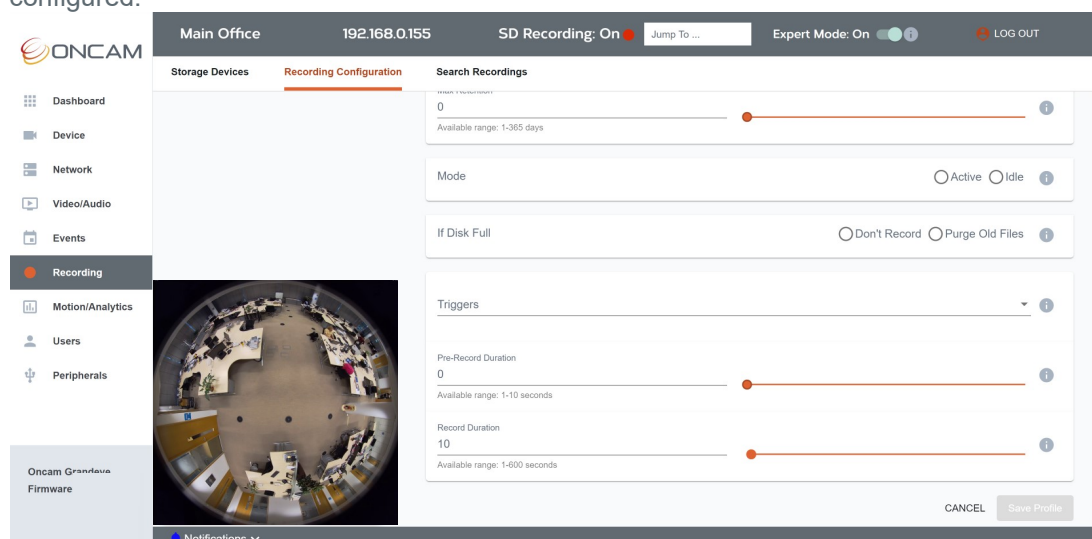


Figure 237 Event Based Recording

5.4.2.1.8.1 Triggers

Select the events that will trigger the recording. There are a number of events to choose from, for a full list and explanation of them **see 5.5.1.2.1 Triggers**. It is possible to select more than

one event to trigger the recording. This recording configuration will also be displayed as an event in the Events summary table; **Events > Alarm Rules**.

5.4.2.1.9 Pre – Record

Set the amount of time prior to the event occurring (maximum 10 seconds) that you want to pre-record to capture the lead-up to the event. This is particularly useful for events triggered by motion.

5.4.2.1.10 Record Duration

Set the total amount of time you want to record an event for after the trigger (not including pre-record).

5.4.2.1.11 Save

Click Save Profile to save your configuration.



After this defined period of time, the recording will automatically stop even if the event is still occurring. The SD card status on the top menu bar will reflect the recording state.

5.4.2.2 Editing a configuration

To edit a Recording Configuration via the Camera Web Interface, go to **Recording > Recording Configuration**. From the table select **Edit** next to the configuration that requires editing.

Make the changes required and save them.



Recording type cannot be changed. To switch between recording types, create two configurations, one of each type and enable one at a time.

Oncam Main Office 192.168.0.155 SD Recording: On Jump To ... Expert Mode: On LOG OUT

Storage Devices **Recording Configuration** Search Recordings

Recording Configuration

Create and manage recording configurations. A maximum of two recording configurations can be created and used at any one time. The table gives you an overview of the key characteristics of each configuration, and enables editing and deletion.

NAME	STATE	PRIORITY	SOURCE PROFILE	TYPE	ACTIONS
Always Recording	Active	1	MP1	Continuous	Edit Delete
Motion Recording	Active	1	MP1	Event	Edit Delete

[+ Create Recording](#)

Oncam Granview Firmware: Notifications

Figure 238 Recording Configuration Editing

5.4.2.3 Deleting Recordings and Configurations

To delete Recordings and a Recording Configuration via the Camera Web Interface, go to **Recording > Recording Configuration**. From the table select **Delete** next to the configuration that requires removal.

You will be asked to confirm your selection.



All recorded video files associated with the configuration **will be deleted** from the SD card when you delete a **Recording Configuration**.

5.4.3 Search Records

5.4.3.1 Searching for Recordings

To search for a Recording via the Camera Web Interface, go to **Recording > Search Recordings**.

Use the parameters available to narrow your search to a specific recording configuration, media profile, date and time, or broaden the search to review a wider range of recordings on the camera. Retrieve and download video, audio and metadata recordings stored on the SD card.

5.4.3.1.1 Search Filters for Video & Audio

5.4.3.1.1.1 Recording Configuration

Select a particular recording configuration or search all configurations.

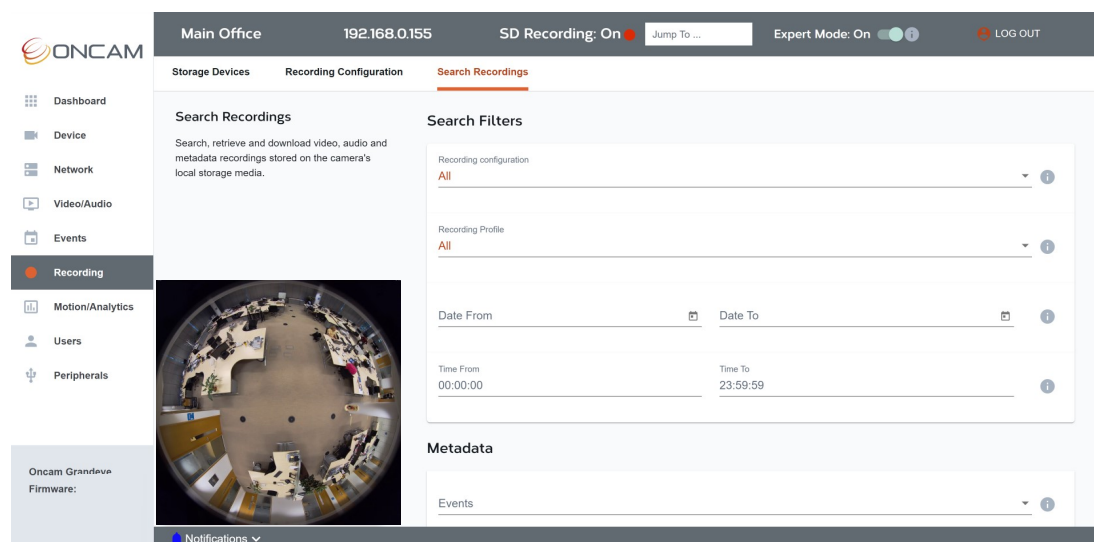


Figure 239 Recording Search

5.4.3.1.1.2 Recording Profile

Restrict the search to a particular media profile, alternatively search all available profiles.



If a particular recording configuration has been selected as a search parameter, then the media profile selected at this stage, must match the profile used in the chosen configuration.

5.4.3.1.1.3 Date

Set the date period for the search using the calendar provided. Leave blank to search for all available recordings.

5.4.3.1.1.4 Time

Set the time period for the search by manually entering the start and end time. Leave blank to search for all available recordings in the selected days.

5.4.3.1.2 Meta Data

5.4.3.1.2.1 Events

Select the events to be included in the metadata search.



The selected events must be among the metadata events that have already been included in the recorded media profile.

5.4.3.1.3 Result Options

5.4.3.1.3.1 Number of Results

To limit the search to a maximum number of results, enter the maximum value here. The search will return the results available so far when this number is reached, and the results will be displayed. Press Next to see more results.

5.4.3.1.3.2 Wait Time

To limit the waiting time before any results are displayed, enter the maximum time in seconds here. The search will return the results available so far when this time limit is reached, and the results will be displayed. Press Next to see more results.

5.4.3.1.4 Results

A results table will be displayed in **Recordings > Search Recordings** showing important recording information including type, date and time, and length of recording. More details are available about each recording if you click **View Details**, under Video, Audio or Metadata. The recording can be downloaded by selecting the **Download** option under actions next to the relevant recording.



Video recordings will be downloaded in H.264 file format. An H.264 compatible media player will be required to play these files. VLC version 2.2.2 Weatherwax is an example of a compatible player and version. Audio recordings will be downloaded in the recording format set in Global Audio Settings.

Search Recordings

Search, retrieve and download video, audio and metadata recordings stored on the camera's local storage media.

[Back To Filters](#)

NAME	DATE	LENGTH	VIDEO	AUDIO	METADATA	ACTIONS
Always Recording	Wed May 12 2021 11:27:46 GMT+0100 (British Summer Time)	05:07:05	View Details	No Audio	View Details	Download
Motion Recording	Sun May 23 2021 16:24:50 GMT+0100 (British Summer Time)	00:00:06	View Details	No Audio	View Details	Download

Oncam Granitview Firmware: [Notifications](#)

Figure 240 Recording Search Result

5.4.3.2 Impact of Camera Reboot or Reset on Recordings

If the camera is **Rebooted**, the camera configuration will be saved and unaffected. However, any active recordings will of course be interrupted while the camera reboots. The recording will restart automatically when the camera is back online and streaming.



If the camera is **Reset to Factory Defaults**, recorded files and recording configuration data will not be deleted from the microSD card. The recording configurations will be copied to the camera once the camera restarts, however the recording configurations will be changed to an inactive state and will need to be activated to restart local recording on the microSD card. The previous recorded data is still searchable and can be downloaded. To delete it, the recording configuration needs to be deleted. Go to **Recording > Recording Configuration** and select **Delete** button next to the recording configuration in the summary table.

5.5 Events

5.5.1 Alarm Rules

5.5.1.1 Alarm Rules Overview

Alarm Rules enable the camera to perform an action, for example turning on a recording or enabling a hardware output, once a specified event trigger has occurred such as motion detected in a specified region of the scene.

In this section you can create and edit event-based alarm rules. The summary table of all alarm rules is accessible via **Events > Alarm Rules** and provides an overview of the key characteristics of each configured rule, such as the event trigger and associated action type and name, as well as the controls to edit and delete them.



Event based Recording Configurations are accessible via **Recording > Recording Configuration**. These are also alarm rules, and therefore will also be displayed in the alarm rules summary table.

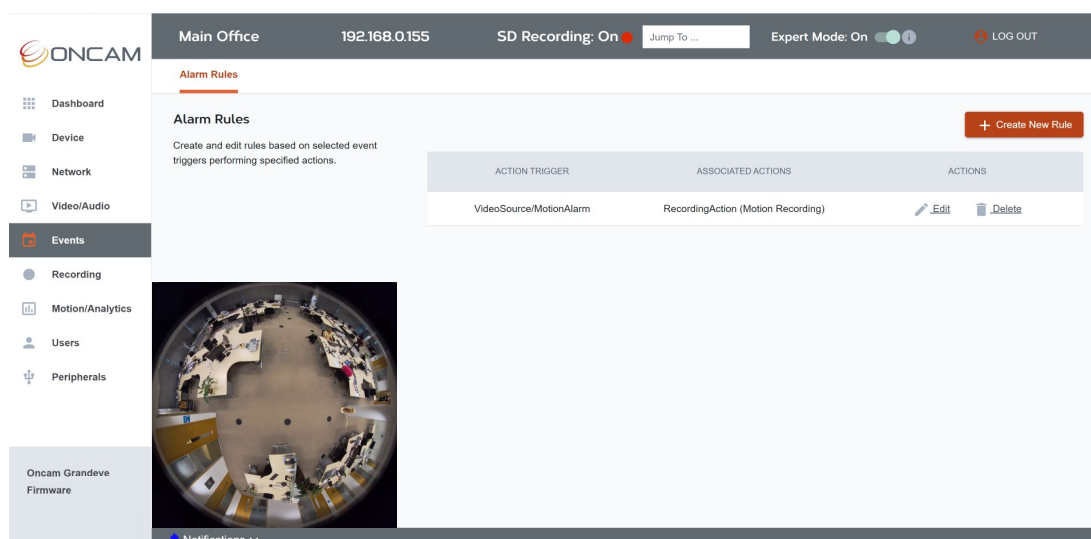


Figure 241 Events Overview

5.5.1.2 How to Create an Alarm Rule

To create an **Alarm Rule** via the Camera Web Interface, go to **Events > Alarm Rules** and select **+ Create New Rule** button located in the top right-hand corner.

The following alarm rule settings can be selected and edited.

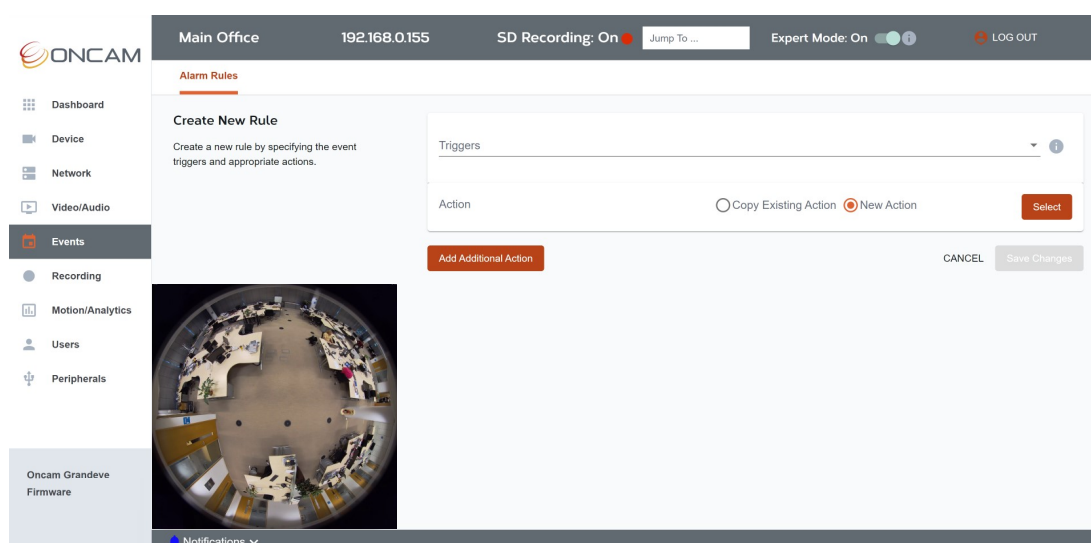


Figure 242 Events Create New Rule

5.5.1.2.1 Triggers

Select the events that will trigger the action. There are several events to choose from, a full list and explanation of them is in the table below. It is possible to select more than one event to trigger the same action.

Category	Event Trigger Name	Description
Action Engine	Completed	Camera can be configured to perform an action on behalf of the user in case of an action trigger in the camera. The following actions are supported on the camera:

Category	Event Trigger Name	Description
		1) Send an Email 2) Start Recording 3) Hardware Output (Outdoor Plus camera). The Completed event is generated when configured action has been successful. This event is sent for following actions: send an email, recording has been successful.
	Failed	A Failed event is generated when the Action configured on the camera has not been successful. This event only applies to the following actions: Failed to send an email, Recording has been unsuccessful.
Configuration	Audio Encoder Configuration	This event is generated when changes are made to the Audio Encoder Configuration such as sample rate or encoder type change. This event includes the token of the changed configuration. The camera has one audio encoder configuration that can be modified. This event can help client systems adjust their settings based on the settings that have changed.
	Metadata Configuration	This event is created when changes are made to the Metadata Configuration such as adding new topics or rules. This event includes the token of the changed configuration. The camera supports two metadata configurations that can be modified. This event can help client systems adjust their settings based on the settings that have changed.
	Profile	An update to the Media Profile triggers this event, such as removing or adding the audio encoder, audio decoder, video encoder, metadata etc. This event includes the token of the changed media profile, and the configuration change details. The camera has 4 predefined configurations and they can only be modified, not deleted.
	Video Analytics Configuration	Video Analytics Configuration event is generated when changes are made to the Analytics engine. The event includes token information for which change has occurred. The camera has a predefined configuration and can be modified only. This event can help client systems adjust their settings based on the settings that have changed.
	Video Encoder Configuration	Video Encoder Configuration event is generated when changes are made to the Video encoder configuration such as FPS or the Encoder type is changed. This event includes the token of the encoder whose configuration has been changed. The camera has four predefined encoder configurations that can be modified only. This event can help client systems adjust to accommodate the settings that have changed.

Category	Event Trigger Name	Description
Configuration/Audio Output Configuration	Media Service	This is like Configuration/Audio Decoder but is included for Profile S conformance.
Configuration/Audio Source Configuration	Media Service	This generates an event when Audio Source is changed. Outdoor Plus camera supports only one audio source.
Configuration/Video Output Configuration	Media Service	The Camera does not generate this event.
Configuration/Video Source Configuration	Media Service	This event occurs when the Video Source is changed. Two video source modes are supported, 50Hz and 60Hz. This is used to indicate a change in the frequency. Changing frequency to 50Hz will support up to a maximum 50fps and 60Hz supports up to 60fps.
Device / Hardware Failure	Storage Failure	The Storage Failure event is generated when the camera's MicroSD card is full. In addition to the event, the camera's Status LED will turn red to indicate the storage is full.
	Temperature Critical	This event monitors the camera temperature and generates an event if camera CPU reaches a threshold of 85 degrees Celsius, considered to be Temperature Critical . This event is especially useful when the camera is running in very hot environments.
Device / Operations Mode	Shutdown Initiated	The device generates a Shutdown Initiated event right before reboot. This can occur when the device is performing a reset or firmware upgrade. This is useful for clients connected to the camera to monitor if the camera is performing shutdown.
	Upload Initiated	This event is generated when an Upload is Initiated . This event precedes the Upload Status event. This is used currently to indicate upload status start.
Device / Trigger	Digital Input	When the camera detects a change in a Digital Input , it triggers this event. It includes information about the token of the digital input and the current state of the digital input, open or closed.
	Relay	When the camera generates an output over the Relay switch (Digital Output) this event is generated. It includes information about the relay token and the status of the relay.
Media	Configuration Changed	This is like Configuration / Audio Encoder but is included for Profile T conformance.
	Profile Changed	This is like Configuration / Profile but is included for Profile T conformance.
Monitor / Active Sessions	Audio Decoder	This event is generated alongside Active Connections. When a client connects to the camera over RTSP stream and the profile requested includes Audio Decoder , this event is generated. It includes information about the audio decoder token.
	Audio Encoder	This event is generated alongside Active Connections. When a client connects to the camera over RTSP stream and the profile

Category	Event Trigger Name	Description
		requested includes Audio Encoder , this event is generated. It includes information about the audio encoder token used for streaming.
	Metadata	This event is generated alongside Active Connections. When a client connects to the camera over RTSP stream and the profile requested includes Metadata , this event is generated. It includes information about the metadata token used for streaming.
	Video Encoder	This event is generated alongside Active Connections. When a client connects to the camera over RTSP stream and the profile requested includes Video Encoder , this event is generated. It includes information about the video encoder token used for streaming.
Monitoring	Link Status	This event monitors network interface status and triggers when the network link goes down or comes back up. When the link status down event is triggered, the connection with the VMS will be lost, but when the connection returns, it can help to identify what time the link went down.
	Multicast Stream Status	This event is generated to indicate when multicast stream is started and stopped.
	Network Status	This event is generated to indicate when the Network Status of the connected RTSP stream from the camera is connected or disconnected.
	Upload Status	This event is generated to confirm the Update Status of files uploaded to the camera. There are two types of uploads supported on the camera. 1. Backup restore and 2. Firmware Update. In both scenarios, this upload event updates about the percentage of the file that has been uploaded on the camera.
	Upgrade Status	This event is generated specially to indicate the firmware Upgrade Status . After the firmware is uploaded to the camera, the upgrade process starts, and this status indicates the upgrade status on the camera.
Monitoring / Profile	Active Connections	The Active Connections event is generated when an RTSP connection disconnects or connects to the camera. It includes information about the IP address of the client connected to the camera, bitrate, fps, media profile and number of clients connected.
Recording Config	Create Recording	This Create Recording event is generated when a recording configuration is created. The camera can support up to 2 recording configurations. Two types of recordings are supported; continuous for recording all the time, and event based for recording based on a trigger such as a motion alarm. Includes information about the tokens that are included in the recording.
	Create Track	The Create Track event is generated when a track is created, this typically happens when

Category	Event Trigger Name	Description
		the camera starts recording. The camera can produce 3 tracks: video, audio and metadata. Which tracks are created depends on the profile configuration.
	Delete Recording	The Delete Recording event is generated when a recording configuration is deleted.
	Delete Track	This Delete Track event is generated when a track is deleted. The reason for track deletion is when a recording is deleted.
	Delete Track Data	The Delete Track Data event is generated when a track's data is deleted to create a space for recording if MicroSD is getting full and the recording configuration's Purge Data option has been selected.
	Job State	The Recording job can be either in Idle or Active state. In Active state, camera keeps recording, in Idle state recording is stopped. This event is generated when Job State is changed.
	Recording Configuration	Recording configuration changes are updated via this event.
	Recording Job Configuration	This is generated when the Recording Job Configuration is changed from Idle to Active or vice versa.
	Track Configuration	The Track Configuration event occurs when the recording track is changed due to changes in media profile.
Recording History/Recording	State	This event is generated when the recording is stored on the MicroSD card. The recording history stores information about the State changes in the SD card.
	Audio Parameters	This event is generated when recording stored includes audio track.
	State	This event is generated when recording Track State is changed and when recording is Idle or Active.
	Video Parameters	This event is generated when recording stored includes video track.
Rule Engine/Region Object Detector	Objects Inside	Region Object Detector event is generated for checked objects state (i.e. object with ID=id is inside or not). This feature requires an analytic rule to configure object rectangles. This feature requires an Advanced Analytics license.
Rule Engine/Loitering Object Detector	Object is Loitering	Object Loitering Detector event is based on the polygon region which reports about objects staying inside it for longer than the designated threshold value. If configured, periodically this event can be sent if the object remains within the region. This feature requires an analytics rule to configure the polygon region. This feature requires an Advanced Analytics license.
Rule Engine/Region Motion Detector	Motion	Region Motion Detector event is generated for the motion alarms for a specific region defined by a polygon. Polygon region needs to be defined via the analytics rule.

Category	Event Trigger Name	Description
Rule Engine/Region Object Occupancy	Count Changed	A Region Object Occupancy event is generated based on a polygon region which would report when objects are inside it for longer than the designated Time Threshold. Every time the number of objects inside the polygon changes (for longer than the Time Threshold), an event is generated containing the information of the said objects (object's ID entry time, and dwell time). This feature requires an analytic rule to configure polygon region. This feature requires an Advanced Analytics license.
Rule Engine/Line Counting	Counter	The Line Counting event is generated based on the tripwire line. It reports the number of left-to-right and right-to-left crossings each time an object passes through it. This feature requires an analytics rule to configure a tripwire line. This feature requires an Advanced Analytics license.
Video Analysis	Motion Data Only	The Motion Data Only event generates an extra information about the motion such as the motion rectangles and the motion percentage in the scene.
	Object Tracking Data Only	This event is created for Object Tracking and generating tracked object rectangles and object ID. This feature requires an Advanced Analytics license.
	Position Coordinates	The Position Coordinates event is generated to update about object co-ordinates. This can be used in conjunction with other events from the object tracking algorithm to get further information about the object detected.
Tampering Detection	Global Scene Change	This generates an event when tampering is detected with the scene. This rule is enabled by default but needs to be enabled in metadata to be streamed.
	Image too Blurry	This event is generated when Image turns blurry, this could be useful if somebody sprays the camera lens to intentionally cause the image to be blurry. This rule is enabled by default but needs to be enabled in metadata to be streamed.
	Image too Bright	This event is generated when Image turns bright, this could be useful when somebody puts a torch light in front of camera and this event will be generated. This rule is enabled by default but needs to be enabled in metadata to be streamed.
	Image too Dark	This event is generated when Image turns dark, this could be useful when somebody puts a cloth in front of camera and this event will be generated. This rule is enabled by default but needs to be enabled in metadata to be streamed.
Video Source	Whole Scene Motion Detector	A Whole Scene Motion Detector event is generated when motion occurs in any part of the scene. This event information is also sent

Category	Event Trigger Name	Description
		over the metadata stream. By default, this rule is set up on the camera to return a Motion Alarm. This event is generated by default as part of metadata configuration.

Table 8 Events Trigger List

5.5.1.2.2 Action

Add an action to the rule that will be triggered by the event. You can add a new action or if you have previously created an action, a **Copy Existing Action** option will also be displayed with a dropdown list of available actions. If creating a new action, there are three different types to choose from, which are explained below. More than one action can be associated to an alarm rule and can be added to the rule here.

5.5.1.2.3 Action Name

Set an easily identifiable action name. The purpose of creating this name is so it is visible in the Alarm Rules summary table that you can easily select the same action again in the future when creating new alarm rules via the **Copy Existing Action** option. This field is required to create the Rule.

5.5.1.2.4 Action Type

Three action types are available to choose from. Select the response that will occur once this rule is triggered. The options are:

- 1) Send an email - Email Action will send a notifying email.
- 2) Record to the MicroSD card - Recording Action will record to the MicroSD Card for a user-defined period.
- 3) Activate Hardware output - Hardware Output (Outdoor Plus version of camera required) will activate a hardware device attached to the hardware I/O.

5.5.1.2.5 Send an Email Notification

If **Email Action** is selected the following parameters need to be completed:

Figure 243 Events Trigger Action

5.5.1.2.5.1 Subject

Enter the text to be displayed in the subject of the email. Include any key identifiers required to ensure it is given the correct level of priority. Many email systems allow rules to be set up to manage messages by subject content to help with this.

5.5.1.2.5.2 Include event

Select this to include details of the event in the email.

5.5.1.2.5.3 Snapshot Profile

The email includes a JPEG still image taken around the time of the event. From the dropdown list, select which **Media Profile** the snapshot will be obtained from. This can be from the default media profiles or from any new profiles that have been created. The resolution of the snapshot is determined by the selected Media Profile encoder resolution.

5.5.1.2.5.4 SMTP Address

Enter the IP address of your email provider's SMTP server. Please note Email notification will not sent on motion under certain circumstances, for example if using IP Address instead of DNS.

5.5.1.2.5.5 SMTP Port

Enter the network port used by your email provider's SMTP server.

5.5.1.2.5.6 Outbox Username

Enter the username of the email account to be used to send email. This must be in the form of an email address. If you need such an email account to use with this camera, free accounts are available at many online email service providers.

5.5.1.2.5.7 Outbox Password

Enter the password of the email account.

5.5.1.2.5.8 Notification Receivers

Enter the email address of the email recipients you would like notified. Separate multiple email addresses with a comma.

5.5.1.2.6 Recording

If **Recording Action** is selected the following parameters need to be completed:

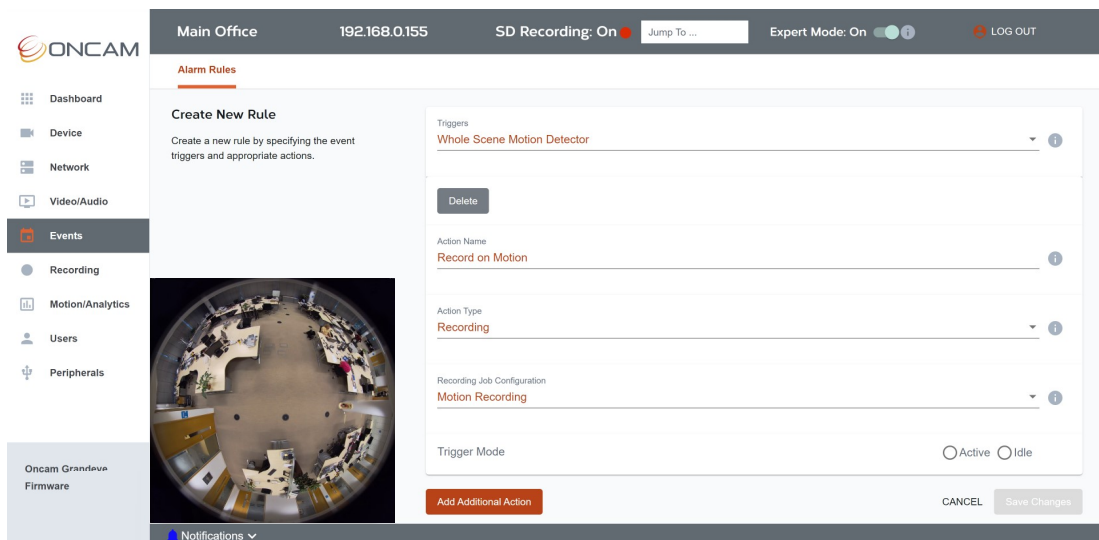


Figure 244 Event Recording Action

5.5.1.2.6.1 Recording Job configuration

Select the **Recording Configuration** action that will be triggered by the event. Only event-based recording configurations will be displayed in this list. These need to be created in the Recording Section of the camera interface **Recording > Recording Configuration**, select **+ Create Recording**.



A maximum of two recording configurations can exist at any one time. Only H.264 codec video streams can be recorded. The output format available for download will be H.264.

With Version 2.0.x firmware and above no other settings will be displayed when setting up an event as event-based recording settings such as Pre-Record Duration and Record Duration can only be set and applied from the Recording Section in the Camera Web Interface.



V2.0.x firmware or above required to access this feature.

For firmware prior to V2.0.x the following additional settings will be displayed:

5.5.1.2.6.2 Pre Record Duration

Set the amount of time prior to the event occurring (maximum 10 seconds) that you want to pre-record in order to capture the lead-up to the event. This is particularly useful for events triggered by motion.



Any changes you make to Pre-Record Duration as part of this action will overwrite the settings in the original recording configuration. The duration shown in the rule therefore may not match the duration set for this recording configuration. Check and match the values to your original recording configuration if you want it to remain the same, accessible via **Recording > Recording Configuration**. From the table select **Edit** next to the configuration to view its details.

5.5.1.2.6.3 Record Duration

Set the total amount of time you want to record an event for after the trigger (not including pre-record). After this defined period, the recording will automatically stop even if the event is still occurring.



Any changes you make to Record Duration as part of this action will overwrite the settings in the original recording configuration. The duration shown in the rule therefore may not match the duration set for this recording configuration. Check and match the values to your original recording configuration if you want it to remain the same, accessible via **Recording > Recording Configuration**. From the table select **Edit** next to the configuration to view its details.

5.5.1.2.6.4 Trigger Mode

Set the status of the recording. Active will enable the configuration to record. Idle will place the recording on hold, which is useful if you want to stop a recording temporarily but plan to initiate it again in the future.

5.5.1.2.7 Hardware Output

If **Hardware Output** is selected (Outdoor Plus version of camera required) the following parameters need to be completed:

5.5.1.2.7.1 Output

Select which Hardware output will be triggered. There are three options to choose from:

- 1) Alarm out
- 2) LED 1
- 3) LED 2

For details on the differences between these, see *Table 11 Plus Module Alarm Output*

5.5.1.2.7.2 State

Set the activity state of the **Hardware Output**. Active will enable the output to operate. Inactive will stop the output from operating, which is useful if you want to stop the signal from being sent temporarily but plan to enable it again in the future.

5.5.1.2.8 Adding another action

Select the **Add Additional Action** button to add further actions to this rule. The same format will be used to set up the next action for the rule.

5.5.1.3 How to Edit an Alarm rule

To edit an Alarm Rule via the camera interface, go to **Events > Alarm Rules**. From the table select **Edit** next to the rule that requires editing.

Make the changes required and save them.

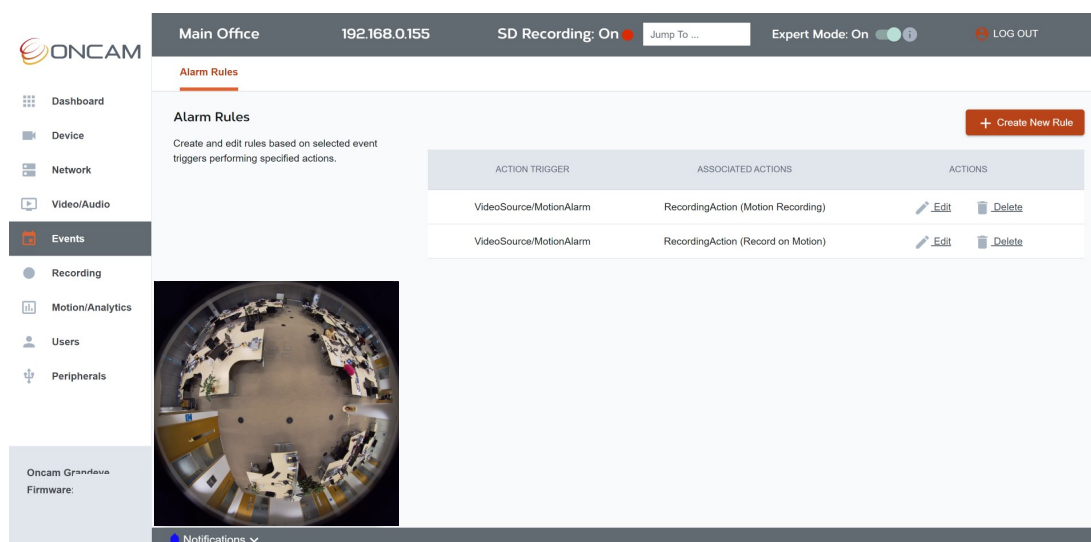


Figure 245 Events Edit Rule

5.5.1.4 How to Delete a Rule

To delete an Alarm Rule via the Camera Web Interface, go to **Events > Alarm Rules**. From the table select **Delete** next to the rule that requires deleting.

You will be asked to confirm your selection.

5.6 Motion / Analytics

5.6.1 Rules

5.6.1.1 Motion and Analytics Rules Overview

This section allows you to configure the advanced analytics engine and create rules for which analytics should run on the camera. You should only turn on rules you need as each one uses camera resources. Each rule creates different events in the camera, these events can then be used in two ways. You can access them in the events section of the camera to trigger actions such as emails or IO control, or you can receive metadata including all the events in your video stream. To add these rules to your streams via the Camera Web Interface, visit **Video/Audio > Media Profiles > Metadata Configuration** section and configure your media profiles to send a set of metadata.

Events from these rules are also available via the ONVIF pull point method.

The standard analytic types are:

- 1) **Region Motion Detector**
- 2) **Motion Data Only**
- 3) **Whole Scene Motion Detector**
- 4) **Tampering**

Depending on your chosen NVR/VMS and the vendor of the solution, you may also have the option of adding an analytics license to the camera.

Depending on your analytics license the following additional Analytics Types are available:

- 1) **Loitering Object Detector**
- 2) **Line Counting**

- 3) **Region Object Detector**
- 4) **Object Tracking Only**
- 5) **Region Object Occupancy**

To request a license, send the Device Serial number and MAC address (which can be found in the **Device > Device Information** section) to a C-Series camera vendor. Licenses are added via the Camera Web Interface in **Device > Licenses**.

It should be noted that the ONVIF **Motion Alarm** output is triggered by any of the following rules:

- Whole Scene Motion Detector
- Region Motion Detector
- Region Object Detector

Global settings for the persistence and delay of the motion alarm event are accessible at: **Motion/Analytics > Global Settings**.

5.6.1.2 How to Create a New Rule

Create a new motion or analytic rule by selecting the **+ ADD RULE** button in top right-hand corner. Each rule creates its own events and data. You must give each rule a unique name and then configure the appropriate options for each rule.

NAME	TYPE	ACTIONS
Default Whole Scene Motion Detection	Whole Scene Motion Detector	Edit Delete
Image Too Dark	Tampering Detection	Edit Delete
Image Too Bright	Tampering Detection	Edit Delete
Global Scene Change	Tampering Detection	Edit Delete
Image Too Blurry	Tampering Detection	Edit Delete

Figure 246 Motion Analytics Overview

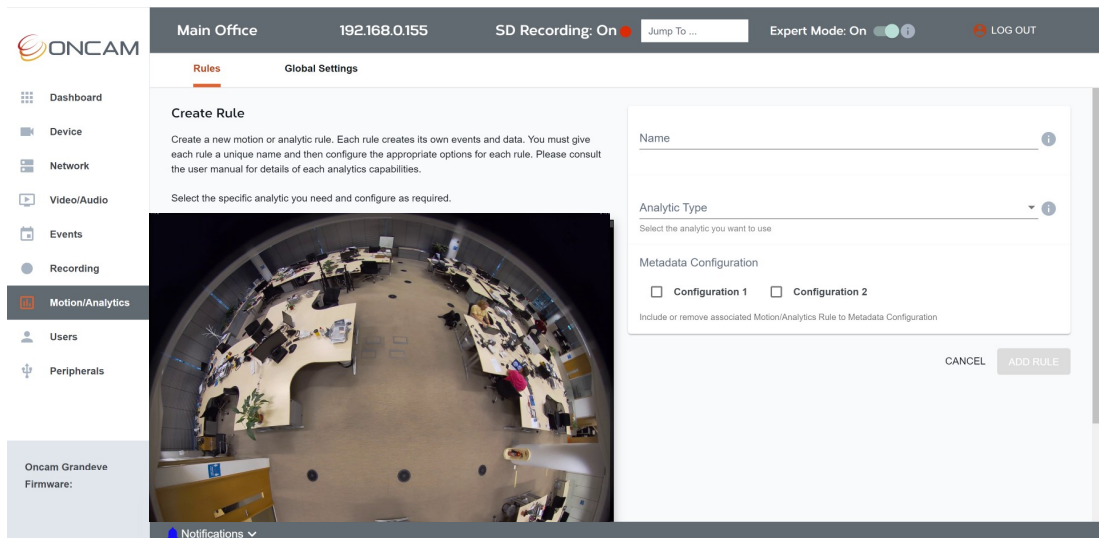


Figure 247 Motion Analytics Create New

5.6.1.2.1 Name

When creating a rule, you must choose a unique name for the rule and the associated events and metadata created.

5.6.1.2.2 Analytic Type

Select the specific analytic you need. This list is dependent on the license you have for your camera so you may need to request a license key to access specific analytics. Depending on the analytic you choose there may be further options to configure which you will see below.

The standard analytic types are:

- 1) **Region Motion Detector**
- 2) **Motion Data Only**
- 3) **Whole Scene Motion Detector**
- 4) **Tampering**

Depending on your chosen NVR/VMS and the vendor of the solution, you may have the option of adding an analytics license to the camera.

Depending on your analytics license the following additional Analytics Types are available:

- **Loitering Object Detector**
- **Line Counting**
- **Region Object Detector**
- **Object Tracking Only**
- **Region Object Occupancy**

5.6.1.2.3 Region Motion Detector

For this analytic, only motion which is centered inside the region will create an event. Motion Alarm is also triggered by this analytic.

Draw and save a region then arm the regions to create associated events and metadata.

Multiple Rules of this type can be created.

This rule creates the following events and metadata:

tns1:RuleEngine/MotionRegionDetector/Motion

Sample Data:

```
<tt:Source>
<tt:SimpleItem Name="VideoSource" Value="VideoSource"/>
<tt:SimpleItem Name="RuleName" Value="MotionRegion1"/>
</tt:Source>
<tt:Data>
<tt:SimpleItem Name="State" Value="true"/>
</tt:Data>
```

This rule also creates the following events and metadata:

tns1:VideoSource/MotionAlarm

Sample Data:

```
<tt:Source>
<tt:SimpleItem Name="Source" Value="VSC"/>
</tt:Source>
<tt:Data>
<tt:SimpleItem Name="State" Value="false"/>
</tt:Data>
```

5.6.1.2.3.1 Region Area

To create a region, click **Draw** and then click up to 16 corners of the region on the video image to create your region. When you have clicked your last point, the region will close automatically when you hit **Save Area**.

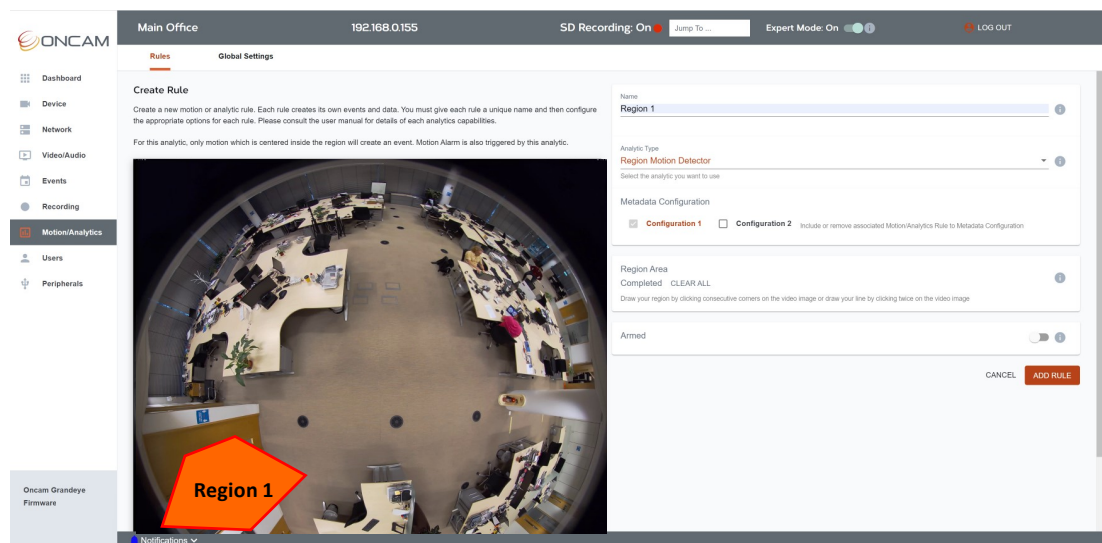


Figure 248 Motion Analytics Draw Region

5.6.1.2.3.2 Arm

Each Motion Region Detector rule can be armed and disarmed via this slider.

5.6.1.2.3.3 Add Rule

Once the rule is created, click **ADD RULE** to apply it.

All rules once created will be listed in the **Motion/Analytics > Rules > table list**.

Currently with Version 2.0.x firmware for Motion regions created, this are not visible on the image Rules overview tab after they have been created.

5.6.1.2.4 Motion Data Only

Motion Data Only is a rule to add raw motion data to a metadata stream. The data includes motion percentage and motion area data and can be read by an integrated VMS/NVR. This data can be for many VMS driven motion analytics tools such as smart region searching and motion percentage representations.

This rule creates the following ONVIF events and metadata:

tns1:VideoAnalytics/ons1:MotionDetection

Sample Data:

```
<tt:Source>
<tt:SimpleItem Name="VideoSourceToken" Value="VideoSource"/>
</tt:Source>
<tt:Data>
<tt:ElementItem Name="MotionMask">
oncam:MotionContent Histogram="0.006622">
<oncam:BoundingBox bottom="0.886702" left="0.589837" right="0.699199" top="0.765621"/>
</oncam:MotionContent>
</tt:ElementItem>
</tt:Data>
```

5.6.1.2.4.1 Add Rule

There are no settings for this rule, once the rule is created, click **ADD RULE** to save it. All rules once created will be listed in the **Motion/Analytics > Rules > table list**.

5.6.1.2.5 Whole Scene Motion Detector

A default whole scene motion detector rule is created as standard on the camera.

This rule creates a **Motion Alarm event** when motion is detected anywhere in the full 360-degree images.

This rule creates the following events and metadata:

tns1:VideoSource/MotionAlarm

Sample Data:

```
<tt:Source>
<tt:SimpleItem Name="Source" Value="VSC"/>
</tt:Source>
<tt:Data>
<tt:SimpleItem Name="State" Value="false"/>
</tt:Data>
```

5.6.1.2.5.1 Add Rule

There are no settings for this rule, once the rule is created, click **ADD RULE** to save it. All rules once created will be listed in the **Motion/Analytics > Rules > table list**.

5.6.1.2.6 Tampering Detection

The camera supports anti-tampering detection, with the ability to notify the user if the camera is tampered with. By default, all tampering rules are applied these can be edited or removed as required.

These following topics can be created for tampering detection:

```
tns1:VideoSource/ImageTooBlurry/AnalyticsService
tns1:VideoSource/ImageTooDark/AnalyticsService
tns1:VideoSource/ImageTooBright/AnalyticsService
tns1:VideoSource/GlobalSceneChange/AnalyticsService
```

Following event/metadata are generated when tampering is detected

```
<tt:Source> <tt:SimpleItem name="Source" value="VSC"/></tt:Source>
<tt:Data> <tt:SimpleItem name="State" value="true"/></tt:Data>
```

5.6.1.2.6.1 Tampering Detection Mode

Select the Tampering detection mode to be used on the camera. Four options are available: Global Scene Change, Too Dark, Too Bright or Too Blurry.

5.6.1.2.6.2 Tampering Minimum Duration time

Select the time in seconds that the tampering must continue for before it is considered as a tampering event and creates an alarm. The Time will only start once the Tampering Detection Threshold has been met.

5.6.1.2.6.3 Tampering Detection Threshold

Set the threshold level of the tampering detection algorithm, that the tampering event must reach before it is considered as tampering. Expressed as a percentage. Correct level setting can help avoid false alarms.

5.6.1.2.7 Loitering Object Detector

This analytic type uses object tracking and reports events when objects remain in the region for a designated time (set by 'Time Threshold'). Each object has a unique number. Periodic events can be sent while the objects remain in the region.

To use this rule the camera must be calibrated for the scene, setting the **Camera Height** correctly and the object size thresholds. Calibration Settings are changed in Camera Web Interface via **Motion/Analytics > Global Settings**.

This rule creates the following events and metadata:

```
tns1:RuleEngine/LoiteringDetector/ObjectIsLoitering
```

Sample Data:

```
<tt:Source>
<tt:SimpleItem Name="VideoSourceConfigurationToken" Value="VideoSource"/>
<tt:SimpleItem Name="VideoAnalyticsConfigurationToken" Value="testToken"/>
<tt:SimpleItem Name="Rule" Value="LoiteringDetector1"/>
</tt:Source>
<tt:Key>
<tt:SimpleItem Name="ObjectId" Value="4"/>
```



```

</tt:Key>
<tt:Data>
<tt:SimpleItem Name="Since" Value="2020-02-27T15:31:41Z"/>
<tt:SimpleItem Name="TimeStamp" Value="2020-02-27T15:31:41Z"/>
</tt:Data>

```

5.6.1.2.7.1 Region Area

To create a region, click **Draw** and then click up to 16 corners of the region on the video image to create your region. When you have clicked your last point, the region will close automatically when you hit **Save Area**.

5.6.1.2.7.2 Time Threshold

Select the time in seconds before an object is loitering. If the object stays inside the region for more than this time the object is considered to be loitering and an event is created.

5.6.1.2.7.3 Periodic Repeat

Turning on Periodic Repeat will send a follow up event if the object is still loitering after a certain number of seconds (Set by 'Repeat Interval'). It will continue to resend until the object is no longer tracked in the zone.

5.6.1.2.7.4 Repeat Interval

Set the Repeat Interval in seconds to control how often the loitering event is sent. When Periodic Repeat is enabled, the camera will send a follow up event if the object is still loitering after a certain number of seconds. It will continue to resend until the object is no longer tracked in the zone.

5.6.1.2.7.5 Add Rule

Once the rule is created, click **ADD RULE** to apply it.
All rules once created will be listed in the **Motion/Analytics > Rules > table list**.

5.6.1.2.8 Line Counting

This analytic type uses object tracking and reports events when objects cross a defined line.

To use this rule the camera must be calibrated for the scene, setting the **Camera Height** correctly and the object size thresholds. Calibration Settings are changed in the Camera Web Interface via **Motion/Analytics > Global Settings**.

This rule created the following Events and metadata:

tns1:RuleEngine/ons1:TripWire/Counter

Sample Data:

```

<tt:Source>
<tt:SimpleItem Name="VideoSourceConfigurationToken" Value="VideoSource"/>
<tt:SimpleItem Name="VideoAnalyticsConfigurationToken" Value="testToken"/>
<tt:SimpleItem Name="Rule" Value="Tripwire1"/>
</tt:Source>
<tt:Data>
<tt:SimpleItem Name="LeftToRight" Value="7"/>
<tt:SimpleItem Name="RightToLeft" Value="1"/>
</tt:Data>

```


5.6.1.2.8.1 Line Count

To create a line, click **draw** and then click twice on the video image to create your line. When you have clicked your second point hit **Save**.

5.6.1.2.8.2 Add Rule

Once the rule is created, click **ADD RULE** to save it.

All rules once created will be listed in the **Motion/Analytics > Rules > table list**.

5.6.1.2.9 Region Object Detector

This analytic type uses object tracking and reports objects which are either inside or outside the region. Each object has a unique number. Motion Alarm is also triggered by this analytic. The rule also creates data for objects both inside and outside the region and highlights them as such. Each object state changes as it enters or leaves the region.

To use this rule the camera must be calibrated for the scene, setting the **Camera Height** correctly and the object size thresholds. Calibration Settings are changed via the Camera Web Interface in **Motion/Analytics > Global Settings**.

This rule creates the following events and metadata:

tns1:RuleEngine/FieldDetector/ObjectsInside

Sample Data:

```
<tt:Source>
<tt:SimpleItem Name="VideoSourceConfigurationToken" Value="VideoSource"/>
<tt:SimpleItem Name="VideoAnalyticsConfigurationToken" Value="testToken"/>
<tt:SimpleItem Name="Rule" Value="FieldDetector1"/>
</tt:Source>
<tt:Key>
<tt:SimpleItem Name="ObjectId" Value="3"/>
</tt:Key>
<tt:Data>
<tt:SimpleItem Name="IsInside" Value="false"/>
</tt:Data>
```

This rule also creates the following events and metadata:

tns1:VideoSource/MotionAlarm

Sample Data:

```
<tt:Source>
<tt:SimpleItem Name="Source" Value="VSC"/>
</tt:Source>
<tt:Data>
<tt:SimpleItem Name="State" Value="false"/>
</tt:Data>
```

5.6.1.2.9.1 Region Area

To create a region, click **Draw** and then click up to 16 corners of the region on the video image to create your region. When you have clicked your last point, the region will close automatically when you hit **Save Area**.

5.6.1.2.9.2 Add Rule

Once the rule is created, click **ADD RULE** to apply it.

All rules once created will be listed in the **Motion/Analytics > Rules > table list**.

5.6.1.2.10 Object Tracking Data Only

Object Tracking Data, the data used for many of the advanced analytics can be sent as raw data in a metadata stream. Enable this rule to create this data.

The data includes identifiers for each object as well as co-ordinate tracking data as the object moves. This can be read by an integrated VMS/NVR. This data can be used by many VMS driven analytics tools such as object path tracking, heat maps, dwell time etc.

To use this rule the camera must be calibrated for the scene, setting the **Camera Height** correctly and the object size thresholds. Calibration Settings are changed via the Camera Web Interface in **Motion/Analytics > Global Settings**.

This rule creates the following ONVIF events and metadata:

tns1:VideoAnalytics/ons1:ObjectTracking

Sample Data:

```
<tt:Source>
<tt:SimpleItem Name="VideoSourceToken" Value="VideoSource"/>
</tt:Source>
<tt:Data>
<tt:ElementItem Name="TrackObjects">
<oncam:TrackObjectsContent Histogram="0.000000">
<oncam:TrackObject ID="124" bottom="0.855451" left="0.539055" right="0.679667"
top="0.714839"/>
</oncam:TrackObjectsContent>
</tt:ElementItem>
</tt:Data>
```

5.6.1.2.10.1 Add Rule

There are no settings for this rule, once the rule is created, click **ADD RULE** to apply it. All rules, once created, will be listed in the **Motion/Analytics > Rules > table list**.

5.6.1.2.11 Region Object Occupancy

This analytic type uses object tracking and counts, and reports live how many objects are inside the region once they are inside for a designated time (set by 'Time Threshold').

To use this rule the camera must be calibrated for the scene, setting the **Camera Height** correctly and the object size thresholds. Calibration Settings are changed via camera Web Interface: **Motion/Analytics > Global Settings**.

This rule creates the following events and metadata:

tns1:RuleEngine/ons1:LiveOccupancy/CountChanged

Sample Data:

```
<tt:Source>
<tt:SimpleItem Name="VideoSourceConfigurationToken" Value="VideoSource"/>
<tt:SimpleItem Name="VideoAnalyticsConfigurationToken" Value="testToken"/>
<tt:SimpleItem Name="Rule" Value="LiveOccupancy1"/>
</tt:Source>
<tt:Data>
```

```

<tt:ElementItem Name="LiveOccupancy">
<oncam:LiveOccupancyContent>
<oncam:LiveOccupancyAlarm id="136" dwelltime="22783" entrytime="2020-02-
27T15:14:30Z"/>
</oncam:LiveOccupancyContent>
</tt:ElementItem>
</tt:Data>

```

5.6.1.2.11.1 Region Area

To create a region, click **Draw** and then click up to 16 corners of the region on the video image to create your region. When you have clicked your last point, the region will close automatically when you hit **Save Area**.

5.6.1.2.11.2 Time Threshold

Select the time in seconds before an object is counted as being in the region. If the object stays inside the region for more than this time the object is added to the occupancy total.

5.6.1.2.11.3 Add Rule

Once the rule is created, click **ADD RULE** to save it.

All rules once created will be listed in the **Motion/Analytics > Rules > table list**.

5.6.1.2.12 Metadata Configuration

There are two metadata configurations created on the camera by default. Each media profile can choose between these two options. This setting adds or removes the data from this created analytic rule from either one or both metadata configurations. This association can also be edited in **Video/Audio > Media Profiles > Metadata**.

5.6.1.3 How to Edit and Delete an Analytic Rule

Analytics rules can be edited or deleted. Some rules have no editable settings so can only be deleted. Choose Edit next to the rule to access the edit screen from the Rule summary table located in **Motion Analytics > Rules**

NAME	TYPE	ACTIONS
Default Whole Scene Motion Detection	Whole Scene Motion Detector	Edit Delete
Image Too Dark	Tampering Detection	Edit Delete
Image Too Bright	Tampering Detection	Edit Delete
Global Scene Change	Tampering Detection	Edit Delete
Image Too Blurry	Tampering Detection	Edit Delete
Region 1	Region Motion Detector	Edit Delete

Figure 249 Motion Analytics Edit Rules

5.6.2 Global Settings

5.6.2.1 Motion and Analytics Global Settings for Rules Overview

This section allows you to configure the advanced analytics engine's global settings. These settings affect the performance of the analytics.

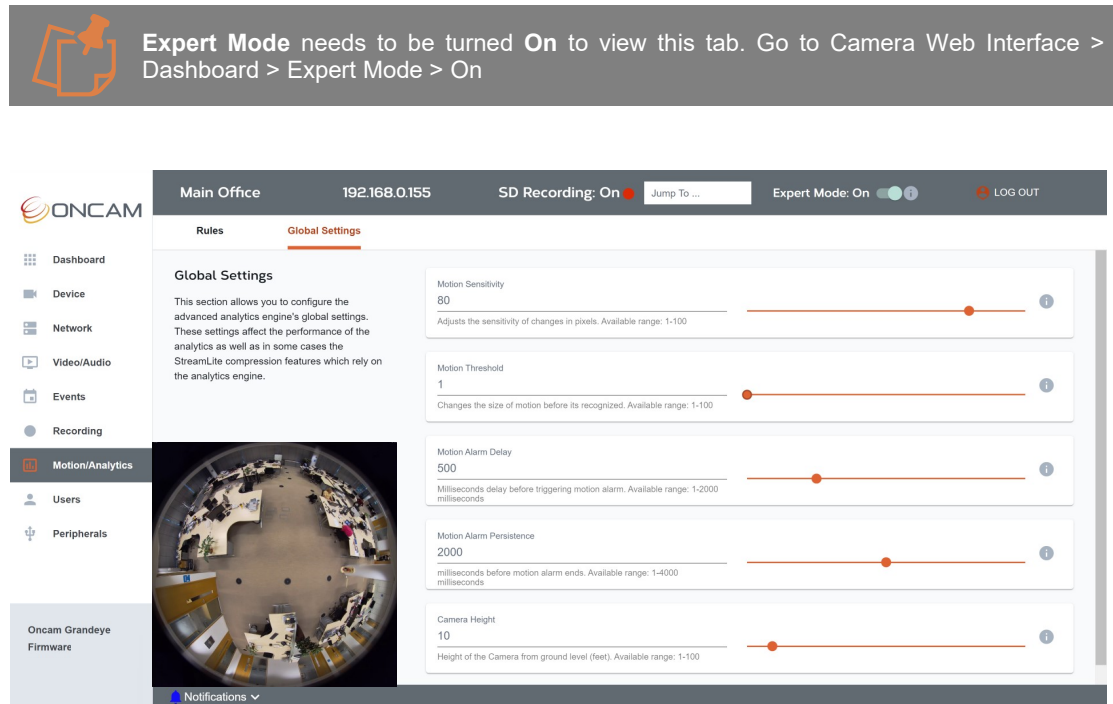


Figure 250 Motion Analytics Global Settings

5.6.2.1.1 Motion Sensitivity

This affects all analytics and motion detection. It is a scale of how sensitive the threshold is on each pixel to determine if it has changed and thus there is motion. Default Settings should work for most scenes.

5.6.2.1.2 Motion Threshold

This affects all analytics and motion detection. It is a scale of how large a group of changing pixels is before it is determined as a motion area for investigation by the analytics engine. Default Settings should work for most scenes.

5.6.2.1.3 Motion Alarm Delay

This setting determines how long motion must be present before a Motion Alarm event is triggered. The camera will wait for this number of milliseconds of consistent motion before triggering an event. This setting only effects Whole Scene Motion Detector, Motion Region Detector and Region Object Detector rules which create motion alarm data.

5.6.2.1.4 Motion Alarm Persistence

This setting determines how long a motion event persists after the motion ends. The camera will wait this number of milliseconds after the end of motion before ending the event. This setting only effects Whole Scene Motion Detector, Motion Region Detector and Region Object Detector rules which create motion alarm data.

5.6.2.1.5 Camera Height

An important setting. Object tracking data is most accurate when the installation height of the camera is set correctly (in feet). This data is used for many of the analytics as well as it being an optional data point for StreamLite compression features.

5.6.2.2 Save Settings

Saving global analytics settings applies the changes immediately but depending on the NVR/VMS using the data, it may be necessary to restart the video stream.

5.6.2.3 Restore Defaults

Select **Restore Defaults** if you want to return to the pre-set defaults of the page.

5.7 Users

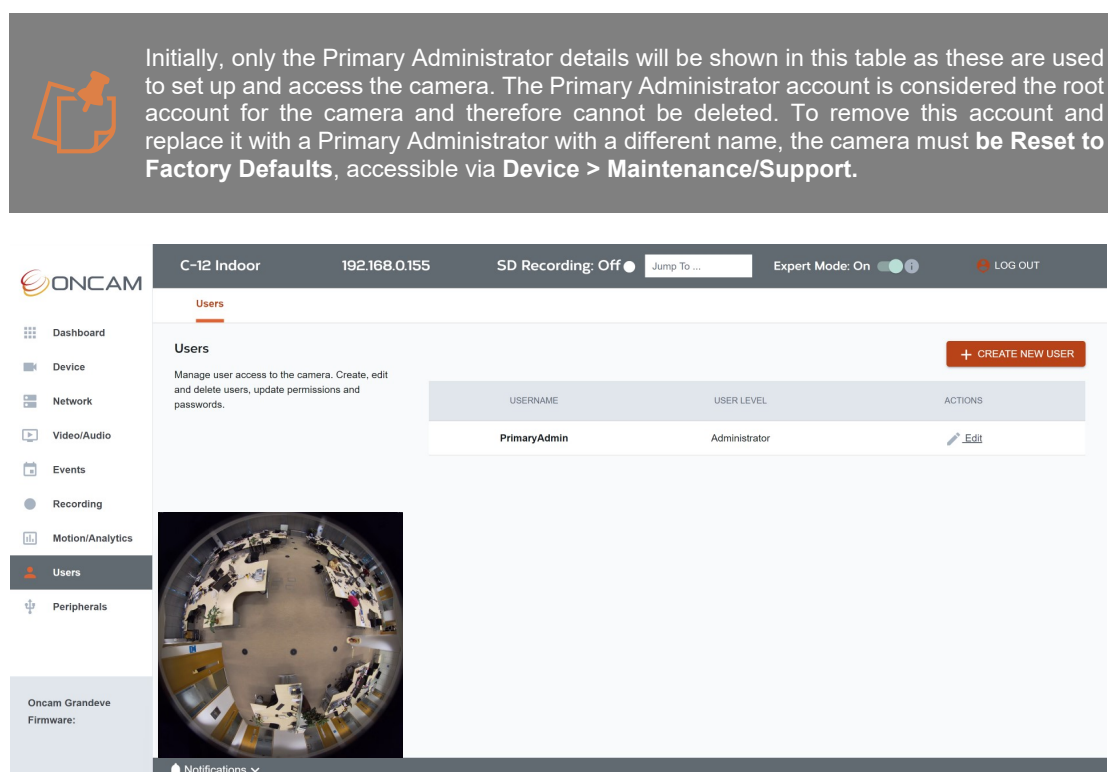
5.7.1 Users Controls

5.7.1.1 User Settings

Control and manage user access to the camera. From the **Users** section you can create new users, edit existing accounts and delete accounts that are no longer required.

A summary table of all active users with their permissions level is displayed in the main page of the User section, accessible from the Camera Web Interface under **Users**.

Initially, only the Primary Administrator details will be shown in this table as these are used to set up and access the camera. The Primary Administrator account is considered the root account for the camera and therefore cannot be deleted. To remove this account and replace it with a Primary Administrator with a different name, the camera must be **Reset to Factory Defaults**, accessible via **Device > Maintenance/Support**.



USERNAME	USER LEVEL	ACTIONS
PrimaryAdmin	Administrator	Edit

Figure 251 Users Overview

5.7.1.2 How to Create a New User

To create a new user account via the Camera Web Interface, go to **Users**, and select the **+ Create New User** button located in the top right-hand corner.



The administrator can create up to 255 user accounts.

The following user settings can be selected and edited.

Figure 252 New User Creation

5.7.1.2.1 Username

Set an easily identifiable and memorable username for the new user. The name must be between 4-12 characters in length. The username can consist of uppercase letters (A-Z), lowercase letters (a-z) and numbers (0-9). Special characters are not supported.



Once created the username cannot be updated, to change it the user would need to be deleted and recreated.


5.7.1.2.2 Password

It is important to always set and use a secure password to access the camera, therefore the camera enforces strong password criteria for all user accounts as specified below:

- Minimum of 8 characters and a maximum of 32.
- The password requires at least one uppercase letter (A-Z), one lowercase letter (a-z), one number (0-9) and one special character. The following special characters are supported (~!@#\$%^&* -+=`|(){}[]:;'.?/).



For enhanced security repetitive or sequential characters (e.g. 'aaa', '123', 'abc' or '321') are no longer supported when creating a new password. V2.0.x firmware or above required to access this feature. For existing installations where repetitive or sequential characters have been setup using Firmware prior to V2.x, these will still be supported, however any new users created will need to follow the new security criteria for password setting.

If you would like to check the Password you have entered and it is safe to do so, select the view icon  and the password will be displayed. Select it again and the password will be hidden.

5.7.1.2.3 Strength Indicator

For guidance, the strength of the password combination is displayed below the password. Use the combination of upper and lower case alphabetic, numeric and special characters until the password strength is strong enough.

5.7.1.2.4 Confirm Password

Please retype your password to confirm it has been correctly entered, if the passwords do not match a notification will appear.

5.7.1.2.5 Access Level

Three camera access levels are supported by the camera: **Administrator**, **Operator** and **User**. This is to provide controlled access to the camera. **Administrators** have full access to all camera features and configuration, whilst **Operator** and **User** have more limited privileges as specified below:

- **Administrators** have unrestricted access to all camera configuration and features and therefore can set/get any operations on the camera.
- **Operators** have limited camera access; they cannot edit the camera configuration or set any values in the camera but can get a SOAP response.
- **User** access level only allows access to live streaming viewing of the camera. Currently with Version 2.0.x firmware for User access level live viewing is not supported in the Camera Web Interface, only a thumbnail is viewable.



It is recommended to set the appropriate access level based on the requirements of each client to protect the integrity of the camera configuration and associated data.



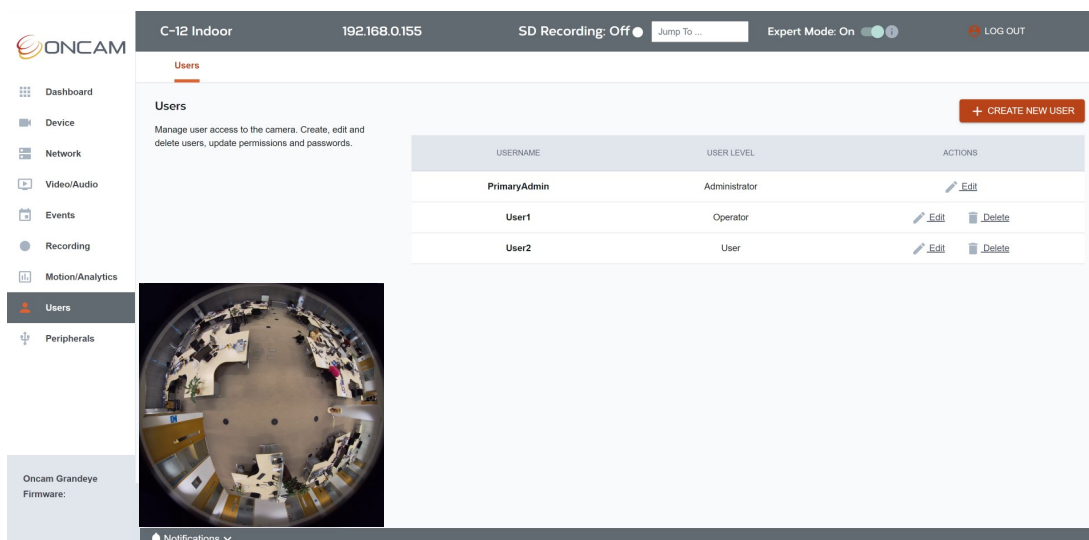
The **Create New User** button will be disabled until all the required fields are completed.

5.7.1.3 How to Edit and Delete a User

Easily manage users by updating user passwords and permission levels or deleting users that no longer require access to the camera.

5.7.1.3.1 How to Edit a User

To edit a user account via the Camera Web Interface, go to **Users**, and select the **Edit** button next to the user account that requires editing




C-12 Indoor 192.168.0.155 SD Recording: Off Jump To ... Expert Mode: On LOG OUT

Users

Manage user access to the camera. Create, edit and delete users, update permissions and passwords.

[+ CREATE NEW USER](#)

USERNAME	USER LEVEL	ACTIONS
PrimaryAdmin	Administrator	Edit
User1	Operator	Edit Delete
User2	User	Edit Delete

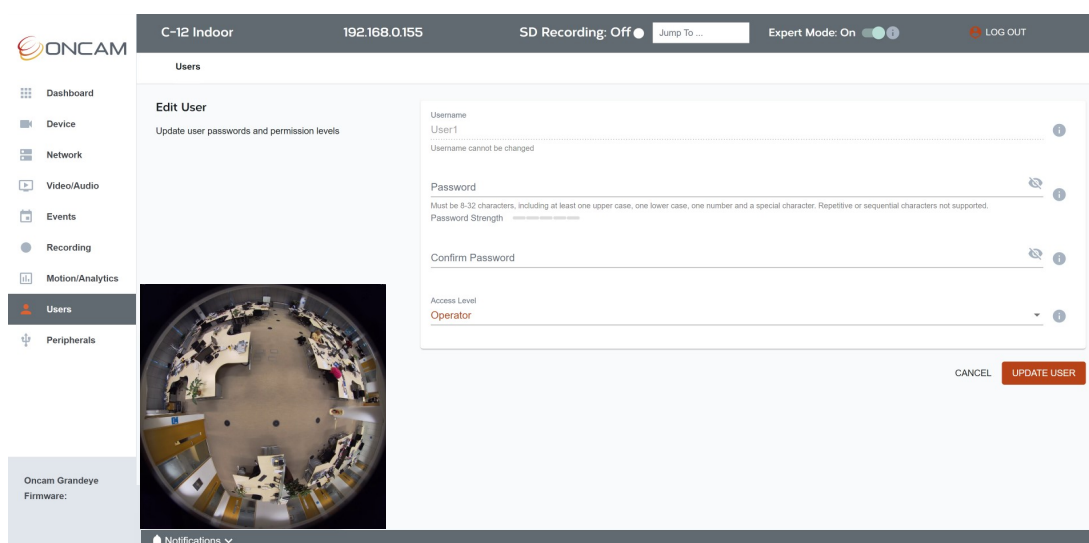
Oncam Grandeye Firmware: 

Notifications

Figure 253 User Summary Table Update



Only password and permission levels can be updated. The username cannot be changed.



C-12 Indoor 192.168.0.155 SD Recording: Off Jump To ... Expert Mode: On LOG OUT

Users


Edit User

Update user passwords and permission levels

Username: User1
Username cannot be changed

Password:
Must be 8-32 characters, including at least one upper case, one lower case, one number and a special character. Repetitive or sequential characters not supported.
Password Strength:
Confirm Password:
Access Level: Operator

[CANCEL](#) [UPDATE USER](#)


Oncam Grandeye Firmware: 

Notifications

Figure 254 User Editing Options

5.7.1.3.2 How to Delete a User

To delete a user account via the Camera Web Interface, go to **Users**, and select the **Delete** button next to the user account that requires deleting. You will need to confirm your selection.



The delete button will not be displayed next to the Primary Administrator account as this account cannot be deleted. To remove this account and replace it with a Primary Administrator with a different name, the camera must be **Reset to Factory**, accessible via **Device > Maintenance/Support**.

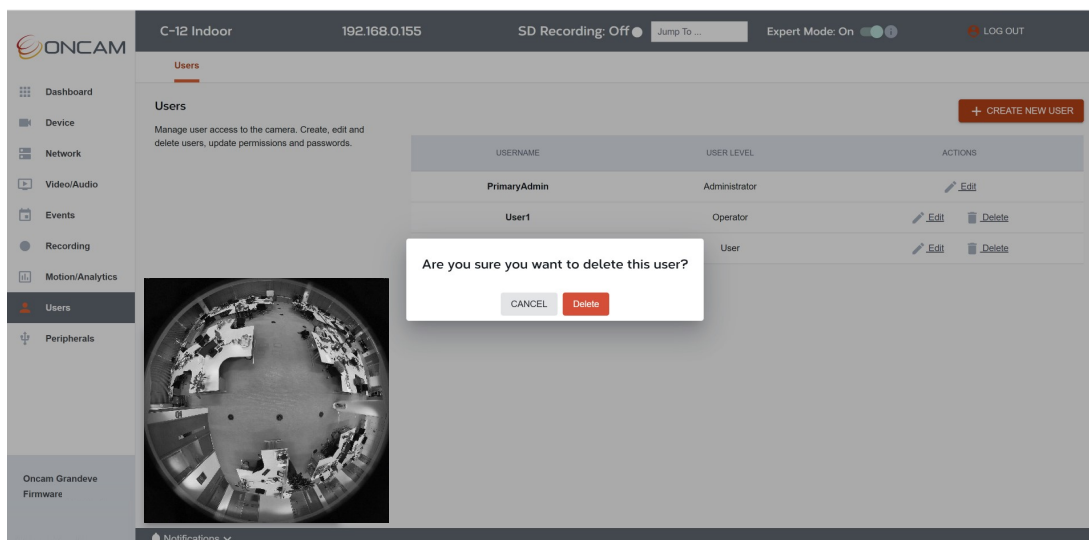


Figure 255 Users, Delete Account Confirmation

5.7.1.3.3 Impact of Resetting the Camera to Factory Defaults on User Accounts

When the camera is **Reset to Factory Settings**, (via the Camera Web Interface accessible via **Device > Maintenance/Support**) all three options will reset all User account details.

5.8 Device

5.8.1 Device Information

5.8.1.1 Available Device Information

All key camera identification information is accessible in this area. This includes the camera name, model number, serial number and the firmware version. The camera model name can also be set here to identify itself as an Oncam Evolution 12 for ease of implementation into existing ONVIF installations.

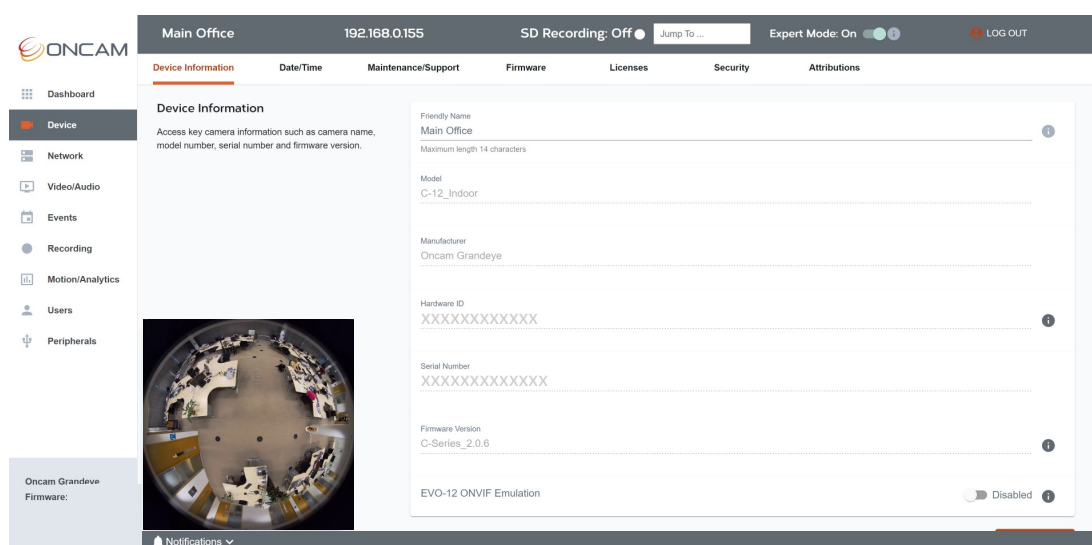


Figure 256 Device Information Overview

The following information is accessible:

5.8.1.1.1 Friendly Name

The friendly name of the camera can be changed to one that is more recognizable. The name can be up to 14 characters in length. Choose one that will help easily identify the camera without the need to reference the MAC ID or Serial number. The friendly name will be displayed in the top left-hand corner of the Camera Web Interface and on the discoverable list in the Camera Configuration Tool. This name is accessible through the ONVIF API via GetScopes and may be displayed in your VMS if supported.

5.8.1.1.2 Model

This is the model name of the camera. It identifies the name and type of camera (Indoor/Outdoor). This is the identification name that will appear in the ONVIF driver of your VMS. The following models' numbers are used:

C-12_Indoor
C-12_Outdoor
C-08_Indoor
C-08_Outdoor



This name is not editable. The Outdoor Model name is derived when the camera module is installed inside the Outdoor camera housing. A physical connection is made between the camera module and the spring on the outdoor housing so that the firmware can determine that the camera is in an outdoor enclosure.

5.8.1.2 Manufacturer

This is the manufacturer name of the camera. This is the name that will appear in the ONVIF driver of your VMS.



This name is not editable.

5.8.1.3 Hardware ID

The Hardware ID is the unique Media Access Control (MAC) ID of the camera, (the colon signs are not displayed). The camera is identifiable on the Local Area Network by this unique ID and an IP address can be automatically or manually allocated based on this ID. This is not editable.

5.8.1.4 Serial Number

The serial number of the camera is a unique identifying numerical sequence that helps identify information related to the production of the camera. This is not editable.

5.8.1.5 Firmware Version

This is the firmware version installed on the camera. Visit <https://www.oncamgrandeye.com> to confirm you have the latest firmware version. If not, the latest Firmware version can be downloaded directly from the website and then uploaded to the camera via the Camera Web Interface, go to **Device > Firmware**, or via the Camera Configuration Tool.



This name is not editable. C-12 camera supports Firmware Version 1.0.2 and above, but some features will not be supported until the later Firmware's are applied.


C-08 camera supports Firmware Version 2.1.5 and above.

Prior to upgrading, check the latest camera firmware available is supported by your NVR/VMS version.

5.8.1.6 EVO-12 ONVIF Emulation

To ensure that C-12 camera can be seamlessly integrated into an existing Oncam Evolution 12 installation, enabling this mode will change the ONVIF Model name of the camera to EVO-12Nx.D. The camera will then be recognized as an Evolution 12 camera and can be configured as required.

This feature is not applicable to the C-08.



HTTP (located in **Device > Security > Client Connectivity**) needs to be enabled to support this feature. It is on by default.

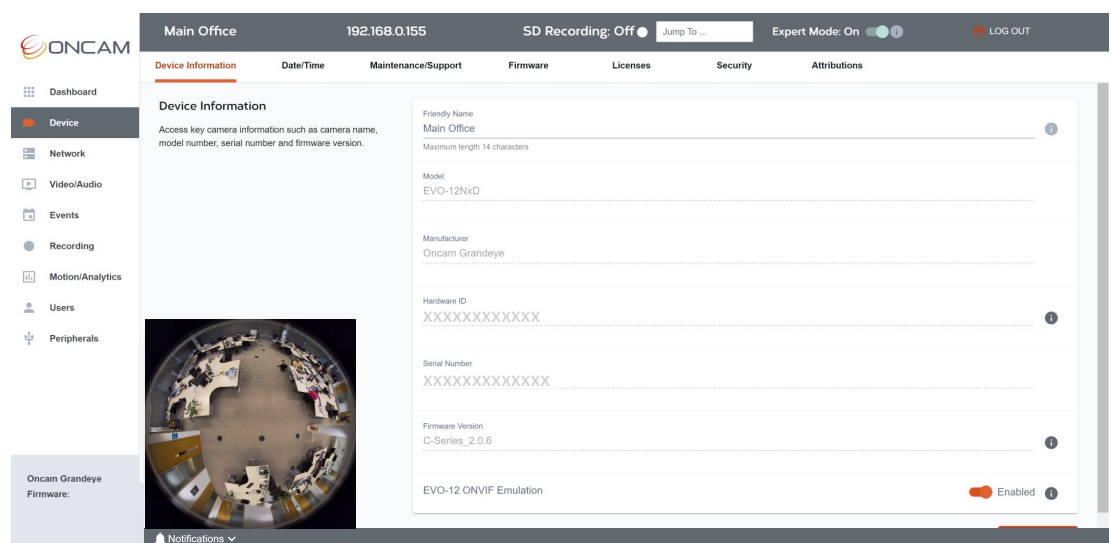



Figure 257 Device Information EVO-12 ONVIF Emulation

5.8.1.6.1 Save Changes

To apply changes made in this section, click the **Save Changes** button in the bottom right-hand corner. A confirmation notification will be briefly displayed in the bottom left-hand corner.



A refresh of the page maybe required to see some of the changes.

5.8.2 Date / Time

5.8.2.1 Setting the Date and Time

For security, streaming video needs to have the correct date and time set, therefore setting the time and date is an important part of the setup process.

Set the date and time on the camera, select from either automatically via NTP or Manually based on synchronizing with the PC time or physically updating these details. Additional areas to consider when setting the time are the appropriate time zone and the use of Daylight savings.

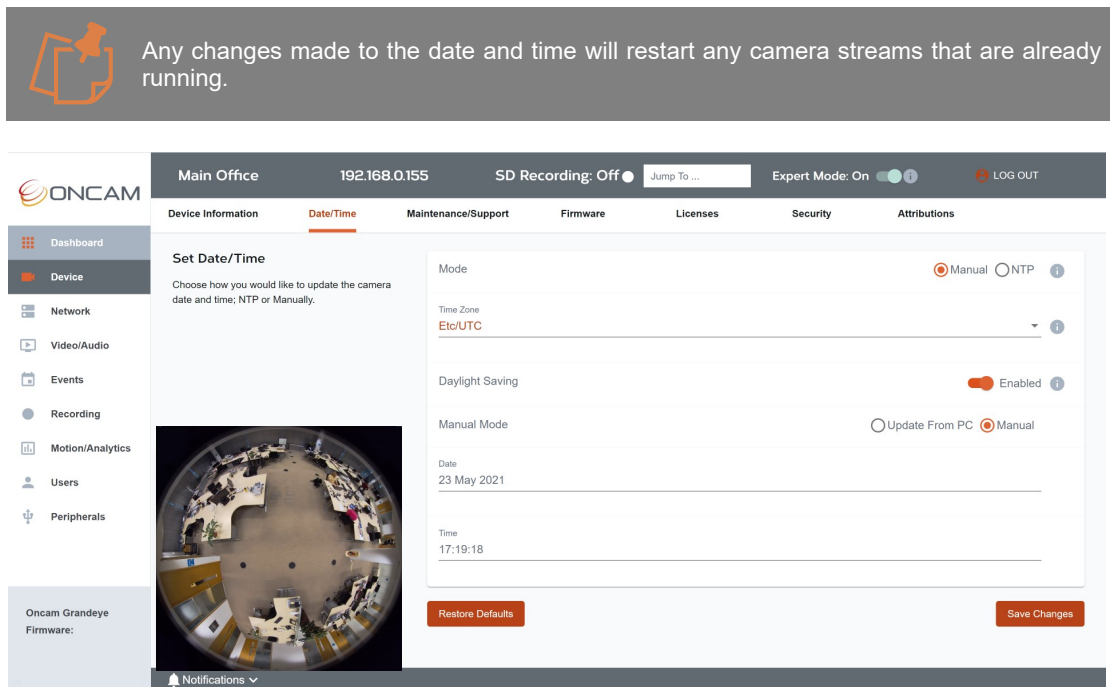


Figure 258 Date / Time Overview

5.8.2.2 Mode

Select from automatic time updates via NTP or set the time manually.

NTP will require an NTP server to be accessible from the camera's network. If this is not possible, the time should be set manually. Default is disabled. NTP will update the camera's clock on reboot and henceforth every 12 hours if the camera time differs by more than 1 minute. Any running camera streams will be restarted to sync the stream to the correct NTP time.

5.8.2.3 Time Zone

Select time zone based on camera location. If the time zone is changed, it will need to be saved and the page refreshed to see the change. If the time zone change impacts a time change, device stream will restart.

5.8.2.4 Daylight Savings

Enable this mode if daylight savings applies in your region. This mode will automatically set the camera time forwards one hour from standard time during the summer months and back again in the fall, to remain in sync with local time.

5.8.2.4.1 How to set Date and Time Manually

When setting the time manually two options will be available under **Manual Mode > Update From PC** or **Manual**.

5.8.2.4.2 Manual Mode

If **Update from PC** is selected, the time, date and time zone will be updated from the client PC once. The Camera's internal Real Time Clock (RTC) is also updated using this time.

If **Manual** is selected, overtype the current displayed time and date with the correct time and date.

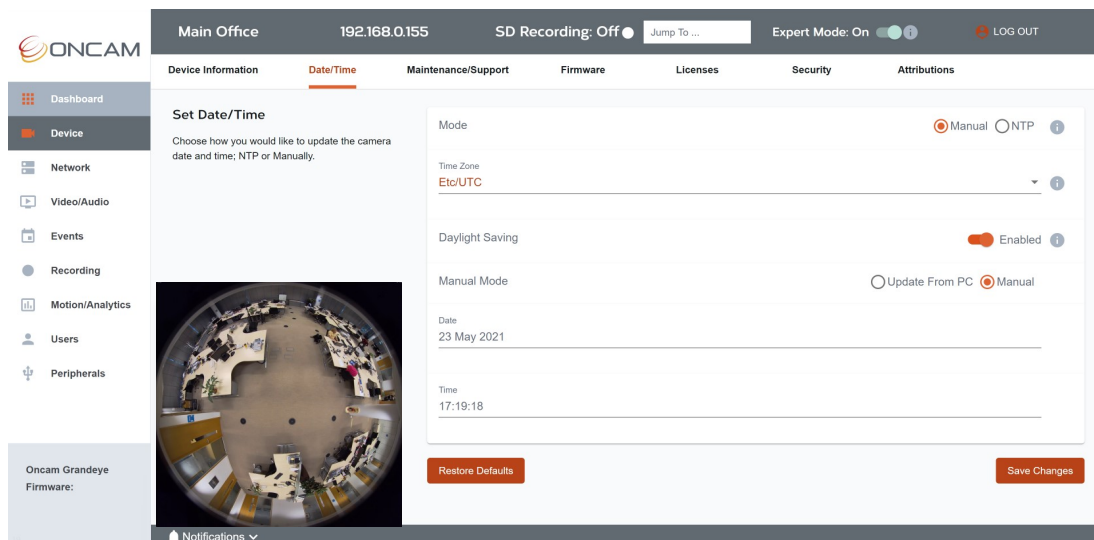


Figure 259 Date / Time Manual Setting

5.8.2.5 Save Changes

To apply changes made in this section, click the **Save Changes** button in the bottom right-hand corner. A confirmation notification will be briefly displayed in the bottom left-hand corner.

5.8.2.6 Restore Defaults

Select **Restore Defaults** if you want to return to the pre-set defaults of the page.



A refresh of the page may be required to see some of the changes.

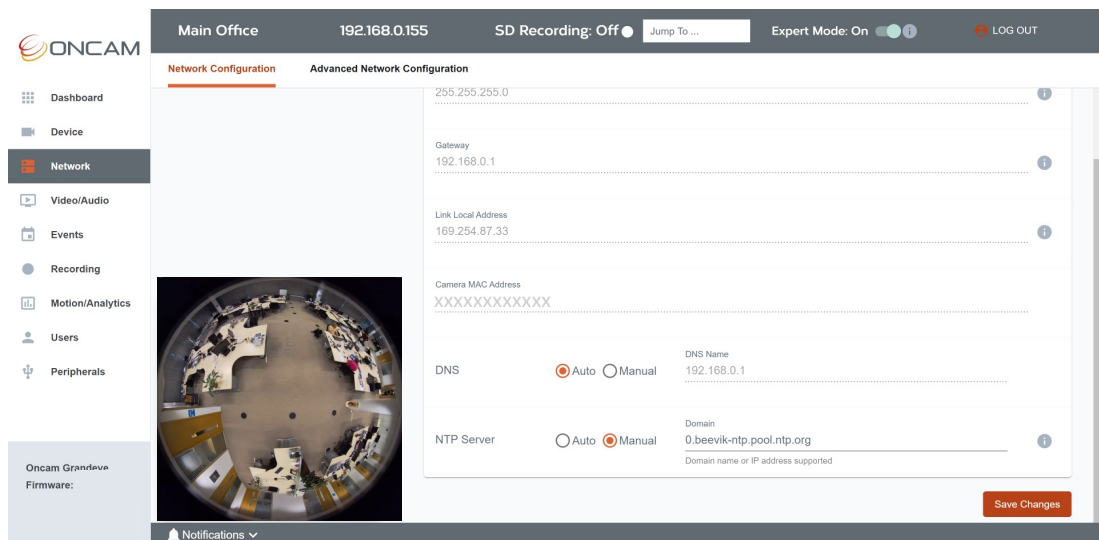
5.8.2.6.1 How to Set the Date and Time using NTP

Network Time Protocol (NTP) is supported to enable automatic synchronization of the camera clock time to the global network time.



Changes to the NTP configuration need to be made in the Network Section. Go to **Network > Network Configuration > NTP Server** or use the link provided.

In this section, the NTP server address can be changed, this has been prepopulated with a Public NTP address. To change it, type your preferred NTP IP address or domain name and save changes.



ONCAM

Main Office 192.168.0.155 SD Recording: Off Jump To ... Expert Mode: On LOG OUT

Network Configuration Advanced Network Configuration

255.255.255.0

Gateway 192.168.0.1

Link Local Address 169.254.87.33

Camera MAC Address XXXXXXXXXXXX

DNS ☒ Auto ☐ Manual DNS Name 192.168.0.1

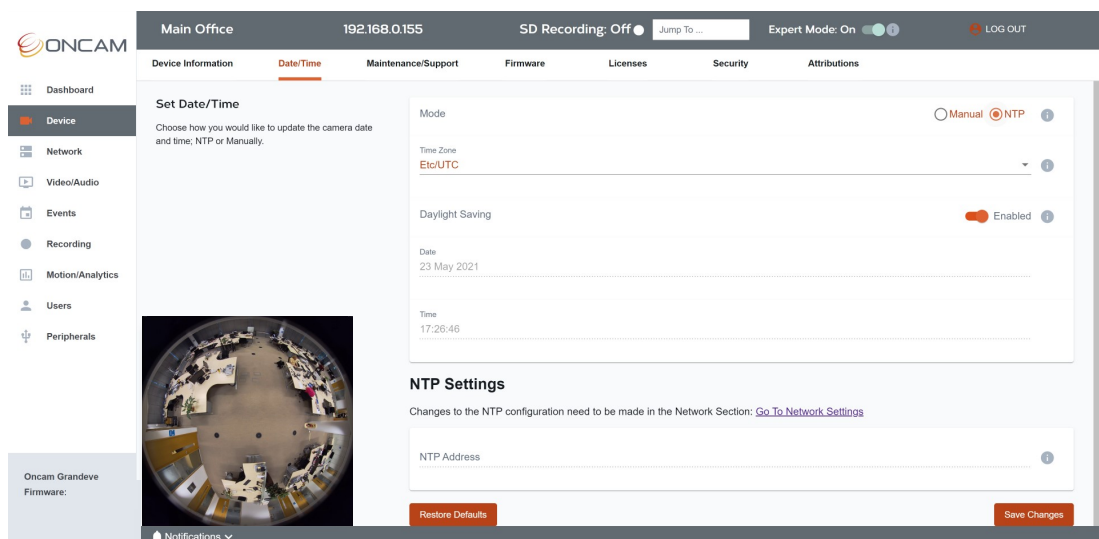
NTP Server ☐ Auto ☒ Manual Domain 0.beevik-ntp.pool.ntp.org

Domain name or IP address supported

Save Changes

Figure 260 Date / Time NTP Network Setting

To fully apply these new NTP settings you will need to return to **Device > Time/Date**, select NTP as your time mode, and scroll to the bottom of the page where the new NTP address is saved and click the **Save Changes** button.



ONCAM

Main Office 192.168.0.155 SD Recording: Off Jump To ... Expert Mode: On LOG OUT

Device Information **Date/Time** Maintenance/Support Firmware Licenses Security Attributions

Set Date/Time

Choose how you would like to update the camera date and time; NTP or Manually.

Mode ☐ Manual ☒ NTP

Time Zone Etc/UTC

Daylight Saving ☒ Enabled

Date 23 May 2021

Time 17:26:46

NTP Settings

Changes to the NTP configuration need to be made in the Network Section: [Go To Network Settings](#)

NTP Address

Restore Defaults Save Changes

Figure 261 Date / Time NTP Save Setting

5.8.2.7 Real Time Clock (RTC)

A battery powered real-time clock (RTC) is integrated into the camera for accurate time management. It keeps count of time and date even when powered down for up to 3 days to accommodate power cuts and network interruptions.

5.8.3 Maintenance / Support

5.8.3.1 Essential Camera Maintenance

If you run into any problems, it is important to get the camera up and running as quickly as possible. Several self-help and escalation tools are available. In this section, you can check in on your camera if something is not working as expected, reboot or reset the camera, download and share support logs and restore from a previously saved backup.

5.8.3.2 Reboot

From time to time the camera may need to be restarted for instance when a significant configuration change is made or when there are changes to external systems affecting the camera. The camera can be rebooted in two ways:

1. Via Software Tool
2. Via Physical Button Press

1. Software tools:

Camera Web Interface: Navigate to; **Device > Maintenance/Support** select **Reboot** and confirm. A countdown will be displayed on screen for 70 seconds while the camera reboots.

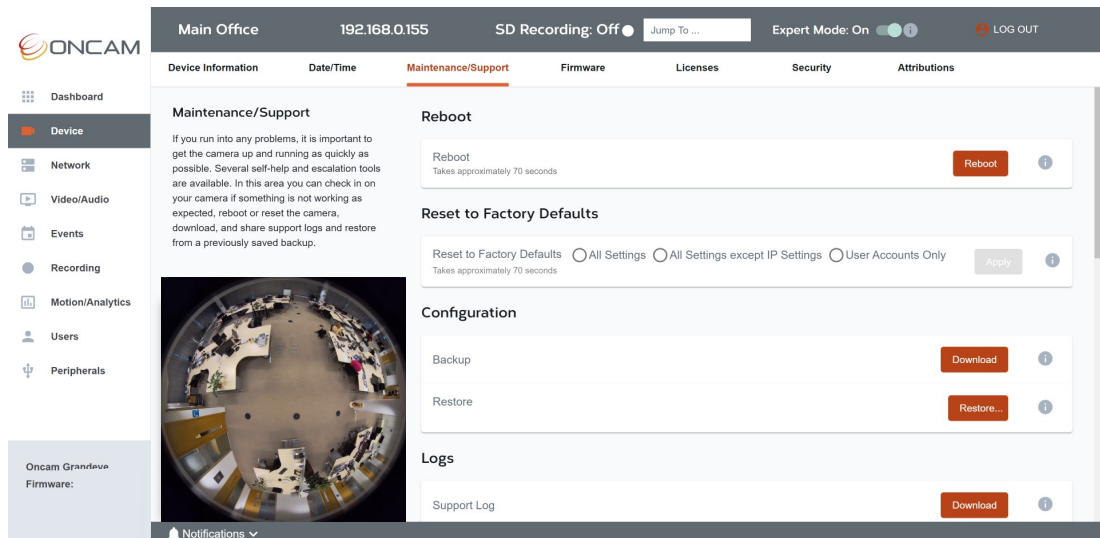
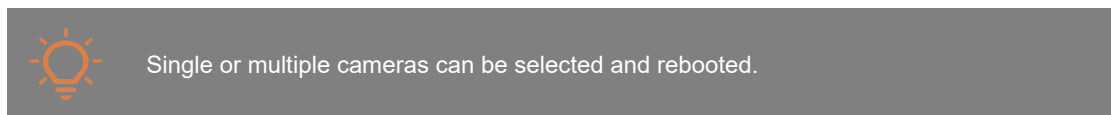


Figure 262 Maintenance Support Reboot

Camera Configuration Tool: Open the tool, **Discover Cameras** and follow the process below:



- Login to the cameras that require rebooting.
- Select the cameras to reboot using the checkbox next to each camera.
- Select the **Reboot** button in the top menu bar.
- The following Reboot Confirmation pop-up will be shown displaying the selected cameras, check all cameras that require a reboot are captured correctly on the list.
- Select the **Tick** icon to apply.

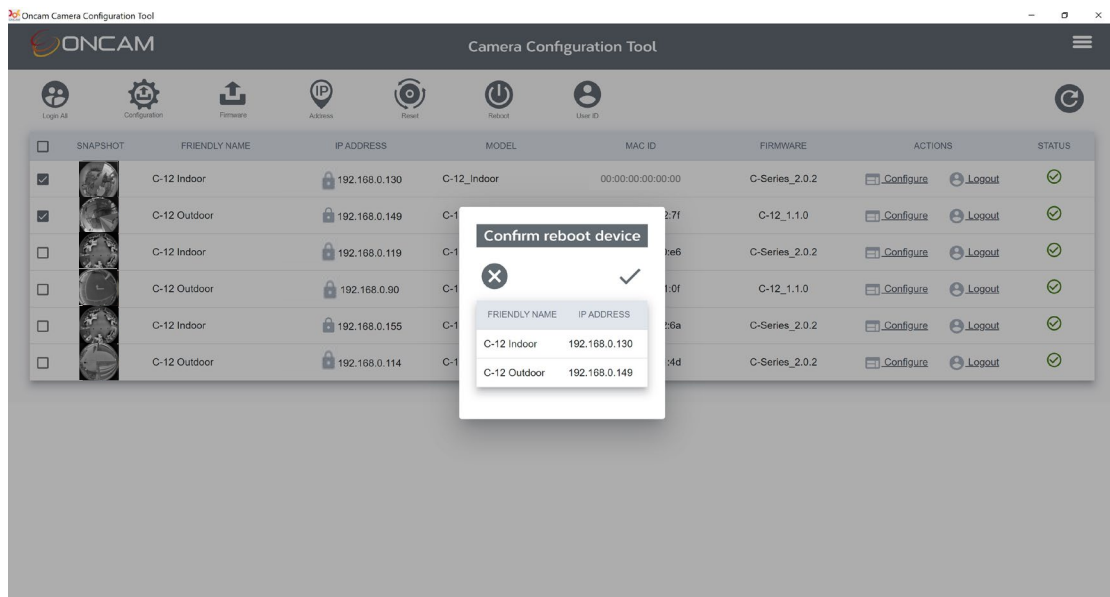


Figure 263 CCT Maintenance Support Reboot

- A warning will be shown to advise that all active streams will be stopped and restarted due to the reboot process. If you would like to proceed, click **Apply**.
- The pop-up will close, and you will return to the CCT dashboard. The cameras will be listed in the Cameras in progress section of the dashboard. Individual progress bars will be displayed on screen while the cameras are rebooted.

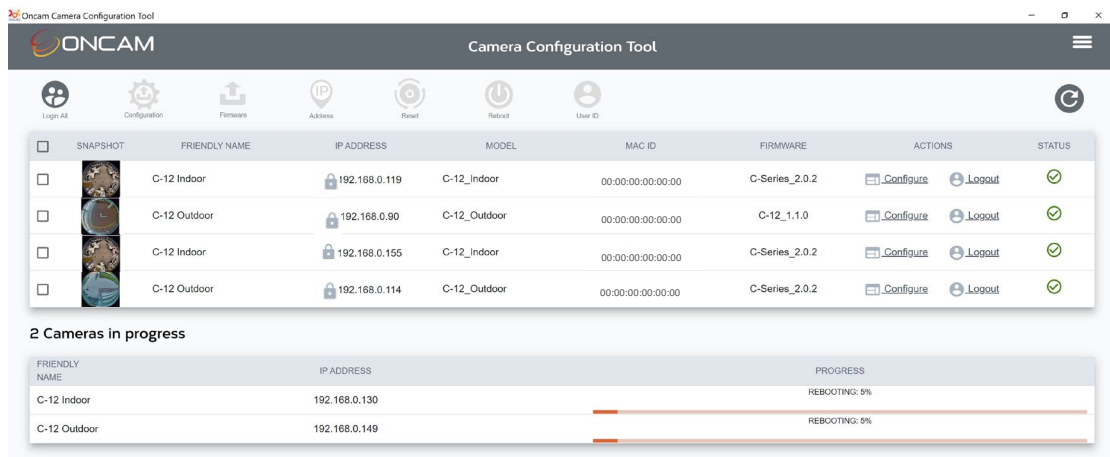


Figure 264 CCT Maintenance Support Reboot Progress Status

- Once rebooted the cameras will be displayed in the discovery list section of the dashboard.

The camera can also be rebooted by an ONVIF compatible VMS interface.

2. Physical Button Press:

Using an appropriate object with a point (e.g. ballpoint pen), with the camera powered, hold down the grey reset button (located on the bottom right hand side) on the front of the camera module for 12 seconds until the Status LED turns off and then let go.



The Status LED will go through the following light sequence, do not let go until the sequence has finished and the LED turns off, otherwise a factory reset may be applied to the camera.

- 0-3 seconds - Flashing Blue - No state change
- 3-6 seconds - Flashing Red - Factory reset except IP settings
- 6 -12 seconds - Solid Red - Factory reset - All settings
- **12 seconds - LED light turns off - Camera rebooted**



Camera stream will be interrupted while the camera reboots.

5.8.3.3 Reset to Factory Defaults

The camera may require a reset to factory defaults if unknown configuration changes have been made and you want to start from a default state.



This option will overwrite existing settings therefore careful consideration is required before applying it.

Three levels of reset to factory defaults are supported:

1. All Settings.
2. All settings except the IP Settings - All settings except essential IP settings - IP Address, subnet mask, Gateway, DNS, NTP, HTTP and HTTPS ports.
3. User accounts only - all other settings will remain.

The camera can be reset to factory defaults in two ways:

1. Via Software Tool
2. Via Physical Button Press

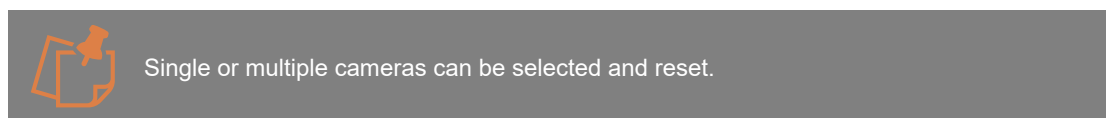
1. Software tools:

Camera Web Interface: Navigate to **Device > Maintenance/Support** select **Reset To Factory Defaults**, choose the preferred reset option and confirm.

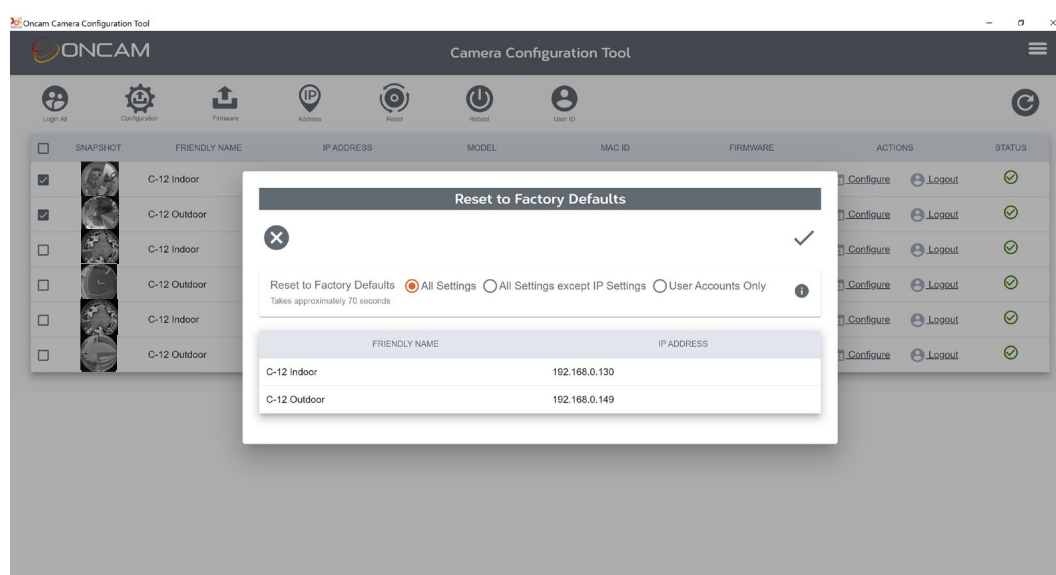
The screenshot displays the Oncam web interface. At the top, there's a header bar with 'Main Office', IP address '192.168.0.155', 'SD Recording: Off', a 'Jump To ...' dropdown, 'Expert Mode: On', and a 'LOG OUT' button. Below the header is a navigation bar with tabs: 'Device Information', 'Date/Time', 'Maintenance/Support' (active), 'Firmware', 'Licenses', 'Security', and 'Attributions'. The left sidebar contains a menu with 'Dashboard', 'Device' (selected), 'Network', 'Video/Audio', 'Events', 'Recording', 'Motion/Analytics', 'Users', and 'Peripherals'. The main content area under 'Maintenance/Support' includes a 'Reboot' section with a 'Reboot' button, a 'Reset to Factory Defaults' section with three radio button options ('All Settings' is selected), and a 'Configuration' section with 'Backup' and 'Restore' buttons. At the bottom, there's a 'Logs' section with a 'Support Log' button. A live camera feed is visible in the bottom left corner of the main content area.

Figure 265 Maintenance Support Reset

Camera Configuration Tool: Open the tool, Discover Cameras and follow the process below:



- Login to the cameras that requires resetting.
- Select the cameras to reset using the checkbox next to each camera (single or multiple cameras can be selected).
- Select the **Reset** button in the top menu bar.
- The following Reset to Factory Defaults pop-up will be shown displaying the selected cameras, check all cameras that require a reset are captured correctly on the list.
- Select the preferred **Reset option**.
- Select the **Tick** icon to apply.
- A warning will be shown to advise that camera settings will be overwritten due to the reset process. If would like to proceed, click **Apply**.

**Figure 266 CCT Maintenance Support Reset**

- The pop-up will close, and you will return to the CCT dashboard. The cameras will be listed in the **Cameras in progress** section of the dashboard. Individual progress bars will be displayed on screen while the reset takes effect.
- As the cameras have been Reset to Factory defaults, the primary administrator username and password will need to be set for the selected cameras, therefore **Set User ID** will be shown in the **ACTIONS** column for the reset cameras.

The camera can also be reset by an ONVIF compatible VMS interface.

2. Physical Button Press:

Using an appropriate object with a point (e.g. ballpoint pen), with the camera powered, hold down the grey reset button (located on the bottom right hand side) on the front of the camera module for a set number of seconds as detailed below depending on the type of reset required.

- 0-3 seconds - Flashing Blue - No state change
- 3-6 seconds - Flashing Red - Factory Reset except IP settings.
- 6 -12 seconds - Solid Red - Factory Reset - All settings.
- 12 seconds - LED light turns off - Camera Rebooted, no settings are changed.



User Accounts Only option reset is not supported by the physical reset button. Holding the button down for 12 seconds or more until the LED turns off will only reboot the camera not reset it. The camera stream will be interrupted while the camera is reset.

After discovering the IP Address of the camera you will need to set the Primary Administrator username and password for first time camera access.



This option will overwrite current cameras settings. If the camera is **Rebooted**, the camera configuration will be saved and unaffected. However, any active recordings will of course be interrupted while the camera reboots. The recording will restart automatically when the camera is back online and streaming.

If the camera is **Reset to Factory Defaults**, recorded files and recording configuration data will not be deleted from the microSD card. The recording configurations will be copied to the camera once the camera restarts, however the recording configurations will be changed to an inactive state and will need to be activated to restart local recording on the microSD card. The previous recorded data is still searchable and can be downloaded. To delete it, the recording configuration needs to be deleted. Go to **Recording > Recording Configuration** and select **Delete** button next to the recording configuration in the summary table.

5.8.3.4 Camera Configuration

All changes made to the camera are stored in a configuration file inside the camera. This configuration can be backed up and saved and then restored in the future if required. This file can also be used to update other compatible Oncam cameras to the same configuration, saving valuable time during installation. A saved configuration file can also make it easier to replicate a precise camera setup as part of the support process.



Create a backup once all camera setting changes have been made.

5.8.3.4.1 Backup

Create a backup and save your current camera configuration settings to your PC, so they can be restored if required in the future. To create a backup file via the Camera Web Interface, go to: **Device > Maintenance/Support > Configuration** and select the **Download** button opposite **Backup**.



Make sure you choose a name that is easily recognizable and references the camera name, F/W version and date. The file will be saved to your downloads folder in an encrypted **.bin** file format. Move it to a safe, easy to find location.

With V1.1.0 F/W if the camera being backed up has a Static IP address this will not be saved in the back up and will default to DHCP to ensure that the camera can be discovered if the backup file is applied.

Note, with V2.0.6 F/W if the camera being backed up has a Static IP address this will be saved in the back up and will be applied other cameras when the restore or apply saved configuration (CCT) features are used.

With V2.1.5 F/W the cameras network settings are no longer saved, therefore when restoring or applying the configuration to other cameras the networks settings of the destination camera will remain unaffected

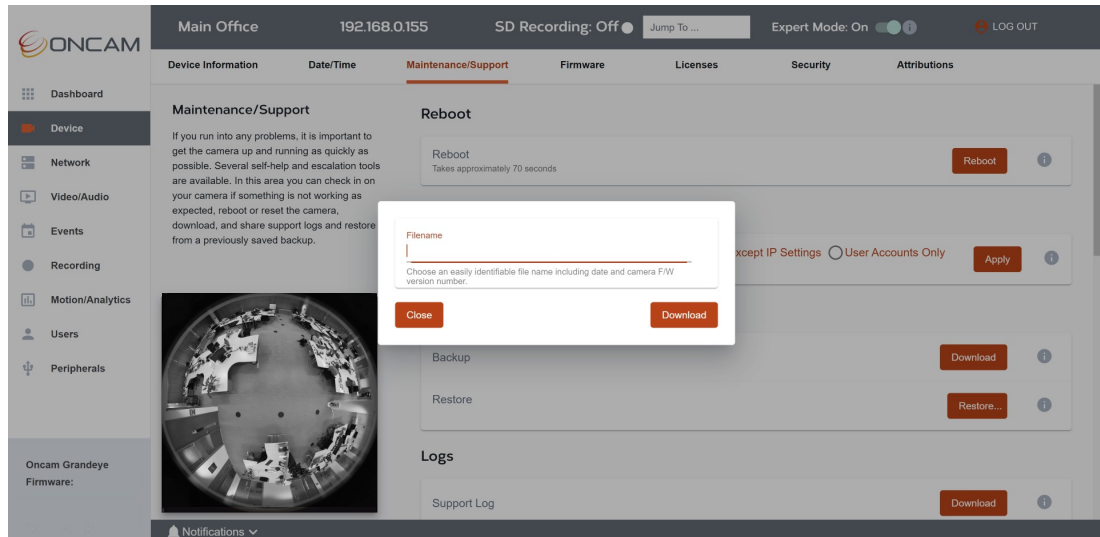


Figure 267 Maintenance and Support Backup

5.8.3.4.2 Restore

Restore your camera configuration settings from a backup stored on your PC. To restore a configuration via the camera interface, go to: **Device > Maintenance/Support > Configuration** and select the **Restore** button. From the file explorer window, navigate to the correct **.bin** file and upload the configuration file. A confirmation message will briefly be shown in the bottom left-hand corner.



Selecting this option will overwrite the current camera settings. Only the same camera type back up file can be restored, for example an Indoor C-12 back up file can only be applied to an Indoor C-12 camera, similarly an Outdoor C-12 back up file is required to restore an Outdoor C-12 camera. The same applies for the C-08.



When a restore is applied to a camera, if the camera has an existing SD card with recordings and recording configurations then these will be overwritten by the backup recording configurations. If the SD card has no recording or configuration the backup recording configurations will be copied to the SD card. Always check the recording configuration settings and status after a backup is applied.

5.8.3.5 Camera Log Information

5.8.3.5.1 Support Logs

The camera gathers essential log information during daily operation that can be helpful in support enquiries. Only information about the internal state of the camera and the configuration is collected in the logs. No sensitive information, such as user credentials is contained in the logs. To download log information collected by the camera, via the camera interface go to: **Device > Maintenance/Support > Logs** and select the **Download** button.



Choose a name that is easily recognizable and that references the camera SN or MAC ID, F/W version and date. The file will be saved to your downloads folder in a secure encrypted **.bin** format.

When requested, share this file with the technical support team who will be able to decrypt it and view the log information.

5.8.3.6 EVO-12 CGI Emulation

5.8.3.6.1 CGI Mode

The camera is ONVIF conformant and works with major NVR/VMS. To extend compatibility into older legacy systems that cannot be upgraded, the camera is also able to emulate the key functions of previous Oncam Evolution cameras. This feature enables a selection of predefined Oncam CGI API commands. For a list of supported commands please contact a member of the Technical Support team. This legacy support can be turned off if necessary.



This feature is enabled by default.



HTTP connection must be left enabled to support this feature, accessible via Camera Web Interface: **Device > Security > Client Connectivity**.

5.8.3.7 Status LED

The Status LED is located on the right-hand side of the camera module. It provides a real time indication of the camera's status.

The table below lists the meaning of the main color states.

Stage	Light Color	Status
Bootup	Blue	Starting OS
	Orange then Yellow	Booting Firmware
	White	Searching for Network
	Green	Connected, Ready
Normal operation	Green	Connected, Ready
	Flashing green	Motion Detected (optional)
	White	Network/Address not found
	Red	SD Card Problem

Table 9 Status LED

5.8.3.7.1 LED Mode

The Status LED can operate in three brightness modes. Set the preferred mode based on your use case. This option is controlled via the Camera Web Interface; **Device > Maintenance/Support > Status LED**.

1. **Always On** - displays the LED at full brightness all the time. The LED brightness level of the Outdoor camera is set lower than the indoor to reduce potential reflections in the dome.
2. **Auto Dimming** - displays the LED at full brightness during the day and automatically reduces it in the evening based in the level of light available, making it less obvious and reducing potential reflections. This is the default mode.
3. **Off** - does not display the LED except during the bootup process.

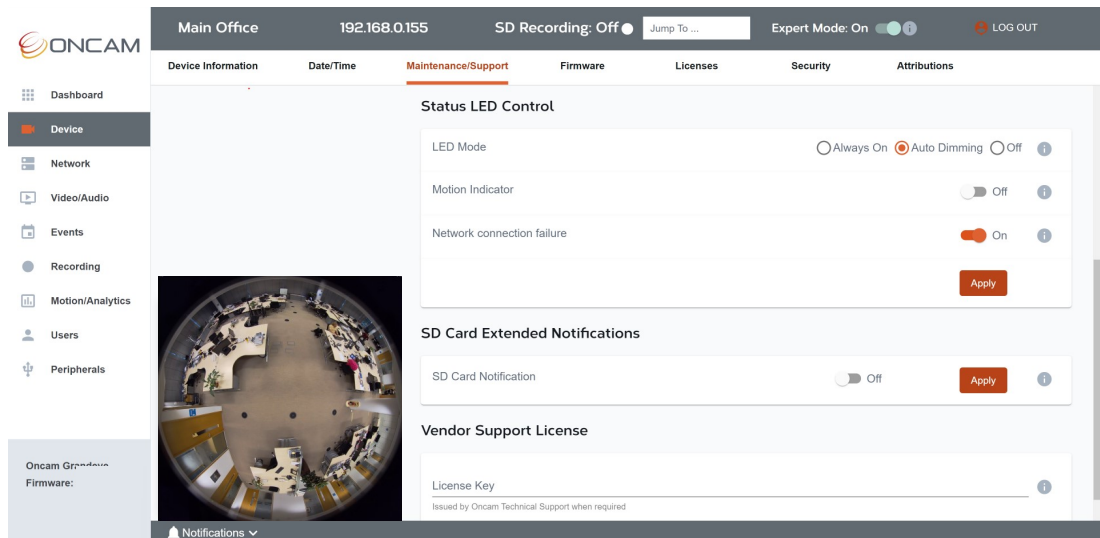


Figure 268 Maintenance Support Status LED

5.8.3.7.2 Motion Indicator

The status LED can be used as a visible indication of triggering of the motion detection system. It will flash green every time the camera detects motion if this option is enabled. This can be particularly useful as visual deterrent. It can also be used as part of the installation process to test that the motion detection regions that have been set up are operating as expected. This option is off by default but can be enabled via the Camera Web Interface; **Device > Maintenance/Support > Status LED**.

5.8.3.7.3 Network connection failure

The status LED can turn white and remain white when the connection to the network is lost or not accessible. This option is on by default but can be disabled from the Camera Web Interface; **Device > Maintenance/Support > Status LED**.

5.8.3.7.3.1 Apply

To apply changes made in this section, click the **Apply** button in the bottom right-hand corner. A confirmation notification will be briefly displayed in the bottom left-hand corner.

5.8.3.8 Vendor Support License

If an advanced level of support information is required, the Oncam Technical Support team will provide a time limited license key that will need to be entered via the Camera Web Interface: **Device > Maintenance/Support > Vendor Support License**. This enables the option to temporarily create more detailed logging information to further assist in the diagnosis of any reported issue. You will be requested to provide specific camera information to generate the unique secure key. Enter the key and select **Apply** to validate the key. Once validated you will be asked to recreate the issue and then download and provide camera logs from: **Device > Maintenance/Support > Logs**.

5.8.4 Firmware

5.8.4.1 How to Check the Camera Firmware Version

To take advantage of the camera's latest product and security features it is important to ensure you have the latest firmware installed. Visit <https://www.oncamgrandeye.com> to check the latest

firmware available for the camera. If a newer version of the firmware is available, check that your NVR/VMS version supports this latest firmware and download the file. The firmware can be updated in two ways:

1. The Camera Web Interface (single camera)
2. The Camera Configuration Tool (single or multiple cameras)

5.8.4.2 How to Update the Camera Firmware

5.8.4.2.1 Select New Firmware

To update the firmware via the Camera Web Interface, go to **Device > Firmware > Update Firmware** and select the **Choose File and Upload** button and follow the process below:

- Navigate to the location where the new firmware file is saved. Select the file and click open to begin the update process.

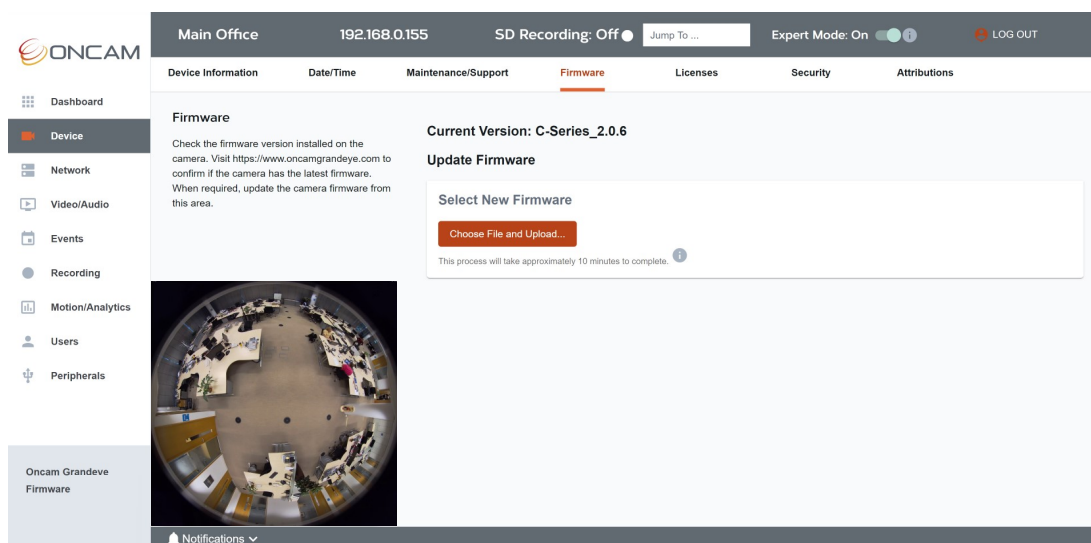


Figure 269 Firmware Update

- The new firmware will be validated, uploaded, and then installed. Once complete the camera will be rebooted.
- Progress bars will be displayed on the screen for each stage. The update process will take approximately 10 minutes depending on network speed and traffic.

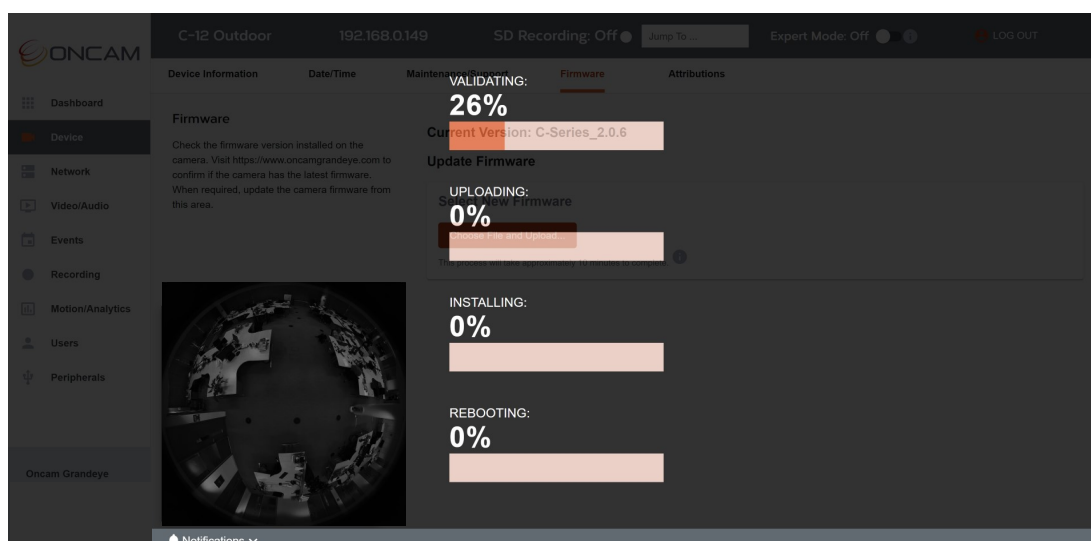


Figure 270 Firmware Update Progress Display

- Once all stages are successfully completed the camera page will be refreshed and you will be asked to log into the camera.
- To confirm the new firmware version has been applied, go to **Device > Device information** and check the firmware version number. It will also be displayed in the grey information box in the bottom left-hand corner of the screen.



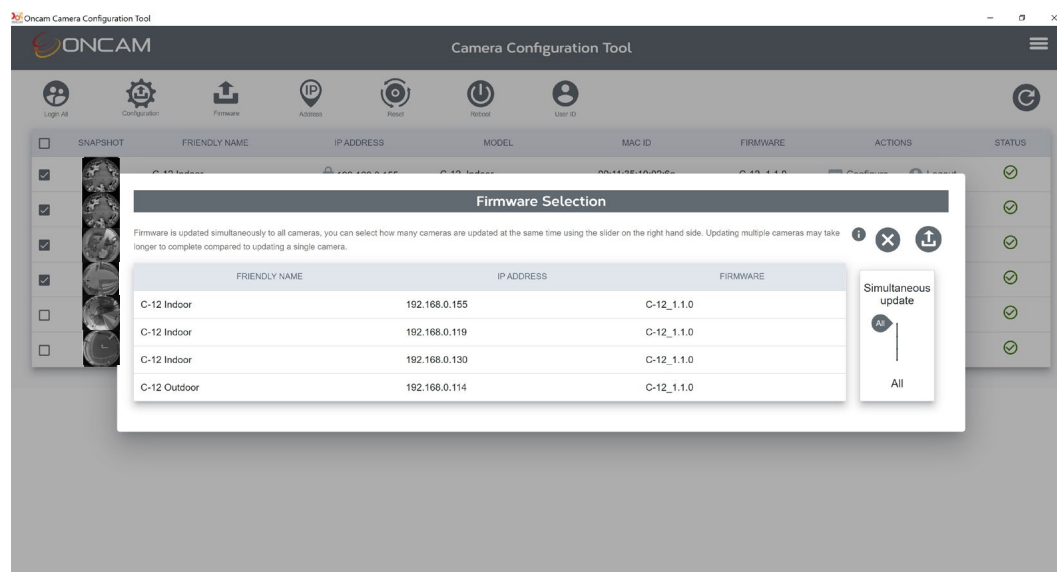
All camera settings will be retained after the firmware update process.

To update the firmware via the Camera Configuration Tool, open the tool, Discover Cameras and follow the process below:



Single or multiple cameras can be selected and updated.

- Login to the cameras that require updating.
- Select the cameras that require updating using the check box (single or multiple cameras can be selected) next to each camera.
- Select the **Firmware** button in the top menu bar.
- The following Firmware Selection pop-up will be shown displaying the selected cameras and their current firmware version, check all cameras that require a firmware update are captured correctly on the list.

**Figure 271 CCT Firmware Update Multiple Cameras**

- Here you can set the number of cameras to be upgraded simultaneously, by default **All** is selected, so in this instance 4 cameras will all be upgraded at the same time. If you only wanted to upgrade 2 cameras at a time (due to network bandwidth limitations for instance), then you can use the slider on the right-hand side to set this to simultaneously update only 2 cameras at a time.
- Select the **Upload** button in the top right-hand corner of the pop-up, it will be highlighted in red when you hover over it.
- Navigate to the location where the new firmware file is saved. Select the file and the update process will begin.

- The firmware will initially be **validated** to check it is suitable and signed by Oncam prior to being uploaded to the cameras.
- Once validated, the pop-up will close, and you will return to the CCT dashboard. The cameras to be updated will be displayed in **Cameras in progress** section of the dashboard. The new firmware will begin to be uploaded to each camera.

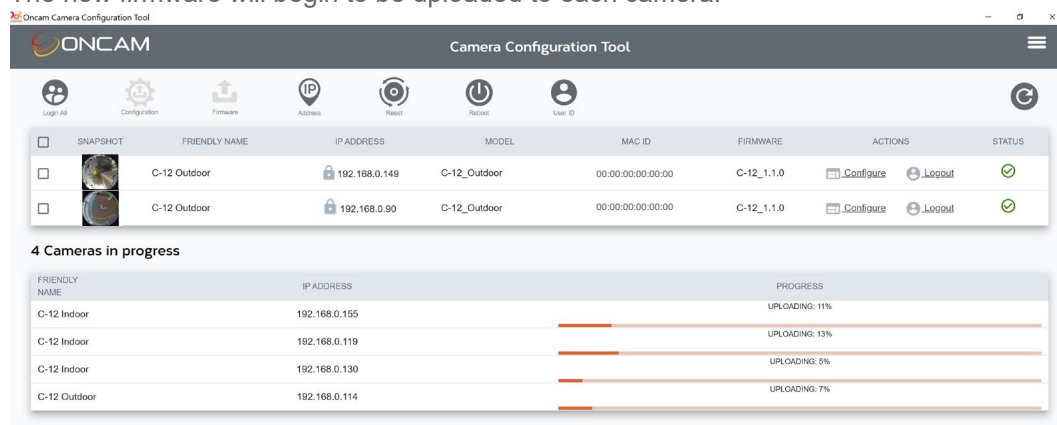




Figure 272 CCT Firmware Update Multiple Cameras Progress bars

- Following the upload stage, the new firmware will be installed on each camera. During each stage, progress bars will be displayed for each camera. Dependent on your network bandwidth cameras may update at different speeds.

 Once a Firmware Update process has started on one or more cameras, another Firmware Update process cannot be initiated from the CCT until the first process has finished.

- Once the installing stage is complete each camera will be rebooted. Please note with version 4.1.4 of the CCT rather than **rebooting** the message displayed onscreen will be **installing** again, this is a known text error that will be fixed in the next version.
- Once the camera has been rebooted it will move to the discovery list section of the Dashboard.
- Once all cameras have been updated, they will be displayed in the discovery section of the dashboard. You may need to click the refresh button if any snapshot images are missing or if the status looks incorrect.
- The upgrade time for each camera will vary based on network speed and traffic.
- To confirm the new firmware version has been applied, check the firmware version number displayed in the discovery table under **Firmware**.

 All camera settings will be retained after the firmware update process.

5.8.4.3 How to downgrade the Camera Firmware

If for any reason you need to downgrade your firmware, you can follow the same process as above using either the CCT or Camera Web interface.

If you downgrade the camera to the same firmware that was previously on the camera the previous camera settings will be applied, any changes that were made after the initial update such as adding / removing / changing user credentials will not be retained and the original credentials reapplied.

If you downgrade to a different version of firmware, then was previously on the camera the camera settings **will not be retained** and the camera will need to be set up again. In very specific and rare scenarios downgrading the firmware to the previous firmware on the camera can result in all configuration settings not being retained.



It is recommended to save/back up your configuration before any update so it can be restored if necessary.

5.8.5 Licenses

5.8.5.1 Camera Licenses

To further increase camera features and functionality, licenses can be added to the camera, for instance for advanced analytic capabilities. To view the status of an existing license or to add a new license via the Camera Web Interface, go to: **Device > Licenses**.



Expert Mode needs to be turned **On** to view this tab. Go to Camera Web Interface > Dashboard > Expert Mode > On

5.8.5.2 How to add an Advanced Analytics license

5.8.5.2.1 License Key

The camera already supports the following analytics:

- Region Motion Detector
- Whole Scene Motion Detector
- Motion Data only

Advanced analytics can be added via a license, in the Camera Web Interface go to **Device > Licenses > Analytics Licenses**.

For More information on Advanced Analytics see: 5.6Motion / Analytics

Please contact your Oncam sales representative for further information and to obtain an advanced analytics license. Once you have been provided with a license key enter it here and validate it to further extend the functionality of the camera. The list of advanced analytics available will be displayed alongside the validity period.

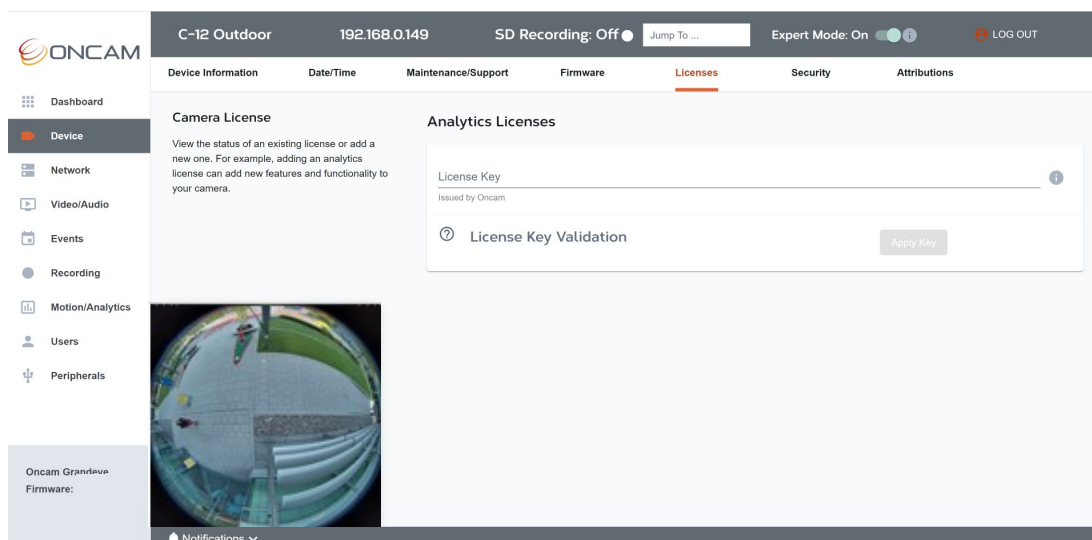


Figure 273 License Overview


5.8.6 Security

5.8.6.1 Camera Security

The camera has several security features enabled by default to ensure it is secure out of the box, while more advanced features such as “IP Address Filtering” are user controlled and offer higher levels of protection against potential attacks.

Please note, the scope of this guide is limited to securing the camera on your network, wider measures need to be put in place to secure your network and environment.

To view the security tab via the Camera Web Interface, go to: **Device > Security**.

 **Expert Mode** needs to be turned **On** to view this tab. Go to Camera Web Interface > Dashboard > Expert Mode > On

5.8.6.2 Secure Configuration

Every effort is made to ensure the product is secure on your network as standard, but we nonetheless recommend enabling and configuring all available security measures. Essentially, these steps involve protecting and controlling access to the camera on the network. We have deployed several measures and features to protect this access as detailed below:

5.8.6.2.1 Secure Bootup

The initial bootup process checks and verifies that the firmware installed on the camera is authorized and signed before proceeding, to ensure only verified firmware is deployed.

5.8.6.2.2 Secure Password

During first time access, default user passwords are not supported, users will be required to set a secure password, which will need to meet a minimum length using a combination of upper- and lower-case letters, numbers and special characters.

5.8.6.2.3 Set Administrator Username and Password

To access the camera for the first time a secure username and password will need to be set for the primary administrator. Default user passwords are not supported, users will be required to

set a secure password, which will need to meet a minimum length using a combination of upper- and lower-case letters, numbers and special characters. This can be set on the Camera Web Interface or the Camera Configuration Tool. (see 4.2 First Time Access - Set Primary Administrator Username and Password).

The camera enforces a strong password as per the minimum criteria outlined:

- Minimum of 8 characters and a maximum of 32.
- The password requires at least one uppercase letter (A-Z), one lowercase letter (a-z), one number (0-9) and one special character (~!@#\$%^&*_-+=`|(){}[]:;'.?/).



For enhanced security repetitive or sequential characters (e.g. 'aaa', '123', 'abc' or '321') are no longer supported when creating a new password. V2.0.x firmware or above required to access this feature. For existing installations where repetitive or sequential characters have been setup using Firmware prior to V2.x, these will still be supported, however any new users created will need to follow the new security criteria for password setting.

For multiple camera installations, the camera can either use the same or different usernames and passwords, for ease of use the Camera Configuration Tool can be used to apply the same credentials to multiple cameras, this makes it easier to manage larger installations but is less secure as if one camera is compromised, effectively all cameras that share those credentials are vulnerable.



The recommendation is to use unique passwords for each camera.

5.8.6.2.4 Secure Authentication

WS-Username Token and HTTP Digest Authentication are supported to ensure clients access the camera over the network with a hashed password, protecting it from network sniffer attacks. We recommend using HTTPS to ensure network traffic is encrypted.

5.8.6.2.5 Brute Force protection

Restrictions are in place as part of the authentication process to slow down the camera's response when multiple incorrect credentials are used to access it to ensure prevention against automated attacks aimed at guessing the password.

Users can also set the maximum number of connection attempts per minute to further restrict access to the camera. To change this via the Camera Web Interface go to **Device > Security > Client Connectivity**.

5.8.6.2.6 User Authorization Levels

Three access levels are supported by the camera, Administrator, Operator and User in an effort to provide controlled access to the camera (see 5.7.1.2.5 User Access Levels). Administrators have full access to all camera features and configuration, whilst Operator and User have very limited viewing privileges only.



It is recommended to set the appropriate access level based on the requirements of each client to protect the integrity of the camera configuration and associated data.

5.8.6.2.7 Secured Firmware

All firmware is digitally signed and authorized by Oncam. During the firmware update process, the camera will check for a digital signature on the firmware and only proceed if it is verified. This prevents tampered firmware that could compromise your camera, from being installed.

To ensure the camera supports the most up-to-date security features and security patches for known vulnerabilities it is important to check that you have the latest firmware installed.

Visit <https://www.oncamgrandeye.com> to check the latest firmware available for the camera. If a newer version of the firmware is available, check that your NVR/VMS version supports this latest firmware.

The firmware can be updated via the Camera Web Interface or the Camera Configuration Tool. (see 5.8.4.2 *How to update the camera firmware*).

5.8.6.2.8 Support Logs – Default

The camera collects important log information during daily operation. These can be particularly useful to help diagnose problems reported by the camera. As the information is sensitive it is encrypted. The downloaded log file can only be viewed by our support team. To download the support log via the camera interface, go to **Device > Maintenance/Support > Logs** and select the **Download** button.

5.8.6.2.9 Access Logs

Details of the last client to access the camera are available including username, date, time and access level. To review the last user to access the camera go to **Device > Security > Logs**.

The following advanced access features can be applied by the user for additional security:

5.8.6.2.10 Communication Protocol

HTTP and HTTPS are both enabled by default. HTTP can be turned off to ensure a secure connection between camera and the client over HTTPS. HTTPS uses TLS, which ensures communication to the camera is encrypted and protected.

5.8.6.2.11 Secure Certificates

When using HTTPS, we also recommend downloading the Oncam Certificate into your client workstation to ensure communication remains secure from end to end.

HTTPS is recommended as the securest way to access the camera as it encrypts traffic between the client and the camera. The camera is HTTPS enabled with a certificate signed by our own Root Certificate Authority (CA); the browser or VMS may warn that the certificate is untrusted, to resolve this download the **Root CA** from the Camera Web Interface and install it as a Trusted Certificate Authority on the PC and VMS.



Once installed, this Root CA will allow you connect securely to all C-Series cameras.

To download the Root CA, go to: **Device > Security > Client Connectivity > Connection** and click on **Download CA Certificate** and then follow the steps below to update your browser:

- 1 Download Root CA From camera web interface
- 2 Accept the download warning by selecting **Keep**. The file will be downloaded.
- 3 Double click on the downloaded.crt file. Accept the security warning by selecting **Open**
- 4 A popup window is displayed with the Certificate Information, select **Install certificate...**, another Pop up window will be shown.

Figure 274 Download Root CA

- 5 Certificate Import wizard will be displayed, select **Current User** and click **Next**
- 6 From the Certificate store presented, select **Place all certificates in the following store** and click **browse**
- 7 Select **Trusted Root Certificate Authorities**, click **OK** and then **Next**
- 8 Check and confirm your settings. Select **Finish**. Click **Yes** if a security warning message is displayed. A confirmation of the successfully imported certificate will be displayed

Figure 275 Install Root CA Certificate

You can now connect to the camera over HTTPS without security warning.

Follow the process defined in your VMS to upload the Root CA to your VMS if required.

HTTPS enables RTP, WebRTC video and all data to be encrypted.



HTTP is enabled by default as it is required by some discovery tools, for secure access it is recommended to turn off HTTP and communicate to the camera over HTTPS only.

To turn off HTTP via the Camera Web Interface go to **Device > Security > Client Connectivity > Connection**.

5.8.6.2.12 IP Address Restrictions

Control which clients have access to the camera by allowing or blocking access to specified IP addresses.

- Set a Blacklist to block access to added IP addresses.
- Set a Whitelist to allow access only to added IP addresses.

To set IP address filtering via the Camera Web Interface go to: **Device > Security > IP Filter Type** and choose between Whitelist and Blacklist. IP addresses can be added individually.



Only one type of list can be in effect at any one time.

5.8.6.2.13 Closed and Controlled Intranet

To minimize the risk of external attack it is strongly recommended to place the camera and associated VMS on a closed controlled intranet.

5.8.6.2.14 Factory Default State

The camera is shipped from the factory in a default state. This is the state where the camera has presets defined by the manufacturer, but no user set configuration. If you are unclear if the camera is in this state, reset the camera to **Factory Default – All Settings** via the Camera Web Interface or Camera Configuration Tool (see 5.8.3.3 Reset to Factory Defaults) before making a change to the settings.

5.8.6.2.15 Date / Time

For security, streaming video needs to have the correct date and time set, therefore setting the date and time is an important part of the setup process. The date and time can be synchronized to a public NTP as long as your camera can reach default NTP and DNS configuration set on the camera. The default NTP server can be changed via NTP settings in the Network section. The date and time can also be set manually. To set the date and time (see 5.8.2.1 **Setting the Date and Time**).

5.9 Peripherals

5.9.1 Input / Output

5.9.1.1 Input / Output Device Support

A Plus version of the camera is required to support Input / Output devices.

The camera's various inputs and outputs are listed in the table on the **IO** Section of the **Peripherals** menu. Only detected inputs and outputs are listed, so what you see in the list will depend on which camera model it is, and what modules are connected at the time.

If you have a C-Series Outdoor Plus camera, and you plug a PoE cable into the camera module while it's removed from the outdoor housing, no IOs will be detected. Bear this in mind if you're going to configure a camera network on the bench before shipping to site, because modules

that are fitted to Outdoor housings at site may need additional settings once installed. If you fit a camera module to an Outdoor Housing to configure it and then remove it, any settings you've made will reappear when the camera is next fitted to an Outdoor Housing.



Give each camera a distinctive name in the **Device > Device Information > Friendly Name** setting so you know which ones are configured for an Outdoor Housing.

5.9.1.2 How to Edit Input / Output device

The table provides a summary of each of the camera's IO connections.

NAME	TYPE	STATE	IDLE STATE	MODE	ACTIONS
HW1	Input	Inactive	Closed		Edit
HW2	Input	Inactive	Closed		Edit
alarm_out_ctrl	Output	Active	Closed	Latching	Edit
led1_ctrl	Output	Inactive	Open	Momentary	Edit
led2_ctrl	Output	Inactive	Open	Momentary	Edit

Figure 276 Peripheral Input / Output Overview

Name - A unique name used for each IO connection in the camera software. The same name is used by the ONVIF-conformant camera API. The name can't be changed.

Type - Describes whether the connection is an Input or an Output. The type is fixed by the camera hardware and can't be changed.

State - Indicates the state of the IO connection the last time the page was updated. To update at will, switch to another menu (such as "Users") for a moment.

Idle State - The electrical state of the Input or Output circuit that should be defined as inactive. The opposite state is therefore defined as active.

Mode - For Outputs only. Defines whether the Output should be Latching or Momentary type.

Click **Edit** next to one of the list items to edit its properties with reference to the details below:

5.9.1.3 Input Devices

There are two alarm input connections on the Plus Module of the C-Series Outdoor Plus camera, labelled "ALM IN 1" and "ALM IN 2". In the camera software and the ONVIF-conformant camera API, they are named as follows:

Plus Module Input Name	Camera Software ONVIF InputToken Name	Input Type & Spec
---------------------------	--	-------------------

ALM IN 1	HW 1	Pull-up: 10 k Ω , 3.3V Max input range: -0.6 V – 40 V Voltage Thresholds: High: >1.9 V Low: <0.4 V
ALM IN 2	HW 2	

Table 10 Plus Module Alarm Input

If you want to assign these inputs to trigger a rule in the camera's internal **Events** system, simply choose the Trigger called **Device/Trigger > Digital Input** and activating either one of these inputs will trigger the rule. For the trigger to be cleared, both inputs must be inactive.

5.9.1.3.1 ALM IN 1 / HW1

The state of the **HW1** input is sent to any connected (known as "subscribing") ONVIF-conformant systems whenever its value changes.

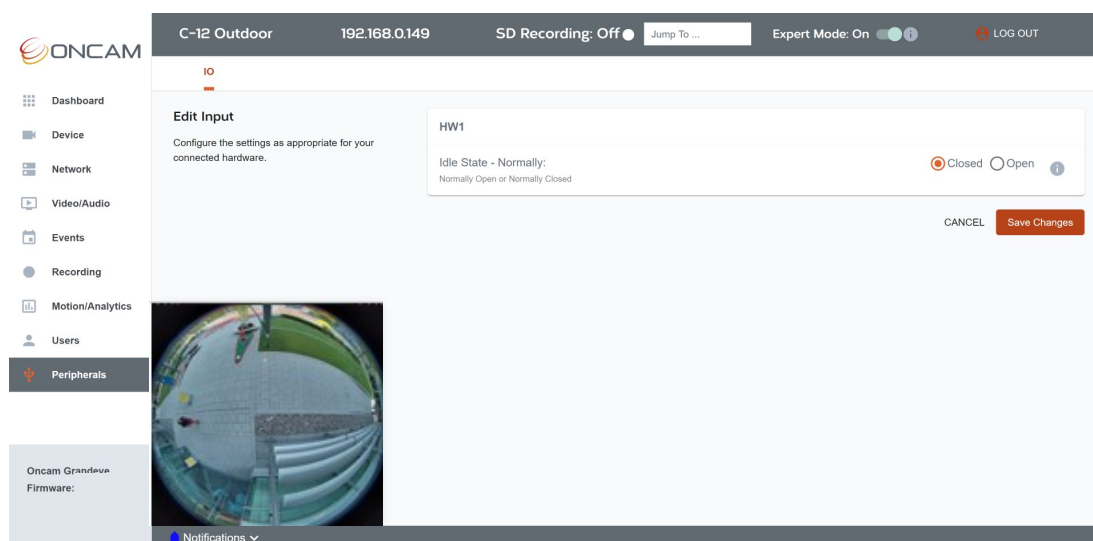


Figure 277 Peripheral Edit Input

5.9.1.3.1.1 Idle State

The Idle State can be defined as Open or Closed (equivalent to normally-open (NO) or normally-closed (NC) on alarm systems).

If Idle State is set to Open, the HW1 input will be **Inactive** when the input is open-circuit, and **Active** when connected to DC GND.

If Idle State is set to Closed, the HW1 input will be **Inactive** when the input is closed-circuit (connected to DC GND), and **Active** when open-circuit.

Choose the setting that corresponds to the behavior of the connected equipment.

5.9.1.3.2 ALM IN 2 / HW2

HW2 works just like HW1, except for the different name of the ONVIF Token and the signal in the camera software.

5.9.1.3.2.1 Idle State

Like **HW1**, the state of the **HW2** input is sent to any connected (known as "subscribing") ONVIF-conformant systems whenever its value changes.

HW2's Idle State can be independently defined as Open or Closed (equivalent to normally-open (NO) or normally-closed (NC) on alarm systems).

If Idle State is set to Open, the HW2 input will be **Inactive** when the input is open-circuit, and **Active** when connected to DC GND.

If Idle State is set to Closed, the HW2 input will be **Inactive** when the input is closed-circuit (connected to DC GND), and **Active** when open-circuit.

Choose the setting that corresponds to the behavior of the connected equipment.

5.9.1.4 Output Devices

There are three digital output connections on the Plus Module of the C-Series Outdoor Plus camera, labelled **ALM OUT**, **LED 1** and **LED 2**. In the camera software and the ONVIF-conformant camera API, they are named similarly as follows:

Plus Module Output Name	Camera Software ONVIF RelayToken Name	Output Type
ALM OUT	alarm_out_ctrl	Open-Drain pull-down to DC GND Max current sink: 2A Max voltage range: -1 V – 40 V
LED 1	led1_ctrl	Positive 3.3V logic outputs Voltage Thresholds: High: >2.5 V Low: <0.04 V Max output current: High: 10 mA Low: -20 µA
LED 2	led2_ctrl	

Table 11 Plus Module Alarm Output

5.9.1.4.1 ALM OUT / alarm_out_ctrl

If you want to assign the ALM OUT output as a rule action in the camera's internal Events system, simply choose the Action Type **oncam:HardwareOutput** in the Create New Rule page and select alarm_out_ctrl as the Output. Go to **Events > Alarm Rules** and click **Create New Rule** to begin.

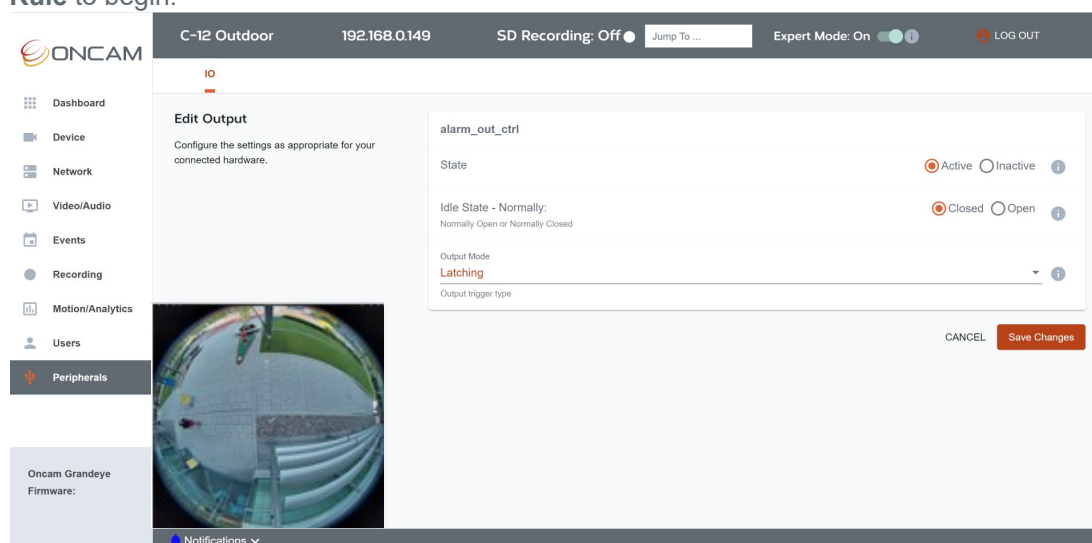


Figure 278 Peripheral Edit Alarm Output

5.9.1.4.1.1 State

The State control allows you to switch the output manually to the Active or Inactive state for testing, or to reset or trigger an alarm, when the Output Mode is set to Latching (see section 5.9.1.4.2.3).

If the Output Mode is set to Momentary (see section 5.9.1.4.2.3) , saving the changes with the State set to Active will immediately trigger the output for the period set in the Pulse/Delay. If you don't want to trigger the output when you save the settings, change it to Inactive. Setting the State to Inactive does not stop the output from operating if activated by an Event rule.

5.9.1.4.1.2 Idle State

The Idle State can be defined as Open or Closed (equivalent to normally-open (NO) or normally-closed (NC) on alarm systems).

If Idle State is set to Open, the ALM OUT output will be open-circuit when alarm_out_ctrl is **Inactive** and connected to DC GND when **Active**.

If Idle State is set to Closed, the ALM OUT output will be closed-circuit (connected to DC GND) when alarm_out_ctrl is **Inactive**, and open-circuit when **Active**.

Choose the setting that corresponds to the behavior of the connected equipment.

5.9.1.4.1.3 Output Mode

The Output Mode has two options:

Latching allows the output to stay in the last state it was switched to until caused to change again. This is useful when one event should cause the output to change, and another should cause it to switch back again.

Momentary allows the output to stay in a default state until triggered to change and then, once triggered, change for a selected period of time and then return to the default state. This is useful when an event should trigger an external device to do something for a period of time, such as sound an alarm, operate a door, etc.

5.9.1.4.1.4 Pulse Delay

When Output Mode is set to Momentary, use the Pulse Delay to control how long the output remains active when triggered. For example, if the output is wired to sound an alarm while active, this would set the duration of the alarm.

5.9.1.4.2 LED 1 / led1_ctrl

The output labelled LED 1 on the Plus Module is controlled by the signal called **led1_ctrl** in the camera's software and ONVIF-conformant API.

If you want to assign the LED 1 output as a rule action in the camera's internal Events system, simply choose the Action Type **oncam:HardwareOutput** in the **Create New Rule** page and select **led1_ctrl** as the Output. Go to **Events > Alarm Rules** and click **Create New Rule** to begin.

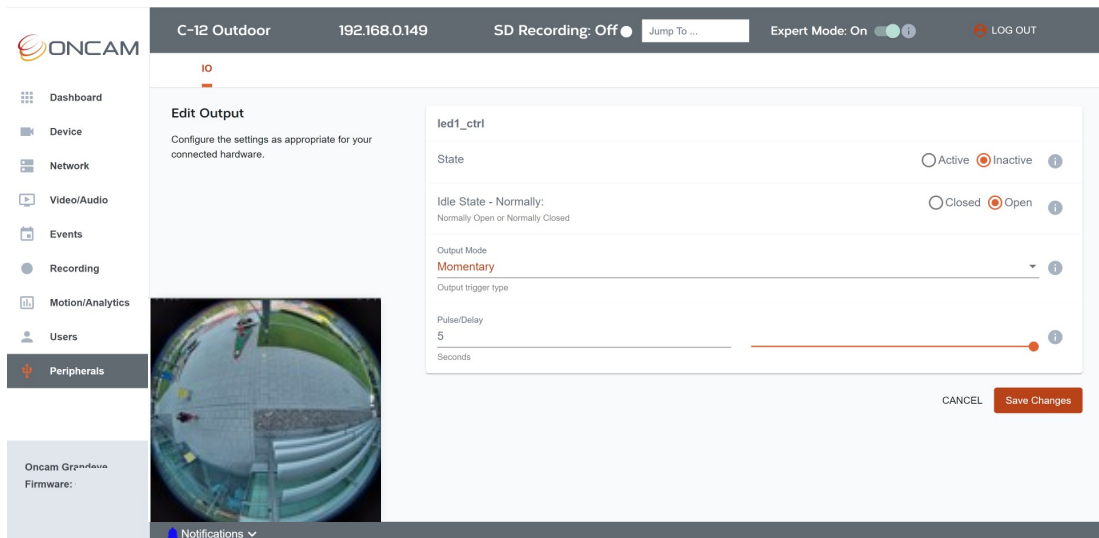


Figure 279 Peripheral Edit LED Output

5.9.1.4.2.1 State

The State control allows you to switch the output manually to the Active or Inactive state for testing, or to reset or trigger an alarm, when the Output Mode is set to Latching.

If the Output Mode is set to Momentary, saving the changes with the State set to Active will immediately trigger the output for the period set in the Pulse/Delay. If you don't want to trigger the output when you save the settings, change it to Inactive. Setting the State to Inactive will not stop the output from operating if activated by an Event rule.

5.9.1.4.2.2 Idle State

The Idle State can be defined as Open or Closed.

If Idle State is set to Open, the LED 1 output will be logical LOW when led1_ctrl is **Inactive**, and logical HIGH when **Active**.

If Idle State is set to Closed, the LED 1 output will be logical HIGH when led1_ctrl is **Inactive**, and logical LOW when **Active**.

In other words, select Closed if you want to invert the output logic.

Choose the setting that corresponds to the behavior of the connected equipment.

5.9.1.4.2.3 Output Mode

The Output Mode has two options:

Latching allows the output to stay in the last state it was switched to until caused to change again. This is useful when one event should cause the output to change, and another should cause it to switch back again.

Momentary allows the output to stay in a default state until triggered to change and then, once triggered, change for a selected period of time and then return to the default state. This is useful when an event should trigger an external device to do something for a period of time, such as sound an alarm, operate a door, etc.

5.9.1.4.2.4 Pulse Delay

When Output Mode is set to Momentary, use the Pulse Delay to control how long the output remains active when triggered. For example, if the output is wired to sound an alarm while active, this would set the duration of the alarm.

5.9.1.4.3 LED 2 / led2_ctrl

The output labelled LED 2 on the Plus Module is controlled by the signal called **led2_ctrl** in the camera's software and ONVIF-conformant API.

If you want to assign the LED 2 output as a rule action in the camera's internal Events system, simply choose the Action Type **oncam:HardwareOutput** in the **Create New Rule** page and select led2_ctrl as the Output. Go to **Events > Alarm Rules** and click **Create New Rule** to begin.

5.9.1.4.3.1 State

The State control allows you to switch the output manually to the Active or Inactive state for testing, or to reset or trigger an alarm, when the Output Mode is set to Latching.

If the Output Mode is set to Momentary, saving the changes with the State set to Active will immediately trigger the output for the period set in the Pulse/Delay. If you don't want to trigger the output when you save the settings, change it to Inactive. Don't worry, setting the State to Inactive will not stop the output from operating if activated by an Event rule.

5.9.1.4.3.2 Idle State

The Idle State can be defined as Open or Closed.

If Idle State is set to Open, the LED 2 output will be logical LOW when led1_ctrl is **Inactive**, and logical HIGH when **Active**.

If Idle State is set to Closed, the LED 2 output will be logical HIGH when led1_ctrl is **Inactive**, and logical LOW when **Active**.

In other words, select Closed if you want to invert the output logic.

Choose the setting that corresponds to the behavior of the connected equipment.

5.9.1.4.3.3 Output Mode

The Output Mode has two options:

Latching allows the output to stay in the last state it was switched to until caused to change again. This is useful when one event should cause the output to change, and another should cause it to switch back again.

Momentary allows the output to stay in a default state until triggered to change and then, once triggered, change for a selected period of time and then return to the default state. This is useful when an event should trigger an external device to do something for a period of time, such as sound an alarm, operate a door, etc.

5.9.1.4.3.4 Pulse Delay

When Output Mode is set to Momentary, use the Pulse Delay to control how long the output remains active when triggered. For example, if the output is wired to sound an alarm while active, this would set the duration of the alarm.

6. Technical Support

Should you require any technical assistance, please contact your Oncam 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 visit to: <https://support.oncamgrandeye.com/s/>

- Download user documentation and software updates.
- Find answers to resolved problems in the FAQ database, search by product, category, or phrase.

To contact us via email, please use: support@oncamgrandeye.com.

Include the following in your email:

- A detailed description of the problem
- Camera model numbers
- Relevant configuration information

Appendix A

Connecting Directly to Camera Streams

The Camera Streams can be tested by connecting directly to camera streams (MJPEG, H.264 & H.265) using your media player. For this you will require your camera's IP address and the appropriate URL as shown below:

URL example format:

```
rtsp://Camera_ip_address:port_number/MJPEG/video.sdp?name=MP1  
rtsp://Camera_ip_address:port_number/MJPEG/video.sdp?name=MP2  
rtsp://Camera_ip_address:port_number/MJPEG/video.sdp?name=MP3  
rtsp://Camera_ip_address:port_number/MJPEG/video.sdp?name=MP4
```

```
rtsp://Camera_ip_address:port_number/h264/video.sdp?name=MP1  
rtsp://Camera_ip_address:port_number/h264/video.sdp?name=MP2  
rtsp://Camera_ip_address:port_number/h264/video.sdp?name=MP3  
rtsp://Camera_ip_address:port_number/h264/video.sdp?name=MP4
```

```
rtsp://Camera_ip_address:port_number/h265/video.sdp?name=MP1  
rtsp://Camera_ip_address:port_number/h265/video.sdp?name=MP2  
rtsp://Camera_ip_address:port_number/h265/video.sdp?name=MP3  
rtsp://Camera_ip_address:port_number/h265/video.sdp?name=MP4
```

For example, if the C-Series camera has the IP address 192.168.0.100, port 554 (H.264 RTSP stream is port 554), then the URL for MP1 would be:

```
rtsp://192.168.0.100:554/h264/video.sdp?name=MP1
```

For access to all streaming URL's the username and password is required.

Required codec (MJPEG, H.264, H.265) must be selected in the media profile to be streamed. Only one MJPEG encoder can be set.

Appendix B

List of Figures

Figure 1 Drilling Template.....	13
Figure 2 Opening of Camera Enclosure.....	13
Figure 3 Mounting of Camera Enclosure.....	13
Figure 4 Punch down Adapter.....	14
Figure 5 Identify Wiring Type for Punch Down.....	14
Figure 6 Punch Down Wires.....	15
Figure 7 Protective Cover Removal.....	15
Figure 8 Connecting of Camera Module.....	15
Figure 9 Connecting of Ethernet Cable.....	16
Figure 10 Securing the Camera Module.....	16
Figure 11 Protective Lens Cover Removal.....	16
Figure 12 Cover Twist.....	17
Figure 13 Drilling Hole.....	17
Figure 14 Feeding Ethernet cable to the hole.....	17
Figure 15 Connecting of RJ45 / Punch down.....	18
Figure 16 Snipping of Support tabs for Punch down.....	18
Figure 17 Snipping of Support tab for Ethernet Cable.....	18
Figure 18 Removal of Plug using Pliers.....	19
Figure 19 Inserting of Grommet.....	19
Figure 20 Mount Screws Removal.....	19
Figure 21 Indoor Enclosure Opening.....	20
Figure 22 Inserting Punch down adaptor.....	20
Figure 23 Punch down Ethernet cable.....	20
Figure 24 Identify Wiring Type for Punch Down.....	21
Figure 25 Punch Down Wires.....	21
Figure 26 Inserting Rear Enclosure into Recessed Mount.....	22
Figure 27 Protective Cover Removal.....	22
Figure 28 Plug in RJ45 Cable.....	22
Figure 29 Plug in of Camera Module into the Recessed Enclosure.....	23
Figure 30 Securing of Recessed Enclosure into the Ceiling.....	23
Figure 31 Protective Lens Cover Removal.....	23
Figure 32 Clipping of Front Cover.....	24
Figure 33 Slot Alignment with LED.....	24
Figure 34 Pendant Mount.....	24
Figure 35 Mounting Screws Removal.....	25
Figure 36 Opening of Camera Enclosure.....	25
Figure 37 Punch Down Adaptor.....	25
Figure 38 Punch Down Ethernet Cable.....	26
Figure 39 Identify Wiring Type for Punch Down.....	26
Figure 40 Punch Down Wires.....	27
Figure 41 Secure Camera Enclosure onto the Pendant Mount.....	27
Figure 42 Protective Cover Removal.....	27
Figure 43 Connecting Camera Using RJ5 / Punch Down.....	28
Figure 44 Camera Image Alignment.....	28
Figure 45 Locking Screw.....	29
Figure 46 Protective Lens Cover Removal.....	29
Figure 47 Align and close the Camera Enclosure Front Cover.....	29
Figure 48 Drilling Template.....	30
Figure 49 Remove Card Insert.....	30
Figure 50 Mount to wall.....	31
Figure 51 Opening of Camera Enclosure.....	31
Figure 52 Mounting of Camera Enclosure.....	31
Figure 53 Punch down Adapter.....	32
Figure 54 Identify Wiring Type for Punch Down.....	32
Figure 55 Punch Down Wires.....	33

Figure 56 Protective Cover Removal.....	33
Figure 57 Connecting of Camera Module.....	33
Figure 58 Connecting of Ethernet Cable.....	34
Figure 59 Securing the Camera Module.....	34
Figure 60 Protective Lens Cover Removal.....	34
Figure 61 Cover Twist.....	35
Figure 62 - Remove Label.....	35
Figure 63 - Hex Tool Unlocks.....	35
Figure 64 Loosen Captive Screws.....	36
Figure 65 Front Camera Enclosure removal.....	36
Figure 66 Drilling Template.....	37
Figure 67 Gland Identification.....	37
Figure 68 Removal of Gland.....	37
Figure 69 Sealing of Cable.....	38
Figure 70 Gland into Rear Enclosure.....	38
Figure 71 Check positioning.....	38
Figure 72 Gland Alignment.....	39
Figure 73 Rear Enclosure.....	39
Figure 74 Plugging RJ45 Connector to RJ45 Socket.....	39
Figure 75 Removal of RJ45 Board.....	40
Figure 76 Insert Punch Down Board.....	40
Figure 77 Punch Down Ethernet Cable.....	40
Figure 78 Identify Wiring Type for Punch Down.....	41
Figure 79 Protective Film Removal.....	41
Figure 80 Protective Cover Removal.....	42
Figure 81 Camera Module Connection.....	42
Figure 82 Reattach Front Cover.....	42
Figure 83 Protective Cover Removal.....	43
Figure 84 Secure the Front Cover.....	43
Figure 85 Protective Cover Removal.....	43
Figure 86 Ethernet Cable onto the Pendant Mount.....	44
Figure 87 Removal of Mounting Screws.....	44
Figure 88 Loosen Captive Screws.....	44
Figure 89 Opening of Camera Enclosure.....	45
Figure 90 Gland Identification.....	45
Figure 91 Removal of Gland.....	45
Figure 92 Sealing of Cable.....	46
Figure 93 Gland into Rear Enclosure.....	46
Figure 94 Check Positioning.....	46
Figure 95 Gland Alignment.....	47
Figure 96 Secure Rear Enclosure to the Pendant Mount.....	47
Figure 97 RJ45 Connector into RJ45 Socket.....	47
Figure 98 Removal of RJ45 Board.....	48
Figure 99 Insert Punch Down Board.....	48
Figure 100 Punch Down of Ethernet Cable.....	48
Figure 101 Identify Wiring Type for Punch Down.....	49
Figure 102 Protective Film Removal.....	49
Figure 103 Protective Cover Removal.....	50
Figure 104 Camera Module.....	50
Figure 105 Camera Module Alignment.....	50
Figure 106 Reattach the front cover.....	51
Figure 107 Protective Lens Cover.....	51
Figure 108 Secure Front Enclosure.....	51
Figure 109 Protective Film.....	52
Figure 110 Camera after installation.....	52
Figure 111 Undo The Locking Screw.....	53
Figure 112 Run Ethernet Cable.....	53
Figure 113 Screw To Pendant.....	53
Figure 114 Adjust The Angle.....	54
Figure 115 Tighten The Locking Screw.....	54
Figure 116 - Screw On Pendant Mount.....	54

Figure 117 – Mounting Screws.....	55
Figure 118 Loosen Captive Screws.....	55
Figure 119 Opening of Camera Enclosure.....	55
Figure 120 Gland Identification.....	56
Figure 121 Removal of Gland.....	56
Figure 122 Sealing of Cable.....	56
Figure 123 Gland into Rear Enclosure.....	57
Figure 124 Check Positioning.....	57
Figure 125 Gland Alignment.....	57
Figure 126 Secure Rear Enclosure to the Pendant Mount.....	58
Figure 127 RJ45 Connector into RJ45 Socket.....	58
Figure 128 Removal of RJ45 Board.....	58
Figure 129 Insert Punch Down Board.....	59
Figure 130 Punch Down of Ethernet Cable.....	59
Figure 131 Identify Wiring Type for Punch Down.....	60
Figure 132 Protective Film Removal.....	60
Figure 133 Protective Cover Removal.....	60
Figure 134 Camera Module.....	61
Figure 135 Reattach the front cover.....	61
Figure 136 Protective Lens Cover.....	61
Figure 137 Secure Front Enclosure.....	62
Figure 138 Protective Film.....	62
Figure 139 Lock Angles.....	62
Figure 140 Remove mounting screws.....	63
Figure 141 Align Rain Guard.....	63
Figure 142 Screw rear enclosure To Pendant mount.....	64
Figure 143 Align Rain Guard.....	64
Figure 144 – Insert Gland, install to surface.....	65
Figure 145 IO Entry Gland.....	65
Figure 146 Multi – Core Cable.....	66
Figure 147 Sealing the Cable Sheath.....	66
Figure 148 Cable through Screw Terminals.....	66
Figure 149 Cable Path to Screw Terminals.....	67
Figure 150 Alarm Output Signal.....	67
Figure 151 Alarm Input Signal.....	67
Figure 152 Audio Microphone.....	68
Figure 153 Audio Speaker.....	68
Figure 154 DC Power.....	68
Figure 155 Camera Module Removal.....	69
Figure 156 Camera Module Box.....	69
Figure 157 Protective Cover Removal.....	70
Figure 158 Camera Module Box.....	70
Figure 159 Remove Protective Film.....	70
Figure 160 Align Heater Module.....	71
Figure 161 Secure the Heater Module.....	71
Figure 162 Camera Module Box.....	71
Figure 163 Step 1 – Wall Mount Plate.....	72
Figure 164 Step 2 – Mounting Holes.....	72
Figure 165 Step 3 – Fixing Wall Mount into the Wall.....	72
Figure 166 Step 4 – Feeding Ethernet Cable through the Hook Plate.....	73
Figure 167 Step 5 – Hook Plate Placement.....	73
Figure 168 Step 6 – Arm Body.....	73
Figure 169 Step 7 – Arm at Right Angle.....	74
Figure 170 Step 8 – Pendant Arm.....	74
Figure 171 microSD Card Slot.....	75
Figure 172 Inserting microSD Card.....	75
Figure 173 microSD Card Insertion / Ejection.....	76
Figure 174 Camera Front Cover.....	76
Figure 175 Retaining Front Screws using Hex Tool.....	76
Figure 176 Camera Module off the Rear.....	77

Figure 177 Undo Wall Mount Fix.....	77
Figure 178 Retaining Front Screws using Hex Tool	78
Figure 179 Undo Retaining Tether.....	78
Figure 180 Remove camera module Screws using Hex Tool	78
Figure 181 Undo Wall Mounting.....	79
Figure 182 CCT Discovery.....	81
Figure 183 Camera Web Interface, Set Password	82
Figure 184 CCT, Set Password.....	83
Figure 185 CCT Username and Password Setting.....	84
Figure 186 CCT Password Confirmation.....	85
Figure 187 Dashboard Overview.....	86
Figure 188 Dashboard Overview Fullscreen	87
Figure 189 Dashboard Logout.....	89
Figure 190 Network Configuration.....	89
Figure 191 Advanced Network Configuration.....	91
Figure 192 Advanced Network SNMP.....	92
Figure 193 Advanced Network EAP.....	94
Figure 194 Media Profile Overview	96
Figure 195 Media Profiles, Camera Mode Change Request.....	97
Figure 196 Media Profiles, Camera Mode Changed.....	97
Figure 197 Media Profile Edit.....	99
Figure 198 Media Profile, New Profile Creation.....	100
Figure 199 Media Profile, Video Source Selection.....	101
Figure 200 Media Profile, Video Source Change Confirmation.....	104
Figure 201 Media Profile, TrueDetail HDR Impact.....	107
Figure 202 Media Profile Bit Rate Control.....	111
Figure 203 Media Profile StreamLite Compression.....	113
Figure 204 Media Profile Video Multicast.....	116
Figure 205 Media Profile Audio	118
Figure 206 Media Profile Metadata	118
Figure 207 Media Profile Adjust Dewarped View.....	121
Figure 208 Media Profile Adjust Panoramic+ View.....	121
Figure 209 Media Profile Adjust Corridor+ View.....	124
Figure 210 Media Profile Adjust T Corridor+ View.....	125
Figure 211 Media Profile Adjust VCam View.....	127
Figure 212 Media Profile Adjusted VCam View.....	128
Figure 213 Image Setting Overview.....	129
Figure 214 Image Preference	131
Figure 215 WDR Image Setting.....	133
Figure 216 Camera Mounting.....	134
Figure 217 IR Cut Filter Mode.....	135
Figure 218 Color Space Mode.....	136
Figure 219 Overlays Overview.....	137
Figure 220 Overlay on Screen Caption.....	138
Figure 221 Overlays Privacy Region.....	139
Figure 222 Video / Audio Overlays Privacy Region.....	140
Figure 223 Video / Audio Overlays Privacy Region Overview.....	141
Figure 224 Global StreamLite Setting ColorMap and Dynamic ROI.....	142
Figure 225 Global StreamLite Dynamic GoP Length Setting.....	144
Figure 226 Global StreamLite Dynamic FPS Reduction Setting.....	146
Figure 227 Global StreamLite Motion Setting.....	147
Figure 228 Global Audio Settings.....	148
Figure 229 Global Audio Settings, Audio Multicast.....	149
Figure 230 Multicast Summary Table.....	151
Figure 231 Recording Format microSD card.....	152
Figure 232 Recording Formatting Warning.....	153
Figure 233 Recording Formatting in progress.....	153
Figure 234 Recording Formatting complete.....	154
Figure 235 Recording Configuration Overview.....	155
Figure 236 Recording Create a Configuration.....	155
Figure 237 Event Based Recording.....	157

Figure 238 Recording Configuration Editing.....	158
Figure 239 Recording Search.....	159
Figure 240 Recording Search Result.....	161
Figure 241 Events Overview.....	162
Figure 242 Events Create New Rule.....	162
Figure 243 Events Trigger Action.....	168
Figure 244 Event Recording Action.....	170
Figure 245 Events Edit Rule.....	172
Figure 246 Motion Analytics Overview.....	173
Figure 247 Motion Analytics Create New.....	174
Figure 248 Motion Analytics Draw Region.....	175
Figure 249 Motion Analytics Edit Rules.....	181
Figure 250 Motion Analytics Global Settings.....	182
Figure 251 Users Overview.....	183
Figure 252 New User Creation.....	184
Figure 253 User Summary Table Update.....	186
Figure 254 User Editing Options.....	186
Figure 255 Users, Delete Account Confirmation.....	187
Figure 256 Device Information Overview.....	187
Figure 257 Device Information EVO-12 ONVIF Emulation.....	189
Figure 258 Date / Time Overview.....	190
Figure 259 Date / Time Manual Setting.....	191
Figure 260 Date / Time NTP Network Setting.....	192
Figure 261 Date / Time NTP Save Setting.....	192
Figure 262 Maintenance Support Reboot.....	193
Figure 263 CCT Maintenance Support Reboot.....	194
Figure 264 CCT Maintenance Support Reboot Progress Status.....	194
Figure 265 Maintenance Support Reset.....	196
Figure 266 CCT Maintenance Support Reset.....	196
Figure 267 Maintenance and Support Backup.....	198
Figure 268 Maintenance Support Status LED.....	200
Figure 269 Firmware Update.....	201
Figure 270 Firmware Update Progress Display.....	202
Figure 271 CCT Firmware Update Multiple Cameras.....	202
Figure 272 CCT Firmware Update Multiple Cameras Progress bars.....	203
Figure 273 License Overview.....	205
Figure 274 Download Root CA.....	208
Figure 275 Install Root CA Certificate.....	208
Figure 276 Peripheral Input / Output Overview.....	210
Figure 277 Peripheral Edit Input.....	211
Figure 278 Peripheral Edit Alarm Output.....	212
Figure 279 Peripheral Edit LED Output.....	214

Appendix C

List of Tables

<i>Table 1 Port Pre - Configuration.....</i>	<i>6</i>
<i>Table 2 Characteristics and Capabilities of Encoders.....</i>	<i>101</i>
<i>Table 3 C-12 Video Resolutions Supported by Encoder and Video Source.....</i>	<i>105</i>
<i>Table 4 C-08 Video Resolutions Supported by Encoder and Video Source.....</i>	<i>106</i>
<i>Table 5 Encoder Bit Rate Level.....</i>	<i>111</i>
<i>Table 6 Encoder Bit Rate Level.....</i>	<i>112</i>
<i>Table 7 Storage Requirements Estimation.....</i>	<i>156</i>
<i>Table 8 Events Trigger List.....</i>	<i>168</i>
<i>Table 9 Status LED.....</i>	<i>199</i>
<i>Table 10 Plus Module Alarm Input.....</i>	<i>211</i>
<i>Table 11 Plus Module Alarm Output.....</i>	<i>212</i>