

在SD-WAN XE邊緣路由器上配置HSEC許可證

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[概念](#)

[吞吐量行為](#)

[許可證可用性驗證](#)

[路由器操作模式](#)

[設定](#)

[CSSM的線上方法](#)

[配置傳輸型別並設定預設CSSM URL](#)

[生成產品例項註冊令牌](#)

[在邊緣路由器和CSSM之間生成信任建立](#)

[驗證信任建立成功計數器](#)

[請求授權](#)

[驗證啟用是否成功](#)

[CSSM的離線方法](#)

[生成本地許可證保留](#)

[獲取邊緣路由器UDI資訊](#)

[在預留表單中填寫邊緣路由器UDI](#)

[選擇要保留的許可證數量](#)

[選擇許可證裝置型別](#)

[生成授權碼](#)

[下載SLAC](#)

[將SLAC複製到邊緣路由器](#)

[安裝SLAC](#)

[驗證安裝是否成功](#)

[vManage Workflows方法](#)

[線上工作流](#)

[與CSSM同步許可證](#)

[安裝獲取的許可證](#)

[離線工作流](#)

[與CSSM同步許可證](#)

[安裝獲取的許可證](#)

[返回HSECK9許可證](#)

[線上方法](#)

[離線方法](#)

[生成退貨代碼](#)

[刪除保留](#)

[啟用 — 是否需要重新載入？](#)

[在基於8500的平台上，需要重新載入才能啟用HSEC嗎？](#)

[啟用HSEC後C8000v是否需要重新載入？](#)

[HSEC啟用後CSR1000v是否重新載入？](#)

[SD-WAN和非SD-WAN模式的重新載入行為是否相同？](#)

[停用HSEC許可證是否同樣適用？](#)

[許可證可用性驗證](#)

[驗證](#)

[有用的命令](#)

[疑難排解](#)

[常見問題](#)

[DNS解析不起作用](#)

[SD-WAN隧道阻止DNS](#)

[傳輸URL不正確](#)

[SD-WAN隧道阻止HTTPS](#)

[外部防火牆阻止CSSM URL、IP或埠443](#)

[多個網際網路介面](#)

[相關資訊](#)

簡介

本文檔介紹如何在SD-WAN XE邊緣路由器上安裝HSECK9許可證並對其進行故障排除。

必要條件

需求

思科建議您瞭解以下主題：

- 思科軟體定義廣域網路(SD-WAN)
- Cisco IOS® XE命令列介面(CLI)
- 智慧型授權
- Cisco Software Central

採用元件

本檔案是根據以下軟體和硬體版本所編制：

- 思科邊緣路由器C1111-8PWE版本17.6.3
- 思科邊緣路由器c8000v 17.12.3
- 思科智慧軟體管理員(CSSM)
- Cisco vManage 20.12.3.1

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

概念

使用策略的智慧許可可使用多種新概念，例如：

- 許可證實施型別
- 許可證持續時間
- 授權碼
- 需要智慧許可授權碼(SLAC)的吞吐量級別 — 需要SLAC的路由器平台
- 政策
- 資源利用率度量報告 (RUM報告) 和報告確認
- 信任代碼

有關詳細資訊，請導航至[使用策略概念的智慧許可。](#)

吞吐量行為

- 如果產品沒有任何形式的HSECK9許可證，則所有ISR1000系列、ISR4000系列、C8200、C8300、CSR1000v、C8000v和ISRV的預設值都是250 Mbps。
- 如果吞吐量需要高於250 Mbps，則所有ISR1000系列、ISR4000系列、C8200、C8300、CSR1000v、C8000v和ISRV都需要安裝HSECK9許可證。
- 所有ASR1000系列都不需要HSECK9 (大於250 Mbps)。
- 所有C8500都應安裝HSECK9許可證。否則，可以手動安裝HSECK9許可證。
- 在控制器管理模式沒有吞吐量配置。HSECK9許可證安裝會自動啟用轉發核心/資料包處理器引擎，以釋放吞吐量。
- HSECK9許可證安裝後的最大吞吐量取決於平台的硬體功能。有關詳細資訊，請檢視特定平台資料表。

 附註：從20.9.2和17.9.2a起，HSEC許可證可以直接從vManage進行管理。更多詳細資訊如下：

[Cisco Catalyst SD-WAN入門指南 — 管理HSEC許可證\[Cisco SD-WAN\] - Cisco](#)

許可證可用性驗證

步驟1.導航至 [Cisco Software Central](#).

步驟2.按一下「Smart Software Manager」。

步驟3.從頂部選單中選擇Inventory。

步驟4.選擇適當的虛擬帳戶。

步驟5.選擇Virtual Account下的Licenses頁籤。

步驟6.驗證許可證已新增且可用，且餘額為正。

Cisco Software Central > Smart Software Licensing

Cisco Systems, TACSupportHelp

Smart Software Licensing

AlertsInventoryConvert to Smart LicensingReportsPreferencesOn-Prem AccountsActivity

Virtual Account: sdwan-lab

GeneralLicensesProduct InstancesEvent Log

Available Actions

Manage License TagsLicense Reservation...

By NameBy Tag

Show License Transactions

Search by License

☐ License	Billing	Available to Use	In Use	Substitution	Balance	Alerts	Actions
Router US Export Lic. for DNA	Prepaid	1	0	-	+1		Actions

Showing 1 Record

如果沒有可用的許可證或餘額為負（紅色），請向思科許可團隊[提交案例](#)。

 附註：本指南假設您已購買了HSECK9許可證或用於DNA的路由器美國出口許可證，該許可證會新增到智慧帳戶中的有效虛擬帳戶中。

路由器操作模式

使用其中一個命令檢驗路由器是否處於控制器管理模式。

<#root>

show platform software device-mode

show version | include mode

範例：

<#root>

EdgeRouter#

show platform software device-mode

Device Operating-mode: Controller-Managed
Device-mode bootup status:
8/03 00:44:16 System is green

Bootup Success

EdgeRouter#

show version | in mode

Router operating mode: Controller-Managed



附註：如果工作模式導致Autonomous (自治) ，請使用命令將路由器移至Controller-Managed(控制器管 controller-mode enable理)。

設定

CSSM的線上方法

配置傳輸型別並設定預設CSSM URL

步驟1.配置正確的傳輸型別和URL。

<#root>

EdgeRouter#

config-transaction

EdgeRouter(config)#

license smart transport smart

EdgeRouter(config)#

license smart url default

EdgeRouter(config)#

commit

Commit complete.



附註：如果路由器附加了模板：支援傳輸和URL的智慧命令，可以使用CLI附加功能模板進行配置。有關詳細資訊，請導航至[CLI附加功能模板。](#)

步驟2.檢驗更改是否正確提交。

<#root>

show lic tech support | begin Smart Licensing Status

=====

Status: Not started

<none>

Status: DISABLED

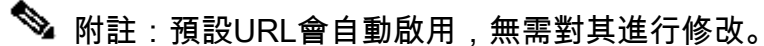
Status: ENABLED

Version privacy: DISABLED

[illegible]

URL: https://smartreceiver.cisco.com/licservice/license <<<<<<<<<< URL must be pointed to smartrece

```
Server Identity Check: True
```



在許可證所在的同一虛擬帳戶中，導航到General頁籤，然後按一下New Token。

Virtual Account: [sdwan-lab](#) ▼

General

Licenses

Product Instances

Event Log

Virtual Account

Description:

Default Virtual Account: No

Product Instance Registration Tokens

The registration tokens below can be used to register new product instances to this virtual account.

New Token...

Token	Expiration Date	Uses	Export-Controlled	Description	Created By	Actions
No Records Found						

The token will be expired when either the expiration or the maximum uses is reached

No Records to Display

步驟2.填寫新令牌資訊。

說明:令牌用途簡短說明。
到期時間：令牌對產品註冊有效的天數。
最大使用次數：令牌最大使用次數。可選。

確保選中Allow export-controlled選項。否則，許可證註冊失敗，然後按一下Create Token。

 附註：當達到過期或最大使用量時，令牌將過期。

 附註：如需詳細資訊，請導覽至[Cisco Export Trade](#)。

步驟3.複製權杖。

將剛生成的令牌複製到剪貼簿；導航至操作>複製，或手動在令牌字串旁邊的小藍色圖示中顯示。

Virtual Account: **sdwan-lab** ▼

General | Licenses | Product Instances | Event Log

Virtual Account

Description:

Default Virtual Account: No

product instances to this virtual account.

Press ctrl + c to copy selected text to clipboard.

ODRIMjg0YWQtMDk4ZC00NWlxLTgzYmYtODMxNjU3NTQwMTY0LTE2NjM0ODM2%0ANjU4MDB8S2lFK3BsUXZlZWpCaEJBK2lkREMvJmUTB0bzluZit4MEwyb3hX%0AVTl4ND0%3D%0A

Uses	Export-Controlled	Description	Created By	Actions
ODRIMjg0YWQtMDk...	Allowed	hseckk9 Installation	ericnar	Copy Download... Revoke...

The token will be expired when either the expiration or the maximum uses is reached

在邊緣路由器和CSSM之間生成信任建立

為了提供使用出口管制許可證的授權，邊緣路由器必須與CSSM建立信任。對於握手，邊緣路由器使用上一步中在CSSM上生成的令牌。

```
<#root>
```

```
license smart trust idtoken TOKEN local force
```

範例：

```
<#root>
```

```
EdgeRouter#
```

```
license smart trust idtoken ZThjOTlmM2UtMjQ2ZC00YjI1LTgwNjctZGIxZjIzYjZiYmVmLTE2NjM0NjI1%0AMjgyNTh8YWNV
```

建立信任後，日誌會顯示與CSSM的通訊。

```
<#root>
```

```
EdgeRouter#
```

```
show logging last 50
```

```
<snip>
```

```
*Aug 18 21:03:44.730: %CRYPTO_ENGINE-5-KEY_DELETED: A key named SLA-KeyPair2 has been removed from key
*Aug 18 21:03:46.146: %CRYPTO_ENGINE-5-KEY_ADDITION: A key named SLA-KeyPair2 has been generated or imp
*Aug 18 21:03:53.221: %SYS-6-PRIVCFG_ENCRYPT_SUCCESS: Successfully encrypted private config file
*Aug 18 21:03:56.107: %SMART_LIC-5-COMM_RESTORED: Communications with Cisco Smart Software Manager (CSSM
*Aug 18 21:03:56.347: %SMART_LIC-6-TRUST_INSTALL_SUCCESS: A new licensing trust code was successfully i
```

驗證信任建立成功計數器

驗證信任建立成功計數器是否增加。這表示授權代理可以訪問CSSM。

```
<#root>
```

```
EdgeRouter#
```

```
show lic tech support | begin Communication Statistics
```

```
Communication Statistics:
```

```
=====
```

```
Communication Level Allowed: DIRECT
```

```
Overall State: <empty>
```

```
Trust Establishment:
```

```
Attempts: Total=1, Success=1, Fail=0 Ongoing Failure: Overall=0 Communication=0 <<<<<<<<<
```

```
Last Response: OK on Aug 18 21:03:56 2022 UTC
```

```
Failure Reason: <none>
```

```
Last Success Time: Aug 18 21:03:56 2022 UTC
```

```
Last Failure Time: Aug 18 21:00:43 2022 UTC
```

```
<snip>
```



附註：如果失敗計數器增加，請導航至本文檔中的故障排除部分。

請求授權

此時，信任已建立，但HSECK9許可證尚未使用。之所以發生這種情況，是因為需要路由器向CSSM請求許可證。要獲取許可證，請運行授權請求。

```
<#root>
```

```
EdgeRouter#
```

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

日誌：

<#root>

EdgeRouter#

show logging | include SMART

```
*Aug 18 21:11:41.553: %SMART_LIC-6-AUTHORIZATION_INSTALL_SUCCESS: A new licensing authorization code was generated
*Aug 18 21:11:41.641: %SMART_LIC-6-EXPORT_CONTROLLED: Usage of export controlled features is allowed for this device
```

在智慧許可事件日誌中，將儲存許可請求資訊，以備需要更多資訊。

<#root>

EdgeRouter#

show lic eventlog 0

```
**** Event Log ****
2022-08-18 21:11:41.538 UTC SAEVT_RESERVE_INSTALL_START udi="PID:C1111-8PWE,SN:FGL2149XXXX" authorization=
2022-08-18 21:11:41.552 UTC SAEVT_TAG_EXPORT exportAllowed="False" count="0" entitlementTag="regid.2019-03.com.cisco.DNA.3.1 licenses"
2022-08-18 21:11:41.576 UTC SAEVT_TAG_EXPORT exportAllowed="True" count="0" entitlementTag="regid.2019-03.com.cisco.DNA.3.1 licenses"
2022-08-18 21:11:41.576 UTC SAEVT_STATE_RESERVE_AUTHORIZED
2022-08-18 21:11:41.641 UTC SAEVT_TAG_AUTHORIZED count="1" entitlementTag="regid.2019-03.com.cisco.DNA.3.1 licenses"
2022-08-18 21:11:41.641 UTC SAEVT_TAG_EXPORT exportAllowed="True" count="1" entitlementTag="regid.2019-03.com.cisco.DNA.3.1 licenses"
2022-08-18 21:12:06.119 UTC SAEVT_RESERVE_INSTALL_START udi="PID:C1111-8PWE,SN:FGL2149XXXX" authorization=
```

驗證啟用是否成功

有些命令用於驗證許可證現在是否可用並正確啟用。

<#root>

show license tech support | begin License Usage

show license authorization

show license summary

show license usage

範例：

License Usage:
License Entitlement Tag Count Status

hseck9 (DNA_HSEC) 1 IN USE <<<<<<<<<<

CSSM的離線方法

對於不允許訪問Internet的空中連線網路，可以通過在CSSM上本地預留SLAC來執行出口控制許可證安裝。



附註：此方法不需要傳輸型別或有效的智慧統一資源定位器(URL)。

生成本地許可證保留

在許可證所在的同一虛擬帳戶中，導航到產品例項>授權許可證強制功能。

Cisco Software Central > Smart Software Licensing

Smart Software Licensing

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

Virtual Account: **sdwan-lab**

General | Licenses | **Product Instances** | Event Log

Authorize License-Enforced Features...

Search by Device or by Product Type

Name	Product Type	Last Contact	Alerts	Actions
No Records Found				

No Records to Display

獲取邊緣路由器UDI資訊

show license udi 本地許可證保留需要來自邊緣路由器的唯一裝置識別符號(UDI)，請運行命令以獲取產品ID(PID)和序列號(SN)。

<#root>

EdgeRouter#

show license udi

UDI: PID:C1111-8PWE,SN:FGL2149XXXX

在預留表單中填寫邊緣路由器UDI

選擇Single Device，並填寫邊緣路由器的SN和PID。按「Next」（下一步）。

Authorize License-Enforced Features

STEP 1
Enter Request Code

STEP 2
Select Licenses

STEP 3
Review and Confirm

STEP 4
Authorization Code

device to enable the features. [Learn More](#)
Generating an authorization code here is only required for devices that do not connect to the Smart Software Manager directly, or through the Cisco Licensing Manager, to report the features they need.

Single Device

Enter the identifiers for the device to be licensed.

Display Name:

UUID:

Serial Number:

FGL2149XXX[

PID:

C1111-8PWE

Version ID:

Host ID:

MAC Address:

Virtual ID(SUVI)

You can use the 'show license udi' command to see the identifiers for a device

CancelNext

選擇要保留的許可證數量

由於它是單個裝置，因此保留的許可證是1，請在框中鍵入數字。確保數字不超過可用數字。

Authorize License-Enforced Features

STEP 1 ✓
Enter Request Code

STEP 2
Select Licenses

STEP 3
Review and Confirm

STEP 4
Authorization Code

UDI Serial Number:

FGL214991A9

Select the Licenses to Enabled the Features

Select the set of licenses that will enable the desired features. The licenses will be reserved on the devices

License	Purchased	Available	Reserve
Router US Export Lic. for DNA U.S. Export Restriction Compliance license for DNA based Routers	1	1	1

選擇許可證裝置型別

裝置型別可以是內部數位網路架構(DNA)或DNA雲。這取決於購買的許可證型別。

Select a Device Type



Some devices could not be identified based on the identifiers provided.
Please select a device type.

Device Type:

DNA On Prem

Unidentified Devices:

☒	Device
	Search
☒	SN: FGL214991A9 PID: C1111-8PWE

Selected:1

If you want to enable features on different types of devices, you must perform this operation separately for each type.

Continue

Cancel

生成授權碼

檢視配置並按一下Generate Authorization Code。

Authorize License-Enforced Features

✕

STEP 1 ✓
Enter Request Code

STEP 2 ✓
Select Licenses

STEP 3
Review and Confirm

STEP 4
Authorization Code

Product Instance Details

UDI PID: C1111-8PWE
UDI Serial Number: FGL214991A9
Device Type: DNA On Prem

Licenses to Reserve

License	Total Quantity to Reserve
Router US Export Lic. for DNA U.S. Export Restriction Compliance license for DNA based Routers	1

Cancel

Back

Generate Authorization Code

下載SLAC

SLAC可以檔案形式下載，也可以複製到剪貼簿。

將SLAC複製到邊緣路由器

有三種方法可以將SLAC檔案複製到邊緣路由器。

- 使用USB驅動器。

```
<#root>
```

```
EdgeRouter#
```

```
show file systems | include usb|Size
```

```
Size(b)          Free(b)  Type  Flags  Prefixes
15598043136 15596658688 disk  rw      usb0:
```

```
EdgeRouter#
```

```
dir usb0:
```

```
Directory of usb0:/
```

```
5 -rwx 1557 Aug 19 2022 00:43:30 +00:00
```

```
AuthorizationCode_SN_FGL2149XXXX.txt
```

15598043136 bytes total (15596658688 bytes free)

EdgeRouter#

copy usb0:AuthorizationCode_SN_FGL2149XXXX.txt bootflash:

Destination filename [AuthorizationCode_SN_FGL2149XXXX.txt]?

Copy in progress...C

1557 bytes copied in 0.020 secs (77850 bytes/sec)

- 使用vManage至Control Connections，導航至[Transfer Files between a Edge Router and vManage](#)以瞭解詳細資訊。
- 服務端的SCP/FTP/TFTP。

安裝SLAC

使用智慧匯入在bootflash中安裝SLAC檔案。

<#root>

EdgeRouter#

license smart import bootflash:AuthorizationCode_SN_FGL2149XXXX.txt

Import Data Successful

Last Confirmation code UDI: PID:C1111-8PWE,SN:FGL2149XXXX

Confirmation code: aaa6b57e

日誌。

<#root>

EdgeRouter#

show logging | include SMART

*Aug 19 05:42:45.309: %SMART_LIC-6-AUTHORIZATION_INSTALL_SUCCESS: A new licensing authorization code was

*Aug 19 05:42:45.362: %SMART_LIC-6-EXPORT_CONTROLLED: Usage of export controlled features is allowed for

EdgeRouter#

show license eventlog 0

**** Event Log ****

2022-08-19 05:42:45.293 UTC SAEVT_RESERVE_INSTALL_START udi="PID:C1111-8PWE,SN:FGL2149XXXX" authorization

2022-08-19 05:42:45.308 UTC SAEVT_TAG_EXPORT exportAllowed="False" count="0" entitlementTag="regid.2019-

2022-08-19 05:42:45.333 UTC SAEVT_TAG_EXPORT exportAllowed="True" count="0" entitlementTag="regid.2019-

2022-08-19 05:42:45.334 UTC SAEVT_STATE_RESERVE_AUTHORIZED
2022-08-19 05:42:45.362 UTC SAEVT_TAG_AUTHORIZED count="1" entitlementTag="regid.2019-03.com.cisco.DNA_
2022-08-19 05:42:45.362 UTC SAEVT_TAG_EXPORT exportAllowed="True" count="1" entitlementTag="regid.2019-

驗證安裝是否成功

使用線上方法中的相同命令驗證許可證是否正確安裝。

<#root>

show license authorization

show license summary

show license tech support | begin License Usage

如果安裝正確，則虛擬帳戶中的許可證將自動遞增使用中計數器，並遞減可用使用計數器。

Virtual Account: [sdwan-lab](#) ▼

General

Licenses

Product Instances

Event Log

Available Actions

Manage License Tags

License Reservation...

☒ Show License Transactions

By Name | By Tag

Search by License

☐ License

Billing

Available to Use

In Use

Substitution

Balance

Alerts

Actions

☒ Router US Export Lic. for DNA

Prepaid

1

1
(1 Reserved)

-

0

Actions

☐ Source: Manual Entry
Subscription Id: N/A

SKU:
C8000-HSEC=
Family:
DNA On Prem

Quantity:
1

Start Date:
-
Expires:
- never -

Showing 1 Record

此外，在Product Instances頁籤中，還會顯示邊緣路由器的UDI資訊。按一下條目以獲取有關許可證特徵的更多資訊。

Smart Software Licensing

[Support](#) [Help](#)[Alerts](#) | [Inventory](#) | [Convert to Smart Licensing](#) | [Reports](#) | [Preferences](#) | [On-Prem Accounts](#) | [Activity](#)Virtual Account: [sdwan-lab](#)

General

Licenses

Product Instances

Event Log

Authorize License-Enforced Features...

Search by Device or by Product Type

Name	Product Type	Last Contact	Alerts	Actions
UDI_PID:C1111-8PWE; UDI_SN:FGL214	DNA On Prem	2022-Aug-19 05:43:12 (Reserved Licenses)		Actions

Showing 1 Record

vManage Workflows方法

從20.9.2開始，vManage允許藉助工作流安裝HSECK9許可證。

 附註：此方法僅適用於「路由器US匯出許可證」。DNA許可證；裝置特定的HSEC許可證(如ISR4300_HSEC或ISR4400_HSEC)不再有效。有關如何將裝置特定HSEC許可證轉換為DNA HSEC的更多資訊，請訪問[Restrictions for Managing HSEC Licenses](#)部分。

線上工作流

與CSSM同步許可證

1. — 在vManagement GUI中，導航至主選單>工作流>同步和安裝HSEC許可證。

Cisco Catalyst SD-WAN

Monitor

Configuration

Tools

Maintenance

Administration

Workflows

Reports

Analytics

Workflow Library

POPULAR WORKFLOWS

Quick Connect

Firmware Upgrade

Software Upgrade

Sync and Install HSEC Licenses

Configure Teleworker Devices

Create Configuration Group

Deploy Configuration Group

Create Security Policy

Deploy Policy Group

Create NFV Configuration Group

Monitor • Overview

DevicesTunnelsApplicationsSecurityVPNLogsMulticloud

	CERTIFICATE STATUS	LICENSING	REBOOT
	5 Warning	2 Assigned 5 Unassigned	1 Last 24 hrs

Poor Performing Sites

Tunnel Health

17
Tunnels

2. — 按一下彈出視窗中的「讓我們開始做」按鈕。

Welcome to Sync and Install HSEC Licenses

You can sync and install licenses on devices in online or offline mode.

Let's Do It

☐ Don't show this to me again

3. — 選擇Sync Licenses任務，然後按一下Next。

 Cisco Catalyst SD-WAN

Assign HSEC License

1 of 7 steps

Select License Task

To start, select one of the options:

☒ Sync Licenses

Sync licenses from CSSM for all devices.

☐ Install Licenses

Install licenses on devices.

Note: In order to install, you should have already synced your licenses from CSSM.

4. — 選擇Online模式，然後按一下Next。

☰ Cisco Catalyst SD-WAN

Assign HSEC License

2 of 7 steps

Sync Licenses

Select Mode

To start, select the mode for syncing licenses

☒ Online

☐ Offline

5 — 輸入您的Cisco CSSM憑證，然後點選下一步。

☰ Cisco Catalyst SD-WAN

Assign HSEC License

3 of 7 steps

Enter Smart Account Credentials

Now enter your Smart Account credentials

Username*

ericgar

✕

Password*

SHOW

6. — 驗證HSEC許可證同步概述，然後按一下下一步。

☰ Cisco Catalyst SD-WAN

Assign HSEC License

4 of 7 steps

Online Mode | Sync Licenses

HSEC License Sync Overview

This process will sync licenses from CSSM for the selected devices and virtual account.

Select Virtual Account

Select HSEC-Compatible Devices

Summary

7.- vManage連線到雲並查詢所有可用的虛擬帳戶。在下拉選單中，選擇包含有效和正計數HSEC許

可證的虛擬帳戶。

 注意：在步驟6中輸入的憑據必須在存放有HSEC許可證的智慧帳戶和虛擬帳戶中具有管理員角色。

☰ Cisco Catalyst SD-WAN

Assign HSEC License

5 of 7 steps

Select Virtual Account

Select Virtual Account

sdwan-lab - Cisco Systems, TAC

8. — 選擇要安裝HSEC許可證的裝置。

 附註：僅顯示與HSEC相容的裝置

☰ Cisco Catalyst SD-WAN

Assign HSEC License

6 of 7 steps

Online Mode - Sync Licenses Task

Select Devices

Select one or more devices

All Devices (5/47)

🔍 reachable

1 selected

	Hostname	Status	Chassis Number	Reachability	Device Model	IP Address	Tags
☒	cEdge_Site1_West_01	-	C8K-B23B869B-CA3E-970E-CFFF-2D1DB3E339AD	reachable	C8000v	1.1.1.221	--

9. — 檢視並驗證請求摘要，然後按一下Sync。

Assign HSEC License

7 of 7 steps

Summary - Sync Licenses | Online

Review your request and make any changes. If you are satisfied, send the request.

Selected Virtual Account

Virtual Account Name sdwan-lab

Selected Devices

Hostname	Status	Chassis Number	Reachability	Device Model	IP Address	Tags
cEdge_Site1_West_01	-	C8K-B23B869B-CA3E-970E-CFFF-2D1DB3E339AD	reachable	C8000v	1.1.1.221	-

1 Record

Items per page: 251 ~ 1 of 1

10. — 按一下Check HSEC Assignment Status以即時驗證SLAC保留。

Assign HSEC License

Done! We're now syncing licenses from CSSM

What's Next?

Check HSEC Assignment Status

Back to Workflow Library



11. — 從CSSM獲取許可證並儲存在vManage中後，其狀態顯示為「成功」。

Monitor · Overview

HSEC License Fetch | Validation success

Total Task: 1 | Success: 1

Device Group (1)

Search Table

status	message
Success	Done - HSEC License Fetch

View Logs

Host: vmanage_1(1.1.1.7)
Site ID: 1000
Device Model: vManage

[11-Sep-2024 5:27:09 UTC] fetching license
[11-Sep-2024 5:29:11 UTC] vManage got license from CSSM for C8K-B23B869B-CA3E-970E-CFFF-2D1DB3E339AD
[11-Sep-2024 5:29:11 UTC] License fetched for all selected devices
[11-Sep-2024 5:29:11 UTC] fetched

Feedback

Close

安裝獲取的許可證

1. — 在vManagement GUI中，導航至主選單>工作流>同步和安裝HSEC許可證。

Cisco Catalyst SD-WAN

Monitor

Configuration

Tools

Maintenance

Administration

Workflows

Reports

Analytics

Workflow Library

POPULAR WORKFLOWS

Quick Connect

Firmware Upgrade

Software Upgrade

Sync and Install HSEC Licenses

Configure Teleworker Devices

Create Configuration Group

Deploy Configuration Group

Create Security Policy

Deploy Policy Group

Create NFV Configuration Group

Monitor • Overview

DevicesTunnelsApplicationsSecurityVPNLogsMulticloud

	CERTIFICATE STATUS	LICENSING	REBOOT
	5 Warning	2 Assigned 5 Unassigned	1 Last 24 hrs

Poor Performing Sites

Tunnel Health
17
Tunnels

2. — 選擇「安裝許可證」任務。

Cisco Catalyst SD-WAN

Assign HSEC License

1 of 3 steps

Select License Task

To start, select one of the options:

☐ Sync Licenses

Sync licenses from CSSM for all devices.

☒ Install Licenses

Install licenses on devices.

Note: In order to install, you should have already synced your licenses from CSSM.

3. — 選擇為其獲取HSEC許可證的裝置。

Cisco Catalyst SD-WAN
Assign HSEC License

2 of 3 steps

Install Licenses Task

Select Devices

Select one or more devices

All Devices (1/4)

1 selected

	Hostname	Status	Chassis Number	Reachability	Device Model	IP Address	Tags
☒	cEdge_Site1_West_01	fetchd	C8K-B23B869B-CA3E-970E-CFFF-2D1DB3E339AD	reachable	C8000v	1.1.1.221	--

4. — 驗證安裝摘要，然後按一下安裝。

Cisco Catalyst SD-WAN
Assign HSEC License

3 of 3 steps

Summary - Install Licenses

Review your request and make any changes. If you are satisfied, send the request.

^ Selected Devices
Edit

Hostname	Status	Chassis Number	Reachability	Device Model	IP Address	Tags
cEdge_Site1_West_01	fetchd	C8K-B23B869B-CA3E-970E-CFFF-2D1DB3E339AD	reachable	C8000v	1.1.1.221	--

1 Record
Items per page: 25
1 - 1 of 1
|< < > >|

5. — 按一下Check HSEC Assignment Status以即時檢查安裝狀態。

Cisco Catalyst SD-WAN
Assign HSEC License

Done! We're now currently activating HSEC Devices

What's Next?

Check HSEC Assignment Status

Back to Workflow Library

6.- vManage與路由器通訊，將SLAC傳送到路由器並進行安裝。最終狀態必須為Success。

Cisco Catalyst SD-WAN

Select Resource Group

Configuration · Devices

HSEC License Install | Validation success

Initiated By: ericgar

Total Task: 1 | Success : 1

Device Group (1)

Search Table

As of: Sep 10, 2024 11:50 PM

status	chassisNumber	message	startTime	Systemip	Action
Success	C8K-B23B869B-CA3E-970E-CFFF-2D1DB3E339AD	HSEC Installation complete	Sep 10, 2024, 11:50:25 PM	1.1.1.221	

7. — 按一下Action圖示以顯示HSEC安裝的更詳細日誌。

Configuration · Devices

View Logs

Host: cEdge_Site1_West_01(1.1.1.221)
Site ID: 100003
Device Model: C8000v

[11-Sep-2024 5:50:25 UTC] Installing HSEC license
[11-Sep-2024 5:50:26 UTC] RPC call to device for initializing HSEC install is successful.
[11-Sep-2024 5:50:28 UTC] Last Confirmation code UDI: PID:C8000V,SN:C8K-B23B869B-CA3E-970E-CFFF-2D1DB3E339AD
Confirmation code: e293d6a0Import Data CompletedLast Confirmation code UDI: PID:C8000V,SN:C8K-B23B869B-CA3E-970E-CFFF-2D1DB3E339AD Confirmation code: e293d6a0
[11-Sep-2024 5:50:28 UTC] HSEC Installation complete

離線工作流

與CSSM同步許可證

1. — 在vManagement GUI中，導航至主選單>工作流>同步和安裝HSEC許可證。

Cisco Catalyst SD-WAN

Monitor

Configuration

Tools

Maintenance

Administration

Workflows

Reports

Analytics

Workflow Library

POPULAR WORKFLOWS

Quick Connect

Firmware Upgrade

Software Upgrade

Sync and Install HSEC Licenses

Configure Teleworker Devices

Create Configuration Group

Deploy Configuration Group

Create Security Policy

Deploy Policy Group

Create NFV Configuration Group

Monitor • Overview

DevicesTunnelsApplicationsSecurityVPNLogsMulticloud

	CERTIFICATE STATUS	LICENSING	REBOOT
	5 Warning	2 Assigned 5 Unassigned	1 Last 24 hrs

Poor Performing Sites

Tunnel Health

17
Tunnels

2. — 按一下彈出視窗中的「讓我們開始做」按鈕。

Welcome to Sync and Install HSEC Licenses

You can sync and install licenses on devices in online or offline mode.

Let's Do It

☐ Don't show this to me again

3. — 選擇Sync Licenses任務，然後按一下Next。

☰ Cisco Catalyst SD-WAN

Assign HSEC License

1 of 7 steps

Select License Task

To start, select one of the options:

☒ Sync Licenses
Sync licenses from CSSM for all devices.

☐ Install Licenses
Install licenses on devices.
Note: In order to install, you should have already synced your licenses from CSSM.

4. — 選擇Offline模式，然後按一下Next。

2 of 6 steps

Sync Licenses

Select Mode

To start, select the mode for syncing licenses

☐ Online☒ Offline

5. — 仔細檢視流程概述，然後按一下下一步。

3 of 6 steps

Offline Mode

HSEC License Sync Overview

A. Download Process

This process allows you to select HSEC-compatible devices to be added to HSEC device list file.

- Select HSEC-Compatible Devices
- Download HSEC Device List File
- Summary

B. Upload Process

Once you've uploaded the HSEC device list file to CSSM, it will in turn, give you an authorization code file that needs to be uploaded here.

- Upload HSEC Device List File to CSSM and Download Authorization Code File
- Upload Authorization Code File
- Summary

6. — 選擇Download Process選項，然後按一下Next。

4 of 6 steps

Select Task

Before proceeding, select the task you would like to perform.

☒ Download Process

Select and download HSEC Device list file

This task allows you to select HSEC-compatible devices to be added to HSEC device list file. You will be then given a device list file to be uploaded to CSSM.

☐ Upload Process

Upload Authorization Code File

Use this task once you've downloaded the required authorization code file from CSSM.

7. — 在搜尋欄中，過濾要安裝許可證的裝置。

Assign HSEC License

5 of 6 steps

Offline Mode - Sync Licenses Task

Select Devices

Select one or more devices

All Devices (1/46)

Search: C8K-19E2D66D-D5CC-6709-7A73-D050E231C407

1 selected

	Hostname	Status	Chassis Number	Reachability	Device Model	IP Address	Tags
☒	cEdge_Sit1_East_01	-	C8K-19E2D66D-D5CC-6709-7A73-D050E231C407	reachable	C8000v	1.1.1.231	--

8. — 檢視任務摘要，然後按一下下載HSEC裝置檔案(.SUDI)

Assign HSEC License

6 of 6 steps

Summary - Sync Licenses | Offline | Download

Review your request and make any changes. If you are satisfied, send the request.

Selected Devices [Edit](#)

Hostname	Status	Chassis Number	Reachability	Device Model	IP Address	Tags
cEdge_Sit1_East_01	-	C8K-19E2D66D-D5CC-6709-7A73-D050E231C407	reachable	C8000v	1.1.1.231	--

1 Record

Items per page: 25 1 - 1 of 1

Download HSEC Device List

[Download HSEC Device File \(.SUDI\)](#)

9. — 開始自動下載許可證使用情況。

UD_SA_2024_9_11_12_54_56.tar.gz

866 B • Done

10. — 按一下開啟思科智慧軟體管理器或導航至：[思科軟體中心](#)。

Done! You've generated and downloaded your HSEC Device list file

Now that you've generated and downloaded your HSEC device list file, it's time to upload the SUDI file into CSSM. Once CSSM generates the Smart License Authorization Code (SLAC) file, upload it to vManage.

What's Next?

[Open Cisco Smart Software Manager](#)[Upload Authorization Code File](#)[Back to Workflow Library](#)

11. — 在選定的智慧帳戶中，導航至思科軟體中心>智慧軟體許可，然後點選報告>使用資料檔案>上傳使用資料.....

Cisco Software Central



Cisco Software Central > Smart Software Licensing

Cisco Systems, TAC

Smart Software Licensing

[SL Product Details](#) [Support](#) [Help](#)[Alerts](#) | [Inventory](#) | [Convert to Smart Licensing](#) | [Reports](#) | [Preferences](#) | [On-Prem Accounts](#) | [Activity](#) | [Commercial Consumption](#)

Reports

[Report](#) | [Usage Data Files](#) | [Reporting Policy](#) | [Synch File for Device Controllers](#)

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.

[Upload Usage Data...](#)

12. — 在「上傳使用者資料」彈出視窗中，按一下Browse並選擇剛下載的檔案，然後按一下Upload Data。

Upload Usage Data

Please select the Usage File you wish to upload.

* Usage Data File:

[Browse](#)

UD_SA_2024_9_11_12_54_56.tar.gz

1

2

[Upload Data](#)[Cancel](#)

13. — 系統開始處理檔案。大約需要5到10分鐘才能完成。然後按一下「Download」。

附註：要生成ACK檔案，報告狀態必須為「無錯誤」；如果出現錯誤，請按一下展開圖示以獲取有關錯誤的更多資訊。如果需要，請開啟思科TAC案例。

Cisco Software Central > Smart Software Licensing

Cisco Systems, TAC

Smart Software Licensing

SL Product Details Support Help

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

Reports

Report

Usage Data Files

Reporting Policy

Synch File for Device Controllers

Devices can be configured to report the features that they are using.

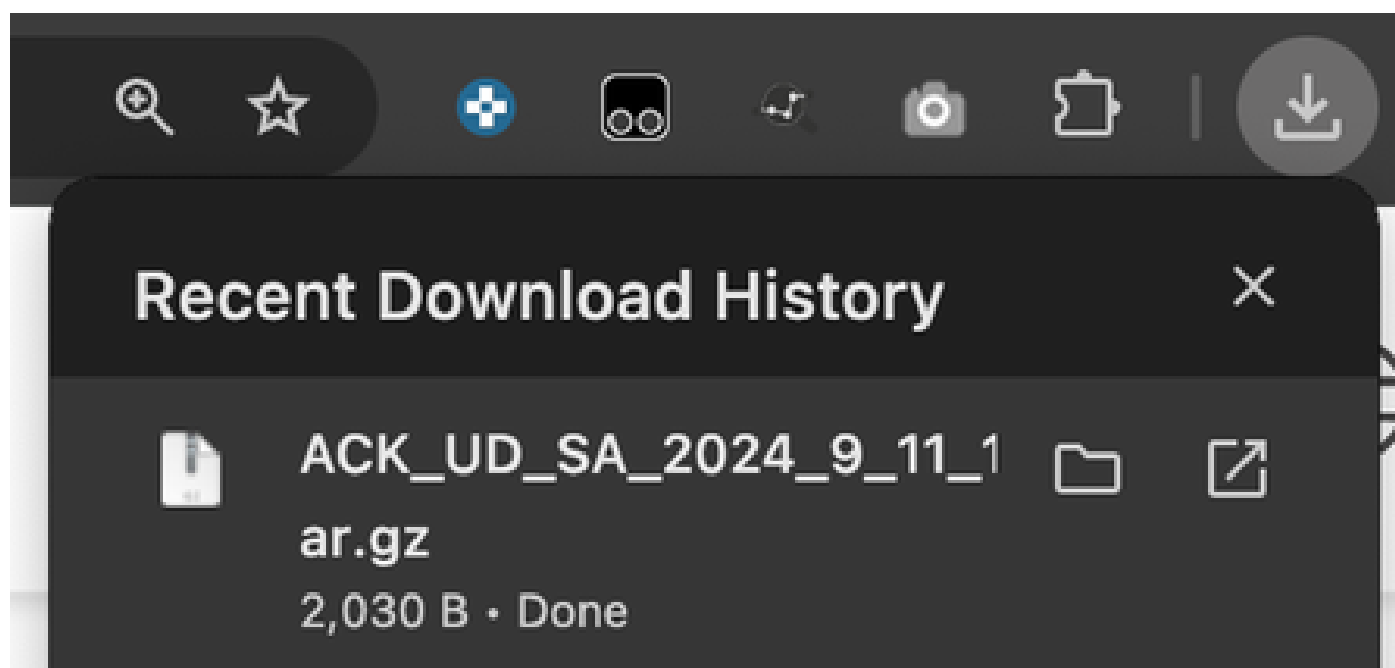
This usage then determines which licenses are needed, in order to be compliant.

Upload Usage Data...

Search by File Name, Virtual Account

+ Usage Data File	Reported	Virtual Account	Reporting Status	Devices	Acknowledgement
- UD_SA_2024_9_11_12_54_56.tar.gz	2024-Sep-11	sdwan-lab	i No Errors	1	Download
UD_VA_2024_09_11_18_54_33.tar.gz		sdwan-lab	i No Errors	1	

14. — 系統生成ACK檔案並自動下載。



15. — 在vManagement GUI中，再次導航到主選單>工作流>同步和安裝HSEC許可證>同步許可證>離線>下一步>上傳流程。

4 of 6 steps

Select Task

Before proceeding, select the task you would like to perform.

☐ Download Process

Select and download HSEC Device list file

This task allows you to select HSEC-compatible devices to be added to HSEC device list file. You will be then given a device list file to be uploaded to CSSM.

☒ Upload Process

Upload Authorization Code File

Use this task once you've downloaded the required authorization code file from CSSM.



16. — 按一下Choose a File，或將下載的檔案拖放到框中，然後按一下Upload。

5 of 6 steps

Upload Smart License Authorization Code File

Upload the Authorization Code (SLAC) file generated by CSSM.



Choose a file or drag and drop to upload.

Accepted files: .gz
Accepted sizes: up to 10MB

ACK_UD_SA_2024_9_11_12... .gz 

Upload

17. — 驗證任務摘要，然後按一下Upload。

Summary - Sync Licenses | Offline | Upload

Review your request and make any changes. If you are satisfied, send the request.

^ Device Entries [Edit](#)

Hostname	Status	Chassis Number	Reachability	Device Model	IP Address	Tags
cEdge_Sir1_East_01	Fetches	C8K-19E2D66D-D5CC-6709-7A73-D050E231C407	-	C8000v	1.1.1.231	--

Done! We're now currently syncing smart account authorization code (SLAC) file for the devices

安裝獲取的許可證

1. — 返回工作流庫同步和安裝許可證，然後按一下安裝許可證。

Select License Task

To start, select one of the options:

☐ Sync Licenses

Sync licenses from CSSM for all devices.

☒ Install Licenses

Install licenses on devices.

Note: In order to install, you should have already synced your licenses from CSSM.

2. — 從清單中選擇為其進行許可證授權的同一裝置，然後按一下下一步。

Cisco Catalyst SD-WAN

Assign HSEC License

2 of 3 steps

Install Licenses Task

Select Devices

Select one or more devices

All Devices (1/5)

CBK-19E2D66D-D5CC-6709-7A73-D050E231C407

1 selected

	Hostname	Status	Chassis Number	Reachability	Device Model	IP Address	Tags
☒	cEdge_Sit1_East_01	fetched	CBK-19E2D66D-D5CC-6709-7A73-D050E231C407	reachable	C8000v	1.1.1.231	--

3. — 檢視任務摘要，然後按一下安裝。

Cisco Catalyst SD-WAN

Assign HSEC License

3 of 3 steps

Summary - Install Licenses

Review your request and make any changes. If you are satisfied, send the request.

^ Selected Devices

Edit

Hostname	Status	Chassis Number	Reachability	Device Model	IP Address	Tags
cEdge_Sit1_East_01	fetched	CBK-19E2D66D-D5CC-6709-7A73-D050E231C407	reachable	C8000v	1.1.1.231	--

4. — 等待進程完成，安裝狀態必須為「成功」。

Cisco Catalyst SD-WAN

Select Resource Group

Monitor · Overview

HSEC License Install | Validation success

Initiated By: ericgar

Total Task: 1 | Success : 1

Device Group (1)

Search Table

status	chassisNumber	message	startTime	Systemip	Action
Success	CBK-19E2D66D-D5CC-6709-7A73-D050E231C407	HSEC Installation complete	Sep 11, 2024, 1:04:13 PM	1.1.1.231	

5. — 按一下Action圖示以顯示HSEC安裝的更詳細日誌。

View Logs

Host: cEdge_Sit1_East_01(1.1.1.231)

Site ID: 100004

Device Model: C8000v

```
[11-Sep-2024 19:04:13 UTC] Installing HSEC license
[11-Sep-2024 19:04:17 UTC] RPC call to device for initializing HSEC install is successful.
[11-Sep-2024 19:04:19 UTC] Last Confirmation code UDI: PID:C8000V,SN:C8K-19E2D66D-D5CC-6709-7A73-D050E231C407
Confirmation code: a599674eImport Data CompletedLast Confirmation code UDI: PID:C8000V,SN:C8K-19E2D66D-D5CC-
6709-7A73-D050E231C407 Confirmation code: a599674e
[11-Sep-2024 19:04:19 UTC] HSEC Installation complete
```

Feedback

返回HSECK9許可證

線上方法

目前，在控制器管理模式下沒有實現以聯機或離線方式返回許可證。

<#root>

EdgeRouter#

license smart authorization return local online

Operation cannot be completed because license is in use

EdgeRouter#

license smart authorization return local offline

Operation cannot be completed because license is in use

要刪除許可證安裝，需要將路由器更改為自主模式。

<#root>

EdgeRouter#

controller-mode disable

Disabling controller mode erases the nvram filesystem, remove all configuration files, and reload the boot image.
Ensure the BOOT variable points to a valid image
Continue? [confirm]

 附註：此模式更改將刪除當前的SD-WAN配置，強烈建議在安全位置備份配置。這有助於在邊緣路由器移回控制器管理模式時重建控制連線。

路由器進入自治模式後，必須完成一些基本配置才能訪問網際網路和域名系統(DNS)解析：

1. 配置WAN介面的IP地址和掩碼
2. 開啟WAN介面的電源
3. 配置預設IP路由
4. 啟用DNS
5. 配置DNS伺服器

 附註：自主模式使用configure terminal命令來進入配置模式，而不是configuration-transaction命令。

 附註：自主模式不需要提交更改，而是將所有完成的配置儲存在運行配置檔案中。

使用HSECK9或Cisco DNA匯出控制許可證所在的同一虛擬帳戶的令牌。如果沒有活動令牌，則生成一個新令牌。

完成與邊緣路由器中相同的過程，生成與CSSM建立的信任。

```
<#root>
```

```
EdgeRouter#
```

```
configure terminal
```

```
EdgeRouter(config)#
```

```
license smart transport smart
```

```
EdgeRouter(config)#
```

```
license smart url default
```

```
EdgeRouter(config)#
```

```
end
```

```
EdgeRouter#
```

```
license smart trust idtoken TOKEN local force
```

```
EdgeRouter#
```

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

 注意：使用前面介紹的相同命令驗證是否啟用了正確的傳輸型別和智慧接收器URL，並且信任建立已成功完成。

通訊完成後，將許可證返回虛擬帳戶中的垃圾桶。

```
<#root>
```

```
EdgeRouter#
```

```
license smart authorization return local online
```

Authorization already returned with this code:

UDI: PID:C1111-8PWE,SN:FGL2149XXXX

Return code: CmJHqn-5CFUkd-effkCh-4XqCpQ-SgK5Sz-fQFfM8-6qH7MA-33hDbX-sXT

日誌。

```
<#root>
```

```
EdgeRouter#
```

```
show logging | include SMART
```

```
*Aug 18 22:00:22.998: %SMART_LIC-6-AUTHORIZATION_REMOVED: A licensing authorization code has been removed
```

```
Router#show license eventlog 0
```

```
**** Event Log ****
```

```
2022-08-18 22:08:53.275 UTC SAEVT_RESERVE_RETURN_START udi="PID:C1111-8PWE,SN:FGL2149XXXX" authorization
```

 附註：使用指令將路由器移回控制器管理模式controller-mode enable。

離線方法

為了生成返回代碼，路由器必須處於自主模式。完成Online Method以更改模式。

生成退貨代碼

使用路由器中的本地授權驗證CSSM中的保留許可證需要返回代碼。

```
<#root>
```

```
EdgeRouter#
```

```
license smart authorization return local offline
```

Enter this return code in Cisco Smart Software Manager portal:

UDI: PID:C1111-8PWE,SN:FGL2149XXXX

Return code:

CCKUTq-Qg2Ytw-ZhSLq5-bDFw7e-VvWgf2-QwwBed-3MaRcT-fFfGcn-X6e <<<< Copy the string

刪除保留

導覽至Product Instances > Actions > Remove。貼上剛從路由器複製的返回代碼，然後按一下 Remove Reservation。

Remove Reservation

To remove a Product Instance that has reserved licenses and make those licenses once again available to other Product Instances, enter in the Reservation Return Code generated by the Product Instance. If you cannot generate a Reservation Return Code, contact [Cisco Support](#)

* Reservation Return Code:

CCKUTq-Qg2Ytw-ZhSLq5-bDFw7e-VvWgf2-QwwBed-3MaRcT-fFfGcn-X6e

Remove Reservation

Cancel

The License reservation removed successfully appears shown been (成功刪除的許可證保留通知)。再次導航到操作>移除>移除例項。

啟用 — 是否需要重新載入？

在基於8500的平台上，需要重新載入才能啟用HSEC嗎？

是，8500平台系列需要在自治模式或控制器模式下重新載入。

啟用HSEC後C8000v是否需要重新載入？

不，沒這個必要。根據C8000v上的設計，許可證仍為「不使用」，但裝置在安裝hsec後立即獲得無限吞吐量。

HSEC啟用後CSR1000v是否重新載入？

不能，啟用hsec後，CSR1000v不需要重新載入。

SD-WAN和非SD-WAN模式的重新載入行為是否相同？

不可以，SD-WAN和非SD-WAN模式在HSEC支援方面截然不同。

在SD-WAN模式下，需要重新載入才能啟用/啟用HSEC，而在非SD-WAN模式下，CLI「license feature hsec」在裝置上啟用/啟用hsec。在SD-WAN模式下的CSR1000v和C8000V平台上不需要重新載入。

停用HSEC許可證是否同樣適用？

可以在非SD-WAN模式(Autonomous)下解除安裝HSEC許可證，但是，使用該功能時無法解除安裝HSEC許可證。使用者必須使用CLI「no license feature hsec」禁用/停用HSEC許可證，並重新載入裝置，使許可證處於「not-in-use」狀態，然後啟動解除安裝命令。不支援SD-WAN模式下的HSEC許可證「uninstall」，因為無法禁用該功能。但是，使用者可以選擇進入自主模式並解除安裝，作為應對模式更改的已知挑戰的解決方法。請開啟TAC案例，以接收有關如何在SD-WAN模式下將許可證返回到CSSM的指導。



附註：有關詳細資訊，請訪問：[SD-WAN的HSEC許可證常見問題解答](#)。

許可證可用性驗證

驗證

使用本節內容，確認您的組態是否正常運作。

有用的命令

線上或離線方法的每個步驟中描述了驗證過程。

```
<#root>
```

```
show license tech support
```

`show license status`

`show license authorization`

`show license summary`

`show license history message`

`show license eventlog`

`license smart clear event log`

`license smart sync local`

`license smart factory reset`

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

使用策略的智慧許可依靠邊緣路由器和CSSM之間通過Internet的安全雙向通訊，以交換有利於註冊和許可證提取的確認和握手。

有些常見情況不允許在裝置之間正確交換消息。

常見問題

DNS解析不起作用

要訪問smartreceiver.com，邊緣路由器必須能夠解析域名。否則，URL不會轉換為可路由IP，通訊失敗。此錯誤通常在嘗試建立信任後顯示。

*Aug 18 20:45:10.345: %SMART_LIC-3-COMM_FAILED: Communications failure with the Cisco Smart License Uti

確保有IP連線至Internet。

```
<#root>
```

```
ping 8.8.8.8
```

對URL執行Ping以驗證DNS是否有效，如果外部裝置使用telnet來封鎖網際網路控制訊息通訊協定(ICMP)。

```
<#root>
```

```
ping cisco.com
```

```
telnet cisco.com 80
```

如果測試失敗，請配置DNS伺服器並啟用DNS解析。

```
<#root>
```

```
ip domain lookup
```

```
ip name-server 8.8.8.8
```

如果無法配置外部DNS伺服器，請在路由器中配置本地DNS解析。

```
<#root>
```

```
EdgeRouter#
```

```
config-transaction
```

```
EdgeRouter(config)#
```

```
ip host smartreceiver.com A.B.C.D
```

```
EdgeRouter(config)#
```

```
commit
```



附註：如果您需要知道哪些IP響應smartreceiver.com，請從Windowsnslookup或Linux電腦運行命令。



附註：不建議使用本地DNS解析，因為響應方IP可以隨著時間的推移而更改，並且Cisco不會通知此更改。

在智慧許可(SL)事件日誌中可看到常見錯誤消息。

<#root>

EdgeRouter#

show license eventlog 0

**** Event Log ****

2022-08-18 20:45:10.345 UTC SAEVT_COMM_FAIL error="Unable to resolve server hostname/domain name"
2022-08-18 20:45:57.804 UTC SAEVT_COMM_FAIL error="Unable to resolve server hostname/domain name"

<#root>

EdgeRouter#

show logging | include SMART

*Aug 18 20:59:44.914: %SMART_LIC-3-COMM_FAILED: Communications failure with the Cisco Smart Software Ma

SD-WAN隧道阻止DNS

如果SD-WAN隧道中的隱含ACL阻止傳入的DNS響應，也會發生類似的問題。

<#root>

EdgeRouter#

show license eventlog 0

**** Event Log ****

2022-08-18 20:45:10.345 UTC SAEVT_COMM_FAIL error="Unable to resolve server hostname/domain name"
2022-08-18 20:45:57.804 UTC SAEVT_COMM_FAIL error="Unable to resolve server hostname/domain name"

<#root>

EdgeRouter#

```
show logging | include SMART
```

```
*Aug 18 20:59:44.914: %SMART_LIC-3-COMM_FAILED: Communications failure with the Cisco Smart Software Ma
```

確保在註冊時允許DNS服務。

<#root>

EdgeRouter#

```
show sdwan running-config sdwan
```

[illegible]

```
allow-service icmp
allow-service sshd
allow-service netconf
no allow-service ntp
no allow-service ospf
no allow-service stun
no allow-service https
no allow-service snmp
no allow-service bfd
exit
```

傳輸URL不正確

對於全新安裝（全新），預設傳輸型別為Cisco Smart Licensing Utility(CSLU)。

<#root>

EdgeRouter#

<#root>

```
EdgeRouter#
```

```
show logging | include SMART
```

```
*Aug 18 20:59:44.914: %SMART_LIC-3-COMM_FAILED: Communications failure with the Cisco Smart Software Ma
```

 附註：Cisco SD-WAN(Cisco vManage)不支援CSLU，CSLU不能用於報告Cisco vManage管理的路由產品例項的許可證使用情況。有關詳細資訊，請導航至[Cisco Smart License Utility\(CSLU\)](#)。

手動配置智慧代理的預設URL和傳輸型別，並再次嘗試使用令牌建立的信任。

```
<#root>
```

```
EdgeRouter#
```

```
configure terminal
```

```
EdgeRouter(config)#
```

```
license smart transport smart
```

```
EdgeRouter(config)#
```

```
license smart url default
```

```
EdgeRouter(config)#
```

```
commit
```

SD-WAN隧道阻止HTTPS

智慧許可通訊基於超文本傳輸協定安全(HTTPS)埠443，因此，如果SD-WAN隧道阻止傳入的HTTPS響應，註冊、授權請求和RUM報告通知將失敗。

日誌和事件日誌中的常見錯誤。

```
*Aug 18 20:59:44.914: %SMART_LIC-3-COMM_FAILED: Communications failure with the Cisco Smart Software Ma
```

確保在註冊時在SD-WAN隧道中允許HTTPS服務。如果沒有，請允許該值，並再次嘗試使用令牌建立信任。

<#root>

EdgeRouter#

```
show sdwan running-config sdwan
```

```
sdwan
interface GigabitEthernet0/0/0
tunnel-interface
encapsulation gre
encapsulation ipsec weight 1
no border
color public-internet
no last-resort-circuit
no low-bandwidth-link
no vbond-as-stun-server
vmanage-connection-preference 5
port-hop
carrier default
nat-refresh-interval 5
hello-interval 1000
no allow-service all
no allow-service bgp
allow-service dhcp
allow-service dns
allow-service icmp
allow-service sshd
allow-service netconf
no allow-service ntp
no allow-service ospf
no allow-service stun
allow-service https <<<<<<<<<<<<<<< MUST be allowed
no allow-service snmp
no allow-service bfd
exit
```

外部防火牆阻止CSSM URL、IP或埠443

如果站點架構使用防火牆控制流量，請確保不會阻止指向smartreceiver.cisco.com的埠443。請與您的防火牆團隊或Internet服務提供商(ISP)聯絡以進一步驗證。

從路由器。

<#root>

EdgeRouter#

telnet smartreceiver.com 443

Trying smartreceiver.com (X.X.X.X, 443)...

Open

從服務VRF主機。

```
<#root>
```

```
ericgar@cisco$
```

```
telnet smartreceiver.cisco.com 443
```

```
Trying X.X.X.X...
```

```
Connected to smartreceiver.cisco.com.
```

```
Escape character is '^]'.
```

多個網際網路介面

在有多個介面的情況下，與CSSM的通訊會失敗；http源介面可以更改為路由器中的任何可用介面。

```
<#root>
```

```
EdgeRouter#
```

```
config-transaction
```

```
EdgeRouter(config)#
```

```
ip http client source-interface INTERFACE
```

```
EdgeRouter(config)#
```

```
commit
```

相關資訊

- [思科企業路由平台的智慧許可使用策略](#)
- [使用策略SD-WAN管理智慧許可的許可證](#)
- [技術支援與文件 - Cisco Systems](#)

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。