Revised: June 3, 2025

Smart Licensing Using Policy on the Cisco Catalyst IR1101, IR1800, IR8140, IR8340 and ESR6300 Routers

Smart Licensing Using Policy Overview

Smart Licensing Using Policy (SLP) is a flexible licensing model that simplifies and streamlines the process of purchasing and managing software. It provides users with a faster, easier, and more consistent experience across the entire Cisco portfolio.

SLP users benefit from:

- Easy Activation: A centralized pool of software licenses for the entire organization, eliminating the need for Product Activation Keys (PAKs).
- Unified Management: Access to My Cisco Entitlements (MCE), offering a comprehensive view of all Cisco products and services through an intuitive portal, ensuring you always know what you have and are using.
- License Flexibility: Software licenses are not tied to specific hardware, allowing for seamless use and transfer as needed.

Note

This guide supports all IIoT Routers and replaces individual chapters in each software configuration guide.

SLP as Default Licensing Model

SLP became the default licensing model for IIOT Routers starting with IOS-XE release 17.3.2. It was formerly known as Smart Licensing Enhanced (SLE), which had replaced Smart Software Licensing model.

Features Supported on IIOT Routers

Table 1: Features Supported on IIOT Routers

Feature	IR1101	IR1800	IR8100	IR8300	ESR6300
Supported in IOS-XE release 17.4.1	NA	Yes	NA	NA	NA
Supported in IOS-XE release 17.3.2	Yes	Yes	Yes	Yes	Yes
Authorization code required for export control compliance	Yes	Yes	Yes	Yes	Yes
HSEC license required for throughput exceeding 250 Mbps	Yes	Yes	Yes	Yes	Yes
No EVAL license. Authorized status changed to In Use or Not In Use with an Enforcement Type class.	Yes	Yes	Yes	Yes	Yes
CSLU serves as a new interface between devices and CSSM in certain customer environments	Yes	Yes	Yes	Yes	Yes

Feature	IR1101	IR1800	IR8100	IR8300	ESR6300
Throughput is defaulted and capped at 250MB	NA	Yes	NA	NA	NA

License Levels

The following license levels are available for all Cisco IR devices.

- Base Licenses
- Add-on Licenses

Base Licenses

Base licenses licenses are ordered through Cisco Commerce Workspace (CCW), and are permanent.

They include:

- Network Essentials
- Network Advantage (includes Network Essentials)

Table 2: Network Essentials

Essential switch capabilities	Layer 2, Routed Access(RIP, EIGRP Stub, OSPF (1000 routes)), PBR, PIM Stub Multicast (1000 routes) PVLAN, VRRP, PBR, CDP, QoS, FHS, 802.1x, Macsec-128, CoPP, SXP, and IP SLA Responder SSO **Note** For the device to be compliant with the DNA Essential License it must not exceed 1000 routes in the routing table regardless of how the routes were learned.
DevOps integration	• Netconf, Restconf, gRPC • Yang Data Models • GuestShell (On-Box Python) • PnP Agent, ZTP

Table 3: Network Advantage

IoT and mobility	CoAP
Full routing functionality	BGP, HSRP, OSPF, ISIS,GLBP
Flexible network segmentation	VRF, VXLAN, LISP, SGT, MPLS
High availability and resiliency	NSF, GIR, Stackwise Virtual*, ISSU/eFSU, Patching (CLI)
Optimize bandwidth utilization with multicast	MSDP, mVPN, AutoRP, PIM-BIDIR

Add-on Licenses

Add-on licenses can be subscribed for a fixed term of three, five, or seven years.

They are:

- Digital Networking Architecture (DNA) Essentials
- DNA Advantage (includes DNA Essentials)

Table 4: DNA Essentials

Advanced Automation	• Encrypted Traffic Analytics • DNA Service for Bonjour
Assurance and Analytics	• Compliance, Custom Reports • Switch 360 & Wired Client 360

Table 5: DNA Advantage

Basic automation	• PnP Application • LAN Automation • Embedded Event Manager
Basic assurance	• Health Dashboards – Network and Client • Basic Device & Wired Client Health Monitoring

Note

These licenses are ordered through Cisco Commerce Workspace (CCW), and relate to DNA-C and SDWAN. For further information, see the Cisco SD-WAN and Cisco DNA Center web pages.

Licensing Throughput Levels

The throughput level on the device sets the bandwidth limit for encrypted traffic. There is no limit imposed on non-encrypted (clear) traffic passing through the device.

Compliance with Global Export Regulations

To comply with global export regulations, if more than 250 Mbps of encrypted traffic is needed, you must select an “uncapped” option—dependent on the platform—on CCW, and obtain an HSEC license.

This limit is imposed bidirectionally.. For instance, if the throughput limit is set to 250 Mbps, the device can handle up to 250 Mbps of encrypted traffic in either direction—both for receiving and transmitting. There is no limit on unencrypted traffic.

When the throughput level on the device is set to ‘uncapped,’ there are no limits on either encrypted or unencrypted traffic passing through it.

Note

To avoid confusion regarding throughput limits on IOS XE software releases, see these points:

- Cisco IOS XE release 17.11.1a and earlier on the ESR6300, IR1800, and IR8140 platforms support boost, uncapped, and unlimited licenses, configured using the **platform hardware throughput level 2G** CLI.
- Cisco IOS XE release 17.12.1 and later on the ESR6300, IR1800, and IR8140 platforms support the same licenses but are configured using the **platform hardware throughput level uncapped** CLI.
- For Cisco IOS XE release 17.12.1 and later, both the **platform hardware throughput level 2G** and the **platform hardware throughput level uncapped** CLIs will deliver the same throughput as the uncapped license.

Throughput Limits on IIoT Routers

The following table shows the throughput limits (also referred to as Tier license) supported on IoT devices.

Table 6: Throughput Limits

Platform	25 Mbps bidirectional (Tier 0)	50 Mbps bidirectional	Up to 200 Mbps bidirectional (Tier 1)	250 Mbps bidirectional	2 Gbps	Uncapped (Tier 2)
IR1101	NA	NA	NA	Yes	NA	Support started from 17.10.1
IR1800	NA	Yes	NA	Yes	Yes	Support started from 17.12.1
IR8100	NA	Yes	Yes	Yes	Yes	Support started from 17.12.1
IR8300	Yes	NA	Yes	NA	NA	Yes
ESR 6300	NA	Yes	NA	Yes	Yes	Support started from 17.12.1
ESR-6300-LIC-K9	NA	Yes	NA	NA	NA	Yes

Commands to Configure Throughput Level

Set License Level

Use the **license boot level** {**network-essentials** | **network-advantage**} command to set the desired license level for the device.

```
Device# license boot level network-advantage
```

Configure Throughput Level

Use the **platform hardware throughput level** *limit* command to configure the throughput level for all the devices, except IR8300.

```
Device# platform hardware throughput level 25
```

Configure Throughput Level on IR8300

Use the **platform hardware throughput crypto** *limit* command to configure the throughput level for IR8300.

```
Device# platform hardware throughput crypto 25
```

Verify Throughput Level

Use the **show version | include throughput** command to see the throughput configured on the device.

```
Device# show version | include throughput
```

License Enforcement Types

Each license falls under one of three enforcement types, indicating whether authorization is required prior to use.

- Unenforced or Not Enforced
- Enforced
- Export-Controlled

Unenforced or Not Enforced

The majority of licenses fall under this category. Unenforced licenses do not require authorization for use in air-gapped networks or registration in connected networks. Their usage is governed by the terms outlined in the End User License Agreement (EULA).

Enforced

Licenses under this enforcement type require authorization before use. This authorization comes in the form of an authorization code, which must be installed on the corresponding product instance.

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

Export-Controlled

Licenses in this enforcement type are restricted by U.S. trade-control laws and require authorization before use. An authorization code must be installed on the corresponding product instance. Cisco may pre-install export-controlled licenses when purchased with hardware.

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

High Security License

The High Security (HSEC) License is an additional feature license that can be configured alongside the network license. It provides export controls for strong encryption levels. HSEC is available to customers in all non-embargoed countries as listed by the U.S. Department of Commerce. The HSEC license removes the default limit of 250 Mbps of IPsec throughput in each direction, allowing for higher performance.

As part of HSEC license, a new bandwidth option called "uncapped" is available. With this new feature, the IR1101 will support the following bandwidth and license types:

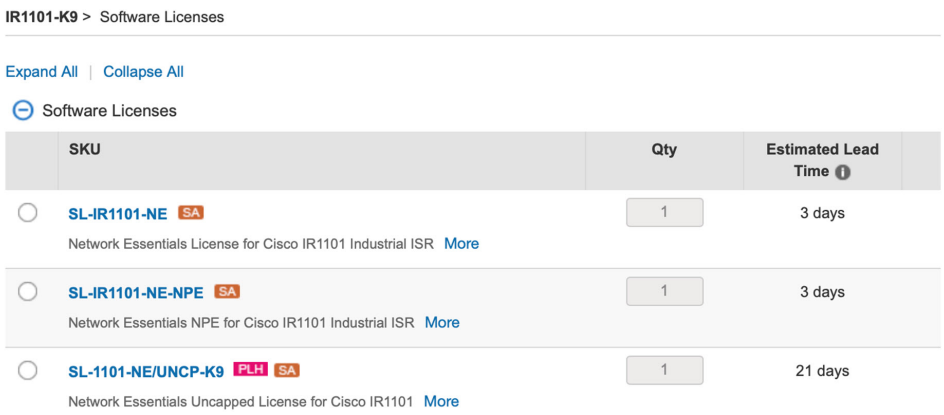
- Network-essentials 250 Mbps
- Network-advantage 250 Mbps
- Network-essentials uncapped
- Network-advantage uncapped
- HSEC

See the Configure Uncapped Throughput Level procedure on how to configure uncapped throughput level on IR1101.

Ordering

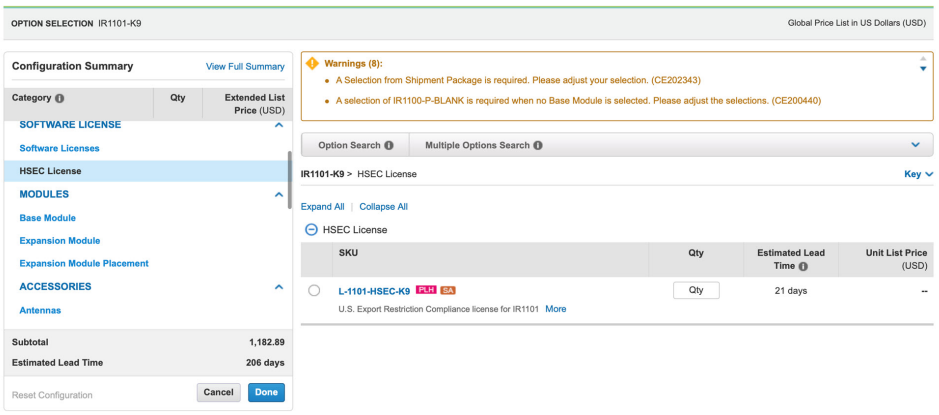
An example of ordering license for the IR1101-K9 is shown here:

1. Select Network Essentials Uncapped License.



The L-1101-HSEC-K9 license is included automatically when you select the uncapped license, as shown below.

2. Click Done.



Cisco Software Central

This guide provides information on how to order, activate, and manage your Cisco Smart Licenses.

Smart Licensing Using Policy Architecture

This section outlines the different components that may be included in your SLP implementation.

Product Instance

A product instance refers to a single unit of a Cisco product, identified by a Unique Device Identifier (UDI). It tracks and reports license usage through RUM reports, and provides alerts and system messages for overdue reports, communication failures, and other issues. Additionally, the RUM reports and usage data are securely stored within the product instance.

RUM Report

A Resource Utilization Measurement (RUM) report is a license usage report that meets the reporting requirements outlined by the policy. Generated by the product instance and processed by CSSM, RUM reports document license usage and any changes in an open report. At predetermined intervals, the system closes open RUM reports and creates new ones to continue recording license usage. Once closed, a RUM report is prepared for submission to CSSM.

RUM Acknowledgement

A RUM acknowledgement (RUM ACK or ACK) is a response from CSSM indicating the status of a RUM report. When an ACK for a report is received by the product instance, it means the corresponding RUM report is no longer required and can be deleted.

CSSM shows license usage information based on the most recent RUM report received.

Cisco Smart Software Manager

CSSM is a portal that allows you to manage all your Cisco software licenses from a central location. It helps you handle current needs, review usage trends, and plan for future licensing 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 or view licenses between virtual accounts
- transfer, remove, or view product instances
- run reports on your virtual accounts
- modify your email notification settings, and
- view overall account information.

Before using CSSM, watch a brief video on New User Introduction to Cisco Smart Software Manager.

Cisco Smart Licensing Utility

CSLU is a Windows-based reporting tool that offers aggregate licensing workflows. It allows you to manage all your licenses and their associated product instances directly from your premises, eliminating the need to connect to CSSM.

This utility performs the following key functions:

- Provides options for triggering workflows, either by CSLU or by the product instance.
- Collects usage reports from the product instance and uploads them to the corresponding smart account or virtual account, either online or offline using files. It also collects RUM report ACKs and returns them to the product instance.
- Sends authorization code requests to CSSM and receives authorization codes from CSSM.

CSLU in SLE Topology

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 without connecting to CSSM. In this case, usage information is downloaded to a file and then uploaded to CSSM, which is suitable for air-gapped networks.
- Embed it in a controller such as Cisco Catalyst Center.

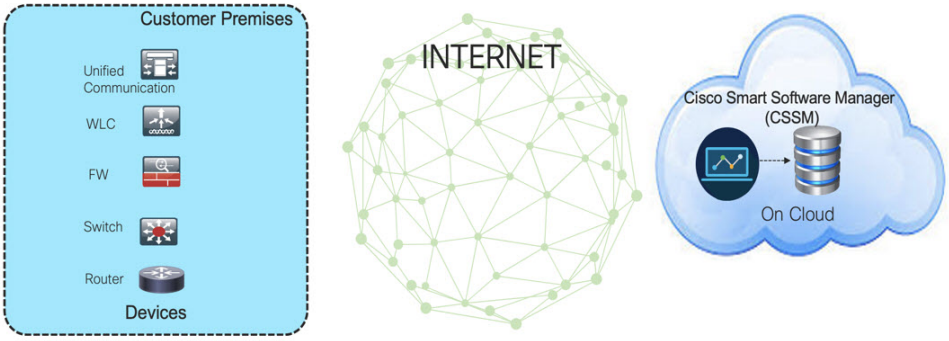
Customer Topologies

IoT Routing platforms use two different topologies. They are

- Full Offline Access
- CSLU has No Access To CSSM

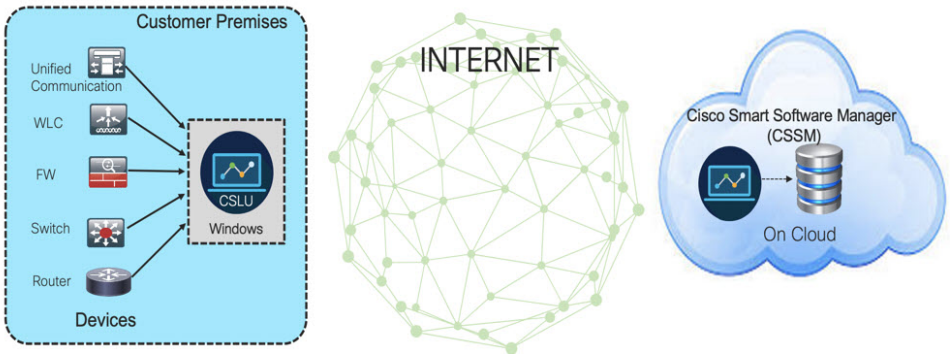
Full Offline Access

The following image illustrates the Full Offline Access topology, where devices do not have connectivity to (Cisco Smart Software Manager – software.cisco.com). The user must manually copy and paste information between Cisco products and CSSM to check in and out licenses.



CSLU has No Access To CSSM

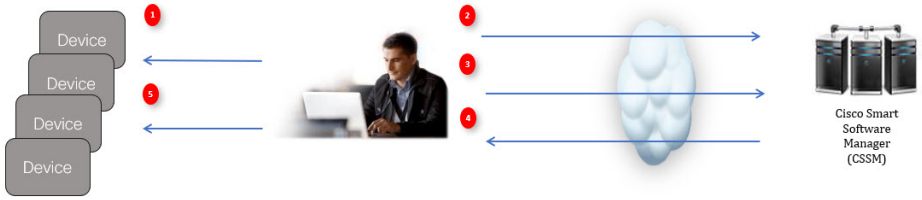
The following image illustrates the CSLU having No Access to CSSM topology, where devices are connected to the CSLU controller. However, there is no connectivity between CSLU and CSSM (Cisco Smart Software Manager – software.cisco.com). Cisco devices will send usage information to the locally installed CSLU. The user must manually copy and paste information between CSLU and CSSM to 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

Register a Product Instance in CSSM

Step 1 Generate a license usage file from the Router.

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

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

Step 3 Import the license usage file to CSSM on Cloud.

a) Click on the **Usage Data Files** tab.

The **Upload Usage Data** window appears.

b) Click **Browse**, and navigate to where the file is.
c) Click on **Upload Data**.
d) Select the **Virtual Account** using the drop-down list.
e) Click **Ok**.

Step 4 Observe the Smart Software Licensing window. Initially, the Reporting Status state will be **Pending**. Wait until the window reflects **No Errors** before continuing.

Step 5 Click **Download** to download the ACK file.

Step 6 Check under the **Product Instances** tab to verify your device is listed.

What's next

Import the ACK file from CSSM to your device.

Import the ACK file from CSSM to your Device

Step 1 Copy the ACK file from CSSM to your host laptop or usbflash device.

```
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 that the Product Instance has imported the data.

Example from an IR1800.

```
Router# show license usage
License Authorization:
  Status: Not Applicable
network-advantage_250M (IR1800_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
```

Example from an ESR6300.

```
Router# show license usage
License Authorization:
  Status: Not Applicable
network-advantage_250M (ESR6300_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 that the license is in use.

Example from an IR1800.

```
Router# show license summary
License Usage:
  License                                          Entitlement tag               Count   Status
  -----------------------------------------------------------------------------------------
```

```
  network-advantage_250M  (IR1800_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
```

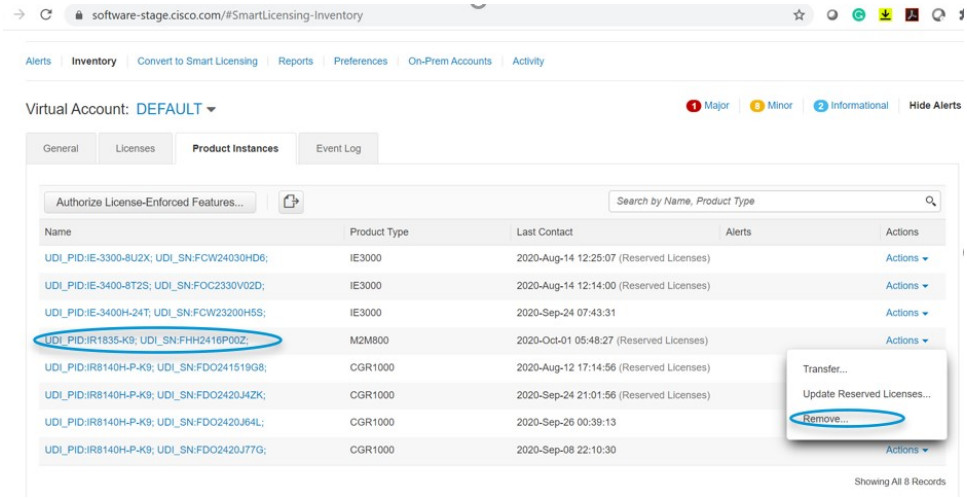
Example from an ESR6300.

```
Router# show license summary
License Usage:
  License                                          Entitlement tag               Count   Status
  -----------------------------------------------------------------------------------------------
  network-advantage_250M  (ESR6300_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
```

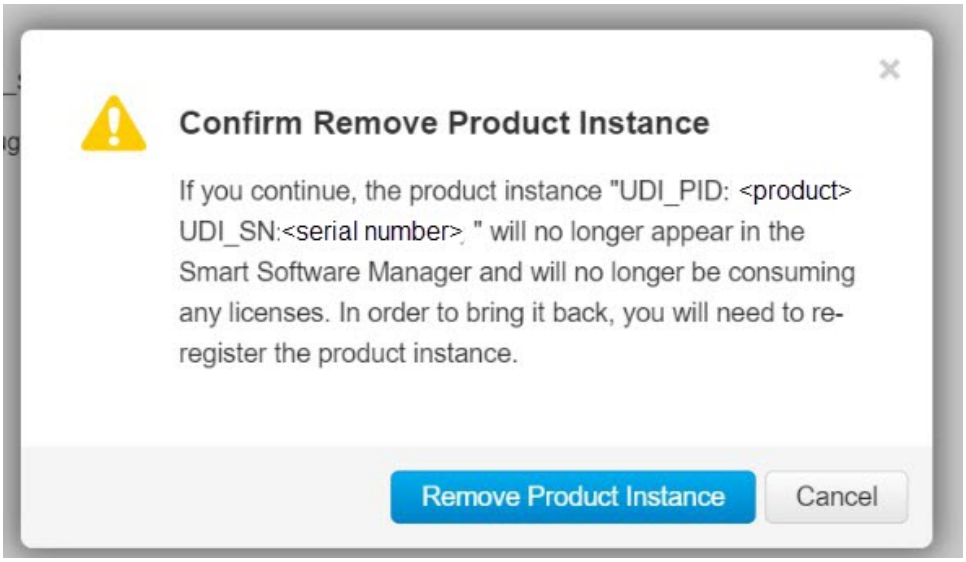
Remove the Device from CSSM

Step 1 Navigate to the **Product Instances** tab and locate your device.



Step 2 Click on **Actions** link beside your device, and from the list of options click **Remove**.

The **Confirm Remove Product Instance** window appears.

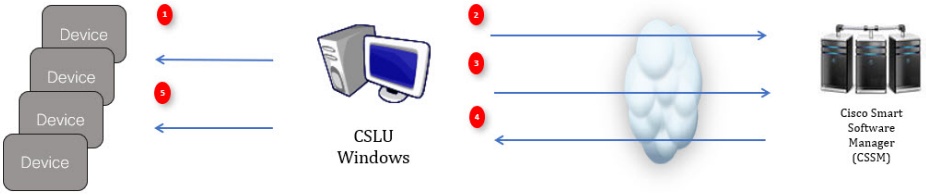


Step 3 Click **Remove Product Instance**.

License Installation When CSLU has No Access to CSSM

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

An image showing the flow of information is given below.



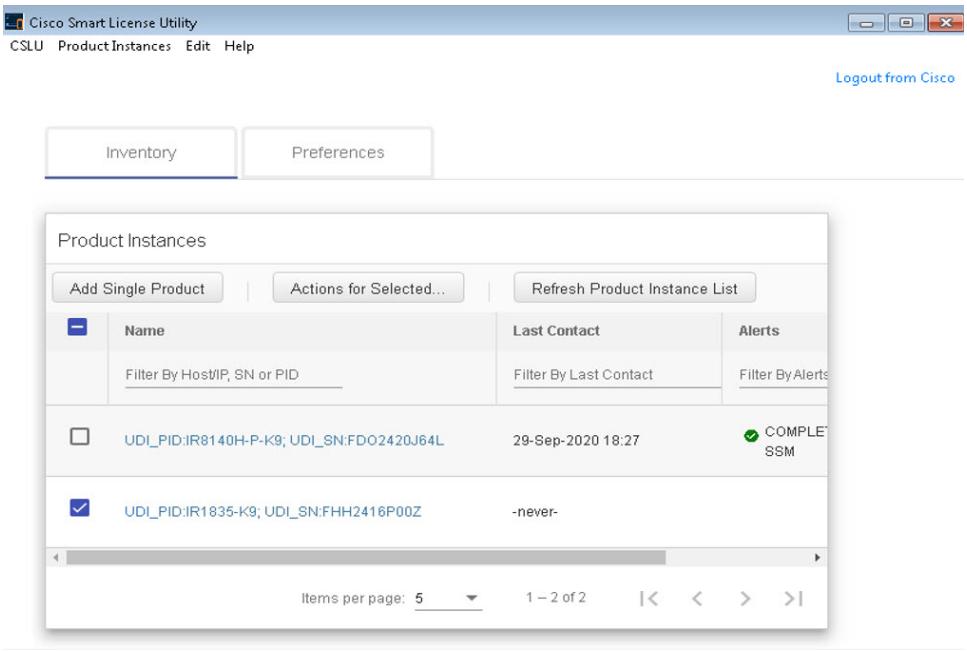
1. In CSLU, identify the devices that require an AuthCode, and initiate the request. An AuthCode file is created.
2. Export the AuthCode file to CSSM.
3. Upload the AuthCode to CSSM SA/VA account.
4. Export the AuthRequestAuthcode file to CSLU.
5. Upload ACK file or AuthRequestAuthCode.

Install License When Devices are Connected to the CSLU

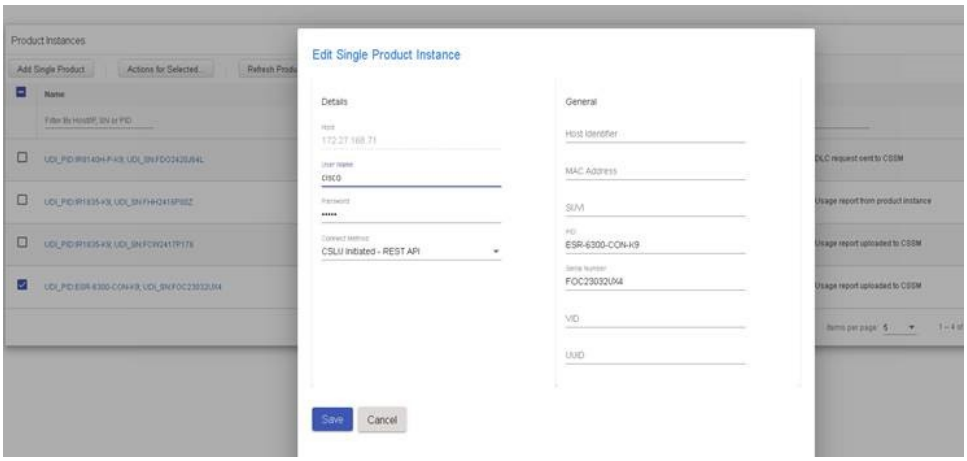
Get the license UDI using the Generate a UDI procedure.

Step 1 Open the Cisco Smart License Utility.

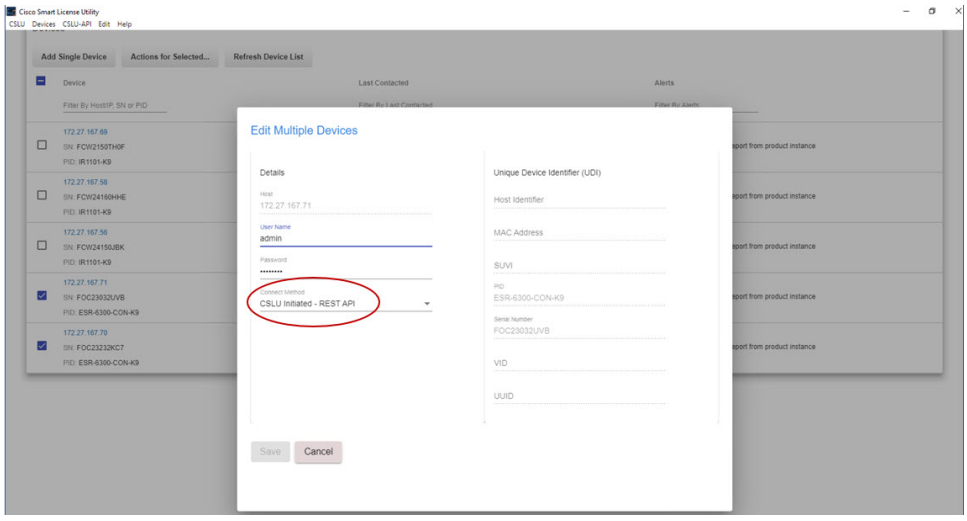
Step 2 Navigate to the **Product Instances** tab, then click on the **UDI**.



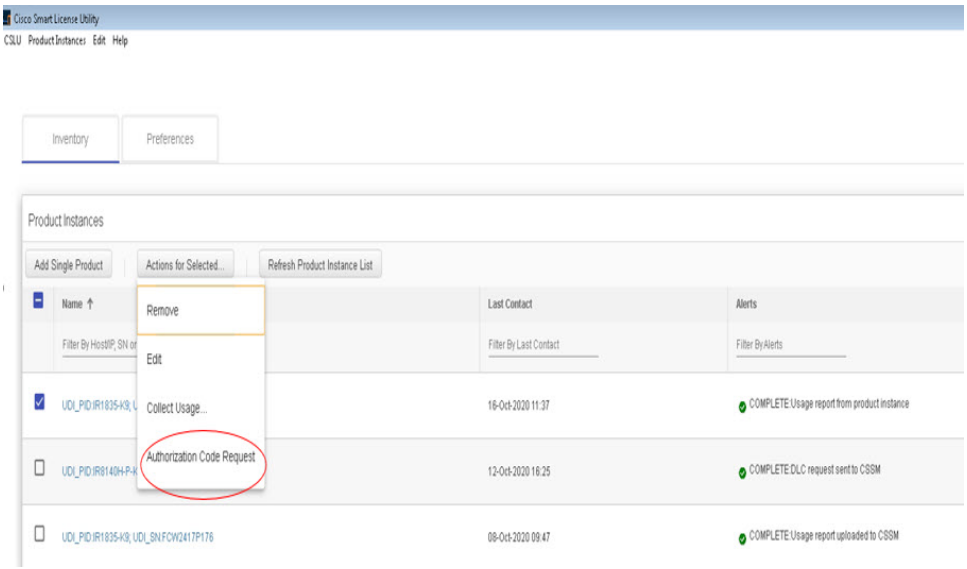
Step 3 The **Edit Single Product Instance** window appears. Enter details and click **Save**.



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

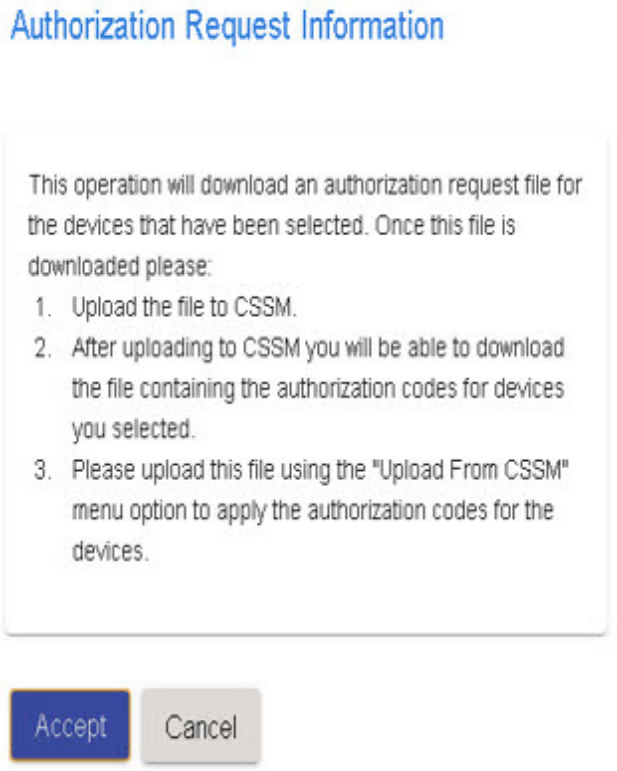


Step 5 In the **Product Instances** window, click on the **Actions for Selected Devices** tab.

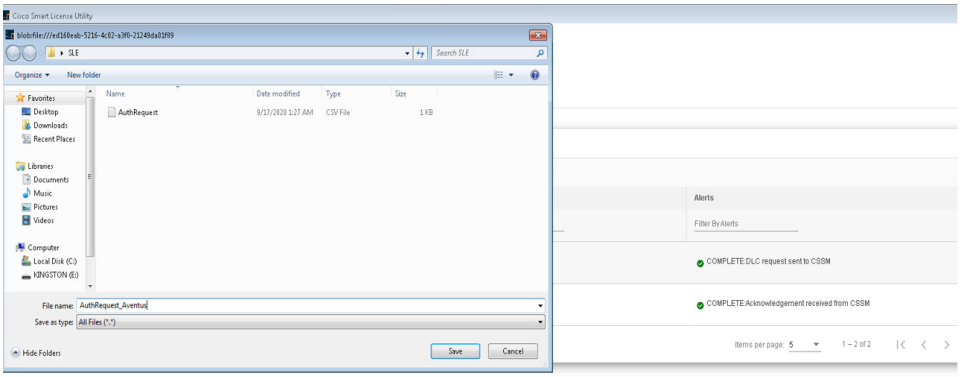


Step 6 Select **Authorization Code Request**.

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



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



What's next

Upload the Authorization Request file to the Cisco Smart Software Manager.

Generate a License UDI from CLI

Step 1 Use the **show license summary** command to get an overview of the licensing status on the router.

```
Router# show license summary

License Reservation is ENABLED
```

```
License Usage:
  License                 Entitlement tag               Count Status
  -----------------------------------------------------------------------------
  network-essentials_250M (IR1800_P_250M_E)                 1 IN USE
  hseck9                  (IR1800_HSEC)                     1 IN USE
```

Step 2 Use the **configure terminal** command to enter global configuration mode.

```
Router# configure terminal
```

Step 3 Use the **platform hardware throughput level 2G** command to configure the total throughput capacity of a router.

```
Router(config)# platform hardware throughput level 2G
```

Step 4 Use the **end** command to exit configuration mode and return to privileged EXEC mode.

```
Router(config)# end
```

Step 5 Use the **show license udi** command to view the Unique Device Identifier (UDI) of the router, which includes the Product ID (PID) and Serial Number (SN).

```
Router# show license udi

UDI: PID:IR1835-K9,SN:FHH2416P00Z
```

Install License in IR1800 from CLI

Step 1 Use the **show license summary** command to get an overview of the licensing status on the router.

```
Router# show license summary

License Reservation is ENABLED
License Usage:
  License                 Entitlement tag               Count Status
  -----------------------------------------------------------------------------
  network-essentials_250M (IR1800_P_250M_E)                 1 IN USE
  hseck9                  (IR1800_HSEC)                     1 IN USE
```

Step 2 Use the **show license usage** command to get detailed information about the status and usage of each license feature on the router.

```
Router# show license usage

License Authorization:
  Status: Not Applicable
network-essentials_250M (IR1800_P_250M_E):
  Description: network-essentials_250M
  Count: 1
  Version: 1.0
  Status: IN USE
  Export status: NOT RESTRICTED
  Feature Name: network-essentials_250M
  Feature Description: network-essentials_250M
  Enforcement type: NOT ENFORCED

hseck9 (IR1800_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
```

Step 3 Use the **configure terminal** command to enter global configuration mode.

```
Router# configure terminal
```

Step 4 Use the **platform hardware throughput level 2G** command to configure the total throughput capacity of a router.

```
Router(config)# platform hardware throughput level 2G
```

Step 5 Use the **end** command to exit configuration mode and return to privileged EXEC mode.

```
Router(config)# end
```

Step 6 Use the **show license summary** command to verify the licensing status on the router

```
Router# show license summary

License Reservation is ENABLED
License Usage:
  License                 Entitlement tag               Count Status
  -----------------------------------------------------------------------------
  network-essentials_250M (IR1800_P_250M_E)                1 IN USE
  hseck9                  (IR1800_HSEC)                    1 IN USE
  network-essentials_2G   (IR1800_P_2G_E)                  1 IN USE
```

Install License in ESR6300 from CLI

Step 1 Use the **show license summary** command to get an overview of the licensing status on the router.

```
Router# show license summary

License Reservation is ENABLED
License Usage:
  License Entitlement tag Count Status
  network-advantage_250M (ESR6300_P_250M_E) 1 IN USE
  hseck9 (ESR6300_HSEC) 1 IN USE
```

Step 2 Use the **show license usage** command to get detailed information about the status and usage of each license feature on the router.

```
Router# show license usage

License Authorization:
  Status: Not Applicable
network-advantage_250M (ESR6300_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
hseck9 (ESR6300_HSEC_License):
  Description: hseck9
```

```
Count: 1
Version: 1.0
Status: IN USE
Export status: RESTRICTED - ALLOWED
Feature Name: hseck9
Feature Description: hseck9
Enforcement type: EXPORT RESTRICTED
```

Step 3 Use the **configure terminal** command to enter global configuration mode.

```
Router# configure terminal
```

Step 4 Use the **platform hardware throughput level 2G** command to configure the total throughput capacity of a router.

```
Router(config)# platform hardware throughput level 2G
```

Step 5 Use the **end** command to exit configuration mode and return to privileged EXEC mode.

```
Router(config)# end
```

Step 6 Use the **show license summary** command to verify the licensing status on the router

```
Router# show license summary

License Reservation is ENABLED License Usage:
  License                   Entitlement tag          Count   Status
  network-advantage_250M   (ESR6300_P_250M_A)        1       IN USE
  hseck9                   (ESR6300_HSEC_License)    1       IN USE
  network-advantage_2G     (ESR6300_P_2G_A)          1       IN USE
```

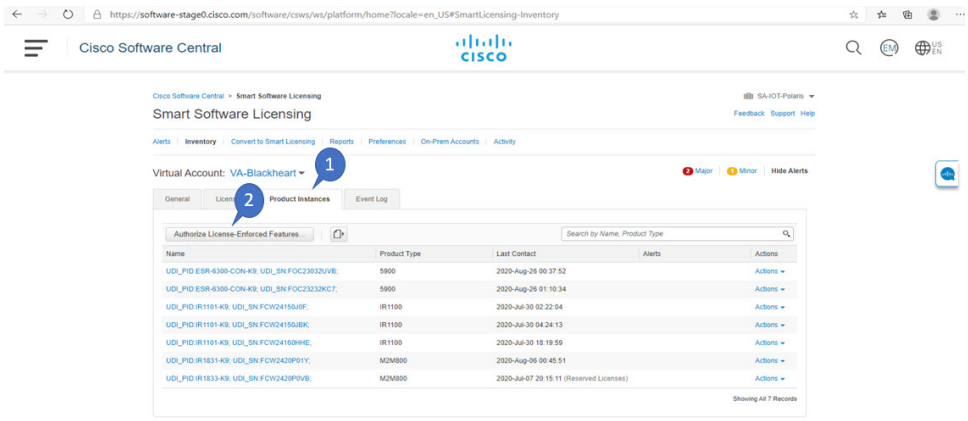
Export the Authorization Request File to CSSM

Step 1 Launch CSSM.

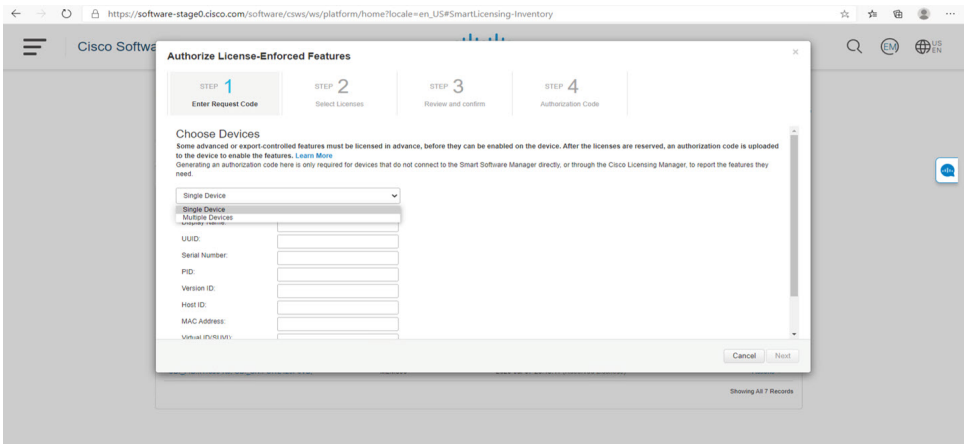
Step 2 Click on the **Inventory** tab, select your Virtual Account.

Step 3 Click on the **Product Instances** tab.

Step 4 Click on **Authorize License-Enforced Features**.

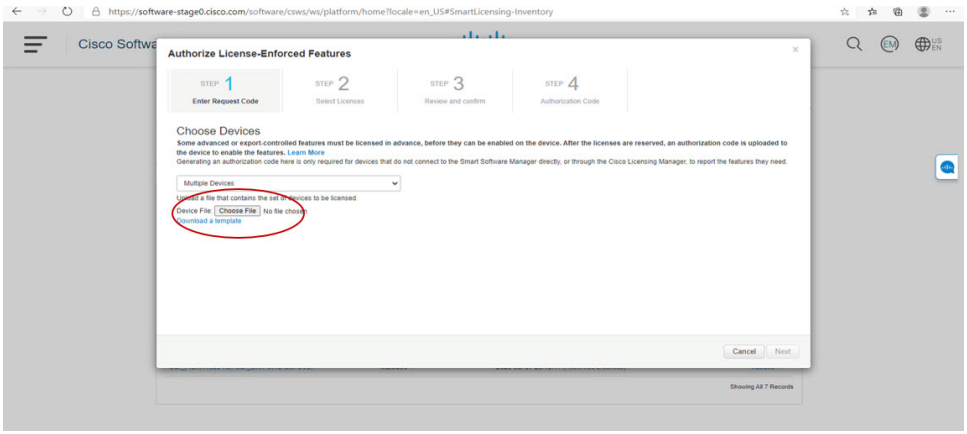


The **Authorize License-Enforced Features** window appears.



Step 5 Choose **Multiple** or **Single** devices from the drop-down.

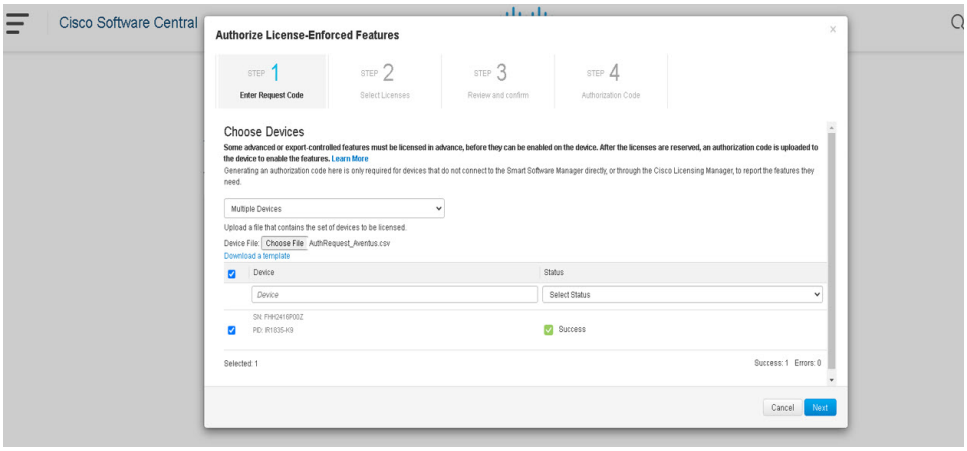
Step 6 Click on **Choose File** when the window displays an option to select a device file.



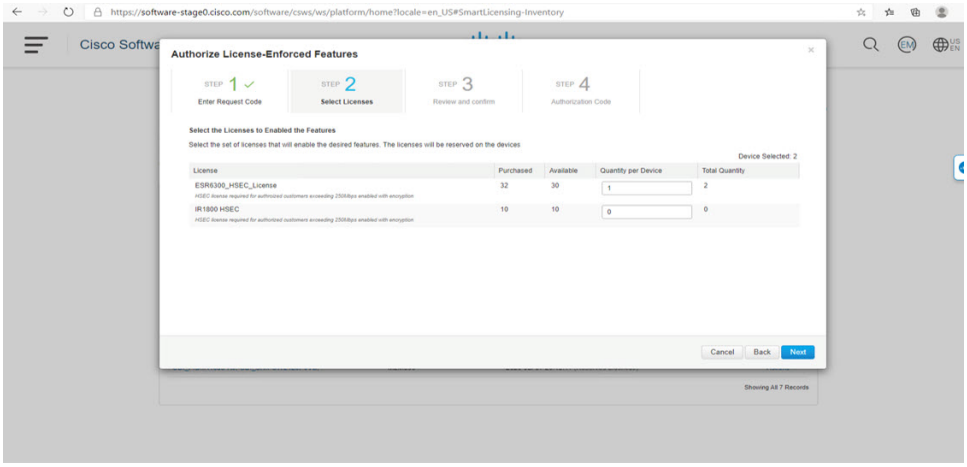
A popup window appears, allowing you to navigate to the location where you saved your Authorization Request file on your laptop.

Step 7 Select your file, and then click **Open**.

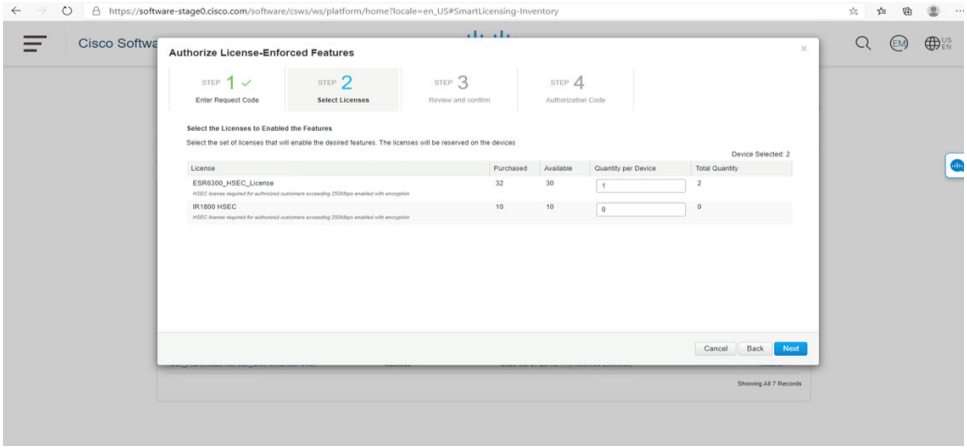
The authorization file loads, and the window changes to present your devices.



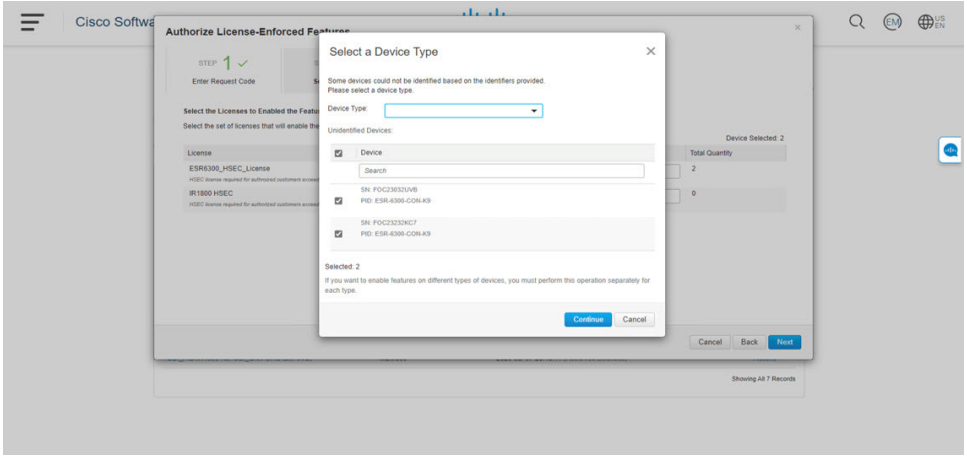
Step 8 Click **Next** to open **Select Licenses** tab.



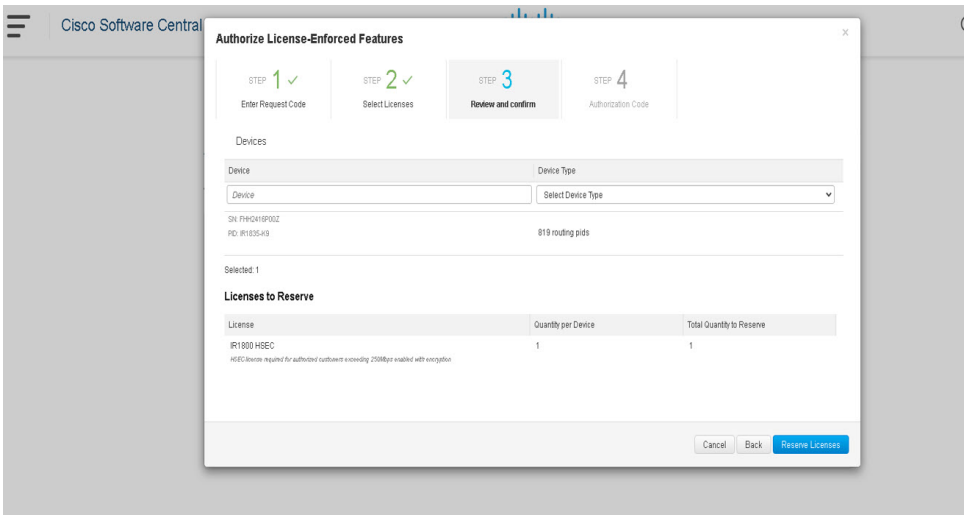
Step 9 Enter a number under **Quantity per Device**.



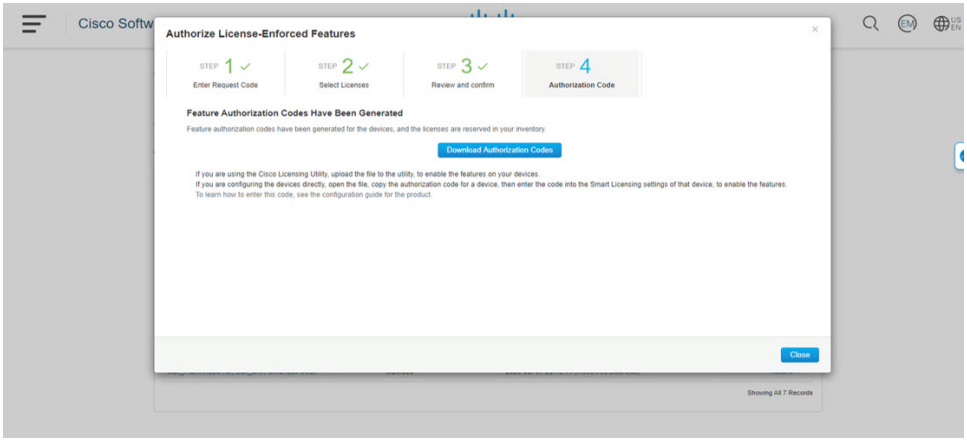
If CSSM cannot identify your device from the identifying information, select it manually.



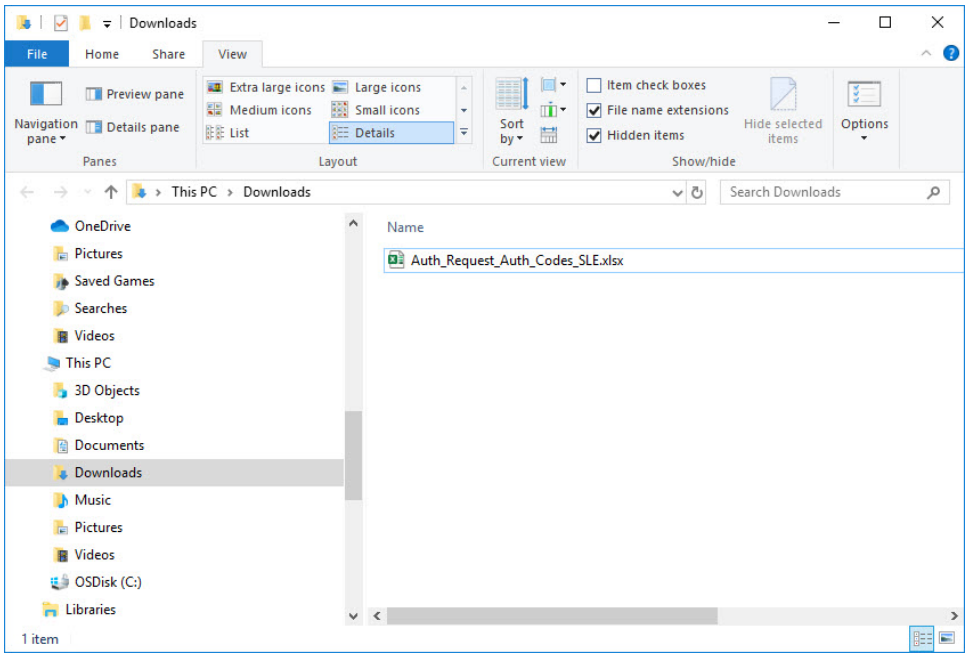
Step 10 Click **Continue**, the window changes to **Review and Confirm**.



Step 11 Click on **Reserve Licenses**, and CSSM generates feature authorization codes.



Step 12 Click **Download Authorization Codes**, and a window opens to navigate to where you wish to save the codes.

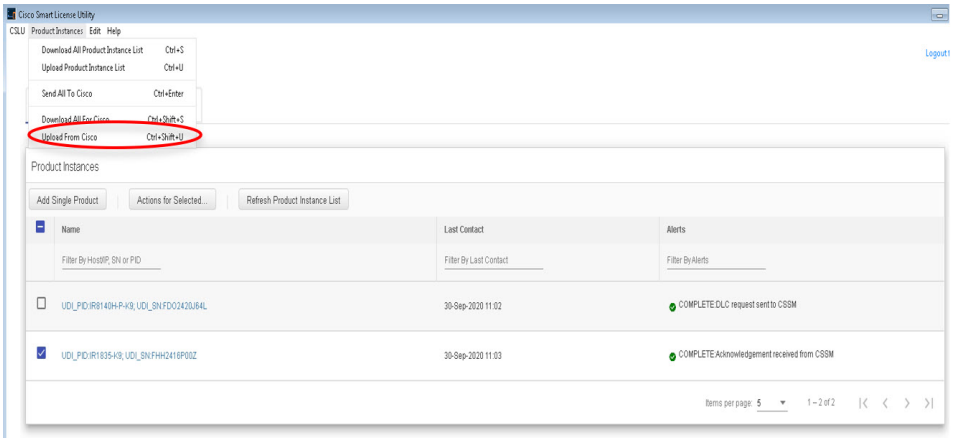


Step 13 Click **OK**.

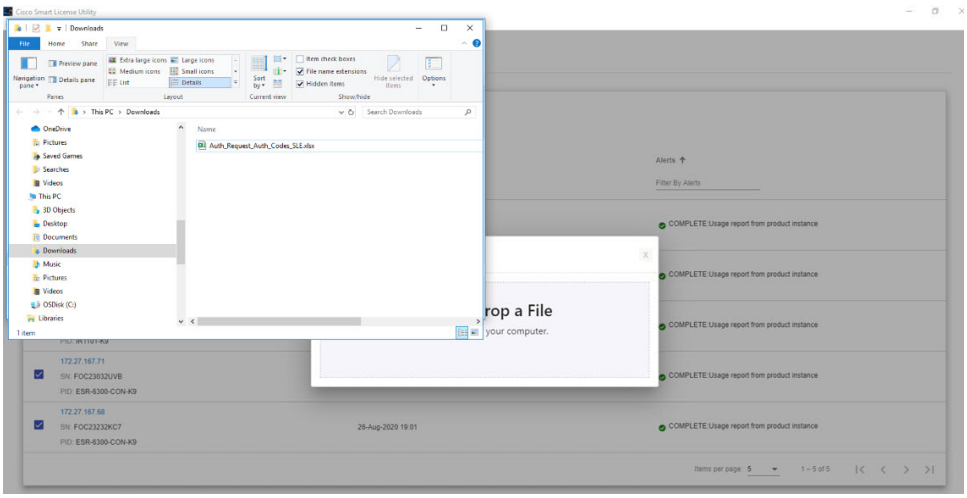
Upload the Authorization Request Code file to CSLU

Step 1 Open the Cisco Smart License Utility.

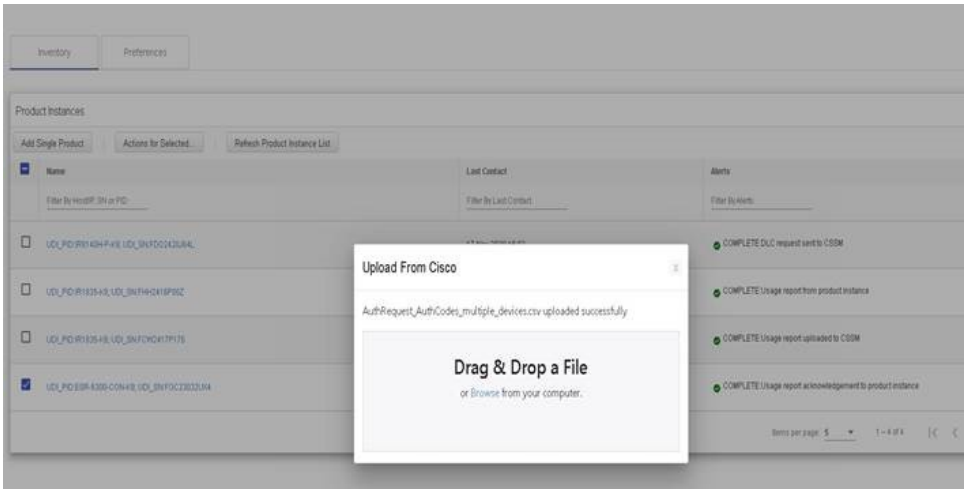
Step 2 Navigate to **Product Instances**, and then select **Upload From Cisco**.



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



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



Enable and Install High Security License

This section contains procedures required to enable and install High Security License from CLI.

Enable High Security License from CLI

To benefit from the HSEC license, a new bandwidth called **uncapped** is available. The new bandwidth is configured using the procedure given here.

Step 1 Use the **configure terminal** command to enter into configuration mode.

```
Device# configure terminal
```

Step 2 Use the **platform hardware throughput level** {**250m** | **uncapped**} command to enter into configuration mode.

```
Device(config)# platform hardware throughput level uncapped
```

Step 3 Use the **exit** command to go to the Privileged EXEC mode.

```
Device(config)# exit
```

Step 4 Use the **write memory** command to save the current running configuration to the device's startup configuration.

```
Device# write memory
```

Step 5 Use the **reload** command to restart the device to apply the configuration changes.

```
Device# reload
```

Install HSEC License from CLI

The procedure given here uses an IR8300 series router.

Step 1 Use **license smart authorization request add hseck9 local** command to generate a local authorization request for HSEC license.

```
Router# license smart authorization request add hseck9 local
```

Step 2 Use the **configure terminal** command to enter global configuration mode.

```
Router# configure terminal
```

Step 3 Use the **license feature hseck9** command to enable the HSEC license on the router. The HSEC license allows access to enhanced cryptographic features, such as high-throughput encryption and VPN services.

```
Router(config)# license feature hseck9
```

Step 4 Use the **end** command to exit configuration mode and return to privileged EXEC mode.

```
Router(config)# end
```

Step 5 Use the **show running-config | i license** command to verify the licensing configuration on the router.

```
Router#show running-config | i license

license feature hseck9
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
```

Step 6 Use the **show license summary** command to get an overview of the licensing status on the 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
```

Step 7 Use the **show license usage** command to get detailed information about the status and usage of each license feature on the 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
```

Configure Uncapped Throughput Level from CLI

Step 1 Use the **license feature hsec9** command to enable HSEC on the IR1101 router.

```
Device# license feature hsec9
```

Step 2 Use the **platform hardware throughput level uncapped** command to configure uncapped throughput.

```
Device# platform hardware throughput level uncapped
```

Step 3 Use the **write** command to save the current configuration.

```
Device# write
```

Step 4 Use the **reload** command reload the device.

```
Device# reload
```