



APPLICATION GUIDE

AURI™ FOR COURTROOMS

AURIAUDIO.COM

AMPETRONIC

LISTEN
TECHNOLOGIES

DEPLOYING THE AURI™ SYSTEM IN COURTROOMS FOR ACCESSIBLE AND CONTROLLED AUDIO DISTRIBUTION

Courtrooms require audio systems that provide clear speech intelligibility and accessibility while maintaining appropriate control over who can access proceedings.

Traditional loudspeaker-based approaches can create challenges including:

- Reduced intelligibility due to room acoustics
- Limited accessibility for hearing assistance users
- Difficulty supporting interpretation or overflow spaces
- Concerns around unauthorized listening in sensitive proceedings

This application note outlines a recommended method for deploying the Auri™ system to deliver courtroom audio while implementing operational controls for privacy, coverage, and listener access. Supported receiver controls include Library Lock, Channel Lock, Auto Connect behavior, and broadcast filtering to limit available listening options.

WHY SECURITY MATTERS IN COURTROOM AUDIO

Security is a critical consideration in courtroom environments because audio may contain sensitive testimony, privileged discussions, confidential case details, or proceedings that are legally restricted to specific participants. Unlike many public listening environments, courts often need to balance accessibility with controlled distribution of information.

Auri™ helps address this challenge in various ways:

1. Encrypted audio - The live broadcast can be encrypted with a Privacy Key as to restrict general access to audio.
2. Coverage optimization - Output power from the transmitter can be reduced to match the room requirements and hence reduce unwanted spill into other room/areas.
3. Receiver controls - If using the RX1 as a receiver, this can be locked down to only access a specific channel or auto-connect to a pre-determined channel. Which eliminates unwanted connections to the wrong broadcast.
4. Restricting access via QR or NFC - Third party devices can be controlled by way of providing the broadcast ID and encryption key via a QR code or NFC tag within the room or at a controlled access point to ensure the right people access the right audio.

Together, these controls help courts improve accessibility and speech intelligibility while maintaining appropriate safeguards for privacy, courtroom integrity, and operational control.

EQUIPMENT / MATERIALS

Required components:

- Auri™ Transmitter(s)
- Auri™ Receiver(s) (optional for managed deployments)
- Auri™ management software
- Audio source (courtroom DSP, mixer, microphone system, or AV processor)
- Network connection (if centralized management is required)
- Compatible listener devices (where permitted)

DEPLOYMENT PROCEDURE

Step 1 - Define Listening Zones

Identify how audio access will be managed.

Typical zones:

- Public gallery
- Jury seating
- Interpretation services
- Overflow rooms
- Restricted hearing spaces

Determine which areas require open access and which require controlled access.

Step 2 - Configure Broadcast Access

Select one of the following operating models:

Open Broadcast

- Users connect to available courtroom audio
- Recommended for public proceedings and accessibility applications

Managed Access

- Court-issued receivers are preconfigured for approved broadcasts
- Recommended for sensitive environments

While dedicated court-managed receivers can prevent users from scanning channels and provide the highest level of control, courts may increasingly need to support approved users connecting with their own compatible devices as Auracast adoption grows.

Access can remain controlled by authorizing users at courtroom entry or a designated security point and providing connection credentials only to approved individuals. Access methods may include restricted QR codes, NFC-based connection where supported, or other controlled onboarding processes. Combined with encrypted broadcasts and Privacy Keys, this approach helps maintain accessibility while protecting sensitive courtroom audio.

Step 3 - Configure Privacy Controls

Where proceedings require additional protection:

- Enable encrypted broadcasts using Privacy Keys
- Assign unique keys for restricted proceedings
- Distribute authorized access credentials only to approved listeners

Step 4 - Design Coverage and Range

Range should be treated as a coverage parameter—not a security mechanism.

Recommended deployment practices:

- Adjust transmitter output to match courtroom size
- Position transmitters centrally
- Validate coverage at courtroom boundaries
- Use multiple lower-power zones where separation is required

Physical construction and RF conditions will affect final coverage performance.

Expected Results

When deployed using this method, courts can expect:

Requirement	Expected Outcome
• Speech intelligibility	• Improved direct audio access
• Accessibility	• Support for assistive listening
• Privacy	• Restricted listener access where required
• Operational control	• Managed receiver behavior
• Scalability	• Support for multiple courtroom configurations

Recommended Safeguards for Sensitive Environments

For higher-security proceedings:

- Use encrypted broadcasts
- Issue court-managed receivers
- Enable receiver channel restrictions
- Minimize RF coverage outside intended areas
- Limit administrative access to authorized personnel
- Establish procedures for rotating Privacy Keys between proceedings

Conclusion

The Auri™ system provides courts with a practical method for delivering accessible courtroom audio while supporting operational controls appropriate for judicial environments. By combining controlled broadcast access, receiver management, configurable coverage, and optional privacy controls, courts can improve listening experiences while maintaining appropriate control over audio distribution.