Troubleshoot CVP Smart License Registration Error

Contents

Introduction							
Prerequisites							
Requirements							
Components Used							
Background Information							
Troubleshooting							
Log Collection							
Log Analysis							
Workaround 1							
Workaround 2							
Workaround 3							
Related Information							

Introduction

This document describes how to troubleshoot when an error is received when registering Cisco Customer Voice Portal with Smart Licensing.

Prerequisites

Requirements

Cisco recommends that you have knowledge on these topics:

- Cisco Unified Contact Center Enterprise (UCCE)
- Cisco Customer Voice Portal (CVP)
- Cisco Smart Software Manager
- Basic Understanding of Security Certificates
- Smart Licensing

Components Used

The information in this document is based on these software versions:

- UCCE Version 12.6.1
- CVP Version 12.6

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

The issue appears when trying to register the device with the Smart Licensing server.



Server Not Registered

After clicking the **Register** button, the Error message "Communication send error" is received.

Smart Licensing Product Registration	×	
	-	Į
Error occurred		
Communication send error.		
A Product license type chosen is Perpetual License . Ensure that chosen license type matches with license type at the time of purchase to avoid product going out of compliance.		
Ensure that you have connectivity to the URL specified in your Smart Call Home settings. By default this requires internet access. See the online help for registering to a On-Prem CSSM.		
To register the product for Smart Software Product registration, paste the Product Instance		J
Registration Token generated from Smart Software Manager or your On-Prem CSSM		
Cancel	jister	

Smart Licensing Registration Error Message

Troubleshooting

Per the error, one of the steps is to confirm that there is communication to the URL that is specified in the

Smart Call Home settings.

Other areas to look into:

- Verify that the Call home address is correct. You can review a sample of the configuration on this video <u>UCCE 12.5 Smart License Registration</u>.
- Confirm network access to tools.cisco.com.
- Verify that port 443 TCP is not being blocked.

Log Collection

Once configuration and network has been cleared. Proceed to collect these logs to isolate the issue:

• Smart Agent

Path to collect the trace is Cisco\CVP\logs\WSM\SmartAgent.<timestamp>

• Tomcat logs (Collect the CCBU text files)

Path to collect the trace is Cisco\ICM\Tomcat\logs

• PCAP while trying to **Register**

Log Analysis

For log analysis starting with the SmartAgent logs we see that there is an SSL exception when trying to establish the connection:

- 0000005990: 10.10.20.21: Feb 21 2023 14:44:28.793 -0500: %_ajp-nio-127.0.0.1-8009-exec-1-6-com.cisco.ccbu.smartagentmanager.SmartAgentManager: Registering product
- 0000005991: 10.10.20.21: Feb 21 2023 14:44:30.325 -0500: %_Thread-26-3-trustpool_log: CertificateException
sun.security.validator.ValidatorException: PKIX path building failed:
sun.security.provider.certpath.SunCertPathBuilderException: unable to find valid certification path to requested target
- 0000005992: 10.10.20.21: Feb 21 2023 14:44:30.325 -0500: %_Thread-26-3-event_msg_sender_log: SSL

- 0000005992: 10.10.20.21: Feb 21 2023 14:44:30.325 -0500: %_1hread-26-3-event_msg_sender_log: S exception javax.net.ssl.SSLHandshakeException: site is not trusted

Then, failed to send the request is seen:

- 0000006000: 10.10.20.21: Feb 21 2023 14:44:30.325 -0500: %_Thread-26-3-com.cisco.nesla.agent.impl.AsyncRequestProcessor: failed to send request / process response: SmartAgentMessageReg
- 0000006001: 10.10.20.21: Feb 21 2023 14:44:30.325 -0500: %_Thread-26-3-com.cisco.nesla.agent.impl.AsyncRequestProcessor: Reason: Communication send error.

From the Logger a Certificate issue is identified:

- 0000007553: 10.10.20.21: Feb 21 2023 14:44:30.512 -0500: %CCBU_ajp-nio-127.0.0.1-8009-exec-1-3-REST_API_EXCEPTION: %[exception=com.sun.jersey.api.client.ClientHandlerException: javax.net.ssl.SSLHandshakeException: No trusted certificate found][message_string=Failed to make request. Exception is caught for rest call: GET

https://:443/unifiedconfig/config/smartlicense/sync/smartlicenseserver]: The REST API has caught an exception

From PCAP is seen that there is 2 way communication. However, an issue with a Certificate is seen.

	Time	Source	Destination	Protocol Le	engt† Info
1	0.000000	and the second se		тср	66 1414 → 443 [SYN, ECN, CWR] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
2	0.029761			TCP	66 443 → 1414 [SYN, ACK] Seq=0 Ack=1 Win=8190 Len=0 MSS=1330 WS=256 SACK_PERM=1
3	0.029804			TCP	54 1414 → 443 [ACK] Seq=1 Ack=1 Win=263168 Len=0
4	0.031564			TLSv1_	333 Client Hello
5	0.061110		and the second second	TCP :	1384 443 → 1414 [PSH, ACK] Seq=1 Ack=280 Win=130560 Len=1330 [TCP segment of a reassembled PDU]
6	0.061217			TCP :	1384 443 → 1414 [PSH, ACK] Seq=1331 Ack=280 Win=130560 Len=1330 [TCP segment of a reassembled PDU]
7	0.061234			TCP	54 1414 → 443 [ACK] Seq=280 Ack=2661 Win=263168 Len=0
8	0.061343			TCP :	1384 443 → 1414 [PSH, ACK] Seq=2661 Ack=280 Win=130560 Len=1330 [TCP segment of a reassembled PDU]
9	0.061344			TLSv1_	1265 Server Hello, Certificate, Server Hello Done
10	0.061369			TCP	54 1414 → 443 [ACK] Seq=280 Ack=5202 Win=263168 Len=0
11	0.063155			TLSv1_	61 Alert (Level: Fatal, Description: Certificate Unknown)
12	0.063198	the second se	the second se	TCP	54 1414 → 443 [FIN, ACK] Seq=287 Ack=5202 Win=263168 Len=0
13	0.092435			тср	60 443 → 1414 [RST, ACK] Seq=5202 Ack=287 Win=2547712 Len=0

Certificate Error Viewed From PCAP

After narrowing down the issue to a Certificate. We move forward to review the certificates by navigating to the "call_home_ca" file and found that this certificate is missing:

-----BEGIN CERTIFICATE-----

MIIFYDCCA0igAwIBAgIQCgFCgAAAAUUjyES1AAAAAjANBgkqhkiG9w0BAQsFADBK MQswCQYDVQQGEwJVUzESMBAGA1UEChMJSWRlblRydXN0MScwJQYDVQQDEx5JZGVu VHJ1c3QgQ29tbWVyY2lhbCBSb290IENBIDEwHhcNMTQwMTE2MTgxMjIzWhcNMzQw MTE2MTgxMjIzWjBKMQswCQYDVQQGEwJVUzESMBAGA1UEChMJSWRlblRydXN0MScw JQYDVQQDEx5JZGVuVHJ1c3QgQ29tbWVyY2lhbCBSb290IENBIDEwggIiMA0GCSqG SIb3DQEBAQUAA4ICDwAwggIKAoICAQCnUBneP5k91DNG8W9RYYKyqU+PZ4ldhNlT 3Qwo2dfw/66VQ3KZ+bVdfIrBQuExUHTRgQ18zZshq0PirK1ehm7zCYofWjK9ouuU +ehcCuz/mNKvcbO0U59Oh++SvL3sTzIwiEsXXlfEU8L2ApeN2WIrvyQfYo3fw7gp S0l4PJNgiCL8mdo2yMKi1CxUAGc1bnO/AljwpN3lsKImesrgNqUZFvX9t++uP0D1 bVoE/c40yiTcdCMbXTMTEl3EASX2MN0CXZ/g1Ue9tOsbobtJSdifWwLziuQkkORi T0/Br4sOdBeo0XKIanoBScy0RnnGF7HamB4HWfp1IYV13ZBWzvurpWCdxJ35UrCL vYf5jysjCiN2O/cz4ckA82n5S6LgTrx+kzmEB/dEcH7+B1rlsazRGMzyNeVJSQjK Vsk9+w8YfYs7wRPCTY/JTw436R+hDmrfYi7LNQZReSzIJTj0+kuniVyc0uMNOYZK dHzVWYfCP04MXFL0PfdSgvHqo6z9STQaKPNBiDoT7uje/5kdX7rL6B7yuVBgwDHT c+XvvqDtMwt0viAgxGds8AgDelWAf0ZOlqf0Hj7h9tgJ4TNkK2PXMl6f+cB7D3hv 17yTmvmcEpB4eoCHFddydJxVdHixuuFucAS6T6C6aMN7/zHwcz091CqxC0EOoP5N iGVreTO01wIDAQABo0IwQDAOBgNVHQ8BAf8EBAMCAQYwDwYDVR0TAQH/BAUwAwEB /zAdBgNVHQ4EFgQU7UQZwNPwBovupHu+QucmVMiONnYwDQYJKoZIhvcNAQELBQAD ggIBAA2ukDL2pkt8RHYZYR4nKM1eVO8lvOMIkPkp165oCOGUAFjvLi5+U1KMtlwH 60i6mYtOlNeCgN9hCOCTrO0U5s7B8jeUeLBfnLOic7iPBZM4zY0+sLj7wM+x8uwt LRvM7Kqas6pgghstO8OEPVeKlh6cdbjTMM1gCIOQ045U8U1mwF10A0Cj7oV+wh93 nAbowacYXVKV7cndJZ5t+qntozo00Fl72u1Q8zW/7esUTTHHYPTa8Yec4kjixsU3 +wYO+nVZZiFHKdp2mhzpgq7vmrlR94gimmmVYjzlVYA2110C//G5Xc7UI2/YRYRK W2XviQzdFKcgyxilJbQN+QHwotL0AMh0jqEqSI5l2xPE4iUXfeu+h1sXIFRRk0pT AwvsXcoz7WL9RccvW9xYoIA55vrX/hMUpu09lEpCdNTDd1lzzY9GvlU47/rokTLq 11gEIt44w8y8bckzOmoKaT+gyOpyj4xjhiO9bTyWnpXgSUyqorkqG5w2gXjtw+hG 4iZZRHUe2XWJUc0QhJ1hYMtd+ZciTY6Y5uN/9lu7rs3KSoFrXgvzUeF0K+1+J6fZ mUlO+KWA2yUPHGNiiskzZ2s8EIPGrd6ozRaOjfAHN3Gf8qv8QfXBi+wAN10J5U6A 7/qxXDgGpRtK4dw4LTzcqx+QGtVKnO7RcGzM7vRX+Bi6hG6H -----END CERTIFICATE-----

The missing certificate is a match to the Cisco bug ID CSCwb04933.

There are available workarounds that can be performed by you to resolve the issue:

Workaround 1

Open port 80 from systems. For example:

- LoggerA
- CVP Call Server

For this workaround there is a waiting period of 24 hours, or 1 hour after the next download attempt, whichever comes first.

Workaround 2

If opening Port 80 is not an option, download manually the Certificate file from <u>here</u>, copy the content to the required smart agent directory and wait up to 24 hours.

Workaround 3

Download the file "QuoVadis_IdenTrust_Migration.zip" from the location:

https://software.cisco.com/download/home/268439622/type/284420243/release/12.6(1)

Apply the fix as per the next steps:

CVP Call server:

- 1. Perform a back up of the folder <cvp_install_drive>:\Cisco\CVP\conf\.sltruststore $\$
- 2. Stop the service "Cisco CVP WebServicesManager (WSM)".
- 3. Remove the file "call_home_ca" present in the path "<cvp_install_drive>:\Cisco\CVP\conf\.sltruststore\"
- 4. Copy the downloaded file "call_home_ca" and place it in the path

"<cvp_install_drive>:\Cisco\CVP\conf\.sltruststore\"

- 5. Start the service "Cisco CVP WebServicesManager (WSM)" and wait for 5 minutes
- 6. After this, attempt the "Renew Authorization" process for Smart Licensing

Related Information

How to Configure Smart License on UCCE 12.5

Cisco bug ID CSCwb04933



- CVP: Smart License - Registration & Authorization fails with "Communication send error"