

AppThing: Service Description & Operational Overview

1. Service Overview

AppThing is a cloud-native, device-agnostic IoT and data platform designed to ingest, manage, process, and visualize data from a wide range of connected devices and external systems. The platform enables organizations to securely connect devices, manage users and roles, configure dashboards and alerts, and extract operational insights through configurable widgets, reports, and analytics.

AppThing is designed for scalability, resilience, and security, and can be deployed either within AppThing-managed AWS infrastructure or within a customer-owned AWS account. The service follows AWS Well-Architected Framework (WAF) principles across security, reliability, performance efficiency, cost optimization, and operational excellence.

2. Data Backup, Restore, and Disaster Recovery

AppThing provides structured data protection and resilience mechanisms aligned with industry best practices for cloud-native systems.

2.1 Data Backup

- Automated backups of application data and configurations
- Backups are stored in geographically redundant AWS storage services
- Backup frequency and retention policies are configurable based on instance criticality
- Default retention period: up to **1 year** (configurable)

2.2 Data Restore

- Point-in-time recovery for supported data stores
- Restore procedures are tested periodically as part of operational readiness
- Restore time objectives (RTO) and restore point objectives (RPO) are defined per deployment and documented in agreed SLAs

2.3 Business Continuity & Disaster Recovery

- Architecture supports multi-AZ (Availability Zone) deployments by default
 - Disaster recovery strategies (e.g., warm standby, pilot light, or multi-region) are selected based on customer requirements
 - Business Continuity and Disaster Recovery (BCDR) plans are maintained and reviewed regularly
 - SLAs for recovery objectives are determined according to the criticality of each instance
-

3. Onboarding and Offboarding Support

3.1 Onboarding Support

AppThing provides structured onboarding to ensure successful adoption and secure operation:

- Environment setup and configuration
- User, role, and permission management
- Support for organizational hierarchies and multi-tenant structures
- Device onboarding and integration support (APIs, protocols, and connectors)
- Initial data validation and operational readiness checks

3.2 Offboarding Support

Upon service termination or contract completion, AppThing provides:

- Export of customer data in standard, machine-readable formats
 - Final usage and operational reports (where applicable)
 - Secure decommissioning of environments following data export confirmation
 - Documentation of offboarding steps for audit and compliance purposes
-

4. Service Constraints and Customization

4.1 Maintenance Windows

- Planned maintenance activities are scheduled during predefined maintenance windows
- Customers are notified with sufficient advance notice
- Maintenance notifications include scope, expected impact, and duration

4.2 Customization

- AppThing is primarily a configurable platform rather than a fully bespoke solution
 - Customization is supported through configuration, integrations, APIs, and extensibility mechanisms
 - Deep custom development or platform modifications are subject to separate agreement and technical assessment
-

5. Service Levels

5.1 Performance and Availability

- Designed for high availability using AWS managed services
- Performance targets and uptime commitments are defined per instance
- Service Level Agreements (SLAs) are tailored based on deployment model and criticality

5.2 Support Hours

- Standard support is provided during agreed business hours
 - Extended or 24/7 support options are available and defined on a per-customer basis
-

6. After-Sales Support

AppThing includes standard after-sales support to ensure continued value:

- Product walkthroughs and demonstrations
 - Usage insights and platform best practices
 - Guidance on new features and capabilities
 - Ongoing collaboration to optimize platform utilization
-

7. Technical Requirements

- Cloud-native architecture built on Amazon Web Services (AWS)
- Designed in alignment with AWS Well-Architected Framework (WAF) principles
- Access via modern web browsers and secure APIs

- No on-premises infrastructure required unless explicitly agreed
-

8. Outage and Maintenance Management

- Incidents and outages are managed using defined operational procedures
 - Root cause analysis is conducted for significant incidents
 - Customers are informed of incidents, progress, and resolution status
 - Incident response SLAs and escalation paths are agreed on a case-by-case basis
-

9. Hosting Options and Locations

AppThing can be hosted using one of the following models:

- **AppThing-managed AWS account** (default)
- **Customer-owned AWS account**, deployed and operated following agreed responsibilities

Hosting regions and data residency requirements are selected in collaboration with the customer and documented as part of the deployment agreement.

10. Access to Data Upon Exit

- Customers retain ownership of their data at all times
- Upon exit, data is provided through secure exports in standard formats
- Data access procedures are documented and auditable

- Post-export data deletion follows agreed retention and compliance requirements
-

11. Security

AppThing implements security controls aligned with government and enterprise expectations:

- Encryption of sensitive data (including PHI, where applicable) **at rest** using industry-standard encryption
 - Encryption of data **in transit** using TLS
 - Role-based access control (RBAC)
 - Secure authentication and authorization mechanisms
 - Network protections including AWS security groups, IAM policies, and web application firewalls
 - Regular security reviews and vulnerability management processes
-

This document is intended to provide a high-level service and operational overview. Final service levels, recovery objectives, and support models are defined contractually based on customer requirements and deployment criticality.