



**IONODES PERCEPT Body Camera /
Milestone XProtect®**

Deployment Guide

Document Date: April 19th, 2022

Contents

Contents.....	2
1 Introduction.....	5
2 Recommended Deployment	5
2.1 Layout	5
2.2 Available Functionalities	7
3 Configuring the PERCEPT Body Camera.....	8
3.1 Deploying Multiple PERCEPT Body Cameras	8
3.2 Configure Networking	8
3.2.1 Configure Cellular.....	8
3.2.2 Configure Cellular Data Usage	9
3.2.3 Configure Wi-Fi Data Usage.....	10
3.2.4 Configure Docking Station(s)	11
3.3 Configure Video	13
3.3.1 Disable orientation metadata	13
3.3.2 Video profiles.....	14
3.4 Setup local recording on the body camera.....	16
3.5 Setup time synchronization on the body camera	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	Configuring XProtect® Before Integration	27
5.1	Configure Time Synchronization	27
5.2	Configure Device Groups.....	28
6	Adding the PERCEPT Body Camera in XProtect®	31
6.1	Configure Camera	39
6.1.1	Settings.....	39
6.1.2	Streams.....	40
6.1.3	Record	41
6.1.4	Motion.....	42
6.1.5	Fisheye Lens	43
6.1.6	Events.....	44
6.1.7	Client	45
6.2	Configure Microphones	46
6.2.1	Settings.....	46
6.2.2	Record	47
6.3	Configure Speaker	48
6.3.1	Settings.....	48

- 6.3.2 Record49
- 7 Configuring XProtect® Rules 50
 - 7.1.1 Default Start Audio Feed Rule.....50
 - 7.1.2 PERCEPT On-demand Audio Feed52
 - 7.1.3 PERCEPT Edge Storage Transfer Rule.....56
- 8 Event to Alarm 59
- 9 Validating the Integration..... 62
 - 9.1 On-Demand Streaming.....62
 - 9.2 Live Streaming.....62
 - 9.3 Recording 65
 - 9.3.1 Edge Storage Transfer67
 - 9.4 Network Interface Switching70

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 Milestone XProtect®. 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.

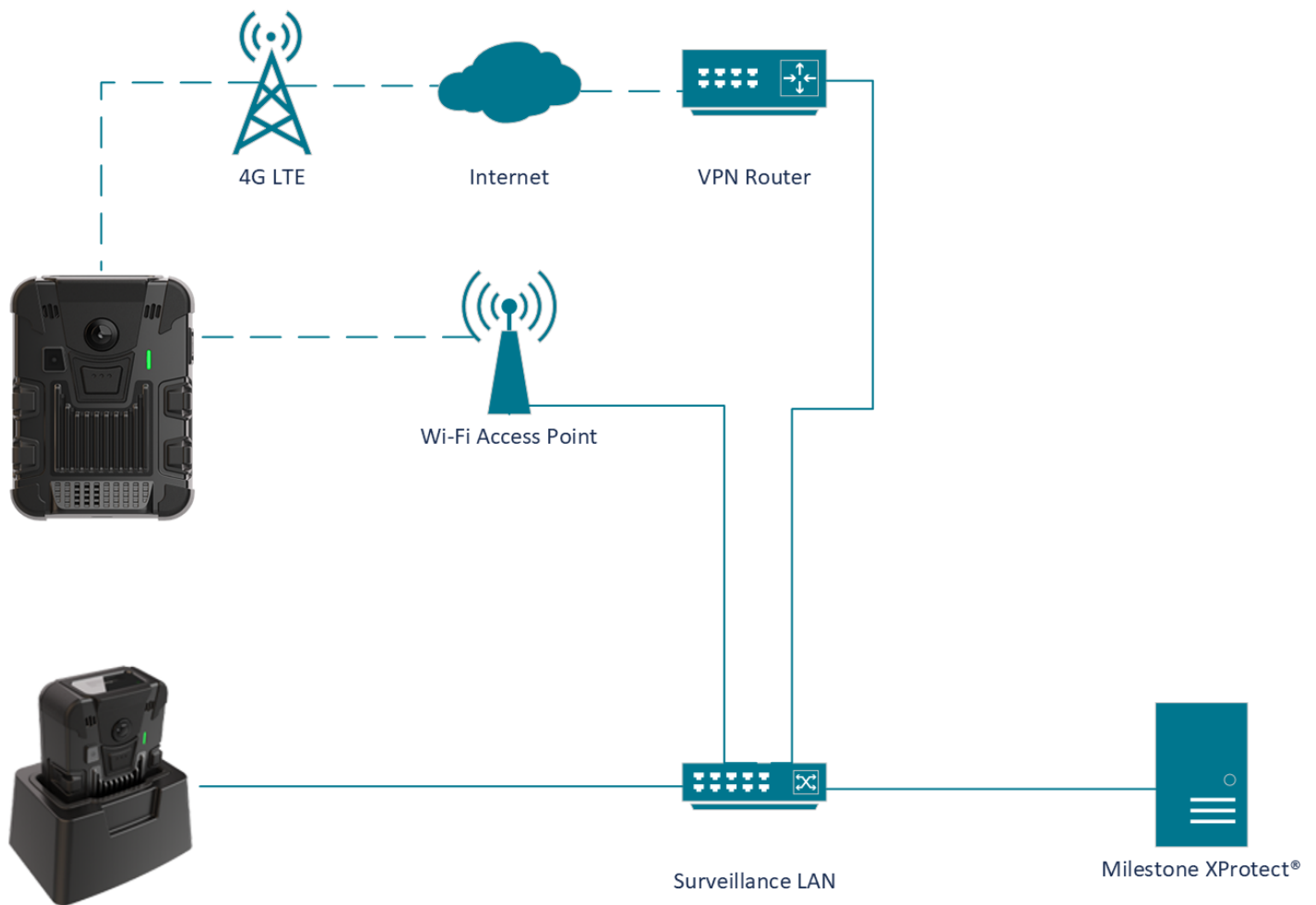
This integration is supported as of IONODES PERCEPT Body Camera firmware 10.7.2.5 and has been validated with XProtect® Expert 2022R3. It requires the Professional+ or higher-featured edition of XProtect®. Essential+ and Express+ editions do not support Edge Storage transfer. This document describes the recommended integration deployment as validated by IONODES and Milestone 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), Milestone XProtect®



The PERCEPT Body Camera can technically record directly to XProtect® 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 XProtect® Recording Server 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 XProtect® Smart Client and XProtect® Web Client	Live stream on-demand to minimize Wi-Fi/LTE data usage
Two-way audio communication using XProtect® Smart Client and XProtect® Web Client	
High-bitrate Audio & Video Recording saved on device Edge Storage (SD card)	
Automatic Edge Storage transfer of Audio & Video to XProtect® Recording Server	With Rules that trigger recurring Edge Storage transfer job
Configurable Events and Alarms triggered by Wearer. Visible in real-time in XProtect® Smart Client and XProtect® Web Client	
Date / Time synchronization	With NTP server common to XProtect® and PERCEPT
Firmware updates from XProtect® Management Client	
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 XProtect® 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 XProtect®.

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 XProtect®, 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.

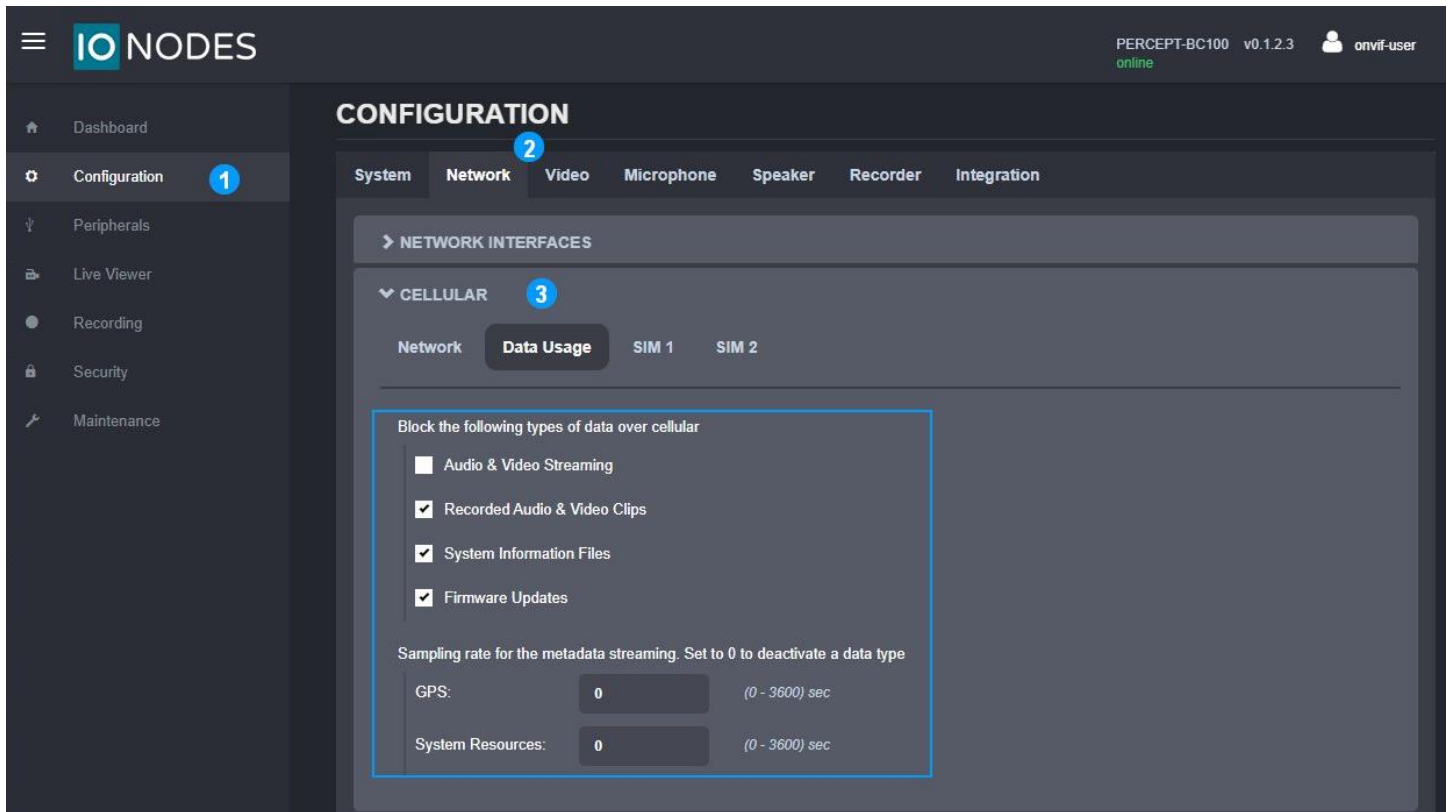
However, static IP addresses can prevent connecting with other networks to access the video LAN via VPN. For that reason, it is recommended to keep the camera's network interfaces to DHCP and configure the VPN router and/or video LAN DHCP server to hand out reserved IP addresses to each camera. This is further detailed in section 3.6 below.

3.2.1 Configure Cellular

All PERCEPT Body Cameras include a SIM card that can be activated at any time. Contact us 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 Milestone XProtect® 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.

XProtect® Recording Server 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.

The screenshot displays the PERCEPT Body Camera Web UI Configuration page. The left sidebar shows the navigation menu with 'Configuration' highlighted. The main content area is titled 'CONFIGURATION' and features several tabs: System, Network, Video, Microphone, Speaker, Recorder, and Integration. The 'Network' tab is selected. Under the 'Network' tab, there are several expandable sections: NETWORK INTERFACES, CELLULAR, HOST NAME CONFIGURATION, STREAMING, HTTP CONFIGURATION, DISCOVERY, RTSP CONFIGURATION, MULTICAST, and MISCELLANEOUS PORTS. The 'STREAMING' section is expanded, showing two sub-sections: Media and Metadata. The 'Metadata' sub-section is selected, and a checkbox labeled 'Prevent Media Playback Over a Wireless Connection' is checked. A blue arrow points from the 'Metadata' sub-section to a box containing the 'Sampling rate for the metadata streaming' settings. This box includes two input fields: 'GPS' and 'System Resources', both set to 0. The text above these fields states: 'Sampling rate for the metadata streaming. Set to 0 to deactivate a data type'. The 'GPS' field has a range of '(0 - 3600) sec' and the 'System Resources' field has a range of '(0 - 60) sec'.

1. From the **Configuration** page
2. Select the **Network** tab
3. Expand the **STREAMING** section and check **Prevent Media Playback Over a Wireless Connection** in the **Media** tab
4. 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.

The screenshot displays the IO NODES web interface. The top navigation bar includes the IO NODES logo, the device status 'PERCEPT-BC100 v0.1.2.3 online', and the user 'onvif-user'. The left sidebar contains a menu with 'Configuration' highlighted and numbered '1'. The main content area is titled 'CONFIGURATION' and has several tabs: 'System' (numbered '2'), 'Network', 'Video', 'Microphone', 'Speaker', 'Recorder', and 'Integration'. Under the 'System' tab, there are expandable sections: 'GENERAL', 'NTP CONFIGURATION', 'SECURITY', 'DEVICE', and 'WEARER ID'. The 'DOCKING STATION' section (numbered '3') is expanded, showing the following settings:

- ☒ Enable Online Mode
The Ethernet connection is activated when thresholds are reached.
- Minimum Battery Level: (20 - 50) %
Minimum battery level to allow the online mode.
- Starting Online Mode Offset: (10 - 30) %
Online mode will be activated only when the battery reaches the minimum battery level plus this offset.
- Network Transfer Inactivity Timeout: (120 - 600) sec
Timeout to switch in charging mode if no playback activity is running.
- Charging Timeout: (600 - 2700) sec
Timeout in charging mode to switch in online mode.
- ☐ Allow Live Media Streaming When Docked
- ☐ Allow Recorded Playback and Clip Download Over WIFI When Docked

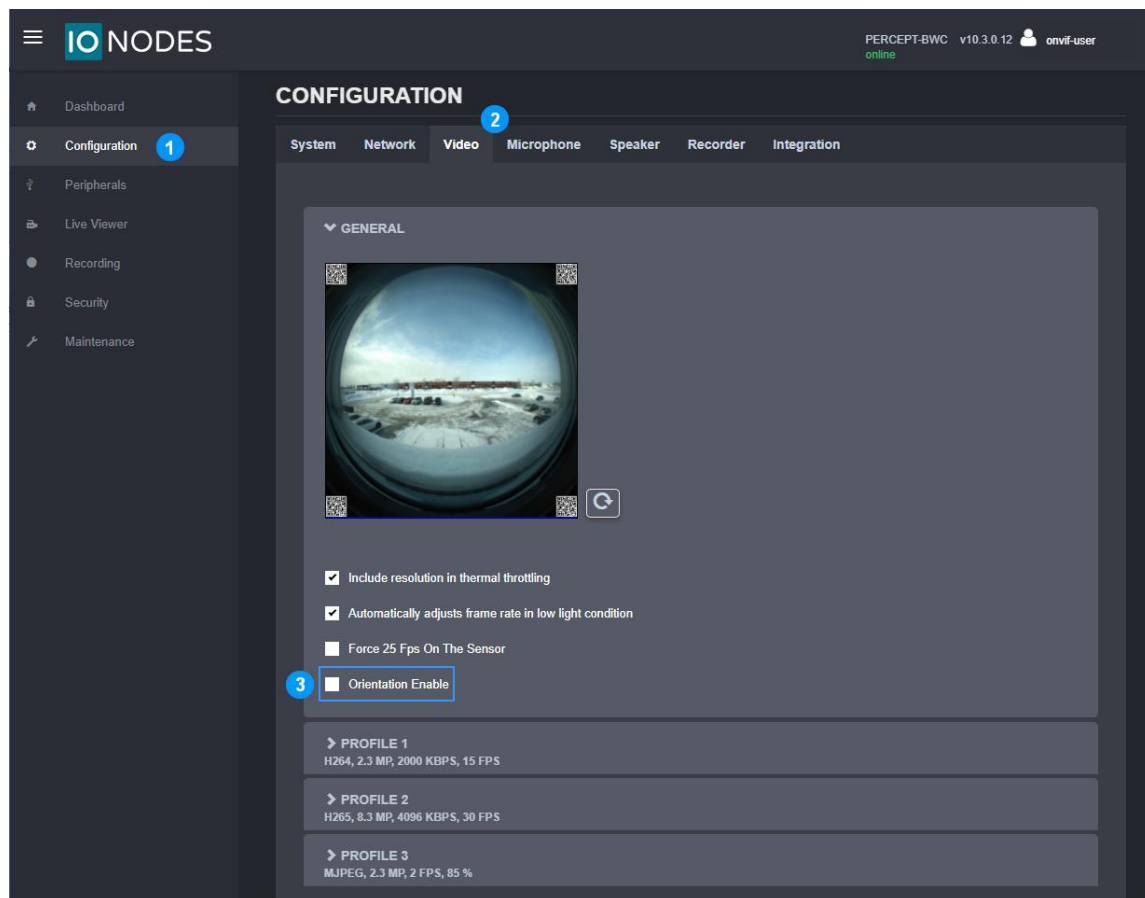
1. From the **Configuration** page
2. Select the **System** tab
3. Expand the **DOCKING STATION** section and configure parameters as follows
 - a. Check **Enable Online Mode**
 - b. Uncheck **Allow Live Media Streaming When Docked**
 - c. Uncheck **Allow Recorded Playback and Clip Download Over Wi-Fi 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. XProtect® Recording Server advanced configuration (RecorderConfig.xml) can be adjusted to limit edge storage jobs based on system scale and capacity.

3.3 Configure Video

3.3.1 Disable orientation metadata

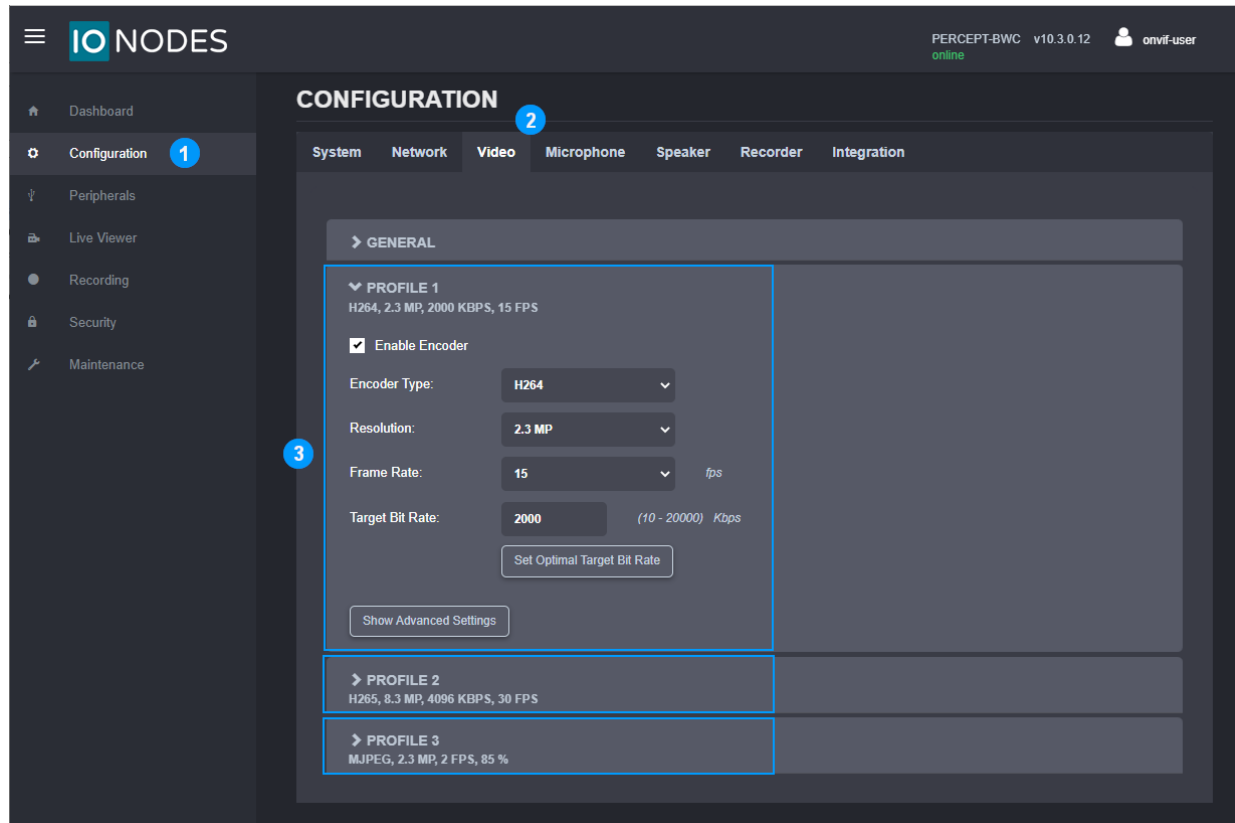
The PERCEPT Body Camera includes orientation metadata used by some client software to stabilize dewarped video. This feature is not supported by XProtect® and must be disabled in the body camera.



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 XProtect®.

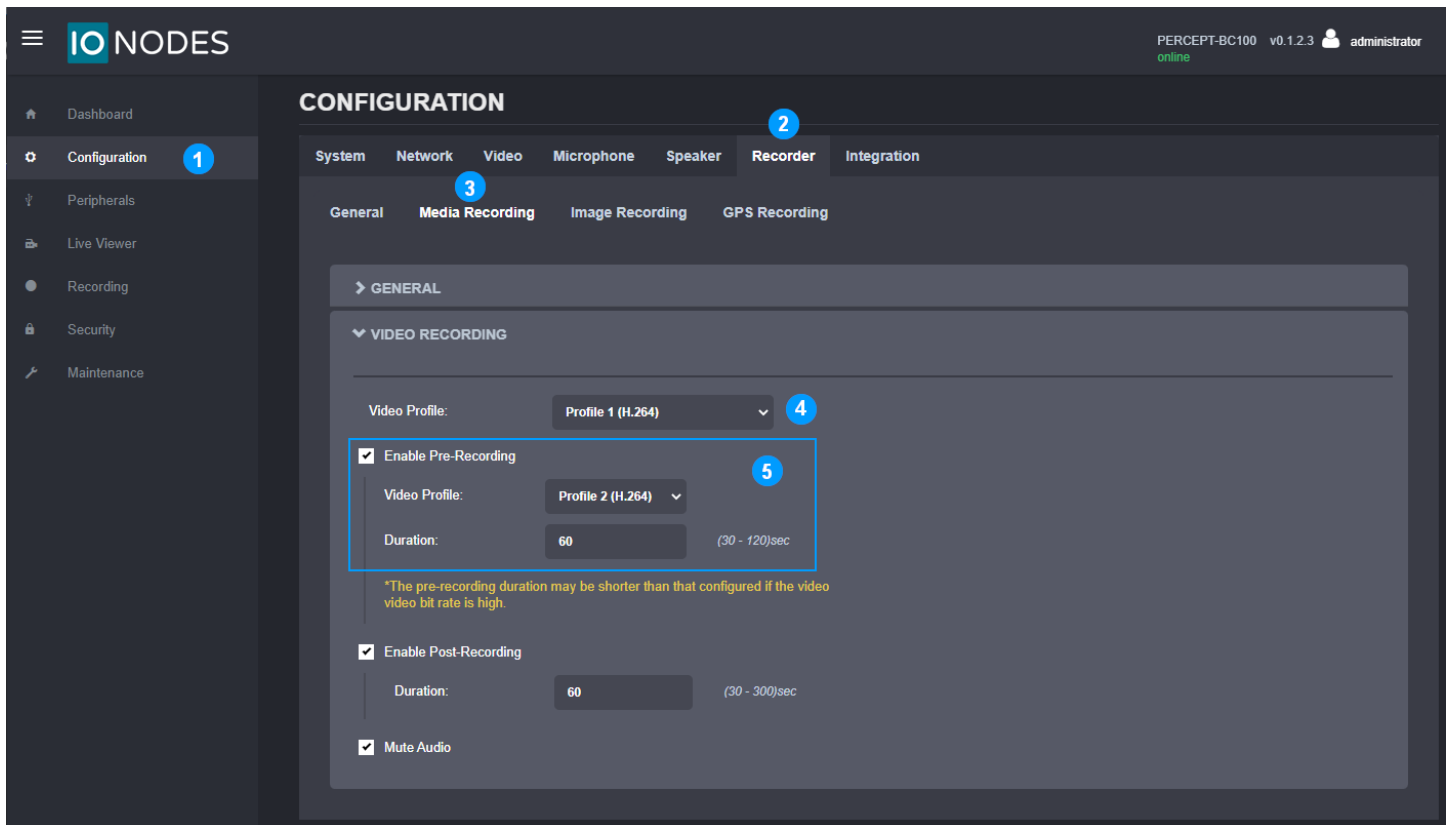


1. From the **Configuration** page
2. Select the **Video** tab
3. Enable and configure each video profile. Recommended settings are:
 - a. PROFILE 1 (Recording Stream):
 - i. **Encoder Type: H264**
 - ii. **Resolution: 6 MP**
 - iii. **Frame Rate: 30 fps**
 - iv. **Target Bit Rate: 8000 kbps**
 - v. **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): **Encoder Type: MJPEG**

Note:	The <i>Encoder Type</i> (codec) and profile's Enabled status are detected by XProtect® when adding the body camera. These settings must therefore be configured in the PERCEPT Body Camera before adding it to XProtect®. Changing <i>Encoder Type</i> requires rebooting the device.
Note:	Once added to XProtect®, video profile settings such as resolution, frame rate, etc shall be configured from within XProtect® Management Client.
Note:	H.264 is recommended for users that intend on viewing streams from XProtect® Web Client without XProtect® Mobile Server 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.

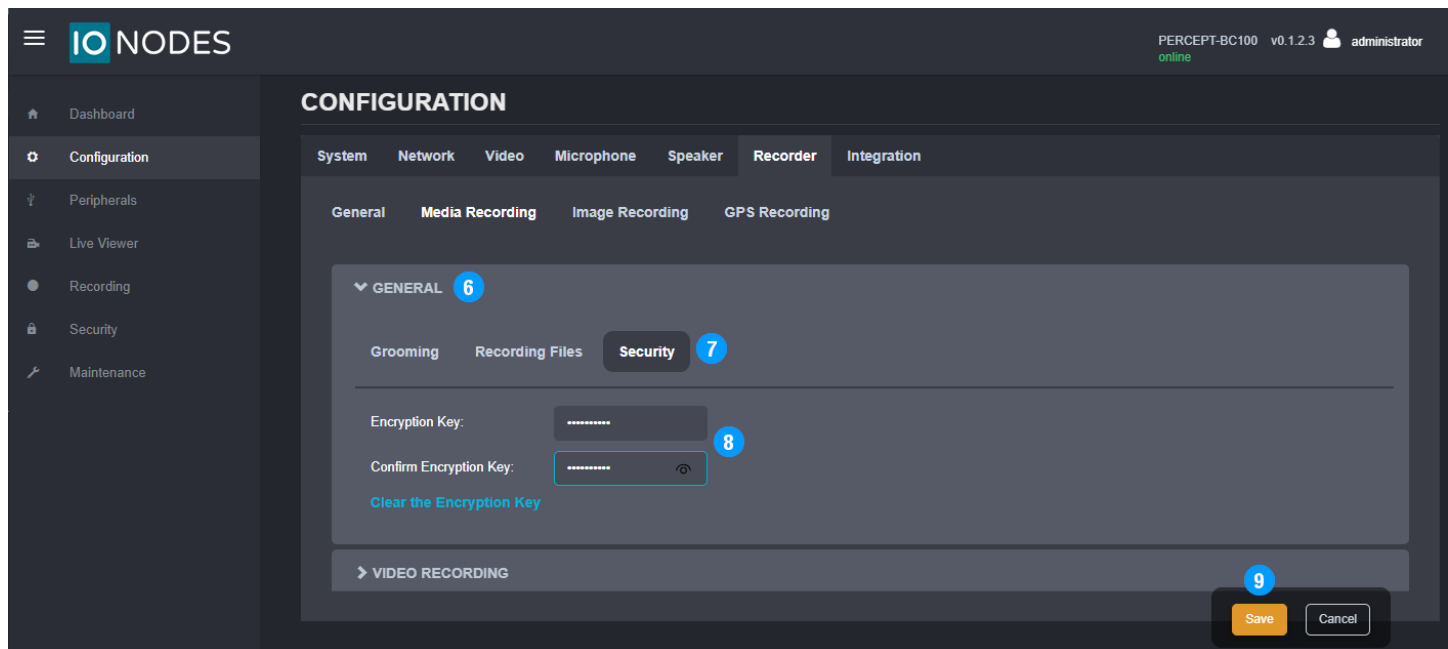
3.4 Setup local recording on the body camera



1. From the **Configuration** page
2. Select the **Recorder** tab
3. Select the **Media Recording** subtab
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)

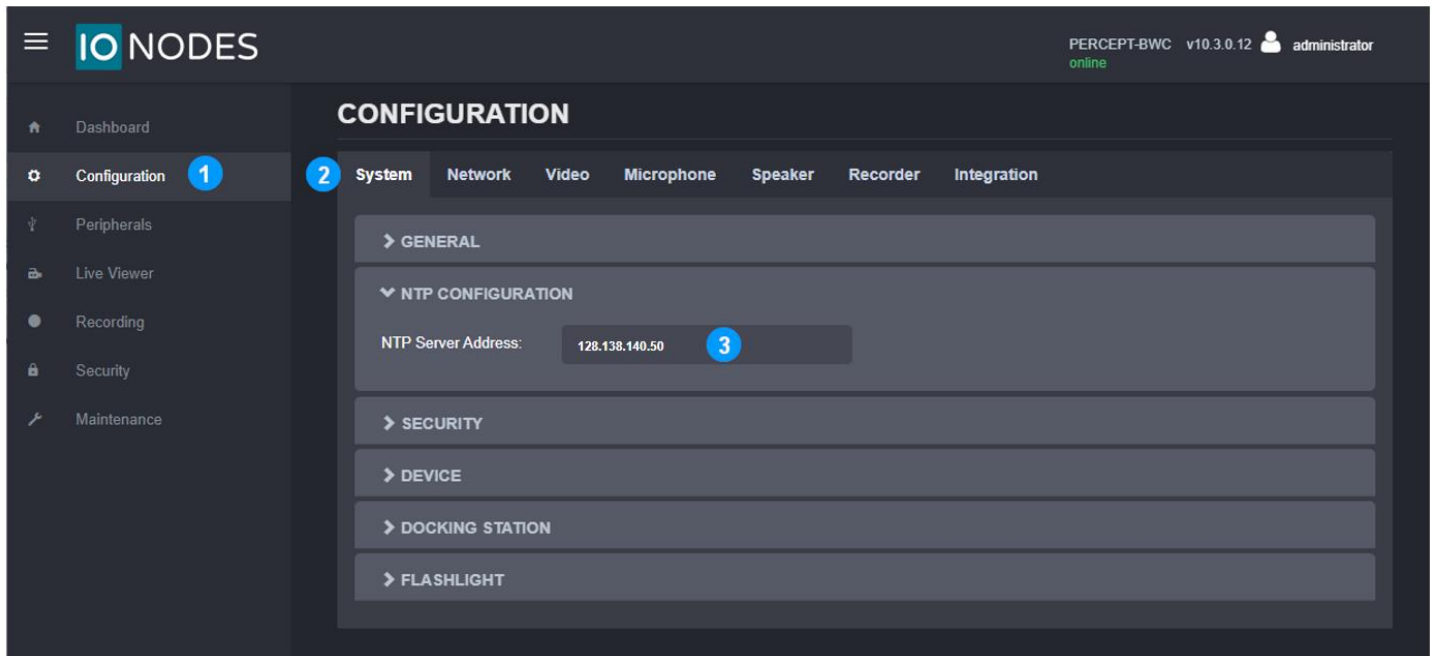
Note: When Pre-Recording is enabled, the camera is constantly encoding and buffering video. If Pre-Recording is not required, disabling it significantly increases battery life. If Pre-Recording is set to the high bitrate profile, the camera will overheat in certain environmental conditions.

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 on the body camera



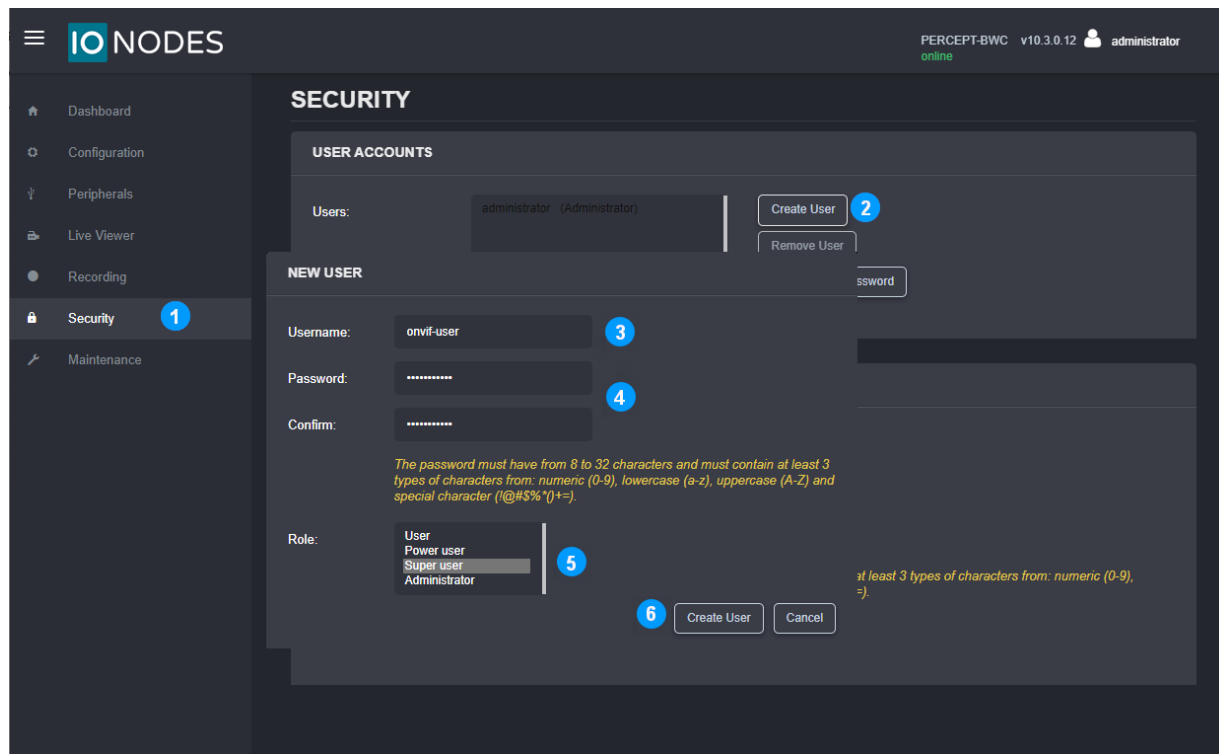
1. From the **Configuration** page
2. Select the **System** tab
3. In the **NTP Configuration** section, enter the IP address of the network time server used by Milestone XProtect® server(s) to synchronize clocks

Note: Time synchronization ensures media recorded on PERCEPT Body Cameras' SD cards and later transferred to XProtect® are accurately timestamped.

Note: By configuring its time service, any computer running Windows® can act as the NTP server for all devices connected to the surveillance LAN. PERCEPT Body Cameras that connect to the LAN directly or via VPN can keep their clocks synchronized with XProtect® using this approach.

3.6 Create a new dedicated ONVIF user (recommended)

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



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 integrate the PERCEPT Body Camera in XProtect®.

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 TP-Link's Omada VPN Router; more specifically, the entry model of the series, the ER605 v2. 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 TP-Link Omada Gigabit Multi-WAN VPN Router web interface. The left sidebar contains a navigation menu with the following items: Status, Quick Setup, Network, Preferences, Transmission, Firewall, Behavior Control, VPN (expanded), IPsec, L2TP (highlighted with a blue circle 1), PPTP, OpenVPN, Users, Authentication, Services, System Tools, and Logout. The main content area is titled 'L2TP Server Settings' and has a tabbed interface with 'L2TP Server' (highlighted with a blue circle 2), 'L2TP Client', 'Global Config', and 'Tunnel List'. Below the tabs 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 ---. To the right of the table are '+ Add' and '- Delete' buttons. Below the table is a configuration form for the selected L2TP server. The form has fields for WAN (WAN/LAN1), IPsec Encryption (Encrypted), Pre-shared Key (SuperSecretKey), and Status (checked Enable). There are OK and Cancel buttons at the bottom of the form. A blue circle 3 is next to the '+ Add' button, and a blue circle 4 is next to the OK button.

ID	WAN	IPsec Encryption	Status	Operation
1	WAN/LAN1	Encrypted	Enabled	---

WAN: WAN/LAN1
IPsec Encryption: Encrypted
Pre-shared Key: SuperSecretKey (1-128 characters)
Status: ☒ Enable
OK Cancel

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 interface, the DHCP server function is enabled in our example.

The screenshot shows the TP-Link web interface for an Omada Gigabit Multi-WAN VPN Router (ER605). The interface is divided into a left sidebar and a main content area. The sidebar contains a 'Network' menu with options like WAN, LAN, IPTV, MAC, Switch, VLAN, IPV6, and USB. The 'LAN' option is highlighted with a blue circle labeled '1'. The main content area has tabs for 'LAN', 'DHCP Client List', and 'Address Reservation'. The 'LAN' tab is selected, and a 'Network List' table is displayed. The table has columns for ID, Name, Vlan, IP Address, Subnet Mask, DHCP Server, DHCP Relay, and Operation. A single entry is shown for LAN with ID 1, IP 10.190.0.1, and Subnet Mask 255.255.0.0. A blue circle labeled '2' points to the 'LAN' tab, and a blue circle labeled '3' points to the '+ Add' button. Below the table, the configuration form for the selected LAN is shown. It includes fields for Name (LAN), IP Address (10.190.0.1), Subnet Mask (255.255.0.0), and Vlan (1). The DHCP section is expanded, showing 'DHCP Mode' set to 'DHCP Server' and 'Status' set to 'Enable'. Other fields include Starting IP Address (10.190.0.5), Ending IP Address (10.190.0.199), Lease Time (2880 minutes), and Default Gateway, Domain, DNS, and Secondary DNS (all optional). A blue circle labeled '3' points to the '+ Add' button. At the bottom, there are 'OK' and 'Cancel' buttons.

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	---

DHCP

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 shows the TP-Link Omada Gigabit Multi-WAN VPN Router web interface. The top navigation bar includes the TP-Link logo and the router model 'ER605'. The left sidebar contains a menu with options like Status, Quick Setup, Network, Preferences, Transmission, Firewall, Behavior Control, VPN, Authentication, Services, System Tools, and Logout. The main content area is titled 'Address Reservation' and features a table with columns for ID, MAC Address, IP Address, Description, Status, and Operation. A blue circle '4' highlights the 'Address Reservation' tab. A blue circle '5' highlights the '+ Add' button. A blue circle '6' highlights the 'Add' dialog box, which contains fields for MAC Address (C4-41-37-53-DA-4C), IP Address (10.190.1.1), Description (PERCEPT-TS), and a Status checkbox (checked). The dialog box also has OK and Cancel buttons.

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 single-address VPN IP pools, and a VPN user for each PERCEPT Body Camera, a connection from a specific VPN user will always be assigned the same IP address.

TP-Link logo

ER605
Omada Gigabit Multi-WAN VPN Router

VPN IP Pool

VPN IP Pool List

+ Add - Delete

<input type="checkbox"/>	ID	IP Pool Name	Starting IP Address	Ending IP Address	Operation
<input type="checkbox"/>	1	C4413753DA4C	10.190.1.1	10.190.1.1	---

IP Pool Name: C4413753DA4C

Starting IP Address: 10.190.1.1

Ending IP Address: 10.190.1.1

OK Cancel

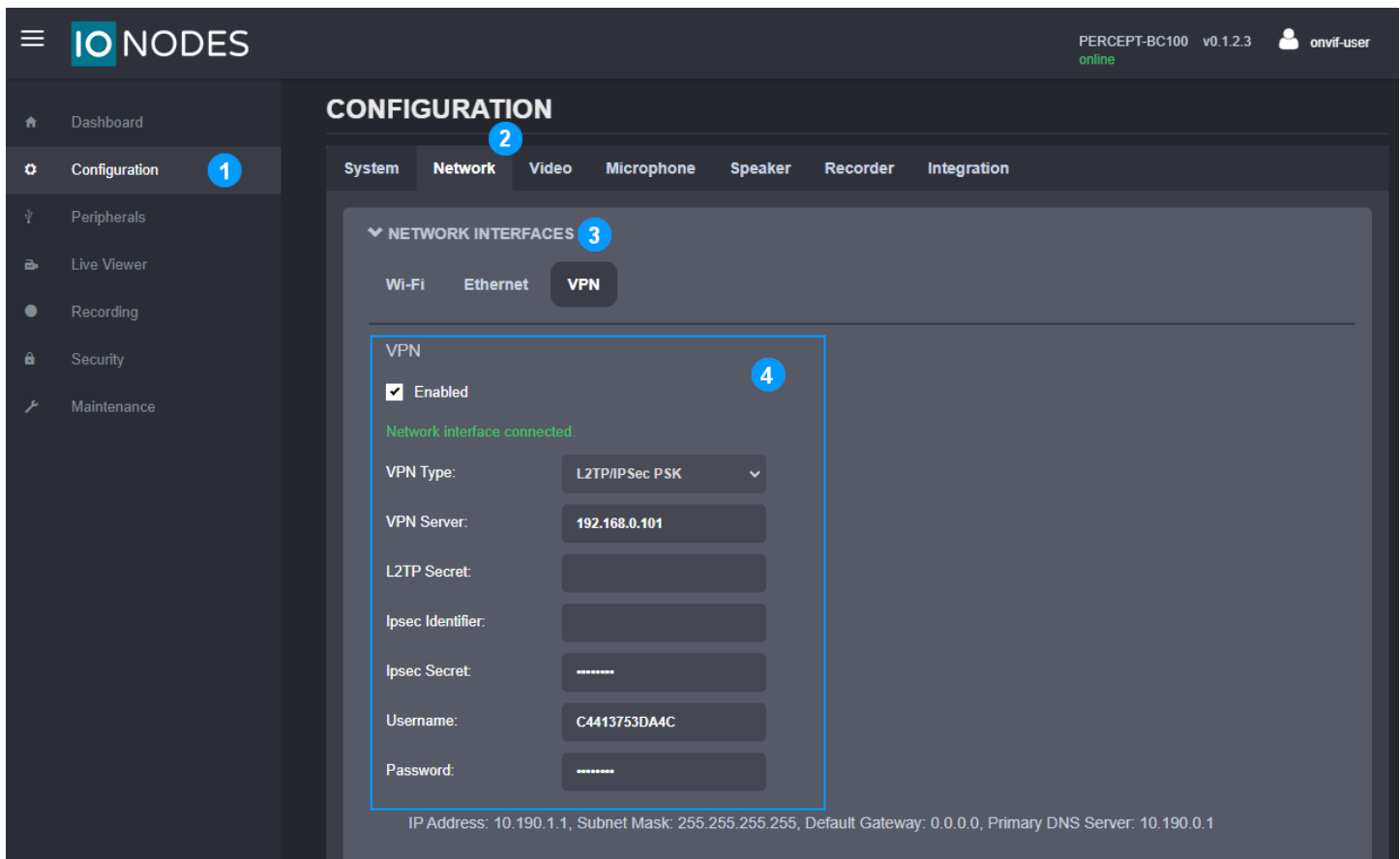
Copyright © 2021
TP-Link Corporation Limited.
All rights reserved.

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.

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

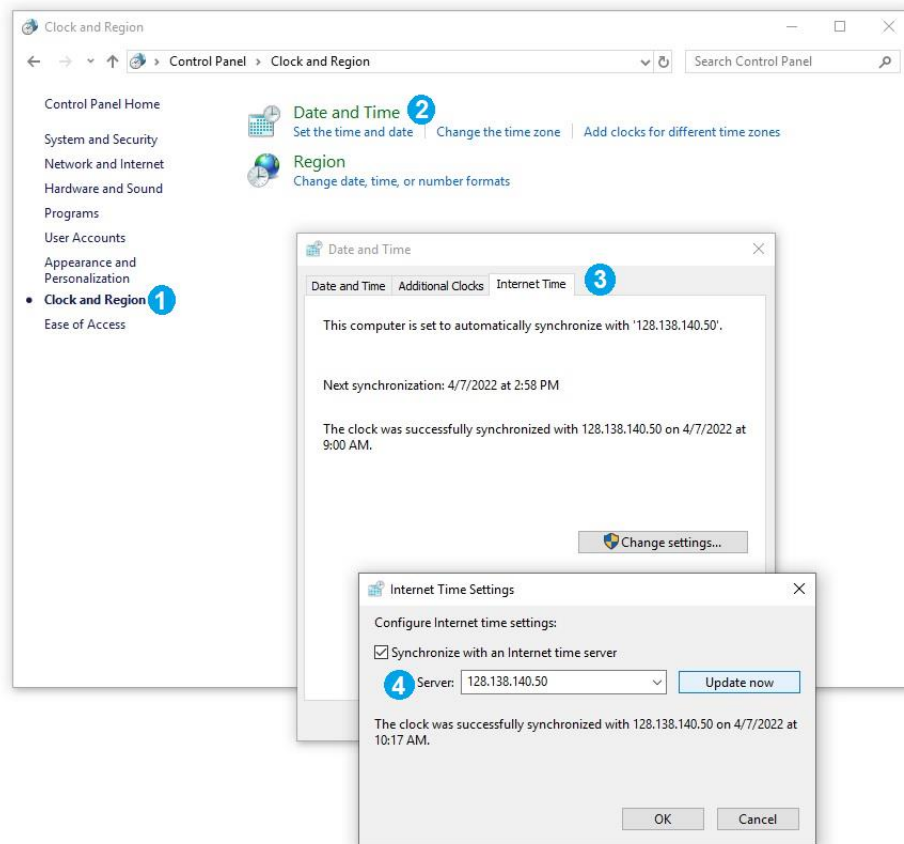
PERCEPT VPN settings shown are based on the VPN IP address reservation example above.



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 Configuring XProtect® Before Integration

5.1 Configure Time Synchronization



By default, XProtect® uses the time set on the computer where it is hosted. To change the time settings on the host PC:

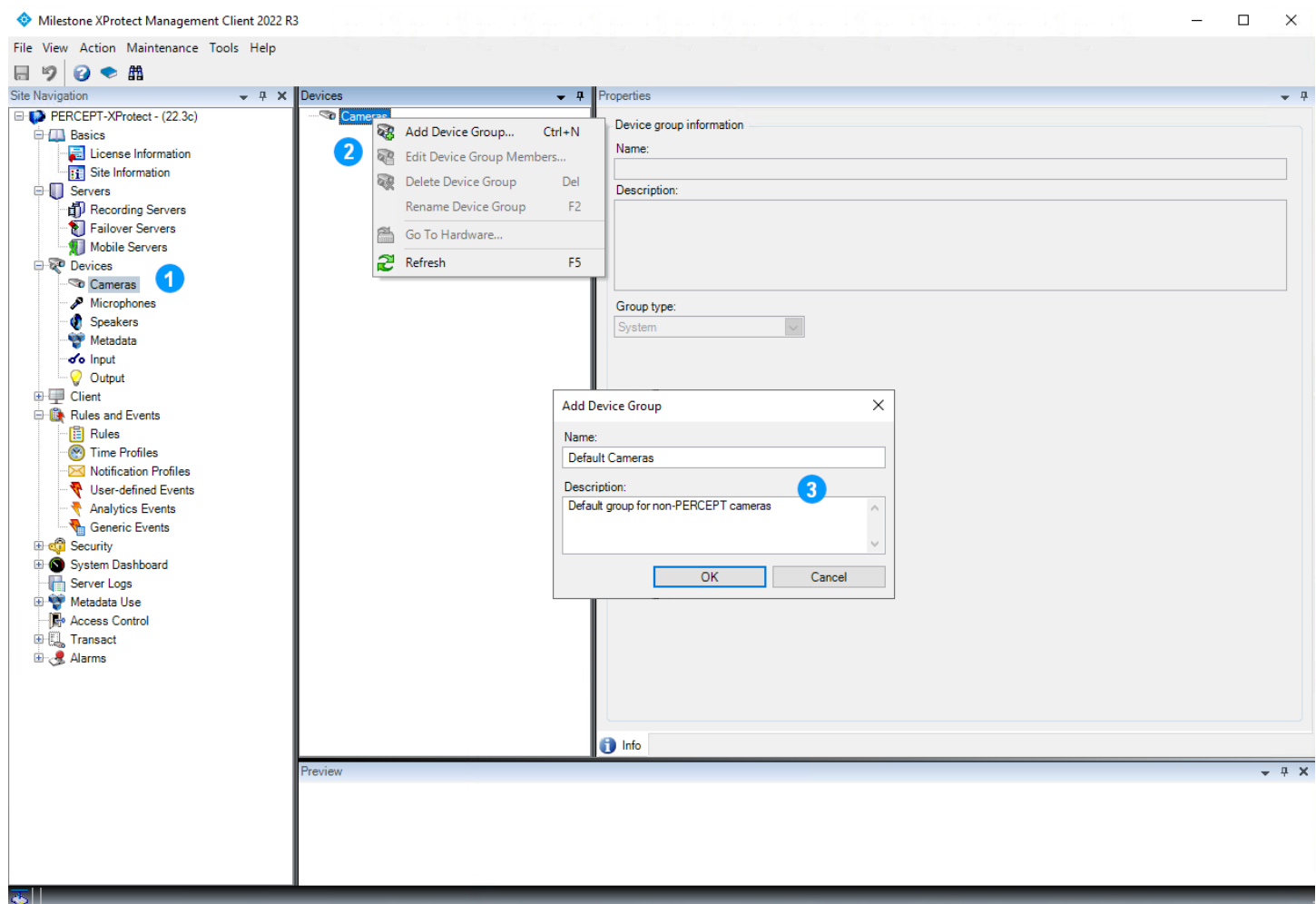
1. From the **Control Panel > Clock and Region**
2. Select the **Set the time and date** tab
3. Select the **Internet Time** and then go to **Change settings...**
4. Select the **Synchronize with an Internet time server** and select a valid time server

Note: PERCEPT Body Cameras shall use the same Network Time Protocol (NTP) server if it is accessible on the LAN. If the XProtect® server connects with this NTP server over the internet, the XProtect® server's time service can be configured to act as an NTP server for local devices.

5.2 Configure Device Groups

When devices are added to XProtect®, they must be added to specific device groups for Cameras, Microphones, Speakers, Metadata, Input and Output. To facilitate configuration and management, rules can then be applied to device groups instead of individual devices.

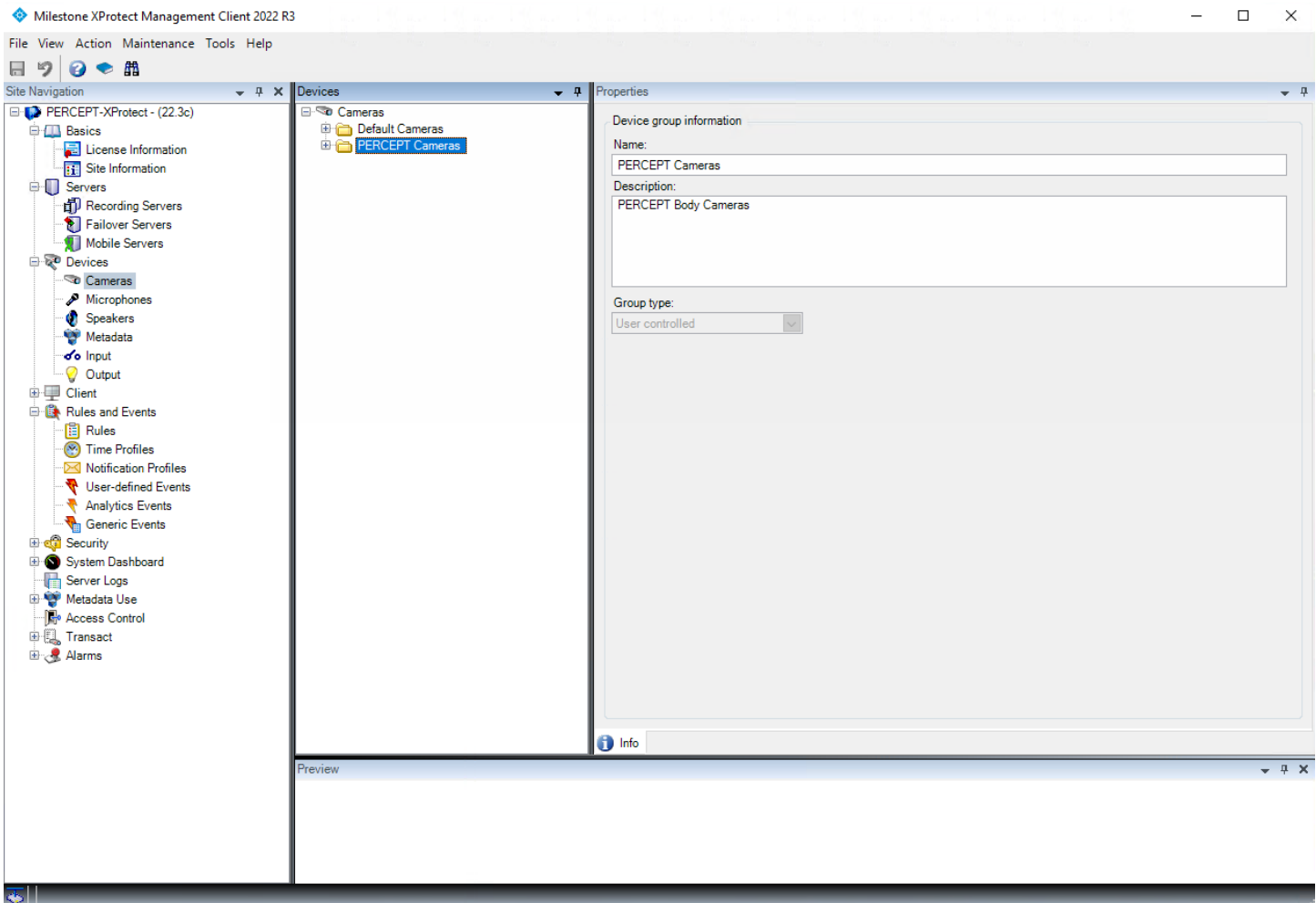
PERCEPT Body Camera's integration differs from typical fixed camera integration, using custom Rules to achieve the desired behavior. As a minimum, the recommended deployment requires creating specific device groups for PERCEPT Cameras and Microphones.



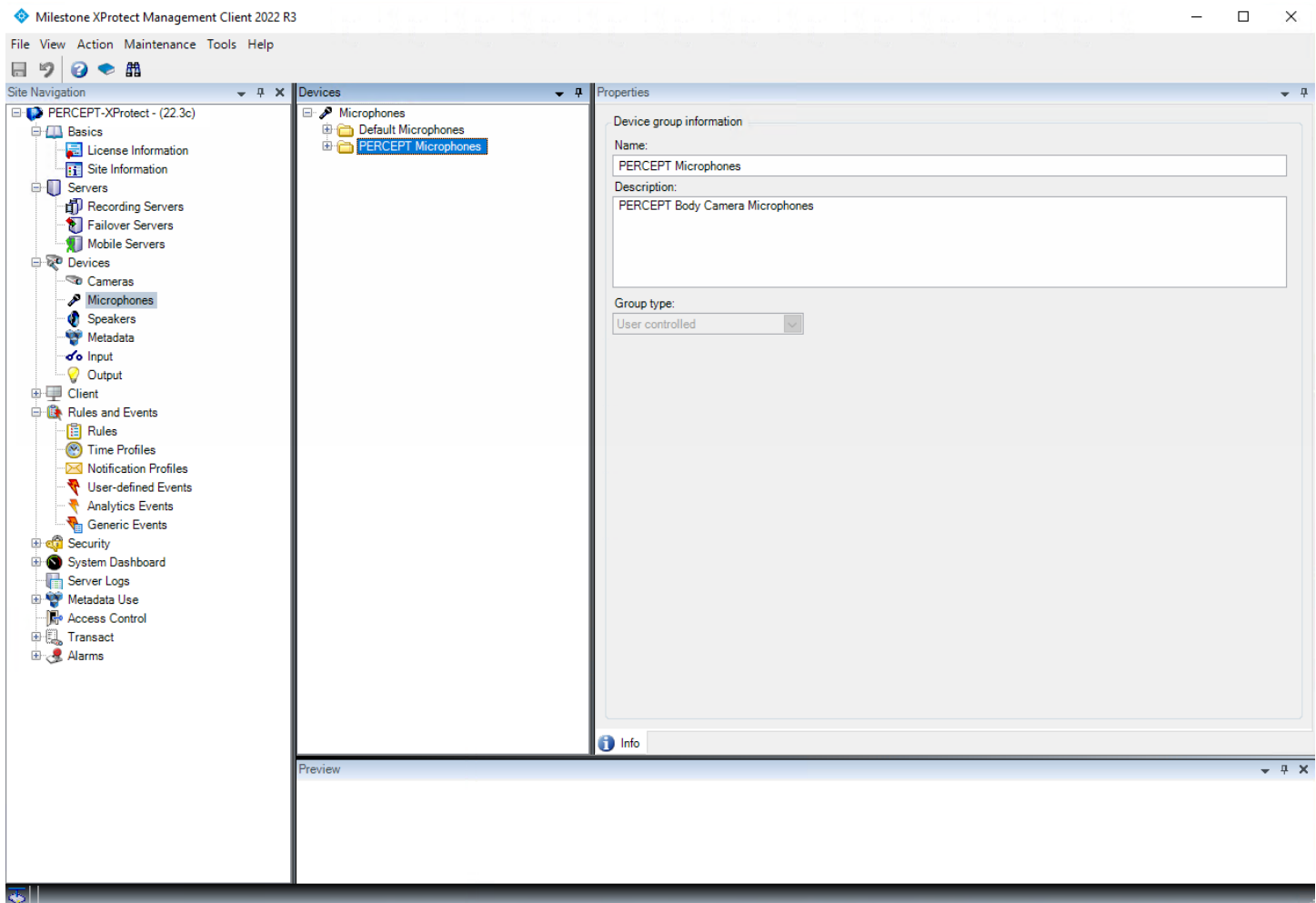
1. From the **XProtect® Management Client**'s left pane, select **Devices** > **Cameras**
2. In the **Devices** center pane, right-click on **Cameras** and select **Add Device Group** from the context menu pop-up
3. Add a default group for non-PERCEPT cameras and an optional description, then click OK.

Note: Adding a default camera group is only required when starting from a clean installation of XProtect®. If cameras are already integrated in the system, a default camera group was already created when adding the first camera.

4. Repeat the steps above, this time creating a Camera group for PERCEPT Cameras. Resulting groups would look like the image below.

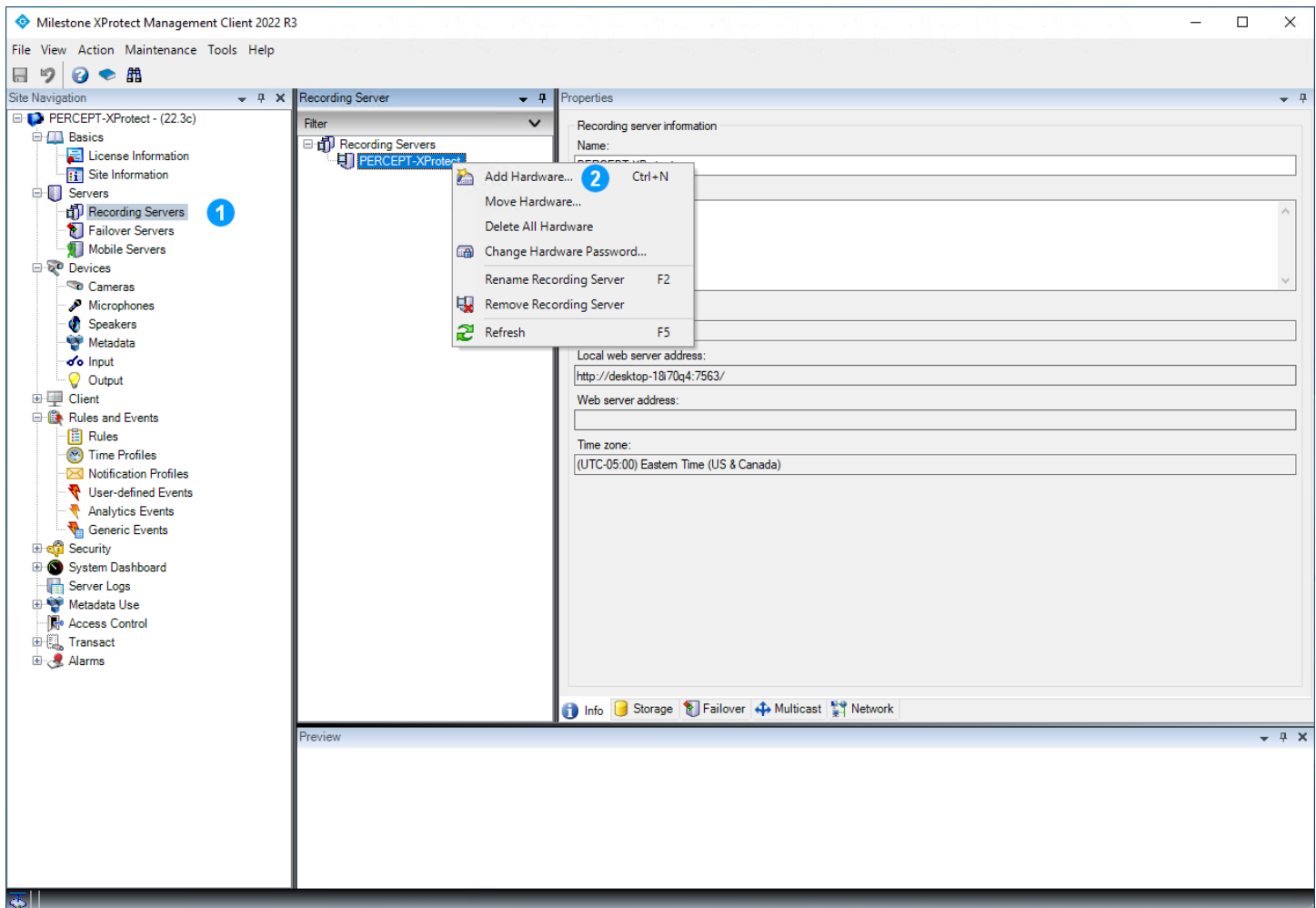


5. Repeat the steps above, this time creating Microphones' Default and PERCEPT groups. Resulting groups would look like the image below.

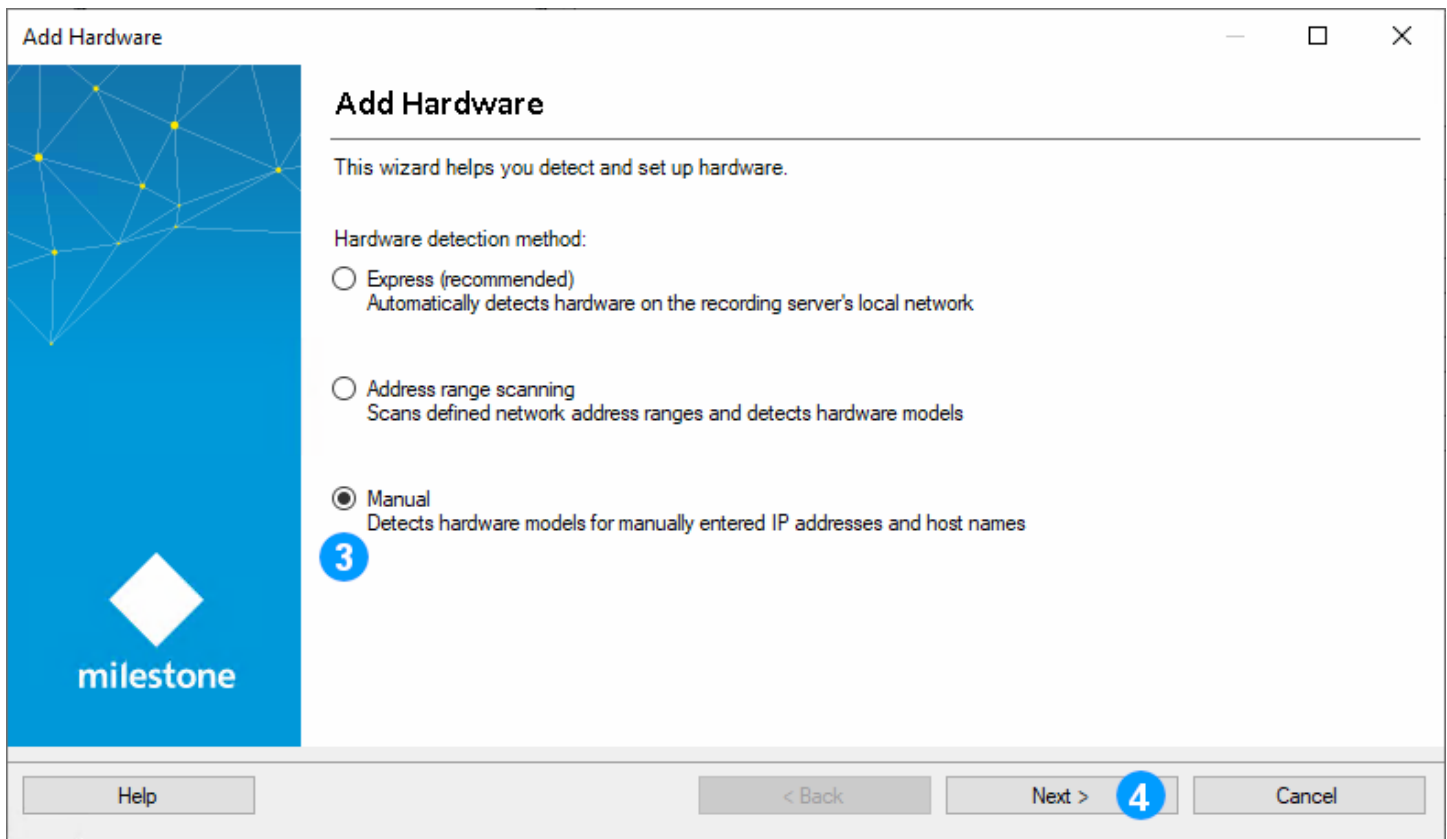


6. PERCEPT Body Camera speakers do not require specific rules, so they can be added to the Default speakers group. If no speaker device was already added in XProtect®, a Default Speakers group can be added at this time. Otherwise, it will be created when adding the first PERCEPT Body Camera.

6 Adding the PERCEPT Body Camera in XProtect®



1. In **XProtect® Management Client**, click on **Recording Servers**
2. Right-click on the recording server where you want to add the PERCEPT Body Camera and choose **Add Hardware** from the pop-up context menu



Add Hardware

This wizard helps you detect and set up hardware.

Hardware detection method:

- ☐ Express (recommended)
Automatically detects hardware on the recording server's local network
- ☐ Address range scanning
Scans defined network address ranges and detects hardware models
- ☒ **Manual**
Detects hardware models for manually entered IP addresses and host names

Help < Back Next > Cancel

3. Select **Manual**
4. Click **Next**

Add Hardware

Optionally, specify additional user credentials to connect with if the hardware is not using the factory defaults.

milestone

Include	User name	Password
<input checked="" type="checkbox"/>	(Factory default)	••••••••
<input checked="" type="checkbox"/>	admin	••••••••
<input checked="" type="checkbox"/>	onvif-user	••••••••

Add

Remove

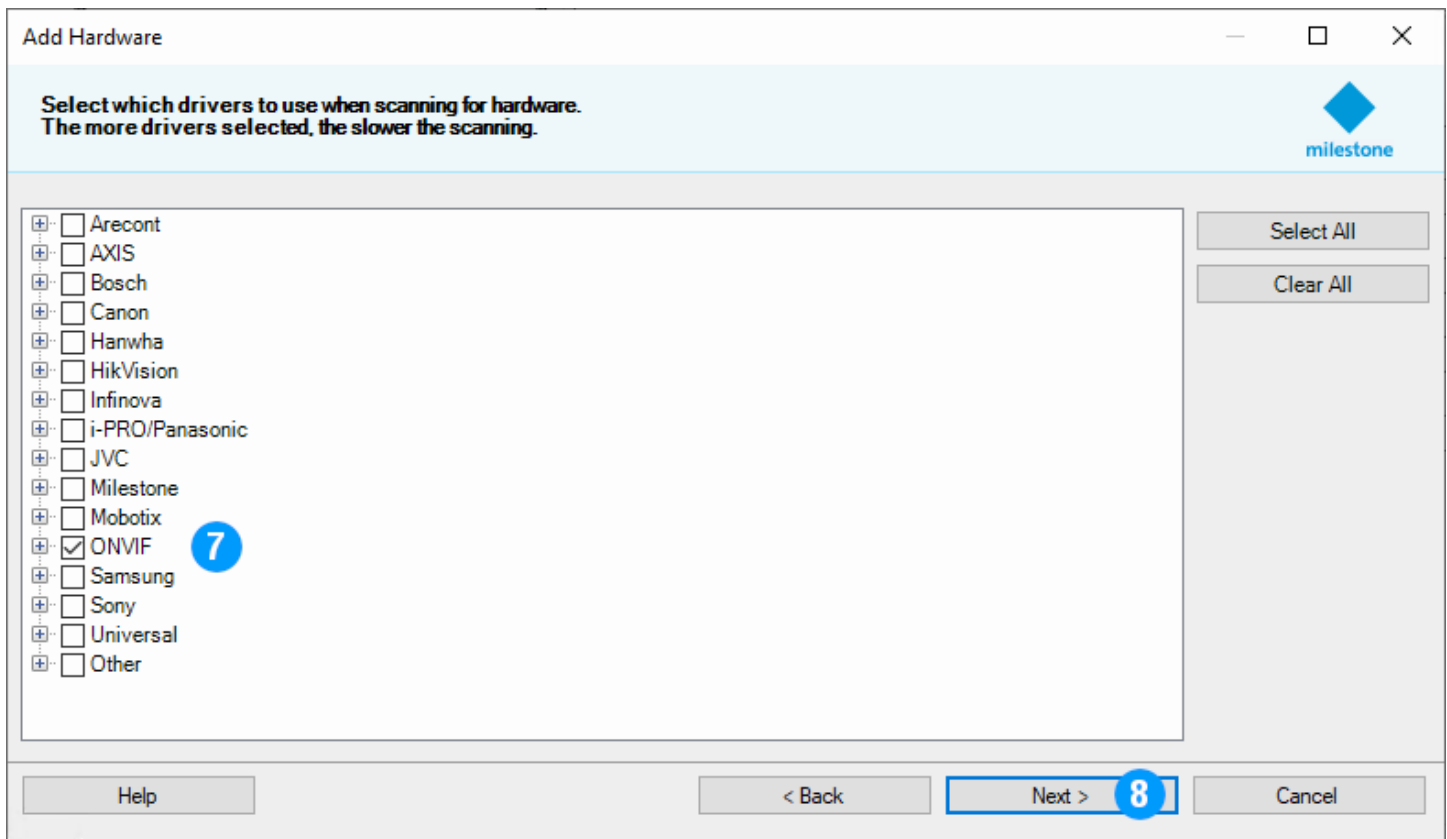
Help

< Back

Next >

Cancel


5. If PERCEPT Body Camera credentials do not already exist, select **Add** to create a new user to connect with the body camera, otherwise select existing credentials (see section 3.6)
6. Click **Next**



7. Select **ONVIF** in order to use the ONVIF generic driver for adding the body camera
8. Click **Next**

Add Hardware

Enter the network address and port of the hardware you want to add.
Optionally, select the hardware model to speed up detection.



	Address	Port	Use HTTPS	HTTPS port	Hardware model
▶	10.190.1.1	80	<input type="checkbox"/>	443	(Auto-detect) ▼

9

10


Help < Back Next > Cancel

9. Input the IP address of the body camera

10. Click **Next**

Add Hardware

Wait while your hardware is being detected.
Once detection has completed, select which hardware to add.



Stop

Detected hardware:

Add	Address	Port	Hardware model	Status
<input checked="" type="checkbox"/>	10.190.1.1	80	IONODES PERCEPT-BC100-NA (ONVIF)	✓ Success

☒ Show hardware running on other recording servers

Help < Back Next > Cancel

11. XProtect® will show a **Success** status message if the IP address and credentials are valid
12. Click **Next**, XProtect® will show another successful status message if the PERCEPT Body Camera is added. Click **Next** in that dialog as well.

Add Hardware

Hardware and cameras are enabled per default. Manually enable additional devices to be used. The hardware and its devices will be assigned auto-generated names. Alternatively, enter names manually.

Hardware name template:
Default

Device name template:
Default

☒ Hardware
☒ Camera
☒ Microphone
☒ Speaker
☐ Metadata
☐ Input
☐ Output

Hardware to Add	Enabled	Name
IONODES PERCEPT-BC100-NA - 10.190.1.1	<input type="checkbox"/>	
Hardware:	<input checked="" type="checkbox"/>	IONODES PERCEPT-BC100-NA (10.190.1.1)
Camera port 1:	<input checked="" type="checkbox"/>	IONODES PERCEPT-BC100-NA (10.190.1.1) - Camera 1
Microphone port 1:	<input checked="" type="checkbox"/>	IONODES PERCEPT-BC100-NA (10.190.1.1) - Microphone 1
Speaker port 1:	<input checked="" type="checkbox"/>	IONODES PERCEPT-BC100-NA (10.190.1.1) - Speaker 1
Metadata port 1:	<input type="checkbox"/>	IONODES PERCEPT-BC100-NA (10.190.1.1) - Metadata 1
Input port 1:	<input type="checkbox"/>	IONODES PERCEPT-BC100-NA (10.190.1.1) - Input 1
Input port 2:	<input type="checkbox"/>	IONODES PERCEPT-BC100-NA (10.190.1.1) - Input 2

Help

< Back

Next >

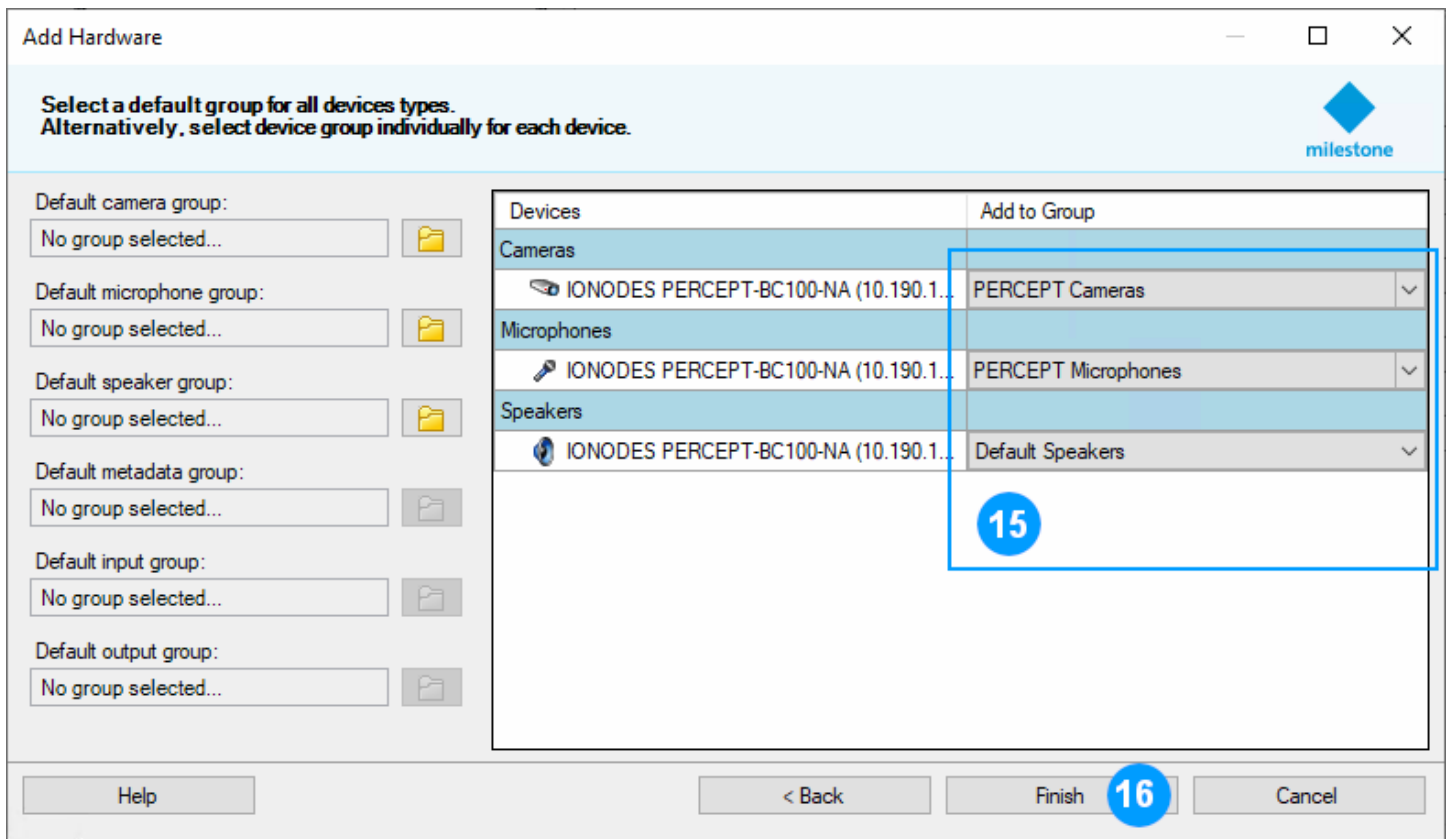
Cancel

13. Select which Device sub-components to enabled within XProtect®. For this deployment, enable the following:

- Hardware
- Camera port 1
- Microphone port 1
- Speaker port 1

14. Click **Next**

Note: It is possible to enable Input ports for XProtect® to receive events when the wearer presses buttons on the body camera. Since the PERCEPT Body Camera uses internal logic, such as same button with different press duration to start/stop recording, there is no one-to-one correlation between a button being pressed and a specific behavior. It is recommended to use ONVIF events instead.

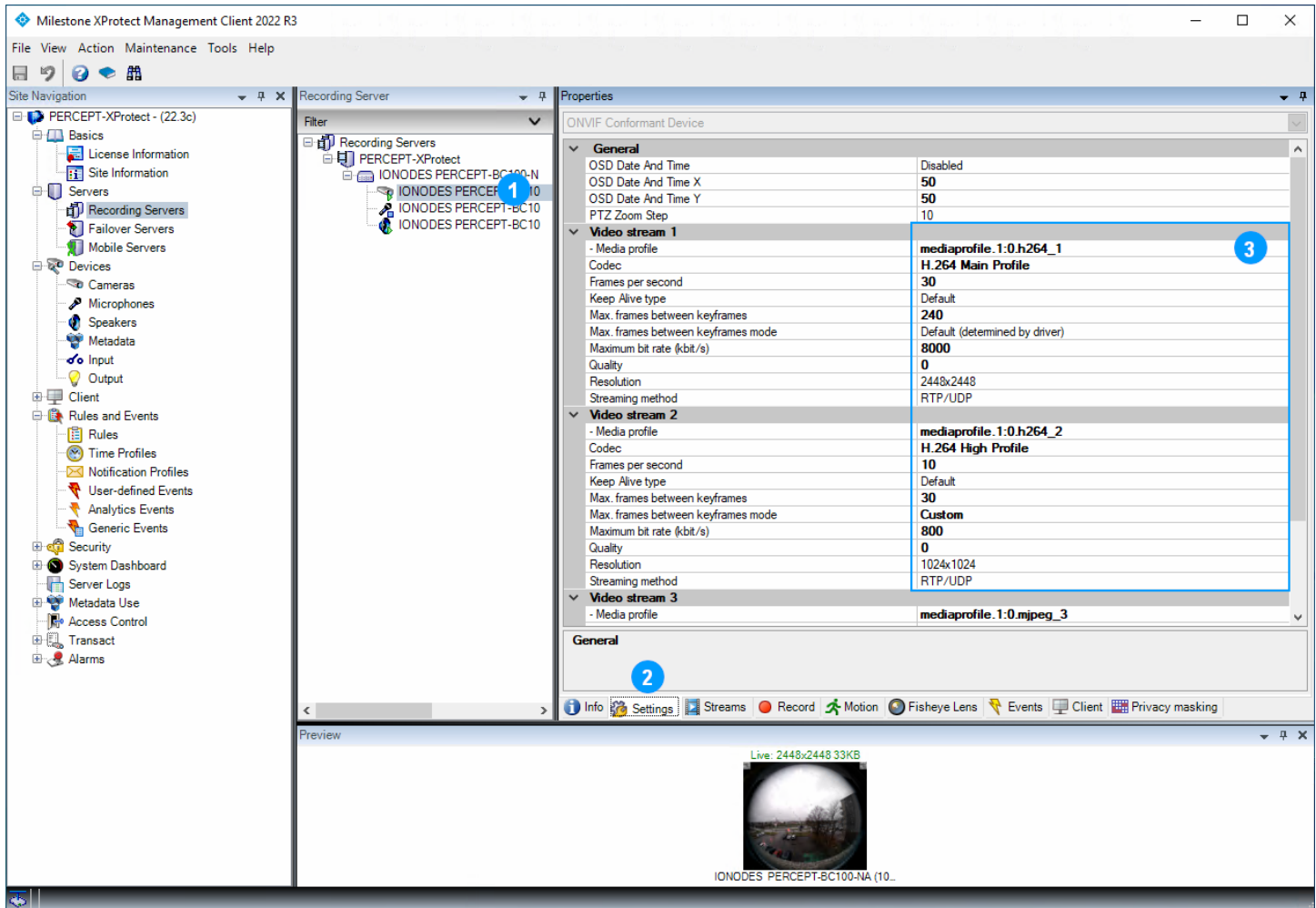


15. Assign each sub-component of the body camera to a Device group (a group can be created at this stage if it was not already as per section 5.2). PERCEPT Body Cameras and Microphones shall be assigned to PERCEPT-specific groups. PERCEPT Speakers can be assigned to the default group since no PERCEPT-specific rule is required for it.

16. Click **Finish**

6.1 Configure Camera

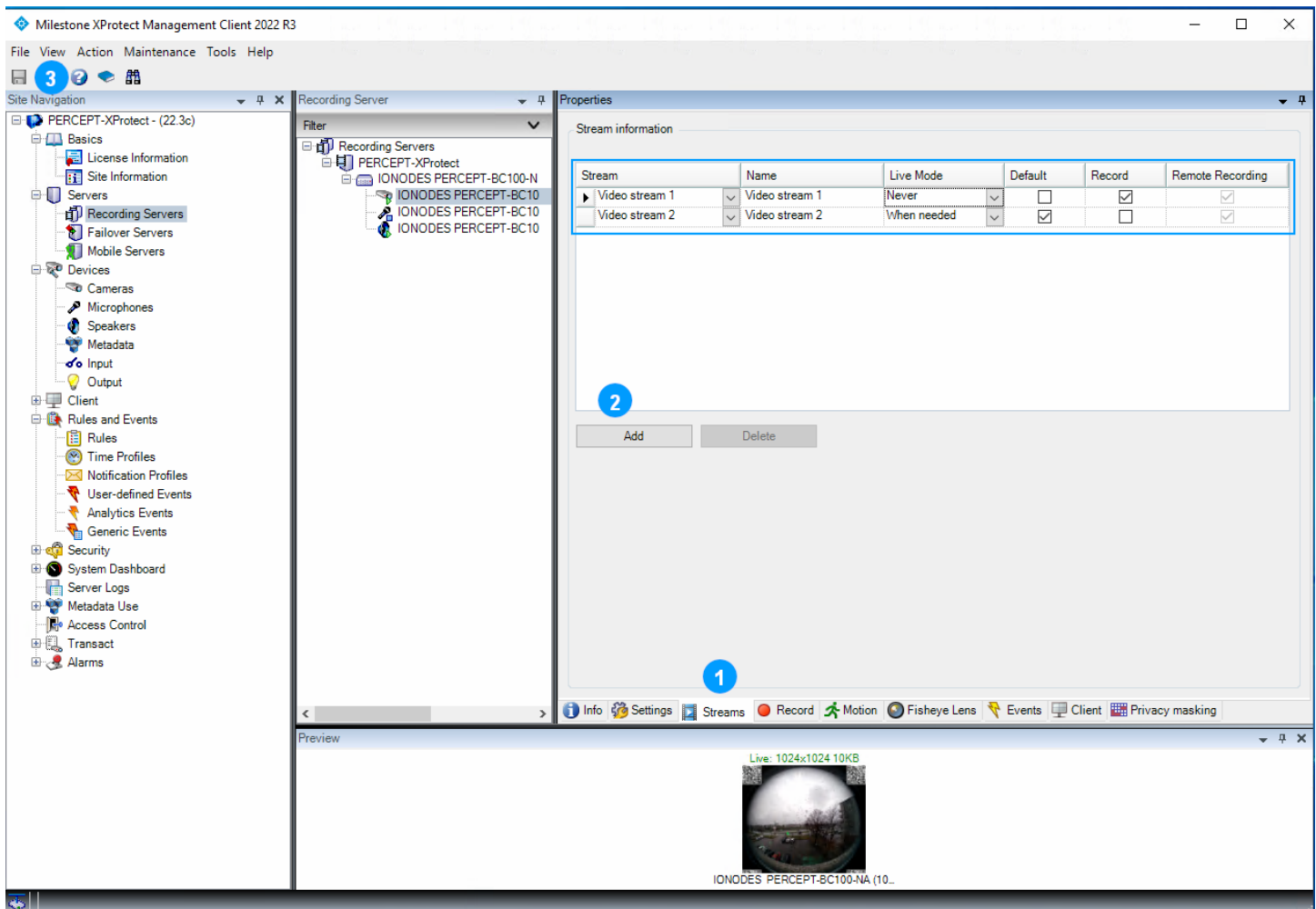
6.1.1 Settings



1. Expand the newly added PERCEPT Body Camera device and select its **Camera 1**
2. Select the **Settings** tab
3. Verify that the **Video stream 1** and **2** settings correspond to configuration from section 3.3.2. Once added in XProtect®, any change shall be done from within XProtect® Management Client; not from the PERCEPT Body Camera Web UI.

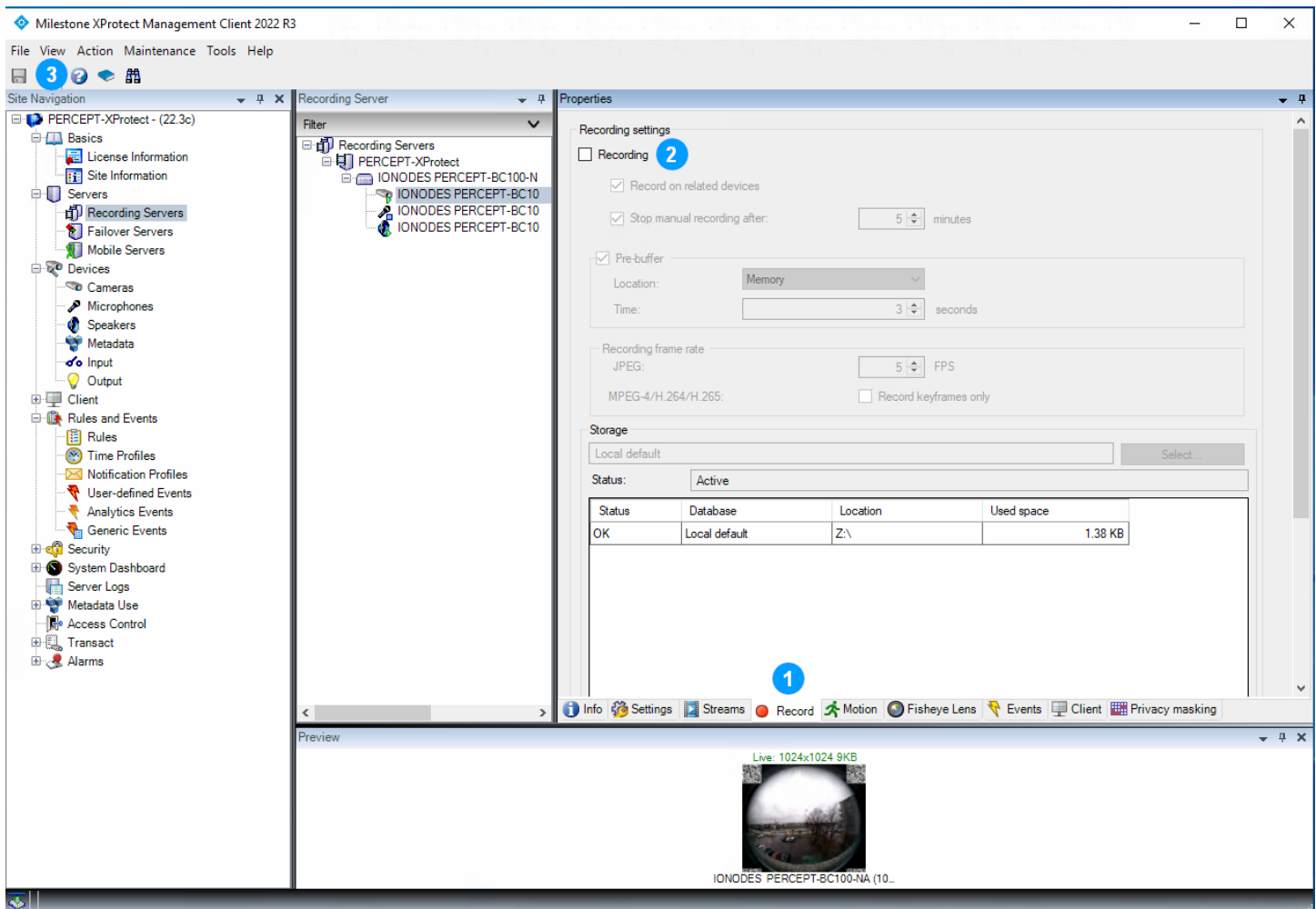
Note: Streaming method will impact live video when connected over LTE or low-strength Wi-Fi networks. Packet losses result in video artefacts over RTP/UDP, while with TCP-based protocols (RTP/RTSP/TCP or RTP/RTSP/HTTP/TCP) they result in inconsistent frame duration (jitter). It is recommended to use RTP/UDP.

6.1.2 Streams



1. Select the **Streams** tab
2. Only stream 1 is enabled by default. **Add** a Video stream then configure as follows:
 - a. **Video stream 1:**
 - i. **Live Mode:** Never
 - ii. **Default:** Unchecked
 - iii. **Record:** Checked
 - b. **Video stream 2:**
 - i. **Live Mode:** When needed
 - ii. **Default:** Checked
 - iii. **Record:** Unchecked
3. Click **Save**

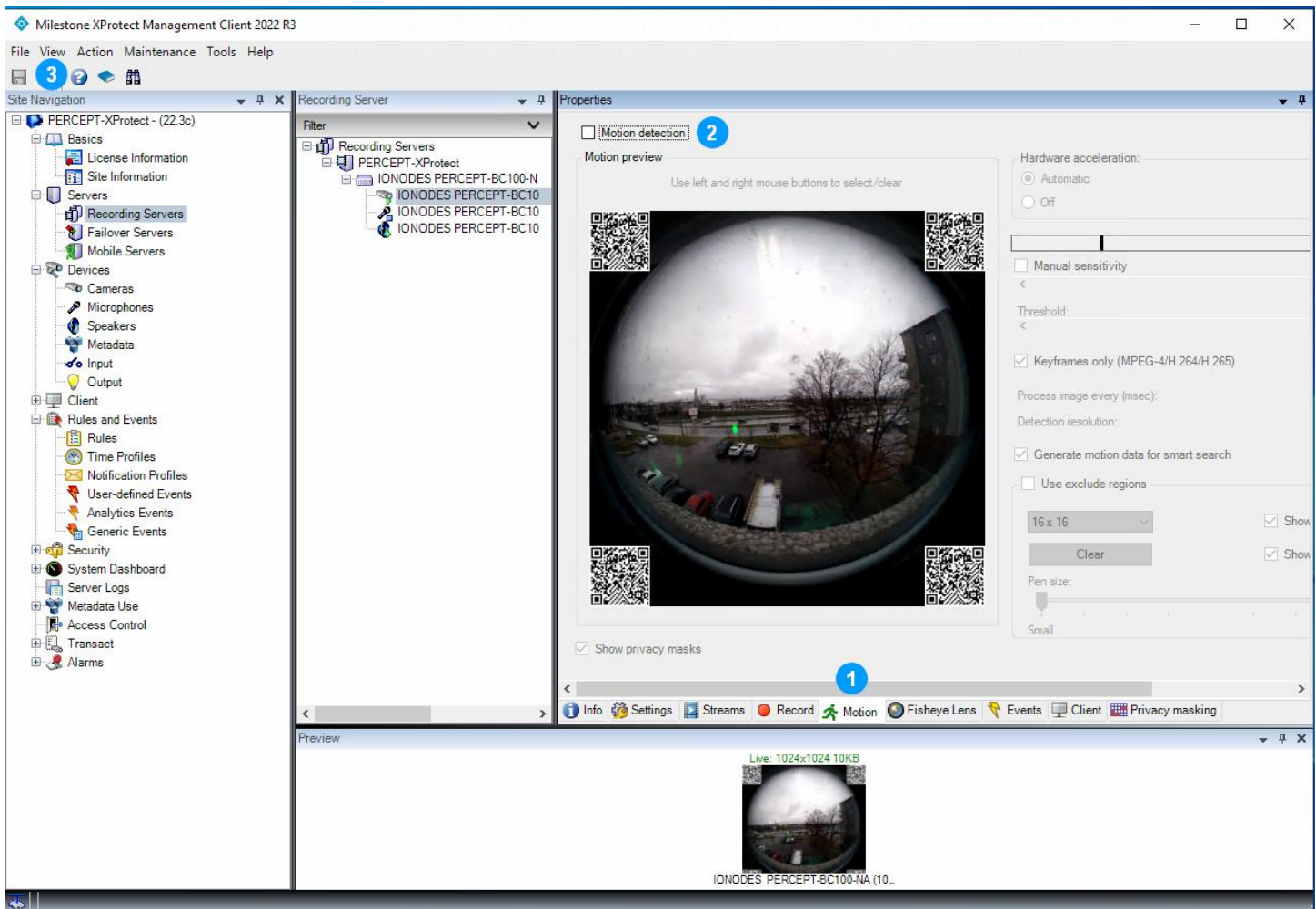
6.1.3 Record



1. Select the **Record** tab
2. Uncheck (disable) **Recording**
3. Click **Save**

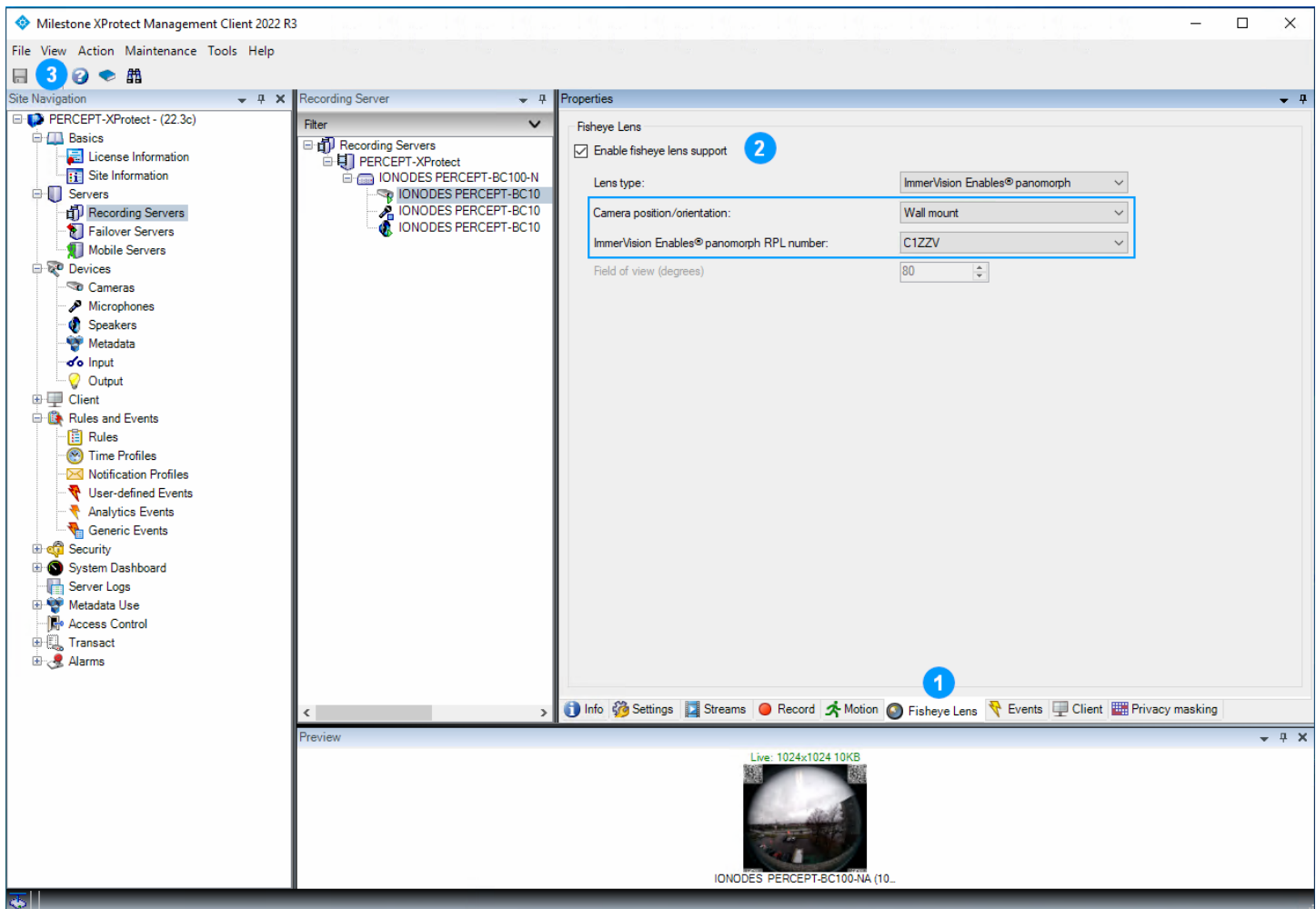
Note: If Recording is enabled, XProtect® always connects to the video stream configured for recording (high-bitrate stream), resulting in high bandwidth and data usage. The recommended deployment consists of disabling automatic recording functions and creating rules for Edge Storage transfer.

6.1.4 Motion



1. Select the **Motion** tab
2. Uncheck (disable) **Motion detection**
3. Click **Save**

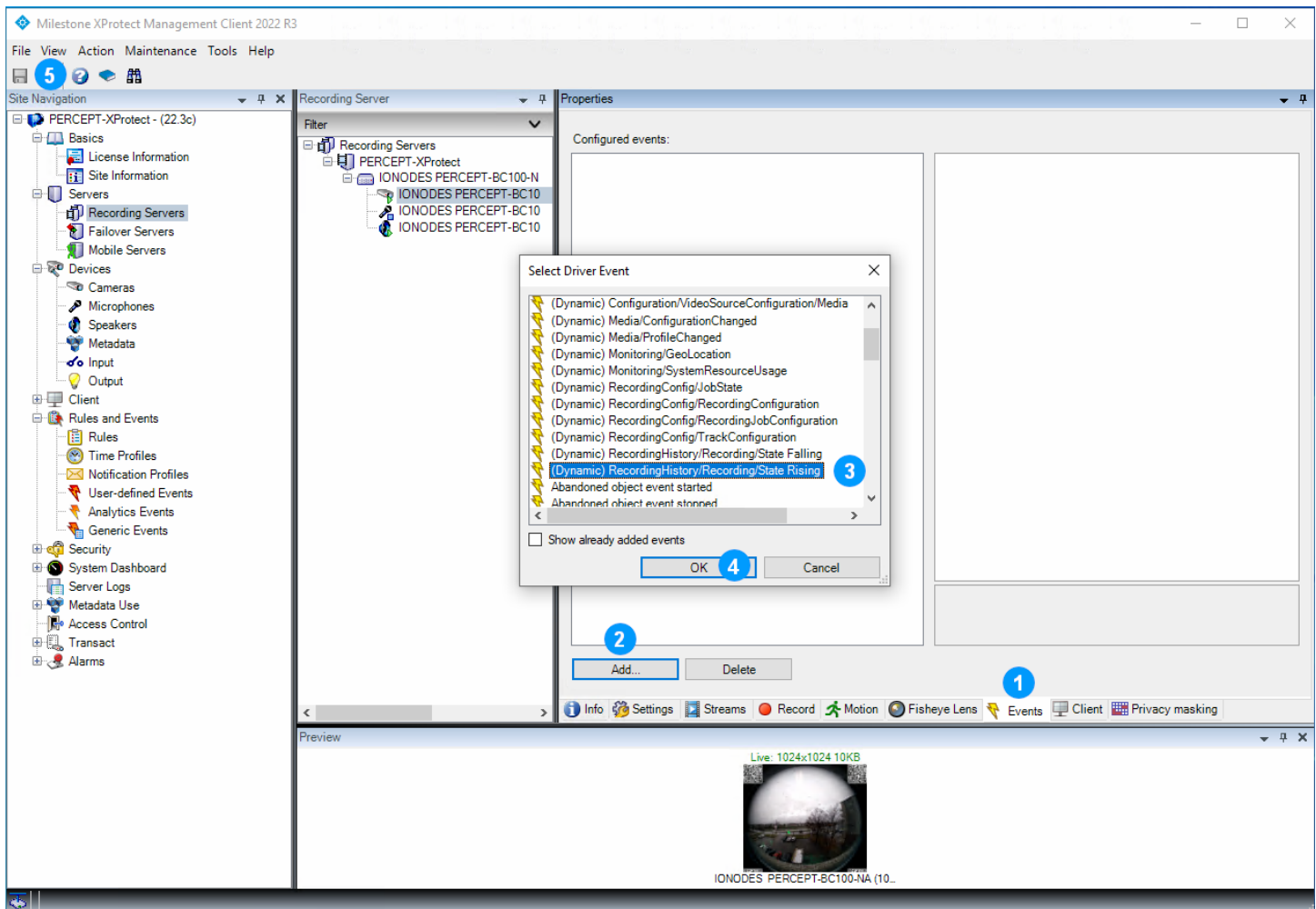
6.1.5 Fisheye Lens



1. Select the **Fisheye Lens** tab
2. Check **Enable fisheye lens support** and configure as follows:
 - a. **Camera position/orientation: Wall mount**
 - b. **ImmerVision Enables® Panomorph RPL number: C1ZZV**
3. Click **Save**

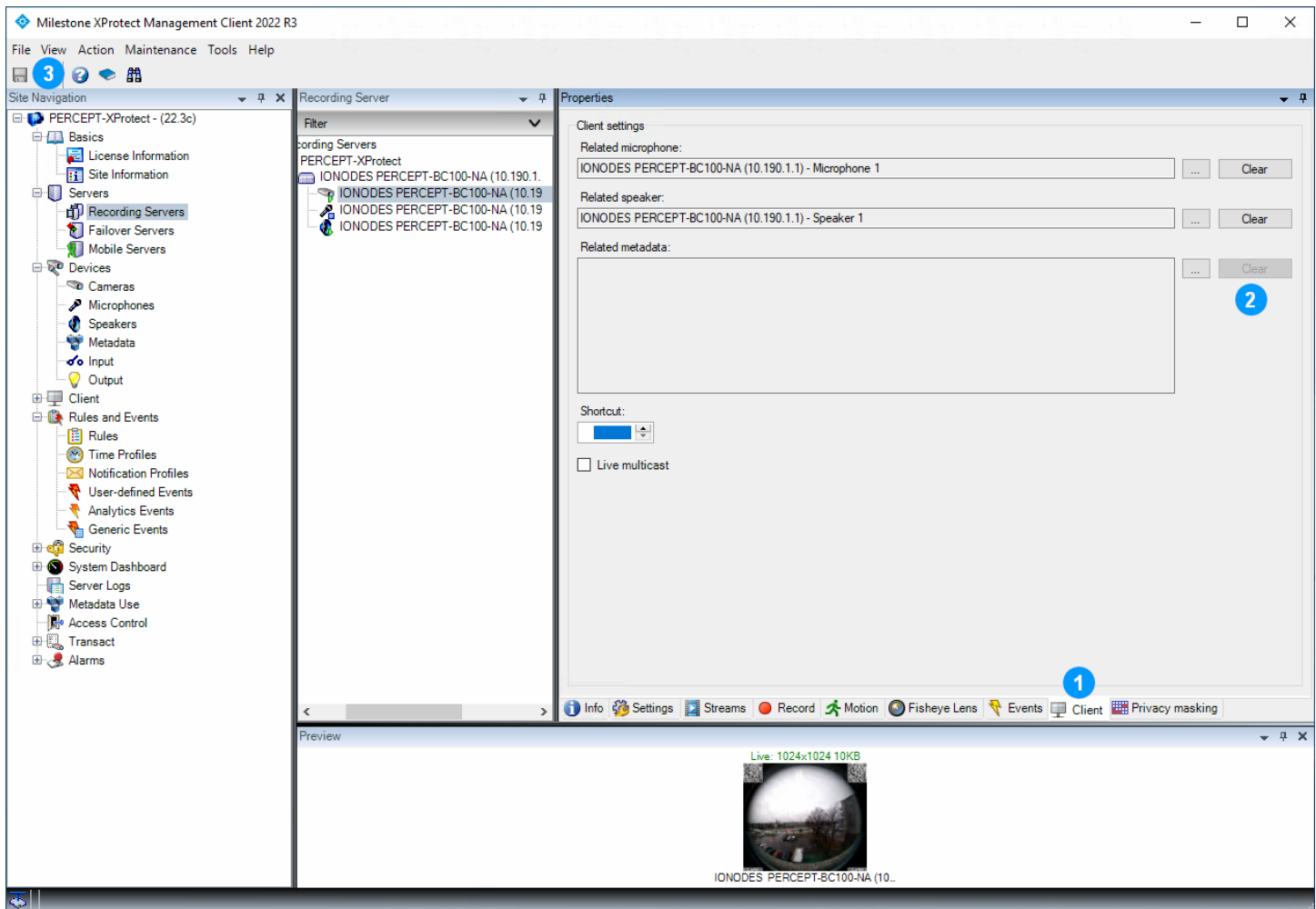
Warning: Some versions and service packs of XProtect® Smart Client may experience crashes toggling between Live and Playback, or when Pre/Post-Recording are at different resolutions with Panomorph-enabled cameras. Install latest service packs and/or disable Panomorph if encountering this issue and no service pack is available for the specific version and edition used.

6.1.6 Events



1. Select the **Events** tab
2. Click **Add**
3. In the pop-up menu, scroll to select **(Dynamic) RecordingHistory/Recording/State Rising**
4. Click **OK**
5. Click **Save**

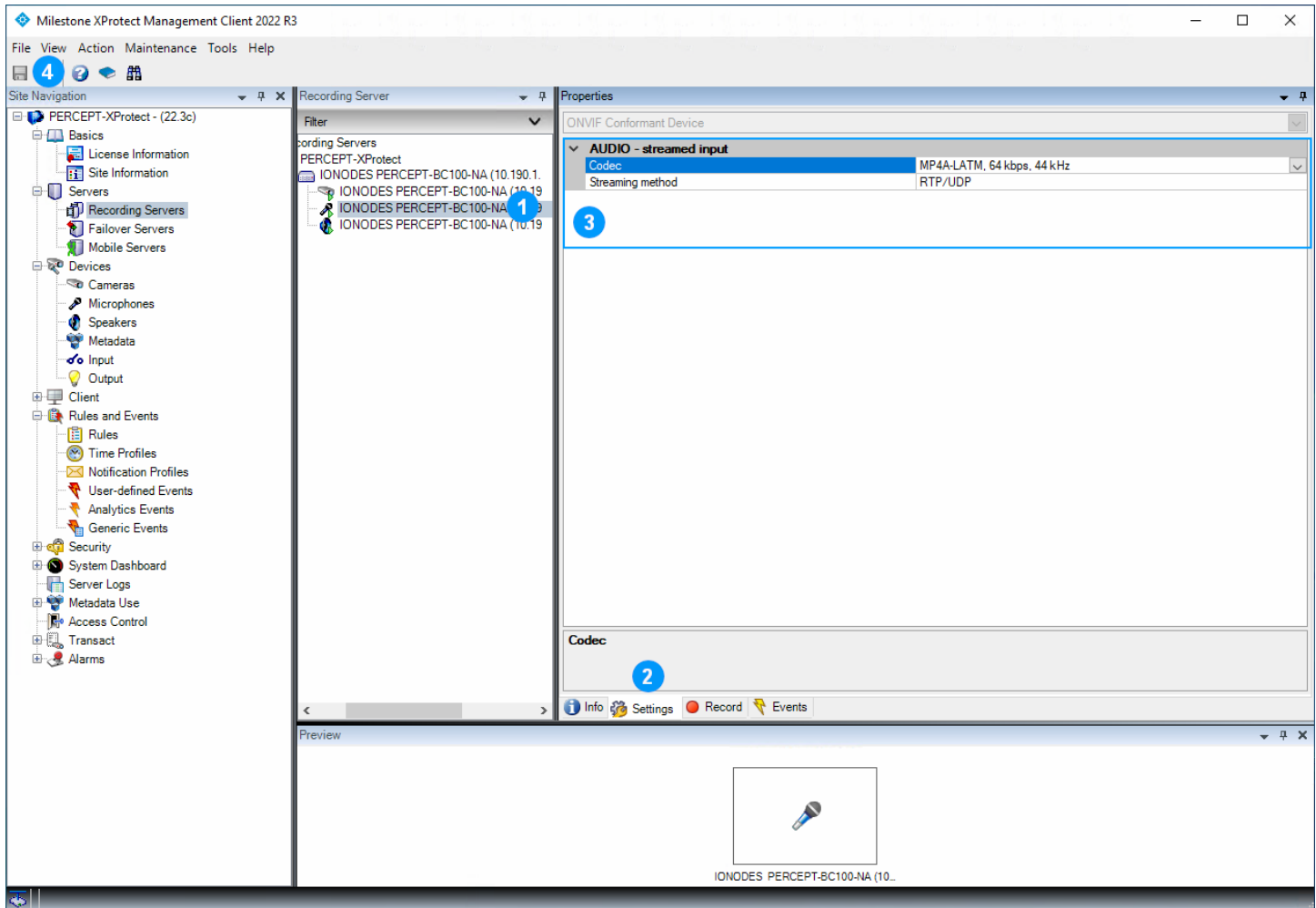
6.1.7 Client



1. Select the **Client** tab
2. In the **Related metadata** section, click **Clear** (shown already cleared above)
3. Click **Save**

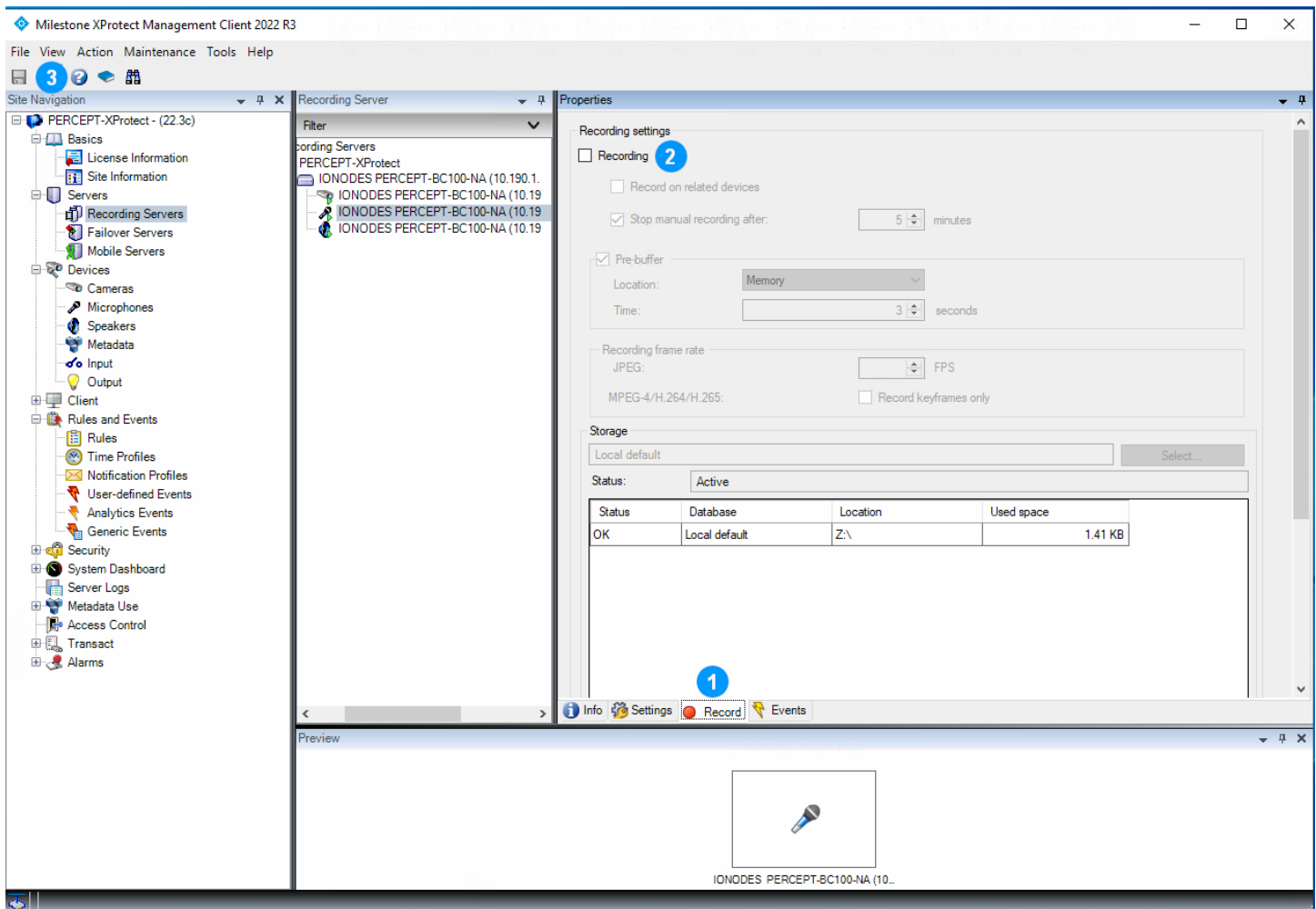
6.2 Configure Microphones

6.2.1 Settings



1. Select the PERCEPT Body Camera's **Microphone 1**
2. Select the **Settings** tab
3. Verify audio settings. XProtect® default settings are acceptable, a relatively low bitrate AAC (MP4A-LATM) at 32kHz or 44kHz is recommended (64kpbs, 44kHz shown above). Recommended **Streaming method** is **RTP/UDP**
4. **Save** if settings were modified

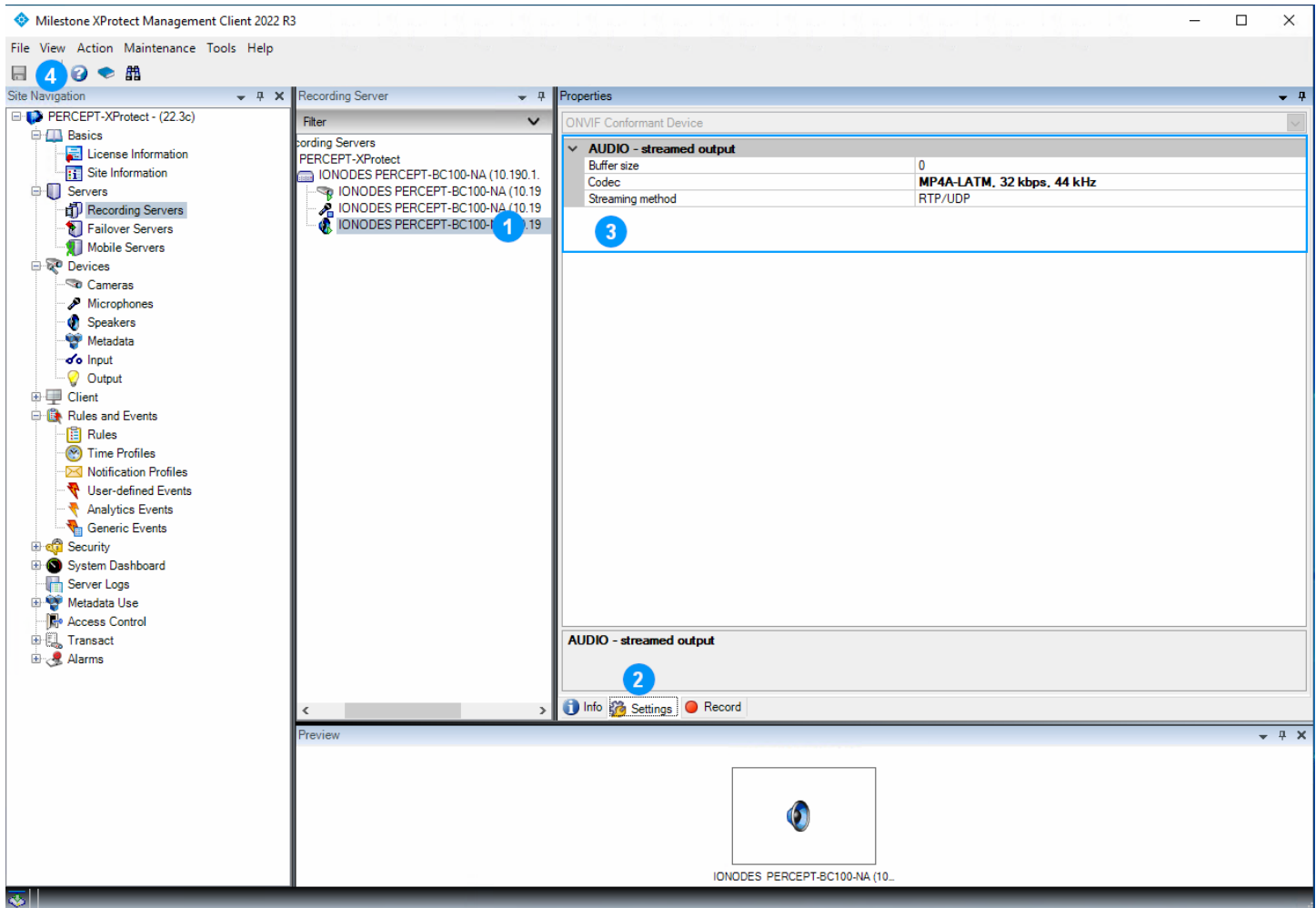
6.2.2 Record



1. Select the **Record** tab
2. **Uncheck** (disable) **Recording**
3. Click **Save**

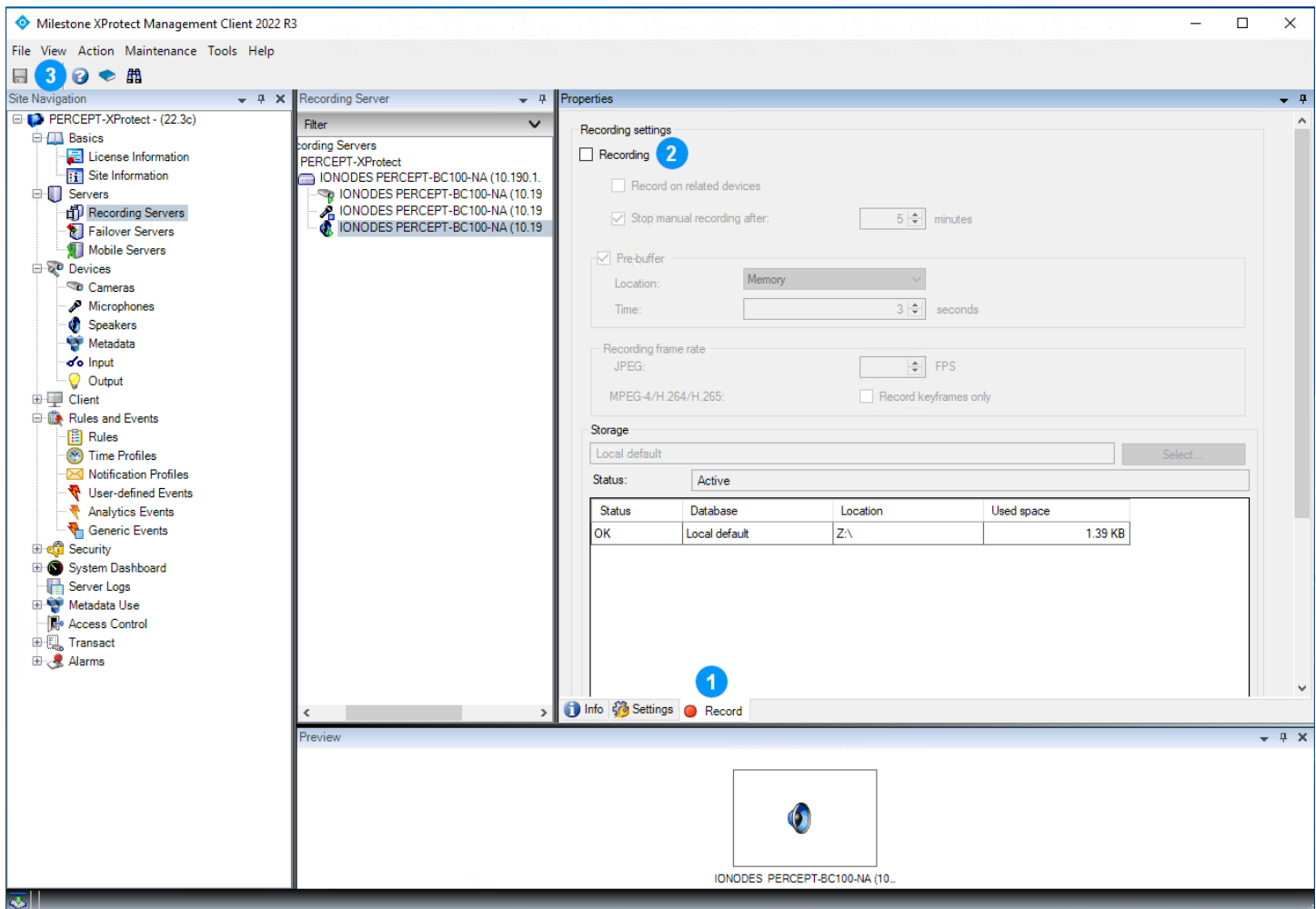
6.3 Configure Speaker

6.3.1 Settings



1. Select the PERCEPT Body Camera's **Speaker 1**
2. Select the **Settings** tab
3. Configure audio settings. A relatively low bitrate AAC (MP4A-LATM) at 32kHz or 44kHz is recommended (32kbps, 44kHz shown above). Recommended **Streaming method** is **RTP/UDP**
4. Click **Save**

6.3.2 Record



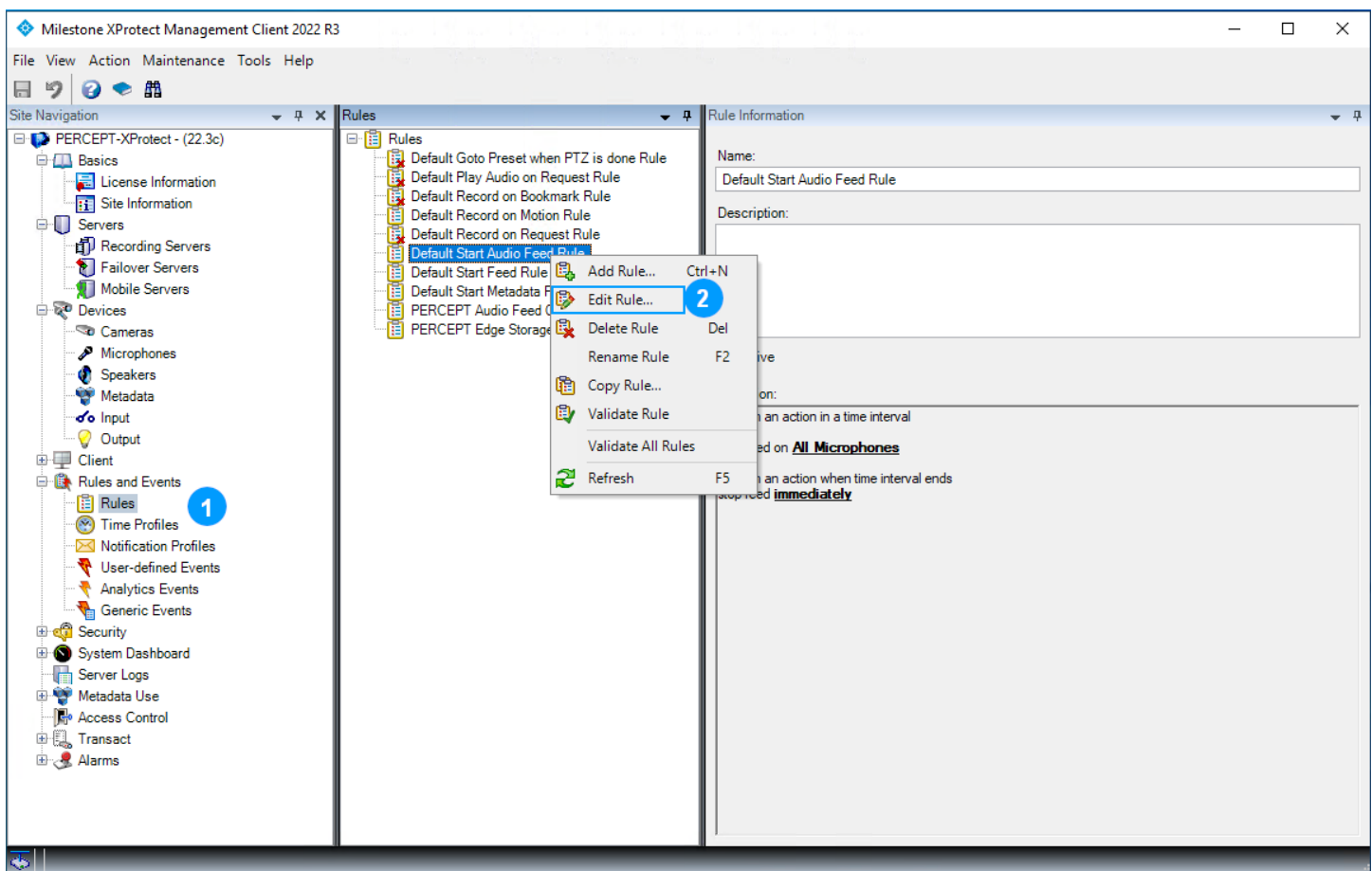
7 Configuring XProtect® Rules

Configuration made in previous section ensures XProtect® will only connect to the low bitrate live video stream on-demand, and never to the high bitrate recording stream. The speaker stream is only activated when XProtect® Smart or Web Client users press push-to-talk.

Default XProtect® rules always connect the microphone stream. XProtect® rules shall be modified to start PERCEPT Body Camera microphone(s) on-demand only, and to tailor Edge Storage transfers.

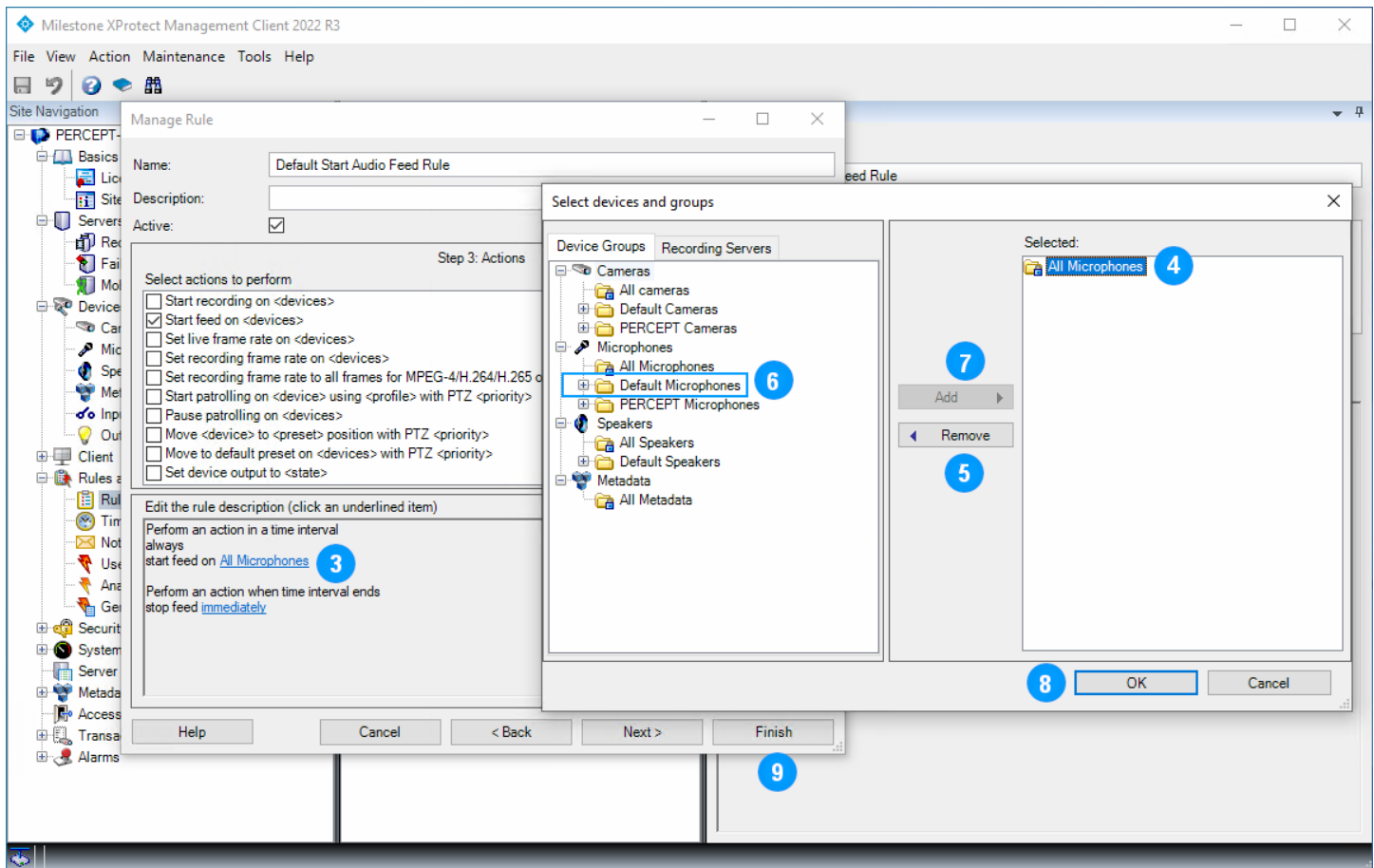
7.1.1 Default Start Audio Feed Rule

Modify this rule to exclude PERCEPT Body Camera microphone(s).



1. From the **XProtect® Management Client**'s left pane, select **Rules and Events > Rules**

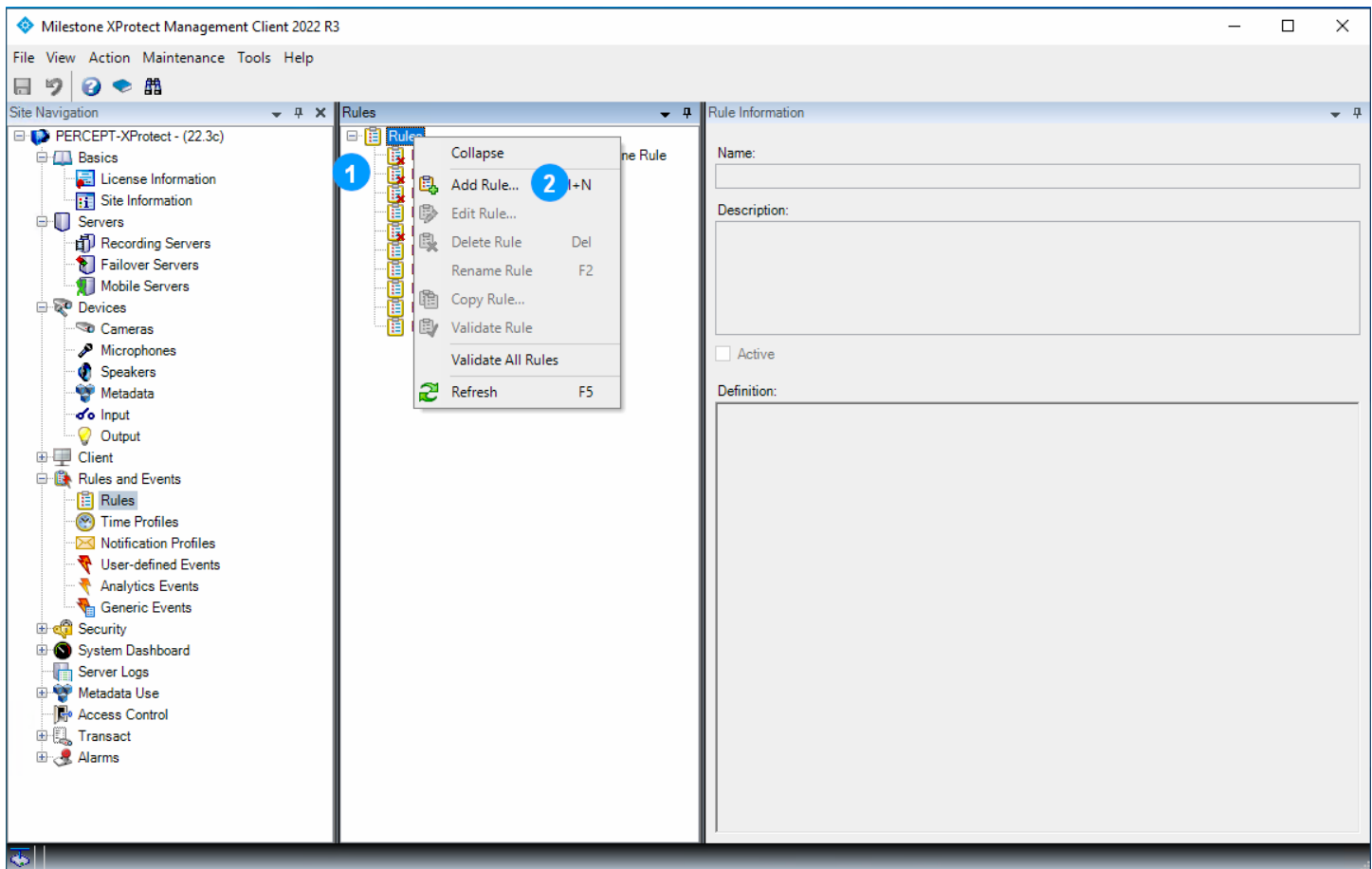
2. In the **Rules** center pane, right-click on **Default Start Audio Feed Rule** and select **Edit Rule...**



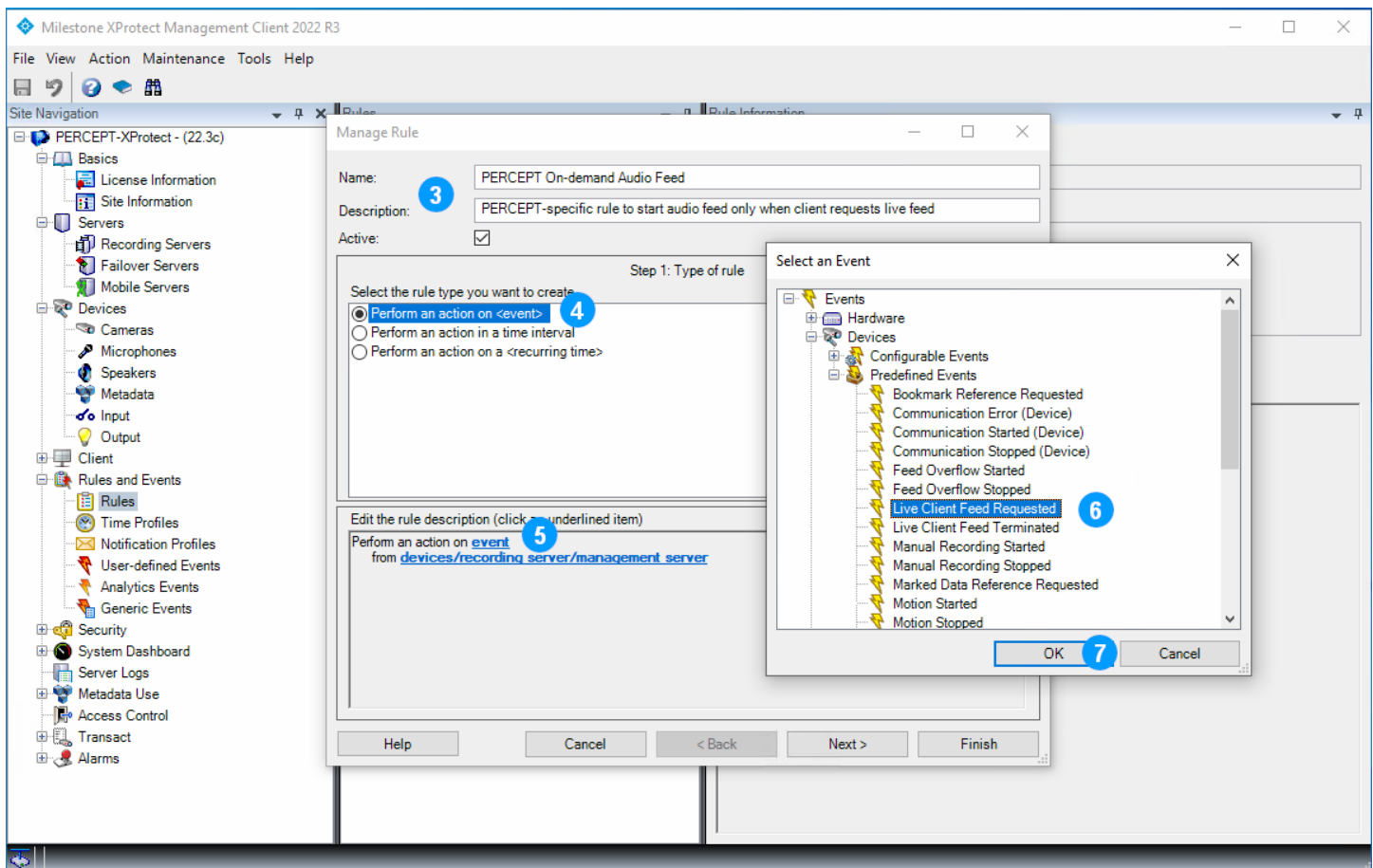
3. In **Step 3: Actions** (**Manage Rule** dialog opens at this step), in the bottom '**Edit the rule description**' pane, click on **All Microphones**
4. In the **Selected** pane of the **Select devices and groups** dialog, select **All Microphones**
5. Click **Remove**
6. In the left pane, under **Device Groups** tab, select **Default Microphones**
7. Click **Add**
8. Click **OK**
9. Click **Finish**

Note: On existing deployment where different microphone groups already exist, the modified rule may differ. The intent is to retain existing rule(s) for all non-PERCEPT Body Camera microphones and create a distinct one for PERCEPT Body Camera (in following subsection).

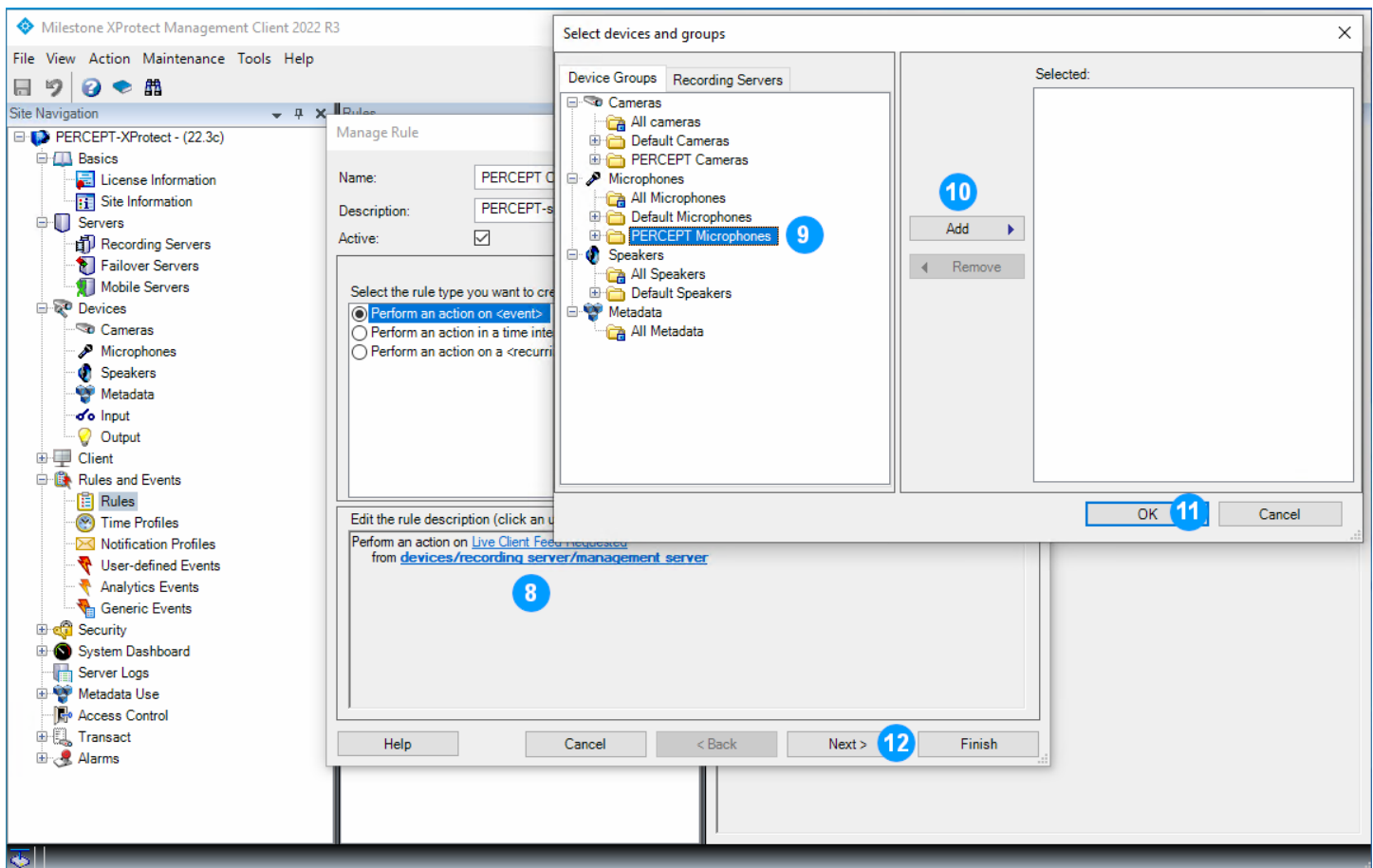
7.1.2 PERCEPT On-demand Audio Feed



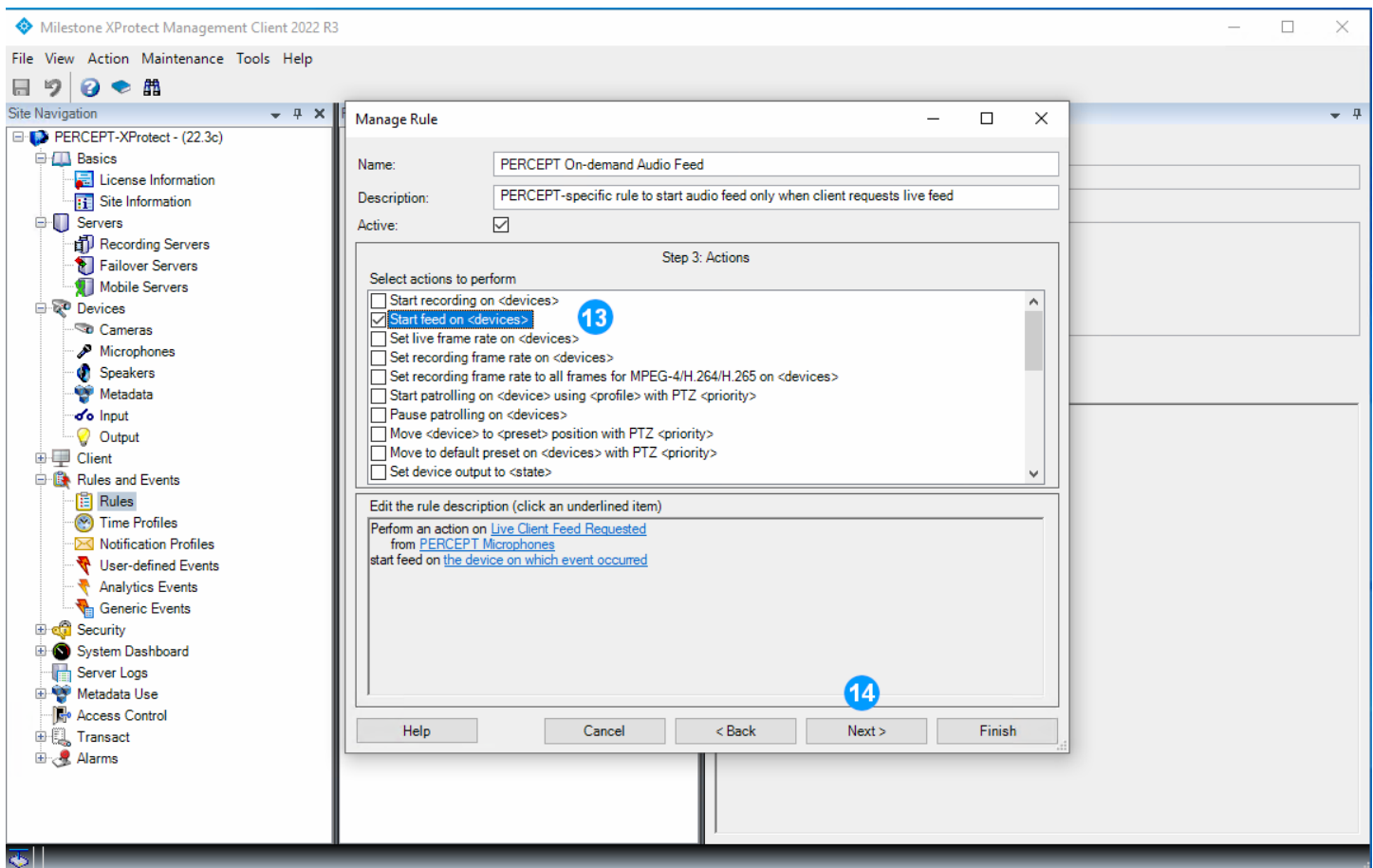
1. In the **Rules** center pane, right-click on **Rules**
2. Select **Add Rule...** from the pop-up context menu



3. In the **Manage Rule** dialog, enter a **Name** for this rule and an optional **Description**
4. From the **Step 1: Type of rule** (center pane), select **Perform an action on <event>**
5. From the **Edit the rule description** (bottom pane), click on **event**
6. In the **Select an Event** pop-up dialog, select **Devices > Predefined Events > Live Client Feed Requested**
7. Click **OK**



8. From the **Edit the rule description** (bottom pane), click on **devices/recording server/management server**
9. In the left pane of the **Select devices and groups** dialog, under **Device Groups** tab, select **PERCEPT Microphones**
10. Click **Add**
11. Click **OK**
12. Click **Next**, then in **Step 2: Conditions** click **Next** again to proceed to **Step 3: Actions**



13. From the **Step 3: Actions** (center pane), check **Start feed on <devices>**. The default 'start feed on the device on which event occurred' that will be created is correct, no need to edit
14. Click **Next**, then in **Step 4: Stop criteria** click **Next** again. Finally in **Step 5: Stop actions** click **Finish**. The default created by XProtect® for these steps are correct, no need to edit.

Definition:

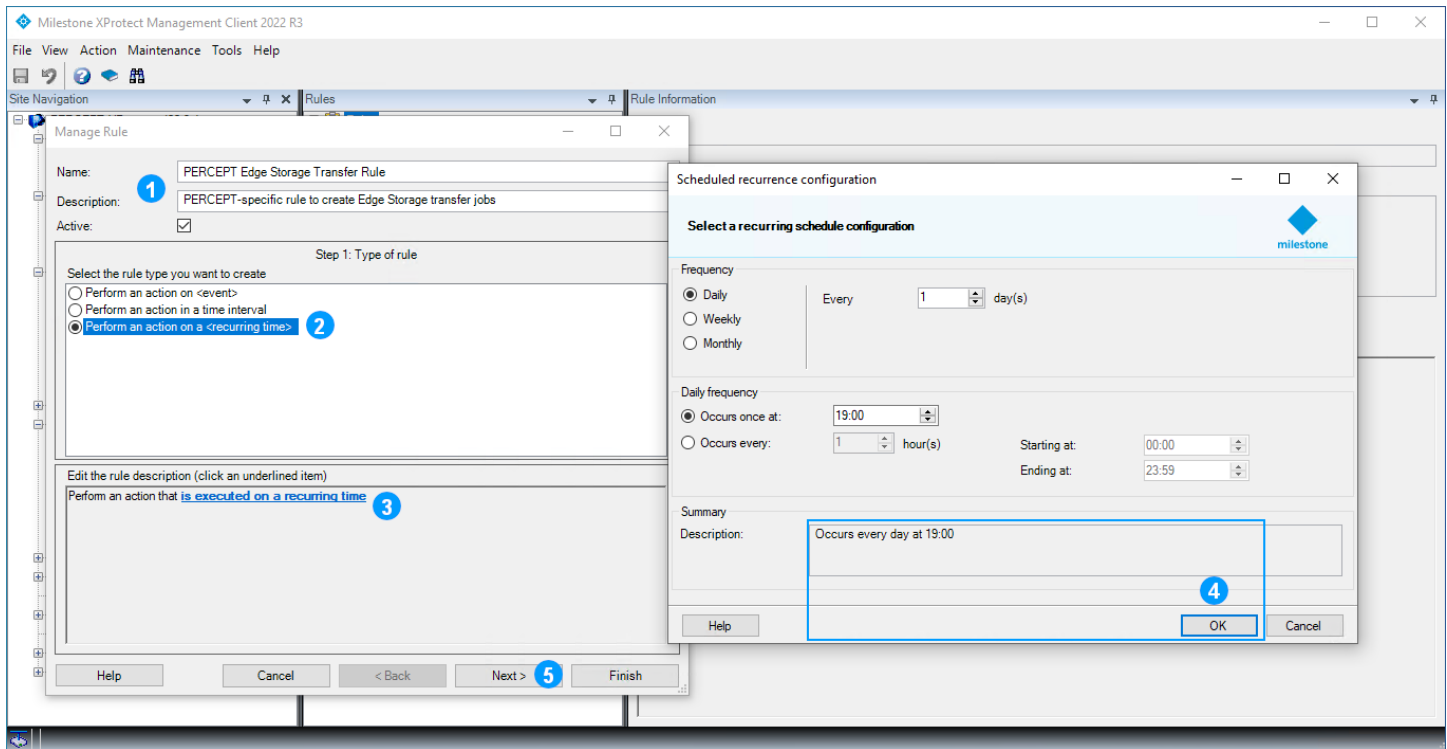
Perform an action on Live Client Feed Requested
from PERCEPT Microphones
start feed on the device on which event occurred

Perform stop action on Live Client Feed Terminated
from PERCEPT Microphones
stop feed immediately

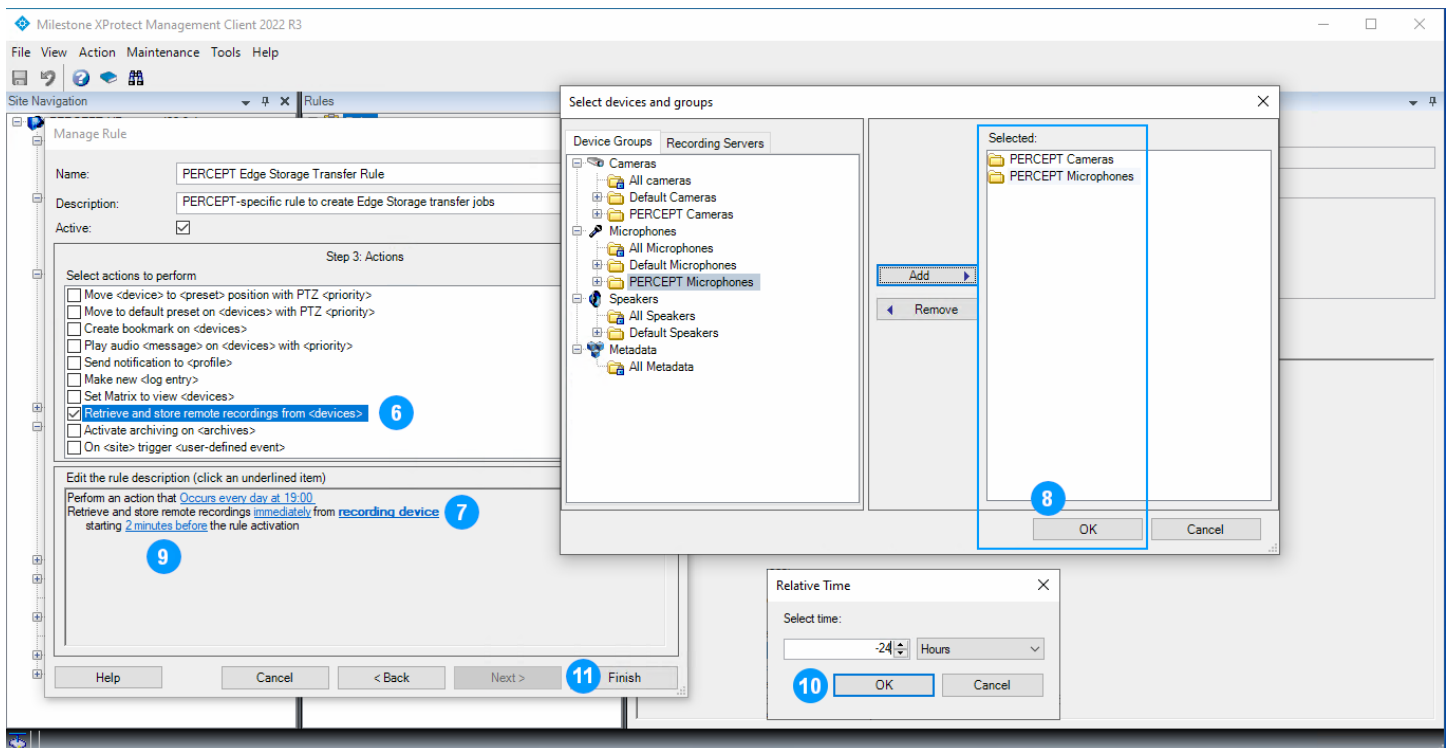
The resulting rule definition should look like:

7.1.3 PERCEPT Edge Storage Transfer Rule

Add a new Rule (refer to first 2 steps of previous subsection).



1. In the **Manage Rule** dialog, enter a **Name** for this rule and an optional **Description**
2. From the **Step 1: Type of rule** (center pane), select **Perform an action on a <recurring time>**
3. From the **Edit the rule description** (bottom pane), click on **is executed on a recurring time**
4. In the **Scheduled recurrence configuration** window, set recurrence and click **OK**
5. Click **Next**, then in **Step 2: Conditions** click **Next** again to proceed to **Step 3: Actions**



6. From the **Step 3: Actions** (center pane), select **Retrieve and store remote recordings from <devices>**
7. From the **Edit the rule description** (bottom pane), click on **recording devices**
8. In the **Select devices and groups** dialog, add **PERCEPT Cameras** and **PERCEPT Microphones** (device groups) to the **Selected** list then click **OK**
9. From the **Edit the rule description** (bottom pane), click on **2 minutes before**
10. In the **Relative Time** dialog window, select **-24 hours** and click **OK**
11. Click **Finish**

The resulting rule definition should look like:

Definition:
 Perform an action that Occurs every day at 19:00
 Retrieve and store remote recordings immediately from PERCEPT Cameras, PERCEPT Microphones
 starting 24 hours before the rule activation

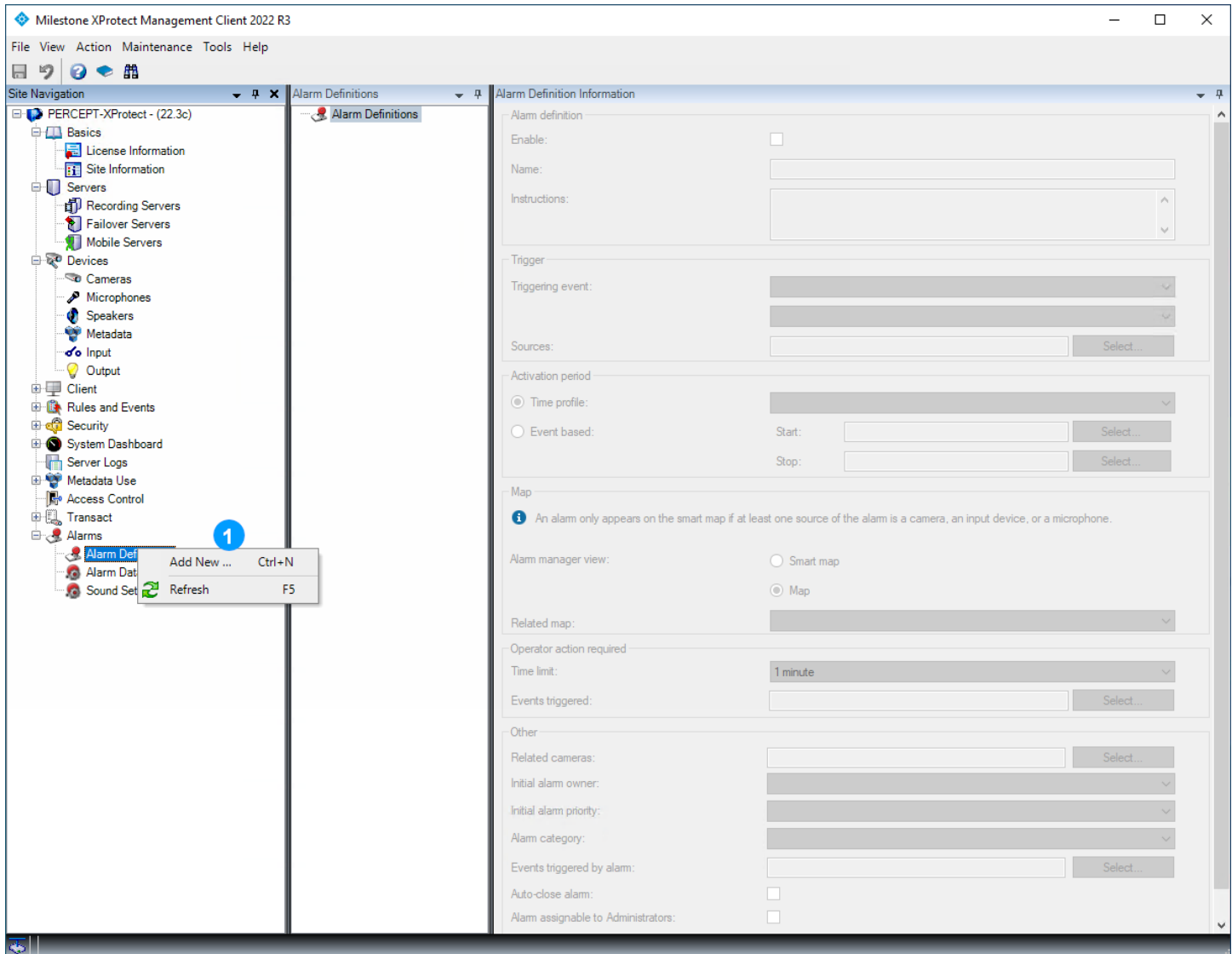
To optimize data usage, recurrence shall be tailored with the expected schedule of PERCEPT Body Cameras usage. The rule shown above will create an edge storage transfer job every evening at 19:00, requesting the previous 24 hours of audio-video recordings be downloaded from all PERCEPT Body Cameras then stored on the XProtect® Recording Server.

When an Edge Storage transfer job is created, XProtect® Edge Storage Manager will attempt to execute every 15 seconds until it succeeds. A camera being powered off, disconnected, or connected to a network interface configured to block playback will cause the XProtect® Edge Storage Manager to fail and reattempt 15 seconds later.

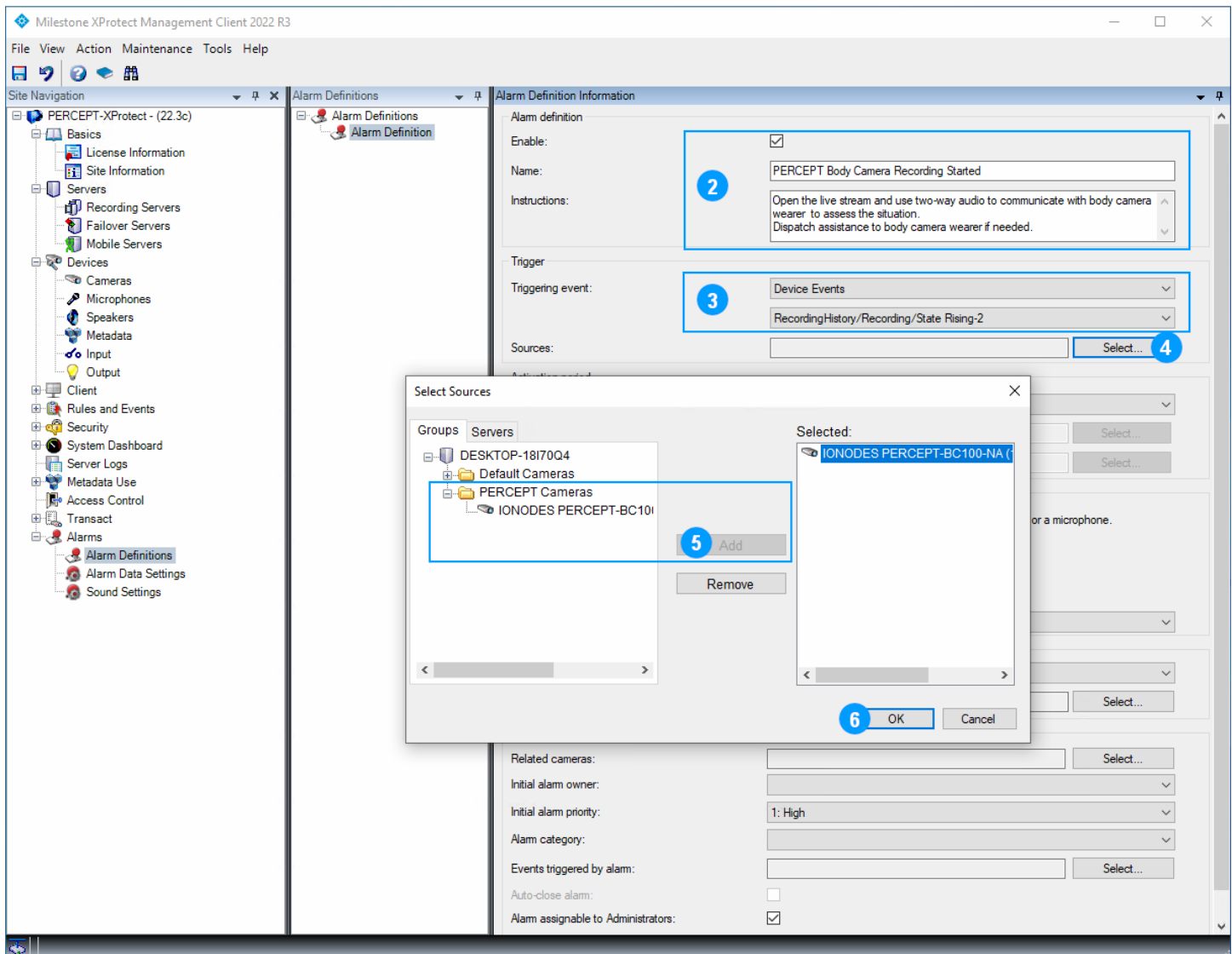
LTE data usage configuration set in section 3.2.2 blocks attempts to retrieve (playback) recordings while connected to cellular network. Recommended configuration in section 3.2.3 for deployment using PERCEPT Docking Station(s) also blocks playback over Wi-Fi. These blocked attempts will consume a few kilobytes of data each. It is best practice to schedule the recurrence at a time when PERCEPT Body Cameras are expected to be docked.

8 Event to Alarm

This section describes a simple use case for PERCEPT Body Camera-generated events. By following configuration in section 6.1.6, XProtect® subscribes to an event triggered each time the body camera wearer starts a recording. That event can be used to trigger alarms within XProtect® Smart and Web Clients.



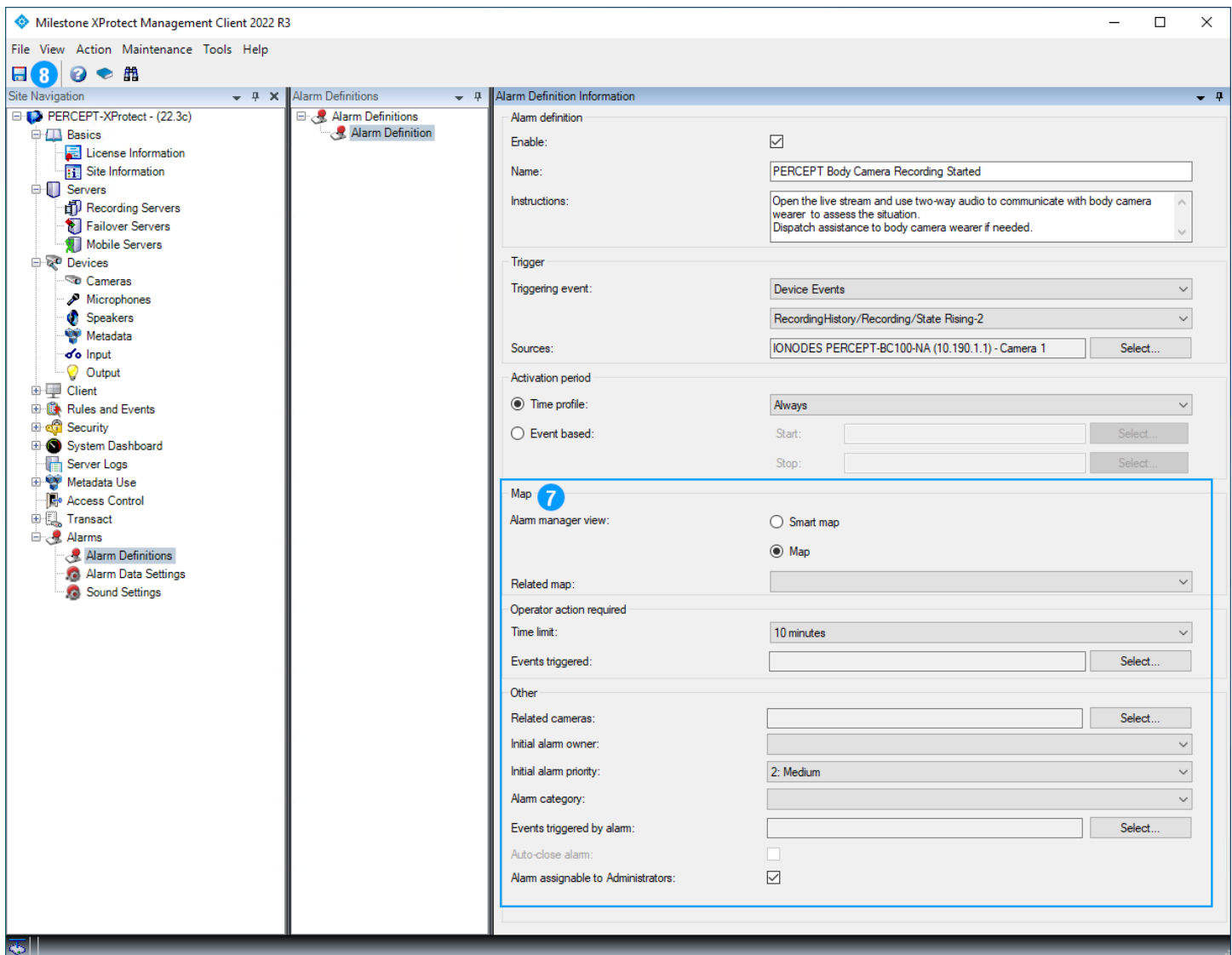
1. From the **XProtect® Management Client**'s left pane, right-click on **Alarms > Alarm Definitions** and select **Add New...** from the pop-up context menu



2. **Enable** the new alarm definition, set a **Name** and provide optional **Instructions**
3. Use drop-down menus to set the **Triggering event**. PERCEPT Body Camera event set in section 6.1.6 is a **Device Event** named **RecordingHistory/Recording/State Rising**

Note: In screenshot above, XProtect® appended an auto-number suffix (-2) to the event name.

4. **Select event Sources**
5. In the **Select Sources** dialog, highlight all PERCEPT Body Cameras for which this event shall generate the alarm and click **Add**
6. Click **OK**



7. Enter remaining parameters as required
8. Click **Save**

Note: Other settings can be configured in **Alarms > Alarm Data Settings**, such as creating distinct **Alarm priority** and/or **Alarm Category** specifically for PERCEPT Body Cameras to customize their states and behaviors.

9 Validating the Integration

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

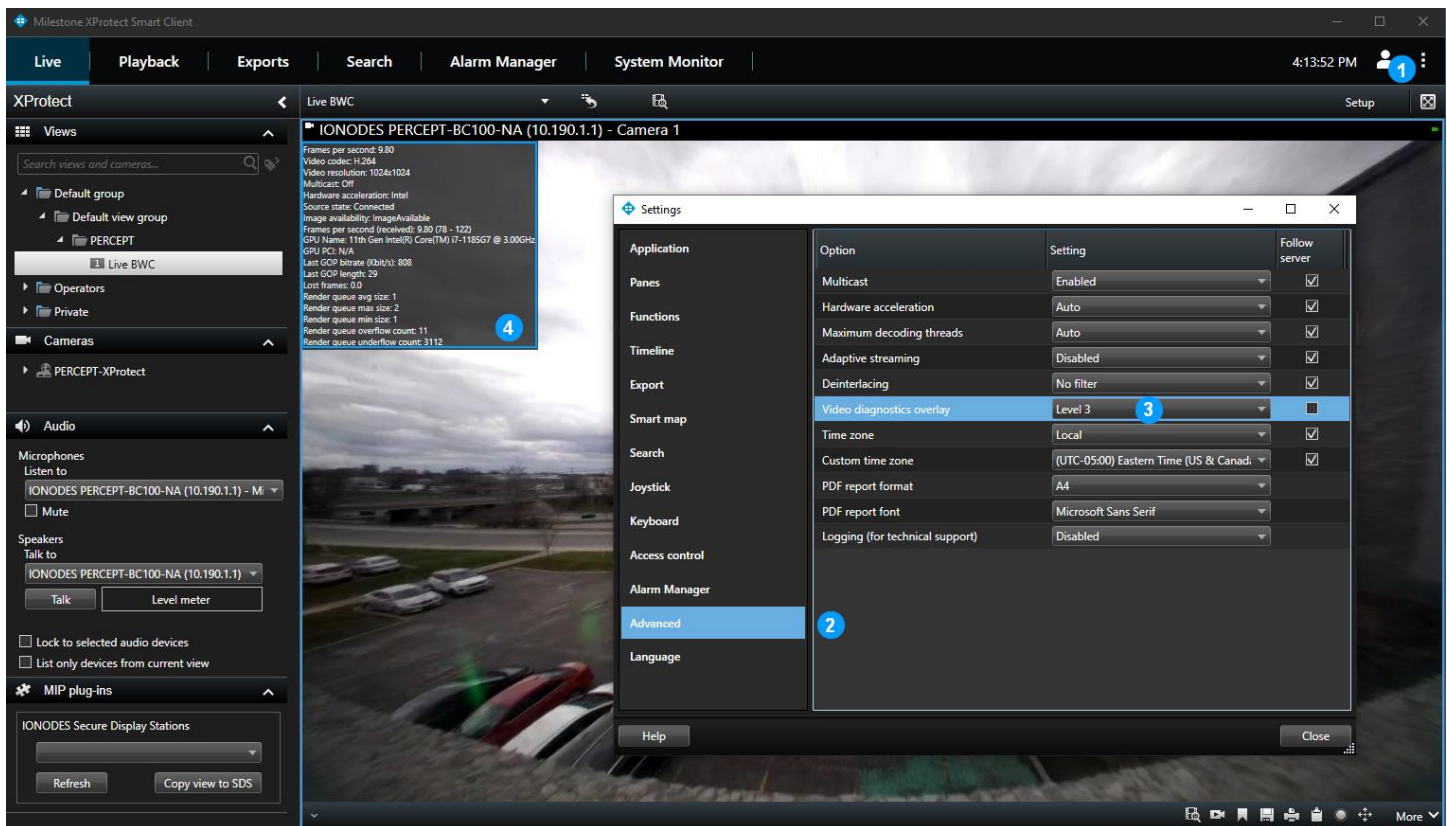
9.1 On-Demand Streaming

When no XProtect® Smart Client, Web Client or Management 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.

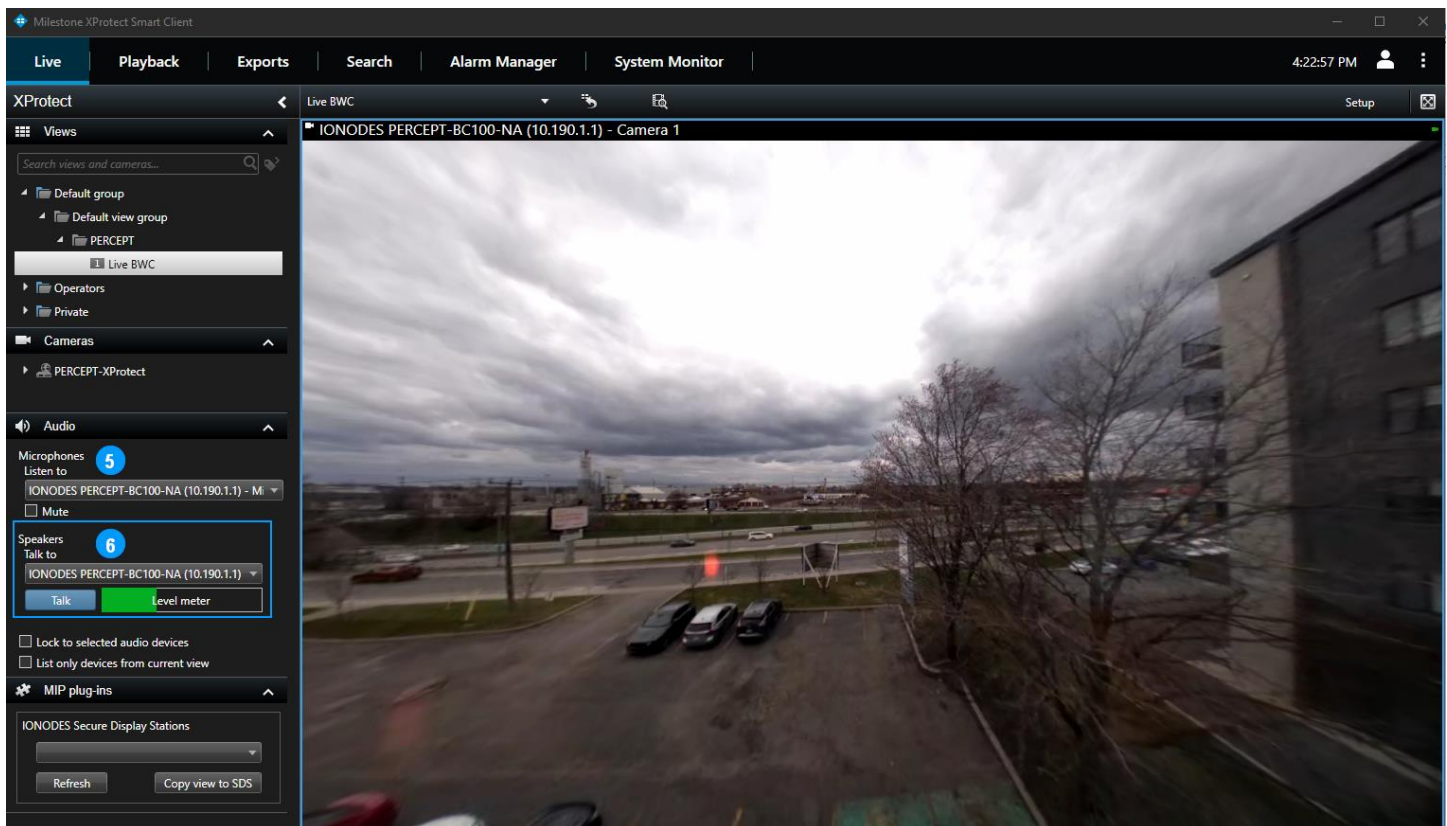
LED blinking in alternating red/green indicates it is sending a stream. If this is not expected, double-check that no client application is connected and review configurations detailed in sections 6.1.2, 6.1.3, 6.1.4, 6.2.2, 6.3.2, 7.1.1 and 7.1.2.

9.2 Live Streaming

Open XProtect® Smart Client and create a view with a PERCEPT Body Camera. Verify that the live video stream starts. If Panomorph was configured in section 6.1.5, verify that you can dewarp the video and pan through the scene. If Panomorph is not configured, panning and zooming in the hemispherical image is enabled, without dewarping.



1. Click on the ... icon and open the **Settings** dialog
2. Select the **Advanced** tab
3. Set **Video diagnostics overlay** to **Level 3**
4. Verify that the video parameters (resolution, frame rate, bitrate, etc.) correspond to the low bitrate stream configured in sections 6.1.1 and 6.1.2



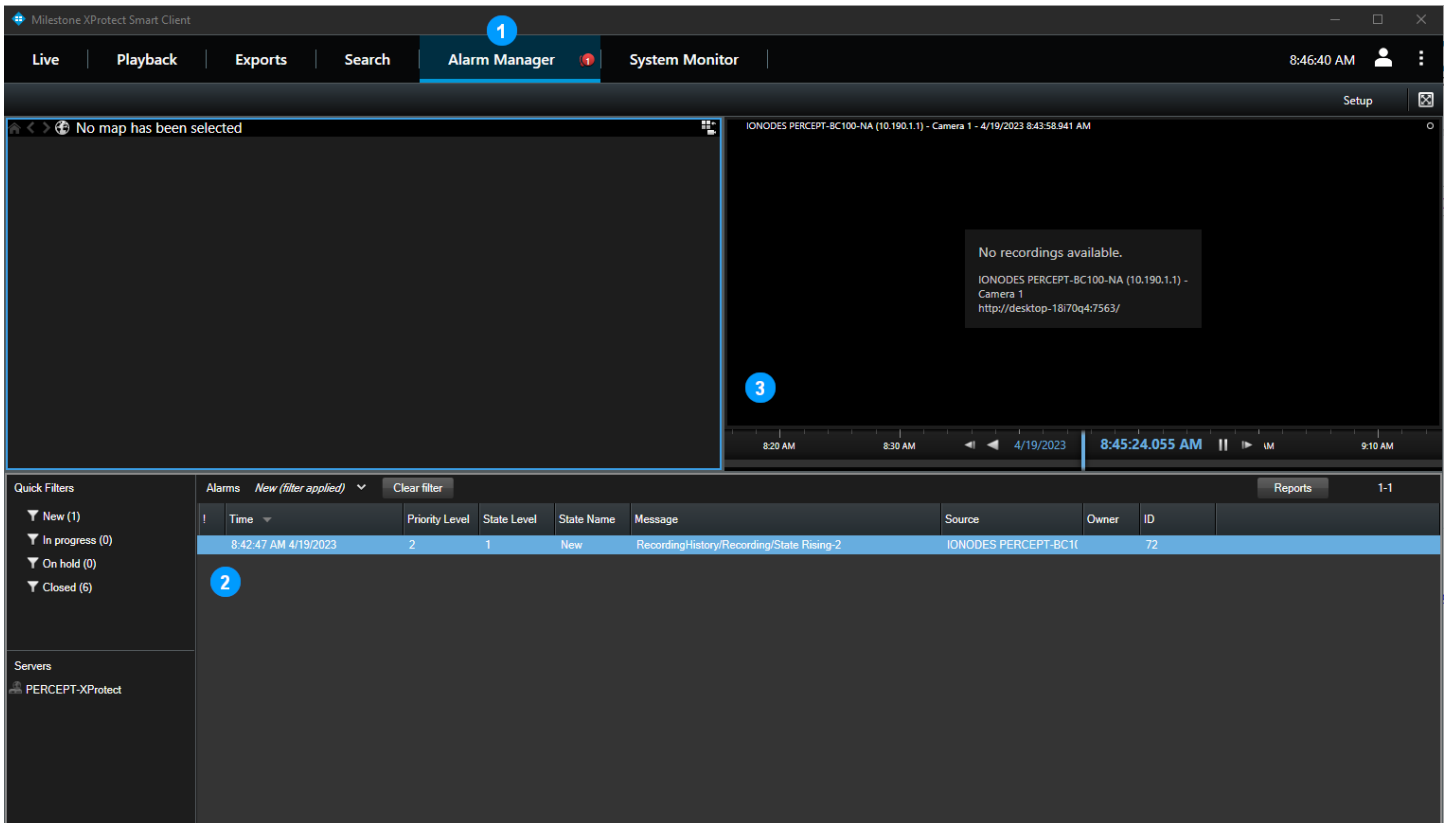
5. If computer is equipped with speakers, headphone or other audio output device, select the PERCEPT Body Camera microphone and verify audio from the camera is audible
6. If computer is equipped with microphone, headset, or other audio input device, select the PERCEPT Body Camera speaker, press the Talk button, and verify:
 - a. Level meter increases when talking in computer microphone
 - b. Audio is audible on the body camera speaker

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.

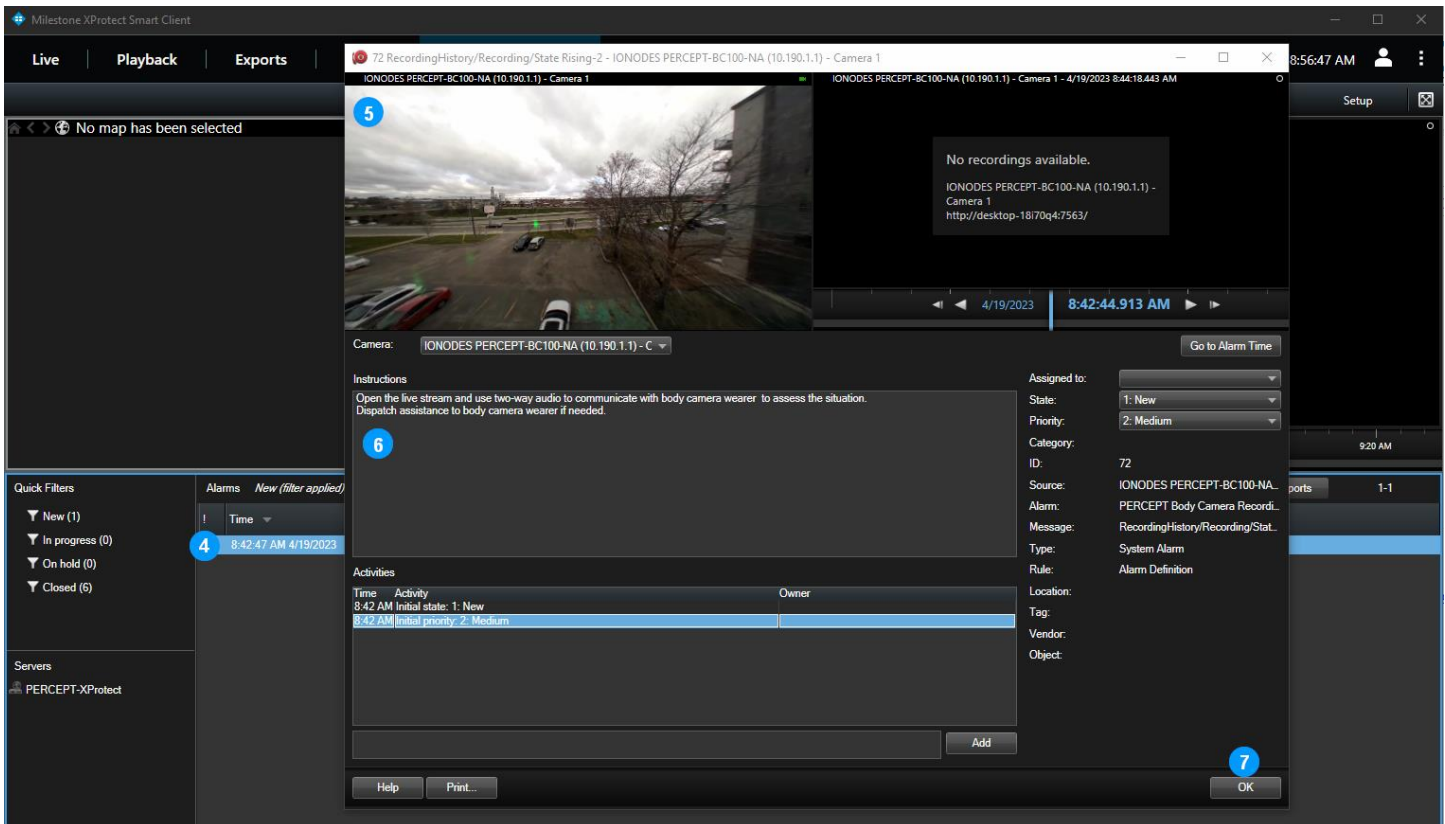
Note: There is half to one second of delay and buffering built into XProtect® audio streaming for both speakers and microphones. Operators shall be aware that the first second after pressing the **Talk** button may not be transmitted to the wearer, and the wearer's response will be slightly delayed.

9.3 Recording

With **XProtect® Smart Client** opened, press on the F5 button of the PERCEPT Body Camera to start a recording. Verify that a new alarm appears in the **Alarm Manager** section of the toolbar.



1. Click on the **Alarm Manager** tab
2. Select the new alarm and verify its parameters correspond to the **Source**, triggering event (**Message**), **Priority Level**, etc. configured in section 0. Verify that alarm time is correct.
3. Notice that recording is not available yet. It will become available after the Edge Storage transfer job, configured in section 7.1.3, successfully executes



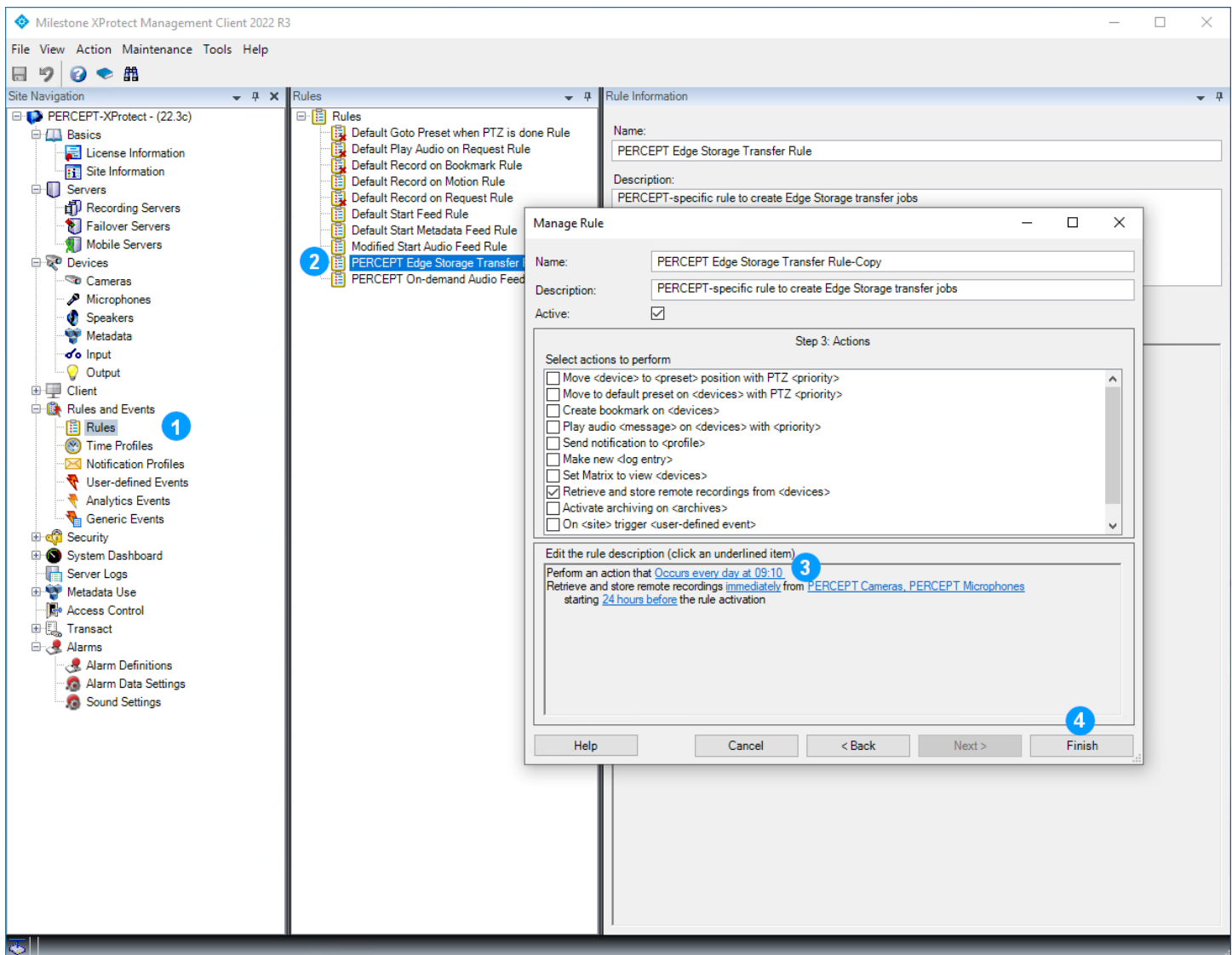
4. Double-click on the alarm to open the alarm detail window
5. Verify that a live preview is available. Note that 2-way audio is not available from this window. If communicating with the wearer is warranted, the operator must display this camera from the **Live** view tab
6. Verify that **Instructions** configured in section 0 are displayed
7. Click **OK** to close

9.3.1 Edge Storage Transfer

If edge storage transfer (playback) was disabled over Wi-Fi in section 3.2.3, insert the PERCEPT Body Camera in a docking station. Otherwise, the body camera will block playback and the XProtect® Edge Storage Manager will reattempt until it succeeds.

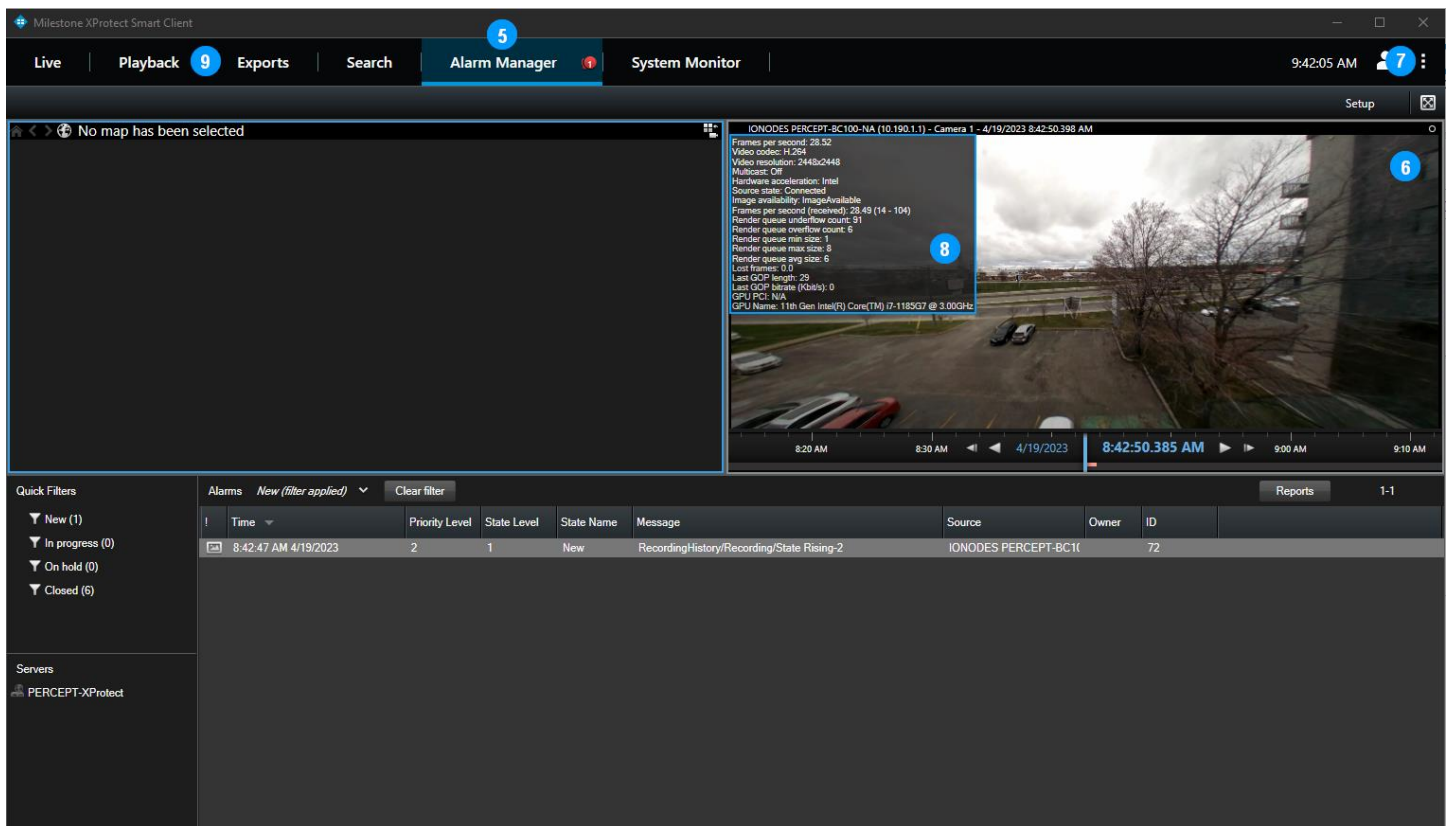


To validate Edge Storage transfer execution, wait for the recurring rule to execute, or test it right away by making a temporary copy of the rule with a modified recurring time.



1. From the **XProtect® Management Client**'s left pane, select **Rules and Events > Rules**
2. In the **Rules** center pane, right-click on the Edge Storage transfer rule created in section 7.1.3 and select **Copy Rule...** from the pop-up context menu
3. In the **Manage Rule** dialog, click on the recurrence time and change it to the nearest upcoming minute
4. Ensure the rule is enabled (**Active** checkbox near top of window) before clicking **Finish**

Wait a few minutes for the rule to trigger and the edge storage transfer job to execute. Edge Storage logs can be accessed from XProtect® Recording Server log folder to monitor job status. Default location: ProgramData\Milestone\XProtect Recording Server\Logs\EdgeStorage.log.



5. Open the **Alarm Manager** tab of **XProtect® Smart Client** with the alarm selected
6. Verify that recording is now available and auto-starts from the time the alarm (recording) was triggered
7. Open the **Settings** dialog, select the **Advanced** tab, and set **Video diagnostics overlay** to **Level 3**
8. Verify that the video parameters (resolution, frame rate, bitrate, etc.) correspond to the high bitrate stream configured in sections 6.1.1 and 6.1.2. If seeking to a time before the alarm, Pre-Recording video parameters shall match the Pre-Recording profile configured in section 3.4.
9. Note that audio is not available from the **Alarm Manager**, open the **Playback** tab to verify audio is available and synchronized with video

Note: If a temporary rule was created to test edge storage transfer, remember to disable or delete it when testing is completed. Same applies to Video diagnostics overlay.

Note: If using XProtect® Web Client, perform the same tests as for XProtect® Smart Client, keeping in mind that Web Client does not support panomorph dewarping and requires XProtect® Mobile Server transcoding if video streams are configured with H.265 codec.

9.4 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:



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 connection are lost.

Verify live streaming, 2-way audio and alarms work over VPN as they do over Wi-Fi. If a live stream is connected when the network interface switches, it can take approximately 20 seconds for the stream to resume on XProtect® Smart Client or Web Client.