



Operational guide for the USB over IP Host and Device Transceivers.

IMPORTANT: Changing IP, USB routing, 802.1X, certificate, password, reboot, or default settings can interrupt service. Record the current configuration and schedule a maintenance window before applying changes.

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 HTTPS-only Security pages require certificate trust on each individual endpoint. The user-supplied Security figures identify a real OMNI UD-210WP on firmware V0.3.7 / Web 04/02/2026; verify labels against the currently installed firmware before applying changes.

Table of contents

Section	Contents
1	Product and capture overview
2	Accessing the Web UI
3	Home and stream setup
4	Network configuration
5	Control and NAV-React
6	System logs and status
7	Security and administration
8	Routine workflows and troubleshooting

1. Product and capture overview

The Ux-210 family transports USB and control services over IP. The UE-210 operates as the USB host-side transceiver; the UD-210 family operates on the USB device/peripheral side. The live decoder used for this manual identifies itself as OMNI UD-210WP, so wallplate-specific labeling is preserved in the figures.

Operational safety and administration

- Confirm that a proposed static address is unused before selecting Accept.
- Keep the service computer connected by a path that will remain valid after an IP or VLAN change.
- Do not enable 802.1X until the switch, identity, certificate, and rollback plan are ready.
- Treat Default Settings, Reboot, password, certificate, and Settings Lock actions as maintenance-window operations.
- Export or record device identity, stream, IP, USB, and control settings before making a broad change.

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.

Model	Capture address	Role
UE-210	192.168.154.68	USB host
UD-210-WP	192.168.154.62	USB device / wallplate

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. For a self-signed certificate warning, verify the address and certificate fingerprint according to site policy; do not train operators to dismiss warnings without validation.

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 UE-210 Home

The UE-210 Home page binds the host endpoint to a USB stream and provides USB-source and management controls.

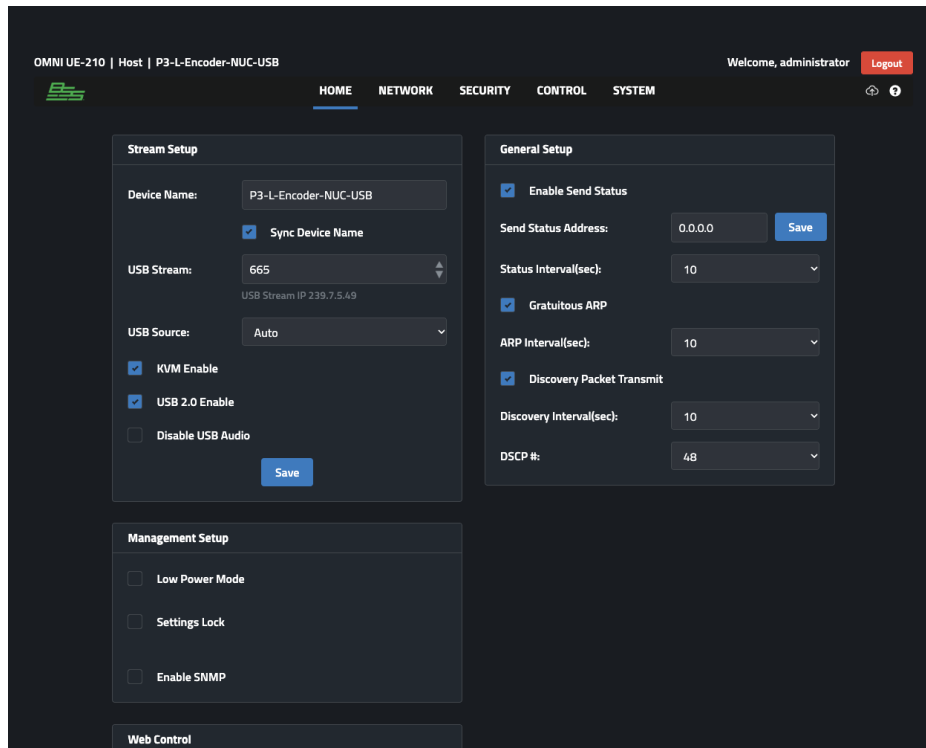


Figure 3-1. Live UE-210 Home page and stream setup

Controls and indicators

Control / area	Purpose and operator guidance
Device Name / Sync	Names the endpoint and optionally synchronizes the configured name.
USB Stream	Selects the USB-over-IP stream; the interface displays the derived multicast address.
USB Source	Chooses Auto, USB-C, or USB-B host input behavior.
KVM Enable / USB 2.0 Enable	Enables the associated USB transport services.
Disable USB Audio	Suppresses USB audio when checked.
Management Setup	Low Power, Settings Lock, and SNMP controls.
General Setup	Status destination, intervals, gratuitous ARP, discovery, and DSCP marking.

Recommended workflow

1. Verify the banner shows UE-210 and Host.
2. Select the intended USB stream and source.
3. Set KVM, USB 2.0, and USB audio behavior.
4. Select Save in the affected panel and verify the displayed stream/IP values.

CAUTION: Settings Lock can prevent further edits. Confirm recovery credentials and the intended final configuration before enabling it.

3.2 UD-210-WP Home

The decoder-side Home page assigns the peripheral endpoint to its USB stream and provides device-side KVM, USB, and management behavior.

The screenshot displays the 'HOME' page of the UD-210-WP device interface. The top navigation bar includes 'HOME', 'NETWORK', 'SECURITY', 'CONTROL', and 'SYSTEM'. The main content area is divided into three sections:

- Stream Setup:** Contains fields for 'Device Name' (P3-L-Decoder-PTZ1), a checked 'Sync Device Name' checkbox, 'USB Stream' (210), and a 'USB Stream IP' (239.7.1.163). It also has checkboxes for 'KVM Enable' and 'USB 2.0 Enable', and a 'Save' button.
- General Setup:** Contains several settings: 'IGMP Join on Stream Loss' (checked), 'IGMP Join Interval' (2), 'Enable Send Status' (checked), 'Send Status Address' (0.0.0.0) with a 'Save' button, 'Status Interval(sec)' (10), 'Gratuitous ARP' (checked), 'ARP Interval(sec)' (10), 'Discovery Packet Transmit' (checked), 'Discovery Interval(sec)' (10), and 'DSCP #' (48).
- Management Setup:** Contains checkboxes for 'Low Power Mode' and 'Settings Lock'.

Figure 3-2. Live UD-210-WP Home page and stream setup

Controls and indicators

Control / area	Purpose and operator guidance
Device Name / Sync	Identifies the device-side endpoint.
USB Stream	Must match the intended host-side route.
KVM Enable / USB 2.0 Enable	Enables the device-side KVM and USB 2.0 paths.
Management Setup	Low Power, Settings Lock, and SNMP.
IGMP Join on Stream Loss	Controls continued multicast membership behavior when the stream is absent.
General Setup	Status reporting, ARP, discovery, and DSCP values.

Recommended workflow

1. Verify the banner identifies the intended UD-210/UD-210-WP.
2. Enter the USB stream that corresponds to the desired UE-210.
3. Confirm KVM and USB 2.0 requirements.
4. Save and then confirm USB status under System > Status.

VERIFY: A matching stream number is necessary but not sufficient; verify the complete USB path and endpoint status after saving.

4. Network configuration

4.1 UE-210 IP Setup

Use IP Setup to configure the host name, DNS, IGMP version, IPv4 method, gateway, and IPv6 behavior.

Figure 4-1. UE-210 IP Setup

Controls and indicators

Control / area	Purpose and operator guidance
Hostname / Domain	Sets the management identity and DNS suffix.
Manual DNS	Enables explicit DNS server entries.
IGMP v3 Support	Enables IGMPv3 behavior when required by the multicast design.
DHCP / Static IP Address	Selects automatic or manual IPv4 addressing.
IPv6 Enable / Disable	Controls IPv6 availability.
Cancel / Accept	Discards or applies the pending page values.

Recommended workflow

1. Record the current address, mask, gateway, DNS, and hostname.
2. Validate the proposed address against the network plan.
3. Choose DHCP or Static and enter the complete set of required values.
4. Select Accept once, then reconnect using the new address and verify reachability.

NETWORK SAFETY: An incorrect gateway, mask, or duplicate IP can make the endpoint unreachable. Maintain a local recovery path.

4.2 UD-210-WP IP Setup

The UD-210-WP page provides the same core management-address controls for the device-side endpoint.

Figure 4-2. UD-210-WP IP Setup

Controls and indicators

Control / area	Purpose and operator guidance
Hostname / Domain	Defines the device-side management identity.
DNS servers	Used when hostnames are required for services such as NTP or LDAP.
IGMP v3	Must align with the network multicast design.
IPv4 / IPv6	Controls management addressing for the endpoint.

Recommended workflow

1. Document the current configuration.
2. Apply the approved device-side address plan.
3. Reconnect to the new address.
4. Verify the banner and System Status identity before continuing.

4.3 UE-210 Date/Time and NTP

Correct time is essential for diagnostics, certificate validation, and correlated logs.

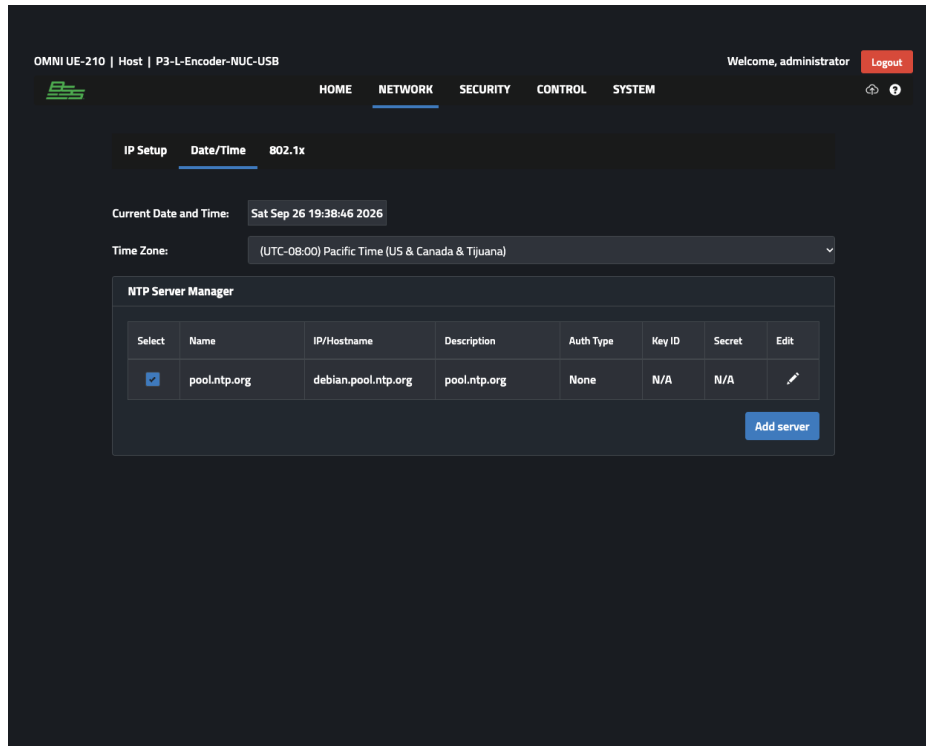


Figure 4-3. UE-210 Date/Time and NTP server manager

Controls and indicators

Control / area	Purpose and operator guidance
Current Date and Time	Read-only device time.
Time Zone	Selects the local display time zone.
NTP Server Manager	Adds, edits, selects, or removes NTP sources and optional authentication.

Recommended workflow

1. Choose the site time zone.
2. Confirm that the configured NTP hostname is resolvable through DNS.
3. Add or edit the approved server and authentication values.
4. Verify that device time converges and remains correct.

4.4 UD-210-WP Date/Time and NTP

Configure decoder-side timekeeping to the same site standard as the host endpoint.

The screenshot shows the web interface for the OMNI UD-210WP device, specifically the 'Date/Time' configuration page under the 'NETWORK' tab. The page displays the current date and time as 'Sun Sep 27 10:30:26 2026' and the time zone as '(UTC) Greenwich Mean Time (Dublin & Edinburgh & Lisbon & London)'. Below this is the 'NTP Server Manager' section, which contains a table with one entry for 'pool.ntp.org'. The table has columns for Select, Name, IP/Hostname, Description, Auth Type, Key ID, Secret, and Edit. An 'Add server' button is located at the bottom right of the table.

Select	Name	IP/Hostname	Description	Auth Type	Key ID	Secret	Edit
☐	pool.ntp.org	debian.pool.ntp.org	pool.ntp.org	None	N/A	N/A	

[Add server](#)

Figure 4-4. UD-210-WP Date/Time and NTP server manager

Controls and indicators

Control / area	Purpose and operator guidance
Time Zone	Controls local display offset.
NTP entries	Define name, host, description, authentication type, key ID, and secret as applicable.

Recommended workflow

1. Use the same approved time source set as the rest of the AV network.
2. Avoid exposing NTP secrets in screenshots or change records.
3. Confirm correct time before troubleshooting event order.

4.5 UE-210 802.1X

The 802.1X page configures port-based network authentication. Fields remain disabled until authentication is enabled.

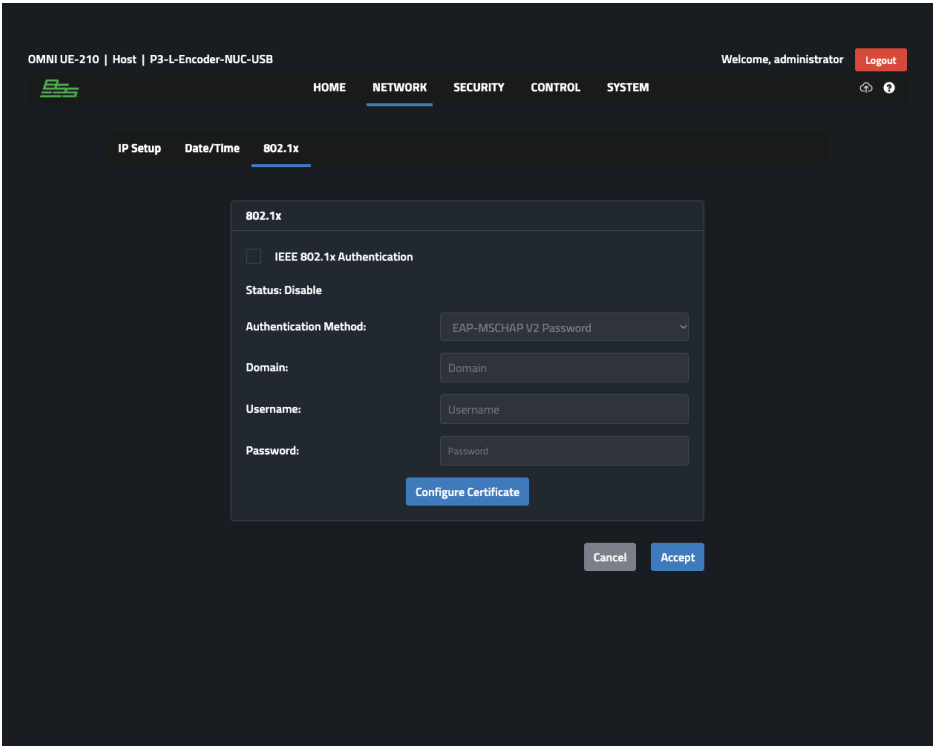


Figure 4-5. UE-210 IEEE 802.1X authentication

Controls and indicators

Control / area	Purpose and operator guidance
IEEE 802.1X Authentication	Enables or disables endpoint authentication.
Status	Shows the current authentication state.
Authentication Method	Provides EAP-MSCHAP V2 Password or EAP-TLS Certificate.
Domain / Username / Password	Identity values for password-based authentication.
Configure Certificate	Installs or selects the EAP-TLS certificate material.

Recommended workflow

- 1. Coordinate with the network administrator and stage the switch policy.
- 2. Install and validate the CA/client certificate before choosing EAP-TLS.
- 3. Enter the approved identity or certificate method.
- 4. Enable authentication and select Accept only with a rollback path available.

LOCKOUT RISK: A mismatched method, identity, certificate, or switch policy can remove network access immediately.

4.6 UD-210-WP 802.1X

The device-side 802.1X page mirrors the host-side authentication workflow.

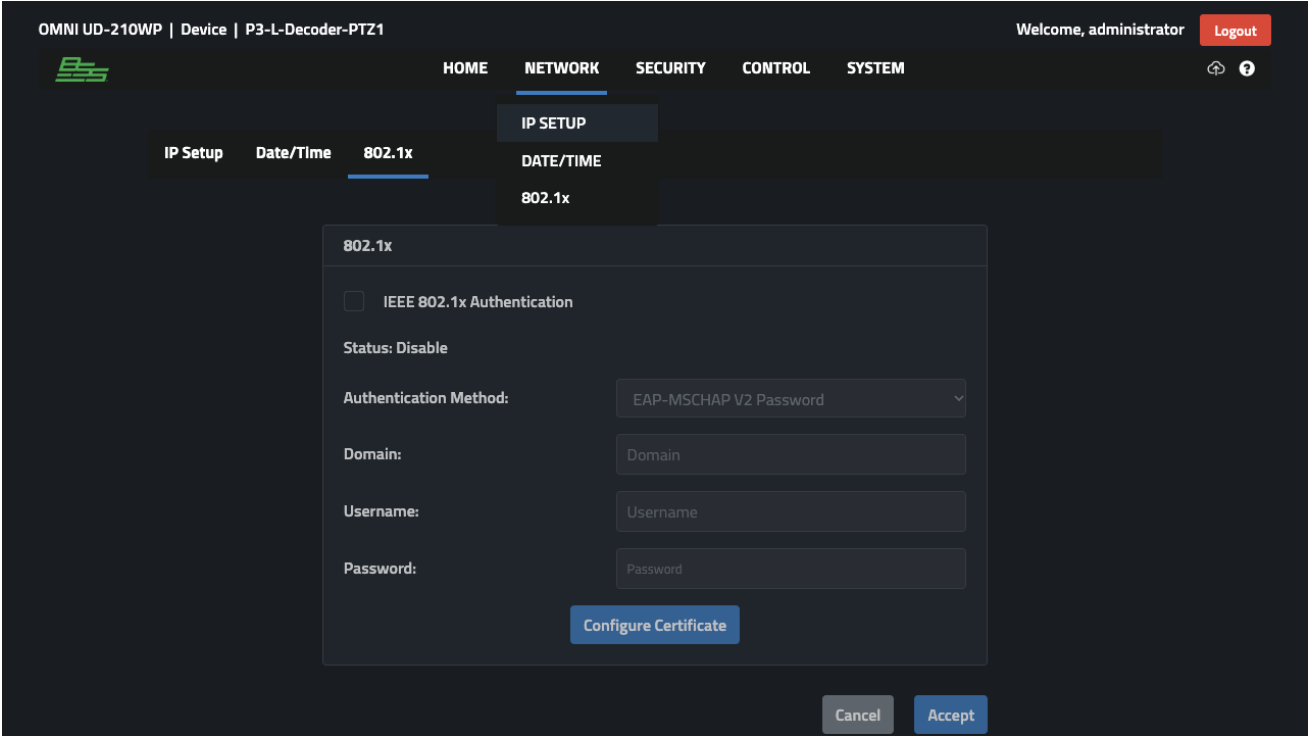


Figure 4-6. UD-210-WP IEEE 802.1X authentication

Controls and indicators

Control / area	Purpose and operator guidance
Enable	Activates port authentication.
Method	Selects password or certificate authentication.
Configure Certificate	Manages the certificate used by EAP-TLS.
Accept	Applies the staged authentication configuration.

Recommended workflow

1. Prepare switch and identity-service policy first.
2. Validate certificate dates, trust chain, and device time.
3. Apply during a staffed maintenance window.
4. Confirm the endpoint authenticates and remains reachable.

5. Control and NAV-React

5.1 UE-210 NAV-React

NAV-React maps device events to outbound control actions. The UE-210 page includes power and USB cable triggers plus generic events.

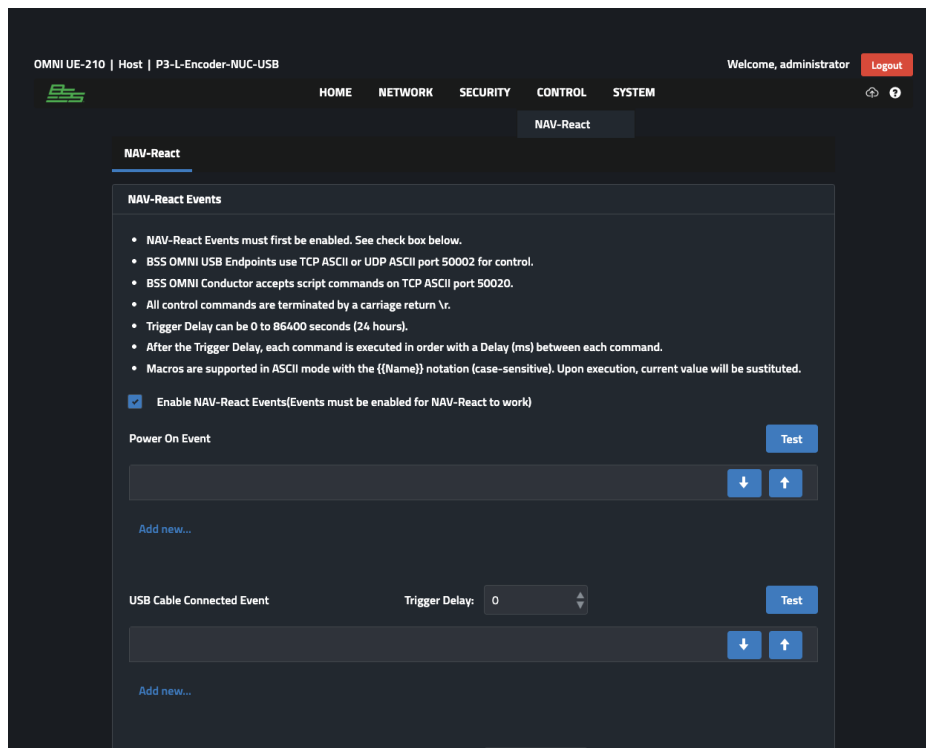


Figure 5-1. UE-210 NAV-React event editor

Controls and indicators

Control / area	Purpose and operator guidance
Enable NAV-React Events	Globally enables configured actions.
Power On / USB Cable events	Trigger when the named device condition occurs.
Trigger Delay	Defers action execution; accepted range shown in the UI is 0–86400 seconds.
Add new / Test / Save Events	Creates, dry-runs, and stores actions.
Import / Export	Moves event definitions between compatible configurations.
Generic Events	Supports reusable events; the UE page includes a stream event option.

Recommended workflow

1. Create one event with a descriptive name and explicit destination.
2. Set protocol and port; TCP/UDP ASCII control uses port 50002 and commands require carriage-return termination.
3. Use Test while monitoring the target system.
4. Save, enable events, and verify the trigger under controlled conditions.

CONTROL SAFETY: Test actions can affect external equipment. Use a non-production target or a coordinated maintenance window.

5.2 UD-210-WP NAV-React

The UD-210-WP uses the same event framework with device-side cable triggers and generic events.

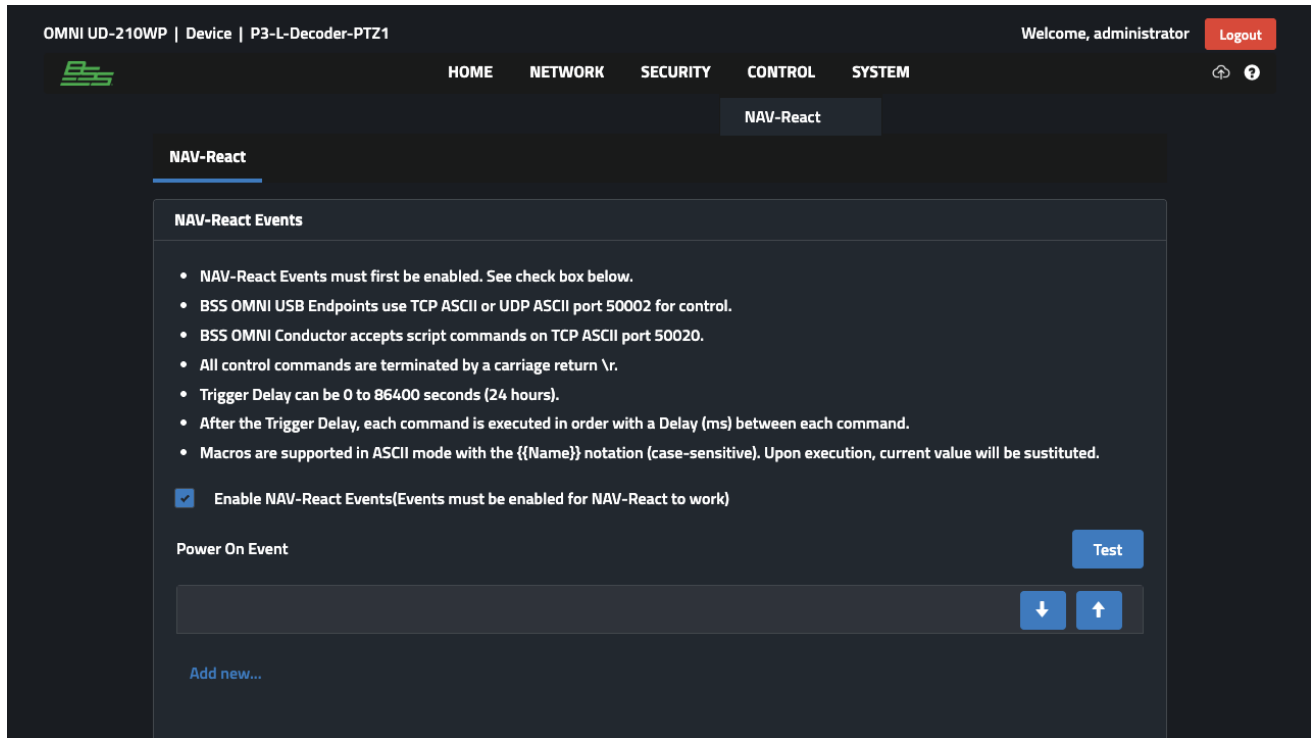


Figure 5-2. UD-210-WP NAV-React event editor

Controls and indicators

Control / area	Purpose and operator guidance
Event groups	Power On, USB cable connected/disconnected, and generic events.
Protocols	TCP ASCII, UDP ASCII, and compatible control action types offered by the UI.
Import / Export	Backs up or transfers event definitions.

Recommended workflow

1. Start with events disabled.
2. Build and test one action at a time.
3. Document the recipient IP, port, command termination, and expected response.
4. Enable only after the target behavior is confirmed.

6. System logs and status

6.1 UE-210 Logs

Logs show command activity, offer a temporary debug capture, and configure remote syslog delivery.

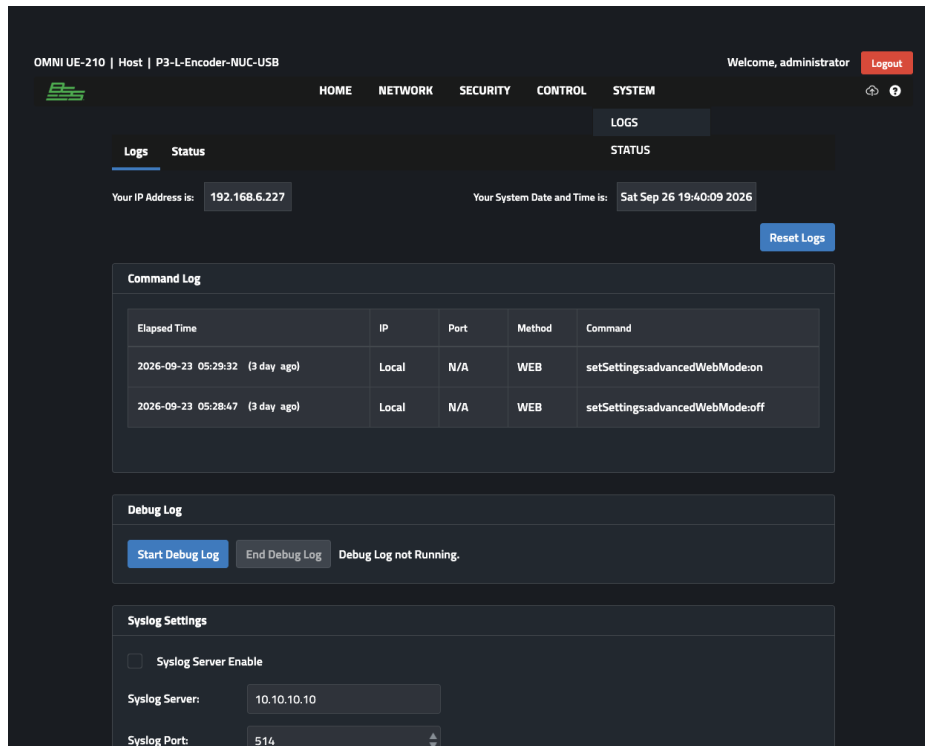


Figure 6-1. UE-210 Logs and Syslog Settings

Controls and indicators

Control / area	Purpose and operator guidance
Client IP / System time	Identifies the management client and device time context.
Command Log	Lists elapsed time, client IP, port, method, and command.
Reset Logs	Clears the available log view; use only after evidence is saved.
Start / End Debug Log	Controls detailed temporary logging.
Syslog Server	Enables a remote server and port for centralized records.

Recommended workflow

1. Verify device time before collecting evidence.
2. Reproduce the issue once with debug logging active.
3. End the debug session promptly and preserve the output.
4. Use remote syslog for persistent operational monitoring.

EVIDENCE: Do not reset logs until the incident record has been exported or otherwise preserved.

6.2 UD-210-WP Logs

Use the decoder-side log page to correlate USB-device activity and control commands with the UE-210.

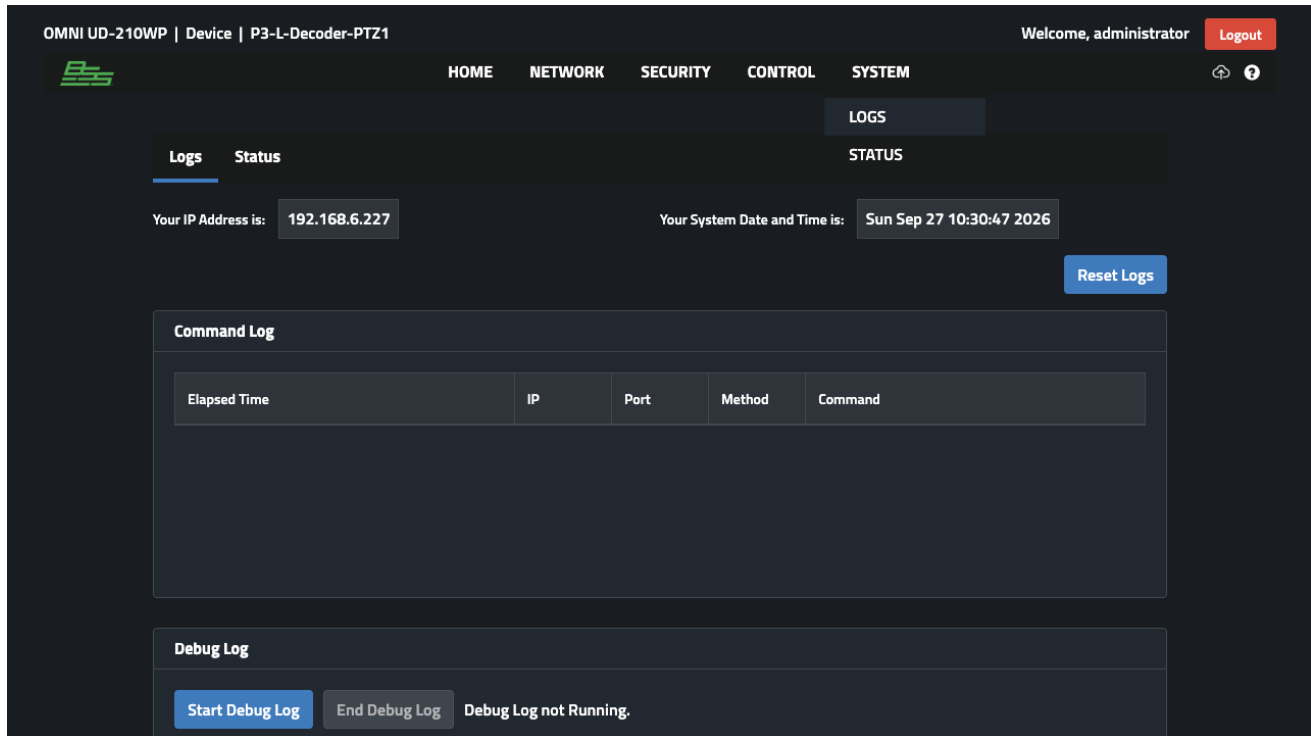


Figure 6-2. UD-210-WP Logs and Syslog Settings

Controls and indicators

Control / area	Purpose and operator guidance
Command Log	Records management/control requests.
Debug Log	Adds short-term detail for reproduction.
Syslog	Forwards events to a central collector.

Recommended workflow

1. Capture both endpoints during an end-to-end USB incident.
2. Record timestamps and client addresses.
3. Stop detailed logging after the reproduction.
4. Protect logs because they may contain device names, addresses, and commands.

6.3 UE-210 Status

Status consolidates service connectivity, USB host state, network link details, device identity, firmware, and maintenance actions.

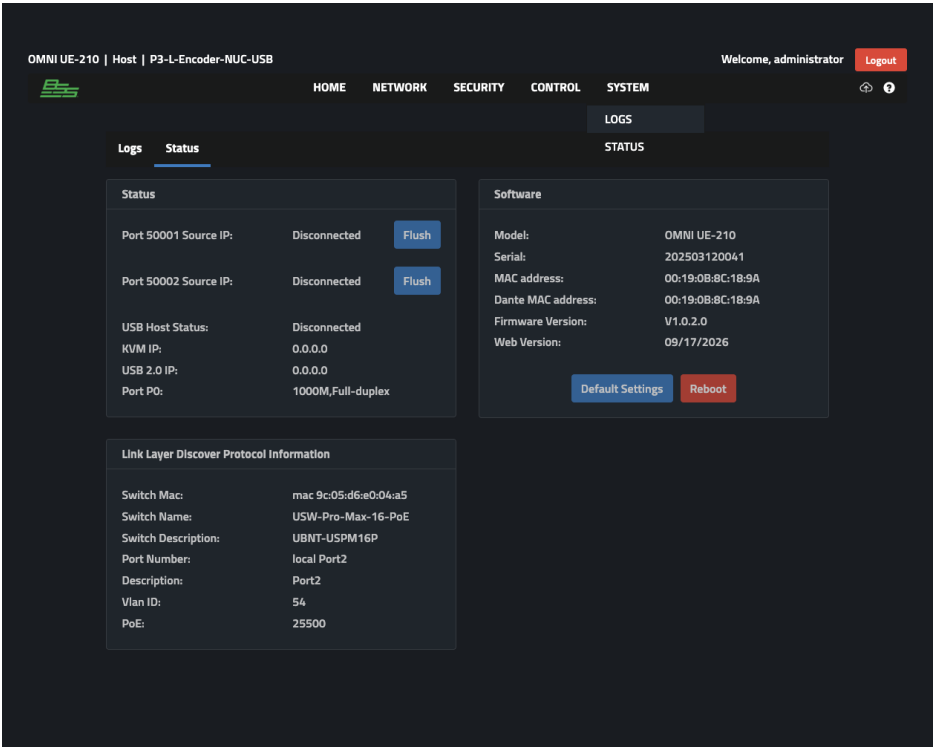


Figure 6-3. UE-210 live System Status

Controls and indicators

Control / area	Purpose and operator guidance
Control ports	Shows port 50001/50002 connection state.
USB Host / KVM / USB 2.0	Shows host cable and service address state.
P0 and switch information	Reports link speed/duplex and discovered switch data.
Identity	Model, serial, MAC, firmware, and Web build.
Default Settings / Reboot	Disruptive maintenance actions.

Recommended workflow

1. Confirm model, serial, and MAC first.
2. Check P0 link and switch discovery.
3. Compare KVM/USB status with the physical cable state and the UD endpoint.
4. Use reboot only after recording state and ruling out configuration causes.

6.4 UD-210-WP Status

The device-side status page adds USB-A/USB-C peripheral-state indicators and the configured KVM/USB service addresses.

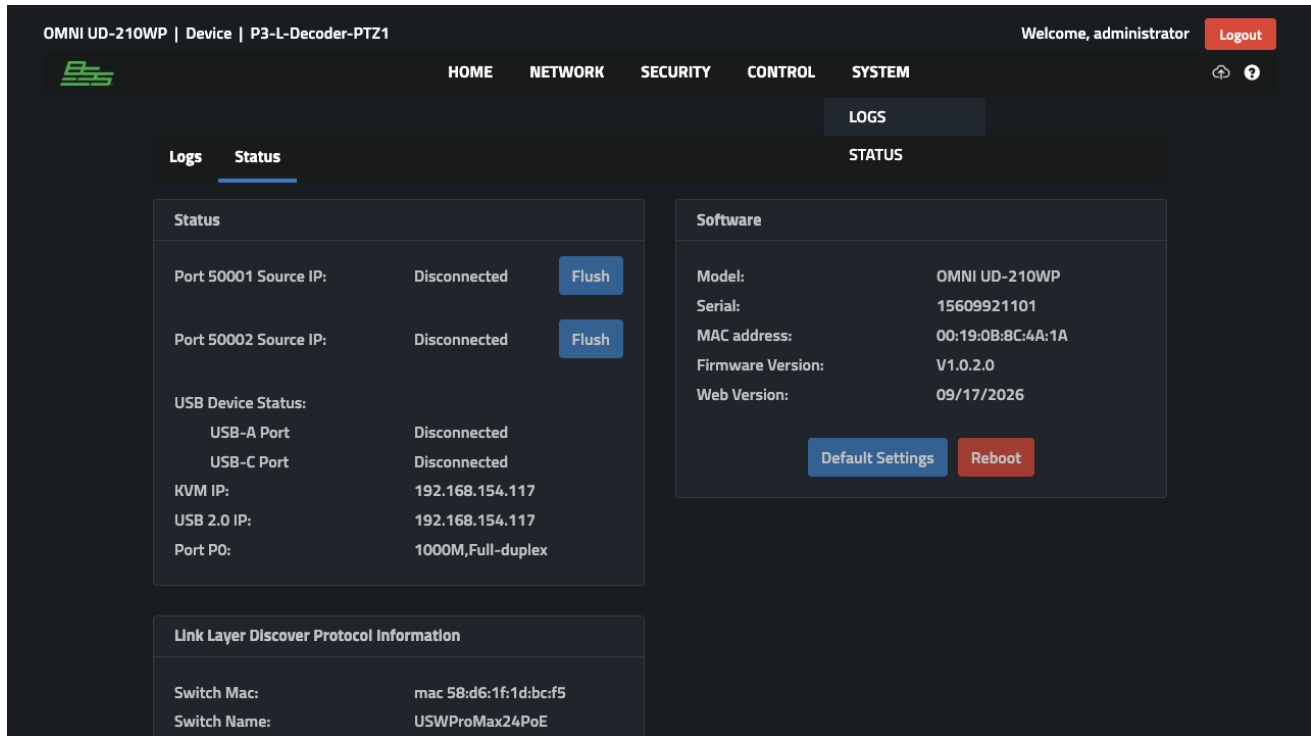


Figure 6-4. UD-210-WP live System Status

Controls and indicators

Control / area	Purpose and operator guidance
USB Device Status	Shows USB-A and USB-C device connection state.
KVM / USB 2.0 IP	Shows service-peer addressing.
P0 / switch	Shows physical network link and LLDP-style discovery.
Identity / firmware	Confirms the exact endpoint and installed software.

Recommended workflow

1. Verify physical USB cable and port selection.
2. Compare stream and service addressing to the UE-210.
3. Check link speed and switch port information.
4. Capture the status page before rebooting or restoring defaults.

7. Security and administration

The Security menu is HTTPS-only. Use it to enforce secure administration, change passwords, manage users and certificates, and configure LDAP. Exact availability can vary with firmware and privilege level; verify the model banner and current firmware before applying a security baseline.

Area	Administrative function	Safe practice
General	Force HTTPS, disable the Web page when required, restrict command control to secure ports, change command/stream-encryption passwords	Enable only after secure access and recovery are validated
Users	Change the current administrator password and manage supported accounts	Use unique managed credentials; do not reuse the lab password
Certificates	Upload CA, private-key, and certificate material for WebServer, 802.1X, or LDAP use	Protect private keys; verify chain, purpose, name, and expiry
LDAP	Set LDAP/LDAPS URL, Base DN, Bind DN, user query attribute, search credential, and certificate	Prefer LDAPS; use a least-privilege bind identity and test before cutover

7.1 UD-210-WP Security — General

The user-supplied real-device capture shows HTTPS enforcement, Web-page and secure-port policy, command password control, and certificate installation by purpose.

The screenshot displays the 'General' tab of the security configuration interface. It includes a 'Web Page' section with checkboxes for 'Force HTTPS', 'Web Page Disable', and 'Command Secure Ports Only'. Below this is a 'Change Command Password' section with a password input field, a 'Reset' button, and a 'Save' button. To the right, the 'Security Certificates' section contains a 'Type of Certificate' dropdown (set to 'CA Certificate'), fields for 'Private Key(.key .pem)' and 'Certificate(.pem)' with 'Browse' buttons, and a 'Password' field with an 'Upload' button. At the bottom, the 'Certificate Directory' section features a table with columns for 'Certificates' (Type, Issued By, Expiration Date) and 'User Setup' (WebServer, 802.1X, LDAP), plus an 'Action' column.

Figure 7-1. Real UD-210WP Security General and certificate directory; firmware V0.3.7 / Web 04/02/2026

Controls and indicators

Control / area	Purpose and operator guidance
Force HTTPS	Redirects management access to HTTPS.
Web Page Disable	Disables the Web UI when required by the security design.

Control / area	Purpose and operator guidance
Command Secure Ports Only	Restricts command traffic to secure ports.
Change Command Password	Changes or resets the protected command credential.
Certificate upload	Selects certificate type, private key, certificate, and optional password.
Certificate Directory	Shows certificate type, issuer, expiry, and assignment to WebServer, 802.1X, or LDAP.

Recommended workflow

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

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

7.2 UD-210-WP Security — Users

The Users tab changes the administrator password. The figure contains no entered password.

The screenshot shows a web interface with three tabs: 'General', 'Users', and 'LDAP'. The 'Users' tab is active. A modal window titled 'User Security Details' is displayed. Inside this modal, there is a header 'administrator'. Below it, there are two password input fields: 'New Password:' and 'Confirm Password:'. Both fields are empty and have a red eye icon to the right of the input box. At the bottom right of the modal, there are two buttons: 'Cancel' and 'Accept'.

Figure 7-2. Real UD-210WP administrator password controls; firmware V0.3.7 / Web 04/02/2026

Controls and indicators

Control / area	Purpose and operator guidance
Administrator	Expands the administrator account.
New Password / Confirm Password	Sets and confirms the replacement credential.
Cancel / Accept	Discards or commits the pending password change.

Recommended workflow

1. Open the approved credential manager.
2. Enter a unique password that meets site policy.
3. Select Accept, then sign out and sign back in.
4. Update the controlled credential record only after the new password is verified.

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

7.3 UD-210-WP Security — LDAP

The LDAP tab configures directory access, search scope, bind identity, query attribute, protected search credential, and certificate trust.

The screenshot shows the LDAP configuration window. At the top, there are three tabs: 'General', 'Users', and 'LDAP'. The 'LDAP' tab is selected. Below the tabs, there is a form titled 'LDAP'. The form contains the following fields and controls:

- LDAP Enabled:** A checkbox that is currently unchecked.
- LDAP/LDAPS URL:** A text input field containing 'LDAP://127.0.0.1:50001'.
- LDAP/LDAPS BASE DN:** A text input field containing 'DC=HarmanLab,DC=local'.
- BIND DN:** A text input field containing 'CN_NAV_'.
- User Query Attr:** A text input field containing 'Person'.
- Search Password:** A password input field with masked characters (dots).
- Buttons:** A blue 'Configure Certificate' button is located below the password field. At the bottom right of the window, there are 'Cancel' and 'Accept/Test' buttons.

Figure 7-3. Real UD-210WP LDAP configuration; firmware V0.3.7 / Web 04/02/2026

Controls and indicators

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

Recommended workflow

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

Credential change workflow

1. Confirm an alternate recovery method and record the device identity.
2. Open Security over validated HTTPS.
3. Set a unique password that meets site policy and store it in the approved credential manager.
4. Sign out and sign back in to verify the new credential before ending the maintenance window.

Certificate workflow

1. Correct date, time, DNS, and hostname first.
2. Obtain the approved CA chain and endpoint certificate/private key in the required format.
3. Upload only to the intended certificate role.
4. Verify HTTPS, 802.1X, or LDAPS functionality before removing prior trust material.

8. Routine workflows and troubleshooting

8.1 Commission a UE/UD pair

1. Record model, serial, MAC, firmware, and current IP for both devices.
2. Apply the approved hostname, IP, DNS, time, and NTP settings.
3. Assign the intended USB stream to both endpoints.
4. Enable KVM, USB 2.0, and USB audio behavior as required.
5. Verify link, USB host/device state, and peer service addressing under System > Status.
6. Add NAV-React actions one at a time and test against a controlled target.
7. Change the lab/default password and complete the security baseline.

8.2 If the endpoint is unreachable

- Check power, P0 link, switch VLAN, and the service computer subnet.
- Confirm the last known IP, mask, gateway, and any newly enabled 802.1X policy.
- Check for duplicate IP use and confirm that the browser is using the intended HTTP/HTTPS scheme.
- Use a local recovery method before choosing Default Settings; a reset can erase addressing and service configuration.

8.3 If USB/KVM is not passing

- Compare USB stream values on both ends.
- Confirm KVM Enable and USB 2.0 Enable on both endpoints.
- Inspect physical USB-A/USB-B/USB-C cable state and selected source.
- Check System Status on both endpoints before rebooting either device.
- Use synchronized timestamps and debug logs for one controlled reproduction.