

Cisco Catalyst 9000 シリーズ スイッチでのライセンスの設定

Cisco Catalyst 9000 シリーズ スイッチでのライセンスの設定

ここでは、Cisco IOS-XE ソフトウェアを実行している Cisco Catalyst 9000 シリーズ スイッチで使用可能なライセンスについて説明します。使用可能なライセンスを設定する方法を示し、コンプライアンスを確保するために使用しているライセンスの使用状況をレポートする方法の概要を示します。

入手可能なライセンス

この項では、Cisco Catalyst 9000 シリーズ スイッチで使用可能なすべてのライセンス、ライセンス使用ガイドライン、および注文に関する考慮事項について説明します。

基本ライセンスとアドオンライセンス

基本ライセンスとは、永続的に有効な永久ライセンスです。こうしたライセンスには使用期限日はありません。

アドオンライセンスは、スイッチおよび Cisco Catalyst Center でのシスコのイノベーションを提供します。このライセンスには有効期間が定義されていて、3年、5年、または7年のサブスクリプション期間で使用できます。

次の表に、Cisco Catalyst 9000 シリーズ スイッチでの基本ライセンスとアドオンライセンスの可用性を示します。

製品	使用可能な基本ライセンス	使用可能なアドオンライセンス
Cisco Catalyst 9200 シリーズ スイッチ	Network Essentials	DNA Essentials
Cisco Catalyst 9300 シリーズ スイッチ	Network Advantage	DNA Advantage
Cisco Catalyst 9400 シリーズ スイッチ		
Cisco Catalyst 9500 シリーズ スイッチ		
Cisco Catalyst 9600 シリーズ スイッチ	Network Advantage	DNA Advantage

詳細については、「[Cisco Catalyst and Cisco DNA Software Subscription Matrix for Switching](#)」を参照してください。

ライセンスと機能のマッピングの情報

Cisco Catalyst 9000 シリーズ スイッチで使用可能なソフトウェア機能には、基本ライセンスまたはアドオンライセンスが必要です。

機能を使用できるライセンスレベルを確認するには、<https://cfngng.cisco.com> にある Cisco Feature Navigator を使用します。cisco.com のアカウントは必要ありません。

基本ライセンスとアドオンライセンスに関する発注ガイドライン

- 基本ライセンスの注文および履行は、無期限または永久ライセンスタイプのみとなります。
- アドオンライセンスの注文および履行は、サブスクリプションまたは有効期間付きライセンスタイプのみとなります。
- ネットワーク ライセンス レベルを選択した場合はアドオンライセンスレベルが含まれています。Cisco DNA 機能を引き続き使用するには、期間が終了する前にアドオンライセンスを更新する必要があります。

アドオンライセンスを非アクティブ化した後にスイッチをリロードすると、使用を中止できます。その後、スイッチは基本ライセンス機能で動作を継続します。

- 基本ライセンスとともにアドオンライセンスを購入する場合、許可されている組み合わせと、許可されていない組み合わせに注意してください。

Figure 1: 許可されている基本ライセンスとアドオンライセンスの組み合わせ

	DNA Essentials	DNA Advantage
Network Essentials	Yes	No
Network Advantage	Yes	Yes



Note

Network Advantage と Cisco DNA Essentials の組み合わせは Cisco DNA ライセンスの更新時にのみ使用でき、Cisco DNA Essentials の初回購入時は使用できません。

これらのライセンスの発注の詳細については、対応する発注ガイドを参照してください。

[Cisco Catalyst 9200 Series Switches Ordering Guide](#)

[Cisco Catalyst 9300 Series Switches Ordering Guide](#)

[Cisco Catalyst 9400 Series Switches Ordering Guide](#)

[Cisco Catalyst 9500 Series Switches Ordering Guide](#)

[Cisco Catalyst 9600 Series Switches Ordering Guide](#)

高セキュリティのための輸出規制キーまたは HSECK9 キー

暗号化機能を提供する製品および機能は、米国輸出規制法、米国政府暗号化および輸出管理規則（EAR）の範囲内です。

高セキュリティの輸出規制キー（HSECK9 キー）は、暗号化機能の使用を許可する輸出規制ライセンスです。

この項では、HSECK9 キーをサポートする Cisco Catalyst 9000 シリーズ スイッチ、HSECK9 キーを必要とするこれらの製品の暗号化機能、注文する際の考慮事項、前提条件、およびサポートされるプラットフォームでの設定方法について説明します。

HSECK9 キーが必要になる場合と HSECK9 キーをサポートしている製品

HSECK9 キーは、米国の輸出規制法の制限対象である、特定の暗号化機能を使用する場合にのみ必要です。これがないと、制限対象の暗号化機能を有効にできません。

この表は、HSECK9 キーをサポートしている製品、サポートが導入されたタイミング、および製品でサポートされている HSECK9 キーを必要とする暗号化機能を示しています。

Table 1: HSECK9 キーの製品のサポートおよびリリース

HSECK9 は次の製品でサポート...	このリリース以降...	対象の暗号化機能...
Cisco Catalyst 9300X シリーズ スイッチ このシリーズの SKU の詳細については、ハードウェア設置ガイドの「 Switch Models 」を参照してください。	Cisco IOS XE Bengaluru 17.6.2	IPsec
Cisco Catalyst 9600 シリーズ スーパーパライザエンジン2 (C9600X-SUP-2) および関連するラインカード	Cisco IOS XE Cupertino 17.8.1	WAN MACsec 具体的には、WAN MACsec 機能が設定されている、ポイントツーポイント (P2P) およびポイントツーマルチポイント (P2MP) ネットワークのカスタマーエッジデバイス
Cisco Catalyst 9500X シリーズ スイッチ このシリーズの SKU の詳細については、ハードウェア設置ガイドの「 Switch Models 」を参照してください。	Cisco IOS XE Cupertino 17.8.1	
Cisco Catalyst 9400 シリーズ スーパーパライザ2 および 2XL モジュール (C9400X-SUP-2 および C9400X-SUP-2XL)	Cisco IOS XE Dublin 17.11.1	IPSec

HSECK9 キーを使用するための前提条件

- プラットフォームのサポートを確認します。


HSECK9 キーを使用するデバイスが、HSECK9 キーをサポートしているデバイスであることを確認します。「[HSECK9 キーが必要になる場合と HSECK9 キーをサポートしている製品](#)」を参照してください。

- 前提条件ライセンスが設定されていることを確認します。

デバイスで Cisco DNA Advantage ライセンスが設定されていることを確認します。DNA Advantage が設定されていない場合、HSECK9 キーを使用することはできません。

- 必要な数の HSECK9 キーの可用性を確認します。

Cisco Smart Software Manager (Cisco SSM) の該当するスマートアカウントおよびバーチャルアカウントに必要な数の HSECK9 キーがあることを確認します。次のプラットフォーム固有のガイドラインが、HSECK9 キーの必要数を評価するために役立ちます。

プラットフォーム	HSECK9 キーの必要数を評価する方法
Cisco Catalyst 9300X シリーズ スイッチ	暗号化機能を使用する UDI ごとに、1 つの HSECK9 キーが必要です。 スタック構成セットアップのコンテキストでこの要件を理解して評価するには、「 Cisco Catalyst 9300X シリーズ スイッチのスタック構成に関する考慮事項 」を参照してください。
Cisco Catalyst 9500X シリーズ スイッチ	暗号化機能を使用する UDI ごとに、1 つの HSECK9 キーが必要です。  Note Cisco Catalyst 9500X シリーズ スイッチでは、HSECK9 キーはスタンドアロンセットアップでのみサポートされます。
Cisco Catalyst 9400 シリーズ スーパーバイザ2および2XL モジュールと Cisco Catalyst 9600 シリーズ スーパーバイザ エンジン 2	モジュラスイッチの場合、HSECK9 キーはシャーシに関連付けられています。 シャーシに取り付けられているスーパーバイザモジュールの数に関係なく、暗号化機能を使用するシャーシUDI ごとにのみ、個別の HSECK9 キーが必要です。 高可用性セットアップのコンテキストでこの要件を理解して評価するには、「 Cisco Catalyst 9400 および 9600 シリーズ スイッチの高可用性に関する考慮事項 」を参照してください。

- ポリシーを使用したスマートライセンスのトポロジを導入します。

HSECK9 キーは、米国の取引規制法（輸出規制）の制限対象であるため、使用前に承認が必要です。この承認は、Cisco SSM から取得してデバイスにインストールする必要があるスマートライセンス承認コード（SLAC）によって提供されます。

デバイスに SLAC をインストールすると、HSECK9 キーのアクティブ化と使用が可能になります。

デバイスを Cisco SSM に接続して SLAC を取得する方法はいくつかあります。Cisco SSM に接続するための各方法はトポロジと呼ばれ、ポリシーを使用したスマート ライセンシング ソリューションのフレームワーク内にあります。

SLAC を取得できるように、サポートされているポリシーを使用したスマートライセンスのトポロジのいずれかを実装します。



Note

このドキュメントの範囲内にあるサポート対象プラットフォームで SLAC を取得してインストールするには、このドキュメントの設定の項を参照してください。他のシスコ製品と比較すると、設定プロセスに違いがあります。

- 正しい順序に従ってください。

必ず最初にデバイスにSLACをインストールしてから、暗号化機能を設定します。インストール前に暗号化機能を設定した場合、SLACのインストール後に再設定する必要があります。

- 適切なインターフェイスを設定します（Cisco Catalyst 9600 シリーズ スーパーバイザ エンジン 2 のみ）。

暗号化機能を設定するインターフェイスは、暗号化機能をサポートするラインカードが取り付けられているラインカードスロットに対応している必要があります。

HSECK9 キーの発注時の考慮事項

注文する新しいハードウェア（サポートされているプラットフォーム）で暗号化機能を使用する予定の場合は、スマートアカウントとバーチャルアカウントの情報を注文時に提供します。これにより、SLACを工場ですべてインストールできるため、ユーザーが行う必要がなくなります。

Cisco Catalyst 9300X シリーズ スイッチのスタック構成に関する考慮事項

このセクションでは、アクティブ、スタンバイ、および1つ以上のメンバーを持つデバイススタックに適用されるHSECK9の考慮事項と要件について説明します。そのため、これはCisco Catalyst 9300X シリーズ スイッチにのみ適用されます。

- 混合スタック構成はサポートされていません。スタック内のすべてのデバイスは、Cisco Catalyst 9300X シリーズ スイッチである必要があります。シリーズで使用可能なC9300X SLUの詳細については、『[Cisco Catalyst 9300 Series Switches Hardware Installation Guide](#)』 [英語] を参照してください。
- 最低限、HSECK9キーを取得し、スタック内のアクティブデバイスのSLACをインストールします。スイッチオーバー時に暗号化機能を中断なく使用するため、スタンバイ用のHSECK9キーも取得することを推奨します。次のシナリオを考えます。

シナリオ 1: スタック内のスタンバイデバイスもHSECK9キーを使用していて、SLACがインストールされている場合、スイッチオーバーが発生すると、システムは新しいアクティブでの暗号化機能の動作を中断することなく続行します。

シナリオ 2: スタック内のスタンバイデバイスがHSECK9キーを使用していない場合は、毎日のシステムメッセージとスイッチオーバー中のシステムメッセージが表示されます。

現在のスタンバイに必要なHSECK9キーがなく、スイッチオーバーが発生すると暗号化機能が無効になる可能性があることを警告する毎日のシステムメッセージ。現在アクティブなデバイスのHSECK9対応機能の動作には影響しません。

```
IOSXE_SMART_AGENT-6-STANDBY_NOT_AUTHORIZED: Standby is in 'not authorized' state for license hseck9
```

スイッチオーバーが発生し、HSECK9キーを持たないスタンバイが新しいアクティブになると、デバイスがリロードされる前にこれらのシステムメッセージが表示されます。

```
%PLATFORM_IPSEC_HSEC-3-UNAUTHORIZED_HSEC: Switchover happened with IPsec configured but HSEC unauthorized, reloading.
```

```
%PMAN-5-EXITACTION: F0/0: pvp: Process manager is exiting: reload fp action requested
```

```
%PMAN-5-EXITACTION: R0/0: pvp: Process manager is exiting: rp processes exit with reload switch code
```

リロード後のスタック起動時に生じ得る結果が2つあります。

リロード後のスタックブートアップ時に選択された次の新しいアクティブにHSECK9キーがある場合、スタートアップコンフィギュレーションの暗号化機能が適用されるか受け入れられ、システムによる暗号化機能の動作が再開されます。

リロード後のスタックブートアップ時に選択された次の新しいアクティブにも HSECK9 キーがない場合、スタートアップ コンフィギュレーションの暗号化機能は拒否され、スタック全体で暗号化機能が無効になります。

- 暗号化機能がすでに使用されている既存のスタックにデバイスを追加するには、次のいずれかの手順を実行します。

デバイスをスタックに追加し、スタック全体の SLAC を再度要求します。C9300X の例: HSECK9 キーが使用されているスタックへのメンバーの追加, on page 27を参照してください。

または

スタンドアロンデバイスに SLAC をインストールし、スタンドアロンデバイスで暗号化機能を設定して、最後に既存のスタックにデバイスを追加します。C9300X の例: スタンドアロンでの SLAC の要求と HSECK9 キーが使用されているスタックへの追加, on page 31を参照してください。

Cisco Catalyst 9400 および 9600 シリーズ スイッチの高可用性に関する考慮事項

この項では、Cisco Catalyst 9400 および 9600 シリーズ スイッチで HSECK9 キーを使用する場合に適用される高可用性に関する考慮事項について説明します。

サポートされる高可用性セットアップ	サポートされるプラットフォーム
デュアル スーパーバイザ セットアップ このセットアップでは、2つのスーパーバイザモジュールがシャーシに取り付けられています。1つはアクティブで、もう1つはスタンバイです	Cisco Catalyst 9600 シリーズ スイッチ および Cisco Catalyst 9400 シリーズ スイッチでサポートされています。
Cisco StackWise Virtual セットアップ このセットアップでは、2つのシャーシが関与しています。各シャーシに1つのスーパーバイザモジュールが取り付けられています。1つはアクティブで、もう1つはスタンバイです。	Cisco Catalyst 9400 シリーズ スイッチ でサポートされています。

どちらの高可用性セットアップでも、信頼コード、SLAC、RUM レポートなどのすべてのライセンス情報はアクティブスーパーバイザ（アクティブ製品インスタンス）に保存され、スタンバイと同期されます。

Note

Cisco Catalyst 9500X シリーズ スイッチで HSECK9 キーを使用する場合、高可用性セットアップはサポートされません。

高可用性セットアップに必要な HSECK9 キーの数

HSECK9 キーはシャーシ UDI に関連付けられているため、取り付けられているスーパーバイザの数に関係なく、シャーシ UDI ごとに1つの HSECK9 キーが必要です。この要件は、サポートされている高可用性セットアップに対して次のように言い換えられます。

デュアル スーパーバイザ セットアップ

デュアル スーパーバイザ セットアップでは、暗号化機能を使用するシャーシ UDI ごとに、1つの HSECK9 キーが必要です。

次の出力例は、デュアルスーパーバイザセットアップでシャーシ UDI がどのように表示されるかを示しています。アクティブとスタンバイに対して同じシャーシ UDI が表示されることに注目してください。

```
Device# show license udi
UDI: PID:C9606R,SN:FXS241201WP <<<< chassis UDI
```

```
HA UDI List:
  Active:PID:C9606R,SN:FXS241201WP
  Standby:PID:C9606R,SN:FXS241201WP
```

Cisco StackWise Virtual セットアップ

Cisco StackWise Virtual セットアップでは、少なくとも、アクティブ スーパーバイザ モジュールを搭載したシャーシの HSECK9 キーを取得する必要があります。ただし、スイッチオーバー時に暗号化機能を中断なく使用するため、両方のシャーシの HSECK9 キーを取得することを推奨します。

この出力例は、Cisco StackWise Virtual セットアップでシャーシ UDI がどのように表示されるかを示しています。ここでの最小要件は、シャーシ UDI C9407R,SN:FXS221500CT の HSECK9 キーを取得することです。スイッチオーバー時に暗号化機能を中断なく使用するには、C9407R,SN:FXS221500BN の HSECK9 キーも取得する必要があります。

```
Device# show license udi
UDI: PID:C9407R,SN:FXS221500CT <<<<<< UDI of chassis with active supervisor
```

```
HA UDI List:
  Active:PID:C9407R,SN:FXS221500CT
  Standby:PID:C9407R,SN:FXS221500BN <<<<<< UDI of chassis with standby supervisor
```

高可用性セットアップに必要な SLAC

各 HSECK9 キーには 1 つの SLAC が必要です。

デュアルスーパーバイザ セットアップ

デュアルスーパーバイザセットアップでは、アクティブとスタンバイのスーパーバイザモジュールが同じシャーシ内にあり、同じ UDI を持っているため、これらに対して同じ SLAC 確認コードが表示されます。

この出力例は、SLAC 情報がどのように表示されるかを示しています。同じ UDI を持っているため、接続されているすべてのデバイスに同じ SLAC 確認コードが表示されることに注目してください。また、HSECK9 キーについては、Total available count に注目してください。各シャーシに必要なキーは 1 つだけです。

```
Device# show license authorization
Overall status:
  Active: PID:C9606R,SN:FXS241201WP
    Status: SMART AUTHORIZATION INSTALLED on Dec 13 05:18:07 2021 UTC
    Last Confirmation code: 7cf1f54a <<<<<< Confirmation code on active.
  Standby: PID:C9606R,SN:FXS241201WP
    Status: SMART AUTHORIZATION INSTALLED on Dec 13 05:18:07 2021 UTC
    Last Confirmation code: 7cf1f54a <<<<<< Same confirmation code on standby.
```

```
Authorizations:
  C9K HSEC (Cat9K HSEC):
    Description: HSEC Key for Export Compliance on Cat9K Series Switches
    Total available count: 1
```

<output truncated>

Cisco StackWise Virtual セットアップ

Cisco StackWise Virtual セットアップでは、各シャーシ UDI に独自の HSECK9 キーと独自の SLAC が必要です。そのため、アクティブとスタンバイの確認コードは異なります。

Device# **show license authorization**

Overall status:

Active: PID:C9407R,SN:FXS221500CT <<<<<< UDI of the chassis with active supervisor
Status: SMART AUTHORIZATION INSTALLED on Jul 07 10:14:04 2022 PDT
Last Confirmation code: 40ba43d2 <<<<<< Confirmation code for chassis with active supervisor

Standby: PID:C9407R,SN:FXS221500BN <<<<<< UDI of the chassis with standby supervisor
Status: SMART AUTHORIZATION INSTALLED on Jul 07 10:13:45 2022 PDT
Last Confirmation code: 649e8b1d <<<<<< Confirmation code for chassis with standby supervisor

Authorizations:

C9K HSEC (Cat9K HSEC):

Description: HSEC Key for Export Compliance on Cat9K Series Switches

Total available count: 2

Enforcement type: EXPORT RESTRICTED

Term information:

Active: PID:C9407R,SN:FXS221500CT

Authorization type: SMART AUTHORIZATION INSTALLED

License type: PERPETUAL

Term Count: 1

Standby: PID:C9407R,SN:FXS221500BN

Authorization type: SMART AUTHORIZATION INSTALLED

License type: PERPETUAL

Term Count: 1

Purchased Licenses:

No Purchase Information Available

スイッチオーバー中のシステムの動作

スイッチオーバー時のシステムの動作は、高可用性セットアップに応じて異なります。

デュアル スーパーバイザ セットアップ

デュアル スーパーバイザ セットアップでは、システムはスイッチオーバー時に暗号化機能の動作を中断することなく続行します。

HSECK9 キーはスーパーバイザモジュールではなくシャーシ UDI に関連付けられ、アクティブのライセンス情報がスタンバイと同期されるため、この高可用性セットアップでのスイッチオーバーによって暗号化機能の動作が中断されることはありません。

Cisco StackWise Virtual セットアップ

Cisco StackWise Virtual セットアップでは、スイッチオーバー時のシステムの動作は、スタンバイ スーパーバイザモジュールを搭載したシャーシに HSECK9 キーがあるかどうかによって決まります。

次のシナリオを見てみましょう。

シナリオ 1: スタンバイに HSECK9 キーがあり、スイッチオーバーが発生すると、システムは新しいアクティブでの暗号化機能の動作を中断することなく続行します。

シナリオ 2: スタンバイに HSECK9 キーがなく、スイッチオーバーが発生すると、次のイベントが発生します。

- 現在のスタンバイに必要な HSECK9 キーがなく、スイッチオーバーが発生すると暗号化機能が無効になる可能性があることを警告する毎日のシステムメッセージ。現在アクティブなデバイスの HSECK9 対応機能の動作には影響しません。

```
%IOSXE_SMART_AGENT-6-STANDBY_NOT_AUTHORIZED: Standby is in 'not authorized' state  
for license hseck9
```


- スイッチオーバーが発生すると、HSECK9キーを持たないスタンバイが新しいアクティブになり、新しいアクティブにHSECK9キーがなく、デバイスがリロード中であることを警告するシステムメッセージが表示されます。

```
%PLATFORM_IPSEC_HSEC-3-UNAUTHORIZED_HSEC: Switchover happened with IPsec configured
but HSEC unauthorized, reloading.
%PMAN-5-EXITACTION: F0/0: pvp: Process manager is exiting: reload fp action requested
%PMAN-5-EXITACTION: R0/0: pvp: Process manager is exiting: rp processes exit with reload switch code
```

リロード後のブートアップで生じ得る結果が2つあります。

リロード後のブートアップ時に選択された次の新しいアクティブにHSECK9キーがある場合、スタートアップコンフィギュレーションの暗号化機能が適用されるか受け入れられ、システムによる暗号化機能の動作が再開されます。

リロード後のブートアップ時に選択された次の新しいアクティブにもHSECK9キーがない場合、スタートアップコンフィギュレーションの暗号化機能は拒否され、暗号化機能が無効になります。

Cisco Catalyst 9400 および 9600 シリーズ スイッチのハードウェアの取り外しと交換に関する考慮事項

この項では、Cisco Catalyst 9400 および 9600 シリーズ スイッチでHSECK9キーを使用する場合に適用されるハードウェアの取り外しと交換に関する考慮事項について説明します。

- Cisco Catalyst 9400 および 9600 シリーズ スイッチの場合:

HSECK9 キーはシャーシに関連付けられています。

ライセンス情報は、アクティブ製品インスタンス（アクティブ スーパーバイザ モジュール）に保存されます。高可用性セットアップでは、ライセンス情報はスタンバイと同期されます。

- Cisco Catalyst 9600 シリーズ スイッチの場合:

暗号化機能は、インターフェイス コンフィギュレーション モードで設定します。これは、暗号化機能をサポートするラインカードが取り付けられているラインカードスロットに対応しています。

交換用のラインカードが同じラインカードスロットに取り付けられている限り、暗号化機能の動作を中断することなく、ラインカードの取り外しと交換を行うことができます。

スーパーバイザモジュールまたはラインカードを取り外して交換する場合は、次のガイドラインに従ってください。

シングル スーパーバイザ セットアップ

シングルスーパーバイザセットアップでは、アクティブスーパーバイザモジュールを取り外して別のものと交換する場合は、SLACを再度インストールする必要があります。

同じスーパーバイザモジュールを取り外して再度取り付ける場合は、SLACを再インストールする必要はありません。

デュアル スーパーバイザ セットアップと Cisco StackWise Virtual セットアップ

デュアルスーパーバイザセットアップ（Cisco Catalyst 9400 および 9600 シリーズ スイッチ）と Cisco StackWise Virtual セットアップ（Cisco Catalyst 9400 シリーズ スイッチのみ）では、一度に1つのスーパーバイザモジュールを取り外して交換します。

アクティブで開始してから次にスタンバイで作業することも、その逆も可能です。スーパーバイザモジュールを一度に1つずつ取り外して交換することで、必要なライセンス情報を常にデバイスに保持できます。また、中断されることなく暗号化機能を動作させることができます。両方のスーパーバイザモジュールを同時に取り外して他のスーパーバイザモジュール

ルと交換すると、必要なライセンス情報がデバイスで使用できなくなるため、SLACを再度インストールする必要があります。

同じスーパーバイザモジュールを取り外して再度取り付ける場合は、SLACを再インストールする必要はありません。

ラインカードの取り外しと交換

交換用のラインカードが同じラインカードスロットに取り付けられている限り、暗号化機能の動作を中断することなく、ラインカードの取り外しと交換を行うことができます。

暗号化機能が設定されているラインカードを取り外し、交換用のラインカードを別のスロットに取り付けた場合は、暗号化機能を再設定する必要があります。

取り外しと交換の手順については、対応するハードウェアに関するドキュメントを参照してください。

「[Cisco Catalyst 9400 Series Supervisor Module Installation Note](#)」。

「[Cisco Catalyst 9600 Series Supervisor Engine Installation Note](#)」および「[Cisco Catalyst 9600 Series Line Card Installation Note](#)」。

基本ライセンスとアドオンライセンスの設定

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

このタスクではライセンスレベルを設定します。設定された変更を有効にする前にリロードが必要です。ライセンスを追加し、現在のライセンスを変更するには、次の手順を実行します。

Step 1 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。

例:

```
Device> enable
```

Step 2 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。

例:

```
Device# configure terminal
```

Step 3 license boot level { network-advantage [addon dna-advantage] | network-essentials [addon 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。

- **network-advantage [addon dna-advantage]**: Network Advantage ライセンスを設定します。オプションで、デジタルネットワークアーキテクチャ (DNA) Advantage ライセンスを設定することもできます。
- **network-essentials [addon dna-essentials]**: Network Essentials ライセンスを設定します。オプションで、デジタルネットワークアーキテクチャ (DNA) Essential ライセンスを設定することもできます。

この例では、DNA Advantage ライセンスはリロード後に製品インスタンスでアクティブ化されます。

例:

```
Device(config)# license boot level network-advantage add-on dna-advantage
```

Step 4 exit

特権 EXEC モードに戻ります。

例:

```
Device(config)# exit
```

Step 5 copy running-config startup-config

構成ファイルへの変更を保存します。

例:

```
Device# copy running-config startup-config
```

Step 6 show version

現在設定されているライセンスの情報と、リロード後に適用可能なライセンスを表示します。

“Technology-package Next reboot” 列には、設定変更を保存した場合にのみ、リロード後に有効になる設定済みライセンスの変更が表示されます。

添付の例では、現在のライセンスレベルは Network Advantage です。設定の変更が保存されたため、“Technology-package Next reboot” 列には、リロード後に Cisco DNA Advantage ライセンスがアクティブ化されることが表示されます。

例:

```
Device# show version
```

```
<output truncated>
```

```
Technology Package License Information:
```

```
-----  
Technology-package           Technology-package  
Current           Type           Next reboot  
-----  
network-advantage   Smart License           network-advantage  
Subscription Smart License dna-advantage
```

```
<output truncated>
```

Step 7 reload

デバイスがリロードされます。

例:

```
Device# reload
```

Step 8 show version

現在設定されているライセンスの情報と、リロード後に適用可能なライセンスを表示します。

例:

```
Device# show version
```

```
<output truncated>
```

Technology Package License Information:

```
-----  
Technology-package           Technology-package  
Current                       Type                       Next reboot  
-----  
network-advantage           Smart License             network-advantage  
dna-advantage                Subscription Smart License dna-advantage  
  
<output truncated>
```

What's next

完全な使用状況レポート（必要な場合）。レポートが必要かどうかを確認するには、システムメッセージを待つか、**show** コマンドを使用してポリシーを参照します。

- レポートが必要であることを示すシステムメッセージは次のとおりです。

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

[dec] は、レポート要件を満たすために残された時間（日数）です。

- **show** コマンドでレポート要件を確認するには、**show license status** 特権 EXEC コマンドの出力を参照し、Next ACK deadline フィールドを確認します。これは、この日付までに RUM レポートを送信して ACK をインストールする必要があることを意味します。

RUM レポートを送信するために使用可能な方法は、実装するトポロジによって異なります。詳細については、「[Smart Licensing Using Policy for Cisco Catalyst 9000 Series Switches](#)」を参照してください。

HSECK9 キー用の SLAC のインストール

この項では、Cisco Catalyst 9300、9400、9500、および 9600 シリーズスイッチに HSECK9 キー用の SLAC をインストールするさまざまな方法を示します。

SLAC のインストールの前提条件

以下の前提条件を満たしていることを確認します。

SLAC をインストールするデバイスが、HSECK9 キーをサポートしているデバイスである。[HSECK9 キーが必要になる場合と HSECK9 キーをサポートしている製品, on page 3](#)を参照してください。

Cisco SSM の該当するスマートアカウントおよびバーチャルアカウントに必要な数の HSECK9 キーがある。

該当するポリシーを使用したスマートライセンシングのトポロジに従って、初期設定を設定している。サポートされているすべてのトポロジの詳細については、「[Smart Licensing Using Policy for Cisco Catalyst 9000 Series Switches](#)」を参照してください。

SLAC のインストールの制約事項

HSECK9 キーを使用する場合に導入できない唯一のトポロジは、製品インスタンスがコントローラを介して Cisco SSM に接続されるトポロジです。ここでの「コントローラ」は、Cisco Catalyst Center のことを指します。Cisco Catalyst Center には、HSECK9 キーをサポートする Cisco Catalyst 9000 シリーズスイッチ用の SLAC を生成するオプションがありません。

インターネットを介して Cisco SSM に接続する場合の SLAC のインストール

このタスクでは、デバイス（製品インスタンス）が Cisco SSM に接続されている場合に、SLAC を要求してインストールする方法を示します。製品インスタンスは、次のいずれかの方法で接続できます。

- インターネットを介した Cisco SSM への直接接続。
- CSLU を介した Cisco SSM への接続。製品インスタンスが通信を開始します。つまり、製品インスタンスが必要な情報を CSLU にプッシュするように設定されます。
- SSM オンプレミスを介した Cisco SSM への接続。製品インスタンスが通信を開始します。

Step 1 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。

例:

```
Device> enable
```

Step 2 license smart authorization request {add | replace} feature_name {all | local}

Cisco SSM、CSLU、または SSM オンプレミスから SLAC を要求します。

- 既存の SLAC に追加するのかわ置換するのかわを指定します。
 - **add:** 要求されたライセンスキーを既存の SLAC に追加します。新しい SLAC には、既存の SLAC のすべてのキーと要求されたキーが含まれます。
 - **replace:** 既存の SLAC を置き換えます。新しい SLAC には、要求されたキーのみが含まれます。既存の SLAC のすべての HSECK9 キーが返却されます。このキーワードを入力すると、製品インスタンスはこれらの既存のキーが使用中かどうかを確認します。使用中の場合は、対応する暗号化機能を最初に無効にするようにエラーメッセージが表示されます。

スタック構成セットアップの Cisco Catalyst 9300X シリーズ スイッチの場合: SLAC がすでにインストールされているスタックに SLAC がインストールされていないデバイスを追加した場合は、**replace** および **all** キーワードを使用します。これにより、既存の SLAC 内のすべての HSECK9 キーが返却され、スタック内のすべてのデバイスに対して SLAC が要求されます。特定のメンバーの SLAC を要求することはできません。選択肢はアクティブまたはスタック全体のみです。

Cisco StackWise Virtual セットアップの Cisco Catalyst 9400 シリーズ スーパーバイザ モジュールの場合: このキーワードはサポートされていません。SLAC がアクティブにのみインストールされていて、スタンバイにもインストールする場合は、アクティブの SLAC を返却してから、アクティブとスタンバイで再度 SLAC を要求してインストールします。

- **feature_name:** hseck9 と入力して、HSECK9 キーの SLAC を要求してインストールします。
- 次のいずれかのオプションを入力して、デバイスを指定します。
 - **all:** 高可用性設定およびスタック設定のすべてのデバイスの承認コードを取得します。

スタック構成セットアップまたは Cisco StackWise Virtual セットアップの場合は、このオプションを使用してアクティブとスタンバイに SLAC をインストールすることを推奨します。これにより、スイッチオーバーが発生した場合でも、暗号化機能が中断されずに使用されます。

- **local**: 高可用性設定およびスタック設定のアクティブなデバイスの承認コードを取得します。これがデフォルトのオプションです。

例:

```
Device# license smart authorization request add hseck9 all
```

Step 3 (任意) license smart sync {all | local}

場合に応じて Cisco SSM、CSLU、または SSM オンプレミスと製品インスタンスの同期がトリガーされ、保留中のデータが送受信されます。

すぐに同期することで、SLAC のインストールプロセスを直後に完了できます。それ以外の場合、製品インスタンスが次回 Cisco SSM、CSLU、または SSM オンプレミスと通信するようにスケジュールされているときにのみ、SLAC が製品インスタンスに適用されます。

例:

```
Device# license smart sync all
```

What's next

「[インストール後に必要なタスク](#)」を参照してください

CSSM への接続なし、CSLU なし

このタスクでは、デバイス（製品インスタンス）がネットワーク外のデバイスとオンラインで通信できない、外部との接続性がないネットワークに SLAC を要求してインストールする方法を示します。

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

CSSM への接続なし、CSLU なしトポロジのステップ 1 が完了していることを確認します。[トポロジのワークフロー: Cisco SSM への接続なし、CSLU なし](#)を参照してください。

Step 1 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。

例:

```
Device> enable
```

Step 2 license smart authorization request {add | replace} feature_name {all | local}

必要なすべての情報を含む SLAC 要求を生成します。

既存の SLAC に追加するのか置換するのかを指定します。

- **add**: 要求されたキーを既存の SLAC に追加します。新しい承認コードには、既存の SLAC のすべてのキーと要求されたライセンスが含まれます。
- **replace**: 既存の SLAC を置き換えます。新しい SLAC には、要求された HSECK9 キーのみが含まれます。既存の SLAC のすべてのキーが返却されます。このキーワードを入力すると、製品インスタンスは

これらの既存のキーが使用中かどうかを確認します。使用中の場合は、対応する機能を最初に無効にするようにエラーメッセージが表示されます。



(注)

スタック構成シナリオ（Cisco Catalyst 9300X シリーズ スイッチ）の場合：SLAC がすでにインストールされている既存のスタックに（SLACがインストールされていない）デバイスを追加した場合は、**replace** および **all** キーワードを使用します。これにより、既存の SLAC 内のすべての HSECK9 キーが返却され、スタック内のすべてのデバイスに対して SLAC が要求されます。特定のメンバーの SLAC を要求することはできません。選択肢はアクティブまたはスタック全体のみです。



(注)

このキーワードは、Cisco StackWise Virtual セットアップの Cisco Catalyst 9400 シリーズ スーパーバイザ モジュールではサポートされていません。SLAC がアクティブにのみインストールされていて、スタンバイにもインストールする場合は、アクティブの SLAC を返却してから、アクティブとスタンバイで再度 SLAC を要求してインストールします。

feature_name に、SLAC の追加または置換を要求する輸出規制ライセンスの名前を入力します。「hseck9」と入力して、HSECK9 キーの SLAC を要求してインストールします。

次のいずれかのオプションを入力して、デバイスを指定します。

- **all**: 高可用性設定のすべてのデバイスの承認コードを取得します。

スタック構成セットアップまたは Cisco StackWise Virtual セットアップの場合は、このオプションを使用してアクティブとスタンバイに SLAC をインストールすることを推奨します。これにより、スイッチオーバーが発生した場合でも、暗号化機能が中断されずに使用されます。

- **local**: 高可用性設定のアクティブなデバイスの承認コードを取得します。これがデフォルトのオプションです。

例:

```
Device# license smart authorization request add hseck9 all
```

Step 3 license smart authorization request savepath

SLAC 要求に必要な UDI 情報を、指定した場所の .txt ファイルに保存します。

例:

```
Device# license smart authorization request save bootflash:slac.txt
```

Step 4

ファイルを Cisco SSM にアップロードし、製品インスタンスで必要になったときにファイルをダウンロードします。

このタスクは、CSSM Web UI で実行します。



(注)

SLAC request ファイルをアップロードしてから SLAC ファイルをダウンロードするこのプロビジョニングは、Cisco IOS XE Cupertino 17.7.1 以降でのみサポートされています。それ以前のリリースでは、CSSM Web UI に必要な情報を入力し、CSSM Web UI で SLAC コードを生成してから、ダウンロードしてインストールする必要があります。古い方法も引き続き使用できますが、新しい方法の方が手作業によるエラーが少なくなる傾向があるため、このトポロジでは推奨される方法です。

- a) <https://software.cisco.com> で Cisco SSM Web UI にログインします。[Smart Software Licensing] で、[Manage licenses] リンクをクリックします。
- b) レポートを受信するスマートアカウントを選択します。
- c) [Smart Software Licensing] > [Reports] > [Usage Data Files] を選択します。
- d) [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。

アップロードされたファイルは削除できません。ただし、必要に応じて別のファイルをアップロードできます。

- e) [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。

ファイルがアップロードされ、[Reports] 画面の [Usage Data Files] テーブルにリストされます。表示される詳細には、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、確認ステータスが含まれています。

- f) [Acknowledgment] 列で [Download] をクリックして、アップロードしたレポートまたは要求の ACK または SLAC を保存します。

[Acknowledgment] 列にファイルが表示されるまで待つ必要があります。処理する RUM レポートまたは要求が多数ある場合、Cisco SSM では数分かかることがあります。

ファイルをダウンロードしたら、ファイルをインポートして製品インスタンスにインストールするか、CSLU または SSM On-Prem に転送します。

Step 5 **copy source filename bootflash:**

(任意) ファイルをソースの場所またはディレクトリから製品インスタンスのフラッシュメモリにコピーします。また、リモートの場所からファイルを直接インポートし、製品インスタンスにインストールすることもできます (次の手順)。

- **コピー元:** これはファイルのコピー元の場所です。コピー元は、ローカルまたはリモートのいずれかです。
- **bootflash::** これはブートフラッシュメモリの場合の宛先です。

例:

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

Step 6 **license smart import filepath_filename**

ファイルを製品インスタンスにインポートしてインストールします。*filepath_filename* には、場所 (ファイル名を含む) を指定します。インストール後、インストールしたファイルのタイプを示すシステムメッセージが表示されます。



(注)

CSSM Web UI で複数の製品インスタンスの SLAC を生成した場合 (スタック構成セットアップなど)、UDI ごとに個別の .txt SLAC ファイルをダウンロードしてください。一度に 1 つのファイルをインポートしてインストールします。

例:


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

What's next

「[インストール後に必要なタスク](#)」を参照してください

CSLU を介して Cisco SSM に接続する場合の SLAC のインストール: CSLU 開始型通信

このタスクでは、デバイス（製品インスタンス）が CSLU を介して Cisco SSM に接続され、CSLU が通信を開始する場合、つまり CSLU が必要な情報を製品インスタンスからプルするように設定されている場合に、SLAC を要求してインストールする方法を示します。

このタスクでは、Cisco SSM で特定のタスクを実行し、CSLU インターフェイスで特定のタスクを実行する必要があります。

Step 1 CSLU で、1 つ以上のデバイスの承認コードを要求します。

- CSLU にログインして、[Inventory] タブに移動します。
- 承認コード要求の対象となる 1 つ以上の製品インスタンスを選択します。
- [Actions for Selected] > [Authorization Code Request] > [Accept] を選択します

アップロードする .csv ファイルを選択する別のポップアップウィンドウが開きます。

Step 2 <https://software.cisco.com> で Cisco SSM にログインします。[Smart Software Licensing] で、[Manage licenses] リンクをクリックします。

Step 3 [Inventory] > [Product Instances] > [Authorize License Enforced Features] をクリックします

Step 4 単一の製品インスタンスまたは複数の製品インスタンスに SLAC を生成します（いずれかを選択）。

Choose from:

• 単一の製品インスタンスの SLAC の生成:

- [PID] と [Serial Number] を入力します。



他のフィールドは入力しないでください。

(注)

- ライセンスを選択し、対応する [Reserve] 列に **1** を入力します。

PID に対して正しいライセンスを選択したことを確認します。HSECK9 がサポートされている Cisco Catalyst アクセス、コア、およびアグリゲーションスイッチでは、[C9K HSEC] を選択します。

- [Next] をクリックします。
- [承認コードを生成 (Generate Authorization Code)] をクリックします。
- 承認コードをダウンロードし、.csv ファイルとして保存します。

• 複数の製品インスタンスの SLAC の生成（この場合、.csv ファイルのアップロードが必要）:

- [Single Device] (デフォルト) というドロップダウンリストで、選択を [Multiple Devices] に変更します。

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

2. [Choose File] をクリックし、SLAC を必要とする製品インスタンスのリストを含む .csv ファイルに移動します。
3. アップロードすると、デバイスのリストが Cisco SSM に表示されます。すべてのデバイスのチェックボックスが有効になったら（すべてのデバイスの SLAC を要求することを意味します） [Next] をクリックします。
4. 各製品インスタンスに必要なライセンス数を指定し、[Next] をクリックします。



「C9K HSEC」ライセンスの場合、UDI ごとに 1 つの SLAC が必要です。

（注）

5. [Reserve Licenses] をクリックします。
6. [Download Authorization Codes] > [Close] をクリックします
すべての承認コードを含む .csv ファイルがダウンロードされます。

Step 5 CSLU インターフェイスに戻り、[Data] > [Import from CSSM] に移動します

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するか、適切な *.xml ファイルを参照して選択します。

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。

アップロードに成功すると、CSLU が次に更新を実行するときに、コードが製品インスタンスに適用されません。

What's next

「[インストール後に必要なタスク](#)」を参照してください

SSM オンプレミスを介して Cisco SSM に接続する場合の SLAC のインストール: SSM オンプレミス開始型通信

このタスクでは、デバイス（製品インスタンス）が SSM オンプレミスに接続され、SSM オンプレミスが通信を開始する場合（つまり、SSM オンプレミスが製品インスタンスから必要な情報をプルするように設定されている場合）に、SLAC を要求してインストールする方法を示します。

ここでは、SSM オンプレミスで要求ファイルを作成し、Cisco SSM Web UI で要求をアップロードし、SLAC を生成して、SSM オンプレミスサーバーにインポートします。最後に、SSM オンプレミスを製品インスタンスと同期します。

Step 1 SSM オンプレミスにログインし、[Smart Licensing] > [Inventory] > [SL Using Policy] に移動します。

- a) SLAC を要求するすべての製品インスタンスを選択します。
- b) [Actions for Selected...] > [Authorization Code Request] > [Accept] をクリックします。

保存された .csv ファイルには、選択した製品インスタンスのリストが、Cisco SSM で SLAC を生成するために必要な形式で含まれています。次の手順で、Cisco SSM からアクセス可能な場所にこのファイルを保存します。

Step 2 <https://software.cisco.com> で Cisco SSM にログインします。[Smart Software Licensing] で、[Manage licenses] リンクをクリックします。

Step 3 [Inventory] > [Product Instances] > [Authorize License Enforced Features] をクリックします

Step 4 複数の製品インスタンスの SLAC の生成

- a) [Single Device] (デフォルト) というドロップダウンリストで、選択を [Multiple Devices] に変更します。
この時点で、[Download a template] リンクが表示されます。必要なテンプレートまたはファイルがまだない場合は、ダウンロードできます。シリアル番号と PID のみが必須です。
- b) [Choose File] をクリックし、SLAC を必要とする製品インスタンスのリストを含む .csv ファイルに移動します。
- c) アップロードすると、デバイスのリストが Cisco SSM に表示されます。すべてのデバイスのチェックボックスが有効になったら (すべてのデバイスの SLAC を要求することを意味します) [Next] をクリックします。
- d) 各製品インスタンスに必要なライセンス数を指定し、[Next] をクリックします。



「C9K HSEC」ライセンスの場合、UDI ごとに 1 つの SLAC が必要です。

(注)

- e) [Reserve Licenses] > [Download Authorization Codes] > [Close] をクリックします
すべての承認コードを含む .csv ファイルがダウンロードされます。

Step 5 SSM オンプレミス UI に戻り、すべての承認コードを含むファイルをインポートします。

- a) [Inventory] > [SL Using Policy] に移動します
- b) [Export/Import All...] をクリックし、[Import From Cisco] をクリックします。

[Inventory] > [SL Using Policy] に移動し、[Alerts] 列を参照して、[Authorization message received from CSSM] というインポートステータスを確認します。

Step 6 [Reports] > [Synchronisation pull schedule with the devices] > [Synchronise now with the device] に移動して、すべての製品インスタンスに SLAC を適用します。

コードのインポート直後に同期を行わない場合、SSM オンプレミスが次に更新を実行するときに、アップロードされたコードが製品インスタンスに適用されます。

What's next

「[インストール後に必要なタスク](#)」を参照してください

インストール後に必要なタスク

このタスクでは、SLAC のインストール後に実行する必要があるアクティビティを示します。ここでの情報は、SLAC のインストール方法すべてに適用されます。

Step 1 SLAC のインストールと HSECK9 キーの使用を確認します。

a) SLAC のインストール後に表示されるシステムメッセージに注目してください。

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

[chars] は、SLAC がインストールされた UDI です

```
%SMART_LIC-6-EXPORT_CONTROLLED: Usage of export controlled features is allowed for feature hseck9
```

b) **show license authorization** 特権 EXEC コマンドの出力に、タイムスタンプと最後の確認コードが表示されていることを確認します。

出力の Overall Status セクションで、Status: SMART AUTHORIZATION INSTALLED on <timestamp> と Last Confirmation code: <code> を探します。これは、SLAC がインストールされていることを意味します。

例:

Cisco Catalyst 9300X シリーズスイッチでは、スタック構成セットアップで複数の SLAC をインストールした場合、SLAC がインストールされている各 UDI のステータス、タイムスタンプ、および確認コードが表示されます。次の出力例では、SLAC はアクティブスイッチにのみインストールされていて、スタンバイスイッチまたはメンバースイッチにはインストールされていません。

```
Device# show license authorization
```

```
Overall status:
```

```
Active: PID:C9300X-24HX,SN:FOC2519L8R7
      Status: SMART AUTHORIZATION INSTALLED on Oct 29 17:45:28 2021 UTC
      Last Confirmation code: 6746c5b5
Standby: PID:C9300X-48HXN,SN:FOC2524L39P
      Status: NOT INSTALLED
Member: PID:C9300X-48HX,SN:FOC2516LC92
      Status: NOT INSTALLED
```

```
Authorizations:
```

```
C9K HSEC (Cat9K HSEC):
  Description: HSEC Key for Export Compliance on Cat9K Series Switches
  Total available count: 1
  Enforcement type: EXPORT RESTRICTED
  Term information:
    Active: PID:C9300X-24HX,SN:FOC2519L8R7
    Authorization type: SMART AUTHORIZATION INSTALLED
    License type: PERPETUAL
    Term Count: 1
```

```
Purchased Licenses:
```

```
No Purchase Information Available
```

```
Device# show license summary
```

```
License Usage:
```

License	Entitlement Tag	Count	Status
network-advantage	(C9300-24 Network Advan...)	1	IN USE
dna-advantage	(C9300-24 DNA Advantage)	1	IN USE
network-advantage	(C9300-48 Network Advan...)	2	IN USE
dna-advantage	(C9300-48 DNA Advantage)	2	IN USE
C9K HSEC	(Cat9K HSEC)	0	NOT IN USE

Cisco Catalyst 9400 シリーズ スーパーバイザ 2 および 2XL モジュールでは、Cisco StaskWise Virtual セットアップで SLAC をインストールした場合、接続されているデバイスごとに異なる確認コードが表示されます。

Device# **show license authorization**

Overall status:

Active: PID:C9407R,SN:FXS2115054R
Status: SMART AUTHORIZATION INSTALLED on Sep 07 22:56:57 2022 UTC
Last Confirmation code: dc206d9d
Standby: PID:C9407R,SN:FXS2115054R
Status: SMART AUTHORIZATION INSTALLED on Sep 07 22:56:57 2022 UTC
Last Confirmation code: dc206d9d

Authorizations:

C9K HSEC (Cat9K HSEC):
Description: HSEC Key for Export Compliance on Cat9K Series Switches
Total available count: 1
Enforcement type: EXPORT RESTRICTED
Term information:
Active: PID:C9407R,SN:FXS2115054R
Authorization type: SMART AUTHORIZATION INSTALLED
License type: PERPETUAL
Term Count: 1
Standby: PID:C9407R,SN:FXS2115054R
Authorization type: SMART AUTHORIZATION INSTALLED
License type: PERPETUAL
Term Count: 1

Purchased Licenses:

No Purchase Information Available

Device# **show license summary**

Account Information:

Smart Account: Eg-SA
Virtual Account: Eg-VA

License Usage:

License	Entitlement Tag	Count	Status
network-advantage	(C9400 Network Advantage)	2	IN USE
dna-advantage	(C9400 DNA Advantage)	1	IN USE
C9K HSEC	(Cat9K HSEC)	0	NOT IN USE

デュアルスーパーバイザセットアップでSLACをインストールした場合は、接続されているすべてのデバイスに同じ確認コードが表示されることに注目してください。次の出力例では、SLACがこのようなデュアルスーパーバイザセットアップにインストールされています。

Device# **show license authorization**

Overall status:

Active: PID:C9606R,SN:FXS241201WP
Status: SMART AUTHORIZATION INSTALLED on Dec 13 05:18:07 2021 UTC
Last Confirmation code: 7cflf54a
Standby: PID:C9606R,SN:FXS241201WP
Status: SMART AUTHORIZATION INSTALLED on Dec 13 05:18:07 2021 UTC
Last Confirmation code: 7cflf54a

Authorizations:

C9K HSEC (Cat9K HSEC):
Description: HSEC Key for Export Compliance on Cat9K Series Switches
Total available count: 1
Enforcement type: EXPORT RESTRICTED
Term information:
Active: PID:C9606R,SN:FXS241201WP
Authorization type: SMART AUTHORIZATION INSTALLED
License type: PERPETUAL
Term Count: 1
Standby: PID:C9606R,SN:FXS241201WP
Authorization type: SMART AUTHORIZATION INSTALLED

```

License type: PERPETUAL
Term Count: 1

Purchased Licenses:
No Purchase Information Available

Device# show license summary
Account Information:
Smart Account: Eg-SA As of Oct 07 05:13:33 2021 UTC
Virtual Account: Eg-VA

License Usage:
License                Entitlement Tag                Count Status
-----
network-advantage     (C9600-NW-A)                   2 IN USE
dna-advantage         (C9600-DNA-A)                   1 IN USE
C9K HSEC              (Cat9K HSEC)                   0 NOT IN USE

```

- c) **show license summary** 特権 EXEC コマンドの出力で、"C9K HSEC" の使用状況のカウントとステータスに、それぞれ 0 と NOT IN USE が表示されていることを確認します。これは、HSECK9 キーは使用可能ですが、まだ使用されていないことを意味します。

Step 2 暗号化機能を設定します。

この機能の設定に関する情報については、対応するプラットフォームの設定ガイドを参照してください。

Cisco Catalyst 9300X シリーズ スイッチについては、『Security Configuration Guide, Cisco IOS XE <applicable release number> (Catalyst 9300 Switches)』の「Configuring IPsec」の章を参照してください。

Cisco Catalyst 9400 シリーズ スーパーバイザ 2 および 2XL モジュールについては、『Security Configuration Guide, Cisco IOS XE <applicable release number> (Catalyst 9300 Switches)』の「Configuring IPsec」の章を参照してください。

Cisco Catalyst 9500X シリーズ スイッチについては、『Security Configuration Guide, Cisco IOS XE <applicable release number> (Catalyst 9500 Switches)』の「MACsec Encryption」の章を参照してください。

Cisco Catalyst 9600 シリーズ スーパーバイザ エンジン 2 (C9600X-SUP-2) および関連するラインカードについては、『Security Configuration Guide, Cisco IOS XE <applicable release number> (Catalyst 9600 Switches)』の「MACsec Encryption」の章を参照してください。

Step 3 再度、HSECK9 キーの使用状況を確認します。

暗号化機能を設定すると、**show license summary** 特権 EXEC コマンドの出力での HSECK9 キーの使用状況のカウントとステータスが、それぞれ 1 と IN USE に変わります。

例:

スタック構成セットアップまたは Cisco StackWise Virtual セットアップで複数の HSECK9 キーを取得した場合でも、**show license summary** コマンドの出力での使用状況のカウントには、1 のみが表示されます。これは、特定の時点でアクティブな HSECK9 キーが 1 つだけ使用されるためです。スイッチオーバーが発生すると、スタンバイの HSECK9 キーが使用されます。スタンバイが新しくアクティブになっても、使用されているキーは 1 つであるため、使用状況のカウントは 1 のままです。

Cisco Catalyst 9300X シリーズ スイッチの場合。

```

Device# show license summary
License Usage:
License                Entitlement Tag                Count Status
-----

```

```

-----
network-advantage      (C9300-24 Network Advan...)  1 IN USE
dna-advantage          (C9300-24 DNA Advantage)    1 IN USE
network-advantage      (C9300-48 Network Advan...)  2 IN USE
dna-advantage          (C9300-48 DNA Advantage)    2 IN USE
hseck9                 (Cat9K HSEC)                 1 IN USE

```

Cisco StackWise Virtual セットアップの Cisco Catalyst 9400 シリーズ スーパーバイザ 2 および 2XL モジュールの場合。

Device# **show license summary**

```

Account Information:
  Smart Account: Eg-SA
  Virtual Account: Eg-VA

```

```

License Usage:
  License                Entitlement Tag                Count Status
-----
network-advantage      (C9400 Network Advantage)      2 IN USE
dna-advantage          (C9400 DNA Advantage)          1 IN USE
C9K HSEC                (Cat9K HSEC)                    1 IN USE

```

Cisco Catalyst 9500X シリーズ スイッチの場合。

Device# **show license summary**

```

Account Information:
  Smart Account: Eg-SA As of Sep 27 10:04:01 2021 UTC
  Virtual Account: Eg-VA

```

```

License Usage:
  License                Entitlement Tag                Count Status
-----
network-advantage      (C9500X_NW_A)                  1 IN USE
dna-advantage          (C9500X_DNA_A)                 1 IN USE
C9K HSEC                (Cat9K HSEC)                    1 IN USE

```

デュアルスーパーバイザセットアップの Cisco Catalyst 9600 シリーズ スーパーバイザ エンジン 2 (C9600X-SUP-2) および関連するラインカードの場合。

Device# **show license summary**

```

Account Information:
  Smart Account: Eg-SA As of Oct 07 05:13:33 2021 UTC
  Virtual Account: Eg-VA

```

```

License Usage:
  License                Entitlement Tag                Count Status
-----
network-advantage      (C9600-NW-A)                   2 IN USE
dna-advantage          (C9600-DNA-A)                  1 IN USE
C9K HSEC                (Cat9K HSEC)                    1 IN USE

```

What's next

完全な使用状況レポート（必要な場合）。レポートが必要かどうかを確認するには、システムメッセージを待つか、**show** コマンドを使用してポリシーを参照します。

- レポートが必要であることを示すシステムメッセージは次のとおりです。

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

[dec] は、レポート要件を満たすために残された時間（日数）です。

- **show** コマンドでレポート要件を確認するには、**show license status** 特権 EXEC コマンドの出力を参照し、Next ACK deadline フィールドを確認します。これは、この日付までに RUM レポートを送信して ACK をインストールする必要があることを意味します。

RUM レポートを送信するために使用可能な方法は、実装するトポロジによって異なります。詳細については、「[Smart Licensing Using Policy for Cisco Catalyst 9000 Series Switches](#)」を参照してください。

SLAC の返却

このタスクを使用して、すべてのトポロジで SLAC を削除し、HSECK9 キーを返却することができます。

次の状況では、SLAC および HSECK9 キーを返却することができます。

- HSECK9 キーが必要な暗号化機能を使用する必要がなくなった場合。
- 返品許可 (RMA) のためにデバイスを返却するか、永久に使用を停止する。デバイスをシスコに返却する場合は、**licence smart factory reset** 特権 EXEC コマンドを設定する必要があります。これにより、承認コード、RUM レポートなどを含めて、すべてのライセンス情報 (使用中のライセンスを除く) が製品インスタンスから削除されます。工場出荷時設定へのリセットを実行する前に、SLAC コードを返却します。また、製品インスタンスからライセンス情報を削除する前に、Cisco SSM に RUM レポートを送信することを推奨します。

1. HSECK9 キーを使用した暗号化機能を無効化または設定解除します。この機能の無効化に関する情報については、対応するプラットフォームの設定ガイドを参照してください。

この機能の無効化に関する情報については、対応するプラットフォームの設定ガイドを参照してください。

Cisco Catalyst 9300X シリーズ スイッチについては、『Security Configuration Guide, Cisco IOS XE <applicable release number> (Catalyst 9300 Switches)』の「Configuring IPsec」の章を参照してください。

Cisco Catalyst 9400 シリーズ スーパーバイザ 2 および 2XL モジュールについては、『Security Configuration Guide, Cisco IOS XE <applicable release number> (Catalyst 9300 Switches)』の「Configuring IPsec」の章を参照してください。

Cisco Catalyst 9500X シリーズ スイッチについては、『Security Configuration Guide, Cisco IOS XE <applicable release number> (Catalyst 9500 Switches)』の「MACsec Encryption」の章を参照してください。

Cisco Catalyst 9600 シリーズ スーパーバイザ エンジン 2 (C9600X-SUP-2) および関連するラインカードについては、『Security Configuration Guide, Cisco IOS XE <applicable release number> (Catalyst 9600 Switches)』の「MACsec Encryption」の章を参照してください。

2. **show license summary** 特権 EXEC コマンドを使用して、HSECK9 キーのライセンス使用ステータスを確認します。

HSECK9 キーのステータスが `NOT IN USE` と表示されている場合は、タスクの手順に進みます。

暗号化機能を無効にした後でも HSECK9 キーのステータスが `IN USE` と表示される場合は、まず HSECK9 キーをリリースするために必要なコマンドを入力します。

対象プラットフォーム...	HSECK9 キーを強制的にリリースするにはこのコマンドを入力します
Cisco Catalyst 9300X シリーズ スイッチ Cisco Catalyst 9400 シリーズ スーパーバイザ 2 および 2XL モジュール。	platform hsec-license-release Device# configure terminal Device(config)# platform hsec-license-release HSEC license is released Device(config)# exit
Cisco Catalyst 9500X シリーズ スイッチ Cisco Catalyst 9600 シリーズ スーパーバイザ エンジン 2 および関連するラインカード。	platform wanmacsec hsec-license-release Device# configure terminal Device(config)# platform wanmacsec hsec-license-release HSEC license is released Device(config)# exit

SLAC を削除し、HSECK9 キーを Cisco SSM のライセンスプールに返却するには、次の手順を実行します。

Step 1 show license summary

(任意) ライセンスの使用状況の概要を表示します。この手順は、SLAC を返却する場合にのみ適用されません。

返却するライセンスのステータスが [NOT IN USE] であることを確認します。

例:

```
Device# show license summary
License Usage:
-----
License           Entitlement Tag           Count Status
-----
network-advantage (C9300-24 Network Advan...) 1 IN USE
dna-advantage     (C9300-24 DNA Advantage) 1 IN USE
network-advantage (C9300-48 Network Advan...) 2 IN USE
dna-advantage     (C9300-48 DNA Advantage) 2 IN USE
C9K HSEC          (Cat9K HSEC)             0 NOT IN USE
```

Step 2 license smart authorization return {all |local} {offline [path] |online}

例:

```
Device# license smart authorization return all online
```

OR

```
Device# license smart authorization return all offline
Enter this return code in Cisco Smart Software Manager portal:
UDI: PID:C9300X-24HX,SN:FOC2519L8R7
Return code: Cr9JHx-L1x5Rj-ftwzgl-h9QZAU-LE5DT1-babWeL-FABPt9-Wr1Dn7-Rp7
```

OR

```
Device# license smart authorization return all offline bootflash:return-code.txt
```

Cisco SSM のライセンスプールに承認コードを返却します。このコマンドを入力すると、戻りコードが表示されます。

製品インスタンスを指定します。

- **all:** 高可用性セットアップまたはスタック構成セットアップで接続されたすべての製品インスタンスに対してアクションを実行します。
- **local:** アクティブな製品インスタンスに対してアクションを実行します。これがデフォルトのオプションです。

Cisco SSM に接続しているかどうかを指定します。

- 製品インスタンスが Cisco SSM に直接接続されている場合、または CSLU または SSM オンプレミスを通じて Cisco SSM に接続されていて、製品インスタンスが通信を開始する場合は、**online** を入力します。コードは自動的に Cisco SSM に返され、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、リターンコードが自動的に Cisco SSM に送信されます。
- 製品インスタンスが Cisco SSM に接続されていない場合、または CSLU 開始型通信または SSM オンプレミス開始型通信のトポロジを導入した場合は、**offline** *[filepath_filename]* を入力します。
offline オプションを選択した場合は、これを Cisco SSM に送信する追加の手順を完了する必要があります。

Step 3 **offline** オプションを選択した場合は、Cisco SSM に返却情報をアップロードします。

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

シスコから提供されたユーザー名とパスワードを使用してログインします。

- b) レポートを受信するスマートアカウントを選択します。
- c) [Smart Software Licensing] > [Reports] > [Usage Data Files] > [Upload Usage Data] を選択します。
- d) 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
- e) [...] をクリックして、SLAC 返却要求ファイル (.txt 形式) をアップロードします

アップロードされたファイルは削除できません。ただし、必要に応じて別のファイルをアップロードできます。

- f) [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 Cisco SSM にアップロードされ、[Reports] > [Usage Data Files] の下に、ファイル名、報告された時刻、アップロード先のバーチャルアカウントなどとともにリストされます。

- g) [Acknowledgement] 列で [Download] をクリックして、ACK を保存します。

[Acknowledgment] 列にファイルが表示されるまで待つ必要があります。処理する RUM レポートまたは要求が多数ある場合、CSSM では数分かかることがあります。

ファイルをダウンロードしたら、特権 EXEC モードで **license smart import***filepath_filename* コマンドを使用してファイルをインポートして製品インスタンスにインストールするか、CSLU または SSM オンプレミスにインポートします。

Step 4 **show license authorization**

ライセンス情報を表示します。返却プロセスが正常に完了すると、Last return code: フィールドに戻りコードが表示されます。

例:

```
Device# show license authorization
Overall status:
  Active: PID:C9300X-24HX,SN:FOC2519L8R7
          Status: NOT INSTALLED
          Last return code: Cr9JHx-L1x5Rj-ftwzgL-h9QZAU-LE5DT1-
babWeL-FABPt9-Wr1Dn7-Rp7
  Standby: PID:C9300X-48HXN,SN:FOC2524L39P
          Status: NOT INSTALLED
  Member: PID:C9300X-48HX,SN:FOC2516LC92
          Status: NOT INSTALLED
```

<output truncated>

設定例

C9300X の例: HSECK9 キーが使用されているスタックへのメンバーの追加

この例では、暗号化機能が設定され、HSECK9 キーが使用されている既存のスタックにデバイスを追加する方法の1つを示します。

この方法の全体的な流れは次のとおりです。既存のスタックに新しいメンバーを追加する > スタック全体の SLAC を再度要求してインストールする。

1. 既存のスタックに関する情報を表示して確認します。

show switch detail コマンドの出力は、これが 2 メンバースタックであることを示しています。

show license authorisation コマンドの出力は、SLAC がアクティブ (C9300X-24HX、SN: FOC2519L8R7) およびスタンバイ (PID: C9300X-48HXN、SN: FOC2524L39P) にインストールされていることを示しています。

show license summary コマンドの出力は、暗号化機能が設定されていることを示しています (C9KHSEC-INUSE)。

この **show license all** コマンドの出力 (省略された出力) では、デバイスが Cisco SSM に直接接続されていて、Cisco SSM との通信に **smart** 転送オプションが使用されていることが示されています。

```
Device# show switch detail
Switch/Stack Mac Address : b08b.d02b.5b80 - Local Mac Address
Mac persistency wait time: Indefinite
```

Switch#	Role	Mac Address	Priority	H/W Version	Current State
*1	Active	b08b.d02b.5b80	15	P2B	Ready
2	Standby	b08b.d08d.bb00	14	P2B	Ready
3	Member	0000.0000.0000	0	PP	Removed

Switch#	Stack Port Status		Neighbors	
	Port 1	Port 2	Port 1	Port 2
1	DOWN	OK	None	2
2	OK	DOWN	1	None

```

Device# show license authorization
Overall status:
  Active: PID:C9300X-24HX,SN:FOC2519L8R7
    Status: SMART AUTHORIZATION INSTALLED on Dec 03 18:34:03 2021 UTC
    Last Confirmation code: 72ad37d5
  Standby: PID:C9300X-48HXN,SN:FOC2524L39P
    Status: SMART AUTHORIZATION INSTALLED on Dec 03 18:34:03 2021 UTC
    Last Confirmation code: 842584db

```

```

Authorizations:
  C9K HSEC (Cat9K HSEC):
    Description: HSEC Key for Export Compliance on Cat9K Series Switches
    Total available count: 2
    Enforcement type: EXPORT RESTRICTED
    Term information:
      Active: PID:C9300X-24HX,SN:FOC2519L8R7
        Authorization type: SMART AUTHORIZATION INSTALLED
        License type: PERPETUAL
        Term Count: 1
      Standby: PID:C9300X-48HXN,SN:FOC2524L39P
        Authorization type: SMART AUTHORIZATION INSTALLED
        License type: PERPETUAL
        Term Count: 1

```

```

Purchased Licenses:
  No Purchase Information Available

```

```

Device# show license summary
Account Information:
  Smart Account: Eg-SA As of Dec 03 18:51:59 2021 UTC
  Virtual Account: Eg-VA

```

```

License Usage:
  License                Entitlement Tag                Count Status
  -----
  network-advantage     (C9300-24 Network Advan...)    1 IN USE
  dna-advantage         (C9300-24 DNA Advantage)       1 IN USE
  network-advantage     (C9300-48 Network Advan...)    1 IN USE
  dna-advantage         (C9300-48 DNA Advantage)       1 IN USE
  C9K HSEC              (Cat9K HSEC)                   1 IN USE

```

```

Device# show license all

```

```

Smart Licensing Status
=====

```

```

Smart Licensing is ENABLED

```

```

<output truncated>

```

```

Transport:
  Type: Smart
  URL: https://smartreceiver-stage.cisco.com/licservice/license
  Proxy:
    Not Configured
  VRF:
    Not Configured

```

```

Miscellaneous:
  Custom Id: <empty>

```

```

<output truncated>

```

2. 新しいメンバーをスタックに追加します。

syslog には、新しいメンバーがスタックに追加された後の一連のイベントが表示されます。新しく追加されたメンバー(%SMART_LIC-6-TRUST_INSTALL_SUCCESS)に信頼コードが正常にインストールされたことに注目してください。

show switch stack-ports コマンドと **show switch detail** コマンドの出力には、新しく追加されたメンバーであるスイッチ 3 のステータスが表示されます。

show license udi コマンドの出力には、新しいメンバー (C9300X-48HX、SN: FOC2516LC92) を含むスタック構成セットアップ内のコネクテッドデバイスすべての PID が表示されます。

show license authorisation コマンドの出力は、SLAC がアクティブ (C9300X-24HX、SN: FOC2519L8R7) およびスタンバイ (PID: C9300X-48HXN、SN: FOC2524L39P) にインストールされているものの、新しく追加されたメンバーにはインストールされていないことを示しています。

```
<output truncated>
Dec  3 18:42:49.885: %STACKMGR-6-STACK_LINK_CHANGE: Switch 2 R0/0: stack_mgr: Stack port 2 on Switch 2 is up
Dec  3 18:42:57.213: %STACKMGR-6-STACK_LINK_CHANGE: Switch 1 R0/0: stack_mgr: Stack port 1 on Switch 1 is up
Dec  3 18:42:57.229: %STACKMGR-4-SWITCH_ADDED: Switch 1 R0/0: stack_mgr: Switch 3 has been added to the stack.
Dec  3 18:42:57.228: %STACKMGR-4-SWITCH_ADDED: Switch 2 R0/0: stack_mgr: Switch 3 has been added to the stack.
Applying config on Switch 3...[DONE]
Dec  3 18:42:59.179: %STACKMGR-4-SWITCH_ADDED: Switch 2 R0/0: stack_mgr: Switch 3 has been added to the stack.
.
.
.
Dec  3 18:42:36.633: %STACKMGR-6-STACK_LINK_CHANGE: Switch 3 R0/0: stack_mgr: Stack port 1 on Switch 3 is down
Dec  3 18:42:36.633: %STACKMGR-6-STACK_LINK_CHANGE: Switch 3 R0/0: stack_mgr: Stack port 2 on Switch 3 is down
Dec  3 18:42:50.369: %STACKMGR-6-STACK_LINK_CHANGE: Switch 3 R0/0: stack_mgr: Stack port 1 on Switch 3 is up
Dec  3 18:42:57.067: %STACKMGR-6-STACK_LINK_CHANGE: Switch 3 R0/0: stack_mgr: Stack port 2 on Switch 3 is up
Dec  3 18:42:57.070: %STACKMGR-4-SWITCH_ADDED: Switch 3 R0/0: stack_mgr: Switch 3 has been added to the stack.
.
.
.
Dec  3 18:43:04.079: Slot add triggered 3
Dec  3 18:43:06.233: ILP:: switch 3 POE mode : IEEE BT
Dec  3 18:43:06.233: ILP:: POE POST detail for switch 3: PASS
Dec  3 18:43:06.233: ILP:: Able to get POE POST from switch 3 MCU
.
.
.
Dec  3 18:43:29.665: %SMART_LIC-6-TRUST_INSTALL_SUCCESS: A new licensing trust code was successfully installed on P:C9300X-48HX,S:FOC2516LC92.
Dec  3 18:43:45.239: %LINK-3-UPDOWN: Interface TenGigabitEthernet3/0/4, changed state to up
Dec  3 18:43:46.239: %LINEPROTO-5-UPDOWN: Line protocol on Interface TenGigabitEthernet3/0/4, changed state to up
<output truncated>
```

```
Device# show switch stack-ports
Switch#  Port1      Port2
-----
1         OK          OK
2         OK          OK
3         OK          OK
```

Device# **show switch detail**

Switch/Stack Mac Address : b08b.d02b.5b80 - Local Mac Address
Mac persistency wait time: Indefinite

Switch#	Role	Mac Address	Priority	H/W Version	Current State
*1	Active	b08b.d02b.5b80	15	P2B	Ready
2	Standby	b08b.d08d.bb00	14	P2B	Ready
3	Member	f87a.414b.5580	1	PP	Ready

Switch#	Stack Port Status		Neighbors	
	Port 1	Port 2	Port 1	Port 2
1	OK	OK	3	2
2	OK	OK	1	3
3	OK	OK	2	1

Device# **show license udi**

UDI: PID:C9300X-24HX,SN:FOC2519L8R7

HA UDI List:

Active:PID:C9300X-24HX,SN:FOC2519L8R7
Standby:PID:C9300X-48HXN,SN:FOC2524L39P
Member:PID:C9300X-48HX,SN:FOC2516LC92

Device# **show license authorization**

Overall status:

Active: PID:C9300X-24HX,SN:FOC2519L8R7
Status: SMART AUTHORIZATION INSTALLED on Dec 03 18:34:03 2021 UTC
Last Confirmation code: 72ad37d5
Standby: PID:C9300X-48HXN,SN:FOC2524L39P
Status: SMART AUTHORIZATION INSTALLED on Dec 03 18:34:03 2021 UTC
Last Confirmation code: 842584db
Member: PID:C9300X-48HX,SN:FOC2516LC92
Status: NOT INSTALLED

Authorizations:

C9K HSEC (Cat9K HSEC):
Description: HSEC Key for Export Compliance on Cat9K Series Switches
Total available count: 2
Enforcement type: EXPORT RESTRICTED
Term information:
Active: PID:C9300X-24HX,SN:FOC2519L8R7
Authorization type: SMART AUTHORIZATION INSTALLED
License type: PERPETUAL
Term Count: 1
Standby: PID:C9300X-48HXN,SN:FOC2524L39P
Authorization type: SMART AUTHORIZATION INSTALLED
License type: PERPETUAL
Term Count: 1

Purchased Licenses:

No Purchase Information Available

3. スタック全体の SLAC を再要求します。

ここでの SLAC を要求してインストールする方法は、デバイスが Cisco SSM に直接接続されているトポロジに対応しています。導入するトポロジに適用されるメソッドに従う必要があります。

システムメッセージは、このセットアップの全コネクテッドデバイス（アクティブ（SN: FOC2519L8R7）、スタンバイ（SN: FOC2524L39P）、およびメンバー（SN: FOC2516LC92））に SLAC がインストールされていることを示しています。

show license authorisation コマンドの出力には、更新されたタイムスタンプと SLAC インストールの新しい確認コードが表示されます。

SN:FOC2519L8R7 および SN:FOC2524L39P（スタック内の既存のデバイス）の確認コードは、72ad37d5 および 842584db からそれぞれ f6c6978d および 7ae69c8c に変更されました。

新しいメンバー（SN:FOC2516LC92）の確認コードは e3fd6642 です。

```
Device# license smart authorization request replace hseck9 all
```

```
Dec 3 18:45:33.145: %SMART_LIC-6-AUTHORIZATION_INSTALL_SUCCESS: A new licensing authorization code was successfully installed on PID:C9300X-24HX,SN:FOC2519L8R7
Dec 3 18:45:33.235: %SMART_LIC-6-AUTHORIZATION_INSTALL_SUCCESS: A new licensing authorization code was successfully installed on PID:C9300X-48HXN,SN:FOC2524L39P
Dec 3 18:45:33.319: %SMART_LIC-6-AUTHORIZATION_INSTALL_SUCCESS: A new licensing authorization code was successfully installed on PID:C9300X-48HX,SN:FOC2516LC92
```

```
Device# show license authorization
```

```
Overall status:
```

```
Active: PID:C9300X-24HX,SN:FOC2519L8R7
```

```
Status: SMART AUTHORIZATION INSTALLED on Dec 03 18:45:33 2021 UTC
```

```
Last Confirmation code: f6c6978d
```

```
Standby: PID:C9300X-48HXN,SN:FOC2524L39P
```

```
Status: SMART AUTHORIZATION INSTALLED on Dec 03 18:45:33 2021 UTC
```

```
Last Confirmation code: 7ae69c8c
```

```
Member: PID:C9300X-48HX,SN:FOC2516LC92
```

```
Status: SMART AUTHORIZATION INSTALLED on Dec 03 18:45:33 2021 UTC
```

```
Last Confirmation code: e3fd6642
```

```
Authorizations:
```

```
C9K HSEC (Cat9K HSEC):
```

```
Description: HSEC Key for Export Compliance on Cat9K Series Switches
```

```
Total available count: 3
```

```
Enforcement type: EXPORT RESTRICTED
```

```
Term information:
```

```
Active: PID:C9300X-24HX,SN:FOC2519L8R7
```

```
Authorization type: SMART AUTHORIZATION INSTALLED
```

```
License type: PERPETUAL
```

```
Term Count: 1
```

```
Standby: PID:C9300X-48HXN,SN:FOC2524L39P
```

```
Authorization type: SMART AUTHORIZATION INSTALLED
```

```
License type: PERPETUAL
```

```
Term Count: 1
```

```
Member: PID:C9300X-48HX,SN:FOC2516LC92
```

```
Authorization type: SMART AUTHORIZATION INSTALLED
```

```
License type: PERPETUAL
```

```
Term Count: 1
```

```
Purchased Licenses:
```

```
No Purchase Information Available
```

HSECK9キーが使用されているスタックにメンバーを追加するには、別の方法もあります。[C9300Xの例：スタンドアロンでのSLACの要求とHSECK9キーが使用されているスタックへの追加](#), [on page 31](#)を参照してください。

C9300Xの例：スタンドアロンでのSLACの要求とHSECK9キーが使用されているスタックへの追加

この例は、暗号化機能が使用されている既存のスタックにデバイスを追加する方法の1つを示しています。

この方法の全体的な流れは次のとおりです。スタンドアロンに SLAC をインストールする > スタンドアロンで暗号化機能を設定する > 暗号化機能が使用されている既存のスタックにデバイスを追加する。

1. 既存のスタックに関する情報を表示して確認します。

show switch detail コマンドの出力は、これが 2 メンバースタックであることを示しています。

show license authorisation コマンドの出力は、SLAC がアクティブ (C9300X-24HX、SN: FOC2519L8R7) およびスタンバイ (PID: C9300X-48HXN、SN: FOC2524L39P) にインストールされていることを示しています。

show license summary コマンドの出力は、暗号化機能が設定されていることを示しています (C9K HSEC-INUSE)。

この **show license all** コマンドの出力 (省略された出力) では、デバイスが Cisco SSM に直接接続されていることが示されています。smart 転送オプションが、Cisco SSM との通信に使用されています。

```
Device# show switch detail
Switch/Stack Mac Address : b08b.d02b.5b80 - Local Mac Address
Mac persistency wait time: Indefinite

Switch#   Role   Mac Address           Priority H/W   Current
-----
*1        Active b08b.d02b.5b80       15     P2B   Ready
2        Standby b08b.d08d.bb00       14     P2B   Ready
3        Member  0000.0000.0000       0      PP    Removed

Switch#   Stack Port Status           Neighbors
Port 1    Port 2           Port 1    Port 2
-----
1         DOWN    OK              None     2
2         OK      DOWN            1       None

Device# show license authorization
Overall status:
  Active: PID:C9300X-24HX,SN:FOC2519L8R7
    Status: SMART AUTHORIZATION INSTALLED on Dec 03 18:34:03 2021 UTC
    Last Confirmation code: 72ad37d5
  Standby: PID:C9300X-48HXN,SN:FOC2524L39P
    Status: SMART AUTHORIZATION INSTALLED on Dec 03 18:34:03 2021 UTC
    Last Confirmation code: 842584db

Authorizations:
  C9K HSEC (Cat9K HSEC):
    Description: HSEC Key for Export Compliance on Cat9K Series Switches
    Total available count: 2
    Enforcement type: EXPORT RESTRICTED
    Term information:
      Active: PID:C9300X-24HX,SN:FOC2519L8R7
        Authorization type: SMART AUTHORIZATION INSTALLED
        License type: PERPETUAL
        Term Count: 1
      Standby: PID:C9300X-48HXN,SN:FOC2524L39P
        Authorization type: SMART AUTHORIZATION INSTALLED
        License type: PERPETUAL
        Term Count: 1

Purchased Licenses:
  No Purchase Information Available

Device# show license summary
Account Information:
  Smart Account: Eg-SA As of Dec 03 18:51:59 2021 UTC
  Virtual Account: Eg-VA
```



```
License Usage:
License          Entitlement Tag          Count Status
-----
network-advantage (C9300-24 Network Advan...) 1 IN USE
dna-advantage     (C9300-24 DNA Advantage) 1 IN USE
network-advantage (C9300-48 Network Advan...) 1 IN USE
dna-advantage     (C9300-48 DNA Advantage) 1 IN USE
C9K HSEC         (Cat9K HSEC)             1 IN USE
```

Device# **show license all**

Smart Licensing Status
=====

Smart Licensing is ENABLED

<output truncated>

Transport:

```
Type: Smart
URL: https://smartreceiver-stage.cisco.com/licservice/license
Proxy:
  Not Configured
VRF:
  Not Configured
```

Miscellaneous:

```
Custom Id: <empty>
```

<output truncated>

2. 3 番目のスイッチをスタンドアロンとして起動します。

syslog には、ブートアップシーケンスが表示されます。

show switch detail コマンドの出力は、これがスタンドアロンセットアップであることを示しています。

<output truncated>

```
switch:boot
boot: attempting to boot from [flash:packages.conf]
boot: reading file packages.conf
#
Waiting for 120 seconds for other switches to boot
#####
Switch number is 3
.
.
.
Press RETURN to get started!
*Dec 3 18:29:30.097: %SMART_LIC-6-AGENT_ENABLED: Smart Agent for Licensing is enabled
*Dec 3 18:29:30.145: %SMART_LIC-6-EXPORT_CONTROLLED: Usage of export controlled features is not allowed
*Dec 3 18:29:41.412: %SYS-5-RESTART: System restarted -
<output truncated>
```

Device# **show switch detail**

```
Switch/Stack Mac Address : f87a.414b.5580 - Local Mac Address
Mac persistency wait time: Indefinite
```

Switch#	Role	Mac Address	Priority	H/W Version	Current State
1	Member	0000.0000.0000	0		Provisioned
2	Member	0000.0000.0000	0		Provisioned
*3	Active	f87a.414b.5580	1	PP	Ready

Switch#	Stack Port Status		Neighbors	
	Port 1	Port 2	Port 1	Port 2
3	DOWN	DOWN	None	None

3. スタンドアロンで、ポリシーを使用したスマートライセンスのトポロジを設定します。

この設定例は、Cisco SSM への接続なし、CSLU なしのトポロジが導入されていることを示しています。導入するトポロジに応じて、該当するコマンドを設定します。

show license authorisation コマンドの出力は、SLAC がスタンドアロンにインストールされていないことを示しています。

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

Device# show license authorization
```

```
Overall status:
  Active: PID:C9300X-48HX,SN:FOC2516LC92
  Status: NOT INSTALLED
Purchased Licenses:
  No Purchase Information Available
```

4. SLAC をインポートしてインストールします

SLAC ファイルは Cisco SSM から取得されるため、ここには示されていません。この設定例は、**license smart import** コマンドを使用して SLAC ファイルをデバイスにインストールする方法を示しています。

show license authorisation コマンドの出力は、SLAC がインストールされていることを示しています。

```
Device# license smart import tftp://10.8.0.6/user-01/SLAC-standalone.txt
Import Data Successful
Last Confirmation code UDI: PID:C9300X-48HX,SN:FOC2516LC92
  Confirmation code: 59e155ae
Device#
*Dec  3 18:58:39.026: %SMART_LIC-6-AUTHORIZATION_INSTALL_SUCCESS: A new licensing authorization code was
successfully installed on PID:C9300X-48HX,SN:FOC2516LC92
```

```
Device# show license authorization
Overall status:
  Active: PID:C9300X-48HX,SN:FOC2516LC92
  Status: SMART AUTHORIZATION INSTALLED on Dec 03 18:58:39 2021 UTC
  Last Confirmation code: 59e155ae
```

```
Authorizations:
  C9K HSEC (Cat9K HSEC):
  Description: HSEC Key for Export Compliance on Cat9K Series Switches
  Total available count: 1
  Enforcement type: EXPORT RESTRICTED
  Term information:
  Active: PID:C9300X-48HX,SN:FOC2516LC92
  Authorization type: SMART AUTHORIZATION INSTALLED
  License type: PERPETUAL
  Term Count: 1
```

```
Purchased Licenses:
  No Purchase Information Available
```

5. 暗号化機能を設定します

show license summary コマンドの出力には、暗号化機能の設定前 (NOT IN USE) および設定後 (IN USE) の HSECK9 キーのステータスが表示されます。

```
Device# show license summary
```

```
Account Information:
```

```
Smart Account: Eg-SA As of Dec 03 18:57:27 2021 UTC
```

```
Virtual Account: Eg-VA
```

```
License Usage:
```

License	Entitlement Tag	Count	Status
network-advantage	(C9300-48 Network Advan...)	1	IN USE
dna-advantage	(C9300-48 DNA Advantage)	1	IN USE
C9K HSEC	(Cat9K HSEC)	0	NOT IN USE

```
Device# configure terminal
```

```
Enter configuration commands, one per line. End with CNTL/Z.
```

```
Device(config)# interface tu10
```

```
Device(config-if)# tunnel mode ipsec ipv4
```

```
Device(config-if)# end
```

```
*Dec 3 18:59:29.309: %SMART_LIC-6-EXPORT_CONTROLLED: Usage of export controlled features is allowed for feature hseck9
```

```
Device# show license summary
```

```
Account Information:
```

```
Smart Account: Eg-SA As of Dec 03 18:57:27 2021 UTC
```

```
Virtual Account: Eg-VA
```

```
License Usage:
```

License	Entitlement Tag	Count	Status
network-advantage	(C9300-48 Network Advan...)	1	IN USE
dna-advantage	(C9300-48 DNA Advantage)	1	IN USE
C9K HSEC	(Cat9K HSEC)	1	IN USE

6. 既存のスタックに対してスタンドアロンスイッチを追加します

show switch detail コマンドの出力は、新しいメンバーがスタックに追加されたことを示しています。

show license all コマンドの出力は、新しいメンバーで SLAC が保持されていることを示しています。ここでの出力の「Status」および「Last Confirmation code」フィールドを、スタンドアロンでの SLAC インストール後の **show license authorization** コマンドの出力（上記）と比較します。

show license summary の出力は、暗号化機能が引き続き動作することを示しています（HSECK9 キーは IN-USE になっています）。

```
Chassis 3 reloading, reason - stack merge
```

```
*Dec 3 19:00:59.575: %STACKMGR-6-STACK_LINK_CHANGE: Switch 3 R0/0: stack_mgr: Stack port 1 on Switch 3 is up
```

```
*Dec 3 19:00:59.577: %STACKMGR-1-RELOAD: Switch 3 R0/0: stack_mgr: Reloading due to reason stack merge
```

```
Dec 3 19:01:08.683: %PMAN-5-EXITACTION: F0/0: pvp: Process manager is exiting: reload fp action requested
```

```
Dec 3 19:01:10.171: %PMAN-5-EXITACTION: R0/vp: Process manager is exiting: rp processes exit with reload switch code
```

```
Initializing Hardware.....
```

```
<output truncated>
```

Device# **show switch detail**

Switch/Stack Mac Address : b08b.d02b.5b80 - Local Mac Address
Mac persistency wait time: Indefinite

Switch#	Role	Mac Address	Priority	H/W Version	Current State
*1	Active	b08b.d02b.5b80	15	P2B	Ready
2	Standby	b08b.d08d.bb00	14	P2B	Ready
3	Member	f87a.414b.5580	1	PP	Ready

Switch#	Stack Port 1	Stack Port 2	Status	Neighbors Port 1	Neighbors Port 2
1	OK	OK		3	2
2	OK	OK		1	3
3	OK	OK		2	1

Device# **show license all**

Smart Licensing Status
=====

Smart Licensing is ENABLED

Export Authorization Key:
Features Authorized:
<none>

Utility:
Status: DISABLED

Smart Licensing Using Policy:
Status: ENABLED

Account Information:
Smart Account: Eg-SA As of Dec 03 18:51:59 2021 UTC
Virtual Account: Eg-VA

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

Transport:
Type: Smart
URL: https://smartreceiver-stage.cisco.com/licservice/license
Proxy:
Not Configured
VRF:
Not Configured

Miscellaneous:

Custom Id: <empty>

Policy:

Policy in use: Installed On Dec 03 18:32:37 2021 UTC
Policy name: Custom Policy
Reporting ACK required: yes (Customer Policy)
Unenforced/Non-Export Perpetual Attributes:
 First report requirement (days): 365 (Customer Policy)
 Reporting frequency (days): 0 (Customer Policy)
 Report on change (days): 90 (Customer Policy)
Unenforced/Non-Export Subscription Attributes:
 First report requirement (days): 90 (Customer Policy)
 Reporting frequency (days): 90 (Customer Policy)
 Report on change (days): 90 (Customer Policy)
Enforced (Perpetual/Subscription) License Attributes:
 First report requirement (days): 365 (Customer Policy)
 Reporting frequency (days): 90 (Customer Policy)
 Report on change (days): 90 (Customer Policy)
Export (Perpetual/Subscription) License Attributes:
 First report requirement (days): 365 (Customer Policy)
 Reporting frequency (days): 90 (Customer Policy)
 Report on change (days): 90 (Customer Policy)

Usage Reporting:

Last ACK received: Dec 03 18:37:21 2021 UTC
Next ACK deadline: Mar 03 18:37:21 2022 UTC
Reporting push interval: 30 days
Next ACK push check: Dec 03 19:04:55 2021 UTC
Next report push: Dec 03 19:05:03 2021 UTC
Last report push: Dec 03 18:52:53 2021 UTC
Last report file write: <none>

Trust Code Installed:

Active: PID:C9300X-24HX,SN:FOC2519L8R7
 INSTALLED on Dec 03 18:32:37 2021 UTC
Standby: PID:C9300X-48HXN,SN:FOC2524L39P
 INSTALLED on Dec 03 18:32:37 2021 UTC
Member: PID:C9300X-48HX,SN:FOC2516LC92
 INSTALLED on Dec 03 18:43:29 2021 UTC

License Usage

=====

network-advantage (C9300-24 Network Advantage):

Description: C9300-24 Network Advantage
Count: 1
Version: 1.0
Status: IN USE
Export status: NOT RESTRICTED
Feature Name: network-advantage
Feature Description: C9300-24 Network Advantage
Enforcement type: NOT ENFORCED
License type: Perpetual

dna-advantage (C9300-24 DNA Advantage):

Description: C9300-24 DNA Advantage
Count: 1
Version: 1.0

Status: IN USE
Export status: NOT RESTRICTED
Feature Name: dna-advantage
Feature Description: C9300-24 DNA Advantage
Enforcement type: NOT ENFORCED
License type: Subscription

network-advantage (C9300-48 Network Advantage):
Description: C9300-48 Network Advantage
Count: 2
Version: 1.0
Status: IN USE
Export status: NOT RESTRICTED
Feature Name: network-advantage
Feature Description: C9300-48 Network Advantage
Enforcement type: NOT ENFORCED
License type: Perpetual

dna-advantage (C9300-48 DNA Advantage):
Description: C9300-48 DNA Advantage
Count: 2
Version: 1.0
Status: IN USE
Export status: NOT RESTRICTED
Feature Name: dna-advantage
Feature Description: C9300-48 DNA Advantage
Enforcement type: NOT ENFORCED
License type: Subscription

C9K HSEC (Cat9K HSEC):
Description: HSEC Key for Export Compliance on Cat9K Series Switches
Count: 1
Version: 1.0
Status: IN USE
Export status: RESTRICTED - ALLOWED
Feature Name: hseck9
Feature Description: hseck9
Enforcement type: EXPORT RESTRICTED
License type: Export

Product Information

=====
UDI: PID:C9300X-24HX,SN:FOC2519L8R7

HA UDI List:

Active:PID:C9300X-24HX,SN:FOC2519L8R7
Standby:PID:C9300X-48HXN,SN:FOC2524L39P
Member:PID:C9300X-48HX,SN:FOC2516LC92

Agent Version

=====
Smart Agent for Licensing: 5.3.15_rel/49

License Authorizations

=====
Overall status:
Active: PID:C9300X-24HX,SN:FOC2519L8R7

```

Status: SMART AUTHORIZATION INSTALLED on Dec 03 18:51:56 2021 UTC
Last Confirmation code: fa4c0d80
Standby: PID:C9300X-48HXN,SN:FOC2524L39P
Status: SMART AUTHORIZATION INSTALLED on Dec 03 18:51:56 2021 UTC
Last Confirmation code: 450243e2
Member: PID:C9300X-48HX,SN:FOC2516LC92
Status: SMART AUTHORIZATION INSTALLED on Dec 03 18:58:39 2021 UTC
Last Confirmation code: 59e155ae

```

Authorizations:

```

C9K HSEC (Cat9K HSEC):
Description: HSEC Key for Export Compliance on Cat9K Series Switches
Total available count: 3
Enforcement type: EXPORT RESTRICTED
Term information:
Active: PID:C9300X-24HX,SN:FOC2519L8R7
Authorization type: SMART AUTHORIZATION INSTALLED
License type: PERPETUAL
Term Count: 1
Standby: PID:C9300X-48HXN,SN:FOC2524L39P
Authorization type: SMART AUTHORIZATION INSTALLED
License type: PERPETUAL
Term Count: 1
Member: PID:C9300X-48HX,SN:FOC2516LC92
Authorization type: SMART AUTHORIZATION INSTALLED
License type: PERPETUAL
Term Count: 1

```

Purchased Licenses:

No Purchase Information Available

Usage Report Summary:

```

=====
Total: 58, Purged: 0
Total Acknowledged Received: 20, Waiting for Ack: 33
Available to Report: 5 Collecting Data: 0

```

Device# **show license summary**

```

Load for five secs: 1%/0%; one minute: 9%; five minutes: 5%
Time source is NTP, 19:05:29.741 UTC Fri Dec 3 2021

```

Account Information:

```

Smart Account: Eg-SA As of Dec 03 19:04:56 2021 UTC
Virtual Account: Eg-VA

```

License Usage:

License	Entitlement Tag	Count	Status
network-advantage	(C9300-24 Network Advan...)	1	IN USE
dna-advantage	(C9300-24 DNA Advantage)	1	IN USE
network-advantage	(C9300-48 Network Advan...)	2	IN USE
dna-advantage	(C9300-48 DNA Advantage)	2	IN USE
C9K HSEC	(Cat9K HSEC)	1	IN USE

HSECK9 キーが使用されているスタックにメンバーを追加する他の方法については、[C9300X の例: HSECK9 キーが使用されているスタックへのメンバーの追加](#), [on page 27](#)を参照してください。

例: HSECK9 キー数の不足による SLAC のインストール失敗

この例では、SLAC をインストールしようとしたときに、Cisco SSM の該当するスマートアカウントおよびバーチャルアカウントで必要な数の HSECK9 キーが使用できない場合に何が起るかを示します。

これは、スイッチオーバーが発生した場合に中断されずに暗号化機能を使用するために、SLAC が両方のシャーシ UDI (SN:FXS221500CT および SN:FXS221500BN) にインストールされている Cisco StackWise Virtual セットアップです。

```
Device# show license udi
UDI: PID:C9407R,SN:FXS221500CT
```

```
HA UDI List:
  Active:PID:C9407R,SN:FXS221500CT
  Standby:PID:C9407R,SN:FXS221500BN
```

製品インスタンスは Cisco SSM に直接接続されていて、**license smart authorization request add hseck9 all** コマンドは、接続されているすべてのデバイス（つまり、アクティブとスタンバイ）に対して SLAC を要求してインストールするように設定されています。

最初のシステムメッセージは、SLAC がアクティブに対して正常にインストールされたことを示しています。

2 番目のシステムメッセージは、SLAC がスタンバイ (SN:FXS221500BN) に対してインストールされていないことを示しています。メッセージ内の `ERROR_ALL_COUNTS_IN_USE` コードは、Cisco SSM のスマートアカウントとバーチャルアカウントで十分な数の HSECK9 キーが使用できなかったため、インストールが失敗したことを示しています。

```
Device# license smart authorization request add hseck9 all
*Sep  6 16:58:25.528 PDT: %SMART_LIC-6-AUTHORIZATION_INSTALL_SUCCESS: A new licensing authorization code
was successfully installed on PID:C9407R,SN:FXS221500CT
```

```
*Sep  6 16:58:25.575 PDT: %SMART_LIC-3-AUTHORIZATION_INSTALL_FAILED: The install of a new licensing
authorization code has failed on PID:C9407R,SN:FXS221500BN: ERROR_ALL_COUNTS_IN_USE.
```

上記の問題を解決し、接続されているすべてのデバイスに SLAC をインストールするには、次の手順を実行します。

- Cisco SSM の該当するスマートアカウントおよびバーチャルアカウントで、必要な数の HSECK9 キーが使用可能であることを確認します。上記の例では、シャーシ UDI ごとに 1 つの HSECK9 が必要です。
- アクティブ製品インスタンスにある SLAC を返却します。
- 最後に、アクティブとスタンバイで再度 SLAC を要求してインストールします。

使用可能なライセンスの機能履歴

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 Everest 16.5.1a	基本ライセンスとアドオンライセンス	<p>デバイスでソフトウェア機能の使用を有効にします。</p> <p>基本ライセンスとアドオンライセンス, on page 1および基本ライセンスとアドオンライセンスの設定, on page 10を参照してください。</p> <p>この機能は、以下に対して導入されました</p> <ul style="list-style-type: none"> • Cisco Catalyst 9300 シリーズ スイッチ。 • Cisco Catalyst 9500 シリーズ スイッチの C9500-12Q、C9500-16X、C9500-24Q、C9500-40X モデル。
Cisco IOS XE Everest 16.6.1	基本ライセンスとアドオンライセンス	この機能は、Cisco Catalyst 9400 シリーズ スイッチに実装されました。
Cisco IOS XE Fuji 16.8.1a	基本ライセンスとアドオンライセンス	この機能は、Cisco Catalyst 9500 シリーズ スイッチのハイパフォーマンスモデル（C9500-32C、C9500-32QC、C9500-48Y4C、およびC9500-24Y4C）に導入されました。
Cisco IOS XE Fuji 16.9.2	基本ライセンスとアドオンライセンス	この機能は、Cisco Catalyst 9200 シリーズ スイッチに実装されました。
Cisco IOS XE Gibraltar 16.11.1	基本ライセンスとアドオンライセンス	この機能は、Cisco Catalyst 9600 シリーズ スイッチに導入されました。
Cisco IOS XE Bengaluru 17.6.2	高セキュリティのための輸出規制キー（HSECK9 キー）	<p>米国輸出規制法で制限されている暗号化機能の使用を許可します。制限付き暗号化機能を使用する場合は、HSECK9 キーが必要です。</p> <p>高セキュリティのための輸出規制キーまたはHSECK9キー, on page 2およびHSECK9 キー用の SLAC のインストール, on page 12を参照してください。</p> <p>この機能は、Cisco Catalyst 9300X シリーズ スイッチで導入されました。これは、IPsec 機能のために必要です。</p> <p>HSECK9 キーは Cisco Catalyst 9300X シリーズ スイッチでのみサポートされ、Cisco Catalyst 9300 シリーズ スイッチの他のモデルではサポートされません。</p>

リリース	機能	機能情報
Cisco IOS XE Cupertino 17.7.1	SLAC 要求をファイルに保存する機能。	SLAC 要求および SLAC 返却要求に必要な UDI 情報を、指定された場所の .txt ファイルに保存するオプションを導入します。その後、SLAC 要求ファイルを RUM レポートと同じ方法と場所で Cisco SSM にアップロードする必要があります。 license smart authorization request save path コマンドは特権 EXEC モードで使用します。
	基本ライセンスとアドオンライセンス	この機能は、以下に対して導入されました <ul style="list-style-type: none"> • C9400X-SUP-2 および C9400X-SUP-2XL スーパーバイザ モジュール。 • Cisco Catalyst 9500X シリーズ スイッチの C9500X-28C8D モデル。
Cisco IOS XE Cupertino 17.8.1	HSECK9 キー	この機能は、以下のプラットフォームに導入されていて、WAN MACsec 機能のために必要です。 <ul style="list-style-type: none"> • Cisco Catalyst 9500X シリーズ スイッチ。 HSECK9 は Cisco Catalyst 9500X シリーズ スイッチでのみサポートされ、Cisco Catalyst 9500 シリーズ スイッチの他のモデルではサポートされません。 <ul style="list-style-type: none"> • Cisco Catalyst 9600 シリーズ スーパーバイザ エンジン 2 (C9600X-SUP-2) および関連するラインカード。
Cisco IOS XE Dublin 17.11.1	HSECK9 キー	この機能は、スーパーバイザモジュールの C9400X-SUP-2 および C9400X-SUP-2XL に導入されていて、IPsec 機能のために必要です。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェアイメージのサポート情報を検索できます。Cisco Feature Navigator にアクセスするには、<https://cfng.cisco.com> に進みます。

翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。