SD-WAN XEエッジルータでのHSECライセンスの設定

内容

- はじめに
- 前提条件
  - 要件
  - 使用するコンポーネント
- 背景説明
  - コンセプト
  - スループット動作
  - ライセンスの有効性の検証
  - ルータの動作モード
- 設定
  - CSSMへのオンライン方式
    - トランスポートタイプの設定とデフォルトCSSM URLの設定
    - 製品インスタンス登録トークンの生成
    - エッジルータとCSSM間の信頼確立の生成
    - Trust Establishment Successカウンタの確認
    - 承認の要求
    - アクティブ化が正常に行われたことを確認する
  - CSSMへのオフラインメソッド
    - ローカルライセンス予約の生成
    - エッジルータのUDI情報の取得
    - 予約フォームにエッジルータのUDIを入力する
    - 予約するライセンス数の選択
    - ライセンスのデバイスタイプの選択
    - 認証コードの生成
    - SLACのダウンロード
    - エッジルータへのSLACのコピー
    - SLACのインストール
    - インストールが成功したことを確認する
- vManageワークフローメソッド
  - オンラインワークフロー
    - ライセンスとCSSMの同期
    - 取得したライセンスのインストール
  - オフラインワークフロー
    - ライセンスとCSSMの同期
    - 取得したライセンスのインストール
- HSECK9ライセンスの返却
  - リターンコードの動作
  - リターンコードの生成
  - 予約の削除
- アクティベーション：リロードは必要ですか。

8500ベースのプラットフォームでは、HSECをアクティブにするためにリロードが必要だというのは本当ですか。
HSECのアクティベーション後にC8000vのリロードが必要ですか
HSECのアクティベート後のCSR1000vのリロードについて
リロード動作はSD-WANモードと非SD-WANモードで同じですか。
HSECライセンスの非アクティブ化についても同様ですか。
ライセンスの有効性の検証
確認
便利なコマンド
トラブルシュート
一般的な問題
DNS解決が機能しない
SD-WANトンネルがDNSをブロックする
トランスポートURLが正しくありません
SD-WANトンネルがHTTPSをブロック
外部ファイアウォールがCSSM URL、IP、またはポート443をブロック
インターネットへの複数のインターフェイス
関連情報

はじめに

このドキュメントでは、SD-WAN XEエッジルータにHSECK9ライセンスをインストールしてトラブルシューティングする方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Cisco Software-Defined Wide Area Network(SD-WAN)
- Cisco IOS® XEコマンドラインインターフェイス(CLI)
- Smart Licensing
- Cisco Software Central（登録ユーザ専用）

使用するコンポーネント

このドキュメントは、次のソフトウェアとハードウェアのバージョンに基づいています。

- CiscoエッジルータC1111-8PWEバージョン17.6.3
- Ciscoエッジルータc8000v 17.12.3
- Cisco Smart Software Manager(CSSM)
- Cisco vManage 20.12.3.1

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始していま

す。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

コンセプト

ポリシーを使用したスマートライセンスでは、次のようなさまざまな新しい概念が使用されます。

- ライセンス適用タイプ
- ライセンス期間
- 承認コード
- Smart Licensing Authorization Code(SLAC)を必要とするスループットレベル – SLACを必要とするルータプラットフォーム
- ポリシー
- 生産資源稼働率の測定レポート（RUMレポート）およびレポート通知
- 信頼コード

詳細については、「ポリシー概念を使用したスマートライセンス」を参照してください。

注：このドキュメントで説明されているHSECK9ライセンスインストールプロセスは、物理ルータと仮想ルータに同じように適用されます。プラットフォーム固有のインストールプロセスはありません。

スループット動作

- 製品にHSECK9ライセンスの形式がない場合、すべてのISR1000シリーズ、ISR4000シリーズ、C8200、C8300、CSR1000v、C8000v、およびISRvのデフォルトは250 Mbpsです。
- スループットを250 Mbpsより高くする必要がある場合は、すべてのISR1000シリーズ、ISR4000シリーズ、C8200、C8300、CSR1000v、C8000v、およびISRvにHSECK9ライセンスをインストールする必要があります。
- すべてのASR1000シリーズで、250 Mbpsを超える場合はHSECK9を使用する必要はありません。
- すべてのC8500には、製造元でHSECK9ライセンスがインストールされている必要があります。インストールされていない場合は、HSECK9ライセンスを手動でインストールできます。
- コントローラ管理モードにはスループット設定はありません。HSECK9ライセンスのインストールにより、フォワーディングコア/パケットプロセッサエンジンでスループットが自動的に解放されます。
- HSECK9ライセンスのインストール後の最大スループットは、プラットフォームのハードウェア機能によって異なります。詳細については、各プラットフォームのデータシートを参照してください。

注:20.9.2および17.9.2aの時点で、HSECライセンスはvManageから直接管理できます。詳細については、次のリンクを参照してください。
[Cisco Catalyst SD-WANスタートアップガイド – HSECライセンスの管理[Cisco SD-WAN] – シスコ]

注：インストール後にルータでHSECK9ライセンスをアクティブにするには、仮想ルータC8000vを除くすべての物理ルータで手動リロードが必要です。

ライセンスの有効性の検証

ステップ 1：**Cisco Software Central**に移動します。

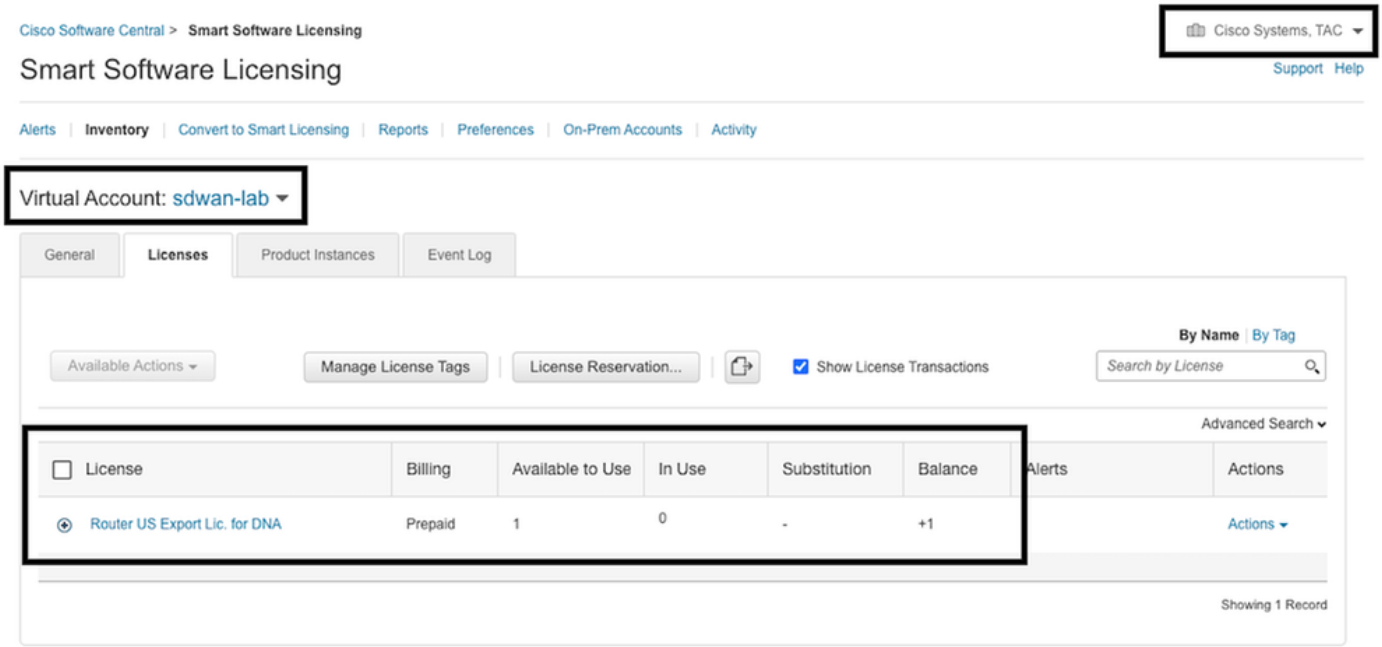
ステップ 2：Smart Software Managerをクリックします。

ステップ 3：トップメニューからInventoryを選択します。

ステップ 4：適切な仮想アカウントを選択します。

ステップ 5：Virtual Accountの下にあるLicensesタブを選択します。

手順 6：ライセンスが追加され、使用可能で、プラスのバランスになっていることを確認します。



ライセンスがないか、残高がマイナス（赤）の場合は、シスコライセンスチームでケースをオープンしてください。

注：このガイドでは、Cisco DNAのHSECK9ライセンスまたはルータUSエクスポートライセンスをすでに購入し、スマートアカウント内の有効な仮想アカウントに追加していることを前提としています。

ルータの動作モード

次のいずれかのコマンドを使用して、ルータがコントローラ管理モードになっていることを確認します。

<#root>

```
show platform software device-mode
```

```
show version | include mode
```

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
```

注：動作モードがAutonomousになる場合、**controller-mode enable**コマンドを使用して、ルータをController-Managedに移動します。

設定

CSSMへのオンライン方式

トランスポートタイプの設定とデフォルトCSSM URLの設定

ステップ 1：正しいトランスポートタイプとURLを設定します。

<#root>

```
EdgeRouter#
config-transaction

EdgeRouter(config)#
license smart transport smart

EdgeRouter(config)#
license smart url default

EdgeRouter(config)#
commit

Commit complete.
```

注：ルータにテンプレートが添付されている場合：トランスポートおよびURLのスマートコマンドがサポートされており、CLIアドオン機能テンプレートを使用して設定できます。詳細については、「CLIアドオン機能テンプレート」を参照してください。

ステップ 2：変更が正しくコミットされていることを確認します。

<#root>

```
EdgeRouter#
show lic tech support | begin Smart Licensing Status

Smart Licensing Tech Support info

Smart Licensing Status
======================

Smart Licensing is ENABLED

License Conversion:
Automatic Conversion Enabled: True
Status: Not started

Export Authorization Key:
Features Authorized:
<none>

Utility:
Status: DISABLED
```

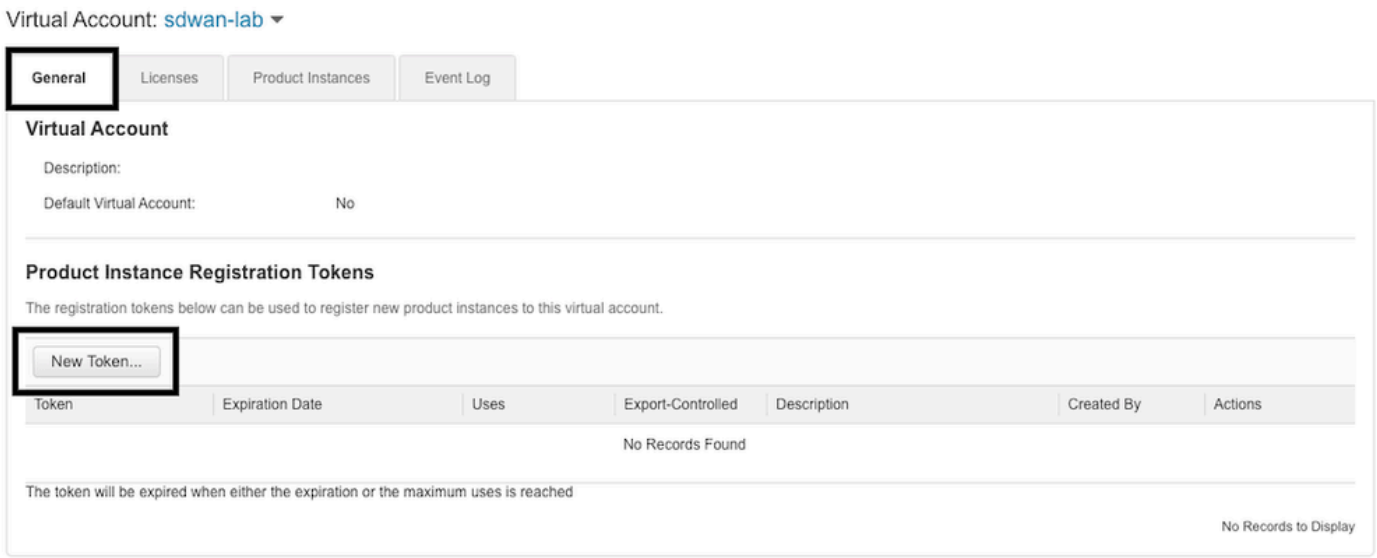
```
Smart Licensing Using Policy:
Status: ENABLED

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

Transport:
Type: Smart <<<<<<<<<<<<<<<<<<<<<<<<<<<<<< This must be Smart


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


Proxy:
Address: <empty>
Port: <empty>
Username: <empty>
Password: <empty>
Server Identity Check: True
```

注：デフォルトのURLは自動的に有効になるため、変更する必要はありません。

製品インスタンス登録トークンの生成

ステップ 1： 新しいトークンを生成します。

ライセンスが存在する同じ仮想アカウントで、Generalタブに移動し、New Tokenをクリックします。



ステップ 2：新しいトークン情報を入力します。

説明：トークンの使用目的の簡単な説明。
有効期限：トークンが製品登録に有効な日数。
最大使用数：トークンの最大使用数。オプション。

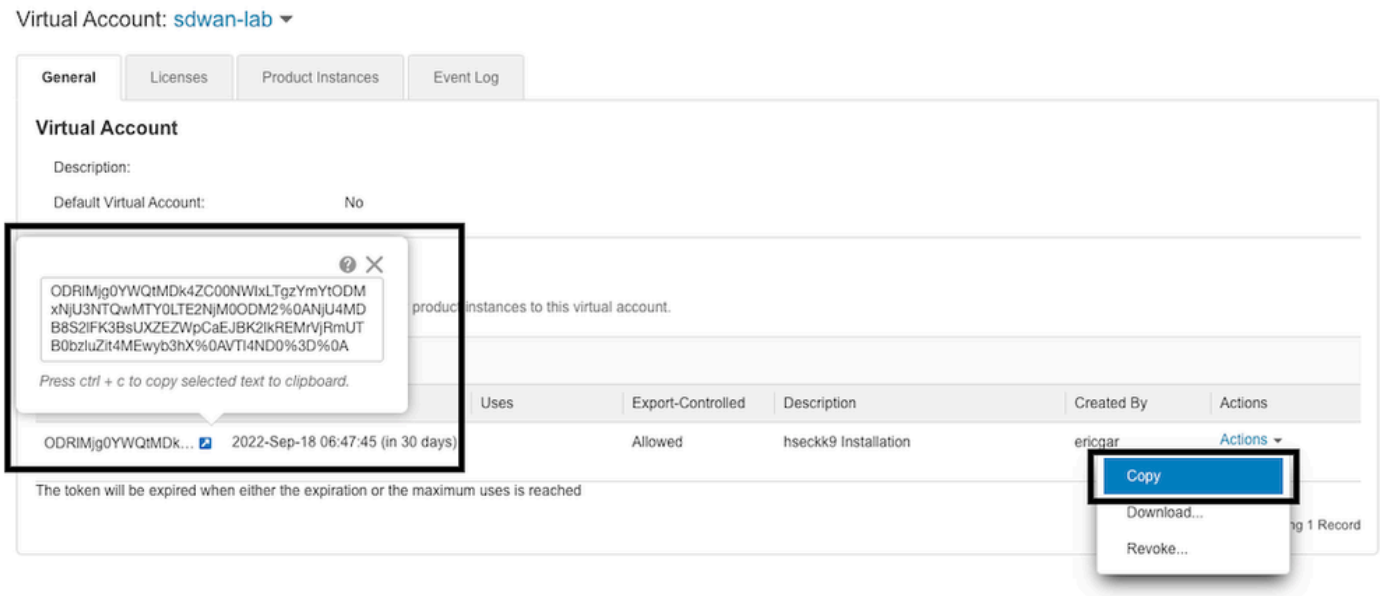
Allow export-controlledオプションにチェックマークが付いていることを確認する。そうしないと、ライセンス登録が失敗し、Create Tokenをクリックします。

注：トークンは、有効期限または最大使用量に達すると期限切れになります。

注：詳細については、Cisco Export Tradeを参照してください。

ステップ 3：トークンをコピーします。

生成したばかりのトークンをクリップボードにコピーします。Actions > Copyに移動するか、トークン文字列の横にある小さな青いアイコンを手動でクリックします。



エッジルータとCSSM間の信頼確立の生成

エクスポート制御されたライセンスを使用するための許可を提供するには、エッジルータがCSSMとの信頼を確立する必要があります。ハンドシェイクでは、エッジルータは前のステップでCSSMで生成されたトークンを使用します。

<#root>

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

例：

<#root>

```
EdgeRouter#

license smart trust idtoken ZThjOTlmM2UtMjQ2ZC00YjI1LTgwNjctZGIxZjIzYjZiYmVmLTE2NjM0NjI1%0AMjgyNTh8YWNVe
```

信頼が確立された直後に、ログにCSSMとの通信が表示されます。

<#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 (CSS
*Aug 18 21:03:56.347: %SMART_LIC-6-TRUST_INSTALL_SUCCESS: A new licensing trust code was successfully i
```

Trust Establishment Successカウンタの確認

trust establishment successカウンタが増加していることを確認します。つまり、ライセンスエージェントはCSSMに到達できます。

<#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>
```

注:failカウンタが増加する場合は、このドキュメントの「トラブルシューティング」の項に進んでください。

承認の要求

この時点で、信頼は確立されますが、HSECK9ライセンスはまだ使用されていません。これは、CSSMへのルータ要求でライセンスの使用状況を確認する必要があるためです。ライセンスを取得するには、認証要求を実行します。

<#root>

```
EdgeRouter#
```

`license smart authorization request add hseck9 local`

ログ:

<#root>

```
EdgeRouter#
show logging | include SMART

*Aug 18 21:11:41.553: %SMART_LIC-6-AUTHORIZATION_INSTALL_SUCCESS: A new licensing authorization code wa
*Aug 18 21:11:41.641: %SMART_LIC-6-EXPORT_CONTROLLED: Usage of export controlled features is allowed fo
```

スマートライセンスのイベントログには、より多くの情報が必要になった場合に備えて、ライセンス要求情報が保存されます。

<#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" authorizati
2022-08-18 21:11:41.552 UTC SAEVT_TAG_EXPORT exportAllowed="False" count="0" entitlementTag="regid.2019
2022-08-18 21:11:41.576 UTC SAEVT_TAG_EXPORT exportAllowed="True" count="0" entitlementTag="regid.2019-
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_
2022-08-18 21:11:41.641 UTC SAEVT_TAG_EXPORT exportAllowed="True" count="1" entitlementTag="regid.2019-
2022-08-18 21:12:06.119 UTC SAEVT_RESERVE_INSTALL_START udi="PID:C1111-8PWE,SN:FGL2149XXXX" authorizati
```

アクティブ化が正常に行われたことを確認する

ライセンスが使用可能で、正しくアクティブ化されているかどうかを確認するコマンドがいくつかあります。

<#root>

```
show license tech support | begin License Usage

show license authorization

show license summary

show license usage
```

例：

<#root>

```
EdgeRouter#
show license tech support | begin License Usage


License Usage
=============
Handle: 1
License: hseck9
Entitlement Tag: regid.2019-03.com.cisco.DNA_HSEC,1.0_509c41ab-05a8-431f-95fe-ec28086e8844
Description: hseck9
Count: 1
Version: 1.0
Status: IN USE(15)               <<<<<<<<<<<<<<<<<<<<<<<


Status time: Aug 18 21:11:41 2022 UTC
Request Time: Aug 18 21:11:41 2022 UTC
Export status: RESTRICTED - ALLOWED
Feature Name: hseck9
Feature Description: hseck9
Enforcement type: EXPORT RESTRICTED
License type: Perpetual
Measurements:
ENTITLEMENT:
Interval: 00:15:00
Current Value: 1

EdgeRouter#
show license authorization


Overall status:
Active: PID:C1111-8PWE,SN:FGL2149XXXX
Status: SMART AUTHORIZATION INSTALLED on Aug 18 21:11:41 2022 UTC   <<<<<<<<<<<<<<<


Last Confirmation code: 0cde51c5

Authorizations:
Router US Export Lic. for DNA (DNA_HSEC):
Description: U.S. Export Restriction Compliance license for DNA based Routers
Total available count: 1
Enforcement type: EXPORT RESTRICTED
Term information:
Active: PID:C1111-8PWE,SN:FGL2149XXXX
Authorization type: SMART AUTHORIZATION INSTALLED  <<<<<<<<<<<<<


License type: PERPETUAL
Term Count: 1

Purchased Licenses:
No Purchase Information Available


Edge#
show license summary
```

```
License Usage:
License Entitlement Tag Count Status
-----------------------------------------------------------------------------

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

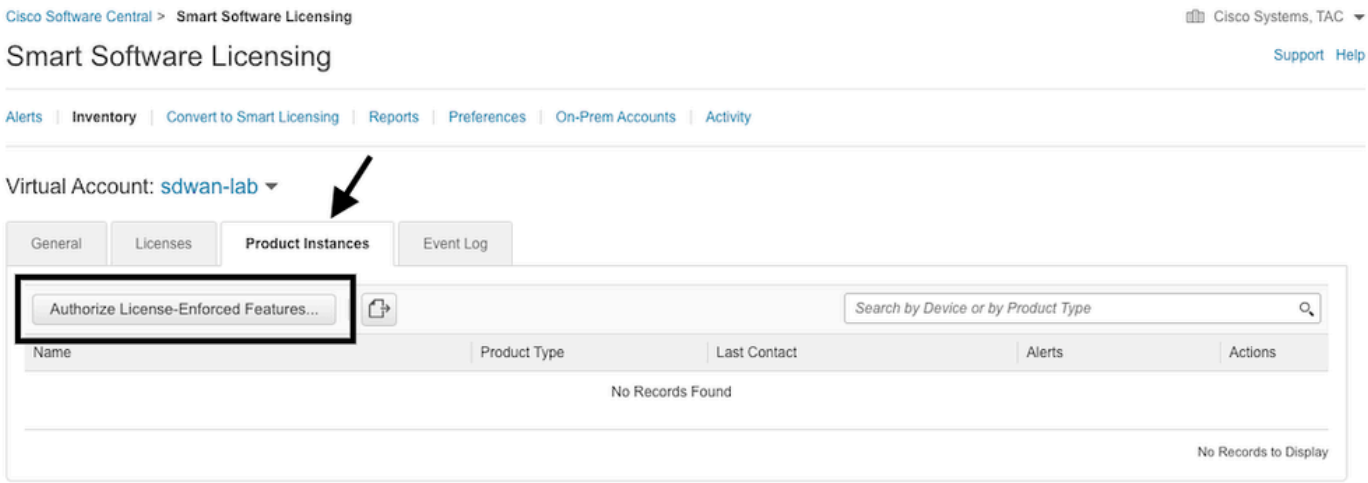
CSSMへのオフラインメソッド

インターネットへのアクセスが許可されていないエアギャップ型ネットワークでは、CSSMでSLACのローカル予約を使用して、輸出規制ライセンスのインストールを実行できます。

注：このメソッドでは、トランスポートの種類や有効なスマートURL (Uniform Resource Locator)は必要ありません。

ローカルライセンス予約の生成

ライセンスが存在する同じ仮想アカウントで、Product Instances > Authorize License-Enforced Featuresの順に移動します。



エッジルータのUDI情報の取得

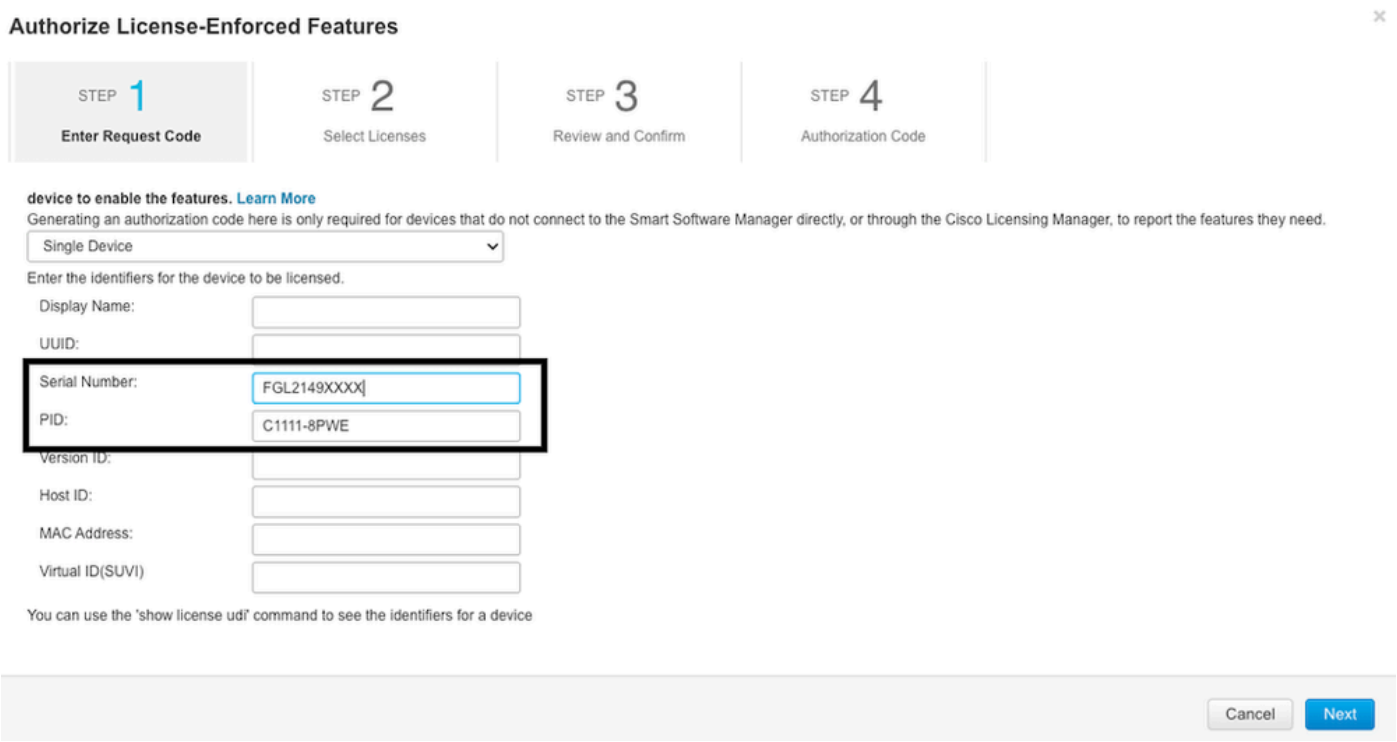
ローカルライセンスの予約には、エッジルータからのUnique Device Identifier(UDI)が必要です。**show license udi**コマンドを実行して、製品ID(PID)とシリアル番号(SN)を取得します。

<#root>

```
EdgeRouter#

show license udi

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

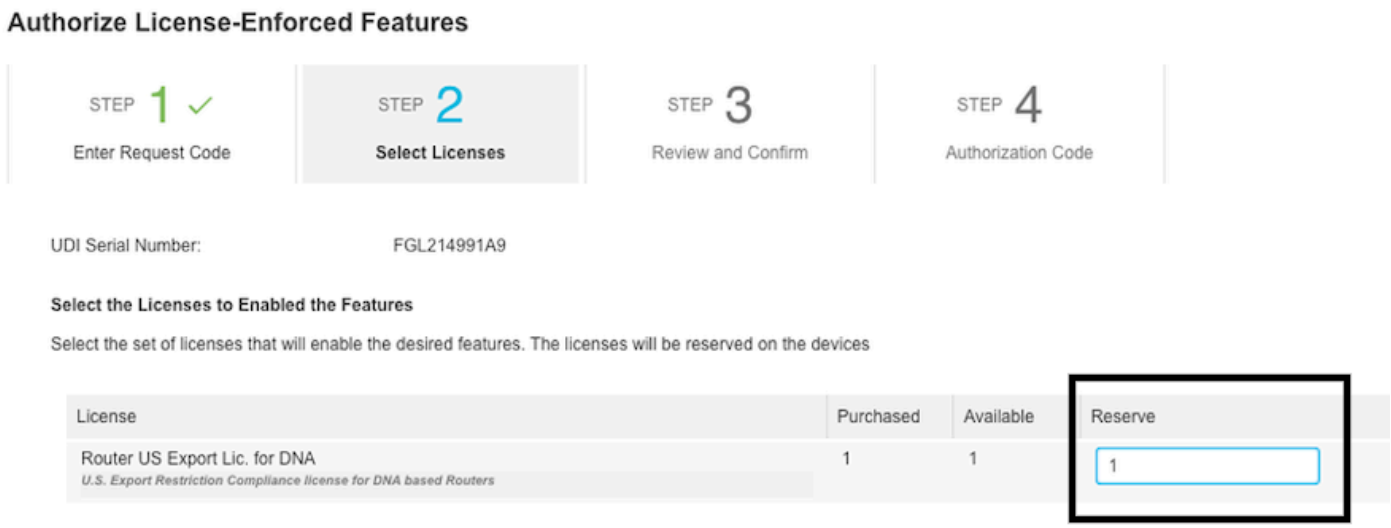
予約フォームにエッジルータのUDIを入力する

Single Deviceを選択し、エッジルータのSNとPIDを入力します。[Next] をクリックします。



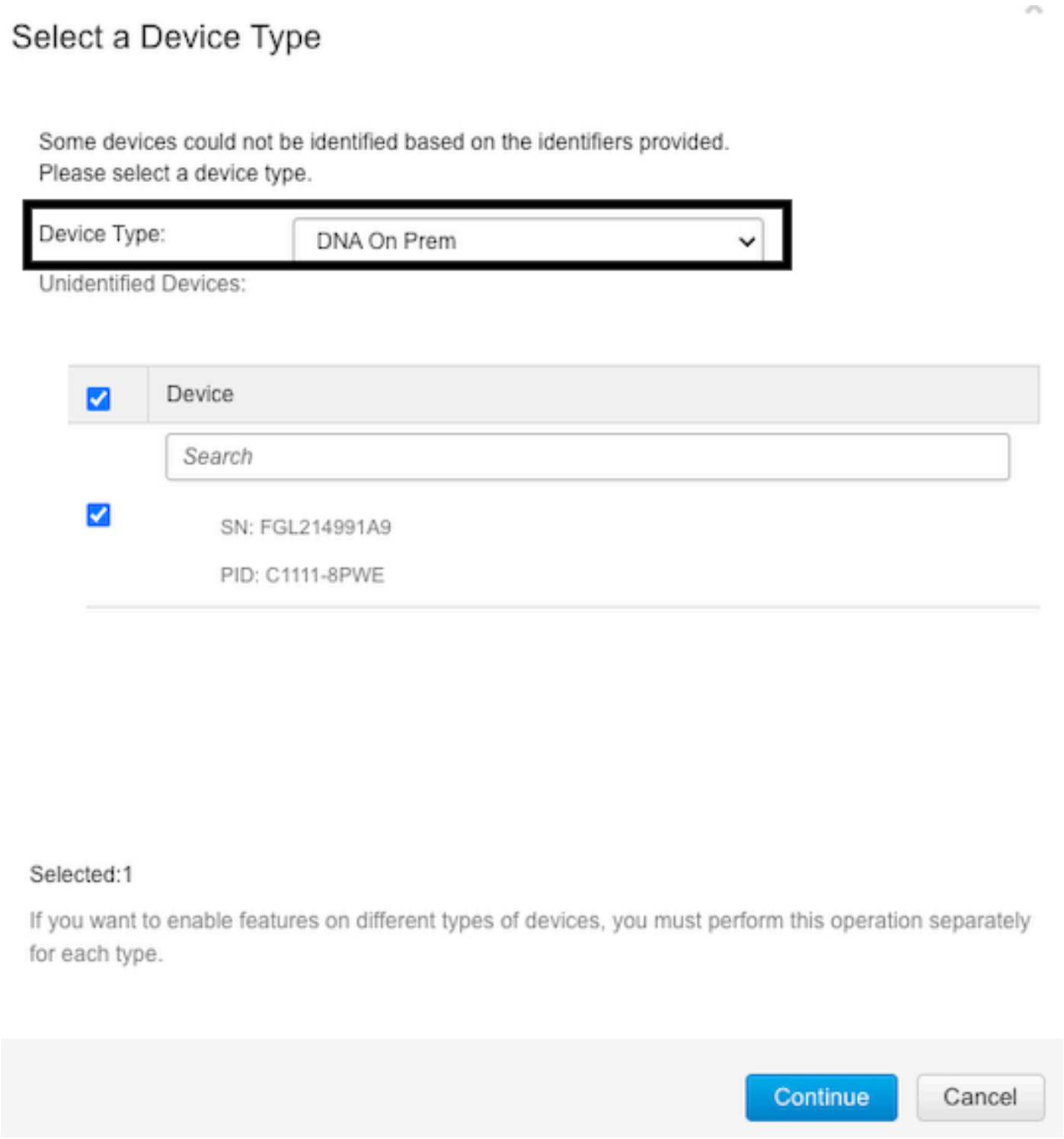
予約するライセンス数の選択

これは単一デバイスであるため、予約されているライセンスは1です。ボックスに番号を入力します。使用可能な数を超えないようにしてください。



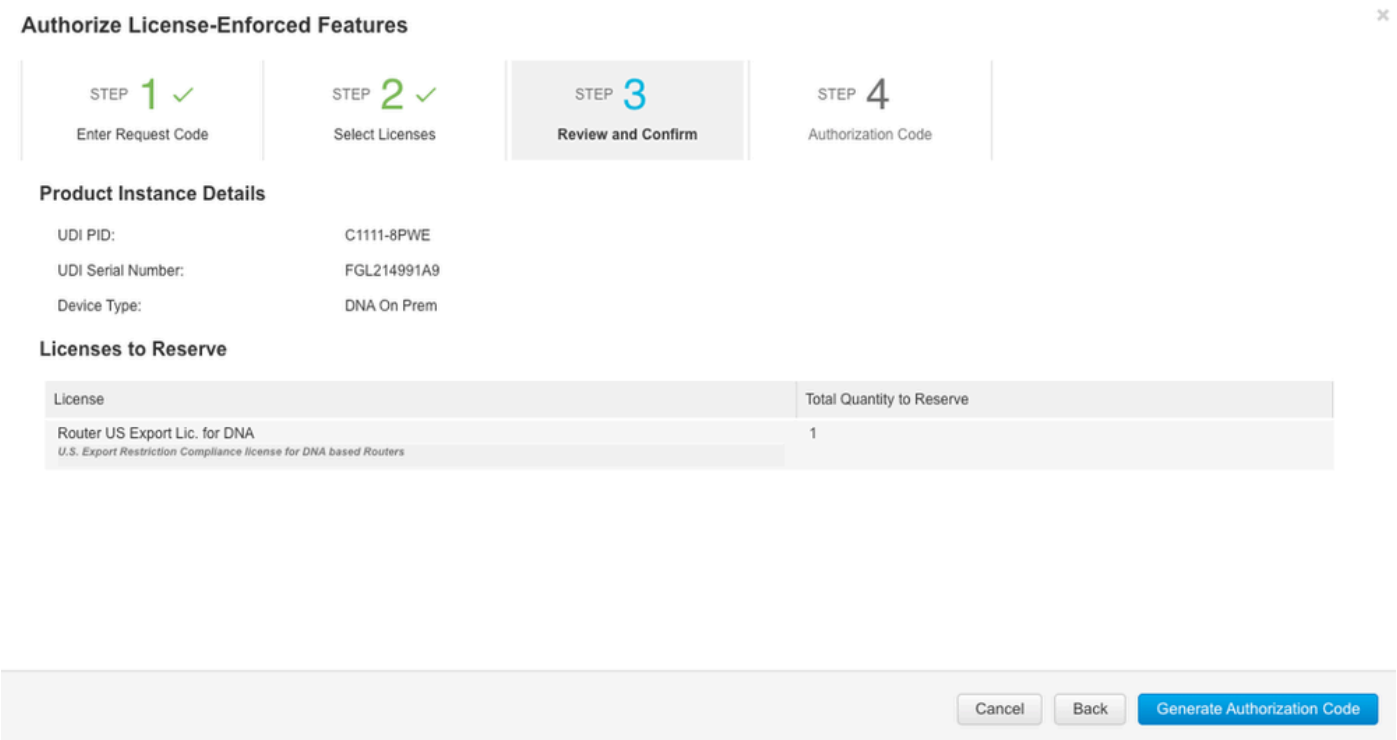
ライセンスのデバイスタイプの選択

デバイスタイプは、デジタルネットワークアーキテクチャ(Cisco DNA)オンプレミスまたはDNAクラウドのいずれかです。これは、購入したライセンスのタイプによって異なります。



認証コードの生成

設定を確認し、Generate Authorization Codeをクリックします。



SLACのダウンロード

SLACはファイルとしてダウンロードすることも、クリップボードにコピーすることもできます。

エッジルータへのSLACのコピー

SLACファイルをエッジルータにコピーするには、3つのオプションがあります。

- USBドライブ付き。

<#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)
```

- 制御接続を介したvManageでは、「エッジルータとvManageの間でのファイル転送」に移動して、詳細を確認してください。
- サービス側のSCP/FTP/TFTP。

SLACのインストール

Smart Importを使用して、ブートフラッシュにSLACファイルをインストールします。

<#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
```

が表示されてしまいます。

<#root>

```
EdgeRouter#
```

```
show logging | include SMART
```

```
*Aug 19 05:42:45.309: %SMART_LIC-6-AUTHORIZATION_INSTALL_SUCCESS: A new licensing authorization code wa
*Aug 19 05:42:45.362: %SMART_LIC-6-EXPORT_CONTROLLED: Usage of export controlled features is allowed fo
```

```
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" authorizati
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-
```

インストールが成功したことを確認する

ライセンスが正しくインストールされているかどうかを確認するには、オンライン方式と同じコマンドを使用します。

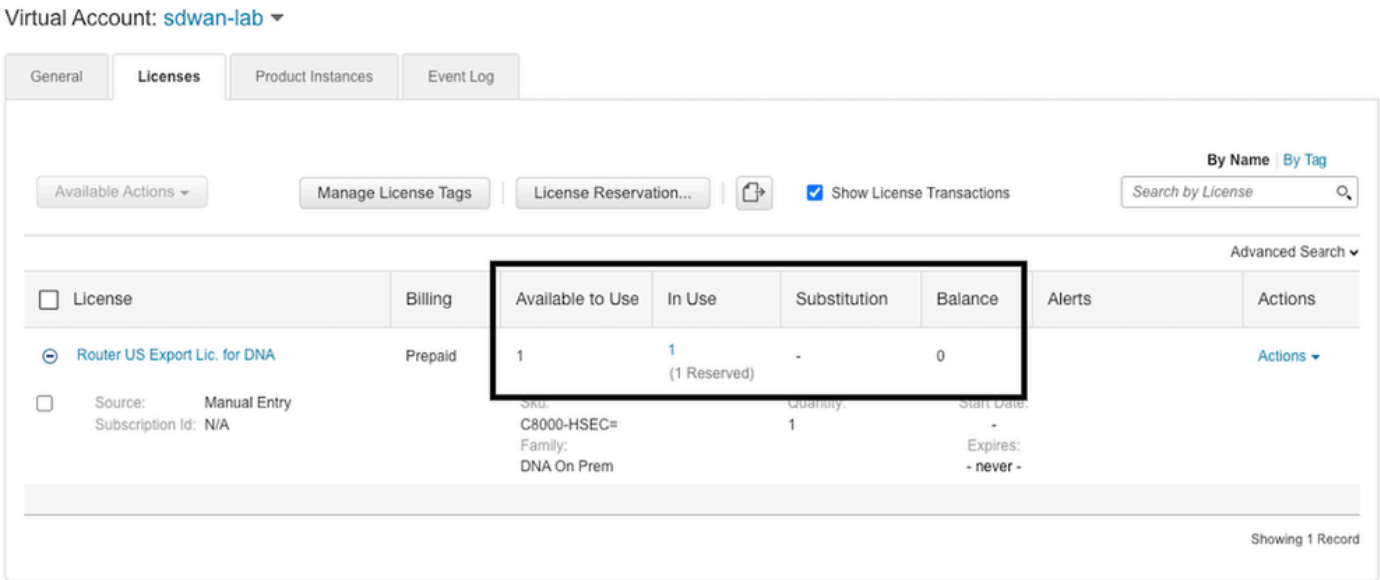
<#root>

```
show license authorization
```

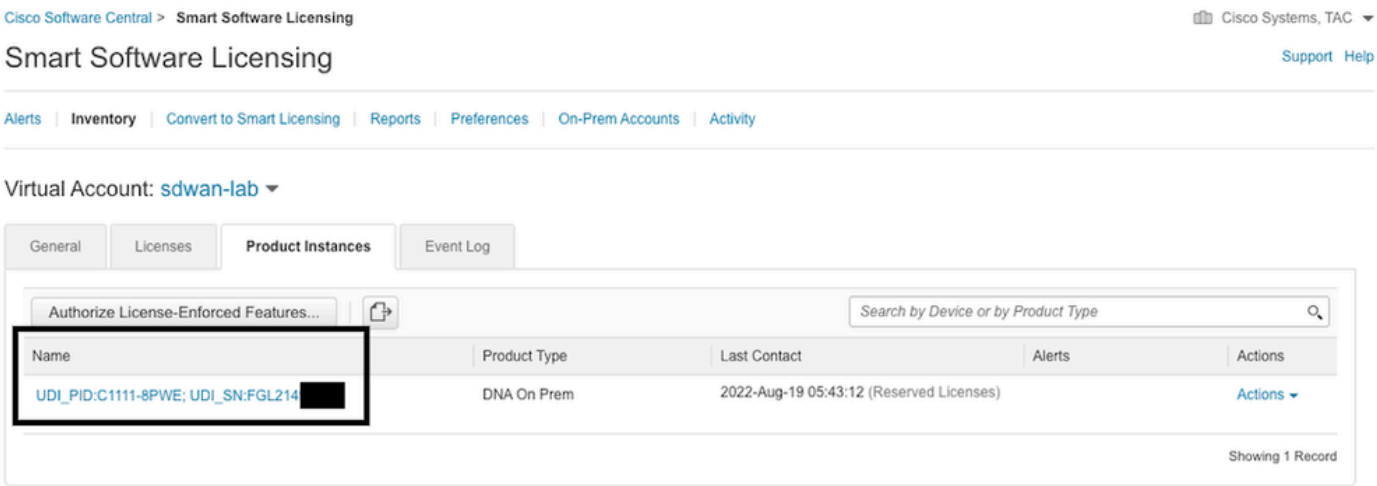
```
show license summary
```

```
show license tech support | begin License Usage
```

インストールが正しい場合、仮想アカウントのライセンスは自動的にIn Useカウンタを増分し、Available to Useカウンタを減分します。



また、製品インスタンスタブには、エッジルータのUDI情報が表示されます。エントリをクリックすると、ライセンスの特性の詳細が表示されます。



vManageワークフローメソッド

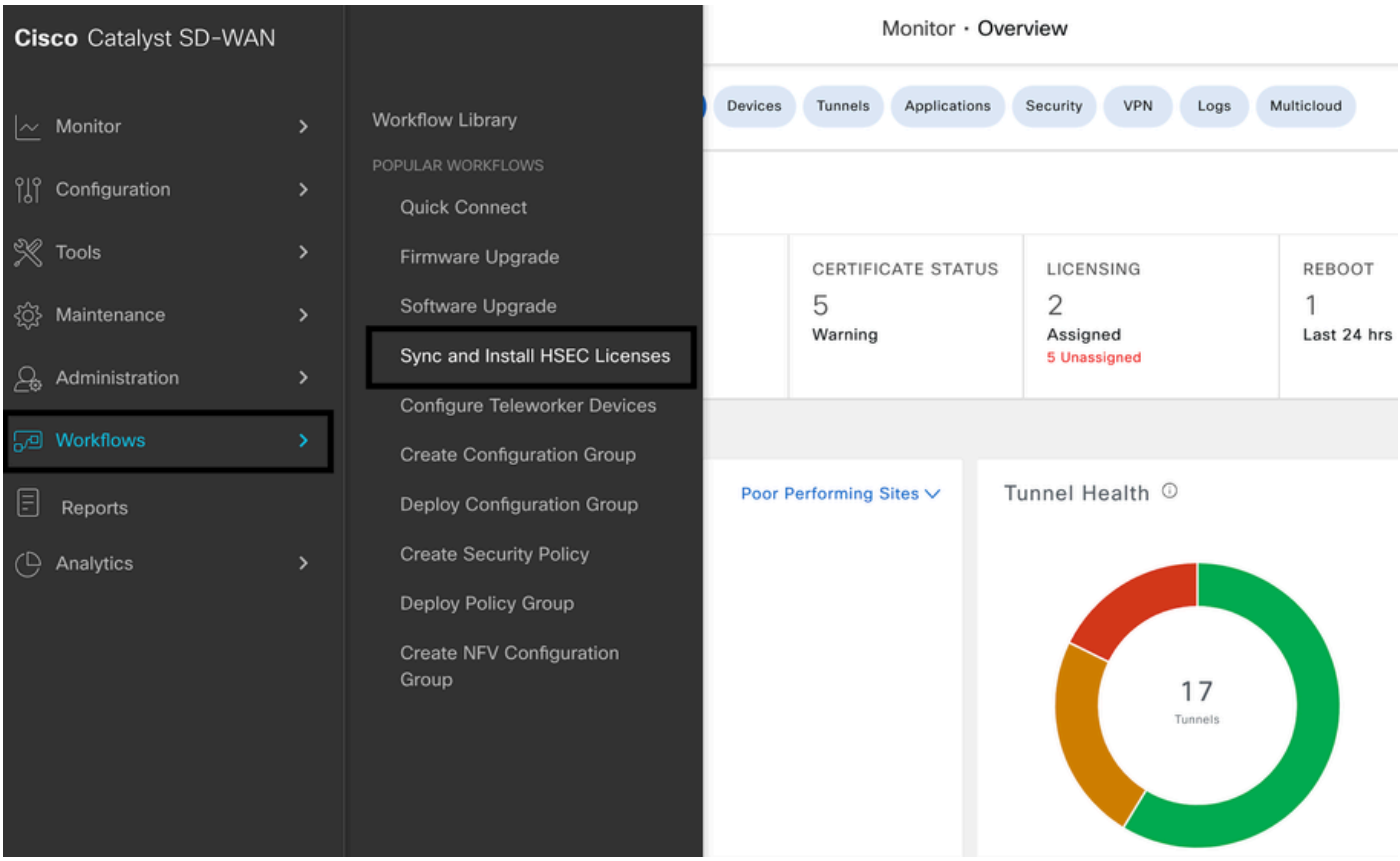
20.9.2以降では、vManageでワークフローを使用してHSECK9ライセンスをインストールできるようになりました。

注：この方法は、Router US Export Lic. for DNAライセンスでのみ機能します。ISR4300_HSECやISR4400_HSECなどのデバイス固有のHSECライセンスは機能しません。デバイス固有のHSECライセンスをCisco DNA HSECに変換する方法の詳細については、「HSECライセンスの管理に関する制限事項」セクションを参照してください。

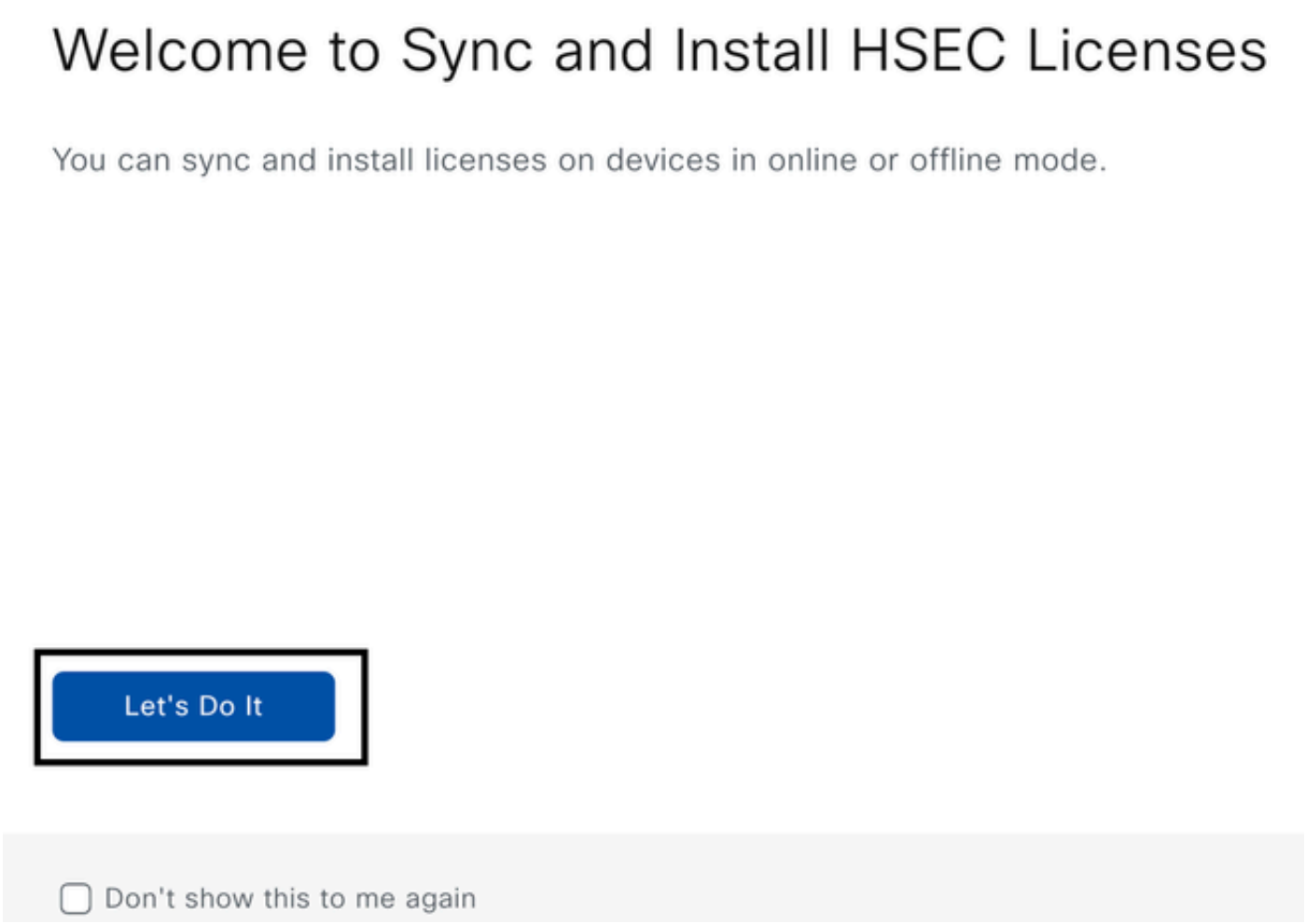
オンラインワークフロー

ライセンスとCSSMの同期

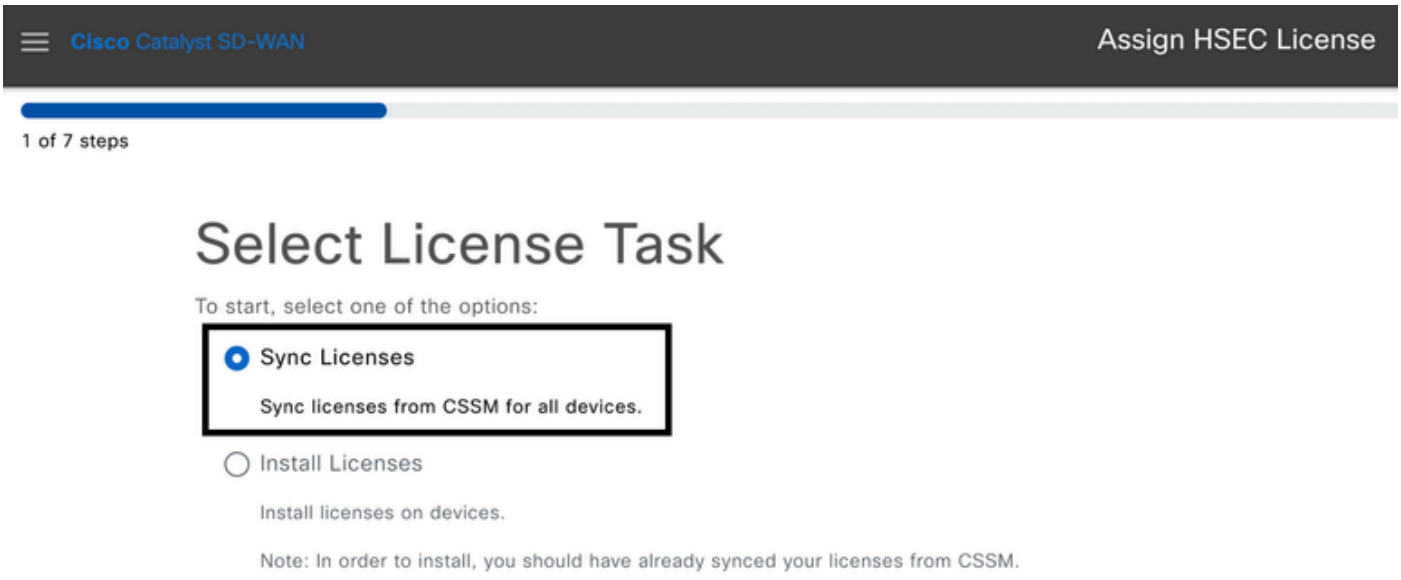
1.- vMange GUIで、Main Menu > Workflows > Sync and Install HSEC Licensesの順に移動します。



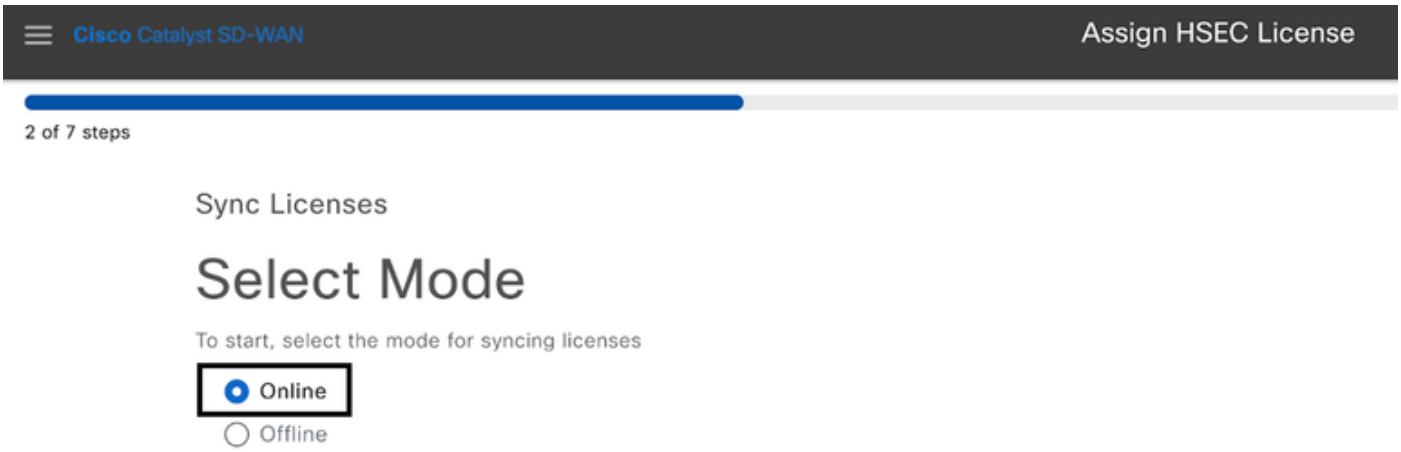
2. – ポップアップウィンドウでLet's Do itボタンをクリックします。



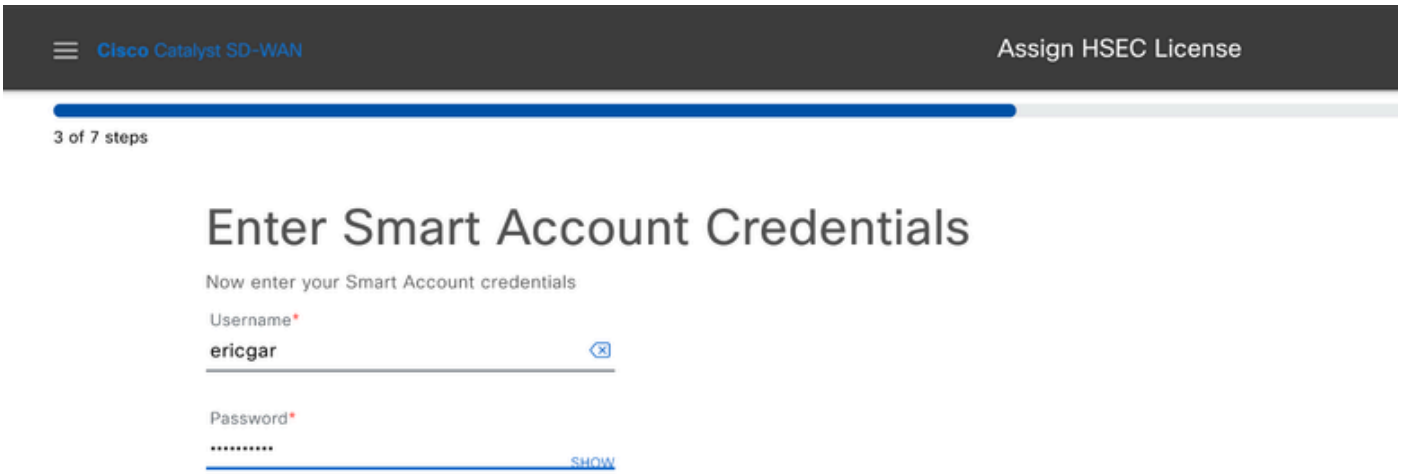
3.- Sync Licensesタスクを選択し、Nextをクリックします。



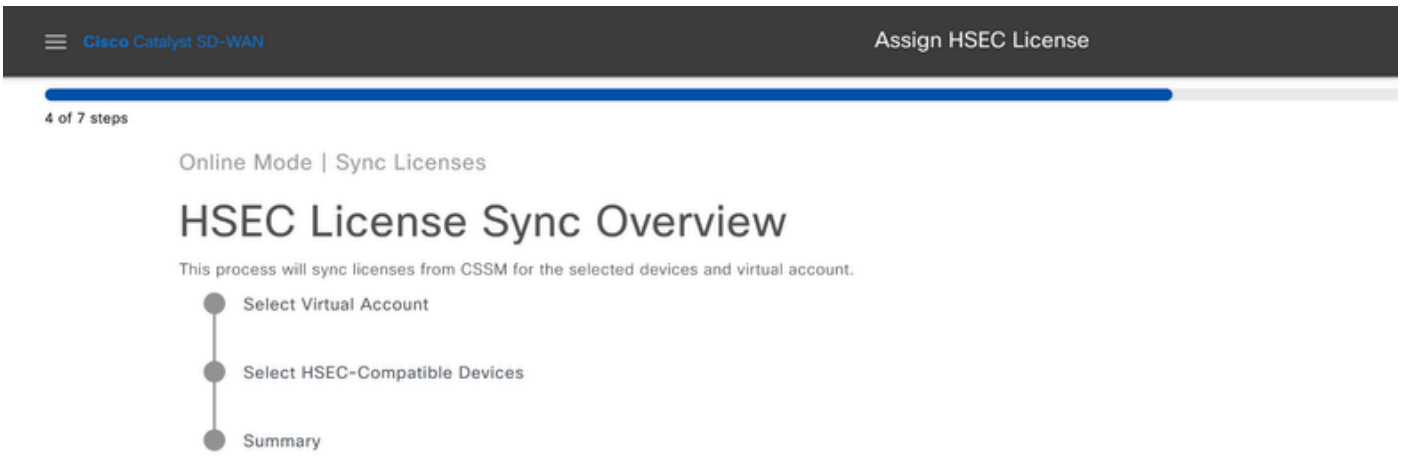
4.- Online modeを選択し、Nextをクリックします。



5- Cisco CSSMクレデンシャルを入力し、Nextをクリックします。



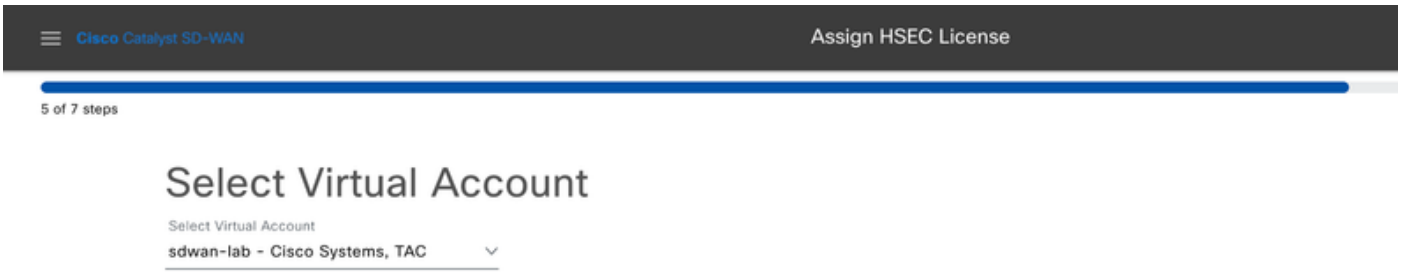
6.- HSEC License Sync Overviewを確認し、Nextをクリックします。



7.- vManageがクラウドに接続し、利用可能なすべての仮想アカウントを照会します。有効な正数

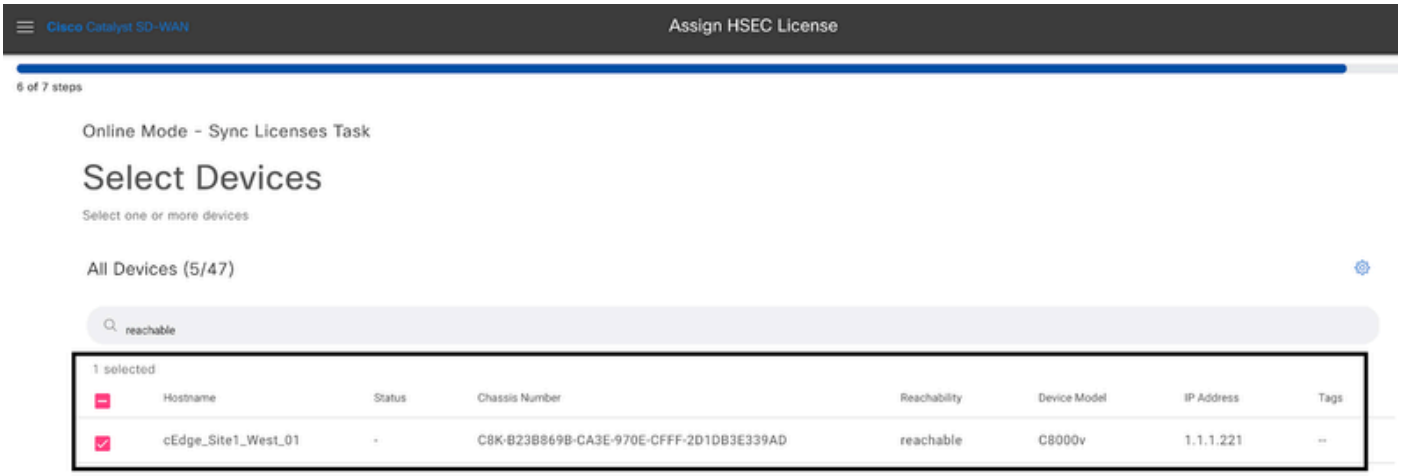
のHSECライセンスを含む仮想アカウントをドロップダウンから選択します。

注：手順6で入力したクレデンシャルには、HSECライセンスが格納されるスマートアカウントと仮想アカウントの管理者ロールが必要です。

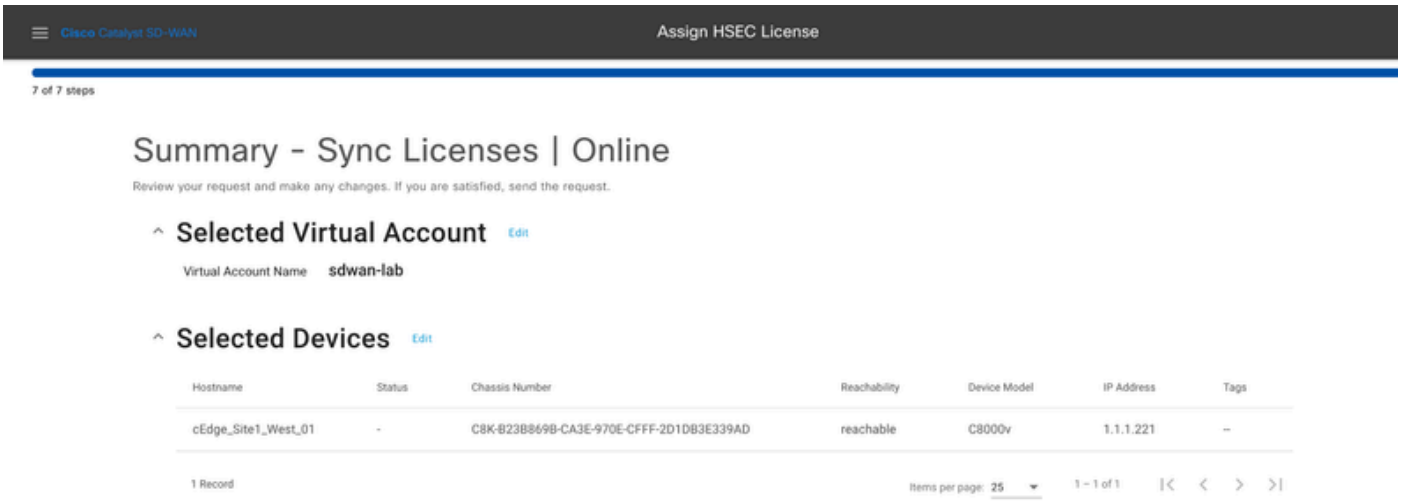


8.- HSECライセンスをインストールする対象のデバイスを選択します。

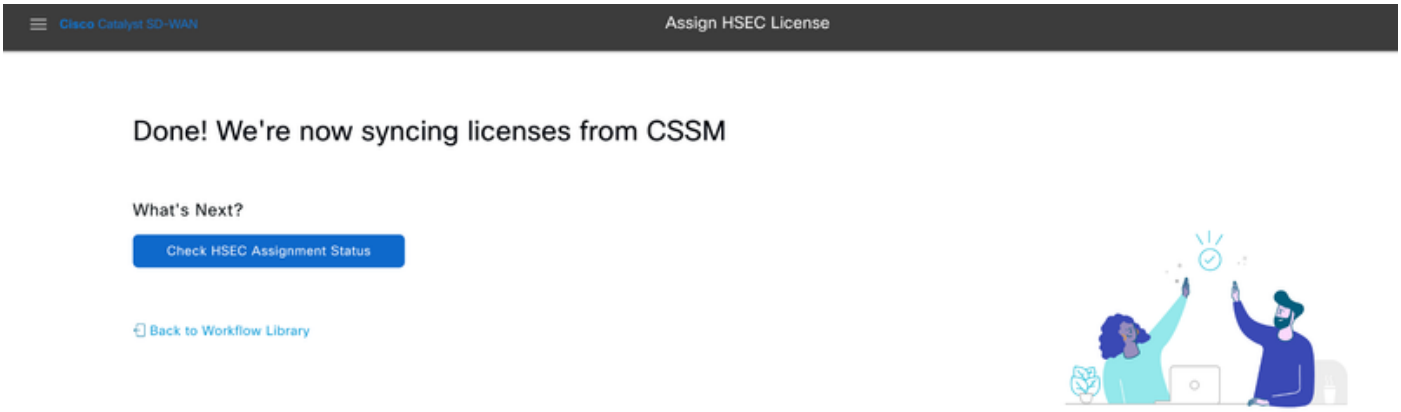
注:HSECと互換性のあるデバイスのみが表示されます。



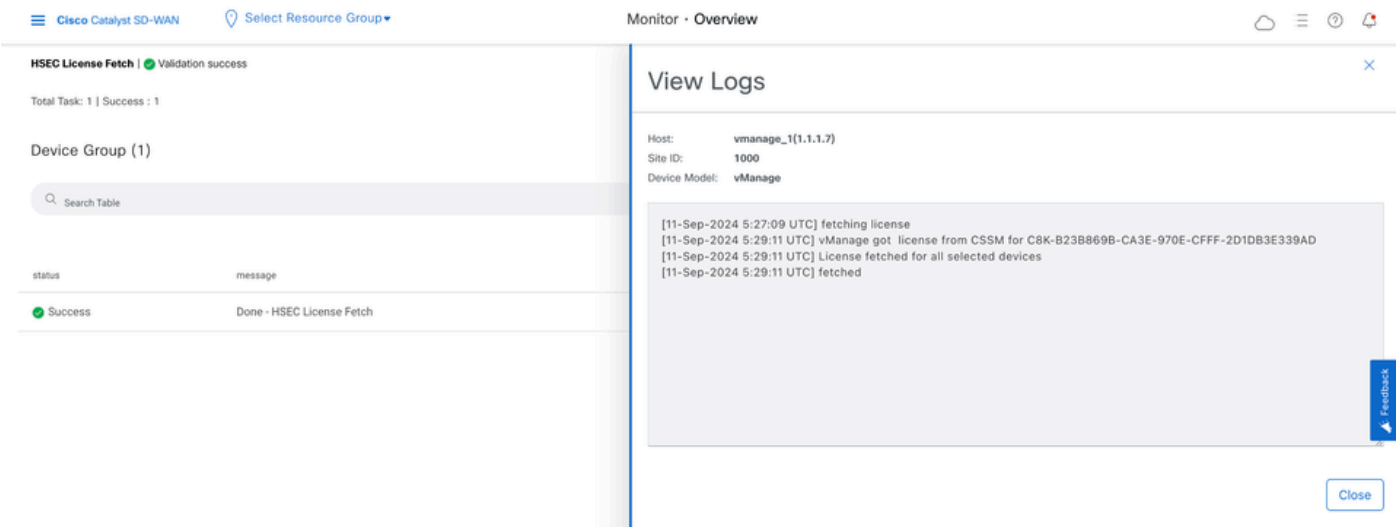
9. – 要求の要約を確認し、Syncをクリックします。



10.- Check HSEC Assignment Statusをクリックして、SLAC予約をリアルタイムで確認します。

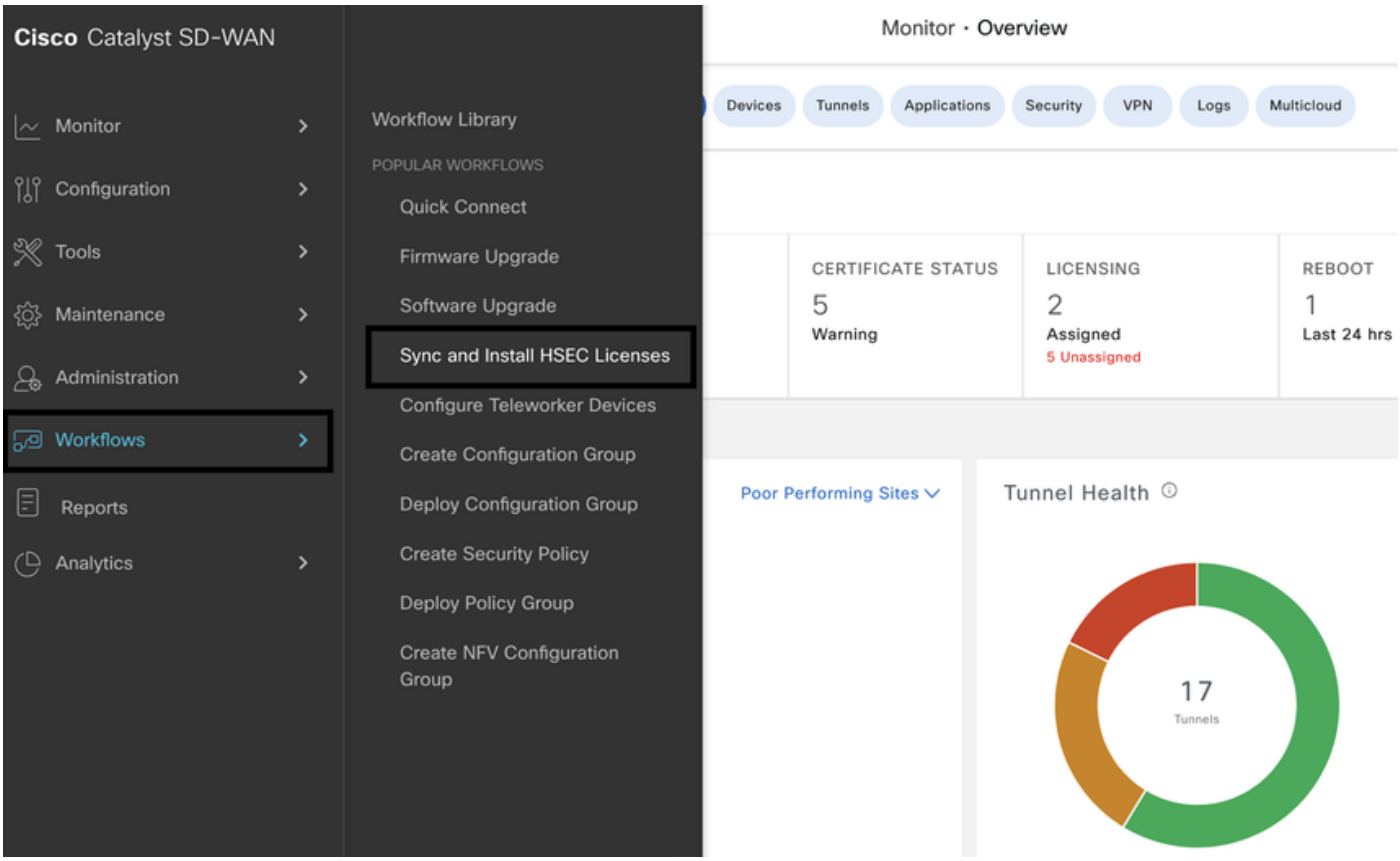


11. – ライセンスがCSSMからフェッチされ、vManageに保存されると、ステータスはSuccessと表示されます。

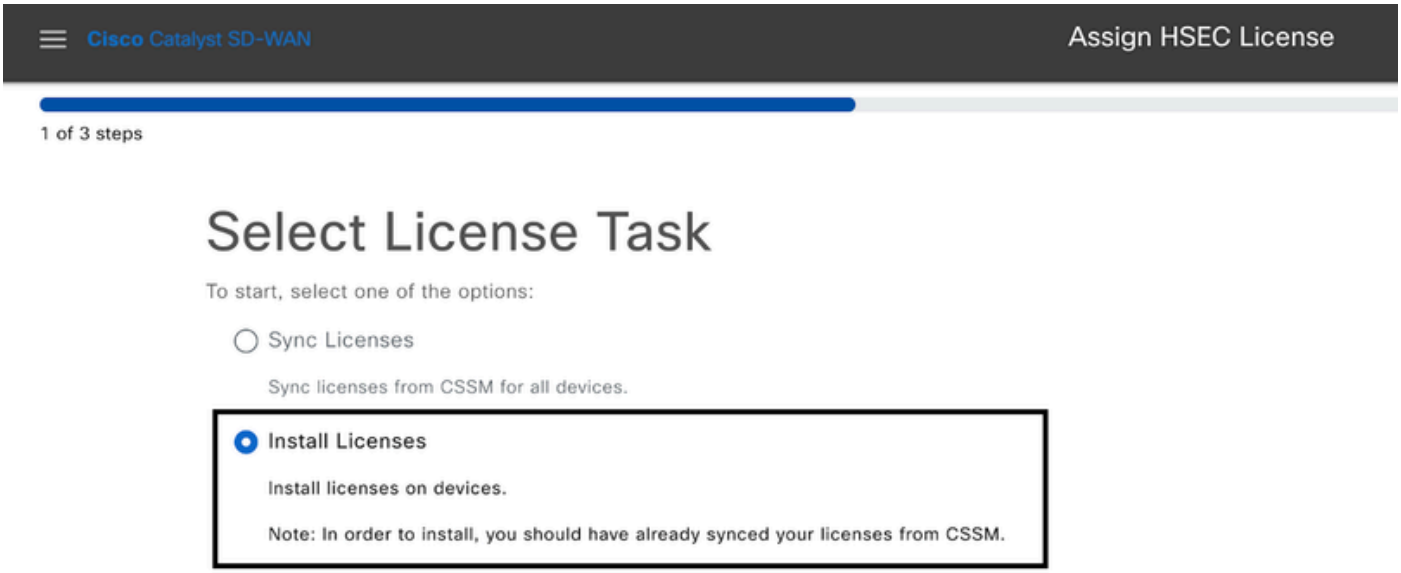


取得したライセンスのインストール

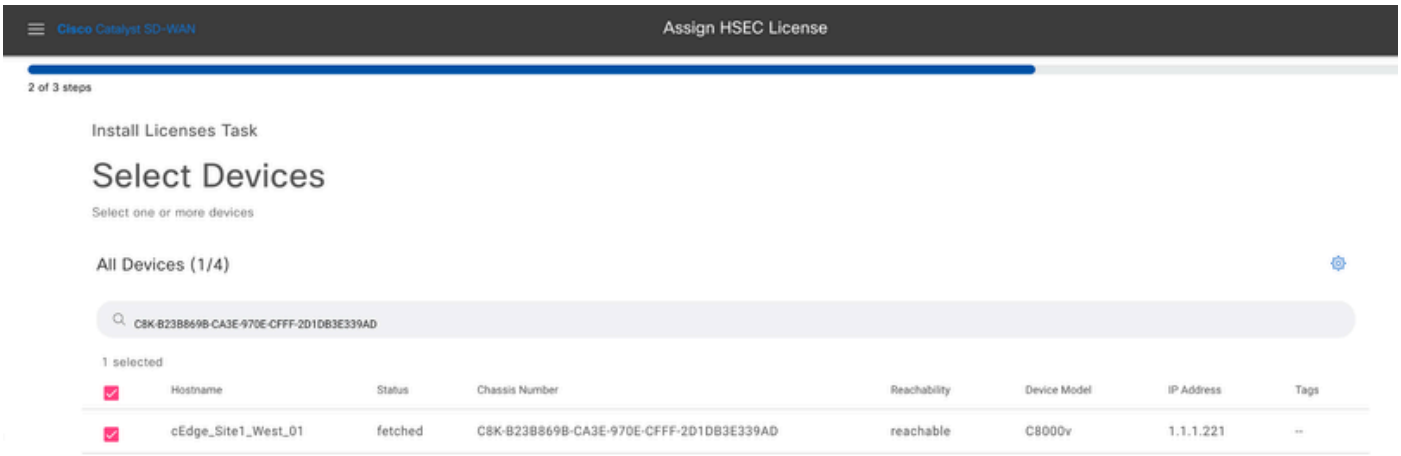
1.- vMange GUIで、Main Menu > Workflows > Sync and Install HSEC Licensesの順に移動します。



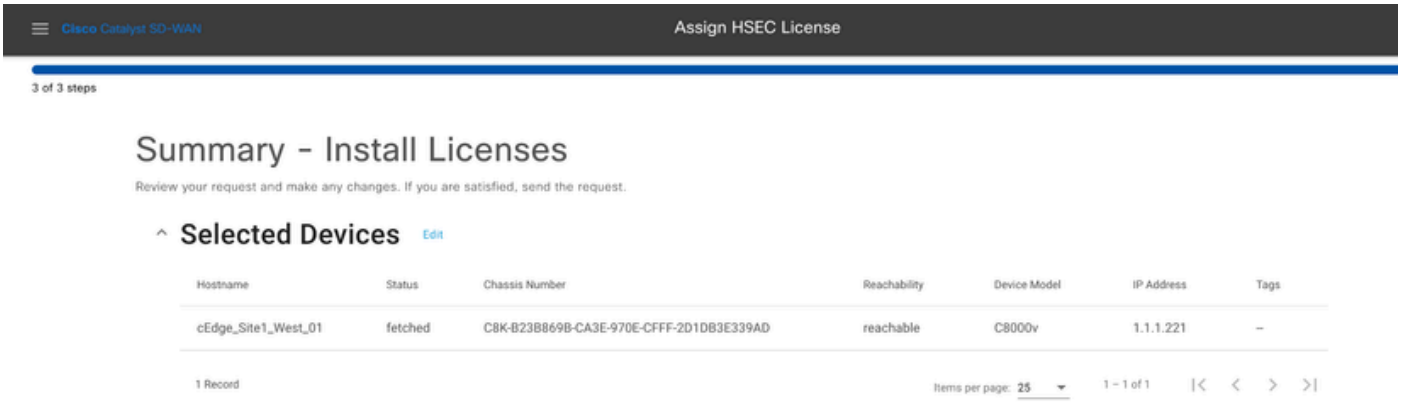
2.- Install Licensesタスクを選択します。



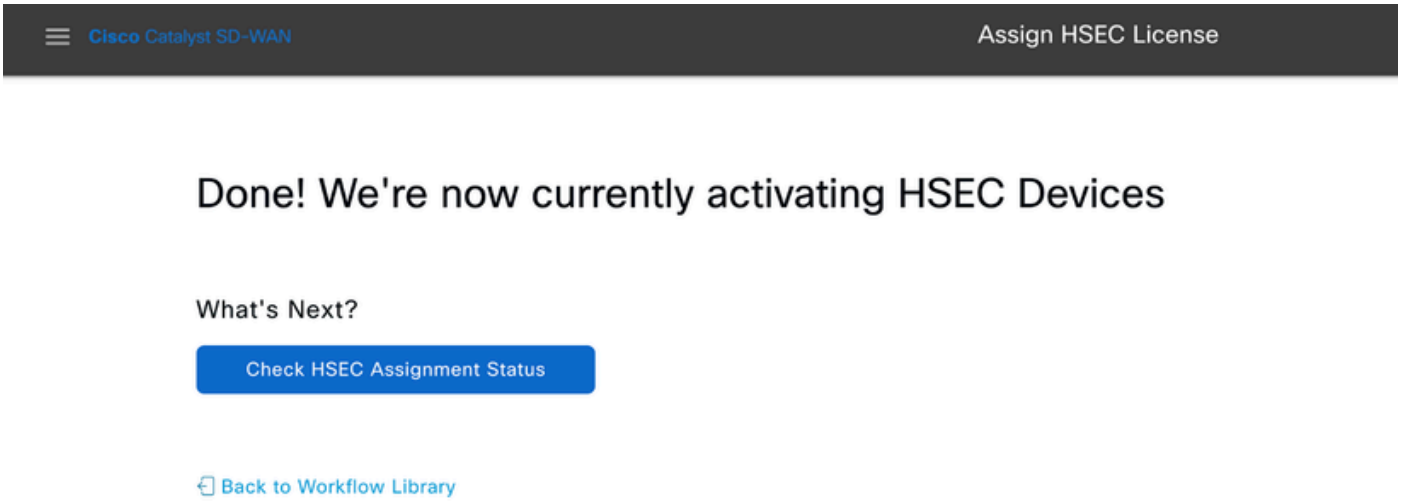
3.- HSECライセンスがフェッチされたデバイスを選択します。



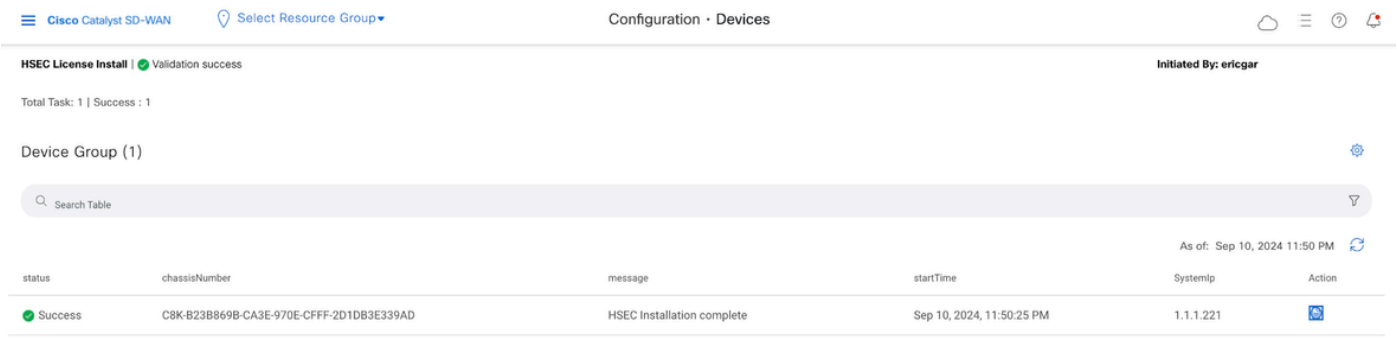
4. – インストールの概要を確認し、Installをクリックします。



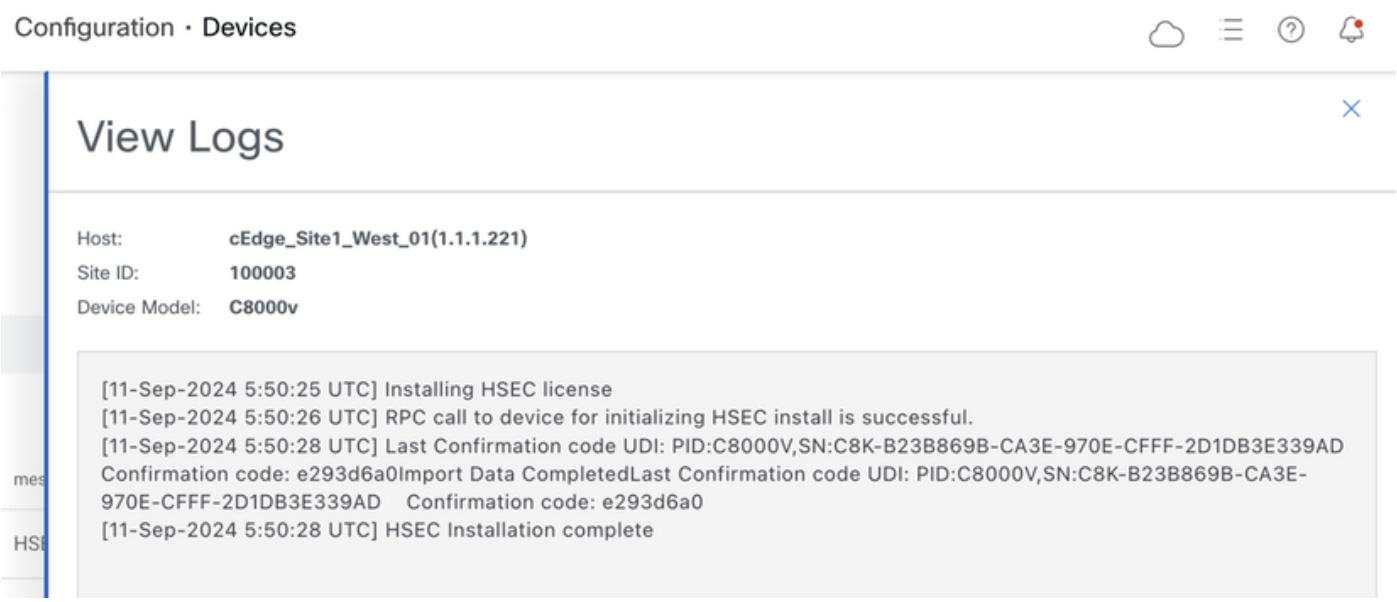
5.- Check HSEC Assignment Statusをクリックして、リアルタイムでインストールステータスを確認します。



6.- vManageはルータと通信し、ルータにSLACを送信してインストールします。最後のステータスはSuccessである必要があります。



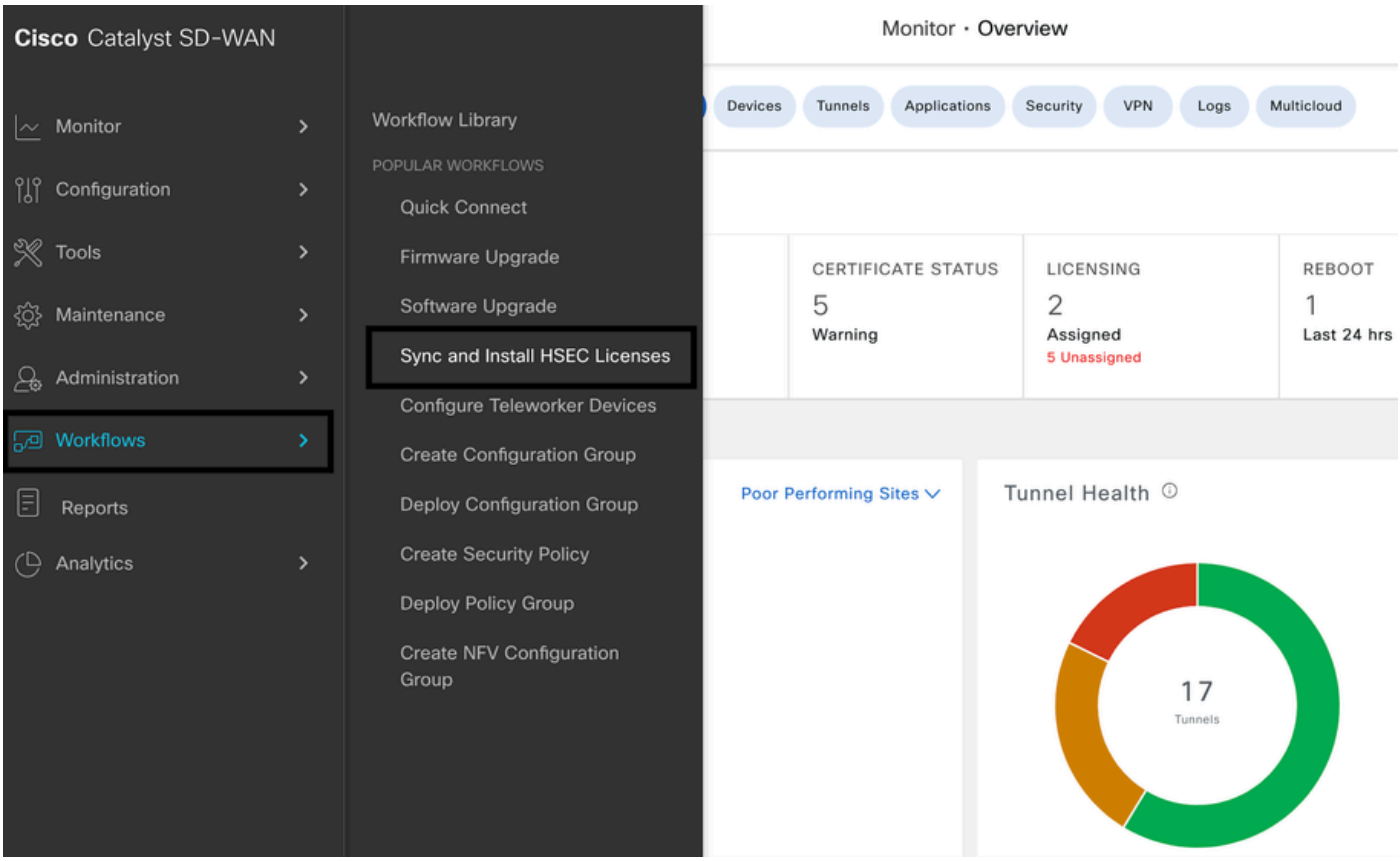
7.- Actionアイコンをクリックして、HSECのインストールに関するより詳細なログを表示します。



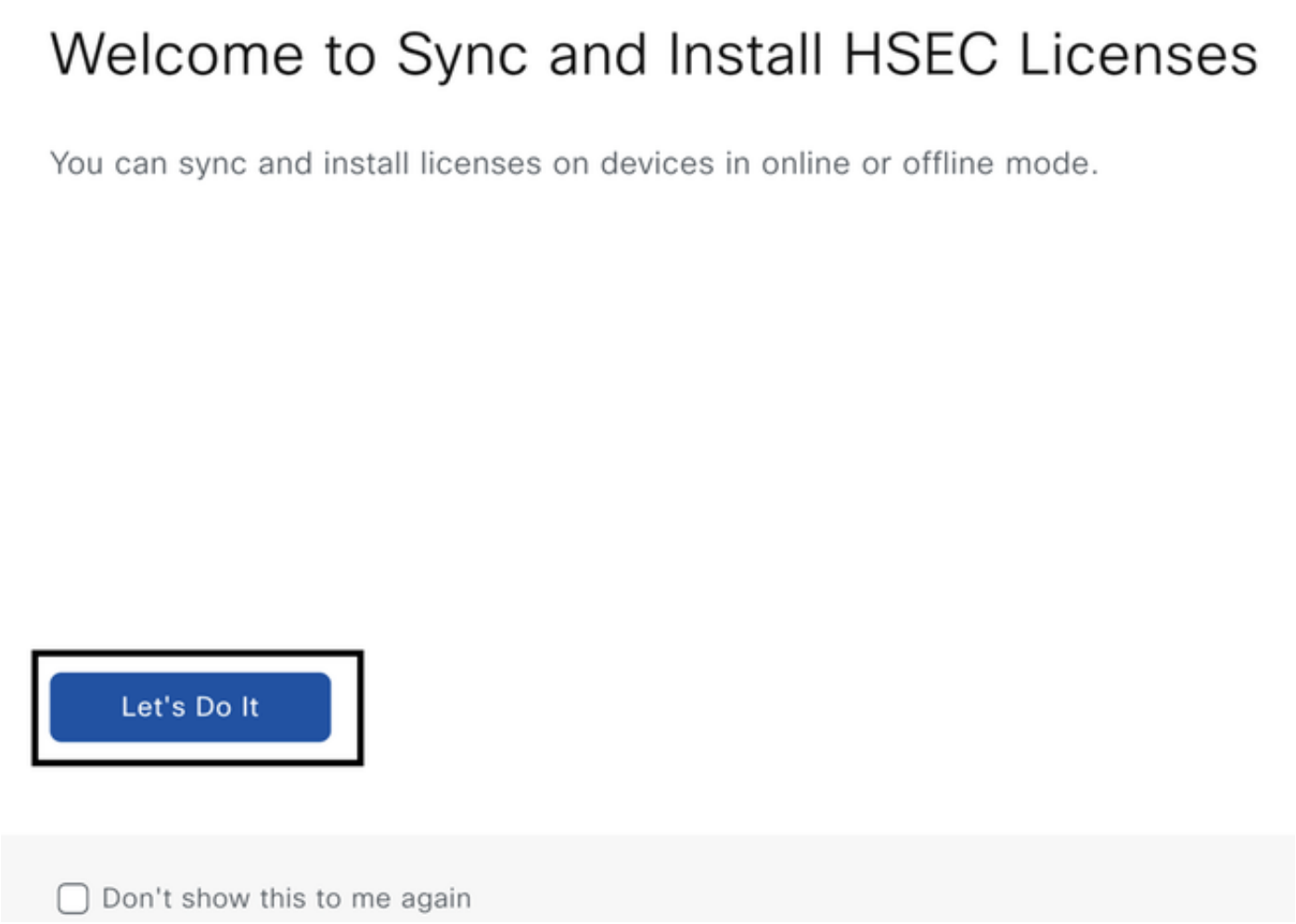
オフラインワークフロー

ライセンスとCSSMの同期

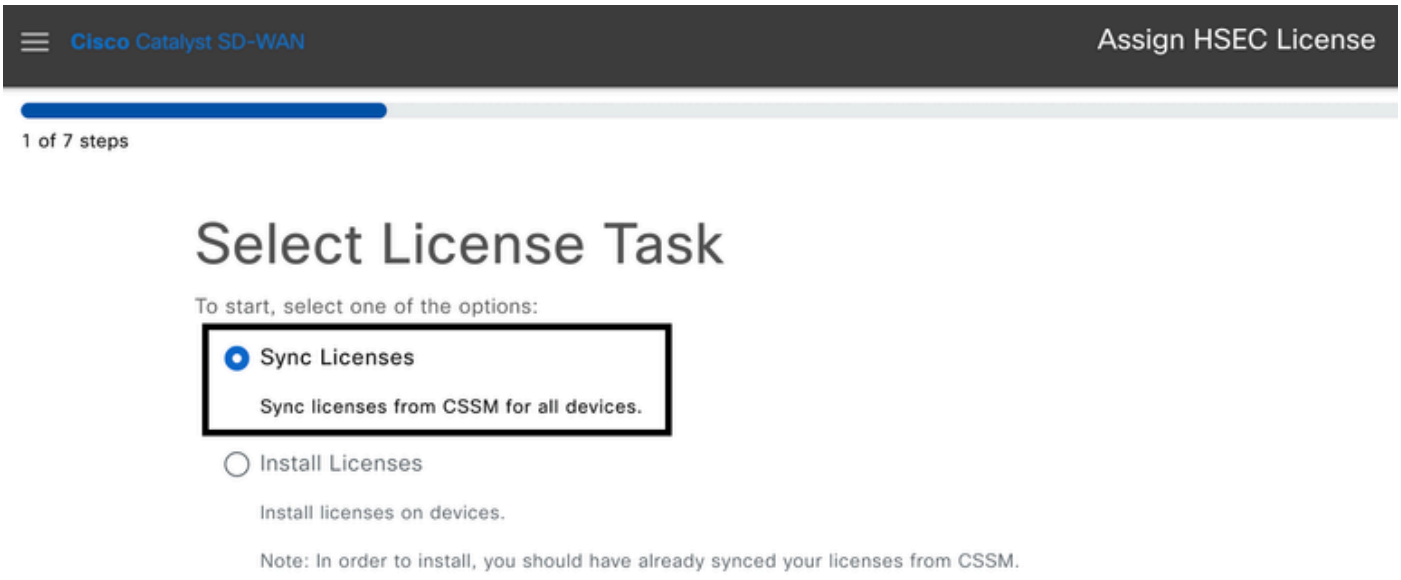
1.- vMange GUIで、Main Menu > Workflows > Sync and Install HSEC Licensesの順に移動します。



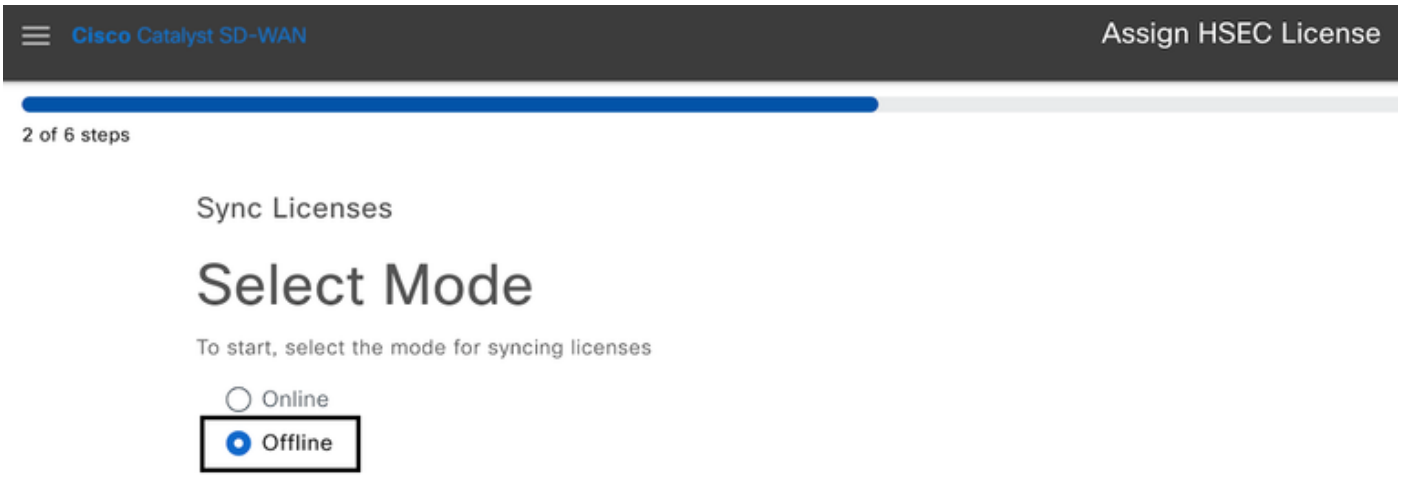
2. – ポップアップウィンドウでLet's Do itボタンをクリックします。



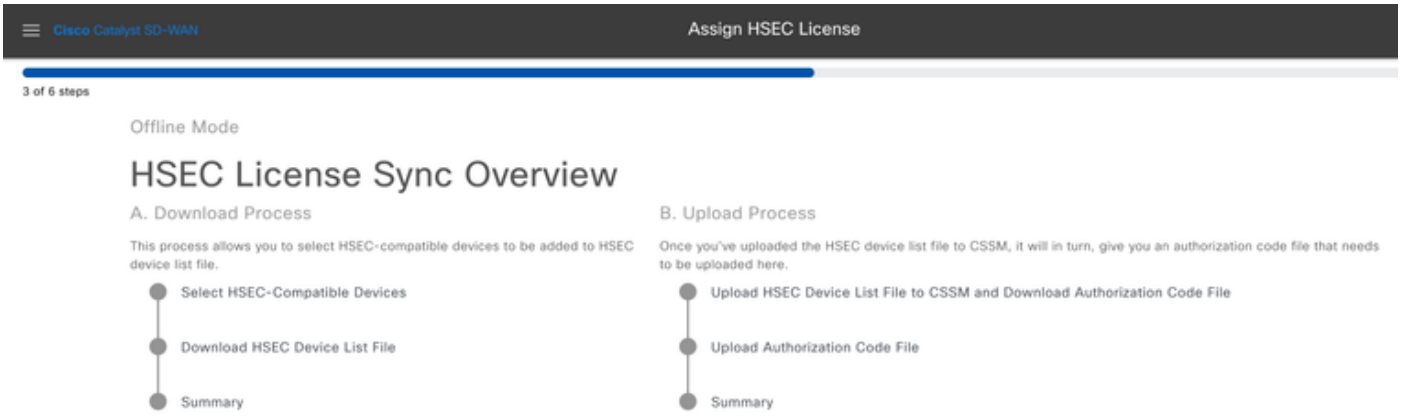
3.- Sync Licensesタスクを選択し、Nextをクリックします。



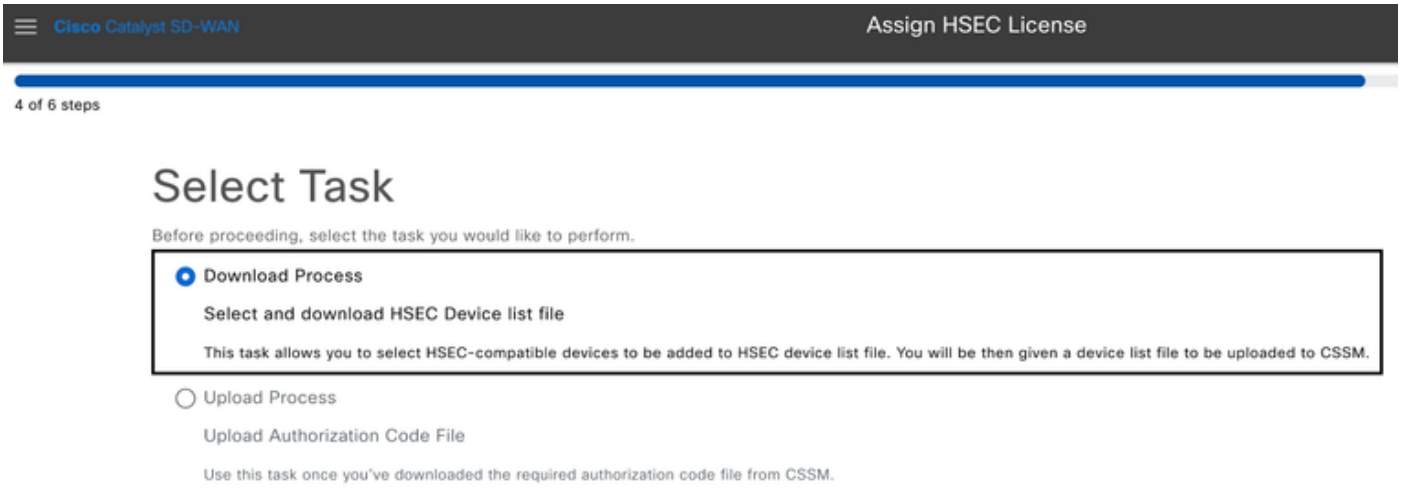
4.- Offline modeを選択し、Nextをクリックします。



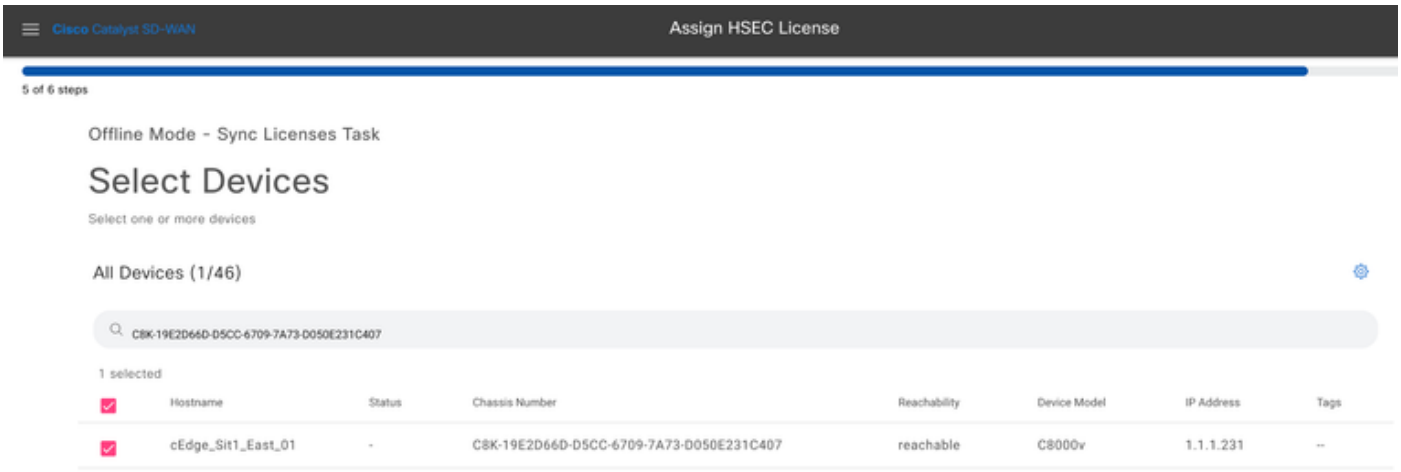
5. – プロセスの概要を注意深く確認し、Nextをクリックします。



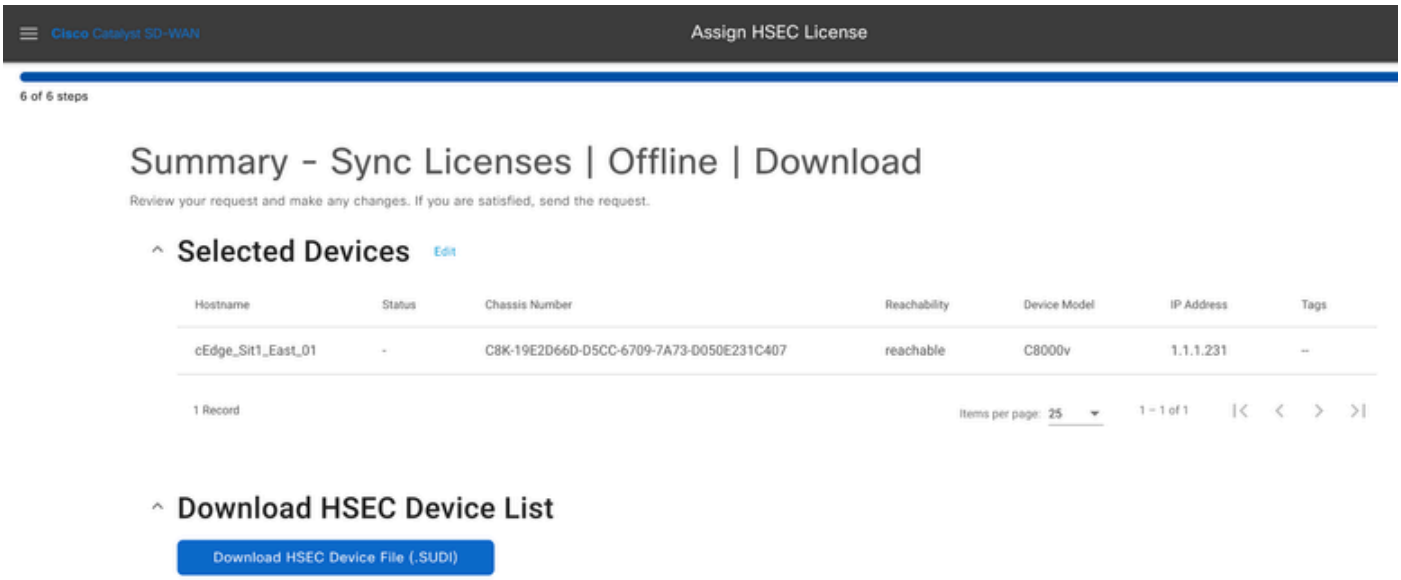
6.- Download Processオプションを選択し、Nextをクリックします。



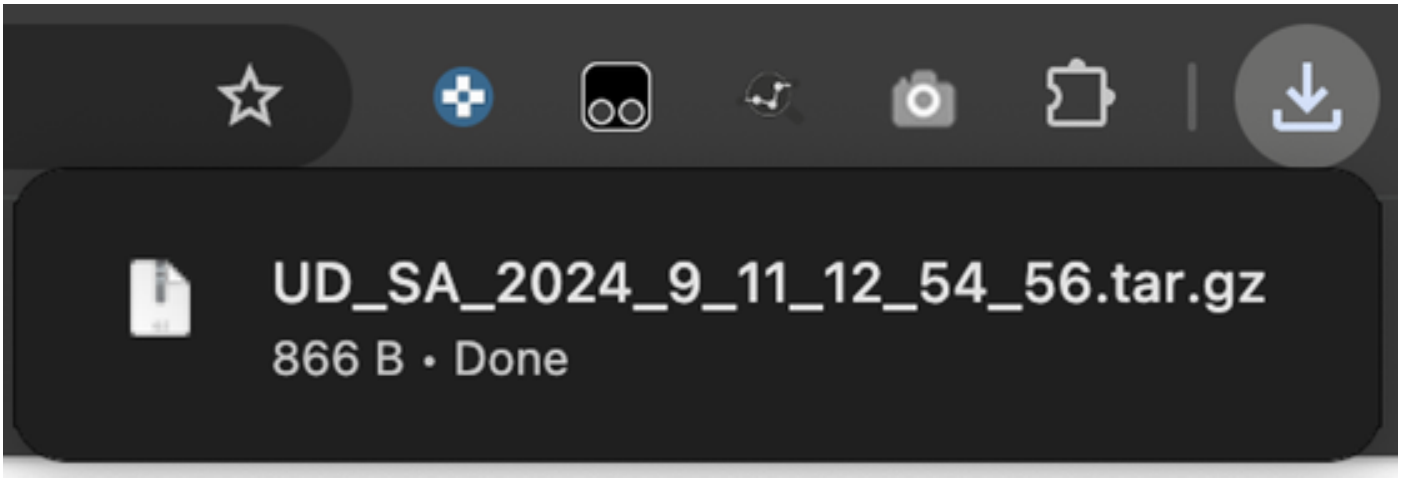
7. – 検索バーで、ライセンスをインストールするデバイスをフィルタリングします。



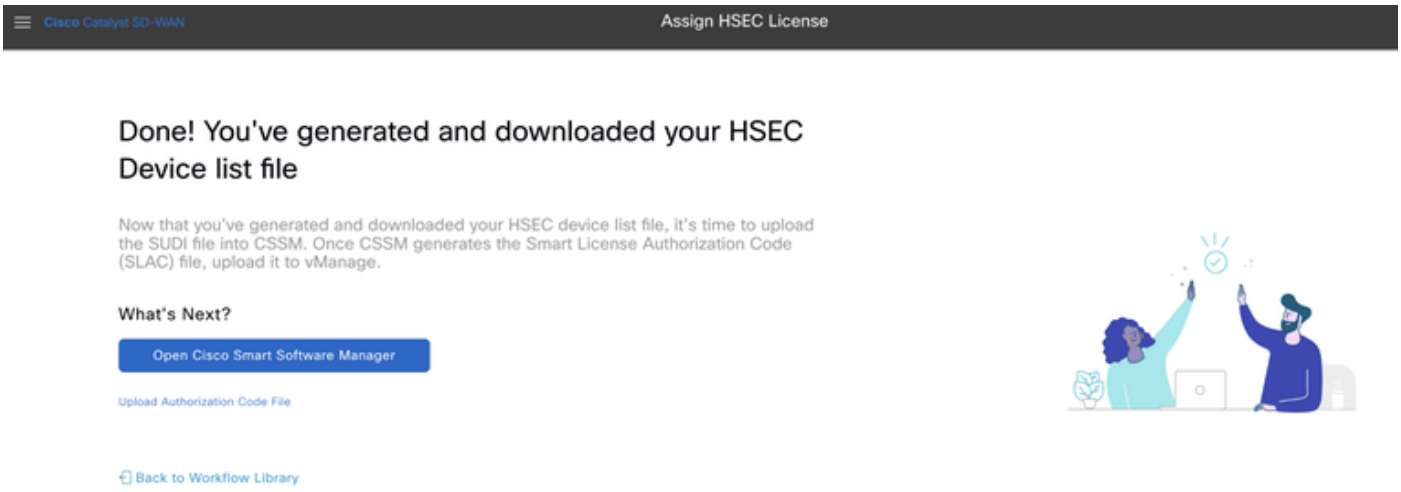
8. – タスクの概要を確認し、Download HSEC Device File (.SUDI)をクリックします。



9. – ライセンス使用状況の自動ダウンロードが開始されます。

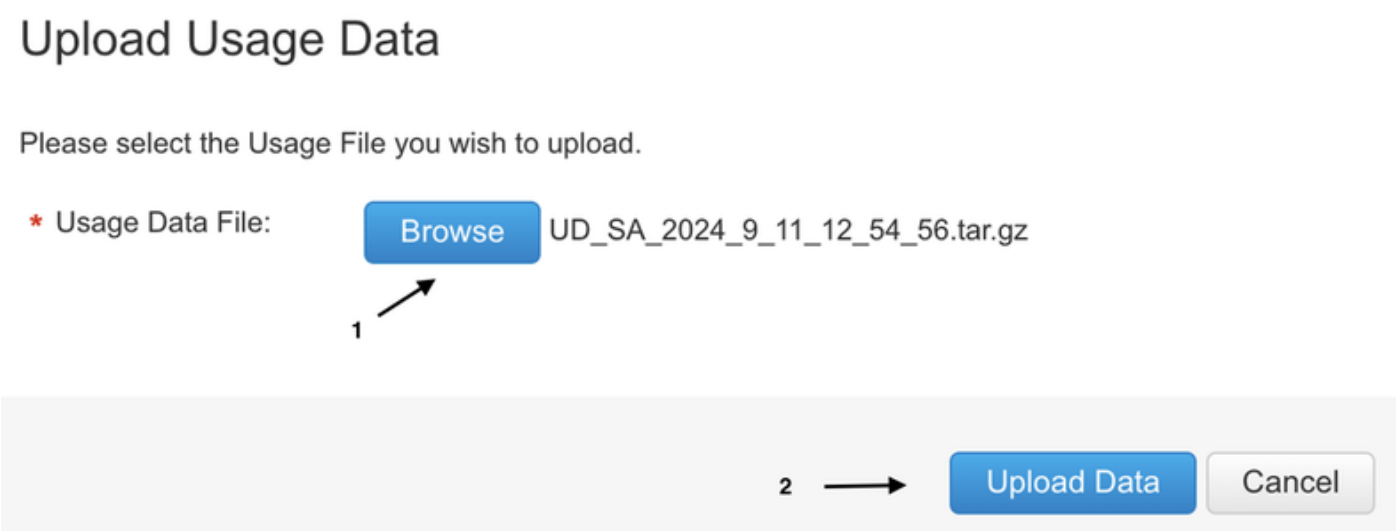


10.- Open Cisco Smart Software Managerをクリックするか、Cisco Software Centralに移動します。



11. – 選択したスマートアカウントで、Cisco Software Central > Smart Software Licensingに移動し、Reports > Usage Data Files > Upload Usage Data...の順にクリックします。

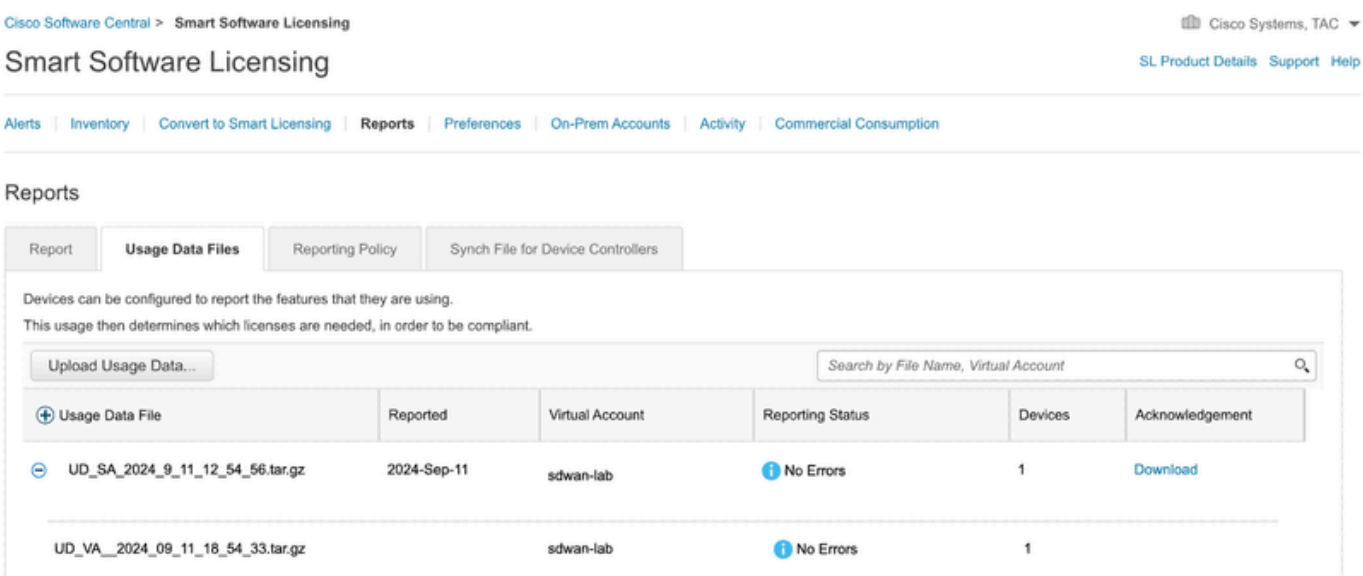
12.- Upload Usage DataポップアップでBrowseをクリックし、ダウンロードしたばかりのファイルを選択してUpload Dataをクリックします。



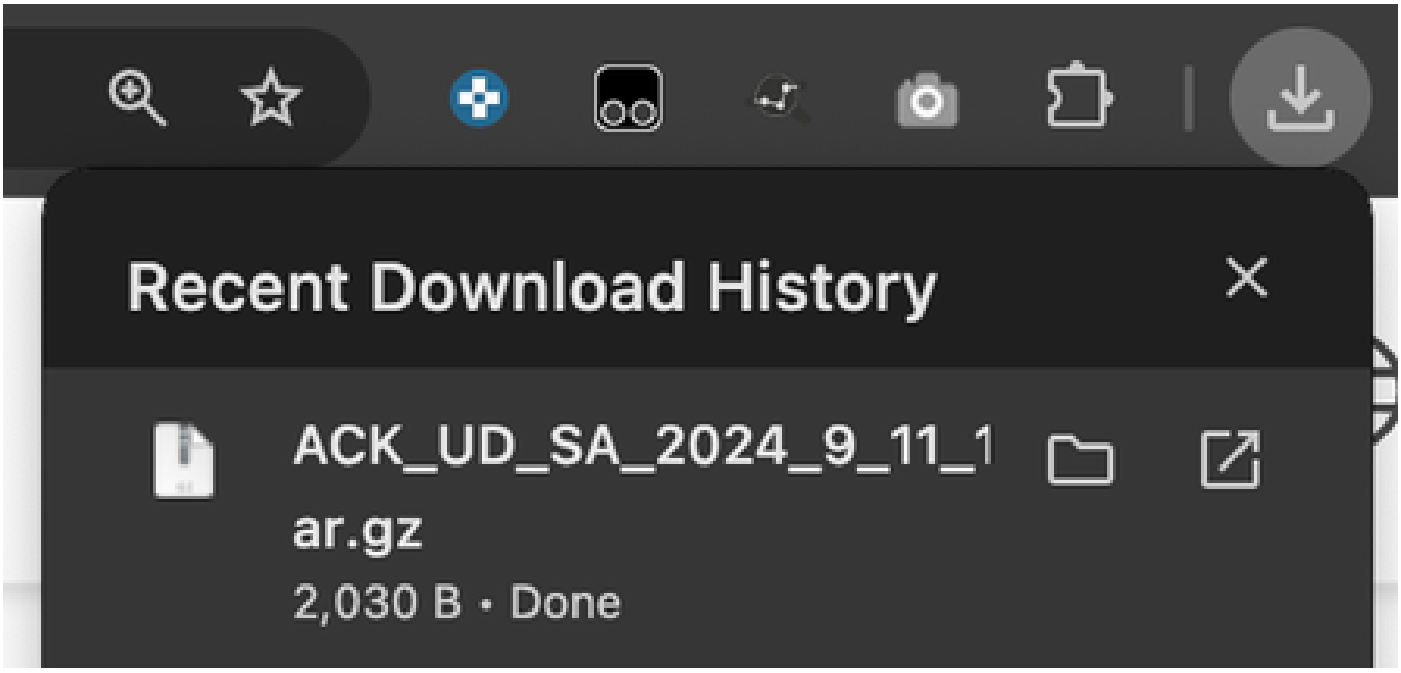
13. – システムがファイルの処理を開始します。所要時間は約5 ~ 10分です。次にDownloadをク

リックします。

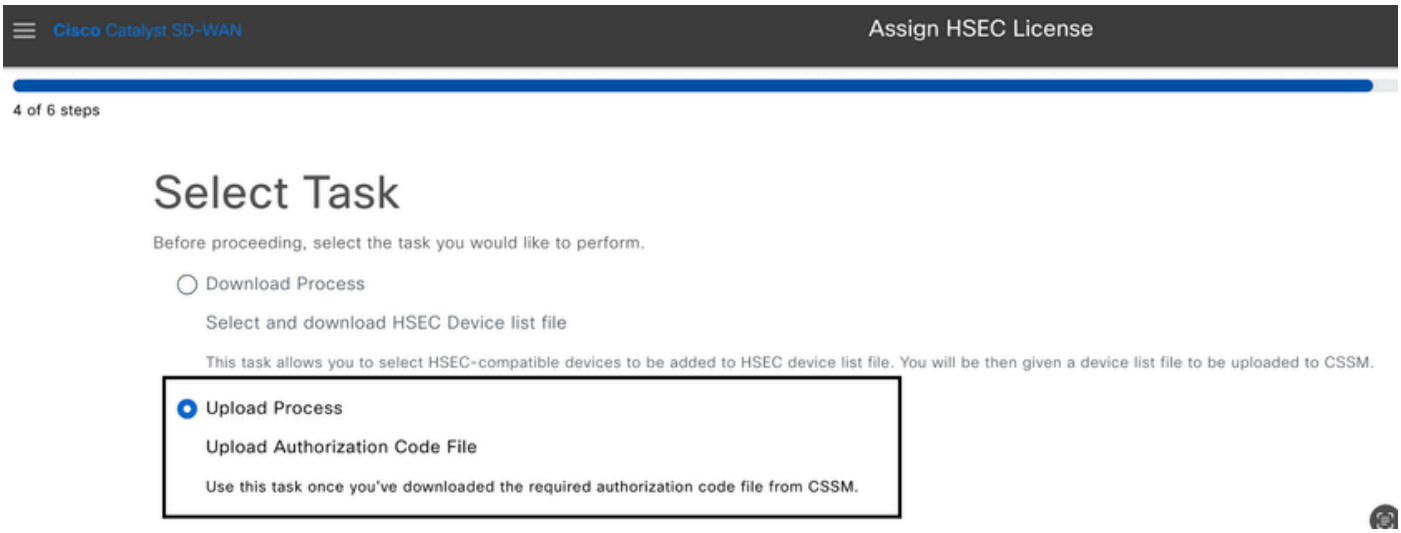
注:ACKファイルを生成するには、レポートステータスが「エラーなし」である必要があります。エラーが発生した場合は、展開アイコンをクリックしてエラーの詳細を取得します。必要に応じて、Cisco TACサービスリクエストをオープンします。



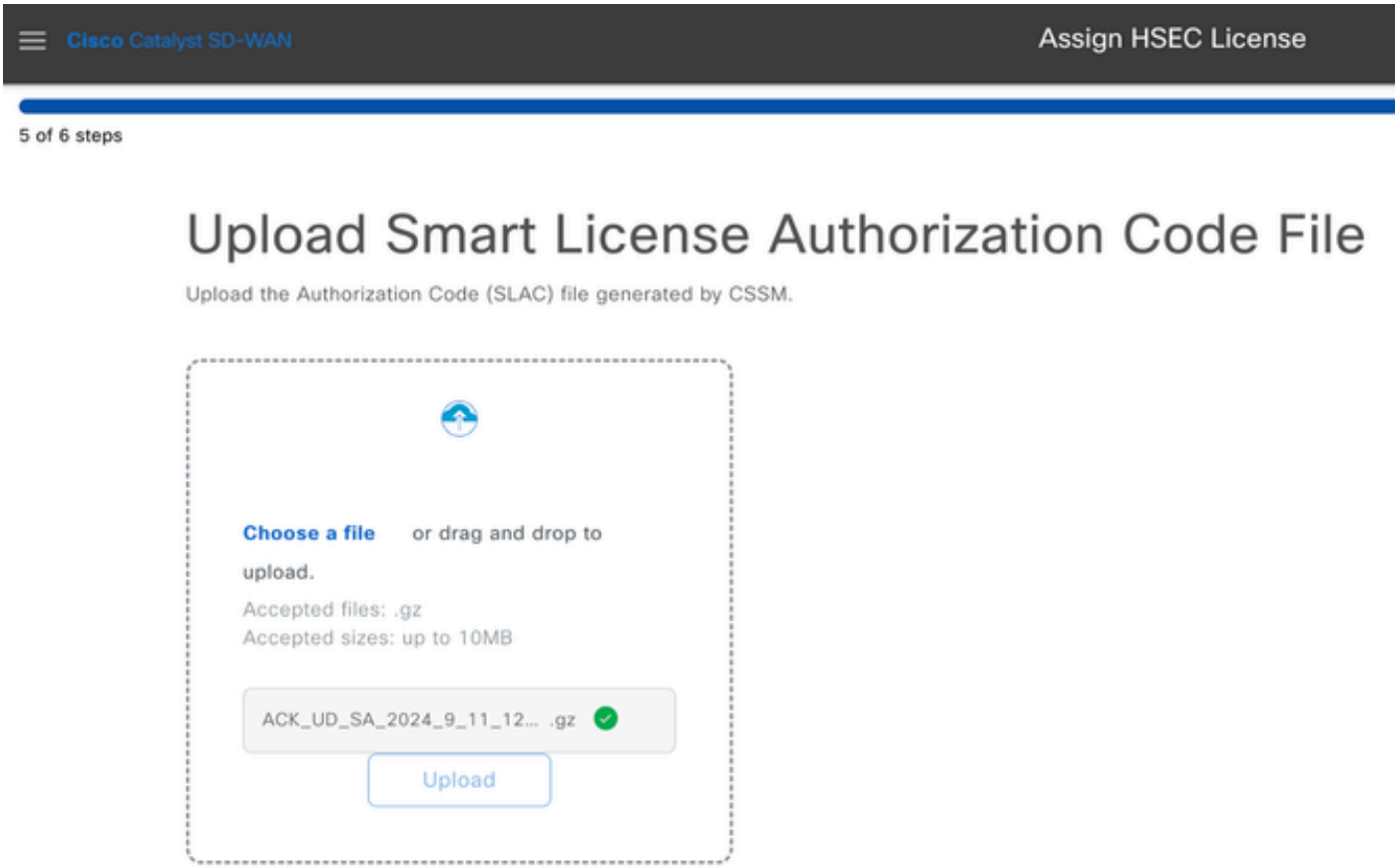
14. – システムがACKファイルを生成し、自動的にダウンロードします。



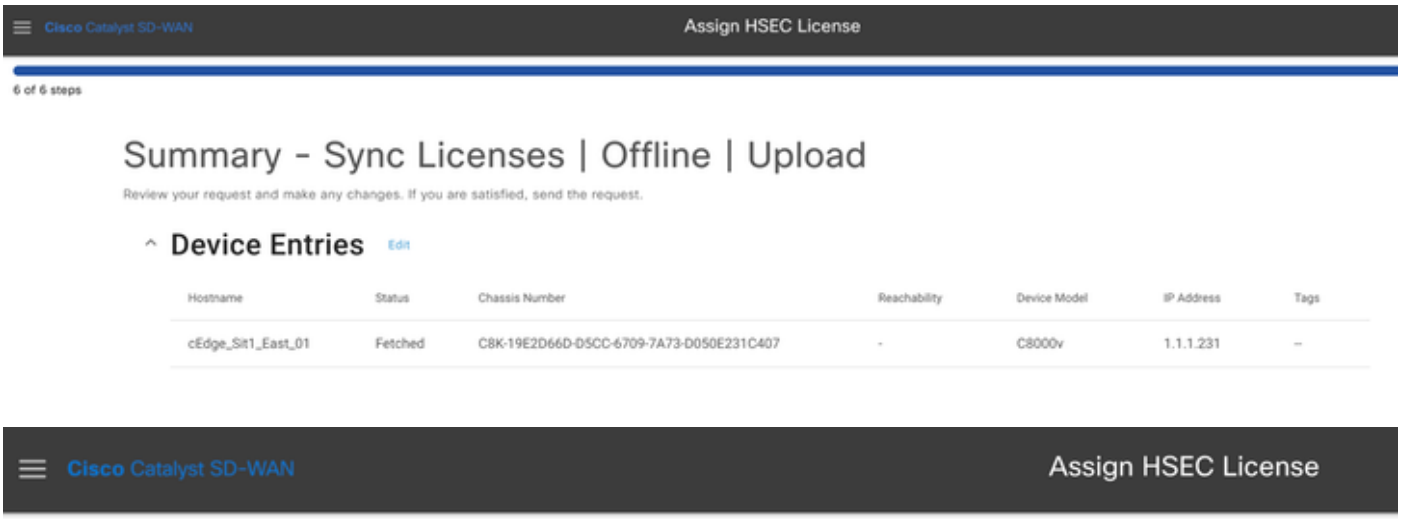
15.- vMange GUIで、メインメニュー>ワークフロー> HSECライセンスの同期とインストール>ライセンスの同期>オフライン>次>アップロードプロセスの順に移動します。

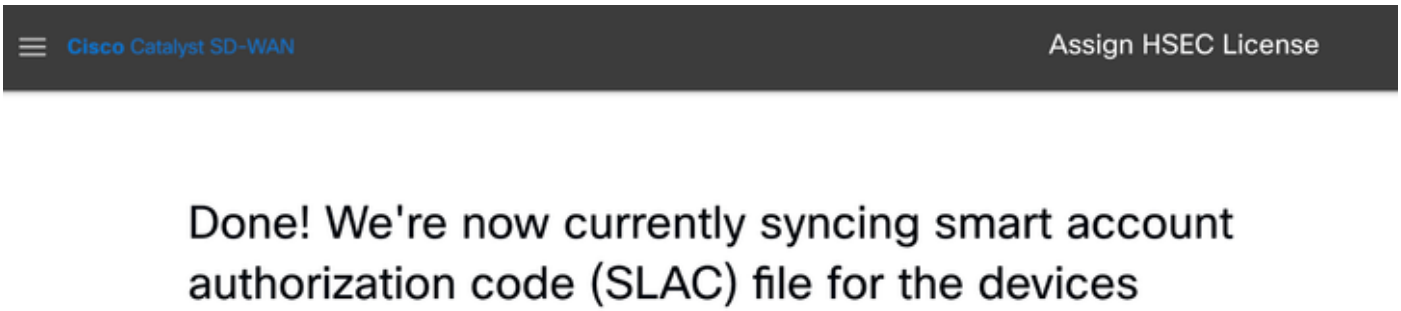


16.- Choose a Fileをクリックするか、ダウンロードしたファイルをボックスにドラッグアンドドロップし、Uploadをクリックします。



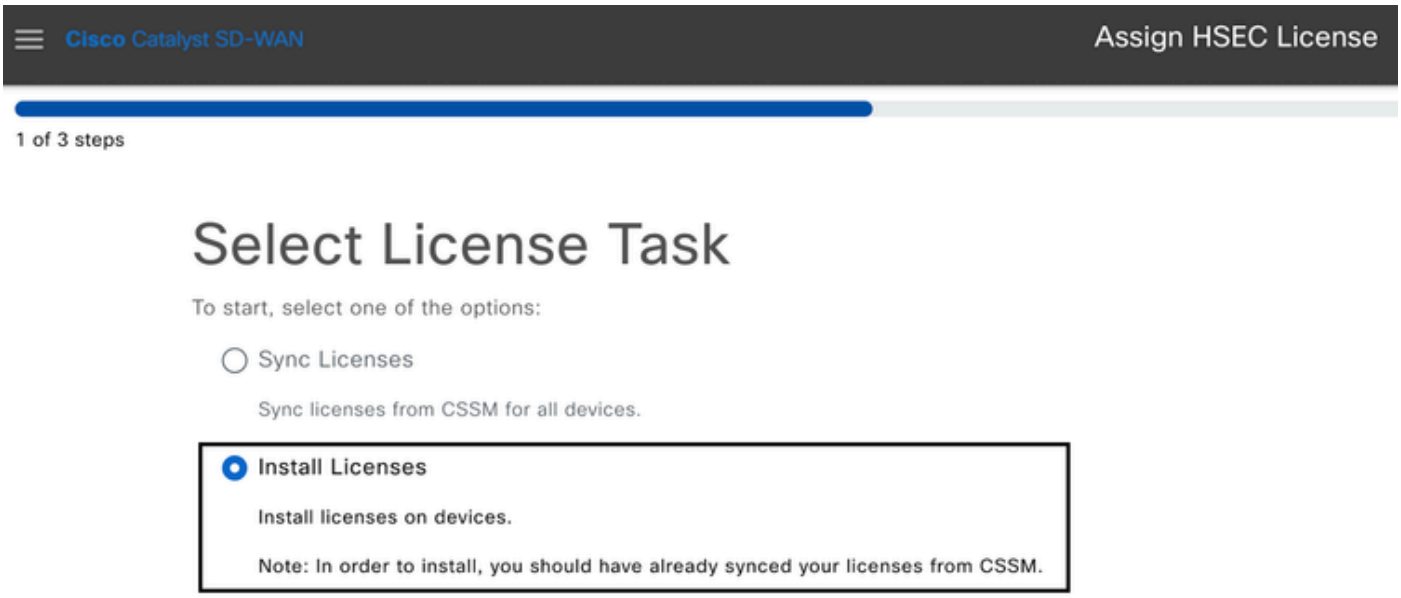
17. – タスクの要約を確認し、Uploadをクリックします。



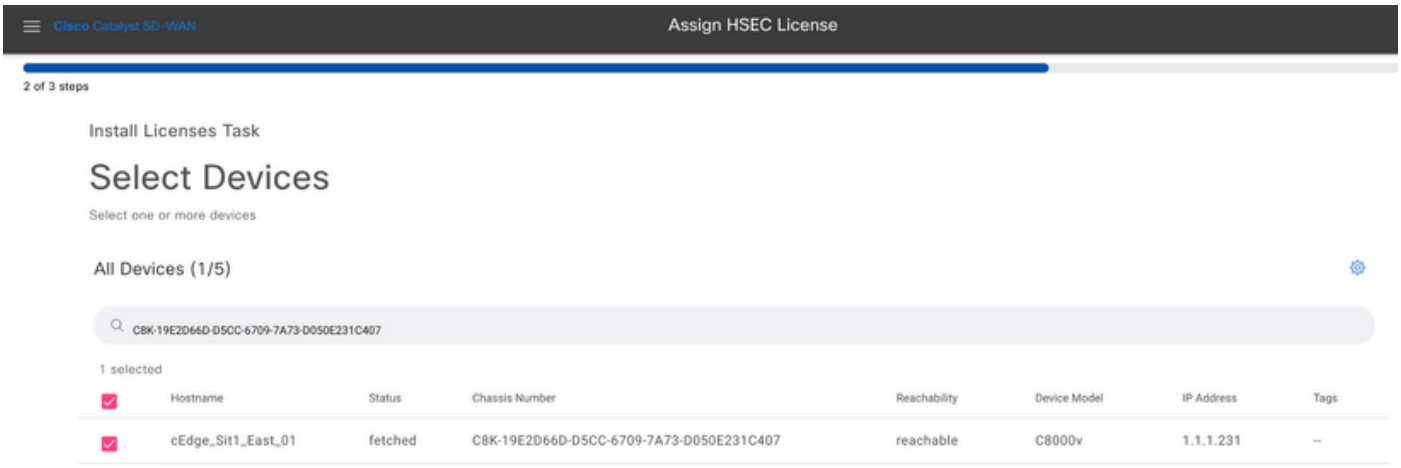


取得したライセンスのインストール

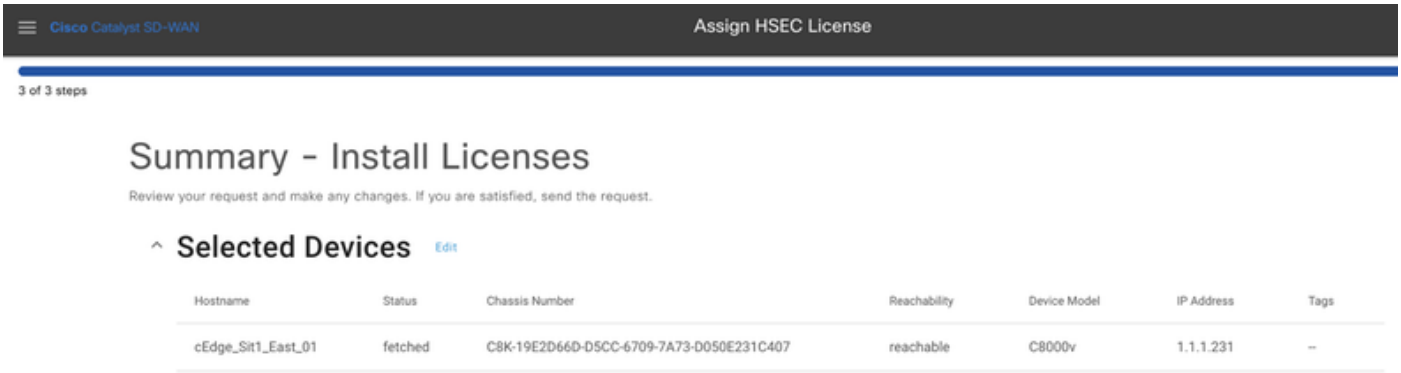
1. – ワークフローライブラリのSync and Install Licensesに戻り、Install Licensesをクリックします。



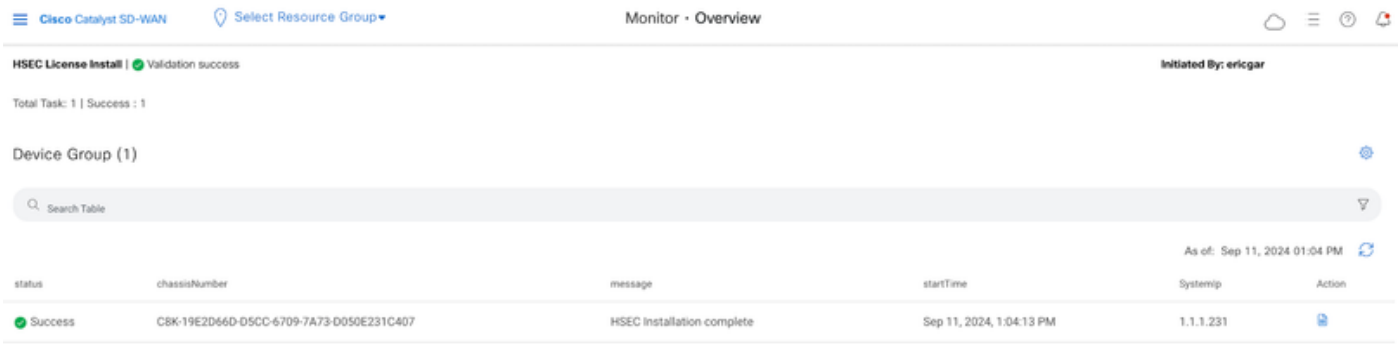
2. – ライセンス認証が行われたのと同じデバイスをリストから選択し、Nextをクリックします。



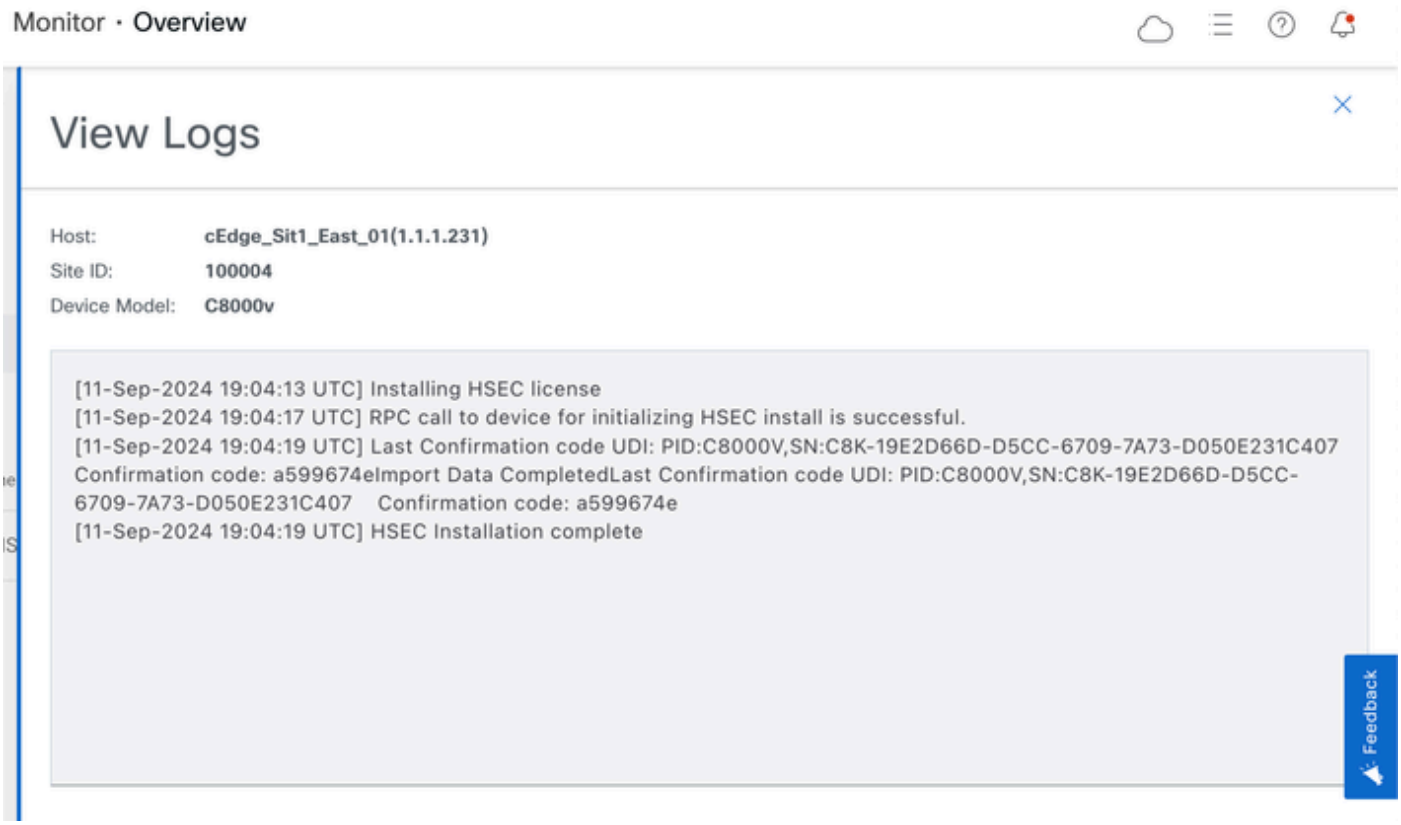
3. – タスクの要約を確認し、Installをクリックします。



4. – プロセスが完了するのを待ちます。インストールのステータスはSuccessでなければなりません。



5.- Actionアイコンをクリックして、HSECのインストールに関するより詳細なログを表示します。



HSECK9ライセンスの返却

リターンコードの動作

このタスクの目的は、ルータからライセンスを削除し、CSSMポータルのHSECK9ライセンスプールに正の数として戻すことです。

予約方法	リターンコード生成	アクション プラン
[オンライン]	はい、可能です	ライセンスとルータの関連付けを解除するためのリターンコードを生成します。次のセクションを確認します。
オフライン	はい、可能です	ライセンスとルータの関連付けを解除するためのリターンコードを生成します。次のセクションを確認します。

注：リターンコードの生成に失敗した場合は、TACケースをオープンし、ルータとCSSMポータルからライセンスを手動で削除してください。

リターンコードの生成

CSSMで予約されているライセンスをルータのローカル認証と照合して検証し、後で削除するには、リターンコードが必要です。

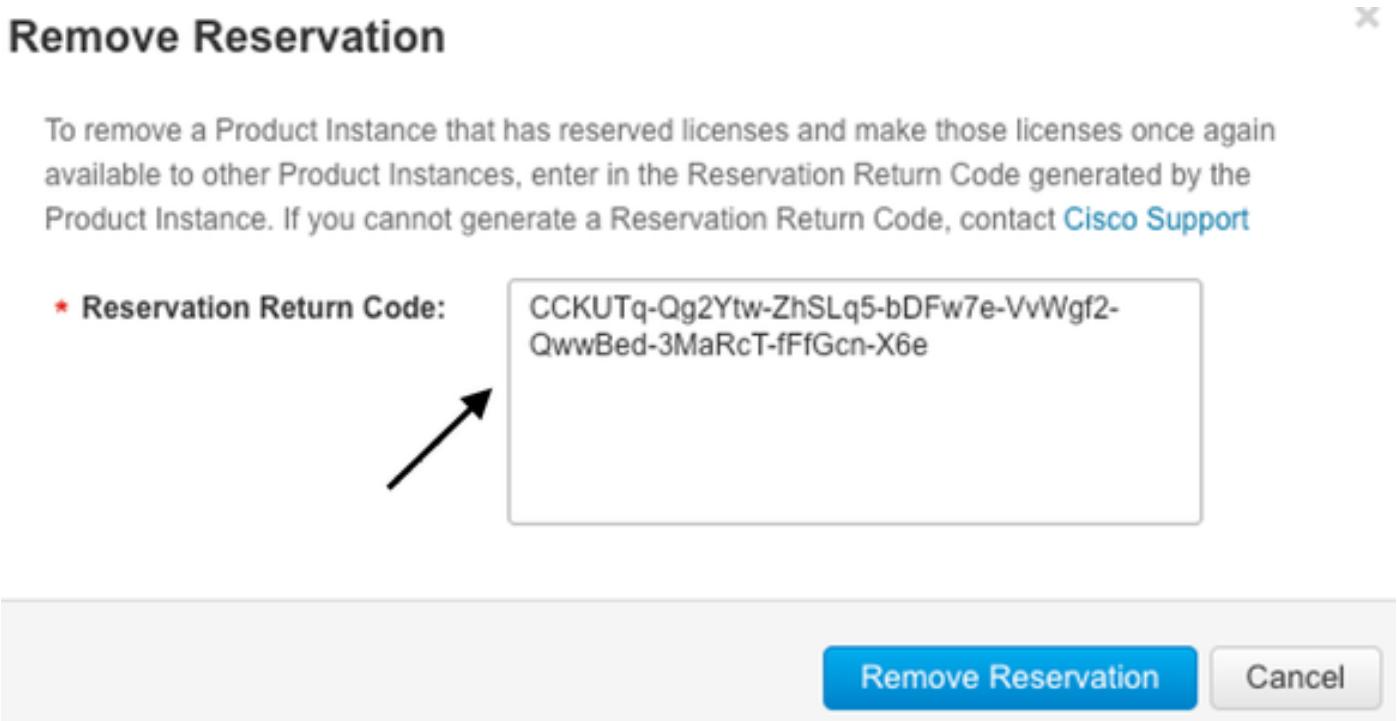
<#root>

```
EdgeRouter# license smart authorization return local online

Authorization already returned with this code:
UDI: PID:C1111-8PWE,SN:FGL2149XXXX
Return code:

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


<<<< Copy the string
```

注:「license smart authorization return local online」コマンドは、オンラインまたはオフラインの両方の予約方法で機能します。「license smart authorization return local offline」コマンドは、コントローラ管理モード（SD-WANモード）では機能しません。 これは、物理ルータと仮想ルータの両方に適用されます。

予約の削除

CSSMで、Product Instances > Actions > Removeの順に移動します。 ルータからコピーしたリターンコードを貼り付け、Remove Reservationをクリックします。



「License reservation removed successfully（ライセンス予約が正常に削除されました）」という通知が直後に表示されます。これは、ライセンスがライセンスプールに送り返され、ライセンス数が1増加することを示します。

アクティベーション：リロードは必要ですか。

8500ベースのプラットフォームでは、HSECをアクティブにするためにリロードが必要だというのは本当ですか。

はい、8500プラットフォームファミリでは、自律モードまたはコントローラモードのいずれかでリロードする必要があります。

HSECのアクティベーション後にC8000vのリロードが必要ですか

いいえ、必要ありません。ライセンスはC8000vの設計に従って「not-in-use」のままですが、デバイスはhsecのインストール直後に無制限のスループットを取得します。

HSECのアクティベート後のCSR1000vのリロードについて

いいえ。hsecのアクティベート後は、CSR1000vのリロードは必要ありません。

リロード動作はSD-WANモードと非SD-WANモードで同じですか。

いいえ、HSECの有効化に関して、SD-WANモードと非SD-WANモードは大きく異なります。

SD-WANモードでは、リロードによってHSECを有効またはアクティブ化する必要がありますが、非SD-WANモードでは、CLI license feature hsec コマンドによってデバイスのHSECが有効またはアクティブ化されます。SD-WANモードのCSR1000vおよびC8000Vプラットフォームでは、リロードは不要です。

HSECライセンスの非アクティブ化についても同様ですか。

HSECライセンスは非SD-WANモード(Autonomous)でアンインストールできますが、機能の使用中にHSECライセンスをアンインストールすることはできません。ユーザはCLI no license feature hsec コマンドを使用してHSECライセンスを無効/非アクティブ化し、ライセンスが「not-in-use」状態になるようにデバイスをリロードしてから、uninstallコマンドを開始する必要があります。SD-WANモードでは機能を無効にできないため、HSECライセンスのアンインストールはサポートされません。ただし、モードの変更に関する既知の課題に対する回避策として、自律モードに切り替えてアンインストールするオプションがあります。SD-WANモードでCSSMにライセンスを返却する方法に関するガイダンスを受けるには、TACケースをオープンしてください。

✎ 注：詳細については、『SD-WAN用HSECライセンスに関するFAQ』を参照してください。

ライセンスの有効性の検証

確認

このセクションでは、設定が正常に動作していることを確認します。

便利なコマンド

検証手順は、オンラインまたはオフラインの方法の各ステップで説明します。

<#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
```

トラブルシュート

このセクションでは、設定のトラブルシューティングに役立つ情報を紹介します。

ポリシーを使用するスマートライセンスは、エッジルータとCSSMの間のインターネットを介したセキュアな双方向通信に依存し、登録とライセンスの取得に同意する確認応答とハンドシェイクを交換します。

デバイス間でメッセージを正しく交換できない一般的なシナリオがあります。

一般的な問題

DNS解決が機能しない

smartreceiver.comに到達するには、エッジルータがドメイン名を解決できる必要があります。そうしないと、URLがルーティング可能なIPに変換されず、通信が失敗します。通常、このエラーは信頼確立の試行後に表示されます。

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

インターネットへのIP接続があることを確認します。

<#root>

```
ping 8.8.8.8
```

URLに対してpingを発行し、代わりにURLへのtelnetを使用して、インターネット制御メッセージプロトコル(ICMP)が外部デバイスによってブロックされているかどうか確認します。

<#root>

```
ping cisco.com
```

```
telnet cisco.com 80
```

テストが失敗した場合は、DNSサーバを設定し、DNS解決を有効にします。

<#root>

```
ip domain lookup
```

```
ip name-server 8.8.8.8
```

外部DNSサーバを設定できない場合は、ルータでローカルDNS解決を設定します。

<#root>

```
EdgeRouter#
config-transaction

EdgeRouter(config)#
ip host smartreceiver.com A.B.C.D

EdgeRouter(config)#
commit
```

注:smartreceiver.comに応答するIPを把握する必要がある場合は、WindowsまたはLinuxマシンから**nslookup <URL>**コマンドを実行してください。

注：ローカルDNS解決は、レスポンダIPが時間の経過とともに変化する可能性があり、シスコが変更について通知しないため、推奨されません。

Smart Licensing(SL)イベントログに一般的なエラーメッセージが表示される。

<#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トンネルがDNSをブロックする

同様の問題は、SD-WANトンネルの暗黙的ACLが着信DNS応答をブロックする場合にも発生します。

<#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
```

登録時に、DNSサービスが許可されていることを確認します。

<#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 <<<<<<<<<<<<<<<<<<< MUST be allowed

```
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
```

トランスポートURLが正しくありません

新規（新規）インストールの場合、デフォルトの転送タイプはCisco Smart Licensing Utility(CSLU)です。

<#root>

```
EdgeRouter#
```

show license tech support | include Smart Licensing Status

```
Smart Licensing Tech Support info

Smart Licensing Status
======================

Smart Licensing is ENABLED

License Conversion:
Automatic Conversion Enabled: True
Status: Not started

Export Authorization Key:
Features Authorized:
<none>

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: <empty>
Proxy:
Address: <empty>
Port: <empty>
Username: <empty>
Password: <empty>
Server Identity Check: False
```

ログの一般的なエラー。

<#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
```

注:CSLUはCisco SD-WAN(Cisco vManage)ではサポートされていないため、CSLUを使用して、Cisco vManageで管理されるルーティング製品インスタンスのライセンス使用状況をレポートすることはできません。 詳細については、Cisco Smart License Utility(CSLU)を参照してください。

スマートエージェントのデフォルトのURLとトランスポートタイプを手動で設定し、トークンで確立された信頼を再試行します。

<#root>

```
EdgeRouter#
```

```
configure terminal
```

```
EdgeRouter(config)#
```

```
license smart transport smart
```

```
EdgeRouter(config)#
```

```
license smart url default
```

```
EdgeRouter(config)#
```

```
 commit
```

SD-WANトンネルがHTTPSをブロック

Smart Licensing通信は、Hypertext Transfer Protocol Secure(HTTPS)ポート443に基づいています。そのため、着信するHTTPS応答がSD-WANトンネルによってブロックされると、登録、認証要求、およびRUMレポートの通知が失敗します。

logおよびeventlogの一般的なエラー。

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

登録時にHTTPSサービスがSD-WANトンネルで許可されていることを確認します。そうでない場合は、許可してから、トークンによる信頼確立を再試行します。

<#root>

```
EdgeRouter#
```

```
show sdwan runnning-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
```

外部ファイアウォールがCSSM URL、IP、またはポート443をブロック

サイトアーキテクチャでファイアウォールを使用してトラフィックを制御している場合は、smartreceiver.cisco.comへのポート443がブロックされていないことを確認します。ファイアウォールチームまたはインターネットサービスプロバイダー(ISP)に問い合わせて、さらに確認してください。

ルータから。

<#root>

```
EdgeRouter#
```

telnet smartreceiver.com 443

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

Open

サービスVRFホストから。

<#root>

```
ericgar@cisco$
```

telnet smartreceiver.cisco.com 443

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

Connected to smartreceiver.cisco.com.

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

インターネットへの複数のインターフェイス

複数のインターフェイスがある一部のシナリオでは、CSSMとの通信が失敗します。HTTP送信元インターフェイスは、ルータで使用可能な任意のインターフェイスに変更できます。

<#root>

```
EdgeRouter#
config-transaction

EdgeRouter(config)#
ip http client source-interface INTERFACE

EdgeRouter(config)#
commit
```

関連情報

- Ciscoエンタープライズルーティングプラットフォームのポリシーを使用したスマートライセンス
- ポリシーSD-WANを使用したスマートライセンスのライセンス管理
- テクニカル サポートとドキュメント - Cisco Systems

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。