Smart Licensing Using Policy

This chapter contains the following sections:

SLP Overview

Smart Licensing Using Policy (SLP), previously known as Smart Licensing Enhanced (SLE), is the default mode for IoT routers. SLE replaced Smart Software Licensing.

This guide supports all IoT routers, and replaces individual chapters in each of the software configuration guides.

The following sections show the features and software differences between the IoT routers.

IR1800

The IR1800 series only supports SLP. Some of the feature differences are:

- Support started with IOS-XE release 17.3.2

- An Authorization Code is required only for export control requirement

- Throughput greater than 250MB 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.

IR1101

The IR1100 series only supports SLP. Some of the feature differences are:

- Support started with IOS-XE release 17.3.2

- An Authorization Code is required only for export control requirement

- 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.

- Throughput is defaulted and capped at 250MB.

IR8100

The IR8100 series only supports SLP. Some of the feature differences are:

- Support started with IOS-XE release 17.3.2

- 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.

IR8300

The IR8300 series only supports SLP. Some of the feature differences are:

- Support started with IOS-XE release 17.3.2

- 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.

ESR6300

The ESR6300 embedded router operates slightly different than the other IoT routers. Some of the feature differences are:

- Support started with IOS-XE release 17.4.1

- 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.

High Security (HSEC) License

HSEC (High Security) license is a feature license that can be configured in addition to the network license (NE/NA). An HSEC license provides export controls for strong levels of encryption. HSEC is available to customers in all currently non-embargoed countries as listed by the U.S. Department of Commerce. Without an HSEC license, SEC performance is limited to a total of 250 Mbps of IPsec throughput in each direction. An HSEC license removes this limitation.

Command Line Interface

The configuration mode CLI to enable HSEC on the IR1101 is the following:

```
IR1101(config)# license feature hsec9
```

To benefit from the HSEC license, a new bandwidth will be available. The new bandwidth is called **uncapped**, and it is available with the following CLI from configuration mode:

```
IR1101(config)# platform hardware throughput level ?
250M throughput in bps
uncapped throughput in bps
IR1101# platform hardware throughput level uncapped
```

After performing the above commands, write mem and reload the router. The configuration will take effect when the router comes back up.

License Types

With this new feature, the IR1101 will support the following bandwidth/license types:

- Network-essentials 250 Mbps

- Network-advantage 250 Mbps

- Network-essentials uncapped

- Network-advantage uncapped

- HSEC

Ordering

The following is an example from the IR1101-K9. The license will be available on the IR1101-A-K9 as well.

In the following example, select the SL-1101-NE/UNCP-K9 (Network Essentials Uncapped License):

The L-1101-HSEC-K9 license will get auto included when you select the uncapped license, as shown in the following:

Cisco Software Central

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

https://software.cisco.com/software/csws/ws/platform/home?locale=en_US&locale=en_US&locale=en_US#

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 fulfils 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 codes1 from CSSM.

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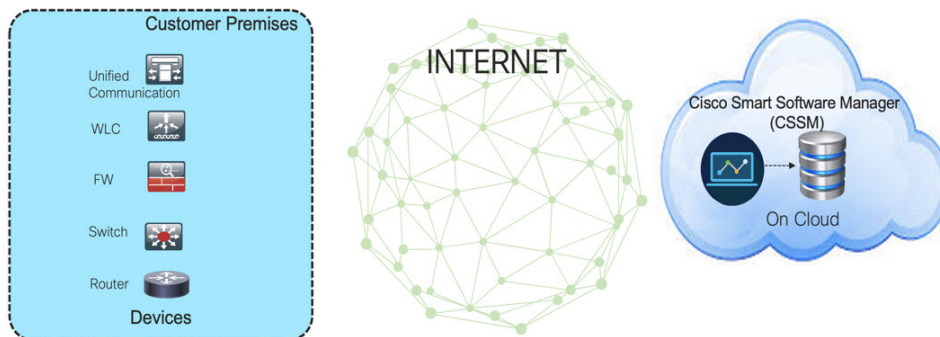
In this topology, devices do not have connectivity to CSSM (software.cisco.com). The user must copy and paste information between Cisco products and CSSM to manually check in and out licenses.

The following figure illustrates the CSLU having No Access to CSSM:
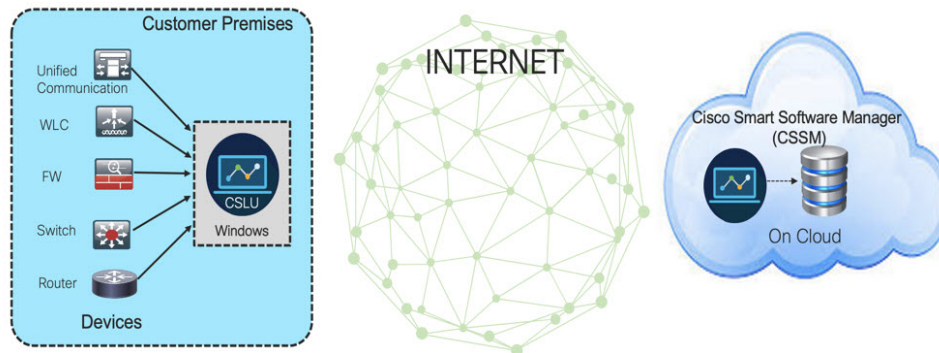
In this topology the devices are connected to the CSLU controller, but there is no connectivity between CSLU and CSSM (Cisco Smart Software Manager – software.cisco.com).

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:
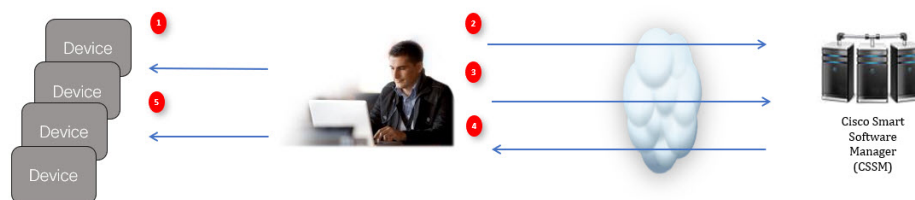
1. Generate a License Usage Data file or AuthCode Request

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

This section contains the following topics:

Procedure to Register Product Instance in CSSM

Step 1   Generate a license usage file from the Router.

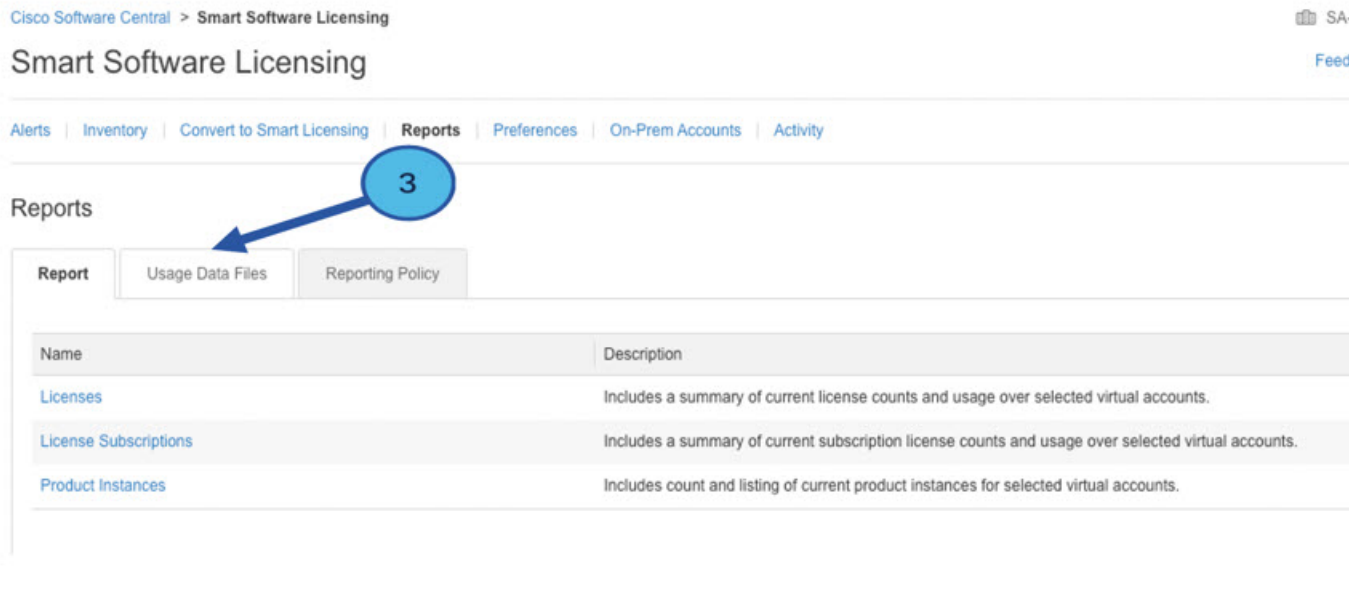In exec mode, perform the following:

Example:

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

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

Step 3   Importing the license usage file to CSSM on Cloud. Click on the **Usage Data Files** tab.
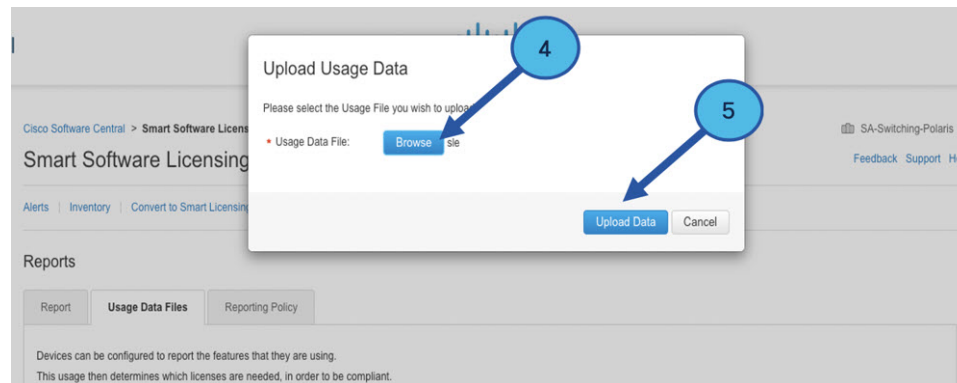
Figure 1: Usage Data File

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

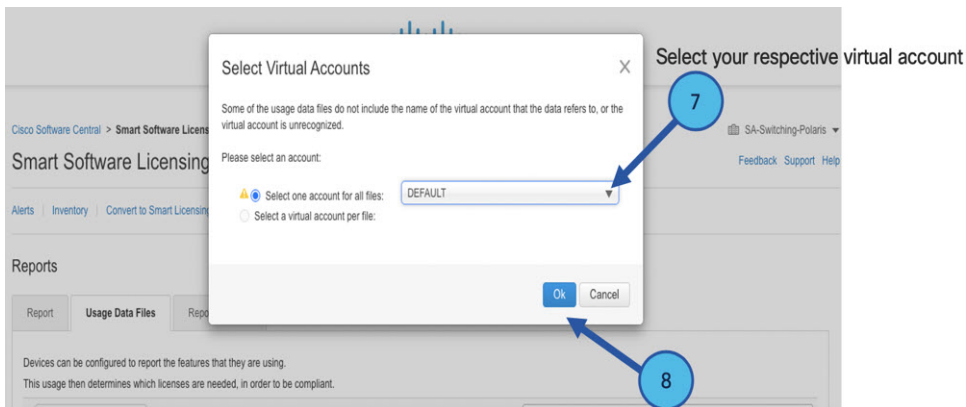**Step 6**   Select the Virtual Account.

Figure 3: Select Account
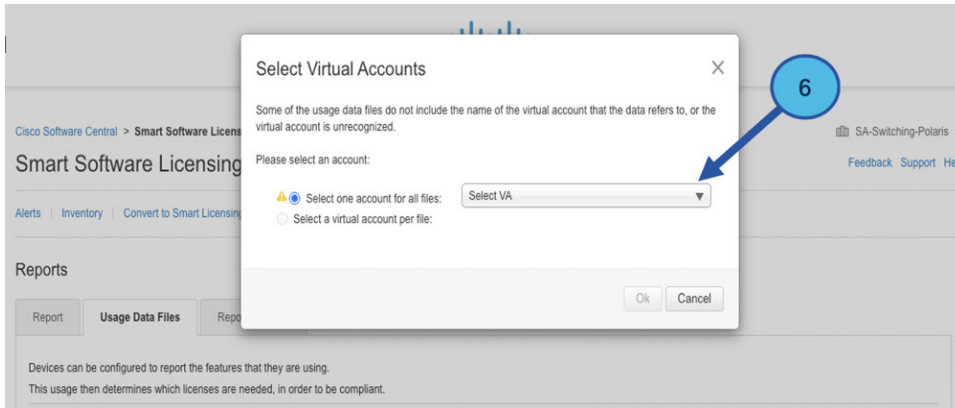
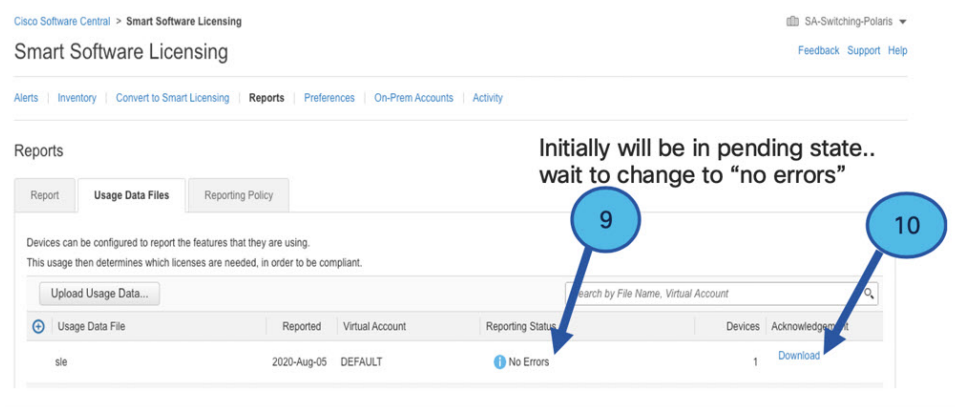**Step 7** From the pull-down, select your respective virtual account.

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

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:FCW2420P0VB;	M2M800	2020-Jul-07 20:15:11 (Reserved Licenses)		Actions ▾
UDI_PID:IR1835-K9; UDI_SN:FHH2416P00Z;	M2M800	2020-Sep-30 01:01:21		Actions ▾
UDI_PID:IR8140H-P-K9; UDI_SN:FDO2420J786;	CGR1000	2020-Sep-08 18:37:24		Actions ▾

Virtual Account: VA-Blackheart ▾

General   Licenses   **Product Instances**   Event Log

Authorize License-Enforced Features...

Search by Name, Product Type

Showing All 6 Records

1 Minor   Hide Alerts

Note   This example shows an IR1835 highlighted. Your product name might be different.

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

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 <flash: | usbflash0:> ACK_slp
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.

a)   The following example is from an IR1800:

Example:

```
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
```

b)   The following example is from an ESR6300:

Example:

```
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 the license is in use.

a) The following example is from an IR1800:

Example:

```
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
```

b) The following example is from an ESR6300:

Example:

```
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
```

Removing the Device from CSSM

Step 1   Navigate back to the product instances tab. Locate your device.
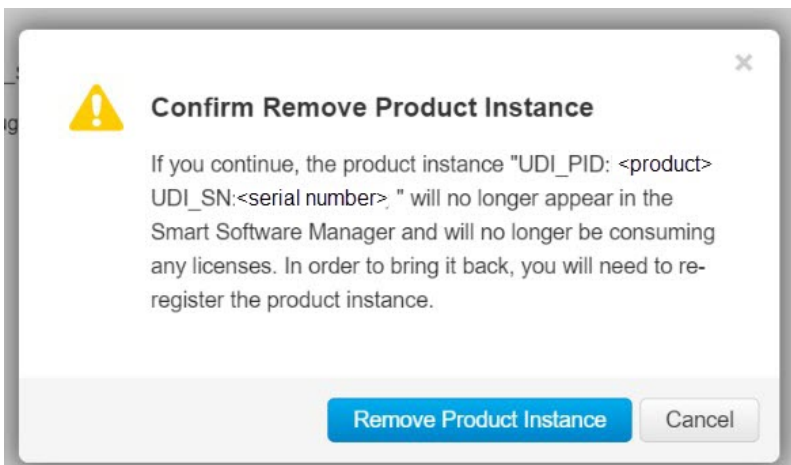
Figure 7: Product Instances
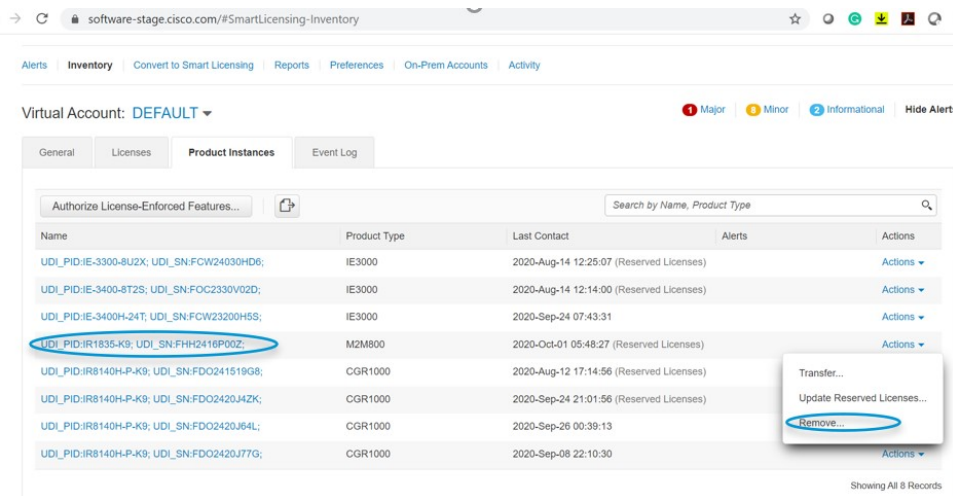
Step 2   Click on **Actions** beside your device, and from those options click **Remove**.

The Confirm Remove Product Instance window appears.
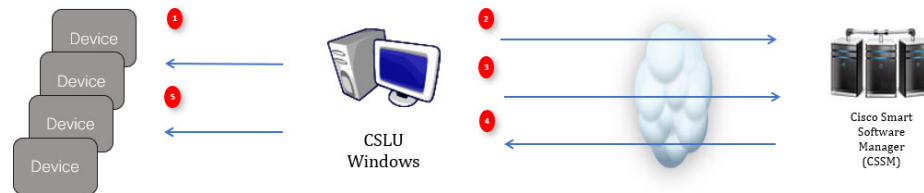
Figure 8: Confirm Remove Product Instance

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:

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.

What to do next

This section contains the following:

Procedure when devices are connected to the CSLU

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

Example from an IR1800:

```
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

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
```

Example from an ESR6300:

```
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

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!
```
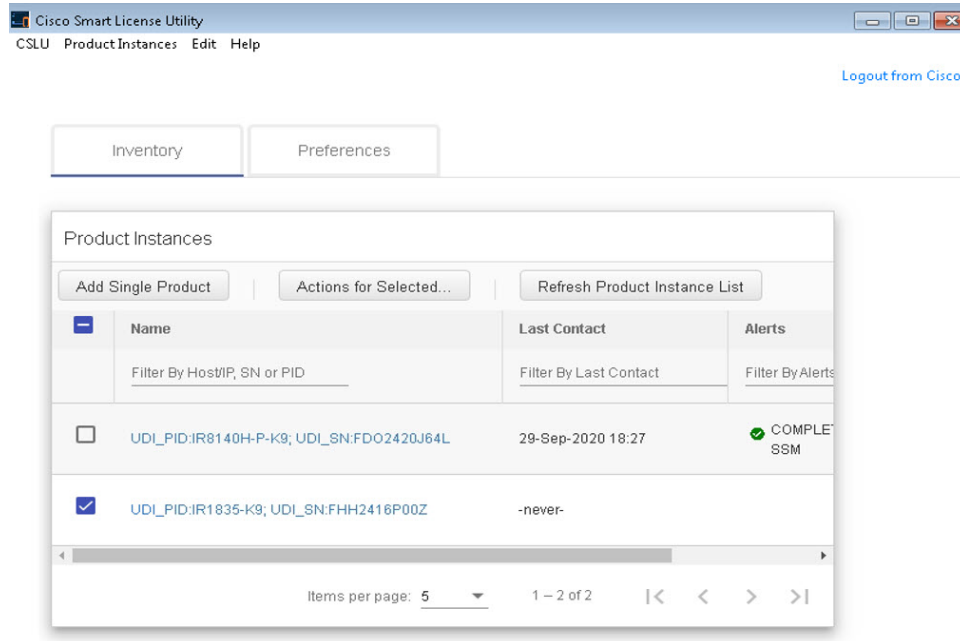
```
Router(config)#end
Router#sh license udi
UDI: PID:ESR-6300-CON-K9,SN:FOC23032UVB
```

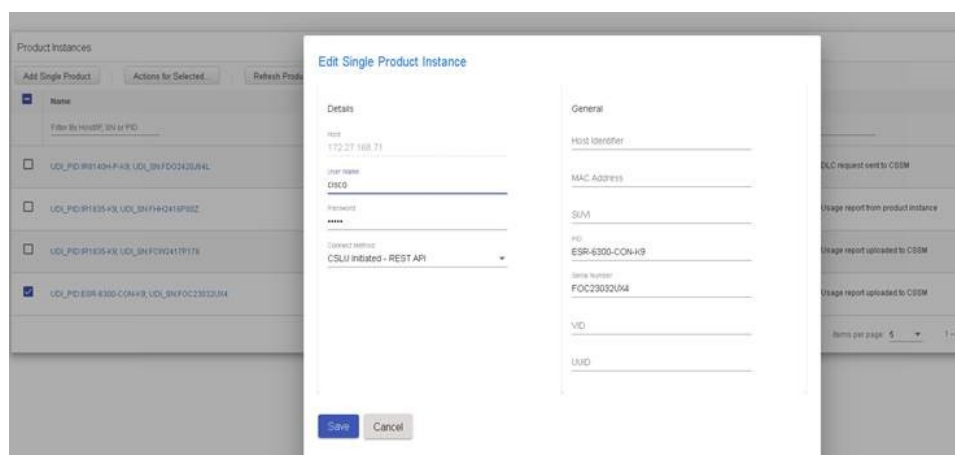**Step 1**   Open the Cisco Smart License Utility (CSLU).

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

Figure 9: Select UDI - IR1835 Example
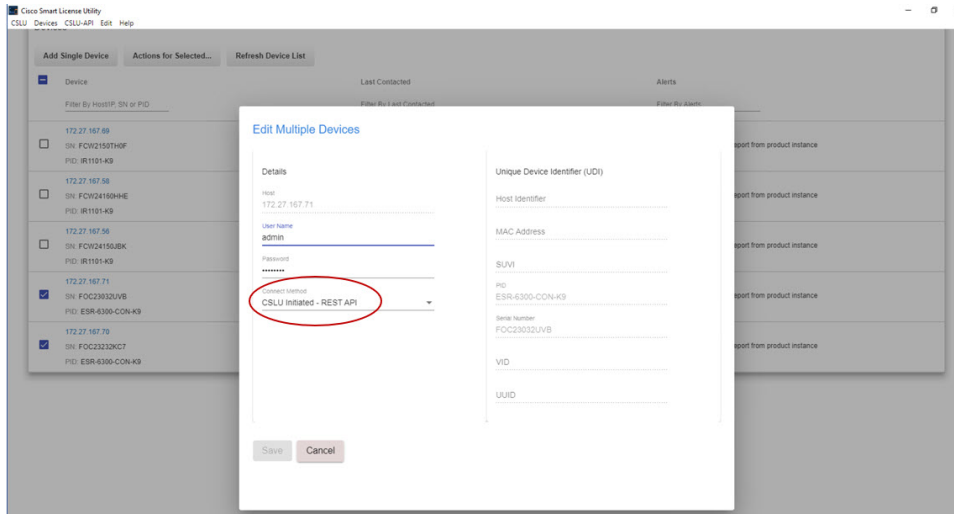

Step 3   The **Edit Single Product Instance** window appears.
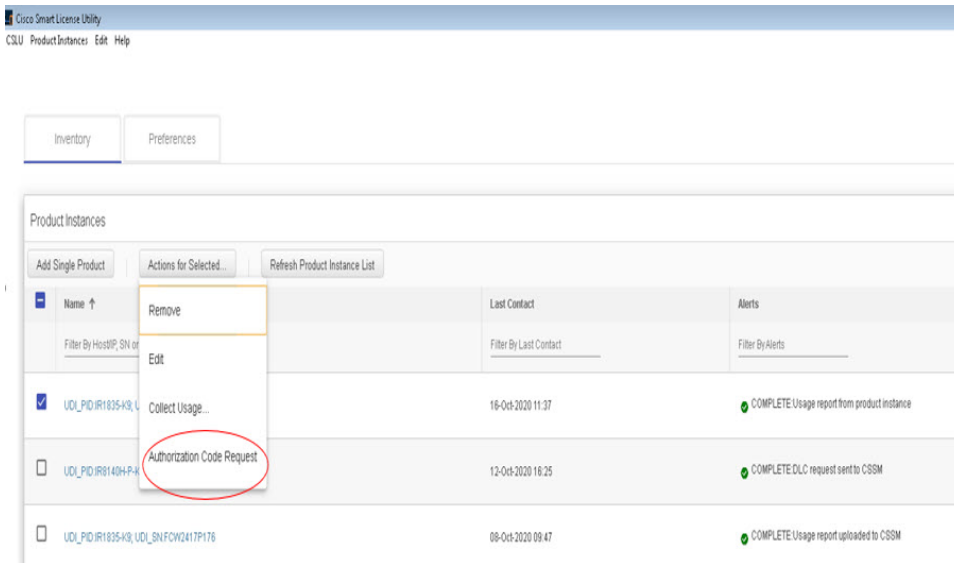
Figure 10: Edit Single Product Instance

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

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

Figure 14: Authorization Request File
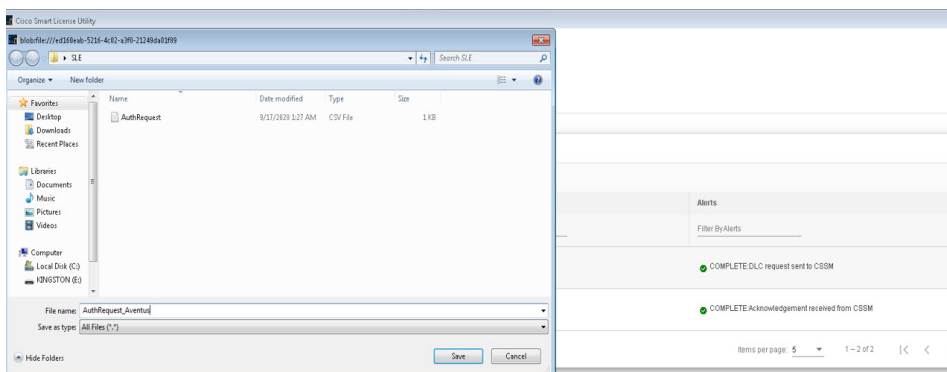
Exporting the AuthRequest File to CSSM

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.

Step 1 Click on the **Product Instances** Tab.

Step 2 Click on **Authorize License-Enforced Features**.

Figure 15: Authorize License-Enforced Features
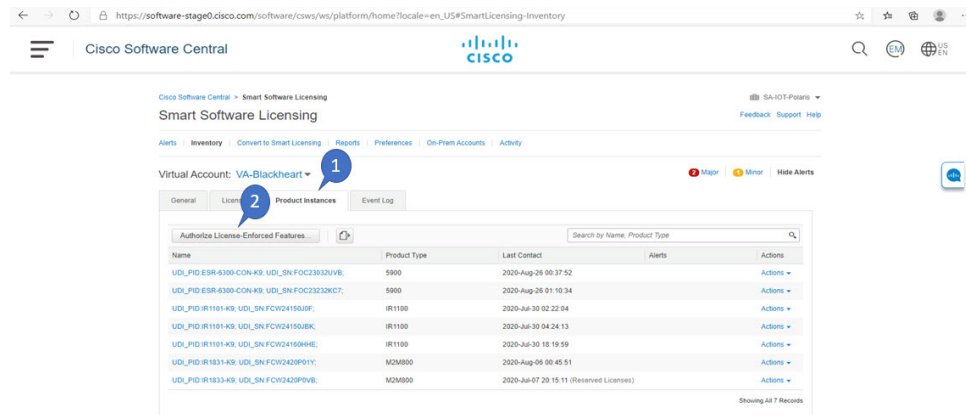
The **Authorize License-Enforced Features** window appears.

Figure 16: Authorize License-Enforced Features
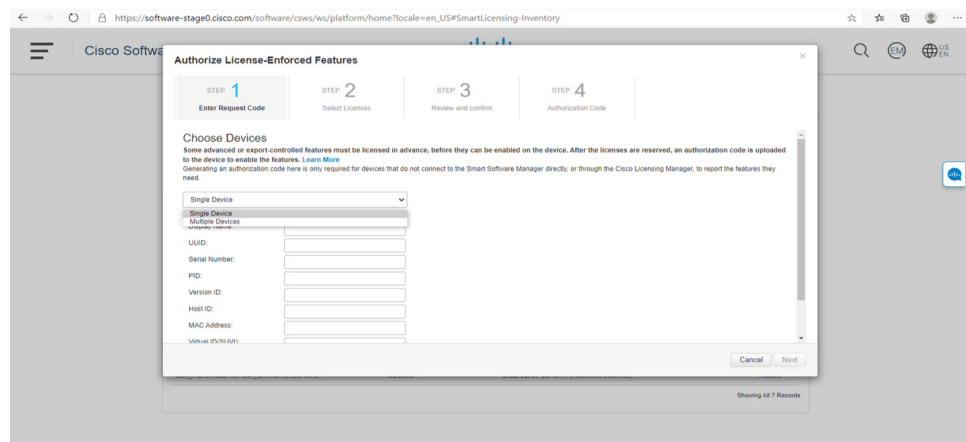
Step 3 Choose **Multiple** or **Single** devices from the pull-down.

Step 4 The window changes to an option to select a device file. Click on **Choose File**.
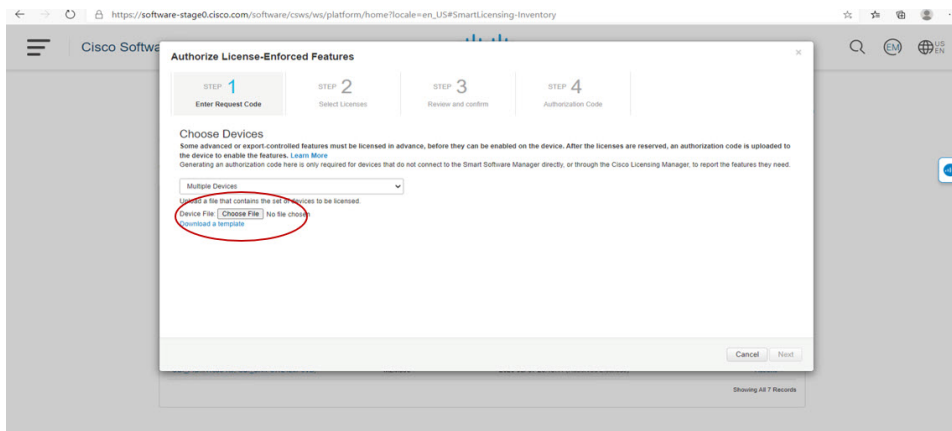
Step 5   A popup window opens to navigate to where you saved your Authorization Request file on your laptop.

Figure 17: Open File Navigation Window
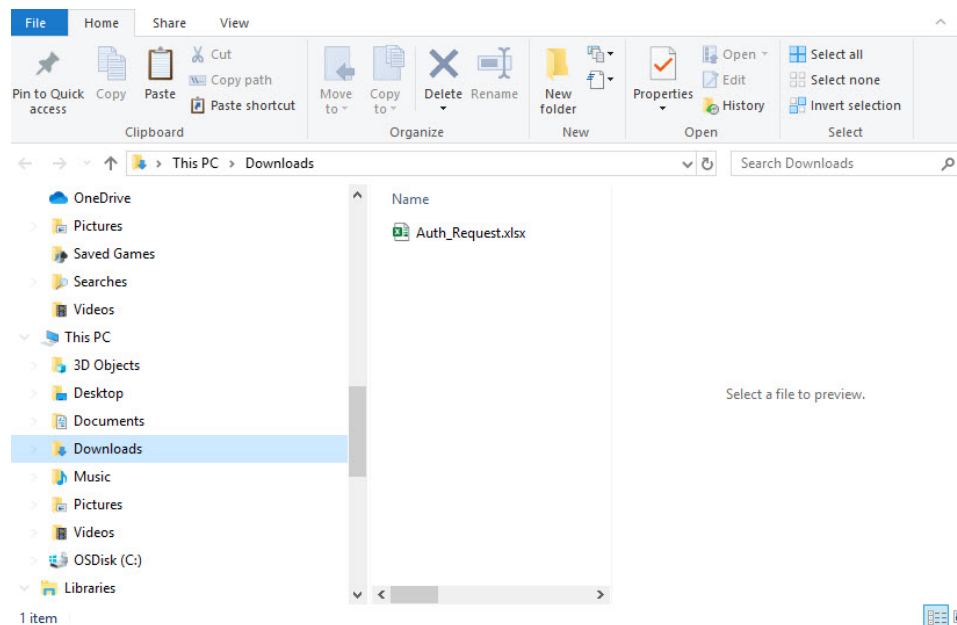
Step 6   Select your file, and then click **Open**.

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

Figure 18: Present Devices
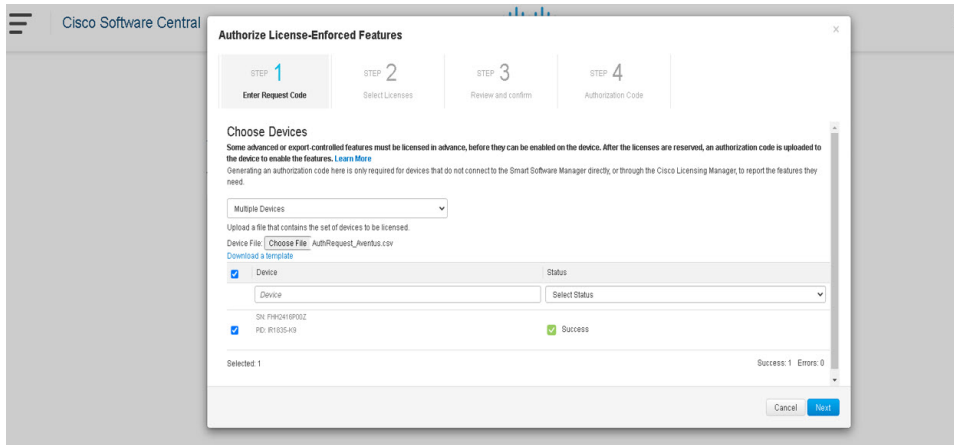
Step 8　　　When successful, click **Next**.

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

Figure 19: Select Licenses
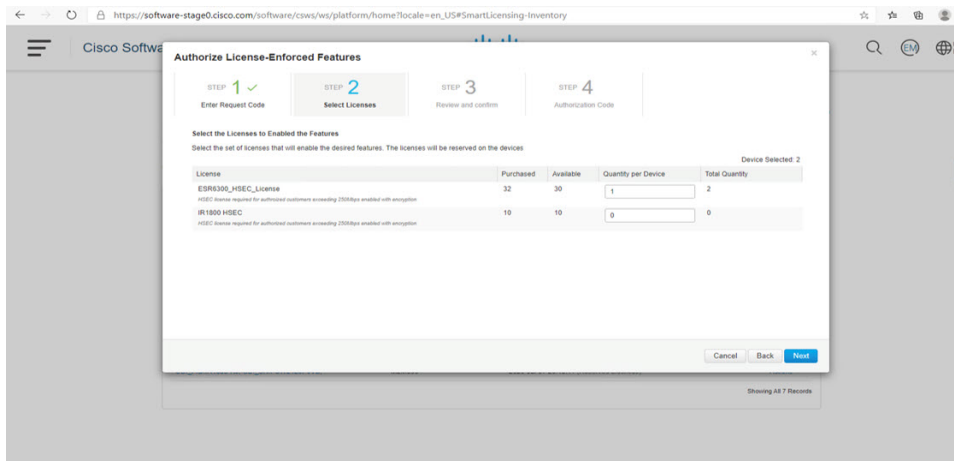
Step 10　　　Under **Quantity per Device**, enter the number you wish.

Figure 20: Enter Number
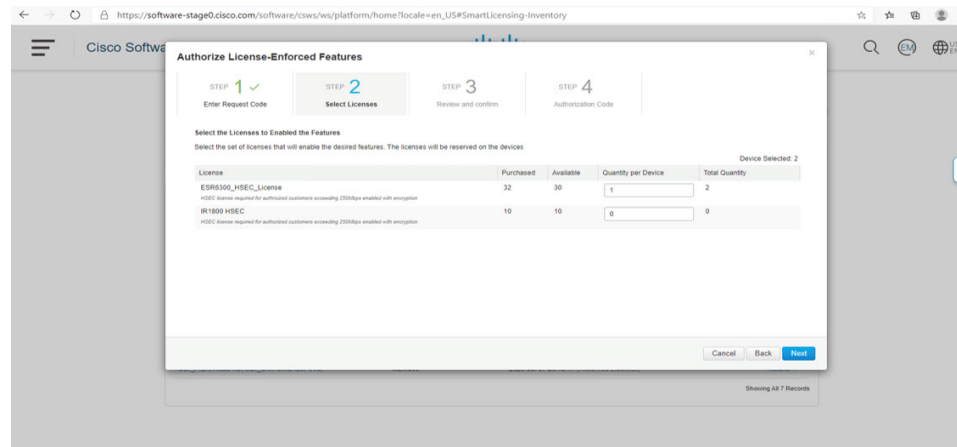
Step 11 If CSSM cannot identify your device from the identifying information, you can select it manually.

Figure 21: Select a Device Type
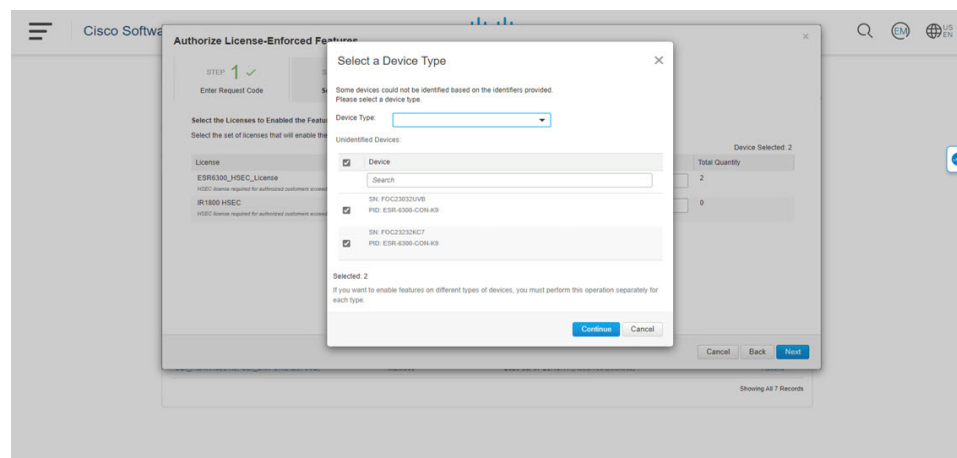
Step 12 Click **Continue**, and the window changes to **Review and Confirm**.

Figure 22: Review and Confirm
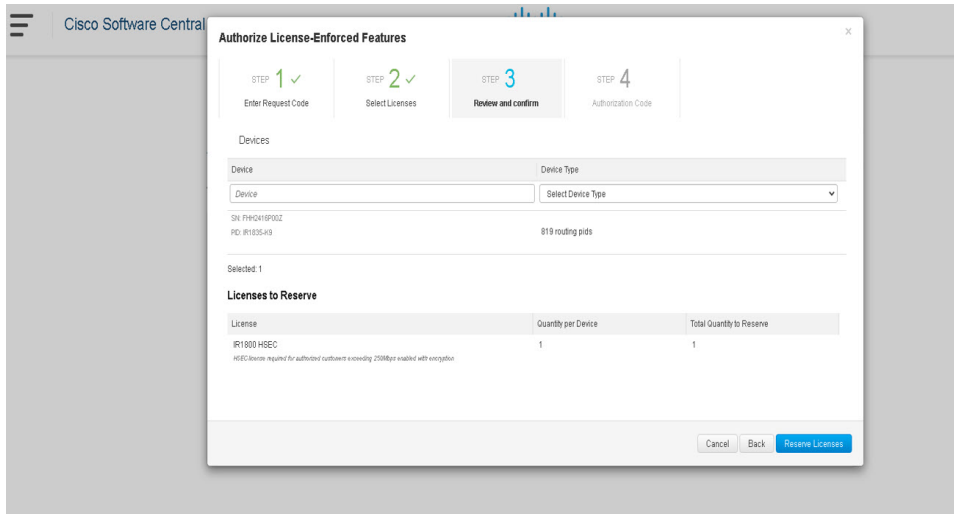
Step 13 Click on **Reserve Licenses**, and CSSM generates feature authorization codes.

Figure 23: Feature Authorization Codes
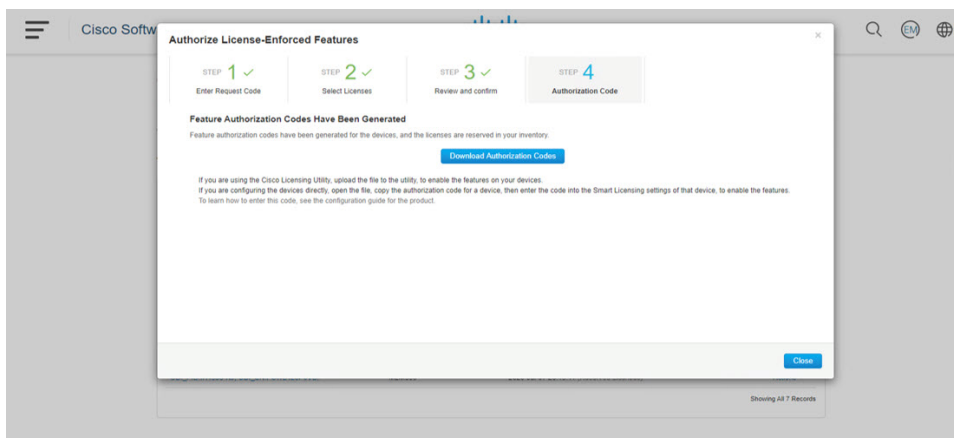
Step 14 Click **Download Authorization Codes**, and a window opens to navigate to where you wish to save the codes.

Figure 24: Save Authorization Code
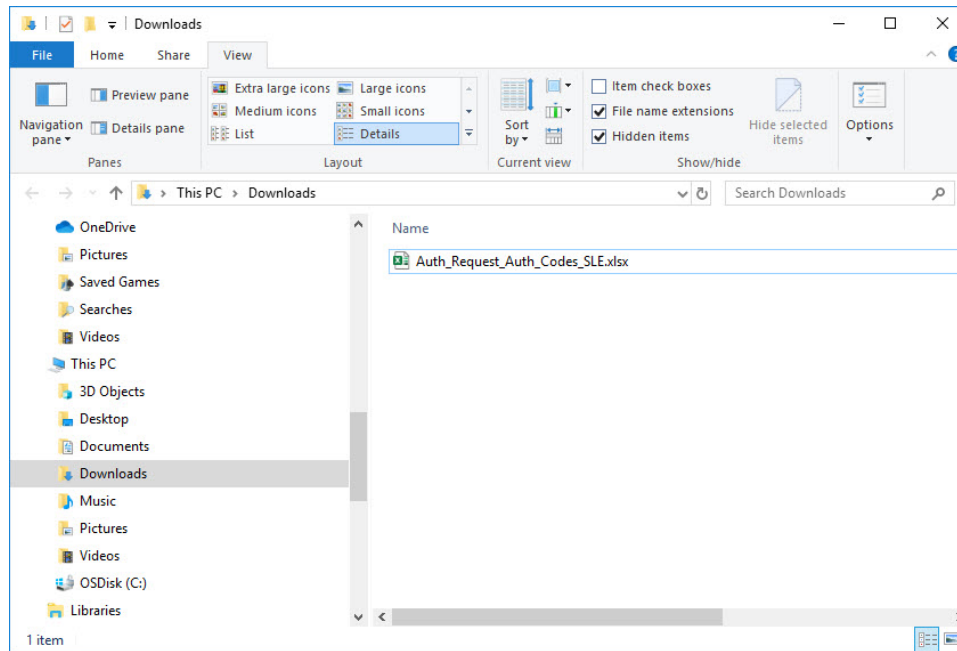
Step 15   Click **Ok**.

Uploading the Authorization Request Code file into CSLU

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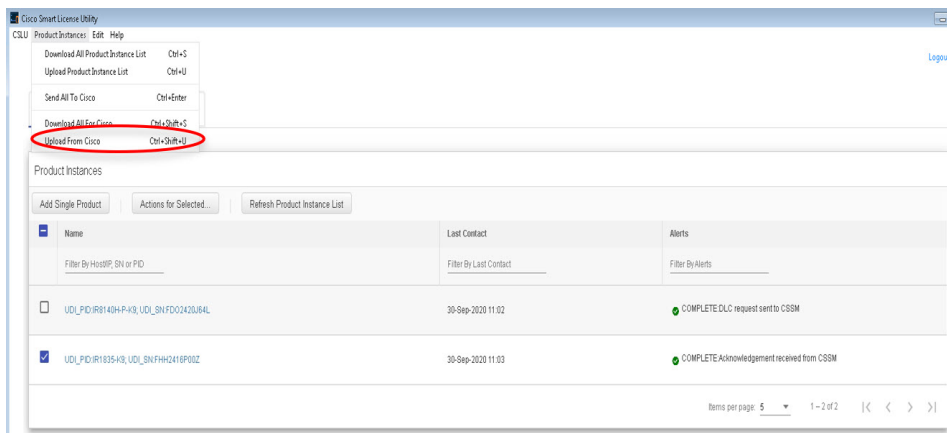
Step 3   There are two options to load your file. **Drag and Drop**, or **Browse** to where you saved your file. This example shows Browse.

Figure 26: Browse to File
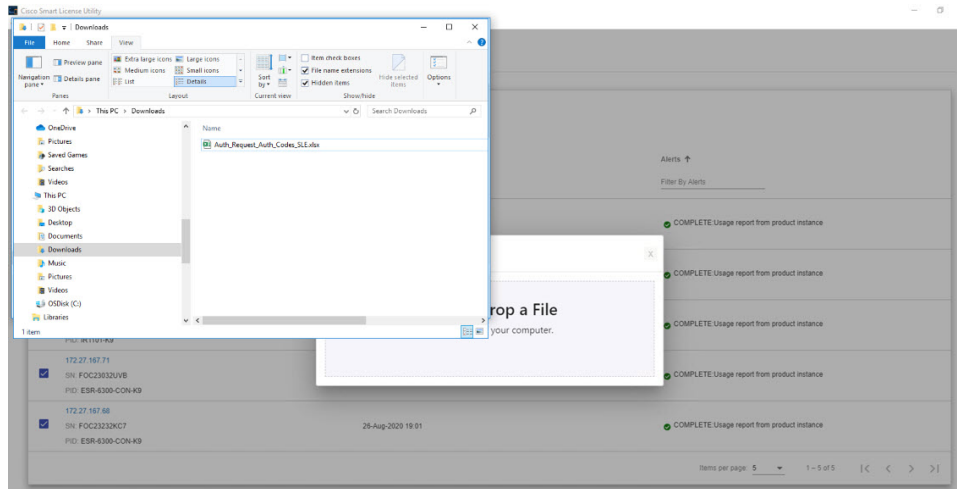
Step 4 Select your authorization code file, and then click **Open**. The system uploads the authorization code file, then a successful upload message appears.

Figure 27: Successful Upload
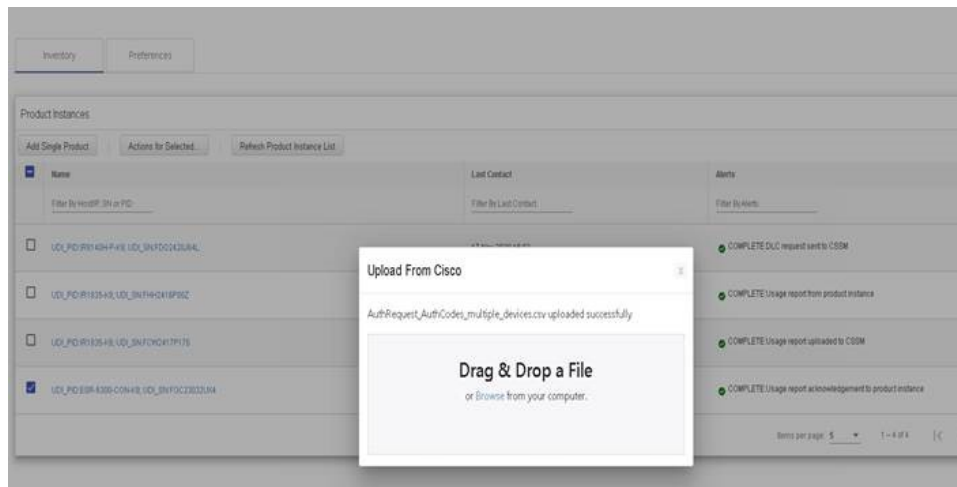
License Installation Process in the Router

Perform the following from the command line interface.

IR1800 Example

Perform the following from the command line interface.

```
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
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
Router(config)#platform hardware throughput level 2G
% Please write mem and reload
% The config will take effect on next reboot
Router(config)#end
Router#
*Sep 30 18:05:55.654: %SYS-5-CONFIG_I: Configured from console by cisco on console
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
```

ESR6300 Example

Perform the following from the command line interface.

```
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

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


Router(config)#platform hardware throughput level 2G
% Please write mem and reload
% The config will take effect on next reboot
Router(config)#end
Router#
*Sep 30 18:05:55.654: %SYS-5-CONFIG_I: Configured from console by cisco on console
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
```

HSEC Installation

This example uses the IR8300 series router.

Perform the following from the command line interface.

```
Router#license smart authorization request add hseck9 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 hseck9
Router(config)#end
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
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
```

Change to Smart Licensing Packaging

This release brings the IoT routing products inline with other Integrated Service Routers (ISR).

Smart Licensing Overview

Cisco Smart Licensing is a flexible licensing model that provides users with an easier, faster, and more consistent way to purchase and manage software across the Cisco portfolio and across their organization. And it's secure. With Smart Licensing users get:

- Easy Activation: Smart Licensing establishes a pool of software licenses that can be used across the entire organization—no more Product Activation Keys (PAKs).

- Unified Management: My Cisco Entitlements (MCE) provides a complete view into all of your Cisco products and services in an easy-to-use portal, so you always know what you have and what you are using.

- License Flexibility: Your software is not node-locked to your hardware, so you can easily use and transfer licenses as needed.

Smart Licensing Using Policy (SLP), was previously referred to as Smart Licensing Enhanced (SLE), and is the default mode starting with Cisco IOS-XE release 17.3.2. SLE replaced Smart Software Licensing. This feature change for Cisco IOS XE release 17.11.1a focuses on the licensing packaging.

License Levels

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

Base Licenses

- Network Essentials

- Network Advantage (includes Network Essentials)

✎

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

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

- Digital Networking Architecture (DNA) Essentials

- DNA Advantage (includes DNA Essentials)

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.

The following tables provide details on the licensing levels:

Table 1: Network Essentials (Perpetual License)

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, 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 2: Network Advantage (Perpetual License) Contains all of the Network Essentials plus the following:

IoT & Mobility	CoAP
Full Routing Functionality	BGP, HSRP, OSPF, ISIS,GLBP
Flexible Network Segmentation	VRF, VXLAN, LISP, SGT, MPLS
High Availability & Resiliency	NSF, GIR, Stackwise Virtual*, ISSU/eFSU, Patching (CLI)
Optimize Bandwidth Utilization with Multicast	MSDP, mVPN, AutoRP, PIM-BIDIR

Table 3: DNA Essentials (3,5,7 year terms)

Basic Automation	- PnP Application - LAN Automation - Embedded Event Manager
Basic Assurance	- Health Dashboards – Network and Client - Basic Device & Wired Client Health Monitoring

Table 4: DNA Advantage (3,5,7 year terms) Contains all of the DNA Essentials plus the following:

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

Licensing Throughput Levels

In addition to configuring the license level, it is also possible to configure the throughput level on the device. The throughput level determines the bandwidth limit which is applied to encrypted traffic. There is no limit applied to the non-encrypted (clear) traffic going through a device.

☞

Important To comply with global export regulations, if more than 250Mbs of encrypted traffic is required, then an "uncapped" – platform dependent – selection must be done on CCW, as well as an HSEC license.

This limit is imposed bidirectionally. This means that if the throughput limit is set to 250Mbps then up to 250Mbps of encrypted traffic can flow through the device in either direction. For example, the device can both receive and transmit up to 250Mbps of encrypted traffic. There is no limit applied on unencrypted traffic.

When the throughput level on the device is set to 'uncapped' there are no limits imposed on both encrypted and unencrypted traffic flowing through it.

✎

Note To avoid confusion on throughput limits and IOS XE software releases, please note the following:

Cisco IOS XE release 17.11.1a and earlier running on the ESR6300, IR1800, and IR8140 platforms support boost, uncapped, and unlimited licenses. These are configured using the **platform hardware throughput level 2G** CLI.

Future Cisco IOS XE release 17.12.1 and later running on the ESR6300, IR1800, and IR8140 support the same licenses, but will be configured using the **platform hardware throughput level uncapped** CLI.

With future Cisco IOS XE release 17.12.1 and later, the **platform hardware throughput level 2G** and the **platform hardware throughput level uncapped** CLIs will both provide the same throughput as the uncapped license.

The following table shows the throughput limits (also referred to as Tier license) supported on IoT devices as of Cisco IOS XE 17.11.1a release.

Platform	25 Mbps bidirectional (Tier 0)	50 Mbps bidirectional	Up to 200 Mbps bidirectional (Tier 1)	250 Mbps bidirectional	2 Gbps	Uncapped (Tier 2)
ESR 6300	N/A	Yes	N/A	Yes	Yes	To be supported starting with 17.12.1

Platform	25 Mbps bidirectional (Tier 0)	50 Mbps bidirectional	Up to 200 Mbps bidirectional (Tier 1)	250 Mbps bidirectional	2 Gbps	Uncapped (Tier 2)
ESR-6300-LIC-K9	N/A	Yes	N/A	N/A	N/A	Yes
IR1101	N/A	N/A	N/A	Yes	N/A	Supported starting with 17.10.1.
IR1800	N/A	Yes	N/A	Yes	Yes	To be supported starting with 17.12.1
IR8100	N/A	Yes	Yes	Yes	Yes	To be supported starting with 17.12.1
IR8300	Yes	N/A	Yes	N/A	N/A	Yes

Command Line Interface

The following commands are available:

`license boot level` `<network-essentials/network-advantage>`

The throughput level can be configured using the following CLI on all IR devices except IR8300:

`platform hardware throughput level` `<limit>`

On the IR8300, the throughput level can be configured using the following CLI:

`platform hardware throughput crypto` `<limit>`

To see the throughput configured on the device, use the following CLI:

`show version | include throughput`
```
The current crypto throughput level is: 50000 kbps
```

Uncapped License Implementation

The Cisco IOS XE 17.11.1 release introduced a new throughput level called "uncapped". This release extends the new throughput level to all of the Cisco IoT routing platforms. The following is a recap of the uncapped license implementation:

Licensing Throughput Levels

The throughput level determines the bandwidth limit which is applied to encrypted traffic. There is no limit applied to the non-encrypted (clear) traffic going through a device.

Important To comply with global export regulations, if more than 250Mbs of encrypted traffic is required, then an "uncapped" – platform dependent – selection must be done on CCW, as well as an HSEC license.

This limit is imposed bidirectionally. This means that if the throughput limit is set to 250Mbps then up to 250Mbps of encrypted traffic can flow through the device in either direction. For example, the device can both receive and transmit up to 250Mbps of encrypted traffic. There is no limit applied on unencrypted traffic.

When the throughput level on the device is set to "uncapped" there are no limits imposed on both encrypted and unencrypted traffic flowing through it.

Note To avoid confusion on throughput limits and IOS XE software releases, please note the following:

Cisco IOS XE release 17.11.1a and earlier running on the ESR6300, IR1800, and IR8140 platforms support boost, uncapped, and unlimited licenses. These are configured using the **platform hardware throughput level 2G** CLI.

Future Cisco IOS XE release 17.12.1a and later running on the ESR6300, IR1800, and IR8140 support the same licenses, but will be configured using the **platform hardware throughput level uncapped** CLI.

With Cisco IOS XE release 17.12.1a and later, the **platform hardware throughput level 2G** and the **platform hardware throughput level uncapped** CLIs will both provide the same throughput as the uncapped license.

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

Platform	25 Mbps bidirectional (Tier 0)	50 Mbps bidirectional	Up to 200 Mbps bidirectional (Tier 1)	250 Mbps bidirectional	2 Gbps	Uncapped (Tier 2)
ESR 6300	N/A	Yes	N/A	Yes	Yes	Supported starting with 17.12.1a
ESR-6300-LIC-K9	N/A	Yes	N/A	N/A	N/A	Yes
IR1101	N/A	N/A	N/A	Yes	N/A	Supported starting with 17.10.1.
IR1800	N/A	Yes	N/A	Yes	Yes	Supported starting with 17.12.1a
IR8100	N/A	Yes	Yes	Yes	Yes	Supported starting with 17.12.1a
IR8300	Yes	N/A	Yes	N/A	N/A	No