ポリシーを使用したスマートライセンシングのタスクライブラリ

このセクションでは、ポリシーを使用したスマートライセンシングに適用されるタスクのグループについて説明します。

特定のトポロジを実装する場合は、対応するワークフローを参照してください。適用されるタスクの順序を確認するには、「ポリシーを使用したスマートライセンシングの設定方法：トポロジ別のワークフロー」を参照してください。

シスコへのログイン（CSLU インターフェイス）

必要に応じて、CSLU で作業するときに接続モードまたは切断モードのいずれかにすることができます。接続モードで作業するには、次の手順を実行してシスコに接続します。

手順

ステップ 1 CSLU のメイン画面で、[Login to Cisco]（画面の右上隅）をクリックします。

ステップ 2 [CCO User Name] と [CCO Password] を入力します。

ステップ 3 CSLU の [Preferences] タブで、シスコ接続トグルに「Cisco Is Available」と表示されていることを確認します。

スマートアカウントとバーチャルアカウントの設定（CSLU インターフェイス）

スマートアカウントとバーチャルアカウントはどちらも [Preferences] タブで設定します。シスコに接続するためのスマートアカウントとバーチャルアカウントの両方を設定するには、次の手順を実行します。

手順

ステップ 1 CSLU のホーム画面から [Preferences] タブを選択します。

ステップ 2 スマートアカウントとバーチャルアカウントの両方を追加するには、次の手順を実行します。

a) [Preferences] 画面で、[Smart Account] フィールドに移動し、[Smart Account Name] を追加します。

b) 次に、[Virtual Account] フィールドに移動し、[Virtual Account Name] を追加します。

CSSM に接続している場合（[Preferences] タブに「Cisco is Available」）、使用可能な SA/VA のリストから選択できます。

CSSM に接続していない場合（[Preferences] タブに「Cisco Is Not Available」）、SA/VA を手動で入力します。

（注） SA/VA 名では大文字と小文字が区別されます。

ステップ 3 [Save] をクリックします。SA/VA アカウントがシステムに保存されます。

一度に 1 つの SA/VA ペアのみが CSLU に存在できます。複数のアカウントを追加することはできません。別の SA/VA ペアに変更するには、ステップ 2a および 2b を繰り返してから [Save] をクリックします。新しい SA/VA アカウントペアは、以前に保存されたペアを置き換えます。

CSLU での製品開始型製品インスタンスの追加（CSLU インターフェイス）

[Preferences] タブを使用してデバイス作成の製品インスタンスを追加するには、次の手順を実行します。

手順

ステップ 1 [Preferences] タブを選択します。

ステップ 2 [Preferences] 画面で、[Validate Instance] チェックボックスをオフにします。

ステップ 3 [Default Instance Method] を [Product Instance Initiated] に設定し、[Save] をクリックします。

製品インスタンス開始型通信のネットワーク到達可能性の確認

このタスクでは、製品インスタンス開始型通信のネットワーク到達可能性を確認するために必要になる可能性のある設定を提供します。「（必須）」と付いている手順は、すべての製品インスタンスで必須です。他のすべての手順は、製品インスタンスの種類とネットワーク要件に応じて、必須の場合も任意の場合もあります。該当するコマンドを設定します。

始める前に

サポートされるトポロジ：CSLU を介して CSSM に接続（製品インスタンス開始型通信）。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。プロンプトが表示されたらパスワードを入力します。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *interface-type-number* 例： `Device (config)# interface gigabitethernet0/0`	インターフェイス コンフィギュレーション モードを開始し、VRF に関連付けられたイーサネットインターフェイス、サブインターフェイス、または VLAN を指定します。
ステップ 4	**vrf forwarding** *vrf-name* 例： `Device(config-if)# vrf forwarding SLP_VRF`	VRF をレイヤ 3 インターフェイスに対応付けます。このコマンドは、インターフェイスでマルチプロトコル VRF をアクティブにします。
ステップ 5	**ip address** *ip-address mask* 例： `Device(config-if)# ip address 192.168.0.1 255.255.0.0`	VRF の IP アドレスを定義します。

	コマンドまたはアクション	目的
ステップ 6	**negotiation auto** 例： `Device(config-if)# negotiation auto`	インターフェイスの速度およびデュプレックスパラメータの自動ネゴシエーション動作を有効にします。
ステップ 7	**end** 例： `Device(config-if)# end`	インターフェイス コンフィギュレーションモードを終了し、グローバル コンフィギュレーションモードを開始します。
ステップ 8	**ip http client source-interface** *interface-type-number* 例： `Device(config)# ip http client source-interface gigabitethernet0/0`	HTTP クライアントのソース インターフェイスを設定します。
ステップ 9	**ip route** *ip-address ip-mask subnet mask* 例： `Device(config)# ip route vrf SLP_VRF 192.168.0.1 255.255.0.0 192.168.255.1`	（必須）製品インスタンスにルートとゲートウェイを設定します。スタティックルートまたはダイナミックルートのいずれかを設定できます。
ステップ 10	{**ip** | **ipv6**} **name-server** *server-address 1 ...server-address 6*] 例： `Device(config)# ip name-server vrf SLP_VRF 173.37.137.85`	VRF インターフェイスでドメインネームシステム（DNS）を設定します。
ステップ 11	**license smart vrf** *vrf_string* 例： `Device(config)# Device(config)# license smart vrf SLP_VRF`	製品インスタンスで使用される VRF 名を設定します。製品インスタンスは VRF を使用して、ライセンス関連のデータを CSSM、CSLU、または SSM オンプレミスに送信します。 製品インスタンスが VRF をサポートするインスタンスであり、対応する URL を使用してトランスポートタイプが **smart** または **cslu** に設定されていることを確認します。
ステップ 12	**ip domain lookup source-interface** *interface-type-number* 例：	DNS ドメインルックアップ用のソースインターフェイスを設定します。

	コマンドまたはアクション	目的
	`Device(config)# ip domain lookup source-interface gigabitethernet0/0`	（注） レイヤ 3 物理インターフェイスでこのコマンドを設定した場合、ポートモードが変更されるかデバイスがリロードされると、そのコマンドは実行コンフィギュレーションから自動的に削除されます。これは、コマンドを再設定することでのみ回避できます。Cisco IOS XE Dublin 17.12.1 以降では、この問題は解決されています。
ステップ 13	**ip domain name** *domain-name* 例： `Device(config)# ip domain name example.com`	ドメインの DNS ディスカバリを設定します。ここの例では、ネームサーバはエントリ `cslu-local.example.com` を作成します。

CSLU での CSLU 開始型製品インスタンスの追加（CSLU インターフェイス）

CSLU インターフェイスを使用して、接続方法を CSLU 開始型に設定できます。この接続方法（モード）により、CSLU は製品インスタンスから製品インスタンス情報を取得できます。

（注） デフォルトの接続方法は、[Preferences] タブで設定されます。

[Inventory] タブから製品インスタンスを追加するには、次の手順を実行します。

手順

ステップ 1 [Inventory] タブに移動し、[Product Instances] テーブルから [Add Single Product] を選択します。

ステップ 2 [Host] に入力します（ホストの IP アドレス）。

ステップ 3 [Connect Method] を選択し、CSLU 開始の接続方法を 1 つを選択します。

ステップ 4 右側のパネルで、[Product Instance Login Credentials] をクリックします。画面の左側のパネルが変化して [User Name] フィールドと [Password] フィールドに変わります。

ステップ 5 製品インスタンスの [User Name] と [Password] を入力します。

ステップ 6 [保存（**Save**）] をクリックします。

情報がシステムに保存され、デバイスが [Product Instances] テーブルにリストされて、[Last Contact] には [never] と表示されます。

使用状況レポートの収集：CSLU開始（CSLUインターフェイス）

CSLU では、デバイスからの使用状況レポートの収集を手動でトリガーすることもできます。

製品インスタンスを設定して選択した後（[Add Single Product] を選択し、[Host] に名前を入力して [CSLU Initiated] 接続メソッドを選択）、[Actions for Selected] > [Collect Usage] を選択します。CSLU は選択した製品インスタンスに接続し、使用状況レポートを収集します。収集された使用状況レポートは、CSLU のローカルライブラリに保存されます。これらのレポートは、CSLU がシスコに接続されている場合はシスコに転送できます。または（シスコに接続されていない場合は）[Data] > [Export to CSSM] の順に選択して、手動で使用状況の収集をトリガーできます。

CSLU 開始モードで作業している場合は、次の手順を実行して、製品インスタンスから RUM レポートを収集するように CSLU を設定します。

手順

ステップ 1 [Preferences] タブをクリックし、有効な [Smart Account] と [Virtual Account] を入力して、適切な CSLU 開始型収集メソッドを選択します。（[Preferences] に変更があった場合は、[Save] をクリックします）。

ステップ 2 [Inventory] タブをクリックし、1 つまたは複数の製品インスタンスを選択します。

ステップ 3 [Actions for Selected] > [Collect Usage] をクリックします。

RUM レポートは、選択した各デバイスから取得され、CSLU ローカルライブラリに保存されます。[Last Contacted] 列が更新され、レポートが受信された時刻が表示されます。[Alerts] 列にはステータスが表示されます。

CSLU が現在シスコにログインしている場合、レポートはシスコの関連するスマートアカウントとバーチャルアカウントに自動的に送信され、シスコはCSLU と製品インスタンスに確認応答を送信します。確認応答は、[Product Instance] テーブルの [Alerts] 列に表示されます。シスコに手動で使用状況レポートを転送するには、CSLU のメイン画面から [Data] > [Export to CSSM] を選択します。

ステップ 4 [Export to Cisco] モーダルから、レポートを保存するローカルディレクトリを選択します。（<CSLU_WORKING_Directory>/data/default/rum/unsent）

この時点で、使用状況レポートがローカルディレクトリ（ライブラリ）に保存されます。使用状況レポートをシスコにアップロードするには、CSSMへのデータまたは要求のアップロードとファイルのダウンロード （57 ページ） の手順に従ってください。

（注） Windows オペレーティングシステムでは、ファイルの名前が変更されたときに拡張子をドロップすることで、使用状況レポートファイルのプロパティの動作を変更できます。動作の変更は、ダウンロードしたファイルの名前を変更し、名前を変更したファイルが拡張子をドロップすると発生します。たとえば、`UD_xxx.tar` という名前のダウンロード済みデフォルトファイルの名前が `UD_yyy` に変更されたとします。ファイルは tar 拡張子を失い、機能しなくなります。使用状況ファイルを正常に機能させるには、使用状況レポートファイルの名前を変更した後、`UD_yyy.tar` のように、ファイル名に tar 拡張子を追加する必要があります。

CSLU 開始型通信のネットワーク到達可能性の確認

このタスクでは、CSLU 開始型通信のネットワーク到達可能性を確認するために必要になる可能性のある設定を提供します。「（必須）」と付いている手順は、すべての製品インスタンスで必須です。他のすべての手順は、製品インスタンスの種類とネットワーク要件に応じて、必須の場合も任意の場合もあります。該当するコマンドを設定します。

始める前に

サポートされるトポロジ：CSLU を介して CSSM に接続（CSLU 開始型通信）。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。プロンプトが表示されたらパスワードを入力します。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**aaa new model** 例： `Device(config)# aaa new model`	（必須）認証、許可、アカウンティング（AAA）アクセスコントロールモデルをイネーブルにします。

	コマンドまたはアクション	目的
ステップ 4	**aaa authentication login default local** 例： `Device(config)# aaa authentication login default local`	（必須）認証時にローカルのユーザ名データベースを使用するように、AAA 認証を設定します。
ステップ 5	**aaa authorization exec default local** 例： `Device(config)# aaa authorization exec default local`	ネットワークへのユーザアクセスを制限するパラメータを設定します。ユーザは EXEC シェルの実行が許可されます。
ステップ 6	ip routing 例： `Device(config)# ip routing`	IP ルーティングを有効にします。
ステップ 7	{**ip** | **ipv6**} **name-server** *server-address 1 ...server-address 6*] 例： `Device(config)# ip name-server vrf Mgmt-vrf 192.168.1.100 192.168.1.200 192.168.1.300`	（任意）名前とアドレスの解決に使用する 1 つまたは複数のネームサーバのアドレスを指定します。 最大 6 つのネーム サーバを指定できます。各サーバアドレスはスペースで区切ります。最初に指定されたサーバが、プライマリ サーバです。デバイスは、プライマリサーバへDNS クエリを最初に送信します。そのクエリが失敗した場合は、バックアップ サーバにクエリが送信されます。
ステップ 8	**ip domain lookup source-interface** *interface-type-number* 例： `Device(config)# ip domain lookup source-interface gigabitethernet0/0`	デバイス上で、DNS に基づくホスト名からアドレスへの変換を有効にします。この機能は、デフォルトでイネーブルにされています。 ユーザのネットワークデバイスが、名前の割り当てを制御できないネットワーク内のデバイスと接続する必要がある場合、グローバルなインターネットのネーミング方式（DNS）を使用して、ユーザのデバイスを一意に識別するデバイス名を動的に割り当てることができます。

	コマンドまたはアクション	目的
		（注） レイヤ 3 物理インターフェイスでこのコマンドを設定した場合、ポートモードが変更されるかデバイスがリロードされると、そのコマンドは実行コンフィギュレーションから自動的に削除されることに注意してください。これは、コマンドを再設定することでのみ回避できます。Cisco IOS XE Dublin 17.12.1 以降では、この問題は解決されています。
ステップ 9	**ip domain name** *name* 例： `Device(config)# ip domain name vrf Mgmt-vrf cisco.com`	非完全修飾ホスト名（ドット付き 10 進表記ドメイン名のない名前）を完成させるためにソフトウェアが使用する、デフォルトのドメイン名を定義します。
ステップ 10	**no username** *name* 例： `Device(config)# no username admin`	（必須）指定されたユーザ名が存在する場合はクリアします。*name* には、次のステップで作成するユーザ名と同じものを入力します。これにより、次のステップで作成するユーザ名が重複していないことが保証されます。 CSLU 開始型の RUM レポート取得に REST API を使用する場合は、CSLU にログインする必要があります。ここでユーザ名が重複していると、システムにユーザ名が重複している場合にこの機能が正しく動作しないことがあります。
ステップ 11	**username** *name* **privilege** *level* **password** *password* 例： `Device(config)# username admin privilege 15 password 0 lab`	（必須）ユーザ名をベースとした認証システムを構築します。 **privilege** キーワードにより、ユーザの権限レベルを設定します。ユーザの権限レベルを指定する 0 ～ 15 の数字です。 password を使用すると、name 引数にアクセスできます。パスワードは 1 ～ 25

	コマンドまたはアクション	目的
		文字で、埋め込みスペースを使用でき、**username** コマンドの最後のオプションとして指定します。 これにより、CSLU が製品インスタンスのネイティブ REST を使用できるようになります。 （注） このユーザ名とパスワードをCSLUで入力します（使用状況レポートの収集：CSLU 開始（CSLU インターフェイス） （7 ページ）→ステップ 4.f）。その後、CSLU は製品インスタンスから RUM レポートを収集できます。
ステップ 12	**interface** *interface-type-number* 例： `Device (config)# interface gigabitethernet0/0`	インターフェイス コンフィギュレーション モードを開始し、VRF に関連付けられたイーサネットインターフェイス、サブインターフェイス、または VLAN を指定します。
ステップ 13	**vrf forwarding** *vrf-name* 例： `Device(config-if)# vrf forwarding Mgmt-vrf`	VRF をレイヤ 3 インターフェイスに対応付けます。このコマンドは、インターフェイスでマルチプロトコル VRF をアクティブにします。
ステップ 14	**ip address** *ip-address mask* 例： `Device(config-if)# ip address 192.168.0.1 255.255.0.0`	VRF の IP アドレスを定義します。
ステップ 15	**negotiation auto** 例： `Device(config-if)# negotiation auto`	インターフェイスの速度およびデュプレックスパラメータの自動ネゴシエーション動作を有効にします。
ステップ 16	**no shutdown** 例： `Device(config-if)# no shutdown`	無効にされたインターフェイスを再起動します。
ステップ 17	**end** 例：	インターフェイス コンフィギュレーション モードを終了し、グローバル コ

	コマンドまたはアクション	目的
	`Device(config-if)# end`	ンフィギュレーションモードを開始します。
ステップ 18	**ip http server** 例： `Device(config)# ip http server`	（必須）シスコの Web ブラウザ ユーザ インターフェイスを含む IP または IPv6 システムで HTTP サーバを有効にします。HTTP サーバは、デフォルトにより標準のポート 80 を使用します。
ステップ 19	**ip http authentication local** 例： `ip http authentication local` `Device(config)#`	（必須）HTTP サーバユーザに対して特定の認証方法を指定します。 **local** キーワードは、認証および許可に、ローカルシステム設定で（username グローバル コンフィギュレーション コマンドによって）指定したログイン ユーザ名、パスワード、権限レベル アクセスの組み合わせを使用することを示します。
ステップ 20	**ip http secure-server** 例： `Device(config)# ip http server`	（必須）セキュア HTTP（HTTPS）サーバを有効にします。HTTPS サーバは、セキュア ソケット レイヤ（SSL）バージョン 3.0 プロトコルを使用します。
ステップ 21	**ip http max-connections** 例： `Device(config)# ip http max-connections 16`	（必須）HTTP サーバへの同時最大接続数を設定します。1 ～ 16 の範囲の整数を入力します。デフォルトは 5 です。
ステップ 22	**ip tftp source-interface** *interface-type-number* 例： `Device(config)# ip tftp source-interface GigabitEthernet0/0`	TFTP 接続用の送信元アドレスとして、インターフェイスの IP アドレスを指定します。
ステップ 23	**ip route** *ip-address ip-mask subnet mask* 例： `Device(config)# ip route vrf mgmt-vrf 192.168.0.1 255.255.0.0 192.168.255.1`	製品インスタンスにルートとゲートウェイを設定します。スタティック ルートまたはダイナミック ルートのいずれかを設定できます。
ステップ 24	**logging host** 例：	リモート ホストへのシステム メッセージおよびデバッグ出力を記録します。

	コマンドまたはアクション	目的
	`Device(config)# logging host 172.25.33.20 vrf Mgmt-vrf`	
ステップ 25	**end** 例： `Device(config)# end`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。
ステップ 26	**show ip http server session-module** 例： `Device# show ip http server session-module`	（必須）HTTP 接続を確認します。出力で、SL_HTTP がアクティブであることを確認します。また、次のチェックも実行できます。 • CSLU がインストールされているデバイスから、製品インスタンスに ping できることを確認します。ping が成功すると、製品インスタンスが到達可能であることが確認されます • CSLU がインストールされているデバイスの Web ブラウザで、`https://<product-instance-ip>/` を確認します。これにより、CSLU から製品インスタンスへの REST API が期待どおりに動作することが保証されます。

CSSM へのエクスポート（CSLU インターフェイス）

このオプションは、セキュリティのためにワークステーションを隔離する場合に、手動ダウンロード手順の一部として使用できます。

手順

ステップ 1 [Preferences] タブに移動し、[Cisco Connectivity] トグルスイッチをオフにします。

フィールドが「Cisco Is Not Available」に切り替わります。

ステップ 2 ホーム画面から、[Data] > [Export to CSSM] の順に移動します。

ステップ 3 開いたウィンドウからファイルを選択し、[Save] をクリックします。これでファイルが保存されました。

（注） この時点で、DLC ファイル、RUM ファイル、またはその両方があります。

ステップ 4 シスコに接続できるワークステーションから、次の手順を実行します：CSSMへのデータまたは要求のアップロードとファイルのダウンロード （57 ページ）

ファイルがダウンロードされたら、CSLU にインポートできます。「CSSM からのインポート（CSLU インターフェイス） （14 ページ）」を参照してください。

CSSM からのインポート（CSLU インターフェイス）

シスコから ACK またはその他のファイル（承認コードなど）を受信すると、そのファイルをシステムにアップロードできます。この手順は、オフラインのワークステーションに使用できます。シスコからファイルを選択してアップロードするには、次の手順を実行します。

手順

ステップ 1 CSLU にアクセス可能な場所にファイルがダウンロードされていることを確認します。

ステップ 2 CSU のホーム画面から、[Data] > [Import from CSSM] の順に移動します。

ステップ 3 [Import from CSSM] モーダルが開き、次のいずれかを実行できます。

- ローカルドライブにあるファイルをドラッグアンドドロップします。または、
- 適切な *.xml ファイルを参照し、ファイルを選択して [Open] をクリックします。

アップロードが成功すると、ファイルがサーバーに正常に送信されたことを示すメッセージが表示されます。アップロードが成功しない場合は、インポートエラーが発生します。

ステップ 4 アップロードが完了したら、ウィンドウの右上隅にある [x] をクリックして閉じます。

複数の製品インスタンスの SLAC の要求（CSLU インターフェイス）

[Authorization Code Request] メニューオプションは、複数の製品インスタンスの SLAC を手動で要求する場合に使用します。

始める前に

サポートされるトポロジ：

- CSLU を介して CSSM に接続
- CSLU は CSSM から切断

手順

ステップ 1 [Product Instances] テーブルから、承認コード要求の対象となる製品インスタンスを選択します。

ステップ 2 1 つ以上の製品インスタンスを選択した状態で、[Available Actions] メニューから [Authorization Code Request] オプションを選択します。

ステップ 3 実行するステップを説明するウィンドウで、[Accept] をクリックします。

アップロードする CSV ファイルを選択するアップロードウィンドウが開きます。（ローカル）

ステップ 4 次に、ウィンドウでも説明されている次の手順を実行します。

a) ディレクトリパス software.cisco.com > [Smart Software Licensing] > [Inventory] > [Product Instances] > [Authorize License Enforced Features] に移動して、ファイルをシスコにアップロードします。

b) 画面に表示される手順を実行します。

1. [Multiple Product Instances] を選択します。

   複数の製品インスタンスの場合は、[Choose File] をクリックしてアップロードするか、または今後のアップロード用に**テンプレートをダウンロード**できます（csv ファイルテンプレート）。

2. 次のパネルで、**ライセンスを選択**します。

3. ライセンスの選択をレビューして確認します

4. ダウンロードする承認コードを作成します

c) ファイルと選択したライセンスがシスコにアップロードされたら、（ファイルとして）選択した製品インスタンスの**承認コードをダウンロード**して CSLU に戻します。

ステップ 5 [Upload From Cisco (in the CSLU interface)] を選択します。

CSLU が製品開始モードの場合：製品インスタンスが次回 CSLU に接続したときに、アップロードされたコードが製品インスタンスに適用されます。

CSLU が CSLU 開始モードの場合：CSLU が次回更新を実行するときに、アップロードされたコードが製品インスタンスに適用されます。

CSSM への接続の設定

次の手順では、CSSM へのレイヤ 3 接続を設定してネットワーク到達可能性を確認する方法を説明します。「（必須）」と付いている手順は、すべての製品インスタンスで必須です。他のすべての手順は、製品インスタンスの種類とネットワーク要件に応じて、必須の場合も任意の場合もあります。該当するコマンドを設定します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。プロンプトが表示されたらパスワードを入力します。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	{**ip** | **ipv6**} **name-server** *server-address 1 ...server-address 6*] 例： `Device(config)# ip name-server 209.165.201.1 209.165.200.225 209.165.201.14 209.165.200.230`	名前とアドレスの解決に使用する 1 つまたは複数のネーム サーバのアドレスを指定します。 最大 6 つのネーム サーバを指定できます。各サーバアドレスはスペースで区切ります。最初に指定されたサーバが、プライマリ サーバです。デバイスは、プライマリサーバへDNS クエリを最初に送信します。そのクエリが失敗した場合は、バックアップ サーバにクエリが送信されます。
ステップ 4	**ip name-server vrf Mgmt-vrf** *server-address 1...server-address 6* 例： `Device(config)# ip name-server vrf SLP_VRF 209.165.201.1 209.165.200.225 209.165.201.14 209.165.200.230`	（任意）VRF インターフェイスで DNS を設定します。最大 6 つのネーム サーバを指定できます。各サーバアドレスはスペースで区切ります。 （注） このコマンドは、**ip name-server** コマンドの代わりです。
ステップ 5	**license smart vrf** *vrf_string* 例： `Device(config)# Device(config)# license smart vrf SLP_VRF`	製品インスタンスで使用される VRF 名を設定します。製品インスタンスは VRF を使用して、ライセンス関連のデータを CSSM、CSLU、または SSM オンプレミスに送信します。 製品インスタンスが VRF をサポートするインスタンスであり、対応する URL を使用してトランスポートタイプが **smart** または **cslu** に設定されていることを確認します。

	コマンドまたはアクション	目的
ステップ 6	**ip domain lookup source-interface** *interface-type interface-number* 例： `Device(config)# ip domain lookup source-interface Vlan100`	DNS ドメインルックアップ用のソースインターフェイスを設定します。
ステップ 7	**ip domain name** *domain-name* 例： `Device(config)# ip domain name example.com`	ドメイン名を設定します。
ステップ 8	**ip host tools.cisco.com** *ip-address* 例： `Device(config)# ip host tools.cisco.com 209.165.201.30`	自動 DNS マッピングが使用できない場合は、DNS ホスト名キャッシュ内のホスト名/アドレス静的マッピングを設定します。
ステップ 9	**interface** *interface-type-number* 例： `Device(config)# interface Vlan100` `Device(config-if)# ip address 192.0.2.10 255.255.255.0` `Device(config-if)# exit`	レイヤ 3 インターフェイスを設定します。インターフェイスのタイプと番号、または VLAN を入力します。
ステップ 10	**ntp server** *ip-address* [**version** *number*] [**key** *key-id*] [**prefer**] 例： `Device(config)# ntp server 198.51.100.100 version 2 prefer`	（必須）NTP サービスをアクティブにし（まだアクティブになっていない場合）、システムがシステム ソフトウェア クロックを指定された NTP サーバと同期できるようにします。これにより、デバイスの時刻が CSSM と同期されます。 このコマンドを複数回使用する必要があるために優先サーバを設定する場合は、**prefer** キーワードを使用します。このキーワードを使用すると、サーバ間の切り換え回数が減少します。

	コマンドまたはアクション	目的
		ヒント　この設定が完了したら、**show license tech** を使用してクロックが実際に同期されているかどうかを確認します。正常に同期されると、[Clock sync-ed with NTP] フィールドが [True] に設定されます。同期されていない場合、このフィールドは [False] に設定されます。 クロックが同期されていない場合、信頼の確立時や SLAC の要求時などの**試行**は **show license tech** の出力に反映されません。次に例を示します。 `Trust Establishment:` `  Attempts: Total=0,` `Success=0, Fail=0  Ongoing` `  Failure: Overall=0` `Communication=0`
ステップ 11	**switchport access vlan** *vlan_id* 例： `Device(config)# interface GigabitEthernet1/0/1` `Device(config-if)# switchport access vlan 100` `Device(config-if)# switchport mode access` `Device(config-if)# exit` `OR` `Device(config)#`	このアクセスポートがトラフィックを伝送する VLAN を有効にし、非トランキングで非タグ付きのシングル VLAN イーサネットインターフェイスとしてインターフェイスを設定します。 （注）　このステップは、スイッチポート アクセス モードが必要な場合にのみ設定します。**switchport access vlan** コマンドは、たとえば Catalyst スイッチング製品インスタンスに適用できます。ルーティング製品インスタンスの場合は、代わりに **ip address** *ip-address mask* コマンドを設定できます。

	コマンドまたはアクション	目的
ステップ 12	**ip route** *ip-address ip-mask subnet mask* 例： `Device(config)# ip route 192.0.2.0 255.255.255.255 192.0.2.1`	デバイスにルートを設定します。スタティックルートまたはダイナミックルートのいずれかを設定できます。
ステップ 13	**ip http client source-interface** *interface-type-number* 例： `Device(config)# ip http client source-interface Vlan100`	（必須）HTTP クライアントのソースインターフェイスを設定します。インターフェイスのタイプと番号、または VLAN を入力します。
ステップ 14	**exit** 例： `Device(config)# exit`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 15	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	コンフィギュレーションファイルに設定を保存します。

HTTPS プロキシを介したスマート転送の設定

スマート転送モードを使用している場合にプロキシサーバを使用してCSSMと通信するには、次の手順を実行します。

（注） 認証された HTTPS プロキシ設定はサポートされていません。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。プロンプトが表示されたらパスワードを入力します。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**license smart transport smart** 例：	スマート転送モードを有効にします。

	コマンドまたはアクション	目的
	`Device(config)# license smart transport smart`	
ステップ 4	**license smart url default** 例： `Device(config)# license smart transport default`	スマート URL を自動的に設定します（https://smartreceiver.cisco.com/licservice/license）。このオプションを想定どおりに動作させるには、前の手順の転送モードを smart に設定する必要があります。
ステップ 5	**license smart proxy** {**address** *address_hostname* | **port** *port_num*} 例： `Device(config)# license smart proxy address 192.168.0.1` `Device(config)# license smart proxy port 3128`	スマート転送モードのプロキシを設定します。プロキシが設定されている場合、ライセンスメッセージは最終宛先 URL（CSSM）に加えてプロキシにも送信されます。プロキシはメッセージを CSSM に送信します。プロキシ IP アドレスとポート情報を個別に設定します。 • **address** *address_hostname*：プロキシアドレスを指定します。プロキシサーバの IP アドレスまたはホスト名を入力します。 • **port** *port_num*：プロキシポートを指定します。プロキシ ポートポート番号を入力します。 Cisco IOS XE Bengaluru 17.6.1 以降、プロキシサーバーの受け入れ基準が変更されたことに注意してください。プロキシサーバーの応答のステータスコードのみがシステムによって検証され、理由フレーズは検証されません。RFC形式は、`status-line = HTTP-version SP status-code SP reason-phrase CRLF` です。ステータス行の詳細については、RFC 7230 のセクション 3.1.2 を参照してください。
ステップ 6	**exit** 例： `Device(config)# exit`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 7	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	コンフィギュレーション ファイルに設定を保存します。

ダイレクトクラウドアクセス用の Call Home サービスの設定

Call Home サービスは、CSSM に対してクリティカルなシステムイベントを電子メールおよび Web 上で通知します。転送モードを設定するには、Call Home サービスを有効にし、宛先プロファイルを設定して（宛先プロファイルには、アラート通知に必要な配信情報が含まれます。少なくとも 1 つの宛先プロファイルが必要です）、次の手順を実行します。

（注） 「（任意）」と特に明記されていない限り、すべての手順を実行する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。プロンプトが表示されたらパスワードを入力します。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**license smart transport callhome** 例： `Device(config)# license smart transport callhome`	転送モードとして Call Home を有効にします。
ステップ 4	**license smart url** *url* 例： `Device(config)# license smart url https://tools.cisco.com/its/service/oddce/services/DDCEService`	**callhome** 転送モードの場合は、例に示すように CSSM URL を設定します。
ステップ 5	**service call-home** 例： `Device(config)# service call-home`	Call Home 機能をイネーブルにします。
ステップ 6	**call-home** 例： `Device(config)# call-home`	Call Home コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 7	**contact-email-address** *email-address* 例： `Device(config-call-home)# contact-email-addr username@example.com`	お客様の電子メールアドレスを割り当て、Smart Call Home サービスのフルレポート機能を有効にし、フルインベントリメッセージを Call Home TAC プロファイルから Smart Call Home サーバに送信してフル登録プロセスを開始します。電子メールアドレスフォーマットには、スペースなしで最大 200 文字まで入力できます。
ステップ 8	**profile** *name* 例： `Device(config-call-home)# profile CiscoTAC-1` `Device(config-call-home-profile)#`	指定された宛先プロファイルに対する Call Home 宛先プロファイル設定サブモードに入ります。 デフォルトは次のとおりです。 • CiscoTAC-1 プロファイルは非アクティブです。このプロファイルを Call Home サービスで使用するには、プロファイルを有効にする必要があります。 • CiscoTAC-1 プロファイルは、プロファイルに登録されているすべてのイベントタイプが記載された完全なレポートを送信します。または、`Device(cfg-call-home-profile)# anonymous-reporting-only` anonymous-reporting-only を追加で設定します。これが設定されている場合は、クラッシュ、インベントリ、およびテストメッセージのみが送信されます。 プロファイルのステータスを確認するには、**show call-home profile all** コマンドを使用します。
ステップ 9	**active** 例： `Device(config-call-home-profile)# active`	宛先プロファイルをイネーブルにします。

	コマンドまたはアクション	目的
ステップ 10	**destination transport-method http**{**email** |**http**} 例： `Device(config-call-home-profile)# destination transport-method http` AND `Device(config-call-home-profile)# no destination transport-method email`	メッセージの転送形式をイネーブルにします。この例では、HTTP 経由で Call Home サービスが有効になり、電子メールによる転送が無効になります。 このコマンドの no 形式を使用すると、メソッドが無効になります。
ステップ 11	**destination address** {**email** *email_address* |**http** *url*} 例： `Device(config-call-home-profile)# destination address http https://tools.cisco.com/its/service/oddce/services/DDCService` AND `Device(config-call-home-profile)# no destination address http https://tools.cisco.com/its/service/oddce/services/DDCService`	Call Home メッセージを送信する宛先 E メール アドレスまたは URL を設定します。宛先 URL を入力する場合は、サーバがセキュアサーバであるかどうかに応じて http://（デフォルト）または https:// を指定します。 ここに示す例では、http:// の形式で宛先 URL が設定されています。コマンドの **no** 形式では https:// に設定されます。
ステップ 12	**exit** 例： `Device(config-call-home-profile)# exit`	Call Home 宛先プロファイル コンフィギュレーション モードを終了して、Call Home コンフィギュレーション モードに戻ります。
ステップ 13	**exit** 例： `Device(config-call-home)# end`	Call Home コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。
ステップ 14	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	コンフィギュレーション ファイルに設定を保存します。
ステップ 15	**show call-home profile** {*name* |**all**}	指定されたプロファイル、または設定済みのすべてのプロファイルに関する宛先プロファイル設定を表示します。

HTTPS プロキシサーバを介したダイレクトクラウドアクセス用の Call Home サービスの設定

Call Home サービスは、HTTPS プロキシサーバを介して設定できます。この設定では、CSSM への接続にユーザ認証は必要ありません。

（注） 認証された HTTPS プロキシ設定はサポートされていません。

HTTPS プロキシを介して Call Home サービスを設定して有効にするには、次の手順を実行します。

（注） 「（任意）」と特に明記されていない限り、すべての手順を実行する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。プロンプトが表示されたらパスワードを入力します。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**license smart transport callhome** 例： `Device(config)# license smart transport callhome`	転送モードとして Call Home を有効にします。
ステップ 4	**service call-home** 例： `Device(config)# service call-home`	Call Home 機能をイネーブルにします。
ステップ 5	**call-home** 例： `Device(config)# call-home`	Call Home コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 6	**http-proxy** *proxy-address* **proxy-port** *port-number* 例： `Device(config-call-home)# http-proxy 198.51.100.10 port 5000`	Call Home サービスへのプロキシサーバ情報を設定します。 Cisco IOS XE Bengaluru 17.6.1 以降、プロキシサーバーの受け入れ基準が変更されたことに注意してください。プロキシサーバーの応答のステータスコードのみがシステムによって検証され、理由フレーズは検証されません。RFC形式は、`status-line = HTTP-version SP status-code SP reason-phrase CRLF` です。ステータス行の詳細については、RFC 7230 のセクション 3.1.2 を参照してください。
ステップ 7	**exit** 例： `Device(config-call-home)# exit`	Call Home コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 8	**exit** 例： `Device(config)# exit`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。
ステップ 9	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	コンフィギュレーション ファイルに設定を保存します。

スマートアカウントとバーチャルアカウントの割り当て（SSM オンプレミス UI）

この手順を使用して、1 つ以上の製品インスタンスを対応するスマートアカウントおよびバーチャルアカウント情報とともに SSM オンプレミスのデータベースにインポートできます。これにより、SSM オンプレミスは、ローカルバーチャルアカウント（デフォルトのローカル バーチャル アカウント以外）の一部である製品インスタンスを CSSM の正しいライセンスプールにマッピングできます。

始める前に

サポートされているトポロジ：SSM オンプレミス展開（製品スタンス開始型通信）。

手順

ステップ 1 SSM オンプレミスにログインし、[Smart Licensing] ワークスペースを選択します。

ステップ 2 [Inventory] > [SL Using Policy] > [Export/Import All] > [Import Product Instances List] に移動します。

[Upload Product Instances] ウィンドウが表示されます。

ステップ 3 [Download] をクリックして .csv テンプレートファイルをダウンロードし、テンプレート内のすべての製品インスタンスに必要な情報を入力します。

ステップ 4 テンプレートに入力したら、[Inventory] > [SL Using Policy] > [Export/Import All] > [Import Product Instances List] をクリックします。

[Upload Product Instances] ウィンドウが表示されます。

ステップ 5 [Browse] をクリックし、入力した .csv テンプレートをアップロードします。

アップロードしたすべての製品インスタンスのスマートアカウント情報とバーチャルアカウント情報が SSM オンプレミスで使用できるようになりました。

デバイスの検証（SSM オンプレミス UI）

デバイス検証が有効になっている場合、不明な製品インスタンス（SSM オンプレミスデータベース内にない）からの RUM レポートは拒否されます。

デフォルトでは、デバイスは検証されません。検証を有効にするには、次の手順を実行します。

始める前に

サポートされているトポロジ：SSM オンプレミス展開（製品スタンス開始型通信）。

手順

ステップ 1 [On-Prem License Workspace] ウィンドウで、[Admin Workspace] をクリックし、プロンプトが表示されたらログインします。

[On-Prem Admin Workspace] ウィンドウが表示されます。

ステップ 2 [Settings] ウィジェットをクリックします。

[Settings] ウィンドウが表示されます。

ステップ 3 [CSLU] タブに移動し、[Validate Device] トグルスイッチをオンにします。

不明な製品インスタンスからの RUM レポートが拒否されるようになりました。必要な製品インスタンスを SSM オンプレミスデータベースにまだ追加していない場合は、RUM レポートを

送信する前に追加する必要があります。スマートアカウントとバーチャルアカウントの割り当て（SSM オンプレミス UI） （25 ページ） を参照してください

製品インスタンス開始型通信のネットワーク到達可能性の確認

このタスクでは、製品インスタンス開始型通信のネットワーク到達可能性を確認するために必要になる可能性のある設定を提供します。「（必須）」と付いている手順は、すべての製品インスタンスで必須です。他のすべての手順は、製品インスタンスの種類とネットワーク要件に応じて、必須の場合も任意の場合もあります。該当するコマンドを設定します。

（注） ステップ 14、15、および 16 では、必ず次のように設定してください。これらのコマンドは、正しいトラストポイントが使用され、ネットワーク到達可能性に必要な証明書が受け入れられるように設定する必要があります。

始める前に

サポートされているトポロジ：SSM オンプレミス展開（製品スタンス開始型通信）。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。プロンプトが表示されたらパスワードを入力します。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *interface-type-number* 例： `Device (config)# interface gigabitethernet0/0`	インターフェイス コンフィギュレーション モードを開始し、VRF に関連付けられたイーサネットインターフェイス、サブインターフェイス、または VLAN を指定します。
ステップ 4	**vrf forwarding** *vrf-name* 例： `Device(config-if)# vrf forwarding SLP_VRF`	VRF をレイヤ 3 インターフェイスに対応付けます。このコマンドは、インターフェイスでマルチプロトコル VRF をアクティブにします。

	コマンドまたはアクション	目的
ステップ 5	**ip address** *ip-address mask* 例： `Device(config-if)# ip address 192.168.0.1 255.255.0.0`	VRF の IP アドレスを定義します。
ステップ 6	**negotiation auto** 例： `Device(config-if)# negotiation auto`	インターフェイスの速度およびデュプレックスパラメータの自動ネゴシエーション動作を有効にします。
ステップ 7	**end** 例： `Device(config-if)# end`	インターフェイス コンフィギュレーションモードを終了し、グローバル コンフィギュレーションモードを開始します。
ステップ 8	**ip http client source-interface** *interface-type-number* 例： `Device(config)# ip http client source-interface gigabitethernet0/0`	HTTP クライアントのソース インターフェイスを設定します。
ステップ 9	**ip route** *ip-address ip-mask subnet mask* 例： `Device(config)# ip route vrf SLP_VRF 192.168.0.1 255.255.0.0 192.168.255.1`	（必須）製品インスタンスにルートとゲートウェイを設定します。スタティックルートまたはダイナミックルートのいずれかを設定できます。
ステップ 10	{**ip** | **ipv6**} **name-server** *server-address 1 ...server-address 6*] 例： `Device(config)# ip name-server vrf SLP_VRF 198.51.100.1`	VRF インターフェイスでドメインネームシステム（DNS）を設定します。
ステップ 11	**license smart vrf** *vrf_string* 例： `Device(config)# Device(config)# license smart vrf SLP_VRF`	製品インスタンスで使用される VRF 名を設定します。製品インスタンスは VRF を使用して、ライセンス関連のデータを CSSM、CSLU、または SSM オンプレミスに送信します。 製品インスタンスが VRF をサポートするインスタンスであり、対応する URL を使用してトランスポートタイプが **smart** または **cslu** に設定されていることを確認します。

	コマンドまたはアクション	目的
ステップ 12	**ip domain lookup source-interface** *interface-type-number* 例： `Device(config)# ip domain lookup source-interface gigabitethernet0/0`	DNS ドメインルックアップ用のソースインターフェイスを設定します。
ステップ 13	**ip domain name** *domain-name* 例： `Device(config)# ip domain name example.com`	ドメインの DNS ディスカバリを設定します。この例では、ネームサーバがエントリ `cslu-local.example.com` を作成します。
ステップ 14	**crypto pki trustpoint SLA-TrustPoint** 例： `Device(config)# crypto pki trustpoint SLA-TrustPoint` `Device(ca-trustpoint)#`	（必須）製品インスタンスがトランスポイント「SLA-TrustPoint」を使用する必要があることを宣言し、CA トランスポイント コンフィギュレーション モードを開始します。このコマンドを使用してトラストポイントを宣言するまで、製品インスタンスはトラストポイントを認識しません。
ステップ 15	enrollment terminal 例： `Device(ca-trustpoint)# enrollment terminal`	（必須）証明書登録方式を指定します。
ステップ 16	**revocation-check none** 例： `Device(ca-trustpoint)# revocation-check none`	（必須）ピアの証明書が失効していないことを確認するために使用する方法を指定します。SSM オンプレミス展開トポロジの場合は、**none** キーワードを入力します。つまり、失効チェックは実行されず、証明書は常に受け入れられます。
ステップ 17	**exit** 例： `Device(ca-trustpoint)# exit` `Device(config)# exit`	CA トランスポイント コンフィギュレーション モードを終了し、次にグローバル コンフィギュレーション モードを終了してから、特権 EXEC モードに戻ります。
ステップ 18	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	コンフィギュレーション ファイルに設定を保存します。

トランスポート URL の取得（SSM オンプレミス UI）

製品インスタンス開始型通信を SSM オンプレミス展開で展開するときに、製品インスタンスでトランスポート URL を設定する必要があります。このタスクでは、テナント ID を含む完全な URL を SSM オンプレミスから簡単にコピーする方法を示します。

始める前に

サポートされているトポロジ：SSM オンプレミス展開（製品スタンス開始型通信）。

手順

ステップ 1 SSM オンプレミスにログインし、[Smart Licensing] ワークスペースを選択します。

ステップ 2 [Inventory] タブに移動し、ローカルバーチャルアカウントのドロップダウンリスト（右上隅）から、デフォルトのローカルバーチャルアカウントを選択します。この場合、[Inventory] タブの下の領域に [Local Virtual Account: Default] が表示されます。

ステップ 3 [General] タブに移動します。

[Product Instance Registration Tokens] 領域が表示されます。

ステップ 4 [Product Instance Registration Tokens] 領域で、[CSLU Transport URL] をクリックします。

[Product Registration URL] ポップアップウィンドウが表示されます。

ステップ 5 URL 全体をコピーし、アクセス可能な場所に保存します。

製品インスタンスでトランスポートタイプと URL を設定するときに、この URL が必要になります。

ステップ 6 トランスポートタイプと URL を設定します。転送タイプ、URL、およびレポート間隔の設定（60 ページ）を参照してください。

承認コード要求の送信（SSMオンプレミスUI、接続モード）

この手順では、SSM オンプレミスが CSSM に接続されている場合に、輸出規制ライセンスおよび適用済みライセンスにSLACをインストールする方法を示します。最初に、製品インスタンスから SSM オンプレミスに SLAC 要求を送信します。次に、SSM オンプレミスを CSSM と同期する必要があります。CSSM が要求を処理し、応答が SSM オンプレミスに送り返されます。最後に、応答が SSM オンプレミスから製品インスタンスに送信され、SLAC がデバイスにインストールされます。

始める前に

サポートされているトポロジ：SSM オンプレミス展開（製品インスタンス開始型通信）。

CSSMのスマートアカウントとバーチャルアカウントにおける、必要な輸出規制ライセンスまたは適用済みライセンスのバランスが十分にプラスであることを確認します。

手順

ステップ 1 製品インスタンスで、**license smart authorization request** {**add** | **replace**} *feature_name* {**all** | **local** } コマンドを設定します。

SLAC 要求が SSM オンプレミスに送信されます。

既存の SLAC に追加するのか置換するのかを指定します。

- **add**：要求されたライセンスを既存の SLAC に追加します。新しい承認コードには、既存の SLAC のすべてのライセンスと要求されたライセンスが含まれます。
- **replace**：既存のSLACを置き換えます。新しいSLACには、要求されたライセンスのみが含まれます。既存のSLACのすべてのライセンスが返却されます。このキーワードを入力すると、製品インスタンスはこれらの既存のライセンスが使用中かどうかを確認します。使用中の場合は、対応する機能を最初に無効にするようにエラーメッセージが表示されます。

feature_name には、SLAC の追加または置換を要求するライセンスの名前を入力します。たとえば、HSECK9 ライセンスの場合は `hseck9` と入力します。

次のいずれかのオプションを入力して、デバイスを指定します。

- **all**：高可用性設定のすべてのデバイスの承認コードを取得します。
- **local**：高可用性設定のアクティブなデバイスの承認コードを取得します。これがデフォルトのオプションです。

ステップ 2 SSM オンプレミスにログインします。

ステップ 3 SSM オンプレミス UI の [Smart Licensing] ワークスペースで、[Reports] > [Usage Schedules] > [Synchronize now with Cisco] に移動します。

SLAC 要求が CSSM に送信されます。CSSM が要求を処理し、SLAC 応答が SSM オンプレミスに送信されます。SSMオンプレミスは製品インスタンスに応答を送信します。応答は製品インスタンスに自動的にインストールされます。

SSM オンプレミス UI のイベントログを監視して、SLAC が製品インスタンスに送信された時刻を知ることができます。

ステップ 4 製品インスタンスで、特権 EXEC モードで **show license authorization** コマンドを入力して、SLAC 情報を表示します。

承認コード要求の送信（SSMオンプレミスUI、切断モード）

SSM オンプレミス展開のトポロジを使用すると、SSM オンプレミスが CSSM に接続されていない場合、製品インスタンスが同じ承認コードを要求する前に、輸出規制ライセンスと適用済みライセンスに必要な承認コードを CSSM で生成して、SSM オンプレミスにインポートする必要があります。

この手順には、SSM オンプレミスで実行する必要がある手順（要求を送信して、その後に SLAC をインポートする）を説明し、CSSM で実行する必要がある手順（SLAC を生成してダウンロードする）と製品インスタンスで実行する必要がある手順（最終的にSLACを要求してインストールする）を示します。

始める前に

サポートされているトポロジ：

- SSM オンプレミス展開（SSM オンプレミス開始型通信）
- SSM オンプレミス展開（製品インスタンス開始型通信）。

CSSMのスマートアカウントとバーチャルアカウントにおける、必要な輸出規制ライセンスまたは適用済みライセンスのバランスが十分にプラスであることを確認します。

手順

ステップ 1 SSM オンプレミスにログインし、[Smart Licensing] を選択します。

ステップ 2 [Inventory] > [SL Using Policy] に移動します。SLAC を要求するすべての製品インスタンスを選択します。

ステップ 3 [Actions for Selected…] > [Authorization Code Request] をクリックします。

[Authorization Request Information] ポップアップウィンドウが表示されます。

ステップ 4 [Accept] をクリックし、プロンプトが表示されたら .csv ファイルを保存します。

generated.csv ファイルには、選択した製品インスタンスのリストが、CSSM で SLAC を生成するために必要な形式で含まれています。（次のステップで）CSSM Web UI で作業しているときにアクセス可能な場所にこのファイルを保存します。

ステップ 5 CSSM でCSSMへのデータまたは要求のアップロードとファイルのダウンロード（57ページ）のタスクを実行します。

上記の手順を使用して、単一の製品インスタンスに対しても、複数の製品インスタンスに対しても SLAC を生成できます。SSM オンプレミス展開トポロジの場合は、複数の製品インスタンスに SLAC を生成する手順に従います。

ステップ 6 SSM オンプレミス UI に戻り、[Inventory] > [SL Using Policy] に移動します。

ステップ 7 [Export/Import All…] をクリックし、[Import From Cisco] をクリックします。

前述のステップ 5 の最後で CSSM からダウンロードしたファイルをインポートします。

インポートを確認するには、[Inventory] > [SL Using Policy] の下にある [Alerts] 列を参照します。「Authorization message received from CSSM」というメッセージが表示されます。

ステップ 8 製品インスタンスでこのタスクを完了します。SLAC の手動要求と自動インストール （44 ページ）

このタスクでは、SSM オンプレミスから SLAC を要求してインストールする方法を示します。

使用状況データのエクスポートとインポート（SSM オンプレミス UI）

SSM オンプレミスが CSSM から切断されている場合は、この手順を使用して SSMオンプレミスと CSSM との間で使用状況の同期を実行できます。

始める前に

サポートされているトポロジ：

- SSM オンプレミス展開（SSM オンプレミス開始型通信）
- SSM オンプレミス展開（製品インスタンス開始型通信）。

レポートデータは、SSM オンプレミスで使用できる必要があります。必要なレポートデータを製品インスタンスから SSM オンプレミスにプッシュする（製品インスタンス開始型通信）か、または必要なレポートデータを製品インスタンスから取得する（SSM オンプレミス開始型通信）必要があります。

手順

ステップ 1 SSM オンプレミスにログインし、[Smart Licensing] を選択します。

ステップ 2 [Inventory] > [SL Using Policy] タブに移動します。

ステップ 3 [SL Using Policy] タブ領域で、[Export/Import All ...] > [Export Usage to Cisco] をクリックします。

これにより、SSM オンプレミスサーバで使用可能なすべての使用状況レポートを含む .tar ファイルが 1 つ生成されます。

ステップ 4 CSSM でCSSM へのデータまたは要求のアップロードとファイルのダウンロード （57 ページ）のタスクを実行します。

このタスクの最後に、SSM オンプレミスにインポートする ACK ファイルを取得します。

ステップ 5 再度、[Inventory] > [SL Using Policy] タブに移動します。

ステップ 6 [SL Using Policy] タブ領域で、[Export/Import All ...] > [Import From Cisco] をクリックします。.tar ACK ファイルをアップロードします。

ACK インポートを確認するには、[SL Using Policy] タブ領域で、対応する製品インスタンスの [Alerts] 列を確認します。「Acknowledgmentreceived from CSSM」というメッセージが表示されます。

1 つ以上の製品インスタンスの追加（SSM オンプレミス UI）

次の手順を使用して、1 つの製品インスタンスを追加したり、複数の製品インスタンスをインポートして追加したりできます。これにより、SSM オンプレミスは製品インスタンスから情報を取得できるようになります。

始める前に

サポートされているトポロジ：SSM オンプレミス展開（SSM オンプレミス開始型通信）。

手順

ステップ 1 SSM オンプレミス UI にログインし、[Smart Licensing] をクリックします。

ステップ 2 [Inventory] タブに移動します。右上隅にあるドロップダウンリストからローカル バーチャル アカウントを選択します。

ステップ 3 [SL Using Policy] に移動します。

ステップ 4 単一の製品インスタンスを追加するか、または複数の製品インスタンスをインポートします（いずれかを選択します）。

- **単一の製品インスタンスを追加**するには、次の手順を実行します。
  1. [SL Using Policy] タブ領域で、[Add Single Product] をクリックします。
  2. [Host] フィールドにホストの IP アドレスを入力します（製品インスタンス）。
  3. [Connect Method] ドロップダウンリストから、適切な SSM オンプレミス開始型の接続方式を選択します。

     SSM オンプレミス開始型通信に使用できる接続方法は、NETCONF、RESTCONF、および REST API です。
  4. 右側のパネルで、[Product Instance Login Credentials] をクリックします。

     [Product Instance Login Credentials] ウィンドウが表示されます。

（注） 製品インスタンスに SLAC が必要な場合は、ログインクレデンシャルが必要です。さらに、SLAC 要求を処理する前に、有効なスマートアカウントとバーチャルアカウントを追加しておく必要もがあります。

5. [User ID] と [Password] に入力し、[Save] をクリックします。

   これは、ネットワーク到達可能性を確立するために必要なコマンドの一部として設定したものと同じユーザ ID とパスワードです（SSM オンプレミス開始型通信のネットワーク到達可能性の確保 （36 ページ））。

   検証が完了すると、製品インスタンスが [SL Using Policy] タブ領域のリストに表示されます。

- **複数の製品インスタンスをインポート**するには、次の手順を実行します。

1. [SL Using Policy] タブで、[Export/Import All ...] > [Import Product Instances List] をクリックします。

   [Upload Product Instances] ウィンドウが表示されます。

2. [Download] をクリックし、事前に定義した .csv テンプレートをダウンロードします。

3. .csv テンプレートのすべての製品インスタンスに必要な情報を入力します。

   テンプレートで、すべての製品インスタンスの [Host]、[Connect Method]、および [Login Credentials] を必ず指定してください。

   SSM オンプレミス開始型通信に使用できる接続方法は、NETCONF、RESTCONF、および REST API です。

   ログインクレデンシャルは、ネットワーク到達可能性を確立するために必要なコマンドの一部として設定したユーザ ID とパスワードを参照します（SSM オンプレミス開始型通信のネットワーク到達可能性の確保 （36 ページ））。

4. 再度、[Inventory] > [SL Using Policy] タブに移動します。[Export/Import All....] > [Import Product Instances List] をクリックします。

   [Upload Product Instances] ウィンドウが表示されます。

5. 次に、入力した .csv テンプレートをアップロードします。

   検証されると、製品インスタンスが [SL Using Policy] タブのリストに表示されます。

SSMオンプレミス開始型通信のネットワーク到達可能性の確保

このタスクでは、SSMオンプレミス開始型通信のネットワーク到達可能性を確保するために必要になる可能性のある設定を実行します。「（必須）」と付いている手順は、すべての製品インスタンスで必須です。他のすべての手順は、製品インスタンスの種類とネットワーク要件に応じて、必須の場合も任意の場合もあります。該当するコマンドを設定します。

（注） 手順 25、26、および 27 では、必ず次のように設定してください。これらのコマンドは、正しいトラストポイントが使用され、ネットワーク到達可能性に必要な証明書が受け入れられるように設定する必要があります。

始める前に

サポートされているトポロジ：SSM オンプレミス展開（SSM オンプレミス開始型通信）。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。プロンプトが表示されたらパスワードを入力します。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**aaa new model** 例： `Device(config)# aaa new model`	（必須）認証、許可、アカウンティング（AAA）アクセスコントロールモデルをイネーブルにします。
ステップ 4	**aaa authentication login default local** 例： `Device(config)# aaa authentication login default local`	（必須）認証時にローカルのユーザ名データベースを使用するように、AAA 認証を設定します。
ステップ 5	**aaa authorization exec default local** 例： `Device(config)# aaa authorization exec default local`	ネットワークへのユーザアクセスを制限するパラメータを設定します。ユーザは EXEC シェルの実行が許可されます。

	コマンドまたはアクション	目的
ステップ 6	ip routing 例： `Device(config)# ip routing`	IP ルーティングを有効にします。
ステップ 7	{**ip** | **ipv6**} **name-server** *server-address 1 ...server-address 6*] 例： `Device(config)# ip name-server vrf Mgmt-vrf 192.168.1.100 192.168.1.200 192.168.1.300`	（任意）名前とアドレスの解決に使用する 1 つまたは複数のネームサーバのアドレスを指定します。 最大 6 つのネーム サーバを指定できます。各サーバアドレスはスペースで区切ります。最初に指定されたサーバが、プライマリ サーバです。デバイスは、プライマリサーバへDNS クエリを最初に送信します。そのクエリが失敗した場合は、バックアップ サーバにクエリが送信されます。
ステップ 8	**ip domain lookup source-interface** *interface-type-number* 例： `Device(config)# ip domain lookup source-interface gigabitethernet0/0`	デバイス上で、DNS に基づくホスト名からアドレスへの変換を有効にします。この機能は、デフォルトでイネーブルにされています。 ユーザのネットワークデバイスが、名前の割り当てを制御できないネットワーク内のデバイスと接続する必要がある場合、グローバルなインターネットのネーミング方式（DNS）を使用して、ユーザのデバイスを一意に識別するデバイス名を動的に割り当てることができます。 （注） レイヤ 3 物理インターフェイスでこのコマンドを設定した場合、ポートモードが変更されるかデバイスがリロードされると、そのコマンドは実行コンフィギュレーションから自動的に削除されます。これは、コマンドを再設定することでのみ回避できます。Cisco IOS XE Dublin 17.12.1 以降では、この問題は解決されています。

	コマンドまたはアクション	目的
ステップ 9	**ip domain name** *name* 例： `Device(config)# ip domain name vrf Mgmt-vrf cisco.com`	非完全修飾ホスト名（ドット付き10進表記ドメイン名のない名前）を完成させるためにソフトウェアが使用する、デフォルトのドメイン名を定義します。
ステップ 10	**no username** *name* 例： `Device(config)# no username admin`	（必須）指定されたユーザ名が存在する場合はクリアします。*name* には、次のステップで作成するユーザ名と同じものを入力します。これにより、次のステップで作成するユーザ名が重複していないことが保証されます。 SSM オンプレミス開始型の RUM レポートを取得に REST API を使用する場合は、SSMオンプレミスにログインする必要があります。ユーザ名が重複していると、システムにそのユーザ名がある場合はこの機能が正しく動作しない場合があります。
ステップ 11	**username** *name* **privilege** *level* **password** *password* 例： `Device(config)# username admin privilege 15 password 0 lab`	（必須）ユーザ名をベースとした認証システムを構築します。 **privilege** キーワードにより、ユーザの権限レベルを設定します。ユーザの権限レベルを指定する 0 ～ 15 の数字です。 password を使用すると、name 引数にアクセスできます。パスワードは 1 ～ 25 文字で、埋め込みスペースを使用でき、**username** コマンドの最後のオプションとして指定します。 これにより、SSMオンプレミスが製品インスタンスのネイティブ REST を使用できるようになります。

	コマンドまたはアクション	目的
		（注） このユーザ名とパスワードを SSM オンプレミスに入力します（1 つ以上の製品インスタンスの追加（SSM オンプレミス UI）（34 ページ））。これにより、SSM オンプレミスは製品インスタンスから RUM レポートを収集できるようになります。
ステップ 12	**interface** *interface-type-number* 例： `Device (config)# interface gigabitethernet0/0`	インターフェイス コンフィギュレーション モードを開始し、VRF に関連付けられたイーサネットインターフェイス、サブインターフェイス、または VLAN を指定します。
ステップ 13	**vrf forwarding** *vrf-name* 例： `Device(config-if)# vrf forwarding Mgmt-vrf`	VRF をレイヤ 3 インターフェイスに対応付けます。このコマンドは、インターフェイスでマルチプロトコル VRF をアクティブにします。
ステップ 14	**ip address** *ip-address mask* 例： `Device(config-if)# ip address 192.168.0.1 255.255.0.0`	VRF の IP アドレスを定義します。
ステップ 15	**negotiation auto** 例： `Device(config-if)# negotiation auto`	インターフェイスの速度およびデュプレックスパラメータの自動ネゴシエーション動作を有効にします。
ステップ 16	**no shutdown** 例： `Device(config-if)# no shutdown`	無効にされたインターフェイスを再起動します。
ステップ 17	**end** 例： `Device(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 18	**ip http server** 例： `Device(config)# ip http server`	（必須）シスコの Web ブラウザ ユーザ インターフェイスを含む IP または IPv6 システムで HTTP サーバを有効に

	コマンドまたはアクション	目的
		します。HTTP サーバは、デフォルトにより標準のポート 80 を使用します。
ステップ 19	**ip http authentication local** 例： `ip http authentication local` `Device(config)#`	（必須）HTTP サーバユーザに対して特定の認証方法を指定します。 **local** キーワードは、認証および許可に、ローカルシステム設定で（username グローバル コンフィギュレーション コマンドによって）指定したログイン ユーザ名、パスワード、権限レベル アクセスの組み合わせを使用することを示します。
ステップ 20	**ip http secure-server** 例： `Device(config)# ip http server`	（必須）セキュア HTTP（HTTPS）サーバを有効にします。HTTPS サーバは、セキュア ソケット レイヤ（SSL）バージョン 3.0 プロトコルを使用します。
ステップ 21	**ip http max-connections** 例： `Device(config)# ip http max-connections 16`	（必須）HTTP サーバへの同時最大接続数を設定します。1 ～ 16 の範囲の整数を入力します。デフォルトは 5 です。
ステップ 22	**ip tftp source-interface** *interface-type-number* 例： `Device(config)# ip tftp source-interface GigabitEthernet0/0`	TFTP 接続用の送信元アドレスとして、インターフェイスの IP アドレスを指定します。
ステップ 23	**ip route** *ip-address ip-mask subnet mask* 例： `Device(config)# ip route vrf mgmt-vrf` `192.168.0.1 255.255.0.0 192.168.255.1`	製品インスタンスにルートとゲートウェイを設定します。スタティック ルートまたはダイナミック ルートのいずれかを設定できます。
ステップ 24	**logging host** 例： `Device(config)# logging host 172.25.33.20` `vrf Mgmt-vrf`	リモート ホストへのシステム メッセージおよびデバッグ出力を記録します。
ステップ 25	**crypto pki trustpoint SLA-TrustPoint** 例：	（必須）製品インスタンスがトランスポイント「SLA-TrustPoint」を使用する必要があることを宣言し、CA トラン

	コマンドまたはアクション	目的
	Device(config)# **crypto pki trustpoint SLA-TrustPoint** Device(ca-trustpoint)#	スポイント コンフィギュレーション モードを開始します。このコマンドを使用してトラストポイントを宣言するまで、製品インスタンスはトラストポイントを認識しません。
ステップ 26	enrollment terminal 例： Device(ca-trustpoint)# **enrollment terminal**	（必須）証明書登録方式を指定します。
ステップ 27	**revocation-check none** 例： Device(ca-trustpoint)# **revocation-check none**	（必須）ピアの証明書が失効していないことを確認するために使用する方法を指定します。SSM オンプレミス展開トポロジの場合は、**none** キーワードを入力します。つまり、失効チェックは実行されず、証明書は常に受け入れられます。
ステップ 28	**end** 例： Device(ca-trustpoint)# **exit** Device(config)# **end**	CA トランスポイントコンフィギュレーションモードを終了し、次にグローバル コンフィギュレーションモードを終了してから、特権 EXEC モードに戻ります。
ステップ 29	**show ip http server session-module** 例： Device# **show ip http server session-module**	（必須）HTTP 接続を確認します。出力で、SL_HTTP がアクティブであることを確認します。また、次のチェックも実行できます。 • SSM オンプレミスがインストールされているデバイスから、製品インスタンスに ping できることを確認します。ping が成功すると、製品インスタンスが到達可能であることが確認されます • SSM オンプレミスがインストールされているデバイスの Web ブラウザで、https://<product-instance-ip>/ を確認します。これにより、SSM オンプレミスから製品インスタンスへの REST API が期待どおりに動作することが保証されます。

	コマンドまたはアクション	目的
ステップ 30	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	コンフィギュレーションファイルに設定を保存します。

CSSM からの SLAC の生成とファイルへのダウンロード

CSSM で SLAC を生成してファイルにダウンロードするには、CSSM で次の手順を実行します。

始める前に

サポートされるトポロジ：

- CSSM への接続なし、CSLU なし
- CSLU は CSSM から切断
- SSM オンプレミス展開（製品インスタンス開始型通信と SSM オンプレミス開始型通信）

この手順を使用して、単一の製品インスタンスに対しても、複数の製品インスタンスに対しても SLAC を生成できます。

単一の製品インスタンスの場合、このタスクを実行するにはPIDとシリアル番号が必要です。製品インスタンスで、特権 EXEC モードで **show license udi** コマンドを入力し、情報を控えておきます。

複数の製品インスタンスの場合は、.csvファイル（必要な製品インスタンス情報を含む）をアクセス可能な場所に保存します。

手順

ステップ 1 https://software.cisco.com で CSSM Web UI にログインし、[Manage licenses] をクリックします。

シスコから提供されたユーザ名とパスワードを使用してログインします。[Smart Software Licensing] ページが表示されます。

ステップ 2 [Inventory] タブをクリックします。

ステップ 3 [Product Instances] タブをクリックします。

ステップ 4 [Authorize License Enforced Features] タブをクリックします。

ステップ 5 単一の製品インスタンスまたは複数の製品インスタンスにSLACを生成します（いずれかを選択）。

- **単一の製品インスタンスに SLAC を生成するには、次の手順を実行します。**

1. [PID] と [Serial Number] を入力します。

   （注） 他のフィールドは入力しないでください。

2. ライセンスを選択し、対応する [Reserve] 列に **1** を入力します。

   PID に対して正しいライセンスを選択したことを確認します。参考情報については、ルーティング製品インスタンスの HSECK9 ライセンス マッピング テーブル （81 ページ） を参照してください。

3. [Next] をクリックします。
4. [承認コードを生成（Generate Authorization Code）] をクリックします。
5. 承認コードをダウンロードし、.csv ファイルとして保存します。
6. 製品インスタンスへのファイルのインストール「製品インスタンスへのファイルのインストール （59 ページ）」を参照してください。

- **複数の製品インスタンスに SLAC を生成するには次の手順を実行します（この場合、.csv ファイルをアップロードします）。**

1. [Single Device]（デフォルト）というドロップダウンリストで、選択を [Multiple Devices] に変更します。
2. [Browse] をクリックし、SLAC を必要とする製品インスタンスのリストを含む .csv ファイルに移動します。
3. アップロードすると、デバイスのリストが CSSM に表示されます。すべてのデバイスのチェックボックスが有効になったら（すべてのデバイスの SLAC を要求することを意味します） [Next] をクリックします。
4. 各製品インスタンスに必要なライセンス数を指定し、[Next] をクリックします。

   （注） Smart Licensing Using Policy 環境で輸出規制ライセンスまたは適用済みのライセンスに SLAC を要求する場合は、製品インスタンスごとに必要な SLAC は 1 つのみです。

5. [Device Type] ドロップダウンリストから [DNA On-Prem] を選択し、[Continue] をクリックします。
6. [Reserve Licenses] をクリックします。

   [Download Authorization Code] ボタンが表示されます。

7. [Download Authorization Codes] をクリックして、この .csv ファイルをダウンロードします。このファイルには、上記の手順 c. のすべての製品インスタンスの SLAC が含まれています。[**閉じる（Close）**] をクリックします。

8. これで、この .csv ファイルを SSM オンプレミスにインポートできるようになりました。承認コード要求の送信（SSM オンプレミス UI、切断モード） （32 ページ）に戻り、残りの手順を実行してこのファイルをインポートします。

SLAC の手動要求と自動インストール

CSSM、CSLU、または SSM オンプレミスに SLAC を要求し、製品インスタンスに自動的にインストールするには、製品インスタンスで次の手順を実行します。

始める前に

サポートされるトポロジ：

- CSLU を介して CSSM に接続
- CSSM に直接接続
- SSM オンプレミス展開（製品インスタンス開始型通信）

続行する前に、次の点も確認してください。

- SLAC を要求している製品インスタンスが CSSM、CSLU、または SSM オンプレミスに接続されています。
- 転送タイプがそれに応じて設定されている（CSSM の場合は **smart**、CSLU の場合は **cslu**）。**show license all** コマンドは特権 EXEC モードで入力します。出力で、`Transport:` フィールドを確認します。
- CSSM に直接接続している場合は、信頼コードがインストールされています。**show license all** コマンドは特権 EXEC モードで入力します。出力で、`Trust Code Installed:` フィールドを確認します。
- SSM オンプレミスが切断モードになる SSM オンプレミス展開の場合、このタスクで製品インスタンスから SLAC の SSM オンプレミスが要求されるため、このタスクを開始する前に、必要な SLAC ファイルが SSM オンプレミスサーバーで使用可能になっている必要があります。「承認コード要求の送信（SSM オンプレミス UI、切断モード） （32 ページ）」を参照してください

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。プロンプトが表示されたら、パスワードを入力します。

	コマンドまたはアクション	目的
ステップ 2	**license smart authorization request** {**add** | **replace**} *feature_name* {**all** | **local**} 例： `Device# license smart authorization request add hseck9 local`	**license smart authorization request** コマンドは、SLAC を CSSM または CSLU（CSLU は CSSM から取得）または SSM オンプレミスから要求します。SLAC が返され、製品インスタンスに自動的にインストールされます。 既存の SLAC に追加するのか置換するのかを指定します。 • **add**：要求されたライセンスを既存の SLAC に追加します。新しい承認コードには、既存の SLAC のすべてのライセンスと要求されたライセンスが含まれます。 • **replace**：既存の SLAC を置き換えます。新しい SLAC には、要求されたライセンスのみが含まれます。既存の SLAC のすべてのライセンスが返却されます。このキーワードを入力すると、製品インスタンスはこれらの既存のライセンスが使用中かどうかを確認します。使用中の場合は、対応する機能を最初に無効にするようにエラーメッセージが表示されます。 *feature_name* には、SLAC の追加または置換を要求するライセンスの名前を入力します。 次のいずれかのオプションを入力して、デバイスを指定します。 • **all**：高可用性設定のすべてのデバイスの承認コードを取得します。 • **local**：高可用性設定のアクティブなデバイスの承認コードを取得します。これがデフォルトのオプションです。 または、次のいずれかの方法を使用して SLAC を要求してインストールします。各オプションでサポートされるプラットフォームに注意してください。

	コマンドまたはアクション	目的
		• Cisco 1000、4000 シリーズ サービス統合型ルータ、Catalyst 8200 エッジプラットフォーム、および 8300 エッジプラットフォームのみ： **license feature** *feature_name*：機能が自動的にコードを要求できるようにします。 `Device(config)# license feature hseck9` • Catalyst 8000V エッジソフトウェア、シスコ クラウド サービス ルータ 1000v、シスコサービス統合型仮想ルータのみ **platform hardware throughput level MB** {**500** |**1000** | **2500** | **5000**}：必要な SLAC を要求してインストールします。これは、ここで指定されたスループット値キーワード（250 MB を超える値）でのみサポートされます。 `Device(config)# platform hardware throughput level MB 5000`
ステップ 3	**show license authorization** 例： `Device# show license authorization`	製品インスタンスにインストールされている承認コード（SLAC）を表示します。

製品インスタンスでの SLAC 要求の生成と保存

HSECK9 キーの SLAC 要求を生成し、製品インスタンスのファイルに保存するには、次のタスクを実行します。

（注） SLAC を要求するこの方法は、Cisco IOS XE cupertino 17.7.1a 以降でのみサポートされています。

始める前に

サポートされるトポロジ：CSSM への接続なし、CSLU なし

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**license smart authorization request** {**add** | **replace**} *feature_name* {**all**| **local**} 例： `Device# license smart authorization request add hseck9 local`	必要なライセンスと UDI の詳細を含む SLAC 要求を生成します。 既存の SLAC に追加するのか置換するのかを指定します。 • **add**：要求されたライセンスを既存の SLAC に追加します。新しい承認コードには、既存の SLAC のすべてのライセンスと要求されたライセンスが含まれます。 • **replace**：既存の SLAC を置き換えます。新しい SLAC には、要求されたライセンスのみが含まれます。既存の SLAC のすべてのライセンスが返却されます。このキーワードを入力すると、製品インスタンスはこれらの既存のライセンスが使用中かどうかを確認します。使用中の場合は、対応する機能を最初に無効にするようにエラーメッセージが表示されます。 *feature_name* には、SLAC の追加または置換を要求するライセンスの名前を入力します。 次のいずれかのオプションを入力して、デバイスを指定します。 • **all**：高可用性設定のすべてのデバイスの承認コードを取得します。 • **local**：高可用性設定のアクティブなデバイスの承認コードを取得します。これがデフォルトのオプションです。

	コマンドまたはアクション	目的
ステップ 3	**license smart authorization request save** *path* 例： `Device# license smart authorization request save bootflash:slac.txt`	SLAC 要求に必要な UDI およびライセンスの詳細を、指定した場所の .txt ファイルに保存します。
ステップ 4	CSSM Web UI にファイルをアップロードし、SLAC コードを含むファイルをダウンロードします。	次のタスクを実行します：CSSM へのデータまたは要求のアップロードとファイルのダウンロード （57 ページ）
ステップ 5	製品インスタンスへのファイルのインストール	次のタスクを実行します：製品インスタンスへのファイルのインストール （59 ページ）

承認コードの削除と返却

このタスクでは、ライセンスの承認コードを削除し、CSSMのライセンスプールに返却する方法を示します。デバイスの承認コードは、Smart Licensing Authorization Code（SLAC）、特定のライセンス予約（SLR）承認コード、製品アクティベーションキー（PAK）、パーマネントライセンス予約（PLR）承認コードのいずれかです。

次の状況では、製品インスタンスの承認コードを削除して返却する必要がある場合があります。

- HSECK9 ライセンスが必要な暗号化機能を使用する必要がなくなった場合。
- 返品許可（RMA）のためにデバイスを返却するか、永久にデコミッションする場合。RMA またはデコミッションプロセスの一環として、工場出荷時の状態へのリセットを実行する必要がありますが、実行する前に、承認コードを削除し、ライセンスを CSSM のライセンスプールに返却します。

（注） すべての承認コードについて、手順全体を実行する必要があるわけではありません。また、一部の製品インスタンスでは、コードを自分で削除して返却することはできません。「**はじめる前に**」に記載されている、承認コードの種類ごとの具体的なガイドラインと、製品インスタンス間の前提条件の違いに注意してください。

始める前に

サポートされるトポロジ：すべて

- HSECK9 ライセンス用の SLAC を返却するには、次の手順を実行します。

- Cisco 1000、4000 シリーズ サービス統合型ルータでは、最初に SLAC がインストールされている HSECK9 ライセンスを無効にします。次に、構成の変更を保存し、デバイスをリロードすると、HSECK9 ライセンスのステータスが NOT IN USE と表示されます。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# no license feature hseck9
% use 'write' command to disable 'hseck9' license on next boot
Device(config)# end
Device# copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
Device# reload
Proceed with reload? [confirm]
.
.
.
Device# show license summary
Account Information:
  Smart Account: Eg-SA As of Jan 29 07:10:00 2023 UTC
  Virtual Account: Eg-VA
License Usage:
  License                 Entitlement tag               Count Status
  -----------------------------------------------------------------------------

  hseck9                  (ISR_4331_Hsec)                   0 NOT IN USE
  booster_performance     (ISR_4331_BOOST)                  1 IN USE
  appxk9                  (ISR_4331_Application)            1 IN USE
  uck9                    (ISR_4331_UnifiedCommun...)       1 IN USE
  securityk9              (ISR_4331_Security)               1 IN USE
```

前述の前提条件が満たされたら、残りの手順を実行し、SLAC を削除してから返却します。以下の手順を参照してください。

- Cisco Catalyst 8200 および 8300 エッジプラットフォームでは、最初にスループットを 250 Mbps 未満に設定します。値は、階層ベースの値または数値にできます。次に、SLAC がインストールされている HSECK9 ライセンスを無効にします。最後に、構成の変更を保存し、デバイスをリロードすると、HSECK9 ライセンスのステータスが NOT IN USE と表示されます。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# platform hardware throughput crypto ?
  100M  100 mbps bidirectional thput
  10M   10 mbps bidirectional thput
  15M   15 mbps bidirectional thput
  1G    2 gbps aggregate thput
  2.5G  5 gbps aggregate thput
  250M  250 mbps bidirectional thput
  25M   25 mbps bidirectional thput
  500M  1gbps aggregate thput
  50M   50 mbps bidirectional thput
  T0    T0(up to 15 mbps) bidirectional thput
  T1    T1(up to 100 mbps) bidirectional thput
  T2    T2(up to 2 gbps) aggregate thput
  T3    T3(up to 5 gbps) aggregate thput
Device(config)# platform hardware throughput crypto 10M

Device(config)# no license feature hseck9
```

```
% use 'write' command to disable 'hseck9' license on next boot
Device(config)# end
Device# copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
*Jan 31 05:13:22.556: %SYS-6-PRIVCFG_ENCRYPT_SUCCESS: Successfully encrypted
private config file
*Jan 31 05:13:22.563: %CRYPTO_SL_TP_LEVELS-6-VAR_NEW_VALUE: Setting crypto bidir
 throughput to: 10000 kbps

Device# reload
Proceed with reload? [confirm]
.
.
.
Device# show license summary
Account Information:
  Smart Account: Eg-SA As of Jan 29 07:10:00 2023 UTC
  Virtual Account: Eg-VA

License Usage:
  License                 Entitlement Tag     Count Status
  -----------------------------------------------------------
  network-advantage_10M   (ESR_P_10M_A)           1 IN USE
  dna-advantage_10M       (DNA_P_10M_A)           1 IN USE
  Router US Export Lic... (DNA_HSEC)              0 NOT IN USE
```

前述の前提条件が満たされたら、残りの手順を実行し、SLAC を削除してから返却します。以下の手順を参照してください。

- Catalyst 8000V エッジソフトウェア（.bin イメージが Catalyst 8000V ソフトウェアイメージにアップグレードされたシスコ クラウド サービス ルータ 1000v およびシスコ サービス統合型仮想ルータを含む）では、最初にスループットを 250 Mbps 未満に設定します。値は、階層ベースの値または数値にできます。変更を有効にするために、デバイスをリロードする必要はありません。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# platform hardware throughput level MB ?
  100    Mbps
  1000   Mbps
  10000  Mbps
  15     Mbps
  25     Mbps
  250    Mbps
  2500   Mbps
  50     Mbps
  500    Mbps
  5000   Mbps
  T0     Tier0(up to 15M throughput)
  T1     Tier1(up to 100M throughput)
  T2     Tier2(up to 1G throughput)
  T3     Tier3(up to 10G throughput)
  T4     Tier4(unthrottled)

Device(config)# platform hardware throughput level MB T1
The current throughput level is 100000 kb/s
Device(config)# end
```

前述の前提条件が満たされたら、残りの手順を実行し、SLAC を削除してから返却します。以下の手順を参照してください。

- Catalyst 8500 エッジプラットフォームでは、HSECK9 ライセンスを自分で無効化することはできません。SLAC を返却するには、代わりにケースを開く必要があります。Support Case Manager に移動します。[Open New Case] をクリックして、[Software Licensing] を選択します。適切なカテゴリを選択し、[Open Case] をクリックします。ケースにスマートアカウント、バーチャルアカウント、デバイスの UDI 情報を入力していることを確認します。ライセンスチームから、プロセスの開始や追加情報について連絡があります。

  以下の手順のステップは、このプラットフォームには適用されません。

- SLR 承認コードを返却する場合は、以下の手順を実行します。SLR 承認コードに HSECK9 ライセンスが含まれているかどうかに関係なく、手順は同じです。
- PAK の返却については、PAK ライセンスの削除 （68 ページ）を参照してください。
- PLR 承認コードの返却については、PLR の非アクティブ化 （79 ページ）を参照してください。

手順

	コマンドまたはアクション	目的
ステップ 1	**license smart authorization return** {**all** | **local**} {**offline** [*path*] | **online**} 例： `Device# license smart authorization return local online` `OR` `Device# license smart authorization return local offline` `Enter this return code in Cisco Smart Software Manager portal:` `UDI: PID:C8300-1N1S-4T2X,SN:FDO2349A00R` `Return code: CrMfaJ-9odPW7-gr2DzP-t3srpf-ATqzGS-wGF3c6-U3Kg77-GdiABx-gud` `*Jan 31 05:18:00.804: %SMART_LIC-6-AUTHORIZATION_REMOVED: A licensing authorization code has been removed from PID:C8300-1N1S-4T2X,SN:FDO2349A00R.` `OR` `Device# license smart authorization return local offline bootflash:return-code.txt`	CSSM のライセンスプールに承認コードを返却します。このコマンドを入力すると、戻りコードが表示されます。 製品インスタンスを指定します。 • all：高可用性セットアップで接続されたすべての製品インスタンスに対してアクションを実行します。 • local：アクティブな製品インスタンスに対してアクションを実行します。これがデフォルトのオプションです。 CSSM に接続しているかどうかを指定します。 • CSSM に接続している場合は、**online** を入力します。コードは自動的に CSSM に返却され、確認が返されて製品インスタンスにインストールされます。このオプションを

	コマンドまたはアクション	目的
		選択すると、戻りコードが自動的にCSSM に送信されます。 • CSSM に接続していない場合は、**offline** を入力します。 オフラインオプションを選択した場合は、これを CSSM に送信する追加の手順を完了する必要があります。 • CLI または保存されたファイルから返却コードをコピーし、CSSM に入力します：CSSM でのリターンコードの入力と製品インスタンスの削除 （53 ページ）17.7.1a より以前のソフトウェアバージョンでは、この手順のみを使用してコードを返却することができます。 • ファイルを保存するパスを指定し、ファイルを CSSM にアップロードします。このコードを返却する手順は、17.7.1a 以降で使用できます：CSSM へのデータまたは要求のアップロードとファイルのダウンロード （57 ページ） ファイル形式は、読み取り可能な任意の形式にすることができます。例：`Device# license smart authorization return local offline bootflash:return-code.txt`. （注） SSM オンプレミス展開の場合は、**online** オプションのみを使用します。**offline** オプションはサポートされていません。
ステップ 2	**show license all** 例：	ライセンス情報を表示します。出力の `License Authorizations` ヘッダーを確認します。返却プロセスが正常に完了する

	コマンドまたはアクション	目的
	Device# **show license all** . . . License Authorizations ========== Overall status: Active: PID:C8300-1N1S-4T2X,SN:FDO2349A00R Status: NOT INSTALLED Last return code: CrMfaJ-9odPW7-gr2DzP-t3srpf-ATqzGS-wGF3c6-U3Kg77-GdiABx-gud . . .	と、Last return code: フィールドに戻りコードが表示されます。
ステップ 3	**show license summary** 例： Device# **show license summary** Account Information: Smart Account: Eg-SA As of Jan 31 05:31:20 2023 UTC Virtual Account: Eg-VA License Usage: License Entitlement Tag Count Status network-advantage_10M (ESR_P_10M_A) 1 IN USE dna-advantage_10M (DNA_P_10M_A) 1 IN USE	製品インスタンスで使用可能なライセンスがすべて表示されます。添付の例では、HSECK9 ライセンスが表示されなくなりました。

CSSM でのリターンコードの入力と製品インスタンスの削除

設定済みの **license smart authorization return** {**all** | **local**} **offline** を設定して承認コードを返す場合は、CSSM にリターンコードを入力して、返却処理を完了する必要があります。

この手順は、すべての承認コード（SLAC、SLR、PLR など）に使用できます

始める前に

サポートされるトポロジ：CSSM への接続なし、CSLU なし

手順

ステップ 1 https://software.cisco.com で CSSM Web UI にログインし、[Manage licenses] をクリックします。

シスコから提供されたユーザ名とパスワードを使用してログインします。[Smart Software Licensing] ページが表示されます。

ステップ 2 [Inventory] タブをクリックします。

ステップ 3 [Virtual Account] ドロップダウンリストから、バーチャルアカウントを選択します。

ステップ 4 [Product Instances] タブをクリックします。

使用可能な製品インスタンスのリストが表示されます。

ステップ 5 製品インスタンスリストから必要な製品インスタンスを見つけます。オプションで、検索タブに名前または製品タイプの文字列を入力して、製品インスタンスを検索できます。

ステップ 6 製品インスタンスの [Actions] 列で、[Actions] ドロップダウンリストから [Remove] を選択します。

[Remove Reservation] ウィンドウが表示されます。

ステップ 7 [Reservation Return Code] フィールドに、戻りコードを入力します。

ライセンスがライセンスプールに戻されます。[Remove Reservation] ウィンドウが自動的に閉じ、[Product Instances] タブに戻ります。

（注） ライセンスの返却のみの場合、これでタスクは終了です。CSSMから製品インスタンスも削除する場合は、次の手順に進みます。

ステップ 8 製品インスタンスの [Actions] 列で、[Actions] ドロップダウンリストから再度 [Remove] を選択します。

[Confirm Remove Product Instance] ウィンドウが表示されます。

ステップ 9 [Remove Product Instance] をクリックします。

製品インスタンスが CSSM から削除され、ライセンスが消費されなくなります。

CSSM からの信頼コード用新規トークンの生成

信頼コードを要求するトークンを生成するには、次の手順を実行します。

所有するバーチャルアカウントごとに 1 つのトークンを生成します。1 つのバーチャルアカウントに属するすべての製品インスタンスに同じトークンを使用できます。

始める前に

サポートされるトポロジ：CSSM に直接接続

手順

ステップ 1 https://software.cisco.com で CSSM Web UI にログインし、[Manage licenses] をクリックします。

シスコから提供されたユーザ名とパスワードを使用してログインします。[Smart Software Licensing] ページが表示されます。

ステップ 2 [Inventory] タブをクリックします。

ステップ 3 [Virtual Account] ドロップダウンリストから、必要なバーチャルアカウントを選択します。

ステップ 4 [General] タブをクリックします。

ステップ 5 [New Token] をクリックします。[Create Registration Token] ウィンドウが表示されます。

ステップ 6 [Description] フィールドに、トークンの説明を入力します。

ステップ 7 [Expire After] フィールドに、トークンをアクティブにする必要がある日数を入力します。

ステップ 8 （オプション）[Max. Number of Uses] フィールドに、トークンの有効期限が切れるまでの最大使用回数を入力します。

（注） ここで値を入力する場合は、プロセスの次の部分で信頼コードのインストールのタイミングを調整してください。多数の製品インスタンスに信頼コードを同時にインストールする場合は、このフィールドを空白のままにしておくことをお勧めします。ここで上限を入力して多数のデバイスに信頼コードを同時にインストールすると、CSSMにおけるこれらの要求の処理でボトルネックが発生し、一部のデバイスへのインストールが「`Failure Reason: Server error occurred: LS_LICENGINE_FAIL_TO_CONNECT`」というエラーで失敗する可能性があります。

ステップ 9 [Create Token] をクリックします。

ステップ 10 リストに新しいトークンが表示されます。[Actions] をクリックし、トークンを `.txt` ファイルとしてダウンロードします。

ID トークンによる信頼の確立

CSSM との信頼できる接続を確立するには、次の手順を実行します。

始める前に

サポートされるトポロジ：CSSM に直接接続

このタスクを実行する前に、CSSM から ID トークンファイルを生成してダウンロードしたことを確認してください。CSSM からの信頼コード用新規トークンの生成 （54 ページ）

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**license smart trust idtoken** *id_token_value* {**local** | **all**} [**force**] 例： `Device# license smart trust idtoken NGMwMjk5mYtNZaxMS00NzMZmtgWm all force`	信頼要求を送信して、CSSM との信頼できる接続を確立します。*id_token_value* には、CSSM で生成したトークンを入力します。 次のいずれかのオプションを入力します。 • **local**：高可用性セットアップのアクティブデバイスに対してのみ信頼要求を送信します。これがデフォルトのオプションです。 • **all**：高可用性セットアップのすべてのデバイスに対して信頼要求を送信します。 製品インスタンスに既存の信頼コードがあるにもかかわらず、信頼コード要求を送信するには、**force** キーワードを入力します。 信頼コードは、製品インスタンスの UDI にノードロックされます。UDI に信頼コード（CSSM との信頼できる接続）がすでにある場合、CSSM では同じ UDI に対する新しい信頼コードは許可されません。**force** キーワードを入力すると、CSSM に送信されるメッセージに強制フラグが設定され、すでに存在する場合でも新しい信頼コードが作成されます。
ステップ 3	**show license status** 例： `<output truncated>` `Trust Code Installed:` `  Active:` `PID:C9500-24Y4C,SN:CAT2344L4GH` `  INSTALLED on Sep 04 01:01:46 2020 EDT` `  Standby:` `PID:C9500-24Y4C,SN:CAT2344L4GJ`	信頼コードがインストールされている場合は、日時が表示されます。日時はローカルタイムゾーンで表示されます。`Trust Code Installed:` フィールドを参照してください。

	コマンドまたはアクション	目的
	INSTALLED on Sep 04 01:01:46 2020 EDT	

CSSM からのポリシーファイルのダウンロード

カスタムポリシーを要求した場合、または製品インスタンスに適用されるデフォルトとは異なるポリシーを適用する場合は、次のタスクを実行します。

始める前に

サポートされるトポロジ：

- CSSM への接続なし、CSLU なし
- CSLU は CSSM から切断

手順

ステップ 1 https://software.cisco.com で CSSM Web UI にログインし、[Manage licenses] をクリックします。

シスコから提供されたユーザ名とパスワードを使用してログインします。[Smart Software Licensing] ページが表示されます。

ステップ 2 次のディレクトリパス、[Reports] > [Reporting Policy] を移動します。

ステップ 3 [Download] をクリックして、`.xml` ポリシーファイルを保存します。

これで、ファイルを製品インスタンスにインストールできます。製品インスタンスへのファイルのインストール （59 ページ） を参照してください

CSSM へのデータまたは要求のアップロードとファイルのダウンロード

このタスクは、次の目的で使用できます。

- RUM レポートを CSSM にアップロードし、ACK をダウンロードします。
- SLAC 要求ファイルをアップロードし、SLAC コードファイルをダウンロードします。

  この方法は、Cisco IOS XE Cupertino 17.7.1a 以降でサポートされています。
- SLAC 返却ファイルをアップロードします。

  この方法は、Cisco IOS XE Cupertino 17.7.1a 以降でサポートされています。

製品インスタンスが CSSM に接続されていない場合、または CSLU や SSM オンプレミスが CSSM に接続されていない場合にファイルを CSSM にアップロードし、ファイルをダウンロードするには、次のタスクを実行します。

始める前に

サポートされるトポロジ：

- CSSM への接続なし、CSLU なし
- CSLU は CSSM から切断
- SSM オンプレミス展開（製品インスタンス開始型通信と SSM オンプレミス開始型通信）

手順

ステップ 1 https://software.cisco.com で CSSM Web UI にログインし、[Manage licenses] をクリックします。

シスコから提供されたユーザ名とパスワードを使用してログインします。[Smart Software Licensing] ページが表示されます。

ステップ 2 レポートを受信する**スマートアカウント**（画面の左上隅）を選択します。

ステップ 3 [Smart Software Licensing] → [Reports] → [Usage Data Files] を選択します。

ステップ 4 [Upload Usage Data] をクリックします。ファイルの場所（tar 形式の RUM レポート）を参照して選択し、[Upload Data] をクリックします。

RUM レポート（.tar形式）、SLAC 要求ファイル（.txt形式）、または SLAC 返却要求ファイル（.txt 形式）をアップロードします。

アップロードされたファイルは削除できません。ただし、必要に応じて別のファイルをアップロードできます。

ステップ 5 [Select Virtual Accounts] ポップアップから、アップロードされたファイルを受信する**バーチャルアカウント**を選択します。ファイルがシスコにアップロードされ、[Reports] 画面の [Usage Data Files] テーブルにファイル名、レポートの時刻、アップロード先のバーチャルアカウント、レポートステータス、レポートされた製品インスタンス数、確認ステータスが表示されます。

ステップ 6 [Acknowledgment] 列で [Download] をクリックして、アップロードしたレポートまたは要求の ACK または SLAC を保存します。

[Acknowledgment] 列にファイルが表示されるまで待つ必要があります。処理する RUM レポートまたは要求が多数ある場合、CSSM では数分かかることがあります。

ファイルをダウンロードしたら、ファイルをインポートして製品インスタンスにインストールするか、CSLU または SSM On-Prem に転送します。

製品インスタンスへのファイルのインストール

SLAC、ポリシー、またはACKを製品インスタンスにインストールするには、次のタスクを実行します。

始める前に

サポートされるトポロジ：CSSMへの接続なし、CSLUなし

製品インスタンスにアクセスできる場所に、対応するファイルを保存しておく必要があります。

- SLACについては、CSSMからのSLACの生成とファイルへのダウンロード（42ページ）またはCSSMへのデータまたは要求のアップロードとファイルのダウンロード（57ページ）（エアーギャップネットワークでSLACファイルを取得する方法は複数あります）を参照してください。
- ポリシーについては、CSSMからのポリシーファイルのダウンロード（57ページ）を参照してください。
- ACKについては、CSSMへのデータまたは要求のアップロードとファイルのダウンロード（57ページ）を参照してください。

手順

	コマンドまたはアクション	目的
ステップ1	**enable** 例： `Device> enable`	特権EXECモードを有効にします。プロンプトが表示されたら、パスワードを入力します。
ステップ2	**copy** *source* **bootflash:***file-name* 例： `Device# copy tftp://10.8.0.6/user01/example.txt bootflash:`	ファイルをソースの場所またはディレクトリから製品インスタンスのフラッシュメモリにコピーします。 • *source*：これは、コピー元となるファイルまたはディレクトリの場所です。コピー元は、ローカルまたはリモートのいずれかです。 • **bootflash:**：これはブートフラッシュメモリの場合の宛先です。
ステップ3	**license smart import bootflash:** *file-name* 例： `Device# license smart import bootflash:example.txt`	ファイルを製品インスタンスにインポートしてインストールします。インストール後、システムメッセージが表示されま

	コマンドまたはアクション	目的
		す。これは、インストールしたファイルのタイプを示します。 SLACの場合、製品インスタンスは、この新しいファイルが使用中のすべてのライセンスを正しく説明していることを確認します。正常にインストールされると、既存のコードが新しいコードに置き換えられます。
ステップ4	**show license all** 例： `Device# show license all`	製品インスタンスのライセンス承認、ポリシー、およびレポート情報を表示します。

転送タイプ、URL、およびレポート間隔の設定

製品インスタンスの転送モードを設定するには、次のタスクを実行します。

始める前に

サポートされるトポロジ：すべて

手順

	コマンドまたはアクション	目的
ステップ1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。プロンプトが表示されたらパスワードを入力します。
ステップ2	**configure terminal** 例： `Device# configure terminal`	
ステップ3	**license smart transport** {**automatic** | **callhome** | **cslu** | **off** | **smart**} 例： `Device(config)# license smart transport cslu`	製品インスタンスが使用するメッセージ転送のタイプを選択します。次のオプションから選択します。 • **automatic**：転送モードをデフォルト（CSLU）に設定します。 • **callhome**：転送モードとして Call Home を有効にします。

	コマンドまたはアクション	目的
		• **cslu**：これがデフォルトのトランスポートモードです。製品インスタンス開始型通信で CSLU または SSM オンプレミスを使用している場合は、このキーワードを入力します。 （注） CSLU と SSM オンプレミスの両方に同じトランスポートモードが適用されますが、URL が異なります。次のステップの **cslu***cslu_or_on-prem_url* を参照してください。 • **off**：製品インスタンスからのすべての通信を無効にします。 • **smart**：スマート転送を有効にします。 （注） 転送方式を **callhome** から **smart** に変更する場合、Smart Licensing Using Policy を期待どおりに機能させるために「CiscoTAC-1」Call Home プロファイルを無効化する必要はありません。
ステップ 4	**license smart url** {*url* | **cslu** *cslu_or_on-prem_url* | **default** | **smart** *smart_url* | **utility** *smart_url*} 例： `Device(config)# license smart url cslu` `http://192.168.0.1:8182/cslu/v1/pi`	設定されたトランスポートモードに使用する URL を設定します。前のステップで選択した転送モードに応じて、対応する URL をここで設定します。 • *url*：転送モードとして **callhome** を設定している場合は、このオプションを設定します。CSSM URL を次のように正確に入力します。 `https://software.cisco.com/#module/SmartLicensing` **no license smart url** *url* コマンドは、デフォルトの URL に戻ります。

	コマンドまたはアクション	目的
		• **cslu** *cslu_or_on-prem_url*：トランスポートモードを **cslu** として設定している場合は、必要に応じてCSLUまたはSSMオンプレミスのURLを使用してこのオプションを設定します。 • CSLUを使用している場合は、次のようにURLを入力します。 `http://<cslu_ip_or_host>:8182/cslu/v1/pi` `<cslu_ip_or_host>`には、CSLUをインストールしたWindowsホストのホスト名やIPアドレスを入力します。8182はポート番号であり、CSLUが使用する唯一のポート番号です。 **no license smart url cslu** *cslu_or_on-prem_url* コマンドは`http://cslu-local:8182/cslu/v1/pi`に戻ります。 • SSMオンプレミスを使用している場合は、次のようにURLを入力します。 `http://<ip>/cslu/v1/pi/<tenant ID>` <ip>には、SSMオンプレミスをインストールしたサーバのホスト名またはIPアドレスを入力します。<tenantID>はデフォルトのローカル バーチャル アカウントIDにする必要があります。 **ヒント** SSMオンプレミスからURL全体を取得できます。「トランスポートURLの取得（SSMオンプレミスUI）（30ページ）」を参照してください

	コマンドまたはアクション	目的
		no license smart url cslu *cslu_or_on-prem_url* コマンドは http://cslu-local:8182/cslu/v1/pi に戻ります。 • **default**：設定されている転送モードによって異なります。このオプションでは、**smart** および **cslu** 転送モードのみがサポートされます。 転送モードが **cslu** に設定されている場合、**license smart url default** を設定すると、CSLU URL は自動的に設定されます（https://cslu-local:8182/cslu/v1/pi）。 転送モードが **smart** に設定されている場合、**license smart url default** を設定すると、スマート URL は自動的に設定されます（https://smartreceiver.cisco.com/licservice/license）。 • **smart** *smart_url*：転送タイプとして **smart** を設定している場合は、このオプションを設定します。URL を次のように正確に入力します。 https://smartreceiver.cisco.com/licservice/license このオプションを設定すると、システムは **license smart url** *url* で自動的に URL の複製を作成します。重複するエントリは無視できます。これ以上の操作は必要ありません。 **no license smart url smart***smart_url* コマンドは、デフォルトの URL に戻ります。 • **utility** *smart_url*：このオプションは CLI では使用できますがサポートされていません。
ステップ 5	**license smart usage interval** *interval_in_days* 例： `Device(config)# license smart usage interval 40`	（任意）レポート間隔の日数を設定します。デフォルトでは、RUM レポートは 30 日ごとに送信されます。有効な値の範囲は 1 ～ 3650 です。

	コマンドまたはアクション	目的
		ユーティリティモードを使用している場合、レポート間隔は7日以内にすることを推奨します。7日以内にすることで、ユーティリティモードの製品インスタンスに適用される 30 日間の ACK 要件がタイムリーに満たされます。 間隔を設定しない場合、レポート間隔は完全にポリシーによって決定されます。

ユーティリティモードの有効化

MSLAがある場合のみ、サポートされているすべてのトポロジの製品インスタンスでこのモードを有効にする必要があります。

始める前に

サポートされるトポロジ：

- CSSM に直接接続
- CSLU を介して CSSM に接続、CSLU は CSSM から切断（製品インスタンス開始型通信および CSLU 開始型通信）
- SSM オンプレミス展開（製品インスタンス開始型通信と SSM オンプレミス開始型通信）
- CSSM への接続なし、CSLU なし

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。プロンプトが表示されたらパスワードを入力します。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	
ステップ 3	**license smart utility** 例： `Device (config)# license smart utility`	製品インスタンスのユーティリティモードを有効にして、MSLAが使用されることを示します。有効にすると、次のことが発生します。

	コマンドまたはアクション	目的
		• トランスポートタイプと URL がチェックされます。 この設定が正しく構成されていない場合、%SMART_LIC-4-UTILITY_TRANSPORT_NOT_CONFIG システムメッセージが表示されます。 • RUM レポートには、製品インスタンスがユーティリティモードであることを示すフラグが含まれています。 ユーティリティモードを初めて有効にしたときに、RUM レポートにユーティリティフラグが設定されます。スマートアカウントとバーチャルアカウントにサブスクリプションが存在する場合、サブスクリプション ID は RUM ACK で返されます。後続の RUM レポートには、サブスクリプション ID が含まれます。サブスクリプション ID もすべての RUM ACK で返されます。 %SMART_LIC-4-UTILITY_SUBSCRIPTION_LICENSE メッセージは、ユーティリティモードが有効になっていて、サブスクリプション ID のないライセンスが製品インスタンスで使用されている場合に表示されます。 • ユーティリティモードに固有のポリシーが製品インスタンスに設定されています。ユーティリティポリシーには、RUM ACK を 30 日ごとにインストールする必要があると記載されています。 ACK が期限を過ぎている場合、%SMART_LIC-4-UTILITY_NO_ACK システムメッセージが表示されます。 • 情報メッセージ %SMART_LIC-3-UTILITY_STARTED

	コマンドまたはアクション	目的
		が表示されます。これは、ユーティリティモードが有効になっており、サブスクリプション ID が使用可能であることを示しています。
ステップ 4	**exit** 例： `Device (config)# exit`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 5	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	コンフィギュレーション ファイルに設定を保存します。

PAK ライセンスの使用を継続する

PAK ライセンスがあり、製品インスタンスで引き続き使用する場合は、次の手順を実行します。

（注） この手順は、HSECK9 を含む、PAK 履行済みのすべてのライセンスに適用されます。

始める前に

サポートされるトポロジ：すべて

手順

ステップ 1 製品インスタンスのソフトウェアバージョンを、PAK ライセンスのスナップショットが取得されるリリースにアップグレードします。

PAK ライセンスのスナップショットが取得されるには、次のいずれかのリリースにアップグレードする必要があります。

- 17.3.x トレインの Cisco IOS XE Amsterdam 17.3.5 以降のリリース。
- 17.6.x トレインの Cisco IOS XE Bengaluru 17.6.2 以降のリリース。
- 17.7.x トレインの Cisco IOS XE Cupertino 17.7.1 以降のリリース、および後続のトレインのすべてのリリース、つまり Cisco IOS XE Cupertino 17.8.x、Cisco IOS XE Cupertino 17.9.x、および Cisco IOS XE Dublin 17.10.x まで。

アップグレード情報については、次を参照してください。

製品シリーズ	PAK がサポートされているか	アップグレード情報へのリンク
Cisco 1000 シリーズ サービス統合型ルータ	はい	ソフトウェアのインストール方法とアップグレード方法
Cisco 4000 シリーズ サービス統合型ルータ	はい	ソフトウェアのインストール方法とアップグレード方法
Cisco ASR 1000 シリーズ アグリゲーション サービス ルータ	はい	Cisco ASR 1000 シリーズ ルータでサポートされているソフトウェアのアップグレードプロセス
Cisco クラウド サービス ルータ 1000v	はい	Cisco IOS XE ソフトウェアのアップグレード
Catalyst 8000V エッジ ソフトウェア	はい。ただし、CSR1000v から Catalyst 8000V エッジソフトウェアへの .bin アップグレードの場合のみ	Cisco IOS XE ソフトウェアのアップグレード

アップグレード後、特権 EXEC モードで **show platform software sl-infra pak-info** コマンドを入力して、作成されたスナップショットを表示して確認します。

ステップ 2 DLC が完了したことを確認します。

DLC がトリガーされます。DLC 後、PAK 履行済みライセンスをスマートアカウントで使用できます。製品インスタンスで **show license all** コマンドを入力して、ライセンスが引き続き PAK 履行済みライセンスとして識別されることを確認します。たとえば、スナップショットが作成された HSECK9 PAK は、引き続き `Status:PAK` で表示されます。

Smart Licensing Using Policy をサポートするリリースにアップグレードすると、製品インスタンスで DLC プロセスが自動的にトリガーされます。DLC データは製品インスタンスが Smart Licensing Using Policy をサポートするソフトウェアバージョンにアップされた 1 時間後に収集されます。

製品インスタンスに ACK がインストールされると、DLC プロセスが完了します（ACK は、使用状況の同期が完了すると利用可能になります。これが次のステップです）。

```
Device# show platform software license dlc

<output truncated>

DLC Process Status: Completed

DLC Conversion Status: SUCCESS
```

ステップ 3 ライセンスの使用状況を CSSM と同期します。

実装したトポロジに適用される方法に従い、RUM レポートが CSSM に送信されるようにします。

結果：

- PAK ライセンスのスナップショットは利用可能で、PAK 管理ライブラリが廃止された後も引き続き有効です。
- ライセンス数は、CSSM 内のスマートアカウントとバーチャルアカウントに保管されます。
- ライセンスの使用状況は CSSM に報告されます。

PAK ライセンスの削除

製品インスタンスにある PAK ライセンスを削除する場合は、次の手順を実行します。

（注） この手順は、HSECK9 を含む、PAK 履行済みのすべてのライセンスに適用されます。

このタスクを完了すると、CSSMのライセンスプールに返却されるデバイスとライセンスで実行できる内容に関して複数のオプションを選択できます。それらのオプションについては、タスクの最後にある「**結果**」セクションを参照してください。

始める前に

サポートされるトポロジ：すべて

手順

ステップ 1 DLC が完了したことを確認します。

DLC がトリガーされます。DLC 後、PAK 履行済みライセンスをスマートアカウントで使用できます。製品インスタンスで **show license all** コマンドを入力して、ライセンスが引き続き PAK 履行済みライセンスとして識別されることを確認します。たとえば、HSECK9 PAK は引き続き `Status:PAK` で表示されます。

Smart Licensing Using Policy をサポートするリリースにアップグレードすると、製品インスタンスで DLC プロセスが自動的にトリガーされます。DLC データは製品インスタンスが Smart Licensing Using Policy をサポートするソフトウェアバージョンにアップされた 1 時間後に収集されます。

製品インスタンスにACKがインストールされると、DLCプロセスが完了します（ACKは、使用状況の同期が完了すると利用可能になります。これが次のステップです）。

```
Device# show platform software license dlc

<output truncated>

DLC Process Status: Completed

DLC Conversion Status: SUCCESS
```

ステップ 2 工場出荷時の状態へのリセット

製品インスタンスに応じて、対応するリンクを参照してください。

製品シリーズ	工場出荷時の状態へのリセット情報へのリンク
Cisco 1000 シリーズ サービス統合型ルータ	factory reset コマンドの使用
Cisco 4000 シリーズ サービス統合型ルータ	工場出荷時の状態へのリセット
Cisco ASR 1000 シリーズ アグリゲーション サービス ルータ	工場出荷時の状態へのリセット
Cisco クラウド サービス ルータ 1000v	工場出荷時の状態へのリセット
Catalyst 8000V エッジソフトウェア	工場出荷時の状態へのリセット

ステップ 3 PAK ライセンスに HSECK9 ライセンスが含まれている場合は、製品インスタンスをリロードします。

PAK ライセンスに HSECK9 ライセンスが含まれていない場合、このステップは不要です。

前のステップで工場出荷時の状態へのリセットを実行すると、このリロードにより、HSECK9 ライセンスなしでデバイスを起動できるようになります。

ステップ 4 ライセンスの使用状況と CSSM の同期

実装したトポロジに適用される方法に従い、RUM レポートが CSSM に送信されるようにします。RUM レポートを送信すると、次のことが可能になります。

- 製品インスタンスでライセンスが消費されていないことを CSSM に通知します。
- PAK 履行済みライセンスが CSSM のライセンスプールに返却され、スマートライセンスとして使用可能になります。たとえば、「PAK 履行済み securityk9」ライセンスを所有している場合、「securityk9」ライセンスとして使用可能になります。

結果：

以下の選択肢があります。

- 通常のスマートライセンスと同じ製品インスタンスで、PAK 履行済みライセンスを使用する。

製品インスタンスでライセンスを使用するには、該当するコマンドを使用してライセンスを設定します。ライセンスのレポート要件は、他のライセンスと同じです。ポリシーに従って、またはシステムメッセージにそのように示されている場合。

- 別の製品インスタンスで、通常のスマートライセンスとして PAK 履行済みライセンスを使用する。

  別の製品インスタンスでライセンスを使用するには、その製品インスタンスに該当するコマンドを使用してライセンスを設定します。ライセンスのレポート要件は、他のライセンスと同じです。ポリシーに従って、またはシステムメッセージにそのように示されている場合。

- 製品インスタンスの使用を継続する。
- 製品インスタンスをデコミッションするか、返品許可（RMA）を実行する場合は、CSSM から製品インスタンスを削除します。

障害が発生した製品インスタンスの PAK ライセンスの削除

このタスクでは、まったく機能していない（コンソールにアクセスして Cisco IOS コマンドを設定できない）製品インスタンスで PAK ライセンスを返却する方法を示します。

障害が発生した製品インスタンスの PAK ライセンスを返却するには、ケースを開く必要があります。Support Case Manager に移動します。[OPEN NEW CASE] をクリックして、[Software Licensing] を選択します。

ケースを開き、サポートチームから連絡があったら、返却プロセスを開始し、CSSMから製品インスタンスを削除します。

PLR のアクティブ化

サポートする製品インスタンスで PLR をアクティブ化するには、次の手順を実行します。

この手順の一部のステップは製品インスタンスで実行する必要があり、一部のステップはCSSM Web UI で実行する必要があります。CSSM Web UI で実行する必要があるステップには、混乱を避けるために「（CSSM）」というプレフィックスが付いています。他のステップはすべて、製品インスタンスで実行する必要があります。

始める前に

- サポートされるトポロジ：該当なし
- CSSM内のスマートアカウントと必要なバーチャルアカウントへの適切なアクセス権を持つユーザーロールがあることを確認します。

- スマートアカウントが PLR に対して有効になっていることを確認します。

  有効になっているか確認するには、CSSM https://software.cisco.com にログインし、[Manage licenses] をクリックします。[Inventory] タブをクリックします。自分のバーチャルアカウントを選択します。[ライセンス（Licenses）] タブをクリックします。[License Reservation] ボタンが有効になっている場合、スマートアカウントが PLR に対して有効になっています。ボタンがグレー表示になっていか、表示されていない場合は、Support Case Manager（SCM）でケースを開きます。

- 製品インスタンスで実行されているソフトウェアバージョンが Cisco IOS XE Dublin 17.10.1a 以降であることを確認します。確認するには、特権 EXEC モードで **show version** コマンドを入力します。

手順

ステップ 1 **configure terminal**

例：

```
Device#configure terminal
```

グローバル コンフィギュレーション モードを開始します。

ステップ 2 **license smart reservation**

例：

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

予約モードを有効にします。

ステップ 3 **exit**

例：

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

グローバル コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

ステップ 4 **license smart reservation request local**

例：

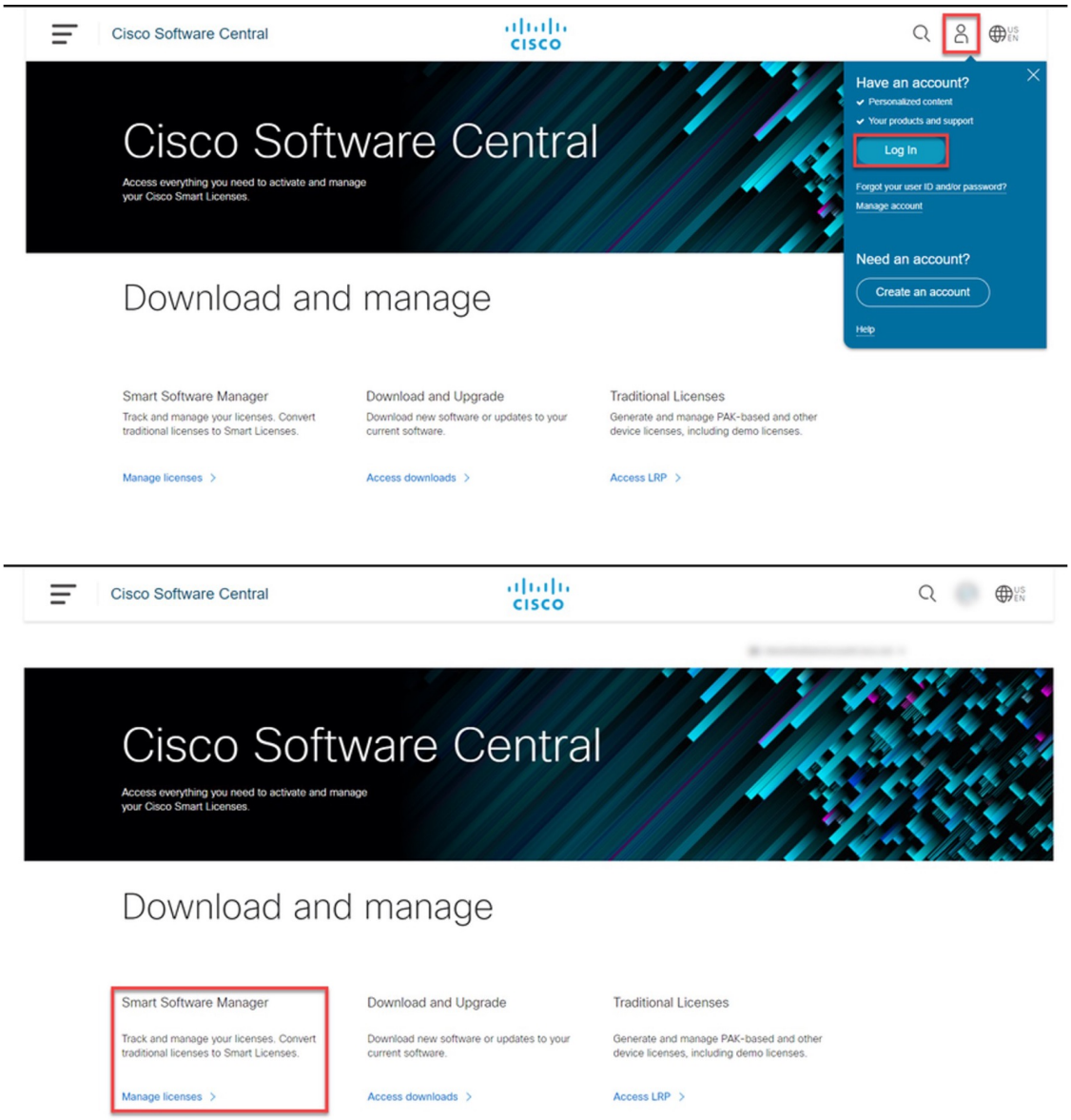
```
Device# license smart reservation request local
Enter this request code in the Cisco Smart Software Manager portal:
UDI: PID:C8000V,SN:96QKIABBZ1H
Request code: DB-ZC8000V:96QKIABBZ1H-AYk3ndtp6-F1
```

製品インスタンスで予約要求コードを生成します。

生成したコードは、後のステップで CSSM Web UI に貼り付ける必要があります。コードは .txt またはその他のアクセス可能なファイルに保存できます。

ステップ 5 （CSSM）https://software.cisco.com にアクセスし、[Manage licenses] をクリックします。シスコから提供されたユーザ名とパスワードを使用してログインします。

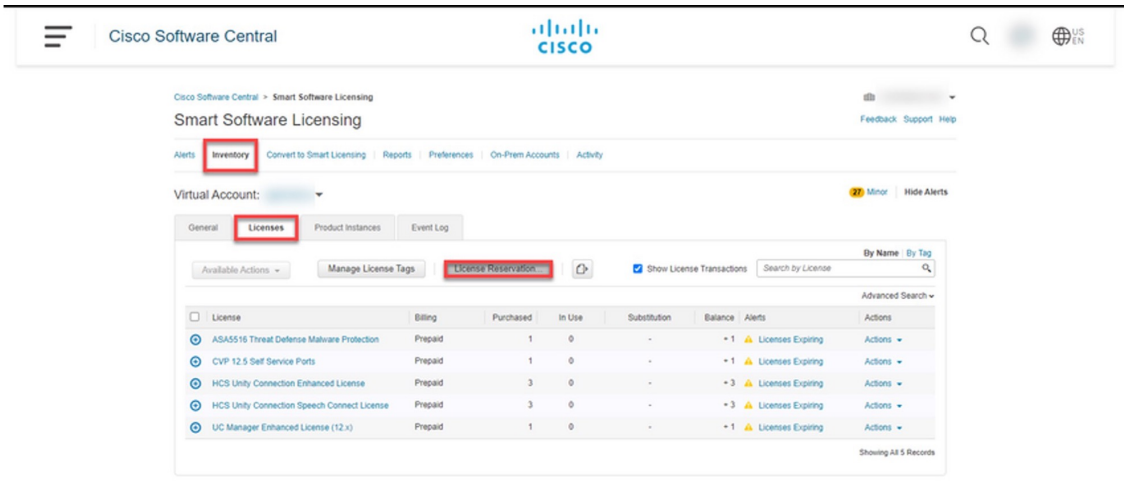
例：



[Smart Software Licensing] ページが表示されます。

ステップ 6 （CSSM）[Inventory] タブをクリックします。自分のバーチャルアカウントを選択します。[Licenses] タブをクリックし、[License Reservation] ボタンをクリックします。

例：

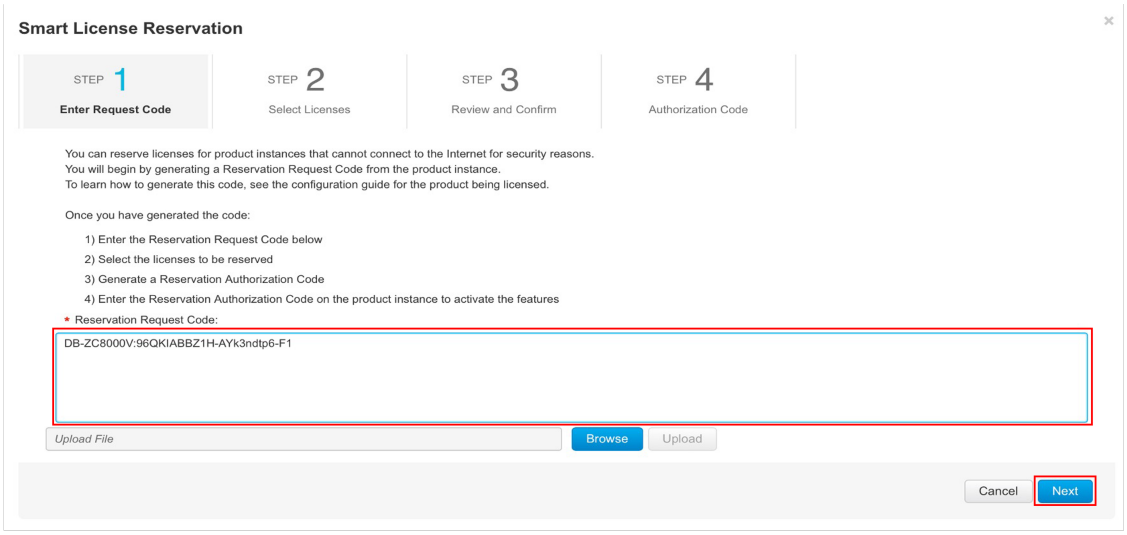


[Smart License Reservation] ダイアログボックスが表示されます。

ヒント スマートアカウントとバーチャルアカウントが PLR に対して有効になっていない場合、[License Reservation] ボタンは有効になりません。この場合、Support Case Manager（SCM）でサポートケースを開いてボタンを有効にする必要があります。

ステップ 7 （CSSM）[Step 1: Enter Request Code] で、[Reservation Request Code] テキストボックスに要求コードを入力します。[Next] をクリックします。

例：

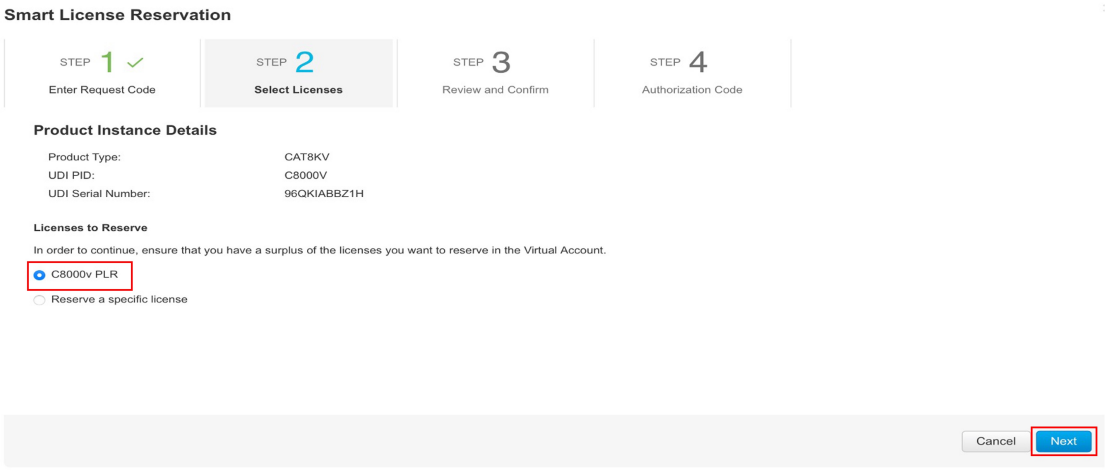


ステップ 3 で製品インスタンスで生成した予約要求コードを入力します。

[Next] をクリックすると、[Step 2: Select Licenses] ダイアログボックスが表示されます。

ステップ 8 （CSSM）[Step 2: Select Licenses] で、[C8000v PLR] を選択します。[Next] をクリックします。

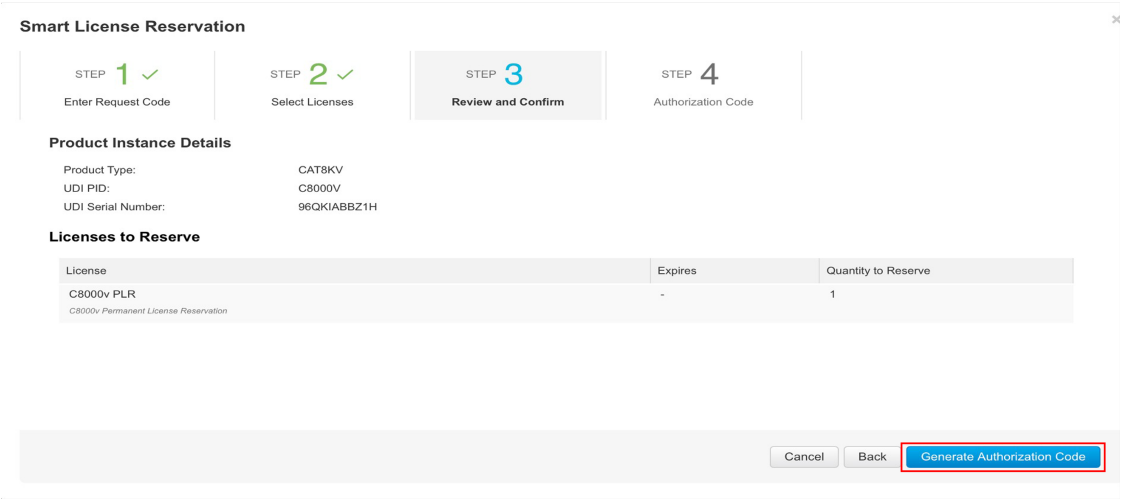
例：



[Next] をクリックすると、選択できるライセンスのリストが表示されます。

ステップ 9 （CSSM）[Quantity to Reserve] に 1 を入力し、[Expires] 列を空白のままにします。[Next] をクリックします。

例：



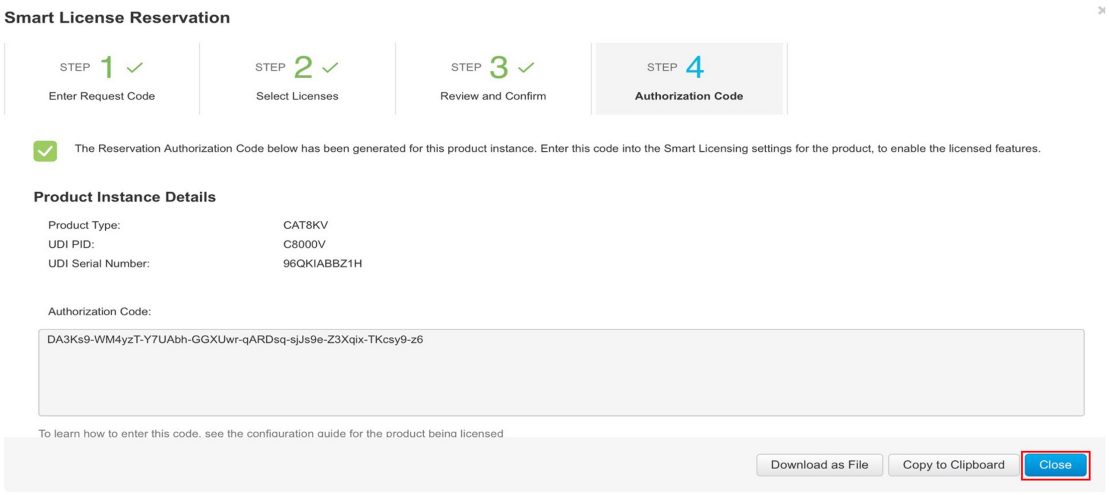
[Next] をクリックすると、[Step 3: Review and Confirm] ダイアログボックスが表示されます。

ステップ 10 （CSSM）[Step 3: Review and Confirm] ダイアログボックスで [Generate Authorization Code] ボタンをクリックします。

[Generate Authorization Code] ボタンをクリックすると、[Step 4: Authorization Code] ダイアログボックスが表示されます。

ステップ 11 （CSSM）[Step 4: Authorization Code] ダイアログボックスで、[Copy to Clipboard] または [Download as File] をクリックします。[Close] をクリックします。

例：



PLR 承認コードをクリップボードにコピーするか、ファイルとしてダウンロードします。

ファイルにダウンロードする場合、次のステップで製品インスタンスにそのファイルをインストールする必要があるため、保存したファイルをフラッシュドライブやネットワークリソース（TFTP サーバーなど）に転送する必要があります。

ステップ 12 **license smart reservation install** *PLR-Code*

例：

```
Device# license smart reservation install
DA3Ks9-WM4yzT-Y7UAbh-GGXUwr-qARDsq-sjJs9e-Z3Xqix-TKcsy9-z6
Reservation install successful
```

PLR コードのバージョン 3 をインストールし、成功メッセージを表示します。

ヒント PLR コードのバージョン 3 は、常に文字「D」で始まり、長さは 58 文字です。

ステップ 13 **show license reservation**

例：

```
Device# show license reservation
License reservation: ENABLED
Overall status:
   Active: PID:C8000V,SN:96QKIABBZ1H
   Reservation status: UNIVERSAL INSTALLED on Oct 25 17:50:48 2022 UTC
```

ライセンス予約情報を表示します。

PLR コードが製品インスタンスにインストールされている場合、このコマンドの出力の予約ステータスには `UNIVERSAL INSTALLED` と表示されます。

ステップ 14 **configure terminal**

例：

```
Device# configure terminal
```

グローバル コンフィギュレーション モードを開始します。

ステップ 15 **platform hardware throughput level MB** {**100** | **1000** | **10000** | **15** | **25** | **50** | **250** | **2500** | **50** | **500** | **5000**}

例：

```
Device(config)# platform hardware throughput level MB 1000
```

スループットレベルを設定します。

少なくとも、ネットワークスタック ライセンスを設定しておく必要があります。そうしないと、コマンドがコマンド ライン インターフェイスで有効なものとして認識されません。

（注） 250 Mbps を超えるスループットを設定する場合は、SLAC をインストールする必要はありません。PLR コードでは、250 Mbps を超えるスループットが許可されます。

ステップ 16 **exit**

例：

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

グローバル コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

ステップ 17 **show platform hardware throughput level MB**

例：

```
Device# show platform hardware throughput level MB
The current throughput level is 2000000 kb/s
```

デバイスで現在実行されているスループットを表示します。

PLR のアップグレード

PLR バージョンコードをアップグレードして、Smart Licensing Using Policy 環境で引き続き PLR を使用するには、次の手順を実行します。

この手順の一部のステップは製品インスタンスで実行する必要があり、一部のステップはCSSM Web UI で実行する必要があります。CSSM Web UI で実行する必要があるステップには、混乱を避けるために「（CSSM）」というプレフィックスが付いています。他のステップはすべて、製品インスタンスで実行する必要があります。

始める前に

- サポートされるトポロジ：該当なし
- 既存の古いバージョンの PLR コードがあるため、次の設定が想定されます。
  - CSSM 内のスマートアカウントと必要なバーチャルアカウントへの適切なアクセス権を持つユーザーロールを保有している。
  - スマートアカウントが PLR に対して有効になっている。

- 製品インスタンスのソフトウェアバージョンを Cisco IOS XE Dublin 17.10.1a 以降に .bin アップグレードしたことを確認します。確認するには、特権 EXEC モードで **show version** コマンドを入力します。

（注） 製品インスタンスのスループットレベルがアップグレード前に 250 Mbps を超えていた場合、アップグレード時に 250 Mbps に設定されます。以下のようなシステムメッセージも表示されますが、無視してかまいません。以下の手順は、PLR コードをバージョン 3 にアップグレードして、スループットを自動的に回復する方法を示しています。

```
%SMART_LIC-6-RESERVE_AUTH_FAILED: Failed to validate the
Universal Reservation
Authorization Code for udi PID:CSR1000V,SN:9QLBLATKXM4.
Changing to the unregistered state.
```

手順

ステップ 1 （CSSM）https://software.cisco.com にアクセスし、[Manage licenses] をクリックします。シスコから提供されたユーザ名とパスワードを使用してログインします。

CSSM Web UI にログインします。

ステップ 2 （CSSM）[Inventory] タブをクリックします。自分のバーチャルアカウントを選択します。[Product Instances] タブをクリックします。

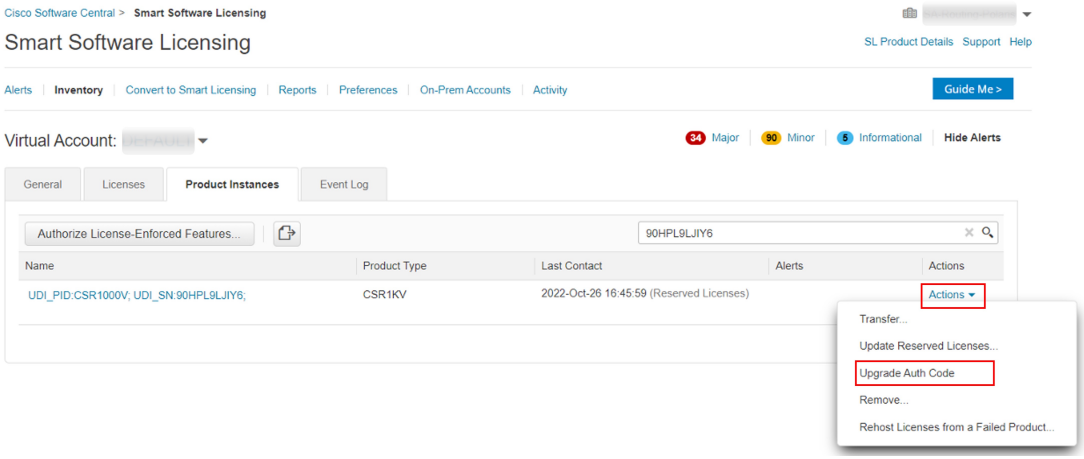
製品インスタンスのリストが表示されます。

ステップ 3 （CSSM）PLR コードをアップグレードする製品インスタンスを見つけて、対応する [Actions] ドロップダウンをクリックします。

使用可能なアクションのリストが表示されます。

ステップ 4 （CSSM）[Upgrade Auth Code] を選択します。

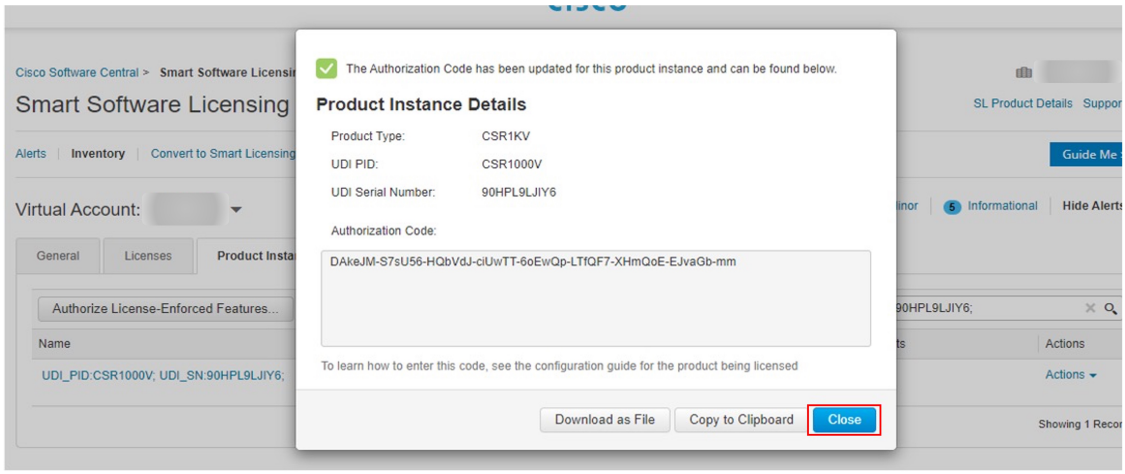
例：



[Product Instance Details] ポップアップウィンドウが表示されます。

ステップ 5 （CSSM）[Copy to Clipboard] または [Download as File] をクリックします。[Close] をクリックします。

例：



PLR 承認コードをクリップボードにコピーするか、ファイルとしてダウンロードします。

ファイルにダウンロードする場合、次のステップで製品インスタンスにそのファイルをインストールする必要があるため、保存したファイルをフラッシュドライブやネットワークリソース（TFTP サーバーなど）に転送する必要があります。

ステップ 6 **license smart reservation install** *PLR-Code*

例：

```
Device# license smart reservation
DA3Ks9-WM4yzT-Y7UAbh-GGXUwr-qARDsq-sjJs9e-Z3Xqix-TKcsy9-z6

Reservation install successful
```

PLR コードのバージョン 3 をインストールし、成功メッセージを表示します。既存の古い PLR コードバージョンは、プロセス中に削除されます。

ソフトウェアバージョンのアップグレード前に製品インスタンスのスループットレベルが 250 Mbps を超えていた場合、スループットレベルが復元されるようになりました。

ヒント　　PLR コードのバージョン 3 は、常に文字「D」で始まり、長さは 58 文字です。

ステップ 7　show platform hardware throughput level MB

例：

```
Device# show platform hardware throughput level MB
The current throughput level is 2000000 kb/s
```

デバイスで現在実行されているスループットを表示します。

ステップ 8　show license reservation

例：

```
Device# show license reservation
License reservation: ENABLED
Overall status:
      Active: PID:CSR1000V,SN:9QLBLATKXM4
      Status: UNIVERSAL INSTALLED on Oct 25 20:54:08 2022 UTC
```

ライセンス予約情報を表示します。

PLR コードが製品インスタンスにインストールされている場合、このコマンドの出力の予約ステータスには `UNIVERSAL INSTALLED` と表示されます。

PLR の非アクティブ化

サポートする製品インスタンスで PLR を非アクティブ化するには、次の手順を実行します。

この手順の一部のステップは製品インスタンスで実行する必要があり、一部のステップはCSSM Web UI で実行する必要があります。CSSM Web UI で実行する必要があるステップには、混乱を避けるために「（CSSM）」というプレフィックスが付いています。他のステップはすべて、製品インスタンスで実行する必要があります。

始める前に

サポートされるトポロジ：該当なし

手順

ステップ 1　license smart reservation return local

例：

```
Device# license smart reservation return local
This command will remove the license authorization code.
Some features may not function properly.
```

```
Do you want to continue? [yes/no]:
Enter this return code in Cisco Smart Software Manager portal:
UDI: PID:CSR1000V,SN:9QLBLATKXM4
    Return code: CNcjZD-aGrAPP-SpCkkD-nZtES8-46zCDq-jZP
```

製品インスタンスに予約返却要求コードを生成します。

生成したコードは、後のステップで CSSM Web UI に貼り付ける必要があります。コードは .txt またはその他のアクセス可能なファイルに保存できます。

ステップ 2 （CSSM）https://software.cisco.com にアクセスし、[Manage licenses] をクリックします。シスコから提供されたユーザ名とパスワードを使用してログインします。

CSSM Web UI にログインします。

ステップ 3 （CSSM）[Inventory] タブをクリックします。自分のバーチャルアカウントを選択します。[Product Instances] タブをクリックします。

製品インスタンスのリストが表示されます。

ステップ 4 （CSSM）PLR コードをアップグレードする製品インスタンスを見つけて、対応する [Actions] ドロップダウンをクリックします。

ステップ 5 （CSSM）[Remove Product Instance] を選択します。ステップ 1 で生成したリターンコードをテキストボックスに貼り付けます。[Remove] をクリックします。

250 Mbps を超えるスループットが PLR で実行されていた場合、スループットは 250 Mbps に設定されます。スループットが 250 Mbps 以下だった場合、変化はありません。

ステップ 6 **configure terminal**

例：

```
Device# configure terminal
```

グローバル コンフィギュレーション モードを開始します。

ステップ 7 **no license smart reservation**

例：

```
Device (config)# no license smart reservation
```

予約モードを無効にします。

ステップ 8 **exit**

例：

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

グローバル コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

ルーティング製品インスタンスのHSECK9ライセンス マッピング テーブル

CSSM で SLAC を生成する場合（CSSM からの SLAC の生成とファイルへのダウンロード（42 ページ））、PID の正しいライセンス名を選択する必要があります。この表は、Cisco アグリゲーション、統合、およびクラウドサービスルータの PID とライセンス名のマッピングの簡単なリファレンスです。

製品ファミリ	PID	Cisco IOS XE Bengaluru 17.5.x 以前のリリースで使用するライセンス名	Cisco IOS XE Bengaluru 17.6.1 以降のリリースで使用するライセンス名
ISR1K -8P	C1111-8P	ISR_1100_8P_Hsec	オフラインモードを使用する場合、またはインストールのために以前のソフトウェアリリースにダウングレードしてから 17.6.1 以降に戻す場合は、**ISR_1100_8P_Hsec** を使用します。 デバイスに固有の HSECK9 ライセンスが変換される場合は、**Router US Export Lic for DNA** を使用します。 詳細については、デバイスに固有の HSECK9 ライセンスの段階的廃止を参照してください。
	C1111-8PLTEEA		
	C1111-8PLTELA		
	C1111-8PWE		
	C1111-8PWB		
	C1111-8PWA		
	C1111-8PWZ		
	C1111-8PWN		
	C1111-8PWQ		
	C1111-8PWC		
	C1111-8PWR		
	C1111-8PWK		
	C1111-8PWS		
	C1111-8PLTEEAWE		
	C1111-8PLTEEAWB		
	C1111-8PLTEEAWA		
	C1111-8PLTEEAWR		
	C1111-8PLTELAWZ		
	C1111-8PLTELAWN		
	C1111-8PLTELAWQ		
	C1111-8PLTELAWC		
	C1111-8PLTELAWK		
	C1111-8PLTELAWD		
	C1111-8PLTELAWA		
	C1111-8PLTELAWE		
	C1111-8PLTELAWS		
	C1116-8P		
	C1116-8PLTEEA		
	C1117-8P		
	C1117-8PM		

製品ファミリ	**PID**	**Cisco IOS XE Bengaluru 17.5.x** 以前のリリースで使用するライセンス名	**Cisco IOS XE Bengaluru 17.6.1** 以降のリリースで使用するライセンス名
	C1117-8PLTEEA		
	C1117-8PLTELA		
	C1117-8PMLTEEA		
	C1117-8PWE		
	C1117-8PWA		
	C1117-8PWZ		
	C1117-8PMWE		
	C1117-8PLTEEAWE		
	C1117-8PLTELAWE		
	C1117-8PLTELAWZ		
	C1111X-8P		
	C1112-8P		
	C1112-8PLTEEA		
	C1113-8P		
	C1113-8PM		
	C1113-8PLTEEA		
	C1113-8PLTELA		
	C1113-8PMLTEEA		
	C1113-8PWE		
	C1113-8PWA		
	C1113-8PWZ		
	C1113-8PMWE		
	C1113-8PLTEEAWE		
	C1113-8PLTELAWE		
	C1113-8PLTELAWZ		
	C1114-8P		
	C1114-8PLTEEA		
	C1115-8P		
	C1115-8PLTEEA		
	C1115-8PM		

製品ファミリ	**PID**	**Cisco IOS XE Bengaluru 17.5.x** 以前のリリースで使用するライセンス名	**Cisco IOS XE Bengaluru 17.6.1** 以降のリリースで使用するライセンス名
	C1115-8PMLTEEA		
	C1118-8P		
	C1121-8PLTEPWE		
	C1121-8PLTEPWB		
	C1121-8PLTEPWZ		
	C1121-8PLTEPWQ		
	C1121-8PLTEP		
	C1121X-8PLTEP		
	C1121-8P		
	C1121X-8P		
	C1161-8P		
	C1161X-8P		
	C1161-8PLTEP		
	C1161X-8PLTEP		
	C1126-8PLTEP		
	C1127-8PLTEP		
	C1127-8PMLTEP		
	C1126X-8PLTEP		
	C1127X-8PLTEP		
	C1127X-8PMLTEP		
	C1128-8PLTEP		
	C1121X-8PLTEPWE		
	C1121X-8PLTEPWB		
	C1121X-8PLTEPWZ		
	C1121X-8PLTEPWA		

製品ファミリ	PID	Cisco IOS XE Bengaluru 17.5.x 以前のリリースで使用するライセンス名	Cisco IOS XE Bengaluru 17.6.1 以降のリリースで使用するライセンス名
ISR1K - 4P	C1111-4P	ISR_1100_4P_Hsec	オフラインモードを使用する場合、またはインストールのために以前のソフトウェアリリースにダウングレードしてから 17.6.1 以降に戻す場合は、**ISR_1100_4P_Hsec** を使用します。 デバイスに固有の HSECK9 ライセンスが変換される場合は、**Router US Export Lic for DNA** を使用します。 詳細については、デバイスに固有の HSECK9 ライセンスの段階的廃止を参照してください。
	C1111-4PLTEEA		
	C1111-4PLTELA		
	C1111-4PWE		
	C1111-4PWB		
	C1111-4PWA		
	C1111-4PWZ		
	C1111-4PWN		
	C1111-4PWQ		
	C1111-4PWC		
	C1111-4PWR		
	C1111-4PWK		
	C1111-4PWD		
	C1111X-4P		
	C1116-4P		
	C1116-4PLTEEA		
	C1116-4PLTEEAWE		
	C1116-4PWE		
	C1117-4P		
	C1117-4PLTEEA		
	C1117-4PLTELA		
	C1117-4PLTEEAWE		
	C1117-4PLTEEAWA		
	C1117-4PLTELAWZ		
	C1117-4PWE		
	C1117-4PWA		
	C1117-4PWZ		
	C1117-4PM		
	C1117-4PMLTEEA		
	C1117-4PMLTEEAWE		

製品ファミリ	**PID**	**Cisco IOS XE Bengaluru 17.5.x** 以前のリリースで使用するライセンス名	**Cisco IOS XE Bengaluru 17.6.1** 以降のリリースで使用するライセンス名
	C1117-4PMWE		
	C1101-4P		
	C1101-4PLTEP C1101-4PLTEPWE		
	C1101-4PLTEPWB		
	C1101-4PLTEPWD		
	C1101-4PLTEPWZ		
	C1101-4PLTEPWA		
	C1101-4PLTEPWH		
	C1101-4PLTEPWQ		
	C1101-4PLTEPWR		
	C1101-4PLTEPWN		
	C1101-4PLTEPWF		
	C1109-4PLTE2P		
	C1109-4PLTE2PWB		
	C1109-4PLTE2PWD		
	C1109-4PLTE2PWE		
	C1109-4PLTE2PWZ		
	C1109-4PLTE2PWA		
	C1109-4PLTE2PWH		
	C1109-4PLTE2PWQ		
	C1109-4PLTE2PWR		
	C1109-4PLTE2PWN		
	C1109-4PLTE2PWF		
	C1118-4P		
	C1121-4P		
	C1121-4PLTEP		

製品ファミリ	PID	Cisco IOS XE Bengaluru 17.5.x 以前のリリースで使用するライセンス名	Cisco IOS XE Bengaluru 17.6.1 以降のリリースで使用するライセンス名
ISR1K-2P	C1109-2PLTEGB	ISR_1100_2P_Hsec	オフラインモードを使用する場合、またはインストールのために以前のソフトウェアリリースにダウングレードしてから 17.6.1 以降に戻す場合は、**ISR_1100_2P_Hsec** を使用します。 デバイスに固有の HSECK9 ライセンスが変換される場合は、**Router US Export Lic for DNA** を使用します。 詳細については、デバイスに固有の HSECK9 ライセンスの段階的廃止を参照してください。
	C1109-2PLTEUS		
	C1109-2PLTEVZ		
	C1109-2PLTEJN		
	C1109-2PLTEAU		
	C1109-2PLTEIN		
ISR4200	ISR4221/K9	ISR4220_HSEC	オフラインモードを使用する場合、またはインストールのために以前のソフトウェアリリースにダウングレードしてから 17.6.1 以降に戻す場合は、**ISR4220_HSEC** を使用します。 デバイスに固有の HSECK9 ライセンスが変換される場合は、**Router US Export Lic for DNA** を使用します。 詳細については、デバイスに固有の HSECK9 ライセンスの段階的廃止を参照してください。
	ISR4221X/K9		

製品ファミリ	PID	Cisco IOS XE Bengaluru 17.5.x 以前のリリースで使用するライセンス名	Cisco IOS XE Bengaluru 17.6.1 以降のリリースで使用するライセンス名
ISR4300	ISR4321/K9	ISR_4321_Hsec	オフラインモードを使用する場合、またはインストールのために以前のソフトウェアリリースにダウングレードしてから 17.6.1 以降に戻す場合は、**ISR_4321_Hsec** を使用します。 デバイスに固有の HSECK9 ライセンスが変換される場合は、**Router US Export Lic for DNA** を使用します。 詳細については、デバイスに固有の HSECK9 ライセンスの段階的廃止を参照してください。
	ISR4331/K9	ISR_4331_Hsec	オフラインモードを使用する場合、またはインストールのために以前のソフトウェアリリースにダウングレードしてから 17.6.1 以降に戻す場合は、**ISR_4331_Hsec** を使用します。 デバイスに固有の HSECK9 ライセンスが変換される場合は、**Router US Export Lic for DNA** を使用します。 詳細については、デバイスに固有の HSECK9 ライセンスの段階的廃止を参照してください。
	ISR4351/K9	ISR_4531_Hsec	

製品ファミリ	PID	Cisco IOS XE Bengaluru 17.5.x 以前のリリースで使用するライセンス名	Cisco IOS XE Bengaluru 17.6.1 以降のリリースで使用するライセンス名
			オフラインモードを使用する場合、またはインストールのために以前のソフトウェアリリースにダウングレードしてから 17.6.1 以降に戻す場合は、**ISR_4531_Hsec** を使用します。 デバイスに固有の HSECK9 ライセンスが変換される場合は、**Router US Export Lic for DNA** を使用します。 詳細については、デバイスに固有の HSECK9 ライセンスの段階的廃止を参照してください。
ISR4400	ISR4431/K9 ISR4451/K9 ISR4451-X/K9 ISR4461/K9	ISR_4400_Hsec	オフラインモードを使用する場合、またはインストールのために以前のソフトウェアリリースにダウングレードしてから 17.6.1 以降に戻す場合は、**ISR_4400_Hsec** を使用します。 デバイスに固有の HSECK9 ライセンスが変換される場合は、**Router US Export Lic for DNA** を使用します。 詳細については、デバイスに固有の HSECK9 ライセンスの段階的廃止を参照してください。

製品ファミリ	PID	Cisco IOS XE Bengaluru 17.5.x 以前のリリースで使用するライセンス名	Cisco IOS XE Bengaluru 17.6.1 以降のリリースで使用するライセンス名
C8300	C8300-1N1S-4T2X	Router US Export Lic for DNA	Router US Export Lic for DNA（変更なし）
	C8300-1N1S-6T		
	C8300-2N2S-4T2X		
	C8300-2N2S-6T		
	C8300-1N1S-4G2X		
	C8300-1N1S-6G		
	C8300-2N2S-4G2X		
	C8300-2N2S-6G		
C8200	C8200-1N-4T		
	C8200-1N-1G		
ISR1100	ISR1100-6G		
	ISR1100X-6G		
C8500	C8500-12X4QC		
	C8500-12X		
	C8500L-8S4X		
C8000V	C8000V		
CSR1000V	CSR1000V		
ISRV	ISRV		

デバイスに固有の HSECK9 ライセンスの変換

このタスクでは、ISR_1100_8P_Hsec や ISR_4321_Hsec といった、未使用のデバイスに固有の HSECK9 ライセンスを Router US Export Lic for DNA（DNA_HSEC）ライセンスに変換する方法について説明します。変換できるデバイスに固有の HSECK9 ライセンスの完全なリストについては、「ルーティング製品インスタンスの HSECK9 ライセンス マッピング テーブル （81 ページ）」を参照してください。

このタスクを実行するには、インターネットにアクセスできるデバイスが必要です。

始める前に

変換するデバイスに固有の HSECK9 ライセンスの数に応じて、Cisco Commerce Workspace（CCW）で対応する数のスペアのアップグレードライセンス PID を注文します。製品番号 DNA-HSEC-UPGD= を使用します。この PID の表示単価は 0.00 米ドルです。

（注） 正しいスマートアカウントとバーチャルアカウントが注文に記載されていることを確認してください。アカウントは、（変換する）デバイスに固有の HSECK9 ライセンスが保管されているバーチャルアカウントと同じである必要があります。

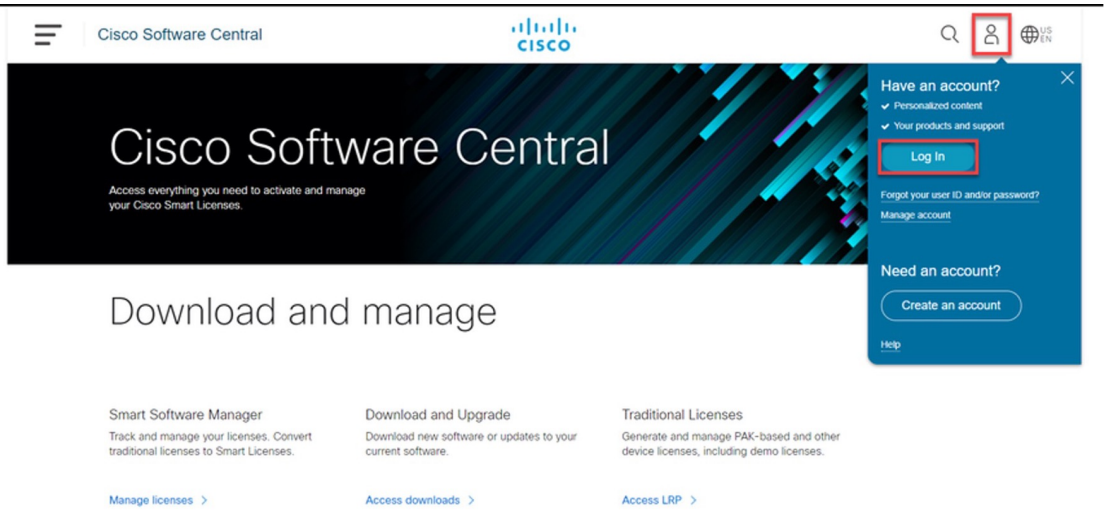
手順

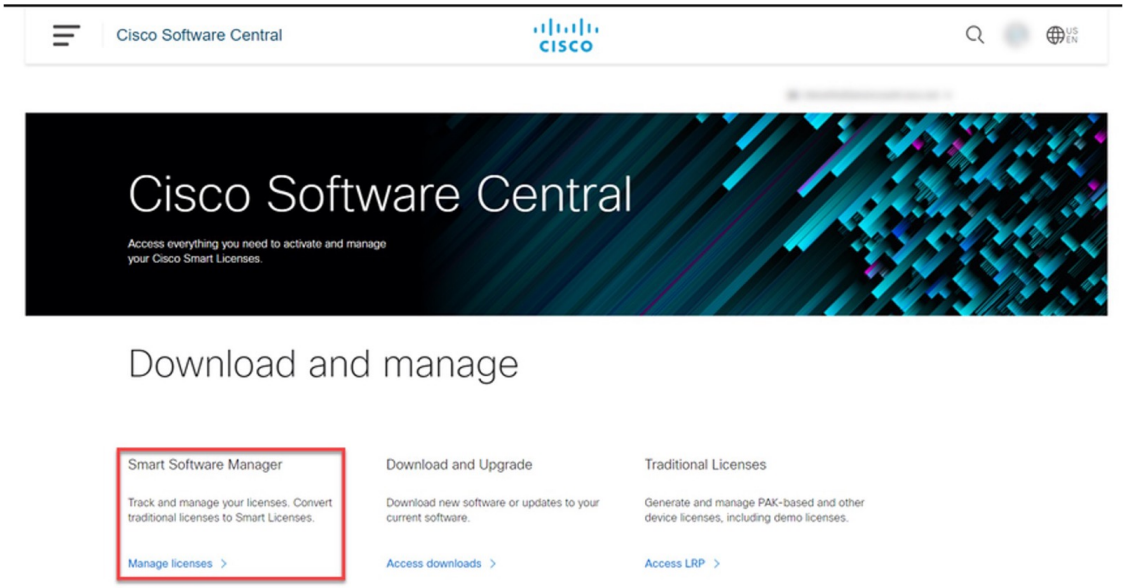
ステップ 1 https://software.cisco.com [英語] に移動し、[Manage licenses] をクリックします。

シスコから提供されたユーザー名とパスワードを使用してログインします。

[Smart Software Licensing] ページが表示されます。

例：



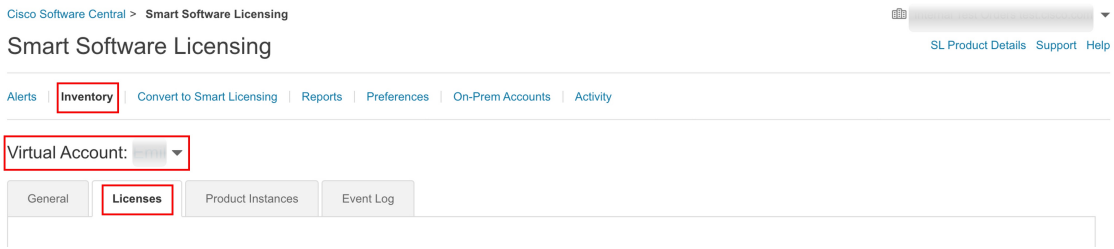


ステップ 2 [Inventory] タブをクリックします。

ステップ 3 [Virtual Account] ドロップダウンリストから、該当するバーチャルアカウントを選択します。

ステップ 4 [ライセンス（Licenses）] タブをクリックします。

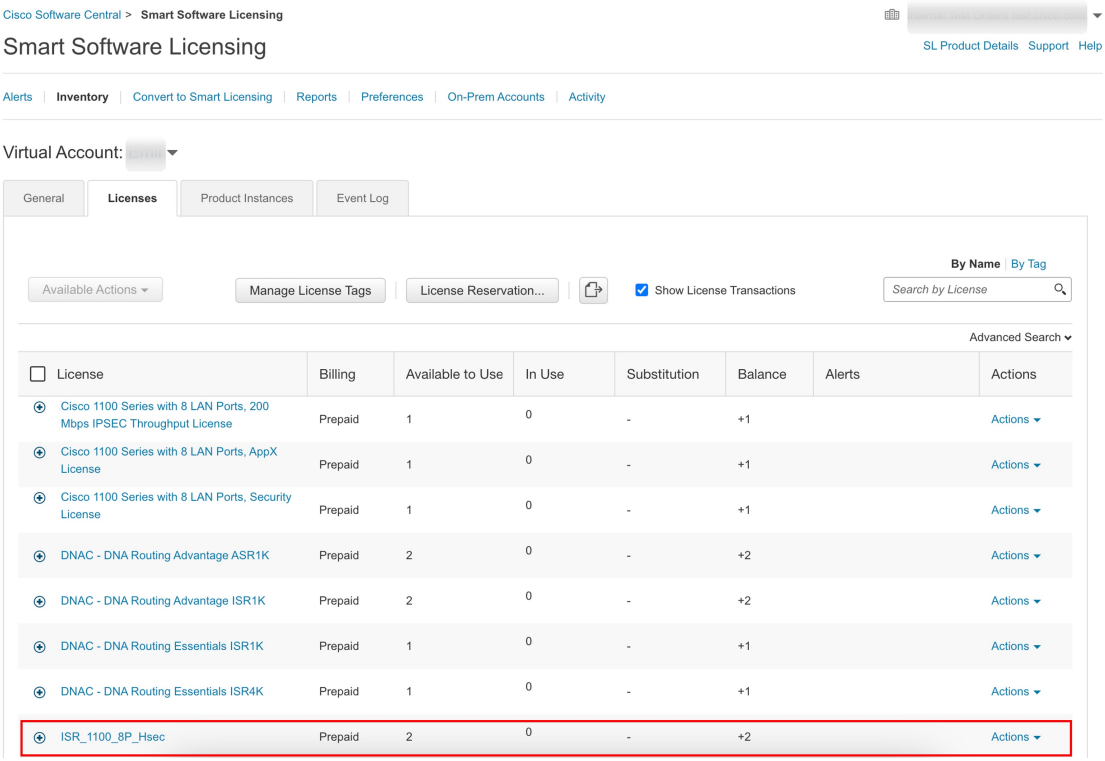
例：



ステップ 5 デバイスに固有の HSECK9 ライセンスと Router US Export Lic for DNA ライセンスがこの同じバーチャルアカウントにあることを確認します。

検索バーを使用して、デバイスに固有の HSECK9 ライセンスを見つけます。以下のサンプルのスクリーンショットでは、これは「ISR_1100_8P_Hsec」HSECK9 ライセンスであり、そのうちの 2 つがあります。

例：

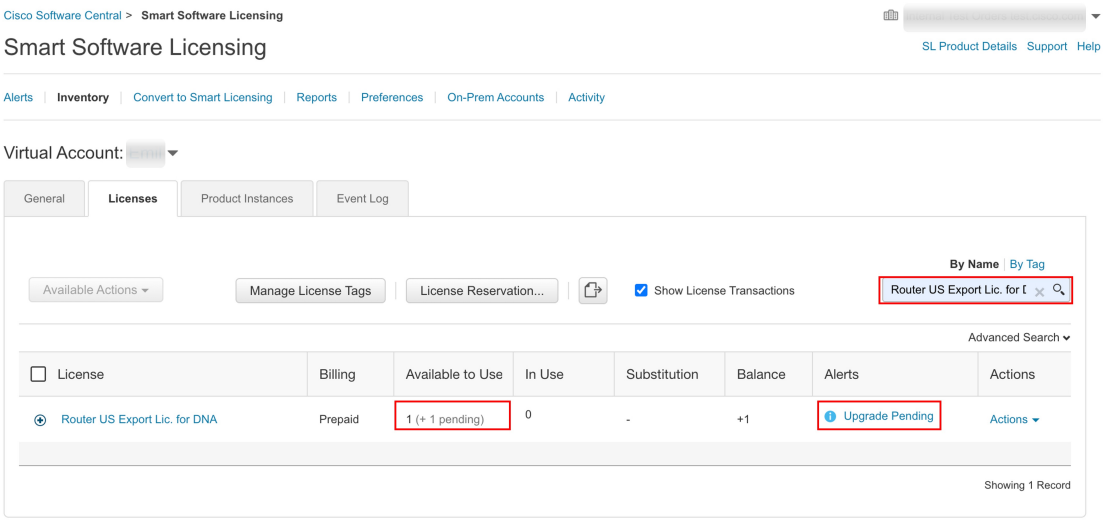


再度検索バーを使用して、Router US Export Lic for DNA を見つけます。このライセンスの [Alerts] 列で、[Upgrade Pending] と表示されていることを確認します。これにより、正しいスペアのアップグレードライセンス PID があることがわかります。さらに、[Available to Use] 列には、アップグレードが保留中の PID の数が括弧内に表示されます。以下のサンプルのスクリーンショットでは、保留中のライセンスが 1 つあります。

手順

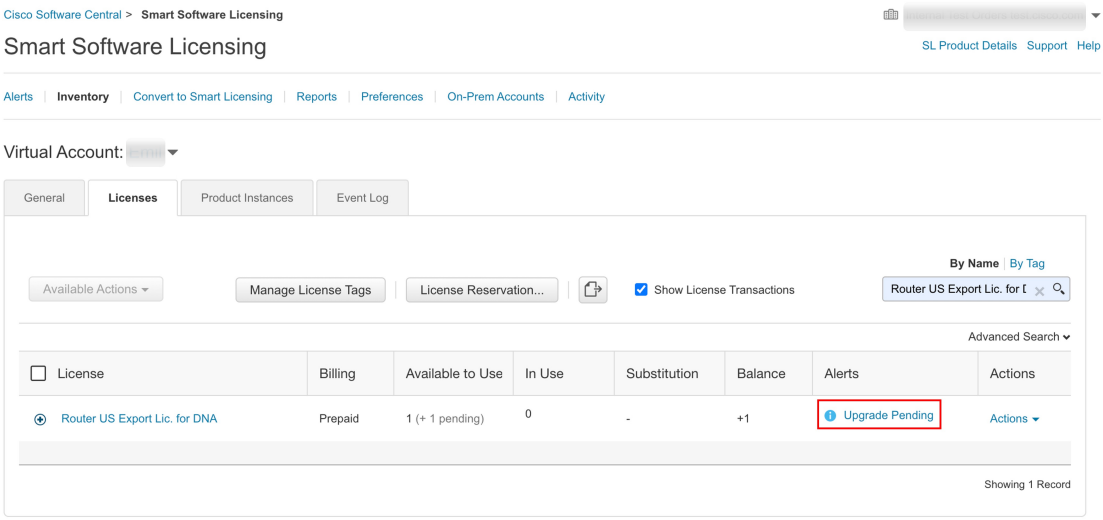
（注） サンプルのスクリーンショットには 2 つのデバイスに固有の HSECK9 ライセンスがありますが、使用可能なアップグレードライセンス PID は 1 つだけのため、この例ではそのうちの 1 つだけが変換されます。また、バーチャルアカウントに（ISR_1100_8P_Hsec と ISR4220_HSEC などの）デバイスに固有の HSECK9 ライセンスが複数ある場合は、DNA_HSEC に変換するライセンスを選択できます。

例：



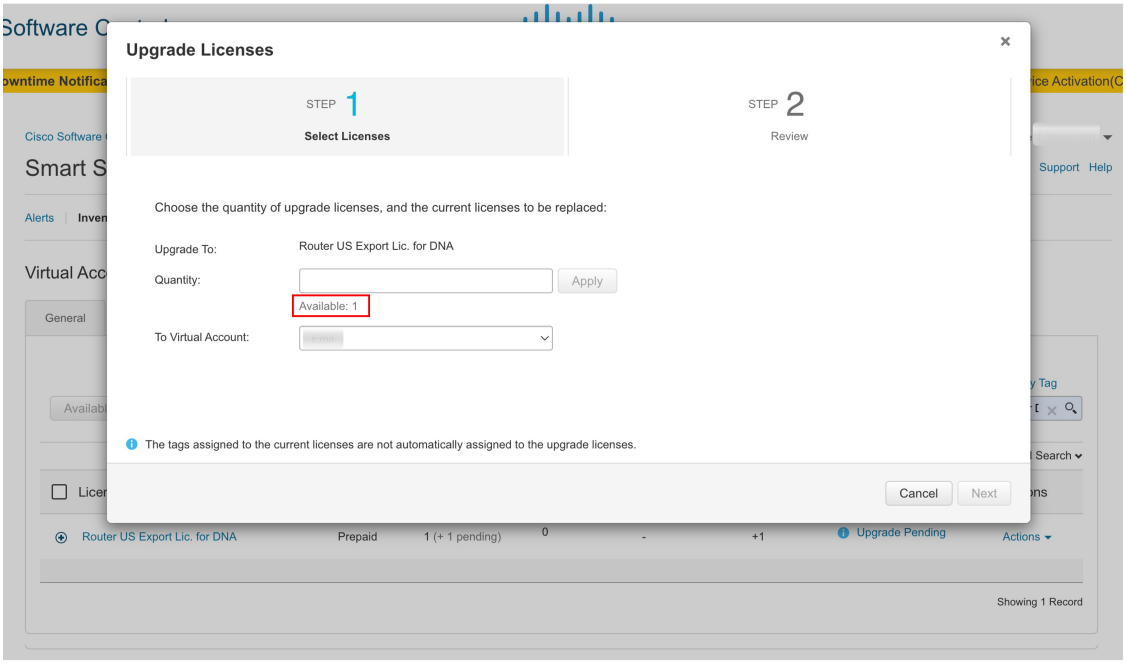
ステップ 6 [Upgrade Pending] をクリックします。

例：



[Upgrade Licenses] ポップアップウィンドウが表示されます。[Quantity] フィールドの下に、使用可能なアップグレードライセンスの数が表示されます。

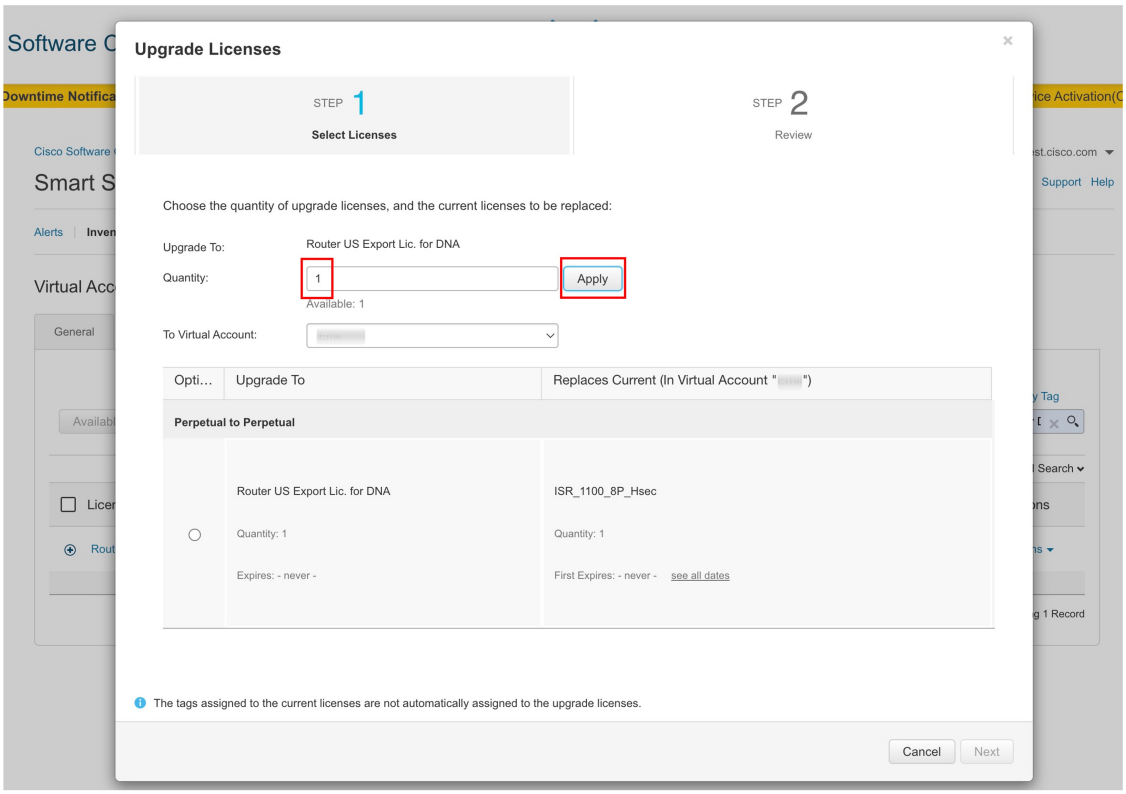
例：



ステップ 7 [Quantity] フィールドに変換するアップグレードライセンスの数を入力し、[Apply] をクリックします。

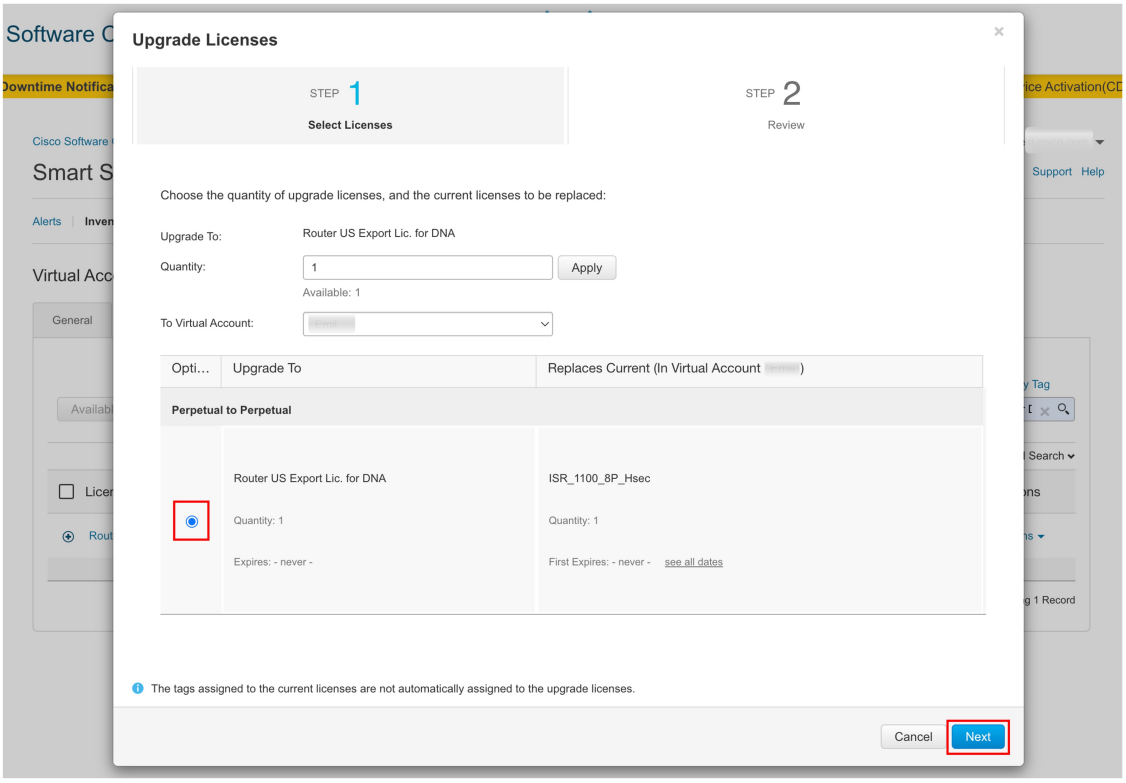
Router US Export Lic for DNA ライセンスの数と置き換えられるデバイスに固有の HSECK9 ライセンスの数が、同じウィンドウのテーブルに表示されます。

例：



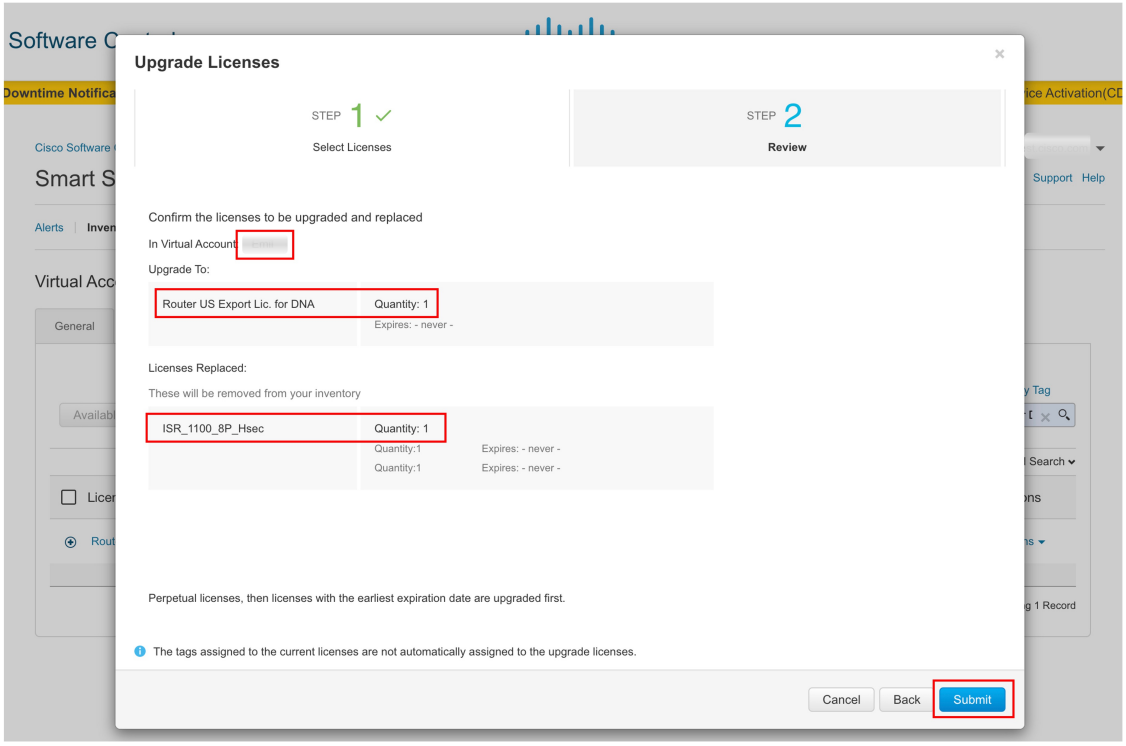
ステップ 8 オプションボタンを選択し、[Next] をクリックします。

例：



ステップ 9 すべての情報を確認し、[Submit] をクリックします。

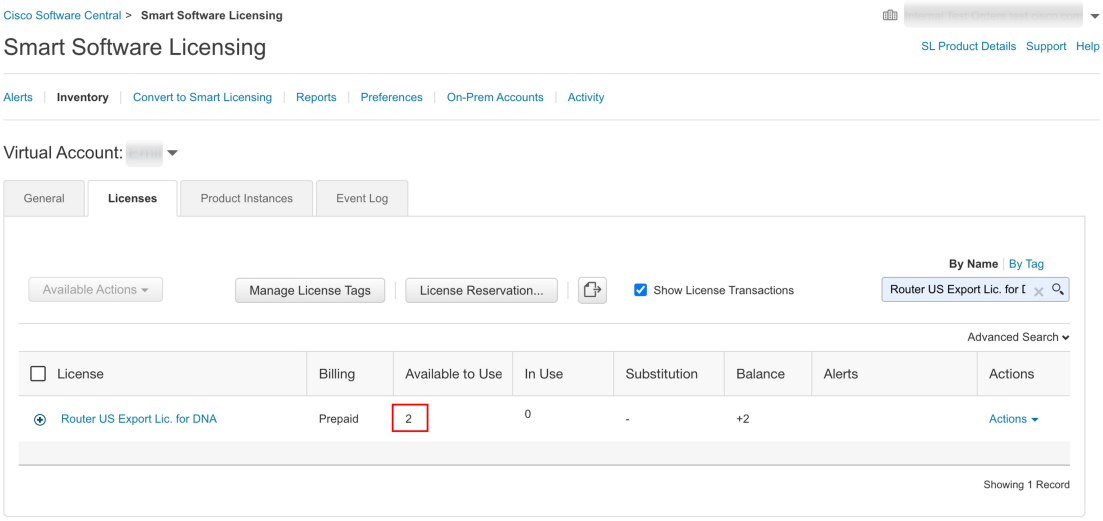
例：



ステップ 10 [Licenses] タブで、再度検索バーを使用して Router US Export Lic for DNA を見つけます。更新された数については、[Available to Use] を確認します。

以下のサンプルのスクリーンショットでは、Router US Export Lic for DNA ライセンスの数が 1 から 2 に増えています。

例：



次のタスク

Router US Export Lic for DNA HSECK9 ライセンスを使用するには、導入したトポロジに従って（デバイスに）SLAC をインストールします。

リソース使用率測定レポートの例

次に、XML 形式のサンプルリソース使用率測定（RUM）レポートを示します（「RUM レポートおよびレポート確認応答」を参照）。このような複数のレポートを連結して 1 つのレポートを形成できます。

```
<?xml version="1.0" encoding="UTF-8"?>
  <smartLicense>
```

[redacted]

```
  </smartLicense>
```

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。