Titanium Intelligent Solutions LLC
email: info@titaniumintel.com
phone: 646-868-8582
website: https://www.titaniumintelligentsolutions.com

Titanium Global SaaS IoT - Security Practices

Titanium is a *Global Software-as-a-Service (SaaS) Internet of Things (IoT) platform* providing powerful and intelligent solutions to help our customers. Titanium delivers a scalable platform that is available anywhere from any internet enabled device. Titanium provides a comprehensive enterprise tool for monitoring, control, data, and analytics for smart buildings and smart cities.

TITANIUM SECURITY

Titanium built the SaaS IoT platform based on a visionary design that includes the highest standards for security to ensure a platform that is reliable and trusted.

WI-FI SECURITY

Security for wireless communication requires encryption using a known good standard.

- All wireless communications are encrypted with standard WPA2 (for Client to AP and Uplinks) or IBSS/RSN (for Mesh-to-Mesh links)
- Each method utilizes 256-bit AES encryption keys

CONTROL SECURITY

Control security is essential when managing communications across thousands of IoT devices and networks.

- All communication between nodes and the cloud utilizes SSL encryption, more specifically TLSv1.2, the latest and most secure version of SSL
- X.509 certificates are used to authenticate clients and nodes with new and unique keys generated every five (5) minutes
- All data is protected at rest and in transit

APPLICATION SECURITY

Security is required across the entire process chain for application security.

- The cloud web front end is SSL encrypted
- Employ various techniques to prevent known attacks, such as cross-site scripting (XSS), SQL injection, man-in-the middle (MITM), etc…
- Ongoing vulnerability and penetration (passive and active) testing to prevent regression of business logic
- Conduct rigorous, automated, QA testing
- Data back-ups are encrypted
- Production, development, and staging environments are strictly segregated

IDENTITY AND ACCESS SECURITY

Highest standards for identity and access security are required.

- Each device and every network require a secure password, with a two-factor-authentication available, and different access levels (i.e., owner, administrator, observer)
- OKTA integration available for SSO via OIDC
- Use rule of least privilege (access required for job function) for personnel access to IT systems

INFRASTRUCTURE SECURITY

Titanium uses Amazon Web Services to host our application. Titanium makes full use of the security products embedded within the AWS ecosystem.