**List of cases for troubleshooting, when you have problems with CEM connection**

**All these cases are described, using SMP 7.5 SP1 release**

* **Case:** Impossible to enable "**Reporting**" for added SMP Server in CEM Gateway and you're receiving "Failed to contact the server and retrieve the certificate details" pop-up message





Error message appears in Altiris Log Viewer on SMP Server:

* Unable to get the client certificate response XML associated with the specified request (Request: , Exception: Altiris.NS.Exceptions.NSComException (0x00000005): The caller is unauthorized to request a new client certificate.at Altiris.Web.NS.Agent.GetClientCertificateBase.GetClientCertificateXml())

**1st Root cause:**

* You're using a non "***Application Identity***" credentials.

**1st Solution:**

* Make sure that you're using account from "Symantec Administrators" role and which is also "Application Identity" account as well = You need to use "Application Identity" account to enable reporting for added SMP Server in "CEM Gateway".

****

**2nd Root cause:**

* You have "SMP Agent CA" certificate is without private key in "Trusted Root Certification Authorities" on SMP Server. Probably due manual incorrect export/import when private key wasn't included to export.

An error message will appears in Altiris Log Viewer on SMP Server:

* Unable to get the client certificate associated with the specified request (Request: <resource typeGuid="2C3CB3BB-FEE9-48DF-804F-90856198B600" name="gateway\_server" policyKey="AAAAAQAB1gdc1fHZ39lhs0AcRYGeoQa03QcSREnObHFykbYbAxa/gDG5IlDq8LXifUAZfV45uaR52rPlKHDUZU6ePSu++W5021/bfZhsIfLfbP5x6rUtQB8AI11C6IHc3NnqrA4aN6SQxgnWuhePqXDVRPXSNLGZrHlTWN5sqkya6Dm9Zi+mpEuhM64ig4jZkwaVJqaw55GmMOBZKc3folKteSUgd7Y+pLZa+xdO1fFK4W1iU47Zl9rd9HYgh7xgVfcCVfyHwO8Nkc4cdTVK+Q2zKqS1V+9+9Fj2IoT7HdLTtvkpXxuHzNeb3m+pw==">
                                <key name="name.domain" value="gateway\_server"/>
                                <key name="fqdn" value="gateway\_server"/>
                                <regRequest fqdn="gateway\_server"

**2nd Solution:**

* If you have "SMP Agent CA" certificate without private key, then ask support to restore "SMP Agent CA".
* **Case:** Managed endpoint is in Internet and has CEM enabled and connected to NS via CEM Gateway but unable to register with SMP



But in SMA logs it throws an error:

* <![CDATA[Tunnel connection using IP: ***<Your CEM Gateway address>***, Port: 443]]>
<![CDATA[WARNING: Unexpected response from URL 'https:// ***<Your SMP Server address>***:443/Altiris/NS/Agent/GetClientCertificate.aspx': Unable to get the client certificate response XML associated with the specified request (Exception: The caller is unauthorized to request a new client certificate.)]]>
severity='1' hostName='client' source='ConfigServer' module='AeXNSAgent.exe' process='AeXNSAgent.exe' pid='8144' thread='9056' tickCount='15455187' >
  <![CDATA[Attempted CEM nsagent certificate negotiation failed.]]>
severity='2' hostName='client' source='ConfigServer' module='AeXNSAgent.exe' process='AeXNSAgent.exe' pid='8144' thread='9056' tickCount='15455187' >
  <![CDATA[Configure Server Mode: CEM mode was not initialized succesfully, will retry]]>
severity='2' hostName='client' source='Agent' module='AeXNSAgent.exe' process='AeXNSAgent.exe' pid='8144' thread='9056' tickCount='15455187' >
  <![CDATA[Failed to register agent. Registration status 'Not registered'. Next retry in 8 min.]]>

**1st Root cause:**

* You've added a SMP Web Site :443 in CEM Gateway, instead of "Symantec Agent" Web Site :4726

**1st Solution:**

* Remove SMP Web Site:443 from CEM Gateway and add required "Symantec Agent" Web Site :4726

**2nd Root cause:**

* You've installed "CEM Offline" package on new computer, which is unknown for SMP Server, but this computer is currently in Intranet and isn't in Internet network.

**2nd Solution:**

* <http://www.symantec.com/docs/TECH213911>
* **Case:** CEM offline Agent package generation fails

An error appears in Altiris Log Viewer on SMP Server:

* "Error executing Task  (6bfeb1d8-b6ff-4e28-aae5-391d709854fb). Exception: System.InvalidOperationException: Https NS base URL must be used Internet-based Client Management agent. The agent package cannot be correctly created.
   at Altiris.NS.AgentManagement.AgentPackageBuilder.BuildSitePackageFile(String siteIdentifier, IEnumerable`1 gateways, IEnumerable`1 resourceTargets, IEnumerable`1 organizationalGroups, String additionalInstallParams, DateTime requestedPackageExpiry, AgentPackageParameters packageParams, DateTime& packageExpiry, Guid& packageID)
   at Altiris.NS.AgentManagement.BuildAgentPackageItemTask.ExecuteTask(Hashtable taskArgs, ItemTaskState state)

**Root cause:**

* You have a HTTP URL for SMP Server in "Agent Install" settings page.

**Solution:**

* Open SMP Console -> Settings -> Agents/Plug-ins -> Symantec Management Agent -> Settings - > Symantec Management Agent Install
* Click on settings, Be sure that if "Specify different Notification Server" is check that the provided URL schema is HTTPS
* <http://www.symantec.com/docs/TECH226441>
* **Case:** Warning message appears in log viewer on CEM Gateway machine after each restart of Gateway service

Warning message in log viewer on CEM Gateway machine:

* RSA server certificate CommonName (CN) ` ' does NOT match server name!?","InternetGateway.Status","InternetGateway","1036","Warnings"

**Root cause:**

* By default "Server Name" is set to "localhost" in "C:\Program Files\Symantec\SMP Internet Gateway\Apache\Conf\httpd.conf



**Solution:**

* Change current "Server Name" to your Common name of server in "C:\Program Files\Symantec\SMP Internet Gateway\Apache\Conf\httpd.conf where CEM Gateway is running -> restart CEM gateway service. This warning message should not appear anymore in log.
* **Case:** Client has lost connection with CEM Gateway because client's date is different than on CEM Gateway.

SMA log throws these messages:

* source='ServerSettings' module='AeXNSAgent.exe' process='AeXNSAgent.exe' pid='7088' thread='6524' tickCount='104539623' >
* <![CDATA[Detected invalid basic inventory update time (2015-01-30 20:32:11), resetting time for next update (this can happen when changing time zones)]]>
* source='ServerSettings' module='AeXNSAgent.exe' process='AeXNSAgent.exe' pid='7088' thread='6524' tickCount='104539623' >
* <![CDATA[Next basic inventory update will be sent to server ***<Your SMP Server address>*** at 2015-01-26 20:33:15, in 1440 minutes]]>
* source='MsCryptoSslDataTransformerImpl' module='AeXNetComms.dll' process='AeXNSAgent.exe' pid='7088' thread='6524' tickCount='104540169' >
* <![CDATA[NS Server certificate is expired or not yet valid. (0x80090328)]]>
* source='ConfigServer' module='AeXNSAgent.exe' process='AeXNSAgent.exe' pid='7088' thread='6524' tickCount='104542478' >
* <![CDATA[Policy request failed: The requested name is valid, but no data of the requested type was found (0x80072AFC)]]>

**Root cause:**

This problem occurs, when client has date older than, for example for a 2 days than on CEM Gateway.

* CEM Gateway date: 1/25/2015
* Client in CEM date: 1/23/2015

**Solution:**

* Make sure that you have a correct date on CEM client machine.
* **Case:** Client in CEM mode has lost connection with CEM Gateway because administrator has changed current certificate to another self-signed or "3rd party" certificate for "Symantec Agent" :4726 Web Site on SMP Server.

SMA throws these messages in log:

* source='MsCryptoSslDataTransformerImpl' module='AeXNetComms.dll' process='AeXNSAgent.exe' pid='7088' thread='6524' tickCount='104683971' >
* <![CDATA[InitializeSecurityContext error while client handshake: The certificate chain was issued by an authority that is not trusted (0x80090325)]]>
* source='NetworkOperation' module='AeXNetComms.dll' process='AeXNSAgent.exe' pid='7088' thread='6524' tickCount='104686280' >
* <![CDATA[Operation 'Connect' failed.
* Protocol: http
* Host: ***<Your SMP Server Address>***
* Port: 443
* Path: /
* Http status: 0
* Secure: Yes
* Error type: DNS error
* Error result: 0x80072AFC
* Error code: 0
* Error note: Failed to resolve FQDN and short name to IP address
* Error message: The requested name is valid, but no data of the requested type was found]]>
* source='ConfigServer' module='AeXNSAgent.exe' process='AeXNSAgent.exe' pid='7088' thread='6524' tickCount='104686280' >
* <![CDATA[Policy request failed: The requested name is valid, but no data of the requested type was found (0x80072AFC)]]>

**Root cause:**

* Client is running in CEM mode, but administrator has changed current certificate to another self-signed or "3rd party" certificate for "Symantec Agent" web site :4726 on SMP -> "CEM Gateway" server hasn't yet refreshed/installed this new certificate on own side.

**1st step Solution:**

* After changing a certificate for "Symantec Agent" Web Site :4726 on SMP Server to another self-signed certificate or "3rd party", administrator must as soon as possible refresh this new certificate on "CEM Gateway" machine and then install this new certificate in "Trusted Root Certification Authorities" on CEM gateway machine.



Even if "Symantec Agent" web site new certificate is refreshed/installed on CEM Gateway server, client in CEM mode still doesn't have connection with CEM Gateway due this error:

* InitializeSecurityContext error while client handshake: The certificate chain was issued by an authority that is not trusted (0x80090325)

**2nd step Solution:**

* You need to create a new "CEM Offline" package and deliver it to affected CEM clients.
* Or return affected CEM client back from Internet to Intranet -> disable current "Cloud-Enabled management Settings" policy on SMP Console -> refresh policy on affected CEM client computer(s) -> enable back "Cloud-Enabled management Settings" policy on SMP Console -> refresh policy = Now CEM client will receive updated certificates and will be able to successfully establish connection with CEM Gateway.
* **Case:** CEM Client is unable to register with remote Task Server

CEM Client SMA throws these messages in log:

* Registering with Task Server list:","Client Task Agent","client task agent.dll","6796","Informational"
* Task Server: ***[<Your Task Server Address>***], Active: [false], Http: [80], Https: [443], Value: [6545454], Shares: [1]","Client Task Agent","client task agent.dll","6796","Informational"
* "InitializeSecurityContext error while client handshake: The certificate chain was issued by an authority that is not trusted (0x80090325)","MsCryptoSslDataTransformerImpl","AeXNetComms.dll","6796","Errors"

**Root cause:**

* Remote Site Server has self-signed or 3rd party certificate in own IIS HTTPs binding, but CEM client doesn't have remote Site Server's certificate installed in own "*Trusted Root Certification Authorities*"

**Solution:**

* You need to install remote Site Server's certificate in "*Trusted Root Certification Authorities*"

on CEM Client computer. If problems still appears, then make sure that you have installed 3rd party issuer certificate as well on CEM Client computer.

* **Case:** CEM Client unable to establish connection to CEM Gateway or to SMP Server via CEM Gateway.

CEM Client throws these messages in log when connection fails to CEM Gateway:

source='NetworkOperation' module='AeXNetComms.dll' process='AeXNSAgent.exe' pid='1168' thread='9728' tickCount='16505576' >  <![CDATA[Operation 'Connect' failed. Protocol: http Host: <***Your CEM Gateway server address>*** Port: 443 Path: / Http status: 0 Secure: Yes Id: {82EBF9A9-D193-4456-9187-75F8DF3D53F8} Error type: Connection error Error result: 0x80072751 Error code: 0 Error note: Unable to connect via secure gateway Error message: A socket operation was attempted to an unreachable host]]>source='Client Task Agent' module='client task agent.dll' process='AeXNSAgent.exe' pid='1168' thread='9728' tickCount='16505576' >  <![CDATA[Failed to call web interface by url [https://***<Your SMP Server Address>***:443/Altiris/TaskManagement/CTAgent/GetClientTaskServers.aspx?resourceGuid=9007647a-9fa9-41e0-a92b-b1f59c73543a&shares=1], error [0x80072751, A socket operation was attempted to an unreachable host.].]]>

**Root cause:**

* You have network connection problems between CEM Client and CEM Gateway server.

**Solution:**

* Make sure that CEM Gateway server and CEM Client are able to resolve each other by Hostname/FQDN/IPv4. Required ports are opened <http://www.symantec.com/docs/HOWTO83503>
* Make sure that you have correct CEM Gateway Address/Port received in "Cloud-Enabled Management Settings" policy.



CEM Client throws these messages in log when connection with SMP via CEM Gateway:

* source='NetworkOperation' module='AeXNetComms.dll' process='AeXNSAgent.exe' pid='6408' thread='6644' tickCount='163698837' >
* <![CDATA[Operation 'Connect' failed.
* Protocol: http
* Host: ***<YourSMPServerAddress>***
* Port: 443
* Path: /
* Http status: 0
* Secure: Yes
* Id: {CF8C8DC1-ED90-44E7-A2BE-EB754F5DE8FC}
* Error type: DNS error
* Error result: 0x80072AFC
* Error code: 0
* Error note: Failed to resolve FQDN and short name to IP address
* Error message: The requested name is valid, but no data of the requested type was found]]>
* severity='1' hostName=***'<CEM Client hostname>'*** source='ConfigServer' module='AeXNSAgent.exe' process='AeXNSAgent.exe' pid='6408' thread='6644' tickCount='163698837' >
* <![CDATA[Failed to send basic inventory: The requested name is valid, but no data of the requested type was found (0x80072AFC)]]>

**Root cause:**

* You have network connection problems between CEM Gateway server and SMP Server.

**Solution:**

* Make sure that CEM Gateway server and SMP Server are able to resolve each other by Hostname/FQDN/IPv4. Required ports are opened <http://www.symantec.com/docs/HOWTO83503>
* **Case:** CEM Client unable to establish connection to CEM Gateway due certificate thumbprint mismatch

CEM Client throws these messages in log:

* <![CDATA[Certificate for the gateway ***<Your CEM Gateway address>*** is invalid. Thumbprint mismatch.]]>
* hostName='***<CEM Client hostname>***' source='MsCryptoSslDataTransformerImpl' module='AeXNetComms.dll' process='AeXNSAgent.exe' pid='6408' thread='5424' tickCount='165276288' >
* <![CDATA[Server certificate is not valid. Remote host name: ***<Your CEM Gateway address>***]]>
* <![CDATA[Operation 'Connect' failed.
* Protocol: http
* Host: ***<Your CEM Gateway address>***
* Port: 443
* Path: /
* Http status: 0
* Secure: Yes
* Id: {63541059-2125-4C20-8280-F871C64DC0EE}
* Error type: Connection error
* Error result: 0x80072751
* Error code: 0
* Error note: Unable to connect via secure gateway
* Error message: A socket operation was attempted to an unreachable host]]>

**Root cause:**

* Administrator has re-generated self-signed certificate on CEM Gateway server, therefore its certificate thumbprint has been changed as well.

**Solution:**

* Check current CEM gateway's certificate thumbprint on CEM Gateway server and in "Cloud-Enabled Management Settings" policy on SMP Console. If they are mismatch, then update current thumbprint in "Cloud-enabled Management Settings" policy.
* ! Pay attention that all clients, which currently are in CEM mode and CEM Gateway thumbprint was changed on CEM gateway Server and in "Cloud-enabled Management settings" policy, then these clients will lose their connection with CEM Gateway and with SMP Server, until they will return back to intranet mode and receive updated "Cloud-enabled Management Settings" policy.



* **Case:** CEM Client unable to establish connection to SMP Server via CEM Gateway due 403 Forbidden Error in CEM Gateway log

CEM Client throws error message in log:

<![CDATA[Tunnel connection using IP: ***<Your CEM Gateway address>,*** Port: 443]]>

hostName='***<Your CEM Client hostname>***' source='NetworkOperation' module='AeXNetComms.dll' process='AeXNSAgent.exe' pid='6524' thread='5680' tickCount='169054133' >

<![CDATA[Operation 'Head' failed.

Protocol: http

Host: ***<Your SMP Server address>***

Port: 443

Path: /Altiris/NS/Agent/CreateResource.aspx

Http status: 403

Secure: Yes

Id: {15F953F2-DB3C-478C-B840-A6306F9F84BB}

Error type: HTTP error

Error result: 0x80042D21

Error code: 0

Error note: HTTP status: 403 Forbidden. Empty response content received, probably web server is not running or URL is invalid. In some cases Windows can return response header with Content-Length field but with empty response payload

Error message: Error 0x80042D21 (No description available)]]>

hostName='***<Your CEM Client hostname>***' source='ConfigServer' module='AeXNSAgent.exe' process='AeXNSAgent.exe' pid='6524' thread='5680' tickCount='169054133' >

<![CDATA[Failed to send data to '***<Your SMP Server address>/***Altiris/NS/Agent/CreateResource.aspx?nsversion=1', error: HTTP status: 403 Forbidden. Empty response content received, probably web server is not running or URL is invalid. In some cases Windows can return response header with Content-Length field but with empty response payload (0x80042D21)]]>

CEM gateway throws this warning message in log:

"mod\_ns\_support -> Post payload to ***<Your SMP Server Address>***:4726/Altiris/NS/Agent/PostEvent.aspx failed. Http status = 403.","InternetGateway.Status","InternetGateway"

**Root cause:**

* This problem appears only on Windows 2012 R2 with SMP installed for CEM
* Your SMP Web Site is using a non self-signed (3rd party) certificate and this certificate is installed in "*Trusted Root Certification Authorities*" on SMP Server.
* Links to read more about these problems on Windows 2012 R2 IIS8

<http://support.microsoft.com/kb/2802568>

[About "403.16 Problem in ISS8 on MP in DMZ"](https://social.technet.microsoft.com/Forums/en-US/fae724e8-628e-45a5-bf39-6e812d8a1a70/40316-problem-in-iss8-on-mp-in-dmz?forum=configmanagerdeployment)

**Solution:**

* You can find your current non self-signed certificate which is used by SMP Web Site (Not CEM Web Site!)



* You need to delete this non self-signed certificate from "*Trusted Root Certification Authorities*" on SMP Server - which is used by SMP Web Site (**! Not "Symantec Agent" web site:4726 !)**

Before deletion, please backup this certificate (do not forget to include private key in backup as well!) and then delete it -> restart CEM Gateway service -> now CEM connection should work.