Troubleshoot Smart Licensing on Catalyst Platforms

Contents

- **Introduction**
  - What is Cisco Smart Licensing
  - Smart Licensing Implementation Methods
    - Direct Cloud Access
    - Access through an HTTPS Proxy
    - On-Premise License Server (Also Known as Cisco Smart Software Manager Satellite)
  - Supported Cisco IOS XE Platforms
  - Migration from Legacy Licenses to Smart Licenses
    - Converting through Device-Led Conversion (DLC)
    - Converting through Cisco Smart Software Manager (CSSM) or License Registration Portal (LRP)
    - Convert through and Contact Cisco Global Licensing Operations (GLO) Department
  - Catalyst 9500 High Performance Behavior Change from 16.9 to 16.12.3
    - Cisco IOS XE Version 16.11.x and Earlier
    - Cisco IOS XE Version 16.12.3 and Later
    - C9500 High Performance Change FAQ
- **Configuration**
  - Basic Configuration
  - Registration Token / Device ID Token
  - Registration and License States
    - Evaluation (Unidentified) State
    - Registered State
    - Authorized State
    - Out of Compliance State
    - Authorization Expired State
- **Considerations and Caveats**
- **Troubleshoot**
  - Device Fails to Register
- **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: Failure Reason: "Missing Id Cert Serial Number Field; Missing Signing Cert Serial Number Field; Signed Data and Certificate does not Match" Log
  - Scenario #7: Switch License Authorization: "Failure reason: Waiting for reply."
  - Scenario #8: License in "OUT OF COMPLIANCE" Status
  - Scenario #9: Switch License Authorization: "Failure Reason: Data and Signature do not Match."
- **References**

Introduction

This document describes how to work with Cisco Smart Licensing (cloud-based system) to manage software licenses on Catalyst switches.

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 you 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 to track 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



Tip: For more information on the new Smart Licensing using Policy method in Cisco IOS® XE 17.3.2 and later, visit Smart Licensing using Policy on Catalyst Switches.

New to Smart Licensing and/or Smart Account administration? Visit and sign up for the new administrator training course and recording:
Cisco Community - Get Smart with Cisco Smart Accounts/Smart Licensing and Cisco License Central.

Smart accounts can be created here: Smart Accounts

Smart accounts can be managed here: Smart Software Licensing

Smart Licensing Implementation Methods

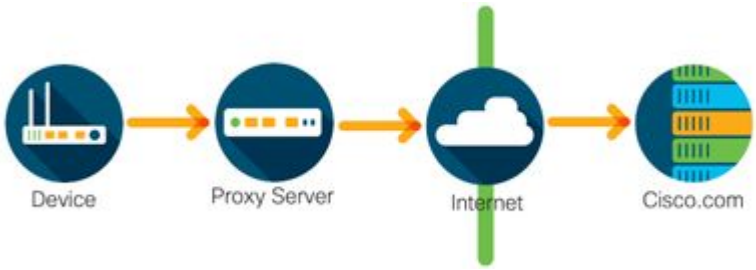
There are multiple methods in deploying Cisco Smart Licensing that can be leveraged depending on a company’s security profile such as:

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 the Cisco Transport Gateway (click here for some additional information).

On-Premise License Server (Also Known as 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 On-prem (Satellite) is available as a Virtual Machine (VM) and can be downloaded. For additional information, visit Smart Software Manager Satellite page.

Supported Cisco IOS XE Platforms

- From Cisco IOS XE version 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 Cisco IOS XE version 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.

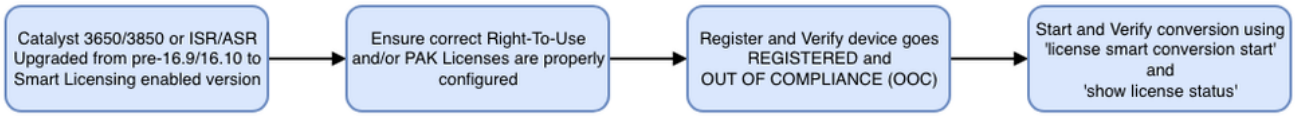
Migration from Legacy Licenses to Smart Licenses

There are two methods to convert 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, refer to the relevant release notes and/or configuration guide for the specific Cisco device.

Converting through Device-Led Conversion (DLC)

- Device-Led Conversion (DLC) is a one-time method where the Cisco Product can report what licenses it uses 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, refer to the individual platform configuration guide and release notes. Example: DLC procedure for Catalyst 3850 running Fuji 16.9.x releases.



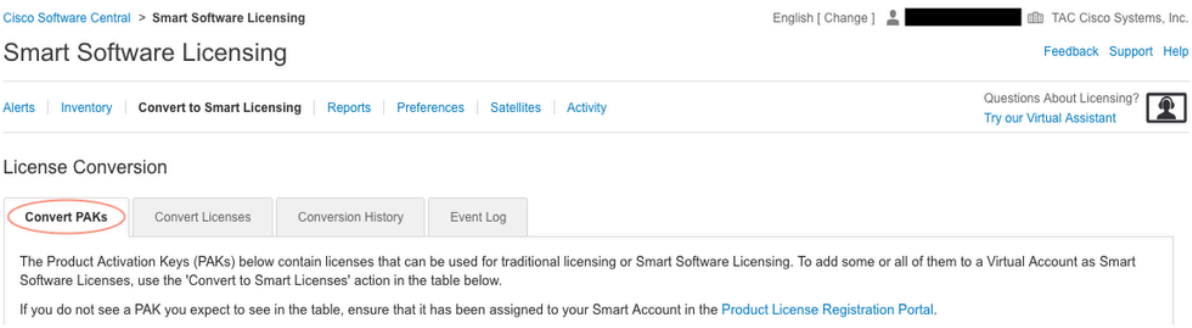
Converting through Cisco Smart Software Manager (CSSM) or License Registration Portal (LRP)

Cisco Smart Software Manager (CSSM) Method:

1. Log in to Cisco Smart Software Manager (CSSM) at Cisco Software

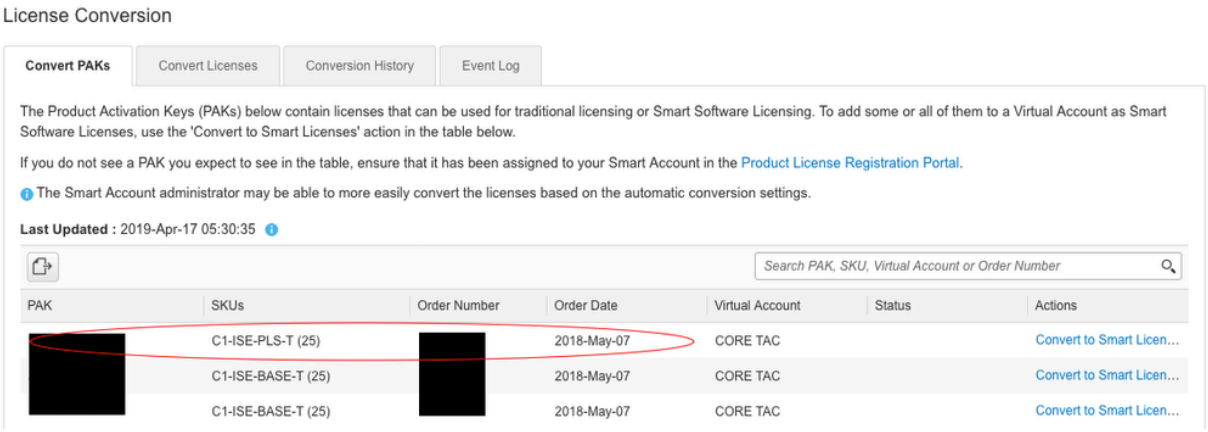
2. Navigate to **Smart Software Licensing > Convert to Smart Licensing.**

3. Choose **Convert PAK** or **Convert Licenses.**

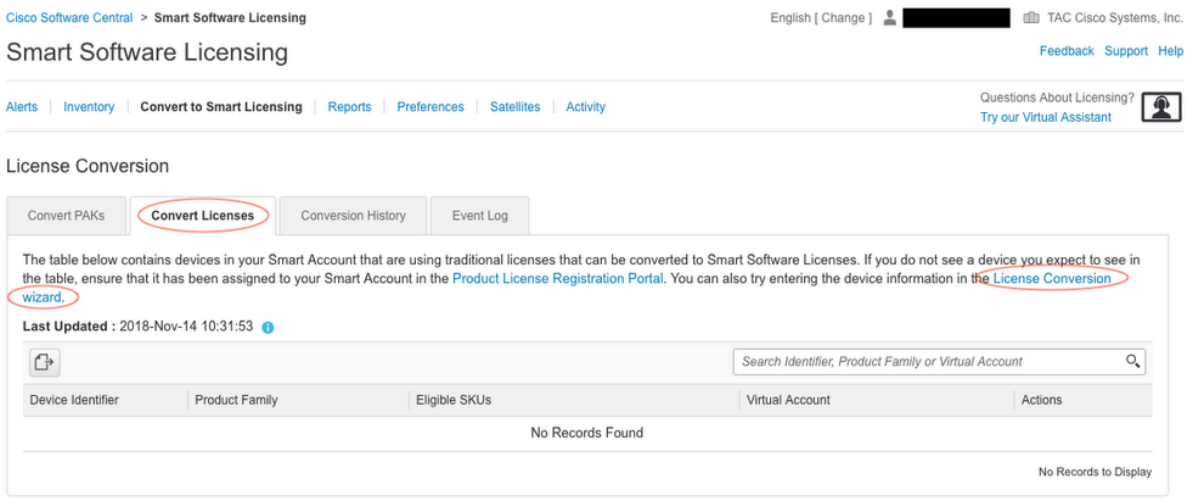


4. To convert a PAK license, locate the license in this table. ***To convert a non-PAK license*** and use the **License Conversion Wizard** for step-by-step directions.

Location of known PAK files associated with Account:

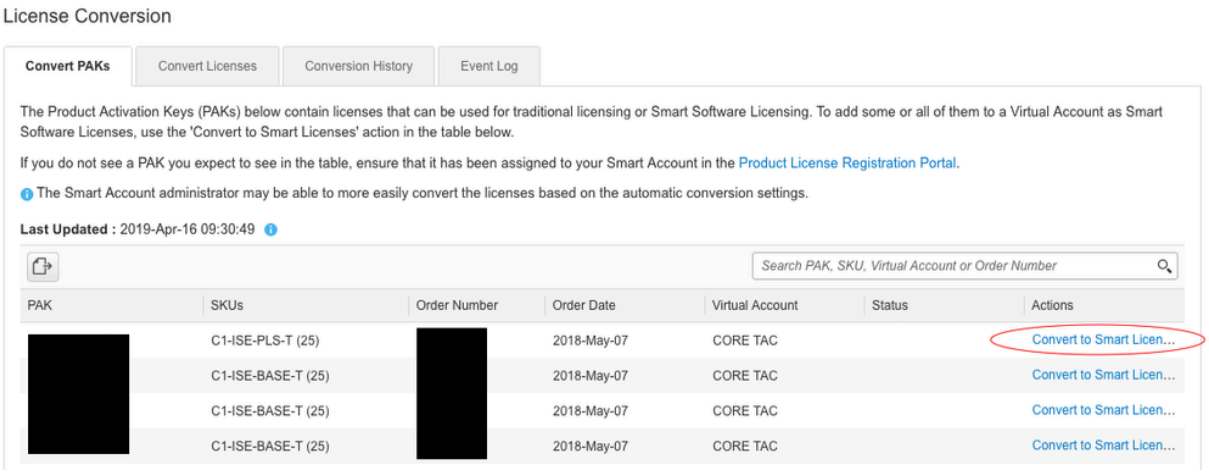


Location of **License Conversion Wizard** link:

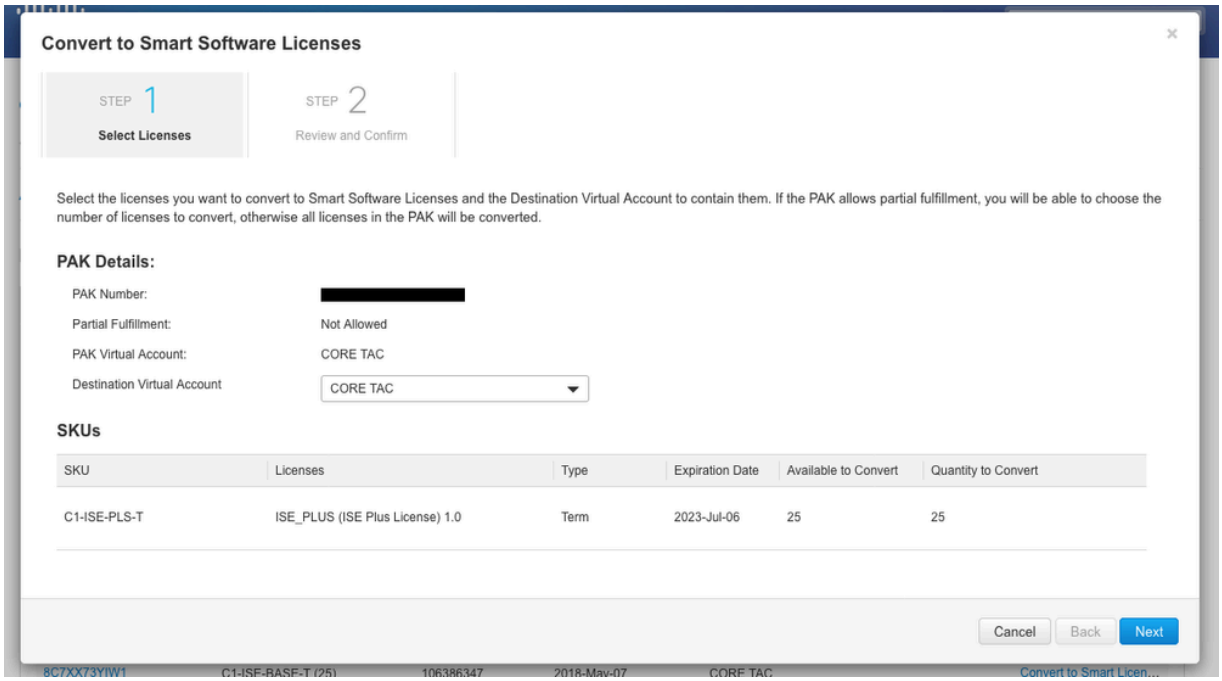


5. Locate the Desired License and Product combination.

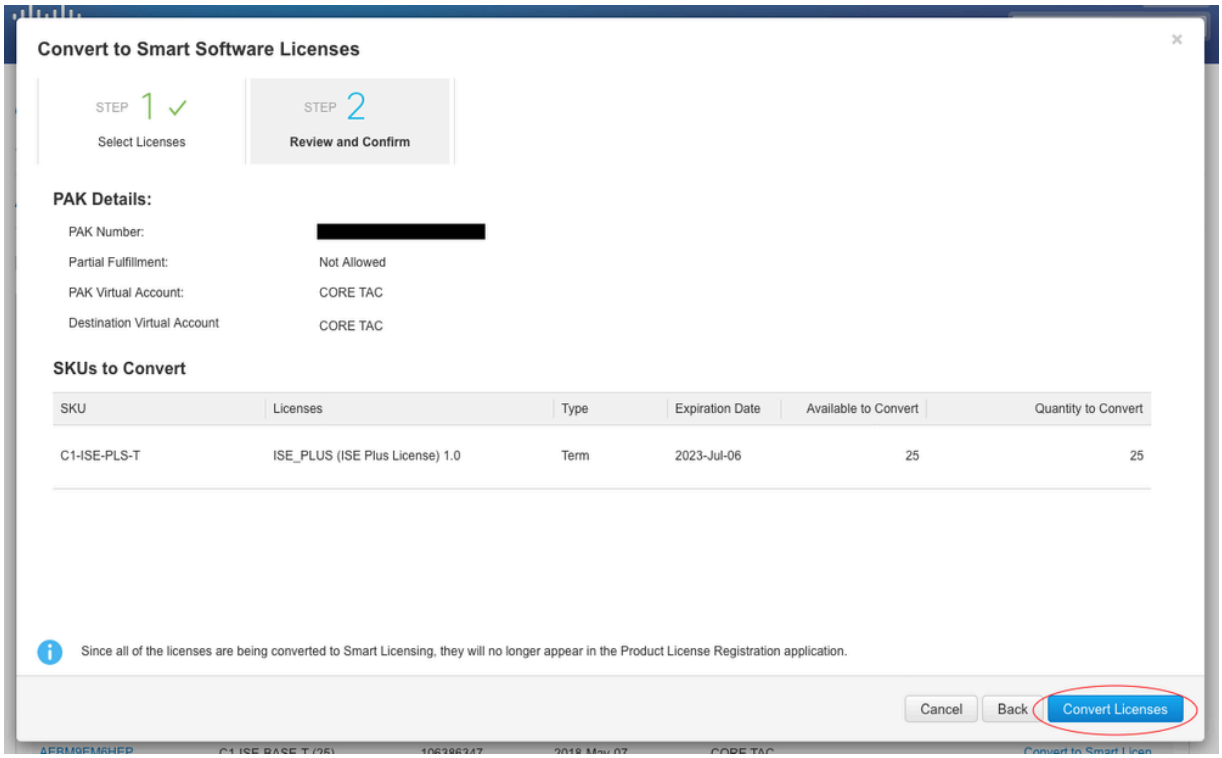
6. Click **Actions Convert to Smart Licensing**.



7. Choose **virtual account**, **license**, and click **Next**.



8. Review **Selections**, then click **Convert Licenses**.

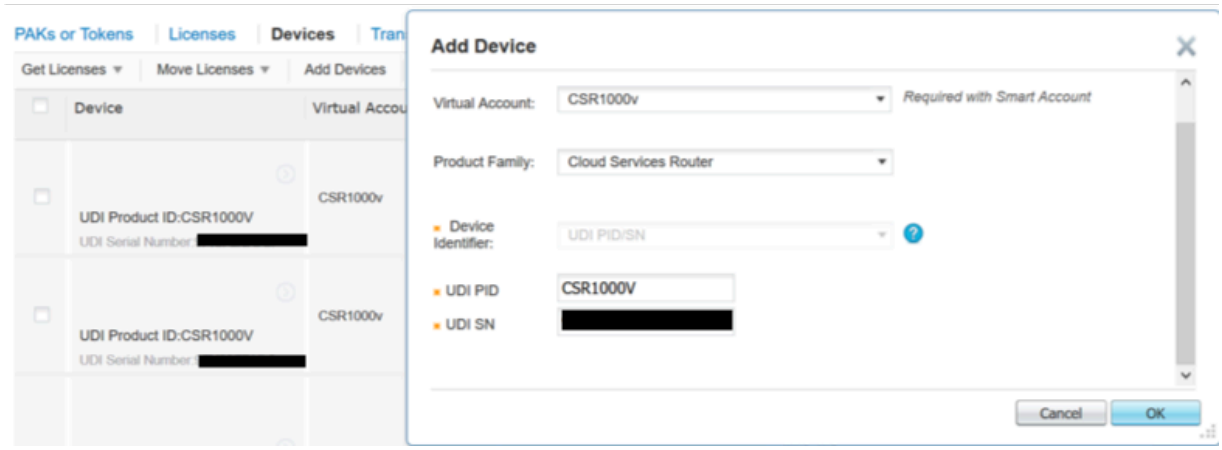


License Registration Portal (LRP) method:

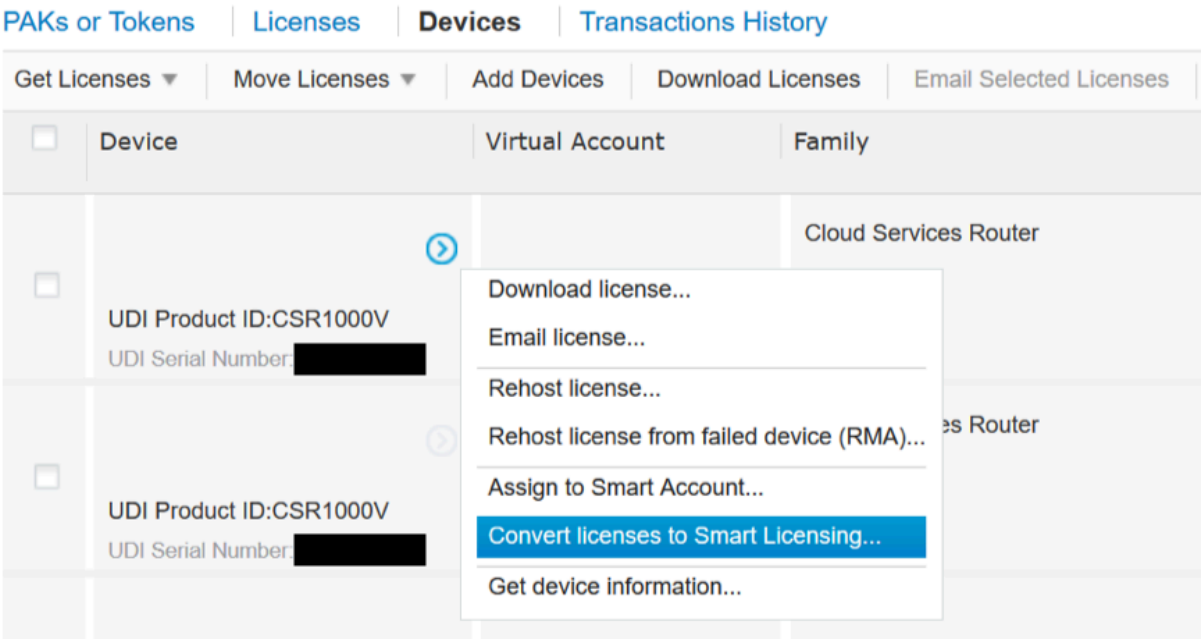
1. Log in to the License Registration Portal (LRP) [SWIFT Licensing Home]

2. Navigate to **Devices > Add Devices**.

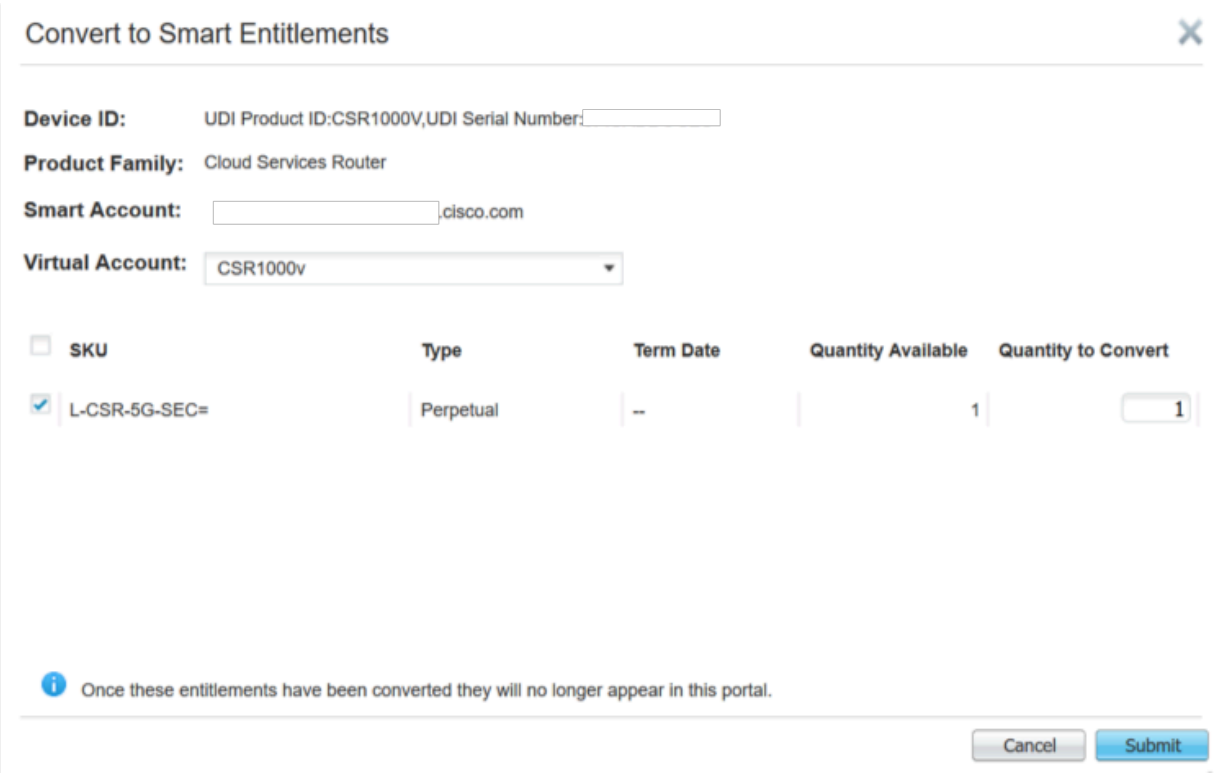
3. Enter the proper **Product Family and Unique Device Identifier (UDI) product ID** and **serial number**, then click **Ok**. UDI information can be obtained from show version or show inventory taken from the command line interface (CLI) of the Cisco device.



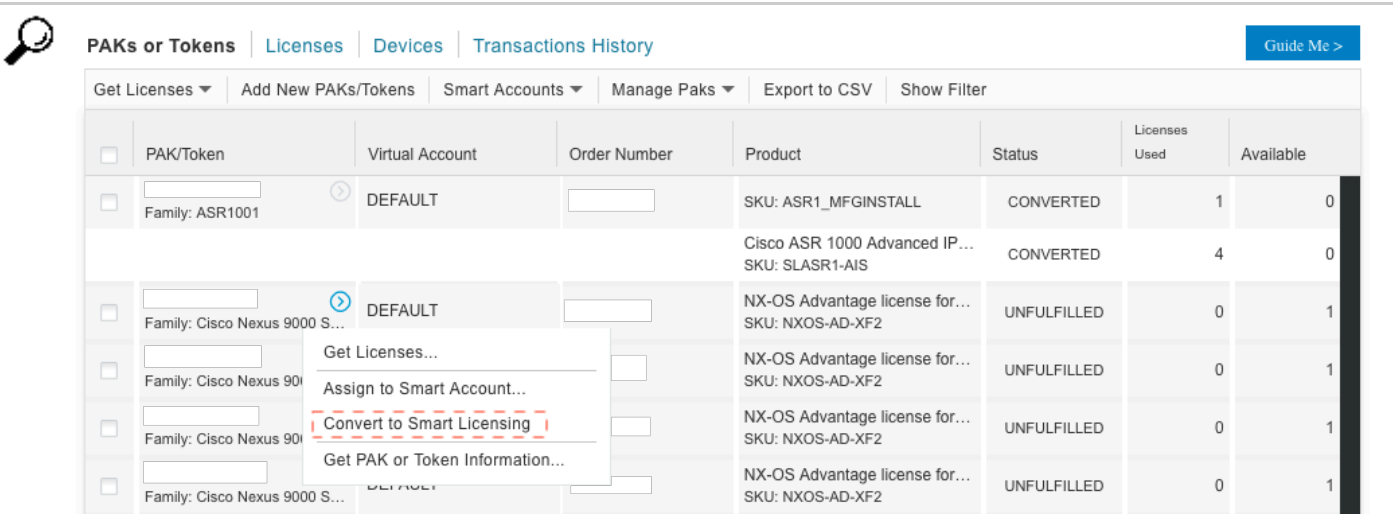
4. Choose the added device and **Convert Licenses to Smart Licensing**.



5. Assign to proper Virtual Account, choose **licenses** to convert and click **Submit**.



Tip: LRP tool can also be used by looking up the license/product family on the PAKs or Tokens tab. Click the **circle drop down** next to the PAK/Token and choose **Convert to Smart Licensing**:



Convert through and Contact Cisco Global Licensing Operations (GLO) Department

The Global Licensing Operations department can be reached here at our worldwide contact centers.

Catalyst 9500 High Performance Behavior Change from 16.9 to 16.12.3

Like other Catalyst 9000 models, the Catalyst 9500 High Performance models were enabled with Smart Licensing in the Cisco IOS XE version 16.9 train and onwards. For the Catalyst 9500 High Performance models, however, each model had its own specific license entitlement tag. It was decided later, by the product and marketing teams, to unify the C9500 platforms entitlement tags. This decision changed the behavior on the C9500 High Performance models from using specific entitlement tags to generic C9500 licenses.

This change in behavior is documented in these defects:

a) Cisco bug ID CSCvp30661

b) Cisco bug ID CSCvt01955

Here is the before and after of the above-mentioned changes license changes for C9500 High Performance models:

Cisco IOS XE Version 16.11.x and Earlier

Each C9600 High Performance model has its own entitlement tags.

Model	**License**
C9500-32C	**C9500 32C NW Essentials**

	C9500 32C NW Advantage C9500 32C DNA Essentials C9500 32C DNA Advantage
C9500-32QC	**C9500 32QC NW Essentials** **C9500 32QC NW Advantage** C9500 32QC DNA Essentials C9500 32QC DNA Advantage
C9500-24Y4C	**C9500 24Y4C NW Essentials** **C9500 24Y4C NW Advantage** C9500 24Y4C DNA Essentials C9500 24Y4C DNA Advantage
C9500-48Y4C	**C9500 48Y4C NW Essentials** **C9500 48Y4C NW Advantage** C9500 48Y4C DNA Essentials C9500 48Y4C DNA Advantage

Note: Cisco IOS XE versions 16.12.1 and 16.12.2 have defects Cisco bug ID CSCvp30661 and Cisco bug ID CSCvt01955. These defects are addressed in 16.12.3a and later.

Cisco IOS XE Version 16.12.3 and Later

Catalyst 9500 High Performance platforms now use generic network license tags and separate DNA license tags. This table shows the entitlements changes that are highlighted in Cisco IOS XE version 16.12.3 and later:

Model	License
C9500-32C	**C9500 Network Essentials** **C9500 Network Advantage** C9500 32C DNA Essentials C9500 32C DNA Advantage

C9500-32QC	**C9500 Network Essentials** **C9500 Network Advantage** C9500 32QC DNA Essentials C9500 32QC DNA Advantage
C9500-24Y4C	**C9500 Network Essentials** **C9500 Network Advantage** C9500 24Y4C DNA Essentials C9500 24Y4C DNA Advantage
C9500-48Y4C	**C9500 Network Essentials** **C9500 Network Advantage** C9500 48Y4C DNA Essentials C9500 48Y4C DNA Advantage



Note: Upgrades from Cisco IOS XE versions 16.12.1 and 16.12.2 display this license behavior. Upgrades from Cisco IOS XE versions 16.9.x ,16.10.x, 16.11.x to 16.12.3 recognize old license configurations.

C9500 High Performance Change FAQ

1. Why does Cisco support allocate a generic network license, when my device is consuming a device-specific network license?

Generic tags are provided as they are the right entitlement tags for the network device. This allows usage of the entitlement tags across the entire Cat9500 platform, not just the specific C9500 high performance models. Pre-16.12.3 images that ask for device-specific license tags are in compliance with the generic license tags as the more specific licenses fall under the generic licenses in the licensing hierarchy.

2. Why do two network tags sometimes show up in the Smart Account?

This behavior is due to the licensing hierarchy and happens when the device is running on an older image that utilizes device-specific licensing tags. Older images that ask for device-specific license tags are in compliance with the generic license tags as the more specific tags fall under the generic licenses in the licensing hierarchy.

Configuration

Basic Configuration

Exact procedure on how to configure Smart Licensing can be found in System Management Configuration Guide available for each release / platform.

For example: System Management Configuration Guide, Cisco IOS XE Fuji 16.9.x (Catalyst 9300 Switches)

Registration Token / Device ID Token

Before registering device, a 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 on-prem 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, refer to the general Cisco guide. For more details, please refer to the configuration guide for the specific Cisco device.

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.

Here is a list of all states and their description:

Evaluation (Unidentified) State

- Evaluation is the default state of the device when it is 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 does not attempt to communicate with Cisco in this state.
- This evaluation period is 90 days of usage and not 90 calendar days. Once the evaluation period expires, it is never reset.

- There is one evaluation period for the entire device; it is not one evaluation period per entitlement.
- When the evaluation period expires at the end of 90 days, the device goes in to 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 these two messages from the Cisco backend:
    1. Successful response to a registration request.
    2. Successful response to an entitlement authorization request.

Registered State

- Registered is the expected state after registration has been completed successfully.
- This state indicates that the Cisco device has been able to successfully communicate with a Cisco Smart Account and register.
- The device receives an ID certificate, valid for one year, which is used for future communications.
- The device sends a request to CSSM to authorize the entitlements for the licenses that are in use on the device.
- Depending on the CSSM response, the device then enters either the Authorized or Out of Compliance state.
- The ID certificate expires at the end of one year. After six months, the software Agent process tries to renew the certificate. If the Agent cannot communicate with the CSSM, it continues to try and renew the ID certificate until the expiration date (one year). At the end of one year, the agent goes back to the Un-Identified state and tries to enable the Evaluation period. The CSSM removes the product instance from its database.

Authorized State

- Authorized is the expected state when the device is using an entitlement and is in Compliance (no negative balance).
- This state indicates that the Virtual Account on CSSM had the correct type and number of licenses to authorize the consumption of the licenses for this device.
- At the end of 30 days, the device sends a new request to CSSM to renew the authorization.
- This state has a time span of 90 days. After 90 days (if not successfully renewed), the device is moved to the Authorization Expired state.

Out of Compliance State

- Out of Compliance is the state when the device is using an entitlement and is not in Compliance (negative balance).
- This state is seen when the device 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 the Compliance / Authorized state, you must add the correct number and type of licenses to the Smart Account.
- When a device is in the Out of Compliance state, it automatically sends an authorization renewal request every day.

- Licenses and features continue to operate and there is no functional impact.

Authorization Expired State

- Authorization Expired is the state when the device is using an entitlement and has not been able to communicate with the associated Cisco Smart Account for over 90 days.
- This state 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 returns all in-use licenses for this device back to the pool since it has not had any communications with the device for 90 days.
- While in this state, the device continues to try to contact Cisco every hour in order 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 processes that reply normally and enters into one of the established states.

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.

<#root>

```
#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

<snip>
```

When utilizing a Cisco Smart Software Manager on-premise server, the destination address under the active call-home configuration must point to it (case-sensitive!):

<#root>

```
(config)#call-home
(cfg-call-home)#profile "CiscoTAC-1"
(cfg-call-home-profile)#destination address http https://
```

<IP/FQDN>

```
/Transportgateway/services/DeviceRequestHandler
```

DNS is required to resolve tools.cisco.com. If DNS server connectivity is in a VRF, ensure that the proper source-interface and VRF are defined:

Global Routing Table Used:

```
(config)#ip domain-lookup [source-interface <INTERFACE>]
(config)#ip name-server <IP>
```

VRF Routing Table Used:

```
(config)#ip domain-lookup [source-interface <INTERFACE>]     <<-- "ip vrf forwarding <VRF-NAME>" define
(config)#ip name-server vrf <VRF-NAME> <SERVER-IP>
```

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 on-prem use its own DNS name instead of tools.cisco.com):

```
(config)#ip host tools.cisco.com <x.x.x.x>
```

If communication to tools.cisco.com needs to be originated from the interface in a specific VRF (for example, Mgmt-vrf), then this CLI must be configured:

```
(config)#ip http client source-interface <VRF_INTERFACE>
```

A different number of licenses can be consumed based on the configuration of the Cisco device, such as with Catalyst switches that run in StackWise or StackWise Virtual:

Traditional Stack-wise Supported Switches (for example, 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 (for example, 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 (for example, 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 that are configured for Smart Licensing must be configured with the correct system time and date to ensure that they are properly synchronized with the corresponding Cisco Smart Account. If the time offset of the Cisco device is too far off it, the device can fail to register. The clock must 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, refer to the configuration guide for the specific Cisco device.
- The Public Key Infrastructure (PKI) key that is generated during the Cisco device registration must be saved if it is not automatically saved after registration. If the device fails to save the PKI key, a syslog is generated that prompts you to save the configuration via the **copy running-config startup-config** or **write memory** command.
- 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 third-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.

<#root>

How to Manually Import Certification as a TrustPoint:

```
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 chan

Device#conf t
Device(config)#crypto pki trustpoint LicRoot
Device(ca-trustpoint)#enrollment terminal
Device(ca-trustpoint)#revocation-check none
Device(ca-trustpoint)#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-----
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
-----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 must be changed from tools.cisco.com to the Proxy like this example:

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

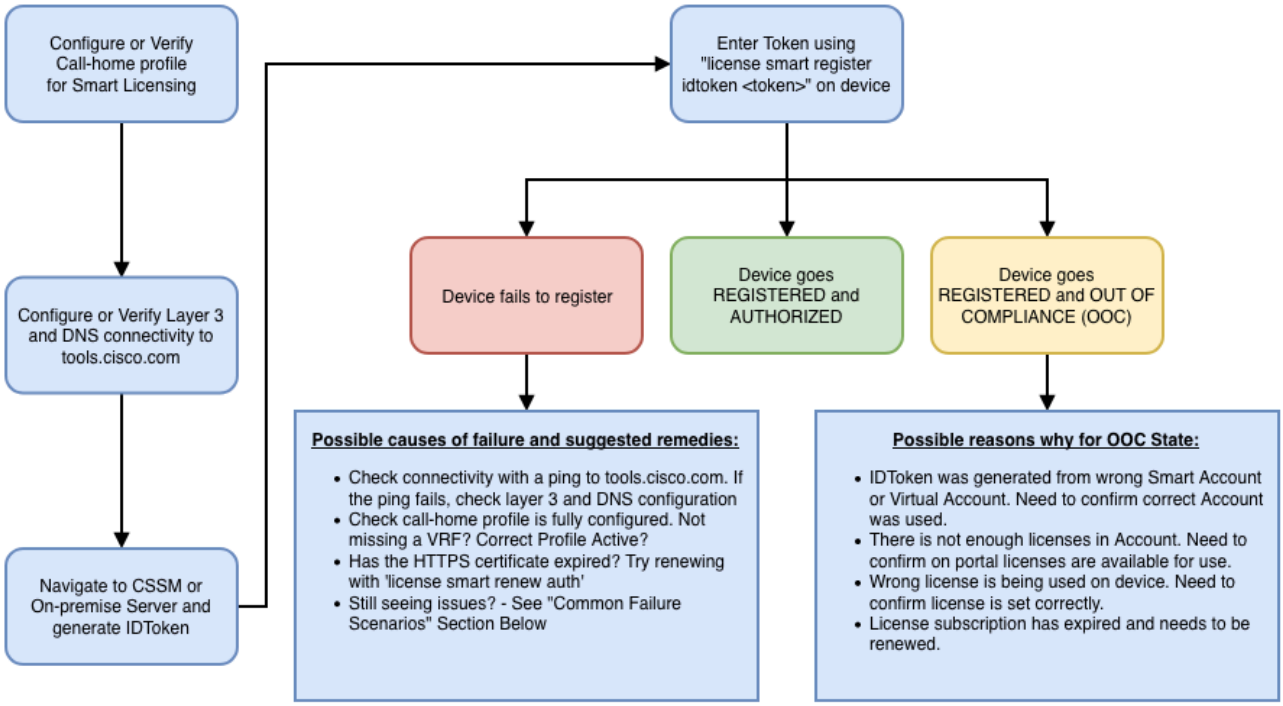
The Transport Gateway IP address can found by navigating to the HTTP Settings and looking under the HTTP Service URLs on the Cisco Transport Gateway GUI.

For more information, see the configuration guide for the Cisco Transport Gateway.

Troubleshoot

When you migrate a Cisco device to a Smart Licensing-enabled software version, you can use this flowchart as a general guide for all three methods (Direct Cloud Access, HTTPS Proxy, and Cisco Smart Software Manager On-prem).

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



These steps to troubleshoot mainly concentrate on a scenario in which the device fails to register.

Device Fails to Register

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

```
license smart register idtoken <TOKEN>
```

This action generates these events:

<#root>

```
! Smart licensing process starts
```

```
!
```

```
Registration process is in progress. Use the 'show license status' command to check the progress and re
```

```
!
```

! 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 configura

!

! Call-home start registration process

!

%CALL_HOME-6-SCH_REGISTRATION_IN_PROGRESS: SCH device registration is in progress. Call-home will poll

!

! 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 Ma

%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 satelli

To check call-home configuration, run this CLI:

<#root>

#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 this CLI:

<#root>

#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
  Next Renewal Attempt: Nov 22 21:24:32 2019 UTC

License Authorization:
```

Status: AUTHORIZED

```
Last Communication Attempt: SUCCEEDED

 Next Communication Attempt: Jun 25 21:24:37 2019 UTC


License Usage:
  License                  Entitlement tag               Count Status
  -----------------------------------------------------------------------------
  C9500 Network Advantage (C9500 Network Advantage)         1 AUTHORIZED
  C9500-DNA-40X-A          (C9500-40X DNA Advantage)        1 AUTHORIZED
```

If the device fails to register (and if Status is different from REGISTERED), Out-of-Compliance points to an issue on CSSM such as missing license in Smart Virtual Account, incorrect mapping (for example, a token from a different virtual account was used where licenses are not available), and so on.

Check these items:

1. Verify configuration settings and common failure scenarios.

Refer to section 2.1 for basic configuration steps. Also, look at section 5 for common failure scenarios observed in the field.

2. Check basic connectivity.

Verify that the device can reach (and open the TCP port) to tools.cisco.com (in case of direct access) or to Cisco Smart Software Manager on-premise server:

<#root>

```
#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 (x.x.x.x, 443)... Open
[Connection to tools.cisco.com closed by foreign host]
```

If these commands do not work, double-check your routing rules, source-interface, and firewall settings.



Note: The 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:

```
#show tech-support license
```

and validate collected configuration / logs (attach this output in case you decide to open Cisco TAC case for further investigation).

4. Enable debugs.

Enable these debugs to collect additional information about the Smart Licensing process.



Note: After enabling debugs, you need to try to register the license once again via CLi as mentioned in point 4.1.

```
#debug call-home smart-licensing [all | trace | error]
```

```
#debug ip http client [all | api | cache | error | main | msg | socket]
```

For internal debugs, enable and read binary traces:

```
! enable debug

#set platform software trace ios [switch] active R0 infra-sl debug

!

! read binary traces infra-sl process logs

#show platform software trace message ios [switch] active R0
```

Common Failure Scenarios

This section describes 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 must be registered again.

- If the Cisco device is seen in the CSSM, the force parameter must be used (that is, license smart register idtoken <TOKEN> force).

Note: The failure reason can also show as:
- 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 1117:55:46 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, enter reporting smart-licensing-data under profile mode to configure that profile for smart licensing. For more details about SCH, check Cisco.com
%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:

%CALL_HOME-5-SL_MESSAGE_FAILED: Fail to send out Smart Licensing message to: https://<ip>/its/service/oddce/services/DDCEService (ERR 205 : Request Aborted)

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

%SMART_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.

- If DNS is not configured, configure a DNS server or a ip host statement for the local nslookup IP for tools.cisco.com.

- 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 defined and 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 443is not being blocked on the Cisco device, the path to Smart Call Home Server, or the Cisco Smart Software Manager on-prem (satellite).

- Ensure that the correct Virtual Routing and Forwarding (VRF) instance is configured under call-home, if applicable.

Scenario #6: Failure Reason: "Missing Id Cert Serial Number Field; Missing Signing Cert Serial Number Field; Signed Data and Certificate does not Match" Log

This behavior is seen when working with a CSSM on-premise server that has had its crypto certificate expire as documented in Cisco bug ID CSCvr41393. This is expected behavior as the CSSM on-prem must be allowed to sync and renew its certificate in order to prevent a certification sync issue with any registering devices.

Snip of **show license all:**

```
Registration:
  Status: UNREGISTERED
  Smart Account: Example Account
  Export-Controlled Functionality: ALLOWED

License Authorization:
 Status: EVAL MODE
```

Evaluation Period Remaining: 65 days, 18 hours, 43 minutes, 0 seconds

Possible Logs Seen:

This error is seen under show logging or show license eventlog:
SAEVT_DEREGISTER_STATUS msgStatus="LS_INVALID_DATA" error="Missing Id cert serial number field; Missing signing cert serial number field; Signed data and certificate does not match"

Next Steps:

- Verify that the Cisco device has IP connectivity to CSSM on-premise server.
- If using HTTPS, confirm the certification C-Name is being used in the devices call-home configuration.
- If a DNS server is not available to resolve the certification C-Name, configure a static ip host statement to map the domain name and IP address.

- Verify status of certificate on CSSM on-premise is still valid.
- If CSSM on-premise certificate is expired, use one of the workarounds documented in Cisco bug ID CSCvr41393

Note: By default, HTTPS performs a server identity check during the SSL handshake to verify the URL or IP is the same as the provided certificate from the server. This can cause issues when using IP addresses instead of a DNS entry if the hostname and IP do not match. If DNS is not possible, or a static ip host statement, no http secure server-identity-check can be configured to disable this certification check.

Scenario #7: 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
Communication Deadline: Oct 25 09:21:39 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 must be configured as **none** under the running configuration

show 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 #8: 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
Communication Deadline: Oct 25 09:21:39 2018 UTC

Possible logs are seen:

%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.

Scenario #9: Switch License Authorization: "Failure Reason: Data and Signature do not Match."

Snip of **show license all:**

License Authorization:

Status: AUTHORIZED on Mar 12 09:17:45 2020 EDT

Last Communication Attempt: FAILED on Mar 12 09:17:45 2020 EDT

Failure reason: Data and signature do not match

Next Communication Attempt: Mar 12 09:18:15 2020 EDT

Communication Deadline: May 09 21:22:43 2020 EDT

Possible logs are seen:

%SMART_LIC-3-AUTH_RENEW_FAILED: Authorization renewal with the Cisco Smart Software Manager (CSSM) : Error received from Smart Software Manager: Data and signature do not match for udi PID:C9000,SN:XXXXXXXXXXX

Next Steps:

- Deregister the switch with License smart deregister.

- Then register the switch using a new token with license smart register idtoken <TOKEN> force.

References

- Cisco Smart Licensing Home Page
- Cisco Community - On-Demand Trainings.
- Smart Account - management portal: Smart Software Licensing
- Smart Account - create new accounts: Smart Accounts
- Configuration Guide (example) - System Management Configuration Guide, Cisco IOS XE Fuji 16.9.x (Catalyst 9300 Switches)