Infinium® Auracast Security

Auracast utilizes AES-128-CCM encryption, which is considered cryptographically sound, to implement optional public broadcast encryption. The data is encoded and decoded with two 128 bit (16 byte) keys: the Group Session Key (GSK) and the Group Long-Term Key (GLTK). The GSK is effectively transmitted in the open. The GLTK is derived from the Broadcast Code (i.e. password).

The Williams AV implementation of the broadcast code uses 6 digits of numeric values 0 through 9. This provides one million possible combinations. Assuming an unsophisticated brute force attack taking 1 second to confirm success/failure status, it would take 11.6 days to try all combinations.

Revision History:

Rev	By	Date	Description	ECO
0	KWC	4/7/2026	Initial Release	N/A
1	PBP	4/23/2026	Edits for length and style	N/A

Author: Keith W. Carlson