Cisco Smart Licensing - Troubleshooting Steps and Considerations on Catalyst platforms

Contents

1. Introduction
1.1. What is Cisco Smart Licensing?
1.2. Smart Licensing Implementation Methods
1.3. Supported IOS XE Platforms
1.4. Migration from Legacy Licenses to Smart Licenses
   1.4.1. Converting through Device Led Conversion (DLC)
   1.4.2. Converting through Cisco Smart Software Manager (CSSM) or License Registration Portal (LRP)
   1.4.3. Converting through contacting Cisco Global Licensing Operations (GLO) department
2. Configuration
   2.1. Basic configuration
   2.2. Registration Token / Device ID Token
   2.3. Registration and License States
3. Considerations and Caveats
4. Troubleshooting
   4.1. Device Fails to register
5. Common Failure Scenarios
   Scenario #1: Switch Registration "Failure Reason: Product Already Registered"
   Scenario #2: Switch Registration "Failure Reason: Your request could not be processed right now. Please try again"
   Scenario #3: Failure Reason "The device date 1526135268653 is offset beyond the allowed tolerance limit"
   Scenario #4: Switch Registration "Failure Reason: Communication transport not available."
   Scenario #5: Switch License Authorization "Failure reason: Fail to send out Call Home HTTP message."
   Scenario #6: Switch License Authorization "Failure reason: Waiting for reply"
   Scenario #7: License in "OUT OF COMPLIANCE" status
6. References

1. Introduction

1.1. What is Cisco Smart Licensing?

Cisco Smart Licensing is a cloud-based unified license management system that manages all of the software licenses across Cisco products. It enables customers to purchase, deploy, manage, track and renew Cisco Software licenses. It also provides information about license ownership and consumption through a single user interface
The solution is comprised of online Smart Accounts (at Cisco Smart Licensing Portal) used for tracking Cisco software assets and the Cisco Smart Software Manager (CSSM) which is used to manage the Smart Accounts. CSSM is where all licensing management related tasks, such as registering, de-registering, moving, and transferring licenses can be performed. Users can be added and given access and permissions to the smart account and specific virtual accounts.

To learn more about Cisco Smart Licensing, visit:

a) Cisco Smart Licensing home page

b) Cisco Community - On-Demand Trainings.

Smart accounts can be created here: Smart Accounts

Smart accounts can be managed here: Smart Software Licensing

1.2. Smart Licensing Implementation Methods

There are multiple methods in deploying Cisco Smart Licensing that can be leveraged depending on a company’s security profile such as:

Direct Cloud Access

Cisco products send usage information directly over the Internet securely using HTTPS. No additional components are needed.

Access through an HTTPS Proxy
Cisco products send usage information through an HTTP proxy server securely using HTTPS. An existing proxy server can be used or this can be deployed through Cisco's Transport Gateway. (click here for some additional information).

On-premise License Server (Cisco Smart Software Manager satellite)

Cisco products send usage information to an on-premise server instead of directly over the internet. Once a month the server reaches out over the internet for all devices via HTTPS or can be manually transferred to synchronize its database. CSSM Satellite is available as a Virtual Machine (VM) and can be downloaded here. For additional information, visit Smart Software Manager Satellite page.

1.3. Supported IOS XE Platforms

- From 16.9.1 release onwards, the Catalyst 3650/3850 and Catalyst 9000 series switch platforms support the Cisco Smart Licensing method as the only licensing method.
- From 16.10.1 release onwards, router platforms such as the ASR1K, ISR1K, ISR4K, and virtual routers (CSRv / ISrv) support the Cisco Smart Licensing method as the only licensing method.

1.4. Migration from Legacy Licenses to Smart Licenses
There are two methods for converting a legacy license, like Right-To-Use (RTU) or Product Activation Key (PAK) to a Smart License. For details on which method needs to be followed please refer to the relevant release notes and/or configuration guide for the specific Cisco device.

1.4.1. Converting through Device Led Conversion (DLC)

- Device Led Conversion (DLC) is a one-time method where the Cisco Product can report what licenses it is using and the licenses are automatically deposited into their corresponding Smart Account on the Cisco Smart Software Manager (CSSM). The DLC procedure is performed directly from the Command Line Interface (CLI) of the specific Cisco device.

- The DLC process is only supported on the Catalyst 3650/3850 and selected router platforms. For specific router models please refer to the individual platform configuration guide and release notes. Example: [DLC procedure for Catalyst 3850 running Fuji 16.9.x releases](#).

1.4.2. Converting through Cisco Smart Software Manager (CSSM) or License Registration Portal (LRP)

**Cisco Smart Software Manager (CSSM) Method:**

1. Login to Cisco Smart Software Manager (CSSM) at [https://software.cisco.com/](https://software.cisco.com/)
2. Navigate to Smart Software Licensing > Convert to Smart Licensing
3. Select Convert PAK or Convert Licenses

4. Locate the license in the table below if converting PAK license. If converting a non-PAK license use the "License Conversion Wizard" for step by step directions.

**Location of known PAK files associated with Account:**
5. Locate the Desired License and Product combination

6. Click (under Actions): Convert to Smart Licensing

7. Select desired virtual account, license, and click Next
1.4.3. Converting through contacting Cisco Global Licensing Operations (GLO) department

The Global Licensing Operations department can be reached [here](#) at our worldwide contact centers.

2. Configuration

2.1. Basic configuration

Exact procedure how to configure Smart Licensing can be found in System Management
2.2. Registration Token / Device ID Token

Before registering device, Token needs to be generated. The registration token, also known as the device id token, is a unique token generated from the smart licensing portal or Cisco Smart Software Manager satellite when initially registering a Cisco device to the corresponding smart account. An individual token can be used to register multiple Cisco devices depending on the parameters used during creation.

The registration token is also only required during initial registration of a Cisco device as it provides the information to the device to call-home to the Cisco back end and be tied to the correct Smart Account. After the Cisco device is registered the token is no longer required.

For more information in regard to registration tokens and how they are generated, please click here for a general guide. For more details, please refer to the configuration guide for the specific Cisco device.

2.3. Registration and License States

While deploying and configuring Smart Licensing there are multiple possible states that a Cisco device can be in. These states can be displayed by looking at `show license all` or `show license status` from the Command Line Interface (CLI) of the Cisco device.

Below is a list of all states and their meaning:

- **Evaluation (Unidentified) State** This is a default state of the device when first booted. Usually, this state is seen when a Cisco device has not yet been configured for Smart Licensing or registered to a Smart Account. In this state all features are available and the device can freely change license levels. The evaluation period is used when the device is in the unidentified state. The device will not attempt to communicate with Cisco in this state. This will be 90 days of usage and not 90 calendar days. Once it is expired it is never reset. There is one evaluation period for the entire device it is not per entitlement. When the evaluation period expires at the end of 90 days, the device goes into EVAL EXPIRY mode, however there is no functional impact or disruption in functionality, even after reload. Currently there is no enforcement in place. The countdown time is maintained across reboots. The evaluation period is used if the device has not yet registered with Cisco and has not received the following two messages from the Cisco backend: Successful response to a registration request, Successful response to an entitlement authorization request.

- **Registered State** This is the expected state after successfully completing registration. The Cisco device has been able to successfully communicate with a Cisco Smart Account and register. The device receives an ID certificate valid for 1 year which will be used for future communications. The device will send a request to CSSM to authorize the entitlements for the licenses in use on the device. Depending on the CSSM response the device will then enter Authorized or Out of Compliance. The ID certificate expires at the end of one year. After 6 months the software Agent process will try to renew the certificate. If the Agent cannot
communicate with the Cisco Smart Software Manager it will continue to try and renew the Id certificate until the expiration date (1 year). At the end of one year, the agent will go back to the Un-Identified state and will try to enable the Evaluation period. The CSSM will remove the product instance from its database.

- **Authorized State** This is the expected state when device is using an entitlement and is in Compliance (no negative balance), The Virtual Account on CSSM had the correct type and number of licenses to authorize the consumption of the device’s licenses. At the end of 30 days, the device will send a new request to CSSM to renew the authorization. Has a time span of 90 days after which (if not successfully renewed) is moved to Authorization Expired state.

- **Out of Compliance State** This is the state when device is using an entitlement and is not in Compliance (negative balance), This state is seen when the license does not have an available license in the corresponding Virtual Account that the Cisco device is registered to in the Cisco Smart Account. To enter into Compliance / Authorized state, a customer must add the correct number and type of licenses to the Smart Account. When in this state the device will automatically send an authorization renewal request every day. Licenses and features will continue to operate and there is no functional impact.

- **Authorization Expired State** This is the state when device is using an entitlement has not been able to communicate with the Cisco Smart Account associated for over 90 days. This is typically seen if the Cisco device loses internet access or cannot connect to tools.cisco.com after initial registration. Online methods of smart licensing require Cisco devices to communicate a minimum of every 90 days to prevent this status. CSSM will return all in use licenses for this device back to the pool since it has not had any communications for 90 days. While in this state the device will continue to try to contact Cisco, every hour, to renew the entitlement authorization, until the registration period (id certificate) expires. If the software Agent re-establishes communications with Cisco and receives its request for authorization it will process that reply normally and enter into one of the established states.

### 3. Considerations and Caveats

- Starting in 16.9.1 for switches and 16.10.1 for routers, a default Call-home profile named "CiscoTAC-1" is generated to assist with migrating to Smart Licensing. By default, this profile is set up for the Direct Cloud Access method.

```
#show call-home profile CiscoTAC-1
Profile Name: CiscoTAC-1
Profile status: ACTIVE
Profile mode: Full Reporting
Reporting Data: Smart Call Home, Smart Licensing
Preferred Message Format: xml
Message Size Limit: 3145728 Bytes
Transport Method: http
HTTP address(es): https://tools.cisco.com/its/service/oddce/services/DDCEService
Other address(es): default
```

- When utilizing a Cisco Smart Software Manager satellite, the destination address under the active call-home configuration must point to it (case-sensitive!):
If DNS needs to be resolved in a VRF, then DNS can be configured in the following way:

Alternatively, if DNS is not available, statically configure local DNS to IP mapping (based on local DNS resolution on your end-device) or replace DNS name in call-home configuration with IP address. Refer to example for direct cloud access (for Cisco Smart Software Manager satellite use its own DNS name instead of tools.cisco.com):

A different number of licenses might be consumed depending on the configuration of the Cisco device such as with Catalyst switches running in StackWise or StackWise Virtual:

**Traditional Stack-wise Supported Switches (e.g. Catalyst 9300 series):**

- Network License: 1 license is consumed per switch in the stack
- DNA License: 1 license is consumed per switch in the stack

**Modular Chassis (e.g. Catalyst 9400 series):**

- Network License: 1 license is consumed per supervisor in the chassis
- DNA License: 1 license is consumed per chassis

**Fixed Stack-wise Virtual Supported Switches (e.g. Catalyst 9500 series):**

- Network License: 1 license is consumed per switch in the stack
- DNA License: 1 license is consumed per switch in the stack

Only one call-home profile can be active for Smart Licensing.

Licenses are only consumed if a corresponding feature is configured.

Cisco devices configured for Smart Licensing need to be configured with the correct system time and date to ensure they are properly synchronized with the corresponding Cisco Smart Licensing service.
Account. If the time offset of the Cisco device is too far off it, the device can fail to register. The clock will need to be manually set or configured via a timing protocol such as Network Time Protocol (NTP) or Precision Time Protocol (PTP). For the exact steps required to implement these changes please refer to the configuration guide for the specific Cisco device.

- The Public Key Infrastructure (PKI) key generated during the Cisco device registration needs to be saved if it is not automatically saved after registration. If the device fails to save the PKI key then a syslog is generated stating to save the configuration via “copy running-config startup-config” or “write memory”.
- If the PKI key of the Cisco device is not properly saved, then the license state can be lost on failovers or reloads.
- Smart Licensing does not support HTTPS Proxy SSL certificate interception by default when using 3rd party proxies for the HTTPS Proxy method. To support this feature, you can either disable SSL interception on the Proxy, or manually import the certification sent from the Proxy.

**How to Manually Import Certification as a TrustPoint:**

Note, the certificate will need be in a BASE64 format to be copied and pasted onto the device as a TrustPoint.

The following example shown below uses "LicRoot" as the TrustPoint name, however, this name can be changed as desired.

```
Device#conf t
Device(config)#crypto pki trustpoint LicRoot
Device(config)##enrollment terminal
Device(config)##revocation-check none
Device(config)##exit
Device(config)#crypto pki authenticate LicRoot
Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself
-----BEGIN CERTIFICATE-----
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
-----END CERTIFICATE-----
Certificate has the following attributes:
Fingerprint MD5: XXXXXXXX
Fingerprint SHA1: XXXXXXX
% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
% Certificate successfully imported
```

- When using the Transport Gateway HTTP Proxy the IP address needs to be changed from tools.cisco.com to the Proxy like the following:
  destination address http https://tools.cisco.com/its/service/oddce/services/DDCEService
  TO
  destination address http https://<TransportGW-IP_Address>:<port_number>/TransportGateway/services/DeviceRequestHandler
- The Transport Gateway IP address can be found by navigating to the HTTP Settings and looking under the HTTP Service URLs on the Cisco Transport Gateway GUI.

For more information please see the following configuration guide for the Cisco Transport Gateway [here](#).

4. Troubleshooting

When migrating a Cisco device to a Smart Licensing enabled software version the following
flowchart can be used as a general guide for all three methods (Direct Cloud Access, HTTPS Proxy, and Cisco Smart Software Manager satellite).

Device Upgraded or Shipped with software release that supports Smart Licensing (refer to section 1.3 for list of supported IOS-XE releases).

Below troubleshooting steps mainly concentrate on a scenario in which 'device fails to register'.

### 4.1. Device Fails to register

After initial configuration, in order to enable Smart Licensing, Token, which is generated on CSSM / Cisco Smart Software Manager satellite, needs to be registered on the device via CLI:

**How to Manually Import Certification as a TrustPoint:**

Note, the certificate will need be in a BASE64 format to be copied and pasted onto the device as a TrustPoint.

The following example shown below uses "LicRoot" as the TrustPoint name, however, this name can be changed as desired.

```
Device#conf t
Device(config)#crypto pki trustpoint LicRoot
Device(config)#crypto pki enrollment terminal
Device(config)#crypto pki revocation-check none
Device(config)#crypto pki exit
Device(config)#crypto pki authenticate LicRoot

Enter the base 64 encoded CA certificate. End with a blank line or the word "quit" on a line by itself

-----BEGIN CERTIFICATE-----
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
-----END CERTIFICATE-----

Certificate has the following attributes:
- Fingerprint MD5: XXXXXXXX
- Fingerprint SHA1: XXXXXXX

% Do you accept this certificate? [yes/no]: yes
```
Trustpoint CA certificate accepted.
% Certificate successfully imported

This should generate the following events:

- Smart licensing process starts
  Registration process is in progress. Use the 'show license status' command to check the progress and result.
- Crypto key is automatically generated for HTTPS communication
  Generating 2048 bit RSA keys, keys will be exportable... [OK] (elapsed time was 1 seconds)

%CRYPTO_ENGINE-5-KEY_ADDITION: A key named SLA-KeyPair has been generated or imported by crypto-engine
%PKI-4-NOCONFIGAUTOSAVE: Configuration was modified. Issue "write memory" to save new IOS PKI configuration.
- Call-home start registration process
  %CALL_HOME-6-SCH_REGISTRATION_IN_PROGRESS: SCH device registration is in progress. Call-home will poll SCH server for registration result. You can also check SCH registration status with "call-home request registration-info" under EXEC mode.
- Smart Licensing process connects with CSSM and check entitlement.
  %SMART_LIC-6-EXPORT_CONTROLLED: Usage of export controlled features is allowed
  %SMART_LIC-6-AGENT_REG_SUCCESS: Smart Agent for Licensing Registration with the Cisco Smart Software Manager or satellite for udi PID:<PID>,SN:<SN>
  %SMART_LIC-4-CONFIG_NOT_SAVED: Smart Licensing configuration has not been saved
  %SMART_LIC-5-IN_COMPLIANCE: All entitlements and licenses in use on this device are authorized
  %SMART_LIC-6-AUTH_RENEW_SUCCESS: Authorization renewal with the Cisco Smart Software Manager or satellite. State=authorized for udi PID:<PID>,SN:<SN>

To check call-home configuration, run the following CLI:

```
#show call-home profile all
```

Profile Name: CiscoTAC-1
Profile status: ACTIVE
Profile mode: Full Reporting
Reporting Data: Smart Call Home, Smart Licensing
Preferred Message Format: xml
Message Size Limit: 3145728 Bytes
Transport Method: http
HTTP address(es): https://tools.cisco.com/its/service/oddce/services/DDCEService
Other address(es): default

Periodic configuration info message is scheduled every 1 day of the month at 09:15
Periodic inventory info message is scheduled every 1 day of the month at 09:00

Alert-group            Severity
------------------------  ------------
crash                   debug
diagnostic              minor
environment             warning
inventory               normal

Syslog-Pattern    Severity
------------------------  ------------
APF-.-.WLC_.*        warning
.*                      major

To check Smart Licensing status, run the following CLI:
#show license summary
Smart Licensing is ENABLED

Registration:
**Status: REGISTERED**
Smart Account: TAC Cisco Systems, Inc.
Virtual Account: Krakow LAN-SW
Export-Controlled Functionality: ALLOWED
Last Renewal Attempt: None

License Authorization:
**Status: AUTHORIZED**
Last Communication Attempt: SUCCEEDED
Next Communication Attempt: Jun 25 21:24:37 2019 UTC

License Usage:
<table>
<thead>
<tr>
<th>License</th>
<th>Entitlement tag</th>
<th>Count Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>C9500 Network Advantage (C9500 Network Advantage)</td>
<td>1 AUTHORIZED</td>
<td></td>
</tr>
<tr>
<td>C9500-DNA-40X-A (C9500-40X DNA Advantage)</td>
<td>1 AUTHORIZED</td>
<td></td>
</tr>
</tbody>
</table>

In case device fail to register (and Status is different from REGISTERED as shown above; note that Out-of-Compliance points to an issue on CSSM like missing license in Smart Virtual Account, incorrect mapping (i.e. Token from different virtual account was used where licenses are not available, etc.) check the following:

1. **Verify configuration settings and common failure scenarios**
   Refer to section 2.1 for basic configuration steps. Look also at section 5 for common failure scenarios observed in the field.

2. **Check basic connectivity**
   Verify that device can reach (and open TCP port) to tools.cisco.com (in case of direct access) or to Cisco Smart Software Manager satellite:

   ```
   #show run all | in destination address http
   destination address http https://tools.cisco.com/its/service/oddce/services/DDCEService
   !
   ! check connectivity
   !
   #telnet tools.cisco.com 443 /source-interface gi0/0
   Trying tools.cisco.com (173.37.145.8, 443)... Open
   [Connection to tools.cisco.com closed by foreign host]
   ```

   In case above does not work, double-check your routing rules, source-interface and firewall settings.

   Note that HTTP (TCP/80) is being deprecated and the recommended protocol is HTTPS (TCP/443).

   Refer to section: "3. Considerations and Caveats" in this document for further guidelines how to configure DNS and HTTP details.

3. **Verify Smart License settings**
   Collect the output of:
and validate collected configuration / logs (attach this output in case you decide to open Cisco TAC case for further investigation).

4. Enable debugs

Enable the following debugs to collect additional information about Smart Licensing process (note that after enabling debugs, you need to try to register license once again via CLI mentioned in point 4.1):

For internal debugs, enable and read binary traces:

5. Common Failure Scenarios

The following are some common failure scenarios that could be experienced during or after a Cisco device registration:

Scenario #1: Switch Registration "Failure Reason: Product Already Registered"

Snip of "show license all":

Registration:

Status: UNREGISTERED - REGISTRATION FAILED

Export-Controlled Functionality: NotAllowed

Initial Registration: FAILED on Oct 22 14:25:31 2018 EST
Failure reason: **Product Already Registered**

Next Registration Attempt: Oct 22 14:45:34 2018 EST

**Next Steps:**

- The Cisco device will need to be registered again.

- If the Cisco device is seen in the Cisco Smart Software Manager (CSSM), the "force" parameter will need to be used (i.e. "license smart register idtoken <TOKEN> force")

**NOTE:** The failure reason can also show as the following:

- Failure reason: The product <X> and sudi containing udiSerialNumber:<SerialNumber>,udiPid:<Product> has already been registered.

- Failure reason: Existing Product Instance has Consumption and Force Flag is False

**Scenario #2: Switch Registration "Failure Reason: Your request could not be processed right now. Please try again"**

Snip of "show license all":

Registration:

- Status: REGISTERING - REGISTRATION IN PROGRESS
- Export-Controlled Functionality: NotAllowed
- Initial Registration: FAILED on Oct 24 15:55:26 2018 EST
- Failure reason: **Your request could not be processed right now. Please try again**

Next Registration Attempt: Oct 24 16:12:15 2018 EST

**Next Steps:**

- Enable debugs as mentioned in section 4 to get more insights on the issue,

- Generate new Token in CSSM in your Smart Licensing and take an another attempt.

**Scenario #3: Failure Reason "The device date 1526135268653 is offset beyond the allowed tolerance limit"**

Snip of "show license all":

Registration:

- Status: REGISTERING - REGISTRATION IN PROGRESS
- Export-Controlled Functionality: NotAllowed
Initial Registration: FAILED on Nov 11 17:55:46 2018 EST

Failure reason: {
"timestamp": [{"The device date '1526135268653' is offset beyond the allowed tolerance limit."}]

Next Registration Attempt: Nov 11 18:12:17 2018 EST

Possible Logs Seen:

%PKI-3-CERTIFICATE_INVALID_NOT_YET_VALID: Certificate chain validation has failed. The certificate (SN: XXXXXX) is not yet valid. Validity period starts on 2018-12-12:43Z

Next Steps:

- Verify that the Cisco device clock is showing the correct time (show clock)
- Configure the Network Time Protocol (NTP) if possible to ensure the clock is set correctly
- If NTP is not possible, verify that the manually set clock (clock set) is correct (show clock) and configured as a trusted time source by verifying that "clock calendar-valid" is configured

**NOTE** - By default, the system clock is not trusted. "clock calendar-valid" is required.

Scenario #4: Switch Registration "Failure Reason: Communication transport not available."

Snip of "show license all":

Registration: Status: UNREGISTERED - REGISTRATION FAILED

Export-Controlled Functionality: Not Allowed

Initial Registration: FAILED on Mar 09 21:42:02 2019 CST

Failure reason: Communication transport not available.

Possible Logs Seen:

%CALL_HOME-3-CALL_HOME_FAILED_TO_ENABLE: Failed to enable call-home from Smart Agent for Licensing: The command failed to enable smart call home due to an existing active user profile. If you are using a user profile other than "CiscoTAC-1" profile to send data to SCH server in Cisco, please enter "reporting smart-licensing-data" under profile mode to configure that profile for smart licensing. For more details about SCH, please check [http://www.cisco.com/go/smartcallhome](http://www.cisco.com/go/smartcallhome)

%SMART_LIC-3-AGENT_REG_FAILED: Smart Agent for Licensing Registration with the Cisco Smart Software Manager or satellite failed: Communication transport not available.

%SMART_LIC-3-COMM_FAILED: Communications failure with the Cisco Smart Software Manager or satellite: Communication transport not available.
Next Steps:

- Verify that call-home is enabled with "service call-home" in the "show running-config" output of the Cisco device

- Ensure that the correct call-home profile is active

- Verify that "reporting smart-licensing-data" is configured under the active call-home profile

Scenario #5: Switch License Authorization "Failure reason: Fail to send out Call Home HTTP message."

Snip of "show license all":

License Authorization:

Status: OUT OF COMPLIANCE on Jul 26 09:24:09 2018 UTC

Last Communication Attempt: FAILED on Aug 02 14:26:23 2018 UTC

Failure reason: **Fail to send out Call Home HTTP message.**

Next Communication Attempt: Aug 02 14:26:53 2018 UTC

Communication Deadline: Oct 25 09:21:38 2018 UTC

Possible logs are seen:

%sSMART_LIC-3-COMM_FAILED:Communications failure with the Cisco Smart Software Manager or satellite: Fail to send out Call Home HTTP message.

%sSMART_LIC-3-AUTH_RENEW_FAILED:Authorization renewal with the Cisco Smart Software Manager or satellite: Communication message send error for udi PID:XXX, SN: XXX

Next Steps:

- Verify that the Cisco device can ping **tools.cisco.com** or the nslookup translated IP

- Attempt to telnet from the Cisco device to tools.cisco.com on TCP port 443 (port used by HTTPS)

- Verify that the HTTPs client source interface is correct

- Verify that the URL/IP in the call home profile is set correctly on the Cisco device via "**show call-home profile all**"

- Verify the ip route is pointing to the correct next hop

- Ensure **TCP port 443** is not being blocked on the Cisco device, the path to Smart Call Home Server, or the Cisco Smart Software Manager satellite
- Ensure that the correct Virtual Routing and Forwarding (VRF) instance is configured if applicable

**Scenario #6: Switch License Authorization "Failure reason: Waiting for reply"

Snip of "show license all":

License Authorization:
Status: OUT OF COMPLIANCE on Jul 26 09:24:09 2018 UTC
Last Communication Attempt: PENDING on Aug 02 14:34:51 2018 UTC
Failure reason: **Waiting for reply**
Next Communication Attempt: Aug 02 14:53:58 2018 UTC

**Possible logs are seen:**

- %PKI-3-CRL_FETCH_FAIL: CRL fetch for trustpoint SLA-TrustPoint failed Reason : Failed to select socket. Timeout : 5 (Connection timed out)
- %PKI-3-CRL_FETCH_FAIL: CRL fetch for trustpoint SLA-TrustPoint failed Reason : Failed to select socket. Timeout : 5 (Connection timed out)

**Next Steps:**

- To correct this issue the SLA-TrustPoint should be configured as **none** under the running configuration

```bash
crunch running-config
<omitted>
crypto pki trustpoint SLA-TrustPoint
revocation-check none
```

**What is a CRL?**

A Certificate Revocation List (CRL) is a list of revoked certificates. The CRL is created and digitally signed by the certificate authority (CA) that originally issued the certificates. The CRL contains dates for when each certificate was issued and when it expires. Further information in regards to CRL is available [here](#).

**Scenario #7: License in "OUT OF COMPLIANCE" status**

Snip of "show license all":

License Authorization:
Status: OUT OF COMPLIANCE on Jul 26 09:24:09 2018 UTC
Last Communication Attempt: PENDING on Aug 02 14:34:51 2018 UTC
Failure reason: **Waiting for reply**
Next Communication Attempt: Aug 02 14:53:58 2018 UTC
Possible logs are seen:

```bash
%SMART_LIC-3-OUT_OF_COMPLIANCE: One or more entitlements are out of compliance
```

Next Steps:

- Verify if Token from proper Smart Virtual Account has been used,
- Verify amount of available licenses [here].

6. References

1) Cisco Smart Licensing home page

2) Cisco Community - On-Demand Trainings.

3) Smart Account - management portal: Smart Software Licensing

4) Smart Account - create new accounts: Smart Accounts

5) Configuration guide (example) - System Management Configuration Guide, Cisco IOS XE Fuji 16.9.x (Catalyst 9300 Switches)