



# Smart Licensing Using Policy (SLP)

- [SLP Overview, on page 1](#)
- [Customer Topologies, on page 3](#)
- [License Installation Procedure - Full Offline Access Topology, on page 4](#)
- [License Installation Procedure - CSLU has No Access to CSSM, on page 9](#)
- [License Installation Process in the Router, on page 20](#)
- [HSEC Installation, on page 21](#)

## SLP Overview

Smart Licensing Using Policy (SLP), previously known as Smart Licensing Enhanced (SLE), is the default mode with IOS-XE release 17.3.2. SLE replaces Smart Software Licensing. The IR8340 router only supports SLP. Some of the feature differences are:

- An Authorization Code is required only for export control requirement
- Throughput greater than 250 Mbps requires an HSEC license
- No more EVAL licenses. Authorized status has changed to In Use or Not In Use with an Enforcement Type class.
- Cisco Smart Licensing Utility (CSLU) is a new tool interfacing between the devices and Cisco Smart Software Manager (CSSM) in specific customer topologies.

## License Enforcement Types

A given license belongs to one of three enforcement types. The enforcement type indicates if the license requires authorization before use, or not.

- Unenforced or Not Enforced

The vast majority of licenses belong to this enforcement type. Unenforced licenses do not require authorization before use in air-gapped networks, or registration, in connected networks. The terms of use for such licenses are as per the end user license agreement (EULA).

- Enforced

Licenses that belong to this enforcement type require authorization before use. The required authorization is in the form of an authorization code, which must be installed in the corresponding product instance.

An example of an enforced license is the Media Redundancy Protocol (MRP) Client license, which is available on Industrial Ethernet Switches.

- Export-Controlled

Licenses that belong to this enforcement type are export-restricted by U.S. trade-control laws and these licenses require authorization before use. The required authorization code must be installed in the corresponding product instance for these licenses as well. Cisco may pre-install export-controlled licenses when ordered with hardware purchase.

An example of an export-controlled license is the High Security (HSEC) license, which is available on certain Cisco Routers.

## SLP Architecture

This section explains the various components that can be part of your SLP implementation.

### Product Instance

A product instance is a single instance of a Cisco product, identified by a Unique Device Identifier (UDI).

A product instance records and reports license usage (RUM reports), and provides alerts and system messages about overdue reports, communication failures, etc. The RUM reports and usage data are also stored securely in the product instance.

A Resource Utilization Measurement report (RUM report) is a license usage report, which fulfills reporting requirements as specified by the policy. RUM reports are generated by the product instance and consumed by CSSM. The product instance records license usage information and all license usage changes in an open RUM report. At system-determined intervals, open RUM reports are closed and new RUM reports are opened to continue recording license usage. A closed RUM report is ready to be sent to CSSM.

A RUM acknowledgement (RUM ACK or ACK) is a response from CSSM and provides information about the status of a RUM report. Once the ACK for a report is available on the product instance, it indicates that the corresponding RUM report is no longer required and can be deleted.

CSSM displays license usage information as per the last received RUM report.

### Cisco Smart Software Manager (CSSM)

CSSM is a portal that enables you to manage all your Cisco software licenses from a centralized location. CSSM helps you manage current requirements and review usage trends to plan for future license requirements.

You can access CSSM at <https://software.cisco.com>. Under the License tab, click the Smart Software Licensing link.

In CSSM you can:

- Create, manage, or view virtual accounts.
- Create and manage Product Instance Registration Tokens.
- Transfer licenses between virtual accounts or view licenses.
- Transfer, remove, or view product instances.
- Run reports against your virtual accounts.
- Modify your email notification settings.
- View overall account information.

Prior to using CSSM, please view a short video about how to use the portal found here:

<https://www.cisco.com/c/en/us/buy/smart-accounts/software-manager.html>

Click on the **View Video** button.

## Cisco Smart Licensing Utility (CSLU)

CSLU is a Windows-based reporting utility that provides aggregate licensing work-flows. It helps you administer all your licenses and their associated product instances from your premises instead of having to connect to CSSM.

This utility performs the following key functions:

- Provides the options relating to how work-flows are triggered. The work-flows can be triggered by CSLU or by the product instance
- Collects usage reports from the product instance and upload these usage reports to the corresponding smart account or virtual account – online, or offline, using files. Similarly, the RUM report ACK is collected online, or offline, and provided back to the product instance.
- Sends authorization code requests to CSSM and receives authorization codes<sup>1</sup> from CSSM.

CSLU can be part of your SLE topology in the following ways:

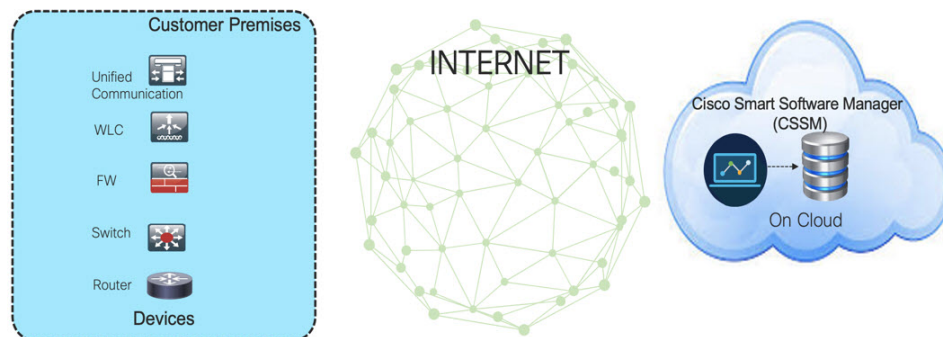
- Install the windows application, to use CSLU as a standalone tool and connect it to CSSM.
- Install the windows application, to use CSLU as a standalone tool and not connect it to CSSM. With this option, the required usage information is downloaded to a file and then uploaded to CSSM. This is suited to air-gapped networks.
- Embed it in a controller such as Cisco DNA Center.

## Customer Topologies

IoT Routing platforms use two different topologies.

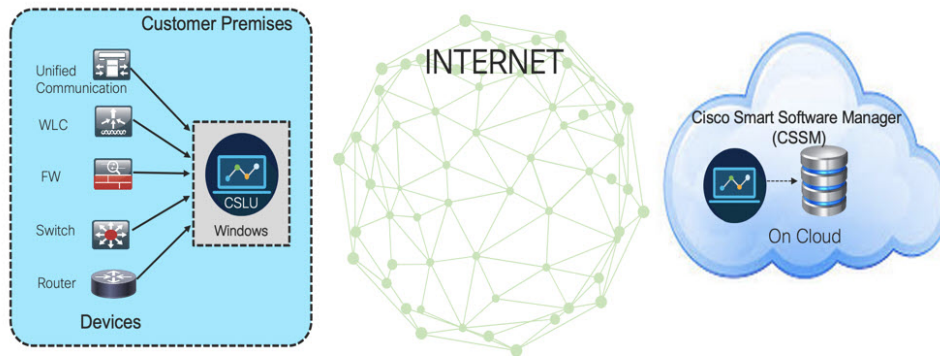
- Full Offline Access
- CSLU has No Access to CSSM

The following figure illustrates the Full Offline Access:



In this topology, devices do not have connectivity to CSSM (software.cisco.com). The user must copy and paste information between Cisco products and CSSM to manually check in and out licenses.

The following figure illustrates the CSLU having No Access to CSSM:



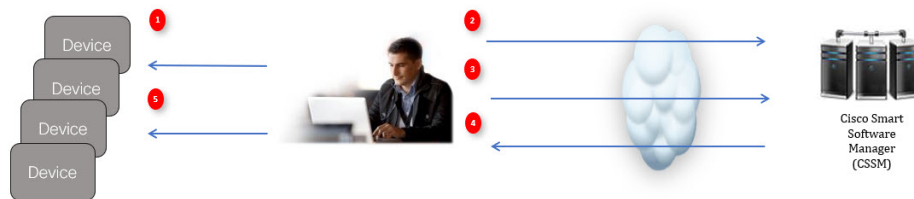
In this topology the devices are connected to the CSLU controller, but there is no connectivity between CSLU and CSSM (Cisco Smart Software Manager – software.cisco.com).

Cisco devices will send usage information to a locally installed CSLU. The user must copy and paste information between the CSLU and CSSM to manually check-in and check-out licenses.

## License Installation Procedure - Full Offline Access Topology

This procedure requires a manual exchange of required information between the router and CSSM.

Refer to the following graphic for the flow of information:



1. Generate a License Usage Data file or AuthCode Request.
2. Export to CSSM.
3. Upload License Usage Data or AuthCode Request.
4. Export ACK/AuthRequest file to Router.
5. Upload ACK file or AuthRequestAuthCode

## Procedure to Register Product Instance in CSSM

### Procedure

#### Step 1

Generate a license usage file from the Router.

In exec mode, perform the following:

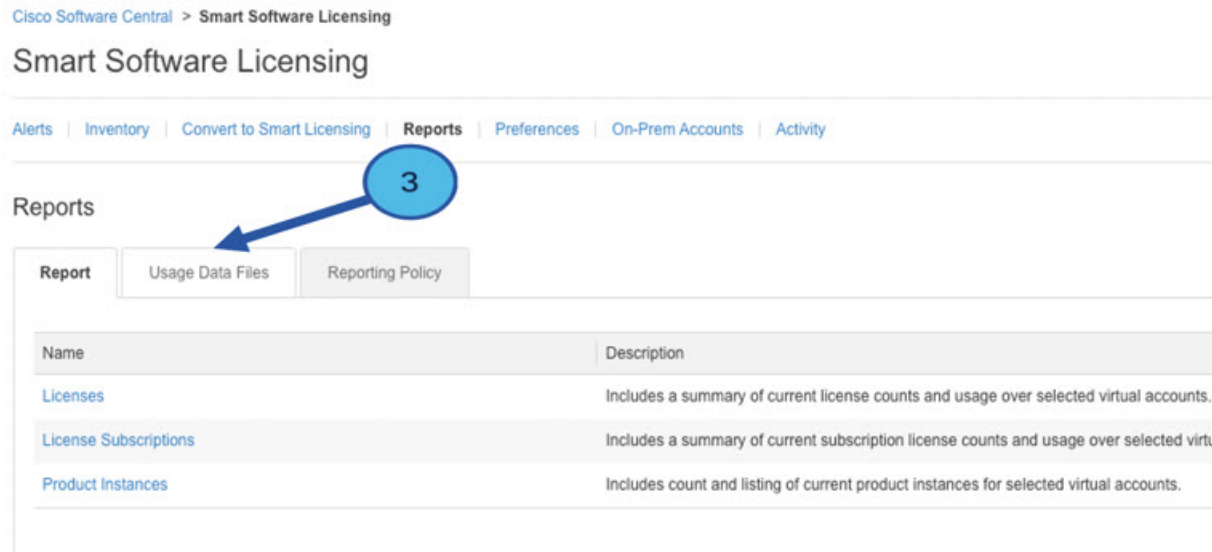
#### Example:

```
Router# license smart save usage all file flash:sle
```

**Step 2** Export the license usage file (sle) to your host laptop/PC.

**Step 3** Importing the license usage file to CSSM on Cloud. Click on the **Usage Data Files** tab.

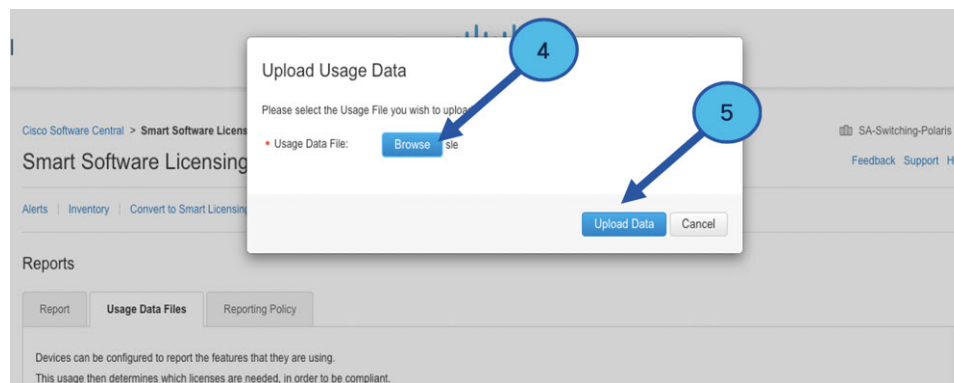
**Figure 1: Usage Data File**



**Step 4** The **Upload Usage Data** window appears. Click **Browse**, and navigate to where the file is.

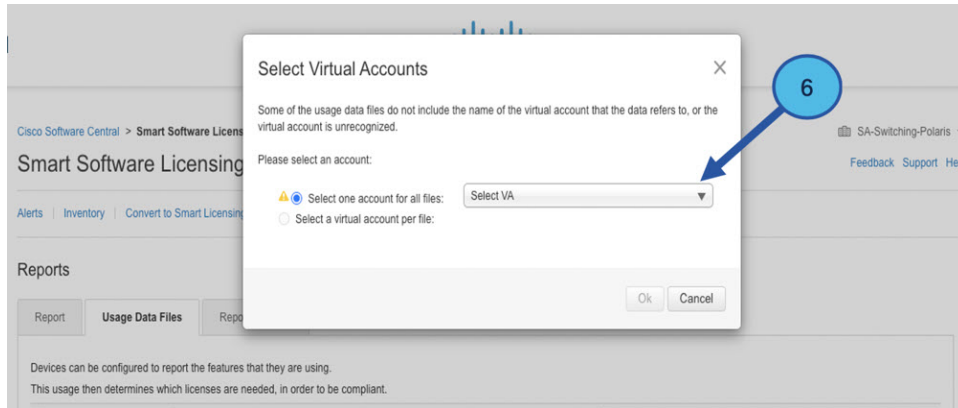
**Step 5** Click on **Upload Data**.

**Figure 2: Browse and Upload**



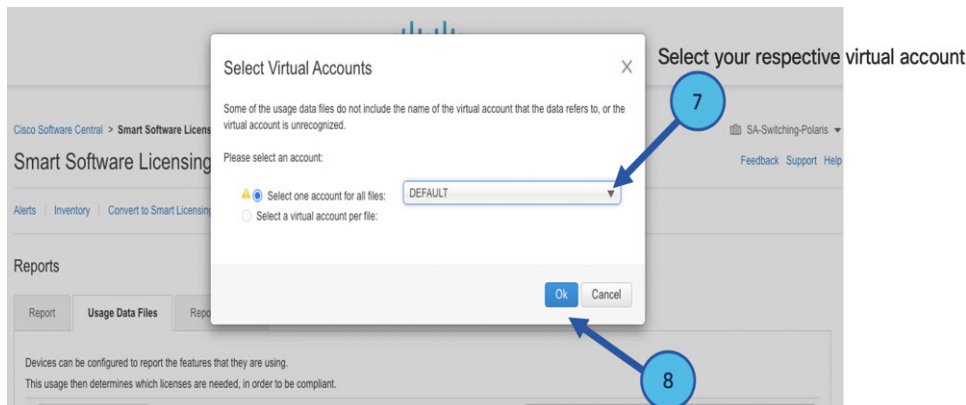
**Step 6** Select the Virtual Account.

Figure 3: Select Account



**Step 7** From the pull-down, select your respective virtual account.

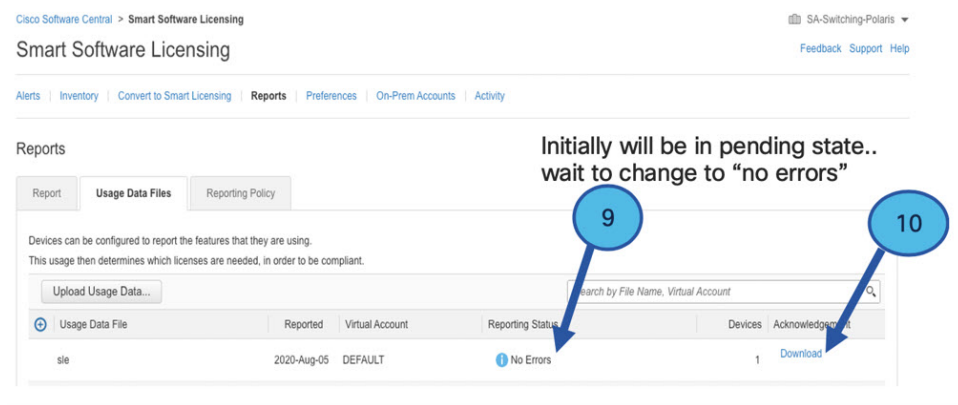
Figure 4: Select Your Account



**Step 8** Click **Ok**.

**Step 9** Observe the Smart Software Licensing window. Initially, the Reporting Status state will be **Pending**. Wait until the window reflects **No Errors** before continuing.

Figure 5: Reporting Status



**Step 10** Click **Download** to download the ACK file.

**Step 11** Check under the **Product Instances** tab to verify your device is listed.

**Figure 6: Product Instances**

Virtual Account: VA-Blackheart Minor Hide Alerts

General Licenses **Product Instances** Event Log

Authorize License-Enforced Features... Search by Name, Product Type

Name	Product Type	Last Contact	Alerts	Actions
UDI_PID:ESR-6300-CON-K9; UDI_SN:FOC23032UWF;	5900	2020-Sep-24 20:23:59 (Reserved Licenses)		Actions
UDI_PID:ESR-6300-CON-K9; UDI_SN:SJC19700415;	5900	2020-Sep-24 20:41:41 (Reserved Licenses)		Actions
UDI_PID:IR1101-K9; UDI_SN:FCW24150J0F;	IR1100	2020-Jul-30 02:22:04		Actions
UDI_PID:IR1833-K9; UDI_SN:FCW2420POVB;	M2M800	2020-Jul-07 20:15:11 (Reserved Licenses)		Actions
UDI_PID:IR1835-K9; UDI_SN:FHH2416P002;	M2M800	2020-Sep-30 01:01:21		Actions
UDI_PID:IR8140H-P-K9; UDI_SN:FDO2420J786;	CGR1000	2020-Sep-08 18:37:24		Actions

Showing All 6 Records

**Step 12** Import the ACK file from CSSM to your device using the command line interface.

## Importing the ACK file from CSSM to your Device

### Procedure

**Step 1** Copy the ACK file from CSSM to your host laptop or usbflash device. In exec mode on the device:

#### Example:

```
Router#license smart import bootflash: ACK_sle
Import Data Successful
Router#
*Sep 1 21:12:58.576: %SIP-1-LICENSING: SIP service is Up. License report acknowledged.
*Sep 1 21:12:58.616: %SMART_LIC-6-POLICY_INSTALL_SUCCESS: A new licensing policy was
successfully installed
```

**Step 2** Verify Product Instance has imported the data

#### Example:

```
Router# show license usage
License Authorization:
  Status: Not Applicable
network-advantage_250M (IR8340_P_250M_A):
  Description: network-advantage_250M
  Count: 1
  Version: 1.0
  Status: IN USE
  Export status: NOT RESTRICTED
  Feature Name: network-advantage_250M
  Feature Description: network-advantage_250M
  Enforcement type: NOT ENFORCED
```

**Step 3** Verify the license is in use.

**Example:**

```

Router# show license summary
License Usage:
License                               Entitlement tag          Count  Status
-----
network-advantage_250M (IR8340_P_250M_A) 1      IN USE

Router#
Router#show license all | beg Usage Reporting:
Usage Reporting:
  Last ACK received: Sep 01 21:12:58 2020 UTC
  Next ACK deadline: <none>
  Reporting Interval: 0 (no reporting)
  Next ACK push check: <none>
  Next report push: <none>
  Last report push: <none>
  Last report file write: <none>
Trust Code Installed: Sep 01 00:28:48 2020 UTC

```

## Removing the Device from CSSM

### Procedure

**Step 1** Navigate back to the product instances tab. Locate your device.

*Figure 7: Product Instances*

The screenshot shows the Cisco Smart Licensing Inventory web interface. The 'Product Instances' tab is active. A table displays the following data:

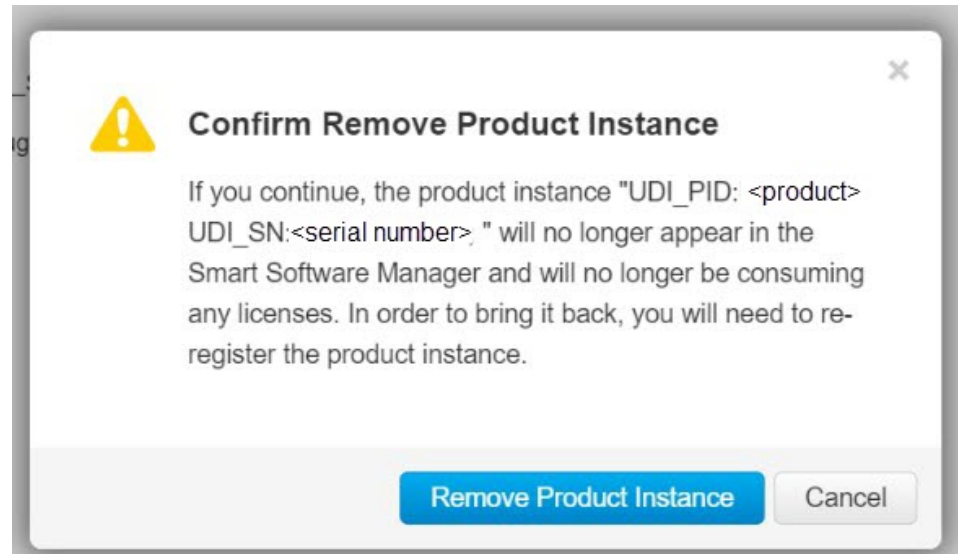
Name	Product Type	Last Contact	Alerts	Actions
UDI_PID:IE-3300-8U2X; UDI_SN:FCW24030HD6;	IE3000	2020-Aug-14 12:25:07 (Reserved Licenses)		Actions ▾
UDI_PID:IE-3400-8T2S; UDI_SN:FOC2330V02D;	IE3000	2020-Aug-14 12:14:00 (Reserved Licenses)		Actions ▾
UDI_PID:IE-3400H-24T; UDI_SN:FCW23200H5S;	IE3000	2020-Sep-24 07:43:31		Actions ▾
UDI_PID:IR1835-K9; UDI_SN:FHH2416P00Z;	M2M800	2020-Oct-01 05:48:27 (Reserved Licenses)		Actions ▾
UDI_PID:IR8140H-P-K9; UDI_SN:FDO241519G8;	CGR1000	2020-Aug-12 17:14:56 (Reserved Licenses)		Actions ▾
UDI_PID:IR8140H-P-K9; UDI_SN:FDO2420J4ZK;	CGR1000	2020-Sep-24 21:01:56 (Reserved Licenses)		Actions ▾
UDI_PID:IR8140H-P-K9; UDI_SN:FDO2420J64L;	CGR1000	2020-Sep-26 00:39:13		Actions ▾
UDI_PID:IR8140H-P-K9; UDI_SN:FDO2420J77G;	CGR1000	2020-Sep-08 22:10:30		Actions ▾

The 'Remove...' option in the context menu is highlighted with a blue circle.

**Step 2** Click on **Actions** beside your device, and from those options click **Remove**.  
The Confirm Remove Product Instance window appears.



Figure 8: Confirm Remove Product Instance

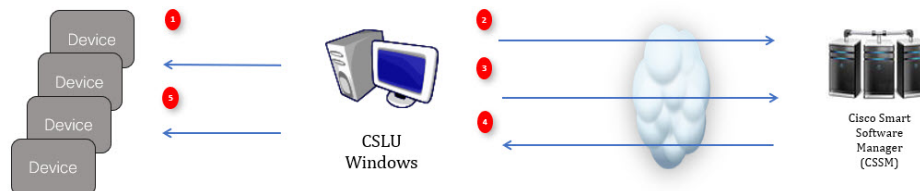


**Step 3** Click **Remove Product Instance**.

## License Installation Procedure - CSLU has No Access to CSSM

This procedure performs an online exchange of required information between the Router and CSLU.

Refer to the following graphic for the flow of information:



### Procedure

- Step 1** In CSLU, identify the devices that require an AuthCode, and initiate the request. An AuthCode file is created.
- Step 2** Export the AuthCode file to CSSM.
- Step 3** Upload the AuthCode to CSSM SA/VA account.
- Step 4** Export the AuthRequestAuthcode file to CSLU.
- Step 5** Upload ACK file or AuthRequestAuthCode

## Procedure when devices are connected to the CSLU

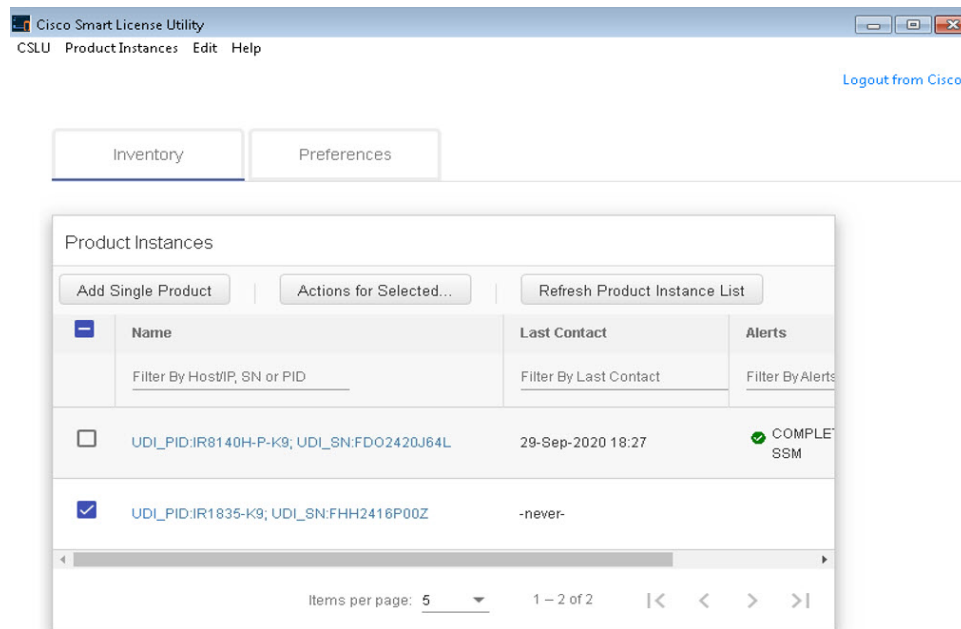
First, perform these steps on the router using the CLI to get a license UDI:

```
Router#show license summary
License Reservation is ENABLED
License Usage:
License Entitlement tag Count Status
-----
network-essentials_250M (IR8340_P_250M_E) 1 IN USE
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#platform hardware throughput level 2G
% 2G throughput level requires hseck9 license!
Router(config)#end
Router#sh license udi
UDI: PID:IR1835-K9,SN:FHH2416P00Z
```

### Procedure

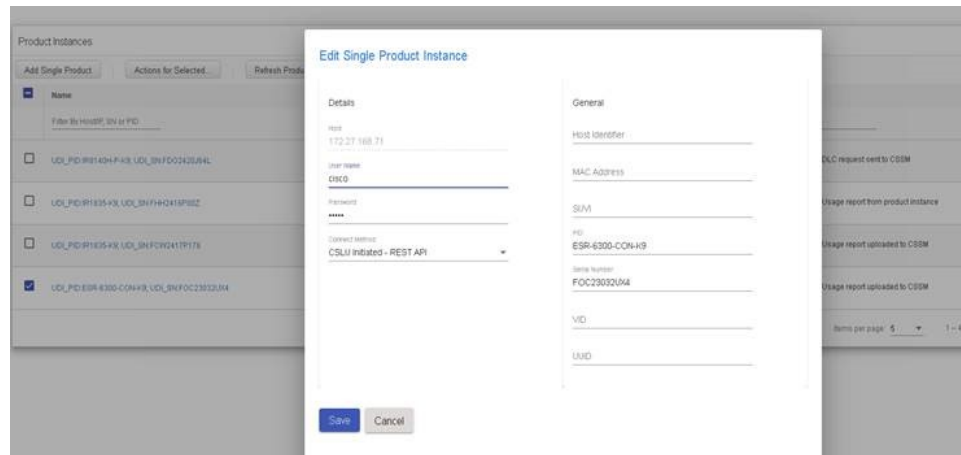
- Step 1** Open the Cisco Smart License Utility (CSLU).
- Step 2** Navigate to the **Product Instances** tab, then click on the UDI.

*Figure 9: Select UDI*



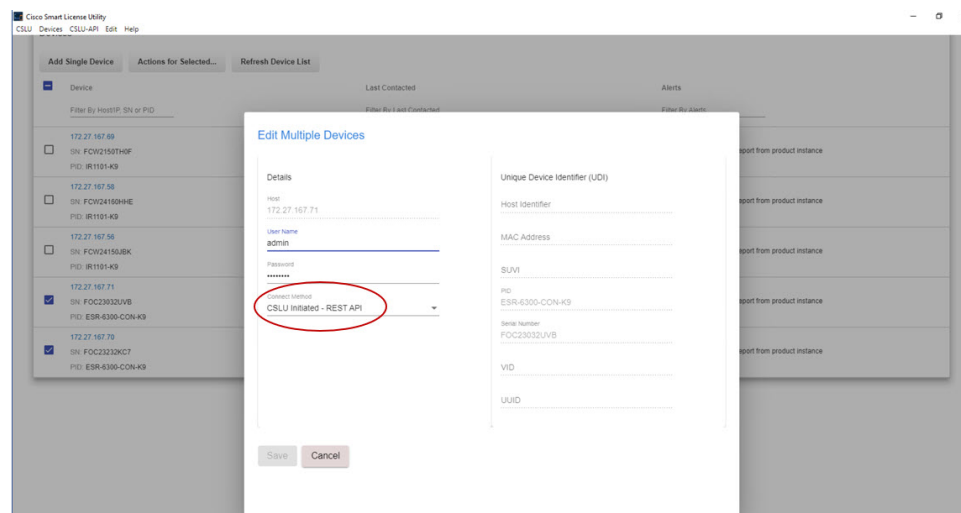
- Step 3** The **Edit Single Product Instance** window appears.

Figure 10: Edit Single Product Instance



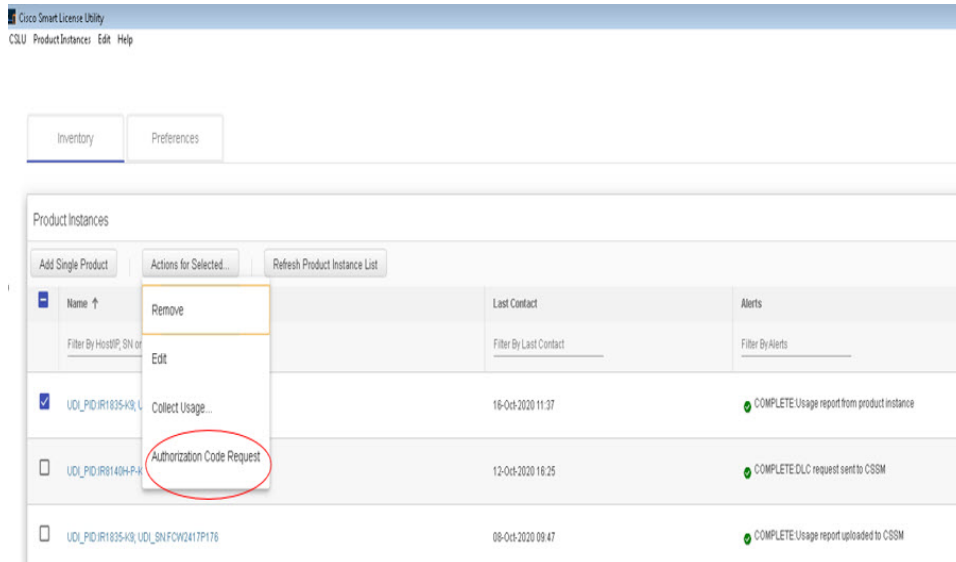
**Step 4** The **Edit Multiple Devices** window appears. Supply your account password and click **Save**.

Figure 11: Edit Multiple Devices



**Step 5** In the **Product Instances** window, click on the **Actions for Selected Devices** Tab.

Figure 12: Actions for Selected Devices



**Step 6** Select **Authorization Code Request**.

**Step 7** The **Authorization Request Information** window appears. Read the contents and then click **Accept**.

Figure 13: Authorization Request Information

### Authorization Request Information

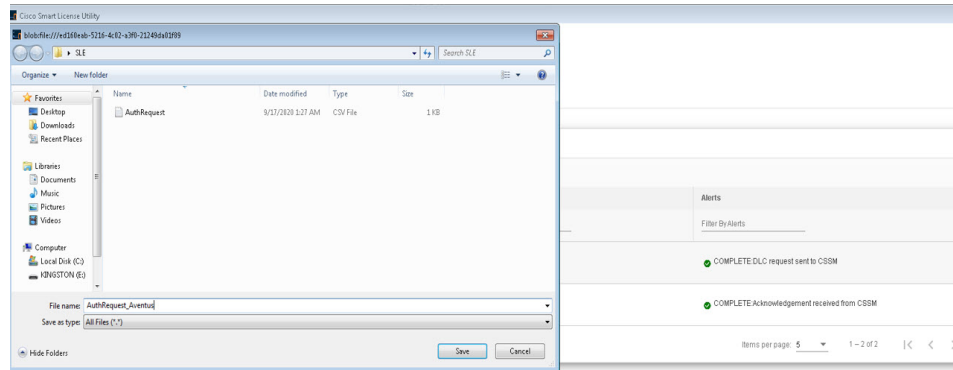
This operation will download an authorization request file for the devices that have been selected. Once this file is downloaded please:

1. Upload the file to CSSM.
2. After uploading to CSSM you will be able to download the file containing the authorization codes for devices you selected.
3. Please upload this file using the "Upload From CSSM" menu option to apply the authorization codes for the devices.



**Step 8** The CSLU downloads a Authorization Request file to your laptop. Click **Save**.

Figure 14: Authorization Request File



## Exporting the AuthRequest File to CSSM

The next step is to take the Authorization Request file you just saved, and export it into Cisco Smart Software Manager (CSSM).

Launch CSSM.

Click on the **Inventory** Tab, select your Virtual Account.

### Procedure

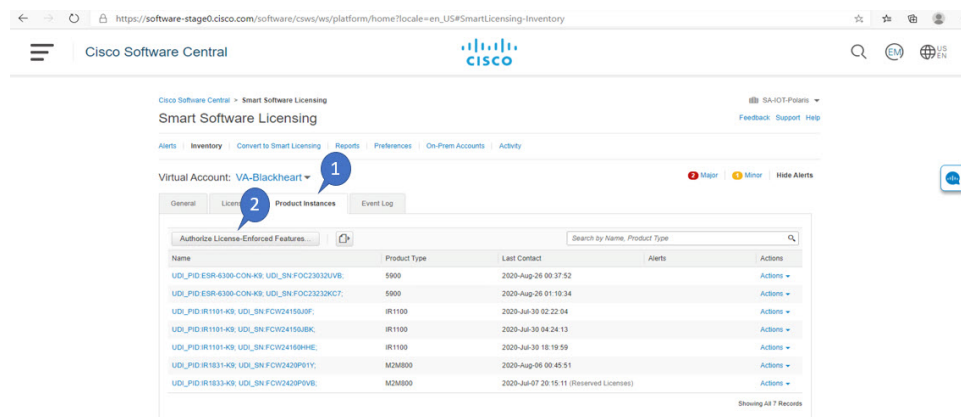
#### Step 1

Click on the **Product Instances** Tab.

#### Step 2

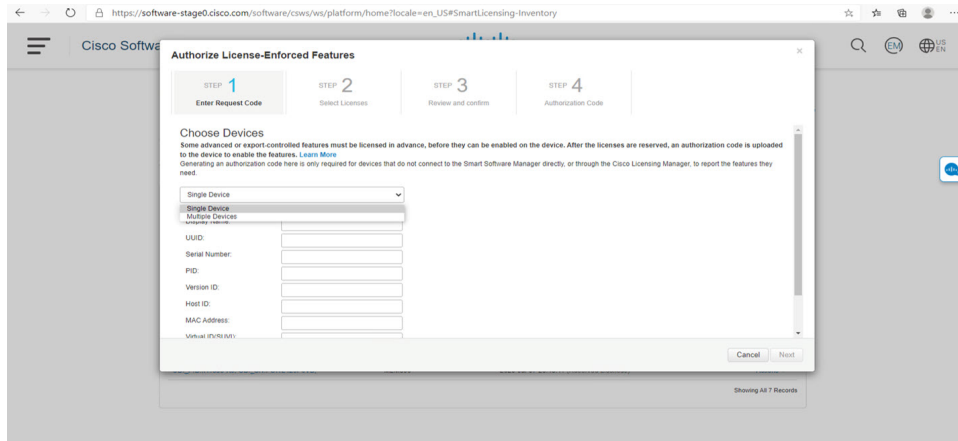
Click on **Authorize License-Enforced Features**.

Figure 15: Authorize License-Enforced Features



The **Authorize License-Enforced Features** window appears.

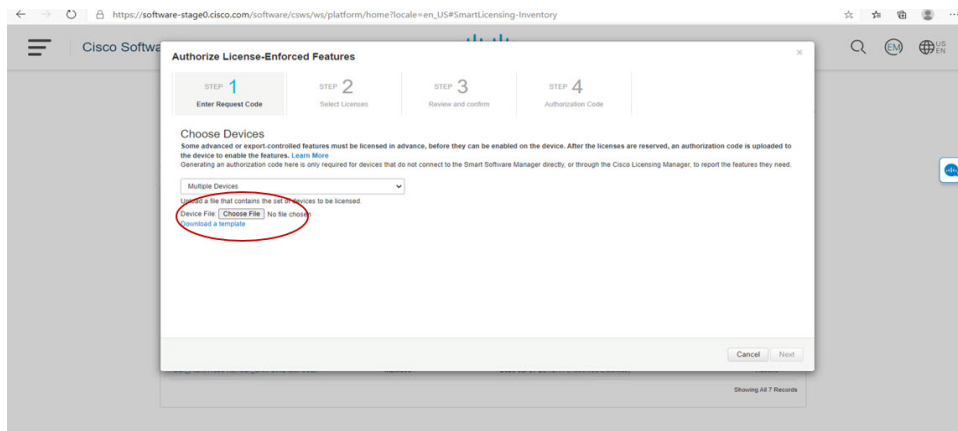
Figure 16: Authorize License-Enforced Features

**Step 3**

Choose **Multiple** or **Single** devices from the pull-down.

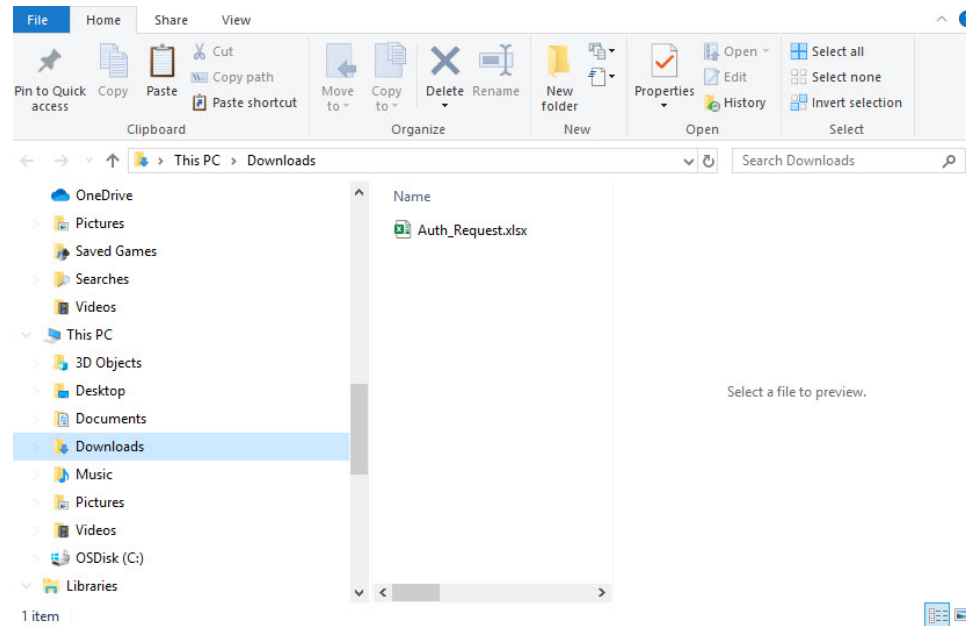
**Step 4**

The window changes to an option to select a device file. Click on **Choose File**.

**Step 5**

A popup window opens to navigate to where you saved your Authorization Request file on your laptop.

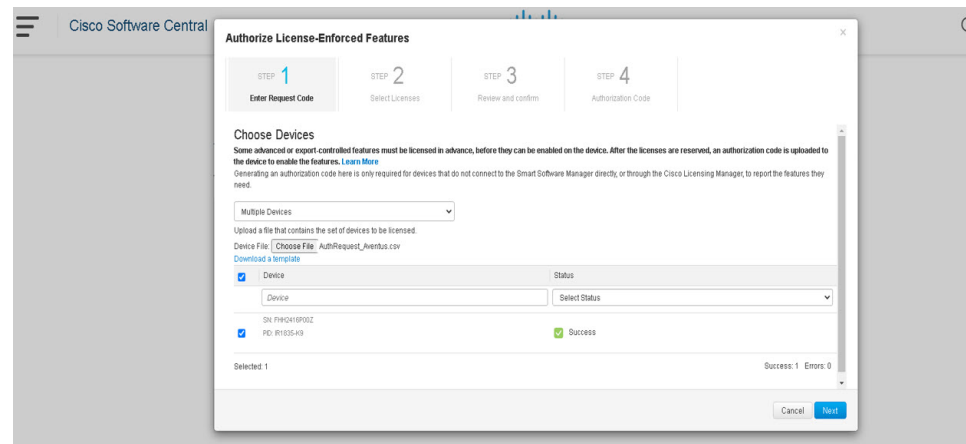
Figure 17: Open File Navigation Window



**Step 6** Select your file, and then click **Open**.

**Step 7** The authorization file loads, and the window changes to present your devices.

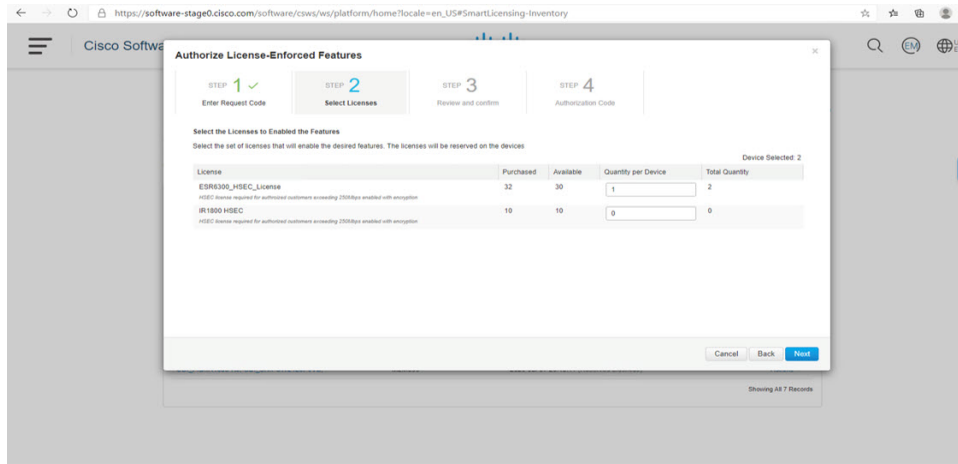
Figure 18: Present Devices



**Step 8** When successful, click **Next**.

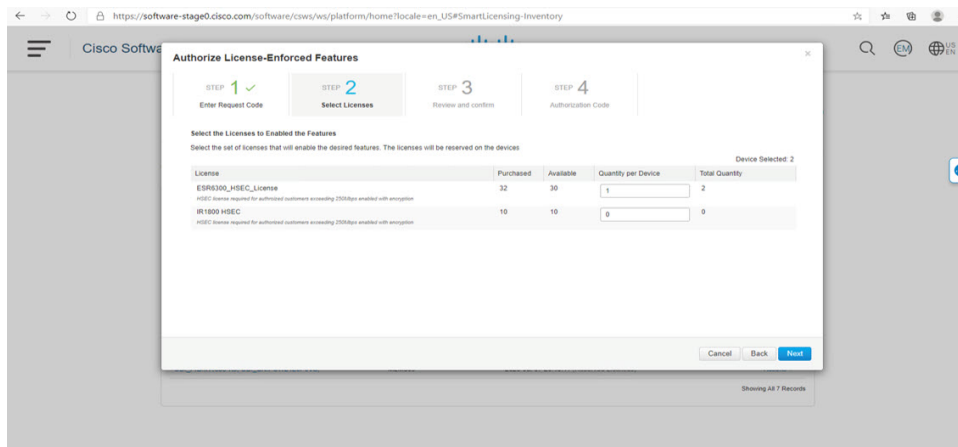
**Step 9** The **Select Licenses** Tab opens.

Figure 19: Select Licenses



**Step 10** Under **Quantity per Device**, enter the number you wish.

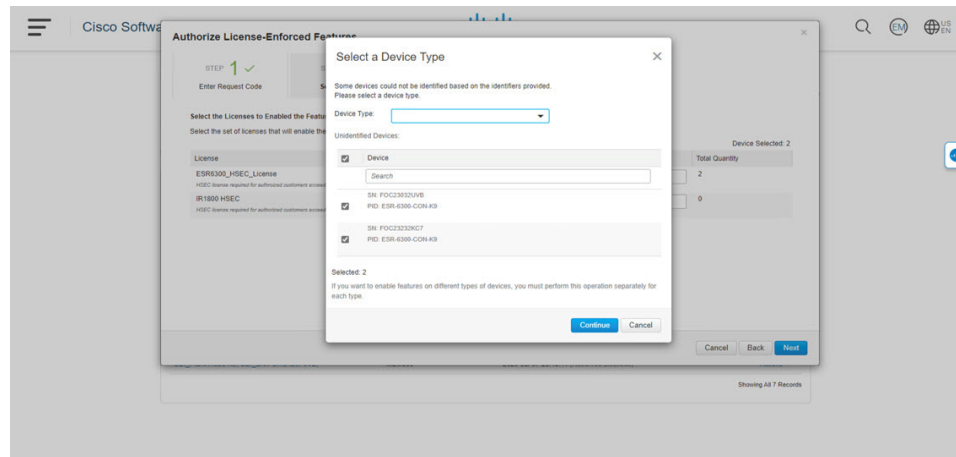
Figure 20: Enter Number



**Step 11** If CSSM cannot identify your device from the identifying information, you can select it manually.

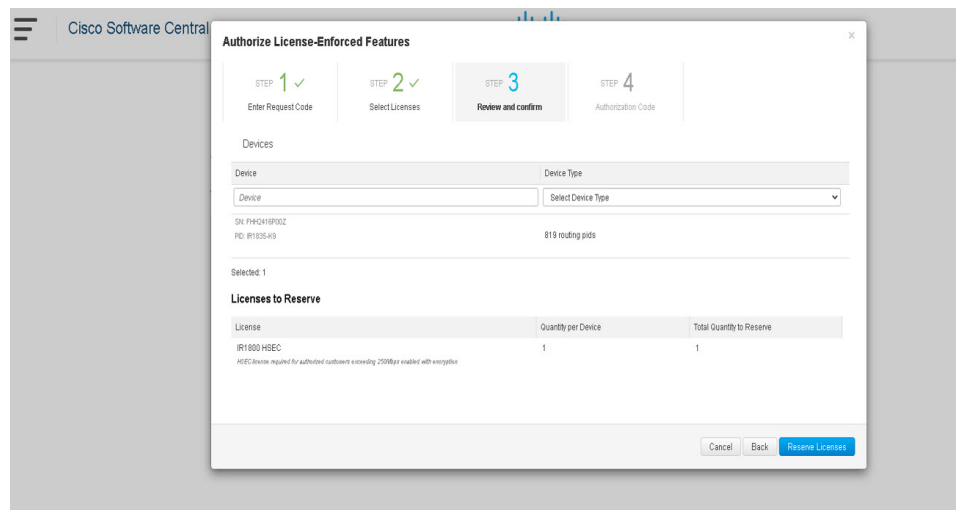


Figure 21: Select a Device Type



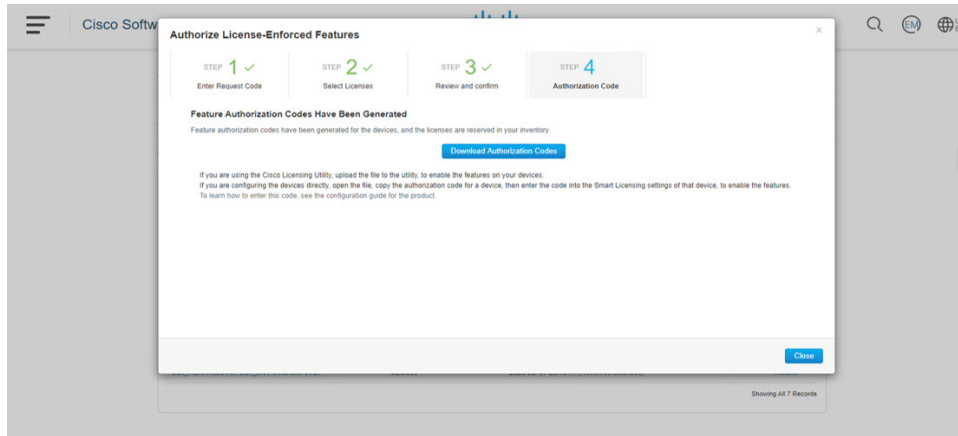
**Step 12** Click **Continue**, and the window changes to **Review and Confirm**.

Figure 22: Review and Confirm



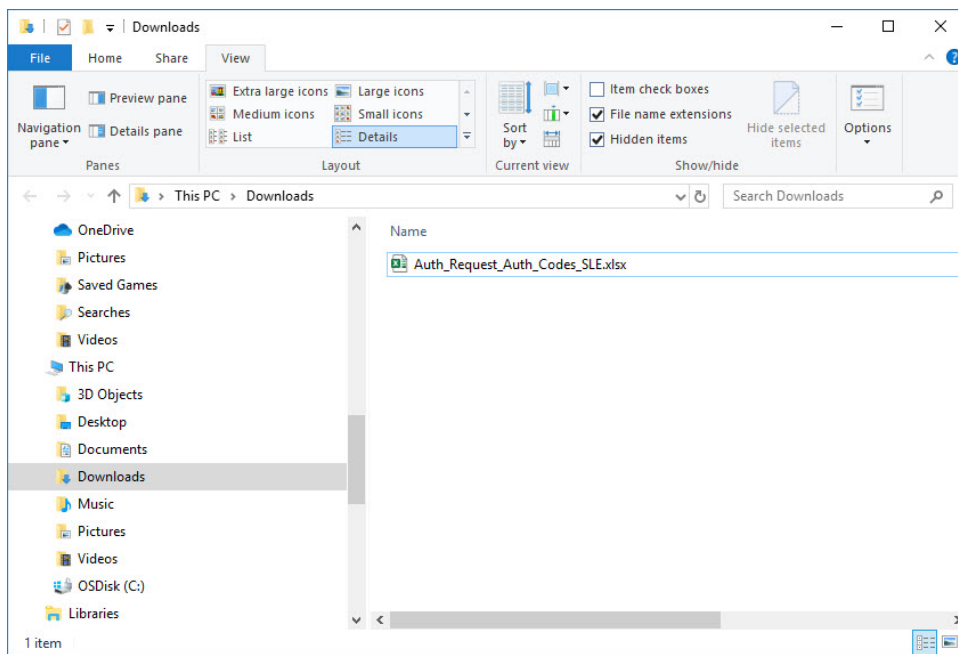
**Step 13** Click on **Reserve Licenses**, and CSSM generates feature authorization codes.

Figure 23: Feature Authorization Codes



**Step 14** Click **Download Authorization Codes**, and a window opens to navigate to where you wish to save the codes.

Figure 24: Save Authorization Code



**Step 15** Click **Ok**.

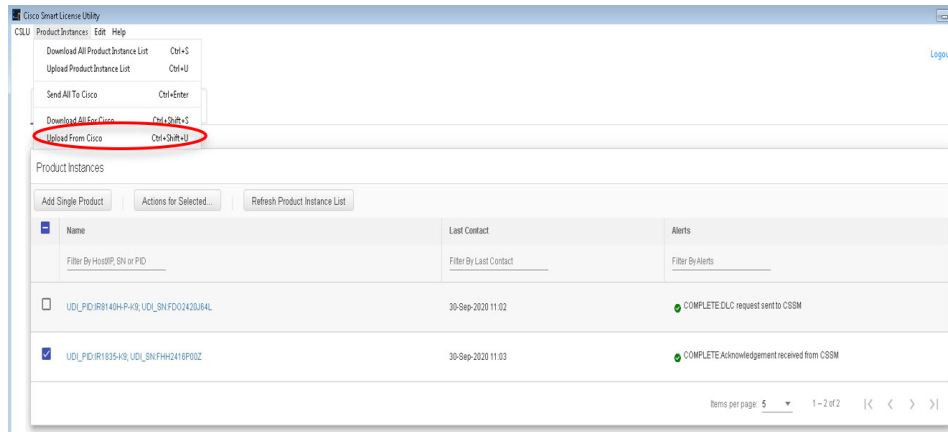
## Uploading the Authorization Request Code file into CSLU

### Procedure

**Step 1** Open the Cisco Smart License Utility (CSLU).

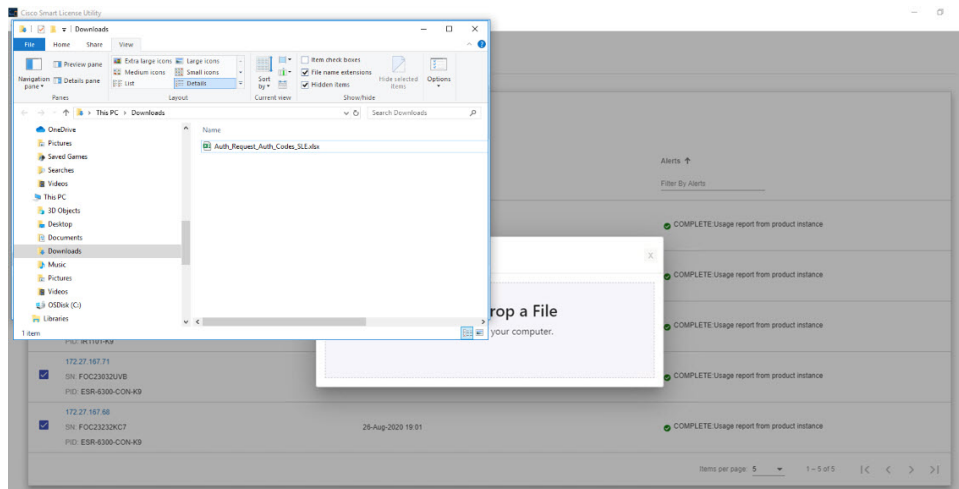
**Step 2** Navigate to **Product Instances**, and then select **Upload From Cisco**.

**Figure 25: Upload From Cisco**



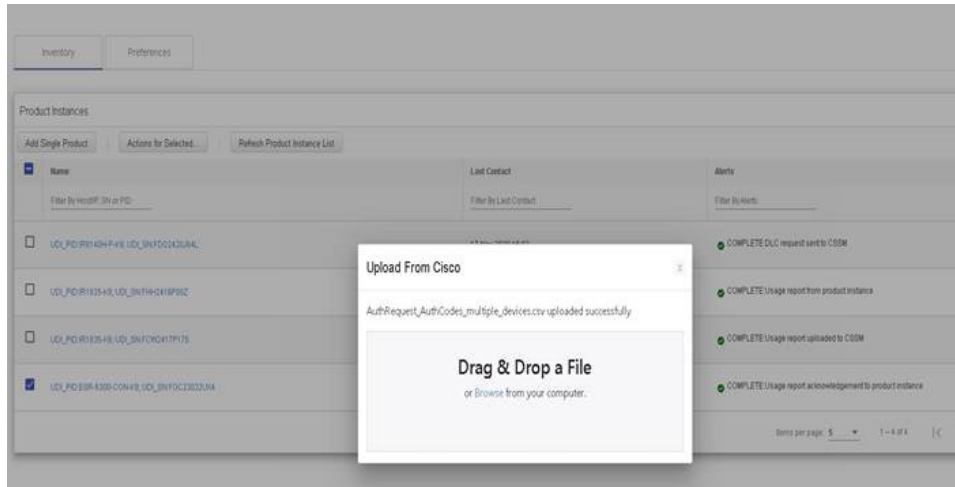
**Step 3** There are two options to load your file. **Drag and Drop**, or **Browse** to where you saved your file. This example shows Browse.

**Figure 26: Browse to File**



**Step 4** Select your authorization code file, and then click **Open**. The system uploads the authorization code file, then a successful upload message appears.

Figure 27: Successful Upload



## License Installation Process in the Router

Perform the following from the command line interface.

```
Router(config)#license boot level ?
  network-advantage  License Level Network-Advantage
  network-essentials License Level Network-Essentials
Router(config)#license boot level
Router(config)#platform hardware throughput crypto ?
  T0    T0 (up to 15 mbps) bidirectional thput
  T1    T1 (up to 100 mbps) bidirectional thput
  T2    T2 (up to 1 gbps) bidirectional thput
Router(config)#platform hardware throughput crypto

Router# license smart trust idtoken <tokened> local force
*Sep 21 17:25:15.726: %CRYPTO_ENGINE-5-KEY_ADDITION: A key named SLA-KeyPair has been
generated or imported by crypto-engine

*Sep 21 17:25:15.808: %PKI-4-NOCONFIGAUTOSAVE: Configuration was modified. Issue "write
memory" to save new IOS PKI configuration

*Sep 21 17:25:24.310: %SMART_LIC-5-COMM_RESTORED: Communications with Cisco Smart Software
Manager (CSSM) restored

*Sep 21 17:25:24.490: %SMART_LIC-6-TRUST_INSTALL_SUCCESS: A new licensing trust code was
successfully installed on P:IR8340-K9,S:FDO2523J6N1.

Router# show license tech support | i Trust
Trust Establishment:
Trust Acknowledgement:
Trust Sync:
Trusted Store Interface: True
Local Device: P:IR8340-K9,S:FDO2523J6N1, state[2], Trust Data INSTALLED TrustId:869
Overall Trust: INSTALLED (2)

Router#show license summary
Account Information:
```

```
Smart Account: SA-IOT-Polaris As of Sep 23 04:58:01 2021 UTC
Virtual Account: Router
```

```
License Usage:
License                Entitlement Tag                Count Status
-----
network-advantage_T1  (IR8300_NA_T1_PERF)                1 IN USE
```

```
Router#
```

```
Router#show license usage
```

```
License Authorization:
  Status: Not Applicable
```

```
network-advantage_T1 (IR8300_NA_T1_PERF):
  Description: network-advantage_T1
  Count: 1
  Version: 1.0
```

```
Status: IN USE
  Export status: NOT RESTRICTED
  Feature Name: network-advantage_T1
  Feature Description: network-advantage_T1
  Enforcement type: NOT ENFORCED
  License type: Perpetual
```

```
Router#
```

```
Router#show running-config | i license
license udi pid IR8340-K9 sn FDO2523J6N1
license boot level network-advantage
license smart url https://smartreceiver-stage.cisco.com/licservice/license
license smart url smart https://smartreceiver-stage.cisco.com/licservice/license
license smart transport smart
Router#
```

## HSEC Installation

This example uses the IR8300 series router.

Perform the following from the command line interface.

```
Router#license smart authorization request add hsec9 local
Router#
Sep 23 05:29:37.894: %SMART_LIC-6-AUTHORIZATION_INSTALL_SUCCESS: A new licensing authorization
code was successfully installed on PID:IR8340-K9,SN:FDO2523J6N1
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#license feature hsec9
Router(config)#end
Router#show running-config | i license
license feature hsec9
license udi pid IR8340-K9 sn FDO2523J6N1
license boot level network-advantage
license smart url https://smartreceiver-stage.cisco.com/licservice/license
license smart url smart https://smartreceiver-stage.cisco.com/licservice/license
license smart transport smart
Router#
Router#show license summary
Account Information:
  Smart Account: SA-IOT-Polaris As of Sep 23 05:29:41 2021 UTC
  Virtual Account: Router
```

```
License Usage:
License           Entitlement Tag           Count Status
-----
network-advantage_T1  (IR8300_NA_T1_PERF)      1 IN USE
hseck9              (IR8300_HSEC)             1 IN USE
```

```
Router#
Router#show license usage
License Authorization:
  Status: Not Applicable
.
.
.
hseck9 (IR8300_HSEC):
  Description: hseck9
  Count: 1
  Version: 1.0
  Status: IN USE
  Export status: RESTRICTED - ALLOWED
  Feature Name: hseck9
  Feature Description: hseck9
  Enforcement type: EXPORT RESTRICTED
  License type: Export
```