CAPTIVEAIRE Commercial Ventilation Technologies

CASLINK SECURITY FEATURES

CASLink Website & APIs

Customer Access

- Multifactor authentication required for customer access.
- Visibility into all connected user access devices.
- Enforcement of security standards for user devices before granting access.
- User and device access audit logs.

Data Authorization

- Multitenant data authorization policies protect access to data from separate tenants and unauthorized employees.
- Authorization policies protect access to features from unauthorized users.

Microsoft Azure Application Proxy

Private Network

- Enhanced protection of sensitive employee features through Microsoft Azure Application Proxy.
- Sensitive employee features are kept on CaptiveAire's private network, inaccessible from the internet and thus from potential hackers.

Microsoft Azure Active Directory

Employee Access

- Multifactor authentication required for employee access.
- User access audit logs.

Encryption

- SSL required for all user connections to CASLink.

CASLink IoT Device

Zipit Wireless IoT

Secure Cellular Connection

- Secured cellular connection for sending and receiving data from IoT devices.
- Provides isolation from a facilities network.

Microsoft Azure IoT Hub

IoT Security

- Per device authentication.
- Security-enhanced communication channel for sending and receiving data from IoT devices.
- Over-the-air deployment of updates to help keep IoT devices up to date and secure.

Encryption

- AES-256 Encryption for one way telemetry device streams over UDP to CASLink.

*Device streams over UDP for sending telemetry data will be deprecated in the future and replaced with Microsoft Azure IoT Hub.