



Operational guide for 5K60 MWC / Dante AV-A encoder and decoder endpoints.

Revision history

Revision	Date	Description	Basis
1.0	26 Sep 2026	Initial editable release	Live Web UI capture plus approved project references

How to use this manual

Each screen section identifies the page purpose, visible controls, a safe operating workflow, and the result to verify. The screenshots show one lab configuration; addresses, stream numbers, device names, firmware, and status values are examples rather than factory defaults.

ADMINISTRATOR NOTE: The encoder and decoder captures show different firmware generations. Verify labels and available choices against the installed firmware before applying a production change.

Table of contents

Section	Contents
1	Product and capture overview
2	Accessing the Web UI
3	Home and stream setup
4	Network configuration
5	Video, audio, EDID, wall, and playlists
6	Security and administration
7	Control: Serial and NAV-React
8	System logs and status
9	Routine workflows and troubleshooting

1. Product and capture overview

The Vx-610 family provides high-resolution AVoIP encode/decode workflows with multicast video, audio, control, EDID, playlist, and status functions.

Operational safety and administration

- Confirm the endpoint role and device name in the banner before changing a stream.
- Coordinate multicast, IGMP, DSCP, VLAN, and address settings with the network design.
- Treat EDID, HDCP, wall, playlist, serial, and NAV-React changes as signal-path changes.
- Do not upload certificate private keys or LDAP credentials to the wrong device or role.
- Preserve logs and status evidence before rebooting or restoring defaults.

FIRMWARE SCOPE: The VE-610 was captured on firmware V1.0.3.0 and the VD-610 on firmware V0.3.15. Use each figure as a workflow reference and confirm the current endpoint's labels before changing it.

2. Accessing the Web UI

Connect the service computer to the same routed management network as the endpoint. Use a modern browser and enter the device management address. The Web UI opens over HTTP for normal pages and redirects to HTTPS for protected security functions.

Sign in

1. Open the device IP address in the browser.
2. Enter the authorized administrator credentials. The capture environment used username admin and password password.
3. Confirm the model, role, and device name in the banner before making a change.
4. After administration, select Logout and close the browser session.

SECURITY: The lab credential shown above must not be retained in production. Change it immediately, use a unique managed password, and limit management access to trusted networks. Security pages may require HTTPS and acceptance of a device certificate. Address values shown are capture-environment examples; use the approved address plan for deployment.

Navigation model

Menu	Typical contents
Home	Stream assignment, device name, management options, source preview, status transmission
Network	IP, DNS, VLAN where supported, date/time, NTP, and 802.1X
Video/Audio	600 Series media, EDID, playlist, wall, and audio functions
Security	HTTPS policy, users, passwords, certificates, and LDAP
Control	Serial and NAV-React event actions
System	Logs, live status, identity, firmware, reboot, and default settings

3. Home and stream setup

3.1 VE-610 Home

The encoder Home page defines the transmitted stream, audio-for-host-play behavior, management options, source preview, and periodic status/discovery behavior.

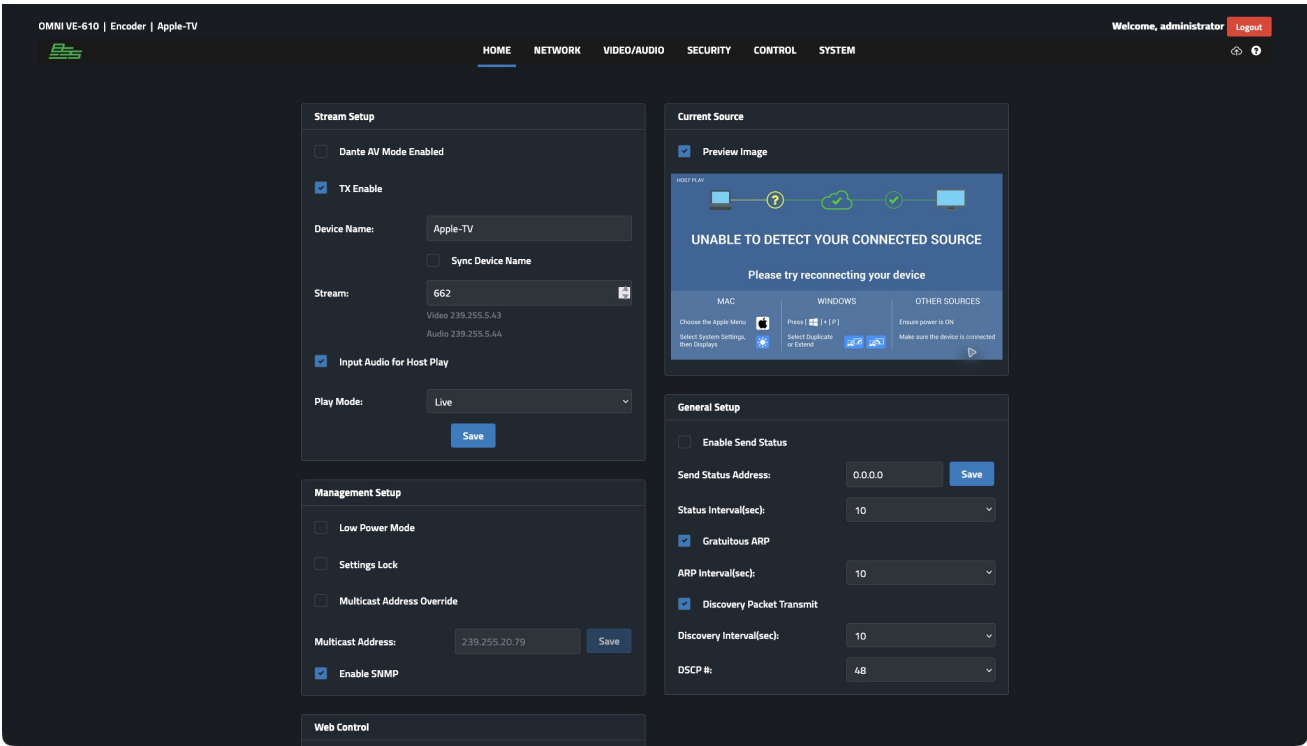


Figure 3-1. Live VE-610 Home page

Controls and indicators

Control / area	Purpose and operator guidance
Dante AV Mode Enabled	Enables Dante AV mode when required by the deployment.
TX Enable	Enables video transmission.
Device Name / Sync	Names the encoder and controls synchronized naming.
Stream	Defines the multicast stream; the UI shows derived video and audio multicast addresses.
Input Audio for Host Play	Includes input audio for local/host playback behavior.
Play Mode	Selects Live or a host-play playlist mode.
Current Source	Shows preview and connected-source state.
Management / General Setup	Low power, lock, multicast override, SNMP, status, ARP, discovery, and DSCP.

Recommended workflow

1. Confirm VE-610 and Encoder in the banner.
2. Choose the approved stream and TX state; changing Stream, TX Enable, Dante AV mode, or multicast override can interrupt receivers immediately.
3. Confirm play mode and audio-for-host-play requirement.
4. Save the affected panel and verify multicast values and source status.

3.2 VD-610 Home

The physical decoder Home page selects the received video and audio streams, local-play behavior, management options, source preview, and periodic network announcements.

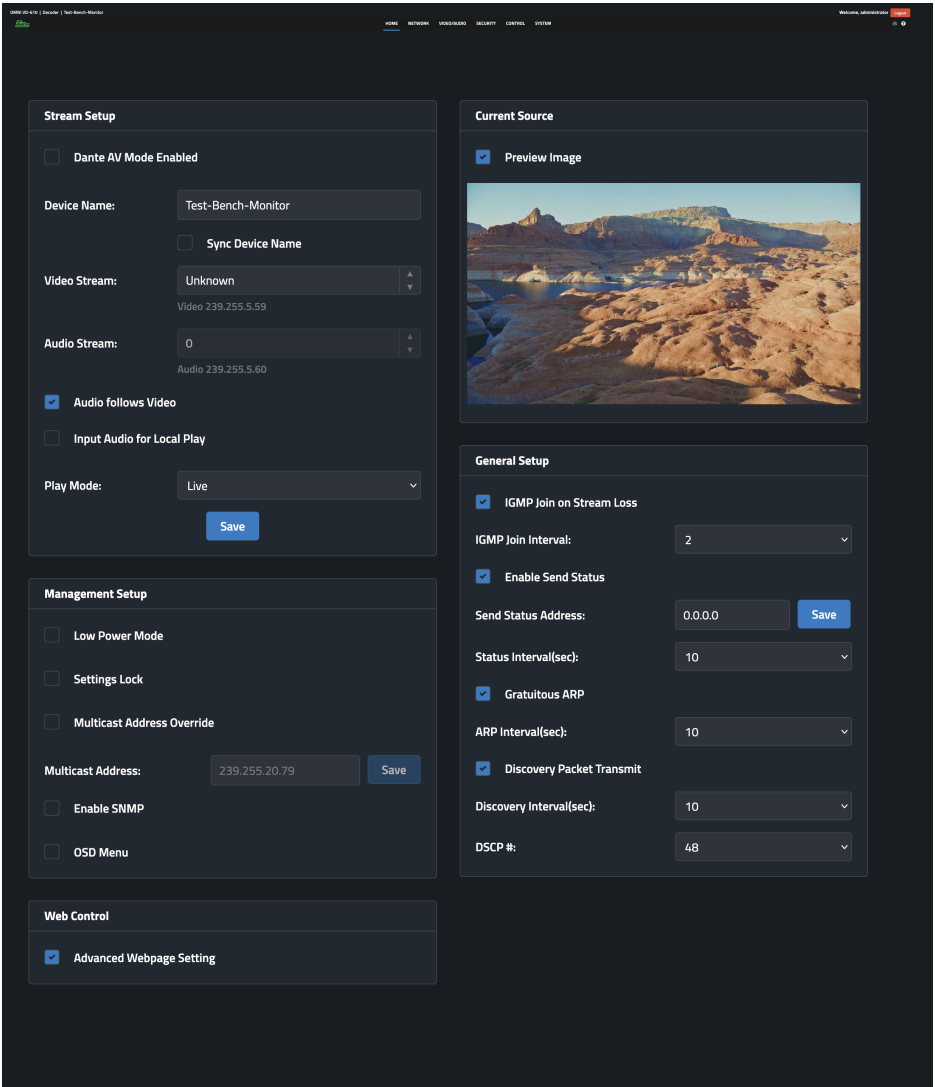


Figure 3-2. Physical VD-610 Home page; firmware V0.3.15

Controls and indicators

Control / area	Purpose and operator guidance
Dante AV Mode Enabled	Enables the Dante AV operating mode when required.
Device Name / Sync	Names the decoder and controls synchronized naming.
Video / Audio Stream	Selects stream numbers; the UI shows derived multicast addresses.
Audio follows Video	Keeps audio routing tied to the selected video stream.
Input Audio for Local Play	Includes input audio during local playback when enabled.
Play Mode	Selects Live or local playback.
Management Setup	Low power, settings lock, multicast override, SNMP, and OSD Menu.
General Setup	IGMP join-on-loss, status, ARP, discovery, and DSCP behavior.

Recommended workflow

1. Confirm VD-610 and Decoder in the banner.
2. Select the intended video and audio streams.
3. Set audio-follow and local-play behavior.
4. Save, then confirm output and stream activity on Status.

SIGNAL IMPACT: Changing stream numbers, Dante AV mode, multicast override, or play mode can interrupt the displayed program.

4. Network configuration

4.1 VE-610 IP Setup

Configure management identity, DNS, IGMP version, IPv4, and IPv6 from the encoder Network menu.

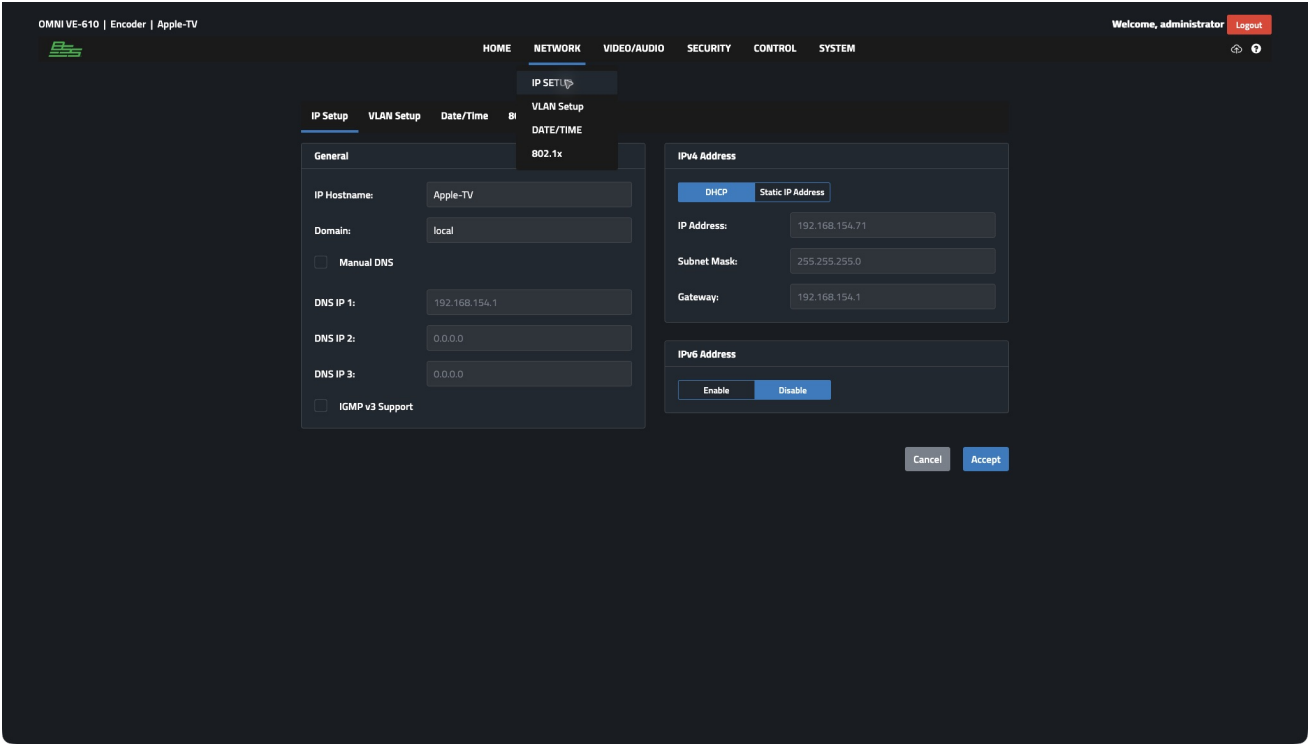


Figure 4-1. VE-610 IP Setup

Controls and indicators

Control / area	Purpose and operator guidance
Hostname / Domain	Management identity and DNS suffix.
Manual DNS	Enables explicit resolver addresses.
IGMP v3	Selects IGMPv3 support.
DHCP / Static	Selects the IPv4 address method.
IPv6	Enables or disables IPv6 management.

Recommended workflow

1. Record the current address set.
2. Validate the new address against the network plan.
3. Apply the complete DNS/IP/gateway configuration.
4. Reconnect and verify the endpoint identity.

NETWORK SAFETY: Keep a local recovery path; an incorrect address, mask, gateway, or VLAN can make the device unreachable.

4.2 VE-610 VLAN Setup

VLAN Setup separates Dante traffic and provides its IPv4/DNS parameters.

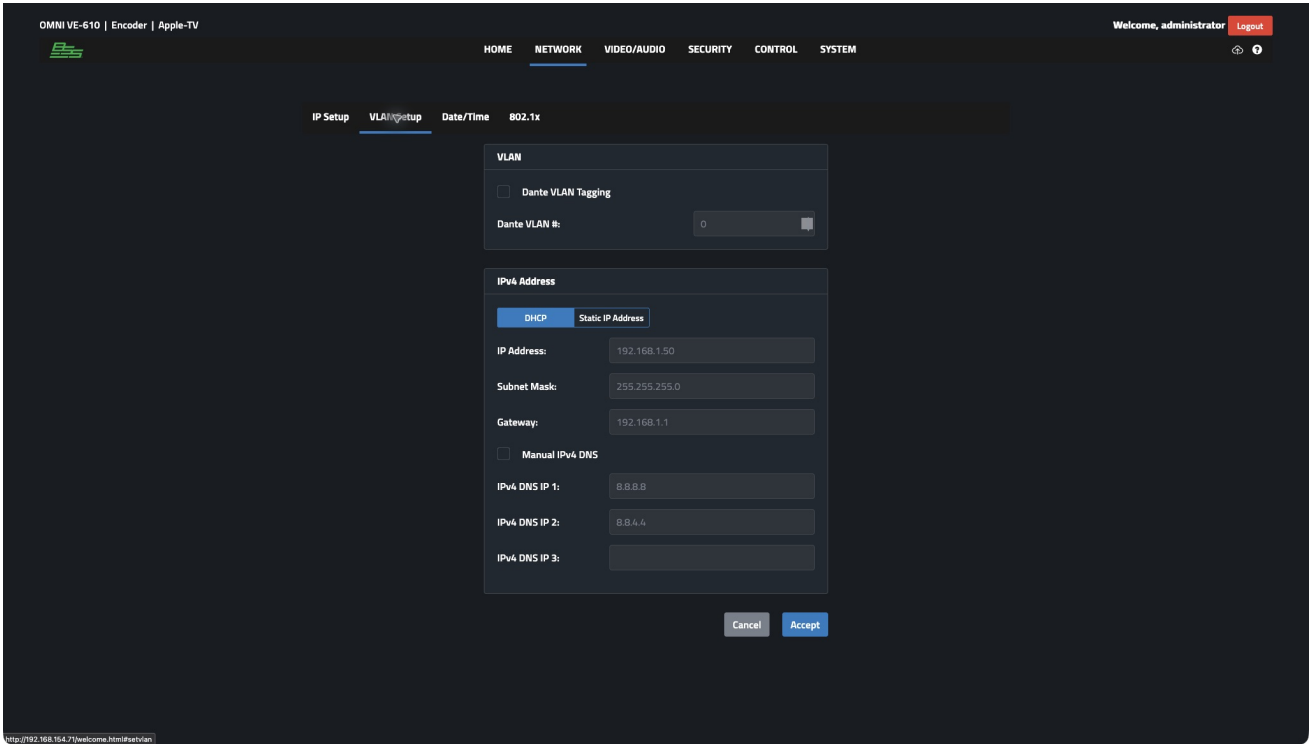


Figure 4-2. VE-610 Dante VLAN configuration

Controls and indicators

Control / area	Purpose and operator guidance
Dante VLAN Tagging	Enables VLAN tagging for Dante traffic.
Dante VLAN #	Sets the VLAN identifier.
IPv4 DHCP / Static	Defines the address on the Dante network.
Manual IPv4 DNS	Sets resolvers used on that interface.

Recommended workflow

1. Confirm switch trunk/access policy and the approved VLAN ID.
2. Stage IP, gateway, and DNS values.
3. Enable tagging only when both endpoint and switch configuration are ready.
4. Verify Dante discovery and audio status after applying.

4.3 VE-610 Date/Time

Set the time zone and NTP sources used for logs and certificate validation.

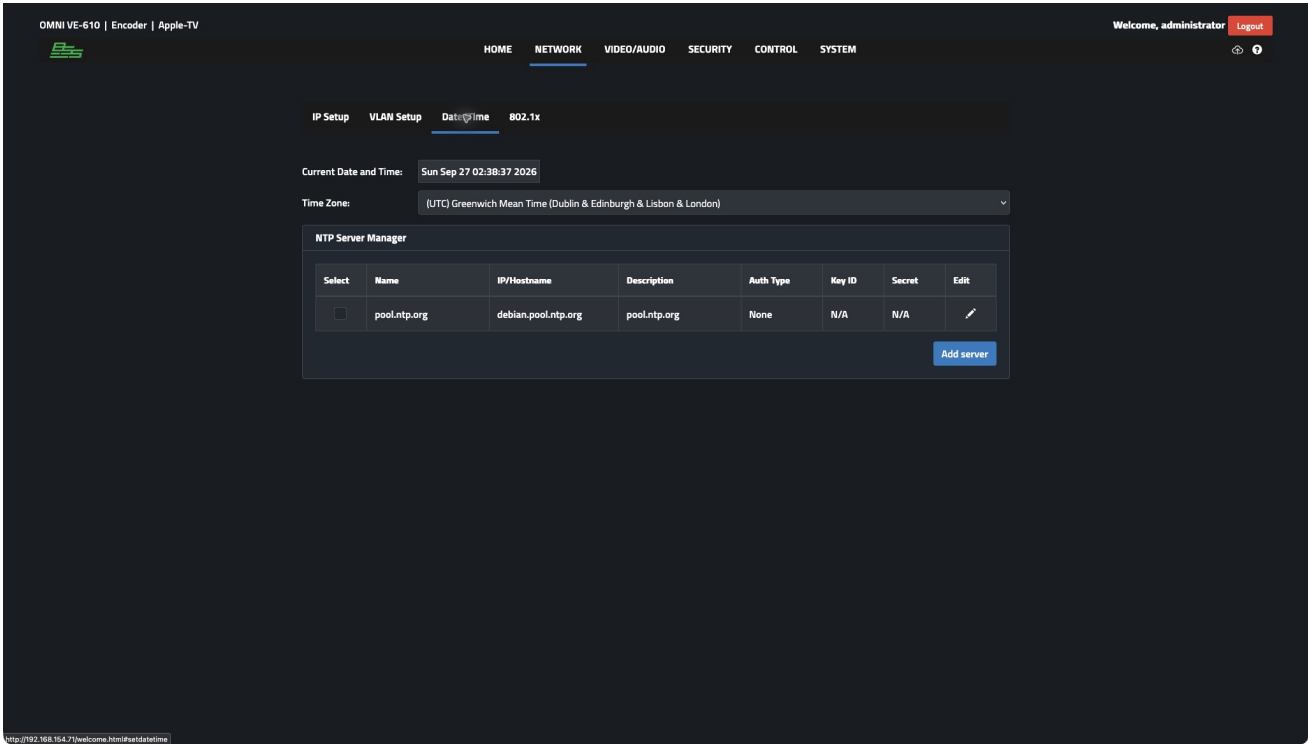


Figure 4-3. VE-610 Date/Time and NTP manager

Controls and indicators

Control / area	Purpose and operator guidance
Time Zone	Local display offset.
NTP Server Manager	Adds and edits name, host, description, authentication type, key ID, and secret.

Recommended workflow

- 1. Select the site time zone.
- 2. Use resolvable approved NTP servers.
- 3. Verify time before certificate or log troubleshooting.

4.4 VE-610 802.1X

The protected 802.1X page supports password or certificate authentication.

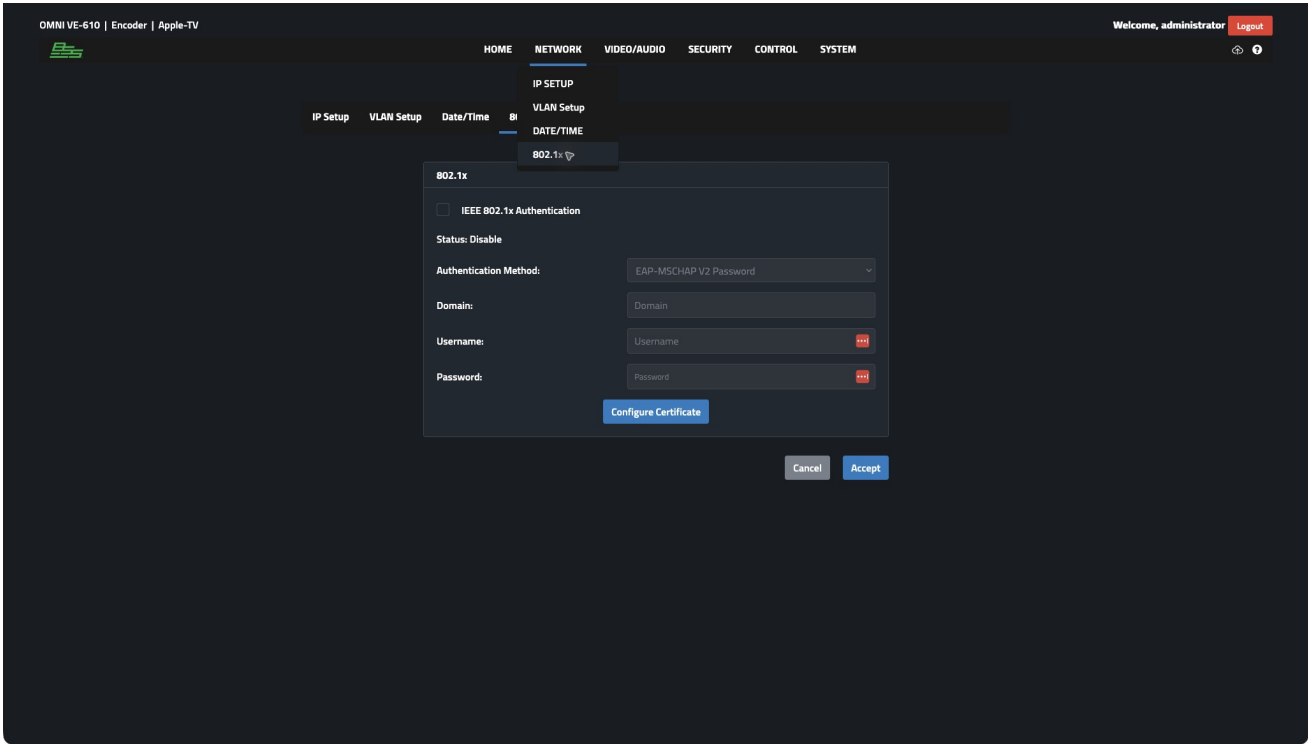


Figure 4-4. VE-610 IEEE 802.1X authentication

Controls and indicators

Control / area	Purpose and operator guidance
Enable	Activates port authentication.
Method	EAP-MSCHAP V2 Password or EAP-TLS Certificate.
Identity	Domain, username, and password for password-based authentication.
Configure Certificate	Stages EAP-TLS certificate material.

Recommended workflow

1. Prepare switch and identity policy.
2. Verify device time and trust chain.
3. Stage the selected method and credentials.
4. Enable during a staffed maintenance window and verify continued access.

LOCKOUT RISK: A policy, certificate, or credential mismatch can remove management and media connectivity.

4.5 VD-610 IP Setup

The decoder exposes host identity, DNS, IGMP, IPv4, and IPv6 controls.

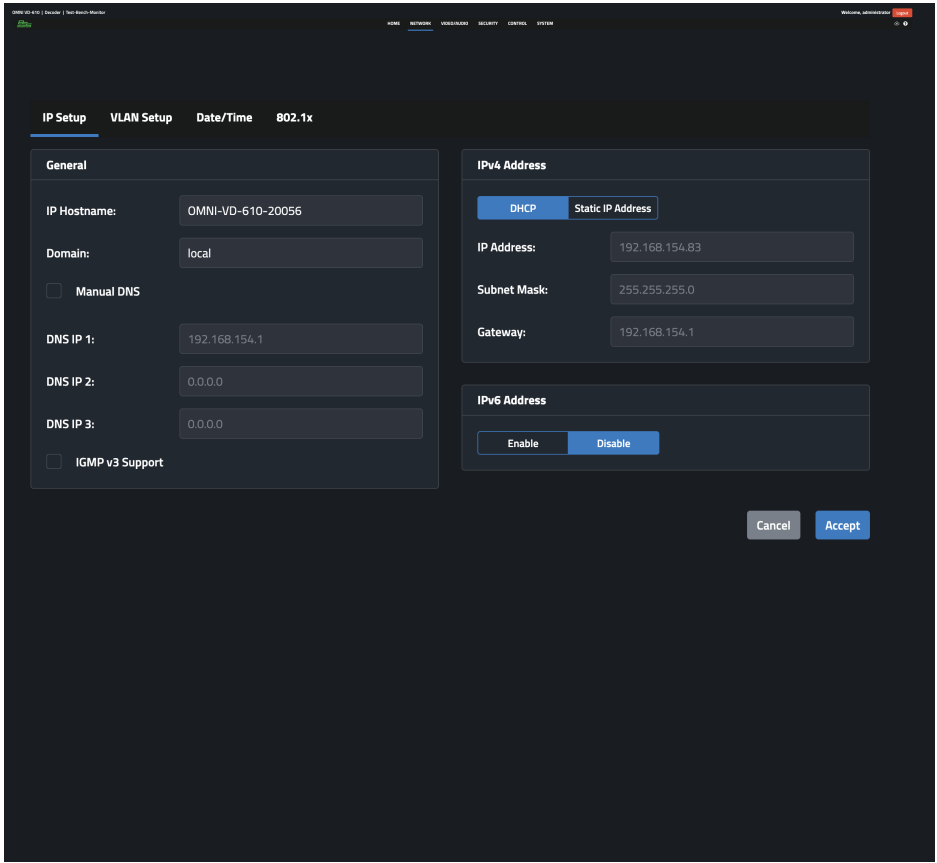


Figure 4-5. Physical VD-610 IP Setup

Controls and indicators

Control / area	Purpose and operator guidance
Hostname / Domain	Decoder management identity.
DNS / IGMP	Name resolution and multicast membership behavior.
DHCP / Static	Selects the IPv4 address method.
IPv6	Enables or disables IPv6 management.

Recommended workflow

1. Record the current address set.
2. Validate the target address, mask, gateway, and DNS values.
3. Apply, reconnect at the resulting address, and confirm the banner identity.

NETWORK SAFETY: Keep a local recovery path; an incorrect address or mask can make the decoder unreachable.

4.6 VD-610 VLAN Setup

The physical decoder provides Dante VLAN tagging, a dedicated-P1-to-Dante option, and interface addressing.

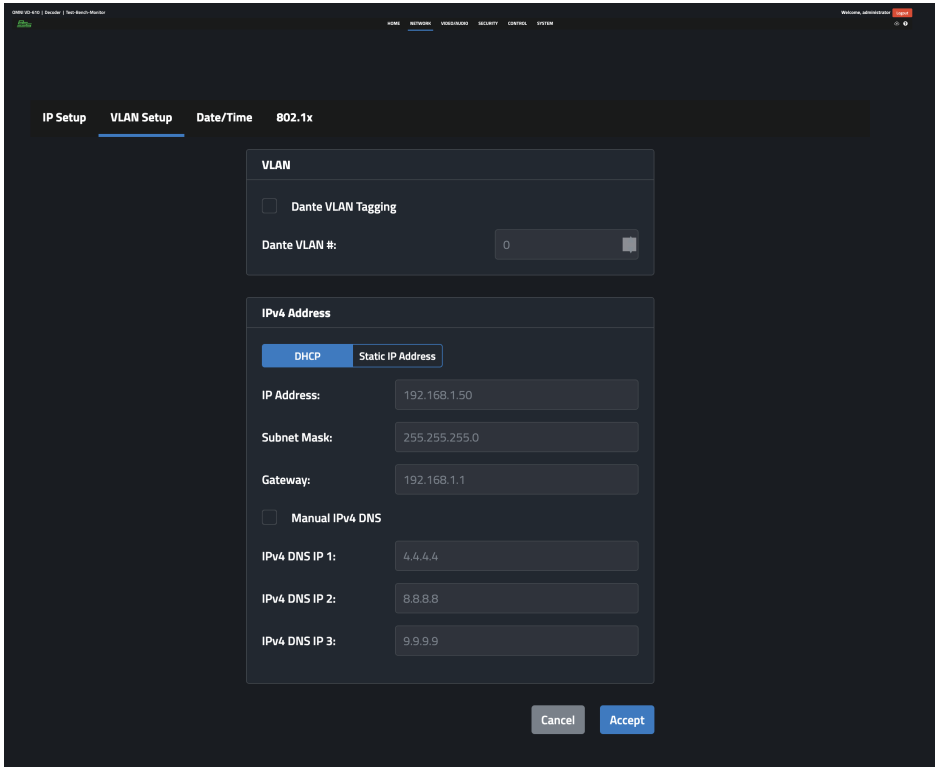


Figure 4-6. Physical VD-610 Dante VLAN setup

Controls and indicators

Control / area	Purpose and operator guidance
Dante VLAN Tagging / VLAN #	Tags decoder Dante traffic.
Dedicated P1 to Dante	Assigns the secondary physical port to Dante where supported.
IPv4 / DNS	Defines the Dante network address and resolvers.

Recommended workflow

1. Confirm physical port mapping.
2. Coordinate tagging and port mode with the switch.
3. Verify Dante discovery and audio after deployment.

4.7 VD-610 Date/Time

The decoder provides time-zone and NTP management used by logs and certificate validation.

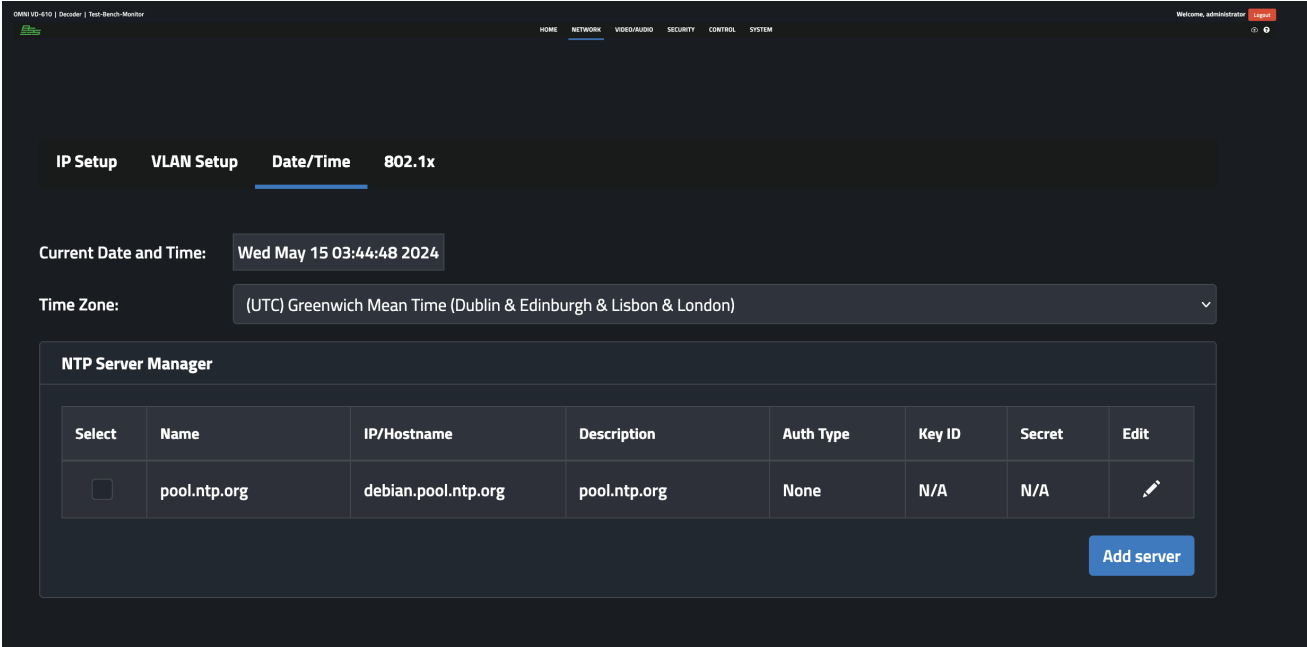


Figure 4-7. Physical VD-610 Date/Time and NTP manager

Controls and indicators

Control / area	Purpose and operator guidance
Time Zone	Local display offset.
NTP table	Server name, host, description, and authentication values.

Recommended workflow

1. Use the site-standard time zone and approved NTP sources.
2. Confirm correct time before secure deployment or troubleshooting.

4.8 VD-610 802.1X

The physical decoder supports password- or certificate-based network access control.

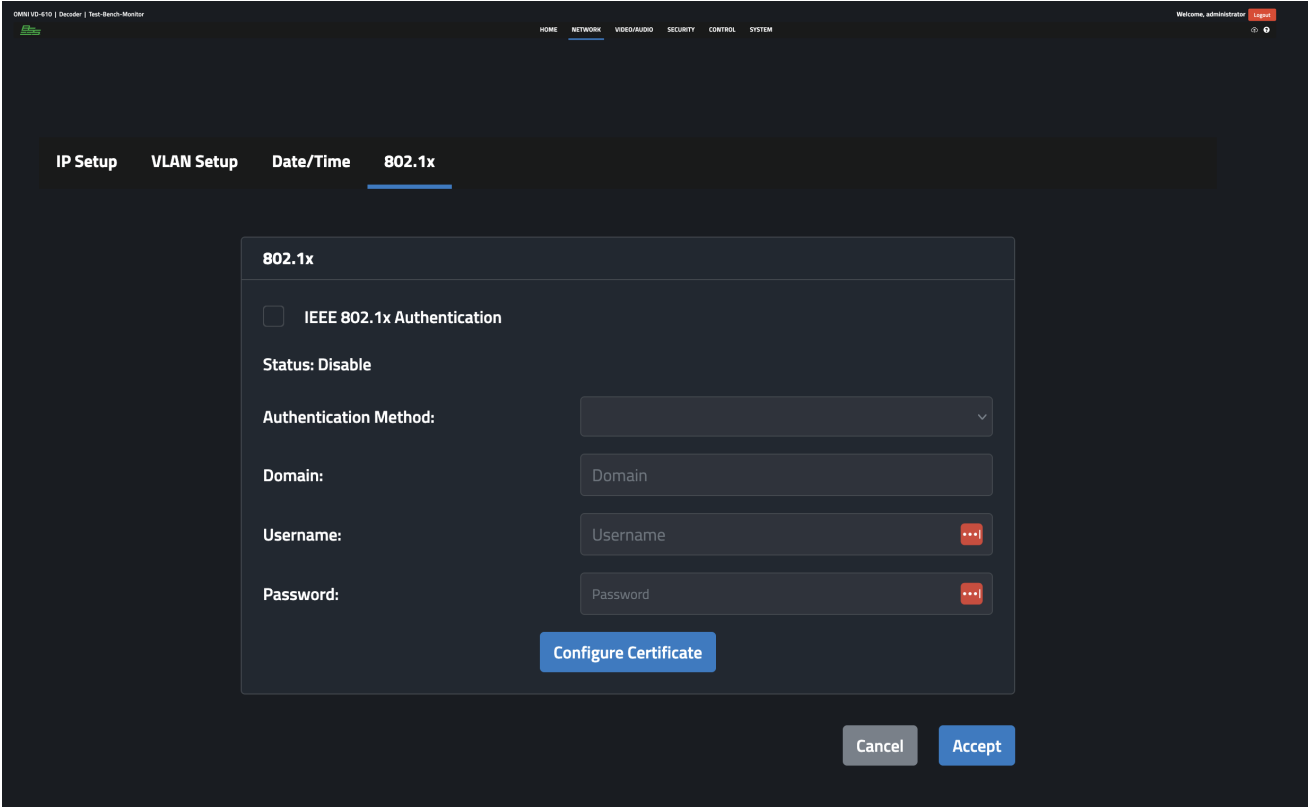


Figure 4-8. Physical VD-610 IEEE 802.1X authentication

Controls and indicators

Control / area	Purpose and operator guidance
Enable	Activates port authentication.
Method	Selects password or certificate authentication.
Identity fields	Supplies domain, username, and protected password when required.
Configure Certificate	Stages certificate material for EAP-TLS.

Recommended workflow

1. Prepare the switch and identity policy first.
2. Verify time and the trust chain.
3. Stage the method and identity material.
4. Enable during a staffed window and verify continued access.

LOCKOUT RISK: A policy, certificate, or credential mismatch can remove network access.

5. Video, audio, EDID, wall, and playlists

5.1 VE-610 Video

The encoder Video page controls HDCP support and video mute while reporting input HDMI state, resolution, and HDCP status.

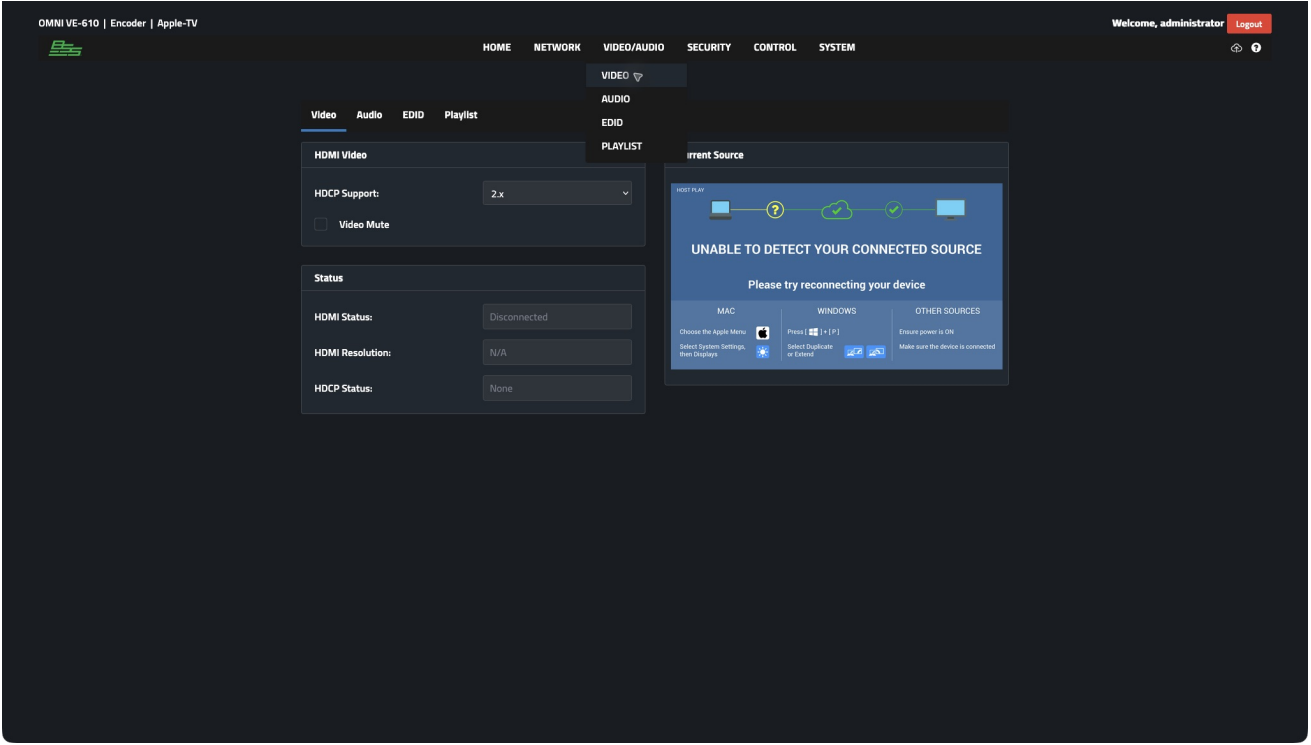


Figure 5-1. VE-610 Video settings and HDMI status

Controls and indicators

Control / area	Purpose and operator guidance
HDCP Support	Selects supported HDCP mode.
Video Mute	Suppresses transmitted video.
HDMI Status / Resolution / HDCP	Read-only source diagnostics.
Current Source	Preview and source guidance.

Recommended workflow

1. Confirm the source and display-chain HDCP requirement.
2. Choose the approved HDCP mode.
3. Use mute only for planned blanking.
4. Verify live HDMI status and resolution after saving.

5.2 VE-610 Audio

The encoder Audio page controls Dante audio availability and stream mute.

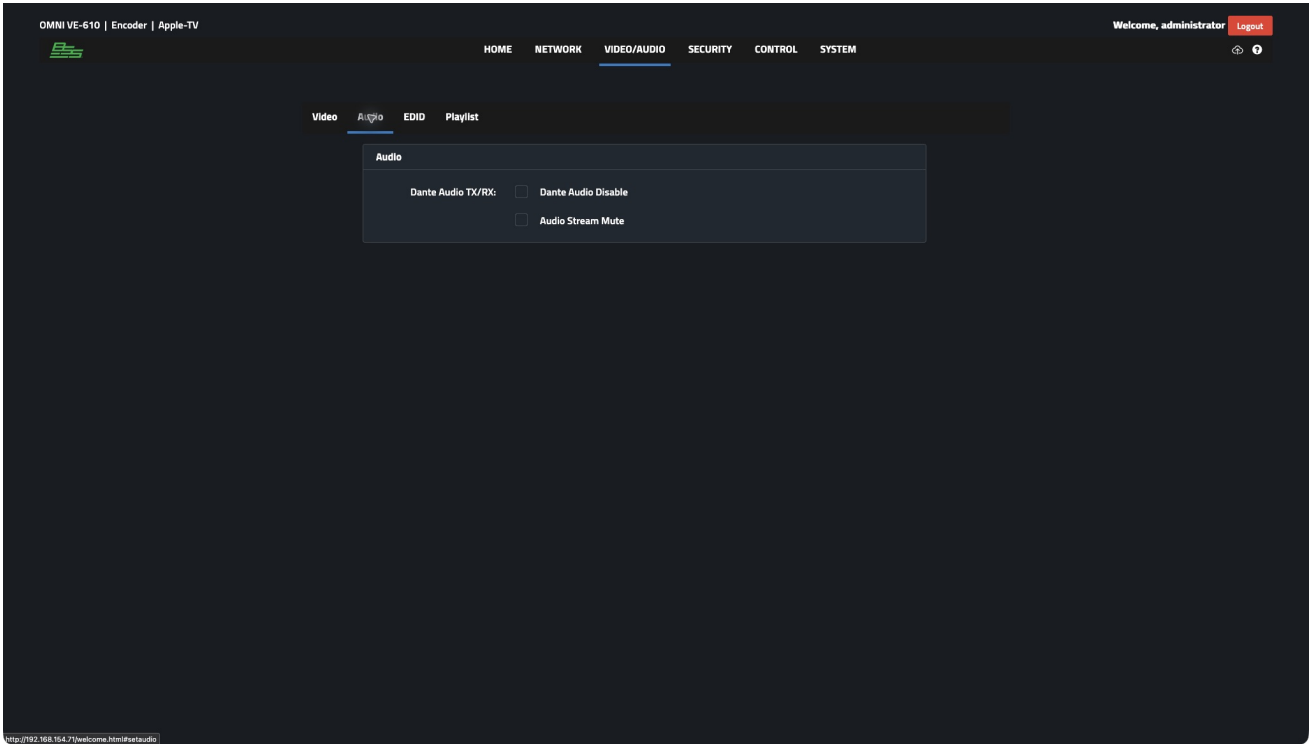


Figure 5-2. VE-610 Audio controls

Controls and indicators

Control / area	Purpose and operator guidance
Dante Audio Disable	Disables Dante audio transport.
Audio Stream Mute	Mutes the transmitted audio stream.

Recommended workflow

1. Confirm the intended audio transport.
2. Apply mute or disable only with operator awareness.
3. Verify Dante/audio status after saving.

5.3 VE-610 EDID

The encoder EDID editor provides raw EDID data, presets/reset actions, set/decode/encode functions, and decoded capability sections.

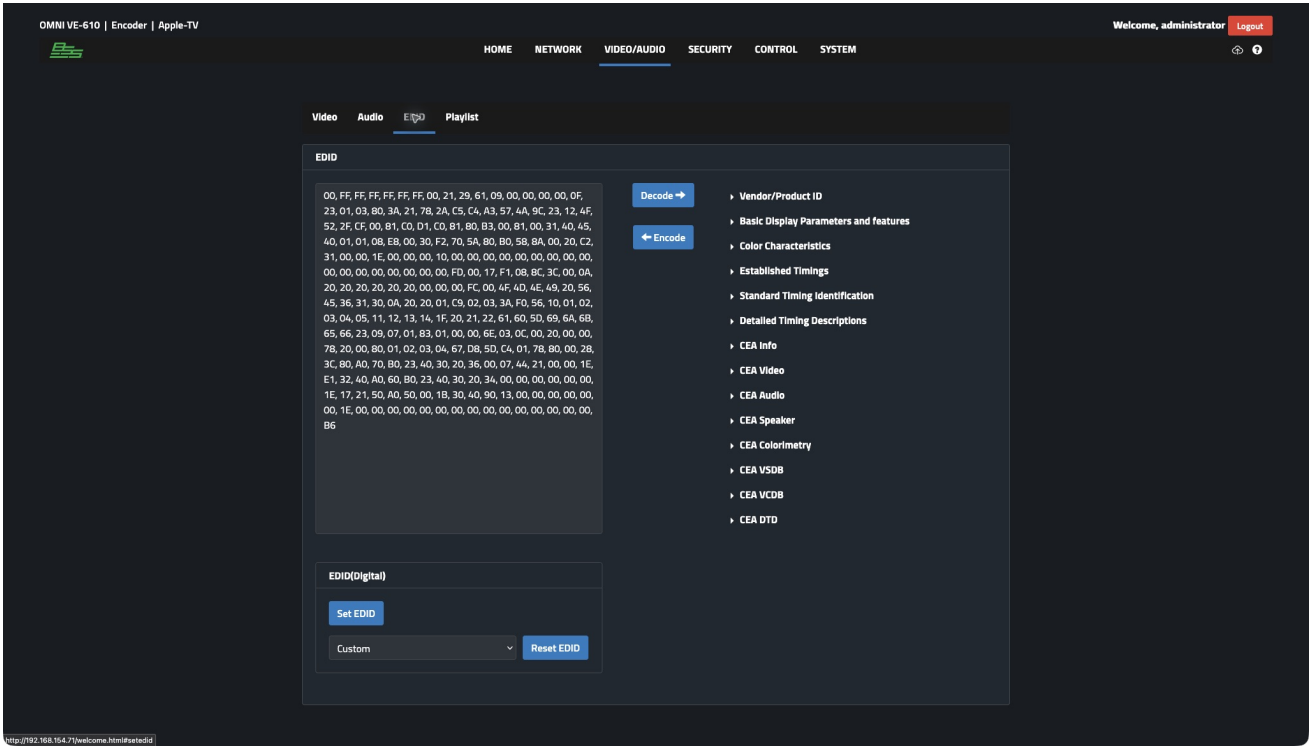


Figure 5-3. VE-610 EDID editor

Controls and indicators

Control / area	Purpose and operator guidance
EDID data	Displays or accepts the hexadecimal EDID block.
Custom / Reset / Set EDID	Selects and applies EDID behavior.
Decode / Encode	Converts between raw and structured views.
Capability sections	Vendor, display, color, timing, and CEA audio/video details.

Recommended workflow

1. Export or copy the current EDID before editing.
2. Choose a known-good preset or validate the complete custom block.
3. Set the EDID and reconnect the source if required.
4. Verify source resolution, color, audio, and HDCP.

SIGNAL RISK: An invalid EDID can remove video or audio. Preserve a known-good EDID and recovery path.

5.4 VE-610 Playlist

The encoder playlist/image database stores host-play images and shows available capacity.

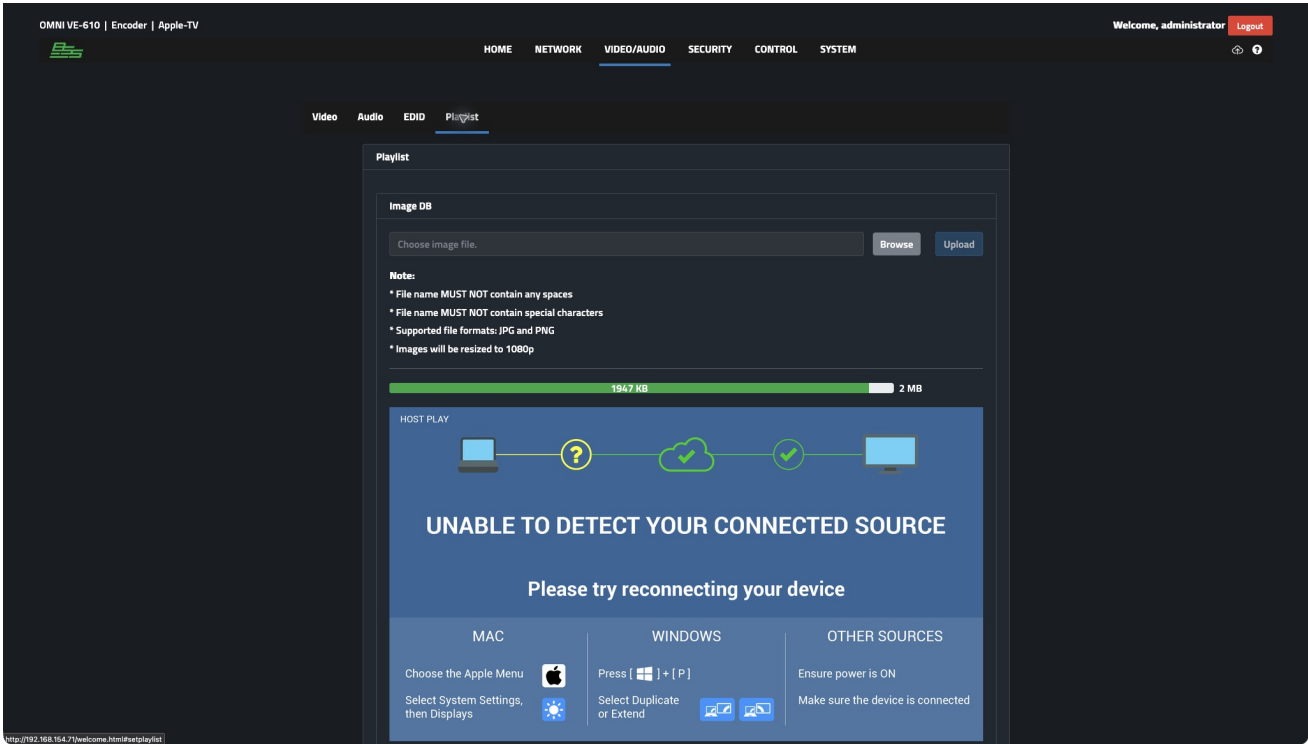


Figure 5-4. VE-610 Playlist and Image DB

Controls and indicators

Control / area	Purpose and operator guidance
Choose File	Uploads a JPG or PNG.
File rules	No spaces or special characters; images are resized to 1080p.
Image DB	Lists file name, resolution, and available capacity.
Play Mode	Home page selects Live or playlist playback.

Recommended workflow

1. Prepare a compliant JPG/PNG filename.
2. Confirm image content and available database space.
3. Upload and verify the listed resolution.
4. Select the intended play mode and validate output.

5.5 VD-610 Video

The physical decoder Video page enables the output and scaler, chooses output format, controls stream-loss behavior, and reports the active source.

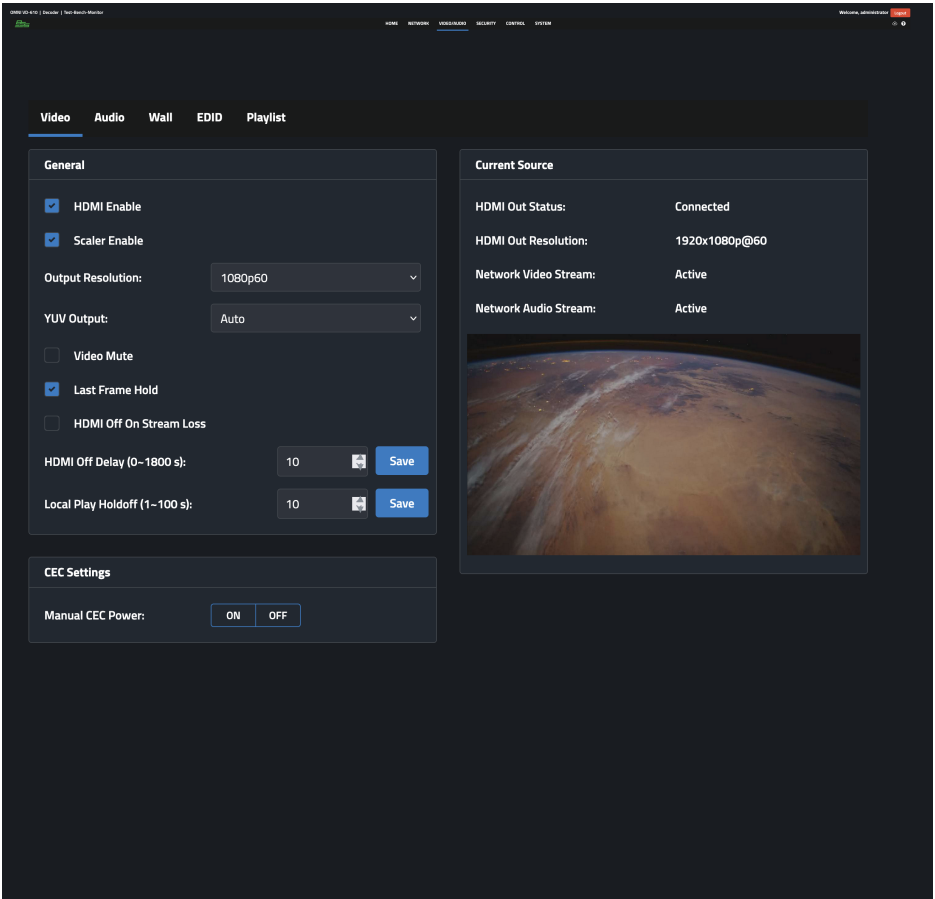


Figure 5-5. Physical VD-610 output video controls and Current Source

Controls and indicators

Control / area	Purpose and operator guidance
HDMI Enable / Scaler Enable	Controls the HDMI output and scaling path.
Output Resolution / YUV Output	Chooses the display format and color-output behavior.
Video Mute / Last Frame Hold	Controls blanking and loss-of-stream presentation.
HDMI Off On Stream Loss / delays	Controls power-off and local-play timing.
Manual CEC Power	Sends an ON or OFF CEC power action.
Current Source	Shows HDMI output, resolution, network activity, and preview.

Recommended workflow

- 1. Record the current output format.
- 2. Choose a resolution supported by the display chain.
- 3. Set stream-loss and CEC behavior deliberately.
- 4. Save and verify output status and picture.

DISPLAY IMPACT: Disabling HDMI, changing resolution, or changing stream-loss behavior can blank the display.

5.6 VD-610 Audio

The decoder Audio page controls Dante transport, audio stream selection, mute, and whether audio follows video.

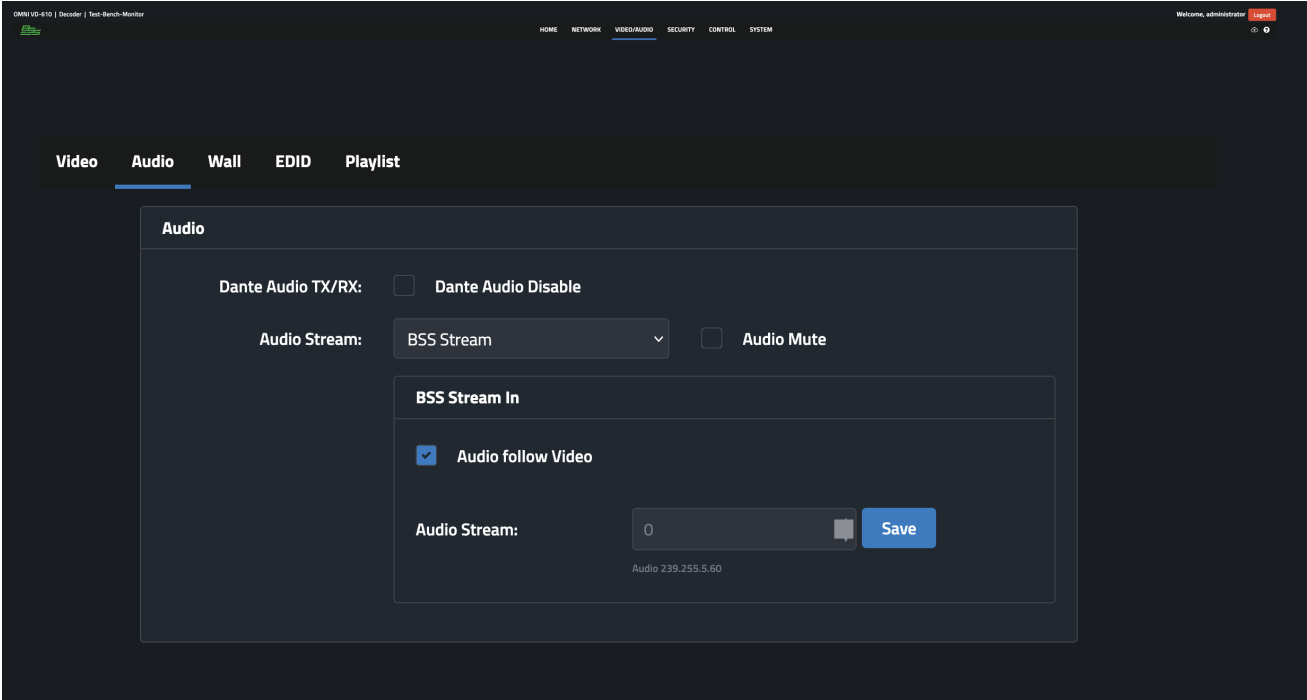


Figure 5-6. Physical VD-610 audio controls

Controls and indicators

Control / area	Purpose and operator guidance
Dante Audio TX/RX	Disables Dante audio transport when selected.
Audio Stream	Selects the supported audio-stream mode.
Audio Mute	Mutes decoder output audio.
Audio follow Video	Uses the video selection to derive the audio stream.
Audio Stream value	Sets the audio stream when follow-video is not used.

Recommended workflow

1. Confirm the intended audio routing.
2. Choose follow-video or a specific audio stream.
3. Set mute and Dante state.
4. Verify audio activity and sample rate on Status.

5.7 VD-610 Video Wall

Video Wall maps the decoder to a row and column in a tiled display and provides bezel adjustment.

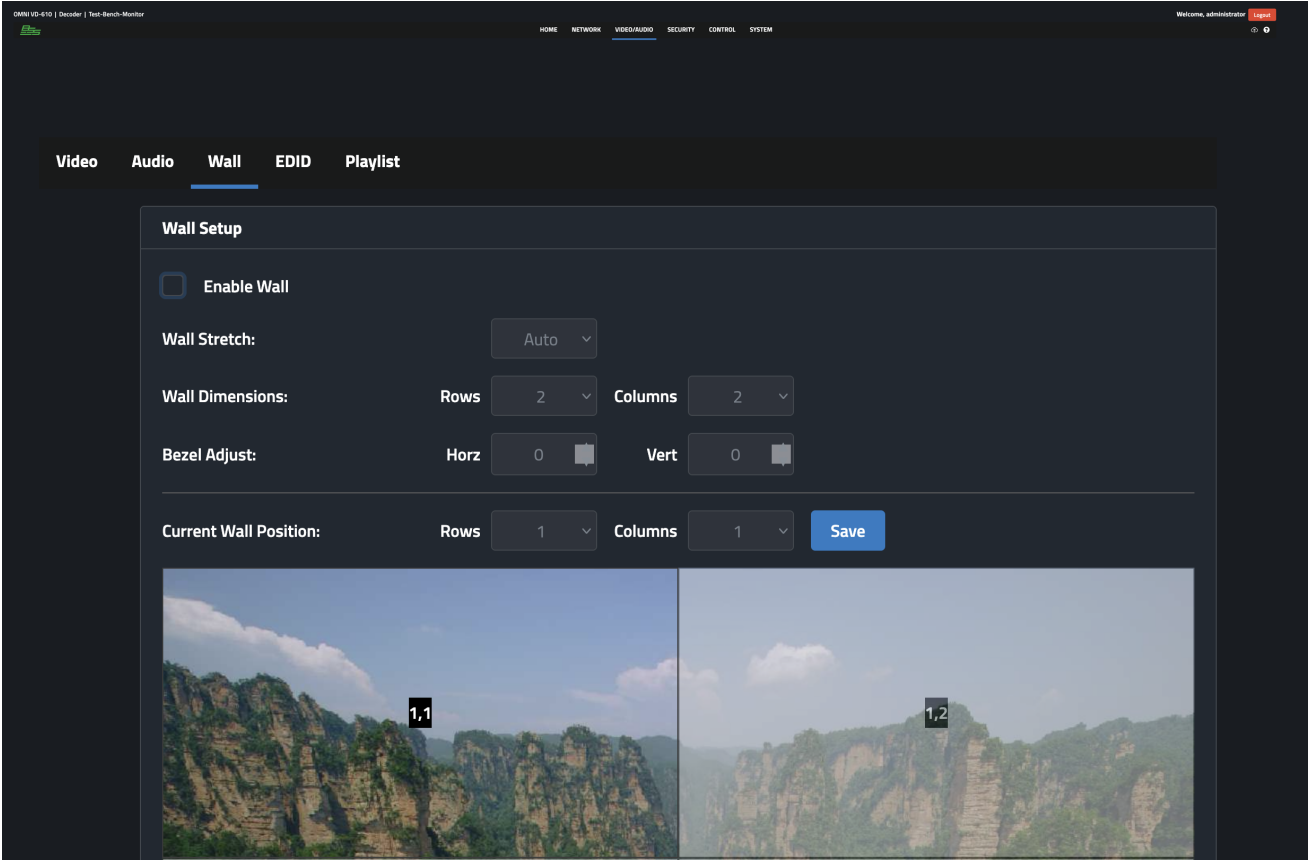


Figure 5-7. Physical VD-610 Video Wall setup

Controls and indicators

Control / area	Purpose and operator guidance
Enable Wall	Activates wall processing.
Wall Stretch	Selects the wall scaling behavior.
Rows / Columns	Defines the wall geometry.
Bezel Adjust	Compensates for horizontal and vertical bezel width.
Current Wall Position	Assigns this decoder within the wall.

Recommended workflow

1. Map displays and decoder positions first.
2. Enter identical geometry on all wall decoders.
3. Assign each position once and adjust bezels consistently.
4. Verify crop and alignment on the physical displays.

5.8 VD-610 EDID

The decoder EDID page displays raw display data and decodes it into structured capability sections.

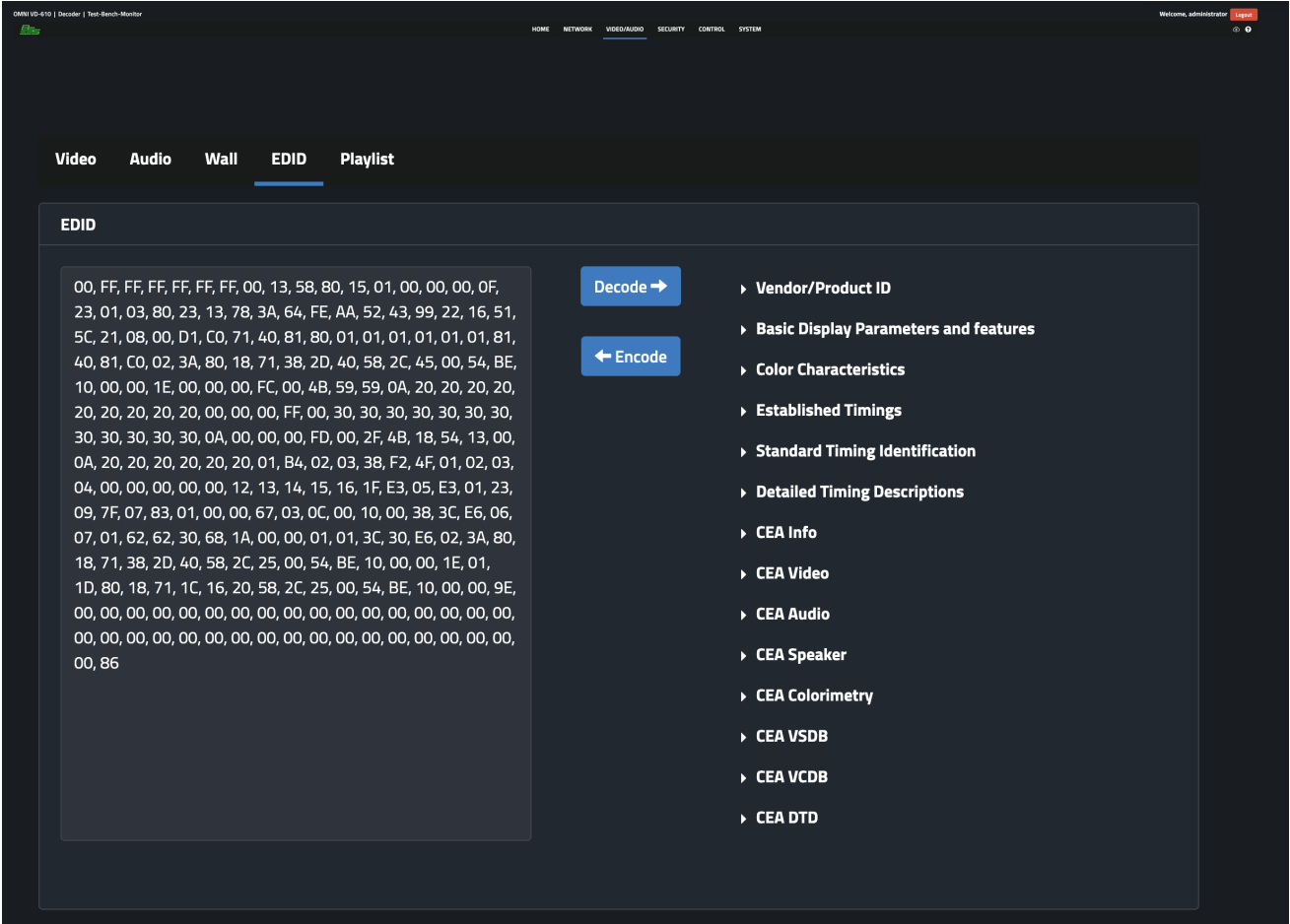


Figure 5-8. Physical VD-610 EDID editor

Controls and indicators

Control / area	Purpose and operator guidance
EDID data	Displays or accepts the hexadecimal EDID block.
Decode / Encode	Converts between raw and structured views.
Capability sections	Vendor, display, color, timing, and CEA audio/video details.

Recommended workflow

1. Preserve the current EDID before editing.
2. Validate the complete block and connected-display requirements.
3. Encode or decode as needed, then verify video, color, audio, and HDCP end to end.

SIGNAL RISK: An invalid EDID can remove video or audio. Preserve a known-good copy and recovery path.

5.9 VD-610 Playlist / Image DB

The decoder stores a local-play image for use when a live network AV source is unavailable.

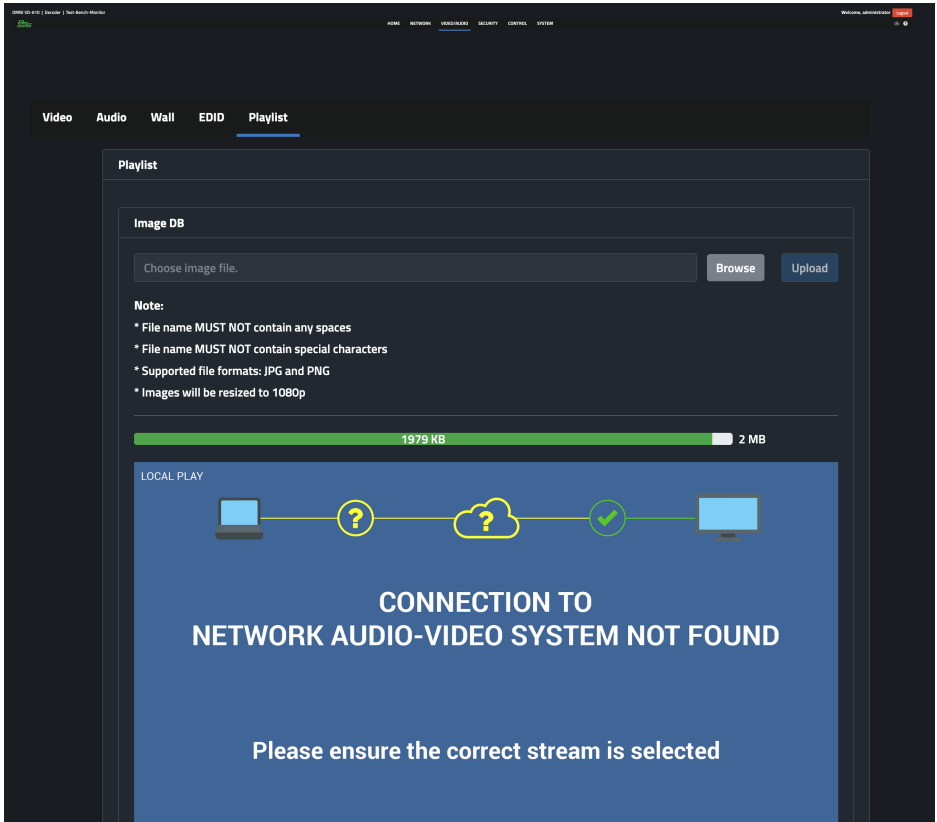


Figure 5-9. Physical VD-610 Playlist Image DB and local-play image

Controls and indicators

Control / area	Purpose and operator guidance
Choose image file / Browse	Selects a local JPG or PNG for upload.
Upload	Stores the selected image.
File rules	No spaces or special characters; images are resized to 1080p.
Capacity bar	Shows used and available image storage.
LOCAL PLAY preview	Shows the fallback image and its resolution.

Recommended workflow

1. Prepare a compliant JPG/PNG filename.
2. Confirm content and available space.
3. Upload and verify the preview and listed resolution.
4. Test local play during an approved window.

6. Security and administration

6.1 VE-610 Security — General

General security settings enforce HTTPS and secure control, manage command/stream passwords, and install certificates by role.

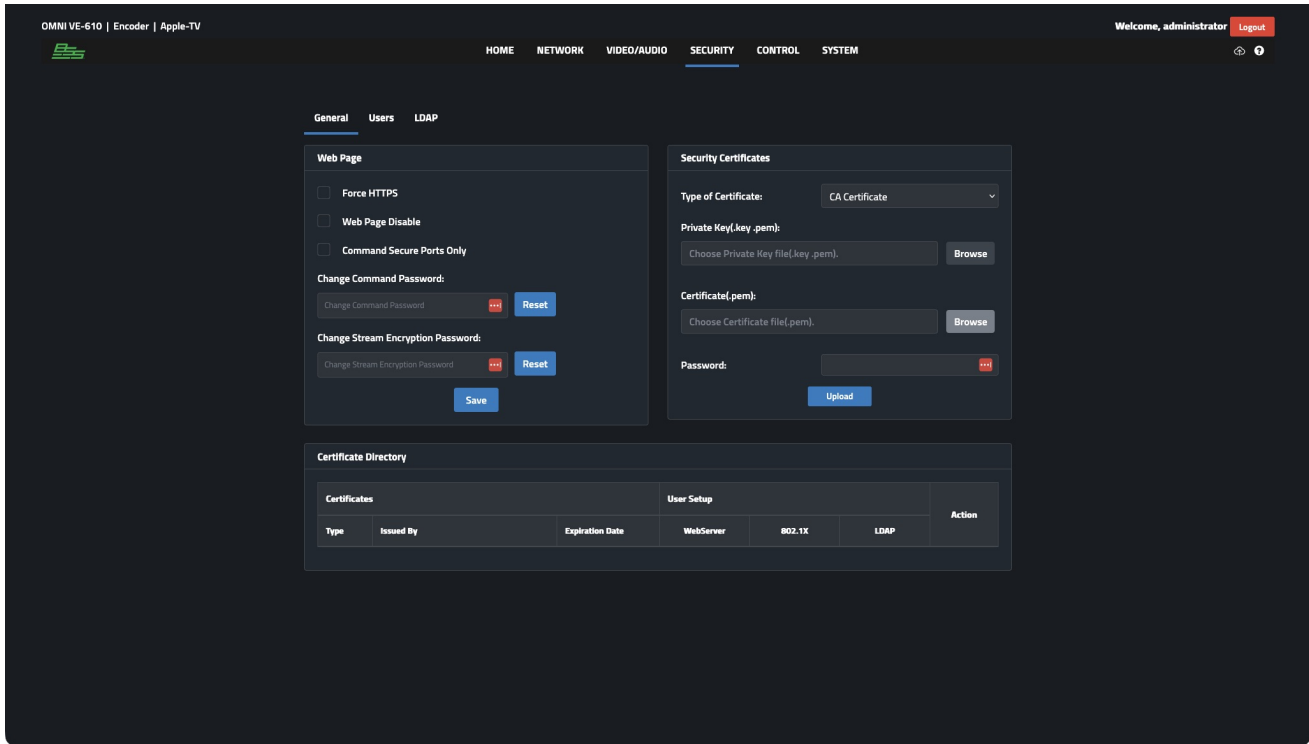


Figure 6-1. VE-610 Security General and certificate directory

Controls and indicators

Control / area	Purpose and operator guidance
Force HTTPS	Redirects management to HTTPS.
Web Page Disable	Disables Web UI access when required by policy.
Command Secure Ports Only	Restricts command control to secure ports.
Command / Stream passwords	Changes or resets protected-service credentials.
Certificate upload	Stages CA, private key, certificate, and optional password.
Certificate directory	Shows type, issuer, expiry, WebServer/802.1X/LDAP use, and actions.

Recommended workflow

1. Correct time, DNS, and hostname.
2. Install and verify approved certificate material.
3. Test HTTPS and secure control before enforcing secure-only modes.
4. Retain a documented recovery method.

PRIVATE KEYS: Never include certificate private keys or passwords in screenshots, tickets, or this manual.

6.2 VE-610 Security — Users

The Users tab changes the administrator password.

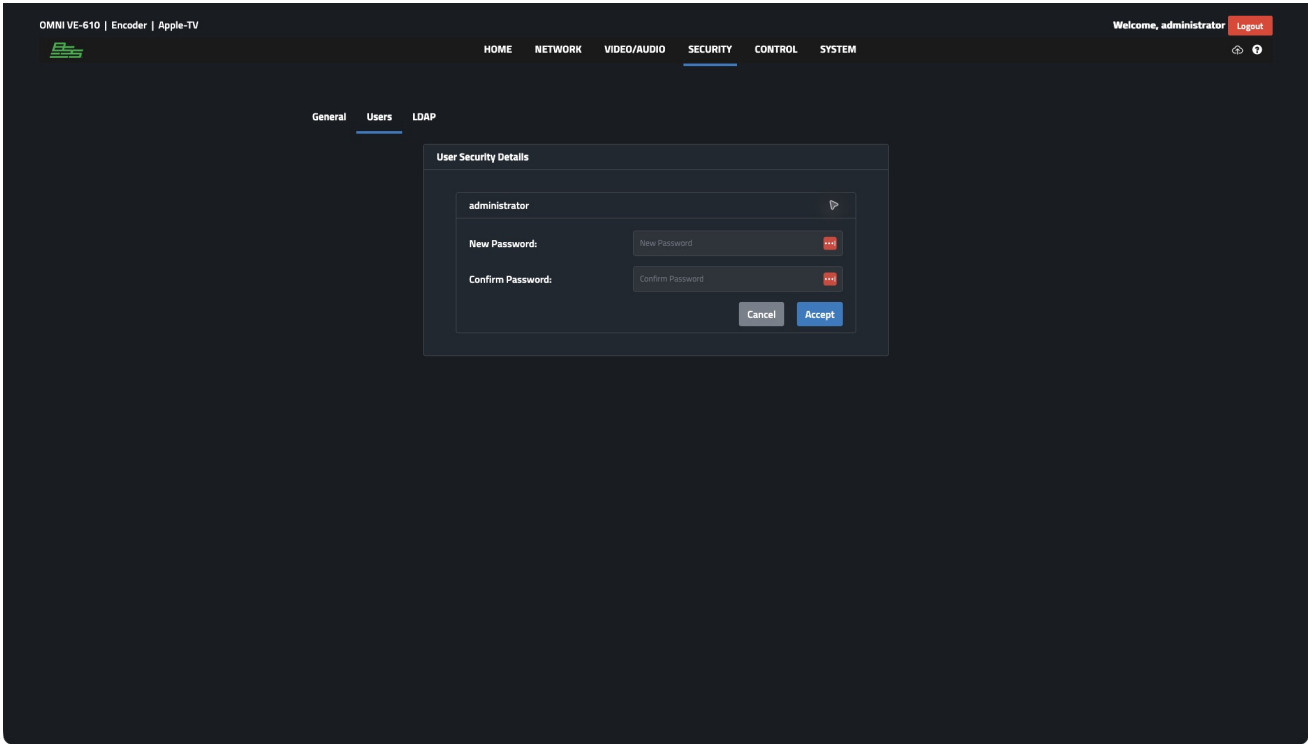


Figure 6-2. VE-610 administrator password controls

Controls and indicators

Control / area	Purpose and operator guidance
Administrator	Expands the current administrator account.
New / Confirm Password	Sets and confirms the replacement credential.
Accept	Commits the credential change.

Recommended workflow

1. Open an approved credential manager.
2. Set a unique password that meets site policy.
3. Accept the change, sign out, and sign back in.
4. Update the controlled credential record only after successful verification.

CRITICAL: Do not end the maintenance session until the new credential has been tested successfully.

6.3 VE-610 Security — LDAP

LDAP integrates central directory authentication and supports certificate configuration for secure directory access.

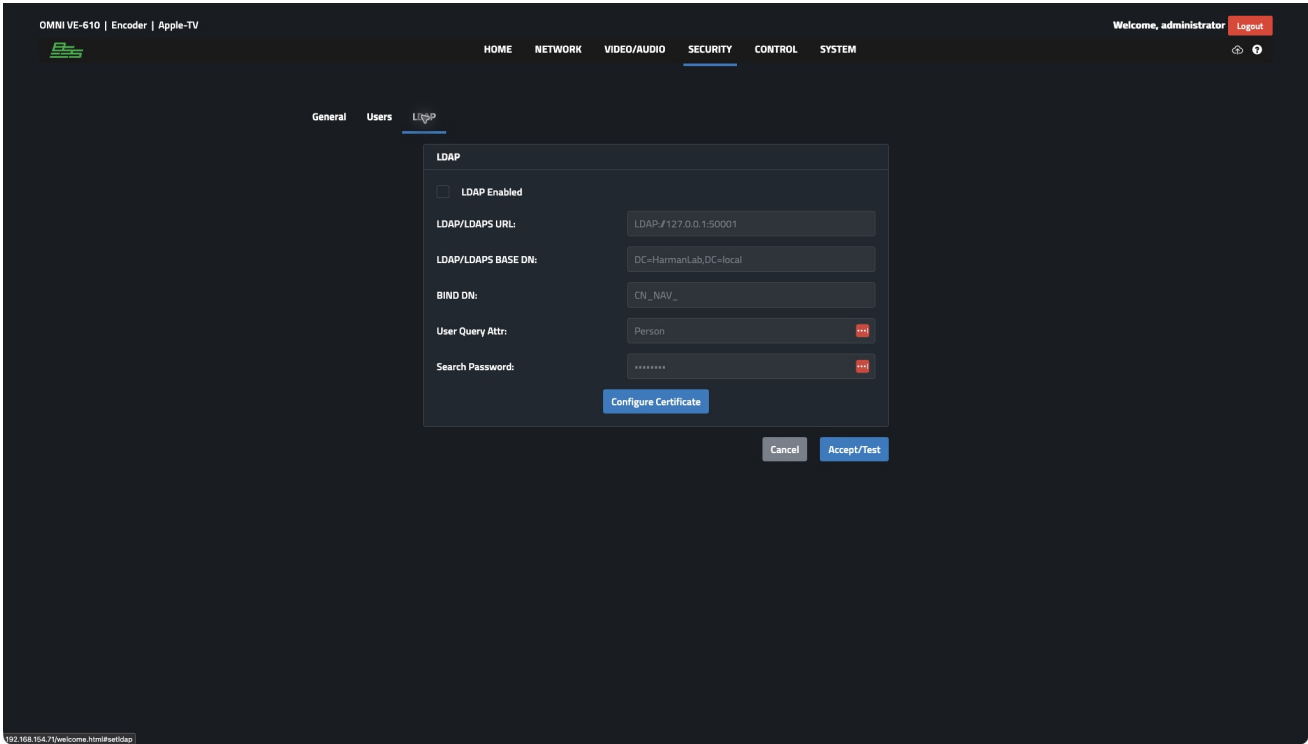


Figure 6-3. VE-610 LDAP configuration

Controls and indicators

Control / area	Purpose and operator guidance
LDAP Enabled	Activates directory authentication.
LDAP/LDAPS URL	Defines scheme, host, and port.
Base DN / Bind DN	Sets search base and bind identity.
User Query Attr	Defines the login lookup attribute.
Search Password	Credential for the bind identity.
Configure Certificate	Installs the trust material used by LDAPS.
Accept/Test	Tests and stages the directory configuration.

Recommended workflow

1. Prefer LDAPS and a least-privilege bind identity.
2. Install the trusted CA certificate.
3. Enter URL, DNS, query attribute, and managed secret.
4. Use Accept/Test and verify both directory and local recovery access before enabling.

6.4 VD-610 Security — General

The physical decoder exposes HTTPS, secure-control, command/stream password, and certificate controls.

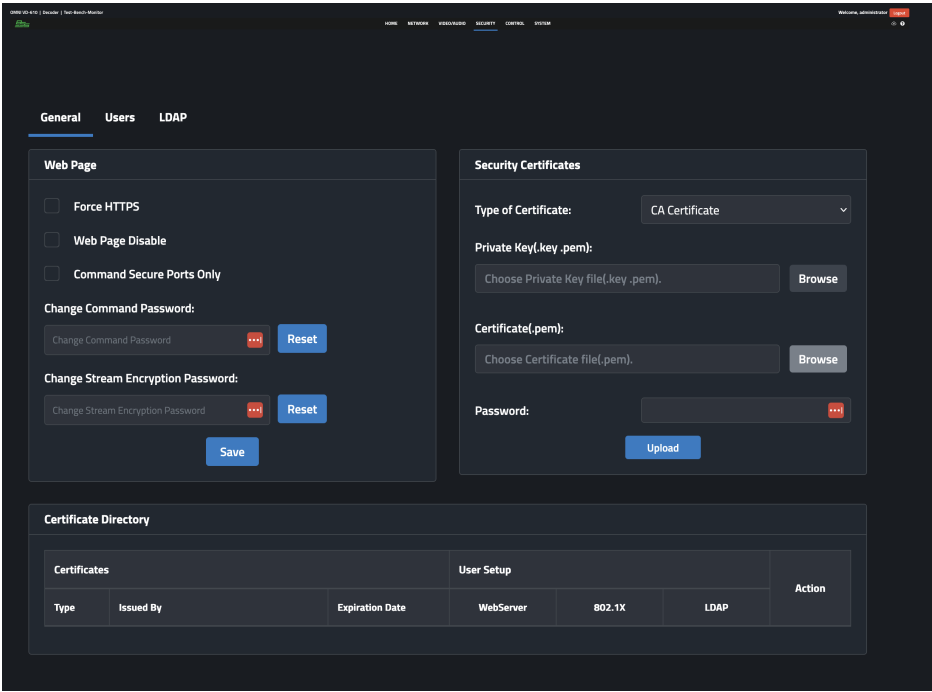


Figure 6-4. Physical VD-610 Security General and certificate directory

Controls and indicators

Control / area	Purpose and operator guidance
Force HTTPS / Web Page Disable	Controls secure Web access and whether the Web UI remains available.
Command Secure Ports Only	Restricts control to secure ports.
Command / Stream passwords	Changes or resets protected-service credentials.
Certificate upload	Stages CA, private key, certificate, and optional password.
Certificate directory	Shows certificate identity, expiry, assignment, and actions.

Recommended workflow

1. Correct device time, DNS, and hostname.
2. Install approved certificate material.
3. Test HTTPS and secure control before enforcing secure-only modes.
4. Retain a documented recovery method.

PRIVATE KEYS: Never include certificate private keys or passwords in screenshots, tickets, or this manual.

6.5 VD-610 Security — Users

The Users tab changes the decoder administrator password.

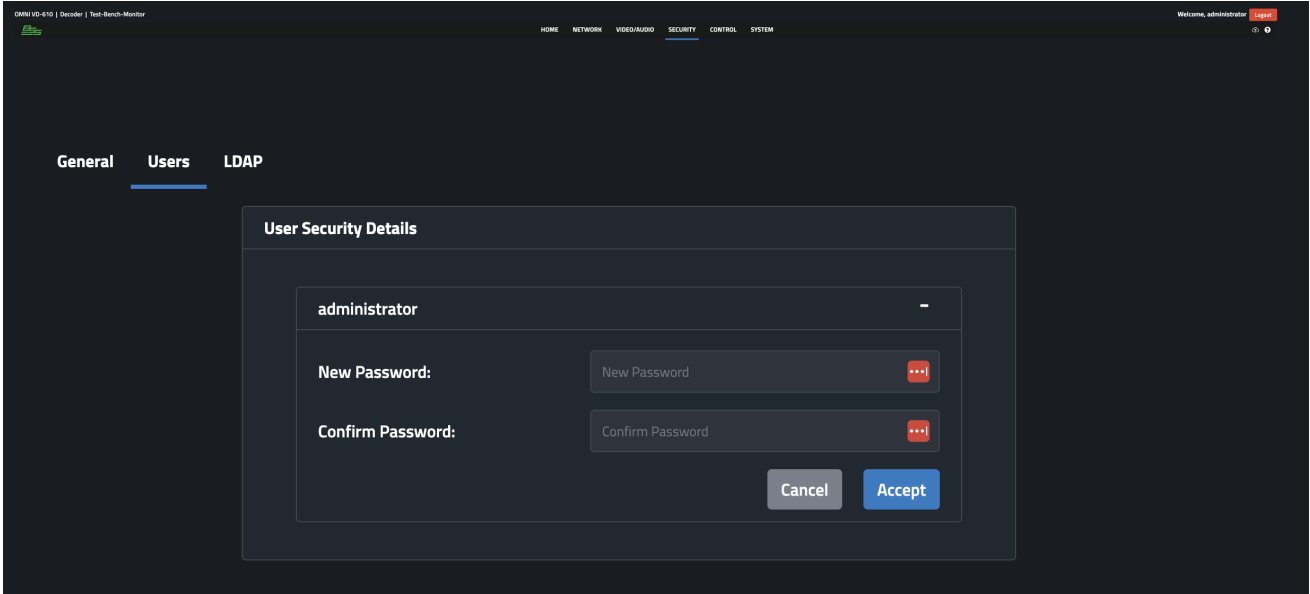


Figure 6-5. Physical VD-610 administrator password controls

Controls and indicators

Control / area	Purpose and operator guidance
Administrator	Expands the administrator account.
New / Confirm Password	Sets and confirms the replacement credential.
Accept	Commits the credential change.

Recommended workflow

1. Open the approved credential manager.
2. Set a unique policy-compliant password.
3. Accept, sign out, and sign back in.
4. Update the controlled record after successful verification.

CRITICAL: Do not end the maintenance session until the new credential has been tested successfully.

6.6 VD-610 Security — LDAP

The decoder LDAP tab supports directory authentication and certificate configuration for secure directory access.

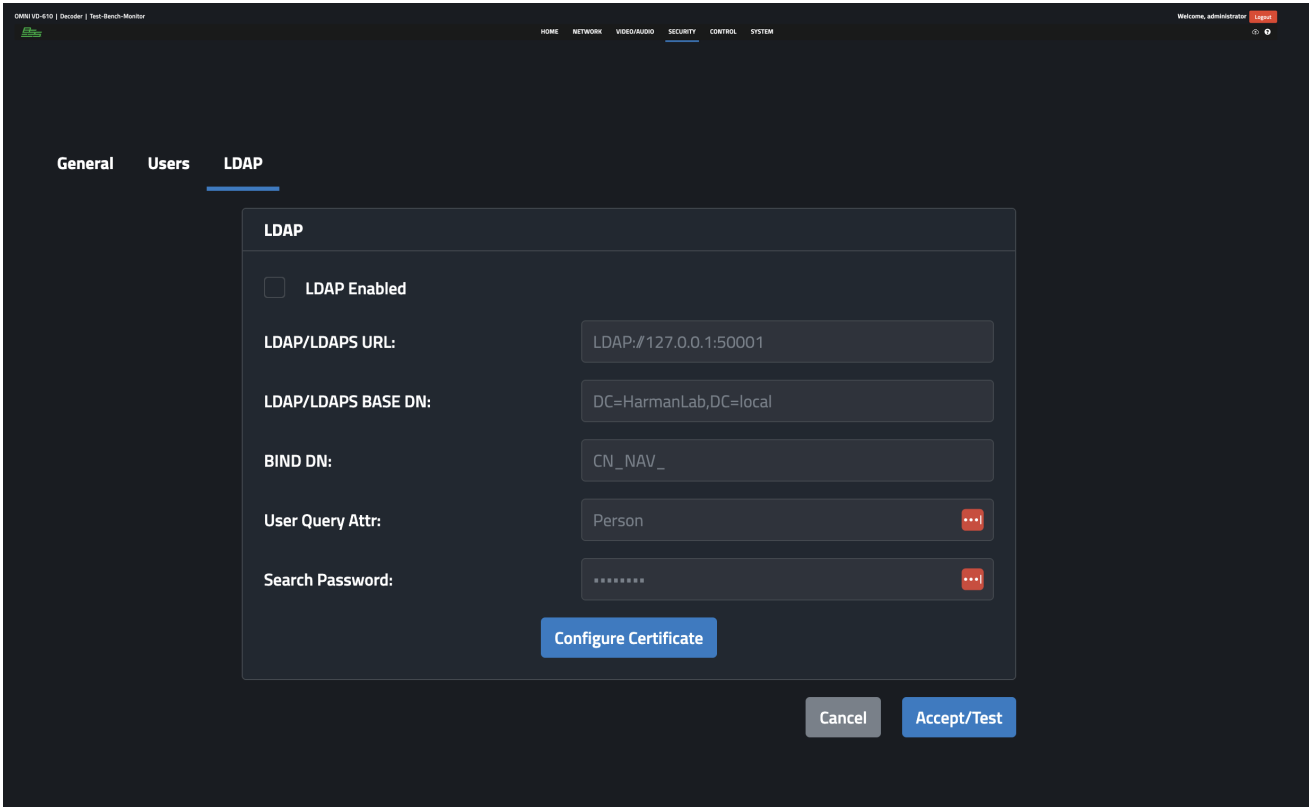


Figure 6-6. Physical VD-610 LDAP configuration

Controls and indicators

Control / area	Purpose and operator guidance
LDAP Enabled	Activates directory authentication.
LDAP/LDAPS URL	Defines scheme, host, and port.
Base DN / Bind DN	Sets the search base and bind identity.
User Query Attr	Defines the login lookup attribute.
Search Password	Protected credential for the bind identity.
Configure Certificate / Accept-Test	Installs trust material and tests the configuration.

Recommended workflow

1. Prefer LDAPS and a least-privilege bind identity.
2. Install the trusted CA certificate.
3. Enter directory values and the managed secret.
4. Test directory and local recovery access before enabling.

7. Control: Serial and NAV-React

7.1 VE-610 Serial

Serial provides stored commands, execution controls, RS-232 framing, and secondary-address configuration.

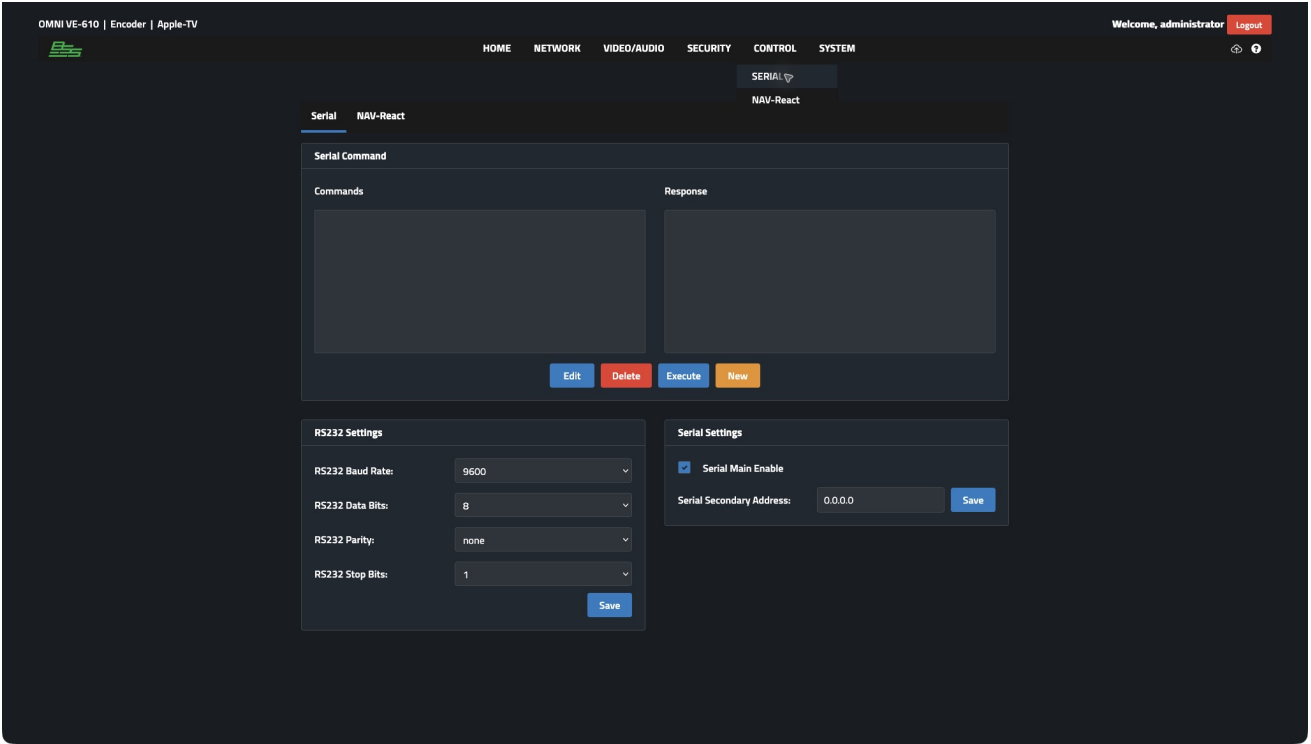


Figure 7-1. VE-610 Serial Command and RS-232 settings

Controls and indicators

Control / area	Purpose and operator guidance
Command table	Stores command/response definitions.
Edit / Delete / Execute / New	Manages and runs selected commands.
Baud / Data / Parity / Stop	Defines RS-232 framing.
Serial Main Enable	Enables the primary serial service.
Serial Secondary Address	Sets the peer/secondary service address.

Recommended workflow

1. Match the controlled device's framing exactly.
2. Create one documented command and expected response.
3. Execute only while observing the target.
4. Enable and verify secondary routing if required.

7.2 VE-610 NAV-React

Encoder NAV-React events include power and video-cable triggers, delay, multiple protocol types, testing, and import/export.

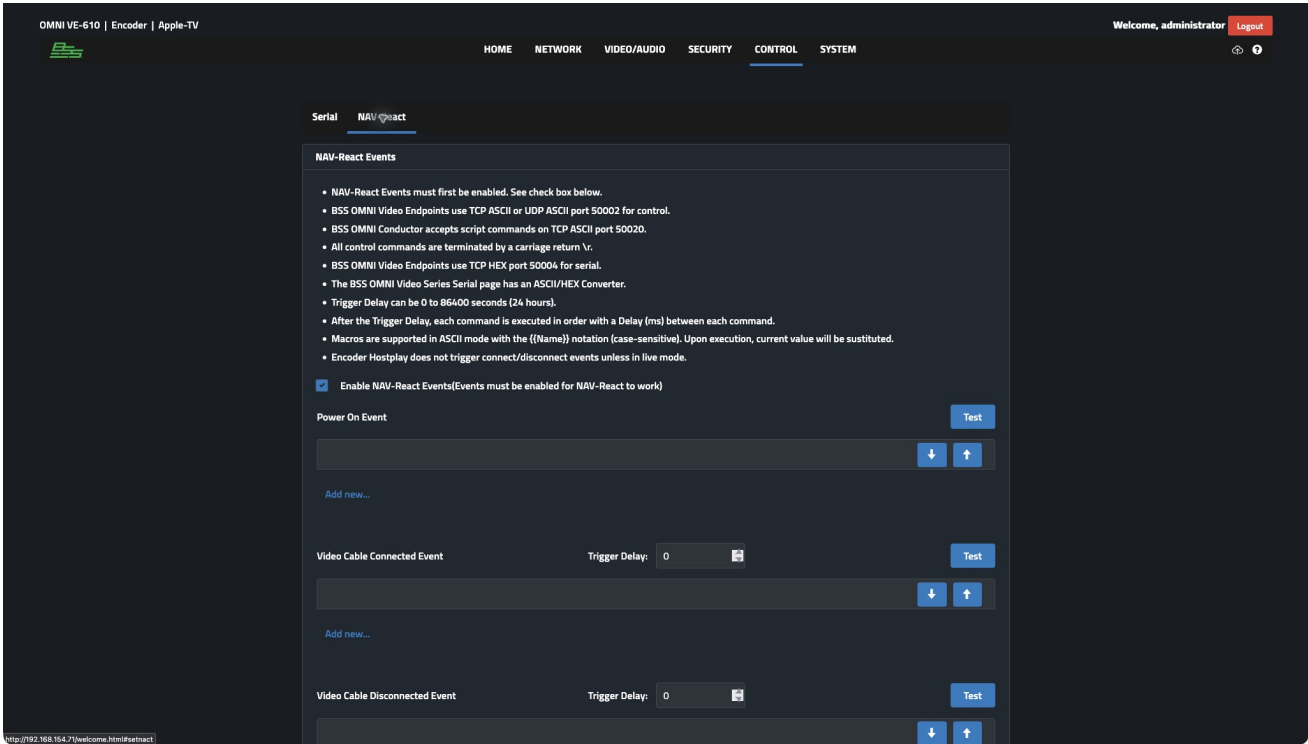


Figure 7-2. VE-610 NAV-React event editor

Controls and indicators

Control / area	Purpose and operator guidance
Enable	Globally enables events.
Power / Video Cable events	Trigger actions on encoder state changes.
Protocols	TCP/UDP ASCII port 50002, Conductor TCP 50020, and TCP HEX port 50004 where offered.
Trigger Delay	Defers execution from 0 to 86400 seconds.
Hostplay events	Apply only while Play Mode is Live, as noted in the UI.

Recommended workflow

1. Build actions with events disabled.
2. Use the converter for validated HEX payloads when required.
3. Test against a controlled destination.
4. Save and enable one trigger at a time.

CONTROL SAFETY: A Test action can operate external equipment immediately.

7.3 VD-610 Serial

The physical decoder contains a command table, execution controls, RS-232 framing, and main/secondary serial routing.

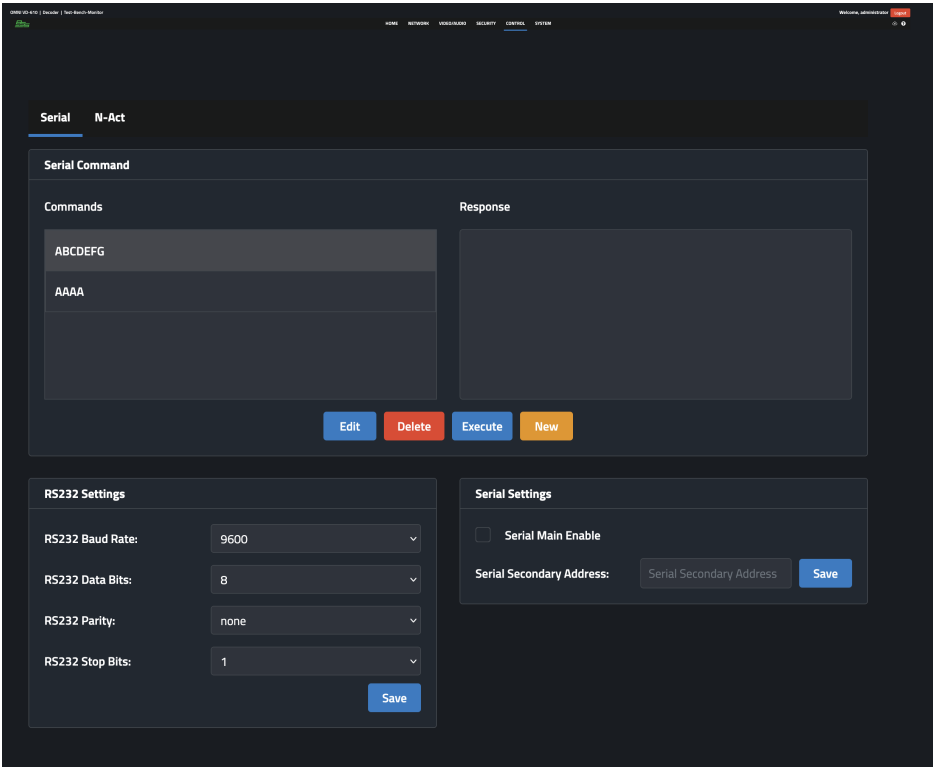


Figure 7-3. Physical VD-610 Serial controls

Controls and indicators

Control / area	Purpose and operator guidance
Command / Response	Stores selected command and response definitions.
Edit / Delete / Execute / New	Manages and runs the selected entry.
RS232 Settings	Sets baud, data bits, parity, and stop bits.
Serial Main Enable / Secondary Address	Enables routing and identifies the secondary endpoint.

Recommended workflow

- 1. Match the controlled device's framing exactly.
- 2. Create and test one command at a time.
- 3. Document all payloads and expected responses.

7.4 VD-610 N-Act

The decoder event editor provides power, video-cable, and generic triggers plus import/export.

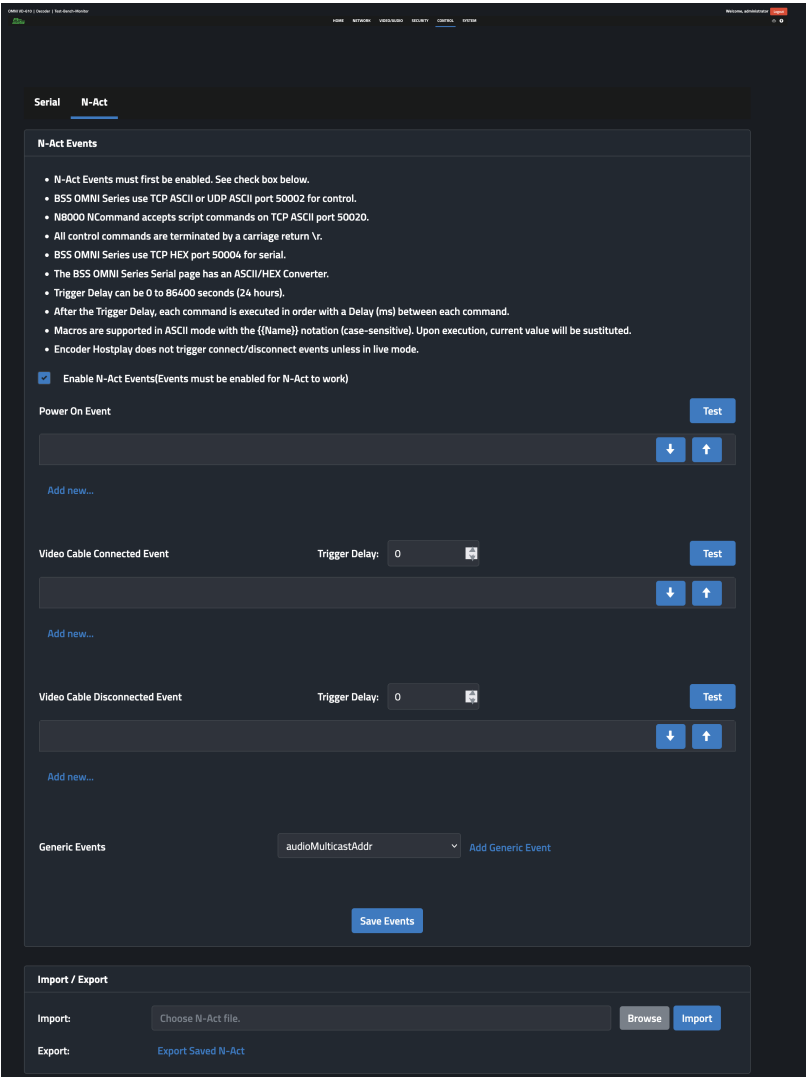


Figure 7-4. Physical VD-610 N-Act event editor

Controls and indicators

Control / area	Purpose and operator guidance
Enable N-Act Events	Globally enables event processing.
Power / Video Cable events	Decoder-specific triggers with ordered actions.
Trigger Delay / Test	Defers or exercises a configured action.
Generic Events	Adds a selected reusable event type.
Import / Export	Loads or saves the N-Act definition.

Recommended workflow

1. Build actions while global events are disabled.
2. Validate destinations, ports, carriage-return termination, and delay.
3. Use Test only against a controlled target because it can operate external equipment immediately.
4. Save, export a backup, and enable one trigger at a time.

8. System logs and status

8.1 VE-610 Logs

The encoder log page provides command history, temporary debug logging, and remote syslog settings.

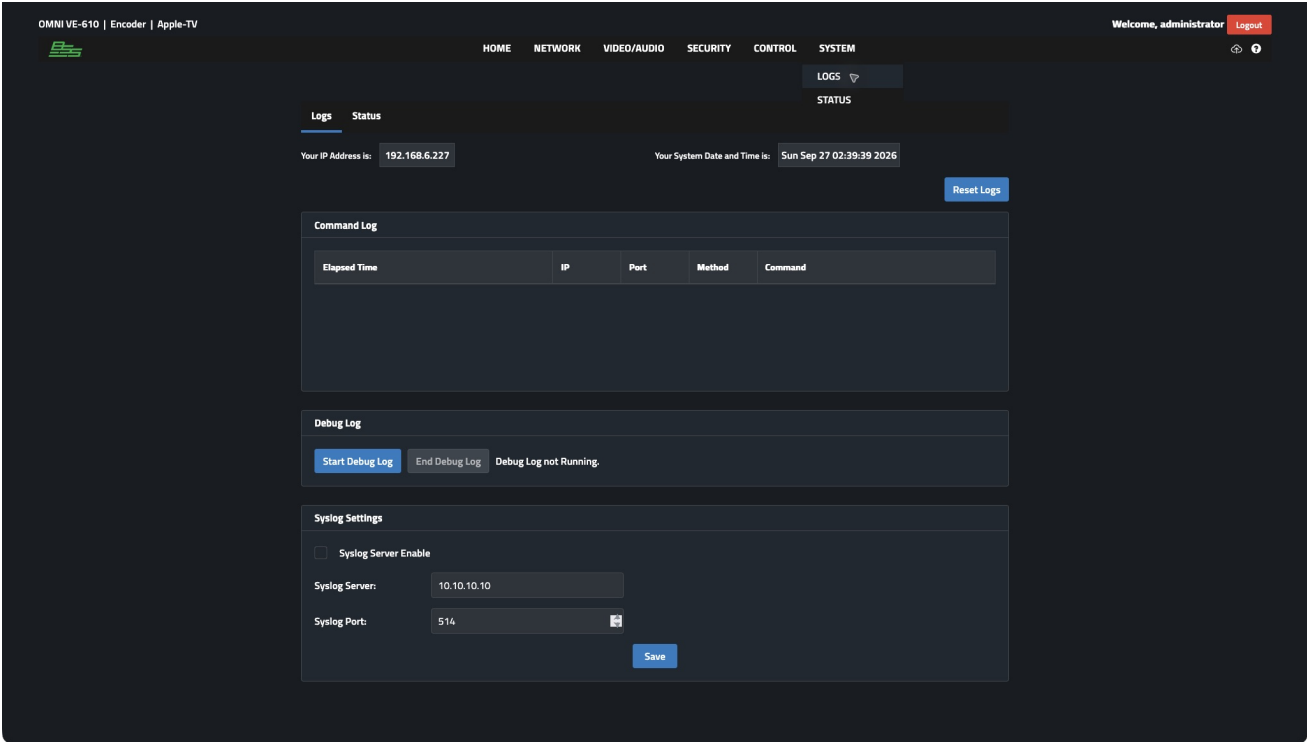


Figure 8-1. VE-610 Logs and Syslog Settings

Controls and indicators

Control / area	Purpose and operator guidance
Command Log	Elapsed time, source IP, port, method, and command.
Reset Logs	Clears available log history.
Debug Log	Starts and ends detailed temporary capture.
Syslog	Enables centralized logging to a server and port.

Recommended workflow

1. Verify time and preserve current evidence.
2. Start debug logging only for a controlled reproduction.
3. End capture promptly.
4. Use syslog for persistent operations monitoring.

EVIDENCE: Do not reset logs before the incident record is preserved.

8.2 VE-610 Status

The live encoder status page consolidates HDMI, control ports, serial, network, audio, LLDP, identity, firmware, and maintenance controls.

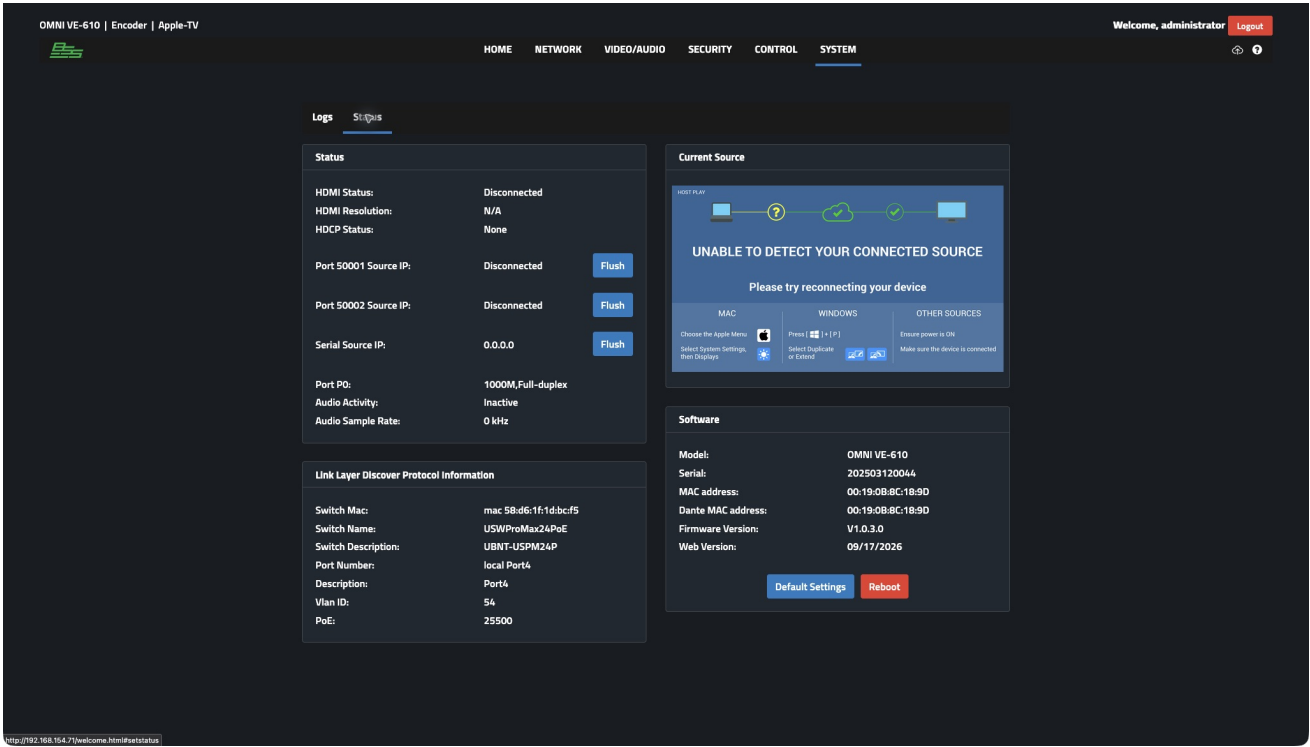


Figure 8-2. VE-610 live System Status

Controls and indicators

Control / area	Purpose and operator guidance
HDMI	Connection, resolution, and HDCP state.
Control ports	Port 50001 and 50002 connection status.
Serial source	Current serial peer address.
P0 / audio / LLDP	Link, audio activity/sample rate, and switch discovery.
Identity	Model, serial, MAC, firmware, and Web build.
Default Settings / Reboot	Disruptive maintenance actions.

Recommended workflow

- 1. Confirm identity.
- 2. Check HDMI, stream, audio, and control-port state.
- 3. Review link and LLDP information.
- 4. Capture the page before reboot or reset.

8.3 VD-610 Logs

The physical decoder log page provides command history, temporary debug logging, and remote syslog settings.

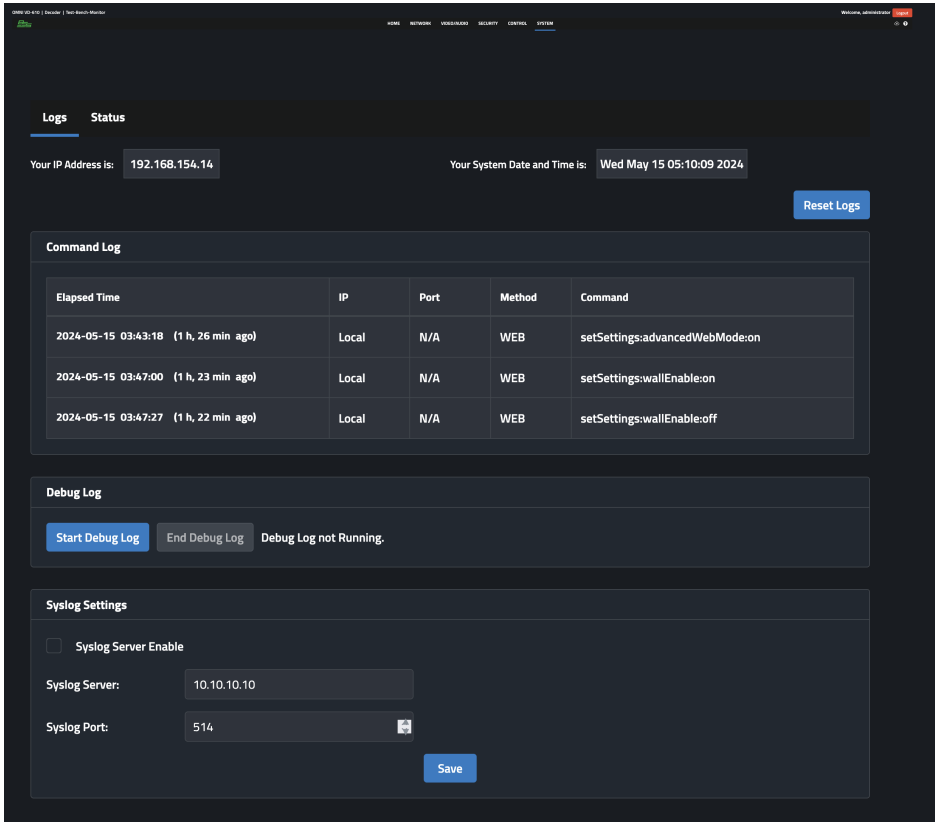


Figure 8-3. Physical VD-610 Logs and Syslog Settings

Controls and indicators

Control / area	Purpose and operator guidance
Command Log	Elapsed time, source IP, port, method, and command.
Reset Logs	Clears available command history.
Debug Log	Starts and ends detailed temporary capture.
Syslog	Sets the remote server and UDP port.

Recommended workflow

- 1. Verify time and preserve current evidence.
- 2. Start debug capture only for a controlled reproduction.
- 3. End capture promptly and preserve the output.
- 4. Configure syslog for persistent monitoring when required.

EVIDENCE: Do not reset logs before the incident record is preserved.

8.4 VD-610 Status

The physical decoder status page consolidates HDMI output, control and serial peers, network/audio state, LLDP, identity, firmware, and maintenance actions.

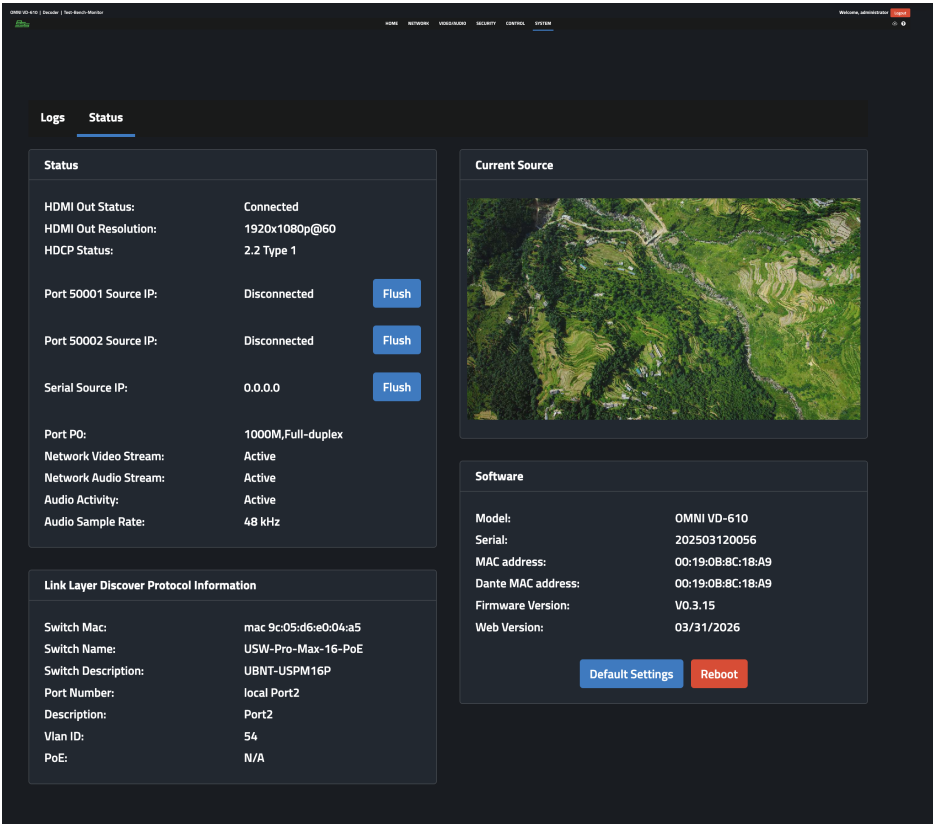


Figure 8-4. Physical VD-610 System Status; firmware V0.3.15 / Web 03/31/2026

Controls and indicators

Control / area	Purpose and operator guidance
HDMI Out	Connection, resolution, and HDCP state.
Control / Serial source IP	Current peers with flush actions.
P0 / stream / audio	Link, video/audio stream state, activity, and sample rate.
LLDP	Switch MAC, name, port, VLAN, and PoE information.
Software	Model, serial, MAC, Dante MAC, firmware, and Web build.
Default Settings / Reboot	Disruptive maintenance actions.

Recommended workflow

- 1. Confirm device identity.
- 2. Check HDMI, streams, audio, and control peers.
- 3. Review link and LLDP information.
- 4. Capture the page before reboot or reset.

DISRUPTIVE: Reboot interrupts service; Default Settings may remove network and security configuration.

9. Routine workflows and troubleshooting

9.1 Commission a VE/VD route

1. Record encoder and decoder identity, firmware, IP, and current stream values.
2. Apply approved management and Dante network settings.
3. Set correct date/time and validate security prerequisites.
4. Assign the VE-610 transmit stream and the VD-610 receive stream.
5. Configure HDCP, EDID, audio, wall, and playlist behavior as required.
6. Verify HDMI/source/output status, audio, multicast, and control ports.
7. Add Serial or NAV-React automation one action at a time.
8. Change the lab/default credential and complete the security baseline.

9.2 If video is absent

- Confirm VE TX Enable, VD receive source, and matching stream values.
- Check source HDMI state, resolution, and HDCP on the VE-610.
- Check output HDMI state, resolution, and HDCP on the VD-610.
- Verify IGMP/VLAN/multicast routing and any multicast override.
- Restore a known-good EDID and retest before rebooting.

9.3 If audio is absent

- Check Dante Audio Disable and mute states on both endpoints.
- Verify VD audio source, Audio follows Video, downmix, and local-play settings.
- Confirm Dante VLAN, IP, discovery, and sample-rate/status information.
- Test one known-good source and output path.

9.4 If management access is lost

- Check physical link, address/VLAN, and 802.1X authentication state.
- Confirm the last known IP, certificate/HTTPS policy, and user credential.
- Use a local recovery path before Default Settings.
- Preserve network and identity records for the service report.