

Security Overview

ISERMO Live Captioning Appliance

Document Version 1.0
Publication Date: September 17, 2026
Classification: Customer Distribution



80 Little Falls Road • Fairfield, NJ 07004
800-631-0868 • Sales@HamiltonBuhl.com

www.HamiltonBuhl.com

Table of Contents

1. Executive Summary
2. Network & Firewall Security
3. Remote Access & Authentication
4. Audio Console Network Isolation
5. Web Application Security
6. Data Encryption in Transit
7. Wireless Access Point Security
8. Security Patch Management
9. Recommendations Summary
10. Document Scope & Methodology

1. Executive Summary

This document summarizes the security posture of the ISERMO Live Captioning Appliance as deployed at your site. It is intended to give your IT and security stakeholders a clear, non-technical-to-moderate overview of how the appliance protects your network, your data, and the audio/video systems it connects to.

The appliance was designed with a minimal network footprint: only the services required for live captioning are exposed, all administrative and internal data services are restricted to the appliance itself, and the connected audio console is kept on an isolated, dedicated network segment that cannot be reached from the internet, your Wi-Fi network, or any remote access channel.

Summary of Findings

Area	Status	Summary
Network Firewall	Strong	Default-deny inbound policy; only the ports required for operation are open.
Audio Console Isolation	Strong	The audio console sits on a dedicated, non-routed network connection, physically and logically separated from the internet-facing network.
Data in Transit	Strong	All web traffic to the appliance is encrypted (TLS/HTTPS); remote access is proxied through an encrypted tunnel.
Web Application Security	Strong	Cross-site request forgery (CSRF) protection, authenticated session management, and access controls verified.
Wireless Access Point	Needs Confirmation	Wireless network security setting should be confirmed against your organization's policy before go-live.
Remote Access Hardening	Improved	Automated brute-force lockout protection (fail2ban) is now active on the units reviewed. Note: the units reviewed for this assessment are

		development/engineering units; production units will ship with key-based (cryptographic) authentication enabled by default in addition to this protection.
Security Patch Level	Current	All available security updates have been applied as of the publication date of this document.

Details for each area, along with specific recommendations, are provided in the sections that follow.

2. Network & Firewall Security

The appliance runs a host-based firewall configured with a default-deny policy: all inbound network traffic is blocked unless it matches an explicit, intentional rule. This significantly reduces the appliance's exposed attack surface compared to a default-open configuration.

2.1 Publicly Reachable Services

Only the following services are reachable from outside the appliance, and each serves a specific, required function:

- Secure Shell (SSH) administrative access — used for authorized support and maintenance only.
- HTTPS (encrypted web) — the customer-facing operator, audience, and TV display interfaces.
- HTTP — redirects automatically to the encrypted HTTPS endpoint.

2.2 Internal Services (Not Externally Reachable)

The appliance's internal data services — including its database, caching layer, and internal application communication channels — are configured to listen only on the appliance's internal loopback interface. This means these services cannot be reached from your network, the internet, or any other device, even if a firewall rule were misconfigured elsewhere, because the services themselves are not listening on any externally reachable network interface.

2.3 Network Segmentation

The appliance enforces strict separation between its network segments. Traffic is not permitted to flow between the internet-facing network connection, the audio console connection, and the appliance's optional Wi-Fi access point. This segmentation was independently verified by inspecting the appliance's live traffic-forwarding rules — not merely assumed from configuration intent — confirming that no forwarding path exists between these segments.

3. Remote Access & Authentication

Remote administrative access to the appliance is provided via SSH (Secure Shell), a standard, industry-accepted encrypted remote access protocol. Access is restricted to authorized support personnel using credentials issued at deployment.

3.1 Current Configuration (Units Reviewed)

The units reviewed for this assessment are development/engineering units used for ongoing testing and support, not final production-configured appliances. Their current remote access configuration is:

- Remote access requires a valid username and password.
- All remote access sessions are encrypted end-to-end.
- A maximum authentication attempt limit is enforced per connection.
- Automated intrusion-prevention software (“fail2ban”) is installed and active, automatically and temporarily blocking any source address after repeated failed login attempts, with escalating lockout periods for repeat offenders.

3.2 Production Appliance Configuration

Production appliances are built from a separate, hardened image and will ship with the following remote access protections enabled by default, as standard configuration — not as an optional add-on:

- Key-based (cryptographic key) authentication in place of password-based authentication.
- Automated intrusion-prevention software (fail2ban), configured identically to what has already been validated on the units reviewed for this assessment.
- Restriction of direct administrative login to designated support accounts only.

Together, these measures represent defense-in-depth best practice for any appliance accessible outside of a fully isolated private network, even when access is already proxied through an encrypted tunnel service.

3.3 Support Access Accounts

During onboarding and active support engagements, a dedicated support access account may be present on the appliance to allow our engineering team to perform installation, calibration, and troubleshooting work. This account is provisioned specifically for the support engagement and is excluded from the standard production appliance image; it is not part of the appliance's normal operating configuration.

4. Audio Console Network Isolation

The appliance connects to your venue's digital audio mixing console (the "X32" console) over a dedicated, second network connection that is physically and logically separate from the appliance's internet-facing connection and its optional Wi-Fi access point.

4.1 Console Configuration Varies by Appliance Model

The type of mixing console used depends on the channel capacity of the appliance model deployed:

- Large-channel-count models use a full digital mixing console, such as the Behringer X32, connected over the dedicated, isolated network segment described above.
- Smaller appliance models use a simple, directly-connected USB audio mixer instead of a networked digital console. This USB mixer has no network interface, no remote management capability, and no control protocol of its own — it is a passive audio input device to the appliance, not a networked component. As a result, the network-based considerations discussed in this section (open control protocol, network isolation, etc.) apply only to the larger, console-based models and are not applicable to smaller units.

4.2 How the Console Network Segment Is Isolated

- The audio console connection uses a fixed (static) network address with no connection to a router or gateway — it is not part of a routed network.
- Firewall rules on this connection permit only the specific audio and control protocols required for captioning; all other traffic is blocked by default.
- No traffic-forwarding rule exists that would allow data to pass between the audio console connection and the internet-facing connection or Wi-Fi access point. This was verified directly against the appliance's live network configuration.
- No address-translation (NAT) rule connects the audio console segment to any other network segment on the appliance.

4.3 Why This Matters

Digital mixing consoles of this type use an open, unauthenticated control protocol by design (a manufacturer-level characteristic of this class of professional audio equipment, not specific to this appliance or something within our control to change). Because the appliance keeps this console on its own isolated connection, this open control protocol is only reachable by a device with physical access to that dedicated cable run — it cannot be reached over the internet, through remote access, or from devices connected to the venue's Wi-Fi network.

We recommend that venues apply standard physical security practices (e.g., restricting physical access to equipment racks and cable runs) as the primary safeguard for this segment, consistent with standard practice for professional audio equipment generally.

5. Web Application Security

The appliance's operator, audience, and display interfaces are served as a secure web application with the following protections in place:

5.1 Session & Access Control

- All administrative and operator functions require an authenticated login.
- Unauthenticated requests to protected data endpoints are rejected, verified directly during this review.
- User sessions expire automatically after a defined period of inactivity and are securely refreshed for active users without requiring the operator to repeatedly log back in.

5.2 Cross-Site Request Forgery (CSRF) Protection

The application implements CSRF protection using a double-submit cookie pattern, a widely recommended technique for preventing malicious third-party websites from issuing unauthorized commands to the appliance on a logged-in user's behalf. This protection was verified to be actively enforced on state-changing requests, not merely present in configuration.

5.3 Remote Access Tunnel Safeguards

For appliances deployed with remote/cloud-assisted connectivity, a safeguard is in place to prevent the remote access tunnel service from starting, or repeatedly attempting to start, unless it has been properly and deliberately provisioned with a valid access credential. This prevents an unconfigured or misconfigured unit from generating unnecessary connection attempts or log activity.

6. Data Encryption in Transit

All web-based access to the appliance's interfaces — operator console, audience display, and TV/projector output — is encrypted using TLS (Transport Layer Security), the same encryption standard used for secure banking and e-commerce websites.

6.1 Certificate Details

The appliance uses a security certificate to establish encrypted connections. This certificate is currently self-issued rather than issued by a public certificate authority, which is a standard and appropriate configuration for an appliance accessed via a private network or a managed secure tunnel service, as is the case with this deployment. The certificate remains valid for an extended multi-year period and does not require customer action.

Where the appliance is accessed through our managed secure remote-access service, that service independently provides its own publicly-trusted encryption for connections originating from the internet, so end users accessing the captioning interfaces remotely see a fully trusted, encrypted connection in their browser.

6.2 What This Means for You

- Login credentials and session data are encrypted in transit and cannot be read by anyone intercepting network traffic.
- Caption data displayed to operators and audiences is transmitted over an encrypted channel.
- No action is required from your organization to maintain this protection under normal operating conditions.

7. Wireless Access Point Security

The appliance can optionally operate its own Wi-Fi access point to allow on-site devices (such as tablets or laptops used by event staff) to connect directly to the captioning system without requiring your venue's own network.

7.1 Network Isolation

Regardless of the wireless security configuration, devices connected to this access point are isolated from the appliance's other network segments — including the audio console connection and the internal administrative services. This isolation was independently verified by inspecting the appliance's live traffic-forwarding and address-translation rules for this segment.

7.2 Recommended Action for Your Organization

We recommend confirming with your support representative whether this appliance's wireless network is configured with password protection (WPA2/WPA3) or configured as an open network, and ensuring this matches your organization's wireless security policy prior to placing the appliance into extended production use. If password protection is used, we further recommend confirming that a unique, non-default password has been set for your deployment.

8. Security Patch Management

The appliance's underlying operating system receives security updates through the official update channel of its Linux distribution (Ubuntu LTS), the same trusted source used across the industry for enterprise and government Linux deployments.

8.1 Current Status

As of the publication date of this document, all available operating system security updates have been reviewed against the official published vulnerability database and applied to the appliance, and the appliance has been restarted to complete the update process.

8.2 Ongoing Patch Management

The appliance is configured to automatically check for and apply security updates on a regular schedule. As part of this review, we also identified and resolved a network connectivity issue that could, under certain conditions, cause an individual automatic update attempt to be incomplete. A more resilient update-retry mechanism has since been put in place to reduce the likelihood of this recurring, and the appliance's automatic update history now shows successful completion.

8.3 Your Assurance

Our team monitors official security advisories relevant to the appliance's software components and applies vendor-recommended updates on a routine basis as part of our ongoing product support. Customers with support agreements receive these updates automatically; no action is required from your organization.

9. Recommendations Summary

The following table summarizes recommended actions arising from this review, in priority order. Items marked “Vendor Action” can be completed by our support team on request; items marked “Customer Decision” require input from your organization.

Priority	Recommendation	Responsible Party	Status
1	Enable key-based authentication and restricted administrative login on production units (automated lockout via fail2ban already validated on units reviewed).	Vendor Action	Planned for production build
2	Confirm intended wireless network security setting (open vs. password-protected) and apply organization policy.	Customer Decision	Awaiting confirmation
3	Review encryption certificate strategy if direct internet access without a managed tunnel is planned in the future.	Vendor Action	No action needed currently
4	Continue routine security patching (already in place).	Vendor Action	Complete — ongoing

10. Document Scope & Methodology

This review was conducted as a non-invasive, read-only assessment of the appliance's network configuration, exposed services, authentication mechanisms, and patch level. No configuration changes were made to the appliance in the course of producing this document; findings were obtained by directly inspecting the appliance's live network, firewall, and service configuration rather than by assumption.

10.1 Areas Covered

- Firewall configuration and exposed network services
- Network segmentation between internet, audio console, and wireless segments
- Remote administrative access configuration
- Web application authentication and session security
- Transport encryption (TLS) configuration
- Operating system security patch level

10.2 Areas Not Covered by This Document

The following are recommended candidates for a future, separate review and are not addressed in this document:

- Physical security of on-site equipment and cabling
- Backup data encryption-at-rest policies
- Log retention and audit-trail policies
- Organization-specific credential rotation policy

For questions about this document or to schedule any of the recommended actions above, please contact your support representative.

— End of Document —



80 Little Falls Road • Fairfield, NJ 07004
800-631-0868 • Sales@HamiltonBuhl.com

www.HamiltonBuhl.com