DL Connect

Security Prospectus

Security & Technical Architecture Prospectus

Datalogic – DL Connect
Version: 1.6
Date: May 14, 2026
Prepared for: Any Customer (referred as “Customer” in this document)

---

1. Executive Summary

This document, structured to support third-party security assessment and cybersecurity review processes, provides an overview of the security architecture, data flows, and technical requirements for deploying the **DL Connect** solution within the Customer environment.

The solution consists of:

- POS Middleware (installed on POS or local systems)
- Edge Server (on-premise component)
- Cloud Platform (hosted in Microsoft Azure and managed by Datalogic)

The purpose of this document is to enable Customer IT and Cybersecurity teams to:

- Assess security risks
- Approve deployment architecture
- Configure network and firewall settings

2. Solution Overview

DL Connect has the mission to deliver a powerful cloud solution for remote management of devices with the confidence that Customer's organization can operate securely, today and in the future. Security is built by design into the core of the platform, to provide a layered, defense-in-depth approach that safeguards data, applications, and users. Iterative Penetration Tests by R&D department and by an external Company are included in the process.

2.1 Components

POS Middleware (AladdinSDS)

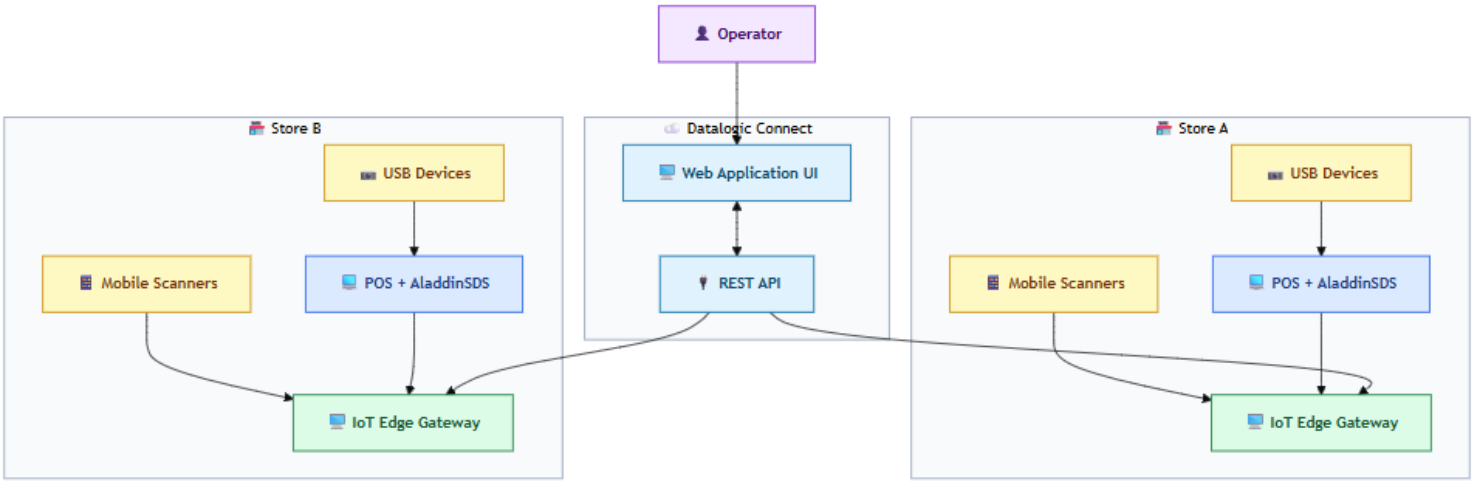
- Installed on: POS terminal (Windows and Linux)
- Function: Datalogic device management, communication with IoT Edge Gateway

IoT Edge Gateway

- Installed on customer infrastructure: on-prem/cloud VM / physical server
- Function: data aggregation, buffering, secure communication with cloud

Cloud Platform

- Hosted in: Azure Cloud West Europe (Netherlands)
- Function: data processing, APIs, management dashboards



3. Architecture Overview

3.1 High-Level Description

The solution follows a **secure outbound-only communication model**. All Edge Gateways and cloud components initiate outbound connections using encrypted protocols (TLS 1.2 or higher). No inbound connectivity from the Internet to the customer network is required. Communication from field devices to the Edge Gateway is confined to the local network.

3.2 Data Flow Summary

1. POS Middleware collects operational data (operates transparently in the background)
2. Data is sent to Edge Server over internal network
3. Edge Server securely transmits data to Azure Cloud services
4. Cloud processes and optionally return responses (if applicable)

---

4. Network Requirements

4.1 Connectivity Model

- Communication is **outbound only** from the customer network toward the cloud.
- No inbound firewall rules from the Internet are required.
- Inbound connections are limited to **LAN-local communication** between field devices and the Edge Gateway.

4.2 Ports and Endpoints

Purpose	Source	Destination	Port	Protocol	Direction
Device telemetry & commands	Edge Gateway	*.azure-devices.net	8883	MQTT over TLS	Outbound
IoT Hub fallback	Edge Gateway	*.azure-devices.net	443	HTTPS (MQTT over WebSocket)	Outbound
Device provisioning	Edge Gateway	global.azure-devices-provisioning.net	443	HTTPS	Outbound
Storage access	Edge Gateway	*.blob.core.windows.net	443	HTTPS	Outbound
Container Registry — IoT Edge module images	Edge Gateway	crsolinfraprodeuw.azurecr.io	443	HTTPS	Outbound
Container Registry data endpoint	Edge Gateway	crsolinfraprodeuw.westeurope.data.azurecr.io	443	HTTPS	Outbound

Device Smart Enrollment	Edge Gateway	*.azureiotcentral.com	443	HTTPS	Outbound

4.3 Whitelisting Requirements

- Preferred: FQDN-based allowlisting
- Domains to whitelist:
    - *.azure-devices.net
    - global.azure-devices-provisioning.net
    - *.blob.core.windows.net
    - crsolinfraprodeuw.azurecr.io
    - crsolinfraprodeuw.westeurope.data.azurecr.io
    - *.azureiotcentral.com

---

5. Security

5.1 Encryption

- Data in transit: TLS 1.2 enforced across all Azure services; TLS 1.3 used for Temporal Cloud gRPC communication
- Data at rest: AES-256 encryption

5.2 Authentication & Authorization

User authentication:

- OAuth 2.0 / OpenID Connect federated authentication via Microsoft Entra ID with MFA support

Device authentication:

- Edge Gateway: Azure Device Provisioning Service (symmetric key)
- Field devices: X.509 certificates with mutual TLS

Authorization:

- Role Based Access Control (Owner, Administrator, Operator, Viewer)

5.3 Credential Management

- Credentials stored securely using encryption
- No plaintext storage of sensitive information
- Support for credential rotation

6. Data Protection & Compliance

6.1 Data Types Processed

- Device telemetry and status information
- Device properties (model, serial number, firmware version)
- Configuration and operational metadata
- User identity data limited to business contact information for authentication
- No PII or payment card data is involved

6.2 Compliance

- DL Connect is hosted by Microsoft Azure, which maintains certifications including ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018, and ISO 9001:2015. Microsoft Azure is SOC 2 Type 2 audited.
- Datalogic follows security best practices aligned with ISO 27001 principles, including: Access control policies, Incident response procedures, Risk management practices, Logging & monitoring.
- GDPR (EU data protection): DL Connect is designed with data protection and privacy by default and by design, in accordance with the EU General Data Protection Regulation. Datalogic acts as a data processor on behalf of our customers and process telemetry data strictly according to documented instructions and applicable data processing agreements (DPA). Datalogic implements appropriate technical and organizational security measures to protect personal data against unauthorized access, alteration, disclosure, or destruction. Where applicable, we support data subject rights (including access, rectification, and deletion) and ensure data is retained only for as long as necessary for the intended processing purposes.
- EU Cyber Resilience Act (CRA): reporting rules compliance from September 11, 2026
- Data minimization principles applied
- Data residency: European Union – Azure West Europe (Netherlands)

6.3 Data Retention

- Retention period: Database backups retained for 7 days by default (configurable)
- Deletion policy: Automatic based on retention rules or on customer request

7. Logging & Monitoring

- The platform maintains audit logs for authentication, access, and administrative activities to support security monitoring and incident investigation

- Logs include:
    - Connection events
    - Errors and failures

---

8. Patch Management & Updates

- Updates delivered via:
    - Automatic / Manual deployment
- Security patches:
    - Applied regularly (monthly basis)
- Versioning and rollback supported

---

9. Vulnerability Management

- Security assessments performed: white/gray/black Box security assessments on the infrastructure are performed by accessing the public IoT Edge, the Web App REST APIs, the Web App GUI, and the Authentication Endpoint.
- Vulnerability remediation process in place within CI/CD pipeline.
- **Penetration testing** is periodically performed by Datalogic to discover, fix and validate possible vulnerabilities. Exemplary last report below:

TYPE	TEST GROUP	RESULT
Security by-design	Cloud/Edge services selection and configuration	PASS
	Network protocols selection and configuration	PASS
Reconnaissance	Identified Doors and Services	PASS
	Open Doors	PASS
Vulnerability	MQTT Protocol: client-edge connection	PASS
	MQTT Protocol: edge-server connection	PASS
	gRPC Services	PASS
	OpsMessaging API	PASS
	Authentication system OAuth2.0	PASS
REST API	API documentation discovery	PASS
	API Authentication and Authorization	PASS
	Multi-tenant isolation	PASS
	JSON Web Token (JWT)	PASS
	Insecure Direct Object References (IDOR) enumeration	PASS
	Injection attacks	PASS
	Business Logic (race, boundary, timing)	PASS
	Data validation	PASS
Web Application	Front-end component	PASS
	Swagger Web UI	PASS
Networking and Cryptography	TLSv1.2	PASS
	HTTP	PASS
	Web Socket	PASS

10. Incident Response

In the event of a security incident:

- Detection and analysis performed by Datalogic
- Customer notified within agreed Service Level Agreement (see SLA matrix)
- Mitigation and remediation actions as defined in agreed SLA

---

11. Deployment Checklist

- Edge Server installed on approved infrastructure
- POS Middleware installed on target systems
- Outbound connectivity to cloud endpoints enabled
- OAuth connectivity validated
- DNS resolution verified
- System tested and verified

---

12. Support & Contacts

Technical Support Contact:
Datalogic Connect Technical Support: connect.support@datalogic.com

---

13. Appendix

13.1 Definitions

- POS: Point of Sale
- Middleware: Software layer enabling communication
- Edge Server: Local processing and communication node

13.2 Additional Documentation

- API documentation (available upon request)
- Installation guide
- A Data Processing Agreement (DPA) can be provided upon request

---

End of Document

Datalogic Group

Datalogic S.p.A.
Via Candini, 2 - 40012 Lippo di Calderara di Reno - Bologna (Italy)
Tel. +39 051 3147011 | Fax +39 051 3147205
corporate@datalogic.com
ww.datalogic.com