Configure HSEC License on SD-WAN XE Edge Router

Contents

- Introduction
- Prerequisites
  - Requirements
  - Components Used
- Background Information
  - Concepts
  - Throughput Behavior
  - License Availability Verification
  - Router Operation Mode
- Configure
  - Online Method to Cisco License Central
    - Configure Transport Type and Set Default Cisco License Central URL
    - Generate a Product Instance Registration Token
    - Generate a Trust Establishment between the Edge Router and Cisco License Central
    - Verify the Trust Establishment SuccessCounter
    - Request Authorization
    - Verify the Activation is Successful
  - Offline Method to Cisco License Central
    - Generate a Local License Reservation
    - Get the Edge Router UDI Information
    - Fill the Edge Router UDI in the Reservation Form
    - Select the Number of Licenses to Reserve
    - Select the License Device Type
    - Generate the Authorization Code
    - Download the SLAC
    - Copy the SLAC to the Edge Router
    - Install the SLAC
    - Verify the Installation is Successful
- vManage Workflows Method
  - Online Workflow
    - Sync Licenses with Cisco License Central
    - Install Fetched Licenses
  - Offline Workflow
    - Sync Licenses with Cisco License Central
    - Install Fetched Licenses
- Return the HSECK9 License
  - Return Code Behavior
  - Generate the Return Code
  - Remove the Reservation
- Activation - Is Reload Required?
  - Is it True that on 8500-based Platforms a Reload is Required for HSEC to be Activated?

Is a Reload Needed for C8000v Post Activation of HSEC?
Is a Reload for CSR1000v Post Activation of HSEC?
Is the Reload Behavior the Same for SD-WAN and non-SD-WAN Modes?
Is it Also True for the Deactivation of HSEC License?
License Availability Verification
Verify
Useful Commands
Troubleshoot
Common Issues
DNS Resolution does not Work
SD-WAN Tunnel Blocks DNS
Transport URL is Not Correct
SD-WAN Tunnel Blocks HTTPS
External Firewall Blocks Cisco License Central URL, IPs, or Port 443
Multiple Interfaces to the Internet
Related Information

Introduction

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

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:

- Cisco Edge Router C1111-8PWE version 17.6.3
- Cisco Edge Router c8000v 17.12.3
- Cisco License Central
- Cisco vManage 20.12.3.1

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.

Note: The HSECK9 license installation processes described in this document apply equally to physical and virtual routers. There is no platform-specific installation process.

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.

Note: As of 20.9.2 and 17.9.2a, HSEC licenses are capable of management directly from vManage. More details are here:
Cisco Catalyst SD-WAN Getting Started Guide - Manage HSEC Licenses [Cisco SD-WAN] - Cisco

---

Note: To activate the HSECK9 license in the router after the installation, a manual reload is required for all physical routers except the virtual router C8000v.

License Availability Verification

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

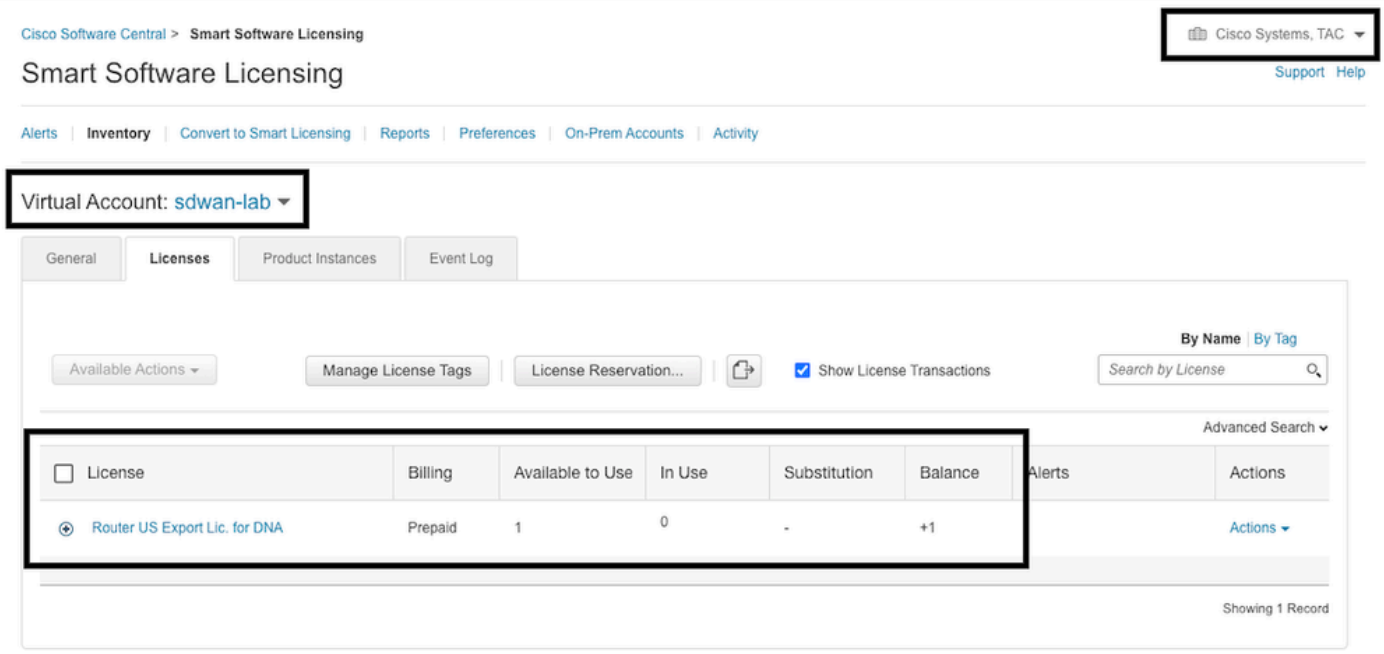
Step 2. Click **Cisco License Central**.

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.



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 Cisco 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.

<#root>

```
show platform software device-mode
```

```
show version | include mode
```

Example:

```
<#root>

EdgeRouter#

show platform software device-mode


Device Operating-mode: Controller-Managed
Device-mode bootup status:
8/03 00:44:16 System is green
Bootup Success

EdgeRouter#

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 Cisco License Central

Configure Transport Type and Set Default Cisco License Central URL

Step 1. Configure the correct Transport Type and URL.

```
<#root>

EdgeRouter#

config-transaction


EdgeRouter(config)#

license smart transport smart
```

```
EdgeRouter(config)#

license smart url default


EdgeRouter(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.

<#root>

```
EdgeRouter#

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 smartrece

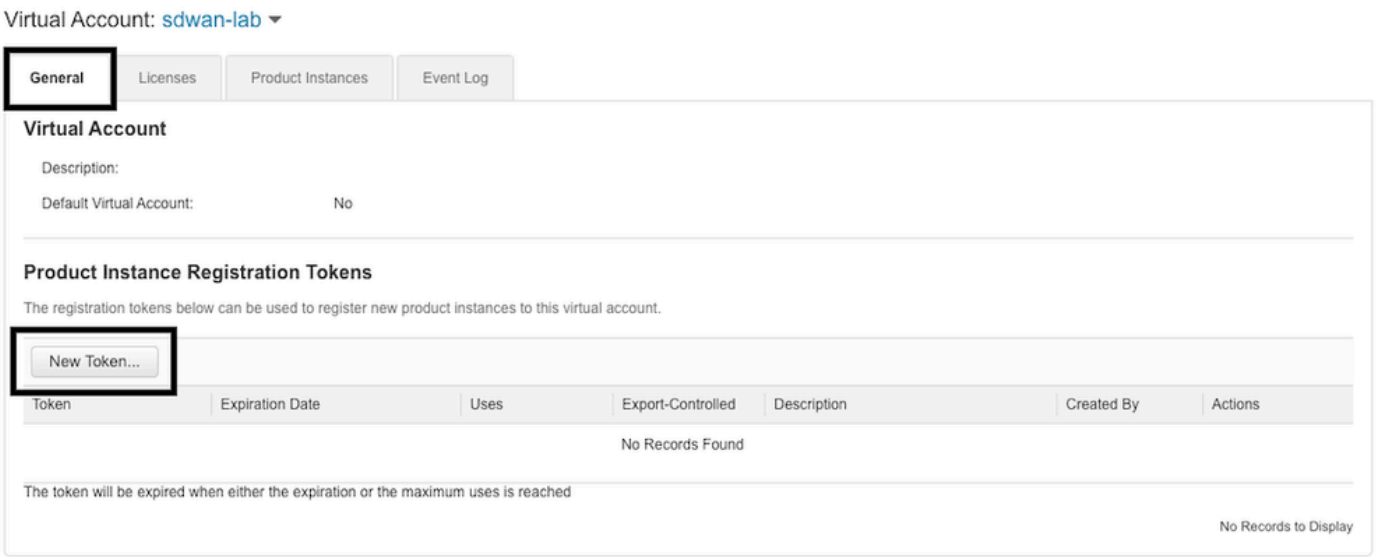

Proxy:
Address: <empty>
Port: <empty>
Username: <empty>
Password: <empty>
Server Identity Check: True
```

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

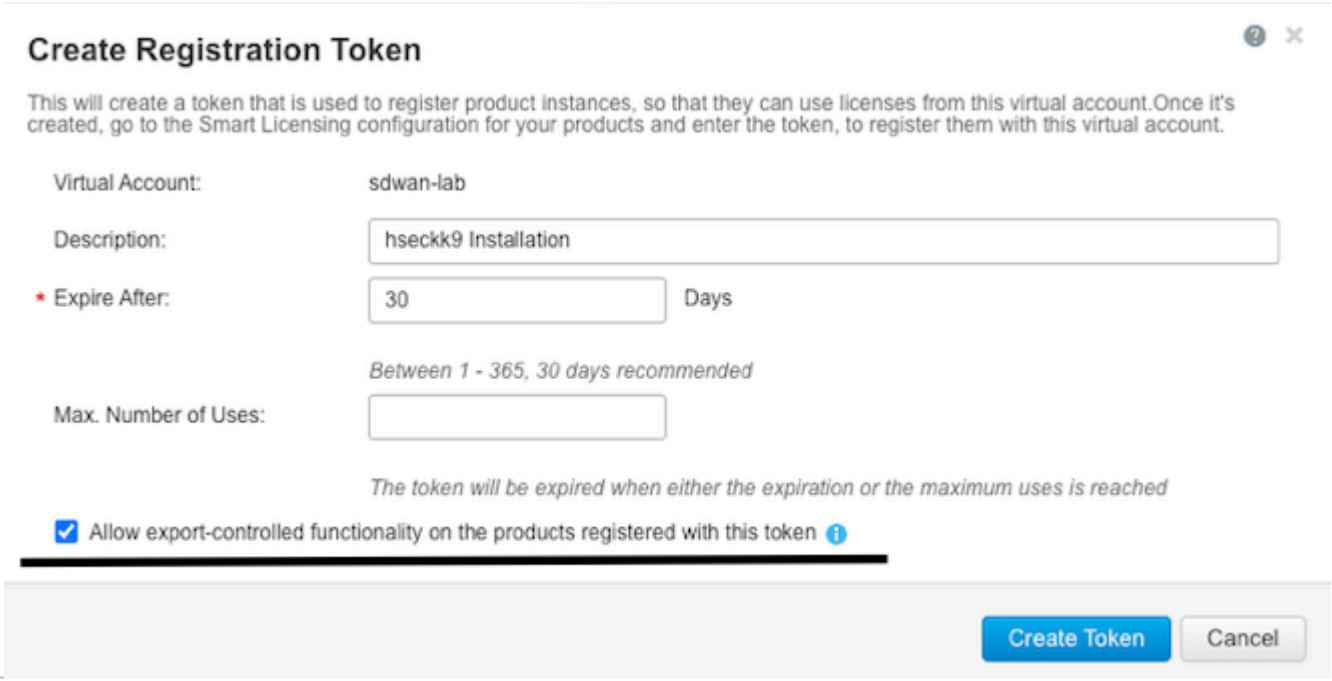
Generate a Product Instance Registration Token

Step 1. Generate a New Token.

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



Step 2. Fill up the new token information.



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.

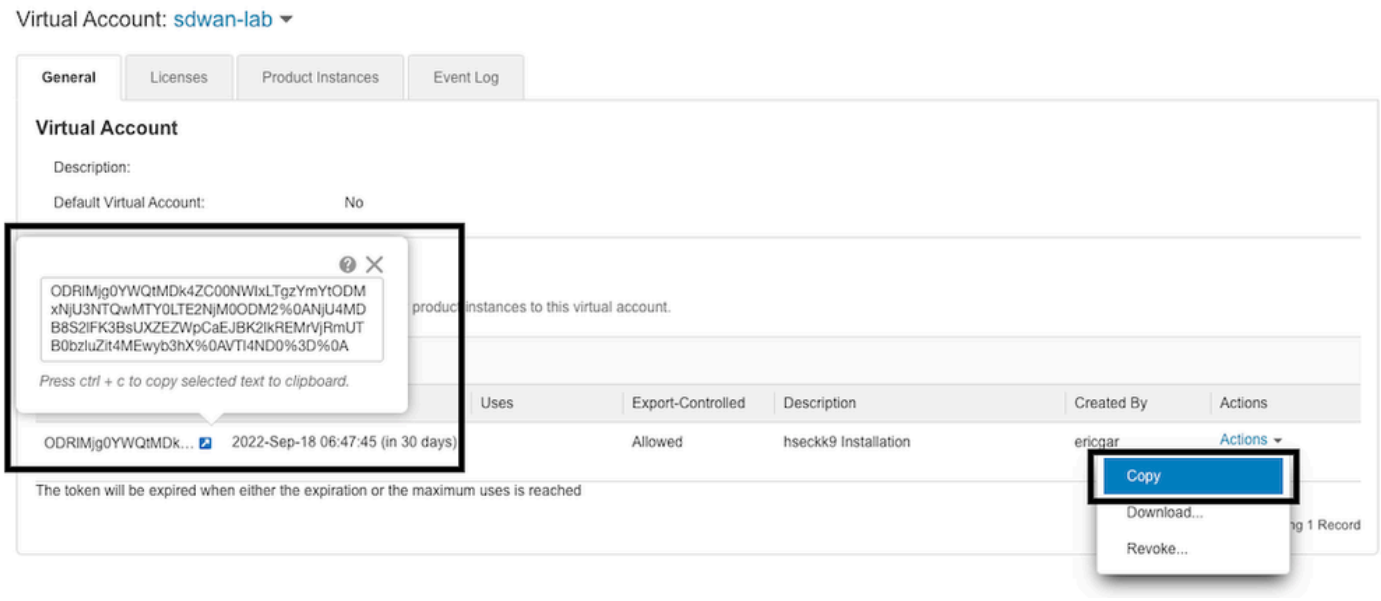
Ensure the **Allow export-controlled** the option is checked. Otherwise, the license registration fails and then click **Create Token**.

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 Edge Router and Cisco License Central

In order to provide authorization to use an export-controlled license, the Edge Router must establish trust with [Cisco License Central](). For the handshake, the Edge Router uses the token generated on Cisco License Central in the previous step.

<#root>

license smart trust idtoken TOKEN local force

Example:

<#root>

EdgeRouter#

license smart trust idtoken ZThjOTlmM2UtMjQ2ZC00YjI1LTgwNjctZGIxZjIzYjZiYmVmLTE2NjM0NjI1%0AMjgyNTh8YWNVe

Right after the trust is established, the logs show communication with Cisco License Central.

<#root>

```
EdgeRouter#
```

```
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
*Aug 18 21:03:46.146: %CRYPTO_ENGINE-5-KEY_ADDITION: A key named SLA-KeyPair2 has been generated or imp
*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 (CSS
*Aug 18 21:03:56.347: %SMART_LIC-6-TRUST_INSTALL_SUCCESS: A new licensing trust code was successfully i
```

Verify the Trust Establishment Success Counter

Verify that the trust establishment success counter increases. This means the licensing agent can reach Cisco License Central.

<#root>

```
EdgeRouter#
```

```
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 Cisco License Central license usage. To fetch the license, run the

authorization request.

```
<#root>

EdgeRouter#

 license smart authorization request add hseck9 local
```

Logs:

```
<#root>

EdgeRouter#

show logging | include SMART


*Aug 18 21:11:41.553: %SMART_LIC-6-AUTHORIZATION_INSTALL_SUCCESS: A new licensing authorization code wa
*Aug 18 21:11:41.641: %SMART_LIC-6-EXPORT_CONTROLLED: Usage of export controlled features is allowed fo
```

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

```
<#root>

EdgeRouter#

show lic eventlog 0


**** Event Log ****
2022-08-18 21:11:41.538 UTC SAEVT_RESERVE_INSTALL_START udi="PID:C1111-8PWE,SN:FGL2149XXXX" authorizati
2022-08-18 21:11:41.552 UTC SAEVT_TAG_EXPORT exportAllowed="False" count="0" entitlementTag="regid.2019
2022-08-18 21:11:41.576 UTC SAEVT_TAG_EXPORT exportAllowed="True" count="0" entitlementTag="regid.2019-
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_
2022-08-18 21:11:41.641 UTC SAEVT_TAG_EXPORT exportAllowed="True" count="1" entitlementTag="regid.2019-
2022-08-18 21:12:06.119 UTC SAEVT_RESERVE_INSTALL_START udi="PID:C1111-8PWE,SN:FGL2149XXXX" authorizati
```

Verify the Activation is Successful

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

<#root>

show license tech support | begin License Usage

show license authorization

show license summary

show license usage

Example:

<#root>

```
EdgeRouter#

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

EdgeRouter#
```

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   <<<<<<<<<<

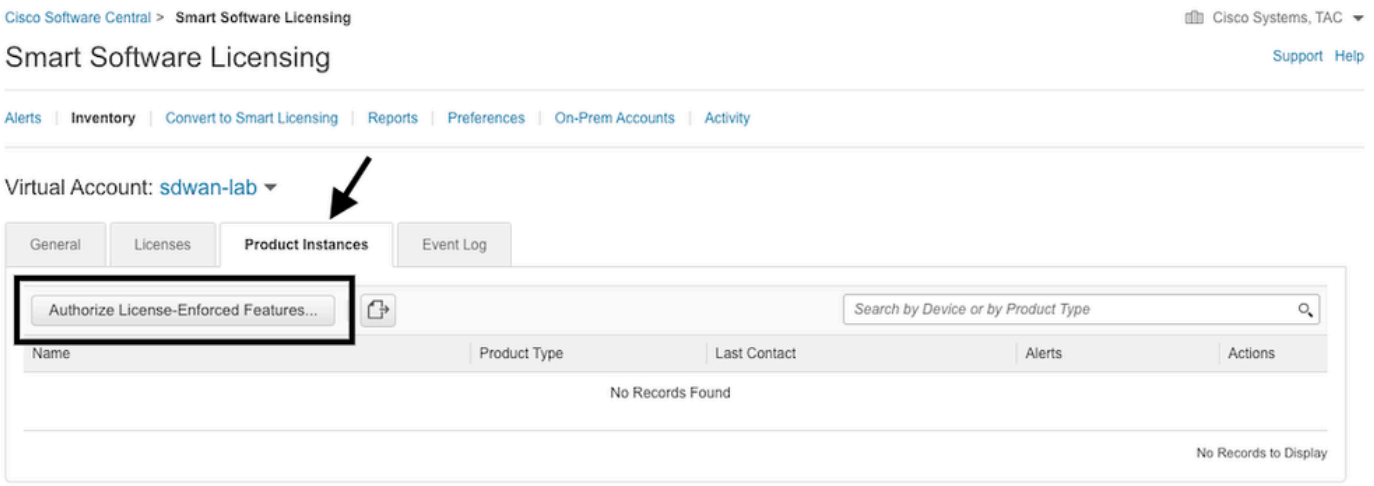
Offline Method to Cisco License Central

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 Cisco License Central.

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 Edge Router UDI Information

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

<#root>

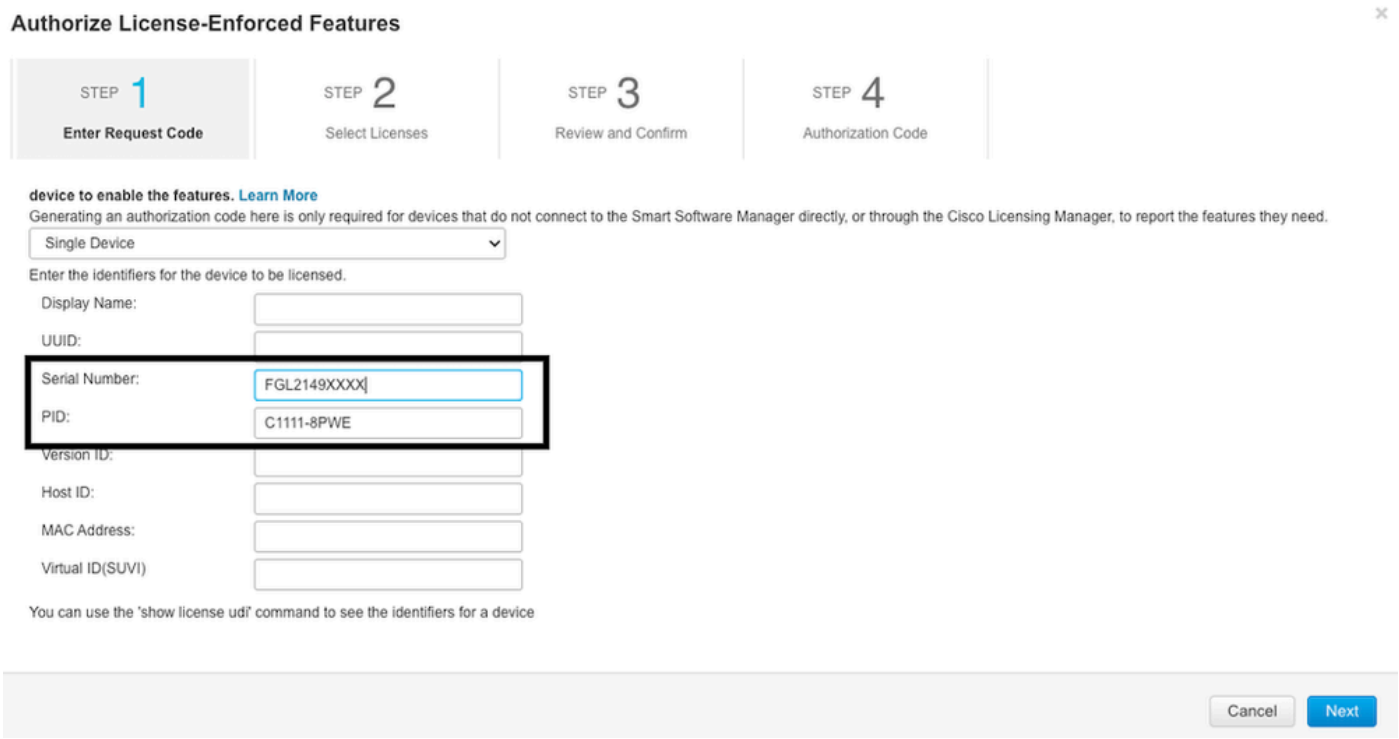
```
EdgeRouter#
```

```
show license udi
```

```
UDI: PID:C1111-8PWE,SN:FGL2149XXXX
```

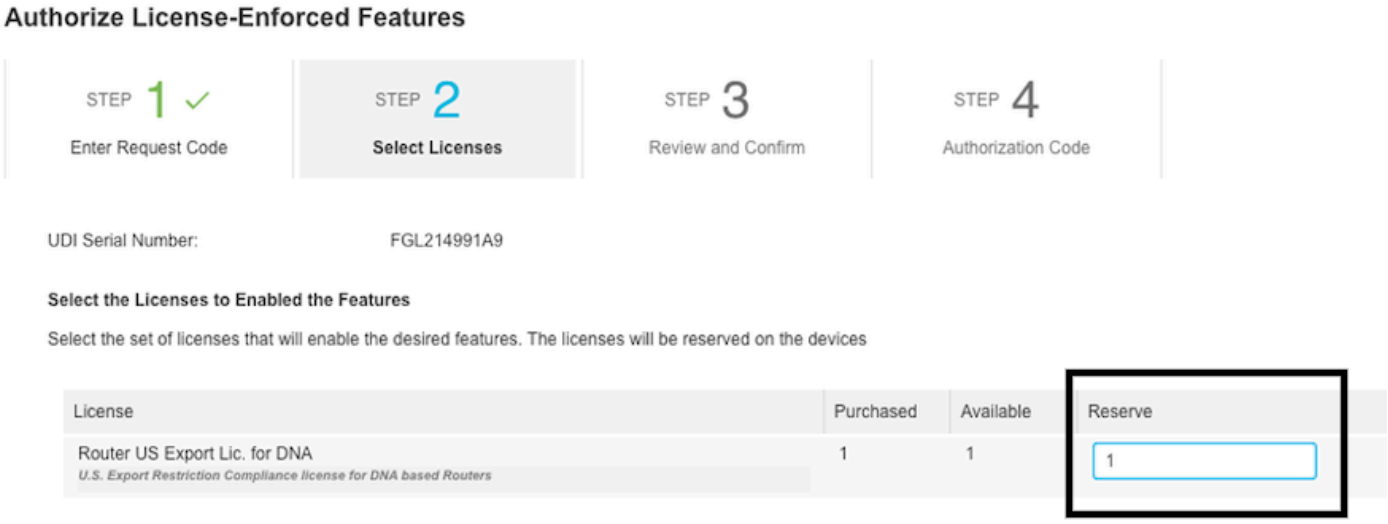
Fill the Edge Router UDI in the Reservation Form

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



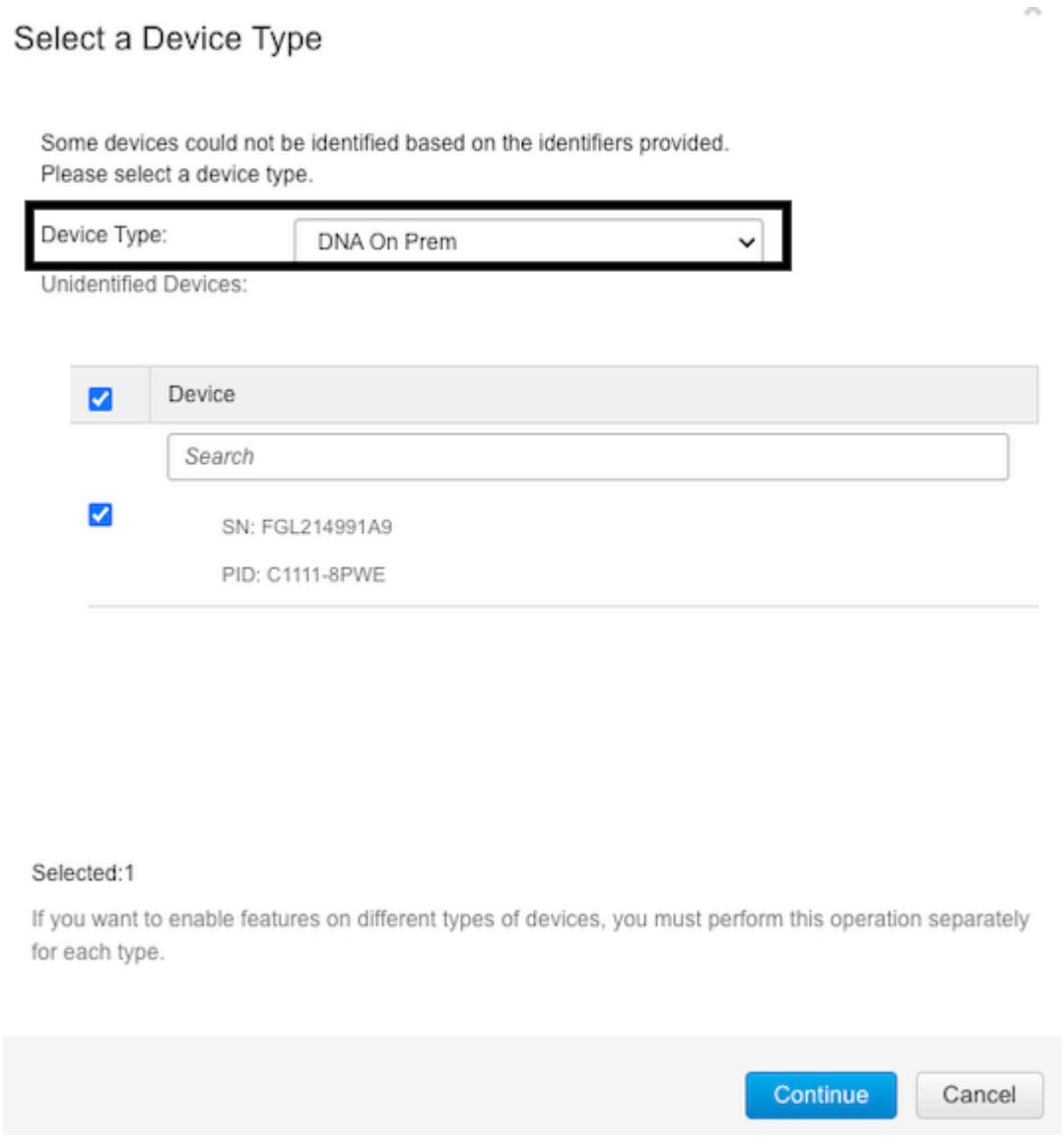
Select the Number of Licenses to Reserve

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.



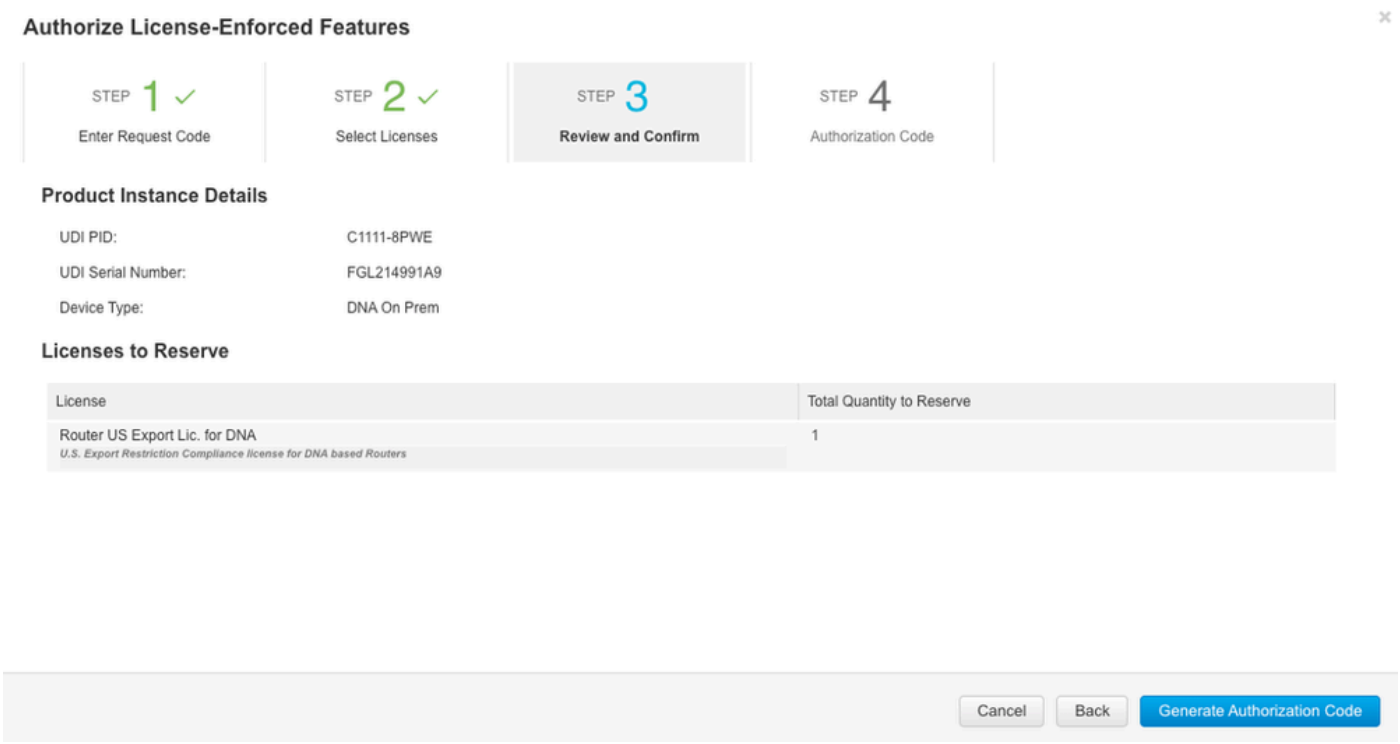
Select the License Device Type

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



Generate the Authorization Code

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



Download the SLAC

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

Copy the SLAC to the Edge Router

There are three options to copy the SLAC file to the Edge Router.

- With a USB Drive.

<#root>

```
EdgeRouter#
```

```
show file systems | include usb|Size
```

```
Size(b)       Free(b)  Type Flags Prefixes
```

```
15598043136 15596658688 disk  rw     usb0:
```

```
EdgeRouter#
```

```
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)

EdgeRouter#
```

```
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 Edge Router 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.

<#root>

```
EdgeRouter#
```

```
license smart import bootflash:AuthorizationCode_SN_FGL2149XXXX.txt
```

```
Import Data Successful
Last Confirmation code UDI: PID:C1111-8PWE,SN:FGL2149XXXX
Confirmation code: aaa6b57e
```

Logs.

<#root>

```
EdgeRouter#
```

show logging | include SMART

```
*Aug 19 05:42:45.309: %SMART_LIC-6-AUTHORIZATION_INSTALL_SUCCESS: A new licensing authorization code wa
*Aug 19 05:42:45.362: %SMART_LIC-6-EXPORT_CONTROLLED: Usage of export controlled features is allowed fo

EdgeRouter#
```

show license eventlog 0

```
**** Event Log ****

2022-08-19 05:42:45.293 UTC SAEVT_RESERVE_INSTALL_START udi="PID:C1111-8PWE,SN:FGL2149XXXX" authorizati
2022-08-19 05:42:45.308 UTC SAEVT_TAG_EXPORT exportAllowed="False" count="0" entitlementTag="regid.2019
2022-08-19 05:42:45.333 UTC SAEVT_TAG_EXPORT exportAllowed="True" count="0" entitlementTag="regid.2019-
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_
2022-08-19 05:42:45.362 UTC SAEVT_TAG_EXPORT exportAllowed="True" count="1" entitlementTag="regid.2019-
```

Verify the Installation is Successful

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

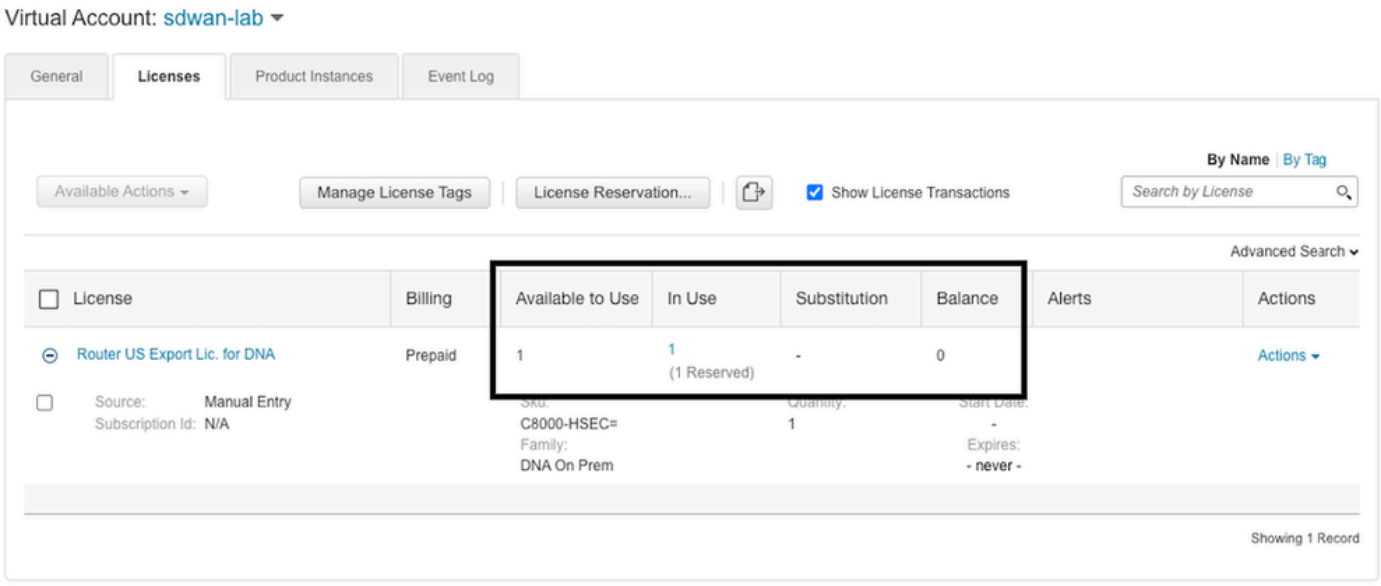
<#root>

show license authorization

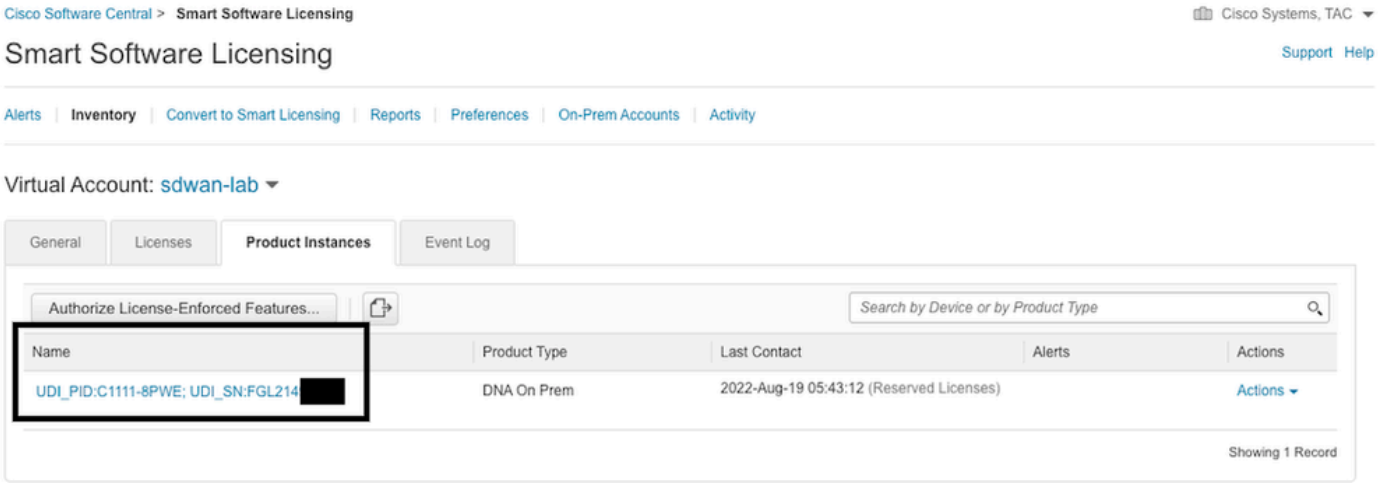
show license summary

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 Edge Router is shown. click the entry to get more information about the license characteristics.



vManage Workflows Method

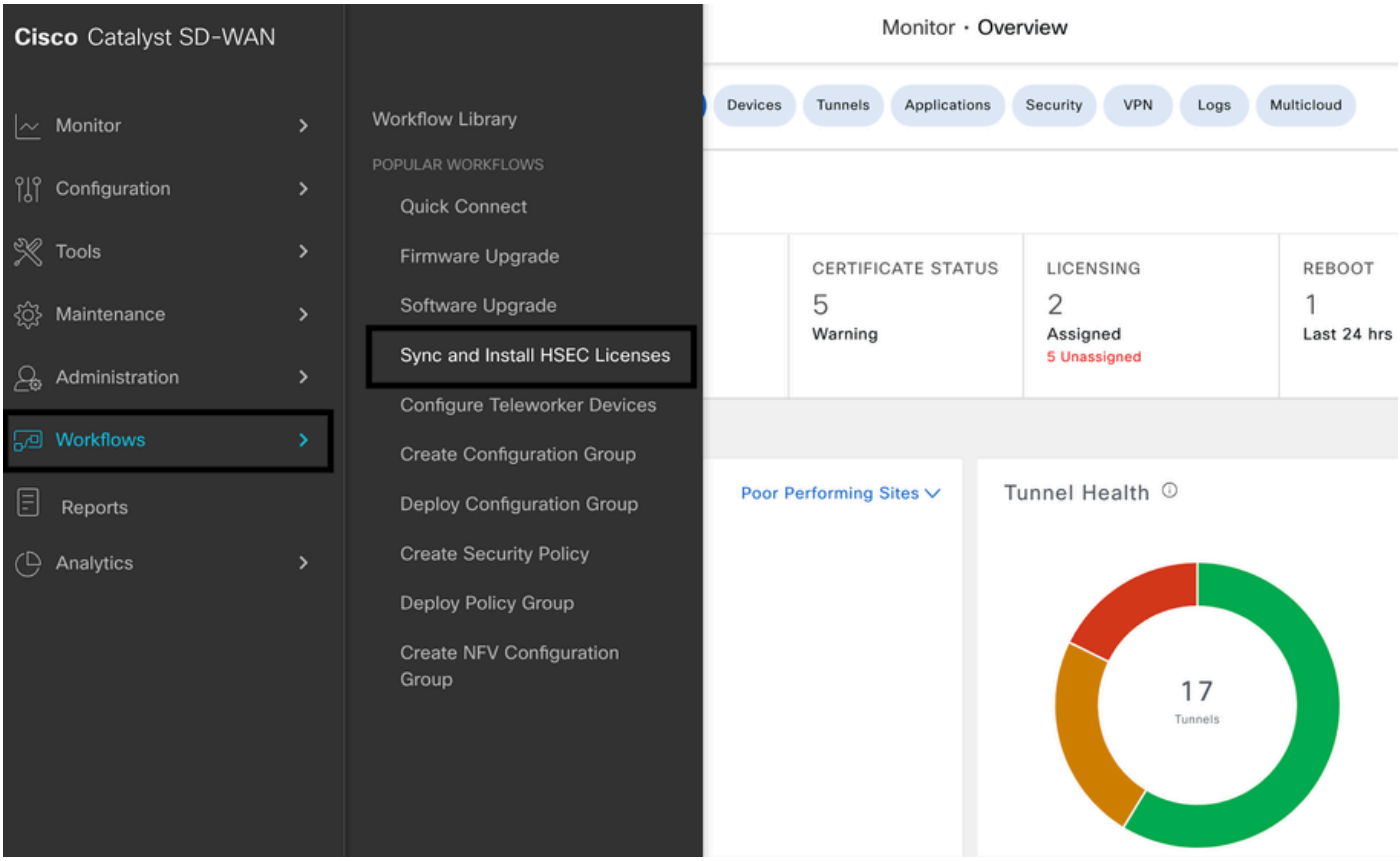
From 20.9.2 onwards, vManage enables the ability to install an HSECK9 license with the help of Workflows.

Note: This method only works with *Router US Export Lic. for DNA* licenses; device specific HSEC licenses such as *ISR4300_HSEC* or *ISR4400_HSEC* no longer work. For more information on how to convert a Device Specific HSEC license to Cisco DNA HSEC visit Restrictions for Managing HSEC Licenses section.

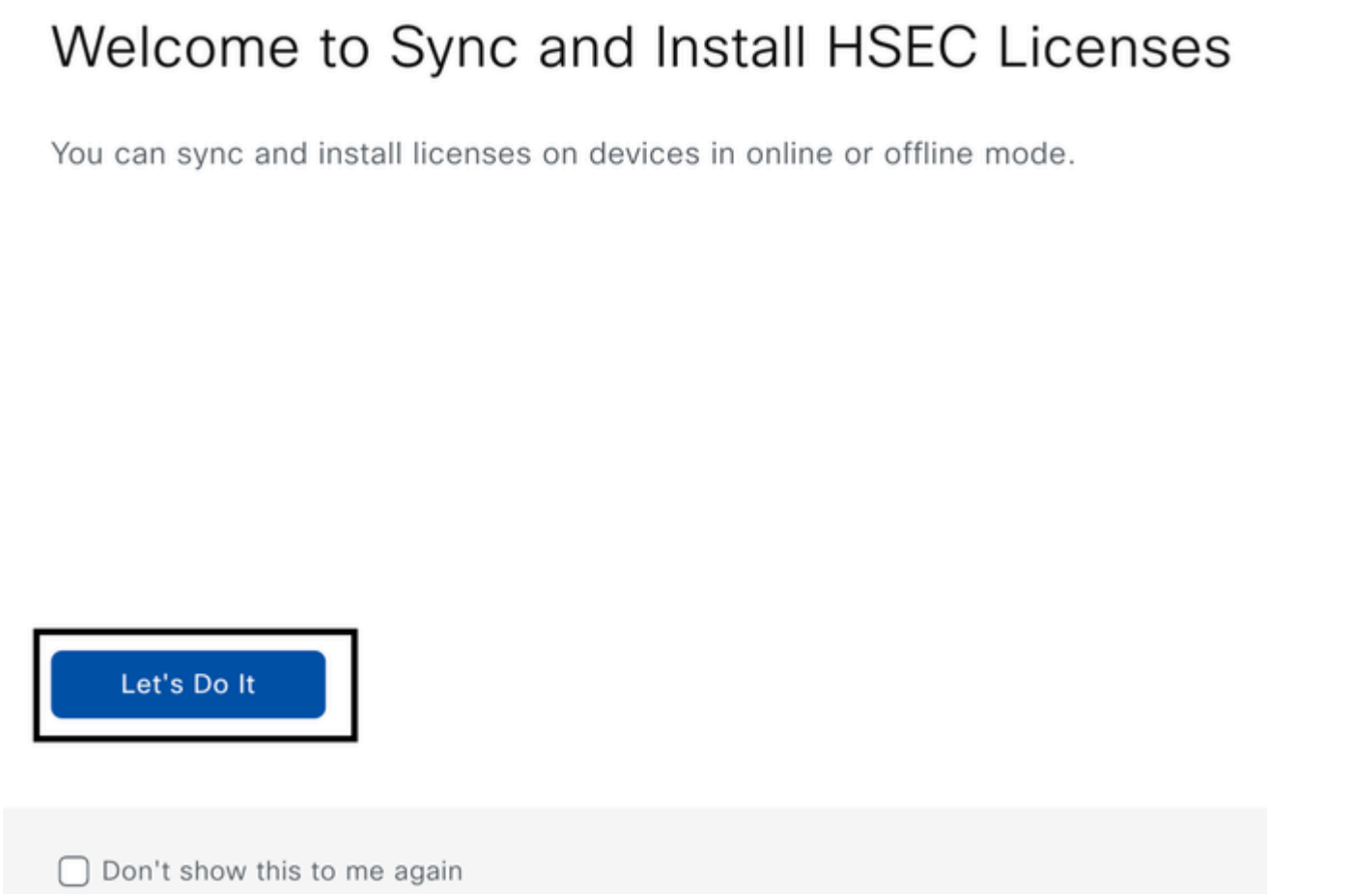
Online Workflow

Sync Licenses with Cisco License Central

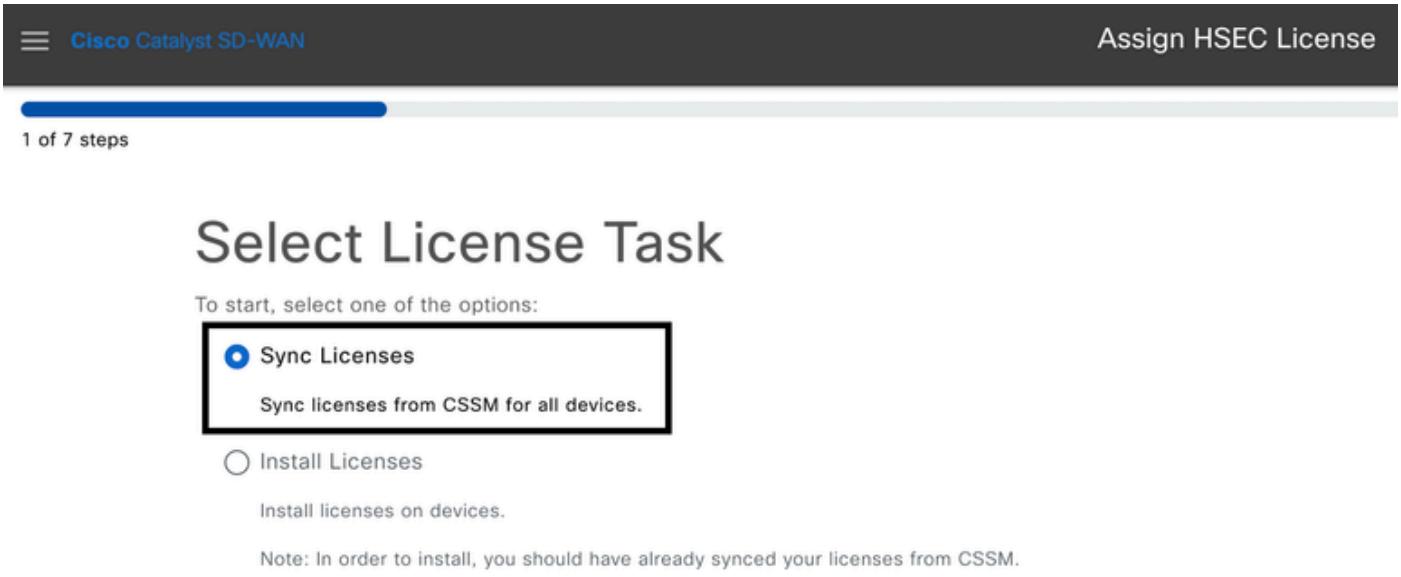
1.- In vMange GUI navigate to **Main Menu > Workflows > Sync and Install HSEC Licenses.**



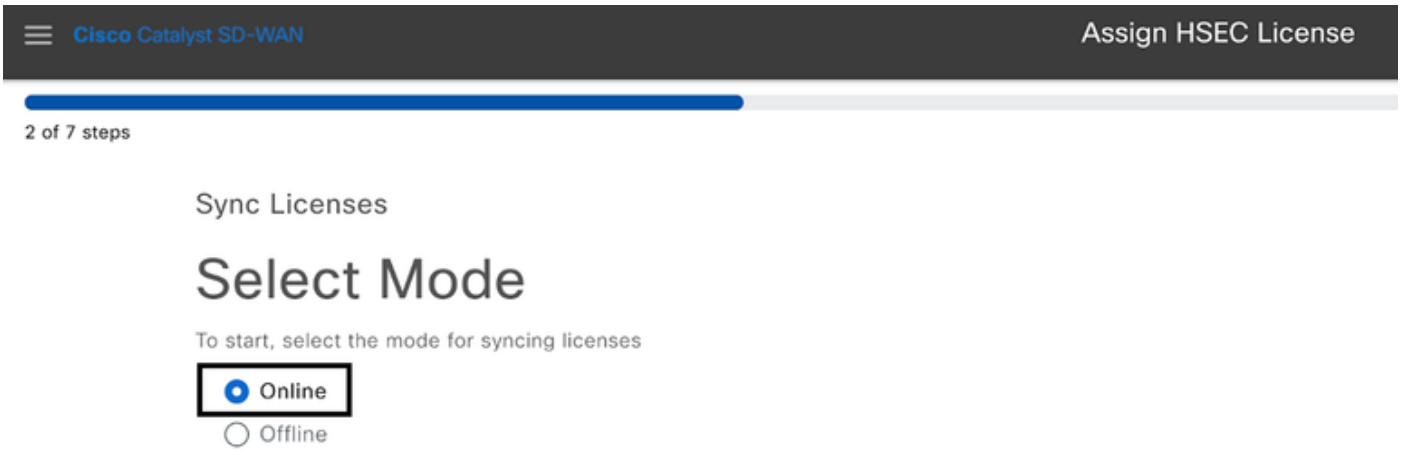
2.- Click **Let's Do it** button on the pop-up window.



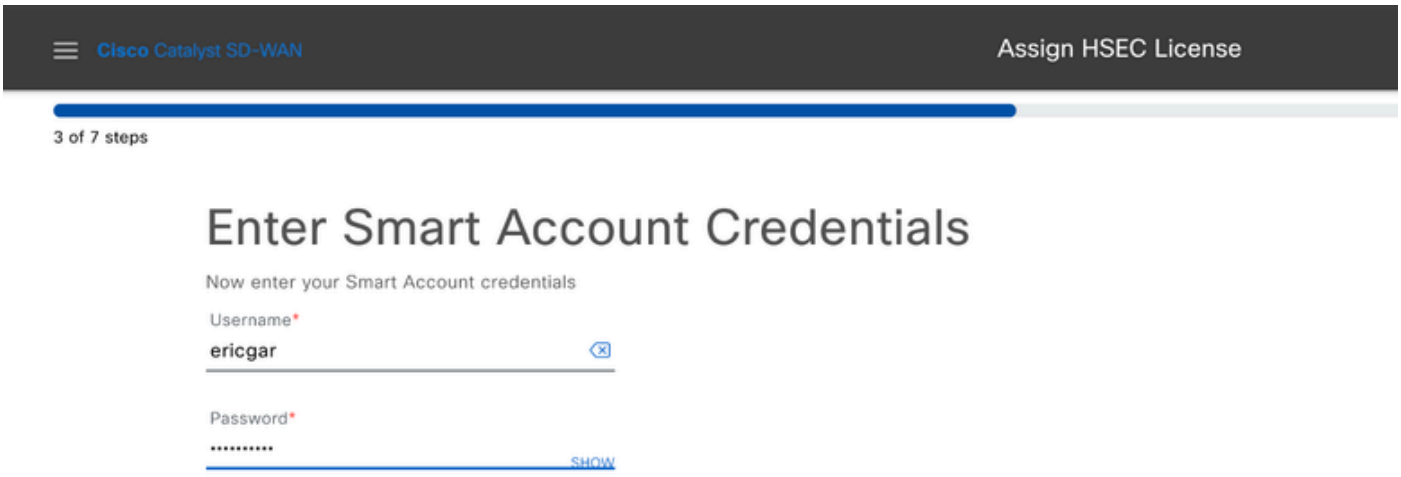
3.- Select **Sync Licenses** task and click **Next**.



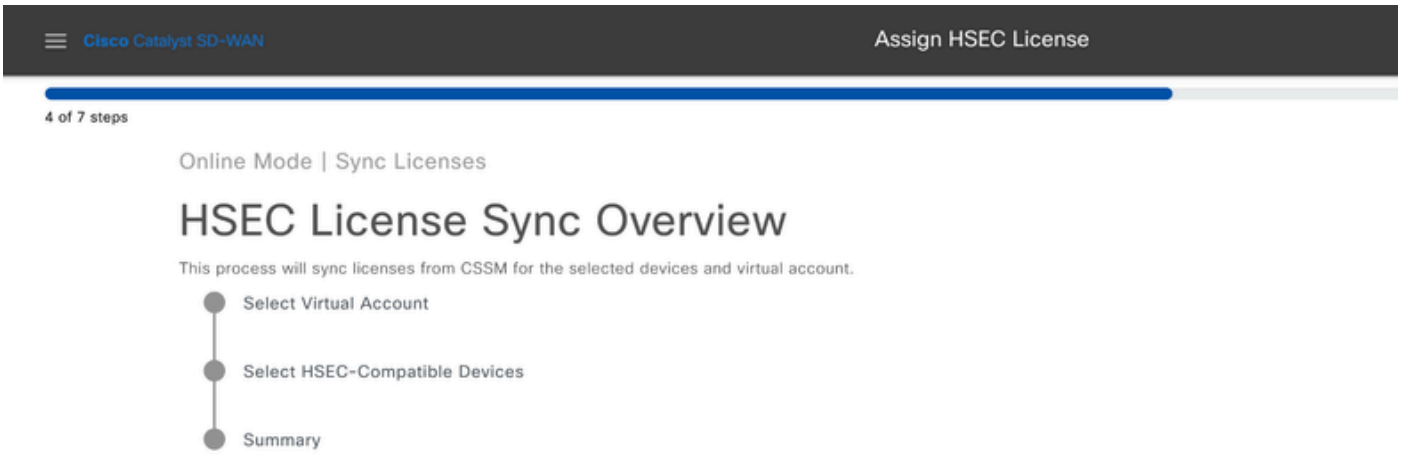
4.- Select **Online** mode and click **Next**.



5- Enter your Cisco License Central credentials and click **Next**.

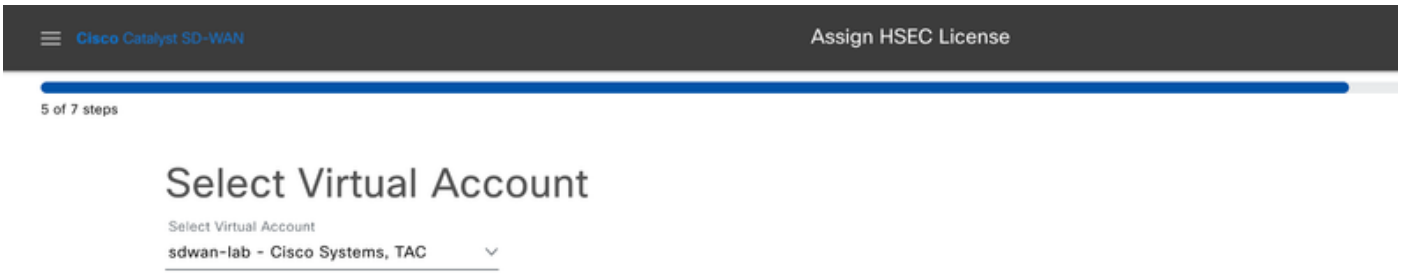


6.- Verify the HSEC License Sync Overview and click **Next**.



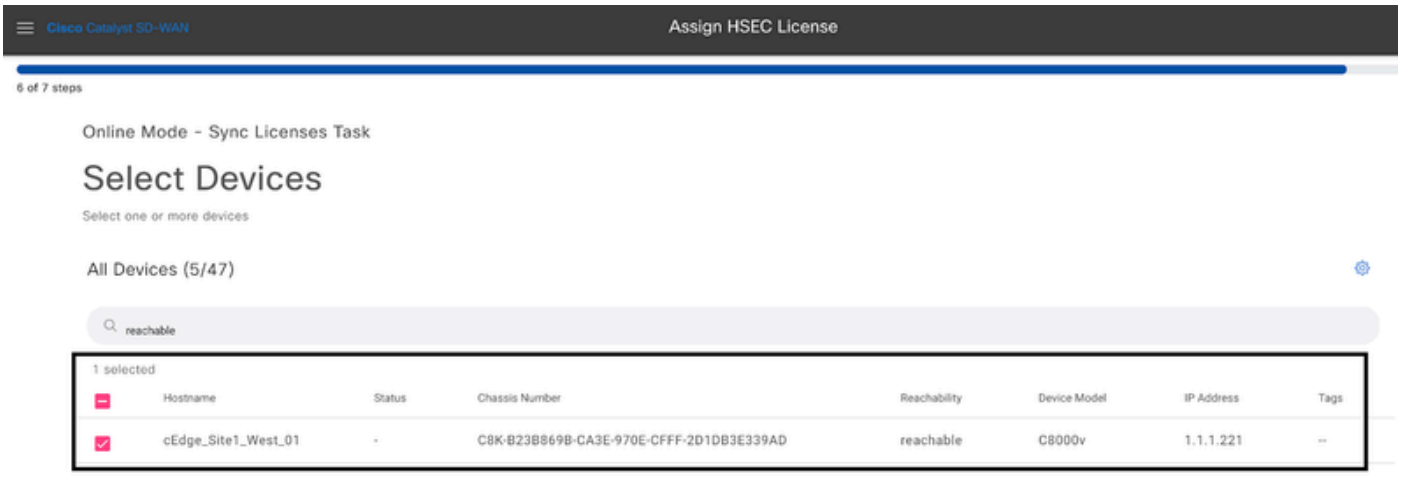
7.- vManage connects to the cloud and queries all available Virtual Accounts. Select in the dropdown the Virtual Account that contains a valid and positive count HSEC license.

Note: The credentials entered in step 6 must have an administrator role in the Smart Account and Virtual Account where the HSEC licenses are deposited in.

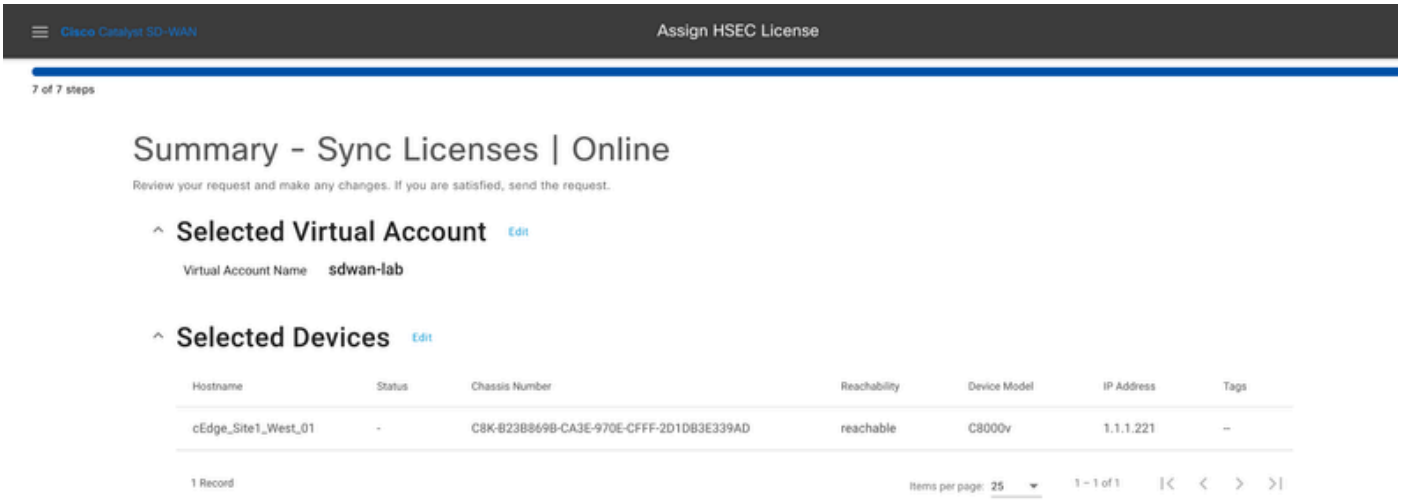


8.- Select the device in which the HSEC license is targeted to be installed.

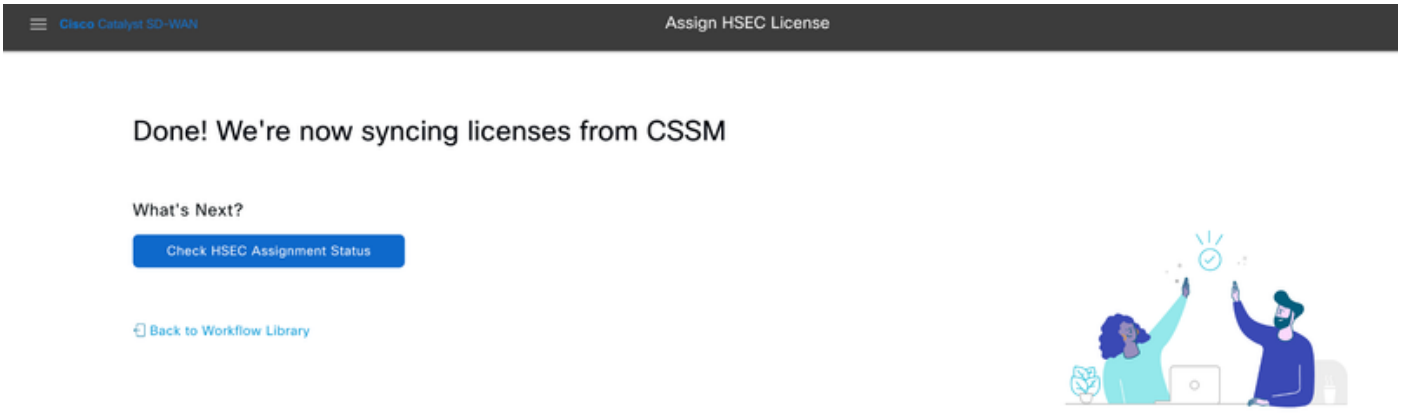
Note: Only devices compatible with HSEC are displayed.



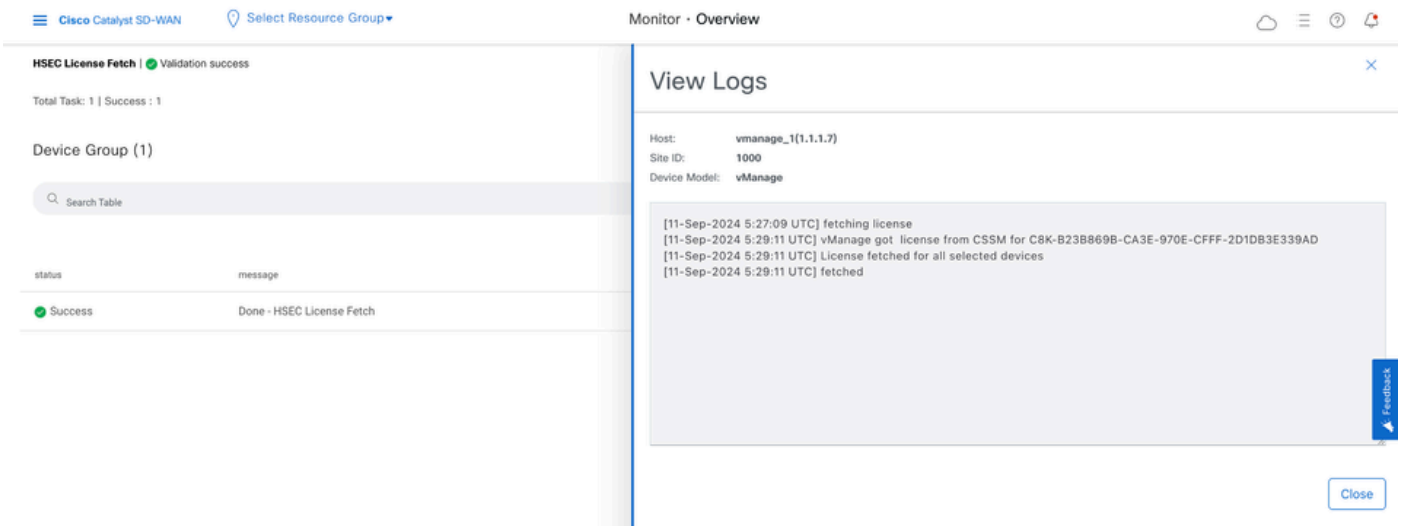
9.- Review and verify the request summary and click **Sync**.



10.- Click **Check HSEC Assignment Status** to verify the SLAC reservation in real time.

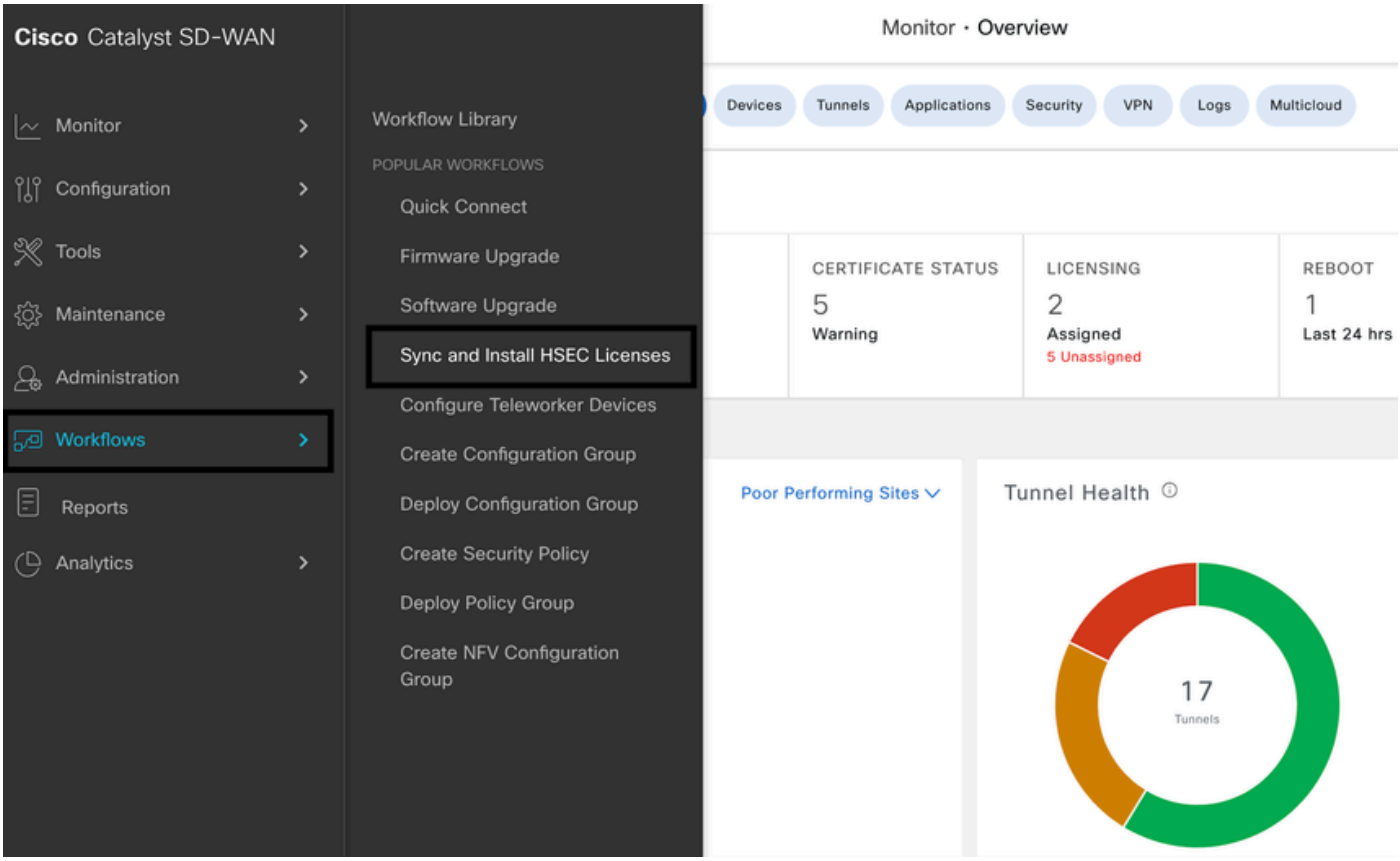


11.- Once the license is fetched from Cisco License Central and stored in vManage, the status is shown as **Success**.

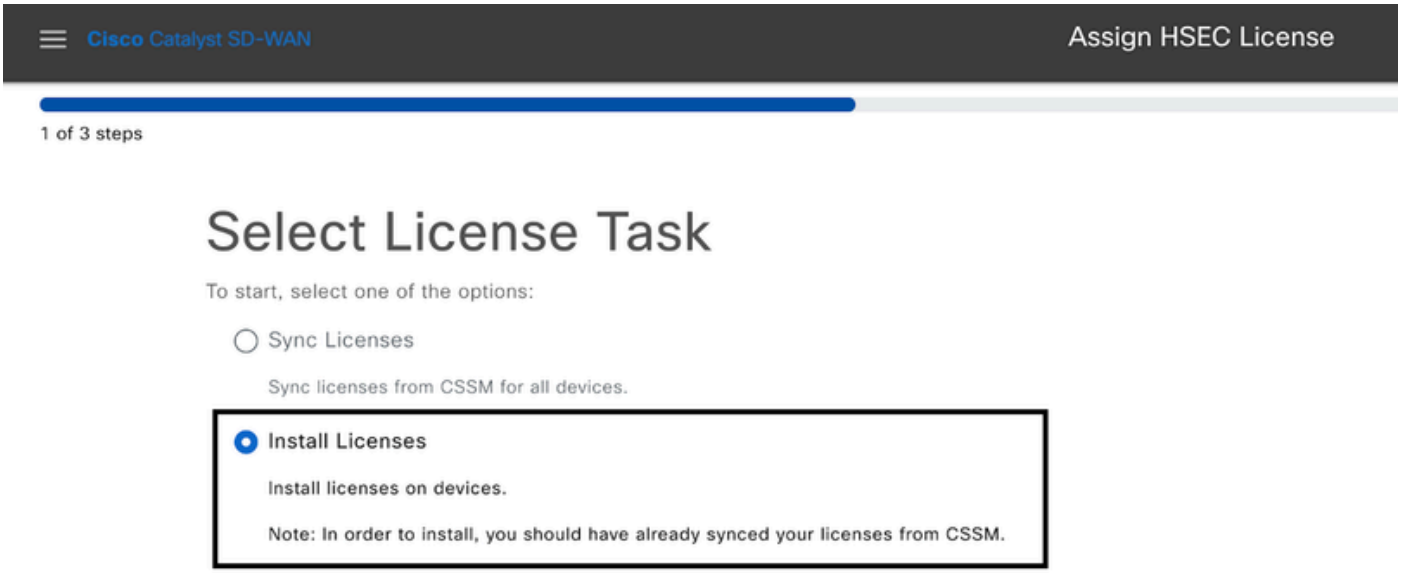


Install Fetched Licenses

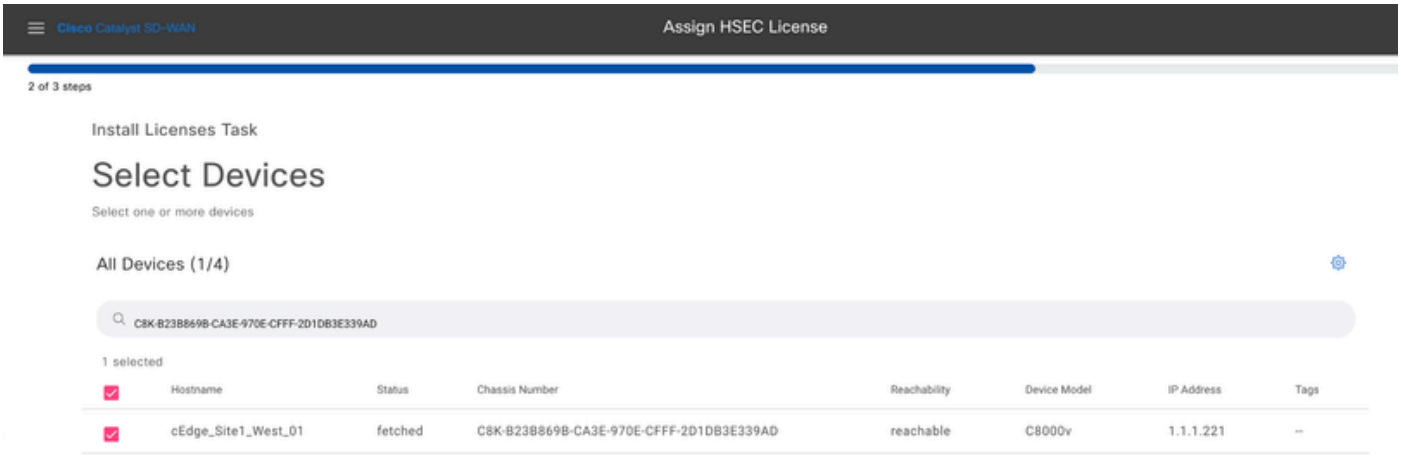
1.- In vMange GUI navigate to **Main Menu > Workflows > Sync and Install HSEC Licenses.**



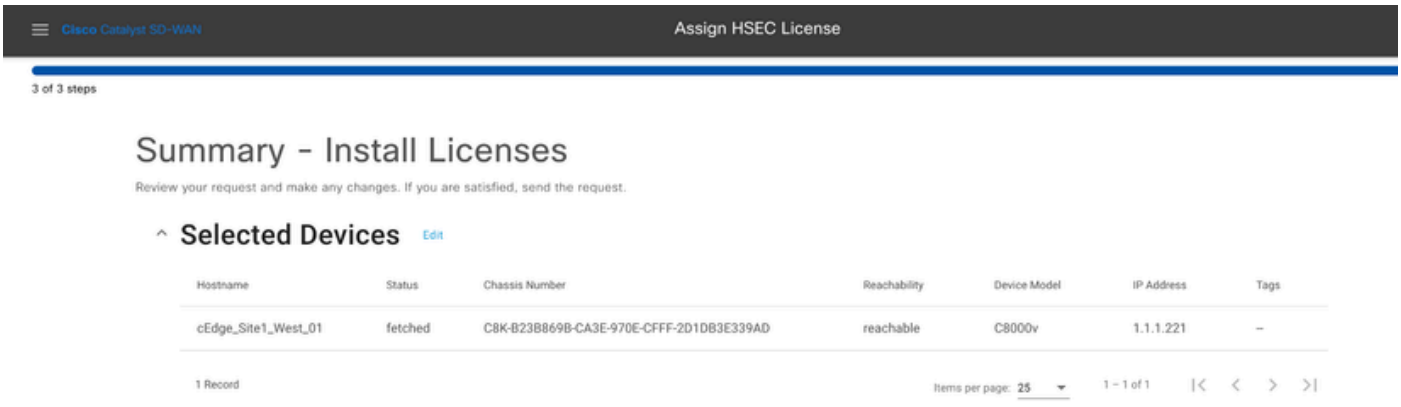
2.- Select the **Install Licenses** task.



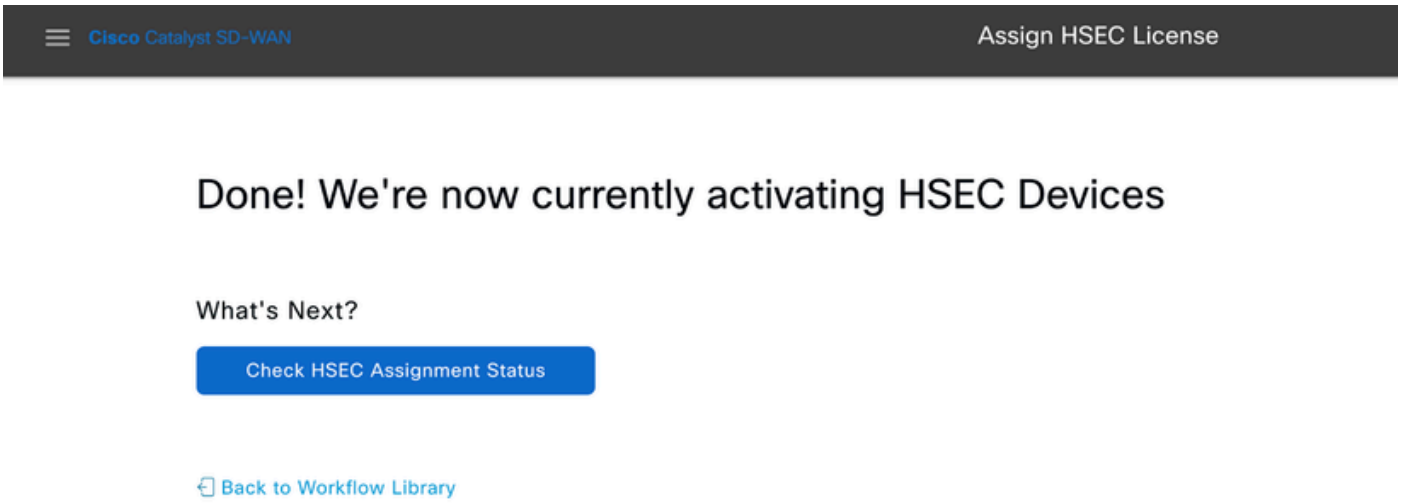
3.- Select the device for which the HSEC licenses was fetched.



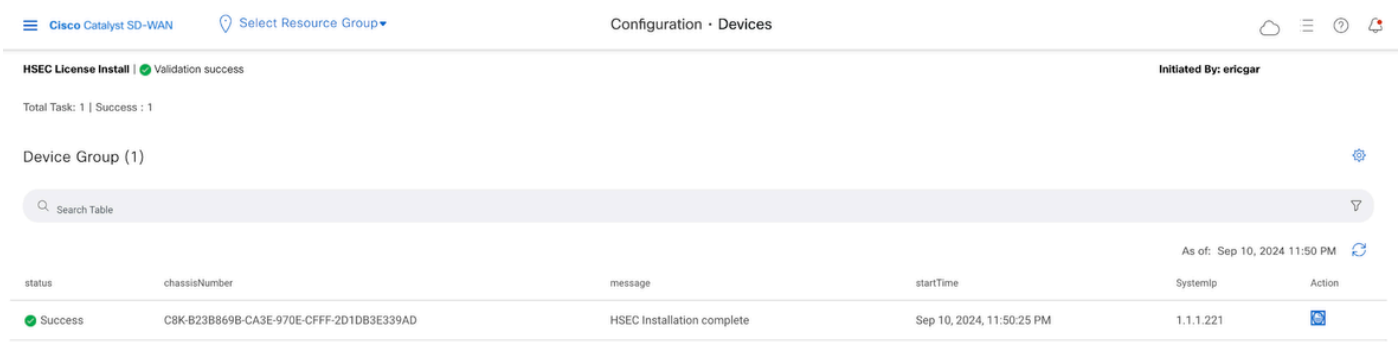
4.- Verify the installation summary and click **Install**.



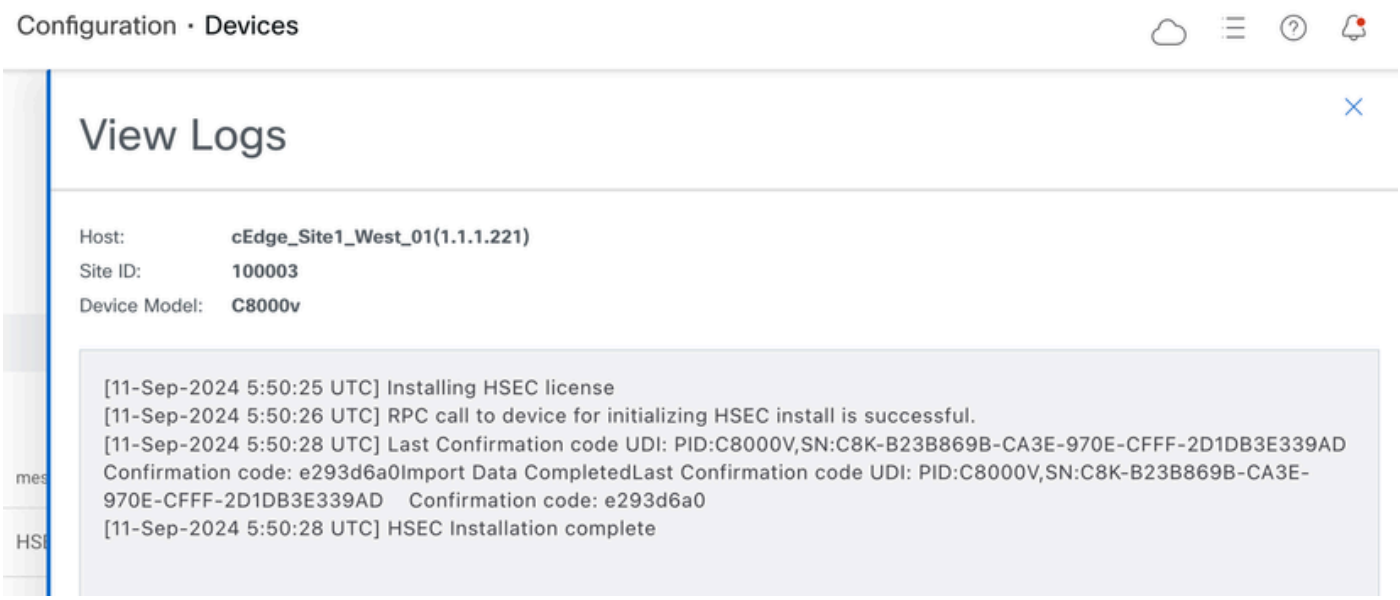
5.- Click **Check HSEC Assignment Status** to check the installation status in real time.



6.- vManage communicates with the router, sends the SLAC to it and installs it. The final status must be **Success**.



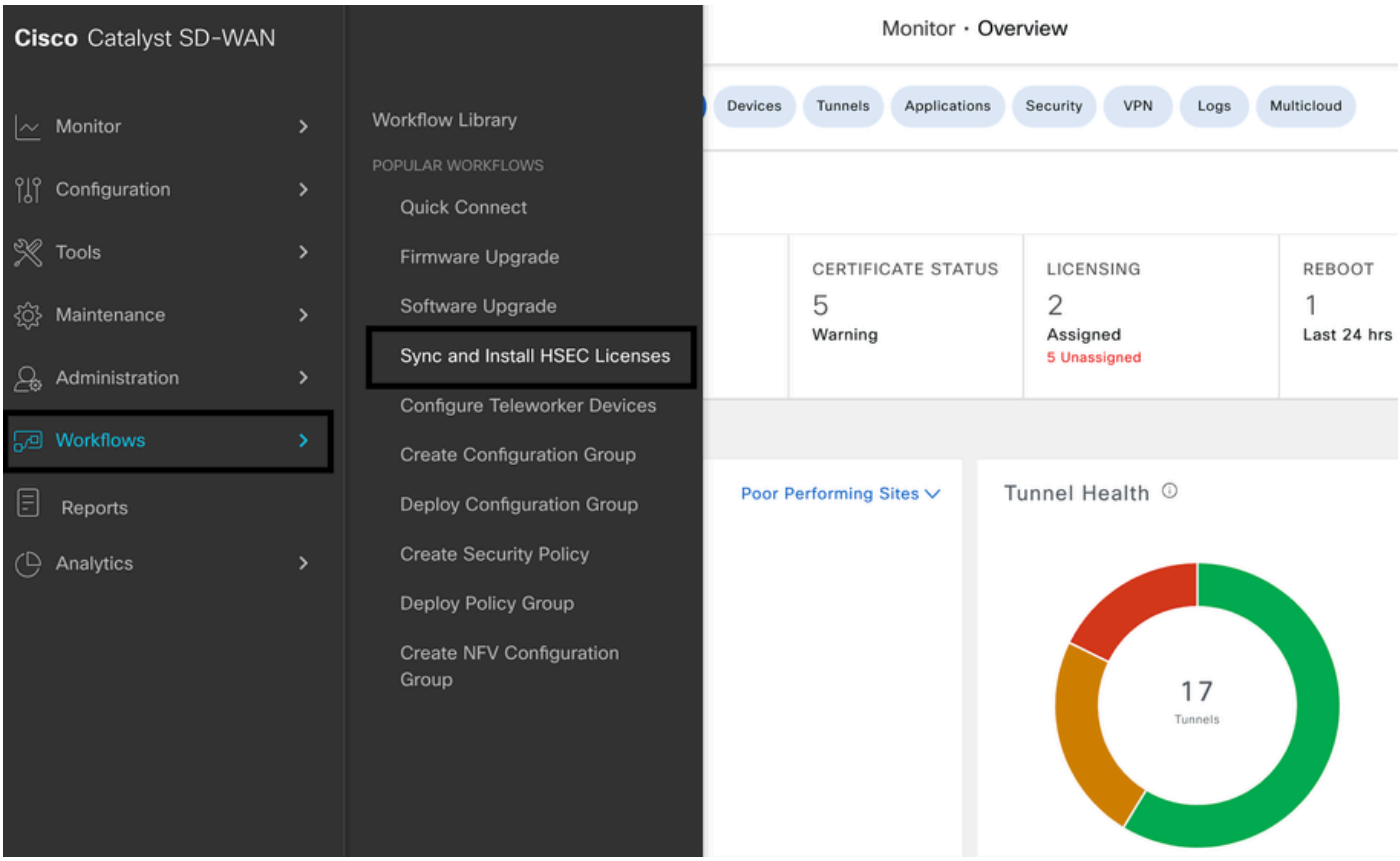
7.- Click **Action** icon to display more detailed logs of the HSEC installation.



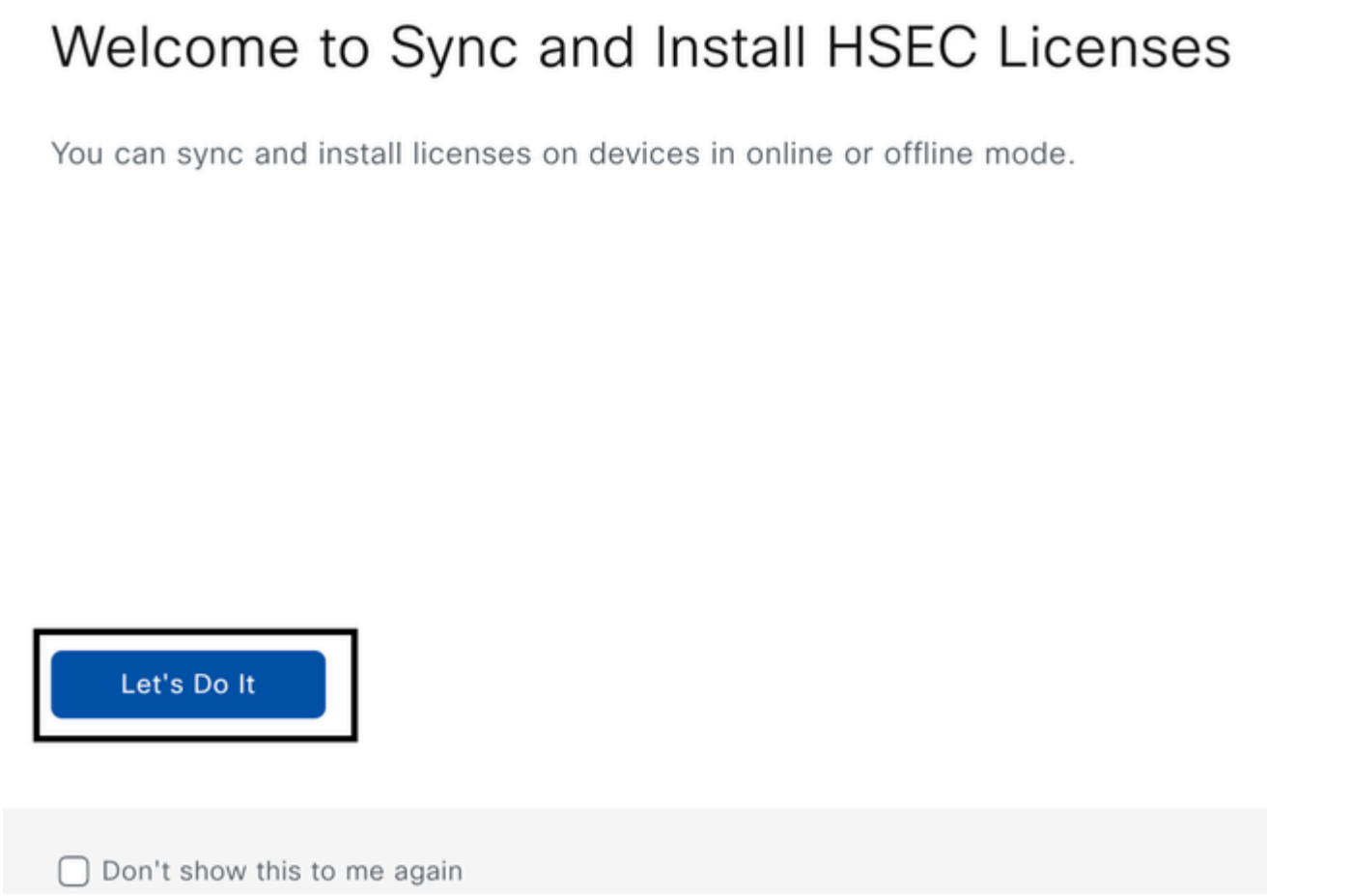
Offline Workflow

Sync Licenses with Cisco License Central

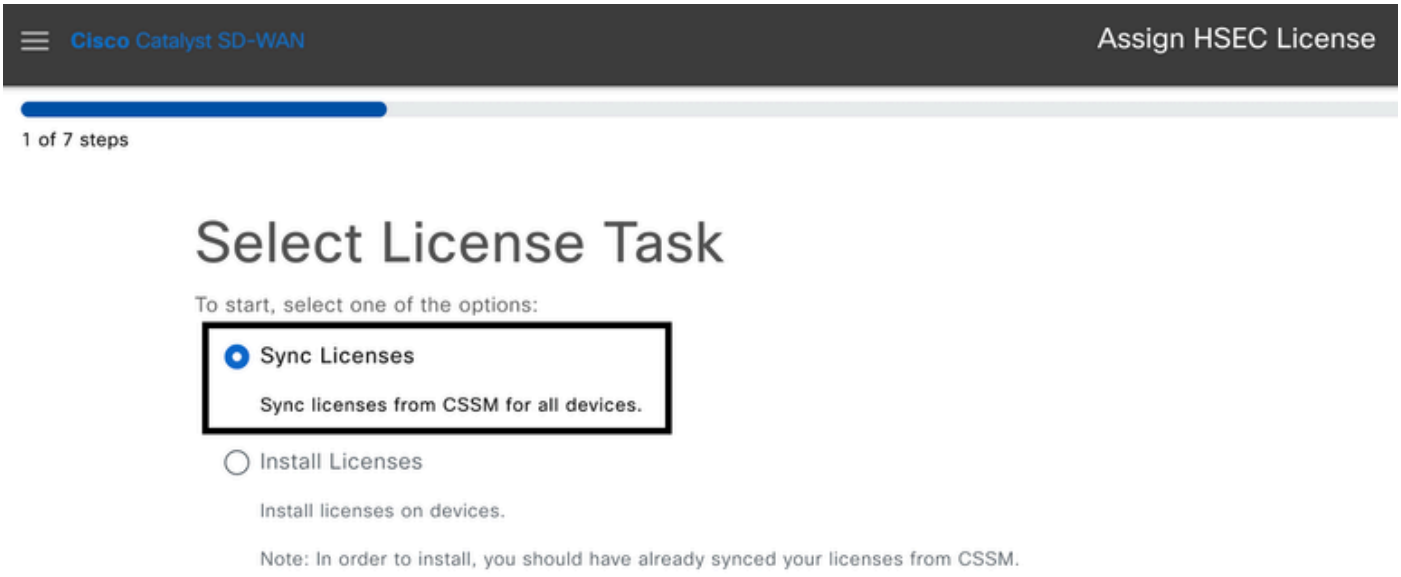
1.- In vMange GUI navigate to **Main Menu > Workflows > Sync and Install HSEC Licenses.**



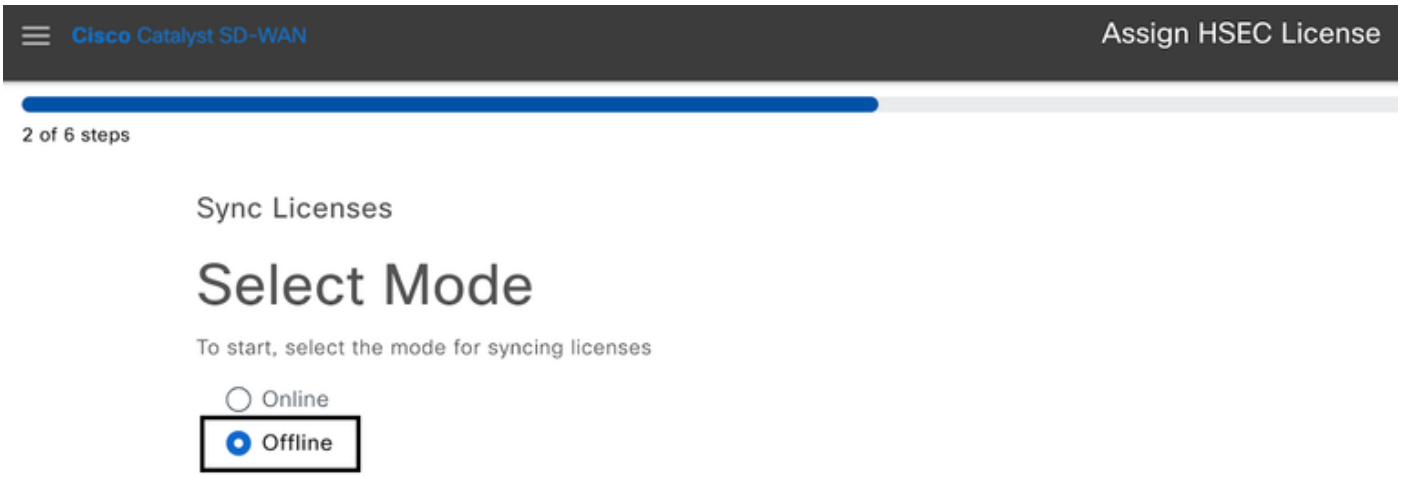
2.- Click **Let's Do it** button on the pop-up window.



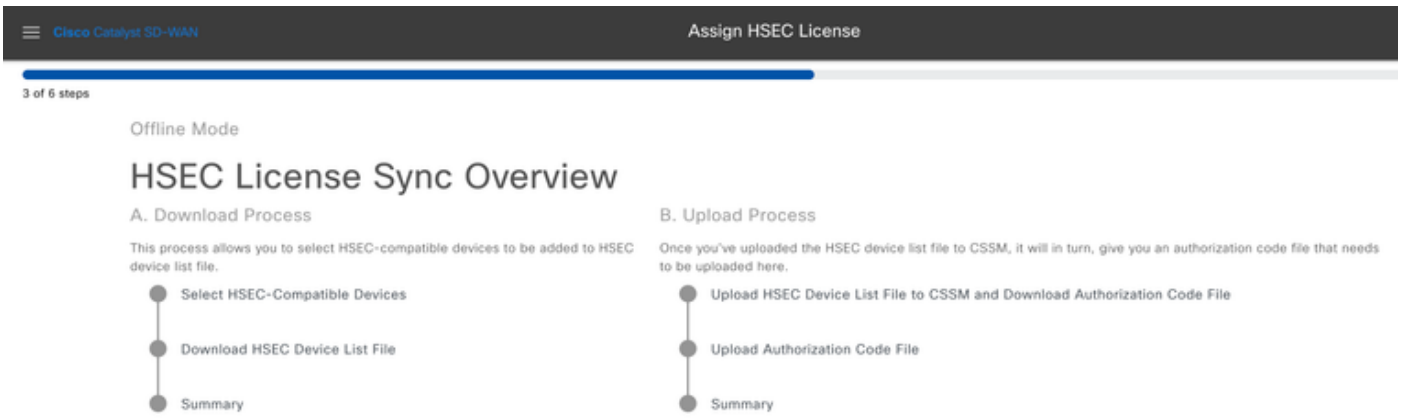
3.- Select **Sync Licenses** task and click **Next**.



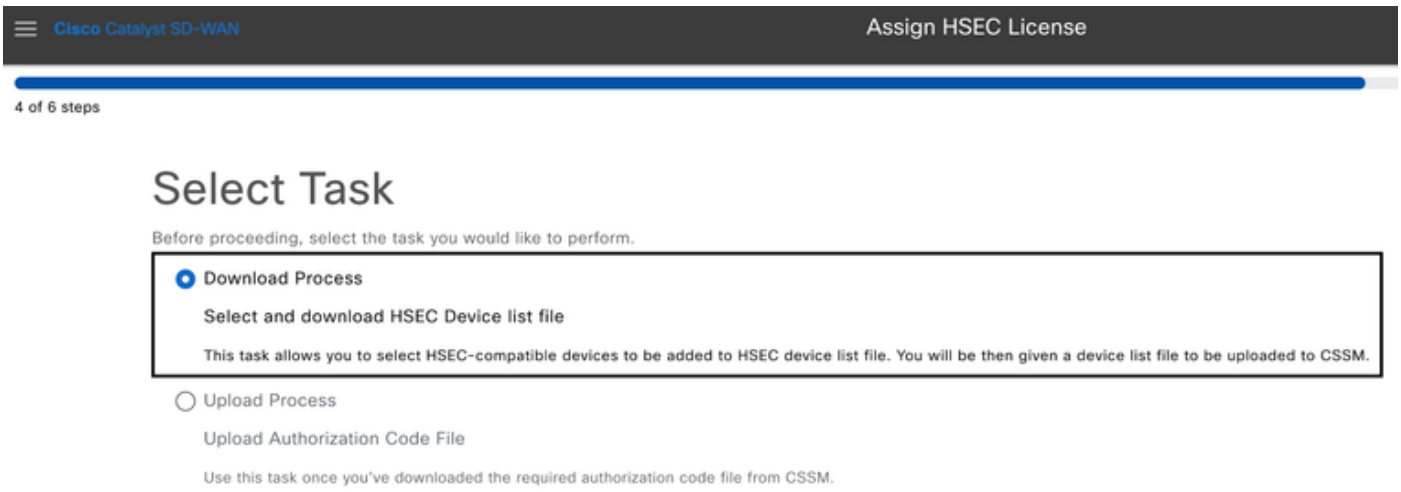
4.- Select **Offline** mode and click **Next**.



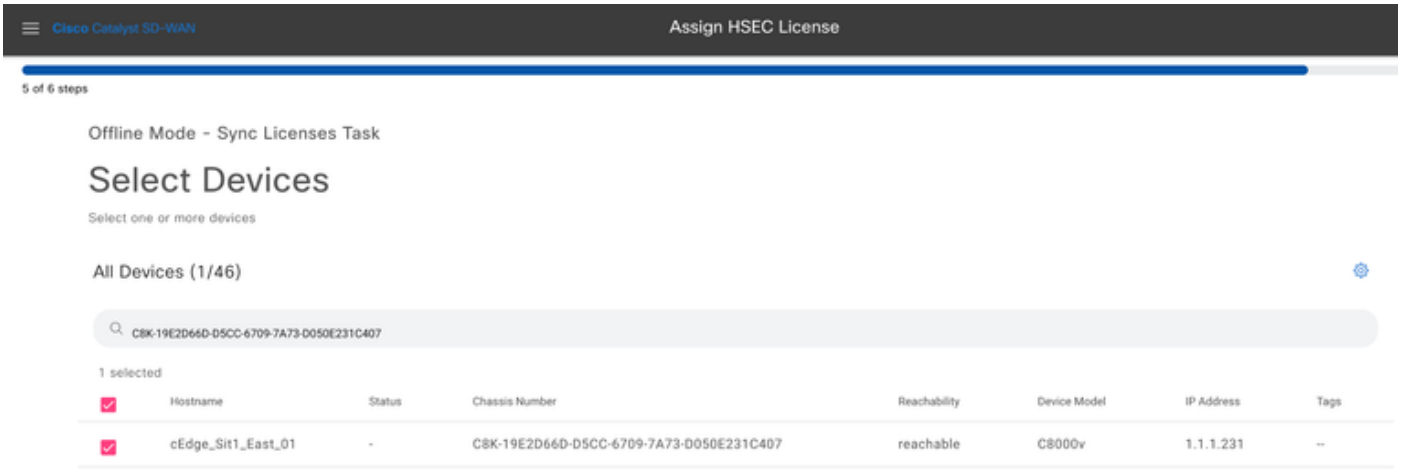
5.- Carefully review the process overview and click **Next**.



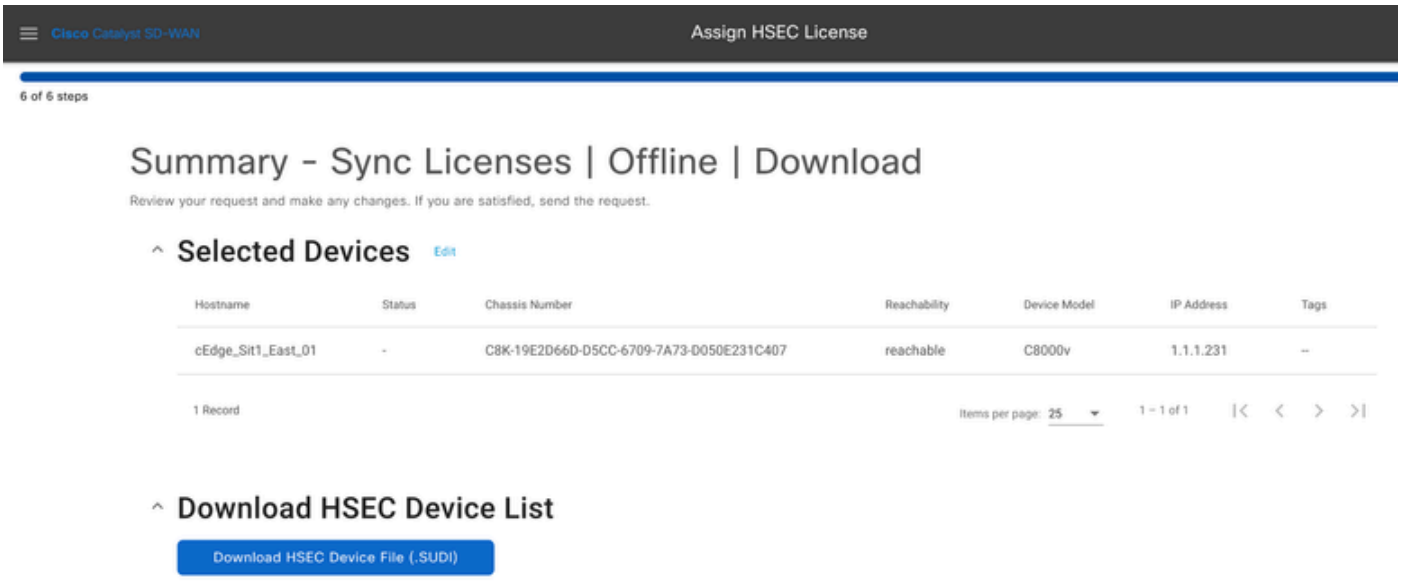
6.- Select **Download Process** option and click **Next**.



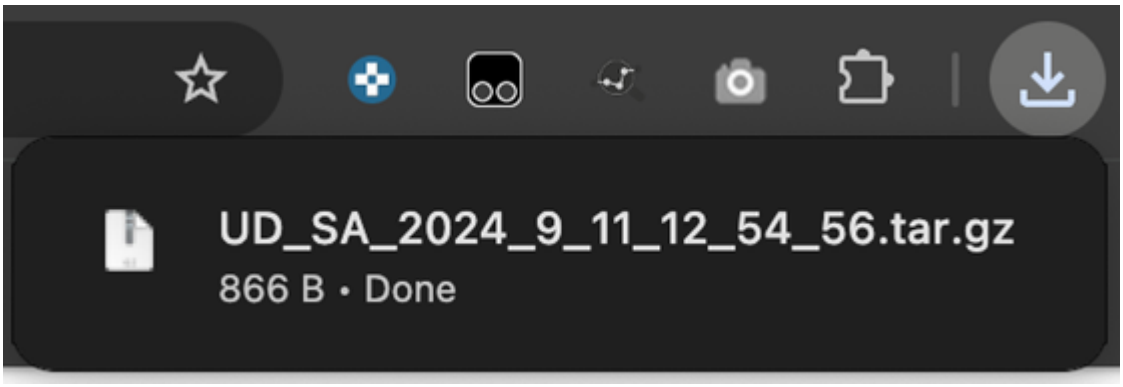
7.- In the search bar, filter the device for which the license is intended to be installed.



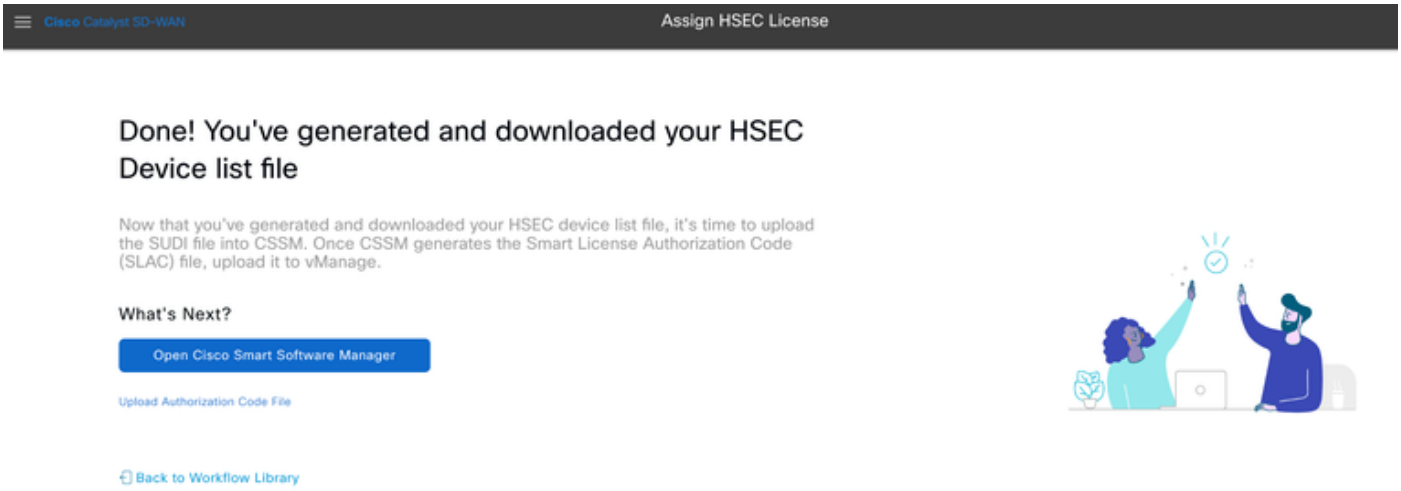
8.- Review the summary of the task and click **Download HSEC Device File (.SUDI)**



9.- An automatic download of the license usage starts.



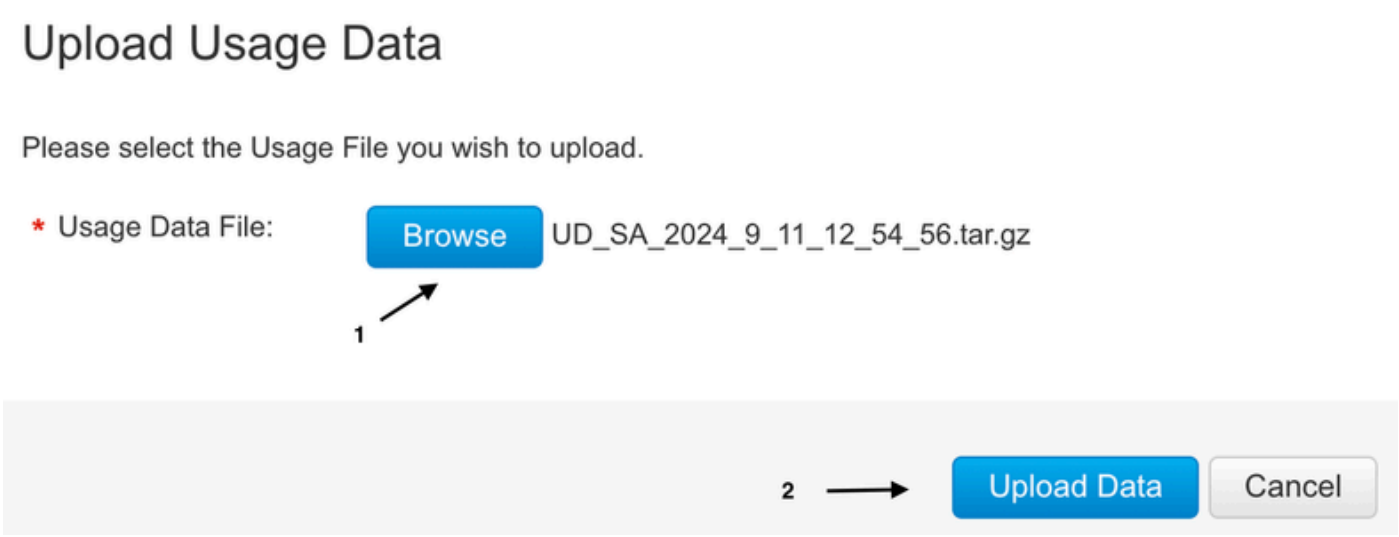
10.- Click **Open Cisco License Central** or navigate to: [Cisco License Central.]



11.- In the selected Smart Account, navigate to **Cisco Software Central > Smart Software Licensing** and click **Reports > Usage Data Files > Upload Usage Data...**.

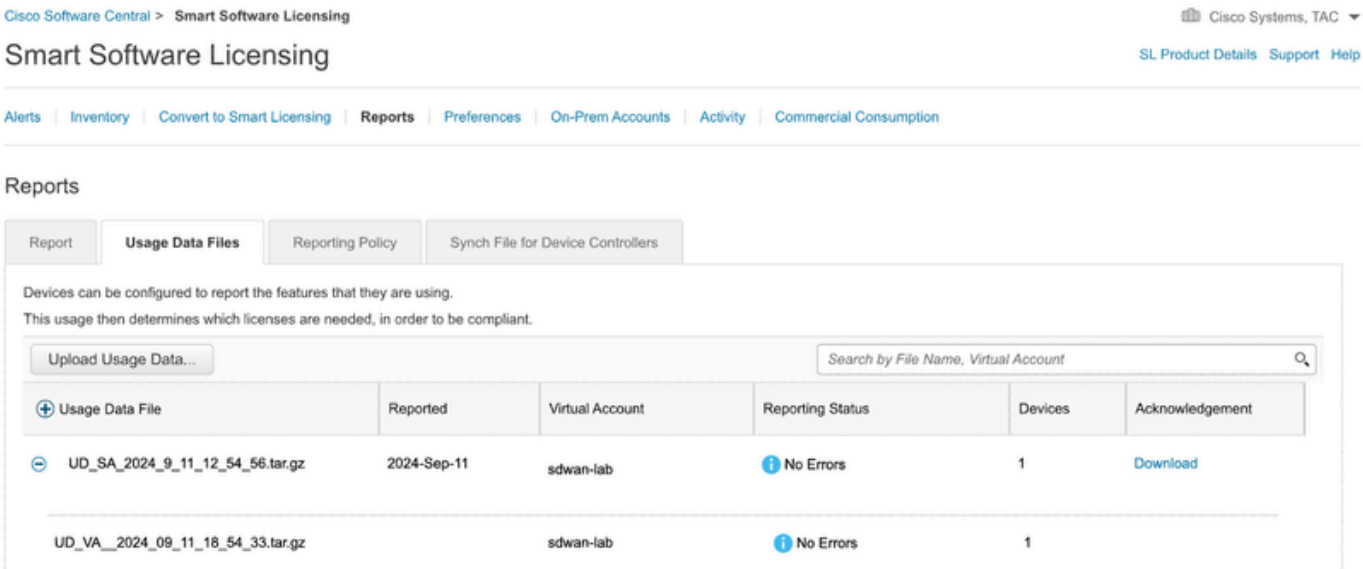


12.- In the **Upload Usage Data** Pop-up, click **Browse** and select the file just downloaded and click **Upload Data**.

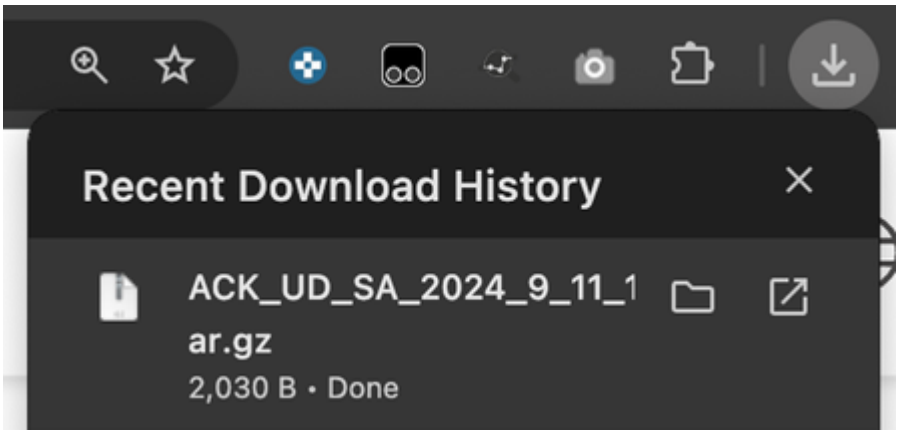


13.- The system starts to process the file. It takes around 5 to 10 minutes to complete. Then click **Download**.

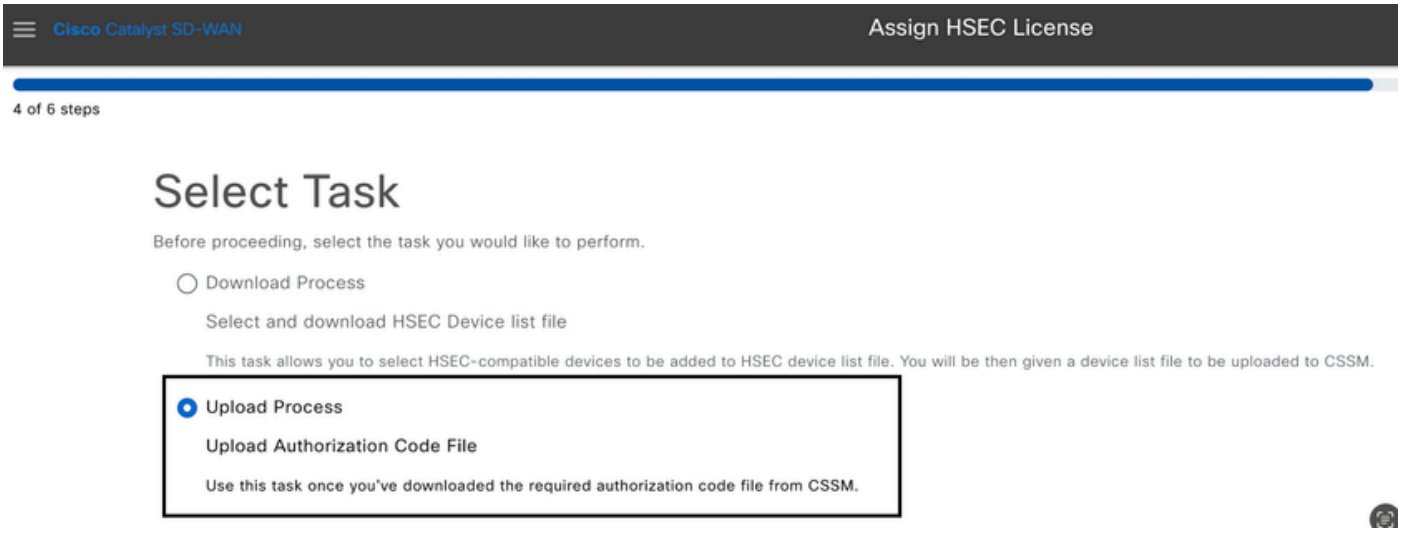
Note: To generate the ACK file, the Reporting Status must be "No errors"; if there is an error, click the expand icon to obtain more information about the error. Open a Cisco TAC case if needed.



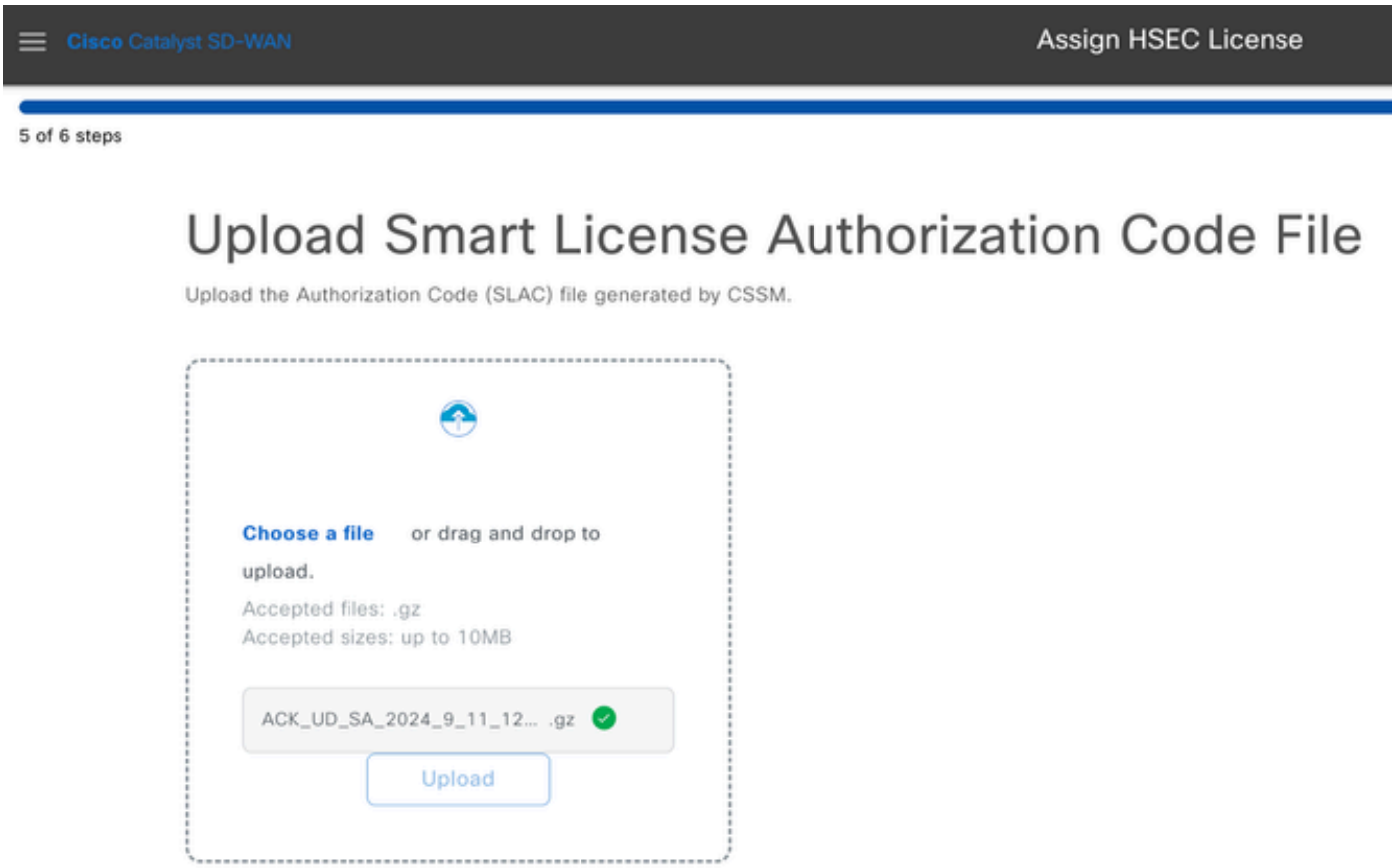
14.- The system generates the ACK file and it downloads it automatically.



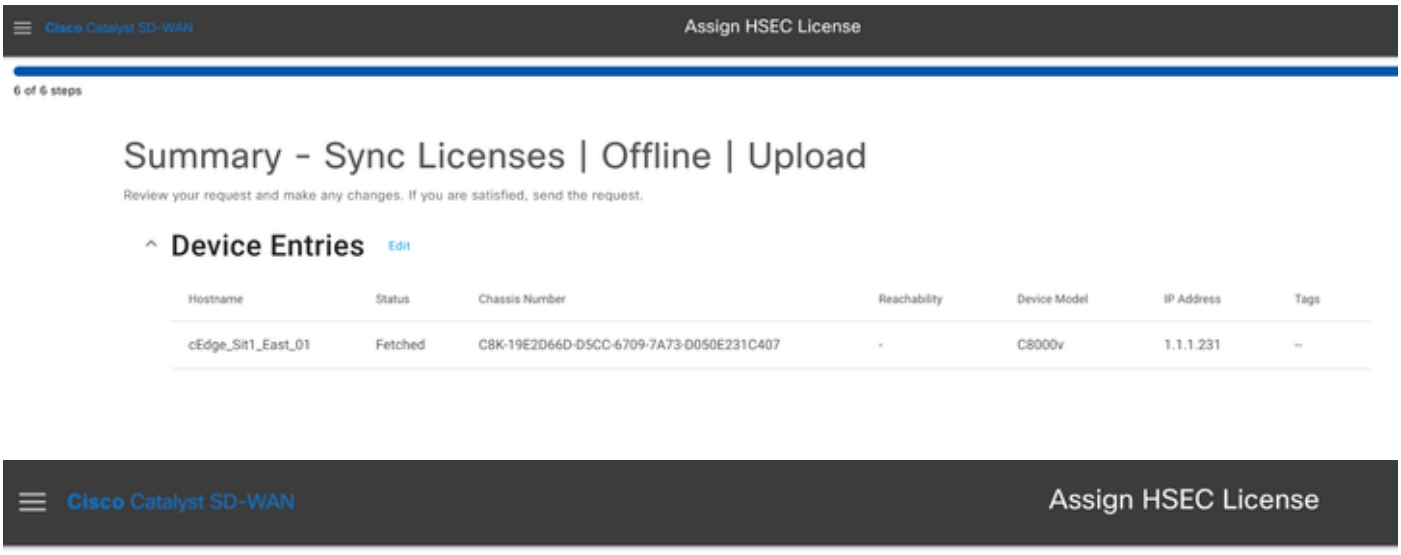
15.- In vMange GUI, navigate again to **Main Menu > Workflows > Sync and Install HSEC Licenses > Sync Licenses > Offline > Next > Upload Process.**

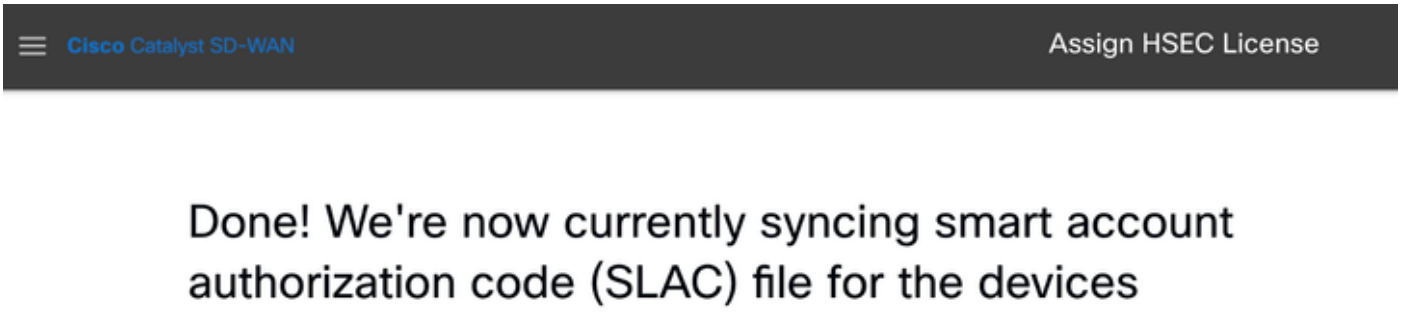


16.- Click **Choose a File** or drag and drop the downloaded file in the box and click **Upload**.



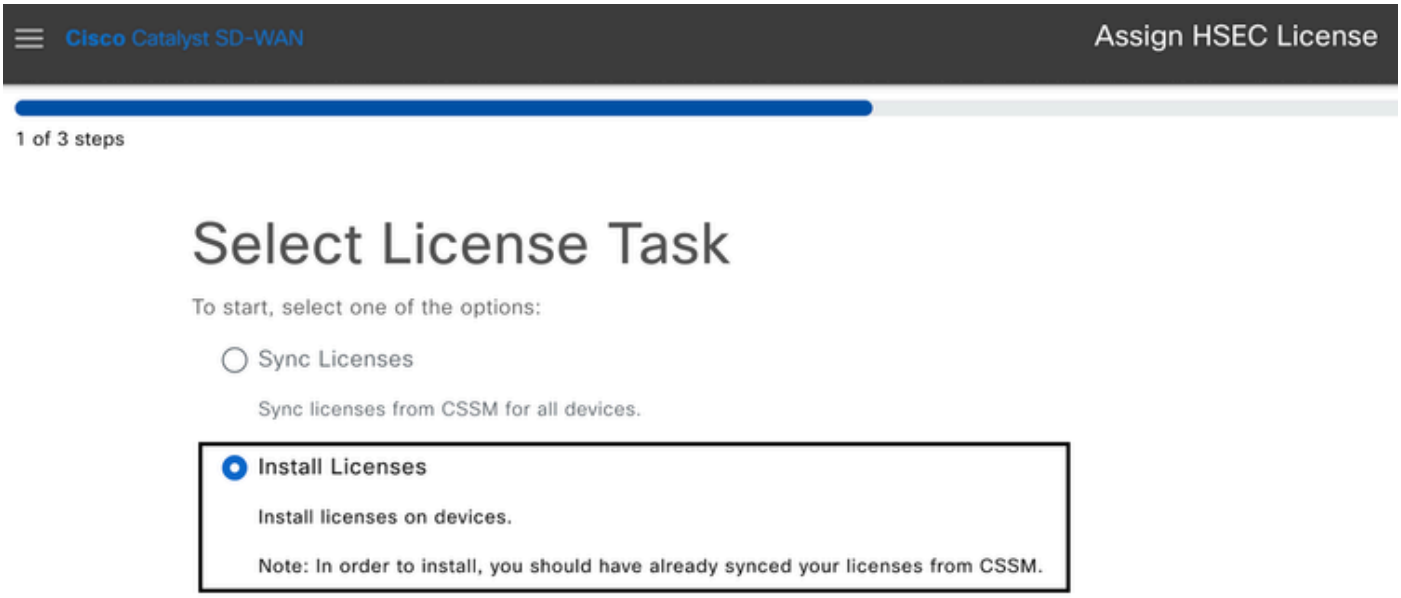
17.- Verify the summary of the task and click **Upload**.



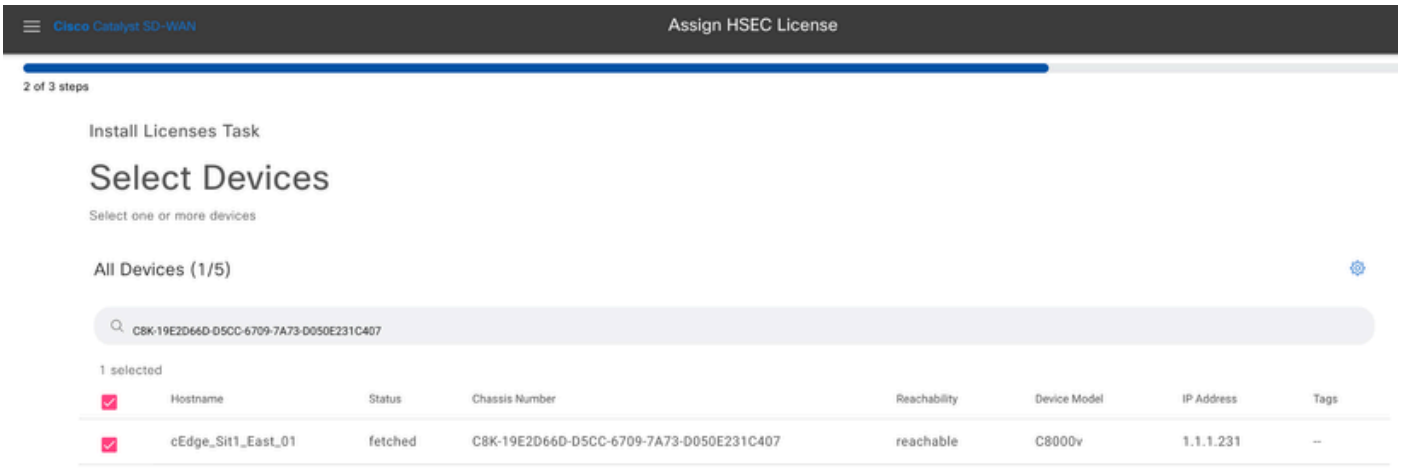


Install Fetched Licenses

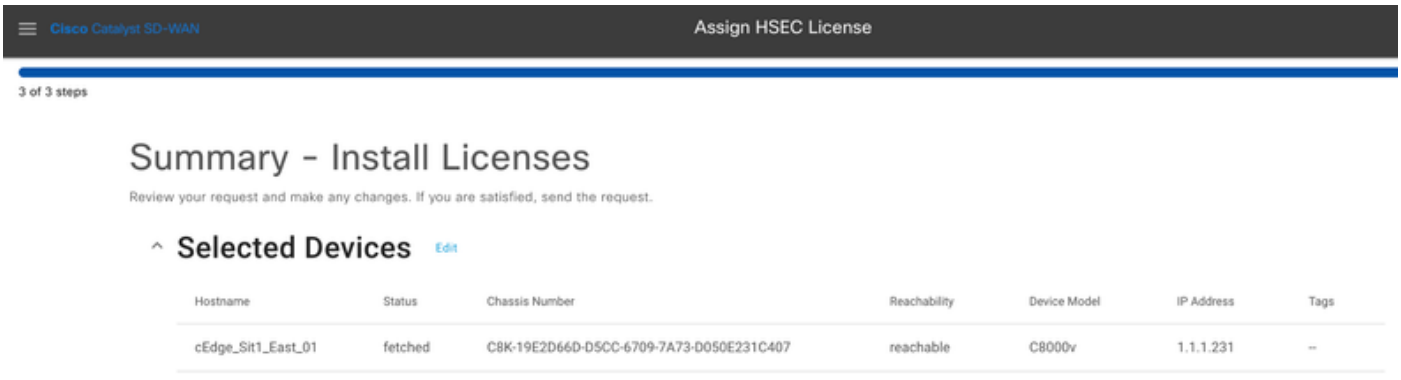
1.- Go back to workflow library **Sync and Install Licenses** and click **Install Licenses**.



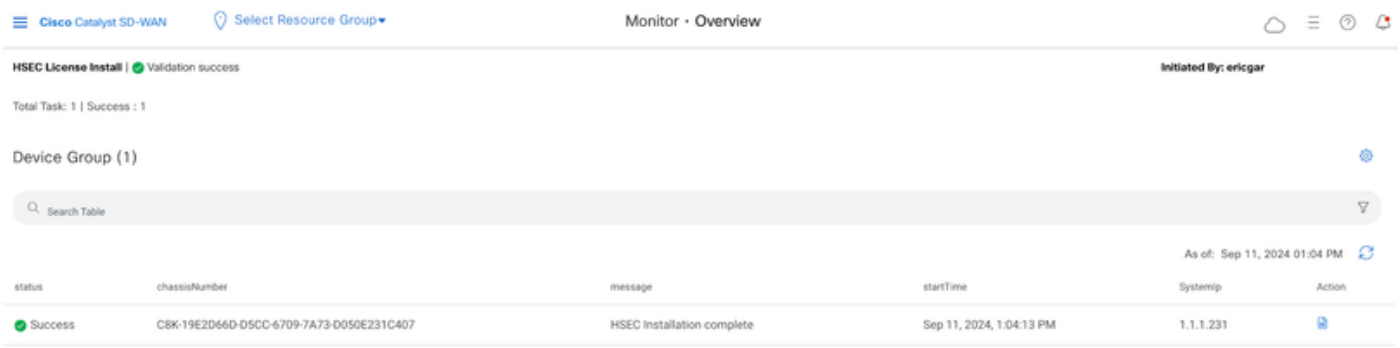
2.- Select from the list the same device for which the license authorization was made and click **Next**.



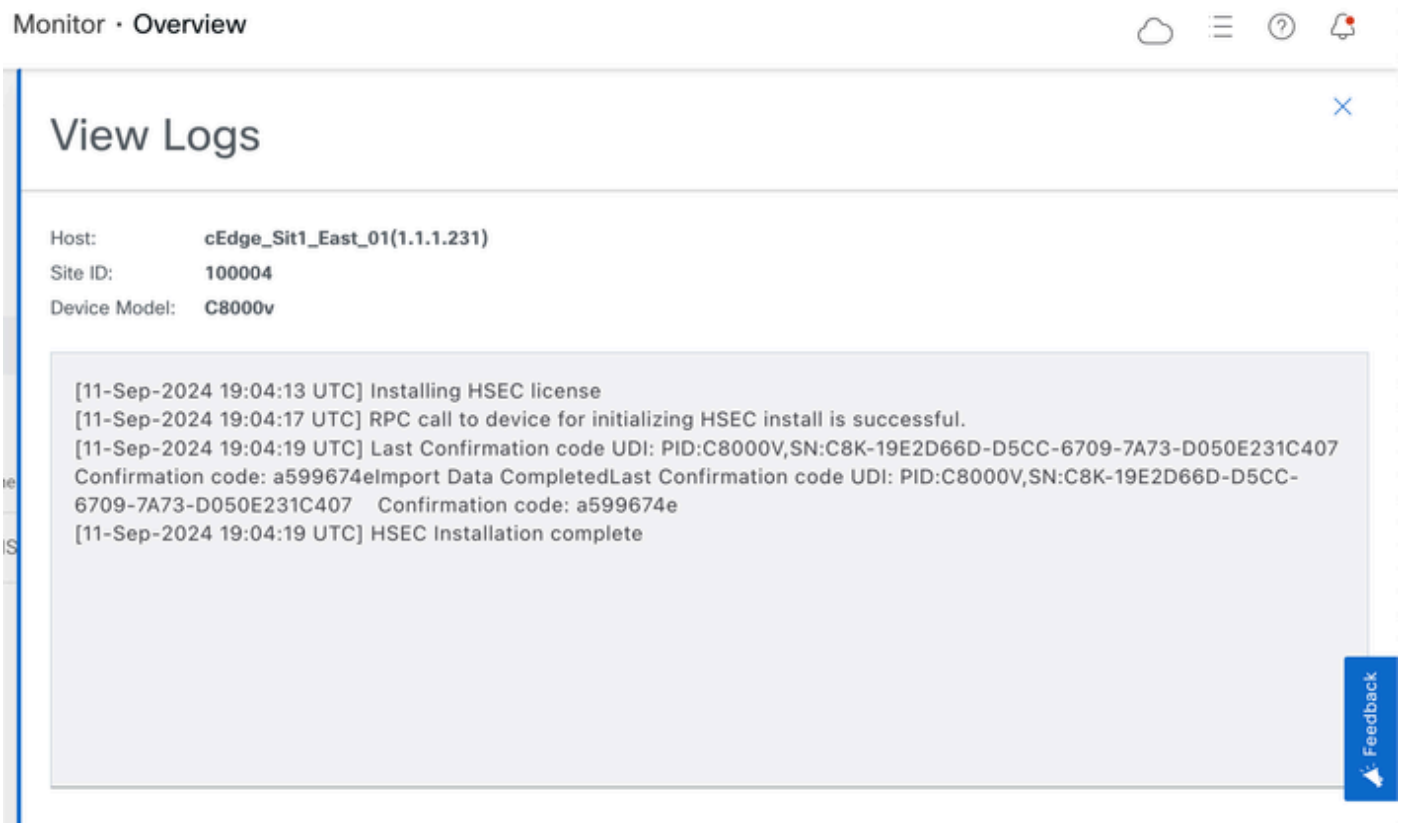
3.- Review the task summary and click **Install**.



4.- Wait for the process to finish, the status of the installation must be **Success**.



5.- Click **Action** icon to display more detailed logs of the HSEC installation.



Return the HSECK9 License

Return Code Behavior

The purpose of this task is to eliminate the license from the router and return it as positive count to the HSECK9 license pool in the Cisco License Central portal.

Reservation Method	Return Code Generation	Action Plan
Online	Yes, it is possible	Generate the return code to disassociate the license with the router. Verify the next section.
Offline	Yes, it is possible	Generate the return code to disassociate the license with the router. Verify the next section.

Note: In case the return code generation fails, open a TAC case to manually remove the license from the router and the Cisco License Central portal.

Generate the Return Code

The return code is required to validate the reserved license in Cisco License Central against the router's local authorization, and to remove it afterward.

<#root>

```
EdgeRouter# license smart authorization return local online

Authorization already returned with this code:
UDI: PID:C1111-8PWE,SN:FGL2149XXXX
Return code:

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

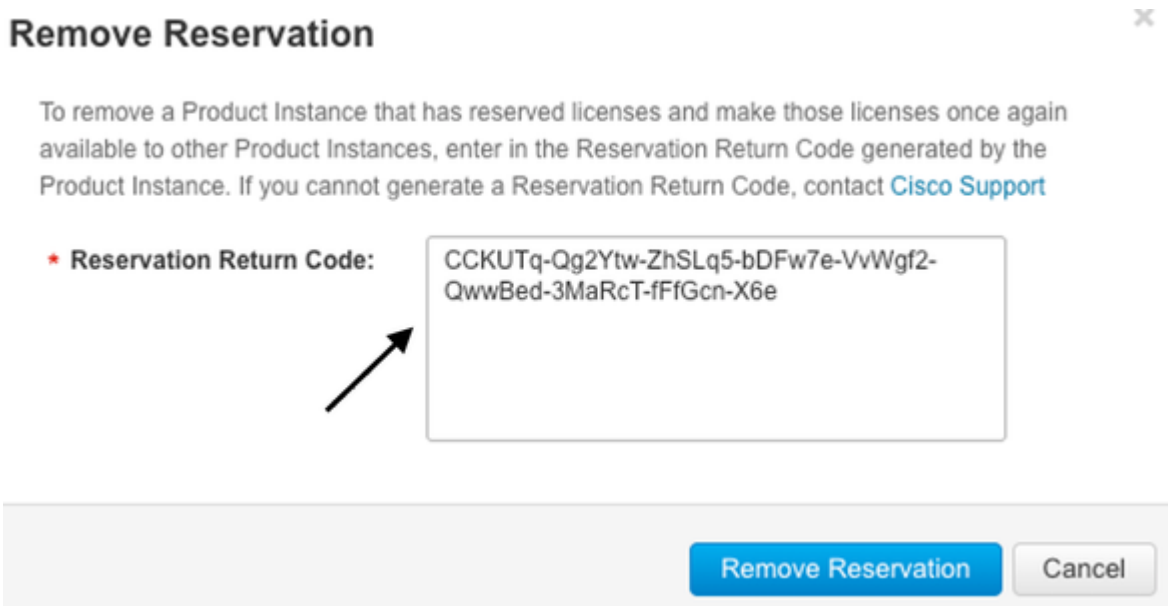


<<<< Copy the string
```

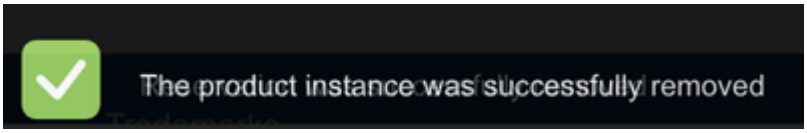
Note: The command "**license smart authorization return local online"** works for both reservation methods, online or oflline. The command **"license smart authorization return local offline"** does not work in controller-managed mode (SD-WAN mode). This applies for both, physical and virtual routers.

Remove the Reservation

In Cisco License Central, navigate to **Product Instances > Actions > Remove.** Paste the return code just copied from the router and click **Remove Reservation**.



The **License reservation removed successfully** notification shows up right after. This indicates that the license is sent back to the licenses pool; the license count increases in 1.



Activation - Is Reload Required?

Is it True that on 8500-based Platforms a Reload is Required for HSEC to be Activated?

Yes, the 8500 platform family requires a reload in either autonomous or controller mode.

Is a Reload Needed for C8000v Post Activation of HSEC?

No, it is not needed. The license stays as 'not-in-use' as per the design on C8000v, but the device gets unlimited throughput immediately after the hsec install.

Is a Reload for CSR1000v Post Activation of HSEC?

No, post activation of hsec, the CSR1000v does not require a reload.

Is the Reload Behavior the Same for SD-WAN and non-SD-WAN Modes?

No, the SD-WAN and non-SD-WAN modes with respect to the HSEC enablement are quite different.

In the SD-WAN mode, a reload is required to enable/activate HSEC, while in the non-SD-WAN mode, the CLI **license feature hsec** command enables/activates hsec on the device. A reload is not needed on CSR1000v and C8000V platforms in the SD-WAN mode.

Is it Also True for the Deactivation of HSEC License?

The HSEC license can be uninstalled in the non-SD-WAN mode (Autonomous), however, the HSEC license cannot be uninstalled while the feature is in use. The user is required to disable/deactivate HSEC license with CLI **no license feature hsec** command and reload the device for the license to be in the 'not-in-use' state and then initiate the uninstall command. The HSEC license **uninstall** in the SD-WAN mode is not supported as the feature cannot be disabled. However, the user has an option to go to the autonomous mode and uninstall as a workaround upon known challenges with the mode changes. Please open a TAC case to receive guidance on how to return the license to Cisco License Central while in SD-WAN Mode.

Note: For more information visit: HSEC License FAQs for SD-WAN.

License Availability Verification

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.

<#root>

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 Edge Router and Cisco License Central 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 Edge Router 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 Uti
```

Ensure there is IP connectivity to the Internet.

<#root>

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.

<#root>

ping cisco.com

telnet cisco.com 80

If the test fails, configure a DNS Server and enable DNS resolution.

<#root>

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.

<#root>

EdgeRouter#

config-transaction

EdgeRouter(config)#

ip host smartreceiver.com A.B.C.D

EdgeRouter(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**.**

<#root>

EdgeRouter#

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"
```

<#root>

```
EdgeRouter#

show logging | include SMART


*Aug 18 20:59:44.914: %SMART_LIC-3-COMM_FAILED: Communications failure with the Cisco Smart Software Ma
```

SD-WAN Tunnel Blocks DNS

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

<#root>

```
EdgeRouter#

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"
```

<#root>

```
EdgeRouter#

show logging | include SMART


*Aug 18 20:59:44.914: %SMART_LIC-3-COMM_FAILED: Communications failure with the Cisco Smart Software Ma
```

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

<#root>

EdgeRouter#

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).

<#root>

EdgeRouter#

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.

<#root>

```
EdgeRouter#

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"
```

```
<#root>

EdgeRouter#

show logging | include SMART


*Aug 18 20:59:44.914: %SMART_LIC-3-COMM_FAILED: Communications failure with the Cisco Smart Software Ma
```

> **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.

```
<#root>

EdgeRouter#

configure terminal


EdgeRouter(config)#

license smart transport smart


EdgeRouter(config)#

license smart url default


EdgeRouter(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 Ma
```

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.

<#root>

```
EdgeRouter#
```

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 Cisco License Central 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.

```
<#root>
EdgeRouter#
telnet smartreceiver.com 443

Trying smartreceiver.com (X.X.X.X, 443)...
Open
```

From a Service VRF host.

```
<#root>
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 Cisco License Central

fails; the HTTP source interface can be changed to any available in the router.

<#root>

```
EdgeRouter#
```

config-transaction

```
EdgeRouter(config)#
```

ip http client source-interface INTERFACE

```
EdgeRouter(config)#
```

commit

Related Information

- Smart Licensing Using Policy for Cisco Enterprise Routing Platforms
- Manage Licenses for Smart Licensing Using Policy SD-WAN
- Technical Support & Documentation - Cisco Systems