

Why IT trusts Sockeye and how to get its approval

"Technical deployment was a piece of cake with Sockeye!"

IT Director, AV Nackawic Inc.

Sockeye is an easy-to-use maintenance scheduling tool. It bolts on to SAP, IBM Maximo, JD Edwards or any other CMMS and helps planners build and manage the weekly schedule. This is for the IT person who's been asked to check it before a trial.

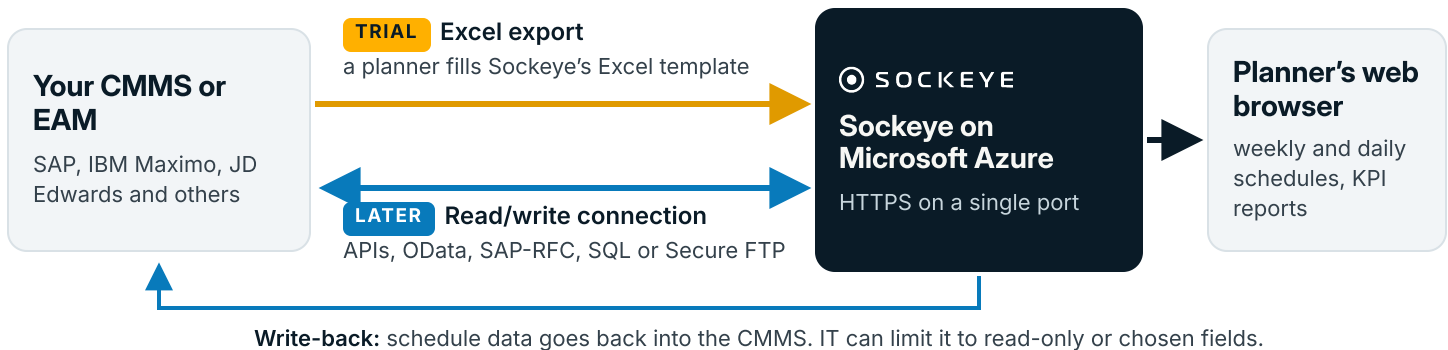
WHY IT TRUSTS SOCKEYE

- **Nothing to install:** it runs in a web browser.
- **The trial starts from an Excel export.** No IT resources needed.
- **Read/write with your CMMS,** scoped to your policy.
- **Hosted on Microsoft Azure,** HTTPS on one port.

HOW TO GET APPROVAL FROM IT

- **Forward these two pages to IT:** how it connects, where the data lives.
- **IT ticks the checklist on page 2.** Two of the five items are already done.
- **Start the trial from an Excel export.** A direct connection and its scope come later, if you choose.

How the data moves



FOR THE TRIAL

File-based start: Excel export

- A planner saves the list of ready work orders from the CMMS to Excel (in SAP, the IW37N list) and fills Sockeye's template, along with crew shift patterns.
- To update, they export again and click Refresh in Sockeye.
- No IT resources and no custom coding. Setup takes about 1 to 2 weeks, then a 1-hour training call.

What data Sockeye uses

- **Work orders:** work order details and scheduling fields for the work that's ready to schedule.
- **Resources:** technician and contractor shift patterns, so Sockeye knows who's available.

AFTER THE TRIAL, IF YOU CHOOSE

Direct connection: read/write

- **Read/write with your CMMS:** Sockeye reads ready work orders and writes schedule data back.
- Options: web services (SOAP or REST), OData, SAP-RFC, SQL (ADO.NET or ODBC), Secure FTP or vendor APIs. For Maximo, the REST API of the Maximo Integration Framework.
- If your EAM has an internet-facing endpoint, the Sockeye Connector runs in Sockeye's cloud and nothing is installed on site. If not, it installs on site as a Windows service.
- IT provides access (API endpoints or database views) and some oversight. Sockeye's team does most of the work; a full rollout takes 4 to 6 weeks.
- IT sets the scope to fit its policy: full read/write, read-only or write-back to specific fields only.

Hosting and security

From Sockeye's security white paper and IT evaluation outline, both linked at the bottom of this page.

Where it's hosted

- Sockeye's back end runs on **Microsoft Azure**. The front end is web-based, with no browser plugins or extensions.
- Azure's datacenters meet ISO/IEC 27001 and 27018, SOC 1, SOC 2, CSA, PCI DSS and HIPAA, among others. These apply to Microsoft's datacenters, not to Sockeye itself.
- Availability guarantee: **99.5%, measured monthly**.
- Test and staging environments are kept physically and logically separate from production.

Network and encryption

- All communication with Sockeye's cloud uses **HTTPS on a single port**, which keeps firewall and gateway rules simple.
- Traffic between users and Sockeye's servers is encrypted with HTTPS and TLS. Backup storage is encrypted at rest.
- Redundant firewalls and intrusion detection or prevention (IDS/IPS) protect the application network.
- Servers run with non-essential services disabled or removed.

Sign-in and access

- Configurable access rights, with several user permission levels.
- Built-in sign-in never stores passwords. It keeps salted one-way bcrypt hashes, following OWASP practice.
- Enterprise accounts can add **SSO (SAML)** and **IP address restrictions**. Those on Sockeye's built-in sign-in can also turn on **2FA** (Azure Multi-Factor Authentication) and a password policy.
- Only Sockeye employees can access Sockeye's servers, on a need-to-know, least-privilege basis that's audited and monitored.

Backups, testing and patching

- **Nightly automated backups** of all production databases, kept on separate Azure servers in a different region. Backup integrity is checked weekly.
- A third-party service scans the application against the OWASP Top 10 continuously, and the code gets regular static analysis.
- Findings from outside scans of the network and servers are ranked by CVSS score; fixes can ship within hours if needed.
- Security updates are applied as soon as practical, typically daily.

What IT needs to do for a trial (ticked = nothing for you to do)

- ☒ **Nothing to install.** Users open Sockeye in a web browser.
- ☐ **Firewall:** Sockeye is reached over HTTPS on a single port. If your network restricts outbound web traffic, ask Sockeye for the address to allow.
- ☐ **Later, only for a direct connection:** give Sockeye read/write access (API endpoints or database views; read-only if your policy needs it) and agree where the connector runs.
- ☒ **No CMMS connection to set up.** During the trial an Excel sheet is the data connector.
- ☐ **Security review:** the white paper covers hosting, access, encryption and monitoring.

Questions from IT before the trial?

getsockeye.com/book-a-demo · sockeyeinfo@getsockeye.com · +1-833-303-3073

[Book a call →](#)

Full detail online: getsockeye.com/sockeye-security-white-paper and getsockeye.com/it-evaluation-outline