使用可能なライセンス

- 使用可能なライセンスに関する情報 （1 ページ）
- 使用可能なライセンスの設定方法 （5 ページ）
- 使用可能なライセンスの機能履歴 （26 ページ）

使用可能なライセンスに関する情報

ここでは、Cisco IOS-XE ソフトウェアを実行している Cisco Catalyst 9300 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。特に指定のない限り、この情報はシリーズのすべてのモデルに適用されます。

基本ライセンスとアドオンライセンス

次の基本ライセンスとアドオンライセンスを使用できます。

基本ライセンス

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。

- Network Essentials
- Network Advantage：Network Essentials ライセンスで使用可能な機能と追加機能が含まれます。

アドオン ライセンス

アドオンライセンスでは、スイッチだけでなく Cisco Digital Network Architecture Center（Cisco DNA Center）でもシスコのイノベーションを提供しています。

アドオンライセンスは特定の日付まで有効です。アドオンライセンスは 3 年、5 年、または 7 年のサブスクリプション期間にわたって購入できます。

- DNA Essentials

- DNA Advantage：DNA Essentials ライセンスで使用可能な機能と追加機能が含まれます。

基本ライセンスとアドオンライセンスの使用に関するガイドライン

- 基本ライセンス（Network Essentials および Network-Advantage）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（DNA Essentials および DNA Advantage）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。DNA 機能を使用する場合は、期限が切れる前にライセンスを更新して、使用を継続してください。DNA 機能の使用を継続しない場合は、アドオンライセンスを非アクティブ化してからスイッチをリロードして基本ライセンス機能での運用を継続します。

  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。

表 *1*：表 *4* 許可されている組み合わせ

	DNA Essentials	DNA Advantage
Network Essentials	対応	非対応
Network Advantage	可[1]	対応

[1] この組み合わせは DNA ライセンスの更新時にのみ購入できます。DNA-Essentials の初回購入時には購入できません。

- 機能を使用できるライセンスレベルを確認するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、https://cfnng.cisco.com に進みます。cisco.com のアカウントは必要ありません。

高セキュリティライセンス

暗号化機能を提供する製品および機能は、米国輸出管理法、米国政府暗号化および輸出管理規則（EAR）の範囲内です。[2]高セキュリティ（HSECK9）は、輸出規制対象のライセンスであり、暗号化機能の使用を許可します。

このサブセクションでは、ライセンスをサポートする製品、ライセンスを必要とする暗号化機能、ライセンスを注文する際の考慮事項、ライセンスを使用するための前提条件、およびサポートされるプラットフォームでのライセンスの設定方法について説明します。

[2]

サポートされているプラットフォームとリリース

HSECK9 ライセンスは、Cisco IOS XE Bengaluru 17.6.2 以降の Cisco Catalyst 9300X シリーズ スイッチでのみ使用できます。

シリーズで使用可能な SLU の詳細については、『Cisco Catalyst 9300 Series Switches Hardware Installation Guide』を参照してください。

HSECK9 ライセンスが必要な場合

HSECK9 ライセンスは、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。HSECK9 ライセンスがないと、制限対象の暗号化機能を有効にできません。

IPsec 機能には HSECK9 ライセンスが必要です。

HSECK9 ライセンスを使用するための前提条件

次の要件を満たしていることを確認します。

- デバイスが HSECK9 ライセンスをサポートしていること。サポートされているプラットフォームとリリース （3 ページ）を参照してください。
- Cisco Smart Software Manager（CSSM）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 ライセンスがあること。暗号化機能を使用する UDI ごとに、HSECK9 ライセンスが 1 つ必要です。必要なライセンス数に関しては、スタック構成の考慮事項を確認してください。スタッキングに関する考慮事項 （4 ページ）を参照してください。
- サポートされている Smart Licensing Using Policy トポロジのいずれかを実装していること。これにより、使用する HSECK9 ライセンスごとにスマートライセンス承認コード（SLAC）をインストールできます。

  HSECK9 ライセンスは、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。SLAC はこの承認を提供し、輸出規制対象のライセンスの有効化と継続的な使用を可能にします。SLAC は CSSM で生成され、CSSM から取得されます。デバイスを CSSM に接続して SLAC を取得する方法はいくつかあります。CSSM に接続する各方法がトポロジと呼ばれます。設定セクションは、各トポロジで SLAC を取得する方法を示します（HSECK9 ライセンス用の SLAC のインストール （7 ページ））。

（注） このドキュメント（サポートされているプラットフォームとリリース （3 ページ））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セクション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。

- 暗号化機能の設定は、SLAC をインストールしてから行います。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。

発注時の考慮事項

ここでは、HSECK9 ライセンスの発注に関する重要な考慮事項について説明します。

暗号化機能を使用する UDI ごとに、個別の HSECK9 ライセンスが必要です。デバイススタックがある場合は、スタッキングに関する考慮事項 （4 ページ）セクションで必要なライセンス数に関する情報を参照してください。

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 を工場でインストールできます。

ライセンスの注文については、『Cisco Catalyst 9300 Series Ordering Guide』を参照してください。https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9300-series-switches/nb-06-cat9300-swit-ser-cte-en.html

スタッキングに関する考慮事項

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 ライセンスの考慮事項と要件について説明します。

- 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。

- 最低限、HSECK9 ライセンスを取得し、スタック内のアクティブデバイスの SLAC をインストールする必要があります。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 ライセンスも取得することを推奨します。

  スイッチオーバーが発生し、スタンバイに HSECK9 ライセンスがない場合、暗号化機能は無効になります。システムは自動的にデバイススタックをリロードし、スタック全体で暗号化機能を無効にします。

  - デバイススタックのスタンバイに HSECK9 ライセンスがインストールされていない場合に表示される、毎日のシステムメッセージ。これは、スイッチオーバーが発生したときに暗号化機能が無効になることのみを警告するものです。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たときに表示されるシステムメッセージ。この場合、スタンバイに HSECK9 ライセンスがありません。これらのメッセージは、デバイスがリロードされていることを警告します。リロード後にシステムが起動すると、暗号化機能はスタック全体で無効になります。

    ```
    %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
```

- 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。
  - 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、最後に既存のスタックにデバイスを追加します。
  - 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。

使用可能なライセンスの設定方法

ここでは、使用可能なライセンスの設定方法と、ライセンスを設定する前後に必要なタスク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の設定

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

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

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

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** **例**： `Device> enable`	特権 EXEC モードを有効にします。 プロンプトが表示されたらパスワードを入力します。
ステップ 2	**configure terminal** **例**： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**license boot level** *license_level* 例： `Device(config)# license boot level network-advantage add-on dna-advantage`	製品インスタンスで設定されたライセンスをアクティブにします。この例では、DNA Advantage ライセンスはリロード後に製品インスタンスでアクティブ化されます。
ステップ 4	**exit** 例： `Device(config)# exit`	特権 EXEC モードに戻ります。
ステップ 5	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	構成ファイルへの変更を保存します。

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

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

次のタスク

ライセンスレベルを設定すると、変更はリロード後に有効になります。レポートが必要かどうかを確認するには、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：`%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 コマンドを使用する場合は、**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。このガイドの「*Smart Licensing Using Policy*」の章のポリシーを使用したスマートライセンシングの設定方法：トポロジ別のワークフローセクションで、該当するトポロジのワークフローを参照してください。

HSECK9 ライセンス用の SLAC のインストール

このセクションでは、HSECK9 ライセンス用の SLAC をインストールする各種方法について説明します。各方法は、Smart Licensing Using Policy 環境の特定のトポロジに対応します。

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、このガイドの「Smart Licensing Using Policy」章のサポートされるトポロジセクションを参照してください。

（注） HSECK9 ライセンスを使用する場合に実装できない唯一のトポロジは、「コントローラを介して CSSM に接続」です。ここで、「コントローラ」は Cisco DNA Center を指します。Cisco DNA Center GUI には、HSECK9 をサポートする Cisco Catalyst スイッチの SLAC を生成するオプションはありません。

SLAC のインストール：CSSM に直接接続

このタスクでは、デバイス（製品インスタンス）が CSSM に直接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。

始める前に

- デバイスが HSECK9 ライセンスをサポートしていることを確認します。サポートされているプラットフォームとリリース （3 ページ）を参照してください。
- CSSM 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 ライセンスがあることを確認します。
- *CSSM* に直接接続トポロジのステップ 1 ー 3 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：CSSM に直接接続を参照してください。

手順

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

	コマンドまたはアクション	目的
ステップ 2	**license smart authorization request**{**add** | **replace**}*feature_name*{**all** | **local**} 例： `Device# license smart authorization request add hseck9 local`	• **license smart authorization request**：このオプションは、CSSM、CSLU またはSSMオンプレミスからSLACを要求します。SLACが返され、製品インスタンスに自動的にインストールされます。 既存のSLACに追加するのか置換するのかを指定します。 • **add**：要求されたライセンスを既存のSLACに追加します。新しい承認コードには、既存のSLACのすべてのライセンスと要求されたライセンスが含まれます。 • **replace**：既存の SLAC を置き換えます。新しいSLACには、要求されたライセンスのみが含まれます。既存のSLACのすべてのライセンスが返却されます。このキーワードを入力すると、製品インスタンスはこれらの既存のライセンスが使用中かどうかを確認します。使用中の場合は、対応する機能を最初に無効にするようにエラーメッセージが表示されます。 *feature_name*：SLAC の追加または置換を要求するライセンスの名前を入力します。「hseck9」と入力して、HSECK9 ライセンスの 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。

	コマンドまたはアクション	目的
		（注） SLAC がすでにインストールされている既存のスタックに（SLAC がインストールされていない）デバイスを追加した場合は、replace および all オプションを使用します。これにより、スタック内のすべてのデバイスの SLAC が要求されます。特定のメンバーの SLAC を要求することはできません。選択肢はアクティブまたはスタック全体のみです。 • **local**：高可用性設定およびスタック設定のアクティブなデバイスの承認コードを取得します。これがデフォルトのオプションです。
ステップ 3	（任意） **license smart sync{all | local}** 例： `Device# license smart sync local`	CSSM、CSLU または SSM オンプレミスと製品インスタンスの同期がトリガーされ、保留中のデータが送受信されます。 この手順はオプションであり、製品インスタンスが CSSM、CSLU または SSM オンプレミスに接続され、製品インスタンスが通信を開始するシナリオにのみ適用されます。対応するトポロジは、CSSM に直接接続、CSLU を介して CSSM に接続（製品インスタンス開始）、および SSM オンプレミス展開（製品インスタンス開始型通信）です。 このコマンドは、手動で同期をトリガーし、SLAC インストールプロセスを完了します。それ以外の場合、製品インスタンスが次回 CSLU または SSM オンプレ

	コマンドまたはアクション	目的
		ミスに接続するときに、SLAC が製品インスタンスに適用されます。

次のタスク

SLAC のインストール後に必要なタスク （21 ページ）

SLAC のインストール：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、外部との接続姓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。

このタスクは2つの部分で構成されます。最初の部分（最初のステップ）では、CSCMから各HSECK9ライセンスのSLACファイルを生成してダウンロードする必要があります。インターネットおよびCSSM Web UIに接続できるワークステーションが必要です。ステップ2以降は、ダウンロードしたSLACファイルを製品インスタンスにインポートするために設定する必要があるコマンドです。

始める前に

- デバイスが HSECK9 ライセンスをサポートしていることを確認します。サポートされているプラットフォームとリリース （3 ページ）を参照してください。
- CSSM 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 ライセンスがあることを確認します。
- *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：CSSM への接続なし、CSLU なしを参照してください。

手順

	コマンドまたはアクション	目的
ステップ 1	CSSMからのSLACの生成とファイルへのダウンロード	このタスクは、CSSM Web UI で実行します。
ステップ 2	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。プロンプトが表示されたらパスワードを入力します。
ステップ 3	**copy** *source* **bootflash:***file-name* 例： `Device# copy tftp://10.8.0.6/bootflash:example.txt`	（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

	コマンドまたはアクション	目的
		トールすることもできます（次の手順）。 • コピー元：これはファイルのコピー元の場所です。コピー元は、ローカルまたはリモートのいずれかです。 • **bootflash:**：これはブートフラッシュメモリの場合の宛先です。
ステップ 4	**license smart import** *filepath_file-name* 例： `Device# license smart import bootflash:example.txt`	ファイルを製品インスタンスにインポートしてインストールします。*filepath_filename* には、場所（ファイル名を含む）を指定します。インストール後、インストールしたファイルのタイプを示すシステムメッセージが表示されます。 （注） 複数の製品インスタンスに SLAC をインストールする場合（スタック設定など）、UDI ごとに個別の .txt SLAC ファイルをダウンロードしてください。一度に 1 つのファイルをインポートしてインストールします。

次のタスク

SLAC のインストール後に必要なタスク （21 ページ）

SLAC のインストール：CSLU を介した CSSM への接続（製品インスタンス開始）

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 CSSM に接続され、製品インスタンスが通信を開始する場合、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。

始める前に

- デバイスが HSECK9 ライセンスをサポートしていることを確認します。サポートされているプラットフォームとリリース （3 ページ）を参照してください。
- CSSM 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 ライセンスがあることを確認します。

- CSLU を介した CSSM への接続（製品インスタンス開始型通信）トポロジのステップ 1 ー 3 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：CSLU を介して CSSM に接続→製品インスタンス開始型通信の場合のタスクを参照してください。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。プロンプトが表示されたらパスワードを入力します。
ステップ 2	**license smart authorization request** {**add** | **replace**} *feature_name* {**all** | **local**} 例： `Device# license smart authorization request add hseck9 local`	• **license smart authorization request**：このオプションは、CSSM、CSLU または SSM オンプレミスから SLAC を要求します。SLAC が返され、製品インスタンスに自動的にインストールされます。 既存の SLAC に追加するのか置換するのかを指定します。 • **add**：要求されたライセンスを既存の SLAC に追加します。新しい承認コードには、既存の SLAC のすべてのライセンスと要求されたライセンスが含まれます。 • **replace**：既存の SLAC を置き換えます。新しい SLAC には、要求されたライセンスのみが含まれます。既存の SLAC のすべてのライセンスが返却されます。このキーワードを入力すると、製品インスタンスはこれらの既存のライセンスが使用中かどうかを確認します。使用中の場合は、対応する機能を最初に無効にするようにエラーメッセージが表示されます。 *feature_name*：SLAC の追加または置換を要求するライセンスの名前を入力します。「hseck9」と入力して、HSECK9 ライセンスの SLAC を要求してインストールします。

	コマンドまたはアクション	目的
		次のいずれかのオプションを入力して、デバイスを指定します。 • **all**：高可用性設定およびスタック設定のすべてのデバイスの承認コードを取得します。 （注） SLAC がすでにインストールされている既存のスタックに（SLAC がインストールされていない）デバイスを追加した場合は、replace および all オプションを使用します。これにより、スタック内のすべてのデバイスの SLAC が要求されます。特定のメンバーの SLAC を要求することはできません。選択肢はアクティブまたはスタック全体のみです。 • **local**：高可用性設定およびスタック設定のアクティブなデバイスの承認コードを取得します。これがデフォルトのオプションです。
ステップ 3	（任意） **license smart sync{all|local}** 例： `Device# license smart sync local`	CSSM、CSLU または SSM オンプレミスと製品インスタンスの同期がトリガーされ、保留中のデータが送受信されます。 この手順はオプションであり、製品インスタンスが CSSM、CSLU または SSM オンプレミスに接続され、製品インスタンスが通信を開始するシナリオにのみ適用されます。対応するトポロジは、CSSM に直接接続、CSLU を介して CSSM に接続（製品インスタンス開

	コマンドまたはアクション	目的
		始）、および SSM オンプレミス展開（製品インスタンス開始型通信）です。 このコマンドは、手動で同期をトリガーし、SLAC インストールプロセスを完了します。それ以外の場合、製品インスタンスが次回 CSLU または SSM オンプレミスに接続するときに、SLAC が製品インスタンスに適用されます。

次のタスク

SLAC のインストール後に必要なタスク （21 ページ）

SLAC のインストール：CSLU を介した CSSM への接続（CSLU 開始）

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 CSSM 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、製品インスタンスの特定のコマンド、CSSM Web UI の特定のタスク、および CSLU インターフェイスの特定のタスクを設定する必要があります。

始める前に

- デバイスが HSECK9 ライセンスをサポートしていることを確認します。サポートされているプラットフォームとリリース （3 ページ）を参照してください。
- CSSM 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 ライセンスがあることを確認します。
- CSLU を介した CSSM への接続（製品インスタンス開始型通信）トポロジのステップ 1 ー 3 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：CSLU を介して CSSM に接続→CSLU 開始型通信の場合のタスクを参照してください。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。プロンプトが表示されたらパスワードを入力します。
ステップ 2	**license smart authorization request**{**add**|**replace**}*feature_name*{**all**|**local**} 例：	• **license smart authorization request**：このオプションは、CSSM、CSLU または SSM オンプレミスから SLAC を要求します。SLAC が返され、製

	コマンドまたはアクション	目的
	`Device# license smart authorization request add hseck9 local`	品インスタンスに自動的にインストールされます。 既存の SLAC に追加するのか置換するのかを指定します。 • **add**：要求されたライセンスを既存の SLAC に追加します。新しい承認コードには、既存の SLAC のすべてのライセンスと要求されたライセンスが含まれます。 • **replace**：既存の SLAC を置き換えます。新しい SLAC には、要求されたライセンスのみが含まれます。既存の SLAC のすべてのライセンスが返却されます。このキーワードを入力すると、製品インスタンスはこれらの既存のライセンスが使用中かどうかを確認します。使用中の場合は、対応する機能を最初に無効にするようにエラーメッセージが表示されます。 *feature_name*：SLAC の追加または置換を要求するライセンスの名前を入力します。「hseck9」と入力して、HSECK9 ライセンスの 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。

	コマンドまたはアクション	目的
		（注） SLAC がすでにインストールされている既存のスタックに（SLAC がインストールされていない）デバイスを追加した場合は、replace および all オプションを使用します。これにより、スタック内のすべてのデバイスの SLAC が要求されます。特定のメンバーの SLAC を要求することはできません。選択肢はアクティブまたはスタック全体のみです。 • **local**：高可用性設定およびスタック設定のアクティブなデバイスの承認コードを取得します。これがデフォルトのオプションです。
ステップ 3	1 つ以上の製品インスタンスの SLAC の要求（CSLU インターフェイス）	このタスクは、CSLU インターフェイスで実行します。
ステップ 4	CSSM からの SLAC の生成とファイルへのダウンロード	このタスクは、CSSM Web UI で実行します。
ステップ 5	CSSM からのインポート（CSLU インターフェイス）	このタスクは、CSLU インターフェイスで実行します。完了したら、CSLU 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。

次のタスク

SLAC のインストール後に必要なタスク （21 ページ）

SLAC のインストール：SSM オンプレミス展開（製品インスタンス開始）

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、製品インスタンスが通信を開始する場合、つまり製品インスタンスが必要な情報を SSM オンプレミスにプッシュ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、最初に SSM オンプレミスで要求ファイルを作成し、CSSM Web UI で要求をアップロードし、SLAC を生成して、SLAC を SSM オンプレミスサーバーにインポートします。最後に、SLAC を要求してインストールするように製品インスタンスのコマンドを設定します。

始める前に

- デバイスが HSECK9 ライセンスをサポートしていることを確認します。サポートされているプラットフォームとリリース （3 ページ）を参照してください。
- CSSM 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 ライセンスがあることを確認します。
- SSM オンプレミス展開（製品インスタンス開始）トポロジのステップ 1 ー 3 c. を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：SSM オンプレミス展開→製品インスタンス開始型通信の場合のタスクを参照してください。

手順

	コマンドまたはアクション	目的
ステップ 1	承認コード要求の送信（SSM オンプレミス UI）	このタスクは、SSM オンプレミス UI で実行します。
ステップ 2	CSSM からの SLAC の生成とファイルへのダウンロード	このタスクは、CSSM Web UI で実行します。
ステップ 3	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。プロンプトが表示されたらパスワードを入力します。
ステップ 4	**license smart authorization request** {**add** | **replace**} *feature_name* {**all** | **local**} 例： `Device# license smart authorization request add hseck9 local`	• **license smart authorization request**：このオプションは、CSSM、CSLU または SSM オンプレミスから SLAC を要求します。SLAC が返され、製品インスタンスに自動的にインストールされます。 既存の SLAC に追加するのか置換するのかを指定します。 • **add**：要求されたライセンスを既存の SLAC に追加します。新

	コマンドまたはアクション	目的
		しい承認コードには、既存の SLAC のすべてのライセンスと要求されたライセンスが含まれます。 • **replace**：既存の SLAC を置き換えます。新しい SLAC には、要求されたライセンスのみが含まれます。既存の SLAC のすべてのライセンスが返却されます。このキーワードを入力すると、製品インスタンスはこれらの既存のライセンスが使用中かどうかを確認します。使用中の場合は、対応する機能を最初に無効にするようにエラーメッセージが表示されます。 *feature_name*：SLAC の追加または置換を要求するライセンスの名前を入力します。「hseck9」と入力して、HSECK9 ライセンスの 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。

	コマンドまたはアクション	目的
		（注） SLAC がすでにインストールされている既存のスタックに（SLAC がインストールされていない）デバイスを追加した場合は、replace および all オプションを使用します。これにより、スタック内のすべてのデバイスの SLAC が要求されます。特定のメンバーの SLAC を要求することはできません。選択肢はアクティブまたはスタック全体のみです。 • **local**：高可用性設定およびスタック設定のアクティブなデバイスの承認コードを取得します。これがデフォルトのオプションです。
ステップ 5	（任意） **license smart sync{all|local}** 例： `Device# license smart sync local`	CSSM、CSLU または SSM オンプレミスと製品インスタンスの同期がトリガーされ、保留中のデータが送受信されます。 この手順はオプションであり、製品インスタンスが CSSM、CSLU または SSM オンプレミスに接続され、製品インスタンスが通信を開始するシナリオにのみ適用されます。対応するトポロジは、CSSM に直接接続、CSLU を介して CSSM に接続（製品インスタンス開始）、および SSM オンプレミス展開（製品インスタンス開始型通信）です。 このコマンドは、手動で同期をトリガーし、SLAC インストールプロセスを完了します。それ以外の場合、製品インスタンスが次回 CSLU または SSM オンプレ

	コマンドまたはアクション	目的
		ミスに接続するときに、SLAC が製品インスタンスに適用されます。

次のタスク

SLAC のインストール後に必要なタスク （21 ページ）

SLAC のインストール：SSM オンプレミス展開（SSM オンプレミス開始）

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、CSSM 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。

始める前に

- デバイスが HSECK9 ライセンスをサポートしていることを確認します。サポートされているプラットフォームとリリース （3 ページ）を参照してください。
- CSSM 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 ライセンスがあることを確認します。
- SSM オンプレミス展開（製品インスタンス開始）トポロジのステップ 1 ー 3 a. を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：SSM オンプレミス展開→SSM オンプレミスインスタンス開始型通信の場合のタスクを参照してください。

手順

	コマンドまたはアクション	目的
ステップ 1	承認コード要求の送信（SSM オンプレミス UI）。	このタスクは、SSM オンプレミス UI で実行します。
ステップ 2	SSM オンプレミス UI で、[Reports] > [Synchronisation pull schedule with the devices] > [Synchronize now with the device] に移動します。	この手順は任意です。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。

次のタスク

SLAC のインストール後に必要なタスク （21 ページ）

SLAC の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。

手順

ステップ 1 SLAC のインストールと HSECK9 ライセンスの使用を確認します。

- **show license authorization** 特権 EXEC コマンドの出力の承認ステータスが、Status: SMART AUTHORIZATION INSTALLED on <timestamp> と表示されていることを確認します。これは、SLAC がインストールされていることを意味します。複数の SLA Cを（高可用性またはスタック構成セットアップで）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上記のステータスが表示されていることを確認します。
- **show license summary** 特権 EXEC コマンドの出力で、使用状況ステータスとカウントに [NOT IN USE] と 0 が表示されていることを確認します。これは、HSECK9 ライセンスは使用可能ですが、まだ使用されていないことを意味します。
- SLAC のインストール後に、次のシステムメッセージが表示されます。

  `Error Message %SMART_LIC-6-AUTHORIZATION_INSTALL_SUCCESS: A new licensing authorization code was successfully installed on: [chars].` [chars] は、承認コードが正常に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.`

例：

```
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
```

ステップ 2 暗号化機能を設定します。

次の IPsec 設定は例を示すものにすぎません。機能の設定については、 Cisco IOS XE <リリース番号>（Catalyst 9300 スイッチ）『*Security Configuration Guide*』の「*Configuring IPsec*」の章を参照してください。

例：

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# int tu10
Device(config-if)# tunnel mode ipsec ipv4
Device(config-if)# end
```

ステップ 3 再度、HSECK9 ライセンス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使用状況とカウントが、[IN USE] と 1 に変わります。

（注） IN USE としてカウントされるのは、特定の時点で 1 つのライセンスのみです。

スタック構成のステップアップで複数のデバイスにSLACをインストールした場合でも、**show license summary** コマンド出力のライセンス使用カウントには 1 だけが表示されます。これは、特定の時点で 1 つの HSECK9 ライセンス（アクティブなライセンス）だけが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 ライセンスが使用されます。スタンバイが新しくアクティブになっても、使用されているライセンスは 1 つであるため、使用カウントは 1 のままです。

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
  hseck9                  (Cat9K HSEC)                      1 IN USE
```

ステップ 4 レポートが必要かどうかを確認します。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。このガイドの「*Smart Licensing Using Policy*」の章のポリシーを使用したスマートライセンシングの設定方法：トポロジ別のワークフローセクションで、該当するトポロジのワークフローを参照してください。

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：`%SMART_LIC-6-REPORTING_REQUIRED: A Usage report acknowledgement 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 コマンドを使用する場合は、**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。この場合、RUM レポートを送信し、この日付までに ACK がインストールされていることを確認する必要があります。

SLAC の返却

このタスクでは、SLAC を返却し、HSECK9 ライセンスを CSSM のライセンスプールに返却する方法を示します。このタスクは、すべてのトポロジで使用できます。

次の状況では、SLAC および HSECK9 ライセンスを返却することができます。

- デバイスで（HSECK9 ライセンスが必要な）暗号化機能を使用する必要がなくなった。
- 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、CSSM に RUM レポートを送信することが推奨されます。

始める前に

HSECK9 ライセンスを使用した暗号化機能を無効化または設定解除し、HSECK9 ライセンスのライセンス使用状況が [NOT IN USE] であることを確認します。

手順

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

ステップ 2	**show license summary**
	例：
	`Device# show license summary`
	`License Usage:`
	`License Entitlement Tag Count Status`
	`---`
	`network-advantage (C9300-24 Network`
		（任意）ライセンスの使用状況の概要を表示します。この手順は、SLAC を返却する場合にのみ適用されます。
		暗号化機能を無効にした後でも、HSECK9 ライセンスのステータスが [IN USE] と表示される場合は、次の手順を実行します。この例の場合を示します。

	コマンドまたはアクション	目的
	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 ライセンスのステータスが [NOT IN USE] と表示された場合は、ステップ 5 に進みます。

ステップ 3	**platform hsec-license-release**
	例：
	`Device# configure terminal`
	`Device(config)# platform hsec-license-release`
	`HSEC license is released`
	`Device(config)# exit`
		（任意）グローバル コンフィギュレーション モードを開始し、HSECK9 ライセンスを返却したら、特権 EXEC モードに戻ります。
		HSECK9 ライセンスを使用する暗号化機能が無効または未設定で、ライセンスがまだ [IN USE] と表示されている場合、このコマンドにより HSECK9 ライセンスが強制的に [NOT IN USE] に変更されます。

ステップ 4	**show license summary**
	例：
	`Device# show license summary`
	`License Usage:`
	`License  Entitlement Tag  Count Status`
	`---`
	`network-advantage  (C9300-24 Network Advan...)  1 IN USE`
	`dna-advantage  (C9300-24 DNA Advantage)  1 IN USE`
	`network-advantage  (C9300-48 Network Advan...)  2 IN USE`
	`dna-advantage  (C9300-48 DNA Advantage)  2 IN USE`
	`C9K HSEC  (Cat9K HSEC)  0 NOT IN USE`
		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。使用中の場合は、まず機能を無効にする必要があります。

ステップ 5	**license smart authorization return{all | local}{offline[*path*] | online}**
	例：
	`Device# license smart authorization return all online`
	`OR`
	`Device# license smart authorization return all offline`
	`Enter this return code in Cisco Smart Software Manager portal:`
		CSSM のライセンスプールに承認コードを返却します。このコマンドを入力すると、戻りコードが表示されます。
		製品インスタンスを指定します。
		• all：高可用性セットアップまたはスタック構成セットアップで接続されたすべての製品インスタンスに対してアクションを実行します。

	コマンドまたはアクション	目的
	UDI: PID:C9300X-24HX,SN:FOC2519L8R7 Return code: Cr9JHx-L1x5Rj-ftwzg1-h9QZAU-LE5DT1-babWeL-FABPt9-Wr1Dn7-Rp7 OR Device# **license smart authorization return all** **offline bootflash:return-code.txt**	• local：アクティブな製品インスタンスに対してアクションを実行します。これがデフォルトのオプションです。 CSSMに接続しているかどうかを指定します。 • CSSMに接続している場合、または製品インスタンス開始型通信のトポロジ（CSLU または SSM オンプレミス）を実装している場合は、**online** を入力します。コードは自動的に CSSM に返却され、確認が返されて製品インスタンスにインストールされます。このオプションを選択すると、戻りコードが自動的に CSSM に送信されます。 • CSSMに接続されていない場合、または CSLU 開始型通信または SSM オンプレミス開始型通信のトポロジを実装した場合は、**offline**[*filepath_filename*] を入力します。**offline** キーワードのみを入力する場合は、CLIに表示される戻りコードをコピーし、CSSMに入力します。戻りコードをファイルに保存する場合は、ファイルからコードをコピーし、CSSMに同じコードを入力できます。ファイル形式は、読み取り可能な任意の形式にすることができます（これはアップロードされません）。例：`Device# license smart authorization return local offline bootflash:return-code.txt` CSSM に戻りコードを入力するには、次のタスクを実行します。 CSSMでのSLAC戻りコードの入力と製品インスタンスの削除
ステップ 6	**show license authorization** 例：	ライセンス情報を表示します。出力の `License Authorizations` ヘッダーを確認します。返却プロセスが正常に完了する

	コマンドまたはアクション	目的

	`Device# show license authorization`
	
	`License Authorizations`
	`=====================`
	`Overall status:`
	`  Active:`
	`PID:C9300X-24HX,SN:FOC2519L8R7`
	`  Status: NOT INSTALLED`
	`  Last return code:`
	`Cr9JHx-L1x5Rj-ftwzg1-h9QZAU-LE5DT1-`
	`babWeL-FABPt9-Wr1Dn7-Rp7`
	`  Standby:`
	`PID:C9300X-48HXN,SN:FOC2524L39P`
	`  Status: NOT INSTALLED`
	`  Member:`
	`PID:C9300X-48HX,SN:FOC2516LC92`
	`  Status: NOT INSTALLED`
	`<output truncated>`
		と、`Last return code:` フィールドに戻りコードが表示されます。

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	Cisco Catalyst 9300 シリーズ スイッチで使用可能なソフトウェア機能は、基本ライセンスまたはアドオンライセンスレベルに分類されます。 基本ライセンスとアドオンライセンス （1 ページ）および基本ライセンスとアドオンライセンスの設定 （5 ページ）を参照してください。
Cisco IOS XE Bengaluru 17.6.2	高セキュリティ（HSECK9）ライセンス	Cisco Catalyst 9300X シリーズ スイッチでの HSECK9 ライセンスのサポートを導入します。 HSECK9 ライセンスは、米国輸出管理法で制限されている暗号化機能の使用を許可する、輸出規制対象ライセンスです。制限付き暗号化機能を使用する場合は、HSECK9 ライセンスが必要です。高セキュリティライセンス （2 ページ）および HSECK9 ライセンス用の SLAC のインストール （7 ページ）を参照してください。

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://cfnng.cisco.com/にアクセスします。

http://www.cisco.com/go/cfn。