Maintmaster® CMMS Technical White Paper

Maintmaster is a leading CMMS used by manufacturers across the world to optimize operational reliability.

This technical white paper highlights key aspects of the deployment, administration and setup of Maintmaster systems in production and test.

This white paper applies to Maintmaster CMMS version 10.

Maintmaster CMMS Lets You Take Control

Maintmaster CMMS provides the following capabilities:

- Asset management
- Ticket and work order management
- Spare parts and stockroom management
- Integration with OEE and IoT
- Analytics and reports
- Integration with third party systems (for example ERPs)

Our customers rely on Maintmaster CMMS to

- Increase production capacity
- Identify bottlenecks
- Reduce unplanned stops
- Minimize overhead costs

Maintmaster CMMS is designed to be simple to configure and manage. There is no need for the customer to install anything on premises, and you can access the service anywhere if you have a connection to the internet, a web browser or the Maintmaster CMMS app for your mobile device.

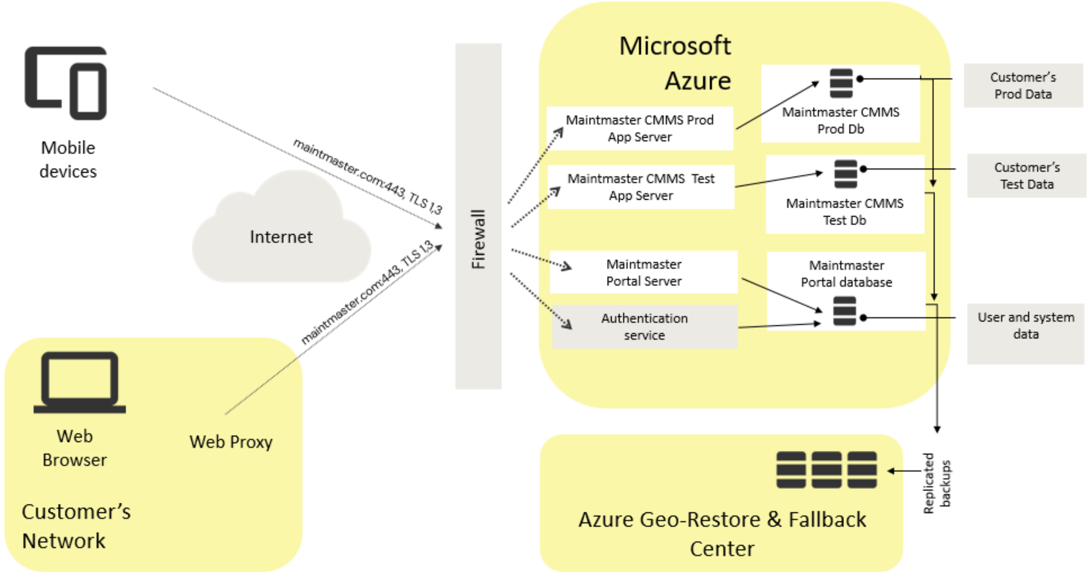

Fig 1. Maintmaster CMMS Architecture Diagram

Maintmaster CMMS is Easy and Scalable

Maintmaster CMMS is delivered as Software-as-a-Service (SaaS) in the public cloud. A web browser, making evaluation and adoption simple. Updates are automatic, eliminating the need for local servers or backup routines, resulting in minimal IT administration. All you need is an Internet connection.

Users can be inside or outside your organization; for example, external service technicians can report their work remotely. Whether you have one user or thousands, Maintmaster CMMS scales to your needs. You can easily add or reduce users as requirements change.

Maintmaster CMMS guarantees up to 99.9% availability outside scheduled maintenance windows. Maintenance windows occur outside normal business hours, last no more than 8 hours, and occur no more than once per quarter unless an emergency security patch is required.

Hosted by Microsoft Azure

Maintmaster recognizes that trust in our deployment in the cloud is crucial. Our hosting partner, Microsoft Azure, is an industry leader in security and privacy. Azure meets a broad set of international and industry-specific compliance standards, including ISO 27001, HIPAA, FedRAMP, SOC 1, and SOC 2. Maintmaster CMMS leverages Azure's robust features to operate, secure, and monitor our services.

By default, Maintmaster CMMS is hosted in Azure West Europe (Netherlands), with Azure North Europe (Ireland) as the fallback location. Backups are replicated to the fallback region to ensure service continuity in the event of a catastrophic failure in the primary region.

Maintmaster uses trusted hosting partners to administer our production systems in Azure under strict supervision and policies. These partners work under the same jurisdiction as the hosted systems. Customers are informed at least 30 days in advance of any significant change to our hosting arrangements.

Security of Your Data – quick points

- Microsoft Azure – Offers more certifications than any other public cloud provider.
- Network security – All data is encrypted (TLS 1.3+) before transmission.
- Encrypted at rest – All data is encrypted at rest using Azure Database encryption (AES-256).
- Privacy security – All passwords are stored in an irreversible format, inaccessible even to Maintmaster technicians and developers.
- Backup – Point-in-time restore available for at least 14 days for all production data, plus monthly distributed backups retained for at least 12 months.
- Disaster recovery – Full environment replication available off-site, including backups, without leaving the designated region.
- Data handling – Maintmaster personnel never access customer data without explicit consent, such as in response to a support request.
- Minimal access – Maintmaster limits access to only those personnel who require it for support and system maintenance.

For a more in-depth look at the security aspects of Maintmaster CMMS, please refer to our security whitepaper.

Backups

Maintmaster uses Microsoft Azure SQL for database management, supporting point-in-time restore (PITR) as well as weekly and monthly backups for long-term storage. PITR allows restoring the system to any point within the configured retention period.

Downloadable backups in BACPAC format are available, which can be read using a supported version of Microsoft SQL Server. From the admin client, you can also export data selections to Excel-readable formats.

Backup retention by edition:

	Sandbox/Test	Team Edition	Standard	Enterprise
Point in time restore	7 days	14 days	14 days	35 days
Weekly backup	-	5 weeks	5 weeks	5 weeks
Monthly backup	-	12 months	12 months	12 months

User Interface

- React
- a11y
- ...

Integrate, Extend, and Connect

Maintmaster CMMS can be integrated with other systems to provide a comprehensive operational view. Maintmaster CMMS Integration Services offers a wide range of ready-made adapters for seamless integration. Maintmaster CMMS Extensions provide a framework for add-ons and custom modifiers, supporting both standardized and enterprise-specific needs.

We Keep an Eye on Your System

Maintmaster continuously monitors system performance, availability, and user interactions. This proactive monitoring helps maintain SLA compliance, detect issues before they affect users, and continuously improve our services. Critical infrastructure is monitored 24/7/365 by experienced technicians.

Maintmaster CMMS User Accounts

Administrators add new users to Maintmaster CMMS and assign roles and permissions during the invitation process. Invitations are sent by email, and new users create a Maintmaster account if they do not already have one.

Azure Entra and SSO

When a new user confirms their account, authentication can be delegated to Microsoft Entra ID (formerly Active Directory). This requires that the customer domain be registered in Entra and authorized for Maintmaster authentication. Setup typically takes around 15 minutes with Maintmaster Support. Once configured, all users in the domain authenticate using Entra ID across all Maintmaster CMMS systems.

Installing Maintmaster CMMS

The server installation is 100% deployed to Microsoft Azure and managed by Maintmaster. Maintmaster CMMS clients are available as modern apps for supported versions of iOS and Android and in your web browser, regardless of operating system. We support most modern browsers.

Reach Our Servers

Maintmaster CMMS communicates via HTTPS (TLS 1.3+) on port 443. Client computers must be able to access all servers in the maintmaster.com domain. Typically, if you can surf the internet using your computer’s web browser, you can use Maintmaster on that computer with no configuration or tweaking needed.

References

Additional resources on Maintmaster CMMS and related topics:

- Maintmaster White Papers
- Maintmaster Downloads
- maintmaster.com

For more information about Microsoft Azure:

- azure.microsoft.com