

hh2 software is now digitally signed

Windows can now confirm that an hh2 program really came from hh2 and hasn't been altered.

PUBLISHER

hh2 Cloud Services

Verified by Microsoft

What this means for finance and payroll teams

You don't need to do anything. This is a security update to the hh2 software installed on your accounting server. Please forward this document to whoever manages that server.

One thing worth knowing: a Windows service named **hh2 Thin Client** needs to stay running. If it's stopped or disabled, data from your accounting system stops reaching hh2. You'd see missing or stale information until it's running again.

01 What changed

Our programs are signed

Every program the hh2 Synchronization Client installs now carries a digital signature issued to **hh2 Cloud Services** and verified by Microsoft. Where the Sync Client Installer used to show the publisher as unknown, it now names us. This starts at 26.29.0.

Our programs say who we are

Some hh2 programs used to report no company name at all, which made them hard to identify in Task Manager or a security console. Every one of them now reports **hh2 Cloud Services** and the product it belongs to.

02 About the hh2 Thin Client service

If your Synchronization Client has updated to 26.28.0 or later, you have a second Windows service named **hh2 Thin Client**. It's a genuine hh2 component, installed by the update your team approved, and it needs to stay running.

What it does

It's the new connection between your accounting system and hh2. Older components ask hh2 for instructions every few seconds, around the clock. The Thin Client instead holds one secure connection out to your own hh2 site and waits to be told when there's work. It's quieter on your network, it recovers from outages on its own, and settings now live in hh2 rather than on your server.

What it does on your network

- Outbound only, over encrypted TCP 443.
- Connects only to your own hh2 web address, the one your staff sign in to. No new destination to allow.
- No inbound listener, no open ports, no firewall changes.
- Not a remote-access tool. It installs no software and reaches no documents, browsers, or mail.
- No long-lived credentials on the machine. Each delivery uses a short-lived, write-only, single-use permission.

03 Signature details

Service name	hh2ThinClient
Executable	hh2.ThinClient.exe
Publisher	hh2 Cloud Services
Certificate subject	CN=hh2 Cloud Services, O=hh2 Cloud Services, L=Kaysville, S=Utah, C=US
Issued through	Azure Artifact Signing
Trust	Chains to a Microsoft root already in Windows
Runs as	LocalSystem, automatic start

For IT: verify the signature yourself.

```
$svc = Get-CimInstance Win32_Service -Filter "Name='hh2ThinClient'"
$exe = $svc.PathName.Trim("")
Get-AuthenticodeSignature $exe | Format-List Status,
SignerCertificate, TimeStamperCertificate
```

Run this in PowerShell on the accounting server to confirm the file is signed by hh2 Cloud Services.

On 26.29.0 and later, **Status** returns **Valid**, the signer is hh2 Cloud Services, and the timestamp is populated. You can see the same under Properties, Digital Signatures. Builds before 26.29.0 were not yet signed. The signing key lives in a Microsoft-managed hardware module certified to FIPS 140-3 Level 3. No hh2 employee can export it.

04 Two things that look wrong but aren't

A SmartScreen warning can still appear

Downloading the installer with a browser can bring up "Windows protected your PC." That check asks whether Microsoft has seen this file downloaded widely yet, not whether it's signed, and a new signing identity starts with no history. Select **More info** and confirm the publisher reads hh2 Cloud Services. If it says anything else, stop and contact our Support Team at support@hh2.com. Machines that update themselves aren't affected.

The folder says Digital Business Integration

The install path and Programs and Features still show that name. It was hh2's registered company name before it became hh2 Cloud Services. The certificate carries the current legal name, which is why the two differ.

05 If your team already disabled it

- Service stopped or disabled: run `sc.exe config hh2ThinClient start= auto`, then `sc.exe start hh2ThinClient`.
- Executable missing: a security product quarantined it. Restore it and allow the service, or re-run the installer.
- If you added an exception by file path, replace it with one based on the publisher **hh2 Cloud Services**. It will survive future updates.
- The service reconnects on its own, and a machine that's been offline catches up. Please contact our Support Team at support@hh2.com or 877.442.9327, so we can confirm it reconnected.

One more thing. When 26.28.0 added the Thin Client, some IT teams found a program they didn't recognize, running with system privileges, with no signature and no company name, and turned it off. That was the right call with the information they had. We should have told you it was coming, and we're sorry we didn't. Signing is our answer. It gives your security team something to verify instead of something to take on trust.

NEED HELP?

support@hh2.com · (877) 442-9327

hh2 Cloud Services
601 Boro Street, Kaysville, UT
84037