

Cloud Link Roadrunner

Enclosure Management Solutions

The Cloud Link Roadrunner™ is an IoT device, purposely built for enclosure management. Built with a focus on cybersecurity, management, and physical security, the Cloud Link Roadrunner is the first of its kind. Designed to withstand the rigors of daily use and extreme environments such as very high or low temperatures and change in weather conditions, it allows facility and infrastructure managers to deploy secure, capable, and expandable access control capabilities across their enclosures. The Cloud Link Roadrunner IoT device supports multiple containerized applications and services, and manages local inputs and outputs, as well as access control hardware. It's a hardened, cybersecure device with all communications secured using TLS 1.3 and authenticated with a certificate. Hardware encryption secures data confidentiality and Secure Boot is used to protect against cyberattacks and malware.



Key features

- Supports up to 10,000 cardholders
- IoT device built for enclosure management
- Extreme temperature and vibration rating
- Expandable capability through containerization
- Network breach operational resiliency
- Embedded threat level management
- Dynamic (DHCP) or static IP addressing
- Encrypted communications with host software
- OSDP Secure Channel
- Cyberattack and malware protection
- Encrypted customer data at rest and in transit
- Secure web interface for basic configuration
- Supports up to two enclosure openings
- Various mounting options

Key benefits/applications

The Cloud Link Roadrunner is designed to meet the specific needs of an enclosure environment. It seamlessly connects to Security Center Synergis™, providing real-time monitoring of events and alarms, advanced cardholder and contractor management, and comprehensive reporting and traceability.

Small form factor

Built to support limited space deployments. It can be mounted on a shelf, wall, c-channel, and 1U rack, with the option to mount up to three devices on a single 1U shelf.

Cybersecure

Secured communications with TLS 1.3 and certificate-based authentication. Hardware encryption secures data confidentiality, and Secure Boot is used to protect against cyberattacks and malware.

IoT platform focused on the future

As an IoT device it's focused on the ability to support internal and third-party applications, allowing it to expand its capabilities without having to change hardware.

Industry Specific Design

Specifically designed to manage enclosures — from traffic and telecommunications cabinets to data server racks. It's NEMA TS2 (National Electrical Manufacturers Association) compliant, which means it can withstand hostile environments and temperatures.

Hardware specifications

Processor	Quad core, 64-bit CPU
System memory	1 GB RAM 4 GB flash storage
Communications	One 10/100BaseT Ethernet Port Two RS-485 (two wire for card reader)
IOs	Two (2) 24v outputs for controlling two HES 630REL (or equivalent) Two (2) normally open inputs for door position sensors Two (2) form C relay (2A max. 30Vdc) Four (4) configurable inputs · Digital normally open · Supervised with 4.7K Ohms EoL
Power output	12Vdc (max 240mA per card reader)
Power input	24Vdc +/-10% (420mA mean / 724 mA Peak)
Mechanical	Appliance dimension (WxLxH) · 126mm (150mm with wall bracket) X 152mm X 37mm Appliance weight 375g
Environment	Temperature Operating -40C to 74C Relative humidity non-condensing 5% to 95%

Certifications

Vibration	IEC 60068-2-64 NEMA TS-2 2.2.8.4
Shock resistance	IEC60068-2-27 NEMA TS-2: 2.2.9
Temperature	IEC 60068-2-1 Tests Ae and Test Ad IEC 60068-2-2 Test Be IEC 60068-2-14 Test Na NEMA TS-2 2.2.7.5, NEMA TS-2 2.2.7.3
Ingress protection	IEC 60529 IP2x
Electromagnetic Emissions and Immunity	FCC Part 15 Subpart B ICES-003. CISPR32/EN 55032 EN 50130-4
CE Marking	EMC Directive 2014/30/EU; RoHS Directive 2011/65/EU (including EU Directive 2015/863)

