SquareOne

Security

Security took center stage throughout the creation, implementation, and operation of SquareOne, our device management software. We worked closely with external security experts to architect a strong security framework.

Effective security of a connected system needs a multi-layered approach and a consideration for the whole lifetime of operation. Here are some key areas:

Device onboarding

All new devices are required to undergo a certificate exchange process and register with the system.

- **Certificate Challenge:** Genuine devices possess certificates verified by a TLS challenge against SquareOne's trusted device list. These certificates can be unique per device (individual) or shared among a device model (batch) for streamlined manufacturing and provisioning.
- **2-Stage Authentication:** An optional security measure mandates device approval post-certificate validation. This can be executed by a local administrator or automated using device information like serial number and MAC address.

Data encryption

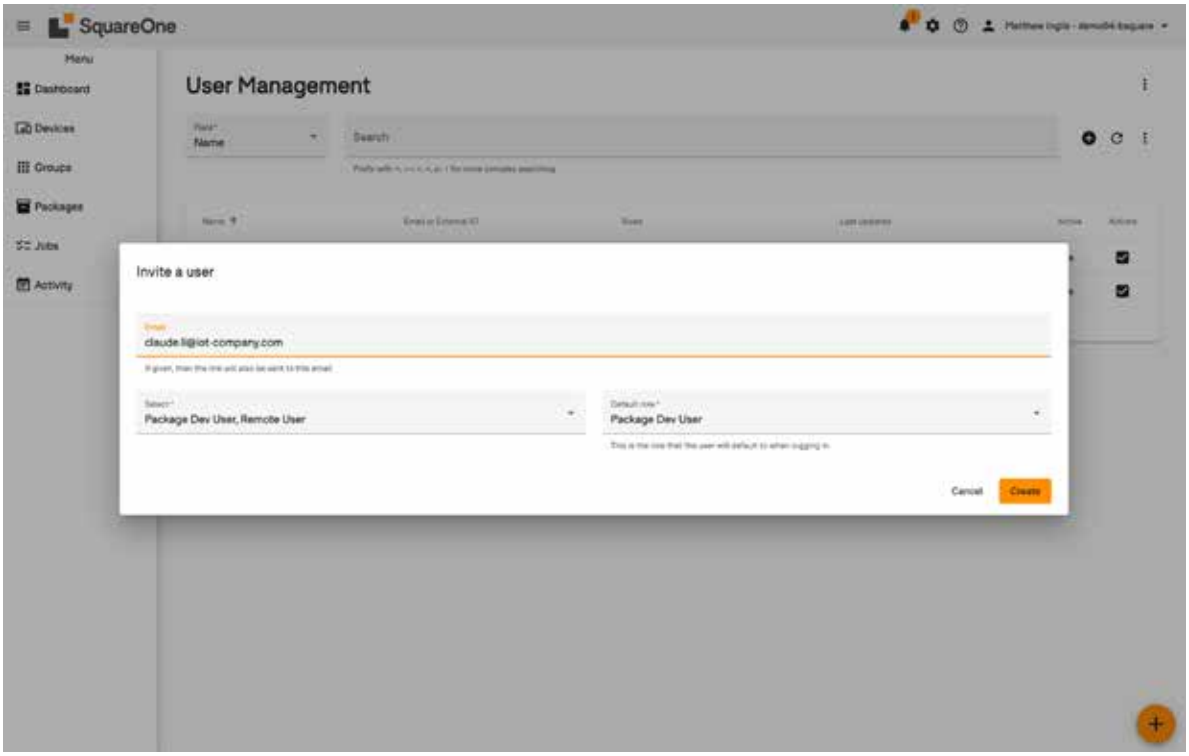
Data is encrypted in transit and at rest.

- **On The Device:** When the device hardware incorporates adequate provisions for autonomous encryption, such as a TPM, data is stored on the device in an encrypted state.
- **In Transit:** All data transmitted between the cloud and device is encrypted.
- **In The Cloud:** Any configuration, status, and telemetry pertaining to devices is stored encrypted in both the cloud database, and in long-term storage.

SquareOne interfaces

All interfaces are protected. On the edge, connections are initiated by the device, meaning no open incoming ports are needed. SquareOne access is authenticated via Single sign on or local log in. Users have associated permissions/roles accessible through the UI.

- **MQTT:** MQTT communication between device and cloud is encrypted via per-device MQTT certificates. Devices are confined to accessing topics with their unique IDs, preventing direct inter-device communication.
- **Software Download:** Package deployments use HTTPS connections with time-limited keys.
- **Remote Access:** SquareOne's remote access relies on a device-initiated, point-to-point encrypted WebRTC tunnel to the operator's web browser throughout the remote session.
- **Cloud Interfaces:** Each SquareOne instance offers a REST API accessible directly or via the Companion Web UI. Access is regulated through Open ID Connect (OIDC) compatible login, facilitating integration with corporate systems for Single Sign-On (SSO) via existing identity providers. Configuration options include MFA and password requirements.
- **Device Interfaces:** The SquareOne Agent on a device provides a WebSocket interface, limited to localhost, enabling the device to transmit supplementary data to the cloud.



Security processes

Bsquare has extensive experience delivering managed hosting services and offers a comprehensive range of solutions to ensure secure and dependable operation of connected systems.

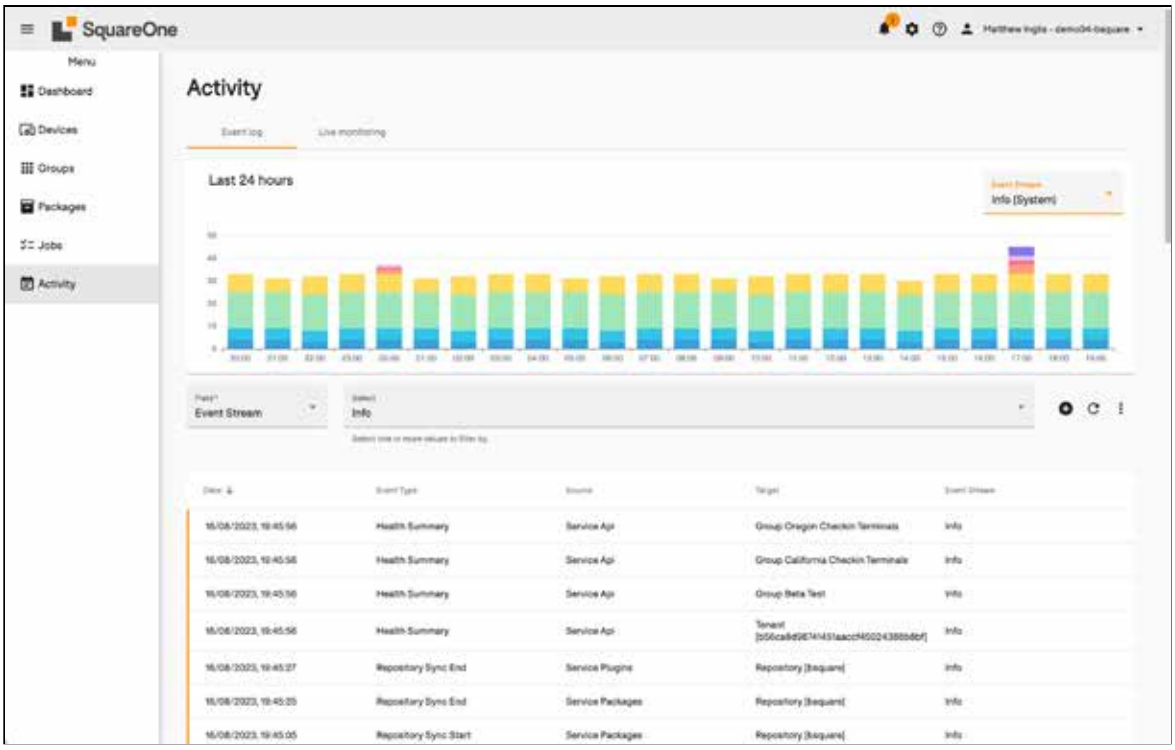
- **SOC 2 Compliance / Penetration Testing:** Bsquare undergoes annual SOC 2 certification for its processes. Additionally, we subject all externally facing systems to third-party penetration testing each year, resolving any identified issues promptly.

- **Monitoring and audit logs:** SquareOne furnishes audit logs for significant system events, encompassing recorded login activities and access logs. These logs are diligently monitored by our DevOps team on a routine basis..

- **Vulnerability Reporting Statement and Process:** Bsquare maintains a transparent vulnerability reporting process. Any problems reported through this channel are integrated into our internal ticketing system and managed to resolution by our support team. Having a well-defined and publicized process of this nature is crucial for promptly and professionally addressing identified vulnerabilities.

Device hardening

An important aspect of creating a secure connected system is to ensure proper device configuration and construct the OS with a strong emphasis on security.



info@bsquare.com 425 519 5900