Installation and Operation Guide V1.2
Firmware 1.5.8X

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

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

HARDWARE Decoder
4K60 10-bit
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

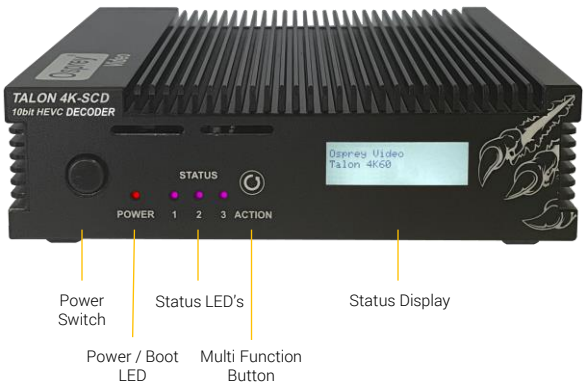
Contents

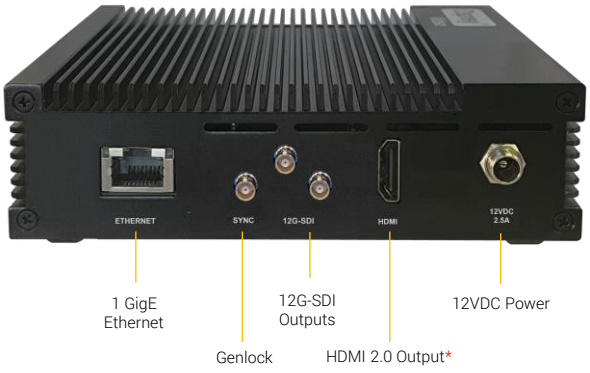
Introduction
- Hardware Features Talon Dektop 3
- Hardware Features Talon openGear 4
- Ross openGear Dashboard 5
- Network Configuration 6
- Block Diagram 7

Web Interface
- **Overview** 8
- **Dashboard** 8
- **System**
  - Device Settings 9
  - 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**
  - Input Protocol 19
  - Input Video Information 20
- **Status Page** 21
- **Actions**
  - Start / Stop 21
- **Support**
  - Firmware Updates 22
  - Factory Restore 23
  - Factory Defaults 23

General Information
- Enterprise and Security 24
- Opensource Listing 25
- Safety and Compliance 26

Hardware Features 4K-SCD and UHD-SCD





- 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
- 1 GigE Ethernet — One Gigabit Ethernet RJ45 connection
- 12G-SDI Outputs — Parallel SDI Outputs
- Genlock — Blackburst or TriSync (4K-SCD only)
- HDMI 2.0 Output — Non-HDCP compliant HDMI 2.0 output * enabled with a future firmware release (4K-SCD only)
- 12VDC Power — Locking 12V Power Input

In the box

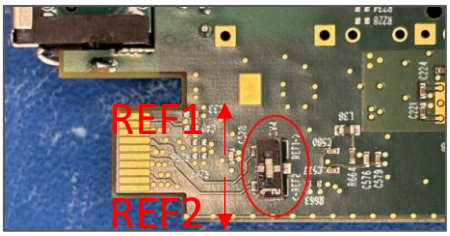
- Talon Decoder
- Locking 12VDC / 36W Power Supply
- Mounting Brackets

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

- 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 Outputs — 3G-SDI on OG-3G-2D (Gold), 6G/12G-SDI on OG-12G-2D (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, Genlock (REF)

Genlock Selection:

There is a physical slide switch on the back side close to the midplane connector that lets the user select between Frame Reference #1 and #2.



Decoding Limitations OG-12G-2D:

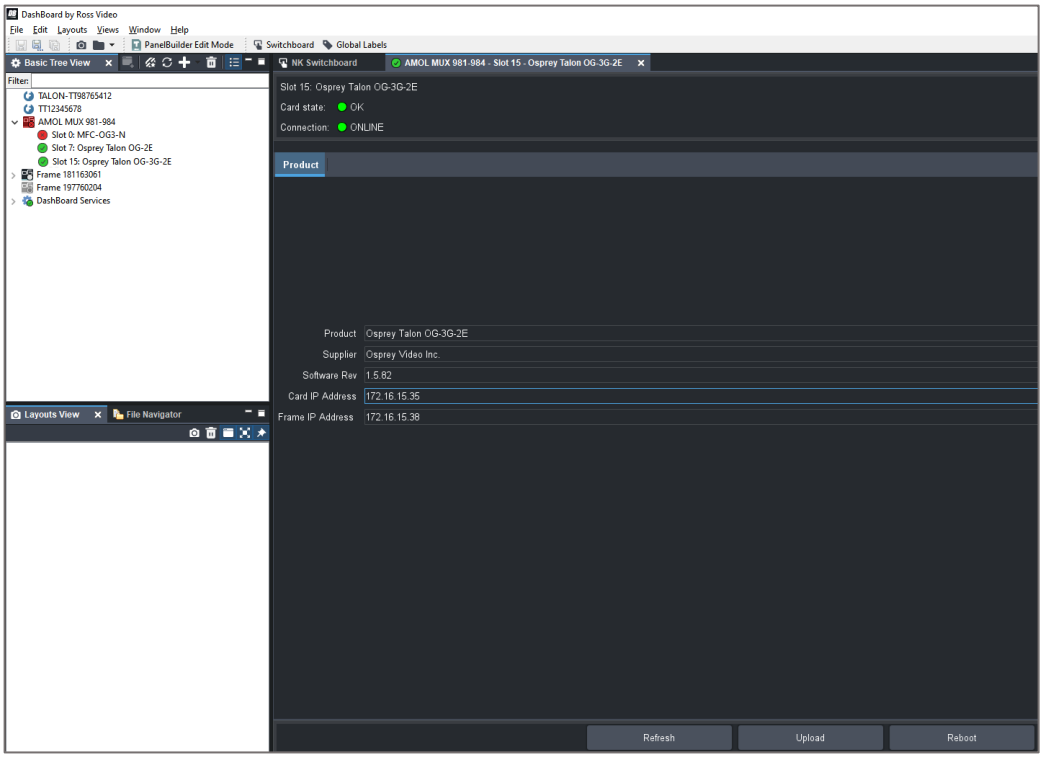
1x decode up to 10-bit **4K60** (single channel decoding to **12G-SDI on output #1**, output #2 not used)
or 2x decode up to 10-bit **4K30** (dual channel decoding to 6G-SDI)

In the box

- Talon Decoder
- Rear I/O Bracket

Ross openGear Dashboard

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



Copy and paste the Decoder 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 Decoder

“Refresh” will refresh the dashboard

“Upload” – not used

Network Configuration

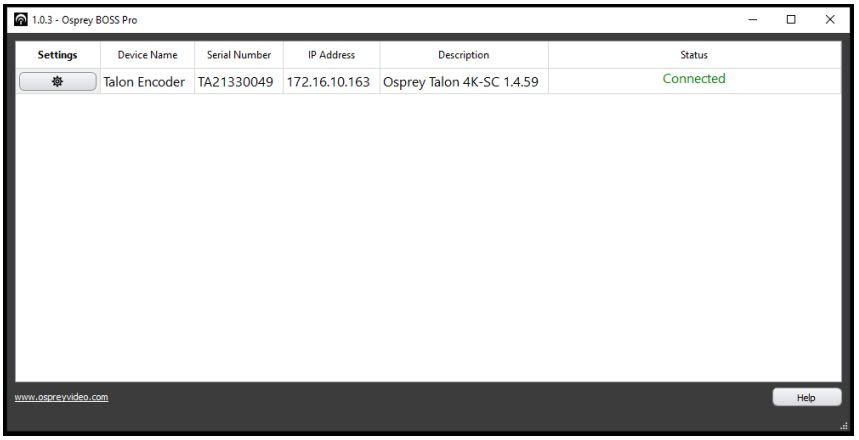
Important! Talon Decoders ship from the factory in DHCP mode. Please ensure your host PC and Talon are connected to the same network supporting DHCP.

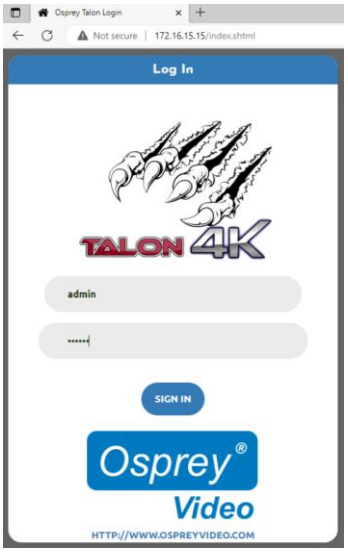
1. Connect Talon to your network using a CAT5 or faster Ethernet cable
2. Connect Talon to power using the supplied 12V adapter. Ensure the barrel connector is fully engaged and locked
3. Power up Talon with the front power switch
    - Red "Power" LED will turn blue once the booting process is complete
    - 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.

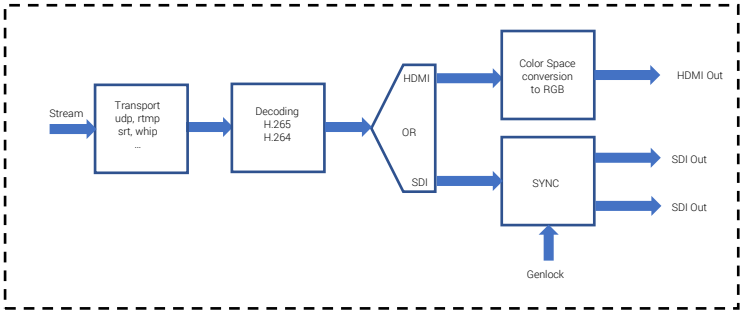
APIPA - Automatic Private IP Addressing (APIPA) is a feature of Windows-based OS -- included since Windows 98 and Windows ME -- that enables a Dynamic Host Configuration Protocol client to automatically assign an IP address to itself when there's no DHCP server available to perform that function.



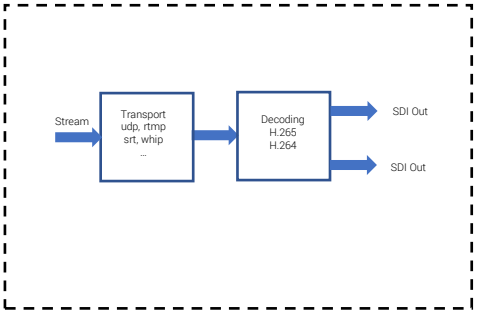


Block Diagrams

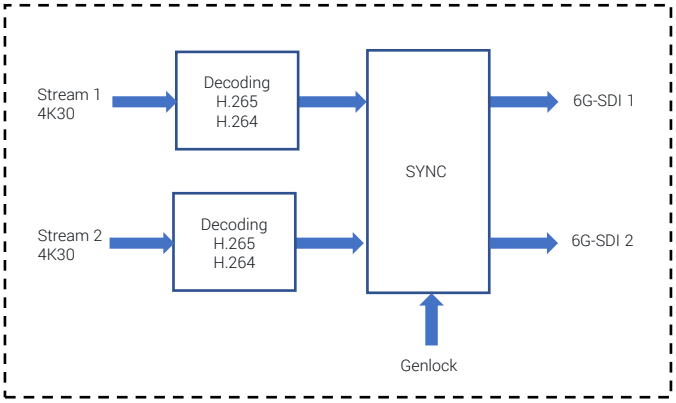
Talon Desktop 4K-SCD

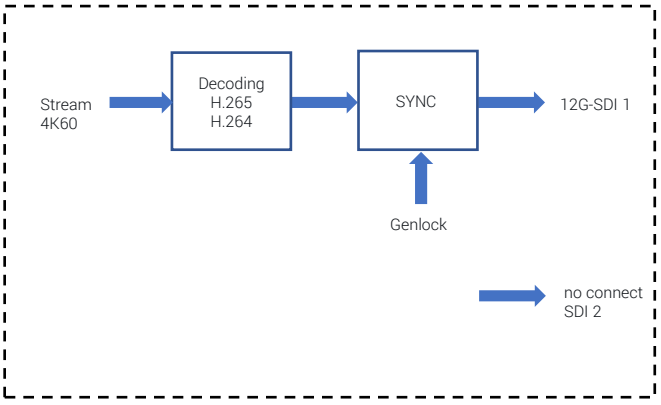


Talon UHD-SCD

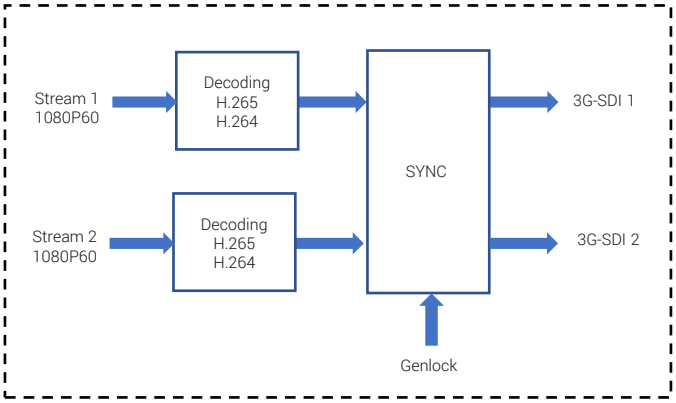


Talon openGear OG-12G-2D





Talon openGear OG-3G-2D



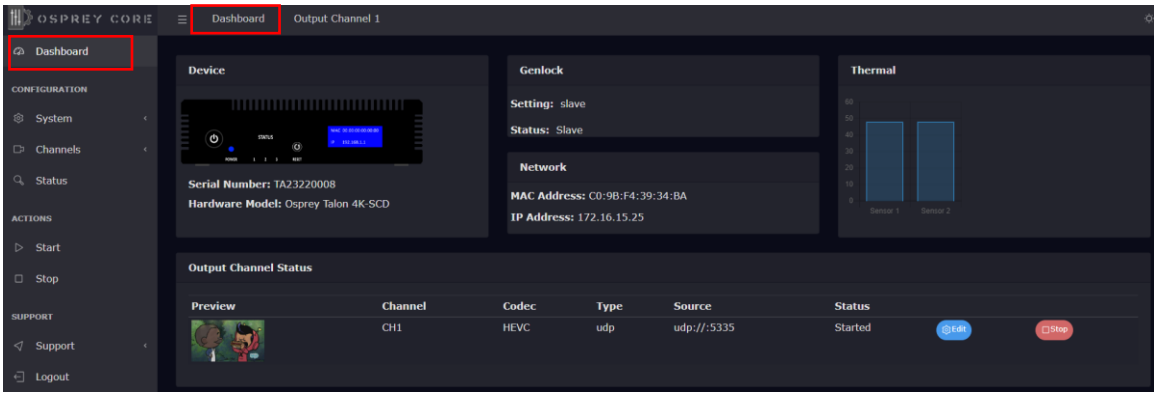
Web Interface - Dashboard

Overview

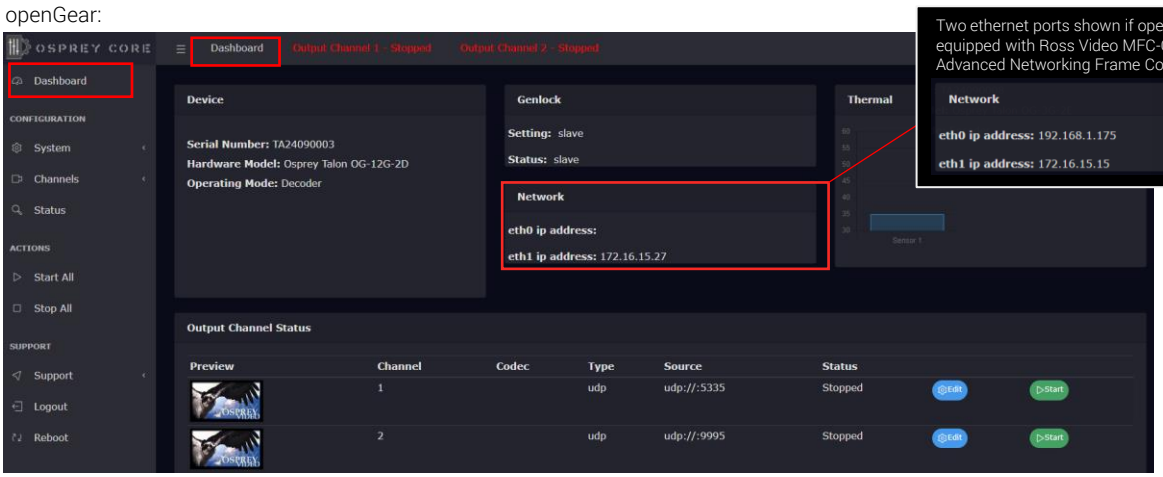
A web server in Talon allows for system control and stream settings via web browser. All commonly used Windows, Mac and Linux web browsers are supported. Please ensure your device is connected to the same network as Talon (see Page 5 for further instructions). To connect to the interface simply enter 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.

Desktop:



openGear:



Genlock

Setting: Displays your Genlock mode selection from the "System – Device" page
Status: **freerun -** no genlock source connected or genlock source mode not matching input frame rate
Status: **slave -** valid genlock source connected
-> Refer to Page 4 for Frame Reference Input Selection

* Preview will start once a Decoder is started

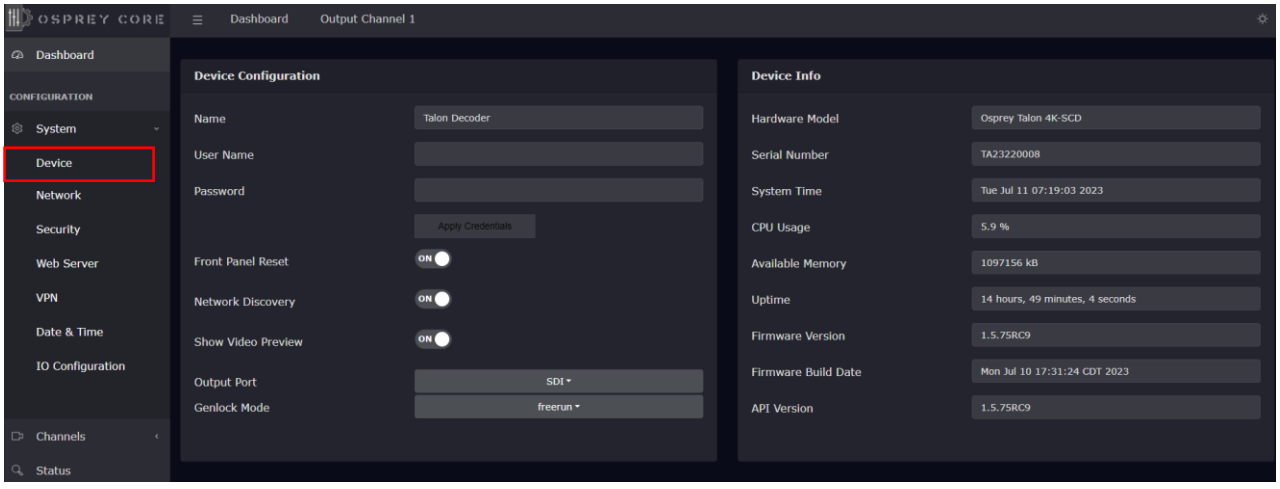
Web Interface - Device

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
Show Video Preview	disable “Dashboard Video Preview” to improve UI responsiveness and CPU usage
Output Port	SDI or HDMI for 4K-SCD, SDI only for UHD-SCD
Genlock Mode	Freerun (no genlock) or slave (Blackburst or Trisysnc)

System Settings - Device Info

Generic system and firmware overview

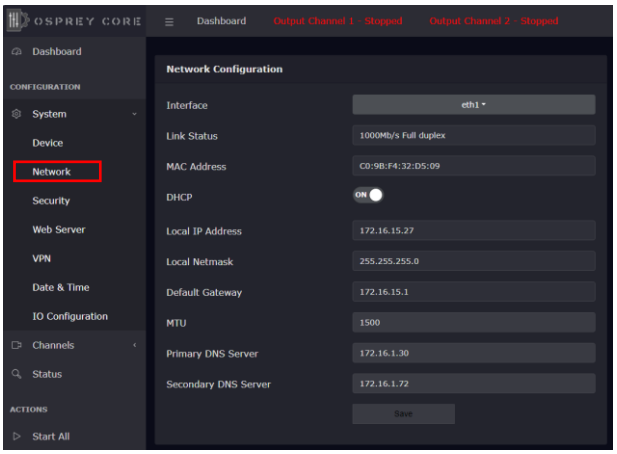


Page intentionally left blank

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
DNS Server	dynamic if DHCP is on. Otherwise, a new valid DNS can be entered here



Important Dual NIC information for openGear

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".

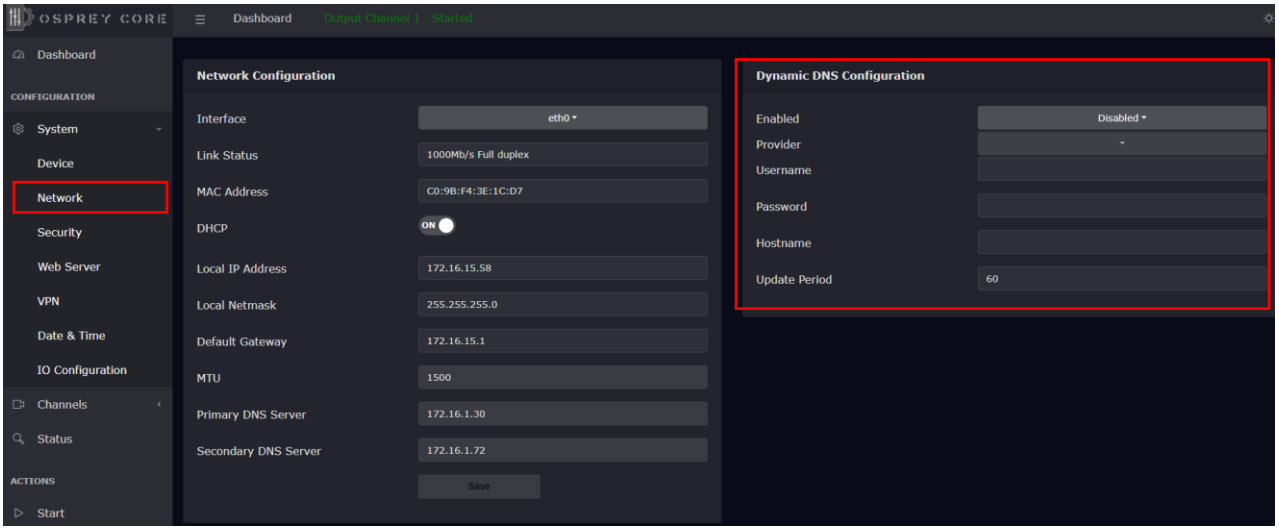
When the two NICs are on separate networks, only one (usually eth0) should be configured as DHCP. The second NIC should be configured as Static. The Default Gateway should only be configured for the network handling the outbound stream. In that case, the second network should be configured without a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

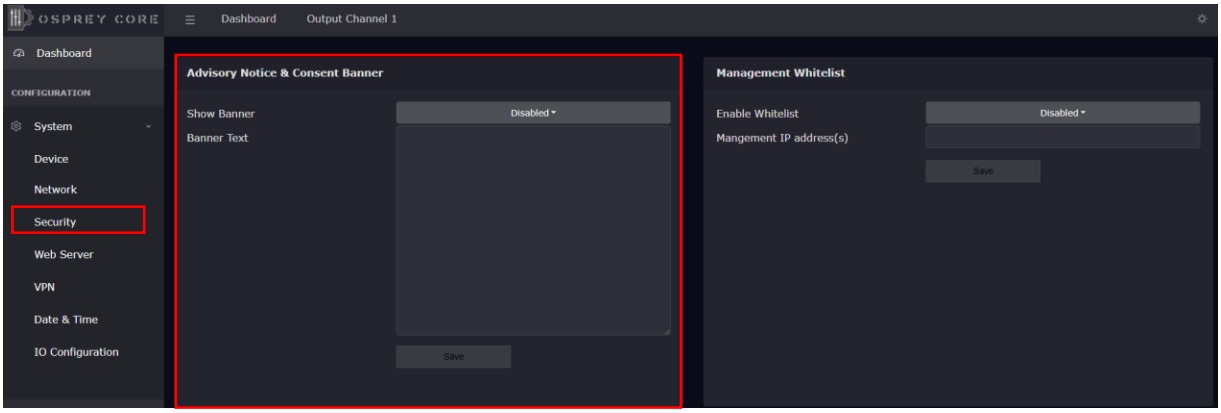
Dynamic DNS configuration



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

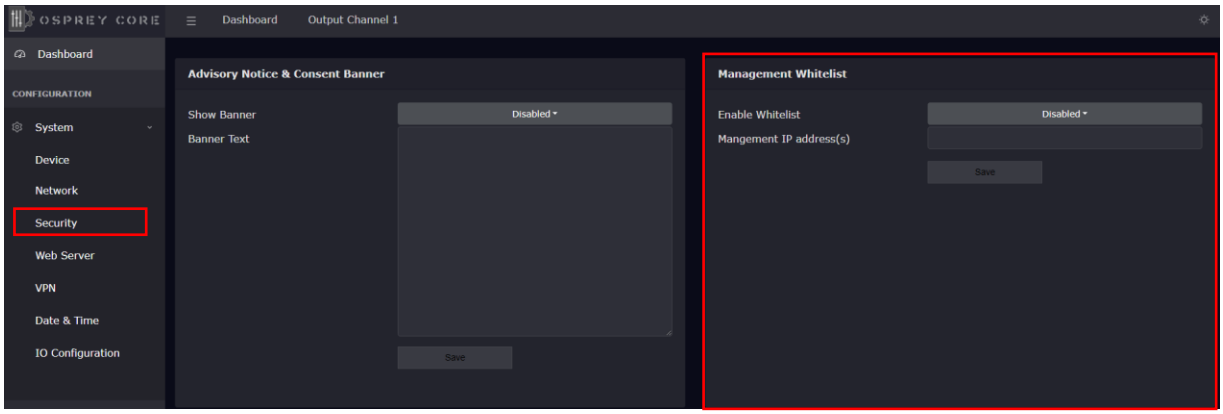


Web Interface –Whitelist and Firewall

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.

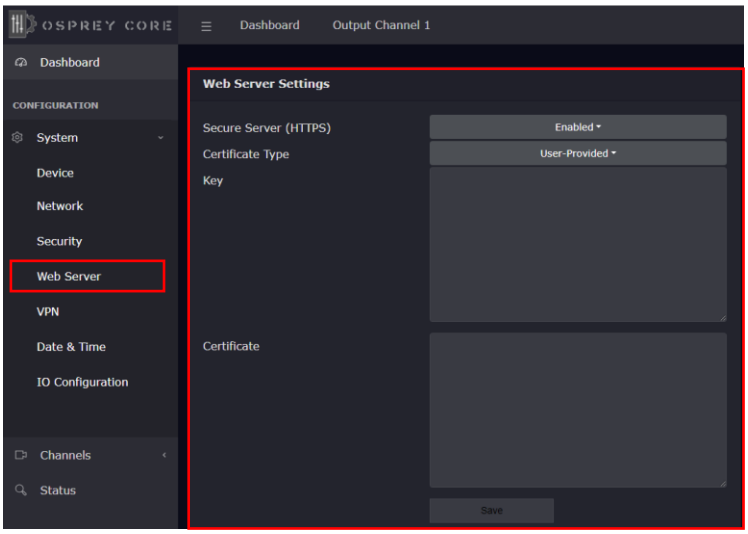
When you change the URL, if you have selected "Self-Signed" for the certificate your browser may warn you that the site is not secure.

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

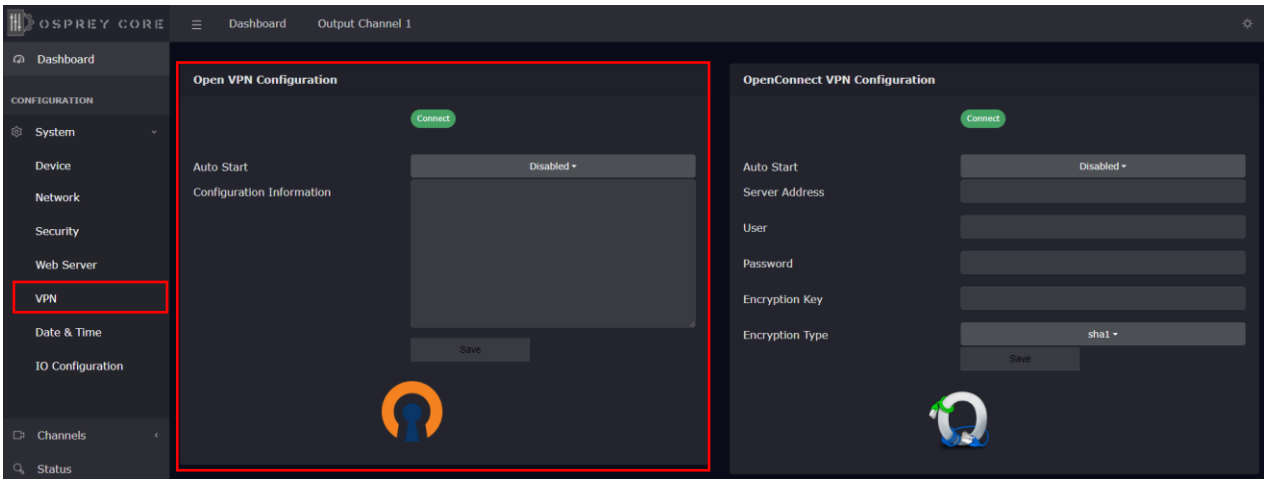
Routers that support OpenVPN generally have a utility to configure the VPN client and download a .ovpn file. To configure the Talon, simply open the .ovpn file in a txt editor and paste the contents into the "Configuration Information" pane.

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.

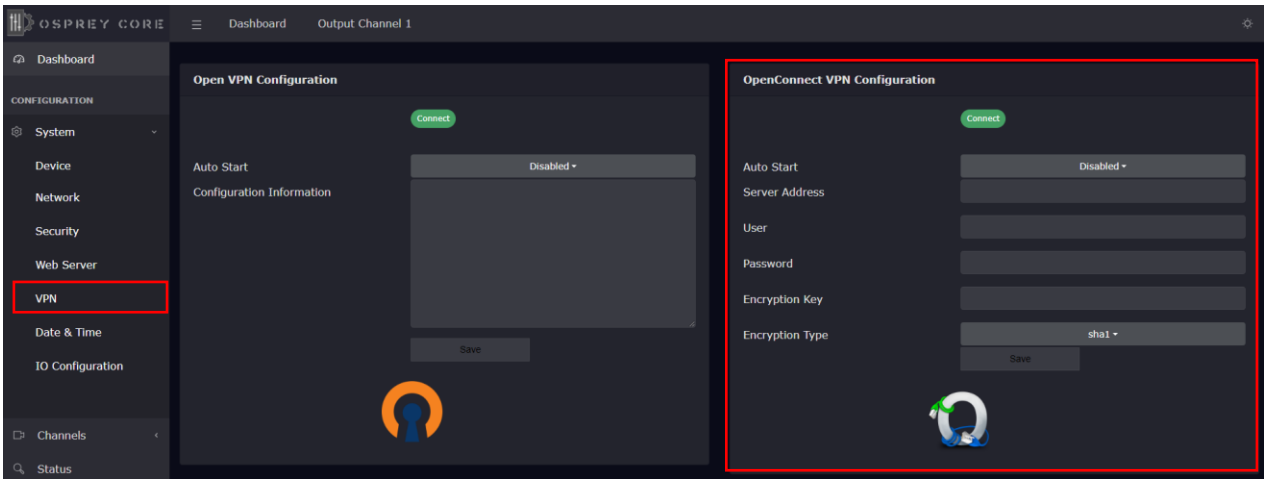


Web Interface –OpenConnect VPN

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.

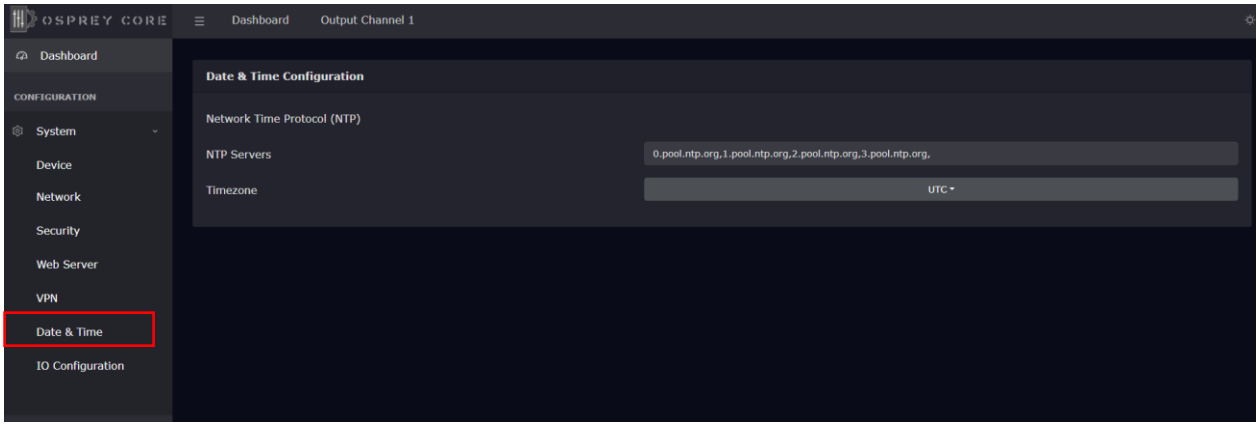


Web Interface – Date and Time

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 decoding

Status LED Configuration - configure the front panel LED's

Disabled: LED will always remain off

Channel Status: LED ON -> Talon is decoding, LED OFF -> Talon is idle

VPN Status: LED ON -> VPN is connected

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

MAC Address

Device Name

IP Address

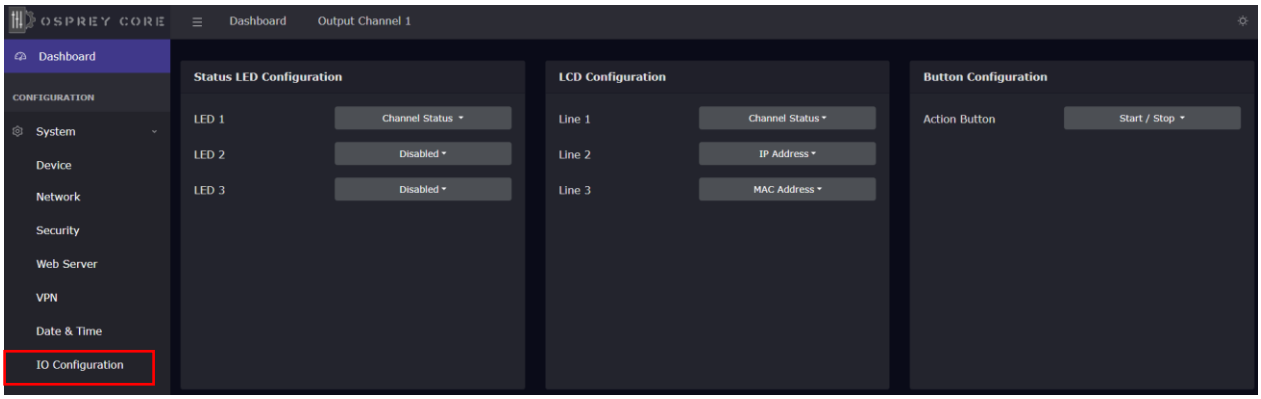
Channel Status (decoding started or decoding stopped)

VPN Status

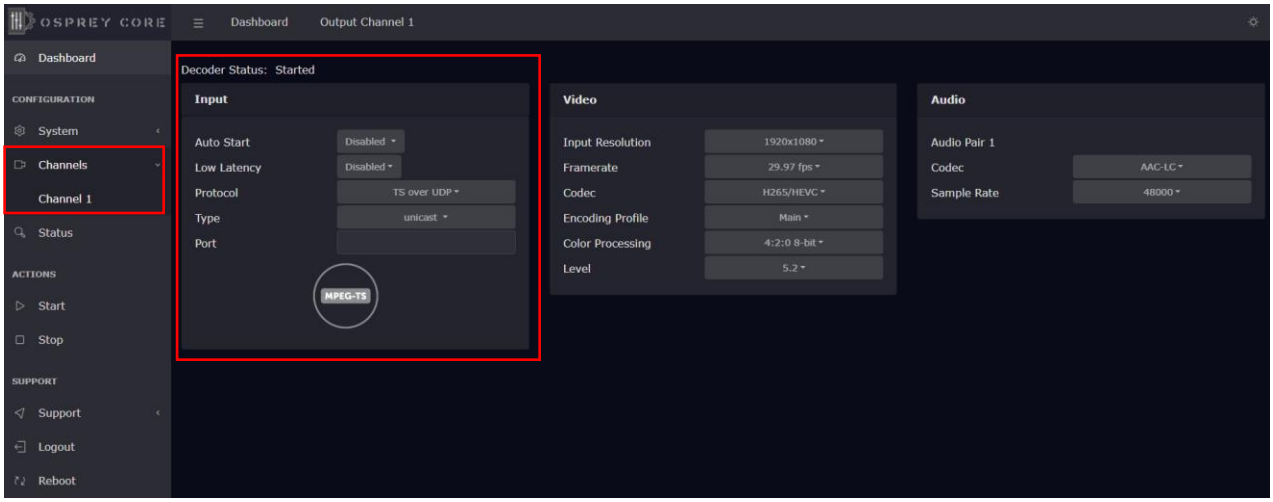
Firmware Version

Disabled (associated line will be blank)

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



Web Interface – Channel Setup Input

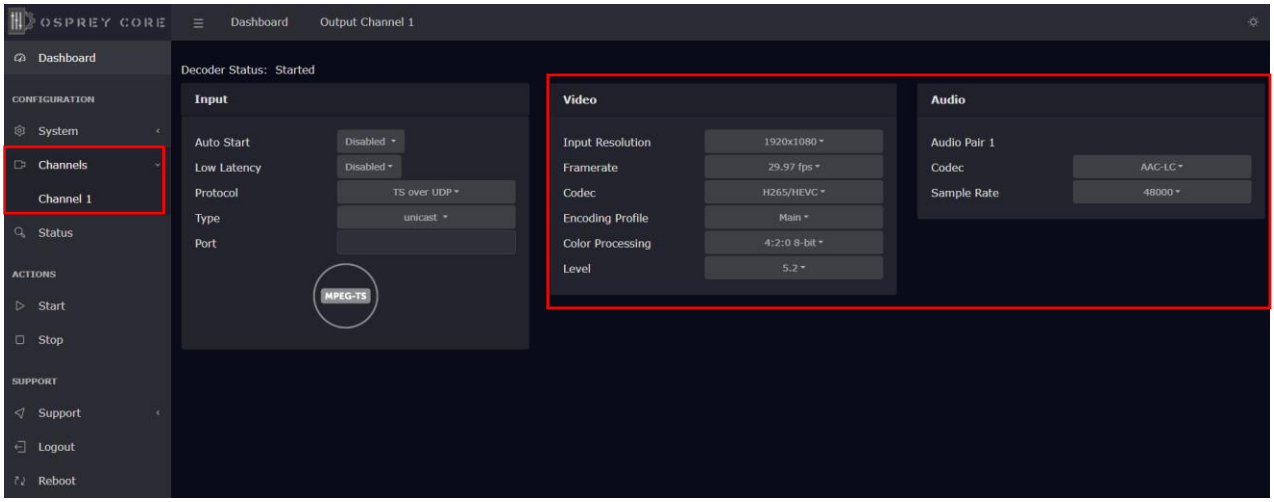


Input Transport Stream

Auto Start	auto start of Talon at “Power Up”
Low Latency	disabled by default, only change for Talon Point to Point workflows
Protocol	supported streaming protocols
Type	unicast or multicast
Port	port number

Web Interface – Channel Input Information

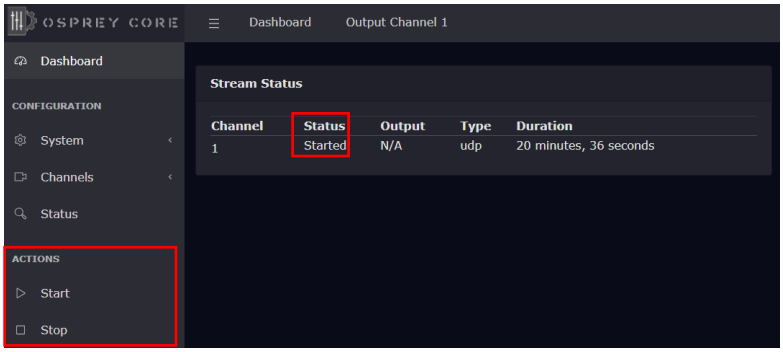
Input Video and Audio information. This information is only available after a decode has started.



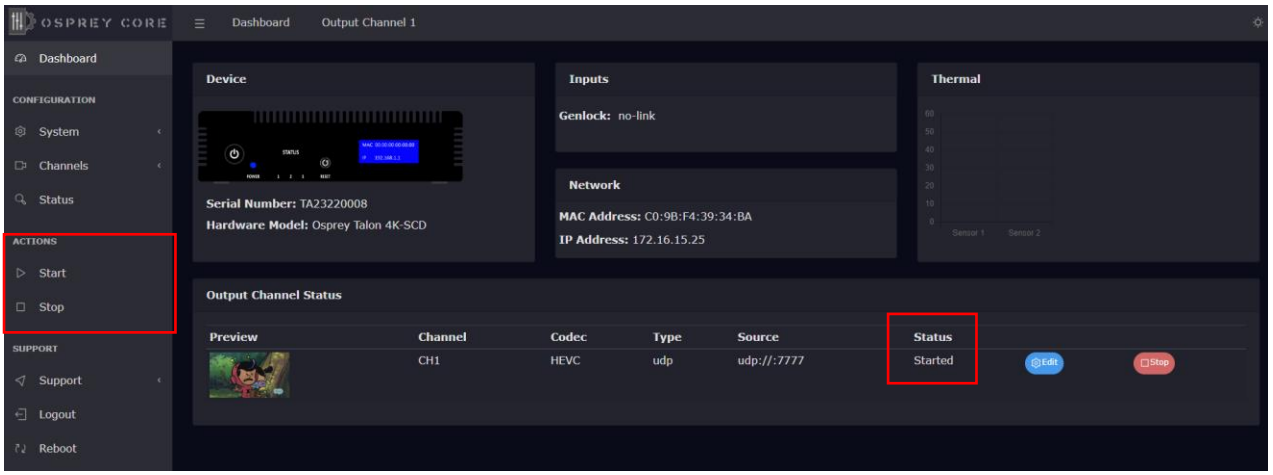
Web Interface – Status and Stream Start/Stop

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.

Status Page



Dashboard



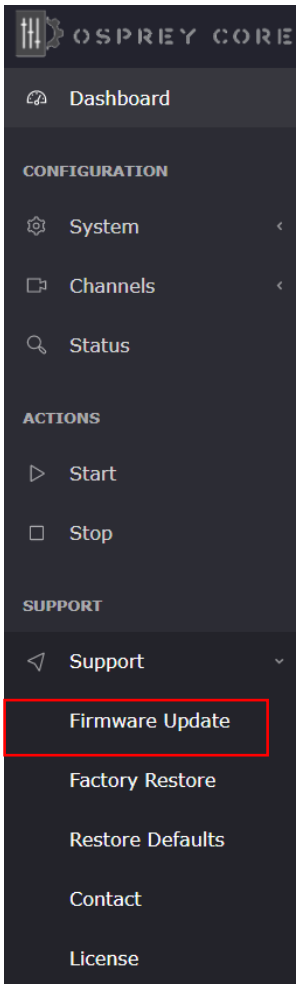
Starting the Decoder: After starting the Decoder, it can take up to 30 seconds for the decoder to identify the input signal format to deliver video frames.

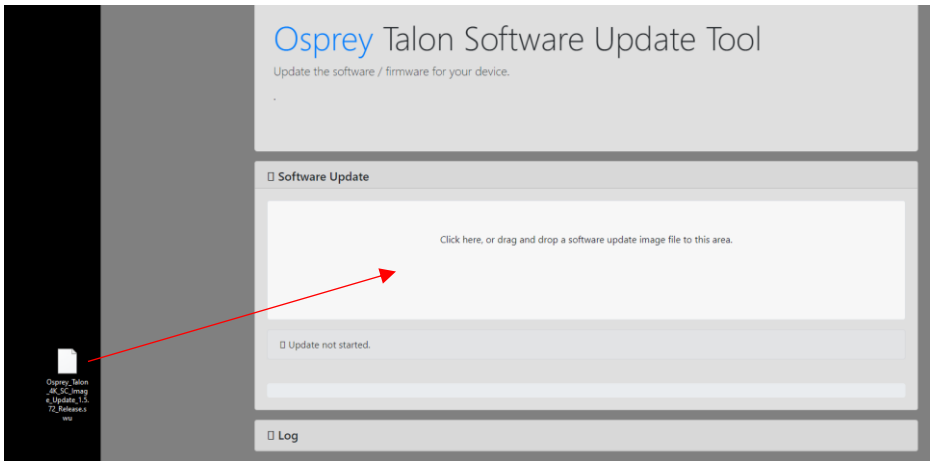
Web Interface – Firmware Update

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

Firmware upgrade steps:

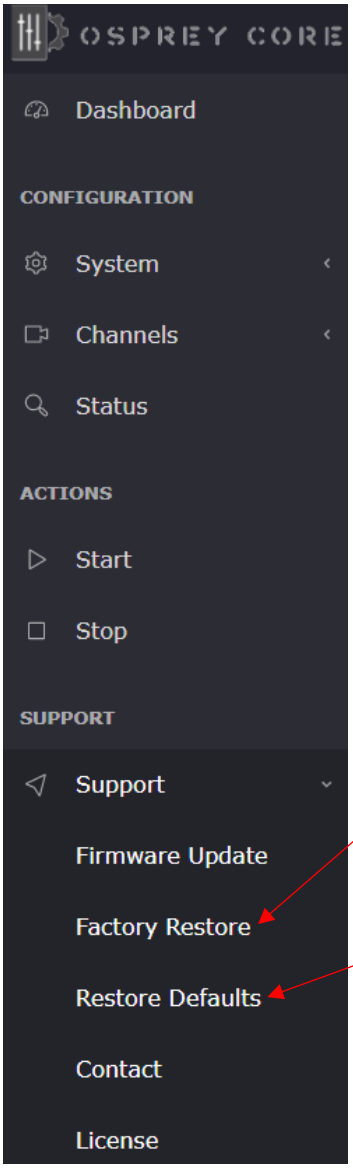
1. Download the latest firmware revision at www.ospreyvideo.com/talon-software-and-firmware
2. Go to 'Firmware Updates' on Talon Web Interface
3. Drop the downloaded firmware file into the 'Software Update Tool'
4. Update will start immediately and might take several minutes





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

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 decoders 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