



How is RAVIN secured?

The information in this article applies to:

RAVIN (all versions), RAVIN Management Server, RAVIN Media Server

Summary

Discusses built-in RAVIN security capabilities.

Content

RAVIN system security is influenced by several factors. These include the physical infrastructure that the application runs in, the policies and procedures adopted and enforced by the users of the application, and the product security features of the product itself.

Physical Infrastructure

The first line of defense in any network application deployment is to ensure that the network and the devices connected to that network are secure. In this area, RAVIN relies on the inherent security features of the network such as IPSEC, VLANs, VPNs, switch port authorization, routing security, etc. Together with inherent network security features, the security of the devices such as computers and servers connected to that network need to be ensured as well. This includes placing devices in secured facilities, use of secured operating systems, and other administrative tasks related to security of the computer network infrastructure.

Policies and Procedures

This heading covers a variety of security measures that are implemented by organizations wishing to ensure the security of their communications networks. Such measures include secured operating system software for computers, government-certified end-user and server applications, software firewalls, and training for end-users. In addition, certain organizations implement varying levels of clearance that make sensitive information and applications available only to those people that are authorized for their use.

Product Security Features

Under this heading, RAVIN's built-in security features make it a compelling application for use in secured environments. These include:

- Support for Secure Sockets Layer (SSL) for all data interaction with the RAVIN Management Server.
- User name and password hash codes stored in a securable database.

- Sensitive information encrypted in the database.
- User authentication via LDAP systems.
- User-by-user assignment of RAVIN Channels.
- User-by-user assignment of individual privileges on each Channel they have access to talk. For example: listen-only, or talk and listen.
- High-speed, low complexity, 40-bit proprietary media stream encryption algorithm.
- US Government standard AES 128, 192, and 256 bit media stream encryption.
- “Black-box” media stream encryption via customer-provider encryption logic.
- “White list” acceptance of telephone calls into the system.
- Built-in Multi-level PINs on RAVIN Media Server sessions.
- Media Server access authorization via customer-provided authentication logic.
- Customizable Media Server scripting to meet customers’ security needs.
- Real-time encryption key rotation on Channels.
- Real-time audio notifications of secrecy levels of conference sessions based on participants’ security levels.

Created: 2004-08-03

Last Reviewed: 2005-03-18

Keywords: RAVIN secure security AES encryption SSL LDAP encrypt PIN key secrecy