

Download Verification Guide

How to Verify the Authenticity and Integrity of SyncBackPro

2BrightSparks Pte Ltd • April 2026

1. Overview

This guide explains how to verify that your SyncBackPro download is authentic (produced by 2BrightSparks) and unmodified (not tampered with since publication). Enterprise customers may need to document these verification steps as part of their software supply chain controls.

Always download SyncBackPro exclusively from the official 2BrightSparks website:
<https://www.2brightsparks.com/download-syncbackpro.html>

2. Verify the Digital Signature (Recommended)

All SyncBackPro installers and executables are digitally signed with a code-signing certificate issued to 2BrightSparks Pte Ltd. This is the most reliable way to verify authenticity.

2.1 Verify the Installer Before Installation

- Right-click the downloaded installer file (e.g., SyncBackPro64_Setup.exe)
- Select Properties, then click the Digital Signatures tab
- You should see a signature from "2BrightSparks Pte. Ltd."
- Click the signature entry, then click Details
- The Digital Signature Details dialog should state: "This digital signature is OK"

If the Digital Signatures tab is missing, or the signature shows as invalid, do not install the file. The download may have been corrupted or tampered with. Re-download from the official website and verify again.

2.2 What to Look For

Signer Name	2BrightSparks Pte. Ltd.
Signature Status	"This digital signature is OK"
Timestamp	A countersignature timestamp from a trusted CA

3. Verify the SHA-256 Hash

2BrightSparks publishes SHA-256 hash values for downloadable packages on the download page. You can use these to independently verify that the file you downloaded matches exactly what was published.

3.1 Using PowerShell (Windows 10/11)

Open PowerShell and run:

```
Get-FileHash .\SyncBackPro64_Setup.exe -Algorithm SHA256 | Format-List
```

Compare the output hash value with the hash published on the 2BrightSparks download page. They must match exactly.

3.2 Using Command Prompt

Open Command Prompt and run:

```
certutil -hashfile SyncBackPro64_Setup.exe SHA256
```

4. Verify After Installation

After installing SyncBackPro, you can verify the installed executable:

- Navigate to the SyncBackPro installation directory (typically C:\Program Files\2BrightSparks\SyncBackPro)
- Right-click SyncBackPro.exe, select Properties, then Digital Signatures
- Confirm the signature from "2BrightSparks Pte. Ltd." is present and valid

5. Ongoing Verification

When SyncBackPro checks for updates, it contacts the 2BrightSparks website over HTTPS to check the current version number. No customer data is transmitted. Updates are downloaded manually by the user from the official website, and are themselves digitally signed. We recommend verifying the digital signature of every update before installation.

For audit documentation, you may wish to screenshot the Digital Signatures properties dialog and the hash comparison as evidence of verification for your records.