

SDS200A Driver Installation and Use Guide

Customer guide for Windows x64

Release 2026.10.27.1 | Guide revision 2 | 27 October 2026

Use this guide with the manufacturer-supplied SDS200A maintenance ZIP and its separate `release.json`. The package repairs the device INF signing gap by enrolling a local publisher certificate with the customer's explicit approval. It is not a Microsoft WHCP-certified driver release.

1 Before you start

Device and computer requirements

This package is for the softDSP SDS200A USB oscilloscope, hardware ID `USB\VID_0DA8&PID_0001`, on Windows 10 or Windows 11 x64 client editions. ARM64, x64 emulation on ARM, and Windows Server are not supported.

SoftScope2 2.5.0 must already be installed. This ZIP is a driver maintenance package, not the SoftScope application installer. Use the supplied launchers, which run Windows PowerShell 5.1. Administrator approval is required for installation and removal.

What has been verified

The verified Windows 10 host had Secure Boot off and HVCI inactive. The tool did not change those settings. The result does not demonstrate operation with Secure Boot or HVCI enabled.

Condition	Verification status
Windows 10 Pro 22H2 x64, build 19045.2006	Connected-device installation passed on an existing SoftScope2 host: device problem code 0, exact INF binding, original WinDriver kernel running.
Windows 11 user confirmation	On 27 October 2026, the user confirmed successful real waveform acquisition in SoftScope2. Windows version/build and security settings were not recorded.
Core installation on a new PC and persistence after restart	Not separately verified. Complete the customer checks on page 3 on each target PC.

Prepare the installation

1. Save your work and close SoftScope2 before changing its driver.
2. Obtain the ZIP and `release.json` from the manufacturer's trusted distribution channel. Check the ZIP SHA-256 against `archiveSha256` in `release.json`.
3. Extract the complete ZIP to a local folder. Keep its folders and files together; do not run it from inside the ZIP.
4. Connect the SDS200A USB cable before installation so the tool can verify the connected device.

2 Check the package and publisher

Customer files

File	Purpose
Check.cmd	Checks package integrity and reports available device, kernel and trust information. It does not change drivers, certificates or security settings.
Install.cmd	Shows publisher identity and trust scope, asks for INSTALL, then requests Windows UAC approval.
Remove.cmd	Asks for REMOVE, then requests UAC approval to remove the exact maintenance device package.
manifest.json / SDS200A-Legacy-Support.cer	Package file hashes and publisher identity / public certificate. No signing private key or PFX is supplied.

Run the check first

Double-click Check.cmd. A successful check reports CHECK_ONLY_NO_CHANGES and packageIntegrity VERIFIED. Read deviceVerification, Ready, kernel and deviceQueryError as well. Check-only exit code 0 means the package checks completed; it does not prove that the device is connected or ready. The device query can be unavailable even when the check exits 0.

Verify the certificate before accepting trust

Expected subject: CN=softDSP SDS200A Legacy Support (Local Trust), O=softDSP.

Expected SHA-1 certificate thumbprint: B8AC53C3A96B7F9CDB0391F08364E09BE0D5229C. Compare all 40 characters with the launcher, manifest.json and the separately supplied release.json. This certificate fingerprint is different from the ZIP SHA-256.

Certificate expiry: 27 October 2031, 10:18:19 UTC. If the certificate is outside its validity period, request an updated package. Do not change the computer clock to bypass the check.

Installation adds this certificate to the local computer's Trusted Root Certification Authorities and Trusted Publishers stores. Trust can also apply to other code signed with the same certificate; it is not limited to one INF file. The signature verifies integrity and signer identity, not code safety, measurement accuracy or Microsoft certification.

3 Install and verify operation

Installation steps

1. Double-click `Install.cmd` in the extracted folder. Review the displayed certificate fingerprint, expiry and trust scope.
2. If you approve that local trust change, type the exact uppercase token `INSTALL` and press Enter. Pressing Enter without `INSTALL` cancels the request.
3. Approve the Windows User Account Control prompt using the customer's authorized administrator account. Enter credentials only in the Windows prompt.
4. Wait for the installer process to finish. Its separate console is hidden; the launcher displays the exit code and result/log locations afterwards. Do not start a second installation while it is running.
5. Read `result.json` where available. Cancellation can exit 0 without installing anything. An exit code alone is never proof of installation or acquisition.

Understand the installation result

Result	Meaning and action
0 + <code>DEVICE_READY_SOFTWARE_NOT_VERIFIED</code>	Connected device problem code 0, exact package INF/service binding and running original kernel were verified. SoftScope acquisition is still unverified.
2 + <code>STAGED_DEVICE_NOT_CONNECTED</code>	The package was staged, but no connected SDS200A was found. Check the USB connection and run <code>Check.cmd</code> ; do not record operation as verified.
3010 + <code>PENDING_REBOOT</code>	Windows requested a restart. Save your work, restart normally, then check the device and application. The tool does not restart automatically.
1 or <code>FAILED_OR_PARTIAL</code>	Installation did not complete or may have made partial changes. Keep the first error and logs; follow page 4 before retrying.

Complete the customer acceptance checks

1. With the USB cable connected, run `Check.cmd` again. Confirm Ready is true, device problem code is 0 and the expected original kernel is running. Resolve any `deviceQueryError` before treating the device check as verified.
2. Open SoftScope2 and confirm that it connects to the physical SDS200A rather than running in demo mode.
3. Follow the original hardware manual's input ratings and grounding instructions, acquire a known safe test signal, and confirm that the waveform updates. Record the SoftScope version and result; the maintenance tool does not perform this test.
4. After a normal Windows restart, repeat the connected-device and waveform checks. Record restart persistence separately.

4 If a check or installation stops

Use the first confirmed error

Do not repeatedly run `Install.cmd` or replace drivers at random. Keep the exact first error, result code and `result.json` if one was created. A launcher precheck failure, cancelled UAC prompt or early removal failure may not create a result file. In that case, record the displayed message.

Message or condition	Next action
SHA256 mismatch, unexpected publisher, invalid catalog or expired certificate	Stop. Obtain a complete, current package and matching <code>release.json</code> from the manufacturer. Do not edit the INF, CAT or manifest to make a check pass.
No connected SDS200A, or Ready is false	Confirm the correct device and USB connection. Reconnect the cable and run <code>Check.cmd</code> . A staged package alone is not a working-device result.
A different WinDriver kernel / incomplete existing WinDriver installation	The tool deliberately stops instead of overwriting it. Send the first error and relevant diagnostics to support so the existing installation can be assessed.
Administrator required or UAC cancelled	No authorized installation has completed. If you intend to proceed, use the approved launcher and the customer's authorized administrator account.
Kernel blocked, device binding not ready, Code 52 or a Windows 11 policy restriction	Stop and request a compatible driver assessment. Local INF certificate trust does not override kernel policy. Do not disable security features.
PENDING_REBOOT / 3010	Perform one normal restart after saving work, then repeat the device and acquisition checks. Do not reinstall merely because the restart is pending.

Windows 11 limitation

The user confirmed successful waveform acquisition on Windows 11. The version/build and security settings were not recorded, so this result does not establish compatibility with every Windows 11 environment. The original Jungo kernel dates from 2010 and may be restricted by the target PC's kernel trust policy.

This package does not enable test mode, disable driver signature enforcement, turn off Secure Boot or HVCI, remove kernel policies, use Windows Update or change wuauserv. If the original kernel cannot run under the customer's policy, installation stops instead of weakening that policy.

5 Removal and support records

Remove the device package

1. Close SoftScope2 and double-click Remove.cmd in the intact extracted package.
2. Review the scope, type the exact uppercase token REMOVE, then approve UAC. Read the final result and any restart request.
3. Normal removal targets only the exact maintenance SDS200A INF package. It preserves the shared Jungo WinDriver kernel and local certificate trust. Removal does not reinstall a previous device driver.

For advanced operations, open administrator Windows PowerShell 5.1 with the extracted folder as its current location. Use the commands below. The execution policy exception applies only to that PowerShell process.

The additional option removes trust only from stores recorded as added by this tool. If no ownership record exists, trust removal is skipped. A record for a different machine or publisher stops removal. First assess the effect on other packages signed with the certificate. The shared kernel remains installed.

Preview the removal target

```
powershell.exe -NoProfile -ExecutionPolicy Bypass `
-File ".\Remove-SDS200A.ps1" -CheckOnly
```

Remove the device package and the trust added by this tool

```
powershell.exe -NoProfile -ExecutionPolicy Bypass `
-File ".\Remove-SDS200A.ps1" -Remove -RemoveLocalPublisherTrust
```

Find the records

Use the actual paths shown by the launcher. ProgramData is normally hidden; paste its path into File Explorer. Check.cmd normally prints its report to the window rather than creating an installation log. Some errors occur before any result record is created.

Location	Contents
%ProgramData%\softDSP\SDS200A-Legacy\runs\	A separate run folder for actual installation/removal: result.json; native.log when native commands ran; setupapi-tail.log and codeintegrity-events.json when failure diagnostics were collected.
%TEMP%\softDSP-SDS200A\	Fallback result.json for an early Install-SDS200A.ps1 failure when available. TEMP belongs to the account running the elevated installer and may differ from the signed-in customer's TEMP.

Send only the information needed

Provide the package version, Windows version/build/architecture, SoftScope version, first exact error, result code and relevant result/log files. Logs are not uploaded automatically. Before sharing, remove unnecessary computer names, user-specific paths, device serial numbers and unrelated device data; retain hardware VID/PID, error codes, hashes and signature details needed for diagnosis.

Never send passwords, access tokens, recovery keys, PFX files or signing private keys. If a renewed release uses a different signing certificate, verify its new fingerprint and trust scope separately; the old certificate's trust does not automatically transfer.