

Reporting a security issue

DOCUMENT	VERSION	STATUS
SB-GD-142	1.0, October 2026	Public. Checked against the product, October 2026

Who this is for

Security researchers, customers and anyone who believes they have found a vulnerability in SynapBridge.

Before you start

- Reports go to one mailbox: security@synapbridge.com.
- Do not post details publicly, and do not access, change or delete data that belongs to other people.
- If you are unsure whether something counts, send a short note first. A borderline report is better than a missed one.

How to report

Email security@synapbridge.com. Plain email is the only reporting channel described here.

Include as much of the following as you can:

- 1 A short summary of the issue and where it occurs (page, endpoint or feature).
- 2 The steps to reproduce it, with any request and response samples.
- 3 What you think an attacker could do with it.
- 4 The time you tested and the account or workspace you used, so the team can find it in logs.
- 5 How you would like to be contacted.

Please do not send real customer data, secrets or tokens you came across. Describe where they appeared instead.

What to expect

The SynapBridge Trust center states these targets for vulnerability reports:

- Acknowledgement within two business days.
- Triage and severity assignment within five business days.
- Updates every fourteen days until the report is closed.
- Remediation targets of seven days for critical, thirty for high and ninety for medium issues.

Source: the Trust center answer to "How do I report a vulnerability?". These are targets, not promised fix dates.

Good-faith research

Please act in good faith:

- Test only against accounts and workspaces you own or have permission to use.
- Use the smallest amount of access needed to show the issue.
- Stop and report as soon as you reach data that is not yours.
- Avoid actions that degrade the service for others, such as heavy automated load or denial of service.
- Allow reasonable time for a fix before you share details.

The Trust center states: "Good faith research within the published scope will not be pursued legally, and we will say so if a third party pursues action against a researcher acting within the policy." This statement does not bind third parties.

Rewards and recognition

There is no paid bug bounty today. The Trust center lists a paid programme as a roadmap item and does not claim it yet.

Limits and notes

Note Our security.txt file is at synapbridge.com/.well-known/security.txt. It lists the same contact address.

- A written scope list is not part of this document. If you are unsure whether a system is covered, email before testing.
- This page is not legal advice.
- Response targets come from the Trust center text and may change when that text changes.