

HOW TO.

Configure AXIS Body Worn Live Self-Hosted

Contents

Introduction	3
1 – AXIS Body Worn Live Self-Hosted deployment layouts	6
1.1 Network connectivity requirements	6
1.2 BWL Self-hosted deployment layouts	6
2 – Self-Hosted setup preparation	7
3 – Scenario 1: Quick Setup	9
4 – Scenario 2: Normal Setup – Corporate Network - APN	12
4.1 Body Worn System Setup	13
4.2 Prepare Self-hosted Server device	15
4.3 Setup Self-hosted Server app	16
4.4 Connect Body Worn Live to Body Worn Manager	18
4.5 Finalize BWL Setup in Body Worn Manager	19
5 – Scenario 3: Normal Setup – Advanced NAT Network	21
5.1 Prepare the router configuration	21
5.2 Body Worn System Setup	24
5.3 Prepare Self-hosted Server device	24
5.4 Setup Self-hosted Server app	26
5.5 Connect Body Worn Live to Body Worn Manager	27
5.6 Finalize BWL Setup in Body Worn Manager	27
6 – Demo livestreaming player	28
7 – Troubleshooting	30
7.1 Setup - Verify the BWM self-hosted configuration	30
7.2 Setup - Verify the signaling server availability	31
7.3 Connection - Enable troubleshooting mode BWM	32
7.4 Connection - Enable troubleshooting mode BWC	32
7.5 Performance - Info tab	33
Considerations and limitations	34

Introduction

This document is a guideline covering only how to configure AXIS Body Worn Live Self-Hosted. For more information about the general Axis Body Worn Configuration please see:

<https://help.axis.com/en-us/axis-body-worn-solution#get-started>

This guide pertains solely to the demonstration streaming via the integrated demo player in AXIS Body Worn Live Self-Hosted. For video management software integration, refer to the resources section for comprehensive setup instructions.

AXIS Body Worn Live Self-Hosted uses WebRTC streaming protocol. The guideline covers briefly the principles of WebRTC streaming and how they are applied in the AXIS Body Worn Live Self-Hosted solution.

WebRTC enables real-time communication (like video calls) directly between browsers or devices, but connecting peers can be tricky due to network setups like NATs and firewalls

STUN (Session Traversal Utilities for NAT): STUN is a protocol used to discover the public IP address and determine any restrictions in the NAT or firewalls for a device. It helps WebRTC applications establish a direct connection between peers by providing the necessary information to connect directly to each other

TURN (Traversal Using Relays around NAT) acts as a relay server when a direct connection is impossible due to restrictive network conditions. Instead of peers connecting directly, data is sent through the TURN server, which forwards it between them.

The **WebRTC signaling server** in AXIS Body Worn Live Self-Hosted is implemented as an app that can be installed and run on an AXIS W401 Body Worn Activation Kit or AXIS D3110 Mk II Connectivity hub

Acronyms

BWC – Axis Body Worn Camera (W120/W102/W110)

SCU - AXIS W800 System Controller

BWL - AXIS Body Worn Live

BWM - AXIS Body Worn Manager

W401 - AXIS W401 Body Worn Activation Kit

D3110 Mk II – AXIS D3110 Mk II Connectivity Hub

Self-hosted Server device - AXIS Body Worn Live Self-hosted Server device (W401/D3110 Mk II)

Self-hosted Server app - AXIS Body Worn Live Self-hosted Server app

VMS- Video Management System

BOM

- Axis BWCs
- Axis Docking Stations
- AXIS W800
- AXIS [W401](#) Body worn activation kit or AXIS [D3110 Mk II](#) Connectivity hub
- Network Infrastructure (customer's): Routers, Switch

SBOM

- Axis Body Worn System device software
- AXIS Body Worn Live Self-Hosted Server device software
- AXIS Body Worn Live Self-Hosted Server app
- Self-Hosted Licenses
- VMS

Ports (Router, Firewall)

- Default inbound/outbound
- Signaling Endpoint: 8082 (TCP)
- STUN and TURN Endpoint: 3478 (TCP and UDP).
- Dynamic Endpoint Range (UDP) - 49152-65535 (Data: Video, Audio, etc....)

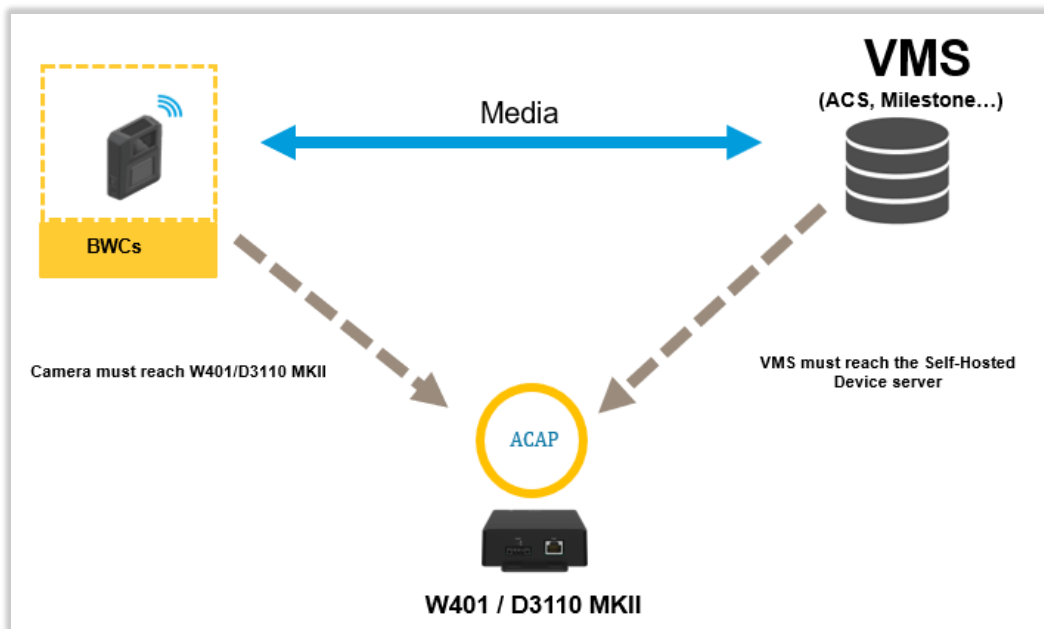
Resources

- Manual: <https://help.axis.com/en-us/axis-body-worn-live-self-hosted>
- Axis Body Worn System device software: <https://www.axis.com/support/device-software?name=axis%20body%20worn%20system>
- AXIS OS Device software: <https://www.axis.com/support/device-software>
- AXIS Body Worn Live Self-Hosted Server app: <https://www.axis.com/en-us/products/axis-body-worn-live#download-block>
- Tutorial video how set up Self-hosted in Milestone XProtect®: <https://youtu.be/QSYfOCTYdWw?si=dyQAwtA5CVvkdxsO>

1 – AXIS Body Worn Live Self-Hosted deployment layouts

1.1 Network connectivity requirements

For seamless operation, the following components must establish network connections with each other:



BWC: Connect to the network via Wi-Fi or LTE for streaming.

Self-hosted Server device (W401/D3110 Mk II) requires network access for communication with BWCs and VMS.

VMS (e.g. AXIS Camera Station, Milestone XProtect): Connects to the network for live streaming and communication with the **Self-hosted Server device**

1.2 BWL Self-hosted deployment layouts

BWL Self-hosted offers flexibility and adaptability, catering to diverse network requirements, existing infrastructure, and desired outcomes. In this guide, we'll explore three common deployment scenarios encountered during the solution's piloting phase. Keep in mind that these are not the only possible configurations.

Deployment Scenario 1: Quick Setup

Deployment Scenario 2: Normal Setup – Corporate Network - APN

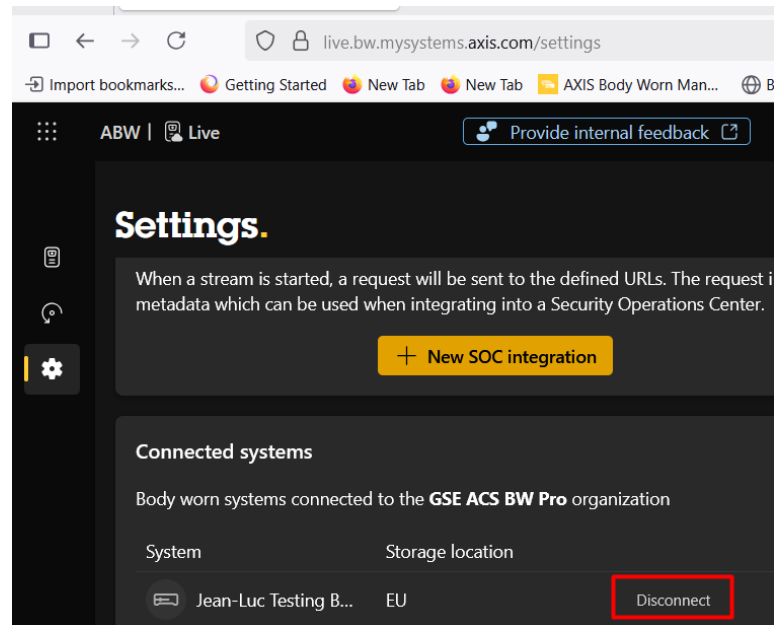
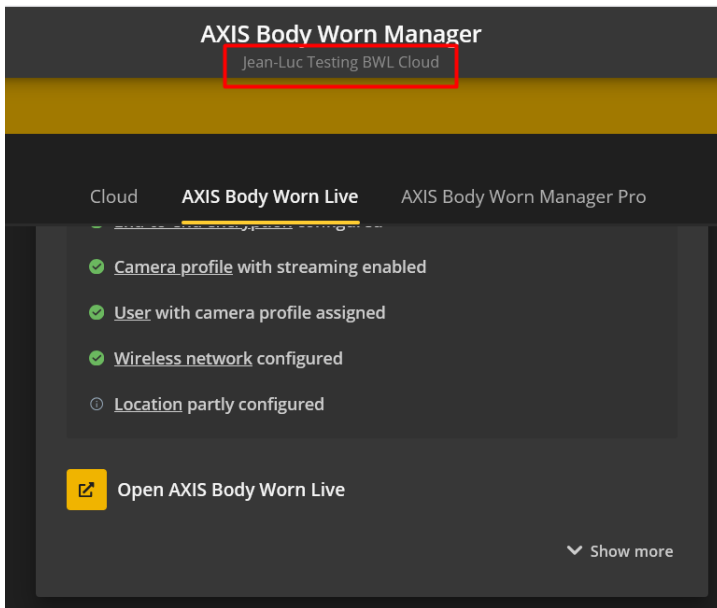
Deployment Scenario 3: Normal Setup – Advanced NAT Network

2 – Self-Hosted setup preparation

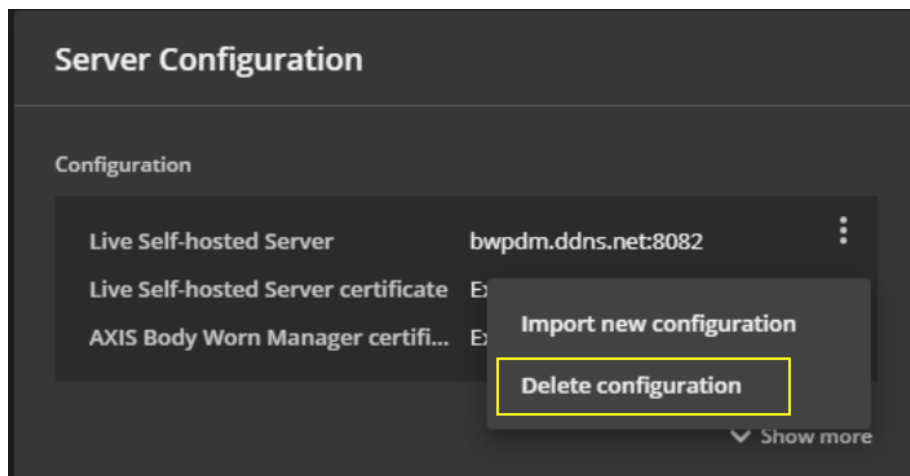
In this guide we use the W401 as the Self-hosted Server device.

1. Upgrade the W800 to the latest device software.
2. If the BWL is already configured – Reset BWL configuration

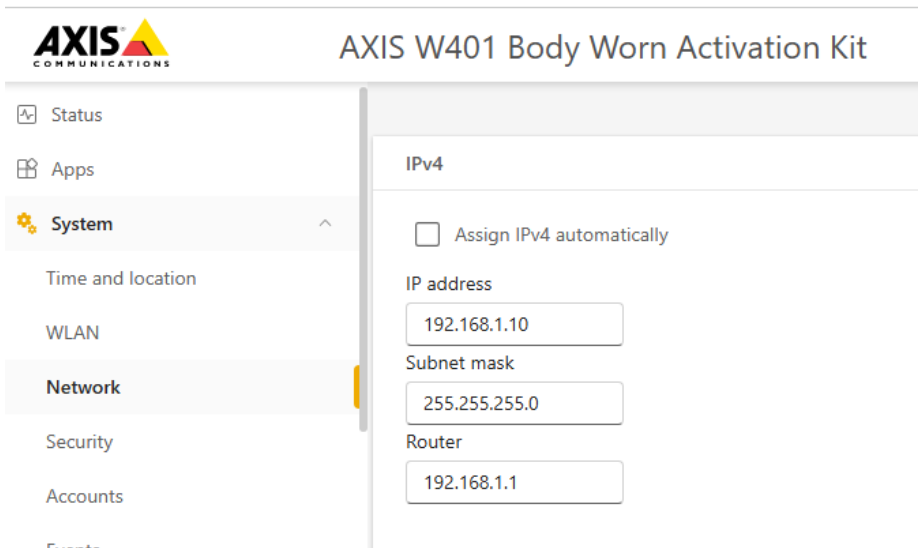
Axis-hosted – Disconnect the system from BWL



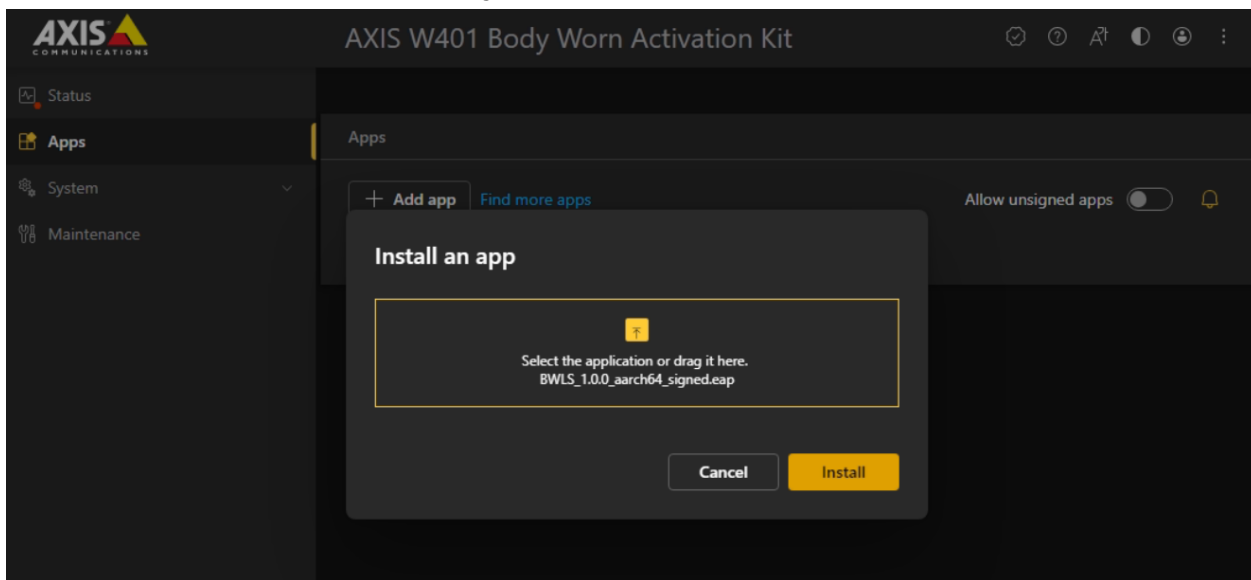
Self-hosted - Reset BWL Self-Hosted



3. If the Self-hosted Server device isn't new, reset it to factory default settings. For instructions, see the device's user manual at help.axis.com
4. Upgrade the Self-Hosted Server device with the latest AXIS OS device software.
5. Go to **System > Network** and assign a static IP address.

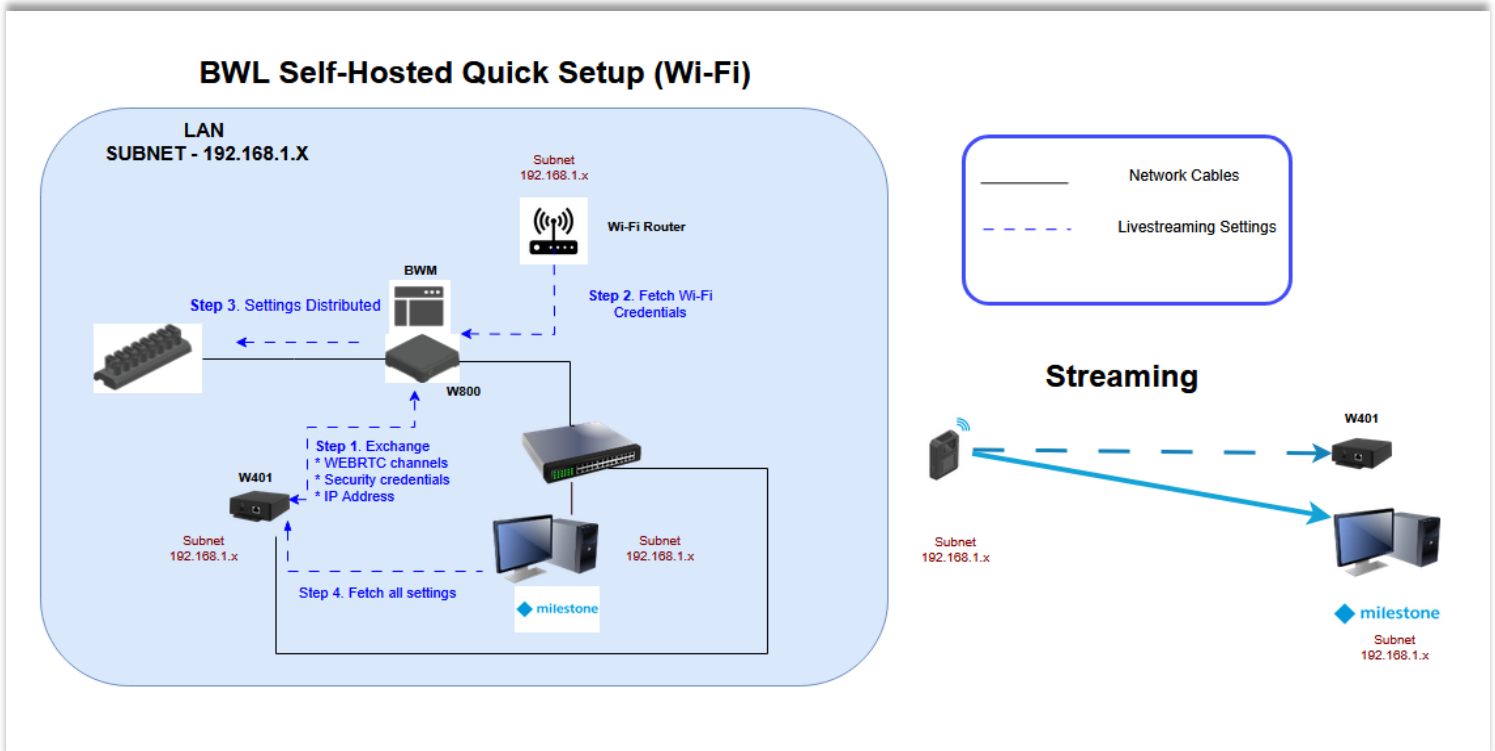


6. Download the Self-hosted Server app
7. In W401, go to **Apps**.
8. Click **Add app**.
9. Drag-and-drop the app and click **Install**.
10. Use the switch to start the **AXIS Body Worn Live Self-hosted Server** app.



11. Proceed with steps in one of the three scenarios of your choice in the next sections.

3 – Scenario 1: Quick Setup



In this scenario, all three components reside on the same network without any network obstacles:

BWCs: Utilize **Wi-Fi** for streaming.

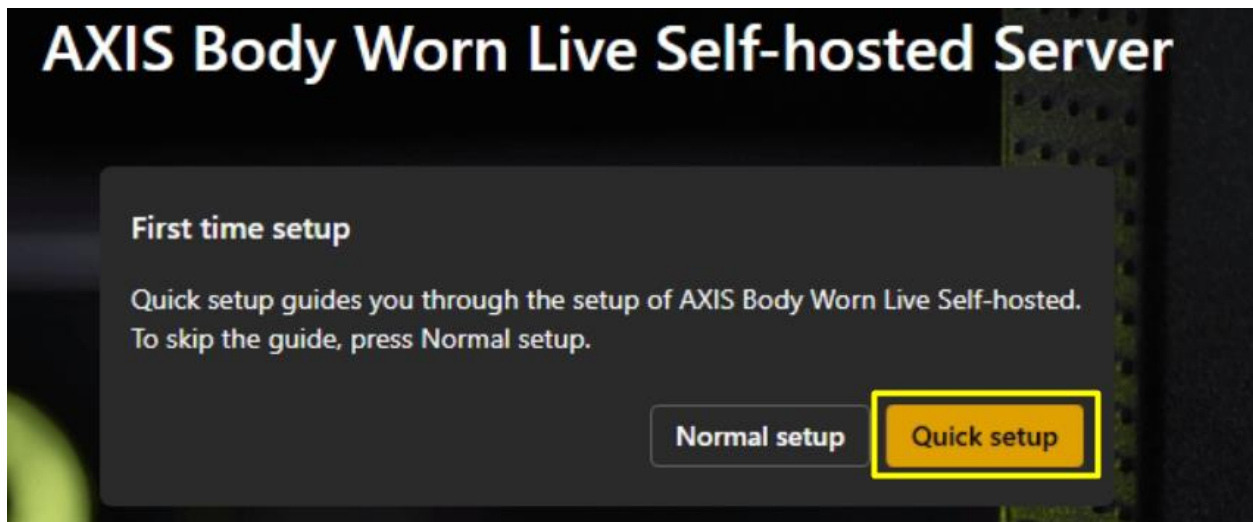
Self-Hosted Server device: W401/D3110 Mk II

VMS (e.g. AXIS Camera Station, Milestone XProtect): Managing livestreaming
All components share the same subnet (e.g., LAN 192.168.1.X)

Use Case: Primarily used for demos and Proof of Concepts (PoCs).


Advantages: Easiest to configure, utilizing the BWL Self-Hosted Server app quick setup.


1. Perform the steps in [2 Self-Hosted setup preparation](#)
2. Open the app. Select **Quick setup**



3. Enter the credentials for W800:
 - Hostname (IP address)
 - Username
 - Password
4. Click **Continue** and finish the wizard.
5. Wait until everything is verified OK:



6. In **BWM** go to **Settings**  > Camera.
7. Under Wi-Fi networks, click **Add**.
8. Enter the Name (SSID) and Password for the Wi-Fi network.
9. Click **Add**.

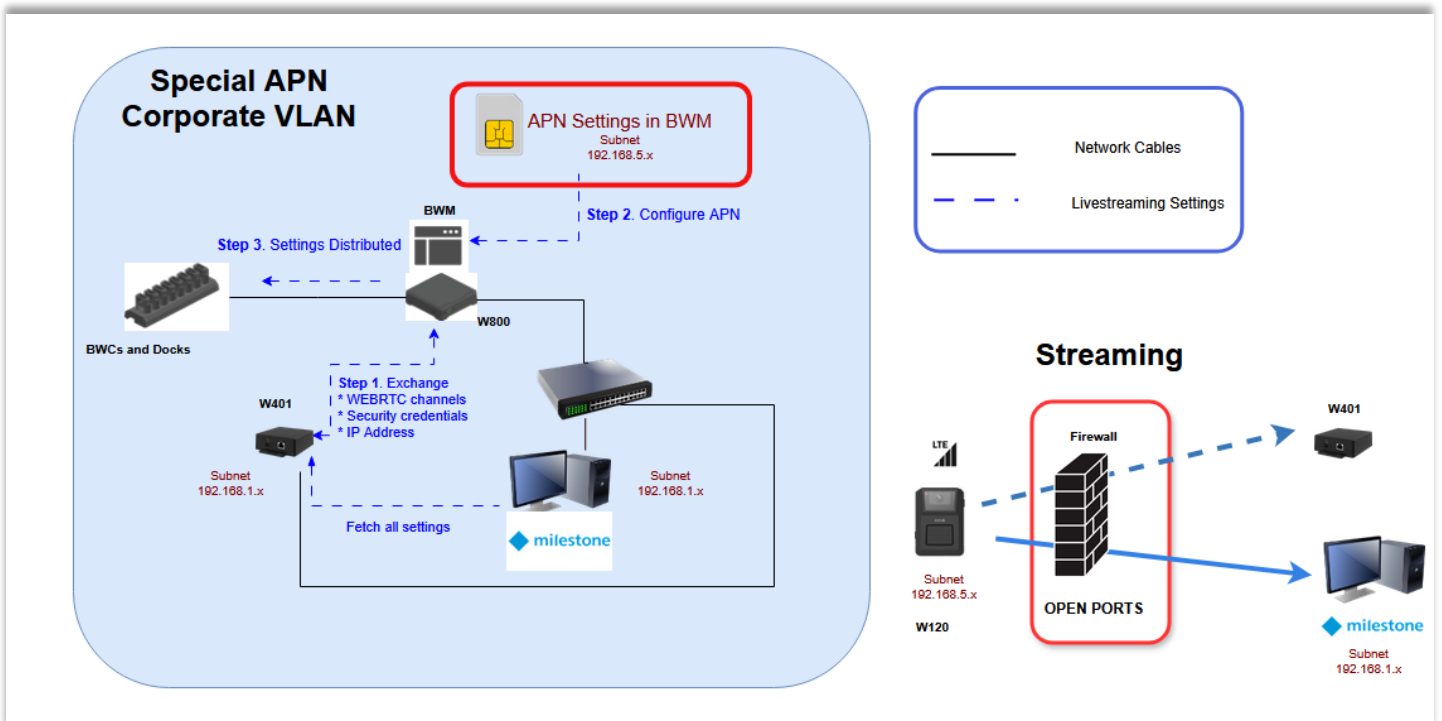
10. Go to **Camera profiles** 
11. Select the camera profile you want to assign the Wi-Fi network to.
12. Expand the **Wireless connection** panel.
13. Select a Wi-Fi network to assign it to the camera profile.
14. Go to **Users** and select the camera user you want to assign the Wi-Fi network to.
15. Select the camera profile that has the appropriate Wi-Fi network.

NOTE

For a successful quick setup, ensure that:

- All network components are in the same network
- There are no network obstacles, such as firewalls, between the components
- The quick setup can only be used one time per Self-Hosted Server device. If adding more body worn systems, normal setup is required.

4 – Scenario 2: Normal Setup – Corporate Network - APN



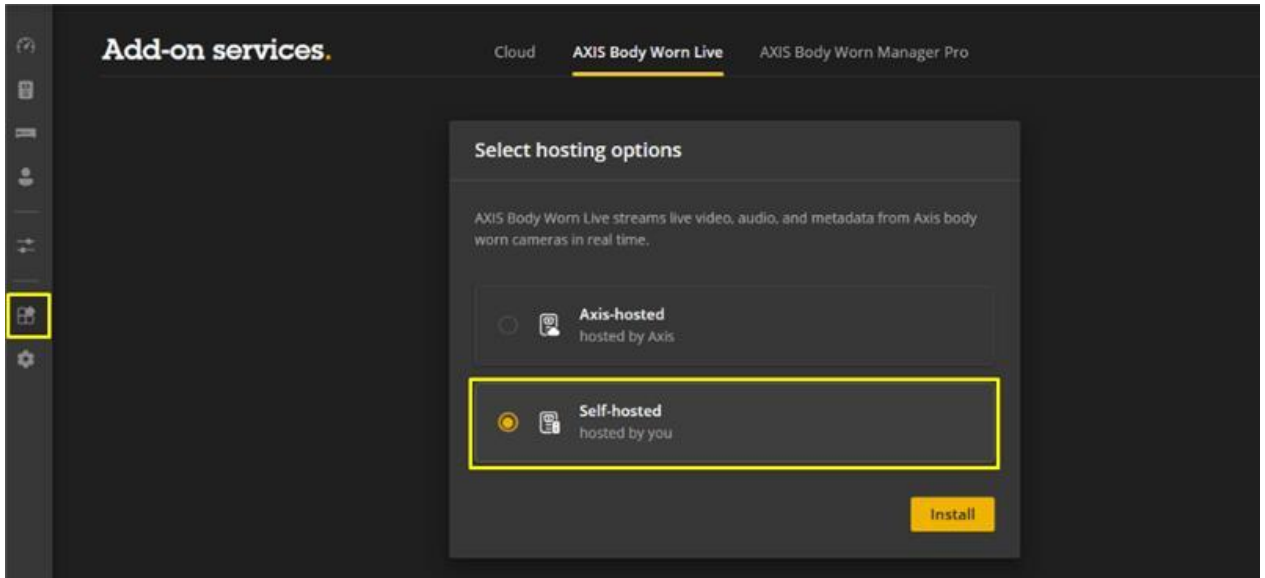
This is by far the most used scenario in professional deployments. In this **normal setup** scenario, all the devices are in the corporate network but in different subnets. To enable direct communication between the cameras and the internal corporate network, you'll need to enter the APN address for the SIM cards of the LTE devices in the body worn system. This will assign a corporate IP address to the SIM cards and LTE devices, even though they are on a public network. The APN details are typically provided by your SIM card operator.

As an example:

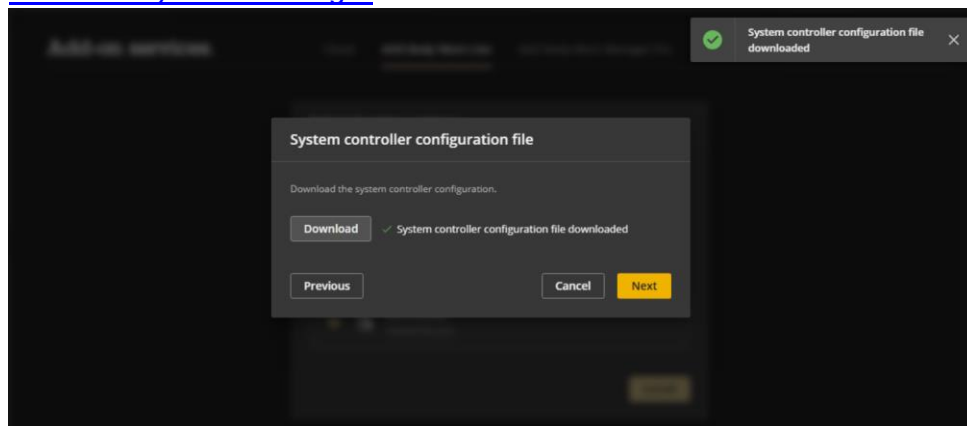
The VMS, W800, and W401 can be on different subnets but still be able to communicate with over the network. Typically, a firewall separates the subnets, so you'll need to allow stream traffic on the network. For specific port details, please refer to the [port's requirements](#) for self-hosted information.

4.1 Body Worn System Setup

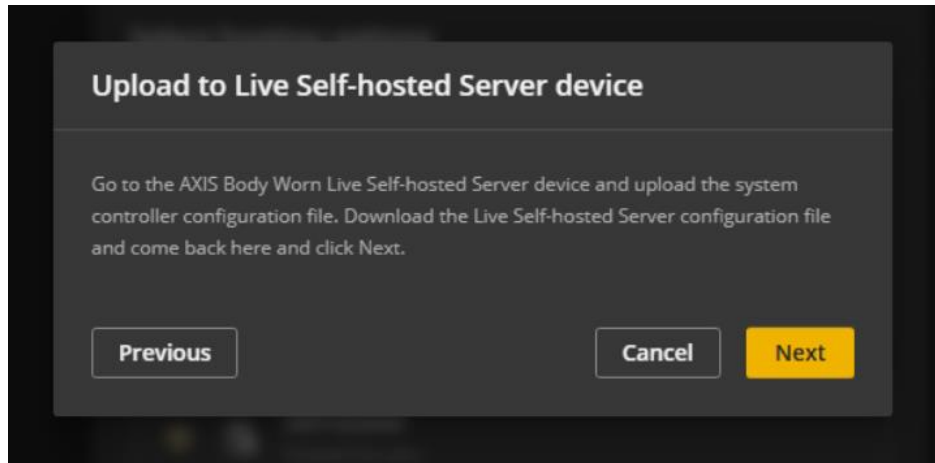
1. Perform the steps in [2 Self-Hosted setup preparation](#)
2. Use **AXIS IP Utility** to locate the IPv4 address of your W800.
3. Use a web browser and enter the IP address of W800.
4. In **BWM**, go to **Add-on services**.
5. Under **AXIS Body Worn Live**, click **Self-hosted**.



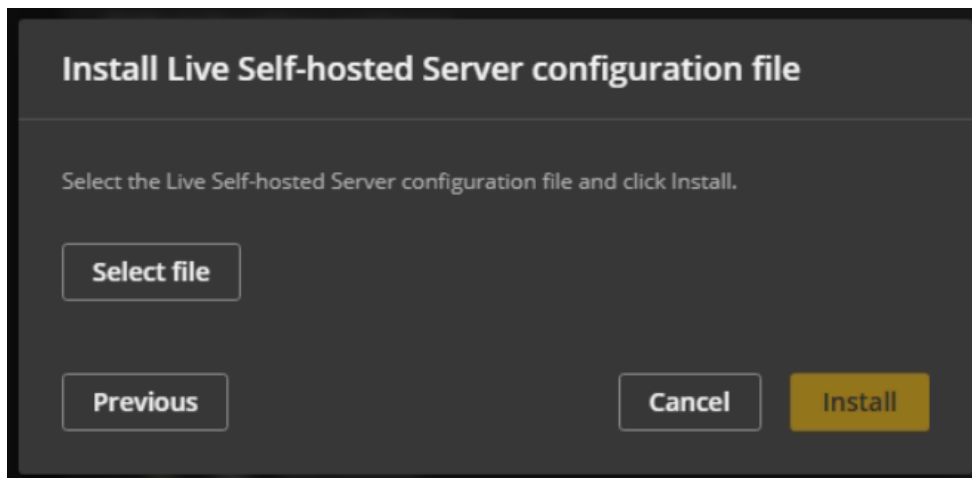
6. Click **Install**.
7. Enter how many days **system controller configuration certificate** should be valid.
8. Download the **system controller configuration file**.
9. Remember where the file is downloaded, as it is later used in [Connect Body Worn Live to Body Worn Manager](#)



10. Click **Next**.



11. Pause the wizard in BWM here, keep the tab open, and proceed with - *Prepare the Live Self-hosted Server device*



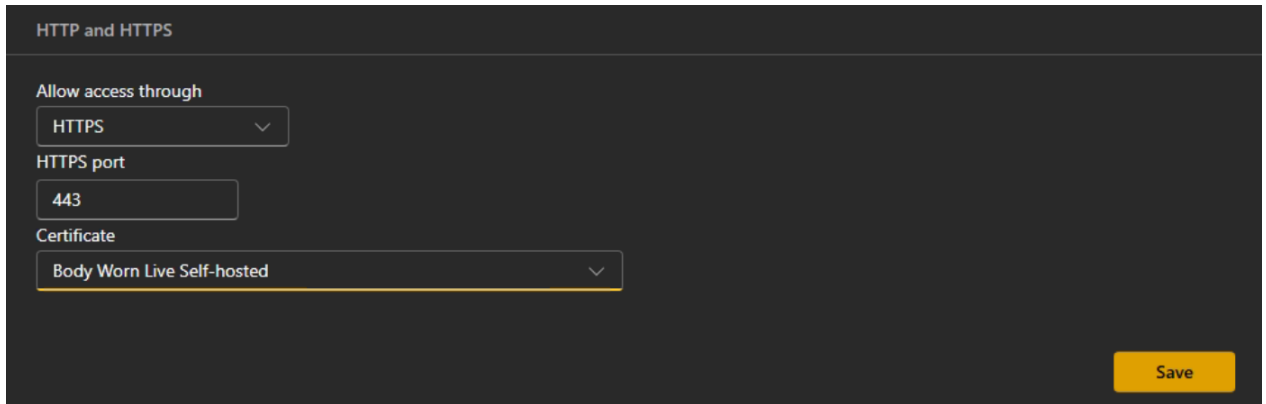
4.2 Prepare Self-hosted Server device

1. In W401 go to **System > Security** and click Add certificate.



2. Choose **Create a self-signed certificate**. (or you can upload and install your organization's client-server certificate)
3. Enter Certificate name, Common name = *IP or DNS Name of the W401*, and Country Code of your country, e.g. SE.

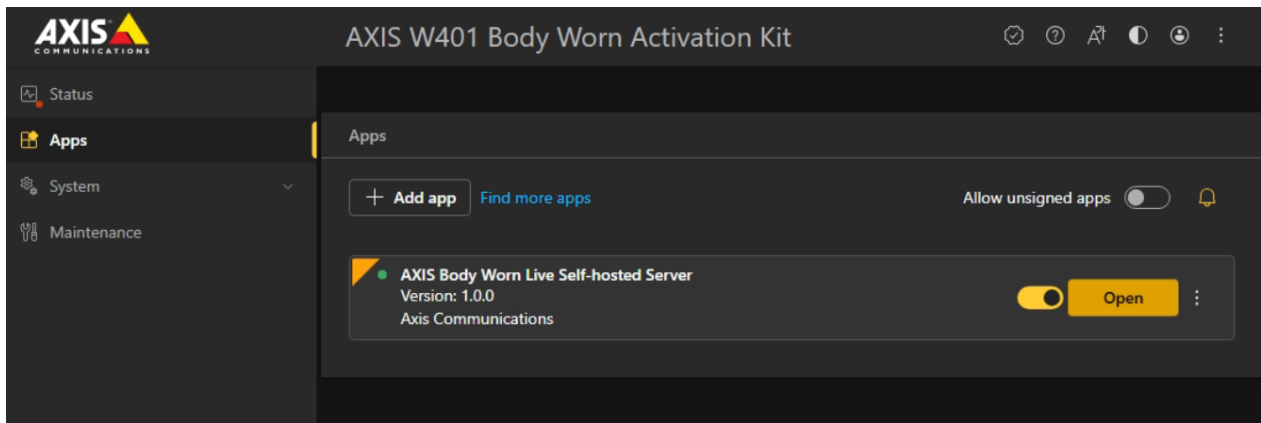
4. Click **Next > Generate**.
5. Go to **System > Network > HTTP and HTTPS**.
6. Under Allow access through, select **HTTPS**.
7. In the list of certificates, select the certificate you installed and click **Save**.



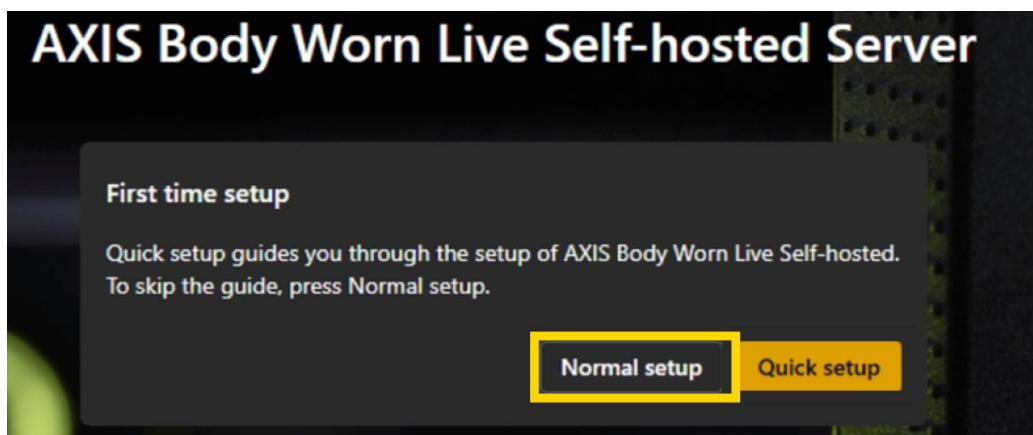
8. If not automatically done, reload and log in to the web page to use the new certificate.

4.3 Setup Self-hosted Server app

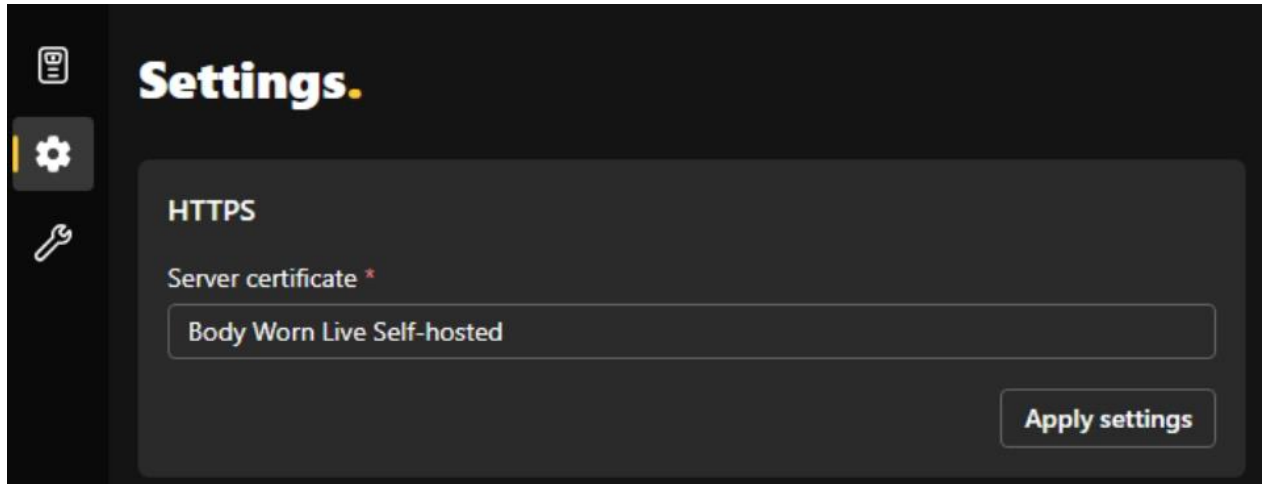
1. In W401 go to **Apps**.
2. Open the app.



3. Select **Normal setup**



4. Go to **Settings**  > **HTTPS**.

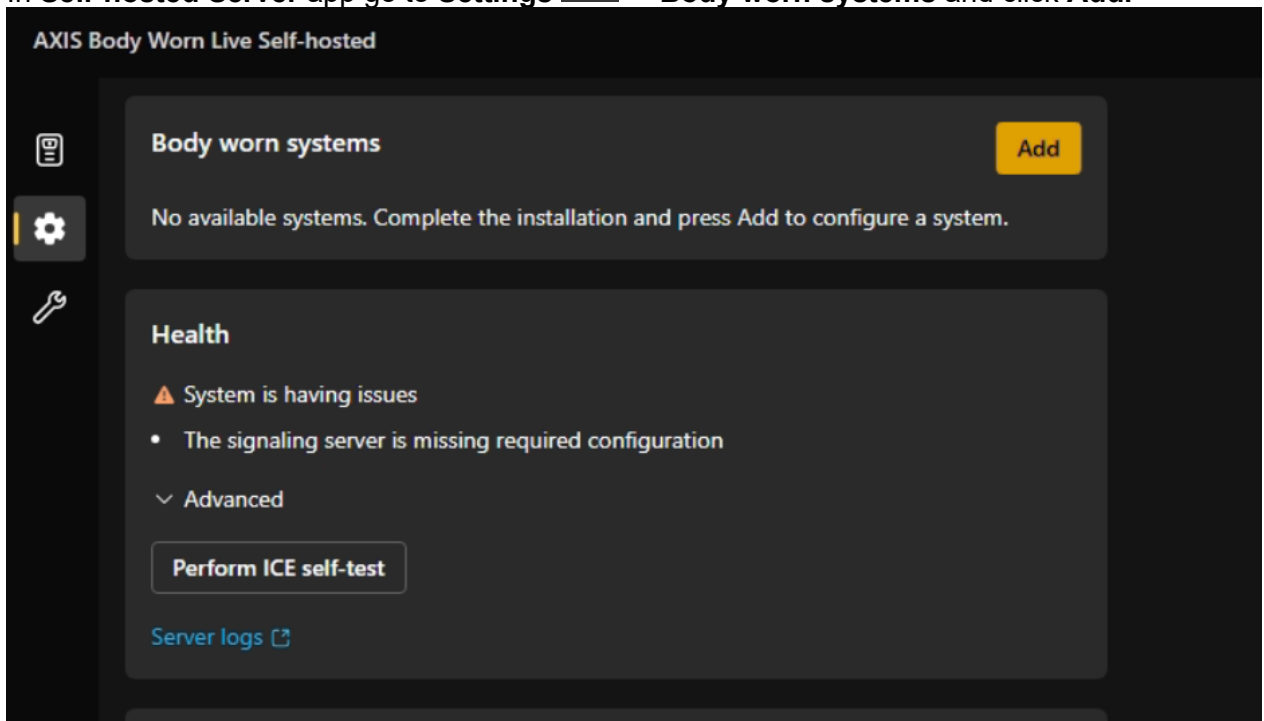


5. In the list of server certificates, select the certificate you installed when you prepared the device.
6. Click **Apply settings**. The server configuration is loaded automatically.
7. Under Server configuration enter the address endpoints/port and click **Apply Settings**

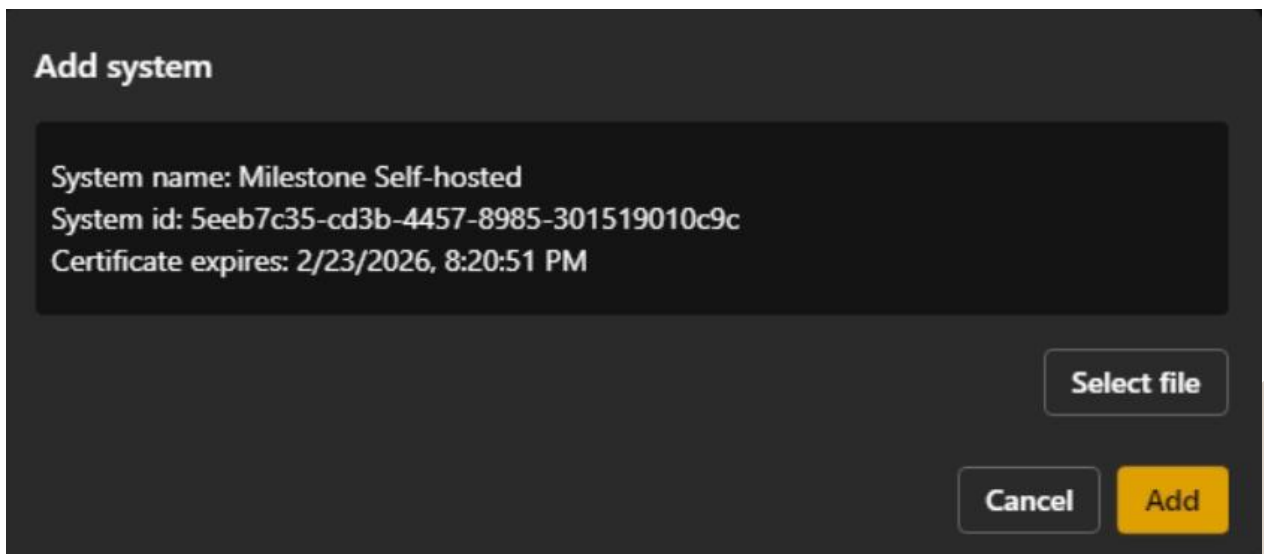


4.4 Connect Body Worn Live to Body Worn Manager

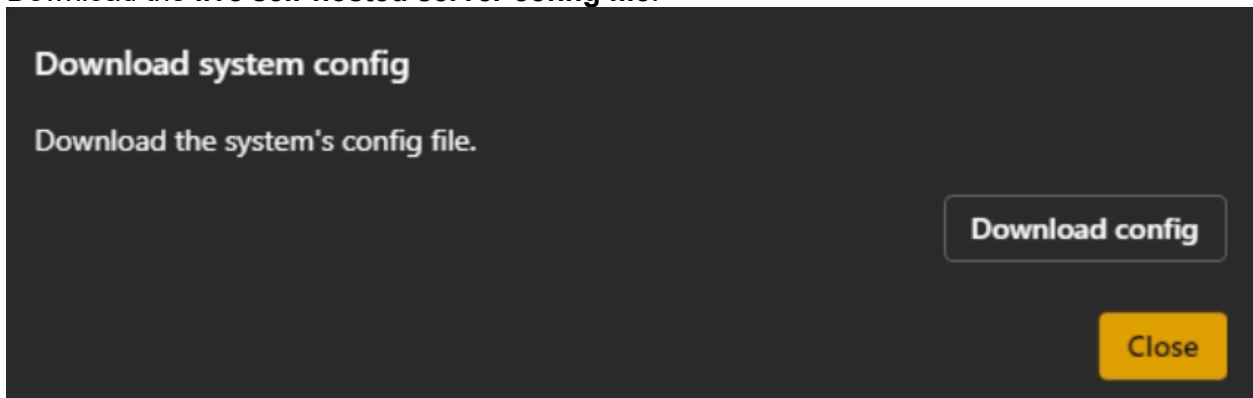
1. In **Self-hosted Server** app go to **Settings**  > **Body worn systems** and click **Add**.



2. Select the **system controller configuration file** previously created in [Body Worn System Setup](#) and click **Add**.

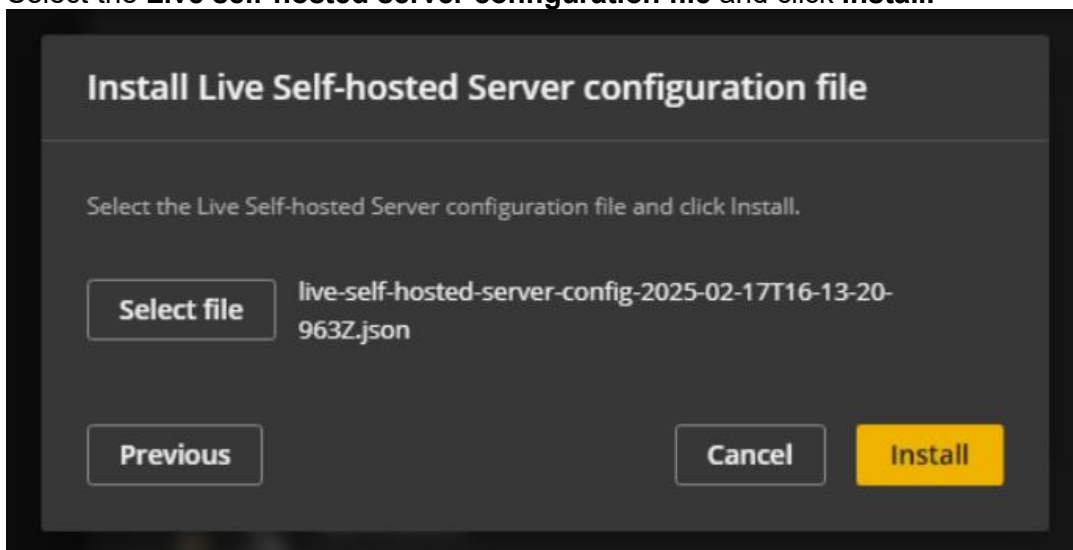


3. Download the **live self-hosted server config file**.





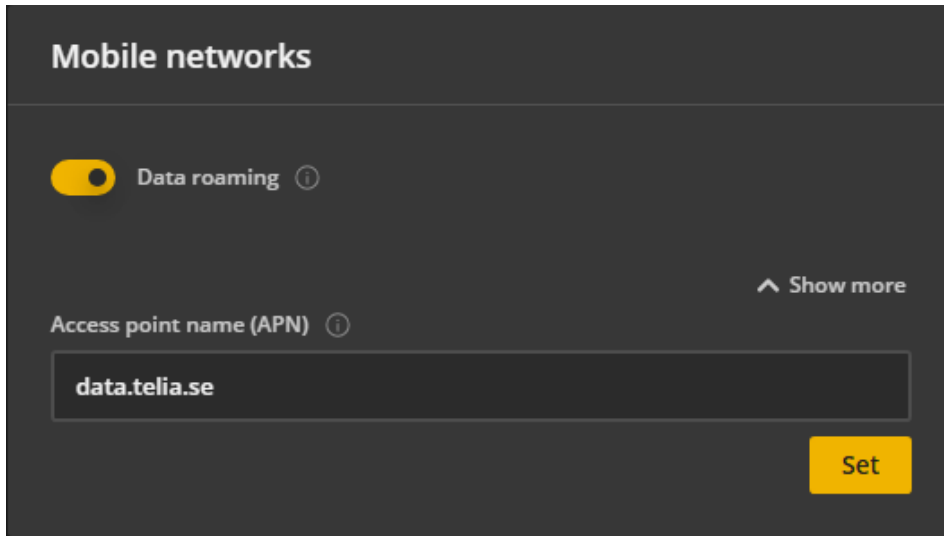
4. Go back to **AXIS Body Worn Manager** resume the wizard that was [paused from - Body Worn System Setup](#).

5. Select the **Live self-hosted server configuration file** and click **Install**.



4.5 Finalize BWL Setup in Body Worn Manager

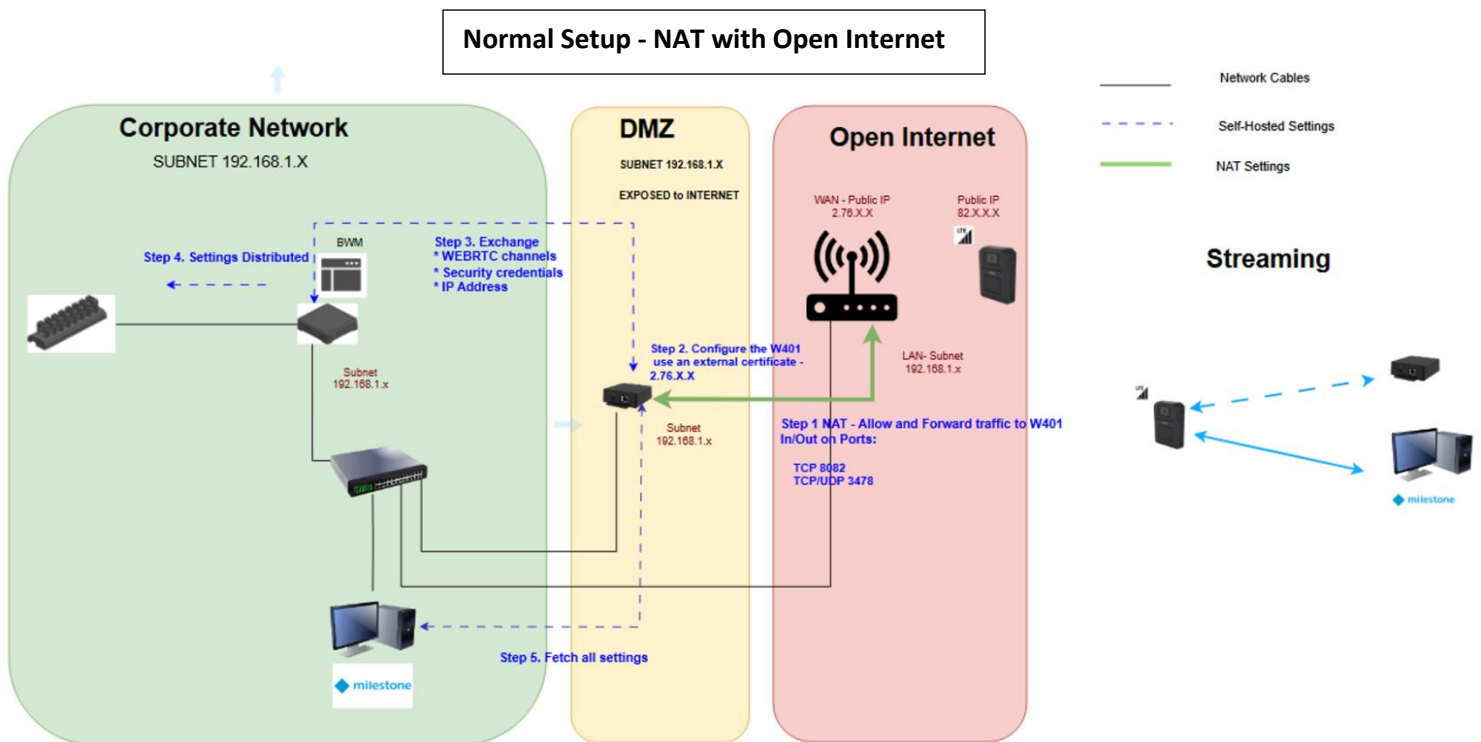
6. Go to **Camera profiles**  > **AXIS Body Worn Live** and allow **Streaming**.
7. Go **Settings**  > **Camera** > **Mobile Networks** > **Show More** > **APN**



5 – Scenario 3: Normal Setup – Advanced NAT Network

This is a complex setup involving router and NAT configuration. It's uncommon in professional deployments but suitable for smaller installations. Some network knowledge is required. The router must support NAT, NAT loopback, NTP, and DNS. The camera with a SIM card and LTE has a public internet address and needs to communicate with an internal corporate address. Place the Self-hosted Server device in the DMZ zone. The body-worn system and VMS should be in a closed corporate network. Firewalls may be involved, requiring specific ports to be opened.

Note: Ensure the router has a public internet address that the body worn camera can reach.

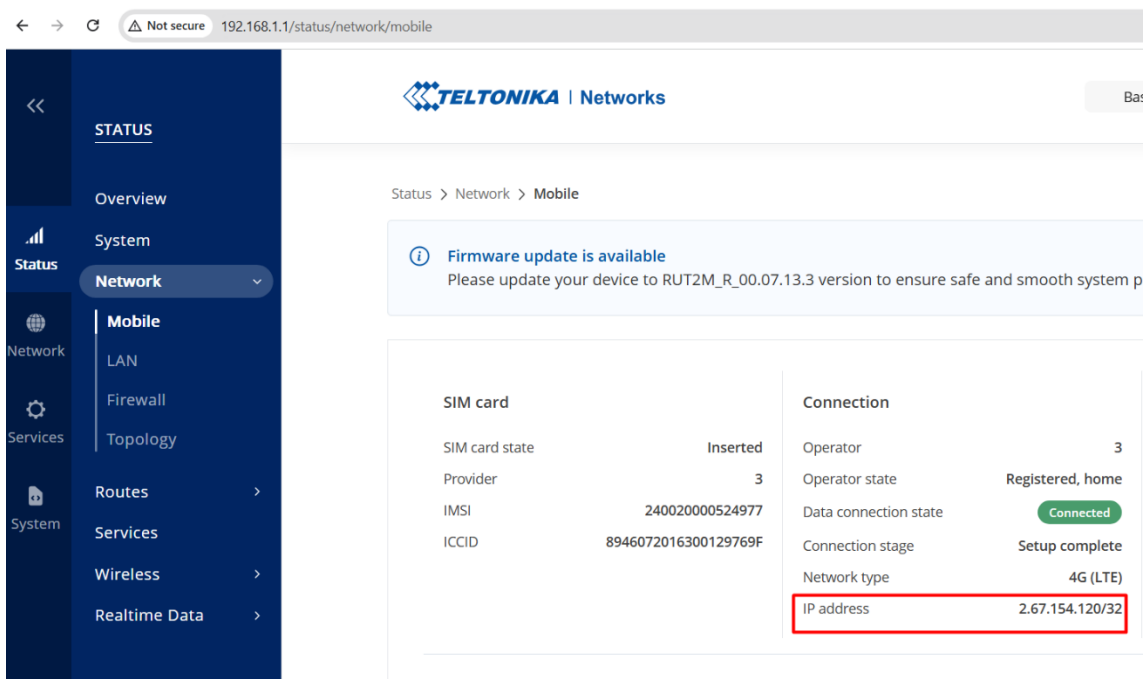


5.1 Prepare the router configuration

In this setup we use Teltonika RUT200 as router, the model has the following features:

- 4G Network support
- NAT loopback Support
- NAT Support (TCP, UDP)
- Wi-Fi
- Static IP via DHCP, DNS

4G LTE with public IP



The screenshot shows the Teltonika Networks web interface. The browser address bar displays "192.168.1.1/status/network/mobile". The left sidebar contains a navigation menu with categories: Status, Network, Services, and System. The main content area shows the "Mobile" status page. A notification banner indicates a firmware update is available. Below this, there are two columns of status information: "SIM card" and "Connection".

SIM card		Connection	
SIM card state	Inserted	Operator	3
Provider	3	Operator state	Registered, home
IMSI	240020000524977	Data connection state	Connected
ICCID	8946072016300129769F	Connection stage	Setup complete
		Network type	4G (LTE)
		IP address	2.67.154.120/32

NAT Loopback

^ "Signaling server group 1" port forward configuration

General Settings **Advanced Settings**

Source MAC address

Source IP address

Source port

External IP address

Enable NAT Loopback on

Extra arguments

NAT (TLS, STUN/TURN, Signaling Server)

You can change the incoming external ports (e.g., TLS 2443) or keep the default settings. However, the internal ports should remain default (e.g., 443, 8082, and 3478).

TLS Group 2	Incoming IPv4 TCP, UDP From <input type="text" value="wan"/> Via port 2443	To <input type="text" value="lan"/> IP 192.168.1.102 port 443
Signaling server group 2	Incoming IPv4 TCP, UDP From <input type="text" value="wan"/> Via port 8084	To <input type="text" value="lan"/> IP 192.168.1.102 port 8082
STUN-TURN group 2	Incoming IPv4 TCP, UDP From <input type="text" value="wan"/> Via port 3480	To <input type="text" value="lan"/> IP 192.168.1.102 port 3478

Dynamic Endpoint Range (UDP) - 49152-65535 (Data: Video, Audio, etc....) might be required to be opened

DNS

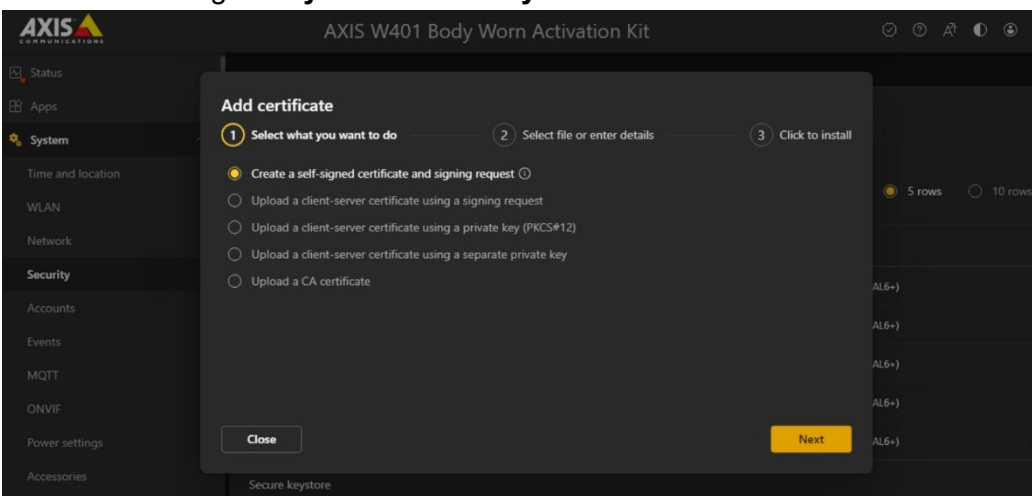
If your router supports built-in DNS services for the public IP, it's best to use them

5.2 Body Worn System Setup

Perform the same steps as in 4.1 [Body Worn System Setup](#) in scenario 2.

5.3 Prepare Self-hosted Server device

1. In W401 go to **System** > **Security** and click Add certificate.



2. Choose **Create a self-signed certificate**. (or you can upload and install your organization's client-server certificate)
3. Enter Certificate name, Common name = *Internet Public IP (2.67.X.X) or better DNS Name of the W401* and Country Code= *your choice*.

4. Click **Next** > **Generate**.
5. Go to **System** > **Network** > **HTTP and HTTPS**.
6. Under Allow access through, select **HTTPS**.
7. In the list of certificates, select the certificate you installed and click **Save**.

HTTP and HTTPS

Allow access through
HTTPS

HTTPS port
443

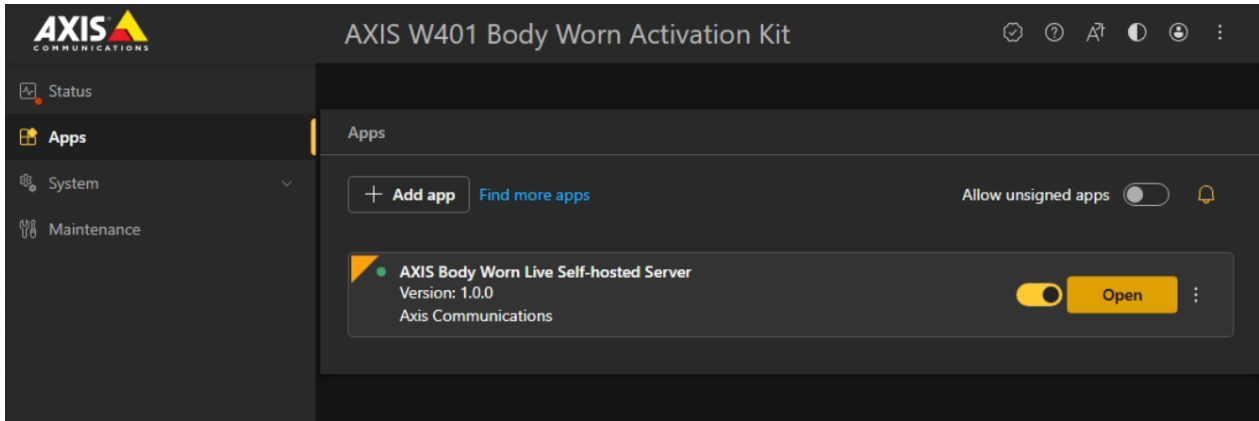
Certificate
Body Worn Live Self-hosted

Save

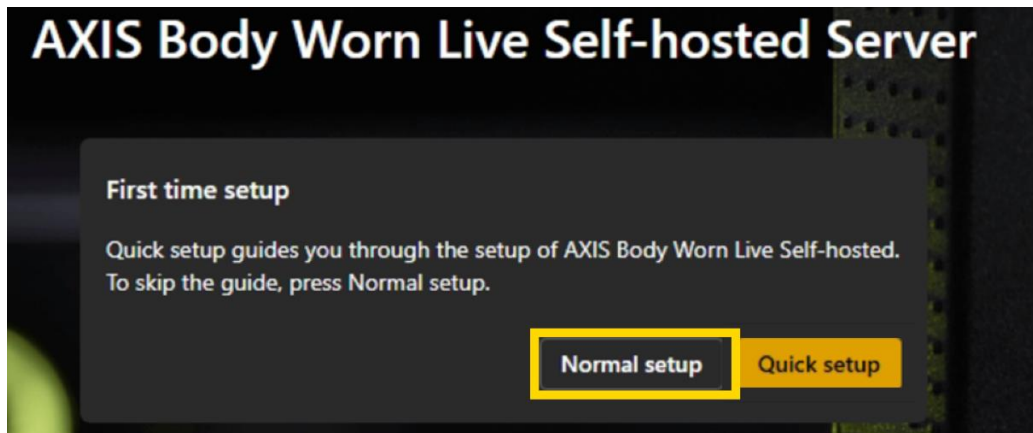
8. If not automatically done, reload and log in to the web page to use the new certificate.
9. Access the W401 using https, the external public IP address or its DNS, the router needs to support **NAT Hairpin** Examples:
 - <https://bwpdm.ddns.xxx> or <https://2.71.X.X>


5.4 Setup Self-hosted Server app

1. In W401 go to **Apps**.
2. Open the app.



3. Select **Normal setup**



4. Go to **Settings**  > **HTTPS**.
5. In the list of server certificates, select the certificate you installed when you prepared the device.
6. Click **Apply settings**. The server configuration is loaded automatically.
7. Under Server configuration enter the address endpoints/port, in the advanced settings enter the routers Public IP and click Apply Settings

AXIS Body Worn Live Self-hosted Server

Server configuration

Signaling endpoint *
bwpedm.ddns.net:8082

STUN endpoint *
bwpedm.ddns.net:3478

TURN endpoint *
bwpedm.ddns.net:3478

Advanced

Public IPv4 address ⓘ
2.70.133.157

Relay endpoint lower bound ⓘ
49152

Relay endpoint upper bound ⓘ
65535

Host endpoint lower bound ⓘ
49152

Host endpoint upper bound ⓘ
65535

TURN firewall exceptions ⓘ
IPv4 address or range (e.g. 10.0.1.2-10.0.1.10) Add

Apply settings

5.5 Connect Body Worn Live to Body Worn Manager

Perform the same steps as in 4.4 [Connect Body Worn Live to Body Worn Manager](#) in scenario 2.

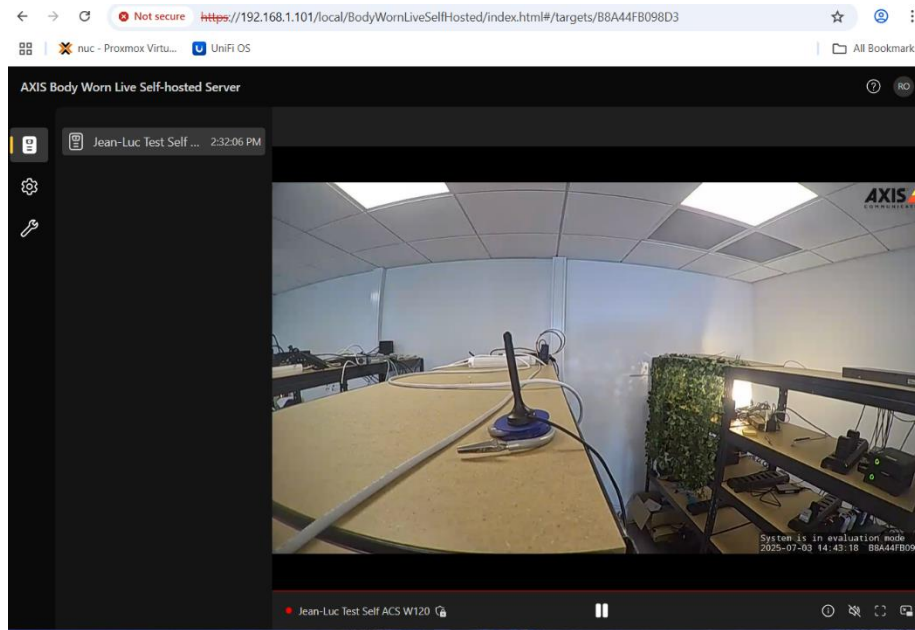
5.6 Finalize BWL Setup in Body Worn Manager

Go to **Camera profiles**  > **AXIS Body Worn Live** and allow **Streaming**.

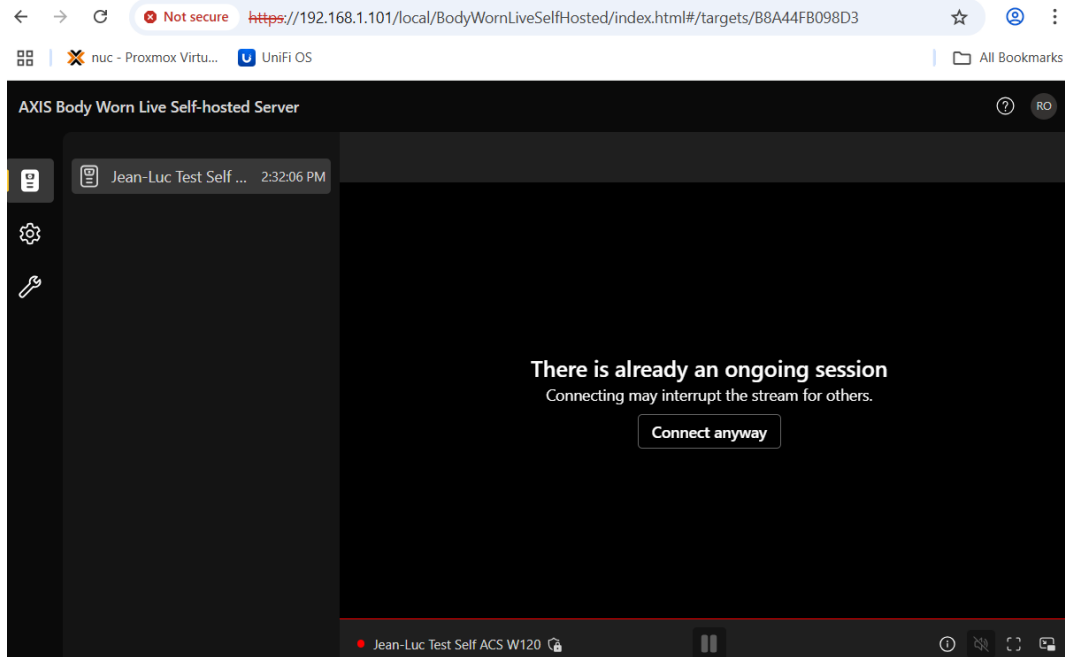
6 – Demo livestreaming player

The Self-hosted Server app includes a basic and limited player. This simple player is not designed to be used for livestream operations but serves as a demo and troubleshooting tool.

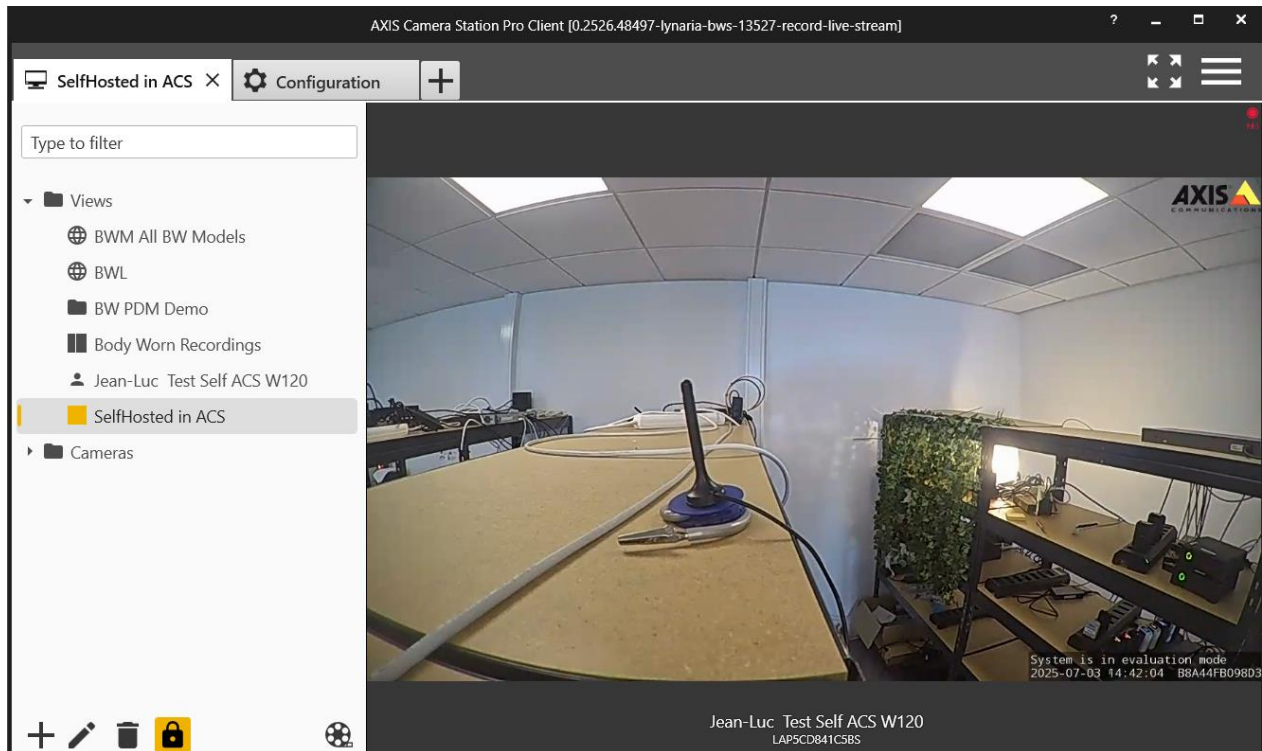
Use the simple demo player to verify if livestreaming is working as expected in the initial setup. After checking the livestream in W401, close the app. Then, proceed with the livestreaming configuration and viewing in the VMS.



Note: Only one viewer can view a livestreaming session from the body worn cameras.



In this case the VMS (ACS Pro) has already taken the channel.



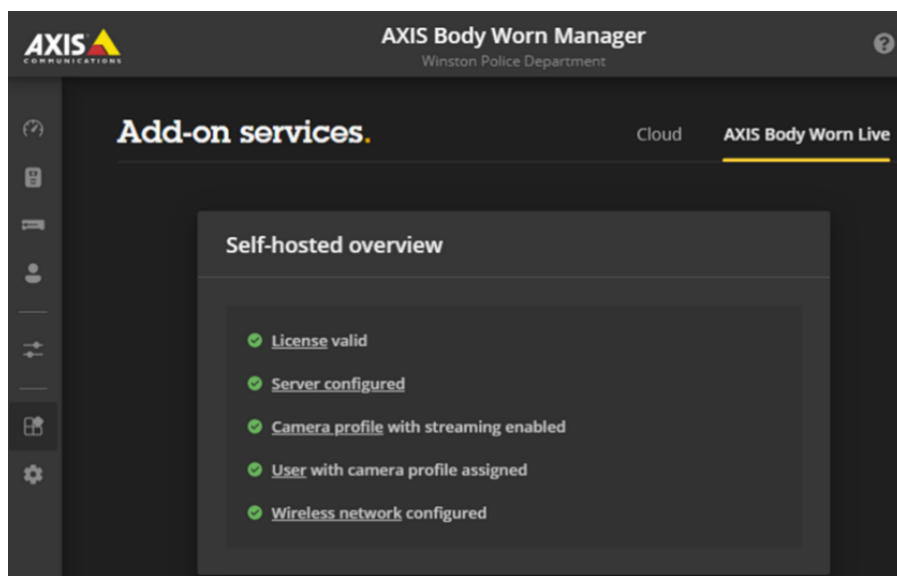
7 – Troubleshooting

General troubleshooting information is found in the manual: <https://help.axis.com/en-us/axis-body-worn-live-self-hosted#troubleshooting>

7.1 Setup - Verify the BWM self-hosted configuration

It's important that the BWM Self-hosted configuration is finalized.

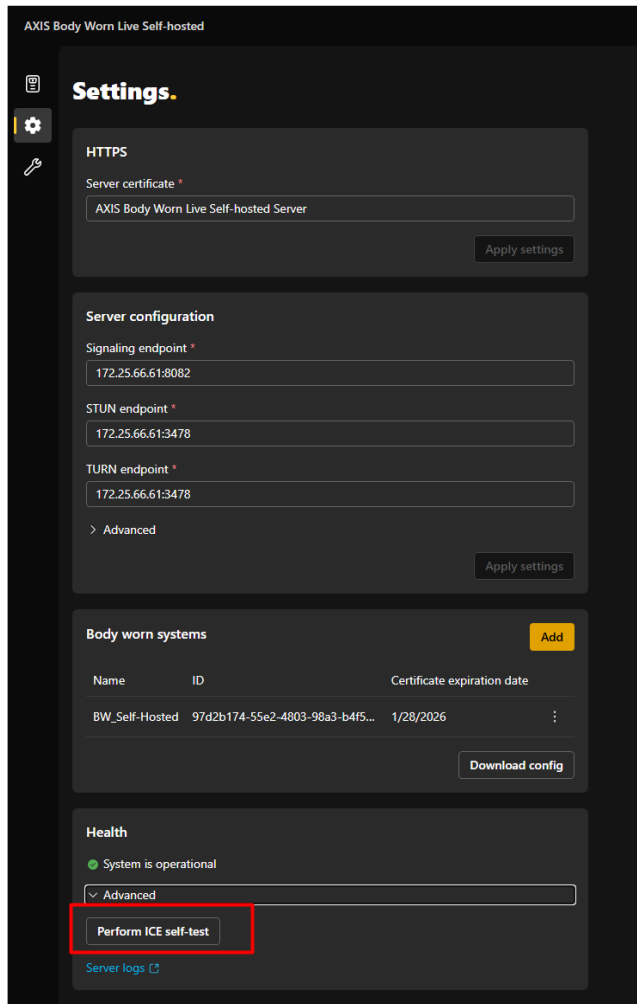
Note: This does not mean that the configuration is correct but rather finalized for streaming.



7.2 Setup - Verify the signaling server availability

Check that the Self-hosted Server app connects to the underlying signaling server without issues. The self-test will ensure that the web client can connect to and use the STUN & TURN server. The test may take a couple of minutes to complete. Leave this page open until it completes.

 Note: This does not validate the streaming availability



AXIS Body Worn Live Self-hosted

Settings.

HTTPS

Server certificate *

AXIS Body Worn Live Self-hosted Server

Apply settings

Server configuration

Signaling endpoint *

172.25.66.61:8082

STUN endpoint *

172.25.66.61:3478

TURN endpoint *

172.25.66.61:3478

> Advanced

Apply settings

Body worn systems Add

Name	ID	Certificate expiration date
BW_Self-Hosted	97d2b174-55e2-4803-98a3-b4f5...	1/28/2026

Download config

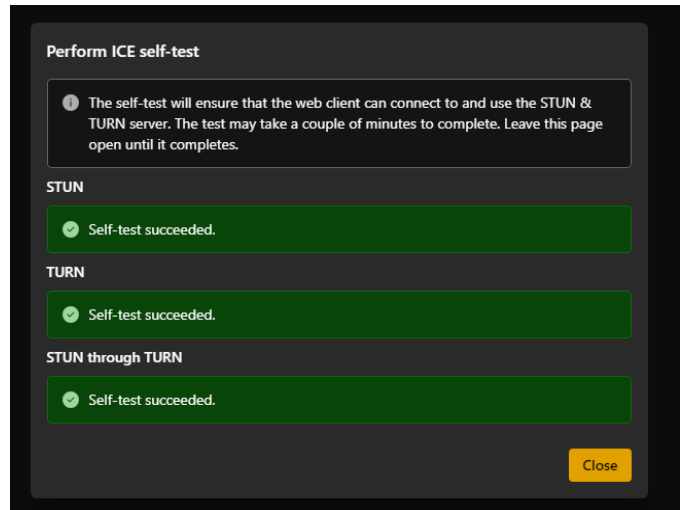
Health

System is operational

Advanced

Perform ICE self-test

Server logs



Perform ICE self-test

The self-test will ensure that the web client can connect to and use the STUN & TURN server. The test may take a couple of minutes to complete. Leave this page open until it completes.

STUN

Self-test succeeded.

TURN

Self-test succeeded.

STUN through TURN

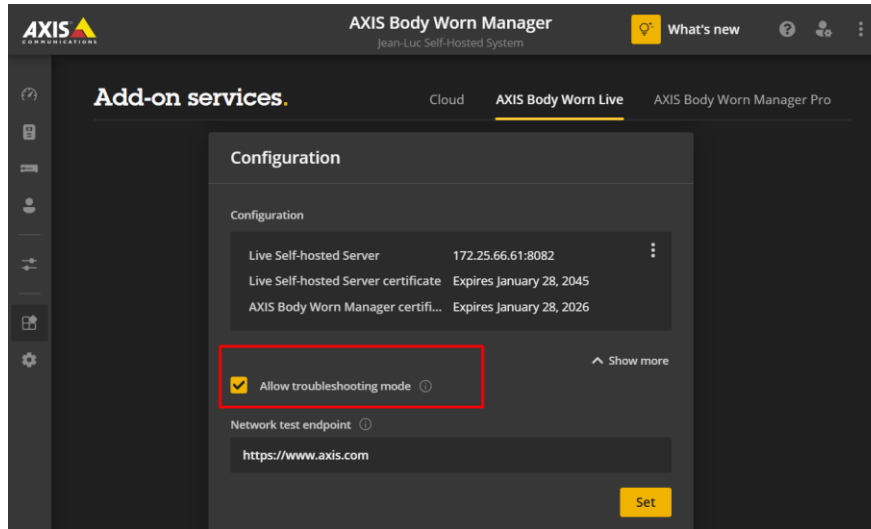
Self-test succeeded.

Close

7.3 Connection - Enable troubleshooting mode BWM

Troubleshooting mode is the ultimate tool in case of streaming error: The camera IP, the connection to the signaling server

1. Go **Add-on services > AXIS Body Worn Live**
2. In Server configuration, click Show more.
3. Turn on Allow troubleshooting mode.
4. Enter e.g. <https://www.axis.com> under Network test endpoint and click Set.



7.4 Connection - Enable troubleshooting mode BWC

1. Start livestreaming – Double tap side button
2. Switch ON Troubleshooting Mode - Double tap top button
3. Switch Screens for more information – Press top button
4. Exit Troubleshooting mode - long press top button



7.5 Performance - Info tab

The screenshot displays the web interface for the AXIS Body Worn Live Self-Hosted Server. The browser address bar shows the URL: `https://192.168.1.101/local/BodyWornLiveSelfHosted/index.html#/targets/B8A44FB098D3`. The interface includes a navigation menu on the left with icons for home, settings, and a wrench. The main content area features a video feed of a room with a desk and a microphone. On the right side, there is an 'Overview' panel with the following performance metrics:

- Overview**
 - Status: connected
- Video**
 - Resolution: 1280x720px
 - FPS: 25
 - Video bytes received: 863.82 KiB (163.10 Kib/s)
 - Video packets lost: 0
 - Video processing latency: 22.04 ms
 - Average video E2E latency: 55.50 ms
- Audio**
 - Audio bytes received: 169.50 KiB (62.55 Kib/s)
 - Audio packets lost: 0
 - Audio processing latency: 0.00 ms
 - Average audio E2E latency: 33.46 ms
- Network**
 - Local: relay over udp
 - Remote: host over udp
 - Current round trip time: 34.00 ms
 - Average round trip time: 66.92 ms

At the bottom right of the video feed, a status message reads: "System is in evaluation mode 2025-07-03 14:44:39 B8A44FB098D". The video player controls at the bottom show a play button, a volume icon, and a full-screen icon.

Network:

Local -

Local - relay over udp > TURN is used

Considerations and limitations

Limitations

- The connection does not fall back from LTE to Wi-Fi if the signal is lost.
- The connection does not fall back from a configured SSID to a second SSID.
- The camera connection doesn't support IEEE 802.1x, IPv6, or proxies.
- You cannot run BWL Axis-Hosted (Cloud) and Self-Hosted in the same system

Recommendations

- If you plan to use Wi-Fi, we recommend that the access points support IEEE 802.11k/v/r.
- Minimum recommended network infrastructure services are DHCP, DNS, and NTP server.
- If your network is connected to the internet, the W401 must be reachable from a public IPv4 address (no CGNAT).
- If your network is connected to the internet and you are using body worn cameras connected to a mobile network, the W401 should have appropriate DDoS mitigation (gateway/firewall solution) in place.
- Infrastructure that supports 2.5 Mbps (360p resolution) or 8 Mbps (720p resolution) per body worn camera.