Maintmaster® CMMS Security White Paper

Welcome to Maintmaster CMMS! Maintmaster CMMS is a leading tool for optimizing operational reliability in discrete manufacturing. This white paper provides an overview of the security aspects of the Maintmaster CMMS system—covering its deployment, data protection, and, to some extent, its development practices.

This white paper applies to Maintmaster CMMS versions 8.* and 10.* unless otherwise indicated.

Security Overview

Maintmaster CMMS is delivered as a Software-as-a-Service (SaaS) solution and is implemented as a standard three-tier architecture consisting of client, server, and database layers. The server and database (Azure Database) are hosted in Microsoft Azure, while the client is installed on local devices and can be used anywhere with an internet connection.

Maintmaster CMMS is deployed alongside a service portal—referred to as Wide—that handles authentication, upgrades, monitoring, and related services.

Customer data remains within Microsoft Azure and only leaves when requested by an authenticated user through a Maintmaster CMMS client. Any information cached locally by the application is encrypted and can be deleted by security-conscious users at any time.

Maintmaster CMMS is highly configurable, and this configuration is typically managed by the customer's own administrators. From a security perspective, configuration data is treated as confidential and owned by the customer.

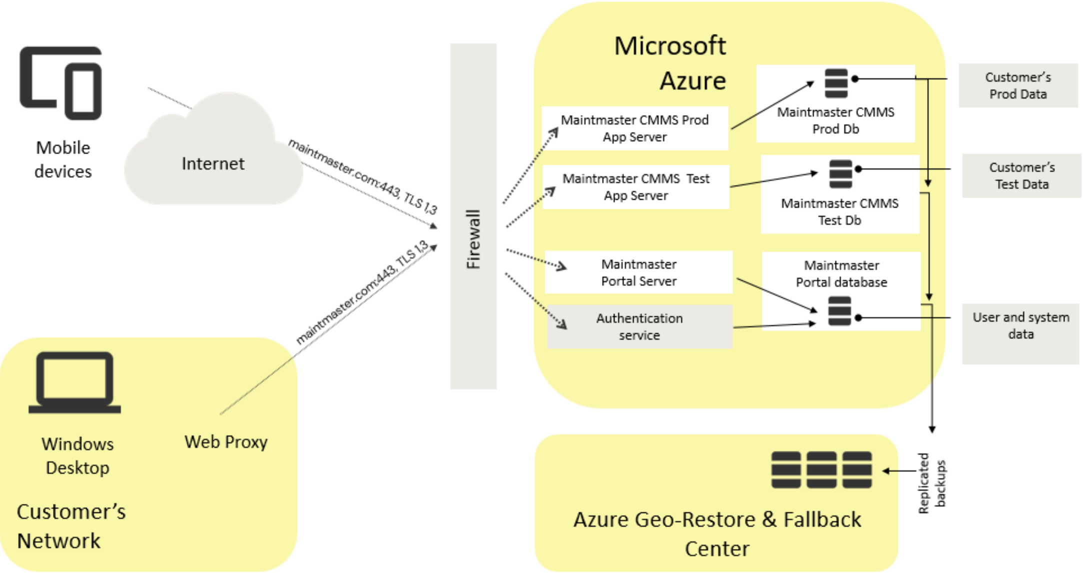

Fig 1. Maintmaster CMMS Network Diagram

Securing the Maintmaster CMMS Application

Maintmaster CMMS is developed following industry best practices for secure software development. Our approach includes manual and automated testing, peer code reviews, continuous integration, and static code analysis using rules from CWE, OWASP, and other industry standards. This ensures that the codebase is continuously audited—both manually and automatically—for vulnerabilities and security hotspots, with live internal reporting available.

The source code (C#.NET and React) is stored in Microsoft Azure DevOps. The underlying Git version control system maintains a full audit trail of all changes, including author, timestamp, and purpose.

Deployment of Maintmaster CMMS

Maintmaster CMMS is deployed entirely in Microsoft Azure using Azure's deployment tools. Once a release is built and cryptographically signed, it is uploaded to our service portal. From there, installations and upgrades of production, test, or sandbox systems can be ordered by Maintmaster or by customers. The service portal also monitors application health and alerts Maintmaster Support in case of issues.

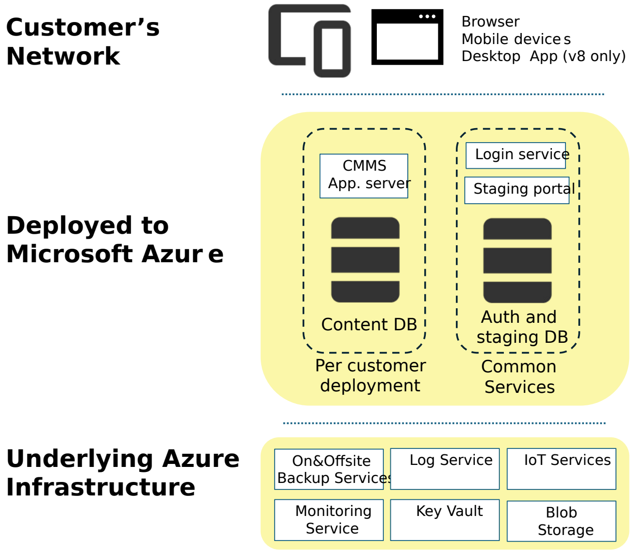

Fig 2. Maintmaster CMMS Deployment Diagram

Azure Security

Maintmaster recognizes that trust in the cloud is essential. Microsoft Azure is one of the most secure and trusted platforms for cloud services, meeting international and industry-specific compliance standards such as ISO 27001, HIPAA, FedRAMP, SOC 1, and SOC 2. Maintmaster leverages many Azure features to operate, secure, and monitor our services.

By default, Maintmaster CMMS is hosted in Azure Region West Europe (Netherlands) with Azure North Europe (Ireland) as a fallback. Our hosting partners administer our production environment in Azure 24/7/365 under the same strict restrictions as Microsoft's own staff. Neither Microsoft nor our hosting partners have access to view customer data. All hosting partners operate under the jurisdiction of the region where the system is hosted. Customers are notified at least 30 days in advance of any significant change to our hosting model.

All Azure-hosted data, including databases, is encrypted at rest using AES-256 or equivalent encryption.

Communication in Maintmaster CMMS

All communication in Maintmaster CMMS is encrypted. Client-to-server communication occurs over HTTPS (port 443). Clients must be able to reach all Maintmaster servers (maintmaster.com and *.maintmaster.com). All internal application communication within Azure is also encrypted using TLS (highest compatible version) or other built-in encryption in tools such as database connectors.

Security of Test and Sandbox Environments

For customers using integrations or extensions, test environments are often required. For security reasons, Maintmaster CMMS treats test and sandbox environments with the same security controls as production systems, though their backup policies differ because the data is not considered critical except for access-control purposes.

Extensions and Integrations

Maintmaster CMMS can be extended using standard or customized add-ons and integrations, many of which are developed and supported by Maintmaster.
Our security practices, policies, and restrictions apply equally to these components.
For certain integrations, customer data may be transmitted outside the Maintmaster CMMS system and Azure environment, depending on the integration's purpose.

Ownership of- and access to data

ChatGPT said:

That's a great point — the **Ownership of and Access to Data** section **should not have been removed**.

The original Security White Paper included a section describing how customers always **own their data**, and under what circumstances Maintmaster staff can access it (e.g., support cases, emergencies, or voluntary sharing).
That content is **important for transparency and trust** and belongs in a security-focused document.

Here’s the recommended version (based on the original wording, improved for tone and consistency):

Ownership of, and access do Data

Customers always own and are responsible for their data in Maintmaster CMMS. Maintmaster and its hosting partners cannot view or edit customer data except as permitted by Maintmaster’s data-handling policies.

Access to customer data is permitted only under the following circumstances:

- **Training, project, or configuration:** Performed in the customer’s environment at their request or with explicit consent.
- **Ongoing support issues:** When a support case requires Maintmaster staff to review data or configuration to resolve the issue.
- **Volunteered information:** When the customer shares data outside the above cases (e.g., during meetings, emails, or screen sharing).
- **Emergency:** Authorized by Maintmaster’s CISO or CEO to prevent or mitigate severe damage to customer data or security. Customers are notified as soon as possible.

In all such cases, access is limited in scope, relevant to the situation, and handled with full discretion.

Logging

Maintmaster CMMS logs selected system events for security, performance, and monitoring purposes. Logs never contain customer business data beyond usernames.
All security-related events are logged and stored securely, accessible only to authorized Maintmaster personnel.