SpaceLogic™
Touchscreen Room Controller

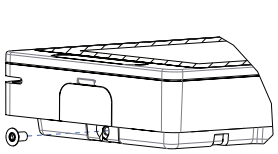
Cybersecurity Hardening Guide

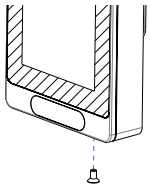
Physical Security

Security Screw

☐ It is important to install the security screw on the bottom of the unit.

If this screw is not installed:
- The device could be stolen.
- An attacker could potentially access the RS-485 communication bus and perform unauthorized actions on the communication network.
- The device could be factory reset by an unauthorized person.



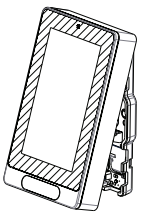


RS-485 Wiring (BACnet/MSTP and Modbus RTU)

☐ BACnet/MSTP and Modbus RTU networks rely on the physical security of RS-485 wiring. It must therefore be installed behind physical barriers, so it is only accessible to authorized personnel.

An attacker with access to the RS-485 communication bus could potentially perform unauthorized actions on the communication network.

RS-485 wiring is present on the base board, so access must be limited to authorized personnel only. Install the security screw, as described in the previous section.



NOTICE

ACCESS TO RS-485 WIRING

Access to the RS-485 wiring of the BACnet/MSTP or Modbus/RTU network gives access to configure, upgrade, read logs or write files to the Touchscreen Room Controller. This must be restricted to authorized personnel only.

Failure to follow these instructions may lead to unauthorized users modifying the firmware or the configuration of the Room Controller.

Communication Networks

Disabled Unused Communication Networks

☐ BACnet/MSTP and Modbus/RTU are disabled by default and should be left disabled on the Touchscreen Room Controller if they are not used.

BACnet and Modbus can be disabled in the Network menu for the Touchscreen Room Controller.

NOTICE

NOT A SECURITY SYSTEM

While the Touchscreen Room Controller supports various sensors (PIR Motion, Door/Window, Water Leak), any alarming or notifications are best effort only. The Touchscreen Room Controller is NOT a security system, and no guarantees are given that an alarm will be generated or delivered to the Building Management System (BMS) or higher-level systems.

Failure to follow these instructions may lead to system failure.

Wi-Fi

Networks

☐ IP networks should be carefully planned and managed to minimize risks:
- Reference: Guidance on Implementing a Cybersecure BMS Architecture with EcoStruxure Building Operation.
- Use VLANs and firewalls to separate networks.
- Separate building control networks from networks or devices that:
  - Are critical systems.
  - Contain payment or private data.
  - Are publicly accessible (e.g., to guests or staff).
- Limit or disable external access to building control networks.

Touchscreen Room Controller

☐ Recommendations:
- Wi-Fi is disabled by default and should only be enabled when required.
- Regularly update your TRC firmware to ensure the latest Wi-Fi security enhancements are in use.
- TRC supports the following security protocols:
  - WPA2-personal
  - WPA3-personal (Recommended).
- TRC does not support connecting to Wi-Fi networks using the following insecure security protocols:
  - No security
  - WEP
  - WPA
- When a TRC is removed from a Wi-Fi network, ensure all security material is removed by performing:
  - “Disconnect and forget” from the Wi-Fi menu, or
  - Factory reset:
    - Full factory reset via reset pin, or
    - Software factory reset via Device info menu, with `Network` selected.
- Wi-Fi can be disabled and re-enabled in the Network menu. Disabling Wi-Fi does not remove network information from the TRC.
- All wireless networks are vulnerable to interference and jamming, which can block or disrupt communication. Carefully consider if wireless communications are appropriate for your application.

BACnet/IP

☐ BACnet/IP relies on security of the IP network:
- The device is intended to operate on a private IP network, without external connectivity, or protected by security aware device(s).
- Use VLANs and firewalls to separate the BACnet/Ip network.
- Prevent access to the network by authorized people and devices by physically protecting IP cabling and managing wireless network access.
- Monitor your network to check for unexpected devices or traffic.
- Do not enable BACnet/Ip on a public network.

NOTICE

UNAUTHORIZED ACCESS

It is very important to plan and manage the BACnet/IP network according to the above guidelines.

Failure to follow these instructions may lead to unintended access to the Room Controller.

Ping

☐ Ping is a useful debugging tool for IP devices, but it can also be used by attackers to perform DDoS attacks to overwhelm a device and attempt to disable it.

To prevent or reduce ping attacks, it is recommended to:
- Use a firewall to shield your network from malicious or unnecessary network traffic.
- Block ICMP ping in your firewalls. This prevents pings from external devices entering your network.
- Add filters to your firewall or router to drop packets from unknown sources.
- Use network monitoring software to detect unusual traffic patterns on your network.

Zigbee

☐ ZigBee is disabled by default and should only be enabled when required.

ZigBee sensors that are no longer used should be removed from the TRC.

ZigBee networks configured for “normal” security are vulnerable to sniffing attacks while Permit Join is active. Ensure Permit Join is only activated when necessary, then deactivate immediately afterwards.

All wireless networks are vulnerable to interference and jamming, which can block or disrupt communication. Carefully consider if wireless communications are appropriate for your application.

User Management

Best Practices

☐ Accounts should not be shared between users. Unique accounts should be created for each user.

☐ When a user is no longer needed (e.g., employee leaves), their account should be removed.

☐ User accounts should be created with roles allowing the least privileges required to perform their tasks.

Roles	Administrator	Technician
Factory Reset via Menu	✓	⊘
General HVAC/device configuration	✓	✓
Lua – Enable remote device access	✓	⊘
Manage users	✓	⊘
Test terminals	✓	✓
USB access	✓	⊘
View status/service information	✓	✓

☐ Passwords should not be obvious or repeated on many devices.

☐ Do not use 1234, or the street number of the site.

☐ Segment devices by area, do not use the same passwords on all devices.

☐ Wipe screen after use to avoid fingerprints from password entry remaining on the screen.

☐ Consider regional privacy requirements when creating user and display names, as user names will appear in event logs.

☐ Ensure user names are unique to help ensure clear traceability. For example, avoid creating both “User1” and “User 1”.

☐ Regularly delete the account or downgrade the role of users who no longer need access to the device.

☐ Update passwords regularly.

Other Scenarios

☐ If shared accounts are used (e.g., for a maintenance team in a large hotel), shared accounts should not have Admin privileges.

Impacts of Shared/Common Passwords

☐ Shared accounts make it unclear who accessed the devices; if someone acts in bad faith, it is not possible to detect who it was.

☐ It is difficult to track who knows the common password, and hence when it should be changed.

☐ If the password is disclosed externally, all users of the shared account will be affected by the required password change.

Store Administrator Passwords Securely

☐ If all administrator passwords are lost, then the device must be factory reset manually by holding the reset button while powering on the device.

For more information, refer to the Touchscreen Room Controller Installation Sheet.

Log Files

The Touchscreen Room Controller contains two log files:

- System Log: Status of the system, including any errors.
- Audit Log: Record of changes made to the system, and by whom.

If unexpected issues occur, log files should be reviewed to determine the cause.

NOTICE

CONFIDENTIAL DATA IN LOG FILES

Log files may contain private or confidential data:
- Encrypt log files before transmitting them.
- Ensure log files are removed when decommissioning devices.

Failure to follow these instructions may lead to the unauthorized sharing of private or confidential information.

Firmware Updates

NOTICE

UNAUTHORIZED ACCESS

The Touchscreen Room Controller firmware should be updated regularly to ensure the latest security improvements are applied.

Failure to follow these instructions may result in unauthorized access to the device.

Lua

NOTICE

UNAUTHORIZED ACCESS

Lua scripts allow customization of the device behavior, but come with risks:
- Only use scripts that are required for your device or site.
- Only use scripts that you understand or are from a trusted source.
- Remove scripts that are no longer required.
- Check scripts contain only the code you need and meet the recommendations of the Lua4RC Programming Guide.
- Carefully review and test scripts before deploying to sites.

Lua scripts can read and write data points on remote BACnet devices:
- Interacting with remote devices increases the scope of the Lua script and hence the risk of unintended behavior.
- Lua access to remote devices is disabled by default. If required, Remote Device Access must be enabled by an Admin in the Lua/Status menu.
- Lua access to remote devices should only be enabled if required.

Excessive writing of non-volatile priority levels may wear out the device's EEPROM memory. Refer to the Lua4RC Programming Guide for more information.

Failure to follow these instructions may result in poorly-written or malicious Lua scripts, which may damage the device or result in unintended behavior.

Decommissioning

To decommission a device:

1. Factory reset:
   - Launch a factory reset to remove all data:
     a. Log in as an administrator.
     b. Tap on Device Info, then Factory Reset, ensuring all categories are selected.
   - Or perform a physical factory reset by holding the reset button while powering on the device. For more information, refer to the Touchscreen Room Controller Installation Sheet.

2. Refer to the End-of-Life Instruction (EoLi) document for information on how to recycle or dispose of the product.

NOTICE
DECOMMISSIONING A DEVICE It is important to decommission a device properly to ensure that no confidential data is left on it. **Failure to follow these instructions may lead to the unauthorized sharing of private or confidential information.**

Reporting an Incident or Vulnerability

Please report any cybersecurity incident or vulnerability via the Cybersecurity Support Portal on www.se.com.

The Schneider Electric Security Operations Center (SOC) operates 24 hours a day, 7 days a week, year-round, and is staffed with security analysts who receive and triage your reports.