

ControlSuite: Delay to View Job list (if the servers have no Internet access)

000017605 | Troubleshooting | Last updated 2026-09-15 | ControlSuite

Problem:

There can be a delay when viewing the job list on the device. After logging in, the jobs are not shown; logging in a second time or refreshing the page displays them. This occurs on ControlSuite servers without internet access.

Cause:

The delay occurs during the TLS handshake between Print Job Management (PJM) and Security Framework (SFS), and can add around 15 seconds to the call.

During the handshake, the Windows Certificate Trust List (CTL) updater engine attempts to refresh its trusted and disallowed certificate lists from Microsoft. On a server with no internet access that request fails, and the handshake waits for it to time out before proceeding. The delay therefore originates in the Windows certificate update path rather than in ControlSuite, which is why it affects any server in that network position.

Solution:

Three options, ordered least to most disruptive. The first two address the cause and leave certificate updating intact. The third suppresses the symptom and carries consequences that the customer should agree to first.

Option 1 - allow the certificate list endpoints through the firewall (recommended)

Allow the affected server outbound access to Microsoft's trusted and disallowed certificate lists:

```
<font face="Courier">http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/authroot
http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab</font>
```

This is a change on the customer's network rather than to ControlSuite, and it resolves the delay without weakening certificate handling. Where outbound access is not permitted at all, an internal CTL distribution point can be configured and maintained instead.

Option 2 - deploy the required root certificates by Group Policy

Where the endpoints above cannot be opened, deploy the third-party certification authority certificates the server needs through Group Policy, on an as-needed basis. This gives more granular control over which authorities the server trusts.

Option 3 - disable the CTL updater engine (last resort)

- 1 Export and save a backup of HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\SystemCertificates\AuthRoot.

- 2 Create the following DWORD values under that key:
"EnableDisallowedCertAutoUpdate"=dword:00000000
"DisableRootAutoUpdate"=dword:00000001
- 3 Reboot the server and test.

To reverse the change, restore the exported key and reboot.

Before applying Option 3, confirm the customer accepts both consequences.

- EnableDisallowedCertAutoUpdate set to 0 stops the server receiving Microsoft's list of revoked and distrusted certification authorities. The server will continue to trust an authority after Microsoft has distrusted it. This is a change to the machine's security posture and the customer's security team may need to approve it.
- DisableRootAutoUpdate set to 1 stops Windows retrieving root certificates on demand. This blocks the remedy described in article 000034640, where ControlSuite components fail to create licence tokens and log "Tamper detected" because a root certificate is missing. A server carrying this setting will not recover on its own even after it regains internet access, and the missing root must then be imported manually.

Applies to:

Product	Version
ControlSuite	All versions

The delay arises from Windows certificate update behavior on a server without internet access, which is not specific to a ControlSuite release.

References:

- ControlSuite : Components fail to create licence tokens and log "Tamper detected" when the server has no internet access.
- Microsoft: [TLS handshake errors and connection timeouts? Maybe it's the CTL engine](#)

<https://aio-eus-uat-cae-aif-app14-local.redglacier-35d7ee4f.eastus.azurecontainerapps.io/article/17605>