

ControlSuite : Components fail to create license tokens and log "Tamper detected" when the server has no internet access

000046006 | Troubleshooting | Last updated 2026-09-15 | ControlSuite, ControlSuite AutoStore, ControlSuite Equitrac, ControlSuite Output Manager, ControlSuite Shared Components

ISSUE

After an installation or upgrade, one or more ControlSuite components fail to obtain a licence on a server with no internet access. Depending on the component:

- Users cannot log in at the MFP, or the device cannot connect to the server after a login attempt.
- Equitrac licence token files are not created under C:\ProgramData\Nuance\Equitrac\CAS, \DCE and \DRE.
- Output Manager reports **A VALID LICENSE IS NOT INSTALLED** (message ID 2691), or shows a blank licence server and ID with status "not installed".

The Configuration Assistant shows the licence as applied and the licensing service as running, so nothing appears wrong on the Licensing page. The distinguishing signature is a tamper-detection error in the component log or the Windows Application event log:

```
<font face="Courier">license reference creation failed. {'Internal error: 1201:516, MID=0, SID=0, EID=6
```

Output Manager records the same fault as Exception description: MID=0, SID=0, EID=6.

CAUSE

ControlSuite licensing uses the Flexera FlexNet Embedded client, a set of digitally signed DLLs installed alongside each licensed component. Before loading them, the Flexera library verifies their signature. "Tamper detected" means that verification failed, not that any file has been altered.

Verification needs the signing chain's root certificate in the server's Trusted Root Certification Authorities store. Windows supplies these on demand from Windows Update rather than shipping them all in advance, so on a server with no internet access, or one whose updates are managed so the root update never arrives, the certificate is missing or stale. Verification fails, the component cannot create its licence token, and it behaves as unlicensed.

Two things make this easy to misdiagnose. The licence server is healthy: it is the client-side signature check that fails, so pointing the server at a different licence server does not help. And no licensing request is issued at all, so a network trace shows nothing and an infrastructure investigation finds nothing.

The root most often missing is **USERTrust RSA Certification Authority** (friendly name Sectigo), which secures the timestamp countersignature. That countersignature became load-bearing when the Flexera signing certificate expired on Sep 4, 2024, so a server can begin failing on a date unconnected to any change made to it.

SOLUTION

1. Confirm the cause

Run this in an elevated PowerShell session on the affected server. Nothing needs downloading or installing:

```
<font face="Courier">Get-ChildItem $env:ProgramFiles -Recurse -Filter 'Flx*.dll' -ErrorAction SilentlyContinue |  
    Select-Object @{n='Folder';e={$_.DirectoryName}}, Name,  
                  @{n='Signature';e={(Get-AuthenticodeSignature $_.FullName).Status}} |  
    Sort-Object Folder | Format-Table -AutoSize</font>
```

Any Signature status other than Valid confirms this cause. Where ControlSuite was installed to a drive other than the system drive, substitute that drive's Program Files path.

Expected locations, for orientation. The command above is the reliable way to find the files, because the install drive varies and the file names differ by component:

Component	Folder	Files
Equitrac CAS, DCE, DRE	%ProgramFiles%\Kofax\Equitrac\{Accounting Service Device Control Engine Document Routing Engine}	FlxCore64.dll, FlxComm64.dll
AutoStore	%ProgramFiles%\Kofax\AutoStore	FlxCore.dll, FlxCClientCommon.dll, FlxLicensingClient.dll
Output Manager	%ProgramFiles%\Kofax\Output Manager, under Services\DBM and Services\Flexera, or DBM and Flexnet depending on release	FlxCore64.dll

2. Let Windows retrieve the certificate

If the server can reach Microsoft's certificate distribution point, Windows retrieves the missing root itself, and this is the least invasive fix. Full internet access is not needed. The server requires outbound **HTTP (TCP 80)** to `ctldl.windowsupdate.com`, and name resolution (**TCP and UDP 53**).

Once that access is in place, re-run the command in step 1. When every DLL reports Valid, restart the affected services as in step 5. If the status has not changed, allow for the daily certificate trust list refresh before moving on.

Check first whether `DisableRootAutoUpdate` is set to 1 under `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\SystemCertificates\AuthRoot`. It is applied deliberately on some ControlSuite servers to remove a job-list delay, and where it is present this step will not work even with the access above. Use step 3 or 4 instead.

3. Import the current Microsoft roots (permanently offline servers)

On a Windows machine that does have internet access, from an elevated command prompt in the folder where the file should be written:

```
<font face="Courier">certutil.exe -generateSSTFromWU roots.sst</font>
```

Copy `roots.sst` to the affected server, then from an elevated command prompt in the folder containing it:

```
<font face="Courier">certutil.exe -addstore -f root roots.sst</font>
```

This adds every current Microsoft third-party root to the machine's Trusted Root store. On a hardened or segregated server that is a change to the machine's trust configuration and the customer's security team may need to approve it. Where a narrower change is required, use step 4.

4. Install only the required root certificate

On a Windows machine in the same environment whose DLLs verify correctly, open `certlm.msc`, expand **Trusted Root Certification Authorities > Certificates**, right-click the required root, then **All Tasks > Export** and choose **DER encoded binary X.509 (.CER)**.

Copy the file to the affected server and import it from an elevated prompt:

```
<font face="Courier">certutil.exe -addstore -f root C:\Temp\root.cer</font>
```

Verify the certificate before installing it. For USERTrust RSA Certification Authority: thumbprint 2B8F1B57330DBBA2D07A6C51F70EE90DDAB9AD8E, serial 01FD6D30FCA3CA51A81BBC640E35032D, valid Feb 1, 2010 to Jan 18, 2038. It can also be downloaded from the [Sectigo Root Certificates](#) page.

5. Restart and confirm

- 1 Restart the services for each component whose DLLs failed verification.
- 2 For Equitrac, confirm licence token files now appear under `C:\ProgramData\Nuance\Equitrac\CAS, \DCE and \DRE`.
- 3 Re-test: log in at a device, or check the Output Manager Licence Information tab.

What does not resolve this

Clearing the licensing server cache is reasonable for other licensing faults and does not address this one. Stopping the licensing service, deleting `C:\ProgramData\flexnetsas` and `C:\Windows\ServiceProfiles\NetworkService\flexnetls`, restarting and re-applying the licences leaves the tamper error in place, because the failure is in the client-side signature check rather than in the licence data. The same applies to requesting a replacement licence file, reinstalling the licensing service, and changing the licence server ID.

When to contact Technical Support

If every Flexera DLL reports Valid and the tamper error persists, the licensing server logs are needed. Stop the licensing service, edit `%ProgramFiles%\Kofax\Shared Services\Licensing\server\flexnetls.xml` to append `-logging-threshold debug` to the `<arguments>` node, restart and reproduce. Provide the contents of `C:\ProgramData\flexnetsas` and `C:\Windows\ServiceProfiles\NetworkService\flexnetls` with the case.

APPLIES TO

Product	Version
ControlSuite — Equitrac (CAS, DCE, DRE), AutoStore, Output Manager, and the licensing service in Shared Services	1.4 through 2025.2. Confirmed on 1.4 FP2, 1.5 and 2025.2.

This is an environmental condition rather than a defect in a particular release, so it is not limited to the versions listed. It is usually noticed after an installation or upgrade, because that is when licence tokens are created afresh.

REFERENCES

- Revenera: [Unpatched Windows system causes XT kit tamper detection](#)
- Microsoft: [certutil command reference](#)
- Microsoft: [Configure trusted roots and disallowed certificates in Windows](#)
- KB 000017605 — ControlSuite: Delay to View Job list (if the servers have no Internet access). Sets DisableRootAutoUpdate, which conflicts with step 2.

<https://aio-eus-uat-cae-aif-app14-local.redglacier-35d7ee4f.eastus.azurecontainerapps.io/article/46006>