Cisco Smart Licensing Utility
User Guide

Version 2.2.0

Table of Contents

Preface

This preface describes the objectives and organization of this document and explains how to find additional information on related products and services.

Objectives

This document provides an overview of software functionality that is specific to the Cisco Smart License Utility (CSLU). This section refers you to other related documentation that also might be useful to you.

Related Documentation

The following documentation items are available for CSLU:

- *CSLU User Guide*

- *CSLU Installation Guide*

- *CSLU Release Notes*

Document Convention

This document uses the following conventions:

Convention	Description
bold	Bold text indicates the commands and keywords used in one or moresteps.
Italic	Italic text indicates arguments for which the user supplies the values ora citation of another document.
[x]	Square brackets enclose an optional element (keyword or argument).
[x | y]	Square brackets enclosing keywords or arguments separated by avertical bar indicate an optional choice.
{x | y}	Braces enclosing keywords or arguments separated by a vertical barindicate a required choice.
[x {y | z}]	Nested set of square brackets or braces indicate optional or required choices within optional or required elements. Braces and a vertical barwithin square brackets indicate a required choice within an optional element.

variable	Indicates a variable for which you supply a value, in context where italicscannot be used.

Examples for the following conventions:

Convention	Description
screen font	Terminal sessions and information the switch displays are in screen font.
boldface screen font	Information you must enter is in boldface screen font.
italic screen font	Arguments for which you supply values are in italic screen font.
< >	Nonprinting characters, such as passwords, are in angle brackets.
[ ]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line ofcode indicates a comment line.

This document uses the following call-out conventions:

✎

NOTE   Notes contain helpful suggestions or references tomaterial not covered in the manual.

⚠

CAUTION   Be careful, in this situation you might do something that could result in equipment damage or loss of data.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation*.

To receive new and revised Cisco technical content directly to your desktop, you can subscribe to the *What's New in Cisco Product Documentation RSS feed*.

NOTE	RSS feeds are a free service.

Introduction to Cisco Smart License Utility

Cisco Smart License Utility Manager (CSLU) is a Windows-based application that enables customers to administer licenses and their associated Product Instances from their premises instead of having to directly connect their Smart Licensed enabled Product Instances to Cisco Smart Software Manager (CSSM) hosted on https://software.cisco.com/ (Smart Software Licensing).

NOTE	Throughout this document, the acronym CSSM (Cisco Smart Software Manager) is represented as Cisco (hosted on https://software.cisco.com/)

Software Packaging

Your installation package for CSLU consists of the following component:

- CSLU (Cisco Smart License Utility)

System Limits and Scalability

Product and user scalability:

- up to 10,000 Product Instances
- single tenant (a virtual account with a Smart Account)

System Requirements

See the following sections for more specific information on system requirements.

Cisco Smart Account Access

Make sure that you have access to a Cisco Smart Account, and have the role of either Smart Account Admin, or Virtual Account Admin, before you proceed with the tasks mentioned in this section.

Supported Operating Systems

The following operating systems are supported:

- Windows 10

- Linux

Localization

This release of CSLU supports the English language.

Hardware-based Requirements

CSLU can be deployed on a machine (laptop or desktop) running Window 10 OS or Linux.

These requirements are recommended for optimal performance on a machine running the Windows 10:

Minimum	Recommended
100 GB Hard Disk	200 GB Hard Disk
4 GB RAM	8 GB RAM
x86 Dual Core	x86 Quad Core
1 Ethernet NIC	1 Ethernet NIC

Installing CSLU

See the *CSLU Quick Start Guide* for installation instructions.

NOTE	Default installation path for Windows: *c:\Users\<username>\AppData\Roaming\CSLU*
	Default installation path for Linux: */opt/CSLU*

NOTE	As part of the installation process, the **CSLU.exe** file is installed on the desktop of your Windows host.
	After a Linux installation, you can find the CSLU icon in **Show Applications** of your machine.

Uninstalling CSLU

See the *CSLU Quick Start Guide* for uninstalling CSLU from your Windows host.

⚠️

CAUTION	When you uninstall CSLU in Windows, you are prompted whether to keep your CSLU data or not. If you choose No, all your data will be deleted permanently.
	In Linux, on uninstallation, the data gets directly deleted. You need to reinstall a version on top of the other to keep the data intact.

Configuring CSLU

After you have installed CSLU on your system, you will need to set the following parameters for proper functioning:

- Open the Preferences tab and configure a Smart Account and Virtual Account.

- Add Product Instances to CSLU (see Adding Product Instances in CSLU).

- If CSLU is not connected to Cisco, you can work locally and log in to Cisco when you need to be connected.

Once these three actions have been completed, you will be able to request authorization (see Requesting Bulk Authorization Codes) to receive license authorizations.

✎

NOTE	If you experience connectivity issues, see Appendix 3: Enabling HTTPS Server on Your Product Instance.

Configuring a Product Instance to Send Usage Reports (RUM)

To connect to a Product Instance, you need to configure that Product Instance (PI) to be able to connect with CSLU. Use one of the three options described here for discovering CSLU in order to send usage (RUM) reports.

Option 1: No action required: Zero-touch DNS discovery of cslu-local.

If you have configured the name server with an entry where the hostname cslu-local is mapped to the CSLU IP address (the windows host where you installed CSLU), no configuration is required. The product instance automatically discovers hostname cslu-local.

Option 2: Configure DNS discovery of your domain.

If you choose this option, you will need to use domain name command shown below. The name- server creates the entry cslu-local.example.com.

In the global configuration mode enter the IP domain-name command: *<domain_name>* shown in this example:

Device(config)#: ip domain-name example.com

Option 3: Configure a specific URL for CSLU

Use this command for configuring a specific URL. Follow this flow:

Enter the *license smart url cslu http://<host or IP>:<port-num>/cslu/v1/pi* command in global configuration mode, where:

- <host or IP> is the **hostname** or **IP address** of the windows host where you have installed CSLU

- <port-num> is **8182**

Here is an example:

Device (config)# license smart url cslu http://192.168.0.1:8182/cslu/v1/pi

Since the product instance initiates communication, it automatically starts by sending out the first RUM report. Along with this first report, if applicable and if required, it sends a trust code request and an authorization code request. CSLU forwards the information to Cisco and the returning acknowledgment (ACK) to the product instance, for installation. It gets the acknowledgment (ACK) from Cisco and sends this back to the product instance for installation.

When you have completed either of these options, you are now able to receive Usage (RUM) reports using CSLU.

Logging in and Opening CSLU

CSLU is a Windows-based application, therefore you only need to login to your local machine using your Windows system credentials (Windows username and password).

When you are successfully logged in to your Windows host, you can open CSLU by double-clicking on the CSLU icon located on the Windows host.

Home Screen

The CSLU home screen has five main menus (functionalities behind each of the menu options are described in their own sections):

CSLU Menu

This menu contains the following options:

- **Preferences**: this option opens the Preferences tab screen.

- **Reload**: this option closes and restarts the application.

- **Quit**: this option enables you to exit the application.

- **Import Cert**: this option enables to import a self-signed certificate file (with .crt extension) and a private key file (with .key extension). You must select two files in one go.

Self-signed certs can be used on network devices. It enables to import a self-signed certificate file (with .crt extension) and a private key file (with .key extension). Both files need to be in PEM format. Self-signed certificates can be generated by the user using the following commands:

- ■ openssl req -new -subj "/C=US/ST=Utah/CN=<name here>" -newkey rsa:2048 -nodes -keyout localhost.key -out localhost.csr
- ■ openssl x509 -req -days 365 -in localhost.csr -signkey localhost.key -out localhost.crt

For the device to communicate to CSLU through https, the device needs to have the CSLU URL inputted with https and port 8543 instead of http and port 8182.

NOTE	The device by default will not have any certificate installed so the user needs to import the default certificate or any self-signed certificate to communicate with CSLU through https.

Product Instances Menu

This menu affects all Product Instances (see Inventory Tab for more information) and is used to download and upload Product Instances from a file using the *.csv* format:

- • **Export CSV**: This option allows you to download all devices from the device list to a local file.

- • **Import CSV**: This option allows you to upload devices to the device list from a local file.

- • **Export Product Diagnostics:** This option allows you to download all the information regarding all the devices which are registered. This file is used to diagnose the faulty device information and will be helpful to troubleshoot.

- • **Export System Diagnostics:** This option allows you to download the system event log. This file is used to diagnose the system events and will be helpful to troubleshoot. This does not require any device/Product Instance to be selected.

NOTE	The default file format for Export Product Diagnostics and Export System Diagnostics is .diag.

See *Product instance menu option* for more information.

Data Menu

This menu is used to immediately send information to Cisco (when the CSLU application is connected to Cisco). The following options are available:

- **Send to CSSM**: when logged into Cisco, this option triggers API calls to immediately send RUM reports and DLC requests using API calls to Cisco from CSLU.

- **Export to CSSM**: creates a file with all the information needed to be sent to Cisco, for example: RUM reports, auth request, DLC requests in a compressed *.tar* file format.

- **Import from CSSM**: allows either downloaded responses from Cisco (such as RUM ACKS, auth codes, DCL ACK), or a single authorization code, or policy file downloaded from Cisco.

See *Data Menu Options* for more information.

Edit Menu

This menu provides basic Windows editing options so that you can perform basic editing functions with your device lists:

- **Cut**

- **Copy**

- **Paste**

Help Menu

This menu provides help resources as well as information on the current version of CSLU:

- **Download Help Manual**: selecting this menu option opens a modal that allows you to both select a directory on your system as well as customizing the name of the user guide. (It is recommended, however, that you keep the default name of the PDF file).

- **Download Log File**: selecting this menu option opens a modal that allows you select files to download into your working directory. The working directory is listed in the Preference Tab under the Working Directory field (<working directory>/var/logs).

NOTE   The working directory will be the repository for log files that you will need when contacting Cisco support.

The maximum size (logfile *maxsize*) for the log file is 10MB. When it exceeds 10MB, that file is automatically renamed, and a new file is created.

The maximum size limit for the directory is 100MB. If the size limit is exceeded, then files are deleted to keep within the size limit.

The maximum number of log files (logfile *maxbackups*) that can be stored is 10. Once the number of files is exceeded, then the oldest file is deleted to make room for the newest file.

- **About CSLU**: selecting this option opens the About Cisco Smart Licensing Utility window which provides the following information:
    - o Cisco Smart Licensing Utility copyright and trademark,
    - o installed modules,
    - o end user license agreement.

Inventory Tab

The Inventory tab allows you to manage your configured Product Instances through the **Product Instances** table.

You can select specific devices by using the selection box in the column located on the left side of the table.

You can also use the **Select All** check box, located to the left of the **Name** column:

- A minus sign (-) indicates that at least one device is selected, but not all devices are selected.
- If you click in the box, the box shows a check mark (√) which means that all devices are selected.

See the following sections for more information on the buttons and columns available in the Product Instances table.

Buttons

The following buttons are available in the Product Instances table:

- **Add Single Product**: this button opens a modal where you add the Host Name and Connect Method to add a Product Instance.
- **Actions for Selected**: this button has a dropdown menu with the following options:
    - o **Remove**: allows you to delete the selected Product Instance(s) from CSLU.

        This button has different variants, depending on the user's status: **Remove** when the user is logged in to Cisco; **Remove (Not Logged in to Cisco)** when the user is not logged in; **Remove (Cisco is not available)** when working in offline mode.
    - o **Edit**: allows you to edit one or more parameters for selected Product Instance(s).
    - o **Collect All Data**: allows you to trigger the collection of all possible data about the device along with the Usage Reports from selected Product Instances on any Product Instance(s) that are configured for one of the CSLU Initiated methods (see Collecting All Data for more information).

NOTE	The '**Collect Usage**' button is **deprecated** from the CSLU 2.0.0 version and it will not available on the UI. All its tasks/functions now would be performed through **'Collect All Data' button**.
	The 'Collect Usage' button is available in the CSLU 1.1.5 and its earlier versions and would not be available from the CSLU 2.0.0 and its further versions.

NOTE	For device older to version 17.8, Authorization Code Request should be done separately through the Authorization Code Request button.

- o **Authorization Code Request**: selecting this option downloads an authorization request file for the devices that have been selected (see Requesting Bulk Authorization Codes for more information).

NOTE	Buttons Authorization Code Request should only be used for pull devices prior to version 17.8.

- **Refresh Product Instance List**: this button allows you to refresh the Product Instances table and show any additions or modifications that have been made to the Product Instances table (for example: adding a new Product Instance). Also, all selection boxes are cleared.

Product Instances Table Columns

The following information is displayed in the Product Instances Table columns:

- **Name**: shows the Product Instances (in column format) registered to an account. Product Instances can be filtered (the filter field is not case sensitive) to Filter by Device Details.

- **Filter by Device Details**: Allows you to filter the devices by searching for any of the device details like Host id, Username, Connection Method, Host Name, Product Version and Role.

- **Last Contact**: the date that the Product Instance was last contacted.

- **Filter by Last Contact**: Allows you to filter the devices by searching for any of the date (for example: 10-May-2022).

- **Alerts**: provides the latest status of this Product Instance (for example: Failed to Connect).

- **Filter by Alerts**: Allows you to filter the devices by searching for any of the status (for example: Failed to Connect).

- **Items per page**: this field enables you to select the number of Product Instances that are listed on each page (available values: 5, 10, 25, and 100).

✎

NOTE	You can search for Product Instances by any Device Details, Last Contact, or Alert.
	Once a device is added, the Host/IP Address displays as a hyperlink to the device recordport field. You can edit the record from this screen.

Preferences Tab

The Preferences Tab contains two panels with parameters. See the following sections for more information on the parameters and their values.

Cisco Connectivity Panel

This panel contains the following fields:

- **Cisco Is Available**: a toggle switch for enabling ability to set the preferences associated with connectivity to Cisco. The default is that connectivity is enabled (blue color). Clicking on the toggle switch disables connectivity (gray color). Cisco connectivity allows you to automatically send daily reports to Cisco. After enabling CCSM is Available, you must login to Cisco each time you load the application to establish connectivity.

- **Proxy is On/Off**: (Default setting is disabled in gray color) a toggle switch for enabling proxy panel and to set the proxy settings.

- **Cisco Connection Timeout (seconds):** a numerical field where you enter the number of seconds that Cisco has not connected before the application times out. The default value is 10.

- **Cisco Response Timeout (seconds):** a numerical field where you enter the number of seconds before the system times out while waiting for a response from Cisco. The default value is 90.

- **Cisco Retry Interval (seconds)**: a numerical field where you can enter the number of seconds that must pass before the application attempts to re-connect to Cisco (after a Cisco Connection Timeout). The default value is 900.

- **Cisco URL (Read only)**: lists the URL (directory location) for Cisco the application uses. It is listed so you can ensure that this URL is available to your network because it is used for Cisco connectivity.\

✎

NOTE	The default URL is:
	https://swapi.cisco.com/services/api/smart-accounts-and-licensing/v2/

- **OAuth URL (Read only)**: lists the URL (directory location) of the Cisco authentication server used to login to your CCO account to allow the application to communicate with CSSM. It is shown so you can ensure Cisco is available to your network because it is used for Cisco connectivity.

NOTE   Default OAuth URL is:

https://cloudsso.cisco.com/as/token.oauth2

It is important to make sure the Cisco URL and OAuth URL fields are correct. Otherwise, the upload and download processes will not work properly.

- **RUM Upload Interval (days)**: a numerical field where you enter a number of days after which a report is requested from a device and uploaded to CSLU.

CSLU Connectivity Panel

This panel contains the following fields:

- **Product Instance Service Port**: (required field) the port the Product Instances use to communicate with the CSLU application.

NOTE   The default value is 8182.

- **REST API Port**: (required field) the port for the REST-API operations supported by the CSLU application if it uses *CSLU: Initiated REST-API* as the collection method.

NOTE   The default value is 8180.

- **Smart Account**: the name of the Smart Account (SA) on CSLU that receives RUM reports. The Smart Account name is case sensitive and must exactly match Cisco.
- **Virtual Account**: The Virtual Account (VA) paired with the Smart Account. The Virtual Account name is case sensitive and must exactly match Cisco.

- **Validate Device**: if you have chosen the **Product Instance Initiated Only** mode (in the Default Connect Method field, below), selecting the **Validate Device** check box will control the automatic creation of Product Instances when the usage report is received.

  When **Validate Device** is enabled and an unknown Product Instance sends a usage (RUM) report, the local database is examined to check whether the device is present. If yes, then the usage (RUM) report will be accepted. If no, the usage report will be rejected.

  If you want the CSLU to 'auto-discover' new Product Instances based on the receipt of usage (RUM) reports, then make sure that the **Validate Device** check box is not selected.

NOTE	For this release, after you have installed CSLU, you will need to configure CSLU from the Product Instance CLI so that devices can send usage (RUM) Reports.

- **CSLU Working Directory (Read only)**: the local directory where records are stored. This is the directory that is established when you install CSLU.

NOTE	The default directory is:
	C:\Users\<user>\AppData\Roaming\CSLU

- **Default Connection Method**: provides different methods for connecting to a Product Instance. Your selection here will be used to pre-populate the Connect Method field when adding Product Instances.

  o **Product Instance Initiated Only**: the default setting; this mode enables CSLU to receive information from a Product Instance (see Configuring a Product Instance to Send Usage Reports for more information).

  o **CSLU Initiated – NETCONF**: enables CSLU to send Product Instance information using Remote Procedure Calls (RPC) to Cisco if CSLU is connected to Cisco.

  o **CSLU Initiated – RESTCONF**: enables CSLU to send Product Instance information using HTTP protocol to Cisco if CSLU is connected to Cisco

  o **CSLU Initiated – REST API**: enables CSLU to send Product Instance information using HTTP protocol to Cisco if CSLU is connected to Cisco.

NOTE	A connection method can be independently changed from the **Add Product Instance** or **Modify Product Instance** screens without affecting the selection in the Preferences tab. See Appendix 2: CSLU Initiated Connection Method for information on CSLU Initiated protocols.

Proxy Panel

This panel contains the following fields:

- **Proxy URL**: This field is obligatory if you want to use a proxy between CSLU and Cisco. If a proxy is used, then set the (URL) for the proxy host here.

- **Proxy Username**: Set a valid username to authenticate access to the proxy server.

- **Proxy password**: Set a valid password for the username to authenticate access to the proxy server.

- **Test Connection**: After setting all the proxy field, click **Test Connection** button to check the whether the proxy connection connects to Cisco or not.

- **Save**: saves all the settings to your system.

- **Reset**: resets all the settings to the last save.

Scheduler Tab

The Scheduler tab allows the user to schedule and edit the jobs through the **Scheduler** table.

There are two sections in the Scheduler Tab:

- **SYSTEM JOBS**:

  This section has the jobs for 'Poll CSSM for Available Data' and 'Clean Up Purged Data'. If the jobs are not scheduled, then they will automatically run at their 'Next Execution Time'. The name field is clickable, and the user can see all the detailed information for the jobs. These are the 'READ-ONLY' Jobs. The user cannot edit any information for these jobs.

NOTE	'Start' button is available only for 'Clean Up Purged Data' job in the System jobs.

- **OPERATIONAL JOBS**:

  This section has the job for 'Pull Device Data'. The user can explicitly start the job by clicking on the 'Start' button.
  If the job is not scheduled, then it will automatically run at their 'Next Execution Time'. On the 'Edit Job Screen' after clicking on the job name, 'Enabled', 'Recurring' and 'Run Interval' are the fields editable for the user. User can modify and save these details. User can schedule this job according to their requirement.
  The 'Run Interval' field has the minimum input limit of 1 day and maximum input limit of 90 days.

The 'start' button is also available on UI, for the user to start the job at any time.

NOTE	On the update of the 'Run Interval' field, then the 'Next Execution Time' according to that change will reflect on the UI, either on manual click on 'start' button or once the job runs automatically on its stated 'Next Execution Time'.

User can see the job information's listed in the Scheduler table and can schedule as per their needs and wants.

See the following sections for more information on the button and columns available in the Scheduler table.

Button

- **Refresh Job Information**: This button allows you to refresh the Scheduler table and shows any modifications that have been made to the Scheduler table (for example: if any changes in next execution time is not displayed correctly, refresh button help to show right one).

Scheduler Table Columns

- **Name**: Shows the job title/name. As default there are four jobs (for more information see type of job table).

  By Clicking on the Job name user can edit job details by Edit Job Details Screen (for more information see Edit Job Details).

- **Status**: Shows the status of job whether the job is Running or in Scheduled mode.

- **Next Execution Time**: Will show the next date and time when the job has to be executed.

- **Start**: Allows the user to run the job manually before the next execution time arrives itself.

NOTE	Version 2.2.0 displays a message 'No poll in queue' only for 'Poll CSSM for Available Data' job. The message will display when there is no poll id to be serviced.
	Initially when CSLU is freshly installed, there would be no poll ids for the job, therefore displaying the message 'No poll in queue'.
	CSLU sends 'Usage Reports' and 'Sync Messages' to CSSM through which we get a poll id from CSSM, due to which the message 'No poll in queue' gets removed from UI.
	If there are no poll ids left to be serviced, the message 'No poll in queue' shows up again.

Type of Job Table

Job Name	Type of Job	Description
Pull Device Data	Operational Job	Pulls data from devices which support pull mode to send to CSSM. The units for Run Interval time are calculated in days.
Poll CSSM for Available Data	System Job	Sends to CSSM any device data that CSLU has on hand. The units for Run Interval time are calculated in minutes.
Clean Up Purged Data	System Jobs	Removes old data that is stored in the system purge folders. The units for Run Interval time are calculated in days.

Edit Job Details

To edit job details, click the job name then the **Edit Job Details** screen opens. Edit Job Details screen has two panels they are Job Details and Job Timings. The Edit/Save option is available only for the Operational Jobs.

Job Details panel has following fields

- **Job Name**: Shows the job title/name (for more information see type of job table).
- **Enabled:** The dropdown to select True or False. True means the job is set to On and False means the job is set to Off. (Editable only for Operational Jobs).
- **Recurring:** the dropdown allows user to select True or False. True means will allow the job to repeat the run function after the defined run interval time and False means set Off the repeat run function. (Editable only for Operational Jobs).
- **Current Status**: Shows the status of job whether the job is in Running or Scheduled mode.

✎

NOTE   Only Enabled, Recurring are the fields editable in Operational Jobs only.

Job Timings panel has following fields

- **Job First Scheduled**: Shows when the job was scheduled at very first time.
- **Next Run Time:** Shows the next date and time when the jobs will be executed.

- **Last Run Time**: Shows the date and time when the jobs had been executed recently.

- **Duration of Last Run**: Shows the time it took for the last run of the job to complete.

- **Run Interval**: Allows user to set the time interval at which the job will be run.

NOTE	The units of Run Interval time will vary for each job.

NOTE	Only Enabled, Recurring, Run Interval fields are editable for user in Operational Jobs only.

Product Instances Menu Options

This menu affects all Product Instances and is used to download and upload Product Instances from a file using the *.csv* and .diag formats. See the following sections for more information on available options.

Export CSV

This option allows you to globally download a full Product Instance list as a *.csv* file. The *.csv* file can then be used for obtaining reports for managing Product Instances.

Complete these steps to download a list of all Product Instances and their associated information:

Step	Action
Step 1	From the CSLU main screen, select **Product Instances > Export CSV**.
Step 2	A download modal opens for you to: • Browse for a folder where the *.csv* file will reside and input the file name that will have the *.csv* extension.
Step 3	Click **Save**. The product usage (*.csv*) files are downloaded for the selected Product Instances.

NOTE	The Windows operating system can change the behavior of a usage report file properties by dropping the extension when that file is renamed. The behavior change happens when you rename the downloaded file, and the renamed file drops the extension.
	For example, the downloaded default file named *DeviceList.csv* is renamed to *MyDeviceList*. The file loses its *.csv* extension. To enable the DeviceList file to function normally, after renaming a usage report file, you must also add the *.csv* extension back to the file name before saving,

NOTE	Error message '**Select the Product Instance to perform the operation**" will be displayed when Exporting CSV without selecting a Device.
	Export CSV will export only the product instance which are been selected by user.
	Export CSV file will have addition of new columns like Hostname, Product Version and Role.

Import CSV

This option allows you to globally upload to CSLU using the Upload Product Instance List feature. The information is uploaded in the *.csv* format.

Complete these steps to upload a list of all Product Instances and their associated information.

Step	Action
Step 1	From the CSLU main screen, select **Product Instance > Import CSV** .
Step 2	An Upload Product Instances modal opens for you to either: • drag & drop a **Product Instance List file** that resides on your local drive, or: • browse for a file, select the appropriate *.csv* file and click **Upload**. **NOTE**: There is a *.csv* template you can use. Click **Download** to download the file to your local drive. Then you can use this template to format your *.csv* files. You can only upload one device list at a time.
Step 3	The files are uploaded to CSLU, and any new Product Instances are added to the device list with the information provided. See Appendix 1: Product Instance Field Definitions for .csv Files for the meaning of each field. **NOTE**: The Smart Account and Virtual account are globally set in the Preference tab, so the SA/VA values entered in the *.csv* are ignored.

NOTE	Export CSV file will have addition of new columns like Hostname, Product Version and Role.

Export Product Diagnostics

This option allows you to globally download a Product Instance details as a *.diag* file.

Complete these steps to download a Product Instance details and their associated information:

Step	Action
Step 1	From the CSLU main screen, select **Product Instances > Export Product Diagnostics**.
Step 2	The file gets automatically downloaded to a system specific path mentioned on the pop up which appears on the click of 'Export Product Diagnostics'. After clicking 'Okay', the user will get the option to save the file to some desired location as well. After clicking 'Okay': A download modal opens for you to: • Browse for a folder where the *.diag* file will reside and input the file name that will have the *.diag* extension.
Step 3	Click **Save**. The Export product Diagnostics (*.diag*) files are downloaded for the selected Product Instances.

NOTE	Error message '**Select the Product Instance to perform the operation**" will be displayed when Exporting Product Diagnostics without selecting a Device.

Export System Diagnostics

This option allows you to globally download the system information's as a *.diag* file.

Complete these steps to download a Product Instance details and the system information's:

Step	Action
Step 1	From the CSLU main screen, select **Product Instances > Export System Diagnostics**.

Step 2	The file gets automatically downloaded to a system specific path mentioned on the pop up which appears on the click of 'Export System Diagnostics'. After clicking 'Okay', the user will get the option to save the file to some desired location as well. After clicking 'Okay': A download modal opens for you to: • Browse for a folder where the *.diag* file will reside and input the file name that will have the *.diag* extension.
Step 3	Click **Save**. The Export System Diagnostics (*.diag*) files are downloaded.

NOTE   You do not need to select any Product Instance for performing this operation.

Data Menu Options

This menu is used to immediately send information to Cisco (when the CSLU application is connected to Cisco). See the following sections for more information on available options.

Send to CSSM

This option is used after you have collected a RUM report from the Product Instances.

When logged in to Cisco, this menu option triggers API calls to immediately send RUM reports and DLC requests (via API REST calls to Cisco from CSLU).

NOTE   To successfully send reports to Cisco, you will need to have selected a Smart Account (SA) and Virtual Account (VA) in CSLU and be logged in to Cisco (see Preferences Tab for details).

By default, these reports are automatically sent on a scheduled basis.

NOTE   Error message '**Select the Product Instance to perform the operation**" will be displayed when you click Send to CSSM without selecting a Device.

Send to CSSM will send only RUM reports of the product instance which are been selected by user.

Export to CSSM

This option can be used as a part of a manual download procedure when you want the workstation isolated for security purposes, for example.

Complete the following steps:

Step	Action
Step 1	To work offline - from the **Preferences Tab** screen, set the **Cisco Connectivity** toggle switch to **Cisco Is Not Available**.
Step 2	Navigate to **Product Instances > Export to CSSM**.
Step 3	Select the file from the modal that opens and click **Save**. The file is now saved. **NOTE**: At this point you have a DLC file, RUM file, or both.
Step 4	Go to a station that has connectivity to Cisco, and complete the following: a.　Navigate to **software.cisco.com** b.　Select the **Smart Account** (upper left-hand corner of the screen) that will receive the report. c.　Next, select **Licensing > Smart Software Licensing > Reports > Usage Data Files**. d.　Click **Upload Usage Data**. (RUM report in tar format.) e.　Browse for and select the **file** to be uploaded, and then click **Upload Data**. f.　From the Select Virtual Accounts pop-up, select the **Virtual Account** that will receive the uploaded file. The file is uploaded to Cisco and is listed in the Usage Data Files table in the Reports screen showing the File Name, time it was Reported, which Virtual Account it was uploaded to, the Reporting Status, Number of Product Instances reported, and the Acknowledgement status. g.　In the Acknowledgement column, click **Download**. The acknowledgement file is downloaded to your third-party device.
Step 6	Once the file is downloaded, you can transfer to **CSLU**.

Step 7	Click **Import From CSSM** (see Import from CSSM for details).

NOTE	Error message '**No data pending for exporting data to offline file**" will be displayed when you click Export to CSSM without selecting a Device.

Import from CSSM

Once you have received the acknowledgment file (ACK) or another file, such as smart licensing authorization code, from Cisco, you are ready to upload that file to your system. This procedure can be used for workstations that are offline.

Complete these steps to select and upload a file(s) from Cisco:

Step	Action
Step 1	Make sure you have downloaded the **ACK file** for the device (see Export to CSSM for details).
Step 2	From the CSLU main screen, select **Product Instance > Import from CSSM**.
Step 3	A Cisco File Upload modal opens for you to either: • drag and drop a file that resides on your local drive, or: • browse for the appropriate *.xml* file, select the file and click **Open**.
Step 4	After a successful upload, you will get a message indicating that the ACK file was successfully sent to the server. If the upload was not successful, you will get an import error. When you have finished uploading, click the **x** at the top right corner of the modal to close it.

Working with CSLU

See the following sections for more details on the most typical working scenarios available in the CSLU application.

Adding Product Instances in CSLU

Using the CSLU interface, there are three ways you can add Product Instances to your system.

- **CSLU Created**: In the Inventory tab, click **Add Single Product**.

- **Upload to CSLU**: Select **Product Instances** in the Home Screen and click **Import CSV** to import a file.

- **Product Created**: CSLU will extract Product Instance related information from the RUM (usage) report sent by the Product Instance and then create corresponding Product Instances. You can configure this by selecting **Preferences Tab > Default Connect Method > Product Instance Initiated Only** and deselecting the **Validate Device** check box. The Product Instances are then added when each Product Instance sends its first usage (RUM) report.

Adding a Single Product-Initiated Product Instance

To know what each field means see Appendix 1: Product Instance Field Definitions for .csv Files or hover over each field entry for the tool tip to show the meaning of field.

Complete these steps to add a single Product Instance from the Inventory tab:

Step	Action
Step 1	From the CSLU main screen, in the **Inventory** tab, select **Add Single Product**.
Step 2	(Required) Enter the **Host** (IP Address of the Host).
Step 3	(Required) Select **Product Instance Initiated Only** as the Connect Method.
Step 4	Click **Save**. The information is saved to the system and the device is listed in the Product Instances.

✎

NOTE   To add individual product-initiated Product Instances, CSLU must be configured for collecting usage reports (see Collecting Usage Reports – CSLU Initiated for details).

Adding a CSLU-Initiated Product Instance

Using the CSLU interface, you can configure the connect method to be CSLU Initiated. This connection method (mode) enables CSLU to request information from devices. If CSLU is connected to Cisco, it will forward to Cisco information received from Product Instances, whether requested by CSLU or pushed by Product Instances.

To know what each field means see Appendix 1: Product Instance Field Definitions for .csv Files or hover over each field entry for the tool tip to show the meaning of field.

Complete these steps to add a Product Instance from the **Inventory** tab:

Step	Action
Step 1	In the **Inventory** tab, select the **Add Single Product** option.
Step 2	Enter the **Host** (IP Address of the Host).
Step 3	Select the **Connect Method** and select an appropriate **CSLU Initiated** connect method.
Step 4	In the right panel, click **Product Instance Login Credentials**. The left panel of the screen changes to show the **User Name** and **Password** fields. **NOTE**: If you click **General**, the detailed **Add Product** modal opens (see Appendix 1: Product Instance Field Definitions for .csv Files for details).
Step 5	Enter the Product Instance **User Name** and **Password**.
Step 6	Click **Save**. The information is saved to the system and the device is listed in the Product Instances with the Last Contact listed as **never**. You can now collect all data reports (see Collecting Usage Reports – CSLU Initiated for details).

Adding a Product-Initiated Product Instance

Complete these steps to add a device-created Product Instance:

Step	Action
Step 1	Select the **Preferences tab**.
Step 2	In the Preferences screen, de-select the **Validate Instance** check box.
Step 3	Set the **Default Connection Method** to **Product Instance Initiated only** and then click **Save**.

Modifying a Product Instance

CSLU allows you to edit one or multiple Product Instance(s) in your system.

Complete these steps to edit Product Instances:

Step	Action
Step 1	Select **one** or **more Product Instances**. **NOTE**: If you select multiple devices, you can only modify the **User Name**, **Password**, and **Connection Method**. The Host, and all UDI fields can only be modified one Product Instance at a time.
Step 2	From the CSLU main screen, select **Actions for Selected > Edit**.
Step 3	(Required) Modify the appropriate fields (see Step 1).
Step 4	Click **Save**. The modifications are listed in the Product Instances.

NOTE You can also modify a single device by clicking on the **Product Instance Name** in the Product Instances table.

New read-only fields like Hostname, Role and Product Version are added in the Product Instances table, for the devices that are configured for them, i.e., device versions 17.9.1 onwards.

Removing a Product Instance

In CSLU, you can remove one or multiple Product Instance(s) from your system.

Complete these steps:

Step	Action
Step 1	From the Inventory tab, select one or more devices.
Step 2	From the CSLU Main screen, select **Actions for Selected > Remove.** **NOTE**: If the device is removed or upgraded, the data associated with the device (reports, for example) will not be removed.

NOTE If you are not logged in to Cisco/CSSM, or 'Cisco is Not Available' button is OFF(greyed out), on the Preferences Tab, then the Product Instances are only removed from the UI, not from CSSM . The information message is displayed on the UI itself. The 'Remove' button in these cases are also renamed as 'Remove(Cisco is not Available)', or the 'Remove(Not Logged in to Cisco)'.

Collecting Usage Reports – CSLU Initiated

CSLU also allows you to manually trigger the gathering of usage reports from devices.

✎

NOTE	By default, the CSLU application is scheduled to collect usage information at 24 hours intervals.

After configuring and selecting a Product Instance (selecting **Add Single Product**, filling in the **Host** name and selecting a **CSLU Initiated** connection method), proceed to **Actions for Selected > Collect All Data**. CSLU connects to the selected Product Instance(s) and collects the usage reports.

These usage reports are then stored in CSLU's local library. These reports can then be transferred to Cisco if CSLU is connected to Cisco, or (if you are not connected to Cisco) you can manually trigger usage collection by selecting **Product Instances > Export to CSSM**.

Complete these steps to collect Product Instance usage reports:

Step	Action
Step 1	Select the **Preference tab** and enter a valid **Smart Account** and **Virtual** Account, and then select an appropriate **CSLU** Initiated collect method (if there have been any changes in Preferences, make sure you click **Save**).
Step 2	Open the Inventory tab and select one or more Product Instances.
Step 3	From the CSLU main screen, select **Actions for Selected > Collect All Data**. RUM reports are retrieved from each selected device and stored in the CSLU local library. The Last Contacted column is updated to show the time the report was received, and the Alerts column shows the status. **NOTE**: If CSLU is currently logged into Cisco the reports will be automatically sent to the associated Smart Account and Virtual Account in Cisco and Cisco will send an acknowledgement to CSLU as well as to the Product Instance. The acknowledgement will be listed in the Alerts column of the Product Instance table. **NOTE**: To manually transfer Usage Reports to Cisco, select **Export to CSSM** from the **Data** menu.

Step 4	From the Download for Cisco modal, select the **local directory** where the reports are to be stored. (*<CSLU_WORKING_Directory>/data/default/rum/unsent*)
	At this point, the usage reports are saved in your local directory (library). To upload these usage reports to Cisco, follow the steps described in Uploading Usage Reports to Cisco.

NOTE The Windows operating system can change the behavior of a usage report file properties by dropping the extension when that file is renamed.

The behavior change happens when you rename the downloaded file, and the renamed file drops the extension. For example, the downloaded default file named *UD_xxx.dat* is renamed to *UD_yyy*. The file loses its *.dat* extension and cannot function.

To allow the usage file to function normally, after renaming a usage report file, you must also add the *.dat* extension back to the file name, for example *UD_yyy.dat*.

NOTE The '**Collect Usage**' button is **deprecated** from the CSLU 2.0.0 version and it will not available on the UI. All its tasks/functions now would be performed through **'Collect All Data' button**.

The 'Collect Usage' button is available in the CSLU 1.1.5 and its earlier versions and would not be available from the CSLU 2.0.0 and its further versions.

After configuring and selecting a Product Instance (selecting **Add Single Product**, filling in the **Host** name and selecting a **CSLU Initiated** connection method), proceed to **Actions for Selected > Collect All Data**. CSLU connects

Collecting All Data

CSLU also allows you to manually trigger the gathering of all data from devices.

This button is used in place of 'Collect Usage' button from CSLU 2.0.0 and further.

NOTE By default, the CSLU application is scheduled to collect data information at 24 hours intervals.

After configuring and selecting a Product Instance (selecting **Add Single Product**, filling in the **Host** name and selecting a **CSLU Initiated** connection method), proceed to **Actions for Selected > Collect All Data**. CSLU connects to the selected Product Instance(s) and collects all the possible data along with usage details.
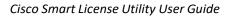
These data are then stored in CSLU's local library. These reports can then be transferred to Cisco if CSLU is connected to Cisco, or (if you are not connected to Cisco) you can manually trigger usage collection by selecting **Product Instances > Export to CSSM**.

Complete these steps to collect Product Instance usage reports:

Step	Action
Step 1	Select the **Preference tab** and enter a valid **Smart Account** and **Virtual** Account, and then select an appropriate **CSLU** Initiated collect method (if there have been any changes in Preferences, make sure you click **Save**).
Step 2	Open the Inventory tab and select one or more Product Instances.
Step 3	From the CSLU main screen, select **Actions for Selected > Collect All Data**. All possible data about the device and RUM reports are retrieved from each selected device and stored in the CSLU local library. The Last Contacted column is updated to show the time the report was received, and the Alerts column shows the status. **NOTE**: If CSLU is currently logged into Cisco the reports will be automatically sent to the associated Smart Account and Virtual Account in Cisco and Cisco will send an acknowledgement to CSLU as well as to the Product Instance. The acknowledgement will be listed in the Alerts column of the Product Instance table. **NOTE**: To manually transfer Usage Reports to Cisco, select **Export to CSSM** from the **Data** menu.
Step 4	From the Download for Cisco modal, select the **local directory** where the reports are to be stored. (*<CSLU_WORKING_Directory>/data/default*) At this point, the usage reports are saved in your local directory (library). To upload these usage reports to Cisco, follow the steps described in Uploading Usage Reports to Cisco.

NOTE	The Windows operating system can change the behavior of a data report file properties by dropping the extension when that file is renamed.
	The behavior change happens when you rename the downloaded file, and the renamed file drops the extension. For example, the downloaded default file named *UD_xxx.dat* is renamed to *UD_yyy*. The file loses its *.dat* extension and cannot function.
	To allow the data report file to function normally, after renaming a usage report file, you must also add the *.dat* extension back to the file name, for example *UD_yyy.dat*.

Uploading Usage Reports to Cisco

If you are logged into Cisco, you can upload Product Instance usage (RUM) reports to a SA/VA.

NOTE	By default, the CSLU is scheduled to upload usage information at 5-minute intervals.
	Before uploading Product Instance usage reports, make sure you have configured CSLU witha valid SA/VA.

Step	Action
Step 1	If you have not already done so, login to **Cisco**.
Step 2	Navigate to: **software.cisco.com** and select the **Smart Account**.
Step 3	From the main page, select **Smart Software Licensing > Reports >Usage Data Files > Upload Usage Data.**
Step 4	Next, at the Upload Usage Data modal, click **Browse**. Navigate to the local directory where the files have been saved and select the file(s) to upload.
Step 5	Click **Upload Data**. The Select Virtual Accounts modal opens.
Step 6	Select the **Virtual Account** that will receive the upload. Once the VA is selected a "This usage data is being processed" prompt opens. Showing that the VA selected is viable and that the report data is being processed. **NOTE**: Depending on the number of reports selected, the processing time could take a while. In the Usage Reporting screen, the reporting status for the selected VA is labeled as **Data Being Processed,** and the Acknowledgement column shows the **Pending** status.

Step 7	When the processing is complete, the VA record Reporting Status any errors that occurred during the upload. The Acknowledgement column shows **Available** (the file shows up in the download queue). Right-click on file in queue and selects **Always open files of this type**.
Step 8	Right-click the file in the **Acknowledgement** column to download the file.
Step 9	Once you have the Acknowledgement file (ACK), then in CSLU select **Product Instance > Send to CSSM**. When the modal opens, you can either browse for the file or drag and drop the file RUM (*.tar*) file. The upload to Cisco is now complete.

Requesting Bulk Authorization Codes

The **Authorization Code Request** menu option is specifically used to manually request authorization codes from Cisco. This option is specifically used for one or more Product Instances.

Complete these steps if you are not connected to Cisco to request authorization codes from Cisco:

Step	Action
Step 1	From the **Product Instance** table, select the **Product Instances** for authorization code request.
Step 2	After selecting one or more Product Instance(s), select **Actions for Selected** > **Authorization Code Request**.
Step 3	A modal pops up, providing additional authorization request information. Click **Accept**. Another modal opens to select a local *.csv* file for uploading.
Step 4	Do the following: a. Upload the file to Cisco by following this directory path: **software.cisco.com > Smart Software Licensing > Inventory > Product Instances > Authorize License Enforced Features**. b. Follow the steps shown in the wizard to select licenses and then download the authorization codes to CSLU.

Step 5	You can now apply the authorization codes by selecting **Product Instances > Import from CSSM** (see Import from CSSM for details).
	• If CSLU is In Product-Initiated mode: the uploaded codes are now applied to the Product Instances the next time the Product Instance contacts CSLU.
	• If CSLU is in a CSLU initiated mode: the uploaded codes are now applied to the Product Instances the next time the CSLU runs an update.

Appendix 1: Product Instance Field Definitions for .csv Files

This table provides the full list of field descriptions for a Product Instance. These fields are listed in the *.csv* files:

Field Name	Description
Name	For a Future Use Requirement: A place holder in case a port number is required to connect to Product Instances in the future.
IP Address	(**Required**) IP address of the Product Instance.
Smart Account	The Smart Account name in Cisco.
Virtual Account	The Virtual Account name in Cisco.
UDI	Universal Device Identifier.
PID	Product ID. **NOTE**: If PID is entered, you must also enter the SN.
Serial Number	Serial Number of the Product Instance. **NOTE**: If SN is entered, you must also enter the PID.
VID	The version of the customer orderable product (PID) so that the customer can see any version improvements that have occurred with the product. **NOTE**: If VID is entered, you must also enter the PID and SN.
UDI Host ID	The Product Instance IP Address.
MAC Address	The physical address of the Product Instance.
SUVI	Secure Unique Version Identifier (This is a trusted unique identifier.)

UUID	Universally Unique Identifier is a value that describes the Product Instance for a certain product family.
User Name	A user name to allow CSLU to login to device and collect information such as, RUM reports, DLC information, and can install Policy and Authorization codes. **NOTE**: Only CSLU Initiated Connect methods need this.
Password	A password to allow CSLU to login to device and collect RUM reports. **NOTE**: Only CSLU-Initiated Connect Methods need this.
Connection Method	**Product Instance Initiated only**: This mode is used for CSLU when it is in "Standalone" mode (not connected to Cisco). It enables CSLU to receive information from a Product Instance. CSLU also has three CSLU initiated modes. These modes provide two-way communication between CSLU and Cisco. See Appendix 2: CSLU Initiated Connection Method for information on these protocols. • **CSLU Initiated**: NETCONF enables CSLU to send Product Instance information using Remote Procedure Calls (RPC) to Cisco if CSLU is connected to Cisco. • **CSLU Initiated**: RESTCONF enables CSLU to send Product Instance information using HTTP protocol to Cisco if CSLU is connected to Cisco. • **CSLU Initiated**: REST API enables CSLU to send Product Instance information using HTTP protocol to Cisco if CSLU is connected to Cisco.
Hostname	The host name of registered product instance, for the devices that are configured for them, i.e., device versions 17.9.1 onwards. It is a read-only field. Use cannot edit it.
Product Version	Displays the current version of the Product, for the devices that are configured for them, i.e., device versions 17.9.1 onwards. It is a read-only field. Use cannot edit it.
Role	Displays the status of the product, whether it is in active mode or inactive mode, for the devices that are configured for them, i.e., device versions 17.9.1 onwards. It is a read-only field. Use cannot edit it.

Appendix 2: CSLU Initiated Connection Method

The table below provides the protocol, reference documentation, and transport information for each of the CSLU-initiated connection methods used:

Network Management Protocol	Reference	Additional information

NETCONF	rfc6241	For a future use requirement: a placeholder in case a port number is required to connect to Product Instances in the future.
RESTCONF	rfc8040	(**Required**) IP address of the Product Instance.
Native REST	Cisco Proprietary	The Smart Account name in Cisco.

Appendix 3: Enabling HTTPS Server on Your Product Instance

If you experience connectivity issues when trying to receive usage reports from a Product Instance, follow these steps:

1. Configure interface and IP route.

2. This is an example of the steps used to enable the HTTP server using an authentication method:

```
ip http server
ip http authentication local
ip http secure-server
!

aaa new-model
aaa authentication login default local
aaa authorization exec default local
username admin privilege 15 password 0 lab
```

3. Verify that the SL-HTTP server is now enabled by following these steps:

```
Switch#show ip http server session-module

HTTP server application session modules:
Session module Name Handle Status Secure-status Description
OPENRESTY_PKI 3 Active IOS OpenResty PKI Server
SL_HTTP 2 Active Active HTTP REST IOS-XE Smart License Server
HTTP_IFS 1 Active Active HTTP based IOS File Server
NBAR2 4 Active Active NBAR2 HTTP(S) Server
HOME_PAGE 5 Active Active IOS Homepage Server
BANNER_PAGE 6 Active Active HTTP Banner Page Server
WEB_EXEC 7 Active Active HTTP based IOS EXEC Server
GSI7F7B53506098-lic 8 Active Active license agent app
GSI7F7B59697718-web 9 Active Active wsma infra
GSI7F7B59699CA0-web 10 Active Active wsma infra
NG_WEBUI 11 Active Active Web GUI

Switch#
```

4. Ping the IP configured from your CSLU_W host.

Appendix 4: Default Data Transfer Intervals

By default, CSLU is scheduled to transfer usage data with Cisco or Product Instance(s) at specific intervals. Listed here are the usage data intervals:

- Retrieve Usage Data from Product Instances: 90-day intervals

- Importing Usage Data to Product Instances: 5-minute intervals

Appendix 5: CSLU Firewall Settings

When the CSLU application is run for the first time, Windows 10 prompts you to confirm your firewall settings. Please refer to the table below for appropriate firewall settings:

CSLU - Connection Mode	CSLU -API Firewall (Backend Server)	CSLU Firewall (UI Client)	Additional information
CSLU-Initiated: REST API RESTCONF NETCONF	Select **Cancel**	Select **Cancel**	In the CSLU-initiated mode, the CSLU will never receive requestsfrom external hosts, therefore, the CSLU firewall ports can be blocked.
Product Instance Initiated Only	Select **Allow Access**	Select **Cancel**	In this mode, the CSLU will receive reports and request from the Product Instances, and therefore the CSLU-API firewall needs to be in the **Allow Access** state **NOTE**: The CSLU firewall is for the UI and the UI does not receive requests from an external host.
Both CSLU-Initiated and Product Instance Initiated	Select **Allow Access**	Select **Cancel**	See: Product Instance initiated note in the Product Instance Initiated Only Mode.