



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

最終更新：2021年11月30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。

このマニュアルでは、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、Cisco Catalyst 8000 エッジプラットフォームファミリー、および Cisco ターミナルサービスゲートウェイでの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。

シスコ ライセンスの詳細については、[cisco.com/go/licensingguide](https://www.cisco.com/go/licensingguide) を参照してください。



第 2 章

ポリシーを使用したスマートライセンスングに関する情報

- 概要 (3 ページ)
- サポート対象製品 (4 ページ)
- アーキテクチャ (6 ページ)
- 概念 (11 ページ)
- サポートされるトポロジ (18 ページ)
- 他の機能との相互作用 (35 ページ)
- 従来のライセンスの変更点 (43 ページ)

概要

ポリシーを使用したスマートライセンスングは、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。

- ライセンスの購入または注文：既存の流通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。

後払いライセンスを注文することもできます。CSSMで各ライセンスを確認することもできます。ライセンスはサブスクリプション ID とともにリストされます。



- (注) 新しいハードウェアまたはソフトウェアの注文の場合、シスコは、次のアイテムを工場ですべてインストールすることで、**Smart Licensing Using Policy** の実装を簡素化します（用語については、以下の「[概念 \(11 ページ\)](#)」の項で説明します）。
- カスタムポリシー（使用可能な場合）
 - 承認コード（該当する場合のみ） この場合、注文時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入力する必要があります。
 - CSSM に送信されるデータの信頼性を保証する信頼コード。
これは、Cisco IOS XE cupertino 17.7.1a 以降でインストールされます。この信頼コードは、CSSM との通信には使用できません。

- 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) を使用し、使用状況情報を CSSM に直接報告し、コントローラ (Cisco DNA Center や Cisco vManage など) を使用し、Smart Software Manager オンプレミス (SSM オンプレミス) を展開して製品とライセンスをオンプレミスで管理できます。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、クラウ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 \(253 ページ\)](#) 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）。これは、後払いライセンスを使用する場合に適用され、使用量に応じて請求されます。

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スをサポートする 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 1: ポリシーを使用したスマートライセンス: サポート対象製品

製品カテゴリ	製品シリーズ	サポートが導入されたときの導入リリース
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		
	Cisco 1000 シリーズ サービス統合型ルータ	Cisco IOS XE Amsterdam 17.3.2
	Cisco 4000 シリーズ サービス統合型ルータ	Cisco IOS XE Amsterdam 17.3.2
	Cisco ASR 1000 シリーズ アグリゲーション サービス ルータ	Cisco IOS XE Amsterdam 17.3.2
	Cisco クラウド サービス ルータ 1000v (CSRv.bin イメージから Catalyst 8000V ソフトウェアイメージにアップグレードする必要があります)。	Cisco IOS XE Bengaluru 17.4.1
	シスコサービス統合型仮想ルータ (ISRv.bin イメージから Catalyst 8000V ソフトウェアイメージにアップグレードする必要があります)。	Cisco IOS XE Bengaluru 17.4.1
Cisco Catalyst 8000 エッジプラットフォーム ファミリ		
	Catalyst 8200 シリーズ エッジプラットフォーム	Cisco IOS XE Bengaluru 17.4.1
	Catalyst 8300 シリーズ エッジプラットフォーム	Cisco IOS XE Amsterdam 17.3.2
	Catalyst 8500 シリーズ エッジプラットフォーム	Cisco IOS XE Amsterdam 17.3.2
	Catalyst 8000V エッジソフトウェア	Cisco IOS XE Bengaluru 17.4.1
Cisco ターミナル サービス ゲートウェイ		
	Cisco 1100 ターミナル サービス ゲートウェイ	Cisco IOS XE Bengaluru 17.4.1

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ス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 \(4 ページ\)](#) 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 \(18 ページ\)](#) 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。
- 仮想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¹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。
- Cisco DNA Center などのコントローラに（シスコが）組み込みます。
- Linux を実行しているマシン（ラップトップまたはデスクトップ）に CSLU を導入します。

CSLU は、Windows 10 および Linux オペレーティングシステムをサポートします。利用可能な最新バージョンの CSLU を常に使用することをお勧めします。リリースノートおよび最新バージョンをダウンロードするには、[Software Download] ページの [Smart Licensing Utility]<https://software.cisco.com/download/home/286285506/type> をクリックします。



- (注) CSLU は Cisco SD-WAN (Cisco vManage) ではサポートされておらず、CSLU を使用して Cisco vManage によって管理されるルーティング製品インスタンスのライセンス使用状況を報告することはできません。

コントローラ

複数の製品インスタンスを管理する管理アプリケーションまたはサービス。

¹ 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。

サポートされているコントローラ、コントローラをサポートする製品インスタンス、およびコントローラと製品インスタンスに必要な最小ソフトウェアバージョンに関する情報を次の表に示します。

- [コントローラのサポート情報 : Cisco DNA Center](#)
- [コントローラのサポート情報 : Cisco vManage](#)

表 2: コントローラのサポート情報 : *Cisco DNA Center*

Smart Licensing Using Policy へ移行するために必要な Cisco DNA Center の最小バージョン ²	Cisco IOS XE に必要な最小バージョン ³	サポート対象製品インスタンス
Cisco DNA Center リリース 2.2.2	Cisco IOS XE Amsterdam 17.3.2	Cisco アグリゲーションルータ、統合型ルータ、およびクラウドサービスルータ : <ul style="list-style-type: none"> • Cisco ASR 1000 シリーズ アグリゲーションサービスルータ • 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 Catalyst 8000 エッジプラットフォームファミリー : <ul style="list-style-type: none"> • 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
	Cisco IOS XE Bengaluru 17.4.1	Cisco Catalyst 8000 エッジプラットフォームファミリー : <ul style="list-style-type: none"> • Catalyst 8200 シリーズ エッジプラットフォーム Cisco ターミナル サービス ゲートウェイ : <ul style="list-style-type: none"> • Cisco 1100 ターミナル サービス ゲートウェイ

² このコントローラに必要な最小バージョン。これは、特に明記されていない限り、後続のすべてのリリースでサポートが継続されることを意味します。

³ 製品インスタンスの Cisco IOS-XE に必要な最小バージョンこれは、特に明記されていない限り、後続のすべてのリリースでサポートが継続されることを意味します。

Cisco DNA Center の詳細については、
<https://www.cisco.com/c/en/us/support/cloud-systems-management/dna-center/series.html> でサポートページを参照してください。

表 3: コントローラのサポート情報 : Cisco vManage

Smart Licensing Using Policy へ移行するために必要な Cisco vManage の最小バージョン ⁴	Cisco IOS XE に必要な最小バージョン ⁵	サポート対象製品インスタンス
Cisco vManage リリース 20.5.1	Cisco IOS XE Bengaluru 17.5.1a	サポート対象製品インスタンスの最新リストについては、 Cisco SD-WAN スタートアップガイド → 「License Management for Smart Licensing Using Policy」 → 「Supported Devices」を参照してください。

⁴ このコントローラに必要な最小バージョン。これは、特に明記されていない限り、後続のすべてのリリースでサポートが継続されることを意味します。

⁵ 製品インスタンスの Cisco IOS-XE に必要な最小バージョンこれは、特に明記されていない限り、後続のすべてのリリースでサポートが継続されることを意味します。

Cisco vManage の詳細については、<https://www.cisco.com/c/en/us/support/routers/sd-wan/series.html> でサポートページを参照してください。

サポートされているコントローラでトポロジを実装する方法については、[コントローラを介して CSSM に接続 \(23 ページ\)](#) を参照してください。

SSM オンプレミス

Smart Software Manager オンプレミス (SSM オンプレミス) は、CSSM と連動するアセットマネージャです。これにより、CSSM に直接接続する代わりに、オンプレミスで製品とライセンスを管理できます。

SSM オンプレミスで Smart Licensing Using Policy を実装するために必要なソフトウェアバージョンについては、次を参照してください。

Smart Licensing Using Policy に必要な SSM オンプレミスの最小バージョン ⁶	Cisco IOS XE に必要な最小バージョン ⁷	サポート対象製品インスタンス
バージョン 8、リリース 202102	Cisco IOS XE Amsterdam 17.3.3	すべての サポート対象製品 (4 ページ)

- ⁶ 必要な SSM オンプレミスの最小バージョンこれは、特に明記されていない限り、後続のすべてのリリースでサポートが継続されることを意味します。
- ⁷ 製品インスタンスに必要な最小ソフトウェアのバージョンこれは、特に明記されていない限り、後続のすべてのリリースでサポートが継続されることを意味します。

MSLA による Smart Licensing Using Policy に必要な最小 SSM オンプレミスバージョン	MSLA による Smart Licensing Using Policy に必要な最小 Cisco IOS XE バージョン	サポート対象製品インスタンス
バージョン 8、リリース 202206	Cisco IOS XE Cupertino 17.9.1	Catalyst 8000V エッジソフトウェア 詳細については、 MSLA (10 ページ) を参照してください。

SSM オンプレミスの詳細については、ソフトウェアダウンロードページの [Smart Software Manager On-Prem \[英語\]](#) を参照してください。ドキュメントリンクを表示するには、.iso イメージにカーソルを合わせます。

MSLA

マネージドサービス ライセンス契約 (MSLA) は、ネットワーク内の製品インスタンスで使用するライセンスについてシスコと締結する契約です。この契約により、ライセンスの使用状況をシスコに報告し、使用するライセンスを前払いする代わりに、ライセンスの使用量に対して請求されることとなります。契約条件の詳細については、<https://www.cisco.com/c/en/us/about/legal/msla-direct-product-terms.html> を参照してください。

MSLA を使用すると、[Cisco commerce workspace \(CCW\)](#) でサブスクリプション ID 付きのライセンスを注文できます。ライセンスは、対応するサブスクリプション ID とともに、CSSM の指定されたスマートアカウントおよびバーチャルアカウントに保管されます。

MSLA による Smart Licensing Using Policy に必要な最小 Cisco IOS XE バージョン	サポート対象製品インスタンス
Cisco IOS XE Cupertino 17.9.1	自律モードで実行されている Catalyst 8000V エッジソフトウェアのみ。



(注) この MSLA は、製品インスタンスが Cisco vManage によって管理される SD-WAN コントローラモードで実行されている製品インスタンスで利用可能な MSLA とは異なります。

サブスクリプション ID を持つライセンスを使用する製品インスタンスも、「ユーティリティモード」で有効にする必要があります。その後、製品インスタンスは、すべてのライセンスワークフローを完了するために、CSSM と直接、または CSLU や SSM オンプレミスを介して相互作用するように構成するか、切断モードで動作するように構成できます。

このような製品インスタンスでサポートされるトポロジの詳細については、「[ユーティリティモード](#)」を参照してください。

概念

ここでは、ポリシーを使用したスマートライセンス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 4: SLAC を必要とするライセンス（12 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

スマートライセンス承認コード（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 から要求できません。

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 4: 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

上記のライセンススループロットに加えて、250 Mbps（Tier 2 以上）を超えるライセンスには SLAC が必要です。

表 5: SLAC を必要とするスループットレベル

製品インスタンス	SLAC を必要とするスループットレベル	その他の考慮事項
<p>Cisco 4000 シリーズ サービス統合型ルータ</p> <p>Cisco 1100 ターミナル サービスゲートウェイ</p>	250 Mbps を超える暗号化されたスループット	製品インスタンスに次のいずれかがすでに含まれている場合は、SLAC を再度インストールする必要はありません。
<p>Cisco 1000 シリーズ サービス統合型ルータ</p> <p>Catalyst 8200 シリーズ エッジプラットフォーム</p> <p>Catalyst 8300 シリーズ エッジプラットフォーム</p> <p>Catalyst 8500 シリーズ エッジプラットフォーム</p> <p>Catalyst 8000V エッジソフトウェア</p>	250 Mbps を超える暗号化されたスループット	<ul style="list-style-type: none"> • HSECK9 ライセンス用の SLAC • HSECK9 PAK ライセンス • HSECK9 ライセンスを含む SLR 承認コード
<p>Catalyst 8000V エッジソフトウェア</p> <p>(Cisco IOS XE Bengaluru 17.4.1 の Catalyst 8000V ソフトウェアイメージが必要とされる Cisco Cloud Services Router 1000v および Cisco Integrated Services Virtual Router にも適用されます)</p>	250 Mbps を超える暗号化および非暗号化スループット (合計)	



(注) 以前のライセンスモデルから **Smart Licensing Using Policy** にアップグレードする場合、いずれかのライセンスを所有している可能性があり、各ライセンスには固有の承認コードである特定のライセンス予約 (SLR)、製品アクティベーションキー (PAK)、パーマネントライセンス予約 (PLR) があります。

SLR 承認コードは、ポリシーを使用したスマートライセンスへのアップグレード後にサポートされるようになります。

PAK 履行済みライセンスを所有している場合は、[PAK ライセンスのスナップショット \(43 ページ\)](#) を参照して必要なタスクを完了し、PAK 履行済みライセンスを引き続き使用してください。

パーマネントライセンス予約 (PLR) 承認コードを所有していて、引き続き使用する場合は、[Smart Licensing Using Policy 環境のパーマネントライセンス予約 \(45 ページ\)](#) を参照してください。

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。
この値がゼロの場合、最初のレポートは必要ありません。
- **Reporting frequency (days)** : 次の RUM 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。
この値がゼロの場合、使用状況が変更されない限り、以降のレポートは必要ありません。
- **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。
この値がゼロの場合、使用状況の変更時のレポートは必要ありません。
この値がゼロでない場合は、変更を加えた後にレポートが必要です。次に示すすべてのシナリオは、製品インスタンスのライセンス使用状況における変更としてカウントされます。
 - 消費されたライセンスの変更 (別のライセンスへの変更やライセンスの追加または削除を含む)。

- ライセンスの消費なしから 1 つ以上のライセンスの消費への移行。
- 1 つ以上のライセンスの消費からライセンスの消費なしへの移行。



(注) 製品インスタンスがライセンスを使用していない場合、ポリシーのレポート要件（最初のレポート要件、レポート頻度、変更に関するレポート）のいずれかにゼロ以外の値が設定されていても、レポートは必要ありません。

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 6：ポリシー：Cisco default（15 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 6: 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 ⁸	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

⁸ 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のライセンス使用状況レポートです。RUM レポートは製品インスタンスによって生成され、CSSMによって使用されます。製品インスタンスは、ライセンス使用状況情報とすべてのライセンス使用状況の変更を、開いている RUM レポートに記録します。システムが決定した間隔で、開いている RUM レポートが閉じられ、新しい RUM レポートが開かれて、ライセンスの使用状況の記録が継続されます。閉じられた RUM レポートは、いつでも CSSM に送信できます。

RUM 確認応答（RUMACK または 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。レポートの ACK が製品インスタンスで使用可能になると、対応する RUM レポートが不要になり、削除できることが示されます。

レポート方式、つまり CSSM への RUM レポートの送信方法は、実装するトポロジによって異なります。

CSSM は、最後に受信した RUM レポートに従ってライセンス使用状況情報を表示します。

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。

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

- 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 レポートの生成、保存、管理

Cisco IOS XE Cupertino 17.7.1 以降、RUM レポートの生成と関連プロセスが次のように最適化および強化されました。

- 製品インスタンスで使用可能なすべての RUM レポートのリストを表示できます（レポートの数、それぞれの処理状態、エラーがあるかどうかなど）。この情報は、[show license rum](#)（306 ページ）、[show license all](#)（286 ページ）、[show license tech](#)（326 ページ） 特権 EXEC コマンドで入手できます。
- RUM レポートは、処理時間を短縮し、メモリ使用量を削減する新しい形式で保存されます。古い形式と新しい形式の違いによって生じる使用状況レポートの不整合を避けるために、次の状況では、トポロジに適用される方法で RUM レポートを送信することをお勧めします。

ポリシーを使用したスマートライセンスをサポートする以前のリリースから、Cisco IOS XE Cupertino 17.7.1 以降のリリースにアップグレードする場合。

Cisco IOS XE Cupertino 17.7.1 以降のリリースから、ポリシーを使用したスマートライセンスをサポートする以前のリリースにダウングレードする場合。

- 継続的なディスク領域とメモリの可用性を確保するために、製品インスタンスは、対象と見なされる RUM レポートの削除を検出してトリガーします。

信頼コード

製品インスタンスが使用する *UDI* に関連付けられた公開キー

- RUM レポートに署名します。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。
- CSSM でセキュア通信を有効化します。

信頼コードを取得する方法は複数あります。

- Cisco IOS XE cupertino 17.7.1a 以降は、すべての新規注文に対して工場出荷時に信頼コードがインストールされています。



(注) 出荷時にインストールされた信頼コードは、CSSM との通信には使用できません。

- 信頼コードは、IDM トークンを使用して CSSM から取得できます。

ここでは SSM Web UI で *ID* トークンを生成して信頼コードを入手して製品インスタンスにインストールする必要があります。出荷時にインストールされた信頼コードがある場合は、上書きする必要があります。製品インスタンスが CSSM に直接接続されている場合は、この方法を使用して、製品インスタンスが CSSM と安全に通信できるようにします。

信頼コードを取得する方法は、CSSMに直接接続するすべてのオプションに適用できます。詳細については、[CSSMに直接接続（21 ページ）](#)を参照してください。

- Cisco IOS XE Cupertino 17.7.1 以降では、信頼コードは、製品インスタンスが CSLU へのデータ送信を開始するトポロジと、製品インスタンスがエアギャップネットワーク内にあるトポロジで自動的に取得されます。

Cisco IOS XE Cupertino 17.9.1a 以降、CSLU が製品インスタンスのデータの取得を開始するトポロジでは、信頼コードが自動的に取得されます。

出荷時にインストールされた信頼コードがある場合は、自動的に上書きされます。この方法で取得した信頼コードは、CSSM とのセキュアな通信に使用できます。

対応するトポロジの説明と対応するワークフローを参照して、各シナリオにおける信頼コードの要求およびインストール方法を確認してください。[サポートされるトポロジ（18 ページ）](#)

信頼コードが製品インスタンスにインストールされている場合、**show license status** コマンドの出力の [Trust Code Installed] フィールドに更新されたタイムスタンプが表示されます。例：Trust Code Installed: 2020 年 10 月 9 日 17 時 56 分 19 秒 (UTC)

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ス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スの設定方法：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。ワークフローにより、トポロジを実装する最も簡単で迅速な方法が提供されます。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スのタスクライブラリ」を参照してください。



(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

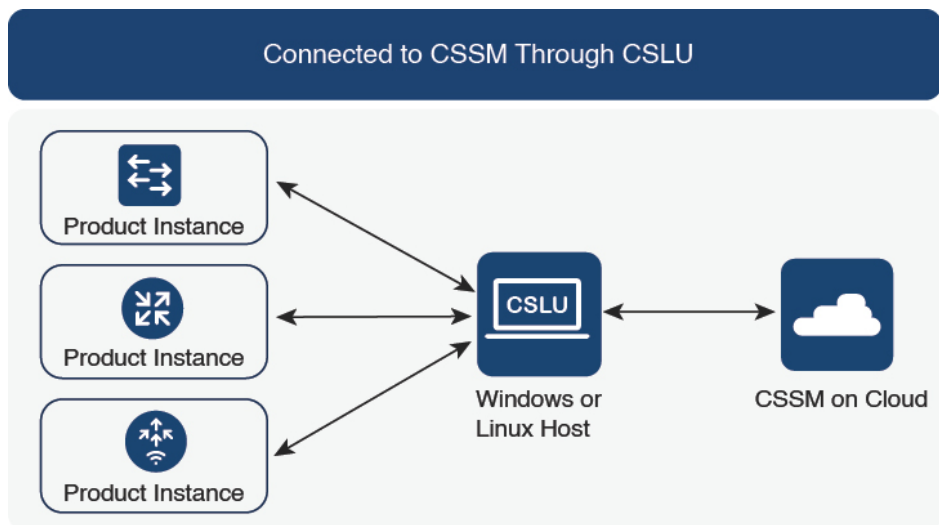
概要 :

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、UDIに関連付けられた信頼コード、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、UDIに関連付けられた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。

リリースごとの変更と拡張 :

このセクションでは、このトポロジに影響するリリースごとのソフトウェアの重要な変更と拡張について概説します。

Cisco IOS XE Cupertino 17.7.1a 以降 :

- 信頼コードの要求とインストール

信頼コードが製品インスタンスで使用できない場合、製品インスタンスは RUM レポートの一部として、信頼コードの要求を検出し、自動的に要求を含めます。CSSM からの対応する ACK には信頼コードが含まれています。出荷時にインストールされた既存の信頼コードがある場合は、自動的に上書きされます。この方法で取得した信頼コードは、CSSM との通信に使用できます。

これは、スタンドアロンおよび高可用性設定でサポートされます。高可用性設定では、アクティブな製品インスタンスは、信頼コードが使用できないすべての接続製品インスタンスの信頼コードを要求します。

このリリースでは、この拡張は、製品インスタンス開始モードにのみ適用されます。

Cisco IOS XE Cupertino 17.9.1a 以降 :

- 信頼コードの要求とインストール

このリリースから、信頼コードの要求とインストールは CSLU 開始モードでもサポートされています。

- Virtual Routing and Forwarding (VRF) のサポート

すべてのライセンスデータを送信するように VRF を設定できます。そのため、製品インスタンスは VRF をサポートするインスタンスである必要があります。また、このトポロジを実装する場合は、製品インスタンス開始モードを実装する必要があります。

- RUM レポートスロットリング

製品インスタンス開始モードでは、レポートの最小頻度は 1 日に制限されます。これは、製品インスタンスが 1 日に複数の RUM レポートを送信しないことを意味します。これにより、特定のライセンスに対して生成および送信される RUM レポートが多すぎるという問題が解決されます。また、RUM レポートの過剰な生成によって引き起こされたメモリ関連の問題とシステムのスローダウンも解決します。

特権 EXEC モードで **license smart sync** コマンドを入力すると、スロットリングの制限をオーバーライドできます。

RUM レポートスロットリングは、17.3.x トレインの Cisco IOS XE Amsterdam 17.3.6 以降のリリース、および 17.6.x トレインの Cisco IOS XE Bengaluru 17.6.4 以降のリリースにも適用されます。17.9.1 以降、RUM レポートスロットリングは後続のすべてのリリースに適用されます。

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 \(49 ページ\)](#) を参照してください。

CSSM に直接接続

概要：

このトポロジは、スマートライセンス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ス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 ID 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。



- (注) 出荷時にインストールされた信頼コードは、CSSM との通信には使用できません。つまり、このトポロジでは、CSSM Web UI で ID トークンを生成して、信頼コードを入手して製品インスタンスにインストールする必要があります。出荷時にインストールされた信頼コードがある場合は、上書きする必要があります。[信頼コード \(17 ページ\)](#) も参照してください。

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、スマートライセンス (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。

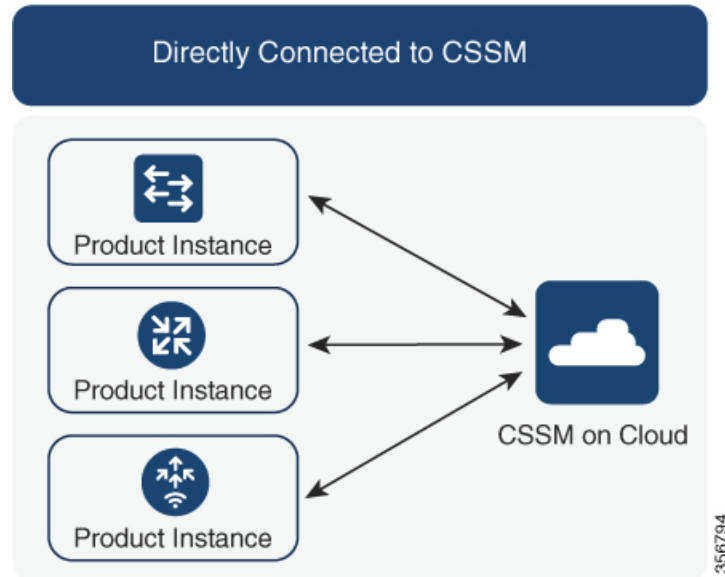
- スマート転送：この方法では、製品インスタンスは特定のスマート転送ライセンスサーバ URL を使用します。これは、ワークフローのセクションに示すとおりを設定する必要があります。
 - HTTPS プロキシを介したスマート転送：この方法では、製品インスタンスはプロキシサーバを使用してライセンスサーバと通信し、最終的には CSSM と通信します。
- Call Home を使用して CSSM と通信する。

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ス環境で使用でき、ポリシーを使用したスマートライセンス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。

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ス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スへの移行後に設定を変更します。



(注) Call Home からスマート転送方式に変更する場合、Smart Licensing Using Policy を期待どおりに機能させるために「CiscoTAC-1」 Call Home プロファイルを無効化する必要はありません。

- 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ス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 \(53 ページ\)](#) 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。

- ユーティリティモード (17.9.1.a 以降で使用可能) で動作しているときにこのトポロジを実装する場合は、スマート転送のみを使用できます。つまり、スマート転送を直接使用するか、HTTP プロキシを介したスマート転送を使用します。Call Home はユーティリティモードではサポートされていません。

リリースごとの変更と拡張 :

このセクションでは、このトポロジに影響するリリースごとのソフトウェアの重要な変更と拡張について概説します。

Cisco IOS XE Cupertino 17.9.1a 以降 :

- Virtual Routing and Forwarding (VRF) のサポート

すべてのライセンスデータを送信するように VRF を設定できます。そのため、製品インスタンスは VRF をサポートするインスタンスである必要があります。このトポロジを実装する場合は、スマート転送オプションのみを使用できます。つまり、スマート転送を直接使用するか、HTTP プロキシを介したスマート転送を使用します。

- RUM レポートスロットリング

このトポロジでは、レポートの最小頻度は1日に制限されます。これは、製品インスタンスが1日に複数の RUM レポートを送信しないことを意味します。これにより、特定のライセンスに対して生成および送信される RUM レポートが多すぎるという問題が解決されます。また、RUM レポートの過剰な生成によって引き起こされたメモリ関連の問題とシステムのスローダウンも解決します。

特権 EXEC モードで **license smart sync** コマンドを入力すると、スロットリングの制限をオーバーライドできます。

RUM レポートスロットリングは、17.3.x トレインの Cisco IOS XE Amsterdam 17.3.6 以降のリリース、および 17.6.x トレインの Cisco IOS XE Bengaluru 17.6.4 以降のリリースにも適用されます。17.9.1 以降、RUM レポートスロットリングは後続のすべてのリリースに適用されます。

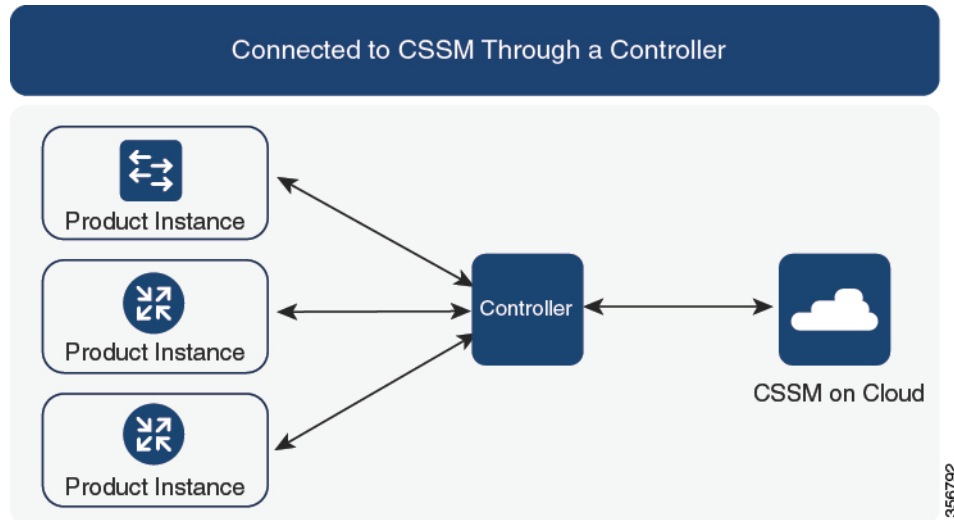
次の手順 :

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 に直接接続 \(53 ページ\)](#) を参照してください。

コントローラを介して CSSM に接続

コントローラを使用して製品インスタンスを管理する場合、コントローラは CSSM に接続して CSSM とのすべての通信のインターフェイスとなります。

図 3: トポロジ : コントローラを介して CSSM に接続



Cisco アグリゲーションルータ、統合型ルータ、およびクラウドサービスルータ、Cisco Catalyst 8000 エッジプラットフォームファミリー、および Cisco ターミナルサービスゲートウェイでは、Cisco DNA Center と Cisco vManage がコントローラとしてサポートされています。実装するコントローラに応じて、トポロジがどのように動作するように設計されているかについては、次の対応する項を参照してください。

コントローラとしての Cisco DNA Center

概要 :

Cisco DNA Center がコントローラとして製品インスタンスを管理している場合、製品インスタンスはライセンスの使用状況を記録し、保存しますが、Cisco DNA Center が RUM レポートを取得し、CSSM に報告し、製品インスタンスにインストールするために ACK を返すために製品インスタンスとの通信を開始します。

Cisco DNA Center で管理する必要があるすべての製品インスタンスは、そのインベントリの一部である必要があり、サイトに割り当てる必要があります。Cisco DNA Center は NETCONF プロトコルを使用して設定をプロビジョニングし、製品インスタンスから必要な情報を取得します。したがって、これを容易にするために製品インスタンスで NETCONF を有効にする必要があります。

レポートの要件を満たすために、Cisco DNA Center は CSSM から該当するポリシーを取得し、次のレポートオプションを提供します。

- **Ad hoc reporting** : 必要に応じてアドホックレポートをトリガーできます。
- **Scheduled reporting** : ポリシーで指定されたレポート頻度に対応し、Cisco DNA Center によって自動的に処理されます。



- (注) 製品インスタンスが定期レポートの対象となる前に、アドホックレポートを少なくとも1回実行する必要があります。

最初のアドホックレポートにより、Cisco DNA Center は、後続の RUM レポートをアップロードする必要があるスマートアカウントとバーチャルアカウントを決定できます。製品インスタンスのアドホックレポートが一度も実行されていない場合は、通知されます。

Cisco DNA Center では、SLAC のインストールと削除ができます。SLAC のインストールと削除は、単一の製品インスタンスでも、複数の製品インスタンスでも実行できます。



- (注) Cisco DNA Center の GUI には、輸出規制ライセンス (HSECK9) と特定の製品インスタンスに対してのみ、SLAC を生成するオプションがあります。表 7: Cisco DNA Center GUI で HSECK9 ライセンスの SLAC 生成をサポートする製品インスタンス (56 ページ) を参照してください。

信頼コードは必要ありません。

考慮事項または推奨事項：

これは、Cisco DNA Center を使用している場合に推奨されるトポロジです。

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：コントローラを介して CSSM に接続 \(55 ページ\)](#) のコントローラとしての [Cisco DNA Center の使用 \(55 ページ\)](#) を参照してください。

コントローラとしての Cisco vManage

概要：

Cisco vManage をコントローラとして使用して製品インスタンスを管理する場合、Cisco vManage は CSSM に接続して CSSM とのすべての通信のインターフェイスとなります。

Cisco vManage はライセンスの使用状況を記録し、RUM レポートを生成し、24 時間ごとに RUM レポートを CSSM に送信します。この時間はポリシーによって決定される固定のレポート間隔であり、変更できません。CSSM から返された RUM ACK も Cisco vManage に送信されます。

製品インスタンスが Cisco vManage によって管理されている場合、製品インスタンスではライセンス使用状況情報の保存や RUM レポートの生成は行われません。

Cisco vManage ポータルでは、エッジデバイスにライセンスを割り当て、使用されているライセンスおよび割り当てに使用可能なライセンスに関する情報を確認できます。



(注) Cisco vManage ポータルには、SLAC のインストールオプションはありません。輸出規制ライセンスまたは 250Mbps を超えるスループットを使用するには、製品インスタンスに必要な CLI コマンドを使用して SLAC を要求してインストールするか、CSSM からファイルをダウンロードして製品インスタンスに同様にインストールする必要があります。

以前のライセンス環境の HSECK9 ライセンスを使用している場合は、ポリシーを使用したスマートライセンスへの移行後に同じライセンスがサポートされます。この場合、SLAC を再度インストールする必要はありません。

SLAC のインストールの詳細については、「[コントローラとしての Cisco vManage の使用](#)」を参照してください。

Cisco vManage でライセンス管理を処理する方法の詳細については、Cisco SD-WAN スタートアップガイドの「[License Management for Smart Licensing Using Policy](#)」セクションを参照してください。

考慮事項または推奨事項：

これは、Cisco vManage を使用している場合に推奨されるトポロジです。

Cisco IOS XE Bengaluru 17.5.1a 以降：Cisco SD-WAN は CSSM と連携して動作し、Cisco SD-WAN で動作するデバイスに対して Cisco vManage によるライセンス管理を提供します。

Cisco IOS XE Amsterdam 17.3.2 ~ Cisco IOS XE Bengaluru 17.4.x：Cisco vManage はコントローラとしてサポートされていますが、ライセンス管理はサポートしていません。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、ポリシーを使用したスマートライセンスの他の機能をサポートしていません。

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：コントローラを介して CSSM に接続 \(55 ページ\)](#) の「[コントローラとしての Cisco vManage の使用](#)」を参照してください。

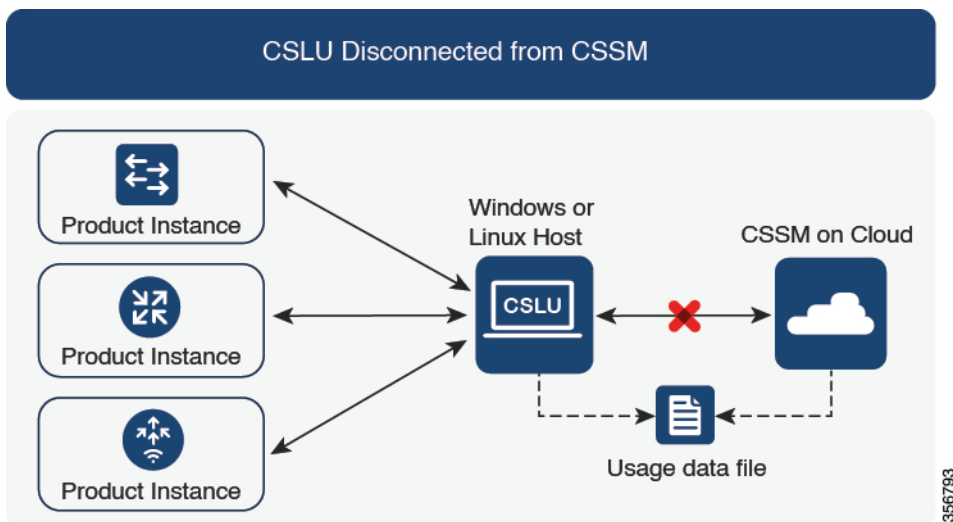
CSLU は CSSM から切断

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 4: トポロジ: CSLU は CSSM から切断



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。

リリースごとの変更と拡張 :

このセクションでは、このトポロジに影響するリリースごとのソフトウェアの重要な変更と拡張について概説します。

Cisco IOS XE Cupertino 17.7.1a 以降 :

- 信頼コードの要求とインストール

信頼コードが製品インスタンスで使用できない場合、製品インスタンスは、CSLU に送信される RUM レポートの一部として要求を検出し、自動的にその要求を含めます。この要求は、CSSM にアップロードされます。CSSM からダウンロードする ACK には信頼コードが含まれています。出荷時にインストールされた既存の信頼コードがある場合は、自動的に上書きされます。この方法で取得した信頼コードは、CSSM との通信に使用できません。

これは、スタンドアロンおよび高可用性設定でサポートされます。高可用性設定では、アクティブな製品インスタンスは、信頼コードが使用できないメンバーやスタンバイの信頼コードを要求します。

このリリースでは、この拡張は、製品インスタンス開始モードにのみ適用されます。

Cisco IOS XE Cupertino 17.9.1a 以降 :

- 信頼コードの要求とインストール

このリリースから、信頼コードの要求とインストールはCSLU開始モードでもサポートされています。

- Virtual Routing and Forwarding (VRF) のサポート

すべてのライセンスデータを CSLU に送信するように VRF を設定できます。そのため、製品インスタンスは VRF をサポートするインスタンスである必要があります。また、このトポロジを実装する場合は、製品インスタンス開始モードを実装する必要があります。

- RUM レポートスロットリング

製品インスタンス開始モードでは、レポートの最小頻度は1日に制限されます。これは、製品インスタンスが1日に複数の RUM レポートを送信しないことを意味します。これにより、特定のライセンスに対して生成および送信される RUM レポートが多すぎるという問題が解決されます。また、RUM レポートの過剰な生成によって引き起こされたメモリ関連の問題とシステムのスローダウンも解決します。

特権 EXEC モードで **license smart sync** コマンドを入力すると、スロットリングの制限をオーバーライドできます。

RUM レポートスロットリングは、17.3.x トレインの Cisco IOS XE Amsterdam 17.3.6 以降のリリース、および 17.6.x トレインの Cisco IOS XE Bengaluru 17.6.4 以降のリリースにも適用されます。17.9.1 以降、RUM レポートスロットリングは後続のすべてのリリースに適用されます。

次の手順：

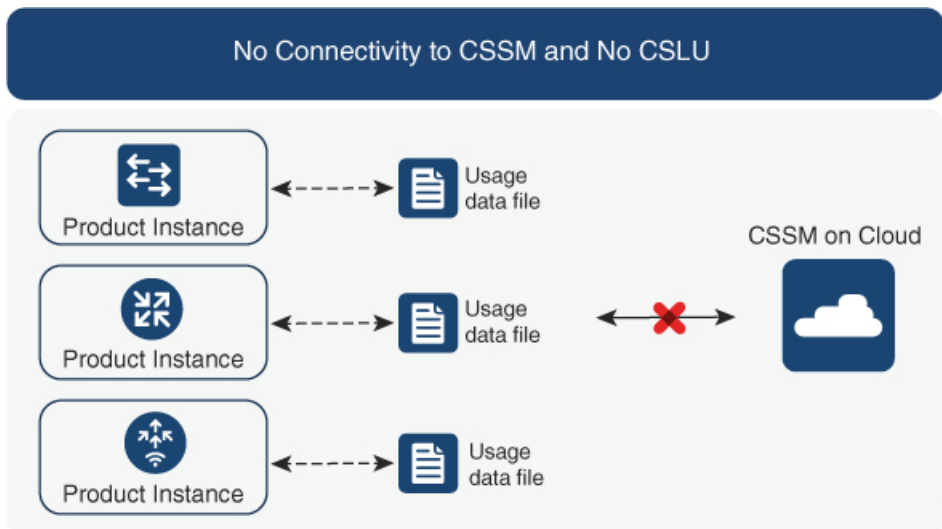
このトポロジを実装するには、[トポロジのワークフロー：CSLU は CSSM から切断（59 ページ）](#) を参照してください。

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。これらのファイルは、RUM レポート、UDI に関連付けられた信頼コードの要求、および SLAC 要求ファイルです。

図 5: 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。

リリースごとの変更と拡張

このセクションでは、このトポロジに影響するリリースごとのソフトウェアの変更と拡張について概説します。

Cisco IOS XE Cupertino 17.7.1a 以降 :

- 信頼コードの要求とインストール

製品インスタンスで信頼コードが使用できない場合、製品インスタンスは、ユーザーが保存し、CSSM にアップロードする RUM レポートに信頼コードの要求を自動的に含めます。CSSM からダウンロードする ACK には信頼コードが含まれています。

出荷時にインストールされた信頼コードがある場合、ACK をインストールすると自動的に上書きされます。この方法で取得した信頼コードは、CSSM とのセキュアな通信に使用できます。

これは、スタンドアロンおよび高可用性設定でサポートされます。高可用性設定では、アクティブな製品インスタンスは、信頼コードが使用できないすべての接続製品インスタンスの信頼コードを要求します。

- SLAC 要求とインストール

SLAC 要求を生成し、製品インスタンスのファイルに保存できます。保存されたファイルには、必要なすべての詳細 (UDI、ライセンス情報など) が含まれます。この方法では、SLAC を生成するために CSSM Web UI で必要な詳細情報を収集して入力する必要はありません。RUM レポートおよび ACK と同様に、SLAC 要求ファイルを CSSM にアップロー

ドし、SLAC コードを含むファイルをダウンロードして製品インスタンスにインストールする必要があります。

同様に、SLAC を返却する場合、正しいバーチャルアカウントの製品インスタンスを見つける必要はありません。RUM レポートと同様に、SLAC 返却ファイルをアップロードします。

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：CSSM への接続なし、CSLU なし \(63 ページ\)](#) を参照してください。

SSM オンプレミス展開

概要：

SSM オンプレミスは、オンプレミスに展開される CSSM の拡張として機能するように設計されています。

ここでは、製品インスタンスが SSM オンプレミスに接続され、SSM オンプレミスが CSSM との単一のインターフェイスポイントになります。SSM オンプレミスの各インスタンスは、SSM オンプレミスのローカルアカウントに必須の登録と同期を通じて、CSSM 内のバーチャルアカウントを使用して CSSM に通知する必要があります。

製品インスタンスを管理するために SSM オンプレミスを展開する場合、SSM オンプレミスに必要な情報をプッシュするように製品インスタンスを設定できます。または、設定可能な頻度で製品インスタンスから必要な情報をプルするように SSM オンプレミス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 SSM オンプレミスの REST エンドポイントを接続することで SSM オンプレミス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。

このモードでの製品インスタンスと SSM オンプレミス間の通信のオプション：

- 必要に応じて、CLI コマンドを使用して SSM オンプレミスに情報をプッシュします。
- スケジュールされた頻度で RUM レポートを SSM オンプレミスに自動的に送信するには、CLI コマンドを使用し、レポート間隔を設定します。

- **SSM オンプレミス開始型通信（プル）**：製品インスタンスからの情報の取得を開始するには、SSM オンプレミスで NETCONF、RESTCONF、およびネイティブの REST API オプションを使用して製品インスタンスを接続します。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。

このモードでの製品インスタンスと SSM オンプレミス間の通信のオプション：

- 必要に応じて（オンデマンドで）、1つ以上の製品インスタンスから使用状況情報を収集します。
- スケジュールされた頻度で1つ以上の製品インスタンスから使用状況情報を収集します。

SSM オンプレミスでは、レポート間隔が製品インスタンスのデフォルトポリシーに設定されます。これは変更できますが、より頻繁に（より短い間隔で）レポートを作成するか、または使用可能な場合はカスタムポリシーをインストールできます。

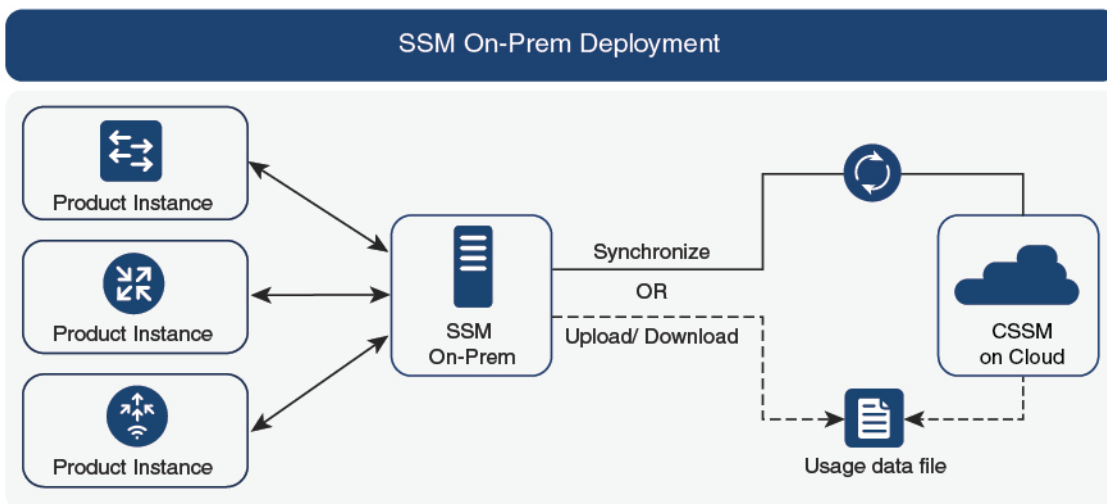
SSM オンプレミスで使用状況が使用できるようになったら、同じ間隔で CSSM と同期して、製品インスタンス数、ライセンス数、およびライセンス使用状況情報が CSSM と SSM オンプレミスの両方と同じであることを確認します。SSM オンプレミスと CSSM 間の使用状況の同期オプション：プッシュとプルモードの場合：

- CSSM でアドホック同期を実行します（Cisco と同期されました）。
- 指定した時刻で CSSM との同期をスケジュールします。
- オフラインで保存されている指名済みファイルを通じて CSSM と通信し、場合によって SSM オンプレミスまたは CSSM からアップロードするか、またはダウンロードします。



(注) このトポロジでは、SSM オンプレミスと CSSM 間で2つの異なる同期が行われます。1つは、ローカルアカウントと CSSM との同期です。この同期は、SSM オンプレミスインスタンスに CSSM を認識させるためであり、SSM オンプレミスの [Synchronization] ウィジェットを使用して実行します。2番目は、CSSM に接続するか、またはファイルをダウンロードおよびアップロードすることのいずれかによるライセンスの使用状況の CSSM との同期です。ライセンスの使用状況を同期する前に、ローカルアカウントを同期する必要があります。

図 6: トポロジ: SSM オンプレミス展開



357508

考慮事項または推奨事項：

- このトポロジは、次の状況に適しています。
 - CSSM と直接通信せずにオンプレミスで製品インスタンスを管理する場合。
 - 会社のポリシーにより、製品インスタンスでライセンスの使用状況をシスコ（CSSM）に直接報告できない場合。
 - 製品インスタンスがエアギャップネットワーク内にあり、ネットワーク外にあるものとオンラインで通信できない場合。
- Smart Licensing Using Policy のサポートとは別に、SSM オンプレミスのバージョン 8 の主な利点は次のとおりです。
 - マルチテナント：1 つのテナントが 1 つのスマートアカウントとバーチャルアカウントのペアを構成します。SSM オンプレミスでは複数のペアを管理できます。ここでは、SSM オンプレミスに存在するローカルアカウントを作成します。CSSM のスマートアカウントとバーチャルアカウントのペアへの複数のローカルアカウントのロールアップ。詳細については、『[Cisco Smart Software Manager On-Prem User Guide](#)』 [英語] の「About Accounts and Local Virtual Accounts」を参照してください。



(注) CSSM と SSM オンプレミスのインスタンス間の関係は、まだ 1 対 1 です。

- スケール：合計 300,000 の製品インスタンスをサポートします。
- 高可用性：2 台の SSM オンプレミスサーバをアクティブ/スタンバイクラスタの形式で実行できます。詳細については、『[Cisco Smart Software On-Prem Installation Guide](#)』 [英語] の「Appendix 4 Managing a High Availability (HA) Cluster in Your System」を参照してください。
高可用性展開は SSM オンプレミスのコンソールでサポートされており、必要なコマンドの詳細については『[Cisco Smart Software On-Prem Console Guide](#)』で確認できます。
- CSSM へのオンライン接続とオフライン接続のオプション。
- SSM オンプレミスの制限：
 - ライセンス使用の同期を目的とした CSSM との通信のプロキシサポートが利用できるのは、バージョン 8.202108 以降のみです。ローカルアカウントの同期を目的とするプロキシの使用はサポートされています。これは [Synchronization] ウィジェットを使用して実行され、Smart Licensing Using Policy がサポートされている SSM オンプレミス導入リリースから利用可能です。
 - SSM オンプレミス開始型通信は、ネットワークアドレス変換（NAT）設定の製品インスタンスではサポートされていません。製品インスタンス開始型通信を使用する必要があります。さらに、NAT 設定の製品インスタンスをサポートするために SSM オ

ンプレミスを有効にする必要があります。詳細は、このトポロジのワークフローで提供されます。

リリースごとの変更と拡張 :

このセクションでは、このトポロジに影響するリリースごとのソフトウェアの重要な変更と拡張について概説します。

Cisco IOS XE Cupertino 17.9.1a 以降 :

- Virtual Routing and Forwarding (VRF) のサポート

すべてのライセンスデータを CSLU に送信するように VRF を設定できます。そのため、製品インスタンスは VRF をサポートするインスタンスである必要があります。また、このトポロジを実装する場合は、製品インスタンス開始モードを実装する必要があります。

- RUM レポートスロットリング

製品インスタンス開始モードでは、レポートの最小頻度は1日に制限されます。これは、製品インスタンスが1日に複数の RUM レポートを送信しないことを意味します。これにより、特定のライセンスに対して生成および送信される RUM レポートが多すぎるという問題が解決されます。また、RUM レポートの過剰な生成によって引き起こされたメモリ関連の問題とシステムのスローダウンも解決します。

特権 EXEC モードで **license smart sync** コマンドを入力すると、スロットリングの制限をオーバーライドできます。

RUM レポートスロットリングは、17.3.x トレインの Cisco IOS XE Amsterdam 17.3.6 以降のリリース、および 17.6.x トレインの Cisco IOS XE Bengaluru 17.6.4 以降のリリースにも適用されます。17.9.1 以降、RUM レポートスロットリングは後続のすべてのリリースに適用されます。

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 : SSM オンプレミス展開 \(65 ページ\)](#) を参照してください。

SSM オンプレミスの既存のバージョンから移行する場合は、アップグレード関連のさまざまなアクティビティを実行する順序が重要です。[Smart Licensing Using Policy をサポートする SSM オンプレミスのバージョンへの移行 \(169 ページ\)](#) を参照してください。

ユーティリティモード

概要 :

これは、必要なライセンスの前払いではなく、ライセンスの実際の使用量に対して支払う後払いモデルであり、[MSLA](#) によって管理されます。

製品インスタンスはサブスクリプションIDを持つライセンスを使用し、「ユーティリティモード」で有効になっています。製品インスタンスは、すべてのライセンスワークフローを完了するために、CSSM と直接、または CSLU や SSM オンプレミスを介して相互作用するように構成するか、切断モードで動作するように構成できます。製品インスタンスとの通信には、ユーティリティモードで動作していることを示すフラグが設定されます。MSLA の使用量が CSSM に達すると、使用量に応じて課金されます。

ユーティリティモードの製品インスタンスでは、30 日ごとに ACK をインストールする必要があります。レポートをタイムリーに作成するために、レポートの間隔は7日以内にすることを推奨します。

ユーティリティモードで実装できるトポロジは次のとおりです。

- [CSSM に直接接続 \(21 ページ\)](#)

ユーティリティモードでこのトポロジを実装する場合は、スマート転送のみを使用できます。つまり、スマート転送を直接使用するか、HTTP プロキシを介したスマート転送を使用します。

- [CSLU を介して CSSM に接続 \(19 ページ\)](#)、[CSLU は CSSM から切断 \(26 ページ\)](#)

- [SSM オンプレミス展開 \(30 ページ\)](#)

- [CSSM への接続なし、CSLU なし \(28 ページ\)](#)

考慮事項または推奨事項：

- **CCW** でプリペイドライセンスを注文する場合、後払いの HSECK9 ライセンスは注文できません。このライセンスはプリペイドライセンスのみです。
- サードパーティの課金プラットフォームに使用状況レポートを送信することはできません。使用できるサポートされている代替手段は、CSLU または SSM オンプレミスを実装することです。実装すると CSSM に送信されます。
- CSLU または SSM オンプレミスを実装する予定の場合は、Smart Licensing Using Policy 環境に、MSLA 対応の必要な最小バージョンをインストールしてください。
 - CSLU の場合：バージョン 2.0.0
 - SSM オンプレミスの場合：バージョン 8、リリース 202206

次の手順：

サポートされるトポロジの 1 つを実装します。



(注) ワークフローのステップはすべて、特に明記されていない限り、ユーティリティモードに適用されます。

[トポロジのワークフロー：CSSM に直接接続 \(53 ページ\)](#)

トポロジのワークフロー：CSLU を介して CSSM に接続 (49 ページ)

トポロジのワークフロー：CSLU は CSSM から切断 (59 ページ)

トポロジのワークフロー：CSSM への接続なし、CSLU なし (63 ページ)

トポロジのワークフロー：SSM オンプレミス展開 (65 ページ)

他の機能との相互作用

ハイ アベイラビリティ

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ス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

デュアルシャーシセットアップ⁹ (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¹⁰。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。



(注) Cisco vManage を使用して製品インスタンスを管理する場合、すべてのデバイスにライセンスが必要です。高可用性はサポートされていません。

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。

- 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 ではなく) シャーシにある場合です。
- 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、アクティブな場合のみ承認コードが必要です。

⁹ 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。

¹⁰ 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ドスーパーバイザが、このようなセットアップの例です。

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。

上記のいずれかのイベントが発生すると、**show license status** 特権EXECコマンドの [Next report push] の日付が更新されます。ただし、レポートが製品インスタンスによって送信されるかどうかは、実装されたトポロジと関連するレポート方法で決まります。たとえば、製品インスタンスが切断されているトポロジ ([Transport Type] が [Off]) を実装した場合は、[Next report push] の日付が更新されても、製品インスタンスは RUM レポートを送信しません。

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

このセクションでは、次の点について説明します。

- 以前のライセンスモデルから **Smart Licensing Using Policy** への移行

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ス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ス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。この [ポリシーを使用したスマートライセンスへの移行（73 ページ）](#) セクションでは、移行シナリオの例を示します。

- **Smart Licensing Using Policy** 環境でのアップグレード：アップグレード元のソフトウェアバージョンとアップグレード先のソフトウェアバージョンの両方で、**Smart Licensing Using Policy** がサポートされます。

アップグレード前に現在のライセンスモデルを識別する

ポリシーを使用したスマートライセンスにアップグレードする前に、製品インスタンスで有効な現在のライセンスモデルを確認するには、特権 EXEC モードで `show license all` コマンドを入力します。このコマンドにより、RTU ライセンスモデルを除くすべてのライセンスモデルに関する情報が表示されます。show license right-to-use 特権 EXEC コマンドでは、ライセンスモデルが RTU の場合にのみライセンス情報が表示されます。

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ス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。

PAK ライセンスを使用している場合は、システムによる PAK ライセンスの処理方法の変更と、使用可能なオプションをよく理解してください。詳細については、[PAK ライセンスのスナップショット \(43 ページ\)](#) 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 \(216 ページ\)](#) 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、一般的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。アップグレード前に、製品インスタンスがスマートアカウントに登録されており、CSSM には 250 Mbps を超えるスループットが許可されるように輸出規制フラグのみが有効になっていて、輸出規制ライセンス (HSECK9) が有効になっていない場合は、Smart Licensing Using Policy への移行の一部として、さらにいくつかの手順を実行する必要があります。これは、米国の輸出規制により、250 Mbps を超えるスループットを許可する方法として輸出規制フラグのみの使用が許可されなくなったためです。

- 仮想製品インスタンス (Cisco Cloud Services Router 1000v (CSR 1000v) または Cisco Integrated Services Virtual Router (ISRv)) でスループットが 250 Mbps を超え、CSSM で輸出規制フラグのみが有効になっている場合は、設定の要件に従って手順を進めます。
 - [SLR](#) 設定のスループットが 250 Mbps を超える CSR 1000v または ISRv : 最初に SLR 承認コードを更新して、該当する HSECK9 ライセンスを含めてから、製品インスタンスのみをアップグレードします。これにより、アップグレード後もスループットが中断されなくなります。



- (注) このシナリオでは、最初に SLR 承認コードを更新せずにソフトウェアイメージをアップグレードして HSECK9 ライセンスを含めると、Smart Licensing Using Policy へのアップグレード後は、SLAC がインストールされるまで、スループットが 250 Mbps に設定されます。SLAC のインストール後すぐに、最後に設定した値が復元されます。

製品固有の HSECK9 ライセンスの名前については、[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 \(253 ページ\)](#) を参照してください。移行シナリオ例については、[例：スマートライセンス \(スループットが 250 Mbps を超える SLR、輸出規制ライセンスなし\)](#) から [Smart Licensing Using Policy へ \(110 ページ\)](#) を参照してください。

- [CSSM](#) に接続され、[自律モード](#)のスループットが 250 Mbps を超える CSR 1000v または ISRv : 250 Mbps を超えるスループットがスタートアップコンフィギュレーションの一部であることを確認します。また、CSSM 内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で該当する HSECK9 ライセンスのバランスがプラスであることも確認します。アップグレード前のアクションは必要ありません。

製品インスタンスがCSSMに接続されている限り、アップグレード時に製品インスタンスは自動的にHSECK9要求をトリガーし、SLACをインストールします。

- スループットが 250 Mbps を超え、CSSM に輸出規制フラグのみが設定されており、CSSM に接続されている自立モードの物理製品インスタンス（Cisco 1000 シリーズ サービス統合型ルータ（ISR 1000）、Cisco 4000 シリーズ サービス統合型ルータ（ISR 4000）、またはCisco 1000 シリーズ アグリゲーションサービスルータ（ASR 1000））の場合：**license feature hseck9** コマンドがスタートアップ コンフィギュレーションに設定されており、CSSM内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で該当するHSECK9ライセンスのバランスがプラスであることを確認します。アップグレード前のアクションは必要ありません。アップグレード時に製品インスタンスがCSSMに接続されている限り、製品インスタンスは自動的にHSECK9要求をトリガーし、SLACをインストールします。
- 物理製品インスタンスまたは仮想製品インスタンスの場合、CSSMで輸出規制フラグのみを使用して 250 Mbps を超えるスループットがあり、SD-WAN コントローラモードで動作している場合：アップグレード後にSLACを要求してインストールする必要があります。アップグレードが完了したら、[CSSMからのSLACの生成とファイルへのダウンロード（214ページ）](#) を実行し、次に製品インスタンスへのファイルのインストール（231ページ）を実行します。

対照的に、輸出規制ライセンスが以前のライセンス環境にある次のシナリオでは、アップグレード後にSLACを再度インストールする必要がないことに注意してください。

- 製品インスタンス（Cisco 1000 シリーズ サービス統合型ルータやCisco 4000 シリーズ サービス統合型ルータなど）に、スマートアカウントに登録されたHSECK9ライセンスがあり、CSSMで輸出規制フラグが有効になっている場合、ポリシーを使用したスマートライセンスにアップグレード後に、承認コードが適用されます。ライセンス使用状況情報は、アップグレード後にのみCSSMと同期する必要があります。SLACを再度インストールする必要はありません。例：[スマートライセンス（登録済みおよび承認済みのライセンス）から Smart Licensing Using Policyへ（77ページ）](#) を参照してください。
- アップグレード前に製品インスタンスにHSECK9 PAK ライセンスが存在した場合、アップグレード後にSLACを再度インストールする必要はありません。例：[Cisco ソフトウェアライセンス（PAK ライセンス）から Smart Licensing Using Policyへ（140ページ）](#) を参照してください。

PAK ライセンスを使用している場合は、システムによる PAK ライセンスの処理方法の変更と、使用可能なオプションをよく理解してください。詳細については、[PAK ライセンスのスナップショット（43ページ）](#) を参照してください。

- 製品インスタンスにHSECK9ライセンスを含むSLR承認コードが含まれていた場合、ポリシーを使用したスマートライセンスにアップグレード後にライセンスが適用されるため、SLACを再度インストールする必要はありません。例：[スマートライセンス（輸入規制ライセンスを使用したSLR）から Smart Licensing Using Policyへ（93ページ）](#) 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レポートに与える影響

既存ライセンス	ポリシーを使用したスマートライセンスへの移行後のレポート要件
使用权 (RTU)	使用されているライセンスによって異なります。 サポートされるトポロジの移行および展開後、 show license usage コマンドの出力で <code>Next ACK deadline</code> フィールドを参照して、レポートが必要かどうか、およびいつ必要かを確認します。
スマートライセンス (登録および承認済みライセンス)	ポリシーによって異なります。
特定のライセンス予約 (SLR)	ライセンス消費に変更がある場合にのみ必要です。 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ス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。
製品認証キー (PAK)	ライセンス消費に変更がある場合にのみ必要です。 PAK ライセンスには永続的な有効期間がありますが、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。 また、システムによる PAK ライセンスの処理方法の変更と、使用可能なオプションをよく理解してください。詳細については、 PAK ライセンスのスナップショット (43 ページ) を参照してください。
パーマネントライセンス予約 (PLR)	不要。 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ス (CSL)	不要。 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。
評価ライセンスまたは期限切れライセンス	シスコのデフォルトポリシーのレポート要件に基づいています。

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スへのアップグレード後も転送タイプが保持されます。

スマートライセンス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ス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スのデフォルト)
	SLR PLR	off
	登録	callhome
smart	評価	off
	SLR PLR	off
	登録	smart
N/A たとえば、既存のライセンスモデルが RTU または PAK の場合。	N/A たとえば、既存のライセンスモデルが RTU または PAK の場合。	cslu

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スでは、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、Smart Licensing Using Policy では不要です。トークン生成機能は、CSSMで引き続き使用でき、Smart Licensing Using Policy 環境の特定のトポロジで信頼を確立するために使用されます。

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スに関する追加の考慮事項は適用されません。

Smart Licensing Using Policy 環境内のアップグレード

この項では、Smart Licensing Using Policy がサポートされているリリースから Smart Licensing Using Policy がサポートされているリリースに製品インスタンスをアップグレードする場合に適用される、リリース固有の考慮事項またはアクションについて説明します。

Cisco IOS XE Cupertino 17.7.1a 以降、RUM レポートは処理時間を短縮する形式で保存されます。古い形式と新しい形式の違いによって生じる使用状況レポートの不整合を避けるために、Smart Licensing Using Policy をサポートする以前のリリースから Cisco IOS XE Cupertino 17.7.1a 以降のリリースにアップグレードする場合は、標準的な方法として1回の使用状況レポートを完了することをお勧めします。

ダウングレード

ここでは、以前のライセンスモデルへのダウングレードについて説明します。また、Smart Licensing Using Policy 環境内のダウングレードに関連する情報についても説明します。

新規展開のダウングレード

このセクションでは、Smart Licensing Using Policy がデフォルトで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、Smart Licensing Using Policy 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された場合に適用される考慮事項とアクションについて説明します。

ダウングレードの結果は、Smart Licensing Using Policy 環境での操作中に信頼コード (信頼コード (17 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。ダウングレード先のリリースによっては、さらにアクションが必要になる場合があります。

ポリシーを使用したスマートライセンス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。そのため、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、スマートライセンス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。次の表を参照してください。

- ポリシーを使用したスマートライセンス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ス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ス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、スマートライセンス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。

Smart Licensing Using Policy 環境内のダウングレード

この項では、Smart Licensing Using Policy がサポートされているリリースから Smart Licensing Using Policy がサポートされている別のリリースに製品インスタンスをダウングレードする場合に適用される、リリース固有の考慮事項またはアクションについて説明します。

Cisco IOS XE Cupertino 17.7.1a 以降、RUM レポートは処理時間を短縮する形式で保存されます。古い形式と新しい形式の違いによって生じる使用状況レポートの不整合を避けるために、Cisco IOS XE Cupertino 17.7.1a 以降のリリースから Smart Licensing Using Policy をサポートする

以前のリリースにダウングレードする際に、1回の使用状況報告を完了することをお勧めします。

従来のライセンスの変更点

ここでは、Smart Licensing Using Policy 環境で引き続きサポートされるために、特定の従来のライセンスで実施されている変更について説明します。変更には、自動的に実行されるアクション、ユーザーが実行する必要があるアクション、または両方のアクションが含まれる場合があります。適宜呼び出されます。

PAK ライセンスのスナップショット

システムの製品アクティベーションキー (PAK) ライセンスの処理方法は大幅に変更されています。ここでは、変更内容、変更がユーザーに与える影響、実行する必要があるアクション (ある場合)、および PAK ライセンス所有者が利用できるオプションについて説明します。

PAK ライセンスとは

PAK フルフィルメントを使用して発行されるライセンスは、PAK ライセンスと呼ばれます。たとえば、Cisco ASR 1000 で使用可能な「adventerprise」ライセンスは PAK 履行済みにすることができ、Cisco 4000 シリーズ ISR で使用できる「securityk9」ライセンスも PAK 履行済みにできます。同様に、さまざまなシスコルータで利用可能な HSECK9 ライセンスは、PAK 履行済みにできます。

PAK ライセンスの変更点：PAK ライセンスのスナップショット

Cisco IOS XE Dublin 17.11.1a 以降、PAK ライセンスを管理するライブラリはソフトウェアイメージから削除されています。既存の PAK ライセンスを引き続きサポートおよび受け入れるために、次のアクションが自動的に実行されます。

- PAK ライセンスのスナップショットが作成されます。このスナップショットは、スナップショットの時点における PAK ライセンスの永続的な記録として機能します。
- Device-Led Conversion (DLC) プロセスがトリガーされます。DLC 後、PAK 履行済みライセンスをスマートアカウントで使用できます。

製品インスタンスで実行されているソフトウェアバージョンが次のいずれかである場合にのみ、PAK ライセンスのスナップショットが作成されます。

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



注意 前述のリリースおよびトレイン以前の場合のみ、PAK ライセンスのスナップショットが作成されます。Cisco IOS XE Dublin 17.11.1a 以降、PAK 管理ライブラリは廃止され、スナップショットを作成するためのプロビジョニングは利用できなくなりました。Cisco IOS XE Dublin 17.11.1a 以降のソフトウェアイメージは、PAK ライセンスに関するスナップショット情報のみに依存しています。

スナップショットのない PAK ライセンスがあり、Cisco IOS XE Dublin 17.11.1a 以降のリリースにアップグレードする場合は、2回アップグレードする必要があります。まず、PAK ライセンスのスナップショットと完全な DLC が作成される前述のリリースのいずれかにアップグレードしてから、必要な後続のリリースに再度アップグレードします。

PAK のパーマネントライセンスのみが受け入れられ、PAK の評価ライセンスは受け入れられません。

スナップショットが作成されると、PAK ライセンスへの変更はサポートされなくなります。スナップショットの作成後に、ソフトウェアバージョンを以前のリリースにダウングレードし、PAK ライセンスに変更を加え（返却を含む）、後続のリリースに戻した場合でも、PAK ライセンスの変更はサポートされません。

製品インスタンスの PAK ライセンスのスナップショットが作成されているか確認するには、特権 EXEC モードで **show platform software sl-infra pak-info** コマンドを入力します。スナップショットが作成されている場合、コマンドの出力に次の情報が表示されます。

```
Device# show platform software sl-infra pak-info
<output truncated>
```

```
Pak License Snapshot Information
=====
Platform Supports PAK License snapshot
PAK License Snapshot integrity check pass
PAK License Snapshot available
```

```
<output truncated>
```

PAK ライセンスをサポートする製品インスタンス

以下の製品インスタンスは PAK ライセンスをサポートしています。以下の製品インスタンスのいずれかを使用しており、製品インスタンスで PAK ライセンスが使用されている場合は、「PAK ライセンスで利用可能なオプション」を参照して、実行可能な内容の詳細を確認してください。

- 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 クラウド サービス ルータ 1000v

- Catalyst 8000V エッジソフトウェア（シスコクラウドサービスルータ 1000v であり、Cisco IOS XE Bengaluru 17.4.1 以降のリリースへの .bin アップグレードが実行されている場合のみ）

PAK ライセンスで利用可能なオプション

PAK ライセンスを所有している場合は、次の方法で続行できます。



(注) 製品インスタンスに複数の PAK ライセンスがある場合は、すべてのライセンスの使用を継続するか、すべてのライセンスを削除して返却します。所有している PAK ライセンスを変更する必要があると思う場合は、すべての PAK ライセンスを削除し、製品インスタンスでスマートライセンスを設定して、最初からやり直してください。

- PAK ライセンスがあり、変更を加えずに製品インスタンスで引き続き使用する場合は、[PAK ライセンスの使用を継続する \(238 ページ\)](#) を参照してください。
- 製品インスタンスに PAK ライセンスがあり、そのライセンスを削除する場合は、[PAK ライセンスの削除 \(240 ページ\)](#) を参照してください。
- 障害が発生した製品インスタンスに PAK ライセンスがあり、ライセンスを返却または削除する場合は、[障害が発生した製品インスタンスの PAK ライセンスの削除 \(242 ページ\)](#) を参照してください。

Smart Licensing Using Policy 環境のパーマネントライセンス予約

パーマネントライセンス予約とは

パーマネントライセンス予約 (PLR) を使用すると、製品インスタンスの任意のライセンスを無制限に使用できます。PLR コードは、CSSM によって生成される承認コードであり、ライセンス要求を認証するために製品インスタンスにインストールする必要があります。

PLR 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または完全なエアギャップネットワークに適しています。

Smart Licensing Using Policy 環境における PLR の要件

Smart Licensing Using Policy 環境で PLR を使用するためには、次のものがが必要です。

- ソフトウェアバージョン：Cisco IOS XE Dublin 17.10.1a 以降。
- PLR コードのバージョン 3。

Smart Licensing Using Policy 環境で PLR をサポートする製品インスタンス

- Catalyst 8000V エッジソフトウェア

- シスコ クラウド サービス ルータ 1000v (CSRv イメージから Catalyst 8000V ソフトウェア イメージに .bin アップグレード済み)

既存の PLR の処理方法 : アップグレードとダウングレード

現在のセットアップ	条件 (このアクションが実行された場合)	結果と影響
<p>製品インスタンス : シスコ クラウド サービス ルータ 1000v</p> <p>PLR ステータス : PLR がアクティブ化されています。古いバージョン (バージョン 1 またはバージョン 2) の PLR コードがインストールされています。</p> <p>ソフトウェアバージョン : Cisco IOS XE Everest 16.5.x から Cisco IOS XE Amsterdam 17.3.x。</p>	<p>ソフトウェアバージョン Cisco IOS XE Dublin 17.10.1a 以降のリリースへの .bin アップグレードを実行します。</p>	<p>250 Mbps を超えるスループットと、HSECK9 ライセンスが必要な輸出規制機能を除き、有効になっている既存の機能はすべて受け入れられ、引き続き機能します。</p> <p>古いバージョンの PLR コードは製品インスタンスから削除されませんが、サポートされません。</p> <p>スループットを復元し、HSECK9 ライセンスを使用するには、PLR コードをバージョン 3 にアップグレードします。 PLR のアップグレード (248 ページ) を参照してください。</p>

現在のセットアップ	条件 (このアクションが実行された場合)	結果と影響
<p>製品インスタンス：シスコクラウドサービスルータ 1000v</p> <p>PLR ステータス：PLR がアクティブ化されています。古いバージョン（バージョン1またはバージョン2）の PLR コードがインストールされています。</p> <p>ソフトウェアバージョン：Cisco IOS XE Everest 16.5.x から Cisco IOS XE Amsterdam 17.3.x。</p>	<p>Cisco IOS XE Bengaluru 17.4.x と Cisco IOS XE Cupertino 17.9.x の間のリリースへの .bin アップグレードを実行します。</p>	<p>250 Mbps を超えるスループットと、HSECK9 ライセンスが必要な輸出規制機能を除き、有効になっている既存の機能はすべて受け入れられ、引き続き機能します。</p> <p>古いバージョンの PLR コードは製品インスタンスから削除されませんが、サポートされません。</p> <p>PLR を使用するには、ソフトウェアバージョンを Cisco IOS XE Dublin 17.10.1a にアップグレードしてから、PLR コードをバージョン3 にアップグレードする必要があります。</p> <p>PLR のアップグレード (248 ページ) を参照してください。</p>
<p>製品インスタンス：シスコクラウドサービスルータ 1000v ルータ (Catalyst 8000V ソフトウェアイメージに .bin アップグレード済み)</p> <p>PLR ステータス：PLR がアクティブ化されています。PLR コードのバージョン3 がインストールされています。</p> <p>ソフトウェアバージョン：Cisco IOS XE Dublin 17.10.1a 以降。</p>	<p>Cisco IOS XE Amsterdam 17.3.x 以前のリリースにダウングレードします。</p>	<p>ダウングレード後、古いバージョンのソフトウェアイメージで PLR コードバージョン3 を検証できず、受け入れもサポートもできません。</p> <p>製品インスタンスは、ライセンスがインストールされていないかのように動作します。</p> <p>PLR コードは製品インスタンスから削除されません。</p>

現在のセットアップ	条件 (このアクションが実行された場合)	結果と影響
<p>製品インスタンス：シスコクラウドサービスルータ 1000v ルータ (Catalyst 8000V ソフトウェアイメージに .bin アップグレード済み)</p> <p>PLR ステータス：PLR アップグレードは完了していません。古いバージョン (バージョン1またはバージョン2) の PLR コードがインストールされています。</p> <p>ソフトウェアバージョン：Cisco IOS XE Dublin 17.10.1a 以降。</p>	Cisco IOS XE Amsterdam 17.3.x 以前のリリースにダウングレードします。	ダウングレード後、古いバージョンのソフトウェアイメージで PLR コードを検証し、コードを使用してライセンス要求を満たすことができます。

Smart Licensing Using Policy 環境での PLR のアクティブ化、アップグレード、非アクティブ化

- Catalyst 8000V エッジソフトウェアに PLR を実装する場合は、[PLR のアクティブ化 \(242 ページ\)](#) を参照してください。
- シスコクラウドサービスルータ 1000v ルータで .bin アップグレードを実行していて、PLR の使用を継続する場合は、[PLR のアップグレード \(248 ページ\)](#) を参照してください。
- PLR を無効にする場合は、[PLR の非アクティブ化 \(251 ページ\)](#) を参照してください。



第 3 章

ポリシーを使用したスマートライセンスिंग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 (49 ページ)
- トポロジのワークフロー：CSSM に直接接続 (53 ページ)
- トポロジのワークフロー：コントローラを介して CSSM に接続 (55 ページ)
- トポロジのワークフロー：CSLU は CSSM から切断 (59 ページ)
- トポロジのワークフロー：CSSM への接続なし、CSLU なし (63 ページ)
- トポロジのワークフロー：SSM オンプレミス展開 (65 ページ)

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場合のタスク
- CSLU 開始型通信の場合のタスク

製品インスタンス開始型通信の場合のタスク

スマートアカウントのセットアップ → 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. 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ーロールがあることを確認します。

MSLA があり、ユーティリティモードを使用する場合は、使用するライセンスがサブスクリプション ID とともに、CSSM の対応するバーチャルアカウントに保管されていることも確認してください。

2. CSLU のインストール

タスクが実行される場所：ラップトップ、デスクトップ、または Windows 10 または Linux を実行している仮想マシン (VM)。

[Smart Software Manager]<https://software.cisco.com/download/home/286285506/type>> [Smart Licensing Utility] からファイルをダウンロードします。

インストールとセットアップの詳細については、『Cisco Smart License Utility クイック スタートセットアップガイド』および『Cisco Smart License Utility ユーザーガイド』を参照してください。

3. CSLU の環境設定

タスクの実行場所：CSLU インターフェイス

1. シスコへのログイン (CSLU インターフェイス) (176 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) (177 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) (177 ページ)

4. 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 (178 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。設定ファイルへの変更は必ず保存してください。

```
Device(config)# license smart transport cslu
Device(config)# exit
Device# copy running-config startup-config
```

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트리 *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 ホストのホスト名や IP アドレスを入力します。8182 はポート番号であり、CSLU が使用する唯一のポート番号です。

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

4. MSLA がある場合에만、ユーティリティモードを有効にします。 [ユーティリティモードの有効化 \(236 ページ\)](#)

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、UDI に関連付けられた信頼コード要求を送信します。CSLU は RUM レポートを CSSM に転送し、信頼コードも含む ACK を取得します。ACK は、製品インスタンスが次回 CSLU に接続したときに製品インスタンスに適用されます。

17.3.x トレインの Cisco IOS XE Amsterdam 17.3.6 以降のリリース、17.6.x トレインの Cisco IOS XE Bengaluru 17.6.4 以降のリリース、および Cisco IOS XE Cupertino 17.9.1a 以降のすべてのリリースでは、製品インスタンス開始モードの製品インスタンスは 1 日に複数の RUM レポートを送信しません。特権 EXEC モードで **license smart sync** コマンドを入力すると、製品インスタンスと CSLU 間のオンデマンド同期のためにこれをオーバーライドできます。

製品インスタンスでユーティリティモードが有効になっている場合、製品インスタンスから CSLU に送信される RUM レポートには適宜フラグが設定されます。CSSM からの ACK には、サブスクリプション ID が含まれています（製品インスタンスのスマートアカウントおよびバーチャルアカウントなど）。送信される後続の RUM レポートには、使用中の各ライセンスのサブスクリプション ID が含まれます。ユーティリティモードでは、30 日ごとに ACK が必要です。

製品インスタンスが次にいつ RUM レポートを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、出力の [Next report push] フィールドの日付を確認します。

CSLU 開始型通信の場合のタスク

スマートアカウントのセットアップ → 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 → 使用状況の同期

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ーロールがあることを確認します。

MSLA があり、ユーティリティモードを使用する場合は、使用するライセンスがサブスクリプション ID とともに、CSSM の対応するバーチャルアカウントに保管されていることも確認してください。

2. CSLU のインストール

タスクが実行される場所：ラップトップ、デスクトップ、または Windows 10 または Linux を実行している仮想マシン (VM)。

[Smart Software Manager]<https://software.cisco.com/download/home/286285506/type>> [Smart Licensing Utility] からファイルをダウンロードします。

インストールとセットアップの詳細については、『Cisco Smart License Utility クイック スタートセットアップガイド』および『Cisco Smart License Utility ユーザーガイド』を参照してください。

3. CSLU の環境設定

タスクの実行場所：CSLU インターフェイス

1. シスコへのログイン (CSLU インターフェイス) (176 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) (177 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) (180 ページ)

4. 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. CSLU 開始型通信のネットワーク到達可能性の確認 (182 ページ)
2. MSLA がある場合にのみ、ユーティリティモードを有効にします。ユーティリティモードの有効化 (236 ページ)

5. 使用状況の同期

タスクの実行場所：CSLU インターフェイス

使用状況レポートの収集：CSLU 開始 (CSLU インターフェイス) (180 ページ)

結果：

CSLU が現在シスコにログインしているため、レポートは CSSM の関連するスマートアカウントとバーチャルアカウントに自動的に送信され、CSSM は CSLU と製品インスタンスに確認応

答を送信します。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。CSSM からの ACK には信頼コードと SLAC が含まれます（要求した場合）。

信頼コードの要求とインストールは、Cisco IOS XE Cupertino 17.9.1a 以降でサポートされています。

製品インスタンスでユーティリティモードが有効になっている場合、CSLU が製品インスタンスから取得する RUM レポートには適宜フラグが設定されます。CSSM からの ACK には、サブスクリプション ID が含まれています（製品インスタンスのスマートアカウントおよびバーチャルアカウントなど）。送信される後続の RUM レポートには、使用中の各ライセンスのサブスクリプション ID が含まれます。ユーティリティモードでは、30 日ごとに ACK が必要です。

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ーロールがあることを確認します。

MSLA があり、ユーティリティモードを使用する場合は、使用するライセンスがサブスクリプション ID とともに、CSSM の対応するバーチャルアカウントに保管されていることも確認してください。

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（189 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。構成ファイルへの変更は必ず保存してください。

```
Device(config)# license smart transport smart
Device(config)# license smart url default
Device(config)# exit
Device# copy running-config startup-config
```

このオプションはユーティリティモードでサポートされています。

• 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（192 ページ）](#) を参照してください。

このオプションはユーティリティモードでサポートされています。

- 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（194 ページ）](#)」の項を参照してください。

このオプションはユーティリティモードでサポートされていません。

- 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（197 ページ）](#)」の項を参照してください。

このオプションはユーティリティモードでサポートされていません。

3. MSLAがある場合にのみ、ユーティリティモードを有効にします。[ユーティリティモードの有効化（236 ページ）](#)

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（[CSSMからの信頼コード用新規トークンの生成（227 ページ）](#)）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。
2. 製品インスタンスでトークンを設定して、CSSM との信頼を確立します。[ID トークンによる信頼の確立（227 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：適用済みまたは輸出規制）、またはサポート対象製品インスタンスで 250 Mbps 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完了する前にこのステップ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（216 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。

17.3.x トレインの Cisco IOS XE Amsterdam 17.3.6 以降のリリース、17.6.x トレインの Cisco IOS XE Bengaluru 17.6.4 以降のリリース、および Cisco IOS XE Cupertino 17.9.1a 以降のすべてのリリースでは、製品インスタンスは 1 日に複数の RUM レポートを送信しません。特権 EXEC

モードで **license smart sync** コマンドを入力すると、製品インスタンスと CSSM 間のオンデマンド同期のためにこれをオーバーライドできます。

製品インスタンスでユーティリティモードが有効になっている場合、製品インスタンスが CSSM に送信する RUM レポートには適宜フラグが設定されます。CSSM からの ACK には、サブスクリプション ID が含まれています（製品インスタンスのスマートアカウントおよびバーチャルアカウントなど）。送信される後続の RUM レポートには、使用中の各ライセンスのサブスクリプション ID が含まれます。ユーティリティモードでは、30 日ごとに ACK が必要です。

レポート間隔を変更するには、**license smart usage interval** コマンドを設定します。詳細については、[license smart \(グローバル コンフィギュレーション\) \(261 ページ\)](#) を参照してください。

トポロジのワークフロー：コントローラを介して CSSM に接続

実装するコントローラに応じて、対応するワークフローを実行します。

コントローラとしての Cisco DNA Center の使用

コントローラとして Cisco DNA Center を展開するには、次のワークフローを実行します。

製品インスタンスの設定 → Cisco DNA Center の設定

1. 製品インスタンスの設定

タスクの実行場所：製品インスタンス

NETCONF を有効にします。Cisco DNA Center は NETCONF プロトコルを使用して設定をプロビジョニングし、製品インスタンスから必要な情報を取得します。したがって、これを容易にするために製品インスタンスで NETCONF を有効にする必要があります。

詳細については、『[Programmability Configuration Guide, Cisco IOS XE Amsterdam 17.3.x](#)』を参照してください。このガイドの「Model-Driven Programmability」の「NETCONF Protocol」を確認します。

2. Cisco DNA Center の設定

タスクの実行場所：Cisco DNA Center GUI

次に、実行する必要があるタスクの概要と、付属のドキュメントリファレンスを示します。このドキュメントには、Cisco DNA Center GUI で実行する必要がある詳細な手順が示されています。

1. スマートアカウントとバーチャルアカウントを設定します。

CSSM Web UI へのログインに使用するのと同じログインクレデンシャルを入力します。これにより、Cisco DNA Center は CSSM との接続を確立できます。

必要なリリース（リリース 2.2.2 以降）の『Cisco DNA Center Administrator Guide』[英語]の「Manage Licenses」の「Set Up License Manager」を参照してください。

- 必要な製品インスタンスを Cisco DNA Center インベントリに追加してサイトに割り当てます。

これにより、Cisco DNA Center は、要求されている証明書を含む必要な設定をプッシュして、Smart Licensing Using Policy が予想どおりに機能するようにします。

必要なリリース（リリース 2.2.2 以降）の『Cisco DNA Center User Guide』[英語]の「Display Your Network Topology」の「Assign Devices to a Site」を参照してください。

- 必要に応じて、必要なワークフローを開始して承認コードをインストールします。

必要なリリース（リリース 2.2.2 以降）の『Cisco DNA Center Administrator Guide』の「Manage Licenses」の「Install the Authorization Code and Enable the High Security License」を参照してください。

Cisco DNA Center GUI では、HSECK9 ライセンスの次の製品インスタンスに対してのみ、SLAC を生成できます。

表 7: Cisco DNA Center GUI で HSECK9 ライセンスの SLAC 生成をサポートする製品インスタンス

製品インスタンス	必要な Cisco DNA Center の最小リリース	必要な Cisco IOS XE の最小バージョン
Cisco 1000 シリーズ サービス統合型ルータ	Cisco DNA Center リリース 2.2.2	Cisco IOS XE Amsterdam 17.3.2
Cisco 4000 シリーズ サービス統合型ルータ		Cisco IOS XE Amsterdam 17.3.2
Catalyst 8300 シリーズ エッジプラットフォーム		Cisco IOS XE Amsterdam 17.3.2
Catalyst 8500 シリーズ エッジプラットフォーム		Cisco IOS XE Amsterdam 17.3.2
Catalyst 8200 シリーズ エッジプラットフォーム		Cisco IOS XE Bengaluru 17.4.1

結果：

トポロジを実装したら、Cisco DNA Center で最初のアドホックレポートをトリガーし、スマートアカウントとバーチャルアカウント、および製品インスタンス間のマッピングを確立する必要があります。必要なリリース（リリース 2.2.2 以降）の『Cisco DNA Center Administrator Guide』[英語]で「Manage Licenses」の「Upload Resource Utilization Details to CSSM」を参照してください。これが完了すると、Cisco DNA Center はレポートポリシーに基づいて後続のレポートを処理します。

複数のポリシーが使用可能な場合、Cisco DNA Centerは最も短いレポート間隔を維持します。この間隔はより頻繁に（より短い間隔で）報告するようにのみ変更できます。必要なリリース（リリース2.2.2以降）の『Cisco DNA Center Administrator Guide』[英語]の「Manage Licenses」の「Modify License Policy」を参照してください。

この後にライセンスレベルを変更する場合は、必要なリリース（リリース2.2.2以降）の『Cisco DNA Center Administrator Guide』[英語]の「Manage Licenses」の「Change License Level」を参照してください。

コントローラとしての Cisco vManage の使用

Cisco vManage をコントローラとして導入するには、次のワークフローを実行します。

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 → Cisco vManage の設定 → 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

タスクの実行場所：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ーロールがあることを確認します。



(注) 以前のリリースから、（Cisco vManage がコントローラとして展開されている）Connected to CSSM Through Controller トポロジに移行する場合は、注文したすべてのライセンスがCSSMのスマートアカウントとバーチャルアカウントに表示されていることを最初に確認します。ライセンスが欠落している場合は、Cisco TAC に連絡して修正を依頼し、その後初めてトポロジの実装に進みます。

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

Cisco vManage を使用して製品インスタンスを管理するには、標準の起動プロセスを完了する必要があります。

Cisco SD-WAN スタートアップガイドの「Cisco SD-WAN Overlay Network Bring-Up Process」を参照してください。

3. Cisco vManage の設定

タスクの実行場所：Cisco vManage ポータル

Cisco SD-WAN スタートアップガイドの「License Management for Smart Licensing Using Policy」を参照してください。

Cisco vManage の設定は、Cisco IOS XE Bengaluru 17.5.1a 以降のリリースにのみ適用されません。

Cisco IOS XE Amsterdam 17.3.2 から Cisco IOS XE Bengaluru 17.4.x では、Cisco vManage はライセンス管理をサポートしていません。製品インスタンスは「コントローラモード」で動作するように設定できますが、使用状況レポートはサポートされません。

4. 承認コードのインストール（該当する場合のみ）

タスクの実行場所：製品インスタンスと CSSM Web UI

輸出規制ライセンスまたは 250 Mbps を超えるスループットを使用するには、SLAC のインストールを完了します（いずれかを選択）。

- オプション 1：

CSSM で SLAC を生成し、ファイルにダウンロードしてインストールします。

1. [CSSM からの SLAC の生成とファイルへのダウンロード（214 ページ）](#)
2. [製品インスタンスへのファイルのインストール（231 ページ）](#)

- オプション 2：

CSSM への接続を確立し、信頼を確立してから、SLAC を要求してインストールします（この例では、CSSM への接続にスマート転送を使用していますが、他のオプションを使用して CSSM に直接接続することもできます）。



(注) CSSM への接続を設定し、信頼を確立している場合でも、SD-WAN 「コントローラモード」の製品インスタンスは RUM レポートを送信しません。

1. 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://smarterceiver.cisco.com/licservice/license>) が自動的に設定されます。設定ファイルへの変更は必ず保存してください。

```
Device(config)# license smart transport smart
Device(config)# license smart url default
Device(config)# exit
Device# copy running-config startup-config
```

2. 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（227 ページ）](#)

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。 [ID トークンによる信頼の確立（227 ページ）](#)

```
Device# license smart trust idtoken NGMwMjk5mYtNZaxMS00NzZmtgWm all force
```

3. SLAC を要求してインストールします。 [SLAC の手動要求と自動インストール（216 ページ）](#)


```
Device# license smart authorization request add hseck9 local
Device(config)# exit
Device# copy running-config startup-config
```

結果：

Cisco vManage は使用状況を記録し、24 時間の固定レポート間隔で RUM レポートを CSSM に自動的に送信します。エッジデバイスにライセンスを割り当て、使用中のライセンスと割り当てに使用できるライセンスに関する情報を表示できます。

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場合のタスク](#)
- [CSLU 開始型通信の場合のタスク](#)

製品インスタンス開始型通信の場合のタスク

スマートアカウントのセットアップ → 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 → 使用状況の同期

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ーロールがあることを確認します。

MSLA があり、ユーティリティモードを使用する場合は、使用するライセンスがサブスクリプション ID とともに、CSSM の対応するバーチャルアカウントに保管されていることも確認してください。

2. CSLU のインストール

タスクが実行される場所：ラップトップ、デスクトップ、または Windows 10 または Linux を実行している仮想マシン (VM)。

[Smart Software Manager]<https://software.cisco.com/download/home/286285506/type>> [Smart Licensing Utility] からファイルをダウンロードします。

インストールとセットアップの詳細については、『[Cisco Smart License Utility クイック スタートセットアップガイド](#)』および『[Cisco Smart License Utility ユーザーガイド](#)』を参照してください。

3. 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) (177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) (177ページ)

4. 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 (178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。設定ファイルへの変更は必ず保存してください。

```
Device(config)# license smart transport cslu
Device(config)# exit
Device# copy running-config startup-config
```

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（ネームサーバーの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 サーバーにある場合、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（ネームサーバーの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 サーバーにある場合、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ホストのホスト名やIPアドレスを入力します。8182はポート番号であり、CSLUが使用する唯一のポート番号です。

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

4. MSLAがある場合にのみ、ユーティリティモードを有効にします。[ユーティリティモードの有効化 \(236 ページ\)](#)

5. 使用状況の同期

タスクの実行場所：CSLU と CSSM

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。これをトリガーする **license smart sync** 特権 EXEC コマンドを入力することもできます。この最初のレポートとともに、必要に応じて、UDI に関連付けられた信頼コード要求を送信します。

製品インスタンスでユーティリティモードが有効になっている場合、製品インスタンスから CSLU に送信される RUM レポートには適宜フラグが設定されます。

CSLU は CSSM から切断されているため、次のタスクを実行して RUM レポートを CSSM に送信します。

1. [CSSM へのエクスポート \(CSLU インターフェイス\) \(186 ページ\)](#)
2. [CSSM へのデータまたは要求のアップロードとファイルのダウンロード \(229 ページ\)](#)
3. [CSSM からのインポート \(CSLU インターフェイス\) \(187 ページ\)](#)

結果：

CSSM からインポートした ACK に信頼コードが含まれます (要求した場合)。ACK は、製品インスタンスが次回 CSLU に接続したときに製品インスタンスに適用されます。

17.3.x トレインの Cisco IOS XE Amsterdam 17.3.6 以降のリリース、17.6.x トレインの Cisco IOS XE Bengaluru 17.6.4 以降のリリース、および Cisco IOS XE Cupertino 17.9.1a 以降のすべてのリリースでは、製品インスタンス開始モードの製品インスタンスは 1 日に複数の RUM レポートを送信しません。特権 EXEC モードで **license smart sync** コマンドを入力すると、製品インスタンスと CSLU 間のオンデマンド同期のためにこれをオーバーライドできます。

RUM レポートにユーティリティモードのフラグが設定されている場合、CSSM からの ACK にはサブスクリプション ID が含まれます (製品インスタンスのスマートアカウントおよびパッチャルアカウントなど)。送信される後続の RUM レポートには、使用中の各ライセンスのサブスクリプション ID が含まれます。ユーティリティモードでは、30 日ごとに ACK が必要です。

製品インスタンスが次にいつ RUM レポートを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、出力の [Next report push] フィールドの日付を確認します。

CSLU 開始型通信の場合のタスク

スマートアカウントのセットアップ → 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 → 使用状況の同期

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ーロールがあることを確認します。

MSLA があり、ユーティリティモードを使用する場合は、使用するライセンスがサブスクリプション ID とともに、CSSM の対応するバーチャルアカウントに保管されていることも確認してください。

2. CSLU のインストール

タスクが実行される場所：ラップトップ、デスクトップ、または Windows 10 または Linux を実行している仮想マシン (VM)。

[Smart Software Manager]<https://software.cisco.com/download/home/286285506/type>> [Smart Licensing Utility] からファイルをダウンロードします。

インストールとセットアップの詳細については、『[Cisco Smart License Utility クイック スタートセットアップガイド](#)』および『[Cisco Smart License Utility ユーザーガイド](#)』を参照してください。

3. 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 \(CSLU インターフェイス\)](#) (177 ページ)
3. [CSLU での CSLU 開始型製品インスタンスの追加 \(CSLU インターフェイス\)](#) (180 ページ)

4. 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. [CSLU 開始型通信のネットワーク到達可能性の確認](#) (182 ページ)
2. MSLA がある場合にのみ、ユーティリティモードを有効にします。[ユーティリティモードの有効化](#) (236 ページ)

5. 使用状況の同期

タスクの実行場所：CSLU と CSSM

製品インスタンスから使用状況データを収集します。CSLU は CSSM から切断されるため、後で 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します。該当する場合、この最初のレポートに加えて、承認コードと UDI に関連付けられた信頼コード要求が RUM レポートに含まれます。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。

製品インスタンスでユーティリティモードが有効になっている場合、CSLU が取得する RUM レポートには適宜フラグが設定されます。

1. [使用状況レポートの収集：CSLU 開始 \(CSLU インターフェイス\)](#) (180 ページ)
2. [CSSM へのエクスポート \(CSLU インターフェイス\)](#) (186 ページ)
3. [CSSM へのデータまたは要求のアップロードとファイルのダウンロード](#) (229 ページ)
4. [CSSM からのインポート \(CSLU インターフェイス\)](#) (187 ページ)

結果：

CSSM からインポートした ACK に信頼コードと SLAC が含まれます（要求した場合）。CSLU が次に更新を実行するときに、アップロードされた ACK が製品インスタンスに適用されます。

信頼コードの要求とインストールは、Cisco IOS XE Cupertino 17.9.1a 以降でサポートされています。

RUM レポートにユーティリティモードのフラグが設定されている場合、CSSM からの ACK にはサブスクリプション ID が含まれます（製品インスタンスのスマートアカウントおよびバーチャルアカウントなど）。送信される後続の RUM レポートには、使用中の各ライセンスのサブスクリプション ID が含まれます。ユーティリティモードでは、30 日ごとに ACK が必要です。

トポロジのワークフロー：CSSM への接続なし、CSLU なし

このトポロジをセットアップするために必要なタスクのリストは短いですが、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。

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 → 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ーロールがあることを確認します。

MSLA があり、ユーティリティモードを使用する場合は、使用するライセンスがサブスクリプション ID とともに、CSSM の対応するバーチャルアカウントに保管されていることも確認してください。

2. 製品インスタンスの設定

タスクの実行場所：製品インスタンス

1. 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。設定ファイルへの変更は必ず保存してください。

```
Device(config)# license smart transport off
Device(config)# exit
Device# copy running-config startup-config
```

2. MSLA がある場合、ユーティリティモードを有効にします。

ユーティリティモードを有効にするには、グローバルコンフィギュレーションモードで **license smart utility** コマンドを入力します。構成ファイルへの変更を保存します。

```
Device (config)# license smart utility
Device(config)# exit
Device# copy running-config startup-config
```

3. 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 Web UI および製品インスタンス

エクスポート制御ライセンスまたは 250 Mbps を超えるスループットを使用する場合は、SLAC をインストールします。（いずれかを選択）

• オプション 1：

CSSM Web UI で SLAC を生成してダウンロードし、製品インスタンスにインストールします。ここでは、SLAC を生成するには、CSSM Web UI に製品インスタンス情報を入力する必要があります。

1. [CSSM からの SLAC の生成とファイルへのダウンロード](#)
2. [製品インスタンスへのファイルのインストール \(231 ページ\)](#)

• オプション 2：

SLAC 要求を生成してファイルに保存し、それを CSSM Web UI にアップロードし、CSSM Web UI から SLAC コードをダウンロードし、製品インスタンスにインストールします。



(注) このオプションは、Cisco IOS XE cupertino 17.7.1a 以降でのみサポートされます。

1. [製品インスタンスでの SLAC 要求の生成と保存 \(219 ページ\)](#)

2. [CSSM へのデータまたは要求のアップロードとファイルのダウンロード](#) (229 ページ)
3. [製品インスタンスへのファイルのインストール](#) (231 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。

Cisco IOS XE cupertino 17.7.1a 以降では、このコマンドを設定すると、信頼コードが製品インスタンスにまだ存在しない場合、RUM レポートに自動的に信頼コード要求が含まれます。

製品インスタンスでユーティリティモードが有効になっている場合、RUM レポートに適宜フラグが設定されます。

下記の例では、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 file bootflash:all_rum.txt
Device# copy bootflash:all_rum.txt tftp://10.8.0.6/all_rum.txt
```

コマンドシンタックスの詳細については、[license smart](#)（特権 EXEC）（277 ページ）コマンドを参照してください。

2. 使用状況データを CSSM にアップロード：[CSSM へのデータまたは要求のアップロードとファイルのダウンロード](#) (229 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](#) (231 ページ)

RUM レポートにユーティリティモードのフラグが含まれている場合、CSSM からの ACK にはサブスクリプション ID が含まれます（製品インスタンスのスマートアカウントおよびバーチャルアカウントなど）。保存される後続の RUM レポートには、使用中の各ライセンスのサブスクリプション ID が含まれます。ユーティリティモードでは、30 日ごとに ACK が必要です。

トポロジのワークフロー：SSM オンプレミス展開

通信に製品インスタンス開始型（プッシュ）方式を実装するか、または SSM オンプレミス開始型（プル）方式を実装するかによって、対応するタスクの手順を実行します。

製品インスタンス開始型通信の場合のタスク

スマートアカウントのセットアップ → SSM オンプレミスのインストールと設定 → 製品インスタンスの追加と検証（該当する場合のみ） → 製品インスタンスの設定 → 使用状況の最初の同期

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ーロールがあることを確認します。

MSLA があり、ユーティリティモードを使用する場合は、使用するライセンスがサブスクリプション ID とともに、CSSM の対応するバーチャルアカウントに保管されていることも確認してください。

2. SSM オンプレミスのインストールと設定

タスクの実行場所：Cisco UCS C220 M3 ラックサーバなどの物理サーバ、または必要な要件を満たしているハードウェアベースのサーバ。

[Smart Software Manager](#) の [Smart Software Manager On-Prem] からファイルをダウンロードします。

インストールのヘルプについては、『[Cisco Smart Software On-Prem Installation Guide](#)』と『[Cisco Smart Software On-Prem User Guide](#)』を参照してください。

SSM オンプレミスを展開し、SSM オンプレミスで共通名を設定し（[Security Widgets] > [Certificates]）、NTP サーバを同期し（[Settings] ウィジェット > [Time Settings]）、SSM オンプレミスアカウントを作成して登録し、CSSM のスマートアカウントとバーチャルアカウントと同期（[Synchronization] ウィジェット）したら、インストールが完了します。



(注) [On-Prem Licensing Workspace] のライセンス機能は、ローカルアカウントを作成し、登録し、CSSM のスマートアカウントと同期するまではグレー表示になります。CSSM とのローカルアカウントの同期は、SSM オンプレミスインスタンスを CSSM に認識させるためであり、次に示す「4. 使用状況の最初の同期」で実行する使用状況の同期とは異なります。

3. 製品インスタンスの追加と検証

タスクの実行場所：SSM オンプレミス UI

この手順により、製品インスタンスが検証され、CSSM の該当するスマートアカウントとバーチャルアカウントにマッピングされます。この手順は、次の場合にのみ必要です。

- 製品インスタンスを CSSM で報告する前に、SSM オンプレミスで追加および検証する場合（セキュリティを強化するため）。
- 使用する前に承認が必要なライセンスを使用する（enforcement type: enforced または export-controlled）か、または 250 Mbps を超えるスループットを設定する場合。次の手

順 3 d で必要な SLAC を要求する前に、このような製品インスタンスを SSM オンプレミスに追加する必要があります。

- (デフォルトのローカルバーチャルアカウントに加えて) ローカルバーチャルアカウントを SSM オンプレミスで作成した場合。この場合は、SSM オンプレミスが CSSM の正しいライセンスプールに使用状況を報告できるように、SSM オンプレミスにこれらのローカルバーチャルアカウントの製品インスタンスのスマートアカウント情報とバーチャルアカウント情報を提供する必要があります。
 - MSLA があり、ユーティリティモードを使用する場合は、このステップを完了すると、正しいサブスクリプションが選択されます。
1. [スマートアカウントとバーチャルアカウントの割り当て \(SSM オンプレミス UI\)](#) (198 ページ)
 2. [デバイスの検証 \(SSM オンプレミス UI\)](#) (199 ページ)



(注) 製品インスタンスが NAT 設定にある場合は、デバイス検証を有効にするときに NAT 設定のサポートも有効にします。両方のトグルスイッチが同じウィンドウにあります。

4. 製品インスタンスの設定

タスクの実行場所：製品インスタンスと SSM オンプレミス UI

特権 EXEC モードで **copy running-config startup-config** コマンドを入力して、製品インスタンスの設定変更を必ず保存してください。

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](#) (200 ページ)
2. [トランスポート URL の取得 \(SSM オンプレミス UI\)](#) (203 ページ)
3. [転送タイプ、URL、およびレポート間隔の設定](#) (232 ページ)

CSLU と SSM オンプレミスのトランスポートタイプ設定は同じですが (グローバルコンフィギュレーションモードの **license smart transport cslu** コマンド)、URL が異なります。

4. 使用前に承認が必要なライセンス (適用タイプ：適用済みまたは輸出規制) を使用するか、またはサポート対象製品インスタンスで 250Mbps を超えるスループットを設定する場合にのみ、このサブステップを実行します (オプションを 1 つ選択)。
 - オプション 1：
SSM オンプレミスが CSSM に接続されている場合：[承認コード要求の送信 \(SSM オンプレミス UI、接続モード\)](#) (203 ページ)
 - オプション 2：
SSM オンプレミスが CSSM に接続されていない場合：[承認コード要求の送信 \(SSM オンプレミス UI、切断モード\)](#) (205 ページ)

5. MSLAがある場合にのみ、ユーティリティモードを有効にします。 [ユーティリティモードの有効化 \(236 ページ\)](#)

5. 使用状況の最初の同期

タスクの実行場所：製品インスタンス、SSM オンプレミス、CSSM

1. 製品インスタンスを SSM オンプレミスと同期します。

製品インスタンスに `license smart sync {all| local}` コマンドを特権 EXEC モードで入力します。これにより、SSM オンプレミスと製品インスタンスが同期され、保留中のデータが送受信されます。次に例を示します。

```
Device# license smart sync local
```

製品インスタンスでユーティリティモードが有効になっている場合、製品インスタンスが SSM オンプレミスに送信する RUM レポートには適宜フラグが設定されます。

これは、SSM オンプレミス UI で確認できます。ログインして、[Smart Licensing] ワークスペースを選択します。[Inventory] > [SL Using Policy] タブに移動します。対応する製品インスタンスの [Alerts] 列に、「Usage report from product instance」というメッセージが表示されます。



- (注) 上記の手順 2 (製品インスタンスの追加と検証) を実行していない場合、このサブ手順を実行すると、製品インスタンスが SSM オンプレミスのデータベースに追加されます。

2. 使用状況情報を CSSM と同期します (いずれかを選択)。

- オプション 1：

SSM オンプレミスが CSSM に接続されている場合：SSM オンプレミス UI の [Smart Licensing] ワークスペースで、[Reports] > [Usage Schedules] > [Synchronize now with Cisco] に移動します。

- オプション 2：

SSM オンプレミスが CSSM に接続されていません。 [使用状況データのエクスポートとインポート \(SSM オンプレミス UI\) \(206 ページ\)](#) を参照してください。

結果：

使用状況の最初の同期が完了しました。製品インスタンスとライセンス使用状況情報が SSM オンプレミスに表示されるようになりました。

CSSM への RUM レポートにユーティリティモードのフラグが設定されている場合、CSSM からの ACK にはサブスクリプション ID が含まれます (製品インスタンスのスマートアカウントおよびバーチャルアカウントなど)。送信される後続の RUM レポートには、使用中の各ライセンスのサブスクリプション ID が含まれます。ユーティリティモードでは、30 日ごとに ACK が必要です。

後続のレポートには、次のオプションが含まれています。

- 製品インスタンスと SSM オンプレミスとの間でデータを同期するには、次の手順を実行します。

レポート間隔を設定して、製品インスタンスと SSM オンプレミスとの間の定期的な同期をスケジュールします。グローバル コンフィギュレーション モードで **license smart usage interval interval_in_days** コマンドを入力します。

17.3.x トレインの Cisco IOS XE Amsterdam 17.3.6 以降のリリース、17.6.x トレインの Cisco IOS XE Bengaluru 17.6.4 以降のリリース、および Cisco IOS XE Cupertino 17.9.1a 以降のすべてのリリースでは、製品インスタンス開始モードの製品インスタンスは1日に複数の RUM レポートを送信しません。特権 EXEC モードで **license smart sync** コマンドを入力すると、製品インスタンスと SSM オンプレミス間のオンデマンド同期のためにこれをオーバーライドできます。

製品インスタンスが次にいつ RUM レポートを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、出力の [Next report push:] フィールドを確認します。

- 使用状況情報を CSSM と同期するには、定期的な同期をスケジュールするか、必要なファイルをアップロードおよびダウンロードします。
 - CSSM との定期的な同期をスケジュールします。SSM オンプレミス UI で、[Reports] > [Usage Schedules] > [Synchronization schedule with Cisco] に移動します。次の頻度情報を入力し、保存します。
 - [Days]：同期が実行される頻度を示します。たとえば、2 を入力すると、同期は 2 日に 1 回行われます。
 - [Time of Day]：24 時間表記法で、同期が実行される時刻を示します。たとえば、14 hours と 0 minutes を入力すると、ローカルタイムゾーンの午後 2 時（1400）に同期が行われます。
 - レポートに必要なファイルのアップロードとダウンロードを実行します（[使用状況データのエクスポートとインポート（SSM オンプレミス UI）](#)（206 ページ））。

SSM オンプレミスインスタンス開始型通信の場合のタスク

SSM オンプレミスのインストールと設定 → 製品インスタンスの追加 → 製品インスタンスの設定 → 初期使用の同期

1. SSM オンプレミスのインストールと設定

タスクの実行場所：Cisco UCS C220 M3 ラックサーバなどの物理サーバ、または必要な要件を満たしているハードウェアベースのサーバ。

[Smart Software Manager](#) の [Smart Software Manager On-Prem] からファイルをダウンロードします。

インストールのヘルプについては、『[Cisco Smart Software On-Prem Installation Guide](#)』と『[Cisco Smart Software On-Prem User Guide](#)』を参照してください。

SSM オンプレミスを展開し、SSM オンプレミスで共通名を設定し（[Security Widgets] > [Certificates]）、NTP サーバを同期し（[Settings] ウィジェット > [Time Settings]）、SSM オンプレミスアカウントを作成して登録し、CSSM のスマートアカウントとバーチャルアカウントと同期（[Synchronization] ウィジェット）したら、インストールが完了します。



- (注) [On-Prem Licensing Workspace] のライセンス機能は、ローカルアカウントを作成し、登録し、CSSM のスマートアカウントと同期するまではグレー表示になります。CSSM とのローカルアカウントの同期は、SSM オンプレミスインスタンスを CSSM に認識させるためであり、次に示す「4. 使用状況の最初の同期」で実行する使用状況の同期とは異なります。

2. 製品インスタンスの追加

タスクの実行場所：SSM オンプレミス UI

単一の製品インスタンスを追加するか、または複数の製品インスタンスを追加するかに応じて、対応するサブ手順（[1 つ以上の製品インスタンスの追加（SSM オンプレミス UI）（207 ページ）](#)）を実行します。

3. 製品インスタンスの設定

タスクの実行場所：製品インスタンスと SSM オンプレミス UI

特権 EXEC モードで **copy running-config startup-config** コマンドを入力して、製品インスタンスの設定変更を必ず保存してください。

1. [SSM オンプレミス開始型通信のネットワーク到達可能性の確保（209 ページ）](#)
2. MSLA がある場合にのみ、ユーティリティモードを有効にします。[ユーティリティモードの有効化（236 ページ）](#)
3. 使用前に承認が必要なライセンス（enforcement type: enforced または export-controlled）を使用するか、または（サポートされている製品インスタンスで）250 Mbps を超えるスループットを設定する場合にのみ、このサブ手順を実行します（[承認コード要求の送信（SSM オンプレミス UI、切断モード）（205 ページ）](#)）。

SSM オンプレミスが次に更新を実行するときに、アップロードされたコードが適用されるようになりました。製品インスタンスとの使用状況の最初の同期は、次の手順 4 で実行されて、その後完了します。

4. 使用状況の最初の同期

タスクの実行場所：SSM オンプレミスと CSSM

1. 製品インスタンスから使用状況情報を取得します。

SSM オンプレミス UI で、[Reports] > [Synchronization pull schedule] > [Synchronize now with the device] に移動します。

製品インスタンスでユーティリティモードが有効になっている場合、SSM オンプレミスが取得する RUM レポートには適宜フラグが設定されます。

[Alerts] 列に、「Usage report from product instance」というメッセージが表示されます。



ヒント 同期がトリガーされるまでに 60 秒かかります。進行状況を表示するには、[On-Prem Admin Workspace] に移動し、[Support Center] ウィジェットをクリックします。このウィジェットにシステムログに進行状況が表示されます。

2. 使用状況情報を CSSM と同期します（いずれかを選択）。

• オプション 1：

SSM オンプレミスが CSSM に接続されている場合：SSM オンプレミス UI の [Smart Licensing] ワークスペースで、[Reports] > [Usage Schedules] > [Synchronize now with Cisco] に移動します。

• オプション 2：

SSM オンプレミスが CSSM に接続されていません。[使用状況データのエクスポートとインポート \(SSM オンプレミス UI\) \(206 ページ\)](#) を参照してください。

結果：

使用状況の最初の同期が完了しました。製品インスタンスとライセンス使用状況情報が SSM オンプレミスに表示されるようになりました。SSM オンプレミスは ACK を製品インスタンスに自動的に返します。製品インスタンスが ACK を受信し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、出力で [Last ACK received] フィールドの日付を確認します。

CSSM への RUM レポートにユーティリティモードのフラグが設定されている場合、CSSM からの ACK にはサブスクリプション ID が含まれます（製品インスタンスのスマートアカウントおよびバーチャルアカウントなど）。送信される後続の RUM レポートには、使用中の各ライセンスのサブスクリプション ID が含まれます。ユーティリティモードでは、30 日ごとに ACK が必要です。

後続のレポートには、次のオプションが含まれています。

• 製品インスタンスから使用状況情報を取得するには、次の手順を実行します。

- SSM オンプレミス UI の [Smart Licensing] ワークスペースで、[Reports] > [Usage Schedules] > [Synchronize now with Cisco] に移動します。
- 頻度を設定して、製品インスタンスから情報を定期的を取得するようにスケジュールします。SSM オンプレミス UI の [Smart Licensing] ワークスペースで、[Reports] > [Usage Schedules] > [Synchronisation pull schedule with the devices] に移動します。次のフィールドに値を入力します。

- **[Days]**：同期が実行される頻度を示します。たとえば、2 を入力すると、同期は 2 日に 1 回行われます。
- **[Time of Day]**：24 時間表記法で、同期が実行される時刻を示します。たとえば、14 hours と 0 minutes と入力すると、午後 2 時（1400）に同期が行われます。
- CSSM に接続せずに製品インスタンスから使用状況データを収集します。SSM オンプレミス UI の **[Smart Licensing]** ワークスペースで、**[Inventory]** > **[SL Using Policy]** タブに移動します。対応するチェックボックスを有効にして、1 つ以上の製品インスタンスを選択します。**[Actions for Selected...]** > **[Collect Usage]** をクリックします。選択した製品インスタンスにオンプレミスが接続し、使用状況レポートを収集します。その後、これらの使用状況レポートはオンプレミスのローカルライブラリに保存されます。これらのレポートは、オンプレミスがシスコに接続されている場合はシスコに転送できます。また、（シスコに接続されていない場合は）**[Export/Import All.]** > **[Export Usage to Cisco]** を選択することで、使用状況の収集を手動でトリガーできます。
- 使用状況情報を CSSM と同期するには、次の手順を実行します。
 - CSSM との定期的な同期をスケジュールします。SSM オンプレミス UI で、**[Reports]** > **[Usage Schedules]** > **[Synchronization schedule with Cisco]** に移動します。次の頻度情報を入力し、保存します。
 - **[Days]**：同期が実行される頻度を示します。たとえば、2 を入力すると、同期は 2 日に 1 回行われます。
 - **[Time of Day]**：24 時間表記法で、同期が実行される時刻を示します。たとえば、14 hours と 0 minutes と入力すると、午後 2 時（1400）に同期が行われます。
 - レポートに必要なファイルのアップロードとダウンロードを実行します（[使用状況データのエクスポートとインポート（SSM オンプレミス UI）（206 ページ）](#)）。



第 4 章

ポリシーを使用したスマートライセンシングへの移行

Smart Licensing Using Policy に移行するには、製品インスタンスのソフトウェアバージョン（イメージ）、アップグレード前セットアップの一部であるその他すべてのコンポーネントをサポートされているバージョンにアップグレードする必要があります。

はじめる前に

「[アップグレード](#)」の項を必ず読み、Smart Licensing Using Policy によって以前のすべてのライセンスモデルがどのように処理するかを理解してください。

その製品インスタンスに必要な最小ソフトウェアバージョンは、Smart Licensing Using Policy が導入されたリリースです。サポートされているルーティング製品の最初のリリースについては、[サポート対象製品（4 ページ）](#)を参照してください。

移行前に使用していたすべてのライセンスは、アップグレード後も使用できることに注意してください。つまり、登録済みライセンスと承認済みライセンス（予約済みライセンスを含む）だけでなく、評価ライセンスもすべて移行されます。ipbasek9 や internal_service などのデフォルトのライセンスは移行されますが、show コマンドの出力には表示されません（デフォルトでは、これらのライセンスに権限付与タグはなく、常に使用可能です）。

登録済みライセンスと承認済みライセンスを移行する利点は、アップグレード後も設定（トランスポートタイプの設定と、CSSM への接続の設定、すべての証人コード）が保持されるため、移行後に実行する設定手順が少なくなります。これにより、Smart Licensing Using Policy 環境への移行がよりスムーズになります。

- [その他のコンポーネントのアップグレード（74 ページ）](#)
- [ソフトウェアバージョンのアップグレード（74 ページ）](#)
- [ソフトウェアバージョンのアップグレード後（75 ページ）](#)
- [移行シナリオの例（76 ページ）](#)

その他のコンポーネントのアップグレード

アップグレード前のセットアップに Cisco DNA Center、Cisco vManage、または SSM オンプレミスが含まれている場合は、Smart Licensing Using Policy に移行する前に、次のことを確認してください。

- コンポーネントが互換性のあるバージョンを実行している場合、またはアップグレードが必要な場合。

各コンポーネントの Smart Licensing Using Policy と互換性のあるバージョン（該当する場合）の詳細については、[アーキテクチャ（6 ページ）](#) を参照してください。

- アップグレードを所定の順序で実行する必要がある場合。これは、コンポーネントと製品インスタンスを正しい順序でアップグレードするために必要なことです。

Cisco DNA Center

Cisco DNA Center については、『Cisco DNA Center Upgrade Guide』を参照してください。
https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/upgrade/b_cisco_dna_center_upgrade_guide.html

Cisco vManage

Cisco vManage については、『Cisco SD-WAN スタートアップガイド』を参照してください。

SSM オンプレミス

SSM オンプレミスについては、[SSM オンプレミス 8 設置ガイド \[英語\]](#) を参照してください。

ソフトウェアバージョンのアップグレード

サポートされている製品インスタンスのアップグレード手順については、次の表を参照してください。

製品シリーズ	アップグレード情報へのリンク
Cisco 1000 シリーズ サービス統合型ルータ	ソフトウェアのインストール方法とアップグレード方法
Cisco 4000 シリーズ サービス統合型ルータ	ソフトウェアのインストール方法とアップグレード方法
Cisco ASR 1000 シリーズ アグリゲーション サービス ルータ	Cisco ASR 1000 シリーズ ルータでサポートされているソフトウェアのアップグレードプロセス
Cisco クラウド サービス ルータ 1000v	Cisco IOS XE ソフトウェアのアップグレード

製品シリーズ	アップグレード情報へのリンク
シスコサービス統合型仮想ルータ	Cisco IOS XE ソフトウェアのアップグレード
Catalyst 8200 シリーズ エッジ プラットフォーム	ソフトウェアのインストール方法とアップグレード方法
Catalyst 8300 シリーズ エッジ プラットフォーム	ソフトウェアのインストール方法とアップグレード方法
Catalyst 8500 シリーズ エッジ プラットフォーム	統合パッケージの管理
Catalyst 8000V エッジソフトウェア	Cisco IOS XE ソフトウェアのアップグレード
Cisco 1100 ターミナル サービス ゲートウェイ	ソフトウェアのインストール方法とアップグレード方法

ソフトウェアバージョンのアップグレード後

- トポロジを実装します。

アップグレード前の設定でトランスポートモードを使用できる場合は、アップグレード後も保持されます。評価ライセンスや、トランスポートタイプの概念が存在しないライセンスモデルの場合など、一部の場合にのみ、デフォルト (cslu) が適用されます。このような場合は、**Smart Licensing Using Policy** 環境で動作するように設定する前に実行する必要があります。ある手順がいくつかある場合があります。

アップグレード元のライセンスモデルに関係なく、アップグレード後にトポロジを変更できます。その場合は、[ポリシーを使用したスマートライセンスの設定方法：トポロジ別のワークフロー \(49 ページ\)](#) に示すように、対応するトポロジを実装します。

- アップグレード後に SLAC を必要とする製品インスタンスがあるかどうかを確認します。

輸出規制ライセンスまたは適用済みライセンスの場合、アップグレード後の SLAC のインストールは特定の場合にのみ必要です。[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 \(37 ページ\)](#) を参照してください。

- Device-Led Conversion (DLC) が適用され、完了しているかどうかを確認します。

DLC は、従来のライセンスをスマートライセンスに変換するプロセスであり、手動での操作は必要ありません。したがって、DLC はスマートライセンス以外のライセンス、つまり Right-To-Use (RTU) ライセンスと製品承認キー (PAK) ライセンスを移行する場合にのみ適用されます。DLC が完了すると、これらの変換されたライセンスの消費が CSSM に反映されます。

Smart Licensing Using Policy をサポートするリリースにアップグレードした場合にのみ、製品スタンスで DLC プロセスが自動的にトリガーされます。

DLC データは製品インスタンスが Smart Licensing Using Policy をサポートするソフトウェアバージョンにアップされた 1 時間後に収集されます。この DLC データは、RUM レポートにも自動的に組み込まれます。したがって、DLC がアップグレードシナリオに適用される場合、製品インスタンスが DLC データの収集 (**show platform software license dlc** 特権 EXEC コマンド) を完了するまで待ってから、最初の使用状況レポートを CSSM に送信できます。DLC データの収集が完了する前に最初の使用状況レポートを送信する場合は、実装するトポロジに適用されるレポート方式に従って、DLC データを送信するための別のレポートを実行します。CSSM は、DLC データの処理後に ACK を生成します。製品インスタンスに ACK がインストールされると、DLC プロセスが完了します。DLC プロセスにかかる時間は、ライセンスの数によって異なります。

DLC 自体には何のアクションも必要ありません。



- (注) DLC は 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 1000 シリーズ アグリゲーション サービス ルータでサポートされています。

シスコクラウド サービス ルータ 1000v と Cisco サービス統合型仮想ルータは DLC をサポートしていません。

- ライセンスの使用状況を CSSM と同期します。

どのライセンスモデルからアップグレードするか、どのトポロジを実装するかに関係なく、使用状況情報を CSSM と同期します。そのためには、実装するトポロジに適用されるレポート方式に従う必要があります。この最初の同期により、使用状況の最新の情報が CSSM に反映され、カスタムポリシー (使用可能な場合) が適用されます。この同期後に適用されるポリシーは、後続のレポート要件も示します。これらのルールを [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 \(40 ページ\)](#) の表にも示します。



- (注) 使用状況の最初の同期が完了した後、ポリシー、またはシステムメッセージに示されている場合にのみ、レポートが必要です。

移行シナリオの例

さまざまな既存のライセンスモデルとライセンスを考慮した移行シナリオの例を示します。すべてのシナリオで、移行前と後の出力例と注意すべき CSSM Web UI の変更を (移行の成功または追加アクションのインジケータとして) 示し、また、必要な移行後の手順を特定して実行する方法も示します。



- (注) SSM オンプレミスでは、アップグレード関連のさまざまなアクティビティを実行する順序が重要です。したがって、このシナリオでのみ、移行の順序が示されています。

例：スマートライセンス（登録済みおよび承認済みのライセンス）から Smart Licensing Using Policy へ

次に、スマートライセンスから Smart Licensing Using Policy に移行する、承認済みライセンスと登録済みライセンスを持つ **Cisco 4461 サービス統合型ルータ** の例を示します。製品インスタンスのソフトウェアバージョンが Cisco IOS XE Gibraltar 16.12.4 から Cisco IOS XE Amsterdam 17.3.2 にアップグレードされます。次に、この例の場合にアップグレード後はどうなるかについての概要を示します。

- 移行後の適用タイプ：このシナリオのすべてのライセンスが登録され、承認されます（つまり、使用前に承認が必要なすべてのライセンスにすでにこれが備わっていることを意味します）。したがって、輸出規制ライセンス (ISR_4400_Hsec) が使用可能になり、移行後の適用タイプは EXPORT RESTRICTED になります。さらに、アップグレード後に SLAC をインストールする必要はありません。スマートアカウントに登録された HSECK9 ライセンスと、CSSM で有効になっている輸出規制フラグについては、[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 \(37 ページ\)](#) を参照してください。

残りのすべての登録済みライセンスと承認済みライセンスの移行後の適用タイプは NOT ENFORCED になります。

- 移行後のトランスポートタイプ：Call Home は、移行前に設定されたトランスポートタイプです。ライセンスが登録されているため、トランスポートタイプ (**callhome**) と CSSM に接続するための設定は、移行後も保持されます。
- Device-Led Conversion (DLC)：DLC は以前のスマートライセンス環境でのライセンスであるため、このシナリオのライセンスには適用されません（すでにスマートライセンスです）。
- 移行後のレポート：この例については、「移行前と後の **show version**」の下にある出力例を参照してください。ソフトウェアバージョンのアップグレード後に表示されるシステムメッセージには、移行後に製品インスタンスが CSSM への接続を保持し、CSSM とすでに正常に同期されている（レポート、承認コード、およびポリシー）ことが示されています。ただし、この例では、十分明確にするために別の同期が実行されます。

後続のレポートはポリシーによって異なります。最初の同期が完了したら、**show license status** コマンドの出力を参照して、レポートが必要かどうか、いつまでに必要かを確認します。出力で [Next report push] フィールドと [Next ACK deadline] フィールドを確認します。また、レポートが必要な場合にもシステムメッセージが表示されます。

移行前と後の show コマンド

移行前と後の **show version**

例：スマートライセンス（登録済みおよび承認済みのライセンス）から Smart Licensing Using Policy へ

show version Before Migration

次の出力には、アップグレード前のソフトウェアバージョンが表示され、その後、これよりも前のソフトウェアバージョンがロードされたときに表示されたライセンス関連のシステムメッセージの抜粋が続いています。

```
Device# show version
Cisco IOS XE Software, Version 16.12.04
Cisco IOS Software [Gibraltar], ISR Software
(X86_64_LINUX_IOSD-UNIVERSALK9-M), Version 16.12.4, RELEASE SOFTWARE (fc5)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2020 by Cisco Systems, Inc.
Compiled Thu 09-Jul-20 21:44 by mcpre
<output truncated>

*Jul 23 13:36:25.062: %SMART_LIC-5-IN_COMPLIANCE: All entitlements and licenses in use
on
this device are authorized
*Jul 23 13:36:25.064: %SMART_LIC-5-END_POINT_RESET: End Point list reset
*Jul 23 13:36:25.065: %SMART_LIC-6-AUTH_RENEW_SUCCESS: Authorization renewal successful.

State=authorized for udi PID:ISR4461/K9,SN:FDO222815Y4
```

show version After Migration

次の出力には、移行後のソフトウェアバージョンが表示され、その後、新しいイメージでシステムを再起動した後のライセンス関連のシステムメッセージの抜粋が続いています。

```
Device# show version
Cisco IOS Software [Amsterdam], ISR Software
(X86_64_LINUX_IOSD-UNIVERSALK9-M), Version 17.3.2, RELEASE SOFTWARE (fc3)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2020 by Cisco Systems, Inc.
Compiled Sat 31-Oct-20 13:21 by mcpre
<output truncated>

<output truncated>
Press RETURN to get started!

*Jan 15 03:21:10.823: %CALL_HOME-6-CALL_HOME_ENABLED: Call-home is enabled by Smart Agent
for Licensing.
*Jan 15 03:21:15.341: %SMART_LIC-6-REPORTING_REQUIRED: A Usage report acknowledgement
will be required
in 365 days.
*Jan 15 03:21:29.510: %SMART_LIC-6-TRUST_INSTALL_SUCCESS: A new licensing trust code was
successfully
installed on PID:ISR4461/K9,S:FDO222815Y4.
*Jan 15 03:21:31.981: %SMART_LIC-6-AUTHORIZATION_INSTALL_SUCCESS: A new licensing
authorization code was
successfully installed on PID:ISR4461/K9,SN:FDO222815Y4
*Jan 15 03:26:07.805: %SIP-1-LICENSING: SIP service is Up. License report acknowledged.
*Jan 15 03:26:07.812: %SMART_LIC-6-EXPORT_CONTROLLED: Usage of export controlled features
is allowed
for feature hseck9
*Jan 15 03:26:08.282: %SMART_LIC-6-POLICY_INSTALL_SUCCESS: A new licensing policy was
```

```
successfully installed
<output truncated>
```

移行前と後の show license summary

show license summary Before Migration

移行前の出力には、すべてのライセンスが登録済み（REGISTERED）であり、承認済み（AUTHORIZED）であることが示されています。したがって、これらのライセンスはすべて移行され、移行後に IN USE として表示されます。

```
Device# show license summary
Smart Licensing is ENABLED

Registration:
  Status: REGISTERED
  Smart Account: Eg-SA-01
  Virtual Account: Eg-VA-01
  Export-Controlled Functionality: ALLOWED
  Last Renewal Attempt: None
  Next Renewal Attempt: Jul 14 02:15:39 2021 UTC

License Authorization:
  Status: AUTHORIZED
  Last Communication Attempt: SUCCEEDED
  Next Communication Attempt: Feb 14 02:37:24 2021 UTC

License Usage:
  License                               Entitlement tag                Count Status
  -----
  ISR_4400_Application (ISR_4400_Application)      1 AUTHORIZED
  ISR_4400_UnifiedComm... (ISR_4400_UnifiedCommun...)  1 AUTHORIZED
  ISR_4400_Security (ISR_4400_Security)          1 AUTHORIZED
  Booster Performance ... (ISR_4460_BOOST)            1 AUTHORIZED
  ISR_4400_Hsec (ISR_4400_Hsec)                    1 AUTHORIZED
```

show license summary After Migration

移行後の出力には、5つのライセンスすべてが移行され、ステータスは IN USE で示されています。

```
Device# show license summary
License Usage:
  License                               Entitlement Tag                Count Status
  -----
  hsec9 (ISR_4400_Hsec)                1 IN USE
  Booster Performance ... (ISR_4460_BOOST)            1 IN USE
  ISR_4400_Application (ISR_4400_Application)      1 IN USE
  ISR_4400_UnifiedComm... (ISR_4400_UnifiedCommun...)  1 IN USE
  ISR_4400_Security (ISR_4400_Security)          1 IN USE
```

移行前と後の show license status

例: スマートライセンス (登録済みおよび承認済みのライセンス) から Smart Licensing Using Policy へ

show license status Before Migration

移行前の出力には、Call Home が設定されたトランスポートタイプであることが示されています。ここではすべてのライセンスのステータスが REGISTERED であるため、トランスポートタイプの設定は移行後も保持されます。

```

Device# show license status
Smart Licensing is ENABLED

Utility:
  Status: DISABLED

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

Transport:
  Type: Callhome

Registration:
  Status: REGISTERED
  Smart Account: Eg-SA-01
  Virtual Account: Eg-VA-01
  Export-Controlled Functionality: ALLOWED
  Initial Registration: SUCCEEDED on Jan 15 02:15:40 2021 UTC
  Last Renewal Attempt: None
  Next Renewal Attempt: Jul 14 02:15:39 2021 UTC
  Registration Expires: Jan 15 01:12:26 2022 UTC

License Authorization:
  Status: AUTHORIZED on Jan 15 02:37:24 2021 UTC
  Last Communication Attempt: SUCCEEDED on Jan 15 02:37:24 2021 UTC
  Next Communication Attempt: Feb 14 02:37:23 2021 UTC
  Communication Deadline: Apr 15 01:34:11 2021 UTC

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

Export Authorization Key:
  Features Authorized:
    <none>

```

show license status After Migration

移行後の出力には、製品インスタンスが Smart Licensing Using Policy であることが示されています (Smart Licensing Using Policy: Status: ENABLED)。

トランスポートタイプは保持されます (Type: Callhome) (ソフトウェアイメージのアップグレード後) システムの再起動時に製品インスタンスが CSSM と通信できていたため、次のイベントがすでに発生しています。

- RUM レポートが送信され、ACK が受信されました (Last report push: Jan 15 03:22:05 2021 UTC, Last ACK received: Jan 15 03:26:07 2021 UTC)。
- ACK とともに返されたポリシーがインストールされています (Policy in use: Installed On Jan 15 03:26:08 2021 UTC)。
- ACK とともに返された信頼コードもインストールされています (Trust Code Installed: Jan 15 03:21:29 2021 UTC)。

```
Device# show license status

Utility:
  Status: DISABLED

Smart Licensing Using Policy:
  Status: ENABLED

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

Transport:
  Type: Callhome

Policy:
  Policy in use: Installed On Jan 15 03:26:08 2021 UTC
  Policy name: SLP Policy
  Reporting ACK required: yes (Customer Policy)
  Unenforced/Non-Export Perpetual Attributes:
    First report requirement (days): 30 (Customer Policy)
    Reporting frequency (days): 60 (Customer Policy)
    Report on change (days): 60 (Customer Policy)
  Unenforced/Non-Export Subscription Attributes:
    First report requirement (days): 120 (Customer Policy)
    Reporting frequency (days): 150 (Customer Policy)
    Report on change (days): 120 (Customer Policy)
  Enforced (Perpetual/Subscription) License Attributes:
    First report requirement (days): 0 (CISCO default)
    Reporting frequency (days): 90 (Customer Policy)
    Report on change (days): 60 (Customer Policy)
  Export (Perpetual/Subscription) License Attributes:
    First report requirement (days): 0 (CISCO default)
    Reporting frequency (days): 30 (Customer Policy)
    Report on change (days): 30 (Customer Policy)

Miscellaneous:
  Custom Id: <empty>

Usage Reporting:
  Last ACK received: Jan 15 03:26:07 2021 UTC
  Next ACK deadline: Mar 16 03:26:07 2021 UTC
  Reporting push interval: 30 days
  Next ACK push check: <none>
  Next report push: Feb 14 03:22:05 2021 UTC
  Last report push: Jan 15 03:22:05 2021 UTC
  Last report file write: <none>

Trust Code Installed: Jan 15 03:21:29 2021 UTC
```

移行前と後の **show license usage**

```
-----
show license usage Before Migration
-----
```

移行前の出力には、使用されているすべてのライセンスが表示されます。

エクスポートステータスが NOT RESTRICTED であるすべてのライセンスは、移行後に適用タイプが NOT ENFORCED になります。

エクスポートステータスが RESTRICTED - ALLOWED のライセンスは、移行後も同じステータスが表示され、適用タイプは EXPORT RESTRICTED になります。

```
Device# show license usage
```

```
License Authorization:
```

```
Status: AUTHORIZED on Jan 15 02:37:24 2021 UTC
```

```
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
```

```
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
```

```
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
```

```
Booster Performance License for 4460 Series (ISR_4460_BOOST):
```

```
Description: Booster Performance License for 4460 Series
```

```
Count: 1
```

```
Version: 1.0
```

```
Status: AUTHORIZED
```

```
Export status: NOT RESTRICTED
```

```
ISR_4400_Hsec (ISR_4400_Hsec):
```

```
Description: U.S. Export Restriction Compliance license for 4400 series
```

```
Count: 1
```

```
Version: 1.0
```

```
Status: AUTHORIZED
```

```
Export status: RESTRICTED - ALLOWED
```

```
Feature Name: hseck9
```

```
Feature Description: Export Controlled Feature hseck9
```

```
-----
show license usage After Migration
-----
```


移行後の出力には、使用されているライセンス（Status: IN USE）とその適用タイプが表示されます。

承認を必要としないライセンスは、Enforcement type: NOT ENFORCED で表示されます。

使用前に承認を必要とする輸出規制ライセンスも、Enforcement type: EXPORT RESTRICTED と Export status: RESTRICTED - ALLOWED で正しく表示されます。つまり、必要な承認が取得されています。

Device# **show license usage**

License Authorization:
Status: Not Applicable

hseck9 (ISR_4400_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
License type: Perpetual

Booster Performance License for 4460 Series (ISR_4460_BOOST):
Description: Booster Performance License for 4460 Series
Count: 1
Version: 1.0
Status: IN USE
Export status: NOT RESTRICTED
Feature Name: booster_performance
Feature Description: booster_performance
Enforcement type: NOT ENFORCED
License type: Perpetual

ISR_4400_Application (ISR_4400_Application):
Description: AppX License for Cisco ISR 4400 Series
Count: 1
Version: 1.0
Status: IN USE
Export status: NOT RESTRICTED
Feature Name: appxk9
Feature Description: appxk9
Enforcement type: NOT ENFORCED
License type: Perpetual

ISR_4400_UnifiedCommunication (ISR_4400_UnifiedCommunication):
Description: Unified Communications License for Cisco ISR 4400 Series
Count: 1
Version: 1.0
Status: IN USE
Export status: NOT RESTRICTED
Feature Name: uck9
Feature Description: uck9
Enforcement type: NOT ENFORCED
License type: Perpetual

ISR_4400_Security (ISR_4400_Security):
Description: Security License for Cisco ISR 4400 Series
Count: 1
Version: 1.0
Status: IN USE

例: スマートライセンス (登録済みおよび承認済みのライセンス) から Smart Licensing Using Policy へ

```
Export status: NOT RESTRICTED
Feature Name: securityk9
Feature Description: securityk9
Enforcement type: NOT ENFORCED
```

移行前と後の show platform hardware throughput level

```
-----
show platform hardware throughput level Before Migration
-----
```

移行前の出力には、スループットレベルがスロットリングされていないことが示されています。Cisco ISR 4000 シリーズ ルータでは、Booster Performance ライセンスによりスロットリングされていない Cisco Express Forwarding (CEF) スループットが有効になります。したがって、移行後もこの設定に変更はありません

```
Device# show platform hardware throughput level
The current throughput level is unthrottled
```

```
-----
show platform hardware throughput level After Migration
-----
```

移行後の出力には、同じスループットレベルの設定が移行後も保持されていることが示されています。

```
Device# show platform hardware throughput level
The current throughput level is unthrottled
```

移行前と後の show platform software cerm-information

```
-----
show platform software cerm-information Before Migration
-----
```

移行前の出力には、CERM機能が無効になっていることが示されています。移行後も、この設定に変更はありません。

```
Device# show platform software cerm-information
Crypto Export Restrictions Manager (CERM) Information:
  CERM functionality: DISABLED
```

```
-----
show platform software cerm-information After Migration
-----
```

移行後の出力には、同じ CERM 設定が移行後も保持されていることが示されています。

```
Device# show platform software cerm-information
Crypto Export Restrictions Manager (CERM) Information:
  CERM functionality: DISABLED
```

移行前と後の show license authorization

show license authorization Before Migration

show license authorization コマンドは、スマートライセンス環境では使用できません。ただし、移行前の確認のために、上記の **show license usage** の出力では必要な許可が取得されていることが示されています。移行前に **show license reservation** コマンドを使用して承認コードをメモしておき、移行後に同じコードが表示されることを確認することもできます。

-

show license authorization After Migration

移行後の出力には、承認コードが移行され、適用されていることが示されています（Status: SMART AUTHORIZATION INSTALLED on Jan 15 03:21:31 2021 UTC）。移行前に承認コードをメモした場合は、[Last Confirmation code:] フィールドで確認できます。このコードは同じになります。

```
Device# show license authorization
Overall status:
  Active: PID:ISR4461/K9,SN:FDO222815Y4
  Status: SMART AUTHORIZATION INSTALLED on Jan 15 03:21:31 2021 UTC
  Last Confirmation code: 30bdf595

Authorizations:
  ISR_4400_Hsec (ISR_4400_Hsec):
    Description: U.S. Export Restriction Compliance license for 4400 series
    Total available count: 1
    Enforcement type: EXPORT RESTRICTED
    Term information:
      Active: PID:ISR4461/K9,SN:FDO222815Y4
      Authorization type: SMART AUTHORIZATION INSTALLED
      License type: PERPETUAL
      Term Count: 1

Purchased Licenses:
  No Purchase Information Available

Derived Licenses:
  Entitlement Tag: regid.2017-12.com.cisco.ISR_4460_BOOST,
  1.0_79633860-0c9a-472c-9306-bb2dfd1b030d
  Entitlement Tag: regid.2015-01.com.cisco.ISR_4400_Application,
  1.0_da87444e-68bb-4821-8aab-63f8531a0430
  Entitlement Tag: regid.2014-12.com.cisco.ISR_4400_UnifiedCommunication,
  1.0_ee2d8156-7e01-4f48-8cad-4859385e6524
  Entitlement Tag: regid.2014-12.com.cisco.ISR_4400_Security,
  1.0_02ea4d4a-2469-46c1-afaf-d6cdfa1980aa
```

移行後に必要なタスク

上記の概要で説明したように、製品インスタンスはすでにアップグレード後すぐに CSSM と同期されており、次のレポートと ACK の期限（Next ACK deadline: Mar 16 03:26:07 2021 UTC）までは移行後に実際に必要になるアクションはありません。十分わかりやすくするために、該当する手順を次に示します。

1. トポロジを実装します。

この例では、移行前の設定（トランスポートタイプが **callhome** の **CSSM に直接接続**（21 ページ）のトポロジ）を保持しています。対応するワークフローについては、**トポロジのワークフロー：CSSM に直接接続**（53 ページ）を参照してください。

スマートアカウントの設定、CSSM への製品インスタンスの接続、接続方式と転送タイプ、および CSSM との信頼の確立はすべて完了しています。これでトポロジの実装は完了です。

2. ライセンスの使用状況を CSSM と同期し、同期を確認し、後続のレポートの要件を確認します。

このトポロジでは、特権 EXEC モードで **license smart sync** コマンドを入力して使用状況を同期できます。これにより、保留中のデータが手動で CSSM と同期（送受信）されます。

次の設定例にはこれが示されています。その後、同期が正常に実行されたことを示し、輸出規制機能の使用が許可されていることを確認するシステムメッセージが続いています。

```
Device# license smart sync local
Device#
*Jan 15 03:55:42.205: %SIP-1-LICENSING: SIP service is Up. License report acknowledged.
*Jan 15 03:55:42.211: %SMART_LIC-6-EXPORT_CONTROLLED: Usage of export controlled
features is allowed for feature hseck9
*Jan 15 03:55:42.686: %SMART_LIC-6-POLICY_INSTALL_SUCCESS: A new licensing policy
was successfully installed
```

同期を確認するには、特権 EXEC モードで **show license all** コマンドを入力します。次の出力例では、次のフィールドを使用して同期を確認できます。

- タイムスタンプの更新：Policy in use: Installed On Jan 15 03:55:42 2021 UTC
- タイムスタンプの更新：Last ACK received: Jan 15 03:55:42 2021 UTC

特権 EXEC モードで **show license all** コマンドを入力して、後続のレポートの要件も確認します。

CSSM への直接接続トポロジでは、製品インスタンスがポリシーに基づいて次の RUM レポートを CSSM に送信します。出力例では、次のフィールドにこの情報が示されています。

- Next ACK deadline: Mar 16 03:55:42 2021 UTC
- Next report push: Feb 14 03:51:41 2021 UTC

```
Device# show license all

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

Smart Licensing Using Policy:
  Status: ENABLED

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

Transport:
  Type: Callhome

Miscellaneous:
  Custom Id: <empty>

Policy:
Policy in use: Installed On Jan 15 03:55:42 2021 UTC
Policy name: SLP Policy
Reporting ACK required: yes (Customer Policy)
Unenforced/Non-Export Perpetual Attributes:
  First report requirement (days): 30 (Customer Policy)
  Reporting frequency (days): 60 (Customer Policy)
  Report on change (days): 60 (Customer Policy)
Unenforced/Non-Export Subscription Attributes:
  First report requirement (days): 120 (Customer Policy)
  Reporting frequency (days): 150 (Customer Policy)
  Report on change (days): 120 (Customer Policy)
Enforced (Perpetual/Subscription) License Attributes:
  First report requirement (days): 0 (CISCO default)
  Reporting frequency (days): 90 (Customer Policy)
  Report on change (days): 60 (Customer Policy)
Export (Perpetual/Subscription) License Attributes:
  First report requirement (days): 0 (CISCO default)
  Reporting frequency (days): 30 (Customer Policy)
  Report on change (days): 30 (Customer Policy)

Usage Reporting:
Last ACK received: Jan 15 03:55:42 2021 UTC
Next ACK deadline: Mar 16 03:55:42 2021 UTC
Reporting push interval: 30 days
Next ACK push check: <none>
Next report push: Feb 14 03:51:41 2021 UTC
Last report push: Jan 15 03:51:41 2021 UTC
Last report file write: <none>

Trust Code Installed: Jan 15 03:21:29 2021 UTC

License Usage
=====

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

例: スマートライセンス (登録済みおよび承認済みのライセンス) から Smart Licensing Using Policy へ

```

Enforcement type: EXPORT RESTRICTED
License type: Perpetual

Booster Performance License for 4460 Series (ISR_4460_BOOST):
Description: Booster Performance License for 4460 Series
Count: 1
Version: 1.0
Status: IN USE
Export status: NOT RESTRICTED
Feature Name: booster_performance
Feature Description: booster_performance
Enforcement type: NOT ENFORCED
License type: Perpetual

ISR_4400_Application (ISR_4400_Application):
Description: AppX License for Cisco ISR 4400 Series
Count: 1
Version: 1.0
Status: IN USE
Export status: NOT RESTRICTED
Feature Name: appxk9
Feature Description: appxk9
Enforcement type: NOT ENFORCED
License type: Perpetual

ISR_4400_UnifiedCommunication (ISR_4400_UnifiedCommunication):
Description: Unified Communications License for Cisco ISR 4400 Series
Count: 1
Version: 1.0
Status: IN USE
Export status: NOT RESTRICTED
Feature Name: uck9
Feature Description: uck9
Enforcement type: NOT ENFORCED
License type: Perpetual

ISR_4400_Security (ISR_4400_Security):
Description: Security License for Cisco ISR 4400 Series
Count: 1
Version: 1.0
Status: IN USE
Export status: NOT RESTRICTED
Feature Name: securityk9
Feature Description: securityk9
Enforcement type: NOT ENFORCED
License type: Perpetual

Product Information
=====
UDI: PID:ISR4461/K9,SN:FDO222815Y4

Agent Version
=====
Smart Agent for Licensing: 5.0.6_rel/47

License Authorizations
=====
Overall status:
  Active: PID:ISR4461/K9,SN:FDO222815Y4
         Status: SMART AUTHORIZATION INSTALLED on Jan 15 03:21:31 2021 UTC
         Last Confirmation code: 30bdf595

Authorizations:
  ISR_4400_Hsec (ISR_4400_Hsec):

```

```

Description: U.S. Export Restriction Compliance license for 4400 series
Total available count: 1
Enforcement type: EXPORT RESTRICTED
Term information:
  Active: PID:ISR4461/K9,SN:FDO222815Y4
  Authorization type: SMART AUTHORIZATION INSTALLED
  License type: PERPETUAL
  Term Count: 1
    
```

```

Purchased Licenses:
  No Purchase Information Available
    
```

```

Derived Licenses:
  Entitlement Tag:
  regid.2017-12.com.cisco.ISR_4460_BOOST,1.0_79633860-0c9a-472c-9306-bb2dfd1b030d
  Entitlement Tag:
  regid.2015-01.com.cisco.ISR_4400_Application,1.0_da87444e-68bb-4821-8aab-63f8531a0430

  Entitlement Tag:
  regid.2014-12.com.cisco.ISR_4400_UnifiedCommunication,1.0_ee2d8156-7e01-4f48-8cad-4859385e6524

  Entitlement Tag:
  regid.2014-12.com.cisco.ISR_4400_Security,1.0_02ea4d4a-2469-46c1-afaf-d6cdfa1980aa
    
```

移行前と後の CSSM Web UI

<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。該当するスマートアカウントとバーチャルアカウントで、[Inventory]>[Product Instances] に移動して、すべての製品インスタンスを表示します。

移行前の CSSM Web UI

スマートライセンス環境では、登録済みのライセンスが製品インスタンスのホスト名とともに [Name] 列に表示されます。次のスクリーンショットに示すように、製品インスタンス名をクリックすると、ライセンス使用状況の詳細情報が表示されます。

例：スマートライセンス（登録済みおよび承認済みのライセンス）から Smart Licensing Using Policy へ

Cisco Software Central > Smart Software Licensing Eg-SA-01

Smart Software Licensing

Feedback Support

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

Virtual Account: **Eg-VA-01** 3 Major 115 Minor Hide Alerts

General Licenses **Product Instances** Event Log

Authorize License-Enforced Features... Search by Device or by Product Type

Name	Product Type	Last Contact	Alerts	Actions
6697d45a0c4811ebbe40562b15b05798	DNASW	2020-Oct-13 21:32:33		Actions
7ef7b996359411eba6e8fe782388d3d8	DNASW	2021-Jan-03 15:23:41		Actions
8c131d90080411eb9efd1e0bd7c2f77d	DNASW	2020-Oct-06 23:36:41		Actions
isr4461	4400ISR	2021-Jan-15 01:18:10		Actions
UDI_PID:C1113-8PMLTEEA; UDI_SN:FGL212491D3;		ISR1K	2020-Nov-18 17:55:49 (Reserved Licenses)	Actions
UDI_PID:C1161X-8P; UDI_SN:FGL23151093;		ISR1K	2020-Oct-18 18:28:33 (Reserved Licenses)	Actions
UDI_PID:C8000V; UDI_SN:9WQCIPHSR8;		CAT8KV	2020-Nov-23 21:16:00	Actions
UDI_PID:C8000V; UDI_SN:9J2V1FUPF7Q;		DNA On Prem	2020-Dec-03 03:28:12 (Reserved Licenses)	Actions
UDI_PID:C8200-1N-4T; UDI_SN:FGL2420L6DT;		CAT8200	2020-Oct-02 21:33:03 (Reserved Licenses)	Actions
UDI_PID:C8300-1N1S-4T2X; UDI_SN:FDO2308A013;		CAT8300	2020-Oct-20 18:05:23	Actions

Showing Page 1 of 3 (25 Records)

isr4461

Overview **Event Log**

Description
ISR 4400 PRD

General

Name: isr4461
 Product: ISR 4400 PRD
 Host Identifier: -
 MAC Address: -
 PID: ISR4461/K9
 Serial Number: FDO222815Y4
 UUID: -
 Virtual Account: Eg-VA-01
 Registration Date: 2021-Jan-15 01:17:28
Last Contact: 2021-Jan-15 01:18:10

License Usage

License	Billing	Expires	Required
ISR_4400_Communication	Prepaid	-	1
ISR_4400_Security	Prepaid	-	1
ISR_4400_Application	Prepaid	-	1
ISR_4400_Usage	Prepaid	-	1

Showing all 4 Rows

移行後の CSSM Web UI

Smart Licensing Using Policy へのアップグレード後、登録済みのライセンスが製品インスタンスの UDI とともに [Name] 列に表示されます。この例では、UDI は PID:ISR4461/K9,SN:FDO222815Y4 です。次のスクリーンショットに示すように、UDI をクリックすると、ライセンス使用状況の詳細な情報が表示されます。

Cisco Software Central > Smart Software Licensing Eg-SA-01

Smart Software Licensing Feedback Support

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

Virtual Account: **Eg-VA-01** 3 Major 115 Minor Hide A

General Licenses **Product Instances** Event Log

Authorize License-Enforced Features... Search by Device or by Product Type

Name	Product Type	Last Contact	Alerts	Actions
UDI_PID:ISR4331/K9; UDI_SN:FDO2139050B;	4300ISR	2020-Sep-18 07:00:10 (Reserved...		Actions
UDI_PID:ISR4431/K9; UDI_SN:FOC21506LVB;	4400ISR	2020-Sep-18 04:56:55 (Reserved...		Actions
UDI_PID:ISR4451-X/K9; UDI_SN:FOC2033A7BP;	4400ISR	2020-Oct-09 18:27:37		Actions
UDI_PID:ISR4461/K9; UDI_SN:FDO222815Y4;	4400ISR	2021-Jan-15 02:53:39		Actions
UDI_PID:ISR4461/K9; UDI_SN:FDO2230A26P;	4400ISR	2020-Oct-08 18:34:20		Actions

10 Showing Page 3 of 3 (25 Records)

例：スマートライセンス（登録済みおよび承認済みのライセンス）から Smart Licensing Using Policy へ

UDI_PID:ISR4461/K9; UDI_SN:FDO222815Y4;

Overview Event Log

Description
ISR 4400 PRD

General

Name: UDI_PID:ISR4461/K9; UDI_SN:FDO222815Y4;
 Product: ISR 4400 PRD
 Host Identifier: -
 MAC Address: -
 PID: ISR4461/K9
 Serial Number: FDO222815Y4
 UUID: -
 Virtual Account: Eg-VA-01
 Registration Date: 2021-Jan-15 02:23:17
 Last Contact: 2021-Jan-15 02:53:39

License Usage

License	Billing	Expires	Required
ISR_4400_Hsec	Prepaid	-	1
ISR_4400_UnifiedCommunication	Prepaid	-	1
ISR_4400_Security	Prepaid	-	1

Showing all 5 Rows

次に、ライセンス使用状況の情報の続きを示します。使用可能なすべてのライセンスを表示するには、スクロールダウンしてください。

License Usage

License	Billing	Expires	Required
ISR_4400_Security	Prepaid	-	1
ISR_4400_Application	Prepaid	-	1
Booster Performance License for 4460 Se..	Prepaid	-	1

Showing all 5 Rows

例：スマートライセンス（輸入規制ライセンスを使用した SLR）から Smart Licensing Using Policy へ

次に、Specific License Reservation（SLR）を使用している場合に **Cisco 1000 シリーズ サービス統合型ルータ**をスマートライセンスから Smart Licensing Using Policy に移行する例を示します。具体的には、輸出規制ライセンスを使用する SLR の場合です。つまり、SLR 承認コードには HSECK9 の承認が含まれます。製品インスタンスのソフトウェアバージョンは、Cisco IOS XE Gibraltar 16.12.4から Cisco IOS XE Bengaluru 17.4.1 にアップグレードされます。



(注) 「予約 (reservation)」の概念は、Smart Licensing Using Policy 環境には適用されません。ここで SLR と同等の機能は、CSSM への接続なしで CSLU なしのトポロジを実装することです。実装されると、製品インスタンスと CSSM は相互に切断されるため、製品インスタンスはネットワークの外部にあるあらゆるものとオンラインで通信できません。SLR からアップグレードすると、既存の SLR 承認コードが移行されます。これには、輸出規制ライセンスの承認コードも含まれています。移行後は、トポロジ自体がエアギャップネットワークで動作できるようになるため、レポート要件を満たす手段が得られます。ライセンスの予約、登録などは適用されません。

- 移行後の適用タイプ：製品インスタンスで使用されている3つのライセンスのうち2つが承認されます（SLR 認証コードを使用）。承認されたライセンスの1つは、輸出規制ライセンス（ISR_1100_8P_Hsec）です。このライセンスは必要な承認が得られているため、移行後も使用でき、移行後の適用タイプは EXPORT RESTRICTED になります。HSECK9 ライセンスを含む SLR 認証コードを持つ製品インスタンスの要点については、[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（37 ページ）](#)を参照してください。アップグレード後に SLAC をインストールする必要はありません。

SLR 承認コード（`show license usage: ISR_1100_8P_UnifiedCommunication, Reservation status: NOT INSTALLED`）がない3番目のライセンスと残りのライセンスは、輸出規制ライセンスではありません（`show license usage: Export status: NOT RESTRICTED`）。このライセンスも移行され、移行後は適用タイプが NOT ENFORCED になります。

- 移行後のトランスポートタイプ：これは SLR からのアップグレードであるため、ソフトウェアバージョンがアップグレードされると、トランスポートタイプはオフになります。
- Device-Led Conversion（DLC）：このシナリオでは、前のスマートライセンス環境からの承認済みライセンスと予約済みライセンスであるため（すでにスマートライセンスであるため）DLC はこれらのライセンスに適用されません。
- 移行後のレポート：最初の同期では、RUM レポートが CSSM に手動でアップロードされ、対応する ACK が製品インスタンスにインストールされます。アップグレード前の環境では承認コードがありませんでしたが、この最初の同期では、ISR_1100_8P_UnifiedCommunication ライセンスの使用状況レポートの要件にも対応します。

同じレポート方式が後続のレポートにも適用されます (レポートが必要な場合)。最初の同期が完了したら、**show license status** コマンドまたは **show license all** コマンドの出力を参照して、レポートが必要かどうかといつまでに必要化を確認します。出力で [Next report push] フィールドと [Next ACK deadline] フィールドを確認します。また、レポートが必要な場合にもシステムメッセージが表示されます。

移行前と後の show コマンド

移行前と後の show version

```
-----
show version Before Migration
-----
```

次の出力には、アップグレード前のソフトウェアバージョンが示されています。

```
Device# show version
Cisco IOS XE Software, Version 16.12.04 Cisco IOS Software [Gibraltar],
ISR Software (ARMV8EL_LINUX_IOSD-UNIVERSALK9-M), Version 16.12.4, RELEASE SOFTWARE (fc4)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2020 by Cisco Systems, Inc.
Compiled Thu 25-Jun-20 12:56 by mcpre
<output truncated>
```

```
-----
show version After Migration
-----
```

この出力には、移行後のソフトウェアバージョンと、新しいイメージでシステムを再起動したときに表示されるライセンス関連のシステムメッセージの抜粋が示されています。

```
Device# show version
Cisco IOS XE Software, Version 17.4.1a Cisco IOS Software [Bengaluru],
ISR Software (ARMV8EL_LINUX_IOSD-UNIVERSALK9-M), Version 17.4.1a, RELEASE SOFTWARE (fc4)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2020 by Cisco Systems, Inc.
Compiled Thu 17-Dec-20 22:38 by mcpre
<output truncated>
```

```
<output truncated>
Press RETURN to get started!
```

```
*Jan 19 07:09:06.615: %SMART_LIC-6-RESERVED_INSTALLED:
Specific License Reservation Authorization Code installed for
udi PID:C1111-8PLTEEAWB,SN:FGL214391JK
*Jan 19 07:09:06.616: %SMART_LIC-6-EXPORT_CONTROLLED:
Usage of export controlled features is not allowed
*Jan 19 07:09:07.174: %SMART_LIC-6-EXPORT_CONTROLLED:
Usage of export controlled features is allowed for feature hseck9
*Jan 19 07:09:09.163: %SMART_LIC-6-REPORTING_REQUIRED:
A Usage report acknowledgement will be required in 365 days.
<output truncated>
```

移行前と後の show license summary

show license summary Before Migration

移行前の出力では、2つのライセンスが **AUTHORIZED**、1つのライセンスが **NOT AUTHORIZED** と示されています。uck9 ライセンスは、輸出規制ライセンスまたは適用済みライセンスではないため、すべてのライセンスが移行され、すべてのライセンスが **IN USE** として表示されます。

Device# **show license summary**

Smart Licensing is ENABLED
 License Reservation is ENABLED

Registration:
 Status: REGISTERED - SPECIFIC LICENSE RESERVATION
 Export-Controlled Functionality: ALLOWED

License Authorization:
 Status: NOT AUTHORIZED

License Usage:

License	Entitlement tag	Count	Status
Cisco 1100 Series wi...	(ISR_1100_8P_Foundation...)	1	AUTHORIZED
uck9	(ISR_1100_8P_UnifiedCom...)	1	NOT AUTHORIZED
hseck9	(ISR_1100_8P_Hsec)	1	AUTHORIZED

show license summary After Migration

移行後の出力には、3つすべてのライセンスが移行されていることが示され、ステータスは **IN USE** で表示されています。

Device# **show license summary**

License Reservation is ENABLED

License Usage:

License	Entitlement Tag	Count	Status
hseck9	(ISR_1100_8P_Hsec)	1	IN USE
uck9	(ISR_1100_8P_UnifiedCom...)	1	IN USE
FoundationSuiteK9	(ISR_1100_8P_Foundation...)	1	IN USE

移行前と後の **show license status**

show license status Before Migration

移行前の出力にはデフォルトのトランスポートタイプが表示されることが示されています。ただし、この製品インスタンスのライセンスは予約済みのライセンスであるため（SLRが有効）、トランスポートタイプは移行後にオフになり、エアギャップネットワークでの動作が継続されます。

例: スマートライセンス (輸入規制ライセンスを使用した SLR) から Smart Licensing Using Policy へ

```
Device# show license status

Smart Licensing is ENABLED

Utility:
  Status: DISABLED
License Reservation is ENABLED

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

Transport:
  Type: Callhome

Registration:
  Status: REGISTERED - SPECIFIC LICENSE RESERVATION
  Export-Controlled Functionality: ALLOWED
  Initial Registration: SUCCEEDED on Jan 19 06:27:47 2021 UTC

License Authorization:
  Status: NOT AUTHORIZED

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

Export Authorization Key:
  Features Authorized:
    <none>
```

show license status After Migration

移行後の出力には、製品インスタンスが Smart Licensing Using Policy であることが示されています (Smart Licensing Using Policy: Status: ENABLED)。

トランスポートタイプはオフに設定されます (Type: Transport Off)。つまり、製品インスタンスは CSSM とも、ネットワーク外のあらゆるものとも通信できません。

ここでは、デフォルトのポリシーが有効になっています。(他のポリシーが使用できない場合、製品インスタンスは表 6: ポリシー: Cisco default ポリシーを適用します)。カスタムポリシーが CSSM で使用可能である場合は、最初の同期の後も同じポリシーがインストールされます。同期は、現在のポリシーが必要とするレポートにも対応します (Next ACK deadline: Jan 19 07:09:09 2022 UTC)。

```
Device# show license status

Utility:
  Status: DISABLED

Smart Licensing Using Policy:
  Status: ENABLED
License Reservation is ENABLED

Data Privacy:
  Sending Hostname: yes
```

```

Callhome hostname privacy: DISABLED
Smart Licensing hostname privacy: DISABLED
Version privacy: DISABLED

Transport:
  Type: Transport Off

Policy:
Policy in use: Merged from multiple sources.
Reporting ACK required: yes (CISCO default)
Unenforced/Non-Export Perpetual Attributes:
  First report requirement (days): 365 (CISCO default)
  Reporting frequency (days): 0 (CISCO default)
  Report on change (days): 90 (CISCO default)
Unenforced/Non-Export Subscription Attributes:
  First report requirement (days): 90 (CISCO default)
  Reporting frequency (days): 90 (CISCO default)
  Report on change (days): 90 (CISCO default)
Enforced (Perpetual/Subscription) License Attributes:
  First report requirement (days): 0 (CISCO default)
  Reporting frequency (days): 0 (CISCO default)
  Report on change (days): 0 (CISCO default)
Export (Perpetual/Subscription) License Attributes:
  First report requirement (days): 0 (CISCO default)
  Reporting frequency (days): 0 (CISCO default)
  Report on change (days): 0 (CISCO default)

Miscellaneous:
  Custom Id: <empty>

Usage Reporting:
  Last ACK received: <none>
  Next ACK deadline: Jan 19 07:09:09 2022 UTC
  Reporting push interval: 30 days
  Next ACK push check: <none>
  Next report push: Jan 19 07:11:09 2021 UTC
  Last report push: <none>
  Last report file write: <none>

Trust Code Installed: <none>

```

移行前と後の show license usage

```
-----
show license usage Before Migration
-----
```

移行前の出力には、使用されているすべてのライセンスが表示されます。

エクスポートステータスが NOT RESTRICTED であるすべてのライセンスは、移行後に適用タイプが NOT ENFORCED になります。（これには、移行前のステータスが NOT AUTHORIZED のライセンスも含まれます）。

エクスポートステータスが RESTRICTED-ALLOWED のライセンスは、移行後も同じステータスが表示され、適用タイプは EXPORT RESTRICTED になります。

使用可能なすべての承認コードが移行されます。これには ISR_1100_8P_FoundationSuite ライセンスの SLR 承認コード（予約ステータス：SPECIFIC INSTALLED）と、輸出規制

例：スマートライセンス（輸入規制ライセンスを使用した SLR）から Smart Licensing Using Policy へ

ISR_1100_8P_Hsec ライセンスの SLR 承認コード（予約ステータス：SPECIFIC EXPORT AUTHORIZATION KEY INSTALLED）が含まれています。

SLR 承認コードは ISR_1100_8P_UnifiedCommunication ライセンスにインストールされないため（予約ステータス：NOT INSTALLED）、移行するコードはありませんが、ライセンスは移行されます。

```
Device# show license usage
```

```
License Authorization:
  Status: NOT AUTHORIZED
```

```
Cisco 1100 Series with 8 LAN Ports, Cisco One Foundation Suite
(ISR_1100_8P_FoundationSuite):
  Description: Cisco 1100 Series with 8 LAN Ports, Cisco One Foundation Suite
  Count: 1
  Version: 1.0
  Status: AUTHORIZED
  Export status: NOT RESTRICTED
  Reservation:
    Reservation status: SPECIFIC INSTALLED
    Total reserved count: 1
```

```
(ISR_1100_8P_UnifiedCommunication):
  Description:
  Count: 1
  Version: 1.0
  Status: NOT AUTHORIZED
  Export status: NOT RESTRICTED
  Reservation:
    Reservation status: NOT INSTALLED
```

```
hsec9 (ISR_1100_8P_Hsec):
  Description: Export Controlled Feature hsec9
  Count: 1
  Version: 1.0
  Status: AUTHORIZED
  Export status: RESTRICTED - ALLOWED
  Feature Name: hsec9
  Feature Description: Export Controlled Feature hsec9
  Reservation:
    Reservation status: SPECIFIC EXPORT AUTHORIZATION KEY INSTALLED
    Total reserved count: UNLIMITED
```

```
-----
show license usage After Migration
-----
```

移行後の出力には、使用されていたすべてのライセンスが移行され、使用可能なすべての認証コードも移行されたことが示されています

```
Device# show license usage
```

```
License Authorization:
  Status: Not Applicable
```

```
hsec9 (ISR_1100_8P_Hsec):
  Description: hsec9
  Count: 1
  Version: 1.0
  Status: IN USE
  Export status: RESTRICTED - ALLOWED
```

```

Feature Name: hseck9
Feature Description: hseck9
Enforcement type: EXPORT RESTRICTED
License type: Perpetual
Reservation:
  Reservation status: SPECIFIC EXPORT AUTHORIZATION KEY INSTALLED
  Total reserved count: UNLIMITED

uck9 (ISR_1100_8P_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
License type: Perpetual
Reservation:
  Reservation status: NOT INSTALLED

FoundationSuiteK9 (ISR_1100_8P_FoundationSuite):
Description: FoundationSuiteK9
Count: 1
Version: 1.0
Status: IN USE
Export status: NOT RESTRICTED
Feature Name: FoundationSuiteK9
Feature Description: FoundationSuiteK9
Enforcement type: NOT ENFORCED
License type: Perpetual
Reservation:
  Reservation status: SPECIFIC INSTALLED
  Total reserved count: 1
    
```

移行前と後の **show platform hardware throughput level** と **show platform hardware throughput crpto**

show platform hardware throughput level and show platform hardware throughput crypto Before Migration

移行前の出力には、Cisco Express Forwarding (CEF) のスループットと暗号化スループットがスロットリングされていないことが示されています。使用可能な HSECK9 ライセンスは、スロットリングされていない暗号化スループットの使用を許可します。したがって、移行後もこの設定に変更はありません

```

Device# show platform hardware throughput level
The current throughput level is unthrottled

Device# show platform hardware throughput crypto
The current crypto level is unthrottled
    
```

show platform hardware throughput level and show platform hardware throughput crypto After Migration

移行後の出力は、移行後のCEFスループットと暗号化設定が同じであることを示しています。

```
Device# show platform hardware throughput level
The current throughput level is unthrottled

Device# show platform hardware throughput crypto
The current crypto level is unthrottled
```

移行前と後の show platform software cerm-information

```
show platform software cerm-information Before Migration
```

移行前の出力には、スループットレベルがスロットリングされていないことが示されています。移行後も、この設定に変更はありません。

```
Device# show platform software cerm-information
Crypto Export Restrictions Manager(CERM) Information:
  CERM functionality: DISABLED
```

```
show platform software cerm-information After Migration
```

移行後の出力には、CERM 設定が移行後も同じであることが示されています。

```
Device# show platform software cerm-information
Crypto Export Restrictions Manager(CERM) Information:
  CERM functionality: DISABLED
```

show license authorization 移行後

```
show license authorization Before Migration
```

show license authorization コマンドは、スマートライセンス環境では使用できません。ただし、移行前の確認のために、上記の **show license usage** の出力では必要な許可が取得されていることが示されています。移行前に **show license reservation** コマンドを使用して承認コードをメモしておき、移行後に同じコードが表示されることを確認することもできます。

```
show license authorization After Migration
```

移行後の出力には、使用可能なすべての承認コードが移行され、適用されていることが示されています (Status: SPECIFIC INSTALLED on Jan 19 05:59:54 2021 UTC、Last Confirmation code: 0708eeec)。

```
Device# show license authorization

Overall status:
  Active: PID:C1111-8PLTEEAWB,SN:FGL214391JK
  Status: SPECIFIC INSTALLED on Jan 19 05:59:54 2021 UTC
  Last Confirmation code: 0708eeec
```

```

Specified license reservations:
  Cisco 1100 Series with 8 LAN Ports,
Cisco One Foundation Suite (ISR_1100_8P_FoundationSuite):
  Description: Cisco 1100 Series with 8 LAN Ports,
Cisco One Foundation Suite
  Total reserved count: 1
  Enforcement type: NOT ENFORCED
  Term information:
    Active: PID:C1111-8PLTEEAWB,SN:FGL214391JK
      Authorization type: SPECIFIC INSTALLED on Jan 19 05:59:54 2021 UTC
      License type: PERPETUAL
      Term Count: 1
  ISR_1100_8P_Hsec (ISR_1100_8P_Hsec):
  Description: Cisco 1100 Series with 8 LAN Ports,
U.S. Export Restriction Compliance license
  Total reserved count: 1
  Enforcement type: EXPORT RESTRICTED
  Term information:
    Active: PID:C1111-8PLTEEAWB,SN:FGL214391JK
      Authorization type: SPECIFIC INSTALLED on Jan 19 05:59:54 2021 UTC
      License type: PERPETUAL
      Term Count: 1

Purchased Licenses:
  No Purchase Information Available

Derived Licenses:
  Entitlement Tag: regid.2017-08.com.cisco.ISR_1100_8P_Hsec,
1.0_34a5e7e7-722a-41ab-bdad-d53d5a3cac14
  Entitlement Tag: regid.2018-12.com.cisco.ISR_1100_8P_UnifiedCommunication,
1.0_55775cb5-538d-482e-b57f-fc8af02f93a3
  Entitlement Tag: regid.2017-04.com.cisco.ISR_1100_8P_FoundationSuite,
1.0_6f4a1f6f-b607-45cb-8bd0-d672ac06a314
    
```

移行後に必要なタスク

1. トポロジを実装します。

この例では、CSSM への接続がなく、CSLU のないトポロジを実装します。[CSSM への接続なし、CSLU なし（28 ページ）](#) 対応するワークフローは [トポロジのワークフロー：CSSM への接続なし、CSLU なし（63 ページ）](#) のとおりです。

SLR から移行すると、トランスポートタイプは自動的にオフに設定されます。移行後の **show license status** コマンドの出力例には、これが実行されたことが示されています。

輸出規制ライセンスが使用されており、これに対応する承認コードが移行されています。アップグレード後に SLAC を再度インストールする必要はありません。

これにより、エアギャップネットワークで動作するトポロジの実装が完了します。

2. ライセンスの使用状況を CSSM と同期し、同期を確認し、後続のレポートの要件を確認します。

このトポロジでは、RUM レポートを（製品インスタンスの）ファイルに保存し、CSSM に（インターネットと CSSM に接続しているワークステーションから）アップロードする必

必要があります。その後に、ACK をダウンロードして製品インスタンスにインストールする必要があります。

1. ライセンスの使用状況と CSSM の同期

次に示す設定例では、RUM レポートは製品インスタンスのフラッシュメモリの `usage_report` というファイルに保存されます。次にレポートは CSSM にアップロードするために TFTP の場所に転送されます。

```
Device# license smart save usage unreported file usage_report
Device# dir bootflash:
Directory of bootflash:/

73441  drwx           40960  Jan 19 2021 07:26:57 +00:00  tracelogs
23     -rw-           3950   Jan 19 2021 07:26:26 +00:00  usage_report
48961  drwx           4096   Jan 19 2021 07:09:15 +00:00  .installer
122401 drwx           4096   Jan 19 2021 07:08:36 +00:00  license_evlog
106082 drwx           4096   Jan 19 2021 07:08:23 +00:00  .geo
13     -rw-            30    Jan 19 2021 07:08:21 +00:00  throughput_monitor_params
171361 drwx           4096   Jan 19 2021 04:17:00 +00:00  .rollback_timer
11     -rw-          542523052 Jan 19 2021 04:14:17 +00:00  c1100-universalk9.16.12.04.SPA.bin

2908606464 bytes total (1558736896 bytes free)
<output truncated>
```

```
Device# copy bootflash:usage_report tftp://10.8.0.6//user01/usage_report
Address or name of remote host [10.8.0.6]?
Destination filename [/user01/usage_report]?
!!
3950 bytes copied in 0.012 secs (329167 bytes/sec)
```

次に示すスクリーンショットと設定例では、RUM レポートは CSSM にアップロードされます。処理されると、ACK がダウンロードされ、製品インスタンスにインストールされます。

ACK が製品インスタンスにインストールされた後に表示されるシステムメッセージが示すように、ACK にはカスタムポリシーも備わっています。

- CSSM Web UI にログインし、[Smart Software Licensing] リンクを選択します。

The screenshot shows the CSSM Web UI interface with three main sections:

- Download & Upgrade:** Includes links for Software Download, eDelivery, and Version Upgrade using MCE (marked as New).
- Network Plug and Play:** Includes links for Plug and Play Connect and Learn about Network Plug and Play.
- License:** Includes links for Traditional Licensing, Smart Software Licensing (highlighted with a red box), Enterprise Agreements, View My Consumption, and True Forward Consumption dashboard.

- [Reports]> [Usage Data Files]> [Upload Usage Data] をクリックして、RUM レポートをアップロードします。

Cisco Software Central > Smart Software Licensing

Smart Software Licensing

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

Virtual Account: Eg-VA-01 3 Major 115

Cisco Software Central > Smart Software Licensing

Smart Software Licensing

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

Reports

Report: Usage Data Files | Reporting Policy | Synch File for Device Controllers

Name	Description
Licenses	Includes a summary of current license counts and usage over selected virtual acc
License Subscriptions	Includes a summary of current subscription license counts and usage over select
Product Instances	Includes count and listing of current product instances for selected virtual account

Reports

Report: Usage Data Files | Reporting Policy | Synch File for Device Controllers

Devices can be configured to report the features that they are using.
This usage then determines which licenses are needed, in order to be compliant.

Upload Usage Data...

Search by File Name, Virtual Account

Usage Data File	Reported	Virtual Account	Reporting Status	Device
-----------------	----------	-----------------	------------------	--------

- [Browse] をクリックしてファイルを見つけ、[Upload Data] をクリックして RUM レポートをアップロードします。

Upload Usage Data

Please select the Usage File you wish to upload.

* Usage Data File: usage_report

- RUM レポートを受信するバーチャルアカウントを選択し、[Acknowledgment] 列に ACK が表示されるまで待ちます。

Select Virtual Accounts

Some of the usage data files do not include the name of the virtual account that the data refers to, or the virtual account is unrecognized.

Please select an account:

- Select one account for all files:
- Select a virtual account per file:

Report	Usage Data Files	Reporting Policy	Synch File for Device Controllers										
<p>Devices can be configured to report the features that they are using. This usage then determines which licenses are needed, in order to be compliant.</p> <p><input type="button" value="Upload Usage Data..."/></p> <p style="text-align: right;"><small>Search by File Name, Virtual Account</small></p> <table border="1"> <thead> <tr> <th>Usage Data File</th> <th>Reported</th> <th>Virtual Account</th> <th>Reporting Status</th> <th>Devices</th> </tr> </thead> <tbody> <tr> <td>usage_report</td> <td>2021-Jan-19</td> <td>Eg-VA-01</td> <td> Data Being Processed</td> <td>0</td> </tr> </tbody> </table>				Usage Data File	Reported	Virtual Account	Reporting Status	Devices	usage_report	2021-Jan-19	Eg-VA-01	Data Being Processed	0
Usage Data File	Reported	Virtual Account	Reporting Status	Devices									
usage_report	2021-Jan-19	Eg-VA-01	Data Being Processed	0									

- レポートステータスが [No Errors] に変わるのを待ってから、ACK をダウンロードします。

Reports

Report Usage Data Files Reporting Policy Synch File for Device Controllers

Devices can be configured to report the features that they are using.
This usage then determines which licenses are needed, in order to be compliant.

Upload Usage Data...

Search by File Name, Virtual Account

Usage Data File	Reported	Virtual Account	Reporting Status	Devices
usage_report	2021-Jan-19	Eg-VA-01	No Errors	1

- ダウンロードした場所からファイルをコピーし、製品インスタンスのフラッシュメモリに保存し（**copy source bootflash:file-name**）、製品インスタンスに **ACK** をインストールします。

```
Device# copy tftp://10.8.0.6//user01 bootflash:ACK_usage_report.txt
```

```
Device# license smart import bootflash: ACK_usage_report.txt
```

```
Import Data Successful
```

```
Device#
```

```
*Jan 19 07:50:33.311: %SIP-1-LICENSING: SIP service is Up. License report acknowledged.
```

```
*Jan 19 07:50:33.667: %SMART_LIC-6-EXPORT_CONTROLLED: Usage of export controlled features is allowed for feature hseck9
```

```
*Jan 19 07:50:34.131: %SMART_LIC-6-POLICY_INSTALL_SUCCESS: A new licensing policy was successfully installed
```

- 同期を確認し、更新されたポリシーをチェックして後続のレポートの要件を確認します。

次の出力例では、次のフィールドを使用して同期を確認できます。

- タイムスタンプの更新：Policy in use: Installed On Jan 19 07:50:34 2021 UTC
- タイムスタンプの更新：Last ACK received: Jan 19 07:50:33 2021 UTC

後続のレポートが必要な場合は、ポリシーに示され、システムメッセージが表示されます。次に、上記の手順2に示すように **RUM** レポートをアップロードする必要があります（すべてのサブ手順を含む）。出力例の次のフィールドには、レポートが必要かどうかといつ必要かの情報が示されています。

- Next report push: Jan 19 07:51:04 2021 UTC
- Next ACK deadline: Feb 18 07:50:34 2021 UTC

```
Device# show license all
```

```
Smart Licensing Status
```

```
=====
```

```
Smart Licensing is ENABLED
```

```
License Reservation is ENABLED
```

```
License Conversion:
```


例: スマートライセンス (輸入規制ライセンスを使用した SLR) から Smart Licensing Using Policy へ

```

Automatic Conversion Enabled: False
Status: Not started

Export Authorization Key:
  Features Authorized:
    <none>

Utility:
  Status: DISABLED

Smart Licensing Using Policy:
  Status: ENABLED

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

Transport:
  Type: Transport Off

Miscellaneous:
  Custom Id: <empty>

Policy:
  Policy in use: Installed On Jan 19 07:50:34 2021 UTC
  Policy name: SLP Policy
  Reporting ACK required: yes (Customer Policy)
  Unenforced/Non-Export Perpetual Attributes:
    First report requirement (days): 30 (Customer Policy)
    Reporting frequency (days): 60 (Customer Policy)
    Report on change (days): 60 (Customer Policy)
  Unenforced/Non-Export Subscription Attributes:
    First report requirement (days): 120 (Customer Policy)
    Reporting frequency (days): 150 (Customer Policy)
    Report on change (days): 120 (Customer Policy)
  Enforced (Perpetual/Subscription) License Attributes:
    First report requirement (days): 0 (CISCO default)
    Reporting frequency (days): 90 (Customer Policy)
    Report on change (days): 60 (Customer Policy)
  Export (Perpetual/Subscription) License Attributes:
    First report requirement (days): 0 (CISCO default)
    Reporting frequency (days): 30 (Customer Policy)
    Report on change (days): 30 (Customer Policy)

Usage Reporting:
  Last ACK received: Jan 19 07:50:33 2021 UTC
  Next ACK deadline: Feb 18 07:50:34 2021 UTC
  Reporting push interval: 30 days
  Next ACK push check: <none>
  Next report push: Jan 19 07:51:04 2021 UTC
  Last report push: <none>
  Last report file write: <none>

Trust Code Installed: <none>

License Usage
=====

hseck9 (ISR_1100_8P_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
License type: Perpetual
Reservation:
  Reservation status: SPECIFIC EXPORT AUTHORIZATION KEY INSTALLED
  Total reserved count: UNLIMITED

uck9 (ISR_1100_8P_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
License type: Perpetual
Reservation:
  Reservation status: NOT INSTALLED

FoundationSuiteK9 (ISR_1100_8P_FoundationSuite):
Description: FoundationSuiteK9
Count: 1
Version: 1.0
Status: IN USE
Export status: NOT RESTRICTED
Feature Name: FoundationSuiteK9
Feature Description: FoundationSuiteK9
Enforcement type: NOT ENFORCED
License type: Perpetual
Reservation:
  Reservation status: SPECIFIC INSTALLED
  Total reserved count: 1

Product Information
=====
UDI: PID:C1111-8PLTEEAWB,SN:FGL214391JK

Agent Version
=====
Smart Agent for Licensing: 5.0.6_rel/47

License Authorizations
=====
Overall status:
  Active: PID:C1111-8PLTEEAWB,SN:FGL214391JK
  Status: SPECIFIC INSTALLED on Jan 19 05:59:54 2021 UTC
  Last Confirmation code: 0708eeec

Specified license reservations:
  Cisco 1100 Series with 8 LAN Ports, Cisco One Foundation Suite
  (ISR_1100_8P_FoundationSuite):
    Description: Cisco 1100 Series with 8 LAN Ports, Cisco One Foundation Suite
    Total reserved count: 1
    Enforcement type: NOT ENFORCED
    Term information:
      Active: PID:C1111-8PLTEEAWB,SN:FGL214391JK
      Authorization type: SPECIFIC INSTALLED on Jan 19 05:59:54 2021 UTC
      License type: PERPETUAL
      Term Count: 1
  ISR_1100_8P_Hsec (ISR_1100_8P_Hsec):

```

例: スマートライセンス (輸入規制ライセンスを使用した SLR) から Smart Licensing Using Policy へ

```
Description: Cisco 1100 Series with 8 LAN Ports, U.S. Export Restriction
Compliance license
Total reserved count: 1
Enforcement type: EXPORT RESTRICTED
Term information:
  Active: PID:C1111-8PLTEEAWB,SN:FGL214391JK
  Authorization type: SPECIFIC INSTALLED on Jan 19 05:59:54 2021 UTC
  License type: PERPETUAL
  Term Count: 1

Purchased Licenses:
  No Purchase Information Available

Derived Licenses:
  Entitlement Tag:
  regid.2017-08.com.cisco.ISR_1100_8P_Hsec,1.0_34a5e7e7-722a-41ab-bdad-d53d5a3cac14

  Entitlement Tag:
  regid.2018-12.com.cisco.ISR_1100_8P_UnifiedCommunication,1.0_55775cb5-538d-482e-b57f-fc8af02f93a3

  Entitlement Tag:
  regid.2017-04.com.cisco.ISR_1100_8P_FoundationSuite,1.0_6f4a1f6f-b607-45cb-8bd0-d672ac06a314
```

移行前と後の CSSM Web UI

<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。該当するスマートアカウントとバーチャルアカウントで、[Inventory]>[Product Instances] に移動して、すべての製品インスタンスを表示します。

移行前の CSSM Web UI

[Product Instances] タブで UDI をクリックし、次に示すように詳細なライセンス使用情報を表示します。

UDI_PID:C1111-8PLTEEAWB; UDI_SN:FGL214391JK;

Overview

Event Log

Description

Cisco 1100 Series Integrated Services Router, 8 LAN Ports

General

Name:	UDI_PID:C1111-8PLTEEAWB; UDI_SN:FGL214391JK;
Product:	Cisco 1100 Series Integrated Services Router, 8 LAN Ports
Host Identifier:	-
MAC Address:	-
PID:	C1111-8PLTEEAWB
Serial Number:	FGL214391JK
UUID:	-
Virtual Account:	Eg-VA-01
Registration Date:	2021-Jan-19 04:43:14
Last Contact:	2021-Jan-19 04:43:14 (Reserved Licenses) - Download Reservation Authorization Code

License Usage These licenses are reserved on this product instance [Update res...](#)

License	Billing	Expires	Required
Cisco 1100 Series with 8 LAN Ports, Cisco One Fou..	Prepaid	-	1
ISR_1100_8P_Hsec	Prepaid	-	1

移行後の CSSM Web UI

[Product Instances] タブで UDI をクリックし、次に示すように詳細なライセンス使用情報を表示します。

Smart Licensing Using Policy へのアップグレード後、および必要な RUM レポートがアップロードされた後で [Last Contact] フィールドが更新されます。

例：スマートライセンス（スループットが **250 Mbps** を超える **SLR**、輸出規制ライセンスなし）から **Smart Licensing Using Policy** へ

UDI_PID:C1111-8PLTEEAWB; UDI_SN:FGL214391JK;

Overview Event Log

Description

Cisco 1100 Series Integrated Services Router, 8 LAN Ports

General

Name: UDI_PID:C1111-8PLTEEAWB; UDI_SN:FGL214391JK;

Product: Cisco 1100 Series Integrated Services Router, 8 LAN Ports

Host Identifier: -

MAC Address: -

PID: C1111-8PLTEEAWB

Serial Number: FGL214391JK

UUID: -

Virtual Account: Eg-VA-01

Registration Date: 2021-Jan-19 06:47:18

Last Contact: 2021-Jan-19 06:47:21

License Usage

License	Billing	Expires	Required
Cisco 1100 Series with 8 LAN Ports, Cisco One Fou..	Prepaid	-	1
ISR_1100_8P_Hsec	Prepaid	-	1
ISR_1100_8P_UnifiedCommunication	Prepaid	-	1

例：スマートライセンス（スループットが **250 Mbps** を超える **SLR**、輸出規制ライセンスなし）から **Smart Licensing Using Policy** へ

次に、特定のライセンス予約（SLR）ライセンスが使用されているシスコクラウドサービスルータ **1000v** のスマートライセンスから **Smart Licensing Using Policy** への移行の例を示します。製品インスタンスのソフトウェアバージョンは、Cisco IOS XE Gibraltar 16.12.2（CSRv .bin イメージ）から Cisco IOS XE Bengaluru 17.6.1（Catalyst 8000V ソフトウェアイメージ）に **Smart Licensing Using Policy** をサポートするためにアップグレードされます。



重要 250 Mbps を超えるスループットが設定されているすべてのシスコクラウドサービスルータ 1000v と Cisco サービス統合型仮想ルータについては、CSSM で輸出規制フラグが有効になっており、250 Mbps を超えるスループットが許可されますが、HSECK9 ライセンスではありません。この例の製品インスタンスのスループットも 250 Mbps を超えており、さらに予約済みライセンスを使用しています。そのため、SLR コードには HSECK9 ライセンスが含まれておらず、逆に CSSM の輸出規制フラグが有効になっています。

米国の輸出管理規制により、250 Mbps を超えるスループットを許可する方法として輸出規制フラグを使用することは許可されなくなりました。したがって、**Smart Licensing Using Policy** 環境では、SLAC のインストールが必要です。（承認コード（12 ページ）を参照）。

スループットが 250 Mbps 以下の場合、SLAC のインストールは必要ありません。

この例のように製品インスタンスをアップグレードする場合、アップグレード後にスループットが中断されないように、製品インスタンスをアップグレードする前に該当する HSECK9 ライセンスが含まれるように SLR 承認コードを更新することをお勧めします。次に、これを行う例を示します。このタスクを最初に実行せずにソフトウェアイメージをアップグレードすると、Smart Licensing Using Policy へのアップグレード後、SLAC がインストールされるまではスループットが 250 Mbps に設定されます。SLAC のインストール後すぐに、最後に設定した値が復元されます。

次に、この例の場合にアップグレード後はどうなるかについての概要を示します。

- 移行後の適用タイプ：SLR 承認コードに HSECK9 ライセンスを含めるために、アップグレード前に製品インスタンスの予約済みライセンスが更新されています。次の「移行前に必要なタスク」の項を参照してください。したがって、アップグレード前に製品インスタンスで2つのライセンスを使用できます。HSECK9 ライセンスは移行後も使用でき、適用タイプは EXPORT RESTRICTED です。残りのライセンスは使用でき、移行後の適用タイプは NOT ENFORCED です。
- 移行後のトランスポートタイプ：これは SLR からのアップグレードであるため、ソフトウェアバージョンがアップグレードされると、トランスポートタイプはオフになります。
- Device-Led Conversion (DLC)：このシナリオでは、前のスマートライセンス環境からの承認済みライセンスと予約済みライセンスであるため（すでにスマートライセンスであるため）DLC はこれらのライセンスに適用されません。
- 移行後のレポート：最初の同期では、RUM レポートが CSSM に手動でアップロードされ、対応する ACK が製品インスタンスにインストールされます。

同じレポート方式が後続のレポートにも適用されます（レポートが必要な場合）。最初の同期が完了したら、**show license status** コマンドまたは **show license all** コマンドの出力を参照して、レポートが必要かどうかといつまでに必要化を確認します。出力で [Next report push] フィールドと [Next ACK deadline] フィールドを確認します。また、レポートが必要な場合にもシステムメッセージが表示されます。

移行前に必要なタスク

CSSM で輸出規制フラグを有効にして 250 Mbps を超えるスループットを使用する場合は、製品インスタンスのソフトウェアバージョンをアップグレードする前に SLR コードに HSECK9 ライセンスを追加することによって、Smart Licensing Using Policy へのアップグレード時にスループットが中断されないようにします。



(注) この時点では、製品インスタンスはまだ以前のスマートライセンス環境にあるため、対応するコマンドが適用されます。

1. 製品インスタンスで現在使用可能なライセンスを表示します。

```
Device# show version
Cisco IOS XE Software, Version 16.12.02
Cisco IOS Software [Gibraltar], Virtual XE Software (X86_64_LINUX_IOSD-UNIVERSALK9-M),
```

例: スマートライセンス (スループットが **250 Mbps** を超える **SLR**、輸出規制ライセンスなし) から **Smart Licensing Using Policy** へ

```

Version 16.12.2, RELEASE SOFTWARE (fc1)
Copyright (c) 1986-2021 by Cisco Systems, Inc.
Compiled Thu 22-Jul-21 10:23 by mcpre

<output truncated>

Device# show license summary
Smart Licensing is ENABLED
License Reservation is ENABLED

Registration:
  Status: REGISTERED - SPECIFIC LICENSE RESERVATION
  Export-Controlled Functionality: ALLOWED

License Authorization:
  Status: AUTHORIZED - RESERVED

License Usage:
  License                               Entitlement tag                Count Status
  -----
  CSR 1KV AX 10G                        (ax_10G)                       1 AUTHORIZED

Device# show license reservation
License reservation: ENABLED

Overall status:
  Active: PID:CSR1000V,SN:95QS2T1KUJX
  Reservation status: SPECIFIC INSTALLED on Jul 09 21:10:37 2021 UTC
  Export-Controlled Functionality: ALLOWED
  Last Confirmation code: 4372613e

Specified license reservations:
  CSR 1KV AX 10G (ax_10G):
  Description: CSR 1KV AX 10G
  Total reserved count: 1
  Term information:
  Active: PID:CSR1000V,SN:95QS2T1KUJX
  License type: PERPETUAL
  Term Count: 1

```

2. CSSM で予約コードを更新します。

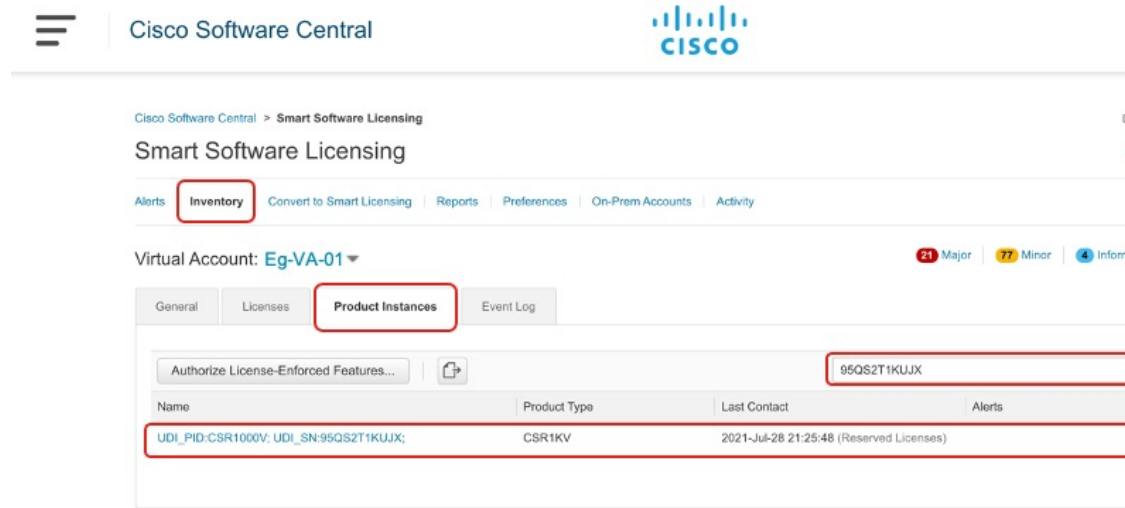
1. <https://software.cisco.com> で CSSM Web UI にログインし、[Smart Software Licensing] をクリックします。

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。

2. 対応するスマートアカウントとバーチャルアカウントで、[Inventory] > [Licences] に移動し、該当する DNA HSECK9 ライセンス (DNA の Router US Export Lic) のバランスがプラスであることを確認します。

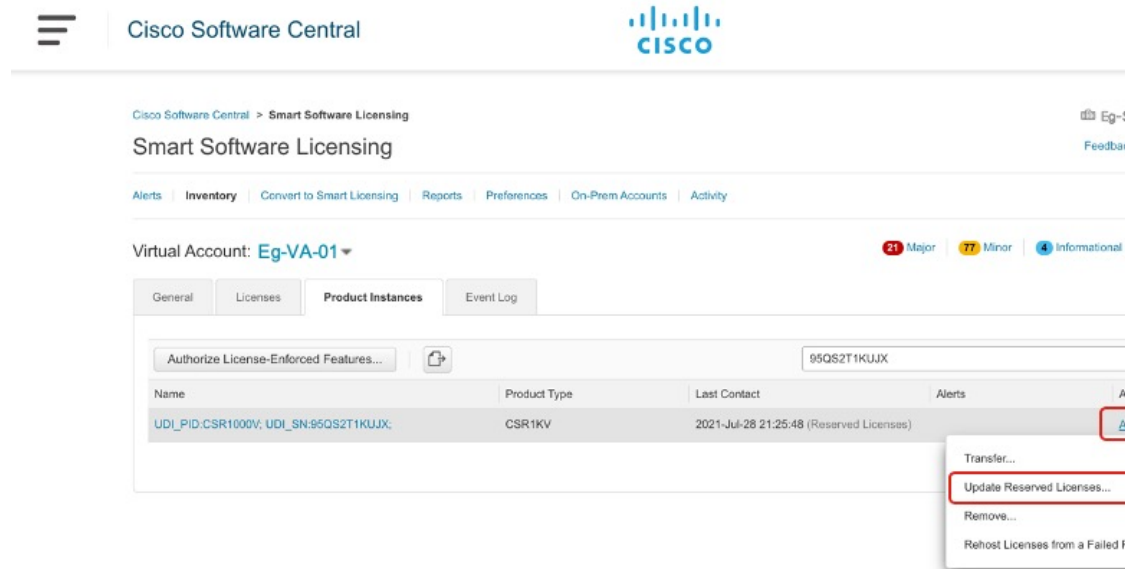
3. [Product Instances] タブをクリックし、検索機能を使用して製品インスタンスを見つけます。

この例では、シリアル番号 (95QS2T1KUJX) を使用して製品インスタンスを見つけます。



- 見つかった製品インスタンスの [Actions] 列から、[Update Reserved Licenses] を選択します。

[Update Reservation License] ウィンドウが表示されます。



- [Reserve a specific license] オプションボタンを選択します。

製品インスタンスで使用可能なすべてのライセンスを含むテーブルが表示され、このスマートアカウントとバーチャルアカウントには HSECK9 ライセンスのバランスがプラスであるため、HSECK9 ライセンスが自動的にリストに組み込まれます。

製品インスタンスに正しい HSECK9 ライセンスを選択していることを確認します。
[ルーティング製品インスタンスの HSECK9 ライセンスマッピングテーブル \(253 ページ\)](#) を参照してください。

例: スマートライセンス (スループットが 250 Mbps を超える SLR、輸出規制ライセンスなし) から Smart Licensing Using Policy へ

この例では、[Router US Export Lic for DNA] が選択されています (すべての仮想プラットフォームがこの HSECK9 ライセンスを使用します。これは「DNA_HSEC」ライセンスとも呼ばれます)。ISR 1000 や ISR 4000 などの他の製品インスタンスには、異なる製品固有の HSECK9 ライセンスが必要な場合があります。

Update License Reservation



Product Instance Details

Product Type: CSR1KV
 UDI PID: CSR1000V
 UDI Serial Number: 95QS2T1KUJX

Licenses to Reserve

In order to continue, ensure that you have a surplus of the licenses you want to reserve in the Virtual Account.

Reserve a specific license

6. 対応する [Reserve] 列に 1 と入力し、[Next] をクリックします。

Update License Reservation



Routing Network Essentials: Tier 0: 15M <small>Routing Network Stack Essentials: Tier 0: 15M</small>	-	0	44	0
Level 12				
Routing Network Essentials: Tier 0: 10M <small>Routing Network Stack Essentials: Tier 0: 10M</small>	-	0	44	0
CSR 1KV SECURITY 10M <small>CSR 1KV SECURITY 10M</small>	-	0	44	0
CSR 1KV IP BASE 10M <small>CSR 1KV IP BASE 10M</small>	-	0	44	0
ISRv IPB 10M <small>ISRv IPB 10M</small>	-	0	44	0
ISRv SEC 10M <small>ISRv SEC 10M</small>	-	0	44	0
NON-TIERED LICENSES				
Router US Export Lic. for DNA <small>U.S. Export Restriction Compliance license for DNA based Routers</small>	-never-	132	52	1

7. [承認コードを生成 (Generate Authorization Code)] をクリックします。

Update License Reservation

STEP 1 ✓ Select Licenses STEP 2 Review and confirm STEP 3 Authorization Code

Product Instance Details

Product Type: CSR1KV
 UDI PID: CSR1000V
 UDI Serial Number: 95QS2T1KUJX

Licenses to Reserve

License	Expires	Quantity to Reserve
Router US Export Lic. for DNA <small>U.S. Export Restriction Compliance license for DNA based Routers</small>	-never-	1
Level 2		
CSR 1KV AX 10G <small>CSR 1KV AX 10G</small>	multiple terms	1

Cancel Back **Generate**

8. [Copy to Clipboard] をクリックし、承認コードをファイルに保存します。

Update License Reservation

STEP 1 ✓ Select Licenses STEP 2 ✓ Review and confirm STEP 3 Authorization Code

✓ The Reservation Authorization Code below has been generated for this product instance. Several steps remain:

1. This code must be entered into the Product Instance's Smart Licensing settings to complete the reservation.
2. When the code has been entered, a Reservation Confirmation Code will be generated.
3. To release licenses in transition, enter confirmation code generated by device into CSSM.

Authorization Code:

```
<specificPLR><authorizationCode><flag>A</flag><version>C</version><pid>bcf8d256-97d1-4444-84aa-691315b3a8b3</pid><timestamp>1627512888369</timestamp><entitlement><tag>regid.2014-05.com.cisco.ax_10G.1.0_251f937f-655c-427d-b181-222784aae79a</tag><count>1</count><startDate></startDate></endDate></endDate></licenseType>PERPETUAL</licenseType><displayName>CSR 1KV AX 10G</displayName><tagDescription>CSR 1KV AX 10G</tagDescription></subscriptionID></subscriptionID></entitlement><entitlement><tag>regid.2019-03.com.cisco.DNA_HSEC.1.0_509c41ab-05a8-431f-95fe-ec28086e8844</tag><count>1</count><startDate></startDate></endDate></endDate></licenseType>PERPETUAL</licenseType><displayName>Router US Export Lic. for DNA</displayName><tagDescription>U.S. Export Restriction Compliance license for DNA based Routers</tagDescription></subscriptionID></subscriptionID></entitlement></entitlements></authorizationCode>
```

To learn how to enter this code, see the configuration guide for the product being licensed

Download as File **Copy to Clipboard** Enter Confirmation



(注) [Close] はまだクリックしないでください。このウィンドウを開いたまま、次の手順に進みません。

3. 正インスタンスに承認コードを保存し、インストールします。

1. 製品インスタンスで、特権 EXEC モードで **copysourcebootflash:file name** コマンドを入力し、製品インスタンスのブートフラッシュに承認コードファイルを保存します。次に例を示します。

```
Device# copy tftp://10.8.0.6/bootflash:slr_code_02
```

2. 製品インスタンスで、特権 EXEC モードで **license smart reservation install file{bootflash:filename}** コマンドを入力し、承認コードをインストールします。次に例を示します。

```
Device# license smart reservation install file bootflash:slr_code_02
Reservation install file successful
Last Confirmation code UDI: PID:CSR1000V,SN:95QS2T1KUJX
Confirmation code: 3290c177
```

3. 確認コードをコピーします。

4. CSSM に確認コードを入力してから、製品インスタンスのライセンスのリストを確認します。

1. CSSM Web UI の [Update License Reservation] ウィンドウに戻り、[Enter Confirmation Code] をクリックします。

[Enter Confirmation Code] ウィンドウが表示されます。

2. 確認コードを貼り付け、[OK] をクリックします。

Enter Confirmation Code

To complete the pending License Reservation, enter the Reservation Confirmation Code that was generated by the Product Instance Reservation Authorization Code was installed.

* Reservation Confirmation Code:

3290c177

Browse

Uplo

Cancel

- 製品インスタンスに特権 EXEC モードで **show license reservation** コマンドを入力します。

既存の ax_10G ライセンスとともに、DNA_HSEC ライセンスと新しい確認コードが表示されます。

```
Device# show license reservation
License reservation: ENABLED

Overall status:
  Active: PID:CSR1000V,SN:95QS2T1KUJX
  Reservation status: SPECIFIC INSTALLED on Jul 28 20:46:46 2021 UTC
  Export-Controlled Functionality: ALLOWED
  Last Confirmation code: 3290c177

Specified license reservations:
  CSR 1KV AX 10G (ax_10G):
  Description: CSR 1KV AX 10G
  Total reserved count: 1
  Term information:
  Active: PID:CSR1000V,SN:95QS2T1KUJX
  License type: PERPETUAL
  Term Count: 1
  Router US Export Lic. for DNA (DNA_HSEC):
  Description: U.S. Export Restriction Compliance license for DNA based Routers

  Total reserved count: 1
  Term information:
  Active: PID:CSR1000V,SN:95QS2T1KUJX
  License type: PERPETUAL
  Term Count: 1
```



(注) これは、SLR 承認コードに HSECK9 ライセンスの承認が含まれている製品インスタンスであり、アップグレード後に有効になります。したがって、アップグレード後に SLAC をインストールする必要はありません。

- Smart Licensing Using Policy をサポートするソフトウェアバージョンでデバイスをリロードします。

製品インスタンスは、以前に設定された（アップグレード前の）スループットで起動します。次の「移行後の show コマンド」の項を参照してください。

移行後の show コマンド

show version 移行後

```
-----
show version After Migration
-----
```

次の出力には、アップグレード後のソフトウェアバージョンが示されています。さらに、インストールされているソフトウェアバージョンが Catalyst 8000V ソフトウェアイメージであることに注意してください。

例: スマートライセンス (スループットが 250 Mbps を超える SLR、輸出規制ライセンスなし) から Smart Licensing Using Policy へ

```
Device# show version
Cisco IOS XE Software, Version 17.6.1
Cisco IOS Software [Bengaluru], Virtual XE Software (X86_64_LINUX_IOSD-UNIVERSALK9-M),
Version 17.6.1
Copyright (c) 1986-2021 by Cisco Systems, Inc.
Compiled Sat 24-Jul-21 11:21 by mcpre

<output truncated>

ROM: IOS-XE ROMMON

Router uptime is 1 minute
Uptime for this control processor is 2 minutes
System returned to ROM by reload
System image file is "bootflash:c8000v-universalk9.SSA.bin"
Last reload reason: Reload Command
```

show show license summary移行後

```
-----
show license summary After Migration
-----
```

次の出力には、輸出規制 HSECK9 ライセンスと ax_10G が移行されたことが示されています。

```
Device# show licence summary
License Reservation is ENABLED
```

License Usage:

License	Entitlement Tag	Count	Status
hseck9	(DNA_HSEC)	1	IN USE
ax_10G	(ax_10G)	1	IN USE

show license usage移行後

```
-----
show license usage After Migration
-----
```

次の出力には、移行されたすべてのライセンスの適用タイプが示されています。HSECK9 ライセンスには Enforcement type: EXPORT RESTRICTED と示されています。輸出規制ライセンスではない ax_10G の適用タイプは Enforcement type: NOT ENFORCED です。

```
Device# show license usage
License Authorization:
  Status: Not Applicable
```

```
hseck9 (DNA_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
License type: Export
Reservation:
  Reservation status: SPECIFIC EXPORT AUTHORIZATION KEY INSTALLED
  Total reserved count: UNLIMITED

ax_10G (ax_10G):
  Description: ax_10G
  Count: 1
  Version: 1.0
  Status: IN USE
Export status: NOT RESTRICTED
Feature Name: ax_10G
Feature Description: ax_10G
Enforcement type: NOT ENFORCED
License type: Subscription
Reservation:
  Reservation status: SPECIFIC INSTALLED
  Total reserved count: 1
    
```

show license authorization移行後

```
-----
show license authorization After Migration
-----
```

次の出力には、HSECK9 ライセンスの一部として含まれている SLR 承認コードが適用されていることが示されています (Last Confirmation code: 3290c177)。

```

Device# show license authorization
Overall status:
  Active: PID:CSR1000V,SN:95QS2T1KUJX
  Status: SPECIFIC INSTALLED on Jul 28 20:46:46 2021 UTC
  Last Confirmation code: 3290c177

Specified license reservations:
CSR 1KV AX 10G (ax_10G):
  Description: CSR 1KV AX 10G
  Total reserved count: 1
  Enforcement type: NOT ENFORCED
  Term information:
    Active: PID:CSR1000V,SN:95QS2T1KUJX
    Authorization type: SPECIFIC INSTALLED on Jul 28 20:46:46 2021 UTC
    License type: PERPETUAL
    Term Count: 1
Router US Export Lic. for DNA (DNA_HSEC):
  Description: U.S. Export Restriction Compliance license for DNA based Routers
  Total reserved count: 1
  Enforcement type: EXPORT RESTRICTED
  Term information:
    Active: PID:CSR1000V,SN:95QS2T1KUJX
    Authorization type: SPECIFIC INSTALLED on Jul 28 20:46:46 2021 UTC
    License type: PERPETUAL
    Term Count: 1

Purchased Licenses:
  No Purchase Information Available

Derived Licenses:
  Entitlement Tag:
    
```

例: スマートライセンス (スループットが 250 Mbps を超える SLR、輸出規制ライセンスなし) から Smart Licensing Using Policy へ

```
regid.2019-03.com.cisco.DNA_HSEC,1.0_509c41ab-05a8-431f-95fe-ec28086e8844
Entitlement Tag: regid.2014-05.com.cisco.ax_10G,1.0_251f937f-655c-427d-b181-222784aae79a
```

show platform hardware throughput level移行後

```
-----
show platform hardware throughput level After Migration
-----
```

次の出力には、移行後に 1250 Mbps のスループットが維持されていることが示されています。

```
Device# show platform hardware throughput level
The current throughput level is 10000000 kb/s
```

show license status移行後

```
-----
show license status After Migration
-----
```

移行後の出力には、製品インスタンスが Smart Licensing Using Policy であることが示されています (Smart Licensing Using Policy: Status: ENABLED)。

トランスポートタイプはオフに設定されます (Type: Transport Off)。つまり、製品インスタンスは CSSM とも、ネットワーク外のあらゆるものとも通信できません。

ここでは、デフォルトのポリシーが有効になっています。(他のポリシーが使用できない場合、製品インスタンスは表 6: ポリシー: Cisco default ポリシーを適用します)。カスタムポリシーが CSSM で使用可能である場合は、最初の同期の後も同じポリシーがインストールされます。同期は、現在のポリシーが必要とするレポートにも対応します (Next ACK deadline: Oct 26 21:17:32 2021 UTC)。

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

```
Smart Licensing Using Policy:
  Status: ENABLED
```

```
Account Information:
  Smart Account: <none>
  Virtual Account: <none>
License Reservation is ENABLED
```

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

```
Transport:
  Type: Transport Off
```

```
Policy:
  Policy in use: Merged from multiple sources.
```

```

Reporting ACK required: yes (CISCO default)
Unenforced/Non-Export Perpetual Attributes:
  First report requirement (days): 365 (CISCO default)
  Reporting frequency (days): 0 (CISCO default)
  Report on change (days): 90 (CISCO default)
Unenforced/Non-Export Subscription Attributes:
  First report requirement (days): 90 (CISCO default)
  Reporting frequency (days): 90 (CISCO default)
  Report on change (days): 90 (CISCO default)
Enforced (Perpetual/Subscription) License Attributes:
  First report requirement (days): 0 (CISCO default)
  Reporting frequency (days): 0 (CISCO default)
  Report on change (days): 0 (CISCO default)
Export (Perpetual/Subscription) License Attributes:
  First report requirement (days): 0 (CISCO default)
  Reporting frequency (days): 0 (CISCO default)
  Report on change (days): 0 (CISCO default)

Miscellaneous:
  Custom Id: <empty>

Usage Reporting:
  Last ACK received: <none>
  Next ACK deadline: Oct 26 21:17:32 2021 UTC
  Reporting push interval: 30 days
  Next ACK push check: <none>
  Next report push: Jul 28 21:19:32 2021 UTC
  Last report push: <none>
  Last report file write: <none>

Trust Code Installed: <none>

```

移行後に必要なタスク

1. トポロジを実装します。

この例では、CSSM への接続がなく、CSLU のないトポロジを実装します。[CSSM への接続なし、CSLU なし \(28 ページ\)](#) 対応するワークフローは [トポロジのワークフロー：CSSM への接続なし、CSLU なし \(63 ページ\)](#) のとおりです。

SLR から移行すると、トランスポートタイプは自動的にオフに設定されます。移行後の **show license status** コマンドの出力例には、これが実行されたことが示されています。

輸出規制ライセンスが使用されており、これに対応する承認コードが移行されています。アップグレード後に SLAC を再度インストールする必要はありません。

これにより、エアギャップネットワークで動作するトポロジの実装が完了します。

2. ライセンスの使用状況を CSSM と同期し、同期を確認し、後続のレポートの要件を確認します。

このトポロジでは、RUM レポートを（製品インスタンスの）ファイルに保存し、CSSM に（インターネットと CSSM に接続しているワークステーションから）アップロードする必要があります。その後に、ACK をダウンロードして製品インスタンスにインストールする必要があります。

1. 使用状況情報を CSSM と同期します。

例: スマートライセンス (スループットが 250 Mbps を超える SLR、輸出規制ライセンスなし) から Smart Licensing Using Policy へ

- 次に示す設定例では、RUM レポートは製品インスタンスのフラッシュメモリの `usage_report` というファイルに保存されます。次にレポートは CSSM にアップロードするために TFTP の場所に転送されます。

```
Device# license smart save usage unreported file usage_report
Device# dir bootflash:
Directory of bootflash:/
```

```
23      -rw-                3950  Jan 19 2021 07:26:26 +00:00  usage_report
```

<output truncated>

```
Device# copy bootflash:usage_report tftp://10.8.0.6//user01/usage_report
Address or name of remote host [10.8.0.6]?
Destination filename [/user01/usage_report]?
!!
3950 bytes copied in 0.012 secs (329167 bytes/sec)
```

- RUM レポートを CSSM にアップロードします。処理が完了したら、ACK をダウンロードします。「[CSSM へのデータまたは要求のアップロードとファイルのダウンロード \(229 ページ\)](#)」を参照してください
- ダウンロードした場所からファイルをコピーし、製品インスタンスのフラッシュメモリに保存し (`copy source bootflash:file-name`)、製品インスタンスに ACK をインストールします。

```
Device# copy tftp://10.8.0.6//user01 bootflash:ACK_usage_report.txt
```

```
Device# license smart import bootflash: ACK_usage_report.txt
Import Data Successful
```

- 同期を確認し、更新されたポリシーをチェックして後続のレポートの要件を確認します。

`show license all` 特権 EXEC コマンドの出力の [Last ACK received:] フィールドの更新されたタイムスタンプは、同期が完了したことを確認するのに役立ちます。

後続のレポートが必要な場合は、ポリシーに示され、システムメッセージが表示されます。次に、上記の手順 2 に示すように RUM レポートをアップロードする必要があります (すべてのサブ手順を含む)。`show license all` 特権 EXEC コマンドの次のフィールドには、レポートが必要かどうかといつ必要かについての情報が示されています。

- Next ACK deadline:

- Next report push:

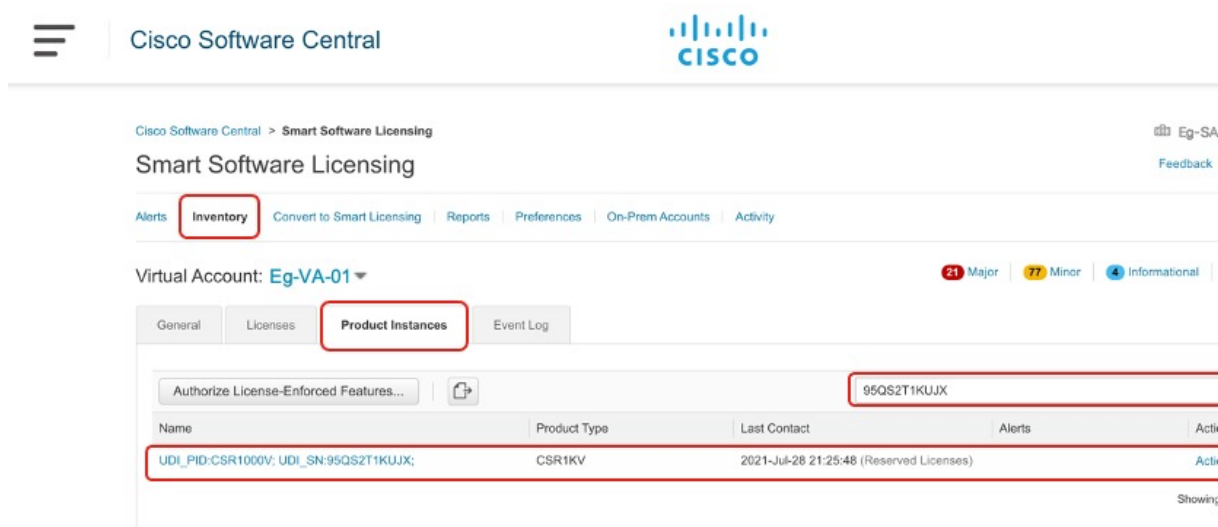
移行前と後の CSSM Web UI

<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。該当するスマートアカウントとバーチャルアカウントで、[Inventory]>[Product Instances] に移動して、すべての製品インスタンスを表示します。

移行前の CSSM Web UI

[Product Instances] タブで UDI をクリックし、次に示すように詳細なライセンス使用情報を表示します。

スマートライセンス環境では、SLR ライセンスは [Last Contact] フィールドに「(Reserved Licenses)」というラベルで表示されます。



移行後の CSSM Web UI

[Product Instances] タブで UDI をクリックして詳細なライセンス使用状況情報を表示します。



- (注) Catalyst 8000V ソフトウェアイメージが製品インスタンスにインストールされていても、PID は変更されません。したがって、この製品インスタンスの PID は引き続き PID:CSR1000V,SN:95QS2T1KUJX です。アップグレードの前後に **show license udi** コマンドを使用してこれを確認することもできます。

Smart Licensing Using Policy へのアップグレード後、および必要な RUM レポートがアップロードされた後で [Last Contact] フィールドが更新されます。

例：スマートライセンス（評価ライセンス）から Smart Licensing Using Policy へ

次に、スマートライセンスから Smart Licensing Using Policy へ移行する評価ライセンスを使用した **Cisco 4351 サービス統合型ルータ** の例を示します。製品インスタンスのソフトウェアバージョンは、Cisco IOS XE Gibraltar 16.12.4 から Cisco IOS XE Bengaluru 17.4.1a にアップグレードされます。次に、この例の場合にアップグレード後はどうなるかについての概要を示します。

- 移行後の適用タイプ：移行前は、すべてのライセンスが評価モードです。使用されているすべてのライセンスが移行され、適用後はすべてのライセンスの適用タイプが NOT ENFORCED になります。

この例では、Smart Licensing Using Policy 環境で輸出規制ライセンスを使用するように移行後に SLAC がインストールされています。次のサブセクション「移行後に必要なタスク」の詳細な手順を参照してください。これは、アップグレード後に SLAC を要求してインストールする方法を示すためのものであり、必須ではありません。

- 移行後のトランスポートタイプ：評価ライセンスを移行すると、デフォルトのトランスポートタイプ（**cslu**）が自動的に設定されます。これは、最終的に実装されるトポロジに応じて変更できます。[サポートされるトポロジ（18ページ）](#)のいずれかを実装できます。

この例では、CSSM への直接接続トポロジ（CSSM への接続にトランスポートタイプ **smart** を使用）が実装されています。



- (注) この例では、製品インスタンスで使用されるすべてのライセンスが評価モードであるため、デフォルトのトランスポートタイプが自動的に設定されています。使用されているライセンスの 1 つでも登録され、承認されているシナリオの場合は、トランスポートタイプの設定が保持され、評価ライセンスがある場合はそのライセンスも適用されていないライセンスとして移行されます（輸出規制ライセンス、つまり HSECK9 は評価モードをサポートしていません）。

- Device-Led Conversion (DLC)：DLC は以前のスマートライセンス環境での評価ライセンスであるため、このシナリオのライセンスには適用されません（すでにスマートライセンスです）。
- 移行後のレポート：最初の同期では、ソフトウェアバージョンのアップグレード後にトポロジが実装されるため、対応するレポート方式に従います。カスタムポリシーが CSSM で使用可能な場合は、この同期の一部として製品インスタンスにインストールされます。後続のレポートの要件は、更新されたポリシーによって異なります。カスタムポリシーが使用できない場合、後続のレポートの要件はデフォルトポリシーに従います。

移行前と後の show コマンド

移行前と後の show version

show version Before Migration

次の出力には、アップグレード前のソフトウェアバージョンが示されています。

```
Device# show version
Cisco IOS XE Software, Version 16.12.04
Cisco IOS Software [Gibraltar], ISR Software (X86_64_LINUX_IOSD-UNIVERSALK9-M),
Version 16.12.4, RELEASE SOFTWARE (fc5)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2020 by Cisco Systems, Inc.
Compiled Thu 09-Jul-20 21:44 by mcpre
```

show version After Migration

次の出力は、移行後のソフトウェアバージョンを示しています。その後にはシステムを新しいイメージで再起動したときに表示されるライセンス関連のシステムメッセージの抜粋が示されています。

```
Device# show version
Cisco IOS XE Software, Version 17.4.1a
Cisco IOS Software [Bengaluru], ISR Software (X86_64_LINUX_IOSD-UNIVERSALK9-M),
Version 17.4.1a, RELEASE SOFTWARE (fc4)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2020 by Cisco Systems, Inc.
Compiled Fri 18-Dec-20 05:04 by mcpre

Press RETURN to get started!
*Jan 21 01:06:50.905: %ISR_THROUGHPUT-6-LEVEL:
Throughput level has been set to 400000 kbps
*Jan 21 01:06:53.874: %SMART_LIC-6-AGENT_ENABLED:
Smart Agent for Licensing is enabled
*Jan 21 01:06:54.485: %SMART_LIC-6-EXPORT_CONTROLLED:
Usage of export controlled features is not allowed
*Jan 21 01:07:34.924: %SYS-5-RESTART: System restarted --
*Jan 21 01:08:05.933: %CALL_HOME-6-CALL_HOME_ENABLED:
Call-home is enabled by Smart Agent for Licensing.
*Jan 21 01:08:07.186: %SMART_LIC-6-REPORTING_REQUIRED:
A Usage report acknowledgement will be required in 365 days.
*Jan 21 01:10:32.210: %SMART_LIC-3-COMM_FAILED:
Communications failure with the Cisco Smart License Utility (CSLU) :
Unable to resolve server hostname/domain name
```

移行前と後の **show license summary**-----
show license summary Before Migration

移行前の出力には、すべてのライセンスが評価モード（EVAL MODE）であることが示されています。これらはすべて、移行後に IN USE として表示されます（Smart Licensing Using Policy 環境には評価モードの概念はありません）。

```
Device# show license summary

Smart Licensing is ENABLED

Registration:
  Status: UNREGISTERED
  Export-Controlled Functionality: NOT ALLOWED

License Authorization:
  Status: EVAL MODE
  Evaluation Period Remaining: 89 days, 23 hours, 58 minutes, 0 seconds

License Usage:
  License                               Entitlement tag                Count Status
  -----
                                     (ISR_4351_Application)        1  EVAL MODE
                                     (ISR_4351_UnifiedCommun...)    1  EVAL MODE
                                     (ISR_4351_Security)           1  EVAL MODE
                                     (ISR_4351_400M_Performance)   1  EVAL MODE
```

show license summary After Migration

移行後の出力には、4つのライセンスすべてが移行されており、ステータスが IN USE で表示されていることが示されています。

Device# **show license summary**

```
License Usage:
License                Entitlement Tag                Count Status
-----
throughput             (ISR_4351_400M_Performance)    1 IN USE
appxk9                 (ISR_4351_Application)        1 IN USE
uck9                   (ISR_4351_UnifiedCommun...)    1 IN USE
securityk9            (ISR_4351_Security)           1 IN USE
```

移行前と後の **show license status**-----
show license status Before Migration

移行前の出力には、ライセンスが登録されていないことが示されています。

評価ライセンスは登録されていないため、スマートライセンス環境のデフォルトのトランスポートタイプ (**callhome**) が有効になっています。移行後は、Smart Licensing Using Policy のデフォルトが有効になります。

Device# **show license status**

Smart Licensing is ENABLED

Utility:
Status: DISABLED

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

Transport:
Type: Callhome

Registration:
Status: **UNREGISTERED**
Export-Controlled Functionality: NOT ALLOWED

License Authorization:
Status: **EVAL MODE**
Evaluation Period Remaining: 89 days, 23 hours, 57 minutes, 0 seconds

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

Export Authorization Key:

```
Features Authorized:  
<none>
```

show license status After Migration

移行後の出力には、製品インスタンスが **Smart Licensing Using Policy** であることが示されています (Smart Licensing Using Policy: Status: ENABLED)。

トランスポートタイプは **CSLU** (Type: cslu) に設定されます。これは、**Smart Licensing Using Policy** 環境のデフォルトです。

ここでは、デフォルトのポリシーが有効になっています。（他のポリシーが使用できない場合、製品インスタンスは表 6: **ポリシー：Cisco default** ポリシーを適用します）。カスタムポリシーが使用可能であれば、トポロジが実装されて最初の同期が完了した後に適用されます。

```
Device# show license status
```

```
Utility:
```

```
Status: DISABLED
```

```
Smart Licensing Using Policy:
```

```
Status: ENABLED
```

```
Data Privacy:
```

```
Sending Hostname: yes
```

```
Callhome hostname privacy: DISABLED
```

```
Smart Licensing hostname privacy: DISABLED
```

```
Version privacy: DISABLED
```

```
Transport:
```

```
Type: cslu
```

```
Cslu address: <empty>
```

```
Proxy:
```

```
Not Configured
```

```
Policy:
```

```
Policy in use: Merged from multiple sources.
```

```
Reporting ACK required: yes (CISCO default)
```

```
Unenforced/Non-Export Perpetual Attributes:
```

```
First report requirement (days): 365 (CISCO default)
```

```
Reporting frequency (days): 0 (CISCO default)
```

```
Report on change (days): 90 (CISCO default)
```

```
Unenforced/Non-Export Subscription Attributes:
```

```
First report requirement (days): 90 (CISCO default)
```

```
Reporting frequency (days): 90 (CISCO default)
```

```
Report on change (days): 90 (CISCO default)
```

```
Enforced (Perpetual/Subscription) License Attributes:
```

```
First report requirement (days): 0 (CISCO default)
```

```
Reporting frequency (days): 0 (CISCO default)
```

```
Report on change (days): 0 (CISCO default)
```

```
Export (Perpetual/Subscription) License Attributes:
```

```
First report requirement (days): 0 (CISCO default)
```

```
Reporting frequency (days): 0 (CISCO default)
```

```
Report on change (days): 0 (CISCO default)
```

```
Miscellaneous:
```

```
Custom Id: <empty>
```

```
Usage Reporting:
```

```
Last ACK received: <none>
```

```

Next ACK deadline: Jan 21 01:08:07 2022 UTC
Reporting push interval: 30 days
Next ACK push check: <none>
Next report push: Jan 21 01:10:07 2021 UTC
Last report push: <none>
Last report file write: <none>

```

```
Trust Code Installed: <none>
```

移行前と後の show license usage

show license usage Before Migration

移行前の出力には、使用されているすべてのライセンスには `Export status: NOT RESTRICTED` と示されていました。移行後、輸出ステータスは同じになります。さらに、すべての適用タイプが `NOT ENFORCED` になります。

```
Device# show license usage
```

```
License Authorization:
  Status: EVAL MODE
  Evaluation Period Remaining: 89 days, 23 hours, 55 minutes, 44 seconds
```

```
(ISR_4351_Application):
```

```
  Description:
  Count: 1
  Version: 1.0
  Status: EVAL MODE
  Export status: NOT RESTRICTED
```

```
(ISR_4351_UnifiedCommunication):
```

```
  Description:
  Count: 1
  Version: 1.0
  Status: EVAL MODE
  Export status: NOT RESTRICTED
```

```
(ISR_4351_Security):
```

```
  Description:
  Count: 1
  Version: 1.0
  Status: EVAL MODE
  Export status: NOT RESTRICTED
```

```
(ISR_4351_400M_Performance):
```

```
  Description:
  Count: 1
  Version: 1.0
  Status: EVAL MODE
  Export status: NOT RESTRICTED
```

show license usage After Migration

移行後の出力には、すべてのライセンスが適用されていないことが示されています (`Export status: NOT RESTRICTED`、`Enforcement type: NOT ENFORCED`)。

```
Device# show license usage

License Authorization:
  Status: Not Applicable

throughput (ISR_4351_400M_Performance):
  Description: throughput
  Count: 1
  Version: 1.0
  Status: IN USE
  Export status: NOT RESTRICTED
  Feature Name: throughput
  Feature Description: throughput
  Enforcement type: NOT ENFORCED
  License type: Perpetual

appxk9 (ISR_4351_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
  License type: Perpetual

uck9 (ISR_4351_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
  License type: Perpetual

securityk9 (ISR_4351_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
  License type: Perpetual
```

移行前と後の show platform hardware throughput level

```
-----
show platform hardware throughput level Before Migration
-----
```

このコマンドは、現在設定されているスループットを表示します。出力例には、スループットが 400000 kbps に設定されていることが示されています。これは、増大するスループットを許可するパフォーマンスライセンスによって承認されます（**show license** の出力、Feature: throughput を参照）。したがって、設定されたスループットは移行後も保持されます。


```
Device# show platform hardware throughput level
The current throughput level is 400000 kb/s
```

```
-----
show platform hardware throughput level After Migration
-----
```

移行後の出力には、スループット設定が移行後も同じであることが示されています。

```
Device# show platform hardware throughput level
The current throughput level is 400000 kb/s
```

移行前と後の **show platform software cerm-information**

```
-----
show platform software cerm-information Before Migration
-----
```

移行前の出力には、CERM機能が有効になっていることが示されています。HSECK9がない場合は、1,000 個のセキュアトンネルと 250 Mbps の暗号化帯域幅がサポートされます。移行後も、この設定に変更はありません。

```
Device# show platform software cerm-information
```

```
Crypto Export Restrictions Manager (CERM) Information:
  CERM functionality: ENABLED
```

```
-----
Resource   Maximum Limit Available
-----
Number of tunnels      1000  1000
Number of TLS sessions 1000  1000
```

```
Resource reservation information:
D - Dynamic
```

```
-----
Client  Tunnels    TLS Sessions
-----
VOICE   0          0
IPSEC   0          N/A
SSLVPN  0          N/A
```

```
Statistics information:
Failed tunnels:          0
Failed sessions:       0
Failed encrypt pkts:    0
Failed encrypt pkt bytes: 0
Failed decrypt pkts:    0
Failed decrypt pkt bytes: 0
```

```
-----
show platform software cerm-information After Migration
-----
```

移行後の出力には、CERM 設定が移行後も同じであることが示されています。

```
Device# show platform software cerm-information
```

```
Crypto Export Restrictions Manager (CERM) Information:
  CERM functionality: ENABLED
```

```

-----
Resource      Maximum Limit  Available
-----
Number of tunnels      1000    1000
Number of TLS sessions 1000    1000

Resource reservation information:
D - Dynamic
-----
Client  Tunnels    TLS Sessions
-----
VOICE   0          0
IPSEC   0          N/A
SSLVPN  0          N/A

Statistics information:
Failed tunnels:          0
Failed sessions:        0
Failed encrypt pkts:    0
Failed encrypt pkt bytes: 0
Failed decrypt pkts:    0
Failed decrypt pkt bytes: 0
    
```

移行後に必要なタスク

1. トポロジを実装します。

この例では、トランスポートタイプに **smart** を使用して **CSSM に直接接続** (21 ページ) トポロジを実装します。対応するワークフローは [トポロジのワークフロー：CSSM に直接接続](#) (53 ページ) のとおりです。

1. スマートアカウントを設定します。

この例では、評価ライセンスはすでにスマートライセンス環境下にあります。スマートアカウントとバーチャルアカウントの設定はすでに完了しています。

2. CSSM への製品インスタンスの接続を設定します。

この設定例では、HTTP 接続の送信元インターフェイスに必要な設定と、名前とアドレスの解決のための 2 つのネームサーバが表示されています。

```

Device(config)# ip http client source-interface gigabitethernet 0/0/2
Device(config)# ip name-server 209.165.201.1 209.165.200.225
    
```

設定に必要なその他の手順については、[CSSM への接続の設定](#) (189 ページ) を参照してください。

3. 接続方式とトランスポートタイプを設定します。

次の設定例には、スマートトランスポートを使用するために必要な設定が示されています。

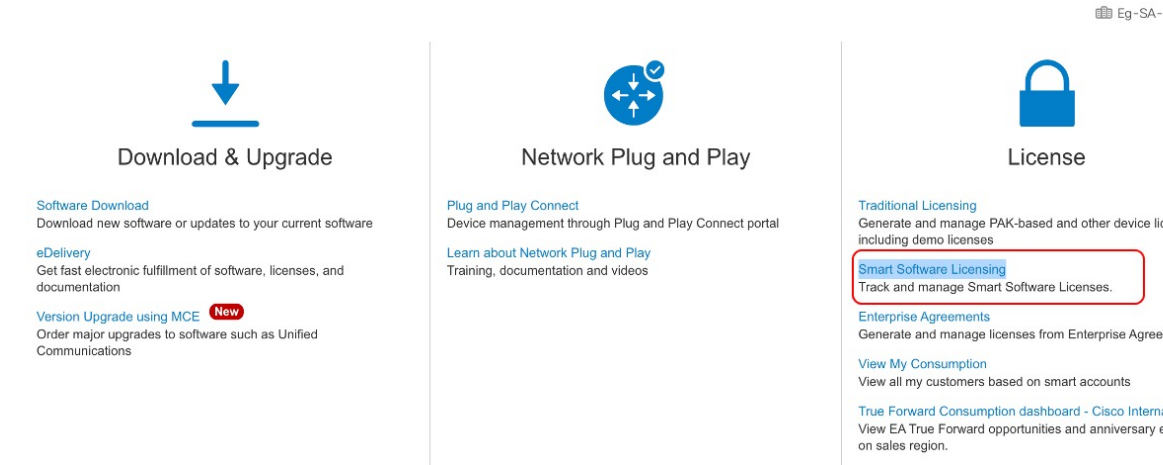
```

Device(config)# license smart transport smart
Device(config)# license smart url default
Device(config)# exit
Device# copy running-config startup-config
    
```

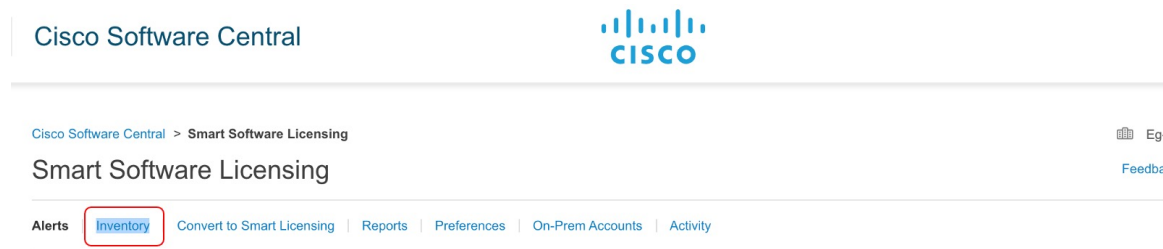
4. CSSM との信頼を確立します。

次の手順に、トークンを生成してインストールする方法と、信頼が正常に確立されたことでポリシーが CSSM からプロビジョニングされる方法を示します（信頼が正常に確立された後、ポリシーが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）。

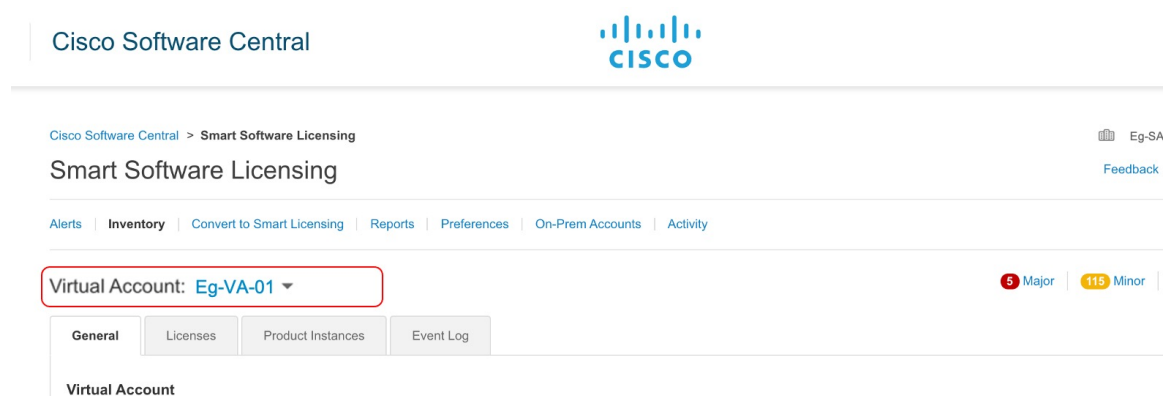
<https://software.cisco.com> で CSSM Web UI にログインし、[Smart Software Licensing] をクリックします。



[Inventory] タブをクリックします。



正しいバーチャルアカウントが選択されていることを確認し、[General] タブをクリックします。



[New Token] をクリックします。[Create Registration Token] ウィンドウが表示します。

Product Instance Registration Tokens

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

[New Token...](#)

Token	Expiration Date	Uses	Export-Controlled	Description
OWJhMTk3ZGMtYjdh...	2021-Feb-14 01:02:49 (in 24...	1 of 100	Allowed	

トークンをアクティブにする必要がある日数を入力し、輸出規制機能のチェックボックスをオンにします。

Create Registration Token

This will create a token that is used to register product instances, so that they can use licenses from this virtual account. Once it's created, you can use the Smart Licensing configuration for your products and enter the token, to register them with this virtual account.

Virtual Account:

Description:

* **Expire After:** Days

Between 1 - 365, 30 days recommended

Max. Number of Uses:

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

Allow export-controlled functionality on the products registered with this token ⓘ

[Create Token](#)



(注) この後に SLAC がインストールされるため、ここでは輸出規制機能のチェックボックスがオンになっています (SLAC のインストール手順は次に示します)。輸出規制ライセンスが不要な場合は、チェックボックスをオフのままにして構いません。

トークンをクリップボードにコピーします。または、[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。

Token



```
OWJhMTk3ZGMtYjdhMy00MDA0LTg3ZDYtNTlwN2M0NzMyMjM3LTE
2MTMyNjQ1%0ANjk0Mjh8cnljbDILVTdjT2xqMmhJUzFBOVJ5czcwQ2
s2RW9paitCTmlyV09t%0AanVBZz0%3D%0A
```

Press ctrl + c to copy selected text to clipboard.

信頼コードをインストールします。

次の設定例には、信頼コードをインストールするために必要な設定が示されています。



- (注) 信頼コードのインストール後に表示されるシステムメッセージには、a) 信頼コードが正常にインストールされたこと、b) 新しいポリシーがインストールされたこと、および c) CSSM とのライセンス使用状況の同期されたことが示されます（CSSM との通信が復元されたため、製品インスタンスが自動的に必須の RUM レポートを送信しました）。

```
Device# license smart trust idtoken
$T2xqMmhJUzFBOVJ5czcwQ2s2RW9paitCTmlyV09t%0AanVBZz0%3D%0A local

*Jan 21 03:37:14.577: %SMART_LIC-5-COMM_RESTORED: Communications with Cisco Smart
Software Manager (CSSM) restored
*Jan 21 03:37:15.404: %SMART_LIC-6-POLICY_INSTALL_SUCCESS: A new licensing policy
was successfully installed
*Jan 21 03:37:15.588: %SMART_LIC-6-TRUST_INSTALL_SUCCESS: A new licensing trust
code was successfully installed on P:ISR4351/K9,S:FDO21512BJB.
*Jan 21 03:42:03.106: %SIP-1-LICENSING: SIP service is Up. License report
acknowledged.
*Jan 21 03:42:03.761: %SMART_LIC-6-POLICY_INSTALL_SUCCESS: A new licensing policy
was successfully installed
```

2. ライセンスの使用状況を CSSM と同期し、同期を確認し、後続のレポートの要件を確認します。

前の手順のシステムメッセージには、同期が完了したことが示されています。次の出力例では、次のフィールドを使用して同期を確認できます。

- タイムスタンプの更新：Policy in use: Installed On Jan 21 03:42:03 2021 UTC
- タイムスタンプの更新：Last ACK received: Jan 21 03:42:02 2021 UTC

CSSM への直接接続トポロジでは、製品インスタンスがポリシーに基づいて次の RUM レポートを CSSM に送信します。出力例では、次のフィールドにこの情報が示されています。

- Next report push: Feb 20 03:38:01 2021 UTC
- Next ACK deadline: Mar 22 03:42:02 2021 UTC

```

Device# show license status
Utility:
  Status: DISABLED

Smart Licensing Using Policy:
  Status: ENABLED

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

Transport:
  Type: Smart
  URL: https://smartreceiver.cisco.com/licservice/license
  Proxy:
    Not Configured

Policy:
Policy in use: Installed On Jan 21 03:42:03 2021 UTC
Policy name: SLP Policy
Reporting ACK required: yes (Customer Policy)
Unenforced/Non-Export Perpetual Attributes:
  First report requirement (days): 30 (Customer Policy)
  Reporting frequency (days): 60 (Customer Policy)
  Report on change (days): 60 (Customer Policy)
Unenforced/Non-Export Subscription Attributes:
  First report requirement (days): 120 (Customer Policy)
  Reporting frequency (days): 150 (Customer Policy)
  Report on change (days): 120 (Customer Policy)
Enforced (Perpetual/Subscription) License Attributes:
  First report requirement (days): 0 (CISCO default)
  Reporting frequency (days): 90 (Customer Policy)
  Report on change (days): 60 (Customer Policy)
Export (Perpetual/Subscription) License Attributes:
  First report requirement (days): 0 (CISCO default)
  Reporting frequency (days): 30 (Customer Policy)
  Report on change (days): 30 (Customer Policy)

Miscellaneous:
  Custom Id: <empty>

Usage Reporting:
Last ACK received: Jan 21 03:42:02 2021 UTC
Next ACK deadline: Mar 22 03:42:02 2021 UTC
Reporting push interval: 30 days
Next ACK push check: <none>
Next report push: Feb 20 03:38:01 2021 UTC
Last report push: Jan 21 03:38:01 2021 UTC
Last report file write: <none>

Trust Code Installed: Jan 21 03:37:15 2021 UTC

```

- 輸出規制ライセンスを使用するには、SLAC を手動で要求し、自動インストールします。**license smart authorization request** は、すべてのエンタープライズルーティング製品インスタンスでサポートされています（さらに、特定の製品インスタンスでは代替コマンドを使用できます）。詳細は、[SLAC の手動要求と自動インストール（216 ページ）](#) を参照してください。

```

Device# license smart authorization request add hseck9 local
Device#
*Jan 21 03:58:37.558: %SMART_LIC-6-AUTHORIZATION_INSTALL_SUCCESS:

```

```

A new licensing authorization code was successfully installed on
PID:ISR4351/K9,SN:FDO21512BJB
*Jan 21 03:58:39.196: %SMART_LIC-6-POLICY_INSTALL_SUCCESS: A new licensing policy
was successfully installed
*Jan 21 03:59:37.087: %SMART_LIC-6-EXPORT_CONTROLLED: Usage of export controlled
features is allowed for feature hseck9
*Jan 21 04:04:10.751: %SIP-1-LICENSING: SIP service is Up. License report acknowledged.
*Jan 21 04:04:10.979: %SMART_LIC-6-EXPORT_CONTROLLED: Usage of export controlled
features is allowed for feature hseck9
*Jan 21 04:04:11.614: %SMART_LIC-6-POLICY_INSTALL_SUCCESS: A new licensing policy
was successfully installed

```

Device# **show license summary**

License Usage:

License	Entitlement Tag	Count	Status
throughput	(ISR_4351_400M_Performance)	1	IN USE
hseck9	(ISR_4351_Hsec)	1	IN USE
appxk9	(ISR_4351_Application)	1	IN USE
uck9	(ISR_4351_UnifiedCommun...)	1	IN USE
securityk9	(ISR_4351_Security)	1	IN USE

Device# **show license all**

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

Smart Licensing Using Policy:

Status: ENABLED

Data Privacy:

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

Transport:

Type: Smart
URL: https://smartreceiver.cisco.com/licservice/license
Proxy:
Not Configured

Miscellaneous:

Custom Id: <empty>

Policy:

Policy in use: Installed On Jan 21 04:04:11 2021 UTC
Policy name: SLE Policy
Reporting ACK required: yes (Customer Policy)
Unenforced/Non-Export Perpetual Attributes:
First report requirement (days): 30 (Customer Policy)
Reporting frequency (days): 60 (Customer Policy)

```

Report on change (days): 60 (Customer Policy)
Unenforced/Non-Export Subscription Attributes:
  First report requirement (days): 120 (Customer Policy)
  Reporting frequency (days): 150 (Customer Policy)
  Report on change (days): 120 (Customer Policy)
Enforced (Perpetual/Subscription) License Attributes:
  First report requirement (days): 0 (CISCO default)
  Reporting frequency (days): 90 (Customer Policy)
  Report on change (days): 60 (Customer Policy)
Export (Perpetual/Subscription) License Attributes:
  First report requirement (days): 0 (CISCO default)
  Reporting frequency (days): 30 (Customer Policy)
  Report on change (days): 30 (Customer Policy)

```

```

Usage Reporting:
  Last ACK received: Jan 21 04:04:10 2021 UTC
  Next ACK deadline: Mar 22 04:04:10 2021 UTC
  Reporting push interval: 30 days
  Next ACK push check: <none>
  Next report push: Feb 20 04:00:10 2021 UTC
  Last report push: Jan 21 04:00:10 2021 UTC
  Last report file write: <none>

```

```
Trust Code Installed: Jan 21 03:37:15 2021 UTC
```

```
License Usage
=====
```

```
throughput (ISR_4351_400M_Performance):
  Description: throughput
  Count: 1
  Version: 1.0
  Status: IN USE
  Export status: NOT RESTRICTED
  Feature Name: throughput
  Feature Description: throughput
  Enforcement type: NOT ENFORCED
  License type: Perpetual

```

```

hseck9 (ISR_4351_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
License type: Perpetual

```

```

appxk9 (ISR_4351_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
  License type: Perpetual

```

```

uck9 (ISR_4351_UnifiedCommunication):
  Description: uck9
  Count: 1

```


例: スマートライセンス (評価ライセンス) から Smart Licensing Using Policy へ

```

Version: 1.0
Status: IN USE
Export status: NOT RESTRICTED
Feature Name: uck9
Feature Description: uck9
Enforcement type: NOT ENFORCED
License type: Perpetual

securityk9 (ISR_4351_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
License type: Perpetual

Product Information
=====
UDI: PID:ISR4351/K9,SN:FDO21512BJB

Agent Version
=====
Smart Agent for Licensing: 5.0.6_rel/47

License Authorizations
=====
Overall status:
  Active: PID:ISR4351/K9,SN:FDO21512BJB
           Status: SMART AUTHORIZATION INSTALLED on Jan 21 03:58:37 2021 UTC
           Last Confirmation code: 76c6a69b

Authorizations:
  ISR_4351_Hsec (ISR_4351_Hsec):
    Description: U.S. Export Restriction Compliance license for 4350 series
    Total available count: 1
    Enforcement type: EXPORT RESTRICTED
    Term information:
      Active: PID:ISR4351/K9,SN:FDO21512BJB
      Authorization type: SMART AUTHORIZATION INSTALLED
      License type: PERPETUAL
      Term Count: 1

Purchased Licenses:
  No Purchase Information Available

Derived Licenses:
  Entitlement Tag:
  regid.2015-01.com.cisco.ISR_4351_400M_Performance,1.0_79a9ccb4-d7c3-46fd-9980-7efe247c90e5

  Entitlement Tag:
  regid.2015-01.com.cisco.ISR_4351_Application,1.0_601ccfff-5601-4293-98d2-2f653d864ce0

  Entitlement Tag:
  regid.2014-12.com.cisco.ISR_4351_UnifiedCommunication,1.0_a04fec0e-e944-4096-bcf8-05d6e9a0a6d3

  Entitlement Tag:
  regid.2014-12.com.cisco.ISR_4351_Security,1.0_df7d8d7f-b71a-4d3d-a9ab-aec7828a37a7

```

移行前と後の CSSM Web UI

<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。該当するスマートアカウントとバーチャルアカウントで、[Inventory]>[Product Instances] に移動して、すべての製品インスタンスを表示します。

移行前の CSSM Web UI

[Product Instances] タブ領域で、検索機能を使用して製品インスタンスを見つけます。検索結果が見つからないことがわかります。これは、この製品インスタンスのすべてのライセンスが評価ライセンスであるためです。つまり、製品インスタンスは CSSM と事前に通信していませんでした。

（評価ライセンスの概念は、スマートライセンス使用ポリシー環境には存在せず、すべての評価ライセンスが移行されます。これは、移行後のスクリーンショットに表示されます）。

The screenshot shows the Cisco Software Central interface for Smart Software Licensing. The breadcrumb path is 'Cisco Software Central > Smart Software Licensing'. The main title is 'Smart Software Licensing'. Below the title are navigation links: Alerts, Inventory, Convert to Smart Licensing, Reports, Preferences, On-Prem Accounts, and Activity. A 'Virtual Account' dropdown is set to 'Eg-VA-01'. There are tabs for 'General', 'Licenses', 'Product Instances', and 'Event Log'. The 'Product Instances' tab is active. A search bar contains the text 'FDO21512BJB'. Below the search bar, a table header is visible with columns 'Name', 'Product Type', and 'Last Contact'. The table content shows '0 results found' and 'No Records Found'.

移行後の CSSM Web UI

[Product Instances] タブで UDI をクリックし、次に示すように詳細なライセンス使用情報を表示します。

例 : Cisco ソフトウェアライセンス (PAK ライセンス) から Smart Licensing Using Policy へ

UDI_PID:ISR4351/K9; UDI_SN:FDO21512BJB;

Overview
Event Log

Description
ISR 4351 PRD

General

Name: UDI_PID:ISR4351/K9; UDI_SN:FDO21512BJB;

Product: ISR 4351 PRD

Host Identifier: -

MAC Address: -

PID: ISR4351/K9

Serial Number: FDO21512BJB

UUID: -

Virtual Account: Eg-VA-01

Registration Date: 2021-Jan-21 02:38:32

Last Contact: 2021-Jan-21 02:39:29

License Usage

License	Billing	Expires	Required
ISR_4351_Performance	Prepaid	-	1
ISR_4351_UnifiedCommunication	Prepaid	-	1
ISR_4351_400M_Performance	Prepaid	-	1
ISR_4351_Application	Prepaid	-	1

例 : Cisco ソフトウェアライセンス (PAK ライセンス) から Smart Licensing Using Policy へ

次に、Cisco 1000 シリーズ サービス統合型ルータと製品認証キー (PAK) ライセンスの例を示します。これは、Cisco ソフトウェアライセンス (CSL) のライセンスモデルに該当し、Smart Licensing Using Policy に移行されます。製品インスタンスのソフトウェアバージョンが Cisco IOS XE Fuji 16.9.1 から Cisco IOS XE Amsterdam 17.3.2 にアップグレードされます。



(注) この例では、PAK ライセンスに焦点を当てて説明しますが、製品インスタンスで使用可能な Right-to-Use (RTU) ライセンスも存在します。この例では、移行プロセス中に RTU ライセンスがどうなるかについても明確に示します。

また、システムによる PAK ライセンスの処理方法の変更と、使用可能なオプションをよく理解してください。詳細については、[PAK ライセンスのスナップショット \(43 ページ\)](#) を参照してください。

次に、この例の場合にアップグレード後はどうなるかについての概要を示します。

- 移行後の適用タイプ : 移行前は製品インスタンスで合計 7 つのライセンスを使用できます。これらのうちの 3 つのライセンスのみが使用されており (`show license feature, Enabled = yes`)、これらのライセンスの適用タイプは次のようになります。

- `hseck9`：これは HSECK9 PAK ライセンスであり、輸出規制ライセンスです。このライセンスは移行後も適用され、適用タイプは EXPORT RESTRICTED になります。移行後に SLAC をインストールする必要はありません。HSECK9 PAK ライセンスの要点については、[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 \(37ページ\)](#) を参照してください。
- `appxk9` と `securityk9`：使用されている残りの 2 つのライセンスは RTU ライセンスです。これらも移行され、移行後の適用タイプは NOT ENFORCED になります。

この例では、`appxk9` と `securityk9` は RTU ライセンスですが、PAK ライセンスである可能性もあります。確認するには、**show license feature** コマンドを使用します。出力の [RightToUse] 列に [yes] と表示されている場合は、RTU ライセンスであることを意味します。出力の [RightToUse] 列に [no] と表示されている場合は、PAK ライセンスです。

`ibasek9` と `internal_services`：製品インスタンスで常に使用可能なデフォルトのライセンスです。これらは移行されますが、表示されません。

`FoundationSuiteK9` と `throughput`：これらは RTU ライセンスです。使用されていない RTU ライセンス (**show license feature**: Enabled = no、および **show license**: License State: Active, Not in Use, EULA not accepted) は移行されません。

- 移行後のトランスポートタイプ：トランスポートタイプは PAK ライセンスには適用されません。そのため、デフォルトのトランスポートタイプ (`cslu`) は移行後も有効になっています。ソフトウェアイメージをアップグレードした後、CSLU を使用するトポロジを実装するか、サポートされている他のトポロジのいずれかを実装し、それに応じて転送タイプを設定できます。

この例では、トランスポートタイプ **smart** での CSSM への直接接続トポロジが実装されています。

- Device-Led Conversion (DLC)：PAK ライセンスと RTU ライセンスはスマートライセンスではないため、このシナリオでは DLC が適用されます。次の「移行後に必要なタスク」の項では、DLC のステータスを確認する方法について説明します。
- 移行後のレポート：ライセンス使用状況情報と DLC データが最初の同期の一部として送信されています。

最初の同期が完了した後ライセンスの消費に変更がある場合にのみ、PAK ライセンスの後続レポートが必要です。**show license status** コマンドの出力 ([Next report push] フィールドと [Next ACK deadline] フィールド) を使用して、レポートが必要かどうかといつまでに必要かを確認できます。また、レポートが必要な場合にもシステムメッセージが表示されます。実装するトポロジは、使用できるレポート方式によって異なります。

移行前と後の show コマンド

Cisco ソフトウェアライセンス環境 (この場合は PAK ライセンス) と、Smart Licensing Using Policy 環境とで使用可能なライセンス関連のコマンドはすべて同じではありません。同じコマンドが使用できない場合は、次の出力例で最も近いものが使用されてきました。

移行前と後の **show version**-----
show version Before Migration

次の出力には、アップグレード前のソフトウェアバージョンが示されています。

```
Device# show version
Cisco IOS XE Software, Version 16.09.01
Cisco IOS Software [Fuji], ISR Software (ARMV8EB_LINUX_IOSD-UNIVERSALK9_IAS-M), Version
16.9.1, RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2018 by Cisco Systems, Inc.
Compiled Tue 17-Jul-18 17:13 by mcpre
<output truncated>
```

show version After Migration

次の出力は、移行後のソフトウェアバージョンを示しています。その後にはシステムを新しいイメージで再起動したときに表示されるライセンス関連のシステムメッセージの抜粋が示されています。

```
Device# show version
Cisco IOS XE Software, Version 17.03.02
Cisco IOS Software [Amsterdam], ISR Software (ARMV8EL_LINUX_IOSD-UNIVERSALK9-M), Version
17.3.2, RELEASE SOFTWARE (fc3)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2020 by Cisco Systems, Inc.
Compiled Sat 31-Oct-20 11:31 by mcpre
<output truncated>

Press RETURN to get started!
*Jan 20 00:05:21.185: %ISR_THROUGHPUT-6-UNTHROTTLED: Crypto level is unthrottled
*Jan 20 00:05:23.766: %SMART_LIC-6-AGENT_ENABLED: Smart Agent for Licensing is enabled
*Jan 20 00:05:26.654: %SMART_LIC-6-EXPORT_CONTROLLED: Usage of export controlled features
is not allowed
*Jan 20 00:05:32.135: %SMART_LIC-6-EXPORT_CONTROLLED: Usage of export controlled features
is allowed for feature hseck9
*Jan 20 00:05:39.261: %SYS-5-RESTART: System restarted --
*Jan 20 00:06:10.308: %CALL_HOME-6-CALL_HOME_ENABLED: Call-home is enabled by Smart Agent
for Licensing.
*Jan 20 00:06:11.574: %SMART_LIC-6-REPORTING_REQUIRED: A Usage report acknowledgement
will be required in 365 days.
<output truncated>
```

移行前の **show license feature** と移行後の **show license summary**-----
show license feature Before Migration

移行前の出力には、製品インスタンスで使用可能なすべてのライセンスが表示されます。

有効になっているライセンス (Enabled = yes) に注意してください。これらは、移行後に使用できるすべてのライセンスです。

また、アップグレード後に2つのデフォルトのライセンス (ipbasek9 と internal_service) が使用可能になりますが、表示されません。デフォルトのライセンスは、有効になっているかどうかに関係なく使用可能になります。

Device# **show license feature**

Feature name	Enforcement	Evaluation	Subscription	Enabled	RightToUse
appxk9	yes	yes	no	yes	yes
securityk9	yes	yes	no	yes	yes
ipbasek9	no	no	no	no	no
FoundationSuiteK9	yes	yes	no	no	yes
hseck9	yes	no	no	yes	no
throughput	yes	yes	no	no	yes
internal_service	yes	no	no	no	no

show license summary After Migration

移行後の出力には、有効になっていた3つのライセンスが移行されていることが示され、IN USE というステータスで表示されます。

Device# **show license summary**

License Usage:	Entitlement Tag	Count	Status
hseck9	(ISR_1100_8P_Hsec)	1	IN USE
appxk9	(ISR_1100_8P_Application)	1	IN USE
securityk9	(ISR_1100_8P_Security)	1	IN USE

移行前の show license と移行後の show license usage

show license Before Migration

移行前の出力には、製品インスタンスで使用可能なすべてのライセンスの状態が示されます。

License State: Active, Not in Use, EULA not accepted と表示されているライセンスは移行されません。デフォルトの ipbasek9 と internal_service を含む他のすべてのライセンスが移行されます。

Device# **show license**

```

Index 1 Feature: appxk9
  Period left: Life time
  License Type: Permanent
  License State: Active, In Use
  License Count: Non-Counted
  License Priority: Medium
Index 2 Feature: securityk9
  Period left: Life time
  License Type: Permanent
  License State: Active, In Use
  License Count: Non-Counted
  License Priority: Medium
  
```

```

Index 3 Feature: ipbasek9
Index 4 Feature: FoundationSuiteK9
  Period left: Not Activated
  Period Used: 0 minute 0 second
  License Type: EvalRightToUse
License State: Active, Not in Use, EULA not accepted
  License Count: Non-Counted
  License Priority: None
Index 5 Feature: hseck9
  Period left: Life time
  License Type: Permanent
    License State: Active, In Use
  License Count: Non-Counted
  License Priority: Medium
Index 6 Feature: throughput
  Period left: Not Activated
  Period Used: 0 minute 0 second
  License Type: EvalRightToUse
License State: Active, Not in Use, EULA not accepted
  License Count: Non-Counted
  License Priority: None
Index 7 Feature: internal_service

```

show license usage After Migration

移行後の出力には、HSECK9 PAK ライセンスが適用され (Export status: RESTRICTED - ALLOWED)、適用タイプが EXPORT RESTRICTED であることが示されています。

他のすべてのライセンスは適用されておらず、適用タイプは NOT ENFORCED になっています。

Device# **show license usage**

```

License Authorization:
  Status: Not Applicable

hseck9 (ISR_1100_8P_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
  License type: Perpetual

appxk9 (ISR_1100_8P_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
  License type: Perpetual

securityk9 (ISR_1100_8P_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
License type: Perpetual
```

移行前と後の show license all

show license all Before Migration

移行前の出力には、製品インスタンスで使用可能なすべてのライセンスの詳細情報が表示されます。

```
Device# show license all

License Store: Primary License Storage
StoreIndex: 0 Feature: hseck9 Version: 1.0
License Type: Permanent
License State: Active, In Use
Lock type: Node locked
Vendor info: <UDI><PID>C1111-8PLTEEAWB</PID><SN>FGL214391J3</SN></UDI>
License Addition: Exclusive
License Generation version: 0x8100000
License Count: Non-Counted
License Priority: Medium
StoreIndex: 1 Feature: securityk9 Version: 1.0
License Type: Permanent
License State: Active, In Use
Lock type: Node locked
Vendor info: <UDI><PID>C1111-8PLTEEAWB</PID><SN>FGL214391J3</SN></UDI>
License Addition: Exclusive
License Generation version: 0x8100000
License Count: Non-Counted
License Priority: Medium
StoreIndex: 2 Feature: appxk9 Version: 1.0
License Type: Permanent
License State: Active, In Use
Lock type: Node locked
Vendor info: <UDI><PID>C1111-8PLTEEAWB</PID><SN>FGL214391J3</SN></UDI>
License Addition: Exclusive
License Generation version: 0x8100000
License Count: Non-Counted
License Priority: Medium
License Store: Built-In License Storage
StoreIndex: 0 Feature: appxk9 Version: 1.0
License Type: EvalRightToUse
License State: Inactive
Evaluation total period: 8 weeks 4 days
Evaluation period left: 8 weeks 4 days
Period used: 0 minute 0 second
Lock type: Non Node locked
Vendor info: <UDI><PID>NOTLOCKED</PID><SN>NOTLOCKED</SN></UDI><T>RTU</T>
License Addition: Additive
License Generation version: 0x8200000
License Count: Non-Counted
License Priority: None
StoreIndex: 1 Feature: securityk9 Version: 1.0
License Type: EvalRightToUse
```



```

License State: Inactive
  Evaluation total period: 8 weeks 4 days
  Evaluation period left: 8 weeks 4 days
  Period used: 0 minute 0 second
Lock type: Non Node locked
Vendor info: <UDI><PID>NOTLOCKED</PID><SN>NOTLOCKED</SN></UDI><T>RTU</T>
License Addition: Additive
License Generation version: 0x8200000
License Count: Non-Counted
License Priority: None
StoreIndex: 2 Feature: FoundationSuiteK9 Version: 1.0
License Type: EvalRightToUse
License State: Active, Not in Use, EULA not accepted
  Evaluation total period: 8 weeks 4 days
  Evaluation period left: 8 weeks 4 days
  Period used: 0 minute 0 second
Lock type: Non Node locked
Vendor info: <UDI><PID>NOTLOCKED</PID><SN>NOTLOCKED</SN></UDI><T>RTU</T>
License Addition: Additive
License Generation version: 0x8200000
License Count: Non-Counted
License Priority: None
StoreIndex: 3 Feature: throughput Version: 1.0
License Type: EvalRightToUse
License State: Active, Not in Use, EULA not accepted
  Evaluation total period: 8 weeks 4 days
  Evaluation period left: 8 weeks 4 days
  Period used: 0 minute 0 second
Lock type: Non Node locked
Vendor info: <UDI><PID>NOTLOCKED</PID><SN>NOTLOCKED</SN></UDI><T>RTU</T>
License Addition: Additive
License Generation version: 0x8200000
License Count: Non-Counted
License Priority: None

```

show license all After Migration

移行後の出力には、製品インスタンスが Smart Licensing Using Policy であることが示されています (Smart Licensing Using Policy: Status: ENABLED)。

PAK ライセンスにはアップグレード前の環境のトランスポートタイプがないため、アップグレード後にデフォルトのトランスポートタイプ (Type: csLu) が有効になります。

現時点では、デフォルトのポリシーが有効です (Policy: の下に CISCO default が表示されます)。他のポリシーが使用できない場合、製品インスタンスは表 6: ポリシー: Cisco default のポリシーを適用します。カスタムポリシーが使用可能であれば、トポロジが実装されて最初の同期が完了した後に適用されます。

HSECK9 PAK ライセンスの場合は SLAC のインストールは必要ないため、License Authorizations の下にある Status: NOT INSTALLED は無視して構いません (License Usage の下にある Export status: RESTRICTED - ALLOWED に注意してください。これは、移行後にライセンスが適用されることを示しています)。

Device# **show license all**

```

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

Smart Licensing Using Policy:
  Status: ENABLED

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

Transport:
  Type: cslu
  Cslu address: <empty>
  Proxy:
    Not Configured

Miscellaneous:
  Custom Id: <empty>

Policy:
  Policy in use: Merged from multiple sources.
  Reporting ACK required: yes (CISCO default)
  Unenforced/Non-Export Perpetual Attributes:
    First report requirement (days): 365 (CISCO default)
    Reporting frequency (days): 0 (CISCO default)
    Report on change (days): 90 (CISCO default)
  Unenforced/Non-Export Subscription Attributes:
    First report requirement (days): 90 (CISCO default)
    Reporting frequency (days): 90 (CISCO default)
    Report on change (days): 90 (CISCO default)
  Enforced (Perpetual/Subscription) License Attributes:
    First report requirement (days): 0 (CISCO default)
    Reporting frequency (days): 0 (CISCO default)
    Report on change (days): 0 (CISCO default)
  Export (Perpetual/Subscription) License Attributes:
    First report requirement (days): 0 (CISCO default)
    Reporting frequency (days): 0 (CISCO default)
    Report on change (days): 0 (CISCO default)

Usage Reporting:
  Last ACK received: <none>
  Next ACK deadline: Jan 20 00:06:11 2022 UTC
  Reporting push interval: 30 days
  Next ACK push check: <none>
  Next report push: Jan 20 00:08:11 2021 UTC
  Last report push: <none>
  Last report file write: <none>

Trust Code Installed: <none>

License Usage
=====

```

例: Cisco ソフトウェアライセンス (PAK ライセンス) から Smart Licensing Using Policy へ

```
hseck9 (ISR_1100_8P_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
  License type: Perpetual

appxk9 (ISR_1100_8P_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
  License type: Perpetual

securityk9 (ISR_1100_8P_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
  License type: Perpetual

Product Information
=====
UDI: PID:C1111-8PLTEEAWB,SN:FGL214391J3

Agent Version
=====
Smart Agent for Licensing: 5.0.6_rel/47

License Authorizations
=====
Overall status:
  Active: PID:C1111-8PLTEEAWB,SN:FGL214391J3
  Status: NOT INSTALLED
  Status:PAK

Legacy License Info:
  regid.2017-04.com.cisco.ISR_1100_8P_Application,
  1.0_c4cf42aa-2d60-4f4e-83dd-c5c9672132c9:
  DisplayName: appxk9
  Description: appxk9
  Total available count: 1
  Term information:
    Active: PID:C1111-8PLTEEAWB,SN:FGL214391J3
    License type: PERPETUAL
    Term Count: 1

  regid.2017-04.com.cisco.ISR_1100_8P_Security,
  1.0_6b61b693-0daa-42d4-8cee-930de5c1b37c:
  DisplayName: securityk9
  Description: securityk9
```

```
Total available count: 1
Term information:
  Active: PID:C1111-8PLTEEAWB,SN:FGL214391J3
  License type: PERPETUAL
  Term Count: 1

regid.2017-08.com.cisco.ISR_1100_8P_Hsec,
1.0_34a5e7e7-722a-41ab-bdad-d53d5a3cac14:
  DisplayName: hseck9
  Description: hseck9
  Total available count: 1
  Term information:
    Active: PID:C1111-8PLTEEAWB,SN:FGL214391J3
    License type: PERPETUAL
    Term Count: 1
```

移行前と後の show platform hardware throughput crypto

show platform hardware throughput crypto Before Migration

移行前の出力には、暗号化スループットがスロットリングされていないことが示されています。使用可能なHSECK9PAKライセンスでは、スロットリングされていない暗号化スループットの使用が許可されます。したがって、移行後もこの設定に変更はありません (Cisco 1000 シリーズサービス統合型ルータでは、デフォルトでスループットはスロットリングされません)。HSECK9ライセンスは、スロットリングされない暗号化スループットを提供します)。

```
Device# show platform hardware throughput crypto
The current crypto level is unthrottled
```

show platform hardware throughput crypto After Migration

移行後の出力には、暗号化スループットの設定が移行後も同じであることが示されています。

```
Device# show platform hardware throughput crypto
The current crypto level is unthrottled
```

移行前と後の show platform software cerm-information

show platform software cerm-information Before Migration

移行前の出力には、CERM機能が有効になっていることが示されています。移行後も、この設定に変更はありません。

```
Device# show platform software cerm-information
Crypto Export Restrictions Manager(CERM) Information:
  CERM functionality: DISABLED
```

show platform software cerm-information After Migration

移行後の出力には、CERM 設定が移行後も同じであることが示されています。

```
Device# show platform software cerm-information
Crypto Export Restrictions Manager (CERM) Information:
  CERM functionality: DISABLED
```

移行後に必要なタスク

1. トポロジを実装します。

この例では、トランスポートタイプに **smart** を使用して [CSSM に直接接続 \(21 ページ\)](#) トポロジを実装します。対応するワークフローについては、[トポロジのワークフロー: CSSM に直接接続 \(53 ページ\)](#) を参照してください。

1. スマートアカウントを設定します。

スマートアカウントとバーチャルアカウントの設定はすでに完了しているため、この例には示していません。

2. CSSM への製品インスタンスの接続を設定します。

設定に必要な手順については、[CSSM への接続の設定 \(189 ページ\)](#) を参照してください。

3. 接続方式とトランスポートタイプを設定します。

次の設定例には、スマートトランスポートを使用するために必要な設定が示されています。

```
Device(config)# license smart transport smart
Device(config)# license smart url default
Device(config)# exit
Device# copy running-config startup-config
```

4. CSSM との信頼を確立します。

トークン生成プロセスはここには示していませんが、実行する必要があります。[CSSM からの信頼コード用新規トークンの生成 \(227 ページ\)](#) を参照してください。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。期限が切れていない限り、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。トークンの有効期限は、トークンの生成時に入力する [Expire After] フィールドに対応します。

信頼コードをインストールします。

次の設定例では、信頼コードのインストール方法を示し、その後にシステムメッセージを示します。システムメッセージには、輸出規制機能の使用が許可され、新しいポリシーがインストールされ、信頼コードが正常にインストールされたことを確認したことが示されています。

```
Device# license smart trust idtoken
V0p1dCtXVXY2ZUxBQ29XYUU2Zys3dzI2aU5ZNDc1%0AQW9URT0%3D%0A a11
```

```

Device#
*Jan 20 02:47:00.173: %SMART_LIC-6-EXPORT_CONTROLLED: Usage of exportcontrolled
features is allowed for feature hseck9
*Jan 20 02:47:00.202: %SMART_LIC-6-POLICY_INSTALL_SUCCESS: A new licensing policy
was successfully installed
*Jan 20 02:47:00.392: %SMART_LIC-6-TRUST_INSTALL_SUCCESS: A new licensing trust
code was successfully installed on P:C1111-8PLTEEAWB,S:FGL214391J3.

```

これでトポロジの実装は完了です。

2. DLC のステータスを確認します。

DLC の進行状況をモニタするには、特権 EXEC モードのコマンドで **show platform software license dlc** コマンドを入力します。出力に DLC Process Status: Completed、DLC Conversion Status: SUCCESS が表示されたら、DLC は完了です。DLC のデータは、次の手順で使用状況レポートの一部として CSSM に送信されます。

次の出力例の最初のインスタンスには、ソフトウェアバージョンがアップグレードされた直後に DLC プロセスのステータスが示されています。出力例の 2 番目のインスタンスには、約 1 時間後の DLC プロセスのステータスが示されています。

```

Device# show platform software license dlc
Index 1 Feature:          appxk9
  Permanent License:    1
  EVAL RTU License:    0
  RTU License:         0
  Paper License:       0
Index 2 Feature:          securityk9
  Permanent License:    1
  EVAL RTU License:    0
  RTU License:         0
  Paper License:       0
Index 3 Feature:          hseck9
  Permanent License:    1
  EVAL RTU License:    0
  RTU License:         0
  Paper License:       0

```

DLC Process Status: Not Complete

<<<<AFTER APPROXIMATELY AN HOUR>>>>

```

Device# show platform software license dlc
Index 1 Feature:          appxk9
  Permanent License:    1
  EVAL RTU License:    0
  RTU License:         0
  Paper License:       0
Index 2 Feature:          securityk9
  Permanent License:    1
  EVAL RTU License:    0
  RTU License:         0
  Paper License:       0
Index 3 Feature:          hseck9
  Permanent License:    1
  EVAL RTU License:    0
  RTU License:         0
  Paper License:       0

```

DLC Process Status: Completed

DLC Conversion Status: SUCCESS

3. ライセンスの使用状況を CSSM と同期し、同期を確認し、後続のレポートの要件を確認します。

このトポロジでは、特権 EXEC モードで **license smart sync** コマンドを入力して使用状況を同期できます。これにより、保留中のデータが手動で CSSM と同期 (送受信) されます。

次の設定例にはこれが示されています。その後、同期が正常に実行されたことが示され、輸出規制機能の使用が許可されていることを確認するシステムメッセージが続いています。

同期が正常に行われたことは、ポリシーのインストールが成功したことによって示されます (カスタムポリシーは RUM ACK 内に含めることができ、送信された RUM レポートに応答して CSSM が RUM ACK を送信します)。

```
Device# license smart sync all
*Jan 20 02:51:36.650: %SMART_LIC-6-EXPORT_CONTROLLED: Usage of export controlled
features is allowed for feature hseck9
*Jan 20 02:51:36.689: %SMART_LIC-6-POLICY_INSTALL_SUCCESS: A new licensing policy
was successfully installed
```

同期を確認するには、特権 EXEC モードで **show license all** コマンドを入力します。次の出力例では、次のフィールドを使用して同期を確認できます。

- タイムスタンプの更新: Policy in use: Installed On Jan 20 02:51:36 2021 UTC
- タイムスタンプの更新: Last ACK received: Jan 20 02:51:36 2021 UTC

CSSM への直接接続トポロジでは、製品インスタンスがポリシーに基づいて次の RUM レポートを CSSM に送信します。出力例では、次のフィールドにこの情報が示されています。

- Next ACK deadline: Feb 19 02:51:36 2021 UTC
- Next report push: Feb 19 02:47:36 2021 UTC

```
Device# show license all
Smart Licensing Status
=====

Smart Licensing is ENABLED

License Conversion:
  Automatic Conversion Enabled: False
  Status: Successful on Jan 20 03:17:23 2021 UTC

Export Authorization Key:
  Features Authorized:
    <none>

Utility:
  Status: DISABLED

Smart Licensing Using Policy:
  Status: ENABLED

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

```

Version privacy: DISABLED

Transport:
  Type: Smart
  URL: https://smartreceiver.cisco.com/licservice/license
  Proxy:
    Not Configured

Miscellaneous:
  Custom Id: <empty>

Policy:
  Policy in use: Installed On Jan 20 02:51:36 2021 UTC
  Policy name: SLP Policy
  Reporting ACK required: yes (Customer Policy)
  Unenforced/Non-Export Perpetual Attributes:
    First report requirement (days): 30 (Customer Policy)
    Reporting frequency (days): 60 (Customer Policy)
    Report on change (days): 60 (Customer Policy)
  Unenforced/Non-Export Subscription Attributes:
    First report requirement (days): 120 (Customer Policy)
    Reporting frequency (days): 150 (Customer Policy)
    Report on change (days): 120 (Customer Policy)
  Enforced (Perpetual/Subscription) License Attributes:
    First report requirement (days): 0 (CISCO default)
    Reporting frequency (days): 90 (Customer Policy)
    Report on change (days): 60 (Customer Policy)
  Export (Perpetual/Subscription) License Attributes:
    First report requirement (days): 0 (CISCO default)
    Reporting frequency (days): 30 (Customer Policy)
    Report on change (days): 30 (Customer Policy)

Usage Reporting:
  Last ACK received: Jan 20 02:51:36 2021 UTC
  Next ACK deadline: Feb 19 02:51:36 2021 UTC
  Reporting push interval: 30 days
  Next ACK push check: <none>
  Next report push: Feb 19 02:47:36 2021 UTC
  Last report push: Jan 20 02:47:36 2021 UTC
  Last report file write: <none>

Trust Code Installed: Jan 20 02:47:00 2021 UTC

License Usage
=====

hseck9 (ISR_1100_8P_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
  License type: Perpetual

appxk9 (ISR_1100_8P_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
License type: Perpetual

securityk9 (ISR_1100_8P_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
License type: Perpetual

Product Information
=====
UDI: PID:C1111-8PLTEEAWB,SN:FGL214391J3

Agent Version
=====
Smart Agent for Licensing: 5.0.6_rel/47

License Authorizations
=====
Overall status:
  Active: PID:C1111-8PLTEEAWB,SN:FGL214391J3
  Status: NOT INSTALLED
  Status:PAK

Legacy License Info:

regid.2017-04.com.cisco.ISR_1100_8P_Application,1.0_c4cf42aa-2d60-4f4e-83dd-c5c9672132c9:

  DisplayName: appxk9
  Description: appxk9
  Total available count: 1
  Term information:
    Active: PID:C1111-8PLTEEAWB,SN:FGL214391J3
    License type: PERPETUAL
    Term Count: 1

regid.2017-04.com.cisco.ISR_1100_8P_Security,1.0_6b61b693-0daa-42d4-8cee-930de5c1b37c:

  DisplayName: securityk9
  Description: securityk9
  Total available count: 1
  Term information:
    Active: PID:C1111-8PLTEEAWB,SN:FGL214391J3
    License type: PERPETUAL
    Term Count: 1

regid.2017-08.com.cisco.ISR_1100_8P_Hsec,1.0_34a5e7e7-722a-41ab-bdad-d53d5a3cac14:

  DisplayName: hseck9
  Description: hseck9
  Total available count: 1
  Term information:
    Active: PID:C1111-8PLTEEAWB,SN:FGL214391J3
    License type: PERPETUAL
    Term Count: 1

```

このシナリオでの移行は完了です。

移行前と後の CSSM Web UI

<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。

移行前の CSSM Web UI

該当するスマートアカウントとバーチャルアカウントで、[Inventory]>[Licenses]に移動して、使用可能なライセンスを表示します。

次のスクリーンショットに、アップグレード前に製品インスタンスでライセンスがどのように表示されるかを示します。

これらはスマートライセンスではないため、[Insufficient Licenses] と表示されます。同じ理由で、それらの数は負になります。

The screenshot shows the 'Smart Software Licensing' interface. The 'Inventory' tab is selected, and the 'Licenses' sub-tab is active. The 'Virtual Account' is 'Eg-VA-01'. The table below shows the license details:

License	Billing	Purchased	In Use	Substitution	Balance	Alerts	Actions
Cisco 1100 Series with 8 LAN Ports, 200 Mbps IPSEC Throughput License	Prepaid	1	1	-	0		Actions
Cisco 1100 Series with 8 LAN Ports, AppX License	Prepaid	1	2	-	-1	Insufficient Licenses	Actions
Cisco 1100 Series with 8 LAN Ports, Security License	Prepaid	1	2	-	-1	Insufficient Licenses	Actions
ISR_1100_8P_Hsec	Prepaid	0	1	-	-1	Insufficient Licenses	Actions
Router US Export Lic. for DNA	Prepaid	1	0	-	+1		Actions

移行後の CSSM Web UI

該当するスマートアカウントで、[Convert to Smart Licensing]>[Conversion History]に移動して、変換ステータスを確認します。

次のスクリーンショットに、アップグレード後に製品インスタンスでライセンスがどのように表示されるかを示します。

成功した DLC は [Conversion Status] 列に反映されます。

例：Cisco ソフトウェアライセンス（RTU ライセンス）から Smart Licensing Using Policy へ

Cisco Software Central > Smart Software Licensing Eg-SA-01

Smart Software Licensing Feedback Support Help

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

License Conversion

Convert PAKs | Convert Licenses | **Conversion History** | Event Log

Search by Device Identifier or Product Family

Source	Device	Product Family	Conversion Status	Time	Actions
Device	UDI_PID:C1111-8PLTEEAWB; UDI...	800 Fixed	Licenses Converted	2021-Jan-20 00:56:00	

[Device] 列の製品インスタンスをクリックすると、その製品インスタンスのライセンス使用状況の詳細が表示されます。これは次のスクリーンショットに表示されます ([Alerts] 列に [Insufficient Licenses] が表示されなくなり、[Balance] 列のすべてのライセンスの数が更新されます)。

Virtual Account: **Eg-VA-01**

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

Available Actions | Manage License Tags | License Reservation... | Show License Transactions | Search by License

License	Billing	Purchased	In Use	Substitution	Balance	Alerts
Cisco 1100 Series with 8 LAN Ports, AppX License	Prepaid	1	1	-	0	
Cisco 1100 Series with 8 LAN Ports, Security License	Prepaid	1	1	-	0	
ISR_1100_8P_Hsec	Prepaid	2	1	-	+1	

Showing All 3 R...

例：Cisco ソフトウェアライセンス（RTU ライセンス）から Smart Licensing Using Policy へ

次に、Cisco 4351 サービス統合型ルータでRight-to-Use (RTU) ライセンスを使用する例を示します。このライセンスは、Cisco Software Licensing (CSL) ライセンスモデルに該当し、Smart Licensing Using Policy です。製品インスタンスのソフトウェアバージョンは、Cisco IOS XE Gibraltar 16.19.6 から Cisco IOS XE Bengaluru 17.3.2 にアップグレードされます。次に、この例の場合にアップグレード後はどうなるかについての概要を示します。

- 移行後の適用タイプ：移行前は製品インスタンスで合計 10 ライセンスを使用できます。
appxk9、uck9、securityk9、および slrूपट：これら 4 つのライセンスのみが使用されており (show license feature, Enabled=yes)、移行されます。これらはすべて RTU ライセンスです (show license feature RightToUse=yes)。いずれも輸出規制の対象でないため、移行後は適用タイプが NOT ENFORCED になります。

ipbasek9 と internal_services：製品インスタンスで常に使用可能なデフォルトのライセンスです。これらは移行されますが、表示されません。

FoundationSuiteK9、AdvUCSuiteK9、cme-srst：これらは RTU ライセンスです。使用されていない RTU ライセンス (**show license feature**: Enabled = no、および **show license**: License State: Active, Not in Use, EULA not accepted) は移行されません。

hseck9：これは輸出規制ライセンスであり、RTU 環境では PAK ライセンスが必要です。ただし、この例では、必須の PAK ライセンスが使用できません。したがって、このライセンスは移行されません。

- 移行後のトランスポートタイプ：トランスポートタイプは RTU ライセンスには適用されません。そのため、デフォルトのトランスポートタイプ (**cslu**) は移行後も有効になっています。ソフトウェアイメージをアップグレードした後、CSLU を使用するトポロジか、またはサポートされている他のいずれかのトポロジを実装し、それに従ってトランスポートタイプを設定できます。

この例では、トランスポートタイプが **cslu** の CSLU を介した CSSM への接続 (製品インスタンス開始型通信を使用) トポロジが実装されます。

- Device-Led Conversion (DLC)：DLC はこのシナリオに適用されます。これは、RTU ライセンスがスマートライセンスではないためです。次の「移行後に必要なタスク」の項では、DLC のステータスを確認する方法について説明します。
- 移行後のレポート：ライセンス使用状況情報と DLC データが最初の同期の一部として送信されています。

最初の同期が完了した後の RTU ライセンスの後続のレポートは、使用されているライセンスによって異なります。**show license status** コマンドの出力 ([Next report push] フィールドと [Next ACK deadline] フィールド) を使用して、レポートが必要かどうかといつまでに必要かを確認できます。また、レポートが必要な場合にもシステムメッセージが表示されます。実装するトポロジは、使用できるレポート方式によって異なります。

移行前と後の show コマンド

Cisco ソフトウェアライセンス環境 (この場合は RTU ライセンス) と、Smart Licensing Using Policy 環境とで使用可能なライセンス関連のコマンドは、すべて同じではありません。同じコマンドが使用できない場合は、次の出力例で最も近いものが使用されてきました。

移行前と後の show version

```
-----
show version Before Migration
-----
```

次の出力には、アップグレード前のソフトウェアバージョンが示されています。

```
Device# show version
Cisco IOS XE Software, Version 16.09.06
Cisco IOS Software [Fuji],
ISR Software (X86_64_LINUX_IOSD-UNIVERSALK9-M),
Version 16.9.6, RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
```

```
Copyright (c) 1986-2020 by Cisco Systems, Inc.
Compiled Thu 27-Aug-20 02:41 by mcpre
```

```
<output truncated>
```

```
show version After Migration
```

次の出力は、移行後のソフトウェアバージョンを示しています。その後にはシステムを新しいイメージで再起動したときに表示されるライセンス関連のシステムメッセージの抜粋が示されています。

```
Device# show version
Cisco IOS XE Software, Version 17.03.02
Cisco IOS Software [Amsterdam],
ISR Software (X86_64_LINUX_IOSD-UNIVERSALK9-M),
Version 17.3.2, RELEASE SOFTWARE (fc3)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2020 by Cisco Systems, Inc.
Compiled Sat 31-Oct-20 13:21 by mcpre
```

```
<output truncated>
```

```
Press RETURN to get started!
```

```
*Jan 29 18:18:31.506: %ISR_THROUGHPUT-6-LEVEL: Throughput level has been set to 400000
kbps
*Jan 29 18:18:34.482: %SMART_LIC-6-AGENT_ENABLED: Smart Agent for Licensing is enabled
*Jan 29 18:18:34.980: %SMART_LIC-6-EXPORT_CONTROLLED: Usage of export controlled features
is not allowed.
*Jan 29 18:19:04.089: %SYS-5-RESTART: System restarted --
*Jan 29 18:19:41.554: %CALL_HOME-6-CALL_HOME_ENABLED: Call-home is enabled by Smart Agent
for Licensing.
*Jan 29 18:19:42.803: %SMART_LIC-6-REPORTING_REQUIRED: A Usage report acknowledgement
will be required in 365 days.
```

移行前の **show license feature** と移行後の **show license summary**

```
show license feature Before Migration
```

移行前の出力には、製品インスタンスで使用可能なすべてのライセンスが表示されます。

有効になっているライセンス (Enabled = yes) に注意してください。これらは、移行後に使用できるすべてのライセンスです。

また、アップグレード後に2つのデフォルトのライセンス (ipbasek9 と internal_service) が使用可能になりますが、表示されません。デフォルトのライセンスは、有効になっているかどうかに関係なく使用可能になります。

```
Device# show license feature
```

Feature name	Enforcement	Evaluation	Subscription	Enabled	RightToUse
appxk9	yes	yes	no	yes	yes
uck9	yes	yes	no	yes	yes

```

securityk9          yes          yes          no          yes          yes
ipbasek9           no          no          no          no          no
FoundationSuiteK9  yes          yes          no          no          yes
AdvUCSuiteK9       yes          yes          no          no          yes
cme-srst           yes          yes          no          no          yes
hseck9             yes          no          no          no          no
throughput         yes          yes          no          yes          yes
internal_service   yes          no          no          no          no
    
```

show license summary After Migration

移行後の出力には、アップグレード前に有効になっていた (Enabled = yes) すべてのライセンスが移行されていることが示され、ステータスは IN USE で表示されます。

デフォルトライセンス (ipbasek9、internal_service) も移行されますが、表示されません。

Device# **show license summary**

```

License Usage:
License              Entitlement Tag              Count Status
-----
throughput          (ISR_4351_400M_Performance)  1 IN USE
appxk9              (ISR_4351_Application)      1 IN USE
uck9                 (ISR_4351_UnifiedCommun...)  1 IN USE
securityk9          (ISR_4351_Security)         1 IN USE
    
```

移行前の **show license** と移行後の **show license all**

show license Before Migration

移行前の出力には、製品インスタンスで使用可能なすべてのライセンスの状態が示されます。

License State: Active, In Use のすべてのライセンスに注意してください。これらは、上記の **show license feature** 特権 EXEC コマンドの出力例で Enabled = yes で表示されているライセンスです。これらのライセンスとデフォルトのライセンスが移行されます。

License State: Active, Not in Use, EULA not accepted と表示されているライセンスは移行されません。

Device# **show license**

```

Index 1 Feature: appxk9
  Period left: 8 weeks 3 days
  Period Used: 5 minutes 27 seconds
  License Type: EvalRightToUse
  License State: Active, In Use
  License Count: Non-Counted
  License Priority: Low
Index 2 Feature: uck9
  Period left: 8 weeks 3 days
  Period Used: 5 minutes 27 seconds
  License Type: EvalRightToUse
  License State: Active, In Use
  License Count: Non-Counted
  License Priority: Low
    
```

例 : Cisco ソフトウェアライセンス (RTU ライセンス) から Smart Licensing Using Policy へ

```

Index 3 Feature: securityk9
  Period left: 8 weeks 3 days
  Period Used: 5 minutes 27 seconds
  License Type: EvalRightToUse
  License State: Active, In Use
  License Count: Non-Counted
  License Priority: Low
Index 4 Feature: ipbasek9
Index 5 Feature: FoundationSuiteK9
  Period left: Not Activated
  Period Used: 0 minute 0 second
  License Type: EvalRightToUse
  License State: Active, Not in Use, EULA not accepted
  License Count: Non-Counted
  License Priority: None
Index 6 Feature: AdvUCSuiteK9
  Period left: Not Activated
  Period Used: 0 minute 0 second
  License Type: EvalRightToUse
  License State: Active, Not in Use, EULA not accepted
  License Count: Non-Counted
  License Priority: None
Index 7 Feature: cme-srst
  Period left: Not Activated
  Period Used: 0 minute 0 second
  License Type: EvalRightToUse
  License State: Active, Not in Use, EULA not accepted
  License Count: 0/0 (In-use/Violation)
  License Priority: None
Index 8 Feature: hseck9
Index 9 Feature: throughput
  Period left: 8 weeks 3 days
  Period Used: 5 minutes 26 seconds
  License Type: EvalRightToUse
  License State: Active, In Use
  License Count: Non-Counted
  License Priority: Low
Index 10 Feature: internal_service

```

show license all After Migration

移行後の出力には、製品インスタンスが Smart Licensing Using Policy であることが示されています (Smart Licensing Using Policy: Status: ENABLED)。

Transport セクション : RTU ライセンスにはアップグレード前の環境のトランスポートタイプがないため、アップグレード後にデフォルトのトランスポートタイプ (Type: cslu) が有効になります。

Policy セクション : 現時点では、デフォルトのポリシーが有効になっています (Policy: の下の CISCO Transport を参照)。他のポリシーが使用できない場合、製品インスタンスは表 6: ポリシー : Cisco default のポリシーを適用します。カスタムポリシーが使用可能であれば、トポログが実装されて最初の同期が完了した後に適用されます。

License Usage セクション : 輸出規制がなく、すべてのライセンスが Enforcement type: NOT ENFORCED になっています。

```

Device# show license all
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

Smart Licensing Using Policy:
  Status: ENABLED

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

Transport:
  Type: cslu
  Cslu address: <empty>
  Proxy:
    Not Configured

Miscellaneous:
  Custom Id: <empty>

Policy:
  Policy in use: Merged from multiple sources.
  Reporting ACK required: yes (CISCO default)
  Unenforced/Non-Export Perpetual Attributes:
    First report requirement (days): 365 (CISCO default)
    Reporting frequency (days): 0 (CISCO default)
    Report on change (days): 90 (CISCO default)
  Unenforced/Non-Export Subscription Attributes:
    First report requirement (days): 90 (CISCO default)
    Reporting frequency (days): 90 (CISCO default)
    Report on change (days): 90 (CISCO default)
  Enforced (Perpetual/Subscription) License Attributes:
    First report requirement (days): 0 (CISCO default)
    Reporting frequency (days): 0 (CISCO default)
    Report on change (days): 0 (CISCO default)
  Export (Perpetual/Subscription) License Attributes:
    First report requirement (days): 0 (CISCO default)
    Reporting frequency (days): 0 (CISCO default)
    Report on change (days): 0 (CISCO default)

Usage Reporting:
  Last ACK received: <none>
  Next ACK deadline: Jan 29 18:19:42 2022 UTC
  Reporting push interval: 30 days
  Next ACK push check: <none>
  Next report push: Jan 29 18:21:42 2021 UTC
  Last report push: <none>
  Last report file write: <none>

Trust Code Installed: <none>

License Usage

```



```
=====
throughput (ISR_4351_400M_Performance):
  Description: throughput
  Count: 1
  Version: 1.0
  Status: IN USE
  Export status: NOT RESTRICTED
  Feature Name: throughput
  Feature Description: throughput
  Enforcement type: NOT ENFORCED
  License type: Perpetual

appxk9 (ISR_4351_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
  License type: Perpetual

uck9 (ISR_4351_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
  License type: Perpetual

securityk9 (ISR_4351_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
  License type: Perpetual

Product Information
=====
UDI: PID:ISR4351/K9,SN:FDO210305DQ

Agent Version
=====
Smart Agent for Licensing: 5.0.6_rel/47

License Authorizations
=====
Overall status:
  Active: PID:ISR4351/K9,SN:FDO210305DQ
  Status: NOT INSTALLED

Purchased Licenses:
  No Purchase Information Available
```

```
Derived Licenses:
  Entitlement Tag: regid.2015-01.com.cisco.ISR_4351_400M_Performance,
1.0_79a9ccb4-d7c3-46fd-9980-7efe247c90e5
  Entitlement Tag: regid.2015-01.com.cisco.ISR_4351_Application,
1.0_601ccfff-5601-4293-98d2-2f653d864ce0
  Entitlement Tag: regid.2014-12.com.cisco.ISR_4351_UnifiedCommunication,
1.0_a04fec0e-e944-4096-bcf8-05d6e9a0a6d3
  Entitlement Tag: regid.2014-12.com.cisco.ISR_4351_Security,
1.0_df7d8d7f-b71a-4d3d-a9ab-aec7828a37a7
```

移行前と後の show platform hardware throughput level

show platform hardware throughput level Before Migration

このコマンドは、現在設定されているスループットを表示します。出力例には、スループットが 400000 kbps に設定されていることが示されています。これは、増大するスループットを許可するパフォーマンスライセンスによって承認されます (**show license** の出力、Feature: throughput を参照)。したがって、設定されたスループットは移行後も保持されます。

```
Device# show platform hardware throughput level
The current throughput level is 400000 kbps
```

show platform hardware throughput level After Migration

出力例には、移行後にスループット設定が保持されることが示されています。

```
Device# show platform hardware throughput level
The current throughput level is 400000 kbps
```

移行後に必要なタスク

1. トポロジを実装します。

この例では、トランスポートタイプ **cslu** を使用して **CSLU** を介して **CSSM** に接続 (19 ページ) (製品インスタンス開始型通信) のトポロジを実装します。対応するワークフローについては、**トポロジのワークフロー：CSLU を介して CSSM に接続 (49 ページ)** の「製品インスタンス開始型通信の場合のタスク」を参照してください。

1. CSLU のインストール

CSLU のインストールはここには示されていませんが、実行する必要があります

[Smart Software Manager]<https://software.cisco.com/download/home/286285506/type>> [Smart Licensing Utility] からファイルをダウンロードします。

インストールとセットアップの詳細については、**Cisco Smart License Utility クイック スタートセットアップガイド** を参照してください。

2. CSLU の環境設定

CSLU の設定はここには示されていませんが、実行する必要があります

[シスコへのログイン \(CSLU インターフェイス\) \(176 ページ\)](#)

[スマートアカウントとバーチャルアカウントの設定 \(CSLU インターフェイス\) \(177 ページ\)](#)

[CSLU での製品開始型製品インスタンスの追加 \(CSLU インターフェイス\) \(177 ページ\)](#)

3. 製品インスタンスの設定

ネットワークの到達可能性を確保するために必要なすべてのコマンドを設定します。設定に必要な手順については、[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の確認 \(178 ページ\)](#) を参照してください。

```
Device(config)# ip route 192.168.0.1 255.255.0.0 192.168.255.1
```

転送タイプが **cslu** に設定されていることを確認します。

CSLU はデフォルトのトランスポートタイプです。これは変更されていないため、再設定する必要はありません (上記の **show license all** 特権 EXEC コマンドの出力例を参照)。

CSLU の検出方法を指定し、CSLU と同期して保留中のデータを送受信します。

次の例では、CSLU 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 ホストのホスト名や IP アドレスを入力します。8182 はポート番号であり、CSLU が使用する唯一のポート番号です。

設定の完了後に表示されるシステムメッセージには、CSLU との通信が確立されていることが示されています。

```
Device(config)# license smart url cslu http://192.168.0.1:8182/cslu/v1/pi
*Jan 29 18:36:35.457: %SMART_LIC-5-COMM_RESTORED: Communications with Cisco Smart License Utility (CSLU) restored.
```

これでトポロジの実装は完了です。

2. DLC のステータスを確認します。

DLC の進行状況をモニタするには、特権 EXEC モードのコマンドで **show platform software license dlc** コマンドを入力します。出力に DLC Process Status: Completed、DLC Conversion Status: SUCCESS が表示されたら、DLC は完了です。DLC のデータは、次の手順で使用状況レポートの一部として CSSM に送信されます。

次の出力例の最初のインスタンスには、ソフトウェアバージョンがアップグレードされた直後に DLC プロセスのステータスが示されています。出力例の 2 番目のインスタンスには、約 1 時間後の DLC プロセスのステータスが示されています。

```
Device# show platform software license dlc
```

```
Index 1 Feature:          appxk9
Permanent License: 0
EVAL RTU License: 1
```

```

RTU License:      0
Paper License:   0
Index 2 Feature:          uck9
Permanent License: 0
EVAL RTU License: 1
RTU License:      0
Paper License:   0
Index 3 Feature:          securityk9
Permanent License: 0
EVAL RTU License: 1
RTU License:      0
Paper License:   0
Index 4 Feature:          throughput
Permanent License: 0
EVAL RTU License: 1
RTU License:      0
Paper License:   0
    
```

DLC Process Status: Not Complete

<<<<AFTER 1 HOUR>>>>

Device# **show platform software license dlc**

```

Index 1 Feature:          appxk9
Permanent License: 0
EVAL RTU License: 1
RTU License:      0
Paper License:   0
Index 2 Feature:          uck9
Permanent License: 0
EVAL RTU License: 1
RTU License:      0
Paper License:   0
Index 3 Feature:          securityk9
Permanent License: 0
EVAL RTU License: 1
RTU License:      0
Paper License:   0
Index 4 Feature:          throughput
Permanent License: 0
EVAL RTU License: 1
RTU License:      0
Paper License:   0
    
```

DLC Process Status: Completed

DLC Conversion Status: SUCCESS

3. ライセンスの使用状況を CSSM と同期し、同期を確認し、後続のレポートの要件を確認します。

このトポロジでは、特権 EXEC モードで **license smart sync** コマンドを入力して使用状況を同期できます。これにより、保留中のデータが CSLU と手動で同期 (送受信) されます。その後で、CSLU が CSSM と同期します。

次の設定例にはこれが示されています。その後に同期が正常に実行されたことを示すシステムメッセージが表示されています。

```

Device# license smart sync all
*Jan 29 18:40:37.836: %SIP-1-LICENSING: SIP service is Up. License report acknowledged.
    
```

```
*Jan 29 18:40:38.484: %SMART_LIC-6-POLICY_INSTALL_SUCCESS: A new licensing policy
was successfully installed
```

同期を確認するには、特権 EXEC モードで **show license status** (または **show license all**) コマンドを入力します。

次の出力例では、次のフィールドを使用して同期が完了していることを確認できます。

- タイムスタンプの更新: Policy in use: Installed On Jan 29 18:40:38 2021 UTC
- タイムスタンプの更新: Last ACK received: Jan 29 18:40:37 2021 UTC

製品インスタンス開始型通信を使用した CSLU を介した CSSM への接続トポロジでは、次の RUM レポートを製品インスタンスがポリシーに基づいて CSSM に送信します。出力例では、次のフィールドにこの情報が示されています。



(注) レポートは、ポリシーまたはシステムメッセージに示されるまで、必要ありません。次のように、最初の同期後、更新されたポリシーはレポートが不要であることが示されます。

- Next report push: <none>
- Next ACK deadline: <none>

```
Device# show license status
```

```
Utility:
```

```
Status: DISABLED
```

```
Smart Licensing Using Policy:
```

```
Status: ENABLED
```

```
Data Privacy:
```

```
Sending Hostname: yes
```

```
Callhome hostname privacy: DISABLED
```

```
Smart Licensing hostname privacy: DISABLED
```

```
Version privacy: DISABLED
```

```
Transport:
```

```
Type: cslu
```

```
Cslu address: http://192.168.0.1:8182/cslu/v1/pi
```

```
Proxy:
```

```
Not Configured
```

```
Policy:
```

```
Policy in use: Installed On Jan 29 18:40:38 2021 UTC
```

```
Policy name: SLP Policy
```

```
Reporting ACK required: yes (Customer Policy)
```

```
Unenforced/Non-Export Perpetual Attributes:
```

```
First report requirement (days): 25 (Customer Policy)
```

```
Reporting frequency (days): 25 (Customer Policy)
```

```
Report on change (days): 25 (Customer Policy)
```

```
Unenforced/Non-Export Subscription Attributes:
```

```
First report requirement (days): 15 (Customer Policy)
```

```
Reporting frequency (days): 15 (Customer Policy)
```

```
Report on change (days): 15 (Customer Policy)
```

```
Enforced (Perpetual/Subscription) License Attributes:
```

```
First report requirement (days): 0 (CISCO default)
```

```
Reporting frequency (days): 35 (Customer Policy)
```

```

Report on change (days): 35 (Customer Policy)
Export (Perpetual/Subscription) License Attributes:
  First report requirement (days): 0 (CISCO default)
  Reporting frequency (days): 30 (Customer Policy)
  Report on change (days): 30 (Customer Policy)

Miscellaneous:
  Custom Id: <empty>

Usage Reporting:
  Last ACK received: Jan 29 18:40:37 2021 UTC
  Next ACK deadline: <none>
  Reporting push interval: 0 (no reporting)
  Next ACK push check: <none>
  Next report push: <none>
  Last report push: Jan 29 18:36:38 2021 UTC
  Last report file write: <none>

Trust Code Installed: <none>
    
```

移行前と後の CSSM Web UI と CSLU UI

移行前の CSSM Web UI

<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。

該当するスマートアカウントとバーチャルアカウントで、[Inventory]>[Licenses]に移動して、使用可能なライセンスを表示します。

次のスクリーンショットに、アップグレード前に製品インスタンスでライセンスがどのように表示されるかを示します。

これらはスマートライセンスではないため、[Insufficient Licenses] と表示されます。同じ理由で、それらの数は負になります。

Virtual Account: **Eg-VA-01** 11 Major | 1 Minor

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

Available Actions ▾ | Manage License Tags | License Reservation... | Show License Transactions | Search by License

<input type="checkbox"/>	License	Billing	Purchased	In Use	Substitution	Balance	Alerts
<input checked="" type="checkbox"/>	ISR_4351_400M_Performance	Prepaid	0	1	-	-1	✖ Insufficient Licenses
<input checked="" type="checkbox"/>	ISR_4351_Application	Prepaid	0	1	-	-1	✖ Insufficient Licenses
<input checked="" type="checkbox"/>	ISR_4351_Security	Prepaid	0	1	-	-1	✖ Insufficient Licenses
<input checked="" type="checkbox"/>	ISR_4351_UnifiedCommunication	Prepaid	0	1	-	-1	✖ Insufficient Licenses

次に、[Product Instances] タブをクリックして、移行する製品インスタンスに関する情報を表示します。

例: Cisco ソフトウェアライセンス (RTU ライセンス) から Smart Licensing Using Policy へ

Virtual Account: **Eg-VA-01** 11 Major | 1 Minor

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

Authorize License-Enforced Features... Search by Device or by Product Type

Name	Product Type	Last Contact	Alerts	Action
UDI_PID:C8500L-8S4X; UDI_SN:JAD2331191E;	CAT8500	2021-Jan-29 09:34:26		Action
UDI_PID:ISR4351/K9; UDI_SN:FDO210305DQ;	4300ISR	2021-Jan-29 18:28:30		Action

Showing All 2

移行後の CSLU UI

CSLU UI で、[Inventory] タブをクリックして [Product Instances] テーブルを表示します。

移行された製品インスタンス（この例では ISR4351/K9:FDO210305DQ）の [Alerts] 列を参照してください。成功した DLC 変換に関する情報がここに表示されます。次のスクリーンショットを参照してください。

CSLU Product Instances Edit Help

Inventory | Preferences

Product Instances

Add Single Product | Actions for Selected... | Refresh Product Instance List

<input type="checkbox"/>	Name	Last Contact	Alerts
<input type="checkbox"/>	UDI_PID:ISR4331/K9; UDI_SN:FDO224917G6	28-Jan-2021 15:36	COMPLETE: DLC acknowledgement to product instance
<input type="checkbox"/>	UDI_PID:C8500L-8S4X; UDI_SN:JAD2331191E	29-Jan-2021 16:34	COMPLETE: Acknowledgement received from CSSM
<input type="checkbox"/>	UDI_PID:ISR4351/K9; UDI_SN:FDO210305DQ	30-Jan-2021 02:09	COMPLETE: DLC acknowledgement received from CSSM

Items per page: 5 | 1 - 3 of 3

[Name] 列の製品インスタンスをクリックすると、製品インスタンスのライセンス使用状況の詳細が表示されます。次のスクリーンショットを参照してください。

UDI_PID:ISR4351/K9; UDI_SN:FDO210305DQ;

Device Details

Device Identifiers: ISR4351/K9 (UDI PID), FDO210305DQ (UDI Serial Number)
 Virtual Account: Eg-VA-01

Conversion Status

Conversion initiated 2021-Jan-29 19:11:29 by System

SKU	Product Family	Quantity	Type	Conversion Status	Smart License
RTU	-	1	Perpetual	Converted	ISR_4351_400M_Pe
RTU	-	1	Perpetual	Converted	ISR_4351_Applicati
RTU	-	1	Perpetual	Converted	ISR_4351_UnifiedC
RTU	-	1	Perpetual	Converted	ISR_4351_Security

また、<https://software.cisco.com> で CSSM Web UI にログインし、[Smart Software Licensing] をクリックして、CSSM Web UI でこれを確認することもできます。該当するスマートアカウントで、[Convert to Smart Licensing] > [Conversion History] に移動して、変換ステータスを確認します。成功した DLC は [Conversion Status] 列に反映されます。

Smart Licensing Using Policy をサポートする SSM オンプレミスのバージョンへの移行

必要な最小バージョンよりも前の SSM オンプレミスのバージョンを使用している場合（[SSM オンプレミス \(9 ページ\)](#) を参照）、SSM オンプレミスのバージョン、製品インスタンスを更新するために従う必要があるプロセスや手順、および他のタスク（SLAC のインストールなど）の概要としてこの項を使用できます（該当する場合）。

1. SSM オンプレミスをアップグレードします。

必要な最小バージョンであるバージョン 8、リリース 202102 以降にアップグレードします。

『[Cisco Smart Software Manager On-Prem Migration Guide](#)』を参照してください。

2. CSSM で SLAC を生成し、SSM オンプレミスにインポートします（該当する場合のみ）。

スループットが 250 Mbps を超える CSR 1000v または ISRv を使用している場合、Smart Licensing Using Policy 環境に HSECK9 ライセンスが必要になります（米国の輸出管理規制により、250 Mbps を超えるスループットを許可するための輸出規制フラグは使用できなくなりました）。

製品インスタンスをアップグレードする前に、この手順を完了してください。[承認コード要求の送信 \(SSM オンプレミス UI、切断モード\) \(205 ページ\)](#)

3. 製品インスタンスをアップグレードします。

必要な最小ソフトウェアバージョンについては、[SSM オンプレミス \(9 ページ\)](#) を参照してください。

アップグレード手順については、[ソフトウェアバージョンのアップグレード \(74 ページ\)](#) を参照してください。

4. CSSM へのローカルアカウントの再登録

オンラインとオフラインのオプションを使用できます。『[Cisco Smart Software Manager On-Prem Migration Guide](#)』[英語]の「[Re-Registering a local Account \(Online Mode\)](#)」または「[Manually Re-Registering a Local Account \(Offline Mode\)](#)」を参照してください。

再登録が完了すると、次のイベントが自動的に発生します。

- SSM オンプレミスは、SSM オンプレミスのテナントを指す新しいトランスポート URL で応答します。
- 製品インスタンスのトランスポートタイプ設定が **call-home** または **smart** から **cslu** に変更されます。トランスポート URL も自動的に更新されます。

5. 該当する製品インスタンスに SLAC を要求してインストールします ([SLAC の手動要求と自動インストール \(216 ページ\)](#))。

製品インスタンスに対してステップ2を実行した場合は、このステップを完了し、SLAC を要求して製品インスタンスにインストールする必要があります (HSECK9 ライセンスの場合)。

6. 特権 EXEC モードで **copy running-config startup-config** コマンドを入力して、製品インスタンスの設定変更を保存します。
7. 製品インスタンスの古いオンプレミススマートライセンス証明書をクリアし、製品インスタンスをリロードします。この後は設定変更を保存しないでください。



- (注) この手順は、製品インスタンスで実行されているソフトウェアバージョンが Cisco IOS XE Amsterdam 17.3.x または Cisco IOS XE Bengaluru 17.4.x の場合にのみ必要です。

特権 EXEC モードで **licence smart factory reset** コマンドと **reload** コマンドを入力します。

```
Device# licence smart factory reset
Device# reload
```

8. Device-Led Conversion (DLC) を適用する場合は、DLC データ収集が完了するまで 1 時間待ちます。

製品インスタンスのアップグレード前に、製品インスタンスが Right-To-Use (RTU) ライセンスまたは製品認証キー (PAK) ライセンスを使用していた場合は、1 時間待つことから次の手順に進みます。1 時間待つことで、最初の使用状況レポートとして DLC データを送信できます。待たない場合は、手順 9 と 10 を繰り返す必要があります。

製品インスタンスのアップグレード前に製品インスタンスがPAKライセンスまたはRTUライセンスを使用していなかった場合は、この手順をスキップして次の手順に進みます。

9. 使用状況の同期を実行します。
 1. 製品インスタンスに特権 EXEC モードで **license smart sync {all|local}** コマンドを入力します。これにより、SSM オンプレミスと製品インスタンスが同期され、保留中のデータが送受信されます。

```
Device(config)# license smart sync local
```

これは、SSM オンプレミス UI で確認できます。[Inventory] > [SL Using Policy] に移動します。[Alerts] 列に、「Usage report from product instance」というメッセージが表示されます。

2. 使用状況情報を CSSM と同期します (いずれかを選択)。

- オプション 1 :

SSM オンプレミスが CSSM に接続されている場合 : SSM オンプレミス UI の [Smart Licensing] ワークスペースで、[Reports] > [Usage Schedules] > [Synchronize now with Cisco] に移動します。

- オプション 2 :

SSM オンプレミスが CSSM に接続されていません。 [使用状況データのエクスポートとインポート \(SSM オンプレミス UI\) \(206 ページ\)](#) を参照してください。

CSSM と使用状況を同期した後、デバイスが SSM オンプレミスから ACK を受信するまで数分間待ちます。製品インスタンスが ACK を受信した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、出力で [Last ACK received] フィールドの日付を確認します。

10. 手順 8 で DLC を適用した場合は、DLC の完了を確認し、ローカルアカウントを同期します。

1. DLC の完了を確認します。

SSM オンプレミス UI で、[On-Prem Admin Workspace] に移動し、[Support Center] ウィジェットをクリックします。[Event Log] タブで、[DLC request sent to CSSM] と [DLC acknowledgement received from CSSM] を探します。

製品インスタンスで **show license all** 特権 EXEC コマンドを入力し、出力の [License Conversion] セクションのタイムスタンプを確認します。

```
Device# show license all
Smart Licensing Status
=====

Smart Licensing is ENABLED

License Conversion:
Automatic Conversion Enabled: False
Status: Successful on Aug 11 05:42:21 2021 UTC
```

<output truncated>

製品インスタンスで、**show platform software license dlc** 特権 EXEC コマンドを入力し、[DLC Process Status] フィールドと [DLC Conversion Status] フィールドを確認します。[Completed] と [SUCCESS] がそれぞれ表示されている必要があります。



- (注) DLC が適用可能であり、使用状況の同期のまで 1 時間待たなかった場合は、DLC データは RUM レポートに含まれていないため、次の出力にはステータス「Completed」が表示されていません。このステータスを表示するには、手順 9 と 10 を繰り返す必要があります。

```
Device# show platform software license dlc
Index 1 Feature:          appxk9
Permanent License:      1
EVAL RTU License:       0
RTU License:            0
Paper License:          0
Index 2 Feature:          securityk9
Permanent License:      1
EVAL RTU License:       0
RTU License:            0
Paper License:          0
Index 3 Feature:          hseck9
Permanent License:      1
EVAL RTU License:       0
RTU License:            0
Paper License:          0
```

DLC Process Status: Completed

DLC Conversion Status: SUCCESS

- SSM オンプレミスの [Synchronization] ウィジェットを使用して、SSM オンプレミスのローカルアカウントと CSSM を同期します。

結果：

移行、使用状況の最初の同期、および DLC（該当する場合）を完了しました。製品インスタンスとライセンス使用状況情報が SSM オンプレミスに表示されるようになりました。

後続のレポートには、次のオプションが含まれています。

- 製品インスタンスと SSM オンプレミスとの間でデータを同期するには、次の手順を実行します。
 - レポート間隔を設定して、製品スタンスと SSM オンプレミスとの間の定期的な同期をスケジュールします。グローバル コンフィギュレーション モードで **license smart usage interval interval_in_days** コマンドを入力します。

製品インスタンスが次にいつ RUM レポートを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、出力の [Next report push:] フィールドを確認します。

- 製品インスタンスと SSM オンプレミスとの間でアドホックまたはオンデマンドの同期を行うには、**license smart sync** 特権 EXEC コマンドを入力します。
- 使用状況情報を CSSM と同期するには、次の手順を実行します。
 - CSSM との定期的な同期をスケジュールします。SSM オンプレミス UI で、[Reports] > [Usage Schedules] > [Synchronization schedule with Cisco] に移動します。次の頻度情報を入力し、保存します。
 - [Days] : 同期が実行される頻度を示します。たとえば、2 を入力すると、同期は 2 日に 1 回行われます。
 - [Time of Day] : 24 時間表記法で、同期が実行される時刻を示します。たとえば、14 hours と 0 minutes を入力すると、ローカルタイムゾーンの午後 2 時 (1400) に同期が行われます。
 - レポートに必要なファイルのアップロードとダウンロードを実行します (使用状況データのエクスポートとインポート (SSM オンプレミス UI) (206 ページ))。



第 5 章

ポリシーを使用したスマートライセンスिंग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ス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スングの設定方法：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 \(CSLU インターフェイス\) \(176 ページ\)](#)
- [スマートアカウントとバーチャルアカウントの設定 \(CSLU インターフェイス\) \(177 ページ\)](#)
- [CSLU での製品開始型製品インスタンスの追加 \(CSLU インターフェイス\) \(177 ページ\)](#)
- [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 \(178 ページ\)](#)
- [CSLU での CSLU 開始型製品インスタンスの追加 \(CSLU インターフェイス\) \(180 ページ\)](#)
- [使用状況レポートの収集：CSLU 開始 \(CSLU インターフェイス\) \(180 ページ\)](#)
- [CSLU 開始型通信のネットワーク到達可能性の確認 \(182 ページ\)](#)
- [CSSM へのエクスポート \(CSLU インターフェイス\) \(186 ページ\)](#)
- [CSSM からのインポート \(CSLU インターフェイス\) \(187 ページ\)](#)
- [複数の製品インスタンスの SLAC の要求 \(CSLU インターフェイス\) \(188 ページ\)](#)
- [CSSM への接続の設定 \(189 ページ\)](#)
- [HTTPS プロキシを介したスマート転送の設定 \(192 ページ\)](#)
- [ダイレクトクラウドアクセス用の Call Home サービスの設定 \(194 ページ\)](#)
- [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 \(197 ページ\)](#)
- [スマートアカウントとバーチャルアカウントの割り当て \(SSM オンプレミス UI\) \(198 ページ\)](#)
- [デバイスの検証 \(SSM オンプレミス UI\) \(199 ページ\)](#)
- [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 \(200 ページ\)](#)
- [トランスポート URL の取得 \(SSM オンプレミス UI\) \(203 ページ\)](#)

- 承認コード要求の送信 (SSM オンプレミス UI、接続モード) (203 ページ)
- 承認コード要求の送信 (SSM オンプレミス UI、切断モード) (205 ページ)
- 使用状況データのエクスポートとインポート (SSM オンプレミス UI) (206 ページ)
- 1 つ以上の製品インスタンスの追加 (SSM オンプレミス UI) (207 ページ)
- SSM オンプレミス開始型通信のネットワーク到達可能性の確保 (209 ページ)
- CSSM からの SLAC の生成とファイルへのダウンロード (214 ページ)
- SLAC の手動要求と自動インストール (216 ページ)
- 製品インスタンスでの SLAC 要求の生成と保存 (219 ページ)
- 承認コードの削除と返却 (220 ページ)
- CSSM でのリターンコードの入力と製品インスタンスの削除 (226 ページ)
- CSSM からの信頼コード用新規トークンの生成 (227 ページ)
- ID トークンによる信頼の確立 (227 ページ)
- CSSM からのポリシーファイルのダウンロード (229 ページ)
- CSSM へのデータまたは要求のアップロードとファイルのダウンロード (229 ページ)
- 製品インスタンスへのファイルのインストール (231 ページ)
- 転送タイプ、URL、およびレポート間隔の設定 (232 ページ)
- ユーティリティモードの有効化 (236 ページ)
- PAK ライセンスの使用を継続する (238 ページ)
- PAK ライセンスの削除 (240 ページ)
- 障害が発生した製品インスタンスの PAK ライセンスの削除 (242 ページ)
- PLR のアクティブ化 (242 ページ)
- PLR のアップグレード (248 ページ)
- PLR の非アクティブ化 (251 ページ)
- リソース使用率測定レポートの例 (253 ページ)
- 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 (253 ページ)

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。システムに接続するためのスマートアカウントとバーチャルアカウントの両方を設定するには、次の手順を実行します。

手順

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

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

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

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

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

(注) SA/VA 名では大文字と小文字が区別されます。

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

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

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

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

手順

ステップ 1 [Preferences] タブを選択します。

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

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

製品インスタンス開始型通信のネットワーク到達可能性の確認

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

始める前に

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

手順

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

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

	コマンドまたはアクション	目的
ステップ 13	ip domain name <i>domain-name</i> 例 : Device(config)# ip domain name example.com	ドメインの DNS ディスカバリを設定します。この例では、ネームサーバはエントリ <code>cslu-local.example.com</code> を作成します。

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

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



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

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

手順

- ステップ 1 [Inventory] タブに移動し、[Product Instances] テーブルから [Add Single Product] を選択します。
- ステップ 2 [Host] に入力します (ホストの IP アドレス)。
- ステップ 3 [Connect Method] を選択し、CSLU 開始の接続方法を 1 つを選択します。
- ステップ 4 右側のパネルで、[Product Instance Login Credentials] をクリックします。画面の左側のパネルが変化して [User Name] フィールドと [Password] フィールドに変わります。
- ステップ 5 製品インスタンスの [User Name] と [Password] を入力します。
- ステップ 6 [保存 (Save)] をクリックします。

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

使用状況レポートの収集 : CSLU 開始 (CSLU インターフェイス)

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

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

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

手順

- ステップ 1** [Preferences] タブをクリックし、有効な [Smart Account] と [Virtual Account] を入力して、適切な CSLU 開始型収集メソッドを選択します。 ([Preferences] に変更があった場合は、[Save] をクリックします)。
- ステップ 2** [Inventory] タブをクリックし、1 つまたは複数の製品インスタンスを選択します。
- ステップ 3** [Actions for Selected] > [Collect Usage] をクリックします。

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

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

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

この時点で、使用状況レポートがローカルディレクトリ (ライブラリ) に保存されます。使用状況レポートをシスコにアップロードするには、[CSSM へのデータまたは要求のアップロードとファイルのダウンロード \(229 ページ\)](#) の手順に従ってください。

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

CSLU 開始型通信のネットワーク到達可能性の確認

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

始める前に

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

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。プロンプトが表示されたらパスワードを入力します。
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	aaa new model 例： Device(config)# aaa new model	(必須) 認証、許可、アカウントिंग (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：	(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。

	コマンドまたはアクション	目的
	<pre>Device(config)# ip name-server vrf Mgmt-vrf 192.168.1.100 192.168.1.200 192.168.1.300</pre>	<p>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。</p>
ステップ 8	<p>ip domain lookup source-interface interface-type-number</p> <p>例 :</p> <pre>Device(config)# ip domain lookup source-interface gigabitethernet0/0</pre>	<p>デバイス上で、DNSに基づくホスト名からアドレスへの変換を有効にします。この機能は、デフォルトでイネーブルにされています。</p> <p>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。</p>
ステップ 9	<p>ip domain name name</p> <p>例 :</p> <pre>Device(config)# ip domain name vrf Mgmt-vrf cisco.com</pre>	<p>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。</p>
ステップ 10	<p>no username name</p> <p>例 :</p> <pre>Device(config)# no username admin</pre>	<p>(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。</p> <p>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。</p>

	コマンドまたはアクション	目的
ステップ 11	<p>username name privilege level password password</p> <p>例 :</p> <pre>Device(config)# username admin privilege 15 password 0 lab</pre>	<p>(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。</p> <p>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。</p> <p>password を使用すると、name 引数にアクセスできます。パスワードは 1 ~ 25 文字で、埋め込みスペースを使用でき、username コマンドの最後のオプションとして指定します。</p> <p>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。</p> <p>(注) このユーザ名とパスワードを CSLU で入力します (使用状況レポートの収集: CSLU 開始 (CSLU インターフェイス) (180 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。</p>
ステップ 12	<p>interface interface-type-number</p> <p>例 :</p> <pre>Device (config)# interface gigabitethernet0/0</pre>	<p>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。</p>
ステップ 13	<p>vrf forwarding vrf-name</p> <p>例 :</p> <pre>Device(config-if)# vrf forwarding Mgmt-vrf</pre>	<p>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。</p>
ステップ 14	<p>ip address ip-address mask</p> <p>例 :</p> <pre>Device(config-if)# ip address 192.168.0.1 255.255.0.0</pre>	<p>VRF の IP アドレスを定義します。</p>

	コマンドまたはアクション	目的
ステップ 15	negotiation auto 例： Device(config-if)# negotiation auto	インターフェイスの速度およびデュプレックスパラメータの自動ネゴシエーション動作を有効にします。
ステップ 16	no shutdown 例： Device(config-if)# no shutdown	無効にされたインターフェイスを再起動します。
ステップ 17	end 例： Device(config-if)# end	インターフェイス コンフィギュレーションモードを終了し、グローバルコンフィギュレーションモードを開始します。
ステップ 18	ip http server 例： Device(config)# ip http server	(必須) シスコの Web ブラウザユーザインターフェイスを含む IP または IPv6 システムで HTTP サーバを有効にします。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。

	コマンドまたはアクション	目的
ステップ 23	ip route ip-address ip-mask subnet mask 例 : Device(config)# ip route vrf mgmt-vrf 192.168.0.1 255.255.0.0 192.168.255.1	製品インスタンスにルートとゲートウェイを設定します。スタティックルートまたはダイナミックルートのいずれかを設定できます。
ステップ 24	logging host 例 : Device(config)# logging host 172.25.33.20 vrf Mgmt-vrf	リモートホストへのシステムメッセージおよびデバッグ出力を記録します。
ステップ 25	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	<p>(必須) HTTP 接続を確認します。出力で、<code>SL_HTTP</code> 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。</p> <ul style="list-style-type: none"> • 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、<code>https://<product-instance-ip>/</code> を確認します。これにより、CSLU から製品インスタンスへの REST API が期待どおりに動作することが保証されます。

CSSM へのエクスポート (CSLU インターフェイス)

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

手順

- ステップ 1** [Preferences] タブに移動し、[Cisco Connectivity] トグルスイッチをオフにします。
フィールドが「Cisco Is Not Available」に切り替わります。
- ステップ 2** ホーム画面から、[Data] > [Export to CSSM] の順に移動します。
- ステップ 3** 開いたウィンドウからファイルを選択し、[Save] をクリックします。これでファイルが保存されました。
(注) この時点で、DLC ファイル、RUM ファイル、またはその両方があります。
- ステップ 4** シスコに接続できるワークステーションから、次の手順を実行します：[CSSM へのデータまたは要求のアップロードとファイルのダウンロード \(229 ページ\)](#)
ファイルがダウンロードされたら、CSLU にインポートできます。「[CSSM からのインポート \(CSLU インターフェイス\) \(187 ページ\)](#)」を参照してください。
-

CSSM からのインポート (CSLU インターフェイス)

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

手順

- ステップ 1** CSLU にアクセス可能な場所にファイルがダウンロードされていることを確認します。
- ステップ 2** CSU のホーム画面から、[Data] > [Import from CSSM] の順に移動します。
- ステップ 3** [Import from CSSM] モーダルが開き、次のいずれかを実行できます。
- ローカルドライブにあるファイルをドラッグアンドドロップします。または、
 - 適切な *.xml ファイルを参照し、ファイルを選択して [Open] をクリックします。
- アップロードが成功すると、ファイルがサーバーに正常に送信されたことを示すメッセージが表示されます。アップロードが成功しない場合は、インポートエラーが発生します。
- ステップ 4** アップロードが完了したら、ウィンドウの右上隅にある [x] をクリックして閉じます。
-

複数の製品インスタンスの SLAC の要求 (CSLU インターフェイス)

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

始める前に

サポートされるトポロジ:

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

手順

-
- ステップ 1** [Product Instances] テーブルから、承認コード要求の対象となる製品インスタンスを選択します。
- ステップ 2** 1つ以上の製品インスタンスを選択した状態で、[Available Actions] メニューから [Authorization Code Request] オプションを選択します。
- ステップ 3** 実行するステップを説明するウィンドウで、[Accept] をクリックします。
アップロードする CSV ファイルを選択するアップロードウィンドウが開きます。(ローカル)
- ステップ 4** 次に、ウィンドウでも説明されている次の手順を実行します。
- a) ディレクトリパス software.cisco.com > [Smart Software Licensing] > [Inventory] > [Product Instances] > [Authorize License Enforced Features] に移動して、ファイルをシスコにアップロードします。
 - b) 画面に表示される手順を実行します。
 1. [Multiple Product Instances] を選択します。
複数の製品インスタンスの場合は、[Choose File] をクリックしてアップロードするか、または今後のアップロード用に **テンプレートをダウンロード** できます (csv ファイルテンプレート)。
 2. 次のパネルで、**ライセンス** を選択します。
 3. ライセンスの選択をレビューして確認します
 4. ダウンロードする承認コードを作成します
 - c) ファイルと選択したライセンスがシスコにアップロードされたら、(ファイルとして) 選択した製品インスタンスの **承認コード** をダウンロードして CSLU に戻します。
- ステップ 5** [Upload From Cisco (in the CSLU interface)] を選択します。

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

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

CSSM への接続の設定

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

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。プロンプトが表示されたらパスワードを入力します。
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーションモードを開始します。
ステップ 3	{ ip ipv6 } name-server <i>server-address 1</i> ... <i>server-address 6</i> 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 <i>server-address 1</i> ... <i>server-address 6</i> 例： Device(config)# ip name-server vrf SLP_VRF	(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。

	コマンドまたはアクション	目的
	<pre>209.165.201.1 209.165.200.225 209.165.201.14 209.165.200.230</pre>	(注) このコマンドは、 ip name-server コマンドの代わりです。
ステップ 5	license smart vrf <i>vrf_string</i> 例： <pre>Device(config)# Device(config)# license smart vrf SLP_VRF</pre>	<p>製品インスタンスで使用される VRF 名を設定します。製品インスタンスは VRF を使用して、ライセンス関連のデータを CSSM、CSLU、または SSM オンプレミスに送信します。</p> <p>製品インスタンスが VRF をサポートするインスタンスであり、対応する URL を使用してトランスポートタイプが smart または slu に設定されていることを確認します。</p>
ステップ 6	ip domain lookup source-interface <i>interface-type interface-number</i> 例： <pre>Device(config)# ip domain lookup source-interface Vlan100</pre>	DNS ドメインルックアップ用のソースインターフェイスを設定します。
ステップ 7	ip domain name <i>domain-name</i> 例： <pre>Device(config)# ip domain name example.com</pre>	ドメイン名を設定します。
ステップ 8	ip host tools.cisco.com <i>ip-address</i> 例： <pre>Device(config)# ip host tools.cisco.com 209.165.201.30</pre>	自動 DNS マッピングが使用できない場合は、DNS ホスト名キャッシュ内のホスト名/アドレス静的マッピングを設定します。
ステップ 9	interface <i>interface-type-number</i> 例： <pre>Device(config)# interface Vlan100 Device(config-if)# ip address 192.0.2.10 255.255.255.0 Device(config-if)# exit</pre>	レイヤ 3 インターフェイスを設定します。インターフェイスのタイプと番号、または VLAN を入力します。
ステップ 10	ntp server <i>ip-address</i> [version number] [key key-id] [prefer] 例： <pre>Device(config)# ntp server 198.51.100.100 version 2 prefer</pre>	(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。

	コマンドまたはアクション	目的
		<p>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。</p> <p>ヒント この設定が完了したら、show license tech を使用してクロックが実際に同期されているかどうかを確認します。正常に同期されると、[Clock sync-ed with NTP] フィールドが [True] に設定されます。同期されていない場合、このフィールドは [False] に設定されます。</p> <p>クロックが同期されていない場合、信頼の確立時や SLAC の要求時などの試行は show license tech の出力に反映されません。次に例を示します。</p> <pre>Trust Establishment: Attempts: Total=0, Success=0, Fail=0 Ongoing Failure: Overall=0 Communication=0</pre>
<p>ステップ 11</p>	<p>switchport access vlan <i>vlan_id</i></p> <p>例 :</p> <pre>Device(config)# interface GigabitEthernet1/0/1 Device(config-if)# switchport access vlan 100</pre>	<p>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。</p>

	コマンドまたはアクション	目的
	<pre>Device(config-if)# switchport mode access Device(config-if)# exit OR Device(config)#</pre>	<p>(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。</p>
ステップ 12	<pre>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</pre>	<p>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。</p>
ステップ 13	<pre>ip http client source-interface interface-type-number 例 : Device(config)# ip http client source-interface Vlan100</pre>	<p>(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。</p>
ステップ 14	<pre>exit 例 : Device(config)# exit</pre>	<p>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。</p>
ステップ 15	<pre>copy running-config startup-config 例 : Device# copy running-config startup-config</pre>	<p>コンフィギュレーションファイルに設定を保存します。</p>

HTTPS プロキシを介したスマート転送の設定

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



(注) 認証された HTTPS プロキシ設定はサポートされていません。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例 : Device> enable	特権 EXEC モードを有効にします。プロンプトが表示されたらパスワードを入力します。
ステップ 2	configure terminal 例 : Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	license smart transport smart 例 : Device (config)# license smart transport smart	スマート転送モードを有効にします。
ステップ 4	license smart url default 例 : Device (config)# license smart transport default	スマート URL を自動的に設定します (https://smartreceiver.cisco.com/licservice/license)。このオプションを想定どおりに動作させるには、前の手順の転送モードを smart に設定する必要があります。
ステップ 5	license smart proxy {address address_hostname port port_num} 例 : Device (config)# license smart proxy address 192.168.0.1 Device (config)# license smart proxy port 3128	スマート転送モードのプロキシを設定します。プロキシが設定されている場合、ライセンスメッセージは最終宛先 URL (CSSM) に加えてプロキシにも送信されます。プロキシはメッセージを CSSM に送信します。プロキシ IP アドレスとポート情報を個別に設定します。 <ul style="list-style-type: none"> • address address_hostname : プロキシアドレスを指定します。プロキシサーバーの IP アドレスまたはホスト名を入力します。 • port port_num : プロキシポートを指定します。プロキシポート番号を入力します。 Cisco IOS XE Bengaluru 17.6.1 以降、プロキシサーバーの受け入れ基準が変更されたことに注意してください。プロキシサーバーの応答のステータスコードのみがシステムによって検証され、理由フレーズは検証されません。RFC 形式は、 status-line = HTTP-version SP status-code SP reason-phrase CRLF で

	コマンドまたはアクション	目的
		す。ステータス行の詳細については、 RFC 7230 のセクション 3.1.2 を参照してください。
ステップ 6	exit 例： Device(config)# exit	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 7	copy running-config startup-config 例： Device# copy running-config startup-config	コンフィギュレーション ファイルに設定を保存します。

ダイレクトクラウドアクセス用の Call Home サービスの設定

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



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

手順

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

	コマンドまたはアクション	目的
ステップ 4	license smart url <i>url</i> 例 : Device (config) # license smart url https://tools.cisco.com/its/service/cthe/services/DCEService	callhome 転送モードの場合は、例に示すように CSSM URL を設定します。
ステップ 5	service call-home 例 : Device (config) # service call-home	Call Home 機能をイネーブルにします。
ステップ 6	call-home 例 : Device (config) # call-home	Call Home コンフィギュレーションモードを開始します。
ステップ 7	contact-email-address <i>email-address</i> 例 : Device (config-call-home) # contact-email-addr username@example.com	お客様の電子メールアドレスを割り当て、Smart Call Home サービスのフルレポート機能を有効にし、フルインベントリメッセージを Call Home TAC プロファイルから Smart Call Home サーバに送信してフル登録プロセスを開始します。電子メールアドレスフォーマットには、スペースなしで最大 200 文字まで入力できます。
ステップ 8	profile <i>name</i> 例 : Device (config-call-home) # profile CiscoTAC-1 Device (config-call-home-profile) #	指定された宛先プロファイルに対する Call Home 宛先プロファイル設定サブモードに入ります。 デフォルトは次のとおりです。 <ul style="list-style-type: none"> • CiscoTAC-1 プロファイルは非アクティブです。このプロファイルを Call Home サービスで使用するには、プロファイルを有効にする必要があります。 • CiscoTAC-1 プロファイルは、プロファイルに登録されているすべてのイベントタイプが記載された完全なレポートを送信します。または、 Device (cfg-call-home-profile) # anonymous-reporting-only anonymous-reporting-only を追加で設定します。これが設定されている場合は、クラッシュ、インベン

	コマンドまたはアクション	目的
		<p>トリ、およびテストメッセージのみが送信されます。</p> <p>プロファイルのステータスを確認するには、show call-home profile all コマンドを使用します。</p>
ステップ 9	<p>active</p> <p>例 :</p> <pre>Device(config-call-home-profile)# active</pre>	宛先プロファイルをイネーブルにします。
ステップ 10	<p>destination transport-method http {email http}</p> <p>例 :</p> <pre>Device(config-call-home-profile)# destination transport-method http AND Device(config-call-home-profile)# no destination transport-method email</pre>	<p>メッセージの転送形式をイネーブルにします。この例では、HTTP 経由で Call Home サービスが有効になり、電子メールによる転送が無効になります。</p> <p>このコマンドの no 形式を使用すると、メソッドが無効になります。</p>
ステップ 11	<p>destination address { email email_address http url }</p> <p>例 :</p> <pre>Device(config-call-home-profile)# destination address http https://tools.cisco.com/its/service/odte/services/DESservice AND Device(config-call-home-profile)# no destination address http https://tools.cisco.com/its/service/odte/services/DESservice</pre>	<p>Call Home メッセージを送信する宛先 E メールアドレスまたは URL を設定します。宛先 URL を入力する場合は、サーバがセキュアサーバであるかどうかに応じて http:// (デフォルト) または https:// を指定します。</p> <p>ここに示す例では、http:// の形式で宛先 URL が設定されています。コマンドの no 形式では https:// に設定されます。</p>
ステップ 12	<p>exit</p> <p>例 :</p> <pre>Device(config-call-home-profile)# exit</pre>	Call Home 宛先プロファイル コンフィギュレーションモードを終了して、Call Home コンフィギュレーションモードに戻ります。
ステップ 13	<p>exit</p> <p>例 :</p> <pre>Device(config-call-home)# end</pre>	Call Home コンフィギュレーションモードを終了して、特権 EXEC モードに戻ります。
ステップ 14	<p>copy running-config startup-config</p> <p>例 :</p> <pre>Device# copy running-config startup-config</pre>	コンフィギュレーションファイルに設定を保存します。

	コマンドまたはアクション	目的
ステップ 15	show call-home profile { <i>name</i> all}	指定されたプロファイル、または設定済みのすべてのプロファイルに関する宛先プロファイル設定を表示します。

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

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



(注) 認証された HTTPS プロキシ設定はサポートされていません。

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



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

手順

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

	コマンドまたはアクション	目的
ステップ 5	call-home 例： Device (config) # call-home	Call Home コンフィギュレーションモードを開始します。
ステップ 6	http-proxy proxy-address proxy-port port-number 例： Device (config-call-home) # http-proxy 198.51.100.10 port 5000	Call Home サービスへのプロキシサーバ情報を設定します。 Cisco IOS XE Bengaluru 17.6.1 以降、プロキシサーバの受け入れ基準が変更されたことに注意してください。プロキシサーバの応答のステータスコードのみがシステムによって検証され、理由フレーズは検証されません。RFC形式は、 status-line = HTTP-version SP status-code SP reason-phrase CRLF です。ステータス行の詳細については、 RFC 7230 のセクション 3.1.2 を参照してください。
ステップ 7	exit 例： Device (config-call-home) # exit	Call Home コンフィギュレーションモードを終了し、グローバル コンフィギュレーションモードを開始します。
ステップ 8	exit 例： Device (config) # exit	グローバル コンフィギュレーションモードを終了し、特権 EXEC モードを開始します。
ステップ 9	copy running-config startup-config 例： Device# copy running-config startup-config	コンフィギュレーションファイルに設定を保存します。

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

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

始める前に

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

手順

-
- ステップ 1** SSM オンプレミスにログインし、[Smart Licensing] ワークスペースを選択します。
 - ステップ 2** [Inventory]>[SL Using Policy]>[Export/Import All]>[Import Product Instances List]に移動します。
[Upload Product Instances] ウィンドウが表示されます。
 - ステップ 3** [Download] をクリックして .csv テンプレートファイルをダウンロードし、テンプレート内のすべての製品インスタンスに必要な情報を入力します。
 - ステップ 4** テンプレートに入力したら、[Inventory]>[SL Using Policy]>[Export/Import All]>[Import Product Instances List] をクリックします。
[Upload Product Instances] ウィンドウが表示されます。
 - ステップ 5** [Browse] をクリックし、入力した .csv テンプレートをアップロードします。
アップロードしたすべての製品インスタンスのスマートアカウント情報とバーチャルアカウント情報が SSM オンプレミスで使用できるようになりました。
-

デバイスの検証 (SSM オンプレミス UI)

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

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

始める前に

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

手順

-
- ステップ 1** [On-Prem License Workspace] ウィンドウで、[Admin Workspace] をクリックし、プロンプトが表示されたらログインします。
[On-Prem Admin Workspace] ウィンドウが表示されます。
 - ステップ 2** [Settings] ウィジェットをクリックします。
[Settings] ウィンドウが表示されます。

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

不明な製品インスタンスからの RUM レポートが拒否されるようになりました。必要な製品インスタンスを SSM オンプレミスデータベースにまだ追加していない場合は、RUM レポートを送信する前に追加する必要があります。[スマートアカウントとバーチャルアカウントの割り当て \(SSM オンプレミス UI\) \(198 ページ\)](#) を参照してください

製品インスタンス開始型通信のネットワーク到達可能性の確認

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



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

始める前に

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

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例 : Device> enable	特権 EXEC モードを有効にします。プロンプトが表示されたらパスワードを入力します。
ステップ 2	configure terminal 例 : Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	interface interface-type-number 例 : Device (config)# interface gigabitethernet0/0	インターフェイス コンフィギュレーションモードを開始し、VRFに関連付けられたイーサネットインターフェイス、サブインターフェイス、または VLAN を指定します。

	コマンドまたはアクション	目的
ステップ 4	vrf forwarding <i>vrf-name</i> 例： Device(config-if)# vrf forwarding SLP_VRF	VRF をレイヤ 3 インターフェイスに対応付けます。このコマンドは、インターフェイスでマルチプロトコル VRF をアクティブにします。
ステップ 5	ip address <i>ip-address mask</i> 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 <i>interface-type-number</i> 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 <i>ip-address ip-mask subnet mask</i> 例： Device(config)# ip route vrf SLP_VRF 192.168.0.1 255.255.0.0 192.168.255.1	(必須) 製品インスタンスにルートとゲートウェイを設定します。スタティックルートまたはダイナミックルートのいずれかを設定できます。
ステップ 10	{ ip ipv6 } name-server <i>server-address 1</i> ... <i>server-address 6</i> 例： Device(config)# ip name-server vrf SLP_VRF 198.51.100.1	VRF インターフェイスでドメインネームシステム (DNS) を設定します。
ステップ 11	license smart vrf <i>vrf_string</i> 例： Device(config)# Device(config)# license smart vrf SLP_VRF	製品インスタンスで使用される VRF 名を設定します。製品インスタンスは VRF を使用して、ライセンス関連のデータを CSSM、CSLU、または SSM オンプレミスに送信します。 製品インスタンスが VRF をサポートするインスタンスであり、対応する URL

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

	コマンドまたはアクション	目的
	Device# <code>copy running-config startup-config</code>	

トランスポート URL の取得 (SSM オンプレミス UI)

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

始める前に

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

手順

- ステップ 1** SSM オンプレミスにログインし、[Smart Licensing] ワークスペースを選択します。
- ステップ 2** [Inventory] タブに移動し、ローカルバーチャルアカウントのドロップダウンリスト（右上隅）から、デフォルトのローカルバーチャルアカウントを選択します。この場合、[Inventory] タブの下領域に [Local Virtual Account: Default] が表示されます。
- ステップ 3** [General] タブに移動します。
[Product Instance Registration Tokens] 領域が表示されます。
- ステップ 4** [Product Instance Registration Tokens] 領域で、[CSLU Transport URL] をクリックします。
[Product Registration URL] ポップアップウィンドウが表示されます。
- ステップ 5** URL 全体をコピーし、アクセス可能な場所に保存します。
製品インスタンスでトランスポートタイプと URL を設定するときに、この URL が必要になります。
- ステップ 6** トランスポートタイプと URL を設定します。[転送タイプ、URL、およびレポート間隔の設定 \(232 ページ\)](#) を参照してください。

承認コード要求の送信 (SSM オンプレミス UI、接続モード)

この手順では、SSM オンプレミスが CSSM に接続されている場合に、輸出規制ライセンスおよび適用済みライセンスに SLAC をインストールする方法を示します。最初に、製品インスタンスから SSM オンプレミスに SLAC 要求を送信します。次に、SSM オンプレミスを CSSM と

同期する必要があります。CSSM が要求を処理し、応答が SSM オンプレミスに送り返されます。最後に、応答が SSM オンプレミスから製品インスタンスに送信され、SLAC がデバイスにインストールされます。

始める前に

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

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

手順

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

SLAC 要求が SSM オンプレミスに送信されます。

既存の SLAC に追加するのか置換するのかを指定します。

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

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

次のいずれかのオプションを入力して、デバイスを指定します。

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

ステップ 2 SSM オンプレミスにログインします。

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

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

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

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

承認コード要求の送信 (SSM オンプレミス UI、切断モード)

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

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

始める前に

サポートされているトポロジ：

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

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

手順

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

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

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

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

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

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

ステップ 5 CSSM で [CSSM へのデータまたは要求のアップロードとファイルのダウンロード \(229 ページ\)](#) のタスクを実行します。

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

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

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

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

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

ステップ 8 製品インスタンスでこのタスクを完了します。[SLACの手動要求と自動インストール \(216ページ\)](#)

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

使用状況データのエクスポートとインポート (SSM オンプレミス UI)

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

始める前に

サポートされているトポロジ:

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

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

手順

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

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

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

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

ステップ 4 CSSMでCSSMへのデータまたは要求のアップロードとファイルのダウンロード (229 ページ) のタスクを実行します。

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

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

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

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

1つ以上の製品インスタンスの追加 (SSM オンプレミス UI)

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

始める前に

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

手順

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

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

ステップ 3 [SL Using Policy] に移動します。

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

- 単一の製品インスタンスを追加するには、次の手順を実行します。

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

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

4. 右側のパネルで、[Product Instance Login Credentials] をクリックします。

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

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

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

これは、ネットワーク到達可能性を確立するために必要なコマンドの一部として設定したものと同一ユーザ ID とパスワードです ([SSM オンプレミス開始型通信のネットワーク到達可能性の確保 \(209 ページ\)](#))。

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

- 複数の製品インスタンスをインポートするには、次の手順を実行します。

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

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

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

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

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

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

ログインクレデンシャルは、ネットワーク到達可能性を確立するために必要なコマンドの一部として設定したユーザ ID とパスワードを参照します ([SSM オンプレミス開始型通信のネットワーク到達可能性の確保 \(209 ページ\)](#))。

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

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

5. 次に、入力した .csv テンプレートをアップロードします。

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

SSM オンプレミス開始型通信のネットワーク到達可能性の確保

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



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

始める前に

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

手順

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

	コマンドまたはアクション	目的
ステップ 6	ip routing 例 : Device(config)# ip routing	IP ルーティングを有効にします。
ステップ 7	{ip ipv6} name-server server-address 1 ...server-address 6] 例 : Device(config)# ip name-server vrf Mgmt-vrf 192.168.1.100 192.168.1.200 192.168.1.300	<p>(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。</p> <p>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。</p>
ステップ 8	ip domain lookup source-interface interface-type-number 例 : Device(config)# ip domain lookup source-interface gigabitethernet0/0	<p>デバイス上で、DNS に基づくホスト名からアドレスへの変換を有効にします。この機能は、デフォルトでイネーブルにされています。</p> <p>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。</p>
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	<p>(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。</p> <p>SSM オンプレミス開始型の RUM レポートを取得に REST API を使用する</p>

	コマンドまたはアクション	目的
		場合は、SSM オンプレミスにログインする必要があります。ユーザ名が重複していると、システムにそのユーザ名がある場合はこの機能が正しく動作しない場合があります。
ステップ 11	<p>username name privilege level password password</p> <p>例 :</p> <pre>Device(config)# username admin privilege 15 password 0 lab</pre>	<p>(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。</p> <p>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。</p> <p>password を使用すると、name 引数にアクセスできます。パスワードは 1 ~ 25 文字で、埋め込みスペースを使用でき、username コマンドの最後のオプションとして指定します。</p> <p>これにより、SSM オンプレミスが製品インスタンスのネイティブ REST を使用できるようになります。</p> <p>(注) このユーザ名とパスワードを SSM オンプレミスに入力します (1 つ以上の製品インスタンスの追加 (SSM オンプレミス UI) (207 ページ))。これにより、SSM オンプレミスは製品インスタンスから RUM レポートを収集できるようになります。</p>
ステップ 12	<p>interface interface-type-number</p> <p>例 :</p> <pre>Device (config)# interface gigabitethernet0/0</pre>	<p>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。</p>
ステップ 13	<p>vrf forwarding vrf-name</p> <p>例 :</p> <pre>Device (config-if)# vrf forwarding Mgmt-vrf</pre>	<p>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。</p>

	コマンドまたはアクション	目的
ステップ 14	ip address ip-address mask 例： Device(config-if)# ip address 192.168.0.1 255.255.0.0	VRF の IP アドレスを定義します。
ステップ 15	negotiation auto 例： Device(config-if)# negotiation auto	インターフェイスの速度およびデュプレックスパラメータの自動ネゴシエーション動作を有効にします。
ステップ 16	no shutdown 例： Device(config-if)# no shutdown	無効にされたインターフェイスを再起動します。
ステップ 17	end 例： Device(config-if)# end	インターフェイス コンフィギュレーションモードを終了し、グローバルコンフィギュレーションモードを開始します。
ステップ 18	ip http server 例： Device(config)# ip http server	(必須) シスコの Web ブラウザ ユーザ インターフェイスを含む IP または IPv6 システムで HTTP サーバを有効にします。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。

	コマンドまたはアクション	目的
ステップ 22	ip tftp source-interface <i>interface-type-number</i> 例 : Device(config)# ip tftp source-interface GigabitEthernet0/0	TFTP 接続用の送信元アドレスとして、インターフェイスの IP アドレスを指定します。
ステップ 23	ip route ip-address ip-mask subnet mask 例 : Device(config)# ip route vrf mgmt-vrf 192.168.0.1 255.255.0.0 192.168.255.1	製品インスタンスにルートとゲートウェイを設定します。スタティックルートまたはダイナミックルートのいずれかを設定できます。
ステップ 24	logging host 例 : Device(config)# logging host 172.25.33.20 vrf Mgmt-vrf	リモートホストへのシステムメッセージおよびデバッグ出力を記録します。
ステップ 25	crypto pki trustpoint SLA-TrustPoint 例 : Device(config)# crypto pki trustpoint SLA-TrustPoint Device(ca-trustpoint)#	(必須) 製品インスタンスがトランスポイント「SLA-TrustPoint」を使用する必要があることを宣言し、CA トランスポイント コンフィギュレーションモードを開始します。このコマンドを使用してトランスポイントを宣言するまで、製品インスタンスはトランスポイントを認識しません。
ステップ 26	enrollment terminal 例 : Device(ca-trustpoint)# enrollment terminal	(必須) 証明書登録方式を指定します。
ステップ 27	revocation-check none 例 : Device(ca-trustpoint)# revocation-check none	(必須) ピアの証明書が失効していないことを確認するために使用する方法を指定します。SSM オンプレミス展開トポロジの場合は、 none キーワードを入力します。つまり、失効チェックは実行されず、証明書は常に受け入れられます。
ステップ 28	end 例 : Device(ca-trustpoint)# exit Device(config)# end	CA トランスポイントコンフィギュレーションモードを終了し、次にグローバルコンフィギュレーションモードを終了してから、特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 29	show ip http server session-module 例： Device# show ip http server session-module	(必須) HTTP 接続を確認します。出力で、 <code>SL_HTTP</code> 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。 <ul style="list-style-type: none"> • SSM オンプレミスがインストールされているデバイスから、製品インスタンスに ping できることを確認します。ping が成功すると、製品インスタンスが到達可能であることが確認されます • SSM オンプレミスがインストールされているデバイスの Web ブラウザで、<code>https://<product-instance-ip>/</code> を確認します。これにより、SSM オンプレミスから製品インスタンスへの REST API が期待どおりに動作することが保証されます。
ステップ 30	copy running-config startup-config 例： Device# copy running-config startup-config	コンフィギュレーションファイルに設定を保存します。

CSSM からの SLAC の生成とファイルへのダウンロード

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

始める前に

サポートされるトポロジ：

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

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

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

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

手順

-
- ステップ 1** <https://software.cisco.com> で CSSM Web UI にログインし、[Manage licenses] をクリックします。シスコから提供されたユーザ名とパスワードを使用してログインします。[Smart Software Licensing] ページが表示されます。
- ステップ 2** [Inventory] タブをクリックします。
- ステップ 3** [Product Instances] タブをクリックします。
- ステップ 4** [Authorize License Enforced Features] タブをクリックします。
- ステップ 5** 単一の製品インスタンスまたは複数の製品インスタンスに SLAC を生成します（いずれかを選択）。
- 単一の製品インスタンスに SLAC を生成するには、次の手順を実行します。
 1. [PID] と [Serial Number] を入力します。

（注） 他のフィールドは入力しないでください。
 2. ライセンスを選択し、対応する [Reserve] 列に **1** を入力します。

PID に対して正しいライセンスを選択したことを確認します。参考情報については、[ルーティング製品インスタンスの HSECK9 ライセンスマッピングテーブル（253 ページ）](#) を参照してください。
 3. [Next] をクリックします。
 4. [承認コードを生成（Generate Authorization Code）] をクリックします。
 5. 承認コードをダウンロードし、.csv ファイルとして保存します。
 6. 製品インスタンスへのファイルのインストール「[製品インスタンスへのファイルのインストール（231 ページ）](#)」を参照してください。
 - 複数の製品インスタンスに SLAC を生成するには次の手順を実行します（この場合、.csv ファイルをアップロードします）。
 1. [Single Device]（デフォルト）というドロップダウンリストで、選択を [Multiple Devices] に変更します。
 2. [Browse] をクリックし、SLAC を必要とする製品インスタンスのリストを含む .csv ファイルに移動します。

3. アップロードすると、デバイスのリストが CSSM に表示されます。すべてのデバイスのチェックボックスが有効になったら（すべてのデバイスの SLAC を要求することを意味します） [Next] をクリックします。
4. 各製品インスタンスに必要なライセンス数を指定し、[Next] をクリックします。

（注） Smart Licensing Using Policy 環境で輸出規制ライセンスまたは適用済みのライセンスに SLAC を要求する場合は、製品インスタンスごとに必要な SLAC は 1 つのみです。
5. [Device Type] ドロップダウンリストから [DNA On-Prem] を選択し、[Continue] をクリックします。
6. [Reserve Licenses] をクリックします。

[Download Authorization Code] ボタンが表示されます。
7. [Download Authorization Codes] をクリックして、この .csv ファイルをダウンロードします。このファイルには、上記の手順 c. のすべての製品インスタンスの SLAC が含まれています。[閉じる (Close)] をクリックします。
8. これで、この .csv ファイルを SSM オンプレミスにインポートできるようになりました。承認コード要求の送信 (SSM オンプレミス UI、切断モード) (205 ページ) に戻り、残りの手順を実行してこのファイルをインポートします。

SLAC の手動要求と自動インストール

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

始める前に

サポートされるトポロジ:

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

続行する前に、次の点も確認してください。

- SLAC を要求している製品インスタンスが CSSM、CSLU、または SSM オンプレミスに接続されています。

- 転送タイプがそれに応じて設定されている（CSSMの場合は **smart**、CSLUの場合は **cslu**）。
show license all コマンドは特権 EXEC モードで入力します。出力で、Transport: フィールドを確認します。
- CSSMに直接接続している場合は、信頼コードがインストールされています。**show license all** コマンドは特権 EXEC モードで入力します。出力で、Trust Code Installed: フィールドを確認します。
- SSM オンプレミスが切断モードになる SSM オンプレミス展開の場合、このタスクで製品インスタンスから SLAC の SSM オンプレミスが要求されるため、このタスクを開始する前に、必要な SLAC ファイルが SSM オンプレミスサーバーで使用可能になっている必要があります。「承認コード要求の送信 (SSM オンプレミス UI、切断モード) (205 ページ)」を参照してください

手順

	コマンドまたはアクション	目的
ステップ 1	<p>enable</p> <p>例 :</p> <pre>Device> enable</pre>	<p>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。</p>
ステップ 2	<p>license smart authorization request {add replace} feature_name {all local}</p> <p>例 :</p> <pre>Device# license smart authorization request add hseck9 local</pre>	<p>license smart authorization request コマンドは、SLAC を CSSM または CSLU (CSLU は CSSM から取得) または SSM オンプレミスから要求します。SLAC が返され、製品インスタンスに自動的にインストールされます。</p> <p>既存の SLAC に追加するのか置換するのかを指定します。</p> <ul style="list-style-type: none"> • 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

	コマンドまたはアクション	目的
		<p>るようにエラーメッセージが表示されます。</p> <p><i>feature_name</i> 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。</p> <p>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。</p> <ul style="list-style-type: none"> • all : 高可用性設定のすべてのデバイスの承認コードを取得します。 • local : 高可用性設定のアクティブなデバイスの承認コードを取得します。これがデフォルトのオプションです。 <p>または、次のいずれかの方法を使用して SLAC を要求してインストールします。各オプションでサポートされるプラットフォームに注意してください。</p> <ul style="list-style-type: none"> • Cisco 1000、4000 シリーズサービス統合型ルータ、Catalyst 8200 エッジプラットフォーム、および 8300 エッジプラットフォームのみ : <p>license feature <i>feature_name</i> : 機能が自動的にコードを要求できるようにします。</p> <pre>Device(config)# license feature hseck9</pre> <ul style="list-style-type: none"> • Catalyst 8000V エッジソフトウェア、シスコクラウドサービスルータ 1000v、シスコサービス統合型仮想ルータのみ <p>platform hardware throughput level MB {500 1000 2500 5000} : 必要な SLAC を要求してインストールします。これは、ここで指定されたスループット値キーワード (250 MB を超える値) でのみサポートされます。</p> <pre>Device(config)# platform hardware throughput level MB 5000</pre>

	コマンドまたはアクション	目的
ステップ 3	show license authorization 例： Device# show license authorization	製品インスタンスにインストールされている承認コード (SLAC) を表示します。

製品インスタンスでの SLAC 要求の生成と保存

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



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

始める前に

サポートされるトポロジ：CSSM への接続なし、CSLU なし

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	license smart authorization request {add replace} feature_name {all local} 例： Device# license smart authorization request add hseck9 local	必要なライセンスと UDI の詳細を含む SLAC 要求を生成します。 既存の SLAC に追加するのかわ換するかを指定します。 <ul style="list-style-type: none"> • 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

	コマンドまたはアクション	目的
		<p>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。</p> <p><i>feature_name</i> 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。</p> <p>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。</p> <ul style="list-style-type: none"> • all : 高可用性設定のすべてのデバイスの承認コードを取得します。 • local : 高可用性設定のアクティブなデバイスの承認コードを取得します。これがデフォルトのオプションです。
ステップ 3	license smart authorization request save path 例 : <pre>Device# license smart authorization request save bootflash:slac.txt</pre>	SLAC 要求に必要な UDI およびライセンスの詳細を、指定した場所の .txt ファイルに保存します。
ステップ 4	CSSM Web UI にファイルをアップロードし、SLAC コードを含むファイルをダウンロードします。	次のタスクを実行します : CSSM へのデータまたは要求のアップロードとファイルのダウンロード (229 ページ)
ステップ 5	製品インスタンスへのファイルのインストール	次のタスクを実行します : 製品インスタンスへのファイルのインストール (231 ページ)

承認コードの削除と返却

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

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

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



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

始める前に

サポートされるトポロジ：すべて

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

```

Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# no license feature hseck9
% use 'write' command to disable 'hseck9' license on next boot
Device(config)# end
Device# copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
Device# reload
Proceed with reload? [confirm]
.
.
.
Device# show license summary
Account Information:
  Smart Account: Eg-SA As of Jan 29 07:10:00 2023 UTC
  Virtual Account: Eg-VA
License Usage:
License                               Entitlement tag                               Count Status
-----
hseck9                                 (ISR_4331_Hsec)                               0 NOT IN USE
booster_performance                    (ISR_4331_BOOST)                              1 IN USE
appxk9                                  (ISR_4331_Application)                       1 IN USE
uck9                                     (ISR_4331_UnifiedCommun...)                  1 IN USE
securityk9                              (ISR_4331_Security)                          1 IN USE
    
```

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

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

```

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

Device(config)# no license feature hseck9
% use 'write' command to disable 'hseck9' license on next boot
Device(config)# end
Device# copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
*Jan 31 05:13:22.556: %SYS-6-PRIVCFG_ENCRYPT_SUCCESS: Successfully encrypted
private config file
*Jan 31 05:13:22.563: %CRYPTO_SL_TP_LEVELS-6-VAR_NEW_VALUE: Setting crypto bidir
throughput to: 10000 kbps

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

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

```

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

- Catalyst 8000V エッジソフトウェア (.bin イメージが Catalyst 8000V ソフトウェアイメージにアップグレードされたシスコクラウドサービスルータ 1000v およびシスコサービス統合型仮想ルータを含む) では、最初にスループットを 250 Mbps 未満に設

定めます。値は、階層ベースの値または数値にできます。変更を有効にするために、デバイスをリロードする必要はありません。

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

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

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

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

以下の手順のステップは、このプラットフォームには適用されません。

- SLR 承認コードを返却する場合は、以下の手順を実行します。SLR 承認コードに HSECK9 ライセンスが含まれているかどうかに関係なく、手順は同じです。
- PAK の返却については、[PAK ライセンスの削除 \(240 ページ\)](#) を参照してください。
- PLR 承認コードの返却については、[PLR の非アクティブ化 \(251 ページ\)](#) を参照してください。

手順

	コマンドまたはアクション	目的
ステップ 1	license smart authorization return {all local} {offline [path] online} 例 :	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
<pre>Device# license smart authorization return local online OR Device# license smart authorization return local offline Enter this return code in Cisco Smart Software Manager portal: UDI: PID:C8300-1N1S-4T2X,SN:FDO2349A00R Return code: CrMfaJ-9odPW7-gr2DzP-t3srpf-ATqzGS-wGF3c6- U3Kg77-GdiABx-gud *Jan 31 05:18:00.804: %SMART_LIC-6-AUTHORIZATION_REMOVED: A licensing authorization code has been removed from PID:C8300-1N1S-4T2X,SN:FDO2349A00R. OR Device# license smart authorization return local offline bootflash:return-code.txt</pre>	<p>製品インスタンスを指定します。</p> <ul style="list-style-type: none"> • 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。 <p>CSSMに接続しているかどうかを指定します。</p> <ul style="list-style-type: none"> • 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。 <p>オフラインオプションを選択した場合は、これをCSSMに送信する追加の手順を完了する必要があります。</p> <ul style="list-style-type: none"> • CLIまたは保存されたファイルから返却コードをコピーし、CSSMに入力します：CSSMでのリターンコードの入力と製品インスタンスの削除 (226ページ) 17.7.1aより以前のソフトウェアバージョンでは、この手順のみを使用してコードを返却することができます。 • ファイルを保存するパスを指定し、ファイルをCSSMにアップロードします。このコードを返却する手順は、17.7.1a以降で使用できます：CSSMへのデータまたは要求のアップロー

	コマンドまたはアクション	目的
		<p>ドとファイルのダウンロード (229 ページ)</p> <p>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：<code>Device# license smart authorization return local offline bootflash:return-code.txt.</code></p> <p>(注) SSM オンプレミス展開の場合は、online オプションのみを使用します。offline オプションはサポートされていません。</p>
<p>ステップ 2</p>	<p>show license all</p> <p>例：</p> <pre>Device# show license all . . . License Authorizations ===== Overall status: Active: PID:C8300-1N1S-4T2X, SN:FDO2349A00R Status: NOT INSTALLED Last return code: CrMfaJ-9odPW7-gr2DzP-t3srpf-ATqzGS-wGF3c6- U3Kg77-GdiABx-gud . . .</pre>	<p>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。</p>
<p>ステップ 3</p>	<p>show license summary</p> <p>例：</p> <pre>Device# show license summary Account Information: Smart Account: Eg-SA As of Jan 31 05:31:20 2023 UTC Virtual Account: Eg-VA License Usage: License Entitlement Tag Count Status ----- network-advantage_10M (ESR_P_10M_A) 1 IN USE dna-advantage_10M (DNA_P_10M_A) 1 IN USE</pre>	<p>製品インスタンスで使用可能なライセンスがすべて表示されます。添付の例では、HSECK9 ライセンスが表示されなくなりました。</p>

CSSM でのリターンコードの入力と製品インスタンスの削除

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

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

始める前に

サポートされるトポロジ：CSSM への接続なし、CSLU なし

手順

- ステップ 1** <https://software.cisco.com> で CSSM Web UI にログインし、[Manage licenses] をクリックします。
シスコから提供されたユーザ名とパスワードを使用してログインします。[Smart Software Licensing] ページが表示されます。
- ステップ 2** [Inventory] タブをクリックします。
- ステップ 3** [Virtual Account] ドロップダウンリストから、バーチャルアカウントを選択します。
- ステップ 4** [Product Instances] タブをクリックします。
使用可能な製品インスタンスのリストが表示されます。
- ステップ 5** 製品インスタンスリストから必要な製品インスタンスを見つけます。オプションで、検索タブに名前または製品タイプの文字列を入力して、製品インスタンスを検索できます。
- ステップ 6** 製品インスタンスの [Actions] 列で、[Actions] ドロップダウンリストから [Remove] を選択します。
[Remove Reservation] ウィンドウが表示されます。
- ステップ 7** [Reservation Return Code] フィールドに、戻りコードを入力します。
ライセンスがライセンスプールに戻されます。[Remove Reservation] ウィンドウが自動的に閉じ、[Product Instances] タブに戻ります。
(注) ライセンスの返却のみの場合、これでタスクは終了です。CSSM から製品インスタンスも削除する場合は、次の手順に進みます。
- ステップ 8** 製品インスタンスの [Actions] 列で、[Actions] ドロップダウンリストから再度 [Remove] を選択します。
[Confirm Remove Product Instance] ウィンドウが表示されます。
- ステップ 9** [Remove Product Instance] をクリックします。

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

CSSM からの信頼コード用新規トークンの生成

信頼コードを要求するトークンを生成するには、次の手順を実行します。

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

始める前に

サポートされるトポロジ：CSSM に直接接続

手順

- ステップ 1 <https://software.cisco.com> で CSSM Web UI にログインし、[Manage licenses] をクリックします。シスコから提供されたユーザ名とパスワードを使用してログインします。[Smart Software Licensing] ページが表示されます。
- ステップ 2 [Inventory] タブをクリックします。
- ステップ 3 [Virtual Account] ドロップダウンリストから、必要なバーチャルアカウントを選択します。
- ステップ 4 [General] タブをクリックします。
- ステップ 5 [New Token] をクリックします。[Create Registration Token] ウィンドウが表示されます。
- ステップ 6 [Description] フィールドに、トークンの説明を入力します。
- ステップ 7 [Expire After] フィールドに、トークンをアクティブにする必要がある日数を入力します。
- ステップ 8 (オプション) [Max. Number of Uses] フィールドに、トークンの有効期限が切れるまでの最大使用回数を入力します。
- ステップ 9 [Create Token] をクリックします。
- ステップ 10 リストに新しいトークンが表示されます。[Actions] をクリックし、トークンを .txt ファイルとしてダウンロードします。

ID トークンによる信頼の確立

CSSM との信頼できる接続を確立するには、次の手順を実行します。

始める前に

サポートされるトポロジ：CSSM に直接接続

このタスクを実行する前に、CSSM から ID トークンファイルを生成してダウンロードしたことを確認してください。[CSSM からの信頼コード用新規トークンの生成 \(227 ページ\)](#)

手順

	コマンドまたはアクション	目的
ステップ 1	<p>enable</p> <p>例 :</p> <pre>Device> enable</pre>	<p>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。</p>
ステップ 2	<p>license smart trust idtoken <i>id_token_value</i>{local all} [force]</p> <p>例 :</p> <pre>Device# license smart trust idtoken NGMwMjksYtNZaxMS00NzZmtgWm all force</pre>	<p>信頼要求を送信して、CSSM との信頼できる接続を確立します。 <i>id_token_value</i> には、CSSM で生成したトークンを入力します。</p> <p>次のいずれかのオプションを入力します。</p> <ul style="list-style-type: none"> • 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。 <p>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。</p> <p>信頼コードは、製品インスタンスの UDI にノードロックされます。UDI に信頼コード (CSSM との信頼できる接続) がすでにある場合、CSSM では同じ UDI に対する新しい信頼コードは許可されません。force キーワードを入力すると、CSSM に送信されるメッセージに強制フラグが設定され、すでに存在する場合でも新しい信頼コードが作成されます。</p>
ステップ 3	<p>show license status</p> <p>例 :</p> <pre><output truncated> Trust Code Installed: Active: PID:C9500-24Y4C, SN:CAT2344L4GH</pre>	<p>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。</p>

	コマンドまたはアクション	目的
	<pre> INSTALLED on Sep 04 01:01:46 2020 EDT Standby: PID:C9500-24Y4C,SN:CAT2344L4GJ INSTALLED on Sep 04 01:01:46 2020 EDT </pre>	

CSSM からのポリシーファイルのダウンロード

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

始める前に

サポートされるトポロジ:

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

手順

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

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

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

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

これで、ファイルを製品インスタンスにインストールできます。[製品インスタンスへのファイルのインストール \(231 ページ\)](#) を参照してください

CSSM へのデータまたは要求のアップロードとファイルのダウンロード

このタスクは、次の目的で使用できます。

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

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

- SLAC 返却ファイルをアップロードします。

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

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

始める前に

サポートされるトポロジ：

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

手順

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

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

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

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

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

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

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

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

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

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

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

製品インスタンスへのファイルのインストール

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

始める前に

サポートされるトポロジ：CSSM への接続なし、CSLU なし

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

- SLACについては、[CSSMからのSLACの生成とファイルへのダウンロード \(214ページ\)](#) または [CSSMへのデータまたは要求のアップロードとファイルのダウンロード \(229ページ\)](#) (エアーギャップネットワークでSLACファイルを取得する方法は複数あります) を参照してください。
- ポリシーについては、[CSSMからのポリシーファイルのダウンロード \(229ページ\)](#) を参照してください。
- ACKについては、[CSSMへのデータまたは要求のアップロードとファイルのダウンロード \(229ページ\)](#) を参照してください。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	copy source bootflash:file-name 例： Device# copy tftp://10.8.0.6/user01/example.txt bootflash:	ファイルをソースの場所またはディレクトリから製品インスタンスのフラッシュメモリにコピーします。 <ul style="list-style-type: none"> • 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。

	コマンドまたはアクション	目的
ステップ 3	license smart import bootflash: <i>file-name</i> 例： <pre>Device# license smart import bootflash:example.txt</pre>	<p>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。</p> <p>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。</p>
ステップ 4	show license all 例： <pre>Device# show license all</pre>	<p>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。</p>

転送タイプ、URL、およびレポート間隔の設定

製品インスタンスの転送モードを設定するには、次のタスクを実行します。

始める前に

サポートされるトポロジ：すべて

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： <pre>Device> enable</pre>	<p>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。</p>
ステップ 2	configure terminal 例： <pre>Device# configure terminal</pre>	
ステップ 3	license smart transport {automatic callhome cslu off smart} 例： <pre>Device(config)# license smart transport cslu</pre>	<p>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。</p> <ul style="list-style-type: none"> • automatic：転送モードをデフォルト (CSLU) に設定します。

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> • callhome : 転送モードとして Call Home を有効にします。 • cslu : これがデフォルトのトランスポートモードです。製品インスタンス開始型通信で CSLU または SSM オンプレミスを使用している場合は、このキーワードを入力します。 (注) CSLU と SSM オンプレミスの両方に同じトランスポートモードが適用されますが、URL が異なります。次のステップの cslu <code>cslu_or_on-prem_url</code> を参照してください。 • off : 製品インスタンスからのすべての通信を無効にします。 • smart : スマート転送を有効にします。 (注) 転送方式を callhome から smart に変更する場合、Smart Licensing Using Policy を期待どおりに機能させるために「CiscoTAC-1」 Call Home プロファイルを無効化する必要はありません。
<p>ステップ 4</p>	<p>license smart url {url cslu <code>cslu_or_on-prem_url</code> default smart <code>smart_url</code> utility <code>smart_url</code>}</p> <p>例 :</p> <pre>Device(config)# license smart url cslu http://192.168.0.1:8182/cslu/v1/pi</pre>	<p>設定されたトランスポートモードに使用する URL を設定します。前のステップで選択した転送モードに応じて、対応する URL をここで設定します。</p> <ul style="list-style-type: none"> • 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

	コマンドまたはアクション	目的
		<p>no license smart url url コマンドは、デフォルトの URL に戻ります。</p> <ul style="list-style-type: none"> • cslu cslu_or_on-prem_url : トランスポートモードを cslu として設定している場合は、必要に応じて CSLU または SSM オンプレミスの URL を使用してこのオプションを設定します。 <ul style="list-style-type: none"> • CSLU を使用している場合は、次のように URL を入力します。 <code>http://<cslu_ip_or_host>:8182/cslu/v1/pi</code> <cslu_ip_or_host> には、CSLU をインストールした Windows ホストのホスト名や IP アドレスを入力します。8182 はポート番号であり、CSLU が使用する唯一のポート番号です。 • no license smart url cslu cslu_or_on-prem_url コマンドは <code>http://cslu-local:8182/cslu/v1/pi</code> に戻ります。 • SSM オンプレミスを使用している場合は、次のように URL を入力します。 <code>http://<ip>/cslu/v1/pi/<tenant ID></code> <ip> には、SSM オンプレミス をインストールしたサーバのホスト名または IP アドレスを入力します。<tenantID> はデフォルトのローカルバーチャルアカウント ID にする必要があります。

	コマンドまたはアクション	目的
		<p>ヒント SSM オンプレミスから URL 全体を取得できます。「トランスポート URL の取得 (SSM オンプレミス UI) (203 ページ)」を参照してください</p> <p>no license smart url cslu <i>cslu_or_on-prem_url</i> コマンドは http://cslu-local:8182/cslu/v1/pi に戻ります。</p> <ul style="list-style-type: none"> • 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。 <p>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)。</p> <p>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)。</p> <ul style="list-style-type: none"> • 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。 <p>https://smartreceiver.cisco.com/licservice/license</p> <p>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。</p> <p>no license smart url smartsmart_url コマンドは、デフォルトの URL に戻ります。</p>

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> • utility smart_url : このオプションは CLI では使用できますがサポートされていません。
ステップ 5	license smart usage interval interval_in_days 例 : Device(config)# license smart usage interval 40	<p>(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。</p> <p>ユーティリティモードを使用している場合、レポート間隔は 7 日以内にすることを推奨します。7 日以内にすることで、ユーティリティモードの製品インスタンスに適用される 30 日間の ACK 要件がタイムリーに満たされます。</p> <p>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。</p>

ユーティリティモードの有効化

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

始める前に

サポートされるトポロジ :

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

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例 : Device> enable	特権 EXEC モードを有効にします。プロンプトが表示されたらパスワードを入力します。
ステップ 2	configure terminal	

	コマンドまたはアクション	目的
	例 : Device# <code>configure terminal</code>	
ステップ 3	license smart utility 例 : Device (config)# <code>license smart utility</code>	<p>製品インスタンスのユーティリティモードを有効にして、MSLAが使用されることを示します。有効にすると、次のことが発生します。</p> <ul style="list-style-type: none"> • トランスポートタイプと URL がチェックされます。 この設定が正しく構成されていない場合、%SMART_LIC4UTILITY_TRANSPORT_CONFIG システムメッセージが表示されます。 • RUM レポートには、製品インスタンスがユーティリティモードであることを示すフラグが含まれています。 ユーティリティモードを初めて有効にしたときに、RUM レポートにユーティリティフラグが設定されず、スマートアカウントとバーチャルアカウントにサブスクリプションが存在する場合、サブスクリプション ID は RUM ACK で返されます。後続の RUM レポートには、サブスクリプション ID が含まれます。サブスクリプション ID もすべての RUM ACK で返されます。 %SMART_LIC4UTILITY_SUBSCRIPTION_LICENSE メッセージは、ユーティリティモードが有効になっていて、サブスクリプション ID のないライセンスが製品インスタンスで使用されている場合に表示されます。 • ユーティリティモードに固有のポリシーが製品インスタンスに設定されています。ユーティリティポリシーには、RUM ACK を 30 日ごとにインストールする必要があると記載されています。

	コマンドまたはアクション	目的
		<p>ACK が期限を過ぎている場合、<code>%SMART_LIC4-UTILITY_NO_ACK</code> システムメッセージが表示されます。</p> <ul style="list-style-type: none"> 情報メッセージ <code>%SMART_LIC-3-UTILITY_STARTED</code> が表示されます。これは、ユーティリティモードが有効になっており、サブスクリプション ID が使用可能であることを示しています。
ステップ 4	exit 例： Device (config)# exit	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 5	copy running-config startup-config 例： Device# copy running-config startup-config	コンフィギュレーション ファイルに設定を保存します。

PAK ライセンスの使用を継続する

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



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

始める前に

サポートされるトポロジ：すべて

手順

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

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

- 17.3.x トレインの Cisco IOS XE Amsterdam 17.3.5 以降のリリース。

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

アップグレード情報については、次を参照してください。

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

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

ステップ 2 DLC が完了したことを確認します。

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

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

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

```
Device# show platform software license dlc
```

```
<output truncated>
```

DLC Process Status: Completed

DLC Conversion Status: SUCCESS

ステップ3 ライセンスの使用状況を CSSM と同期します。

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

結果：

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

PAK ライセンスの削除

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



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

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

始める前に

サポートされるトポロジ：すべて

手順

ステップ1 DLC が完了したことを確認します。

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

Smart Licensing Using Policy をサポートするリリースにアップグレードすると、製品インスタンスで DLC プロセスが自動的にトリガーされます。DLC データは製品インスタンスが Smart

Licensing Using Policy をサポートするソフトウェアバージョンにアップされた 1 時間後に収集されます。

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

```
Device# show platform software license dlc
```

```
<output truncated>
```

```
DLC Process Status: Completed
```

```
DLC Conversion Status: SUCCESS
```

ステップ 2 工場出荷時の状態へのリセット

製品インスタンスに応じて、対応するリンクを参照してください。

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

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

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

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

ステップ 4 ライセンスの使用状況と CSSM の同期

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

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

結果：

以下の選択肢があります。

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

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

- 別の製品インスタンスで、通常のスマートライセンスとして PAK 履行済みライセンスを使用する。
別の製品インスタンスでライセンスを使用するには、その製品インスタンスに該当するコマンドを使用してライセンスを設定します。ライセンスのレポート要件は、他のライセンスと同じです。ポリシーに従って、またはシステムメッセージにそのように示されている場合。
- 製品インスタンスの使用を継続する。
- 製品インスタンスをデコミッションするか、返品許可 (RMA) を実行する場合は、CSSM から製品インスタンスを削除します。

障害が発生した製品インスタンスの PAK ライセンスの削除

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

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

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

PLR のアクティブ化

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

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

始める前に

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

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

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

手順

ステップ 1 **configure terminal**

例：

```
Device#configure terminal
```

グローバル コンフィギュレーション モードを開始します。

ステップ 2 **license smart reservation**

例：

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

予約モードを有効にします。

ステップ 3 **exit**

例：

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

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

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

例：

```
Device# license smart reservation request local
```

Enter this request code in the Cisco Smart Software Manager portal:

UDI: PID:C8000V,SN:96QKIABBZ1H

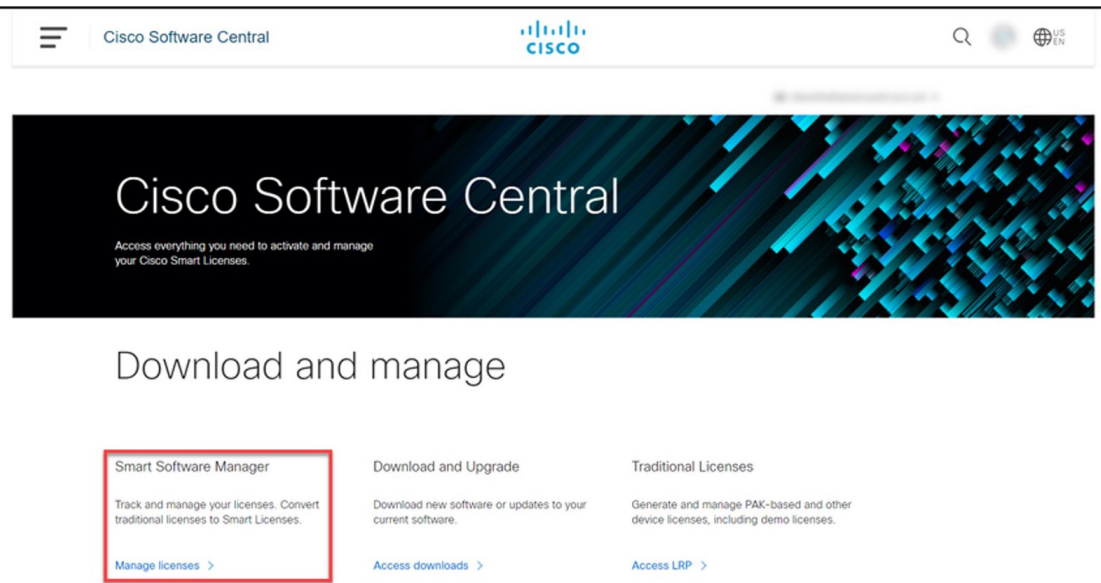
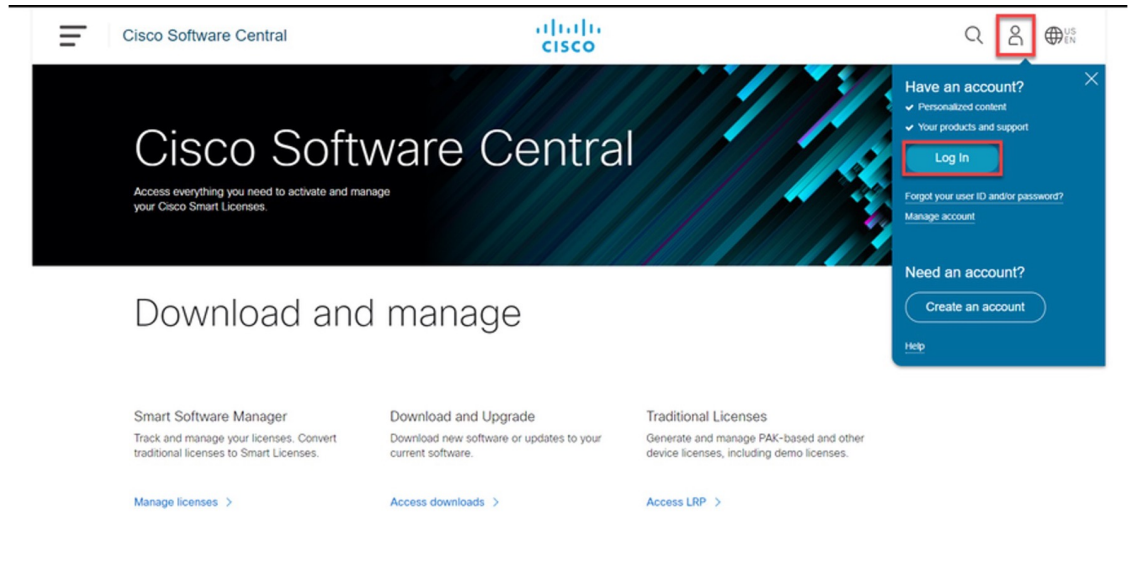
Request code: DB-ZC8000V:96QKIABBZ1H-AYk3ndtp6-F1

製品インスタンスで予約要求コードを生成します。

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

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

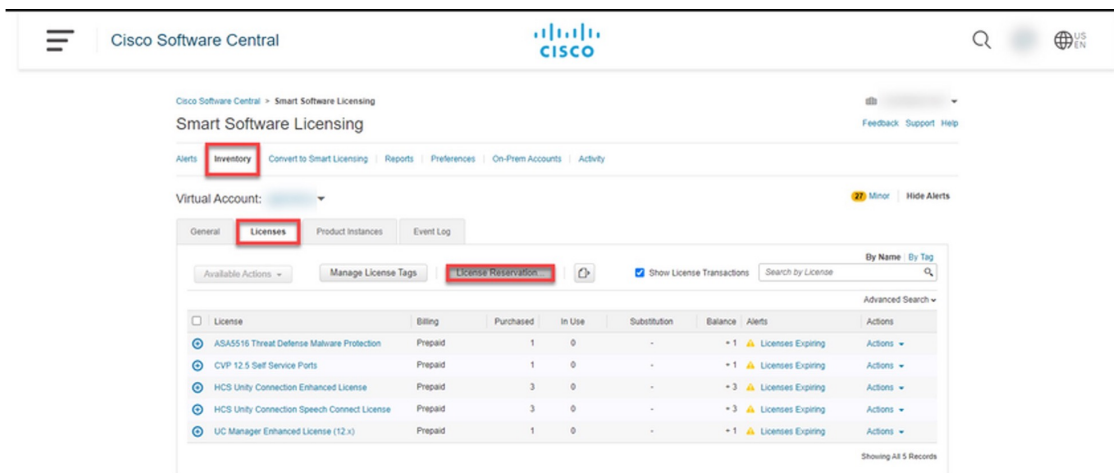
例：



CSSM Web UI にログインします。

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

例：

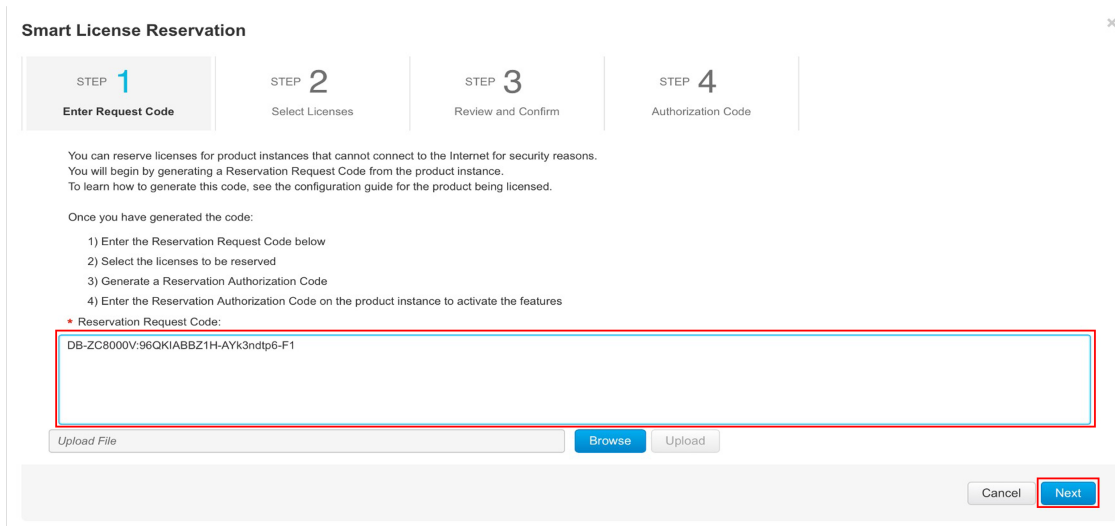


[Smart License Reservation] ダイアログボックスが表示されます。

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

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

例 :



ステップ 3 で製品インスタンスで生成した予約要求コードを入力します。

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

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

例 :

Smart License Reservation

STEP 1 ✓ Enter Request Code | STEP 2 Select Licenses | STEP 3 Review and Confirm | STEP 4 Authorization Code

Product Instance Details

Product Type: CAT8KV
 UDI PID: C8000V
 UDI Serial Number: 96QKIABBZ1H

Licenses to Reserve
 In order to continue, ensure that you have a surplus of the licenses you want to reserve in the Virtual Account.

C8000v PLR
 Reserve a specific license

Cancel Next

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

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

例 :

Smart License Reservation

STEP 1 ✓ Enter Request Code | STEP 2 ✓ Select Licenses | STEP 3 Review and Confirm | STEP 4 Authorization Code

Product Instance Details

Product Type: CAT8KV
 UDI PID: C8000V
 UDI Serial Number: 96QKIABBZ1H

Licenses to Reserve

License	Expires	Quantity to Reserve
C8000v PLR <small>C8000v Permanent License Reservation</small>	-	1

Cancel Back Generate Authorization Code

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

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

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

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

例 :

Smart License Reservation

STEP 1 ✓ Enter Request Code STEP 2 ✓ Select Licenses STEP 3 ✓ Review and Confirm **STEP 4 Authorization Code**

✓ The Reservation Authorization Code below has been generated for this product instance. Enter this code into the Smart Licensing settings for the product, to enable the licensed features.

Product Instance Details

Product Type:	CAT8KV
UDI PID:	C8000V
UDI Serial Number:	96QKIABBZ1H

Authorization Code:

DA3Ks9-WM4yzT-Y7UAbh-GGXUwr-qARDsq-sjJs9e-Z3Xqix-TKcsy9-z6

To learn how to enter this code, see the configuration guide for the product being licensed.

Download as File Copy to Clipboard Close

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

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

ステップ 12 license smart reservation install PLR-Code

例：

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

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

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

ステップ 13 show license reservation

例：

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

ライセンス予約情報を表示します。

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

ステップ 14 configure terminal

例：

```
Device# configure terminal
```

グローバル コンフィギュレーション モードを開始します。

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

例 :

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

スループットレベルを設定します。

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

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

ステップ 16 exit

例 :

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

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

ステップ 17 show platform hardware throughput level MB

例 :

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

デバイスで現在実行されているスループットを表示します。

PLR のアップグレード

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

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

始める前に

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

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



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

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

手順

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

CSSM Web UI にログインします。

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

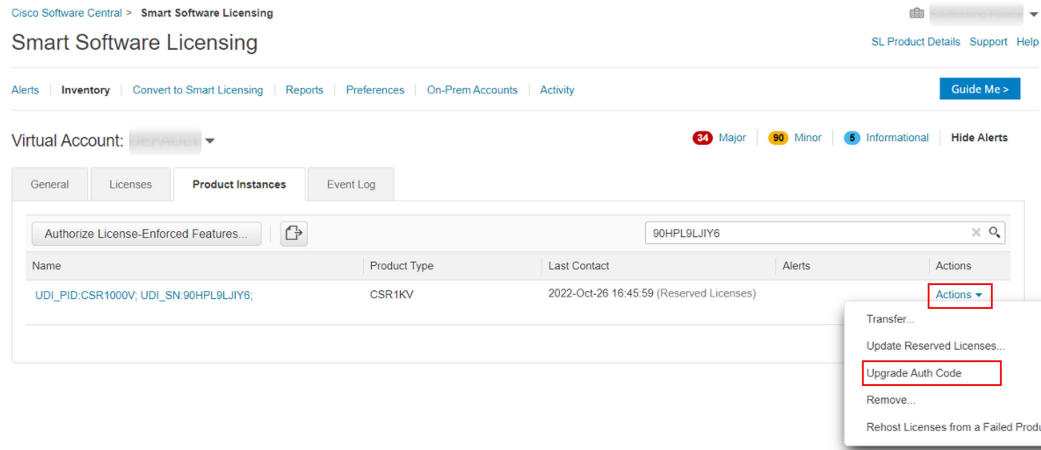
製品インスタンスのリストが表示されます。

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

使用可能なアクションのリストが表示されます。

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

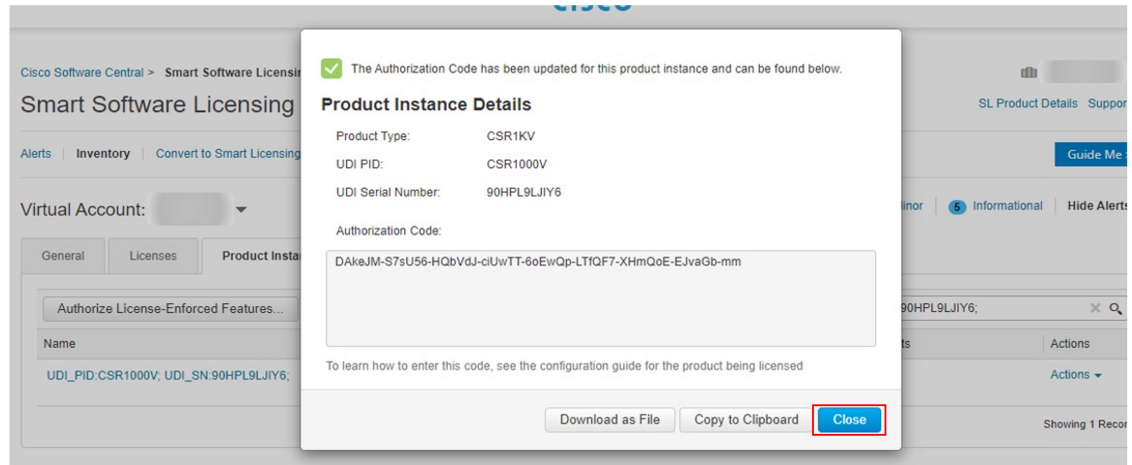
例 :



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

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

例 :



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

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

ステップ 6 license smart reservation install PLR-Code

例 :

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

```
Reservation install successful
```

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

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

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

ステップ 7 show platform hardware throughput level MB

例：

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

デバイスで現在実行されているスループットを表示します。

ステップ 8 show license reservation

例：

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

ライセンス予約情報を表示します。

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

PLR の非アクティブ化

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

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

始める前に

サポートされるトポロジ：該当なし

手順

ステップ 1 license smart reservation return local

例：

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

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

製品インスタンスに予約返却要求コードを生成します。

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

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

CSSM Web UI にログインします。

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

製品インスタンスのリストが表示されます。

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

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

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

ステップ 6 **configure terminal**

例：

```
Device# configure terminal
```

グローバル コンフィギュレーション モードを開始します。

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

例：

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

予約モードを無効にします。

ステップ 8 **exit**

例：

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

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

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（214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	
	C1111-8PLTEEAWA	
	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	
	C1117-8PLTEEAW	
	C1117-8PLTELAW	
	C1117-8PLTELAZ	
	C1111X-8P	
	C1112-8P	
	C1112-8PLTEEA	
	C1113-8P	
	C1113-8PM	
	C1113-8PLTEEA	
	C1113-8PLTELA	
	C1113-8PMLTEEA	
	C1113-8PWE	
	C1113-8PWA	
	C1113-8PWZ	
	C1113-8PMWE	
	C1113-8PLTEEAW	
	C1113-8PLTELAW	
	C1113-8PLTELAZ	
	C1114-8P	
	C1114-8PLTEEA	
	C1115-8P	
	C1115-8PLTEEA	
	C1115-8PM	
	C1115-8PMLTEEA	
	C1118-8P	

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

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	

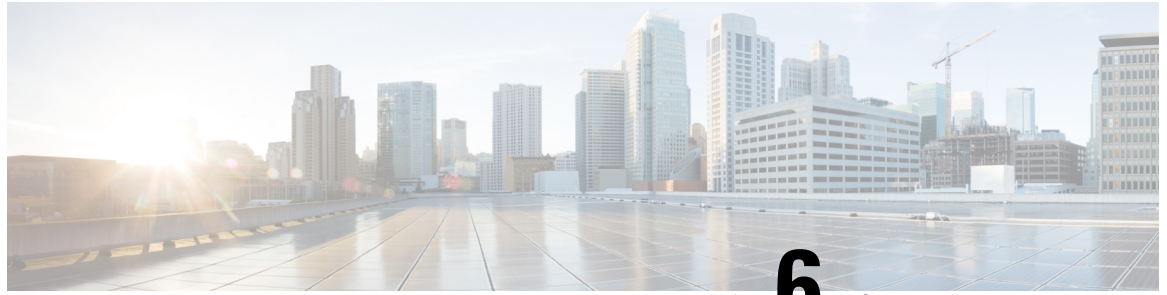
製品ファミリ	PID	ライセンス名
ISR1K - 4P	C1111-4P	ISR_1100_4P_Hsec
	C1111-4PLTEEA	
	C1111-4PLTELA	
	C1111-4PWE	
	C1111-4PWB	
	C1111-4PWA	
	C1111-4PWZ	
	C1111-4PWN	
	C1111-4PWQ	
	C1111-4PWC	
	C1111-4PWR	
	C1111-4PWK	
	C1111-4PWD	
	C1111X-4P	
	C1116-4P	
	C1116-4PLTEEA	
	C1116-4PLTEEAWA	
	C1116-4PWE	
	C1117-4P	
	C1117-4PLTEEA	
	C1117-4PLTELA	
	C1117-4PLTEEAWA	
	C1117-4PLTEELAWZ	
	C1117-4PWE	
	C1117-4PWA	
	C1117-4PWZ	
	C1117-4PM	
	C1117-4PMLTEEA	
	C1117-4PMLTEEAWA	
	C1117-4PMWE	

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

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		
ISR1K-2P	C1109-2PLTEGB	ISR_1100_2P_Hsec
	C1109-2PLTEUS	
	C1109-2PLTEVZ	
	C1109-2PLTEJN	
	C1109-2PLTEAU	
	C1109-2PLTEIN	

製品ファミリ	PID	ライセンス名
ISR4200	ISR4221/K9	ISR4220_HSEC
	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	
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	
C8000V	該当なし	
CSR1000V	該当なし	
ISRV	適用されない	

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



第 6 章

ポリシーを使用したスマートライセンスの 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 \(グローバル コンフィギュレーション\) \(261 ページ\)](#)
- [license smart \(特権 EXEC\) \(277 ページ\)](#)
- [show license all \(286 ページ\)](#)
- [show license authorization \(292 ページ\)](#)
- [show license data \(301 ページ\)](#)
- [show license eventlog \(301 ページ\)](#)
- [show license history message \(304 ページ\)](#)
- [show license reservation \(305 ページ\)](#)
- [show license rum \(306 ページ\)](#)
- [show license status \(314 ページ\)](#)
- [show license summary \(323 ページ\)](#)
- [show license tech \(326 ページ\)](#)
- [show license udi \(337 ページ\)](#)
- [show license usage \(338 ページ\)](#)
- [show platform software sl-infra \(342 ページ\)](#)

license smart (グローバル コンフィギュレーション)

製品インスタンスが Cisco Smart Software Manager (CSSM)、Cisco Smart Licensing Utility (CSLU)、または Smart Software Manager オンプレミス (SSM オンプレミス) との通信に使用するトランスポートモードや URL などのライセンス関連の設定を行い、使用状況レポートの間隔を設定し、ライセンス使用状況レポート (RUM レポート) に含めるか除外する必要がある情報を設定し、ライセンスデータを送信するように VRF 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_or_on-prem_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 | id id | name name |
postalcode postalcode | state state | street street } ] | vrf vrf_string }
```

```
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_or_on-prem_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 | id id | name name | postalcode postalcode | state state | street street } ] | vrf
vrf_string }
```

構文の説明

custom_id <i>ID</i>	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、設定しても効果はありません。スマートライセンスは常に有効になっています。

privacy { all | hostname | version }

プライバシーフラグを設定して、指定されたデータプライバシー関連情報の送信を防止します。

フラグが無効になっている場合、対応する情報は、製品インスタンスによって作成されるメッセージまたはオフラインファイルで送信されます。

トポロジに応じて、CSSM、CSLU、SSM オンプレミスなどの1つ以上のコンポーネントに情報が送信されます。

すべてのデータプライバシー設定はデフォルトで無効になっています。すべての通信から除外するオプションを設定する必要があります。

- **all** : すべてのデータプライバシー関連情報がすべての通信から除外されます。

このコマンドの **no** 形式を使用すると、すべてのデータプライバシー関連情報がメッセージまたはオフラインファイルで送信されます。

(注) データプライバシーが有効かどうかに関係なく、製品 ID (PID) とシリアル番号が RUM レポートに含まれます。

- **hostname** : ホスト名情報がすべての通信から除外されます。ホスト名のプライバシーが有効になっている場合、製品インスタンスの UDI が該当するユーザーインターフェイス (CSSM、CSLU、および SSM オンプレミス) に表示されます。

このコマンドの **no** 形式を使用すると、ホスト名情報がメッセージまたはオフラインファイルで送信されます。ホスト名は、該当するユーザーインターフェイス (CSSM、CSLU、および SSM オンプレミス) に表示されます。

- **version** : 製品インスタンスで実行されている Cisco IOS-XE ソフトウェアバージョンとスマートエージェントのバージョンがすべての通信から除外されます。

このコマンドの **no** 形式を使用すると、バージョン情報がメッセージまたはオフラインファイルで送信されます。

proxy { **address** *address_hostname* | **port** *port* }

CSLUまたはCSSMとライセンス使用状況を同期するためにプロキシを設定します。つまり、トランスポートモードが **license smart transport smart** (CSSM) または **license smart transport cslu** (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。

ただし、トランスポートモードとして **license smart transport cslu** も使用する SSM オンプレミス展開では、ライセンス使用状況の同期にプロキシは設定できません。

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

Smart Licensing Using Policy 環境でパーマネントライセンス予約 (PLR) の予約モードを有効にします。

Smart Licensing Using Policy 環境では、PLR は Cisco IOS XE Dublin 17.10.1 以降でのみサポートされます。PLR をサポートする製品インスタンスは、Catalyst 8000V エッジソフトウェアへの .bin アップグレードが実行される Catalyst 8000V エッジソフトウェアと Cloud Services Router 1000v のみです。

このコマンドの **no** 形式を使用すると、予約が無効になります。

PLR コードをキャンセル、インストール、要求、および返却するために使用される特権 EXEC コマンドにアクセスする前に、このキーワードを使用して予約モードを有効にする必要があります。

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。 <ul style="list-style-type: none">• 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。<p>(注) CSLU と SSM オンプレミスの両方に同じトランスポートモードが適用されますが、URL が異なります。次の行の cslu <i>cslu_or_on-prem_url</i> を参照してください。</p>• 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 | csu cslu_or_on-prem_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_or_on-prem_url** : トランスポートモードを **cslu** として設定している場合は、必要に応じて CSLU または SSM オンプレミスの URL を使用してこのオプションを設定します。

- CSLU を使用している場合は、次のように URL を入力します。

```
http://<cslu_ip_or_host>:8182/cslu/v1/pi
```

<cslu_ip_or_host> には、CSLU をインストールした Windows ホストのホスト名や IP アドレスを入力します。8182 はポート番号であり、CSLU が使用する唯一のポート番号です。

no license smart url cslu cslu_or_on-prem_url コマンドは

```
http://cslu-local:8182/cslu/v1/pi
```

 に戻ります。

- SSM オンプレミスを使用している場合は、次のように URL を入力します。

```
http://<ip>/cslu/v1/pi/<tenant ID>
```

<ip> には、SSM オンプレミスをインストールしたサーバのホスト名または IP アドレスを入力します。<tenantID> はデフォルトのローカルバーチャルアカウント ID にする必要があります。

ヒント SSM オンプレミスから URL 全体を取得できます。「[トランスポート URL の取得 \(SSM オンプレミス UI\)](#) (203 ページ)」を参照してください

no license smart url cslu cslu_or_on-prem_url コマンドは

```
http://cslu-local:8182/cslu/v1/pi
```

 に戻り

ます。

- **default** : 設定されている転送モードによって異なります。このオプションでは、**smart** および **cslu** 転送モードのみがサポートされます。

転送モードが **cslu** に設定されている場合、**license smart url default** を設定すると、CSLU URL は自動的に設定されます

(<https://cslu-local:8182/cslu/v1/pi>)。

転送モードが **smart** に設定されている場合、**license smart url default** を設定すると、スマート URL は自動的に設定されます

(<https://smartreceiver.cisco.com/licservice/license>)。

- **smart smart_url** : 転送タイプとして **smart** を設定している場合は、このオプションを設定します。URL を次のように正確に入力します。

<https://smartreceiver.cisco.com/licservice/license>

このオプションを設定すると、システムは **license smart url url** で自動的に URL の複製を作成します。重複するエントリは無視できません。これ以上の操作は必要ありません。

no license smart url smartsmart_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 では使用できません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せん。

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。

ユーティリティモードを使用している場合、レポート間隔は 7 日以内にすることを推奨します。7 日以内にすることで、ユーティリティモードの製品インスタンスに適用される 30 日間の ACK 要件がタイムリーに満たされます。

utility [**customer_info** { **city** *city* | **country** *country* | **id** *id* | **name** *name* | **postalcode** *postalcode* | **state** *state* | **street** *street* }]

製品インスタンスでユーティリティモードを有効にします。

MSLA があり、サブスクリプション ID 付きのライセンスを使用している場合は、ユーティリティモードを有効にする必要があります。有効にすると、製品インスタンスとのすべての通信に適宜フラグが設定されます。

ユーティリティモードの製品インスタンスの場合、必要に応じて追加情報を RUM レポートに含めることができます。この情報はシスコでは使用されません。

RUM レポートに任意の情報を含めるには、**customer_info** キーワードに続けて以下のオプションを 1 つ以上入力します。

- **city** *city*
- **country** *country*
- **id** *id* : ユーザー定義の ID を入力します。
- **name** *name* : ユーザー定義の名前を入力します。
- **postalcode** *postalcode*
- **state** ステート
- **street** *street*

license smart utility コマンドの **no** 形式を使用すると、ユーティリティモードが無効になります。

vrf *vrf_string*

製品インスタンスで使用される Virtual Routing and Forwarding (VRF) 名を設定します。製品インスタンスは VRF を使用して、ライセンス関連のデータを CSSM、CSLU、または SSM オンプレミスに送信します。

vrf_string には、定義した VRF 名を入力します。

次の要件が満たされていることを確認します。

- 製品インスタンスは VRF をサポートするインスタンスである。
- トランスポートタイプは **smart** または **cslu** であり、対応する URL がある。

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ス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
	<p>Cisco IOS XE Amsterdam 17.3.2 より前のリリースで導入されました。</p>	<p>このコマンドが導入されました。</p>
	<p>Cisco IOS XE Amsterdam 17.3.2</p>	<p>ポリシーを使用したスマートライセンスで、次のキーワードと変数が導入されました。</p> <ul style="list-style-type: none"> • url キーワードの下に、次のオプションが導入されました。 <pre>{ cslu <i>cslu_url</i> smart <i>smart_url</i> }</pre> • transport キーワードの下に、次のオプションが導入されました。 <pre>{ cslu off }</pre> <p>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。</p> <ul style="list-style-type: none"> • usage { customer-tags { tag1 tag2 tag3 tag4 } <i>tag_value</i> interval <i>interval_in_days</i> } <p>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。</p>
	<p>Cisco IOS XE Amsterdam 17.3.3</p>	<p>SSM オンプレミスサポートが導入されました。SSM オンプレミス展開での製品インスタンス開始型通信の場合、既存の [no]license smart url cslucaclu_or_on-prem_url コマンドは SSM オンプレミスの URL の設定もサポートします。ただし、SSM オンプレミスに必要な URL 形式は <code>http://<ip>/cslu/v1/pi/<tenant ID></code> です。</p> <p>設定する必要がある対応するトランスポートモードも、既存のコマンド (license smart transport cslu) です。</p>
	<p>Cisco IOS XE Cupertino 17.7.1a</p>	<p>バージョンプライバシーが無効になっている場合 (no license smart privacy version グローバル コンフィギュレーション コマンド)、製品インスタンスで実行されている Cisco IOS-XE ソフトウェアバージョンとスマートエージェントのバージョンが RUM レポートに含まれます。</p> <p>RUM レポートからバージョン情報を除外するには、バージョンプライバシーを有効にする必要があります (license smart privacy version)。</p>

リリース	変更内容
Cisco IOS XE Cupertino 17.9.1a	<ul style="list-style-type: none"> • utility キーワードのサポートが導入されました。 license smart utility コマンドを設定して、製品インスタンスでユーティリティモードを有効にします。 MSLA があり、サブスクリプション ID 付きのライセンスを使用している場合は、ユーティリティモードを有効にする必要があります。 • すべてのデータプライバシー関連情報を送信する新しいメカニズムが導入されました。この情報は RUM レポートに含まれなくなりました。 データプライバシーが無効になっている場合 (no license smart privacy {all hostname version} グローバル コンフィギュレーション コマンド)、データプライバシー関連情報は、別の同期メッセージまたはオフラインファイルで送信されます。 • ホスト名情報の送信のサポートが導入されました。 ホスト名のプライバシー設定が無効になっている場合 (no license smart privacy hostname グローバル コンフィギュレーション コマンド)、ホスト名情報が別の同期メッセージまたはオフラインファイルで製品インスタンスから送信されます。実装したトポロジに応じて、ホスト名情報は CSSM、CSLU、または SSM オンプレミスによって受信されます。ホスト名情報は、対応するユーザーインターフェイスにも表示されます。 • vrf vrf_string キーワードが導入されました。 VRF がサポートされている製品インスタンスでは、license smart vrf vrf_string コマンドを設定して、すべてのライセンスデータを CSSM、CSLU、または SSM オンプレミスに送信できます。
Cisco IOS XE Dublin 17.10.1	<p>reservation キーワードのサポートが導入されました。</p> <p>[no] license smart reservation コマンドでは、サポート対象製品インスタンスの予約モードを有効または無効にします。</p>

使用上のガイドライン データプライバシー設定

プライバシー設定を無効にすると、実装したトポロジによって、受信者、および情報が宛先に到達する方法が決まります。

- 情報の受信者は、CSSM、CSLU、および SSM オンプレミスのうち 1 つ以上である可能性があります。プライバシー設定は、コントローラ (Cisco DNA Center) には影響を及ぼしません。

hostname キーワードの場合、CSSM、CSLU、または SSM オンプレミスがホスト名情報を受信すると、対応する UI にも表示されます (該当する場合)。その後、プライバシーを有効にすると、対応する UI は製品インスタンスの UDI の表示に戻ります。

- 情報の送信方法。

- 製品インスタンスが通信を開始するトポロジの場合、製品インスタンスは、CSSM、CSLU、または SSM オンプレミスへのメッセージでこの情報の送信を開始します。

製品インスタンスは、イベント（製品インスタンスの起動、ホスト名の変更、高可用性セットアップでのスイッチオーバー）の1つが発生するたびに送信されるホスト名を送信します。

- CSLU または SSM オンプレミスが通信を開始するトポロジの場合、対応するコンポーネントが製品インスタンスからのプライバシー情報の取得を開始します。

ホスト名は、CSLU または SSM オンプレミスで設定した頻度で取得されます。

- 製品インスタンスがエアギャップネットワークにあるトポロジの場合、**license smart save usage** 特権 EXEC コマンドの入力時に生成されるオフラインファイルにプライバシー情報が含まれます。



- (注) すべてのトポロジにおいて、データプライバシー関連情報は RUM レポートに含まれません。

データプライバシー関連情報は、送信または保存する前に製品インスタンスによって保存されないため、情報が送信される場合、送信時または保存時のデータプライバシー設定と一致することが保証されます。

通信障害とレポート

設定したレポート間隔 (**license smart usage interval interval_in_days** コマンド) によって、製品インスタンスが RUM レポートを送信する日時が決まります。スケジュールされた間隔が通信障害と一致する場合、製品インスタンスは、スケジュールされた時間が経過した後、最大4時間 RUM レポートの送信を試みます。(通信障害が続くために) それでもレポートを送信できない場合、システムは間隔を 15 分にリセットします。通信障害が解消されると、レポート間隔はユーザが最後に設定した値に戻ります。

通信障害の場合に表示される可能性があるシステムメッセージ

は、`%SMART_LIC-3-COMM_FAILED` です。このエラーの解決とレポート間隔値の復元については、「ポリシーを使用したスマートライセンスのトラブルシューティング」セクションを参照してください。

プロキシサーバーの受け入れ

license smart proxy {address address_hostname | portport} コマンドを設定するとき、Cisco IOS XE Bengaluru 17.6.1 以降、プロキシサーバーの受け入れ基準が変更されたことに注意してください。プロキシサーバーの応答のステータスコードのみがシステムによって検証され、理由フレーズは検証されません。RFC 形式は、`status-line = HTTP-version SP status-code SP reason-phrase CRLF` で、ステータスコードは 3 桁の数値コードになります。ステータス行の詳細については、[RFC 7230](#) の [セクション 3.1.2](#) を参照してください。

ユーティリティモードの設定

ユーティリティモードが有効になっていて (**license smart utility**)、サブスクリプション ID のないライセンスが使用されている場合、[%SMART_LIC-4-UTILITY_SUBSCRIPTION_LICENSE](#) システムメッセージが生成されます (ライセンスごとに 1 回、およびサブスクリプション ID が検出されない状態でライセンスを使用してから 30 日後に生成)。

この状況を解決するには、サブスクリプション ID が CSSM 内の正しいスマートアカウントとバーチャルアカウントに保存されていることを確認します。これにより、すべての通信に適宜フラグが設定されます。

ユーティリティモードをサポートするには、トランスポートタイプを次のいずれかのオプションに設定する必要があります。

- **smart** : 製品インスタンスが CSSM に直接接続されている場合。
- **cslu** : 製品インスタンスが CSSM、CSLU、または SSM オンプレミスに接続されている場合。
- **off** : 製品インスタンスがエアギャップネットワークにある場合。

VRF の使用

license smart vrf *vrf_string* グローバル コンフィギュレーション コマンドを使用する場合、実装するトポロジは、製品インスタンスが CSSM、CSLU、または SSM オンプレミスに接続されているトポロジである必要があります (VRF の使用時にサポートされるトランスポートタイプは、**smart** および **cslu** のみです)。

さらに、CSLU または SSM オンプレミスを介して CSSM に接続している場合は、製品インスタンス開始型通信のトポロジを実装する必要があります。CSLU または SSM オンプレミスは、CSSM に接続することも切断することもできます。

VRF を使用してライセンスデータを送信するには、サポートする他の VRF 設定も必要な場合があります、ネットワークによって異なります。詳細については、[IP ルーティング：プロトコル非依存コンフィギュレーションガイド](#)、[Cisco IOS XE 17 \[英語\]](#) を参照してください。

サンプルの VRF 設定については、以下の「例」を参照してください。

例

- [データプライバシーの例 \(274 ページ\)](#)
- [転送タイプと URL の例 \(275 ページ\)](#)
- [使用状況レポートのオプションの例 \(276 ページ\)](#)
- [VRF の使用例 \(277 ページ\)](#)

データプライバシーの例

次に、グローバル コンフィギュレーション モードで **license smart privacy** コマンドを使用してデータプライバシー関連情報を設定する例を示します。付随する **show license**

status の出力には、有効になっているプライバシーオプションと無効になっているプライバシーオプションが表示されます。



(注) **show** コマンドの出力は、特定のオプションが有効か無効かを示すだけです。

ここでは、データプライバシー関連の情報は送信されません。

```
Device# configure terminal
Device(config)# license smart privacy all
Device(config)# exit
Device# show license status
<output truncated>
Data Privacy:
  Sending Hostname: no
  Callhome hostname privacy: ENABLED
  Smart Licensing hostname privacy: ENABLED
  Version privacy: ENABLED
```

```
Transport:
  Type: Callhome
<output truncated>
```

ここでは、製品インスタンスから開始されるメッセージには、ホスト名は含まれ、バージョン情報は含まれません。製品インスタンスは CSSM に直接接続されています (トランスポートタイプは **smart** で、対応する URL があります)。

```
Device# configure terminal
Device(config)# license smart privacy version
Device(config)# no license smart privacy hostname
Device(config)# exit
```

```
Device# show license all
<output truncated>
```

```
Data Privacy:
  Sending Hostname: no
  Callhome hostname privacy: DISABLED
  Smart Licensing hostname privacy: ENABLED
  Version privacy: DISABLED
```

```
Transport:
  Type: Smart
  URL: https://smartreceiver.cisco.com/licservice/license
  Proxy:
    Not Configured
  VRF:
    Not Configured
```

```
<output truncated>
```

転送タイプと URL の例

次に、グローバル コンフィギュレーション モードで **license smart transport** および **license smart url** コマンドを使用して、転送タイプの一部を設定する例を示します。**show license all** 出力には、設定された情報が表示されます。

トランスポート **cslu** :

```

Device# configure terminal
Device(config)# license smart transport cslu
Device(config)# license smart url default
Device(config)# exit
Device# show license all
<output truncated>
Transport:
  Type: cslu
  Cslu address: http://192.168.0.1:8182/cslu/v1/pi
  Proxy:
    Not Configured
<output truncated>

```

トランスポート **smart** :

```

Device# configure terminal
Device(config)# license smart transport smart
Device(config)# license smart url smart https://smartreceiver.cisco.com/licservice/license
Device(config)# exit
Device# show license all
<output truncated>
Transport:
  Type: Smart
  URL: https://smartreceiver-stage.cisco.com/licservice/license
  Proxy:
    Not Configured
<output truncated>

```

使用状況レポートのオプションの例

次に、グローバル コンフィギュレーション モードで **license smart usage** コマンドを使用して、使用状況レポートの一部を設定する例を示します。 **show running-config** 出力には、設定された情報が表示されます。

customer-tag オプションの設定 :

```

Device# configure terminal
Device(config)# license smart usage customer-tags tag1 SA/VA:01
Device(config)# exit
Device# show running-config | include tag1
license smart usage customer-tags tag1 SA/VA:01

```

現在適用されているポリシーよりも絞り込んだレポート間隔の設定 :

```

Device# show license status
<output truncated>
Usage Reporting:
Last ACK received: Sep 22 13:49:38 2020 PST
Next ACK deadline: Dec 21 12:02:21 2020 PST
Reporting push interval: 30 days
Next ACK push check: Sep 22 12:20:34 2020 PST
Next report push: Oct 22 12:05:43 2020 PST
Last report push: Sep 22 12:05:43 2020 PST
Last report file write: <none>
<output truncated>

```

```

Device# configure terminal
Device(config)# license smart usage interval 20
Device(config)# exit

```

```

Device# show license status
<output truncated>

Usage Reporting:
Last ACK received: Sep 22 13:49:38 2020 PST
Next ACK deadline: Nov 22 12:02:21 2020 PST
Reporting push interval: 20 days
Next ACK push check: Sep 22 12:20:34 2020 PST
Next report push: Oct 12 12:05:43 2020 PST
Last report push: Sep 22 12:05:43 2020 PST
Last report file write: <none>
<output truncated>

```

VRF の使用例

ここでは、SLP_VRFを使用して、製品インスタンスからライセンスデータを送信しません。**license smart vrf vrf_string** コマンドは、ライセンスデータの送信に使用される VRF を指定するために使用されます。サポートする構成の残りの部分は、例を示すためのものです。

```

Device (config)# vrf definition SLP_VRF
Device (config-vrf)# address-family ipv4
Device (config-vrf-af)# exit
Device (config-vrf)# interface GigabitEthernet 0/0/0
Device (config-if)# no shutdown
Device (config-if)# vrf forwarding SLP_VRF
Device (config-if)# ip address 192.168.0.47 255.255.0.0
Device (config-if)# exit
Device (config)# ip route vrf SLP_VRF 0.0.0.0 0.0.0.0 192.168.0.1
Device (config)# ip name-server vrf SLP_VRF 173.37.137.85
Device (config)# license smart transport smart
Device (config)# license smart url https://smartreceiver.cisco.com/licservice/license
Device (config)# license smart vrf SLP_VRF
Device (config)# ip http client source-interface GigabitEthernet 0/0/0

```

license smart (特権 EXEC)

承認コードの要求または返却、リソース使用状況測定レポート (RUM レポート) の保存、製品インスタンスへのファイルのインポート、Cisco Smart Software Manager (CSSM) との信頼の確立、CSSM または Cisco Smart License Utility (CSLU)、あるいは Smart Software Manager オンプレミス (SSM オンプレミス) との製品インスタンスの同期、製品インスタンスからのライセンス情報の削除などのライセンス機能を設定するには、対応するキーワードまたは引数を指定して特権 EXEC モードで **license smart** コマンドを入力します。

```

license smart { authorization { request { add | replace | save filepath_filename } feature_name { all
| local } [ request_count ] | return { all | local } { offline [ filepath_filename ] | online } } | clear
eventlog | export return { all | local } feature_name | factory reset | import filepath_filename | renew
{ ID | auth } | reservation { cancel [ all | local ] | install { plr_code | file filepath_filename } |
request { all | local | universal } | return [ all | authorization { return_code | file filepath_filename
} | local ] } | save { trust-request filepath_filename | usage { all | days days | rum-id rum-ID |
unreported } { file filepath_filename } } | sync { all | local } | trust idtoken id_token_value { local
| all } [ { force } ] } }

```

構文の説明

smart	スマートライセンス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すオプションを提供します。
request	承認コードを CSSM、CSLU (CSLU は CSSM から承認コードを取得)、または SSM オンプレミスから要求し、そのコードを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	<p>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されます。</p> <p>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。</p>
save filepath_filename	<p>承認コード要求をファイルに保存します。</p> <p><i>filepath_filename</i> 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。</p>
<i>feature_name</i>	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。
<i>request_count</i>	ライセンス要求数を入力します。0 から 4294967295 までの値を入力してください。
return	CSSM のライセンスプールに承認コードを返します。
offline <i>filepath_filename</i>	<p>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。</p> <p><i>file_path</i> 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。</p>
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ス情報をクリアします。
import <i>filepath_filename</i>	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。 <i>filepath_filename</i> には、場所（ファイル名を含む）を指定します。
<pre>{ reservation { cancel [all local] install { plr_code file filepath_filename } request { all local universal } return [all authorization { return_code file filepath_filename } local] }</pre>	<p>予約設定を行います。次のいずれかのオプションを指定する必要があります。</p> <ul style="list-style-type: none"> • cancel [all local] : 承認コードがインストールされる前に予約リクエストをキャンセルします。生成した PLR 要求コードを使用しない場合は、このオプションを使用します。 • install {plr_code file filepath_filename} : PLR コードをインストールします。古い PLR コードバージョンが存在する場合は、インストールプロセス中に削除されます。 • request { all local universal } : 製品インスタンスで予約要求コードを生成します。 • return [all authorization local] : インストールされた PLR 承認コードを返却します。 <p>最初に製品インスタンスで予約要求コードを生成し、CSSM に要求コードを入力し、CSSM で PLR 承認コードを生成して、CSSM からコピーします。その後、このキーワードを使用して製品インスタンスに承認コードをインストールする必要があります。</p> <p>(注) universal キーワードは、CLI には表示されますが、廃止されており、サポートされていません。予約要求コードを生成するには、all を指定して高可用性構成内のすべての製品インスタンスに対してアクションを実行するか、local を指定して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。</p> <p>このコマンドを設定すると、CLI にリターンコードが表示されません。返却プロセスを完了するには、CSSM にこのリターンコードを入力する必要があります。</p>
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 <i>filepath_filename</i>	<p>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。</p> <p><i>filepath_filename</i> 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。</p>
usage { all days <i>days</i> rum-id <i>rum-ID</i> unreported } { file <i>filepath_filename</i> }	<p>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。</p> <ul style="list-style-type: none"> • all : すべての RUM レポートを保存します。 • days <i>days</i> : 過去 <i>n</i> 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 <i>rum-ID</i> : 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。 <p>file <i>filepath_filename</i> : 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。</p>
sync { all local }	<p>CSSM または CSLU、あるいは SSM オンプレミスと同期して、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。</p> <p>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。</p> <ul style="list-style-type: none"> • 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 <i>id_token_value</i>	<p>CSSM との信頼できる接続を確立します。</p> <p>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。<i>id_token_value</i> に生成されたトークン値を指定します。</p>

force	<p>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。</p> <p>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。</p>
--------------	---

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ス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
	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	<p>ポリシーを使用したスマートライセンスで、次のキーワードと変数が導入されました。</p> <ul style="list-style-type: none"> • authorization { request { add replace } <i>feature_name</i> { all local } return { all local } { offline [<i>path</i>] online } } • import <i>file_path</i> • save { trust-request <i>filepath_filename</i> usage { all days <i>days</i> rum-id <i>rum-ID</i> unreported } { file <i>file_path</i> } • sync { all local } • trust idtoken <i>id_token_value</i> { local all } [force] <p>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。</p> <ul style="list-style-type: none"> • register idtoken <i>token_id</i> [force] • renew id { ID auth } • debug { error debug trace all } • mfg reservation { request install install file cancel } • conversion { start stop }
	Cisco IOS XE Amsterdam 17.3.3	SSM オンプレミスのサポートが導入されました。承認コードの要求または返却、リソース使用状況測定レポート (RUMレポート) の保存、製品インスタンスへのファイルのインポート、製品インスタンスの同期、SSM オンプレミス展開での製品インスタンスからのライセンス情報の削除など、ライセンス関連のタスクを実行できます。

リリース	変更内容
Cisco IOS XE Cupertino 17.7.1a	<p>このリリースでは、次の機能拡張が導入されています。</p> <ul style="list-style-type: none"> • save path キーワードと変数が license smart authorization request コマンド文字列に追加されました。このオプションを使用して、SLAC 要求を生成し、ファイルに保存できます。新しいオプションは次のように表示されます。 <pre>license smart authorization request { add replace save path } feature_name { all local } [request_count]</pre> <ul style="list-style-type: none"> • 既存の license smart save usage コマンドは、信頼コード要求がまだ存在しない場合に自動的に含めるように拡張されました。
Cisco IOS XE Dublin 17.10.1	<p>reservation キーワードが復元されました。PLR コードをキャンセル、インストール、要求、および返却できます。</p>

使用上のガイドライン エアーギャップネットワークでの信頼コードの要求

Cisco IOS XE cupertino 17.7.1 a 以降、製品インスタンスで信頼コードが使用できない場合、**license smart save usage** コマンドを入力すると、製品インスタンスは自動的に RUM レポートに信頼コード要求を含めます。これは、スタンドアロン設定と高可用性設定でサポートされません。高可用性設定では、アクティブな製品インスタンスは、信頼コードが使用できないすべての接続製品インスタンスの信頼コードを要求します。CSSM の ACK には信頼コードが含まれており、CSSM Web UI からダウンロードできます。そして ACK を製品インスタンスにインストールする必要があります。信頼コードのインストールを確認するには、特権 EXEC モードで **show license status** コマンドを入力します。[Trust Code Installed] フィールドで更新されたタイムスタンプを確認します。

信頼コードの上書き

license smart trust idtoken コマンドを設定するときの **force** オプションの使用例：

- 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します。製品インスタンスが 1 つのアカウントから別のアカウントに移動した場合（たとえば、別のバーチャルアカウントの一部である高可用性設定に追加されたため）、既存の信頼コードを上書きすることが必要になる場合があります。
- 製品インスタンスに工場出荷時にすでにインストールされている信頼コードがありますが、製品インスタンスが CSSM に直接接続されているトポロジを実装する必要があります。工場出荷時にインストールされている信頼コードは、CSSM とのセキュア通信には使用できません。CSSM Web UI で ID トークンを生成し、信頼コードファイルをダウンロードする必要があります。この新しい信頼コードをインストールする場合は、工場出荷時にインストールされている既存の信頼コードを上書きする必要があります。

エアーギャップネットワークでの SLAC の要求と返却

Cisco IOS XE cupertino 17.7.1a 以降では、必要な PID を入力したり、CSSM Web UI で SLAC を生成したりせずに、SLAC を要求してインストールできます。代わりに、**license smart**

authorization request コマンドを設定し、その後に **license smart authorization request save** コマンドを設定して、SLAC 要求を製品インスタンスのファイルに保存します。SLAC 要求ファイルを CSSM (RUM レポートと同じ場所) にアップロードします。要求が処理されると、CSAC Web UI で SLAC ファイルを使用できるようになります。SLAC ファイルをダウンロードし、製品インスタンスにインポートします。

同様に、SLAC を返すには、**offline** キーワードを指定して **license smart authorization return** コマンドを設定し、ファイルを保存します。ファイルを CSSM にアップロードします (RUM レポートと同じ場所)。

認証コードの設定を確認するには、特権 EXEC モードで **show license authorization** コマンドを入力します。

ライセンス情報の削除

license smart factory reset コマンドを入力すると、承認コード、RUM レポートなど、すべてのライセンス情報 (使用中のライセンスを除く) 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、製品インスタンスを返却する場合 (Return Material Authorization (RMA))、または永続的にデコミットする場合にのみ使用することを推奨します。また、製品インスタンスからライセンス情報を削除する前に CSSM に RUM レポートを送信します。これは、CSSM に最新の使用状況情報が含まれていることを確認するためです。

SSM オンプレミス展開の承認コード

製品インスタンスで **license smart authorization request** コマンドを入力して SSM オンプレミスに SLAC を要求する前に、次の要件が満たされていることを確認します。

- 製品インスタンスを SSM オンプレミスに追加する必要があります。追加のプロセスで、製品インスタンスを検証して CSSM の該当するスマートアカウントとバーチャルアカウントにマッピングします。[スマートアカウントとバーチャルアカウントの割り当て \(SSM オンプレミス UI\) \(198 ページ\)](#) を参照してください。
- 輸出規制ライセンスと適用済みライセンスに必要な承認コードは、CSSM で生成し、SSM オンプレミスにインポートする必要があります。[承認コード要求の送信 \(SSM オンプレミス UI、切断モード\) \(205 ページ\)](#) を参照してください。

例

- 例 : SLAC の要求と SLAC の返却 (CSSM に直接接続) (284 ページ)
- 例 : SLAC の要求と SLAC への返却 (CSSM への接続なし、CSLU なし) (284 ページ)
- 例 : ライセンス使用状況情報の保存 (286 ページ)
- 例 : 信頼コードのインストール (286 ページ)

例：SLAC の要求と SLAC の返却（CSSM に直接接続）

次の例は、SLAC の CSSM を要求する方法と、CSAC に SLAC を返却する方法を示しています。ここでは、製品インスタンスは Cisco 4000 シリーズ サービス統合型ルータで、CSSM と通信するように設定されています。

SLAC の要求とインストール

```
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
```

SLAC の CSSM への返却：

```
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-CHcljc-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.
```

例：SLAC の要求と SLAC への返却（CSSM への接続なし、CSLU なし）

次の例は、SLAC で CSSM を要求する方法と、エアギャップネットワークの製品インスタンスから CSSM に SLAC を返却する方法も示しています。ここでは、製品インスタンスは、Cisco 4000 シリーズ サービス統合型ルータです。製品インスタンスで実行されているソフトウェアバージョンは Cisco IOS XE Cupertino 17.7.1a です。これにより、エアギャップネットワークで SLAC を要求し、返却する方法がより簡単になりました。

SLAC の要求

```
Device# license smart authorization request add hseck9 local
Device# license smart authorization request save bootflash:slac.txt
```

上記の手順の後、ファイルを CSSM にアップロードし、SLAC コードを含むファイルをダウンロードして、製品インスタンスにインストールします。CSSM で実行する必要がある手順については、「[CSSM へのデータまたは要求のアップロードとファイルのダウンロード \(229 ページ\)](#)」を参照してください。ファイルがダウンロードされたら、次の手順を実行します。

```
Device# copy tftp://10.8.0.6/user01/slac_code.txt bootflash:
Device# license smart import bootflash:slac_code.txt
```

SLAC の返却

```
Device# show license summary
Account Information:
  Smart Account: Eg-SA As of Oct 29 17:19:04 2021 UTC
  Virtual Account: EG-VA
```

```
License Usage:
License                               Entitlement Tag                               Count Status
-----
booster_performance                   (ISR_4431_BOOST)                             1 IN USE
appxk9                                 (ISR_4400_Application)                       1 IN USE
AdvUCSuiteK9                           (ISR_4400_AdvancedUCSuite)                   1 IN USE
Router US Export Lic...                 (DNA_HSEC)                                    0 NOT IN USE
ISR_4400_Hsec                           (ISR_4400_Hsec)                              0 NOT IN USE
```

```
Device# license smart authorization return local offline bootflash:auth_return.txt
*Nov 3 05:12:06.515: %SMART_LIC-6-AUTHORIZATION_REMOVED: A licensing authorization code
has been removed from PID:ISR4431/K9,SN:FOC22446T0U.
```

上記の手順の後、CSSM にファイルをアップロードします。CSSM で実行する必要がある手順については、「[CSSM へのデータまたは要求のアップロードとファイルのダウンロード \(229 ページ\)](#)」を参照してください。この後、ファイルをダウンロードできますが、このファイルのインポートとインストールはオプションです。

```
Device# show license authorization
Overall status:
  Active: PID:ISR4431/K9,SN:FOC22446T0U
  Status: NOT INSTALLED
  Last return code: CqAMzh-nsjvdh-ZZCnYK-4pELCF-cZgySA-yBiYgg-qBxfdm-ykmGms-QAT
```

```
Purchased Licenses:
  No Purchase Information Available
```

```
Device# show license summary
Account Information:
  Smart Account: Eg-SA As of Nov 03 05:02:01 2021 UTC
  Virtual Account: Eg-VA
```

```
License Usage:
License                               Entitlement Tag                               Count Status
-----
booster_performance                   (ISR_4431_BOOST)                             1 IN USE
appxk9                                 (ISR_4400_Application)                       1 IN USE
AdvUCSuiteK9                           (ISR_4400_AdvancedUCSuite)                   1 IN USE
```

例：ライセンス使用状況情報の保存

次の例は、製品インスタンスのライセンス使用状況情報を保存する方法を示しています。このオプションを使用して、エアギャップネットワークのレポート要件を満たすことができます。この例では、ファイルはまずフラッシュメモリに保存され、次に TFTP の場所にコピーされます。

```
Device> enable
Device# license smart save usage unreported file flash:RUM-unrep.txt
Device# copy flash:RUM-unrep.txt tftp://192.168.0.1//auto/tftp-user/user01/
Address or name of remote host [192.168.0.1]?
Destination filename [//auto/tftp-user/user01/RUM-unrep.txt]?
!!
15128 bytes copied in 0.161 secs (93963 bytes/sec)
```

RUM レポートをファイルに保存した後、（インターネットに接続しているワークステーションや Cisco から）CSSM にアップロードする必要があります。

例：信頼コードのインストール

次の例は、信頼コードがすでに製品インスタンスにインストールされている場合に、信頼コードをインストールする方法を示しています。これには、CSSM への接続が必要です。正常なインストール後の **show license status** 出力例を次に示します。

信頼コードをインストールする前に、ID トークンを生成し、CSSM から対応するファイルをダウンロードする必要があります。

結果を確認するには、**show license status** コマンド（Trust Code Installed:）を使用します。

```
Device> enable
Device# license smart trust idtoken
NGMwMjk5mYtNZaxMS00NzZmtgWm local force
Device# show license status
<output truncated>
Trust Code Installed:
  Active: PID:C9500-24Y4C,SN:CAT2344L4GH
          INSTALLED on Sep 04 01:01:46 2020 EDT
  Standby: PID:C9500-24Y4C,SN:CAT2344L4GJ
           INSTALLED on Sep 04 01:01:46 2020 EDT
<output truncated>
```

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ス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。
	Cisco IOS XE Cupertino 17.7.1a	コマンドの出力が強化され、次の情報が表示されるようになりました。 <ul style="list-style-type: none"> • RUM レポートの統計情報 ([Usage Report Summary] セクション)。 • [Account Information] セクションにあるスマートアカウントとバーチャルアカウントの情報。

使用上のガイドライン このコマンドは、他の **show license** コマンドの出力を連結して、さまざまな種類のライセンス情報をまとめて表示できるようにします。フィールドの説明については、以下に示すリンクから対応するコマンドを参照してください。

show license all コマンドの [Smart Licensing Status] セクションと [Account Information] セクションは、[show license status \(314 ページ\)](#) コマンドの出力に対応しています。

show license all コマンドの [License Usage] セクションは、[show license usage \(338 ページ\)](#) コマンドの出力に対応しています。

show license all コマンドの [Product Information] セクションは、[show license udi \(337 ページ\)](#) コマンドの出力に対応しています。

show license all コマンドの [Agent Version] セクションには、スマートエージェントのバージョンが表示され、このコマンドでのみ使用できます。

show license all コマンドの [License Authorizations] セクションは、[show license authorization \(292 ページ\)](#) コマンドの出力に対応しています

show license all コマンドの [Usage Report Summary] セクションは、[show license tech \(326 ページ\)](#) コマンドの出力に対応しています。

例

- 例 : [show license all \(Catalyst 8200 シリーズ エッジ プラットフォーム\) \(288 ページ\)](#)
- 例 : [show license all \(Cisco 4000 シリーズ サービス統合型ルータ\) \(290 ページ\)](#)

例 : show license all (Catalyst 8200 シリーズ エッジ プラットフォーム)

次に、ソフトウェアバージョンが Cisco IOS XE cupertino 17.7.1a である製品インスタンスの **show license all** コマンドの出力例を示します。このリリースでは、[Usage Report Summary] と [Usage Report Summary] の 2 つの新しいセクションが追加されています。

```
Device# show license all

Smart Licensing Status
=====

Smart Licensing is ENABLED

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

Export Authorization Key:
  Features Authorized:
    <none>

Utility:
  Status: DISABLED

Smart Licensing Using Policy:
  Status: ENABLED

Account Information:
  Smart Account: <none>
  Virtual Account: <none>

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

Transport:
  Type: cslu
  Cslu address: <empty>
  Proxy:
    Not Configured
  VRF:
    Not Configured

Miscellaneous:
  Custom Id: <empty>

Policy:
  Policy in use: Merged from multiple sources.
  Reporting ACK required: yes (CISCO default)
  Unenforced/Non-Export Perpetual Attributes:
    First report requirement (days): 365 (CISCO default)
    Reporting frequency (days): 0 (CISCO default)
    Report on change (days): 90 (CISCO default)
  Unenforced/Non-Export Subscription Attributes:
    First report requirement (days): 90 (CISCO default)
    Reporting frequency (days): 90 (CISCO default)
    Report on change (days): 90 (CISCO default)
  Enforced (Perpetual/Subscription) License Attributes:
    First report requirement (days): 0 (CISCO default)
    Reporting frequency (days): 0 (CISCO default)
```

```
Report on change (days): 0 (CISCO default)
Export (Perpetual/Subscription) License Attributes:
  First report requirement (days): 0 (CISCO default)
  Reporting frequency (days): 0 (CISCO default)
  Report on change (days): 0 (CISCO default)

Usage Reporting:
  Last ACK received: <none>
  Next ACK deadline: Jan 30 10:27:22 2022 UTC
  Reporting push interval: 30 days
  Next ACK push check: <none>
  Next report push: Nov 01 15:11:57 2021 UTC
  Last report push: <none>
  Last report file write: <none>

Trust Code Installed: <none>

License Usage
=====

network-advantage_250M (ESR_P_250M_A):
  Description: network-advantage_250M
  Count: 1
  Version: 1.0
  Status: IN USE
  Export status: NOT RESTRICTED
  Feature Name: network-advantage_250M
  Feature Description: network-advantage_250M
  Enforcement type: NOT ENFORCED
  License type: Perpetual

dna-advantage_250M (DNA_P_250M_A):
  Description: dna-advantage_250M
  Count: 1
  Version: 1.0
  Status: IN USE
  Export status: NOT RESTRICTED
  Feature Name: dna-advantage_250M
  Feature Description: dna-advantage_250M
  Enforcement type: NOT ENFORCED
  License type: Subscription

Product Information
=====
UDI: PID:C8200-1N-4T,SN:FGL2447LGZ1

Agent Version
=====
Smart Agent for Licensing: 5.3.15_rel/49

License Authorizations
=====
Overall status:
  Active: PID:C8200-1N-4T,SN:FGL2447LGZ1
  Status: NOT INSTALLED

Purchased Licenses:
  No Purchase Information Available

Usage Report Summary:
=====
Total: 6, Purged: 0
Total Acknowledged Received: 0, Waiting for Ack: 0
Available to Report: 6 Collecting Data: 2
```


例 : 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

Miscellaneous:
  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 8 : show license authorization のフィールドの説明 \(293 ページ\)](#) 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の HSECK9 \(296 ページ\)](#)
- [Cisco 1000 シリーズ サービス統合型ルータの HSECK9 PAK \(296 ページ\)](#)
- [Cisco 1000 シリーズ サービス統合型ルータの HSECK9 SLR \(298 ページ\)](#)
- [Cisco 4000 シリーズ サービス統合型ルータの HSEC、SLAC 以外 \(299 ページ\)](#)

SLAC が必要な場合の詳細については、[承認コード \(12 ページ\)](#) を参照してください。

表 8 : 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）。 高可用性設定では、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:	高可用性設定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	<p>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。</p> <p>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。</p>
():	ライセンス名およびライセンス名の短縮形。
説明	ライセンスの説明。
Total available count:	<p>使用可能なライセンスの合計数。</p> <p>これには、高可用性設定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。</p>
Enforcement type	<p>ライセンスの適用タイプ。これは、次のいずれかです。</p> <ul style="list-style-type: none"> • 適用 • 非適用 • 輸出制限（輸出規制と同様） <p>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（11 ページ） を参照してください。</p>
Term information:	

フィールド	説明												
	<p>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。</p> <ul style="list-style-type: none"> • 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。 • 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。 <p>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 (11 ページ) を参照してください。</p>												
Purchased Licenses	<p>ライセンス購入情報のヘッダー。</p> <table border="1" data-bbox="618 1402 1516 1797"> <tr> <td data-bbox="618 1402 808 1465">Active:</td> <td data-bbox="808 1402 1516 1465">アクティブ製品インスタンスとそのUDI。</td> </tr> <tr> <td data-bbox="618 1465 808 1528">Count:</td> <td data-bbox="808 1465 1516 1528">ライセンス数。</td> </tr> <tr> <td data-bbox="618 1528 808 1591">Description:</td> <td data-bbox="808 1528 1516 1591">ライセンスの説明。</td> </tr> <tr> <td data-bbox="618 1591 808 1686">License type:</td> <td data-bbox="808 1591 1516 1686">ライセンス継続期間。これは、SUBSCRIPTION または PERPETUAL です。</td> </tr> <tr> <td data-bbox="618 1686 808 1749">Standby:</td> <td data-bbox="808 1686 1516 1749">スタンバイ製品インスタンスのUDI。</td> </tr> <tr> <td data-bbox="618 1749 808 1797">Member:</td> <td data-bbox="808 1749 1516 1797">メンバー製品インスタンスのUDI。</td> </tr> </table>	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。
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の HSECK9

show license authorization 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に SLAC がインストールされている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
```

Cisco 1000 シリーズ サービス統合型ルータの HSECK9 PAK

show license authorization 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の HSECK9 PAK ライセンスを示しています。

出力の `Status: NOT INSTALLED` フィールドと `Status:PAK` フィールドには、SLAC がインストールされていないこと、および製品インスタンスが PAK ライセンスを使用する以前の Cisco ソフトウェアライセンス (CSL) 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スに移行されたことが示されています。[Legacy License Info] セクションにもこの情報が表示されます。

HSECK9 PAK ライセンスは移行後に有効になり、SLAC を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適用タイプに与える影響 \(37 ページ\)](#) を参照してください。

同じ製品インスタンスの付随する **show license usage** コマンド出力は、必要な承認が存在することを確認するのに役立ちます (`Export status: RESTRICTED - ALLOWED` および `License type: Perpetual`)。

```
Device# show license authorization

Overall status:

  Active: PID:C1111-8PLTEEAWB,SN:FGL214391J3
  Status: NOT INSTALLED
  Status:PAK

Legacy License Info:
  regid.2017-04.com.cisco.ISR_1100_8P_Application,1.0_c4cf42aa-2d60-4f4e-83dd-c5c9672132c9:
```

```
    DisplayName: appxk9
    Description: appxk9
    Total available count: 1
    Term information:
      Active: PID:C1111-8PLTEEAWB,SN:FGL214391J3
      License type: PERPETUAL
      Term Count: 1

regid.2017-04.com.cisco.ISR_1100_8P_Security,1.0_6b61b693-0daa-42d4-8cee-930de5c1b37c:

    DisplayName: securityk9
    Description: securityk9
    Total available count: 1
    Term information:
      Active: PID:C1111-8PLTEEAWB,SN:FGL214391J3
      License type: PERPETUAL
      Term Count: 1

regid.2017-08.com.cisco.ISR_1100_8P_Hsec,1.0_34a5e7e7-722a-41ab-bdad-d53d5a3cac14:
    DisplayName: hseck9
    Description: hseck9
    Total available count: 1
    Term information:
      Active: PID:C1111-8PLTEEAWB,SN:FGL214391J3
      License type: PERPETUAL
      Term Count: 1

Device# show license usage

License Authorization:
  Status: Not Applicable

hseck9 (ISR_1100_8P_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
  License type: Perpetual

appxk9 (ISR_1100_8P_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
  License type: Perpetual

securityk9 (ISR_1100_8P_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
```



```
License type: Perpetual
```

Cisco 1000 シリーズ サービス統合型ルータの HSECK9 SLR

Cisco 1000 シリーズ サービス統合型ルータの **show license authorization** コマンドの次の出力例は、HSECK9 ライセンスを含む特定のライセンス予約 (SLR) 承認コードを示しています。

出力の Status: SPECIFIC INSTALLED on Jan 19 05:59:54 2021 UTC フィールドおよび Last Confirmation code: 0708eeec フィールドには、SLR 承認コードがインストールされていることが示されています。[Specified license reservations] セクションには、HSECK9 ライセンス (ISR_1100_8P_Hsec) が含まれていることが示されています。これは、製品インスタンスが、予約済みライセンス (または SLR ライセンス) を使用する以前のスマートライセンス環境から、ポリシーを使用したスマートライセンスに移行され、HSECK9 ライセンスが含まれていることを示しています。

このシナリオでは、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適用タイプに与える影響 \(37 ページ\)](#) を参照してください。

同じ製品インスタンスの付随する **show license usage** コマンド出力は、必要な承認が存在することを確認するのに役立ちます (Export status: RESTRICTED - ALLOWED)。

```
Device# show license authorization
Overall status:
  Active: PID:C1111-8PLTEEAWB,SN:FGL214391JK
          Status: SPECIFIC INSTALLED on Jan 19 05:59:54 2021 UTC
          Last Confirmation code: 0708eeec

Specified license reservations:
  Cisco 1100 Series with 8 LAN Ports, Cisco One Foundation Suite
  (ISR_1100_8P_FoundationSuite):
    Description: Cisco 1100 Series with 8 LAN Ports, Cisco One Foundation Suite
    Total reserved count: 1
    Enforcement type: NOT ENFORCED
    Term information:
      Active: PID:C1111-8PLTEEAWB,SN:FGL214391JK
      Authorization type: SPECIFIC INSTALLED on Jan 19 05:59:54 2021 UTC
      License type: PERPETUAL
      Term Count: 1
  ISR_1100_8P_Hsec (ISR_1100_8P_Hsec):
    Description: Cisco 1100 Series with 8 LAN Ports, U.S. Export Restriction Compliance
    license
    Total reserved count: 1
    Enforcement type: EXPORT RESTRICTED
    Term information:
      Active: PID:C1111-8PLTEEAWB,SN:FGL214391JK
      Authorization type: SPECIFIC INSTALLED on Jan 19 05:59:54 2021 UTC
      License type: PERPETUAL
      Term Count: 1

Purchased Licenses:
  No Purchase Information Available

Derived Licenses:
  Entitlement Tag:
  regid.2017-08.com.cisco.ISR_1100_8P_Hsec,1.0_34a5e7e7-722a-41ab-bdad-d53d5a3cac14
```

```
Entitlement Tag:
regid.2018-12.com.cisco.ISR_1100_8P_UnifiedCommunication,1.0_55775cb5-538d-482e-b57f-fc8af02f93a3

Entitlement Tag:
regid.2017-04.com.cisco.ISR_1100_8P_FoundationSuite,1.0_6f4a1f6f-b607-45cb-8bd0-d672ac06a314

Device# show license usage

License Authorization:
  Status: Not Applicable

hseck9 (ISR_1100_8P_Hsec):
  Description: hseck9
  Count: 1
  Vecsion: 1.0
  Status: IN USE
  Export status: RESTRICTED - ALLOWED
  Feature Name: hseck9
  Feature Description: hseck9
  Enforcement type: EXPORT RESTRICTED
  License type: Perpetual
  Reservation:
    Reservation status: SPECIFIC EXPORT AUTHORIZATION KEY INSTALLED
    Total reserved count: UNLIMITED

uck9 (ISR_1100_8P_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
  License type: Perpetual
  Reservation:
    Reservation status: NOT INSTALLED

FoundationSuiteK9 (ISR_1100_8P_FoundationSuite):
  Description: FoundationSuiteK9
  count: 1
  Version: 1.0
  Status: IN USE
  Export status: NOT RESTRICTED
  Feature Name: FoundationSuiteK9
  Feature Description: FoundationSuiteK9
  Enforcement type: NOT ENFORCED
  License type: Perpetual
  Reservation:
    Reservation status: SPECIFIC INSTALLED
    Total reserved count: 1
```

Cisco 4000 シリーズ サービス統合型ルータの HSEC、SLAC 以外

show license authorization コマンドの次の出力例は、輸出規制機能または 250 Mbps を超えるスループットを使用していない Cisco 4000 シリーズ サービス統合型ルータのものであります。

出力の `status: NOT INSTALLED` フィールドには、SLAC がインストールされていないことが示されています。

同じ製品インスタンスの付随する **show license usage** コマンド出力は、この製品インスタンスで使用されているすべてのライセンスが適用されていないことを確認するのに役立ちます（すべてのライセンスに `Enforcement type: NOT ENFORCED` が表示されている）。したがって、SLAC をインストールする必要はありません。

```
Device# show license authorization
Overall status:
  Active: PID:ISR4351/K9,SN:FDO21512BJB
  Status: NOT INSTALLED

Purchased Licenses:
  No Purchase Information Available

Derived Licenses:
  Entitlement Tag:
regid.2015-01.com.cisco.ISR_4351_400M_Performance,1.0_79a9ccb4-d7c3-46fd-9980-7efe247c90e5

  Entitlement Tag:
regid.2015-01.com.cisco.ISR_4351_Application,1.0_601ccfff-5601-4293-98d2-2f653d864ce0
  Entitlement Tag:
regid.2014-12.com.cisco.ISR_4351_UnifiedCommunication,1.0_a04fec0e-e944-4096-bcf8-05d6e9a0a6d3

  Entitlement Tag:
regid.2014-12.com.cisco.ISR_4351_Security,1.0_df7d8d7f-b71a-4d3d-a9ab-aec7828a37a7

Device# show license usage
License Authorization:
  Status: Not Applicable

throughput (ISR_4351_400M_Performance):
  Description: throughput
  Count: 1
  Version: 1.0
  Status: IN USE
  Export status: NOT RESTRICTED
  Feature Name: throughput
  Feature Description: throughput
  Enforcement type: NOT ENFORCED
  License type: Perpetual

appxk9 (ISR_4351_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
  License type: Perpetual

uck9 (ISR_4351_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
  License type: Perpetual

securityk9 (ISR_4351_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
License type: Perpetual

```

show license data

ライセンスデータ転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 よりも前のこのコマンドが導入されました。リリースで導入されました。

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ス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	<p>ポリシーを使用したスマートライセンスの導入により、次のイベントが追加されました。</p> <ul style="list-style-type: none"> • 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 \(302 ページ\)](#)
- [例：すべてのイベントログ \(303 ページ\)](#)

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_CRYPT0 success="False" error="Crypto Initialization
has not been completed"
2020-09-22 20:23:27.702 UTC SAEVT_HA_EVENT eventType="SmartAgentEvtHArmRegister"
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="SmartAgentEvtHArmInitialize"
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="SmartAgentEvtHArmRegister"
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_CRYPT0 success="False" error="Crypto Initialization
has not been completed"
2020-09-22 20:24:26.120 UTC SAEVT_INIT_CRYPT0 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_CRYPT0 success="False" error="Crypto Initialization
has not been completed"
2020-09-22 20:39:27.798 UTC SAEVT_HA_EVENT eventType="SmartAgentEvtHArmRegister"
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="SmartAgentEvtHArmInitialize"
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="SmartAgentEvtHArmRegister"
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"
```

show license history message

```

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_CRYPT0 success="False" error="Crypto Initialization
has not been completed"
2020-09-22 20:40:34.458 UTC SAEVT_INIT_CRYPT0 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_CRYPT0 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
snc/csp/nto/ta/pt/a/tye/attant/attants/atoriz/ob/sum/ano/nc/ans/9/9/6/2/4/6/0/s/son/ta/5/0/0/2/4/1/2/0/3/sgae/saffice/atoriz/
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
snc/csp/nto/ta/pt/a/tye/attant/attants/atoriz/ob/sum/ano/nc/ans/9/9/6/2/4/6/0/s/son/ta/5/0/0/2/4/1/2/0/3/sgae/saffice/atoriz/
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	このコマンドにはキーワードまたは引数はありません。	
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。

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スの導入により、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。
	Cisco IOS XE Dublin 17.10.1	このリリースでは PLR のサポートの導入により、このコマンドが復元されました。

例

show licenseReservation : Smart Licensing Using Policy 環境にインストールされた PLR (シスコクラウドサービス ルータ 1000v)

次に、PLR がアクティブになっている製品インスタンスでの **show license reservation** コマンドの出力例を示します。

```
Devide# show license reservation
Overall status:
  Active: PID:CSR1000V,SN:9QLBLATKXM4
        Status: UNIVERSAL INSTALLED on Nov 09 00:12:18 2022 UTC
```

show license rum

製品インスタンスのリソース使用率測定レポート (RUM レポート) に関する情報を表示したり、レポート ID、レポートの現在の処理状態、エラー情報 (ある場合)、および表示された詳細または概要情報を保存するには、特権 EXEC モードで **show license rum** コマンドを入力します。

```
show license rum { feature { license_name | all } | id { rum_id | all } } [ detail ] [ save path ]
```

構文の説明

feature { license_name all }	ライセンス名に基づいて RUM レポート情報を表示します。 特定のライセンス名を指定してそのライセンスのすべての RUM レポートを表示するか、 all キーワードを使用して製品インスタンスで使用可能なすべての RUM レポートを表示します。
id { rum_id all }	RUM レポート ID に基づいて RUM レポート情報を表示します。 単一のレポートの情報を表示するレポート ID を指定するか、製品インスタンスで使用可能なすべての RUM レポートを表示するには、 all キーワードを使用します。
detail	詳細な RUM レポート情報を表示します。 これを使用して、ライセンス名ごとの詳細情報と RUM レポート ID ごとの詳細情報を表示できます。

save path	<p>表示される情報を保存します。これは簡易バージョンまたは詳細バージョンで、入力した先行キーワードによって異なります。</p> <p>200のRUMレポートに関する情報を表示できます。製品インスタンスに200を超えるRUMレポートがある場合は、テキスト(.txt)ファイルに保存することで、すべてのRUMレポートに関する情報を表示できます。</p> <p>(注) このオプションでは、RUMレポートに関する情報が保存され、レポート用ではありません。使用状況情報を含むXMLファイルであるRUMレポートは保存されません。</p>
------------------	--

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 Cupertino 17.7.1a	このコマンドが導入されました。

使用上のガイドライン 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。レポートのACKが製品インスタンスで使用可能になると、対応するRUMレポートが不要になり、削除できることが示されます。**show license rum** コマンドを使用すると、次のことができます。

- IDまたはライセンス名でフィルタリングされた、製品インスタンスで使用可能なRUMレポートに関する情報を表示します。
- 概要を表示するか、情報の詳細ビューを表示します。
- RUMレポートをそのライフサイクル全体(最初に生成されてからCSSMから確認されるまで)を追跡します。レポートの現在の処理状態と条件を表示することで、レポートワークフローに問題があるかどうか、また問題が発生した場合にはそれを確認できます。
- 表示された情報を保存します。CLIには、最大200のレポートに関する情報が表示されません。製品インスタンスに200を超えるレポートがあり、それらすべてに関する情報を表示する場合は、表示された情報を.txtファイルに保存し、表示する目的の場所にエクスポートします。

RUMレポート情報の統計ビュー(製品インスタンスのレポートの総数、対応するACKを含むレポートの数、ACKを待機しているレポートの数など)を表示するには、**show license all**および**show license tech** 特権 EXEC コマンドについては、[Usage Report Summary]セクションを参照してください。

show license tech コマンドは、RUM レポートに問題がある場合に、シスコ 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できる RUM レポート 関連情報も提供します。

例

ディスプレイに表示されるフィールドについては、「[表 9 : show license rum \(簡易ビュー\) のフィールド説明 \(308 ページ\)](#)」と「[表 10 : show license rum \(詳細ビュー\) のフィールド説明 \(309 ページ\)](#)」参照してください。

show license rum コマンドの例については、以下を参照してください。

- [show license rum feature : 簡易ビューと詳細ビュー \(311 ページ\)](#)
- [RUM レポートビューの保存 \(314 ページ\)](#)

表 9 : *show license rum* (簡易ビュー) のフィールド説明

フィールド名	説明
Report Id	RUM レポートを識別する数値フィールドです。製品インスタンスは、生成するすべての RUM レポートに ID を自動的に割り当てます。ID の長さは最大 20 文字です。
状態	このフィールドには、RUM レポートの現在の処理状態が表示され、次のいずれかになります。 <ul style="list-style-type: none"> • OPEN : 新しい測定値がレポートに追加されることを意味します。 • CLOSED : このレポートにそれ以上の測定値を追加できず、CSSM への通信の準備ができていることを意味します。 • PENDING : 送信中にレポートを閲覧した場合に表示される移行ステータスです。 • UNACK : レポートが送信され、CSSM からの確認を待っていることを意味します。 • ACK : レポートが CSSM によって処理または確認され、削除の対象となります。

フィールド名	説明
フラグ	<p>RUM レポートの状態を示し、文字の形式で表示されます。各文字は特定の条件を表し、次のいずれかの値になります。</p> <ul style="list-style-type: none"> • N : 正常。これは、エラーが検出されておらず、レポートが通常の動作を行っていることを意味します。 • P : 消去。これは、システムリソースの制限によりレポートが削除されたことを意味し、ディスク領域の不足またはメモリ不足を示している可能性があります。このフラグが表示された場合は、詳細ビューの [State Change Reason] フィールドを参照してください。 • E : エラー。これは、RUM レポートでエラーが検出されたことを意味します。このフラグが表示される場合、詳細情報については詳細ビューを参照してください。考えられるワークフローの問題には、次のものが含まれますが、これらに限定されません。 <ul style="list-style-type: none"> • RUM レポートが CSSM によってドロップされました。これが問題の場合、[State] フィールドに値 <code>ACK</code> が表示されますが、[State Change Reason] は <code>ACKED</code> に変更されません。 • RUM レポートデータがありません。これが問題の場合は、[Storage State] フィールドに値 <code>MISSING</code> が表示されます。 • 追跡情報がありません。この場合、[State] フィールドには値 <code>UNACK</code> が表示され、[Transaction ID] フィールドには情報がありません。 <p>(注) RUM レポートで時折発生するエラーは、ユーザーによる操作を必要とせず、問題を示すものではありません。シスコテクニカルサポートチームに連絡する必要があるのは、多数のレポート (10 を超える) にエラーがある場合だけです。</p>
機能名	RUM レポートが適用されるライセンスの名前です。

表 10: show license rum (詳細ビュー) のフィールド説明

フィールド名	説明
Report Id	RUM レポートを識別する数値フィールドです。製品インスタンスは、生成するすべての RUM レポートに ID を自動的に割り当てます。ID の長さは最大 20 文字です。

フィールド名	説明
Metric Name :	記録されるデータのタイプを示します。 RUM レポートの場合、唯一の可能な値は ENTITLEMENT で、ライセンスの使用状況の測定値を参照します。
Feature Name :	RUM レポートが適用されるライセンスの名前です。
メトリック値	記録されるデータの一意的識別子です。 これは、 show license tech コマンドの出力の「Entitlement Tag」と同じで、追跡対象のライセンスに関する情報が表示されます。
UDI	製品インスタンスの製品 ID (PID) とシリアル番号で構成されます。
Previous Report Id :	製品インスタンスがライセンスに対して生成した以前の RUM レポート ID です。
Next Report Id :	製品インスタンスがライセンス用に生成する次の RUM レポートに使用する ID です。
State:	RUM レポートの現在の処理状態を表示します。ここに表示される値は、簡易ビューに表示される値と常に同じです。 可能な値のリストについては、上記の「 表 9 : show license rum (簡易ビュー) のフィールド説明 (308 ページ) 」を参照してください。
State Change Reason :	RUM レポートの状態が変更された理由を表示します。すべての状態変更が理由を示すわけではありません。 <ul style="list-style-type: none"> • NONE : これは、RUM レポートが通常のライフサイクル (たとえば、OPEN→CLOSED→ACK) を通過していることを意味します。この状態変更の理由には、通常、簡易ビューで N フラグ (通常という意味) が表示され、ユーザーによる操作は必要ありません。 • ACKED : RUM レポートは CSSM によって正常に処理されました。 • REMOVED : RUM レポートを受信し、CSSM に削除するように要求されました。 • RELOAD : ある種のデバイスのリロードが原因で、RUM レポートの状態が変更されました。 • DECONFIG : ライセンスが設定から削除されました。
Start Time :	RUM レポートの測定開始および測定終了を示すタイムスタンプです。
End Time :	開始時刻と終了時刻を合わせて、測定の対象となる期間を指定します。

フィールド名	説明
Storage State :	<p>RUM レポートの現在のストレージ状態を表示します。次のいずれかの値になります。</p> <ul style="list-style-type: none"> • EXIST : RUM レポートのデータがストレージにあることを意味します。 • DELETED : データが意図的に削除されたことを意味します。このストレージ状態の詳細については、show license tech コマンドの出力の「Storage State Change Reason」を参照してください。 • PURGED : システムリソースの制限によりデータが削除されたことを意味します。このストレージ状態の詳細については、show license tech コマンドの出力の「Storage State Change Reason」を参照してください。 • MISSING : データがストレージから欠落していることを意味します。レポートが欠落していると識別された場合、リカバリプロセスはありません。
Transaction ID :	<p>RUM レポートの追跡情報が含まれます。この情報は、ポーリング情報または ACK インポート情報のいずれかである可能性があります。</p> <p>製品インスタンスが ACK のインポート時にエラーメッセージを受信した場合、トランザクションメッセージにはエラーメッセージが含まれます。</p> <p>これらのフィールドの情報は、RUM レポートの問題をトラブルシューティングする際に、シスコテクニカルサポートチームによって使用されます。</p>
Transaction Message :	

show license rum feature : 簡易ビューと詳細ビュー

次に、Cisco Catalyst 8300 ルータ (C8300-1N1S-4T2X) での **show license rum feature all** および **show license rum feature alldetail** コマンドの出力例を示します。

出力はフィルタ処理されて、製品インスタンスのすべてのライセンスにおける全 RUM レポート簡易ビューが表示され、その後すべてのライセンスにおける全 RUM レポート詳細ビューが表示されます。

```
Router# show license rum feature all
```

```
Smart Licensing Usage Report:
=====
Report Id,          State,   Flag,  Feature Name
1638518477         UNACK   N      network-advantage_10M
1638518478         UNACK   N      dna-advantage_10M
1638518479         ACK     E      network-advantage_10M
1638518480         ACK     E      dna-advantage_10M
1638518482         ACK     N      network-advantage_T2
1638518483         ACK     N      dna-advantage_T2
```

show license rum

```

1638518484      ACK      N      hseck9
1638518485      OPEN     N      network-advantage_T2
1638518486      OPEN     N      dna-advantage_T2
1638518487      OPEN     N      hseck9

```

Router# **show license rum feature all detail**

Smart Licensing Usage Report Detail:

```

=====
Report Id: 1638518477
  Metric Name: ENTITLEMENT
  Feature Name: network-advantage_10M
  Metric Value:
regid.2018-12.com.cisco.ESR_P_10M_A,1.0_8946a476-b904-4d0a-9d0b-2b1e5de891a3
  UDI: PID:C8300-1N1S-4T2X,SN:FDO2250A0J5
  Previous Report Id: 0,      Next Report Id: 1638518479
  State: UNACK,      State Change Reason: REPORTING
  Start Time: Dec 03 08:12:05 2021 UTC,      End Time: Dec 03 08:12:06 2021 UTC
  Storage State: EXIST
  Transaction ID: 715896687973761034
  Transaction Message: <none>

Report Id: 1638518478
  Metric Name: ENTITLEMENT
  Feature Name: dna-advantage_10M
  Metric Value:
regid.2018-12.com.cisco.DNA_P_10M_A,1.0_7f2e8a7a-e74d-4d71-af46-1ae7b3faf320
  UDI: PID:C8300-1N1S-4T2X,SN:FDO2250A0J5
  Previous Report Id: 0,      Next Report Id: 1638518480
  State: UNACK,      State Change Reason: REPORTING
  Start Time: Dec 03 08:12:05 2021 UTC,      End Time: Dec 03 08:12:06 2021 UTC
  Storage State: EXIST
  Transaction ID: 715896687973761034
  Transaction Message: <none>

Report Id: 1638518479
  Metric Name: ENTITLEMENT
  Feature Name: network-advantage_10M
  Metric Value:
regid.2018-12.com.cisco.ESR_P_10M_A,1.0_8946a476-b904-4d0a-9d0b-2b1e5de891a3
  UDI: PID:C8300-1N1S-4T2X,SN:FDO2250A0J5
  Previous Report Id: 1638518477,      Next Report Id: 0
  State: ACK,      State Change Reason: DROPPED
  Start Time: Dec 03 08:12:06 2021 UTC,      End Time: Dec 03 08:24:19 2021 UTC
  Storage State: EXIST
  Transaction ID: 0
  Transaction Message: Report already received.

Report Id: 1638518480
  Metric Name: ENTITLEMENT
  Feature Name: dna-advantage_10M
  Metric Value:
regid.2018-12.com.cisco.DNA_P_10M_A,1.0_7f2e8a7a-e74d-4d71-af46-1ae7b3faf320
  UDI: PID:C8300-1N1S-4T2X,SN:FDO2250A0J5
  Previous Report Id: 1638518478,      Next Report Id: 0
  State: ACK,      State Change Reason: DROPPED
  Start Time: Dec 03 08:12:06 2021 UTC,      End Time: Dec 03 08:24:19 2021 UTC
  Storage State: EXIST
  Transaction ID: 0
  Transaction Message: Report already received.

Report Id: 1638518482
  Metric Name: ENTITLEMENT

```

```
Feature Name: network-advantage_T2
Metric Value:
regid.2020-10.com.cisco.NWSTACK_T2_A,1.0_83edc508-0ee4-468e-8962-0a4fde995e80
UDI: PID:C8300-1N1S-4T2X,SN:FDO2250A0J5
Previous Report Id: 0, Next Report Id: 1638518485
State: ACK, State Change Reason: ACKED
Start Time: Dec 03 08:29:31 2021 UTC, End Time: Dec 03 08:29:32 2021 UTC
Storage State: DELETED
Transaction ID: 0
Transaction Message: Report already received.

Report Id: 1638518483
Metric Name: ENTITLEMENT
Feature Name: dna-advantage_T2
Metric Value:
regid.2020-10.com.cisco.DSTACK_T2_A,1.0_b072e613-aa2c-4ed0-ab46-ae91ddc7dfb5
UDI: PID:C8300-1N1S-4T2X,SN:FDO2250A0J5
Previous Report Id: 0, Next Report Id: 1638518486
State: ACK, State Change Reason: ACKED
Start Time: Dec 03 08:29:31 2021 UTC, End Time: Dec 03 08:29:32 2021 UTC
Storage State: DELETED
Transaction ID: 0
Transaction Message: Report already received.

Report Id: 1638518484
Metric Name: ENTITLEMENT
Feature Name: hseck9
Metric Value: regid.2019-03.com.cisco.DNA_HSEC,1.0_509c41ab-05a8-431f-95fe-ec28086e8844

UDI: PID:C8300-1N1S-4T2X,SN:FDO2250A0J5
Previous Report Id: 0, Next Report Id: 1638518487
State: ACK, State Change Reason: ACKED
Start Time: Dec 03 08:29:31 2021 UTC, End Time: Dec 03 08:29:32 2021 UTC
Storage State: DELETED
Transaction ID: 0
Transaction Message: Report already received.

Report Id: 1638518485
Metric Name: ENTITLEMENT
Feature Name: network-advantage_T2
Metric Value:
regid.2020-10.com.cisco.NWSTACK_T2_A,1.0_83edc508-0ee4-468e-8962-0a4fde995e80
UDI: PID:C8300-1N1S-4T2X,SN:FDO2250A0J5
Previous Report Id: 1638518482, Next Report Id: 0
State: OPEN, State Change Reason: None
Start Time: Dec 03 08:29:32 2021 UTC, End Time: Dec 07 01:45:57 2021 UTC
Storage State: EXIST
Transaction ID: 0
Transaction Message: <none>

Report Id: 1638518486
Metric Name: ENTITLEMENT
Feature Name: dna-advantage_T2
Metric Value:
regid.2020-10.com.cisco.DSTACK_T2_A,1.0_b072e613-aa2c-4ed0-ab46-ae91ddc7dfb5
UDI: PID:C8300-1N1S-4T2X,SN:FDO2250A0J5
Previous Report Id: 1638518483, Next Report Id: 0
State: OPEN, State Change Reason: None
Start Time: Dec 03 08:29:32 2021 UTC, End Time: Dec 07 01:45:57 2021 UTC
Storage State: EXIST
Transaction ID: 0
Transaction Message: <none>

Report Id: 1638518487
```


show license status

```

Metric Name: ENTITLEMENT
Feature Name: hseck9
Metric Value: regid.2019-03.com.cisco.DNA_HSEC,1.0_509c41ab-05a8-431f-95fe-ec28086e8844

UDI: PID:C8300-1N1S-4T2X,SN:FDO2250A0J5
Previous Report Id: 1638518484, Next Report Id: 0
State: OPEN, State Change Reason: None
Start Time: Dec 03 08:29:32 2021 UTC, End Time: Dec 07 01:45:57 2021 UTC
Storage State: EXIST
Transaction ID: 0
Transaction Message: <none>

```

RUM レポートビューの保存

次の例は、**show license rum feature all** コマンドの簡易ビューを保存する方法を示しています。

feature キーワードと **all** キーワードを使用すると、出力がフィルタ処理され、製品インスタンスで使用されているすべてのライセンスにおける全 RUM レポートが表示されます。その後、テキストファイルを開いて情報を表示できる場所に転送できます。

```

Device# show license rum feature all save bootflash:all-rum-stats.txt
Device# copy bootflash:all-rum-stats.txt tftp://10.8.0.6/user01/

```

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ス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。
	Cisco IOS XE Cupertino 17.7.1a	コマンド出力が更新され、スマートアカウントと仮想アカウントの情報が表示されるようになりました。

使用上のガイドライン 出力のアカウント情報

Cisco IOS XE Cupertino 17.7.1a 以降、すべての ACK には、CSSM で報告されたスマートアカウントとバーチャルアカウントが含まれています。ACK を受信すると、製品インスタンスにはこの情報の最新バージョンのみが安全に保存されます。これは、ACK のタイムスタンプによって決定されます。したがって、このコマンドの出力の [Account Information] セクションに表示されるスマートアカウントとバーチャルアカウントの情報は、常に製品インスタンスで使用可能な最新の ACK に基づいています。

製品インスタンスが1つのスマートアカウントとバーチャルアカウントから別のアカウントに移動された場合、移動後の次の ACK にはこの更新された情報が含まれます。この ACK が製品インスタンスで使用可能になると、このコマンドの出力が更新されます。

ACK は、直接的に（製品インスタンスが CSSM に接続されている場合）または間接的に（製品インスタンスが CSLU、Cisco DNA Center、または SSM On-Prem を介して CSSM に接続されている場合）、あるいは手動で ACK をインポートすることによって（製品インスタンスがエアギャップネットワークにある場合）受信することができます。



- (注) 製品インスタンスが Cisco vManage によって管理されている場合、アカウント情報は表示されません。この場合、アカウント情報は維持され、Cisco vManage メニューの [License Management] ページに表示されます。

例

ディスプレイに表示されるフィールドについては、表 11 : show license status のフィールドの説明 (316 ページ) を参照してください。

出力例については、次を参照してください。

- 例 : show license status (Cisco Catalyst 8300 シリーズ エッジ プラットフォーム) (321 ページ)
- 例 : show license status (Cisco 4000 シリーズ サービス統合型ルータ) (322 ページ)。

表 11 : show license status のフィールドの説明

フィールド	説明	
ユーティリティ	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。	
	ステータス :	Status
	ユーティリティレポート :	最後の試行結果 :
	顧客情報 :	次のフィールドが表示されます。 <ul style="list-style-type: none"> • ID: • Name: • Street • City: • State: • Country: • Postal Code:
ポリシーを使用したスマートライセンス	製品インスタンスのポリシー設定のヘッダー。	
	ステータス :	ポリシーを使用したスマートライセンス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スは、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。
アカウント情報 :	製品インスタンスが属するアカウント情報のヘッダー (CSSM内)。 このセクションは、製品インスタンスのソフトウェアバージョンが Cisco IOS XE cupertino 17.7.1a以降のリリースの場合にのみ表示されません。 製品インスタンスに ACK がインストールされていない場合、次のフィールドには <none> が表示されます。	
	スマートアカウント:	製品インスタンスが属するスマートアカウント。この情報は、常に製品インスタンスで使用可能な最新の ACK に基づいています。
	バーチャルアカウント:	製品インスタンスが属するバーチャルアカウント。この情報は、常に製品インスタンスで使用可能な最新の ACK に基づいています。

フィールド	説明
データプライバシー :	<p>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。</p> <p>送信ホスト名 :</p>
トランスポート :	<p>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。</p> <p>Type:</p>

フィールド	説明
ポリシー :	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。
使用中のポリシー :	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。
ポリシー名 :	ポリシーの名前
レポートの ACK が必要 :	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。 <ul style="list-style-type: none"> • 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。その後ポリシー名が続きます
Subscription Attributes:	サブスクリプションライセンスのポリシー値。 <ul style="list-style-type: none"> • 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。その後ポリシー名が続きます
Enforced 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。 <ul style="list-style-type: none"> 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。その後ポリシー名が続きます。
	Export License Attributes:	サブスクリプションライセンスのポリシー値。 <ul style="list-style-type: none"> 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。その後ポリシー名が続きます。
その他	カスタム ID のヘッダー。	
	カスタム ID :	ID

フィールド	説明
使用状況レポート :	使用状況レポート (RUM レポート) 情報のヘッダー。
最後に受信した ACK :	最後に受信した ACK の日時 (ローカルタイムゾーン)。
次の ACK 期限 :	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。
レポート間隔 :	日単位のレポート間隔 ここに表示される値は、 license smart usage intervalinterval_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) (261 ページ) で対応する構文の説明を参照してください。
次の ACK プッシュチェック :	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。
次のレポートプッシュ :	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。
最後のレポートプッシュ :	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。
最後のレポートファイル書き込み :	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。
最後のレポートプル :	

フィールド	説明
	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。
インストール済みの信頼コード:	<p>信頼コード関連情報のヘッダー。</p> <p>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。</p> <p>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。</p>
Active:	<p>アクティブ製品インスタンス。</p> <p>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。</p>
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 : show license status (Cisco Catalyst 8300 シリーズ エッジ プラットフォーム)

次に、ソフトウェアバージョンが Cisco IOS XE cupertino 17.7.1a である製品インスタンスの **show license status** コマンドの出力例を示します。最後にインストールされた ACK のアカウント情報が表示されます (ACK 最終受信日 : 2021 年 12 月 3 日 8 時 34 分 58 秒 (UTC))。

```

Device# show license status

Utility:
  Status: DISABLED

Smart Licensing Using Policy:
  Status: ENABLED

Account Information:
  Smart Account: Eg-SA As of Dec 03 15:26:02 2021 UTC
  Virtual Account: Eg-VA

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

Transport:
  Type: Smart
  URL: https://smartreceiver.cisco.com/licservice/license
  Proxy:
    Not Configured
    
```



```

VRF:
  Not Configured

Policy:
  Policy in use: Installed On Dec 03 08:23:45 2021 UTC
  Policy name: SLE Policy
  Reporting ACK required: yes (Customer Policy)
  Unenforced/Non-Export Perpetual Attributes:
    First report requirement (days): 30 (Customer Policy)
    Reporting frequency (days): 60 (Customer Policy)
    Report on change (days): 60 (Customer Policy)
  Unenforced/Non-Export Subscription Attributes:
    First report requirement (days): 120 (Customer Policy)
    Reporting frequency (days): 111 (Customer Policy)
    Report on change (days): 111 (Customer Policy)
  Enforced (Perpetual/Subscription) License Attributes:
    First report requirement (days): 30 (Customer Policy)
    Reporting frequency (days): 90 (Customer Policy)
    Report on change (days): 60 (Customer Policy)
  Export (Perpetual/Subscription) License Attributes:
    First report requirement (days): 30 (Customer Policy)
    Reporting frequency (days): 30 (Customer Policy)
    Report on change (days): 30 (Customer Policy)

Miscellaneous:
  Custom Id: <empty>

Usage Reporting:
  Last ACK received: Dec 03 08:34:58 2021 UTC
  Next ACK deadline: Jan 02 08:34:58 2022 UTC
  Reporting push interval: 30 days
  Next ACK push check: Dec 07 08:31:32 2021 UTC
  Next report push: Jan 02 08:30:57 2022 UTC
  Last report push: Dec 03 08:30:57 2021 UTC
  Last report file write: <none>

Trust Code Installed: Dec 03 08:23:45 2021 UTC

```

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

次に、Cisco 4000 シリーズ サービス統合型ルータでの **show license status** コマンドの出力例を示します。

```

Device# show license status

Utility:
  Status: DISABLED

Smart Licensing Using Policy:
  Status: ENABLED

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

Transport:
  Type: Smart
  URL: https://smartreceiver.cisco.com/licservice/license
  Proxy:
    Not Configured

```

```

Policy:
  Policy in use: Installed On Oct 29 21:43:33 2020 UTC
  Policy name: SLP Policy
  Reporting ACK required: yes (Customer Policy)
  Unenforced/Non-Export Perpetual Attributes:
    First report requirement (days): 60 (Customer Policy)
    Reporting frequency (days): 60 (Customer Policy)
    Report on change (days): 60 (Customer Policy)
  Unenforced/Non-Export Subscription Attributes:
    First report requirement (days): 30 (Customer Policy)
    Reporting frequency (days): 30 (Customer Policy)
    Report on change (days): 30 (Customer Policy)
  Enforced (Perpetual/Subscription) License Attributes:
    First report requirement (days): 0 (CISCO default)
    Reporting frequency (days): 90 (Customer Policy)
    Report on change (days): 90 (Customer Policy)
  Export (Perpetual/Subscription) License Attributes:
    First report requirement (days): 0 (CISCO default)
    Reporting frequency (days): 90 (Customer Policy)
    Report on change (days): 90 (Customer Policy)

Miscellaneous:
  Custom Id: <empty>

Usage Reporting:
  Last ACK received: Oct 23 23:36:38 2020 UTC
  Next ACK deadline: Dec 22 23:36:38 2020 UTC
  Reporting push interval: 30 days
  Next ACK push check: Oct 30 05:45:45 2020 UTC
  Next report push: Nov 22 23:32:38 2020 UTC
  Last report push: Oct 23 23:32:38 2020 UTC
  Last report file write: <none>

Trust Code Installed: Oct 09 17:56:19 2020 UTC
    
```

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

構文の説明

このコマンドにはキーワードまたは引数はありません。

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。

リリース	変更内容
Cisco IOS XE Amsterdam 17.3.2	<p>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ス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。</p> <p>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。</p> <p>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。</p>
Cisco IOS XE Cupertino 17.7.1a	<p>コマンド出力が更新され、スマートアカウントと仮想アカウントの情報が表示されるようになりました。</p>

使用上のガイドライン 出力のアカウント情報

Cisco IOS XE Cupertino 17.7.1a 以降、すべての ACK には、CSSM で報告されたスマートアカウントとバーチャルアカウントが含まれています。ACK を受信すると、製品インスタンスにはこの情報の最新バージョンのみが安全に保存されます。これは、ACK のタイムスタンプによって決定されます。したがって、このコマンドの出力の [Account Information] セクションに表示されるスマートアカウントとバーチャルアカウントの情報は、常に製品インスタンスで使用可能な最新の ACK に基づいています。

製品インスタンスが1つのスマートアカウントとバーチャルアカウントから別のアカウントに移動された場合、移動後の次の ACK にはこの更新された情報が含まれます。この ACK が製品インスタンスで使用可能になると、このコマンドの出力が更新されます。

ACK は、直接的に（製品インスタンスが CSSM に接続されている場合）または間接的に（製品インスタンスが CSLU、Cisco DNA Center、または SSM On-Prem を介して CSSM に接続されている場合）、あるいは手動で ACK をインポートすることによって（製品インスタンスがエアギャップネットワークにある場合）受信することができます。



- (注) 製品インスタンスが Cisco vManage によって管理されている場合、アカウント情報は表示されません。この場合、アカウント情報は維持され、Cisco vManage メニューの [License Management] ページに表示されます。

例

ディスプレイに表示されるフィールドについては、[表 12 : show license summary のフィールドの説明 \(325 ページ\)](#) を参照してください。

出力例については、次を参照してください。

- [例 : show license summary : アカウント情報の表示 \(Catalyst 8200 シリーズ エッジ プラットフォーム\) \(325 ページ\)](#)

- 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) (326 ページ)

表 12: show license summary のフィールドの説明

フィールド	説明
アカウント情報: Smart Account: Virtual Account:	製品インスタンスが属するスマートアカウントとバーチャルアカウント情報は、常に製品インスタンスで使用可能な最新の ACK に基づいて表示されます。このフィールドは、製品インスタンスのソフトウェアバージョンが Cupertino 17.7.1a 以降のリリースの場合にのみ表示されます。製品インスタンスに ACK がインストールされていない場合は <none> が表示されます。
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
Status	ライセンスのステータスは次のいずれかになります。 <ul style="list-style-type: none"> • 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 のインストールを意味します。詳細については、承認コード (326 ページ) をご覧ください。

例 : show license summary : アカウント情報の表示 (Catalyst 8200 シリーズ エッジ プラットフォーム)

次に、ソフトウェアバージョンが Cisco IOS XE cupertino 17.7.1a である製品インスタンスの show license summary コマンドの出力例を示します。

Device# show license summary

```
Account Information:
  Smart Account: Eg-SA As of Dec 03 15:26:02 2021 UTC
  Virtual Account: Eg-VA
```

```
License Usage:
License                               Entitlement Tag                Count Status
-----
network-advantage_T2                 (NWSTACK_T2_A)                1 IN USE
dna-advantage_T2                     (DSTACK_T2_A)                 1 IN USE
Router US Export Lic... (DNA_HSEC)                    1 IN USE
```

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。

```

Device# show license summary
License Usage:
  License                               Entitlement tag                Count Status
  -----
  hsec9                                  (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 { message | rum { feature { license_name | all } | id { rum_id | all } } [ detail ]
[ save path ] | support }

```

構文の説明

message	信頼の確立、使用状況レポート、結果のポーリング、承認コードの要求と返却、および信頼の同期に関するメッセージを表示します。 これは、 show license history message コマンドの出力に表示される情報と同じです。
rum { feature { license_name all } id { rum_id all } } [detail] [save path]	製品インスタンスのリソース使用率測定レポート (RUM レポート) に関する情報を表示します。これには、レポートID、レポートの現在の処理状態、エラー情報 (ある場合)、および表示された RUM レポート情報を保存するオプションが含まれます。 (注) このオプションでは、RUM レポートに関する情報が保存され、レポート用ではありません。使用状況情報を含む XML ファイルである RUM レポートは保存されません。
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。
	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スに適用可能な新しいフィールドが反映されました。
	Cisco IOS XE Cupertino 17.7.1a	<p>rum キーワードおよびこのキーワードの下に追加のオプションが追加されました。</p> <pre>{ feature { license_name all } id { rum_id all } }</pre> <p>show license tech support コマンドの出力が強化され、次の情報が表示されるようになりました。</p> <ul style="list-style-type: none"> • [License Usage] と [Usage Report Summary] セクションに記載されている RUM レポート情報。 • [Account Information:] セクションにあるスマートアカウントとバーチャルアカウント情報。 <p>data conversion、eventlog、および reservation キーワードがこのコマンドから削除されました。これらは引き続き、個別の show コマンド、つまり、show license data、show license eventlog、および show license reservation として使用できます。</p>

使用上のガイドライン

[Smart Licensing] : デバイス上のソフトウェアバージョンが Cisco IOS XE Amsterdam 17.3.1 以前のリリースの場合、コマンド出力にはスマートライセンスに関連するフィールドが表示されず（スマートライセンスが有効になっているかどうか、関連するすべてのライセンス証明書、コンプライアンスステータスなど）。

[Smart Licensing Using Policy] : デバイス上のソフトウェアバージョン（製品インスタンスとも呼ばれる）が Cisco IOS XE Amsterdam 17.3.2 以降のリリースの場合、コマンド出力には Smart Licensing Using Policy に関連するフィールドが表示されます。次のガイドラインに留意してください。

- サポート担当者によるトラブルシューティング

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。

- 出力の RUM レポート情報

- **show license tech support** コマンドの出力には、RUM レポートに関する次のセクションが表示されます。

表 13 : show license tech support : ヘッダー「ライセンスの使用状況」のフィールドの説明 (328 ページ)

```
<output truncated>
License Usage
=====
Measurements:
  ENTITLEMENT:
    Interval: 00:15:00
    Current Value: 1
    Current Report: 1638518487      Previous: 1638518484
<output truncated>
```

表 13: show license tech support : ヘッダー「ライセンスの使用状況」のフィールドの説明

フィールド名	説明
Interval:	これは固定の測定時間で、常に 15 分です。
Current Value:	現在のライセンス数に関する情報。
Current Report:	ライセンスの現在 OPEN レポートの ID。
Previous:	ライセンスの最後の OPEN レポートの ID。このレポートのステータスは現在 CLOSED です。

- 表 14 : show license tech support : ヘッダー「使用状況レポートの概要」のフィールドの説明 (328 ページ)

```
<output truncated>
Usage Report Summary:
=====
Total: 10, Purged: 0(0)
Total Acknowledged Received: 3, Waiting for Ack: 2(7)
Available to Report: 3 Collecting Data: 3
Maximum Display: 10 In Storage: 7, MIA: 0(0)
Report Module Status: Ready
<output truncated>
```

表 14: show license tech support : ヘッダー「使用状況レポートの概要」のフィールドの説明

フィールド名	説明
Total:	製品インスタンスが生成したレポートの合計数。 (注) この合計は、製品インスタンスで現在使用可能であり、追跡されているレポートの合計数を示すものではありません。このためには、[Total Acknowledged Received:] フィールドと [Available to Report] フィールドを合計する必要があります。

フィールド名	説明
Purged:	システムリソースの制限により削除されたレポートの数。この数には、製品インスタンスにトラッキング情報がない RUM レポートが含まれます。
Total Acknowledged Received:	この製品インスタンスで確認された RUM レポートの数。
Waiting for Ack:	ACK を待機している RUM レポートの数。これは、UNACK 状態のレポートの総数です。この場合、製品インスタンスにはトラッキング情報があります。
Available to Report:	CSSM に送信可能な RUM レポートの数。これは、OPEN または CLOSED 状態のレポートの総数です。この場合、製品インスタンスにはトラッキング情報があります。
Collecting Data:	製品インスタンスが現在測定値を収集しているレポートの数。
Maximum Display:	show コマンドの出力に表示できるレポートの数。
In Storage:	ディスクに現在保存されているレポートの数。
MIA:	欠落しているレポートの数。

- **detail** オプションを指定した **show license tech rum** コマンドの出力には、RUM レポートに関する次のフィールドが表示されます：[表 15 : show license tech rum : ヘッダー「スマートライセンスの使用状況レポート詳細」のフィールドの説明 \(330ページ\)](#)

```
<output truncated>
Smart Licensing Usage Report Detail:
=====
Report Id: 1638518477
  Metric Name: ENTITLEMENT
  Feature Name: network-advantage_10M
  Metric Value:
regid.2018-12.com.cisco.ESR_P_10M_A,1.0_8946a476-b904-4d0a-9d0b-2b1e5de891a3
UDI: PID:C8300-1N1S-4T2X,SN:FDO2250A0J5
Previous Report Id: 0,      Next Report Id: 1638518479
Version: 2.0
State: UNACK,      State Change Reason: REPORTING
Start Time: Dec 03 08:12:05 2021 UTC,      End Time: Dec 03 08:12:06 2021 UTC

Storage State: EXIST, Storage State Change Reason: None
Transaction ID: 715896687973761034
Transaction Message: <none>
Report Size: 1129 (947)
<output truncated>
```

show license tech rum キーワードで使用できるオプションは、**show license rum** 特権 EXEC コマンドで使用できるオプションと同じです。簡易ビューに表示される出力例

も同じです。ただし、**detail** キーワードを使用する場合（たとえば、**show license tech rum feature license_name detail** を入力する場合）、詳細ビューが表示され、**show license rum** と比較していくつかの追加フィールドがあります。

表 15: **show license tech rum** : ヘッダー「スマートライセンスの使用状況レポート詳細」のフィールドの説明

フィールド名	説明
Version:	<p>送信中のレポートの形式を表示します。</p> <p>Cisco IOS XE cupertino 17.7.1a 以降、RUM レポートは処理時間を短縮する新しい形式で保存されます。このフィールドは、製品インスタンスが古い形式を使用しているか、新しい形式を使用しているかを示します。</p>
Storage State:	<p>特定のレポートが現在ストレージにあるかどうかを示します。</p> <p>RUM レポートの現在のストレージ状態の表示に加えて、EXIST、DELETED、PURGED、MISSING の各値が表示されます。ラベルの横に「(1)」が表示されている場合 (Storage State (1))、RUM レポートは古い (17.7.1a より前の) 形式であり、それに応じて処理されます。RUM レポートが新しい形式の場合、フィールドは [Storage State] として表示され、追加情報はありません。</p>
Storage State Change Reason:	<p>ストレージの状態が変化した理由を表示します。すべての状態変更が理由を示すわけではありません。</p> <ul style="list-style-type: none"> • NONE : これは、ストレージの状態変更の理由が記録されなかったことを意味します。 • PROCESSED : これは、CISCO がデータを処理した後に RUM レポートが削除されたことを意味します。 • LIMIT_STORAGE : これは、製品インスタンスがストレージ制限に達したため、RUM レポートが削除されたことを意味します。 • LIMIT_TIME : これは、レポートが永続的な時間制限に達したため、RUM レポートが削除されたことを意味します。

フィールド名	説明
Transaction ID: Transaction Message:	トランザクション ID に関連 ID が表示され、エラーステータスが表示される場合、製品インスタンスのこのセクションにエラーコードフィールドが表示されます。エラーがない場合、データはここに表示されません。
Report Size	このフィールドには 2 つの数字が表示されます。最初の数値は、通信の raw レポートのサイズ (バイト単位) です。2 番目の数値は、レポートの保存に使用されるディスク容量 (バイト単位) です。2 番目の数値は、レポートが新しい形式で保存されている場合にのみ表示されます。

例

[Catalyst 8300 シリーズ エッジ プラットフォームでの show license tech support \(331 ページ\)](#)

Catalyst 8300 シリーズ エッジ プラットフォームでの show license tech support

次に、Cisco IOS XE cupertino 17.7.1a を実行している Catalyst 8300 シリーズ エッジルータでの **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: True
  Status: Not started

Export Authorization Key:
  Features Authorized:
    <none>

Utility:
  Status: DISABLED

Smart Licensing Using Policy:
  Status: ENABLED

Account Information:
  Smart Account: Eg-SA As of Dec 03 15:26:02 2021 UTC
  Virtual Account: Eg-VA

Data Privacy:
  Sending Hostname: yes
  Callhome hostname privacy: DISABLED
```

```

Smart Licensing hostname privacy: DISABLED
Version privacy: DISABLED

Transport:
Type: Smart
URL: https://smartreceiver.cisco.com/licservice/license
Proxy:
  Address: <empty>
  Port: <empty>
  Username: <empty>
  Password: <empty>
Server Identity Check: True
VRF: <empty>

Miscellaneous:
  Custom Id: <empty>

Policy:
Policy in use: Installed On Dec 03 08:23:45 2021 UTC
Policy name: SLE Policy
Reporting ACK required: yes (Customer Policy)
Unenforced/Non-Export Perpetual Attributes:
  First report requirement (days): 30 (Customer Policy)
  Reporting frequency (days): 60 (Customer Policy)
  Report on change (days): 60 (Customer Policy)
Unenforced/Non-Export Subscription Attributes:
  First report requirement (days): 120 (Customer Policy)
  Reporting frequency (days): 111 (Customer Policy)
  Report on change (days): 111 (Customer Policy)
Enforced (Perpetual/Subscription) License Attributes:
  First report requirement (days): 30 (Customer Policy)
  Reporting frequency (days): 90 (Customer Policy)
  Report on change (days): 60 (Customer Policy)
Export (Perpetual/Subscription) License Attributes:
  First report requirement (days): 30 (Customer Policy)
  Reporting frequency (days): 30 (Customer Policy)
  Report on change (days): 30 (Customer Policy)

Usage Reporting:
Last ACK received: Dec 03 08:34:58 2021 UTC
Next ACK deadline: Jan 02 08:34:58 2022 UTC
Reporting push interval: 30 days State(4) InPolicy(30)
Next ACK push check: Dec 07 08:31:32 2021 UTC
Next report push: Jan 02 08:30:57 2022 UTC
Last report push: Dec 03 08:30:57 2021 UTC
Last report file write: <none>

License Usage
=====
Handle: 1
  License: network-advantage_T2
  Entitlement Tag:
regid.2020-10.com.cisco.NWSTACK_T2_A,1.0_83edc508-0ee4-468e-8962-0a4fde995e80
  Description: network-advantage_T2
  Count: 1
  Version: 1.0
  Status: IN USE(15)
  Status time: Dec 03 08:28:54 2021 UTC
  Request Time: Dec 03 08:28:54 2021 UTC
  Export status: NOT RESTRICTED
  Feature Name: network-advantage_T2
  Feature Description: network-advantage_T2
  Enforcement type: NOT ENFORCED
  License type: Perpetual

```

```
Measurements:
  ENTITLEMENT:
    Interval: 00:15:00
    Current Value: 1
    Current Report: 1638518485      Previous: 1638518482
    Soft Enforced: True

Handle: 2
  License: dna-advantage_T2
  Entitlement Tag:
  regid.2020-10.com.cisco.DSTACK_T2_A,1.0_b072e613-aa2c-4ed0-ab46-ae91ddc7dfb5
  Description: dna-advantage_T2
  Count: 1
  Version: 1.0
  Status: IN USE(15)
  Status time: Dec 03 08:28:54 2021 UTC
  Request Time: Dec 03 08:28:54 2021 UTC
  Export status: NOT RESTRICTED
  Feature Name: dna-advantage_T2
  Feature Description: dna-advantage_T2
  Enforcement type: NOT ENFORCED
  License type: Subscription
  Measurements:
    ENTITLEMENT:
      Interval: 00:15:00
      Current Value: 1
      Current Report: 1638518486      Previous: 1638518483
      Soft Enforced: True

Handle: 3
  License: Router US Export Lic. for DNA
  Entitlement Tag:
  regid.2019-03.com.cisco.DNA_HSEC,1.0_509c41ab-05a8-431f-95fe-ec28086e8844
  Description: U.S. Export Restriction Compliance license for DNA based Routers
  Count: 1
  Version: 1.0
  Status: IN USE(15)
  Status time: Dec 03 08:28:57 2021 UTC
  Request Time: Dec 03 08:28:57 2021 UTC
  Export status: RESTRICTED - ALLOWED
  Feature Name: hseck9
  Feature Description: hseck9
  Enforcement type: EXPORT RESTRICTED
  License type: Export
  Measurements:
    ENTITLEMENT:
      Interval: 00:15:00
      Current Value: 1
      Current Report: 1638518487      Previous: 1638518484

Product Information
=====
UDI: PID:C8300-1N1S-4T2X,SN:FDO2250A0J5

Agent Version
=====
Smart Agent for Licensing: 5.3.16_rel/55

Upcoming Scheduled Jobs
=====
Current time: Dec 07 02:12:02 2021 UTC
Daily: Dec 07 08:28:52 2021 UTC (6 hours, 16 minutes, 50 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: Dec 07 08:31:32 2021 UTC (6 hours, 19 minutes, 30 seconds
remaining)
Start Utility Measurements: Dec 07 02:15:57 2021 UTC (3 minutes, 55 seconds remaining)
Send Utility RUM reports: Jan 02 08:30:56 2022 UTC (26 days, 6 hours, 18 minutes, 54
seconds remaining)
Save unreported RUM Reports: Dec 07 03:01:07 2021 UTC (49 minutes, 5 seconds remaining)
Process Utility RUM reports: Dec 07 08:39:57 2021 UTC (6 hours, 27 minutes, 55 seconds
remaining)
External Event: Jan 02 08:34:57 2022 UTC (26 days, 6 hours, 22 minutes, 55 seconds
remaining)
Operational Model: Expired Not Rescheduled

Communication Statistics:
=====
Communication Level Allowed: DIRECT
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=1, Success=1, Fail=0  Ongoing Failure: Overall=0 Communication=0
  Last Response: OK_POLL on Dec 03 08:30:56 2021 UTC
  Failure Reason: <none>
  Last Success Time: Dec 03 08:30:56 2021 UTC
  Last Failure Time: <none>
Result Polling:
  Attempts: Total=5, Success=1, Fail=4  Ongoing Failure: Overall=3 Communication=0
  Last Response: INVALID STATUS CODE on Dec 06 08:31:32 2021 UTC
  Failure Reason: Invalid Polling Id 4294967295 provided in the polling request
  Last Success Time: Dec 03 08:34:58 2021 UTC
  Last Failure Time: Dec 06 08:31:32 2021 UTC
Authorization Request:
  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>
Authorization Confirmation:
  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>
Authorization Return:
  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 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=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>

License Certificates
=====
Production Cert: True
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:C8300-1N1S-4T2X, SN:FDO2250A0J5
Reservation status: SMART AUTHORIZATION INSTALLED on Dec 03 08:24:35 2021 UTC
Request code: <none>
Last return code: <none>
Last Confirmation code: 418b11b3
Reservation authorization code:
<smartLicenseAuthorization><udi>P:C8300-1N1S-4T2X,S:FDO2250A0J5</udi><authorizationCode><customerInfo><smartAccount>EU
Production
Router US Export Lic. for DNA (DNA_HSEC) (U.S. Export Restriction Compliance license for DNA based Routers)
US Export Lic. for DNA</displayName><tagDescription>U.S. Export Restriction Compliance
license for DNA based
Routers)

Authorizations:
Router US Export Lic. for DNA (DNA_HSEC):
Description: U.S. Export Restriction Compliance license for DNA based Routers
Total available count: 1
Enforcement type: EXPORT RESTRICTED
Term information:
Active: PID:C8300-1N1S-4T2X, SN:FDO2250A0J5
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

Usage Report Summary:
=====
Total: 10, Purged: 0(0)
Total Acknowledged Received: 3, Waiting for Ack: 2(7)
Available to Report: 3 Collecting Data: 3

```

```
Maximum Display: 10 In Storage: 7, MIA: 0(0)
Report Module Status: Ready

Other Info
=====
Software ID: regid.2020-05.com.cisco.C8300BE,1.0_5b66594f-27ab-4615-9d15-4aad4969497f
Agent State: authorized
TS enable: True
Transport: Smart
  Default URL: https://smartreceiver.cisco.com/licservice/license
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: True
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
SAPuginMgmtInterfaceMutex: True
SAPuginMgmtIPDomainName: True
SmartTransportVRFSupport: True
SmartAgentClientWaitForServer: 2000
SmartAgentCmRetrySend: True
SmartAgentClientIsUnified: True
SmartAgentCmClient: True
SmartAgentClientName: UnifiedClient
builtInEncryption: True
enableOnInit: True
routingReadyByEvent: True
systemInitByEvent: True
SmartTransportServerIdCheck: True
SmartTransportProxySupport: True
SmartAgentPolicyDisplayFormat: 0
SmartAgentReportOnUpgrade: False
SmartAgentIndividualRUMEncrypt: 2
SmartAgentMaxRumMemory: 50
SmartAgentConcurrentThreadMax: 10
SmartAgentPolicyControllerModel: False
SmartAgentPolicyModel: True
SmartAgentFederalLicense: True
SmartAgentMultiTenant: False
attr365DayEvalSyslog: True
checkPointWriteOnly: False
```

```

SmartAgentDelayCertValidation: False
enableByDefault: False
conversionAutomatic: True
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: 11 KB
Local Device: P:C8300-1N1S-4T2X,S:FDO2250A0J5, state[2], Trust Data INSTALLED TrustId:256
Overall Trust: INSTALLED (2)
Clock sync-ed with NTP: False

Platform Provided Mapping Table
=====
C8300-1N1S-4T2X: Total licenses found: 2595
Enforced Licenses:
P:C8300-1N1S-4T2X,S:FDO2250A0J5:
  hseck9: regid.2019-03.com.cisco.DNA_HSEC,1.0_509c41ab-05a8-431f-95fe-ec28086e8844
(3)
  hseck9: (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	特権 EXEC (Device#)				
コマンド履歴	<table border="1"> <thead> <tr> <th>リリース</th> <th>変更内容</th> </tr> </thead> <tbody> <tr> <td></td> <td>このコマンドは、Cisco IOS XE Amsterdam 17.3.2 よりも前のこのコマンドが導入されました。リリースで導入されました。</td> </tr> </tbody> </table>	リリース	変更内容		このコマンドは、Cisco IOS XE Amsterdam 17.3.2 よりも前のこのコマンドが導入されました。リリースで導入されました。
リリース	変更内容				
	このコマンドは、Cisco IOS XE Amsterdam 17.3.2 よりも前のこのコマンドが導入されました。リリースで導入されました。				

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**（338 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**（338 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	<p>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ス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。</p> <p>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。</p>

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 16 : show license usage のフィールドの説明 \(339 ページ\)](#) 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) (340 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) (341 ページ)

表 16 : 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。
():	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、カウントしません。
Version	バージョン。

フィールド	説明
Status	<p>ライセンスのステータスは次のいずれかになります。</p> <ul style="list-style-type: none"> • 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 のインストールを完了することを意味します。詳細については、承認コード (12 ページ) をご覧ください。
Export Status:	<p>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。そのステータスのいずれかが表示されます。</p> <ul style="list-style-type: none"> • 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。
Enforcement type	<p>ライセンスの適用タイプのステータス。これは、次のいずれかになります。</p> <ul style="list-style-type: none"> • ENFORCED • NOT ENFORCED • EXPORT RESTRICTED - ALLOWED • EXPORT RESTRICTED - NOT ALLOWED <p>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 (強制) タイプ (11 ページ)</p>

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。

show platform software sl-infra { 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スिंगのトラブルシューティング

- [システム メッセージの概要 \(343 ページ\)](#)
- [ポリシーを使用したスマートライセンスングのシステムメッセージ \(345 ページ\)](#)

システム メッセージの概要

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スングに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グインサーバ）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、状態のシビラティ（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 17: メッセージのシビラティ (重大度)

シビラティ (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 18: メッセージの変数フィールド

シビラティ (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

シビラティ (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スのシステムメッセージ

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ス関連の発生する可能性のある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
- %SMART_LIC-4-UTILITY_TRUST_CODE
- %SMART_LIC-4-UTILITY_SUBSCRIPTION_LICENSE
- %SMART_LIC-4-UTILITY_NO_ACK
- %SMART_LIC-4-UTILITY_TRANSPORT_NOT_CONFIG
- %SMART_LIC-3-UTILITY_REPORT_FAILED
- %SMART_LIC-3-UTILITY_STARTED
- %SMART_LIC-6-UTILITY_STOPPED

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。

- 署名の不一致：これは、システムクロックが正確でないことを意味します。
- タイムスタンプの不一致：製品インスタンスのシステムクロックがCSSMと同期していないことを意味します。

推奨するアクション：

考えられる両方の失敗の理由に関しては、システムクロックが正確で、CSSMと同期していることを確認します。**ntp server** コマンドをグローバルコンフィギュレーションモードで設定します。次に例を示します。

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

前述の手順を実行しても、ポリシーのインストールが失敗する場合は、シスコのテクニカルサポート担当者にお問い合わせください。

```
-----
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番目の[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。

- 現在設定されている機能の承認に必要な十分なライセンスがない：これは、必要なすべてのライセンスに必須の承認が生成されていないことを意味します。
- 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ていません。複数のUDIの承認コードを生成した場合、高可用性セットアップでは、承認コードファイルにリストされているすべてのUDIが、高可用性セットアップのすべてのUDIと一致する必要があります。一致しない場合、インストールは失敗します。

次のように、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（スタンダー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：これは、システムクロックが正確でないことを意味します。

推奨処置

- **show license tech support** コマンドの出力で、Failure Reason: フィールドを確認し、失敗した理由を確認します。

```
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承認に必要な十分なライセンスがない、およびUDIの不一致：

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。その後、次のタスクを再度実行します。[CSSMからのSLACの生成とファイルへのダウンロード \(214ページ\)](#) と [製品インスタンスへのファイルのインストール \(231ページ\)](#)

- 署名の不一致：

システムクロックが正確で、CSSM と同期していることを確認します。確認するためには、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
```

前述の手順を実行しても、ポリシーのインストールが失敗する場合は、シスコのテクニカルサポート担当者にお問い合わせください。

```
-----
Error Message %SMART_LIC-3-COMM_FAILED: Communications failure with the [chars] :
[chars]
```

説明： CSSM、CSLU、または SSM オンプレミスのいずれかとのスマートライセンス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 番目の [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、CSLU、または SSM オンプレミスに到達できない：これは、ネットワーク到達可能性に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。
- クライアント証明書が見つからないことにより、TLS または SSL ハンドシェイクが失敗している。証明書は、通信の両側の TLS 認証に必要です。最近のサーバーのアップグレー

ドにより、証明書が削除された可能性があります。これは、製品インスタンスが CSSM に直接接続されているトポロジにのみ当てはまる理由です。



- (注) この理由によりエラーメッセージが表示された場合、CSSM との通信において実際の設定エラーや中断はありません。

正インスタンスが RUM レポートの送信を開始するトポロジ (CSLU を介して CSSM に接続 : 製品インスタンス開始型通信、CSSM から切断されている CSSM、CSLU への直接接続 : 製品インスタンス開始型通信、および SSM オンプレミス展開 : 製品インスタンス開始型通信) では、この通信障害メッセージがスケジュールされたレポート (**license smart usage interval interval_in_days** グローバル コンフィギュレーション コマンド) と一致している場合は、製品インスタンスはスケジュールされた時間が経過した後、最大 4 時間にわたって RUM レポートを送信しようとします。(通信障害が続くために) それでもレポートを送信できない場合、システムは間隔を 15 分にリセットします。通信障害が解消されると、レポート間隔は最後に設定された値に戻ります。

推奨するアクション :

CSSM に到達できない場合、クライアント証明書がない場合、CSLU に到達できない場合、および SSM オンプレミスに到達できない場合のトラブルシューティング手順を示します。

- クライアント証明書がなく、CSSM との通信に実際の設定エラーや中断がない場合 :

グローバル コンフィギュレーション モードで **ip http client secure-trustpoint trustpoint-name** コマンドを設定します。trustpoint-name には、SLA-TrustPoint だけを入力します。このコマンドでは、セキュア HTTP クライアントが trustpoint-name 引数で示されたトラストポイントに関連付けられた証明書を使用する必要があることを指定します。

- CSSM が到達不能で、設定されている転送タイプが smart の場合 :

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
```

- CSSM が到達不能で、設定されている転送タイプが callhome の場合 :

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. 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
```

3. 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
```

前述の方法で解決しない場合は、製品インスタンスの IP ネットワークが稼働している確認します。ネットワークが稼働していることを確認するには、インターフェイスコンフィギュレーションモードで **no shutdown** コマンドを設定します。

デバイスがサブネット IP でサブネットマスクされているかどうか、および DNS IP が設定されているかどうかを確認します。

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。

現在の設定を表示するには、特権 EXEC モードで **show ip http client** コマンドを使用します。グローバル コンフィギュレーションモードで **ip http client source-interface** コマンドを使用して、再設定します。

上記の方法で解決しない場合は、ルーティングルール、およびファイアウォール設定を再確認します。

- CSLU に到達できない場合：

1. CSLU 検出が機能するかどうかを確認します。

- `cslu-local` のゼロタッチ DNS 検出またはドメインの DNS 検出。

show license all コマンドの出力で、`Last ACK received:` フィールドを確認します。このフィールドに最新のタイムスタンプがある場合は、製品インスタンスが CSLU と接続されていることを意味します。ない場合は、次のチェックに進みます。

製品インスタンスが `cslu-local` に対して `ping` を実行できるかどうかを確認します。`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。

上記の方法で解決しない場合は、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** コマンドと **ip name-server server-address** コマ

ドを設定します。この例では、CSLU IPは192.168.0.1で、name-serverによってエントリ `cslu-local.example.com` が作成されます。

```
Device(config)# ip domain name example.com
Device(config)# ip name-server 192.168.0.1
```

- CSLU URL が設定されています。

show license all コマンド出力の `Transport:` ヘッダーで、次の点を確認します。
`Type:` は `cslu` で、`Cslu address:` は CSLU をインストールした Windows ホストのホスト名または IP アドレスになっている必要があります。残りのアドレスが下記のように設定されているかどうかを確認するとともに、ポート番号が 8182 であるかどうかを確認します。

```
Transport:
Type: cslu
Cslu address: http://192.168.0.1:8182/cslu/v1/pi
```

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 transport cslu** および **license smart url cslu http://<cslu_ip_or_host>:8182/cslu/v1/pi** コマンドを設定します。

2. CSLU 開始型通信の場合、上記の CSLU 検出チェックに加えて、次の点を確認します。

HTTP 接続を確認します。特権 EXEC モードで **show ip http server session-module** コマンドを使用します。出力の `HTTP server current connections:` ヘッダーで、`SL_HTTP` がアクティブになっていることを確認します。[CSLU 開始型通信のネットワーク到達可能性の確認 \(182 ページ\)](#) で説明されているとおりに **ip http** コマンドが再設定されていない場合は、次の手順を実行します。

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。

- SSM オンプレミスに到達できない場合：

1. 製品インスタンス開始型通信の場合は、SSM オンプレミスのトランスポートタイプと URL が正しく設定されているかどうかを確認します。

show license all コマンドの出力の `Transport:` ヘッダーの下で、`Type:` が `cslu` であり、`Cslu address:` には、SSM オンプレミスにインストールしたサーバのホスト名または IP アドレスと、デフォルトのローカルバーチャルアカウントの `<tenantID>` があることを確認します。次の例を参照してください。

```
Transport:
Type: cslu
Cslu address: https://192.168.0.1/cslu/v1/pi/on-prem-default
```

SSM オンプレミスの正しい URL があることを確認し ([トランスポート URL の取得 \(SSM オンプレミス UI\) \(203 ページ\)](#) を参照)、次に、グローバル コンフィギュレーション モードで **license smart transport cslu** コマンドと **license smart url cslu http://<ip>/cslu/v1/pi/<tenant ID>** コマンドを設定します。

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 (200 ページ) に記載されているように、ネットワークに必要な他のコマンドが設定されていることを確認します。

2. SSM オンプレミス開始型通信の場合は、HTTPS 接続を確認します。

特権 EXEC モードで **show ip http server session-module** コマンドを使用します。出力の HTTP server current connections: ヘッダーで、SL_HTTP がアクティブになっていることを確認します。SSM オンプレミス開始型通信のネットワーク到達可能性の確保 (209 ページ) で説明されているとおりに **ip http** コマンドが再設定されていない場合は、次の手順を実行します。

3. トラストポイントと証明書が受け入れられることを確認します。

SSM オンプレミス展開の両方の通信形式で、正しいトラストポイントが使用され、必要な証明書が受け入れられることを確認します。

```
Device(config)# crypto pki trustpoint SLA-TrustPoint
Device(ca-trustpoint)#
Device(ca-trustpoint)# enrollment terminal
Device(ca-trustpoint)# revocation-check none
Device(ca-trustpoint)# end
Device# copy running-config startup-config
```

上記がうまくいかず、通信障害が続く場合は、シスコのテクニカルサポート担当者にお問い合わせください。

```
-----
-----
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、CSLU、または SSM オンプレミスのいずれか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したカスタムライセンスポリシーが削除されました。Cisco default ポリシーが自動的に有効になります。これにより、スマートライセンスの動作が変更される可能性があります。

失敗の理由として次が考えられます。

特権 EXEC モードで **license smart factory reset** コマンドを入力すると、ポリシーを含むすべてのライセンス情報が削除されます。

推奨するアクション：

ポリシーが意図的に削除された場合、それ以上のアクションは不要です。

ポリシーが誤って削除された場合は、ポリシーを再適用できます。実装したトポロジに応じて、該当するメソッドに従ってポリシーを取得します。

• CSSM に直接接続：

show license status を入力し、Trust Code Installed: フィールドを確認します。信頼が確立されると、CSSMは再度ポリシーを自動的に返します。ポリシーは、対応する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再インストールされます。

信頼が確立されていない場合は、次のタスクを実行します。[CSSMからの信頼コード用新規トークンの生成 \(227 ページ\)](#) および [ID トークンによる信頼の確立 \(227 ページ\)](#) これらのタスクを完了すると、CSSMは再度ポリシーを自動的に返します。その後、バーチャルアカウントのすべての製品インスタンスにポリシーが自動的にインストールされます。

• CSLU を介して CSSM に接続：

- 製品インスタンス開始型通信の場合は、特権 EXEC モードで **license smart sync** コマンドを入力します。同期要求により、CSLU は欠落している情報 (ポリシーまたは承認コード) を製品インスタンスにプッシュします。

- CSLU 開始型通信の場合は、次のタスクを実行します。[使用状況レポートの収集：CSLU 開始 \(CSLU インターフェイス\) \(180 ページ\)](#) タスクを実行すると、CSLU は ACK 応答で欠落しているポリシーを検出して再提供します。

• CSLU は CSSM から切断：

- 製品インスタンス開始型通信の場合は、特権 EXEC モードで **license smart sync** コマンドを入力します。同期要求により、CSLU は欠落している情報 (ポリシーまたは承認コード) を製品インスタンスにプッシュします。次に、次のタスクを指定された順序で実行します。[CSSM へのエクスポート \(CSLU インターフェイス\) \(186 ページ\)](#) > [CSSM へのデータまたは要求のアップロードとファイルのダウンロード \(229 ページ\)](#) > [CSSM からのインポート \(CSLU インターフェイス\) \(187 ページ\)](#)

- CSLU 開始型通信の場合は、次のタスクを実行します。[使用状況レポートの収集：CSLU 開始 \(CSLU インターフェイス\) \(180 ページ\)](#) タスクを実行すると、CSLU は ACK 応答で欠落しているポリシーを検出して再提供します。次に、次のタスクを指定された順序で実行します。[CSSM へのエクスポート \(CSLU インターフェイス\) \(186 ページ\)](#) > [CSSM へのデータまたは要求のアップロードとファイルのダウンロード \(229 ページ\)](#) > [CSSM からのインポート \(CSLU インターフェイス\) \(187 ページ\)](#)

• CSSM への接続なし、CSLU なし

完全に外部との接続性がないネットワークにいる場合は、インターネットと CSSM に接続できるワークステーションから次のタスクを実行します。[CSSMからのポリシーファイルのダウンロード \(229 ページ\)](#)

次に、製品インスタンスで次のタスクを実行します。[製品インスタンスへのファイルのインストール \(231 ページ\)](#)

- SSM オンプレミス展開

- 製品インスタンス開始型通信の場合は、特権 EXEC モードで **license smart sync** コマンドを入力します。製品インスタンスを SSM オンプレミスと同期させ、必要な情報または欠落している情報を復元する原因です。必要に応じて、SSM オンプレミスと CSSM を同期します。
- SSM オンプレミス開始型通信の場合：SSM オンプレミス UI で、[Reports] > [Synchronization pull schedule] > [Synchronize now with the device] に移動します。

SSM オンプレミス展開の両方の通信形式で、次のいずれかのオプションを使用して CSSM と同期します。

- SSM オンプレミスが CSSM に接続されている場合：SSM オンプレミス UI の [Smart Licensing] ワークスペースで、[Reports] > [Usage Schedules] > [Synchronize now with Cisco] に移動します。
- SSM オンプレミスが CSSM に接続されていません。[使用状況データのエクスポートとインポート \(SSM オンプレミス UI\) \(206 ページ\)](#) を参照してください。

上記がうまくいかず、カスタムポリシーが復元されない場合は、シスコのテクニカルサポート担当者にお問い合わせください。

```
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 番目の [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：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。

- 署名の不一致：これは、システムクロックが正確でないことを意味します。
- 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、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。製品インスタンスに信頼コードがすでに存在する状態で信頼コードをインストールする場合は、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ます。再設定の際、**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：

<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ます。その後、次のタスクを再度実行します。[CSSMからの信頼コード用新規トークンの生成 \(227 ページ\)](#) と [製品インスタンスへのファイルのインストール \(231 ページ\)](#)

- タイムスタンプの不一致と署名の不一致：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： Cisco Smart Software Manager オンプレミス（旧称 Cisco Smart Software Manager サテライト）は、Cisco IOS XE Amsterdam 17.3.3 以降でのみ Smart Licensing Using Policy 環境でサポートされています（[SSM オンプレミス \(9 ページ\)](#) を参照）。サポートされていないリリースでは、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：

次の選択肢があります。

- 代わりに、サポートされているトポロジを参照し、いずれかを実装します。サポートされるトポロジ (18 ページ) を参照してください。
- Smart Licensing Using Policy で SSM オンプレミスがサポートされているリリースにアップグレードします。Smart Licensing Using Policy をサポートする SSM オンプレミスのバージョンへの移行 (169 ページ) を参照してください。

```
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 開始型通信
- 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詳細を確認するには、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権限付与のタイプも確認できます。

```
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、スマートライセンス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。実装したトポロジによって、レポート方式が決まります。

- CSLU を介して CSSM に接続
 - 製品インスタンス開始型通信の場合：特権 EXEC モードで **license smart sync** コマンドを入力します。CSLU が現在 CSSM にログインしている場合、CSSM 内の関連付けられているスマートアカウントとバーチャルアカウントに自動的に送信されます。
 - CSLU 開始型通信の場合は、次のタスクを実行します。[使用状況レポートの収集：CSLU 開始 \(CSLU インターフェイス\) \(180 ページ\)](#)
- CSSM への直接接続：特権 EXEC モードで **license smart sync** コマンドを入力します。
- コントローラを介して CSSM に接続：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。
 Cisco DNA Center をコントローラとして使用している場合は、アドホックレポートのオプションがあります。必要なリリース（リリース 2.2.2 以降）の『[Cisco DNA Center Administrator Guide](#)』[英語]で「Manage Licenses」の「Upload Resource Utilization Details to CSSM」を参照してください。
- CSSM からの CSLU の切断：製品スタンスが CSLU に接続されている場合は、上記の「CSLU を介した CSSM への接続」に示したように製品インスタンスと同期してから、タスク [CSSM へのエクスポート \(CSLU インターフェイス\) \(186 ページ\)](#)、[CSSM へのデータまたは要求のアップロードとファイルのダウンロード \(229 ページ\)](#)、[CSSM からのインポート \(CSLU インターフェイス\) \(187 ページ\)](#) を実行します。
- CSSM への接続なしで CSLU なし：特権 EXEC モードで **license smart save usage** コマンドを入力し、使用状況の必要な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 へのデータまたは要求のアップロードとファイルのダウンロード \(229 ページ\)](#)。
- SSM オンプレミス展開：

製品インスタンスを SSM オンプレミスと同期します。

 - 製品インスタンス開始型通信の場合：特権 EXEC モードで **license smart sync** コマンドを入力します。CSLU が現在 CSSM にログインしている場合、CSSM 内の関連付けられているスマートアカウントとバーチャルアカウントに自動的に送信されます。

- SSM オンプレミス開始型通信の場合は、次の手順を実行します。SSM オンプレミス UI で、[Reports]>[Synchronization pull schedule]>[Synchronize now with the device] に移動します。

使用状況情報を CSSM と同期します（いずれかを選択）。

- SSM オンプレミスが CSSM に接続されている場合：SSM オンプレミス UI の [Smart Licensing] ワークスペースで、[Reports]>[Usage Schedules]>[Synchronize now with Cisco] に移動します。
- SSM オンプレミスが CSSM に接続されていません。[使用状況データのエクスポートとインポート \(SSM オンプレミス UI\) \(206 ページ\)](#) を参照してください。

```
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。

```
Error Message %SMART_LIC-4-UTILITY_TRUST_CODE: Trust establishment with an ID TOKEN is required before utility usage reporting can start.
```

Explanation:

ユーティリティモードが有効になっており、製品インスタンスがスマート転送を使用して CSSM に直接接続されていますが、信頼コードがインストールされていません。このメッセージは、信頼コードがインストールされるか、ユーティリティモードが無効になるまで、週に1回表示されます。

通常の操作中にエラー状態が検出されると、メッセージがすぐに表示されます。エラーが存在する場合、構成が処理された後の起動時にも検出されます。

推奨するアクション：

次のタスクを完了します。[CSSM からの信頼コード用新規トークンの生成 \(227 ページ\)](#) と [ID トークンによる信頼の確立 \(227 ページ\)](#)

```
Error Message %SMART_LIC-4-UTILITY_SUBSCRIPTION_LICENSE: Utility mode is in use with a license that does not have a subscription id: [chars]
```

説明：ユーティリティモードが有効になっており、サブスクリプション ID のないライセンスが使用されています。[chars]は使用中のライセンスです。このメッセージは、ライセンスごとに 1 回だけ生成されます。

考えられる原因は次のとおりです。

- サブスクリプション ID を持つライセンスが使用されていて、新しいサブスクリプション情報が RUM ACK で返されたが、そのライセンスの ID が含まれていない。
- ユーティリティモードが有効になっており、その後しばらくライセンスが使用されている。サブスクリプション ID が使用できない場合、30 日後にこのシステムメッセージが生成されます。
- 通信の遅延。ユーティリティモードを有効にしてから、RUM ACK のサブスクリプション ID やその他のユーティリティ情報が製品インスタンスで利用可能になるまでに、遅延が生じる場合があります。たとえば、CSLU または SSM オンプレミスを使用する場合、製品インスタンスが情報を受信する時期は、CSLU または SSM オンプレミスが製品インスタンスと同期するようにスケジュールされている時期によって異なります。



(注) 権限付与タグに承認コードがインストールされている場合、このシステムメッセージは生成されません。

推奨するアクション：

使用しているライセンスにサブスクリプション ID がない場合は、[CCW](#) で注文できます。ライセンスおよび対応するサブスクリプション ID は、CSSM 内のスマートアカウントとバーチャルアカウントに保管されます。

使用しているライセンスにすでにサブスクリプション ID があり、通信の遅延が原因でこのメッセージが引き続き表示される場合は、実装したトポロジに基づいてオンデマンドの同期を開始できます。

- 製品インスタンスが通信を開始するトポロジを実装している場合、つまり、CSSM またはトポロジに直接接続、CSLU を介して CSSM に接続（製品インスタンス開始モード）、CSLU は CSSM から切断（製品インスタンス開始モード）、または SSM オンプレミス展開（製品インスタンス開始モード）の場合は、特権 EXEC モードで **license smart sync** コマンドを入力します。
- CSLU または SSM オンプレミスが通信を開始するトポロジを実装している場合、つまり、CSLU を介して CSSM に接続（CSLU 開始モード）、CSLU は CSSM から切断（CSLU 開始モード）、または SSM オンプレミス展開（CSLU 開始モード）を使用して、CSLU または SSM オンプレミス UI から製品インスタンスとのオンデマンド同期を開始します。
- CSSM への接続なし、CSLU なしトポロジを使用している場合は、製品インスタンスに ACK をインストールします。[製品インスタンスへのファイルのインストール \(231 ページ\)](#)

Error Message %SMART_LIC-4-UTILITY_NO_ACK: A Usage report acknowledgement has not been received in the last [dec] days. An Acknowledgement is required every 30 days.

説明：過去 30 日以内に RUM ACK メッセージを受信していません。[dec] は日数です。

ユーティリティモードでは、30 日ごとに RUM ACK が必要です。このメッセージは、RUM ACK が受信されるまで 30 日ごとに生成されます。

考えられる原因は次のとおりです。

- 接続の問題。実装したトポロジによっては、CSSM、CSLU、または SSM オンプレミスとの接続の問題を意味する場合があります。
- 通信の遅延。RUM レポートが送信されてから、製品インスタンスで RUM ACK が利用可能になるまでに遅延が生じる場合があります。たとえば、CSLU または SSM オンプレミスを使用する場合、製品インスタンスが情報を受信する時期は、CSLU または SSM オンプレミスが製品インスタンスと同期するようにスケジュールされている時期によって異なります。

推奨するアクション：

接続の問題が発生した場合は、トポロジに適用されるトラブルシューティング手順を参照してください。[%SMART_LIC-3-COMM_FAILED](#)

RUM レポートが送信された場合、**show license all** コマンドの出力の `Next report push` フィールドにこの情報が反映されます。ただし、通信が遅延した場合に ACK が利用できない場合は、実装したトポロジに基づいてオンデマンドの同期を開始します。

- 製品インスタンスが通信を開始するトポロジを実装している場合、つまり、CSSM または トポロジに直接接続、CSLU を介して CSSM に接続（製品インスタンス開始モード）、CSLU は CSSM から切断（製品インスタンス開始モード）、または SSM オンプレミス展開（製品インスタンス開始モード）の場合は、特権 EXEC モードで **license smart sync** コマンドを入力します。
- CSLU または SSM オンプレミスが通信を開始するトポロジを実装している場合、つまり、CSLU を介して CSSM に接続（CSLU 開始モード）、CSLU は CSSM から切断（CSLU 開始モード）、または SSM オンプレミス展開（CSLU 開始モード）を使用して、CSLU または SSM オンプレミス UI から製品インスタンスとのオンデマンド同期を開始します。
- CSSM への接続なし、CSLU なしトポロジを使用している場合は、製品インスタンスに ACK をインストールします。[製品インスタンスへのファイルのインストール \(231 ページ\)](#)

引き続き ACK を正常に受信できない場合は、シスコのテクニカルサポート担当者にお問い合わせください。

Error Message %SMART_LIC-4-UTILITY_TRANSPORT_NOT_CONFIG: To support utility mode the transport must be set to 'smart transport' or 'cslu'.

説明：ユーティリティモードは有効ですが、トランスポートタイプが正しく設定されていません。このシステムメッセージは、正しいトランスポート設定が構成されるか、ユーティリティモードが無効になるまで、週に1回生成されます。

通常の操作中にエラー状態が検出されると、メッセージがすぐに表示されます。また、構成が処理された後の起動時、またはトランスポートモードやユーティリティモードを変更した場合にも検出されます。

推奨するアクション：

ユーティリティモードでは、トランスポートタイプは **smart**、**cslu**、または **off** である必要があります。実装したトポロジに応じて、トランスポートモードを設定します。[転送タイプ、URL、およびレポート間隔の設定 \(232 ページ\)](#)

 Error Message %SMART_LIC-3-UTILITY_REPORT_FAILED: Smart Agent for Licensing Utility has failed to send usage Report.

説明：通信障害のため、製品インスタンスは RUM レポートを送信できませんでした。

推奨するアクション：

RUM レポートの期限が近いか確認します。近くなく、問題がダウンしているサーバーやリンクにある場合は、しばらくしてから再試行できます。

通信エラーが続く場合は、トポロジで必要とされるトランスポートタイプと URL が設定されているか確認してください。

[%SMART_LIC-3-COMM_FAILED](#) も参照してください。

通信障害が続く場合は、シスコのテクニカルサポート担当者にお問い合わせください。

 Error Message %SMART_LIC-6-UTILITY_STARTED: Smart Agent for Licensing Utility has started sending usage reports

説明：CSSM、CSLU、または SSM オンプレミスのいずれか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-6-UTILITY_STOPPED: Smart Agent for Licensing Utility has stopped sending usage reports

説明：ユーティリティモードが無効になっています。

推奨するアクション：アクションは必要ありません。

RUM レポートは引き続き送信されますが、ユーティリティモードであることを示すフラグは設定されません。



第 8 章

ポリシーを使用したスマートライセンシングのその他の参考資料

関連項目	マニュアル タイトル
Cisco Smart Software Manager (CSSM) のヘルプ	Smart Software Manager Help
Cisco Smart License Utility (CSLU) のインストールおよびユーザガイド 利用可能な最新バージョンの CSLU を常に使用することをお勧めします。	[Software Download] ページで [Smart Licensing Utility] をクリックします。 https://software.cisco.com/download/home/286285506/type
SSM オンプレミスのリリースノート、コンソール、インストール、クイックスタート、およびユーザガイド 利用可能な SSM オンプレミスの最新バージョンを常に使用することを推奨します。	[Software Download] ページで [Smart Software Manager On-Prem] をクリックします。 https://software.cisco.com/download/home/286285506/type
システムメッセージガイド (Cisco IOS-XE ソフトウェアを実行するすべての製品に適用可能)。 SMART_LIC を検索して、ライセンス関連のシステムメッセージを見つけます。	エラーとシステムメッセージ



第 9 章

ポリシーを使用したスマートライセンスの機能の履歴

次の表に、このモジュールで説明する機能のリリースおよび関連情報を示します。

これらの機能は、特に明記されていない限り、導入されたリリース以降のすべてのリリースで使用できます。

表 19: ポリシーを使用したスマートライセンスの機能の履歴

機能名	リリース	機能情報
ポリシーを使用したスマートライセンス	Cisco IOS XE Amsterdam 17.3.2	<p>スマートライセンスの拡張バージョンには、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。</p> <p>このリリース以降、ポリシーを使用したスマートライセンスがデバイスで自動的に有効になります。これは、このリリースにアップグレードする場合にも当てはまります。</p> <p>デフォルトでは、CSSM のスマートアカウントとバーチャルアカウントは、ポリシーを使用したスマートライセンスで有効になっています。</p>

機能名	リリース	機能情報
Smart Licensing Using Policy への Cisco DNA Center のサポート	Cisco IOS XE Amsterdam 17.3.2	<p>Cisco DNA Center は、Cisco DNA Center リリース 2.2.2 以降、Smart Licensing Using Policy 機能をサポートしています。</p> <p>Cisco DNA Center を使用して製品インスタンスを管理する場合、Cisco DNA Center は CSSM に接続し、CSSM とのすべての通信のインターフェイスとなります。</p> <p>互換性のあるコントローラと製品インスタンスのバージョンについては、「コントローラのサポート情報：Cisco DNA Center」を参照してください。</p> <p>このトポロジについては、コントローラとしての Cisco DNA Center (24 ページ) と コントローラとしての Cisco DNA Center の使用 (55 ページ) を参照してください。</p>
Smart Licensing Using Policy の場合の Smart Software Manager オンプレミス (SSM オンプレミス) サポート	Cisco IOS XE Amsterdam 17.3.3	<p>SSM オンプレミスは、CSSM と連動するアセットマネージャです。これにより、CSSM に直接接続する代わりに、オンプレミスで製品とライセンスを管理できます。</p> <p>互換性のある SSM オンプレミスと製品インスタンスバージョンについては、SSM オンプレミス (9 ページ) を参照してください。</p> <p>このトポロジの概要についてと実装方法については、SSM オンプレミス展開 (30 ページ) と トポロジのワークフロー：SSM オンプレミス展開 (65 ページ) を参照してください。</p> <p>既存のバージョンの SSM オンプレミスから、Smart Licensing Using Policy への移行をサポートするバージョンへの移行については、Smart Licensing Using Policy をサポートする SSM オンプレミスのバージョンへの移行 (169 ページ) を参照してください。</p>

機能名	リリース	機能情報
<p>ポリシーを使用したスマートライセンス</p>	<p>Cisco IOS XE Bengaluru 17.4.1</p>	<p>このリリース以降、ポリシーを使用したスマートライセンスは次のプラットフォームでサポートされます。</p> <ul style="list-style-type: none"> • Catalyst 8000V エッジソフトウェア • Catalyst 8200 シリーズ エッジプラットフォーム • Cisco 1100 ターミナル サービス ゲートウェイ • シスコクラウドサービスルータ 1000v (このプラットフォームで、ポリシーを使用したスマートライセンスをサポートするには、CSRv.bin イメージから Catalyst 8000V ソフトウェアイメージにアップグレードする必要があります)。 • シスコサービス統合型仮想ルータ (このプラットフォームで、ポリシーを使用したスマートライセンスをサポートするには、ISRv.bin イメージから Catalyst 8000V ソフトウェアイメージにアップグレードする必要があります)。 <p>この機能をサポートする製品の完全なリストについては、サポート対象製品 (4 ページ)を参照してください。</p>

機能名	リリース	機能情報
<p>ポリシーを使用したスマートライセンスのライセンス管理 (Cisco vManage を使用)</p>	<p>Cisco IOS XE Bengaluru 17.5.1a</p>	<p>Cisco SD-WAN は Cisco CSSM と連携して動作し、Cisco SD-WANで動作するデバイスに対して Cisco vManage によるライセンス管理を提供します。これを実現するためには、Cisco vManage が CSSM に接続されているトポロジを実装する必要があります。</p> <p>互換性のあるコントローラと製品インスタンスのバージョンについては、「コントローラのサポート情報：Cisco vManage」を参照してください。</p> <p>このトポロジの詳細については、このマニュアルのコントローラを介して CSSM に接続 (23 ページ) およびトポロジのワークフロー：コントローラを介して CSSM に接続 (55 ページ) を参照してください。</p> <p>Cisco vManage の詳細については、Cisco SD-WAN スタートアップガイド [英語] の「License Management for Smart Licensing Using Policy」セクションを参照してください。</p>
<p>PAK ライセンスのスナップショット</p>	<p>Cisco IOS XE Bengaluru 17.6.2</p>	<p>PAK ライセンスを管理するライブラリは、ソフトウェアイメージから削除されています。ユーザーの既存の PAK ライセンスを引き続きサポートおよび受け入れるために、PAK ライセンスのスナップショットが自動的に作成され、Device-Led Conversion プロセスがトリガーされ、PAK ライセンスがスマートライセンスに変換されます。</p> <p>PAK ライセンスのスナップショット (43 ページ) を参照してください。</p>

機能名	リリース	機能情報
工場でインストールされた信頼コード	Cisco IOS XE Cupertino 17.7.1a	<p>新しいハードウェアの注文では、信頼コードは製造時にインストールされるようになりました。</p> <p>出荷時にインストールされた信頼コードを使用して CSSM と通信することはできません。</p> <p>概要 (3 ページ) および 信頼コード (17 ページ) を参照してください。</p>
追加のトポロジでの信頼コードのサポート		<p>信頼コードは、製品インスタンスが CSLU へのデータ送信を開始するトポロジと、製品インスタンスがエアギャップネットワーク内にあるトポロジで自動的に取得されます。</p> <p>次を参照してください。</p> <ul style="list-style-type: none"> • 信頼コード (17 ページ) • CSLU を介して CSSM に接続 (19 ページ)、製品インスタンス開始型通信の場合のタスク (49 ページ) • CSLU は CSSM から切断 (26 ページ)、製品インスタンス開始型通信の場合のタスク (59 ページ) • CSSM への接続なし、CSLU なし (28 ページ)、トポロジのワークフロー：CSSM への接続なし、CSLU なし (63 ページ)
認証コード要求を保存してファイルに戻し、CSSM Web UI で簡単にアップロードする機能		

機能名	リリース	機能情報
		<p>製品インスタンスがエアギャップネットワークにある場合、SLAC 要求を製品インスタンスのファイルに保存できます。SLAC 要求ファイルを CSSM Web UI にアップロードする必要があります。その後、SLAC コードを含むファイルをダウンロードし、製品インスタンスにインストールできます。返品要求ファイルも同様の方法でアップロードできます。</p> <p>この新しい方法では、SLAC を生成するために CSSM Web UI で必要な詳細情報を収集して入力する必要はありません。また、認証コードを返却するために CSSM Web UI で製品インスタンスを検索する必要はありません。</p> <p>CSSM Web UI では、要求または返信ファイルは、RUM レポートをアップロードするのと同じ場所に同じ方法でアップロードされます。</p> <p>製品インスタンスでの SLAC 要求の生成と保存 (219 ページ)、承認コードの削除と返却 (220 ページ)、および CSSM へのデータまたは要求のアップロードとファイルのダウンロード (229 ページ) を参照してください。</p>
RUM レポートでソフトウェアバージョンを収集するためのサポート		<p>バージョンプライバシーが無効になっている場合 (no license smart privacy version グローバルコンフィギュレーションコマンド)、製品インスタンスで実行されている Cisco IOS-XE ソフトウェアバージョンと Smart Agent バージョン情報が RUM レポートに含まれます。</p> <p>「license smart (グローバルコンフィギュレーション) (261 ページ)」を参照してください。</p>
RUM レポートの最適化と統計情報の可用性		<p>RUM レポートの生成と関連プロセスが最適化されました。これには、RUM レポートの処理にかかる時間の短縮、メモリとディスク領域の使用率の向上、および製品インスタンス上の RUM レポートの可視性 (エラーがある場合、エラーの数、各プロセスの処理状態など) が含まれます。</p> <p>show license rum (306 ページ)、show license tech (326 ページ)、および show license all (286 ページ) を参照してください。</p>

機能名	リリース	機能情報
<p>show コマンドの出力に含まれるアカウント情報</p>		<p>RUM 確認応答 (ACK) には、CSSM で報告されたスマートアカウントとバーチャルアカウントが含まれます。アカウント情報は、さまざまな show コマンドの出力に表示され、常に製品インスタンスで使用可能な最新の ACK に従います。</p> <p>show license summary (323 ページ)、show license status (314 ページ)、show license all (286 ページ)、および show license tech (326 ページ) を参照してください。</p>
<p>Linux の CSLU サポート</p>		<p>Linux を実行するマシン (ラップトップまたはデスクトップ) での CSLU 導入のサポート。CSLU は、次の形式の Linux と互換性があります。</p> <p>「CSLU (7 ページ)」を参照してください。</p>

機能名	リリース	機能情報
Smart Licensing Using Policy によるマネージドサービスライセンス契約 (MSLA) のサポート。	Cisco IOS XE Cupertino 17.9.1a	<p>自律モードで実行されている Catalyst 8000V エッジソフトウェアの場合、必要なライセンスの前払いではなく、ライセンスの実際の使用量に対して支払うライセンスの後払いモデルを実装できます。</p> <p>MSLA (10 ページ) および ユーティリティモード (33 ページ) を参照してください。</p>
データプライバシー関連情報を送信する新しいメカニズム		<p>すべてのデータプライバシー関連情報を送信する新しいメカニズムが導入されました。この情報は RUM レポートに含まれなくなりました。データプライバシーが無効になっている場合 (no license smart privacy {all hostname version}) グローバル コンフィギュレーション コマンド)、データプライバシー関連情報は、別の同期メッセージまたはオフラインファイルで送信されます。</p> <p>実装したトポロジに応じて、製品インスタンスが別のメッセージでこの情報の送信を開始するか、CSLU および SSM オンプレミスが製品インスタンスからのこの情報の取得を開始するか、または license smart save usage 特権 EXEC コマンドを入力すると生成されるオフラインファイルにこの情報が保存されます。</p> <p>license smart (グローバル コンフィギュレーション) (261 ページ) を参照してください。</p>
ホスト名のサポート		<p>製品インスタンスでホスト名を設定し、対応するプライバシー設定を無効にすると (no license smart privacy hostname グローバル コンフィギュレーション コマンド)、ホスト名情報が製品インスタンスから送信されます。</p> <p>実装したトポロジに応じて、ホスト名情報は CSSM、および CSLU または SSM オンプレミスによって受信されます。その後、対応するユーザーインターフェイスに表示されます。</p> <p>license smart (グローバル コンフィギュレーション) (261 ページ) を参照してください。</p>
追加のトポロジでの信頼コードのサポート		

機能名	リリース	機能情報
		<p>CSLU が製品インスタンスからのデータの取得を開始するトポロジでは、信頼コードが自動的に取得されます。</p> <p>信頼コード (17 ページ)、CSLU を介して CSSM に接続 (19 ページ)、CSLU は CSSM から切断 (26 ページ) を参照してください。</p>
VRF のサポート		<p>VRF がサポートされている製品インスタンスでは、すべてのライセンスデータを CSSM、CSLU、または SSM オンプレミスに送信するように VRF を設定できます。</p> <p>VRF 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 vrf vrf_string コマンドを入力します。</p> <p>license smart (グローバル コンフィギュレーション) (261 ページ) を参照してください。</p>
RUM レポートスロットリング		

機能名	リリース	機能情報
		<p>製品インスタンスが通信を開始するすべてのトポロジで、レポートの最小頻度は1日に制限されます。これは、製品インスタンスが1日に複数の RUM レポートを送信しないことを意味します。</p> <p>影響を受けるトポロジは、CSSMに直接接続、CSLUを介してCSSMに接続（製品インスタンス開始型通信）、CSSMから切断されたCSLU（製品インスタンス開始型通信）およびSSM オンプレミス展開（製品インスタンス開始型通信）です。</p> <p>特権 EXEC モードで license smart sync コマンドを入力すると、レポート頻度のスロットリングを無効にできます。これにより CSSM または CSLU、あるいは SSM オンプレミスとのオンデマンドの同期がトリガーされ、保留中のデータが送受信されます。</p> <p>RUM レポートスロットリングは、17.3.x トレインの Cisco IOS XE Amsterdam 17.3.6 以降のリリース、および 17.6.x トレインの Cisco IOS XE Bengaluru 17.6.4 以降のリリースにも適用されます。Cisco IOS XE Cupertino 17.9.1 以降、RUM レポートスロットリングは後続のすべてのリリースに適用されます。</p> <p>CSSM に直接接続 (21 ページ)、CSLU を介して CSSM に接続 (19 ページ)、CSLU は CSSM から切断 (26 ページ)、SSM オンプレミス展開 (30 ページ) を参照。</p>
Smart Licensing Using Policy のパーマネントライセンス予約 (PLR)	Cisco IOS XE Dublin 17.10.1a	<p>PLR を使用すると、製品インスタンスで任意のライセンスを無制限に使用できます。PLR 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または完全なエアギャップネットワークに適しています。</p> <p>を参照してください。 Smart Licensing Using Policy 環境のパーマネントライセンス予約 (45 ページ)</p>

機能名	リリース	機能情報
PAK ライセンスのスナップショット	Cisco IOS XE Dublin 17.11.1a	<p>PAK 管理ライブラリは廃止され、スナップショットを取得するためのプロビジョニングは利用できなくなりました。</p> <p>Cisco IOS XE Dublin 17.11.1a以降のソフトウェアイメージは、PAK ライセンスに関するスナップショット情報のみ依存しています。</p> <p>スナップショットのないPAK ライセンスがあり、Cisco IOS XE Dublin 17.11.1a以降のリリースにアップグレードする場合は、2回アップグレードする必要があります。まず、PAK ライセンスのスナップショットと完全なDLCが作成されるリリースのいずれかにアップグレードしてから、必要な後続のリリースに再度アップグレードします。</p> <p>PAK ライセンスのスナップショット (43ページ) を参照してください。</p>

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェアイメージのサポート情報を検索できます。Cisco Feature Navigator にアクセスするには、<https://cfmng.cisco.com/>にアクセスします。

【注意】シスコ製品をご使用になる前に、安全上の注意（www.cisco.com/jp/go/safety_warning/）をご確認ください。本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on standards documentation, or language that is used by a referenced third-party product.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2020–2023 Cisco Systems, Inc. All rights reserved.

翻訳について

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