



PERCEPT

**PERCEPT Body Camera /
Genetec™ Security Center**

Deployment Guide

Document Date: August 14th, 2023

Contents

1	Introduction.....	4
2	Recommended Deployment	4
2.1	Layout	4
2.2	Available Functionalities	6
3	Configuring the PERCEPT Body Camera.....	7
3.1	Deploying Multiple PERCEPT Body Cameras	7
3.2	Configure Networking	7
3.2.1	Configure Cellular.....	7
3.2.2	Configure Cellular Data Usage	8
3.2.3	Configure Wi-Fi Data Usage.....	9
3.2.4	Configure Docking Station(s)	10
3.3	Configure Video	12
3.3.1	Disable orientation metadata	12
3.3.2	Video profiles.....	13
3.4	Setup local recording on the body camera.....	15
3.5	Setup time synchronization	16
3.5.1	Setting NTP in PERCEPT Body Camera	17
3.5.2	Pushing NTP Settings from GSC.....	18
3.6	Create a new dedicated ONVIF user (recommended)	19
4	Configuring VPN	20

4.1	VPN requirements	20
4.2	VPN example	20
4.2.1	Configure L2TP server	21
4.2.2	LAN IP address reservation	22
4.2.3	VPN IP address reservation	24
4.2.4	Configure PERCEPT VPN Settings.....	26
5	Integrating the PERCEPT Body Camera in GSC	27
5.1	Enroll Camera.....	27
5.2	Configure Camera	29
5.2.1	Identity	29
5.2.2	Peripherals	30
5.2.3	Video.....	32
5.2.4	Recording.....	34
5.2.5	Video analytics	35
5.2.6	Panormorph Lens	36
6	Configuring Edge Storage Transfer	37
7	Validating the Integration.....	39
7.1	On-Demand Streaming.....	39
7.2	Live Streaming.....	39
7.3	Edge Storage Transfer	41
7.4	Network Interface Switching	44

1 Introduction

One of the unique features of the IONODES PERCEPT Body Camera is that it is an open platform device, allowing for integration with industry-leading VMS solutions such as Genetec™ Security Center. It implements extensive features of ONVIF profiles G, S and T, along with flexible network configurations (LAN, Wi-Fi, 4G/LTE) for live video and edge recording retrieval.

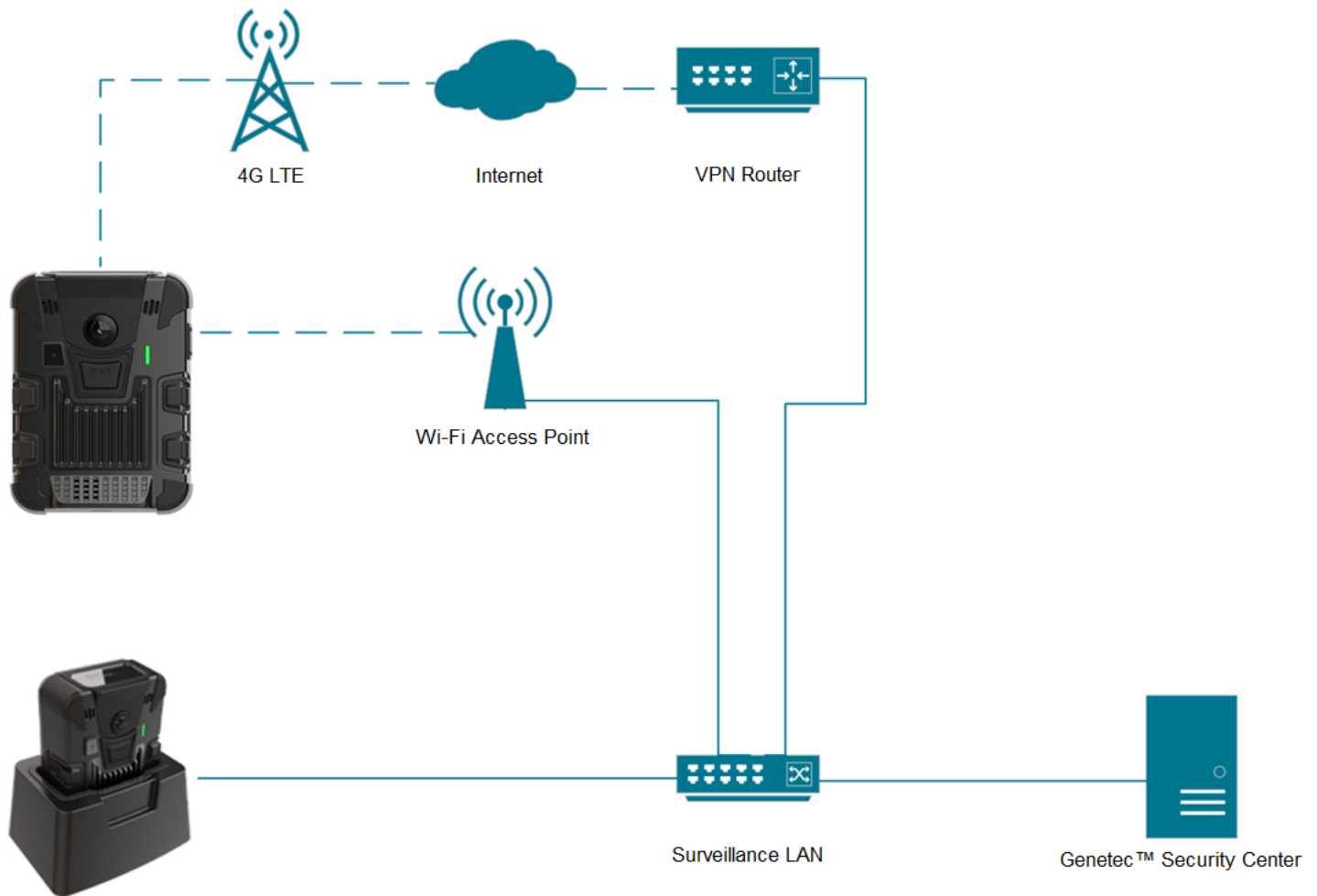
This integration is supported as of IONODES PERCEPT Body Camera firmware 10.7.2.7 and has been validated with Genetec™ Security Center 5.11.3. This document describes the recommended integration deployment as validated by IONODES and a sample scenario is demonstrated to illustrate the various deployment steps. System Integrators and End Users should adjust to their specific needs and system environment.

2 Recommended Deployment

2.1 Layout

A typical deployment scenario, shown in the diagram below, includes the following:

- PERCEPT Body Camera,
- PERCEPT Docking Station,
- Wi-Fi Access Point,
- Virtual Private Network (VPN) server,
- Local Area Network (LAN) infrastructure, and
- Local Video Management Software (VMS), Genetec™ Security Center (GSC)



The PERCEPT Body Camera can technically record directly to GSC through 4G LTE or Wi-Fi streaming, but this is not recommended due to bandwidth constraints. The recommended configuration consists of setting up two (2) video stream settings; an on-demand low-bitrate live stream enabled over 4G LTE and Wi-Fi, and a high-bitrate recording stream saved to the camera's internal storage and later transferred to GSC Archiver via the Docking Station's wired Ethernet.

Note: Although the diagram above shows the Wi-Fi Access Point and Docking Station connected to the LAN infrastructure, these can also connect to the internet. In such a configuration, they reach the LAN infrastructure via the VPN, enabling live video and recording transfer from a remote location with internet access.

2.2 Available Functionalities

The table below summarizes functionalities available with the deployment detailed in this guide.

Functionality	Remark
Low-bitrate Live Audio & Video triggered from Genetec™ Security Desk and Web Client	Live stream on-demand to minimize Wi-Fi/LTE data usage
Two-way audio communication using Genetec™ Security Desk	Known issue with Push-to-talk on some versions of GSC. Contact Genetec Support for update
High-bitrate Audio & Video Recording saved on device Edge Storage (SD card)	
Automatic Edge Storage transfer of Video to GSC Archiver	Audio transfer to GSC Archiver not supported
Date / Time synchronization	With NTP server common to GSC and PERCEPT
Firmware updates from GSC	
Automatic switching between Docking Station, Wi-Fi, and LTE	With VPN server/router
End-to-end Encryption	With VPN server/router

3 Configuring the PERCEPT Body Camera

Start by initializing the PERCEPT Body Camera's network connectivity with GSC via Wi-Fi. Refer to the PERCEPT Quick Start Guide for network initialization instructions.

Note: Instructions in this guide assume the PERCEPT Body Camera's initial state is set to factory default. If the body camera was previously used, it is strongly advised to reset it before integrating it with GSC.

3.1 Deploying Multiple PERCEPT Body Cameras

The PERCEPT Body Camera has multiple configuration settings. To avoid the risk of human error when deploying many cameras, it is recommended to start by configuring and validating a single camera.

Once the configuration is fully validated, the IONConfigTool utility (link [IONConfigTool - IONODES](#)) can be used to export its configuration then import it to other cameras. All configuration parameters are exported/imported except users and credentials, network settings and media at-rest encryption key. These must be re-entered manually after the import.

3.2 Configure Networking

To integrate with GSC, the PERCEPT Body Camera and LAN infrastructure shall be configured for each camera to always obtain the same IP address on all network interfaces; Wi-Fi, Docking Station, and VPN. If the Wi-Fi and Docking Station always connect to the video LAN, setting static IP addresses for these interfaces may be appropriate.

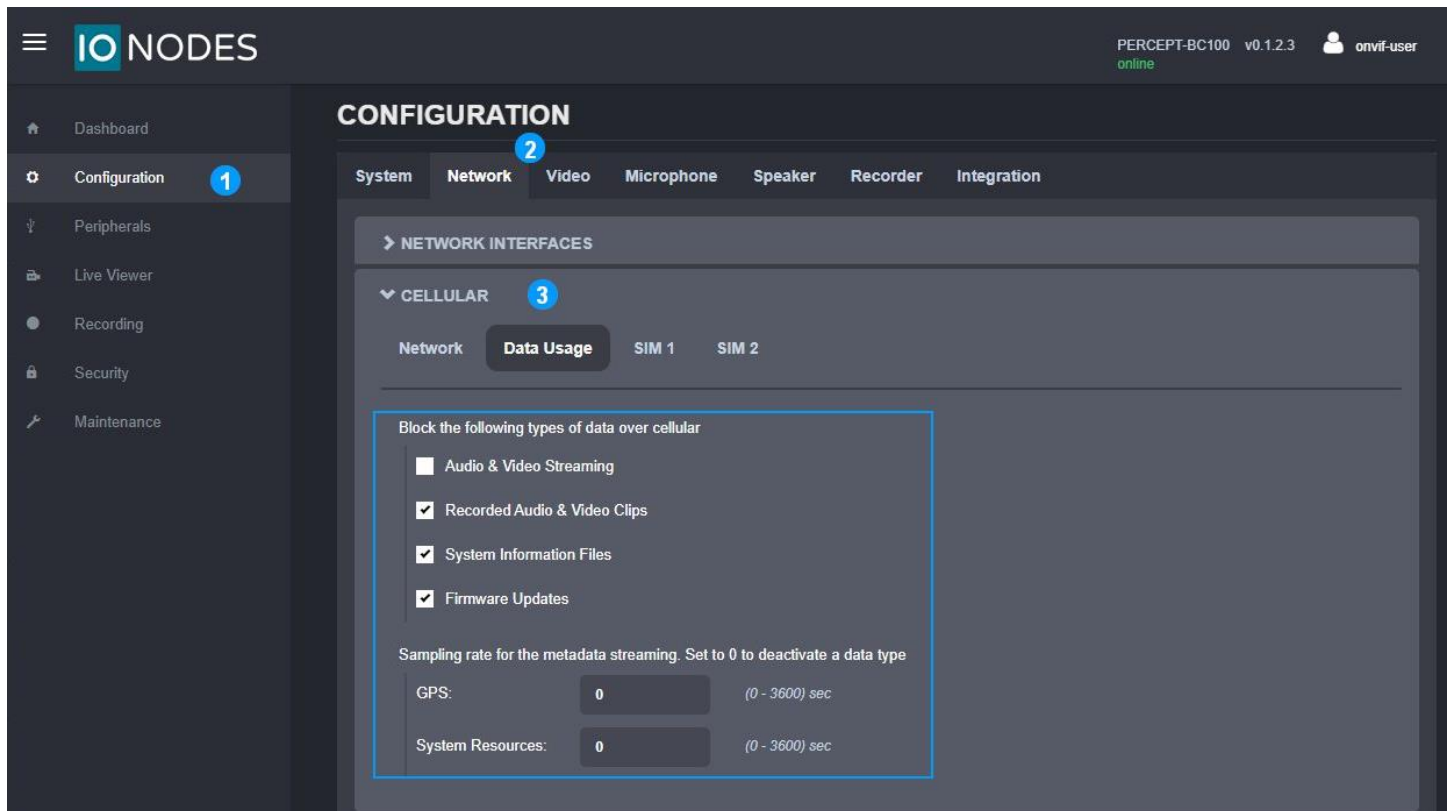
However, static IP addressing can prevent connecting with other networks to access the video LAN via VPN. For that reason, it is recommended to keep the camera's network interfaces to DHCP and configure the VPN router and/or video LAN DHCP server to hand a reserved IP address to each camera. This is further detailed in section 4 below.

3.2.1 Configure Cellular

All PERCEPT Body Cameras include a SIM card that can be activated at any time. Contact your IONODES reseller to activate a data plan.

3.2.2 Configure Cellular Data Usage

To better control data usage, the PERCEPT Body Camera can be configured to block different types of data over cellular links.



1. From the **Configuration** page
2. Select the **Network** tab
3. Expand the **CELLULAR** section and configure parameters in the **Data Usage** tab
 - a. Uncheck **Audio & Video Streaming** to allow live streaming over cellular
 - b. Check **Recorded Audio & Video Clips** to block Edge storage transfer over cellular
 - c. Check **System Information Files** to block troubleshooting log download over cellular
 - d. Check **Firmware Updates** to block firmware upload over cellular
 - e. Set sampling rate to **0** for both **GPS** and **System Resources** to block metadata streaming over cellular

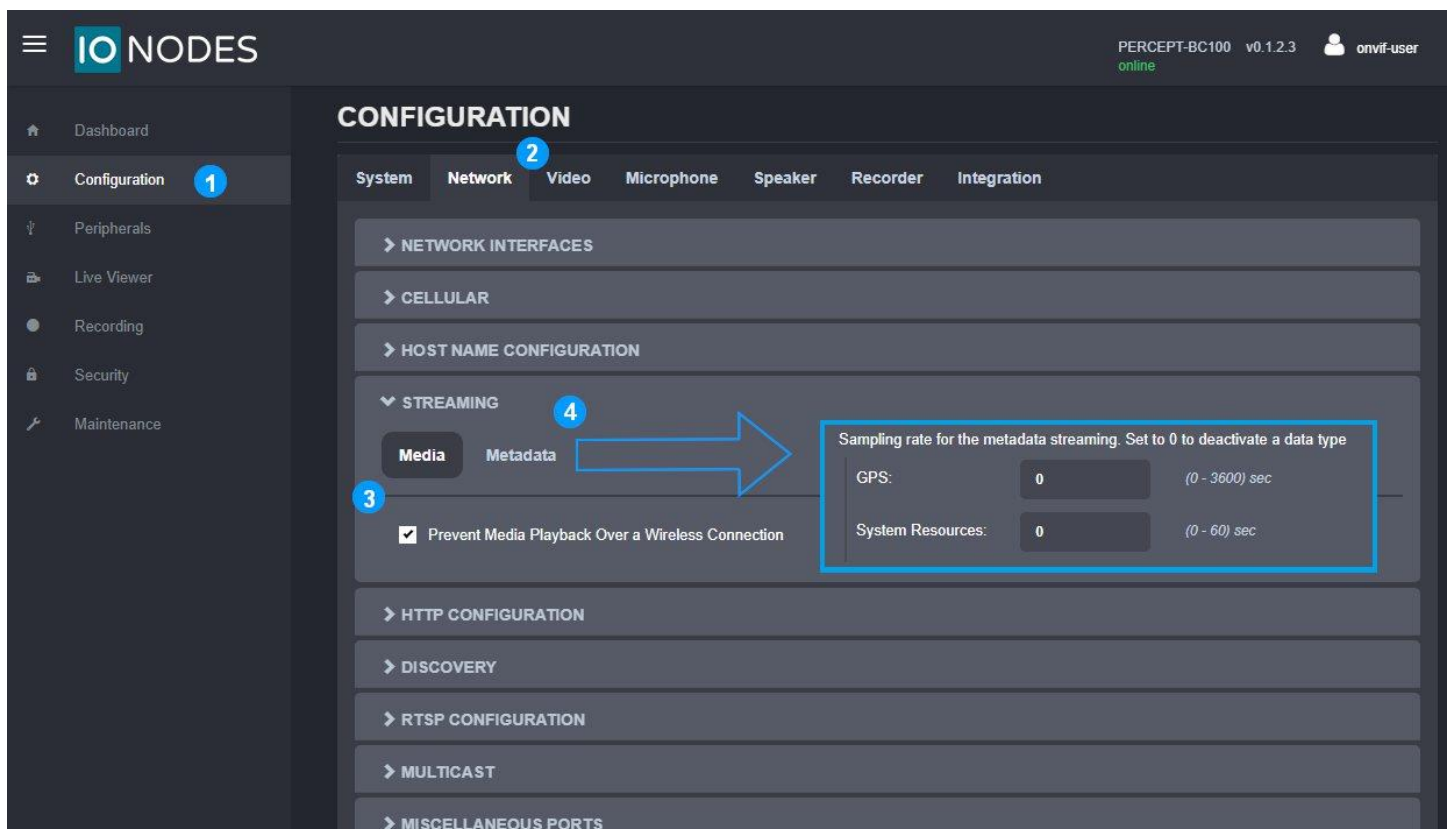
Note: Settings above are intended to keep cellular data to strict minimum to achieve functionalities of this deployment scenario. Other data types can be allowed based on individual use case.

Note: It is recommended to disable metadata because the PERCEPT Body Camera integration with GSC does not currently use it. Future revisions are planned to include use cases for metadata.

3.2.3 Configure Wi-Fi Data Usage

PERCEPT Body Cameras can be configured to block media playback and metadata streaming over Wi-Fi. This impacts Edge Storage transfer since it is achieved through media playback. Playback can take up all the available bandwidth of a Wi-Fi network, especially when multiple camera users return to a central location at the end of a shift.

GSC Archiver can be configured to limit edge storage concurrent jobs and bandwidth, or playback can be disabled over Wi-Fi altogether from the PERCEPT Body Camera Web UI. The latter is recommended when deploying with PERCEPT Docking Stations. Edge storage transfers will be performed exclusively over docking stations' wired Ethernet port.

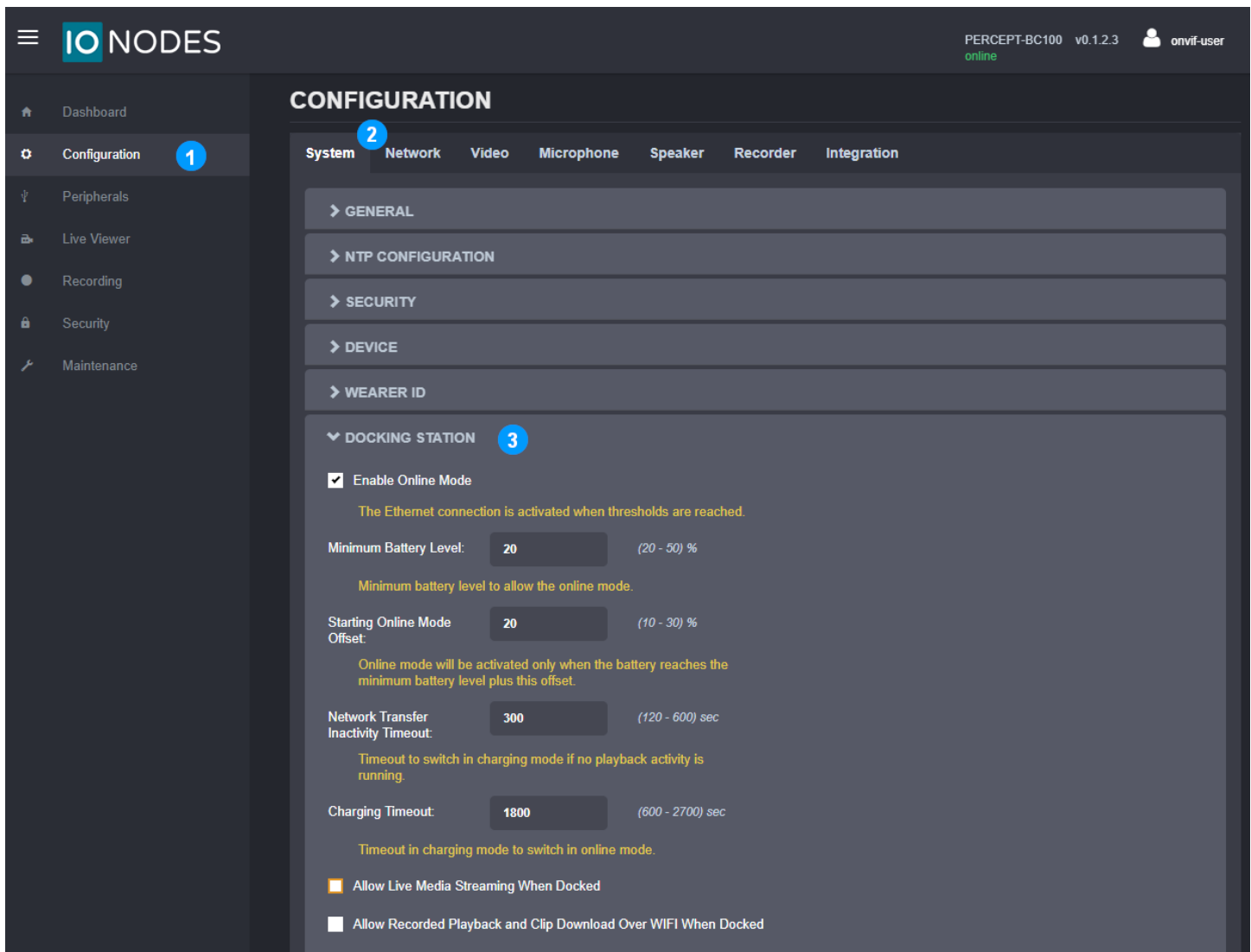


1. From the **Configuration** page
2. Select the **Network** tab

- Expand the **STREAMING** section and check **Prevent Media Playback Over a Wireless Connection** in the **Media** tab
- Select the **Metadata** tab and set both **GPS** and **System Resources** sampling to **0** to disable metadata streaming

3.2.4 Configure Docking Station(s)

When deploying with PERCEPT Docking Station(s). It is recommended to disable live streaming and playback over Wi-Fi when docked.



- From the **Configuration** page
- Select the **System** tab

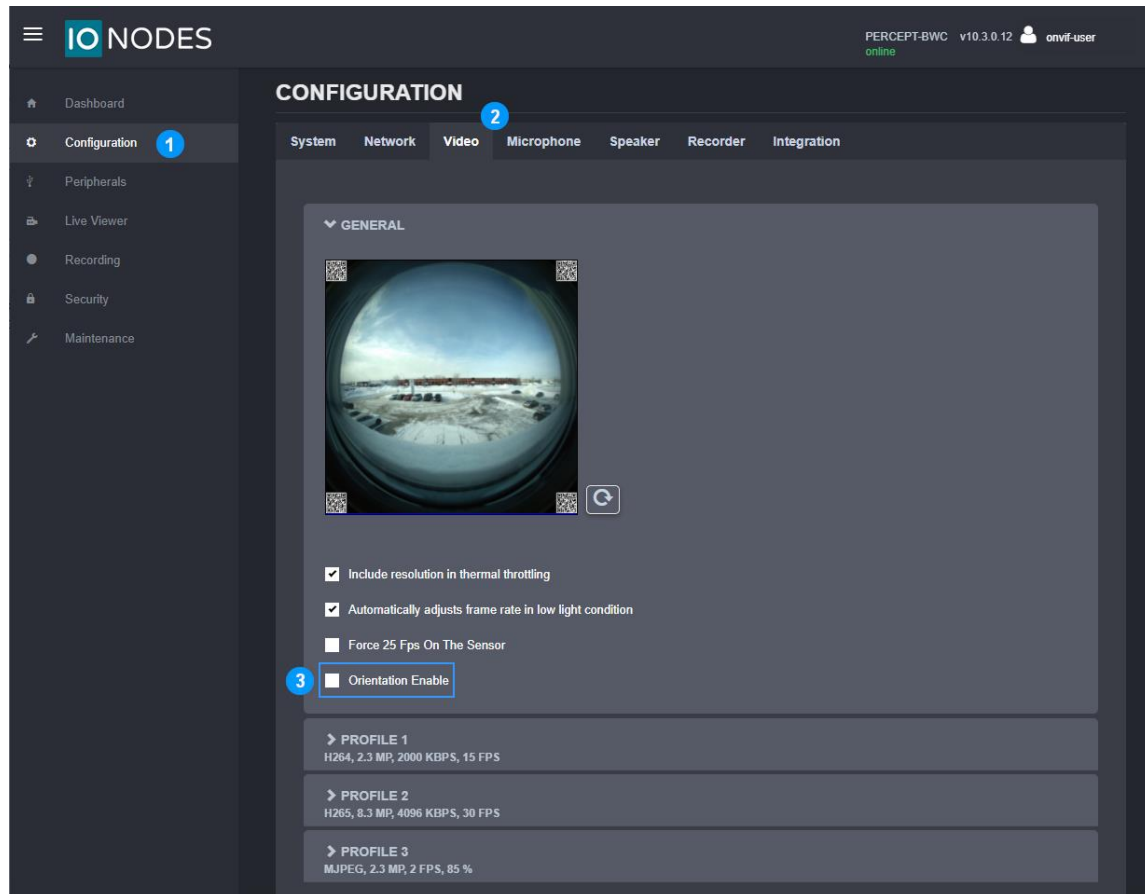
3. Expand the **DOCKING STATION** section and configure parameters as follows
 - a. Check **Enable Online Mode**
 - b. Uncheck **Allow Live Media Streaming When Docked**
 - c. Uncheck **Allow Recorded Playback and Clip Download Over Wi-Fi When Docked**

Note: Edge storage transfer can create bandwidth surges of more than 200Mbps when body cameras start offloading data. Ensure that the network can handle the increased traffic. GSC Archiver advanced settings (Resources->Advanced settings) can be adjusted to limit simultaneous edge storage jobs and throughput based on system scale and capacity.

3.3 Configure Video

3.3.1 Disable orientation metadata

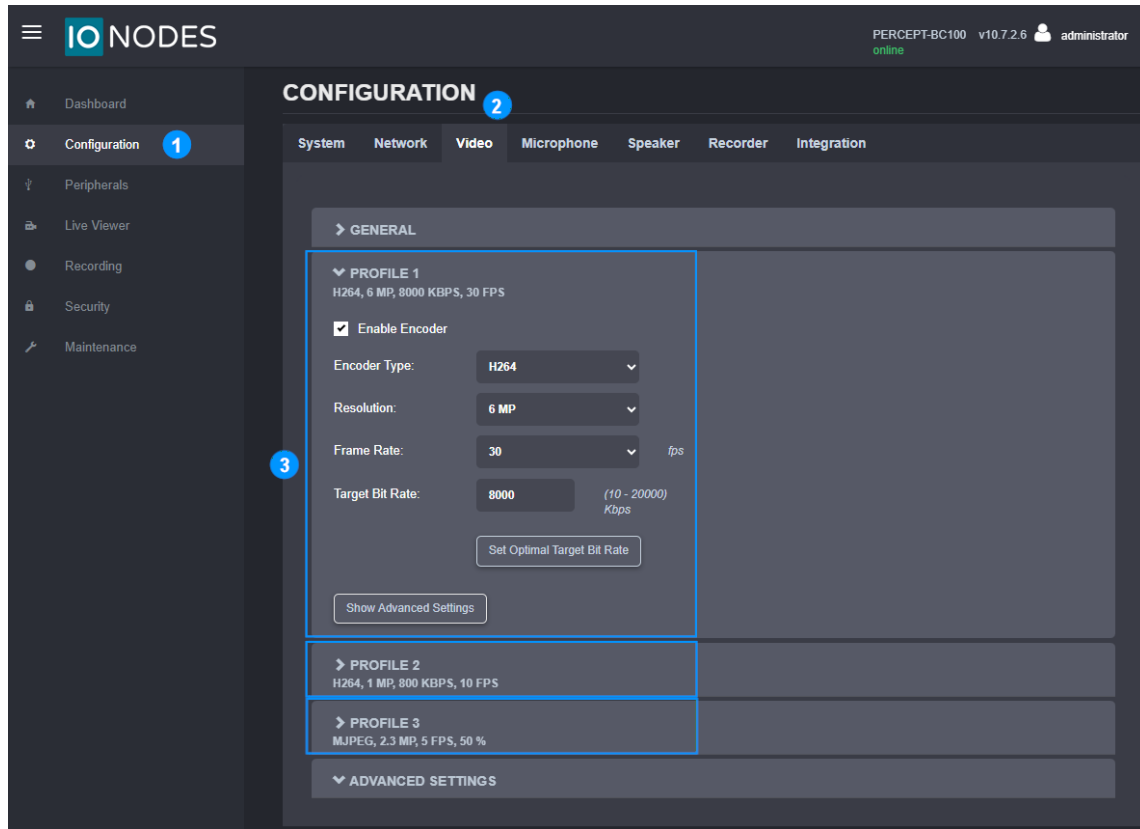
The PERCEPT Body Camera includes orientation metadata used by some client software to stabilize dewarped video. This feature is not supported by GSC and must be disabled in the body camera.



1. From the **Configuration** page
2. Select the **Video** tab
3. Uncheck the **Orientation Enable** box

3.3.2 Video profiles

The PERCEPT Body Camera supports two H.264/265 video encoder profiles and one MJPEG profile. Each profile enabled in the camera will be accessible to GSC.

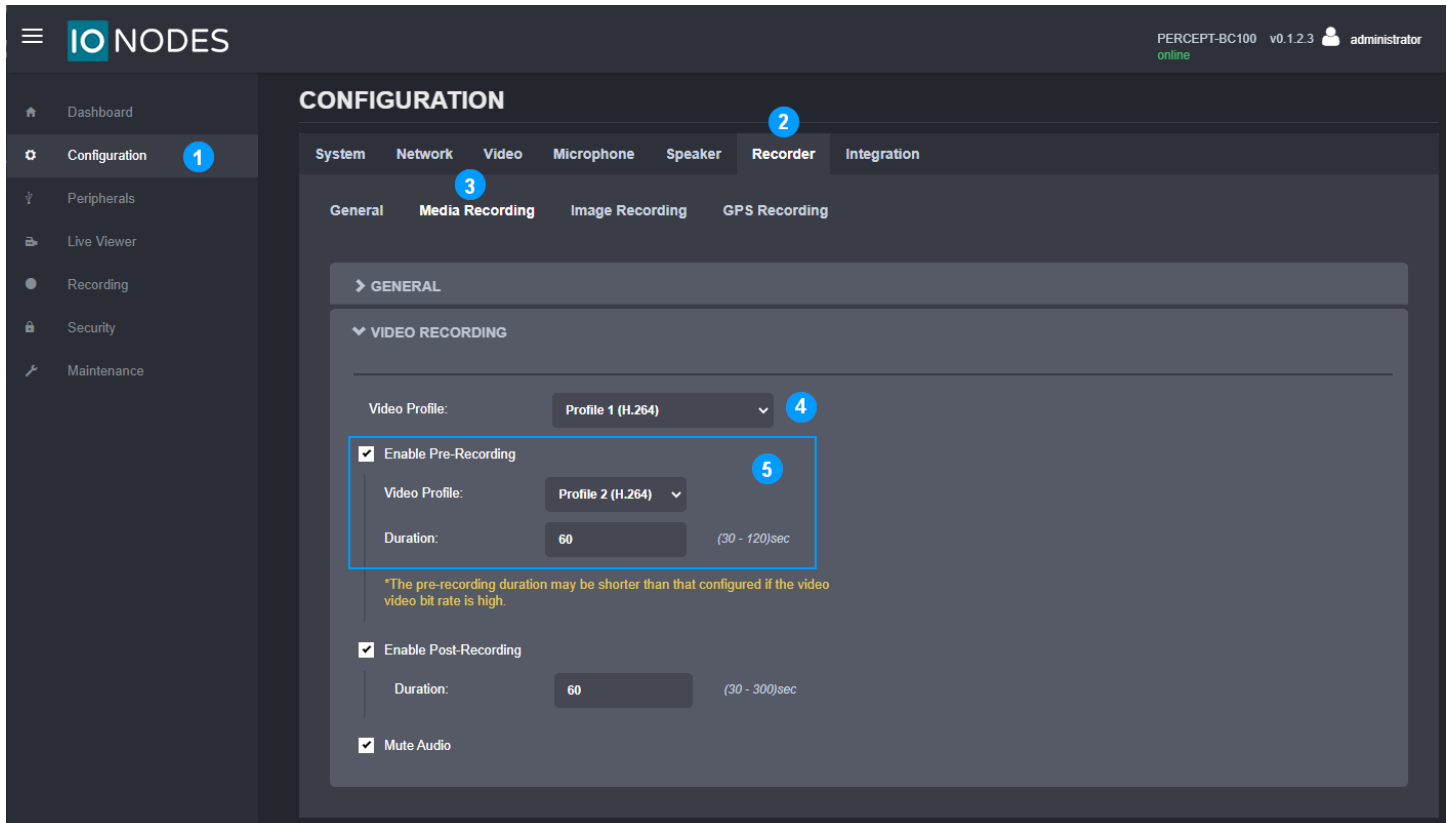


1. From the **Configuration** page
2. Select the **Video** tab
3. Enable and configure each video profile. Recommended settings are:
 - a. PROFILE 1 (Recording Stream):
 - i. **Encoder Type: H264**
 - ii. **Resolution: 6 MP**
 - iii. **Frame Rate: 30 fps**
 - iv. **Target Bit Rate: 8000 kbps**
 - v. **Intra Interval: 240 frames**
 - vi. **Rate Control: Variable Bitrate**
 - vii. **Profile: Main**
 - viii. **VBR Aggressiveness: Moderate**

- b. PROFILE 2 (Live Stream):
 - i. **Encoder Type: H264**
 - ii. **Resolution: 1 MP**
 - iii. **Frame Rate: 10 fps**
 - iv. **Target Bit Rate: 800 kbps**
 - v. **Intra Interval: 30 frames**
 - vi. **Rate Control: Variable Bitrate**
 - vii. **Profile: Main**
 - viii. **VBR Aggressiveness: Moderate**
- c. PROFILE 3 (for PERCEPT Web UI only):
 - i. **Encoder Type: MJPEG**
 - ii. **Resolution: 2.3 MP**
 - iii. **Frame Rate: 1 fps**
 - iv. **Rate Control: Fixed quality**
 - v. **Quality: 50**
 - vi. **Multipart Compliant: Enabled**

Note:	The <i>Encoder Type</i> (codec) and profile's Enabled status are detected by GSC when enrolling the body camera. These settings must therefore be configured in the PERCEPT Body Camera before enrolling it to GSC. Changing <i>Encoder Type</i> requires rebooting the device.
Note:	Once enrolled in GSC, video profile settings such as resolution, frame rate, etc shall be configured from within GSC Config Tool.
Note:	H.264 is recommended for users that intend on viewing streams from Genetec™ Web Client without GSC Media Gateway expending computing resources for transcoding. Video profiles can be configured with H.265 codec if Web Client or transcoding resource limitations is not of concern.

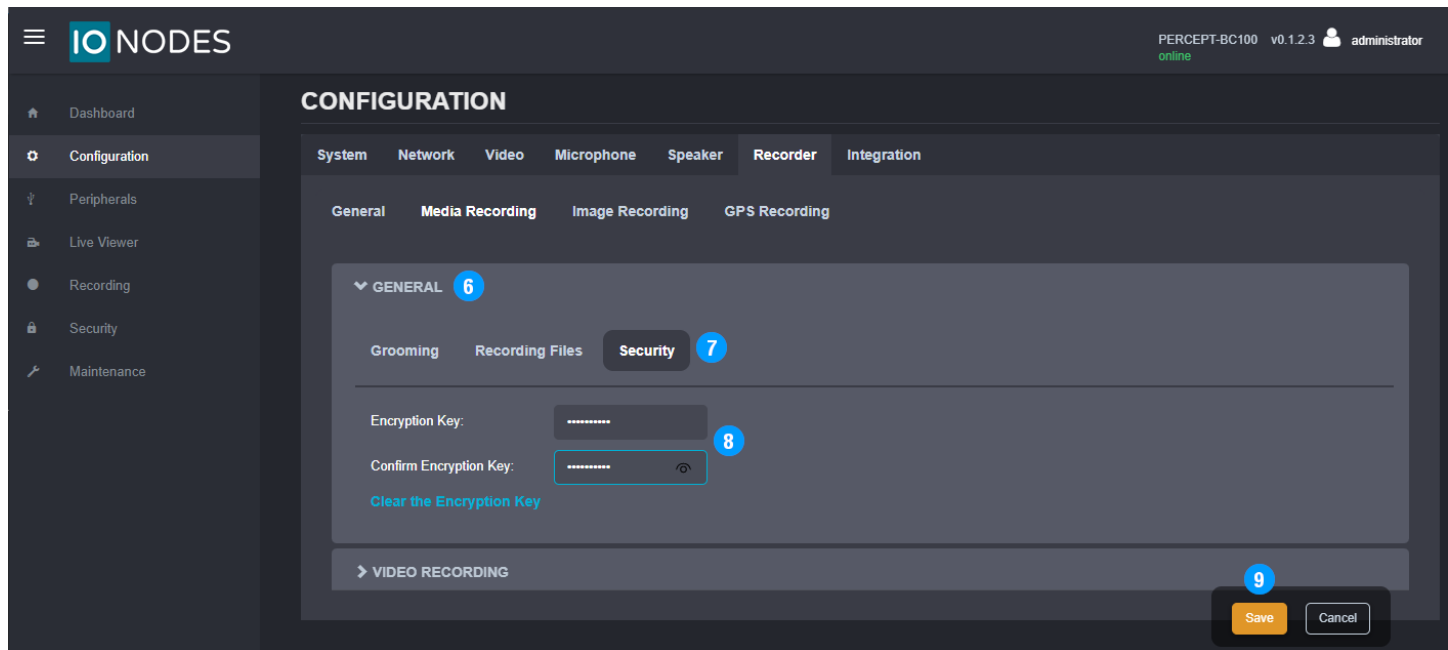
3.4 Setup local recording on the body camera



1. From the **Configuration** page
2. Select the **Recorder** tab
3. Select the **Media Recording** subtab, **Video Recording** section
4. Select the Video Profile for edge/onboard storage recording (**Profile 1** for recording throughout this guide)
5. Enable Pre/Post-Recording as required and set their duration. The Pre-Recording Video Profile shall be set to the low bitrate live streaming profile (**Profile 2** in this guide)

Note: When Pre-Recording is enabled, the camera is constantly encoding and buffering video. If Pre-Recording is not required, disabling it significantly increases battery life. If Pre-Recording is set to the high bitrate profile, the camera will overheat in certain environmental conditions.

Note: To prevent unauthorized usage of locally recorded media in case of loss or theft, the camera features AES-256 encryption for at-rest files.

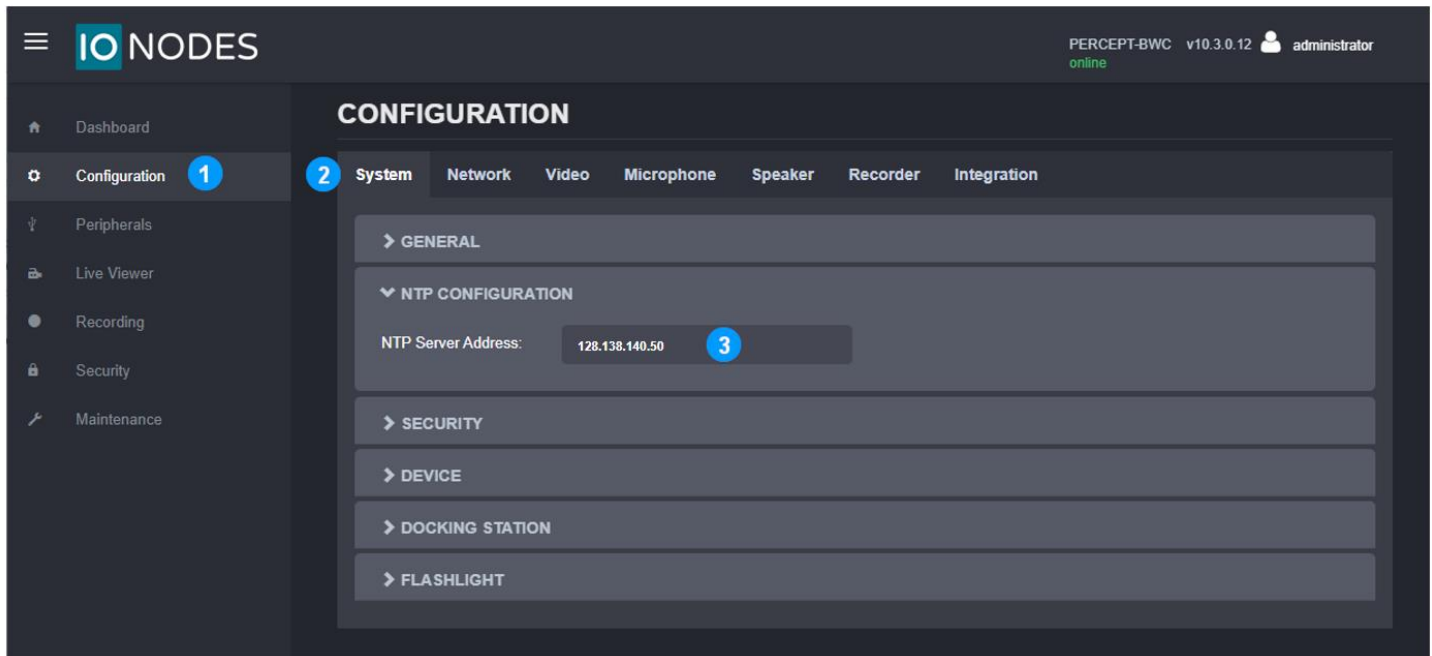


6. Under **Configuration, Recorder, Media Recording** tab, expand the **General** subtab
7. Select the **Security** section
8. Enter a password for AES-256 encryption of at-rest local media recording (enter and confirm **Encryption Key**). There is no password policy or complexity requirement.
9. **Save**

3.5 Setup time synchronization

Time synchronization ensures media recorded on PERCEPT Body Cameras' internal storage and later transferred to GSC are accurately timestamped. This is achieved through network time protocol (NTP) configuration. NTP settings can be entered manually in the PERCEPT Body Camera configuration page or pushed automatically from GSC.

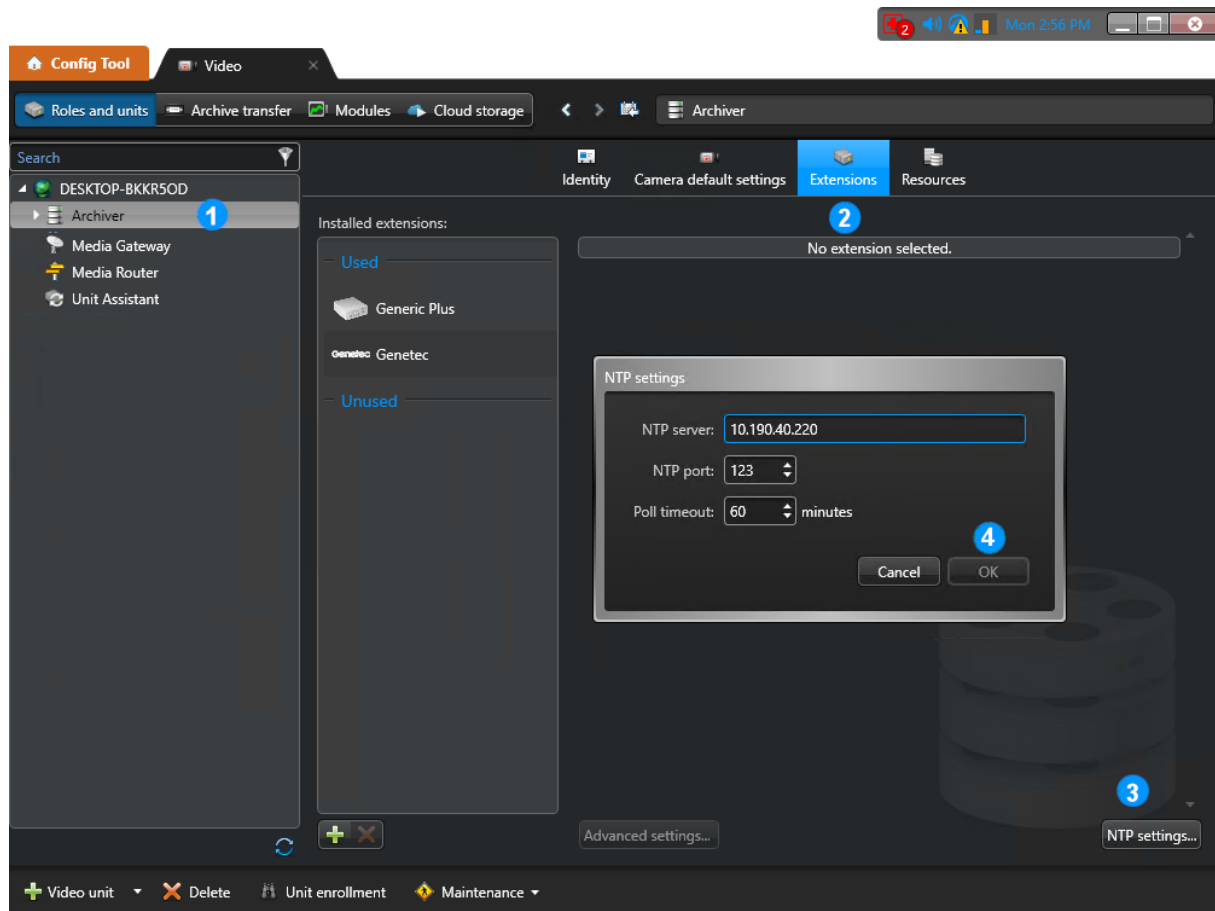
3.5.1 Setting NTP in PERCEPT Body Camera



1. From the **Configuration** page
2. Select the **System** tab
3. In the **NTP Configuration** section, enter the IP address of the network time server used by GSC to synchronize clocks

3.5.2 Pushing NTP Settings from GSC

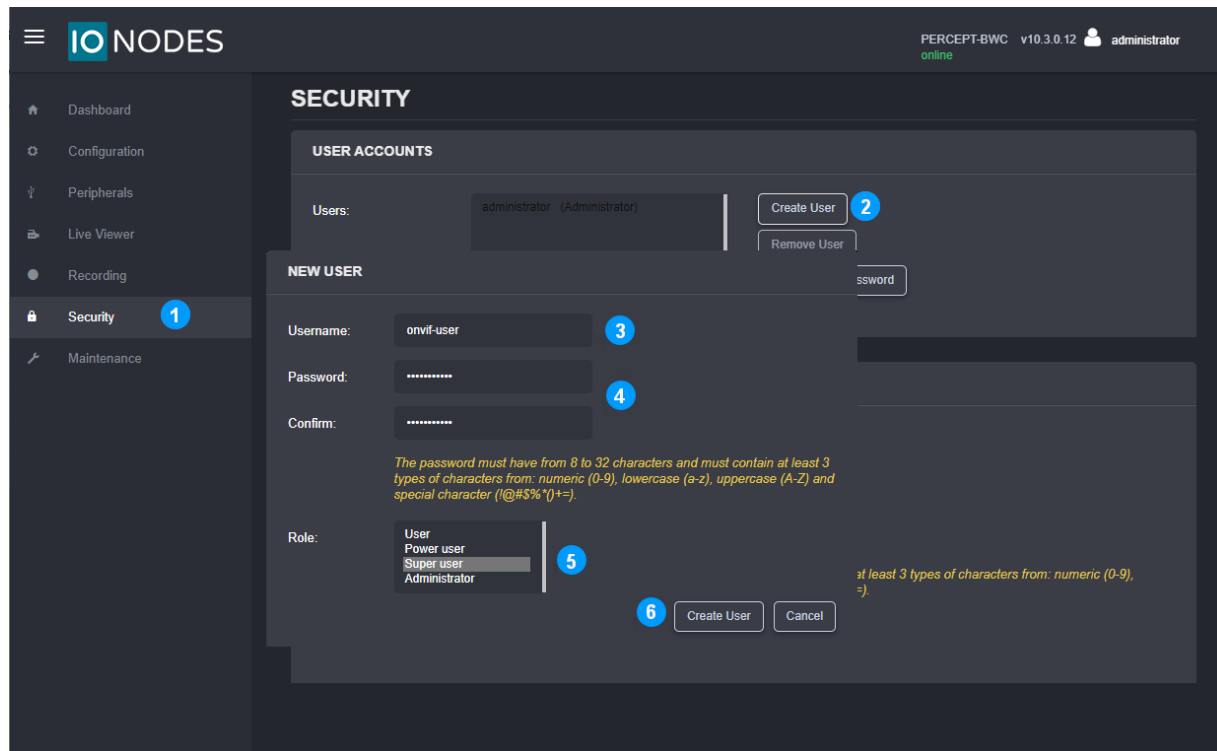
GSC Archiver Extensions include NTP server settings. When these settings are non-null, GSC will automatically push NTP server settings to connected devices, including PERCEPT Body Cameras.



1. Select the **Archiver** where the PERCEPT Body Camera is or will be enrolled
2. Select the **Extensions** tab
3. Click on **NTP settings...**
4. In the **NTP settings** pop-up window, enter the IP address of the network time server used by GSC to synchronize clocks then click **OK** and **Apply**

3.6 Create a new dedicated ONVIF user (recommended)

The default administrator account can be used for integrating the body camera with GSC. However, it is recommended to create a dedicated ONVIF user account for this purpose. The role “Superuser” gives the account permissions for all functions supported from GSC.



1. Once logged into the PERCEPT Body Camera’s Web UI, click on the **Security** page
2. Click on the **Create User** button
3. In the **New User** pop-up window, enter **Username**
4. Enter **Password** and repeat it to confirm
5. Select **Super user** Role
6. Click on **Create User**

Note: Configuration detailed in this guide shall be made using an ‘Administrator’ account, the dedicated ONVIF user is to enroll the PERCEPT Body Camera in GSC.

4 Configuring VPN

This section details VPN requirements, including a practical example.

4.1 VPN requirements

- Protocol: The PERCEPT Body Camera supports VPN protocol L2TP/IPSec with Pre-shared Key (PSK). VPN function is always-on; it connects when it can reach the VPN server.
- Tunnel# and Bandwidth: This protocol encrypts VPN tunnels. When assessing a VPN server (hardware or software), maximum number of VPN tunnels and encrypted bandwidth supported shall cover the number of PERCEPT Body Cameras deployed.
- Public Static IP address: The VPN server or router shall connect to the internet with a public static IP address. Port forwarding for the L2TP/IPSec protocol shall be configured when the VPN server is connected behind another internet router.
- Address reservation: VPN solution shall provide a mean to assign specific IP addresses to each device. This can be implemented by having a distinct VPN user for each device and assigning a specific IP to each user.

4.2 VPN example

Specific VPN selection and configuration is outside the scope of this guide. This example is included to better illustrate VPN requirements.

This example uses a entry-level hardware VPN router. It supports up to sixteen (16) L2TP VPN tunnels with a throughput of 47.11 Mbps encrypted. The recommended settings in this deployment guide yields ~ 1.0–1.2 Mbps per camera when live streaming audio and video on-demand. Presuming edge storage transfer is not performed remotely through VPN, this entry-level router can accommodate a small-scale PERCEPT deployment.

4.2.1 Configure L2TP server

This router supports configurable WAN/LAN ports. Once the router's basic IP settings and WAN/LAN ports are connected and configured, add an L2TP server.

The screenshot shows the IONODES router configuration interface. On the left is a sidebar menu with options: Status, Quick Setup, Network, Preferences, Transmission, Firewall, Behavior Control, VPN (expanded), Authentication, Services, System Tools, and Logout. The VPN menu is expanded, and 'L2TP' is selected, marked with a blue circle '1'. The main area has tabs for L2TP Server, L2TP Client, Global Config, and Tunnel List. The 'L2TP Server' tab is active, marked with a blue circle '2'. Below the tabs is the 'L2TP Server Settings' section. It includes a '+ Add' button (marked with a blue circle '3') and a '- Delete' button. Below these is a table with columns: ID, WAN, IPsec Encryption, Status, and Operation. The table contains one entry with ID '1', WAN 'WAN/LAN1', IPsec Encryption 'Encrypted', Status 'Enabled', and Operation '---'. Below the table is a configuration box (marked with a blue circle '4') for the selected server. It contains fields for: WAN (set to WAN/LAN1), IPsec Encryption (set to Encrypted), Pre-shared Key (set to SuperSecretKey, with a note '(1-128 characters)'), and Status (checked 'Enable'). There are 'OK' and 'Cancel' buttons at the bottom of the configuration box.

1. Expand the **VPN** menu and select **L2TP**
2. Select the **L2TP Server** tab
3. **Add** a new L2TP server
4. Configure the L2TP server then click **OK**
 - a. Select the **WAN** port that will receive incoming PERCEPT connections
 - b. Select **Encrypted**
 - c. Pick a secret **Pre-shared Key**
 - d. **Enable** the L2TP server

4.2.2 LAN IP address reservation

This router can act as DHCP server or relay. To configure LAN and VPN IP addresses from a single device, the DHCP server function is enabled in our example.

The screenshot shows the IONODES router web interface. On the left sidebar, the 'Network' menu is expanded, and 'LAN' is selected. The main content area has three tabs: 'LAN', 'DHCP Client List', and 'Address Reservation'. The 'LAN' tab is active, showing a 'Network List' table with one entry for 'LAN'. Below the table is a form for configuring the LAN network and DHCP settings.

ID	Name	Vlan	IP Address	Subnet Mask	DHCP Server	DHCP Relay	Operation
1	LAN	1	10.190.0.1	255.255.0.0	Enabled	Disabled	---

LAN Configuration Form:

Name: LAN

IP Address: 10.190.0.1

Subnet Mask: 255.255.0.0

Vlan: 1 (1-4086)

DHCP Settings:

DHCP Mode: ☒ DHCP Server ☐ DHCP Relay

Status: ☒ Enable

Starting IP Address: 10.190.0.5

Ending IP Address: 10.190.0.199

Lease Time: 2880 minutes (1-2880. The default value is 120)

Default Gateway: (Optional)

Default Domain: (Optional)

Primary DNS: (Optional)

Secondary DNS: (Optional)

☐ Advanced Settings

OK Cancel

1. Expand the **Network** menu and select **LAN**
2. Select the **LAN** tab
3. Click **Add**
 - a. Enter LAN network settings
 - b. Enable **DHCP Server** and configure its settings

The screenshot displays the IONODES web interface. On the left is a sidebar with navigation links: Status, Quick Setup, Network (expanded), WAN, LAN, IPTV, MAC, Switch, VLAN, IPV6, USB, Preferences, Transmission, Firewall, Behavior Control, VPN, Authentication, Services, System Tools, and Logout. The main content area has tabs for LAN, DHCP Client List, and Address Reservation (selected). Below the tabs is a section titled 'Address Reservation' with a '+ Add' button and a '- Delete' button. A table lists reserved addresses:

ID	MAC Address	IP Address	Description	Status	Operation
1	C4-41-37-53-DA-4C	10.190.1.1	PERCEPT-TS	Enabled	[Edit] [Delete]

A modal window is open for adding a new reservation. It contains the following fields and options:

- MAC Address: C4-41-37-53-DA-4C
- IP Address: 10.190.1.1
- Description: PERCEPT-TS (Optional)
- Status: ☒ Enable
- Buttons: OK, Cancel

4. Select the **Address Reservation** tab
5. Click **Add**
6. Enter the PERCEPT Body Camera's **MAC Address** and desired **IP Address** then **Enable**

Note: MAC address can be found on the PERCEPT Body Camera Web UI's Dashboard or on its OLED display by repeated short presses on the power button to cycle through status info.

4.2.3 VPN IP address reservation

This router assigns IP addresses to VPN clients. Each VPN user can be assigned to a specific VPN IP pool. By creating a single-address VPN IP pool and a VPN user for each PERCEPT Body Camera, a connection from a specific VPN user is always assigned the same IP address.

The screenshot displays the IONODES web interface for configuring VPN IP pools. On the left, the 'Preferences' menu is expanded, and 'VPN IP Pool' is selected, indicated by a blue circle with the number 1. The main content area shows the 'VPN IP Pool List' table, which contains one entry with ID 1, IP Pool Name C4413753DA4C, and Starting/Ending IP Address 10.190.1.1. In the top right corner, there is a '+ Add' button (marked with a blue circle 2) and a '- Delete' button. A modal dialog box is open, showing the 'Add' form for a new VPN IP pool. The form includes fields for 'IP Pool Name', 'Starting IP Address', and 'Ending IP Address', all of which are pre-filled with the same values as the existing pool (C4413753DA4C and 10.190.1.1). The 'OK' and 'Cancel' buttons are at the bottom of the modal, with a blue circle 3 highlighting the 'OK' button.

ID	IP Pool Name	Starting IP Address	Ending IP Address	Operation
1	C4413753DA4C	10.190.1.1	10.190.1.1	---

1. Expand the **Preferences** menu and select **VPN IP Pool**
2. Click **Add**
3. Pick an **IP Pool Name** and set the **Starting** and **Ending address** to the same address reserved on the LAN DHCP server for this PERCEPT Body Camera. To ease configuration in this example, the IP Pool Name is set to the MAC address of the camera.

Status

Quick Setup

Network

Preferences

Transmission

Firewall

Behavior Control

VPN

- IPsec
- L2TP
- PPTP
- OpenVPN
- Users

Authentication

Services

System Tools

Logout

Users

User Account List

5

+ Add - Delete

<input type="checkbox"/>	ID	Account Name	Protocol	Local IP Address	IP Address Pool	Network Mode	Remote Subnet	Operation
--	1	C4413753DA4C	L2TP	10.190.0.1	C4413753DA4C	Client-to-LAN	--	---

Account Name:

C4413753DA4C

Password:

.....

Low Middle High

Protocol:

L2TP

Local IP Address:

10.190.0.1

IP Address Pool:

C4413753DA4C

DNS Address:

10.190.0.1

Network Mode:

Client-to-LAN

Max Connections:

1

(1-100)

OK

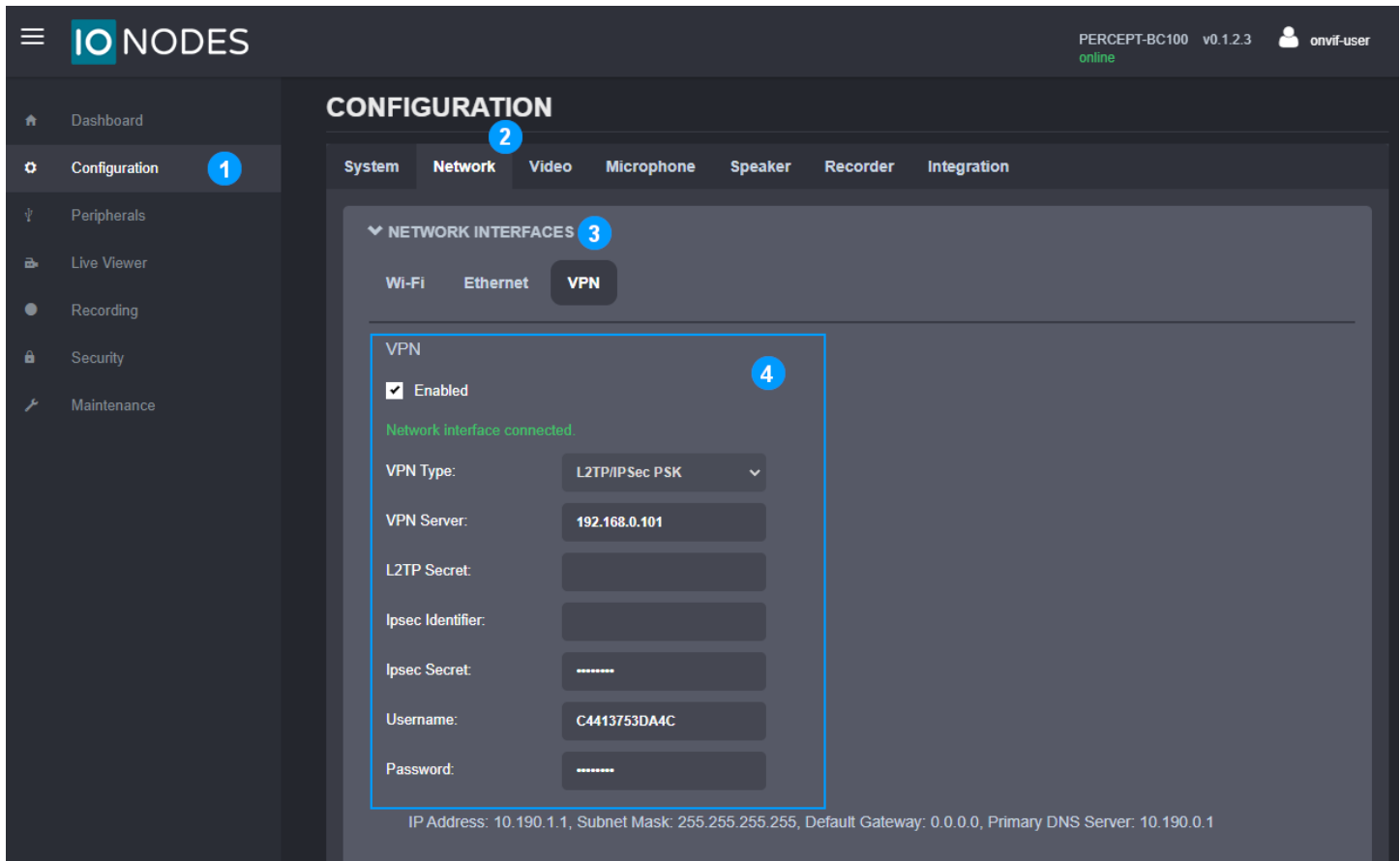
Cancel

6

4. Expand the **VPN** menu and select **Users**
5. Click **Add**
6. Create and configure the VPN user:
 - a. **Account Name:** Pick a unique VPN username for each PERCEPT Body Camera. In this example, it is set to the MAC address of the camera
 - b. **Password:** A password for this VPN user (can be the same for all users)
 - c. **Protocol:** **L2TP**
 - d. **Local IP address:** LAN IP address of the VPN router
 - e. **IP address Pool:** IP Pool created in previous step for this PERCEPT Body Camera. In this example, it is the MAC address of the camera
 - f. **DNS address:** LAN IP address of the VPN router
 - g. **Network Mode:** **Client-to-LAN**
 - h. **Max Connections:** **1**

4.2.4 Configure PERCEPT VPN Settings

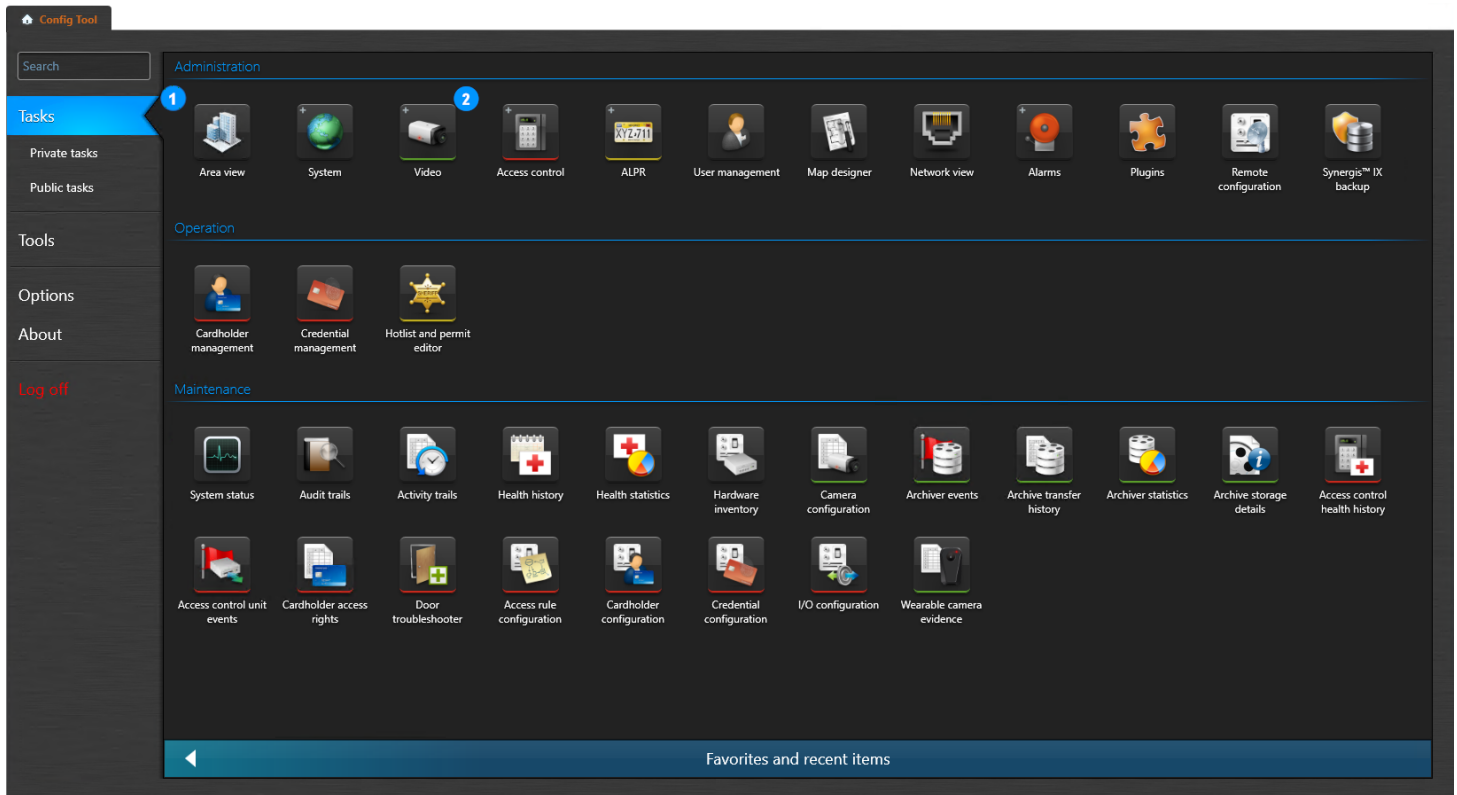
PERCEPT VPN settings shown are based on the VPN IP address reservation example above.



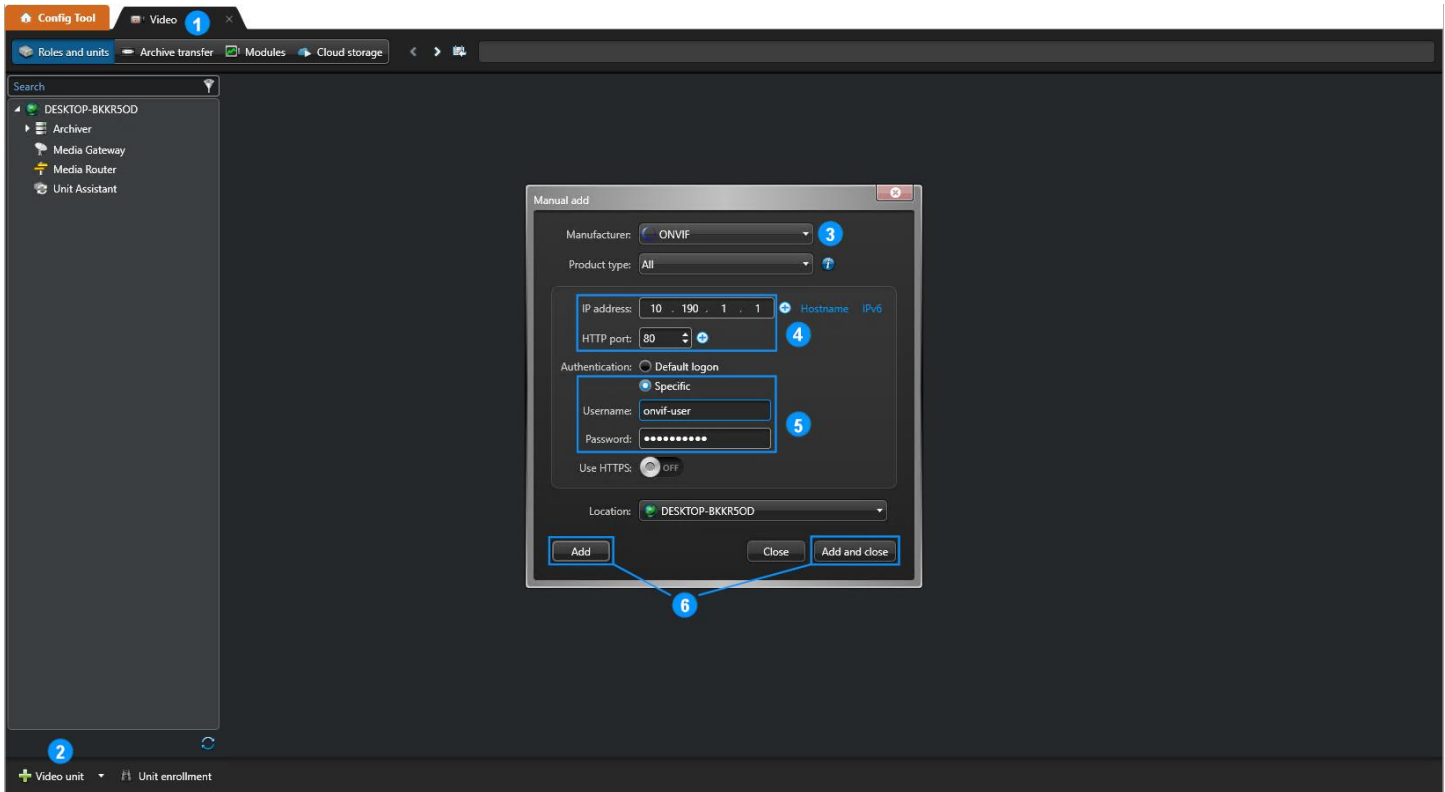
1. From the **Configuration** page
2. Select the **Network** tab
3. Expand the **NETWORK INTERFACES** section and select the **VPN** subtab
4. **Enable** and configure **VPN** parameters
 - a. **VPN Server:** Public static IP address of the VPN router's WAN port
 - b. **IPsec Secret:** L2TP server Pre-Shared Key (set in section 4.2.1)
 - c. **Username:** VPN username (set in section 4.2.3, MAC address of the PERCEPT Body Camera in this example)
 - d. **Password:** VPN user password (set in section 4.2.3)

5 Integrating the PERCEPT Body Camera in GSC

5.1 Enroll Camera



1. In the GSC **Config Tool**, click on the **Tasks** page
2. Click on **Video** to add devices

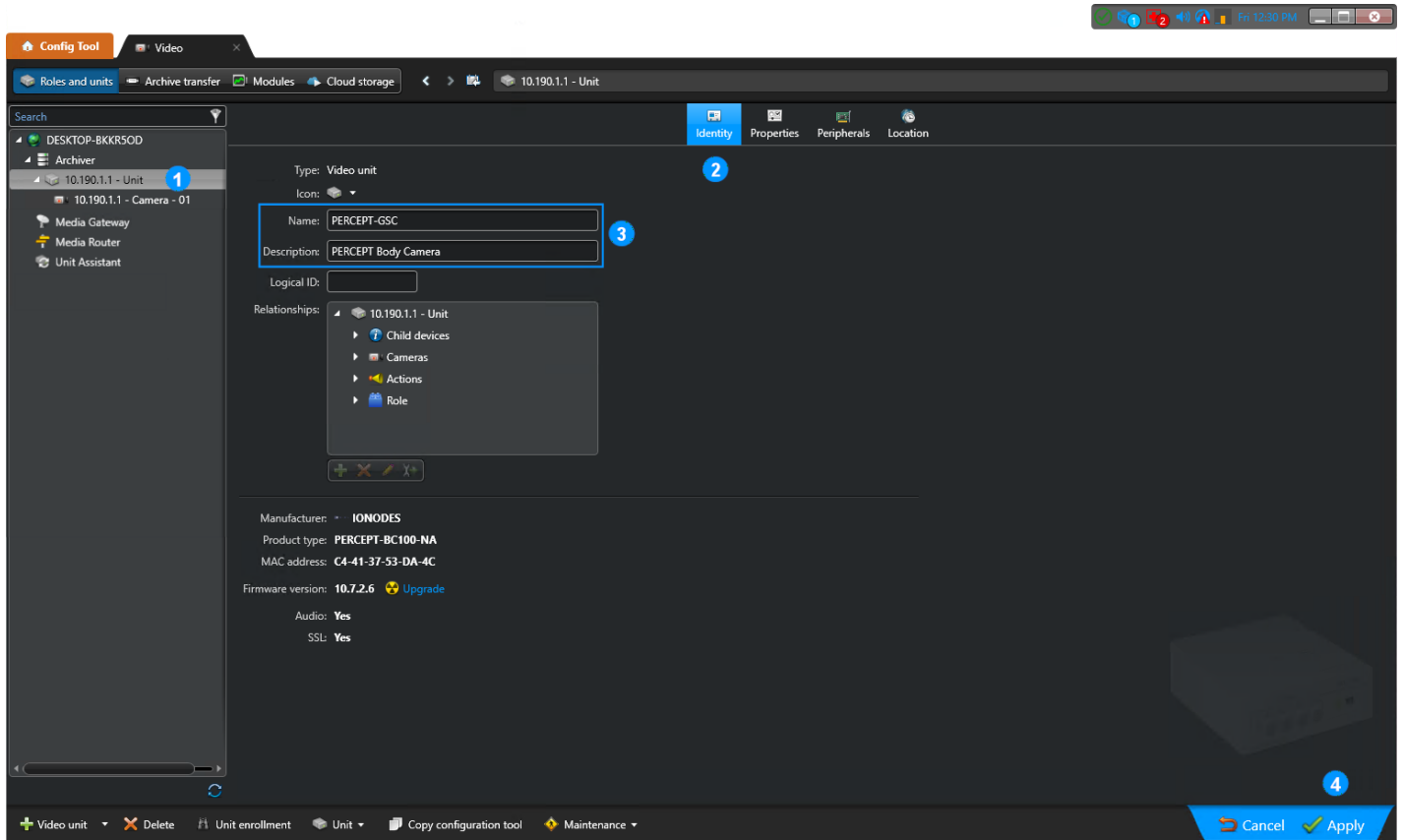


1. From the **Video** tab, **Roles and units** subtab
2. Click on the **+ Video unit** to add a device
3. From the pop-up **Manual add** window, select **ONVIF** from the drop-down list
4. Enter the IP address of your PERCEPT Body Camera
5. If credentials were changed (as recommended), select **Specific** and enter them
6. Click **Add** or **Add and close** if adding only one device

Note: The PERCEPT Body Camera can also be added through *Unit enrollment* discovery wizard, using ONVIF as the manufacturer.

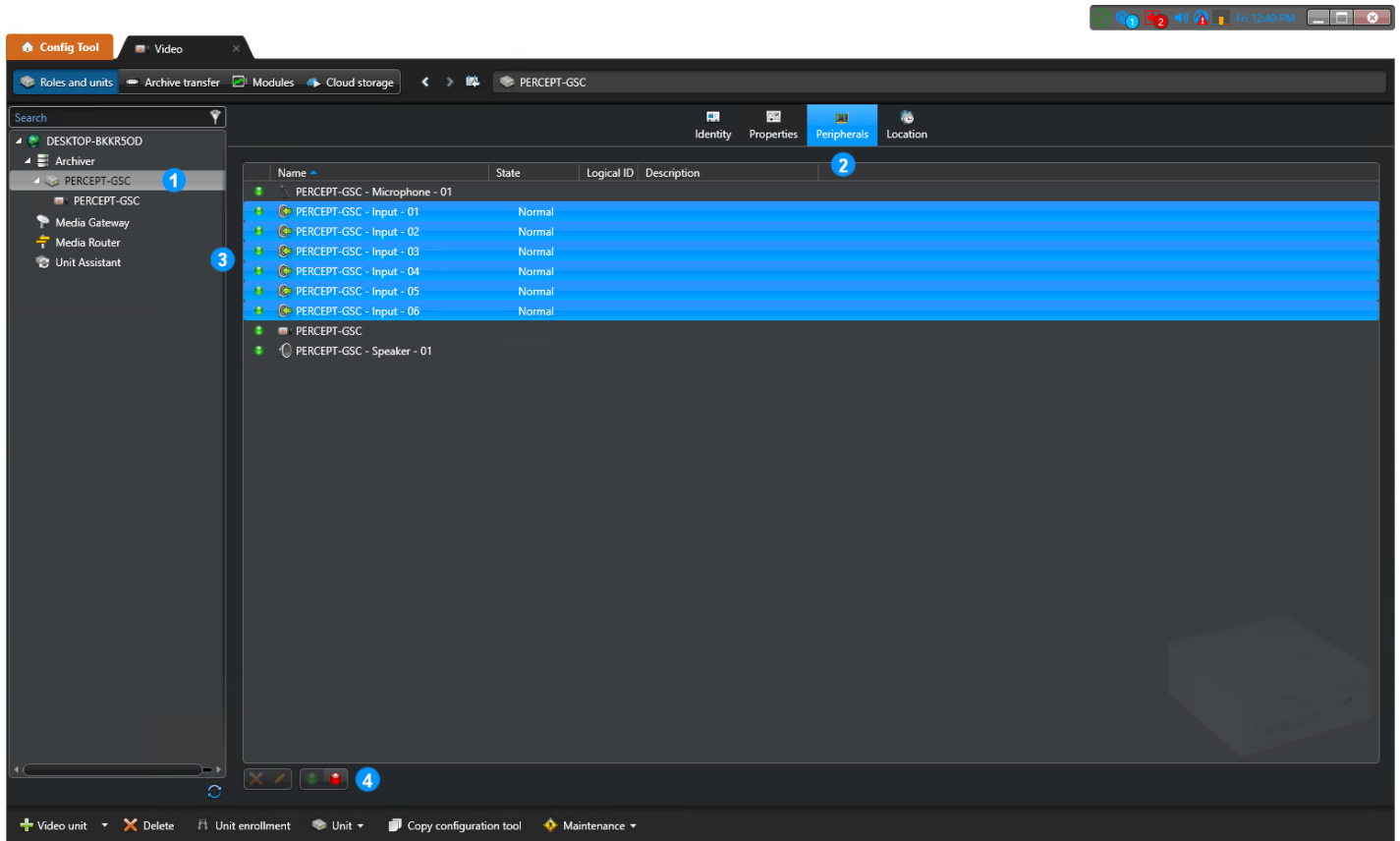
5.2 Configure Camera

5.2.1 Identity

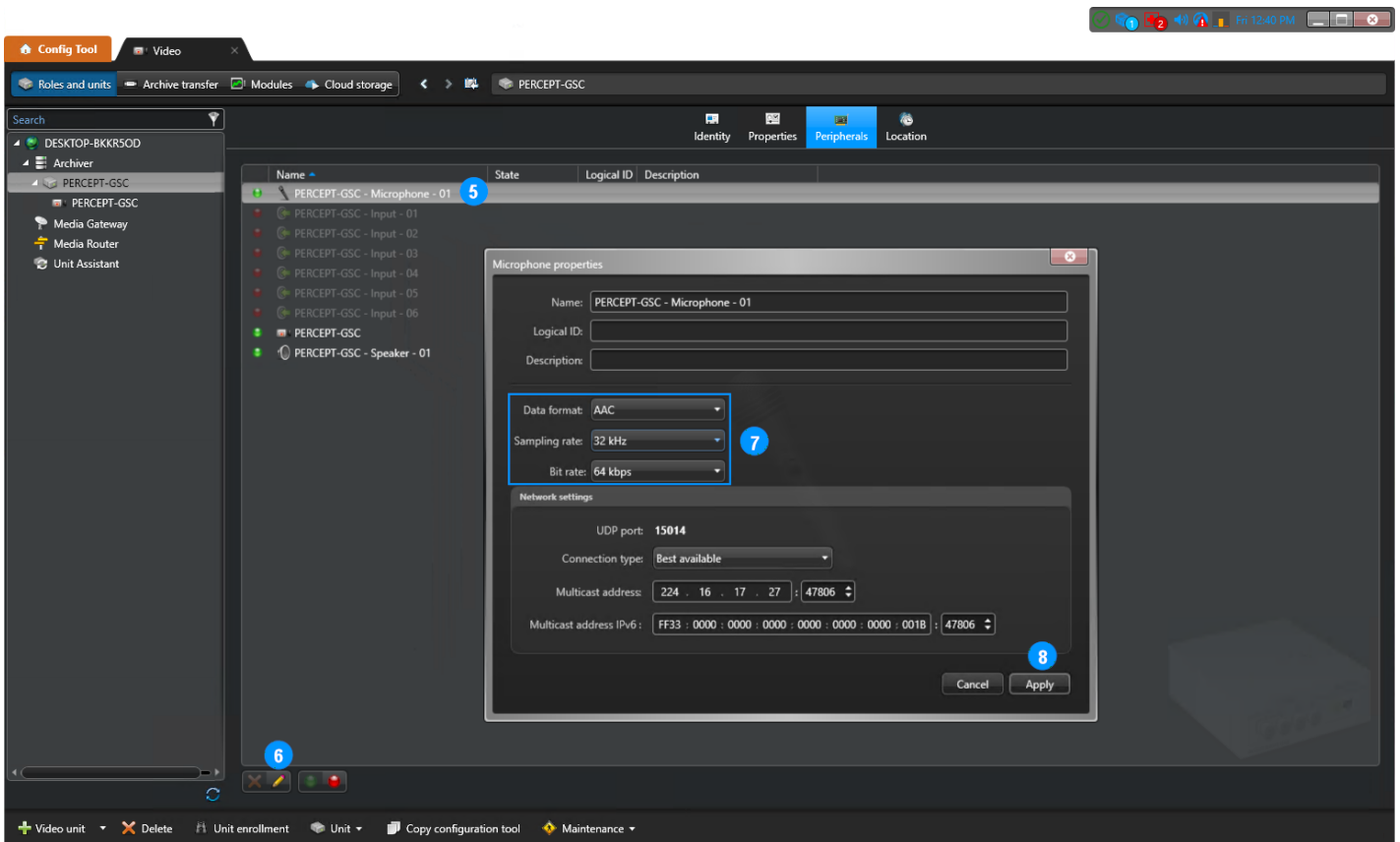


1. Expand the **Archiver** and select the newly added PERCEPT Body Camera
2. Select the **Identity** tab
3. Update its **Name** and **Description**
4. **Apply** changes and confirm whether you want to rename related devices as well

5.2.2 Peripherals

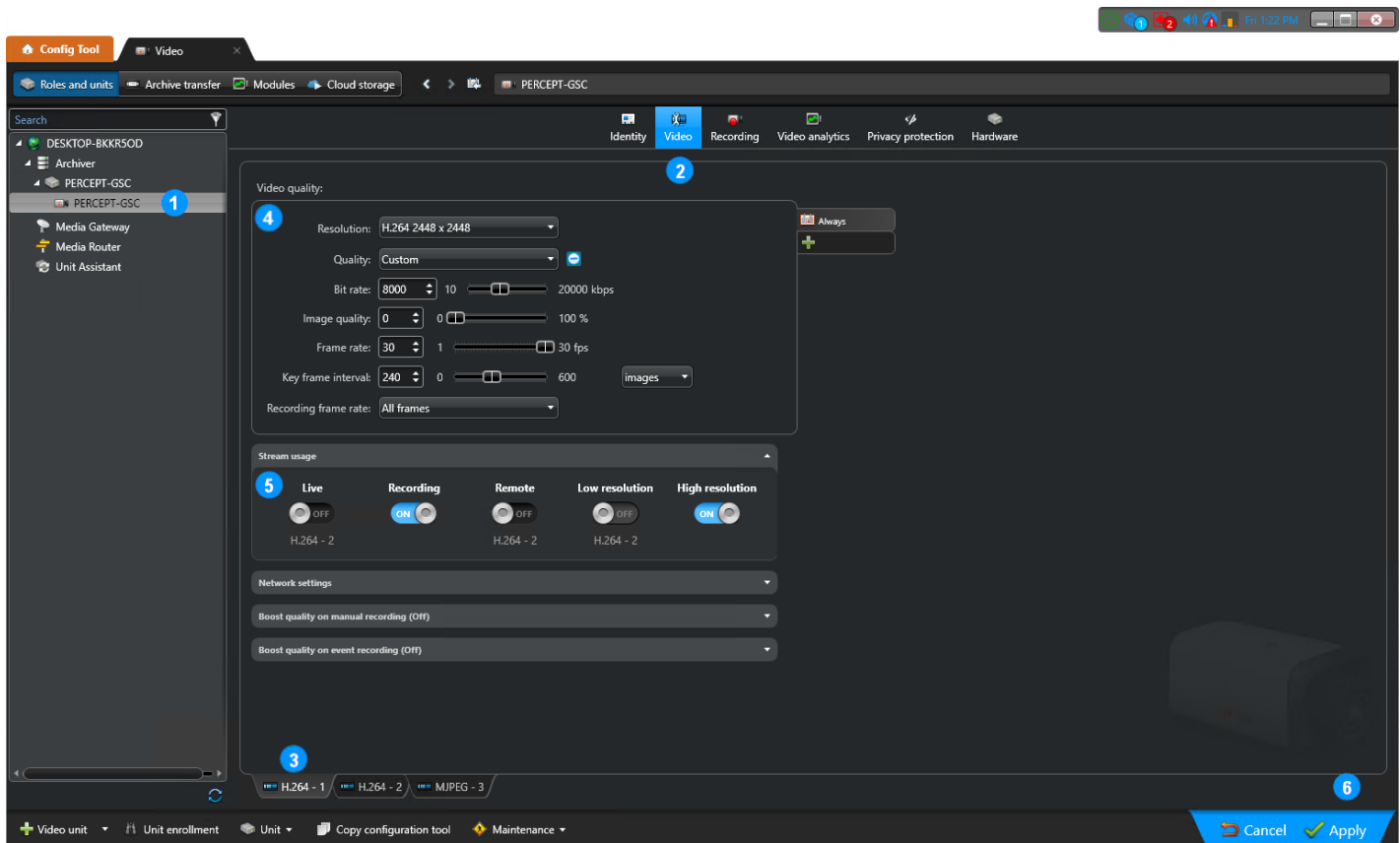


1. With the newly added PERCEPT Body Camera selected
2. Select the **Peripherals** tab
3. Select all six (6) **Input** buttons
4. **Disable** selected inputs then **Apply** changes

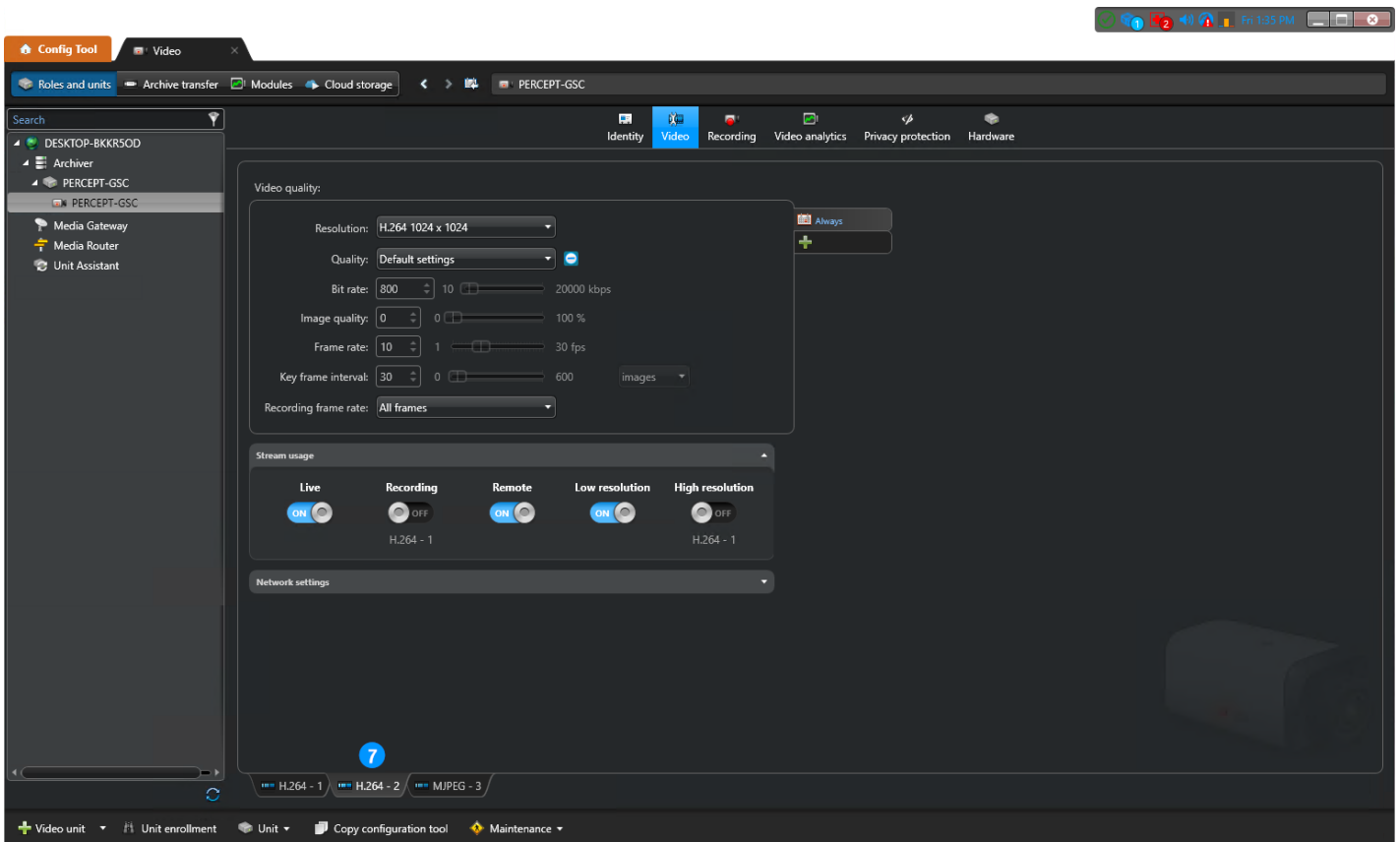


5. Select the PERCEPT Body Camera's **Microphone - 01**
6. Edit its properties by clicking on the stylus icon
7. In the **Microphone properties** pop-up window, edit its audio configuration. The following are recommended for acceptable quality and low bitrate:
 - a. **Data format: AAC**
 - b. **Sampling rate: 32 kHz**
 - c. **Bit rate: 64 kbps**
8. **Apply** to close this window then **Apply** again in **Peripherals** window

5.2.3 Video

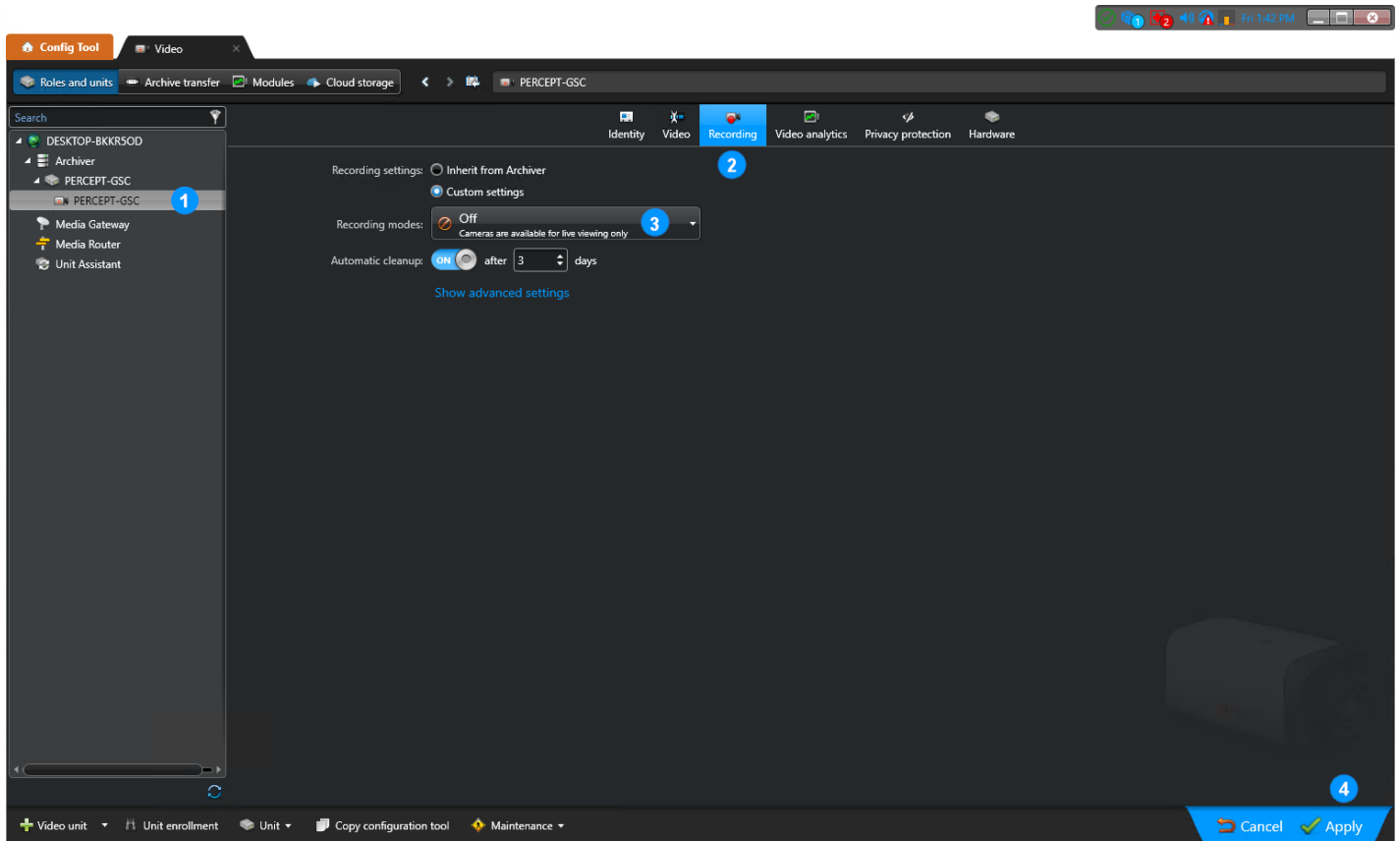


1. Expand the newly added PERCEPT Body Camera and select its camera device
2. Select the **Video** tab
3. Select its primary stream **H.264 - 1**
4. GSC enrollment automatically increases primary video stream settings to highest supported resolution and fps, and default 4Mbps bitrate. Re-enter Profile 1 parameters entered in section 3.3.2
 - a. **Resolution: H.264 2448 x 2448**
 - b. **Bit rate: 8000** kbps
5. Configure **Stream usage** for this profile to **Recording** and **High resolution** only
6. **Apply** these changes



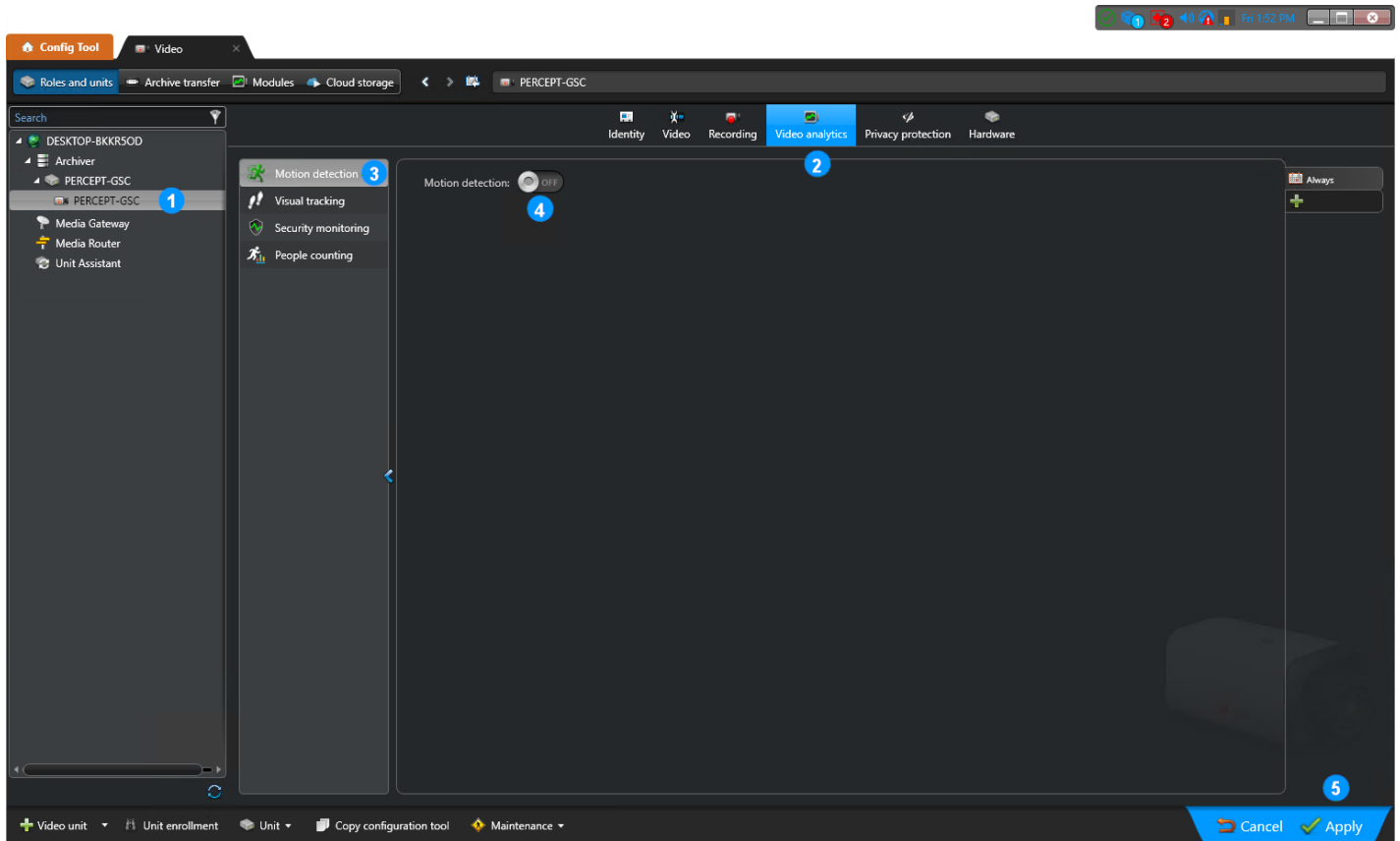
7. Select secondary stream **H.264 - 2** and verify that:
 - a. Profile 2 parameters entered in section 3.3.2 are correctly applied (GSC should not change secondary stream settings during enrollment), and
 - b. All **Stream usage** other than **Recording** and **High resolution** use this profile

5.2.4 Recording



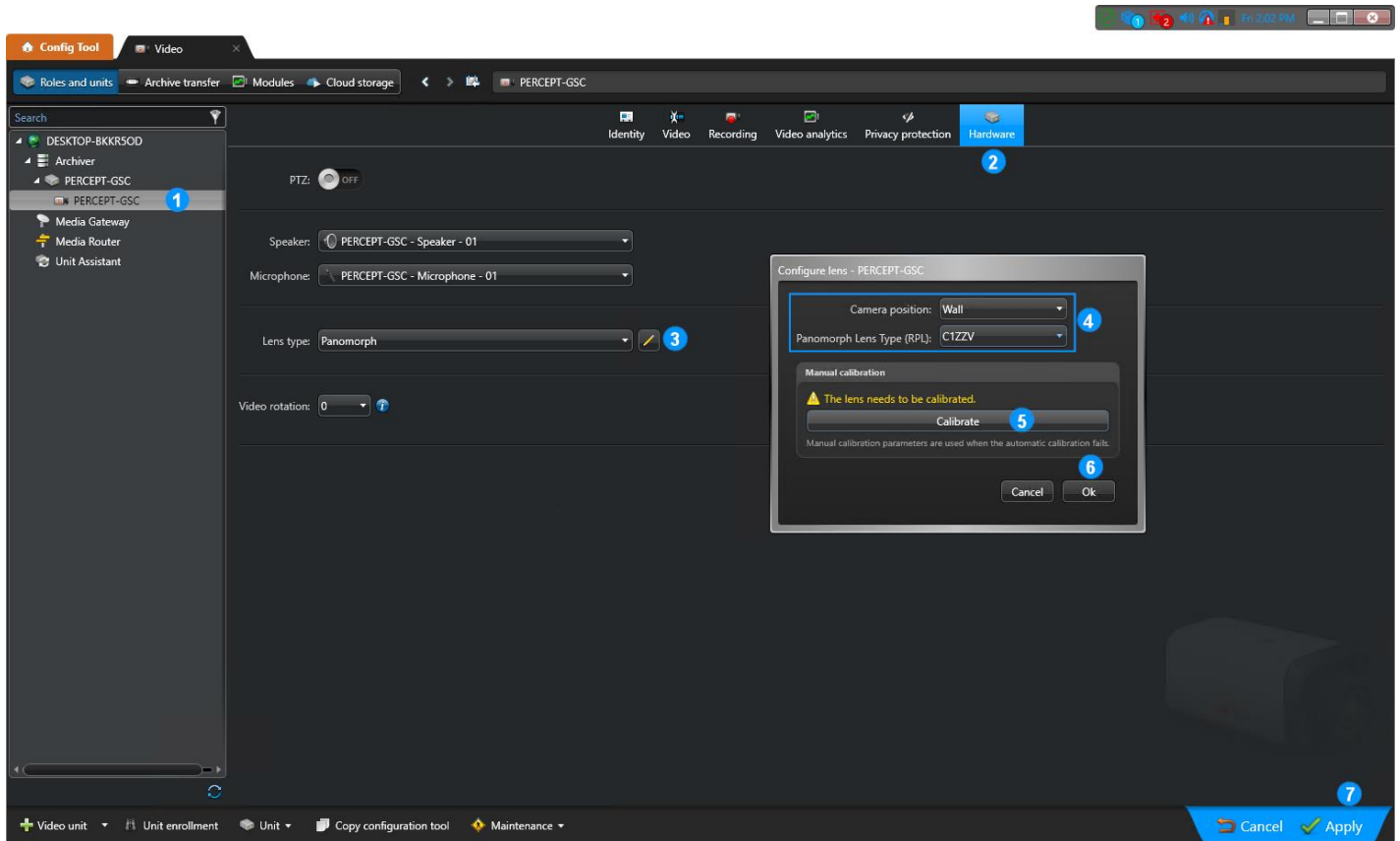
1. Expand the newly added PERCEPT Body Camera and select its camera device
2. Select the **Recording** tab
3. Configure **Recording modes** to **Off**
4. **Apply** this change

5.2.5 Video analytics



1. Expand the newly added PERCEPT Body Camera and select its camera device
2. Select the **Video analytics** tab
3. Select the **Motion detection** subtab
4. Toggle **Motion detection** to **Off**
5. **Apply** this change

5.2.6 Panomorph Lens

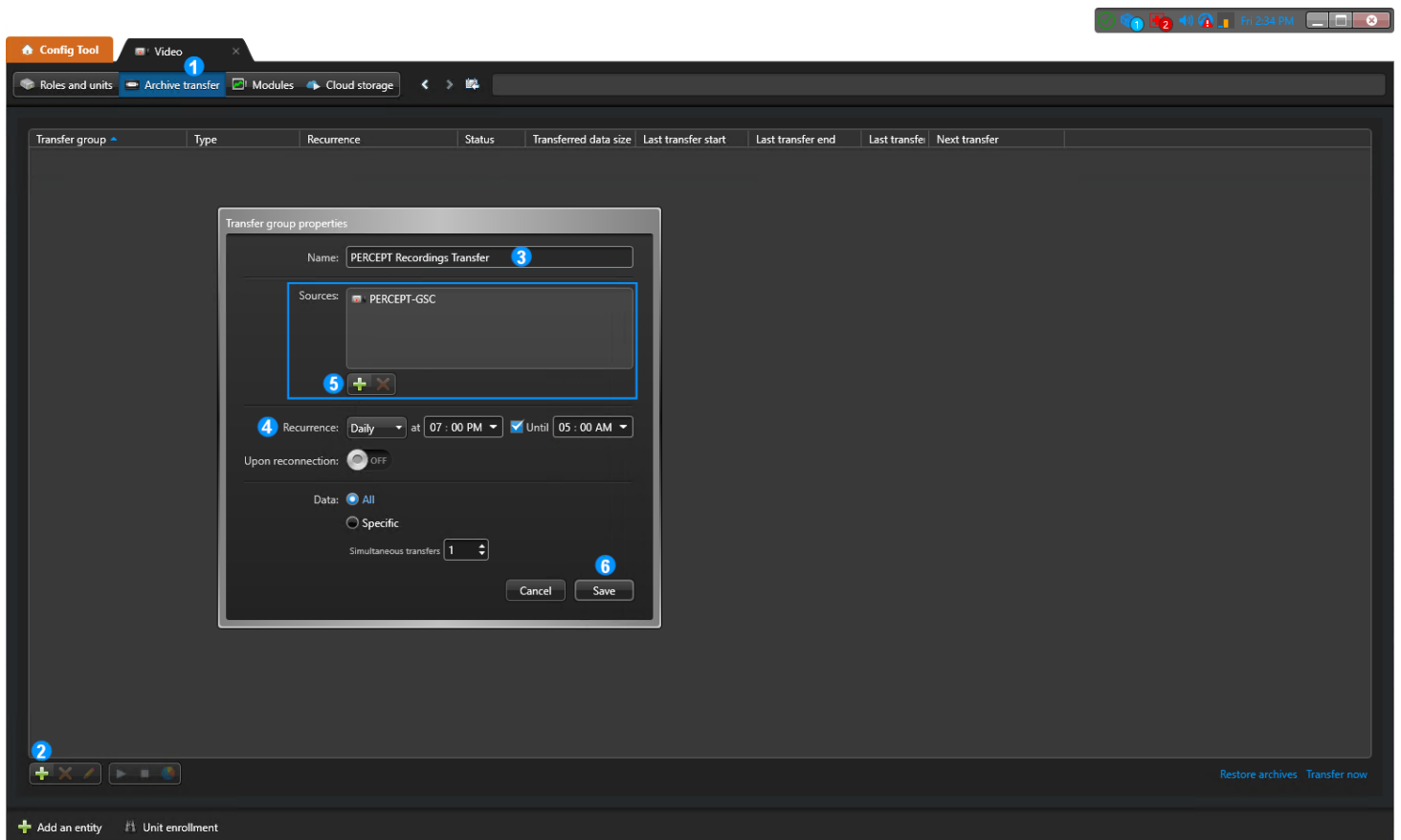


1. Expand the newly added PERCEPT Body Camera and select its camera device
2. Select the **Hardware** tab
3. Set **Lens type** to **Panomorph** and click on the stylus icon to open the **Configure Lens** pop-up window
4. Set **Camera position** to **Wall** (best approximation for a wearable camera) and **Panomorph Lens Type (RPL)** to **C1ZZV**
5. Click on **Calibrate** button
6. Click **Ok**
7. **Apply** this change

6 Configuring Edge Storage Transfer

Configuration made in previous section ensures GSC will connect to the low bitrate live video and audio streams on-demand, and not to the high bitrate recording stream. The speaker stream is only activated when Security Desk users press to talk.

All recordings will be saved on PERCEPT Body Camera's internal storage. This section describes how to configure transfer of these recordings to the GSC Archiver.



1. From the **Video** tab, **Archive transfer** subtab
2. Click on the **+** to create a new archive transfer group
3. From the pop-up **Transfer group properties** window, pick a name for this task
4. Select a **Recurrence** for archive transfer (more explanations below)
5. Click on the **+** icon then select all PERCEPT Body Camera(s) in the **Add sources** pop-up window
6. Click **Save**

To optimize data usage, recurrence shall be tailored to the expected schedule of PERCEPT Body Camera usage. The transfer group shown above will query body cameras between 19:00 and 05:00 every day and transfer all recordings that have not previously been transferred to the GSC Archiver.

LTE and Wi-Fi data usage configuration set in section 3.2 blocks attempt to retrieve (via playback) recordings while connected wirelessly. Blocked attempts will consume a few kilobytes of wireless data each. It is best practice to schedule archive transfer recurrence at a time range when PERCEPT Body Cameras in that transfer group are expected to be docked, allowing the transfers to proceed over the wired Ethernet connection. Distinct transfer groups can be created for PERCEPT Body Cameras deployed over different time periods / work shifts.

7 Validating the Integration

This section describes key features to validate before deploying in the field over LTE/VPN, or on a large scale.

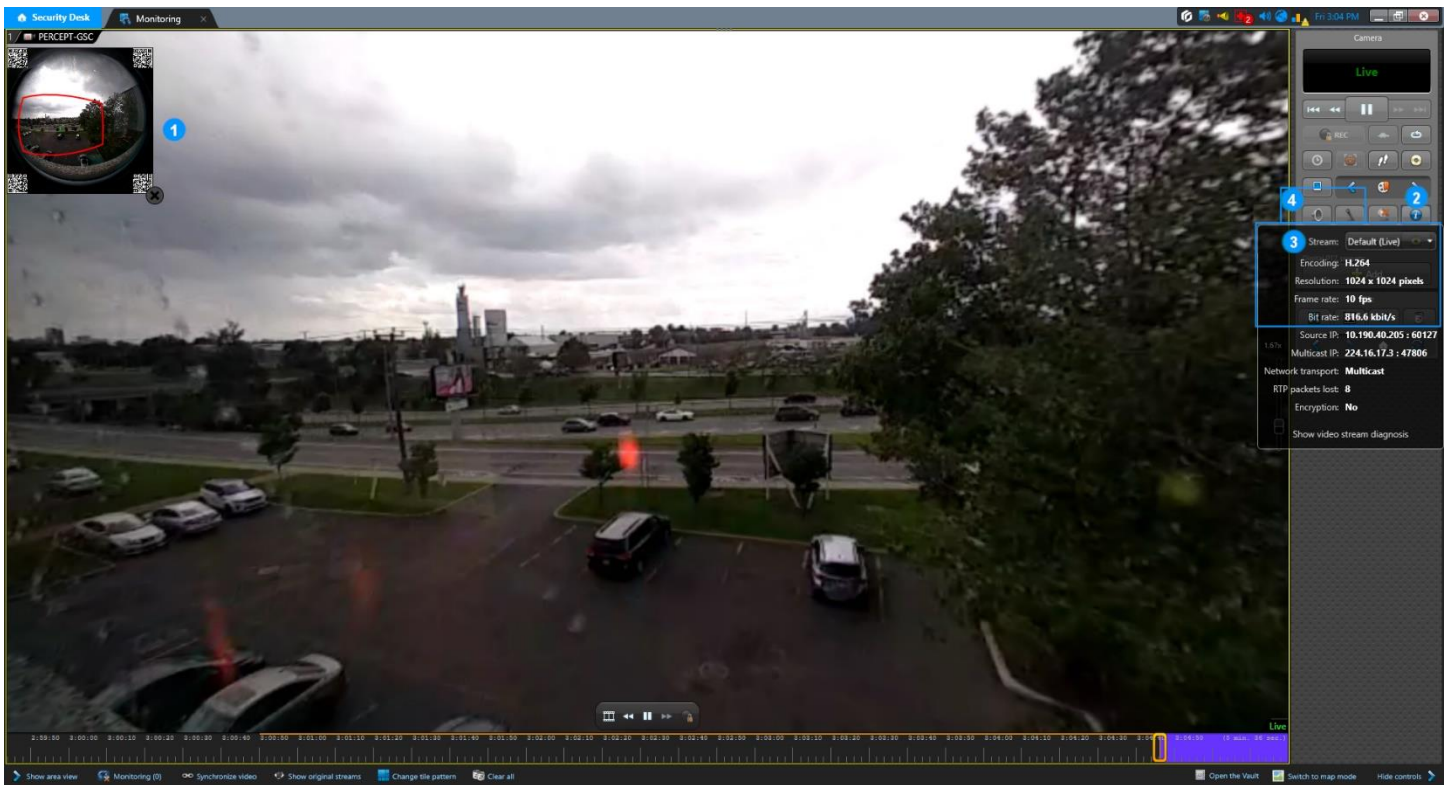
7.1 On-Demand Streaming

When no Genetec™ Security Desk, Web Client or Config Tool Client is displaying live audio/video, PERCEPT Body Cameras should not be streaming. This can be verified by the status LED of the body camera being solid blue. In this state, network communication is limited to ONVIF event polling and heartbeat traffic.

LED blinking in alternating red/green indicates it is sending a stream. If this is not expected, double-check that no client application is connected and review configurations detailed in sections 5.2.3, 5.2.4 and 5.2.5.

7.2 Live Streaming

Open Genetec™ Security Desk (GSD), select Monitoring tab and open a PERCEPT Body Camera. Verify that the live video stream starts. If Panormorph is configured as per section 5.2.6, verify that you can dewarp the video and pan through the scene. If Panormorph is not configured, panning and zooming in the hemispherical image is enabled without dewarping.



1. If Panormorph lens is configured, panning and zooming the scene dewarps the image
2. Click on the **Show stream** icon
3. Verify that video parameters (resolution, frame rate, bitrate, etc.) correspond to the low bitrate **Live** stream configured in sections 3.3.2 and 5.2.3. It is also possible to verify video parameters for the **Recording** stream, keeping in mind that its high bitrate might not be sustainable over wireless network.
4. Enable **Listening** and **Talking**. If computer is equipped with speakers, headphones, or other audio output devices, it shall play audio from the PERCEPT Body Camera's microphone. If equipped with audio input device(s), talking in the computer's microphone shall play on the PERCEPT Body Camera's speaker.

Note: There is a known issue with the **Talking** function on some versions of GSC. If no audio comes out of the PERCEPT Body Camera speaker, ensure the latest updates from Genetec are installed.

After closing all live view streams, verify that the LED status of the PERCEPT Body Camera returns to solid blue, indicating no stream is transmitted over the network.

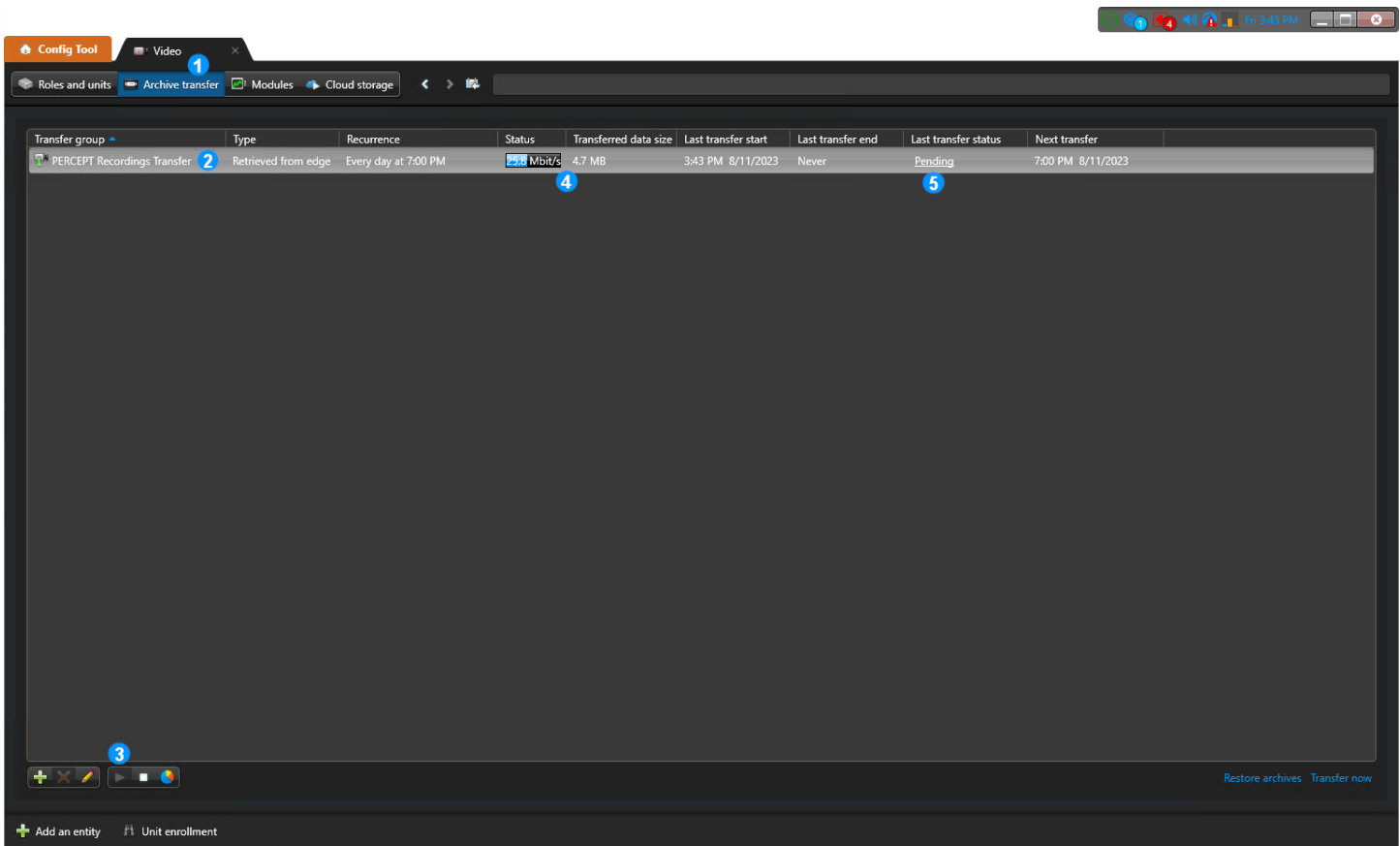
7.3 Edge Storage Transfer

Create a recording on the PERCEPT Body Camera local storage using its function buttons. Long press on F5 button starts / stops continuous recording, while single press on F1 or F3 creates a fixed-duration event recording.

If edge storage transfer (playback) was disabled over wireless as per section 3.2, insert the PERCEPT Body Camera in a docking station.

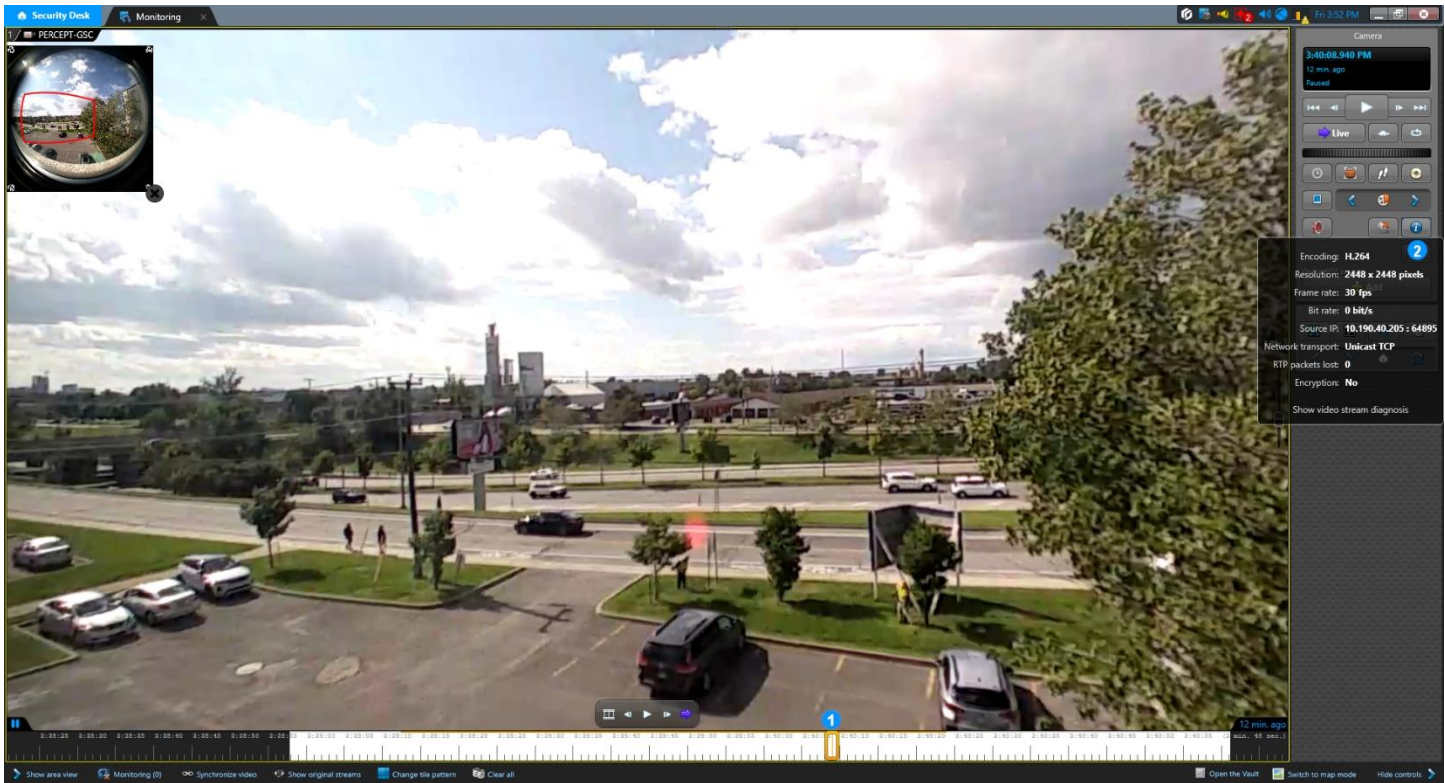


To validate Edge Storage transfer execution, wait for the recurring rule to execute, or start it manually.



1. From the **Video** tab, **Archive transfer** subtab
2. Select the Transfer group created in section 6
3. Click the play icon to **Start transfer for selected transfer groups**
4. Throughput and transfer size can be monitored during the transfer
5. Once the transfer completes, **Last transfer status** should indicate **Completed**

Open Genetec™ Security Desk (GSD), select Monitoring tab and open a PERCEPT Body Camera where a recording was transferred.



1. On the timeline, seek to date/time when or right after the recording was started from the PERCEPT Body Camera function buttons
2. Click on **Show stream** button and verify video parameters correspond to the high bitrate **Recording** stream configured in section 3.3.2 and 5.2.3.

Note: If pre-recording is configured as per section 3.4, there will be video recorded prior to the date/time recording was started from the camera's functions buttons. In our example, pre-recording is configured to use Profile 2 (low bitrate live stream) for 60 seconds. This pre-recording duration and its video parameters can be verified at this stage.

Note: If using Genetec™ Web Client, perform the same tests as for Security Desk, keeping in mind that Web Client does not support push-to-talk and requires GSC Media Gateway transcoding if video streams are configured with H.265 codec.

7.4 Network Interface Switching

If using only Wi-Fi and docking station, network interface switching between both was already tested in previous steps. This section validates switching between LAN and VPN over Wi-Fi and/or LTE.

If a Wi-Fi network with internet access is available, refer to the PERCEPT Body Camera Quick Start Guide to generate a QR code and connect the body camera to this network. From the camera's OLED display, verify the Wi-Fi connection status, signal strength, and that its IP address is as expected for this network. After a few seconds, VPN shall auto-connect and display its IP address. The VPN IP address shall be the same as the LAN IP address:

 WIFI 10:40 Signal: Great	 WIFI 10:40 192.168.0.1	 VPN 10:40 10.190.1.1
---	---	---

Note: Most Wi-Fi routers will not route VPN traffic from its main Wi-Fi network, back to the public static IP address of the primary internet router it is connected to. This can usually be solved by connecting the PERCEPT Body Camera to the Guest Wi-Fi network of the router.

Network interface switching is automatic, based on the following priority:

1. LAN over docking station
2. Wi-Fi
3. LTE / Cellular

If LTE and VPN are properly configured and activated, switching to VPN over LTE is automatic when LAN and Wi-Fi connections are lost.

Verify live streaming work over VPN as it does over Wi-Fi. If a live stream is displayed on Genetec™ Security Desk (GSD) when the network interface switches, and Panomorph is enabled for that stream, it may be required to clear and restart that live stream in GSD to re-establish the connection. There is a known issue on some versions of GSD that prevents auto-restart of live stream in certain circumstances.