IoT Device and Data Operations Requirements Checklist

EdgeIQ

Use this checklist to define the operational requirements for managing connected IoT products and their data. More than a simple list, this guide provides details on the scope of the requirements and the impact they can have on your business when properly implemented. In the feature descriptions and the impact details, we highlight ways to implement these as workflows, not just atomic features. DeviceOps and DataOps are just part of the broader value chain in your connected product business.

Device Operations (DeviceOps)

Requirement	Details	Impact
Device Registry	Device Registry acts as the single source of truth and system of record for all registered, authorized, and discovered devices, regardless of state. Device Registry will maintain a record of state, firmware version, configuration history, software update history, commands, and other relevant device and user actions. Device Registry can import devices from external systems, (e.g. CSV files, ERP and CRM systems).	A reliable single registry significantly reduces the probability of human error resulting from swivel chair management and manual copy/paste. It also acts as a hub for workflows among other systems where devices (products) are registered, and tracks their state from cradle to grave, which is invaluable for support teams.
Fleet Management	Fleet management allows users to group devices by groups or cohorts. This can include device profile, geography, customer account, device state, configuration status, etc. Users can add tags and metadata, and create custom fields to enhance fleet filtering. Users can take actions based on groupings of devices and fleets by tags, metadata, or other fields.	The ability to define and group devices and add tags and metadata provides tremendous flexibility across many DeviceOps workflows. Organizations can gather utilization insights by device profile or customer account, geography, or type of connectivity. Software update workflows can be targeted at only test cohorts or specific accounts and subaccounts in specific geos.
Provisioning and Lifecycle Management	Device Lifecycle Management allows customers to define, view, and manage devices through various states and stages. Device can be registered but not assigned profiles or accounts even before they are activated. Multiple parameters can be configured at the time of activations with zero-touch provisioning. A system must be able to recognize whether a device is in escrow, active, maintenance or decommissioned states. Organizations should also be able to define custom stages.	Some of the most important workflows in Connected Product businesses are driven off Lifecycle Management. As devices move from inventory and distribution to customer locations, it becomes essential to map customer-specific configurations, heartbeat policies, and service event workflows to their lifecycle state and account. It also allows organizations to move devices into maintenance, replacement, and decommissioning states.

Configuration Management	Define and manage settings for devices, networks, applications, or any other endpoint or service that can be configured. This also allows teams to read settings back from devices to understand the current configuration.	In a world of smart, software-defined devices, organizations can take the same physical device and create a multitude of different products simply based on its configurations. Features can be turned on and off, recipes can be sent, and languages changed. Workflows can change device configuration based on customer behavior, purchases, and even service events.
Software Update Management	Define and deliver specific software images to pre-defined device cohorts. Updates can include operating systems, firmware, Snaps, and other applications. Feature includes testing with sample devices, validating existing software version, retry management, roll back capabilities, audit logs of success/failure, and status notifications. Process will work with native installation or containerized systems.	Monolithic FOTA updates are a thing of the past. Testing updates with small cohorts, firmware validation, rollbacks, or workflows tied to specific timezones to avoid operational disruption are all the new norm. Whether fixing bugs, plugging a security hole, or delivering new features as updates, software management workflows are essential and strategic.
Monitoring, Diagnostics, Remediation	Active and continuous monitoring of devices through heartbeats and configurable device data reports is foundational. But there are times organizations will require advanced diagnostic capabilities that might include remote terminal access. A system must be able to diagnose and remediate issues using commands, scripts and also automate responses to common issues via defined support playbooks. "	Imagine that pre-defined device events automatically trigger service event workflows with your FSM platform. Diagnostic and remediation workflows can be driven by playbooks for each level of the support organization responding to an incident. All of these can be tied to unique configurations by device cohort, account, or even geography.
Users and Accounts	Role-based Access Control (RBAC) and permissions management are tied to individuals, accounts and organizations. Includes support for flexible, multi-tier account hierarchy and integration with third-party RBAC and SSO services.	Historical account controls were limited to a small number of roles or maybe an additional dimension of control at the account level. Advanced administrative workflows can be tied to a virtually unlimited user role and organizational hierarchy. Organizations can even define their own custom roles.

Data Operations (DataOps)

Requirement	Details	Impact
Ingest and Normalize	Capture data at the edge through any protocol using local ingest and/or capture data via cloud API integration, normalize to common JSON format for storage, analysis and transmission.	Machines and humans speak different languages. Opening a data pipeline and applying translation and normalization simplifies, streamlines, and reduces the cost of all downstream data-dependent workflows.

Inspection and Action	Inspect data records for patterns, anomalies, or crossing defined thresholds. Take action based on pre-defined policies whether simple actions or complex workflows.	The ability to inspect, analyze, and act upon operational data during the ingest and delivery workflow is incredibly powerful. Different stakeholders should be able to apply completely different filters and policies since each has their own perspectives on what is good data versus operational anomalies.
Data Delivery	Data can be distributed from the edge to any endpoints at the edge or in the cloud. Delivery can occur direct from the edge to a specified cloud service without passing through a third-party cloud.	Single-threaded data capture and delivery into a single repository, or worse, directly to an application, is painful and expensive. The goal is to capture, normalize, filter, and deliver data to one or multiple locations with simple and configurable workflows. The ability to apply granular user, account, and workflow-specific controls adds significant value and ensures that the right data is available to the right people and systems to drive outcomes.
Data Storage	Configurable data storage, both short-term or long-term. Data storage can also define which data elements to store, (e.g., device and network data only, operational telemetry data, or both).	Some data should be stored for the short term, other data for the long term, and other data should not be stored at all. In data-driven workflows, organizations must be able to configure data storage based on use case and business requirements.