WebRTC Connectivity for ODIN and RVON+

Version 01, 2026-08

Table of contents

1 Copyright and Disclaimer

2 Introduction

ODIN and RVON+ (IO card based) intercoms now support WebRTC based connection, allowing users to connect the RTS intercom system on a standard web browser or the RTS client application (app based) — no dedicated hardware panel, no VPN client, and no plug-ins.
WebRTC brings real-time, encrypted, low-latency audio to devices that were previously outside the intercom network, this allows connection to laptops, tablets, and smartphones, whether they are on the studio LAN, in a remote office, or at home behind a domestic router.
This application note helps in understanding:

- How the WebRTC feature works and which network paths it uses (Section 2-3)
- Recommended deployment architectures, from a single LAN to full internet remote access (Section 4)
- Firewall and NAT configuration requirements (Section 5)
- STUN/TURN server guidance, including a sample deployment example (Section 6)
- Security architecture (Section 7)
- Capacity and bandwidth planning (Section 8)
- FAQ and troubleshooting (Sections 9-10)

Notice!
Network behavior described here applies to both ODIN and RVON+. Where channel counts differ between products, the ODIN figures are given; consult the product datasheet for RVON+ capacity figures.

3 Feature Overview

3.1 Core Capabilities

Capability	Detail
Connection type	Full-duplex intercom audio between a client (browser/app) and an intercom port.
Signaling	HTTPs/Secure WebSocket (WSS) server by the intercom itself on TCP port 2083.
Media transport	SRTP over UDP, negotiated with ICE (host, server-reflexive, and relay candidates).
Audio codecs supported	G.711 μ-law (PCMU) G.711 A-law (PCMA) G.722 wideband.
Encryption	TLS 1.2 for signaling; DTLS-SRTP (AES-GCM) for media - always on, cannot be disabled.
Authentication	Per-port username/password, exchanged for a short-lived single use session token.
NAT traversal	ICE with trickle candidates; customer-configurable STUN and TURN servers.
Cloud dependency	NONE. The entire solution is on-premises; STUN/TURN servers may be on-premises or hosted, at the customer's choice.
Capacity	Up to 64 WebRTC ports per ODIN frame (subject to licensing) Up to 32 WebRTC ports per RVON+ card (subject to licensing)
Certificates	Default self-signed certificates (less secure), User Downloadable certificates, Customer certificates.

3.2 What is WebRTC

WebRTC provides a real-time media standard that every modern browser includes. Each session consists of two parts:

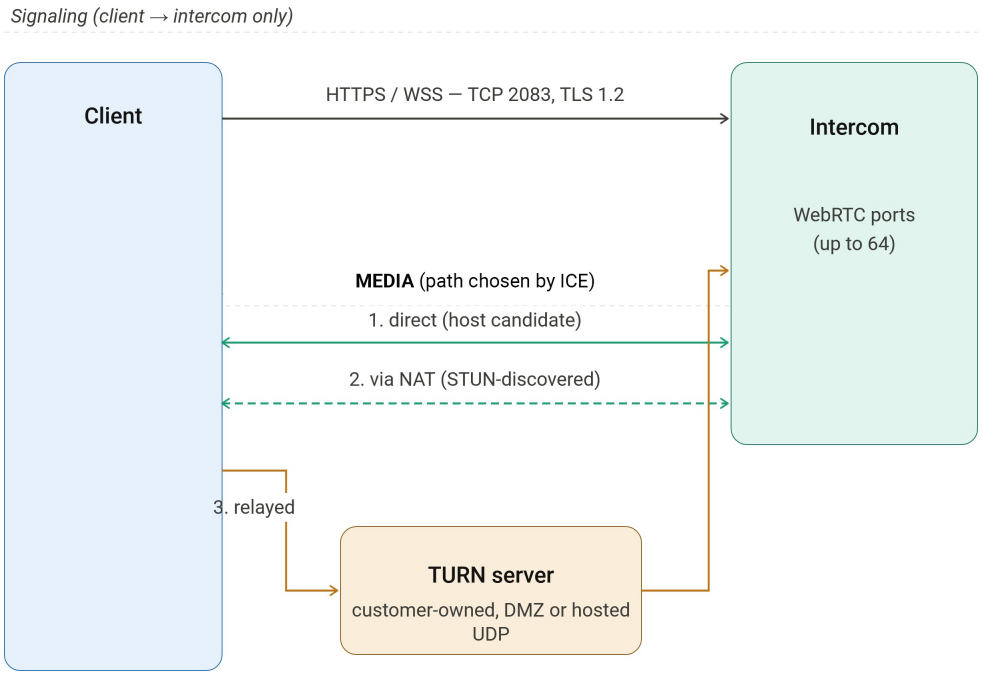
- A signaling channel uses HTTPS or WebSocket connections to exchange session descriptions and network candidates.
- A media path carries encrypted RTP audio over UDP.

ICE (Interactive Connectivity Establishment) establishes the media path. It first attempts the most

direct route by trying a direct LAN connection. If that fails, it discovers a NAT-traversed path using a STUN server. If no direct route exists, it routes traffic through a TURN server.

4 System Architecture

In this system architecture, the intercom acts as the central server, and all clients initiate their signaling connections to it over TCP port 2083. Because the intercom does not open outbound connections, you only need to configure a single inbound rule on the firewall, which keeps deployment simple and predictable. The system handles media dynamically by negotiating UDP ports during session setup instead of relying on fixed assignments. On a local network, the client and intercom exchange audio directly. When NAT or firewall boundaries are present, both sides use a customer-managed TURN server to relay audio reliably.



The system operates entirely within the customer's environment, with no dependency on cloud services. The intercom terminates all signaling, and the customer maintains full control over STUN and TURN servers, whether deployed on-premises, in a DMZ (a segmented network that exposes services to external networks while protecting the internal network), or through a hosting provider. If the system cannot establish a direct connection after two attempts within 90 seconds, the intercom automatically switches to a relay-only mode for 15 minutes. This behavior prioritizes connection reliability and occurs seamlessly, without requiring any user action.

5 Deployment Scenarios

The following deployment scenarios illustrate how to implement the system across different network environments and connectivity requirements:

- LAN Only - Deploy the intercom and clients on the same local network, where they exchange signaling and media directly without NAT or firewall traversal.
- Corporate WAN/LAN - Connect clients and intercoms across enterprise network segments, where internal routing and security policies control traffic between sites.
- Remote Access over Internet - Allow clients outside the corporate network to connect over the public internet, using firewall rules and optional NAT traversal services such as STUN/TURN.
- Relay-Only Mode - Force all media traffic through a TURN relay to maintain reliable connectivity when direct peer-to-peer communication is not possible.

		LAN Only	Corporate WAN/ VPN	Remote Access over Internet	Relay-Only
	Description	Client and intercom operate on the same local network with no NAT. Signaling uses TCP 2083; media flows directly over UDP.	Client connects over a routed WAN or site-to-site VPN with direct IP reachability and no NAT.	Remote clients connect over the public internet. The system uses TURN to relay media when direct paths fail.	The system forces all media through a TURN server due to restricted network policies.
	STUN/TURN Required	No	No	Yes (TURN strongly recommended)	Yes (mandatory)
	Network/Firewall Notes	Allow TCP 2083 and UDP if VLAN segmentation exists. No NAT traversal required.	Ensure WAN/VPN supports UDP and meets latency/ jitter requirements. Avoid TCP-based VPN tunnels.	– Deploy TURN/STUN in a DMZ or hosted environment. – Allow UDP (typically 3478). Configure port forwarding or proxy for TCP 2083.	Use TURN as a central relay. Clients may use UDP, TCP, or TLS (3478/443/5349). Intercom still requires UDP to TURN.
	Recommended Use	On-site operators and facility Wi-Fi deployments	Enterprise multi-site deployments	Remote production, home users, mobile access, OB trucks without VPN	Highly restricted enterprise networks requiring controlled traffic paths

5.1 LAN only

In this scenario, the client and intercom system operate on the same network—either on the same subnet or across a routed campus LAN. Because there is no NAT between them, the connection is direct and simple to configure.

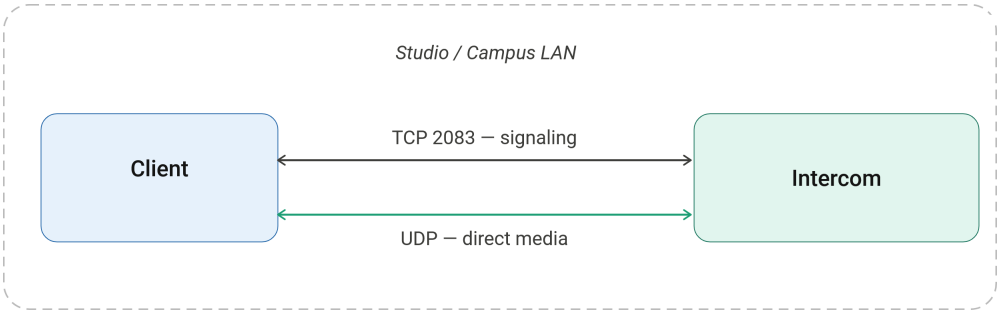


Figure 5.1: Studio/Campus LAN

How it works

- The client connects directly to ODIN/RVON+ over the local network.
- Signaling uses TCP port 2083.
- Media (audio) flows directly over UDP between the client and the intercom system.
- No relay or traversal services are required.

Requirements

- Client and intercom must have direct IP reachability
- No NAT between endpoints
- Network must support:
  - TCP 2083 (signaling)
  - Bidirectional UDP (media)

STUN/TURN

- Not required
  - Local connectivity eliminates the need for NAT traversal or media relays.

Firewall considerations

- Typically not required on flat networks.
- If internal segmentation is in place (for example, separate VLANs):
  - Allow TCP 2083 between the client and ODIN/RVON+
  - Allow UDP media traffic between both endpoints
  - Refer to Section 5 for port details

When to use this scenario

Use this deployment for:

- Operators and producers working inside the facility

- Engineering and testing on the local network
- Wireless beltpack replacement over facility Wi-Fi

This is the simplest and highest-performance deployment, providing low latency and direct media flow with minimal configuration.

5.2 Corporate WAN/LAN

In this scenario, the client connects from a remote site over a routed corporate WAN or an established site-to-site VPN. Because the network provides full end-to-end connectivity, the client and intercom system communicate directly without NAT or relay services.

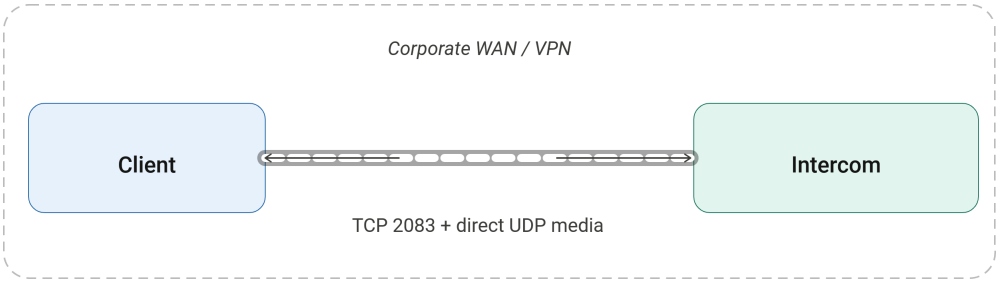


Figure 5.2: Corporate WAN/LAN

How it works

- The client connects directly to the intercom system across the WAN or VPN.
- Signaling uses TCP port 2083.
- Media (audio) flows directly over UDP between the client and ODIN/RVON+.
- No relay or traversal services are needed because the network provides full IP reachability

Requirements

- End-to-end IP connectivity between the client and intercom system
- No NAT in the path
- Firewall rules must allow:
  - TCP 2083 (signaling)
  - UDP media traffic in both directions

STUN/TURN

Not required - The WAN or VPN already provides direct connectivity, so no NAT traversal is needed.

Important notes

- Verify that the WAN or VPN allows UDP traffic and supports real-time media.
- Confirm that network performance meets audio requirements:
  - Low latency
  - Minimal jitter

  - Low packet loss
- Avoid TCP-based VPN tunnels (for example, SSL VPN operating in TCP mode):
  - Encapsulating real-time audio in TCP can introduce retransmissions and buffering delays
  - This often causes audible artifacts such as dropouts or distortion under packet loss

When to use this scenario

Use this deployment for:

- Corporate environments with managed WAN infrastructure
- Permanent remote facilities connected via site-to-site VPN
- Studios, campuses, or broadcast sites linked through private networks

This approach provides the best performance and lowest latency, since media flows directly between endpoints without relay or traversal overhead.

5.3 Remote access over internet

Remote users on home or mobile networks connect to the intercom system over the public internet. This scenario relies on TURN infrastructure to ensure reliable media connectivity when direct UDP paths are not possible.

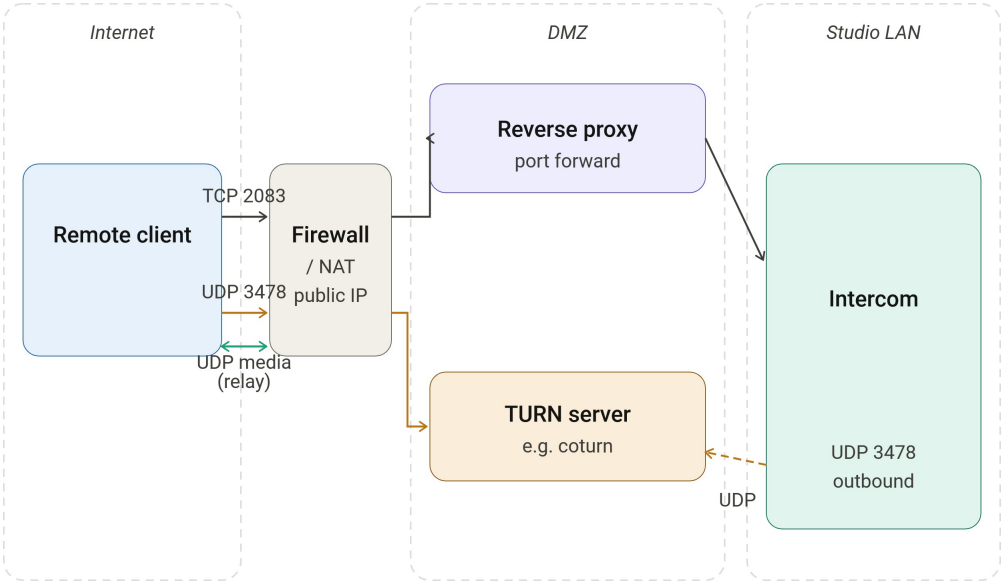


Figure 5.3: Remote Access over the Internet

How it works

- The remote client connects to the intercom system over the internet using TCP 2083 for signaling.
- A firewall, NAT router, or reverse proxy exposes this signaling interface to the public internet.
- Media traffic flows through a TURN server, which relays audio between the remote client and ODIN/RVON+.

- The TURN server ensures connectivity when both the client and intercom system are behind NAT or firewalls.

Key components

Component	Placement	Purpose
Port forward or reverse proxy (TCP 2083)	Firewall / DMZ	Exposes the intercom signaling interface to remote users.
TURN server (i.e., co-turn)	DMZ or cloud VM	Relays media between remote clients and the intercom.

Component	Placement	Purpose
STUN (often part of TURN)	Same as TURN	Allows clients to discover their public IP for direct connection attempts.

Important notes

- TURN is required for reliable internet operation in this scenario.
  - Both the remote client and the intercom are typically behind NAT, preventing direct media paths.
- The intercom system (ODIN/RVON+) must be able to:
  - Send and receive UDP traffic to the TURN server (typically port 3478).
- Place the TURN server where the intercom can reliably reach it:
  - DMZ host or
  - Cloud-hosted VM
- Remote clients can connect to TURN using:
  - UDP (preferred)
  - TCP/TLS (ports 443 or 5349) if UDP is blocked on the client network

When to use this scenario

Use this deployment when supporting:

- Remote production workflows
- At-home commentator or operator positions
- Mobile or field users on public networks
- OB truck connectivity without requiring a site-to-site VPN

This model prioritizes **connectivity and flexibility**, ensuring remote users can reliably access the intercom system from virtually any network.

5.4 Relay-only

Some enterprise networks block direct UDP traffic between network zones. In these environments, all media traffic must pass through a TURN server. This creates a single, controlled path for media that administrators can monitor and audit.

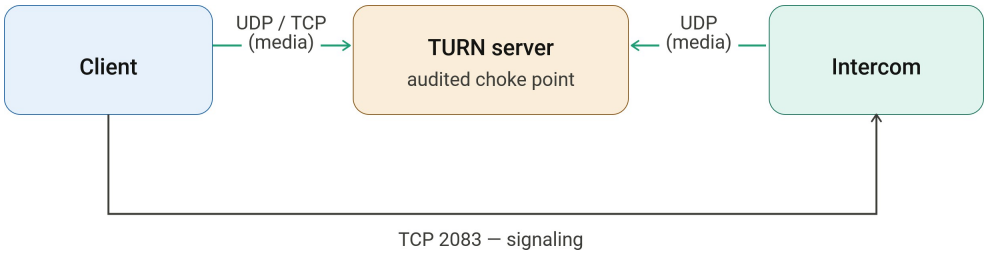


Figure 5.4: Relay Only

How it works

- The client sends all media to the TURN server instead of directly to the intercom system.
- The TURN server relays that media to ODIN/RVON+, acting as a central inspection and control point.
- Signaling continues over TCP port 2083 between the client and the intercom system.

Important notes

- Clients (such as browsers) can connect to the TURN server using:
  - UDP (preferred when available)
  - TCP or TLS (ports 443 or 5349) when UDP is blocked on the client side
- The intercom system (ODIN/RVON+) still requires UDP connectivity to the TURN server for media handling.
- The system automatically switches to relay-only mode after repeated direct connection failures. This behavior provides a built-in fallback for restricted network environments (for example, when direct media paths are not possible).

When to use this scenario

- Networks with strict firewall rules or segmented zones
- Environments that require full visibility and auditing of media traffic
- Deployments where direct peer-to-peer media is not allowed or not reliable

This approach prioritizes security and control over direct connectivity, while keeping media communication fully functional.

6 Firewall Configuration

This section defines the required firewall rules and network behavior for the intercom system, client networks, and TURN infrastructure. Follow these guidelines to ensure reliable, secure audio connectivity across all deployment scenarios.

6.1 Quick Reference

Use this summary for quick configuration:

Component	Required Access
Intercom (ODIN / RVON+)	Inbound TCP 2083 only
Intercom - TURN	Outbound UDP 3478
Client	Outbound TCP2083 + UDP 3478
TURN Server	UDP3478 + relay port range

NOTE: In most environments, no inbound UDP rules are required.

6.2 Intercom (ODIN / RVON+) Requirements

Configure the following network access for the intercom system:

Required Rules

- Allow inbound TCP 2083 from client networks
  - Used for HTTPS/WSS signaling and embedded web client
- Allow outbound UDP 3478 (or configured port) to TURN/STUN servers
  - Used for NAT discovery and media relay
- Allow outbound UDP (ephemeral ports)
  - Used for direct SRTP media

Behavior

- The intercom initiates all UDP media flows
- A stateful firewall automatically allows return traffic
- No inbound UDP rules are required

Important

TCP 2083 is fixed and cannot be changed

- If you must publish a different external port:
  - Configure a reverse proxy, or
  - Use port translation (NAT)
- The proxy must:
  - Support WebSocket (WSS) upgrades
  - Pass traffic without buffering or inspection
  - Operate in transparent / pass-through mode and preserve the original client source IP address. Proxies that present all traffic from a single source address will trigger the device's per-source-IP connection and lockout limits.

Limitations

- IPv4 only
  - WebRTC does not use IPv6 in this release

6.3 Client Network Requirements

Most client networks (enterprise or home) allow these connections by default.

Required Outbound Access (if restricted)

- TCP 2083 - Intercom
  - Signaling and web client access
- UDP 3478 - TURN server
  - NAT discovery and TURN allocation
- UDP relay port range (e.g., 49152-65535) - TURN
  - Relayed media

Optional (Fallback for Restricted Networks)

- TCP 443 or TLS 5349 -TURN server
  - Enables TURN over TCP/TLS when UDP is blocked

Notes

- Clients do not require inbound rules
- TURN fallback ensures connectivity in UDP-restricted environments

6.4 TURN Server Requirements

Use the following rules when deploying a TURN server (e.g., co-turn) in a DMZ or cloud environment.

Required Inbound Access

- UDP 3478 from clients and intercom
  - STUN binding and TURN allocation
- UDP relay port range (configurable)
  - Media relay between endpoints

Optional Inbound Access

- TCP 3478, TCP 443, or TLS 5349 from clients
  - Supports TURN fallback when UDP is unavailable

Deployment Guidelines

- Place the TURN server where the intercom can reach it over UDP
  - DMZ host or cloud VM recommended
- Restrict the relay port range to align with your security policy

6.5 Firewall Configuration Checklist

Use the following checklist to avoid common issues with real-time audio traffic:

Recommended Settings

- Set UDP session timeout ≥ 90 seconds
  - Prevents media drops during active sessions
- Allow bidirectional UDP flows between endpoints or TURN server

Disable or Avoid

- SIP ALG / VoIP helpers
  - These modify packets and break STUN/TURN signaling
- TLS inspection on TCP 2083
  - The signaling channel uses secure WebSocket (WSS)
  - Inspection will break the connection
- Deep packet inspection (DPI) on UDP media
  - Media is DTLS-SRTP encrypted
  - Packet delay or reordering will degrade audio quality

7 STUN/TURN Server Guidance

Network conditions—particularly NAT and firewall behavior—play a key role in how clients establish media paths to the intercom. In simple environments, such as local networks, direct connections typically succeed without additional services. As network complexity increases, especially in internet-facing or enterprise deployments, STUN and TURN help maintain reliable and consistent connectivity by supporting connection establishment when direct paths are not available.

When to Use STUN and TURN

Use the following guidance to determine when to deploy STUN and TURN:

Scenario	STUN	TURN
LAN only	Do not use	Do not use
Routed WAN/VPN	Do not use	Do not use
Internet remote access	Recommended	Required
Relay-only enterprise	Optional	Required

Rule of thumb:

Deploy TURN whenever NAT exists between the client and the intercom.

- STUN works only with permissive NAT types.
- Symmetric NAT—common in enterprise and mobile carrier networks—blocks STUN.
- TURN provides a reliable fallback in all cases.

The intercom's ICE logic always selects the most direct working path. TURN does not degrade performance; the system uses it only when necessary.

7.1 Configure STUN and TURN

Configure STUN and TURN servers in the ODIN management interface (currently through IPedit). Refer to the ODIN configuration manual for the exact menu path.
Provide the following settings for each server:

- Server IP address - Enter the IPv4 address. Configure up to 2 STUN servers and 4 TURN servers.
- Port - Use port 3478 in most deployments.
- Transport (TURN)
  - Use UDP on the intercom side.
  - Apply TCP/TLS TURN transports only on the client side.
- Username / Password (TURN) - Enter the long-term credentials configured on the TURN server. The intercom automatically distributes the ICE server list to clients during session setup. Do not configure clients individually.

Example Configuration — co-turn

Use the following minimal, production-ready /etc/turnserver.conf for a DMZ or cloud-hosted co-turn deployment:
listening-port=3478
tls-listening-port=5349 listening-ip=<DMZ-internal-IP>
external-ip=<public-IP>/<DMZ-internal-IP> # when coturn is behind 1:1 NAT relay-ip=<DMZ-internal-IP>
min-port=49152 max-port=65535
fingerprint lt-cred-mech
user=odin-webrtc:<strong-shared-secret> realm=intercom.example.com
no-multicast-peers no-cli
Restrict relaying to required destinations:
denied-peer-ip=0.0.0.0-255.255.255.255 allowed-peer-ip=<intercom-IP>
allowed-peer-ip=<any other permitted media endpoints>

Sizing guidance:

- TURN relaying uses minimal CPU (it forwards encrypted packets without transcoding).
- TURN consumes bandwidth. Plan for 2× the per-call bitrate for each relayed call, because traffic enters and exits the server.

7.2 Use of Public STUN Servers

Use public STUN servers (for example, stun.1.google.com) only for testing direct-path discovery. Do not rely on public infrastructure for production broadcast paths.

- Public TURN services do not exist in a usable form for production.
- TURN requires controlled credentials and dedicated bandwidth.

Notice!
For production deployments, run your own STUN/TURN infrastructure.

8 Security

This section describes the security mechanisms that protect signaling, media, and access to the intercom system. It outlines how the system secures connections, authenticates users, encrypts media, and limits exposure to unauthorized access.
These controls work together to protect both the control plane and media plane while maintaining secure, reliable operation across LAN, WAN, and internet-facing deployments.

8.1 Security Architecture

Layer	Mechanism
Signaling transport	TLS1.2 (HTTP/WSS) on TCP 2083 HSTS enforces HTTPS for two years
Client authentication	Per-port username and password with a single-use session token (valid for 30 seconds) Clients obtain the token over HTTPS and use it to establish the WebSocket connection
Brute-force protection	Per-source IP lockout after five failed login attempts System enforces a 30-second lockout
Media encryption	DTLS-SRTP with AES-GCM (128- or 256-bit) Encryption is always enabled and cannot be disabled
TURN credentials	TURN long-term credentials allow relay access only Credentials do not grant intercom access
Hardening headers	Embedded web server applies CSP, X-Frame-Options DENY, nosniff, and related browser security headers

Key behaviors:

- The system never exposes user credentials in WebSocket URLs during normal operation.
- The system encrypts all media end-to-end between the client and intercom.
- The TURN server relays encrypted traffic and cannot decrypt audio.

8.2 Certificates

The intercom ships with a self-signed TLS certificate, which causes browsers to display a security warning on the first connection. Replace this certificate in production deployments with one issued by a trusted Certificate Authority (CA).
The intercom supports customer-provided certificates and keys in PEM format, which you can install using AZedit.

Recommendations:

- Assign a proper DNS name to the signaling endpoint (for example, intercom.example.com) and issue the certificate for that hostname. Browsers do not reliably validate certificates presented for IP addresses.
- If you deploy a reverse proxy (Scenario C), install the public CA-issued certificate on the proxy. Use the intercom's device certificate for the proxy-to-intercom connection inside the trusted network.

8.3 Exposure Assessment for Internet Deployment

The following table outlines what the system exposes in an internet-facing deployment and the controls that protect each element:

Exposed Surface	Control
TCP 2083 (TLS web/signaling)	TLS encryption, token-based authentication, brute-force lockout; optionally restrict source IPs or protect with a reverse proxy or WAF
TURN UDP 3478 and relay port range	TURN credentials and allowed-peer-ip restriction limit relay access to the intercom only
Other inbound ports	Not required for WebRTC operation

Security considerations:

- Limit exposure by allowing only required ports and restricting access where possible.
- Use a reverse proxy or firewall policies to enforce additional access controls.
- Ensure adequate monitoring and logging for authentication attempts and traffic patterns.

Media security:

The system encrypts all media end-to-end using DTLS-SRTP. The TURN server forwards encrypted packets and cannot access or decode audio content.

9 Capacity and Bandwidth

Use these guidelines to plan and validate your deployment. Proper sizing and prioritization help maintain consistent audio quality, reduce delays, and keep communication natural and reliable across all supported network scenarios.

9.1 Per-Connection Bandwidth

The following values represent per-direction bandwidth usage, including IP/UDP/RTP/SRTP overhead, based on the default 20 ms packetization interval.

Codec	Audio Quality	Payload Bitrate	On-the-Wire (Approx.)
G.711 (PCMU/PCMA)	Narrowband (3.4kHz)	64 kbit/s	≈ 87 kbit/s
G.722	Wideband (7 kHz)	64 kbit/s	≈ 87 kbit/s

Key considerations:

- G.722 delivers noticeably better intelligibility at the same bandwidth. Use G.722 where the system supports it.
- Each call operates in full duplex. Allocate the listed bandwidth in both directions when sizing links.
- A relayed (TURN) call consumes twice the bandwidth on the TURN server link (ingress + egress).

9.2 System Capacity

Resource	Limit
WebRTC ports per ODIN frame	64 (license-dependent; verify enabled port count)
Worst-case media bandwidth (64 ports)	≈ 5.6 Mbit/s per direction

Capacity Guidance:

- Size the intercom network to hand peak simultaneous port usage.
- Validate license limits before deployment to avoid capacity constraints.

9.3 Network Quality Targets

Use the following targets to maintain consistent audio quality and conversational performance.

Metric	Target	Acceptable	Notes
One-way latency	<50 ms	<150 ms	Latency above ~150 ms degrades conversational turn-taking
Jitter	<10 ms	<30 ms	Excess jitter increases audio distortion and buffering

Metric	Target	Acceptable	Notes
Packet loss	<0.5%	<3%	G.711/G.722 provide limited loss tolerance; keep loss minimal

Design recommendations:

Engineer the network to meet target values, not just acceptable thresholds. Monitor WAN links continuously for latency, jitter, and packet loss.

9.4 QoS Recommendations

Apply the following Quality of Service (QoS) practices to prioritize intercom media traffic:

- Mark intercom WebRTC media as DSCP EF (46) at the network edge where you control the media path (LAN/WAN). Place this traffic in the voice queue end-to-end.
- Do not rely on DSCP markings across public internet paths (Scenario C). Instead, provision sufficient uplink bandwidth for TURN and signaling traffic and use a service with an SLA when possible.
- Use wired connections for production clients whenever possible. If Wi-Fi is required:
  - Enable WMM (Wi-Fi Multimedia)
  - Classify intercom audio traffic as voice priority

10 CPU Load Budgeting

ODIN uses a defined CPU load budget to control how many channels you can run and which channel types you can configure. Each channel consumes a portion of CPU based on its codec and transport method. ODIN evaluates the total CPU load of all configured channels and allows only configurations that stay within the system limit. This approach protects overall performance and prevents system overload.

10.1 Why Channel Limits Exist

An ODIN frame supports up to 64 channels, but all channels share the same CPU. Each channel type consumes a different amount of processing power:

- G.711 (narrowband) uses minimal CPU.
- G.722 (wideband) uses roughly twice the CPU of G.711.
- WebRTC channels add processing overhead for encryption and transport on top of the codec cost.

Because each channel type uses a different share of CPU, you cannot always run all 64 channels at the same time. ODIN calculates the total CPU load and enforces a strict CPU budget for all configured channels.
ODIN also enforces a fixed rule for wideband audio:

- Assign G.722 only to channels 1-32.
- If you assign G.722 to channels above 32, ODIN retains the previous codec setting.

This rule limits the system to a maximum of 32 G.722 channels, regardless of available CPU capacity.

10.2 CPU Cost per Channel

Each configured channel consumes a fixed percentage of CPU based on its codec. WebRTC channels include both codec cost and additional overhead:

- G.711: 0.7% CPU
- G.722: 2.0% CPU
- WebRTC + G.711: 1.2% CPU (0.7 + 0.5)
- WebRTC + G.722: 2.5% CPU (2.0 + 0.5)

ODIN adds the CPU cost of all configured channels:

- If the total stays at 87% or less, ODIN accepts the configuration.
- If the total exceeds 87%, ODIN rejects the configuration.

ODIN reserves the remaining 13% CPU to maintain stable system operation.

10.3 Channel Capacity by Configuration

The maximum number of channels depends on the codec mix:

Configuration	Maximum Channels	Limiting Factor
G.711 only	64	Hardware (48% CPU)
G.722 only	32	G.722 channel rule (64%)
WebRTC + G.711	64	Hardware (76.8% CPU)
WebRTC + G.722	32	G.722 channel rule (80%)

10.3.1 Example Configurations

32 × G.711

- Uses 22.4% CPU — well within budget.

32 × G.722

- Uses 64% CPU — within budget and at the G.722 limit. 64 × WebRTC + G.711
- Uses 76.8% CPU — allowed.

32 × G.722 + 32 × G.711

- Uses 86.4% CPU — this is the highest full-channel configuration within the limit.

32 × WebRTC + G.722 with additional channels

- First 32 channels use 80% CPU
- Remaining budget: 7%
- Add up to 5 WebRTC + G.711 channels (6%)
- Total: 86% → allowed
- Adding more exceeds the limit and ODIN rejects the configuration

Notice!
With WebRTC on wideband, you cannot use all 64 channels.

10.3.2 Mixed Configurations

You can combine channel types freely if you:

- Keep total CPU at or below 87%
- Assign G.722 only to channels 1-32

Examples:

- 20 × G.722 + 30 × WebRTC + G.711 = 76% → allowed
- 30 × G.711 + 20 × G.722 = 61% → allowed

Capacity Planning Guideline

Increase the number of wideband or WebRTC channels only if you reduce the total number of channels. These channel types consume more CPU and reduce overall capacity.

10.4 CPU Budget Exceeded

If a configuration exceeds the CPU limit, ODIN rejects the entire change and does not apply it. IPedit uses the same CPU budget values and warns you before you send a configuration that would be rejected.

11 Frequently Asked Questions

Q: Do I need a STUN or TURN server for use inside our facility?

No. On a LAN or fully routed corporate network, client and intercom connect directly. STUN/TURN only matter when NAT separates the client from the intercom — in practice, when crossing the internet.

Q: The browser shows a certificate warning when I connect. Is the connection insecure?

The connection is still TLS-encrypted, but the browser cannot verify the factory self-signed certificate's identity. Install a CA-signed certificate (Section 7.1) to remove the warning. Do not train users to click through certificate warnings on internet-facing deployments.

Q: Which browsers are supported?

Any current browser with standard WebRTC support. Use a recent release of a mainstream browser (Chrome/Edge/Firefox/Safari). For production positions we recommend standardizing on one browser and version-managing it like any other production tool.

Q: Can I change the signaling port 2083?

Not on the device. Externally you can publish any port you like by port-translating on your firewall or fronting the intercom with a reverse proxy (which must pass WebSocket upgrades).
Q: Why does my connection work from home but not from the office / hotel / mobile hotspot?
Strict (symmetric) NAT and UDP-blocking firewalls defeat direct paths and STUN. Deploy a TURN server (Section 6); the client can fall back to TURN over TCP/TLS on networks that block UDP outright. Note the intercom itself always reaches TURN over UDP — that leg is inside or adjacent to your network and under your control.

Q: Is the audio encrypted? Can the TURN server operator hear calls?

All media is DTLS-SRTP encrypted end-to-end between client and intercom. The TURN server forwards encrypted packets and has no access to keys or audio.

Q: How many remote users can connect at once?

Up to 64 WebRTC ports per ODIN frame, gated by your license. Each connected client occupies one port for the duration of the session.

Q: Does WebRTC replace RVON trunking or OMNEO?

No. WebRTC is a client-access feature for browsers and apps. Matrix-to-matrix trunking and device transport continue to use RVON/OMNEO.

Q: What happens if the direct media path fails mid-deployment — do users have to do anything?
No. If direct connectivity fails twice within 90 seconds, the intercom automatically switches new connection attempts to relay-only mode for 15 minutes. Users just reconnect; the system picks the reliable path.

Q: Can I run the TURN server in the cloud instead of our DMZ?

Yes. Any location works as long as (a) the intercom can reach it over UDP 3478 outbound, and (b) clients can reach it. A small cloud VM is sufficient; size the VM's network, not its CPU (Section 6.3).

Q: Does the feature use IPv6?

No, IPv4 only in this release.
Q: We use a TCP-mode SSL VPN for remote workers — can they use that instead of TURN? It will connect, but real-time audio over a TCP tunnel degrades badly under packet loss (latency spikes, audio gaps). Use the TURN architecture, or a UDP-based VPN, for production audio.

12 Troubleshooting

Symptom	Likely Cause	Action
Browser cannot load the client page at all	TCP 2083 blocked, or port-forward/proxy misconfigured	Verify reachability: curl -vk https://<address>:2083/api/info should return device JSON
Certificate warning	Factory self-signed certificate	Install CA-signed certificate (Section 7.1)
Login rejected immediately after several attempts	Brute-force lockout (5 attempts)	– Wait 30 seconds – Verify credentials – Check for other clients retrying with bad credentials from the same source IP/NAT
Login OK, but WebSocket fails	– Proxy not forwarding WebSocket upgrade – Session token expired (tokens are valid for 30 seconds, single use)	Verify proxy WSS support Check client-to-intercom clock path is not introducing >30 second delays between token issue and connect
Signaling connects, but no audio and the call drops after ~7 seconds	ICE cannot find any working path	LAN: – Check UDP allowed between client and intercom VLANs Internet: – Verify TURN server reachability from both the client and the intercom (UDP 3478), and TURN credentials
Audio works on LAN, fails for remote users	No TURN server or TURN server is unreachable from one side	– Deploy/verify TURN per Section 6 – Test with turnutils_uclient from both network zones
One-way audio	Asymmetric firewall rules or ALG interference	Disable SIP ALG/VoIP helpers Check UDP allowed both directions Confirm state return-path rules

Symptom	Likely Cause	Action
Audio drops after a few minutes of silence	Firewall UDP session timeout too aggressive	Raise UDP time out to ≥90 seconds for media/TURN flows
Choppy/robotic audio	– Packet loss or jitter on the path – Wi-Fi interference – TCP-tunneled VPN	– Check Section 8.3 targets – move client to wired – eliminate TCP tunnels – verify TURN server link is not saturated

Symptom	Likely Cause	Action
Remote connections intermittently take longer path (higher latency)	Automatic relay fallback engaged after direct-path failures	– Expected behavior – Investigate why direct paths fail (NAT type, firewall) if direct paths are desired. – Fallback clears after 15 minutes
Connections refused when many clients connect from one site	Per-source-IP pre-authentication cap (8)	Expected protection behavior, stagger connection attempts, or ensure clients complete login promptly

Diagnostic quick wins

Confirms signaling reachability and returns device identity, without credentials.	**https://<intercom>:2083/api/info**
Shows ICE candidate types in use. relay = TURN path; srflx = STUN-discovered direct path; host = LAN-direct.	chrome://webrtc-internals (or about:webrtc in Firefox) on the client
Validates TURN allocation from any test host (part of coturn)	turnutils_uclient -u <user> -w <pass> <turn-ip>

13 Deployment Checklist

All deployments

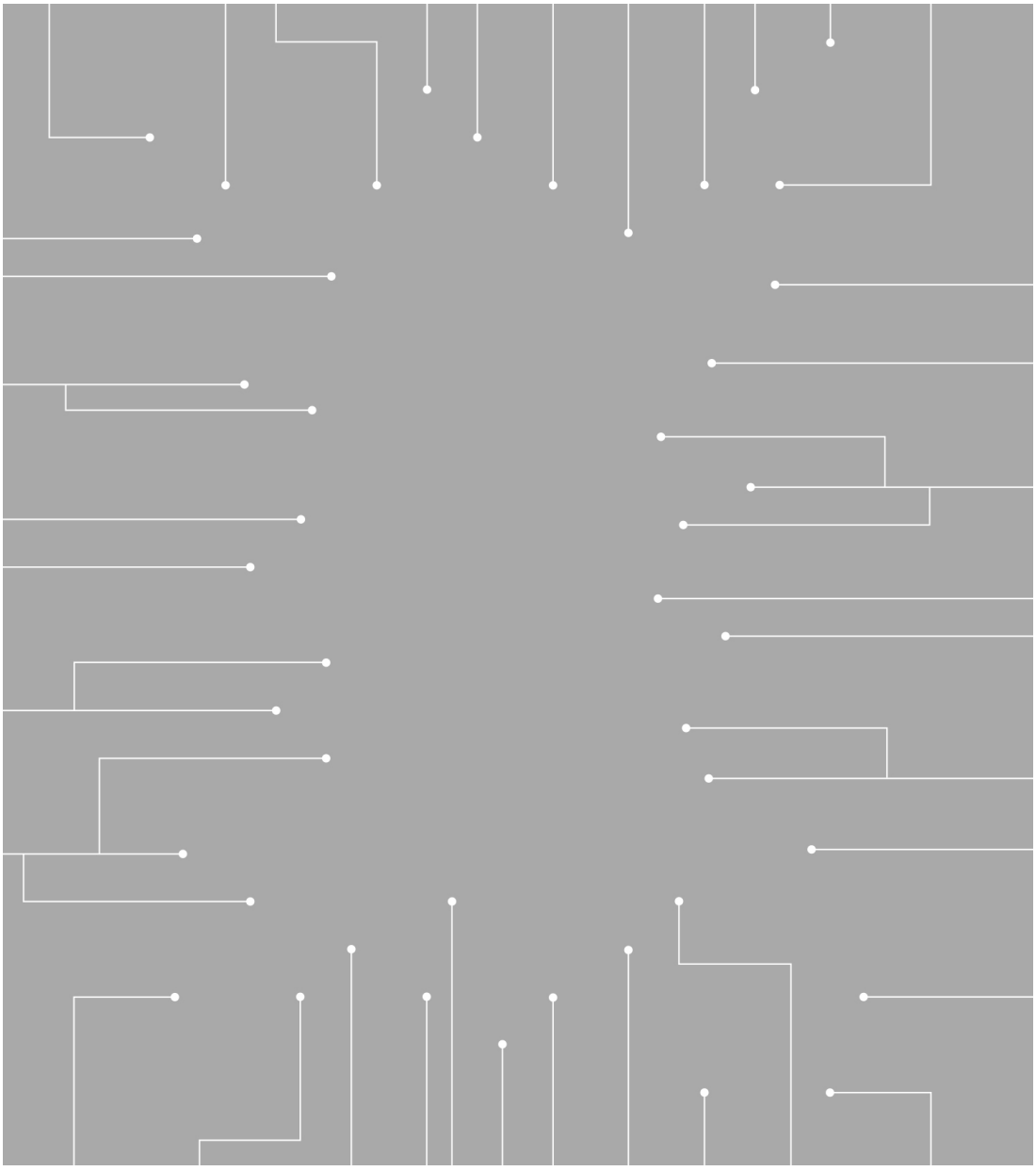
- Intercom reachable from client network on TCP 2083
- WebRTC ports licensed and per-port credentials configured
- CA-signed TLS certificate installed (production)
- SIP ALG / VoIP helpers disabled on firewalls in the path
- Firewall UDP session timeout ≥ 90 seconds

Internet / remote access additionally

- TURN server deployed (DMZ or hosted) with long-term credentials
- TURN reachable on UDP 3478 from both clients and intercom
- TURN relay port range (e.g., UDP 49152-65535) open inbound to the TURN server
- TURN allowed-peer-ip restricted to the intercom (and other permitted endpoints)
- STUN/TURN entries configured on the intercom and verified in a test call
- DNS name + matching certificate for the published signaling endpoint
- Test from a representative remote network (home ISP, mobile hotspot) — verify candidate type in chrome://webrtc-internals
- Bandwidth budget confirmed: ≈ 87 kbit/s per direction per call; 2× per relayed call at the TURN server

14 Glossary

Term	Definition
ICE	Interactive Connectivity Establishment - negotiation that finds a working media path (RFC 8445)
STUN	Session Traversal Utilities for NAT — lets an endpoint discover its public IP/port (RFC 5389)
TURN	Traversal Using Relays around NAT — a media relay used when no direct path exists (RFC 5766)
Trickle ICE	Sending connectivity candidates incrementally as they are discovered, for faster call setup.
DTLS-SRTP	Encrypted media: SRTP keys negotiated via DTLS handshake (RFC 5764)
WSS	WebSocket Secure - TLS-protected WebSocket, used here for signaling
Host / srflx / relay candidate	ICE path types: direct LAN address / public address discoverable via STUN / TURN-relayed address
Symmetric NAT	NAT type that defeats STUN-based traversal; requires TURN
HSTS	HTTP Strict Transport Security - browser policy pinning the endpoint to HTTPS



Electro-Voice Dynacord LLC 12000 Portland Avenue South MN 55337 Burnsville
USA

www.rtsintercoms.com [http://www.rtsintercoms.com/]

EU importer:

EVI Audio GmbH
Sachsenring 60
94315 Straubing Germany