

Smart Licensing Using Policy

This chapter contains the following sections:

- SLP Overview, on page 1
- Customer Topologies, on page 6
- License Installation Procedure Full Offline Access Topology, on page 7
- License Installation Procedure CSLU has No Access to CSSM, on page 13
- Change to Smart Licensing Packaging, on page 26
- Uncapped License Implementation, on page 30

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):

IR1101-K9 > Software Licenses

Expand	All Collapse All		
Θs	oftware Licenses		
	SKU	Qty	Estimated Lead Time 🕕
0	SL-IR1101-NE SA Network Essentials License for Cisco IR1101 Industrial ISR More	1	3 days
0	SL-IR1101-NE-NPE SA Network Essentials NPE for Cisco IR1101 Industrial ISR More	1	3 days
0	SL-1101-NE/UNCP-K9 PLH SA Network Essentials Uncapped License for Cisco IR1101 More	1	21 days

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

				Warnings (8):					
Configuration Summary	Vi	w Full Summary			Shipment Package is required. Please adjust yo	ur selection. (CE2	02343)		
Category ()	Qty	Extended List Price (USD)	·	A selection of IR1	100-P-BLANK is required when no Base Module	e is selected. Pleas	se adjust the sel	lections. (CE200440)	
SOFTWARE LICENSE		^							
Software Licenses			0	ption Search 🚺	Multiple Options Search				~
HSEC License			IR1101	I-K9 > HSEC Licen	ise				Key
MODULES		^							
Base Module				d All Collapse All	1				
Expansion Module			Θŀ	ISEC License					
Expansion Module Placement				SKU			Qty	Estimated Lead Time 🚯	Unit List Price (USD)
ACCESSORIES		^	0	L-1101-HSEC-K	9 PLH SA		Qty	21 days	
Antennas				U.S. Export Restric	ction Compliance license for IR1101 More				
Subtotal		1,182.89							
Estimated Lead Time		206 days							

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:

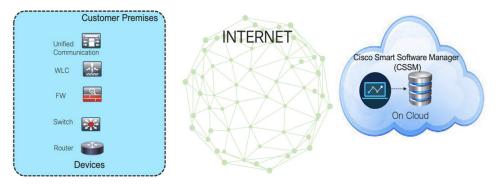
- Install the windows application, to use CSLU as a standalone tool and connect it to CSSM.
- Install the windows application, to use CSLU as a standalone tool and not connect it to CSSM. With this option, the required usage information is downloaded to a file and then uploaded to CSSM. This is suited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

Customer Topologies

IoT Routing platforms use two different topologies.

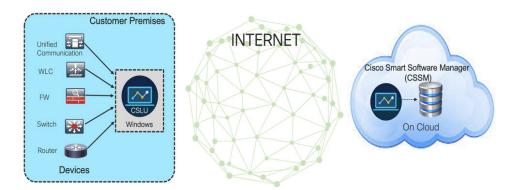
- Full Offline Access
- CSLU has No Access to CSSM

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

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: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

	are Central > Smart Software Lice		1	SA Feed
Alerts In	ventory Convert to Smar	t Licensing Reports Prefer	ences On-Prem Accounts Activity	
Reports	-	3		
Report	Usage Data Files	Reporting Policy		
Name			Description	
License	5		Includes a summary of current license counts and usage over selected virtual accounts.	
License	Subscriptions		Includes a summary of current subscription license counts and usage over selected virtual accounts.	
Product	Instances		Includes count and listing of current product instances for selected virtual accounts.	

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

Click on Upload Data.

Step 5

Figure 2: Browse and Upload

		Upload Usage Data	
	Central > Smart Softwa Software Licer	Usage Data File: Browse Sle	5 In SA-Switching-Polaris - Feedback Support Help
Alerts Inver	ntory Convert to Smart		ncel
Reports			
Report	Usage Data Files	Reporting Policy	
		features that they are using. ses are needed, in order to be compliant.	

Step 6 Select the Virtual Account.

Figure 3: Select Account

		alaala	
	Select Virtual Accounts	×	
Cisco Software Central > Smart Software Licens Smart Software Licensing Alerts Inventory Convert to Smart Licensin	Some of the usage data files do not include t virtual account is unrecognized. Please select an account:	the name of the virtual account that the data refers to, or the Select VA	1 SA-Switching-Polaris - Feedback Support Help
Reports Report Usage Data Files Repo		Ok	
Devices can be configured to report the features to This usage then determines which licenses are no			

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

Figure 4: Select Your Account

	Select Virtual Accounts \times	Select your respective virtual account
Cisco Software Central > Smart Software Licens	Some of the usage data files do not include the name of the virtual account that the data refers to, or the virtual account is unrecognized.	7 t≣ SA-Switching-Polaris ▼
Smart Software Licensing	Please select an account:	Feedback Support Help
Alerts Inventory Convert to Smart Licensin	Select one account for all files: DEFAULT Select a virtual account per file:	
Reports		
Report Usage Data Files Repo	Ok Cancel	
Devices can be configured to report the features This usage then determines which licenses are n		8

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

co Software Central > Smart Software Licen			(B) SA-Switching-Polaris Feedback Support 1		
ts Inventory Convert to Smart Licensir	ng Reports Prefer	ences On-Prem Accour	nts Activity		
eports				vill be in pending state hange to "no errors"	
Report Usage Data Files Rep	orting Policy		wait to c		
Devices can be configured to report the feature This usage then determines which licenses are	, ,	noliant	9		
Upload Usage Data		nymmu.	earch by File	e Name, Virtual Account	
Usage Data File	Reported	Virtual Account	Reporting Status	Devices Acknowledger It	
				Download	

- **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

eneral Licenses Product Instances E	vent Log			
Authorize License-Enforced Features		Search by	Name, Product Type	٩
Name	Product Type	Last Contact	Alerts	Actions
UDI_PID:ESR-6300-CON-K9; UDI_SN:FOC23032UWF;	5900	2020-Sep-24 20:23:59 (Reserve	d Licenses)	Actions -
UDI_PID:ESR-6300-CON-K9; UDI_SN:SJC19700415;	5900	2020-Sep-24 20:41:41 (Reserve	d 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 -

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

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 <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

Procedure

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

Figure 7: Product Instances

Ierts Inventory Convert to Smart Licensing Rep	orts Preferences On-Prem Ad	counts Activity		
/irtual Account: DEFAULT -			1 Major 3 Minor	2 Informational Hide Ale
General Licenses Product Instances	Event Log			
Authorize License-Enforced Features		Searc	h by Name, Product Type	٩
Name	Product Type	Last Contact	Alerts	Actions
UDI_PID:IE-3300-8U2X; UDI_SN:FCW24030HD6;	IE3000	2020-Aug-14 12:25:07 (Res	erved Licenses)	Actions -
UDI_PID:IE-3400-8T2S; UDI_SN:FOC2330V02D;	IE3000	2020-Aug-14 12:14:00 (Rese	erved 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 (Rese	rved Licenses)	Actions -
UDI_PID:IR8140H-P-K9; UDI_SN:FDO241519G8;	CGR1000	2020-Aug-12 17:14:56 (Rese	rved Licenses) T	ransfer
UDI_PID:IR8140H-P-K9; UDI_SN:FDO2420J4ZK;	CGR1000	2020-Sep-24 21:01:56 (Rese	erved Licenses) U	pdate Reserved Licenses
UDI_PID:IR8140H-P-K9; UDI_SN:FDO2420J64L;	CGR1000	2020-Sep-26 00:39:13		emove
UDI PID:IR8140H-P-K9; UDI SN:FDO2420J77G;	CGR1000	2020-Sep-08 22:10:30		Actions -

Step 2 Click on Actions beside your device, and from those options click Remove.

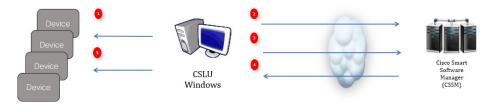
The Confirm Remove Product Instance window appears.

Figure 8: Confirm Remove Product Instance

A	Confirm Remove Product Instance If you continue, the product instance "UDI_PID: <product> UDI_SN:<serial number="">, " will no longer appear in the Smart Software Manager and will no longer be consuming any licenses. In order to bring it back, you will need to re- register the product instance.</serial></product>
	Remove Product Instance Cancel

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.

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#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
```

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 - IR1835 Example

Cisco Sm	mart License Utility				
U Proc	duct Instances Edit H	Help		L	.ogout from Cisc
	Inventory	Preferences			
Pro	oduct Instances				
A	Add Single Product	Actions for Selected	Refresh Product Instance Lis	st	
-	Name		Last Contact	Alerts	
	Filter By Host/IP,	SN or PID	Filter By Last Contact	Filter By Alerts	
C	UDI_PID:IR8140	0H-P-K9; UDI_SN:FDO2420J64L	29-Sep-2020 18:27	COMPLE SSM	
	UDI_PID:IR183	5-K9; UDI_SN:FHH2416P00Z	-never-		
•		ltems per page: 5 💌	1 – 2 of 2 < <	> >	

Step 3 The Edit Single Product Instance window appears.

Figure 10: Edit Single Product Instance

Produ	uct instances	Edit Single Product Instance		
Add	Single Product Actions for Selected Petresh Produ	Eur ongie i rouder materice		
	Natie	Details	General	
	Priller The Heart DP, TAN AN PRO	nin 172.27.568.71	Host Identifier	
	COLIND WITHOUT AND COLINY CODADANAL	Liner Hanne. CISCO	MAC Address	DLC request cent to CS3M
	UCLIPDIRITIES HOL UDLININHONISPIEZ	Parsent	SUM	Usage report from product instance
	UDLIND PRESSAY, UDLING CWANTERINE	Convect Initiated - REST API +	+0 ESR-6300-CON-K9	Lisage report uptoaded to CSSM
	UDI_PEXEMP #300-COMPR_UDI_SN/PCC23032UM		F/0C230321644	Usage report uploaded to CDDM
			VD	dama per page 👩 👻 1
-			UUD	-
		Save Cancel		

Step 4The Edit Multiple Devices window appears. Supply your account password and click Save.Figure 11: Edit Multiple Devices

	Device	Last Contacted		Alerts		
	Filter By HostiTP, SN or PID	Filter Ry Last Contacted	1	Filter Ry Alerts	-	
	172.27.167.69 SN: FCW2150TH0F PID: IR1101-K9	Edit Multiple Devices			apart from product instance	
	172.27.167.58 SN: FCW24150HHE PID: IR1101-K9	Details Heat 172.27.167.71	Unique Device Identifier (UDI) Host Identifier		eport from product instance	
	172.27.167.56 SN: FCW24150JBK PID: IR1101-K9	User Name admin Password	MAC Address		apart from product instance	
	172.27.167.71 SN: FOC23032UVB PID: ESR-6300-CON-K9	Connect Method CSLU Initiated - REST API	PID ESR-6300-CON-K9 Serial Number		eport from product instance	
-	172.27.167.70 SN: FOC23232KC7 PID: ESR-6300-CON-K9		FOC23032UVB		eport from product instance	
			UUID			
		Save Cancel				

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

Figure 12: Actions for Selected Devices

Ci	sco Smart	t License Utility			
CSLU	Produc	tInstances Edit Help			
		Inventory	Preferences		
	_				
	Prode	uct Instances			
	FIQU	uct Instances			
	Add	Single Product	Actions for Selected Refresh Product Instance	e List	
1S	•	Name 🕈	Remove	Last Contact	Alerts
		Filter By HostVP; SN or	Edt	Filter By Last Contact	Filter By Alerts
	V	UDI_PID1R1835-K9; U	Collect Usage	18-0d-2020 11:37	COMPLETE Usage report from product instance
	٥	UDI_PID1R8140H-P-K	Authorization Code Request	12-Oct-2020 18:25	COMPLETE DLC request sent to CSSM
	0	UDI_PID1R1835-K9; U	DL_SNFCW2417P176	08-0tt-2020 09:47	COMPLETE:Usage report uploaded to CSSM

- **Step 6** Select Authorization Code Request.
- Step 7The 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.
- After uploading to CSSM you will be able to download the file containing the authorization codes for devices you selected.
- Please upload this file using the "Upload From CSSM" menu option to apply the authorization codes for the devices.

Accept Cancel

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

Figure 14: Authorization Request File

Gisco Smart License Utility				
blobcfile:///ed160eab-5216-4c02-a3f0-21249da01f89				
OO + at		✓ 4y Search SLE	٩	
Organize 👻 New folder			ii • 😧	
Y Favorites	Date modified Type	Size		
E Deiktop AuthRequest	9/17/2020 1:27 AM CSV File	1 KB		
Courters Documents Music Pictures Videos				Aberts Filter By Aperts
Computer Local Disk (C:) MINGSTON (E:)				COMPLETE DLC request sent to CSSM
File name: AuthRequest_Aventus Save as type: All Files (*.*)				COMPLETE Acknowledgement received from CSSM
Hide Folders		Save	Cancel	ttems per page: <u>5</u> ▼ 1−2 of 2 < <

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

Cisco	Software Central	cisco					(●	₿ ^{US} EN
	Cisco Software Central > Smart Software Licensing				💼 SA-IOT-Polaris 👻			
	Smart Software Licensing				Feedback Support Help			
	Alerts Inventory Convert to Smart Licensing Reports	Preferences On-Prem A	ccounts Activity					
	1				n narada naradari			
								- (
	Virtual Account: VA-Blackheart			0 M	ajor 1 Minor Hide Alerts			l
		Event Log		2 Mi	ajor 🚺 Minor Hide Alerts			(
		Event Log	Search by Name, F		Ajor Minor Hide Alerts			(
	General Licent 2 Product Instances	Event Log Product Type	Bearch by Name, P Last Contact					
	General Licen 2 Product Instances Authorize License-Enforced Features.			Product Type	٩			(
	Central Licen 2 Product Instances Authorize License Enforced Features Name	Product Type	Last Contact	Product Type	Q. Actions			(
	General License Enforced Features	Product Type 5900	Last Contact 2020-Aug-26 00:37:52	Product Type	Q Actions Actions +			(
	General Loom 2 Product Instances Authorize License Enforced Features Rame UD_PD ESR-4309-CON-43, UD_SNF0C220320V7E; UD_PD ESR-4309-CON-43, UD_SNF0C220320V7;	Product Type 5900 5900	Last Contact 2020-Aug-26 00:37:52 2020-Aug-26 01:10:34	Product Type	Q Actions Actions + Actions +			(
	Central Loom 2 Product Instances Authorize License Enforced Features Up, PIO ESH 4300 COH HR, Up, SNF FOC233220476, Up, PIO ESH 4300 COH HR, Up, SNF FOC233220477, Up, PIO ESH 4300 COH HR, Up, SNF FOC23223047, Up, PIO ESH 4300 COH HR, Up, SNF FOC23232047, Up, PIO ESH 4300 COH HR, PIO ESH	Product Type 5900 5900 IR1100	Last Contact 2020-Aup-26 00:37:52 2020-Aup-26 01:10:34 2020-Aup-26 01:00:222:04	Product Type	Q Actions Actions + Actions +			ĺ
	General Loon Product Instance Arborice License Enforced Features Image: Comparison of the	Product Type 5900 5900 IR1100 IR1100	Last Contact 2020-Jug-26 90 37 52 2020-Jug-26 91 10 34 2020-Jug-26 91 10 34 2020-Jug-30 02 22 04 2020-Jug-30 04 24 13	Product Type	م) Actions ب Actions ب Actions ب			ĺ

The Authorize License-Enforced Features window appears.

Figure 16: Authorize License-Enforced Features

\leftrightarrow \rightarrow O \triangle https://softw	vare-stage0.cisco.com/software/	/csws/ws/platform/home?lo	cale=en_US#SmartLicensing	Inventory			☆ ☆	۰۰۰ 😩 的
							~ ~ ~	
Cisco Softwa	Authorize License-Enfor	rced Features				×	Q (
	STEP 1	STEP 2	STEP 3	STEP 4		- 1		
	to the device to enable the feature	es. Learn More			re reserved, an authorization code is upload Licensing Manager, to report the features they			
	Single Device		-			- 11		_
	Single Device Multiple Devices							
	UUID: Serial Number:					- 11		
	PID:							
	Version ID:							
	Host ID:							
	MAC Address:							
	Virtual ID/SI IVIV							
					Cancel	Next		
					Showing AB 7	Records		

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**.

			also also				
Cisco Softwa	Authorize License-Enfor	ced Features			×	Q 🕑	⊕US EN
	STEP 1	STEP 2	STEP 3	STEP 4			
	Enter Request Code	Select Licenses	Review and confirm	Authorization Code			
	the device to enable the features.	Learn More are is only required for devices that		on the device. After the licenses are reserved, an a lanager directly, or through the Cisco Licensing Manag			
					Cancel Next		

Step 5 A popup window opens to navigate to where you saved your Authorization Request file on your laptop.

File Home Share View		~ 🔞
Pin to Quick Copy Paste Copy path access	Move Copy to to to crganize Organize	
← → 🗠 🛧 💺 > This PC > Downloa	ads	✓ ט Search Downloads
 OneDrive Pictures Saved Games Searches Videos This PC 3 D Objects Desktop Documents Downloads Music Pictures Videos OSDisk (C:) 	Auth_Request.xlsx	Select a file to preview.
 item 	v < >	

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

-			بلد باد				0
Cisco Software Central	Authorize License-Enfo	×	Q				
	STEP 1	STEP 2	STEP 3	STEP 4			
	Enter Request Code	Select Licenses	Review and confirm	Authorization Code			
	the device to enable the features	Learn More here is only required for devices that of devices to be licensed.			re reserved, an authorization code is uploaded to sco Licensing Manager, to report the features they	*	
	Device		SI	tatus			
	Device			Select Status	v		
	SRL FHH2416P00Z		C	Surcess		L	
	Selected: 1				Success: 1 Errors: 0		
					Cancel	ext	

- **Step 8** When successful, click **Next**.
- **Step 9** The **Select Licenses** Tab opens.

Figure 19: Select Licenses

Cisco Softwa	Authorize License-Enfo	rced Features					3	×	Q 🖲) (#)
			0							
	STEP 1 🗸	STEP 2	STEP 3		STEP 4					
	Enter Request Code	Select Licenses	Review and confirm		Authorizatio	n Code				
	Select the Licenses to Enabled	the Features								
		I enable the desired features. The lice	inses will be reserved on the de	levices						
							Device Selected: 2			
	License			Purchased	Available	Quantity per Device	Total Quantity			
	ESR6300_HSEC_License	itomars exceeding 2505/bps enabled with encrypti		32	30	1	2			
	IR 1800 HSEC			10	10	0	0			
	HSEC license required for authorized out	stomers acceeding 2505/bps anabled with encrypti	lon .							
							Cancel Back Next			

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

Figure 20: Enter Number

Cisco Softw	Authorize License-Enfo	read Features					×	Q (M)	
	Authorize License-Erro	rced Features							
	STEP 1 🗸	STEP 2	STEP 3		STEP 4				
	Enter Request Code	Select Licenses	Review and confirm		Authorizatio	n Code			
	Select the Licenses to Enabled	I the Features							
	Select the set of licenses that will	I enable the desired features. The lic	enses will be reserved on the	e devices					
	License			Purchased	Available	Quantity per Device	Device Selected: 2 Total Quantity		
	ESR6300_HSEC_License	itomers exceeding 2501/bps enabled with encryp		32	30	1	2		
	IR1800 HSEC			10	10	0	0		
	HSEC license required for authorized out	stomers exceeding 2505/bps enabled with encryp	dion .						
							Cancel Back Next		
							Cancer Dack Inter		
							Showing All 7 Records		

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

Figure 21: Select a Device Type

-		di di		
Cisco Softwa	Authorize License-Enforced Fer	turne	×	
	STEP 1 - S Enter Request Code 5	Select a Device Type × Some devices could not be identified based on the identifiers provided. Parale select a device type.		
	Select the Licenses to Enabled the Featur Select the set of licenses that will enable the	Device Type:	Device Selected: 2	_
	License	Device	Total Quantity	
	ESR6300_HSEC_License HSEC isonae required for authroited customers enceed	Search	2	
	IR1800 HSEC HSEC licence required for authorized customers access	SR FOC23032UVB FID: ESR-6500-CON-KS	0	
		SH: FOC2222067 PID: ESR-8309-COH-K8		
		Belicked 2 If you want to evable features on different types of devices, you must perform this operation separately for each type.		
		Continue Cancel	Cancel Back Next	
			Showing All 7 Records	

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

Figure 22: Review and Confirm

_		ali ali ali a								
=	Cisco Software Central	Authorize License-Enfo	rced Features				×			
		STEP 1 🗸	STEP 2 ✓ Select Licenses	STEP 3 Review and confirm	STEP 4 Authorization Code					
		Devices								
		Device		C	Device Type					
		Device			Select Device Type		~			
		SN: FHH2416P00Z PD: IR1835-K9		8	19 routing pids					
		Selected: 1								
		License		Qu	uantity per Device	Total Quantity to Reserve				
		IR1800 HSEC	ters exceeding 250Mbps enabled with encryptic	1		1				
		metowene ngillel to dated and	то точточку глятуй байла ИСТ босуро	27						
	ļ					Cancel Back Reserve Lic	inses			

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

Figure 23: Feature Authorization Codes

Cisco Softv			de de			_	0		⊕US EN
	Authorize License-Enfor	rced Features				×	C	EM	WEN
	STEP 1 🗸 Enter Request Code	STEP $2 \checkmark$ Select Licenses	STEP 3 ~ Review and confirm	STEP 4 Authorization Code					
		odes Have Been Generated	d the licenses are reserved in your in	wentory.					
			Download Authorizati						•
	If you are configuring the dev	enting Utility, upload the file to the util tics derectly, open the file, copy the av- le, see the configuration guide for the	thorization code for a device, then e		ettings of that device, to enable the features.				
						lose			
					Showing All 7 Re	ecords			

 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

File Home Share	View					~ (
Navigation Details pane	₿₿ List	Small icons	↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓	 ☐ Item check boxes ✓ File name extension ✓ Hidden items 	Hide selected Options	
Panes	La	yout	Current view	Show/h	ide	
$\leftrightarrow \rightarrow \cdots \uparrow i \Rightarrow $ This	PC > Downloads			~ ©	Search Downloads	Q
len OneDrive		^ Name				
🚡 Pictures		Auth	Request Auth Codes	SLE.xlsx		
🍺 Saved Games						
Discourse 🐌 Searches						
🕫 Videos						
interview 🕒 🕒 🕒						
👌 3D Objects						
🔚 Desktop						
Documents						
🐌 Downloads						
🐌 Downloads 🌗 Music						
		1				
Music		1				
) Music		1				
 Music Pictures Videos 		~ <				

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

Cisco Smar	t License Utility		
SLU Produc	tinstances Edit Help		
	wnload All Product Instance List Cbrl+S Ioad Product Instance List Cbrl+U		Lego
Ser	d All To Cisco Ctrl+Enter		
_ Do	emload All For Cisco Chrl+Shift+S		
Up	load From Cisco Ctrl+Shift+U		
Prod	uct Instances		
Add	Single Product Actions for Selected Refresh Product Instance List		
	Name	Last Contact	Alerts
	Filter By HostilP, SN or PID	Filter By Last Contact	Filter By Alerts
	UDL PDIR8140H-P-K9, UDL SN FD02420J84L	30-Sep-2020 11.02	COMPLETE DLC request sent to CSSM
	UDL_PD1R163548; UDL_SNFHH2418P00Z	30-Sep-2020 11:03	COMPLETE Acknowledgement received from CSSM
			Items per page: 5 1−2 of 2 < < > >

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.

🛛 🗹 📕 🖛 🗍 Downloads	- 0 ×	
👔 Weview pane	ten dreck beses Tier name extensions Tier name extensions Standard Ress Standard Ress	
→ ↑ ▲ This PC → Downloads	✓ δ Search Downloads ,P	
OneDrive Name		
Pictures Auth_Request_Auth_Codes_SLExt Auth_Request_Auth_Codes_SLExt	la	
p saved cames b Searches		Alerts 🕈
Tideos		Filter By Alerts
Inis PC		
B 3D Objects		
Desktop Documents		COMPLETE: Usage report from product instance
Downloads		x
Music		
he Pictures		COMPLETE Usage report from product instance
Videos SDisk (C:)		
Elbraries v <	rop a File	
dem .	🔃 🖬 your computer.	COMPLETE Usage report from product instance
PDD. RCTUT-NV		
172.27.167.71		
SN: FOC23032UVB	-	COMPLETE Usage report from product instance
PID: ESR-6300-CON-K9		
172.27.167.68		
SN: F0C23232KC7	26-Aug-2020 19:01	 COMPLETE Usage report from product instance
PID: ESR-6300-CON-K9		
		Items per page: 5

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

roduct instances			
Add Single Product Actions for Selected Refeesh Produ	et Instance List		
C Kana	Last Contact	Allerts:	
File by Heat R 3N or PC	Filler Bri Last Contact	Fine Bollem	
О королониче кориссирае.		COMPLETE DUC request set to CSSM	
	Upload From Cisco	T	
О цоциональны цоцилононализа		COMPLETE Usage report spittaded to CODM	
С ир.но.шинальсоние.ор.дигосталали	Drag & Drop a File or Browne from your computer.	COMPLETE Usage report as non-kedgement to product instance	

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:
                     Entitlement tag
 License
                                                 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
                                                1 IN USE
 hseck9 (IR1800_HSEC)
 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
                         (ESR6300_HSEC_License) 1 IN USE
(ESR6300 P 2G A) 1 IN USE
 hseck9
  network-advantage 2G (ESR6300 P 2G A)
```

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:FD02523J6N1
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:
                Entitlement Tag
 License
                                                      Count Status
  _____
                           _____
 network-advantage_T1 (IR8300_NA_T1_PERF)
                                                        1 IN USE
                        (IR8300 HSEC)
 hseck9
                                                         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)



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)), PBF 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	СоАР
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 AnalyticsDNA Service for Bonjour
Assurance & Analytics	Compliance, Custom ReportsSwitch 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.

Ś

C(-

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
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

It 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.

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

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