Configure HSECK9 License on cEdge SD-WAN XE

Contents

Introduction

This document describes how to install and troubleshoot HSECK9 licenses on SD-WAN XE cEdges.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco Software-defined Wide Area Network (SD-WAN)
- Cisco IOS® XE Command Line Interface (CLI)
- Smart Licensing
- Cisco Software Central

Components Used

This document is based on these software and hardware versions:

- cEdge C1111-8PWE version 17.6.3
- Cisco Smart Software Manager (CSSM)

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

Background Information

Concepts

Smart Licensing Using Policy uses a variety of new concepts, such as:

- License Enforcement Types
- License Duration
- Authorization Code
- Throughput Level That Requires Smart Licensing Authorization Code (SLAC) - Router Platforms that need a SLAC
- Policy
- Resource Utilization Measurement Report (RUM report) and Report Acknowledgement
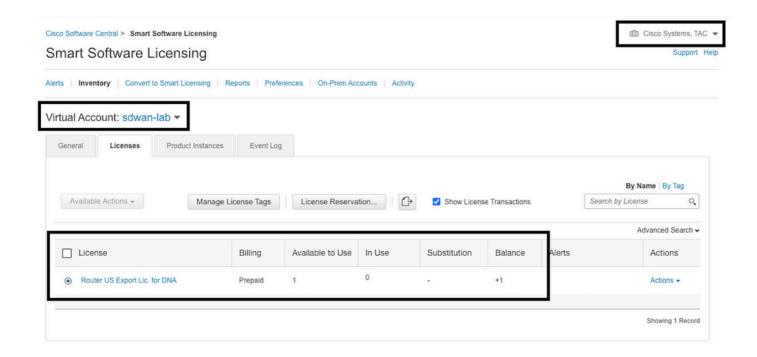
- Trust Code

For more information navigate to [Smart Licensing Using Policy Concepts.](#)

Throughput Behavior

- All ISR1000 Series, ISR4000 Series, C8200, C8300, CSR1000v, C8000v and ISRv default to 250 Mbps if the product does not have any form of HSECK9 license.
- All ISR1000 Series, ISR4000 Series, C8200, C8300, CSR1000v, C8000v and ISRv need to have an HSECK9 license installed if the throughput needs to be higher than 250 Mbps.
- All ASR1000 Series does not need to have HSECK9 for >250 Mbps.
- All C8500 are expected to have an HSECK9 license installed in the manufactory. If not, the HSECK9 license can be installed manually.
- There is no throughput configuration in the Controller-managed Mode. The HSECK9 license installation automatically enables the forwarding Cores/Packet Processor Engines to unleash throughput.
- The maximum throughput after the HSECK9 license installation depends on the hardware capabilities of the platform. Review the specific Platform Datasheet for more information.

License Availability Verification

Step 1. Navigate to **Cisco Software Central.**

Step 2. Click**Smart Software Manager**.

Step 3. Select **Inventory** from the top menu.

Step 4. Choose the appropriate **Virtual Account**.

Step 5. Select the **Licenses** tab under the Virtual Account.

Step 6. Verify that the license is added and available with a positive balance.

Smart Software Licensing

Support Help

Alerts | **Inventory** | Convert to Smart Licensing | Reports | Preferences | On-Prem Accounts | Activity

Virtual Account: sdwan-lab ▾

| General | **Licenses** | Product Instances | Event Log |

By Name | By Tag

| Available Actions ▾ | | Manage License Tags | License Reservation... | ⎋ | ☑ Show License Transactions | Search by License 🔍 |

Advanced Search ❯

☐ License	Billing	Available to Use	In Use	Substitution	Balance	Alerts	Actions
⊕ Router US Export Lic. for DNA	Prepaid	1	0	-	+1		Actions ▾

Showing 1 Record

If no license is available or the balance is negative (red), please open a case with Cisco Licensing Team.

> **Note**: This guide assumes that you already purchased an HSECK9 license or Router US Export License for DNA and it is added to a valid virtual account within a smart account.

Router Operation Mode

Verify the router is on Controller-Managed mode with one of the commands.

```
show platform software device-mode
show version | include mode
```
Example:

```
Router# show platform software device-mode
Device Operating-mode: Controller-Managed
Device-mode bootup status:
8/03 00:44:16 System is green
Bootup Success

Router# show version | in mode
Router operating mode: Controller-Managed
```

> **Note**: If the operating mode results in Autonomous, move the router to Controller-Managed with **controller-mode enable** command.

Configure

Online Method To CSSM

Configure Transport Type and Set Default CSSM URL

Step 1. Configure the correct Transport Type and URL.

```
cEdge#config-transaction
cEdge(config)# license smart transport smart
cEdge(config)# license smart url default
cEdge(config)# commit
Commit complete.
```

> **Note**: If the router has a template attached to it. The smart commands for Transport and URL are supported and can be configured with a CLI-Add On Feature Template. For more information navigate to [CLI Add-On Feature Templates.](#)
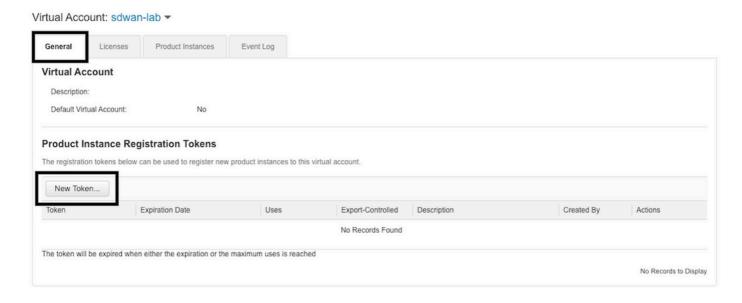
Step 2. Verify the changes are committed correctly.

```
cEdge# show lic tech support | begin Smart Licensing Status
Smart Licensing Tech Support info

Smart Licensing Status
=====================

Smart Licensing is ENABLED

License Conversion:
Automatic Conversion Enabled: True
Status: Not started

Export Authorization Key:
Features Authorized:
<none>

Utility:
Status: DISABLED

Smart Licensing Using Policy:
Status: ENABLED

Data Privacy:
Sending Hostname: yes
Callhome hostname privacy: DISABLED
Smart Licensing hostname privacy: DISABLED
Version privacy: DISABLED

Transport:
Type: Smart <<<<<<<<<<<<<<<<<<<<<<<<<<<< This must be Smart
URL: https://smartreceiver.cisco.com/licservice/license <<<<<<<<<<<<<< URL must be pointed to
smartreceiver.cisco.com
Proxy:
Address: <empty>
Port: <empty>
Username: <empty>
Password: <empty>
Server Identity Check: True
```

> **Note**: The default URL is activated automatically and there is no need to modify it.

Generate a Product Instance Registration Token

Step 1. Generate a New Token.

Within the same virtual account where the license resides, navigate to **General** tab and click **New Token.**

Virtual Account: sdwan-lab ▾

General	Licenses	Product Instances	Event Log

Virtual Account

Description:

Default Virtual Account: No

Product Instance Registration Tokens

The registration tokens below can be used to register new product instances to this virtual account.

[New Token...]

Token	Expiration Date	Uses	Export-Controlled	Description	Created By	Actions
			No Records Found			

The token will be expired when either the expiration or the maximum uses is reached

No Records to Display

Step 2. Fill up the new token information.

Create Registration Token

This will create a token that is used to register product instances, so that they can use licenses from this virtual account. Once it's created, go to the Smart Licensing configuration for your products and enter the token, to register them with this virtual account.

Virtual Account:	sdwan-lab
Description:	hseckk9 Installation
* Expire After:	30 Days
	Between 1 - 365, 30 days recommended
Max. Number of Uses:	
	The token will be expired when either the expiration or the maximum uses is reached

☑ Allow export-controlled functionality on the products registered with this token ⓘ

[Create Token] [Cancel]

Description: Brief description of what the token is used for.
Expire after: Number of days the token is valid for product registrations.
Max. Number of Uses: Token maximum number of uses. Optional.

Ensure the **Allow export-controlled** the option is checked, otherwise, the license registration fails and then click **Create Token.**

> **Note**: The token expires when either the expiration or the maximum use is reached.

> **Note**: For more information navigate to [Cisco Export Trade.](#)

Step 3. Copy the token.

Copy the just generated token to the clipboard; either navigate to **Actions > Copy** or manually in the small blue icon next to the token string.

Generate a Trust Establishment between the cEdge And CSSM

In order to provide authorization to use an export-controlled license, the cEdge must establish trust with the CSSM. For the handshake, the cEdge uses the token generated on CSSM in the previous step.

```
license smart trust idtoken TOKEN local force
```
Example:

```
cEdge# license smart trust idtoken
ZThjOTlmM2UtMjQ2ZC00YjI1LTgwNjctZGIxZjIzYjZiYmVmLTE2NjM0NjI1%0AMjgyNTh8YWNVeTFiZU03N0lCdTFadmJ4e
jZBL0toR2Mva21odElrQmxDa1FN%0AcVI3cz0%3D%0A local force
```
Right after the trust is established, the logs show communication with CSSM.

```
cEdge# show logging last 50
<snip>
*Aug 18 21:03:44.730: %CRYPTO_ENGINE-5-KEY_DELETED: A key named SLA-KeyPair2 has been removed
from key storage
*Aug 18 21:03:46.146: %CRYPTO_ENGINE-5-KEY_ADDITION: A key named SLA-KeyPair2 has been generated
or imported by crypto-engine
*Aug 18 21:03:53.221: %SYS-6-PRIVCFG_ENCRYPT_SUCCESS: Successfully encrypted private config file
*Aug 18 21:03:56.107: %SMART_LIC-5-COMM_RESTORED: Communications with Cisco Smart Software
Manager (CSSM) restored
*Aug 18 21:03:56.347: %SMART_LIC-6-TRUST_INSTALL_SUCCESS: A new licensing trust code was
successfully installed on P:C1111-8PWE,S:FGL2149XXXX.
```

Verify the Trust Establishment Sucess Counter

Verify that the trust establishment success counter increases, this means the licensing agent can

reach CSSM.

```
cEdge# show lic tech support | begin Communication Statistics
Communication Statistics:
========================
Communication Level Allowed: DIRECT
Overall State: <empty>
Trust Establishment:
Attempts: Total=1, Success=1, Fail=0 Ongoing Failure: Overall=0 Communication=0 <<<<<<<<<
Last Response: OK on Aug 18 21:03:56 2022 UTC
Failure Reason: <none>
Last Success Time: Aug 18 21:03:56 2022 UTC
Last Failure Time: Aug 18 21:00:43 2022 UTC
<snip>
```

Note: If the fail counter increments, navigate to the Troubleshoot section in this document.

Request Authorization

At this point, the trust is established but the HSECK9 license is not in use yet. This happens because it is required to make the router request to CSSM the license usage. In order to fetch the license run the authorization request.

```
cEdge# license smart authorization request add hseck9 local
Logs:
```

```
cEdge# show logging | include SMART
*Aug 18 21:11:41.553: %SMART_LIC-6-AUTHORIZATION_INSTALL_SUCCESS: A new licensing authorization
code was successfully installed on PID:C1111-8PWE,SN:FGL2149XXXX
*Aug 18 21:11:41.641: %SMART_LIC-6-EXPORT_CONTROLLED: Usage of export controlled features is
allowed for feature hseck9
```

In the smart licensing eventlog, the license request information is saved in case more information is needed.

```
cEdge# show lic eventlog 0
**** Event Log ****
2022-08-18 21:11:41.538 UTC SAEVT_RESERVE_INSTALL_START udi="PID:C1111-8PWE,SN:FGL2149XXXX"
authorizationCode="<smartLicenseAuthorization><udi>P:C1111-
8PWE,S:FGL2149XXXX</udi><authorizationCode><customerInfo><smartAccount>Cisco Systems,
TAC</smartAccount><virtualAccount>sdwan-
lab</virtualAccount></customerInfo><flag>A</flag><version>C</version><piid>d216f143-7e2c-48df-
aa71-652b15ea1c7e</piid><dateStamp>2022-08-
18T21:17:45</dateStamp><entitlements><entitlement><tag>regid.2019-
03.com.cisco.DNA_HSEC,1.0_509c41ab-05a8-431f-95fe-
ec28086e8844</tag><count>1</count><startDate></startDate><endDate></endDate><licenseType>PERPETU
AL</licenseType><displayName>Router US Export Lic. for DNA</displayName><tagDescription>U.S.
Export Restriction Compliance license for DNA based
Routers</tagDescription><tagType>PERPETUAL</tagType><status><success>true</success></status></en
titlement></entitlements><status><success>true</success><correlationID>62feac79ca9112704623118db
58bbc2c-
09b6eebc91ae833f</correlationID></status></authorizationCode><signature>MEUCIBuNw8+ogfZmJAbsRa+8
B+F0wnDZLrv5RXm822rN/he5AiEAtfzzFV9L3dqht4sUYDxRvnUHF2KYi+vFv2vivDF6rIs=</signature></smartLicen
seAuthorization>"
2022-08-18 21:11:41.552 UTC SAEVT_TAG_EXPORT exportAllowed="False" count="0"
entitlementTag="regid.2019-03.com.cisco.DNA_HSEC,1.0_509c41ab-05a8-431f-95fe-ec28086e8844"
```

2022-08-18 21:11:41.576 UTC SAEVT_TAG_EXPORT exportAllowed="True" count="0"
entitlementTag="regid.2019-03.com.cisco.DNA_HSEC,1.0_509c41ab-05a8-431f-95fe-ec28086e8844"
2022-08-18 21:11:41.576 UTC SAEVT_STATE_RESERVE_AUTHORIZED
2022-08-18 21:11:41.641 UTC SAEVT_TAG_AUTHORIZED count="1" entitlementTag="regid.2019-
03.com.cisco.DNA_HSEC,1.0_509c41ab-05a8-431f-95fe-ec28086e8844"
2022-08-18 21:11:41.641 UTC SAEVT_TAG_EXPORT exportAllowed="True" count="1"
entitlementTag="regid.2019-03.com.cisco.DNA_HSEC,1.0_509c41ab-05a8-431f-95fe-ec28086e8844"
2022-08-18 21:12:06.119 UTC SAEVT_RESERVE_INSTALL_START udi="PID:C1111-8PWE,SN:FGL2149XXXX"
authorizationCode="<smartLicenseAuthorization><udi>P:C1111-
8PWE,S:FGL2149XXXX</udi><authorizationCode><customerInfo><smartAccount>Cisco Systems,
TAC</smartAccount><virtualAccount>sdwan-lab</virtualAccount></customerInfo><piid>d216f143-7e2c-
48df-aa71-652b15ea1c7e</piid><status><success>false</success><message>last update already
confirmed</message><code>last update already
confirmed</code><correlationID>62feac7c4be974f92eefc15a640f938b-
f08787827763ca37</correlationID></status></authorizationCode><signature>MEUCIQDhI8x+Rzf7wyibdohv
YY6q9/8puukf8SuJ4ok48d4y5QIgdl5/z/7rLu+LEd5gK9kgOxA2Vb+vnJUcTOVPo3/R0pc=</signature></smartLicen
seAuthorization>"

Verify the Activation is Successful

There are some commands to verify whether the license is now available and correctly activated.

show license tech support | begin License Usage
show license authorization
show license summary
show license usage

Example:

```
cEdge# show license tech support | begin License Usage
License Usage
=============
Handle: 1
License: hseck9
Entitlement Tag: regid.2019-03.com.cisco.DNA_HSEC,1.0_509c41ab-05a8-431f-95fe-ec28086e8844
Description: hseck9
Count: 1
Version: 1.0
Status: IN USE(15)              <<<<<<<<<<<<<<<<<<<<<
Status time: Aug 18 21:11:41 2022 UTC
Request Time: Aug 18 21:11:41 2022 UTC
Export status: RESTRICTED - ALLOWED
Feature Name: hseck9
Feature Description: hseck9
Enforcement type: EXPORT RESTRICTED
License type: Perpetual
Measurements:
ENTITLEMENT:
Interval: 00:15:00
Current Value: 1

cEdge# show license authorization
Overall status:
Active: PID:C1111-8PWE,SN:FGL2149XXXX
Status: SMART AUTHORIZATION INSTALLED on Aug 18 21:11:41 2022 UTC   <<<<<<<<<<<<<<<
Last Confirmation code: 0cde51c5

Authorizations:
Router US Export Lic. for DNA (DNA_HSEC):
Description: U.S. Export Restriction Compliance license for DNA based Routers
Total available count: 1
```

```
Enforcement type: EXPORT RESTRICTED
Term information:
Active: PID:C1111-8PWE,SN:FGL2149XXXX
Authorization type: SMART AUTHORIZATION INSTALLED   <<<<<<<<<<<<<
License type: PERPETUAL
Term Count: 1

Purchased Licenses:
No Purchase Information Available


Edge# show license summary
License Usage:
License Entitlement Tag Count Status
-------------------------------------------------------------------------
hseck9 (DNA_HSEC) 1 IN USE      <<<<<<<<<<
```
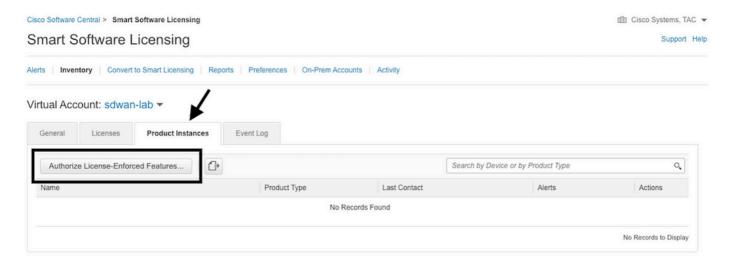
Offline Method To CSSM

For Air-gapped Networks where Internet access is not permitted, the Export-controlled license installation can be performed with a local reservation of a SLAC on the CSSM.

> **Note**: This method does not require a transport type nor a valid smart Uniform Resource Locator (URL).

Generate a Local License Reservation

In the same virtual account in which the license resides, navigate to **Product Instances > Authorize License-Enforced Features.**
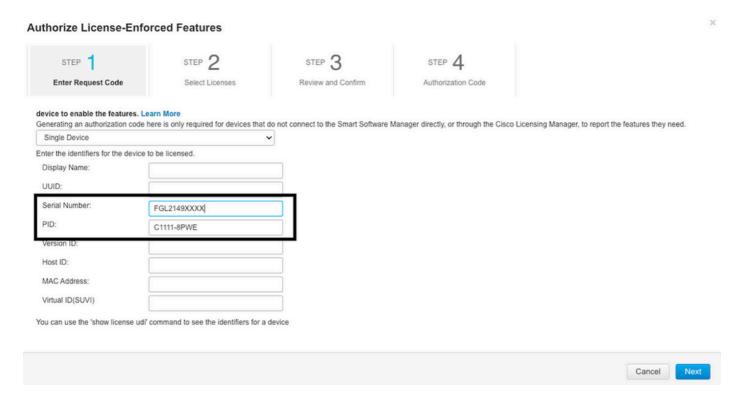

Get the cEdge UDI Information

The local license reservation requires the Unique Device Identifier (UDI) from the cEdge, run **show license udi** command to obtain the Product ID (PID) and Serial Number (SN).

```
cEdge# show license udi
UDI: PID:C1111-8PWE,SN:FGL2149XXXX
```

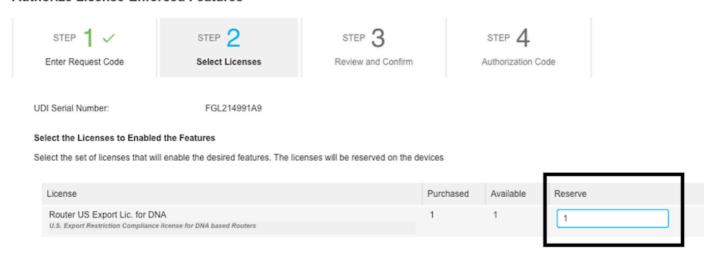### Fill the cEdge UDI in the Reservation Form

Select **Single Device** and fill in the SN and PID of the cEdge. Click **Next**.

Select the Number of Licenses to Reserve

Since it is a Single Device the reserved license is one, type the number in the box. Ensure the number does not exceed the available ones.
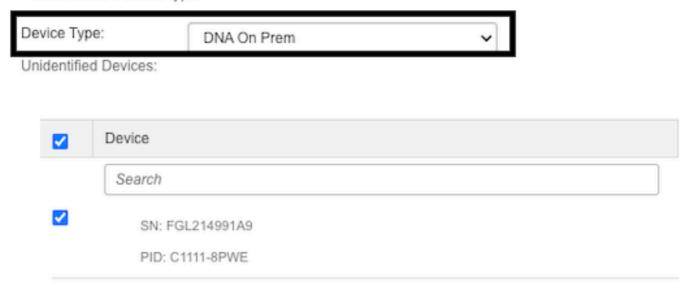

Select the License Device Type

The Device Type can be either Digital Network Architecture (DNA) On-Prem or DNA Cloud, this depends on the type of license purchased.
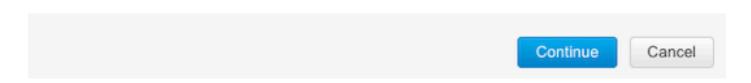
Select a Device Type

Some devices could not be identified based on the identifiers provided.
Please select a device type.

Device Type: DNA On Prem   ⌄

Unidentified Devices:

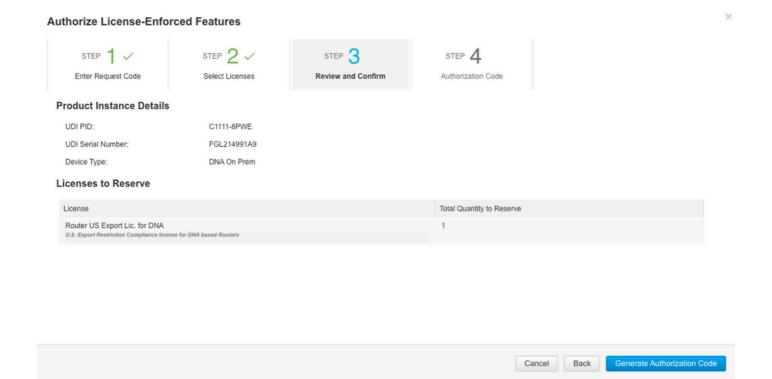| ☑	Device
	Search
☑	SN: FGL214991A9
	PID: C1111-8PWE

Selected:1

If you want to enable features on different types of devices, you must perform this operation separately for each type.

Continue   Cancel

Generate the Authorization Code

Review the configuration and click **Generate Authorization Code.**

Authorize License-Enforced Features

STEP 1 ✓	STEP 2 ✓	STEP 3	STEP 4
Enter Request Code	Select Licenses	**Review and Confirm**	Authorization Code

Product Instance Details

UDI PID: C1111-8PWE

UDI Serial Number: FGL214991A9

Device Type: DNA On Prem

Licenses to Reserve

License	Total Quantity to Reserve
Router US Export Lic. for DNA *U.S. Export Restriction Compliance license for DNA based Routers*	1

Cancel   Back   **Generate Authorization Code**

Download The SLAC

The SLAC can be downloaded as a file or copied to the clipboard.

Copy The SLAC To The cEdge

There are three options to copy the SLAC file to the cEdge.

- With a USB Drive:

```
cEdge# show file systems | include usb|Size
Size(b) Free(b) Type Flags Prefixes
15598043136 15596658688 disk  rw      usb0:

cEdge# dir usb0:
Directory of usb0:/

5 -rwx 1557 Aug 19 2022 00:43:30 +00:00 AuthorizationCode_SN_FGL2149XXXX.txt

15598043136 bytes total (15596658688 bytes free)

cEdge# copy usb0:AuthorizationCode_SN_FGL2149XXXX.txt bootflash:
Destination filename [AuthorizationCode_SN_FGL2149XXXX.txt]?
Copy in progress...C
1557 bytes copied in 0.020 secs (77850 bytes/sec)
```

- With vManage through Control Connections, navigate to [Transfer Files between a cEdge and vManage](#) for more information.
- SCP/FTP/TFTP in the Service Side.

Install The SLAC

Use Smart Import to install the SLAC file in bootflash.

```
cEdge# license smart import bootflash:AuthorizationCode_SN_FGL2149XXXX.txt
Import Data Successful
Last Confirmation code UDI: PID:C1111-8PWE,SN:FGL2149XXXX
Confirmation code: aaa6b57e
```

Logs.

```
cEdge# show logging | include SMART
*Aug 19 05:42:45.309: %SMART_LIC-6-AUTHORIZATION_INSTALL_SUCCESS: A new licensing authorization
code was successfully installed on PID:C1111-8PWE,SN:FGL2149XXXX
*Aug 19 05:42:45.362: %SMART_LIC-6-EXPORT_CONTROLLED: Usage of export controlled features is
allowed for feature hseck9
```

```
cEdge# show license eventlog 0
**** Event Log ****

2022-08-19 05:42:45.293 UTC SAEVT_RESERVE_INSTALL_START udi="PID:C1111-8PWE,SN:FGL2149XXXX"
authorizationCode="<smartLicenseAuthorization><udi>P:C1111-
8PWE,S:FGL2149XXXX</udi><authorizationCode><customerInfo><smartAccount>Cisco Systems,
TAC</smartAccount><virtualAccount>sdwan-
lab</virtualAccount></customerInfo><flag>A</flag><version>C</version><piid>0ceadf0a-3145-4779-
8cbb-743c5a234a05</piid><dateStamp>2022-08-
19T05:43:11</dateStamp><entitlements><entitlement><tag>regid.2019-
03.com.cisco.DNA_HSEC,1.0_509c41ab-05a8-431f-95fe-
ec28086e8844</tag><count>1</count><startDate></startDate><endDate></endDate><licenseType>PERPETU
AL</licenseType><displayName>Router US Export Lic. for DNA</displayName><tagDescription>U.S.
Export Restriction Compliance license for DNA based
Routers</tagDescription><tagType>PERPETUAL</tagType><status><success>true</success></status></en
titlement></entitlements><status><success>true</success><correlationID>62ff22ec38ab5858bde12581a
2589b39-
bde12581a2589b39</correlationID></status></authorizationCode><signature>MEUCIQDrUe11CPAsnjonKRmU
e40arqPiY/q/UfTGSJ1IdmkkrAIgF8G2zoHIxz04IVO2J7ZHA1M51+QMvLzUGyZsfvwK5tk=</signature></smartLicen
seAuthorization>"
2022-08-19 05:42:45.308 UTC SAEVT_TAG_EXPORT exportAllowed="False" count="0"
entitlementTag="regid.2019-03.com.cisco.DNA_HSEC,1.0_509c41ab-05a8-431f-95fe-ec28086e8844"
2022-08-19 05:42:45.333 UTC SAEVT_TAG_EXPORT exportAllowed="True" count="0"
entitlementTag="regid.2019-03.com.cisco.DNA_HSEC,1.0_509c41ab-05a8-431f-95fe-ec28086e8844"
2022-08-19 05:42:45.334 UTC SAEVT_STATE_RESERVE_AUTHORIZED
2022-08-19 05:42:45.362 UTC SAEVT_TAG_AUTHORIZED count="1" entitlementTag="regid.2019-
03.com.cisco.DNA_HSEC,1.0_509c41ab-05a8-431f-95fe-ec28086e8844"
2022-08-19 05:42:45.362 UTC SAEVT_TAG_EXPORT exportAllowed="True" count="1"
entitlementTag="regid.2019-03.com.cisco.DNA_HSEC,1.0_509c41ab-05a8-431f-95fe-ec28086e8844"
```
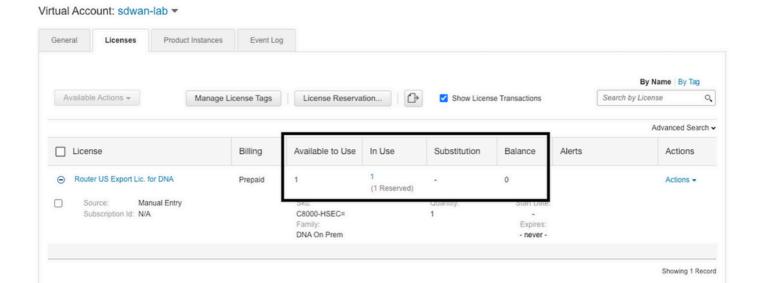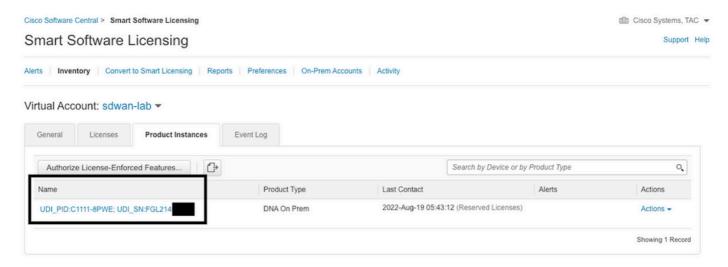
Verify the Installation is Successful

Use the same command as in the online method in order to verify whether the license is installed correctly.

```
show license authorization
show license summary
show license tech support | begin License Usage
```

If the installation is correct, the license in the Virtual Account automatically increments **In Use** counter and decrements the **Available to Use** counter.

Also in **Product Instances** tab, the UDI information of the cEdge is shown, click on the entry to get more information about the license characteristics.

Return The HSECK9 License

Online Method

Currently, there is no implementation in controller-managed mode to return a license in neither online nor offline methods.

```
cEdge# license smart authorization return local online
Operation cannot be completed because license is in use

cEdge# license smart authorization return local offline
Operation cannot be completed because license is in use
```

In order to remove the license installation, the router needs to be changed to autonomous mode.

```
cEdge# controller-mode disable
Disabling controller mode erases the nvram filesystem, remove all configuration files, and
reload the box!
Ensure the BOOT variable points to a valid image
```

```
Continue? [confirm]
```

> **Note**: This mode change removes the current SD-WAN configuration, it is highly recommended to backup the configuration in a safe place. This helps to rebuild Control Connections when the cEdge is moved back to Controller-managed mode.

Once the router is in autonomous mode, some basic configuration must be done to have reachability to Internet and Domain Name System (DNS) resolution:

1. Configure an IP address and mask for the WAN Interface
2. Power on the WAN Interface
3. Configure a default IP route
4. Enable DNS
5. Configure a DNS server

> **Note**: Autonomous Mode uses configure terminal command to get into configuration mode, instead of **configuration-transaction** command.

> **Note**: Autonomous Mode does not need to commit changes, instead any configuration done is saved in the running-configuration file.

Use a token from the same Virtual Account where the HSECK9 or DNA export-controlled license resides in. If there is no active token, generate a new one.

Follow the same procedure as in cEdge to generate a trust established with the CSSM.

```
Router# configure terminal
Router(config)# license smart transport smart
Router(config)# license smart url default
Router(config)# end
Router# license smart trust idtoken TOKEN local force
Router# license smart authorization request add hseck9 local
```

> **Note**: Use the same commands explained before to verify the correct transport type and smart receiver URL are enabled and the trust establishment was completed successfully.

Once the communication is completed, return the license back to the bin in the virtual account.

```
Router# license smart authorization return local online
Authorization already returned with this code:
UDI: PID:C1111-8PWE,SN:FGL2149XXXX
Return code: CmJHqn-5CFUkd-effkCh-4XqCpQ-SgK5Sz-fQFfM8-6qH7MA-33hDbX-sXT
```
Logs.

```
Router# show logging | include SMART
*Aug 18 22:00:22.998: %SMART_LIC-6-AUTHORIZATION_REMOVED: A licensing authorization code has
been removed from PID:C1111-8PWE,SN:FGL2149XXXX.

Router#show license eventlog 0
```

```
**** Event Log ****
2022-08-18 22:08:53.275 UTC SAEVT_RESERVE_RETURN_START udi="PID:C1111-8PWE,SN:FGL2149XXXX"
authorizationCode="<smartLicenseAuthorization><udi>P:C1111-
8PWE,S:FGL2149XXXX</udi><authorizationCode><customerInfo><smartAccount>Cisco Systems,
TAC</smartAccount><virtualAccount>sdwan-
lab</virtualAccount></customerInfo><flag>A</flag><version>C</version><piid>519e0f72-85d6-4a57-
8805-5999e7b712be</piid><dateStamp>2022-08-
18T22:08:17</dateStamp><entitlements><entitlement><tag>regid.2019-
03.com.cisco.DNA_HSEC,1.0_509c41ab-05a8-431f-95fe-
ec28086e8844</tag><count>1</count><startDate></startDate><endDate></endDate><licenseType>PERPETU
AL</licenseType><displayName>Router US Export Lic. for DNA</displayName><tagDescription>U.S.
Export Restriction Compliance license for DNA based
Routers</tagDescription><tagType>PERPETUAL</tagType><status><success>true</success></status></en
titlement></entitlements><status><success>true</success><correlationID>62feb851b0b3a2264144901cb
3491c22-
ff31e87ded74ffde</correlationID></status></authorizationCode><signature>MEUCIQCTL9Y/HrhJXgR3+oxC
WH/mpLxezThnvoAMFRIO7BHzJgIgBNDnvAD4u1eiQZ3Qrg8uGc4I6rLkbR/pn3fDv67eG5c=</signature></smartLicen
seAuthorization>"
```

Note: Move the router back to Controller-managed Mode with **controller-mode enable** command.

Offline Method

In order to generate the return code, the router must be in autonomous mode. Follow the Online Method to change the mode.

Generate the Return Code

The return code is needed to validate the reserved license in CSSM with the local authorization in the router.

```
Router# license smart authorization return local offline
Enter this return code in Cisco Smart Software Manager portal:
UDI: PID:C1111-8PWE,SN:FGL2149XXXX
Return code: CCKUTq-Qg2Ytw-ZhSLq5-bDFw7e-VvWgf2-QwwBed-3MaRcT-fFfGcn-X6e <<<< Copy the string
```

Remove Reservation

Navigate to **Product Instances > Actions > Remove.** Paste the return code just copied from the router and click **Remove Reservation.**

Remove Reservation

To remove a Product Instance that has reserved licenses and make those licenses once again available to other Product Instances, enter in the Reservation Return Code generated by the Product Instance. If you cannot generate a Reservation Return Code, contact Cisco Support

* Reservation Return Code:

CCKUTq-Qg2Ytw-ZhSLq5-bDFw7e-VvWgf2-QwwBed-3MaRcT-fFfGcn-X6e

Remove Reservation   Cancel

The **License reservation removed successfully** notification shows up right after. Again, navigate to **Actions > Remove > Remove Instance.**

Verify

Use this section to confirm that your configuration works properly.

Useful Commands

The verification procedure is described in each step for the online or offline methods.

```
show license tech support
show license status
show license authorization
show license summary
show license history message
show license eventlog <DAYS>
license smart clear event log
license smart sync local
license smart factory reset
```

Troubleshoot

This section provides information you can use to troubleshoot your configuration.

Smart Licensing Using Policy relies on secure bidirectional communication between the cEdge and the CSSM over the Internet, in order to exchange acknowledgements and handshakes which favor the registration and license fetch.

There are common scenarios that do not permit messages to be exchanged correctly between devices.

Common Issues

DNS Resolution Does Not Work

In order to reach smartreceiver.com the cEdge must be able to resolve a domain name, otherwise, the URL is not translated to a routable IP and the communication fails. This error normally shows up after the trust establishment attempt.

```
*Aug 18 20:45:10.345: %SMART_LIC-3-COMM_FAILED: Communications failure with the Cisco Smart
License Utility (CSLU) : Unable to resolve server hostname/domain name
```
Ensure there is IP connectivity to the Internet.

```
ping 8.8.8.8
```
Ping a URL to verify whether DNS works or not if Internet Control Message Protocol (ICMP) is blocked by an external device with the use of telnet to a URL instead.

```
ping cisco.com
telnet cisco.com 80
```
If the test fails, configure a DNS Server and enable DNS resolution.

```
ip domain lookup
ip name-server 8.8.8.8
```
If it is not possible to configure an external DNS server, configure local DNS Resolution in the router.

```
cEdge# config-transaction
cEdge(config)# ip host smartreceiver.com A.B.C.D
cEdge(config)# commit
```

> **Note**: If you need to know which IPs respond to smartreceiver.com, run a **nslookup <URL>** command from a Windows or Linux Machine.

> **Note**: Local DNS resolution is not recommended since the responder IPs can change over time and Cisco does not notify about the change.

Common error message is seen in Smart Licensing (SL) eventlog**.**

```
cEdge# show license eventlog 0
**** Event Log ****

2022-08-18 20:45:10.345 UTC SAEVT_COMM_FAIL error="Unable to resolve server hostname/domain
name"
2022-08-18 20:45:57.804 UTC SAEVT_COMM_FAIL error="Unable to resolve server hostname/domain
name"

cEdge# show logging | include SMART
*Aug 18 20:59:44.914: %SMART_LIC-3-COMM_FAILED: Communications failure with the Cisco Smart
Software Manager (CSSM) : No detailed information given
```

SD-WAN Tunnel Blocks DNS

A similar issue happens if the implicit ACL in the SD-WAN Tunnel blocks incoming DNS responses.

```
cEdge# show license eventlog 0
**** Event Log ****
2022-08-18 20:45:10.345 UTC SAEVT_COMM_FAIL error="Unable to resolve server hostname/domain
name"
2022-08-18 20:45:57.804 UTC SAEVT_COMM_FAIL error="Unable to resolve server hostname/domain
name"
```

```
cEdge# show logging | include SMART
*Aug 18 20:59:44.914: %SMART_LIC-3-COMM_FAILED: Communications failure with the Cisco Smart
Software Manager (CSSM) : No detailed information given
```

Ensure that at the registration time, DNS service is permitted.

```
cEdge# show sdwan running-config sdwan
sdwan
interface GigabitEthernet0/0/0
tunnel-interface
encapsulation gre
encapsulation ipsec weight 1
no border
color public-internet
no last-resort-circuit
no low-bandwidth-link
no vbond-as-stun-server
vmanage-connection-preference 5
port-hop
carrier default
nat-refresh-interval 5
hello-interval 1000
no allow-service all
no allow-service bgp
allow-service dhcp
allow-service dns <<<<<<<<<<<<<<<<<< MUST be allowed
allow-service icmp
allow-service sshd
allow-service netconf
no allow-service ntp
no allow-service ospf
no allow-service stun
no allow-service https
no allow-service snmp
no allow-service bfd
exit
```

Transport URL is Not Correct

For greenfield (fresh) installations, the default transport type is Cisco Smart Licensing Utility (CSLU).

```
cEdge# show license tech support | include Smart Licensing Status
Smart Licensing Tech Support info

Smart Licensing Status
```

```
======================
```

Smart Licensing is ENABLED

License Conversion:
Automatic Conversion Enabled: True
Status: Not started

Export Authorization Key:
Features Authorized:
<none>

Utility:
Status: DISABLED

Smart Licensing Using Policy:
Status: ENABLED

Data Privacy:
Sending Hostname: yes
Callhome hostname privacy: DISABLED
Smart Licensing hostname privacy: DISABLED
Version privacy: DISABLED

Transport:
Type: cslu   <<<<<<<<<<<<<<<<<<
Cslu address: <empty>
Proxy:
Address: <empty>
Port: <empty>
Username: <empty>
Password: <empty>
Server Identity Check: False

Common errors in logs.

```
cEdge# show license eventlog 0
**** Event Log ****
2022-08-18 20:45:10.345 UTC SAEVT_COMM_FAIL error="Unable to resolve server hostname/domain
name"
2022-08-18 20:45:57.804 UTC SAEVT_COMM_FAIL error="Unable to resolve server hostname/domain
name"

cEdge# show logging | include SMART
*Aug 18 20:59:44.914: %SMART_LIC-3-COMM_FAILED: Communications failure with the Cisco Smart
Software Manager (CSSM) : No detailed info
```

> **Note**: CSLU is not supported in Cisco SD-WAN (Cisco vManage) and CSLU cannot be used to report license usage for routing product instances that are managed by Cisco vManage. For more information navigate to [Cisco Smart License Utility (CSLU).](#)

Manually configure the default URL and transport type for the smart agent and try the trust established with the token again.

```
cEdge# configure terminal
cEdge(config)# license smart transport smart
cEdge(config)# license smart url default
cEdge(config)# commit
```

SD-WAN Tunnel Blocks HTTPS

Smart Licensing communication is based on Hypertext Transfer Protocol Secure (HTTPS) port 443, thus, if the SD-WAN tunnel blocks incoming HTTPS responses, the registration, authorization request and RUM reports notification fail.

The common error in log and eventlog.

```
*Aug 18 20:59:44.914: %SMART_LIC-3-COMM_FAILED: Communications failure with the Cisco Smart
Software Manager (CSSM) : No detailed information given
```

Ensure the HTTPS service is allowed in the SD-WAN Tunnel at registration time. If not, allow it and try the Trust Establishment with the token again.

```
cEdge# show sdwan runnning-config sdwan
sdwan
interface GigabitEthernet0/0/0
tunnel-interface
encapsulation gre
encapsulation ipsec weight 1
no border
color public-internet
no last-resort-circuit
no low-bandwidth-link
no vbond-as-stun-server
vmanage-connection-preference 5
port-hop
carrier default
nat-refresh-interval 5
hello-interval 1000
no allow-service all
no allow-service bgp
allow-service dhcp
allow-service dns
allow-service icmp
allow-service sshd
allow-service netconf
no allow-service ntp
no allow-service ospf
no allow-service stun
allow-service https  <<<<<<<<<<<<<<<<<< MUST be allowed
no allow-service snmp
no allow-service bfd
exit
```

External Firewall Blocks CSSM URL, IPs, Or Port 443

If the site architecture uses a firewall to control traffic, ensure port 443 to smartreceiver.cisco.com is not blocked. Contact your firewall team or Internet Service Provider (ISP) to further verify.

From the router.

```
cEdge# telnet smartreceiver.com 443
Trying smartreceiver.com (X.X.X.X, 443)...Open
```

From a Service VRF host.

```
ericgar@cisco$ telnet smartreceiver.cisco.com 443
Trying X.X.X.X...
```

```
Connected to smartreceiver.cisco.com.
Escape character is '^]'.
```

Multiple Interfaces to the Internet

In some scenarios where there is more than one interface, the communication with CSSM fails;
the HTTP source interface can be changed to any available in the router.

```
cEdge# config-transaction
cEdge(config)# ip http client source-interface INTERFACE
cEdge(config)# commit
```

Related Information

- [Smart Licensing Using Policy for Cisco Enterprise Routing Platforms](#)
- [Cisco Smart Licensing and Smart Accounts FAQ](#)
- [Manage Licenses for Smart Licensing Using Policy SDWAN](#)
- [Technical Support & Documentation - Cisco Systems](#)