



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 \(33 ページ\)](#)
- [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 \(121 ページ\)](#)
- [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 \(134 ページ\)](#)
- [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 \(134 ページ\)](#)

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。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。Cisco Catalyst ワイヤレスコントローラには、輸出規制ライセンスや適用ライセンスがなく、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 ワイヤレスコントローラにおける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情報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 [英語] 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、ポリシーを使用したスマートライセンシングの概念、サポートされる製品、サポートされる各トポロジの概要、およびポリシーを使用したスマートライセンシングと他の機能との連携について説明します。

概要

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

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



(注) 新しいハードウェアまたはソフトウェアの注文の場合、シスコは、次のアイテムを工場ですべてインストールすることで、**Smart Licensing Using Policy** の実装を簡素化します（用語については、以下の「[概念 \(7 ページ\)](#)」の項で説明します）。

- カスタムポリシー（使用可能な場合）
- CSSM に送信されるデータの信頼性を保証する信頼コード。これは、Cisco IOS XE Cupertino 17.7.1 以降でインストールされます。この信頼コードは、CSSM との通信には使用できません。

- 使用：Cisco Catalyst ワイヤレスコントローラのライセンスはすべて適用されません。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。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) を使用したり、使用状況情報を CSSM に直接レポートしたりできます。エアギャップネットワークの場合、使用状況情報をダウンロードして CSSM にアップロードする、オフラインレポートのプロビジョニングも使用できます。使用状況レポートはプレーンテキストの XML 形式です。[リソース使用率測定レポートの例 \(120 ページ\)](#) 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、ポリシーを使用したスマートライセンスをサポートする Cisco IOS-XE 製品インスタンスについて説明します。特に指定のない限り、製品シリーズのすべてのモデル（製品 ID または PID）がサポートされます。

表 1: サポート対象製品インスタンス：Cisco Catalyst ワイヤレスコントローラ

| Cisco Catalyst ワイヤレスコントローラ | ポリシーを使用したスマートライセンスのサポート導入時点 |
|---|--------------------------------|
| Cisco Catalyst 9800-40 ワイヤレスコントローラ | Cisco IOS XE Amsterdam 17.3.2a |
| Cisco Catalyst 9800-L ワイヤレス コントローラ | Cisco IOS XE Amsterdam 17.3.2a |
| Cisco Catalyst 9800-CL ワイヤレス コントローラ | Cisco IOS XE Amsterdam 17.3.2a |
| Cisco Catalyst 9800 組み込みワイヤレスコントローラ | Cisco IOS XE Amsterdam 17.3.2a |
| Cisco Catalyst 9100 アクセスポイント上の Cisco 組み込みワイヤレスコントローラ (EWC-AP) | 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スの実装に含めることができるさまざまなコンポーネントについて説明します。1つ以上のコンポーネントでトポロジが構成されます。

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。
- 1 つ以上の製品インスタンスから使用状況レポートを収集し、それら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、オンラインかオフラインで、またはファイルを使用してアップロードします。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。
- Cisco DNA Center などのコントローラに（シスコが）組み込みます。
- Linux を実行しているマシン（ラップトップまたはデスクトップ）に CSLU を導入します。

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

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。[License] タブで、[Smart Software Licensing] のリンクをクリックします。

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

CSSM では、次のことができます。

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



(注) この章における、ポリシーを使用したスマートライセンシングのコンテキストでは、「コントローラ」という用語は、常に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を意味します。「コントローラ」という用語は、製品インスタンスである Cisco Catalyst ワイヤレスコントローラを指すためには使用されません。

Cisco Catalyst ワイヤレスコントローラでは、Cisco DNA Center がサポートされてい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に必要な最小ソフトウェアバージョンに関する情報を次に示します。

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 | <ul style="list-style-type: none"> • Cisco Catalyst 9800-40 ワイヤレス コントローラ • Cisco Catalyst 9800-80 ワイヤレス コントローラ • Cisco Catalyst 9800-L ワイヤレス コントローラ • Cisco Catalyst 9800-CL ワイヤレス コントローラ • Cisco Catalyst 9800 組み込みワイヤレスコントローラ • Cisco Catalyst 9100 アクセスポイント上の Cisco 組み込みワイヤレスコントローラ (EWC-AP) |

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 | <ul style="list-style-type: none"> • Cisco Catalyst 9800-40 ワイヤレス コントローラ • Cisco Catalyst 9800-80 ワイヤレス コントローラ • Cisco Catalyst 9800-L ワイヤレス コントローラ • Cisco Catalyst 9800-CL ワイヤレス コントローラ • Cisco Catalyst 9800 組み込みワイヤレスコントローラ • Cisco Catalyst 9100 アクセスポイント上の Cisco 組み込みワイヤレスコントローラ (EWC-AP) |

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スの主要な概念について説明します。

ライセンス執行（エンフォースメント）タイプ

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

- 不適用または非適用

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。

Cisco Catalyst ワイヤレスコントローラで使用可能なライセンスはすべて、不適用ライセンスです。

- 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。

輸出規制ライセンスの例としては、シスコの特定のルータで使用可能な高速暗号化 (HSECK9) ライセンスがあります。

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。

AIR Network Essentials および AIR Network Advantage ライセンスは、Cisco Catalyst ワイヤレスコントローラで使用可能な不適用の永続的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。

AIR Digital Network Architecture (DNA) Essentials および AIR DNA Advantage ライセンスは、Cisco Catalyst ワイヤレスコントローラで使用可能な不適用の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。

SLAC は、Cisco Catalyst ワイヤレスコントローラで使用可能なライセンスには必要ありませんが、以前のライセンスモデルからポリシーを使用したスマートライセンシングにアップグレードする場合は、独自の承認コードを含む特定のライセンス予約 (SLR) を持つことができます。SLR 承認コードは、ポリシーを使用したスマートライセンシングへのアップグレード後にサポートされるようになります。



- (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。エアギャップネットワークの場合は、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 \(27 ページ\)](#) を参照してください。SLR 承認コードを返す場合は、[承認コードの削除と返却 \(104 ページ\)](#) 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。
この値がゼロの場合、使用状況が変更されない限り、以降のレポートは必要ありません。
- **Report on change (days)** : ライセンスの使用状況が変更された場合は、ここで指定した期間内にレポートが送信される必要があります。
この値がゼロの場合、使用状況の変更時のレポートは必要ありません。
この値がゼロでない場合は、変更を加えた後にレポートが必要です。次に示すすべてのシナリオは、製品インスタンスのライセンス使用状況における変更としてカウントされます。
 - 消費されたライセンスの変更 (別のライセンスへの変更やライセンスの追加または削除を含む)。
 - ライセンスの消費なしから 1 つ以上のライセンスの消費への移行。
 - 1 つ以上のライセンスの消費からライセンスの消費なしへの移行。



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

ポリシー選択について

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

Cisco defaultは、製品インスタンスで常に使用可能なデフォルトポリシーです。他のポリシーが適用されていない場合、製品インスタンスはこのデフォルトポリシーを適用します。次の表（表3：ポリシー：Cisco default（10ページ））に、Cisco default ポリシー値を示します。

お客様はポリシーを設定することはできませんが、Cisco Global Licensing Operations チームに連絡して、カスタマイズされたポリシーを要求することができます。[Support Case Manager](#) に移動します。[OPEN NEW CASE] をクリックして、[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3: 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のライセンス使用状況レポートです。RUM レポートは製品インスタンスによって生成され、CSSMによって使用されます。製品インスタンスは、ライセンス使用状況情報とすべてのライセンス使用状況の変更を、開いている RUM レポートに記録します。システムが決定した間隔で、開いている RUM レポートが閉じられ、新しい RUM レポートが開かれて、ライセンスの使用状況の記録が継続されます。閉じられた RUM レポートは、いつでも CSSM に送信できます。

RUM 確認応答（RUMACK または ACK）は CSSM からの応答であり、RUM レポートのステータスに関する情報を提供します。レポートの ACK が製品インスタンスで使用可能になると、対応する RUM レポートが不要になり、削除できることが示されます。

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

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

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

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

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

RUM レポートの生成、保存、管理

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

- 製品インスタンスで使用可能なすべての RUM レポートのリストを表示できます（レポートの数、それぞれの処理状態、エラーがあるかどうかなど）。この情報は、**show license rum**、**show license all**、**show license tech** 特権 EXEC コマンドで使用できます。出力に表示されるフィールドの詳細については、対応するリリースのコマンドリファレンスを参照してください。
- RUM レポートは、処理時間を短縮し、メモリ使用量を削減する新しい形式で保存されます。古い形式と新しい形式の違いによって生じる使用状況レポートの不整合を避けるために、次の状況では、トポロジに適用される方法で RUM レポートを送信することをお勧めします。

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

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

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

信頼コード

製品インスタンスが使用する *UDI* に関連付けられた公開キー

- RUM レポートに署名します。これにより、改ざんが防止され、データの真正性が確保されます。
- CSSM でセキュア通信を有効化します。

信頼コードを取得する方法は複数あります。

- Cisco IOS XE Cupertino 17.7.1 以降、すべての新規注文の信頼コードは出荷時にインストールされています。



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

- 信頼コードは、IDM トークンを使用して CSSM から取得できます。

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

信頼コードを取得する方法は、CSSMに直接接続するすべてのオプションに適用できます。詳細については、[CSSMに直接接続（15 ページ）](#)を参照してください。

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

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

トポロジの説明と対応するワークフローを参照して、各シナリオにおける信頼コードの要求およびインストール方法を確認してください（[サポートされるトポロジ（13 ページ）](#)）。

信頼コードが製品インスタンスにインストールされている場合、**show license status** コマンドの出力の [Trust Code Installed:] フィールドにタイムスタンプが表示されます。

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（33 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。

既存のライセンス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。

初期実装後、追加の設定タスクを実行する必要がある場合（AIR ライセンスを変更する、RUM レポートを同期する場合など）は、「[ポリシーを使用したスマートライセンシングのタスクライブラリ](#)」を参照してください。



(注) 続行する前に、必ず「サポートされるトポロジ」を確認してください。

CSLU を介して CSSM に接続

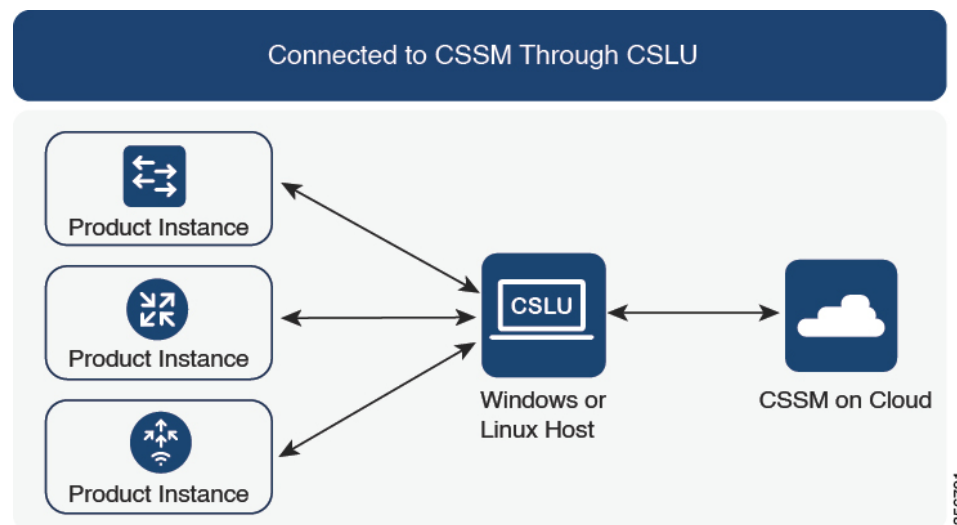
概要：

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

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

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

図 1: トポロジ：CSLU を介して CSSM に接続



考慮事項または推奨事項：

ネットワークのセキュリティポリシーに応じて通信方法を選択します。

リリースごとの変更と拡張：

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

Cisco IOS XE Cupertino 17.7.1 以降：

- 信頼コードの要求とインストール

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

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

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

• RUM レポートスロットリング

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

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

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

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 \(33 ページ\)](#) 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。



- (注) 出荷時にインストールされた信頼コードは、CSSM との通信には使用できません。つまり、このトポロジでは、出荷時にインストールされた信頼コードが存在する場合でも、CSSM で ID トークンを生成して信頼コードを取得し、出荷時にインストールされた既存の信頼コードを上書きする必要があります。[信頼コード \(12 ページ\)](#) も参照してください。

次の方法で CSSM と通信するように製品インスタンスを設定できます。

- スマート転送を使用して CSSM と通信する。

スマート転送は、スマートライセンシング (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。

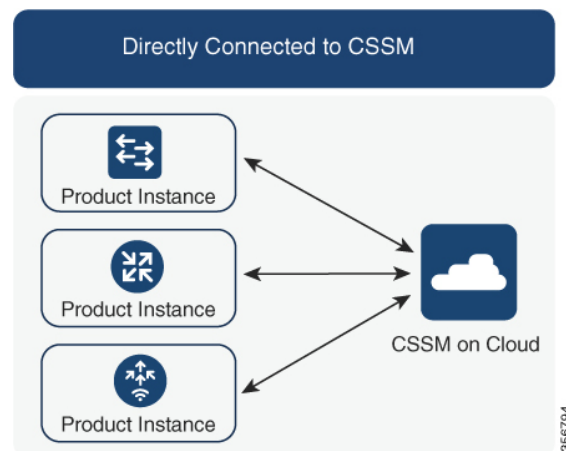
- スマート転送：この方法では、製品インスタンスは特定のスマート転送ライセンスサーバ URL を使用します。これは、ワークフローのセクションに示すとおりを設定する必要があります。
- HTTPS プロキシを介したスマート転送：この方法では、製品インスタンスはプロキシサーバを使用してライセンスサーバと通信し、最終的には CSSM と通信します。

- Call Home を使用して CSSM と通信する。

Call Home を使用すると、E メールベースおよび Web ベースで重大なシステム イベントの通知を行えます。CSSM へのこの接続方法は、以前のスマートライセン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（36 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った問題が解決されます。また、RUM レポートの過剰な生成によって引き起こされたメモリ関連の問題とシステムのスローダウンも解決します。

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

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

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（36 ページ）](#)を参照してください。

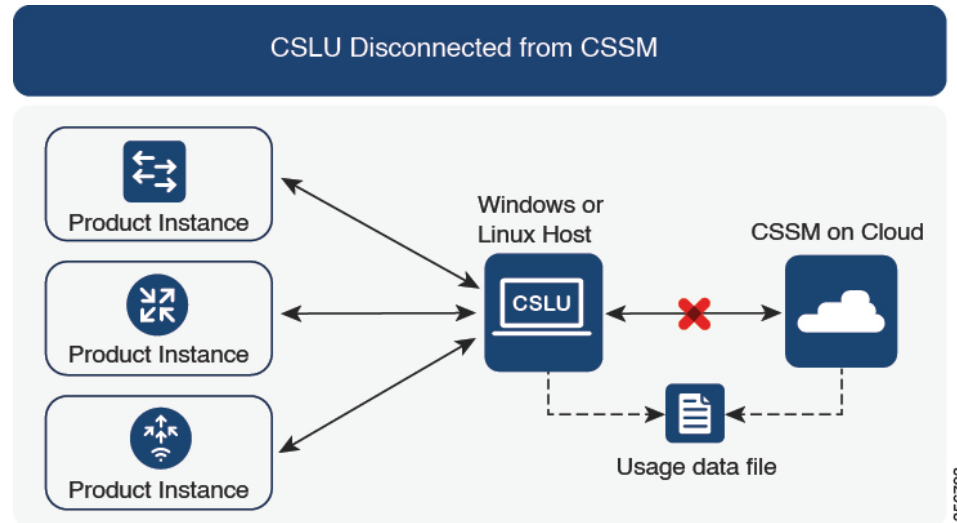
CSLU は CSSM から切断

概要：

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

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

図 3: トポロジ : CSLU は CSSM から切断



考慮事項または推奨事項 :

ネットワークのセキュリティポリシーに応じて通信方法を選択します。

リリースごとの変更と拡張 :

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

Cisco IOS XE Cupertino 17.7.1 以降 :

- 信頼コードの要求とインストール

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

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

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

- RUM レポートスロットリング

製品インスタンス開始モードでは、レポートの最小頻度は1日に制限されます。これは、製品インスタンスが1日に複数の RUM レポートを送信しないことを意味します。これに

より、特定のライセンスに対して生成および送信される RUM レポートが多すぎるという問題が解決されます。また、RUM レポートの過剰な生成によって引き起こされたメモリ関連の問題とシステムのスローダウンも解決します。

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

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

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。

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 ワイヤレスコントローラでサポートされているコントローラは、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。



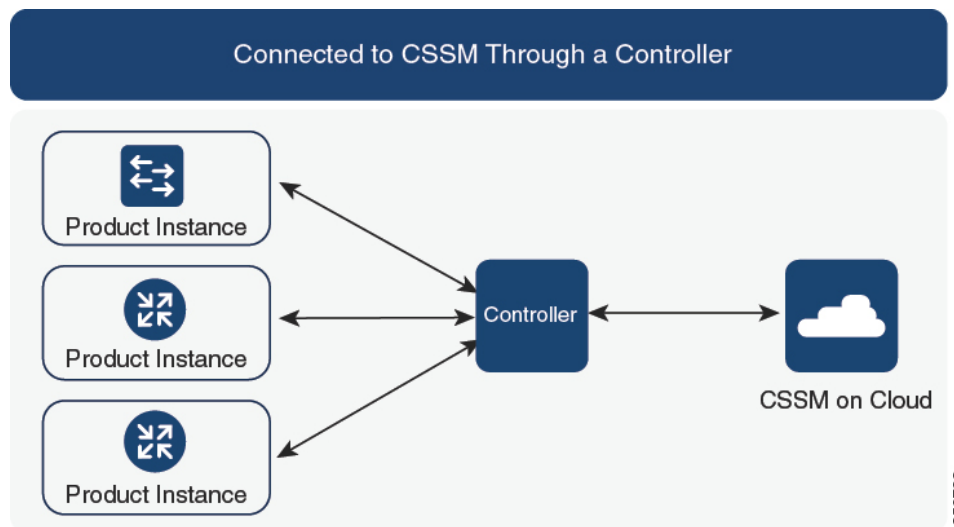
(注) 製品インスタンスが定期レポートの対象となる前に、アドホックレポートを少なくとも 1 回実行する必要があります。

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。

Cisco DNA Center では、輸出規制ライセンス用の SLAC のインストールと削除ができます。Cisco Catalyst ワイヤレスコントローラで使用可能なライセンスはすべて不適用ライセンスであるため、SLAC のインストールと削除は適用されません。

信頼コードは必要ありません。

図 4: 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。

次の手順:

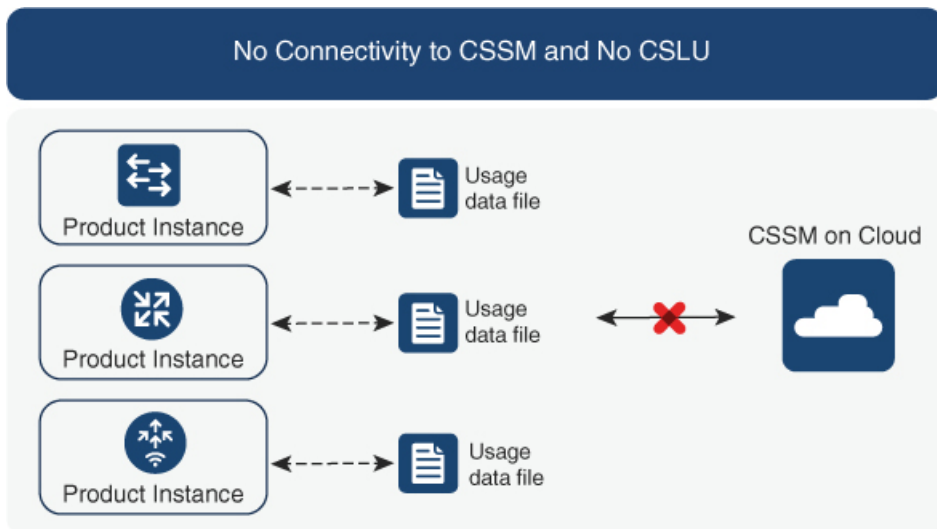
このトポロジを実装するには、[トポロジのワークフロー: コントローラを介して CSSM に接続 \(41 ページ\)](#) を参照してください。

CSSM への接続なし、CSLU なし

概要:

ここでは、製品インスタンスと CSSM は相互に切断され、他の中間ユーティリティまたはコンポーネントはありません。すべての通信は、ファイルのアップロードとダウンロードという形式です。これらのファイルは、RUM レポート UDI に関連付けられた信頼コードの要求です。

図 5: トポロジ : CSSM への接続なし、CSLU なし



考慮事項または推奨事項 :

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

リリースごとの変更と拡張

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

Cisco IOS XE Cupertino 17.7.1 以降 :

- 信頼コードの要求とインストール

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

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

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

- よりシンプルな承認コードの返却

承認コードの返却ファイルをアップロードする簡単な方法を CSSM Web UI で使用できます。CSSM Web UI で正しいバーチャルアカウントの製品インスタンスを見つける必要がなくなりました。RUM レポートと同様に、返却ファイルをアップロードできます。

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 \(42 ページ\)](#) 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。

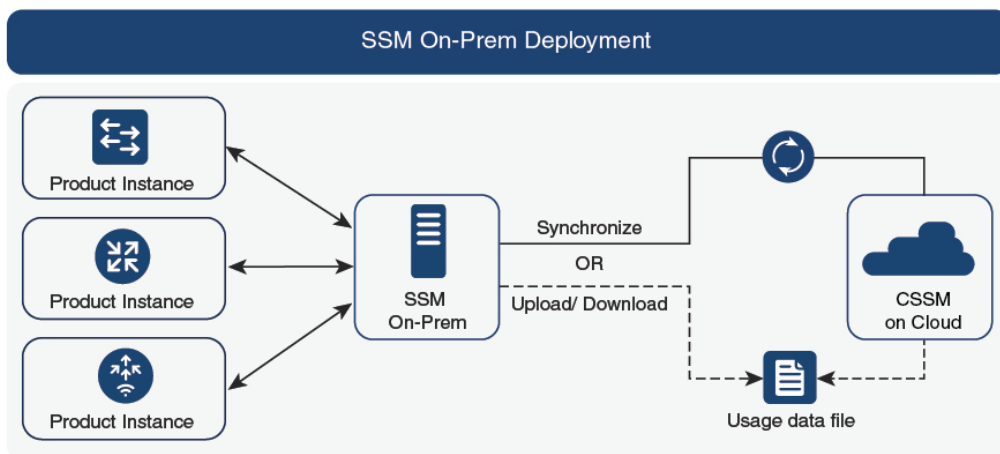
SSM オンプレミスで使用状況が使用できるようになったら、同じ間隔で CSSM と同期して、製品インスタンス数、ライセンス数、およびライセンス使用状況情報が CSSM と SSM オンプレミスの両方と同じであることを確認します。SSM オンプレミスと CSSM 間の使用状況の同期オプション：プッシュとプルモードの場合：

- 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います。必要なコマンドの詳細については、『[Cisco Smart Software On-Prem Console Guide](#)』 [英語] を参照してください。
- 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 8202108 以降のみです。ローカルアカウントの同期を目的とするプロキシの使用はサポートされています。これは [Synchronization] ウィジェットを使用して実行され、Smart Licensing Using Policy がサポートされている SSM オンプレミス導入リリースから利用可能です。
- SSM オンプレミス開始型通信は、ネットワークアドレス変換 (NAT) 設定の製品インスタンスではサポートされていません。製品インスタンス開始型通信を使用する必要があります。さらに、NAT 設定の製品インスタンスをサポートするために SSM オンプレミスを有効にする必要があります。詳細は、このトポロジのワークフローで提供されます。

リリースごとの変更と拡張：

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

Cisco IOS XE Cupertino 17.9.1 以降：

- RUM レポートスロットリング

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

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

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

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

デュアルシャーシのセットアップ（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。

ワイヤレス N+1 トポロジでは、「n」個のワイヤレスコントローラがプライマリとして機能し、「+1」のワイヤレスコントローラがアクセスポイント（AP）のセカンダリまたはフォールバック ワイヤレス コントローラとして機能します。各アクセスポイントには、プライマリ ワイヤレス コントローラとセカンダリ ワイヤレス コントローラが設定されています。プライマリで障害が発生した場合、プライマリに接続されていたすべてのアクセスポイントがセカンダリ ワイヤレス コントローラにフォールバックするようになりました。

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、セットアップのすべてのスタンバイに適用されます。

高可用性セットアップでの製品インスタンス機能

ここでは、高可用性設定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セカンダリが既存の高可用性設定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、スタンバイの承認コードと信頼コードを要求し（必要な場合）、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。アクティブな場合、高可用性設定のすべてのデバイス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。

新しいスタンバイの追加または削除の場合：

- 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。

スタンバイでの信頼コードのインストール（まだインストールされていない場合）。

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。

セカンダリの追加または削除の場合：

セカンダリ製品インスタンスの追加または削除にのみ適用される製品インスタンス機能はありません。さらに、すべてのセカンダリ製品インスタンスは、プライマリ製品インスタンス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ります。

アップグレード

このセクションでは、次の点について説明します。

以前のライセンスモデルから Smart Licensing Using Policy への移行以前のライセンスモデルから移行する場合は、Cisco Catalyst ワイヤレスコントローラに適用される移行シナリオの例について、[ポリシーを使用したスマートライセンシングへの移行 \(48 ページ\)](#) セクションも参照してください。

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

アップグレード前に現在のライセン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。

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。Cisco Catalyst ワイヤレスコントローラのすべてのライセンスは、不適用ライセンスです。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。
 - 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。

サポートされている Cisco Catalyst ワイヤレスコントローラのいずれにも、輸出規制ライセンスや適用ライセンスがないため、これらの適用タイプと必要な SLAC は適用されません。

アップグレードが既存ライセンスのレポートに与える影響

| 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 |
|------------------------------|--|
| 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 (登録および承認済みライセンス) | ポリシーによって異なります。 |
| 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 |

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。

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

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

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

ダウングレード

ここでは、新規展開と既存の展開に関する以前のライセンスモデルへのダウングレードについて説明します。また、ポリシーを使用したスマートライセンシング環境内のダウングレードに関連する情報についても説明します。

新規展開のダウングレード

このセクションでは、Smart Licensing Using Policy がデフォルトで有効になっているソフトウェアバージョンで新しく購入した製品インスタンスが、Smart Licensing Using Policy がサポートされていないソフトウェアバージョンにダウングレードされた場合に適用される考慮事項とアクションについて説明します。

ダウングレードの結果は、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、追加の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あります。以下の表（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）を参照してください。

表 4: 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 |
|--|--|---|
| <p>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。</p> | <p>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</p> | <p>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。</p> |
| | <p>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）</p> | <p>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。</p> |
| <p>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。</p> | <p>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</p> | <p>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。</p> |
| <p>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）</p> | <p>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</p> | <p>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。</p> |

アップグレード後のダウングレード

ここでは、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に製品インスタンスをアップグレードしてから、以前のライセンスモデルにダウングレードする場合に適用される、考慮事項とアクションについて説明します。

そのような製品インスタンスを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。次の表を参照してください。

表 5: 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 | 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 idtokenidtoken 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 |
|---|----------------------------|---|
| 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。

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

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

Cisco IOS XE Cupertino 17.7.1 以降、RUM レポートは処理時間を短縮する形式で保存されます。古い形式と新しい形式の違いによって生じる使用状況レポートの不整合を避けるために、Cisco IOS XE Cupertino 17.7.1 以降のリリースからポリシーを使用したスマートライセンシングをサポートする以前のリリースにダウングレードする際に、使用状況レポートを1回完了することをお勧めします。

ポリシーを使用したスマートライセンシングの設定方法： 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

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

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

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

2. CSLU の環境設定

タスクの実行場所：CSLU

1. [シスコへのログイン \(CSLU インターフェイス\) \(72 ページ\)](#)
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 \(CSLU インターフェイス\) \(74 ページ\)](#)

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、追加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、追加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
```

結果 :

製品インスタンスは通信を開始すると、ポリシーに従って、スケジュールされた時刻に最初の RUM レポートを自動的に送信します。この最初のレポートとともに、必要に応じて、UDI に

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

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

製品インスタンスが次にいつ 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。

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。[Trust Code Installed] フィールドで更新されたタイムスタンプを確認します。

ライセンスの使用状況が変更された場合は、[AIR ライセンスの設定 \(116 ページ\)](#) を参照しレポートへの影響を確認してください。

CSLU 開始型通信の場合のタスク

CSLU のインストール→CSLU の環境設定→製品インスタンスの設定→使用状況の同期

1. CSLU のインストール

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

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

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

2. CSLU の環境設定

タスクの実行場所：CSLU

1. [シスコへのログイン \(CSLU インターフェイス\) \(72 ページ\)](#)
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 \(CSLU インターフェイス\) \(76 ページ\)](#)

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 \(79 ページ\)](#)

4. 使用状況の同期

タスクが実行される場所：製品インスタンス

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。CSSM から ACK を取得し、インストールのために製品インスタンスに送り返します。CSSM からの ACK には信頼コードと SLAC が含まれます (要求した場合)。

ライセンスの使用状況が変更された場合は、[AIR ライセンスの設定 \(116 ページ\)](#) を参照しレポートへの影響を確認してください。

トポロジのワークフロー：CSSM に直接接続

[Smart Account Set-Up] → [Product Instance Configuration] → [Trust Establishment with CSSM]

1. スマートアカウントのセットアップ

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

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

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 \(96 ページ\)](#)

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 \(99 ページ\)](#) 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 \(100 ページ\)](#)」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 \(103 ページ\)](#)」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 \(108 ページ\)](#)
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 \(109 ページ\)](#)

結果：

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

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

レポート間隔を変更するには、グローバル コンフィギュレーション モードで **license smart 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。

ライセンスの使用状況が変更された場合は、[AIR ライセンスの設定 \(116 ページ\)](#) を参照しレポートへの影響を確認してください。

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 の環境設定→製品インスタンスの設定→使用状況の同期

1. CSLU のインストール

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

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

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

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）（74 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、追加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、追加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. 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 \(CSLU インターフェイス\) \(78 ページ\)](#)
2. [CSSM へのデータまたは要求のアップロードとファイルのダウンロード \(111 ページ\)](#)
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。

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

製品インスタンスが次にいつ 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。

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。[Trust Code Installed] フィールドで更新されたタイムスタンプを確認します。

ライセンスの使用状況が変更された場合は、[AIR ライセンスの設定 \(116 ページ\)](#) を参照しレポートへの影響を確認してください。

CSLU 開始型通信の場合のタスク

CSLU のインストール→CSLU の環境設定→製品インスタンスの設定→使用状況の同期

1. CSLU のインストール

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

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

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

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 \(CSLU インターフェイス\) \(76 ページ\)](#)
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 \(79 ページ\)](#)

4. 使用状況の同期

タスクの実行場所：CSLU と CSSM

製品インスタンスから使用状況データを収集します。CSLU は CSSM から切断されるため、後で CSLU が製品インスタンスから収集した使用状況データをファイルに保存します。該当する場合、この最初のレポートに加えて、承認コードと UDI に関連付けられた信頼コード要求が RUM レポートに含まれます。次に、シスコに接続されているワークステーションからファイルを CSSM にアップロードします。この後、CSSM から ACK をダウン

ロードします。CSLU がインストールされて製品インスタンスに接続されているワークステーションで、ファイルを CSLU にアップロードします。

1. [CSSM へのエクスポート \(CSLU インターフェイス\)](#) (78 ページ)
2. [CSSM へのデータまたは要求のアップロードとファイルのダウンロード](#) (111 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 に信頼コードと SLAC が含まれます (要求した場合)。CSLU が次に更新を実行するときに、アップロードされた ACK が製品インスタンスに適用されます。

ライセンスの使用状況が変更された場合は、[AIR ライセンスの設定](#) (116 ページ) を参照しレポートへの影響を確認してください。

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

1. スマートアカウントとバーチャルアカウントを設定します。

CSSM Web UI へのログインに使用する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：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

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
```

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報告するには、RUM レポートを製品インスタンスのファイルに保存する必要があります。インターネットおよびシスコに接続でき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。

1. RUM レポートの生成と保存

license smart save usage コマンドを特権 EXEC モードで入力します。次の例では、すべての RUM レポートがファイル `all_rum.txt` で製品インスタンスのフラッシュメモリに保存されます。

Cisco IOS XE Cupertino 17.7.1 以降では、信頼コードが製品インスタンスにまだ存在しない場合、このコマンドを設定すると、RUM レポートに自動的に信頼コードの要求が含まれます。これは、スタンドアロンおよび高可用性設定でサポートされます。

下記の例では、ファイルはまずブートフラッシュに保存されてから、TFTPの場所にコピーされます。

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

2. 使用状況データを CSSM にアップロード：[CSSM へのデータまたは要求のアップロードとファイルのダウンロード](#) (111 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](#) (112 ページ)

ライセンスの使用方法を変更する場合は、[AIR ライセンスの設定](#) (116 ページ) を参照してください。

SLR 承認コードを返す場合は、[承認コードの削除と返却](#) (104 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）方式を実装するか、または SSM オンプレミス開始型通信（プル）方式を実装するかによって、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

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）。
 - （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 \(SSM オンプレミス UI\)](#) (83 ページ)
 2. [デバイスの検証 \(SSM オンプレミス UI\)](#) (84 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](#) (85 ページ)
2. [トランスポート URL の取得 \(SSM オンプレミス UI\)](#) (87 ページ)
3. [転送タイプ、URL、およびレポート間隔の設定](#) (113 ページ)

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

4. 使用状況の最初の同期

タスクの実行場所：製品インスタンス、SSM オンプレミス、CSSM

1. 製品インスタンスを SSM オンプレミスと同期します。

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

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

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 \(SSM オンプレミス UI\) \(88 ページ\)](#) 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リングします。グローバル コンフィギュレーション モードで **license smart usage interval interval_in_days** コマンドを入力します。

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

製品インスタンスが次にいつ 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、次のように、定期的な同期をスケジュールするか、必要なファイルをアップロードおよびダウンロードします。
 - CSSM との定期的な同期をスケジュールします。SSM オンプレミス UI で、[Reports] > [Usage Schedules] > [Synchronization schedule with Cisco] に移動します。次の頻度情報を入力し、保存します。
 - [Days] : 同期が実行される頻度を示します。たとえば、2 を入力すると、同期は 2 日に 1 回行われます。
 - [Time of Day] : 24 時間表記法で、同期が実行される時刻を示します。たとえば、14 hours と 0 minutes を入力すると、ローカルタイムゾーンの午後 2 時 (1400) に同期が行われます。
 - レポートに必要なファイルのアップロードとダウンロードを実行します ([使用状況データのエクスポートとインポート \(SSM オンプレミス UI\) \(88 ページ\)](#))。

SSM オンプレミスインスタンス開始型通信の場合のタスク

SSM オンプレミスのインストール → 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）（89 ページ）](#)）を実行します。

3. 製品インスタンスの設定

タスクの実行場所：製品インスタンスと SSM オンプレミス UI

特権 EXEC モードで **copy running-config startup-config** コマンドを入力して、製品インスタンスの設定変更を必ず保存してください。[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（90 ページ）](#)

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 UI 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）（88 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り得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キスポートとインポート \(SSM オンプレミス UI\) \(88 ページ\)](#)) 。

ポリシーを使用したスマートライセンシングへの移行

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

「[アップグレード \(27 ページ\)](#)」の項を必ず読み、ポリシーを使用したスマートライセンシングによる以前の全ライセンスモデルの処理方法を理解してください。

ポリシーを使用したスマートライセンシングは、Cisco IOS XE Amsterdam 17.3.2a 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。

ワイヤレスコントローラ ソフトウェアのアップグレード

アップグレード手順の詳細については、以下を参照してください。

- Cisco Catalyst 9100 アクセスポイントの Cisco 組み込みワイヤレスコントローラ については、[Catalyst アクセスポイントのオンラインヘルプの Cisco 組み込みワイヤレスコントローラ](#) の「Software Upgrade」の項を参照してください。
- その他のサポートされるワイヤレスコントローラについては、[Cisco Catalyst 9800 シリーズワイヤレスコントローラのソフトウェア設定ガイドの「System Upgrade」](#) の「Upgrading the Cisco Catalyst 9800 Wireless Controller Software」の項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またはISSUでアップグレードできます（ISSUはサポートされているプラットフォームおよびリリースでのみ）。

ソフトウェアバージョンのアップグレード後

- トポロジを実装します。

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

アップグレード元のライセンスモデルに関係なく、アップグレード後にトポロジを変更できます。

- 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（28 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 9800-CL ワイヤレスコントローラの例を示します。

- [表 6: 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（50 ページ）](#)
- [移行後の CSSM Web UI（54 ページ）](#)
- [移行後のレポート（57 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 6: 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（スマートライセンシング） | アップグレード後（ポリシーを使用したスマートライセンシング） |
|---|---|
| <p>show license summary</p> <p>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。</p> | <p>show license summary</p> <p>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。</p> |

| | |
|--|--|
| <p>アップグレード前 (スマートライセンシング)</p> | <p>アップグレード後 (ポリシーを使用したスマートライセンシング)</p> |
| <pre> Device# show license summary Smart Licensing is ENABLED Registration: Status: REGISTERED Smart Account: SA-Eg-Company-02 Virtual Account: Dept-02 Export-Controlled Functionality: ALLOWED Last Renewal Attempt: None Next Renewal Attempt: May 01 08:19:02 2021 IST License Authorization: Status: AUTHORIZED Last Communication Attempt: SUCCEEDED Next Communication Attempt: Dec 02 08:19:09 2020 IST License Usage: License Entitlement tag Count Status ----- AP Perpetual Network... (DNA_NWSTACK_E) 1 AUTHORIZED Aironet DNA Essentia... (AIR-DNA-E) 1 AUTHORIZED </pre> | <pre> Device# show license summary License Usage: License Entitlement Tag Count Status ----- air-network-essentials (DNA_NWSTACK_E) 1 IN USE air-dna-essentials (AIR-DNA-E) 1 IN USE </pre> |
| <p>アップグレード前 (スマートライセンシング)</p> | <p>アップグレード後 (ポリシーを使用したスマートライセンシング)</p> |
| <p>show license usage</p> <p>アップグレード前に1つの永続的ライセンスと1つのサブスクリプションライセンスが使用されています。</p> | <p>show license usage</p> <p>すべてのライセンスが移行され、[Enforcement Type] フィールドに NOT ENFORCED と表示されます。</p> <p>Cisco Catalyst ワイヤレスコントローラには、輸出規制ライセンスや適用ライセンスはありません。</p> |

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

| アップグレード前（スマートライセンシング） | アップグレード後（ポリシーを使用したスマートライセンシング） |
|---|--|
| <pre> Device# show license usage License Authorization: Status: AUTHORIZED on Nov 02 08:21:29 2020 IST AP Perpetual Networkstack Essentials (DNA_NWSTACK_E): Description: AP Perpetual Network Stack entitled with DNA-E Count: 1 Version: 1.0 Status: AUTHORIZED Export status: NOT RESTRICTED Aironet DNA Essentials Term Licenses (AIR-DNA-E): Description: DNA Essentials for Wireless Count: 1 Version: 1.0 Status: AUTHORIZED Export status: NOT RESTRICTED </pre> | <pre> Device# show license usage License Authorization: Status: Not Applicable air-network-essentials (DNA_NWSTACK_E): Description: air-network-essentials Count: 1 Version: 1.0 Status: IN USE Export status: NOT RESTRICTED Feature Name: air-network-essentials Feature Description: air-network-essentials Enforcement type: NOT ENFORCED License type: Perpetual air-dna-essentials (AIR-DNA-E): Description: air-dna-essentials Count: 1 Version: 1.0 Status: IN USE Export status: NOT RESTRICTED Feature Name: air-dna-essentials Feature Description: air-dna-essentials Enforcement type: NOT ENFORCED License type: Perpetual </pre> |
| アップグレード前（スマートライセンシング） | アップグレード後（ポリシーを使用したスマートライセンシング） |
| <pre> show license status </pre> | <pre> show license status Transport: フィールドには、更新前に設定され、アップグ レード後も保持される転送タイプが表示されます。 Policy: ヘッダーと詳細には、スマートアカウントまたは バーチャルアカウントで使用可能なカスタムポリシーが表 示されます。このポリシーは製品インスタンスにも自動的 にインストールされています。（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。 </pre> |

| アップグレード前 (スマートライセンシング) | アップグレード後 (ポリシーを使用したスマートライセンシング) |
|---|---|
| <pre> 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: SA-Eg-Company-02 Virtual Account: Dept-02 Export-Controlled Functionality: ALLOWED Initial Registration: SUCCEEDED on Nov 02 08:19:02 2020 IST Last Renewal Attempt: None Next Renewal Attempt: May 01 08:19:01 2021 IST Registration Expires: Nov 02 08:14:06 2021 IST License Authorization: Status: AUTHORIZED on Nov 02 08:21:29 2020 IST Last Communication Attempt: SUCCEEDED on Nov 02 08:21:29 2020 IST Next Communication Attempt: Dec 02 08:19:09 2020 IST Communication Deadline: Jan 31 08:14:15 2021 IST Export Authorization Key: Features Authorized: <none> </pre> | <pre> Device# show license status Utility: Status: DISABLED Smart Licensing Using Policy: Status: ENABLED Data Privacy: Sending Hostname: yes Callhome hostname privacy: DISABLED Smart Licensing hostname privacy: DISABLED Version privacy: DISABLED Transport: Type: Callhome Policy: Policy in use: Installed On Nov 02 09:09:47 2020 IST Policy name: SLE Policy Reporting ACK required: yes (Customer Policy) Unenforced/Non-Export Perpetual Attributes: First report requirement (days): 60 (Customer Policy) Reporting frequency (days): 60 (Customer Policy) Report on change (days): 60 (Customer Policy) Unenforced/Non-Export Subscription Attributes: First report requirement (days): 30 (Customer Policy) Reporting frequency (days): 30 (Customer Policy) Report on change (days): 30 (Customer Policy) Enforced (Perpetual/Subscription) License Attributes: First report requirement (days): 0 (CISCO default) Reporting frequency (days): 90 (Customer Policy) Report on change (days): 90 (Customer Policy) Export (Perpetual/Subscription) License Attributes: First report requirement (days): 0 (CISCO default) Reporting frequency (days): 90 (Customer Policy) Report on change (days): 90 (Customer Policy) Miscellaneous: Custom Id: <empty> Usage Reporting: Last ACK received: Nov 02 09:09:47 2020 IST Next ACK deadline: Jan 01 09:09:47 2021 IST Reporting push interval: 30 days Next ACK push check: Nov 02 09:13:54 2020 IST Next report push: Dec 02 09:05:45 2020 IST Last report push: Nov 02 09:05:45 2020 IST Last report file write: <none> Trust Code Installed: Active: PID:C9800-CL-K9,SN:93BBAH93MGS INSTALLED on Nov 02 08:59:26 2020 IST Standby: PID:C9800-CL-K9,SN:9XECPSUU4XN INSTALLED on Nov 02 09:00:45 2020 IST </pre> |

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

| | |
|--|--|
| アップグレード前（スマートライセンシング） | アップグレード後（ポリシーを使用したスマートライセンシング） |
| show license udi | show license udi 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。 移行前と移行後のサンプル出力に変化はありません。 |
| Device# show license udi UDI: PID:C9800-CL-K9, SN:93BBAH93MGS HA UDI List: Active:PID:C9800-CL-K9, SN:93BBAH93MGS Standby:PID:C9800-CL-K9, SN:9XECPSUU4XN | Device# show license udi UDI: PID:C9800-CL-K9, SN:93BBAH93MGS HA UDI List: Active:PID:C9800-CL-K9, SN:93BBAH93MGS Standby:PID:C9800-CL-K9, SN:9XECPSUU4XN |

移行後の CSSM Web UI

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

以前はホスト名で表示されていた製品インスタンス（この例では Catalyst 9800-CL Cloud ワイヤレスコントローラ）が、代わりに UDI で表示されるようになりました。移行されたすべての UDI、つまり、PID:C9800-CL-K9、SN:93BBAH93MGS、および PID:C9800-CL-K9、SN:9XECPSUU4XN が表示されます。

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:C9800-CL-K9、SN:93BBAH93MGS 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] には [No Records Found] と表示されます。

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：移行前の *CSSM Web UI* の製品インスタンスのホスト名

Device

Overview
High Availability
Event Log

Description

Catalyst 9800CL Cloud Wireless Controller

General

| | | |
|--------------------|---|---------------------------|
| Name: | Device | ← Hostname before upgrade |
| Product: | Catalyst 9800CL Cloud Wireless Controller | |
| Host Identifier: | - | |
| MAC Address: | - | |
| PID: | C9800-CL-K9 | |
| Serial Number: | 93BBAH93MGS | |
| UUID | - | |
| Virtual Account: | Dept-02 | |
| Registration Date: | 2020-Nov-02 10:44:08 | |
| Last Contact: | 2020-Nov-02 10:46:33 | |

License Usage

| License | Billing | Expires | Require |
|--------------------------------------|---------|---------|---------|
| Aironet DNA Essentials Term Licenses | Prepaid | - | 1 |
| AP Perpetual Networkstack Essentials | Prepaid | - | 1 |

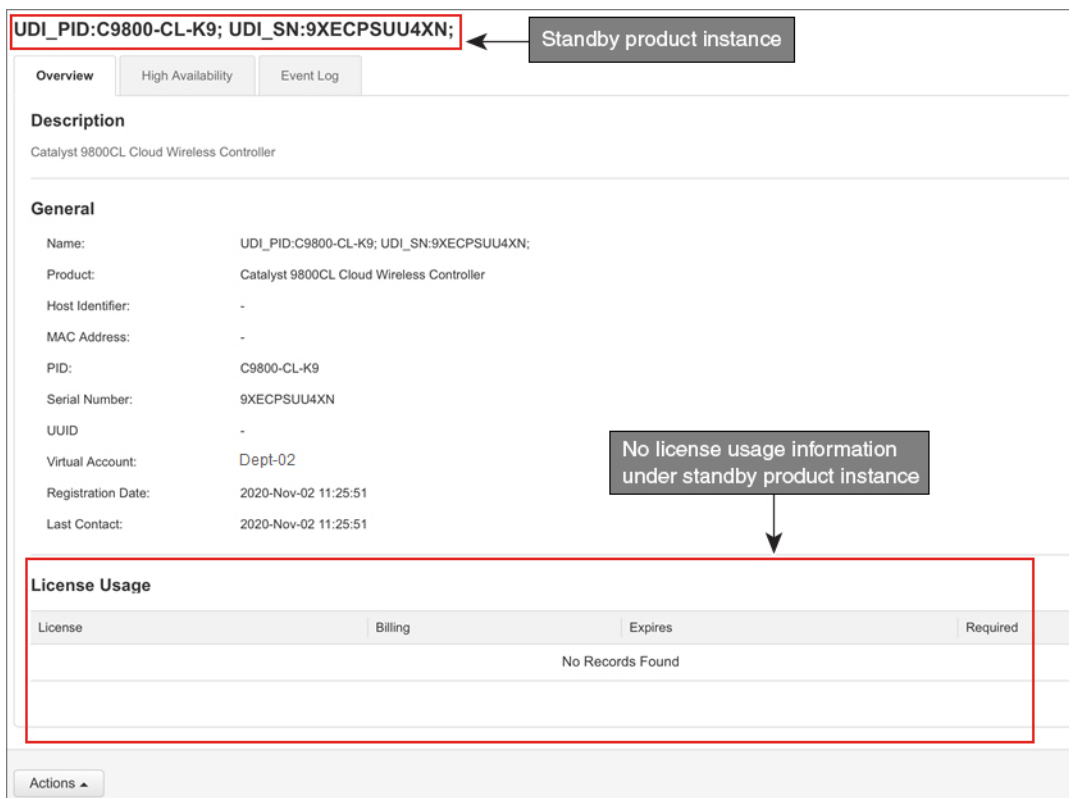
例：スマートライセンシングからポリシーを使用したスマートライセンシングへ

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：移行後の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

The screenshot displays a web interface for an active product instance. At the top, a red box highlights the UDI: `UDI_PID:C9800-CL-K9; UDI_SN:93BBAH93MGS;`, with an arrow pointing to a label 'Active product instance'. Below this are tabs for 'Overview', 'High Availability', and 'Event Log'. The 'Description' section identifies the product as 'Catalyst 9800CL Cloud Wireless Controller'. The 'General' section lists various attributes, with a red box around the 'Name' field containing the same UDI string, labeled 'UDI after upgrade'. The 'License Usage' section at the bottom contains a table with two rows of license information, highlighted by a red box and labeled 'License usage information under active product instance'.

| License | Billing | Expires | Required |
|--------------------------------------|---------|---------|----------|
| Aironet DNA Essentials Term Licenses | Prepaid | - | 1 |
| AP Perpetual Networkstack Essentials | Prepaid | - | 1 |

図 9: 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：移行後のスタンバイ製品インスタンス



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。

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、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 (global config)* コマンドを参照してください。

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 9800-CL ワイヤレスコントローラの例を示します。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。

ライセンス転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 \(20 ページ\)](#) トポロ

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

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（8 ページ）](#) を参照してください。

- [表 7: 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（58 ページ）](#)
- [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 7: 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 (SLR) | アップグレード後 (ポリシーを使用したスマートライセンシング) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---------------------------------|-----------------|------------|--------|-------|--|--|--|---------------------------------------|--|---|------------|-------------------------------------|--|---|------------|--|---------|-----------------|-------|--------|-------|--|--|--|-------------------------------------|--|---|------------|---------------------------------------|--|---|------------|
| <p>show license summary</p> <p>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。</p> <p>Device# show license summary</p> <p>Smart Licensing is ENABLED License Reservation is ENABLED</p> <p>Registration:</p> <p>Status: REGISTERED - SPECIFIC LICENSE RESERVATION Export-Controlled Functionality: ALLOWED</p> <p>License Authorization: Status: AUTHORIZED - RESERVED</p> <p>License Usage:</p> <table border="1"> <thead> <tr> <th>License</th> <th>Entitlement tag</th> <th>Count</th> <th>Status</th> </tr> </thead> <tbody> <tr> <td colspan="4">-----</td> </tr> <tr> <td>AP Perpetual Network... (DNA_NWStack)</td> <td></td> <td>1</td> <td>AUTHORIZED</td> </tr> <tr> <td>Aironet DNA Advantag... (AIR-DNA-A)</td> <td></td> <td>1</td> <td>AUTHORIZED</td> </tr> </tbody> </table> | License | Entitlement tag | Count | Status | ----- | | | | AP Perpetual Network... (DNA_NWStack) | | 1 | AUTHORIZED | Aironet DNA Advantag... (AIR-DNA-A) | | 1 | AUTHORIZED | <p>show license summary</p> <p>ライセンスは移行されますが、いずれの AP もコントローラに接続していないため、現在の使用数 (カウント) はゼロであり、[Status] フィールドにはライセンスが [NOT IN USE] であると表示されます。</p> <p>Device# show license summary License Reservation is ENABLED</p> <p>License Usage:</p> <table border="1"> <thead> <tr> <th>License</th> <th>Entitlement Tag</th> <th>Count</th> <th>Status</th> </tr> </thead> <tbody> <tr> <td colspan="4">-----</td> </tr> <tr> <td>Aironet DNA Advantag... (AIR-DNA-A)</td> <td></td> <td>0</td> <td>NOT IN USE</td> </tr> <tr> <td>AP Perpetual Network... (DNA_NWStack)</td> <td></td> <td>0</td> <td>NOT IN USE</td> </tr> </tbody> </table> | License | Entitlement Tag | Count | Status | ----- | | | | Aironet DNA Advantag... (AIR-DNA-A) | | 0 | NOT IN USE | AP Perpetual Network... (DNA_NWStack) | | 0 | NOT IN USE |
| License | Entitlement tag | Count | Status | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ----- | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| AP Perpetual Network... (DNA_NWStack) | | 1 | AUTHORIZED | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Aironet DNA Advantag... (AIR-DNA-A) | | 1 | AUTHORIZED | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| License | Entitlement Tag | Count | Status | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ----- | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Aironet DNA Advantag... (AIR-DNA-A) | | 0 | NOT IN USE | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| AP Perpetual Network... (DNA_NWStack) | | 0 | NOT IN USE | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

| | |
|--|---|
| <p>アップグレード前 (SLR)</p> | <p>アップグレード後 (ポリシーを使用したスマートライセンシング)</p> |
| <p>show license reservation</p> | <p>show license authorization</p> <p>Last Confirmation code: フィールド: 高可用性設定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。</p> <p>Specified license reservations: ヘッダーは、永続的ライセンス (AP Perpetual Networkstack Advantage) とサブスクリプションライセンス (Aironet DNA Advantage 期間ライセンス) が移行された SLR ライセンスであることを示しています。</p> |

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

| アップグレード前 (SLR) | アップグレード後 (ポリシーを使用したスマートライセンシング) |
|---|---------------------------------|
| <pre> Device# show license reservation License reservation: ENABLED Overall status: Active: PID:C9800-CL-K9,SN:93BBAH93MGS Reservation status: SPECIFIC INSTALLED on Nov 02 03:16:01 2020 IST Export-Controlled Functionality: ALLOWED Last Confirmation code: 102fc949 Standby: PID:C9800-CL-K9,SN:9XECPSUU4XN Reservation status: SPECIFIC INSTALLED on Nov 02 03:15:45 2020 IST Export-Controlled Functionality: ALLOWED Last Confirmation code: ad4382fe Specified license reservations: Aironet DNA Advantage Term Licenses (AIR-DNA-A): Description: DNA Advantage for Wireless Total reserved count: 20 Term information: Active: PID:C9800-CL-K9,SN:93BBAH93MGS License type: TERM Start Date: 2020-OCT-14 UTC End Date: 2021-APR-12 UTC Term Count: 5 License type: TERM Start Date: 2020-JUN-18 UTC End Date: 2020-DEC-15 UTC Term Count: 5 Standby: PID:C9800-CL-K9,SN:9XECPSUU4XN License type: TERM Start Date: 2020-OCT-14 UTC End Date: 2021-APR-12 UTC Term Count: 10 AP Perpetual Networkstack Advantage (DNA_NWStack): Description: AP Perpetual Network Stack entitled with DNA-A Total reserved count: 20 Term information: Active: PID:C9800-CL-K9,SN:93BBAH93MGS License type: TERM Start Date: 2020-OCT-14 UTC End Date: 2021-APR-12 UTC Term Count: 5 License type: TERM Start Date: 2020-JUN-18 UTC End Date: 2020-DEC-15 UTC Term Count: 5 Standby: PID:C9800-CL-K9,SN:9XECPSUU4XN License type: TERM Start Date: 2020-OCT-14 UTC End Date: 2021-APR-12 UTC Term Count: 10 </pre> | |

| アップグレード前 (SLR) | アップグレード後 (ポリシーを使用したスマートライセンシング) |
|----------------|---|
| | <pre> Device# show license authorization Overall status: Active: PID:C9800-CL-K9,SN:93BBAH93MGS Status: SPECIFIC INSTALLED on Nov 02 03:16:01 2020 IST Last Confirmation code: 102fc949 Standby: PID:C9800-CL-K9,SN:9XECPSUU4XN Status: SPECIFIC INSTALLED on Nov 02 03:15:45 2020 IST Last Confirmation code: ad4382fe Specified license reservations: Aironet DNA Advantage Term Licenses (AIR-DNA-A): Description: DNA Advantage for Wireless Total reserved count: 20 Enforcement type: NOT ENFORCED Term information: Active: PID:C9800-CL-K9,SN:93BBAH93MGS Authorization type: SPECIFIC INSTALLED on Nov 02 03:15:45 2020 IST License type: TERM Start Date: 2020-OCT-14 UTC End Date: 2021-APR-12 UTC Term Count: 5 Authorization type: SPECIFIC INSTALLED on Nov 02 03:15:45 2020 IST License type: TERM Start Date: 2020-JUN-18 UTC End Date: 2020-DEC-15 UTC Term Count: 5 Standby: PID:C9800-CL-K9,SN:9XECPSUU4XN Authorization type: SPECIFIC INSTALLED on Nov 02 03:15:45 2020 IST License type: TERM Start Date: 2020-OCT-14 UTC End Date: 2021-APR-12 UTC Term Count: 10 AP Perpetual Networkstack Advantage (DNA_NWStack): Description: AP Perpetual Network Stack entitled with DNA-A Total reserved count: 20 Enforcement type: NOT ENFORCED Term information: Active: PID:C9800-CL-K9,SN:93BBAH93MGS Authorization type: SPECIFIC INSTALLED on Nov 02 03:15:45 2020 IST License type: TERM Start Date: 2020-OCT-14 UTC End Date: 2021-APR-12 UTC Term Count: 5 Authorization type: SPECIFIC INSTALLED on Nov 02 03:15:45 2020 IST License type: TERM Start Date: 2020-JUN-18 UTC End Date: 2020-DEC-15 UTC Term Count: 5 Standby: PID:C9800-CL-K9,SN:9XECPSUU4XN Authorization type: SPECIFIC INSTALLED on Nov 02 03:15:45 2020 IST License type: TERM </pre> |

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

| | |
|---------------------|--|
| アップグレード前 (SLR) | アップグレード後 (ポリシーを使用したスマートライセンシング) |
| | <p>Start Date: 2020-OCT-14 UTC End Date: 2021-APR-12 UTC Term Count: 10</p> <p>Purchased Licenses: No Purchase Information Available</p> |
| アップグレード前 (SLR) | アップグレード後 (ポリシーを使用したスマートライセンシング) |
| show license status | <p>show license status</p> <p>Transport: ヘッダーの下にある Type: フィールドは、転送タイプがオフに設定されていることを示します。</p> <p>Usage Reporting: ヘッダーの下にある 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性の有無とタイミングを示します。</p> |

| アップグレード前 (SLR) | アップグレード後 (ポリシーを使用したスマートライセンシング) |
|----------------|--|
| - | <pre> 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: <none> Reporting push interval: 0 (no reporting) Next ACK push check: Nov 01 20:31:46 2020 IST Next report push: <none> Last report push: <none> Last report file write: <none> Trust Code Installed: <none> </pre> |

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

移行後の CSSM Web UI

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

[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」が表示されていないことが確認されると、ライセンスの使用状況はアクティブな製品インスタンスのみで表示されます。

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：アップグレード前のアクティブな製品インスタンス

UDI_PID:C9800-CL-K9; UDI_SN:93BBAH93MGS; ← Active product instance

Overview | Event Log

Description
Catalyst 9800CL Cloud Wireless Controller

General

Name: UDI_PID:C9800-CL-K9; UDI_SN:93BBAH93MGS;
 Product: Catalyst 9800CL Cloud Wireless Controller
 Host Identifier: -
 MAC Address: -
 PID: C9800-CL-K9
 Serial Number: 93BBAH93MGS
 UUID: -
 Virtual Account: Dept-02
 Registration Date: 2020-Nov-02 05:36:20

Last Contact: 2020-Nov-02 05:36:20 (Reserved Licenses) - [Download Reservation Authorization Code](#) ← SLR before upgrade

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

| License | Billing | Expires | Required |
|-------------------------------------|---------|--------------------------------|----------|
| Aironet DNA Advantage Term Licenses | Prepaid | multiple terms | 10 |
| AP Perpetual Networkstack Advantage | Prepaid | multiple terms | 10 |

図 11: SLR からポリシーを使用したスマートライセンシング：アップグレード後のアクティブな製品インスタンス

The screenshot displays the configuration page for a Catalyst 9800CL Cloud Wireless Controller. At the top, the UDI information is highlighted with a red box and labeled "Active product instance": `UDI_PID:C9800-CL-K9; UDI_SN:93BBAH93MGS;`. Below this, the "General" section lists various identifiers, with the "Last Contact" field highlighted in red and labeled "SLR after upgrade and usage reporting": `2020-Nov-02 06:09:01`. The "License Usage" section contains a table with the following data:

| License | Billing | Expires | Required |
|-------------------------------------|---------|---------|----------|
| Aironet DNA Advantage Term Licenses | Prepaid | - | 1 |
| AP Perpetual Networkstack Advantage | Prepaid | - | 1 |

移行後のレポート

SLR ライセンスは、ライセンスの使用に変化した場合にのみレポートを必要とします（たとえば、サブスクリプションライセンスを指定された期間使用する場合）。

エアギャップネットワークでは、**show license status** の出力の `Next report push:` の日付を使用して、次の使用状況レポートの送信タイミングを確認することで、製品インスタンスと CSSM が同期されます。

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、コマンドリファレンスで **license smart**（特権 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。

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

```
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 へのデータまたは要求のアップロードとファイルのダウンロード \(111 ページ\)](#)
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 \(112 ページ\)](#)

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、評価期限切れライセンス（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 9800-CL ワイヤレスコントローラの例です。

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。Cisco Catalyst ワイヤレスコントローラのライセンスはすべて適用されない（適用タイプ）であるため、機能は失われません。

- [表 8：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 \(66 ページ\)](#)
- [移行後の CSSM Web UI \(70 ページ\)](#)
- [移行後のレポート \(70 ページ\)](#)

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: 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（スマートライセンシング、評価モード） | アップグレード後（ポリシーを使用したスマートライセンシング） |
|---|--|
| show license summary ライセンスは UNREGISTERED で、EVAL MODE になっています。 | show license summary 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（スマートライセンシング、評価モード） | アップグレード後（ポリシーを使用したスマートライセンシング） |
|---|--|
| <pre>Device# show license summary Smart Licensing is ENABLED Registration: Status: UNREGISTERED Export-Controlled Functionality: NOT ALLOWED License Authorization: Status: EVAL EXPIRED License Usage: License Entitlement tag Count Status ----- EXPIRED (DNA_NWStack) 1 EVAL EXPIRED (AIR-DNA-A) 1 EVAL</pre> | <pre>Device# show license summary License Usage: License Entitlement Tag Count Status ----- air-network-advantage (DNA_NWStack) 1 IN USE air-dna-advantage (AIR-DNA-A) 1 IN USE</pre> |

| アップグレード前（スマートライセンシング、評価モード） | アップグレード後（ポリシーを使用したスマートライセンシング） |
|---|---|
| <pre>show license usage Device# show license usage License Authorization: Status: EVAL EXPIRED on Apr 14 18:20:46 2020 UTC (DNA_NWStack): Description: Count: 1 Version: 1.0 Status: EVAL EXPIRED Export status: NOT RESTRICTED (AIR-DNA-A): Description: Count: 1 Version: 1.0 Status: EVAL EXPIRED Export status: NOT RESTRICTED</pre> | <p>Enforcement Type フィールドに NOT ENFORCED と表示されます。（Cisco Catalyst ワイヤレスコントローラには、輸出規制ライセンスや適用ライセンスはありません）。</p> <pre>Device# show license usage License Authorization: Status: Not Applicable air-network-advantage (DNA_NWStack): Description: air-network-advantage Count: 1 Version: 1.0 Status: IN USE Export status: NOT RESTRICTED Feature Name: air-network-advantage Feature Description: air-network-advantage Enforcement type: NOT ENFORCED License type: Perpetual air-dna-advantage (AIR-DNA-A): Description: air-dna-advantage Count: 1 Version: 1.0 Status: IN USE Export status: NOT RESTRICTED Feature Name: air-dna-advantage Feature Description: air-dna-advantage Enforcement type: NOT ENFORCED License type: Perpetual</pre> |

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

| アップグレード前（スマートライセンシング、評価モード） | アップグレード後（ポリシーを使用したスマートライセンシング） |
|-----------------------------------|--|
| <p>show license status</p> | <p>show license status</p> <p>Transport: フィールドには、デフォルトのタイプが設定されていて、製品インスタンスが CSLU を検出するための URL またはメソッドが指定されていないことが表示されます。</p> <p>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。</p> <p>Policy: ヘッダーと詳細には、Cisco default ポリシーが適用されていることが示されます。</p> <p>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。</p> |

| アップグレード前（スマートライセンシング、評価モード） | アップグレード後（ポリシーを使用したスマートライセンシング） |
|---|--|
| <pre> Device# show license status Smart Licensing is ENABLED Utility: Status: DISABLED Data Privacy: Sending Hostname: yes Callhome hostname privacy: DISABLED Smart Licensing hostname privacy: DISABLED Version privacy: DISABLED Transport: Type: Callhome Registration: Status: UNREGISTERED Export-Controlled Functionality: NOT ALLOWED License Authorization: Status: EVAL EXPIRED on Apr 14 18:20:46 2020 UTC Export Authorization Key: Features Authorized: <none> </pre> | <pre> Device# show license status Utility: Status: DISABLED Smart Licensing Using Policy: Status: ENABLED Data Privacy: Sending Hostname: yes Callhome hostname privacy: DISABLED Smart Licensing hostname privacy: DISABLED Version privacy: DISABLED Transport: Type: cslu Cslu address: <empty> Proxy: Not Configured Policy: Policy in use: Merged from multiple sources. Reporting ACK required: yes (CISCO default) Unenforced/Non-Export Perpetual Attributes: First report requirement (days): 365 (CISCO default) Reporting frequency (days): 0 (CISCO default) Report on change (days): 90 (CISCO default) Unenforced/Non-Export Subscription Attributes: First report requirement (days): 90 (CISCO default) Reporting frequency (days): 90 (CISCO default) Report on change (days): 90 (CISCO default) Enforced (Perpetual/Subscription) License Attributes: First report requirement (days): 0 (CISCO default) Reporting frequency (days): 0 (CISCO default) Report on change (days): 0 (CISCO default) Export (Perpetual/Subscription) License Attributes: First report requirement (days): 0 (CISCO default) Reporting frequency (days): 0 (CISCO default) Report on change (days): 0 (CISCO default) Miscellaneous: Custom Id: <empty> Usage Reporting: Last ACK received: <none> Next ACK deadline: <none> Reporting push interval: 0 (no reporting) Next ACK push check: <none> Next report push: <none> Last report push: <none> Last report file write: <none> Trust Code Installed: <none> </pre> |

移行後の CSSM Web UI

<https://software.cisco.com> で CSSM Web UI にログインし、[Smart Software Licensing] をクリックします。[Inventory]>[Product Instances] で、移行された製品インスタンスの [Last Contact] フィールドに、移行後に更新されたタイムスタンプが表示されます。

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 (13 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 (33 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 (6 ページ) を参照)、SSM オンプレミスのバージョンおよび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の概要としてこの項を使用できます。

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。

必要な最小ソフトウェアバージョンについては、SSM オンプレミス (6 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、ワイヤレス コントローラ ソフトウェアのアップグレード (49 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 \(SSM オンプレミス UI\) \(88 ページ\)](#) 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 \(SSM オンプレミス UI\) \(88 ページ\)](#) 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 \(33 ページ\)](#) 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] タブを選択します。

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

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

製品インスタンス開始型通信のネットワーク到達可能性の確認

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

始める前に

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

手順

| | コマンドまたはアクション | 目的 |
|--------|--|--|
| ステップ 1 | enable 例： Device> enable | 特権 EXEC モードを有効にします。プロンプトが表示されたらパスワードを入力します。 |
| ステップ 2 | configure terminal 例： Device# configure terminal | グローバル コンフィギュレーションモードを開始します。 |
| ステップ 3 | interface interface-type-number 例： Device (config)# interface gigabitethernet0/0 | インターフェイス コンフィギュレーションモードを開始し、VRF に関連付けられたイーサネットインターフェイス、サブインターフェイス、または VLAN を指定します。 |
| ステップ 4 | vrf forwarding vrf-name 例： | 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 |

| | コマンドまたはアクション | 目的 |
|---------|--|--|
| | Device (config-if) # vrf forwarding Mgmt-vrf | 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。 (注) Cisco Catalyst 9800-L-F ワイヤレスコントローラ 10G ポートは、自動ネゴシエーション操作をサポートしていません。 |
| 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 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 : | DNS ドメインルックアップ用のソース インターフェイスを設定します。 |

| | コマンドまたはアクション | 目的 |
|---------|---|--|
| | Device(config)# ip domain lookup source-interface gigabitethernet0/0 | |
| 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、ネームサーバはエントリ <code>cslu-local.example.com</code> を作成します。 |

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

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



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

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

手順

- ステップ 1 [Inventory] タブに移動し、[Product Instances] テーブルから [Add Single Product] を選択します。
- ステップ 2 [Host] に入力します (ホストの IP アドレス)。
- ステップ 3 [Connect Method] を選択し、CSLU 開始の接続方法を 1 つを選択します。
- ステップ 4 右側のパネルで、[Product Instance Login Credentials] をクリックします。画面の左側のパネルが変化して [User Name] フィールドと [Password] フィールドに変わります。
- ステップ 5 製品インスタンスの [User Name] と [Password] を入力します。
- ステップ 6 [保存 (Save)] をクリックします。

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

使用状況レポートの収集 : CSLU 開始 (CSLU インターフェイス)

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

製品インスタンスを設定して選択した後 ([Add Single Product] を選択し、[Host] に名前を入力して [CSLU Initiated] 接続メソッドを選択)、[Actions for Selected] > [Collect Usage] を選択します。CSLU は選択した製品インスタンスに接続し、使用状況レポートを収集します。収集された使用状況レポートは、CSLU のローカルライブラリに保存されます。これらのレポートは、

CSLU がシスコに接続されている場合はシスコに転送できます。または (シスコに接続されていない場合は) [Data]>[Export to CSSM] の順に選択して、手動で使用状況の収集をトリガーできます。

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

手順

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

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

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

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

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

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

この時点で、使用状況レポートがローカルディレクトリ (ライブラリ) に保存されます。使用状況レポートをシスコにアップロードするには、[CSSM へのデータまたは要求のアップロードとファイルのダウンロード \(111 ページ\)](#) 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)

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

手順

- ステップ 1** [Preferences] タブに移動し、[Cisco Connectivity] トグルスイッチをオフにします。フィールドが「Cisco Is Not Available」に切り替わります。
- ステップ 2** ホーム画面から、[Data] > [Export to CSSM] の順に移動します。
- ステップ 3** 開いたウィンドウからファイルを選択し、[Save] をクリックします。これでファイルが保存されました。
- (注) この時点で、DLC ファイル、RUM ファイル、またはその両方があります。
- ステップ 4** シスコに接続できる端末に移動し、次の手順を実行します。 [CSSM へのデータまたは要求のアップロードとファイルのダウンロード \(111 ページ\)](#)
- ファイルがダウンロードされたら、CSLU にインポートできます。 [CSSM からのインポート \(CSLU インターフェイス\) \(78 ページ\)](#) を参照してください。
-

CSSM からのインポート (CSLU インターフェイス)

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

手順

- ステップ 1** CSLU にアクセス可能な場所にファイルがダウンロードされていることを確認します。
- ステップ 2** CSU のホーム画面から、[Data] > [Import from CSSM] の順に移動します。
- ステップ 3** [Import from CSSM] モーダルが開き、次のいずれかを実行できます。
- ローカルドライブにあるファイルをドラッグアンドドロップします。または、
 - 適切な *.xml ファイルを参照し、ファイルを選択して [Open] をクリックします。
- アップロードが成功すると、ファイルがサーバーに正常に送信されたことを示すメッセージが表示されます。アップロードが成功しない場合は、インポートエラーが発生します。
- ステップ 4** アップロードが完了したら、ウィンドウの右上隅にある [x] をクリックして閉じます。
-

CSLU 開始型通信のネットワーク到達可能性の確認

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

始める前に

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

手順

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

| | コマンドまたはアクション | 目的 |
|---------|--|---|
| | <pre>192.168.1.100 192.168.1.200 192.168.1.300</pre> | 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 | <p>ip domain lookup source-interface interface-type-number</p> <p>例 :</p> <pre>Device(config)# ip domain lookup source-interface gigabitethernet0/0</pre> | <p>デバイス上で、DNSに基づくホスト名からアドレスへの変換を有効にします。この機能は、デフォルトでイネーブルにされています。</p> <p>ユーザのネットワークデバイスが、名前の割り当てを制御できないネットワーク内のデバイスと接続する必要がある場合、グローバルなインターネットのネーミング方式 (DNS) を使用して、ユーザのデバイスを一意に識別するデバイス名を動的に割り当てることができます。</p> |
| ステップ 9 | <p>ip domain name name</p> <p>例 :</p> <pre>Device(config)# ip domain name vrf Mgmt-vrf cisco.com</pre> | 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 | <p>no username name</p> <p>例 :</p> <pre>Device(config)# no username admin</pre> | <p>(必須) 指定されたユーザ名が存在する場合はクリアします。nameには、次のステップで作成するユーザ名と同じものを入力します。これにより、次のステップで作成するユーザ名が重複していないことが保証されます。</p> <p>CSLU 開始型の RUM レポート取得に REST API を使用する場合は、CSLU にログインする必要があります。ここでユーザ名が重複していると、システムにユーザ名が重複している場合にこの機能が正しく動作しないことがあります。</p> |
| ステップ 11 | <p>username name privilege level password password</p> <p>例 :</p> | (必須) ユーザ名をベースとした認証システムを構築します。 |

| | コマンドまたはアクション | 目的 |
|---------|---|--|
| | <pre>Device(config)# username admin privilege 15 password 0 lab</pre> | <p>privilege キーワードにより、ユーザの権限レベルを設定します。ユーザの権限レベルを指定する 0 ~ 15 の数字です。</p> <p>password を使用すると、name 引数にアクセスできます。パスワードは 1 ~ 25 文字で、埋め込みスペースを使用でき、username コマンドの最後のオプションとして指定します。</p> <p>これにより、CSLU が製品インスタンスのネイティブ REST を使用できるようになります。</p> <p>(注) このユーザ名とパスワードを CSLU で入力します (使用状況レポートの収集: CSLU 開始 (CSLU インターフェイス) (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。</p> |
| ステップ 12 | <p>interface <i>interface-type-number</i></p> <p>例 :</p> <pre>Device (config)# interface gigabitethernet0/0</pre> | <p>インターフェイス コンフィギュレーションモードを開始し、VRF に関連付けられたイーサネットインターフェイス、サブインターフェイス、または VLAN を指定します。</p> |
| ステップ 13 | <p>vrf forwarding <i>vrf-name</i></p> <p>例 :</p> <pre>Device(config-if)# vrf forwarding Mgmt-vrf</pre> | <p>VRF をレイヤ 3 インターフェイスに対応付けます。このコマンドは、インターフェイスでマルチプロトコル VRF をアクティブにします。</p> |
| ステップ 14 | <p>ip address <i>ip-address mask</i></p> <p>例 :</p> <pre>Device(config-if)# ip address 192.168.0.1 255.255.0.0</pre> | <p>VRF の IP アドレスを定義します。</p> |
| ステップ 15 | <p>negotiation auto</p> <p>例 :</p> <pre>Device(config-if)# negotiation auto</pre> | <p>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。</p> |

| | コマンドまたはアクション | 目的 |
|---------|---|--|
| 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。 |
| ステップ 23 | ip route ip-address ip-mask subnet mask 例： | 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 |

| | コマンドまたはアクション | 目的 |
|---------|--|---|
| | Device (config) # <code>ip route vrf mgmt-vrf 192.168.0.1 255.255.0.0 192.168.255.1</code> | 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) # <code>logging host 172.25.33.20 vrf Mgmt-vrf</code> | 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) # <code>end</code> | グローバル コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。 |
| ステップ 26 | show ip http server session-module 例 : Device # <code>show ip http server session-module</code> | (必須) HTTP 接続を確認します。出力で、 <code>SL_HTTP</code> がアクティブであることを確認します。また、次のチェックも実行できます。 <ul style="list-style-type: none"> • CSLU がインストールされているデバイスから、製品インスタンスに ping できることを確認します。ping が成功すると、製品インスタンスが到達可能であることが確認されます • CSLU がインストールされているデバイスの Web ブラウザで、<code>https://<product-instance-ip>/</code> を確認します。これにより、CSLU から製品インスタンスへの REST API が期待どおりに動作することが保証されます。 |

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

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

始める前に

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

手順

-
- ステップ 1** SSM オンプレミスにログインし、[Smart Licensing] ワークスペースを選択します。
 - ステップ 2** [Inventory]>[SL Using Policy]>[Export/Import All]>[Import Product Instances List]に移動します。
[Upload Product Instances] ウィンドウが表示されます。
 - ステップ 3** [Download] をクリックして .csv テンプレートファイルをダウンロードし、テンプレート内のすべての製品インスタンスに必要な情報を入力します。
 - ステップ 4** テンプレートに入力したら、[Inventory]>[SL Using Policy]>[Export/Import All]>[Import Product Instances List] をクリックします。
[Upload Product Instances] ウィンドウが表示されます。
 - ステップ 5** [Browse] をクリックし、入力した .csv テンプレートをアップロードします。
アップロードしたすべての製品インスタンスのスマートアカウント情報とバーチャルアカウント情報が SSM オンプレミスで使用できるようになりました。
-

デバイスの検証 (SSM オンプレミス UI)

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

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

始める前に

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

手順

-
- ステップ 1** [On-Prem License Workspace] ウィンドウで、[Admin Workspace] をクリックし、プロンプトが表示されたらログインします。
[On-Prem Admin Workspace] ウィンドウが表示されます。
 - ステップ 2** [Settings] ウィジェットをクリックします。
[Settings] ウィンドウが表示されます。
 - ステップ 3** [CSLU] タブに移動し、[Validate Device] トグルスイッチをオンにします。

不明な製品インスタンスからの RUM レポートが拒否されるようになりました。必要な製品インスタンスを SSM オンプレミスデータベースにまだ追加していない場合は、RUM レポートを送信する前に追加する必要があります。スマートアカウントとバーチャルアカウントの割り当て (SSM オンプレミス UI) (83 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 <i>ip-address mask</i> 例： Device(config-if)# ip address 192.168.0.1 255.255.0.0 | VRF の IP アドレスを定義します。 |
| ステップ 6 | negotiation auto 例： Device(config-if)# negotiation auto | インターフェイスの速度およびデュプレックスパラメータの自動ネゴシエーション動作を有効にします。 |
| ステップ 7 | end 例： Device(config-if)# end | インターフェイス コンフィギュレーションモードを終了し、グローバルコンフィギュレーションモードを開始します。 |
| ステップ 8 | ip http client source-interface <i>interface-type-number</i> 例： Device(config)# ip http client source-interface gigabitethernet0/0 | HTTP クライアントのソース インターフェイスを設定します。 |
| ステップ 9 | ip route <i>ip-address ip-mask subnet mask</i> 例： Device(config)# ip route vrf 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 <i>server-address 1 ...server-address 6</i> 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 <i>interface-type-number</i> 例： Device(config)# ip domain lookup source-interface gigabitethernet0/0 | DNS ドメインルックアップ用のソース インターフェイスを設定します。 |
| ステップ 12 | ip domain name <i>domain-name</i> 例： Device(config)# ip domain name example.com | ドメインの DNS ディスカバリを設定します。この例では、ネームサーバがエントリ <code>cslu-local.example.com</code> 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ンスポイントを宣言するまで、製品インスタンスはトランスポイントを認識しません。 |
| ステップ 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 \(113 ページ\)](#) 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 へのデータまたは要求のアップロードとファイルのダウンロード \(111 ページ\)](#) 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一ユーザ ID とパスワードです ([SSM オンプレミス開始型通信のネットワーク到達可能性の確保 \(90 ページ\)](#))。
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 \(90 ページ\)](#))。
 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

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、アカウントینگ (AAA) アクセスコントロールモデルをイネーブルにします。 |
| ステップ 4 | aaa authentication login default local 例： Device(config)# aaa authentication login default local | (必須) 認証時にローカルのユーザ名データベースを使用するように、AAA 認証を設定します。 |
| ステップ 5 | aaa authorization exec default local 例： Device(config)# aaa authorization exec default local | ネットワークへのユーザアクセスを制限するパラメータを設定します。ユーザは EXEC シェルの実行が許可されます。 |
| ステップ 6 | ip routing 例： Device(config)# ip routing | IP ルーティングを有効にします。 |
| ステップ 7 | {ip ipv6} name-server server-address 1 ...server-address 6] 例： | (任意) 名前とアドレスの解決に使用する 1 つまたは複数のネームサーバのアドレスを指定します。 |

| | コマンドまたはアクション | 目的 |
|---------|--|---|
| | <pre>Device(config)# ip name-server vrf Mgmt-vrf 192.168.1.100 192.168.1.200 192.168.1.300</pre> | <p>最大6つのネームサーバを指定できます。各サーバアドレスはスペースで区切ります。最初に指定されたサーバが、プライマリサーバです。デバイスは、プライマリサーバへDNSクエリを最初に送信します。そのクエリが失敗した場合は、バックアップサーバにクエリが送信されます。</p> |
| ステップ 8 | <p>ip domain lookup source-interface interface-type-number</p> <p>例 :</p> <pre>Device(config)# ip domain lookup source-interface gigabitethernet0/0</pre> | <p>デバイス上で、DNSに基づくホスト名からアドレスへの変換を有効にします。この機能は、デフォルトでイネーブルにされています。</p> <p>ユーザのネットワークデバイスが、名前の割り当てを制御できないネットワーク内のデバイスと接続する必要がある場合、グローバルなインターネットのネーミング方式 (DNS) を使用して、ユーザのデバイスを一意に識別するデバイス名を動的に割り当てることができます。</p> |
| ステップ 9 | <p>ip domain name name</p> <p>例 :</p> <pre>Device(config)# ip domain name vrf Mgmt-vrf cisco.com</pre> | <p>非完全修飾ホスト名 (ドット付き10進表記ドメイン名のない名前) を完成させるためにソフトウェアが使用する、デフォルトのドメイン名を定義します。</p> |
| ステップ 10 | <p>no username name</p> <p>例 :</p> <pre>Device(config)# no username admin</pre> | <p>(必須) 指定されたユーザ名が存在する場合はクリアします。nameには、次のステップで作成するユーザ名と同じものを入力します。これにより、次のステップで作成するユーザ名が重複していないことが保証されます。</p> <p>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。</p> |

| | コマンドまたはアクション | 目的 |
|---------|--|---|
| ステップ 11 | <p>username name privilege level password password</p> <p>例 :</p> <pre>Device(config)# username admin privilege 15 password 0 lab</pre> | <p>(必須) ユーザ名をベースとした認証システムを構築します。</p> <p>privilege キーワードにより、ユーザの権限レベルを設定します。ユーザの権限レベルを指定する 0 ~ 15 の数字です。</p> <p>password を使用すると、name 引数にアクセスできます。パスワードは 1 ~ 25 文字で、埋め込みスペースを使用でき、username コマンドの最後のオプションとして指定します。</p> <p>これにより、SSM オンプレミスが製品インスタンスのネイティブ REST を使用できるようになります。</p> <p>(注) このユーザ名とパスワードを SSM オンプレミスに入力します (1 つ以上の製品インスタンスの追加 (SSM オンプレミス UI) (89 ページ))。これにより、SSM オンプレミスは製品インスタンスから RUM レポートを収集できるようになります。</p> |
| ステップ 12 | <p>interface interface-type-number</p> <p>例 :</p> <pre>Device (config)# interface gigabitethernet0/0</pre> | <p>インターフェイス コンフィギュレーションモードを開始し、VRF に関連付けられたイーサネットインターフェイス、サブインターフェイス、または VLAN を指定します。</p> |
| ステップ 13 | <p>vrf forwarding vrf-name</p> <p>例 :</p> <pre>Device (config-if)# vrf forwarding Mgmt-vrf</pre> | <p>VRF をレイヤ 3 インターフェイスに対応付けます。このコマンドは、インターフェイスでマルチプロトコル VRF をアクティブにします。</p> |
| ステップ 14 | <p>ip address ip-address mask</p> <p>例 :</p> <pre>Device (config-if)# ip address 192.168.0.1 255.255.0.0</pre> | <p>VRF の IP アドレスを定義します。</p> |

| | コマンドまたはアクション | 目的 |
|---------|---|---|
| ステップ 15 | negotiation auto 例： Device(config-if)# negotiation auto | インターフェイスの速度およびデュプレックスパラメータの自動ネゴシエーション動作を有効にします。 |
| ステップ 16 | no shutdown 例： Device(config-if)# no shutdown | 無効にされたインターフェイスを再起動します。 |
| ステップ 17 | end 例： Device(config-if)# end | インターフェイス コンフィギュレーションモードを終了し、グローバルコンフィギュレーションモードを開始します。 |
| ステップ 18 | ip http server 例： Device(config)# ip http server | (必須) シスコの Web ブラウザ ユーザ インターフェイスを含む IP または IPv6 システムで HTTP サーバを有効にします。HTTP サーバは、デフォルトにより標準のポート 80 を使用します。 |
| ステップ 19 | ip http authentication local 例： ip http authentication local Device(config)# | (必須) HTTP サーバユーザに対して特定の認証方法を指定します。 local キーワードは、認証および許可に、ローカルシステム設定で (username グローバルコンフィギュレーション コマンドによって) 指定したログイン ユーザ名、パスワード、権限レベル アクセスの組み合わせを使用することを示します。 |
| ステップ 20 | ip http secure-server 例： Device(config)# ip http server | (必須) セキュア HTTP (HTTPS) サーバを有効にします。HTTPS サーバは、セキュアソケットレイヤ (SSL) バージョン 3.0 プロトコルを使用します。 |
| ステップ 21 | ip http max-connections 例： Device(config)# ip http max-connections 16 | (必須) HTTP サーバへの同時最大接続数を設定します。1 ~ 16 の範囲の整数を入力します。デフォルトは 5 です。 |
| ステップ 22 | ip tftp source-interface interface-type-number 例： Device(config)# ip tftp source-interface GigabitEthernet0/0 | TFTP 接続用の送信元アドレスとして、インターフェイスの IP アドレスを指定します。 |

| | コマンドまたはアクション | 目的 |
|---------|---|--|
| ステップ 23 | ip route ip-address ip-mask subnet mask 例 : Device(config)# ip route vrf mgmt-vrf 192.168.0.1 255.255.0.0 192.168.255.1 | 製品インスタンスにルートとゲートウェイを設定します。スタティックルートまたはダイナミックルートのいずれかを設定できます。 |
| ステップ 24 | logging host 例 : Device(config)# logging host 172.25.33.20 vrf Mgmt-vrf | リモートホストへのシステムメッセージおよびデバッグ出力を記録します。 |
| ステップ 25 | crypto pki trustpoint SLA-TrustPoint 例 : Device(config)# crypto pki trustpoint SLA-TrustPoint Device(ca-trustpoint)# | (必須) 製品インスタンスがトランスポイント「SLA-TrustPoint」を使用する必要があることを宣言し、CA トランスポイント コンフィギュレーションモードを開始します。このコマンドを使用してトランスポイントを宣言するまで、製品インスタンスはトランスポイントを認識しません。 |
| ステップ 26 | enrollment terminal 例 : Device(ca-trustpoint)# enrollment terminal | (必須) 証明書登録方式を指定します。 |
| ステップ 27 | revocation-check none 例 : Device(ca-trustpoint)# revocation-check none | (必須) ピアの証明書が失効していないことを確認するために使用する方法を指定します。SSM オンプレミス展開トポロジの場合は、 none キーワードを入力します。つまり、失効チェックは実行されず、証明書は常に受け入れられます。 |
| ステップ 28 | end 例 : Device(ca-trustpoint)# exit Device(config)# end | CA トランスポイント コンフィギュレーションモードを終了し、次にグローバルコンフィギュレーションモードを終了してから、特権 EXEC モードに戻ります。 |
| 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 |
|---------|--|---|
| | | <ul style="list-style-type: none"> SSM オンプレミスがインストールされているデバイスから、製品インスタンスに ping できることを確認します。ping が成功すると、製品インスタンスが到達可能であることが確認されます SSM オンプレミスがインストールされているデバイスの Web ブラウザで、 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。 |

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： | 名前とアドレスの解決に使用する 1 つまたは複数のネームサーバのアドレスを指定します。 |

| | コマンドまたはアクション | 目的 |
|-------|---|--|
| | <pre>Device(config)# ip name-server 209.165.201.1 209.165.200.225 209.165.201.14 209.165.200.230</pre> | <p>最大6つのネームサーバを指定できます。各サーバアドレスはスペースで区切ります。最初に指定されたサーバが、プライマリサーバです。デバイスは、プライマリサーバへDNSクエリを最初に送信します。そのクエリが失敗した場合は、バックアップサーバにクエリが送信されます。</p> |
| ステップ4 | <p>ip name-server vrf Mgmt-vrf <i>server-address 1...server-address 6</i></p> <p>例 :</p> <pre>Device(config)# ip name-server vrf Mgmt-vrf 209.165.201.1 209.165.200.225 209.165.201.14 209.165.200.230</pre> | <p>(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。</p> <p>(注) このコマンドは、ip name-server コマンドの代わりです。</p> |
| ステップ5 | <p>ip domain lookup source-interface <i>interface-type interface-number</i></p> <p>例 :</p> <pre>Device(config)# ip domain lookup source-interface Vlan100</pre> | <p>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。</p> |
| ステップ6 | <p>ip domain name <i>domain-name</i></p> <p>例 :</p> <pre>Device(config)# ip domain name example.com</pre> | <p>ドメイン名を設定します。</p> |
| ステップ7 | <p>ip host tools.cisco.com <i>ip-address</i></p> <p>例 :</p> <pre>Device(config)# ip host tools.cisco.com 209.165.201.30</pre> | <p>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。</p> |
| ステップ8 | <p>interface <i>interface-type-number</i></p> <p>例 :</p> <pre>Device(config)# interface Vlan100 Device(config-if)# ip address 192.0.2.10 255.255.255.0 Device(config-if)# exit</pre> | <p>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。</p> |
| ステップ9 | <p>ntp server <i>ip-address</i> [version number] [key key-id] [prefer]</p> <p>例 :</p> <pre>Device(config)# ntp server 198.51.100.100 version 2 prefer</pre> | <p>(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</p> |

| | コマンドまたはアクション | 目的 |
|---------|---|---|
| | | <p>り、デバイスの時刻が CSSM と同期されます。</p> <p>このコマンドを複数回使用する必要があるために優先サーバを設定する場合は、prefer キーワードを使用します。このキーワードを使用すると、サーバ間の切り換え回数が減少します。</p> |
| ステップ 10 | <p>switchport access vlan <i>vlan_id</i></p> <p>例 :</p> <pre>Device(config)# interface GigabitEthernet1/0/1 Device(config-if)# switchport access vlan 100 Device(config-if)# switchport mode access Device(config-if)# exit OR Device(config)#</pre> | <p>このアクセスポートがトラフィックを伝送する VLAN を有効にし、非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。</p> <p>(注) このステップは、スイッチポート アクセス モードが必要な場合にのみ設定します。switchport access vlan コマンドは、たとえば Catalyst スイッチング製品インスタンスに適用できます。ルーティング製品インスタンスの場合は、代わりに ip address ip-address mask コマンドを設定できます。</p> |
| ステップ 11 | <p>ip route <i>ip-address ip-mask subnet mask</i></p> <p>例 :</p> <pre>Device(config)# ip route 192.0.2.0 255.255.255.255 192.0.2.1</pre> | <p>デバイスにルートを設定します。スタティックルートまたはダイナミックルートのいずれかを設定できます。</p> |
| ステップ 12 | <p>ip http client source-interface <i>interface-type-number</i></p> <p>例 :</p> <pre>Device(config)# ip http client source-interface Vlan100</pre> | <p>(必須) HTTP クライアントのソースインターフェイスを設定します。インターフェイスのタイプと番号、または VLAN を入力します。</p> |
| ステップ 13 | <p>exit</p> <p>例 :</p> <pre>Device(config)# exit</pre> | <p>グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。</p> |
| ステップ 14 | <p>copy running-config startup-config</p> <p>例 :</p> | <p>コンフィギュレーションファイルに設定を保存します。</p> |

| | コマンドまたはアクション | 目的 |
|--|---|----|
| | Device# <code>copy running-config startup-config</code> | |

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。

手順

| | コマンドまたはアクション | 目的 |
|--------|---|---|
| ステップ 1 | enable 例： Device> <code>enable</code> | 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# <code>configure terminal</code> | 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)# <code>license smart transport smart</code> | 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)# <code>license smart transport default</code> | 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 <code>smart</code> 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)# <code>license smart proxy address 192.168.0.1</code> Device (config)# <code>license smart proxy port 3128</code> | 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。 <ul style="list-style-type: none"> • address address_hostname : プロキシアドレスを指定します。プロキシサーバの IP アドレスまたはホスト名を入力します。 |

| | コマンドまたはアクション | 目的 |
|--|--------------|--|
| | | <ul style="list-style-type: none"> • port_num : プロキシポートを指定します。プロキシポート番号を入力します。 <p>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、<code>status-line = HTTP-version SP status-code SP reason-phrase CRLF</code> 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。</p> |

ダイレクトクラウドアクセス用の Call Home サービスの設定

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



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

手順

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

| | コマンドまたはアクション | 目的 |
|--------|---|---|
| ステップ 4 | license smart url <i>url</i> 例 : Device (config) # license smart url <code>https://tools.cisco.com/its/service/cthe/services/DCEService</code> | 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 | no http secure server-identity-check 例 : Device (config-call-home) # no http secure server-identity-check | HTTP 接続の確立時のサーバー ID チェックを無効にします。 |
| ステップ 8 | contact-email-address <i>email-address</i> 例 : Device (config-call-home) # contact-email-addr <code>username@example.com</code> | 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 9 | profile <i>name</i> 例 : Device (config-call-home) # profile CiscoTAC-1 Device (config-call-home-profile) # | 指定された宛先プロファイルに対する Call Home 宛先プロファイル設定サブモードに入ります。 デフォルトは次のとおりです。 <ul style="list-style-type: none"> • CiscoTAC-1 プロファイルは非アクティブです。このプロファイルを使用するには、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、 |

| | コマンドまたはアクション | 目的 |
|---------|---|---|
| | | <p>Device(cfg-call-home-profile)# anonymous-reporting-only anonymous-reporting-only を追加で 設定します。これが設定されてい る場合は、クラッシュ、インベン トリ、およびテストメッセージの みが送信されます。</p> <p>プロファイルのステータスを確認する には、show call-home profile all コマ ンドを使用します。</p> |
| ステップ 10 | <p>active</p> <p>例： Device(config-call-home-profile)# active</p> | 宛先プロファイルをイネーブルにしま す。 |
| ステップ 11 | <p>destination transport-method http {email http}</p> <p>例： Device(config-call-home-profile)# destination transport-method http AND Device(config-call-home-profile)# no destination transport-method email</p> | <p>メッセージの転送形式をイネーブルに します。この例では、HTTP 経由で Call Home サービスが有効になり、電子メー ルによる転送が無効になります。</p> <p>このコマンドの no 形式を使用すると、 メソッドが無効になります。</p> |
| ステップ 12 | <p>destination address { email email_address http url}</p> <p>例： Device(config-call-home-profile)# destination address http https://tools.cisco.com/its/service/odte/services/DOService AND Device(config-call-home-profile)# no destination address http https://tools.cisco.com/its/service/odte/services/DOService</p> | <p>Call Home メッセージを送信する宛先 E メールアドレスまたは URL を設定 します。宛先 URL を入力する場合は、 サーバがセキュアサーバであるかどう かに応じて http:// (デフォルト) また は https:// を指定します。</p> <p>ここに示す例では、http:// の形式で宛 先 URL が設定されています。コマンド の no 形式では https:// に設定されます。</p> |
| ステップ 13 | <p>exit</p> <p>例： Device(config-call-home-profile)# exit</p> | 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 14 | <p>exit</p> <p>例： Device(config-call-home)# end</p> | 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。 |

| | コマンドまたはアクション | 目的 |
|---------|--|---|
| ステップ 15 | copy running-config startup-config 例： Device# copy running-config startup-config | コンフィギュレーションファイルに設定を保存します。 |
| ステップ 16 | 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。 |

| | コマンドまたはアクション | 目的 |
|--------|---|--|
| ステップ 4 | service call-home 例： Device(config)# service call-home | Call Home 機能をイネーブルにします。 |
| ステップ 5 | call-home 例： Device(config)# call-home | Call Home コンフィギュレーションモードを開始します。 |
| ステップ 6 | http-proxy proxy-address proxy-port port-number 例： Device(config-call-home)# http-proxy 198.51.100.10 port 5000 | Call Home サービスへのプロキシサーバ情報を設定します。 Cisco IOS XE Bengaluru 17.6.1 以降、プロキシサーバの受け入れ基準が変更されたことに注意してください。プロキシサーバの応答のステータスコードのみがシステムによって検証され、理由フレーズは検証されません。RFC形式は、 status-line = HTTP-version SP status-code SP reason-phrase CRLF です。ステータス行の詳細については、 RFC 7230 のセクション 3.1.2を参照してください。 |
| ステップ 7 | exit 例： Device(config-call-home)# exit | Call Home コンフィギュレーションモードを終了し、グローバルコンフィギュレーションモードを開始します。 |
| ステップ 8 | exit 例： Device(config)# exit | グローバルコンフィギュレーションモードを終了し、特権 EXEC モードを開始します。 |
| ステップ 9 | copy running-config startup-config 例： Device# copy running-config startup-config | コンフィギュレーションファイルに設定を保存します。 |

承認コードの削除と返却

SLR 承認コードを削除して返却するには、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：すべて

手順

| | コマンドまたはアクション | 目的 |
|--------|--|---|
| ステップ 1 | <p>enable</p> <p>例 :</p> <pre>Device> enable</pre> | <p>特権 EXEC モードを有効にします。プロンプトが表示されたらパスワードを入力します。</p> |
| ステップ 2 | <p>show license summary</p> <p>例 :</p> <pre>Device# show license summary</pre> | <p>削除して返却するライセンスが使用中でないことを確認します。使用中の場合は、まず機能を無効にする必要があります。</p> |
| ステップ 3 | <p>license smart authorization return {all local} {offline [path] online}</p> <p>例 :</p> <pre>Device# license smart authorization return all online</pre> <p>Enter this return code in Cisco Smart Software Manager portal: UDI: PID:C9800-CL-K9,SN:93BBAH93MGS Return code: CqaUPW-WSPYiq-ZNU2ci-SnWydS-hBCXHP-MuyPqy-PJ1GiG-tPTGQj-S2h UDI: PID:C9800-CL-K9,SN:9XECPSUU4XN Return code: CNLwxR-eWiAEJ-XaTEQg-j4rrYW-dSRz9j-37VpcP-imjuLD-mNeA4k-TXA</p> <p>OR</p> <pre>Device# license smart authorization return local offline</pre> <p>Enter this return code in Cisco Smart Software Manager portal: UDI: PID:C9800-CL-K9,SN:93BBAH93MGS Return code: CqaUPW-WSPYiq-ZNU2ci-SnWydS-hBCXHP-MuyPqy-PJ1GiG-tPTGQj-S2h UDI: PID:C9800-CL-K9,SN:9XECPSUU4XN Return code: CNLwxR-eWiAEJ-XaTEQg-j4rrYW-dSRz9j-37VpcP-imjuLD-mNeA4k-TXA</p> <p>OR</p> <pre>Device# license smart authorization return local offline bootflash:return-code.txt</pre> | <p>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。</p> <p>製品インスタンスを指定します。</p> <ul style="list-style-type: none"> • all : 高可用性セットアップで接続されたすべての製品インスタンスに対してアクションを実行します。 • local : アクティブな製品インスタンスに対してアクションを実行します。これがデフォルトのオプションです。 <p>CSSM に接続しているかどうかを指定します。</p> <ul style="list-style-type: none"> • CSSM に接続している場合は、online を入力します。コードは自動的に CSSM に返却され、確認が返されて製品インスタンスにインストールされます。このオプションを選択すると、戻りコードが自動的に CSSM に送信されます。 • CSSM に接続していない場合は、offline[path] を入力します。 <p>offline キーワードのみを入力する場合は、CLI に表示されるリターンコードをコピーして、CSSM に入力する必要があります。</p> <p>ファイル名とパスを指定すると、リターンコードは指定した場所に保存されます。ファイル形式は、読み取</p> |

| | コマンドまたはアクション | 目的 |
|--------|--|---|
| | | <p>り可能な任意の形式にすることができます。例：Device# license smart authorization return local offline bootflash:return-code.txt.</p> <p>ソフトウェアバージョン Cisco IOS XE Cupertino 17.7.1 以降では、返却要求をファイルに保存した後、RUM レポートをアップロードする場合と同じ場所に、同じ方法でファイルを CSSM にアップロードできます。 CSSM へのデータまたは要求のアップロードとファイルのダウンロード (111 ページ)</p> <p>CSSM にリターンコードを入力するには、次のタスクを実行します。 CSSM からの製品インスタンスの削除 (107 ページ) この手順を完了してから、次の手順に進みます。</p> |
| ステップ 4 | 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 5 | no license smart reservation 例： Device(config)# no license smart reservation | <p>製品インスタンスの SLR 設定を無効にします。</p> <p>この手順で no license smart reservation コマンドを入力する前に、上記の手順3で (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。</p> |
| ステップ 6 | exit 例： Device(config)# exit | 特権 EXEC モードに戻ります。 |
| ステップ 7 | show license all 例： Device# show license all <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 |

| | コマンドまたはアクション | 目的 |
|--|---|--|
| | <pre>License Authorizations ===== Overall status: Active: PID:C9800-CL-K9,SN:93BBAH93MGS Status: NOT INSTALLED Last return code: CpLEW5P1q-2N2ci-SWyc-HCXHP-MYFoy-RJGIG-tPQj-SZh Standby: PID:C9800-CL-K9,SN:9XECPSUU4XN Status: NOT INSTALLED Last return code: QNwR-dvAEJ-YaTEG-j4mW-dRz9j-37pCP-imjuLD-mN4k-TVA <output truncated></pre> | <p>と、Last return code: フィールドに戻りコードが表示されます。</p> |

CSSM からの製品インスタンスの削除

製品インスタンスを削除し、すべてのライセンスをライセンスプールに戻すには、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

予約済みライセンス (SLR) を使用している製品インスタンスを削除する場合は、[承認コードの削除と返却 \(104 ページ\)](#) に示されているとおり、リターン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、[Smart Software Licensing] をクリックします。
シスコから提供されたユーザ名とパスワードを使用してログインします。
- ステップ 2 [Inventory] タブをクリックします。
- ステップ 3 [Virtual Account] ドロップダウンリストから、バーチャルアカウントを選択します。
- ステップ 4 [Product Instances] タブをクリックします。
使用可能な製品インスタンスのリストが表示されます。
- ステップ 5 製品インスタンスリストから必要な製品インスタンスを見つけます。オプションで、検索タブに名前または製品タイプの文字列を入力して、製品インスタンスを検索できます。
- ステップ 6 削除する製品インスタンスの [Actions] 列で、[Remove] リンクをクリックします。
 - 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、[Smart Software Licensing] をクリックします。
- シスコから提供されたユーザ名とパスワードを使用してログインします。
- ステップ 2** [Inventory] タブをクリックします。
- ステップ 3** [Virtual Account] ドロップダウンリストから、必要なバーチャルアカウントを選択します。
- ステップ 4** [General] タブをクリックします。
- ステップ 5** [New Token] をクリックします。[Create Registration Token] ウィンドウが表示されます。
- ステップ 6** [Description] フィールドに、トークンの説明を入力します。
- ステップ 7** [Expire After] フィールドに、トークンをアクティブにする必要がある日数を入力します。
- ステップ 8** (オプション) [Max. Number of Uses] フィールドに、トークンの有効期限が切れるまでの最大使用回数を入力します。
- ステップ 9** [Create Token] をクリックします。
- ステップ 10** リストに新しいトークンが表示されます。[Actions] をクリックし、トークンを .txt ファイルとしてダウンロードします。
-

信頼コードのインストール

信頼コードを手動でインストールするには、次の手順を実行します。

始める前に

サポートされるトポロジ:

- CSSM に直接接続

手順

| | コマンドまたはアクション | 目的 |
|--------|--|--|
| ステップ 1 | CSSMからの信頼コード用新規トークンの生成 (108 ページ) | まだ CSSM から信頼コードファイルを生成してダウンロードしていない場合は、生成とダウンロードを実行します。 |
| ステップ 2 | enable 例： Device> enable | 特権 EXEC モードを有効にします。プロンプトが表示されたら、パスワードを入力します。 |
| ステップ 3 | license smart trust idtoken <i>id_token_value</i> { local all } [force] 例： Device# license smart trust idtoken NGMwMjk5mYtNZaxMS00NzZmtgWm all force | <p>CSSM との信頼できる接続を確立できません。 <i>id_token_value</i> には、CSSM で生成したトークンを入力します。</p> <p>次のいずれかのオプションを入力します。</p> <ul style="list-style-type: none"> • local : 高可用性セットアップのアクティブデバイスに対してのみ信頼要求を送信します。これがデフォルトのオプションです。 • all : 高可用性セットアップのすべてのデバイスに対して信頼要求を送信します。 <p>製品インスタンスに既存の信頼コードがあるにもかかわらず、信頼コード要求を送信するには、force キーワードを入力します。</p> <p>信頼コードは、製品インスタンスのUDIにノードロックされます。UDI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、</p> |

| | コマンドまたはアクション | 目的 |
|--------|---|---|
| | | 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 : <pre><output truncated> Trust Code Installed: Active: PID:C9800-CL-K9,SN:93BBAH93MGS INSTALLED on Nov 02 08:59:26 2020 IST Standby: PID:C9800-CL-K9,SN:9XECPSUU4XN INSTALLED on Nov 02 09:00:45 2020 IST</pre> | 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、[Smart Software Licensing] をクリックします。

シスコから提供されたユーザ名とパスワードを使用してログインします。

ステップ 2 次のディレクトリパス、[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 \(112 ページ\)](#) を参照してください

CSSM へのデータまたは要求のアップロードとファイルのダウンロード

このタスクは、次の目的で使用できます。

- RUM レポートを CSSM にアップロードし、ACK をダウンロードします。
- SLAC または SLR 承認コードの返却要求をアップロードします。

これは、CSSM への接続なし、CSLU なしのトポロジにのみ適用され、Cisco IOS XE cupertino 17.7.1 以降でサポートされています。

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

始める前に

サポートされるトポロジ：

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

手順

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

シスコから提供されたユーザ名とパスワードを使用してログインします。

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

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

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

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

使用状況レポートは、アップロード後に CSSM で削除できません。

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

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

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

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

製品インスタンスが CSSM や CSLU に接続されていない場合に、製品インスタンスに SLAC、ポリシー、または ACK をインストールするには、次のタスクを実行します。

始める前に

サポートされるトポロジ：CSSM への接続なし、CSLU なし

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

- ポリシーの場合の参照：[CSSM からのポリシーファイルのダウンロード \(110 ページ\)](#)
- ACK の場合の参照：[CSSM へのデータまたは要求のアップロードとファイルのダウンロード \(111 ページ\)](#)

手順

| | コマンドまたはアクション | 目的 |
|--------|---|--|
| ステップ 1 | enable 例： Device> enable | 特権 EXEC モードを有効にします。プロンプトが表示されたら、パスワードを入力します。 |
| ステップ 2 | copy source bootflash:file-name 例： Device# copy tftp://10.8.0.6/example.txt bootflash: | ファイルをソースの場所またはディレクトリから製品インスタンスのフラッシュメモリにコピーします。 <ul style="list-style-type: none"> • source：これは、コピー元となるファイルまたはディレクトリの場所です。コピー元は、ローカルまたはリモートのいずれかです。 • bootflash：これはブートフラッシュメモリの場合の宛先です。 |
| ステップ 3 | license smart import bootflash: file-name 例： Device# license smart import bootflash:example.txt | ファイルを製品インスタンスにインポートしてインストールします。インストール後、インストールしたファイルのタイ |

| | コマンドまたはアクション | 目的 |
|--------|--|--|
| | | プを示すシステムメッセージが表示されます。 |
| ステップ 4 | show license all 例： Device# show license all | 製品インスタンスのライセンス承認、ポリシー、およびレポート情報を表示します。 |

転送タイプ、URL、およびレポート間隔の設定

製品インスタンスの転送モードを設定するには、次のタスクを実行します。

始める前に

サポートされるトポロジ：すべて

手順

| | コマンドまたはアクション | 目的 |
|--------|--|---|
| ステップ 1 | enable 例： Device> enable | 特権 EXEC モードを有効にします。プロンプトが表示されたらパスワードを入力します。 |
| ステップ 2 | configure terminal 例： Device# configure terminal | |
| ステップ 3 | license smart transport{automatic callhome cslu off smart} 例： Device(config)# license smart transport cslu | 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。 <ul style="list-style-type: none"> • automatic：転送モード cslu を設定します。 • callhome：転送モードとして Call Home を有効にします。 • cslu：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。 <p>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</p> |

| | コマンドまたはアクション | 目的 |
|----------------------|--|---|
| | | <p>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。</p> <ul style="list-style-type: none"> • 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。 |
| <p>ステップ 4</p> | <p>license smart url {url cslu cslu_or_on-prem_url default smart smart url url smart url url}</p> <p>例 :</p> <pre>Device(config)# license smart url cslu http://192.168.0.1:8182/cslu/v1/pi</pre> | <p>設定された転送モードの URL を設定します。前のステップで選択した転送モードに応じて、対応する URL をここで設定します。</p> <ul style="list-style-type: none"> • url : 転送モードとして callhome を設定している場合は、このオプションを設定します。CSSM URL を次のように正確に入力します。 https://software.cisco.com/#module/SmartLicensing • 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。 <ul style="list-style-type: none"> • CSLU を使用している場合は、次のように URL を入力します。 <code>http://<cslu_ip_or_host>:8182/cslu/v1/pi</code> <p><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。</p> • no license smart url cslu cslu_url コマンドは <code>http://cslu-local:8182/cslu/v1/pi</code> に戻ります |

| | コマンドまたはアクション | 目的 |
|--|--------------|---|
| | | <ul style="list-style-type: none"> 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。 <pre>http://<ip>/cslu/v1/pi/<tenant ID></pre> <ip> には、SSM オンプレミスをインストールしたサーバのホスト名または IP アドレスを入力します。<tenantID> はデフォルトのローカル バーチャルアカウント ID にする必要があります。 <p>ヒント SSM オンプレミスから URL 全体を取得できます。「トランスポート URL の取得 (SSM オンプレミス UI) (87 ページ)」を参照してください</p> <p>no license smart url cslu cslu_url コマンドは <pre>http://cslu-local:8182/cslu/v1/pi</pre> に戻ります</p> <ul style="list-style-type: none"> default : 設定されている転送モードによって異なります。このオプションでは、smart および cslu 転送モードのみがサポートされます。 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)。 <ul style="list-style-type: none"> smart smart_url : 転送タイプとして smart を設定している場合は、この |

| | コマンドまたはアクション | 目的 |
|--------|---|---|
| | | <p>オプションを設定します。URL を次のように正確に入力します。</p> <p><code>https://smartreceiver.cisco.com/licservice/license</code></p> <p>このオプションを設定すると、システムは license smart url url で自動的に URL の複製を作成します。重複するエントリは無視できます。これ以上の操作は必要ありません。</p> <p>no license smart url smartsmart_url コマンドは、デフォルトの URL に戻ります。</p> <ul style="list-style-type: none"> • utility smart_url : このオプションは CLI では使用できませんがサポートされていません。 |
| ステップ 5 | <p>license smart usage interval interval_in_days</p> <p>例 :</p> <pre>Device(config)# license smart usage interval 40</pre> | <p>(任意) レポート間隔の日数を設定します。デフォルトでは、RUM レポートは 30 日ごとに送信されます。有効な値の範囲は 1 ~ 3650 です。</p> <p>間隔を設定しない場合、レポート間隔はポリシーの値のみで決まります。</p> |
| ステップ 6 | <p>exit</p> <p>例 :</p> <pre>Device(config)# exit</pre> | <p>グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。</p> |
| ステップ 7 | <p>copy running-config startup-config</p> <p>例 :</p> <pre>Device# copy running-config startup-config</pre> | <p>コンフィギュレーション ファイルに設定を保存します。</p> |

AIR ライセンスの設定

ポリシーを使用したスマートライセンシング環境では、このタスクを使用して、ライセンスを変更したり、製品インスタンスで使用されているライセンスを変更したり、製品インスタンスでアドオンライセンスを追加設定したりできます。たとえば、現在 AIR Network Advantage を使用しており、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場合は、このタスクを使用して同じ機能を設定できます。また、アドオンライセンスを使用しない場合などは、AIR Network Advantage ライセンスのみを使用するようにこのコマンドを再設定します。

使用可能なライセンスに関する情報は、スマートアカウントまたはバーチャルアカウントで確認できます。使用可能なライセンスは、次のいずれかです。

- AIR Network Essential
- AIR Network Advantage
- AIR DNA Essential
- AIR DNA Advantage

Cisco IOS XE Bengaluru 17.4.1 以降、EWC-AP の場合のみ、AIR DNA ライセンスの購入をオプトアウトできます。AIR DNA ライセンスをオプトアウトするオプションは、[Cisco Commerce](#) ポータルからのみ利用できます。オプトアウトすると、ポリシーを使用したスマートライセンス機能が無効になります。

新しい製品インスタンスの場合、次のことを意味します。

| 条件 | 必須のアクション | 結果 |
|------------------------|---|--|
| AIR DNA ライセンスをオプトアウトする | なし。 | AIR Network Essentials のみを使用します。 ポリシーを使用したスマートライセンス機能は、製品インスタンス、および CSSM のスマートアカウントとバーチャルアカウントで無効になっています。ライセンスの使用状況は記録されず、レポート要件も適用されません。 |
| AIR DNA ライセンスを購入する | グローバルコンフィギュレーションモードで <code>license air level</code> コマンドを入力し、対応する AIR DNA ライセンスを設定します。対応するライセンスを使用するには、リロードします。 サポートされているトポロジのいずれかを実装し、レポート要件を満たします。トポロジの実装については、このドキュメントの「 サポートされるトポロジ 」セクションを参照してください。 | 購入した AIR DNA および AIR Network ライセンスを使用します。 ポリシーを使用したスマートライセンス機能は、製品インスタンス、および CSSM のスマートアカウントとバーチャルアカウントで有効になっています。 |

既存の製品インスタンスの場合、次のことを意味します。

| 条件 | 必須のアクション | 結果 |
|--------------------------|---|--|
| AIR DNA ライセンスを使用している | なし。 | 変化なし すでにポリシーを使用したスマートライセンシング環境にいます。 |
| 期間満了時に DNA ライセンスを更新したくない | 期限満了時に、グローバル コンフィギュレーション モードで license air level コマンドを入力し、AIR Network Essentials または AIR Network Advantage を設定します。対応するライセンスを使用するには、リロードします。 | AIR DNA Essentials を使用していた場合は、AIR Network Essentials を使用します。 AIR DNA Advantage を使用していた場合は、AIR Network Advantage を使用します。 ポリシーを使用したスマートライセンシング機能は、製品インスタンス、および CSSM のスマートアカウントとバーチャルアカウントで無効になっています。ライセンスの使用状況は記録されず、レポート要件も適用されません。 |

使用中ライセンスを設定または変更するには、次の手順に従います。

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 モードをイネーブルにします。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 air level {air-network-advantage [addon air-dna-advantage] air-network-essentials [addon air-dna-essentials] } 例： Device(config)# license air level air-network-essentials addon air-dna-essentials | 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、製品インスタンスにより、リロード後に AIR DNA Essentials（および AIR Network Essentials）ライセンスがアクティブ化されます。 |

| | コマンドまたはアクション | 目的 |
|--------|--|---|
| | | (注) Cisco IOS XE Bengaluru 17.4.1 より前では、EWC-AP のデフォルトは AIR DNA Essentials でした。17.4.1 以降のデフォルトは AIR Network Essentials です。 |
| ステップ 4 | exit 例： Device(config)# exit | 特権 EXEC モードに戻ります。 |
| ステップ 5 | copy running-config startup-config 例： Device# copy running-config startup-config | 設定変更を保存します。 |
| ステップ 6 | reload 例： Device# reload | デバイスがリロードされます。 |
| ステップ 7 | show version 例： Device# show version Cisco IOS XE Software, Version 17.03.02 Cisco IOS Software [Amsterdam], C9800-CL Software (C9800-CL-K9_IOSXE), Version 17.3.2, RELEASE SOFTWARE <output truncated> AIR License Level: AIR DNA Essentials Next reload AIR license Level: AIR DNA Essentials Smart Licensing Status: Registration Not Applicable/Not Applicable <output truncated> | 現在使用しているライセンスと次回のリロード時に有効なライセンス情報を表示します。 |

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

ポリシーを使用したスマートライセンスのトラブルシューティング

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スに関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 9: 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 10: 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。

- %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
- %IOSXE_RP_EWLC_NOT-2-MSGDEVICENOTREG
- %CAPWAPAC_TRACE_MSG-3-MAX_LICENSE_AP_LIMIT_REACHED

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。



(注) デバイスには、有効なクロックと NTP 設定が必要です。

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].
```

このメッセージは、Cisco Catalyst アクセス、コア、およびアグリゲーションスイッチには該当しません。これらの製品インスタンスには輸出規制ライセンスや適用ライセンスがないためです。

```
-----
-----
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 番目の [chars] はエラーの詳細を示すエラー文字列です。このメッセージは、失敗した通信の試行ごとに表示されます。

失敗の理由として次が考えられます。

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

正インスタンスが RUM レポートの送信を開始するトポロジ（CSLU を介して CSSM に接続：製品インスタンス開始型通信、CSSM から切断されている CSSM、CSLU への直接接続：製品インスタンス開始型通信、および SSM オンプレミス展開：製品インスタンス開始型通信）では、この通信障害メッセージがスケジュールされたレポート（**license smart usage interval interval_in_days** グローバル コンフィギュレーション コマンド）と一致している場合は、製品インスタンスはスケジュールされた時間が経過した後、最大 4 時間にわたって RUM レポートを送信しようとします。（通信障害が続くために）それでもレポートを送信できない場合、システムは間隔を 15 分にリセットします。通信障害が解消されると、レポート間隔は最後に設定された値に戻ります。

推奨するアクション：

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

CSSM 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 \(79 ページ\)](#) 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 \(SSM オンプレミス UI\) \(87 ページ\)](#)）、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 \(85 ページ\)](#) で説明されているよおりに、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 \(90 ページ\)](#) 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
```

前述の手順を実行しても、ポリシーのインストールが失敗する場合は、シスコのテクニカルサポート担当者にお問い合わせください。

```
-----
-----
Error Message %SMART_LIC-3-COMM_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 \(108 ページ\)](#) および [信頼コードのインストール \(109 ページ\)](#) 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 \(CSLU インターフェイス\) \(78 ページ\)](#) > [CSSM へのデータまたは要求のアップロードとファイルのダウンロード \(111 ページ\)](#) > [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 \(CSLU インターフェイス\) \(78 ページ\)](#) > [CSSM へのデータまたは要求のアップロードとファイルのダウンロード](#)

[ド \(111 ページ\)](#) > [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を実行します。 [CSSM からのポリシーファイルのダウンロード \(110 ページ\)](#)

次に、製品インスタンスで次のタスクを実行します。 [製品インスタンスへのファイルのインストール \(112 ページ\)](#)

- SSM オンプレミス展開

- 製品インスタンス開始型通信の場合は、特権 EXEC モードで **license smart sync** コマンドを入力します。製品インスタンスを SSM オンプレミスと同期させ、必要な情報または欠落している情報を復元する原因です。必要に応じて、SSM オンプレミスと CSSM を同期します。

- SSM オンプレミス開始型通信の場合：SSM オンプレミス UI で、[Reports] > [Synchronization pull schedule] > [Synchronize now with the device] に移動します。

SSM オンプレミス展開の両方の通信形式で、次のいずれかのオプションを使用して CSSM と同期します。

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

- SSM オンプレミスが CSSM に接続されていません。 [使用状況データのエクスポートとインポート \(SSM オンプレミス UI\)](#) (88 ページ)

```
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、インストールは失敗します。
- スマートアカウントとバーチャルアカウントの不一致：これは、(トークン ID が生成された) スマートアカウントまたはバーチャルアカウントに、信頼コードをインストールした製品インスタンスが含まれていないことを意味します。CSSM で生成されたトークン

は、スマートアカウントまたはバーチャルアカウントレベルで適用され、そのアカウントのすべての製品インスタンスにのみ適用されます。

- 署名の不一致：これは、システムクロックが正確でないことを意味します。
- タイムスタンプの不一致：製品インスタンスの時刻が CSSM と同期していないため、インストールが失敗する可能性があります。

推奨するアクション：

- 信頼コードはすでにインストールされています。製品インスタンスに信頼コードがすでに存在する状態で信頼コードをインストールする場合は、特権 EXEC モードで **license smart trust idtoken id_token_value {local|all} [force]** コマンドを再設定します。再設定の際、**force** キーワードを必ず含めてください。**force** キーワードを入力すると、CSSM に送信されるメッセージに強制フラグが設定され、すでに存在する場合でも新しい信頼コードが作成されます。

- スマートアカウントとバーチャルアカウントの不一致：

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

トークンを生成する製品インスタンスが、選択したバーチャルアカウントにリストされているかどうかを確認します。リストされている場合は、次のステップに進みます。リストされていない場合は、正しいスマートアカウントとバーチャルアカウントを確認して選択します。その後、次のタスクを再度実行します。[CSSMからの信頼コード用新規トークンの生成 \(108 ページ\)](#) および [信頼コードのインストール \(109 ページ\)](#)

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

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

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

説明：Cisco Smart Software Manager オンプレミス（旧称 Cisco Smart Software Manager サテライト）は、Cisco IOS XE Amsterdam 17.3.3 以降でのみ Smart Licensing Using Policy 環境でサポートされています（[SSM オンプレミス \(6 ページ\)](#) 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 (13 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].
```

このメッセージは、Cisco Catalyst アクセス、コア、およびアグリゲーションスイッチには該当しません。これらの製品インスタンスには輸出規制ライセンスや適用ライセンスがないためです。

```
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 \(CSLU インターフェイス\) \(78 ページ\)](#)、[CSSM へのデータまたは要求のアップロードとファイルのダウンロード \(111 ページ\)](#)、[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 へのデータまたは要求のアップロードとファイルのダウンロード \(111 ページ\)](#) > [製品インスタンスへのファイルのインストール \(112 ページ\)](#)
- 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）](#)（88 ページ）

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

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

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

```
Error Message %IOSXE_RP_EWLC_NOT-2-MSGDEVICENOTREG: Unregistered 9800-CL can only
be used in lab. For production usage, please register this device in [int] days. Failure
to do so
will result in a limited number [50] of Access Points being allowed post this.
```

説明：この製品インスタンスには ACK が必要です。[int] は、製品インスタンスに ACK をインストールするための残り時間です。

このシステムメッセージは、製品インスタンスで最初の ACK が使用可能になるまで、1 日 1 回表示されます。

推奨するアクション：

サポートされているトポロジの 1 つを実装し、完全な使用状況レポートを作成します。RUM レポートを CSSM と ACK のインストールに送信するために使用できる方法は、実装するトポロジによって異なります。[サポートされるトポロジ（13 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（33 ページ）](#) を参照してください。

```
Error Message %CAPWAPAC_TRACE_MSG-3-MAX_LICENSE_AP_LIMIT_REACHED: Chassis 1 R0/0:
wncmgrd: Ap MAC: [enet] is not allowed to join. Please start reporting licensing to Cisco
to get the
ACK for resumption of usual operation.
```

説明：この製品インスタンスの ACK の期限は過ぎましたが、ACK はまだインストールされていません。[enet] は、Cisco Catalyst 9800-CL ワイヤレスコントローラに接続しようとしている AP の MAC アドレスですが、必要な ACK がインストールされていないため許可されません。

推奨するアクション：

サポートされているトポロジの 1 つを実装し、完全な使用状況レポートを作成します。RUM レポートを CSSM と ACK のインストールに送信するために使用できる方法は、実装するトポロジによって異なります。[サポートされるトポロジ \(13 ページ\)](#) 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 \(33 ページ\)](#) 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構文および使用方法の詳細については、対応するリリースのコマンドリファレンスを参照してください。 | Cisco Catalyst 9800 Series Wireless Controller Command Reference |
| 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 Quick Start Setup Guide Cisco Smart License Utility User Guide |

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 Gibraltar 16.10.1 | 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。 |
| 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 | <p>スマートライセンスの拡張バージョンには、ネットワークの運用を中断させないライセンスソリューションを提供するという主目的がありますが、むしろ、購入および使用しているハードウェアおよびソフトウェアライセンスを考慮して、コンプライアンス関係を実現するライセンスソリューションを提供するという目的もあります。</p> <p>このリリース以降、ポリシーを使用したスマートライセンスがデバイスで自動的に有効になります。これは、このリリースにアップグレードする場合にも当てはまります。</p> <p>デフォルトでは、CSSM のスマートアカウントとバーチャルアカウントは、ポリシーを使用したスマートライセンスで有効になっています。</p> |
| | Smart Licensing Using Policy への Cisco DNA Center のサポート | <p>Cisco DNA Center は、Cisco DNA Center リリース 2.2.2 以降、Smart Licensing Using Policy 機能をサポートしています。Cisco DNA Center を使用して製品インスタンスを管理する場合、Cisco DNA Center は CSSM に接続し、CSSM とのすべての通信のインターフェイスとなります。</p> <p>互換性のあるコントローラと製品インスタンス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。</p> <p>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 (19 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 (41 ページ) を参照してください。</p> |

| 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 | <p>SSM オンプレミスは、CSSM と連動するアセットマネージャです。これにより、CSSM に直接接続する代わりに、オンプレミスで製品とライセンスを管理できます。</p> <p>互換性のある SSM オンプレミスと製品インスタンスバージョンについては、SSM オンプレミス (6 ページ) を参照してください。</p> <p>このトポロジの概要と実装方法については、SSM オンプレミス展開 (22 ページ) と トポロジのワークフロー: SSM オンプレミス展開 (43 ページ) を参照してください。</p> <p>既存のバージョンの SSM オンプレミスから、Smart Licensing Using Policy への移行をサポートするバージョンへの移行については、Smart Licensing Using Policy をサポートする SSM オンプレミスのバージョンへの移行 (70 ページ) を参照してください。</p> |
| Cisco IOS XE Bengaluru 17.4.1 | AIR DNA ライセンスをオプトアウトし、EWC-AP のデフォルトのライセンスレベルを変更するオプション。 | <p>AIR DNA ライセンスの購入をオプトアウトするオプションが導入されました。このオプションは、Cisco Commerce ポータルからのみ利用できます。オプトアウトすると、AIR Network Essentials ライセンスのみが使用され、ポリシーを使用したスマートライセンシング機能が製品インスタンスで無効になります。詳細については、本ガイドの「AIR ライセンスの設定」の項を参照してください。</p> <p>このリリース以降、EWC-AP のデフォルトライセンスも AIR Network Essentials に変更されました。</p> |

| リリース | 機能 | 機能情報 |
|-------------------------------|--|---|
| Cisco IOS XE Cupertino 17.7.1 | Cisco Catalyst 9800-CL ワイヤレスコントローラの RUM レポートと確認応答の要件 | Cisco Catalyst 9800-CL ワイヤレスコントローラを使用している場合は、RUM レポートを完了し、製品インスタンスで確認応答 (ACK) が少なくとも 1 回利用できるようにする必要があります。これは、正しい最新の使用状況情報が CSSM に反映されるようにするためです。 |
| | 工場ですべてインストールされた信頼コード | 新しいハードウェアの注文では、信頼コードは製造時にインストールされるようになります。注：出荷時にインストールされた信頼コードを使用して CSSM と通信することはできません。 概要 (2 ページ) および 信頼コード (12 ページ) を参照してください。 |
| | 追加のトポロジでの信頼コードのサポート | 信頼コードは、製品インスタンスが CSLU へのデータ送信を開始するトポロジと、製品インスタンスがエアギャップネットワーク内にあるトポロジで自動的に取得されます。 次を参照してください。 <ul style="list-style-type: none">• 信頼コード (12 ページ)• CSLU を介して CSSM に接続 (13 ページ)、製品インスタンス開始型通信の場合のタスク (33 ページ) を次に示します。• CSLU は CSSM から切断 (17 ページ)、製品インスタンス開始型通信の場合のタスク (38 ページ) を次に示します。• CSSM への接続なし、CSLU なし (20 ページ)、トポロジのワークフロー：CSSM への接続なし、CSLU なし (42 ページ) を次に示します。 |
| RUM レポートの最適化と統計情報の可用性 | | |

| リリース | 機能 | 機能情報 |
|------|---|---|
| | | <p>RUM レポートの生成と関連プロセスが最適化されました。これには、RUM レポートの処理にかかる時間の短縮、メモリとディスク領域の使用率の向上、および製品インスタンス上の RUM レポートの可視性（エラーがある場合、エラーの数、各プロセスの処理状態など）が含まれます。</p> <p>RUM レポートおよびレポート確認応答（11 ページ） を参照してください。</p> <p>該当するリリースのコマンドリファレンスにある show license rum、show license all、および show license tech コマンドも参照してください。</p> |
| | <p>RUM レポートでソフトウェアバージョンを収集するためのサポート</p> | <p>バージョンプライバシーが無効になっている場合（no license smart privacy version グローバルコンフィギュレーションコマンド）、製品インスタンスで実行されている Cisco IOS-XE ソフトウェアバージョンと Smart Agent バージョン情報が RUM レポートに含まれます。</p> <p>該当するリリースのコマンドリファレンスで license smart グローバルコンフィギュレーション コマンドを参照してください。</p> |
| | <p>ACK および show コマンドの出力に含まれるアカウント情報</p> | <p>RUM 確認応答（ACK）には、CSSM で報告されたスマートアカウントとバーチャルアカウントが含まれます。次に、さまざまな show コマンドを使用してアカウント情報を表示できます。このアカウント情報は、製品インスタンスで使用可能な最新の ACK に基づいて常に表示されます。</p> <p>該当するリリースのコマンドリファレンスにある show license all、show license summary、show license status、および show license tech コマンドを参照してください。</p> |
| | <p>Linux の CSLU サポート</p> | |

| リリース | 機能 | 機能情報 |
|------|----|--|
| | | <p>Linux を実行しているマシン（ラップトップまたはデスクトップ）に CSLU を導入できるようになりました。</p> <p>CSLU（4 ページ）、トポロジのワークフロー：CSLU を介して CSSM に接続（33 ページ）、および CSLU は CSSM から切断（17 ページ） を参照してください。</p> |

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。