Cisco Nexus 9000 and 3000 Series NX-OS Smart Licensing Using Policy User Guide

First Published: 2021-08-24

Last Modified: 2024-03-29

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS REFERENCED IN THIS DOCUMENTATION ARE SUBJECT TO CHANGE WITHOUT NOTICE. EXCEPT AS MAY OTHERWISE BE AGREED BY CISCO IN WRITING, ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS DOCUMENTATION ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED.

The Cisco End User License Agreement and any supplemental license terms govern your use of any Cisco software, including this product documentation, and are located at: http://www.cisco.com/go/softwareterms.Cisco product warranty information is available at http://www.cisco.com/go/warranty. US Federal Communications Commission Notices are found here http://www.cisco.com/c/en/us/products/us-fcc-notice.html.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any products and features described herein as in development or available at a future date remain in varying stages of development and will be offered on a when-and if-available basis. Any such product or feature roadmaps are subject to change at the sole discretion of Cisco and Cisco will have no liability for delay in the delivery or failure to deliver any products or feature roadmap items that may be set forth in this document.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

The documentation set for this product strives to use bias-free language. For the purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on RFP documentation, or language that is used by a referenced third-party product.

CONTENTS

PREFACE

CHAPTER 1

CHAPTER 2

CHAPTER 3

CHAPTER 4

Preface

This preface includes the following sections:

Audience

This publication is for network administrators who install, configure, and maintain Cisco Nexus switches.

Document Conventions

Command descriptions use the following conventions:

Convention	Description
bold	Bold text indicates the commands and keywords that you enter literally as shown.
Italic	Italic text indicates arguments for which you supply the values.
[x]	Square brackets enclose an optional element (keyword or argument).
[x | y]	Square brackets enclosing keywords or arguments that are separated by a vertical bar indicate an optional choice.
{x | y}	Braces enclosing keywords or arguments that are separated by a vertical bar indicate 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 bar within square brackets indicate a required choice within an optional element.

Convention	Description
`variable`	Indicates a variable for which you supply values, in context where italics cannot be used.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string includes the quotation marks.

Examples use the following conventions:

Convention	Description
`screen font`	Terminal sessions and information the switch displays are in screen font.
`boldface screen font`	Information that 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 of code indicates a comment line.

Related Documentation for Cisco Nexus 9000 Series Switches

The entire Cisco Nexus 9000 Series switch documentation set is available at the following URL:

http://www.cisco.com/en/US/products/ps13386/tsd_products_support_series_home.html

Documentation Feedback

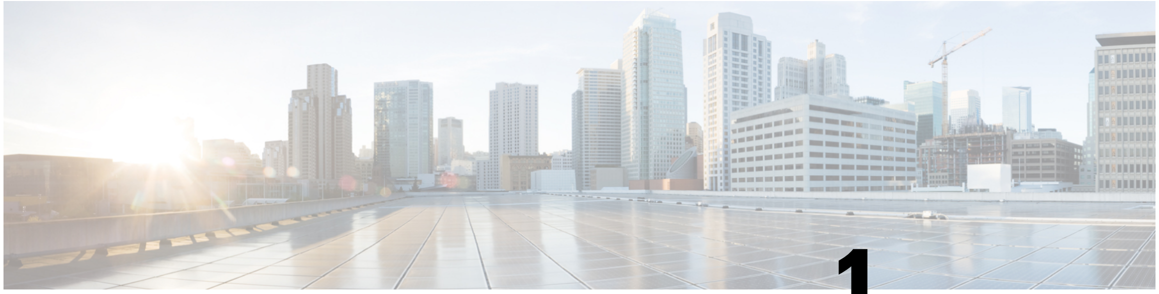
To provide technical feedback on this document, or to report an error or omission, please send your comments to nexus9k-docfeedback@cisco.com. We appreciate your feedback.

Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco Marketplace.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a web-based tool that acts as a gateway to the Cisco bug tracking system that maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. BST provides you with detailed defect information about your products and software.



CHAPTER 1

New and Changed Information

This chapter provides release-specific information for each new and changed feature in the Cisco Nexus 9000 and 3000 Series NX-OS Smart Licensing Using Policy User Guide.

New and Changed Information

Smart Licensing Using Policy is introduced in Cisco NX-OS Release 10.2(1)F for Cisco Nexus 3000 and 9000 series switches.

The following table lists the changes to this document since the smart licensing using policy is introduced.

Date	Description
March 2024	Updated the following section and published for Cisco NX-OS Release 10.4(3)F: • Supported Products, on page 13 • Guidelines and Limitations, on page 7 • Troubleshooting Smart Licensing Using Policy, on page 67 • Resolving SLP Issues on Nexus Switches, on page 67 • Additional References for Smart Licensing Using Policy, on page 85 • Feature History for Smart Licensing Using Policy, on page 87
December 2023	Updated the following sections and published for Cisco NX-OS Release 10.4(2)F: • Supported Products, on page 13 • Feature History for Smart Licensing Using Policy, on page 87 • Guidelines and Limitations, on page 7 • Smart Licensing Using Policy FAQs, on page 91

Date	Description
August 2023	Updated the following sections and published for Cisco NX-OS Release 10.4(1)F: • Supported Products, on page 13 • Feature History for Smart Licensing Using Policy, on page 87
July 2023	Updated the following sections: • Smart Licensing to Smart Licensing Using Policy, on page 53 • Guidelines and Limitations, on page 7
June 2023	Restructured the Smart Licensing Using Policy User Guide. Updated the following sections and published: • RTU Licensing to Smart Licensing Using Policy, on page 60
May 2023	Updated the following sections and published for Cisco NX-OS Release 10.3(3)F: • Guidelines and Limitations, on page 7 • Configuring a DNS Client, on page 39 • Setting the Smart License Parameters, on page 46 • Feature History for Smart Licensing Using Policy, on page 87
April 2023	Updated the following sections and published: • Guidelines and Limitations, on page 7 • Topology 1:Connected to CSSM Through CSLU, on page 18 • Configuring Smart Transport Through an HTTPS Proxy, on page 37 • Configuring a Source Interface to Send Messages Using HTTP, on page 40 • SLP Configuration - Connected to CSSM Through CSLU
February 2023	Updated the following section and published: • Guidelines and Limitations, on page 7

Date	Description
December 2022	Updated the following sections and published for Cisco NX-OS Release 10.3(2)F: • Guidelines and Limitations, on page 7 • Supported Products, on page 13 • Configuring a Source Interface to Send Messages Using HTTP, on page 40 • Setting the Smart License Parameters, on page 46 • Feature History for Smart Licensing Using Policy, on page 87
November 2022	Updated the following sections and published: • SSM On-Prem, on page 15 • Upgrades, on page 50 • Guidelines and Limitations, on page 7
August 2022	Updated the following sections and published for Cisco NX-OS Release 10.3(1)F: • Supported Products, on page 13 • Feature History for Smart Licensing Using Policy, on page 87
July 2022	Updated the following sections and published: • Overview, on page 5 • Topology 4:Connected to CSSM Through SSM On-Prem, on page 27 • Topology 5:SSM On-Prem Disconnected from CSSM, on page 28 • Troubleshooting Smart Licensing Using Policy, on page 67
May 2022	Added/Updated the following sections and published: • Choosing a Topology, on page 18 • Guidelines and Limitations, on page 7

Date	Description
April 2022	Updated the following sections and published: • Guidelines and Limitations, on page 7 • Topology 4:Connected to CSSM Through SSM On-Prem, on page 27 • Topology 5:SSM On-Prem Disconnected from CSSM, on page 28 • Upgrades, on page 50 • SLP Configuration - Connected Directly to CSSM, on page 22 • Configuring an HTTP Proxy Server, on page 37 • Tasks for Product Instance-Initiated Communication, on page 27 • Migrating to Smart Licensing Using Policy, on page 53 • Configuring a DNS Client, on page 39 • Smart Licensing Using Policy FAQs, on page 91
December 2021	Updated the following sections and published: • SLP Configuration - No Connectivity to CSSM and No CSLU, on page 31 • Guidelines and Limitations, on page 7
August 2021	Published for Cisco NX-OS Release 10.2(1)F.

CHAPTER 2

Smart Licensing Using Policy

About this Guide

This document provides information about Smart Licensing Using Policy such as the concept, architecture, supported products and topologies, configuration, migration, tasks, and troubleshooting only for Cisco Nexus 9000 and 3000 Series switches.

Overview

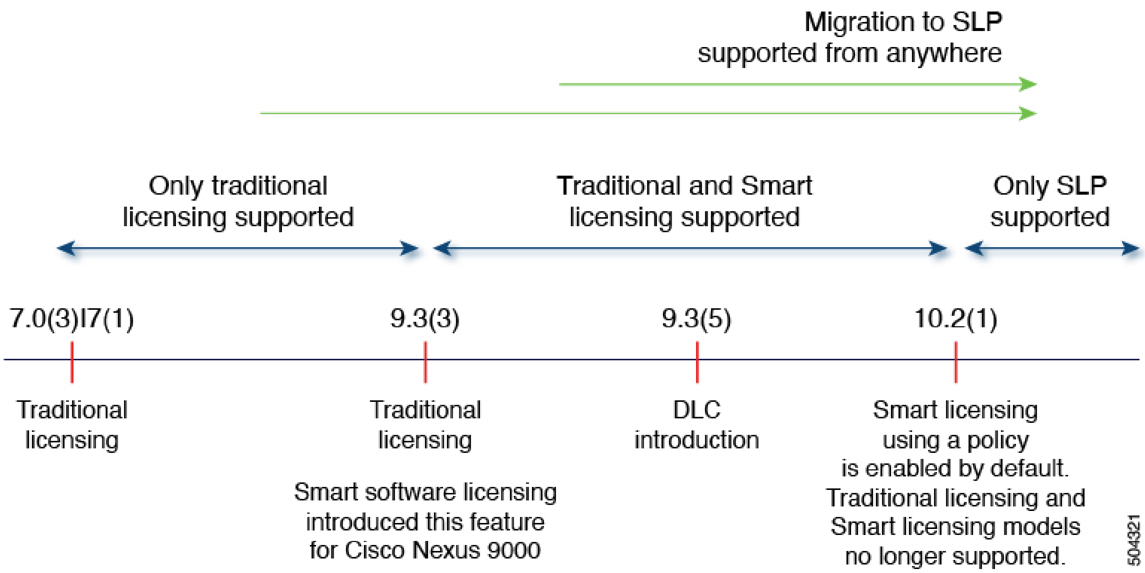
Introduction to Smart Licensing Using Policy

Smart Licensing Using Policy (SLP) is an enhanced version of Smart Licensing, the objective of which is to provide a licensing solution that does not interrupt the operations of your network and to enable a compliance relationship to account for the hardware and software licenses you purchase and use.

Smart Licensing Using Policy is introduced in Cisco NX-OS Release 10.2(1)F for Cisco Nexus 3000 and 9000 series switches.

The following image illustrates the evolution of Smart Licensing Using Policy (SLP) from the traditional licensing model through Cisco NX-OS Releases.

Figure 1: Evolution of licensing in Nexus 9000/3000 Series Platform Switches


Migration to SLP supported from anywhere
Only traditional licensing supported
Traditional and Smart licensing supported
Only SLP supported
7.0(3)I7(1)
9.3(3)
9.3(5)
10.2(1)
Traditional licensing
Traditional licensing
Smart software licensing introduced this feature for Cisco Nexus 9000
DLC introduction
Smart licensing using a policy is enabled by default. Traditional licensing and Smart licensing models no longer supported.
504321

This document provides information only on SLP. For information on older version licensing, refer to Cisco Smart License Utility User Guide.

The primary benefits of this enhanced licensing model are:

- Seamless day-0 operations

  After a license is ordered, no preliminary steps, such as registration or generation of keys, are required unless you use an export-controlled or enforced license. There are no export-controlled or enforced licenses on Cisco Nexus Switches, and product features can be configured on the device right-away.

- Consistency in Cisco NX-OS

  Devices that run Cisco NX-OS software have a uniform licensing experience.

- Visibility and manageability

  Tools, telemetry, and product tagging.

- Flexible, time series reporting to remain compliant

  Easy reporting options are available, whether you are directly or indirectly connected to Cisco Smart Software Manager (CSSM) or are in an air-gapped network.

This document provides conceptual, configuration, and troubleshooting information for SLP on Cisco Nexus Switches. For a more detailed overview on Cisco Licensing, go to cisco.com/go/licensingguide.

The conceptual information includes an overview of SLP, supported products, supported topology, and explains how SLP interacts with other features. SLP is a software license management solution that provides a seamless experience with the following aspects of licensing:

- Purchase: Purchase licenses through the existing channels and use the Cisco Smart Software Manager (CSSM) portal to view product instances and licenses.

  To simplify the implementation of SLP, provide your Smart Account and Virtual Account information when placing an order for new hardware or software. This allows Cisco to install applicable policies (terms explained in the Concepts section below), at the time of manufacturing.

- License Type: All licenses on Cisco Nexus Switches are unenforced. This means that you do not have to complete any licensing-specific operations, such as registering or generating keys before you start using the software and the licenses that are tied to it. License usage is recorded on your device with timestamps and the required workflows can be completed later.
- Report: License usage should be reported to CSSM. Multiple options are available for license usage reporting. You can use the Cisco Smart Licensing Utility (CSLU), or report usage information directly to CSSM. For air-gapped networks, a provision for offline reporting where you download usage information and upload it to CSSM, is also available. The usage report is in plain text XML format.
- Reconcile: For situations where delta billing applies (purchased versus consumed).

Guidelines and Limitations

The SLP feature has the following guidelines and limitations:

- In Cisco NX-OS Release 10.2(x), management VRF is supported on CSLU, Smart, and Callhome modes, and non-management VRF is supported only on Callhome. Beginning with Cisco NX-OS Release 10.3(2)F, non-management VRF is also supported on Smart and CSLU modes of transport.
- Beginning with Cisco NX-OS Release 10.3(2)F, source-interface is supported on Callhome mode with direct CSSM connectivity only. Beginning with Cisco NX-OS Release 10.3(3)F, support is introduced for source-interface with CSLU and Smart transport with both direct and indirect CSSM connectivity.
- When configuring the DNS resolution, configure it under the management VRF, as only management VRF is supported.
- IPv6 is only supported on callhome transport mode.
- CSLU-initiated communication/pull mode is not supported in Cisco NX-OS Release 10.2(1)F.
- CSLU configuration is mandatory if callhome is not configured and the device is not registered with CSSM, when moving from pre-SLP releases to SLP in Cisco NX-OS Release 10.2(1)F. For more information, see SLP Configuration - Connected to CSSM Through CSLU.
- Standalone CSLU does not support multi-tenancy, it supports only single SA/VA. However, SSM On-Prem supports multi-tenancy.
- For auto discovery, only one CSLU can be used in the network.
- SLP MIB is not supported.
- Only CSLU mode of transport is supported on On-Prem.
- For SL registered devices, when upgrading from Cisco NX-OS Release 9.3(3) or 9.3(4) to Cisco NX-OS Release 10.2(1)F, the transport mode may go to CSLU instead of callhome. It is recommended that you configure the transport mode to callhome manually and establish the trust with CSSM.
- During upgrade from earlier release with Traditional Licensing (PAK) to Cisco NX-OS Release 10.2(1)F, reflection of RUM sync in show command may take up to 24 hrs after migration.
- The output of the **show license status** command may show discrepancy in timer values, but has no functional impact. The timer gets updated automatically and the RUM Reporting will be retried after 24 hours.

- While using the transport mode as CSLU, if licenses do not get released from the SA/VA after write-erase and reload of the switch, it is recommended to delete the product instance from the SA/VA.
- For SL registered devices that are connected to On-Prem, when upgrading from any Traditional Licensing (PAK) to Cisco NX-OS Release 10.2(1)F, the license consumption may not adhere hierarchy rules of tier licenses at On-Prem. It is recommended that CSSM to be referred for proper consumption of licenses post sync from On-Prem.
- For SL registered devices with CSSM, when upgrading from Cisco NX-OS Release 9.3(3) or 9.3(4) to Cisco NX-OS Release 10.2(1)F, duplicate entry may occur for the same product instance on CSSM/On-Prem for a day.
- When a switch is being reset to factory defaults using the **write erase** command, it is recommended to do a **license smart factory reset** before reloading the switch.
- Cisco NX-OS Release 10.2(1)F supports only the SLP licensing mode.
- Cisco NX-OS Release 10.2(1)F does not support SL and PAK-based licensing.
- The following commands do not support XMLized output:
  - **show-tech support license**
  - **show license eventlog**
  - **show license history message**
  - **show license rum id all**
  - **show license data conversion**
- To find more information about rum reports, use the following show commands:
  - **show license rum id all** - The output of this show command displays the list of all rum ids.

Note The **show license rum id 0** command also displays the list of all rum reports. The value **0** also represents **all** in the case of this command.

  - **show license rum id** *report_id* - This command allows you to select one rum id from the list and the output of this command displays a short summary of the report.
  - **show license rum id all detail** - The output of this command provides a list of all rum ids in a detailed format.
  - **show license rum id** *report_id* **detail** - This command allows you to select one rum id, about which you want to know the details, from the list and the output displays a detailed format of the report.

- In Cisco NX-OS Release 10.3(2)F, **license smart vrf** is not supported on Cisco Nexus C92348GC-X switch. When management VRF is configured, upgrade of Cisco Nexus C92348GC-X switch from Cisco NX-OS Release 10.3(2)F to 10.3(3)F is supported. When management VRF is not configured, to upgrade Cisco Nexus C92348GC-X switch from Cisco NX-OS Release 10.3(2)F to 10.3(3)F, first configure **no license smart vrf** and then proceed with the upgrade.
- Beginning with Cisco NX-OS Release 10.4(3)F, Cisco Nexus switches provide TLSv1.3 support in SLP licensing mode.

Concepts

This section explains the key concepts of SLP.

License Enforcement Types

The only enforcement type supported on Cisco Nexus 9000 and 3000 platform switches is Unenforced or Not Enforced. Unenforced licenses do not require authorization before use in air-gapped networks or in connected networks. The terms of use for such licenses are as per the end user license agreement (EULA).

Note Enforced and Export licenses are not supported on Cisco Nexus 9000 platform switches.

License Duration

This refers to the duration or term for which a purchased license is valid. A given license may belong to any one of the enforcement types mentioned above and be valid for the following durations:

- Perpetual: A perpetual license enables you to make a one-time purchase of a license that does not expire.
- Subscription: A subscription-based license enables you to purchase a license for a specific period of time based on your requirement.

Policy

A policy provides the switch with these reporting instructions:

- License usage report acknowledgment requirement (Reporting ACK required): The license usage report is known as a RUM Report and the acknowledgment is referred to as an ACK (See RUM Report and Report Acknowledgment). This is a yes or no value that specifies if the report for this product instance requires CSSM acknowledgment. The default policy is always set to yes.
- First report requirement (days): The first report must be sent within the duration specified here.
- Reporting frequency (days): The subsequent report must be sent within the duration specified here.
- Report on change (days): If there is a change in license usage, a report must be sent within the duration specified here.

Understanding the Policy Selection

CSSM determines the policy that is applied to a switch. Only one policy is in use at a given point in time. The policy and its values are based on several factors, including the licenses being used.

Cisco default is the default policy that is always available in the product instance. If no other policy is applied, the product instance applies this default policy. Table 1: Policy Cisco default for NX-OS, on page 10 shows the Cisco default policy values.

If you cannot configure a policy, you can request for a customized one, by contacting the Cisco Global Licensing Operations team. Go to Support Case Manager. Click **OPEN NEW CASE** > **Select Software**

Licensing. The licensing team will contact you to start the process or for any additional information. Customized policies are also made available through your Smart account in CSSM.

Note To know which policy is applied (the policy in-use) and its reporting requirements, enter the **show license all** command in privileged EXEC mode.

Table 1: Policy Cisco default for NX-OS

Policy: Cisco Default	Default Policy Values
Unenforced/Non-Export	Reporting ACK required: Yes First report requirement (days): 90 Reporting frequency (days): 365 Report on change (days): 90

RUM Report and Report Acknowledgment

A Resource Utilization Measurement report (RUM report) is a license usage report, which the product instance generates, to fulfill reporting requirements as specified by the policy.

An acknowledgment (ACK) is a response from CSSM and provides information about the status of a RUM report.

The policy that is applied to a product instance determines the following reporting requirements:

- Whether a RUM report is sent to CSSM, and the maximum number of days provided to meet this requirement.
- Whether the RUM report requires an acknowledgment (ACK) from CSSM.
- The maximum number of days provided to report a change in license consumption.

A RUM report sent to CSSM from device/CSLU may be accompanied by other requests.

Note System logs are generated at X and X-30 days if reporting is not done. X is the reporting interval per the policy.

Below is the example for RUM:

```
<?xml version="1.0" encoding="UTF-8"?>
<smartLicense>
<RUMReport>
<![CDATA[
{
   "payload":{
      "asset_identification":{
         "asset":{

"name":"regid.2017-11.com.cisco.Nexus_9300,1.0_ac6ddieu7-89ju-4dne7-8699-4eeeklljnk"
         },
         "instance":{
            "sudi":{
               "udi_pid":"N9K-C9364C-GX",
               "udi_serial_number":"FDjhjudyw8778"
            },
            "product_instance_identifier":"f804e59b-7296-4c6d-a4f4-e61207ddf150"
         },
         "signature":{
            "signing_type":"CISC123",
            "key":"00000000",
            "value":"A0EPZ4grbhDeNG2q1wJxeRAkEIFabnHp8UCB+qoFMFRA3oMkZ3G572mm
             FDFZXVSaA2yfVRym0GMgKDo2glzz7er1RVIyB8XnrqgdgFBMkvJiuHb5B9Bdvs
             8qABGErQZP7m5HTUQcHNwczYYAoflIMo2ltaaUzhbmjppoh1b6cIvjUqTVTyg37cj/

Z0r7hIviUxrzvHBVFFVA50Ik8wXPFWS24aLC4ubXvEDNzDv1UWQwfJy0XmkegJ07PBVAfcRPhfZ4/5J9YtsQ1xRb5ot+

             IdogZmhX7ISVOAh3WFjvAMVhQrH4xeSKD1wgIZtLAC+TnixvU6HAc4p168UK6aZV4A=="
         }
      },
      "meta":{
         "entitlement_tag":"regid.2019-06.com.cisco.LAN_Nexus9300_XF2,1.0_
ac6ddieu7-89ju-4dne7-8699-4eeeklljnk",
         "report_id":16283555555,
         "software_version":"10.2(1)FI9(1)",
         "ha_udi":[
            {
               "role":"Active",
               "sudi":{
                  "udi_pid":"N9K-C9364C-GX",
                  "udi_serial_number":" FDjhjudyw8778"
               }
            }
         ]
      },
      "measurements":[
         {
            "log_time":1628323253,
            "metric_name":"ENTITLEMENT",
            "start_time":1628323253,
            "end_time":1628323254,
            "sample_interval":1,
            "num_samples":1,
            "meta":{
               "termination_reason":"CurrentUsageRequested"
            },
            "value":{
               "type":"COUNT",
               "value":"1"
            }
         }
      ]
   },
   "header":{
      "type":"rum"
   },
   "signature":{
      "sudi":{
         "udi_pid":"N9K-C9364C-GX",
         "udi_serial_number":"FDOkjahwdiuw78"
      },
      "signing_type":"CISC123",
      "key":"782198723987",
      "value":"BIoW16suShhDdAJZgRGtxdk/b4yhdvtDJQzE4eujgG+w/
```

```
UKICJ40oEsh2HfIy0kcbfSn3gaAPwhlwHxFUVjLh+kYHxuwSvsI0RwwyIgBIlYbc9JojQ40dZGLRVmJt05djYIRkRHI5dYMO0Fn/

a/F+VnaEQ2hVbbTWMW0pDLnJksPyQ9Mn91RmI4ZCfkS5gGNeS9U0CyeBpSYfh/r+N4bn/gmf+XDmK30x6yukTflvUC6IV/

lNMxJYOpZ87mV/4XX6Bw88Ab1K3KX6VHVpeMr45UeUNGd0efaigReB9ERISJnERxAEs4SuU/ZhnFMONAwW/4WCpDXD/p8bcw76mmSkw=="

   }
}
]]>
</RUMReport>
</smartLicense>
```

Below is the example for RUM ACK

```
<?xml version="1.0" encoding="UTF-8"?>
<smartLicense>
   <smartLicenseRumAck>
      <data>
        <![CDATA[[
        {
           "status_code":"OK",
           "status_message":"Rum Report is accepted.",
           "localized_message":"Rum Report is accepted.",
           "product_instance_identifier":"f80003456-1234-3g5h-b6b6-e1234hrtu5678",
           "sudi":{
              "udi_pid":"N9K-C9364C-GX",
              "udi_serial_number":"FDO3456yuth"
           },
           "report_id":162123456,
           "correlation_id":"610e4fcecebababeyro678990-bf94ajdu47878787hdj",
           "subscription_id":null
        }
      ]]]>
    </data>
    <signature>MEQCIBtBcrLc384LDGgD9axXIMFiV4usLWOeOvJiP4nL9PKhAiA16
yiPufFIFwfEPIGbqMbfTKB+gGxB52m5tPVWZ/MP6Q==</signature>
   </smartLicenseRumAck>
   <smartLicenseAccountInfo>
      <customerInfo>
         <timestamp>1628327760658</timestamp>
         <smartAccount>InternalTestDemoAccount10.cisco.com</smartAccount>
         <virtualAccount>nxofirst</virtualAccount>
         <smartAccountId>2312345</smartAccountId>
         <virtualAccountId>509876</virtualAccountId>
         <smartAccountDomain>internaltestdemoaccount10.cisco.com</smartAccountDomain>
      </customerInfo>
      <signature>MEQCIBelsrxUBMzZSi406NeeHOJRlboJedEThjgyutwiqwge2iuey2
uehdufydwinGOsmgLaef1HAG+naWneLqZ139ARFiTsmA==</signature>
   </smartLicenseAccountInfo>
   <correlationID>ngnx-d3chwyt37hgdytf1924b4a57c190bc6</correlationID>
</smartLicense>
```

Trust Code

Trust code is a UDI-tied public key with which the product instance signs a RUM report. This prevents tampering and ensures data authenticity.

Supported Products

This section provides information about the Cisco NX-OS switches that are within the scope of this document and support SLP. All models (Product IDs or PIDs) in a product series are supported – unless indicated otherwise.

Table 2: Cisco Nexus Switches

Cisco Nexus Switches	When Support was Introduced
Cisco Nexus 9364C-H1 switch	Cisco NX-OS Release 10.4(3)F
Cisco Nexus 93108TC-FX3 switch, Cisco Nexus 93400LD-H1 switch	Cisco NX-OS Release 10.4(2)F
Cisco Nexus 9804 switch, Cisco Nexus 9332D-H2R switch, Cisco Nexus 9348GC-FX3 switch, Cisco Nexus 9348GC-FX3PH switch	Cisco NX-OS Release 10.4(1)F
Cisco Nexus 9408 Platform Switches	Cisco NX-OS Release 10.3(2)F
Cisco Nexus 9808 Platform Switches	Cisco NX-OS Release 10.3(1)F
Cisco Nexus 9500 Series Switches	Cisco NX-OS Release 10.2(1)F
Cisco Nexus 9300 Series Switches	Cisco NX-OS Release 10.2(1)F **Note** Beginning from Cisco NX-OS Release 10.3(1)F, 24-port licensing support is provided for the following Cisco Nexus platform switches: • N9K-C93108TC-FX3P • N9K-C93180YC-FX3 • N9K-C93180YC-FX3H
Cisco Nexus 3600 Series Switches	Cisco NX-OS Release 10.2(1)F
Cisco Nexus 3500 Series Switches	Cisco NX-OS Release 10.2(1)F

Note For the hardware that are not supported, refer to Cisco Nexus 9000 Series NX-OS Release Notes, Release 10.1(1) - Cisco.

Architecture

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

Product Instance or Switch

A Product Instance (PI), for example, a switch, is a single instance of a Cisco product, which is identified by a Unique Device Identifier (UDI).

A PI records and reports license usage (Resource Utilization Measurement reports) and provides alerts and system messages about issues such as overdue reports and communication failures. Resource Utilization Measurement (RUM) reports and usage data are securely stored in the product instance.

Throughout this document, the term product instance refers to all supported physical and virtual product instances, unless noted otherwise. For information about the product instances that are within the scope of this document, see Supported Products.

CSSM

Cisco Smart Software Manager (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 the CSSM Web UI at https://software.cisco.com/software/smart-licensing/alerts. Navigate to Manage licenses link.

See the Supported Topologies section to know about the different ways in which you can connect to CSSM.

In CSSM you can perform the following:

- 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 Instance
- Run reports against your virtual accounts
- Modify your email notification settings
- View overall account information

CSLU

Cisco Smart License Utility (CSLU) is a Windows-based reporting utility that provides aggregate licensing workflows. This utility performs the following key functions:

- Provides options relating to how workflows are triggered. The workflows can be triggered by CSLU or by the product instance.

- Collects usage reports from the product instance and uploads 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 sent back to the product instance.
- Sends authorization code requests to CSSM and receives authorization codes from CSSM, if applicable.

CSLU can be part of your implementation in the following ways:

- Install the Windows application to use CSLU as a standalone tool that is connected to CSSM.
- Install the Windows application to use CSLU as a standalone tool that is disconnected from CSSM. With this option, the required usage information is downloaded to a file and then uploaded to CSSM. This is suited for air-gapped networks.

SSM On-Prem

Smart Software Manager On-Prem (SSM On-Prem) is an asset manager, which works in conjunction with CSSM. It enables you to administer products and licenses on your premises instead of having to directly connect to CSSM.

Information about the required software versions to implement SLP with SSM On-Prem, is provided below:

Minimum Required SSM On-Prem Version for SLP[1]	**Minimum Required Cisco NX-OS Version**[2]
Version 8, August, 2021	Cisco NX-OS Release 10.2(1)F

[1] The minimum required SSM On-Prem version. This means support continues on all subsequent releases - unless noted otherwise.

[2] The minimum required software version on the product instance. This means support continues on all subsequent releases - unless noted otherwise.

Note The latest version of SSM On-Prem for SLP is Version 8, June 2022.

For more information about SSM On-Prem, see Smart Software Manager On-Prem on the Software Download page. Hover mouse over the `.iso` image to display the documentation links to the following guides:

- Installation Guide – SSM On-Prem Installation Guide
- Release Notes – Cisco Smart Software Manager On-Prem Release Notes
- User Guide – Smart Software Manager On-Prem User Guide
- Console Guide – Smart Software Manager On-Prem Console Reference Guide
- Quick Start Guide – Smart Software Manager On-Prem Quick Start Installation Guide

CHAPTER 3

Configuring Smart Licensing Using Policy

This chapter provides the simplest and fastest way to implement a topology.

Note These workflows are meant for new deployments only. If you are migrating from an existing licensing model, see Migrating to Smart Licensing Using Policy, on page 53.

Supported Topologies

This section describes the various ways in which you can implement smart licensing policy. For each topology, refer to the accompanying overview to know how the setup is designed to work, and refer to the considerations and recommendations, if any.

After Topology Selection

After you have selected a topology, see Configuring Smart Licensing Using Policy. These workflows are only for new deployments. They provide the simplest and fastest way to implement a topology.

If you want to perform any additional configuration tasks, for instance, if you want to configure different license, or use add-on license, or if you want to configure a narrower reporting interval, see the Common

Tasks for Configuring Smart Licensing Using Policy, on page 33. Check the Supported Topologies, before you proceed.

Choosing a Topology

The following table allows you to choose a topology depending on your network deployment.

Topology	Recommendations
Topology 1:Connected to CSSM Through CSLU, on page 18	Use this topology when you do not want the switches to be directly connected to CSSM. This topology will support only one SA/VA combination.
Topology 2:Connected Directly to CSSM, on page 21	Use this topology when you have switches that are already registered to CSSM and need to continue in the same mode. If you need to continue using this topology after upgrading to SLP, then Smart Transport is the preferred transport method.
Topology 3:CSLU Disconnected from CSSM, on page 24	Use this topology when you need to manage or view license consumption locally. You can also use multiple VA.
Topology 4:Connected to CSSM Through SSM On-Prem, on page 27	Use this topology when you want to collect licensing information from each switch in the network and when there is no connectivity to CSSM.
Topology 5:SSM On-Prem Disconnected from CSSM, on page 28	Use this topology when you want to manage or view licenses from a single source. You can view license consumption locally. You can also use multiple SA/VA combinations.
Topology 6:No Connectivity to CSSM and No CSLU (Offline Mode), on page 31	Use this topology when you want to collect licensing information from a single source and when there is no connectivity to CSSM. You cannot view license consumption locally. Also, only a single VA can be used.

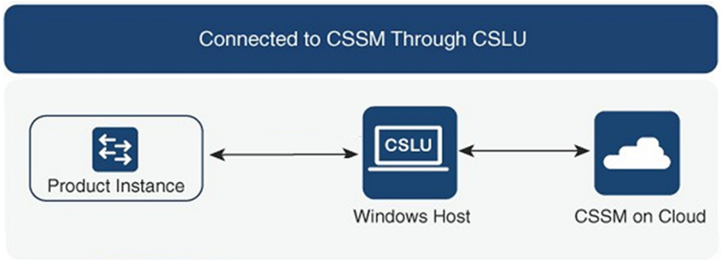
Topology 1:Connected to CSSM Through CSLU

Here, switches in the network are connected to CSLU, and CSLU becomes the single point of interface with CSSM. A switch can be configured to push the required information to CSLU.

The communication between PI to CSLU, and CSLU to CSSM occurs online through HTTPS mode. The switch Service Port is 8182, and the REST API Port number is 8180.

Switch-initiated communication (push): A switch initiates communication with CSLU, by connecting to a REST endpoint in CSLU. Data that is sent includes RUM reports. You can configure the switch to automatically send RUM reports to CSLU at required intervals.

Figure 2: Topology: Connected to CSSM Through CSLU



Considerations or Recommendations:

Choose the method of communication depending on your network's security policy.

SLP Configuration - Connected to CSSM Through CSLU

When implementing the product instance-initiated method of communication, complete the following tasks:

Tasks for Product Instance-Initiated Communication

CSLU Installation > **CSLU Preference Settings** > **Product Instance Configuration**

Step 1 CSLU Installation

Where task is performed: A Windows host (laptop, desktop, or a Virtual Machine (VM) Download the file from Smart Software Manager > **Smart Licensing Utility**.

Refer to the Cisco Smart License Utility Quick Start Setup Guide for help with installation and setup.

Step 2 CSLU Preference Settings

Where tasks are performed: CSLU

a) Logging into Cisco (CSLU Interface), on page 34
b) Configuring a Smart Account and a Virtual Account (CSLU Interface), on page 34
c) Adding a Product-Initiated Product Instance in CSLU (CSLU Interface), on page 35

Step 3 Product Instance Configuration

Where tasks are performed: Product Instance

a) Ensuring Network Reachability for Product Instance-Initiated Communication, on page 36.
b) Ensure that transport type is set to **cslu**.

CSLU is the default transport type. If you have configured a different option, enter the **license smart transport cslu** command in global configuration mode. Save any changes to the configuration file.

```
Device(config)# license smart transport cslu

Device(config)# exit

Device# copy running-config startup-config
```

c) Specify how you want CSLU to be discovered (choose one):

- Option 1:

  No action required. Name server configured for Zero-touch DNS discovery of **cslu-local**.

  Here, if you have configured DNS (The name server IP address is configured on the product instance), and the DNS server has an entry where hostname **cslu-local** is mapped to the CSLU IP address, then no further action is required. The product instance automatically discovers hostname **cslu-local**.

- Option 2:

  No action required. Name server and domain configured for Zero-touch DNS discovery of **cslu-local.<domain>**.

  Here if you have configured DNS, (the name server IP address and domain is configured on the product instance), and the DNS server has an entry where **cslu-local.<domain>** is mapped to the CSLU IP address, then no further action is required. The product instance automatically discovers hostname cslu-local.

- Option 3:

  Configure a specific URL for CSLU.

  Enter the **license smart url cslu** *http://<cslu_ip_or_host>:8182/cslu/v1/pi* command in global configuration mode. For **<cslu_ip_or_host>**, enter the hostname or the IP address of the Windows host where you have installed CSLU. 8182 is the port number and it is the only port number that CSLU uses.

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

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

  ```
  Device# copy running-config startup-config
  ```

As the product instance initiates communication, it automatically sends out the first RUM report at the scheduled time, per the policy. To know when the product instance will be sending this information, enter the **show license status** command in privileged EXEC mode and in the output, check the date for field `Next report push:`.

```
switch# show license  status
Utility:
    Status: DISABLED

Smart Licensing using Policy:
    Status: ENABLED

Data Privacy:
    Sending Hostname: yes
    Callhome Hostname Privacy: DISABLED
        Smart Licensing Hostname Privacy: DISABLED
    Version Privacy: DISABLED

Transport:
    Type: CSLU
    Cslu address: cslu-local
    VRF: cisco

Policy:
    Policy in use: Merged from multiple sources
    Reporting ACK required: Yes
    Unenforced/Non-Export:
        First report requirement (days): 90 (Installed)
```

```
        Ongoing reporting frequency (days): 365 (Installed)
        On change reporting (days): 120 (Installed)
    Enforced (Perpetual/Subscription):
        First report requirement (days): 30 (Installed)
        Ongoing reporting frequency (days): 90 (Installed)
        On change reporting (days): 60 (Installed)
    Export (Perpetual/Subscription):
        First report requirement (days): 30 (Installed)
        Ongoing reporting frequency (days): 30 (Installed)
        On change reporting (days): 30 (Installed)

Miscellaneous:
    Custom Id: <empty>

Usage reporting:
    Last ACK received: Nov 15 02:51:57 2022  UTC
    Next ACK deadline: Nov 15 02:51:57 2023  UTC
    Reporting push interval: 30 days
    Next ACK push check: <none>
    Next report push: Dec 15 02:46:56 2022  UTC
    Last report push: Nov 15 02:46:56 2022  UTC
    Last report file write: <none>

Trust Code installed: Nov 13 22:36:48 2022  UTC
    Active: PID: N9K-C93180YC-FX3H, SN: FDO26170Q6A
        Nov 13 22:36:48 2022  UTC
```

CSLU forwards the information to CSSM and the returning ACK from CSSM, to the product instance.

In case of a change in license usage, see Setting the Smart License Parameters, on page 46 to know how it affects reporting.

Topology 2:Connected Directly to CSSM

This topology is available in the earlier version of Smart Licensing and continues to be supported with SLP.

Here, you establish a direct and trusted connection from a switch to CSSM. The direct connection requires network availability to CSSM. For the switch to then exchange messages and communicate with CSSM, configure one of the transport options available with this topology (described below). Lastly, the establishment of trust requires the generation of a token from the corresponding Smart Account and Virtual Account in CSSM, and installation on the switch.

You can configure a switch to communicate with CSSM in the following ways:

- Use Smart transport to communicate with CSSM

  Smart transport is a transport method where a Smart Licensing (JSON) message is contained within an HTTPs message, and exchanged between a switch and CSSM, to communicate. The following Smart transport configuration options are available:

  - Smart transport: In this method, a switch uses a specific Smart transport licensing server URL. This must be configured exactly as shown in the workflow section.

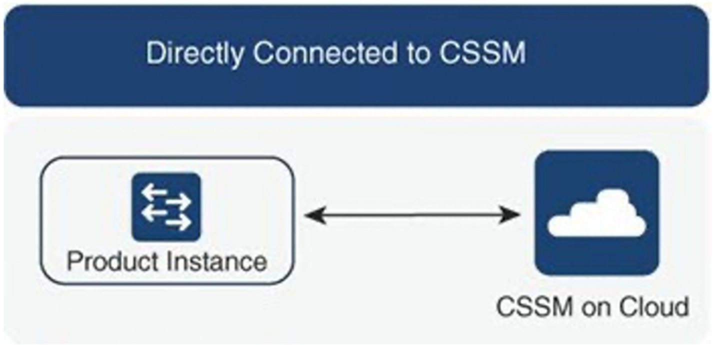
  - Smart transport through an HTTPS proxy: In this method, a switch uses a proxy server to communicate with the licensing server, and eventually, CSSM.

- Use Call Home to communicate with CSSM.

Call Home provides e-mail-based and web-based notification of critical system events. This method of connecting to CSSM is available in the earlier Smart Licensing environment and remains available with SLP. The following Call Home configuration options are available:

- Direct cloud access: In this method, a switch sends usage information directly over the internet to CSSM; no additional components are needed for the connection.
- Direct cloud access through an HTTPS proxy: In this method, a switch sends usage information over the internet through a proxy server - either a Call Home Transport Gateway or an off-the-shelf proxy (such as Apache) to CSSM.

Figure 3: Topology: Connected Directly to CSSM



Considerations or Recommendations:

Smart transport is the recommended transport method when directly connecting to CSSM. This recommendation applies to:

- New deployments.
- Earlier licensing models. Change configuration after migration to SLP.
- Registered licenses that currently use the Call Home transport method. Change configuration after migration to SLP.
- Evaluation or expired licenses in an earlier licensing model. Change configuration after migration to SLP.

To change configuration after migration, navigate **Connected Directly to CSSM** > **Switch Configuration** > **Configure a connection method and transport type** > **Option 1**.

SLP Configuration - Connected Directly to CSSM

Smart Account Set-Up > **Product Instance Configuration** > **Trust Establishment with CSSM**

Step 1 Smart Account Set-Up

Where task is performed: CSSM Web UI, Smart Software Manager.

Ensure that you have a user role with proper access rights to a Smart Account and the required Virtual Accounts.

Step 2 Product Instance Configuration

Where tasks are performed: Product Instance.

a) Set up product instance connection to CSSM: Setting Up a Connection to CSSM, on page 37.

b) Configure a connection method and transport type (choose one):

- Option 1:

  Smart transport: Set transport type to **smart** using the **license smart transport smart**. Save any changes to the configuration file.

  ```
  Device(config)# license smart transport smart
  ```

  ```
  Device(config)# license smart url smart
  https://smartreceiver.cisco.com/licservice/license
  ```

  ```
  Device(config)# copy running-config startup-config
  ```

- Option 2:

  Configure Smart transport through an HTTPS proxy. See Configuring Smart Transport Through an HTTPS Proxy, on page 37.

- Option 3:

  Configure Call Home service for direct cloud access. See Configuring the Call Home Service for Direct Cloud Access, on page 40.

- Option 4:

  Configure Call Home service for direct cloud access through an HTTPS proxy. See Configuring an HTTP Proxy Server, on page 37.

Step 3 Trust Establishment with CSSM

Where task is performed: CSSM Web UI and then the product instance

a) Generate one token for each Virtual Account you have. You can use the same token for all the product instances that are part of one Virtual Account: Generating a New Token for a Trust Code from CSSM, on page 42.

b) Having downloaded the token, you can now install the trust code on the product instance: Installing a Trust Code, on page 43.

Result:

After establishing trust, CSSM returns a policy. The policy is automatically installed on all product instances of that Virtual Account. The policy specifies if and how often the product instance reports usage.

If you want to change your reporting interval to report more frequently: on the product instance, configure the **license smart usage interval** command in global configuration mode. For syntax details see the **license smart (privileged EXEC)** command in the Command Reference for the corresponding release.

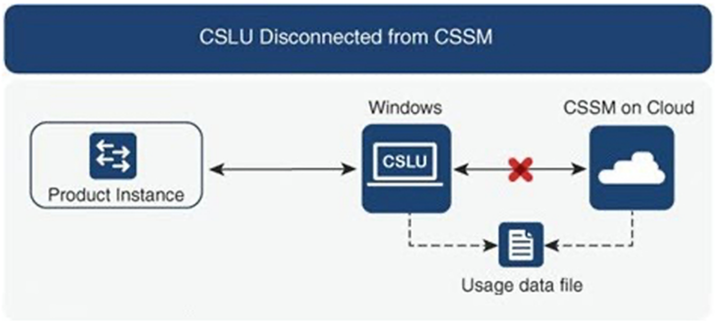
In case of a change in license usage, see Setting the Smart License Parameters, on page 46 to know how it affects reporting.

Topology 3:CSLU Disconnected from CSSM

Here, a switch communicates with CSLU, and you can implement the switch-initiated communication. The other side of the communication, between CSLU and CSSM, is offline. CSLU provides you with the option of working in a move that is disconnected from CSSM.

Communication between CSLU and CSSM is sent and received in the form of signed files that are saved offline and then uploaded to or downloaded from CSLU or CSSM.

Figure 4: Topology: CSLU Disconnected from CSSM



Considerations or Recommendations:

None.

SLP Configuration - CSLU Disconnected from CSSM

Depending on whether you want to implement a product instance-initiated method of communication. Complete the following tasks:

Tasks for Product Instance-Initiated Communication

CSLU Installation > **CSLU Preference Settings** > **Product Instance Configuration** > **Download All for Cisco and Upload From Cisco**

Step 1 CSLU Installation

Where task is performed: A Windows host (laptop, desktop, or a Virtual Machine (VM) Download the file from Smart Software Manager > **Smart Licensing Utility**.

Refer to the Cisco Smart License Utility Quick Start Setup Guide for help with installation and setup.

Step 2 CSLU Preference Settings

Where tasks are performed: CSLU.

a) In the CSLU Preferences tab, click the Cisco Connectivity toggle switch to **off**. The field switches to "Cisco Is Not Available‟.
b) Configuring a Smart Account and a Virtual Account (CSLU Interface), on page 34.
c) Adding a Product-Initiated Product Instance in CSLU (CSLU Interface), on page 35.

Step 3 Product Instance Configuration

Where tasks are performed: Product Instance

a) Ensuring Network Reachability for Product Instance-Initiated Communication, on page 36.
b) Ensure that transport type is set to **cslu**.

CSLU is the default transport type. If you have configured a different option, enter the **license smart transport cslu** command in global configuration mode. Save any changes to the configuration file.

```
Device(config)# license smart transport cslu

Device(config)# exit

Device# copy running-config startup-config
```

c) Specify how you want CSLU to be discovered (choose one):

- Option 1:

  No action required. Name server configured for Zero-touch DNS discovery of cslu-local.

  Here, if you have configured DNS (The name server IP address is configured on the product instance), and the DNS server has an entry where hostname **cslu-local** is mapped to the CSLU IP address, then no further action is required. The product instance automatically discovers hostname **cslu-local**.

- Option 2:

  No action required. Name server and domain that is configured for Zero-touch DNS discovery of **cslu-local.<domain>**.

  Here if you have configured DNS, (the name server IP address and domain is configured on the product instance), and the DNS server has an entry where **cslu-local.<domain>** is mapped to the CSLU IP address, then no further action is required. The product instance automatically discovers hostname **cslu-local**.

- Option 3:

  Configure a specific URL for CSLU.

  Enter the **license smart url cslu** *http://<cslu_ip_or_host>:8182/cslu/v1/pi* command in global configuration mode. For **<cslu_ip_or_host>**, enter the hostname or the IP address of the windows host where you have installed CSLU. 8182 is the port number and it is the only port number that CSLU uses.

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

Device(config)# exit

Device# copy running-config startup-config
```

Step 4 Download All for Cisco and Upload From Cisco.

Where tasks are performed: CSLU and CSSM

a) Download All for Cisco (CSLU Interface).
b) Uploading Usage Data to CSSM and Downloading an ACK, on page 44.
c) Upload From Cisco (CSLU Interface).

As the product instance initiates communication, it automatically sends out the first RUM report at the scheduled time, as per the policy. To know when the product instance will be sending this information, enter the **show**

license status command in privileged EXEC mode and in the output, check the date for field **Next report push:**.

```
switch# show license  status
Utility:
    Status: DISABLED

Smart Licensing using Policy:
    Status: ENABLED

Data Privacy:
    Sending Hostname: yes
    Callhome Hostname Privacy: DISABLED
        Smart Licensing Hostname Privacy: DISABLED
    Version Privacy: DISABLED

Transport:
    Type: CSLU
    Cslu address: cslu-local
    VRF: cisco

Policy:
    Policy in use: Merged from multiple sources
    Reporting ACK required: Yes
    Unenforced/Non-Export:
        First report requirement (days): 90 (Installed)
        Ongoing reporting frequency (days): 365 (Installed)
        On change reporting (days): 120 (Installed)
    Enforced (Perpetual/Subscription):
        First report requirement (days): 30 (Installed)
        Ongoing reporting frequency (days): 90 (Installed)
        On change reporting (days): 60 (Installed)
    Export (Perpetual/Subscription):
        First report requirement (days): 30 (Installed)
        Ongoing reporting frequency (days): 30 (Installed)
        On change reporting (days): 30 (Installed)

Miscellaneous:
    Custom Id: <empty>

Usage reporting:
    Last ACK received: Nov 15 02:51:57 2022  UTC
    Next ACK deadline: Nov 15 02:51:57 2023  UTC
    Reporting push interval: 30 days
    Next ACK push check: <none>
    Next report push: Dec 15 02:46:56 2022  UTC
    Last report push: Nov 15 02:46:56 2022  UTC
    Last report file write: <none>

Trust Code installed: Nov 13 22:36:48 2022  UTC
    Active: PID: N9K-C93180YC-FX3H, SN: FDO26170Q6A
        Nov 13 22:36:48 2022  UTC
```

As the CSLU is disconnected from CSSM, you must save usage data which CSLU has collected from the product instance to a file. Then, from a workstation that is connected to Cisco, upload it to CSSM. After this, download the ACK from CSSM. In the workstation where CSLU is installed and connected to the product instance, upload the file to CSLU.

In case of a change in license usage, see Setting the Smart License Parameters, on page 46 to know how it affects reporting.

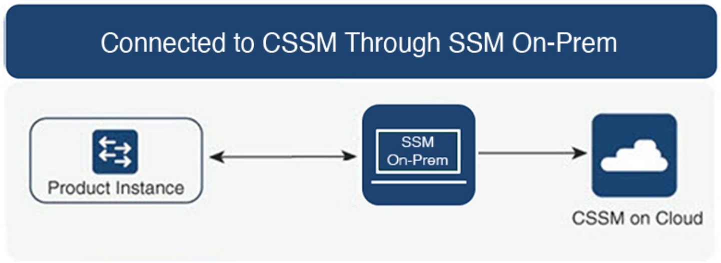
Topology 4:Connected to CSSM Through SSM On-Prem

Switches in the network are connected to Smart Software Manager (SSM) On-Prem, and SSM On-Prem becomes the single point of interface with CSSM. A switch can be configured to push the required information to SSM On-Prem.

Switch-initiated communication (push): A switch initiates communication with SSM On-Prem, by connecting to a REST endpoint in SSM On-Prem. Data that is sent includes RUM reports. You can configure the switch to automatically send RUM reports to SSM On-Prem at required intervals.

For more information about VRF management, see the Guidelines and Limitations, on page 7 and Configuring the Call Home Service for Direct Cloud Access, on page 40 sections.

Figure 5: Topology: Connected to CSSM Through SSM On-Prem



Considerations or Recommendations:

Choose the method of communication depending on your network’s security policy.

SLP Configuration - Connected to CSSM Through SSM On-Prem

When implementing the product instance-initiated method of communication, complete the corresponding sequence of tasks:

- Tasks for Product Instance-Initiated Communication, on page 27

Note If the device is registered to SSM On-Prem with pre-SLP release using callhome transport, then the transport mode changes to CSLU after the migration. Also, the url will be populated on the product instance from **OnPrem CSLU tenant ID**. Ensure that you save the configuration using the **copy running-config startup-config** command.

Tasks for Product Instance-Initiated Communication

SSM On-prem Installation > **On-prem Settings** > **Product Instance Configuration**

Step 1 SSM On-Prem Installation

Where task is performed: Download the file from Smart Software Manager.

Refer to the Cisco Smart License Utility Quick Start Setup Guide for help with installation and setup.

Step 2 On-Prem Settings

Where tasks are performed: On-Prem.

Refer Smart Software Manager On-Prem User Guide.

Step 3 Product Instance Configuration

Where tasks are performed: Product Instance.

a) Ensuring Network Reachability for Product Instance-Initiated Communication, on page 36.

b) Ensure that transport type is set to **cslu**.

If you have configured a different option, enter the **license smart transport cslu** command in global configuration mode. Save any changes to the configuration file.

```
Device(config)# license smart transport cslu
```

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

```
Device# copy running-config startup-config
```

c) The SSM On-Prem url will be populated on the product instance from SSU On-Prem tenant ID.

This configuration is visible as license smart url `https://Cisco_SSM_OnPrem/cslu/v1/pi/XYZ-ON-PREM-1`.

In the above url **XYZ-ON-PREM-1** is the tenant ID.

d) To discover SSM On-Prem:

No action required. Name server configured for Zero-touch DNS discovery of **Cisco_SSM_OnPrem**.

Here, if you have configured DNS (The name server IP address is configured on the product instance), and the DNS server has an entry where hostname **Cisco_SSM_OnPrem** is mapped to the On-Prem IP address, then no further action is required. The product instance automatically discovers hostname **Cisco_SSM_OnPrem**.

Result:

Since the product instance initiates communication, it automatically sends out the first RUM report at the scheduled time, as per the policy. To know when the product instance will be sending this information, enter the **show license all** command in privileged EXEC mode and in the output, check the date for field `Next report push:`.

On-Prem forwards the information to CSSM and the returning ACK from CSSM, to the product instance.

In case of a change in license usage, see Setting the Smart License Parameters, on page 46 to know how it affects reporting.

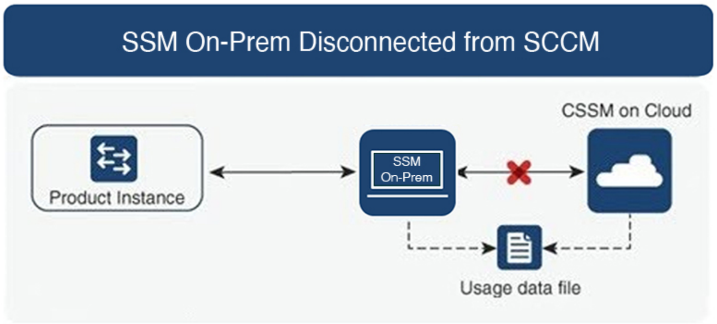
Topology 5:SSM On-Prem Disconnected from CSSM

Here, a switch communicates with SSM On-Prem, and you can implement the switch-initiated communication. The other side of the communication, between SSM On-Prem and CSSM, is offline. SSM On-Prem provides you with the option of working in a mode that is disconnected from CSSM.

Communication between SSM On-Prem and CSSM is sent and received in the form of signed files that are saved offline and then uploaded to or downloaded from SSM On-Prem or CSSM.

For more information about VRF management, see the Guidelines and Limitations, on page 7 and Configuring the Call Home Service for Direct Cloud Access, on page 40 sections.

Figure 6: Topology: SSM On-Prem Disconnected from CSSM



Considerations or Recommendations:

None.

SLP Configuration - SSM On-Prem Disconnected from CSSM

Depending on whether you want to implement a product instance-initiated method of communication. Complete the following tasks:

Note If the device is registered SSM On-Prem with pre-SLP release, the transport mode will change to CSLU after the migration. Also, the url will be populated on the product instance from **OnPrem CSLU tenant ID**. Ensure that you save the configuration using the **copy running-config startup-config** command.

Tasks for Product Instance-Initiated Communication

SSM On-prem Installation > On-prem Settings > Product Instance Configuration

Step 1 SSM On-Prem Installation

Where task is performed: Download the file from Smart Software Manager.

Refer to the Cisco Smart License Utility Quick Start Setup Guide for help with installation and setup.

Step 2 On-Prem Settings

Where tasks are performed: On-Prem

Refer Smart Software Manager On-Prem User Guide.

Step 3 Product Instance Configuration

Where tasks are performed: Product Instance

a) Ensuring Network Reachability for Product Instance-Initiated Communication, on page 36.
b) Ensure that transport type is set to **cslu**.

   If you have configured a different option, enter the **license smart transport cslu** command in global configuration mode. Save any changes to the configuration file.

```
Device(config)# license smart transport cslu
```

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

```
Device# copy running-config startup-config
```

c) The SSM On-Prem url will be populated on the product instance from SSM On-Prem tenant ID. This configuration is visible as license smart url https://Cisco_SSM_OnPrem/cslu/v1/pi/XYZ-ON-PREM-1.

   In the above url, **XYZ-ON-PREM-1** is the tenant ID.

d) To discover SSM On-Prem:

   No action required. Name server configured for Zero-touch DNS discovery of **Cisco_SSM_OnPrem**.

   Here, if you have configured DNS (The name server IP address is configured on the product instance), and the DNS server has an entry where hostname **Cisco_SSM_OnPrem** is mapped to the On-Prem IP address, then no further action is required. The product instance automatically discovers hostname **Cisco_SSM_OnPrem**.

Step 4 Download All for Cisco and Upload From Cisco.

Where tasks are performed: On-Prem and CSSM.

a) Log in to SSM On-Prem licensing workspace GUI.
   1. Click **SL Using Policy** tab.
   2. Click **Export/Import All** drop-down.
   3. Select **Export Usage Cisco** to upload and save the file.

b) Uploading Usage Data to CSSM and Downloading an ACK, on page 44.
c) Log in to SSM On-Prem licensing workspace GUI.
   1. Click **SL Using Policy** tab.
   2. Click **Export/Import All** drop-down.
   3. Select **Import From Cisco** to upload the ACK that is downloaded from CSSM.

Result:

Since the product instance initiates communication, it automatically sends out the first RUM report at the scheduled time, as per the policy. To know when the product instance will be sending this information, enter the **show license all** command in privileged EXEC mode and in the output, check the date for field `Next report push:`.

Since On-Prem is disconnected from CSSM, you must save usage data which On-Prem has collected from the product instance to a file. Then, from a workstation that is connected to Cisco, upload it to CSSM. After this, download the ACK from CSSM. In the workstation where On-Prem is installed and connected to the product instance, upload the file to On-Prem.

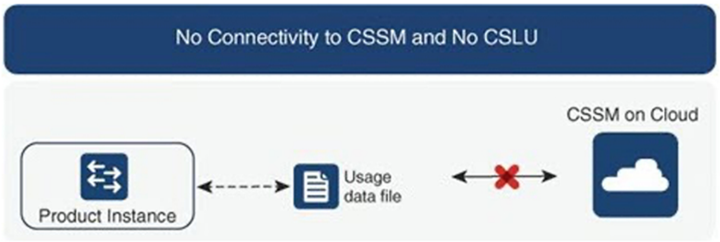
In case of a change in license usage, see Setting the Smart License Parameters, on page 46 to know how it affects reporting.

Topology 6:No Connectivity to CSSM and No CSLU (Offline Mode)

In the offline mode, a switch and CSSM are disconnected from each other, and without any other intermediary utilities or components. All communication is in the form of uploaded and downloaded files.

Note RUM reports cannot be saved if no licensing features are active.

Figure 7: Topology: No Connectivity to CSSM and No CSLU (Offline Mode)



Considerations or Recommendations:

This topology is suited to a high-security deployment where a switch cannot communicate online, with anything outside its network.

SLP Configuration - No Connectivity to CSSM and No CSLU

Since you do not have to configure connectivity to any other component, the list of tasks that are required to set up the topology is a small one. See, the Results section at the end of the workflow to know how you can complete requisite usage reporting after you have implemented this topology.

Product Instance Configuration

Where task is performed: Product Instance Set transport type to **off**.

Enter the **license smart transport off** command in global configuration mode. Save any changes to the configuration file.

```
Device(config)# license smart transport off

Device(config)# exit

Device# copy running-config startup-config
```

Result:

All communication to and from the product instance is disabled. To report license usage, you must save RUM reports to a file (on your product instance) and upload it to CSSM (from a workstation that has connectivity to the internet, and Cisco):

1. Generate and save RUM reports

   Enter the **license smart save usage** command in privileged EXEC mode. In the example below, all RUM reports are saved to the flash memory of the product instance, in the all_rum.txt file. In the example, the file is first saved to the bootflash and then copied to a TFTP location:

   ```
   Device# license smart save usage all bootflash:all_rum.txt
   ```

   ```
   Device# copy bootflash:all_rum.txt tftp://10.8.0.6/all_rum.txt
   ```

Note The RUM reports capture the licensing transactions in the device for upload. On a greenfield device, there is nothing to report, so it is empty and not generated. Also, when there are no licensing transactions, and the user tries to save the report, the **"Failure: save status: The requested item was not found"** error appears. After a few licensing transactions, such as enabling a licensing feature, the report gets populated and generated for online/offline upload.

2. Upload usage data to CSSM: Uploading Usage Data to CSSM and Downloading an ACK, on page 44.

3. Install the ACK on the product instance: Installing a File on the Switch, on page 45.

In case of a change in license usage, see Setting the Smart License Parameters, on page 46 to know how it affects reporting.

CHAPTER 4

Common Tasks for Configuring Smart Licensing Using Policy

This section is a grouping of tasks that apply to SLP. It includes tasks that are performed on a product instance, on the CSLU interface, and on the CSSM Web UI.

To implement a particular topology, refer to the corresponding workflow to know the sequential order of tasks that apply. See Configuring Smart Licensing Using Policy, on page 17.

To perform any additional configuration tasks, for instance, to configure a different license, or use an add-on license, or to configure a narrower reporting interval, refer to the corresponding task here. Check the Supported Topologies, before you proceed.

Logging into Cisco (CSLU Interface)

Depending on your needs, when working in CSLU, you can either be in connected or disconnected mode. To work in the connected mode, complete these steps to connect with Cisco.

Step 1 From the CSLU home screen, click **Login to Cisco** (located at the top-right corner of the screen).

Step 2 Enter your **CCO User Name** and **CCO Password**.

Step 3 In the CSLU **Preferences** tab, check that the Cisco connectivity toggle displays "Cisco Is Available".

Logging into Cisco (SSM On-Prem Interface)

Based on your requirement, when working in SSM On-Prem, either be in connected or disconnected mode. To work in the connected mode, perform these steps to connect to Cisco.

Step 1 Go to software download page.

Step 2 Click the appropriate release.

Step 3 Click **Related Links and Documentation** > **User Guide**.

Step 4 In User Guide, view the **Logging into Cisco SSM On-Prem** section.

Configuring a Smart Account and a Virtual Account (CSLU Interface)

Both the Smart Account and Virtual Account are configured through the Preferences tab. Complete the following steps to configure both the Smart and Virtual Accounts for connecting to Cisco.

Step 1 Select the **Preferences** tab from the CSLU home screen.

Step 2 Perform the following steps for adding both a Smart Account and Virtual Account:

a) In the **Preferences** window, navigate to the **Smart Account** field and add the **Smart AccountName**.

b) Next, navigate to the **Virtual Account** field and add the **Virtual Account Name.**

If you are connected to CSSM (in the Preferences tab, Cisco is Available), you can select from the list of available Smart Accounts (SA) and Virtual Accounts (VA).

If you are not connected to CSSM (in the Preferences tab, Cisco Is Not Available), enter the SA/VAs manually.

Note SA/VA names are case-sensitive.

Step 3 Click **Save**. The SA/VA accounts are saved to the system.

Only one SA/VA pair can reside on CSLU at a time. You cannot add multiple accounts. To change to another SA/VA pair, repeat Steps 2a and 2b then Save. A new SA/VA account pair replaces the previous saved pair.

Adding a Product-Initiated Product Instance in CSLU (CSLU Interface)

View the instructions for this section in the Cisco Smart License Utility User Guide.

Step 1 Go to https://software.cisco.com/download/home/286285506/type/286327971/release/.

Step 2 Click the appropriate release.

Step 3 Under the **Related Links and Documentation** section, click **User Guide**.

Export CSV (CSLU Interface)

Before you begin

View the instructions for this section in the Cisco Smart License Utility (CSLU) User Guide.

Step 1 Go to https://software.cisco.com/download/home/286285506/type/286327971/release/.

Step 2 Click the appropriate release.

Step 3 Under the **Related Links and Documentation** section, click **User Guide**.

Import CSV (CSLU Interface)

Before you begin

View the instructions for this section in the Cisco Smart License Utility (CSLU) User Guide.

Step 1 Go to https://software.cisco.com/download/home/286285506/type/286327971/release/.

Step 2 Click the appropriate release.

Step 3 Under the **Related Links and Documentation** section, click **User Guide**.

Export to CSSM

Before you begin

View the instructions for this section in the Cisco Smart License Utility (CSLU) User Guide.

Step 1 Go to https://software.cisco.com/download/home/286285506/type/286327971/release/.

Step 2 Click the appropriate release.

Step 3 Under the **Related Links and Documentation** section, click **User Guide**.

Import from CSSM

Before you begin

View the instructions for this section in the Cisco Smart License Utility (CSLU) User Guide.

Step 1 Go to https://software.cisco.com/download/home/286285506/type/286327971/release/.

Step 2 Click the appropriate release.

Step 3 Under the **Related Links and Documentation** section, click **User Guide**.

Ensuring Network Reachability for Product Instance-Initiated Communication

This task provides possible configurations that may be required to ensure network reachability for product instance-initiated communication. Steps marked as "(Required)" are required for all product instances, all other steps may be required or optional, depending on the kind of product instance and network requirements. Configure the applicable commands:

Before you begin

Supported topologies: Connected to CSSM Through CSLU (product instance-initiated communication).

Procedure

Ensure that CSLU is reachable from Product instance. For more information, see SLP Configuration - Connected to CSSM Through CSLU, on page 19.

Setting Up a Connection to CSSM

Ensure that product instance is reachable to CSSM. For more information about DNS configuration, see Configuring the Call Home Service for Direct Cloud Access, on page 40.

Configuring an HTTP Proxy Server

You can configure Smart Call Home to send HTTP messages through an HTTP proxy server. If you do not configure an HTTP proxy server, Smart Call Home sends HTTP messages directly to the Cisco Transport Gateway (TG).

To configure an HTTP proxy server, follow these steps:

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters configuration mode.
Step 2	switch(config)# **callhome**	Enters Call Home configuration submode.
Step 3	switch(config-callhome)# **transport http proxy server** *ip address*	Configures the HTTP proxy server domain name server (DNS) name, IPv4 address, or IPv6 address. Optionally configures the port number. The port range is from 1 to 65535. The default port number is 8080.
Step 4	switch(config-callhome)# **transport http proxy enable**	Enables Smart Call Home to send all HTTP messages through the HTTP proxy server. **Note** You can execute this command only after the proxy server address has been configured.
Step 5	Optional: switch(config-callhome)# **show callhome transport**	Displays the transport-related configuration for Smart Call Home. **Note** The default value for full text destination and for XML is 1 MB.

Configuring Smart Transport Through an HTTPS Proxy

To use a proxy server to communicate with CSSM when using the Smart transport mode, complete the following steps:

Note Authenticated HTTPS proxy configurations are not supported.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**license smart transport smart** **Example:** `Device(config)# license smart transport smart`	Enables Smart transport mode.
Step 3	**license smart proxy address** *address_hostname* **Example:** `Device(config)# license smart proxy address 198.51.100.10`	Perform this step only when HTTPS proxy is used in the network. Configures a proxy for the Smart transport mode. When a proxy is configured, licensing messages are sent to the proxy along with the final destination URL (CSSM). The proxy sends the message on to CSSM. Provide the address information: • **address** *address_hostname:* Specifies the proxy address. Enter the IP address or hostname of the proxy server.
Step 4	**license smart proxy port** *port_num* **Example:** `Device(config)# license smart proxy port 3128`	Perform this step only when HTTPS proxy is used in the network. Configures a proxy for the Smart transport mode. When a proxy is configured, licensing messages are sent to the proxy along with the final destination URL (CSSM). The proxy sends the message on to CSSM. Provide the port information: • **port** *port_num:* Specifies the proxy port. Enter the proxy port number.
Step 5	**exit** **Example:** `Device(config)# exit`	Exits global configuration mode and returns to privileged EXEC mode.
Step 6	**copy running-config startup-config** **Example:** `Device# copy running-config startup-config`	Saves your entries in the configuration file.

Configuring a DNS Client

Before you begin

Make sure that the name server is reachable before you configure a DNS client.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **ip domain-lookup**	Enables DNS-based address translation.
Step 3	switch(config)# **vrf context** *vrf-name*	Creates a new VRF and enters VRF configuration mode. The *name* can be any case-sensitive, alphanumeric string up to 32 characters.
Step 4	switch(config-vrf)# **ip domain-name** *domain name*	Defines the default domain name that Cisco NX-OS uses to resolve unqualified hostnames. Cisco NX-OS uses each entry in the domain list to append that domain name to any hostname that does not contain a complete domain name before starting a domain-name lookup. Cisco NX-OS continues this process for each entry in the domain list until it finds a match.
Step 5	switch(config-vrf)# **ip name-server** *address1 [address2... address6]* [**source-interface** {**loopback** | **port-channel** | **ethernet** | **mgmt.** | **vlan**}] [**use-vrf** *vrf-name*]	Defines up to six name servers. The address can be either an IPv4 or IPv6 address. • **source-interface** - Configures the source interface for all DNS packets. Available options for source-interface are loopback, port-channel, ethernet, management, or vlan interface. Only one source-interface can be mapped to one or more ip name-servers. **Note** Multiple DNS servers are for the case of unresponsive servers. If the first DNS server in the list replies to the DNS query with a reject, the remaining DNS servers are not queried. If the first one doesn't respond, the next DNS server in list is queried. • **use-vrf**- Configures the VRF on which the IP name server can be reached.

Configuring the Call Home Service for Direct Cloud Access

Make sure that Smart Call Home is enabled on the switch before configuring Smart Software Licensing.

Configuring a Source Interface to Send Messages Using HTTP

Beginning with Cisco NX-OS 10.3(2)F, you can optionally specify a source interface to send Smart Call Home messages over HTTP. If a source interface is not configured, the interface used to reach the Call Home server will be chosen.

SUMMARY STEPS

1. **configure terminal**
2. **callhome**
3. **source-interface** *interface*
4. **enable**
5. (Optional) **show callhome**
6. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**callhome**
	Example:
	`switch(config)# callhome`
	`switch(config-callhome)#`
		Enters Smart Call Home configuration mode.

Step 3	**source-interface** *interface*
	Example:
	`switch(config-callhome)# source-interface Ethernet1/1`
	`switch(config-callhome)#`
		Configures Smart Call Home to use this source interface when connecting to the Call Home server.

Step 4	**enable**
	Example:
	`switch(config-callhome)# enable`
	`switch(config-callhome)#`
		Enables callhome.

Step 5	(Optional) **show callhome**
	Example:
	`switch(config-callhome)# show callhome`
	`switch(config-callhome)#`
		(Optional) Displays information about Smart Call Home.

	Command or Action	Purpose

Step 6	(Optional) **copy running-config startup-config**
	Example:
	`switch(config)# copy running-config startup-config`
	`switch(config-callhome)#`
		(Optional) Copies the running configuration to the startup configuration.

What to do next

Optionally use VRFs to send Smart Call Home messages over HTTP.

Configuring a VRF to Send Messages Using HTTP

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **callhome**
3. switch(config-callhome)# **transport http use-vrf** *vrf-name*

DETAILED STEPS

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **callhome**	Enters Call Home configuration mode.
Step 3	switch(config-callhome)# **transport http use-vrf** *vrf-name*	Configures the VRF used to send email and other Smart Call Home messages over HTTP.

Viewing a Smart Call Home Profile

SUMMARY STEPS

1. switch# **show running-config callhome**

DETAILED STEPS

	Command or Action	Purpose
Step 1	switch# **show running-config callhome**	Displays the Smart Call Home profile.

Removing the Product Instance from CSSM

To remove a product instance and return all licenses to the license pool, complete the following task:

Before you begin

Supported topologies: all

Step 1 Log in to the CSSM Web UI at https://software.cisco.com and click **Smart SoftwareLicensing**.

Log in using the username and password that is provided by Cisco.

Step 2 Click the **Inventory** tab.

Step 3 From the **Virtual Account** drop-down list, choose your Virtual Account.

Step 4 Click the **Product Instances** tab.

The list of product instances that are available is displayed.

Step 5 Locate the required product instance from the product instances list. Optionally, you can enter a name or product type string in the search tab to locate the product instance.

Step 6 In the **Actions** column of the product instance you want to remove, click the **Remove** link.

Step 7 Click **Remove Product Instance**.

The license is returned to the license pool and the product instance is removed.

Generating a New Token for a Trust Code from CSSM

To generate a token to request a trust code, complete the following steps.

Generate one token for each Virtual Account you have. You can use the same token for all the product instances that are part of one Virtual Account.

Before you begin

Supported topology: Connected Directly to CSSM

Step 1 Log in to the CSSM Web UI at https://software.cisco.com/software/smart-licensing/alerts and click **Smart SoftwareLicensing**.

Log in using the username and password that is provided by Cisco.

Step 2 Click the **Inventory** tab.

Step 3 From the **Virtual Account** drop-down list, choose the required virtual account.

Step 4 Click the **General** tab.

Step 5 Click **New Token**. The **Create Registration Token** window is displayed.

Step 6 In the **Description** field, enter the token description.

Step 7 In the **Expire After** field, enter the number of days the token must be active.

Step 8 (Optional) **In the Max. Number of Uses** field, enter the maximum number of uses allowed after which the token expires.

Step 9 Click **Create Token**.

Step 10 You will see your new token in the list. Click **Actions** and download the token as a `.txt` file.

Installing a Trust Code

To manually install a trust code, complete the following steps:

Before you begin

Supported topology: Connected Directly to CSSM

Procedure

	Command or Action	Purpose
Step 1	Generating a New Token for a Trust Code from CSSM, on page 42	In case you have not completed this already, generate and download a trust code file from CSSM.
Step 2	**license smart trust idtoken** *id_token_value* {**local**|**all**} [**force**] **Example:** `Device# license smart trust idtoken NGMwMjk5mYtNZaxMS00NzMZmtgWm all force`	Enables you to establish a trusted connection with CSSM. For *id_token_value*, enter the token you generated in CSSM. Enter one of following options: • **local**: Submits the trust request only for the active device in a High Availability setup. This is the default option. • **all**: Submits the trust request for active and standby supervisors in HA setup. Enter the **force** keyword to submit the trust code request despite an existing trust code on the product instance. Trust codes are node-locked to the UDI of the product instance. If a UDI is already registered, CSSM does not allow a new registration for the same UDI. Entering the **force** keyword sets a force flag in the message sent to CSSM to create a new trust code even if one already exists.

Step 3	**show license status**
	Example:
	`<output truncated>`
	`Trust Code installed: Jul 16 15:15:47 2021 UTC`
	`    Active: PID: N9K-C9504, SN: FOX2308PCEN`
	`        Jul 16 15:15:47 2021 UTC`
	`    Standby: PID: N9K-C9504, SN: FOX2308PCEN`
	`        Jul 16 15:15:47 2021 UTC`
		Displays date and time if trust code is installed. Date and time are in the local time zone. See field `Trust Code Installed:`.

Downloading a Policy File from CSSM

If you have requested a custom policy or if you want to apply a policy that is different from the default that is applied to the product instance, complete the following task:

Before you begin

Supported topologies:

- No Connectivity to CSSM and No CSLU
- CSLU Disconnected from CSSM
- On-Prem CSLU disconnected from CSSM

Step 1 Log in to the CSSM Web UI at https://software.cisco.com/software/smart-licensing/alerts and click **Smart Software Licensing**.

Log in using the username and password that is provided by Cisco.

Step 2 Follow this directory path: **Reports** > **Reporting Policy**.

Step 3 Click **Download**, to save the `.xml` policy file.

You can now install the file on the product instance. See Installing a File on the Switch, on page 45.

Uploading Usage Data to CSSM and Downloading an ACK

To upload a RUM report to CSSM and download an ACK when the product instance is not connected to CSSM or CSLU, complete the following task:

Before you begin

Supported topologies: No Connectivity to CSSM and No CSLU

Step 1 Log in to the CSSM Web UI at https://software.cisco.com/software/smart-licensing/alerts.

Log in using the username and password that is provided by Cisco.

Step 2 Select the **Smart Account** (upper left corner of the screen) that will receive the report.

Step 3 Select **Smart Software Licensing** > **Reports** > **Usage Data Files**.

Step 4 Click **Upload Usage Data**. Browse to the file location (RUM report in tar format), select, and click **Upload Data**.

You cannot delete a usage report in CSSM, after it has been uploaded.

Step 5 From the Select Virtual Accounts pop-up, select the **Virtual Account** that receives 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, the time it was Reported, which Virtual Account it was uploaded to, the Reporting Status, the Number of Product Instances reported, and the Acknowledgment status.

Step 6 In the Acknowledgment column, click **Download** to save the `.txt` ACK file for the report you uploaded.

Wait for the ACK to appear in the Acknowledgment column. If there many RUM reports to process, CSSM may take a few minutes.

You can now install the file on the product instance, or you can transfer it to CSLU or On-Prem CSLU.

Installing a File on the Switch

To install a policy or ACK on the product instance when the product instance is not connected to CSSM, CSLU, or On-Prem CSLU, complete the following task:

Before you begin

Supported topologies: No Connectivity to CSSM and No CSLU

You must have the corresponding file saved in a location that is accessible to the product instance.

- For a policy, see Downloading a Policy File from CSSM, on page 44
- For an ACK, see Uploading Usage Data to CSSM and Downloading an ACK, on page 44

SUMMARY STEPS

1. **copy source bootflash**:`file-name`
2. **license smart import bootflash**: `file-name`
3. **show license all**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**copy source bootflash**:`file-name` **Example:** `Device# copy tftp://10.8.0.6/example.txt bootflash:`	Copies the file from its source location or directory to the flash memory of the product instance. **source**: This is the location of the source file or directory to be copied. The source can be either local or remote **bootflash:**: This is the destination for boot flash memory.
Step 2	**license smart import bootflash**: `file-name` **Example:** `Device# license smart import bootflash:example.txt`	Imports and installs the file on the product instance. After installation, a system message displays the type of file you installed.
Step 3	**show license all** **Example:** `Device# show license all`	Displays license authorization, policy, and reporting information for the product instance.

Setting the Smart License Parameters

To configure the mode of transport for a product instance, complete the following task:

Before you begin

Supported topologies: all

SUMMARY STEPS

1. **configure terminal**
2. **license smart transport**{ **callhome**|**cslu**|**off**|**smart**}
3. **license smart url**{**cslu** *cslu_url*|**smart** *smart_url*}
4. [**no**] **license smart vrf** *<vrf-name>*
5. **license smart usage interval** *interval_in_days*
6. **license smart source-interface** *source-interface*
7. **exit**
8. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

Step 2	**license smart transport**{ **callhome**|**cslu**|**off**|**smart**}
	Example:
	`Device(config)# license smart transport cslu`
		Selects the type of message transport the product instance uses. Choose from the following options:
		• **callhome**: Enables Call Home as the transport mode.
		• **cslu**: Enables CSLU as the transport mode. This is the default transport mode.
		• **off**: Disables all communication from the product instance.
		• **smart**: Enables Smart transport.

Step 3	**license smart url**{**cslu** *cslu_url*|**smart** *smart_url*}
	Example:
	`Device(config)# license smart url cslu http://192.168.0.1:8182/cslu/v1/pi`
		Sets a URL for the configured transport mode (except callhome, which is in the callhome configuration). Depending on the transport mode you have chosen to configure in the previous step, configure the corresponding URL here:
		• **cslu** *cslu_url*: The default value for cslu_url is set to cslu_local. If you want to set a custom url, then follow below steps:

	Command or Action	Purpose
		If you have configured the transport mode as **cslu**, configure this option. Enter the CSLU URL as follows: **https://<cslu_ip_or_host>:8182/cslu/v1/pi** For `<cslu_ip_or_host>`, enter the hostname or the IP address of the Windows host where you have installed CSLU. 8182 is the port number and it is the only port number that CSLU uses. The **no license smart url cslu** *cslu_url* command reverts to cslu_local. • **smart** *smart_url*: If you have configured the transport type as **smart**, then url is automatically configured to: https://smartreceiver.cisco.com/licservice/license. The **no license smart url smart** *smart_url* command reverts to the default URL as above.
Step 4	[**no**] **license smart vrf** <*vrf-name*> **Example:** `switch (conf)# license smart vrf vrf1`	Configures non-default VRF for smart and CSLU modes of transports. The **no** form of this command reverts to management VRF. **Note** To verify this configuration, use the **show run license** command.
Step 5	**license smart usage interval** *interval_in_days* **Example:** `Device(config)# license smart usage interval 40`	(Optional) Sets the reporting interval in days. By default, the RUM report is sent every 30 days. The valid value range is 1 to 365. If you set a value that is greater than zero and the transport type is set to **off**, then, between the *interval_in_days* and the policy value for ongoing reporting frequency(days):, the lower of the two values is applied. For example, if *interval_in_days* is set to 100, and the value in the policy says `Ongoing reporting frequency (days):90`, RUM reports are sent every 90 days. If you do not set an interval, and the default is effective, the reporting interval is determined entirely by the policy value. For example, if the default value is effective and only unenforced licenses are in use, if the policy states that reporting is not required, then RUM reports are not sent.
Step 6	**license smart source-interface** *source-interface* **Example:** `switch (config)# license smart source-interface Ethernet1/22`	Configures source interface only for smart and CSLU modes of transport, and not for callhome. The **no** form of this command removes the configured source interface.

	Command or Action	Purpose
		Note • If source-interface doesn’t have IP address, then forwarding decision is based on configured VRF. • If source-interface IP is present but the interface is down, then forwarding fails. • If the VRF of source interface does not match with the configured VRF as part of **license smart vrf**, then forwarding fails.
Step 7	**exit** **Example:** `Device(config)# exit`	Exits global configuration mode and returns to privileged EXEC mode.
Step 8	**copy running-config startup-config** **Example:** `Device# copy running-config startup-config`	Saves your entries in the configuration file.

CHAPTER 5

Interactions with Other Features

Interactions with Other Features

High Availability

This section explains considerations that apply to a High Availability configuration, when running a software version that supports SLP.

Trust Code Requirements in a High Availability Setup

In Dual Supervisor setup, two trust codes are installed. The active Product instance can submit the requests for both the supervisors and install the trust codes that are returned in an ACK.

Policy Requirements in a High Availability Setup

There are no policy requirements that apply exclusively to a High Availability setup. As in case of a standalone product instance, only one policy exists in a High Availability setup as well, and this is on the active. The policy on the active applies to the standby in the setup.

Product Instance Functions in a High Availability Setup

This section explains general product instance functions in a High Availability setup, and what the product instance does when a standby is added.

For trust codes: The active product instance can request (if necessary) and install trust codes for standby.

For policies: The active product instance synchronizes with the standby.

For reporting: Only the active product instance reports usage. The active reports usage information for standby.

In addition to scheduled reporting, the following events trigger reporting:

- The addition or removal of a standby. The RUM report includes information about the standby that was added or removed.
- A switchover.
- A reload.

For addition of a standby:

- A product instance that is connected to CSLU, does not take any further action.
- A product instance that is directly connected to CSSM, performs trust synchronization. Trust synchronization involves the following:
  - Installation of trust code on the standby if not installed already.
  - Installation of policy and purchase information, if applicable.
  - Sending of a RUM report with current usage information.

Upgrades

This section describes how upgrade or migration to SLP is handled. It also clarifies how SLP handles all earlier licensing models including: the earlier version of Smart Licensing, Right-to-Use Licensing (RTU), and how evaluation or expired licenses from any of the earlier licensing models are handled in SLP environment.

To migrate to SLP, you must upgrade to a software version that supports SLP. After you upgrade, SLP is the only supported licensing model and the switch continues to operate *without any licensing changes*. The SLP section provides details and examples for migration scenarios that apply to Cisco Nexus Switches.

Note When migrating from traditional licensing model to SLP, license conversion takes place automatically. This Device Led Conversion (DLC) process is triggered when traditional licenses are detected on the device during an upgrade. DLC request is sent to CSSM as part of the license report and may take up to an hour to complete.

Identifying the Current Licensing Model Before Upgrade

Before you upgrade to SLP, if you want to know the current licensing model that is effective on the switch, enter the show running license all command in privileged EXEC mode. This command displays information about the current licensing model for all except the RTU licensing model.

How an Upgrade Affects Enforcement Types for Existing Licenses

An unenforced license that was being used before upgrade, remains available after upgrade. All licenses on Cisco Nexus Switches are unenforced licenses. This includes licenses from the earlier licensing models as follows:

- Traditional Licensing (PAK)
- Smart Licensing
- Right-to-Use (RTU) Licensing
- Evaluation or expired licenses from any of the above-mentioned licensing models

How an Upgrade Affects Reporting for Existing Licenses

When you upgrade to a software version which supports SLP, reporting is based on the reporting requirements in the policy which can be displayed in the output of the **show license status** command for the following licenses:

- Traditional Licenses (PAK)
- Smart Licenses (Registered and Authorized licenses)
- Right-to-Use (RTU) Licenses
- Evaluation or expired licenses

How an Upgrade Affects Transport Type for Existing Licenses

The transport type, if configured in your existing setup, is retained after upgrade to SLP.

When compared to the earlier version of Smart Licensing, other transport types are available with SLP. There is also a change in the default transport mode. The following table clarifies how this may affect upgrades:

Migration	Transport Type Before Upgrade	Transport Type After Upgrade
SL (EVAL)	Callhome	CSLU
SL (Registered)		Callhome
PAK-based	NA	CSLU
SL (Registered) with On-Prem	callhome	CSLU

How an Upgrade Affects the Token Registration Process

In the earlier version of Smart Licensing, a token was used to register and connect to CSSM. ID token registration is not required in SLP. The token generation feature is still available in CSSM and is used to establish trust when a switch is directly connected to CSSM. For more information, see Topology 2:Connected Directly to CSSM.

Downgrades

To downgrade, you must downgrade the software version on the switch. This section provides information about downgrades for new deployments and existing deployments (you upgraded to SLP and now want to downgrade).

New Deployment Downgrade

This section applies if you had a newly purchased switch with a software version where SLP was already enabled by default, and you want to downgrade to a software version where SLP is not supported.

The outcome of the downgrade depends on whether a Trust Code was installed while you were still operating in the SLP environment, and further action may be required depending on the release you downgrade to.

If the topology you implemented while in the SLP environment was connected directly to CSSM, then a trust code installation can be expected or assumed, because it is required as part of topology implementation. For any of the other topologies, trust establishment is not mandatory. Downgrading switches with one of these other topologies will therefore mean that you must restore licenses to a registered and authorized state by following the procedures that are applicable in the Smart Licensing environment. The following table displays the outcome and action for new deployment downgrade to Smart Licensing.

Table 3: Outcome and Action for New Deployment Downgrade to Smart Licensing

In the SLP Environment	Downgrade to…	Outcome and Further Action
Standalone product instance, which is connected directly to CSSM, and trust established.	Action is required: You must reregister the product instance.	Action is required: You must reregister the product instance.
High Availability setup, which is connected directly to CSSM, and trust established.	Any release that supports Smart Licensing.	Action is required: You must reregister the product instance. Generate an ID token in the CSSM Web UI and on the product instance, enable smart licensing using **license smart enable** and configure the **license smart register idtoken** *idtoken* **all** command in global configuration mode.
Any other topology. (Connected to CSSM Through CSLU, CSLU Disconnected from CSSM, No Connectivity to CSSM and No CSLU)	Any release that supports Smart Licensing.	Action is required: Restore licenses to a registered and authorized state by following the procedures that are applicable in the Smart Licensing environment.

Upgrade and Then Downgrade

If you upgrade to a software version that supports SLP and then downgrade to any of the earlier licensing models, *license consumption does not change*, and any product features you have configured on the product instance are preserved – only the features and functions that are available with SLP are not available anymore. Refer to the corresponding section below to know more about reverting to an earlier licensing model.

Upgrade to SLP and Then Downgrade to Smart Licensing

The outcome of the downgrade depends on whether a Trust Code was installed while you were still operating in the SLP environment, and further action may be required depending on the release you downgrade to. See Table 3: Outcome and Action for New Deployment Downgrade to Smart Licensing, on page 52.

CHAPTER 6

Migrating to Smart Licensing Using Policy

To upgrade to SLP, you must upgrade the software version (image) on the switch to a supported version.

Before You Begin

Ensure that you have read the Upgrades, on page 50 section, to understand how SLP handles various aspects of all earlier licensing models.

When migrating from traditional licensing model to SLP, license conversion takes place automatically. This Device Led Conversion (DLC) process is triggered when traditional licenses are detected on the device during an upgrade. DLC request is sent to CSSM as part of the license report and may take up to an hour to complete.

Upgrading the Switch Software

See the corresponding release note for the upgrade procedure. If there are any general release-specific considerations, these are called-out in the corresponding release notes.

Also refer to the sample show command outputs of the migration scenarios provided below. Sample outputs are provided for before and after migration, for comparison.

- Smart Licensing to Smart Licensing Using Policy, on page 53
- RTU Licensing to Smart Licensing Using Policy, on page 60
- Evaluation or Eval Expired to Smart Licensing Using Policy, on page 61

Smart Licensing to Smart Licensing Using Policy

The following is an example of a Cisco Nexus 9000 switch migrating from Smart Licensing to SLP. This is a High Availability setup with an active and a standby.

The show command outputs below call-out key fields to check, before and after migration.

Table 4: Smart Licensing to Smart Licensing Using Policy: Show Commands

<table>
<tr><th>Before Upgrade</th><th>After Upgrade</th></tr>
<tr><td>

show license summary (Smart Licensing)

```
Device# show license summary

Smart Licensing is ENABLED

Registration:
  Status: REGISTERED
  Smart Account: BU Production Test 1
  Virtual Account: N9K_SA_49_Testing
  Export-Controlled Functionality: Allowed

License Authorization:
  Status: AUTHORIZED on Jul 16 14:26:01 2021
 UTC

  Last Communication Attempt: SUCCEEDED
  Next Communication Attempt: Aug 15 14:26:01
 2021 UTC
  Communication Deadline: Oct 14 14:20:59 2021
 UTC

Smart License Conversion:
  Automatic Conversion Enabled: False
  Status: Not started

License Usage:
License                    Entitlement tag
               Count   Status
---------------------------------------------
LAN license for Nexus 9...
(LAN_ENTERPRISE_SERVICES_PKG)    1
AUTHORIZED
Network Services for Ne...
(NETWORK_SERVICES_PKG)           1
AUTHORIZED
```

The **Status** and **License Authorization** fields show that the license is **REGISTERED** and **AUTHORIZED**.

</td><td>

show license summary (SLP)

```
Device# show license summary

License Usage:
License                    Entitlement tag
               Count   Status
---------------------------------------------
DCN NDB Add-On License ... (DCN_NDB)
                1       IN USE
Network Services for Ne...
(NETWORK_SERVICES_PKG)           1       IN
USE
LAN license for Nexus 9...
(LAN_ENTERPRISE_SERVICES_PKG)    1       IN
USE
```

The **Status** field shows that the licenses are now **IN USE** instead of registered and authorized.

</td></tr>
</table>

Before Upgrade	After Upgrade

show license usage (Smart Licensing)
`Device# show license usage`
`License Authorization:`
`  Status: AUTHORIZED on Jul 16 14:26:01 2021 UTC`
 	
`(LAN_ENTERPRISE_SERVICES_PKG):`
`  Description: LAN license for Nexus 9500-M4`
`  Count: 1`
`  Version: 1.0`
`  Status: AUTHORIZED`
 	
`(NETWORK_SERVICES_PKG):`
`  Description: Network Services for Nexus 9500-M4`
`  Count: 1`
`  Version: 1.0`
`  Status: AUTHORIZED`
	show license usage (SLP)
	`License Authorization: Status: Not Applicable`
	
	`(DCN_NDB):`
	`Description: DCN NDB Add-On License N9K Modular <<< This is RTU license`
	`Count: 1`
	`Version: 1.0`
	`Status: IN USE`
	`Enforcement Type: NOT ENFORCED`
	`License Type: Generic`
	
	`(NETWORK_SERVICES_PKG):`
	`Description: Network Services for Nexus 9500-M4`
	`Count: 1`
	`Version: 1.0`
	`Status: IN USE`
	`Enforcement Type: NOT ENFORCED`
	`License Type: Generic`
	
	`(LAN_ENTERPRISE_SERVICES_PKG):`
	`Description: LAN license for Nexus 9500-M4`
	`Count: 1`
	`Version: 1.0`
	`Status: IN USE`
	`Enforcement Type: NOT ENFORCED`
	`License Type: Generic`
	The license counts remain the same.
	The **Enforcement Type** field displays NOT ENFORCED. (There are no export-controlled or enforced licenses on Cisco Nexus Switches).

<table>
<tr><th>Before Upgrade</th><th>After Upgrade</th></tr>
<tr><td>

show license status (Smart Licensing)

```
Device# show license status
Smart Licensing is ENABLED

Registration:
  Status: REGISTERED
  Smart Account: BU Production Test 1
  Virtual Account: N9K_SA_49_Testing
  Export-Controlled Functionality: Allowed
  Initial Registration: SUCCEEDED on Jul 16
14:25:49 2021 UTC
  Last Renewal Attempt: None
  Next Renewal Attempt: Jan 12 14:25:48 2022
 UTC
  Registration Expires: Jul 16 14:20:45 2022
 UTC

License Authorization:
  Status: AUTHORIZED on Jul 16 14:26:01 2021
 UTC

  Last Communication Attempt: SUCCEEDED on
Jul 16 14:26:01 2021 UTC
  Next Communication Attempt: Aug 15 14:26:00
 2021 UTC
  Communication Deadline: Oct 14 14:20:58 2021
 UTC

Smart License Conversion:
  Automatic Conversion Enabled: False
  Status: Not started
```

</td><td></td></tr>
</table>

Before Upgrade	After Upgrade
	show license status (SLP)

```
Device# show license status

Utility:
    Status: DISABLED

Smart Licensing using Policy:
    Status: ENABLED

Data Privacy:
    Sending Hostname: yes
    Callhome Hostname Privacy: DISABLED
        Smart Licensing Hostname Privacy:
DISABLED
    Version Privacy: DISABLED

Transport:
     Type: Callhome

Policy:
    Policy in use: Merged from multiple
sources
    Reporting ACK required: Yes
    Unenforced/Non-Export:
        First report requirement (days): 90
(CISCO default)
        Ongoing reporting frequency (days):
365 (CISCO default)
       On change reporting (days): 90 (CISCO
 default)
    Enforced (Perpetual/Subscription):
        First report requirement (days): 0
(CISCO default)
        Ongoing reporting frequency (days):
0 (CISCO default)
        On change reporting (days): 0 (CISCO
 default)
Export (Perpetual/Subscription):
        First report requirement (days): 0
(CISCO default)
        Ongoing reporting frequency (days):
0 (CISCO default)
        On change reporting (days): 0 (CISCO
 default)
Miscellaneous:
    Custom Id: <empty>

Usage reporting:
    Last ACK received: Jul 16 15:22:31 2021
UTC
    Next ACK deadline: Jul 16 15:22:31 2022
UTC
    Reporting push interval: 30 days
    Next ACK push check: <none>
    Next report push: Aug 15 15:18:28 2021
UTC
    Last report push: Jul 16 15:18:28 2021
UTC
    Last report file write: <none>

Trust Code installed: Jul 16 15:15:47 2021
```

Before Upgrade	After Upgrade

	`UTC`
	`    Active: PID: N9K-C9504, SN: FOX2308PCEN`
	`        Jul 16 15:15:47 2021 UTC`
	`    Standby: PID: N9K-C9504, SN: FOX2308PCEN`
	
	`        Jul 16 15:15:47 2021 UTC`
	The Transport: **field**: A transport type was configured and therefore retained after upgrade.
	The `Policy:` header and details: A custom policy was available in the Smart Account or Virtual Account – this has also been automatically installed on the switch. (After establishing trust, CSSM returns a policy. The policy is then automatically installed.)
	The `Usage Reporting: header: The Next report push:` field provides information about when the switch will send the next RUM report to CSSM.
	The `Trust Code Installed: field:` The ID token is successfully converted and a trusted connected has been established with CSSM.

show license udi (Smart Licensing)
`Device# show license udi`
`UDI: PID:N9K-C9504, SN:FOX2308PCEN`
	show license udi (SLP)
	`Device# show license udi`
	`UDI: PID:N9K-C9504, SN:FOX2308PCEN`
	`HA UDI List:`
	` Active: PID:N9K-C9504, SN:FOX2308PCEN`
	`HA UDI List:`
	` Standby: PID:N9K-C9504, SN:FOX2308PCEN`
	This is a High Availability setup, and the command displays all UDIs in the setup.

CSSM Web UI After Migration

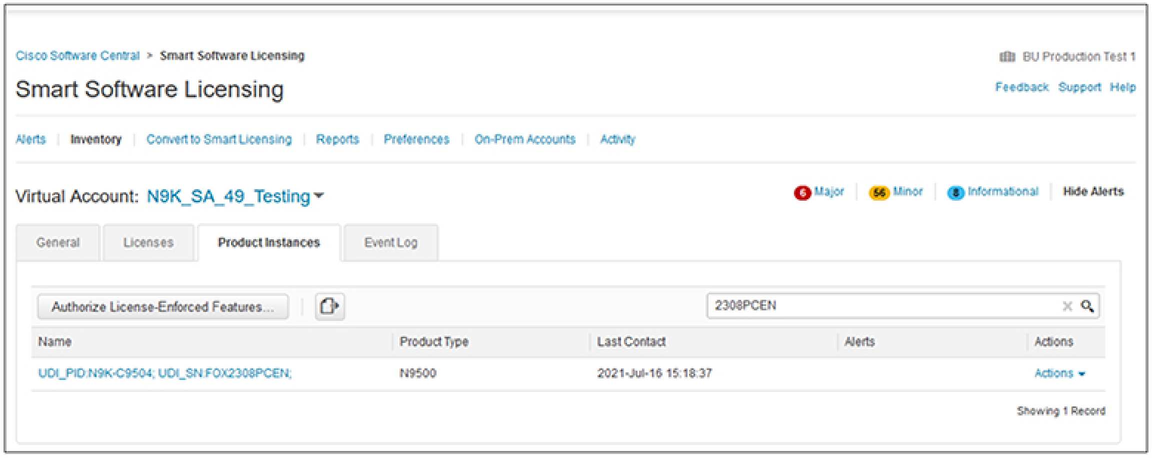
Log in to the CSSM Web UI at https://software.cisco.com/software/smart-licensing/alerts and click **Smart Software Licensing**. Under **Inventory** > **Product Instances**.

Registered licenses in the Smart Licensing environment were displayed with the hostname of the product instance in the Name column. After upgrade to SLP, they are displayed with the UDI of the product instance. All migrated UDIs are displayed. In this example, they are

PID:C9500-16X,SN:FCW2233A5ZV and PID:C9500-16X,SN:FCW2233A5ZY.

Only the active product instance reports usage, therefore PID:C9500-16X,SN:FCW2233A5ZV displays license consumption information under **License Usage**.

Figure 8: Smart Licensing to Smart Licensing Using Policy: Active and Standby Product Instances After Migration



Cisco Software Central > Smart Software Licensing

BU Production Test 1

Smart Software Licensing

Feedback Support Help

Alerts | Inventory | Convert to Smart Licensing | Reports | Preferences | On-Prem Accounts | Activity

Virtual Account: N9K_SA_49_Testing

6 Major | 56 Minor | 8 Informational | Hide Alerts

General | Licenses | Product Instances | Event Log

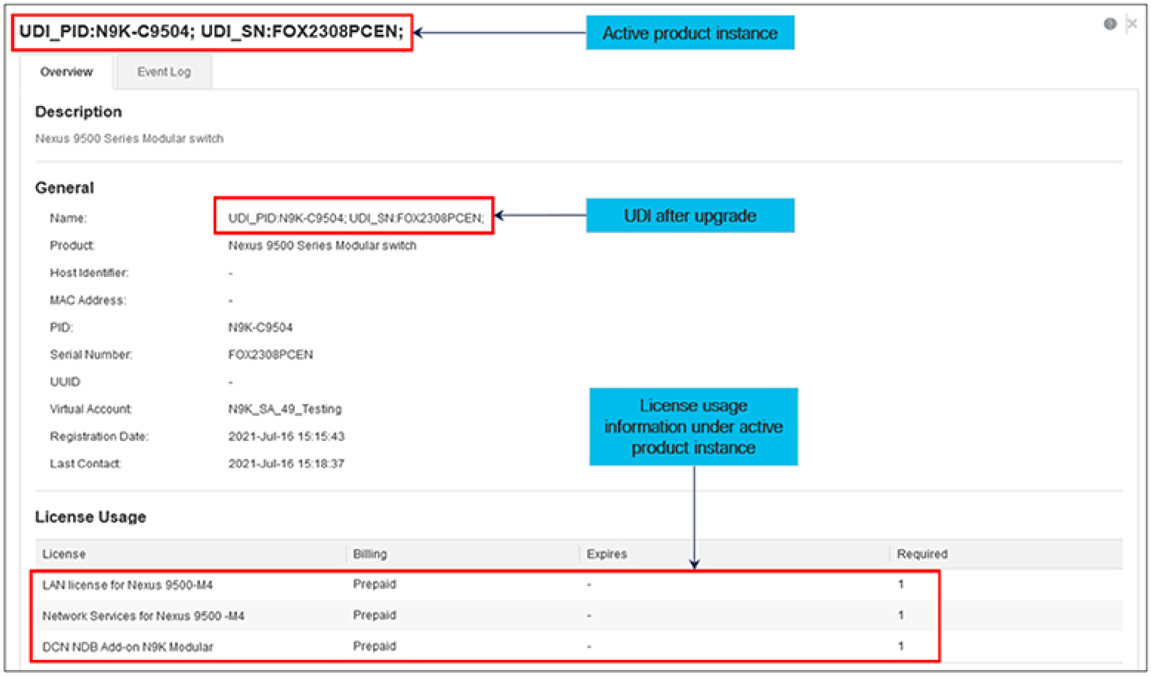
Authorize License-Enforced Features...

2308PCEN

Name	Product Type	Last Contact	Alerts	Actions
UDI_PID:N9K-C9504; UDI_SN:FOX2308PCEN;	N9500	2021-Jul-16 15:18:37		Actions

Showing 1 Record

Figure 9: Smart Licensing to Smart Licensing Using Policy: UDI and License Usage under Active Product Instance



UDI_PID:N9K-C9504; UDI_SN:FOX2308PCEN;

Active product instance

Overview | Event Log

Description

Nexus 9500 Series Modular switch

General

Name:	UDI_PID:N9K-C9504; UDI_SN:FOX2308PCEN;
Product:	Nexus 9500 Series Modular switch
Host Identifier:	-
MAC Address:	-
PID:	N9K-C9504
Serial Number:	FOX2308PCEN
UUID	-
Virtual Account:	N9K_SA_49_Testing
Registration Date:	2021-Jul-16 15:15:43
Last Contact:	2021-Jul-16 15:18:37

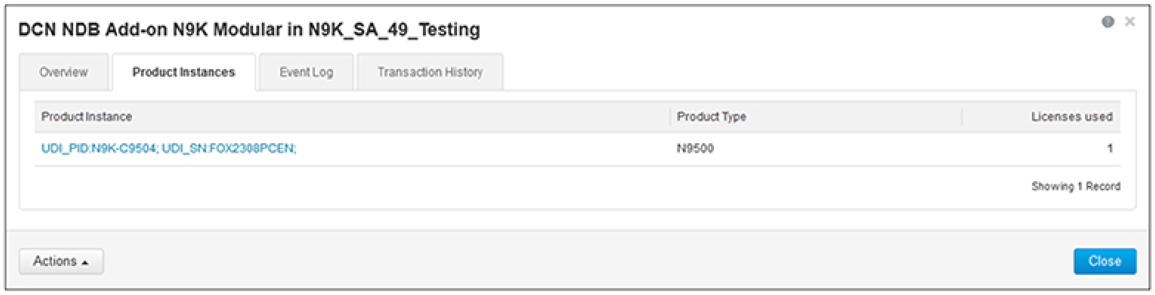
UDI after upgrade

License usage information under active product instance

License Usage

License	Billing	Expires	Required
LAN license for Nexus 9500-M4	Prepaid	-	1
Network Services for Nexus 9500 -M4	Prepaid	-	1
DCN NDB Add-on N9K Modular	Prepaid	-	1

Figure 10: Smart Licensing to Smart Licensing Using Policy: DCN NDB/RTU Licenses Showing up After Upgrade



DCN NDB Add-on N9K Modular in N9K_SA_49_Testing

Product Instance	Product Type	Licenses used
UDI_PID:N9K-C9504; UDI_SN:FOX2308PCEN;	N9500	1

Showing 1 Record

Reporting After Migration

The product instance sends the next RUM report to CSSM, based on the policy.

If you want to change your reporting interval to report more frequently: on the product instance, configure the **license smart usage interval** command. For syntax details see the **license smart (global config)** command in the Command Reference for the corresponding release.

RTU Licensing to Smart Licensing Using Policy

This section provides information about migrating a Cisco Nexus 9000 Series switch from Right-to-Use (RTU) licensing to Smart Licensing Using Policy.

RTU Licensing is available for Cisco Nexus 9000 Series Switches until Cisco NX-OS Release 10.1(2), and SLP is introduced from Cisco NX-OS Release 10.2(1)F.

When the software version is upgraded from a pre-SLP version to the SLP version, all licenses are displayed as IN USE and the Cisco default policy is applied on the product instance. If any add-on licenses are used, the Cisco default policy requires usage reporting in 90 days. As all licenses on Cisco Nexus Switches are unenforced, no functionality is lost.

RTU Licensing to SLP Migration - Feature TAP Aggregation

In a scenario where a Cisco Nexus 9000 Series switch is migrated from a pre-SLP to an SLP-supported release, an NDB license, which is the only RTU license, cannot be consumed unless ACL is configured as below in the pre-SLP release. This is equivalent of the consumption of NDB RTU license in pre-SLP release.

A sample configuration for pre-SLP release is as follows:

```
switch# config
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# ip access-list iptest
switch(config-acl)# permit ip any any redirect Ethernet1/1
switch(config-acl)#
```

A sample show command output after ACL configuration for a pre-SLP release is as follows:

sh ip access-lists iptest

```
IP access list iptest
10 permit ip any any redirect Ethernet1/1
```

A sample show command output for license verification after upgrading to an SLP-supported release is as follows and the show feature command shows that the feature tap-aggregation is enabled, and NDB license is consumed:

show license usage

```
Device# show license usage
License Authorization:
  Status: Not Applicable
(DCN_NDB):
  Description: DCN NDB Add-On License N9K Modular
  Count: 1
  Version: 1.0
  Status: IN USE
  Enforcement Type: NOT ENFORCED
  License Type: Generic
```

show feature

```
sh feature | inc tap
tap-aggregation        1          enabled
```

> **Note** Beginning with Cisco NX-OS Release 10.2(1)F, feature tap-aggregation is licensed, supported on all Cisco Nexus 9000 Series switches, and requires you to configure feature tap-aggregation before configuring related commands.

CSSM Web UI After Migration

No changes in the CSSM Web UI.

Reporting After Migration

Implement any one of the supported topologies and fulfil reporting requirements. SeeSupported Topologies, on page 17 and Configuring Smart Licensing Using Policy, on page 17. The reporting method you can use depends on the topology you implement.

Evaluation or Eval Expired to Smart Licensing Using Policy

The following is an example of a Cisco Nexus 9000 switch with evaluation licenses (Smart Licensing) that are migrated to SLP.

The notion of evaluation licenses does not apply to SLP. When the software version is upgraded to one that supports SLP, all licenses are displayed as IN USE and the Cisco default policy is applied to the product instance. Since all licenses on Cisco Nexus Switches are unenforced, no functionality is lost.

The table below calls out key changes or new fields to check for in the show command outputs, after upgrade to SLP:

Table 5: Evaluation or Eval Expired to Smart Licensing Using Policy: show Commands

Before Upgrade	After Upgrade

PGBL-FX2-203(config)# show license usage
`License Authorization:`
`  Status: EVAL MODE`
`  Evaluation Period Remaining: 86 days, 11 hours, 49 minutes, 40 seconds`
 	
`(LAN_ENTERPRISE_SERVICES_PKG):`
`  Description: <empty>`
`  Count: 1`
`  Version: 1.0`
`  Status: EVAL MODE`
 	
`(NETWORK_SERVICES_PKG):`
`  Description: <empty>`
`  Count: 1`
`  Version: 1.0`
`  Status: EVAL MODE`
 	
`(VPN_FABRIC):`
`  Description: <empty>`
`  Count: 1`
`  Version: 1.0`
`  Status: EVAL MODE`
	PGBL-FX2-203# show license usage
	`License Authorization:`
	`  Status: Not Applicable`
	
	`(NETWORK_SERVICES_PKG):`
	`  Description: Network Services for Nexus9300-XF`
	`  Count: 1`
	`  Version: 1.0`
	`    `**`Status: IN USE`**`    Enforcement Type: NOT ENFORCED`
	`  License Type: Generic`
	
	`(VPN_FABRIC):`
	`  Description: FAB License for Nexus 9300-XF`
	`  Count: 1`
	`  Version: 1.0`
	`    `**`Status: IN USE`**
	`    Enforcement Type: NOT ENFORCED`
	`  License Type: Generic`
	
	`(LAN_ENTERPRISE_SERVICES_PKG):`
	`  Description: LAN license for Nexus 9300-XF`
	`  Count: 1`
	`  Version: 1.0`
	`  `**`Status: IN USE`**`   Enforcement Type: NOT ENFORCED`
	`  License Type: Generic`

<table>
<tr><th>Before Upgrade</th><th>After Upgrade</th></tr>
<tr><td>

PGBL-FX2-203(config)# show license summary

```
Registration:
  Status: UNREGISTERED
  Smart Account: VDANI-ON-PREM-004
  Virtual Account: Default
  Export-Controlled Functionality: Allowed

License Authorization:
  Status: EVAL MODE
  Evaluation Period Remaining: 86 days, 11
hours, 49 minutes, 6 seconds

Smart License Conversion:
  Automatic Conversion Enabled: False
  Status: Successful on Aug 13 17:19:07 2021
 UTC

License Usage:
License                    Entitlement tag
               Count   Status
---------------------------------------------
<empty>
(LAN_ENTERPRISE_SERVICES_PKG)    1       EVAL
 MODE
<empty>
(NETWORK_SERVICES_PKG)           1       EVAL
 MODE
<empty>                    (VPN_FABRIC)
                1       EVAL MODE
```

</td><td>

PGBL-FX2-203# show license summary

```
License Usage:
License                    Entitlement tag
               Count   Status
---------------------------------------------
Network Services for Ne...
(NETWORK_SERVICES_PKG)           1        IN
USE
FAB License for Nexus 9... (VPN_FABRIC)
                1       IN USE
LAN license for Nexus 9...
(LAN_ENTERPRISE_SERVICES_PKG)    1        IN
USE
```

</td></tr>
</table>

<table>
<tr><th>Before Upgrade</th><th>After Upgrade</th></tr>
<tr><td>

PGBL-FX2-203(config)# show license status

<pre>
Smart Licensing is ENABLED

Registration:
  Status: UNREGISTERED
  Smart Account: VDANI-ON-PREM-004
  Virtual Account: Default
  Export-Controlled Functionality: Allowed

License Authorization:
  Status: EVAL MODE
  Evaluation Period Remaining: 86 days, 11
hours, 49 minutes, 3 seconds

Smart License Conversion:
  Automatic Conversion Enabled: False
  Status: Successful on Aug 13 17:19:07 2021
 UTC
</pre>

</td><td>

PGBL-FX2-203# show license status

<pre>
Utility:
    Status: DISABLED

Smart Licensing using Policy:
    Status: ENABLED

Data Privacy:
    Sending Hostname: yes
    Callhome Hostname Privacy: DISABLED
        Smart Licensing Hostname Privacy:
DISABLED
    Version Privacy: DISABLED

Transport:
    Type: CSLU
    Cslu address: cslu-local
Policy:
    Policy in use: Merged from multiple
sources
    Reporting ACK required: Yes
    Unenforced/Non-Export:
        First report requirement (days): 90
(CISCO default)
        Ongoing reporting frequency (days):
365 (CISCO default)
        On change reporting (days): 90 (CISCO
 default)
    Enforced (Perpetual/Subscription):
        First report requirement (days): 0
(CISCO default)
        Ongoing reporting frequency (days):
0 (CISCO default)
        On change reporting (days): 0 (CISCO
 default)
    Export (Perpetual/Subscription):
        First report requirement (days): 0
(CISCO default)
        Ongoing reporting frequency (days):
0 (CISCO default)
        On change reporting (days): 0 (CISCO
 default)

Miscellaneous:
    Custom Id: <empty>

Usage reporting:
    Last ACK received: <none>
    Next ACK deadline: Nov 16 09:38:37 2021
UTC
    Reporting push interval: 30 days
    Next ACK push check: <none>
    Next report push: Aug 18 09:39:14 2021
UTC
    Last report push: <none>
    Last report file write: <none>

Trust Code installed: <none>
</pre>

</td></tr>
</table>

CSSM Web UI After Migration

No changes in the CSSM Web UI.

Reporting After Migration

Implement any one of the supported topologies and fulfill reporting requirements. See Supported Topologies, on page 17 and Configuring Smart Licensing Using Policy, on page 17. The reporting method that you can use depends on the topology you implement.

CHAPTER 7

Troubleshooting Smart Licensing Using Policy

This chapter provides step-by-step instructions to resolve SLP issues on Nexus switches.

The first section covers common problems related to connectivity of switch to CSSM, along with their respective solutions.

The second section provides the list of SLP-related system messages you may encounter, possible reasons for failure, and recommended action.

Resolving SLP Issues on Nexus Switches

This section provides information about common problems related to connectivity of switch to CSSM and their resolution.

The following issues are covered in this section:

- Issue: Trust code installation failed
- Issue: Smart Licensing communication with CSSM/CSLU/SSM On-Prem failed
- Issue: Failed to send usage Report
- Issue: Failed to receive Report Acknowledgment

Issue: Trust code installation failed

Possible reasons for failure include:

- A trust code is already installed: Trust codes are linked to the **Unique Device Identifier** (UDI) of the product instance. If the UDI is already registered, and you try to install another one, installation fails.
- Timestamp mismatch: This means the product instance time is not in sync with **Cisco Smart Software Manager** (CSSM), and can cause installation to fail.

Recommended Action:

- A trust code is already installed: If you want to install a trust code in spite of an existing trust code on the product instance, re-configure the **license smart trust idtoken** *id_token_value* [**force**] command in privileged EXEC mode, and be sure to include the **force** keyword. Entering the **force** keyword asks CSSM to create a new trust code even if it exists already.

- Timestamp mismatch: Configure the **ntp server** command in global configuration mode. For example:

  switch (config)# **ntp server 10.28.13.90 prefer**

Note If there is a difference in time between device and CSSM then it should be less than one hour.

Issue: Smart Licensing communication with CSSM/CSLU/SSM On-Prem failed

Possible reasons for failure include:

- Missing DNS configurations.
- CSSM, CSLU, SSM On-Prem is not reachable: This means that there may be network problem.

Recommended Action for DNS:

Troubleshooting steps are provided for missing DNS configurations, when CSSM/CSLU/SSM On-Prem is not reachable.

- If ping to cisco.com in the configured vrf for SLP throws error **% Invalid host/interface <URL>**:

1. Execute the following commands from global configuration mode to configure DNS,

```
switch# config terminal
switch(config)# ip domain-lookup
switch(config)# ip domain-name cisco.com
switch(config)# ip name-server <dns-server-ip> use-vrf <vrf-name>
switch(config)# vrf context <vrf-name>
switch(config-vrf)# ip domain-name cisco.com
switch(config-vrf)# ip name-server <dns-server-ip>
```

2. Check if ping to cisco.com is working or not, using **vrf** <*vrf-name*>. The following example shows working DNS scenario:

```
switch(config)# ping cisco.com vrf <vrf-name>
PING cisco.com (<ip-address>): 56 data bytes
64 bytes from <ip-address>: icmp_seq=0 ttl=236 time=242.279 ms
64 bytes from <ip-address>: icmp_seq=1 ttl=236 time=242.108 ms
64 bytes from <ip-address>: icmp_seq=2 ttl=236 time=242.032 ms
64 bytes from <ip-address>: icmp_seq=3 ttl=236 time=242.278 ms
64 bytes from <ip-address>: icmp_seq=4 ttl=236 time=241.968 ms
--- cisco.com ping statistics ---
5 packets transmitted, 5 packets received, 0.00% packet loss
round-trip min/avg/max = 241.968/242.133/242.279 ms
```

Note For transport mode CSLU, either configure **ip host cslu-local** <*cslu_address*> or cslu-local should be part of DNS server. For SSM On-Prem, the URL configured in switch should be **Fully Qualified Domain Name** (FQDN) and not the ip-address.

Recommended Action for Network Reachability:

- If the configured transport mode is **smart** transport:

  1. In the **show license status** command output, under the **Transport:** header, check the following:

     a. **Type:** must be **Smart** and

     b. **URL:** must be https://smartreceiver.cisco.com/licservice/license. For example,

        Transport:

        Type: Smart

        URL: https://smartreceiver.cisco.com/licservice/license

        Proxy:

        Not configured

        VRF: <*vrf-name*>

     If it is not, configure using the **license smart transport smart** and **license smart url smart** https://smartreceiver.cisco.com/licservice/license commands in global configuration mode.

  2. Check DNS resolution. Verify that the URL https://smartreceiver.cisco.com/licservice/license is reachable through the browser. The following example shows reachability for the smart URL.

     ```
     This is the Smart Receiver!

     Environment Information:
       cisco.life = prod
       License Engine = https://swapi.cisco.com/software/csws/ssm/services
       License EngineSLE = https://swapi.cisco.com/software/csws/ssm/v2/services
       License Crypto Service = https://lcs.cisco.com/LCS
       Crypto Enabled = true
       Retry Enabled = true
       Retry Timeout = 55000
       Rate Limit Window Length = 3600
       Rate Limit Max Allowed in Window = 12
     ```

  Optionally, you can ping smart URL (https://smartreceiver.cisco.com/licservice/license) and verify.

  Example:

  ```
  bash-4.4$ ping smartreceiver.cisco.com
  PING smartreceiver.cisco.com (<ip-address>) 56(84) bytes of data.
  64 bytes from <ip-address> (<ip-address>): icmp_seq=1 ttl=53 time=2.57 ms
  64 bytes from <ip-address> (<ip-address>): icmp_seq=2 ttl=53 time=2.79 ms
  64 bytes from <ip-address> (<ip-address>): icmp _seq=3 ttl=53 time=2.54 ms
  64 bytes from <ip-address> (<ip-address>): icmp_seq=4 ttl=53 time=2.43 ms
  64 bytes from <ip-address> (<ip-address>): icmp_seq=5 ttl=53 time=3.23 ms
  64 bytes from <ip-address> (<ip-address>): icmp_seq=6 ttl=53 time=2.100 ms
  ^C
  --- smartreceiver.cisco.com ping statistics ---
  6 packets transmitted, 6 received, 0% packet loss, time 5009ms
  rtt min/avg/max/mdev = 2.429/2.757/3.231/0.289 ms
  bash-4.4$
  ```

- If the configured transport mode is **cslu**:

  1. In the **show license status** command output, under the **Transport:** header, check the following:

     a. **Type:** must be CSLU and

b. **Cslu address:** must be cslu-local

Example

Transport:

Type: CSLU

Cslu address: cslu-local

VRF: <*vrf-name*>

If it is not, configure using the **license smart transport cslu** and **license smart url cslu** <*cslu-local-url*> commands in global configuration mode.

2. Check DNS resolution. Verify that the configured cslu-local-url is reachable through the browser.

- If the configured transport mode is callhome:

1. In the **show license status** command output, under the **Transport:** header, check the following:

   - **Type:** must be Callhome.

     For example,

     Transport:

     Type: Callhome

     If it is not, configure using the **license smart transport callhome** commands in global configuration mode.

2. Check if callhome is configured correctly. Use the **show running-config callhome all** command in privileged EXEC mode, to check callhome configuration as follows:

```
switch(config)# show running-config callhome all
!Command: show running-config callhome all
!Running configuration last done at: Thu Aug  3 20:38:37 2023
!Time: Thu Aug  3 20:43:58 2023
version 10.3(1) Bios:version 05.45
callhome
  email-contact <email-address>
  destination-profile xml transport-method http
  destination-profile xml index 1 email-addr <email-address>
  destination-profile xml index 1 http
https://tools.cisco.com/its/service/oddce/services/DDCEService
  transport email smtp-server <ip-address> port <port-number>
  transport email from <email-address>
  transport email reply-to <email-address>
  transport http use-vrf <vrf-name>
  enable
  periodic-inventory notification interval 1
```

3. Check DNS Resolution. Verify that the product instance can ping tools.cisco.com through configured vrf using the **ping tools.cisco.com vrf** <vrf-name> command.

Example

```
switch(config) # ping tools.cisco.com vrf <vrf-name>
PING tools.cisco.com (<ip-address>): 56 data bytes
64 bytes from <ip-address>: icmp_seq=0 ttl=236 time=244.692 ms
64 bytes from <ip-address>: icmp_seq=1 ttl=236 time=244.532 ms
64 bytes from <ip-address>: icmp_seq=2 ttl=236 time=244.396 ms.
```

```
64 bytes from <ip-address>: icmp_seq=3 ttl=236 time=244.502 ms.
64 bytes from <ip-address>: icmp_seq=4 ttl=236 time=244.607 ms

-- tools.cisco.com ping statistics ---
5 packets transmitted, 5 packets received, 0.00% packet loss
round-trip min/avg/max = 244.396/244.545/244.692 ms.
switch(config)#
```

You can also ping directly to the callhome URL tools.cisco.com.

Example

```
bash-4.4$ ping tools.cisco.com
PING tools.cisco.com (<ip-address>) 56(84) bytes of data.
64 bytes from tools2.cisco.com (<ip-address>): icmp_seq=1 ttl=242 time=43.7 ms
64 bytes from tools2.cisco.com (<ip-address>): icmp_seq=2 ttl=242 time=43.7 ms
64 bytes from tools2.cisco.com (<ip-address>): icmp_seq=3 ttl=242 time=43.7 ms
64 bytes from tools2.cisco.com (<ip-address>): icmp_seq=4 ttl=242 time=43.8 ms
64 bytes from tools2.cisco.com (<ip-address>): icmp_seq=5 ttl=242 time=43.8 ms
64 bytes from tools2.cisco.com (<ip-address>): icmp_seq=6 ttl=242 time=43.7 ms
^C
--- tools.cisco.com ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5009ms
rtt min/avg/max/mdev = 43.656/43.703/43.770/0.214 ms
bash-4.4$
```

Issue: Failed to send usage Report

Possible reasons for failure include:

- Because of a communication failure, the product instance failed to send the RUM report.

Recommended Action:

- Check if the RUM report is due any time soon using the **show license tech support** command. If not, and the problem is with a server or link that is down, you can try again after some time.
- If the communication failure persists, check if the transport type and URL have been set as required by the topology.

Issue: Failed to receive Report Acknowledgment

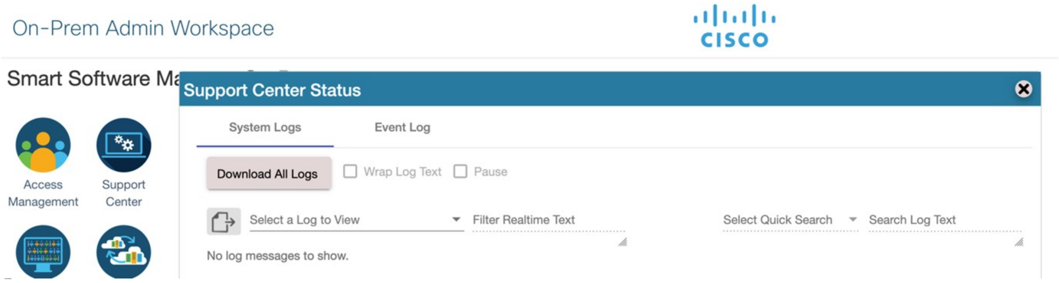
Possible reasons for failure include:

- Connectivity problems. Depending on the implemented topology, this can mean a connectivity problem with CSSM, or CSLU, or SSM On-Prem.
- Delayed communication. There may be a lag between the time that a RUM Report is sent and the RUM acknowledgment (ACK) is available on the product instance. For example, if you use CSLU or SSM On-Prem, the time at which the product instance receives information depends on when CSLU or SSM On-Prem is scheduled to synchronize with CSSM and with the product instance. In direct connectivity mode, acknowledgment takes around 15 minutes to be updated on the switch.
- The ACK received can fail, if the product instance (switch) was previously registered with a different On-Prem account.

  Recommended Action:

  To troubleshoot this issue, perform the following steps:

1. Navigate to **On-Prem Admin Workspace** > **Support Center**. The **Support Center Status** window opens.
2. In the **Support Center Status** window, click the **System Logs** tab and click **Download All Logs**. After a few seconds, a dialog window opens to save the zip file.
3. Save the **AllFiles.zip** file.
4. Extract the **AllFiles.zip**



No log messages to show.

5. Check for the following symptoms inside the file named **messages** and search for the error: "**failed due to the following error: record not found.**" For example,

```
Aug 7 17:02:36 rtp-dcrs-licensing cf881d42a1b7: 2023/08/07
 17:02:36#011[ERROR]#011adapters/pi_routes_impl.go:1322#011
 Finding SL product by UDI {<switch> FDO212100YT} failed due to the following error:
 record not found.
```

6. It is also possible that the CSSM does not have the product instance but On-Prem has the product instance.

Recommended Action:

1. Ensure that the trust code is installed.
2. When the trust code is installed, check for **Usage reporting:** in **show license status** to know whether the report is synced or not. The **Next report push** field displays the following information about the synchronization:

```
Usage reporting:
         Last ACK received: <none>
         Next ACK deadline: <none>
         Reporting push interval: <none>
         Next ACK push check: <none>
         Next report push: <none>
         Last report push: <none>
         Last report file write: <none>
Trust Code installed: Jul 14 11:40:36 2023 UTC
         Active: PID: <device_pid>, SN: <device_sn>
                 Jul 14 11:40:36 2023 UTC
```

3. If the synchronization does not take place automatically, then initiate an on-demand synchronization based on the implemented topology as follows:
   - For online topologies, use the **license smart sync** command in privileged EXEC mode. If SSM On-Prem is used in topology, then, additionally, sync to Cisco as well as the switch on SSM On-Prem.
   - For offline topologies, upload the RUM report to CSSM and install the ACK back on the switch.

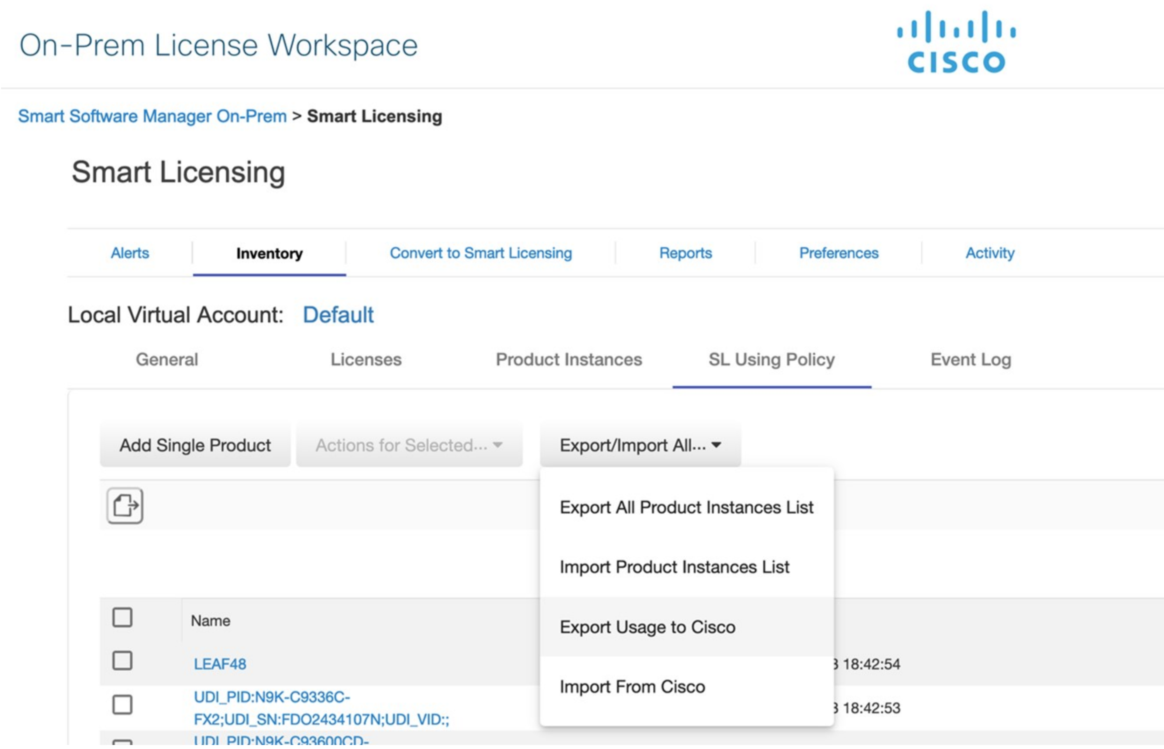
4. After the sync is completed, wait for 15 minutes to receive acknowledgment for the CSSM.

5. Perform On-Prem Report Synchronization out-of-band (**Export/Import Cisco Usage Report/ACK**) if acknowledgment fails due to already registered device reason on On-Prem.

   a. On the On-Prem server, navigate to **Smart Software Manager On-Prem** > **Smart Licensing** > **Inventory** > **SL Using Policy**.

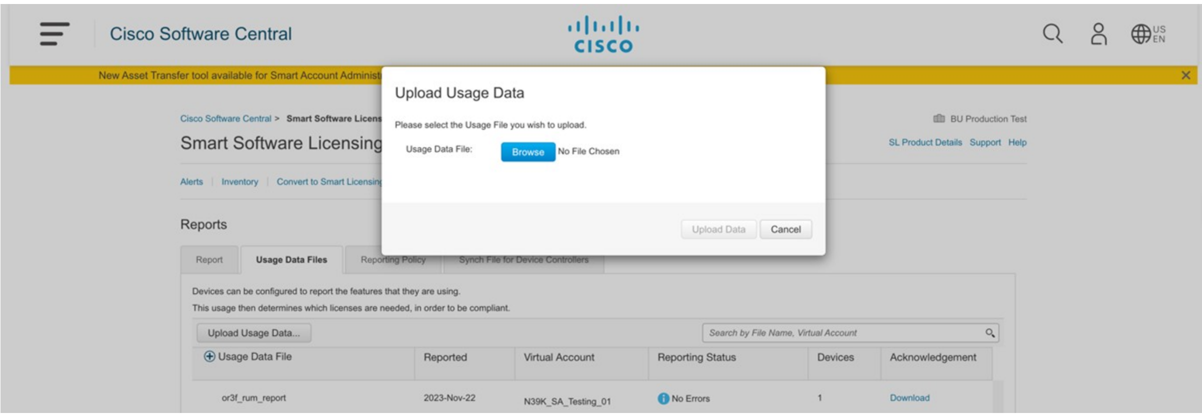
      Then, select the product names for which you require the acknowledgment.

      Next, from the **Export/Import All** drop-down menu, select **Export Usage to Cisco** and download the exported report onto your system.



□	Name	
□	LEAF48	3 18:42:54
□	UDI_PID:N9K-C9336C-FX2;UDI_SN:FDO2434107N;UDI_VID:;	3 18:42:53
□	UDI_PID:N9K-C93600CD-	

   b. To upload the downloaded report and generate the ACK report, go to the respective CSSM On-Prem account and navigate to **Reports** > **Usage Data Files** > **Upload Usage Data File**. Click the **Upload Usage Data** button. The **Upload Usage Data** dialog box opens.


Cisco Software Central
cisco
US EN
New Asset Transfer tool available for Smart Account Administ
Cisco Software Central > Smart Software Licens
Smart Software Licensing
BU Production Test
SL Product Details Support Help
Alerts | Inventory | Convert to Smart Licensing
Reports
Report
Usage Data Files
Reporting Policy
Synch File for Device Controllers
Upload Usage Data...
Search by File Name, Virtual Account
Upload Usage Data
Usage Data File:
Browse
No File Chosen
Upload Data
Cancel

Please select the Usage File you wish to upload.

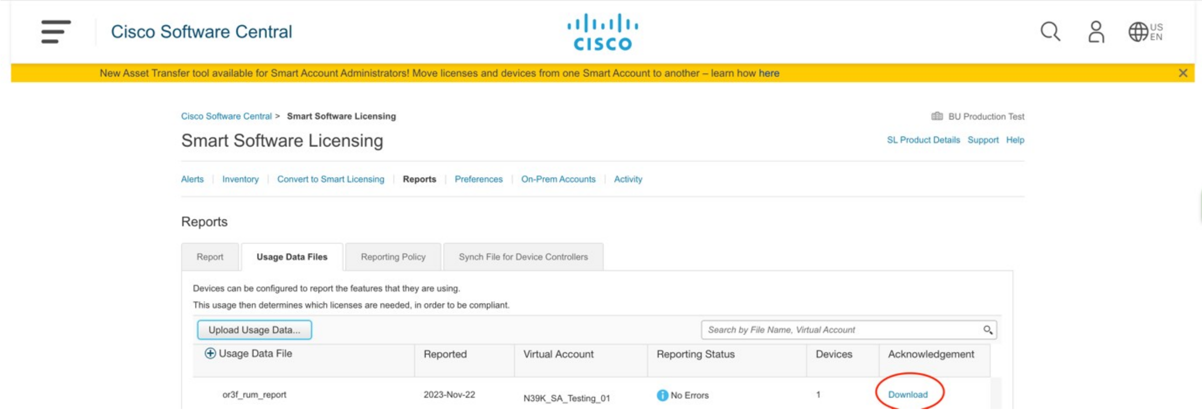
Devices can be configured to report the features that they are using.
This usage then determines which licenses are needed, in order to be compliant.

Usage Data File	Reported	Virtual Account	Reporting Status	Devices	Acknowledgement
or3f_rum_report	2023-Nov-22	N39K_SA_Testing_01	No Errors	1	Download

c. In the **Upload Usage Data** dialog box, click the **Browse** button and select the report from your system (downloaded earlier) that you want to upload and then click the **Upload Data** button.

Wait for a while as it takes some time to process. Ignore the errors that appear, if any. The file is uploaded to the **Usage Data Files** tab.

d. To download the ACK report for the uploaded Usage Data File, select the file and click the **Download** link in the **Acknowledgment** column.


Cisco Software Central
cisco
US EN
Cisco Software Central > Smart Software Licensing
Smart Software Licensing
BU Production Test
SL Product Details Support Help
Alerts | Inventory | Convert to Smart Licensing | Reports | Preferences | On-Prem Accounts | Activity
Reports
Report
Usage Data Files
Reporting Policy
Synch File for Device Controllers
Upload Usage Data...
Search by File Name, Virtual Account

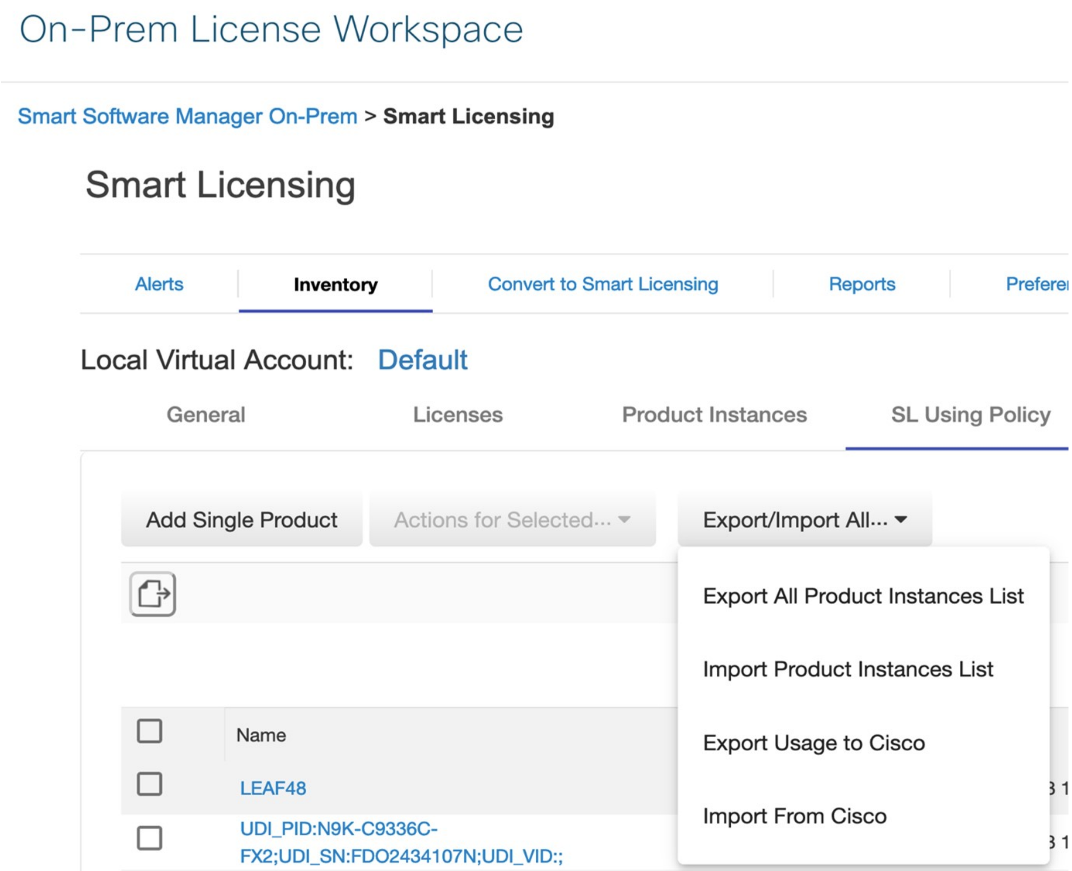
New Asset Transfer tool available for Smart Account Administrators! Move licenses and devices from one Smart Account to another – learn how here

Devices can be configured to report the features that they are using.
This usage then determines which licenses are needed, in order to be compliant.

Usage Data File	Reported	Virtual Account	Reporting Status	Devices	Acknowledgement
or3f_rum_report	2023-Nov-22	N39K_SA_Testing_01	No Errors	1	Download

e. Upload the downloaded ACK file to On-Prem. To do so, navigate to **Smart Software Manager On-Prem** > **Smart Licensing** > **Inventory** > **SL Using Policy**.

Then, from the **Export/Import All** drop-down menu, select **Import From Cisco** and upload the downloaded acknowledgment report.


On-Prem License Workspace
Smart Software Manager On-Prem > Smart Licensing
Smart Licensing
Alerts
Inventory
Convert to Smart Licensing
Reports
Prefere
Local Virtual Account: Default
General
Licenses
Product Instances
SL Using Policy
Add Single Product
Actions for Selected...
Export/Import All...
Export All Product Instances List
Import Product Instances List
Export Usage to Cisco
Import From Cisco

□	Name
□	LEAF48
□	UDI_PID:N9K-C9336C-FX2;UDI_SN:FDO2434107N;UDI_VID:;

f. After the report is uploaded, the respective devices reflect the received acknowledgment status.

Note Not receiving acknowledgment does not affect any function of the switch. You can receive syslog for not reporting, if the reporting period is expired or near to expiry as per the configured policy. If you do not receive an acknowledgment, you can contact the Cisco technical support representative.

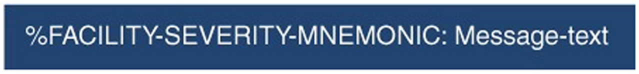
System Message Overview

The system software sends system messages to the console (and, optionally, to a logging server on another system). Not all system messages mean problems with your system. Some messages are informational, and others can help diagnose problems with communications lines, internal hardware, or the system software.

How to Read System Messages

System log messages can contain up to 80 characters. Each system message begins with a percent sign (%) and is structured as follows:

Figure 11:



%FACILITY-SEVERITY-MNEMONIC: Message-text

%FACILITY

Two or more uppercase letters that show the facility to which the message refers. A facility can be a hardware device, a protocol, or a module of the system software.

SEVERITY

A single-digit code from 0 to 7 that reflects the severity of the condition. The lower the number, the more serious the situation.

Table 6: Message Severity Levels

Severity Level	Description
0 – emergency	System is unusable.
1 – alert	Immediate action required.
2 – critical	Critical condition.
3 – error	Error condition.
4 – warning	Warning condition.
5 – notification	Normal but significant condition.
6 – informational	Informational message only.
7 - debugging	Message that appears during debugging only.

MNEMONIC

A code that uniquely identifies the message.

Message-text

Message-text is a text string describing the condition. This portion of the message sometimes contains detailed information about the event, including terminal port numbers, network addresses, or addresses that correspond to locations in the system memory address space. Because the information in these variable fields changes from message to message, it is represented here by short strings enclosed in square brackets ([ ]). A decimal number, for example, is represented as [dec].

Table 7: Variable Fields in Messages

Severity Level	Description
[char]	Single character
[chars]	Character string
[dec]	Decimal number
[enet]	Ethernet address (for example, 0000.FEED.00C0)
[hex]	Hexadecimal number

Severity Level	Description
[inet]	Internet address (for example, 10.0.2.16)
[int]	Integer
[node]	Address or node name
[t-line]	Terminalline number in octal (or in decimal if the decimal-TTY service is enabled)
[clock]	Clock (for example, 01:20:08 UTC Tue Mar 2 1993

System Messages

This section provides the list of SLP-related system messages you may encounter, possible reasons for failure (in case it is a failure message), and recommended action (if action is required).

For all error messages, if you are not able to solve the problem, contact your Cisco technical support representative with the following information:

- The message, exactly as it appears on the console or in the system log.
- The output from the show license tech support and show license history message commands.

SLP-related system messages:

- %LICMGR-3-LOG_SMART_LIC_POLICY_INSTALL_FAILED
- %LICMGR-3-LOG_SMART_LIC_AUTHORIZATION_INSTALL_FAILED
- %LICMGR-3-LOG_SMART_LIC_COMM_FAILED
- %LICMGR-3-LOG_SMART_LIC_COMM_RESTORED
- %LICMGR-3-LOG_SMART_LIC_POLICY_REMOVED
- %LICMGR-3-LOG_SMART_LIC_TRUST_CODE_INSTALL_FAILED
- %LICMGR-4-LOG_SMART_LIC_REPORTING_NOT_SUPPORTED
- %LICMGR-6-LOG_SMART_LIC_POLICY_INSTALL_SUCCESS
- %LICMGR-6-LOG_SMART_LIC_AUTHORIZATION_INSTALL_SUCCESS
- %LICMGR-6-LOG_SMART_LIC_AUTHORIZATION_REMOVED
- %LICMGR-6-LOG_SMART_LIC_REPORTING_REQUIRED
- %LICMGR-6-LOG_SMART_LIC_TRUST_CODE_INSTALL_SUCCESS

```
Error Message %LICMGR-3-LOG_SMART_LIC_POLICY_INSTALL_FAILED: The
installation of a new licensing policy has failed: [chars].
```

Explanation: A policy was installed, but an error was detected while parsing the policy code, and installation failed. [chars] is the error string with details of the failure.

Possible reasons for failure include:

- A signature mismatch: This means that the system clock is not accurate.
- A timestamp mismatch: This means the system clock on the product instance is not synchronized with CSSM.

Recommended Action:

For both possible failure reasons, ensure that the system clock is accurate and synchronized with CSSM. Configure the ntp server command in global configuration mode. For example:

Device(config)# **ntp server 198.51.100.100 version 2 prefer**

If the above does not work and policy installation still fails, contact your Cisco technical support representative.

```
-----------------------------------------------------------------------------------------
-----------------------------------------------------------------------------------------
```

```
Error Message %LICMGR-3-LOG_SMART_LIC_AUTHORIZATION_INSTALL_FAILED: The
install of a new licensing authorization code has failed on [chars]:
[chars].
```

This message is not applicable to Cisco Nexus Switches, because there are no enforced or export-controlled licenses on these product instances.

```
-----------------------------------------------------------------------------------------
-----------------------------------------------------------------------------------------
```

```
Error Message %LICMGR-3-LOG_SMART_LIC_COMM_FAILED: Communications failure
with the [chars] : [chars]
```

Explanation: Smart Licensing communication either with CSSM or with CSLU failed. The first [chars] is the currently configured transport type, and the second [chars] is the error string with details of the failure. This message appears for every communication attempt that fails.

Possible reasons for failure include:

- CSSM or CSLU is not reachable: This means that there is a network reachability problem.
- 404 host not found: This means that the CSSM server is down.

For topologies where the product instance initiates the sending of RUM reports (Connected to CSSM Through CSLU: Product Instance-Initiated Communication, Connected Directly to CSSM, and CSLU Disconnected from CSSM: Product Instance-Initiated Communication) if this communication failure message coincides with scheduled reporting (**license smart usage interval** `interval_in_days` global configuration command), the product instance attempts to send out the RUM report for up to four hours after the scheduled time has expired. If it is still unable to send out the report (because the communication failure persists), the system resets the interval to 15 minutes. Once the communication failure is resolved, the system reverts the reporting interval to the value that you last configured.

Recommended Action:

Troubleshooting steps are provided for when CSSM is not reachable and when CSLU is not reachable. If CSSM is not reachable and the configured transport type is smart:

1. Check if the smart URL is configured correctly. Use the **show license status** command in privileged EXEC mode, to check if the URL is exactly as follows: https://smartreceiver.cisco.com/licservice/license. If it is not, reconfigure the **license smart url smart** `smart_URL` command in global configuration mode.

2. Check DNS resolution. Verify that the product instance can ping smartreceiver.cisco.com or the nslookup translated IP. The following example shows how to ping the translated IP:

   ```
   Device# ping 171.70.168.183 Type escape sequence to abort.
   Sending 5, 100-byte ICMP Echos to 171.70.168.183, timeout is 2 seconds:
   !!!!!
   Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms
   ```

If CSSM is not reachable and the configured transport type is **callhome**:

1. Check if the URL is entered correctly. Use the **show license status** command in privileged EXEC mode, to check if the URL is exactly as follows: https://tools.cisco.com/its/service/oddce/services/DDCEService.

2. Check if Call Home profile **CiscoTAC-1** is active and destination URL is correct. Use the **show call-home profile all** command in privileged EXEC mode:

   ```
   Current smart-licensing transport settings: Smart-license messages: enabled
   Profile: CiscoTAC-1 (status: ACTIVE)
   Destination  URL(s): https://tools.cisco.com/its/service/oddce/services/DDCEService
   ```

3. Check DNS Resolution. Verify that the product instance can ping tools.cisco.com, or the nslookup translated IP.

   ```
   Device# ping tools.cisco.com Type escape sequence to abort.
   Sending 5, 100-byte ICMP Echos to 173.37.145.8, timeout is 2 seconds:
   !!!!!
   Success rate is 100 percent (5/5), round-trip min/avg/max = 41/41/42 ms
   ```

   If the above does not work check the following: if the product instance is set, if the product instance IP network is up. To ensure that the network is up, configure the **no shutdown** command in interface configuration mode.

   Check if the device is subnet that is masked with a subnet IP, and if the DNS IP is configured.

4. Verify that the HTTPs client source interface is correct.

   Use the **show ip http client** command in privileged EXEC mode to display current configuration. Use **ip http client source-interface** command in global configuration mode to reconfigure it. In case the above does not work, double-check your routing rules, and firewall settings.

If CSLU is not reachable:

- Check if CSLU discovery works.

  - Zero-touch DNS discovery of cslu-local or DNS discovery of your domain.

    In the **show license all** command output, check if the Last ACK received: field. If this has a recent timestamp, it means that the product instance has connectivity with CSLU. If it is not, proceed with the following checks:

    Check if the product instance can ping **cslu-local**. A successful ping confirms that the product instance is reachable.

    If the above does not work, configure the name server with an entry where hostname **cslu-local** is mapped to the CSLU IP address (the Windows host where you installed CSLU). Configure the **ip domain name** domain-name and **ip name-server** server-address commands in global configuration mode. Here the CSLU IP is 192.168.0.1 and name-server creates entry **cslu-local.example.com**:

    ```
    Device(config)# ip domain name example.com
    ```

    ```
    Device(config)# ip name-server 192.168.0.1
    ```

- CSLU URL is configured.

  In the **show license all** command output, under the **Transport:** header check the following: The **Type:** must be **cslu** and **Cslu address:** must have the hostname or the IP address of the Windows host where you have installed CSLU. Check if the rest of the address is configured as shown below and check if the port number is 8182.

  ```
  Transport:
  Type: cslu
  Cslu address: http://192.168.0.1:8182/cslu/v1/pi
  ```

  If it is not, configure the **license smart transport cslu** and **license smart url cslu** *http://<cslu_ip_or_host>:8182/cslu/v1/pi* commands in global configuration mode.

If the above does not work and policy installation still fails, contact your Cisco technical support representative.

```
------------------------------------------------------------------------------------------
------------------------------------------------------------------------------------------
```

```
Error Message %LICMGR-3-LOG_SMART_LIC_COMM_RESTORED: Communications with the [chars] restored.
 [chars] - depends on the transport type
-  Cisco Smart Software Manager (CSSM)
-  Cisco Smart License utility (CSLU)
Smart Agent communication with either the Cisco Smart Software Manager (CSSM) or the Cisco
 Smart License
utility (CSLU) has been restored. No action required.
```

Explanation: Product instance communication with either the CSSM or CSLU is restored.

Recommended Action: No action required.

```
------------------------------------------------------------------------------------------
------------------------------------------------------------------------------------------
```

```
Error Message %LICMGR-3-LOG_SMART_LIC_POLICY_REMOVED: The licensing policy
has been removed.
```

Explanation: A previously installed licensing policy has been removed. The Cisco default policy is then automatically effective. This may cause a change in the behavior of smart licensing.

Possible reasons for failure include:

If you have entered the **license smart factory reset** command in privileged EXEC mode all licensing information including the policy is removed.

Recommended Action:

If the policy was removed intentionally, then no further action is required.

If the policy was removed inadvertently, you can reapply the policy. Depending on the topology you have implemented, follow the corresponding method to retrieve the policy:

- Connected Directly to CSSM:

  Enter **show license status**, and check field **Trust Code Installed:**. If trust is established, then CSSM will automatically return the policy again. The policy is automatically re-installed on product instances of the corresponding Virtual Account.

If trust has not been established, complete these tasks: Generating a New Token for a Trust Code from CSSM, on page 42 and Installing a Trust Code, on page 43. When you have completed these tasks, CSSM will automatically return the policy again. The policy is then automatically installed on all product instances of that Virtual Account.

- Connected to CSSM Through CSLU:
  - For product instance-initiated communication), enter the **license smart sync** command in privileged EXEC mode. The synchronization request causes CSLU to push the missing information (a policy or authorization code) to the product instance.

- CSLU Disconnected from CSSM:
  - For product instance-initiated communication), enter the **license smart sync** command in privileged EXEC mode. The synchronization request causes CSLU to push the missing information (a policy or authorization code) to the product instance. Then complete these tasks in the given order: **Download All For Cisco (CSLU Interface)** > Uploading Usage Data to CSSM and Downloading an ACK > **Upload From Cisco (CSLU Interface)**.

- No Connectivity to CSSM and No CSLU

  If you are in an entirely air-gapped network, from a workstation that has connectivity to the internet and CSSM complete this task: Downloading a Policy File from CSSM, on page 44.

  Then complete this task on the product instance: Installing a File on the Switch, on page 45.

```
-----------------------------------------------------------------------------------------
-----------------------------------------------------------------------------------------
```

```
Error Message %LICMGR-3-LOG_SMART_LIC_TRUST_CODE_INSTALL_FAILED: The
install of a new licensing trust code has failed on [chars]: [chars].
```

Explanation: Trust code installation has failed. The first [chars] is the UDI where trust code installation was attempted. The second [chars] is the error string with details of the failure.

Possible reasons for failure include:

- A trust code is already installed: Trust codes are node-locked to the UDI of the product instance. If the UDI is already registered, and you try to install another one, installation fails.
- Smart Account-Virtual Account mismatch: This means the Smart Account or Virtual Account (for which the token ID was generated) does not include the product instance on which you installed the trust code. The token generated in CSSM, applies at the Smart Account or Virtual Account level, and applies only to all product instances in that account.
- A signature mismatch: This means that the system clock is not accurate.
- Timestamp mismatch: This means the product instance time is not synchronized with CSSM and can cause installation to fail.

Recommended Action:

- A trust code is already installed: If you want to install a trust code despite an existing trust code on the product instance, re-configure the **license smart trust idtoken** `id_token_value`{**local**|**all**}[**force**] command in privileged EXEC mode, and be sure to include the **force** keyword this time. Entering the **force** keyword sets a force flag in the message sent to CSSM to create a new trust code even if one exists.

- Smart Account-Virtual Account mismatch: Log in to the CSSM Web UI at https://software.cisco.com/software/smart-licensing/alerts and click **Smart Software Licensing** > **Inventory** > **Product Instances**.
- Check if the product instance on which you want to generate the token is listed in the selected Virtual Account. If it is, proceed to the next step. If not, check and select the correct Smart Account and Virtual Account. Then complete these tasks again: Generating a New Token for a Trust Code from CSSM, on page 42 and Installing a Trust Code, on page 43.
- Timestamp mismatch and signature mismatch: Configure the ntp server command in global configuration mode. For example:

```
Device(config)# ntp server 198.51.100.100 version 2 prefer
```

```
----------------------------------------------------------------------------------------
----------------------------------------------------------------------------------------
```

```
Error Message %LICMGR-4-LOG_SMART_LIC_REPORTING_NOT_SUPPORTED: The CSSM
OnPrem that this product instance is connected to is down rev and does
not support the enhanced policy and usage reporting mode.
```

Explanation: Cisco Smart Software Manager On-Prem (formerly known as Cisco Smart Software Manager satellite) is not supported in the SLP environment. The product instance behaves as follows:

- Stop sending registration renewals and authorization renewals.
- Start recording usage and saving RUM reports locally.

Recommended Action: Refer to and implement one of the supported topologies instead. See: Supported Topologies, on page 17.

```
----------------------------------------------------------------------------------------
----------------------------------------------------------------------------------------
```

```
Error Message %LICMGR-6-LOG_SMART_LIC_POLICY_INSTALL_SUCCESS: A new
licensing policy was successfully installed.
```

Explanation: A policy was installed in the following way:

- As part of an ACK response.

Recommended Action: No action is required. If you want to know which policy is applied (the policy in-use) and its reporting requirements, enter the **show license all** command in privileged EXEC mode.

```
----------------------------------------------------------------------------------------
----------------------------------------------------------------------------------------
```

```
Error Message %LICMGR-6-LOG_SMART_LIC_AUTHORIZATION_INSTALL_SUCCESS: A
new licensing authorization code was successfully installed on: [chars].
```

This message is not applicable to Cisco Nexus Switches, because there are no enforced or export-controlled licenses on these product instances.

```
----------------------------------------------------------------------------------------
----------------------------------------------------------------------------------------
```

```
Error Message %LICMGR-6-LOG_SMART_LIC_AUTHORIZATION_REMOVED: A licensing
authorization code has been removed from [chars]
```

Explanation: [chars] is the UDI where the authorization code was installed. The authorization code has been removed. This removes the licenses from the product instance and may cause change in the behavior of smart licensing and the features using licenses.

Recommended Action: No action is required. If you want to see the current state of the license, enter the **show license all** command in privileged EXEC mode.

```
------------------------------------------------------------------------------------------
------------------------------------------------------------------------------------------
```

```
Error Message %LICMGR-6-LOG_SMART_LIC_REPORTING_REQUIRED: A Usage report
acknowledgement will be required in [dec] days.
```

Explanation: This is an alert which means that RUM reporting to Cisco is required. [dec] is the amount of time (in days) left to meet this reporting requirements.

Recommended Action: Ensure that RUM reports are sent within the requested time.

- If the product instance is directly connected to CSSM, or to CSLU and the product instance is configured to initiate communication complete this step on the product instance, the product instance will automatically send usage information at the scheduled time.
- If it is not sent at the scheduled time, because of technical difficulties, you can **license smart sync** command in privileged EXEC mode. For syntax details, see the license smart (privileged EXEC) in the Command Reference.
- If the product instance is connected to CSLU, but CSLU is disconnected from CSSM, complete these tasks: **Download All For Cisco (CSLU Interface),** Uploading Usage Data to CSSM and Downloading an ACK**, and Upload From Cisco (CSLU Interface)**.
- If the product instance is disconnected from CSSM and you are not using CSLU either, enter the **license smart save usage** command in privileged EXEC mode, to save the required usage information in a file. Then, from a workstation where you have connectivity to CSSM, complete these tasks: Uploading Usage Data to CSSM and Downloading an ACK > **Installing a File on the Product Instance**.

```
------------------------------------------------------------------------------------------
------------------------------------------------------------------------------------------
```

```
Error Message %LICMGR-6-LOG_SMART_LIC_TRUST_CODE_INSTALL_SUCCESS: A new
licensing trust code was successfully installed on [chars].
```

Explanation: [chars] is the UDI where the trust code was successfully installed.

Recommended Action: No action is required. If you want to verify that the trust code is installed, enter the show license status command in privileged EXEC mode. Look for the updated timestamp under header **Trust Code Installed:** in the output.

```
------------------------------------------------------------------------------------------
------------------------------------------------------------------------------------------
```

CHAPTER 8

Additional References for Smart Licensing Using Policy

Additional References for Smart Licensing Using Policy

Topic	Document Title
Cisco Smart Software Manager Help	Smart Software Manager Help
Cisco Smart License Utility (CSLU) installation and user guides	Cisco Smart License Utility Quick Start Setup Guide Cisco Smart License Utility User Guide
Licensing options for Cisco Nexus 9000 and 3000 series switches	Cisco NX-OS Licensing Options Guide
Cisco Smart Software Licensing for Cisco Nexus 3000 and 9000 Series Switches	Cisco NX-OS Licensing Guide

CHAPTER 9

Feature History for Smart Licensing Using Policy

Feature History for Smart Licensing Using Policy

This table provides release and related information for features that are explained in this module.

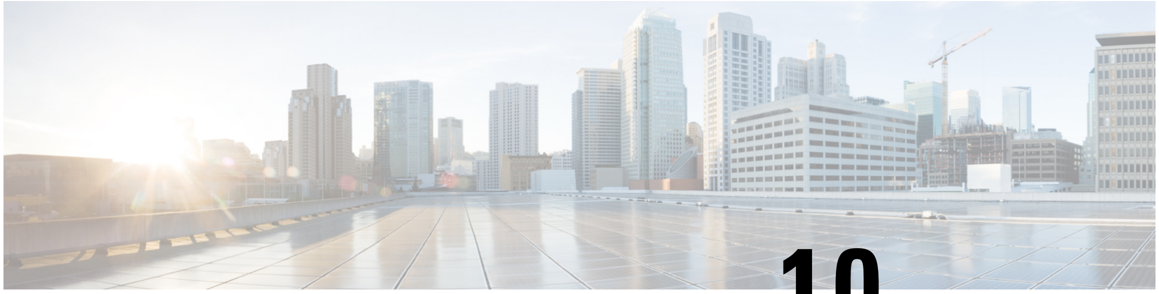
These features are available on all releases after the one they were introduced in, unless noted otherwise.

Release	Feature	Feature Information
Cisco NX-OS Release 10.4(3)F	Licensing (SLP) Support for Cisco Nexus 9364C-H1 platform switch	Added support for SLP on Cisco Nexus 9364C-H1 platform switch.
Cisco NX-OS Release 10.4(3)F	TLS v1.3	Added Transport Layer Security protocol version 1.3 support on SLP Licensing mode for Cisco Nexus platform switches.
Cisco NX-OS Release 10.4(2)F	Licensing (SLP) Support for the following Cisco Nexus platform switches: • N9K-C93108TC-FX3 • N9K-C93400LD-H1	Added support for SLP on the following Cisco Nexus platform switches. • N9K-C93108TC-FX3 • N9K-C93400LD-H1
Cisco NX-OS Release 10.4(1)F	Licensing (SLP) Support for the following Cisco Nexus platform switches: • 9804 • N9K-C9332D-H2R • N9K-C9348GC-FX3 • N9K-C9348GC-FX3PH	Added support for SLP on the following Cisco Nexus platform switches. • 9804 • N9K-C9332D-H2R • N9K-C9348GC-FX3 • N9K-C9348GC-FX3PH

Release	Feature	Feature Information
Cisco NX-OS Release 10.3(3)F	Ability to select Source Interface for DNS	Provides the user an option to define a source-interface through which the name server can be reached. • Only one source interface can be mapped against one ip name-server. • The same source interface cannot be configured for more than one use-vrf.
Cisco NX-OS Release 10.3(3)F	Source interface support for Smart and CSLU modes of transport	Added a command to configure the source interface for Smart and CSLU modes of transport.
Cisco NX-OS Release 10.3(2)F	Support for Source Interface for callhome	Added a CLI option source-interface under callhome context.
Cisco NX-OS Release 10.3(2)F	Licensing (SLP) Support for Cisco Nexus 9408 platform switches	Added support for SLP on Cisco Nexus 9408 platform switches.
Cisco NX-OS Release 10.3(2)F	CSSM to display the host name of the Product Instance	CSSM displays the host name of the Product Instance instead of UDI.
Cisco NX-OS Release 10.3(2)F	Support SLP on Non-Management VRF	Added support for SLP on non-management VRF for smart transport and CSLU mode of transport.
Cisco NX-OS Release 10.3(1)F	24-port Licensing (SLP) Support on Cisco Nexus 9300-FX3, 9300-FX3H, and 9300-FX3P platform switches	Added support for 24-port SLP on Cisco Nexus 9300-FX3, 9300-FX3H, and 9300-FX3P platform switches.
Cisco NX-OS Release 10.3(1)F	Licensing (SLP) Support for Cisco Nexus 9808 platform switches	Added support for SLP on Cisco Nexus 9808 platform switches.

Release	Feature	Feature Information
Cisco NX-OS Release 10.2(1)F	Smart Licensing Using Policy (SLP)	An enhanced version of Smart Licensing, with the overarching objective of providing a licensing solution that does not interrupt the operations of your network, rather, one that enables a compliance relationship to account for the hardware and software licenses you purchase and use. Starting with this release, SLP is automatically enabled on the device. This is also the case when you upgrade to this release. By default, your Smart Account and Virtual Account in CSSM is enabled for SLP.

Use Cisco Feature Navigator to find information about platform and software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn.



CHAPTER 10

Smart Licensing Using Policy FAQs

Smart Licensing Using Policy FAQs

Smart Licensing Using Policy

1. What is Smart Licensing Using Policy?

   The Smart Licensing Using Policy is an evolved version of Smart Licensing.

   The Smart Licensing Using Policy simplifies the day-0 operations for customers. The product will not boot in evaluation-mode, per product software registration is not required, and ongoing communication every 30 days with the Cisco Cloud is not required. However, license use compliance does require software reporting. Reporting is and can be done:

   - From Cisco factory, when all new purchases include a Smart Account on an order
   - Smart Software Manager (SSM) On-Prem (Version XXXX)
   - Cisco Smart Licensing Utility (CSLU) lite-windows application
   - Through APIs / CLIs for any 3rd party system
   - Directly to a Smart Account

2. Which platform and software release supports Smart Licensing Using Policy?

   Smart Licensing Using Policy is required from Cisco NX-OS Release 10.2(1)F onwards and is supported on Cisco Nexus 9000 and 3000 platform switches. Enforced and Export licenses are not supported on Cisco Nexus 9000 platform switches.

3. What are the key differences between Smart Licensing and Smart Licensing Using Policy?

Smart Licensing Using Policy	Smart Licensing
Mandatory evaluation mode	No registration, No evaluation mode
Day0 registration to CSSM or SSM On-Prem per device for software compliance	Allows unenforced license change, but reporting required

Smart Licensing Using Policy	Smart Licensing
On-going license reporting every 30 days	On-change reporting policies and customer-specific reporting policies
Software compliance is a preuse per product activity requirement	Software compliance is managed on-change, automation tools that are provided to assist with SW

4. What is different in CSSM with Cisco NX-OS Release 10.1(2) and Cisco Nexus Release 10.2(1)F?

In CSSM, users need not register devices before use. However, to set up automated reporting a Cisco tool, API reporting, or direct connection from a product using a trusted connection to CSSM can be used. Alternatively, users can manually upload software use records (RUM reports) directly to CSSM via the Upload Usage Data button under the Reporting and Usage Data Files tabs. An active Smart Account is required to submit software use RUM reports.

5. How often is reporting required?

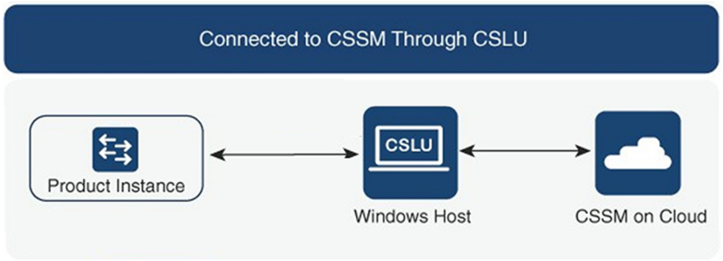
- Report is required within 90 days only when there is a change in software use.
- Ongoing reporting frequency: 365 days.
- Unenforced/Non-Export, first report is required within 90 days.

6. What are the supported topologies for connecting to Cisco Smart Software Manager (CSSM)?

The following are the supported topologies.

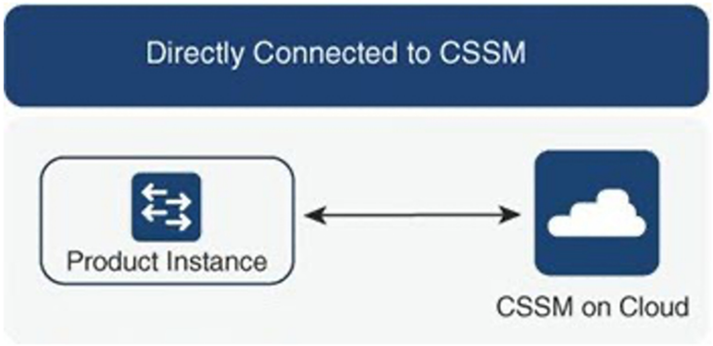
Topology 1: Connected to CSSM Through CSLU

Figure 12:



Topology 2: Connected Directly to CSSM

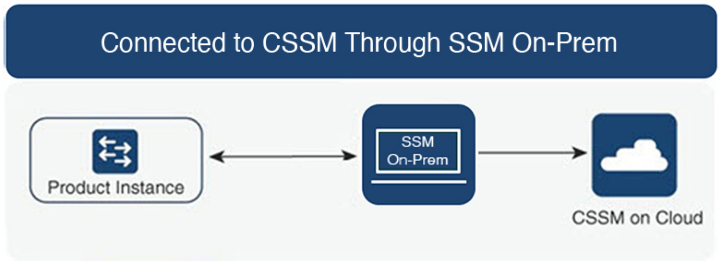
Figure 13:



Note A trust token is required only for this topology.

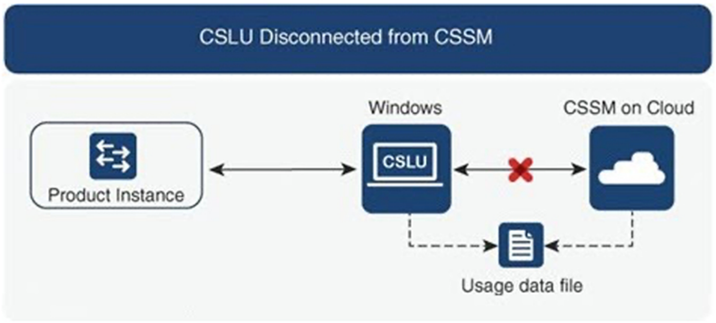
Topology 3: Connected to CSSM Through SSM On-Prem

Figure 14:



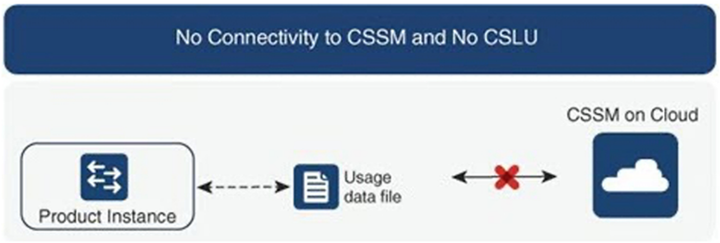
Topology 4: CSLU Disconnected from CSSM

Figure 15:



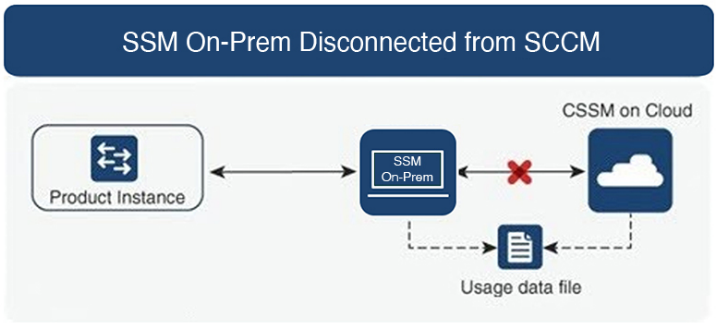
Topology 5: No Connectivity to CSSM and No CSLU

Figure 16:



Topology 6: SSM On-Prem Disconnected from CSSM

Figure 17:



7. How do customers Report software use?

   Cisco Smart Licensing Using Policy provides various reporting options using online and offline modes to report software use.

   - From the switch in off-line or direct connect mode.
   - Cisco Smart License Utility (CSLU) Lite-Windows application
   - SSM On-Prem
   - Direct to CSSM via APIs

8. Does the customer require to install a trust token?

   No, unless customer is using a direct connection to CSSM then a one-time trust exchange is established.

9. What will happen if customers upgrade from legacy licenses or from Smart Licensing to a Smart Licensing Using Policy for non-export-controlled software?

   When a customer migrates from a legacy licensing scheme [such as PAK (Product Activation Key) files or traditional Smart Licensing] to a Smart Licensing Using Policy, license conversion is expected to happen automatically.

Note

- For Topology 5: No Connectivity to CSSM and No CSLU, we recommend waiting for one hour after Smart Licensing Using Policy migration to generate the first RUM report.
- If the transport mode is off, you must collect the first rum report after an hour of migration to SLP to support PAK-based license conversion. Ensure that before you gather the rum report, show license data conversion is not blank.

10. Will the Smart Account/Virtual Account migrate to Smart Licensing Using Policy by default, or does it must be requested?

    Smart Account/Virtual Account will be enabled with Smart Licensing Using Policy functionality. No migration of Smart Account is necessary.

11. Are all Virtual Accounts inside a Smart Account enabled for Smart Licensing Using Policy?

    Yes.

12. Can a Smart Licensing Using Policy-enabled SA/VA handle non-Smart Licensing Using Policy Images?

    Yes.

13. Can a non-Smart Licensing Using Policy connect to a Smart Licensing Using Policy SA/VA?

    Yes.

14. Does anything change with the existing software subscription tiers?

    There is no change in the software subscription tier, it remains the same.

15. Does Release 10.2(1)F support only Smart Licensing Using Policy?

    Starting with Release 10.2(1)F devices will only support Smart Licensing Using Policy. There is no support for traditional licensing and smart licensing in this release.

16. After migrating to Smart Licensing Using Policy, what's the maximum amount of time I get before I send the first report.

    If at least one feature on the Nexus requires a license, a report is required within 90 days.

17. Who determines the policy and how many policies can be applied on a single device?

    CSSM determines the policy that is applied to a product. Only one policy is in use at a given point in time.

18. Is the Policy a hard requirement?

    The policy is a requirement from Cisco. It is a soft requirement on device and not an enforcement. Excluding a limited set of advanced VXLAN features, functionality is not disabled by the Nexus due to insufficient licensing.

19. What is Cisco Smart Licensing Utility (CSLU)?

    Cisco Smart Licensing Utility (CSLU) is a Windows application that is used to automate receiving or pulling software use reports from a Cisco product and report the software use to a Smart Account on Cisco Smart Software Manager (CSSM).

20. What are the minimum Windows system requirements to install CSLU?

Component	Minimum	Recommended
Hard disk	100 GB	200 GB
RAM	8 GB	8 GB
CPU	x86 Dual Core	x86 Quad Core
Ethernet NIC	1	1

21. What are the key features of CSLU?

    - Collect license usage reports from the product instances in either a push or pull modes.
    - Store and forward usage reports to CSSM for billing and analytics.
    - Obtain and distribute policy and authorization codes from CSSM.
    - It can be deployed as standalone micro service:
        - Windows host (up to 10,000 Product Instances (PI))
    - It can also be integrated as software component with controller-based products.
    - Regardless how the micro service is deployed, it is able to deliver an on-line or off-line connectivity model for the license data.

22. What is the report format in CSLU?

    The CSLU report format is based on ISO 19770-4 standard RUM report format. It is delivered in JSON format and is signed per trust model.

23. What are the various tools to collect software use report?

    Customers can use various sets of APIs that are available on NX-OS.

24. Which data does Cisco care about?

    Below are the required data fields for software reconciliation for each Cisco product that supports Smart Licensing Using Policy.

UDI	HardwareProduct serial number
SN	Software Unique ID Serial Number
Software Package and Reg ID	Software product package and entitlement tag
Count	Software use count per license entitlement
Time and date stamp	Per license entitlement change and use

Below are optional data fields for software reconciliation for each Cisco product that support Smart Licensing Using Policy.

SA-VA Level 1	example, Entity (map to a SA)
SA-VA Level 2	example, GEO (map to a SA)
SA-VA Level 3	example, department (map to a SA)
SA-VA Level 4	example, building (map to a SA)
SA-VA Level 5	example, room (map to a SA)
Free form	Data does not go back to Cisco
Free form	Data does not go back to Cisco

(SA = Smart Account, VA = Virtual Account)

25. How does Smart Licensing Using Policy work with device replacement (RMA)?

The Smart Licensing Using Policy configuration from the replaced device must be applied to the replacement device. If the existing configuration is unavailable or not functional on the new device, see the Configuring Smart Licensing Using Policy section of this document

26. What are Licenses Enforcement types?

The enforcement type indicates if the license requires authorization before use. Following are the two types of license enforcement.

- Unenforced - Unenforced licenses do not require authorization before use in air-gapped networks or 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.

Note Only unenforced licenses are supported in Release 10.2(1)F.

27. When we order hardware along with licenses, how much time does it take to reflect smart licenses under a particular smart account after allocation?

Smart Licenses will be reflected on CSSM in about 24 to 96 hours.

28. What happens if customers upgrade from smart licensing to a SLP for non-export-controlled software?

If a customer upgrades from a legacy license to a SLP, there will be no operational changes. All keys will persist through the upgrade

29. When the SLP Report doesn't sync automatically after ASCII Reload, should the sync be triggered manually?

This is a rare scenario. When the SLP transport mode is SMART, trust is established, report is synced, and ACK received, if the **copy r s** and **reload** command is issued, then when the box comes up, the report syncs automatically and the ACK is received as expected. However, if the **ascii reload** command is issued, and, when the box comes up, if the report does not sync automatically, then, to initiate the process, run the **license smart sync all** command.

CHAPTER 11

Glossary

Glossary

The following list describes acronyms and definitions for terms used throughout this document:

- **SLP:** Smart License using Policy

  A Cisco NX-OS feature that allows a switch to integrate with the Cisco cloud-based licensing infrastructure.

- **CSLU:** Cisco Smart Licensing Utility

  A software agent that collects license usage (RUM) reports from a switch and forwards them to the CSSM. If used, this agent runs on a customer premise server.

- **PI:** Product Instance

  A Nexus switch running Cisco Nexus NX-OS.

- **SA:** Smart Account

  The top level customer account in CSSM where purchased licenses are deposited by Cisco.

- **UDI:** Unique Device Identifier

  An identifier made of the Product ID (PI) and serial number. This is used by the PI to identify itself to the CSSM.

- **CSSM:** Cisco Smart Software Manager

  Cisco cloud portal where Cisco licenses can be activated and managed.

- **RUM report:** Resource Utilization Measurement (ISO19770-4)

  A license usage report created by a PI and consumed by the CSSM.

- **Push mode:** A mode in which the PI initiates communications with the CSLU by sending requests to a REST endpoint in the CSLU.

- **Enforced license:** Enforced license represents a feature that the product should not allow to be used without authorization.

- **Unenforced license:** Unenforced license represents a feature that the product does not enforce use.

- **PAK:** Product Authorization Key

  The PAK allows you to obtain a license key from one of the sites listed in the software license claim certificate document. After registering at the specified website, you will receive your license key file and installation instructions through email. Customers using PAK licenses should migrate to SLP at their earliest convenience.

- **Reported state:** Occurs when the device license state has been reported to be in use to the CSSM. This occurs when shipped or later when the device first reports.

- **Un-Reported state:** The device has not yet been reported its license usage to the CSSM and received an acknowledgment back from CSSM.