BALLUFF

Cyber Security

SMART REORDERING SYSTEM

innovating automation

The Balluff Smart Reordering System helps you to manage your inventory in a simple and intelligent way and optimizes your material flow. Since it is a cloud application, you don't have to worry about infrastructure, technology, operations, security, backup and other aspects. This document describes data security and business continuity aspects of the services.

1. DATA SECURITY AND PRIVACY

1.1 Physical Security

The Smart Reordering System runs on the Microsoft Azure Cloud Infrastructure. Microsoft designs, builds, and operates datacentres in a way that strictly controls physical access to the areas where your data is stored. Microsoft has hundreds of Azure datacentres in 54 regions (as of 2019), and each of them has extensive multi-layered protections to ensure unauthorized users cannot gain physical access to your data. Layered physical security measures at Microsoft datacentres include access approval:

- At the facility's perimeter.
- At the building's perimeter.
- Inside the building.
- On the datacentre floor.

Physical security reviews of the facilities are conducted periodically to ensure the datacentres properly address Azure security requirements.

1.2 Encryption of Data at Rest

LoRaWAN Network Server:
The last 14 messages of every sensor are stored in the Networkserver. The stored data is encrypted with AES-128.

Azure:
All data is stored in secure data bases and is encrypted using AES-256. The location of the servers can be chosen according to the customer preferences. (e.g.. inside the EU, US etc.)
For more information about the data security and standards visit

https://docs.microsoft.com/en-us/azure/compliance/

Rest API:
Access to the REST APIs is protected by API keys.

1.3 Encryption of Data in Transit

Data traffic between the LoRaWan sensor and the LoRaWan Gateway is protected by the LoRaWan specific security mechanisms. These include the specification of several security keys. All keys have a length of 128 bits. The algorithm used for this is AES-128, similar to the algorithm used in the 802.15.4 standard. For more information see the following link:

https://www.thethingsnetwork.org/docs/lorawan/security.html

Data exchanged between the LoRaWAN Network Server and the application on Microsoft Azure is protected by Transport Layer Security. (TLS)

1.4 Data Segregation

Data is stored in Storage Accounts on MS Azure servers. access keys to customers accounts are stored in a separate key vault. Customer applications will only have access to the storage accounts that are directed to them.

1.5 Authentication

Strong user authentication is available through OAuth2-based single sign-on (SSO) integrated with the customers' identity provider (Microsoft ADFS) through federated authentication using SAML v2.0.

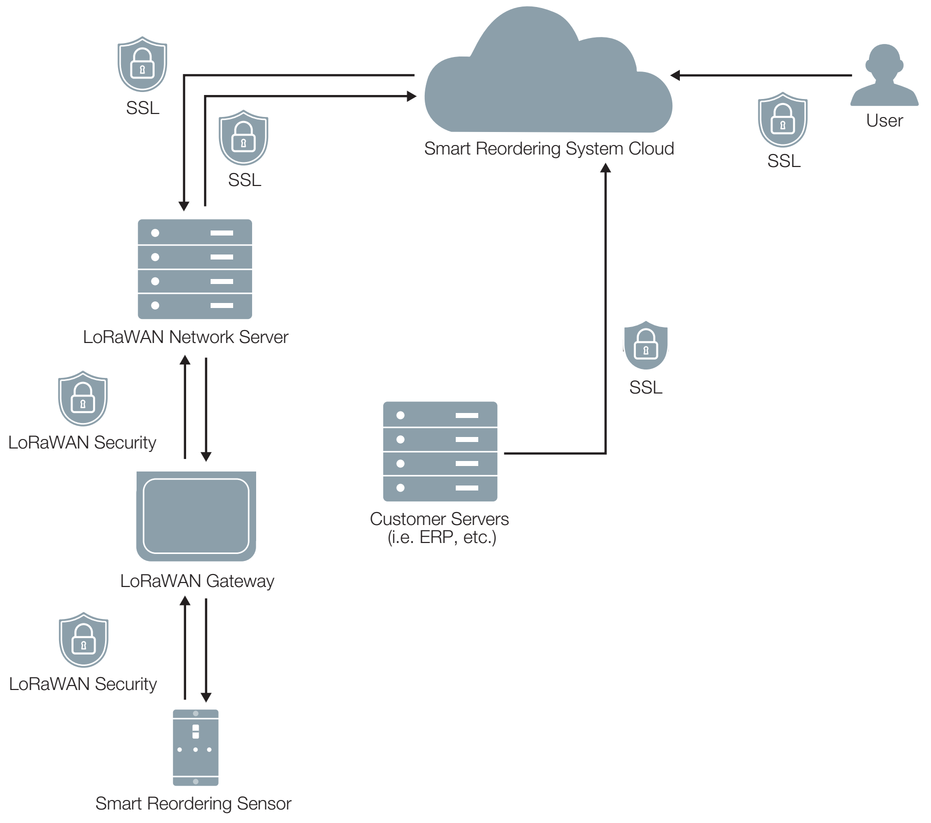
The customer does not need to change default passwords since the user can simply sign in with his Microsoft account. After the account has been activated the user will receive a registration link which will securely guide him through the registration.

Multi factor authentication (MFA) can be enabled.
The authentication protocol used is OpenID Connect.

1.6 Authorization

There are two roles which can operate the system, an admin role and a user role.

- **User:**
  has limited access to system settings and is only able to read data
- **Admin:**
  is able to fully control and configure the system. The admin role is also able to invite other users to the application and control their privileges.



1.7 Security Incident Notification

If Balluff becomes aware of any unlawful access to any customer data or support data, or unauthorized access to such equipment or facilities resulting in loss, disclosure, or alteration of customer data or support data, Balluff will:
(1) promptly notify the customer of the security incident,
(2) investigate the security incident and provide the customer with detailed information about the security incident, and
(3) take reasonable steps to mitigate the effects and to minimize any damage resulting from the security incident.

2. BUSINESS CONTINUITY MANAGEMENT

2.1 Backups and Disaster Recovery

The Smart Reordering System uses the Geo-redundant storage solution offered by Microsoft Azure.

Geo-redundant storage (GRS) copies your data synchronously three times within a single physical location in the primary region using LRS. It then copies your data asynchronously to a single physical location in a secondary region that is hundreds of miles away from the primary region. GRS offers durability for Azure Storage data objects of at least 99.99% over a given year.

A write operation is first committed to the primary location and replicated using LRS. The update is then replicated asynchronously to the secondary region.

When data is written to the secondary location, it's also replicated within that location using Locally Redundant Storge (LRS).

https://docs.microsoft.com/en-us/azure/storage/common/storage-redundancy#locally-redundant-storage

2.2 Updates

Updates are provided by Balluff and need no interaction from the customer. All devices are automatically updated over the air and the application is updated constantly without any customer involvement.

2.3 Availability

The Smart Reordering application is developed and hosted on the Microsoft Azure infrastructure (IaaS). Microsoft guarantees a 99,9% availability for their customers.

https://azure.microsoft.com/en-us/support/legal/sla/summary/

2.4 Monitoring

All environments are monitored by Balluff with operators on duty taking the necessary actions to ensure that systems are available for use, i.e. that users are able to log on and perform a standard set of operations. System performance can be inspected by customers using the integrated monitoring tools. (e.g. device list, device details etc.)

3. CYBER SECURITY AT BALLUFF

3.1 Annual Cyber Security Audits

In order to meet the highest IT-Security standards annual cyber security audits are conducted at Balluff. The goal is to ensure that data security objectives are met during the whole product life cycle from the basic idea to end of life. The foundation for these assessments is the Consensus Assessment Initiative Questionnaire (CAIQ) from the Cloud Security Alliance CSA. Results are shared among the stakeholders /and actions resulting from this are continuously checked for their degree of implementation.

3.2 Development practices

IT-Security relevant guidelines have been established within the development department and developers are constantly trained in courses regarding Secure Software Development. Coding Guidelines as well as Baseline Security Requirements like OWASP ASVS are followed during the product creation processes. Code reviews and continuous testing ensure the system integrity.

Generally applicable best practices regarding IT-Security and the development of standard-oriented (security) metrics are applied.