Troubleshoot Licensing Failures on Nexus 9000

Contents

Introduction

This document describes the most commonly seen types of errors with Smart Licensing on Nexus 9000 series switches.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

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

- Smart Licensing on Nexus 9000 series switch
- Cisco Smart License Utility (CSLU)

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.

Communications Failure Errors

"Cannot establish secure connection because server TLS cert cannot be validated"

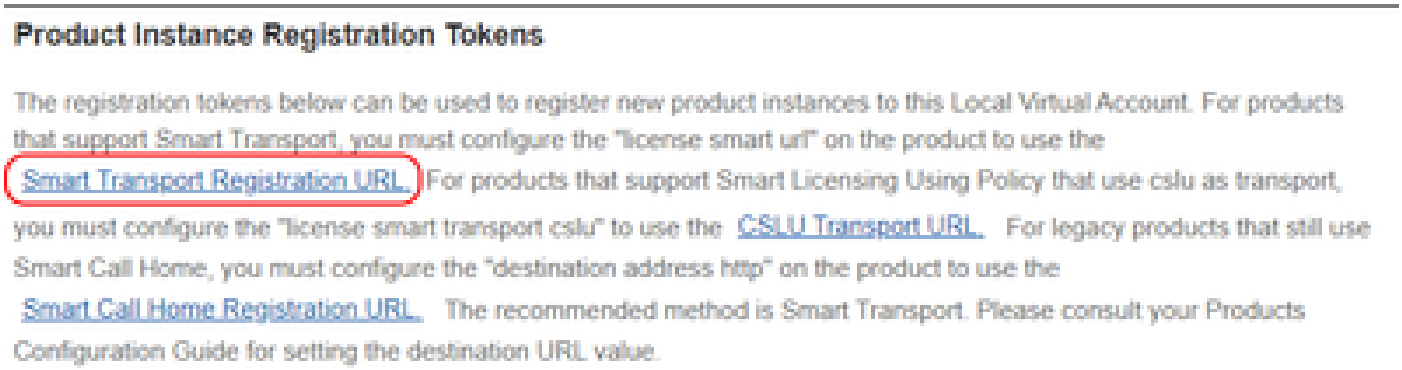
This CSLU error is typically caused either by configuring an incorrect FQDN using either the **license smart url cslu** or the **license smart url smart** commands, or by some device in the path doing SSL spoofing (typically a firewall with SSL inspection enabled).

HTTPS on a Nexus switch is no different than on any typical client OS. When accesing an HTTPS link, the client would verify the FQDN it is trying to access against the FQDN received in the certificate - either the CN field in the Subject header, or the SAN field. The client also validates whether the received certificate is

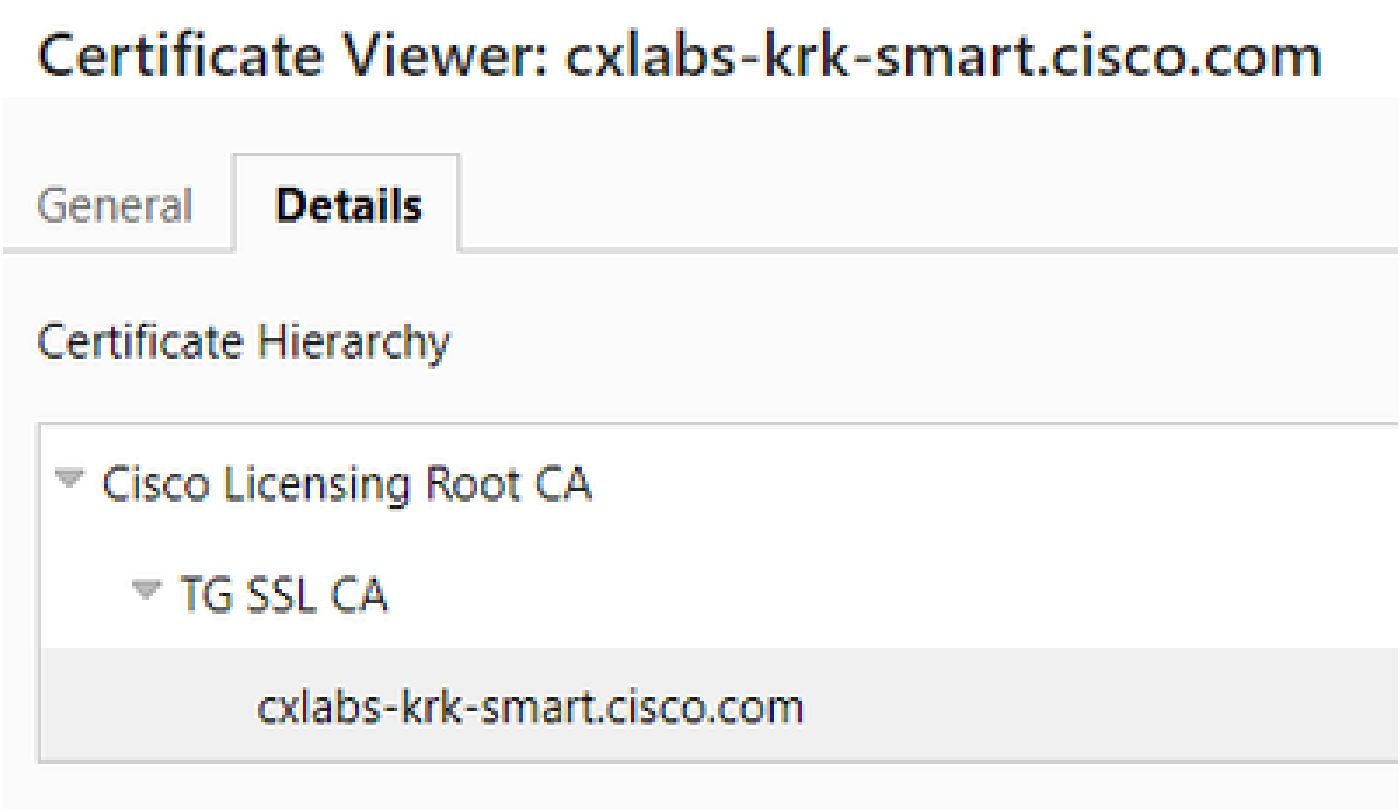
signed by a trusted certification authority.

If you attempt to access https://www.cisco.com, your browser opens it without issues. However, if you open https://173.37.145.84, you get a warning that the connection cannot be trusted, even though www.cisco.com would resolve to 173.37.145.84. The browser is trying to access 173.37.145.84, it does not see "173.37.145.84" in the certificate presented by the server, so the certificate is not considered valid.

This is why when configuring the CSSM address on the switch, it is critical to use exactly the URL proposed by CSSM itself; it contains the FQDN embedded in the certificate:



It is also important to remember that there are separate certificates used for CSSM On-prem management (port 8443 by default) and license registration (port 443 by default). The management certificate can be self-signed, or signed by a local enterprise CA trusted within the organization, or by a globally trusted CA, but licensing always uses a special Cisco Licensing Root CA. This is done automatically without any additional user involvement:



This CA is trusted by Cisco switches, but not by ordinary client PCs. If you attempt to access the URL proposed by CSSM using a PC, the browser displays an error due to not trusting the CA, but the switch does not have any issues:

Your connection is not private

Attackers might be trying to steal your information from **10.62.146.116** (for example, passwords, messages, or credit cards). Learn more about this warning

NET::ERR_CERT_AUTHORITY_INVALID

However, if there is a firewall doing SSL inspection with certificate spoofing between the switch and the CSSM server, the firewall replaces the certificate signed by Cisco CA with a different certificate signed typically by an enterprise CA, which is trusted by all PCs and servers in the organization, but not by the switch. Make sure to exclude any traffic to CSSM from HTTPS inspection.

When troubleshooting the "server TLS cert cannot be validated" error, access the URL configured on the switch with a browser and inspect if the certificate is correctly signed by Cisco CA, and the FQDN in the URL string matches the FQDN in the certificate.

"Communications failure" or "Could not resolve host: cslu-local"

The CSSM is typically configured with an FQDN in the URL, and in most Nexus deployments DNS is not configured, which frequently leads to this type of failure.

The first step of troubleshooting would be to ping the configured FQDN from the VRF used for Smart Licensing. For example, with this configuration:

```
license smart transport smart
license smart url smart https://smartreceiver.cisco.com/licservice/license
license smart vrf management
```

```
switch# ping smartreceiver.cisco.com vrf management
% Invalid host/interface smartreceiver.cisco.com
```

This error indicates that DNS resolution in VRF management does not work. Verify the **ip name-server** configuration under the specified VRF. Note that DNS server configuration is per VRF, so the **ip name-server** configuration in the default VRF does not take effect in VRF Management. As a stop-gap solution, **ip host** can be used to add a manual entry, but assume that in the future, the IP address of the server can change, and this entry can become invalid.

If the domain name is resolved, but pings fail, this coud be caused by a firewall blocking outgoing pings. In this case, you can use telnet to test if port 443 is open.

```
switch# telnet smartreceiver.cisco.com 443 vrf management
```

If this does not work either, troubleshoot the network path towards the server and make sure it works.

"Fail to send out Call Home HTTP message"

This message is fundamentally similar to the "Communications failure" message. The difference is that it is generally seen on switches running legacy Smart Licensing, not Smart Licensing using Policy that was introduced in NXOS release 10.2. With legacy Smart licensing, the URL to be accessed is configured using the **callhome** command.

```
callhome
...
destination-profile CiscoTAC-1 transport-method http
destination-profile CiscoTAC-1 index 1 http https://tools.cisco.com/its/service/oddce/services/DDCEServ
transport http use-vrf management
```

Make sure the configuration is correct, uses HTTPS, and there is reachability to the URL (typically tools.cisco.com) over the selected VRF.

Further Troubleshooting

Please refer to Smart Licensing using Policy Troubleshooting on Data Center Solution for a detailed troubleshooting checklist involving other steps that could be taken to resolve issues related to licensing.