

# Catalyst プラットフォームでのスマートライセンスのトラブルシューティング

## 内容

---

### [はじめに](#)

[Cisco Smart Licensing とは](#)

[Smart Licensing の実装方式](#)

[サポート対象の Cisco IOS XE プラットフォーム](#)

[レガシーライセンスからスマートライセンスへの移行](#)

[Device Led Conversion \( DLC \) による変換](#)

[Cisco Smart Software Manager \( CSSM \) または License Registration Portal \( LRP \) による変換](#)

[Cisco Global Licensing Operations \( GLO \) 部門への連絡による変換](#)

[16.9 から 16.12.3 へのバージョン変更に伴う Catalyst 9500 ハイパフォーマンスモデルの動作の変更](#)

[Cisco IOS XE バージョン 16.11.x 以前](#)

[Cisco IOS XE バージョン 16.12.3 以降](#)

[C9500 ハイパフォーマンスモデルの変更に関する FAQ](#)

### [コンフィギュレーション](#)

[基本設定](#)

[登録トークン/デバイス ID トークン](#)

[登録とライセンスの状態](#)

### [考慮事項と注意事項](#)

### [トラブルシュート](#)

[デバイスを登録できない](#)

### [一般的な失敗のシナリオ](#)

[シナリオ #1 : スイッチ登録 "Failure Reason: Product Already Registered"](#)

[シナリオ #2 : スイッチ登録 "Failure Reason: Your Request could not be Processed Right Now"\(Please try again \)」](#)

[シナリオ #3 : "Failure Reason: The Device Date 1526135268653 is Offset beyond the Allowed Tolerance Limit"](#)

[シナリオ #4 : スイッチ登録 "Failure Reason: Communication Transport not Available"](#)

[シナリオ #5 : スイッチライセンス承認 "Failure Reason: Fail to Send out Call Home HTTP Message"](#)

[シナリオ #6 : "Failure Reason: Missing Id Cert Serial Number Field: Missing Signing Cert Serial Number Field: Signed Data and Certificate does not Match" ログ](#)

[シナリオ #7 : スイッチライセンス承認 "Failure reason: Waiting for reply"](#)

[シナリオ #8 : ステータスが "OUT OF COMPLIANCE" のライセンス](#)

[シナリオ #9 : スイッチライセンス承認 "Failure Reason: Data and Signature do not Match."](#)

---

## はじめに

このドキュメントでは、Cisco Smart Licensing ( クラウドベースシステム ) を使用して Catalyst

スイッチのソフトウェアライセンスを管理する方法について説明します。

## Cisco Smart Licensing とは

Cisco Smart Licensing は、複数のシスコ製品間ですべてのソフトウェアライセンスを管理する、クラウドベースの統合ライセンス管理システムです。このシステムを使用して、シスコソフトウェアライセンスを購入、導入、管理、追跡、更新できます。また、単一のユーザインターフェイスでライセンスの所有権と使用状況に関する情報を得られます。

このソリューションは、シスコのソフトウェア資産の追跡に使用する ( Cisco スマートライセンスポータル ) オンライン スマート アカウントとスマートアカウントの管理に使用する Cisco Smart Software Manager ( CSSM ) で構成されます。CSSM では、ライセンスの登録、登録解除、移行、転送といった、ライセンス管理に関連するすべてのタスクを実行できます。ユーザを追加して、スマートアカウントや特定のバーチャルアカウントに対するアクセスと権限を付与できます。

Cisco Smart Licensing の詳細については、以下を参照してください。

a ) [Cisco Smart Licensing のホームページ](#)

b ) [シスココミュニティのオンデマンドトレーニング](#)

Cisco IOS® XE 17.3.2 以降のスマートライセンスを使用したポリシー方式の詳細については、「[Catalyst スイッチング プラットフォームのポリシーを使用したスマートライセンス](#)」を参照してください。

スマートライセンスまたはスマートアカウントの管理が初めてという方は、シスココミュニティにアクセスし、新しい管理者向けトレーニングコースに登録してください。過去の録画トレーニングも参照できます。

[シスココミュニティ - Cisco スマートアカウント/スマートライセンス、My Cisco Entitlements でスマートに](#)

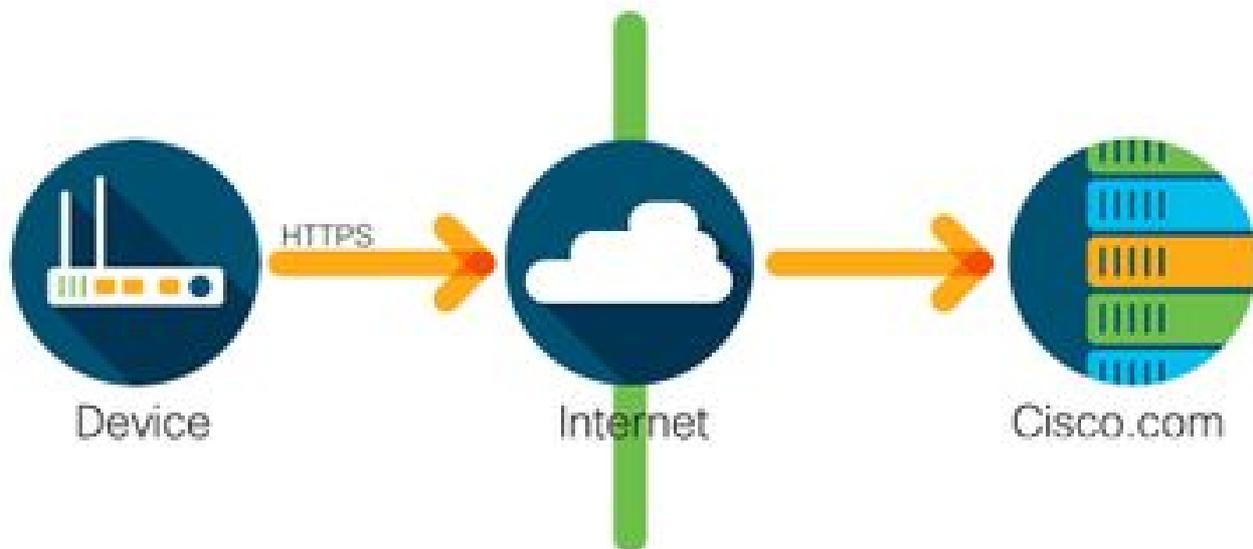
スマートアカウントの作成はこちらで行えます：[スマートアカウント](#)

スマートアカウントの管理はこちらで行えます：[スマート ソフトウェア ライセンス](#)

## Smart Licensing の実装方式

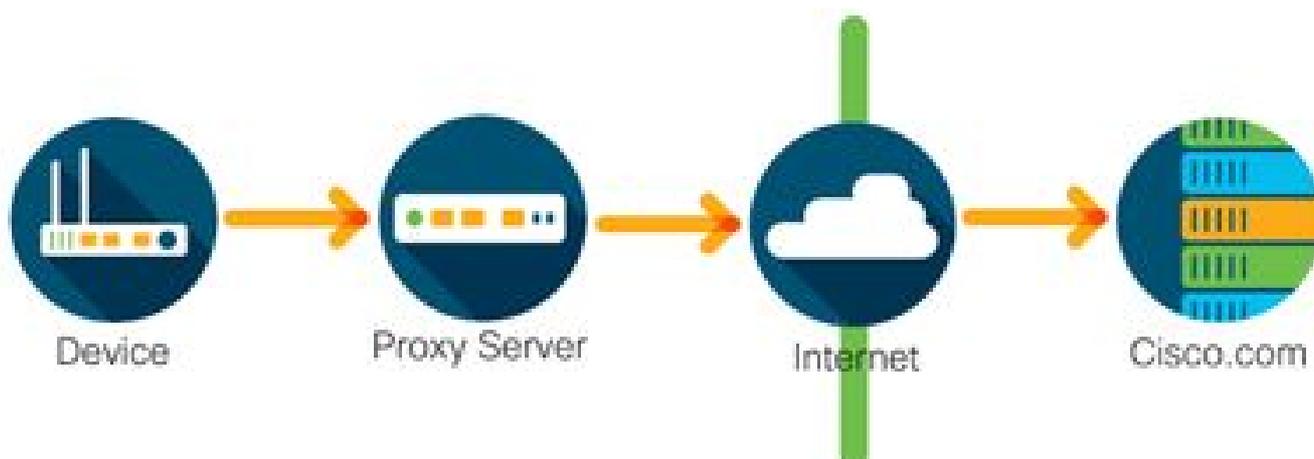
Cisco Smart Licensing は、企業のセキュリティプロファイルに応じて以下に示す複数の方式で導入できます。

ダイレクトクラウドアクセス



HTTPS を使用して、シスコ製品からインターネット経由で安全に使用状況に関する情報が直接送信されます。追加のコンポーネントは不要です。

#### HTTPS プロキシによるアクセス



HTTPS を使用して、シスコ製品から HTTP プロキシサーバ経由で安全に使用状況に関する情報が直接送信されます。既存のプロキシサーバを使用することも、シスコのトランスポートゲートウェイを介して導入することもできます ( 詳細については、 [ここをクリックしてください](#) )。

オンプレミス ライセンス サーバー ( 別名 Cisco Smart Software Manager サテライト )



シスコ製品から、インターネットを介して直接ではなく、オンプレミスのサーバに使用状況に関する情報が送信されます。サーバが 1 ヶ月に 1 回 HTTPS を使用してインターネット経由ですべてのデバイスにアクセスするか、手動で転送してデータベースを同期できます。CSSM オンプレミス ( サテライト ) は仮想マシン ( VM ) として使用でき、[ここでダウンロード可能](#)です。詳細については、[Smart Software Manager サテライトのページを参照してください](#)。

## サポート対象の Cisco IOS XE プラットフォーム

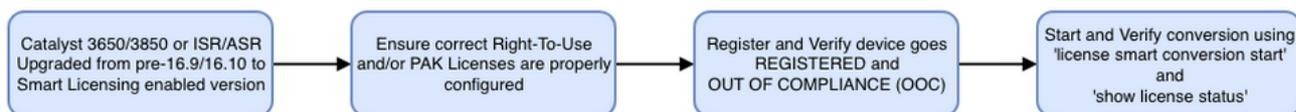
- Cisco IOS XE バージョン 16.9.1 のリリース以降、Catalyst 3650/3850 および Catalyst 9000 シリーズ スイッチプラットフォームは、唯一のライセンス方式として Cisco Smart Licensing 方式をサポートしています。
- Cisco IOS XE バージョン 16.10.1 のリリース以降、ASR1K、ISR1K、ISR4K、仮想ルータ ( CSRv/ISRv ) などのルータプラットフォームは、唯一のライセンス方式として Cisco Smart Licensing 方式をサポートしています。

## レガシーライセンスからスマートライセンスへの移行

使用权 ( RTU ) や製品アクティベーションキー ( PAK ) などのレガシーライセンスをスマートライセンスに変換する方式は 2 つあります。従う必要がある方法の詳細については、特定のシスコデバイスの関連するリリースノート、コンフィギュレーション ガイド、またはその両方を参照してください。

### Device Led Conversion ( DLC ) による変換

- Device Led Conversion ( DLC ) は、シスコ製品が使用しているライセンスを報告でき、それらのライセンスが Cisco Smart Software Manager ( CSSM ) の対応するスマートアカウントに自動的に取り込まれる 1 回限りの方式です。DLC の手順は、特定のシスコデバイスのコマンドライン インターフェイス ( CLI ) から直接実行されます。
- DLC のプロセスは、Catalyst 3650/3850 と特定のルータプラットフォームでのみサポートされています。特定のルータモデルについては、各プラットフォームのコンフィギュレーション ガイドとリリースノートを参照してください。例：[Fuji 16.9.x リリースを実行する Catalyst 3850 での DLC の手順](#)。



## Cisco Smart Software Manager ( CSSM ) または License Registration Portal ( LRP ) による変換

Cisco Smart Software Manager ( CSSM ) 方式 :

1. <https://software.cisco.com/> で Cisco Smart Software Manager ( CSSM ) にログインします。
2. [Smart Software Licensing] > [スマートライセンスに変換 ( Convert to Smart Licensing ) ] の順に移動します。
3. [PAKの変換 ( Convert PAK ) ] または [ライセンスの変換 ( Convert Licenses ) ] を選択します。

License Conversion

**Convert PAKs** | Convert Licenses | Conversion History | Event Log

The Product Activation Keys (PAKs) below contain licenses that can be used for traditional licensing or Smart Software Licensing. To add some or all of them to a Virtual Account as Smart Software Licenses, use the 'Convert to Smart Licenses' action in the table below.

If you do not see a PAK you expect to see in the table, ensure that it has been assigned to your Smart Account in the [Product License Registration Portal](#).

4. PAK ライセンスを変換するには、次の表で該当するライセンスを見つけます。PAK 以外のライセンスを変換する場合は、[ライセンス変換ウィザード ( License Conversion Wizard ) ] の段階的な指示に従います。

アカウントに関連付けられている既知の PAK ファイルの場所 :

License Conversion

**Convert PAKs** | Convert Licenses | Conversion History | Event Log

The Product Activation Keys (PAKs) below contain licenses that can be used for traditional licensing or Smart Software Licensing. To add some or all of them to a Virtual Account as Smart Software Licenses, use the 'Convert to Smart Licenses' action in the table below.

If you do not see a PAK you expect to see in the table, ensure that it has been assigned to your Smart Account in the [Product License Registration Portal](#).

**The Smart Account administrator may be able to more easily convert the licenses based on the automatic conversion settings.**

Last Updated : 2019-Apr-17 05:30:35

Search PAK, SKU, Virtual Account or Order Number

PAK	SKUs	Order Number	Order Date	Virtual Account	Status	Actions
	C1-ISE-PLS-T (25)		2018-May-07	CORE TAC		<a href="#">Convert to Smart Licen...</a>
	C1-ISE-BASE-T (25)		2018-May-07	CORE TAC		<a href="#">Convert to Smart Licen...</a>
	C1-ISE-BASE-T (25)		2018-May-07	CORE TAC		<a href="#">Convert to Smart Licen...</a>

[ライセンス変換ウィザード ( License Conversion Wizard ) ] のリンクの場所 :

## Smart Software Licensing

[Feedback](#) [Support](#) [Help](#)[Alerts](#) | [Inventory](#) | [Convert to Smart Licensing](#) | [Reports](#) | [Preferences](#) | [Satellites](#) | [Activity](#)Questions About Licensing?   
[Try our Virtual Assistant](#)

## License Conversion

Convert PAKs | **Convert Licenses** | Conversion History | Event Log

The table below contains devices in your Smart Account that are using traditional licenses that can be converted to Smart Software Licenses. If you do not see a device you expect to see in the table, ensure that it has been assigned to your Smart Account in the [Product License Registration Portal](#). You can also try entering the device information in the [License Conversion wizard](#).

Last Updated : 2018-Nov-14 10:31:53 ⓘ



Device Identifier	Product Family	Eligible SKUs	Virtual Account	Actions
No Records Found				

No Records to Display

5. 目的のライセンスと製品の組み合わせを探します。

6. ( [アクション ( Actions ) ] で ) [スマートライセンスへの変換 ( Convert to Smart Licensing ) ] をクリックします。

## License Conversion

Convert PAKs | Convert Licenses | Conversion History | Event Log

The Product Activation Keys (PAKs) below contain licenses that can be used for traditional licensing or Smart Software Licensing. To add some or all of them to a Virtual Account as Smart Software Licenses, use the 'Convert to Smart Licenses' action in the table below.

If you do not see a PAK you expect to see in the table, ensure that it has been assigned to your Smart Account in the [Product License Registration Portal](#).

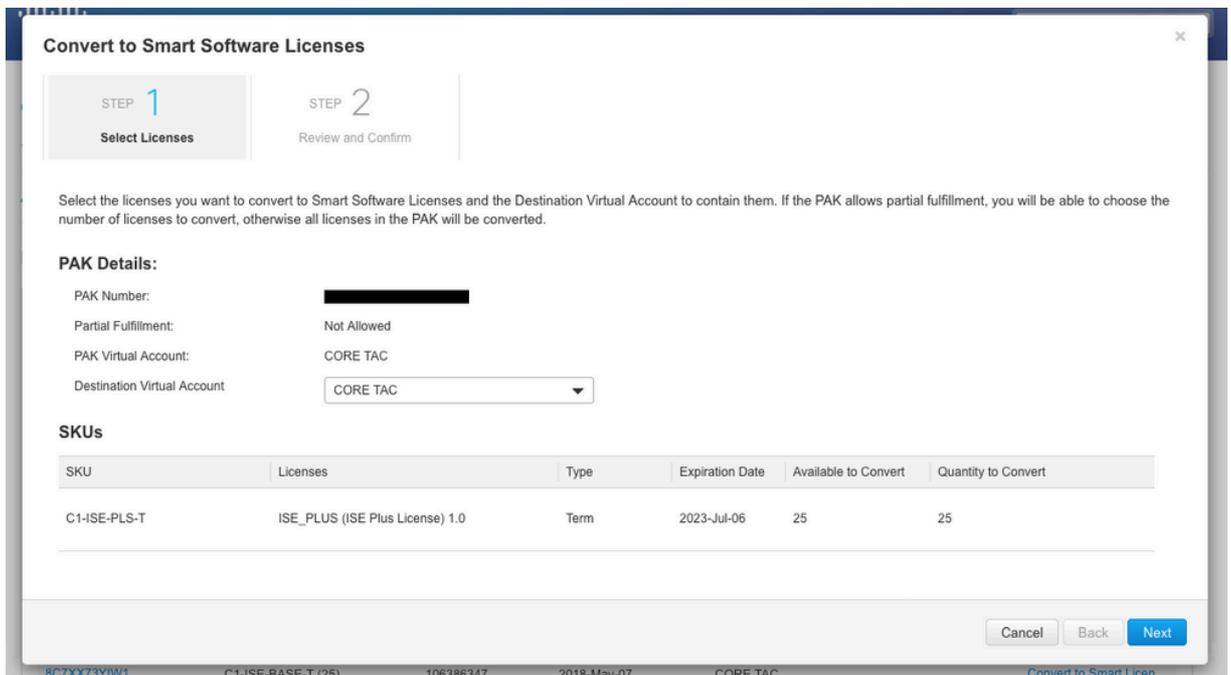
ⓘ The Smart Account administrator may be able to more easily convert the licenses based on the automatic conversion settings.

Last Updated : 2019-Apr-16 09:30:49 ⓘ



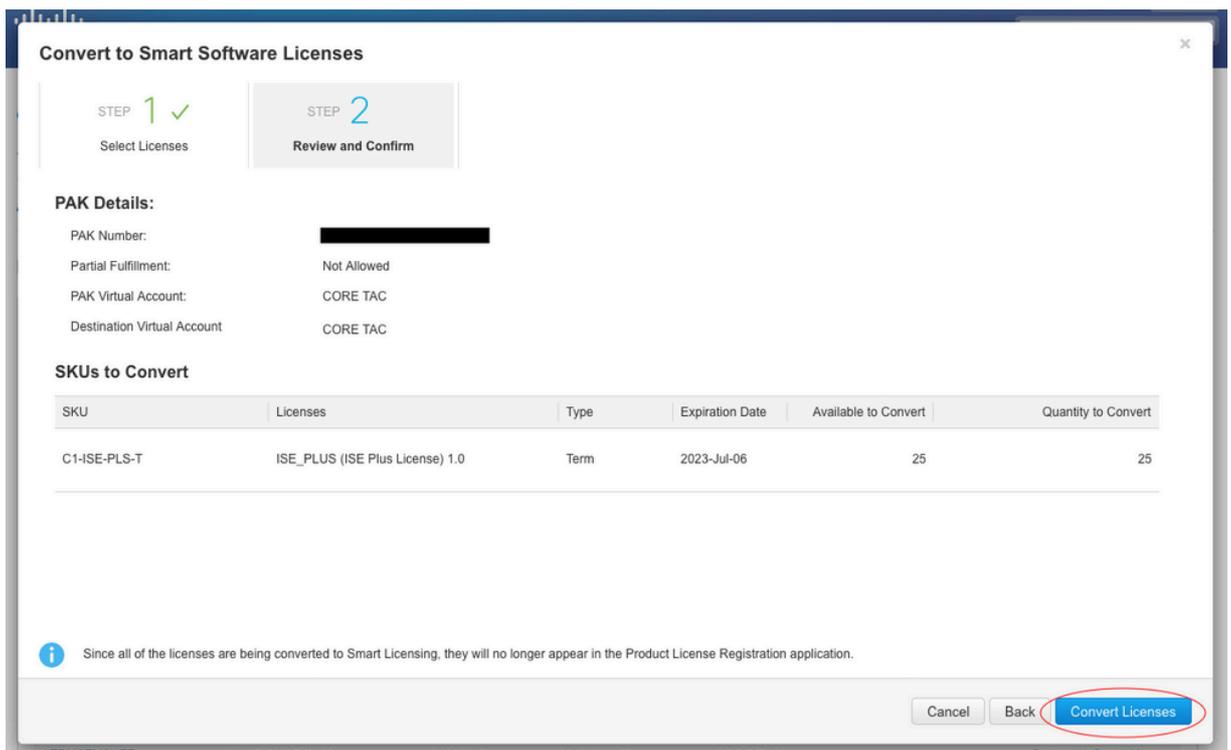
PAK	SKUs	Order Number	Order Date	Virtual Account	Status	Actions
██████████	C1-ISE-PLS-T (25)	██████████	2018-May-07	CORE TAC		<a href="#">Convert to Smart Licen...</a>
██████████	C1-ISE-BASE-T (25)	██████████	2018-May-07	CORE TAC		<a href="#">Convert to Smart Licen...</a>
██████████	C1-ISE-BASE-T (25)	██████████	2018-May-07	CORE TAC		<a href="#">Convert to Smart Licen...</a>
██████████	C1-ISE-BASE-T (25)	██████████	2018-May-07	CORE TAC		<a href="#">Convert to Smart Licen...</a>

7. バーチャルアカウントとライセンスを選択し、[次へ ( Next ) ] をクリックします。



8. 選択内容を確認してから [ライセンスの変換 ( Convert Licenses ) ] をクリックします

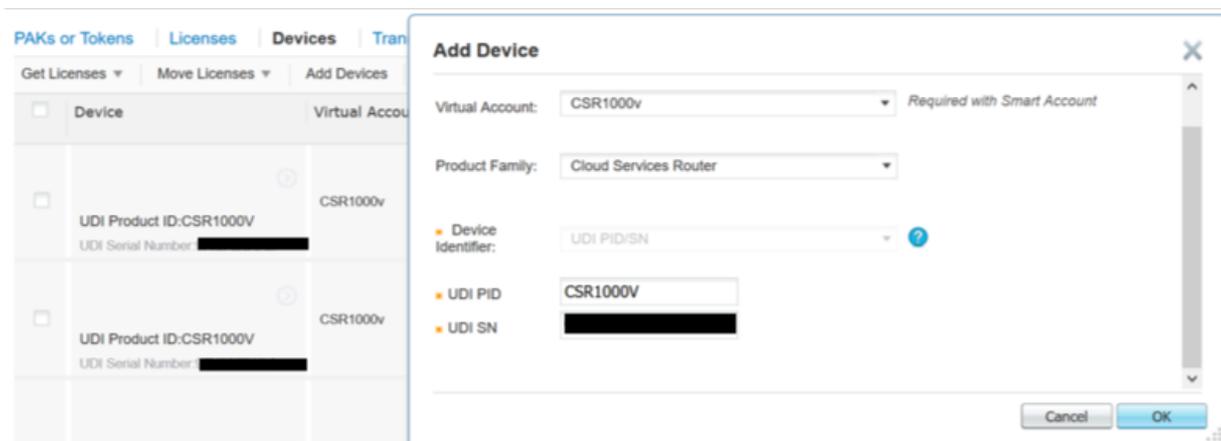
o



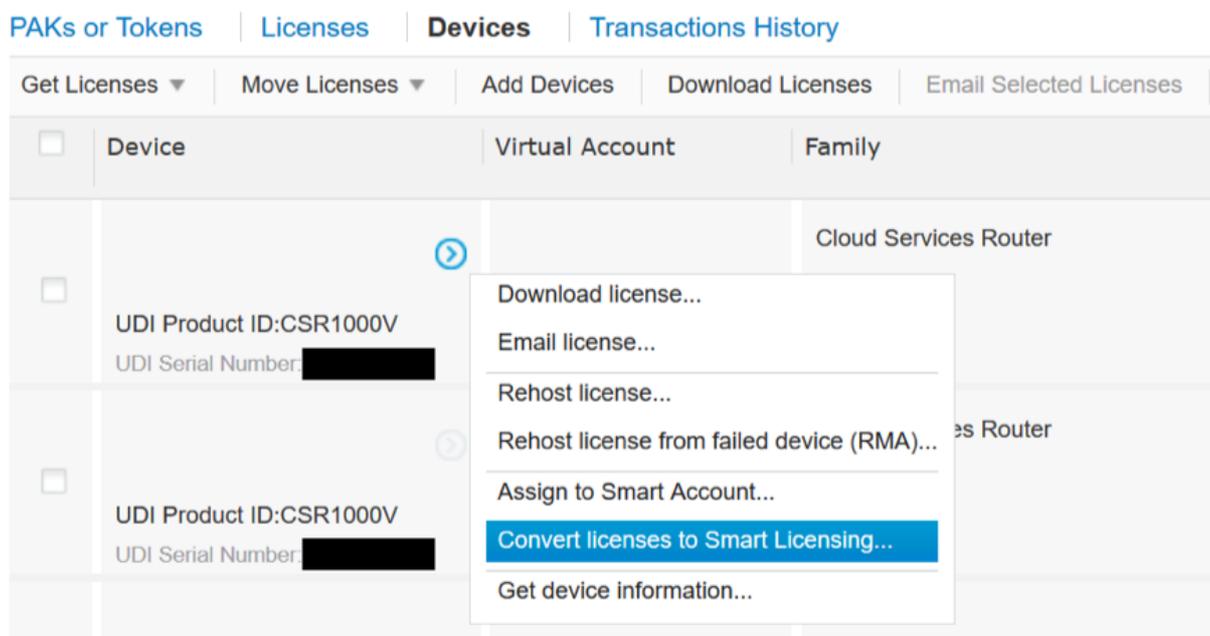
## License Registration Portal ( LRP ) を使用する方法

1. License Registration Portal ( LRP ) にログインします。  
<http://tools.cisco.com/SWIFT/LicensingUI/Home>
2. [デバイス ( Devices ) ] > [デバイスの追加 ( Add Devices ) ] に移動します。
3. 該当する製品ファミリと固有のデバイス識別子 ( UDI ) の製品 ID、シリアル番号を入力して [OK] をクリックします。UDI の情報は、シスコデバイスの CLI ( コマンドライン

インターフェイス) で show version または show inventory コマンドを実行して取得できます。



4. 追加したデバイスを選択し、[ライセンスをスマートライセンスに変換 ( Convert Licenses to Smart Licensing ) ] を実行します。



5. 適切なバーチャルアカウントに割り当て、変換するライセンスを選択して [送信 ( Submit ) ] をクリックします。

### Convert to Smart Entitlements ✕

**Device ID:** UDI Product ID:CSR1000V,UDI Serial Number:

**Product Family:** Cloud Services Router

**Smart Account:** ,cisco.com

**Virtual Account:**

<input type="checkbox"/> SKU	Type	Term Date	Quantity Available	Quantity to Convert
<input checked="" type="checkbox"/> L-CSR-5G-SEC=	Perpetual	--	1	<input type="text" value="1"/>

*i* Once these entitlements have been converted they will no longer appear in this portal.

 ヒント : LRP ツールは、[PAK] または [トークン ( Tokens ) ] タブでライセンス/製品ファミリーを検索して使用することもできます。[PAK]/[トークン ( Token ) ] の横にある丸いドロップダウンをクリックし、[スマートライセンスへの変換 ( Convert to Smart Licensing ) ] を選択します。

PAKs or Tokens | Licenses | Devices | Transactions History Guide Me >

Get Licenses ▾ | Add New PAKs/Tokens | Smart Accounts ▾ | Manage Paks ▾ | Export to CSV | Show Filter

<input type="checkbox"/>	PAK/Token	Virtual Account	Order Number	Product	Status	Licenses Used	Available
<input type="checkbox"/>	<input type="text"/> Family: ASR1001	DEFAULT	<input type="text"/>	SKU: ASR1_MFGINSTALL Cisco ASR 1000 Advanced IP... SKU: SLASR1-AIS	CONVERTED CONVERTED	1 4	0 0
<input type="checkbox"/>	<input type="text"/> Family: Cisco Nexus 9000 S...	DEFAULT	<input type="text"/>	NX-OS Advantage license for... SKU: NXOS-AD-XF2	UNFULFILLED	0	1
<input type="checkbox"/>	<input type="text"/> Family: Cisco Nexus 9000 S...	DEFAULT	<input type="text"/>	NX-OS Advantage license for... SKU: NXOS-AD-XF2	UNFULFILLED	0	1
<input type="checkbox"/>	<input type="text"/> Family: Cisco Nexus 9000 S...	DEFAULT	<input type="text"/>	NX-OS Advantage license for... SKU: NXOS-AD-XF2	UNFULFILLED	0	1
<input type="checkbox"/>	<input type="text"/> Family: Cisco Nexus 9000 S...	DEFAULT	<input type="text"/>	NX-OS Advantage license for... SKU: NXOS-AD-XF2	UNFULFILLED	0	1

Cisco Global Licensing Operations ( GLO ) 部門への連絡による変換

Global Licensing Operations 部門には、ワールドワイド コンタクト センターの[ここからアクセス](#)できます。

16.9 から 16.12.3 へのバージョン変更に伴う Catalyst 9500 ハイパフォーマンスモデルの動作の変更

他の Catalyst 9000 モデルと同様に、Catalyst 9500 ハイパフォーマンスモデルでも Cisco IOS XE

バージョン 16.9 トレイン以降のスマートライセンスに対応しました。Catalyst 9500 ハイパフォーマンスモデルの場合、各モデルには固有のライセンス権限タグがありましたが、その後、C9500 プラットフォームの権限タグを統合することが製品チームとマーケティングチームによって決定されました。この決定により、C9500 ハイパフォーマンスモデルは専用の権限タグではなく、C9500 汎用ライセンスを使用する仕組みに変更されました。

この動作の変更は、次の不具合情報で説明されています。

a) [Cisco Bug ID CSCvp30661](#)

b) [Cisco Bug ID CSCvt01955](#)

次の表は、前述の C9500 ハイパフォーマンスモデルのライセンス変更に関する変更前後のライセンス名をまとめたものです。

Cisco IOS XE バージョン 16.11.x 以前

C9600 ハイパフォーマンスモデルには、モデルごとに固有の権限タグがあります。

モデル	ライセンス
C9500-32C	C9500 32C NW Essentials C9500 32C NW Advantage C9500 32C Cisco DNA Essentials C9500 32C Cisco DNA Advantage
C9500-32QC	C9500 32QC NW Essentials C9500 32QC NW Advantage C9500 32QC Cisco DNA Essentials C9500 32QC Cisco DNA Advantage
C9500-24Y4C	C9500 24Y4C NW Essentials C9500 24Y4C NW Advantage C9500 24Y4C Cisco DNA Essentials C9500 24Y4C Cisco DNA Advantage
C9500-48Y4C	C9500 48Y4C NW Essentials

	C9500 48Y4C NW Advantage C9500 48Y4C Cisco DNA Essentials C9500 48Y4C Cisco DNA Advantage
--	-------------------------------------------------------------------------------------------------

 注 : Cisco IOS XE バージョン 16.12.1 および 16.12.2 には、[Cisco bug ID CSCvp30661](#) および [Cisco bug ID CSCvt01955](#) の不具合があります。これらの不具合は、16.12.3a 以降対処されています。

#### Cisco IOS XE バージョン 16.12.3 以降

Catalyst 9500 ハイ パフォーマンス プラットフォームでは、汎用ネットワークライセンスタグと個別の Cisco DNA ライセンスタグが使用されるようになりました。次の表では、Cisco IOS XE バージョン 16.12.3 以降での権限の変更を強調表示しています。

モデル	ライセンス
C9500-32C	C9500 Network Essentials C9500 Network Advantage C9500 32C Cisco DNA Essentials C9500 32C Cisco DNA Advantage
C9500-32QC	C9500 Network Essentials C9500 Network Advantage C9500 32QC Cisco DNA Essentials C9500 32QC Cisco DNA Advantage
C9500-24Y4C	C9500 Network Essentials C9500 Network Advantage C9500 24Y4C Cisco DNA Essentials C9500 24Y4C Cisco DNA Advantage
C9500-48Y4C	C9500 Network Essentials

	C9500 Network Advantage C9500 48Y4C Cisco DNA Essentials C9500 48Y4C Cisco DNA Advantage
--	------------------------------------------------------------------------------------------------

 注：Cisco IOS XE バージョン 16.12.1 および 16.12.2 からのアップグレードは、このライセンス動作になります。Cisco IOS XE バージョン 16.9.x、16.10.x、16.11.x から 16.12.3 へのアップグレードでは、古いライセンス設定が認識されます。

## C9500 ハイパフォーマンスモデルの変更に関する FAQ

1. デバイス固有のネットワークライセンスを使用しているのにシスコサポートから汎用ネットワークライセンスが割り当てられるのはなぜですか。

汎用タグは、ネットワークデバイスに最適な権限タグとして提供されます。このタグにより、特定の C9500 ハイパフォーマンスモデルだけでなく、Cat9500 プラットフォーム全体で権限タグを使用できるようになります。16.12.3 よりも前の、デバイス固有のライセンスタグを要求するイメージは、汎用ライセンスタグに準拠します。これはより固有のライセンスが、ライセンス階層における汎用ライセンスに分類されるためです。

2. スマートアカウントに 2 つのネットワークタグが表示されることがあるのはなぜですか。

この動作はライセンス階層に起因するものです。デバイス固有のライセンスタグを使用する旧式のイメージでデバイスが動作している場合に発生します。デバイス固有のライセンスタグを要求する旧式のイメージは、汎用ライセンスタグに準拠します。これは、より固有のタグが、ライセンス階層における汎用ライセンスに分類されるためです。

## コンフィギュレーション

### 基本設定

スマートライセンスの正確な設定手順については、各リリース/プラットフォームのシステム管理コンフィギュレーションガイドを参照してください。

例：『[System Management Configuration Guide, Cisco IOS XE Fuji 16.9.x \(Catalyst 9300 Switches\)](#)』

### 登録トークン/デバイス ID トークン

デバイスを登録する前にトークンを生成する必要があります。デバイス ID トークンとも呼ばれる登録トークンは、シスコデバイスに対応するスマートアカウントに最初に登録するときに Smart Licensing Portal か Cisco Smart Software Manager オンプレミスから生成される一意のトークンです。各トークンは、作成中に使用されるパラメータに応じて複数のシスコデバイスを登録する際に使用できます。

また登録トークンは、シスコデバイスを最初に登録するときのみ必要です。登録トークンは、Call Home を使用してシスコのバックエンドに通知を送り、正しいスマートアカウントに関連付けるための情報をデバイスに提供するものであるためです。シスコデバイスが登録されると、トークンは不要になります。

登録トークンとその作成方法の詳細については、[ここをクリック](#)して一般的なガイドを参照してください。詳細については、特定のシスコデバイスのコンフィギュレーションガイドを参照してください。

## 登録とライセンスの状態

スマートライセンスを導入して設定するとき、シスコデバイスはさまざまな異なる状態になっていると考えられます。これらの状態は、シスコデバイスのコマンドライン インターフェイス ( CLI ) で `show license all` か `show license status` の出力を見るとわかります。

次に、すべての状態とその説明のリストを示します。

### [評価 ( 未確認 ) ( Evaluation (Unidentified) ) ] 状態

- [評価 ( Evaluation ) ] は、デバイスを最初に起動したときのデフォルトの状態です。
- この状態は通常、シスコデバイスがまだスマートライセンス用に設定されていないか、スマートアカウントに登録されていない場合に表示されます。
- この状態では、すべての機能が使用可能となっており、デバイスでライセンスレベルを自由に変更できます。
- 評価期間は、デバイスが未確認状態の場合に使用されます。この状態でデバイスがシスコとの通信を試みることはありません。
- 評価期間は使用日 90 日で、90 カレンダー日ではありません。評価期間が期限切れになると、リセットすることはできません。
- 権限ごとに 1 つの評価期間ではなく、デバイス全体に対して 1 つの評価期間が設けられます。
- 90 日が経過した時点で評価期間が終了すると、デバイスは EVAL EXPIRY モードになります。ただし、リロード後でも、機能への影響や中断はありません。現在のところ、適用されているものではありません。
- カウントダウン時間は再起動後も維持されます。
- 評価期間は、デバイスがまだシスコに登録されておらず、シスコのバックエンドから次の 2 つのメッセージを受信していない場合に使用されます。
  1. 登録要求に対する成功応答。
  2. 権限承認要求に対する成功応答

### [登録済み ( Registered ) ] 状態

- [登録済み ( Registered ) ] は、登録が正常に完了した後に想定される状態です。
- この状態は、シスコデバイスが Cisco スマートアカウントと正常に通信することが可能になっており、登録できていることを示します。
- デバイスは、今後の通信に使用される 1 年間有効な ID 証明書を受け取ります。
- デバイスは、デバイスで使用されているライセンスの権限承認要求を CSSM に送信します。
- CSSM の応答に応じて、デバイスは [承認済み ( Authorized ) ] 状態または [不適合 ( Out of

Compliance ) ] 状態のいずれかになります。

- ID 証明書の有効期限は 1 年です。6 カ月後にソフトウェア エージェント プロセスで証明書の更新が試みられます。CSSM と通信できない場合、エージェントは有効期限 ( 1 年 ) まで引き続き ID 証明書の更新を試みます。1 年が経過すると、エージェントは [未確認 ( Un-Identified ) ] 状態に戻り、評価期間を有効にしようとします。CSSM は製品インスタンスをデータベースから削除します。
- [承認済み ( Authorized ) ] 状態
- [承認済み ( Authorized ) ] は、デバイスが権限を使用しており、適合している ( 負のバランスになっていない ) 場合に想定される状態です。
- この状態は、CSSM のバーチャルアカウントに正しい種類と数のライセンスがあり、デバイスでのライセンスの使用が承認されていることを示しています。
- デバイスは、30 日後に承認を更新するための新しい要求を CSSM に送信します。
- この状態の期間は 90 日間です。 ( 正常に更新されなかった場合 ) 90 日後に、デバイスは [承認の期限切れ ( Authorization Expired ) ] 状態に移行します。

[不適合 ( Out of Compliance ) ] 状態

- [不適合 ( Out of Compliance ) ] は、デバイスが権限を使用しており、適合していない ( 負のバランスになっている ) 場合の状態です。
- この状態は、シスコデバイスの登録先である対応するバーチャルアカウントに使用可能なライセンスがない場合に、Cisco スマートアカウントで表示されます。
- [適合 ( Compliance ) ][承認済み ( Authorized ) ] 状態にするには、スマートアカウントに正しい数と種類のライセンスを追加する必要があります。
- デバイスが [不適合 ( Out of Compliance ) ] 状態になっている場合、デバイスは毎日自動的に承認更新要求を送信します。
- ライセンスと機能は引き続き使用でき、機能への影響はありません。

[承認の期限切れ ( Authorization Expired ) ] 状態

- [承認の期限切れ ( Authorization Expired ) ] は、権限を使用しているデバイスが、関連付けられた Cisco スマートアカウントと 90 日超にわたって通信できていない場合の状態です。
- この状態は通常、シスコデバイスがインターネットにアクセスできなくなったか、最初の登録の後に tools.cisco.com に接続できない場合に表示されます。
- スマートライセンスのオンライン方式では、この状態にならないようにするために、シスコデバイスが少なくとも 90 日に 1 回通信する必要があります。
- CSSM は、90 日間このデバイスとの通信がなかったことを理由として、デバイスで使用されているすべてのライセンスをプールに戻します。
- この状態になっている場合、デバイスは、登録期間 ( ID 証明書 ) が期限切れになるまで、権限承認を更新するために 1 時間ごとにシスコへの連絡を試み続けます。
- ソフトウェアエージェントは、シスコとの通信を再確立して承認要求を受け取ると、その応答を正常に処理していずれかの確立状態になります。

## 考慮事項と注意事項

16.9.1 以降のスイッチと 16.10.1 以降のルータでは、スマートライセンスへの移行を支援するために CiscoTAC-1 という名前のデフォルトの Call Home プロファイルが生成されます。 デフォ

ルトでは、このプロファイルはダイレクトクラウドアクセス方式用に設定されます。

<#root>

```
#show call-home profile CiscoTAC-1
```

```
Profile Name: CiscoTAC-1
Profile status: ACTIVE
Profile mode: Full Reporting
Reporting Data: Smart Call Home, Smart Licensing
Preferred Message Format: xml
Message Size Limit: 3145728 Bytes
Transport Method: http
HTTP address(es): https://tools.cisco.com/its/service/oddce/services/DDCEService
Other address(es): default
<snip>
```

Cisco Smart Software Manager オンプレミスサーバーを使用している場合、アクティブな Call-Home 設定の下にある宛先アドレスは、そのプロファイル（大文字と小文字を区別）を指している必要があります。

<#root>

```
(config)#call-home
(cfg-call-home)#profile "CiscoTAC-1"
(cfg-call-home-profile)#destination address http https://
```

<IP/FQDN>

```
/Transportgateway/services/DeviceRequestHandler
```

tools.cisco.com を解決するには DNS が必要です。DNS サーバーとの接続が VRF 内で設定されている場合は、対象の送信元インターフェイスと VRF が次のように定義されていることを確認します。

Global Routing Table Used:

```
(config)#ip domain-lookup [source-interface <INTERFACE>]
(config)#ip name-server <IP>
```

VRF Routing Table Used:

```
(config)#ip domain-lookup [source-interface <INTERFACE>] <<-- "ip vrf forwarding <VRF-NAME>" defined
(config)#ip name-server vrf <VRF-NAME> <SERVER-IP>
```

また、NDS を使用できない場合は、（エンドデバイスのローカル DNS 解決に基づいて）ローカル DNS から IP へのマッピングを静的に設定するか、Call Home 設定の DNS 名を IP アドレスに置き換えます。ダイレクトクラウドアクセスの例を参照してください（Cisco Smart Software Manager オンプレミスで tools.cisco.com ではなく DNS 名を使用する場合）。

```
(config)#ip host tools.cisco.com <x.x.x.x>
```

( Mgmt-vrf など ) 特定の VRF のインターフェイスから tools.cisco.com への通信が必要な場合は、次の CLI を設定する必要があります。

```
(config)#ip http client source-interface <VRF_INTERFACE>
```

StackWise や StackWise Virtual で動作する Catalyst スイッチなど、シスコデバイスの設定によって使用されるライセンスの数が異なる場合があります。

従来の StackWise でサポートされるスイッチ ( Catalyst 9300 シリーズなど ) :

ネットワークライセンス : スタック内のスイッチごとに 1 つのライセンスが使用されます。

Cisco DNA ライセンス : スタック内のスイッチごとに 1 つのライセンスが使用されます。

モジュラ型シャーシ ( Catalyst 9400 シリーズなど ) :

ネットワークライセンス : シャーシ内のスーパーバイザごとに 1 つのライセンスが使用されます。

Cisco DNA ライセンス : シャーシごとに 1 つのライセンスが使用されます。

固定の StackWise Virtual でサポートされるスイッチ ( Catalyst 9500 シリーズなど ) :

ネットワークライセンス : スタック内のスイッチごとに 1 つのライセンスが使用されます。

Cisco DNA ライセンス : スタック内のスイッチごとに 1 つのライセンスが使用されます。

- スマートライセンスに対してアクティブにできる Call Home プロファイルは 1 つだけです。
- ライセンスは対応する機能が設定されている場合にのみ使用されます。
- スマートライセンス用に設定されたシスコデバイスは、対応する Cisco スマートアカウントと適切に同期されるように正しいシステム日時を設定する必要があります。シスコデバイスのタイムオフセットが離れすぎていると、デバイスを登録できない可能性があります。クロックは手動で設定するか、Network Time Protocol ( NTP ) や Precision Time Protocol ( PTP ) などのタイムプロトコルを使用して設定する必要があります。これらの変更に必要な正確な手順については、特定のシスコデバイスのコンフィギュレーション ガイドを参照してください。
- シスコデバイスの登録中に生成される Public Key Infrastructure ( PKI ) キーは、登録後に自

動的に保存されなければ保存する必要があります。デバイスで PKI キーを保存できなかった場合は、copy running-config startup-config または write memory コマンドを使用して設定を保存するよう指示する syslog が生成されます。

- シスコデバイスの PKI キーが適切に保存されていない場合、フェールオーバーカリロードのときにライセンスの状態が失われる可能性があります。
- HTTPS プロキシ方式でサードパーティのプロキシを使用する場合、スマートライセンスはデフォルトで HTTPS プロキシの SSL 証明書の代行受信をサポートしません。この機能をサポートするには、プロキシで SSL の代行受信を無効にするか、プロキシから送信された証明書を手動でインポートします。

<#root>

#### How to Manually Import Certification as a TrustPoint:

The certificate will need be in a BASE64 format to be copied and pasted onto the device as a TrustPoint

The following example shown below uses "LicRoot" as the TrustPoint name, however, this name can be changed

```
Device#conf t
Device(config)#crypto pki trustpoint LicRoot
Device(ca-trustpoint)#enrollment terminal
Device(ca-trustpoint)#revocation-check none
Device(ca-trustpoint)#exit
Device(config)#crypto pki authenticate LicRoot
Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself
-----BEGIN CERTIFICATE-----
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
-----END CERTIFICATE-----
Certificate has the following attributes:
  Fingerprint MD5: XXXXXXXX
  Fingerprint SHA1: XXXXXXXX
% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
% Certificate successfully imported
```

トランスポートゲートウェイの HTTP プロキシを使用する場合は、次の例のように IP アドレスを tools.cisco.com からプロキシに変更する必要があります。

```
destination address http https://tools.cisco.com/its/service/oddce/services/DDCEService
TO
destination address http https://<TransportGW-
IP_Address>:<port_number>/Transportgateway/services/DeviceRequestHandler
```

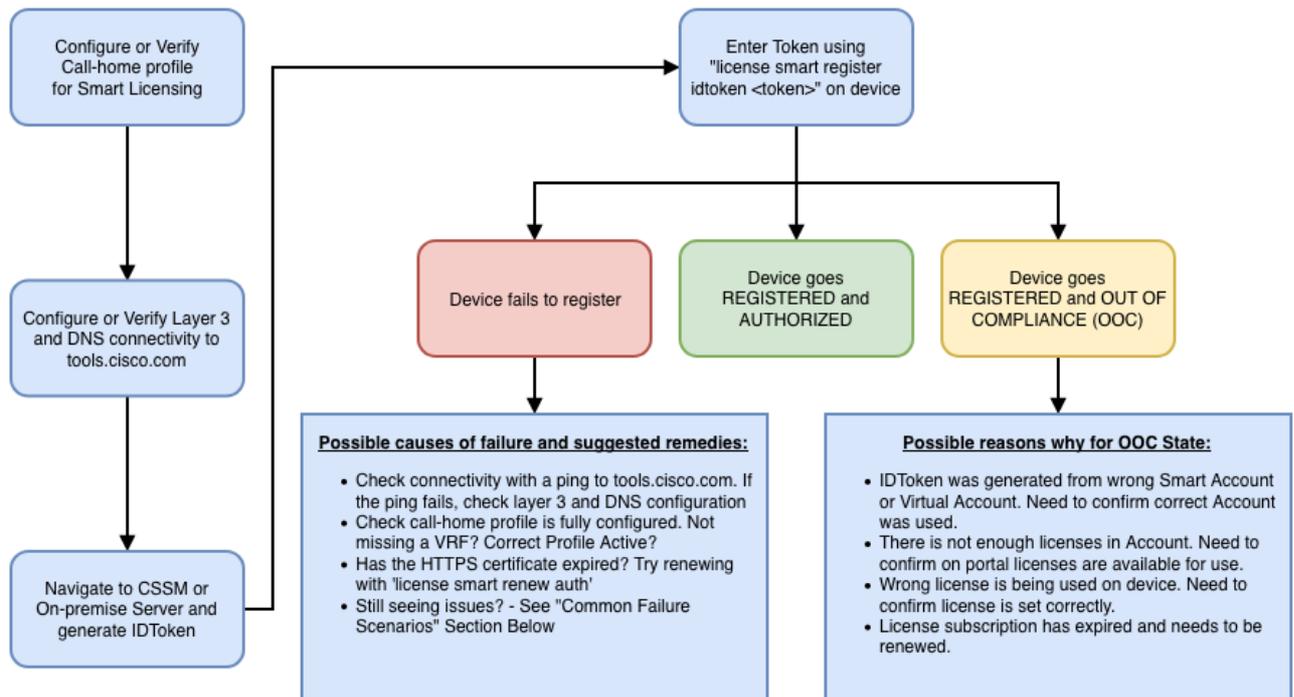
トランスポートゲートウェイの IP アドレスは、Cisco トランスポートゲートウェイの GUI で [HTTP設定 ( HTTP Settings ) ] に移動し、HTTP サービスの URL の下を見るとわかります。

詳細については、Cisco トランスポートゲートウェイのコンフィギュレーションガイド ( [こちら](#) ) を参照してください。

# トラブルシューティング

シスコデバイスをスマートライセンス対応のソフトウェアバージョンに移行するときは、3 つすべての方式 ( ダイレクトクラウドアクセス、HTTPS プロキシ、Cisco Smart Software Manager オンプレミス ) の一般的なガイドとして、次のフローチャートを使用できます。

スマートライセンスをサポートするソフトウェアリリースでアップグレードされるか、そのソフトウェアリリースとともに出荷されるデバイス ( セクション 1.3 にあるサポート対象の Cisco IOS XE リリースの一覧を参照 ) 。



次のトラブルシューティング手順は、主にデバイスを登録できないシナリオに焦点を置いています。

## デバイスを登録できない

初期設定が終わったら、スマートライセンスを有効にするために、CSSM/Cisco Smart Software Manager オンプレミスで生成されるトークンを CLI を使用してデバイスに登録する必要があります。

```
license smart register idtoken <TOKEN>
```

このアクションにより、次のイベントが生成されます。

```
<#root>
```

```
! Smart licensing process starts
```

!

Registration process is in progress. Use the 'show license status' command to check the progress and re

!

! Crypto key is automatically generated for HTTPS communication

!

Generating 2048 bit RSA keys, keys will be exportable... [OK] (elapsed time was 1 seconds)

%CRYPTO\_ENGINE-5-KEY\_ADDITION: A key named SLA-KeyPair has been generated or imported by crypto-engine

%PKI-4-NOCONFIGAUTOSAVE: Configuration was modified. Issue "write memory" to save new IOS PKI configur

!

! Call-home start registration process

!

%CALL\_HOME-6-SCH\_REGISTRATION\_IN\_PROGRESS: SCH device registration is in progress. Call-home will poll

!

! Smart Licensing process connects with CSSM and check entitlement.

!

%SMART\_LIC-6-EXPORT\_CONTROLLED: Usage of export controlled features is allowed

%SMART\_LIC-6-AGENT\_REG\_SUCCESS: Smart Agent for Licensing Registration with the Cisco Smart Software Ma

%SMART\_LIC-4-CONFIG\_NOT\_SAVED: Smart Licensing configuration has not been saved

%SMART\_LIC-5-IN\_COMPLIANCE: All entitlements and licenses in use on this device are authorized

%SMART\_LIC-6-AUTH\_RENEW\_SUCCESS: Authorization renewal with the Cisco Smart Software Manager or satellit

Call Home の設定を確認するには、次の CLI を実行します。

<#root>

```
#show call-home profile all
```

Profile Name: CiscoTAC-1

Profile status: ACTIVE

Profile mode: Full Reporting

Reporting Data: Smart Call Home, Smart Licensing

Preferred Message Format: xml  
Message Size Limit: 3145728 Bytes

Transport Method: http

HTTP address(es): https://tools.cisco.com/its/service/oddce/services/DDCEService

Other address(es): default

Periodic configuration info message is scheduled every 1 day of the month at 09:15

Periodic inventory info message is scheduled every 1 day of the month at 09:00

Alert-group	Severity
crash	debug
diagnostic	minor
environment	warning
inventory	normal

Syslog-Pattern	Severity
APF-.-WLC_.*	warning
.*	major

スマートライセンスのステータスを確認するには、次の CLI を実行します。

```
<#root>
```

```
#show license summary
```

```
Smart Licensing is ENABLED
```

```
Registration:
```

```
Status: REGISTERED
```

```
Smart Account: TAC Cisco Systems, Inc.  
Virtual Account: Krakow LAN-SW  
Export-Controlled Functionality: ALLOWED  
Last Renewal Attempt: None  
Next Renewal Attempt: Nov 22 21:24:32 2019 UTC
```

```
License Authorization:
```

```
Status: AUTHORIZED
```

```
Last Communication Attempt: SUCCEEDED
```

```
Next Communication Attempt: Jun 25 21:24:37 2019 UTC
```

```
License Usage:
```

```
License                Entitlement tag                Count Status
```

```
-----
```

C9500 Network Advantage (C9500 Network Advantage)  
C9500-DNA-40X-A (C9500-40X DNA Advantage)

1 AUTHORIZED  
1 AUTHORIZED

デバイスが登録に失敗した場合（および状態が「登録済み（REGISTERED）」ではない場合）、「コンプライアンス不適合（Out-of-Compliance）」は CSSM に問題があることを示します。この場合の問題としては、スマート バーチャル アカウントのライセンスがない、マッピングが不適切な状態（たとえば、有効なライセンスがない別のバーチャルアカウントからのトークンが使用された場合）などが考えられます。 次のことを確認してください。

## 1. 設定と一般的な失敗のシナリオを確認する

セクション 2.1 の基本設定の手順を参照してください。また、セクション 5 に記載されている、このフィールドで確認された一般的な失敗のシナリオも参照してください。

## 2. 基本接続のチェック

デバイスが tools.cisco.com（ダイレクトアクセスの場合）、または Cisco Smart Software Manager オンプレミスサーバーに到達できる（そして TCP ポートを開けられる）ことを確認します。

<#root>

```
#show run all | in destination address http
    destination address http
https://tools.cisco.com
/its/service/oddce/services/DDCEService
!
! check connectivity
!
#telnet tools.cisco.com 443 /source-interface gi0/0
Trying tools.cisco.com (x.x.x.x, 443)... Open
[Connection to tools.cisco.com closed by foreign host]
```

上のコマンドが機能しない場合は、ルーティングルール、送信元インターフェイス、およびファイアウォール設定をダブルチェックします。

---

注：HTTP ( TCP/80 ) は廃止されており、HTTPS ( TCP/443 ) が推奨のプロトコルとなっています。

---

DNS および HTTP の詳細設定に関する詳しいガイドラインについては、セクション「3. 考慮事項と注意事項」を参照してください。

### 3. スマートライセンスの設定を確認する

次の出力を収集します。

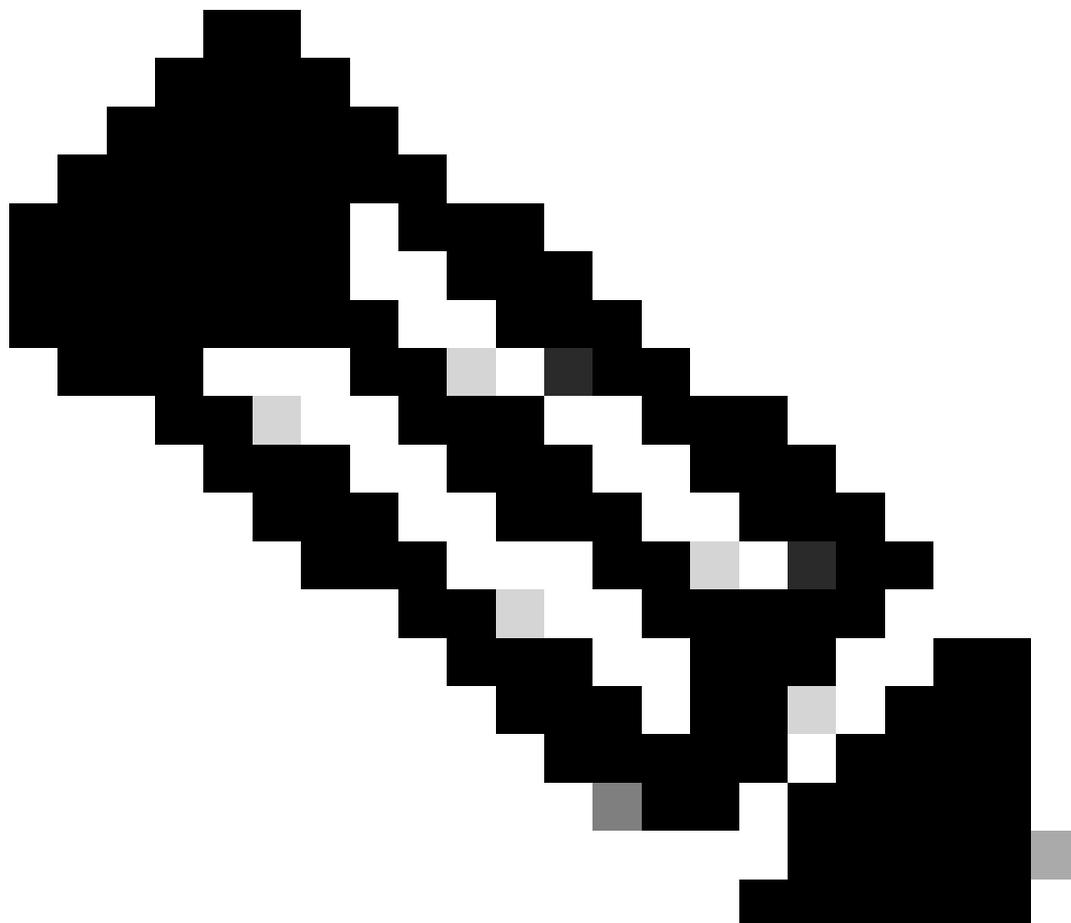
```
#show tech-support license
```

収集した設定/ログを確認します ( 詳細な調査のために Cisco TAC のケースをオープンする場合は、この出力を添付します ) 。

#### 4. デバッグをイネーブルにする

スマートライセンスプロセスに関する追加情報を収集するには、これらのデバッグを有効にします。

---



注：デバッグを有効にした後、ポイント 4.1 で説明したように、CLI を使用してライセンスを再度登録する必要があります。

---

```
#debug call-home smart-licensing [all | trace | error]
#debug ip http client [all | api | cache | error | main | msg | socket]
```

内部デバッグの場合は、バイナリトレースを有効にして内容を確認します。

```
! enable debug
#set platform software trace ios [switch] active R0 infra-s1 debug
```

```
!  
! read binary traces infra-s1 process logs  
#show platform software trace message ios [switch] active R0
```

## 一般的な失敗のシナリオ

このセクションでは、シスコデバイスの登録中または登録後に発生する可能性がある、一般的な失敗のシナリオのいくつかについて説明します。

### シナリオ #1 : スイッチ登録 "Failure Reason: Product Already Registered"

「show license all」の一部 :

Registration:

Status: UNREGISTERED - REGISTRATION FAILED

輸出規制機能 : NotAllowed

初期登録 : FAILED on Oct 22 14:25:31 2018 EST

失敗の理由 : Product Already Registered

次回の登録試行 : Oct 22 14:45:34 2018 EST

次のステップ :

- シスコデバイスをもう一度登録する必要があります。
- CSSM にシスコデバイスが表示されている場合は、force パラメータを使用する必要があります ( license smart register idtoken <TOKEN> force を使用 ) 。

---

 注 : 失敗の理由は、次のように表示されることもあります。

- Failure reason: The product <X> and sudi containing udiSerialNumber:<SerialNumber>,udiPid:<Product> has already been registered.
  - Failure reason: Existing Product Instance has Consumption and Force Flag is False
- 

### シナリオ #2 : スイッチ登録 "Failure Reason: Your Request could not be Processed Right Now>Please try again ) 」

「show license all」の一部 :

Registration:

ステータス : REGISTERING - REGISTRATION IN PROGRESS

輸出規制機能 : NotAllowed

初期登録 : FAILED on Oct 24 15:55:26 2018 EST

Failure reason: Your request could not be processed right now. Please try again

次回の登録試行 : Oct 24 16:12:15 2018 EST

次のステップ :

- セクション 4 に記載されているようにデバッグを有効にして問題の詳細情報を取得します。
- CSSM でスマートライセンスの新しいトークンを生成してもう一度試みます。

シナリオ #3 : "Failure Reason: The Device Date 1526135268653 is Offset beyond the Allowed Tolerance Limit"

「show license all」の一部 :

Registration:

ステータス : REGISTERING - REGISTRATION IN PROGRESS

輸出規制機能 : NotAllowed

初期登録 : FAILED on Nov 11 17:55:46 2018 EST

Failure reason: {"timestamp": ["The device date '1526135268653' is offset beyond the allowed tolerance limit."]}

次回の登録試行 : Nov 11 18:12:17 2018 EST

表示される可能性のあるログ :

```
%PKI-3-CERTIFICATE_INVALID_NOT_YET_VALID: Certificate chain validation has failed. The certificate (SN: XXXXXX) is not yet valid. Validity period starts on 2018-12-12:43Z
```

次のステップ :

- シスコデバイスのクロックに正しい時刻が表示されていることを確認します ( show clock )。
- クロックが正しく設定されるように、可能な場合は Network Time Protocol ( NTP ) を設定します。
- NTP を設定できない場合は、clock calendar-valid が設定されていることを確認し、手動で設定したクロック ( clock set ) が正しく ( show clock )、信頼できるタイムソースとして設定されていることを確認します。

---

 注 : デフォルトのシステムクロックは信頼できません。clock calendar-valid を実行する必要

---

---

 があります。

---

## シナリオ #4 : スイッチ登録 "Failure Reason: Communication Transport not Available"

「show license all」の一部 :

ステータス : UNREGISTERED - REGISTRATION FAILED

輸出規制機能 : NotAllowed

初期登録 : FAILED on Mar 09 21:42:02 2019 CST

失敗の理由 : Communication transport not available.

表示される可能性のあるログ :

%CALL\_HOME-3-CALL\_HOME\_FAILED\_TO\_ENABLE: Failed to enable call-home from Smart Agent for Licensing: The command failed to enable smart call home due to an existing active user profile.If you are using a user profile other than CiscoTAC-1 profile to send data to SCH server in Cisco, enter reporting smart-licensing-data under profile mode to configure that profile for smart licensing.For more details about SCH, check <http://www.cisco.com/go/smartcallhome>

%SMART\_LIC-3-AGENT\_REG\_FAILED: Smart Agent for Licensing Registration with the Cisco Smart Software Manager or satellite failed: Communication transport not available.

%SMART\_LIC-3-COMM\_FAILED: Communications failure with the Cisco Smart Software Manager or satellite: Communication transport not available.

次のステップ :

- シスコデバイスの show running-config の出力で service call-home によって Call Home が有効になっていることを確認します。
- 正しい Call Home プロファイルがアクティブになっていることを確認します。
- アクティブな Call Home プロファイルで reporting smart-licensing-data が設定されていることを確認します。

## シナリオ #5 : スイッチライセンス承認 "Failure Reason: Fail to Send out Call Home HTTP Message"

「show license all」の一部 :

License Authorization:

ステータス : OUT OF COMPLIANCE on Jul 26 09:24:09 2018 UTC

最後の通信試行 : FAILED on Aug 02 14:26:23 2018 UTC

失敗の理由 : Fail to send out Call Home HTTP message.

次回の通信試行 : Aug 02 14:26:53 2018 UTC

通信期限 : Oct 25 09:21:38 2018 UTC

表示される可能性のあるログ :

```
%CALL_HOME-5-SL_MESSAGE_FAILED: Fail to send out Smart Licensing message to: https://<ip>/its/service/oddce/services/DDCEService (ERR 205 : Request Aborted)
```

```
%SMART_LIC-3-COMM_FAILED:Communications failure with the Cisco Smart Software Manager or satellite: Fail to send out Call Home HTTP message.
```

```
%SMART_LIC-3-AUTH_RENEW_FAILED:Authorization renewal with the Cisco Smart Software Manager or satellite: Communication message send error for udi PID:XXX, SN: XXX
```

次のステップ :

- シスコデバイスで tools.cisco.com を ping できることを確認します。
- DNS が設定されていない場合は、tools.cisco.com のローカル nslookup IP に DNS サーバーを指定するか、ip host ステートメントを設定します。
- TCP ポート 443 ( HTTPS で使用するポート ) でシスコデバイスから tools.cisco.com への telnet を試行します。
- HTTPS クライアントの送信元インターフェイスが正しく定義されていることを確認します。
- show call-home profile all を使用して、シスコデバイスで Call Home プロファイルの URL/IP が正しく設定されていることを確認します。
- IP ルートが正しいネクストホップを指していることを確認します。
- シスコデバイス、Smart Call Home サーバーへのパス、または Cisco Smart Software Manager オンプレミス ( サテライト ) で TCP ポート 443 がブロックされていないことを確認します。
- 正しい Virtual Routing and Forwarding ( VRF ) インスタンスが設定されていることを Call Home 設定で確認します ( 該当する場合 ) 。

シナリオ #6 : "Failure Reason: Missing Id Cert Serial Number Field; Missing Signing Cert Serial Number Field; Signed Data and Certificate does not Match" ログ

この動作は [Cisco Bug ID CSCvr41393](#) で説明されているように、使用している CSSM オンプレミスサーバーの暗号化用証明書の有効期限が切れている場合に見られます。これは正常な動作で、登録デバイスとの証明書の同期に問題が生じないように、CSSM オンプレミスで証明書の同期および更新を許可する必要があるために生じます。

「show license all」の一部：

Registration:

ステータス: UNREGISTERED  
スマートアカウント : Example Account  
輸出規制機能 : ALLOWED

License Authorization:

ステータス: EVAL MODE  
残りの評価期間 : 65 days, 18 hours, 43 minutes, 0 seconds

表示される可能性のあるログ：

show logging または show license eventlog 以下に、次のエラーが表示されます。  
SAEVT\_DEREGISTER\_STATUS msgStatus="LS\_INVALID\_DATA" error="Missing Id cert serial number field; Missing signing cert serial number field; Signed data and certificate does not match"

次のステップ：

- シスコデバイスで CSSM オンプレミスサーバーとの IP 接続が確立されていることを確認します。
- HTTPS を使用している場合は、証明書 の CNAME がデバイスの Call Home 設定で使用されていることを確認します。
- DNS サーバーで証明書の CNAME を解決できない場合は、静的な ip host ステートメントを記述して、ドメイン名と IP アドレスをマッピングします。
- CSSM オンプレミス証明書の有効期限が切れていないことを確認します。
- CSSM オンプレミス証明書の有効期限が切れている場合は、[Cisco Bug ID CSCvr41393](#) に記載されている解決策のいずれかに従ってください。

---

 注：デフォルトでは、HTTPS は SSL ハンドシェイクのときにサーバー ID をチェックして、URL または IP がサーバーから提供された証明書と同じであることを確認します。この動作により、ホスト名と IP が一致していない場合に DNS エントリではなく IP アドレスを使用していると、問題が起きる可能性があります。DNS が使用できない場合、または静的な ip host ステートメントを使用する場合は、no http secure server-identity-check を設定することで、この証明書チェックを無効にできます。

---

## シナリオ #7：スイッチライセンス承認 "Failure reason: Waiting for reply"

「show license all」の一部：

License Authorization:

ステータス : OUT OF COMPLIANCE on Jul 26 09:24:09 2018 UTC  
最後の通信試行 : PENDING on Aug 02 14:34:51 2018 UTC  
失敗の理由 : Waiting for reply  
次の通信試行 : Aug 02 14:53:58 2018 UTC

通信期限 : Oct 25 09:21:39 2018 UTC

表示される可能性のあるログ :

```
%PKI-3-CRL_FETCH_FAIL: CRL fetch for trustpoint SLA-TrustPoint failed Reason :  
Failed to select socket.Timeout : 5 (Connection timed out)
```

```
%PKI-3-CRL_FETCH_FAIL: CRL fetch for trustpoint SLA-TrustPoint failed Reason :  
Failed to select socket.Timeout : 5 (Connection timed out)
```

次のステップ :

- この問題を修正するには、実行コンフィギュレーションで SLA-TrustPoint を none に設定する必要があります。

```
show running-config
```

```
<omitted>
```

```
crypto pki trustpoint SLA-TrustPoint
```

```
revocation-check none
```

CRL とは

証明書失効リスト ( CRL ) とは、失効した証明書のリストです。CRL は、証明書を発行した認証局 ( CA ) によって作成され、デジタル署名されます。CRL には、各証明書の発行日と失効日が含まれています。CRL の詳細については、[こちら](#)を参照してください。

## シナリオ #8 : ステータスが "OUT OF COMPLIANCE" のライセンス

「show license all」の一部 :

```
License Authorization:
```

```
ステータス : OUT OF COMPLIANCE on Jul 26 09:24:09 2018 UTC
```

```
最後の通信試行 : PENDING on Aug 02 14:34:51 2018 UTC
```

```
失敗の理由 : Waiting for reply
```

```
次回の通信試行 : Aug 02 14:53:58 2018 UTC
```

```
通信期限 : Oct 25 09:21:39 2018 UTC
```

表示される可能性のあるログ :

```
%SMART_LIC-3-OUT_OF_COMPLIANCE: One or more entitlements are out of  
compliance.
```

次のステップ :

- 適切なスマート パーチャル アカウントのトークンが使用されているかどうかを確認します。

- [ここ](#)で使用可能なライセンスの数を確認します。

## シナリオ #9 : スイッチライセンス承認 "Failure Reason: Data and Signature do not Match "

「show license all」の一部 :

License Authorization:

ステータス : AUTHORIZED on Mar 12 09:17:45 2020 EDT

最後の通信試行 : FAILED on Mar 12 09:17:45 2020 EDT

失敗の理由 : Data and signature do not match

次の通信試行 : Mar 12 09:18:15 2020 EDT

通信期限 : May 09 21:22:43 2020 EDT

表示される可能性のあるログ :

```
%SMART_LIC-3-AUTH_RENEW_FAILED: Authorization renewal with the Cisco Smart Software Manager (CSSM) : Error received from Smart Software Manager: Data and signature do not match for udi PID:C9000,SN:XXXXXXXXXXXX
```

次のステップ :

- license smart deregister コマンドでスイッチの登録を解除します。
- 次に、license smart register idtoken <TOKEN> force コマンドで、新しいトークンを使用して同じスイッチを登録します。

## 参考資料

- 1) [Cisco Smart Licensing のホームページ](#)
- 2) [シスココミュニティ - オンデマンドトレーニング](#)。
- 3) スマートアカウント - 管理ポータル : [スマート ソフトウェア ライセンシング](#)
- 4) スマートアカウント - 新しいアカウントの作成 : [スマートアカウント](#)
- 5) コンフィギュレーション ガイド ( 例 ) - 『[System Management Configuration Guide, Cisco IOS XE Fuji 16.9.x \(Catalyst 9300 Switches\)](#)』

## 翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。