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。

	コマンドまたはアクション	目的
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 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 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 mgmt-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：	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。

	コマンドまたはアクション	目的
	`Device(config)# Device(config)# ip name-server vrf mgmt-vrf 173.37.137.85`	
ステップ 11	**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 12	**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 [Available Actions] → [Add Single Product Instance] を選択します。

ステップ 2 [Host]（ホストの IP アドレス）を入力します。

ステップ 3 [Connect Method] を選択し、適切な [CSLU Initiated] 接続方法を選択します。

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。

[General] をクリックすると、詳細な [Add Product] ウィンドウが開きます。

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 [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] にリストされて、[Last Contact] には [-never] と表示されます。

RUM レポートを受信するための CSLU での CSLU 開始型製品インスタンスの設定（CSLU インターフェイス）

CSLU 開始型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 レポートを受信するように CSLU を設定します。

手順

ステップ 1 [Preferences] タブで、[Cisco is Available] をクリックします。

ステップ 2 [Cisco User ID] と [Cisco Password] を使用してシスコにログインします。

ステップ 3 適切な**スマートアカウント（SA）**と**バーチャルアカウント**を選択します。

ステップ 4 次のサブステップを実行します。

a) [Actions for Selected] をクリックします。
b) メニューから [Edit] を選択します。
c) [Host] に入力します。
d) 適切な **CSLU 開始型接続方式**を選択します。
e) [Host Identifier] をクリックします。
f) 製品インスタンスの [User Name] と [Password] を入力します。
g) [Save] をクリックします。

ステップ 5 RUM レポートを収集してシスコ（CSSM）に送信するには、[Actions for Selected] メニューに移動し、[Collect Usage] を選択します。

RUM レポートがシスコに送信されます。

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。
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。

	コマンドまたはアクション	目的
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、デフォルトで有効にされています。 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。
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文字で、埋め込みスペースを使用で

	コマンドまたはアクション	目的
		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（RUM レポートを受信するための CSLU での CSLU 開始型製品インスタンスの設定（CSLU インターフェイス）（6 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。

Download All For Cisco（CSLU インターフェイス）

[Download All for Cisco] メニューオプションは、オフラインの目的で使用される手動プロセスです。[Download For Cisco] メニューオプションを使用するには、次の手順を実行します。

手順

ステップ 1 CSLU の [Preferences] タブ画面で、[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 [Product Instances] > [Download All For Cisco] 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端末に移動し、次の手順を実行します。CSSM への使用状況データのアップロードと ACK のダウンロード （24 ページ）

ファイルがダウンロードされたら、**CSLU** に転送できます。

ステップ 5 [Upload from Cisco] をクリックします。Upload From Cisco（CSLU インターフェイス） （12 ページ）を参照してください。

Upload From Cisco（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 デバイスの **ACK ファイル**がダウンロードされていることを確認します。次を参照してください。Download All For Cisco（CSLU インターフェイス） （11 ページ）

ステップ 2 CSLU のメイン画面から、[Product Instance] > [Upload from Cisco] を選択します。

ステップ 3 [Cisco File Upload] ウィンドウが開き、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、[File] 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、ACK ファイルがサーバ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。

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 Mgmt-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	**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 6	**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 7	**ip host tools.cisco.com** *ip-address* 例：	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

	コマンドまたはアクション	目的
	`Device(config)# ip host tools.cisco.com 209.165.201.30`	スト名/アドレス静的マッピングを設定します。

ステップ 8	**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 9	**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。

ステップ 10	**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。

ステップ 11	**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。

	コマンドまたはアクション	目的
ステップ 12	**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 13	**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 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。

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 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

このタスクを完了するには、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。

手順

ステップ 1 https://software.cisco.com で CSSM Web UI にログインし、[Smart Software Licensing] 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。

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 [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。

ステップ 6 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 （29 ページ） を参照してください。

ステップ 7 [Next] をクリックします。

ステップ 8 [Generate Authorization Code] をクリックします。

ステップ 9 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。

SLAC の手動要求と自動インストール

CSSM 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

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 または CSLU に接続されている。
- 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る。**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。

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`	**license smart authorization request** コマンドは、CSSM または CSLU に SLAC を要求します（CSLU は CSSM から取得します）。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。

	コマンドまたはアクション	目的
		• **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、Cisco 1000 および 4000 シリーズサービス統合型ルータ、および Catalyst 8300 エッジソフトウェアでは、次のコマンドを使用して SLAC を要求およびインストールできます。 **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# license feature hseck9`
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を表示します。

承認コードの削除と返却

ライセンスの承認コードを削除して CSSM のライセンスプールに戻すには、次の手順を実行します。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：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	**show license summary** 例： `Device# show license summary`	削除して返却するライセンスが使用中でないことを確認します。使用中の場合は、まず機能を無効にする必要があります。
ステップ 3	**license smart authorization return** {**all** | **local**} {**offline** [*path*] | **online**} 例：	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。

	コマンドまたはアクション	目的
	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:CSR1000V,SN:9NOG5XBLC07 Return code: Cr9Hx-L1x5Rj-ftwzgl-h9QZAU-1E5DT1-bakWeL-rAEPt9-Wr1Dn7-Rp7	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。 ファイルを保存するパスを指定することもできます。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` **offline** オプションを選択する場合は、CLIや保存したファイルから戻りコードをコピーして CSSM に入力する、という追加の手順を実行する必要があります。CSSMからの製品インスタンスの削除 （21 ページ）を参照してください。
ステップ 4	show license all **例**： Device# **show license all** <output truncated> License Authorizations ========== Overall status: Active: PID:C8000V,SN:9DGLFX6E1EK	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と、`Last return code:` フィールドに戻りコードが表示されます。

	コマンドまたはアクション	目的
	Status: NOT INSTALLED Last return code: 0cjLk8-2SBwKP-dL5Bir-AFJECP-89QpiJ-HCUrbi-ZFp2ij-txSCuD-8Ci <output truncated>	

CSSM からの製品インスタンスの削除

offline キーワードを使用して承認コードを返却する場合、つまり **license smart authorization return** {**all** | **local**} **offline**[*path* を設定した場合は、CSSM で戻りコードを手動で入力する必要があります。**offline** オプションの返却プロセスを実行するには、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

手順

ステップ 1 https://software.cisco.com で CSSM Web UI にログインし、[Smart Software Licensing] 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。

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 必要な製品インスタンスをクリックして展開します。

[Overview] ウィンドウが表示されます。

ステップ 7 [Actions] ドロップダウンリストから、[Remove] を選択します。

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

ステップ 8 [Reservation Return Code] フィールドに、戻りコードを入力します。

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

ライセンスがライセンスプールに戻されます。

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、[Smart Software Licensing] 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。

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。

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。

信頼コードのインストール

信頼コードを手動でインストールするには、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

手順

	コマンドまたはアクション	目的
ステップ 1	CSSM からの信頼コード用新規トークンの生成 （22 ページ）	まだ CSSM から信頼コードファイルを生成してダウンロードしていない場合は、生成とダウンロードを実行します。
ステップ 2	**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 3	**license smart trust idtoken** *id_token_value* {**local** | **all**} [**force**] 例： `Device# license smart trust idtoken NGMwMjk5mYtNZaxMS00NzMZmtgWm all force`	CSSM との信頼できる接続を確立できます。*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 がすでに登録されている場合、CSSM は同じ UDI の新規登録を許可しません。**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 4	**show license status**
	例：
	`<output truncated>`
	`Trust Code Installed:`
	`  Active:`
	`PID:C9500-24Y4C,SN:CAT2344L4GH`
	`    INSTALLED on Sep 04 01:01:46 2020 EDT`
		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
	Standby: PID:C9500-24Y4C,SN:CAT2344L4GJ 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、[Smart Software Licensing] 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。

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

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 （25 ページ） を参照してください

CSSM への使用状況データのアップロードと ACK のダウンロード

製品インスタンスが CSSM や CSLU に接続されていない場合に RUM レポートを CSSM にアップロードして ACK 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

手順

ステップ 1 https://software.cisco.com で CSSM Web UI にログインします。

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。

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。

使用状況レポートは、アップロード後に CSSM で削除できません。

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の `.txt` ACK ファイルを保存します。

[Acknowledgment] 列に「ACK」が表示されるまで待ちます。処理する RUM レポートが多数ある場合、CSSM では数分かかることがあります。

これで、ファイルを製品インスタンスにインストールすることも、CSLU に転送することもできます。

製品インスタンスへのファイルのインストール

製品インスタンスが CSSM または CSLU に接続されていない場合に、製品インスタンスに SLAC、ポリシー、ACK、またはトークンを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 の場合の参照： CSSM からの SLAC の生成とファイルへのダウンロード （16 ページ）
- ポリシーの場合の参照： CSSM からのポリシーファイルのダウンロード （24 ページ）
- ACK の場合の参照： CSSM への使用状況データのアップロードと ACK のダウンロード （24 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	**copy** *source* **bootflash:***file-name* 例： `Device# copy tftp://10.8.0.6/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。

転送タイプと URL 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。 • **cslu**：転送モードとして CSLU を有効にします。これがデフォルトの転送モードです。 • **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。
ステップ 4	**license smart url** {*url* | **cslu** *cslu_url* | **default** | **smart** *smart_url* | **utility** *smart_url*} 例： `Device(config)# license smart url cslu` **http://192.168.0.1:8182/cslu/v1/pi**	設定された転送モードに使用する 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 • **cslu** *cslu_url*：転送モードとして **cslu** を設定している場合は、このオプションを設定します。CSLU URL を次のように入力します。 http://<cslu_ip_or_host>:8182/cslu/v1/pi

	コマンドまたはアクション	目的
		<cslu_ip_or_host> には、CSLU をインストールした Windows ホストのホスト名または 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。 • **default**：CSSM へのデフォルト接続を使用するには、このオプションを設定します。デフォルトの URL は次のとおりです。 http://cslu-local:8182/cslu/v1/pi • **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。この重複エントリに対してこれ以上のアクションは必要ありません。 • **utility** *smart_url*：このオプションは CLE には表示されますが、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。 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。

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>

  </smartLicense>
```

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（16 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**	ライセンス名
ISR1K-8P	C1111-8P	ISR_1100_8P_Hsec
	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	
	C1117-8PLTEEA	

製品ファミリ	PID	ライセンス名
	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	
	C1115-8PMLTEEA	
	C1118-8P	

製品ファミリ	**PID**	ライセンス名
	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**	ライセンス名
ISR1K - 4P	C1111-4P	ISR_1100_4P_Hsec
	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	
	C1117-4PMWE	

製品ファミリ	**PID**	ライセンス名
	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**	ライセンス名
ISR1K-2P	C1109-2PLTEGB	ISR_1100_2P_Hsec
	C1109-2PLTEUS	
	C1109-2PLTEVZ	
	C1109-2PLTEJN	
	C1109-2PLTEAU	
	C1109-2PLTEIN	
ISR4200	ISR4221/K9	<エントリの欠落>
	ISR4221X/K9	
ISR4300	ISR4321/K9	ISR_4321_Hsec
	ISR4331/K9	ISR_4331_Hsec
	ISR4351/K9	ISR_4531_Hsec
ISR4400	ISR4431/K9	ISR_4400_Hsec
	ISR4451/K9	
	ISR4451-X/K9	
	ISR4461/K9	
	ISR9431 ???	
	ISR9331 ???	

製品ファミリ	PID	ライセンス名
C8300	C8300-1N1S-4T2X	Router US Export Lic for DNA
	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	
	ISR1100-4G	
	ISR1100-4GLTENA	
	ISR1100-4GLTEGB	
	ISR1100X-4G	
	ISR1100X-6G	
C8500	C8500-12X4QC	
	C8500-12X	
	C8500L-8S4X	