

POSTMAN @ DT IT

Regine Schickentanz | Thomas Ganter



The main issue

“Postman automatically syncs ...”

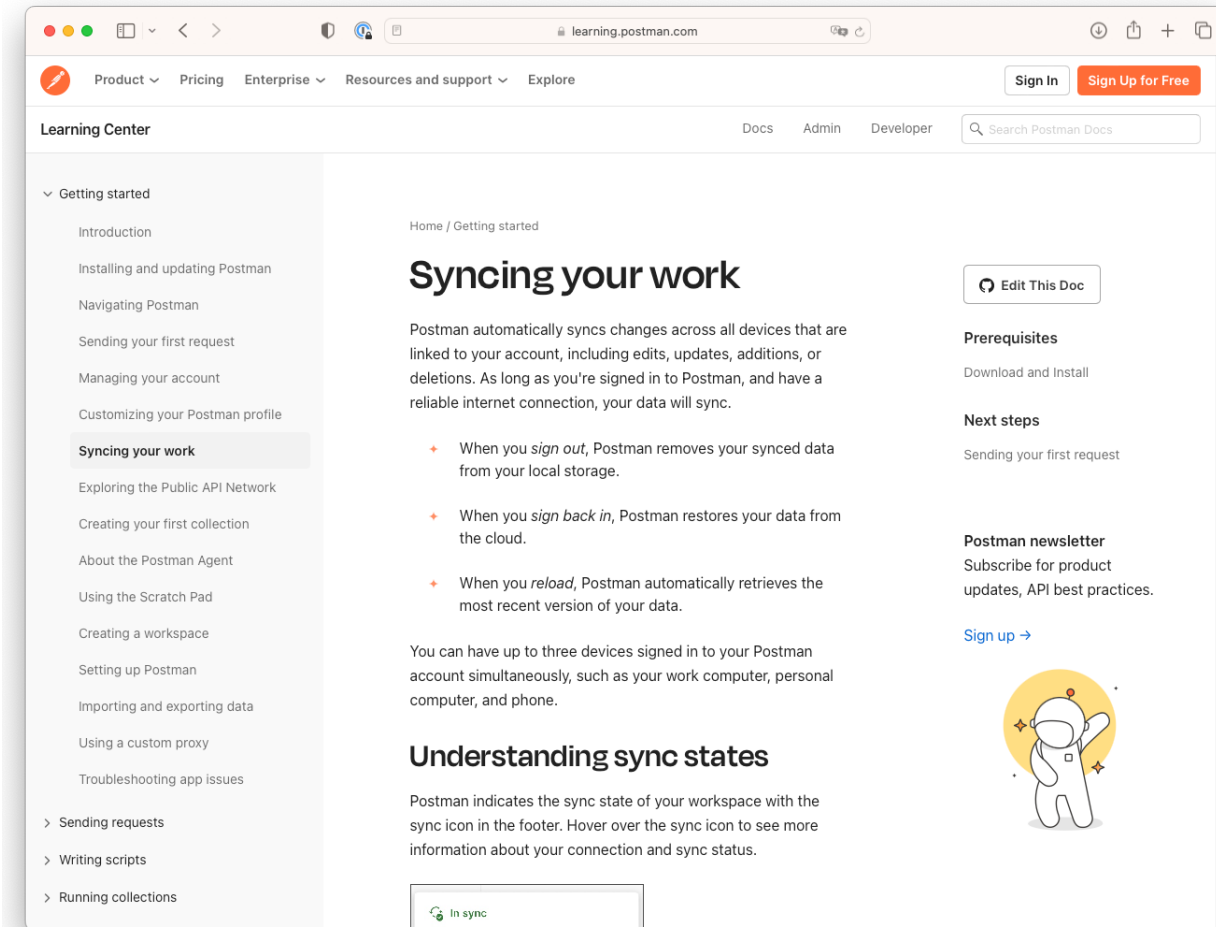
The documentation in the Postman “trust center” confirms that

All customer data is stored in databases on Amazon RDS, which are configured securely. [...]

this posts a serious problem, as this customer data also includes API keys, Client IDs+Secrets and all API details. Postman claims to strongly encrypt the data.

As we have seen — in DTIT Stability Learning Sessions — that Postman was used as part of post-install verification procedures, this exposes confidential data into the public cloud.

Also ... there is no self-hosted version for Postman to run isolated on-premises. Hence, we have a problem.



While we sort this out — the interim recommendation

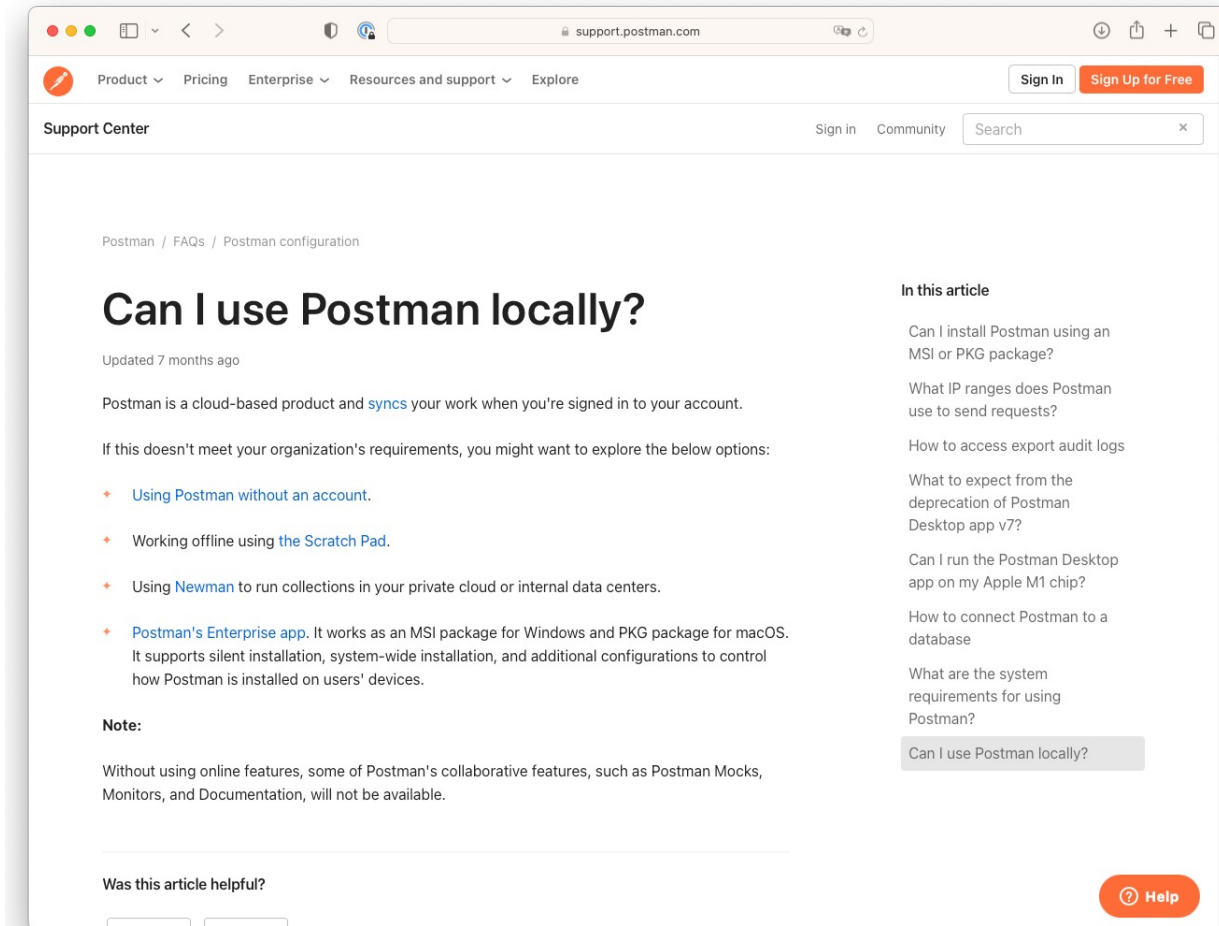
Sorting this out, alongside the friends from License Management and T-Sec, is still ongoing and probably will need some more time.

Until there is a final word on Postman usage, these are the mandatory steps to **implement immediately**:

- **Sign Out** of the Postman Account in the GUI
- **Delete** any Postman Account that was used for work at DT
➤ <https://tiny.telekom.de/3t3>
- **Change** all secrets that were stored in Postman

Note:

Compliance to these steps is not optional nor open to interpretation.

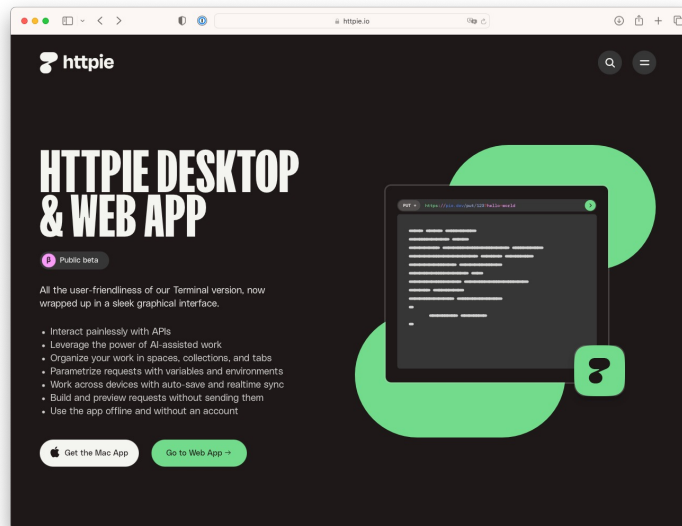


But wait — there are alternatives

Other GUI Products

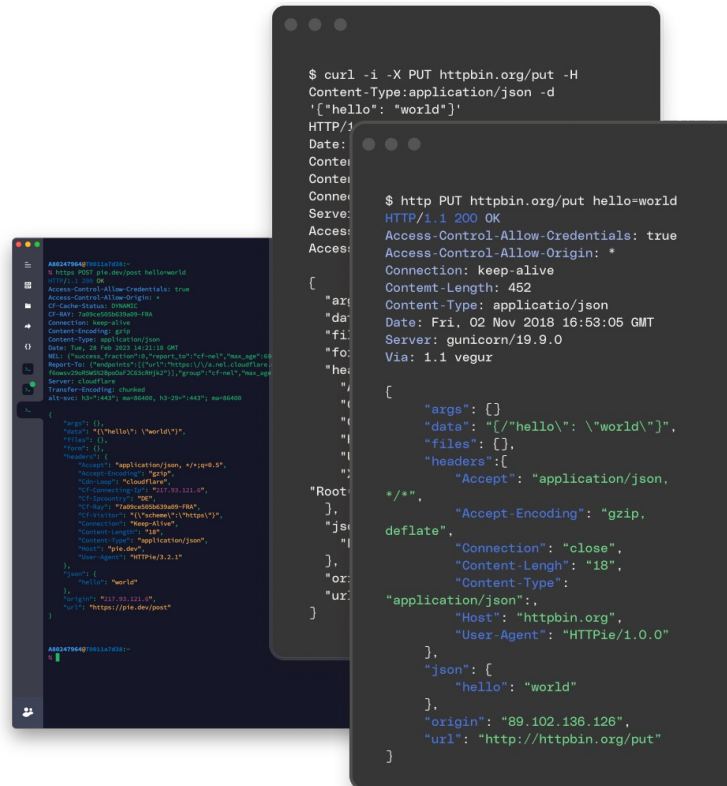
There are a few hundred API testing tools out there, and currently there is not one recommended tool as the issue only surfaced.

When looking around, look for tools *without account* and for *offline usage*.



Using the Terminal

Sounds crazy, but curl or HTTPie can be easily scripted to create API tests that are reliable and repeatable.

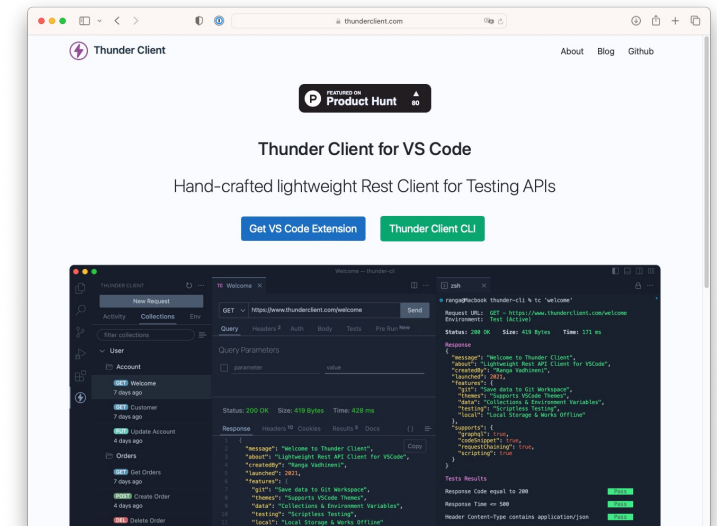


IDE Integration

In many IDEs, API testing plugins exist and can be used with the same caveats as for other GUI products:

no account and *no synchronization*.

A very popular plugin for VSCode is thunder client:



Next step:

“GO FORTH AND SYNC NO MORE”

“I’m a BO IT and don’t know what to to”

- ▶ Share Slide 4 with your teams!