SMB Solutions
CLOUD SERVICES

SMB SOLUTIONS
KNOWLEDGE BASE ARTICLE

How to Create a Read-Only User for the SAP Business One Service Layer

Article type	Knowledge base article
Topic	Read only User SAP Business One Service Layer
Applies to	SAP Business One 10.0, version for SAP HANA, on SUSE Linux Enterprise Server
Last updated	2 November 2026
Audience	Customers and business owners (non-technical)
Classification	Customer

Knowledge Base Article · Updated November 2026

Overview

Yes, you can create a read-only user for the SAP Business One Service Layer. The Service Layer has no security model of its own: it signs in with a standard SAP Business One user and enforces the same authorisations as the SAP Business One client. A user with **Read Only** authorisations can retrieve data (GET) but is refused when it tries to create, change or delete data (POST, PATCH, DELETE).

This is the recommended approach for reporting tools, dashboards, integrations and AI agents that only need to read data from SAP Business One.

Applies to: SAP Business One (SQL Server and SAP HANA editions) with the Service Layer enabled.

> **Who to contact:** SMB Solutions manages your hosting infrastructure. Your SAP Business One support partner manages SAP Business One and application-level support, including users, authorisations, licensing and integrations. Please ask your SAP Business One support partner to carry out the steps in this article.

Procedure

Create a dedicated user for the integration, grant it Read Only authorisations on only what it needs, then confirm that write requests are refused.

1. In SAP Business One, go to **Administration > Setup > General > Users** and create a new user for the integration. Do not use a superuser, and do not reuse a person's login.
2. Go to **Administration > System Initialization > Authorizations > General Authorizations** and select the new user.

© 2026 SMB Solutions Cloud Services. All rights reserved. | smbsolutions.com.au | support@smbsolutions.com.au

3. Set **Read Only** on the windows and objects the integration needs. Setting a parent node cascades to its child nodes, but any child item that has no Read Only option is set to No Authorization, so check the result (see SAP KBA 3767657). Leave everything else at **No Authorization**, because least privilege is safer than blanket read access.
4. Save the changes.
5. Test the user through the Service Layer (see below) before handing the credentials to the consuming application.

Testing the user

1. Log in to the Service Layer with the new user (POST to the `Login` endpoint).
2. Send a GET request to an entity the user should be able to read, for example `BusinessPartners?$top=1`. It should return data.
3. Send a POST or PATCH request to the same entity. It should fail with a permission error, which confirms the user cannot write.
4. Test the specific endpoints your integration uses, not just one. Authorisations are set per entity, so a user can read one entity and be refused on another.

Things to check

Most problems with read-only Service Layer users come from a handful of easily missed settings.

- **Authorisations are per entity.** Each Service Layer entity maps to an SAP Business One window or object authorisation, so you need the right ones for each endpoint the integration calls. Business Partners, Items and Sales Orders are straightforward.
- **User-defined tables and objects.** User-defined tables (UDTs) and user-defined objects (UDOs) have their own authorisation sections, including under **Authorizations > General Authorizations > User-Defined Objects**. These are easy to miss.
- **SQL queries and views.** If the integration uses `SQLQueries` or `SQLViews`, set the query authorisations accordingly. A read-only user running a saved query can read anything that query exposes, so review what each query returns.
- **Actions such as Close and Cancel.** These should map to write authority, but test the specific actions you care about rather than assuming.
- **Licensing is separate from authorisations.** The user type and licence (Professional, Limited or Indirect Access) is a different matter from what the user is authorised to do. Each Service Layer session consumes a licence, and third-party or integration access is typically covered by Indirect Access licensing. Confirm your requirements with your SAP Business One support partner.
- **Enforcement is at the application level.** The Service Layer connects to the database with its own service account, so there is no database-level read-only equivalent. The restriction relies entirely on the SAP Business One authorisations.

Best practices when connecting an LLM to live ERP data

A read-only user stops an AI tool from changing your data, but it does not stop the tool from exposing, misreading or overloading it. Treat the large language model (LLM) as an untrusted component, and control what it can see, where that data goes and how hard it can query your live system.

- **Limit what it can read, not just what it can write.** Read Only still means the user can read everything it is authorised for, including costs, margins, pricing, employee and bank details. Grant access only to the entities the use case needs, and create a separate user for each tool or use case rather than one

© 2026 SMB Solutions Cloud Services. All rights reserved. | smbsolutions.com.au | support@smbsolutions.com.au

broad shared account. OWASP lists excessive permissions as a root cause of its “Excessive Agency” risk (OWASP).

- **Respect individual permissions.** Where possible, have the AI act with the permissions of the person asking, so staff cannot use it to see data they could not open in SAP Business One.
- **Treat all ERP data as untrusted input (prompt injection).** Text stored in records, such as item descriptions, remarks, business partner notes, attachments and emailed documents, can contain hidden instructions that a model may follow. OWASP describes this as indirect prompt injection and ranks prompt injection as the top LLM risk (OWASP). Do not combine broad access to sensitive data with the ability to send information out (email, web requests, webhooks) in the same agent.
- **Know where your data goes.** Check where the model is hosted, whether prompts and responses are retained or used for training, and where data is processed. Confirm the terms meet your privacy and data residency obligations. Send only the fields needed, and exclude or mask bank account numbers, tax identifiers and personal data where you can. For Australian organisations, the OAIC recommends due diligence on any AI product and a privacy impact assessment before adoption (OAIC).
- **Prefer curated access over free-form queries.** Give the AI a defined set of approved queries or tools, with an allowlist of entities and parameters, rather than letting it build arbitrary Service Layer requests. This addresses the excessive functionality cause of Excessive Agency (OWASP).
- **Protect production performance.** Unbounded queries against live data can slow SAP Business One for everyone. Use filters, `$select`, `$top` and paging, prefer saved SQL queries or views for heavy reporting, apply rate limits, and consider a reporting copy for large analysis. Reuse and close Service Layer sessions, since each one consumes a licence. OWASP covers runaway resource use as “Unbounded Consumption” (OWASP).
- **Do not trust figures without checking.** An LLM can misread a result or make arithmetic errors. For financial and operational numbers, use deterministic queries or reports as the source, have the AI show the records or query it used, and verify before acting on the answer. OWASP covers this as “Misinformation” (OWASP).
- **Keep humans in control of any writes.** If you later allow the AI to create or change data, use a separate user, create drafts rather than posting documents, and require human approval for each action. The Australian Cyber Security Centre has warned that AI agents can take unexpected actions their operators did not intend or authorise (ASD’s ACSC).
- **Secure the credentials.** Store the Service Layer password in a secrets manager, never in prompts or files the model can read. Rotate it regularly, restrict access by network address where possible, and use a valid TLS certificate. The ACSC advises strong authentication, access controls and network segmentation around AI systems (ASD’s ACSC).
- **Log, monitor and test.** A dedicated user makes auditing simple: log requests, review them for unusual volumes or entities, and alert on anomalies. Test first against a non-production company database, including attempts to trick the AI into revealing or misusing data. See the joint guidance on deploying AI systems securely (CISA, ASD’s ACSC and partners).
- **Set governance.** Document the approved use cases and an owner for each integration, review the user’s authorisations periodically, and tell staff what the AI can and cannot access. The NIST AI Risk Management Framework is a widely used structure for this (NIST).

Optional: add a second layer of protection

If you need a hard guarantee that nothing can write through the Service Layer, restrict HTTP methods at the load balancer or reverse proxy in front of it, allowing only GET plus POST for the login and logout endpoints. This is an infrastructure change, so request it through SMB Solutions Support. Your SAP Business One support partner can confirm which requests the integration needs.

© 2026 SMB Solutions Cloud Services. All rights reserved. | smbsolutions.com.au | support@smbsolutions.com.au

Be aware that `$batch` requests are sent as POST. If the consuming application uses `$batch` to read data, blocking POST broadly will break it. In that case, restrict by path or rely on the SAP Business One authorisations alone.

Need help?

SMB Solutions manages the hosting infrastructure, and your SAP Business One support partner manages SAP Business One and application-level support. Contact the right team for your request:

- **Your SAP Business One support partner:** creating the user, setting authorisations, licensing, working out which entities an integration needs, and troubleshooting permission errors.
- **SMB Solutions Support:** infrastructure matters, such as network access to the Service Layer, load balancer restrictions and server availability.

SMB Solutions Support contact details:

- **Email:** support@smbsolutions.com.au (creates a support ticket automatically)
- **Australia:** +61 1300 442 059
- **New Zealand:** +64 9 974 9196
- **USA:** +1 800 241 3213
- **UK / Ireland:** +44 20 3005 2737

Sources and further reading

SAP Business One

- SAP Community: Service Layer authorisations follow the same restrictions as the SAP Business One client. Answered by an SAP expert, who also notes that restrictions do not apply to superusers.
- SAP Knowledge Base Article 3767657: Understanding the “Read Only” permission behaviour in general authorizations. Requires an SAP support login.
- For the Authorizations window itself, see the SAP Business One documentation on help.sap.com for the version and patch level you run.

AI security and privacy

- OWASP GenAI Security Project: Top 10 for LLM Applications. OWASP has also published a newer edition, so check the project page for the current release.
- ASD’s ACSC: Engaging with Artificial Intelligence
- ASD’s ACSC: Risks of AI misalignment to Australian organisations
- CISA, NSA, FBI, ASD’s ACSC and partners: Deploying AI Systems Securely
- OAIC: Guidance on privacy and the use of commercially available AI products
- NIST: AI Risk Management Framework

© 2026 SMB Solutions Cloud Services. All rights reserved. | smbsolutions.com.au | support@smbsolutions.com.au