

Issues when ControlSuite server is not internet connected

000017776 | Troubleshooting | Last updated 2026-09-15 | ControlSuite

Question:

What problems will I have if my ControlSuite server is not internet connected?

Answer:

Support has reported cases where on the Equitac DCE server, internet (or specific communications) was not available.

Delays may be caused by attempts to update TLS certificates by CTL (Certificate Trust List) engine on a new login (connection) and TLS establishment from Print Job Management (PJM) servers.

THE WORKAROUND:

According to the following Microsoft (MS) article, TLS handshake delays could be caused by CTL (Certificate Trust List) updater engine on machines which do not have internet access: <https://techcommunity.microsoft.com/t5/ask-the-directory-services-team/tls-handshake-errors-and-connection-time-outs-maybe-it-8217-s-the/ba-p/400501>

To verify if the Windows CTL updater engine is causing a TLS handshake delay, there is a need to temporarily disable it for both the trusted and untrusted CTLs and then attempt our TLS connections again.

To disable it:

- Create a backup of this registry key (export and save a copy)
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\SystemCertificates\AuthRoot
- Then create the following DWORD registry values under the key
"EnableDisallowedCertAutoUpdate"=dword:00000000
"DisableRootAutoUpdate"=dword:00000001

To revert the above registry changes, restore the backup.

Please evaluate the following for more permanent solutions:

For the untrusted CTL:

- The automatic disallowed root update mechanism is a built-in OS feature, so consider allowing access to the public Microsoft disallowed CTL URL from users' machines; <http://crl.dl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab>
OR
- Configure and maintain an internal untrusted CTL distribution point.

For the trusted CTL:

- For server systems, consider deploying the trusted 3rd party Certificate Authority (CA) certificates via Group Policy (GPO) on an as-needed basis.
- For workstation client systems, consider:
 - Allowing access to the public allowed Microsoft CTL
URL <http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/authrootstl.cab>
OR
 - Defining and maintaining an internal trusted CTL distribution point as outlined in Configure Trusted Roots and Disallowed Certificates.
OR
 - If you require a more granular control of which CAs are trusted by client machines, you can deploy the 3rd Party CA certificates as needed via GPO.

Applies to:

Product	Version
ControlSuite	1.0
ControlSuite	1.1
ControlSuite	1.2

<https://aio-eus-uat-cae-aif-app14-local.redglacier-35d7ee4f.eastus.azurecontainerapps.io/article/17776>