Installation and User Guide

Saros™ Dome Camera

Important Instructions and Notices to the User:

This device complies with part 15 of the FCC Rules and ISED's license-exempt RSSs. 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.

L'appareil est conforme à la section 15 des règles de la FCC et aux RSS exempts de licence de ISED. Le fonctionnement de l'appareil est soumis aux conditions suivantes: (1) Il ne doit pas causer d'interférences nuisibles, and (2) il peut accepter toute interférence, y compris celle susceptible de provoquer un fonctionnement indésirable de l'appareil.

This equipment complies with FCC radiation exposure limits and Canada radiation RF exposure limits set forth in CFR 47 Section 2.1091 and ISED RSS-102 set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20cm between the user and/or bystanders and this device. This device must not be co-located or operating in conjunction with any other antenna or transmitter, unless permitted under existing FCC certification condition.

Cet appareil est conforme aux limites d'exposition aux rayonnements de la FCC et aux limites d'exposition aux RF du Canada établies dans le CFR 47, section 2.1091 et ISED RSS-102 pour un environnement non contrôlé. Cet équipement doit être installé et utilisé avec une distance minimale de 20 cm entre l'utilisateur et / ou des tiers et cet appareil. Cet appareil ne doit pas être co-localisé ou fonctionner en conjonction avec une autre antenne ou un autre émetteur.

Modification of this device without the express authorization of FLIR Systems, Inc. may void the user's authority under FCC rules to operate this device.

Note 1: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at the user's own expense.

Note 2: If this equipment came with shielded cables, it was tested for compliance with the FCC limits for a Class A digital device using shielded cables and therefore shielded cables must be used with the device

Industry Canada Notice:
This Class A digital apparatus complies with Canadian ICES-003.

Avis d'Industrie Canada:
Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

Proper Disposal of Electrical and Electronic Equipment (EEE)

The European Union (EU) has enacted Waste Electrical and Electronic Equipment Directive 2002/96/EC (WEEE), which aims to prevent EEE waste from arising; to encourage reuse, recycling, and recovery of EEE waste; and to promote environmental responsibility.

In accordance with these regulations, all EEE products labeled with the "crossed out wheeled bin" either on the product itself or in the product literature must not be disposed of in regular rubbish bins, mixed with regular household or other commercial waste, or by other regular municipal waste collection means. Instead, and in order to prevent possible harm to the environment or human health, all EEE products (including any cables that came with the product) should be responsibly discarded or recycled.

To identify a responsible disposal method nearby, please contact the local waste collection or recycling service, the original place of purchase or product supplier, or the responsible government authority in the area. Business users should contact their supplier or refer to their purchase contract.

Document History

Revision	Date	Comment
100	December 2018	Initial release of Saros Dome camera with video analytics intrusion detection
110	April 2019	V1.0.3 - Added Saros Cloud Web Application, Wi-Fi, InstallerApp, audio input support
120	August 2019	Removed UL from specifications

Table of Contents

Table of Contents

1   Installation

This chapter provides an overview of the Saros Dome security camera, and describes how to install and configure it for networking.

1.1   Camera Overview

Saros Dome includes multiple thermal sensors, a 1080p visible light camera, IR and visible LED illuminators, advanced on-board thermal video analytics, audio, and digital I/O. The thermal video analytics provides tripwire, detection, and masking area configuration; human & vehicle detection and classification; and manual and automatic scene analysis.

When the camera is connected to an IP network, it functions as a server, providing services such as camera control, video streaming, network communications, and video analytics alarm capabilities. The server uses an open, standards-based communication protocol to communicate with FLIR and third-party video management system (VMS) clients, including systems that are compatible with ONVIF®.[1] These clients can be used to control the camera and stream video during day-to-day operations. For a list of supported VMS clients, refer to the individual product web page at https://www.flir.com/browse/security/thermal-security-cameras/.

Saros cameras can be onboarded to FLIR Cloud, which allows private, secure access to the camera:

- Over the internet using a standard web browser, via the camera's FLIR Cloud web application. You can perform tasks such as viewing the camera's live video feed and managing its video analytics settings.

- Using the FLIR Cloud REST API.

The video from the camera is viewed by streaming it over an IP network using M-JPEG and H.264 encoding.

The Saros cameras are components within the FLIR Thermal Fence, which combines FLIR thermal security cameras, the FLIR Cloud, and control and management software in a fully integrated perimeter security solution. The FLIR Thermal Fence provides automated perimeter surveillance, intrusion detection, and alert capabilities for perimeter security applications. The FLIR Thermal Fence gives you instant, automated threat detection and visual threat assessment capability around the clock in one easy-to-use package.

If help is needed during the installation process, contact the local FLIR service representative or call the appropriate support number listed at: https://www.flir.com/support-center/support-hq/. All installers and integrators are encouraged to take advantage of the training offered by FLIR; visit https://www.flir.com/support-center/training/ for more information.

For safety, and to achieve the highest levels of performance from the Saros Dome camera system, always follow the warnings and cautions in this manual when handling and operating the camera.

Warning!

> ⚠️ Before drilling into surfaces for camera mounting, verify that electrical or other utility service lines are not present. Serious injury or death may result from failure to heed this warning.

---

1. ONVIF is a trademark of Onvif, Inc.

1.2   Installation Overview

The Saros Dome camera can be used for indoor or outdoor security applications.

1.2.1   Camera Connections

The camera can be powered using Power over Ethernet (PoE) or with a conventional 24 Vac or 12 Vdc power supply. To be powered using PoE, the camera must be connected to either a PoE switch or a standalone PoE power supply (also called a PoE injector). The maximum Ethernet cable run is 100 meters, including the PoE power supply. For installations using PoE power and IP video, a single Ethernet cable is the only required connection. The Saros Dome camera is a Powered Device compliant with the IEEE 802.3af-2003 standard.

Input/Output

The camera can receive one input signal and can provide one output signal. By default, the signals are configured for normally open alarm switch circuits. Refer to Power & I/O Connector.

Input Signal—When an external alarm device closes a switch to complete the circuit for the camera, an input signal is generated to cause an action or an alarm when configured on the Alarm Page. See also Input/Output (I/O) Page.

Output Signal—When an output alarm is generated, the camera closes its internal switch to complete the circuit for the receiving device.

1.2.2 Supplied Components

The Saros Dome camera kit includes these standard components:

Items Included in Kit

1.2.3 Additional Supplies

The installer might need to supply the following items as required (specific to the installation).

- PoE power supply or PoE switch for camera power.
- Cat5e or Cat6 Ethernet cable for digital video and PoE for system power.
- Ten-conductor accessory cable for auxiliary power and alarm in/out.
- Camera grounding strap, camera mount, electrical hardware, connectors, and tools.

1.2.4 Site Preparation

The following recommendations provide for proper installation and operation of the unit. Adhere to all local and industry standards, codes, and best practices.

- **Ambient Environment Conditions**: Avoid positioning the unit near heaters or heating system outputs. Avoid exposure to direct sunlight.
- **Safety**: Cables and electrical cords should be routed in a manner that prevents safety hazards. Ensure that nothing rests on the unit's cables or power cords.
- **Ample Air Circulation**: Leave enough space around the unit to allow free air circulation.
- **Cabling Considerations**: Using a cable longer than the manufacturer's specifications for optimal video signal may result in degradation of color and video parameters.

- **Physical Security**: The unit provides threat detection for physical security systems. In order to ensure that the unit cannot be disabled or tampered with, the system should be installed with security measures regarding physical access by trusted and untrusted parties.

- **Network Security**: The unit transmits over IP to security personnel for video surveillance. Proper network security measures should be in place to assure networks remain operating and free from malicious interference. Install the unit on the backbone of a trusted network.

- **Electrostatic Discharge Safeguards**: The unit and other equipment connected to it (relay outputs, alarm inputs, racks, carpeting, etc.) shall be properly grounded to prevent electrostatic discharge.

1.2.5   Configure for Networking

The Saros Dome camera ball and back box are shipped in separate boxes. The camera ball can be configured for networking while still in its shipping box using PoE, or after installation. If you are configuring the camera for networking before installation, power the camera using a PoE switch or PoE injector.

By default, a Dynamic Host Configuration Protocol (DHCP) server on your network dynamically sets the camera's IP address. If there is no DHCP server on the network, 192.168.0.250 is the camera's default IP address.

You can specify another IP address for the camera and configure it for networking with the FLIR InstallerApp, the FLIR Discovery Network Assistant (DNA) software tool, or the camera's web page.

The procedure for configuring the camera for networking using InstallerApp for iOS is slightly different than when using InstallerApp for Android. For information about configuring the camera for networking using InstallerApp for iOS, see the InstallerApp for iOS *User Guide*.

To configure the camera for networking using the InstallerApp for Android:

Step 1   Install the InstallerApp for Android from the Google Play Store[TM] (https://play.google.com/store/apps/details?id=com.flir.installerapp).

Step 1   Open the InstallerApp by tapping the app icon ◆.
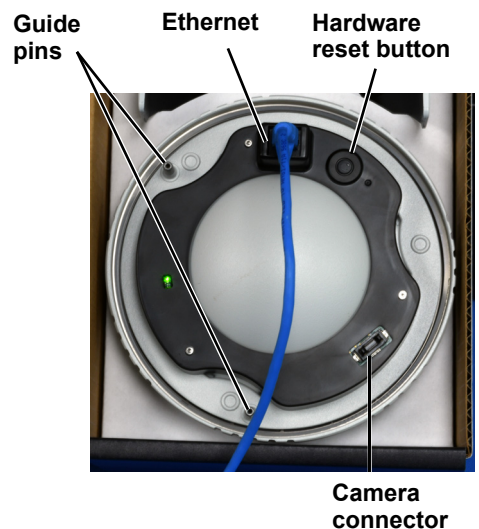
When using the InstallerApp for the first time, Android prompts you to allow the app to access the device's location. The InstallerApp requires this access.

The User Login to Cloud screen appears.

Step 2   Either log in to FLIR Cloud or tap **Skip**.

Tip

If you are onboarding the camera to FLIR Cloud, log in to FLIR Cloud now.

If you tap **Skip** instead of logging in to FLIR Cloud, to use the InstallerApp, you need to accept FLIR's Privacy Policy and Terms of Use.

Step 3 On the Choose a Camera screen, tap the camera you are installing. The InstallerApp attempts to connect to the camera using a wireless connection.

If the camera you are installing does not appear in the list, you might need to re-enable its wireless network by performing a factory default. The camera automatically disables its wireless network after one hour. You can perform a factory default by pressing the camera's hardware reset button or by accessing the camera's Firmware & Info Page.

The first time the InstallerApp attempts to connect to a camera, the InstallerApp prompts you to specify a password for the camera's admin login. After specifying and confirming the password, tap **Save**. For User name, type *admin*; type the password you specified; and then tap **Connect**.

When the connection is made, the Camera Setup screen appears.

Step 4 On the Camera Setup screen, tap the **Network Settings** area.
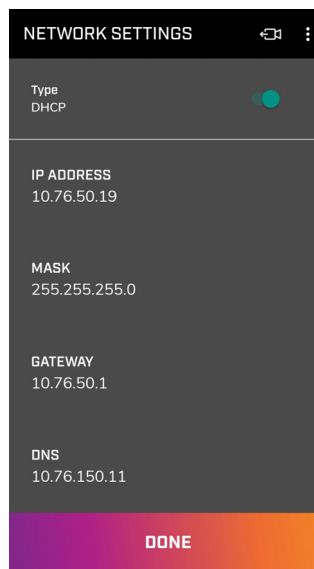
Step 5 On the Network Settings screen, set network parameters such as static IP or DHCP addressing, and then tap **Done**.
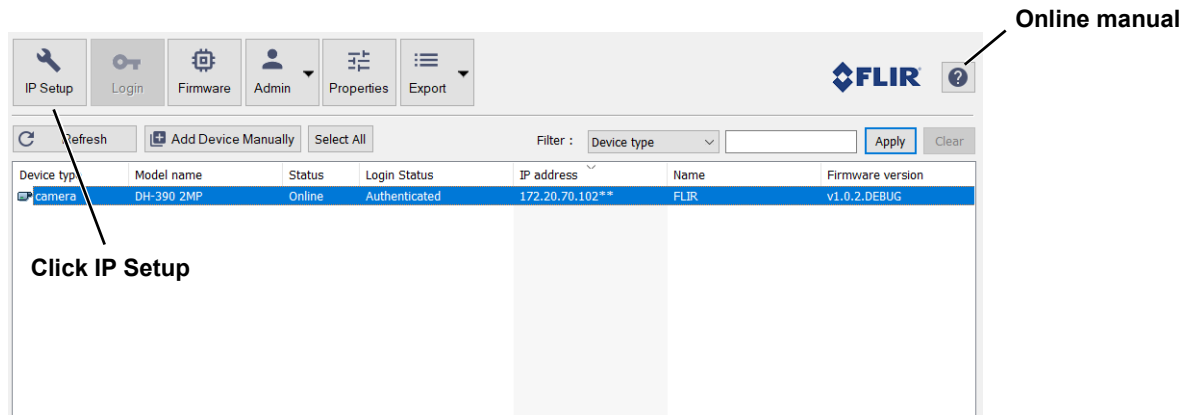
Note

> For instructions on other functions available using the InstallerApp, such as performing scene analysis and locking down the camera, refer to the relevant FLIR InstallerApp user guide (Android or iOS).

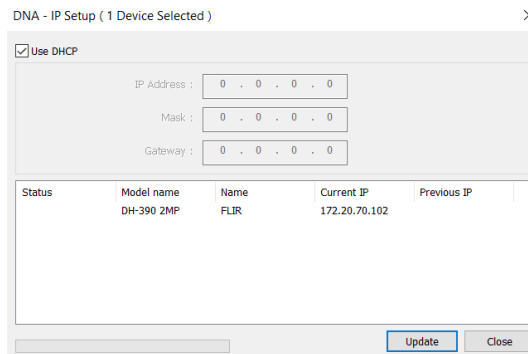**To configure the camera for networking using the DNA tool:**

Step 1 Make sure the PC and the camera are on the same network.

Step 2   On the PC, download the DNA software from the FLIR individual product web page at: https://www.flir.com/browse/security/thermal-security-cameras/

Step 3   Un-zip the downloaded file, and then double-click and run DNA.**exe**. All camera units on the VLAN are discovered.

Online manual

Click IP Setup

Step 4   Select the camera, and then click **IP Setup.**

Step 5   Set network parameters such as static IP or DHCP addressing, and then click **Update**.


Note

For instructions on other functions available using DNA, such as updating the firmware for multiple cameras at the same time, click the help icon while DNA is running.

To configure the camera for networking using the camera's web page:

Step 1   Make sure the camera and the PC are on the same network.

Step 2   Open the camera's web page either by double-clicking the camera in the DNA Discovery List or by typing the camera's IP address in the browser's address bar (when the PC and the camera are on the same network).

Step 3   On the login page, type *admin* for the user name and the admin user password (default: admin).
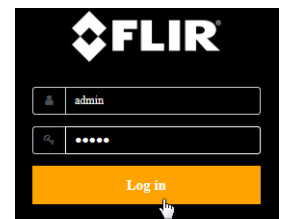
            The View Settings page appears.

This document does not contain any export-controlled information.

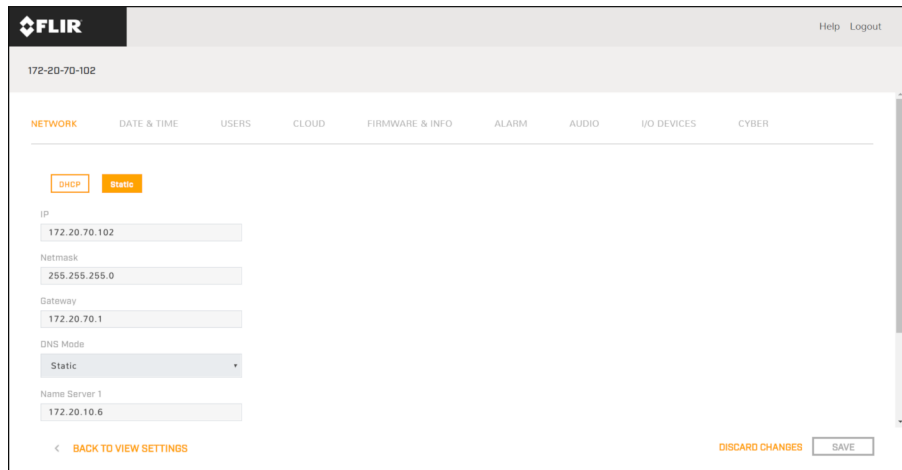Step 4   The first time you log in to the camera, you must change the password for the admin user and then log in again using the new password.
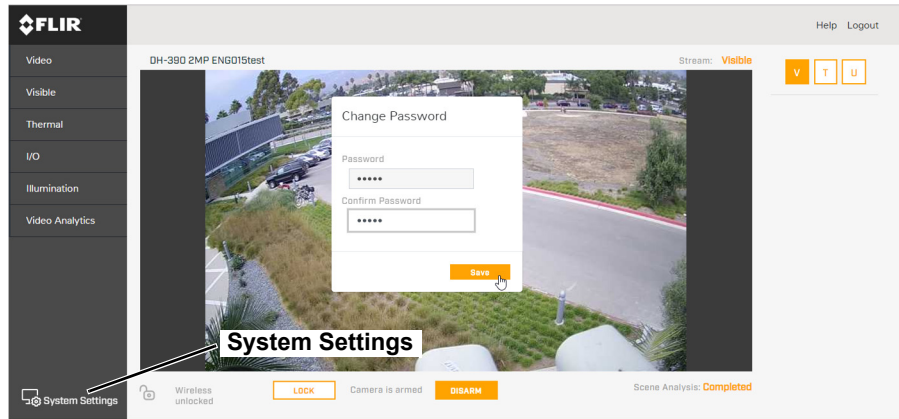
Users can be added as well (refer to Users Page).

Step 5   Click **System Settings**.

Step 6   On the Network tab, set network parameters such as static IP or DHCP addressing, and then click **Save**.

1.2.6   Onboarding the Camera to FLIR Cloud

You can onboard the camera to FLIR Cloud while it is still in its shipping box or after installation, using either the FLIR InstallerApp or the camera's web page.

The procedure for onboarding the camera using InstallerApp for iOS is slightly different than when using InstallerApp for Android. For information about onboarding the camera using InstallerApp for iOS, see the InstallerApp for iOS *User Guide*.

To onboard a camera using InstallerApp for Android:

You can onboard a camera from the Network Settings screen or from

the Pending Cameras screen (tap [icon] and then **Pending cameras**).

Step 1 Make sure the Android device has an active mobile data connection. The InstallerApp uses the Android device's other wireless capabilities to connect to the camera. Therefore, to connect to FLIR Cloud via the internet, the InstallerApp requires the device to have an mobile data connection.

Step 2 Make sure the InstallerApp is logged in to FLIR Cloud. If it is

not logged in, tap [icon] and then **Log in**.

Step 3 From the Network Settings screen, tap **Onboard to Cloud**. The Onboarding screen appears.

Step 4 Enter a friendly and unique camera name using only alphanumeric characters (required). You can also provide additional camera information or description (optional).
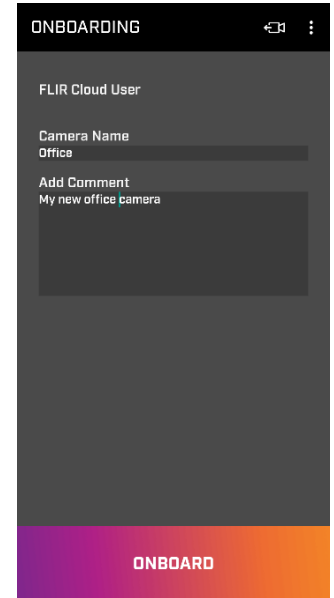
From the Pending Cameras screen, select one or more cameras to onboard.

Step 5 Tap **Onboard**. The InstallerApp attempts to onboard the camera(s) to FLIR Cloud.

If onboarding is not successful for one or more cameras, try onboarding the camera(s) again. You can also save a camera as a pending camera.
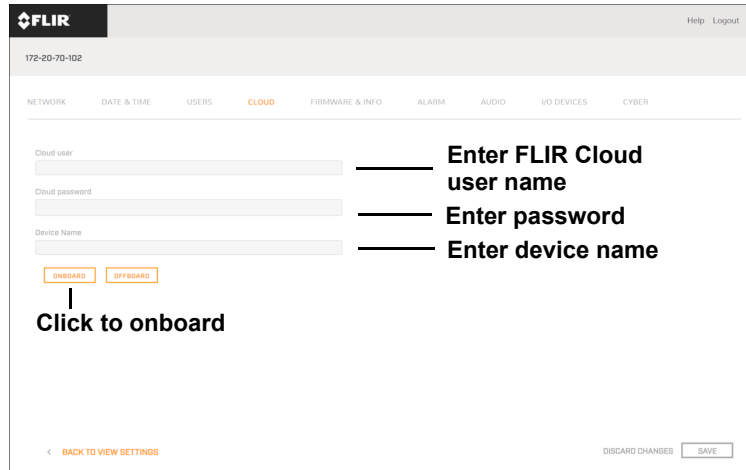
You can onboard cameras to FLIR Cloud using the InstallerApp, but you cannot use it to offboard cameras from FLIR Cloud. To offboard a camera from FLIR Cloud, use the Cyber Page.

After successfully onboarding a camera, the Camera Setup screen appears, indicating the camera is onboarded.

This document does not contain any export-controlled information.

To onboard a camera using the camera's web page:

Step 1   On the camera's System Settings page, click **Cloud**.

Step 2   Enter the user name and password for the FLIR Cloud account to which the camera will be onboarded.

Step 3   For the device name, enter a name using alphanumeric characters, blank spaces, and hyphens. Do not use any other special characters such as @, &, or *. This name identifies the camera in FLIR Cloud.

Step 4   Click **Onboard**.

1.2.7   Camera Placement

For installations with incorporating multiple cameras with on-board video analytics, the cameras' fields of view of cameras should overlap to remove all dead zones in which a camera cannot see a target "head to toe", as demonstrated in the figure below. The camera's on-board analytics must be calibrated to detect targets. Refer to Video Analytics Setup.
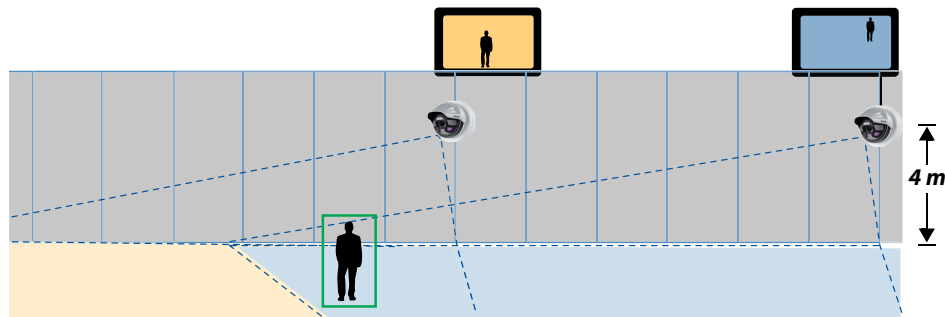

• Install the camera at a height of approximately 4 m (13 ft) or more.

• Typically, you will direct the camera towards the ground with the maximum angle that still allows the camera to image the area of interest. Include as little skyline as possible in the field of view.

• Ensure that cameras are on stable mounts with minimal vibrations and resistance to wind.

1.2.8 Install the Wall Mount

The wall mount bracket fits standard electrical boxes. For surface mounting, secure the bracket, and route the conduit through the side cover on the back box.

A: SINGLE GANG
B: DOUBLE GANG
C: 4" ROUND BOX
D: 4" SQUARE BOX
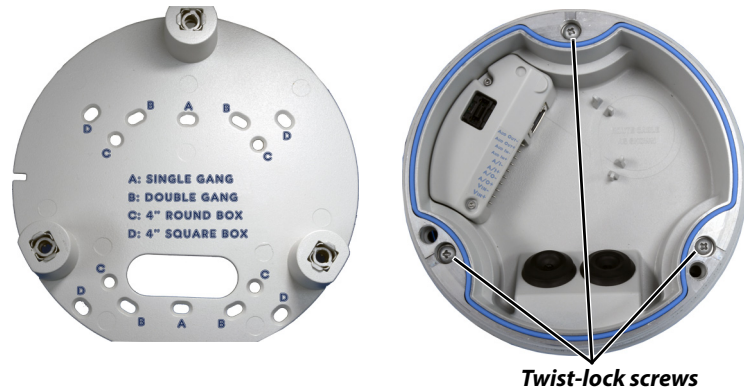
Twist-lock screws

Step 1   Using the screwdriver, undo the three quarter-turn twist-lock assemblies to release the wall mount bracket.

Step 2   Secure the wall mount bracket using the screw holes for the installed electrical box.

1.2.9 Install the Back Box

Step 1   For each cable, use the Torx wrench to punch a hole in the center of the grommet from the underside. Insert the cable from the conduit though the hole.

For surface mount remove with Torx wrench

Punch through grommet from underside here
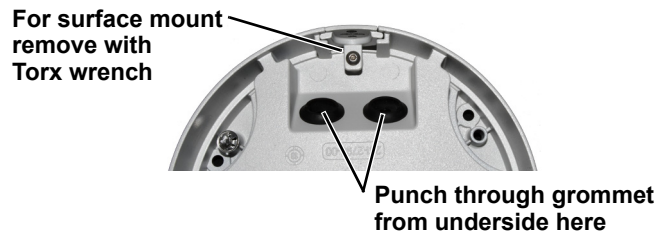
Step 2   Push cables back through the seal so the seal is extended out of the back box, as shown:

Inside back box

Wrong

Correct
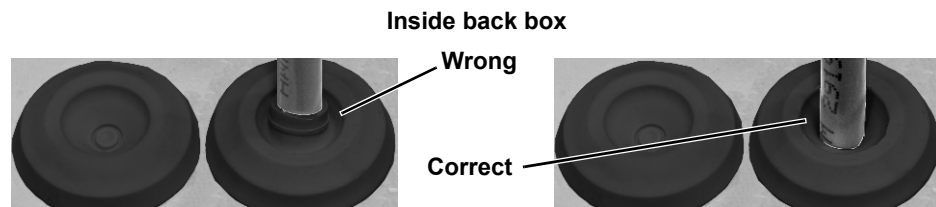
Step 3   Seal all exposed connections. Cable connections are not waterproof.

Connection	Purpose
Ethernet	Power and IP communications
10-pin connector	Power I/O terminal: alarm I/O, audio I/O, Vac or Vdc power

Step 4   Terminate cables and plug into connectors.

Power & I/O Connector

Pin	Connection	Notes
1	Vac/Vdc power +	12 Vdc/24 Vac optional power when PoE is not available
2	Vac/Vdc power -	
3	Alarm Output +	Relay contact: 1A max at 24 Vac/30 Vdc
4	Alarm Output -	
5	Alarm Input +	Dry alarm contact
6	Alarm Input -	
7	Audio In +	1 V P-P line level
8	Audio In -	
9	Audio Out +	1 V P-P line level, connect to amplified speaker
10	Audio Out -	

Step 5   Route the PoE cable as shown below. The PoE cable is all that is required.

Step 6   Secure the back box onto the wall mount bracket using the screwdriver to tighten the three quarter-turn twist-lock assemblies.

1.3   Camera Connections

All connections for the camera are made to the back box assembly. The camera is simply plugged into the back box.

1.3.1   Grounding

Ensure the camera is properly grounded. Failure to properly ground the camera can lead to permanent damage to the camera. Typical to good grounding practices, the camera back box chassis ground should be connected to the lowest resistance path possible.

1.3.2   Connecting Power

The camera is powered over Ethernet using IEEE 802.3af-2003 standard PoE switch or PoE injector. A conventional 24 Vac or 12 Vdc power supply can also be used for powering the camera. Prior to installing the camera onto the back box, ensure the power supply or circuit breaker is off.

1.3.3 Aim the Camera

Ensure the camera ball set screws are loose so that the camera ball can be pushed into its base slightly and rotated.

Camera ball set screw (2)

Step 1   Set the camera ball into the back box. Align the guide pins and screw the camera assembly onto the back box. Make sure to securely tighten the camera ball's outer circular ring onto back box.

Also, when removing the camera ball from back box, take precautions to prevent the ball from becoming a drop hazard for persons or property.

Step 2   Aim the camera by manipulating the camera ball while viewing the image either in the FLIR InstallerApp or on the camera's web page. (See the diagram in Camera Placement.) Then tighten the two set screws.

Step 3   Attach the sunshield for outdoor applications where required.

1.4 Camera Specifications

Camera Model		DH-390 2MP
	Camera Platform Type	Dome
Thermal Sensor Specifications	Array Format	Native 320 × 120, 960 × 360 VividIR
	Detector Type	Long-Life, Uncooled VOx Microbolometer
	Pixel Pitch	12 µm
	Thermal Sensitivity	<50 mK
	Spectral Range	8 µm to 14 µm
	Lens	Athermalized, focus-free; f/1.1
	Optical FoV	2X 57° × 40°, Stitched 102° × 40°
	Thermal Video	Controls for Brightness, Contrast, Colorization, and MSX video overlay
	Thermal AGC Region of Interest (ROI)	Default, Presets and User definable to ensure thermal viewing quality in regions of interest
	Image Uniformity Optimization	Automatic Flat Field Correction (FFC) - Thermal and Temporal Triggers
Visible Light Camera Specifications	Sensor Type	1920 × 1080, 2.1 MP, 1/2.8"
	Lens Type	3-9 mm, f/1.6, P-Iris
	Frame Rate	30 FPS
	Optical FoV	95° × 53°
	Aspect Ratio	16:9
	White Balance	Automatic
	Back Light Compensation	Yes
	Day Night Mode	Automatic with white light and NIR
	PAL/NTSC Environment	Select either 50 Hz (PAL) or 60 Hz (NTSC) shutter timing to match indoor lighting frequency in order to reduce flicker.
System Integration	Ethernet	10/100 Mbps
	Control Interfaces	Nexus SDK for comprehensive system control and integration; Nexus CGI for http command interfaces; ONVIF
	External Analytics Compatible	Yes
	Wi-Fi	Yes, can be disabled using the camera's web page, FLIR InstallerApp, and the Saros Cloud Web Application
Measurement and Analysis	Video Compression	Independent channels of streaming H.264 or M-JPEG
	Analytics Features	Region Entrance/Intrusion Detection, Crossover/Fence Trespassing; Auto/Manual Depth Setup, Human and Vehicle Rules, Hand-off target to autonomous PTZ tracking, Tampering Detection
	Analytics Management	Web-based configuration and management, Masking of detection areas, adjustable sensitivity, automatic responses, remote I/O control

| General	Camera Platform Type	Dome
	Weight	4 lb (1.8 kg) configuration dependent
	Dimensions (H,D)	5.75" x 6.35" (146 mm x 160 mm)
	Power Input/Output	One input dry alarm contacts; One output relay contact 1A max at 24 Vac/30 Vdc
	Input Voltage dc	12 Vdc (±10 %)
	Input Voltage ac	24 Vac (±10 %)
	PoE Input Voltage	IEEE 802.3af-2003 standard
	Shipping weight	6.8 lb (3.1 kg)
	Shipping Dimensions	15" x 11" x 7" (381 mm x 279 mm x 178 mm)
Environmental	IP rating (dust and water ingress)	IP66
	Operating temperature range	-40 °C to 50 °C (-40 °F to 122 °F) continuous operation
	Storage Temperature range	-50 °C to 85 °C (-58 °F to 185 °F)
	Fog/Salt, Humidity	NEMA 4X, Mil-Std-810G
	Vibration	IEC 60068-2-27
	Shock	MIL-STD-810F Transportation
	Drop Testing	FedEx drop test packaging
	Approvals	FCC Part 15 (Subpart B, Class A), CE mark, ISED, EN55032, EN55024, RoHS, WEEE
	Safety	IEC/EN 62368-1, IEC/EN 62471

2   Operation

This chapter describes how to operate the Saros Dome security camera using the camera's web page or the Saros Cloud Web Application.

2.1   Saros Cloud Web Application

To operate and configure a Saros Dome camera using the Saros Cloud Web Application, you must have a FLIR Cloud account and you must onboard the camera to that account (refer to Onboarding the Camera to FLIR Cloud).

To create a FLIR Cloud account:

Step 1   Using a browser, open https://saros.cloud.flir (the Saros Cloud Web Application). The FLIR Cloud Sign In page appears:

Step 2   Click or tap **New to FLIR Cloud? Sign up!**. The FLIR Cloud Sign Up page appears.

Step 3   Enter your first and last name, your email address, and a password; agree to the privacy policy; and click or tap **Sign up**. A message appears confirming registration and you should receive a verification email.
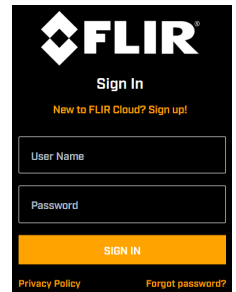
2.2   Accessing a Camera

To access a camera, do one of the following:

- In the DNA tool, double-click the camera in the DNA Discovery List and then log in to the camera.
- Type the camera's IP address in a browser's address bar (when the PC and the camera are on the same network), and then log in to the camera.
- Log in to the Saros Cloud Web Application and select an onboarded camera:
    - a   Open https://saros.cloud.flir.
    - b   Enter your user name and password. Cameras onboarded to your account appear with the names defined when they were onboarded.
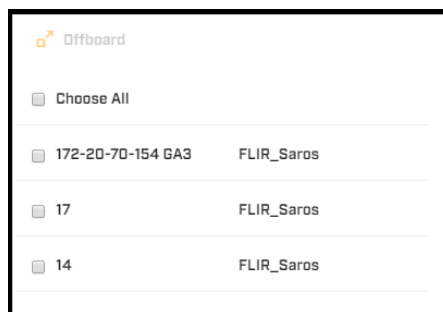
    - c   Select a camera.

The View Settings home page appears.

2.3   View Settings Home Page

The View Settings page displays a live image from the selected video view and a view settings menu along the left side banner, including Video, Visible, Thermal, I/O, Illumination, and Video Analytics.

> **Note**
>
> The Saros Cloud Web Application is similar to the camera's web page. The View Settings pages and operations are available. Some System Settings pages and operations are available. This guide and the example images in it reflect the camera's web page.

Click **System Settings** to configure network and date/time parameters, user accounts and password access, alarm settings, and to perform firmware updates (refer to System Settings Pages). The video detection analytics can be armed/disarmed from this screen and the wireless network can be locked/unlocked. After unlocking the wireless network, the camera automatically locks it after one hour.

Additional choices are for Help and Logout.
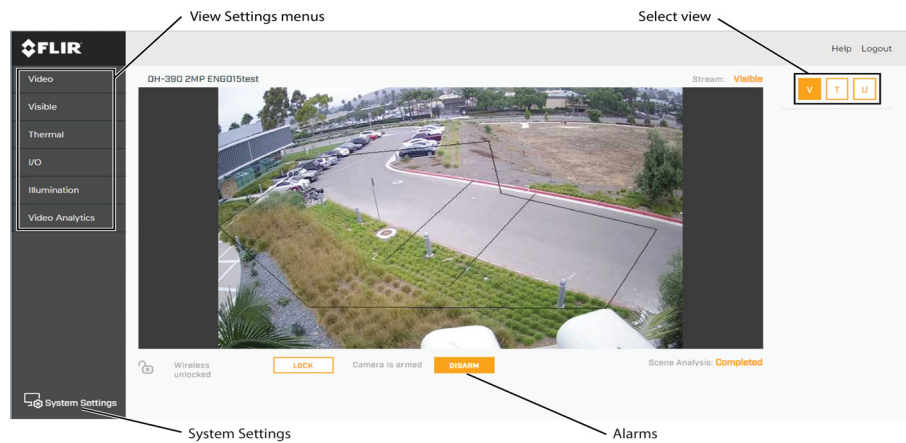
2.3.1   Video Page

In general, it is not necessary to modify the default parameters. In some cases, such as when a video stream is sent over a wireless network, it may be useful to "tune" the video streams to reduce the bandwidth requirements.

By default, three video streams are enabled for the camera: Visible 1 (V1), Visible 2 (V2), and Thermal/Unified (T1). All video streams are available for viewing from a client program or third-party

ONVIF systems. To modify parameters that affect a particular IP Video stream from the camera, click the link.
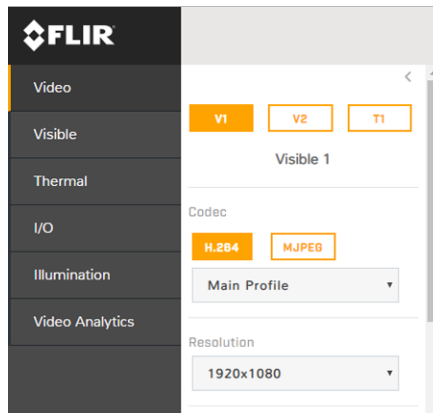
Visible 1

The default parameters provide a 1920x1080, 30 FPS frame-rate stream. Codec options are H.264 or MJPEG.

Visible 2

The default parameters provide a 1280x720, 15 FPS frame-rate stream. Codec options are H.264 or MJPEG.
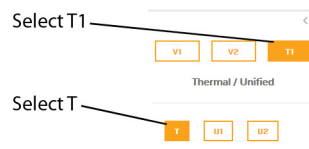
Thermal/Unified

Options for the T1 stream are a 960x360 thermal image (T), a 960x720 unified image (U1), or a 1020x760 unified image (U2); default frame-rate is 10 FPS. Codec options are H.264 or MJPEG.
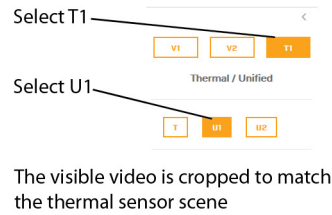
On the Saros Cloud Web Application, the T1 stream only supports a 960x360 thermal image (T) and the H.264 codec. It does not allow you to set the T1 stream to U1/U2 or the codec to MJPEG.
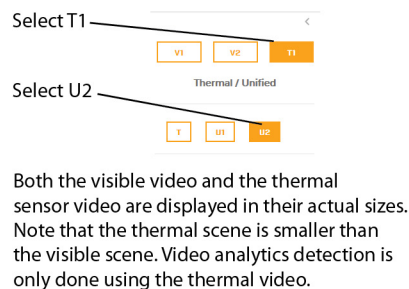
Select Format for the T1 Stream

Thermal only

This document does not contain any export-controlled information.

Unified 1

Select T1

Select U1

The visible video is cropped to match the thermal sensor scene

Thermal / Unified

rtsp://192 168.0.250:554/ch2

Unified 2

Select T1

Select U2

Thermal / Unified

Both the visible video and the thermal sensor video are displayed in their actual sizes. Note that the thermal scene is smaller than the visible scene. Video analytics detection is only done using the thermal video.

rtsp://192.168.0.250:554/ch2

Codecs, Quality, and Bandwidth

The codec used determines which parameters you can set that have a significant impact on the quality and bandwidth requirements of the video stream. Use the default values initially, and then individual parameters can be modified and tested incrementally to determine when bandwidth and quality requirements are met.

With the H.264 codec, you can set Rate Control to:

- CBR (constant bit rate): The Bit Rate parameter defines the target bit rate; the camera attempts to keep the video at or near the target bit rate.
- VBR (variable bit rate): The Bit Rate parameter defines the average bit rate.

The I-Frame Interval parameter controls the number of P-frames used between I-frames. I-frames are full frames of video and the P-frames contain the changes that occurred since the last I-frame. A smaller I-Frame Interval results in higher bandwidth (more full frames sent) and better video quality.

Operation

A higher I-Frame Interval number means fewer I-frames are sent and therefore results in possibly lower bandwidth and possibly lower quality.
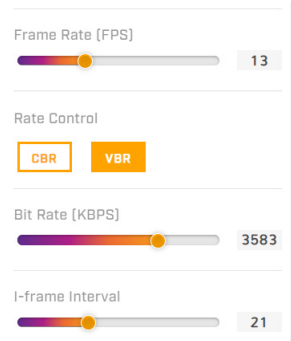
With the MJPEG codec, you can set the Quality parameter.

Network Options

By default, multicast is enabled. Multicast video packets are shared by streaming clients. Additional clients do not cause bandwidth to increase as dramatically as with unicast. Video stream requests for ch0/stream1 are unicast. Client-specific multicast requests vary according to the client.

Visible 1   Visible 2   Thermal/Unified 1
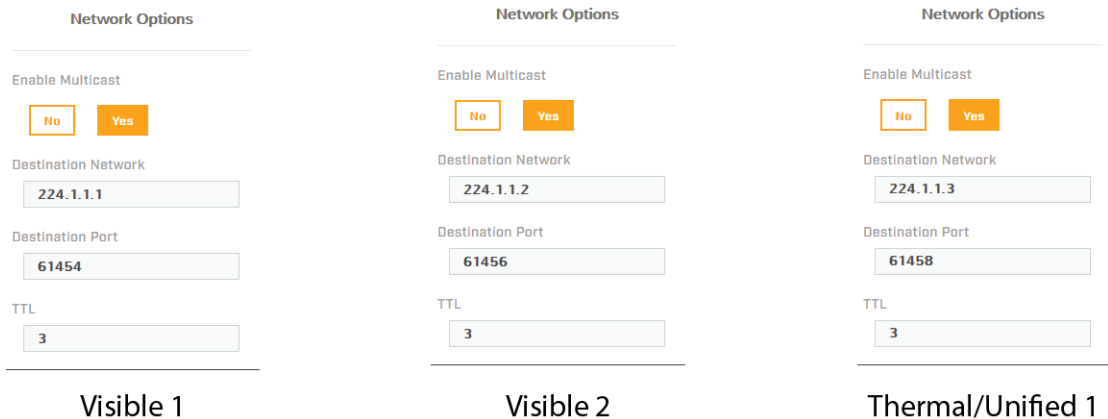
If more than one camera is providing multicast streams on the network, make sure the Destination Network/IP address is unique for each camera (the Destination Port can be reused). By default, the port assignment is unique per stream.

The time-to-live field controls the ability of IP packets to traverse network boundaries. A value of 1 restricts the stream to the same subnet. Greater values allow increasing access between networks.

The video streaming is done using a protocol generally referred to as Real-time Transport Protocol (RTP), but there are actually many protocols involved, including Real-Time Transport Control Protocol (RTCP) and Real Time Streaming Protocol (RTSP). The complete connection strings are: rtsp://192.168.0.250:554/stream1 for Visible 1, rtsp://192.168.0.250:554/stream2 for Visible 2, and rtsp://192.168.0.250:554/stream3 for Thermal/Unified 1

By default the video stream uses the IP address of the camera. To maintain compatibility with legacy systems the stream names are aliased as: ch0 = stream1, ch1 = stream2, and ch2 = stream3.

Authentication is required when logging into the camera stream using any of the user/passwords setup by an administrator (admin level login). Refer to Users Page.

2.3.2   Visible Page

After making adjustments to the visible video, click **SAVE** or **RESET**. When reset is selected you will be given the choice to discard the changes or return to factory defaults. Scroll down to open the Advanced Settings dialog.

Thermal sensor detection region
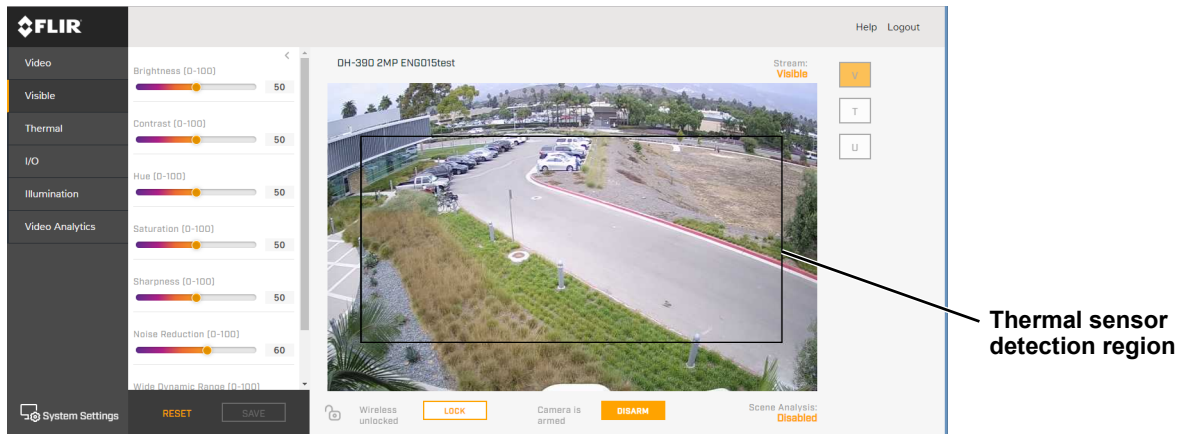
Advanced Settings

- **Focus**

- **Night Mode**

- **Video Format**
  When mounted indoors, the visible camera shutter speed may be synchronized to the 50 Hz or 60 Hz power used for lighting the scene. If lighting is connected to 50 Hz power, the PAL setting may provide better video and conversely, NTSC may provide better video under 60 Hz lighting.
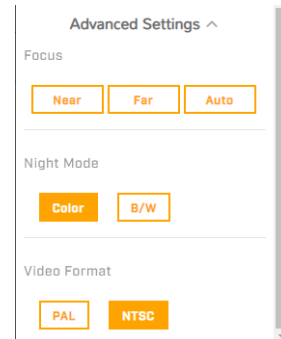
### 2.3.3   Thermal Image Setup - Thermal Page

In most installations it is not necessary to change the default settings of the thermal sensor. However in some situations, depending on weather, time of day, or scene, it may be useful to make changes to the video image to enhance the image by modifying one or more parameters. Be aware that when the conditions change the camera may need to be adjusted again; it is also a good idea to know how to restore the factory default settings.

Note

The Video Analytics detection is performed on video frames directly from the thermal sensor before any adjustments such as AGC are made. The AGC and other adjustments are made only to the thermal video streams and do not have an effect on Video Analytics.

AGC ROI

The region of interest (ROI) determines what portion of the image is used by the Automatic Gain Control (AGC) algorithm to make adjustments to the IR sensor parameters. By default all of the pixels in the image are considered; in some cases it may provide an improved image if a portion of the image is excluded. For example, the sky is generally very cold, so if the ROI excludes the sky it may add more contrast to the rest of the image. A pull-down list offers some convenient options.
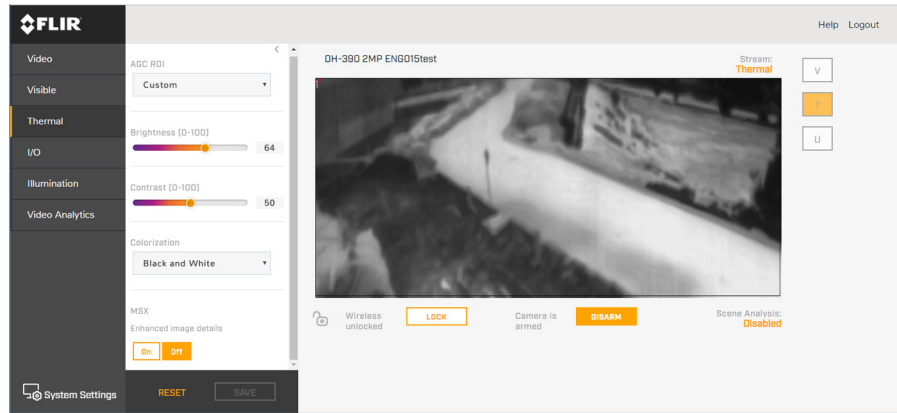
A handle is shown in the corner of the ROI.

Drag the handle to change the size of the ROI box.

Drag the ROI box over the portion of the scene that will control the AGC.

AGC

The AGC parameters control how the overall video image appears. Manual adjustments to the Brightness and Contrast, in some cases may provide a more appealing image, depending on personal preferences.

- **Brightness** (gamma) setting determines the allocation of the 256 "shades of gray" produced by the AGC. Values above 50 allocate more shades of gray to hotter objects, while values below 50 allocate more shades of gray to lower temperature objects. Range 0 to 100.

- **Contrast** (Max Gain) can be used to increase contrast, especially for scenes with little temperature variation (it may also increase noise due to increased gain). Range 0 to 100.

- **Colorization** palette provides a different representation of the detected levels of thermal energy as colors or gray-scale values. White hot and black hot are gray scale palettes; other palettes assign different colors to different temperatures.

- **MSX** provides a visible video overlay on the thermal stream to enhance the image. This may be helpful when setting up analytics detection zones.

Click **Save** to store the current settings as power up defaults. To restore the original settings, click **Reset**.

2.3.4 Input/Output (I/O) Page

The I/O Info page shows the status of the I/O signals.

Select Input
Current state
Select idle state
Save

Select Output
Set current state
Select idle state
Set Reset Interval
Save
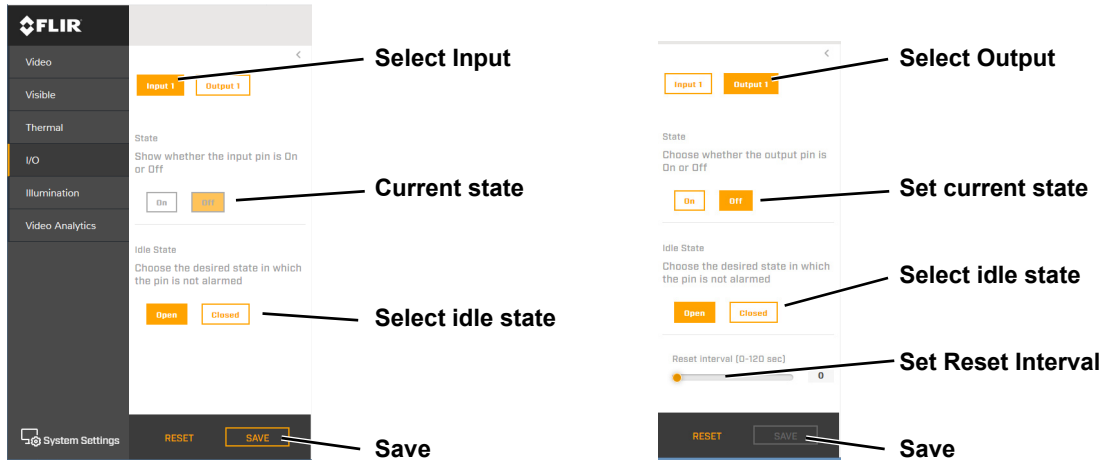
2.3.5 Illumination Page

The camera has both visible and infrared LED lights for illuminating the scene for the visible camera. The Illumination page controls the state of these lights.

The default sets the visible LEDs off, while the infrared LEDs are set to Auto. When Infrared illumination is set to Auto, when the scene is dark enough the Infrared LEDs will turn on and the visible camera will change to Night mode (black and white). Refer to Visible Page.

By default when Analytics detection regions have been configured and trigger an alarm, the visible LEDs will turn on. Refer to Alarm Page to disable this option.

Both lights can not be on at the same time.

Click **Save** to store the current settings as power up defaults.
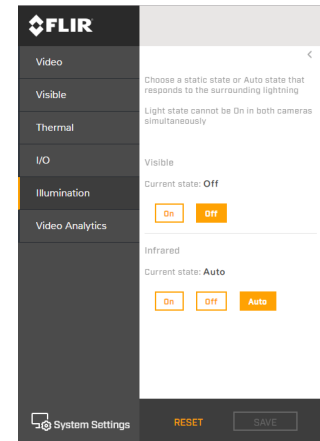
2.3.6 Video Analytics Setup

The Analytics function of the Saros Dome camera provides the capability to detect motion, send an alarm, and classify detected objects based on size and aspect ratio (height and width). Based on these settings, the video analytics calculate a human size that is proportional over the detection area. The vehicle size is extrapolated from the human size. If a detected object matches these parameters, a box will be labeled either H for human or V for vehicle.

Use the Video Analytics page to create motion detection areas, tripwire lines, or masking regions—up to four of each. Each detection area or tripwire has independent detection properties (such as detecting a vehicle or human sized object). Each area/tripwire is assigned an Alarm ID number (1 to

8) based on the order in which they are created and the available IDs. If an area is deleted, its Alarm ID will be available for reuse.
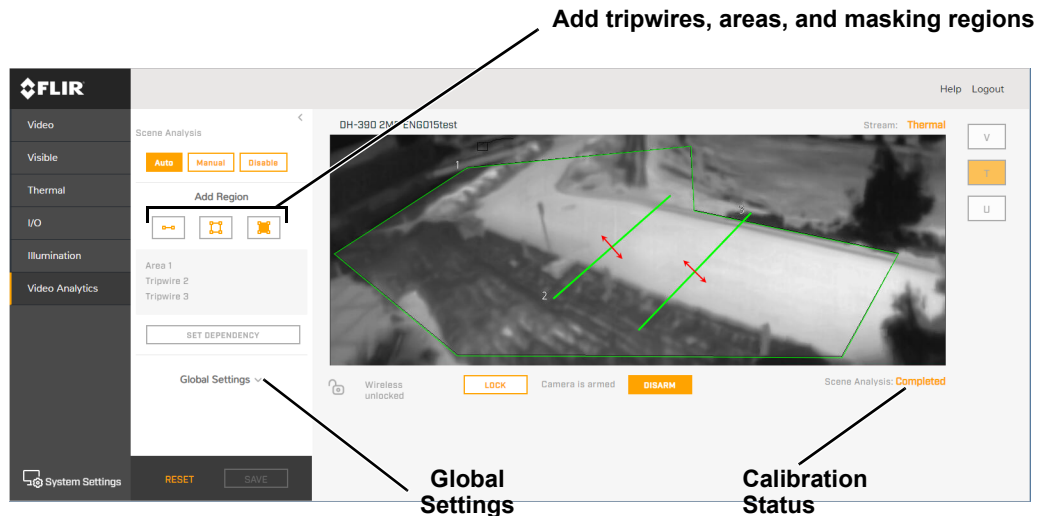

Figure 2-1: Video Analytics Page

Analytics Calibration

Analytics calibration consists of:

Step 1   Making sure the camera is mounted in its final location and properly aimed.

Step 2   Defining masking regions.

Step 3   Calibrating the scene in the field of view using either the auto or manual calibration.

Step 4   (Optional) Set up detection areas and tripwires.

Step 5   Verify that the analytics detect and classify objects as expected.

Analytics calibration and recalibration can be performed using:

- The FLIR InstallerApp: See the relevant FLIR InstallerApp user guide (Android or iOS).
- The camera's web page: Described below.
- The Saros Cloud Web Application: Described below, with a similar interface. The camera must be onboarded to the FLIR Cloud (see Cloud Page).

Auto Calibration

If the scene is well ordered and without random motion from things such as trees, shrubs, or small animals, and access is limited to people (the calibration target), then Auto calibration is a good choice. Auto calibration adjusts the detection size parameters as people (the calibration target) are detected walking in all areas of the scene. The progress of the auto calibration status is shown as a percent Scene Analysis.

To aid scene analysis, mask regions of the scene that contain moving bushes or branches, as well as areas that are not on the same ground plane as the detection areas.
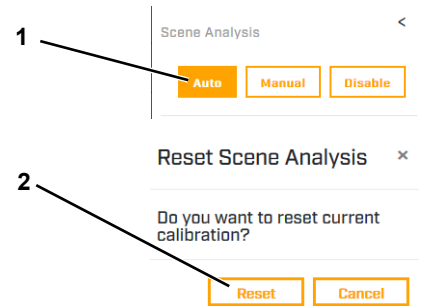
Operation

Calibrate Analytics

After setting up masking regions, calibrate the scene.

Step 1   Have people walking through the detection region at various distances when you start Auto scene analysis.


Step 2   Click **Reset**. The camera automatically analyzes the depth of the FoV based on the people walking in the scene. Be sure to have target people walking along the entire vertical axis of the FoV and along diagonals until scene analysis is completed.

Step 3   After calibration is complete, set up detection areas and check calibration. Refer to Global Settings, Creating Analytics Regions, and Check Calibration.

Manual Calibration

Step 1   On the camera's **Video Analytics** web page, click **Manual**.
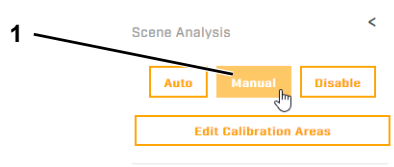
Step 2   Click **Edit Calibration Areas** for the Calibration mode.
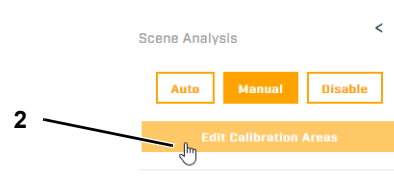
Step 3   Set the far size aspect ratio for a person. Have a person walk around near the center of the area. Select the blue box at the top of the screen and drag to fit the subject. Set the size of the box to the smallest aspect of the thermal image of the subject person.
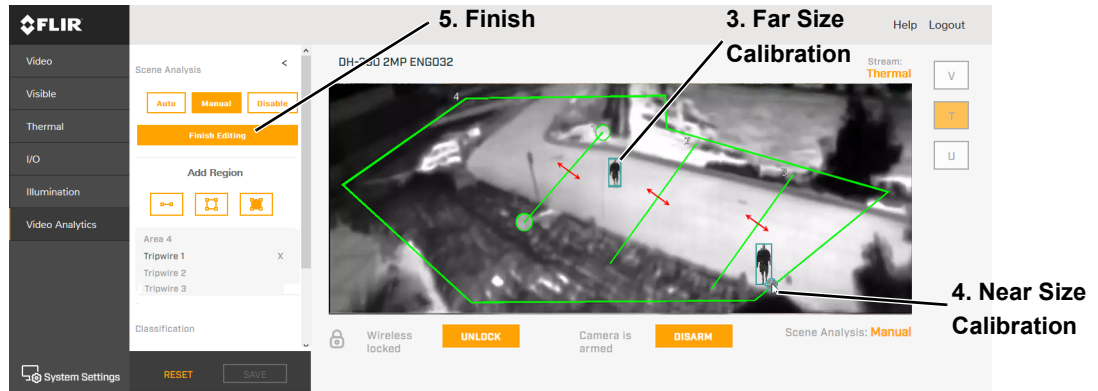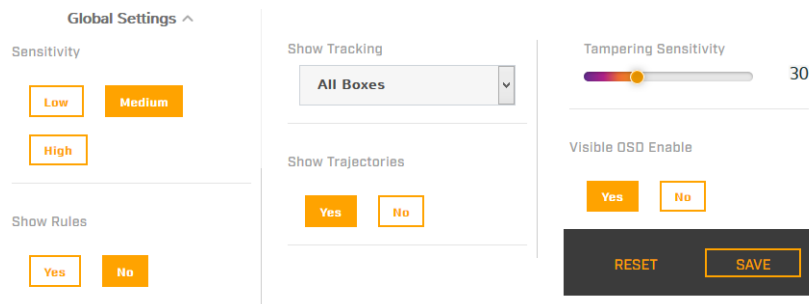

Figure 2-2: Manual Calibration

Step 4   Set the near size aspect ratio for a person. Have a person walk around closer to the camera. Select the blue box at the bottom of the screen and drag to fit the subject.

Step 5   Click **Finish Editing**.

Check calibration. Refer to Global Settings, Creating Analytics Regions, and Check Calibration.

Global Settings

There are three settings for sensitivity which control the threshold for detection (as well as false alarms): Low, Medium, and High. When set to low, the analytics will detect fewer objects (also fewer false alarms) than when set to high.

Set Show Rules to Yes to show any detection areas as black outlines and tripwires as black lines in the thermal video streams.

There are four tracking display options: No Boxes, Classified Boxes, All Boxes and Show Triggered. If Classified, All, or Show Triggered is selected, a check box, Show Trajectories, is displayed that when selected enables a tracking line with each detection box.

- **All Boxes**—every detected motion is shown with a box around it.
- **Classified Boxes**—detected motion classified as vehicle, human, or object of interest is shown with a box around it labeled "H", "V", or "O".

- **No Boxes**—detected motion is not shown with a box.
- **Show Triggered**—detected motion is shown with a box around it when it triggers an alarm.
- **Show Trajectories**—shows the track of an object based on its position from prior frames. This helps to visually represent speed and direction of motion (not available if No Boxes is selected).
- **Tamper Sensitivity**—enables the camera to alarm with tampering such as blocking, paint-spraying, or obscuring the lens. The higher the value; the greater the sensitivity. The camera interprets such events as ONVIF "Bad Video" and can react by sending ONVIF notifications. After 24 hours of constant operation (no reboot or power cycle) with Video Analytics enabled, the camera system will generate the reference files used in Tampering detection. Thus for the first 24 hours of operation, no Tampering event will be triggered. Also, if a reboot or power cycle occurs, it will take another 24 hours to again generate the reference files.

When Show Rules is set to Yes, set Visible OSD Enable to Yes to show detection areas in the visible video streams.

When done, click **Save**.

Creating Analytics Regions

To create a detection rule, click an **Add Region** icon and then click on the video to place the corners that define the detection area.

- With Tripwire selected, click in the video to create the first point of the line. Continue to the second point (and more if desired), then double-click to complete the line.
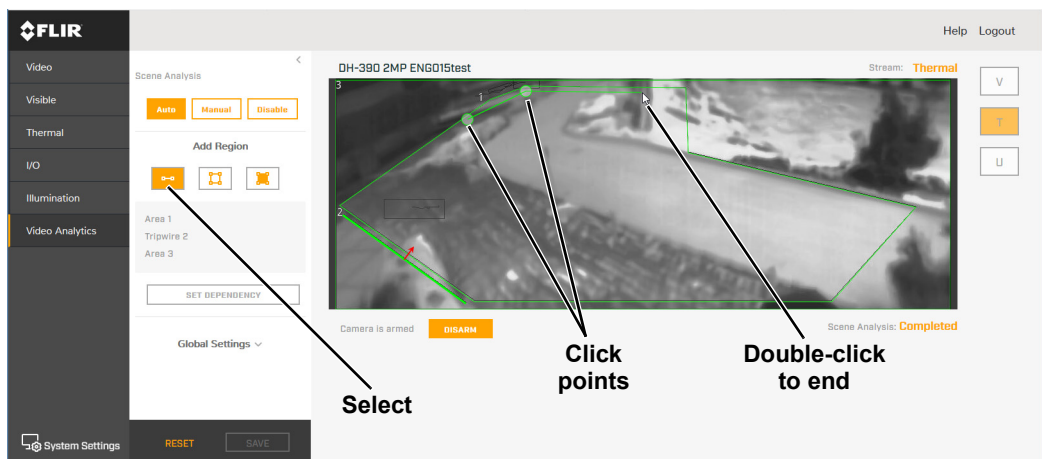

Figure 2-3: Creating a Tripwire

Operation

- Select the newly created region to configure the direction and detection classification specific to this region. Once the parameters are set, scroll down and click **Save**.
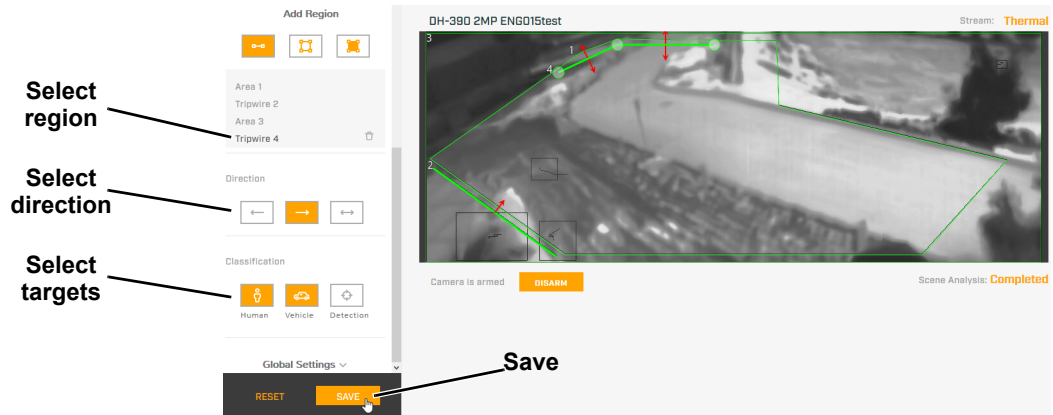

Figure 2-4: Finishing a Region

Note

> The direction (left or right) for an alarm over a tripwire line is controlled by both the properties of each tripwire and the direction in which the line was originally drawn. A direction to the right is to the right of a person moving from the first point to the second point of the line, etc.

- With Detection area selected, click in the video to create the first corner of the area. Continue adding corners (up to 16), then double-click to complete the area. Select the newly created region to configure the detection classification specific to this region. Once the parameters are set up properly, scroll down and click **Save**.

- With Masking area selected, click in the video to create the first corner of the area. Continue adding corners (up to 16), then double-click to complete the area.
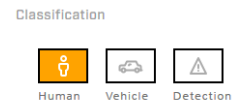
Note

> This is motion detection masking; not privacy masking. The video image will still be seen, but alarms will not be generated. Analytics will be disabled in the masked area. The purpose is to manually define regions that will not generate motion alarms. For example, this can be helpful to eliminate alarms from a tree or bush moving in the wind.

Check Calibration

Step 1   Ensure camera is armed.

Step 2   Click **Yes** for Show Rules.

Step 3   Set Show Tracking to **Classified Boxes**.

Step 4   Click **Yes** for Show Trajectories.

Step 5   Click **Save**.
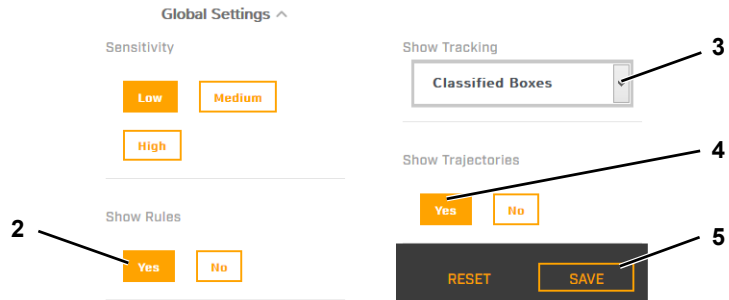
Step 6   Have subjects (person, car, truck, etc) enter the area or cross the tripwire at various distances from the camera. The boxes should be classified correctly and the direction across tripwires should be as expected.

The image below shows a classified human box in a detection region. The box is white, indicating an alarm condition has occurred.
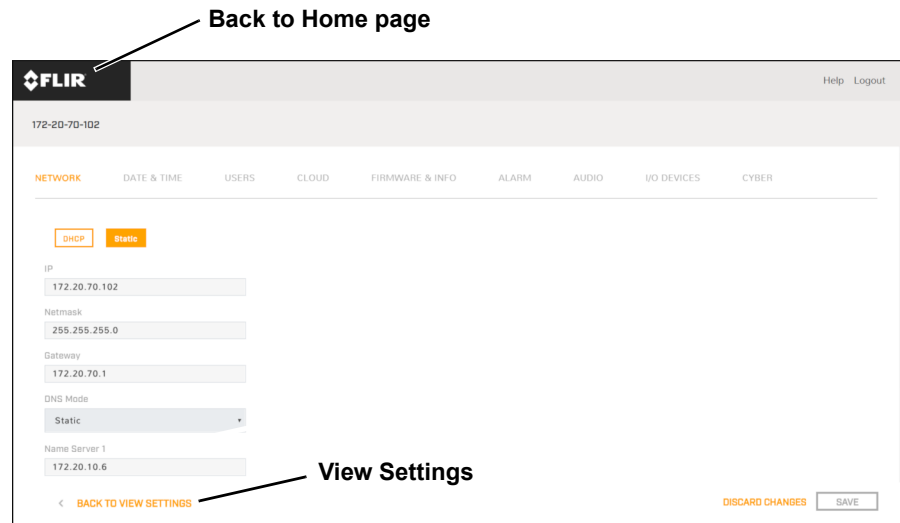
3　Configuration

This chapter describes how to configure the Saros Dome security camera using the camera's web page or the Saros Cloud Web Application.

3.1　System Settings Pages

When a user logs in with expert or admin privileges, the System Settings pages are available. The pages are described below. A login with expert privileges has access to these Server pages, but will only see the security settings for their own login.

3.1.1　Network Page

Set the IP address for the camera. Scroll down to see settings for the Domain Name System (DNS) server. The IP Address mode can be set to DHCP or Static. When set to DHCP, if a DHCP server is not available on the network, the IP address will default to 192.168.0.250. Refer to Configure for Networking to set the address using DNA.

Once the IP address of the camera is changed, the PC may no longer be on the same network and therefore may not be able to access the camera until the IP address on the PC is changed also.

3.1.2 Date & Time Page

The Date & Time page is used to configure the date and time settings. The date, time, and time zone can be obtained from an NTP server, or can be entered manually. If NTP mode is selected, the NTP server information can be entered.
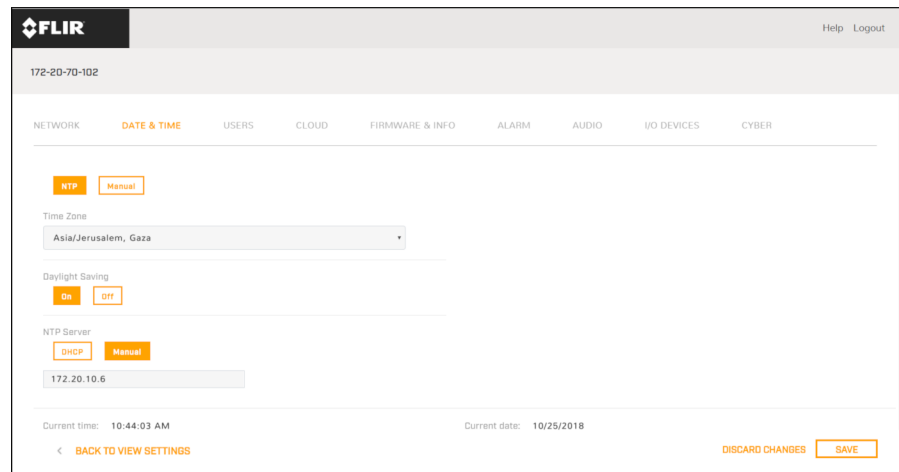
Set the date and time parameters, then click **Save** at the bottom of the page.

When Manual mode is selected, you can select to use the PC time, select and type hour, minute, second, or date values, or select a pop-up window to select a calender date.

After setting the date and time, the camera will require a reboot. A confirmation prompt will appear.
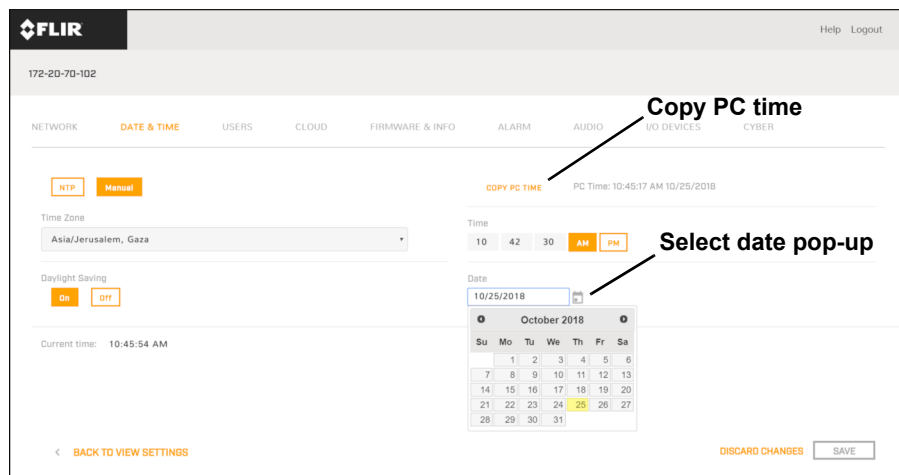
3.1.3 Users Page

Admin level login privileges are required to add users and change or set all passwords.
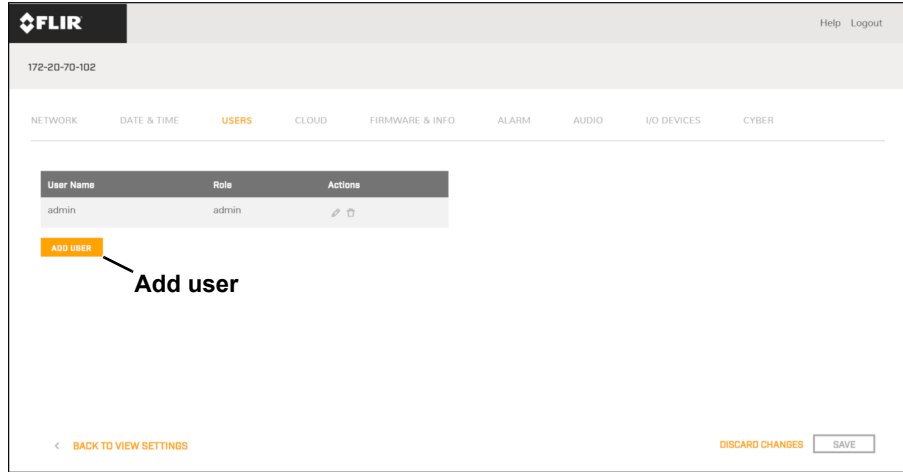
To maintain security of the system, set up User Names and passwords for each required login account.

Three levels of access are provided for each new User Name added to the system.

*   **user**—The user level account can only use the View Settings page and controls.
*   **expert**—The expert level account can use the View Settings page and the System Settings page menus, but can not add/delete user names or change passwords.
*   **admin**—The admin account can use all pages, add/delete user names, and set all passwords.
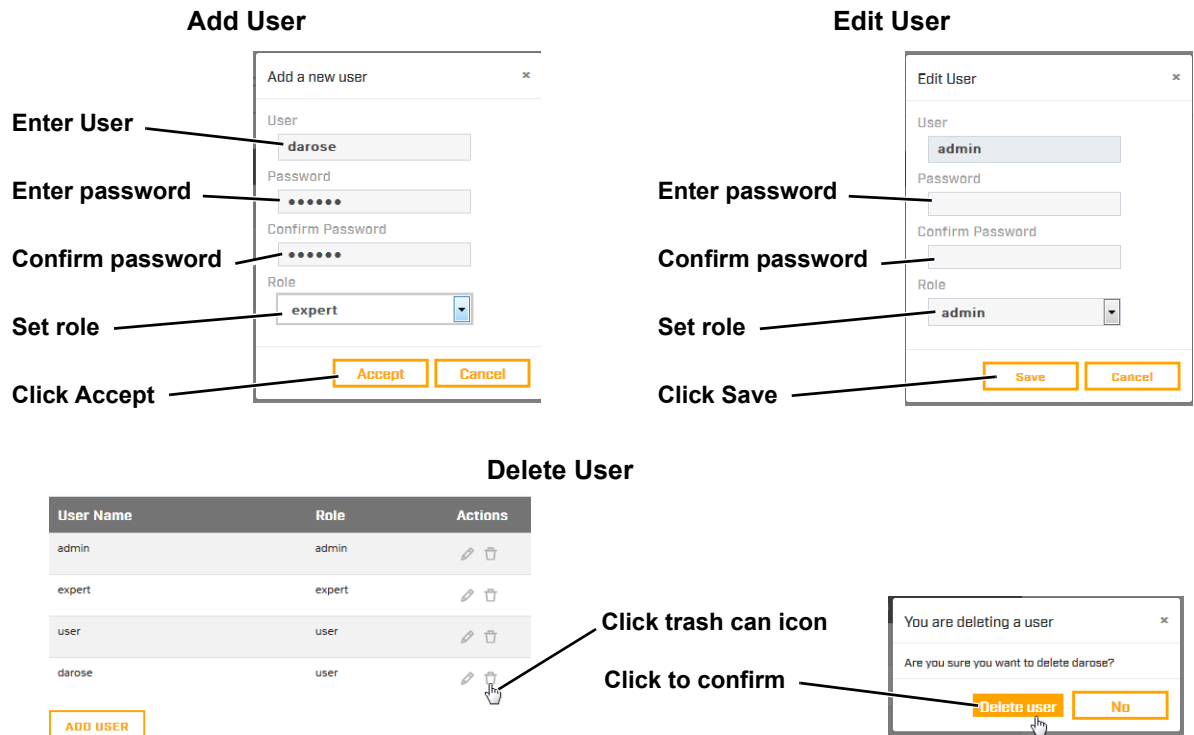
3.1.4 Cloud Page

The Cloud page can be used to onboard to and offboard the camera from the Saros Cloud Web Application, and shows the camera's onboarding status.

3.1.5 Firmware & Info Page

For camera firmware updates, manually install a firmware update file by browsing to select the update file on your computer, and then selecting Upgrade. The firmware files will be uploaded and installed.

Factory Defaults

Click **Full Reset** to return the camera its original factory configuration.

Click **Partial Reset** to maintain network and IP settings while returning all other settings to the factory configuration.

Click **Reboot** to cause the camera to power cycle and reinstall configuration files.

Support System Info

Set the logging details up to four log levels. Including more levels will increase the size of the log file.
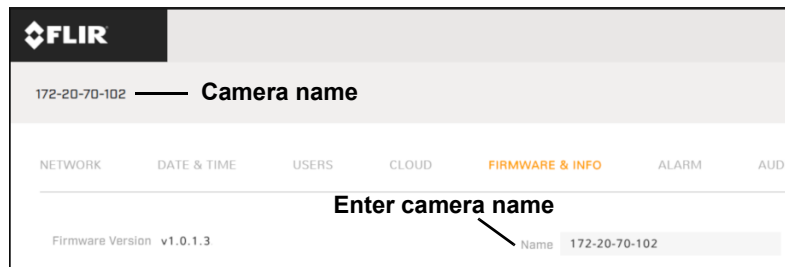
Set the compatibility mode for legacy VMS versions.

Name

Enter a unique, friendly name for the camera, using only alphanumeric characters. The default name for the camera is the camera model followed by the camera's serial number.


3.1.6 Alarm Page

Two default alarms have been provided to react to motion detected in a video analytics region.

- **Visible LED on Motion**—When a alarm is triggered by the video analytics, the visible LEDs are turned on. Enabled by default.
- **Output on Motion**—When a alarm is triggered by the video analytics, the system generates an output signal at the I/O connector as well as a virtual output for connected VMS systems. Enabled by default.

By default, the Alarm logic can also process an input signal to Arm/Disarm the video analytics detection.

- **Arm/Disarm Analytics with Input**—An input signal on the I/O connector as well as a virtual input from a connected VMS systems can arm or disarm the video analytics. Disabled by default.
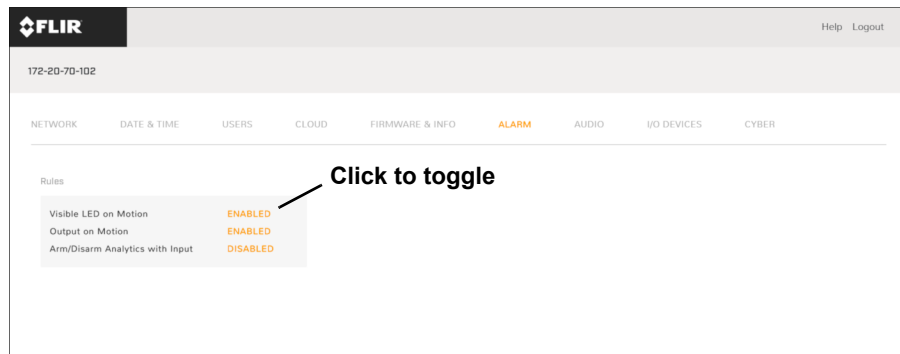
3.1.7 Audio Page

The Audio page provides configuration settings for the camera's audio input and output.
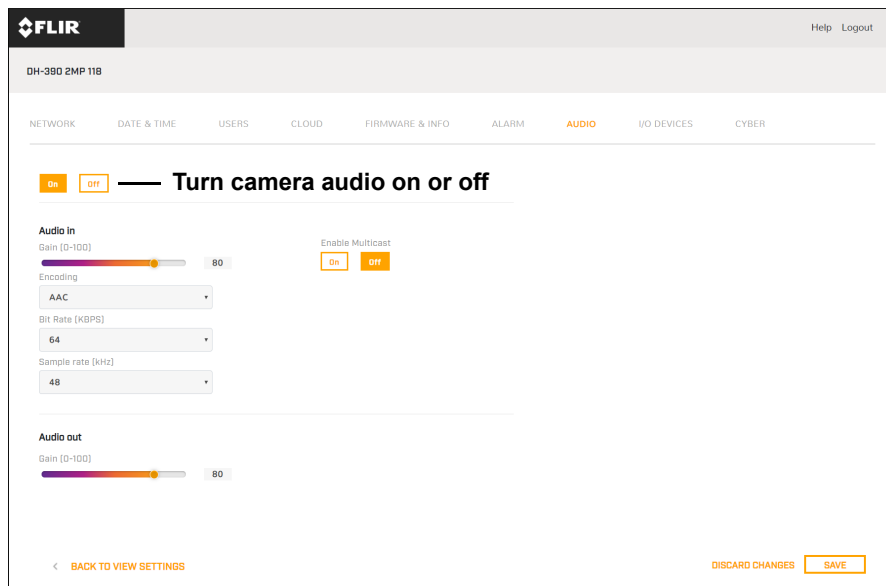
The On/Off buttons affect all audio input and output. Turning audio off immediately turns off all camera audio.

Audio in

When audio is On, you can adjust the following audio input settings:

- **Gain**—You can adjust the audio input gain from 0-100 percent. The default is 80 percent.
- **Encoding**—You can select G.711 or AAC audio input encoding.
- **Enable Multicast**—You can enable multicast streaming of the audio input. When enabled, you can specify the destination network and port, and the time-to-live (TTL).
- **Bit Rate**—With G.711 encoding, the camera supports an audio input bit rate of 64 kilobits per second (kbps). With AAC encoding, you can select 32, 64, or 128 kbps.

Sampling Rate—With G.711 encoding, the camera supports a sample rate of 8 kHz. With AAC encoding, the camera supports a sample rate of 48 kHz.

Audio out

When audio is On, you can adjust the audio line output gain from 0-100 percent. The default gain is 80 percent.

Tip

If you are monitoring the audio IP output with a video stream and change any of the audio configuration settings except gain, restart the stream. For example, if you are monitoring a video stream and turn audio on, you need to restart the stream to hear the audio with the stream.

3.1.8 I/O Devices Page

The I/O Devices page provides configuration settings for virtual I/O devices connected to the camera network. Refer to the documentation for the I/O device connected.

3.1.9 Cyber Page

The Cyber page provides security configuration settings for certificates, TLS/HTTPS, and other services.

Before you can enable TLS/HTTPS, you need to generate or upload a valid certificate. You can:

• Use the camera web interface to generate a self-signed certificate.

• Upload a self-signed certificate.

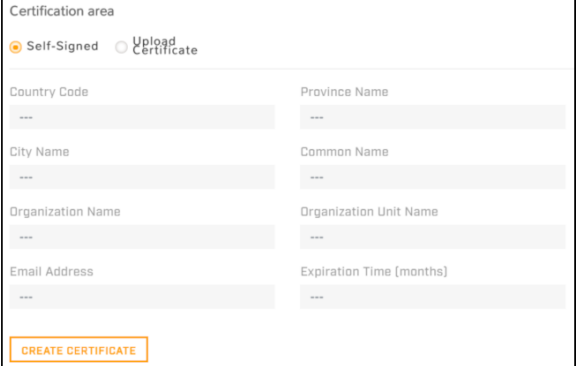• Upload a certificate signed by a third-party.

Certificates and keys must be in PEM format. Common file extensions for TLS files in PEM format are:

- **For certificate and public key files:** *.crt, *.cer, *.cert, *.pem
- **For private key files:** *.key

From the Certificates section of the Cyber page, you can download certificates and keys previously uploaded to or generated by the camera. If the certificate saved on the camera is self-signed, you can download the private and public key files. If the certificate was signed by a third-party CA, you can download the CA Certificate and the private and public key files.

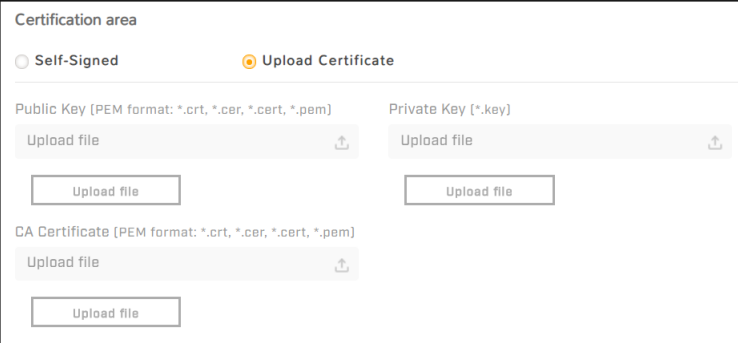**To generate and install a self-signed certificate:**

Step 1   In the Certificates section, under Certification area, select **Self-Signed**.

Step 1   Enter information such as country code, city name, and organization name.

Step 2   Click **Create Certificate**.

Step 3   Allow 15 seconds for the camera to generate the certificate, at which point a confirmation appears.
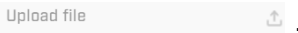
To upload a self-signed or third-party CA signed certificate:

Step 1   Select **Upload Certificates**.

Step 2   If you are uploading a self-signed certificate, under **Public Key** and then under **Private Key**:

    a   Click Upload file.

    b   Select the appropriate key file.

    c   Click Upload file.

    If you are uploading a third-party CA signed certificate, select and upload the **Public Key**, **Private Key**, and **CA Certificate**.

This document does not contain any export-controlled information.

Step 3   Verify that the camera certificate files are valid. Make sure *Certificates are OK* appears under the certificate information. Certificate information appears at the bottom of the Certificates section, under Download certificate.

TLS/HTTPS

Enable or disable camera control using Transport Layer Security (TLS)/secure HTTP (HTTPS).

Enable or disable HTTPS redirect.
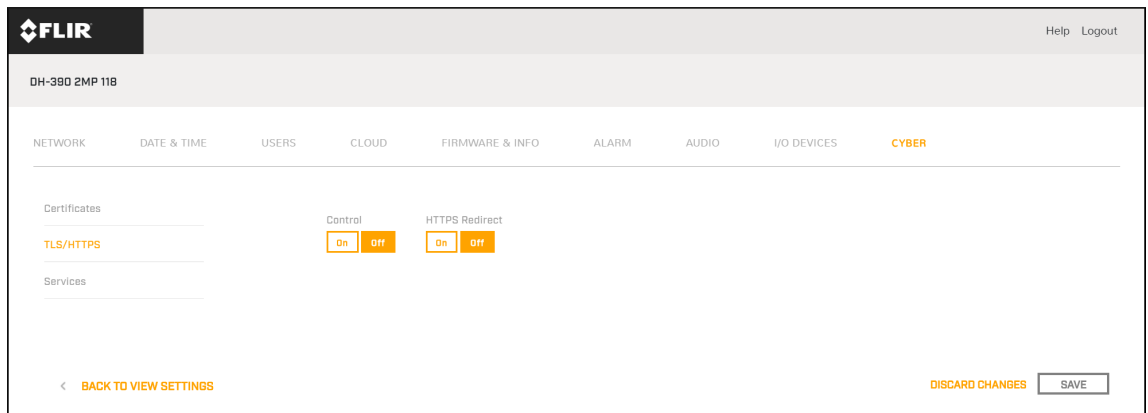
Services

Enable or disable digest authentication for the Nexus CGI control interface. The default setting is On. Changing this setting does not immediately take effect. To apply a change to this setting, click **Save** and then reboot the camera.
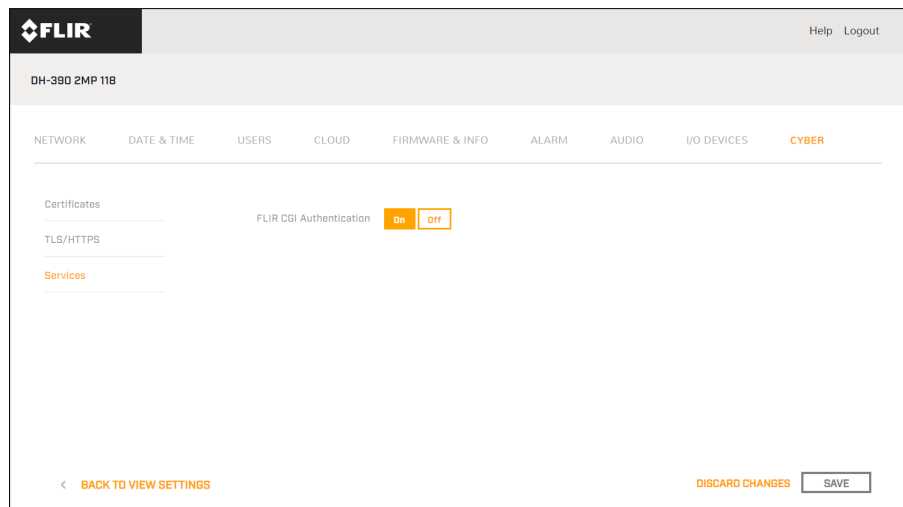
3.2   Maintenance and Troubleshooting Tips

If help is needed during the installation process, contact the local FLIR representative, or visit the FLIR Support Center at: https://www.flir.com/support-center/support-hq/. FLIR Systems, Inc. offers a

comprehensive selection of training courses to help get the best performance and value from the thermal imaging camera.

Find out more at the FLIR training web page: https://www.flir.com/support-center/training/.

3.2.1 Cleaning

Great care should be used with your camera's optics. They are delicate and can be damaged by improper cleaning. The Saros Dome camera lenses and windows are designed for a harsh outdoor environment and have a coating for durability and anti-reflection, but may require cleaning occasionally. FLIR Systems, Inc. suggests that you clean the lens when image quality degradation is noticed or excessive contaminant build-up is seen on the lens.

Note

Do not disturb or move camera during cleaning. The detection analytics on the Saros Dome camera are set and calibrated based on the exact position and camera angle. Inadvertent realignment may require relocation and recalibration of detection regions.

Rinse the camera housing and optics with low pressure fresh water to remove any salt deposits and to keep it clean. If the front window of the camera gets water spots, wipe it with a clean soft cotton cloth dampened with fresh water.

Do not use abrasive materials, such as paper or scrub brushes as this will possibly damage the lens by scratching it. Only wipe the lens clean when you can visually see contamination on the surface.

Use the following procedure and solvents, as required:

- Acetone – removal of grease
- Ethanol – removal of fingerprints and other contaminants
- Alcohol – final cleaning (before use)

Step 1   Immerse lens tissue (optical grade) in Alcohol, Acetone, or Ethanol (reagent grade).

Step 2   With a new tissue each time, wipe the lens in an "S" motion
(so that each area of the lens will not be wiped more than once).

Step 3   Repeat until the lens is clean. Use a new tissue each time.

3.2.2 Troubleshooting

No video

If the camera will not produce an image, check the connections at the camera and at the display. If the connectors appear to be properly connected but the camera still does not produce an image, ensure that power has been properly applied to the camera and the circuit breaker is set properly. If a fuse was used, be sure the fuse is not blown.

If the camera still does not produce an image, contact the FLIR dealer or reseller who provided the camera, or contact FLIR directly.

Performance of thermal sensor varies with time of day

There may be differences in the way the thermal sensor performs at different times of the day, due to the diurnal cycle of the sun. Recall that the thermal sensor produces an image based on temperature differences.

At certain times of the day, such as just before dawn, the objects in the scene may all be roughly the same temperature. Compare this to imagery right after sunset, when objects in the scene may be radiating heat energy that has been absorbed during the day due to solar loading. Greater temperature differences in the scene will allow the thermal sensor to produce high-contrast imagery.

Performance may also be affected when objects in the scene are wet rather than dry, such as on a foggy day or in the early morning when everything may be coated with dew. Under these conditions, it may be difficult for the thermal sensor to detect the temperature of the object itself, rather than of the water coating.

Unable To Communicate Over Ethernet

First check to ensure the physical connections are intact and that the camera is powered on and providing analog video to the monitor.

By default the camera will broadcast a discovery packet two times per second. Use the FLIR Discovery Network Assistant (DNA) or a packet sniffer utility such as Wireshark and confirm the packets are being received by the PC from the camera.

Unable to View Video Stream

If the video stream from the camera is not displayed, it could be that the packets are blocked by the firewall, or there could be a conflict with video codecs that are installed for other video programs.

When displaying video with a VMS for the first time, the Windows Personal Firewall may ask for permission to allow the video player to communicate on the network. Select the check boxes (domain/private/public) that are appropriate for the network.

If necessary, test to make sure the video from the camera can be viewed by a generic video player such as VLC media player (http://www.videolan.org/vlc/). To view the video stream, specify RTSP port 554 and the appropriate stream name. For example:
rtsp://192.168.0.250:554/stream1 for Visible 1,
rtsp://192.168.0.250:554/stream2 for Visible 2, and
rtsp://192.168.0.250:554/stream3 for Thermal/Unified

Authentication is required when logging into the camera stream using any of the user/passwords setup by an administrator (admin level login). Refer to Users Page.

Refer to Network Options for additional information on RTP settings and stream names.

FLIR Systems, Inc.
6769 Hollister Ave
Goleta, CA 93117
USA

Corporate Headquarters
FLIR Systems, Inc.
27700 SW Parkway Ave.
Wilsonville, OR 97070
USA

Support:
https://www.flir.com/support-center/support-hq/

Document:
427-0100-00-12
Revision: 120
Date: August 2019