SMB Solutions
CLOUD SERVICES

Direct Backend Access for AI, MCP and LLM Tools

What it involves, the risks you take on, and the terms on which we can grant the access

More of our customers are asking us to open up direct access to their SAP Business One Service Layer, or to their database, so they can connect their own choice of MCP server, database client or LLM. We're glad to see this level of curiosity and ambition. It tells us you're taking AI seriously, and we want to support you.

Before we do, we owe you an honest conversation. Connecting an AI tool to a live ERP backend is not the same as connecting it to a spreadsheet or a read-only report. Once the connection exists, the AI (or whatever tool you've pointed at it) can read, and often write, real transactional data: the same data your invoicing, stock, general ledger and reporting depend on. This document explains in plain language what can go wrong, why we can't fully protect you from it once you hold the keys, and what we ask of you before we switch it on.

1. What “Direct Access” Actually Means

When you ask us for direct Service Layer or database access so you can bring your own MCP server or LLM, you are asking for a connection that sits outside our managed hosting environment. In practical terms:

- Your chosen tool talks to SAP Business One directly, using credentials we issue to you.
- Queries and, in many setups, write operations are generated by an AI model from natural-language prompts, yours or your users'.
- There is no SMB Solutions logic sitting between the model's output and your live data to check whether a query or update makes business sense.
- Whatever guardrails exist are only the ones you or your chosen tool provider have built in. We cannot see, test or vouch for them.

This is fundamentally different from a managed, vendor-controlled integration, where requests pass through a tested layer of business logic before they touch your data. With a direct connection that layer doesn't exist.

2. The Risks, in Plain Language

None of this is meant to scare you off. It's meant to make sure you go in with your eyes open. An AI model is very good at sounding confident and entirely capable of being confidently wrong, and a live ERP backend does not forgive mistakes the way a document or spreadsheet does.

Risk area	What can go wrong	Why it happens
Data integrity and corruption	Records created or changed in ways that bypass SAP Business One's own business logic, validations and add-on triggers, leaving stock, GL postings or document numbering inconsistent.	The Service Layer and database will accept a technically valid call even if it makes no business sense. A direct or AI-generated call can step around rules that the SAP Business One client enforces.

Risk area	What can go wrong	Why it happens
Incorrect or invented answers	The AI confidently reports a wrong figure, joins the wrong tables, or misreads a user-defined field or customisation unique to your database, and the person reading it can't tell.	LLMs generate plausible output, not verified output. Without a validation layer that understands your specific configuration, a wrong query can still produce a convincing-looking answer.
Security exposure	A compromised laptop, account or third-party MCP tool becomes a direct path into your live ERP data. Credentials may be stored or logged in places you don't control.	Direct access widens the attack surface beyond what we can monitor. We secure our infrastructure; we cannot secure the tool, device or model you choose to connect.
Performance and stability	Slow, unindexed or poorly scoped queries place unexpected load on the database and can affect every other user on the system.	An LLM has no inherent sense of query cost. A prompt that seems simple can generate an expensive or table-locking query.
Support and accountability	When something looks wrong, it becomes much harder to establish whether the cause was the hosting, SAP Business One itself, or the tool you connected.	A third-party MCP server or LLM sits outside our visibility and, in most cases, we can't see its logs.

3. It's Not as Simple as It's Been Made to Sound

Much of the marketing around “connect your database to any LLM” makes it sound like a five-minute job. Technically, plugging in a connection is often quick. What gets glossed over is everything downstream of that connection:

- SAP Business One's data model is complex: header and line tables, user-defined tables and fields, and add-on customisations that a generic AI tool knows nothing about.
- “The AI will figure it out” is not a safety mechanism. A model will answer confidently even when it has misunderstood your schema.
- Read access can still cause real problems when wrong answers drive real decisions. Write access can cause immediate and sometimes irreversible data damage.
- Most off-the-shelf MCP servers and “connect your database” tools are built for generic databases, not for SAP Business One's structure, locking behaviour or business rules.

We say this not to discourage you, but because we'd rather you hear it from us now than discover it the hard way in your live environment.

4. Our Position on Direct Access Requests

Please read this section carefully. It sets out the terms on which we can grant this access.

The data in your SAP Business One system is yours, and it is reasonable for you to want to use it with tools of your choosing. If, having read this document, you still want direct Service Layer or database access, we will support that request on the following terms:

- **Access is granted at your request and for your purposes. You choose the tool, the model and the prompts. We do not control or review any of them.**
- **We are not responsible for the behaviour of AI models, MCP servers or other software you connect. We did not build them and cannot guarantee what they will do with the access you have asked us to grant.**
- **To the maximum extent permitted by law, we are not liable for data loss, data corruption, incorrect business decisions, downtime or any other loss or damage arising from your use, or misuse, of the access granted or the tools you connect to it.**
- **SMB Solutions manages the hosting infrastructure only. Support for SAP Business One itself, including users, authorisations, licensing and integrations, remains with your SAP Business One support partner. We are not able to diagnose or repair problems caused by third-party AI tools or MCP servers acting on your data, and where we agree to assist, that work will be charged as professional services.**
- **You are responsible for maintaining backups you are comfortable relying on, and for the security of the credentials and devices used to connect.**

This is a risk acknowledgement, not legal advice. We recommend your own advisor reviews the access agreement before you sign.

5. Safeguards We Recommend

We'd rather help you do this safely. Options worth considering, several of which we can configure on request:

- **Start read-only.** Grant read access only, adding write access later and only if genuinely needed.
- **Use a restricted account.** A dedicated Service Layer user with least-privilege permissions, scoped to only the objects and companies it needs.
- **Query a copy, not production.** A reporting replica removes the risk of an inefficient or malformed query affecting live operations.
- **Test in a sandbox first.** Trial the integration against a test company database before pointing it at live data.
- **Keep activity logs.** So that if something goes wrong there is a record of what the tool actually did.
- **Limit query cost and volume** where your chosen platform allows it, to protect performance for everyone else.

6. Next Steps

If you'd like to proceed, tell us which safeguards above you'd like configured and we will prepare the access, together with a short access agreement referencing the terms in Section 4, for signature.

Contact us

Richard Duffy, CEO · richard@smbsolutions.com.au · +61 407 460061
Support: support@smbsolutions.com.au
AU +61 1300 442 059 · NZ +64 9 974 9196 · USA +1 800 241 3213 · UK/IRE +44 20 3005 2737

7. Acknowledgement

By signing below, you confirm that you have read and understood this document and accept the terms in Section 4 in respect of any direct Service Layer or database access granted to your organisation.

Company _____

Name _____

Position _____

Signature _____

Date _____