Configure and Troubleshoot Smart Licensing on Nexus Platforms

Contents

- Introduction
- What is Cisco Smart Licensing?
- New to Smart Licensing and/or Smart Account Administration
- Supported Cisco Nexus Platforms
  - Nexus 3000 and 9000
  - Nexus 7000
- Supported Methods of Smart licensing on Nexus Switches
- Smart Licensing User Workflow
- Smart License Product States
  - Registered
  - Licenses
  - Request or Renewal
  - Renewal
- Registration and License States
  - Evaluation (Unidentified) State
  - Registered State
  - Authorized State
  - Out-of-Compliance State
  - Authorization Expired State
- Supported Methods on Nexus and Config
  - Method-1 (Direct Cloud Access)
  - Method-2 (Access through an HTTP Proxy)
  - Method-3 (On-Prem – Online)
  - Method-4 (On-Prem – Offline)
- What is ID Token?
  - How to Generate ID Token from CSSM
- Troubleshoot
  - Workflow
  - Known Issues
    - 1. Error -Fail to Send Out Call Home HTTP
    - 2. Error -Fail to Parse Response Data from SCH Server
    - 3. Error - Fail to Send Out Call Home HTTP Message (Fails to Establish IPC Connect with Call Home – Quo Vadis Root CA)
    - 4. Error - Lack of DNS Response Causes Callhome MTS Messages Stuck

Introduction

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

What is Cisco Smart Licensing?

A Cisco Smart Account is a managed data repository that provides full visibility and access control to Cisco software licenses, entitlements and product instances across the company

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

Supported Cisco Nexus Platforms

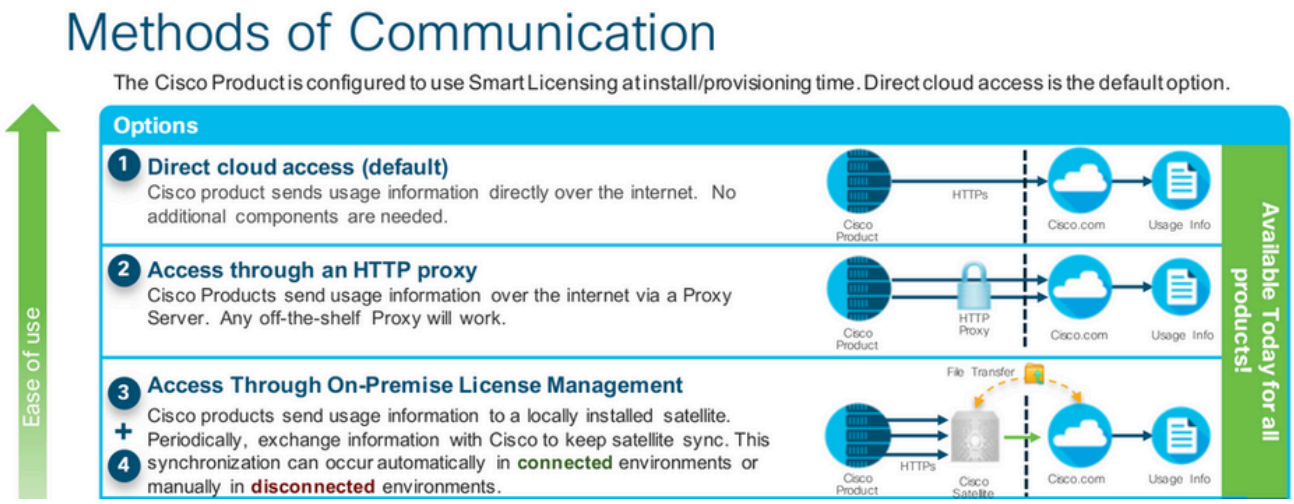
Nexus 3000 and 9000

NX-OS versions before 9.3(3) support only traditional licensing. NX-OS versions from 9.3(3) to 10.1(2) support both traditional licensing and Smart Licensing, which is covered in this document. NX-OS versions after 10.1(2) support only Smart Licensing Using Policy, which is different from Smart Licensing. For versions newer than 10.1(2), instead refer to this guide.

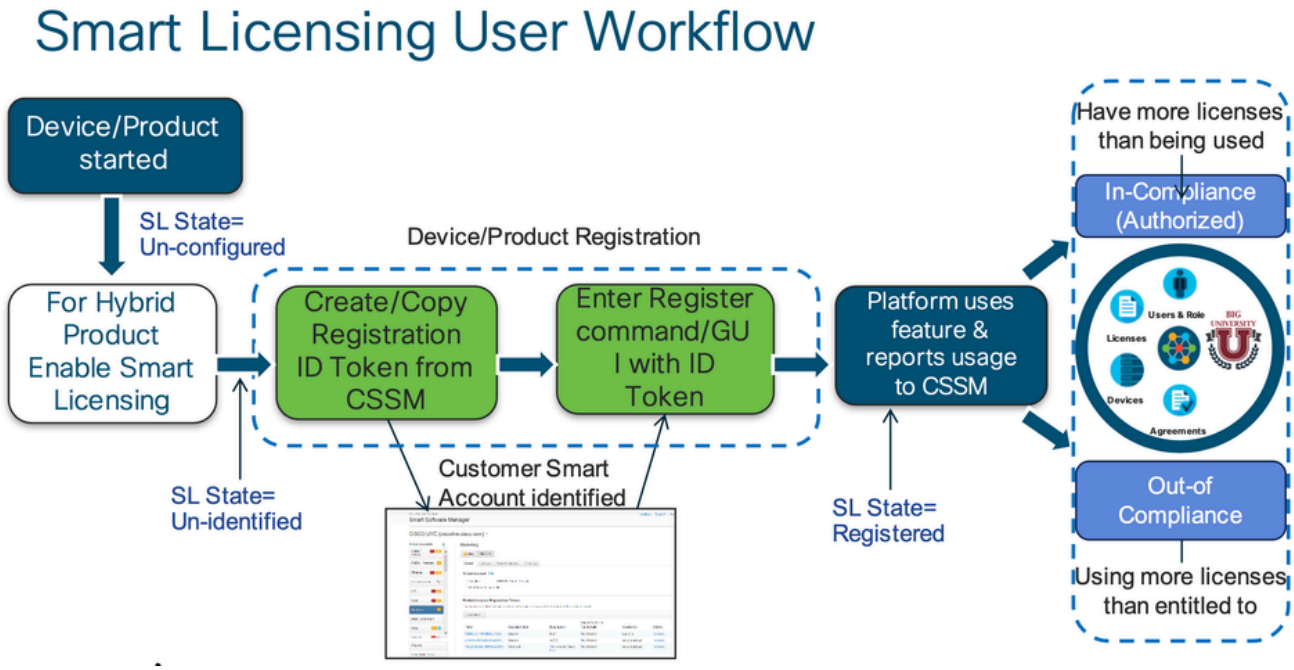
Nexus 7000

Smart Licensing is supported on Cisco Nexus 7000 with NX-OS 8.0(1) and newer.

Supported Methods of Smart licensing on Nexus Switches



Smart Licensing User Workflow



Smart License Product States

Smart License Product States

- Registered state

  Product has been associated with a valid Smart Account

- Authorized state (In Compliance)

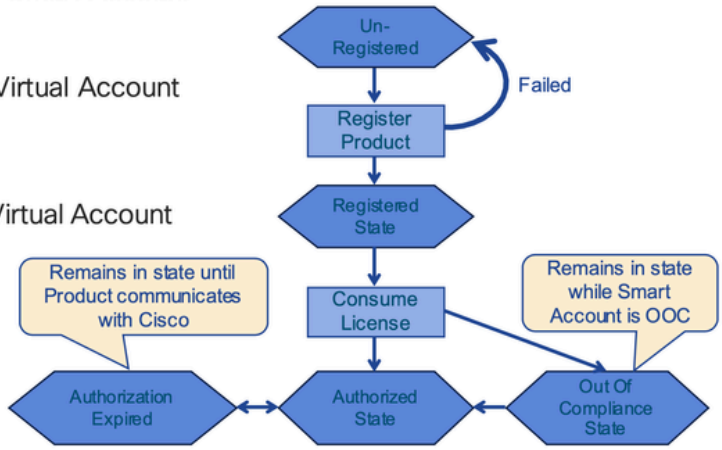
  Product is using an entitlement, and the Virtual Account does not have a negative balance

- Out of Compliance state

  Product is using an entitlement, but the Virtual Account has a negative balance

- Authorization expired state

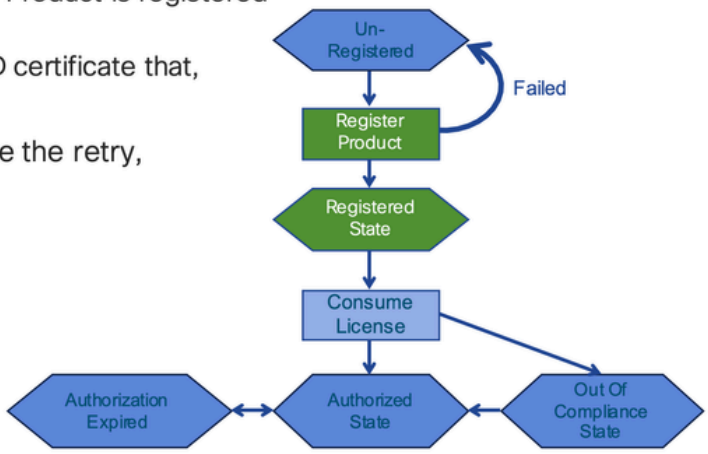
  Product has not communicated with Cisco within a maximum of 90 days



Registered

Smart License Product States – Registered

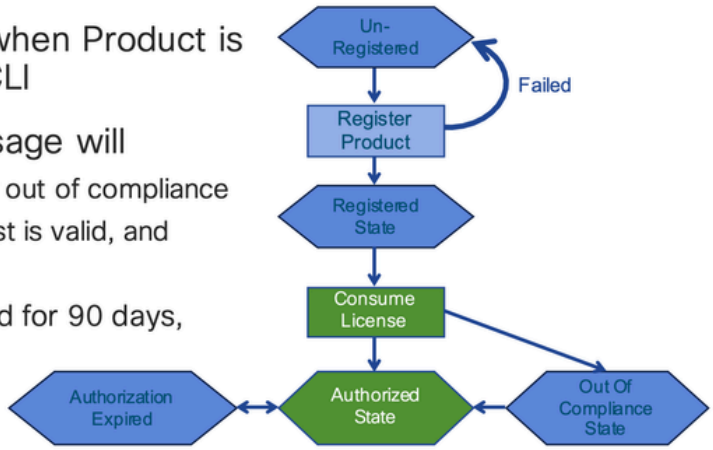
- Initial registration
  1. A Registration Message is sent when Product is registered via CLI with a valid ID Token.
  2. Cisco will reply with a Cryptograph ID certificate that, by default, is valid for one year.
- If there is a failure sending the message the retry, interval will be as follows:
  - Every 15 minutes for 4 hours.
  - Then every hour until successful, or Smart License is disabled via CLI



Licenses

Smart License Product States – Licenses

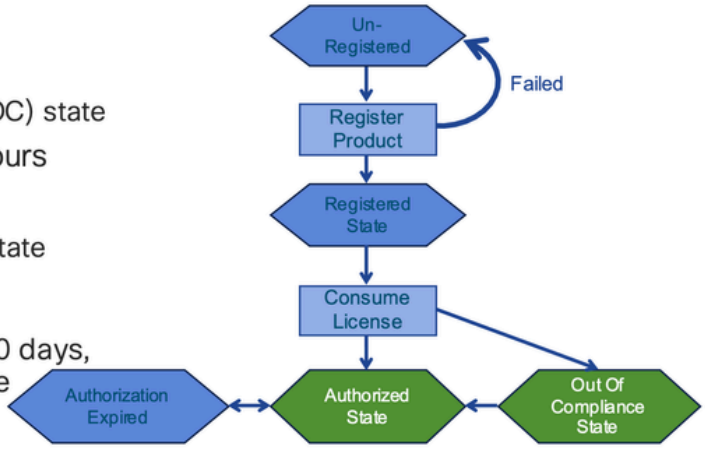
- One a product has been successfully registered, it can be configured to use an licenses via CLI
- A Entitlement Message is sent when Product is configured to use licenses via CLI
- The Entitlement Response message will
  1. Indicate if the Virtual Account is in or out of compliance
  2. Provide the length of time the request is valid, and the renewal interval.
- By default the Licenses usage is valid for 90 days, and renewed every 30 days



Request or Renewal

Entitlement Authorization Request or Renewal

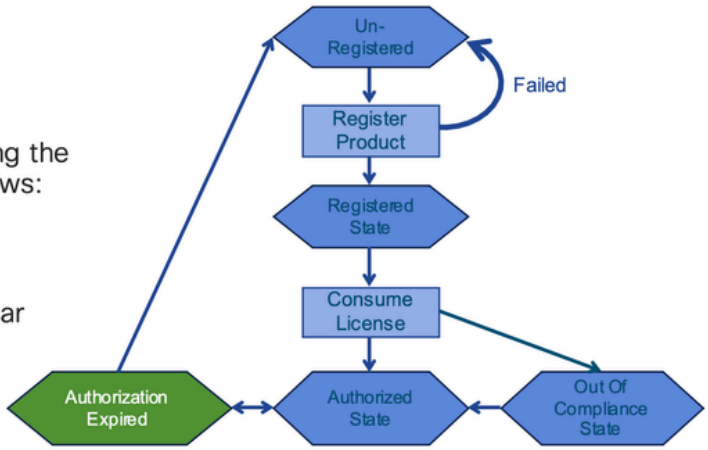
- If there is a communications failure sending the renewal, the retry interval will be as follows:
  - If the agent is in the authorized state
    - ➢Retry every 23 hours
  - If agent is in the Out of Compliance (OOC) state
    - ➢Retry every 15 minutes for two hours
    - ➢Then once every 4 hours.
  - If agent is in the authorization expired state
    - ➢Retry once every hour.
- If there is NO communications within 90 days, License usage is released and available for use by other products



Renewal

Registration ID Certificate Renewal

- By default the Cryptograph ID certificate
  - Valid duration (one Year) and renewal period is sent in with the Registration Response message .
- The Cryptograph ID certificate
  - Renewal will be sent every six months
- If there is a communications failure sending the message, the retry interval will be as follows:
  - One per hour until success
  - Or until Cryptograph ID certificate expires.
- If there is NO communications within 1 year
  - Device become “unregistered”
  - Device must be re-registered
  - Use any remaining evaluation time



Registration and License States

While Smart Licensing is setup, there are multiple possible states that a Cisco device can be in. These states can be displayed by "**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 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 does not attempt to communicate with Cisco in this state.
- This is 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 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

- This is the expected state after successfully registration is complete.
- 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 is used for future communications.
- The device sends a request to CSSM to authorize the entitlements for the licenses in use on the device.
- Based on the CSSM response the device then enters Authorized or Out-of-Compliance
- The Id certificate expires at the end of one year. After 6 months the software Agent process tries to renew the certificate. If the Agent cannot communicate with the Cisco Smart Software Manager it continues to try and renew the Id certificate until the expiration date (1 year). At the end of one year, the agent goes back to the Unidentified state and tries to enable the Evaluation period. The CSSM removes remove the product instance from its database.

Authorized State

- This is the expected state when device uses 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 licenses.
- At the end of 30 days, the device sends 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 uses 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 Compliance / Authorized state, you must add the correct number and type of licenses to the Smart Account.
- When in this state the device automatically sends an authorization renewal request every day.
- Licenses and features continue to operate and there is no functional impact.

Authorization Expired State

- This is the state when device uses 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 returns 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 continues to try to contact Cisco, every hour, to renew the entitlement authorization, until the registration period (id certificate) expires.
- Licenses and features continue to operate and there is no functional impact.
- If the software Agent re-establishes communications with Cisco and receives to its request for

authorization it processes that reply normally and enter into one of the established states.

Supported Methods on Nexus and Config

Method-1 (Direct Cloud Access)

Basic configuration:

```
switch# show run callhome

!Command: show running-config callhome
!Running configuration last done at: Wed Jun 22 16:14:37 2022
!Time: Wed Jun 22 16:16:28 2022

version 9.3(4) Bios:version 07.67
callhome
  email-contact sch-smart-licensing@cisco.com
  destination-profile CiscoTAC-1 transport-method http
  destination-profile CiscoTAC-1 index 1 http https://tools.cisco.com/its/service/oddce/services/DDCESe
transport http use-vrf management
 enable

Switch# license smart register idtoken XXXX (force)
Initiated device registration with backend. run show license status, for registration status

switch# show license status
Smart Licensing is ENABLED

Registration:
  Status: REGISTERED
  Smart Account: ldap_user_test
  Virtual Account: Default
```

```
  Export-Controlled Functionality: Allowed

  Initial Registration: SUCCEEDED on Jun 22 16:15:41 2022 UTC

  Last Renewal Attempt: None

  Next Renewal Attempt: Dec 19 16:15:41 2022 UTC

  Registration Expires: Jun 22 16:13:53 2023 UTC


License Authorization:

  Status: AUTHORIZED on Jun 22 16:15:44 2022 UTC


  Last Communication Attempt: SUCCEEDED on Jun 22 16:15:44 2022 UTC

  Next Communication Attempt: Jul 22 16:15:43 2022 UTC

  Communication Deadline: Sep 20 16:12:55 2022 UTC


Smart License Conversion:

  Automatic Conversion Enabled: False

 Status: Not started
```

https://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/nx-os/licensing/guide/b_Cisco_NX-OS_Licensing_Guide/m-smart-licensing-for-cisco-nexus-3000-and-9000-series-switches.html

Method-2 (Access through an HTTP Proxy)

```
switch# show run callhome


version 9.3(4) Bios:version 07.67


call home

email-contact sch-smart-licensing@cisco.com<mailto:sch-smart-licensing@cisco.com>

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 proxy server X.X.X.X port 80
```

```
transport http use-vrf management

transport http proxy enable


Switch# license smart register idtoken XXXX (force)
Initiated device registration with backend. run show license status, for registration status
```

Method-3 (On-Prem – Online)

```
switch# show run callhome


version 9.3(4) Bios:version 07.67

callhome

  email-contact sch-smart-licensing@cisco.com

  destination-profile CiscoTAC-1 transport-method http

  destination-profile CiscoTAC-1 index 1 http https://10.106.41.xx/Transportgateway/services/DeviceRequ

  transport http use-vrf management

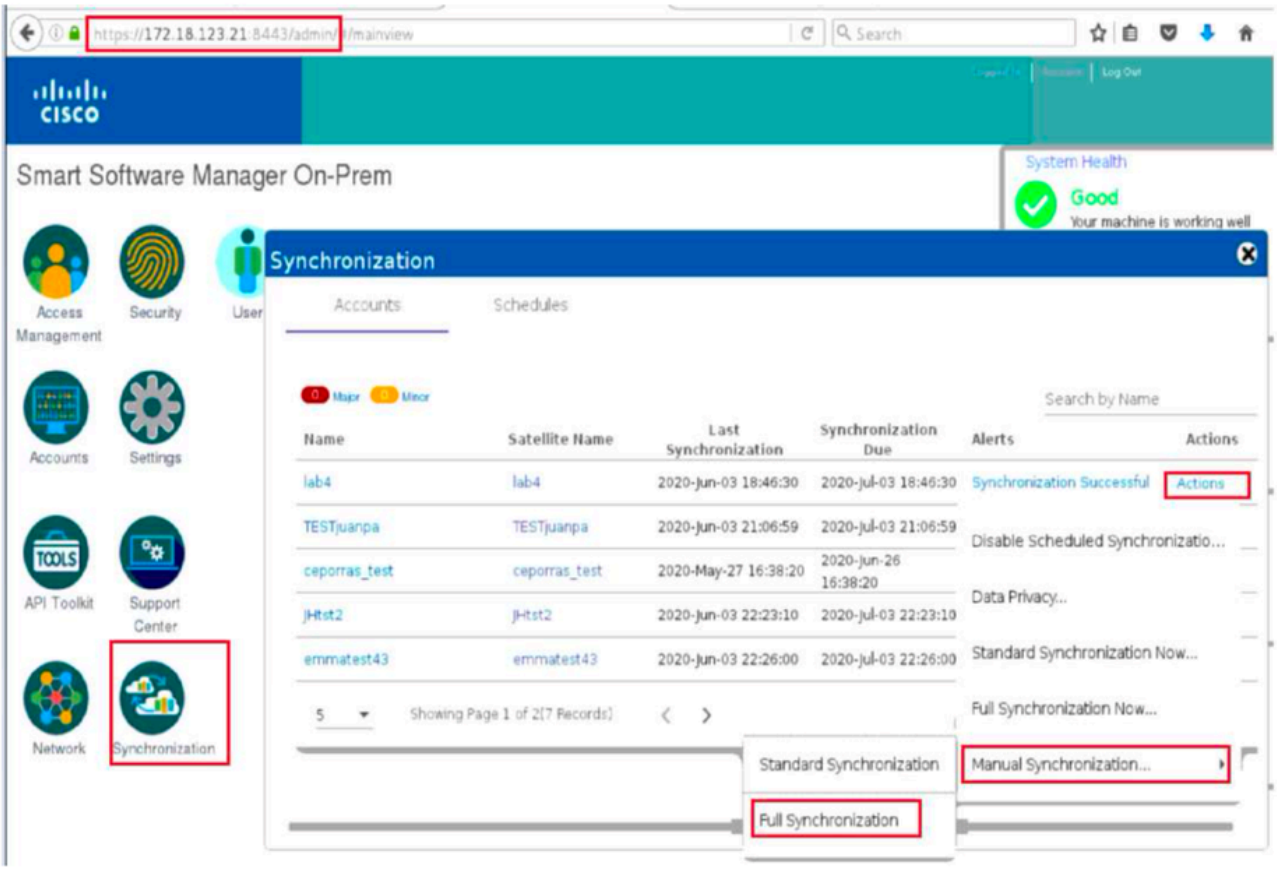
  enable


Switch# license smart register idtoken XXXX (force)

Initiated device registration with backend. run show license status, for registration status
```

Method-4 (On-Prem – Offline)

Manual sync (for when there's no internet connection)



Manual Synchronization

1. Download the satellite synchronization data file to your PC

Download File...

2. Upload the file to Smart Software Manager, and receive a synchronization response file.

- Log into Smart Software Manager, and navigate to the Satellites page
- Use the File Sync... action listed for this satellite to upload this synchronization file
- Save the synchronization response file generated by Smart Software Manager

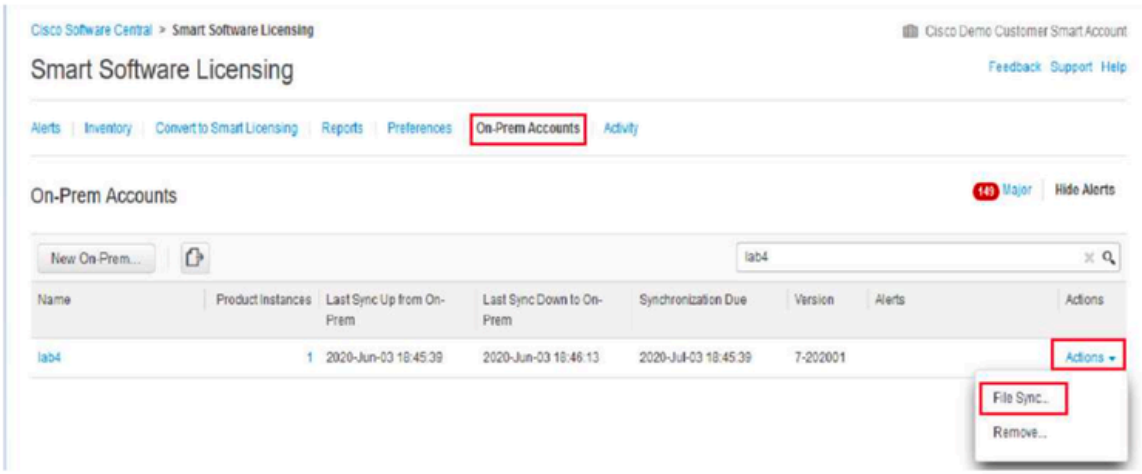
3. Upload synchronization response file to the satellite

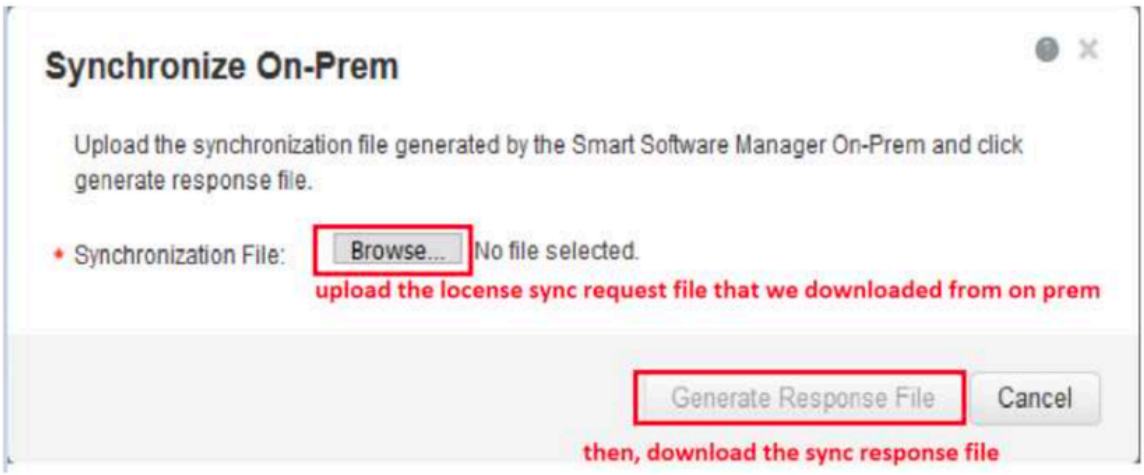
Browse... No file selected. Upload

This will download a sync request .yml file like this one:

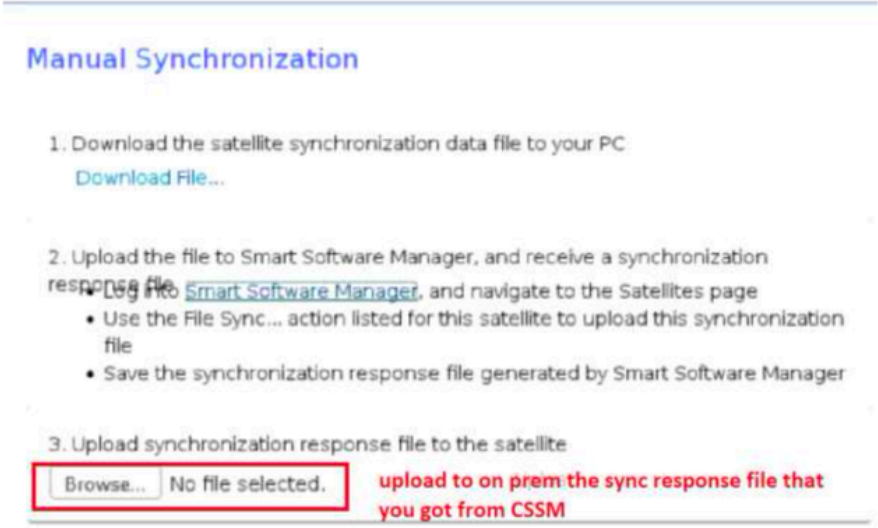
license-sync-request-Sat_20200605-1.yml

Go to CSSM (software.cisco.com)





Go back to the on prem GUI to upload the sync response file



What is ID Token?

Used to securely Register products to a Smart Account and Virtual Account

ID Tokens are organizational identifier used to establish identity when a product is registered.

How to Generate ID Token from CSSM

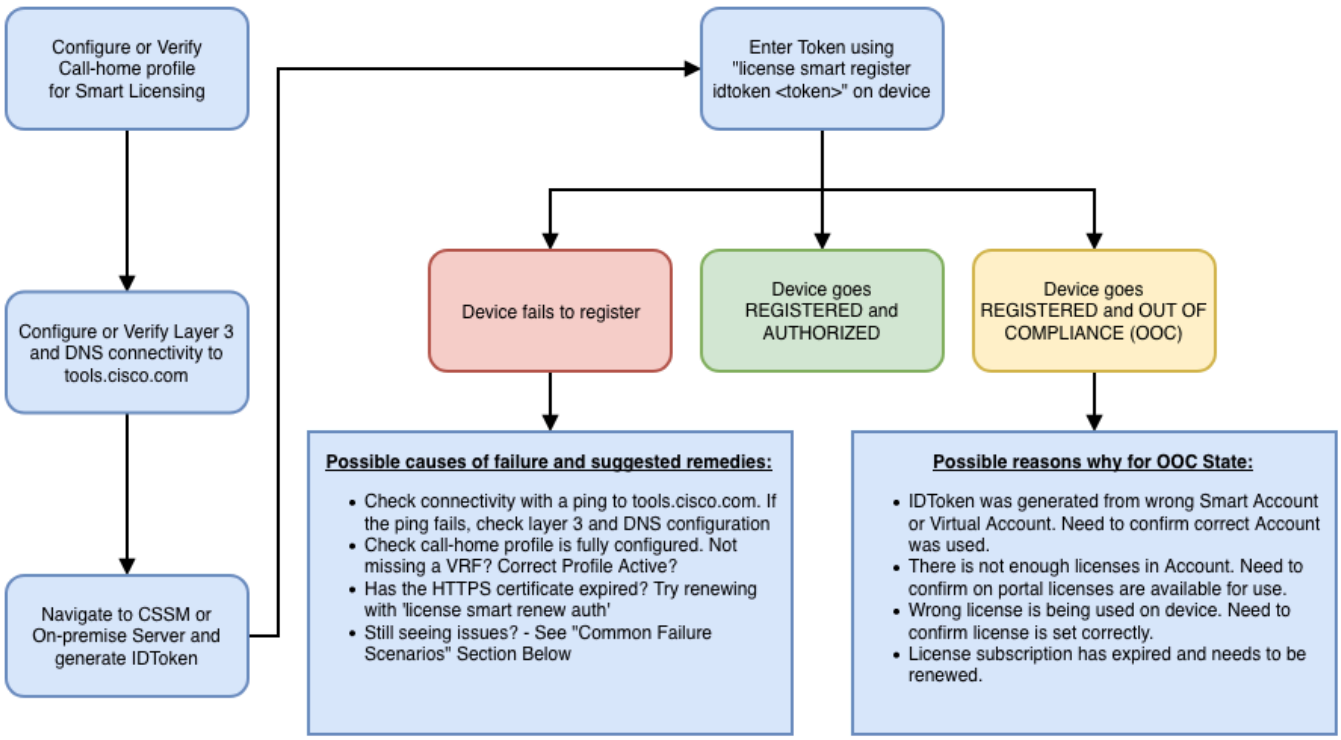
https://software.cisco.com/software/csws/ws/platform/home?locale=en_US#

Manage licenses -> Inventory -> General -> New token -> Create token

Troubleshoot

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

Workflow



Known Issues

- The issue to get N9K-C9348GC-FXP registered for smart licensing.

1. Error -Fail to Send Out Call Home HTTP

[+] Call home configs

```
Switch# show running-config callhome

version 9.3(5) Bios:version 07.68
callhome
email-contact abc@example.com
phone-contact +919XXXXXXXXX
streetaddress ST3, RD 4, Bangalore
```

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

[+] Confirmed reachablility to tools.cisco.com.

```
DC-DMZ(config)# ping tools.cisco.com vrf management
PING tools.cisco.com (72.163.4.38): 56 data bytes
64 bytes from 72.163.4.38: icmp_seq=0 ttl=232 time=237.581 ms
64 bytes from 72.163.4.38: icmp_seq=1 ttl=232 time=237.859 ms
64 bytes from 72.163.4.38: icmp_seq=2 ttl=232 time=237.562 ms
64 bytes from 72.163.4.38: icmp_seq=3 ttl=232 time=237.413 ms
64 bytes from 72.163.4.38: icmp_seq=4 ttl=232 time=237.995 ms

DC-DMZ(config)# telnet tools.cisco.com 443 vrf management
Trying 2001:420:1101:5::a...
Trying 72.163.4.38...
Connected to tools.cisco.com.
Escape character is '^]'.
^CConnection closed by foreign host.
```

+ **HTTP source interface was configured to interface vlan 27, Changed it to mgmt0**

2. Error -Fail to Parse Response Data from SCH Server

++ HTTP is no longer supported to reach backend of Cisco; HTTPS is only supported. Removed current configuration and updated the destination address to use HTTPS.

<#root>

Previous config

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

<#root>

New config added

```
(config)#callhome
```

```
(config-callhome)#enable
(config-callhome)# destination-profile CiscoTAC-1 transport-method http
(config-callhome no destination-profile CiscoTAC-1 index 1 http http://tools.cisco.com/its/service/oddc
(config-callhome destination-profile CiscoTAC-1 http https://tools.cisco.com/its/service/oddce/services
```

3. Error - Fail to Send Out Call Home HTTP Message (Fails to Establish IPC Connect with Call Home – Quo Vadis Root CA)

https://www.cisco.com/c/en/us/support/docs/field-notices/721/fn72115.html

4. Error - Lack of DNS Response Causes Callhome MTS Messages Stuck

Cisco Bug ID CSCvv67469