Installation and Operation Guide V1.1
Firmware 1.5.81

Desktop Models:
4K-SC
UHD-SC
Rugged Variants

openGear Models:
OG-3G-2E
OG-12G-2E

HARDWARE ENCODERS

H265 HEVC | H264 AVC

User guide notes:
- The screenshots in this manual might not exactly reflect your user interface due to variations in firmware revisions
- The user interface between Desktop and openGear differs slightly due to feature differences

© 2023 Osprey Video. All rights reserved. Osprey® is the registered trademark of Osprey Video. Any other product names, trademarks, trade names, service marks, or service names owned or registered by any other company and mentioned herein are the property of their respective companies. No part of this specification may be reproduced, transcribed, transmitted or stored in a retrieval system in any part or by any means without the express written consent of Osprey Video. Osprey Video reserves the right to change any products herein at any time and without notice. Osprey Video makes no representations or warranties regarding the content of this document and assumes no responsibility for any errors contained herein.

openGear is a registered trademark of Ross Video Ltd

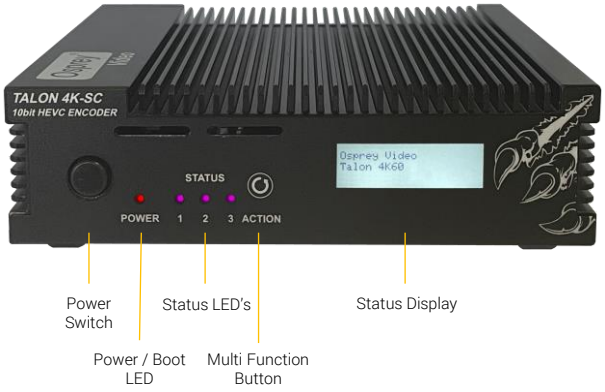
Contents

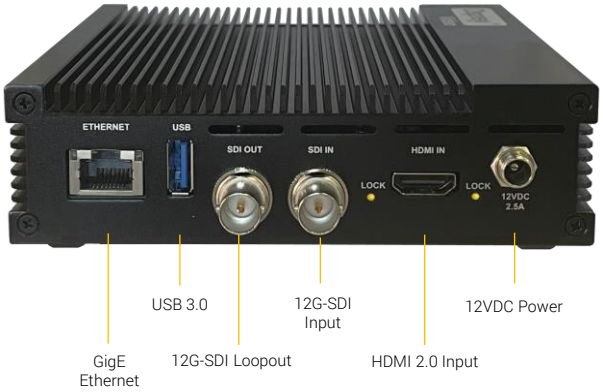
Introduction
- Hardware Features Talon Desktop ... 3
- Hardware Features Talon openGear ... 4
- Ross openGear Dashboard ... 5
- Network Configuration Desktop Encoders ... 6
- Block Diagram ... 7
- Simulcast RTMP(S) ... 7

Web Interface
- **Overview** ... 8
- **Dashboard** ... 8
- **System**
  - Device Settings ... 9
  - Storage ... 10
  - Network
    - Network Settings ... 11
    - Dynamic DNS Configuration ... 12
  - Security
    - Advisory Notice & Consent Banner ... 13
    - Management Whitelist ... 13
  - Secure Web Server (HTTPS) ... 14
  - VPN
    - Open VPN ... 15
    - OpenConnect VPN ... 16
  - Date & Time ... 17
  - LCD, LED, Button Config ... 18
- **Channel Setup**
  - Output Protocol ... 19
  - Video Archiving ... 20
  - Streaming Protocols
    - RTMP, RTMPS, UDP ... 21
    - RTP, SRT ... 22
    - RTSP, WebRTC ... 23
    - Zixi ... 24
  - Video Encoding Settings ... 25
  - Audio Encoding Settings ... 27
  - KLV ... 28
- **Status Page** ... 29
  - **Actions**
  - Start / Stop ... 29
- **Support**
  - Firmware Updates ... 30
  - Factory Restore ... 31
  - Factory Defaults ... 31

General Information
- Enterprise and Security ... 34
- Opensource Listing ... 35
- Safety and Compliance ... 36

Hardware Features 4K-SC and UHD-SC





- Power Switch — Physical ON/OFF Switch
- Power / Boot LED — Red at Power Up, turning blue once booting process is complete
- Status LED's — Status LED's that can be configured in Talon UI – System – IO Configuration
- Multi Function Button — Start, Stop, Reset
- Status Display — Displayed information can be configured in Talon UI – System – IO Configuration (4K-SC only)
- GigE Ethernet — One Gigabit Ethernet RJ45 connection
- USB 3.0 — Save to File for an MP4 copy of the live stream
- 12G-SDI Loopout — Loopout of the SDI Input (4K-SC only)
- 12G-SDI Input — SDI Input up to DCI60
- HDMI 2.0 Input — Non-HDCP compliant HDMI 2.0 input (4K-SC only)
- 12VDC Power — Locking 12V Power Input

In the box

- Talon Encoder
- Locking 12VDC / 36W Power Supply
- Mounting Brackets

UHD-SC:

Hardware Features OG-3G-2E and OG-12G-2E

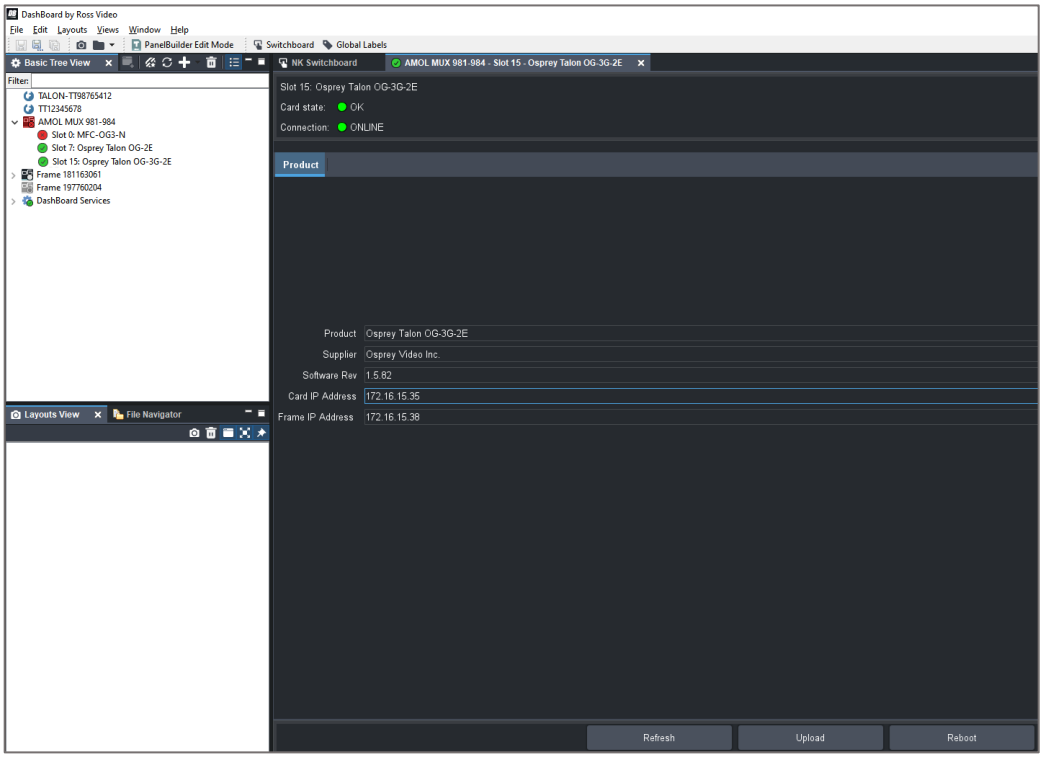
- Power / Boot LED — Red at Power Up, turning blue once booting process is complete
- Status LED's — Status LED's that can be configured in Talon UI – System – IO Configuration
- SDI Inputs — 3G-SDI on OG-3G-2E (Gold), 12G-SDI on OG-12G-2E (Silver)
- GigE Ethernet — Gigabit Ethernet #1 RJ45 connection
- Midplane Connector — Gigabit Ethernet #2 (requires Ross Video MFC-OG3-N12VDC Network Controller), Can Bus (for ROSS Dashboard), 12VDC Power
- NVME 2280 — PCIe x1 NVME Slot for Video Archiving (Drive not included)

In the box

- Talon Encoder
- Rear I/O Bracket

Ross openGear Dashboard

The DashBoard provides basic information about the openGear cards configured for the frame



Copy and paste the Encoder IP address into a web browser to access its user interface. Default user “admin” and password “osprey”

“Reboot” will perform a hard reboot for the Talon Encoder

“Refresh” will refresh the dashboard

“Upload” – not used

Network Configuration Desktop Models

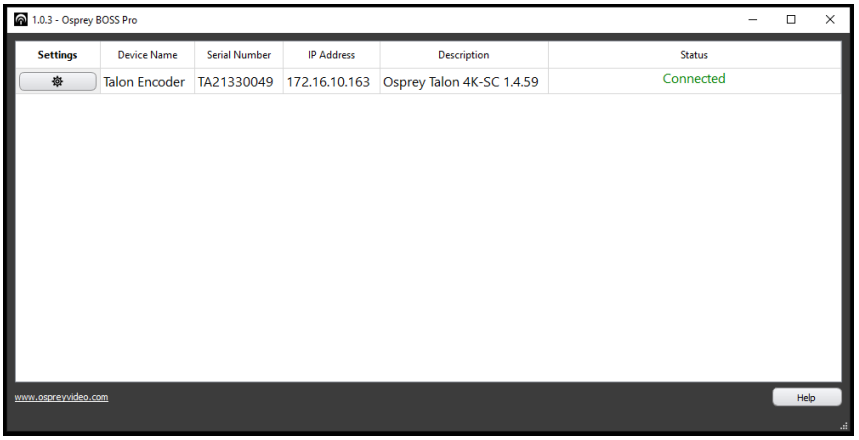
Important! Talon Encoders ship from the factory in DHCP mode. Please ensure your host PC and Talon are connected to the same network supporting DHCP.

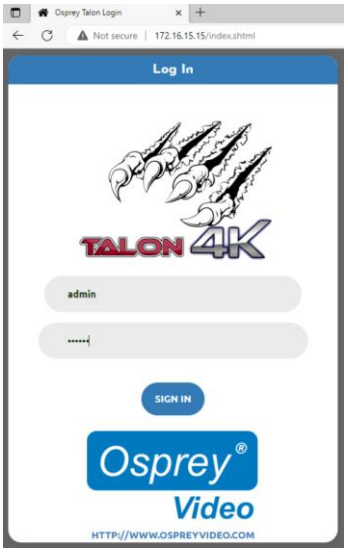
1. Connect Talon to your network using a CAT5 or faster Ethernet cable
2. Connect Talon to power using the supplied 12V adapter. Ensure the barrel connector is fully engaged and locked
3. Power up Talon with the front power switch
    - Red "Power" LED will turn blue once the booting process is complete
    - The assigned IP address will display (4K-SC only). This might take up to a minute
4. Connect to Talon from your host PC
    - Option #1: Type the IP address into your web browser
    - Option #2: Download "Boss Pro" from www.ospreyvideo.com to find all Talons on your network
5. Default login credentials
    - Username: admin
    - Password: osprey

Setting up Talon without Network access or with Network without DHCP server using APIPA

1. Verify your PC is set to Automatic IP
2. Connect Talon directly to your PC with an Ethernet cable (ensure the PC doesn't have network connection though Wifi, USB, etc)
3. Follow above instructions beginning with step 2.

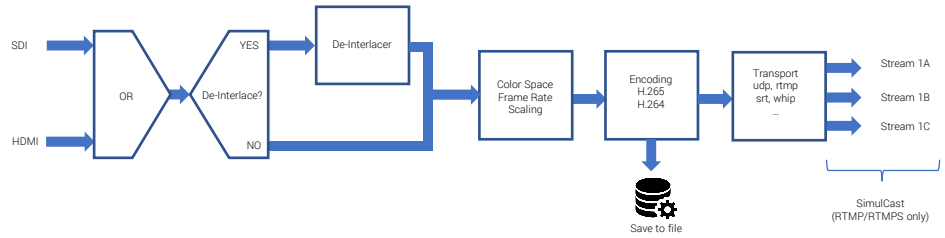
APIPA - Automatic Private IP Addressing (APIPA) is a feature of Windows-based OS -- included since Windows 98 and Windows ME -- that enables a Dynamic Host Configuration Protocol client to automatically assign an IP address to itself when there's no DHCP server available to perform that function.



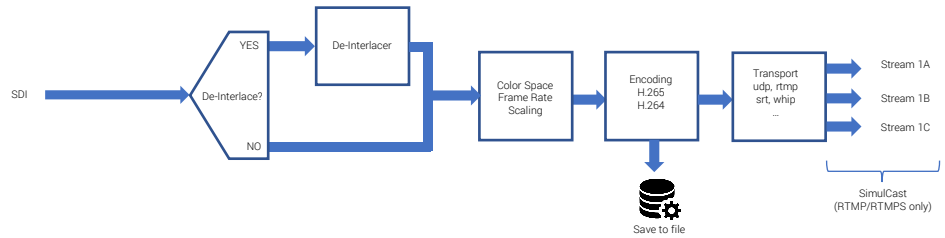


Block Diagrams

Talon 4K-SC



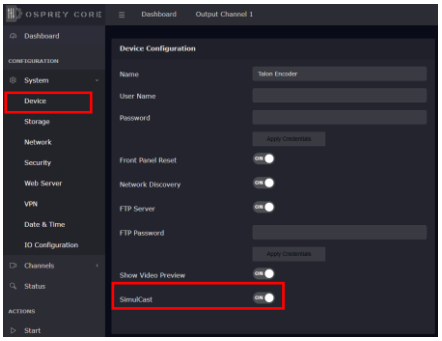
Talon UHD-SC and openGear (two independent channels on openGear)



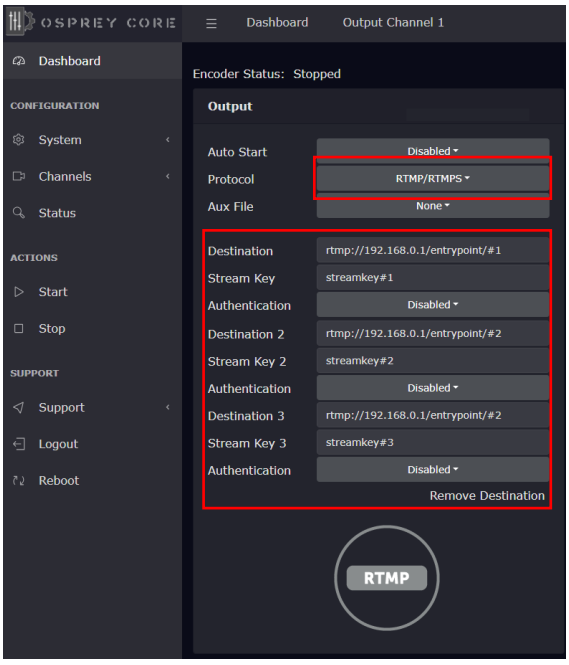
Simulcast for RTMP and RTMPS

Multiple Streams using **Simulcast**

Simulcast must be enabled under **Device - Simulcast**



RTMP and **RTMPS** protocols allow for up to 3 transport streams to independent destinations. The Video and audio encode settings for all streams are identical.



Connection or link errors will stop all active streams

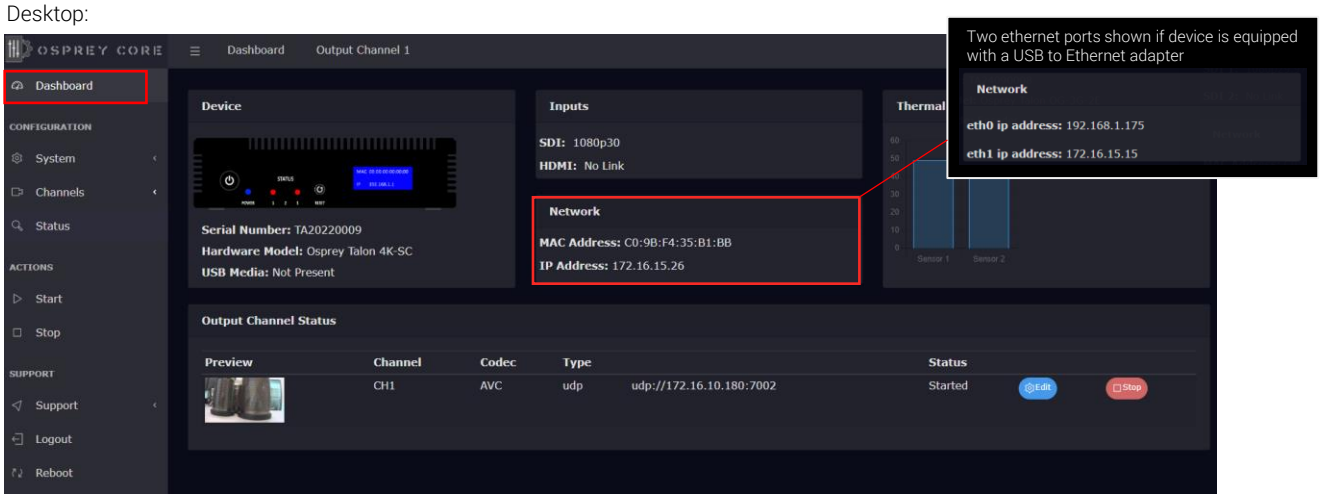
Web Interface - Dashboard

Overview

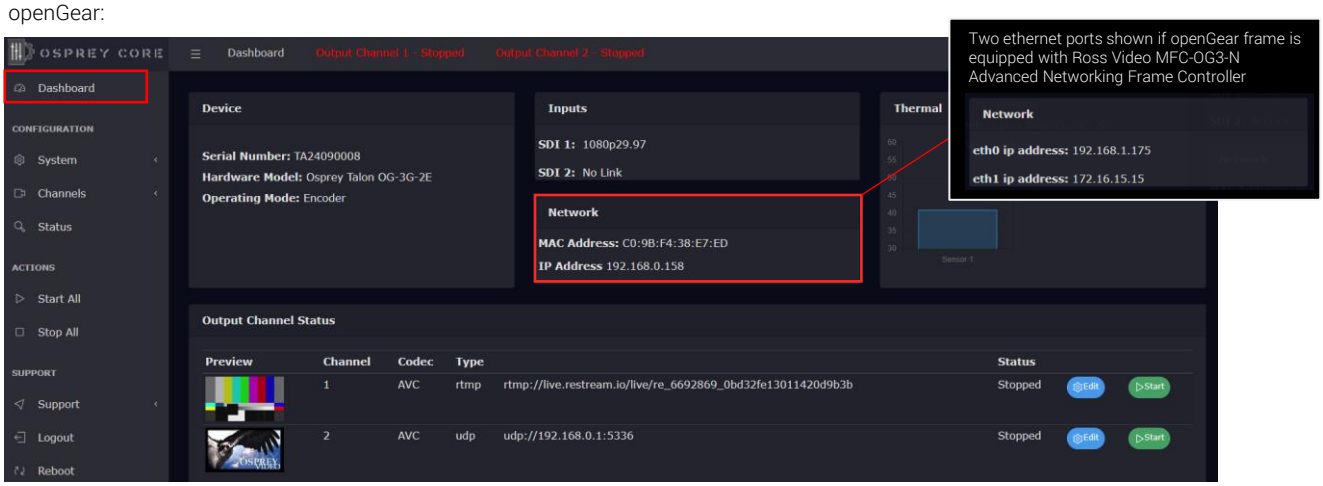
A web server in Talon allows for system control and stream settings via web browser. All commonly used Windows, Mac and Linux web browsers are supported. Please ensure your device is connected to the same network as Talon (see Page 5 for further instructions). To connect to the interface simply enter the IP address of your Talon into the web browser. Default login for a factory default Talon is **user: admin** and **password: osprey**.

The Dashboard provides basic information about the status of your Talon and a video preview* of your output channel.

Desktop:



openGear:



* Preview will stop once an Encoder is started

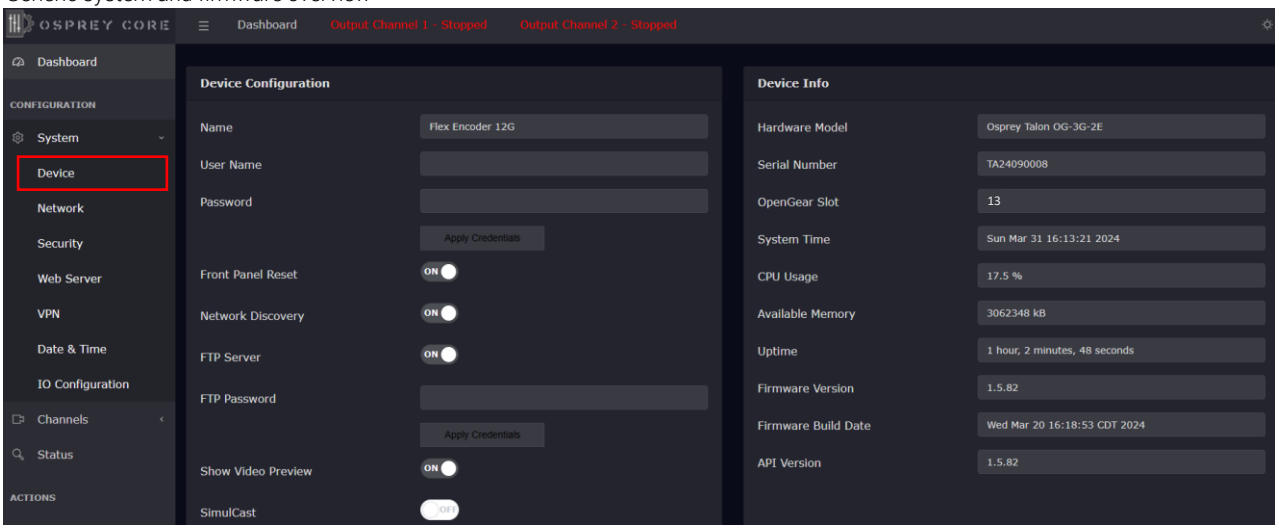
Web Interface - Device

System Settings - Device Configuration

Name	change your device name
User Name	change user login name credentials
Password	change user login password credentials
Front Panel Reset	enable/disable front panel “ACTION” button reset feature
Network Discovery	Network Discovery allows computers and devices to find one another when they are on the same network. This service is turned ‘on’ by default. To stop Discovery services, select ‘off’. Note that monitoring tools such as Osprey Boss require Discovery to locate Talon devices on the network. Osprey Boss will not be able to see any system that has Discovery turned off
FTP Server	on unit ftp server - default user: ‘talon’. Remote access to USB/NVME storage drive
FTP Password	on unit ftp server - password: ‘access’. Remote access to USB/NVME storage drive
Show Video Preview	disable “Dashboard Video Preview” to improve UI responsiveness and CPU usage
Simulcast	enable Simulcast for RTMP protocols to configure up to three simultaneous destinations for single RTMP stream

System Settings - Device Info

Generic system and firmware overview



* “openGear Slot” is only displayed on openGear devices

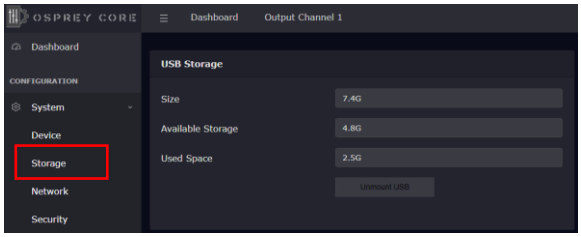
Web Interface –Storage and Network Configuration

System Settings –Storage

This option is only displayed if a valid storage media is present (USB for Desktop, NVME for openGear)

Please refresh the browser page after inserting a drive as the page doesn't dynamically refresh.

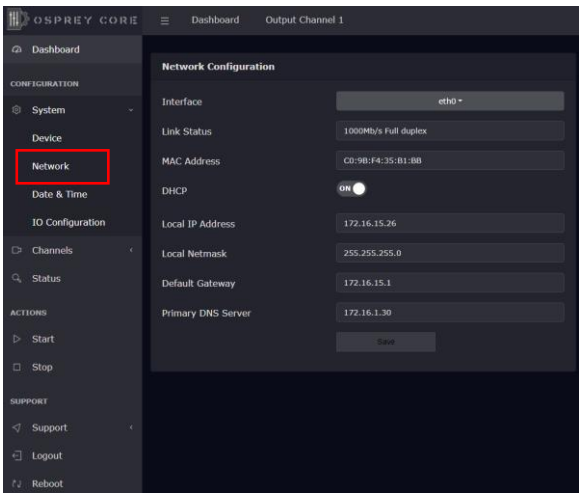
Always unmount the USB drive before unplugging it!!!



see page 20 for further details

System Settings – Network Configuration

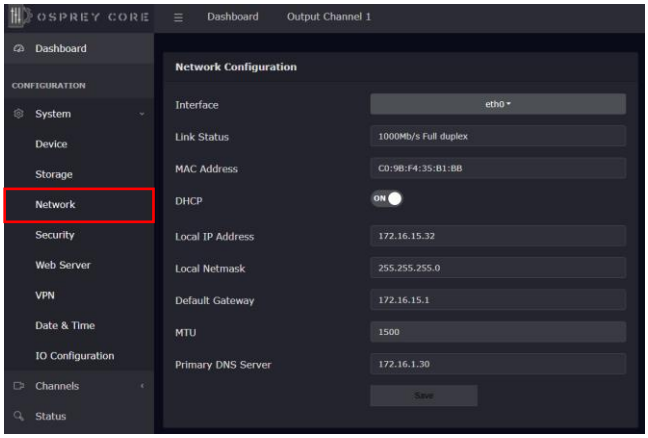
Interface	network port identification. If additional network devices are installed, they would be selectable here.
Link Status	Indicates link speed 10/100/1000Mbps (not network speed) and port status, full or half duplex.
MAC Address	Talon MAC ID
DHCP	enable/disable DHCP
Local IP Address	dynamic if DHCP is on. Otherwise, a new valid IP address can be entered here
Local Netmask	dynamic if DHCP is on. Otherwise, a new valid netmask can be entered here
Default Gateway	dynamic if DHCP is on. Otherwise, a new valid gateway can be entered here
Primary DNS Server	dynamic if DHCP is on. Otherwise, a new valid DNS can be entered here



Web Interface – Network Configuration

System Settings – Network Configuration

Interface	network port identification. If additional network devices are installed, they would be selectable here.
Link Status	Indicates link speed 10/100/1000Mbps (not network speed) and port status, full or half duplex.
MAC Address	Talon MAC ID
DHCP	enable/disable DHCP
Local IP Address	dynamic if DHCP is on. Otherwise, a new valid IP address can be entered here
Local Netmask	dynamic if DHCP is on. Otherwise, a new valid netmask can be entered here
Default Gateway	dynamic if DHCP is on. Otherwise, a new valid gateway can be entered here
MTU	maximum transmission unit in bytes – packet size maximum is 1500
Primary DNS Server	dynamic if DHCP is on. Otherwise, a new valid DNS can be entered here



Important Dual NIC information

Where two NIC's are used the Interface pull down will have "eth0' and "eth1"

Each configuration now includes "Primary DNS Server" and "Secondary DNS Server".

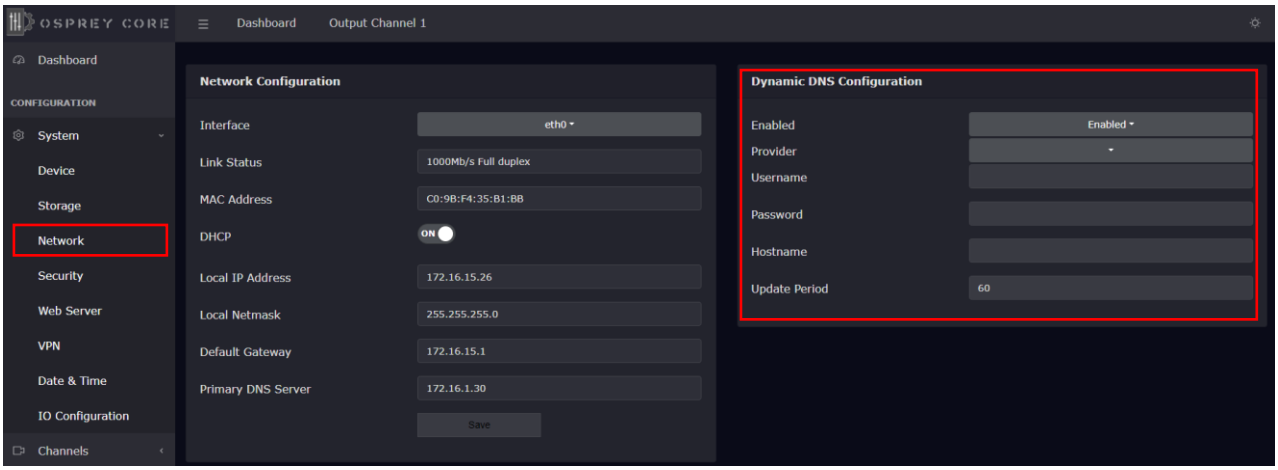
When the two NICs are on separate networks, only one (usually eth0) should be configured as DHCP. The second NIC should be configured as Static. The Default Gateway should only be configured for the network handling the outbound stream. In that case, the second network should be configured without a default gateway.

NOTE: When saving network settings, save each NIC settings separately. Performing a SAVE on eth0 will not have any effect on eth1.

DNS settings: The OS only allows for one pair of DNS servers. Usually, the DHCP server sets the DNS servers as well. If a static DNS server is needed, then both NICs must be set to STATIC addresses for the change to take effect.

Web Interface – DNS Configuration

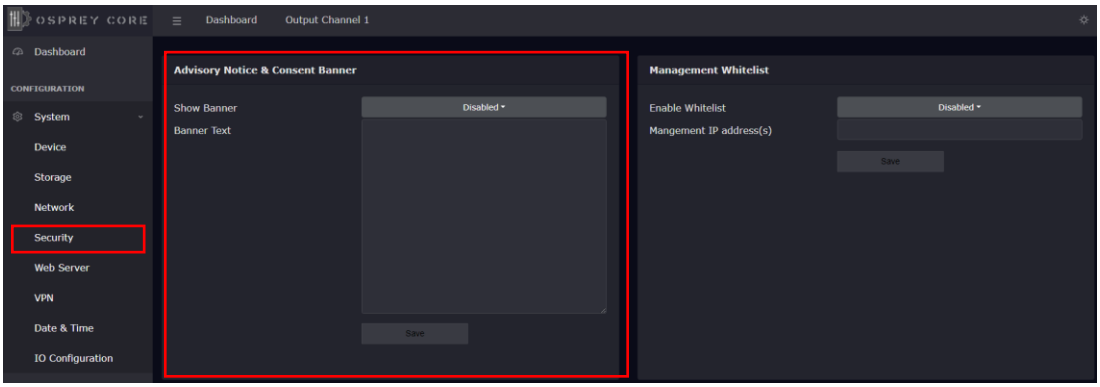
Dynamic DNS configuration



Web Interface –Advisory Notice & Consent Banner

US Government entities and many other governments and corporations require an approved use notification before granting access to publicly accessible systems.

Show Banner enable or disable
Banner Text: enter text for the banner here.
Save: enables banner

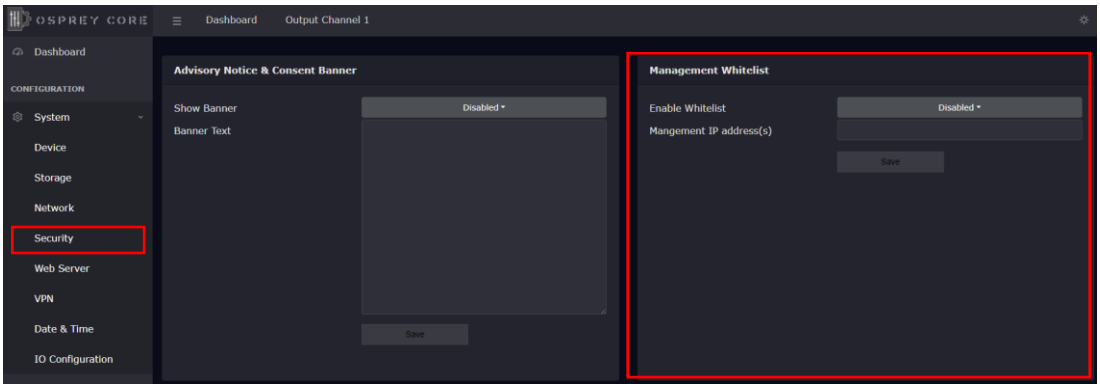


Web Interface –Whitelist and Firewall

Whitelist/Firewall

Blocks all incoming ICMP (ping) requests. Blocks incoming traffic on ports 80 (http) ,8080,8088,443 (SSL), 21 (FTP) and 22 (SSH) unless it originates from an address on the whitelist. RTMP and RTSP TCP ports are not blocked.
Multiple addresses may be added to the list, separated by comma.

Before applying care should be taken to not inadvertently lock all users out by typing in an invalid address.



Web Interface – Secure Web Server

Enabling Secure Server (HTTPS) adds a secure encryption layer to the Talon internal web server, along with certificate-based authentication.

Secure Server (HTTPS)

Enabled Only HTTPS will be supported on the Web Interface. (Server certificate required)
Disabled Only HTTP will be supported on the Web Interface. A certificate is not required.

NOTE: Once Secure Server is enabled Talon will reboot. When it finishes the reboot, the page you were on will not be accessible as it is not secure. You will need to change the URL to "HTTPS://" to login again.

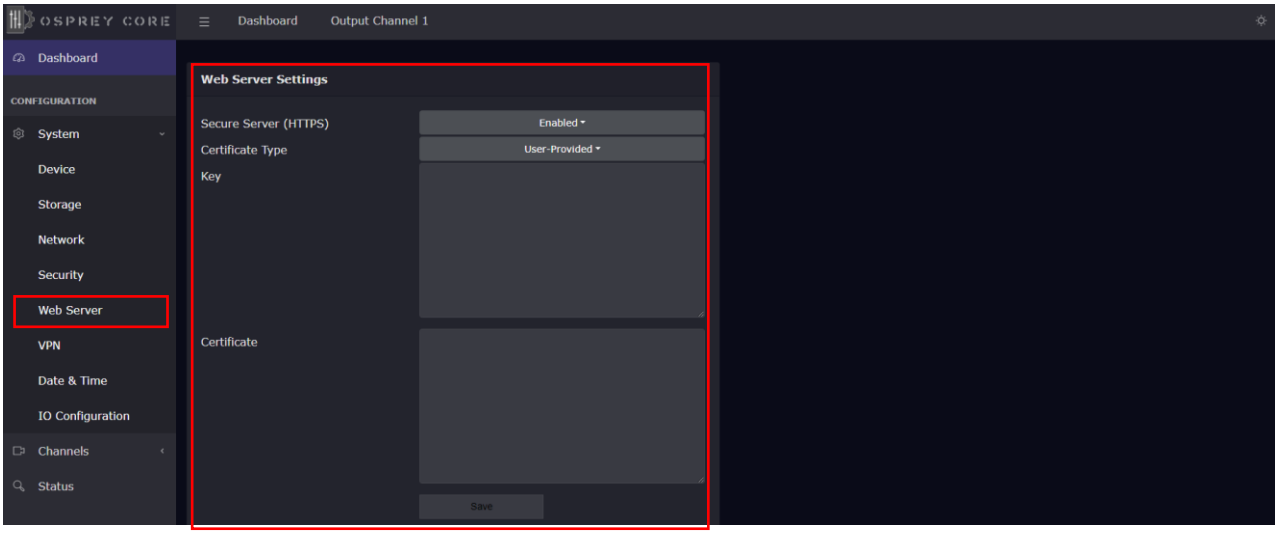
When you change the URL, if you have selected "Self-Signed" for the certificate your browser may warn you that the site is not secure.

Certificate Type

Self-Signed: Talon will self-generate an SSL Certificate to secure the website. While this will allow access via HTTPS, it is usually only a temporary solution for security as the certificate isn't signed by a Certificate Authority (CA).
NOTE: When this option is chosen, users accessing the Web Interface for the first time will receive a warning in their browser not to proceed because a self-signed certificate cannot be validated by any outside authority. The accessing browser will always show following warning:

User Provided: If your organization has their own private key, it can be installed. The server only requires the private key provided by the certification authority, and the security certificate. These are easily cut and pasted from the information provided by your signing authority.

Key Insert Private Key here.
Certificate Insert Security Certificate here.



Web Interface –Open VPN

A VPN creates a private network tunnel over the public internet, that securely connects and encrypts data between two networks. When properly connected via a VPN, a remote Talon can be administered as if it were on your home network, regardless of location. Talon has included two standalone VPN clients, both licensed under GPLv2. Between these two clients, access is available to most VPN users.

Open VPN Configuration:
OpenVPN is an open-source virtual private network system that can create secure point-to-point connections. It is offered in both client and server applications. OpenVPN is used by many manufacturers home and SMB routers, allowing users to create tunneled access into their own private networks. It can be configured as a Site-to-Site VPN or a Client to Server VPN. More information about the software is available at www.openvpn.net

Auto Start

ENABLED: When Auto Start is enabled, the VPN will connect as Talon boots without requiring user intervention. This is useful for lights-out operations where power may be interrupted. Or, for systems at locations which always require remote administration. CAUTION: Thoroughly test the VPN settings before enabling Auto Start.

DISABLED: VPN will only start when "connect" is pressed

Configuration Information

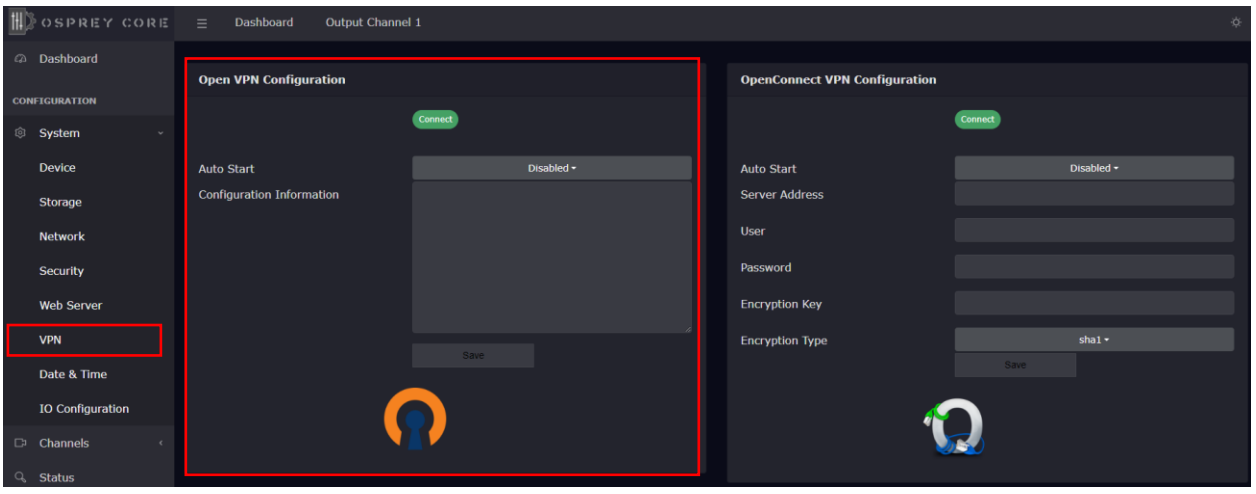
Routers that support OpenVPN generally have a utility to configure the VPN client and download a .ovpn file. To configure the Talon, simply open the .ovpn file in a txt editor and paste the contents into the "Configuration Information" pane.

Save

Press "Save" to preserve the connection information. Unless it is saved, it will be lost at the next reboot.

Connect

The connect button uses the information in the .ovpn file to create a VPN tunnel. If the tunnel is successful, the Connect button will turn RED and the label will say "disconnect". Below the button the local address of the Talon will show as "Local" and the address of the remote connection will be shown as "Remote". Pressing "disconnect" will stop the VPN service.

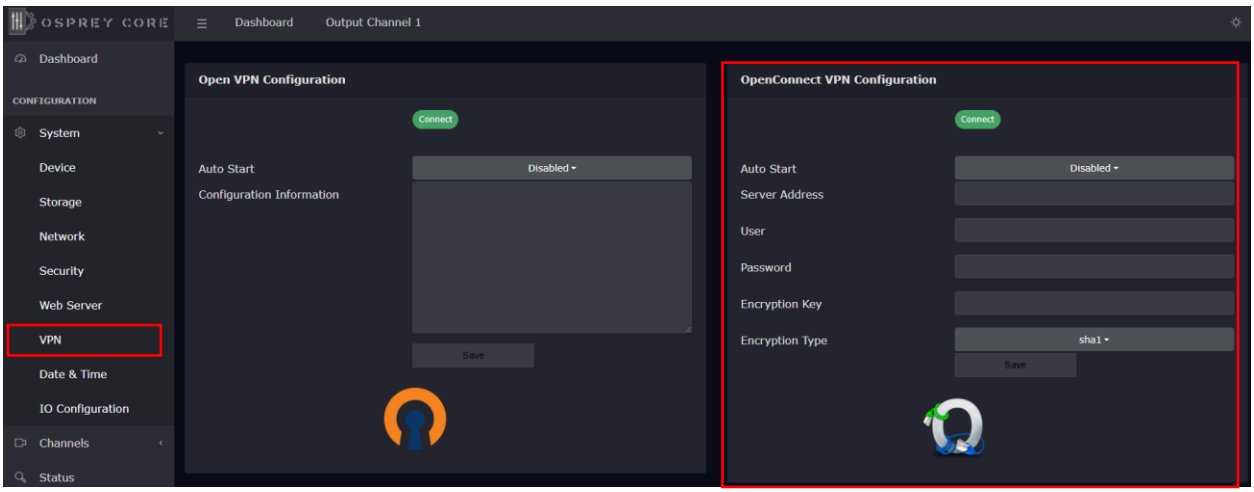


Web Interface –OpenConnect VPN

OpenConnect VPN Configuration:

OpenConnect is a cross-platform multi-protocol SSL VPN client. It was selected for Talon because it is compatible with the Cisco AnyConnect®. OpenConnect is not officially supported by or associated in any way with Cisco Systems. It just happened to interoperate with their equipment.

Auto Start	ENABLED: When Auto Start is enabled, the VPN will connect as Talon boots without requiring user intervention. This is useful for lights-out operations where power may be interrupted. Or, for systems at locations which always require remote administration. CAUTION: Thoroughly test the VPN settings before enabling Auto Start. DISABLED: VPN will only start when "connect" is pressed
Server Address	URL or IP address of the VPN server
User	username for the VPN account
Password	password for the VPN account
Encryption Key	key provided by your VPN
Encryption Type	sha1, sha256 and pin-sha256 are the available options. Encryption Type must match the type assigned by the server.
Save	Press "Save" to preserve the connection information. Unless it is saved, it will be lost at the next reboot.
Connect	Selecting "Connect" will establish a tunnel connection via OpenConnect VPN. Upon successful connection the IP address of your connection will appear below the "Disconnect" button.

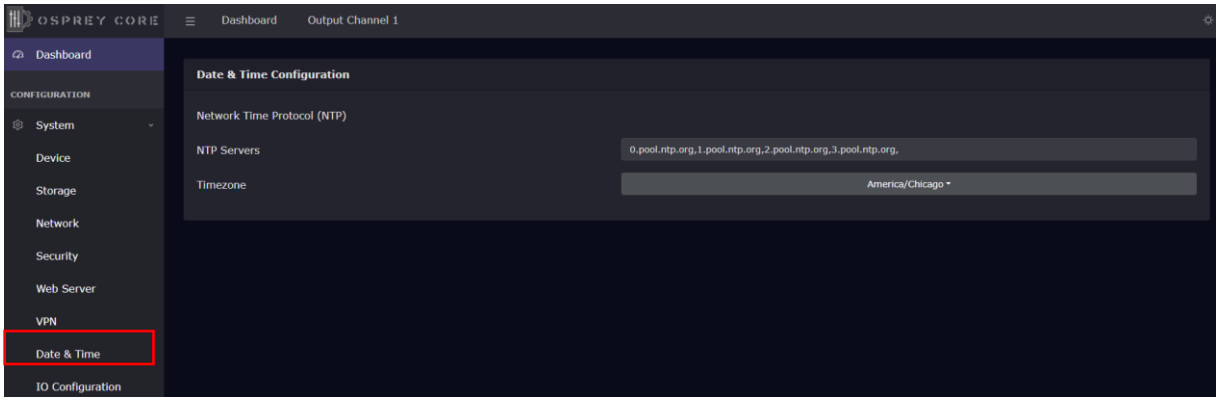


Web Interface – Date and Time

System Settings – Date & Time

NTP Servers preselect time servers, additional time servers can be manually added separated by ‘,’

Timezone your selected time zone



Web Interface – I/O Configuration

System Settings – I/O Configuration

The I/O configuration can be changed while Talon is actively encoding

Status LED Configuration - configure the front panel LED's

Disabled: LED will always remain off

Ethernet Link: Ethernet connected and IP assigned

Channel 1 Status: LED ON -> Talon channel 1 is encoding, LED OFF -> Talon is idle

Channel 2 Status: LED ON -> Talon channel 2 is encoding, LED OFF -> Talon is idle (openGear only)

VPN Connected: LED ON -> VPN is connected

SDI 1 Signal: LED ON -> valid input on SDI port 1, LED OFF -> no input on SDI port

SDI 2 Signal: LED ON -> valid input on SDI port 2, LED OFF -> no input on SDI port (openGear only)

HDMI Signal: LED ON -> valid input on HDMI port, LED OFF -> no input on HDMI port (Desktop only)

LCD Configuration - configure the front panel LCD Screen. Three of below options can be displayed simultaneously.

MAC Address

Device Name

IP Address

Channel Status (encoding started or encoding stopped)

SDI Status (resolution and frame rate of SDI input will display)

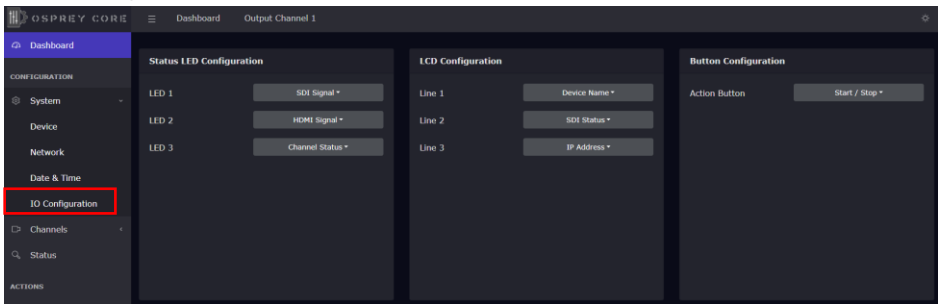
HDMI Status (resolution and frame rate of HDMI input will display)

VPN Status

Firmware Version

Disabled (associated line will be blank)

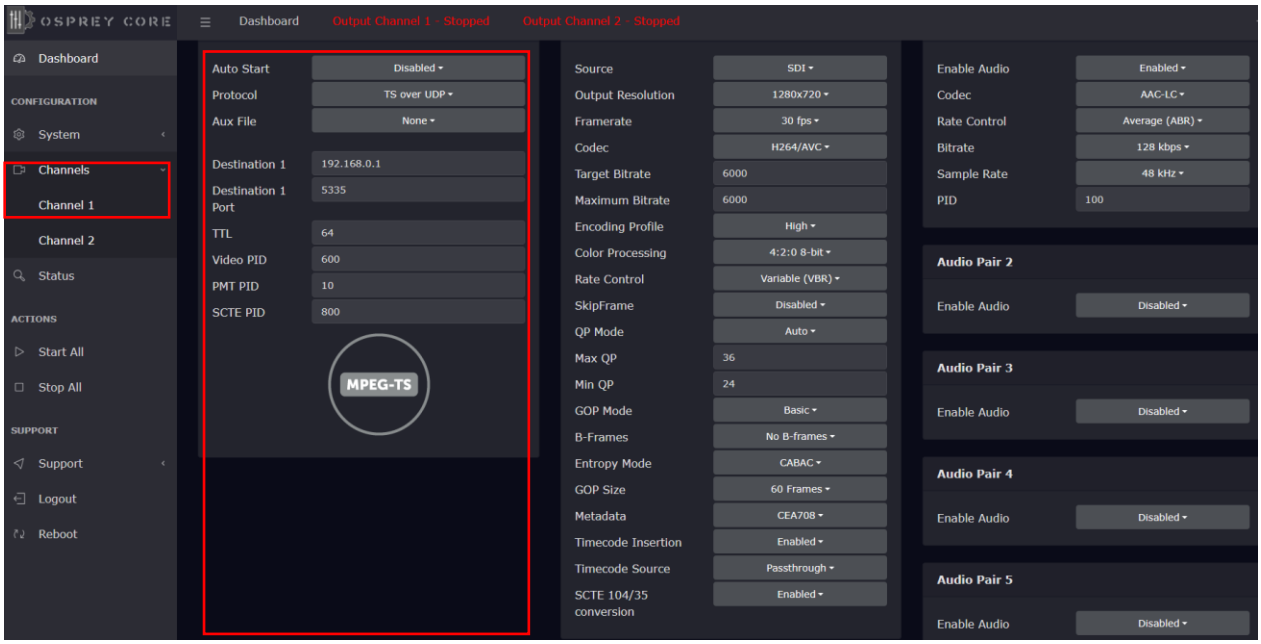
Button Configuration - enable/disable front button start/stop function



Web Interface – Channel Setup Output Protocol

Channel Setup - Output

Important: The selection of the output stream protocol dynamically changes the available options for video and audio encoding. Therefore, the streaming protocol must always be set before proceeding to the video and audio settings.



Output Transport Stream

Auto Start	auto start of Talon at “Power Up”
Protocol	streaming protocols and native integrations - see pages 21 through 24 for setup information
AUX File	archive a copy of your stream in .mp4 – see page 20 for additional information
Device Type	select between saving to USB or Network Share – see page 20 for additional information

Protocol: When sending media over networks, protocol can mean Transport Protocol or Payload Format. For instance, TS over UDP refers to using the MPEG-TS payload format to deliver media via the UDP protocol. Selecting which protocol to use will dictate several other settings within the video and audio encoding sections. Selecting RTMP/RTMPS will limit the “codec” setting to “H.264”. Selecting “TS over RTP” allows the selection of both “H.264” and “HEVC” for codec. Select “Protocol” first when setting up an encoder output and the rest of the Video and Audio settings will conform to your Protocol selection.

Web Interface – Video Archiving

Channel Setup – Video Archiving

Save MP4 (USB3.0 port in the back of Talon, internal NVME for openGear)

- Only FAT and FAT32 formatted USB drives are accepted
- A correctly mounted drive will show in 'Dashboard',
- Unmount USB drive from 'Dashboard'
- Files are never automatically deleted from the drive, if the folder fills up the encode will stop with an error

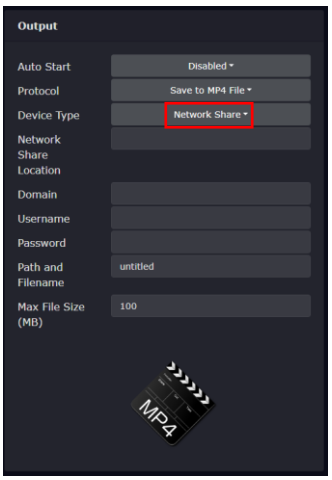
Path and Filename	Path to file location: /folder/filename
Maximum File Size	file size in MB for each video segment

Output file format example:

ch1_filename_20230420-153253_0.mp4

ch{channelnumber}_{user_provided_filename}_{year}{date}-{time}_{indexnumber}.mp4

Save MP4 to Network Share



Network Share Location	Network URI: //ip_address/myshare
Domain	Domain name for authentication to the network share. If you do not have a domain name, use the local computer name you are connecting to.
Username	Account username with permission to access the network
Password	Password to account referenced above
Path and Filename	Path to file location: /folder/filename
Max File Size	file size in MB for each video segment

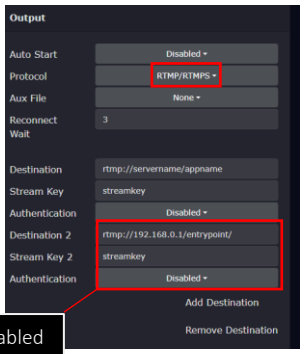
Output file format example:

ch1_filename_20230420-153253_0.mp4

ch{channelnumber}_{user_provided_filename}_{year}{date}-{time}_{indexnumber}.mp4

Web Interface – Transport Protocols RTMP, RTMPS, UDP

Channel Setup – Transport Protocols



With Simulcast enabled on the Device page, up to 3 destinations can be added

RTMP/RTMPS (Real-Time Messaging Protocol)

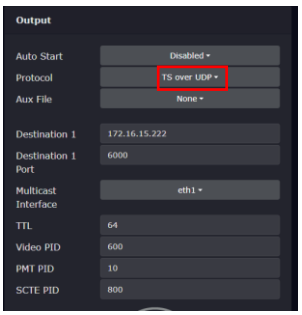
Destination	server address of your endpoint
Streamkey	key assigned by your endpoint
Authentication	enable/disable stream authentication
User	username for authentication
Password	username for authentication

Destination Stream URL Example: rtmp://a.rtmp.youtube.com/live2

RTMP is a legacy protocol developed by Adobe® to transfer audio and video files between a streaming server and the Adobe Flash Player. With the phasing out of Flash, it has shifted its primary use case away from viewer-facing content delivery and toward ingesting live streams through RTMP-enabled encoders.

TS over UDP (User Datagram Protocol)

Destination	IP address of your endpoint
Destination Port	UDP destination port
Multicast Interface	User can select which NIC will act as the Multicast Interface if there are two NICs available.
TTL	Destination time to live. Maximum number of 'hops' that data exists on a network before being discarded (to prevent endless loops)
Video PID	ID for your video transport stream
PMT PID	PMT ID for your transport stream
SCTE PID	SCTE ID for your transport stream



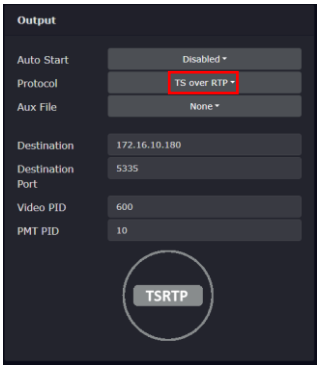
Destination IP Example: 172.16.10.180

Destination Port Example: 7002

UDP is a connectionless protocol with minimal mechanisms. It doesn't require recipients to let the sender know that all data packets have arrived, which can make it unreliable. This protocol is stateless and ideal for transmitting data to large numbers of clients. UDP features multicast support for service discovery and broadcasting. Its low rate of retransmission delays makes it the perfect match for real-time applications

Web Interface – Transport Protocols RTP, SRT

Channel Setup – Transport Protocols

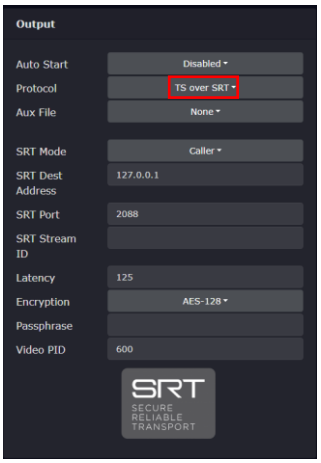


TS over RTP (Real-Time Protocol)

Destination	IP address of your endpoint
Destination Port	IP address of your endpoint
Video PID	ID for your video transport stream
PMT PID	PMT ID for your transport stream

RTP is designed for end-to-end, real-time transfer of streaming media. The protocol provides facilities for jitter compensation and detection of packet loss and out-of-order delivery, which are common especially during UDP transmissions on an IP network.

TS over SRT (Secure Reliable Transport)



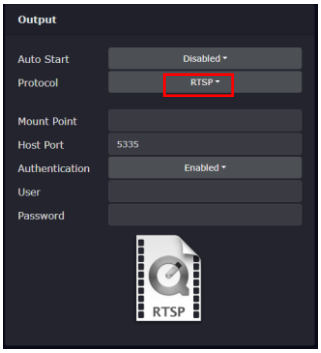
SRT Mode	selection of 'caller' or 'listener' mode
SRT Destination Address	IP address of your endpoint (visible only in caller mode)
SRT Port	port used to listen or transmit, default 2088
SRT Stream ID	stream identification
Latency	maximum accepted latency in ms. Should be set to >= 2.5 times round trip time (RTT), default 125
Encryption	enable/disable 128-bit encryption
Passphrase	encrypted transmission, 16-character alpha-numeric
Video PID	Video PID for transport stream

SRT Mode **'Listener'**: The "agent" waits to be contacted by any peer caller. Note that a listener can accept multiple callers, but Talon does not support this ability; after the first connection, it no longer accepts new connections.
SRT Mode '**Caller**': The "agent" (this application) sends the connection request to the peer, which must be listener, and this way it initiates the connection.

SRT is known for its security, reliability, compatibility, and low-latency streaming it is the preferred protocol for members of the SRT Alliance. This protocol does not rely on a single codec, which allows developers to pair it with any audio and video codecs they desire.

Web Interface – Transport Protocols RTSP, WebRTC

Channel Setup – Transport Protocols



RTSP (Real-Time Streaming Protocol)

Mount Point	mount point port
Host Port	host destination port
Authentication	enable/disable stream authentication
User	username for authentication
Password	username for authentication

RTSP is a legacy protocol, it cannot transmit live streaming data alone and require RTSP servers to work together with RTP and other protocols to accomplish their streaming tasks. It can deliver low-latency streaming to a select group of small audiences from a dedicated server.

WebRTC

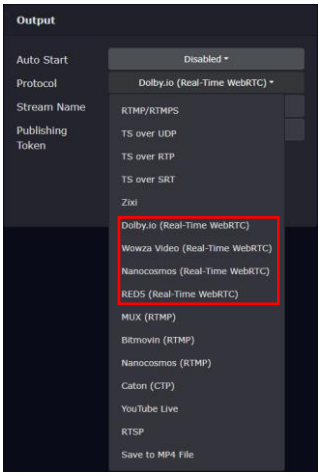
Due to the open-source nature of webRTC, this is only available though custom integrations currently supporting:

Dolby.io

nanocosmos

RED5 PRO®

WOWZA

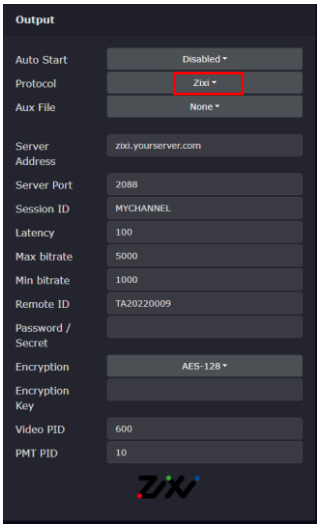


WebRTC is an open-source project that delivers video streams to viewers with real-time latency. Initially developed for text-based chat apps and VoIP usage.. The WebRTC protocol is a low-latency streaming solution using WHIP.

Web Interface - Zixi

Channel Setup – ZIXI

While not a protocol, Zixi defines itself as a "software-Defined video Platform" (SDVP). Talon's implementation was built upon the Zixi SDK and serves as a Zixi Feeder. It can deliver to a Zixi Broadcaster, which can deliver to a decoder. The Talon cannot deliver Zixi directly to another decoder.



Server Address IP address of the stream destination

Server Port port of the stream destination. The default is 2088

Session ID unique name of the stream. This name can be created by the user or assigned by the Zixi Broadcaster.

Latency the latency setting or "smoothing" as it is sometimes referred to in Zixi, enables transmission of the output at the correct rate. Required when the receiving device is sensitive and can't lock onto the stream. Default setting is 100ms. The available range is between 100 and 1000ms.

Max Bitrate specify the maximum expected bitrate for memory allocation. Recommended: For CBR start with 10% higher than the stream bitrate. For VBR use 2X the actual bitrate, which will prevent buffer overruns (especially with VBR streams). Default: 5000. Note – Overflows will typically occur when the Max Bitrate isn't sufficient.

Min Bitrate currently, min bitrate is not configured.

Remote ID the name that identifies the Feeder to the Broadcaster. Default is the serial number of the encoder. Do not change unless Broadcaster configuration requires it.

Password/Secret this is the "Zixi Secret". By default, any publish point in Broadcaster can be accessed by any encoder. Zixi Broadcaster can provide a Feeder with a password which gives that encoder priority over any other encoder connected to that publish point. If an encoder with the password attempts to connect, the publish point will remove any other encoder connected to it and replace it with the password protected version.

Encryption enable/disable AES-128, AES-192 or AES-256 stream encryption

Encryption Key cut and paste the encryption key provided by your Zixi Broadcaster in the allotted space.

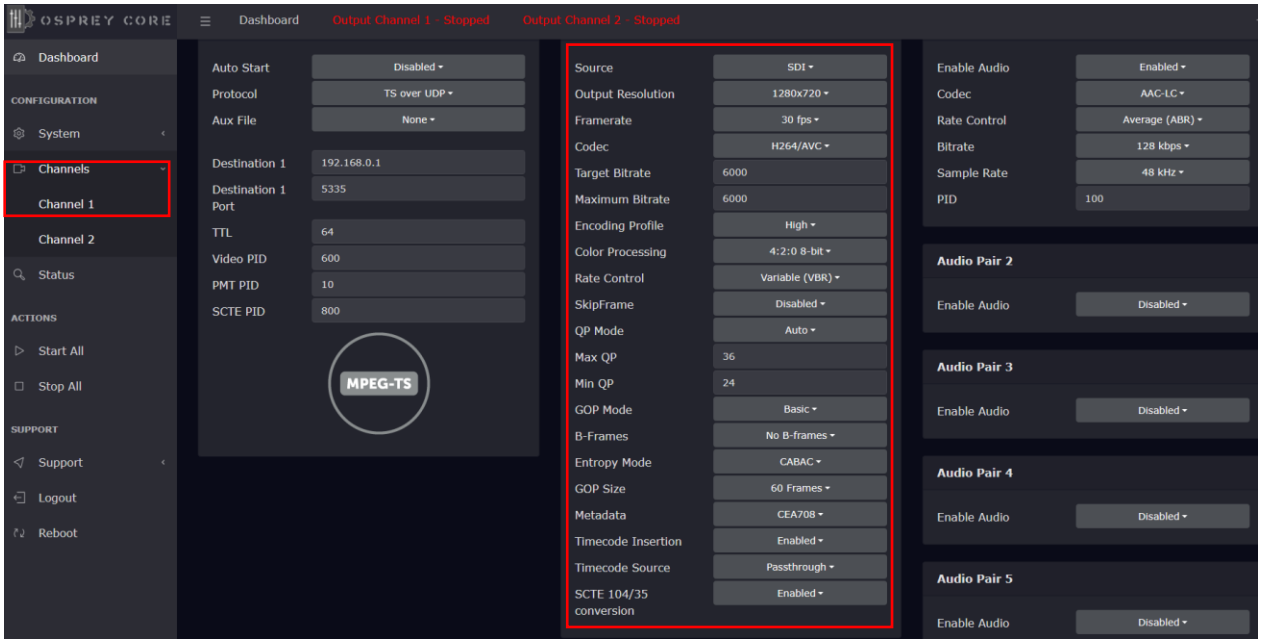
Video PID the Default PID is 600. Any ID greater than 0 but less than 8192 may be used.

PMT PID the default PMT PID is 10. Other values can be used where specified by the transport stream.

Web Interface – Video Encoding Settings

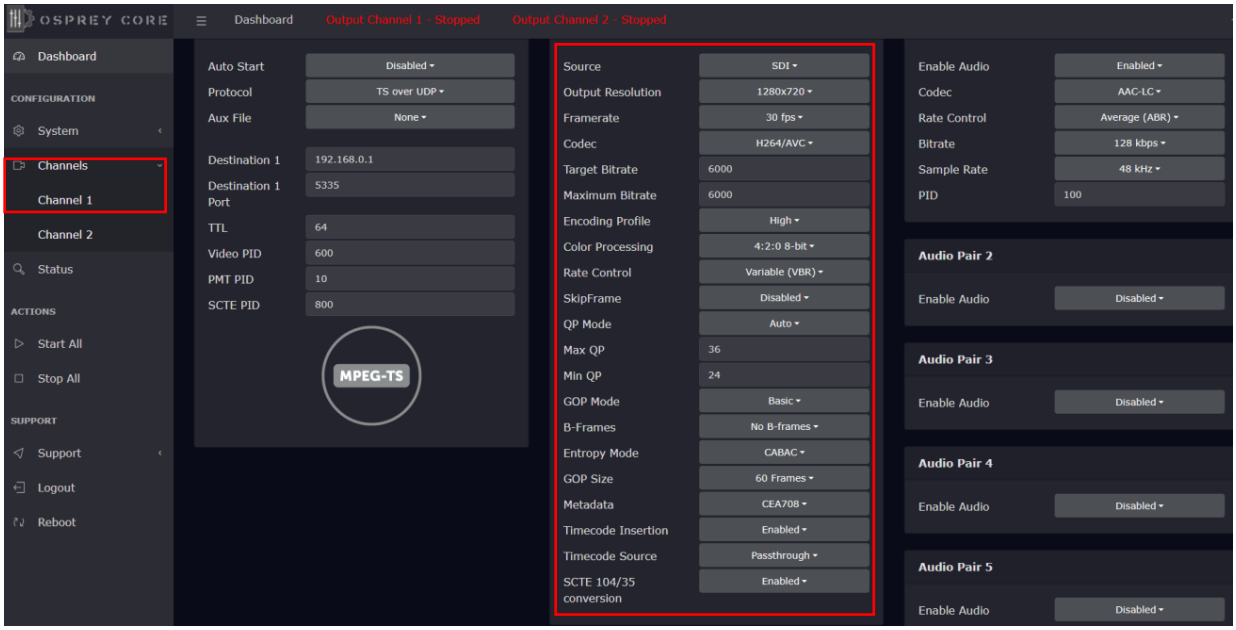
Channel Setup - Video

Important: The selection of the output stream protocol dynamically changes the available options for video and audio encoding. The options outlined in this chapter are based on UDP and might slightly differ from your settings.



Source	select your input video source
Output Resolution	for best quality and lowest latency it is recommended to match your input and output resolutions
Framerate	for best quality and lowest latency it is recommended to match your input and output framerate
Codec	select between HEVC (H.265) and AVC (H.264). Note that not all streaming protocols support HEVC.
Target Bitrate	Target Bitrate is set based on the rate control method used. For CBR, the Target Bitrate equals the bitrate to maintain throughout the encode. For VBR, it is the rate you want to average.
Maximum Bitrate	maximum Bitrate is only enabled when VBR is selected. Maximum bitrate to be >= 'Target Bitrate'
Encoding Profile	different profiles are available depending on the codec: HEVC - Main, Main 10, Main 4:2:2 10 AVC - Baseline, Main, High, High-10, High 4:2:2
Color Processing	for best quality and lowest latency it is recommended to match your input and output color space. The options change depending on the selected codec and encoding profile.

Web Interface – Video Encoding Settings



Rate Control select between CBR, VBR, QP and Low Latency. Constant QP means that the bitrate can vary greatly to achieve the set QP. This can result in wild fluctuations of bitrate and is not recommended for live streaming.

Enable SkipFrame Encoder will drop frames in order to not exceed the selected Maximum Bitrate

Deinterlacing select the deinterlacing mode to encode progressive of an interlaced video input signal.

QP Mode 'Auto' or 'Uniform', default is 'Auto'

Max QP Default '36', a higher number results in a lower bitrate and lower quality (delta between max QP and min QP should always be <12). Maximum is 51.

Min QP Default '24', a higher number results in a lower bitrate and lower quality (delta between max QP and min QP should always be <12).

GOP Mode Low Delay P/Low Delay B/Basic (IPPP)/Basic-B/Adaptive.
Choose '**Low Delay P**' if you are unfamiliar with GOP settings.

B-Frames Number of B-frames between I-frames. 0 – 4. This feature is only available for certain GOP modes.

GOP Size 5 – 240 frames, choose twice your encoding framerate as default

Metadata OFF, CEA708, SMPTE-2038

Timecode Insertion Enabled/Disabled

Timecode Source Passthrough, System Time (UTC)

SCTE 104/35 Enabled/Disabled. Supports embedding the SCTE 104 messages from the SDI source into the output stream as SCTE35.

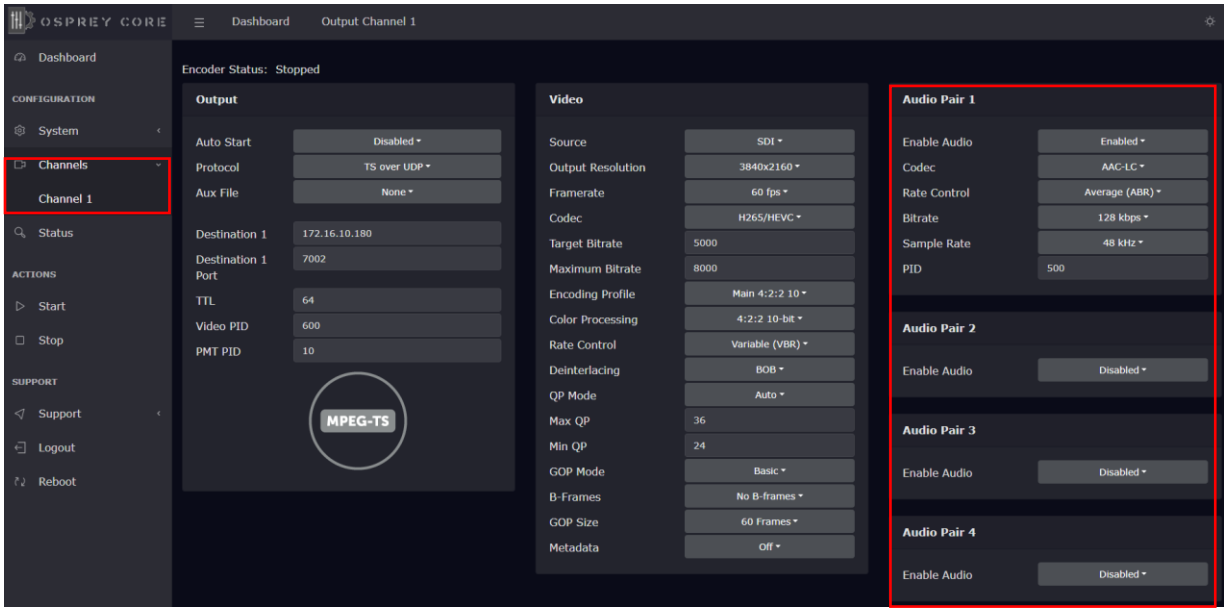
QP: The Quantization Parameter controls the amount of compression for every macroblock in a frame. Large values mean that there will be higher quantization, more compression, and lower quality. QP ranges from 0 to 51.

GOP: GOP parameters define the basic pattern of the video stream in terms of how the encoder uses I-, P-, and B- frames.

B-Frame: A compressed video frame which is reconstructed based on its differences from the previous and the subsequent frame

Web Interface – Audio Encoding Settings

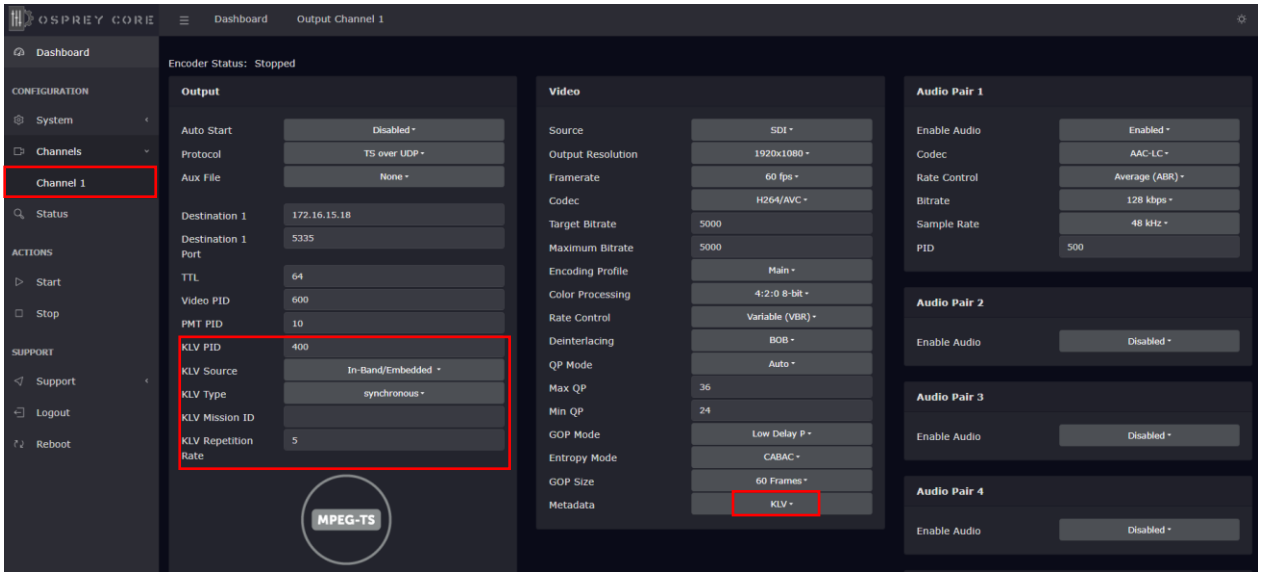
Talon supports up to 16 embedded Audio Channels of SDI (8 Stereo Pairs) or 8 Audio Channels of HDMI (4 Stereo Pairs)



Enable Audio	enable/disable select audio channels. If encoding video only it is recommended to disable all audio
Codec	choose between AAC-LC and Opus
Rate Control	choose between Average Bitrate (ABR) and Variable Bitrate (VBR)
Bitrate	range 12kbps to 196kbps. For best encoding results match your input rate, if unknown 128kbps is recommended
Sample Rate	44.1kHz or 48kHz, 48kHz is recommended
PID	Audio Stream ID

Web Interface – Channel Setup - KLV

SDI in-band KLV Metadata (Key-Length-Value) is enabled under Channel - Video – Metadata.



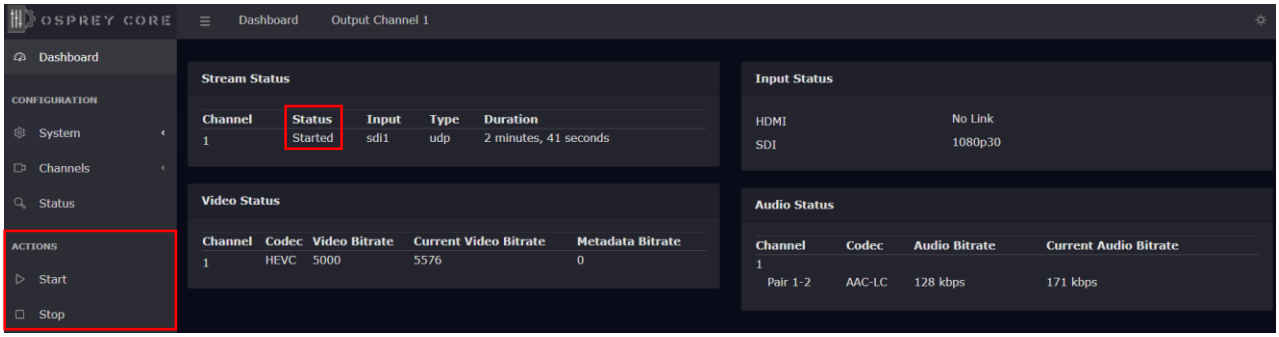
Web Interface – Status and Stream Start/Stop

The Stream 'Start' and 'Stop' buttons are always available in the main menu. It is recommended to start and stop your streams from the 'Status' page or from the 'Dashboard'. This allows for immediate monitoring of your stream data.

The status page provides information about your video inputs and live stream data

- Audio, Video and Metadata Bitrates
- Video Input resolutions and frame rates

Status Page



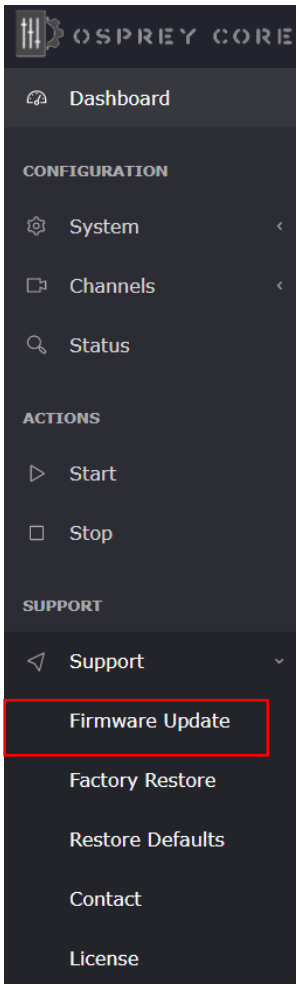
Dashboard

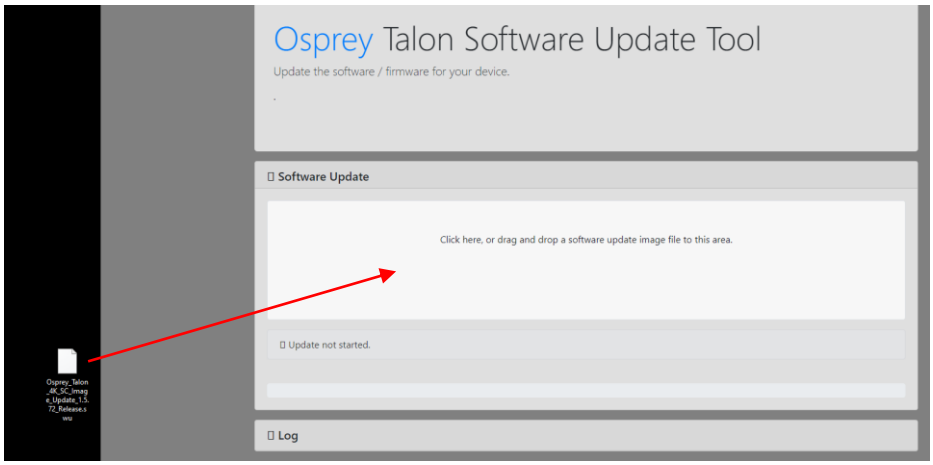
Web Interface – Firmware Update

As we constantly add features and maintain our Talon line of products, we suggest you keep your Encoder Firmware up to date.

Firmware upgrade steps:

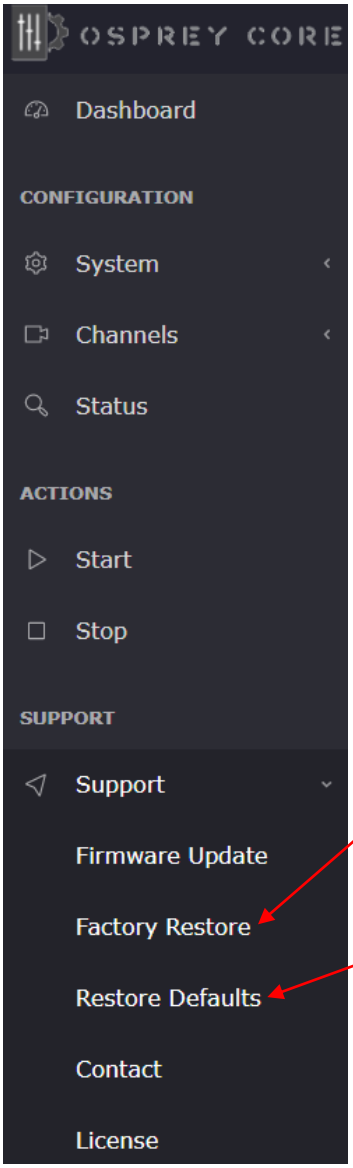
1. Download the latest firmware revision at www.ospreyvideo.com/talon-software-and-firmware
2. Go to 'Firmware Updates' on Talon Web Interface
3. Drop the downloaded firmware file into the 'Software Update Tool'
4. Update will start immediately and might take several minutes





Web Interface – Restore

Please read carefully before attempting to restore Talon's firmware and settings



Factory Restore will reset Talon and restore it with the original firmware it shipped with. Settings will be reset to default

Restore Defaults will reset all user settings with its default values

Page intentionally left blank

Page intentionally left blank

Enterprise and Security

To protect the Talon OS and to ensure data integrity, multiple security features are included by default. These require no user intervention and are active upon the first startup.

NDAA compliant
Talon 4K series encoders are manufactured in the USA from globally sourced components. All parts are vetted to ensure NDAA compliance.

Operating system firmware
All OS firmware is AES encrypted and RSA authenticated. No part of the operating system can be modified except by Osprey.

Trusted image/update control
The initial firmware, as well as all updates are encrypted, digitally signed and only available from Osprey. This ensures that only approved software can be loaded. Any attempt to load outside software will fail.

Certificate encrypted SSH
All SSH access is keyed and encrypted. Only Osprey can access the device via SSH.

Telnet access blocked (no telnet client installed)
To comply with most secure networks, Telnet access is not enabled. There is no Telnet client on the Talon. Because of the Trusted Image, none can be installed.

OpensSource Listing

Package	Version	Description	License
Linux Kernel	5.15.19		GPLv2
bash	51.8	Bourne Again Shell	GPLv3+
busybox	1.34.1	Lightweight common UNIX utilities	GPLv2 & bzipi2
alsa-conf	1.2.5.1	Advanced Linux Sound Architecture utilities	GPLv2+
alsa-utils	1.2.5.1	Advanced Linux Sound Architecture utilities	GPLv2+
apache2	2.4.52	Opensource web server	Apache-2.0
passwd	3.5.29	System user password management	GPLv2+
cronie	1.5.7	scheduled process management	GPLv2+
curl	7.78.0	Tool for transferring data using various network protocols	MIT
daemontools	0.76	supervisor and monitor services	PD
dhcpd	9.4.0	DHCP client	BSD
e2fsprogs	1.45.3	EXT2/3/4 filesystem utilities	GPLv2
ethtool	5.13	query and control network device drivers	GPLv2+
faad2	2.8.8	Freeware Advanced Audio (AAC) decoder	GPLv2
faac	1.30	AAC audio support	LGPLv2+
gst-interpipes	1.1.8	Tools for monitoring gstreamer	LGPL2.1
gst-perf	1	Tools for monitoring gstreamer	LGPLv2+
gst-shark	0.7.2	Tools for monitoring gstreamer	GPLv2+
gstreamer1.0		Multimedia Pipeline control	LGPLv2+
gstreamer1.0-plugins-bad	1.18.0	Multimedia Pipeline control	GPLv2+
gstreamer1.0-plugins-good	1.18.0	Multimedia Pipeline control	GPLv2+
gstreamer1.0-plugins-base	1.18.0	Multimedia Pipeline control	GPLv2+
i2c-tools	4.3	Accessing i2c devices	GPLv2+
init-ifupdown	1.0	Tools to bring network configuration	MIT
initscripts	1.0	Scripts for run level processing	GPLv2
iproute2	5.15.0	Linux TCP/IP traffic control	GPLv2+
iptables	1.8.7	Linux TCP/IP firewall	GPLv2+
libcrypto	1.1.1l	Crypto library	Openssl+

Safety and Compliance

FCC Notice

The Osprey Talon has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this device does cause harmful interference to radio or television reception, the user is encouraged to try to correct the interference by one or more of the following measures:

•Reorient or relocate the receiving antenna.
•Increase the separation between the equipment and receiver.
•Connect the computer into an outlet on a circuit different from that to which the receiver is connected.
•Consult the dealer or an experienced radio/TV technician for help.

If the above measures are unsuccessful, please consult the dealer or manufacturer of your radio or television receiver or speak with an experienced Radio/TV technician.

Shielded Cables: Connections between this device and peripherals must be made using shielded cables in order to maintain compliance with FCC radio emission limits.

Modifications: Modifications to this device not approved by Osprey Video could void the authority granted to the user by the FCC to operate the device.

Product Disposal Information

Dispose of this product in accordance with local and national disposal regulations (if any), including those governing the recovery and recycling of waste electrical and electronic equipment (WEEE).

RoHS Compliant: Osprey Video is committed to compliance with the European directive on the Restriction of the Use of Certain Hazardous Substances in Electrical and Electronic Equipment, Directive 2002/95/EC, the RoHS directive.

Osprey Video
400 Gerault Rd
Flower Mound, TX 75028
United States of America