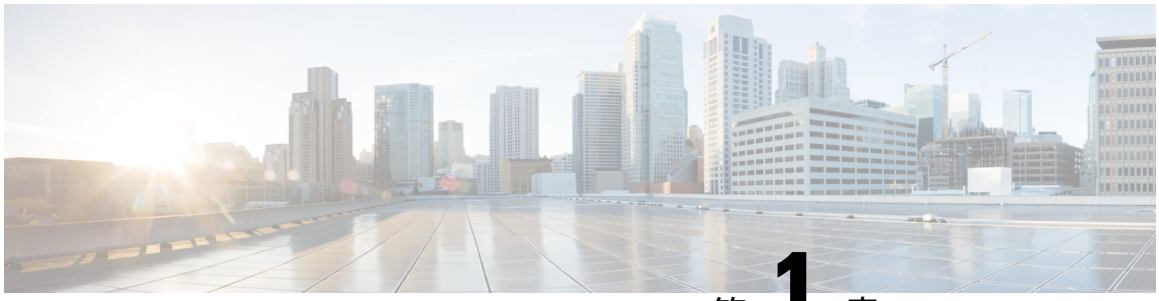
シスコ エンタープライズ ルーティング プラットフォーム向けポリシーを使用したスマートライセンス管理

初版：2020 年 9 月 25 日

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/



第 1 章

ポリシーを使用したスマートライセンシングの概要

ポリシーを使用したスマートライセンシングの概要

ポリシーを使用したスマートライセンシングは、スマートライセンシングの拡張バージョンであり、ネットワークの運用を中断させないライセンスソリューションを提供するという主目的がありますが、むしろ、購入および使用しているハードウェアおよびソフトウェアライセンスを考慮してコンプライアンス関係を実現するライセンスソリューションを提供するという目的もあります。

この拡張ライセンスモデルの主な利点は次のとおりです。

- シームレスな初日運用

  ライセンスを注文した後は、輸出規制または適用ライセンスを使用しない限り、キーの登録や生成などの準備手順は必要ありません。これらのライセンスは、使用前に承認が必要です。他のすべてのライセンスについては、製品機能をデバイスですぐに設定できます。

- Cisco IOS XE の一貫性

  Cisco IOS XE ソフトウェアを実行するキャンパスおよび産業用イーサネットスイッチング、ルーティング、およびワイヤレスデバイスには、均一なライセンスエクスペリエンスがあります。

- 可視性と管理性

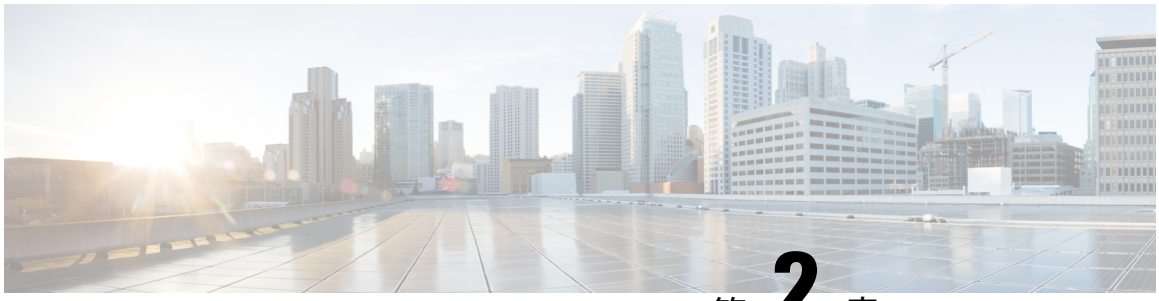
  使用中の情報を把握するためのツール、テレメトリ、製品タギング。

- コンプライアンスを維持するための柔軟な時系列レポート

  Cisco Smart Software Manager（CSSM）に直接または間接的に接続しているか、外部との接続性のないネットワークに接続しているかにかかわらず、簡単なレポートオプションを使用できます。

ポリシーを使用したスマートライセンシングの概要

このドキュメントでは、ポリシーを使用したスマートライセンシングの概念、設定、およびトラブルシューティングについて説明します。



第 2 章

はじめに

ここでは、このマニュアルの構成、このマニュアルで使用される表記法、および関連製品やサービスに関する詳細の入手方法について説明します。

コンテンツ内の移動

このドキュメントは、次の主要なセクションに分かれています。

- ポリシーを使用したスマートライセンシングに関する情報：ポリシーを使用したスマートライセンシングの概念、サポートされる各トポロジの概要、サポートされる製品、およびポリシーを使用したスマートライセンシングと他の機能との連携について説明します。
- 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：新規展開でのみ、サポートされるトポロジを実装するための設定情報について説明します。
- 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：すべてのタスクをグループ化しています。製品インスタンス、CSLU インターフェイス、および CSSM Web UI で実行されるタスクが含まれます。
- ポリシーを使用したスマートライセンシングのコマンドリファレンス：コマンドシンタックスの詳細について説明します。スマート ライセンシング コマンドのみが含まれます。

このドキュメントでは、発注と請求に関連する詳細な手順については説明しませんが、これらの点については適宜このドキュメントで参考情報を紹介しています。発注と請求の詳細については、「その他の参考資料」セクションに記載されているドキュメントリンクを参照してください。

表記法

このマニュアルでは、以下の表記法を使用しています。

表記法	説明
^ または Ctrl	^ 記号と Ctrl は両方ともキーボードの Control（Ctrl）キーを表します。たとえば、^D または Ctrl+D というキーの組み合わせは、Ctrl キーを押しながら D キーを押すことを意味します（ここではキーを大文字で表記していますが、小文字で入力してもかまいません）。
太字	コマンド、キーワード、およびユーザーが入力するテキストは**太字**で記載されます。
イタリック フォント	文書のタイトル、新規用語、強調する用語、およびユーザが値を指定する引数は、イタリック体で示しています。
`Courier` フォント	システムが表示する端末セッションおよび情報は、`courier` フォントで示しています。
`太字の courier` フォント	**`太字の Courier`** フォントは、ユーザが入力しなければならないテキストを示します。
[x]	角カッコの中の要素は、省略可能です。
...	構文要素の後の省略記号（3 つの連続する太字ではないピリオドでスペースを含まない）は、その要素を繰り返すことができることを示します。
|	パイプと呼ばれる縦棒は、一連のキーワードまたは引数の選択肢であることを示します。
[x | y]	どれか 1 つを選択できる省略可能なキーワードは、角カッコで囲み、縦棒で区切って示しています。
{x | y}	どれか 1 つを選択しなければならない必須キーワードは、波カッコで囲み、縦棒で区切って示しています。
[x {y | z}]	角かっこまたは波かっこが入れ子になっている箇所は、任意または必須の要素内の任意または必須の選択肢であることを表します。角かっこ内の波かっこと縦棒は、省略可能な要素内で選択すべき必須の要素を示しています。
string	引用符を付けない一組の文字。string の前後には引用符を使用しません。引用符を使用すると、その引用符も含めて string とみなされます。
< >	パスワードのように出力されない文字は、山カッコで囲んで示しています。
[ ]	システム プロンプトに対するデフォルトの応答は、角カッコで囲んで示しています。
!、#	コードの先頭に感嘆符（!）またはポンド記号（#）がある場合には、コメント行であることを示します。

読者への警告の表記法

このマニュアルでは、読者への警告に次の表記法を使用しています。

（注） 「注釈」です。役立つ情報やこのマニュアルに記載されていない参照資料を紹介しています。

ヒント 「問題解決に役立つ情報」です。

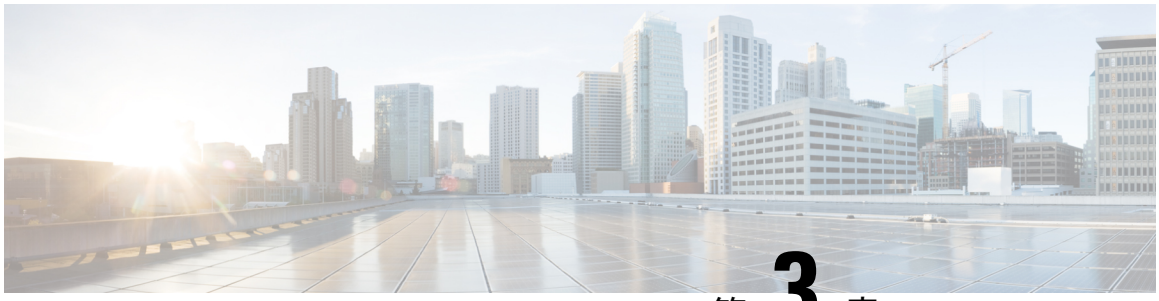
注意 「要注意」の意味です。機器の損傷またはデータ損失を予防するための注意事項が記述されています。

ワンポイント アドバイス 時間を節約する方法です。ここに紹介している方法で作業を行うと、時間を短縮できます。

警告 安全上の重要な注意事項

この警告マークは「危険」の意味です。人身事故を予防するための注意事項が記述されています。機器の取り扱い作業を行うときは、電気回路の危険性に注意し、一般的な事故防止対策に留意してください。各警告の最後に記載されているステートメント番号を基に、装置に付属の安全についての警告を参照してください。ステートメント 1071

これらの注意事項を保管しておいてください。



第 3 章

ポリシーを使用したスマートライセンシングに関する情報

概要

ポリシーを使用したスマートライセンシングは、ライセンスのさまざまな側面をシームレスに体験できるソフトウェアライセンス管理ソリューションです。

- ライセンスの購入：既存のチャネルからライセンスを購入し、Cisco Smart Software Manager（CSSM）ポータルを使用して製品インスタンスとライセンスを表示します。

（注） ポリシーを使用したスマートライセンシングの実装を簡素化するには、新しいハードウェアまたはソフトウェアを注文する際にスマートアカウントとバーチャルアカウントの情報を提供します。これにより、シスコは製造時に該当するポリシーおよび承認コード（用語は以下のセクション概念 （8 ページ）で説明）をインストールできます。

- 使用：ほとんどのライセンスは適用（エンフォース）されません。つまり、ソフトウェアとそれに関連付けられているライセンスの使用を開始する前に、キーの登録や生成などのライセンス固有の操作を完了する必要はありません。輸出規制および適用されたライセンスのみ、使用前にシスコの承認が必要です。ライセンスの使用状況はタイムスタンプとともにデバイスに記録され、必要なワークフローは後日完了できます。

- ライセンスの使用状況をCSSMにレポート：ライセンス使用状況レポートには複数のオプションを使用できます。Cisco Smart Licensing Utility（CSLU）を使用することも、CSSMに使用状況の情報を直接レポートすることもできます。使用状況情報をダウンロードしてCSSMにアップロードする、クローズドネットワークのオフラインレポートのプロビジョニングも使用できます。使用状況レポートはプレーンテキストのXML形式です。リソース使用率測定レポートの例 （62 ページ）を参照してください。
- 調整：差分請求が適用される状況用（購入と消費を比較して差分がある場合）。

概念

ここでは、ポリシーを使用したスマートライセンシングの主要な概念について説明します。

ライセンス執行（エンフォースメント）タイプ

所与のライセンスは、3つの適用タイプのいずれかに属します。適用タイプは、ライセンスを使用する前に承認が必要かどうかを示します。

- 不適用または非適用

  ライセンスの大半はこの適用タイプに属します。不適用ライセンスは、外部との接続がないネットワークで使用する前、または接続されたネットワークでの登録前に承認を必要としません。このようなライセンスの使用条件は、エンドユーザライセンス契約（EULA）に基づきます。

- 適用

  この適用タイプに属するライセンスは、使用前に承認が必要です。必要な承認は承認コードの形式で行われ、対応する製品インスタンスにインストールする必要があります。

  適用ライセンスの例としては、シスコの産業用イーサネットスイッチで利用可能なMedia Redundancy Protocol（MRP）クライアントライセンスがあります。

- 輸出規制

  この適用タイプに属するライセンスは米国の取引規制法によって輸出が制限されていて、これらのライセンスは使用前に承認が必要です。これらのライセンスの場合も、必要な承認コードは、対応する製品インスタンスにインストールする必要があります。シスコは、ハードウェア購入の際に発注がある場合、輸出規制ライセンスをプリインストールすることがあります。

  輸出規制ライセンスの例としては、特定のシスコルータで使用可能な高セキュリティ（HSECK9）ライセンスがあります。

適用および輸出規制ライセンスのリストは限定されています。シスコは、ハードウェア購入の際に発注がある場合、輸出規制および適用ライセンスに必要な承認をプリインストールすることがあります。完全で最新のリストについては、「承認コード」セクションの表 1 : SLAC を必要とするライセンス （9 ページ）を参照してください。

ライセンス継続期間

これは、購入したライセンスが有効な期間を指します。所与のライセンスは、上記のいずれかの適用タイプに属し、次の期間有効です。

- 永久：このライセンスには使用期限日はありません。
- サブスクリプション：ライセンスは特定の日付まで有効です。

承認コード

スマートライセンシング承認コード（SLAC）は、輸出規制または適用（エンフォース）ライセンスの有効化および継続使用を可能にします。承認コードは製品インスタンスにインストールされます。使用しているライセンスに承認コードが必要な場合は、CSSM から要求できます。

SLAC を削除して CSSM ライセンスプールに戻すことができます。ただし、これを行うには、まずライセンスを使用する機能を無効にする必要があります。使用中の SLAC は返却できません。

表 *1 : SLAC* を必要とするライセンス

適用タイプ	ライセンス
輸出規制	HSECK9
適用	MRP クライアント MRP マネージャ

（注） 以前のライセンスモデルからポリシーを使用したスマートライセンシングにアップグレードする場合は、これらのライセンスのうちいずれかを所有している可能性がありますが、それぞれのライセンスには固有の承認コードである特定ライセンス予約（SLR）または製品認証キー（PAK）があります。これらの既存のライセンスの承認コードは、ポリシーを使用したスマートライセンシングへのアップグレード後にサポートされます。

ポリシー

ポリシーは、製品インスタンスに次のレポート手順を提供します。

- License usage report acknowledgement requirement (Reporting ACK required)：ライセンス使用状況レポートは RUM レポートと呼ばれ、確認応答は ACK と呼ばれます（「RUM レポートおよびレポート確認応答」を参照）。これは、この製品インスタンスのレポートに CSSM 確認応答が必要かどうかを指定する yes または no の値です。デフォルトポリシーは常に「yes」に設定されます。

- First report requirement (days)：最初のレポートは、ここで指定した期間内に送信される必要があります。
- Reporting frequency (days)：後続のレポートは、ここで指定した期間内に送信される必要があります。
- Report on change (days)：ライセンスの使用状況が変更された場合は、ここで指定した期間内にレポートが送信される必要があります。

ポリシー選択について

CSSMは、製品インスタンスに適用されるポリシーを決定します。特定の時点で使用されているポリシーは1つだけです。ポリシーとその値は、使用されているライセンスなど、さまざまな要因に基づいています。

`Cisco default`は、製品インスタンスで常に使用可能なデフォルトポリシーです。他のポリシーが適用されていない場合、製品インスタンスはこのデフォルトポリシーを適用します。次の表（表 2 : ポリシー：Cisco default （10 ページ））に、`Cisco default` ポリシー値を示します。

お客様はポリシーを設定することはできませんが、Cisco Global Licensing Operations チームに連絡して、カスタマイズされたポリシーを要求することができます。Support Case Manager に移動します。[OPEN NEW CASE] をクリックし、[Software Licensing] を選択します。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。カスタマイズされたポリシーは、CSSM のスマートアカウントを介して使用することもできます。

（注） 適用されているポリシー（使用中のポリシー）とそのレポート要件を確認するには、特権EXECモードで **show license all** コマンドを入力します。

表 *2 :* ポリシー：***Cisco default***

ポリシー：`Cisco default`	デフォルトポリシー値
Export (Perpetual/Subscription) （注） 適用タイプが「輸出規制」のライセンスにのみ適用されます。	Reporting ACK required：Yes First report requirement (days)：0 Reporting frequency (days)：0 Report on change (days)：0
Enforced (Perpetual/Subscription) （注） 適用タイプが「適用（エンフォース）」のライセンスにのみ適用されます。	Reporting ACK required：Yes First report requirement (days)：0 Reporting frequency (days)：0 Report on change (days)：0

ポリシー：`Cisco default`	デフォルトポリシー値
Unenforced/Non-Export Perpetual[1]	Reporting ACK required：Yes First report requirement (days)：365 Reporting frequency (days)：0 Report on change (days)：90
Unenforced/Non-Export Subscription	Reporting ACK required：Yes First report requirement (days)：90 Reporting frequency (days)：90 Report on change (days)：90

[1] Unenforced/Non-Export Perpetual の場合：デフォルトポリシーの最初のレポート要件（365日以内）は、ディストリビュータやパートナーからハードウェアやソフトウェアを購入した場合にのみ適用されます。

RUM レポートおよびレポート確認応答

リソース使用率測定レポート（RUM レポート）は、ポリシーで指定されたレポート要件を満たすために製品インスタンスが生成するライセンス使用状況レポートです。

確認応答（ACK）は CSSM からの応答であり、RUM レポートのステータスに関する情報を提供します。

製品インスタンスに適用されるポリシーによって、次のレポート要件が決まります。

- RUM レポートが CSSM に送信されるかどうか、およびこの要件を満たすために提供される最大日数。
- RUM レポートに CSSM からの確認応答（ACK）が必要かどうか。
- ライセンス消費の変化を報告するために提供される最大日数。

RUM レポートには、信頼コード要求や SLAC 要求などの他の要求が伴う場合があります。そのため、受信した RUM レポート ID に加えて、CSSM からの ACK には承認コード、信頼コード、およびポリシーファイルが含まれることがあります。

信頼コード

製品インスタンスがすべての RUM レポートに署名するために使用する、UDI に関連付けられた公開キー。これにより、改ざんが防止され、データの真正性が確保されます。

アーキテクチャ

ここでは、ポリシーを使用したスマートライセンシングの実装に含めることができるさまざまなコンポーネントについて説明します。

製品インスタンス

製品インスタンスとは、Unique Device Identifier（UDI）によって識別されるシスコ製品の単一インスタンスです。

製品インスタンスは、ライセンス使用状況（RUM レポート）を記録および報告し、期限切れのレポートや通信障害などに関するアラートとシステムメッセージを提供します。RUM レポートおよび使用状況データは、製品インスタンスに安全に保存されます。

このドキュメントでは、「製品インスタンス」という用語は、特に明記しない限り、サポートされているすべての物理および仮想製品インスタンスを指します。このドキュメントの範囲内にある製品インスタンスについては、サポート対象製品 （18 ページ）を参照してください。

CSSM

Cisco Smart Software Manager（CSSM）は、一元化された場所からすべてのシスコ ソフトウェア ライセンスを管理できるポータルです。CSSM は、現在の要件を管理し、将来のライセンス要件を計画するための使用傾向を確認するのに役立ちます。

CSSM Web UI には https://software.cisco.com からアクセスできます。[License] タブで、[Smart Software Licensing] のリンクをクリックします。

CSSM に接続できるさまざまな方法については、サポートされるトポロジ （13 ページ） のセクションを参照してください

CSSM では、次のことができます。

- バーチャルアカウントを作成、管理、または表示する。
- 製品インスタンスの登録トークンを作成および管理する。
- バーチャルアカウント間または表示ライセンス間でライセンスを転送する。
- 製品インスタンスを転送、削除、または表示する。
- バーチャルアカウントに関するレポートを実行する。
- 電子メール通知の設定を変更する。
- バーチャルアカウント情報を表示する。

CSLU

Cisco Smart License Utility（CSLU）は Windows ベースのレポートユーティリティで、CSSM に接続されている間、または切断モードの際の、ライセンス集約ワークフローを提供します。このユーティリティが実行する主な機能は次のとおりです。

- ワークフローのトリガー方法に関するオプションを提供します。ワークフローは、CSLU や製品インスタンスによってトリガーできます。
- 製品インスタンスから使用状況レポートを収集し、その使用状況レポートを対応するスマートアカウントやバーチャルアカウントにアップロードします。オンラインでもオフライン（ファイルを使用）でも可能です。同様に、RUM レポート ACK をオンラインまたはオフラインで収集し、製品インスタンスに返送します。
- 承認コード要求を CSSM に送信し、承認コード[2]を CSSM から受信します。

CSLU は、次の方法で実装に含めることができます。

- CSSM に接続されているスタンドアロンツールとして CSLU を使用するための Windows アプリケーションをインストールします。
- CSSM から切断されているスタンドアロンツールとして CSLU を使用するための Windows アプリケーションをインストールします。このオプションを使用すると、必要な使用状況情報がファイルにダウンロードされ、CSSM にアップロードされます。これは、外部と接続していないネットワークに適しています。

サポートされるトポロジ

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を実装するさまざまな方法について説明します。各トポロジについて、付属の概要を参照してセットアップの動作設計を確認し、考慮事項と推奨事項（ある場合）を参照してください。

トポロジを選択した後

トポロジを選択したら、「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」の対応するワークフローを参照して、その実装方法を確認してください。これらのワークフローは、トポロジを実装する最も簡単で迅速な方法を提供します。これらのワークフローは、新しい展開用であり、既存のライセンスソリューションからのアップグレード用や移行用ではありません。

初期実装後、追加の設定タスクを実行する必要がある場合（たとえば、一括で承認コードを手動で要求する場合、または RUM レポートの同期などのメンテナンスタスクを実行する場合）は、「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」を参照してください。

[2] CSLU を使用して、コントローラモード（Cisco SD-WAN 機能用）で動作するシスコルータの承認コード要求を転送できます。

（注） 続行する前に、必ず「サポートされるトポロジ」を確認してください。

CSLU を介して CSSM に接続

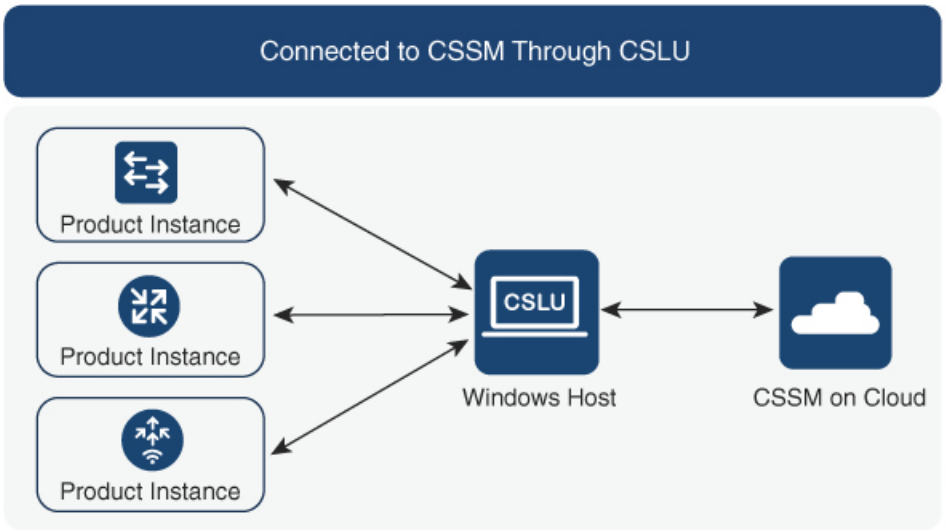
概要：

ここでは、ネットワーク内の製品インスタンスは CSLU に接続され、CSLU は CSSM との単一のインターフェイスポイントになります。製品インスタンスは、必要な情報を CSLU にプッシュするように設定できます。または、構成可能な頻度で製品インスタンスから必要な情報を取得するように CSLU を設定することもできます。

製品インスタンス開始型通信（プッシュ）：製品インスタンスは、CSLU の REST エンドポイントに接続することで、CSLU との通信を開始します。送信されるデータには、RUM レポート、および承認コード、信頼コード、ポリシーの要求が含まれます。必要な間隔で自動的に RUM レポートを CSLU に送信するように製品インスタンスを設定できます。これは、製品インスタンスのデフォルトの方法です。

CSLU 開始型通信（pull 型）：製品インスタンスからの情報の取得を開始するために、CSLU は YANG を使用した NETCONF、RESTCONF、gRPC のモデル、またはネイティブ REST API を使用して製品インスタンスに接続します。サポートされるワークフローには、RUM レポートの製品インスタンスからの受信と CSSM への送信、承認コードのインストール、信頼コードのインストール、およびポリシーの適用が含まれます。

図 *1:* トポロジ：***CSLU*** を介して ***CSSM*** に接続



考慮事項または推奨事項：

ネットワークのセキュリティポリシーに応じて通信方法を選択します。

次の手順：

このトポロジを実装するには、トポロジのワークフロー：CSLU を介して CSSM に接続 （25 ページ）を参照してください。

CSSM に直接接続

概要：

このトポロジは、スマートライセンシングの以前のバージョンで使用でき、ポリシーを使用したスマートライセンシングで引き続きサポートされます。

ここでは、製品インスタンスからCSSMへの直接かつ信頼できる接続を確立します。直接接続には、CSSMへのネットワーク到達可能性が要求されます。その後、製品インスタンスがメッセージを交換し、CSSMと通信するには、このトポロジで使用可能な転送オプションのいずれかを設定します（以下を参照）。最後に、信頼を確立するには、CSSMの対応するスマートアカウントとバーチャルアカウントからトークンを生成し、製品インスタンスにインストールする必要があります。

次の方法で CSSM と通信するように製品インスタンスを設定できます。

- スマート転送を使用して CSSM と通信する。

  スマート転送は、スマートライセンシング（JSON）メッセージがHTTPSメッセージ内に含まれ、製品インスタンスとCSSMの間で交換されることにより通信する転送方法です。次のスマート転送設定オプションを使用できます。

  - スマート転送：この方法では、製品インスタンスは特定のスマート転送ライセンスサーバ URL を使用します。これは、ワークフローのセクションに示すとおりに設定する必要があります。
  - HTTPS プロキシを介したスマート転送：この方法では、製品インスタンスはプロキシサーバを使用してライセンスサーバと通信し、最終的には CSSM と通信します。

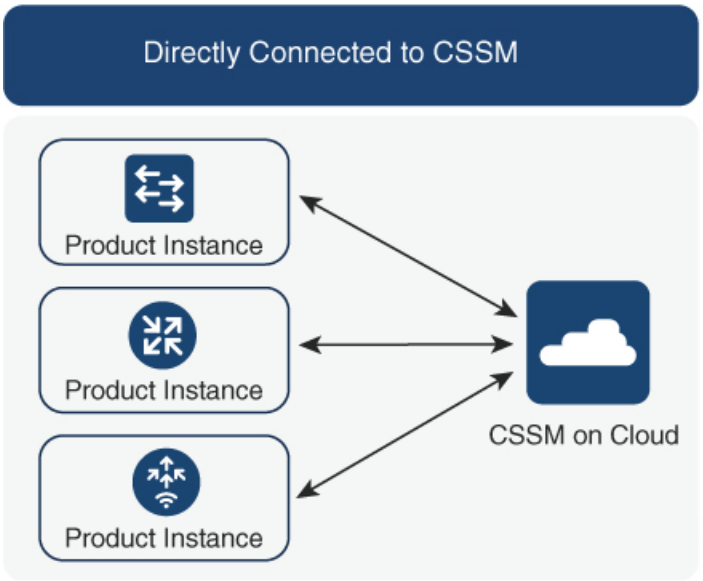
- Call Home を使用して CSSM と通信する。

  Call Home を使用すると、E メールベースおよび Web ベースで重大なシステム イベントの通知を行えます。CSSMへのこの接続方法は、以前のスマートライセンシング環境で使用でき、ポリシーを使用したスマートライセンシングで引き続き使用できます。次の Call Home 設定オプションを使用できます。

  - ダイレクトクラウドアクセス：この方法では、製品インスタンスはインターネット経由でCSSMに使用状況情報を直接送信します。接続に追加のコンポーネントは必要ありません。
  - HTTPS プロキシを介したダイレクトクラウドアクセス：この方法では、製品インスタンスはインターネット経由でプロキシサーバ（Call Home Transport Gateway または市販のプロキシ（Apache など）のいずれか）を介して CSSM に使用状況情報を送信します。

（注） ポリシーを使用したスマートライセンシングは、Cisco Smart Software Manager On-Prem（旧称 Cisco Smart Software Manager サテライト）をサポートしていません。

図 *2:* トポロジ：*CSSM* に直接接続



考慮事項または推奨事項：

CSSMに直接接続する場合は、スマート転送が推奨される転送方法です。この推奨事項は以下に適用されます。

- 新規展開
- 以前のライセンスモデル。ポリシーを使用したスマートライセンシングへの移行後に設定を変更します。
- 現在 Call Home 転送方法を使用している登録済みライセンス。ポリシーを使用したスマートライセンシングへの移行後に設定を変更します。
- 以前のライセンスモデルの評価ライセンスや期限切れのライセンス。ポリシーを使用したスマートライセンシングへの移行後に設定を変更します。

移行後に設定を変更するには、トポロジのワークフロー：CSSM に直接接続 （28 ページ）の「製品インスタンスの設定」にある「接続方法と転送タイプの設定」のオプション1を参照してください。

次の手順：

このトポロジを実装するには、トポロジのワークフロー：CSSM に直接接続 （28 ページ）を参照してください。

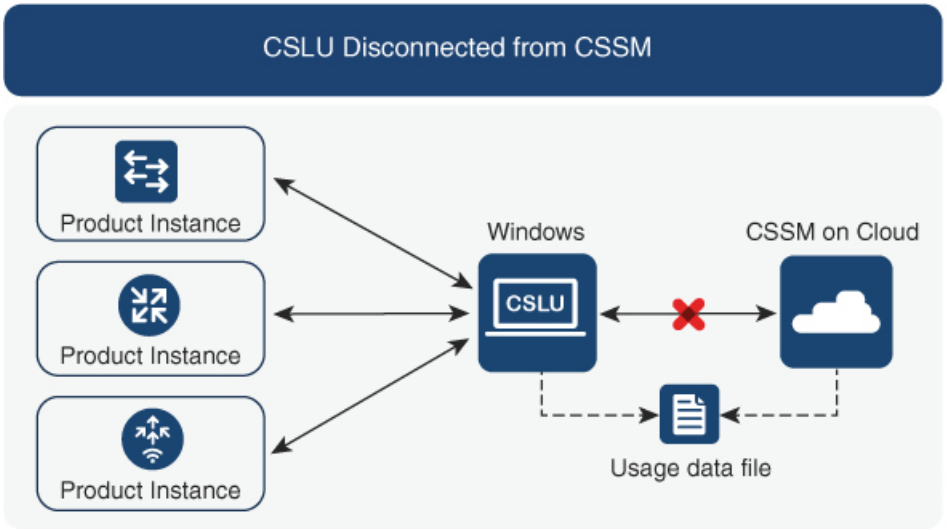
CSLU は CSSM から切断

概要：

ここでは、製品インスタンスが CSLU と通信し、製品インスタンス開始の通信または CSLU 開始の通信を実装するオプションがあります（CSLU を介して CSSM に接続のトポロジと同様）。CSLU と CSSM 間の通信のもう一方はオフラインです。CSLU には、CSSM から切断されたモードで動作するオプションがあります。

CSLU と CSSM 間の通信は、署名済みファイルの形式で送受信され、オフラインで保存された後、場合によっては CSLU または CSSM にアップロードまたはダウンロードされます。

図 *3:* トポロジ：*CSLU* は *CSSM* から切断



考慮事項または推奨事項：

なし。

次の手順：

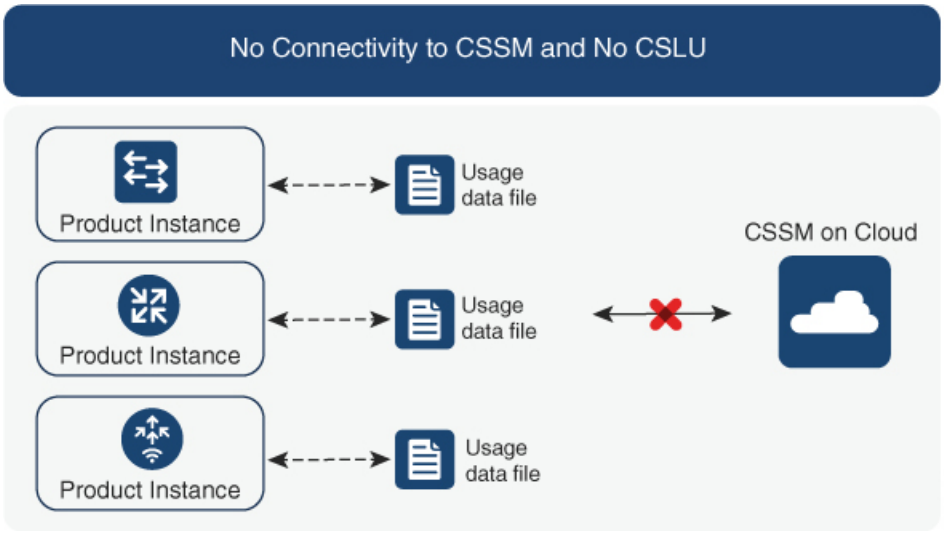
このトポロジを実装するには、トポロジのワークフロー：CSLU は CSSM から切断 （29 ページ）を参照してください。

CSSM への接続なし、CSLU なし

概要：

ここでは、製品インスタンスとCSSMは相互に切断され、他の中間ユーティリティまたはコンポーネントはありません。すべての通信は、ファイルのアップロードとダウンロードという形式です。

図 *4:* トポロジ：*CSSM* への接続なし、*CSLU* なし



考慮事項または推奨事項：

このトポロジは、製品インスタンスがネットワークの外部とオンラインで通信できない高セキュリティ展開に適しています。

次の手順：

このトポロジを実装するには、トポロジのワークフロー：CSSM への接続なし、CSLU なし（32 ページ）を参照してください。

サポート対象製品

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をサポートするCisco IOS-XE製品インスタンスについて説明します。特に指定のない限り、製品シリーズのすべてのモデル（製品 ID または PID）がサポートされます。

表 *3:* ポリシーを使用したスマートライセンシング：サポート対象製品

製品カテゴリ	製品シリーズ
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	

製品カテゴリ	製品シリーズ
	Cisco 1000 シリーズ サービス統合型ルータ
	Cisco 4000 シリーズ サービス統合型ルータ
	Cisco ASR 1000 シリーズ アグリゲーション サービス ルータ
Cisco Catalyst 8000 エッジ プラットフォーム ファミリ	
	Catalyst 8300 シリーズ エッジ プラットフォーム
	Catalyst 8500 シリーズ エッジ プラットフォーム

他の機能との相互作用

高可用性

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をサポートするソフトウェアバージョンを実行するときに、高可用性設定に適用される考慮事項について説明します。次の高可用性セットアップは、このドキュメントの範囲内です。

1つのアクティブ、1つのスタンバイ、および1つ以上のメンバーで構成されるデバイススタック

デュアル RP（ルートプロセッサ）セットアップ。1 つのシャーシに 2 つの RP がインストールされ、1 つはアクティブ、もう 1 つはスタンバイです。

デュアルシャーシ セットアップ[3]（固定またはモジュラ）。一方のシャーシにアクティブ、もう一方のシャーシにスタンバイがあります。

モジュラシャーシでの、デュアルシャーシとデュアル RP のセットアップ[4]。ここでも 2 つのシャーシが関係し、1 つのシャーシにアクティブ RP、もう 1 つのシャーシにスタンバイ RP があります。デュアル RP とは、最小要件である 1 つのシャーシだけに追加のシャーシ内スタンバイ RP、または各シャーシにシャーシ内スタンバイ RP があることを指します。

高可用性セットアップでの承認コード要件

使用前に承認が必要なライセンスを使用していて（SLAC または SLR、PLR など）、上記の高可用性セットアップのいずれかを使用している場合、必要な承認コードの数は、UDI の数に対応します。

[3] Cisco Catalyst スイッチで使用可能な Cisco StackWise Virtual 機能が、このようなセットアップの例です。
[4] Cisco Catalyst スイッチで使用可能なルートプロセッサ冗長性を備えたクアッドスーパーバイザが、このようなセットアップの例です。

- アクティブとスタンバイの UDI が同じ場合は、1 つの承認コードのみが必要です。これは、UDI が（個々の RP にではなく）シャーシにある場合です。
- 同じシャーシ内のデュアル RP に 2 つの異なる UDI がある場合（つまり UDI が RP にある場合）、各 RP に専用の承認コードが必要です。
- 高可用性セットアップで 2 つのシャーシが関係している場合は、各シャーシに専用の UDI があるため、専用の承認コードが必要です。
- デバイススタックの場合は、アクティブのみに承認コードが必要です。

UDI 情報を表示するには、特権 EXEC モードで **show license udi** コマンドを使用します。高可用性セットアップの場合は、すべての UDI が表示されます。

高可用性セットアップでの信頼コード要件

必要な信頼コードの数は、UDI の数によって異なります。アクティブな製品インスタンスは、高可用性セットアップのすべてのデバイスに対する要求を送信し、ACK で返されるすべての信頼コードをインストールできます。

高可用性セットアップでのポリシー要件

高可用性セットアップにのみ適用されるポリシー要件はありません。スタンドアロン製品インスタンスの場合と同様に、高可用性セットアップにも 1 つのポリシーのみが存在し、これがアクティブになります。アクティブのポリシーは、設定のすべてのスタンバイまたはメンバーに適用されます。

高可用性セットアップでの製品インスタンス機能

このセクションでは、高可用性セットアップでの一般的な製品インスタンス機能と、新しいスタンバイまたはメンバーが既存の高可用性セットアップに追加された場合の製品インスタンスの動作について説明します。

承認コードと信頼コードの場合：アクティブな製品インスタンスは、スタンバイおよびメンバーの承認コードと信頼コードを（必要な場合に）要求し、インストールできます。

ポリシーの場合：アクティブな製品インスタンスがスタンバイと同期します。

レポートの場合：アクティブな製品インスタンスのみが使用状況を報告します。アクティブは、高可用性セットアップのすべてのデバイス（スタンバイまたはメンバーを適宜）の使用状況情報を報告します。スケジュールされたレポートに加えて、次のイベントがレポートをトリガーします。

- スタンバイの追加または削除。RUM レポートには、新しく追加または削除されたスタンバイまたはメンバーに関する情報が含まれます。
- スイッチオーバー。
- リロード。

新規メンバーまたはスタンバイ追加の場合：

- CSLU に接続されている製品インスタンスは、それ以上のアクションを実行しません。
- CSSMに直接接続されている製品インスタンスは、信頼の同期を実行します。信頼の同期には、次のものが含まれます。

  スタンバイまたはメンバーに信頼コードがまだインストールされていない場合は、信頼コードのインストール。

  信頼コードがすでにインストールされている場合は、信頼の同期プロセスにより、新しいスタンバイまたはメンバーがアクティブと同じスマートアカウントおよびバーチャルアカウントにあることが保証されます。そうでない場合、新しいスタンバイまたはメンバーは、アクティブと同じスマートアカウントとバーチャルアカウントに移動されます。

  承認コード、ポリシー、および購入情報のインストール（該当する場合）

  現在の使用状況情報を含む RUM レポートの送信。

アップグレードとダウングレード

以前のライセンスモデルから、ポリシーを使用したスマートライセンシングをサポートするソフトウェアイメージにアップグレードした後は、ポリシーを使用したスマートライセンシングが唯一のサポートされるライセンスモデルであり、製品インスタンスはライセンスの変更なしで動作し続けます。ただし、ライセンスワークフローのすべての側面が期待どおりに機能し続けるように、他の設定が必要な場合があります。このセクションでは、そのような変更の概要について説明します。

（注） ポリシーを使用したスマートライセンシングをサポートするソフトウェアバージョンにアップグレードまたは移行するには、『Early Field Trial Guide』を参照してください。

アップグレードが既存ライセンスの適用タイプに与える影響

ポリシーを使用したスマートライセンシングをサポートするソフトウェアバージョンにアップグレードする場合、既存のPLR、SLR、CSL、PAK、およびRTUライセンスの処理方法は、適用タイプによって異なります。

- アップグレード前に使用されていた不適用ライセンスは、アップグレード後も引き続き使用できます。
- アップグレード前に使用されていた適用ライセンスは、必要な承認が存在する場合、アップグレード後も引き続き使用できます。これは、アップグレード時にシステムによって認証されます。必要な承認が存在しない場合は、使用する前にSLACをインストールする必要があります。SLACの手動要求と自動インストール （51ページ）を参照してください。
- アップグレード前に使用されていた輸出規制ライセンスは、必要な承認が存在する場合、一般にはアップグレード後も引き続き使用できます。

ただし、例外があります。製品インスタンスが輸出規制フラグを持つスマートアカウントに登録されているために HSECK9 ライセンスを持っている場合、ポリシーを使用してスマートライセンシングにアップグレードした後に、SLAC をインストールする必要があります。

対照的に、後述する例のように、以前のスマートライセンシング環境の輸出規制ライセンスでは、アップグレード後に SLAC を再インストールする必要はありません。アップグレード前に製品インスタンスに HSECK9 PAK ライセンスがあった場合、または製品インスタンスに HSECK9 ライセンスを含む SLR 承認コードがあった場合は、ポリシーを使用したスマートライセンシングへのアップグレード後にライセンスが適用されます。SLAC を再度インストールする必要はありません。

アップグレードが既存ライセンスのレポートに与える影響

使用権（RTU）レポート：レポートの要件はライセンスによって異なります。詳細については、適用されるポリシーを参照してください。また、**show license usage** コマンドの `Next ACK deadline` フィールドを参照して、レポートが必要かどうかを確認することもできます。

特定ライセンス予約（SLR）レポート：既存の SLR 承認コードは、ポリシーを使用したスマートライセンシングへのアップグレード後に既存のライセンス消費を承認します。したがって、ライセンス消費に変更がある場合は、レポートが必要です。

製品承認キー（PAK）レポート：PAK ライセンスには永続的な有効期間（ライセンス期間）がありますが、ライセンス消費に変更がある場合はレポートが必要です。

永続ライセンス予約（PLR）レポート：PLR ライセンスには永続的な有効期間があり、ライセンス消費に変更がある場合でもレポートは必要ありません。

Cisco ソフトウェアライセンシング（CSL）レポート：CSL ライセンスには永続的な有効期間があり、ライセンス消費に変更がある場合でもレポートは必要ありません。

アップグレードが既存ライセンスの転送タイプに与える影響

既存の設定で転送タイプが設定されている場合、ポリシーを使用したスマートライセンシングへのアップグレード後も転送タイプが保持されます。

スマートライセンシングの以前のバージョンと比較した場合、ポリシーを使用したスマートライセンシングでは追加の転送タイプを使用できます。デフォルトの転送モードにも変更があります。次の表に、これがアップグレードに与える影響を示します。

アップグレード前の転送タイプ	アップグレード前のライセンスまたはライセンスの状態	アップグレード後の転送タイプ
デフォルト（callhome）	評価	cslu（ポリシーを使用したスマートライセンシングのデフォルト）
	SLR PLR	off
	登録	callhome
smart	評価	smart
	SLR PLR	smart
	登録	smart

アップグレードがトークン登録プロセスに与える影響

以前のバージョンのスマートライセンシングでは、CSSMへの登録と接続にトークンが使用されていました。ID トークンの登録は、ポリシーを使用したスマートライセンシングでは必要ありません。トークン生成機能はCSSM でも引き続き使用でき、該当するトポロジの信頼の確立に使用されます。

インサービス ソフトウェア アップグレード

あるリリースから別のリリースにアップグレードする場合、ISSU 方式を使用することで、適用（エンフォースメント）、レポート、および転送の面では通常のアップグレードと同じルールに従います（上記を参照）。

ポリシーを使用したスマートライセンシングに関する追加の考慮事項は適用されません。

ダウングレード

ダウングレードするには、製品インスタンスのソフトウェアバージョンをダウングレードする必要があります。このセクションでは、新規展開のダウングレードについてのみ説明します。

新規展開のダウングレード

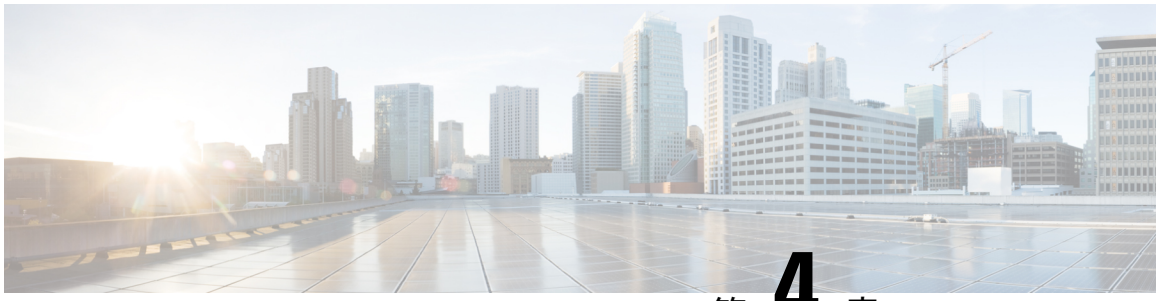
ポリシーを使用したスマートライセンシングがデフォルトですでに有効になっているソフトウェアバージョンで新しく購入した製品インスタンスがあり、ポリシーを使用したスマートライセンシングがサポートされていないソフトウェアバージョンにダウングレードする場合、ダウングレードの結果は、ポリシーを使用したスマートライセンシング環境での操作中に 信頼コード （11 ページ） がインストールされたかどうかによって異なります。

ポリシーを使用したスマートライセンシング環境で実装したトポロジが「CSSMに直接接続」である場合、トポロジ実装の一部として信頼コードが必要であるため、信頼コードのインストールが想定または仮定されます。他のトポロジでは、信頼の確立は必須ではありません。したがって、これらの他のトポロジのいずれかを使用する製品インスタンスをダウングレードすると、スマートライセンシング環境で適用される手順に従って、ライセンスを登録済みおよび承認済みの状態に復元する必要があります。

- ポリシーを使用したスマートライセンシング環境で信頼が確立された場合、製品インスタンスはダウングレード後に CSSM との信頼を更新しようとします。

  更新が正常に完了すると、ライセンスは登録済みの状態になり、以前のバージョンのスマートライセンシングが製品インスタンスで有効になります。

- ポリシーを使用したスマートライセンシング環境で信頼が確立されなかった場合、製品インスタンスのライセンスはダウングレード後に評価モードになり、スマートライセンシングの以前のバージョンが製品インスタンスで有効になります。



第 4 章

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

このセクションでは、サポートされるトポロジを最も簡単かつ迅速に実装するための設定情報を順番に説明します。

トポロジのワークフロー：CSLU を介して CSSM に接続

製品インスタンス開始型通信とCSLU開始型通信のどちらを実装するかに応じて、対応する一連のタスクを実行します。

- 製品インスタンス開始型通信のためのタスク
- CSLU 開始型通信のためのタスク

製品インスタンス開始型通信のためのタスク

CSLU のインストール→CSLU の環境設定→製品インスタンスの設定

1. ***CSLU* のインストール**

   タスクの実行場所：Windows ホスト（ラップトップ、デスクトップ、または仮想マシン（VM））

   『Cisco Smart License Utility Quick Start Setup Guide』を参照してください。

2. ***CSLU* の環境設定**

   タスクの実行場所：CSLU

   1. シスコへのログイン（CSLU インターフェイス） （36 ページ）

2. 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） （36 ページ）
3. 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） （37 ページ）

3. 製品インスタンスの設定

タスクが実行される場所：製品インスタンス

1. 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 （37 ページ）
2. 転送タイプが **cslu** に設定されていることを確認します。

   CSLU がデフォルトの転送タイプです。別のオプションを設定した場合は、グローバル コンフィギュレーション モードで **license smart transport cslu** コマンドを入力します。

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

3. CSLU の検出方法を指定します（1 つ選択）

   - オプション 1：

     アクションは不要です。`cslu-local` のゼロタッチ DNS ディスカバリ。

     ホスト名 `cslu-local` が CSLU の IP アドレス（CSLU をインストールした Windows ホスト）にマッピングされているエントリを使用してネームサーバを設定した場合、設定は不要です。製品インスタンスは、ホスト名 `cslu-local` を自動的に検出します。

   - オプション 2：

     ドメインの DNS ディスカバリを設定します。

     グローバル コンフィギュレーション モードで **ip domain-name** *domain_name* コマンドを入力します。次の例では、ネームサーバはエントリ `cslu-local.example.com` を作成します。

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

   - オプション 3：

     CSLU に特定の URL を設定します。

     グローバル コンフィギュレーション モードで **license smart url cslu** *http://<cslu_ip_or_host>:8182/cslu/v1/pi* コマンドを入力します。`<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。

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

結果：

製品インスタンスは通信を開始すると、ポリシーに従って、スケジュールされた時刻に最初の RUM レポートを自動的に送信します。この最初のレポートとともに、必要に応じて、信頼コード要求を送信します。製品インスタンスがこの情報をいつ送信するかを確認するには、特権 EXEC モードで **show license all** コマンドを入力し、出力で `Next report push:` フィールドの日付を確認します。

CSLU は、情報を CSSM に転送し、返される ACK を製品インスタンスにインストールします。CSSM から ACK を取得し、インストールのために製品インスタンスに送り返します。

CSLU 開始型通信のためのタスク

CSLU のインストール→CSLU の環境設定→製品インスタンスの設定

1. ***CSLU* のインストール**

   タスクの実行場所：Windows ホスト（ラップトップ、デスクトップ、または仮想マシン（VM））

   『Cisco Smart License Utility Quick Start Setup Guide』を参照してください。

2. ***CSLU* の環境設定**

   タスクが実行される場所：製品インスタンス

   1. シスコへのログイン（CSLU インターフェイス） （36 ページ）
   2. 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） （36 ページ）
   3. 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） （39 ページ）
   4. 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） （40 ページ）

3. **製品インスタンスの設定**

   タスクが実行される場所：製品インスタンス

   CSLU 開始型通信のネットワーク到達可能性の確認 （40 ページ）

結果：

CSLU から RUM レポートを収集し、CSSM に送信できるようになりました。それには、[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 CSSM に送信されます。この最初のレポートとともに、必要に応じて、CSLU は信頼コード要求と承認コード要求を CSSM に送信します。CSSM から ACK を取得し、インストールのために製品インスタンスに送り返します。

トポロジのワークフロー：CSSM に直接接続

スマートアカウントのセットアップ→製品インスタンスの設定→CSSMによる信頼の確立→承認コードのインストール（該当する場合のみ）

1. **スマートアカウントのセットアップ**

   タスクが実行される場所：CSSM Web UI、 https://software.cisco.com/

   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ロールがあることを確認します。

2. **製品インスタンスの設定**

   タスクが実行される場所：製品インスタンス

   1. CSSM への製品インスタンス接続の設定： CSSM への接続の設定 （46 ページ）
   2. 接続方法と転送タイプの設定（1 つ選択）

      - オプション 1：

        スマート転送：転送タイプを **smart** に設定し、対応する URL を設定します。

        転送モードが **license smart transport smart** に設定されている場合は、**license smart url default** を設定すると、スマート URL（https://smartreceiver.cisco.com/licservice/license）が自動的に設定されます。

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

      - オプション 2：

        HTTPS プロキシを介したスマート転送：「HTTPS プロキシを介したスマート転送の設定」セクションを参照してください。

      - オプション 3：

        ダイレクトクラウドアクセス用に Call Home サービスを設定します。「ダイレクトクラウドアクセス用の Call Home サービスの設定」セクションを参照してください。

      - オプション 4：

        HTTPS プロキシを介したダイレクトクラウドアクセス用に Call Home サービスを設定します。「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」セクションを参照してください。

3. ***CSSM* との信頼の確立**

   タスクが実行される場所：CSSM Web UI、次に製品インスタンス

1. 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。CSSM からの信頼コード用新規トークンの生成 （56 ページ）
2. トークンをダウンロードしたら、製品インスタンスに信頼コードをインストールできます。信頼コードのインストール （56 ページ）

4. **承認コードのインストール（該当する場合のみ）**

   使用前に承認が必要なライセンスを使用する場合（適用タイプ：適用（エンフォース）または輸出規制）、または（サポートされる製品インスタンスで）250 MB を超えるスループットを設定する場合は、このトポロジの展開を行う前にこの手順を完了する必要があります。SLAC の手動要求と自動インストール （51 ページ）

結果：

信頼を確立した後、CSSMはポリシーを返します。ポリシーは、そのバーチャルアカウントのすべての製品インスタンスに自動的にインストールされます。ポリシーは、製品インスタンスが使用状況をレポートするかどうか、およびその頻度を指定します。

より頻繁にレポートを作成するようにレポート間隔を変更する場合は、製品インスタンスで **license smart usage interval** コマンドを設定します。詳細については、license smart（グローバル コンフィギュレーション） （71 ページ）を参照してください。

トポロジのワークフロー：CSLU は CSSM から切断

製品インスタンス開始型通信またはCSLU開始型通信のどちらの方法を実装するかによって異なります。以下の対応するタスク一覧を実行します。

- 製品インスタンス開始型通信のためのタスク
- CSLU 開始型通信のためのタスク

製品インスタンス開始型通信のためのタスク

CSLU のインストール→CSLU の環境設定→製品インスタンスの設定→ [Download All for Cisco] と [Upload From Cisco]

1. ***CSLU* のインストール**

   タスクの実行場所：Windows ホスト（ラップトップ、デスクトップ、または仮想マシン（VM））

   『Cisco Smart License Utility Quick Start Setup Guide』を参照してください。

2. ***CSLU* の環境設定**

   タスクの実行場所：CSLU

1. CSLU の [Preferences] タブで、[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。
2. 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）（36 ページ）
3. 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）（37 ページ）

3. 製品インスタンスの設定

タスクが実行される場所：製品インスタンス

1. 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（37 ページ）
2. 転送タイプが **cslu** に設定されていることを確認します。

   CSLU がデフォルトの転送タイプです。別のオプションを設定した場合は、グローバル コンフィギュレーション モードで **license smart transport cslu** コマンドを入力します。

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

3. CSLU の検出方法を指定します（1 つ選択）

   - オプション 1：

     No action required.`cslu-local` のゼロタッチ DNS ディスカバリ用に設定されたネームサーバ

     ここでは、DNS を設定してあり（ネームサーバの IP アドレスが製品インスタンスで設定されている）、ホスト名 `cslu-local` が CSLU IP アドレスにマッピングされているエントリが DNS サーバにある場合、それ以上のアクションは不要です。製品インスタンスは、ホスト名 `cslu-local` を自動的に検出します。

   - オプション 2：

     No action required.`cslu-local.<domain>` のゼロタッチ DNS ディスカバリ用に設定されたネームサーバとドメイン

     ここでは、DNS を設定してあり（ネームサーバの IP アドレスとドメインが製品インスタンスで設定されている）、`cslu-local.<domain>` が CSLU IP アドレスにマッピングされているエントリが DNS サーバにある場合、それ以上のアクションは不要です。製品インスタンスは、ホスト名 cslu-local を自動的に検出します。

   - オプション 3：

     CSLU に特定の URL を設定します。

     グローバル コンフィギュレーション モードで **license smart url cslu** *http://<cslu_ip_or_host>:8182/cslu/v1/pi* コマンドを入力します。`<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。

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

4. *[Download All for Cisco] と [Upload From Cisco]*

   タスクの実行場所：CSLU と CSSM

   1. Download All For Cisco（CSLU インターフェイス）（45 ページ）
   2. 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（58 ページ）
   3. Upload From Cisco（CSLU インターフェイス）（46 ページ）

結果：

製品インスタンスは通信を開始すると、ポリシーに従って、スケジュールされた時刻に最初の RUM レポートを自動的に送信します。この最初のレポートとともに、必要に応じて、信頼コード要求を送信します。製品インスタンスがこの情報をいつ送信するかを確認するには、特権 EXEC モードで **show license all** コマンドを入力し、出力で `Next report push:` フィールドの日付を確認します。

CSLU は CSSM から切断されるため、CSLU が製品インスタンスから収集した使用状況データをファイルに保存する必要があります。次に、シスコに接続されているワークステーションからファイルを CSSM にアップロードします。この後、CSSM から ACK をダウンロードします。CSLU がインストールされて製品インスタンスに接続されているワークステーションで、ファイルを CSLU にアップロードします。

CSLU 開始型通信のためのタスク

CSLU のインストール→CSLU の環境設定→製品インスタンスの設定→ [Download All for Cisco] と [Upload From Cisco]

1. ***CSLU* のインストール**

   タスクの実行場所：Windows ホスト（ラップトップ、デスクトップ、または仮想マシン（VM））

   『Cisco Smart License Utility Quick Start Setup Guide』を参照してください。

2. ***CSLU* の環境設定**

   タスクが実行される場所：製品インスタンス

   1. CSLU の [Preferences] タブで、[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。
   2. 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）（36 ページ）
   3. 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）（39 ページ）
   4. 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）（40 ページ）

3. **製品インスタンスの設定**

   タスクが実行される場所：製品インスタンス

   CSLU 開始型通信のネットワーク到達可能性の確認 （40 ページ）

4. ***[Download All for Cisco]* と *[Upload From Cisco]***

   タスクの実行場所：CSLU と CSSM

   1. Download All For Cisco（CSLU インターフェイス） （45 ページ）
   2. 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 （58 ページ）
   3. Upload From Cisco（CSLU インターフェイス） （46 ページ）

結果：

CSLUからRUMレポートを収集し、CSSMに送信できるようになりました。それには、[Actions for Selected] メニューに移動し、[Collect Usage] を選択します。該当する場合、レポートには信頼コード要求と承認コード要求も含まれます。

CSLU は CSSM から切断されるため、CSLU が製品インスタンスから収集した使用状況データをファイルに保存する必要があります。次に、シスコに接続されているワークステーションからファイルをCSSMにアップロードします。この後、CSSMからACKをダウンロードします。CSLU がインストールされて製品インスタンスに接続されているワークステーションで、ファイルを CSLU にアップロードします。

トポロジのワークフロー：CSSM への接続なし、CSLU なし

他のコンポーネントへの接続を設定する必要がないため、トポロジの設定に必要なタスクのリストは短くなります。このトポロジを実装した後に必要な使用状況レポートを作成する方法については、ワークフローの最後にある「結果」セクションを参照してください。

製品インスタンスの設定→承認コードのインストール（該当する場合のみ）

1. **製品インスタンスの設定**

   タスクが実行される場所：製品インスタンス

   転送タイプを**オフ**に設定します。

   グローバル コンフィギュレーション モードで **license smart transport off** コマンドを入力します。

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

2. **承認コードのインストール（該当する場合のみ）**

   タスクが実行される場所：CSSM、次に製品インスタンス

1. 使用前に承認が必要なライセンスを使用する場合（適用タイプ：適用（エンフォースメント）または輸出規制）：CSSM からの SLAC の生成とファイルへのダウンロード（50 ページ）
2. ダウンロードした SLAC 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）

結果：

製品インスタンスとのすべての通信を無効にしているため、ライセンスの使用状況をレポートするには、RUM レポートを（製品インスタンス上の）ファイルに保存してから、CSSM にアップロードする必要があります（インターネットとシスコに接続されているワークステーションから）。

1. RUM レポートの生成と保存

   license smart save usage コマンドを特権 EXEC モードで入力します。次の例では、すべての RUM レポートがファイル `all_rum.txt` で製品インスタンスのフラッシュメモリに保存されます。コマンドシンタックスの詳細については、license smart（特権 EXEC）（77 ページ）コマンドを参照してください。この例では、ファイルはまずブートフラッシュに保存され、次に TFTP の場所にコピーされます。

   ```
   Device# license smart save usage all bootflash:all_rum.txt
   Device# copy bootflash:all_rum.txt tftp://10.8.0.6/all_rum.txt
   ```

2. 使用状況データを CSSM にアップロード：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（58 ページ）
3. ACK を製品インスタンスにインストール：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）

vManage を使用して製品インスタンスを管理するためのワークフロー

製品インスタンスが vManage によって管理される場合：

（注） Cisco vManage はコントローラとしてサポートされていません。また、Cisco SD-WAN コントローラモードで実行されているエッジデバイスは、HSECK9 ライセンスの処理を除き、ポリシーを使用するスマートライセンシングの他の機能をサポートしていません。

- 製品インスタンスは、RUM レポートを生成せず、ライセンス使用状況情報を保存しません。
- 250 MB を超えるスループットが必要な場合は、製品インスタンスに承認コードが必要です。

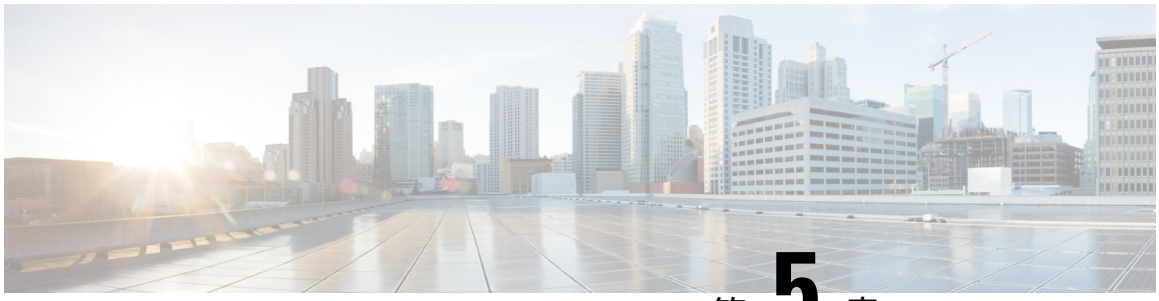
以前のスマートライセンシング環境でインストールされた HSECK9 PAK ライセンスにすることも、ポリシーを使用したスマートライセンシングをサポートするソフトウェアバージョンにアップグレードした後に SLAC をインストールすることもできます。

- 信頼コードは必要ありません。

vManage を使用して製品インスタンスを管理するには、製品インスタンスを「コントローラモード」で動作するように設定する必要があります。ポリシーを使用したスマートライセンシングの観点からは、追加の設定は必要ありません。

使用前に承認が必要なライセンスを使用する場合（適用タイプ：適用（エンフォース）または輸出規制）、または（サポートされる製品インスタンスで）250 MB を超えるスループットが必要な場合は、使用される接続に応じて SLAC のインストールを完了する必要があります。

- CSSM に直接接続、または CSLU を介して CSSM に接続： SLAC の手動要求と自動インストール （51 ページ）
- CSSM への接続なし、CSLU なし：CSSM からの SLAC の生成とファイルへのダウンロード （50 ページ）。



第 5 章

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）（40 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 （58 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） （46 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） （45 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 （63 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-EAEPt9-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 （55 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 （56 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 （59 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 （50 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 （58 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 （58 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（50 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	

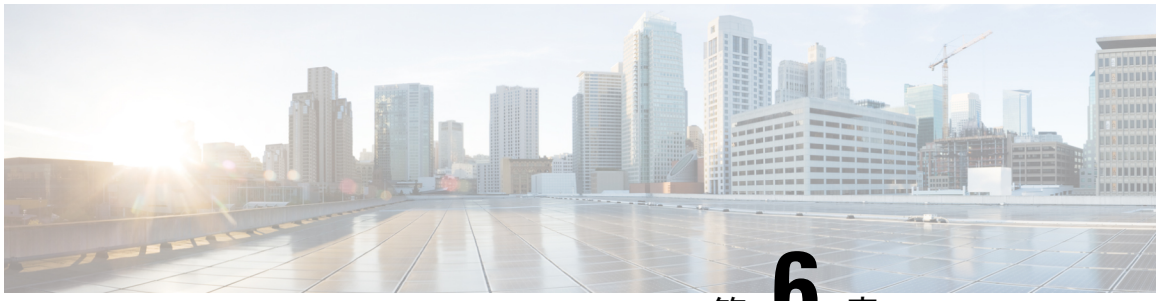
製品ファミリ	**PID**	ライセンス名
	C1121-8PLTEPWE	
	C1121-8PLTEPWB	
	C1121-8PLTEPWZ	
	C1121-8PLTEPWQ	
	C1121-8PLTEP	
	C1121X-8PLTEP	
	C1121-8P	
	C1121X-8P	
	C1161-8P	
	C1161X-8P	
	C1161-8PLTEP	
	C1161X-8PLTEP	
	C1126-8PLTEP	
	C1127-8PLTEP	
	C1127-8PMLTEP	
	C1126X-8PLTEP	
	C1127X-8PLTEP	
	C1127X-8PMLTEP	
	C1128-8PLTEP	
	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	



第 6 章

ポリシーを使用したスマートライセンシングのコマンドリファレンス

ここでは、スマート ライセンシング コマンドの完全なコマンド構文について説明します。

license smart（グローバル コンフィギュレーション）

ライセンス関連の機能を設定するには、グローバル コンフィギュレーション モードで **license smart** コマンドを入力します。デフォルト値に戻すには、コマンドの **no** 形式を使用します。

license smart { **custom_id** *ID* | **enable** | **privacy** { **all** | **hostname** | **version** } | **proxy** { **address** *address_hostname* | **port** *port* } | **reservation** | **server-identity-check** | **transport** { **automatic** | **callhome** | **cslu** | **off** | **smart** } | **url** {*url* | **cslu** *cslu_url* | **default** | **smart** *smart_url* | **utility** *secondary_url* } | **usage** { **customer-tags** { **tag1** | **tag2** | **tag3** | **tag4** }*tag_value* | **interval** *interval_in_days* } | **utility** [**customer_info** { **city** *city* | **country** *country* | **postalcode** *postalcode* | **state** *state* | **street** *street* }] }

no license smart { **custom_id** | **enable** | **privacy** { **all** | **hostname** | **version** } | **proxy** { **address** *address_hostname* | **port** *port* } | **reservation** | **server-identity-check** | **transport** | **url** {*url* | **cslu** *cslu_url* | **default** | **smart** *smart_url* | **utility** *secondary_url* } | **usage** { **customer-tags** { **tag1** | **tag2** | **tag3** | **tag4** }*tag_value* | **interval** *interval_in_days* } | **utility** [**customer_info** { **city** *city* | **country** *country* | **postalcode** *postalcode* | **state** *state* | **street** *street* }] }

構文の説明

custom_id *ID*	このオプションはCLIには表示されますが、サポートされていません。
enable	このキーワードは CLI には表示されますが、設定しても適用されません。スマートライセンシングは常に有効になっています。
privacy { **all**	**hostname**	**version** }	CSSMに送信される使用状況レポートから特定の情報を除外できます。次のオプションから選択します。 • **all**：すべての通信で最小限のライセンス情報のみを送信します。 • **hostname**：通信からホスト名を除外します。 • **version**：通信からスマートエージェントのバージョン情報を除外します。スマートエージェントは、すべての製品インスタンスに存在します。
proxy { **address** *address_hostname*	**port** *port* }	プロキシを設定します。転送モードが **license smart transport smart** または **license smart transport cslu** の場合にのみ、このオプションを使用してプロキシを設定できます。 プロキシが設定されている場合、メッセージは最終宛先URL（CSSM）とともにプロキシに送信されます。プロキシはメッセージをCSSMに送信します。 次のオプションを設定します。 • **address** *address_hostname*：プロキシアドレスを設定します。 *address_hostname* には、プロキシの IP アドレスまたはホスト名を入力します。 • **port***port*：プロキシポートを設定します。 *port* には、プロキシポート番号を入力します。

reservation	ライセンス予約機能を有効または無効にします。 （注） このオプションは、CLI で表示されますが、ライセンスの予約が不要になったため、ポリシーを使用したスマートライセンシングの環境では適用されません。承認コードを要求してインストールするには、代わりに特権 EXEC モードで **license smart authorization request** コマンドを使用します。license smart（特権 EXEC）（77 ページ）を参照してください。
server-identity-check	HTTP セキュアサーバの ID チェックを有効または無効にします。
transport { **automatic** | **callhome** | **cslu** | **off** | **smart** }	製品インスタンスが CSSM との通信に使用する転送モードを設定します。次のオプションから選択します。 • **automatic**：転送モード **cslu** を設定します。 • **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。

url {*url* | **cslu** *cslu_url* | **default** | **smart**
smart_url | **utility** *secondary_url* }

設定された転送モードに使用する URL を設定します。次のオプションから選択します。

- *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。

- **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`

  `<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。

  no license smart url cslu *cslu_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。
usage { **customer-tags** { **tag1** | **tag2** | **tag3** | **tag4** }*tag_value* | **interval** *interval_in_days* }	使用状況レポートの設定を提供します。次のオプションを設定できます。 • **customer-tags**{**tag1** | **tag2** | **tag3** | **tag4**}*tag_value*：テレメトリ用のデータモデルに含める文字列を定義します。最大4つの文字列（またはタグ）を定義できます。 *tag_value* には、定義する各タグの文字列値を入力します。 • **interval** *interval_in_days*：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。 この値をゼロに設定すると、適用されるポリシーの指示に関係なく、RUM レポートは送信されません。これは、CSLUまたはCSSMが受信側にある可能性があるトポロジに適用されます。 ゼロより大きい値を設定し、通信タイプが**オフ**に設定されている場合、*interval_in_days* と `Ongoing reporting frequency(days):` のポリシー値の間で、値の小さい方が適用されます。たとえば、*interval_in_days* が 100 に設定され、ポリシーの値が `Ongoing reporting frequency (days):90` の場合、RUM レポートは 90 日ごとに送信されます。 間隔を設定せず、デフォルトが有効な場合、レポート間隔は完全にポリシー値によって決定されます。たとえば、デフォルト値が有効で、適用されていないライセンスのみが使用されている場合、ポリシーでレポートが不要と記述されていると、RUM レポートは送信されません。
utility [**customer_info** { **city** *city* | **country** *country* | **postalcode** *postalcode* | **state** *state* | **street** *street* }]	このオプションはCLIには表示されますが、サポートされていません。

コマンド デフォルト

Cisco IOS XE Amsterdam 17.3.2 以降、ポリシーを使用したスマートライセンシングはデフォルトで有効になっています。

コマンド モード

Global config (Device(config)#)

コマンド履歴

リリース	変更内容
このコマンドは、Cisco IOS XE Amsterdam 17.3.2 よりも前のリリースで導入されました。	このコマンドが導入されました。
Cisco IOS XE Amsterdam 17.3.2	ポリシーを使用したスマートライセンシングで、次のキーワードと変数が導入されました。 • **url** キーワードの下に、次のオプションが導入されました。 { **cslu** *cslu_url* | **smart** *smart_url* } • **transport** キーワードの下に、次のオプションが導入されました。 { **cslu** | **off** } さらに、デフォルトの通信タイプが **callhome** から **cslu** に変更されました。 • **usage** { **customer-tags** { **tag1** | **tag2** | **tag3** | **tag4** }*tag_value* | **interval** *interval_in_days* } **license smart** コマンドの次のキーワードと変数は廃止され、CLI では使用できなくなりました：**enable**、**conversion automatic**。

license smart（特権 EXEC）

スマートライセンスを管理するには、**license smart** コマンドを特権 EXEC モードで入力します。

license smart { **authorization** { **request** { **add** \| **replace** }*feature_name* { **all** \| **local** } \| **return** { **all** \| **local** } { **offline** [*path*] \| **online** } } \| **clear eventlog** \| **export return** { **all** \| **local** }*feature_name* \| **factory reset** \| **import** *file_path* \| **save** { **trust-request** *filepath_filename* \| **usage** { **all** \| **days** *days* \| **rum-id** *rum-ID* \| **unreported** } { **file** *file_path* } } \| **sync** { **all** \| **local** } \| **trust idtoken** *id_token_value* { **local** \| **all** } [{ **force** }] }

構文の説明

smart	スマートライセンシングのオプションを提供します。
authorization	承認コードを要求する、または承認コードを返却するオプションを提供します。
request	CSSM や CSLU から承認コードを要求し（CSLU は CSSM から承認コードを取得）、製品インスタンスにインストールします。

add	要求されたライセンスを既存の承認コードに追加します。新しい承認コードには、既存の承認コード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	既存の承認コードを置き換えます。新しい承認コードには、要求されたライセンスのみが含まれます。現在の承認コードのすべてのライセンスが返却されます。 このオプションを入力すると、製品インスタンスは、削除される承認コードに対応するライセンスが使用中であるかどうかを確認します。ライセンスが使用されている場合は、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	承認コードを要求するライセンスの名前。
all	高可用性セットアップで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。
return	CSSM のライセンスプールに承認コードを返却します。
offline *file_path*	製品インスタンスが CSSM に接続されていないことを意味します。承認コードはオフラインで返却されます。このオプションでは、戻りコードをファイルに出力する必要があります。 *file_path* には、戻りコードを保存したファイルの場所を指定します。
online	製品インスタンスが接続モードであることを意味します。承認コードは、CSLU や CSSM に直接返されます。
clear eventlog	製品インスタンスからすべてのイベントログファイルをクリアします。
export return	輸出規制ライセンスの承認キーを返却します。
factory reset	製品インスタンスから保存されているすべてのスマートライセンシング情報をクリアします。
import *filepath_filename*	製品インスタンスにファイルをインポートします。ファイルは、承認コード、信頼コード、またはポリシーのファイルである場合があります。 *filepath_filename* には、場所（ファイル名を含む）を指定します。
save	RUM レポートや信頼コード要求を保存するオプションを提供します。
trust-request *filepath_filename*	アクティブな製品インスタンスの信頼コード要求を指定した場所に保存します。 *filepath_filename* には、ファイルの絶対パス（ファイル名を含む）を指定します。

usage { **all** | **days** *days* | **rum-id** *rum-ID* | **unreported** } { **file** *file_path* }	RUM レポート（ライセンス使用状況情報）を指定した場所に保存します。次のいずれかのオプションを指定する必要があります。 • **all**：すべての RUM レポートを保存します。 • **days** *days*：過去 n 日間（現在の日を除く）の RUM レポートを保存します。番号を入力します。有効範囲は 0 ～ 4294967295 です。 たとえば、3 と入力すると、過去 3 日間の RUM レポートが保存されます。 • **rum-Id** *rum-ID*：指定した RUM ID を保存します。値の有効な範囲は 0 ～ 18446744073709551615 です。 • **unreported**：すべての未報告の RUM レポートを保存します。 **file** *filepath_filename*：指定した使用状況情報をファイルに保存します。ファイルの絶対パス（ファイル名を含む）を指定します。
sync { **all** | **local** }	CSLU や CSSM と同期して、保留中のデータを送受信します。これには、保留中の RUM レポートのアップロード、ACK 応答のダウンロード、および製品インスタンスの保留中の承認コード、信頼コード、ポリシーが含まれます。 次のいずれかのオプションを入力して、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すべての製品インスタンスに対して同期を実行します。このオプションを選択すると、製品インスタンスは同期要求内にあるすべての UDI のリストも送信します。 • **local**：要求を送信するアクティブな製品インスタンス、つまり自身の UDI に対してのみ同期を実行します。これがデフォルトのオプションです。
trust idtoken *id_token_value*	CSSM との信頼できる接続を確立します。 このオプションを使用するには、最初に CSSM ポータルでトークンを生成する必要があります。*id_token_value* に生成されたトークン値を指定します。
force	信頼コードが製品インスタンスにすでに存在する場合でも、信頼コード要求を送信します。 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、この動作が上書きされます。

コマンド デフォルト

Cisco IOS XE Amsterdam 17.3.2 以降、ポリシーを使用したスマートライセンシングはデフォルトで有効になっています。

コマンド モード

特権 EXEC（Device#）

コマンド履歴

リリース	変更内容
このコマンドは、Cisco IOS XE Amsterdam 17.3.2 よりも前のリリースで導入されました。	このコマンドが導入されました。
Cisco IOS XE Amsterdam 17.3.2	ポリシーを使用したスマートライセンシングで、次のキーワードと変数が導入されました。 • **authorization** { **request** { **add** | **replace** }*feature_name* { **all** | **local** } | **return** { **all** | **local** } { **offline** [*path*] | **online** } } • **import** *file_path* • **save** { **trust-request** *filepath_filename* | **usage** { **all** | **days** *days* | **rum-id** *rum-ID* | **unreported** } { **file** *file_path* } } • **sync** { **all** | **local** } • **trust idtoken** *id_token_value* { **local** | **all** } [**force**] **license smart** コマンドの次のキーワードと変数は廃止され、CLI では使用できなくなりました。 • **register idtoken** *token_id* [**force**] • **renew id** { **ID** | **auth** } • **debug** { **error** | **debug** | **trace** | **all** } • **mfg reservation** { **request** | **install** | **install file** | **cancel** } • **conversion** { **start** | **stop** }

使用上のガイドライン

ポリシーを使用したスマートライセンシングはデフォルトで有効になっています。特権 EXEC モードで **license smart** コマンドの **no** 形式は使用できません。

licence smart factory reset を入力すると、承認コードや RUM レポートなど、すべてのスマートライセンシング情報が製品インスタンスから削除されます。そのため、このコマンドは、製品インスタンスが返却される場合（Return Material Authorization（RMA））、または永続的にデコミッションされる場合にのみ使用することを推奨します。また、ライセンス情報が製品インスタンスから削除される前に CSSM に RUM レポートを送信して、CSSM に最新の使用状況情報を含めることをお勧めします。

例

• 例：Cisco 4000 シリーズ サービス統合型ルータにインストールされた SLAC （81 ページ）
• 例：Cisco 4000 シリーズ サービス統合型ルータで返却された SLAC （81 ページ）

例：Cisco 4000 シリーズ サービス統合型ルータにインストールされた SLAC

license smart authorization request add コマンドの次の出力例は、Cisco 4000 シリーズ サービス統合型ルータで SLAC が要求され、自動的にインストールされる方法を示しています。**show license authorization** に、インストール後の出力例を示します。

```
Device# license smart authorization request add hseck9 all
*Sep 23 17:41:10.938: %SMART_LIC-6-AUTHORIZATION_INSTALL_SUCCESS: A new licensing
authorization code
was successfully installed on PID:ISR4331/K9,SN:FDO224917Q6
*Sep 23 17:41:12.929: %SMART_LIC-6-POLICY_INSTALL_SUCCESS: A new licensing policy was
successfully
installed
```

```
Device# show license authorization
Overall status:
  Active: PID:ISR4331/K9,SN:FDO224917Q6
Status: SMART AUTHORIZATION INSTALLED on Sep 23 17:41:10 2020 UTC
      Last Confirmation code: 5fd33d79

Authorizations:
  ISR_4331_Hsec (ISR_4331_Hsec):
    Description: U.S. Export Restriction Compliance license for 4330 series
    Total available count: 1
    Enforcement type: EXPORT RESTRICTED
    Term information:
      Active: PID:ISR4331/K9,SN:FDO224917Q6
        Authorization type: SMART AUTHORIZATION INSTALLED
        License type: PERPETUAL
          Term Count: 1

Purchased Licenses:
  No Purchase Information Available
```

例：Cisco 4000 シリーズ サービス統合型ルータで返却された SLAC

license smart authorization return コマンドの次の出力例は、Cisco 4000 シリーズ サービス統合型ルータで SLAC がオンラインで返却される方法を示しています（オフラインで返却された場合は、ここに表示される戻りコードを返す必要があるため、CSSM に戻りコードを手動で入力します）。

```
Device# license smart authorization return all online

Enter this return code in Cisco Smart Software Manager portal:
UDI: PID:ISR4331/K9,SN:FDO224917Q6
    Return code: CPo1Sb-CHc1jc-dFu2Fj-R9qkZc-V46wAG-7KWxKB-8vmQgp-4xZAE4-BAS
*Sep 23 17:46:12.284: %SMART_LIC-6-AUTHORIZATION_REMOVED: A licensing authorization code
 has been removed from PID:ISR4331/K9,SN:FDO224917Q6.
```

show license all

すべてのライセンス情報を表示するには、特権 EXEC モードで **show license all** コマンドを入力します。このコマンドは、ステータス、承認、UDI、および使用状況の情報をすべて組み合わせて表示します。

show license all

このコマンドには引数またはキーワードはありません。

コマンド モード

特権 EXEC（Device#）

コマンド履歴

リリース	変更内容
このコマンドは、Cisco IOS XE Amsterdam 17.3.2 よりも前のリリースで導入されました。	このコマンドが導入されました。
Cisco IOS XE Amsterdam 17.3.2	コマンド出力が更新され、ポリシーを使用したスマートライセンシングに関する情報が表示されるようになりました。 コマンド出力にスマートアカウントとバーチャルアカウントの情報が表示されなくなりました。

show license all（Cisco 4000 シリーズ サービス統合型ルータ）

次に、**show license all** コマンドの出力例を示します。

```
Device# show license all

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

Smart Licensing is ENABLED
License Reservation is ENABLED

Registration:
  Status: REGISTERED - SPECIFIC LICENSE RESERVATION
  Export-Controlled Functionality: ALLOWED
  Initial Registration: SUCCEEDED on Sep 23 22:08:22 2020 UTC

License Authorization:
  Status: AUTHORIZED - RESERVED on Sep 23 22:08:22 2020 UTC

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

Export Authorization Key:
  Features Authorized:
    <none>

Utility:
```

```
  Status: DISABLED

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

Transport:
  Type: Callhome

Miscellaneus:
  Custom Id: <empty>

License Usage
==============

ISR_4400_Application (ISR_4400_Application):
  Description: AppX License for Cisco ISR 4400 Series
  Count: 1
  Version: 1.0
  Status: AUTHORIZED
  Export status: NOT RESTRICTED
  Reservation:
    Reservation status: SPECIFIC INSTALLED
    Total reserved count: 1

ISR_4400_UnifiedCommunication (ISR_4400_UnifiedCommunication):
  Description: Unified Communications License for Cisco ISR 4400 Series
  Count: 1
  Version: 1.0
  Status: AUTHORIZED
  Export status: NOT RESTRICTED
  Reservation:
    Reservation status: SPECIFIC INSTALLED
    Total reserved count: 1

ISR_4400_Security (ISR_4400_Security):
  Description: Security License for Cisco ISR 4400 Series
  Count: 1
  Version: 1.0
  Status: AUTHORIZED
  Export status: NOT RESTRICTED
  Reservation:
    Reservation status: SPECIFIC INSTALLED
    Total reserved count: 1

ISR_4431_1G_Performance (ISR_4431_1G_Performance):
  Description: Performance on Demand License for 4430 Series
  Count: 1
  Version: 1.0
  Status: AUTHORIZED
  Export status: NOT RESTRICTED
  Reservation:
    Reservation status: SPECIFIC INSTALLED
    Total reserved count: 1

hseck9 (ISR_4400_Hsec):
  Description: Export Controlled Feature hseck9
  Count: 1
  Version: 1.0
  Status: AUTHORIZED
  Export status: RESTRICTED - ALLOWED
  Feature Name: hseck9
```

```
  Feature Description: Export Controlled Feature hseck9
  Reservation:
    Reservation status: SPECIFIC EXPORT AUTHORIZATION KEY INSTALLED
    Total reserved count: UNLIMITED

Product Information
===================
UDI: PID:ISR4431/K9,SN:FOC21030CHG

Agent Version
=============
Smart Agent for Licensing: 4.11.5_rel/41

Reservation Info
================
License reservation: ENABLED

Overall status:
  Active: PID:ISR4431/K9,SN:FOC21030CHG
      Reservation status: SPECIFIC INSTALLED on Sep 23 22:08:22 2020 UTC
      Export-Controlled Functionality: ALLOWED
      Last Confirmation code: ea24d89a

Specified license reservations:
  ISR_4400_Application (ISR_4400_Application):
    Description: AppX License for Cisco ISR 4400 Series
    Total reserved count: 1
    Term information:
      Active: PID:ISR4431/K9,SN:FOC21030CHG
        License type: PERPETUAL
          Term Count: 1
  ISR_4400_Hsec (ISR_4400_Hsec):
    Description: U.S. Export Restriction Compliance license for 4400 series
    Total reserved count: 1
    Term information:
      Active: PID:ISR4431/K9,SN:FOC21030CHG
        License type: PERPETUAL
          Term Count: 1
  ISR_4400_Security (ISR_4400_Security):
    Description: Security License for Cisco ISR 4400 Series
    Total reserved count: 1
    Term information:
      Active: PID:ISR4431/K9,SN:FOC21030CHG
        License type: PERPETUAL
          Term Count: 1
  ISR_4400_UnifiedCommunication (ISR_4400_UnifiedCommunication):
    Description: Unified Communications License for Cisco ISR 4400 Series
    Total reserved count: 1
    Term information:
      Active: PID:ISR4431/K9,SN:FOC21030CHG
        License type: PERPETUAL
          Term Count: 1
  ISR_4431_1G_Performance (ISR_4431_1G_Performance):
    Description: Performance on Demand License for 4430 Series
    Total reserved count: 1
    Term information:
      Active: PID:ISR4431/K9,SN:FOC21030CHG
        License type: PERPETUAL
          Term Count: 1
```

show license authorization

ライセンス（輸出規制および適用）の承認関連情報を表示するには、特権EXECモードで**show license authorization** コマンドを入力します。

show license authorization

このコマンドには引数またはキーワードはありません。

コマンド モード

特権 EXEC（Device#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Amsterdam 17.3.2	このコマンドが導入されました。

例

次に、さまざまなシスコ製品インスタンスでの **show license authorization** コマンドの出力例を示します。ディスプレイに表示されるフィールドについては、表 4 : show license authorization のフィールドの説明 （86 ページ）を参照してください。

- Cisco 4000 シリーズ サービス統合型ルータにおける HSECK9 （89 ページ）

表 *4 : show license authorization* のフィールドの説明

フィールド		説明
Overall Status	設定内にあるすべての製品インスタンスの UDI 情報のヘッダー、インストールされている承認のタイプ、および設定エラー（存在する場合）。 高可用性セットアップでは、設定内にあるすべての UDI がリストされます。	
	Active: ステータス：	アクティブ製品インスタンス UDI と、それに続いてこの UDI の承認コードインストールのステータス。 承認コードがインストールされていることを示すステータスであり、確認コードがある場合は、これも表示されます。
	Standby: ステータス：	スタンバイ製品インスタンス UDI と、それに続いてこの UDI の承認コードインストールのステータス。 承認コードがインストールされていることを示すステータスであり、確認コードがある場合は、これも表示されます。
	Member: ステータス：	メンバー製品インスタンス UDI と、それに続いてこの UDI の承認コードインストールのステータス。 承認コードがインストールされていることを示すステータスであり、確認コードがある場合は、これも表示されます。
	ERROR:	高可用性セットアップの設定エラーまたは不一致（存在する場合）。

フィールド		説明
承認	詳細なライセンス承認情報のヘッダー。すべてのライセンス、その適用タイプ、および有効期間が表示されます。承認またはモードがアクティブにインストールされているものと一致しない場合、製品インスタンスごとにエラーが表示されます。 このセクションは、製品インスタンスがSLAC、SLR、PAK、RTU のいずれかの承認コードを必要とするライセンスを使用している場合にのみ表示されます。製品インスタンスに PLR 承認コードがインストールされている場合、このセクションは表示されません。	
	():	ライセンス名およびライセンス名の短縮形。
	Description	ライセンスの説明。
	Total available count:	使用可能なライセンスの合計数。 これには、高可用性セットアップのすべての製品インスタンスに関して、期限切れのサブスクリプション ライセンスを含む、すべての期間のライセンス（永久ライセンスおよびサブスクリプション）が含まれます。
	Enforcement type	ライセンスの適用タイプ。これは、次のいずれかです。 • 適用 • 非適用 • 輸出規制 適用タイプの詳細については、ライセンス執行（エンフォースメント）タイプ （8 ページ） を参照してください。
	Term information:	

フィールド		説明
		ライセンス期間情報を提供するヘッダー。このヘッダーには、次のフィールドが含まれることがあります。 • Active：アクティブ製品インスタンス UDI と、それに続いてこの UDI の承認コードインストールのステータス。 • Authorization type：インストールされている承認コードのタイプとインストール日。タイプは、SLAC、UNIVERSAL、SPECIFIED、PAK、RTU です。 • Start Date：ライセンスが特定の期間または時間の場合に、有効期間の開始日を表示します。 • Start Date：ライセンスが特定の期間または時間の場合に、有効期間の終了日を表示します。 • Term Count：ライセンス数。 • Subscription ID：ライセンスが特定の期間または時間の場合に、ID を表示します。 • License type：ライセンス継続期間。これは、SUBSCRIPTION または PERPETUAL です。 • Standby：スタンバイ製品インスタンス UDI と、それに続いてこの UDI の承認コードインストールのステータス。

フィールド		説明
		• Member：メンバー製品インスタンス UDI と、それに続いてこの UDI の承認コードインストールのステータス。 ライセンスの有効期間の詳細については、ライセンス継続期間 （9 ページ） を参照してください。
Purchased Licenses	ライセンス購入情報のヘッダー。	
	Active:	アクティブ製品インスタンスとその UDI。
	Count:	ライセンス数。
	Description:	ライセンスの説明。
	License type:	ライセンス継続期間。これは、SUBSCRIPTION または PERPETUAL です。
	Standby:	スタンバイ製品インスタンスの UDI。
	Member:	メンバー製品インスタンスの UDI。

Cisco 4000 シリーズ サービス統合型ルータにおける HSECK9

次の **show license authorization** コマンドの出力例は、Cisco 4000 シリーズ サービス統合型ルータに SLAC がインストールされた輸出規制ライセンス（HSECK9）を示しています。

```
Device# show license authorization

Overall status:
  Active: PID:ISR4331/K9,SN:FDO224917Q6
Status: SMART AUTHORIZATION INSTALLED on Sep 23 17:41:10 2020 UTC
      Last Confirmation code: 5fd33d79

Authorizations:
  ISR_4331_Hsec (ISR_4331_Hsec):
    Description: U.S. Export Restriction Compliance license for 4330 series
    Total available count: 1
    Enforcement type: EXPORT RESTRICTED
    Term information:
      Active: PID:ISR4331/K9,SN:FDO224917Q6
```

```
          Authorization type: SMART AUTHORIZATION INSTALLED
          License type: PERPETUAL
            Term Count: 1

Purchased Licenses:
  No Purchase Information Available
```

show license data

ライセンスデータ変換情報を表示するには、特権 EXEC モードで **show license data** コマンドを入力します。

show license data　conversion

構文の説明

conversion	ライセンス変換に関する情報を表示します。

コマンド モード

特権 EXEC（Device#）

コマンド履歴

リリース	変更内容
このコマンドは、Cisco IOS XE Amsterdam 17.3.2 よりも前のリリースで導入されました。	このコマンドが導入されました。

show license data translation

次に、**show license data conversion** コマンドの出力例を示します。

```
Device# show license data conversion
Smart Licensing Data - Conversion
================================
```

show license eventlog

ポリシーを使用したスマートライセンシングに関連するイベントログを表示するには、特権 EXEC モードで **show license eventlog** コマンドを入力します。

show license eventlog　[*days*]

構文の説明

days	イベントログを表示する日数を入力します。0 ～ 2147483647 の範囲の値を指定できます。

コマンド モード

特権 EXEC（Device#）

コマンド履歴

リリース	変更内容
このコマンドは、Cisco IOS XE Amsterdam 17.3.2 よりも前のリリースで導入されました。	このコマンドが導入されました。
Cisco IOS XE Amsterdam 17.3.2	ポリシーを使用したスマートライセンシングの導入により、次のイベントが追加されました。 • ポリシーのインストールと削除。 • 承認コードの要求、インストール、および削除。 • 信頼コードのインストールと削除。 • ライセンス使用状況に関する承認ソース情報の追加。

例

• 例：1 日分のイベントログ （91 ページ）
• 例：すべてのイベントログ （92 ページ）

例：1 日分のイベントログ

次に、**show license eventlog** コマンドの出力例を示します。このコマンドは、1 日分のイベントを表示するように設定されています。

```
Device# show license eventlog 1

Load for five secs: 0%/0%; one minute: 0%; five minutes: 0%
No time source, 12:50:20.640 EDT Fri Sep 11 2020

**** Event Log ****

2020-09-11 00:50:17.693 EDT SAEVT_PLATFORM eventSource="INFRA_SL"
eventName="INFRA_SL_EVLOG_ERM_RESET" MSG="ERM-Reset: Client 0, AP-GROUP group, 2 features
 air-network-advantage,air-dna-advantage"
2020-09-11 00:50:17.695 EDT SAEVT_ENDPOINT_USAGE count="0"
entitlementTag="regid.2018-06.com.cisco.DNA_NWStack,1.0_e7244e71-3ad5-4608-8bf0-d12f67c80896"
2020-09-11 00:50:17.695 EDT SAEVT_ENDPOINT_USAGE count="0"
entitlementTag="regid.2017-08.com.cisco.AIR-DNA-A,1.0_b6308627-3ab0-4a11-a3d9-586911a0d790"
2020-09-11 00:50:50.175 EDT SAEVT_POLL_MESSAGE messageType="LICENSE_USAGE"
2020-09-11 08:50:17.694 EDT SAEVT_PLATFORM eventSource="INFRA_SL"
eventName="INFRA_SL_EVLOG_ERM_RESET" MSG="ERM-Reset: Client 0, AP-GROUP group, 2 features
 air-network-advantage,air-dna-advantage"
2020-09-11 08:50:17.696 EDT SAEVT_ENDPOINT_USAGE count="0"
entitlementTag="regid.2018-06.com.cisco.DNA_NWStack,1.0_e7244e71-3ad5-4608-8bf0-d12f67c80896"
2020-09-11 08:50:17.696 EDT SAEVT_ENDPOINT_USAGE count="0"
entitlementTag="regid.2017-08.com.cisco.AIR-DNA-A,1.0_b6308627-3ab0-4a11-a3d9-586911a0d790"
2020-09-11 08:50:52.804 EDT SAEVT_POLL_MESSAGE messageType="LICENSE_USAGE"
```

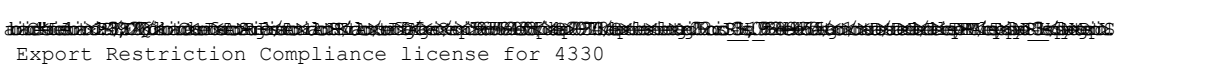
例：すべてのイベントログ

次に、**show license eventlog** コマンドの出力例を示します。このコマンドは、すべてのイベントを表示するように設定されています。

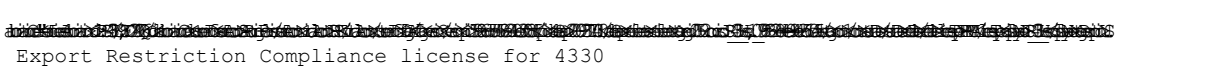
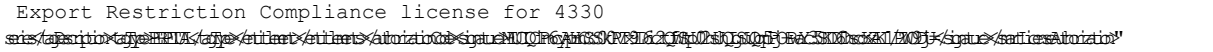
```
Device# show license eventlog
**** Event Log ****

2020-09-22 20:23:27.699 UTC SAEVT_INIT_START version="4.13.23_rel/62"
2020-09-22 20:23:27.701 UTC SAEVT_INIT_CRYPTO success="False" error="Crypto Initialization
 has not been completed"
2020-09-22 20:23:27.702 UTC SAEVT_HA_EVENT eventType="SmartAgentEvtHArmfRegister"
2020-09-22 20:23:32.840 UTC SAEVT_READY
2020-09-22 20:23:32.841 UTC SAEVT_ENABLED
2020-09-22 20:23:33.455 UTC SAEVT_EXPORT_FLAG exportAllowed="False"
2020-09-22 20:23:35.806 UTC SAEVT_HA_EVENT eventType="SmartAgentEvtHArmfInitialize"
2020-09-22 20:23:35.815 UTC SAEVT_HA_CHASSIS_ROLE udi="PID:ISR4331/K9,SN:FDO224917Q6"
2020-09-22 20:23:35.816 UTC SAEVT_HA_EVENT eventType="SmartAgentEvtHAchkptRegister"
2020-09-22 20:23:49.682 UTC SAEVT_HA_ROLE udi="PID:ISR4331/K9,SN:FDO224917Q6"
haRole="Active"
2020-09-22 20:23:49.735 UTC SAEVT_HA_CHASSIS_ROLE udi="PID:ISR4331/K9,SN:FDO224917Q6"
haRole="Active"
2020-09-22 20:23:49.737 UTC SAEVT_HA_ROLE udi="PID:ISR4331/K9,SN:FDO224917Q6"
haRole="Active"
2020-09-22 20:23:50.043 UTC SAEVT_INIT_CONFIG_READ_BEGIN
2020-09-22 20:23:54.353 UTC SAEVT_INIT_CONFIG_READ_DONE
2020-09-22 20:23:55.112 UTC SAEVT_INIT_SYSTEM_INIT
2020-09-22 20:23:56.114 UTC SAEVT_INIT_CRYPTO success="False" error="Crypto Initialization
 has not been completed"
2020-09-22 20:24:26.120 UTC SAEVT_INIT_CRYPTO success="True"
2020-09-22 20:24:26.133 UTC SAEVT_COMM_RESTORED
2020-09-22 20:24:26.402 UTC SAEVT_INIT_COMPLETE
2020-09-22 20:25:26.132 UTC SAEVT_PRIVACY_CHANGED enabled="True"
2020-09-22 20:31:34.912 UTC SAEVT_HOSTNAME_CHANGE
2020-09-22 20:35:30.873 UTC SAEVT_CONFIG_PERSISTED
2020-09-22 20:39:27.795 UTC SAEVT_INIT_START version="4.13.23_rel/62"
2020-09-22 20:39:27.798 UTC SAEVT_INIT_CRYPTO success="False" error="Crypto Initialization
 has not been completed"
2020-09-22 20:39:27.798 UTC SAEVT_HA_EVENT eventType="SmartAgentEvtHArmfRegister"
2020-09-22 20:39:33.333 UTC SAEVT_READY
2020-09-22 20:39:33.334 UTC SAEVT_ENABLED
2020-09-22 20:39:33.914 UTC SAEVT_EXPORT_FLAG exportAllowed="False"
2020-09-22 20:39:36.300 UTC SAEVT_HA_EVENT eventType="SmartAgentEvtHArmfInitialize"
2020-09-22 20:39:36.311 UTC SAEVT_HA_CHASSIS_ROLE udi="PID:ISR4331/K9,SN:FDO224917Q6"
2020-09-22 20:39:36.312 UTC SAEVT_HA_EVENT eventType="SmartAgentEvtHAchkptRegister"
2020-09-22 20:39:52.391 UTC SAEVT_TAG_EXPORT exportAllowed="False" count="0"
entitlementTag="regid.2015-02.com.cisco.ISR_4331_Hsec,1.0_7998f136-248d-4ee9-94be-2b561c04a51e"
2020-09-22 20:39:53.058 UTC SAEVT_HA_ROLE udi="PID:ISR4331/K9,SN:FDO224917Q6"
haRole="Active"
2020-09-22 20:39:53.300 UTC SAEVT_HA_CHASSIS_ROLE udi="PID:ISR4331/K9,SN:FDO224917Q6"
haRole="Active"
2020-09-22 20:39:53.300 UTC SAEVT_HA_ROLE udi="PID:ISR4331/K9,SN:FDO224917Q6"
haRole="Active"
2020-09-22 20:39:55.146 UTC SAEVT_INIT_CONFIG_READ_BEGIN
2020-09-22 20:40:01.700 UTC SAEVT_TAG_AUTHORIZED count="1"
entitlementTag="regid.2017-05.com.cisco.ISR_4331_BOOST,1.0_d5ca3d93-a3a9-480d-98f7-c7b06ddcc973"
2020-09-22 20:40:01.704 UTC SAEVT_HOSTNAME_CHANGE
2020-09-22 20:40:02.140 UTC SAEVT_TAG_AUTHORIZED count="1"
entitlementTag="regid.2015-01.com.cisco.ISR_4331_Application,1.0_4dd5e243-4754-4fed-b8aa-cdd9ff0e82c0"
2020-09-22 20:40:02.142 UTC SAEVT_PLATFORM eventSource="INFRA_SL"
eventName="INFRA_SL_EVLOG_LICENSE_REQUEST" MSG="License appxk9, dev ISR4331, count 1,
reslt 0, alt 0"
```

```
2020-09-22 20:40:02.374 UTC SAEVT_TAG_AUTHORIZED count="1"
entitlementTag="regid.2014-12.com.cisco.ISR_4331_UnifiedCommunication,1.0_fc59e79d-8a80-469b-b1fb-0307e6e76108"
2020-09-22 20:40:02.376 UTC SAEVT_PLATFORM eventSource="INFRA_SL"
eventName="INFRA_SL_EVLOG_LICENSE_REQUEST" MSG="License uck9, dev ISR4331, count 1, reslt
 0, alt 0"
2020-09-22 20:40:02.608 UTC SAEVT_TAG_AUTHORIZED count="1"
entitlementTag="regid.2014-12.com.cisco.ISR_4331_Security,1.0_dba7c7eb-f2b3-4824-9690-10e46d998fa5"
2020-09-22 20:40:02.610 UTC SAEVT_PLATFORM eventSource="INFRA_SL"
eventName="INFRA_SL_EVLOG_LICENSE_REQUEST" MSG="License securityk9, dev ISR4331, count
1, reslt 0, alt 0"
2020-09-22 20:40:02.651 UTC SAEVT_INIT_CONFIG_READ_DONE
2020-09-22 20:40:03.445 UTC SAEVT_INIT_SYSTEM_INIT
2020-09-22 20:40:04.456 UTC SAEVT_INIT_CRYPTO success="False" error="Crypto Initialization
 has not been completed"
2020-09-22 20:40:34.458 UTC SAEVT_INIT_CRYPTO success="True"
2020-09-22 20:40:34.461 UTC SAEVT_COMM_RESTORED
2020-09-22 20:40:34.739 UTC SAEVT_INIT_COMPLETE
2020-09-22 20:41:34.459 UTC SAEVT_PRIVACY_CHANGED enabled="True"
2020-09-22 20:41:39.216 UTC SAEVT_INIT_CRYPTO success="True"
2020-09-22 20:42:35.750 UTC SAEVT_UTILITY_REPORT_START
2020-09-22 20:42:36.725 UTC SAEVT_UTILITY_RUM_FAIL error="[CSSM_ACCOUNT_ACCESS_DENIED]
Smart Account access denied, user has no permission."
2020-09-22 21:33:20.102 UTC SAEVT_UTILITY_RUM_FAIL error="[ERROR_CSSMCONN_PING_ERR] CSLU
 could not connect to the Cisco network. Please check your network settings."
2020-09-22 21:36:21.869 UTC SAEVT_POLL_MESSAGE messageType="LICENSE_USAGE"
2020-09-23 00:07:15.577 UTC SAEVT_UTILITY_RUM_FAIL error="[ERROR_CSSMCONN_API] CSSM
connector API failed"
2020-09-23 06:25:36.828 UTC SAEVT_POLL_MESSAGE messageType="LICENSE_USAGE"
2020-09-23 16:23:05.822 UTC SAEVT_POLL_MESSAGE messageType="LICENSE_USAGE"
2020-09-23 16:31:11.018 UTC SAEVT_POLL_MESSAGE messageType="LICENSE_USAGE"
2020-09-23 17:41:10.921 UTC SAEVT_RESERVE_INSTALL_START udi="PID:ISR4331/K9,SN:FDO224917Q6"


 Export Restriction Compliance license for 4330

2020-09-23 17:41:10.937 UTC SAEVT_TAG_EXPORT exportAllowed="False" count="0"
entitlementTag="regid.2015-02.com.cisco.ISR_4331_Hsec,1.0_7998f136-248d-4ee9-94be-2b561c04a51e"
2020-09-23 17:41:10.965 UTC SAEVT_TAG_EXPORT exportAllowed="True" count="0"
entitlementTag="regid.2015-02.com.cisco.ISR_4331_Hsec,1.0_7998f136-248d-4ee9-94be-2b561c04a51e"
2020-09-23 17:41:11.965 UTC SAEVT_STATE_RESERVE_AUTHORIZED
2020-09-23 17:46:12.269 UTC SAEVT_RESERVE_RETURN_START udi="PID:ISR4331/K9,SN:FDO224917Q6"


 Export Restriction Compliance license for 4330

2020-09-23 17:46:12.283 UTC SAEVT_TAG_EXPORT exportAllowed="False" count="0"
entitlementTag="regid.2015-02.com.cisco.ISR_4331_Hsec,1.0_7998f136-248d-4ee9-94be-2b561c04a51e"
```

show license history message

製品インスタンスとCSSMまたはCSLU（該当する場合）の間の通信履歴を表示するには、特権EXECモードで **show license history message** コマンドを入力します。このコマンドの出力は、テクニカルサポートチームがトラブルシューティングに使用します。

show license history message

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド モード

特権 EXEC（Device#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Amsterdam 17.3.2	このコマンドが導入されました。

使用上のガイドライン

解決できないエラーメッセージが表示された場合は、コンソールまたはシステムログに表示されるメッセージともに、シスコのテクニカルサポート担当者に **show license tech support**、**show license history message**、および **show platform software sl-infra** 特権 EXEC コマンドの出力例を提供してください。

show license reservation

ライセンス予約情報を表示するには、特権 EXEC モードで **show license reservation** コマンドを入力します。

（注） Cisco IOS XE Amsterdam 17.3.2 以降では、**show license reservation** の代わりに **show license authorization** コマンドを使用して、使用前に承認が必要なライセンスの情報を表示します。

show license reservation

このコマンドには引数またはキーワードはありません。

コマンド モード

特権 EXEC（Device#）

コマンド履歴

リリース	変更内容
このコマンドは、Cisco IOS XE Amsterdam 17.3.2 よりも前のリリースで導入されました。	このコマンドが導入されました。
Cisco IOS XE Amsterdam 17.3.2	コマンドは引き続き使用できますが、ポリシーを使用したスマートライセンシングの導入により、SLR および PLR ライセンスには適用されなくなりました。代わりに、特権 EXEC モードで **show license authorization** コマンドを使用してください。

show license status

ライセンスステータス情報を表示するには、特権 EXEC モードで **show license status** コマンドを入力します。

show license status

コマンド モード

特権 EXEC（Device#）

コマンド履歴

リリース	変更内容
このコマンドは、Cisco IOS XE Amsterdam 17.3.2 よりも前のリリースで導入されました。	このコマンドが導入されました。
Cisco IOS XE Amsterdam 17.3.2	コマンド出力が更新され、ポリシーを使用したスマートライセンシングに適用可能な新しいフィールドが反映されました。これには、`Trust code installed:`、`Policy in use`、`Policy name:` 、ポリシーと同様のレポート要件（`Attributes:`）および使用状況レポートに関連するフィールドが含まれます。 コマンド出力にスマートアカウントとバーチャルアカウントの情報が表示されなくなりました。

例

次に、さまざまなシスコ製品インスタンスでの **show license status** コマンドの出力例を示します。ディスプレイに表示されるフィールドについては、表 5 : show license status のフィールドの説明 （96 ページ）を参照してください。

- 例：Cisco 4000 シリーズ サービス統合型ルータでの show license status （103 ページ）

表 *5 : show license status* のフィールドの説明

フィールド		説明
Utility	製品インスタンスで設定されているユーティリティ設定のヘッダー。	
	Status:	ステータス
	Utility report:	最後の試行結果：
	Customer Information:	次のフィールドが表示されます。 • ID: • Name: • Street • City: • State: • Country: • Postal Code:
SLE Policy:	製品インスタンスのポリシー設定のヘッダー。	
	Status:	ポリシーを使用したスマートライセンシングが有効になっているかどうかを示します。 ポリシーを使用したスマートライセンシングは、Cisco IOS XE Amsterdam 17.3.2 以降でサポートされ、サポートされているソフトウェアイメージでは常に有効になっています。

フィールド		説明
Data Privacy:	製品インスタンスで設定されているプライバシー設定のヘッダー。	
	Sending Hostname:	ホスト名が使用状況レポートで送信されるかどうかを示す *yes* または *no* の値。
	Callhome hostname privacy:	Call Home 機能がレポートの転送モードとして設定されているかどうかを示します。設定されている場合、次のいずれかの値が表示されます。 • ENABLED • DISABLED
	Smart Licensing hostname privacy:	次のいずれかの値が表示されます。 • ENABLED • DISABLED
	Version privacy:	次のいずれかの値が表示されます。 • ENABLED • DISABLED
Transport:	製品インスタンスで設定されているトランスポート設定のヘッダー。	
	Type:	使用中の転送モード。 特定の転送モードでは、追加のフィールドが表示されます。たとえば、通信タイプが CSLU に設定されている場合、CSLU アドレスも表示されます。

フィールド		説明
Policy:	製品インスタンスに適用されるポリシー情報のヘッダー。	
	Policy in use:	適用されるポリシー。 これは、Cisco default、Product default、Permanent License Reservation、Specific License Reservation、PAK license、Installed on <date>、Controller のいずれかです。
	Policy name:	ポリシーの名前。
	Reporting ACK required:	この製品インスタンスのレポートに CSSM 確認応答（ACK）が必要かどうかを指定する *yes* または *no* の値。デフォルトポリシーは常に「yes」に設定されます。
	Perpetual Attributes	永久ライセンスのポリシー値。 • 最初のレポート要件（日）：最初のレポートを送信するまでに使用可能な最大時間。その後にポリシー名が続きます。 • レポート頻度（日）：次のレポートを送信するまでに使用可能な最大時間。その後にポリシー名が続きます。 • 変化レポート（日）：ライセンスの使用状況が変化した場合にレポートを送信できる最大時間。その後にポリシー名が続きます。
	Subscription Attributes:	

フィールド		説明
		サブスクリプション ライセンスのポリシー値。 • 最初のレポート要件（日）：最初のレポートを送信するまでに使用可能な最大時間。その後にポリシー名が続きます。 • レポート頻度（日）：次のレポートを送信するまでに使用可能な最大時間。その後にポリシー名が続きます。 • 変化レポート（日）：ライセンスの使用状況が変化した場合にレポートを送信できる最大時間。その後にポリシー名が続きます。
	Enforced License Attributes:	サブスクリプション ライセンスのポリシー値。 • 最初のレポート要件（日）：最初のレポートを送信するまでに使用可能な最大時間。その後にポリシー名が続きます。 • レポート頻度（日）：次のレポートを送信するまでに使用可能な最大時間。その後にポリシー名が続きます。 • 変化レポート（日）：ライセンスの使用状況が変化した場合にレポートを送信できる最大時間。その後にポリシー名が続きます。
	Export License Attributes:	

フィールド		説明
		サブスクリプション ライセンスのポリシー値。 • 最初のレポート要件（日）：最初のレポートを送信するまでに使用可能な最大時間。その後にポリシー名が続きます。 • レポート頻度（日）：次のレポートを送信するまでに使用可能な最大時間。その後にポリシー名が続きます。 • 変化レポート（日）：ライセンスの使用状況が変化した場合にレポートを送信できる最大時間。その後にポリシー名が続きます。
Miscellaneous	カスタム ID のヘッダー。	
	Custom Id:	ID

フィールド		説明
Usage Reporting:	使用状況レポート（RUM レポート）情報のヘッダー。	
	Last ACK received:	最後に受信した ACK の日時（ローカルタイムゾーン）。
	Next ACK deadline:	次の ACK の日時。ACK が不要であることがポリシーで示されている場合、このフィールドには none と表示されます。 （注） ACK が必要で、この期限までに受信されない場合、syslog が表示されます。
	Reporting Interval:	日単位のレポート間隔。 ここに表示される値は、**license smart usage interval***interval_in_days* とポリシー値の設定によって異なります。詳細については、license smart（グローバル コンフィギュレーション） （71 ページ） で対応する構文の説明を参照してください。
	Next ACK push check:	製品インスタンスが ACK の次のポーリング要求を送信する日時。日時はローカルタイムゾーンで表示されます。 これは、CSSM または CSLU への製品インスタンスによって開始された通信にのみ適用されます。レポート間隔がゼロの場合、または ACK ポーリングが保留されていない場合、このフィールドには none と表示されます。
	Next report push:	

フィールド		説明
		製品インスタンスが次のRUMレポートを送信する日時。日時はローカルタイムゾーンで表示されます。レポート間隔がゼロの場合、または保留中のRUMレポートがない場合、このフィールドには none と表示されます。
	Last report push:	製品インスタンスが最後のRUMレポートを送信した日時。日時はローカルタイムゾーンで表示されます。
	Last report file write:	製品インスタンスが最後にオフラインRUMレポートを保存した日時。日時はローカルタイムゾーンで表示されます。
	Last report pull:	データモデルを使用して使用状況レポート情報が取得された日時。日時はローカルタイムゾーンで表示されます。
Trust Code Installed:	信頼コード関連情報のヘッダー。 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。 信頼コードがインストールされていない場合、このフィールドには none と表示されます。	
	Active:	アクティブ製品インスタンス。 高可用性セットアップでは、セットアップ内のすべての製品インスタンスのUDIと、対応する信頼コードのインストール日時が表示されます。
	Standby:	スタンバイ製品インスタンス。
	Member:	メンバー製品インスタンス

例：Cisco 4000 シリーズ サービス統合型ルータでの show license status

次に、**show license status** コマンドの出力例を示します。カスタムポリシーを適用します。

```
Device# show license status
Sword#show license status
Utility:
  Status: DISABLED

SLE Policy:
  Status: ENABLED

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

Transport:
  Type: cslu
  Cslu address: http://192.168.0.1:8182/cslu/v1/pi
  Proxy:
    Not Configured

Policy:
  Policy in use: Installed On Sep 23 17:51:50 2020 UTC
  Policy name: Test Policy-13apr
  Reporting ACK required: yes (Customer Policy)
  Perpetual Attributes:
    First report requirement (days): 25 (Customer Policy)
    Reporting frequency (days): 25 (Customer Policy)
    Report on change (days): 25 (Customer Policy)
  Subscription Attributes:
    First report requirement (days): 15 (Customer Policy)
    Reporting frequency (days): 15 (Customer Policy)
    Report on change (days): 15 (Customer Policy)
  Enforced License Attributes:
    First report requirement (days): 90 (CISCO default)
    Reporting frequency (days): 35 (Customer Policy)
    Report on change (days): 35 (Customer Policy)
  Export License Attributes:
    First report requirement (days): 90 (CISCO default)
    Reporting frequency (days): 30 (Customer Policy)
    Report on change (days): 30 (Customer Policy)

Miscellaneus:
  Custom Id: <empty>

Usage Reporting:
  Last ACK received: Sep 23 16:35:10 2020 UTC
  Next ACK deadline: Oct 18 16:35:10 2020 UTC
  Reporting push interval: 25  days
  Next ACK push check: Sep 23 17:52:59 2020 UTC
  Next report push: Sep 23 17:52:58 2020 UTC
  Last report push: Sep 23 16:31:12 2020 UTC
  Last report file write: <none>

Trust Code Installed: <none>
```

show license summary

使用されているライセンス、カウント、およびステータスに関する情報を含む、ライセンス使用状況の概要を表示するには、特権 EXEC モードで **show license summary** コマンドを入力します。

show license summary

このコマンドには引数またはキーワードはありません。

コマンド モード

特権 EXEC（Device#）

コマンド履歴

リリース	変更内容
このコマンドは、Cisco IOS XE Amsterdam 17.3.2 よりも前のリリースで導入されました。	このコマンドが導入されました。
Cisco IOS XE Amsterdam 17.3.2	コマンド出力が更新され、ポリシーを使用したスマートライセンシングの有効なライセンスステータスが反映されました。有効なライセンスステータスには、`IN USE`、`NOT IN USE`、`NOT AUTHORIZED` などがあります。 コマンド出力が更新され、登録および承認情報が削除されました。 コマンド出力にスマートアカウントとバーチャルアカウントの情報が表示されなくなりました。

例

次に、さまざまなシスコ製品インスタンスでの **show license summary** コマンドの出力例を示します。ディスプレイに表示されるフィールドについては、表 6 : show license summary のフィールドの説明 （104 ページ）を参照してください。

- 例：show license summary：すべて IN USE（Cisco 4000 シリーズ サービス統合型ルータ）（105 ページ）

表 *6 : show license summary* のフィールドの説明

フィールド	説明
License	使用中のライセンスの名前
Entitlement Tag	ライセンスの短縮名
Count	ライセンス数

フィールド	説明
Status	ライセンスのステータスは次のいずれかになります。 • In-Use：有効なライセンスかつ使用中。 • Not In-Use • Not Authorized：ライセンスを使用する前に SLAC のインストールが必要であることを意味します。詳細については、承認コード （9 ページ）を参照してください。

例：show license summary：すべて IN USE（Cisco 4000 シリーズ サービス統合型ルータ）

次に、すべてのライセンスが使用中である場合の **show license summary** コマンドの出力例を示します。

```
Devide# show license summary

Sword#show license summary
License Usage:
  License                 Entitlement tag               Count Status
  -----------------------------------------------------------------------------
  hseck9                  (ISR_4331_Hsec)                   1 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
```

show license tech

テクニカルサポートチーム用にライセンス情報を表示するには、特権 EXEC モードで **show license tech** コマンドを入力します。このコマンドの出力には、他のいくつかの **show license** コマンドの出力などが含まれます。

show license tech { **data** { **conversion** } | **eventlog** [{*days* }] | **reservation** | **support** }

構文の説明

data { **conversion** }	ライセンスデータ変換情報を表示します。
eventlog [{*days* }]	ポリシーを使用したスマートライセンシングに関連するイベントログを表示します。 *days* には、イベントログを表示する日数を入力します。0 ～ 2147483647 の範囲の値を指定できます。
reservation	ライセンス予約情報を表示します。

support	テクニカルサポートチームが問題をデバッグするのに役立つライセンス情報を表示します。

コマンド モード

特権 EXEC（Device#）

コマンド履歴

リリース	変更内容
このコマンドは、Cisco IOS XE Amsterdam 17.3.2 よりも前のリリースで導入されました。	このコマンドが導入されました。
Cisco IOS XE Amsterdam 17.3.2。	コマンド出力が更新され、ポリシーを使用したスマートライセンシングに適用可能な新しいフィールドが反映されました。

例

次に、さまざまなシスコ製品インスタンスでの **show license tech support** コマンドの出力例を示します。

• 例：Cisco 4000 シリーズ サービス統合型ルータでの show license tech support （106 ページ）

例：Cisco 4000 シリーズ サービス統合型ルータでの show license tech support

次に、**show license tech support** コマンドの出力例を示します。

```
Device# show license tech support
Smart Licensing Tech Support info

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

Smart Licensing is ENABLED

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

Export Authorization Key:
  Features Authorized:
    <none>

Utility:
  Status: DISABLED

SLE Policy:
  Status: ENABLED

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

```
Transport:
  Type: cslu
  Cslu address: http://10.195.85.83:8182/cslu/v1/pi
  Proxy:
    Address: <empty>
    Port: <empty>
    Username: <empty>
    Password: <empty>
  Server Identity Check: False

Miscellaneus:
  Custom Id: <empty>

Policy:
  Policy in use: Installed On Sep 23 17:51:50 2020 UTC
  Policy name: Test Policy-13apr
  Reporting ACK required: yes (Customer Policy)
  Perpetual Attributes:
    First report requirement (days): 25 (Customer Policy)
    Reporting frequency (days): 25 (Customer Policy)
    Report on change (days): 25 (Customer Policy)
  Subscription Attributes:
    First report requirement (days): 15 (Customer Policy)
    Reporting frequency (days): 15 (Customer Policy)
    Report on change (days): 15 (Customer Policy)
  Enforced License Attributes:
    First report requirement (days): 90 (CISCO default)
    Reporting frequency (days): 35 (Customer Policy)
    Report on change (days): 35 (Customer Policy)
  Export License Attributes:
    First report requirement (days): 90 (CISCO default)
    Reporting frequency (days): 30 (Customer Policy)
    Report on change (days): 30 (Customer Policy)

Usage Reporting:
  Last ACK received: Sep 23 16:35:10 2020 UTC
  Next ACK deadline: Oct 18 16:35:10 2020 UTC
  Reporting push interval: 25  days State(4) InPolicy(25)
  Next ACK push check: Sep 23 17:56:59 2020 UTC
  Next report push: Oct 18 17:53:00 2020 UTC
  Last report push: Sep 23 17:53:00 2020 UTC
  Last report file write: <none>

License Usage
=============
Handle: 1
  License: hseck9
  Entitlement tag:
regid.2015-02.com.cisco.ISR_4331_Hsec,1.0_7998f136-248d-4ee9-94be-2b561c04a51e
  Description: hseck9
  Count: 1
  Version: 1.0
  Status: IN USE(15)
  Status time: Sep 23 17:52:27 2020 UTC
  Request Time: Sep 23 17:52:28 2020 UTC
  Export status: RESTRICTED - ALLOWED
  Feature Name: hseck9
  Feature Description: hseck9
  Measurements:
    ENTITLEMENT:
      Interval: 00:15:00
      Current Value: 1

Handle: 2
```

```
  License: booster_performance
  Entitlement tag:
regid.2017-05.com.cisco.ISR_4331_BOOST,1.0_d5ca3d93-a3a9-480d-98f7-c7b06ddcc973
  Description: booster_performance
  Count: 1
  Version: 1.0
  Status: IN USE(15)
  Status time: Sep 22 20:40:01 2020 UTC
  Request Time: Sep 22 20:40:01 2020 UTC
  Export status: NOT RESTRICTED
  Feature Name: booster_performance
  Feature Description: booster_performance
  Measurements:
    ENTITLEMENT:
      Interval: 00:15:00
      Current Value: 1
  Soft Enforced: True

Handle: 3
  License: appxk9
  Entitlement tag:
regid.2015-01.com.cisco.ISR_4331_Application,1.0_4dd5e243-4754-4fed-b8aa-cdd9ff0e82c0
  Description: appxk9
  Count: 1
  Version: 1.0
  Status: IN USE(15)
  Status time: Sep 22 20:40:02 2020 UTC
  Request Time: Sep 22 20:40:02 2020 UTC
  Export status: NOT RESTRICTED
  Feature Name: appxk9
  Feature Description: appxk9
  Measurements:
    ENTITLEMENT:
      Interval: 00:15:00
      Current Value: 1
  Soft Enforced: True

Handle: 4
  License: uck9
  Entitlement tag:
regid.2014-12.com.cisco.ISR_4331_UnifiedCommunication,1.0_fc59e79d-8a80-469b-b1fb-0307e6e76108

  Description: uck9
  Count: 1
  Version: 1.0
  Status: IN USE(15)
  Status time: Sep 22 20:40:02 2020 UTC
  Request Time: Sep 22 20:40:02 2020 UTC
  Export status: NOT RESTRICTED
  Feature Name: uck9
  Feature Description: uck9
  Measurements:
    ENTITLEMENT:
      Interval: 00:15:00
      Current Value: 1
  Soft Enforced: True

Handle: 5
  License: securityk9
  Entitlement tag:
regid.2014-12.com.cisco.ISR_4331_Security,1.0_dba7c7eb-f2b3-4824-9690-10e46d998fa5
  Description: securityk9
  Count: 1
  Version: 1.0
```

```
  Status: IN USE(15)
  Status time: Sep 22 20:40:02 2020 UTC
  Request Time: Sep 22 20:40:02 2020 UTC
  Export status: NOT RESTRICTED
  Feature Name: securityk9
  Feature Description: securityk9
  Measurements:
    ENTITLEMENT:
      Interval: 00:15:00
      Current Value: 1
  Soft Enforced: True

Product Information
===================
UDI: PID:ISR4331/K9,SN:FDO224917Q6

Agent Version
=============
Smart Agent for Licensing: 4.13.23_rel/62

Upcoming Scheduled Jobs
=======================
Current time: Sep 23 17:53:15 2020 UTC
Daily: Sep 23 20:39:35 2020 UTC (2 hours, 46 minutes, 20 seconds remaining)
Authorization Renewal: Expired Not Rescheduled
Init Flag Check: Expired Not Rescheduled
Reservation configuration mismatch between nodes in HA mode: Expired Not Rescheduled
Retrieve data processing result: Sep 23 17:56:59 2020 UTC (3 minutes, 44 seconds remaining)
Start Utility Measurements: Sep 23 18:07:59 2020 UTC (14 minutes, 44 seconds remaining)
Send Utility RUM reports: Oct 18 17:52:59 2020 UTC (24 days, 23 hours, 59 minutes, 44
seconds remaining)
Save unreported RUM Reports: Sep 23 17:53:29 2020 UTC (14 seconds remaining)
Process Utility RUM reports: Sep 24 06:25:37 2020 UTC (12 hours, 32 minutes, 22 seconds
 remaining)
Authorization Code Process: Expired Not Rescheduled
Authorization Confirmation Code Process: Expired Not Rescheduled
Authorization Return Code Process: Expired Not Rescheduled
External Event: Oct 18 16:35:09 2020 UTC (24 days, 22 hours, 41 minutes, 54 seconds
remaining)
Operational Model: Expired Not Rescheduled

Communication Statistics:
=========================
Communication Level Allowed: INDIRECT
Overall State: <empty>
Trust Establishment:
  Attempts: Total=0, Success=0, Fail=0  Ongoing Failure: Overall=0 Communication=0
  Last Response: <none>
    Failure Reason: <none>
  Last Success Time: <none>
  Last Failure Time: <none>
Trust Acknowledgement:
  Attempts: Total=0, Success=0, Fail=0  Ongoing Failure: Overall=0 Communication=0
  Last Response: <none>
    Failure Reason: <none>
  Last Success Time: <none>
  Last Failure Time: <none>
Usage Reporting:
  Attempts: Total=8, Success=5, Fail=3  Ongoing Failure: Overall=0 Communication=0
  Last Response: OK_POLL on Sep 23 17:52:59 2020 UTC
    Failure Reason: <none>
  Last Success Time: Sep 23 17:52:59 2020 UTC
  Last Failure Time: Sep 23 00:07:15 2020 UTC
Result Polling:
```

```
  Attempts: Total=284, Success=280, Fail=4  Ongoing Failure: Overall=0 Communication=0
  Last Response: OK_POLL on Sep 23 17:53:00 2020 UTC
    Failure Reason: <none>
  Last Success Time: Sep 23 17:53:00 2020 UTC
  Last Failure Time: Sep 23 10:07:47 2020 UTC
Authorization Request:
  Attempts: Total=2, Success=2, Fail=0  Ongoing Failure: Overall=0 Communication=0
  Last Response: OK on Sep 23 17:51:50 2020 UTC
    Failure Reason: <none>
  Last Success Time: Sep 23 17:51:50 2020 UTC
  Last Failure Time: <none>
Authorization Confirmation:
  Attempts: Total=2, Success=2, Fail=0  Ongoing Failure: Overall=0 Communication=0
  Last Response: OK on Sep 23 17:51:52 2020 UTC
    Failure Reason: <none>
  Last Success Time: Sep 23 17:51:52 2020 UTC
  Last Failure Time: <none>
Authorization Return:
  Attempts: Total=1, Success=1, Fail=0  Ongoing Failure: Overall=0 Communication=0
  Last Response: OK on Sep 23 17:46:19 2020 UTC
    Failure Reason: <none>
  Last Success Time: Sep 23 17:46:19 2020 UTC
  Last Failure Time: <none>
Trust Sync:
  Attempts: Total=0, Success=0, Fail=0  Ongoing Failure: Overall=0 Communication=0
  Last Response: <none>
    Failure Reason: <none>
  Last Success Time: <none>
  Last Failure Time: <none>
Hello Message:
  Attempts: Total=8, Success=8, Fail=0  Ongoing Failure: Overall=0 Communication=0
  Last Response: OK on Sep 23 17:52:58 2020 UTC
    Failure Reason: <none>
  Last Success Time: Sep 23 17:52:58 2020 UTC
  Last Failure Time: <none>

License Certificates
====================
Production Cert: False
Not registered. No certificates installed

HA Info
==========
RP Role: Active
Chassis Role: Active
Behavior Role: Active
RMF: True
CF: True
CF State: Stateless
Message Flow Allowed: True

Reservation Info
================
License reservation: DISABLED

Overall status:
  Active: PID:ISR4331/K9,SN:FDO224917Q6
      Reservation status: SMART AUTHORIZATION INSTALLED on Sep 23 17:51:48 2020 UTC
      Request code: <none>
      Last return code: <none>
      Last Confirmation code: 7e0f9388
      Reservation authorization code:
<redacted>
 Export Restriction Compliance license for 4330
```

[illegible]

```
Authorizations:
  ISR_4331_Hsec (ISR_4331_Hsec):
    Description: U.S. Export Restriction Compliance license for 4330 series
    Total available count: 1
    Enforcement type: EXPORT RESTRICTED
    Term information:
      Active: PID:ISR4331/K9,SN:FDO224917Q6
        Authorization type: SMART AUTHORIZATION INSTALLED
        License type: PERPETUAL
          Start Date: <none>
          End Date: <none>
          Term Count: 1
          Subscription ID: <none>

Purchased Licenses:
  No Purchase Information Available


Last Reporting Not Required:
  Entitlement
tag:regid.2017-05.com.cisco.ISR_4331_BOOST,1.0_d5ca3d93-a3a9-480d-98f7-c7b06ddcc973
  Entitlement
tag:regid.2015-01.com.cisco.ISR_4331_Application,1.0_4dd5e243-4754-4fed-b8aa-cdd9ff0e82c0

  Entitlement
tag:regid.2014-12.com.cisco.ISR_4331_UnifiedCommunication,1.0_fc59e79d-8a80-469b-b1fb-0307e6e76108

  Entitlement
tag:regid.2014-12.com.cisco.ISR_4331_Security,1.0_dba7c7eb-f2b3-4824-9690-10e46d998fa5

Other Info
==========
Software ID: regid.2014-12.com.cisco.ISR_4331,1.0_35288778-c93c-4fad-8e9b-41abf0339cc7
Agent State: authorized
TS enable: True
Transport: cslu
Locale: en_US.UTF-8
Debug flags: 0x7
Privacy Send Hostname: True
Privacy Send IP: True
Build type:: Production
sizeof(char)  : 1
sizeof(int)   : 4
sizeof(long)  : 4
sizeof(char *): 8
sizeof(time_t): 4
sizeof(size_t): 8
Endian: Big
Write Erase Occurred: False
XOS version: 0.12.0.0
Config Persist Received: False
Message Version: 1.3
connect_info.name: <empty>
connect_info.version: <empty>
connect_info.additional: <empty>
connect_info.prod: False
connect_info.capabilities: <empty>
agent.capabilities: UTILITY, DLC, AppHA, MULTITIER, EXPORT_2, OK_TRY_AGAIN, POLICY_USAGE
Check Point Interface: True
Config Management Interface: False
License Map Interface: True
```

```
HA Interface: True
Trusted Store Interface: True
Platform Data Interface: True
Crypto Version 2 Interface: False
SAPluginMgmtInterfaceMutex: True
SAPluginMgmtIPDomainName: True
SmartAgentClientWaitForServer: 2000
SmartAgentCmReTrySend: True
SmartAgentClientIsUnified: True
SmartAgentCmClient: True
SmartAgentClientName: UnifiedClient
builtInEncryption: True
enableOnInit: True
routingReadyByEvent: True
systemInitByEvent: True
SmartTransportServerIdCheck: True
SmartTransportProxySupport: True
SmartAgentConcurrentThreadMax: 10
SmartAgentPolicyControllerModel: False
SmartAgentPolicyModel: True
SmartAgentFederalLicense: True
SmartAgentMultiTenant: False
attr365DayEvalSyslog: True
checkPointWriteOnly: False
SmartAgentDelayCertValidation: False
enableByDefault: False
conversionAutomatic: False
conversionAllowed: True
storageEncryptDisable: False
storageLoadUnencryptedDisable: False
TSPluginDisable: False
bypassUDICheck: False
loggingAddTStamp: False
loggingAddTid: True
HighAvailabilityOverrideEvent: UnknownPlatformEvent
platformIndependentOverrideEvent: UnknownPlatformEvent
platformOverrideEvent: UnknownPlatformEvent
WaitForHaRole: False
standbyIsHot: False
chkPtType: 2
delayCommInit: False
roleByEvent: True
maxTraceLength: 150
traceAlwaysOn: True
debugFlags: 0
Event log max size: 5120 KB
Event log current size: 10 KB
Local Device: No Trust Data
Overall Trust: No ID

Platform Provided Mapping Table
================================
  ISR4331/K9: Total licenses found: 2863
Enforced Licenses:
  P:ISR4331/K9,S:FDO224917Q6:
    hseck9: regid.2015-02.com.cisco.ISR_4331_Hsec,1.0_7998f136-248d-4ee9-94be-2b561c04a51e
 (3)
```

show license udi

製品インスタンスの UDI 情報を表示するには、特権 EXEC モードで **show license udi** コマンドを入力します。高可用性セットアップでは、接続されたすべての製品インスタンスの UDI 情報が出力に表示されます。

show license UDI

このコマンドには引数またはキーワードはありません。

コマンド モード

Privileged EXEC (Device#)

コマンド履歴

リリース	変更内容
このコマンドは、Cisco IOS XE Amsterdam 17.3.2 よりも前のリリースで導入されました。	このコマンドが導入されました。

例

次に、さまざまなシスコ製品インスタンスとさまざまなセットアップでの **show license summary** コマンドの出力例を示します。

- 例：スタンドアロン（Cisco 4000 シリーズ サービス統合型ルータ）での show license udi （113 ページ）
- 例：アクティブとスタンバイ（Cisco Catalyst 8000 エッジ プラットフォーム ファミリ）での show license udi （113 ページ）

例：スタンドアロン（Cisco 4000 シリーズ サービス統合型ルータ）での show license udi

次に、単一 RP の製品インスタンスでの **show license udi** コマンドの出力例を示します。

```
Device# show license udi

UDI: PID:ISR4331/K9,SN:FDO224917Q6
```

例：アクティブとスタンバイ（Cisco Catalyst 8000 エッジ プラットフォーム ファミリ）での show license udi

次に、アクティブ製品インスタンスとスタンバイ製品インスタンスが存在する高可用性セットアップでの **show license udi** コマンドの出力例を示します。両方の UDI 情報が表示されます。

```
Device# show license udi

UDI: PID:C8500L-8S4X,SN:JAD2331191E
HA UDI List:
```

```
Active:PID:C8500L-8S4X,SN:JAD2331191E
Standby:PID:C8500L-8S4X,SN:JAD2331191E
```

show license usage

製品インスタンス上にあるすべてのライセンスのライセンス情報を表示するには、特権EXECモードで **show license usage** コマンドを入力します。

show license usage

このコマンドには引数またはキーワードはありません。

コマンド モード

特権 EXEC（Device#）

コマンド履歴

リリース	変更内容
このコマンドは、Cisco IOS XE Amsterdam 17.3.2 よりも前のリリースで導入されました。	このコマンドが導入されました。
Cisco IOS XE Amsterdam 17.3.2	コマンド出力が更新され、ポリシーを使用したスマートライセンシングに適用可能な新しいフィールドが反映されました。これには、`Status`、`Enforcement type` フィールドが含まれます。 コマンド出力が更新され、予約関連情報、承認ステータス情報、および輸出ステータス情報が削除されました。

例

次に、さまざまな製品インスタンスでの **show license usage** コマンドの出力例を示します。ディスプレイに表示されるフィールドについては、表 7 : show license usage のフィールドの説明 （114 ページ）を参照してください。

- 例：不適用および輸出規制ライセンスでの show license usage（Cisco 4000 シリーズ サービス統合型ルータ） （116 ページ）
- 例：不適用ライセンスでの show license usage（Cisco Catalyst 9500 シリーズ スイッチ） （117 ページ）

表 7 : show license usage のフィールドの説明

フィールド	説明
License Authorization: Status:	全体的な承認ステータスを表示します。

フィールド	説明
():	CSSM におけるようなライセンスの名前。 このライセンスが承認コードを必要とする場合、ライセンスの名前はコードから取得されます。
Description	CSSM におけるようなライセンスの説明。
Count	ライセンス数。ライセンスが使用中でない場合、カウントはゼロとして反映されます。
Version	バージョン。
Status	ライセンスのステータスは次のいずれかになります。 • In-Use：有効なライセンスかつ使用中。 • Not In-Use • Not Authorized：ライセンスを使用する前に SLAC のインストールが必要であることを意味します。詳細については、承認コード （9 ページ）を参照してください。
Export Status:	このライセンスが輸出規制されているかどうかを示します。それに応じて次のステータスのいずれかが表示されます。 • RESTRICTED - ALLOWED • RESTRICTED - NOT ALLOWED • NOT RESTRICTED
Feature name	このライセンスを使用する機能の名前。
Feature Description:	このライセンスを使用する機能の説明。

フィールド	説明
Enforcement type	ライセンスの適用タイプのステータス。これは、次のいずれかです。 • ENFORCED • NOT ENFORCED • EXPORT RESTRICTED - ALLOWED • EXPORT RESTRICTED - NOT ALLOWED 適用タイプの詳細については、次を参照してください： ライセンス執行（エンフォースメント）タイプ （8 ページ）

例：不適用および輸出規制ライセンスでの show license usage（Cisco 4000 シリーズ サービス統合型ルータ）

次に、**show license usage** コマンドの出力例を示します。ここでは、不適用および輸出規制ライセンスを使用中です。

```
Device# show license usage

License Authorization:
  Status: Not Applicable

hseck9 (ISR_4331_Hsec):
  Description: hseck9
  Count: 1
  Version: 1.0
  Status: IN USE
  Export status: RESTRICTED - ALLOWED
  Feature Name: hseck9
  Feature Description: hseck9
  Enforcement type: EXPORT RESTRICTED

booster_performance (ISR_4331_BOOST):
  Description: booster_performance
  Count: 1
  Version: 1.0
  Status: IN USE
  Export status: NOT RESTRICTED
  Feature Name: booster_performance
  Feature Description: booster_performance
  Enforcement type: NOT ENFORCED

appxk9 (ISR_4331_Application):
  Description: appxk9
  Count: 1
  Version: 1.0
  Status: IN USE
  Export status: NOT RESTRICTED
  Feature Name: appxk9
  Feature Description: appxk9
  Enforcement type: NOT ENFORCED
```

```
uck9 (ISR_4331_UnifiedCommunication):
  Description: uck9
  Count: 1
  Version: 1.0
  Status: IN USE
  Export status: NOT RESTRICTED
  Feature Name: uck9
  Feature Description: uck9
  Enforcement type: NOT ENFORCED

securityk9 (ISR_4331_Security):
  Description: securityk9
  Count: 1
  Version: 1.0
  Status: IN USE
  Export status: NOT RESTRICTED
  Feature Name: securityk9
  Feature Description: securityk9
  Enforcement type: NOT ENFORCED
```

例：不適用ライセンスでの show license usage（Cisco Catalyst 9500 シリーズ スイッチ）

次に、**show license usage** コマンドの出力例を示します。ここでは、不適用ライセンスのみが使用されます。

```
Device# show license usage
Load for five secs: 1%/0%; one minute: 0%; five minutes: 0%
No time source, 12:59:18.941 EDT Fri Sep 11 2020

License Authorization:
  Status: Not Applicable
network-advantage (C9500 Network Advantage):
  Description: C9500 Network Advantage
  Count: 2
  Version: 1.0
  Status: IN USE
  Export status: NOT RESTRICTED
  Feature Name: network-advantage
  Feature Description: C9500 Network Advantage
  Enforcement type: NOT ENFORCED
dna-essentials (C9500 24Y4C DNA Essentials):
  Description: C9500-24Y4C DNA Essentials
  Count: 2
  Version: 1.0
  Status: IN USE
  Export status: NOT RESTRICTED
  Feature Name: dna-essentials
  Feature Description: C9500-24Y4C DNA Essentials
  Enforcement type: NOT ENFORCED
```

show platform software sl-infra

トラブルシューティング情報を表示し、デバッグに関する情報を表示するには、特権 EXEC モードで **show platform software sl-infra** コマンドを入力します。このコマンドの出力は、テクニカルサポートチームがトラブルシューティングとデバッグに使用します。

license call-home { **all** | **current** | **debug** | **stored** }

構文の説明

all	現在の情報、デバッグ情報、および保存されている情報を表示します。
current	現在のライセンス関連情報を表示します。
debug	デバッグを有効にします。
stored	製品インスタンスに保存されている情報を表示します。

コマンド モード

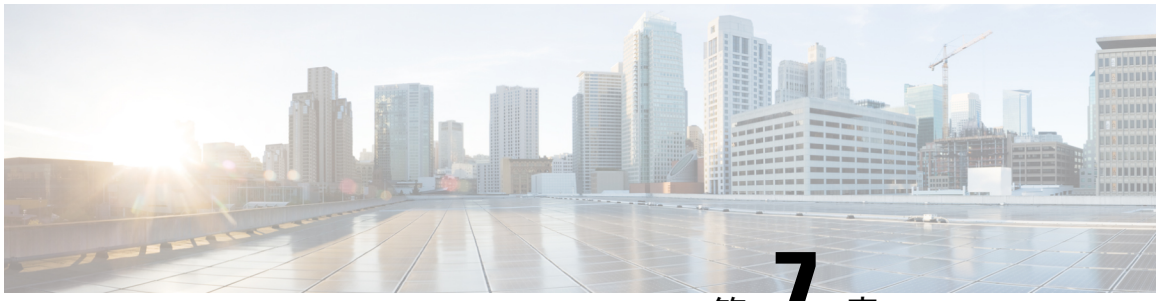
特権 EXEC（Device#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Amsterdam 17.3.2	このコマンドが導入されました。

使用上のガイドライン

解決できないエラーメッセージが表示された場合は、コンソールまたはシステムログに表示されるメッセージともに、シスコのテクニカルサポート担当者に **show license tech support**、**show license history message**、および **show platform software sl-infra all** 特権 EXEC コマンドの出力例を提供してください。



第 7 章

ポリシーを使用したスマートライセンシングのトラブルシューティング

システム メッセージの概要

ここでは、ポリシーを使用したスマートライセンシング固有のシステムメッセージについて説明します。これらのメッセージは、システムソフトウェアからコンソール（および任意で別のシステムのロギングサーバ）に送信されます。すべてのシステム メッセージがシステムの問題を示すわけではありません。通知目的のメッセージもあれば、通信回線、内蔵ハードウェア、またはシステム ソフトウェアの問題を診断するうえで役立つメッセージもあります。

システム メッセージの読み方

システムログメッセージには最大 80 文字を含めることができます。各システム メッセージはパーセント記号（%）から始まります。構成は次のとおりです。

```
%FACILITY-SEVERITY-MNEMONIC: Message-text
```

%FACILITY

メッセージが参照するファシリティを示す2 文字以上の大文字です。ファシリティは、ハードウェアデバイス、プロトコル、またはシステムソフトウェアのモジュールなどです。

SEVERITY

0 ～ 7 の 1 桁のコードで、状態の重大度を表します。この値が小さいほど、重大な状況を意味します。

表 *8:* メッセージの重大度

重大度	説明
0：緊急	システムが使用不可能な状態。
1：アラート	ただちに対応が必要な状態。
2：クリティカル	危険な状態。
3：エラー	エラー条件。
4：警告	警告条件。
5：通知	正常だが注意を要する状態。
6：情報	情報メッセージのみ。
7：デバッグ	デバッグ時に限り表示されるメッセージのみ。

MNEMONIC

メッセージを一意に識別するコード。

Message-text

メッセージテキストは、状態を説明したテキスト文字列です。メッセージのこの部分には、端末ポート番号、ネットワーク アドレス、またはシステム メモリ アドレス空間の位置に対応するアドレスなど、イベントの詳細情報が含まれることがあります。この可変フィールドの情報はメッセージごとに異なるので、ここでは角カッコ（[]）で囲んだ短い文字列で示します。たとえば 10 進数は [dec] で表します。

表 *9:* メッセージの変数フィールド

重大度	説明
[char]	1 文字
[chars]	文字列
[dec]	10 進数
[enet]	イーサネット アドレス（たとえば 0000.FEED.00C0）
[hex]	16 進数
[inet]	インターネット アドレス（10.0.2.16）
[int]	整数
[node]	アドレス名またはノード名

重大度	説明
[t-line]	8 進数のターミナルライン番号（10 進数 TTY サービスが有効な場合は 10 進数）
[clock]	クロック（例：01:20:08 UTC Tue Mar 2 1993

ポリシーを使用したスマートライセンシングのシステムメッセージ

このセクションでは、発生する可能性のあるポリシーを使用したスマートライセンシング関連のシステムメッセージ、考えられる理由（失敗メッセージの場合）、および推奨するアクション（アクションが必要な場合）を示します。

- %SMART_LIC-3-POLICY_INSTALL_FAILED
- %SMART_LIC-3-AUTHORIZATION_INSTALL_FAILED
- %SMART_LIC-3-COMM_FAILED
- %SMART_LIC-3-COMM_RESTORED
- %SMART_LIC-3-POLICY_REMOVED
- %SMART_LIC-3-TRUST_CODE_INSTALL_FAILED
- %SMART_LIC-4-REPORTING_NOT_SUPPORTED
- %SMART_LIC-6-POLICY_INSTALL_SUCCESS
- %SMART_LIC-6-AUTHORIZATION_INSTALL_SUCCESS
- %SMART_LIC-6-AUTHORIZATION_REMOVED
- %SMART_LIC-6-REPORTING_REQUIRED
- %SMART_LIC-6-TRUST_CODE_INSTALL_SUCCESS

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

説明：ポリシーがインストールされましたが、ポリシーコードの解析中にエラーが検出され、インストールに失敗しました。[chars] はエラーの詳細を示すエラー文字列です。

失敗の理由として次が考えられます。

- 製品インスタンスとポリシーの不一致：CSSMのポリシーは、スマートアカウントまたはバーチャルアカウントレベルで適用され、そのアカウントのすべての製品インスタンスにのみ適用されます。対応するアカウントの一部ではない製品インスタンスに **license smart import bootflash:** 特権 EXEC コマンドを使用してポリシーファイルを手動でインストールする場合、ポリシーのインストールは失敗します。
- 署名の不一致：これは、2 つのうちのいずれかを意味します。

- 正しい必須の証明書が製品インスタンスにインストールされていません。**show license tech support** コマンドの `License Certificates` セクションを確認します。`Production Cert:` が `False` と表示されている場合、ポリシーのインストールが失敗する可能性があります。

```
License Certificates
====================
Production Cert: False
Not registered. No certificates installed
```

- 特定のバーチャルアカウント（CSSM からの信頼コード用新規トークンの生成 （56 ページ））のトークンを生成した場合、結果のファイルにポリシーファイルが含まれることがあります。対応するアカウントの一部ではない製品インスタンスに **license smart import bootflash:** 特権 EXEC コマンドを使用してそのようなファイルを手動でインストールする場合、ポリシーのインストールは失敗します。

- タイムスタンプの不一致：製品インスタンスの時刻が CSSM と同期していないため、ポリシーのインストールが失敗する可能性があります。

推奨するアクション：

- 製品インスタンスとポリシーの不一致：CSSM Web UI で、バーチャルアカウントを選択し、製品インスタンスがポリシーのダウンロード元に含まれているかどうかを確認します。ポリシーをダウンロードします。

  1. https://software.cisco.com で CSSM Web UI にログインし、[Smart Software Licensing] > [Inventory] > [Product Instances] をクリックします。

     製品インスタンスが選択したバーチャルアカウントにリストされているかどうかを確認します。リストされている場合は、次のステップに進みます。そうでない場合は、正しいバーチャルアカウントを確認して選択し、次のステップに進みます。

  2. ここで、タスク CSSM からのポリシーファイルのダウンロード （58 ページ） および 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） を実行します。

- 署名の不一致：

  - 必要な証明書がインストールされていません：コンソールまたはシステムログに出力された正確なメッセージをコピーし、シスコのテクニカルサポート担当者に連絡し、正しい証明書を入手してインストールしてください。

  - 不正なバーチャルアカウントに対して生成されたトークン：

    1. https://software.cisco.com で CSSM Web UI にログインし、[Smart Software Licensing] > [Inventory] > [Product Instances] をクリックします。

       製品インスタンスが選択したバーチャルアカウントにリストされているかどうかを確認します。リストされている場合は、次のステップに進みます。そうでない場合は、正しいバーチャルアカウントを確認して選択し、次のステップに進みます。

2. ここで、タスク CSSM からの信頼コード用新規トークンの生成 （56 ページ） および 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） を実行します。

- タイムスタンプの不一致：グローバル コンフィギュレーション モードで **ntp server** コマンドを設定します。次に例を示します。

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

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

説明：承認コードがインストールされましたが、インストールに失敗しました。最初の [chars] は承認コードのインストールが失敗した UDI、2 番めの [chars] はエラーの詳細を示すエラー文字列です。

インストール失敗の理由として次が考えられます。

- UDI の不一致：承認コードファイル内の 1 つ以上の UDI が、承認コードファイルをインストールする製品インスタンスと一致しません。

  たとえば、高可用性セットアップ用に複数の UDI の承認コードを生成した場合です。承認コードファイルにリストされている UDI が設定の 1 つ以上のメンバーの UDI と一致しない場合、それらのメンバーでのインストールは失敗します。

  承認コードファイル内のすべての UDI を製品インスタンスの UDI（スタンドアロンまたは高可用性）と照合します。

  UDI 情報を含む承認コードファイルの例：

```
<smartLicenseAuthorization>
<udi>P:CSR1000V,S:9D1YXJM3LKC</udi>

<output truncated>
</smartLicenseAuthorization>
```

  製品インスタンスの UDI 情報の出力例：

```
Device# show license udi
UDI: PID:CSR1000V,SN:9D1YXJM3LKC
```

- 署名の不一致：承認コードファイルの署名を検証できなかったことを意味します。

  show license tech support コマンドの出力で、`Failure Reason:` フィールドを確認します。署名の検証がインストールの失敗の理由である場合、対応する情報がこのフィールドに表示されます。

```
Device# show license tech support
<output truncated>
Authorization Confirmation:
  Attempts: Total=2, Success=2, Fail=0  Ongoing Failure: Overall=0 Communication=0
  Last Response: OK on Sep 23 17:51:52 2020 UTC
    Failure Reason: <none>
  Last Success Time: Sep 23 17:51:52 2020 UTC
  Last Failure Time: <none>
```

- 現在設定されている機能の認証に十分なライセンスがありません：必要なすべてのライセンスに承認が生成されていないことを意味します。

推奨するアクション

- UDI の不一致：

  1. **show license udi** コマンドを使用して、UID の正しい完全なリストがあることを確認します。このコマンドは、高可用性セットアップの場合にすべての製品インスタンスを表示します。
  2. ここで、再度タスクCSSM からの SLAC の生成とファイルへのダウンロード（50 ページ）および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）を実行します。

- 署名の不一致：コンソールまたはシステムログに出力された正確なメッセージと **show license tech support** コマンドの出力をコピーし、シスコのテクニカルサポートに連絡してください。
- 現在設定されている機能の認証に十分なライセンスがありません：

  1. **show license udi** コマンドを使用して、UID の正しい完全なリストがあることを確認します。このコマンドは、高可用性セットアップの場合にすべての製品インスタンスを表示します。
  2. ここで、再度タスクCSSM からの SLAC の生成とファイルへのダウンロード（50 ページ）および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）を実行します。

```
Error Message %SMART_LIC-3-COMM_FAILED: Communications failure with the [chars] : [chars]
[chars] - depends on the transport type
        - Cisco Smart Software Manager (CSSM)
        - Cisco Smart License utility (CSLU)
[chars] - An error string with details of the failure
```

説明：CSSM または CSLU とのスマートライセンシング通信が失敗しました。最初の [chars] は現在設定されている転送タイプで、2 番めの [chars] はエラーの詳細を示すエラー文字列です。このメッセージは、失敗した通信の試行ごとに表示されます。

失敗の理由として次が考えられます。

- CSSM または CSLU に到達できない：これは、ネットワーク到達可能性の問題があることを意味します。
- 404 ホストが見つからない：これは CSSM サーバがダウンしていることを意味します。

推奨するアクション：

CSSM に到達できない場合、および CSLU に到達できない場合のトラブルシューティング手順を説明します。

CSSM に到達できない：製品インスタンスが CSSM に直接接続されている場合は、転送タイプに応じて次の手順を実行します。

- 転送タイプ **smart** を使用している場合：

1. スマート URL が正しく設定されているかどうかを確認します。特権 EXEC モードで **show license status** コマンドを使用して、URL が次のようになっているかどうかを確認します。https://smartreceiver.cisco.com/licservice/licenseそうでない場合は、グローバル コンフィギュレーション モードで license smart url smart smar_URL コマンドを再設定します。
2. DNS 解決を確認します。製品インスタンスが `smartreceiver.cisco.com` または nslookup で変換された IP に対して ping を実行できることを確認します。次の例は、変換された IP に対して ping を実行する方法を示しています。

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

- 転送タイプ **callhome** を使用している場合：

1. URL が正しく入力されているかどうかを確認します。特権 EXEC モードで **show license status** コマンドを使用して、URL が次のようになっているかどうかを確認します。https://tools.cisco.com/its/service/oddce/services/DDCEService
2. DNS 解決を確認します。製品インスタンスが `tools.cisco.com` または nslookup で変換された IP に対して ping を実行できることを確認します。

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

   上記が機能しない場合は、ルーティングルール、送信元インターフェイス、およびファイアウォール設定を再確認します。

3. Call Home プロファイル `CiscoTAC-1` がアクティブで、接続先 URL が正しいことを確認します。**show call-home profile all** コマンドは特権 EXEC モードで使用してください。

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

4. HTTPS クライアントの送信元インターフェイスが正しいことを確認します。

-

CSLU に到達できない：

- CSLU URL を確認し、ポート番号を確認します（8180 または 8182 のみ）。**show license status** コマンドは特権 EXEC モードで使用してください。

```
Device# show license status
<output truncated>
Transport:
  Type: cslu
  Cslu address: http://192.168.0.1:8182/cslu/v1/pi
  Proxy:
```

```
    Not Configured
<output truncated>
```

- 通信タイプ **cslu** および製品インスタンスで開始される通信を使用する場合：

  1. 製品インスタンスが、CSLU がインストールされているデバイスに ping できることを確認します。ping が成功すると、CSLU が到達可能であることが確認されます

- 通信タイプ **cslu** および CSLU で開始される通信を使用する場合：

  1. HTTP 接続を確認します。特権 EXEC モードで **show ip http server session-module** コマンドを使用し、`SL_HTTP` がアクティブであることを確認します。
  2. 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。
  3. 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。

それでも通信障害の原因を解決できない場合は、コンソールまたはシステムログに出力されたメッセージをそのまま **show license tech support** コマンドの出力とともにコピーし、シスコのテクニカルサポート担当者に連絡してください。

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

説明：CSSM または CSLU との製品インスタンス通信が復元されます。

推奨するアクション：アクションは必要ありません。

```
Error Message %SMART_LIC-3-POLICY_REMOVED: The licensing policy has been removed.
```

説明：以前にインストールされたライセンスポリシーが削除されました。デフォルトのポリシーが有効になりました。これにより、スマートライセンシングの動作が変更される可能性があります。

ポリシーを製品インスタンスから削除するには、特権 EXEC モードで **license smart factory reset** コマンドを使用する必要があります。

推奨するアクション：

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

説明：信頼コードのインストールに失敗しました。最初の [chars] は、信頼コードのインストールが試行された UDI です。2 番めの [chars] は、エラーの詳細を示すエラー文字列です。

失敗の理由として次が考えられます。

- 信頼コードがすでにインストールされています。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ています。UDI がすでに登録されている場合に別の UDI をインストールしようとすると、インストールは失敗します。
- スマートアカウントとバーチャルアカウントの不一致または署名の不一致：これは、（トークン ID が生成された）スマートアカウントまたはバーチャルアカウントに、信頼コードをインストールした製品インスタンスが含まれていないことを意味します。CSSM で生成されたトークンは、スマートアカウントまたはバーチャルアカウントレベルで適用され、そのアカウントのすべての製品インスタンスにのみ適用されます。
- タイムスタンプの不一致：製品インスタンスの時刻が CSSM と同期していないため、インストールが失敗する可能性があります。

推奨するアクション：

- 信頼コードはすでにインストールされています：特権 EXEC モードで **license smart trust idtoken** *id_token_value* {**local** | **all**} [**force**] コマンドを再設定し、このときに **force** キーワードを必ず含めてください。**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。
- スマートアカウントとバーチャルアカウントの不一致または署名の不一致：

  1. https://software.cisco.com で CSSM Web UI にログインし、[Smart Software Licensing] > [Inventory] > [Product Instances] をクリックします。

     トークンを生成する製品インスタンスが、選択したバーチャルアカウントにリストされているかどうかを確認します。リストされている場合は、次のステップに進みます。リストされていない場合は、正しいスマートアカウントとバーチャルアカウントを確認して選択してから次の手順に進みます。

  2. ここで、タスク CSSM からの信頼コード用新規トークンの生成 （56 ページ） および 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） を実行します。

- タイムスタンプの不一致：グローバル コンフィギュレーション モードで **ntp server** コマンドを設定します。次に例を示します。

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

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

説明：ポリシーを使用したスマートライセンシングは現在、Cisco Smart Software Manager On-Prem（旧称 Cisco Smart Software Manager サテライト）をサポートしていません。製品インスタンスは次のように動作します。

- 登録の更新と承認の更新の送信を停止します。
- 使用状況の記録を開始し、RUM レポートをローカルに保存します。

推奨するアクション：サポートされるトポロジ （13 ページ） を参照し、代わりにサポートされているトポロジのいずれかを実装します。

```
Error Message %SMART_LIC-6-POLICY_INSTALL_SUCCESS: A new licensing policy
was successfully installed.
```

説明：次のいずれかの方法でポリシーがインストールされました。

- Cisco IOS コマンドの使用
- CSLU からのプッシュ
- ACK 応答の一部として

推奨するアクション：アクションは必要ありません。適用されているポリシー（使用中のポリシー）とそのレポート要件を確認するには、特権 EXEC モードで **show license all** コマンドを入力します。

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

説明： [chars] は、承認コードが正常にインストールされた UDI です。

推奨するアクション：アクションは必要ありません。インストールされた承認コードのタイプと関連情報を確認するには、特権 EXEC モードで **show license authorization** コマンドを入力します。

また、特権 EXEC モードで **show license all** および **show license tech support** コマンドを使用して、インストールされている承認の種類と、製品インスタンスが使用できる契約適応資格のタイプを確認することもできます。

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

説明： [chars] は、承認コードがインストールされた UDI です。承認コードが削除されました。これにより、製品インスタンスからライセンスが削除され、スマートライセンシングとライセンスを使用する機能の動作が変更される可能性があります。

推奨するアクション：アクションは必要ありません。ライセンスの現在の状態を確認するには、特権 EXEC モードで **show license all** コマンドを入力します。

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

説明：これは、シスコへの RUM レポートが必要であることを意味するアラートです。[dec] は、このレポート要件を満たすために残された時間（日数）です。

推奨するアクション：要求された時間内に RUM レポートが送信されるようにします。

- 製品インスタンスが CSSM または CSLU に直接接続され、通信を開始し製品インスタンスでこのステップを完了するよう製品インスタンスが設定されている場合、製品インスタンスはスケジュールされた時間に使用状況情報を自動的に送信します。

  技術的な問題により、スケジュールされた時間に送信されない場合は、特権 EXEC モードで **license smart sync** コマンドを実行できます。構文の詳細については、license smart（特権 EXEC） （77 ページ）を参照してください。

- 製品インスタンスが CSLU に接続され、CSLU が通信を開始するように設定されている場合、次のタスクを実行します：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）（40 ページ）。
- 製品インスタンスが CSLU に接続されているが、CSLU が CSSM から切断されている場合は、次のタスクを実行します： Download All For Cisco（CSLU インターフェイス）（45 ページ）、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（58 ページ）、Upload From Cisco（CSLU インターフェイス）（46 ページ）。
- 製品インスタンスが CSSM から切断され、CSLU も使用していない場合は、特権 EXEC モードで **license smart save usage** コマンドを入力して、必要な使用状況情報をファイルに保存します。次に、CSSM に接続しているワークステーションから、次のタスクを実行します：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（58 ページ）。
- 製品インスタンスがコントローラによって管理されている場合、コントローラはスケジュールされた時間に RUM レポートを送信します。アドホックレポートをトリガーする場合は、Cisco DNA Center GUI でトリガーできます。

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

説明：[chars] は、信頼コードが正常にインストールされた UDI です。

推奨するアクション：アクションは必要ありません。信頼コードがインストールされていることを確認するには、特権 EXEC モードで **show license status** コマンドを入力します。出力のヘッダー `Trust Code Installed:` で更新されたタイムスタンプを探します。