COOLAUTOMATION

# COOL AUTOMATION SECURITY BRIEF

## SECURITY HIGHLIGHTS

Secure & Authenticated communication channel

-

Data encrypted at transit

-

TLS 1.2 & Encryption compliant with **NIST standards**

-

Secure FW updates

-

Full control over Remote Management

-

Secure Cloud Infrastructure

-

Data encrypted at rest

Cool Automation (CA) incorporates the highest industry standards for the security of the CoolMaster* devices and the CoolRemote Cloud architecture. CA's security strategy includes secure communication, encryption and authentication, and general network security policies which eliminate most attack vectors and surfaces.

## CoolMaster Device Security

### COMMUNICATION

CoolMaster family of devices protect customer's data in transit by using an industry standard secure transport protocol (TLS 1.2) for communicating with CA's cloud. Each device has a unique and random key, which is authenticated by the cloud upon connection. The cipher suites used in the TLS protocol and the TRNG used for the unique key generation meet the NIST SP 800-52 and NIST SP 800-22 requirements respectively.
The CoolMaster devices don't accept incoming connection requests. This restriction eliminates most remote attack vectors against the device.

### FIRMWARE UPDATE

By default, the devices only allow firmware updates by physical access (USB). Remote firmware update is supported only if enabled using the physical LCD Touch Screen on the CoolMaster device, or through the secured connection with the CoolAutomation cloud infrastructure.

### REMOTE MANAGEMENT

The Remote Management Interface is disabled by default and can only be enabled using the physical LCD Touch Screen on the CoolMaster device.
When enabled, the Remote Management Interface uses the safe and secure communication protocols described in the "Communication" section.

## CoolRemote Cloud Security

### NETWORK ISOLATION AND SECURITY

The cloud is built on AWS infrastructure and uses AWS security features, such as firewalls and Security Groups, to restrict incoming connections to CoolMaster devices and CA employees only.
Only TLS 1.2 connections are accepted for the device interface. The devices are authenticated by their unique keys, as described in the device "Communication" section.
Management connections are accepted from CA offices only and are authenticated using asymmetric cryptography in accordance with Public Key Infrastructure industry security standards.

### CLOUD ENCRYPTION

Data stored in the cloud is protected at rest using database encryption. The encryption is provided by AWS, and CA's other vendors and meets the highest requirements of industry standards.

*All security measures mentioned apply to CoolMasterNet, CoolMaster-LT, CoolMaster, CoolMasterPRO and CloudBox communication devices

COOLAUTOMATION