

API Integration and Local Deployment: Diyu as an On-Premise IoT Platform Provider for Property Management

PC01 Engineering LoRaWAN Smart Lock

1:50 Node Convergence | 2km Coverage | 4-in-1 Access



The Ultimate Solution for High-Density Apartment Projects

Shenzhen, Guangdong Oct 12, 2026 ([Issuewire.com](https://www.issuewire.com)) - Deploying intelligent building technology requires choosing an operating architecture that balances administrative convenience, integration flexibility, and enterprise data control. Deploying a dedicated on premise iot platform or private server gateway environment allows property managers to retain physical custody of access credentials and metering records within internal networks.

As an adaptable hardware and software partner, Shenzhen Diyu Smart Co., Ltd. (<https://diyusmart.com/q/h/com/index.html>) operates as an IoT solution provider (<https://diyusmart.com/q/h/product/index.html>), delivering open APIs, flexible network-server paths, and private-server deployment options for commercial properties.

The choice between multi-tenant Software-as-a-Service and local on-premise deployment is fundamentally an operational governance decision. Conflating application programming interfaces with true on-premise hosting often leads to misaligned expectations during project commissioning. Examining the infrastructure commitments, API contracts, and lifecycle responsibilities of local deployment ensures that property technology teams select the right software model for their facility.

Define What “On-Premise” Means Before Comparing It with SaaS

A disciplined technical evaluation requires defining terms precisely, as API integration and on-premise deployment describe fundamentally different layers of a software architecture. API integration refers to the programmatic mechanism by which distinct applications exchange structured data. Cloud-hosted IoT platforms expose RESTful endpoints or MQTT topics to building management systems, while locally deployed servers query cloud services via outbound webhooks.

True IoT local deployment means that core application software, database storage, device connection brokers, and administrative logic run entirely on physical servers or virtualized appliances within customer-controlled infrastructure. By keeping data inside the customer's private local area network, the facility remains completely isolated from external public cloud dependencies.

Diyu's Verified Integration Path Starts with Device Management and APIs

Diyu Smart establishes verified integration pathways that enable system integrators to bridge field hardware with proprietary enterprise platforms. For commercial access control, Diyu Smart provides dedicated PC management software alongside mobile applications for its PC01 engineering smart locks, allowing direct integration into customer property management systems.

Through an open smart lock API, enterprise software can issue dynamic access passcodes, register RFID credentials, and retrieve door entry audit logs programmatically.

In wireless sensor and metering networks, Diyu Smart's 255MG-801 industrial LoRaWAN gateway provides complete network-server autonomy. Integrators can bind the gateway to public platforms like The Things Network or point it directly to a private ChirpStack network server in the building server room.

For qualifying enterprise projects with strict data boundaries, Diyu Smart provides custom firmware configurations where devices communicate via standardized RESTful endpoints and MQTT message brokers directly to private customer servers without third-party cloud intermediaries.

SaaS and Local Deployment Shift Operating Responsibility in Opposite Directions

Choosing between cloud hosting and on-premise deployment involves trading administrative convenience for operational autonomy. Each deployment path distributes infrastructure and cybersecurity responsibilities differently between vendors and building operators.

SaaS Centralizes Hosting and Updates with the Provider

A multi-tenant cloud model shifts infrastructure maintenance to the software provider. System integrators avoid purchasing dedicated server hardware, provisioning uninterruptible power supplies, or configuring complex firewall demilitarized zones. Software updates, security patches, and database backups occur automatically in the background. Field devices connect outbound over standard HTTPS and MQTTS ports, simplifying network router configurations.

However, property owners remain dependent on continuous wide-area internet connectivity and must accept ongoing recurring subscription licensing costs.

Local Deployment Gives the Customer More Infrastructure Control

Local deployment places data storage, user permissions, and network access entirely under the property owner's direct supervision. In high-security government facilities, hospital complexes, and European properties with strict data residency rules, keeping occupancy records and credential databases on-site is an operational mandate.

Furthermore, local deployment provides complete offline survivability, allowing staff to issue keycards, monitor electrical sub-meters, and adjust HVAC setpoints across the internal local area network even if external fiber-optic connectivity is severed.

However, local deployment requires the customer's IT department to maintain server hardware, execute regular database backups, manage operating system security updates, and implement disaster recovery procedures.

PMS, BMS, and Property Platforms Need Explicit API Contracts

Seamless interoperability between field hardware and enterprise software depends on formal, well-documented application programming interface contracts. When connecting field devices to hotel management systems, a robust property management system api supports bidirectional synchronization. The PMS generates room access rights during guest check-in, while the lock network reports battery warnings and unauthorized entry attempts back to security.

In commercial automation, a standardized smart building api coordinates diverse subsystems, illuminating designated office floors and adjusting thermal setpoints whenever an employee badge is scanned at a turnstile.

Similarly, an enterprise iot platform api ingests sub-metering telemetry from electrical panels and water risers, streaming normalized consumption data into corporate carbon reporting software. Clear API contracts specifying payload schemas, authentication tokens, and rate limits prevent integration bottlenecks across property subsystems.

Data Security and Compliance Depend on Architecture Details

Local deployment supports data residency and network isolation, but achieving regulatory compliance requires independent operational controls. Physical custody of a server remains ineffective without rigorous cybersecurity governance.

System administrators must establish database encryption at rest, enforce automated data pruning schedules for sensitive user access logs, and implement granular role-based access permissions requiring multi-factor authentication for administrative personnel. Enforcing TLS encryption secures all

HTTP, MQTT, and database connections traversing local network switches.

Organizations must also schedule automated off-site cryptographic backups to prevent ransomware data loss, while assigning clear organizational responsibility for applying software patches and firmware updates throughout the system lifecycle.

Require a Local-Deployment Specification Before Solution Commitment

System integrators and facility directors should mandate a comprehensive technical specification before committing to an on-premise architecture. This engineering document must detail server hardware requirements, CPU core counts, memory allocation, and supported operating system distributions, while defining database licensing, storage capacity forecasts, and database indexing strategies.

Network engineers must map local IP addressing, internal VLAN segmentation, and firewall port allowances, while documenting precisely which device features remain operational during network interruptions. The specification must establish clear service level agreements for ongoing software updates, security patches, and long-term technical support.

Choose Deployment Mode by Data Ownership and Operations

Selecting the right software architecture requires aligning property operational capabilities with long-term governance goals. Multi-tenant cloud SaaS remains ideal when rapid deployment, minimal upfront capital expenditure, and vendor-managed maintenance outweigh internal control requirements.

Conversely, on-premise local deployment proves superior when data sovereignty, internal network isolation, mission-critical offline operation, and custom software integration represent essential facility requirements. An effective smart building solution makes data ownership boundaries, API responsibilities, and maintenance workflows explicit prior to hardware installation.

System integrators and IT architects planning enterprise building deployments can contact Diyu Smart to evaluate API documentation, or explore the platform lineup on the Diyu Smart official website (<https://www.diyusmart.com/>).



Media Contact

Diyu Smart

*****@diyusmart.com

<http://www.diyusmart.com/>

Source : Shenzhen Diyu Smart Co., Ltd.

[See on IssueWire](#)