Notes for IT & Auditors

A factual description of how the DataWise Connector stores and moves data, written to be handed to an IT provider, auditor or client.

> This document describes how the software behaves. It is written to be read by someone assessing risk, so it states limitations as plainly as it states controls.

1. What the software does

The DataWise Connector is a Windows desktop application. It reads data from a MYOB company file through MYOB's published API and writes a copy into a database on the same computer. It is a one-way copy: the Connector has no facility to create, alter or delete anything in MYOB.

2. Where data is stored

What	Where
The accounting data	A database file in a folder chosen by the customer at install, on the customer's own PC.
Connection settings and MYOB access token	A small registry database in the same folder.
Application settings	The Windows user's application-data folder.

There is no DataWise server involved in storage. DataWise operates no cloud service holding customer accounting data and has no technical means of retrieving it.

3. Data flows

There are three, and they are different from one another. This section is the one most worth reading carefully.

3.1 Synchronisation (MYOB > the customer's PC)

Outbound HTTPS requests from the PC to MYOB's API endpoints. Responses are written to the local database. No other destination is contacted. This traffic is initiated by the PC; no inbound connection to the PC is required, and no port needs opening.

3.2 Local use (Excel, Power BI, reporting tools)

Entirely local. The database is read from disk by whatever tool the customer points at it. Nothing leaves the machine.

3.3 Asking questions in plain English (optional feature)

This flow does send data off the machine, and should be assessed separately from the other two.

The optional question-and-answer feature uses Anthropic's Claude. The database itself is never uploaded — it stays on the PC. However, to answer a question the AI must be shown the relevant results, and **those results are transmitted to Anthropic's API** in the same way as any other prompt the user types.

- The feature is **optional** and is not installed or enabled by default.
- It is **read-only**: the tool that reads the database is opened in read-only mode and accepts only retrieval queries.
- Stored MYOB credentials are **excluded by design** and cannot be read by it.
- Password-locked companies (section 6) obey the same rule as every other tool: **the AI inherits the user's access, never more**. Where the Windows user holds the key, questions work; anywhere else the company is reported as locked and no data is read. The password itself never appears in any output.
- Only data relevant to the question asked is involved; the whole database is not sent.
- Customers with a policy against sending financial data to third-party AI services should simply not enable this feature. Everything else in the product works without it.

> Organisations assessing this feature should review it as they would any other use of a hosted AI service, and refer to Anthropic's own terms regarding data handling and retention.

4. Authentication to MYOB

- Authentication uses **MYOB's OAuth authorisation flow**. The user signs in on MYOB's own web page.
- The customer's MYOB password is never entered into the Connector and is never held by it or by DataWise.
- MYOB issues a limited access token, scoped to reading the data the product needs.
- An administrator of the company file must approve the connection the first time — this is a MYOB requirement, not ours.
- Access can be **withdrawn at any time from within MYOB**, by the customer, without contacting DataWise.

5. Storage of credentials — current position

Credentials the customer supplies — their own MYOB developer key and secret, where they use one, and company database passwords (section 6) — are **encrypted at rest** using the Windows Data Protection API, tied to the Windows user account, so a copied file yields nothing on another machine or under another account.

The access and refresh tokens issued by MYOB are held in the local registry database described in section 2. **They are presently stored without additional encryption at rest**, and are protected by the Windows account and file-system permissions of the machine they sit on.

> **Planned change.** DataWise intends to bring the MYOB tokens under the same DPAPI encryption already used for the credentials above. Ask us for the current status before relying on this in an assessment.

Practical consequence today: a copy of the customer's data folder taken to another machine could be used to reach that MYOB company file until the customer revokes access in MYOB. The folder should therefore be treated with the same care as any folder containing financial records.

6. Optional company-file encryption

From Connector 1.20.0 a company's database can be locked with a password set by the customer. It is off by default; a customer who does nothing keeps plain SQLite files.

- The password becomes the encryption key of that company's database file — **SQLCipher 4, AES-256**, the whole file encrypted on disk. Standard SQLCipher format is used deliberately, so compatible third-party drivers can still open the file *with* the password.
- Without the password the file is unreadable by any software on any machine. A copied folder, an old PC or a lost backup exposes nothing for a locked company.
- On the syncing machine the key is held DPAPI-protected so unattended scheduled syncs continue. The key does not travel with the data folder.

- DataWise never sees or stores the password and **cannot recover it**. A forgotten password is resolved by resetting and re-syncing the company from MYOB — time is lost, data is not.
- Unlocking a company re-encrypts it back to plain SQLite.

A customer-facing description, including the support and Excel/Power BI implications, is in the separate **Company File Security** guide.

7. Access control

The application does not implement its own user accounts. Access is governed by the controls already in place on the computer:

- **The Windows account login** is the primary control.
- **File-system permissions** on the chosen data folder.
- **Full-disk encryption** (for example BitLocker) where organisational policy requires it.

This is a deliberate choice. An application-level password alone would gate the user interface while leaving the database file beside it readable by any other tool. Where a customer wants the file itself protected, the company-file encryption in section 6 provides the substance: there the password is the encryption key, not a screen in front of a readable file.

8. What DataWise can see

Nothing. DataWise holds no copy of customer accounting data, has no remote access to customer machines, and could not produce customer data if required to. Support is provided by conversation; where a customer chooses to send us a file to diagnose a problem, they control what is sent.

9. Third parties involved

Party	Role
MYOB	Source of the data. The customer's own MYOB subscription and terms apply.
Anthropic	**Only if** the optional question feature is enabled — see section 3.3.
DataWise	Supplies the software and a licence check. Holds no accounting data.

What the licence check involves: at registration the customer supplies a name, company and email address; nothing further is required and no verification email is sent. Each periodic check sends the product, the MYOB company-file identifier, the application version and sync counts — **never accounting data** — and the reply is cryptographically signed so the application cannot be fooled by an impostor server. Trials and licences are bound to the MYOB company-file identifier, not to the email address. An email-confirmation facility (six-digit code, stored only as a hash, expiring in minutes, with limited attempts) exists and can be invoked from the application when confirming an address matters; it is not part of routine setup.

10. Integrity and reversibility

- The Connector cannot write to MYOB. There is no code path that creates, edits or deletes MYOB records.
- The local database is a copy. If it is lost, it can be rebuilt from MYOB.
- If the subscription ends, synchronisation stops and the existing database remains on the customer's PC, fully readable.
- No customer data is held hostage by, or dependent on, DataWise continuing to trade.

11. Recommended customer controls

- Include the data folder in the organisation's normal backup routine.
- Restrict the data folder to the users who need it.
- Apply full-disk encryption where the machine is portable or shared.
- Consider the per-company password (section 6) for company files whose contents are sensitive within the organisation.
- Review who holds administrator rights on the MYOB company file.
- Decide deliberately whether the optional AI question feature is permitted, and document that decision.

> **Questions from an auditor or IT provider are welcome.** Email sales1@datawise.co.nz or ring Mark on 021 296 5298. We would rather answer a hard question directly than have someone guess from a brochure.