GatesAir Service

Bulletin

EQUIPMENT:	All Gatesair Equipment that can be networked on a wide area network or local area network.	**BULLETIN No:**	GA-001
		PART No:	7734520047
		DATE:	16DEC2025
UNIT(S) AFFECTED:	All Gatesair Transmitters, Exciters and Ancillary devices that can be networked.	**ECO:**	73872
		REVISION:	A
		PAGES:	Page **1** of **2**
PURPOSE:	This Service Bulletin formally advises customers that GatesAir transmitters and associated control systems must not be directly connected to or exposed to the public internet.		

Review the following documentation thoroughly prior to implementing.

ATTENTION:

All work pertaining to this bulletin must be carried out by a trained competent person using appropriate skills, knowledge, and experience for their own safety and that of others as well as what is adequate for successfully working on the equipment and installation.

"Competence of Personnel" as defined in the IEC-60215:2016 Safety Standard

Introduction: GatesAir transmitters may be remotely accessed through secure network architecture but must not be directly exposed to the public internet

---

Reasons Why:

1. Direct exposure increases the risk of unauthorized access, configuration changes, and service disruptions.
2. Unauthorized access may affect RF output and system interlocks, posing risks to equipment and personnel.
3. Licensees are responsible for secure transmitter control to maintain regulatory compliance.

What is supported:

GatesAir transmitters may be internet-reachable *only when access is mediated by security controls*, such as:

- VPN (client or site-to-site)
- Firewall with default-deny rules
- Isolated management network or VLAN
- Secure jump host / bastion PC
- Centralized NOC systems behind protected infrastructure

In these cases:

- The transmitter has no public IP
- No ports are open to the internet
- Access is authenticated, logged, and controlled

This is a supported and recommended architecture.

What is NOT supported:

GatesAir does not support transmitters being internet-facing, including:

- Direct public IP assignment
- Port forwarding from the internet to transmitter interfaces
- Exposing HTML GUI, SNMP, SSH, or service ports to the open internet

Even if:

- Passwords are set
- HTTPS is enabled
- Access “seems to work”

If the internet can initiate a session directly to the transmitter, the transmitter is internet-facing — and that configuration is not supported.

Service Bulletins and Application Guides are available on the GatesAir support Portal at https://www.gatesair.com/ click ‘CUSTOMER LOGIN’.