ポリシーを使用したスマートライセンス

- ポリシーを使用したスマートライセンシングの概要 （1 ページ）
- ポリシーを使用したスマートライセンシングに関する情報 （2 ページ）
- ポリシーを使用したスマートライセンシングの設定方法：トポロジ別のワークフロー （30 ページ）
- ポリシーを使用したスマートライセンシングへの移行 （48 ページ）
- ポリシーを使用したスマートライセンシングのタスクライブラリ （72 ページ）
- ポリシーを使用したスマートライセンシングのトラブルシューティング （132 ページ）
- 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 （145 ページ）
- ポリシーを使用したスマートライセンシングの機能の履歴 （146 ページ）

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。

Smart Licensing Using Policy は、Cisco IOS XE Amsterdam 17.3.2a 以降でサポートされます。

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。使用前に承認が必要なのはこれらのライセンスのみです。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。

このドキュメントでは、Cisco Catalystアクセス、コア、およびアグリゲーションスイッチ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 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シングに関する情報

このセクションでは、Smart Licensing Using Policy の実装に含めることができるコンポーネント、機能に関連する主要な概念、サポートされる製品、サポートされるすべてのトポロジの概要（機能を実装するさまざまな方法）、Smart Licensing Using Policy が他の機能とどのように連携するかについて説明します。

概要

ポリシーを使用したスマートライセンシングは、ライセンスのさまざまな側面をシームレスに体験できるソフトウェアライセンス管理ソリューションです。次に、この環境での操作の概要を示します。

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

（注） ポリシーを使用したスマートライセンシングの実装を簡素化するには、新しいハードウェアまたはソフトウェアを注文する際にスマートアカウントとバーチャルアカウントの情報を提供します。これにより、シスコは製造時に該当するポリシーおよび承認コード（用語は以下のセクション概念 （6 ページ）で説明）をインストールできます。

- 使用：ほとんどのライセンスは適用（エンフォース）されません。つまり、ソフトウェアとそれに関連付けられているライセンスの使用を開始する前に、キーの登録や生成などのライセンス固有の操作を完了する必要はありません。輸出規制および適用されたライセンスのみ、使用前にシスコの承認が必要です。また、特定の製品のみが輸出規制ライセンス

をサポートします。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 （131 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）。

サポート対象製品

このセクションでは、本マニュアルの対象範囲に含まれる、ポリシーを使用したスマートライセンシングをサポートするCisco IOS-XE製品インスタンスについての情報を提供します。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*：サポートされる製品インスタンス：*Cisco Catalyst* アクセス、コア、およびアグリゲーションスイッチ

Cisco Catalyst アクセス、コア、およびアグリゲーションスイッチ	**サポートが導入されたバージョン**
Cisco Catalyst 9200 シリーズ スイッチ	Cisco IOS XE Amsterdam 17.3.2a
Cisco Catalyst 9300 シリーズ スイッチ	Cisco IOS XE Amsterdam 17.3.2a
Cisco Catalyst 9400 シリーズ スイッチ	Cisco IOS XE Amsterdam 17.3.2a
Cisco Catalyst 9500 シリーズ スイッチ	Cisco IOS XE Amsterdam 17.3.2a
Cisco Catalyst 9600 シリーズ スイッチ	Cisco IOS XE Amsterdam 17.3.2a

アーキテクチャ

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

製品インスタンス

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

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

このドキュメントでは、「製品インスタンス」という用語は、特に明記しない限り、サポートされているすべての物理および仮想製品インスタンスを指します。このドキュメントの範囲内にある製品インスタンスについては、サポート対象製品 （3 ページ）を参照してください。

CSLU

Cisco Smart License Utility（CSLU）は、集約ライセンスワークフローを提供する Windows ベースのレポートユーティリティです。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、CSSM から承認コードを受信します（該当する場合）。

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。

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 でアクセスできます。[Smart Software Manager] で、[Manage licenses] リンクをクリックします。

このドキュメントのサポートされるトポロジ （11 ページ）では、CSSM に接続するさまざまな方法について説明します。

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。
- 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。

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。

Cisco Catalyst アクセス、コア、およびアグリゲーションスイッチでは、Cisco DNA Center がサポートされるコントローラです。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で必要な最小ソフトウェアバージョンに関する情報を次に示します。

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[1]	**Cisco IOS XE に必要な最小バージョン**[2]	**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 17.3.2a	• Cisco Catalyst 9200 シリーズ スイッチ • Cisco Catalyst 9300 シリーズ スイッチ • Cisco Catalyst 9400 シリーズ スイッチ • Cisco Catalyst 9500 シリーズ スイッチ • Cisco Catalyst 9600 シリーズ スイッチ

[1] コントローラに必要な最小ソフトウェアバージョン。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。

[2] 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。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 [英語] でサポート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[3]	Cisco IOS XE に必要な最小バージョン[4]	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	• Cisco Catalyst 9200 シリーズ スイッチ • Cisco Catalyst 9300 シリーズ スイッチ • Cisco Catalyst 9400 シリーズ スイッチ • Cisco Catalyst 9500 シリーズ スイッチ • Cisco Catalyst 9600 シリーズ スイッチ

[3] 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。

[4] 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。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。

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。

概念

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

ライセンス執行（エンフォースメント）タイプ

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

- 不適用または非適用

  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。

  Network Essentials、Network Advantage、Digital Network Architecture（DNA）Essentials、および DNA Advantage は、Cisco Catalyst アクセス、コア、およびアグリゲーションスイッチでサポートされる不適用ライセンスの例です。

- 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。

  輸出規制されたライセンスの例は、特定の Cisco スイッチで使用可能な高セキュリティの輸出規制キー（HSECK9）です。

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。

  Network Essentials、Network Advantage、および HSECK9 は、永久ライセンスの例です。

- 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。

  DNA Essentials および DNA Advantage ライセンスは、サブスクリプション ライセンスの例です。

承認コード

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

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

表 *3 : SLAC* を必要とするライセンス、サポートされるプラットフォーム、およびリリース

適用タイプ	輸出規制キー	サポートされているプラットフォームとサポートされている導入リリース
輸出規制	HSECK9	Cisco IOS XE Bengaluru 17.6.2 以降の Cisco Catalyst 9300X シリーズ スイッチのみ。

HSECK9 キーの詳細については、このガイドの「使用可能なライセンス」章の高セキュリティのための輸出規制キーセクションを参照してください。

SLR 承認コード

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、固有の承認コードを使用する Specific License Reservation（SLR）を設定することができます。SLR 承認コードは、Smart Licensing Using Policy へのアップグレード後にサポートされます。

（注） 既存の SLR はアップグレード後に引き継がれますが、「予約」の概念が適用されないため、ポリシーを使用したスマートライセンシング環境で新しい SLR を要求することはできません。完全に外部との接続性がないネットワーク内にいる場合は、代わりに CSSM への接続なし、CSLU なしのトポロジが適用されます。

SLR 承認コードの処理方法の詳細については、アップグレード （24 ページ） を参照してください。SLR 承認コードを返す場合は、承認コードの返却 （112 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)：後続のレポートは、ここで指定した期間内に送信される必要があります。

  こ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 4 : ポリシー：Cisco default （9 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] をクリックして、[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 *4 :* 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[5]	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

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

RUM レポートおよびレポート確認応答

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

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

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

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

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

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。

信頼コード

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

サポートされるトポロジ

このセクションでは、ポリシーを使用したスマートライセンシングを実装するさまざまな方法について説明します。各トポロジについて、付属の概要を参照してセットアップの動作設計を確認し、考慮事項と推奨事項（ある場合）を参照してください。

トポロジを選択した後

トポロジを選択した後、ポリシーを使用したスマートライセンシングの設定方法：トポロジ別のワークフロー （30 ページ） を参照してください。これらのワークフローは、新規展開のみに該当します。これらの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実現します。

既存のライセンシングモデルから移行する場合は、ポリシーを使用したスマートライセンシングへの移行 （48 ページ） を参照してください。

追加の設定タスクを実行する場合（たとえば別のライセンスを設定する場合、アドオンライセンスを使用する場合、またはより短いレポート間隔を設定する場合）は、ポリシーを使用したスマートライセンシングのタスクライブラリ （72 ページ） を参照してください。続行する前に、入手可能な場合には「サポートされるトポロジ」を確認してください。

CSLU を介して CSSM に接続

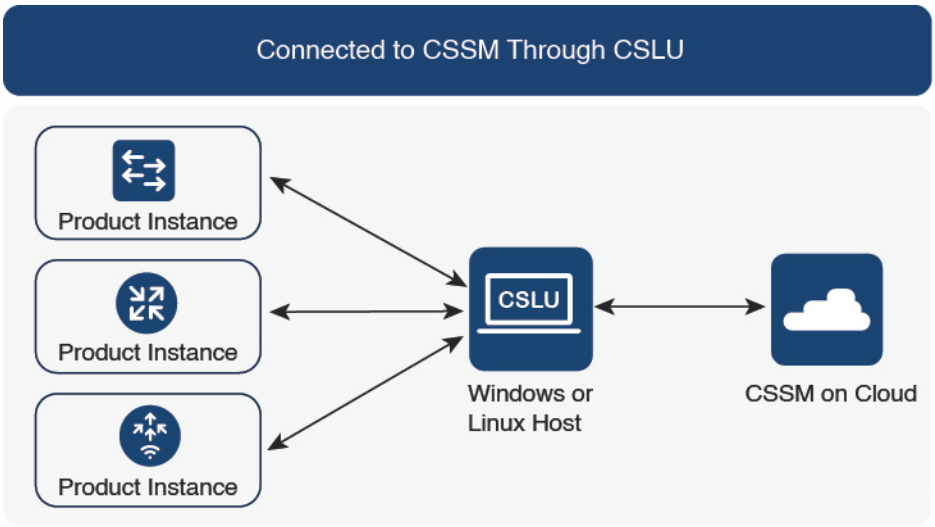
概要：

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

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

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

図 *1:* トポロジ：*CSLU* を介して *CSSM* に接続



考慮事項または推奨事項：

ネットワークのセキュリティポリシーに応じて通信方法を選択します。

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。

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 以降のリリースのみに適用されます。

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 （30 ページ）を参照してください。

CSSM に直接接続

概要：

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

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

次の方法で CSSM と通信するように製品インスタンスを設定できます。

- スマート転送を使用して CSSM と通信する。

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

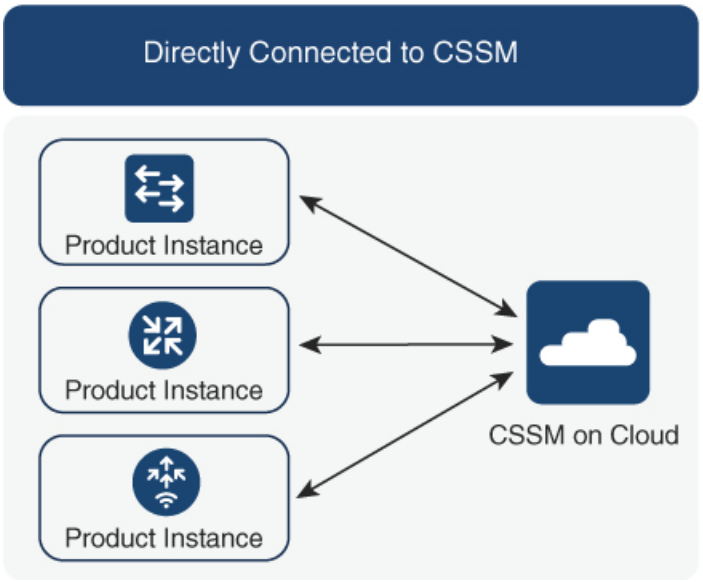
  - スマート転送：この方法では、製品インスタンスは特定のスマート転送ライセンスサーバ URL を使用します。これは、ワークフローのセクションに示すとおりに設定する必要があります。
  - HTTPS プロキシを介したスマート転送：この方法では、製品インスタンスはプロキシサーバを使用してライセンスサーバと通信し、最終的には CSSM と通信します。

- Call Home を使用して CSSM と通信する。

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

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

図 *2:* トポロジ：*CSSM* に直接接続



考慮事項または推奨事項：

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

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

移行後に設定を変更するには、トポロジのワークフロー：CSSM に直接接続 （34 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。

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。

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 以降のリリースのみに適用されます。

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 （34 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。Cisco Catalyst アクセス、コア、およびアグリゲーションスイッチのサポートされるコントローラは、Cisco DNA Center です。

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。

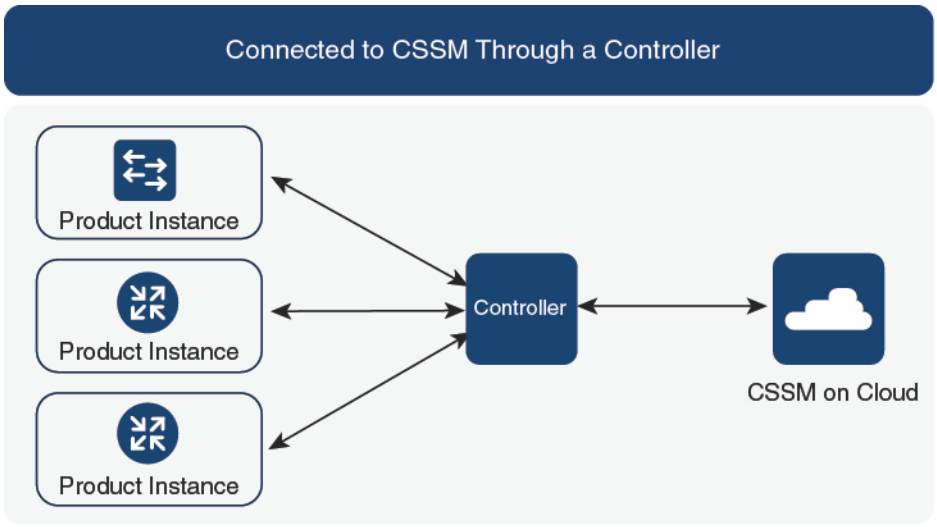
- Ad hoc reporting：必要に応じてアドホックレポートをトリガーできます。
- Scheduled reporting：ポリシーで指定されたレポート頻度に対応し、Cisco DNA Center によって自動的に処理されます。

（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。

信頼コードは必要ありません。

図 *3:* トポロジ：コントローラを介して *CSSM* に接続



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。

（注） 輸出規制ライセンスである HSECK9 キーは、Cisco Catalyst アクセス、アグリゲーションスイッチ、およびコアスイッチの特定のモデルでサポートされています（承認コード （7 ページ）を参照）。HSECK9 キーがサポートされている製品インスタンスを使用している場合は、Cisco DNA Center GUI に SLAC を生成するオプションが表示されないことに注意してください。

次の手順：

このトポロジを実装するには、トポロジのワークフロー：コントローラを介して CSSM に接続（35 ページ）を参照してください。

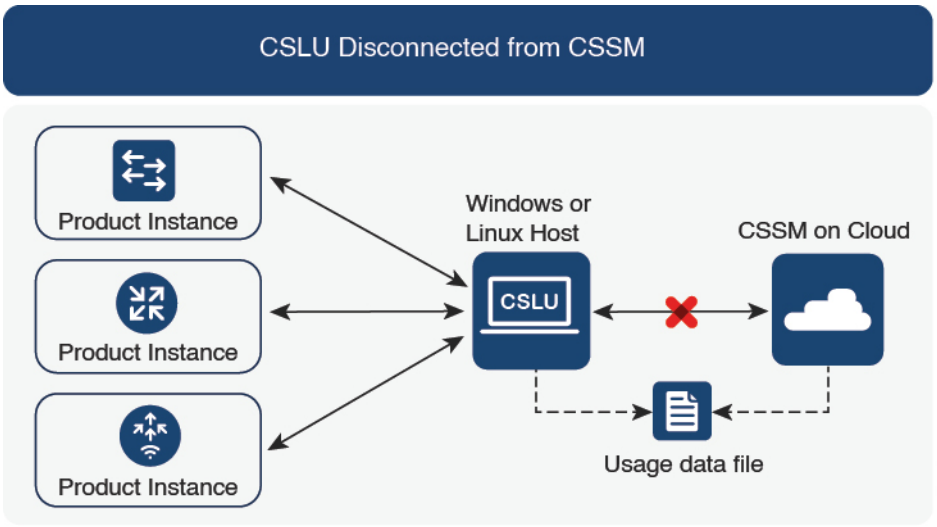
CSLU は CSSM から切断

概要：

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

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

図 *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。

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 以降のリリースのみに適用されます。

次の手順：

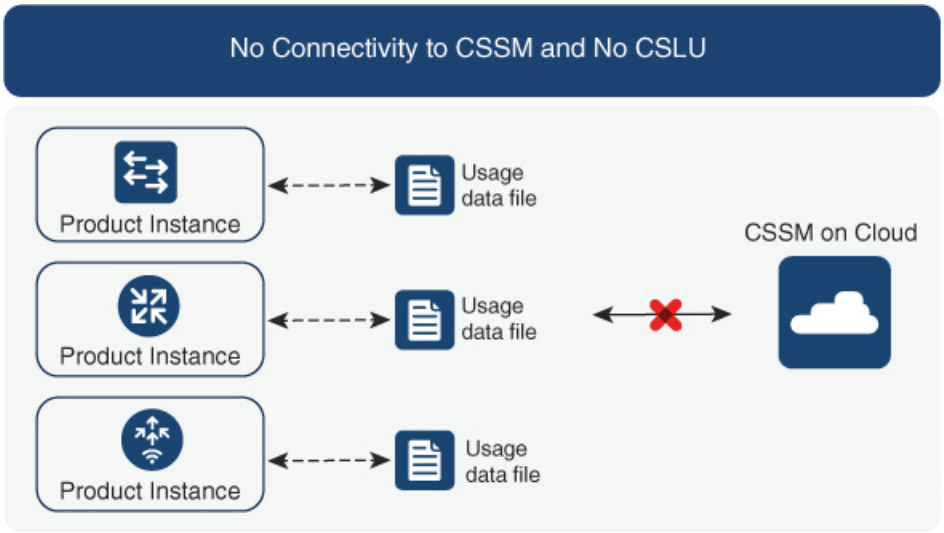
このトポロジを実装するには、トポロジのワークフロー：CSLU は CSSM から切断 （37 ページ）を参照してください。

CSSM への接続なし、CSLU なし

概要：

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

図 *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。

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（41 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。

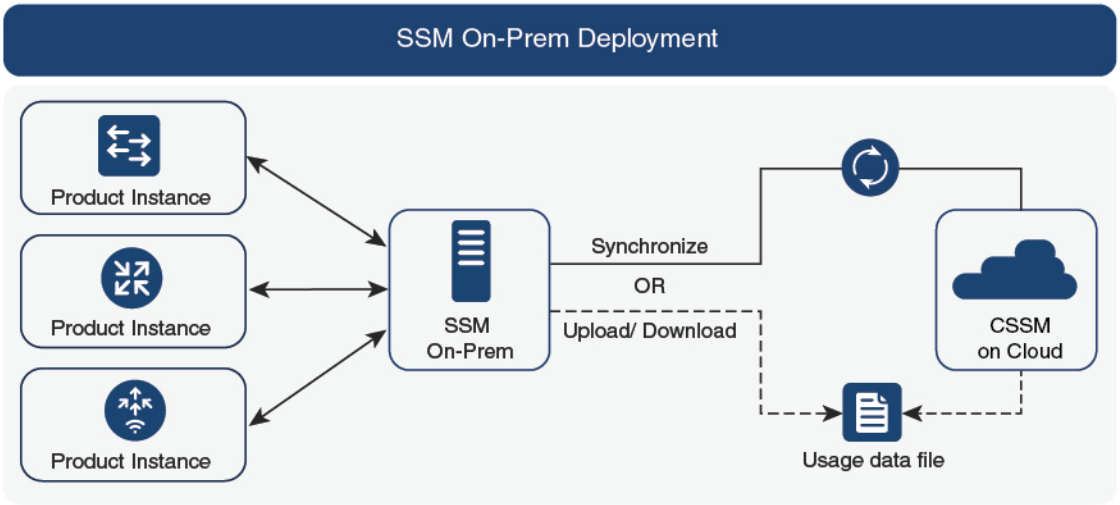
SSM オンプレミスでは、レポート間隔が製品インスタンスのデフォルトポリシーに設定されます。これは変更できますが、より頻繁に（より短い間隔で）レポートを作成するか、または使用可能な場合はカスタムポリシーをインストールできます。

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



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。

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 以降のリリースのみに適用されます。

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 （42 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 （70 ページ）を参照してください。

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

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

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

デュアルシャーシ セットアップ[6]（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[7]。ここでも 2 つのシャーシが関係し、1 つのシャーシにアクティブ RP、もう 1 つのシャーシにスタンバイ RP があります。デュアル RP とは、最小要件である 1 つのシャーシだけに追加のシャーシ内スタンバイ RP、または各シャーシにシャーシ内スタンバイ RP があることを指します。

高可用性セットアップでの信頼コード要件

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、セットアップのスタンバイまたはメンバーに適用されます。

[6] 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。
[7] Cisco Catalyst スイッチで使用可能なルートプロセッサ冗長性を備えたクアッドスーパーバイザが、このようなセットアップの例です。

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、追加または削除されたスタンバイに関する情報が含まれます。
- スタックマージおよびスタック分割イベントを含む、メンバーの追加または削除。RUM レポートには、追加または削除された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、ポリシーを使用したスマートライセンシングへのアップグレードまたは移行の処理方法について説明します。また、ポリシーを使用したスマートライセンシングが、以前のバージョンのスマートライセンシング、特定のライセンス予約（SLR）、使用権ライセンシング（RTU）を含む以前のライセンスモデルすべてを処理する方法、および以前のライセンシングモデルの評価ライセンスまたは期限切れライセンスがポリシーを使用したスマートライセンシング環境で処理される方法を具体的に説明します。

ポリシーを使用したスマートライセンシングに移行するには、ポリシーを使用したスマートライセンシングをサポートするソフトウェアバージョンにアップグレードする必要があります。アップグレードした後は、ポリシーを使用したスマートライセンシングが唯一のサポートされるライセンスモデルとなり、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。ポリシーを使用したスマートライセンシングへの移行 （48 ページ） セクションでは、Cisco Catalyst アクセス、コア、およびアグリゲーションスイッチに適用される移行シナリオの詳細と例を示します。

デバイス先行の変換は、ポリシーを使用したスマートライセンシングへの移行ではサポートされていません。

アップグレード前に現在のライセンシングモデルを識別する

ポリシーを使用したスマートライセンシング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シング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 ライセンシングモデルを除くすべてのライセンシング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、ライセンシングモデルが 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シングをサポートするソフトウェアバージョンにアップグレードする場合、既存ライセンスの処理方法は、主に適用タイプによって決まります。

- 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。これには、以前のすべてのライセンシングモデルのライセンスがすべて含まれます。
  - スマート ライセンス。
  - 特定のライセンス予約（SLR）。承認コードが付属しています。承認コードは、ポリシーを使用したスマートライセンシングへのアップグレード後も引き続き有効であり、既存のライセンスの使用を承認します。
  - 使用権（RTU）ライセンシング。
  - 上記のライセンシングモデルのいずれかの評価ライセンスまたは期限切れライセンス。
- アップグレード前に使用されていた適用ライセンスや輸出規制ライセンスは、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。

輸出規制ライセンスは、Cisco IOS XE Bengaluru 17.6.2 以降の特定のモデルでのみサポートされています。それ以前の Cisco Catalyst アクセス、コア、およびアグリゲーションスイッチで使用可能な輸出規制ライセンスや適用ライセンスはありませんでした。

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シングへの移行後のレポート要件
使用権（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 `Next ACK deadline` 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。
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シングへのアップグレード後に既存のライセンス消費を承認します。
スマートライセンシング（登録済みライセンスと承認済みライセンス）：これらのライセンスのレポートは、ポリシーのレポート要件に基づいています。	ポリシーによって異なります。
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シングへのアップグレード後も転送タイプが保持されます。

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

アップグレード前の転送タイプ	アップグレード前のライセンスまたはライセンスの状態	アップグレード後の転送タイプ
デフォルト（callhome）	評価	cslu（ポリシーを使用したスマートライセンシングのデフォルト）
	SLR	off
	登録	callhome
smart	評価	off
	SLR	off
	登録	smart
N/A たとえば、既存のライセンスモデルが RTU の場合。	N/A たとえば、既存のライセンスモデルが RTU 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シングでは、CSSMへの登録と接続にトークンが使用されていました。ID トークンの登録は、ポリシーを使用したスマートライセンシングでは必要ありません。トークン生成機能はCSSMでも引き続き使用でき、製品インスタンスがCSSMに直接接続されている場合に信頼を確立するために使用されます。「CSSMに直接接続」を参照してください。

ダウングレード

ダウングレードするには、製品インスタンスのソフトウェアバージョンをダウングレードする必要があります。このセクションでは、新規展開および既存の展開のダウングレードに関する情報を提供します（ポリシーを使用したスマートライセンシングにアップグレードした後にダウングレードする場合）。

新規展開のダウングレード

このセクションは、ポリシーを使用したスマートライセンシングがデフォルトですでに有効になっているソフトウェアバージョンで新しく購入した製品インスタンスがあり、ポリシーを使用したスマートライセンシングがサポートされていないソフトウェアバージョンにダウングレードする場合に該当します。

ダウングレードの結果は、ポリシーを使用したスマートライセンシング環境での操作中に信頼コード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シング環境で実装したトポロジが「CSSMに直接接続」である場合、トポロジ実装の一部として信頼コードが必要であるため、信頼コードのインス

トールが想定または仮定されます。他のトポロジでは、信頼の確立は必須ではありません。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、スマートライセンシング環境で適用される手順に従って、ライセンスを登録済みおよび承認済みの状態に復元する必要が生じます。以下の表 5 : スマートライセンシングへの新規展開のダウングレードの結果とアクション （27 ページ）を参照してください。

表 *5:* スマートライセンシングへの新規展開のダウングレードの結果とアクション

ポリシーを使用したスマートライセンシング環境で	以下にダウングレードした場合…	結果と追加のアクション
CSSM に直接接続され、信頼が確立されたスタンドアロン製品インスタンス。	Cisco IOS XE Amsterdam 17.3.1 または Cisco IOS XE Gibraltar 16.12.x の Cisco IOS XE Gibraltar 16.12.4 以降のリリース または Cisco IOS XE Fuji 16.9.x の Cisco IOS XE Fuji 16.9.6 以降のリリース	これ以上の操作は不要です。 製品インスタンスは、ダウングレード後に CSSM からの信頼を更新しようとします。 更新が正常に完了すると、ライセンスは登録済みの状態になり、以前のバージョンのスマートライセンシングが製品インスタンスで有効になります。
	スマートライセンシングをサポートするその他のリリース（上の行に記載されているものを除く）	アクションが必要です。製品インスタンスを再登録する必要があります。 CSSM Web UI で ID トークンを生成し、製品インスタンスで、グローバル コンフィギュレーション モードで **license smart register idtoken** *idtoken* コマンドを設定します。
CSSM に直接接続され、信頼が確立された高可用性セットアップ。	スマートライセンシングをサポートするすべてのリリース	アクションが必要です。製品インスタンスを再登録する必要があります。 CSSM Web UI で ID トークンを生成し、製品インスタンスで、グローバル コンフィギュレーション モードで **license smart register idtoken** *idtoken* **all** コマンドを設定します。

ポリシーを使用したスマートライセンシング環境で	以下にダウングレードした場合...	結果と追加のアクション
その他のトポロジ。（CSLUを介したCSSMへの接続、CSLUはCSSMから切断、CSSMへの接続なし、CSLUなし）	スマートライセンシングをサポートするすべてのリリース	アクションが必要です。 スマートライセンシング環境で適用される手順に従って、ライセンスを登録済みおよび承認済みの状態に復元します。

アップグレード後のダウングレード

ポリシーを使用したスマートライセンシングをサポートするソフトウェアバージョンにアップグレードした後、以前のライセンシングモデルのいずれかにダウングレードしても、ライセンスの使用は変更されず、製品インスタンスで設定した製品機能は維持されます。ポリシーを使用したスマートライセンシングで使用可能な機能のみが使用できなくなります。以前のライセンシングモデルへの復帰の詳細については、以下の対応するセクション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シングへのアップグレード後のスマートライセンシングへのダウングレード

ダウングレードの結果は、ポリシーを使用したスマートライセンシング環境での操作中に信頼コード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。「表6:ポリシーを使用したスマートライセンシングへのアップグレード後のスマートライセンシングへのダウングレードの結果とアクション （29ページ）」を参照してください。

表 *6:* ポリシーを使用したスマートライセンシングへのアップグレード後のスマートライセンシングへのダウングレードの結果とアクション

ポリシーを使用したスマートライセンシング環境で	以下にダウングレードした場合…	結果と追加のアクション
CSSM に直接接続され、信頼が確立されたスタンドアロン製品インスタンス。	Cisco IOS XE Amsterdam 17.3.1 または Cisco IOS XE Gibraltar 16.12.x の Cisco IOS XE Gibraltar 16.12.4 以降のリリース または Cisco IOS XE Fuji 16.9.x の Cisco IOS XE Fuji 16.9.6 以降のリリース	これ以上の操作は不要です。 システムは信頼コードを認識し、元の登録済み ID トークンに変換します。これにより、ライセンスは AUTHORIZED および REGISTERED の状態に戻ります。
	スマートライセンシングをサポートするその他のリリース（上の行に記載されているものを除く）	アクションが必要です。製品インスタンスを再登録する必要があります。 CSSM Web UI で ID トークンを生成し、製品インスタンスで、グローバル コンフィギュレーション モードで **license smart register idtoken***idtoken* コマンドを設定します。
CSSM に直接接続され、信頼が確立された高可用性セットアップ。	スマートライセンシングをサポートするすべてのリリース	アクションが必要です。製品インスタンスを再登録する必要があります。 CSSM Web UI で ID トークンを生成し、製品インスタンスで、グローバル コンフィギュレーション モードで **license smart register idtoken** *idtoken* **all** コマンドを設定します。
その他のトポロジ（CSLU を介した CSSM への接続、CSLU は CSSM から切断、CSSM への接続なし、CSLU なし）	スマートライセンシングをサポートするすべてのリリース	アクションが必要です。 スマートライセンシング環境で適用される手順に従って、ライセンスを登録済みおよび承認済みの状態に復元します。

（注） スマートライセンシング環境で評価状態または期限切れ状態になっていたライセンスは、ダウングレード後に同じ状態に戻ります。

ポリシーを使用したスマートライセンシングへのアップグレード後の SLR へのダウングレード

SLR に戻すのに必要な操作は、イメージのダウングレードのみです。ライセンスは予約済みおよび承認済みのままになります。これ以上の操作は必要ありません。

ただし、ポリシーを使用したスマートライセンシング環境で SLR に戻した場合は、サポートされているリリースで、必要に応じて SLR を取得するプロセスを繰り返す必要があります。

RTU へのダウングレード

RTU に戻すのに必要な操作は、イメージのダウングレードのみです。

RTU ライセンシング環境で評価状態または期限切れ状態であったライセンスは、ダウングレード後に同じ状態に戻ります。

ポリシーを使用したスマートライセンシングの設定方法：トポロジ別のワークフロー

このセクションでは、トポロジを実装する最も簡単で迅速な方法について説明します。

（注） これらのワークフローは、新規展開のみに該当します。既存のライセンシングモデルから移行する場合は、ポリシーを使用したスマートライセンシングへの移行 （48 ページ） を参照してください。

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

CSLU のインストール→CSLU の環境設定→製品インスタンスの設定

1. ***CSLU* のインストール**

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

[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 Quick Start Setup Guide』を参照してください。

2. ***CSLU* の環境設定**

   タスクの実行場所：CSLU 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） （72 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） （73 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） （73 ページ）

3. **製品インスタンスの設定**

   タスクが実行される場所：製品インスタンス

   1. 製品インスタンス開始型通信のネットワーク到達可能性の確認 （74 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。構成ファイルへの変更を保存します。

      ```
      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
Device(config)# exit
Device# copy running-config startup-config
```

4. **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：製品インスタンス

   輸出規制ライセンスは、Cisco Catalyst アクセス、コア、およびアグリゲーションスイッチの特定のモデルでのみサポートされます（承認コード （7 ページ）を参照）。輸出規制ライセンスを使用する場合は、サポートされているプラットフォームで次のタスク：SLAC の手動要求と自動インストール （106 ページ）を実行します。

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、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、信頼コードを含む 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。

製品インスタンスがこの情報をいつ送信するかを確認するには、特権 EXEC モードで **show license all** コマンドを入力し、出力で `Next report push:` フィールドの日付を確認します。

ブートレベルライセンスを変更する場合は、基本ライセンスまたはアドオンライセンスの設定（128 ページ）を参照してください。

承認コードを返す場合は、承認コードの返却 （112 ページ）を参照してください。

CSLU 開始型通信の場合のタスク

CSLU のインストール → CSLU の設定 → 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） → 使用状況の同期

1. ***CSLU* のインストール**

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

[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 Quick Start Setup Guide』を参照してください。

2. ***CSLU* の環境設定**

   タスクの実行場所：CSLU 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） （72 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） （73 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） （75 ページ）

3. **製品インスタンスの設定**

   タスクが実行される場所：製品インスタンス

   CSLU 開始型通信のネットワーク到達可能性の確認 （78 ページ）

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：CSLU インターフェイスと CSSM Web UI

   輸出規制ライセンスは、Cisco Catalyst アクセス、コア、およびアグリゲーションスイッチの特定のモデルでのみサポートされます（承認コード （7 ページ）を参照）。輸出規制ライセンスを使用する場合は、サポートされているプラットフォームで次のタスクを実行します。

   1. SLAC の手動要求と自動インストール （106 ページ）
   2. 1 つ以上の製品インスタンスの SLAC の要求（CSLU インターフェイス） （83 ページ）
   3. CSSM からの SLAC の生成とファイルへのダウンロード （110 ページ）
   4. CSSM からのインポート（CSLU インターフェイス） （78 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） （76 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。この最初のレポートとともに、CSLU は承認コード要求を CSSM に送信します（該当する場合）。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。

ブートレベルライセンスを変更する場合は、基本ライセンスまたはアドオンライセンスの設定（128 ページ）を参照してください。

承認コードを返す場合は、承認コードの返却 （112 ページ）を参照してください。

トポロジのワークフロー：CSSM に直接接続

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

1. **スマートアカウントのセットアップ**

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

   スマートアカウントと必要なバーチャルアカウントへの適切なアクセス権を持つユーザロールがあることを確認します。

2. **製品インスタンスの設定**

   タスクが実行される場所：製品インスタンス

   1. CSSM への製品インスタンス接続の設定：CSSM への接続の設定 （84 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を保存します。

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

      - オプション 2：

        HTTPS プロキシを介してスマートトランスポートを設定します。HTTPS プロキシを介したスマート転送の設定 （86 ページ） を参照してください

      - オプション 3：

        ダイレクトクラウドアクセス用に Call Home サービスを設定します。「ダイレクトクラウドアクセス用の Call Home サービスの設定 （88 ページ）」を参照してください。

      - オプション 4：

        HTTPS プロキシを介したダイレクトクラウドアクセス用に Call Home サービスを設定します。「HTTPS プロキシサーバを介したダイレクトクラウドアクセス用の Call Home サービスの設定 （91 ページ）」を参照してください。

3. ***CSSM* との信頼の確立**

   タスクが実行される場所：CSSM Web UI、次に製品インスタンス

   1. 所有するバーチャルアカウントごとに 1 つのトークンを生成します。1 つのバーチャルアカウントに属するすべての製品インスタンスに同じトークンを使用できます（CSSM からの信頼コード用新規トークンの生成 （118 ページ））。
   2. トークンをダウンロードしたら、製品インスタンスに信頼コードをインストールできます（信頼コードのインストール （119 ページ））。

4. **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：製品インスタンス

   輸出規制ライセンスは、Cisco Catalyst アクセス、コア、およびアグリゲーションスイッチの特定のモデルでのみサポートされます（承認コード （7 ページ）を参照）。輸出規制ライセンスを使用する場合は、サポートされているプラットフォームで次のタスク：SLAC の手動要求と自動インストール （106 ページ）を実行します。

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。

以下は、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 以降のリリースのみに適用されます。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。

より頻繁にレポートを作成するようにレポート間隔を変更する場合は、製品インスタンスで、グローバル コンフィギュレーション モードで **license smart usage interval** コマンドを設定します。シンタックスの詳細については、対応するリリースのコマンドリファレンスで *license smart (privileged EXEC)* コマンドを参照してください。

ブートレベルライセンスを変更する場合は、基本ライセンスまたはアドオンライセンスの設定 （128 ページ）を参照してください。

承認コードを返す場合は、承認コードの返却 （112 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

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、実行する必要の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。

   2. 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。

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。

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

CSLU のインストール → CSLU の設定 → 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） → 使用状況の同期

1. ***CSLU* のインストール**

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

   [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 Quick Start Setup Guide』を参照してください。

2. ***CSLU* の環境設定**

   タスクの実行場所：CSLU インターフェイス

   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） （73 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） （73 ページ）

3. **製品インスタンスの設定**

   タスクが実行される場所：製品インスタンス

   1. 製品インスタンス開始型通信のネットワーク到達可能性の確認 （74 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。構成ファイルへの変更を保存します。

      ```
      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
Device(config)# exit
Device# copy running-config startup-config
```

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は、Cisco Catalyst アクセス、コア、およびアグリゲーションスイッチの特定のモデルでのみサポートされます（承認コード （7 ページ）を参照）。輸出規制ライセンスを使用する場合は、サポートされているプラットフォームで次のタスクを実行します。

   1. SLAC の手動要求と自動インストール （106 ページ）
   2. 1 つ以上の製品インスタンスの SLAC の要求（CSLU インターフェイス） （83 ページ）
   3. CSSM からの SLAC の生成とファイルへのダウンロード （110 ページ）
   4. CSSM からのインポート（CSLU インターフェイス） （78 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。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）（77 ページ）
2. CSSM への使用状況データのアップロードと ACK のダウンロード（121 ページ）
3. CSSM からのインポート（CSLU インターフェイス）（78 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。

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。

ブートレベルライセンスを変更する場合は、基本ライセンスまたはアドオンライセンスの設定（128 ページ）を参照してください。

承認コードを返す場合は、承認コードの返却（112 ページ）を参照してください。

CSLU 開始型通信の場合のタスク

CSLU のインストール → CSLU の設定 → 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） → 使用状況の同期

1. ***CSLU* のインストール**

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

   [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 Quick Start Setup Guide』を参照してください。

2. ***CSLU* の環境設定**

   タスクの実行場所：CSLU

   1. CSLU の [Preferences] タブで、[Cisco Connectivity] トグルスイッチを**オフ**にします。フィールドが「Cisco Is Not Available」に切り替わります。
   2. スマートアカウントとバーチャルアカウントの設定（CSLU インターフェイス）（73 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）（75 ページ）
4. 使用状況レポートの収集：CSLU 開始（CSLU インターフェイス）（76 ページ）

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

   CSLU 開始型通信のネットワーク到達可能性の確認（78 ページ）

4. **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：製品インスタンス

   輸出規制ライセンスは、Cisco Catalyst アクセス、コア、およびアグリゲーションスイッチの特定のモデルでのみサポートされます（承認コード（7 ページ）を参照）。輸出規制ライセンスを使用する場合は、サポートされているプラットフォームで次のタスクを実行します。

   1. SLAC の手動要求と自動インストール（106 ページ）
   2. 1 つ以上の製品インスタンスの SLAC の要求（CSLU インターフェイス）（83 ページ）
   3. CSSM からの SLAC の生成とファイルへのダウンロード（110 ページ）
   4. CSSM からのインポート（CSLU インターフェイス）（78 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。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。

   1. CSSM へのエクスポート（CSLU インターフェイス）（77 ページ）
   2. CSSM への使用状況データのアップロードと ACK のダウンロード（121 ページ）
   3. CSSM からのインポート（CSLU インターフェイス）（78 ページ）

結果：

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。

ブートレベルライセンスを変更する場合は、基本ライセンスまたはアドオンライセンスの設定（128 ページ）を参照してください。

承認コードを返す場合は、承認コードの返却 （112 ページ）を参照してください。

トポロジのワークフロー：CSSM への接続なし、CSLU なし

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

製品インスタンスの設定→承認コードのインストール（該当する場合のみ）

1. **製品インスタンスの設定**

   タスクの実行場所：製品インスタンス

   転送タイプを**オフ**に設定します。

   グローバル コンフィギュレーション モードで **license smart transport off** コマンドを入力します。構成ファイルへの変更を保存します。

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

2. **承認コードのインストール（該当する場合のみ）**

   タスクが実行される場所：CSSM Web UI および製品インスタンス

   輸出規制ライセンスは、Cisco Catalyst アクセス、コア、およびアグリゲーションスイッチの特定のモデルでのみサポートされます（承認コード （7 ページ）を参照）。輸出規制ライセンスを使用する場合は、サポートされているプラットフォームで次のタスクを実行します。

   1. CSSM からの SLAC の生成とファイルへのダウンロード （110 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 （122 ページ）。

結果：

製品インスタンスからのすべての通信を無効にします。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アップロード）。

1. RUM レポートの生成と保存

   license smart save usage コマンドは特権 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。この例では、ファイルはまずブートフラッシュに保存され、次に TFTP の場所にコピーされます。

   ```
   Device# license smart save usage all bootflash:all_rum.txt
   Device# copy bootflash:all_rum.txt tftp://10.8.0.6/user01/
   ```

2. 使用状況データを CSSM にアップロード： CSSM への使用状況データのアップロードと ACK のダウンロード （121 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 （122 ページ）

ブートレベルライセンスを変更する場合は、基本ライセンスまたはアドオンライセンスの設定（128 ページ）を参照してください。

承認コードを返す場合は、承認コードの返却 （112 ページ）を参照してください。

トポロジのワークフロー：SSM オンプレミス展開

製品インスタンス開始型通信（プッシュ）を実装するか、または SSM オンプレミス開始型通信（プル）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

SSM オンプレミスのインストール → 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. ***SSM* オンプレミスのインストール**

   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）。
- 使用前に承認が必要なライセンスを使用する場合（適用タイプ：適用（エンフォースメント）または輸出規制）：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。

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）（92ページ）
2. デバイスの検証（SSM オンプレミス UI）（93 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。

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. 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（94 ページ）
   2. トランスポート URL の取得（SSM オンプレミス UI）（96 ページ）
   3. 転送タイプ、URL、およびレポート間隔の設定（124 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. 輸出規制ライセンスは、Cisco Catalystアクセス、コア、およびアグリゲーションスイッチの特定のモデルでのみサポートされます（承認コード（7ページ）を参照）。サポートされているプラットフォームで輸出規制対象ライセンスを使用する場合にのみ、次のサブステップ：承認コード要求の送信（SSMオンプレミスUI）（105ページ）およびSLACの手動要求と自動インストール（106ページ）を実行します。

4. **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 UI、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。

```
Device(config)# license smart sync local
```

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）（97 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。

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。

  以下は、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 以降のリリースのみに適用されます。製品インスタンス開始モードで、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、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） （97 ページ））。

ブートレベルライセンスを変更する場合は、基本ライセンスまたはアドオンライセンスの設定（128 ページ）を参照してください。

承認コードを返す場合は、承認コードの返却 （112 ページ）を参照してください。

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 → 製品インスタンスの追加 → 製品インスタンスの設定 → 使用状況の最初の同期

1. ***SSM* オンプレミスのインストール**

   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）（98 ページ））を実行します。

3. **製品インスタンスの設定**

   タスクが実行される場所：製品インスタンス

   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 （99 ページ）
   2. 輸出規制ライセンスは、Cisco Catalyst アクセス、コア、およびアグリゲーションスイッチの特定のモデルでのみサポートされます（承認コード （7 ページ）を参照）。サポートされているプラットフォームで輸出規制ライセンスを使用する場合にのみ、次のサブステップを実行します。承認コード要求の送信（SSM オンプレミス UI） （105 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ます。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、その後に完了します。

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。

      [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） （97 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。

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に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） （97 ページ））。

ブートレベルライセンスを変更する場合は、基本ライセンスまたはアドオンライセンスの設定（128 ページ）を参照してください。

承認コードを返す場合は、承認コードの返却 （112 ページ）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シングへの移行

ポリシーを使用したスマートライセンシングにアップグレードするには、製品インスタンスのソフトウェアバージョン（イメージ）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

ポリシーを使用したスマートライセンシングによって以前の全ライセンスモデルのさまざまな側面がどのように処理されるかを理解するため、アップグレード （24 ページ） のセクションを必ずお読みください。

ポリシーを使用したスマートライセンシングは、Cisco IOS XE Amsterdam 17.3.2 で導入されました。そのため、これがポリシーを使用したスマートライセンシングに最低限必要なバージョンになります。

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。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。

デバイス先行の変換は、ポリシーを使用したスマートライセンシングへの移行ではサポートされていません。

スイッチ ソフトウェアのアップグレード

アップグレードの手順については、対応するリリースノートを参照してください。一般的なリリース固有の考慮事項がある場合は、対応するリリースノートに記載されています。たとえば、Cisco IOS XE Amsterdam 17.3.2 にアップグレードするには、『*Release Notes for Cisco* <プラットフォーム名>*, Cisco IOS XE Amsterdam 17.3.x*』を参照してください。

この手順を使用して、インストールモードで、または In-Service Software Upgrade（ISSU）を使用してアップグレードできます（サポートされているプラットフォームおよびサポートされているリリースで実行）。

Release Notes for Cisco Catalyst 9300 シリーズ スイッチ：https://www.cisco.com/c/en/us/support/switches/catalyst-9300-series-switches/products-release-notes-list.html。「スイッチソフトウェアのアップグレード」を参照してください。ISSU は、この製品インスタンスではサポートされていません。

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。

- ライセンスの使用状況と CSSM の同期

  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 （25 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、例ではなく、移行の順序が示されています。

例：スマートライセンシングからポリシーを使用したスマートライセンシングへ

次に、スマートライセンシングからポリシーを使用したスマートライセンシングに移行する Cisco Catalyst 9500 スイッチの例を示します。これはアクティブとスタンバイを含む高可用性セットアップの例です。

- 表 7 : スマートライセンシングからポリシーを使用したスマートライセンシングへ：show コマンド
- 移行後の CSSM Web UI （53 ページ）
- 移行後のレポート （54 ページ）

show コマンドは、移行の前後に確認すべき以下の重要なフィールドを抽出して出力します。

表 7 : スマートライセンシングからポリシーを使用したスマートライセンシングへ：*show* コマンド

アップグレード前	アップグレード後

show license summary（スマートライセンシング）
 	
Statusフィールドと License Authorization フィールドに、ライセンスについて REGISTERED および AUTHORIZED と表示されます。
 	
`Device# show license summary`
 	
`Smart Licensing is ENABLED`
`Registration:`
`Status: REGISTERED`
`Smart Account: SA-Eg-Company-01`
`Virtual Account: SLE_Test`
`Export-Controlled Functionality: ALLOWED`
`Last Renewal Attempt: None`
`Next Renewal Attempt: Mar 21 11:08:58 2021 PST`
`License Authorization:`
`Status: AUTHORIZED`
`Last Communication Attempt: SUCCEEDED`
`Next Communication Attempt: Oct 22 11:09:07 2020 PST`
`License Usage:`
`License Entitlement tag Count Status`
`---`
`C9500 Network Advantage (C9500 Network Advantage) 2 AUTHORIZED`
`C9500-DNA-16X-A (C9500-16X DNA Advantage) 2 AUTHORIZED`
	show license summary（ポリシーを使用したスマートライセンシング）
	
	Status フィールドに、ライセンスについて、登録済みおよび承認済みではなく IN USE と表示されます。
	
	`Device# show license summary`
	`License Usage:`
	`License Entitlement tag Count Status`
	`---`
	`network-advantage (C9500 Network Advantage) 2 IN USE`
	`dna-advantage (C9500-16X DNA Advantage) 2 IN USE`

show license usage（スマートライセンシング）	**show license usage**（ポリシーを使用したスマートライセンシ ライセンス数は変わりません。 [Enforcement Type] フィールドに NOT ENFORCED と表示さす。これは、アップグレード前に使用されていたすべてのラスが不適用ライセンスであったためです。

```
Device# show license usage
License Authorization:
Status: AUTHORIZED on Sep 22 11:09:07 2020 PST
C9500 Network Advantage (C9500 Network Advantage):
Description: C9500 Network Advantage
Count: 2
Version: 1.0
Status: AUTHORIZED
Export status: NOT RESTRICTED
C9500-DNA-16X-A (C9500-16X DNA Advantage):
Description: C9500-DNA-16X-A
Count: 2
Version: 1.0
Status: AUTHORIZED
Export status: NOT RESTRICTED
```

```
Device# show license usage


License Authorization:
  Status: Not Applicable
network-advantage (C9500 Network Advantage):
  Description: network-advantage
  Count: 2
  Version: 1.0
  Status: IN USE
  Export status: NOT RESTRICTED
  Feature Name: network-advantage
  Feature Description: network-advantage
  Enforcement type: NOT ENFORCED
  License type: Perpetual
dna-advantage (C9500-16X DNA Advantage):
  Description: C9500-16X DNA Advantage
  Count: 2  Version: 1.0
  Status: IN USE
  Export status: NOT RESTRICTED
  Feature Name: dna-advantage
  Feature Description: C9500-16X DNA Advantage
  Enforcement type: NOT ENFORCED
  License type: Subscription
```

show license status（スマートライセンシング）

show license status（ポリシーを使用したスマートライセンシング）

`Transport:` フィールド：特定の転送タイプが設定されたため、アップグレード後もその設定が保持されます。

`Policy:` ヘッダーと詳細：スマートアカウントまたはバーチャルアカウントでカスタムポリシーを使用できます。これは製品インスタンスにも自動的にインストールされます。（信頼を確立した後、CSSMはポリシーを返します。その後、このポリシーが自動的にインストールされます）。

`Usage Reporting:` ヘッダー：`Next report push:` フィールドには、製品インスタンスが次のRUMレポートをCSSMに送信するタイミングについての情報が表示されます。

`Trust Code Installed:` フィールド：IDトークンが正常に変換され、信頼できる接続がCSSMで確立されたことを示します。

例：スマートライセンシングからポリシーを使用したスマートライセンシングへ

```
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 Sep 22 11:08:58 2020 PST
Last Renewal Attempt: None
Next Renewal Attempt: Mar 21 11:08:57 2021 PST
Registration Expires: Sep 22 11:04:23 2021 PST
License Authorization:
Status: AUTHORIZED on Sep 22 11:09:07 2020 PST
Last Communication Attempt: SUCCEEDED on Sep 22 11:09:07 2020
PST
Next Communication Attempt: Oct 22 11:09:06 2020 PST
Communication Deadline: Dec 21 11:04:34 2020 PST
Export Authorization Key:
Features Authorized:
<none>
Miscellaneus:
Custom Id: <empty>
```

```
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: 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: 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>
Trust Code Installed:
  Active: PID:C9500-16X,SN:FCW2233A5ZV
  INSTALLED on Sep 22 12:02:20 2020 PST
  Standby: PID:C9500-16X,SN:FCW2233A5ZY
  INSTALLED on Sep 22 12:02:20 2020 PST
```

show license udi（スマートライセンシング）	**show license udi**（スマートライセンシング）
	これは高可用性セットアップであり、このコマンドによってセットアップ内のすべての UDI が表示されます。

`Device# show license udi`
 	
`UDI: PID:C9500-16X,SN:FCW2233A5ZV`
`HA UDI List:`
`Active:PID:C9500-16X,SN:FCW2233A5ZV`
`Standby:PID:C9500-16X,SN:FCW2233A5ZY`
	`Device# show license udi`
	
	`UDI: PID:C9500-16X,SN:FCW2233A5ZV`
	`HA UDI List:`
	`Active:PID:C9500-16X,SN:FCW2233A5ZV`
	`Standby:PID:C9500-16X,SN:FCW2233A5ZY`

移行後の CSSM Web UI

https://software.cisco.com で CSSM Web UI にログインします。[Smart Software Licensing] で、[Manage licenses] リンクをクリックします。

[Inventory] タブをクリックします。[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。[Product Instances] タブをクリックします。

スマートライセンシング環境で登録されたライセンスは、製品インスタンスのホスト名と共に [Name] 列に表示されていました。ポリシーを使用したスマートライセンシングにアップグレードすると、製品インスタンスの UDI と共に表示されるようになります。移行したすべての UDI が表示されます。この例では、PID:C9500-16X,SN:FCW2233A5ZV および PID:C9500-16X,SN:FCW2233A5ZY がこれに該当します。

アクティブな製品インスタンスの使用状況のみが報告されるため、PID:C9500-16X,SN:FCW2233A5ZV の [License Usage] にはライセンス使用情報が表示されます。スタンバイの使用状況は報告されず、スタンバイの [License Usage] セクションには [No Records Found] と表示されます。

常にアクティブの使用状況が報告されるため、この高可用性セットアップのアクティブが変更されると、新しいアクティブな製品インスタンスのライセンス使用情報が表示され、使用状況が報告されるようになります。

図 7:スマートライセンシングからポリシーを使用したスマートライセンシングへ：移行後のアクティブおよびスタンバイ製品インスタンス

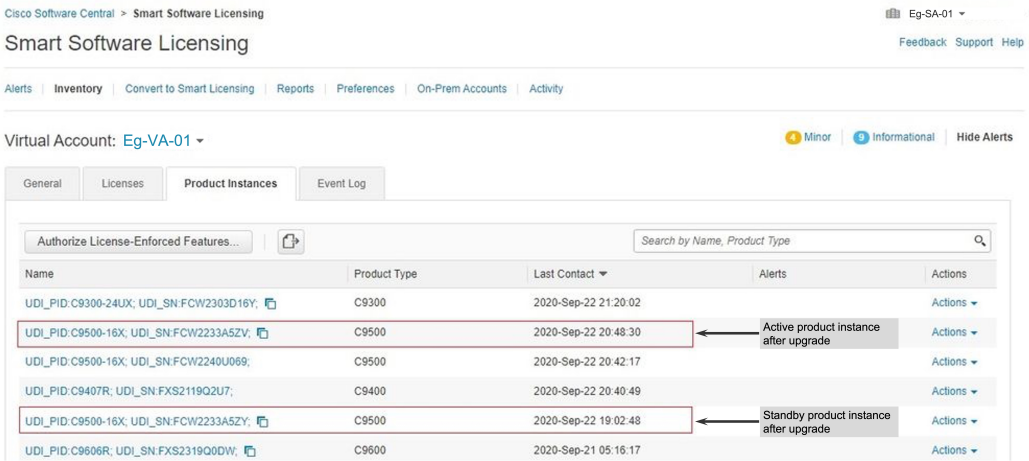
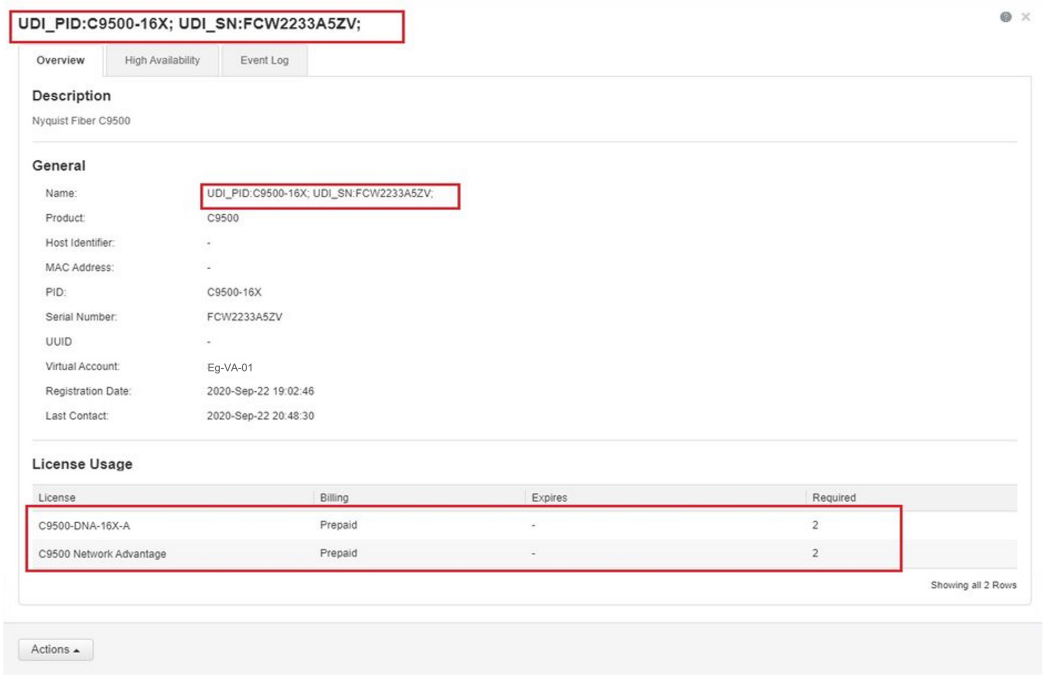


図 *8:* スマートライセンシングからポリシーを使用したスマートライセンシングへ：アクティブな製品インスタンスでの *UDI* とライセンス使用状況



移行後のレポート

製品インスタンスは、ポリシーに基づいて次の RUM レポートを CSSM に送信します。

より頻繁にレポートを作成するようにレポート間隔を変更する場合は、製品インスタンスで **license smart usage interval** コマンドを設定します。シンタックスの詳細については、対応するリリースのコマンドリファレンスで *license smart (global config)* コマンドを参照してください。

例：RTU ライセンシングからポリシーを使用したスマートライセンシングへ

次に、使用権（RTU）ライセンシングからポリシーを使用したスマートライセンシングに移行する Cisco Catalyst 9300 スイッチの例を示します。これはアクティブと他のメンバーを含むセットアップの例です。

RTU ライセンシングは、Cisco IOS XE Fuji 16.8.x までの Cisco Catalyst 9300、9400、および 9500 シリーズ スイッチで使用できます。スマートライセンシングは、Cisco IOS XE Fuji 16.9.1 から導入されました。

ソフトウェアバージョンを、ポリシーを使用したスマートライセンシングをサポートするバージョンにアップグレードすると、すべてのライセンスが IN USE として表示され、`Cisco default` ポリシーが製品インスタンスに適用されます。アドオンライセンスが使用されている場合、`Cisco default` ポリシーでは 90 日間の使用状況レポートが必要です。RTU ライセンスモデルがサポートされていたときに Cisco Catalyst アクセス、コア、およびアグリゲーションスイッチ

で使用可能な輸出規制ライセンスまたは適用ライセンスはなかったため、どの機能も失われていません。

- 表 8 : RTU ライセンシングからポリシーを使用したスマートライセンシングへ：show コマンド
- 移行後の CSSM Web UI （57 ページ）
- 移行後のレポート （57 ページ）

次の表に、ポリシーを使用したスマートライセンシングへのアップグレード後に、**show** コマンドの出力でチェックすべき主な変更点または新しいフィールドを示します。

表 *8 : RTU* ライセンシングからポリシーを使用したスマートライセンシングへ：*show* コマンド

アップグレード前	アップグレード後

show license right-to-use summary（RTU ライセンシング）
 	
`Device# show license right-to-use summary`
`License Name Type Period left`
`------------------------------------------------`
`network-essentials Permanent Lifetime`
`dna-essentials Subscription CSSM Managed`
`------------------------------------------------`
 	
`License Level In Use: network-essentials+dna-essentials Subscription`
`License Level on Reboot:`
`network-essentials+dna-essentials Subscription`
	show license summary（ポリシーを使用したスマートライセンシング）
	
	すべてのライセンスが移行され、IN USE になっています。
	
	`Device#show license summary`
	`License Usage:`
	`License Entitlement Tag Count Status`
	`------------------------------------------------------------`
	`network-essentials (C9300-24 Network Essen...) 2 IN USE`
	`dna-essentials (C9300-24 DNA Essentials) 2 IN USE`
	`network-essentials (C9300-48 Network Essen...) 1 IN USE`
	`dna-essentials (C9300-48 DNA Essentials) 1 IN USE`

show license right-to-use usage（スマートライセンシング）	**show license usage**（ポリシーを使用したスマートライセンシング） すべてのライセンス（無期限、サブスクリプション）が移行され、それらのライセンスは現在 IN USE になっており、タイプには Perpetual と Subscription があります。 [Enforcement Type] フィールドに NOT ENFORCED と表示されます。これは、アップグレード前に使用されていたすべてのライセンスが不適用ライセンスであったためです。

```
Device# show license right-to-use usage

Slot# License Name Type usage-duration(y:m:d) In-Use
EULA
-------------------------------------------------------
1 network-essentials Permanent 00:00:00 yes yes
1 network-essentials Evaluation 00:00:00 no no
1 network-essentials Subscription 00:00:00 no no
1 network-advantage Permanent 00:00:00 no no
1 network-advantage Evaluation 00:00:00 no no
1 network-advantage Subscription 00:00:00 no no
1 dna-essentials Evaluation 00:00:00 no no
1 dna-essentials Subscription 00:00:00 yes yes
1 dna-advantage Evaluation 00:00:00 no no
1 dna-advantage Subscription 00:00:00 no no
-------------------------------------------------------
Slot# License Name Type usage-duration(y:m:d) In-Use
EULA
-------------------------------------------------------
2 network-essentials Permanent 00:00:00 yes yes
2 network-essentials Evaluation 00:00:00 no no
2 network-essentials Subscription 00:00:00 no no
2 network-advantage Permanent 00:00:00 no no
2 network-advantage Evaluation 00:00:00 no no
2 network-advantage Subscription 00:00:00 no no
2 dna-essentials Evaluation 00:00:00 no no
2 dna-essentials Subscription 00:00:00 yes yes
2 dna-advantage Evaluation 00:00:00 no no
2 dna-advantage Subscription 00:00:00 no no
-------------------------------------------------------
Slot# License Name Type usage-duration(y:m:d) In-Use
EULA
-------------------------------------------------------
3 network-essentials Permanent 00:00:00 yes yes
3 network-essentials Evaluation 00:00:00 no no
3 network-essentials Subscription 00:00:00 no no
3 network-advantage Permanent 00:00:00 no no
3 network-advantage Evaluation 00:00:00 no no
3 network-advantage Subscription 00:00:00 no no
3 dna-essentials Evaluation 00:00:00 no no
3 dna-essentials Subscription 00:00:00 yes yes
3 dna-advantage Evaluation 00:00:00 no no
3 dna-advantage Subscription 00:00:00 no no
-------------------------------------------------------
```

```
Device# show license usage

License Authorization:
  Status: Not Applicable
network-advantage (C9300-24 Network Advantage):
  Description: C9300-24 Network Advantage
  Count: 2
  Version: 1.0
  Status: IN USE
  Export status: NOT RESTRICTED
  Feature Name: network-advantage
  Feature Description: C9300-24 Network Advantage
  Enforcement type: NOT ENFORCED
  License type: Perpetual
dna-advantage (C9300-24 DNA Advantage):
  Description: C9300-24 DNA Advantage
  Count: 2
  Version: 1.0
  Status: IN USE
  Export status: NOT RESTRICTED
  Feature Name: dna-advantage
  Feature Description: C9300-24 DNA Advantage
  Enforcement type: NOT ENFORCED
  License type: Subscription
network-advantage (C9300-48 Network Advantage):
  Description: C9300-48 Network Advantage
  Count: 1
  Version: 1.0
  Status: IN USE
  Export status: NOT RESTRICTED
  Feature Name: network-advantage
  Feature Description: C9300-48 Network Advantage
  Enforcement type: NOT ENFORCED
  License type: Perpetual
dna-advantage (C9300-48 DNA Advantage):
  Description: C9300-48 DNA Advantage
  Count: 1
  Version: 1.0
  Status: IN USE
  Export status: NOT RESTRICTED
  Feature Name: dna-advantage
  Feature Description: C9300-48 DNA Advantage
  Enforcement type: NOT ENFORCED
  License type: Subscription
```

show license right-to-use（RTU ライセンシング）

show license status（ポリシーを使用したスマートライセンシング）

`Transport:` フィールドにオフになっていることが表示されます。

`Trust Code Installed:` フィールドには、信頼コードがインストールされていないことが表示されます。

`Usage Reporting:` ヘッダーの `Next report push:` フィールドには、次の RUM レポートを CSSM に送信するタイミングに関する情報が表示されます。

```
Device# show license right-to-use
Slot# License Name Type Period left
--------------------------------------------------
1 network-essentials Permanent Lifetime
1 dna-essentials Subscription CSSM Managed
--------------------------------------------------
License Level on Reboot:
network-essentials+dna-essentials
Subscription

Slot# License Name Type Period left
--------------------------------------------------
2 network-essentials Permanent Lifetime
2 dna-essentials Subscription CSSM Managed
--------------------------------------------------
License Level on Reboot:
network-essentials+dna-essentials
Subscription

Slot# License Name Type Period left
--------------------------------------------------
3 network-essentials Permanent Lifetime
3 dna-essentials Subscription CSSM Managed
--------------------------------------------------
License Level on Reboot:
network-essentials+dna-essentials
Subscription
```

```
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: 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 26 10:27:59 2021 PST
  Reporting push interval: 20  days
  Next ACK push check: <none>
  Next report push: Oct 28 10:29:59 2020 PST
  Last report push: <none>
  Last report file write: <none>
Trust Code Installed: <none>
```

移行後の CSSM Web UI

CSSM Web UI に変更はありません。

移行後のレポート

サポートされているトポロジのいずれかを実装し、レポート要件に適合するようにします。サポートされるトポロジ （11 ページ）およびポリシーを使用したスマートライセンシングの設定方法：トポロジ別のワークフロー （30 ページ）を参照してください。使用可能なレポートメソッドは、実装するトポロジによって異なります。

例：SLR からポリシーを使用したスマートライセンシングへ

次に、特定のライセンス予約（SLR）からポリシーを使用したスマートライセンシングに移行する Cisco Catalyst 9500 スイッチの例を示します。これはアクティブとスタンバイを含む高可用性セットアップの例です。

ライセンスの変換は自動的に行われ、承認コードが移行されます。移行を完了するためにこれ以上の操作は必要ありません。移行後は CSSM への接続なし、CSLU なし （18 ページ） トポロジが有効になります。ポリシーを使用したスマートライセンシング環境の SLR 承認コードについては、承認コード （7 ページ） を参照してください。

- 表 9 : SLR からポリシーを使用したスマートライセンシングへ：show コマンド
- 移行後の CSSM Web UI （64 ページ）
- 移行後のレポート （65 ページ）

show コマンドは、移行の前後に確認すべき以下の重要なフィールドを抽出して出力します。

表 *9 : SLR* からポリシーを使用したスマートライセンシングへ：*show* コマンド

アップグレード前	アップグレード後

show license summary（SLR）
 	
`Registration` ステータスフィールドと `License Authorization` ステータスフィールドに、ライセンスについて `REGISTERED - SPECIFIC LICENSE RESERVATION` および `AUTHORIZED - RESERVED` と表示されます。
 	
`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: AUTHORIZED - RESERVED`
`License Usage:`
`License  Entitlement tag  Count Status`
`---`
`C9500 Network Advantage(C9500 Network Advantage)  2 AUTHORIZED`
`C9500-DNA-16X-A  (C9500-16X DNA Advantage)  2 AUTHORIZED`
	show license summary（ポリシーを使用したスマートライセンシング）
	
	`Status` フィールドに、ライセンスについて、登録済みおよび承認済みではなく `IN USE` と表示されます。
	
	`Device# show license summary`
	
	`License Reservation is ENABLED`
	`License Usage:`
	`License  Entitlement tag  Count Status`
	`---`
	`network-advantage(C9500 Network Advantage)  2 IN USE`
	`dna-advantage  (C9500-16X DNA Advantage)  2 IN USE`

show license reservation（SLR）	**show license all**（ポリシーを使用したスマートライセンシング） `License Authorizations` ヘッダー：アクティブおよびスタンバイ製品インスタンスのベース（C9500 Network Advantage）ライセンスおよびアドオン（C9500-DNA-16X-A）ライセンスが特定のライセンス予約で承認されたことを示します。`Authorization type:` フィールドに SPECIFIC INSTALLED と表示されます。 `Last Confirmation code:` フィールド：高可用性セットアップのアクティブおよびスタンバイ製品インスタンスの SLR 承認コードが正常に移行されたことを示します。

例：**SLR** からポリシーを使用したスマートライセンシングへ

```
Device# show license reservation
License reservation: ENABLED
Overall status:
  Active: PID:C9500-16X,SN:FCW2233A5ZV
       Reservation status: SPECIFIC INSTALLED on Aug 31
 10:15:01 2020 PDT
       Export-Controlled Functionality: ALLOWED
       Last Confirmation code: 4bfbea7f
  Standby: PID:C9500-16X,SN:FCW2233A5ZY
       Reservation status: SPECIFIC INSTALLED on Aug 31
 10:15:01 2020 PDT
       Export-Controlled Functionality: ALLOWED
       Last Confirmation code: 9394f196
Specified license reservations:
  C9500 Network Advantage (C9500 Network Advantage):
    Description: C9500 Network Advantage
    Total reserved count: 2
    Term information:
      Active: PID:C9500-16X,SN:FCW2233A5ZV
        License type: PERPETUAL
          Term Count: 1
      Standby: PID:C9500-16X,SN:FCW2233A5ZY
        License type: PERPETUAL
          Term Count: 1
  C9500-DNA-16X-A (C9500-16X DNA Advantage):
    Description: C9500-DNA-16X-A
    Total reserved count: 2
    Term information:
      Active: PID:C9500-16X,SN:FCW2233A5ZV
        License type: TERM
          Start Date: 2020-MAR-17 UTC
          End Date: 2021-MAR-17 UTC
          Term Count: 1
      Standby: PID:C9500-16X,SN:FCW2233A5ZY
```

```
Device# show license reservation

Smart Licensing Status
======================
Smart Licensing is ENABLED
License Reservation is ENABLED
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: 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: Nov 29 10:50:05 2020 PDT
  Reporting Interval: 30
  Next ACK push check: <none>
  Next report push: Aug 31 10:52:05 2020 PDT
  Last report push: <none>
  Last report file write: <none>
Trust Code Installed: <none>
License Usage
=============
network-advantage (C9500 Network Advantage):
  Description: network-advantage
  Count: 2
  Version: 1.0
  Status: IN USE
  Export status: NOT RESTRICTED
  Feature Name: network-advantage
  Feature Description: network-advantage
  Enforcement type: NOT ENFORCED
```

```
  License type: Perpetual
  Reservation:
    Reservation status: SPECIFIC INSTALLED
    Total reserved count: 2
dna-advantage (C9500-16X DNA Advantage):
  Description: C9500-16X DNA Advantage
  Count: 2
  Version: 1.0
  Status: IN USE
  Export status: NOT RESTRICTED
  Feature Name: dna-advantage
  Feature Description: C9500-16X DNA Advantage
  Enforcement type: NOT ENFORCED
  License type: Subscription
  Reservation:
    Reservation status: SPECIFIC INSTALLED
    Total reserved count: 2
Product Information
==================
UDI: PID:C9500-16X,SN:FCW2233A5ZV
HA UDI List:
    Active:PID:C9500-16X,SN:FCW2233A5ZV
    Standby:PID:C9500-16X,SN:FCW2233A5ZY
Agent Version
=============
Smart Agent for Licensing: 5.0.5_rel/42
License Authorizations
======================
Overall status:
  Active: PID:C9500-16X,SN:FCW2233A5ZV
     Status: SPECIFIC INSTALLED on Aug 31 10:15:01 2020
 PDT
      Last Confirmation code: 4bfbea7f
  Standby: PID:C9500-16X,SN:FCW2233A5ZY
     Status: SPECIFIC INSTALLED on Aug 31 10:15:01 2020
 PDT
      Last Confirmation code: 9394f196
Specified license reservations:
  C9500 Network Advantage (C9500 Network Advantage):
    Description: C9500 Network Advantage
    Total reserved count: 2
    Enforcement type: NOT ENFORCED
    Term information:
      Active: PID:C9500-16X,SN:FCW2233A5ZV
        Authorization type: SPECIFIC INSTALLED on Aug
31 10:15:01 2020 PDT
        License type: PERPETUAL
          Term Count: 1
      Standby: PID:C9500-16X,SN:FCW2233A5ZY
        Authorization type: SPECIFIC INSTALLED on Aug
31 10:15:01 2020 PDT
        License type: PERPETUAL
          Term Count: 1
  C9500-DNA-16X-A (C9500-16X DNA Advantage):
    Description: C9500-DNA-16X-A
    Total reserved count: 2
    Enforcement type: NOT ENFORCED
    Term information:
      Active: PID:C9500-16X,SN:FCW2233A5ZV
        Authorization type: SPECIFIC INSTALLED on Aug
31 10:15:01 2020 PDT
        License type: PERPETUAL
          Term Count: 1
      Standby: PID:C9500-16X,SN:FCW2233A5ZY
```

	Authorization type: SPECIFIC INSTALLED on Aug 31 10:15:01 2020 PDT License type: PERPETUAL Term Count: 1 Purchased Licenses: No Purchase Information Available Derived Licenses: Entitlement Tag: regid.2017-03.com.cisco.advantagek9-Nyquist-C9500, 1.0_f1563759-2e03-4a4c-bec5-5feec525a12c Entitlement Tag: regid.2017-07.com.cisco.C9500-DNA-16X-A, 1.0_ef3574d1-156b-486a-864f-9f779ff3ee49
show license status（SLR）	**show license status**（ポリシーを使用したスマートライセンシング） `Transport:` ヘッダー：`Type:` は、転送タイプがオフに設定されていることを示します。 `Usage Reporting:` ヘッダー：`Next report push:` フィールドは、次の RUM レポートを CSSM にアップロードする必要があるかどうか、およびアップロードする必要があるのはいつかを示します。

```
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 Aug 31 11:07:39
2020 PDT
License Authorization:
  Status: AUTHORIZED - RESERVED on Aug 31 10:15:01 2020
 PDT
Export Authorization Key:
  Features Authorized:
    <none>
        License type: TERM
          Start Date: 2020-MAR-17 UTC
          End Date: 2021-MAR-17 UTC
          Term Count: 1
```

```
Device# show license status

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: 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: Nov 29 10:50:05 2020 PDT
  Reporting Interval: 30
  Next ACK push check: <none>
  Next report push: Aug 31 10:52:05 2020 PDT
  Last report push: <none>
  Last report file write: <none>
Trust Code Installed: <none>
```

移行後の CSSM Web UI

CSSM では、[Product Instances] タブに変更はありません。使用状況レポートがまだないため、[Last Contact] 列には「Reserved Licenses」と表示されます。

必要な RUM レポートがアップロードされ、「Reserved Licenses（予約済みライセンス）」が確認されると、ライセンスの使用状況がアクティブな PID 製品インスタンスのみで表示されるようになります。

図 *9*：*SLR* からポリシーを使用したスマートライセンシングへ：移行後、レポート前のアクティブおよびスタンバイ製品インスタンス

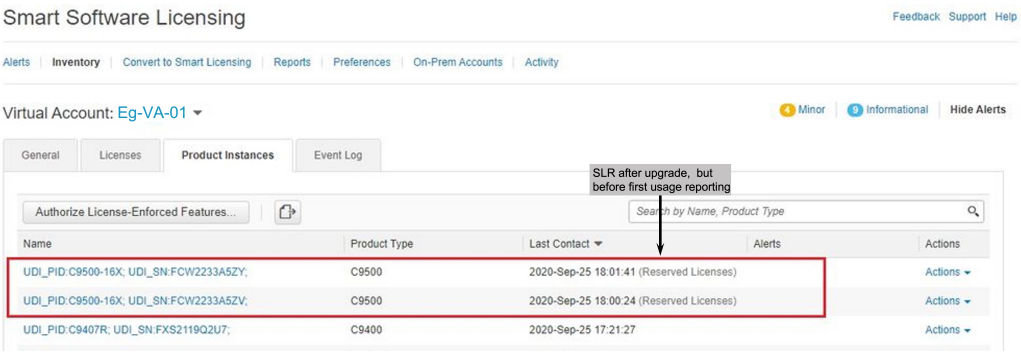
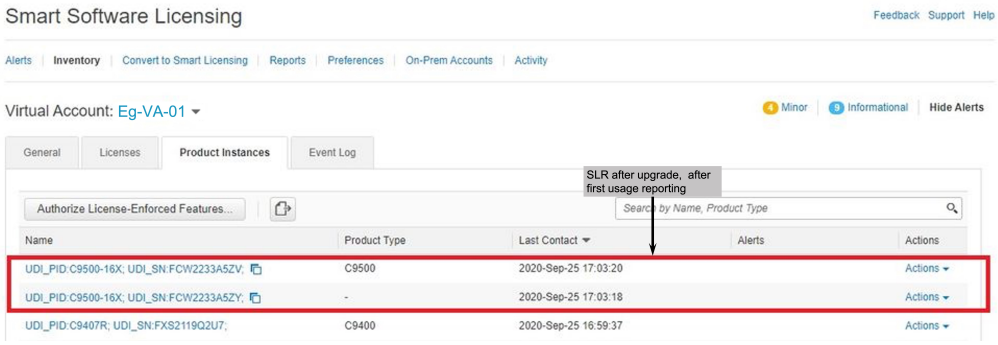


図 *10*：*SLR* からポリシーを使用したスマートライセンシングへ：移行後、レポート後のアクティブおよびスタンバイ製品インスタンス



移行後のレポート

SLR ライセンスは、ライセンスの使用状況が変化した場合にのみレポートを必要とします（たとえば、アドオンライセンスを指定された期間使用する場合）。ポリシー（**show license status**）によって変化が示されるか、変化に関する syslog メッセージが発信されます。

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アップロード）。

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。シンタックスの詳細については、対応するリリースのコマンドリファレンスで *license smart (privileged EXEC)* コマンドを参照してください。この例では、ファイルはまずブートフラッシュに保存され、次に TFTP の場所にコピーされます。

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

2. 使用状況データを CSSM にアップロード：CSSM への使用状況データのアップロードと ACK のダウンロード （121 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 （122 ページ）

例：評価ライセンスまたは期限切れライセンスからポリシーを使用したスマートライセンシングへ

以下は、評価ライセンス（スマートライセンシング）を、ポリシーを使用したスマートライセンシングに移行した Cisco Catalyst 9500 スイッチの例です。

評価ライセンスの概念は、ポリシーを使用したスマートライセンスには適用されません。ソフトウェアバージョンを、ポリシーを使用したスマートライセンシングをサポートするバージョンにアップグレードすると、すべてのライセンスが IN USE として表示され、シスコのデフォルトポリシーが製品インスタンスに適用されます。以前のライセンスモデルが有効であったときに Cisco Catalyst アクセス、コア、およびアグリゲーションスイッチで使用可能なエクスポート制御されたライセンスまたは適用されたライセンスはなかったため、どの機能も失われていません。

- 表 10 : 評価ライセンスまたは期限切れライセンスからポリシーを使用したスマートライセンシングへ：show コマンド
- 移行後の CSSM Web UI （69 ページ）
- 移行後のレポート （69 ページ）

次の表に、ポリシーを使用したスマートライセンシングへのアップグレード後に、**show** コマンドの出力でチェックすべき主な変更点または新しいフィールドを示します。

表 *10* : 評価ライセンスまたは期限切れライセンスからポリシーを使用したスマートライセンシングへ：*show* コマンド

アップグレード前	アップグレード後
show license summary（スマートライセンシング、評価モード） ライセンスは UNREGISTERED で、`EVAL MODE` になっています。	**show license summary**（ポリシーを使用したスマートライセンシング） すべてのライセンスが移行され、`IN USE`になっています。評価モードライセンスがありません。

アップグレード前	アップグレード後
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, 21 hours, 37 minutes, 30 seconds License Usage: License Entitlement tag Count Status --- (C9500 Network Advantage) 2 **EVAL MODE** (C9500-16X DNA Advantage) 2 **EVAL MODE**	Device# show license summary License Usage: License Entitlement tag Count Status --- network-advantage (C9500 Network Advantage) 2 **IN USE** dna-advantage (C9500-16X DNA Advantage) 2 **IN USE**

show license usage（スマートライセンシング、評価モード）	**show license usage**（ポリシーを使用したスマートライセンシング） [Enforcement Type] フィールドに NOT ENFORCED と表示されます。これは、アップグレード前に使用されていたすべてのライセンスが適用されていないためです。
Device# **show license usage** License Authorization: Status: EVAL MODE Evaluation Period Remaining: 89 days, 21 hours, 37 minutes, 21 seconds (C9500 Network Advantage): Description: Count: 2 Version: 1.0 Status: EVAL MODE Export status: NOT RESTRICTED (C9500-16X DNA Advantage): Description: Count: 2 Version: 1.0 Status: EVAL MODE Export status: NOT RESTRICTED	Device# **show license usage** License Authorization: Status: Not Applicable network-advantage (C9500 Network Advantage): Description: network-advantage Count: 2 Version: 1.0 Status: IN USE Export status: NOT RESTRICTED Feature Name: network-advantage Feature Description: network-advantage **Enforcement type: NOT ENFORCED** **License type: Perpetual** dna-advantage (C9500-16X DNA Advantage): Description: C9500-16X DNA Advantage Count: 2 Version: 1.0 Status: IN USE Export status: NOT RESTRICTED Feature Name: dna-advantage Feature Description: C9500-16X DNA Advantage **Enforcement type: NOT ENFORCED** **License type: Subscription**

show license status（スマートライセンス、評価モード）	**show license status**（ポリシーを使用したスマートライセンシング） `Transport:` フィールドにオフになっていることが表示されます。 `Policy` フィールドには、シスコのデフォルトポリシーが適用されていることが示されます。 `Trust Code Installed:` フィールドには、信頼コードがインストールされていないことが表示されます。 `Usage Reporting:` ヘッダー：`Next report push:` フィールドには、次の RUM レポートを CSSM に送信するタイミングに関する情報が表示されます。

```
Switch# 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, 21 hours, 37
minutes, 15 seconds
Export Authorization Key:
Features Authorized:
<none>
Miscellaneus:
Custom Id: <empty>
```

```
Switch# 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: 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 26 10:27:59 2021 PST
  Reporting push interval: 20  days
  Next ACK push check: <none>
  Next report push: Oct 28 10:29:59 2020 PST
  Last report push: <none>
  Last report file write: <none>
Trust Code Installed: <none>
```

移行後の CSSM Web UI

CSSM Web UI に変更はありません。

移行後のレポート

サポートされているトポロジのいずれかを実装し、レポート要件に適合するようにします。サポートされるトポロジ（11 ページ）およびポリシーを使用したスマートライセンシングの設定方法：トポロジ別のワークフロー（30 ページ）を参照してください。使用可能なレポートメソッドは、実装するトポロジによって異なります。

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 （5 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移行するために従う必要があるプロセスや手順、および該当する場合はSLACのインストールのような他のタスクの概要として使用してください。

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. 製品インスタンスをアップグレードします。

   サポートされている製品インスタンスに Smart Licensing Using Policy が導入された時期については、サポート対象製品 （3 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、スイッチ ソフトウェアのアップグレード （48 ページ）を参照してください。

3. 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。

4. 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。

5. 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
```

6. 使用状況の同期の実行

   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）　（97 ページ）を参照してください。

結果：

移行および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。

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） （97 ページ））。

ポリシーを使用したスマートライセンシングのタスクライブラリ

このセクションでは、ポリシーを使用したスマートライセンシングに適用されるタスクのグループ化について説明します。製品インスタンス、CSLU インターフェイス、および CSSM Web UI で実行されるタスクが含まれます。

特定のトポロジを実装するには、対応するワークフローを参照して、適用されるタスクの順序を確認します。ポリシーを使用したスマートライセンシングの設定方法：トポロジ別のワークフロー （30 ページ） を参照してください

追加の設定タスクを実行する場合（たとえば別のライセンスの設定、アドオンライセンスの使用、またはより短いレポート間隔の設定）は、対応するタスクを参照してください。続行する前に、入手可能な場合には「サポートされるトポロジ」を確認してください。

シスコへのログイン（CSLU インターフェイス）

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

手順

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

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

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

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

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

手順

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

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

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

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

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

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

（注） SA/VA 名では大文字と小文字が区別されます。

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

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

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

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

手順

ステップ 1 [Preferences] タブをクリックします。

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 Mgmt-vrf`	VRF をレイヤ 3 インターフェイスに対応付けます。このコマンドは、インターフェイスでマルチプロトコル VRF をアクティブにします。
ステップ 5	**ip address** *ip-address mask* 例： `Device(config-if)# ip address 192.168.0.1 255.255.0.0`	VRF の IP アドレスを定義します。
ステップ 6	**negotiation auto** 例： `Device(config-if)# negotiation auto`	インターフェイスの速度およびデュプレックスパラメータの自動ネゴシエーション動作を有効にします。
ステップ 7	**end** 例：	インターフェイス コンフィギュレーション モードを終了し、グローバル コ

	コマンドまたはアクション	目的
	`Device(config-if)# end`	ンフィギュレーションモードを開始します。
ステップ 8	**ip http client source-interface** *interface-type-number* 例： `Device(config)# ip http client source-interface gigabitethernet0/0`	HTTP クライアントのソース インターフェイスを設定します。
ステップ 9	**ip route** *ip-address ip-mask subnet mask* 例： `Device(config)# ip route vrf mgmt-vrf 192.168.0.1 255.255.0.0 192.168.255.1`	（必須）製品インスタンスにルートとゲートウェイを設定します。スタティックルートまたはダイナミックルートのいずれかを設定できます。
ステップ 10	{**ip** | **ipv6**} **name-server** *server-address 1 ...server-address 6*] 例： `Device(config)# Device(config)# ip name-server vrf mgmt-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	**ip domain lookup source-interface** *interface-type-number* 例： `Device(config)# ip domain lookup source-interface gigabitethernet0/0`	DNS ドメインルックアップ用のソースインターフェイスを設定します。
ステップ 12	**ip domain name** *domain-name* 例： `Device(config)# ip domain name example.com`	ドメインの DNS ディスカバリを設定します。ここの例では、ネームサーバはエントリ `cslu-local.example.com` を作成します。

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

CSLU インターフェイスを使用して、接続方法を CSLU 開始型に設定できます。この接続方法（モード）により、CSLU は製品インスタンス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、適切な [CSLU Initiated] 接続方法を選択します。

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

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 Instance] を選択し、ホスト名を入力して CSLU 開始型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）[Product Instances] > [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 Contact] 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できます。（<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への使用状況データのアップロードとACK のダウンロード （121 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。

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 CSLU のホーム画面から、[Data] > [Export to CSSM] 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 への使用状況データのアップロードと ACK のダウンロード （121 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。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） （78 ページ）

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 CSLU のホーム画面から、[Data] > [Import from CSSM] 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。

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。

	コマンドまたはアクション	目的
ステップ 3	**aaa new model** 例： `Device(config)# aaa new model`	（必須）認証、許可、アカウンティング（AAA）アクセスコントロールモデルをイネーブルにします。
ステップ 4	**aaa authentication login default local** 例： `Device(config)# aaa authentication login default local`	（必須）認証時にローカルのユーザ名データベースを使用するように、AAA 認証を設定します。
ステップ 5	**aaa authorization exec default local** 例： `Device(config)# aaa authorization exec default local`	ネットワークへのユーザアクセスを制限するパラメータを設定します。ユーザは EXEC シェルの実行が許可されます。
ステップ 6	ip routing 例： `Device(config)# ip routing`	IP ルーティングを有効にします。
ステップ 7	{**ip** | **ipv6**} **name-server** *server-address 1 ...server-address 6*] 例： `Device(config)# ip name-server vrf Mgmt-vrf 192.168.1.100 192.168.1.200 192.168.1.300`	（任意）名前とアドレスの解決に使用する 1 つまたは複数のネームサーバのアドレスを指定します。 最大 6 つのネーム サーバを指定できます。各サーバアドレスはスペースで区切ります。最初に指定されたサーバが、プライマリ サーバです。デバイスは、プライマリサーバへDNS クエリを最初に送信します。そのクエリが失敗した場合は、バックアップ サーバにクエリが送信されます。
ステップ 8	**ip domain lookup source-interface** *interface-type-number* 例： `Device(config)# ip domain lookup source-interface gigabitethernet0/0`	デバイス上で、DNS に基づくホスト名からアドレスへの変換を有効にします。この機能は、デフォルトでイネーブルにされています。 ユーザのネットワークデバイスが、名前の割り当てを制御できないネットワーク内のデバイスと接続する必要がある場合、グローバルなインターネットのネーミング方式（DNS）を使用して、ユーザのデバイスを一意に識別するデバイス名を動的に割り当てることができます。

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

	コマンドまたはアクション	目的
		（注） このユーザ名とパスワードを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）（76 ページ）→ステップ 4.f）。その後、CSLU は製品インスタンスから RUM レポートを収集できます。
ステップ 12	**interface** *interface-type-number* 例： `Device (config)# interface gigabitethernet0/0`	インターフェイス コンフィギュレーション モードを開始し、VRF に関連付けられたイーサネット インターフェイス、サブインターフェイス、または VLAN を指定します。
ステップ 13	**vrf forwarding** *vrf-name* 例： `Device(config-if)# vrf forwarding Mgmt-vrf`	VRF をレイヤ 3 インターフェイスに対応付けます。このコマンドは、インターフェイスでマルチプロトコル VRF をアクティブにします。
ステップ 14	**ip address** *ip-address mask* 例： `Device(config-if)# ip address 192.168.0.1 255.255.0.0`	VRF の IP アドレスを定義します。
ステップ 15	**negotiation auto** 例： `Device(config-if)# negotiation auto`	インターフェイスの速度およびデュプレックスパラメータの自動ネゴシエーション動作を有効にします。
ステップ 16	**no shutdown** 例： `Device(config-if)# no shutdown`	無効にされたインターフェイスを再起動します。
ステップ 17	**end** 例： `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。

	コマンドまたはアクション	目的

ステップ 19	**ip http authentication local**
	例：
	`ip http authentication local`
	`Device(config)#`
		（必須）HTTP サーバユーザに対して特定の認証方法を指定します。
		local キーワードは、認証および許可に、ローカルシステム設定で（username グローバル コンフィギュレーション コマンドによって）指定したログイン ユーザ名、パスワード、権限レベル アクセスの組み合わせを使用することを示します。

ステップ 20	**ip http secure-server** 例： `Device(config)# ip http server`	（必須）セキュア HTTP（HTTPS）サーバを有効にします。HTTPS サーバは、セキュア ソケット レイヤ（SSL）バージョン 3.0 プロトコルを使用します。
ステップ 21	**ip http max-connections** 例： `Device(config)# ip http max-connections 16`	（必須）HTTP サーバへの同時最大接続数を設定します。1 ～ 16 の範囲の整数を入力します。デフォルトは 5 です。
ステップ 22	**ip tftp source-interface** *interface-type-number* 例： `Device(config)# ip tftp source-interface GigabitEthernet0/0`	TFTP 接続用の送信元アドレスとして、インターフェイスの IP アドレスを指定します。
ステップ 23	**ip route** *ip-address ip-mask subnet mask* 例： `Device(config)# ip route vrf mgmt-vrf 192.168.0.1 255.255.0.0 192.168.255.1`	製品インスタンスにルートとゲートウェイを設定します。スタティック ルートまたはダイナミック ルートのいずれかを設定できます。
ステップ 24	**logging host** 例： `Device(config)# logging host 172.25.33.20 vrf Mgmt-vrf`	リモート ホストへのシステム メッセージおよびデバッグ出力を記録します。
ステップ 25	**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：	（必須）HTTP 接続を確認します。出力で、`SL_HTTP` がアクティブであるこ

	コマンドまたはアクション	目的
	`Device# show ip http server session-module`	とを確認します。また、次のチェックも実行できます。 • CSLU がインストールされているデバイスから、製品インスタンスに ping できることを確認します。ping が成功すると、製品インスタンスが到達可能であることが確認されます • CSLU がインストールされているデバイスの Web ブラウザで、`https://<product-instance-ip>/` を確認します。これにより、CSLU から製品インスタンスへの REST API が期待どおりに動作することが保証されます。

1つ以上の製品インスタンスのSLACの要求（CSLUインターフェイス）

このタスクでは、CSLU で 1 つ以上の製品インスタンスの SLAC を手動で要求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：

- CSLU を介した CSSM への接続（製品インスタンス開始および CSLU 開始）
- CSLU は CSSM から切断（製品インスタンス開始および CSLU 開始）

手順

ステップ 1 [Inventory] タブに移動します。[Product Instances] テーブルから、承認コード要求の対象となる 1 つ以上の製品インスタンスを選択します。

ステップ 2 [Actions for Selected] メニューから、[Authorization Code Request] オプションを選択します。

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

ステップ 3 [承認（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別のポップアップウィンドウが開きます。

ステップ 4 ファイルをCSSMにアップロードし、承認コードを生成して、コードを含むファイルをダウンロードします。CSSM からの SLAC の生成とファイルへのダウンロード （110 ページ）を参照してください。

ステップ 5 CSLU インターフェイスに戻ります。

ステップ 6 [Data] > [Import from CSSM] を選択して、承認コードを適用します。「CSSM からのインポート（CSLU インターフェイス） （78 ページ）」を参照してください

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

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

CSSM への接続の設定

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

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。プロンプトが表示されたらパスワードを入力します。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	{**ip** | **ipv6**} **name-server** *server-address 1 ...server-address 6*] 例： `Device(config)# ip name-server 209.165.201.1 209.165.200.225 209.165.201.14 209.165.200.230`	名前とアドレスの解決に使用する 1 つまたは複数のネーム サーバのアドレスを指定します。 最大 6 つのネーム サーバを指定できます。各サーバアドレスはスペースで区切ります。最初に指定されたサーバが、プライマリ サーバです。デバイスは、プライマリサーバへDNS クエリを最初に送信します。そのクエリが失敗した場合は、バックアップ サーバにクエリが送信されます。

	コマンドまたはアクション	目的
ステップ 4	**ip name-server vrf Mgmt-vrf** *server-address 1...server-address 6* 例： `Device(config)# ip name-server vrf Mgmt-vrf 209.165.201.1 209.165.200.225 209.165.201.14 209.165.200.230`	（任意）VRF インターフェイスで DNS を設定します。最大 6 つのネーム サーバを指定できます。各サーバアドレスはスペースで区切ります。 （注） このコマンドは、**ip name-server** コマンドの代わりです。
ステップ 5	**ip domain lookup source-interface** *interface-type interface-number* 例： `Device(config)# ip domain lookup source-interface Vlan100`	DNS ドメインルックアップ用のソース インターフェイスを設定します。
ステップ 6	**ip domain name** *domain-name* 例： `Device(config)# ip domain name example.com`	ドメイン名を設定します。
ステップ 7	**ip host tools.cisco.com** *ip-address* 例： `Device(config)# ip host tools.cisco.com 209.165.201.30`	自動 DNS マッピングが使用できない場合は、DNS ホスト名キャッシュ内のホスト名/アドレス静的マッピングを設定します。

ステップ 8	**interface** *interface-type-number*
	例：
	`Device(config)# interface Vlan100`
	`Device(config-if)# ip address 192.0.2.10 255.255.255.0`
	`Device(config-if)# exit`
		レイヤ 3 インターフェイスを設定します。インターフェイスのタイプと番号、または VLAN を入力します。

ステップ 9	**ntp server** *ip-address* [**version** *number*] [**key** *key-id*] [**prefer**] 例： `Device(config)# ntp server 198.51.100.100 version 2 prefer`	（必須）NTP サービスをアクティブにし（まだアクティブになっていない場合）、システムがシステム ソフトウェア クロックを指定された NTP サーバと同期できるようにします。これにより、デバイスの時刻が CSSM と同期されます。 このコマンドを複数回使用する必要があるために優先サーバを設定する場合は、**prefer** キーワードを使用します。このキーワードを使用すると、サーバ間の切り換え回数が減少します。

	コマンドまたはアクション	目的

ステップ 10	**switchport access vlan** *vlan_id*
	例：
	`Device(config)# interface GigabitEthernet1/0/1`
	`Device(config-if)# switchport access vlan 100`
	`Device(config-if)# switchport mode access`
	`Device(config-if)# exit`
	`OR`
	`Device(config)#`
		このアクセスポートがトラフィックを伝送する VLAN を有効にし、非トランキングで非タグ付きのシングル VLAN イーサネットインターフェイスとしてインターフェイスを設定します。
		（注） このステップは、スイッチポート アクセス モードが必要な場合にのみ設定します。**switchport access vlan** コマンドは、たとえば Catalyst スイッチング製品インスタンスに適用できます。ルーティング製品インスタンスの場合は、代わりに **ip address** *ip-address mask* コマンドを設定できます。

ステップ 11	**ip route** *ip-address ip-mask subnet mask* 例： `Device(config)# ip route 192.0.2.0 255.255.255.255 192.0.2.1`	デバイスにルートを設定します。スタティックルートまたはダイナミックルートのいずれかを設定できます。
ステップ 12	**ip http client source-interface** *interface-type-number* 例： `Device(config)# ip http client source-interface Vlan100`	（必須）HTTP クライアントのソースインターフェイスを設定します。インターフェイスのタイプと番号、または VLAN を入力します。
ステップ 13	**exit** 例： `Device(config)# exit`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 14	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	コンフィギュレーションファイルに設定を保存します。

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。プロキシアドレスとポート番号を個別に設定します。
		• **address** *address_hostname*：プロキシアドレスを指定します。プロキシサーバの IP アドレスまたはホスト名を入力します。
		• **port** *port_num*：プロキシポートを指定します。プロキシ ポートポート番号を入力します。
		Cisco IOS XE Bengaluru 17.6.1 以降、プロキシサーバーの受け入れ基準が変更されたことに注意してください。プロキシ

	コマンドまたはアクション	目的
		サーバーの応答のステータスコードのみがシステムによって検証され、理由フレーズは検証されません。RFC形式は、`status-line = HTTP-version SP status-code SP reason-phrase CRLF` です。ステータス行の詳細については、RFC 7230 のセクション 3.1.2 を参照してください。
ステップ 6	**exit** 例： `Device(config)# exit`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 7	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	コンフィギュレーション ファイルに設定を保存します。

ダイレクトクラウドアクセス用の Call Home サービスの設定

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

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

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。プロンプトが表示されたらパスワードを入力します。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**license smart transport callhome** 例：	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
	`Device(config)# license smart transport callhome`	
ステップ 4	**license smart url** *url* 例： `Device(config)# license smart url https://tools.cisco.com/its/service/oddce/services/DDCEService`	**callhome** 転送モードの場合は、例に示すように CSSM URL を設定します。
ステップ 5	**service call-home** 例： `Device(config)# service call-home`	Call Home 機能をイネーブルにします。
ステップ 6	**call-home** 例： `Device(config)# call-home`	Call Home コンフィギュレーションモードを開始します。
ステップ 7	**contact-email-address** *email-address* 例： `Device(config-call-home)# contact-email-addr username@example.com`	お客様の電子メールアドレスを割り当て、Smart Call Home サービスのフルレポート機能を有効にし、フルインベントリメッセージを Call Home TAC プロファイルから Smart Call Home サーバに送信してフル登録プロセスを開始します。電子メールアドレスフォーマットには、スペースなしで最大 200 文字まで入力できます。

ステップ 8	**profile** *name*
	例：
	`Device(config-call-home)# profile CiscoTAC-1`
	`Device(config-call-home-profile)#`
		指定された宛先プロファイルに対する Call Home 宛先プロファイル設定サブモードに入ります。
		デフォルトは次のとおりです。
		• CiscoTAC-1 プロファイルは非アクティブです。このプロファイルを Call Home サービスで使用するには、プロファイルを有効にする必要があります。
		• CiscoTAC-1 プロファイルは、プロファイルに登録されているすべてのイベントタイプが記載された完全なレポートを送信します。または、`Device(cfg-call-home-profile)# anonymous-reporting-only` anonymous-reporting-only を追加で設定します。これが設定されてい

	コマンドまたはアクション	目的
		る場合は、クラッシュ、インベントリ、およびテストメッセージのみが送信されます。 プロファイルのステータスを確認するには、**show call-home profile all** コマンドを使用します。
ステップ 9	**active** 例： `Device(config-call-home-profile)# active`	宛先プロファイルをイネーブルにします。

ステップ 10	**destination transport-method http** {**email** | **http**}
	例：
	`Device(config-call-home-profile)# destination transport-method http`
	AND
	`Device(config-call-home-profile)# no destination transport-method email`
		メッセージの転送形式をイネーブルにします。この例では、HTTP経由でCall Homeサービスが有効になり、電子メールによる転送が無効になります。
		
		このコマンドのno形式を使用すると、メソッドが無効になります。

ステップ 11	**destination address** { **email** *email_address* | **http** *url*}
	例：
	`Device(config-call-home-profile)# destination address http https://tools.cisco.com/its/service/oddce/services/DDCEService`
	AND
	`Device(config-call-home-profile)# no destination address http https://tools.cisco.com/its/service/oddce/services/DDCEService`
		Call Home メッセージを送信する宛先 E メール アドレスまたは URL を設定します。宛先URLを入力する場合は、サーバがセキュアサーバであるかどうかに応じて http://（デフォルト）または https:// を指定します。
		
		ここに示す例では、http:// の形式で宛先URLが設定されています。コマンドの **no** 形式ではhttps://に設定されます。

ステップ 12	**exit** 例： `Device(config-call-home-profile)# exit`	Call Home 宛先プロファイル コンフィギュレーションモードを終了して、Call Home コンフィギュレーション モードに戻ります。
ステップ 13	**exit** 例： `Device(config-call-home)# end`	Call Homeコンフィギュレーションモードを終了して、特権 EXEC モードに戻ります。
ステップ 14	**copy running-config startup-config** 例：	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# copy running-config startup-config`	
ステップ 15	**show call-home profile** {*name* |**all**}	指定されたプロファイル、または設定済みのすべてのプロファイルに関する宛先プロファイル設定を表示します。

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

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

（注） 認証された HTTPS プロキシ設定はサポートされていません。

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

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

手順

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

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

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

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

始める前に

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

手順

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

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

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

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

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

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

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

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

デバイスの検証（SSM オンプレミス UI）

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

デフォルトでは、デバイスは検証されません。この機能を有効にするには、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）（92 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） 手順 13、14、および 15 では、必ず次のように設定してください。これらのコマンドは、正しいトラストポイントが使用され、ネットワーク到達可能性に必要な証明書が受け入れられるように設定する必要があります。

始める前に

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

手順

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

	コマンドまたはアクション	目的
ステップ 5	**ip address** *ip-address mask* 例： `Device(config-if)# ip address 192.168.0.1 255.255.0.0`	VRF の IP アドレスを定義します。
ステップ 6	**negotiation auto** 例： `Device(config-if)# negotiation auto`	インターフェイスの速度およびデュプレックスパラメータの自動ネゴシエーション動作を有効にします。
ステップ 7	**end** 例： `Device(config-if)# end`	インターフェイス コンフィギュレーションモードを終了し、グローバル コンフィギュレーションモードを開始します。
ステップ 8	**ip http client source-interface** *interface-type-number* 例： `Device(config)# ip http client source-interface gigabitethernet0/0`	HTTP クライアントのソース インターフェイスを設定します。
ステップ 9	**ip route** *ip-address ip-mask subnet mask* 例： `Device(config)# ip route vrf mgmt-vrf 192.168.0.1 255.255.0.0 192.168.255.1`	（必須）製品インスタンスにルートとゲートウェイを設定します。スタティックルートまたはダイナミックルートのいずれかを設定できます。
ステップ 10	{**ip** | **ipv6**} **name-server** *server-address 1 ...server-address 6*] 例： `Device(config)# Device(config)# ip name-server vrf mgmt-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	**ip domain lookup source-interface** *interface-type-number* 例： `Device(config)# ip domain lookup source-interface gigabitethernet0/0`	DNS ドメインルックアップ用のソースインターフェイスを設定します。
ステップ 12	**ip domain name** *domain-name* 例： `Device(config)# ip domain name example.com`	ドメインの DNS ディスカバリを設定します。この例では、ネームサーバがエントリ `cslu-local.example.com` を作成します。

	コマンドまたはアクション	目的

ステップ 13	**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 14	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 15	**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 16	**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 17	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	コンフィギュレーションファイルに設定を保存します。

トランスポート URL の取得（SSM オンプレミス UI）

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

始める前に

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

手順

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

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

ステップ 3 [General] タブに移動します。

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

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

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

ステップ 5 URL 全体をコピーし、アクセス可能な場所に保存します。

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

ステップ 6 トランスポートタイプと URL を設定します。転送タイプ、URL、およびレポート間隔の設定（124 ページ）を参照してください。

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 への使用状況データのアップロードと ACK のダウンロード（121 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のみが必要です。

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

   これは、ネットワーク到達可能性を確立するために必要なコマンドの一部として設定したものと同じユーザ ID とパスワードです（SSM オンプレミス開始型通信のネットワーク到達可能性の確保 （99 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 （99 ページ））。

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

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

5. 次に、入力した .csv テンプレートをアップロードします。

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

SSM オンプレミス開始型通信のネットワーク到達可能性の確保

このタスクでは、SSMオンプレミス開始型通信のネットワーク到達可能性を確保するために必要になる可能性のある設定を実行します。「（必須）」と付いている手順は、すべての製品イ

ンスタンスで必須です。他のすべての手順は、製品インスタンスの種類とネットワーク要件に応じて、必須の場合も任意の場合もあります。該当するコマンドを設定します。

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

始める前に

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

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。プロンプトが表示されたらパスワードを入力します。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**aaa new model** 例： `Device(config)# aaa new model`	（必須）認証、許可、アカウンティング（AAA）アクセスコントロールモデルをイネーブルにします。
ステップ 4	**aaa authentication login default local** 例： `Device(config)# aaa authentication login default local`	（必須）認証時にローカルのユーザ名データベースを使用するように、AAA 認証を設定します。
ステップ 5	**aaa authorization exec default local** 例： `Device(config)# aaa authorization exec default local`	ネットワークへのユーザアクセスを制限するパラメータを設定します。ユーザは EXEC シェルの実行が許可されます。
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
	`Device(config)# ip name-server vrf Mgmt-vrf 192.168.1.100 192.168.1.200 192.168.1.300`	最大 6 つのネーム サーバを指定できます。各サーバアドレスはスペースで区切ります。最初に指定されたサーバが、プライマリ サーバです。デバイスは、プライマリサーバへDNS クエリを最初に送信します。そのクエリが失敗した場合は、バックアップ サーバにクエリが送信されます。
ステップ 8	**ip domain lookup source-interface** *interface-type-number* 例： `Device(config)# ip domain lookup source-interface gigabitethernet0/0`	デバイス上で、DNS に基づくホスト名からアドレスへの変換を有効にします。この機能は、デフォルトでイネーブルにされています。 ユーザのネットワークデバイスが、名前の割り当てを制御できないネットワーク内のデバイスと接続する必要がある場合、グローバルなインターネットのネーミング方式（DNS）を使用して、ユーザのデバイスを一意に識別するデバイス名を動的に割り当てることができます。
ステップ 9	**ip domain name** *name* 例： `Device(config)# ip domain name vrf Mgmt-vrf cisco.com`	非完全修飾ホスト名（ドット付き 10 進表記ドメイン名のない名前）を完成させるためにソフトウェアが使用する、デフォルトのドメイン名を定義します。
ステップ 10	**no username** *name* 例： `Device(config)# no username admin`	（必須）指定されたユーザ名が存在する場合はクリアします。*name* には、次のステップで作成するユーザ名と同じものを入力します。これにより、次のステップで作成するユーザ名が重複していないことが保証されます。 SSM オンプレミス開始型の RUM レポートを取得に REST API を使用する場合は、SSM オンプレミスにログインする必要があります。ユーザ名が重複していると、システムにそのユーザ名がある場合はこの機能が正しく動作しない場合があります。

	コマンドまたはアクション	目的
ステップ 11	**username** *name* **privilege** *level* **password** *password* 例： `Device(config)# username admin privilege 15 password 0 lab`	（必須）ユーザ名をベースとした認証システムを構築します。 **privilege** キーワードにより、ユーザの権限レベルを設定します。ユーザの権限レベルを指定する 0 ～ 15 の数字です。 password を使用すると、name 引数にアクセスできます。パスワードは 1 ～ 25 文字で、埋め込みスペースを使用でき、**username** コマンドの最後のオプションとして指定します。 これにより、SSM オンプレミスが製品インスタンスのネイティブ REST を使用できるようになります。 （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） （98 ページ））。これにより、SSM オンプレミスは製品インスタンスから RUM レポートを収集できるようになります。
ステップ 12	**interface** *interface-type-number* 例： `Device (config)# interface gigabitethernet0/0`	インターフェイス コンフィギュレーション モードを開始し、VRF に関連付けられたイーサネットインターフェイス、サブインターフェイス、または VLAN を指定します。
ステップ 13	**vrf forwarding** *vrf-name* 例： `Device(config-if)# vrf forwarding Mgmt-vrf`	VRF をレイヤ 3 インターフェイスに対応付けます。このコマンドは、インターフェイスでマルチプロトコル VRF をアクティブにします。
ステップ 14	**ip address** *ip-address mask* 例： `Device(config-if)# ip address 192.168.0.1 255.255.0.0`	VRF の IP アドレスを定義します。

	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	**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 26	enrollment terminal 例： `Device(ca-trustpoint)# enrollment terminal`	（必須）証明書登録方式を指定します。
ステップ 27	**revocation-check none** 例： `Device(ca-trustpoint)# revocation-check none`	（必須）ピアの証明書が失効していないことを確認するために使用する方法を指定します。SSM オンプレミス展開トポロジの場合は、**none** キーワードを入力します。つまり、失効チェックは実行されず、証明書は常に受け入れられます。

ステップ 28	**end**
	例：
	`Device(ca-trustpoint)# exit`
	`Device(config)# end`
		CA トランスポイント コンフィギュレーション モードを終了し、次にグローバル コンフィギュレーション モードを終了してから、特権 EXEC モードに戻ります。

ステップ 29	**show ip http server session-module** 例： `Device# show ip http server session-module`	（必須）HTTP 接続を確認します。出力で、`SL_HTTP` がアクティブであることを確認します。また、次のチェックも実行できます。

	コマンドまたはアクション	目的
		• SSMオンプレミスがインストールされているデバイスから、製品インスタンスにpingできることを確認します。pingが成功すると、製品インスタンスが到達可能であることが確認されます • SSMオンプレミスがインストールされているデバイスのWebブラウザで、`https://<product-instance-ip>/` を確認します。これにより、SSMオンプレミスから製品インスタンスへのREST APIが期待どおりに動作することが保証されます。
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。

承認コード要求の送信（SSM オンプレミス UI）

SSMオンプレミス展開のトポロジを使用すると、製品インスタンスが要求する前に、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、必要な輸出規制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 からの SLAC の生成とファイルへのダウンロード（110 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 再度、[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。

上記の手順 4 の最後にダウンロードした .csv 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 製品インスタンスまたは SSM オンプレミスが通信を開始するかどうかに応じて、最後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、SSM オンプレミスから SLAC を要求してインストールするように製品インスタンスを設定します。次を参照してください。SLAC の手動要求と自動インストール（106 ページ）
- SSM オンプレミス開始型通信の場合、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製品インスタンスに適用されます。

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 を介した CSSM への接続（製品インスタンス開始型通信および CSLU 開始型通信）
- CSSM に直接接続

- 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）

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。
- トランスポートタイプと URL がそれに応じて設定されます。特権 EXEC モードで **show license all** コマンドを使用します。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、トークンを生成することで信頼コードをインストールしています。**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 オンプレミス展開の場合、製品インスタンスは SLAC の SSM オンプレミスを要求するため、このタスクを開始する前に、必要な数の SLAC ファイルが SSM オンプレミスサーバーで使用可能な状態に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	**license smart authorization request** {**add** | **replace**} *feature_name* {**all** | **local**} 例： `Device# license smart authorization request add hseck9 local`	CSSM または CSLU または SSM オンプレミスから SLAC を要求します。 • 既存の SLAC に追加するのか置換するのかを指定します。 • **add**：要求されたライセンスキーを既存の SLAC に追加します。新しい SLAC には、既存の SLAC のすべてのキーと要求されたキーが含まれます。 • **replace**：既存の SLAC を置き換えます。新しい SLAC には、要求されたキーのみが含まれます。既存の SLAC のすべての HSECK9 キー 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キーが使用中かどうかを確認します。使用中の場合

	コマンドまたはアクション	目的
		は、対応する暗号化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*：SLAC の追加または置換を要求する輸出規制ライセンスの名前を入力します。「hseck9」と入力して、HSECK9 キーの SLAC を要求してインストールします。 • 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**：高可用性設定およびスタック設定のすべてのデバイスの承認コードを取得します。 （注） SLAC がすでにインストールされている既存のスタックに（SLAC がインストールされていない）デバイスを追加した場合は、**replace** および **all** オプションを使用します。これにより、スタック内のすべてのデバイスの SLAC が要求されます。特定のメンバーの SLAC を要求することはできません。選択肢はアクティブまたはスタック全体のみです。 • **local**：高可用性設定およびスタック設定のアクティブなデバイスの承認コードを取得します。これがデフォルトのオプションです。

	コマンドまたはアクション	目的
ステップ 3	（任意）**license smart sync** {**all** | **local**} 例： `Device# license smart sync local`	CSSM、CSLU または SSM オンプレミスと製品インスタンス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。 この手順はオプションであり、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、製品インスタンスが通信を開始するシナリオにのみ適用されます。対応するトポロジは、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）、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。 このコマンドは、手動で同期をトリガーし、SLAC インストールプロセスを完了します。それ以外の場合、製品インスタンスが次回 CSLU または SSM オンプレミスに接続するときに、SLAC が製品インスタンスに適用されます。
ステップ 4	該当するトポロジの残りの手順を実行します。	• CSLU を介して CSSM に接続（CSLU 開始型通信）については、CSLU 開始型通信の場合のタスク（32 ページ）を参照してください。 • 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）については、トポロジのワークフロー：CSLU は CSSM から切断 （37 ページ）を参照してください。 • SSM オンプレミス展開（製品インスタンス開始型通信）については、トポロジのワークフロー：SSM オンプレミス展開 （42 ページ）を参照してください。

ステップ 5	**show license authorization**
	例：
	`Device# show license authorization`
	`Overall status:`
	`  Active:`
	`PID:C9300X-24HX,SN:FOC2519L8R7`
		製品インスタンスにインストールされている SLAC を表示します。

	コマンドまたはアクション	目的
	Status: **SMART AUTHORIZATION INSTALLED on Oct 29 17:45:28 2021 UTC** Last Confirmation code: 6746c5b5 Standby: PID:C9300X-48HXN,SN:FOC2524L39P Status: NOT INSTALLED Member: PID:C9300X-48HX,SN:FOC2516LC92 Status: NOT INSTALLED Authorizations: C9K HSEC (Cat9K HSEC): Description: HSEC Key for Export Compliance on Cat9K Series Switches Total available count: 1 Enforcement type: EXPORT RESTRICTED Term information: Active: PID:C9300X-24HX,SN:FOC2519L8R7 Authorization type: SMART AUTHORIZATION INSTALLED License type: PERPETUAL Term Count: 1 Purchased Licenses: No Purchase Information Available	

CSSM からの SLAC の生成とファイルへのダウンロード

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、該当するすべての製品インスタンスのPIDとシリアル番号を含む .csv ファイルをアクセス可能な場所に保存します。

始める前に

サポートされているトポロジ：

- CSLU を介した CSSM への接続（製品インスタンス開始および CSLU 開始）
- CSLU は CSSM から切断（製品インスタンス開始および CSLU 開始）
- CSSM への接続なし、CSLU なし
- 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 にログインします。[Smart Software Licensing] で、[Manage licenses] リンクをクリックします。

シスコから提供されたユーザ名とパスワードを使用してログインします。

ステップ 2 [Inventory] タブをクリックします。

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

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

ステップ 5 [Authorize License Enforced Features] タブをクリックします。

ステップ 6 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。HSECK9 がサポートされている Cisco Catalyst アクセス、コア、およびアグリゲーションスイッチでは、[C9K HSEC] を選択します。

  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 （122 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てください）。**

  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。

     この時点で、[Download a template] リンクが表示されます。必要なテンプレートまたはファイルがまだない場合は、ダウンロードできます。シリアル番号 PID のみが必須です。

  2. [Choose File] 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） 「C9K HSEC」ライセンスの場合、UDI ごとに 1 つの SLAC が必要です。

5. [Reserve Licenses] をクリックします。
6. トポロジに従ってダウンロードします。
   - 「CSLUを介したCSSMへの接続」、「CSLUはCSSMから切断」、「SSMオンプレミス展開」トポロジの場合は、[Download Authorization Codes] をクリックして、すべての承認コードを含む .csv ファイルをダウンロードします。[**閉じる（Close**）] をクリックします。

     これで、この .csv ファイルを CSLU または SSM オンプレミスにインポートできるようになりました。CSLUまたはSSMオンプレミスインターフェイスに戻り、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。
   - 「CSMへの接続なし、CSLUなし」トポロジ（外部との接続性がないネットワークで、コードを製品インスタンスにインポートする必要がある場合）では、各製品インスタンスの承認コードを別の .txt ファイルにダウンロードします。すべてのコードを含む .csv ファイルをダウンロードしないでください。

     CSSM Web UI で、[Inventory] > [Product Instances] タブに戻ります。各製品インスタンスをPIDまたはシリアル番号で検索します。UDIをクリックして、[Overview] タブを表示します。[Last Contact] フィールドに、[Download Reservation Authorization Code] というリンクが表示されます。リンクをクリックして、選択した製品インスタンスのみの承認コードを .txt 形式でダウンロードします。

     各 SLAC を製品インスタンスにインポートします。製品インスタンスへのファイルのインストール （122 ページ）を参照してください。

承認コードの返却

このタスクでは、許可コードを返し、CSSMのライセンスプールにライセンスまたはキーを返す方法を示します。この手順は、すべての承認コード（SLACおよびSLR）に使用できます。

始める前に

サポートされるトポロジ：すべて

SLACおよびSLR：返却するライセンスまたはキーが使用中でないことを確認します。使用中の場合は、まず機能を無効にする必要があります。

手順

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

ステップ 2	**show license summary**
	例：
	`Device# show license summary`
	`License Usage:`
	`License Entitlement Tag Count Status`
	`---`
	`network-advantage (C9300-24 Network Advan...) 1 IN USE`
	`dna-advantage (C9300-24 DNA Advantage) 1 IN USE`
	`network-advantage (C9300-48 Network Advan...) 2 IN USE`
	`dna-advantage (C9300-48 DNA Advantage) 2 IN USE`
	`C9K HSEC (Cat9K HSEC) 1 IN USE`
		（任意）ライセンスの使用状況の概要を表示します。この手順は、SLAC を返却する場合にのみ適用されます。
		暗号化機能を無効にした後でも、HSECK9 キー のステータスが `[IN USE]` と表示される場合は、次の手順を実行します。この例の場合を示します。
		HSECK9 キー のステータスが `[NOT IN USE]` と表示された場合は、ステップ 5 に進みます。

ステップ 3	**platform hsec-license-release**
	例：
	`Device# configure terminal`
	`Device(config)# platform hsec-license-release`
	`HSEC license is released`
	`Device(config)# exit`
		（任意）グローバル コンフィギュレーション モードを開始し、HSECK9 キーをリリースしたら、特権 EXEC モードに戻ります。この手順は、SLAC を返却する場合にのみ適用されます。
		HSECK9 キー を使用する暗号化機能が無効または未設定で、キーがまだ `[IN USE]` と表示されている場合、このコマンドにより強制的に HSECK9 キー が `[NOT IN USE]` としてマークされます。

ステップ 4	**show license summary**
	例：
	`Device# show license summary`
	`License Usage:`
	`License Entitlement Tag Count Status`
	`---`
	`network-advantage (C9300-24 Network Advan...) 1 IN USE`
	`dna-advantage (C9300-24 DNA Advantage) 1 IN USE`
	`network-advantage (C9300-48 Network Advan...) 2 IN USE`
		返却するライセンスまたはキーのステータスが `[NOT IN USE]` であることを確認します。使用中の場合は、まず機能を無効にする必要があります。

	コマンドまたはアクション	目的
	dna-advantage (C9300-48 DNA Advantage) 2 IN USE C9K HSEC (Cat9K HSEC) 0 NOT IN USE	

ステップ 5	**license smart authorization return** {**all** | **local**} { **offline** [*path*] | **online** }
	例：
	`Device# license smart authorization return all online`
	OR
	`Device# license smart authorization return all offline`
	`Enter this return code in Cisco Smart Software Manager portal:`
	`UDI: PID:C9300X-24HX,SN:FOC2519L8R7`
	`Return code:`
	`Cr9Jhx-Llx5Rj-ftwzgi-h9QZAU-1E5DT1-bakWeL-rABPt9-WrlDn7-Rp7`
	OR
	`Device# license smart authorization return all offline bootflash:return-code.txt`
		CSSMのライセンスプールに承認コードを返却します。このコマンドを入力すると、戻りコードが表示されます。
		製品インスタンスを指定します。
		• all：高可用性セットアップまたはスタック構成セットアップで接続されたすべての製品インスタンスに対してアクションを実行します。
		• local：アクティブな製品インスタンスに対してアクションを実行します。これがデフォルトのオプションです。
		CSSMに接続しているかどうかを指定します。
		• 製品インスタンスが CSSM に直接接続されている場合、またはCSLUまたは SSM オンプレミスを介してCSSMに接続されていて、製品インスタンスが通信を開始する場合は、**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。
		• 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開始型通信または SSM オンプレミス開始型通信のトポロジを実装した場合は、**offline** [*filepath_filename*] を入力します。**offline** キーワードのみを入力する場合は、CLIに表示される戻りコードをコピーし、CSSMに入力します。戻りコードをファイルに保存する場合は、ファイルからコードをコピーし、CSSM に同じコードを入力できます。ファイル形

	コマンドまたはアクション	目的
		式は、読み取り可能な任意の形式にすることができます（これはアップロードされません）。例：`Device# license smart authorization return local offline bootflash:return-code.txt` • SLACを返却する場合は、次のタスクを実行してCSSMに戻りコードを入力します。CSSMでのSLAC戻りコードの入力と製品インスタンスの削除（116ページ） • SLR承認コードを返却する場合は、次のタスクを実行してCSSMに戻りコードを入力します。CSSMでのSLR戻りコードの入力と製品インスタンスの削除（117ページ）この手順を完了してから、次の手順に進みます。

ステップ6	**no license smart reservation**
	例：
	`Device# configure terminal`
	`Device(config)# no license smart reservation`
	`Device(config)# exit`
		グローバルコンフィギュレーションモードを開始し、製品インスタンスでSLR設定を無効化して、特権EXECモードに戻ります。
		この手順は、返却する承認コードがSLR承認コードである場合にのみ必要です。返却するコードがHSECK9キーのSLACである場合は、この手順をスキップします。

	コマンドまたはアクション	目的
		（注） この手順で **no license smart reservation** コマンドを入力する前に、オンラインまたはオフラインで承認コードの返却プロセス（**license smart authorization return**）を完了する必要があります。そうしないと、返却がCSSMまたは**show**コマンドに反映されない場合があります。問題を修正するには、シスコのテクニカルサポート担当者に連絡する必要があります。

ステップ 7	**show license authorization**
	例：
	`Device# show license authorization`
	
	`License Authorizations`
	`=====================`
	`Overall status:`
	`  Active:`
	`PID:C9300X-24HX,SN:FOC2519L8R7`
	`  Status: NOT INSTALLED`
	`  Last return code:`
	`Cr9JHx-L1x5Rj-ftwzg1-h9QZAU-LE5DT1-`
	`babWeL-FABPt9-Wr1Dn7-Rp7`
	`  Standby:`
	`PID:C9300X-48HXN,SN:FOC2524L39P`
	`  Status: NOT INSTALLED`
	`  Member:`
	`PID:C9300X-48HX,SN:FOC2516LC92`
	`  Status: NOT INSTALLED`
	`<output truncated>`
		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。

CSSM での SLAC 戻りコードの入力と製品インスタンスの削除

このタスクを使用して、製品インスタンスがCSSMに接続されていない場合に、SLACの返却手順を実行できます。これにより、HSECK9キーがライセンスプールに戻されます。さらに、CSSMから製品インスタンスを削除することもできます。

始める前に

サポートされるトポロジ：すべて

この手順は、SLACを返却する場合にのみ実行してください。

承認コードの返却（112ページ）に示すように、戻りコードが生成されていることを確認します。（このタスクの手順 7 で入力します）。

手順

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

シスコから提供されたユーザ名とパスワードを使用してログインします。

ステップ 2 [Inventory] タブをクリックします。

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

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

使用可能な製品インスタンスのリストが表示されます。

ステップ 5 製品インスタンスリストから必要な製品インスタンスを見つけます。[Search] タブに PID またはシリアル番号を入力して検索できます。

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、作成した SLAC 戻りコードを入力します。

ステップ 8 [Remove Reservation] をクリックします。

HSECK9 キー 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） SLAC 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 9 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 10 [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 での SLR 戻りコードの入力と製品インスタンスの削除

このタスクを使用して、SLR 承認コードの返却手順を実行できます。これによりライセンスがライセンスプールに返され、製品インスタンスが削除されます。

始める前に

サポートされるトポロジ：すべて

この手順は、SLR 承認コードを返す場合にのみ実行してください。

承認コードの返却（112ページ）に示すように、戻りコードが生成されていることを確認します。（このタスクの手順 7 で入力します）。

手順

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

シスコから提供されたユーザ名とパスワードを使用してログインします。

ステップ 2 [Inventory] タブをクリックします。

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

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

使用可能な製品インスタンスのリストが表示されます。

ステップ 5 製品インスタンスリストから必要な製品インスタンスを見つけます。[Search] タブに PID またはシリアル番号を入力して検索できます。

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。

- 製品インスタンスが SLR 承認コードを含むライセンスを使用していない場合は、[Confirm Remove Product Instance] ウィンドウが表示されます。
- 製品インスタンスが SLR 承認コードを含むライセンスを使用している場合は、リターンコードを入力するためのフィールドのある [Remove Product Instance] 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、作成したリターンコードを入力します。

（注） この手順は、製品インスタンスが SLR 承認コードを含むライセンスを使用している場合にのみ適用されます。

ステップ 8 [Remove Product Instance] をクリックします。

ライセンスがライセンスプールに返され、製品インスタンスが削除されます。

CSSM からの信頼コード用新規トークンの生成

信頼コードを要求するトークンを生成するには、次の手順を実行します。

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

始める前に

サポートされるトポロジ：CSSM に直接接続

手順

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

シスコから提供されたユーザ名とパスワードを使用してログインします。

ステップ 2 [Inventory] タブをクリックします。

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

ステップ 4 [General] タブをクリックします。

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

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

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

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

ステップ 9 [Create Token] をクリックします。

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

信頼コードのインストール

信頼コードを手動でインストールするには、次の手順を実行します。

始める前に

サポートされるトポロジ：

- CSSM に直接接続

手順

	コマンドまたはアクション	目的
ステップ 1	CSSMからの信頼コード用新規トークンの生成 （118 ページ）	まだ CSSM から信頼コードファイルを生成してダウンロードしていない場合は、生成とダウンロードを実行します。

	コマンドまたはアクション	目的
ステップ 2	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。プロンプトが表示されたら、パスワードを入力します。
ステップ 3	**license smart trust idtoken** *id_token_value* {**local** | **all**} [**force**] 例： `Device# license smart trust idtoken NGMwMjk5mYtNZaxMS00NzMZmtgWm all force`	CSSM との信頼できる接続を確立できます。*id_token_value* には、CSSM で生成したトークンを入力します。 次のいずれかのオプションを入力します。 • **local**：高可用性セットアップのアクティブデバイスに対してのみ信頼要求を送信します。これがデフォルトのオプションです。 • **all**：高可用性セットアップのすべてのデバイスに対して信頼要求を送信します。 製品インスタンスに既存の信頼コードがあるにもかかわらず、信頼コード要求を送信するには、**force** キーワードを入力します。 信頼コードは、製品インスタンスの UDI にノードロックされます。UDI がすでに登録されている場合、CSSM は同じ UDI の新規登録を許可しません。**force** キーワードを入力すると、CSSM に送信されるメッセージに強制フラグが設定され、すでに存在する場合でも新しい信頼コードが作成されます。

ステップ 4	**show license status**
	例：
	`<output truncated>`
	`Trust Code Installed:`
	`  Active:`
	`PID:C9500-24Y4C,SN:CAT2344L4GH`
	`  INSTALLED on Sep 04 01:01:46 2020 EDT`
	`  Standby:`
	`PID:C9500-24Y4C,SN:CAT2344L4GJ`
	`  INSTALLED on Sep 04 01:01:46 2020 EDT`
		信頼コードがインストールされている場合は、日時が表示されます。日時はローカルタイムゾーンで表示されます。`Trust Code Installed:` フィールドを参照してください。

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 にログインします。[Smart Software Licensing] で、[Manage licenses] リンクをクリックします。

シスコから提供されたユーザ名とパスワードを使用してログインします。

ステップ 2 次のディレクトリパス、[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 （122 ページ）を参照してください。

CSSM への使用状況データのアップロードと ACK のダウンロード

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

始める前に

サポートされるトポロジ：

- CSSM への接続なし、CSLU なし
- 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 にログインします。[Smart Software Licensing] で、[Manage licenses] リンクをクリックします。

シスコから提供されたユーザー名とパスワードを使用してログインします。

ステップ 2 レポートを受信する**スマートアカウント**を選択します。

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

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

使用状況レポートは、アップロード後に CSSM で削除できません。

ステップ 5 [Select Virtual Accounts] ポップアップから、アップロードされたファイルを受信する**バーチャルアカウント**を選択します。ファイルが CSSM にアップロードされ、[Usage Data Files] タブエリアにファイル名、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、確認ステータスとともに表示されます。

ステップ 6 [Acknowledgment] 列で [Download] をクリックして、アップロードしたレポートの `.txt` ACK ファイルを保存します。

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

実装したトポロジに応じて、ファイルを製品インスタンスにインストールするか、またはCSLUに転送する、あるいは SSM オンプレミスにインポートすることができます。

製品インスタンスへのファイルのインストール

製品インスタンスにポリシーまたは ACK または SLAC をインポートして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

対応するファイルは、製品インスタンスにアクセスできる場所に保存しています。

- 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（121 ページ）を参照してください。
- ACK については、CSSM への使用状況データのアップロードと ACK のダウンロード（121 ページ）を参照してください。
- 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（110 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 filename* **bootflash:** 例： `Device# copy tftp://10.8.0.6/user01/example.txt bootflash:`	（任意）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。また、リモートの場所からファイルを直接インポートし、製品インスタンスにインストールすることもできます（次の手順）。 • コピー元：これはファイルのコピー元の場所です。コピー元は、ローカルまたはリモートのいずれかです。 • **bootflash:**：これはブートフラッシュメモリの場合の宛先です。
ステップ 3	**license smart import** *filepath_filename* 例： `Device# license smart import bootflash:example.txt`	ファイルを製品インスタンスにインポートしてインストールします。*filepath_filename* には、場所（ファイル名を含む）を指定します。インストール後、インストールしたファイルのタイプを示すシステムメッセージが表示されます。 （注） 複数の製品インスタンスに SLAC をインストールする場合（スタック設定など）、UDI ごとに個別の .txt SLACファイルをダウンロードしてください。一度に 1 つのファイルをインポートしてインストールします。
ステップ 4	**show license all** 例： `Device# show license all`	製品インスタンスのライセンス承認、ポリシー、およびレポート情報を表示します。

転送タイプ、URL、およびレポート間隔の設定

製品インスタンスの転送モードを設定するには、次のタスクを実行します。

始める前に

サポートされるトポロジ：すべて

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。プロンプトが表示されたらパスワードを入力します。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	
ステップ 3	**license smart transport** {**automatic** | **callhome** | **cslu** | **off** | **smart**} 例： `Device(config)# license smart transport cslu`	使用する製品インスタンスの転送モードを設定します。次のオプションから選択します。 • **automatic**：転送モード **cslu** を設定します。 • **callhome**：転送モードとして Call Home を有効にします。 • **cslu**：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。 トランスポート モード キーワードは CSLU と SSM オンプレミスで同じですが、トランスポート URL は異なります。次の手順の **license smart url cslu** *cslu_or_on-prem_url* を参照してください。 • **off**：製品インスタンスからのすべての通信を無効にします。 • **smart**：スマート転送を有効にします。

	コマンドまたはアクション	目的

ステップ 4	**license smart url** {*url* | **cslu** *cslu_url* | **default** | **smart** *smart_url* | **utility** *smart_url*}
	例：
	`Device(config)# license smart url cslu http://192.168.0.1:8182/cslu/v1/pi`
		設定された転送モードの URL を設定します。前の手順で選択した転送モードに応じて、対応する URL をここで設定します。
		• *url*：転送モードとして **callhome** を設定している場合は、このオプションを設定します。CSSM URL を次のように正確に入力します。
		`https://software.cisco.com/#module/SmartLicensing`
		no license smart url *url* コマンドは、デフォルトの URL に戻ります。
		• **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_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

	コマンドまたはアクション	目的
		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）（96 ページ）」を参照してください **no license smart url cslu** *cslu_url* コマンドは `http://cslu-local:8182/cslu/v1/pi` に戻ります • **default**：設定されている転送モードによって異なります。このオプションでは、**smart** および **cslu** 転送モードのみがサポートされます。 転送モードが **cslu** に設定されている場合、**license smart url default** を設定すると、CSLU URL は自動的に設定されます（`https://cslu-local:8182/cslu/v1/pi`）。 転送モードが **smart** に設定されている場合、**license smart url default** を設定すると、スマート URL は自動的に設定されます（`https://smartreceiver.cisco.com/licservice/license`）。 • **smart** *smart_url*：転送タイプとして **smart** を設定している場合は、このオプションを設定します。URL を次のように正確に入力します。 `https://smartreceiver.cisco.com/licservice/license` このオプションを設定すると、システムは **license smart url** *url* で自動的に URL の複製を作成します。重複するエントリは無視できます。これ以上の操作は必要ありません。

	コマンドまたはアクション	目的
		no license smart url smart*smart_url* コマンドは、デフォルトの URL に戻ります。 • **utility** *smart_url*：このオプションは CLI では使用できますがサポートされていません。
ステップ 5	**license smart usage interval** *interval_in_days* 例： `Device(config)# license smart usage interval 40`	（任意）レポート間隔の日数を設定します。デフォルトでは、RUM レポートは 30 日ごとに送信されます。有効な値の範囲は 1 ～ 3650 です。 この値をゼロに設定すると、適用されるポリシーの指定内容に関係なく、RUM レポートは送信されません。これは、CSLU または CSSM が受信側にある可能性があるトポロジに適用されます。 ゼロより大きい値を設定し、通信タイプが**オフ**に設定されている場合、*interval_in_days* と `Ongoing reporting frequency(days):` のポリシー値の間で、値の小さい方が適用されます。たとえば、*interval_in_days* が 100 に設定され、ポリシーの値が `Ongoing reporting frequency (days):90` の場合、RUM レポートは 90 日ごとに送信されます。 間隔を設定せず、デフォルトが有効な場合、レポート間隔は完全にポリシー値によって決定されます。たとえば、デフォルト値が有効で、不適用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。
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。

基本ライセンスまたはアドオンライセンスの設定

基本ライセンスまたはアドオンライセンスを注文および購入したら、使用する前にデバイスでライセンスを設定する必要があります。

このタスクではライセンスレベルを設定します。設定された変更を有効にする前にリロードが必要です。このタスクは、次の目的で使用できます。

- 現在のライセンスを変更する。
- 別のライセンスを追加する。たとえば、現在 Network Advantage を使用している場合、対応する Digital Networking Architecture（DNA）Advantage ライセンスで使用可能な機能も使用することができます。
- ライセンスを削除する。

始める前に

サポートされるトポロジ：すべて

使用可能な基本ライセンスとアドオンライセンスについては、基本ライセンスとアドオンライセンスを参照してください。

購入したライセンスに関する情報は、Cisco Smart Software Manager（CSSM）Web UI の製品インスタンスのスマートアカウントとバーチャルアカウントで確認できます。

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 boot level** *license_level* 例： `Device(config)# license boot level network-advantage add-on dna-advantage`	製品インスタンスで設定されたライセンスをアクティブにします。この例では、DNA Advantage ライセンスはリロード後に製品インスタンスでアクティブ化されます。
ステップ 4	**exit** 例： `Device(config)# exit`	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 5	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	構成ファイルへの変更を保存します。

ステップ 6	**show version**
	例：
	`Device# show version`
	
	`<output truncated>`
	`Technology Package License Information:`
	
	`------------------------------------------------`
	`Technology-package`
	`Technology-package`
	`Current Type`
	`Next reboot`
	`------------------------------------------------`
	`network-advantage Smart License`
	`network-advantage`
	`Subscription Smart License dna-advantage`
	
	`<output truncated>`
		現在設定されているライセンスの情報と、リロード後に適用可能なライセンスを表示します。

ステップ 7	**reload** 例： `Device# reload`	デバイスがリロードされます。

次のタスク

ライセンスレベルを設定すると、変更はリロード後に有効になります。レポートが必要かどうかを確認するには、**show license status** 特権EXECコマンドの出力を参照し、`Next ACK deadline:` フィールドと `Next report push:` フィールドを確認します。

（注） ライセンスの使用状況の変更は、製品インスタンスに記録されます。レポートに関連した次の手順は、必要に応じて実行しますが、現在のトポロジによって異なります。

- CSLU を介して CSSM に接続
  - 製品インスタンス開始型通信：アクションは不要です。製品インスタンスは通信を開始すると、ポリシー（**show license status** —> [Next report push]）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 CSLU に送信します。（製品インスタンスでこれを手動でトリガーするには、**license smart syncalllocal** 特権EXECコマンドを入力します。これにより、CSLU 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）。CSLU は RUM レポートを CSSM に転送し、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。

- CSLU 開始型通信：CSLU インターフェイスで製品インスタンスから使用状況を収集します。使用状況レポートの収集：CSLU 開始（CSLU インターフェイス）（76 ページ）CSLU は RUM レポートを CSSM に送信し、CSSM から ACK を取得します。CSLU が次に更新を実行するときに、ACK が製品インスタンスに適用されます。

- CSSM に直接接続：アクションは必要ありません。製品インスタンスは通信を開始すると、ポリシー（**show license status** —> [Next report push]）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 CSSM に送信します。（製品インスタンスでこれを手動でトリガーするには、**license smart syncalllocal** 特権EXECコマンドを入力します。これにより、CSSM 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）。ACK が使用可能になると、CSSM はこれを製品インスタンスに送り返します。

- CSLU は CSSM から切断

  - 製品インスタンス開始型通信：アクションは不要です。製品インスタンスは通信を開始すると、ポリシー（**show license status** —> [Next report push]）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 CSLU に送信します。（製品インスタンスでこれを手動でトリガーするには、**license smart syncalllocal** 特権EXECコマンドを入力します。これにより、CSLU 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）。

    CSLU が CSSM から切断されているため、CSLU インターフェイスと CSSM Web UI でタスク CSSM へのエクスポート（CSLU インターフェイス）（77 ページ）>CSSM への使用状況データのアップロードと ACK のダウンロード（121 ページ）>CSSM からのインポート（CSLU インターフェイス）（78 ページ）を実行します。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。

  - CSLU 開始型通信：CSLU インターフェイスで製品インスタンスから使用状況を収集します。使用状況レポートの収集：CSLU 開始（CSLU インターフェイス）（76 ページ）

    CSLU が CSSM から切断されているため、CSLU インターフェイスと CSSM Web UI でタスク CSSM へのエクスポート（CSLU インターフェイス）（77 ページ）>CSSM への使用状況データのアップロードと ACK のダウンロード（121 ページ）>CSSM からのインポート（CSLU インターフェイス）（78 ページ）を実行します。CSLU が次に更新を実行するときに、ACK が製品インスタンスに適用されます。

- コントローラを介して CSSM に接続：アクションは必要ありません（Cisco DNA Center GUI で最初のアドホックレポートをすでに完了している場合）。Cisco DNA Center は、後続のすべてのレポートを処理し、製品インスタンスに ACK を返します。

- CSSM への接続なし、CSLU なし：RUM レポートを（製品インスタンスの）ファイルに保存してから、CSSM にアップロードします（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）。**license smart save usage** コマンドを特権 EXEC モードで実行し、RUM レポートをファイルに保存します。次に、CSSM にファイルをアップロードして ACK をダウンロードするため、次のタスクを実行します。CSSM への使用状況データ

のアップロードと ACK のダウンロード（121 ページ）最後に、製品インスタンスに ACK をインストールするため、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（122 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：アクションは不要です。製品インスタンスは通信を開始すると、ポリシー（**show license status** —> [Next report push]）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 SSM オンプレミスに送信します。（製品インスタンスでこれを手動でトリガーするには、**license smart syncalllocal** 特権 EXEC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）。
    - 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 インターフェイスで、[Reports] > [Usage Schedules] > [Synchronization schedule with Cisco] に移動します。
    - SSM オンプレミスが CSSM から切断されている場合は、レポートに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。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）（97 ページ）
  - SSM オンプレミス開始型通信：SSM オンプレミス インターフェイスで、製品インスタンスから使用状況情報を収集します。[Reports] > [Synchronisation pull schedule with the devices] > [Synchronize now with the device] に移動します。
    - 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 インターフェイスで、[Reports] > [Usage Schedules] > [Synchronization schedule with Cisco] に移動します。
    - SSM オンプレミスが CSSM から切断されている場合は、レポートに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。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）（97 ページ）

リソース使用率測定レポートの例

次に、リソース使用率測定（RUM）レポートの例を XML 形式で示します（RUM レポートおよびレポート確認応答（10 ページ） を参照）。このような複数のレポートを連結して 1 つのレポートを形成できます。

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

[redacted]

```
  </smartLicense>
```

ポリシーを使用したスマートライセンシングのトラブルシューティング

このセクションでは、発生する可能性のあるポリシーを使用したスマートライセンシングに関連するシステムメッセージ、考えられる失敗の理由、および推奨するアクションを示します。

システム メッセージの概要

システムメッセージは、システムソフトウェアからコンソール（および任意で別のシステムのロギングサーバー）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 *11 :* 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。

シビラティ（重大度）	説明
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 *12*：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
[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）

システム メッセージ

このセクションでは、発生する可能性のあるポリシーを使用したスマートライセンシングに関連するシステムメッセージ、考えられる失敗の理由（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。

すべてのエラーメッセージについて、問題を解決できない場合は、シスコのテクニカルサポート担当者に次の情報をお知らせください。

コンソールまたはシステムログに出力されたとおりのメッセージ。

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。

ポリシーを使用したスマートライセンシング関連のシステムメッセージ：

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

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

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

失敗の理由として次が考えられます。

- 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：承認コードのインストールを試みましたが、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、必要な数の承認コードを提供していなかったことを意味します。
- 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、高可用性またはスタック構成セットアップでは、承認コードファイルにリストされているすべてのUDIが、高可用性またはスタック構成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。

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

```
Excerpt of UDI information in a SLAC file:
<smartLicenseAuthorization>
<udi>P:C9300X-24HX,SN:FOC2519L8R7</udi>

<output truncated>
</smartLicenseAuthorization>

Sample output of UDI information on a product instance:
Device# show license udi
UDI: PID:C9300X-24HX,SN:FOC2519L8R7
```

- 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。クロックが同期されていない場合、SLACの要求時の試行は**show license tech**の出力に反映されません。

```
Authorization Confirmation:
  Attempts: Total=0, Success=0, Fail=0  Ongoing Failure: Overall=0 Communication=0
```

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>

Communication Statistics:
=========================
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、高可用性およびスタック構成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、SLACを再度インストールします。

- 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
  ```

  この設定が完了したら、再度 **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。

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

失敗の理由として次が考えられます。

- CSSM、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。

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、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。

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
```

   上記の方法で解決しない場合は、製品インスタンスが設定されているかどうか、製品インスタンスの IP ネットワークが稼働しているかどうかを確認します。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* コマンドを設定します。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（78 ページ） で説明されているとおりに **ip http** が再設定されていない場合：

   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） （96 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 （94 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 （99 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、スマートライセンシング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（118ページ）および信頼コードのインストール（119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）（76 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）（77ページ）>CSSM への使用状況データのアップロードと ACK のダウンロード（121 ページ）>CSSM からのインポート（CSLU インターフェイス）（78 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）（76 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）（77 ページ）>CSSM への使用状況データのアップロードと ACK のダウンロード（121 ページ）>CSSM からのインポート（CSLU インターフェイス）（78 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：CSSM からのポリシーファイルのダウンロード（121 ページ）および製品インスタンスへのファイルのインストール（122 ページ）を実行します。

- 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）（97 ページ）を参照してください。

```
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況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 にログインします。[Smart Software Licensing] で、[Manage licenses] リンクをクリックします。[Inventory] タブをクリックします。[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。[Product Instances] タブをクリックします。

  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。その場合は、次の手順：CSSMからの信頼コード用新規トークンの生成 （118 ページ）および信頼コードのインストール （119 ページ）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、次の手順を実行します。
- 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 （5 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 （11 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 （70 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。

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

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

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

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

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

推奨するアクション：要求された時間内に RUM レポートが送信されるようにします。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） （76 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） （77 ページ）、CSSM への使用状況データのアップロードと ACK のダウンロード （121 ページ）、CSSM からのインポート（CSLU インターフェイス） （78 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 への使用状況データのアップロードと ACK のダウンロード （121 ページ） > 製品インスタンスへのファイルのインストール （122 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） （97 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。

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

トピック	マニュアル タイトル
この章で使用するコマンドのシンタックスおよび使用方法の詳細については、必要なリリースのコマンドリファレンスで [System Mangement] > [System Mangement Commands] を参照してください。	Command Reference （Catalyst 9300 シリーズ スイッチ）
Cisco Smart Software Manager 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	Cisco Smart License Utility クイック スタート セットアップ ガイド Cisco Smart License Utility ユーザーガイド
スマートライセンシングの全般情報	スマート ソフトウェア ライセンシング

トピック	マニュアル タイトル
Troubleshooting TechNotes	Catalyst スイッチング プラットフォームでのポリシーを使用したスマートライセンシング ポリシーを使用したスマートライセンシングへの Catalyst ライセンスの移行
スイッチングのための Cisco DNA	スイッチング向け Cisco DNA ソフトウェア サブスクリプション マトリックス

ポリシーを使用したスマートライセンシングの機能の履歴

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。

リリース	機能	機能情報
Cisco IOS XE Fuji 16.9.1	スマートライセンス	クラウドベースのソフトウェアライセンス管理ソリューションであり、ライセンス、ハードウェア、およびソフトウェアの使用状況の傾向を管理および追跡できます。 このリリース以降、スマートライセンスはデフォルトであり、ライセンスを管理するために使用できる唯一の方法です。 Cisco IOS XE Fuji 16.9.1 以降では、使用権（RTU）ライセンスモードが廃止され、関連する CLI の **license right-to-use** コマンドも使用できなくなりました。

リリース	機能	機能情報
Cisco IOS XE Amsterdam 17.3.2a	ポリシーを使用したスマートライセンス	スマートライセンシング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。 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。 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。
	Cisco DNA Center での Smart Licensing Using Policy のサポート	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。 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。 互換性のあるコントローラと製品インスタンスバージョンについては、コントローラ（5 ページ）を参照してください。 このトポロジについては、コントローラを介して CSSM に接続 （15 ページ）と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 （35 ページ）を参照してください。

リリース	機能	機能情報
Cisco IOS XE Amsterdam 17.3.3	Smart Licensing Using Policy 用の Smart Software Manager オンプレミス（SSM オンプレミス）サポート	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。 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 （5 ページ）を参照してください。 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 （18 ページ）とトポロジのワークフロー：SSM オンプレミス展開 （42 ページ）を参照してください。 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 （70 ページ）を参照してください。

リリース	機能	機能情報
Cisco IOS XE Bengaluru 17.6.2	高セキュリティのための輸出規制キー（HSECK9）	輸出規制ライセンスである HSECK9 キーは、Cisco Catalyst 9300X シリーズ スイッチに導入されました。 HSECK9 キーは、米国輸出管理法で制限されている暗号化機能の使用を許可する、輸出規制対象ライセンスです。制限付き暗号化機能を使用する場合は、HSECK9 キーが必要です。 承認コード （7 ページ）を参照してください。 次のトポロジで、サポートされている製品インスタンスに HSECK9 ライセンスの SLAC を取得してインストールできます。 • トポロジのワークフロー：CSLU を介して CSSM に接続 （30 ページ） • トポロジのワークフロー：CSSM に直接接続 （34 ページ） • トポロジのワークフロー：CSLU は CSSM から切断 （37 ページ） • トポロジのワークフロー：CSSM への接続なし、CSLU なし （41 ページ） • トポロジのワークフロー：SSM オンプレミス展開 （42 ページ）

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 には、http://www.cisco.com/go/cfn からアクセスします。

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。