RoomWizard Security

Thank you for your interest in RoomWizard. Below is a summary that details both the physical security of the device to keep hardware safe, and network security to avoid potential threats and cyberattacks. This document gives a brief overview of what RoomWizard is, what RoomWizard stores and what we are securing. If you have further questions regarding RoomWizard security, please contact your regional Technology Sales Consultant.

What is a RoomWizard?

- RoomWizard is an embedded device that solves the dilemma of connecting workers to meeting spaces. The device is installed outside of a meeting space to physically display its availability and schedule. RoomWizard also works with a variety of calendaring systems including Microsoft Outlook, while giving individuals the ability to book an available space using the touchscreen on the device.
- A synchronization package, also known as a connector, is a piece of software that enables RoomWizards to stay synchronized with a room's calendar inside an existing scheduling system, such as Microsoft Exchange. When there is a change to that space's calendar, either made in the scheduling system or at the RoomWizard itself, the connector allows the two entities to stay in sync. Connectors are not installed directly on the scheduling system.
- RoomWizard Administrative Console manages the implementation and ongoing operation of multiple RoomWizard devices. Steelcase developed this software for the benefit of our customers' IT needs.
- For more information about the RoomWizard infrastructure, including diagrams and the Implementation Journey, please see the "RoomWizard Technical Infrastructure Guide."

Our approach to RoomWizard technology has been to develop a product that has a minimal security profile and follows general security best practices. The Steelcase development team works to stay informed on trends in IT security and will respond to vulnerabilities by updating software and firmware when necessary.

Below are a few specific ways RoomWizard has been made secure.

SOFTWARE SECURITY

- The RoomWizard device runs a version of Ångström Linux (a distribution specifically designed for embedded devices) that has been customized and hardened.
- There is no secret handshake. From in front of the device, there is no way to use RoomWizard as anything other than a scheduling system interface. No amount of interaction or combination of activity can bring down the RoomWizard application interface, exposing the Linux OS beneath.
- HTTPS – During normal operation, a RoomWizard will establish communication with the connector software via HTTP or HTTPS.
- If an organization chooses to use HTTPS, it can import its own SSL Certificates.
- TLS 1.2 and SSL encryption up to 2048-bit, SHA1.

To ensure that RoomWizard devices and supporting software do not introduce unnecessary security vulnerabilities, Steelcase works with an independent security auditing organization to perform Security Vulnerability Testing and Risk Assessment.

HARDWARE SECURITY

- RoomWizard has no wireless communication hardware. The current-generation RoomWizard device (RW20) only has the hardware ability to communicate via a single RJ-45 Ethernet port on the back of the device. Because there is no wireless communication hardware, there is no possibility of an attack over the air.
- Kensington locks can be attached to the bottom of every RoomWizard device to prevent theft.
- Micro USB port on the bottom of the device can be disabled via the device configuration. The port exists as a method for imaging the device during the manufacturing process.
- Mounting hardware (included) enables the RoomWizard to be affixed securely to its mounting surface and also conceals the network connection.

What is stored and secured on a RoomWizard?

Meeting room usage information is stored locally on the device, to be retrieved later by the RoomWizard Analytics Console for reporting purposes. This data includes meeting times, organizer name and email address, number of attendees, attendees' names and email addresses.

The SSL certificate, if one has been uploaded to enable HTTPS communication, is stored locally on the device.

Device configuration includes information such as the connector URL, name of the calendar that the device synchronizes with, and credentials for the RoomWizard service account that authenticates the scheduling system and the specific calendar that is synced. Optional information that could be configured and stored on the RoomWizard includes an SMTP server address and credentials, an LDAP server address and credentials, and an FTP server and credentials (used for device backups).