

# 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 CSSM](#)

[Configure Transport Type and Set Default CSSM URL](#)

[Generate a Product Instance Registration Token](#)

[Generate a Trust Establishment between the Edge Router and CSSM](#)

[Verify the Trust Establishment Success Counter](#)

[Request Authorization](#)

[Verify the Activation is Successful](#)

#### [Offline Method To CSSM](#)

[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 CSSM](#)

[Install fetched licenses](#)

#### [Offline Workflow](#)

[Sync Licenses with CSSM](#)

[Install fetched licenses](#)

### [Return the HSECK9License](#)

#### [Online Method](#)

#### [Offline Method](#)

[Generate the Return Code](#)

[Remove Reservation](#)

### [Activation - Is Reload Required?](#)

---

[Is it true that on 8500-based platforms a reload is required for HSEC to get 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 CSSM 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 Smart Software Manager (CSSM)
- 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](#).

## 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](#)

---

## 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.

Cisco Software Central > Smart Software Licensing Cisco Systems, TAC

## 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

Available Actions | Manage License Tags | License Reservation... |  Show License Transactions | Search by License

| License   | Billing | Available to Use | In Use | Substitution | Balance | Alerts | Actions |
|---|---------|------------------|--------|--------------|---------|--------|---------|
| <input checked="" type="checkbox"/> 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.

```
<#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 CSSM

#### Configure Transport Type and Set Default CSSM 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
```



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.



*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.

Virtual Account: **sdwan-lab** ▾

General Licenses Product Instances Event Log

**Virtual Account**

Description:

Default Virtual Account: No

product instances to this virtual account.

ODRIMjg0YWQIMdk4ZC00NWlxLTgzYmYtODMxNjU3NTQwMTY0LTE2NmM0ODM2%0ANJU4MDB8S2lFK3BsUXZEZwPcaEJBK2ikREMvJRmUTB0bzluZit4MEwyb3hX%0AVTI4ND0%3D%0A

Press ctrl + c to copy selected text to clipboard.

| Uses               | Export-Controlled | Description          | Created By | Actions   |
|--------------------|-------------------|----------------------|------------|-----------|
| ODRIMjg0YWQIMdk... | Allowed           | hseckk9 Installation | ericgar    | Actions ▾ |

Copy

Download...

Revoke...

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

### Generate a Trust Establishment between the Edge Router and CSSM

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

```
<#root>
```

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

Example:

```
<#root>
```

```
EdgeRouter#
```

```
license smart trust idtoken ZThjOTlmM2UtMjQ2ZC00YjI1LTgwNjctZGIxZjIzYjZiYmVmLTE2NmM0NjI1%0AMjgyNTh8YWNV
```

Right after the trust is established, the logs show communication with CSSM.

```
<#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 (CSSM
*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 CSSM.

<#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 CSSM the 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
```





## Authorize License-Enforced Features



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

device to enable the features. [Learn More](#)

Generating an authorization code here is only required for devices that do not connect to the Smart Software Manager directly, or through the Cisco Licensing Manager, to report the features they need.

Single Device

Enter the identifiers for the device to be licensed.

Display Name:   
UUID:   
Serial Number:   
PID:   
Version ID:   
Host ID:   
MAC Address:   
Virtual ID(SUVI)

You can use the 'show license udi' command to see the identifiers for a device

Cancel 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.

## Authorize License-Enforced Features

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

UDI Serial Number: FGL214991A9

### Select the Licenses to Enabled the Features

Select the set of licenses that will enable the desired features. The licenses will be reserved on the devices

| License  | Purchased | Available | Reserve                        |
|--|-----------|-----------|--------------------------------|
| Router US Export Lic. for DNA<br><small>U.S. Export Restriction Compliance license for DNA based Routers</small> | 1         | 1         | <input type="text" value="1"/> |

## 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:

Unidentified Devices:

| <input checked="" type="checkbox"/> | Device                              |
|-------------------------------------|-------------------------------------|
|                                     | <input type="text" value="Search"/> |
| <input checked="" type="checkbox"/> | SN: FGL214991A9<br>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

x

STEP 1 ✓  
Enter Request Code

STEP 2 ✓  
Select Licenses

STEP 3  
Review and Confirm

STEP 4  
Authorization Code

### Product Instance Details

UDI PID: C1111-8PWEE  
UDI Serial Number: FGL214991A9  
Device Type: DNA On Prem

### Licenses to Reserve

| License  | Total Quantity to Reserve |
|--|---------------------------|
| Router US Export Lic. for DNA<br><small>U.S. Export Restriction Compliance license for DNA based Routers</small> | 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 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.

Virtual Account: [sdwan-lab](#) ▾

| General  |  | Licenses               | Product Instances      | Event Log   |                       |        |           |
|--|--|------------------------|------------------------|---|-----------------------|--------|-----------|
| Available Actions ▾  |  | Manage License Tags    | License Reservation... | <input checked="" type="checkbox"/> Show License Transactions |                       |        |           |
|  |  |                        |                        | Search by License 🔍   |                       |        |           |
|  |  |                        |                        | Advanced Search ▾   |                       |        |           |
| <input type="checkbox"/> License                               | Billing                                      | Available to Use       | In Use                 | Substitution  | Balance               | Alerts | Actions   |
| <input checked="" type="radio"/> Router US Export Lic. for DNA | Prepaid                                      | 1                      | 1<br>(1 Reserved)      | -   | 0                     |        | Actions ▾ |
| <input type="checkbox"/>                                       | Source: Manual Entry<br>Subscription Id: N/A | SKU:<br>C8000-HSEC=    | Quantity:<br>1         | Start Date:<br>-  | Expires:<br>- never - |        |           |
|  |  | Family:<br>DNA On Prem |                        |   |                       |        |           |
| Showing 1 Record   |  |                        |                        |   |                       |        |           |

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

## 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

| Name                              | Product Type | Last Contact                             | Alerts | Actions                 |
|-----------------------------------|--------------|--|--------|-------------------------|
| UDI_PID:C1111-8PWE; UDI_SN:FGL214 | DNA On Prem  | 2022-Aug-19 05:43:12 (Reserved Licenses) |        | <a href="#">Actions</a> |

Showing 1 Record

## 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 DNA HSEC visit [Restrictions for Managing HSEC Licenses](#) section.

## Online Workflow

### Sync Licenses with CSSM

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

**Cisco Catalyst SD-WAN**

Monitor > Configuration > Tools > Maintenance > Administration > **Workflows >** Reports > Analytics >

**Workflow Library**

POPULAR WORKFLOWS

- Quick Connect
- Firmware Upgrade
- Software Upgrade
- Sync and Install HSEC Licenses**
- Configure Teleworker Devices
- Create Configuration Group
- Deploy Configuration Group
- Create Security Policy
- Deploy Policy Group
- Create NFV Configuration Group

Monitor • Overview

Devices Tunnels Applications Security VPN Logs Multicloud

| CERTIFICATE STATUS | LICENSING                     | REBOOT           |
|--------------------|-------------------------------|------------------|
| 5<br>Warning       | 2<br>Assigned<br>5 Unassigned | 1<br>Last 24 hrs |

Poor Performing Sites ▾

Tunnel Health ⓘ

17  
Tunnels

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

# Welcome to Sync and Install HSEC Licenses

You can sync and install licenses on devices in online or offline mode.

Let's Do It

Don't show this to me again

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

☰ Cisco Catalyst SD-WAN Assign HSEC License

---

1 of 7 steps

## Select License Task

To start, select one of the options:

Sync Licenses  
Sync licenses from CSSM for all devices.

Install Licenses  
Install licenses on devices.

Note: In order to install, you should have already synced your licenses from CSSM.

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

2 of 7 steps

Sync Licenses

## Select Mode

To start, select the mode for syncing licenses

Online

Offline

5- Enter your Cisco CSSM credentials and click on **Next**.

3 of 7 steps

## Enter Smart Account Credentials

Now enter your Smart Account credentials

Username\*

ericgar

Password\*

.....

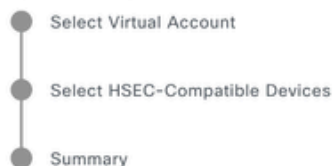
6.- Verify the HSEC License Sync Overview and click on **Next**.

4 of 7 steps


Online Mode | Sync Licenses

## HSEC License Sync Overview

This process will sync licenses from CSSM for the selected devices and virtual account.



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.

Cisco Catalyst SD-WAN Assign HSEC License

5 of 7 steps

## Select Virtual Account

Select Virtual Account

sdwan-lab - Cisco Systems, TAC

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

 **Note:** Only devices compatible with HSEC are displayed

Cisco Catalyst SD-WAN Assign HSEC License

6 of 7 steps

Online Mode - Sync Licenses Task

## Select Devices

Select one or more devices

All Devices (5/47)

reachable

| 1 selected                          | Hostname            | Status | Chassis Number                           | Reachability | Device Model | IP Address | Tags |
|-------------------------------------|---------------------|--------|--|--------------|--------------|------------|------|
| <input checked="" type="checkbox"/> | cEdge_Site1_West_01 | -      | C8K-B23B869B-CA3E-970E-CFFF-2D1DB3E339AD | reachable    | C8000v       | 1.1.1.221  | --   |

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

Cisco Catalyst SD-WAN Assign HSEC License

7 of 7 steps

## Summary - Sync Licenses | Online

Review your request and make any changes. If you are satisfied, send the request.

^ **Selected Virtual Account** [Edit](#)

Virtual Account Name **sdwan-lab**

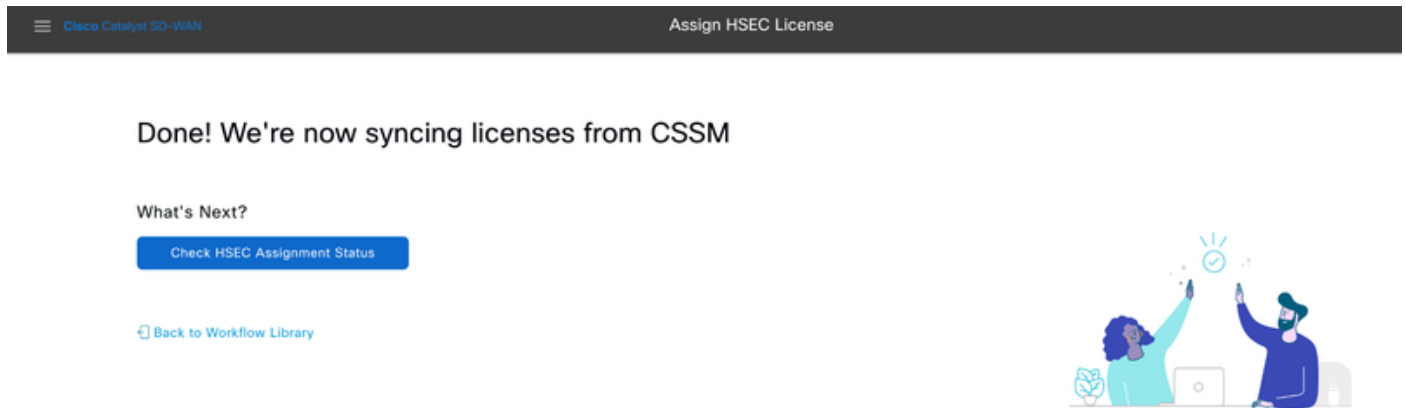
^ **Selected Devices** [Edit](#)

| Hostname            | Status | Chassis Number                           | Reachability | Device Model | IP Address | Tags |
|---------------------|--------|--|--------------|--------------|------------|------|
| cEdge_Site1_West_01 | -      | C8K-B23B869B-CA3E-970E-CFFF-2D1DB3E339AD | reachable    | C8000v       | 1.1.1.221  | --   |

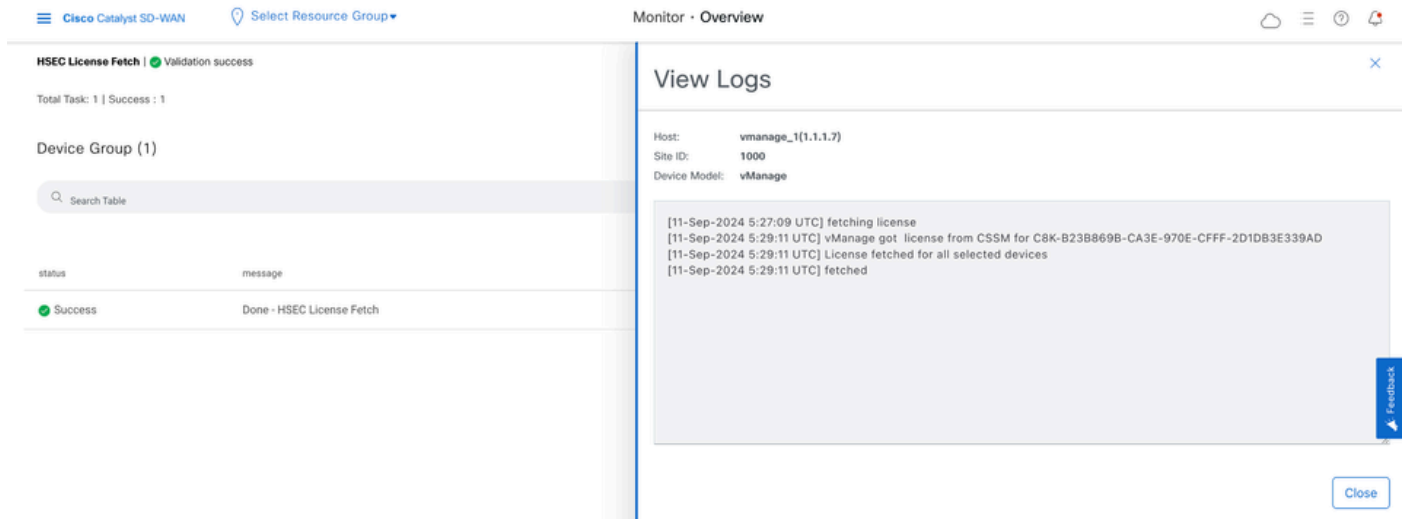
1 Record

Items per page: 25 1 - 1 of 1 |< < > >|

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



11.- Once the license is fetched from the CSSM 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**.

Cisco Catalyst SD-WAN

Monitor • Overview

Devices Tunnels Applications Security VPN Logs Multicloud

| CERTIFICATE STATUS | LICENSING                     | REBOOT           |
|--------------------|-------------------------------|------------------|
| 5<br>Warning       | 2<br>Assigned<br>5 Unassigned | 1<br>Last 24 hrs |

Workflow Library

POPULAR WORKFLOWS

- Quick Connect
- Firmware Upgrade
- Software Upgrade
- Sync and Install HSEC Licenses**
- Configure Teleworker Devices
- Create Configuration Group
- Deploy Configuration Group
- Create Security Policy
- Deploy Policy Group
- Create NFV Configuration Group

Monitor Configuration Tools Maintenance Administration Workflows Reports Analytics

Poor Performing Sites

Tunnel Health

17 Tunnels

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

Cisco Catalyst SD-WAN Assign HSEC License

1 of 3 steps

## Select License Task

To start, select one of the options:

Sync Licenses  
Sync licenses from CSSM for all devices.

**Install Licenses**  
Install licenses on devices.  
Note: In order to install, you should have already synced your licenses from CSSM.

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



Cisco Catalyst SD-WAN Assign HSEC License

2 of 3 steps

### Install Licenses Task

## Select Devices

Select one or more devices

All Devices (1/4)

C8K-B23B869B-CA3E-970E-CFFF-2D1DB3E339AD

1 selected

| <input checked="" type="checkbox"/> | Hostname            | Status  | Chassis Number                           | Reachability | Device Model | IP Address | Tags |
|-------------------------------------|---------------------|---------|--|--------------|--------------|------------|------|
| <input checked="" type="checkbox"/> | cEdge_Site1_West_01 | fetches | C8K-B23B869B-CA3E-970E-CFFF-2D1DB3E339AD | reachable    | C8000v       | 1.1.1.221  | --   |

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

Cisco Catalyst SD-WAN Assign HSEC License

3 of 3 steps

## Summary - Install Licenses

Review your request and make any changes. If you are satisfied, send the request.

### Selected Devices [Edit](#)

| Hostname            | Status  | Chassis Number                           | Reachability | Device Model | IP Address | Tags |
|---------------------|---------|--|--------------|--------------|------------|------|
| cEdge_Site1_West_01 | fetches | C8K-B23B869B-CA3E-970E-CFFF-2D1DB3E339AD | reachable    | C8000v       | 1.1.1.221  | --   |

1 Record Items per page: 25 1 - 1 of 1

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

Cisco Catalyst SD-WAN Assign HSEC License

## Done! We're now currently activating HSEC Devices

### What's Next?

[Check HSEC Assignment Status](#)

[Back to Workflow Library](#)

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

Configuration · Devices

HSEC License Install | Validation success Initiated By: ericgar

Total Task: 1 | Success : 1

Device Group (1)

Search Table

| status  | chassisNumber                            | message                    | startTime                 | Systemip  | Action |
|---------|--|----------------------------|---------------------------|-----------|--------|
| Success | C8K-B23B869B-CA3E-970E-CFFF-2D1DB3E339AD | HSEC Installation complete | Sep 10, 2024, 11:50:25 PM | 1.1.1.221 |        |

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

Configuration · Devices

## View Logs

Host: **cEdge\_Site1\_West\_01(1.1.1.221)**  
 Site ID: **100003**  
 Device Model: **C8000v**

```
[11-Sep-2024 5:50:25 UTC] Installing HSEC license
[11-Sep-2024 5:50:26 UTC] RPC call to device for initializing HSEC install is successful.
[11-Sep-2024 5:50:28 UTC] Last Confirmation code UDI: PID:C8000V,SN:C8K-B23B869B-CA3E-970E-CFFF-2D1DB3E339AD
Confirmation code: e293d6a0Import Data CompletedLast Confirmation code UDI: PID:C8000V,SN:C8K-B23B869B-CA3E-970E-CFFF-2D1DB3E339AD Confirmation code: e293d6a0
[11-Sep-2024 5:50:28 UTC] HSEC Installation complete
```

## Offline Workflow

### Sync Licenses with CSSM

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

**Cisco Catalyst SD-WAN**

Monitor > Configuration > Tools > Maintenance > Administration > **Workflows >** Reports > Analytics >

**Workflow Library**

POPULAR WORKFLOWS

- Quick Connect
- Firmware Upgrade
- Software Upgrade
- Sync and Install HSEC Licenses**
- Configure Teleworker Devices
- Create Configuration Group
- Deploy Configuration Group
- Create Security Policy
- Deploy Policy Group
- Create NFV Configuration Group

Monitor • Overview

Devices Tunnels Applications Security VPN Logs Multicloud

| CERTIFICATE STATUS | LICENSING                     | REBOOT           |
|--------------------|-------------------------------|------------------|
| 5<br>Warning       | 2<br>Assigned<br>5 Unassigned | 1<br>Last 24 hrs |

Poor Performing Sites ▾

Tunnel Health ⓘ

17  
Tunnels

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

# Welcome to Sync and Install HSEC Licenses

You can sync and install licenses on devices in online or offline mode.

Let's Do It

Don't show this to me again

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

☰ Cisco Catalyst SD-WAN Assign HSEC License

---

1 of 7 steps

## Select License Task

To start, select one of the options:

Sync Licenses  
Sync licenses from CSSM for all devices.

Install Licenses  
Install licenses on devices.

Note: In order to install, you should have already synced your licenses from CSSM.

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

2 of 6 steps

Sync Licenses

## Select Mode

To start, select the mode for syncing licenses

 Online Offline

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

3 of 6 steps

Offline Mode

## HSEC License Sync Overview

### A. Download Process

This process allows you to select HSEC-compatible devices to be added to HSEC device list file.

- Select HSEC-Compatible Devices
- Download HSEC Device List File
- Summary

### B. Upload Process

Once you've uploaded the HSEC device list file to CSSM, it will in turn, give you an authorization code file that needs to be uploaded here.

- Upload HSEC Device List File to CSSM and Download Authorization Code File
- Upload Authorization Code File
- Summary

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

4 of 6 steps

## Select Task

Before proceeding, select the task you would like to perform.

 Download Process

Select and download HSEC Device list file

This task allows you to select HSEC-compatible devices to be added to HSEC device list file. You will be then given a device list file to be uploaded to CSSM.

 Upload Process

Upload Authorization Code File

Use this task once you've downloaded the required authorization code file from CSSM.

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

5 of 6 steps

Assign HSEC License

Offline Mode - Sync Licenses Task

## Select Devices

Select one or more devices

All Devices (1/46)

CBK-19E2D66D-D5CC-6709-7A73-D050E231C407

1 selected

| <input checked="" type="checkbox"/> | Hostname           | Status | Chassis Number                           | Reachability | Device Model | IP Address | Tags |
|-------------------------------------|--------------------|--------|--|--------------|--------------|------------|------|
| <input checked="" type="checkbox"/> | cEdge_Sit1_East_01 | -      | CBK-19E2D66D-D5CC-6709-7A73-D050E231C407 | reachable    | C8000v       | 1.1.1.231  | --   |

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

6 of 6 steps

Assign HSEC License

## Summary - Sync Licenses | Offline | Download

Review your request and make any changes. If you are satisfied, send the request.

^ **Selected Devices** [Edit](#)

| Hostname           | Status | Chassis Number                           | Reachability | Device Model | IP Address | Tags |
|--------------------|--------|--|--------------|--------------|------------|------|
| cEdge_Sit1_East_01 | -      | CBK-19E2D66D-D5CC-6709-7A73-D050E231C407 | reachable    | C8000v       | 1.1.1.231  | --   |

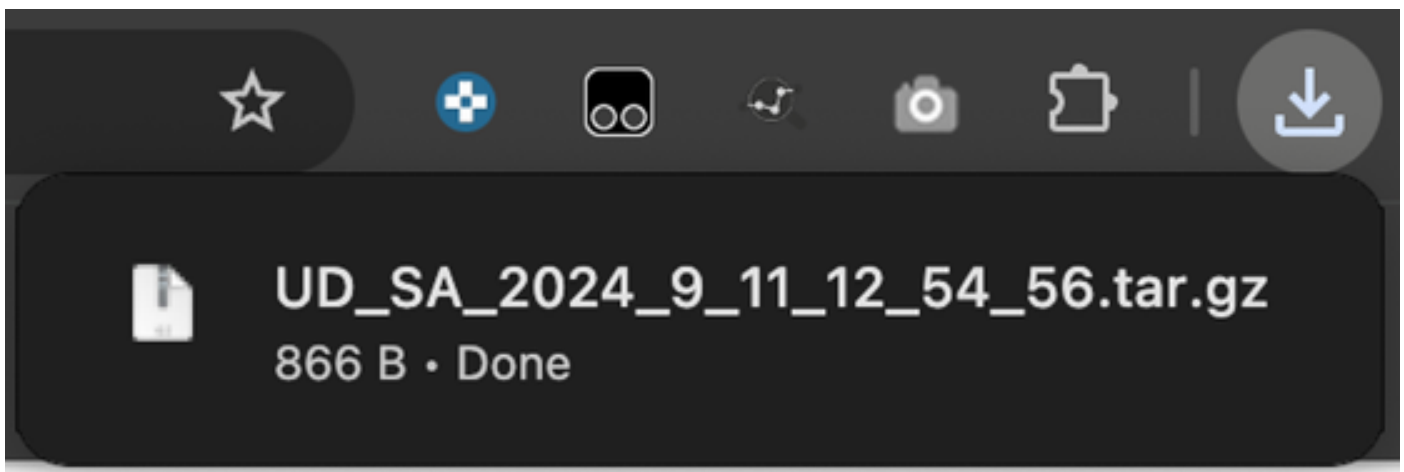
1 Record

Items per page: 25 1 - 1 of 1

^ **Download HSEC Device List**

[Download HSEC Device File \(.SUDI\)](#)

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



A mobile notification bar is shown with a dark background. On the left, there is a file icon. To its right, the text reads "UD\_SA\_2024\_9\_11\_12\_54\_56.tar.gz" in a large, white, sans-serif font. Below this, in a smaller white font, it says "866 B • Done". On the far right of the notification bar, there is a white download icon (a square with a downward-pointing arrow).

10.- Click on **Open Cisco Smart Software Manager** or navigate to: [Cisco Software Central](#).

## Done! You've generated and downloaded your HSEC Device list file

Now that you've generated and downloaded your HSEC device list file, it's time to upload the SUDI file into CSSM. Once CSSM generates the Smart License Authorization Code (SLAC) file, upload it to vManage.

### What's Next?

[Open Cisco Smart Software Manager](#)

[Upload Authorization Code File](#)

[Back to Workflow Library](#)



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

Cisco Software Central

Smart Software Licensing

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

Report | **Usage Data Files** | Reporting Policy | Synch File for Device Controllers

Devices can be configured to report the features that they are using. This usage then determines which licenses are needed, in order to be compliant.

[Upload Usage Data...](#) | Search by File Name, Virtual Account

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

## Upload Usage Data

Please select the Usage File you wish to upload.

\* Usage Data File:

[Browse](#)

UD\_SA\_2024\_9\_11\_12\_54\_56.tar.gz


1

2

[Upload Data](#)

[Cancel](#)

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

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

Cisco Software Central > Smart Software Licensing Cisco Systems, TAC

## Smart Software Licensing SL Product Details Support Help




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

### Reports

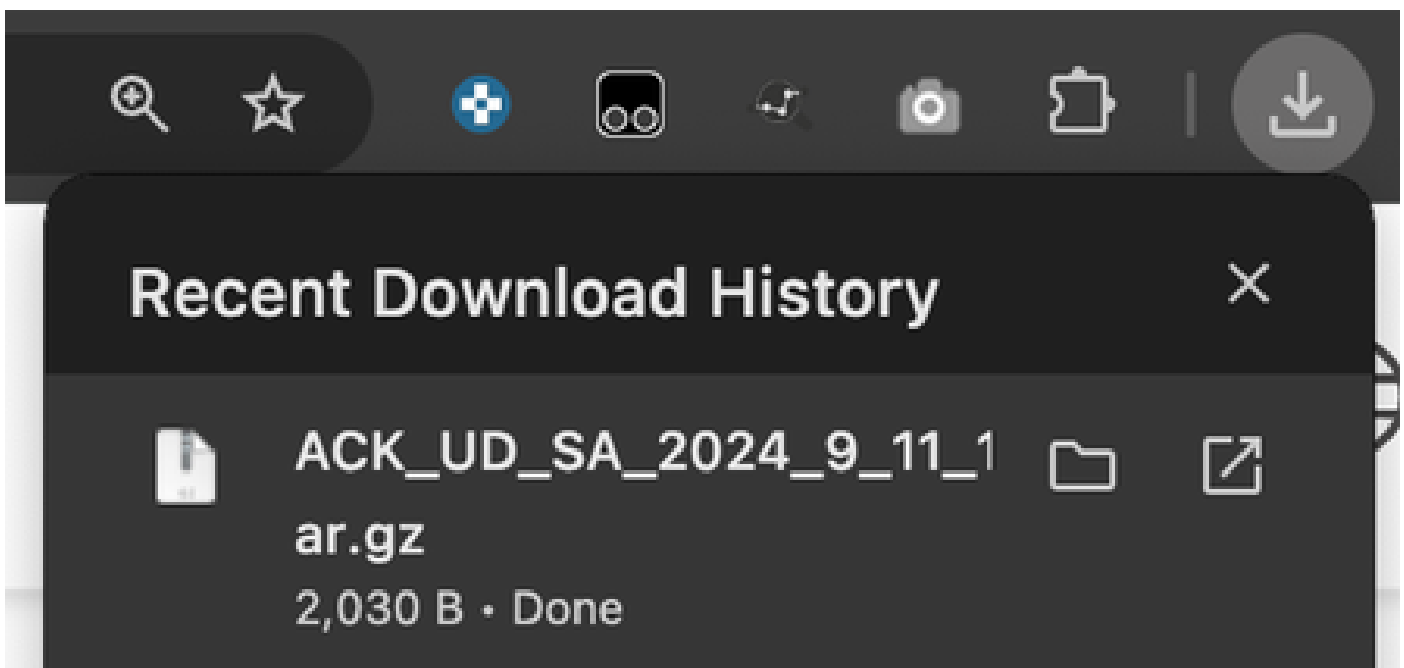
Report | **Usage Data Files** | Reporting Policy | Synch File for Device Controllers

Devices can be configured to report the features that they are using.  
This usage then determines which licenses are needed, in order to be compliant.

Upload Usage Data... Search by File Name, Virtual Account

| Usage Data File   | Reported    | Virtual Account | Reporting Status  | Devices | Acknowledgement          |
|---|-------------|-----------------|---|---------|--------------------------|
|  UD_SA_2024_9_11_12_54_56.tar.gz | 2024-Sep-11 | sdwan-lab       |  No Errors | 1       | <a href="#">Download</a> |
| UD_VA_2024_09_11_18_54_33.tar.gz  |             | sdwan-lab       |  No Errors | 1       |                          |

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.**



4 of 6 steps

## Select Task

Before proceeding, select the task you would like to perform.

Download Process

Select and download HSEC Device list file

This task allows you to select HSEC-compatible devices to be added to HSEC device list file. You will be then given a device list file to be uploaded to CSSM.

Upload Process

Upload Authorization Code File


Use this task once you've downloaded the required authorization code file from CSSM.

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

5 of 6 steps


## Upload Smart License Authorization Code File

Upload the Authorization Code (SLAC) file generated by CSSM.



**Choose a file** or drag and drop to upload.

Accepted files: .gz  
Accepted sizes: up to 10MB

ACK\_UD\_SA\_2024\_9\_11\_12... .gz 

**Upload**

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

6 of 6 steps

## Summary - Sync Licenses | Offline | Upload

Review your request and make any changes. If you are satisfied, send the request.

### ^ Device Entries [Edit](#)

| Hostname           | Status | Chassis Number                           | Reachability | Device Model | IP Address | Tags |
|--------------------|--------|--|--------------|--------------|------------|------|
| cEdge_Sit1_East_01 | Fetchd | C8K-19E2066D-D5CC-6709-7A73-D050E231C407 | -            | C8000v       | 1.1.1.231  | --   |

Done! We're now currently syncing smart account authorization code (SLAC) file for the devices

### Install fetched licenses

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

1 of 3 steps

## Select License Task

To start, select one of the options:

Sync Licenses

Sync licenses from CSSM for all devices.

Install Licenses

Install licenses on devices.

Note: In order to install, you should have already synced your licenses from CSSM.

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


Cisco Catalyst SD-WAN Assign HSEC License

2 of 3 steps

### Install Licenses Task

## Select Devices

Select one or more devices

All Devices (1/5) 

🔍 CBK-19E2D66D-D5CC-6709-7A73-D050E231C407

1 selected

| <input checked="" type="checkbox"/> | Hostname           | Status  | Chassis Number                           | Reachability | Device Model | IP Address | Tags |
|-------------------------------------|--------------------|---------|--|--------------|--------------|------------|------|
| <input checked="" type="checkbox"/> | cEdge_Sit1_East_01 | fetches | CBK-19E2D66D-D5CC-6709-7A73-D050E231C407 | reachable    | C8000v       | 1.1.1.231  | --   |

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

Cisco Catalyst SD-WAN Assign HSEC License

3 of 3 steps





## Summary - Install Licenses

Review your request and make any changes. If you are satisfied, send the request.

^ **Selected Devices** [Edit](#)


| Hostname           | Status  | Chassis Number                           | Reachability | Device Model | IP Address | Tags |
|--------------------|---------|--|--------------|--------------|------------|------|
| cEdge_Sit1_East_01 | fetches | CBK-19E2D66D-D5CC-6709-7A73-D050E231C407 | reachable    | C8000v       | 1.1.1.231  | --   |


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


Cisco Catalyst SD-WAN Select Resource Group Monitor · Overview    


HSEC License Install | ● Validation success Initiated By: ericgar

Total Task: 1 | Success : 1

Device Group (1) 

🔍 Search Table 

As of: Sep 11, 2024 01:04 PM 

| status                                       | chassisNumber                            | message                    | startTime                | Systemip  | Action  |
|--|--|----------------------------|--------------------------|-----------|---|
| <span style="color: green;">●</span> Success | CBK-19E2D66D-D5CC-6709-7A73-D050E231C407 | HSEC Installation complete | Sep 11, 2024, 1:04:13 PM | 1.1.1.231 |  |

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

## View Logs

Host: cEdge\_Sit1\_East\_01(1.1.1.231)  
Site ID: 100004  
Device Model: C8000v

```
[11-Sep-2024 19:04:13 UTC] Installing HSEC license  
[11-Sep-2024 19:04:17 UTC] RPC call to device for initializing HSEC install is successful.  
[11-Sep-2024 19:04:19 UTC] Last Confirmation code UDI: PID:C8000V,SN:C8K-19E2D66D-D5CC-6709-7A73-D050E231C407  
Confirmation code: a599674eImport Data CompletedLast Confirmation code UDI: PID:C8000V,SN:C8K-19E2D66D-D5CC-  
6709-7A73-D050E231C407 Confirmation code: a599674e  
[11-Sep-2024 19:04:19 UTC] HSEC Installation complete
```

[Feedback](#)

## 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.

```
<#root>
```

```
EdgeRouter#
```

```
license smart authorization return local online
```

```
Operation cannot be completed because license is in use
```

```
EdgeRouter#
```

```
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.


```
<#root>
```

```
EdgeRouter#
```

```
controller-mode disable
```

Disabling controller mode erases the nvram filesystem, remove all configuration files, and reload the boot image. 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 Edge Router 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 Cisco DNA export-controlled license resides in. If there is no active token, generate a new one.

Complete the same procedure as in Edge Router to generate a trust established with the CSSM.

```
<#root>
```

```
EdgeRouter#
```

```
configure terminal
```

```
EdgeRouter(config)#
```

```
license smart transport smart
```

```
EdgeRouter(config)#
```

```
license smart url default
```

```
EdgeRouter(config)#
```

```
end
```


EdgeRouter#

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

EdgeRouter#

```
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.

<#root>

EdgeRouter#

```
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.

<#root>

EdgeRouter#

```
show logging | include SMART
```

```
*Aug 18 22:00:22.998: %SMART_LIC-6-AUTHORIZATION_REMOVED: A licensing authorization code has been removed
```

```
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" authorization
```

---

 **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. Complete 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.

```
<#root>
```

```
EdgeRouter#
```

```
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

X

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**.

## Activation - Is Reload Required?

**Is it true that on 8500-based platforms a reload is required for HSEC to get 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'** 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'** 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 the CSSM 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 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 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
```



```
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 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
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.

```

<#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 CSSM 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](#)