



ライセンス：スマート ソフトウェア ライセンシング

スマート ソフトウェア ライセンシングによって、ライセンスを購入し、ライセンスのプールを一元管理することができます。製品認証キー（PAK）ライセンスとは異なり、スマートライセンスは特定のシリアル番号に関連付けられません。各ユニットのライセンスキーを管理しなくても、簡単にASAを導入したり使用を終了したりできます。スマート ソフトウェア ライセンスを利用すれば、ライセンスの使用状況と要件をひと目で確認することもできます。



(注) スマート ソフトウェア ライセンシングは、ISA 3000 ではサポートされていません。PAK ライセンスを使用します。[PAK ライセンスについて](#)を参照してください。

プラットフォーム別のスマートライセンスの機能と動作の詳細については、「[Smart Enabled Product Families](#)」を参照してください。

- [スマート ソフトウェア ライセンスについて](#) (1 ページ)
- [スマート ソフトウェア ライセンスの前提条件](#) (30 ページ)
- [スマート ソフトウェア ライセンスのガイドライン](#) (31 ページ)
- [スマート ソフトウェア ライセンスのデフォルト](#) (31 ページ)
- [ASA 仮想：スマート ソフトウェア ライセンスの設定](#) (32 ページ)
- [Firepower 4100/9300：スマート ソフトウェア ライセンスの設定](#) (54 ページ)
- [その他のモデル：スマート ソフトウェア ライセンシングの設定](#) (57 ページ)
- [モデルごとのライセンス](#) (74 ページ)
- [スマート ソフトウェア ライセンシングのモニタリング](#) (89 ページ)
- [Smart Software Manager 通信](#) (92 ページ)
- [スマート ソフトウェア ライセンスの履歴](#) (95 ページ)

スマート ソフトウェア ライセンスについて

シスコ スマート ライセンシングは、シスコ ポートフォリオ全体および組織全体でソフトウェアをより簡単かつ迅速に一貫して購入および管理できる柔軟なライセンスモデルです。また、

これは安全です。ユーザがアクセスできるものを制御できます。スマートライセンスを使用すると、次のことが可能になります。

- **簡単なアクティベーション**：スマートライセンスは、組織全体で利用できるソフトウェアライセンスのプールを確立します。PAK（製品アクティベーションキー）は不要です。
- **管理の統合**：Cisco License Central は、使いやすいポータルですべてのシスコ製品とサービスの完全なビューを提供します。所有しているものと使用しているものを常に把握できます。
- **ライセンスの柔軟性**：ライセンスはハードウェアにノードロックされていないため、必要に応じてライセンスを簡単に使用および転送できます。

スマートライセンスを使用するには、まず Cisco Software Central でスマートアカウントを設定する必要があります（software.cisco.com）。

シスコライセンスの概要については詳しくは、cisco.com/go/licensingguide を参照してください。

Firepower 4100/9300 シャーシの ASA のスマート ソフトウェア ライセンシング

Firepower 4100/9300 シャーシ 上の ASA では、スマート ソフトウェア ライセンシングの設定は、Firepower 4100/9300 シャーシ スーパーバイザと ASA に分割されています。

- Firepower 4100/9300 シャーシ：Smart Software Manager との通信に使用するパラメータなど、すべてのスマート ソフトウェア ライセンシング インフラストラクチャをシャーシで設定します。Firepower 4100/9300 シャーシ 自体の動作にライセンスは必要ありません。ライセンスの手順については、[FXOS configuration guide](#) を参照してください。



(注) シャーシ間クラスタリングでは、クラスタ内の各シャーシで同じスマートライセンス方式を有効にする必要があります。

- ASA アプリケーション：ASA のすべてのライセンスの権限付与を設定します。

Smart Software Manager とアカウント

デバイスの 1 つ以上のライセンスを購入する場合は、Cisco Smart Software Manager で管理します。

<https://software.cisco.com/#module/SmartLicensing>

Smart Software Manager では、組織のマスター アカウントを作成できます。



- (注) まだアカウントをお持ちでない場合は、リンクをクリックして[新しいアカウントを設定](#)してください。Smart Software Manager では、組織のマスター アカウントを作成できます。

デフォルトでは、ライセンスはマスターアカウントの下でのデフォルトの仮想アカウントに割り当てられます。アカウントの管理者として、オプションで追加の仮想アカウントを作成できます。たとえば、地域、部門、または子会社ごとにアカウントを作成できます。複数の仮想アカウントを使用することで、多数のライセンスおよびデバイスの管理をより簡単に行うことができます。

オフライン管理

デバイスにインターネットアクセスがなく、Smart Software Manager に登録できない場合は、オフラインライセンスを構成する必要があります。

永久ライセンスの予約

デバイスがセキュリティ上の理由でインターネットにアクセスできない場合、オプションで、各 ASA の永続ライセンスを要求できます。永続ライセンスでは、Smart Software Manager への定期的なアクセスは必要ありません。PAK ライセンスの場合と同様にライセンスを購入し、Cisco ASA のライセンスキーをインストールすることができます。PAK ライセンスとは異なり、ライセンスの取得と管理に Smart Software Manager を使用することができます。通常のスマート ライセンス モードと永続ライセンスの予約モード間で簡単に切り替えることができます。



- (注) ASA は特定のライセンス予約 (SLR) をサポートしていません。SLR では、特定の機能権限が永続的に有効になっています。Cisco ASA は、すべての機能が永続的に有効になっている PLR のみをサポートします。

ASA Virtual 永久ライセンス予約



- (注) 永続ライセンス予約は、VMware と KVM のみでサポートされます。

次のすべての機能を有効にするモデル固有のライセンスを取得できます。

- 使用中のモデルの最大スループット
- Essentials 層
- 高度暗号化 (3DES および AES) ライセンス (スマート ライセンシング アカウントで有効にしている場合)
- プラットフォームに対して有効化される セキュアクライアント の機能



- (注) セキュアクライアントの機能を使用するには、セキュアクライアントの使用権を有効にするセキュアクライアントライセンスを購入する必要があります（[Secure Client Advantage](#)、[Secure Client Premier](#)、および[Secure Client VPNのみライセンス](#)（9 ページ）を参照）。

メモリおよびvCPUに基づく永続ライセンス予約モード

ASA 仮想に割り当てられた RAM と vCPU に基づいて、モデル固有のライセンスを設定できます。たとえば、8 GB RAM と 4 つの vCPU を搭載した ASA 仮想の場合、常に 2G のスループットを備えた ASAv30 ライセンスを使用します。

vCPU およびメモリとライセンスの関係は次のとおりです。

- 2 GB、1 vCPU : ASAv5 (100 M) (**license smart set_plr5** コマンドを実行する必要があります。それ以外の場合は、ASAv10 ライセンスが 1 G のスループットを可能にするように割り当てられます)。



- (注) バージョン 9.13 で、ASAv5 の RAM 要件が 2 GB に増加しました。Cisco ASA は、割り当てられたメモリをチェックし、2 GB の RAM が ASAv5 ではなく ASAv10 であると判断していたため、この増加により、ASAv5 の永続ライセンスが機能しなくなっています。ASAv5 の永続ライセンスを機能させるために、このモデルの追加メモリを認識するように Cisco ASA を設定できます。

- 2 GB、1 vCPU : ASAv10 (1G)
- 8 GB、4 vCPU : ASAv30 (2G)
- 16 GB、8 vCPU : ASAv50 (10G)
- 32 GB、16 vCPU : ASAv100 (20G)

後でモデルレベルを変更したい場合は、現在のライセンスを返却し、変更後のモデルレベルに対応する新規ライセンスを要求する必要があります。展開済みの ASA 仮想のモデルを変更するには、新しいモデルの要件に合わせるために、ハイパーバイザから vCPU と DRAM の設定を変更します。これらの値については、『[ASA 仮想 Virtual Getting Started Guide](#)』を参照してください。

ライセンスの使用を停止した場合、ASA 仮想でリターンコードを生成し、そのコードを Smart Software Manager に入力して、ライセンスを返却する必要があります。使用していないライセンスの料金を支払うことのないように、返却プロセスに正確に従ってください。

永続ライセンス予約の設定の詳細については、[ASA 仮想：永続ライセンス予約の設定](#)（49 ページ）を参照してください。

Firepower 1010 永続ライセンスの予約

すべての機能を有効にするライセンスを取得できます。

- Essentials 層
- Security Plus
- 高度暗号化（3DES/AES）ライセンス（アカウントが適格の場合）
- プラットフォームの上限まで有効化される セキュアクライアント の機能

セキュアクライアント の機能を使用するには、セキュアクライアント の使用権を有効にするセキュアクライアントライセンスを購入する必要があります（[Secure Client Advantage](#)、[Secure Client Premier](#)、および[Secure Client VPN のみライセンス](#)（9 ページ）を参照）。



(注) また、ASA の設定で権限付与を要求することにより、ASA でそれらを使用できるようにする必要があります。

ライセンスの使用を停止した場合、ASA で戻りコードを生成し、そのコードを Smart Software Manager に入力して、ライセンスを返却する必要があります。使用していないライセンスの料金の支払うことのないように、返却プロセスに正確に従ってください。

Firepower 1100 永続ライセンスの予約

すべての機能を有効にするライセンスを取得できます。

- Essentials 層
- 最大セキュリティコンテキスト数
- 高度暗号化（3DES/AES）ライセンス（アカウントが適格の場合）
- プラットフォームの上限まで有効化される セキュアクライアント の機能

セキュアクライアント の機能を使用するには、セキュアクライアント の使用権を有効にするセキュアクライアントライセンスを購入する必要があります（[Secure Client Advantage](#)、[Secure Client Premier](#)、および[Secure Client VPN のみライセンス](#)（9 ページ）を参照）。



(注) また、ASA の設定で権限付与を要求することにより、ASA でそれらを使用できるようにする必要があります。

ライセンスの使用を停止した場合、ASA で戻りコードを生成し、そのコードを Smart Software Manager に入力して、ライセンスを返却する必要があります。使用していないライセンスの料金の支払うことのないように、返却プロセスに正確に従ってください。

Firepower 2100 永続ライセンスの予約

すべての機能を有効にするライセンスを取得できます。

- Essentials 層
- 最大セキュリティコンテキスト数
- 高度暗号化 (3DES/AES) ライセンス (アカウントが適格の場合)
- プラットフォームの上限まで有効化される セキュアクライアント の機能

セキュアクライアント の機能を使用するには、セキュアクライアント の使用権を有効にするセキュアクライアント ライセンスを購入する必要があります ([Secure Client Advantage](#)、[Secure Client Premier](#)、および[Secure Client VPN のみライセンス \(9 ページ\)](#) を参照)。



(注) また、ASA の設定で権限付与を要求することにより、ASA でそれらを使用できるようにする必要があります。

ライセンスの使用を停止した場合、ASA で戻りコードを生成し、そのコードを Smart Software Manager に入力して、ライセンスを返却する必要があります。使用していないライセンスの料金の支払うことのないように、返却プロセスに正確に従ってください。

Cisco Secure Firewall 3100/4200 永続ライセンス予約

すべての機能を有効にするライセンスを取得できます。

- Essentials 層
- 最大セキュリティコンテキスト数
- キャリア ライセンス
- 高度暗号化 (3DES/AES) ライセンス (アカウントが適格の場合)
- プラットフォームの上限まで有効化される セキュアクライアント の機能

セキュアクライアント の機能を使用するには、セキュアクライアント の使用権を有効にするセキュアクライアント ライセンスを購入する必要があります ([Secure Client Advantage](#)、[Secure Client Premier](#)、および[Secure Client VPN のみライセンス \(9 ページ\)](#) を参照)。



(注) また、ASA の設定で権限付与を要求することにより、ASA でそれらを使用できるようにする必要があります。

ライセンスの使用を停止した場合、ASA で戻りコードを生成し、そのコードを Smart Software Manager に入力して、ライセンスを返却する必要があります。使用していないライセンスの料金の支払うことのないように、返却プロセスに正確に従ってください。

Firepower 4100/9300 シャーシ永久ライセンス予約

すべての機能を有効にするライセンスを取得できます。

- Essentials 層。
- 最大セキュリティコンテキスト数
- キャリア ライセンス
- 高度暗号化（3DES/AES）ライセンス（アカウントが適格の場合）
- プラットフォームの上限まで有効化される セキュアクライアント の機能

セキュアクライアント の機能を使用するには、セキュアクライアント の使用権を有効にするセキュアクライアントライセンスを購入する必要があります（[Secure Client Advantage](#)、[Secure Client Premier](#)、および[Secure Client VPN のみライセンス](#)（9 ページ）を参照）。



(注) ライセンスは Firepower 4100/9300 シャーシ上で管理されますが、それに加えて ASA の設定で権限付与を要求することにより、ASA でそれらを使用できるようにする必要があります。ライセンスを管理するには、『[FXOS configuration guide](#)』を参照します。

ライセンスの使用を停止した場合、Firepower 4100/9300 シャーシで戻りコードを生成し、そのコードを Smart Software Manager に入力して、ライセンスを返却する必要があります。使用していないライセンスの料金の支払うことのないように、返却プロセスに正確に従ってください。

Smart Software Manager オンプレミス

デバイスがセキュリティ上の理由でインターネットにアクセスできない場合、オプションで、仮想マシン（VM）としてローカル Smart Software Manager オンプレミスサーバー（旧「Smart Software サテライトサーバー」）をインストールできます。Smart Software Manager オンプレミスは、Smart Software Manager の機能の一部を提供します。これにより、すべてのローカルデバイスに不可欠なライセンシングサービスを提供できます。ライセンスの使用状況を同期するためにメインの Smart Software Manager に定期的に接続する必要があるのは、Smart Software Manager オンプレミスだけです。スケジュールに沿って同期するか、または手動で同期できます。

Smart Software Manager オンプレミスでは、次の機能を実行できます。

- ライセンスの有効化または登録
- 企業ライセンスの表示
- 会社のエンティティ間でのライセンス移動

詳細については、『[Cisco Smart Software Manager On-Prem Data Sheet](#)』を参照してください。

仮想アカウントごとに管理されるライセンスとデバイス

ライセンスとデバイスは仮想アカウントごとに管理されます。つまり、その仮想アカウントのデバイスのみが、そのアカウントに割り当てられたライセンスを使用できます。追加のライセンスが必要な場合は、別の仮想アカウントから未使用のライセンスを転用できます。仮想アカウント間でデバイスを転送することもできます。

Firepower 4100/9300 シャーシ上で動作する ASA の場合：シャーシのみがデバイスとして登録される一方で、シャーシ内の ASA アプリケーションはそれぞれ固有のライセンスを要求します。たとえば、3つのセキュリティ モジュールを搭載した Firepower 9300 シャーシでは、全シャーシが1つのデバイスとして登録されますが、各モジュールは合計3つのライセンスを別個に使用します。

評価ライセンス

ASA 仮想

ASA 仮想 は、評価モードをサポートしません。Smart Software Manager への登録の前に、ASA 仮想 は厳しいレート制限状態で動作します。

Firepower 1000

Firepower 1000 は、Smart Software Manager への登録の前に 90 日間（合計使用時間）評価モードで動作します。デフォルトの権限のみが有効になります。この期間が終了すると、Firepower 1000 はコンプライアンス違反の状態になります。



(注) 高度暗号化（3DES/AES）の評価ライセンスを受け取ることはできません。高度暗号化（3DES/AES）ライセンスを有効にするエクスポートコンプライアンス トークンを受け取るには、Smart Software Manager に登録する必要があります。

Firepower 2100

Firepower 2100 は、Smart Software Manager への登録の前に 90 日間（合計使用時間）評価モードで動作します。デフォルトの権限のみが有効になります。この期間が終了すると、Firepower 2100 はコンプライアンス違反の状態になります。



(注) 高度暗号化（3DES/AES）の評価ライセンスを受け取ることはできません。高度暗号化（3DES/AES）ライセンスを有効にするエクスポートコンプライアンス トークンを受け取るには、Smart Software Manager に登録する必要があります。

Cisco Secure Firewall 3100/4200

Cisco Secure Firewall 3100/4200 は、Smart Software Manager への登録の前に 90 日間（合計使用時間）評価モードで動作します。デフォルトの権限のみが有効になります。この期間が終了すると、Cisco Secure Firewall 3100/4200 はコンプライアンス違反の状態になります。



- (注) 高度暗号化（3DES/AES）の評価ライセンスを受け取ることはできません。高度暗号化（3DES/AES）ライセンスを有効にするエクスポートコンプライアンス トークンを受け取るには、Smart Software Manager に登録する必要があります。

Firepower 4100/9300 シャーシ

Firepower 4100/9300 シャーシ は、次の 2 種類の評価ライセンスをサポートしています。

- シャーシレベル評価モード：Firepower 4100/9300 シャーシ は、Smart Software Manager への登録の前に 90 日間（合計使用時間）評価モードで動作します。このモードでは、ASA は固有の権限付与を要求できません。デフォルトの権限のみが有効になります。この期間が終了すると、Firepower 4100/9300 シャーシはコンプライアンス違反の状態になります。
- 権限付与ベースの評価モード：Firepower 4100/9300 シャーシ が Smart Software Manager に登録された後、ASA に割り当て可能な時間ベースの評価ライセンスを取得できます。ASA で、通常どおりに権限付与を要求します。時間ベースのライセンスの期限が切れると、時間ベースのライセンスを更新するか、または永続ライセンスを取得する必要があります。



- (注) 高度暗号化（3DES/AES）の評価ライセンスを受け取ることはできません。高度暗号化（3DES/AES）ライセンスを有効にするエクスポートコンプライアンス トークンを受け取るには、Smart Software Manager に登録して永続ライセンスを取得する必要があります。

ライセンスについて（タイプ別）

ここでは、ライセンスに関する追加情報をタイプ別に説明します。

Secure Client Advantage、Secure Client Premier、および Secure Client VPN のみライセンス

セキュアクライアントライセンスは ASA に直接適用されません。ただし、ASA をセキュアクライアントヘッドエンドとして使用する権利を保証するには、ライセンスを購入してスマートアカウントに追加する必要があります。

- Secure Client Advantage および Secure Client Premier ライセンスの場合は、スマートアカウントのすべての ASA で使用する予定のピアの数を合計し、その多くのピア用にライセンスを購入します。

- Secure Client VPN のみの場合は、ASA ごとに1つのライセンスを購入します。複数の ASA で共有できるピアのプールを提供する他のライセンスとは異なり、Secure Client VPN のみライセンスはヘッドエンド単位です。

詳細については、以下を参照してください。

- [Cisco セキュアクライアント 発注ガイド](#)
- [セキュアクライアント ライセンスに関するよくある質問 \(FAQ\)](#)

その他の VPN ピア

その他の VPN ピアには、次の VPN タイプが含まれています。

- IKEv1 を使用した IPsec リモート アクセス VPN
- IKEv1 を使用した IPsec サイトツーサイト VPN
- IKEv2 を使用した IPsec サイトツーサイト VPN

このライセンスは基本ライセンスに含まれています。

合計 VPN ピア。全タイプの合計

- 合計 VPN ピアは、セキュアクライアント とその他の VPN ピアを合算した、許可される VPN ピアの最大数となります。たとえば、合計が 1000 の場合はセキュアクライアント とその他の VPN ピアを 500 ずつ、またはセキュアクライアント を 700 とその他の VPN ピア 300 を同時に許可できます。あるいは、1000 すべてをセキュアクライアント に使用することも可能です。合計 VPN ピアが最大数を超えた場合は、ASA をオーバーロードして、適切なネットワークのサイズに設定してください。

暗号化ライセンス

高度暗号化：ASA 仮想

Smart Software Manager または Smart Software Manager オンプレミスサーバーに接続する前に、管理接続に高度暗号化（3DES/AES）を使用できるため、ASDM を起動して Smart Software Manager に接続することが可能です。（VPN などの）高度暗号化を必要とする through-the-box トラフィックの場合、Smart Software Manager に接続して高度暗号化ライセンスを取得するまで、スループットは厳しく制限されます。

スマート ソフトウェア ライセンシング アカウントから ASA 仮想 の登録トークンを要求する場合、[このトークンに登録した製品でエクスポート制御機能を許可する（Allow export-controlled functionality on the products registered with this token）] チェックボックスをオンにして、高度暗号化（3DES/AES）のライセンスが適用されるようにします（お使いのアカウントでその使用が許可されている必要があります）。ASA 仮想 が後でコンプライアンス違反になった場合、エクスポートコンプライアンス トークンが正常に適用されていれば、ASA 仮想 はライセンスを保持し、レート制限状態に戻ることはありません。ASA 仮想 を再登録し、エクスポートコ

ンプライアンスが無効になっている場合、または ASA 仮想 を工場出荷時の設定に復元した場合、ライセンスは削除されます。

最初に高度暗号化なしで ASA 仮想 を登録し、後で高度暗号化を追加する場合は、新しいライセンスを有効にするために ASA 仮想 をリロードする必要があります。

永続ライセンス予約のライセンスの場合、アカウントに使用資格があれば、高度暗号化 (3DES/AES) ライセンスが有効になります。

スマートアカウントで強力な暗号化が許可されていないが、強力な暗号化の使用が許可されているとシスコが判断した場合、強力な暗号化ライセンスをアカウントに手動で追加できます。

高度暗号化：Firepower 1000、Firepower 2100（アプライアンスモード）、Cisco Secure Firewall 3100/4200

ASA には、管理アクセスのみを対象にした 3DES 機能がデフォルトで含まれているので、Smart Software Manager に接続でき、すぐに ASDM を使用することもできます。後に ASA で SSH アクセスを設定する場合は、SSH および SCP を使用することもできます。高度な暗号化を必要とするその他の機能（VPN など）では、最初に Smart Software Manager に登録する必要がある高度暗号化が有効になっている必要があります。



- (注) 登録する前に高度な暗号化を使用できる機能の設定を試みると（脆弱な暗号化のみ設定している場合でも）、HTTPS 接続はそのインターフェイスでドロップされ、再接続できません。この規則の例外は、管理 1/1 などの管理専用インターフェイスに接続されている場合です。SSH は影響を受けません。HTTPS 接続が失われた場合は、コンソールポートに接続して ASA を再設定するか、管理専用インターフェイスに接続するか、または高度暗号化機能用に設定されていないインターフェイスに接続することができます。

スマートソフトウェアライセンシングアカウントから ASA の登録トークンを要求する場合、[Allow export-controlled functionality on the products registered with this token] チェックボックスをオンにして、高度暗号化 (3DES/AES) のライセンスが適用されるようにします（ご使用のアカウントでその使用が許可されている必要があります）。ASA が後でコンプライアンス違反になった場合、エクスポート コンプライアンス トークンが正常に適用されていれば、ASA は引き続き through the box トラフィックを許可します。ASA を再登録し、エクスポート コンプライアンスが無効になっていても、ライセンスは有効なままです。ASA を工場出荷時の設定に復元すると、ライセンスは削除されます。

最初に高度な暗号化なしで ASA を登録し、後で高度な暗号化を追加する場合は、新しいライセンスを有効にするために ASA をリロードする必要があります。

永続ライセンス予約のライセンスの場合、アカウントに使用資格があれば、高度暗号化 (3DES/AES) ライセンスが有効になります。

スマートアカウントで強力な暗号化が許可されていないが、強力な暗号化の使用が許可されているとシスコが判断した場合、強力な暗号化ライセンスをアカウントに手動で追加できます。



- (注) 1年以上ライセンス登録が期限切れのデバイスをリロードすると、輸出規制対象の機能が無効になります。IPSec 暗号化が有効になっている場合、VPN のダウンタイムやフェールオーバーのスプリットブレインシナリオなどの重大な問題が発生する可能性があります。

高度暗号化：プラットフォームモードの Firepower 2100

Smart Software Manager または Smart Software Manager オンプレミスサーバーに接続する前に、管理接続に高度暗号化（3DES/AES）を使用できるため、ASDM を起動することが可能です。ASDM アクセスは、デフォルトの暗号化を適用する管理専用インターフェイスでのみ使用することに注意してください。高度暗号化ライセンスに接続して取得するまで、（VPN などの）高度暗号化を必要とする through the box トラフィックは許可されません。

スマートソフトウェアライセンシングアカウントから ASA の登録トークンを要求する場合、[Allow export-controlled functionality on the products registered with this token] チェックボックスをオンにして、高度暗号化（3DES/AES）のライセンスが適用されるようにします（ご使用のアカウントでその使用が許可されている必要があります）。ASA が後でコンプライアンス違反になった場合、エクスポート コンプライアンス トークンが正常に適用されていれば、ASA は引き続き through the box トラフィックを許可します。ASA を再登録し、エクスポート コンプライアンスが無効になっていても、ライセンスは有効なままです。ASA を工場出荷時の設定に復元すると、ライセンスは削除されます。

最初に高度な暗号化なしで ASA を登録し、後で高度な暗号化を追加する場合は、新しいライセンスを有効にするために ASA をリロードする必要があります。

永続ライセンス予約のライセンスの場合、アカウントに使用資格があれば、高度暗号化（3DES/AES）ライセンスが有効になります。

スマートアカウントで強力な暗号化が許可されていないが、強力な暗号化の使用が許可されているとシスコが判断した場合、強力な暗号化ライセンスをアカウントに手動で追加できます。

高度暗号化：Firepower 4100/9300 シャーシ

ASA を論理デバイスとして展開すると、すぐに ASDM を起動できます。高度暗号化ライセンスに接続して取得するまで、（VPN などの）高度暗号化を必要とする through the box トラフィックは許可されません。

スマートソフトウェアライセンシングアカウントからシャーシの登録トークンを要求する場合、[このトークンに登録した製品でエクスポート制御機能を許可する（Allow export-controlled functionality on the products registered with this token）] チェックボックスをオンにして、高度暗号化（3DES/AES）ライセンスが適用されるようにします（お使いのアカウントでその使用が許可されている必要があります）。

ASA が後でコンプライアンス違反になった場合、エクスポート コンプライアンス トークンが正常に適用されていれば、ASA は引き続き through the box トラフィックを許可します。シャーシを再登録し、エクスポート コンプライアンスが無効になっている場合、またはシャーシを工場出荷時の設定に復元した場合、ライセンスは削除されます。

最初に高度な暗号化なしでシャーシを登録し、後で高度な暗号化を追加する場合は、新しいライセンスを有効にするために ASA アプリケーションをリロードする必要があります。

永続ライセンス予約のライセンスの場合、アカウントに使用資格があれば、高度暗号化 (3DES/AES) ライセンスが有効になります。

スマートアカウントで強力な暗号化が許可されていないが、強力な暗号化の使用が許可されているとシスコが判断した場合、強力な暗号化ライセンスをアカウントに手動で追加できます。

DES：すべてのモデル

高度暗号化を有効にしている場合、DES を使用することはできません。

キャリア ライセンス

キャリア ライセンスでは、以下のインスペクション機能が有効になります。

- **Diameter** : Diameter は、LTE (Long Term Evolution) および IMS (IP Multimedia Subsystem) 用の EPS (Evolved Packet System) などの次世代モバイルと固定電気通信ネットワークで使用される認証、認可、およびアカウントティング (AAA) プロトコルです。RADIUS や TACACS がこれらのネットワークで Diameter に置き換えられます。
- **GTP/GPRS** : GPRS トンネリングプロトコルは、General Packet Radio Service (GPRS) トラフィック用に GSM、UMTS、および LTE ネットワークで使用されます。GTP は、トンネル制御および管理プロトコルを提供します。このプロトコルによるトンネルの作成、変更、および削除により、モバイルステーションに GPRS ネットワーク アクセスが提供されます。GTP は、ユーザー データ パケットの伝送にもトンネリング メカニズムを使用します。
- **M3UA** : MTP3 User Adaptation (M3UA) は、SS7 Message Transfer Part 3 (MTP3) レイヤと連動する IP ベースアプリケーション用の SS7 ネットワークへのゲートウェイを提供するクライアント/サーバープロトコルです。M3UA により、IP ネットワーク上で SS7 ユーザーパート (ISUP など) を実行することが可能になります。M3UA は RFC 4666 で定義されています。
- **CTP** : SCTP (Stream Control Transmission Protocol) は RFC 4960 で説明されています。プロトコルは IP 経由のテレフォニー シグナリングプロトコル SS7 をサポートしており、4G LTE モバイル ネットワーク アーキテクチャにおける複数のインターフェイス用の転送プロトコルでもあります。

合計 TLS プロキシ セッション

Encrypted Voice Inspection の各 TLS プロキシ セッションは、TLS ライセンスの制限に対してカウントされます。

TLS プロキシ セッションを使用するその他のアプリケーション (ライセンスが不要な Mobility Advantage Proxy など) では、TLS 制限に対してカウントしません。

アプリケーションによっては、1つの接続に複数のセッションを使用する場合があります。たとえば、プライマリとバックアップの Cisco Unified Communications Manager を電話に設定した場合は、TLS プロキシ接続は2つ使用されます。

TLS プロキシの制限は、**tls-proxy maximum-sessions** コマンドまたは ASDM で [Configuration] > [Firewall] > [Unified Communications] > [TLS Proxy] ペインを使用して個別に設定できます。モデルの制限を表示するには、**tls-proxy maximum-sessions ?** コマンドを入力します。デフォルトの TLS プロキシ制限よりも高い TLS プロキシライセンスを適用する場合、ASA では、そのライセンスに一致するように TLS プロキシの制限が自動的に設定されます。ライセンスの制限よりも TLS プロキシ制限が優先されます。TLS プロキシ制限をライセンスよりも少なく設定すると、ライセンスですべてのセッションを使用できません。



(注) 「K8」で終わるライセンス製品番号（たとえばユーザー数が250未満のライセンス）では、TLS プロキシセッション数は1000までに制限されます。「K9」で終わるライセンス製品番号（たとえばユーザー数が250以上のライセンス）では、TLS プロキシの制限はコンフィギュレーションに依存し、モデルの制限が最大数になります。K8とK9は、エクスポートについてそのライセンスが制限されるかどうかを示します。K8は制限されず、K9は制限されます。

（たとえば **clear configure all** コマンドを使用して）コンフィギュレーションをクリアすると、TLS プロキシ制限がモデルのデフォルトに設定されます。このデフォルトがライセンスの制限よりも小さいと、**tls-proxy maximum-sessions** コマンドを使用したときに、再び制限を高めるようにエラーメッセージが表示されます（ASDM の [TLS Proxy] ペインを使用）。フェールオーバーを使用して、**write standby** コマンドを入力するか、または ASDM でプライマリ装置に対して [File] > [Save Running Configuration to Standby Unit] を使用して強制的にコンフィギュレーションの同期を行うと、セカンダリ装置で **clear configure all** コマンドが自動的に生成され、セカンダリ装置に警告メッセージが表示されることがあります。コンフィギュレーションの同期によりプライマリ装置の TLS プロキシ制限の設定が復元されるため、この警告は無視できます。

接続には、SRTP 暗号化セッションを使用する場合もあります。

- K8 ライセンスでは、SRTP セッション数は250までに制限されます。
- K9 ライセンスでは、制限はありません。



(注) メディアの暗号化/復号化を必要とするコールだけが、SRTP 制限に対してカウントされます。コールに対してパススルーが設定されている場合は、両方のレッグが SRTP であっても、SRTP 制限に対してカウントされません。

VLAN、最大

VLAN 制限の対象としてカウントするインターフェイスに、VLAN を割り当てます。次に例を示します。

```
interface gigabitethernet 0/0.100
vlan 100
```

ボットネットトラフィック フィルタ ライセンス

ダイナミック データベースをダウンロードするには、強力な暗号化（3DES/AES）ライセンスが必要です。

フェールオーバーまたは ASA クラスタ ライセンス

ASA のフェールオーバー ライセンス

スタンバイ ユニットにはプライマリ ユニットと同じモデル ライセンスが必要です。

Firepower 1010 のフェールオーバー ライセンス

Smart Software Manager Regular およびオンプレミス

両方の Firepower 1010 ユニットは、Smart Software Manager または Smart Software Manager オンプレミスサーバーに登録する必要があります。フェールオーバーを設定する前に、両方のユニットで Essentials ライセンスと Security Plus ライセンスを有効にする必要があります。

通常は、ユニットの登録時に両方のユニットが強力な暗号化トークンを取得する必要があるため、ASA で強力な暗号化（3DES/AES）機能ライセンスを有効にする必要もありません。登録トークンを使用する場合、両方のユニットに同じ暗号化レベルが設定されている必要があります。

スマートアカウントで強力な暗号化が許可されていないが、強力な暗号化の使用が許可されているとシスコが判断した場合、強力な暗号化ライセンスをアカウントに手動で追加できます。この場合、フェールオーバーを有効にした後、アクティブユニットで有効にします。設定はスタンバイ ユニットに複製されますが、スタンバイ ユニットは設定を使用しません。この設定はキャッシュの状態のままになります。アクティブユニットのみサーバーからライセンスを要求します。ライセンスは単一のフェールオーバーライセンスにまとめられ、フェールオーバーのペアで共有されます。この集約ライセンスはスタンバイユニットにもキャッシュされ、将来アクティブなユニットとなったときに使用されます。フェールオーバーの後には、新しいアクティブ装置は集約ライセンスを引き続き使用します。キャッシュされたライセンス設定を使用し、サーバーに権限付与を再要求します。古いアクティブ装置がペアにスタンバイとして参加した場合、ライセンス権限を解放します。アカウントに十分なライセンスがない場合、スタンバイ装置が権限を解放する前に、新しいアクティブ装置のライセンスがコンプライアンス違反状態になることがあります。フェールオーバーのペアは集約ライセンスを 30 日間使用できますが、この猶予期間以降もコンプライアンス違反となり、高度暗号化トークンを使用する場合は、高度暗号化（3DES/AES）機能ライセンスを必要とする機能の設定変更を行えなくなります。動作には影響しません。新しいアクティブ装置は、ライセンスのコンプライアンスが確保されるまで 35 秒ごとに権限承認更新要求を送信します。フェールオーバーのペアを解消した場合は、アクティブな装置は権限を解放し、両方のユニットはライセンス設定をキャッシュ状

態にして保持します。ライセンスを再アクティベートするには、各ユニットの設定をクリアし、再設定する必要があります。

永続ライセンスの予約

永続ライセンスを予約するには、シャードごとに個別のライセンスを購入し、フェールオーバーを設定する前にライセンスを有効にする必要があります。

Firepower 1100 のフェールオーバー ライセンス

Smart Software Manager Regular およびオンプレミス

アクティブユニットのみサーバからライセンスを要求します。ライセンスは、フェールオーバーペアで共有される単一のフェールオーバーライセンスに集約されます。セカンダリユニットに追加費用はかかりません。

アクティブ/スタンバイフェールオーバーのフェールオーバーを有効にした後は、アクティブユニットにのみスマートライセンスを設定できます。アクティブ/アクティブフェールオーバーでは、フェールオーバーグループ1がアクティブになっている装置にのみスマートライセンスを設定できます。設定はスタンバイユニットに複製されますが、スタンバイユニットは設定を使用しません。この設定はキャッシュの状態のままになります。集約されたライセンスは、スタンバイユニットにキャッシュされ、将来アクティブユニットになる場合に使用されます。



(注) フェールオーバーペアを形成する場合は、各ASAに同じ暗号化ライセンスが必要です。スマートライセンスサーバにASAを登録すると、高度暗号化ライセンスは、登録トークンを適用するときに、対象となるお客様の場合に自動的に有効化されます。この要件のため、フェールオーバーで高度暗号化トークンを使用する場合は、次の2つのライセンスを選択できます。

- フェールオーバーを有効にする前に、両方のユニットをスマートライセンスサーバに登録します。この場合、両方のユニットに高度暗号化が適用されます。次に、フェールオーバーを有効にした後、アクティブユニットでライセンス権限の設定を続行します。フェールオーバーリンクの暗号化を有効にすると、AES/3DES（高度暗号化）が使用されます。
- アクティブユニットをスマートライセンスサーバに登録する前に、フェールオーバーを有効にします。この場合、両方のユニットに高度暗号化はまだ適用されません。次に、ライセンス権限を設定し、アクティブユニットをスマートライセンスサーバに登録します。両方のユニットが集約ライセンスから高度暗号化を取得します。フェールオーバーリンクで暗号化を有効にした場合、ユニットが高度暗号化を取得する前にフェールオーバーリンクが確立されているため、DES（脆弱な暗号化）が使用されます。リンクでAES/3DESを使用するには、両方のユニットをリロードする必要があります。1つのユニットだけをリロードすると、そのユニットはAES/3DESを使用しようとしていますが、元のユニットはDESを使用するため、両方のユニットがアクティブになります（スプリットブレイン）。

各アドオンライセンスタイプは次のように管理されます。

- **Essentials**：アクティブな装置のみがサーバにこのライセンスを要求しますが、スタンバイ装置にはデフォルトで有効になっている **Essentials** ライセンスがあります。その使用のためにサーバに登録を行う必要はありません。
- **Context**：このライセンスはアクティブな装置のみが要求します。ただし、デフォルトで **Essentials** ライセンスには2のコンテキストが含まれ、これは両方のユニットにあります。各ユニットの **Essentials** ライセンスの値と、アクティブな装置の **Context** ライセンスの値はプラットフォームの上限まで加算されます。次に例を示します。
 - **アクティブ/スタンバイ**：**Essentials** ライセンスには2つのコンテキストが含まれています。2つの **Firepower 1120** ユニットの場合、これらのライセンスは最大4つのコンテキストを追加します。アクティブ/スタンバイペアのアクティブな装置に3 **Context** ライセンスを設定します。この場合、集約されたフェールオーバーライセンスには7つのコンテキストが含まれています。ただし、ユニットごとのプラットフォームの制限が5なので、結合されたライセンスでは最大5つのコンテキストのみ許可されます。この場合、アクティブな **Context** ライセンスを1つのコンテキストとしてのみ設定することになる場合があります。
 - **アクティブ/アクティブ**：**Essentials** ライセンスには2つのコンテキストが含まれています。2つの **Firepower 1140** ユニットの場合、これらのライセンスは最大4つのコンテキストを追加します。アクティブ/アクティブペアのプライマリユニットに4 **Context** ライセンスを設定します。この場合、集約されたフェールオーバーライセンスには8つのコンテキストが含まれています。たとえば、一方のユニットが5コンテキストを使用し、他方が3コンテキストを使用しますが、障害発生時には1ユニットが8コンテキストすべてを使用します。ユニットごとのプラットフォームの制限が10なので、結合されたライセンスでは最大10のコンテキストが許可されます。8コンテキストは制限の範囲内です。
- **高度な暗号化（3DES/AES）**：スマートアカウントで高度な暗号化が許可されていないが、高度な暗号化の使用が許可されているとシスコが判断した場合、高度な暗号化ライセンスをアカウントに手動で追加できます。アクティブユニットのみがこのライセンスを要求し、ライセンスの集約により両方のユニットがこれを使用できます。

フェールオーバーの後には、新しいアクティブ装置は集約ライセンスを引き続き使用します。キャッシュされたライセンス設定を使用し、サーバーに権限付与を再要求します。古いアクティブ装置がペアにスタンバイとして参加した場合、ライセンス権限を解放します。アカウントに十分なライセンスがない場合、スタンバイ装置が権限を解放する前に、新しいアクティブ装置のライセンスがコンプライアンス違反状態になることがあります。フェールオーバーのペアは集約ライセンスを30日間使用できますが、この猶予期間以降もコンプライアンス違反となる場合は、特殊なライセンスを必要とする機能の設定変更（つまり、追加コンテキストの追加）を行えなくなります。動作には影響しません。新しいアクティブ装置は、ライセンスのコンプライアンスが確保されるまで35秒ごとに権限承認更新要求を送信します。フェールオーバーのペアを解消した場合は、アクティブな装置は権限を解放し、両方のユニットはライセンス設定をキャッシュ状態にして保持します。ライセンスを再アクティベートするには、各ユニットの設定をクリアし、再設定する必要があります。

永続ライセンスの予約

永続ライセンスを予約するには、シャードごとに個別のライセンスを購入し、フェールオーバーを設定する前にライセンスを有効にする必要があります。

Firepower 2100 のフェールオーバー ライセンス

Smart Software Manager Regular およびオンプレミス

アクティブユニットのみサーバからライセンスを要求します。ライセンスは、フェールオーバーペアで共有される単一のフェールオーバーライセンスに集約されます。セカンダリユニットに追加費用はかかりません。

アクティブ/スタンバイフェールオーバーのフェールオーバーを有効にした後は、アクティブユニットにのみスマートライセンスを設定できます。アクティブ/アクティブフェールオーバーでは、フェールオーバーグループ1がアクティブになっている装置にのみスマートライセンスを設定できます。設定はスタンバイユニットに複製されますが、スタンバイユニットは設定を使用しません。この設定はキャッシュの状態のままになります。集約されたライセンスは、スタンバイユニットにキャッシュされ、将来アクティブユニットになる場合に使用されます。



(注) フェールオーバーペアを形成する場合は、各ASAに同じ暗号化ライセンスが必要です。スマートライセンスサーバにASAを登録すると、高度暗号化ライセンスは、登録トークンを適用するときに、対象となるお客様の場合に自動的に有効化されます。この要件のため、フェールオーバーで高度暗号化トークンを使用する場合は、次の2つのライセンスを選択できます。

- フェールオーバーを有効にする前に、両方のユニットをスマートライセンスサーバに登録します。この場合、両方のユニットに高度暗号化が適用されます。次に、フェールオーバーを有効にした後、アクティブユニットでライセンス権限の設定を続行します。フェールオーバーリンクの暗号化を有効にすると、AES/3DES（高度暗号化）が使用されます。
- アクティブユニットをスマートライセンスサーバに登録する前に、フェールオーバーを有効にします。この場合、両方のユニットに高度暗号化はまだ適用されません。次に、ライセンス権限を設定し、アクティブユニットをスマートライセンスサーバに登録します。両方のユニットが集約ライセンスから高度暗号化を取得します。フェールオーバーリンクで暗号化を有効にした場合、ユニットが高度暗号化を取得する前にフェールオーバーリンクが確立されているため、DES（脆弱な暗号化）が使用されます。リンクでAES/3DESを使用するには、両方のユニットをリロードする必要があります。1つのユニットだけをリロードすると、そのユニットはAES/3DESを使用しようとしていますが、元のユニットはDESを使用するため、両方のユニットがアクティブになります（スプリットブレイン）。

各アドオンライセンスタイプは次のように管理されます。

- **Essentials**：アクティブな装置のみがサーバにこのライセンスを要求しますが、スタンバイ装置にはデフォルトで有効になっている **Essentials** ライセンスがあります。その使用のためにサーバに登録を行う必要はありません。

- **Context**：このライセンスはアクティブな装置のみが要求します。ただし、デフォルトで Essentials ライセンスには2のコンテキストが含まれ、これは両方のユニットにあります。各ユニットの Essentials ライセンスの値と、アクティブな装置の Context ライセンスの値はプラットフォームの上限まで加算されます。次に例を示します。
 - **アクティブ/スタンバイ**：Essentials ライセンスには2つのコンテキストが含まれています。2つの Firepower 2130 ユニットの case、これらのライセンスは最大4つのコンテキストを追加します。アクティブ/スタンバイペアのアクティブな装置に30 Context ライセンスを設定します。この場合、集約されたフェールオーバーライセンスには34のコンテキストが含まれています。しかし、ユニットごとのプラットフォームの制限が30であるため、結合されたライセンスでは最大30のコンテキストが許容されます。この場合では、アクティブな Context ライセンスとして25のコンテキストのみを設定できます。
 - **アクティブ/アクティブ**：Essentials ライセンスには2つのコンテキストが含まれています。2つの Firepower 2130 ユニットの case、これらのライセンスは最大4つのコンテキストを追加します。アクティブ/アクティブペアのプライマリユニットに10 Context ライセンスを設定します。この場合、集約されたフェールオーバーライセンスには14のコンテキストが含まれています。たとえば、一方のユニットが9コンテキストを使用し、他方が5コンテキストを使用しますが、障害発生時には1つのユニットが14コンテキストすべてを使用します。ユニットごとのプラットフォームの制限が30であるため、結合されたライセンスでは最大30のコンテキストが許容されます。14コンテキストは制限の範囲内です。
- **高度な暗号化 (3DES/AES)**：スマートアカウントで高度な暗号化が許可されていないが、高度な暗号化の使用が許可されているとシスコが判断した場合、高度な暗号化ライセンスをアカウントに手動で追加できます。アクティブユニットのみがこのライセンスを要求し、ライセンスの集約により両方のユニットがこれを使用できます。

フェールオーバーの後には、新しいアクティブ装置は集約ライセンスを引き続き使用します。キャッシュされたライセンス設定を使用し、サーバーに権限付与を再要求します。古いアクティブ装置がペアにスタンバイとして参加した場合、ライセンス権限を解放します。アカウントに十分なライセンスがない場合、スタンバイ装置が権限を解放する前に、新しいアクティブ装置のライセンスがコンプライアンス違反状態になることがあります。フェールオーバーのペアは集約ライセンスを30日間使用できますが、この猶予期間以降もコンプライアンス違反となる場合は、特殊なライセンスを必要とする機能の設定変更（つまり、追加コンテキストの追加）を行えなくなります。動作には影響しません。新しいアクティブ装置は、ライセンスのコンプライアンスが確保されるまで35秒ごとに権限承認更新要求を送信します。フェールオーバーのペアを解消した場合は、アクティブな装置は権限を解放し、両方のユニットはライセンス設定をキャッシュ状態にして保持します。ライセンスを再アクティベートするには、各ユニットの設定をクリアし、再設定する必要があります。

永続ライセンスの予約

永続ライセンスを予約するには、シャードごとに個別のライセンスを購入し、フェールオーバーを設定する前にライセンスを有効にする必要があります。

Secure Firewall 3100 のフェールオーバーライセンス

Smart Software Manager Regular およびオンプレミス

各ユニットには、Essentialsライセンス（デフォルトで有効）と同じ暗号化ライセンスが必要です。ライセンス不一致の問題を回避するために、フェールオーバーを有効にする前に、ライセンスサーバで各ユニットのライセンスを取得することをお勧めします。また、高度暗号化ライセンスを使用する場合は、フェールオーバーリンクの暗号化に関する問題も発生します。

フェールオーバー機能自体にライセンスは必要ありません。データユニットのコンテキストライセンスに追加料金はかかりません。

高度暗号化ライセンスは、登録トークンを適用すると、対象となるお客様の場合自動的に有効化されます。ASA 設定で有効化される高度暗号化（3DES/AES）機能ライセンスについては、以下を参照してください。

Cisco ASA ライセンス構成では、Essentials ライセンスは両方のユニットで常にデフォルトで有効になっています。アクティブ/スタンバイフェールオーバーのフェールオーバーを有効にした後は、アクティブユニットにのみスマートライセンシングを設定できます。アクティブ/アクティブ フェールオーバーでは、フェールオーバー グループ 1 がアクティブになっている装置にのみスマートライセンシングを設定できます。設定はスタンバイユニットに複製されますが、スタンバイユニットは設定を使用しません。この設定はキャッシュの状態のままになります。集約されたライセンスは、スタンバイユニットにキャッシュされ、将来アクティブユニットになる場合に使用されます。

各アドオンライセンスタイプは次のように管理されます。

- **Essentials**：各ユニットには、サーバーからのEssentialsのライセンスが必要です。
- **Context**：このライセンスはアクティブな装置のみが要求します。ただし、デフォルトでEssentials ライセンスには2のコンテキストが含まれ、これは両方のユニットにあります。各ユニットのEssentials ライセンスの値と、アクティブな装置のContext ライセンスの値はプラットフォームの上限まで加算されます。次に例を示します。
 - **アクティブ/スタンバイ**：Essentialsライセンスには2つのコンテキストが含まれています。2つのCisco Secure Firewall 3130 ユニットの場合、それらのライセンスで最大4つのコンテキストが追加されます。アクティブ/スタンバイペアのアクティブな装置に100 Context ライセンスを設定します。この場合、集約されたフェールオーバーライセンスには104のコンテキストが含まれています。ただし、ユニットごとのプラットフォームの制限が100であるため、結合されたライセンスでは最大100のコンテキストのみが許容されます。この場合では、アクティブなContext ライセンスとして95のコンテキストのみを設定できます。
 - **アクティブ/スタンバイ**：Essentials ライセンスには2つのコンテキストが含まれています。2つのCisco Secure Firewall 3130 ユニットの場合、これらのライセンスは最大4つのコンテキストを追加します。アクティブ/アクティブペアのプライマリユニットに10 Context ライセンスを設定します。この場合、集約されたフェールオーバーライセンスには14のコンテキストが含まれています。たとえば、一方のユニットが9コンテキストを使用し、他方が5コンテキストを使用しますが、障害発生時には1つのユニットが14コンテキストすべてを使用します。ユニットごとのプラットフォーム

の制限が 100 であるため、結合されたライセンスでは最大 100 のコンテキストが許容されます。14 コンテキストは制限の範囲内です。

- 高度な暗号化（3DES/AES）：スマートアカウントで高度な暗号化が許可されていないが、高度な暗号化の使用が許可されているとシスコが判断した場合、高度な暗号化ライセンスをアカウントに手動で追加できます。アクティブユニットのみがこのライセンスを要求し、ライセンスの集約により両方のユニットがこれを使用できます。

フェールオーバーの後には、新しいアクティブ装置は集約ライセンスを引き続き使用します。キャッシュされたライセンス設定を使用し、サーバーに権限付与を再要求します。古いアクティブ装置がペアにスタンバイとして参加した場合、ライセンス権限を解放します。アカウントに十分なライセンスがない場合、スタンバイ装置が権限を解放する前に、新しいアクティブ装置のライセンスがコンプライアンス違反状態になることがあります。フェールオーバーのペアは集約ライセンスを 30 日間使用できますが、この猶予期間以降もコンプライアンス違反となる場合は、特殊なライセンスを必要とする機能の設定変更（つまり、追加コンテキストの追加）を行えなくなります。動作には影響しません。新しいアクティブ装置は、ライセンスのコンプライアンスが確保されるまで 35 秒ごとに権限承認更新要求を送信します。フェールオーバーのペアを解消した場合は、アクティブな装置は権限を解放し、両方のユニットはライセンス設定をキャッシュ状態にして保持します。ライセンスを再アクティベートするには、各ユニットの設定をクリアし、再設定する必要があります。

永続ライセンスの予約

永続ライセンスを予約するには、シャージごとに個別のライセンスを購入し、フェールオーバーを設定する前にライセンスを有効にする必要があります。

Secure Firewall 4200 のフェールオーバーライセンス

Smart Software Manager Regular およびオンプレミス

各ユニットには、Essentialsライセンス（デフォルトで有効）と同じ暗号化ライセンスが必要です。ライセンス不一致の問題を回避するために、フェールオーバーを有効にする前に、ライセンスサーバで各ユニットのライセンスを取得することをお勧めします。また、高度暗号化ライセンスを使用する場合は、フェールオーバーリンクの暗号化に関する問題も発生します。

フェールオーバー機能自体にライセンスは必要ありません。データユニットのコンテキストライセンスに追加料金はかかりません。

高度暗号化ライセンスは、登録トークンを適用すると、対象となるお客様の場合自動的に有効化されます。ASA 設定で有効化される高度暗号化（3DES/AES）機能ライセンスについては、以下を参照してください。

Cisco ASA ライセンス構成では、Essentials ライセンスは両方のユニットで常にデフォルトで有効になっています。アクティブ/スタンバイフェールオーバーのフェールオーバーを有効にした後は、アクティブユニットにのみスマートライセンスを設定できます。アクティブ/アクティブフェールオーバーでは、フェールオーバーグループ 1 がアクティブになっている装置にのみスマートライセンスを設定できます。設定はスタンバイユニットに複製されますが、スタンバイユニットは設定を使用しません。この設定はキャッシュの状態のままになります。

す。集約されたライセンスは、スタンバイユニットにキャッシュされ、将来アクティブユニットになる場合に使用されます。

各アドオンライセンスタイプは次のように管理されます。

- **Essentials**：各ユニットがサーバーから標準Essentials準ライセンスを要求します。
- **Context**：このライセンスはアクティブな装置のみが要求します。ただし、デフォルトでEssentials ライセンスには2のコンテキストが含まれ、これは両方のユニットにあります。各ユニットのEssentials ライセンスの値と、アクティブな装置のContext ライセンスの値はプラットフォームの上限まで加算されます。次に例を示します。
 - **アクティブ/スタンバイ**：Essentials ライセンスには10のコンテキストが含まれています。Cisco Secure Firewall 4215 を2台使用する場合、これらのライセンスを合計すると20のコンテキストになります。アクティブ/スタンバイペアのアクティブな装置に250 Context ライセンスを設定します。この場合、集約されたフェールオーバーライセンスには270のコンテキストが含まれています。しかし、ユニットごとのプラットフォームの制限が250であるため、結合されたライセンスでは最大250のコンテキストが許容されます。この場合では、アクティブなContext ライセンスとして230のコンテキストのみを設定できます。
 - **アクティブ/アクティブ**：Essentials ライセンスには10のコンテキストが含まれています。Cisco Secure Firewall 4215 を2台使用する場合、これらのライセンスを合計すると10のコンテキストになります。アクティブ/アクティブペアのプライマリユニットに10 Context ライセンスを設定します。この場合、集約されたフェールオーバーライセンスには30のコンテキストが含まれています。たとえば、一方のユニットが15コンテキストを使用し、他方が15コンテキストを使用しますが、障害発生時には1ユニットが30コンテキストすべてを使用します。ユニットごとのプラットフォームの制限が250であるため、結合されたライセンスでは最大250のコンテキストが許容されます。30コンテキストは制限の範囲内です。
- **高度な暗号化（3DES/AES）**：スマートアカウントで高度な暗号化が許可されていないが、高度な暗号化の使用が許可されているとシスコが判断した場合、高度な暗号化ライセンスをアカウントに手動で追加できます。アクティブユニットのみがこのライセンスを要求し、ライセンスの集約により両方のユニットがこれを使用できます。

フェールオーバーの後には、新しいアクティブ装置は集約ライセンスを引き続き使用します。キャッシュされたライセンス設定を使用し、サーバーに権限付与を再要求します。古いアクティブ装置がペアにスタンバイとして参加した場合、ライセンス権限を解放します。アカウントに十分なライセンスがない場合、スタンバイ装置が権限を解放する前に、新しいアクティブ装置のライセンスがコンプライアンス違反状態になることがあります。フェールオーバーのペアは集約ライセンスを30日間使用できますが、この猶予期間以降もコンプライアンス違反となる場合は、特殊なライセンスを必要とする機能の設定変更（つまり、追加コンテキストの追加）を行なえなくなります。動作には影響しません。新しいアクティブ装置は、ライセンスのコンプライアンスが確保されるまで35秒ごとに権限承認更新要求を送信します。フェールオーバーのペアを解消した場合は、アクティブな装置は権限を解放し、両方のユニットはライセンス設定をキャッシュ状態にして保持します。ライセンスを再アクティベートするには、各ユニットの設定をクリアし、再設定する必要があります。

永続ライセンスの予約

永続ライセンスを予約するには、シャーンシごとに個別のライセンスを購入し、フェールオーバーを設定する前にライセンスを有効にする必要があります。

Firepower 4100/9300のフェールオーバーライセンス

Smart Software Manager Regular およびオンプレミス

フェールオーバーを設定する前に、両方の Firepower 4100/9300 は、Smart Software Manager または Smart Software Manager オンプレミスサーバーに登録する必要があります。セカンダリ ユニットに追加費用はかかりません。

高度暗号化ライセンスは、登録トークンを適用すると、対象となるお客様の場合自動的に有効化されます。トークンを使用している場合、各シャーンシに同じ暗号化ライセンスが必要です。ASA 設定で有効化される高度暗号化（3DES/AES）機能ライセンスについては、以下を参照してください。

アクティブ/スタンバイフェールオーバーの ASA ライセンス設定のフェールオーバーを有効にした後は、アクティブユニットにのみスマートライセンスを設定できます。アクティブ/アクティブ フェールオーバーでは、フェールオーバー グループ 1 がアクティブになっている装置にのみスマートライセンスを設定できます。設定はスタンバイユニットに複製されますが、スタンバイユニットは設定を使用しません。この設定はキャッシュの状態のままになります。アクティブな装置のみサーバーからライセンスを要求します。ライセンスは単一のフェールオーバーライセンスにまとめられ、フェールオーバーのペアで共有されます。この集約ライセンスはスタンバイユニットにもキャッシュされ、将来アクティブなユニットとなったときに使用されます。各ライセンス タイプは次のように処理されます：

- **Essentials**：アクティブな装置のみがサーバにこのライセンスを要求しますが、スタンバイ装置にはデフォルトで有効になっている Essentials ライセンスがあります。その使用のためにサーバに登録を行う必要はありません。
- **Context**：このライセンスはアクティブな装置のみが要求します。ただし、デフォルトで Essentials ライセンスには 10 のコンテキストが含まれ、これは両方のユニットにあります。各ユニットの Essentials ライセンスの値と、アクティブな装置の Context ライセンスの値はプラットフォームの上限まで加算されます。次に例を示します。
 - **アクティブ/スタンバイ**：Essentials ライセンスは 10 のコンテキストを含みます。2 ユニットの場合、合計で 20 のコンテキストが加算されます。アクティブ/スタンバイペアのアクティブな装置に 250 Context ライセンスを設定します。この場合、集約されたフェールオーバーライセンスには 270 のコンテキストが含まれています。しかし、ユニットごとのプラットフォームの制限が 250 であるため、結合されたライセンスでは最大 250 のコンテキストが許容されます。この場合では、アクティブな Context ライセンスとして 230 コンテキストを設定する必要があります。
 - **アクティブ/アクティブ**：Essentials ライセンスは 10 のコンテキストを含みます。2 ユニットの場合、合計で 20 のコンテキストが加算されます。アクティブ/アクティブペアのプライマリユニットに 10 Context ライセンスを設定します。この場合、集約されたフェールオーバーライセンスには 30 のコンテキストが含まれています。たとえば、一方のユニットが 17 コンテキストを使用し、他方が 13 コンテキストを使用します。

が、障害発生時には1ユニットが30コンテキストすべてを使用します。ユニットごとのプラットフォームの制限が250であるため、結合されたライセンスでは最大250のコンテキストが許容されます。30コンテキストは制限の範囲内です。

- キャリア：アクティブのみがこのライセンスを要求し、ライセンスの集約により両方のユニットがこれを使用できます。
- 高度な暗号化（3DES）：スマートアカウントで高度な暗号化が許可されていないが、高度な暗号化の使用が許可されているとシスコが判断した場合、高度な暗号化ライセンスをアカウントに手動で追加できます。アクティブユニットのみがこのライセンスを要求し、ライセンスの集約により両方のユニットがこれを使用できます。

フェールオーバーの後には、新しいアクティブ装置は集約ライセンスを引き続き使用します。キャッシュされたライセンス設定を使用し、サーバーに権限付与を再要求します。古いアクティブ装置がペアにスタンバイとして参加した場合、ライセンス権限を解放します。アカウントに十分なライセンスがない場合、スタンバイ装置が権限を解放する前に、新しいアクティブ装置のライセンスがコンプライアンス違反状態になることがあります。フェールオーバーのペアは集約ライセンスを30日間使用できますが、この猶予期間以降もコンプライアンス違反となる場合は、特殊なライセンスを必要とする機能の設定変更を行えなくなります。動作には影響しません。新しいアクティブ装置は、ライセンスのコンプライアンスが確保されるまで35秒ごとに権限承認更新要求を送信します。フェールオーバーのペアを解消した場合は、アクティブな装置は権限を解放し、両方のユニットはライセンス設定をキャッシュ状態にして保持します。ライセンスを再アクティベートするには、各ユニットの設定をクリアし、再設定する必要があります。

永続ライセンスの予約

永続ライセンスを予約するには、シャーシごとに個別のライセンスを購入し、フェールオーバーを設定する前にライセンスを有効にする必要があります。

Secure Firewall 3100 の ASA クラスタライセンス

Smart Software Manager Regular およびオンプレミス

各ユニットには、Essentialsライセンス（デフォルトで有効）と同じ暗号化ライセンスが必要です。ライセンス不一致の問題を回避するために、クラスタリングを有効にする前に、ライセンスサーバで各ユニットのライセンスを取得することをお勧めします。また、高度暗号化ライセンスを使用する場合は、クラスタ制御リンクの暗号化に関する問題も発生します。

クラスタリング機能自体にライセンスは必要ありません。データユニットのコンテキストライセンスに追加料金はかかりません。

高度暗号化ライセンスは、登録トークンを適用すると、対象となるお客様の場合自動的に有効化されます。ASA設定で有効化される高度暗号化（3DES/AES）機能ライセンスについては、以下を参照してください。

ASAライセンス設定では、Essentialsライセンスはすべてのユニットで常にデフォルトで有効になっています。制御ユニットにのみスマートライセンスを設定できます。設定はデータユニットに複製されますが、一部のライセンスに対しては、データユニットはこの設定を使用しませ

ん。この設定はキャッシュ状態のままになり、制御ユニットのみがこのライセンスを要求します。ライセンスは単一のクラスライセンスにまとめられ、クラスタの各ユニットで共有されます。この集約ライセンスはデータユニットにもキャッシュされ、その中の1つが将来制御ユニットとなったときに使用されます。各ライセンスタイプは次のように処理されます：

- **Essentials**：各ユニットには、サーバーからのEssentialsのライセンスが必要です。
- **コンテキスト**：制御ユニットのみがサーバーからコンテキストライセンスを要求します。デフォルトでEssentialsライセンスは2のコンテキストを含み、すべてのクラスタメンバー上に存在します。各ユニットのEssentialsライセンスの値と、制御ユニットのコンテキストライセンスの値は、集約されたクラスライセンスでのプラットフォーム制限まで統合されます。次に例を示します。
 - クラスタ内に6つのSecure Firewall 3100があります。Essentialsライセンスは2のコンテキストを含みます。6ユニットの場合、合計で12のコンテキストが加算されます。制御ユニット上で追加の20コンテキストライセンスを設定します。したがって、集約されたクラスライセンスは32のコンテキストを含みます。シャーシごとのプラットフォームの制限が100であるため、結合されたライセンスでは最大100のコンテキストが許容されます。32コンテキストは制限の範囲内です。したがって、制御ユニット上で最大32コンテキストを設定できます。各データユニットも、コンフィギュレーションの複製を介して32コンテキストを持つことになります。
 - クラスタ内に3つのCisco Secure Firewall 3100があります。Essentialsライセンスは2のコンテキストを含みます。3ユニットの場合、合計で6のコンテキストが加算されます。制御ユニット上で追加の100コンテキストライセンスを設定します。したがって、集約されたクラスライセンスは106のコンテキストを含みます。ユニットごとのプラットフォームの制限が100であるため、統合されたライセンスでは最大100のコンテキストが許容されます。106コンテキストは制限を超えています。したがって、制御ユニット上で最大100のコンテキストのみを設定できます。各データユニットも、設定の複製を介して100のコンテキストを持つことになります。この場合では、制御ユニットのコンテキストライセンスとして94のコンテキストのみを設定する必要があります。
- **高度な暗号化（3DES）**：スマートアカウントで高度な暗号化が許可されていないが、高度な暗号化の使用が許可されているとシスコが判断した場合、高度な暗号化ライセンスをアカウントに手動で追加できます。制御ユニットのみがこのライセンスを要求し、ライセンスの集約により、すべてのユニットがそれを使用できます。

新しい制御ユニットが選定されると、このユニットが集約ライセンスを引き続き使用します。また、制御ユニットのライセンスを再要求するために、キャッシュされたライセンス設定も使用します。古い制御ユニットがデータユニットとしてクラスタに再度参加すると、制御ユニットのライセンス権限付与が解放されます。アカウントに利用可能なライセンスがない場合、データユニットがライセンスを解放する前に、制御ユニットのライセンスがコンプライアンス違反状態になることがあります。保持されたライセンスは30日間有効ですが、この猶予期間以降もコンプライアンス違反となる場合、特別なライセンスを必要とする機能の設定変更を行なえません。ただし、動作には影響ありません。新しいアクティブ装置は、ライセンスのコンプライアンスが確保されるまで35秒ごとに権限承認更新要求を送信します。ライセンス要求

が完全に処理されるまで、設定の変更を控えてください。ユニットがクラスタから離れた場合、キャッシュされた制御ユニットの設定は削除されます。一方で、ユニットごとの権限は保持されます。この場合、クラスタ外のユニットのコンテキストライセンスを再要求する必要があります。

永続ライセンスの予約

永続ライセンスを予約するには、シャーシごとに個別のライセンスを購入し、クラスタリングを設定する前にライセンスを有効にする必要があります。

Secure Firewall 4200 の ASA クラスタライセンス

Smart Software Manager Regular およびオンプレミス

各ユニットには、Essentialsライセンス（デフォルトで有効）と同じ暗号化ライセンスが必要です。ライセンス不一致の問題を回避するために、クラスタリングを有効にする前に、ライセンスサーバで各ユニットのライセンスを取得することをお勧めします。また、高度暗号化ライセンスを使用する場合は、クラスタ制御リンクの暗号化に関する問題も発生します。

クラスタリング機能自体にライセンスは必要ありません。データユニットのコンテキストライセンスに追加料金はかかりません。

高度暗号化ライセンスは、登録トークンを適用すると、対象となるお客様の場合自動的に有効化されます。ASA 設定で有効化される高度暗号化（3DES/AES）機能ライセンスについては、以下を参照してください。

ASA ライセンス設定では、Essentialsライセンスはすべてのユニットで常にデフォルトで有効になっています。制御ユニットにのみスマートライセンスを設定できます。設定はデータユニットに複製されますが、一部のライセンスに対しては、データユニットはこの設定を使用しません。この設定はキャッシュ状態のままになり、制御ユニットのみがこのライセンスを要求します。ライセンスは単一のクラスタライセンスにまとめられ、クラスタの各ユニットで共有されます。この集約ライセンスはデータユニットにもキャッシュされ、その中の1つが将来制御ユニットとなったときに使用されます。各ライセンスタイプは次のように処理されます：

- **Essentials**：各ユニットには、サーバーからのEssentialsのライセンスが必要です。
- **コンテキスト**：制御ユニットのみがサーバーからコンテキストライセンスを要求します。デフォルトでEssentialsライセンスは2のコンテキストを含み、すべてのクラスタメンバー上に存在します。各ユニットのEssentialsライセンスの値と、制御ユニットのコンテキストライセンスの値は、集約されたクラスタライセンスでのプラットフォーム制限まで統合されます。次に例を示します。
 - クラスタ内に6つのCisco Secure Firewall 4200があります。Essentialsライセンスは2のコンテキストを含みます。6ユニットの場合、合計で12のコンテキストが加算されます。制御ユニット上で追加の20コンテキストライセンスを設定します。したがって、集約されたクラスタライセンスは32のコンテキストを含みます。シャーシごとのプラットフォームの制限が250であるため、結合されたライセンスでは最大250のコンテキストが許容されます。32コンテキストは制限の範囲内です。したがって、制御ユニット上で最大32コンテキストを設定できます。各データユニットも、コンフィギュレーションの複製を介して32コンテキストを持つことになります。

- クラスタ内に 3 つの Cisco Secure Firewall 4200 があります。Essentials ライセンスは 2 のコンテキストを含みます。3 ユニットの場合、合計で 6 のコンテキストが加算されます。制御ユニット上で追加の 250 コンテキストライセンスを設定します。したがって、集約されたクラスタライセンスは 256 のコンテキストを含みます。ユニットごとのプラットフォームの制限が 250 であるため、統合されたライセンスでは最大 250 のコンテキストが許容されます。256 コンテキストは制限を超えています。したがって、制御ユニット上で最大 250 のコンテキストのみを設定できます。各データユニットも、コンフィギュレーションの複製を介して 250 のコンテキストを持つことになります。この場合では、制御ユニットのコンテキストライセンスとして 244 のコンテキストのみを設定する必要があります。
- 高度な暗号化（3DES）：スマートアカウントで高度な暗号化が許可されていないが、高度な暗号化の使用が許可されているとシスコが判断した場合、高度な暗号化ライセンスをアカウントに手動で追加できます。制御ユニットのみがこのライセンスを要求し、ライセンスの集約により、すべてのユニットがそれを使用できます。

新しい制御ユニットが選定されると、このユニットが集約ライセンスを引き続き使用します。また、制御ユニットのライセンスを再要求するために、キャッシュされたライセンス設定も使用します。古い制御ユニットがデータユニットとしてクラスタに再度参加すると、制御ユニットのライセンス権限付与が解放されます。アカウントに利用可能なライセンスがない場合、データユニットがライセンスを解放する前に、制御ユニットのライセンスがコンプライアンス違反状態になることがあります。保持されたライセンスは 30 日間有効ですが、この猶予期間以降もコンプライアンス違反となる場合、特別なライセンスを必要とする機能の設定変更を行なえません。ただし、動作には影響ありません。新しいアクティブ装置は、ライセンスのコンプライアンスが確保されるまで 35 秒ごとに権限承認更新要求を送信します。ライセンス要求が完全に処理されるまで、設定の変更を控えてください。ユニットがクラスタから離れた場合、キャッシュされた制御ユニットの設定は削除されます。一方で、ユニットごとの権限は保持されます。この場合、クラスタ外のユニットのコンテキストライセンスを再要求する必要があります。

永続ライセンスの予約

永続ライセンスを予約するには、シャードごとに個別のライセンスを購入し、クラスタリングを設定する前にライセンスを有効にする必要があります。

ASAv の ASA クラスタライセンス

Smart Software Manager Regular およびオンプレミス

各ユニットには、同じスループットライセンスと同じ暗号化ライセンスが必要です。ライセンス不一致の問題を回避するために、クラスタリングを有効にする前に、ライセンスサーバで各ユニットのライセンスを取得することをお勧めします。また、高度暗号化ライセンスを使用する場合は、クラスタ制御リンクの暗号化に関する問題も発生します。

クラスタリング機能自体にライセンスは必要ありません。

高度暗号化ライセンスは、登録トークンを適用すると、対象となるお客様の場合自動的に有効化されます。ASA 設定で有効化される高度暗号化（3DES/AES）機能ライセンスについては、以下を参照してください。

ASA ライセンス設定では、制御ユニットに対するスマートライセンスの設定のみを行えます。設定はデータユニットに複製されますが、一部のライセンスに対しては、データユニットはこの設定を使用しません。この設定はキャッシュ状態のままになり、制御ユニットのみがこのライセンスを要求します。ライセンスは単一のクラスライセンスにまとめられ、クラスタの各ユニットで共有されます。この集約ライセンスはデータユニットにもキャッシュされ、その中の1つが将来制御ユニットとなったときに使用されます。各ライセンスタイプは次のように処理されます：

- **Essentials**：制御ユニットのみがサーバーから Essentials ライセンスを要求し、ライセンスの集約により、すべてのユニットがそれを使用できます。
- **スループット**：各ユニットには、サーバからの各自のスループットライセンスが必要です。
- **高度な暗号化（3DES）**：スマートアカウントで高度な暗号化が許可されていないが、高度な暗号化の使用が許可されているとシスコが判断した場合、高度な暗号化ライセンスをアカウントに手動で追加できます。制御ユニットのみがこのライセンスを要求し、ライセンスの集約により、すべてのユニットがそれを使用できます。

永続ライセンスの予約

永続ライセンスを予約するには、ユニットごとに個別のライセンスを購入し、クラスターリングを設定する前にライセンスを有効にする必要があります。

Firepower 4100/9300 の ASA クラスライセンス

Smart Software Manager Regular およびオンプレミス

クラスターリング機能自体にライセンスは必要ありません。強力な暗号化およびその他のオプションのライセンスを使用するには、それぞれの Firepower 4100/9300 シャーシがライセンス機関または Smart Software Manager の通常およびオンプレミスサーバーに登録されている必要があります。データユニットは追加料金なしで使用できます。

高度暗号化ライセンスは、登録トークンを適用すると、対象となるお客様の場合自動的に有効化されます。トークンを使用している場合、各シャーシに同じ暗号化ライセンスが必要です。ASA 設定で有効化される高度暗号化（3DES/AES）機能ライセンスについては、以下を参照してください。

ASA ライセンス設定では、制御ユニットに対するスマートライセンスの設定のみを行えます。設定はデータユニットに複製されますが、一部のライセンスに対しては、データユニットはこの設定を使用しません。この設定はキャッシュ状態のままになり、制御ユニットのみがこのライセンスを要求します。ライセンスは単一のクラスライセンスにまとめられ、クラスタの各ユニットで共有されます。この集約ライセンスはデータユニットにもキャッシュされ、その中の1つが将来制御ユニットとなったときに使用されます。各ライセンスタイプは次のように処理されます：

- **Essentials**：制御ユニットのみがサーバーからEssentialsライセンスを要求し、ライセンスの集約により、両方のユニットがそれを使用できます。
- **コンテキスト**：制御ユニットのみがサーバーからコンテキストライセンスを要求します。デフォルトでEssentialsライセンスは10のコンテキストを含み、すべてのクラスタメンバー上に存在します。各ユニットのEssentialsライセンスの値と、制御ユニットのコンテキストライセンスの値は、集約されたクラスタライセンスでのプラットフォーム制限まで統合されます。次に例を示します。
 - クラスタに6台のFirepower9300モジュールがある場合を考えます。Essentialsライセンスは10のコンテキストを含みます。6つユニットの場合、合計で60のコンテキストが加算されます。制御ユニット上で追加の20コンテキストライセンスを設定します。したがって、集約されたクラスタライセンスは80のコンテキストを含みます。モジュールごとのプラットフォーム制限は250であるため、統合されたライセンスに最大250のコンテキストが許容されます。80のコンテキストは制限範囲内です。したがって、制御ユニット上で最大80コンテキストを設定できます。各データユニットも、コンフィギュレーションの複製を介して80コンテキストを持つことになります。
 - クラスタにFirepower 4112が3台あるとします。Essentialsライセンスは10のコンテキストを含みます。3つユニットの場合、合計で30のコンテキストが加算されます。制御ユニット上で追加の250コンテキストライセンスを設定します。したがって、集約されたクラスタライセンスは280のコンテキストを含みます。ユニットごとのプラットフォームの制限が250であるため、統合されたライセンスでは最大250のコンテキストが許容されます。280コンテキストは制限を超えています。したがって、制御ユニット上で最大250のコンテキストのみを設定できます。各データユニットも、コンフィギュレーションの複製を介して250のコンテキストを持つことになります。この場合では、制御ユニットのコンテキストライセンスとして220のコンテキストのみを設定する必要があります。
- **キャリア**：分散型S2S VPNに必要。このライセンスはユニットごとの権限付与であり、各ユニットはサーバーから各自のライセンスを要求します。
- **高度な暗号化（3DES）**：2.3.0以前のCisco Smart Software Manager オンプレミス展開の場合。またはスマートアカウントで高度な暗号化が許可されていないが、高度な暗号化の使用が許可されているとシスコが判断した場合、高度な暗号化ライセンスをアカウントに手動で追加できます。このライセンスはユニットごとの権限付与であり、各ユニットはサーバーから各自のライセンスを要求します。

新しい制御ユニットが選定されると、このユニットが集約ライセンスを引き続き使用します。また、制御ユニットのライセンスを再要求するために、キャッシュされたライセンス設定も使用します。古い制御ユニットがデータユニットとしてクラスタに再度参加すると、制御ユニットのライセンス権限付与が解放されます。アカウントに利用可能なライセンスがない場合、データユニットがライセンスを解放する前に、制御ユニットのライセンスがコンプライアンス違反状態になることがあります。保持されたライセンスは30日間有効ですが、この猶予期間以降もコンプライアンス違反となる場合、特別なライセンスを必要とする機能の設定変更を行なえません。ただし、動作には影響ありません。新しいアクティブユニットは、ライセンスのコンプライアンスが確保されるまで12時間ごとに権限承認更新要求を送信します。ライセン

ス要求が完全に処理されるまで、設定の変更を控えてください。ユニットがクラスタから離れた場合、キャッシュされた制御ユニットの設定は削除されます。一方で、ユニットごとの権限は保持されます。この場合、クラスタ外のユニットのコンテキストライセンスを再要求する必要があります。

永続ライセンスの予約

永続ライセンスを予約するには、シャーシごとに個別のライセンスを購入し、クラスタリングを設定する前にライセンスを有効にする必要があります。

スマートソフトウェアライセンスの前提条件

Smart Software Manager 定期およびオンプレミスの前提条件

Firepower 4100/9300

ASA ライセンス資格を設定する前に、Firepower 4100/9300 シャーシでスマートソフトウェアライセンスインフラストラクチャを設定します。

他のすべてのモデル

- デバイスからのインターネットアクセス、HTTP プロキシアクセス、Smart Software Manager オンプレミスサーバーへのアクセスを確保します。
- デバイスが Smart Software Manager の名前を解決できるように DNS サーバーを設定します。
- デバイスのクロックを設定します。プラットフォームモードの Firepower 2100 では、FXOS でクロックを設定します。
- Cisco Smart Software Manager でアカウントを作成します。

<https://software.cisco.com/#module/SmartLicensing>

まだアカウントをお持ちでない場合は、リンクをクリックして[新しいアカウントを設定](#)してください。Smart Software Manager では、組織のアカウントを作成できます。

永続ライセンス予約の前提条件

- Cisco Smart Software Manager でマスターアカウントを作成します。

<https://software.cisco.com/#module/SmartLicensing>

まだアカウントをお持ちでない場合は、リンクをクリックして[新しいアカウントを設定](#)してください。Smart Software Manager では、組織のマスターアカウントを作成できます。永続ライセンス予約には ASA からスマートライセンスサーバーへのインターネット接続が必要ですが、永続ライセンスの管理には Smart Software Manager が使用されます。

- 永続ライセンス予約のサポートはライセンスチームから受けられます。永続ライセンス予約を使用する理由を示す必要があります。アカウントが承認されていない場合、永続ライセンスを購入して適用することはできません。
- 専用の永続ライセンスを購入します。アカウントに正しいライセンスがない場合、ASAでライセンスを予約しようとする、「The licenses cannot be reserved because the Virtual Account does not contain a sufficient surplus of the following perpetual licenses: 1 - Firepower 4100 ASA PERM UNIV(perpetual)」のようなエラーメッセージが表示されます。
- 永続ライセンスには、高度暗号化（3DES/AES）ライセンス（アカウントに資格がある場合）を含むすべての機能が含まれます。セキュアクライアントの使用権を有効にするセキュアクライアントライセンスを購入すれば、セキュアクライアントの機能もプラットフォームの上限まで有効になります（「[Secure Client Advantage](#)、[Secure Client Premier](#)、および[Secure Client VPNのみライセンス（9ページ）](#)」を参照）。
- ASA 仮想：永続ライセンスの予約は Azure ハイパーバイザではサポートされません。

スマートソフトウェアライセンスのガイドライン

- スマートソフトウェアライセンスのみがサポートされます。ASA 仮想の古いソフトウェアについては、PAK ライセンスが供与された既存の ASA 仮想をアップグレードする場合、前にインストールしたアクティベーションキーは無視されますが、デバイスに保持されます。ASA 仮想をダウングレードする場合は、アクティベーションキーが復活します。
- 永続ライセンスの予約については、デバイスを廃棄する前にライセンスを戻す必要があります。ライセンスを正式に戻さないと、ライセンスが使用中の状態のままになり、新しいデバイスに再使用できません。
- Cisco Transport Gateway は非標準の国番号の証明書を使用するため、ASA をその製品と組み合わせて使用する場合は HTTPS を使用できません。Cisco Transport Gateway で HTTP を使用する必要があります。

スマートソフトウェアライセンスのデフォルト

スマート転送

デフォルトでは、すべてのデバイスモデルがスマートソフトウェアライセンス通信に Smart Transport を使用し、次の URL を使用します。

`https://smartreceiver.cisco.com/licservice/license`

デバイスが `www.smartreceiver.cisco.com` に接続できることを確認します。この URL に到達できない場合は、callhome 転送タイプを使用します。

Firepower 4100/9300 では、シャーシレベルでスマートソフトウェアライセンスの通信を有効にする必要があります。

ASA 仮想

- ASA 仮想 を展開するときに、機能層とスループットレベルを設定します。現時点では、Essentials レベルのみを使用できます。永続ライセンス予約の場合、これらのパラメータを設定する必要はありません。永続ライセンス予約を有効にすると、これらのコマンドはコンフィギュレーションから削除されます。



(注) Essentials ライセンスは以前は標準ライセンスと呼ばれていました。CLI では引き続き「標準」という用語が使用されています。

```
license smart
  feature tier standard
  throughput level {100M | 1G | 2G | 10G | 20G}
```

ASA 仮想：スマートソフトウェアライセンスの設定

このセクションでは、ASA 仮想にスマートソフトウェアライセンシングを構成する方法を説明します。

ASA 仮想：定期スマートソフトウェアライセンシングの設定

ASA 仮想 を展開する場合は、デバイスを事前に設定し、Smart Software Manager に登録するために登録トークンを適用して、スマートソフトウェアライセンシングを有効にできます。HTTP プロキシサーバー、ライセンス権限付与を変更する必要がある場合、または ASA 仮想 を登録する必要がある場合（Day0 設定に ID トークンを含めなかった場合など）は、このタスクを実行します。



(注) ASA 仮想 を展開したときに、HTTP プロキシとライセンス権限付与が事前に設定されている可能性があります。また、ASA 仮想 を展開したときに Day0 設定で登録トークンが含まれている可能性があります。その場合は、この手順を使用して再登録する必要はありません。

手順

ステップ 1 ([Cisco Smart Software Manager](#)) で、このデバイスを追加するバーチャルアカウントの登録トークンを要求してコピーします。

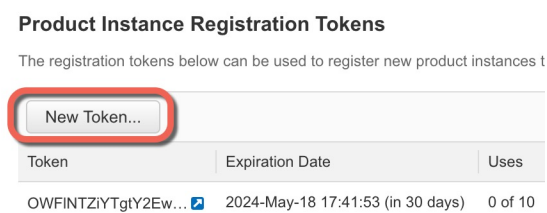
- a) [Inventory] をクリックします。

図 1: インベントリ



- b) [General] タブで、[New Token] をクリックします。

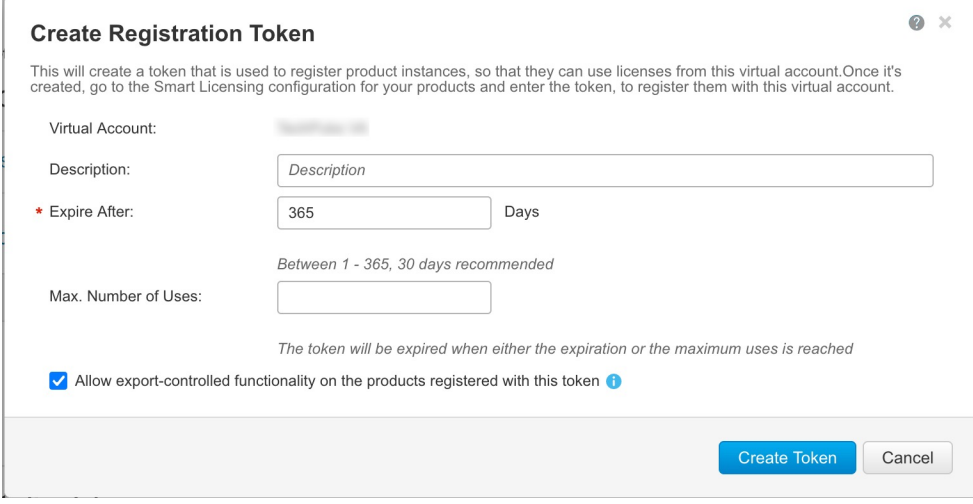
図 2: 新しいトークン



- c) [登録トークンを作成 (Create Registration Token)] ダイアログボックスで、以下の設定値を入力してから [トークンを作成 (Create Token)] をクリックします。

- 説明
- [有効期限 (Expire After)] : 推奨値は 30 日です。
- 最大使用回数 (Max. Number of Uses)
- [このトークンに登録された製品で輸出管理機能を許可する (Allow export-controlled functionality on the products registered with this token)] : 輸出コンプライアンス フラグを有効にします。

図 3: 登録トークンの作成



Create Registration Token

This will create a token that is used to register product instances, so that they can use licenses from this virtual account. Once it's created, go to the Smart Licensing configuration for your products and enter the token, to register them with this virtual account.

Virtual Account: [Redacted]

Description:

* Expire After: Days
Between 1 - 365, 30 days recommended

Max. Number of Uses:

The token will be expired when either the expiration or the maximum uses is reached

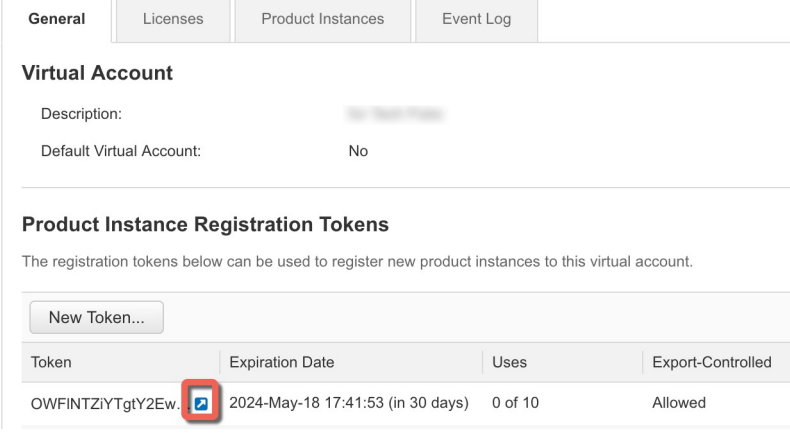
☒ Allow export-controlled functionality on the products registered with this token ⓘ

Create Token **Cancel**

トークンはインベントリに追加されます。

- d) トークンの右側にある矢印アイコンをクリックして[トークン (Token)]ダイアログボックスを開き、トークン ID をクリップボードにコピーできるようにします。ASA の登録が必要なときに後の手順で使用するために、このトークンを準備しておきます。

図 4: トークンの表示



General | Licenses | Product Instances | Event Log

Virtual Account

Description: [Redacted]

Default Virtual Account: No

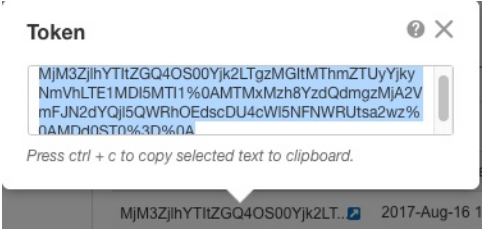
Product Instance Registration Tokens

The registration tokens below can be used to register new product instances to this virtual account.

New Token...

Token	Expiration Date	Uses	Export-Controlled
OWFINTZiYtGtY2Ew. ⓘ	2024-May-18 17:41:53 (in 30 days)	0 of 10	Allowed

図 5: トークンのコピー



Token

MjM3ZjIhYTItZGQ4OS00Yjk2LTgzMGltMTNmZTUyYjkyNmVhLTE1MDI5MTI1%0AMTMxMzh8YzdQdmgzMjA2VmFJN2dYQjI5QWRhOEEdscDU4cWl5NFNWRUtsa2wz%0AMdnd0STn%3dn%0A

Press ctrl + c to copy selected text to clipboard.

MjM3ZjIhYTItZGQ4OS00Yjk2LTgzMGltMTNmZTUyYjkyNmVhLTE1MDI5MTI1%0AMTMxMzh8YzdQdmgzMjA2VmFJN2dYQjI5QWRhOEEdscDU4cWl5NFNWRUtsa2wz%0AMdnd0STn%3dn%0A 2017-Aug-16 1

ステップ 2 (任意)

ステップ 3 (任意) ASA 仮想 で、Smart Transport の HTTP プロキシ URL を指定します。

license smart

transport proxy proxy_server_ip port port

Smart Transport の代わりに Smart Call Home を使用するには、[ステップ 5 \(36 ページ\)](#) を参照してください。

(注)

- 認証を使用する HTTP プロキシはサポートされません。
- プロキシサーバーの URL を設定する場合は、プロトコルを指定しないでください。

例 :

```
ciscoasa(config)# license smart
ciscoasa(config-smart-lic)# transport proxy 10.1.1.1 port 10101
```

例 :

```
ciscoasa(config)# license smart
ciscoasa(config-smart-lic)# transport proxy proxy.esl.cisco.com port 80
```

ステップ 4 ライセンス権限付与を設定します。

a) ライセンス スマート コンフィギュレーション モードを開始します。

license smart

例 :

```
ciscoasa(config)# license smart
ciscoasa(config-smart-lic)#
```

b) 機能層を設定します。

feature tier standard

使用できるのは標準 (Essentials) 層のみですが、設定で有効にする必要があります。Essentials ライセンスは、以前は標準ライセンスと呼ばれていました。「標準」は引き続き CLI で使用されています。

c) Smart Software Manager から要求されるライセンスを決定するスループットレベルを設定します。

throughput level {100M | 1G | 2G | 10G | 20G}

次のスループットとライセンスの関係を参照してください。

- 100M : ASAv5
- 1G : ASAv10
- 2G : ASAv30

- 10G : ASAv50
- 20G : ASAv100

例：

```
ciscoasa(config-smart-lic)# throughput level 2G
```

- d) ライセンス スマート モードを終了して、変更を適用します。

exit

明示的にモードを終了する (**exit** または **end**) か、別のモードに移行するコマンドを入力することによってライセンス スマート コンフィギュレーション モードを終了するまで、変更が有効になりません。

例：

```
ciscoasa(config-smart-lic)# exit
ciscoasa(config)#
```

- ステップ 5** (任意) スマートライセンスサーバーとの通信には、デフォルトの Smart Transport の代わりに Smart Call Home を使用します。

Smart Transport の代わりに Smart Call Home を使用する必要があることがわかっている場合は、次の手順を実行します。それ以外の場合は、デフォルトの Smart Transport を使用する必要があります。

- a) 転送タイプを [Smart Call Home] に設定します。

license smart

transport type callhome

構成には、Smart Software Manager の URL を指定する **ライセンス** と呼ばれる Smart Call Home のプロファイルが含まれます。

```
call-home
  profile License
    destination address http
    https://tools.cisco.com/its/service/oddce/services/DDCEService
```

例：

```
ciscoasa(config)# license smart
ciscoasa(config-smart-lic)#transport type callhome
```

- b) (任意) HTTP プロキシの URL を指定します。

call-home

http-proxy ip_address port port

(注)

認証を使用する HTTP プロキシはサポートされません。

例：

```
ciscoasa(config)# call-home
ciscoasa(cfg-call-home)# http-proxy 10.1.1.1 port 443
```

ステップ 6 Smart Software Manager で ASA 仮想 を登録します。

license smart register idtoken id_token [force]

ASA 仮想 が、Smart Software Manager への登録と設定されたライセンス権限付与の承認要求を試行します。

ASA 仮想 を登録すると、Smart Software Manager は ASA 仮想 と Smart Software Manager 間の通信用の ID 証明書を発行します。また、ASA 仮想 が該当する仮想アカウントに割り当てられます。通常、この手順は 1 回限りのインスタンスです。ただし、通信の問題などが原因で ID 証明書の期限が切れた場合は、ASA 仮想 の再登録が必要になります。

force キーワードを使用して、Smart Software Manager と同期されていない可能性がある登録済みの ASA 仮想 を登録します。たとえば、Smart Software Manager から誤って ASA 仮想 を削除した場合に **force** を使用します。

例：

```
ciscoasa# license smart register idtoken YjE3Njc5MzYtMGQzMj00OTA4
LWJhODItNzBhMGQ5NGRlYjUxLTE0MTQ5NDYy%0AODQzNz18NXk2bzV3SDE0ZkgwQk
dYRmZlNTNCNGlVRnBHUFpjcm02WTB4TU4w%0Ac2NnMD0%3D%0A
```

ステップ 7 ライセンスのステータスを確認します。

show license status または **show running-config license**

Smart Software Manager との通信に失敗した場合は、DNS サーバーが設定されていることと、サーバーに到達するための正しいルーティングがあることを確認します。

例：

```
asav1# show license status

Smart Licensing is ENABLED

Utility:
  Status: DISABLED

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

Transport:
  Type: Callhome

Registration:
  Status: REGISTERING - REGISTRATION IN PROGRESS
```

```
Export-Controlled Functionality: NOT ALLOWED
Initial Registration: FAILED on Aug 31 2023 19:38:45 UTC
  Failure reason: Communication message send error
Next Registration Attempt: Aug 31 2023 19:56:56 UTC
```

```
License Authorization:
  Status: EVAL EXPIRED on Feb 25 2023 16:39:25 UTC
```

```
Export Authorization Key:
  Features Authorized:
    <none>
```

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

例 :

```
ciscoasa(config)# show running-config license
license smart
feature tier standard
throughput level 1G
transport proxy proxy.esl.cisco.com port 80
```

ASA 仮想 : Smart Software Manager オンプレミスライセンスングの設定

この手順は、Smart Software Manager オンプレミスを使用する ASA 仮想 に適用されます。

始める前に

- Smart Software Manager オンプレミス OVA ファイルを [Cisco.com](https://www.cisco.com) からダウンロードし、VMware ESXi サーバーにインストールして設定します。詳細については、『[Cisco Smart Software Manager On-Prem Data Sheet](#)』を参照してください。
- バージョン 7.0 では、Smart Transport が Smart Software Manager オンプレミスに追加されました。これより古いバージョンを使用する場合、この手順に従って、ASA 仮想 で Smart Call Home を有効にします。
- デバイスをエアギャップネットワークに配置する前に、クリプト CA トラストプールをダウンロードします。このトラストプールは通常、自動的にダウンロードされますが、エアギャップネットワークでは失効している可能性があります。

```
crypto ca trustpool import url http://www.cisco.com/security/pki/trs/ios_core.p7b
```

手順

ステップ 1 Smart Software Manager オンプレミスで登録トークンを要求します。

ステップ 2 (任意) ASA 仮想 で、Smart Transport の HTTP プロキシ URL を指定します。

license smart**transport proxy proxy_server_ip port port**

Smart Transport の代わりに Smart Call Home を使用するには、[ステップ 7（40 ページ）](#) を参照してください。

（注）

認証を使用する HTTP プロキシはサポートされません。

例：

```
ciscoasa(config)# license smart
ciscoasa(config-smart-lic)# transport proxy 10.1.1.1 port 10101
```

ステップ 3 ライセンスサーバーの URL を変更して、Smart Software Manager オンプレミスに移動します。

license smart**transport url https://on-prem_ip_address/SmartTransport**

Smart Transport の代わりに Smart Call Home を使用するには、[ステップ 7（40 ページ）](#) を参照してください。

例：

```
ciscoasa(config)# license smart
ciscoasa(config-smart-lic)# transport url https://10.1.5.5/SmartTransport
```

ステップ 4 （任意）

ステップ 5

ステップ 6 ライセンス権限付与を設定します。

a) ライセンス スマート コンフィギュレーション モードを開始します。

license smart

例：

```
ciscoasa(config)# license smart
ciscoasa(config-smart-lic)#
```

b) 機能層を設定します。

feature tier standard

使用できるのは標準（Essentials）層のみですが、設定で有効にする必要があります。

Essentials ライセンスは、以前は標準ライセンスと呼ばれていました。標準は引き続き CLI で使用されています。

c) Smart Software Manager から要求されるライセンスを決定するスループットレベルを設定します。

throughput level {100M | 1G | 2G | 10G | 20G}

次のスループットとライセンスの関係を参照してください。

- 100M : ASAv5
- 1G : ASAv10
- 2G : ASAv30
- 10G : ASAv50
- 20G : ASAv100

例 :

```
ciscoasa(config-smart-lic)# throughput level 2G
```

- d) ライセンス スマート モードを終了して、変更を適用します。

exit

明示的にモードを終了する (**exit** または **end**) か、別のモードに移行するコマンドを入力することによってライセンス スマート コンフィギュレーション モードを終了するまで、変更が有効になりません。

例 :

```
ciscoasa(config-smart-lic)# exit
ciscoasa(config)#
```

ステップ 7 (任意) スマートライセンスサーバーとの通信には、デフォルトの Smart Transport の代わりに Smart Call Home を使用します。

Smart Transport の代わりに Smart Call Home を使用する必要があることがわかっている場合は、次の手順を実行します。それ以外の場合は、デフォルトの Smart Transport を使用する必要があります。

- a) 転送タイプを [Smart Call Home] に設定します。

license smart

transport type callhome

構成には、Smart Software Manager の URL を指定する **ライセンス** と呼ばれる Smart Call Home のプロファイルが含まれます。

```
call-home
  profile License
    destination address http
    https://tools.cisco.com/its/service/oddce/services/DDCEService
```

例 :

```
ciscoasa(config)# license smart
```

```
ciscoasa(config-smart-lic)#transport type callhome
```

- b) (任意) HTTP プロキシの URL を指定します。

call-home

http-proxy ip_address port port

(注)

認証を使用する HTTP プロキシはサポートされません。

例：

```
ciscoasa(config)# call-home
ciscoasa(cfg-call-home)# http-proxy 10.1.1.1 port 443
```

- c) ライセンスサーバーの URL を変更して、Smart Software Manager オンプレミスに移動します。

call-home

profile License

destination address http

https://on-prem_ip_address/Transportgateway/services/DeviceRequestHandler

例：

```
ciscoasa(config)# call-home
ciscoasa(cfg-call-home)# profile License
ciscoasa(cfg-call-home-profile)#destination address http
https://10.1.5.5/Transportgateway/services/DeviceRequestHandler
```

ステップ 8 手順 1 で要求したトークンを使用して ASA を登録します。

license smart register idtoken id_token

ASA が Smart Software Manager オンプレミスに登録され、設定されたライセンス権限付与の承認を要求します。Smart Software Manager オンプレミスは、お使いのアカウントで許可すれば高度暗号化 (3DES/AES) ライセンスも適用します。

ASA 仮想 を登録すると、Smart Software Manager オンプレミスは ASA 仮想 と Smart Software Manager 間の通信用の ID 証明書を発行します。また、ASA 仮想 が該当する仮想アカウントに割り当てられます。通常、この手順は1回限りのインスタンスです。ただし、通信の問題などが原因で ID 証明書の期限が切れた場合は、ASA 仮想 の再登録が必要になります。

例：

```
ciscoasa# license smart register idtoken YjE3Njc5MzYtMGQzMj00OTA4
LWJhODItNzBhMGQ5NGRlYjUxLTE0MTQ5NDAY%0AODQzNz18NXk2bzV3SDE0ZkgwQk
dYRmZlNTNCNGlvRnBHUFpjcm02WTB4TU4w%0Ac2NnMD0%3D%0A
```

ステップ 9 ライセンスのステータスを確認します。

show license status

Smart Software Manager との通信に失敗した場合は、DNS サーバーが設定されていることと、サーバーに到達するための正しいルーティングがあることを確認します。

例：

```
asav1# show license status

Smart Licensing is ENABLED

Utility:
  Status: DISABLED

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

Transport:
  Type: Callhome

Registration:
  Status: REGISTERING - REGISTRATION IN PROGRESS
  Export-Controlled Functionality: NOT ALLOWED
  Initial Registration: FAILED on Aug 31 2023 19:38:45 UTC
  Failure reason: Communication message send error
  Next Registration Attempt: Aug 31 2023 19:56:56 UTC

License Authorization:
  Status: EVAL EXPIRED on Feb 25 2023 16:39:25 UTC

Export Authorization Key:
  Features Authorized:
    <none>

Miscellaneous:
  Custom Id: <empty>
```

ASA 仮想：ユーティリティ（MSLA）スマートソフトウェアライセンスングの設定

マネージドサービス ライセンス契約（MSLA）のユーティリティ ライセンシングでは、ライセンス サブスクリプションまたは永久的ライセンスの1回かぎりの料金を支払うのではなく、ライセンスの使用時間に応じて支払うことができます。ユーティリティ ライセンシング モードでは、ASA 仮想がライセンスの使用状況を時間単位（15 分間隔）で追跡します。ASA 仮想は、Smart Software Manager に4時間ごとにライセンス使用状況レポート（「RUM レポート」と呼ばれます）を送信します。その後、使用状況レポートは、課金サーバーに転送されます。ユーティリティ ライセンシングでは、Smart Call Home は、ライセンスングメッセージのトランスポートとして使用されません。代わりに、メッセージが、スマートトランスポートを使用して HTTP/HTTPS 経由で直接送信されます。

始める前に

Download the Smart Software Manager オンプレミス OVA ファイルを [Cisco.com](https://www.cisco.com) からダウンロードし、VMware ESXi サーバーにインストールして構成します。詳細については、『[Cisco Smart Software Manager On-Prem Data Sheet](#)』を参照してください。

手順

ステップ 1 Smart Software Manager オンプレミスで、このデバイスを追加する仮想アカウントの登録トークンを要求してコピーします。

a) [Inventory] をクリックします。

図 6: インベントリ

Cisco Software Central > Smart Software Licensing

Smart Software Licensing

Alerts

Inventory

Convert to Smart Licensing

b) [General] タブで、[New Token] をクリックします。

図 7: 新しいトークン

Product Instance Registration Tokens

The registration tokens below can be used to register new product instances t

New Token...

Token

Expiration Date

Uses

OWFINTZIYTgtY2Ew... 2024-May-18 17:41:53 (in 30 days) 0 of 10

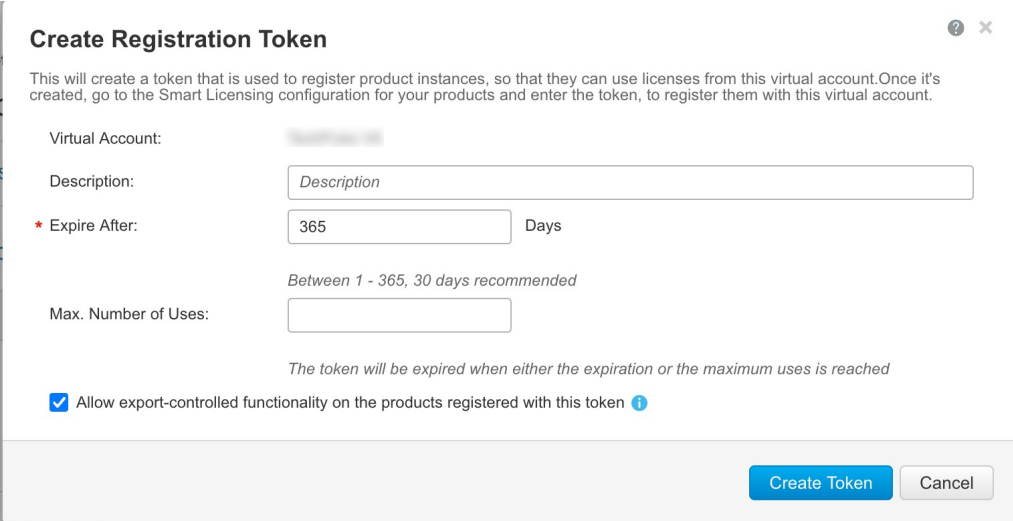
c) [登録トークンを作成（Create Registration Token）] ダイアログボックスで、以下の設定値を入力してから [トークンを作成（Create Token）] をクリックします。

• 説明

• [有効期限（Expire After）]：推奨値は 30 日です。

• [このトークンに登録された製品で輸出管理機能を許可する（Allow export-controlled functionality on the products registered with this token）]：輸出コンプライアンス フラグを有効にします。

図 8: 登録トークンの作成



Create Registration Token

This will create a token that is used to register product instances, so that they can use licenses from this virtual account. Once it's created, go to the Smart Licensing configuration for your products and enter the token, to register them with this virtual account.

Virtual Account: [Redacted]

Description:

* Expire After: Days

Between 1 - 365, 30 days recommended

Max. Number of Uses:

The token will be expired when either the expiration or the maximum uses is reached

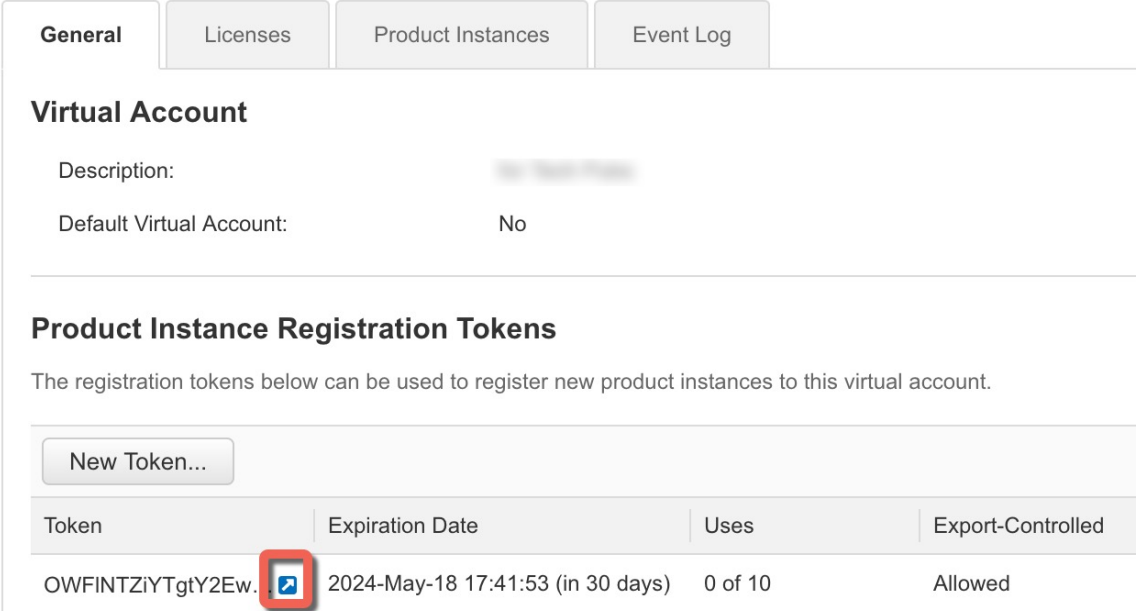
☒ Allow export-controlled functionality on the products registered with this token ⓘ

Create Token **Cancel**

トークンはインベントリに追加されます。

- d) トークンの右側にある矢印アイコンをクリックして [トークン (Token)] ダイアログボックスを開き、トークン ID をクリップボードにコピーできるようにします。ASA の登録が必要なときに後の手順で使用するために、このトークンを準備しておきます。

図 9: トークンの表示



General Licenses Product Instances Event Log

Virtual Account

Description: [Redacted]

Default Virtual Account: No

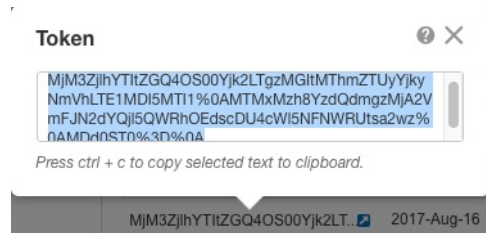
Product Instance Registration Tokens

The registration tokens below can be used to register new product instances to this virtual account.

New Token...

Token	Expiration Date	Uses	Export-Controlled
OWFINTZiYTgtY2Ew.	2024-May-18 17:41:53 (in 30 days)	0 of 10	Allowed

図 10: トークンのコピー



ステップ 2 ASA 仮想 で、スマートライセンスングのパラメータを構成します。

- a) ライセンス スマート コンフィギュレーション モードを開始します。

license smart

例：

```
ciscoasa(config)# license smart
ciscoasa(config-smart-lic)#
```

- b) スマートトランスポートを有効にします。

transport type smart

ユーティリティ ライセンスングには、Smart Call Home ではなくスマートトランスポートが必要です。

例：

```
ciscoasa(config-smart-lic)# transport type smart
```

- c) (任意) Smart Software Manager 定期またはオンプレミスの URL を指定します。必要に応じて、ライセンス使用状況レポートの代替宛先を指定できます。

transport url {transport_url | utility utility_url | default }

URLを設定しない場合、スマートトランスポートとライセンス使用状況レポートの両方に **default** が使用されます。これは、**https://smartreceiver.cisco.com/licservice/license** です。

例：

```
ciscoasa(config-smart-lic)# transport url http://server99.cisco.com/SmartTransport
ciscoasa(config-smart-lic)# transport url utility
http://server-utility.cisco.com/SmartTransport
```

- d) (任意) ネットワークでインターネットアクセスに HTTP プロキシを使用する場合は、プロキシアドレスを設定します。

transport proxy proxy-url port proxy-port-number

(注)

認証を使用する HTTP プロキシはサポートされません。

例：

```
ciscoasa(config-smart-lic)# transport proxy 10.1.1.1 port 443
```

- e) ライセンスメッセージでライセンスデバイスのホスト名または Smart Agent バージョン番号を抑制します。

privacy {all | hostname | version}

例：

```
ciscoasa(config-smart-lic)# privacy all
```

- f) 機能層を設定します。

feature tier standard

使用できるのは標準 (Essentials) 層のみですが、設定で有効にする必要があります。Essentials ライセンスは、以前は標準ライセンスと呼ばれていました。標準は引き続き CLI で使用されています。

- g) Smart Software Manager から要求されるライセンスを決定するスループットレベルを設定します。

throughput level {100M | 1G | 2G | 10G | 20G}

次のスループットとライセンスの関係を参照してください。

- 100M : ASAv5
- 1G : ASAv10
- 2G : ASAv30
- 10G : ASAv50
- 20G : ASAv100

例：

```
ciscoasa(config-smart-lic)# throughput level 2G
```

- h) (任意) 高度暗号化を有効にします。

feature strong-encryption

Smart Software Manager から高度暗号化トークンを受け取った場合、このライセンスは必要ありません。ただし、スマートアカウントで高度暗号化が許可されていないものの、高度暗号化の使用が許可されているとシスコが判断した場合、高度暗号化ライセンスをアカウントに手動で追加できます。アクティブユニットのみがこのライセンスを要求し、ライセンスの集約により両方のユニットがこれを使用できます。

例：

```
ciscoasa(config-smart-lic)# feature strong-encryption
```

- i) ライセンス スマート モードを終了して、変更を適用します。

exit

明示的にモードを終了する (**exit** または **end**) か、別のモードに移行するコマンドを入力することによってライセンス スマート コンフィギュレーション モードを終了するまで、変更が有効になりません。

例 :

```
ciscoasa(config-smart-lic)# exit
ciscoasa(config)#
```

ステップ 3 ユーティリティ ライセンシングを設定します。

- a) ユーティリティ コンフィギュレーション モードを開始します。

utility

例 :

```
ciscoasa(config-smart-lic)# utility
ciscoasa(config-smart-lic-util)#
```

- b) 一意の顧客 ID を作成します。この ID は、Utility Licensing 使用状況レポートメッセージに含まれます。

custom-id *custom-identifier*

例 :

```
ciscoasa(config-smart-lic-util)# custom-id MyCustomID
```

- c) 一意の顧客プロフィールを作成します。この情報は、Utility Licensing 使用状況レポートに含まれます。

customer-info {city | country | id | name | postalcode | state | street} value

例 :

```
ciscoasa(config-smart-lic-util)# customer-info city MyCity
ciscoasa(config-smart-lic-util)# customer-info country MyCountry
ciscoasa(config-smart-lic-util)# customer-info id MyID
ciscoasa(config-smart-lic-util)# customer-info name MyName
ciscoasa(config-smart-lic-util)# customer-info postalcode MyPostalCode
ciscoasa(config-smart-lic-util)# customer-info state MyState
ciscoasa(config-smart-lic-util)# customer-info street MyStreet
```

- d) ユーティリティ ライセンシングを有効にします。

mode standard

例：

```
ciscoasa(config-smart-lic-util)# mode standard
```

ステップ 4 手順 1 で要求したトークンを使用して ASA を登録します。

license smart register idtoken id_token

例：

```
ciscoasa# license smart register idtoken YjE3Njc5MzYtMGQzMj00OTA4
LWJhODItNzBhMGQ5NGRlYjUxLTE0MTQ5NDAY%0AODQzNz18NXk2bzV3SDE0ZkgwQk
dYRmZlNTNCNGlvRnBHUFpjcm02WTB4TU4w%0Ac2NnMD0%3D%0A
```

ステップ 5 ライセンスのステータスを確認します。

show license status

Smart Software Manager との通信に失敗した場合は、DNS サーバーが設定されていることと、サーバーに到達するための正しいルーティングがあることを確認します。

例：

```
asav1# show license status

Smart Licensing is ENABLED

Utility:
  Status: ENABLED
  Utility report:
    Last success: May 14 2018 21:37:25 UTC
    Last attempt: SUCCEEDED on May 14 2018 21:37:24 UTC
    Next attempt: May 15 2018 01:37:24 UTC

Customer Information:
  Id: MyID
  Name: MyName
  Street: MyStreet
  City: MyCity
  State: MyState
  Country: MyCountry
  Postal Code: MyPostalCode

Data Privacy:
  Sending Hostname: no
  Callhome hostname privacy: DISABLED
  Smart Licensing hostname privacy: ENABLED
  Version privacy: ENABLED

Transport:
  Type: Smart
  Registration URL: http://server99.cisco.com/SmartTransport
  Utility URL: http://server-utility.cisco.com/SmartTransport

Registration:
  Status: REGISTERED
  Export-Controlled Functionality: Allowed
```

```
Initial Registration: SUCCEEDED on May 14 2018 21:37:20 UTC
Last Renewal Attempt: None
Next Renewal Attempt: Sep 13 2018 13:34:40 UTC
Registration Expires: May 14 2019 21:29:20 UTC

License Authorization:
Status: AUTHORIZED on May 14 2018 21:37:22 UTC
Last Communication Attempt: NOT STARTED
Failure reason: Device in Thirdparty Utility Mode
Next Communication Attempt: None
Communication Deadline: Aug 12 2018 21:37:24 UTC
```

ASA 仮想：永続ライセンス予約の設定

ASA 仮想に永続ライセンスを割り当てることができます。このセクションでは、ASA 仮想の廃止やモデル層の変更などによって新しいライセンスが必要となった場合に、ライセンスを返却する方法についても説明します。

手順

ステップ1 [ASA 仮想 永続ライセンスのインストール \(49 ページ\)](#)

ステップ2 (オプション) [ASA 仮想の永続ライセンスの返却 \(52 ページ\)](#)

ASA 仮想 永続ライセンスのインストール

インターネットアクセスを持たない ASA 仮想の場合は、Smart Software Manager から永続ライセンスを要求できます。ASA 仮想 永続ライセンス予約の詳細については、「[ASA Virtual 永久ライセンス予約 \(3 ページ\)](#)」を参照してください。



- (注)
- 永続ライセンスの予約については、ASA 仮想を廃棄する前にライセンスを戻す必要があります。ライセンスを正式に戻さないと、ライセンスが使用中の状態のままになり、新しい ASA 仮想に再使用できません。[\(オプション\) ASA 仮想の永続ライセンスの返却 \(52 ページ\)](#) を参照してください。
 - 永続ライセンスをインストールした後に設定をクリアした場合 (**write erase** コマンドを使用するなど)、引数を指定せずに **license smart reservation** コマンドを使用して永続ライセンス予約を再度有効にする必要があります。この場合、この手順の残りの部分を完了する必要はありません。

始める前に

- 永続ライセンスを購入すると、Smart Software Manager でそれらのライセンスを使用できます。すべてのアカウントが永続ライセンスの予約について承認されているわけではありません。設定を開始する前にこの機能についてシスコの承認があることを確認します。
- ASA 仮想 の起動後に永続ライセンスを要求します。Day0 設定の一部として永続ライセンスをインストールすることはできません。

手順

ステップ 1 (Cisco ASAv5 のみ) DRAM が 2 GB (9.13 以降で必要な最小容量) の場合に Cisco ASAv5 永続ライセンスの使用を許可します。

license smart set_plr5

ステップ 2 ASA 仮想 CLI で、永続ライセンス予約を次のように有効にします。

license smart reservation

例：

```
ciscoasa (config)# license smart reservation
ciscoasa (config)#
```

通常のスマートライセンスを使用するには、このコマンド。

次のコマンドが削除されます。

```
license smart
  feature tier standard
  throughput level {100M | 1G | 2G | 10G | 20G}
```

ステップ 3 Smart Software Manager に入力するライセンス コードを次のように要求します。

license smart reservation request universal

例：

```
ciscoasa# license smart reservation request universal
Enter this request code in the Cisco Smart Software Manager portal:
ABP:ASAv,S:9AU5ET6UQHD{A8ug5/1jRDasp3w8uGlfeQ{53C13E
ciscoasa#
```

メモリまたはvCPUを変更する場合は、現在のライセンスを返却し、新しいモデルレベルで新しいライセンスを要求する必要があります。要求されたライセンスは、インストールされているメモリとvCPUと一致する必要があります。ASA 仮想 永続ライセンス予約のためのvCPUおよびメモリとライセンス間のマトリックスの詳細については、「[ASA Virtual 永久ライセンス予約 \(3 ページ\)](#)」を参照してください。

展開済みの ASA 仮想 のモデルを変更するには、新しいモデルの要件に合わせるために、ハイパーバイザからvCPUとDRAMの設定を変更します。各値については、ASA 仮想 のクイック

スタートガイドを参照してください。現在のモデルを表示するには、**show vm** コマンドを使用します。

このコマンドを再入力すると、リロード後にも同じコードが表示されます。このコードをまだ Smart Software Manager に入力していない場合、要求をキャンセルするには、以下を入力します。

license smart reservation cancel

パーマネントライセンスの予約をディセーブルにすると、保留中のすべての要求がキャンセルされます。すでに Smart Software Manager にコードを入力している場合は、その手順を完了して ASA 仮想 にライセンスを適用する必要があります。その時点から、必要に応じてライセンスを戻すことが可能になります。 [（オプション）ASA 仮想の永続ライセンスの返却（52 ページ）](#) を参照してください。

ステップ 4 Smart Software Manager インベントリ画面に移動して、[Instances] タブをクリックします。

<https://software.cisco.com/#SmartLicensing-Inventory>

[Licenses] タブにアカウントに関連するすべての既存のライセンスが、標準およびパーマネントの両方とも表示されます。

ステップ 5 [ライセンス予約 (License Reservation)] をクリックし、[予約要求コード (Reservation Request Code)] フィールドに ASA 仮想 コードを入力します。

ステップ 6 [ライセンスを予約 (Reserve License)] をクリックします。

Smart Software Manager が承認コードを生成します。コードをダウンロードまたはクリップボードにコピーできます。この時点で、ライセンスは、Smart Software Manager に従って使用中です。

[License Reservation] ボタンが表示されない場合、お使いのアカウントはパーマネントライセンスの予約について承認されていません。この場合、パーマネントライセンスの予約を無効にして標準のスマートライセンス コマンドを再入力する必要があります。

ステップ 7 ASA 仮想 CLI から、次のコマンドを実行し、承認コードを入力します。

license smart reservation install code

例 :

```
ciscoasa# license smart reservation install AAu3431rGRS00Ig5HQ12vpzg{MEYCIQCBw$  
INFO: ASAv platform license state is Licensed.  
ciscoasa#
```

これで、ASA 仮想 ライセンスが完全に適用されました。

ステップ 8 コマンドを実行して実行構成をスタートアップ構成に保存して、再起動中の構成の損失を避けます。

write memory

ステップ 9 ASA 仮想 からこのコマンドを実行すると、Cisco ASA に永続ライセンスが付与されていることを確認できます。

show license features

ASA 仮想 バージョン間でデフォルトのトランスポートモードが異なっていて、ダウングレードする場合は、次の手順を実行します。

1. 永続ライセンス予約の登録を解除します。
2. ASA 仮想 をダウングレードします。
3. 永続ライセンス予約を再度登録します。

バージョン 9.20.4 以降では Smart Transport がデフォルトになっていて、バージョン 9.20.3 以前では Smart Call Home がデフォルトになっています。

たとえば、ROM バージョン 9.20.4 から 9.18.1 にダウングレードする場合は、上記の手順を実行して永続ライセンス予約が登録解除されないようにします。

(オプション) ASA 仮想 の永続ライセンスの返却

ASA 仮想 を廃棄する場合やモデルレベルの変更によって（新しいライセンスが必要になった場合など）永続ライセンスが不要になった場合、以下の手順に従ってライセンスを正式に Smart Software Manager に戻す必要があります。すべての手順を実行しないと、ライセンスが使用中のままになり、他の場所で使用するために解除できなくなります。

手順

ステップ 1 ASA 仮想 CLI から、リターンコードを生成します。

license smart reservation return

例：

```
ciscoasa# license smart reservation return
Enter this return code in the Cisco Smart Software Manager portal:
Au3431rGRS00Ig5HQ12vpcg{uXiTRfVrp7M/zDpirLwYCaq8oSv60yZJuFDVBS2Q1iQ=
```

ただちに ASA 仮想 のライセンスがなくなり、評価状態に移行します。このコードを再度表示する必要がある場合は、このコマンドを再入力します。新しい永続ライセンスを要求する

(**license smart reservation request universal**) か、ASA 仮想 のモデルレベルを変更する（電源を切って vCPU/RAM を変更する）と、このコードを再表示できなくなることに注意してください。必ず、コードをキャプチャして、戻す作業を完了してください。

ステップ 2 ASA 仮想 ユニバーサルデバイス識別子 (UDI) が表示されるため、Smart Software Manager で ASA 仮想 インスタンスを見つけることができます。

show license udi

例：

```
ciscoasa# show license udi
UDI: PID:ASAv,SN:9AHV3KJBEKE
ciscoasa#
```

ステップ 3 Smart Software Manager インベントリ画面に移動して、[Product Instances] タブをクリックします。

<https://software.cisco.com/#SmartLicensing-Inventory>

[Product Instances] タブに、ライセンスが付与されているすべての製品が UDI によって表示されます。

ステップ 4 ライセンスを解除する ASA 仮想を確認し、[アクション (Actions)] > [削除 (Remove)] の順に選択して、ASA 仮想のリターンコードを [予約リターンコード (Reservation Return Code)] フィールドに入力します。

パーマネント ライセンスが使用可能なライセンスのプールに戻されます。

ステップ 5 [製品インスタンスの削除 (Remove Product Instance)] をクリックします。

ステップ 6 永続ライセンス予約を無効にするには、次の手順を行います。

a) 永続ライセンス予約を無効にするには、次のコマンドを実行します。

```
no license smart reservation
```

b) 次のコマンドを実行して、ライセンスの登録が解除されたことを確認します。

```
show license features
```

コマンド出力には、No active entitlement と表示されます。

ステップ 7 コマンドを実行して実行構成をスタートアップ構成に保存して、再起動中の構成の損失を避けます。

```
write memory
```

(オプション) ASA 仮想の登録解除（定期およびオンプレミス）

ASA 仮想の登録を解除すると、アカウントから ASA 仮想が削除され、ASA 仮想のすべてのライセンス資格と証明書が削除されます。登録を解除することで、ライセンスを新しい ASA 仮想に利用することもできます。あるいは、Smart Software Manager から ASA 仮想を削除できます。



(注) ASA 仮想を登録解除した場合、ASA 仮想をリロードすると重大なレート制限状態に戻ります。

手順

ASA 仮想 の登録を解除します。

license smart deregister

その後、ASA 仮想 がリロードされます。

(オプション) ASA 仮想 ID 証明書またはライセンス権限付与の更新 (定期およびオンプレミス)

デフォルトでは、アイデンティティ証明書は 6 ヶ月ごと、ライセンス資格は 30 日ごとに自動的に更新されます。インターネット アクセスの期間が限られている場合や、Smart Software Manager でライセンスを変更した場合などは、これらの登録を手動で更新することもできます。

手順

ステップ 1 アイデンティティ証明書を更新します。

license smart renew id

ステップ 2 Renew the license entitlement:

license smart renew auth

Firepower 4100/9300 : スマート ソフトウェア ライセンス の設定

この手順は、Smart Software Manager、Smart Software Manager オンプレミス、または永続ライセンス予約に適用されます。方法を前提条件として設定するには、『[FXOS configuration guide](#)』を参照してください。

永続ライセンス予約の場合、ライセンスはすべての機能、すなわちセキュリティ コンテキストが最大の標準ティアおよびキャリアライセンスを有効にします。ただし、Cisco ASA がこれらの機能を使用することを認識するためには、Cisco ASA でそれらを有効にする必要があります。

始める前に

ASA クラスタの場合は、設定作業のために制御ユニットにアクセスする必要があります。
Firewall Chassis Manager でどのユニットが制御ノードなのかを確認してください。この手順に示すように、ASA CLI から確認できます。

手順

- ステップ 1** Firepower 4100/9300 シャーシ CLI（コンソールまたは SSH）に接続し、次に ASA にセッション接続します。

connect module slot console connect asa

例：

```
Firepower> connect module 1 console
Firepower-module1> connect asa

asa>
```

次回 ASA コンソールに接続するときは、ASA に直接移動します。**connect asa** を再入力する必要はありません。

ASA クラスタの場合、ライセンス設定などの設定を行う場合にのみ、制御ユニットにアクセスする必要があります。通常、制御ユニットがスロット 1 にあるため、このモジュールにまず接続する必要があります。

- ステップ 2** ASA CLI で、グローバル コンフィギュレーション モードを入力します。論理デバイスの展開時に設定しない限り、デフォルトではイネーブルパスワードは空白ですが、**enable** コマンドを最初に入力したときに変更するように求められます。

enable configure terminal

例：

```
asa> enable
Password:
The enable password is not set. Please set it now.
Enter Password: *****
Repeat Password: *****
asa# configure terminal
asa(config)#
```

- ステップ 3** ASA クラスタの場合は、必要に応じて、このユニットが制御ユニットであることを確認します。

show cluster info

例：

```
asa(config)# show cluster info
Cluster stbu: On
```

```

This is "unit-1-1" in state SLAVE
  ID : 0
  Version : 9.5(2)
  Serial No.: P30000000025
  CCL IP : 127.2.1.1
  CCL MAC : 000b.fcf8.c192
  Last join : 17:08:59 UTC Sep 26 2015
  Last leave: N/A
Other members in the cluster:
  Unit "unit-1-2" in state SLAVE
    ID : 1
    Version : 9.5(2)
    Serial No.: P30000000001
    CCL IP : 127.2.1.2
    CCL MAC : 000b.fcf8.c162
    Last join : 19:13:11 UTC Sep 23 2015
    Last leave: N/A
  Unit "unit-1-3" in state MASTER
    ID : 2
    Version : 9.5(2)
    Serial No.: JAB0815R0JY
    CCL IP : 127.2.1.3
    CCL MAC : 000f.f775.541e
    Last join : 19:13:20 UTC Sep 23 2015
    Last leave: N/A

```

別のユニットが制御ユニットの場合は、接続を終了し、正しいユニットに接続します。接続の終了については、以下を参照してください。

ステップ 4 ライセンス スマート コンフィギュレーション モードを開始します。

license smart

例 :

```

ciscoasa(config)# license smart
ciscoasa(config-smart-lic)#

```

ステップ 5 機能層を設定します。

feature tier standard

使用できるのは標準層だけです。ティアライセンスは、他の機能ライセンスを追加するための前提条件です。アカウントに十分なティアライセンスが必要です。そうでないと、他の機能ライセンスまたはライセンスを必要とする機能を設定できません。

ステップ 6 次の機能の 1 つ以上をリクエストします。

- キャリア (GTP/GPRS、Diameter、および SCTP インспекション)

feature carrier

- セキュリティ コンテキスト

feature context <1-248>

永続ライセンスの予約では、最大コンテキスト (248) を指定できます。

- 強力な暗号化 (3DES/AES)

feature strong-encryption

Smart Software Manager から高度暗号化トークンを受け取った場合、このライセンスは必要ありません。ただし、スマートアカウントで高度暗号化が許可されていないものの、高度暗号化の使用が許可されているとシスコが判断した場合、高度暗号化ライセンスをアカウントに手動で追加できます。アクティブユニットのみがこのライセンスを要求し、ライセンスの集約により両方のユニットがこれを使用できます。

例：

```
ciscoasa(config-smart-lic)# feature carrier
ciscoasa(config-smart-lic)# feature context 50
```

ステップ 7 ASA コンソールを終了して Telnet アプリケーションに戻るには、プロンプトで「~」と入力します。スーパーバイザ CLI に戻るには、「quit」と入力します。

その他のモデル：スマートソフトウェアライセンスの設定

このセクションでは、次のモデル向けにスマートソフトウェアライセンスを構成する方法について説明します。

- Firepower 1010
- Firepower 1100
- Firepower 2100
- Cisco Secure Firewall 3100
- Cisco Secure Firewall 4200

次のいずれかの方法を選択します。

- [その他のモデル：定期スマートソフトウェアライセンスの設定（58 ページ）](#)
（任意）その他のモデル：Cisco ASA の登録解除（定期およびオンプレミス）（73 ページ）または（任意）その他のモデル：Cisco ASA ID 証明書またはソフトウェア利用資格の更新（定期およびオンプレミス）（73 ページ）も可能です。
- [その他のモデル：Smart Software Manager オンプレミスライセンスの設定（63 ページ）](#)
（任意）その他のモデル：Cisco ASA の登録解除（定期およびオンプレミス）（73 ページ）または（任意）その他のモデル：Cisco ASA ID 証明書またはソフトウェア利用資格の更新（定期およびオンプレミス）（73 ページ）も可能です。
- [その他のモデル：永続ライセンス予約の設定（68 ページ）](#)

その他のモデル：定期スマートソフトウェアライセンスングの設定

この手順は、Smart Software Manager を使用する ASA に適用されます。

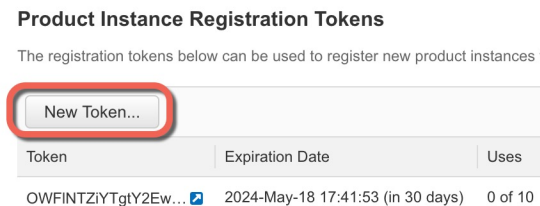
手順

ステップ 1 Cisco Smart Software Manager で、このデバイスを追加する仮想アカウントの登録トークンを要求してコピーします。

a) [Inventory] をクリックします。



b) [General] タブで、[New Token] をクリックします。



c) [登録トークンを作成（Create Registration Token）] ダイアログボックスで、以下の設定値を入力してから [トークンを作成（Create Token）] をクリックします。

?

×

Create Registration Token

This will create a token that is used to register product instances, so that they can use licenses from this virtual account. Once it's created, go to the Smart Licensing configuration for your products and enter the token, to register them with this virtual account.

Virtual Account: XXXXXXXXXX

Description:

* Expire After: Days

Between 1 - 365, 30 days recommended

Max. Number of Uses:

The token will be expired when either the expiration or the maximum uses is reached

☒ Allow export-controlled functionality on the products registered with this token ?

Create Token

Cancel

• 説明

• [有効期限（Expire After）]：推奨値は 30 日です。

- 最大使用回数（Max. Number of Uses）
- [このトークンに登録された製品で輸出管理機能を許可する（Allow export-controlled functionality on the products registered with this token）]：輸出コンプライアンス フラグを有効にします。

トークンはインベントリに追加されます。

- d) トークンの右側にある矢印アイコンをクリックして[トークン（Token）]ダイアログボックスを開き、トークン ID をクリップボードにコピーできるようにします。ASA の登録が必要なときに後の手順で使用するために、このトークンを準備しておきます。

図 11: トークンの表示

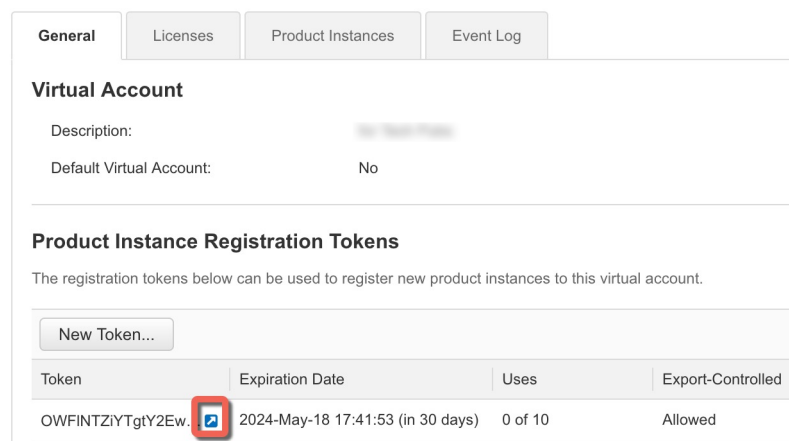
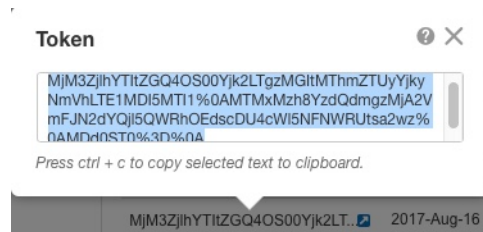


図 12: トークンのコピー



ステップ 2 （任意） Cisco ASA で、Smart Transport の HTTP プロキシ URL を指定します。

license smart

transport proxy proxy_server_ip port port

Smart Transport の代わりに Smart Call Home を使用するには、ステップ [ステップ 4](#)（62 ページ）を参照してください。

（注）

- 認証を使用する HTTP プロキシはサポートされません。
- プロキシサーバーの URL を設定する場合は、プロトコルを指定しないでください。

例：

```
ciscoasa(config)# license smart
ciscoasa(config-smart-lic)# transport proxy 10.1.1.1 port 10101
```

例：

```
ciscoasa(config)# license smart
ciscoasa(config-smart-lic)# transport proxy proxy.esl.cisco.com port 80
```

ステップ3 ASA でライセンス権限付与を要求します。

- a) ライセンス スマート コンフィギュレーション モードを開始します。

license smart

例：

```
ciscoasa(config)# license smart
ciscoasa(config-smart-lic)#
```

- b) (Firepower 1000/2100) 機能階層を設定します。

feature tier standard

使用できるのは標準 (Essentials) 層のみですが、設定で有効にする必要があります。階層ライセンスは、他の機能ライセンスを追加するための前提条件になります。Essentials ライセンスは、以前は標準ライセンスと呼ばれていました。「標準」は引き続き CLI で使用されています。Cisco Secure Firewall モデルの場合、Essentials ライセンスは常に有効であり、無効にすることはできません。

- c) (任意) (サポートされるモデル) セキュリティ コンテキストライセンスを要求します。

feature context number

デフォルトでは、Cisco ASA は 2 または 10 のコンテキストをサポートしているため、必要なコンテキストの数からデフォルトコンテキスト数を差し引いた数を要求する必要があります。コンテキストの最大数は、モデルによって異なります。

- Firepower 1120 : 5 コンテキスト
- Firepower 1140 : 10 コンテキスト
- Firepower 1150 : 25 コンテキスト
- Firepower 2110 : 25 コンテキスト
- Firepower 2120 : 25 コンテキスト
- Firepower 2130 : 30 コンテキスト
- Firepower 2140 : 40 コンテキスト
- Secure Firewall 3100 : 100 コンテキスト

- Cisco Secure Firewall 4200：250 コンテキスト

たとえば、Firepower 1150 で最大 25 のコンテキストを使用するには、コンテキストの数として 23 を入力します。この値は、デフォルトの 2 に追加されます。

例：

```
ciscoasa(config-smart-lic)# feature context 18
```

- d) (任意) (Firepower 1010) フェールオーバーを有効にするために Security Plus License を要求します。

feature security-plus

例：

```
ciscoasa(config-smart-lic)# feature security-plus
```

- e) (任意) (サポートされるモデル) Diameter、GTP/GPRS、SCTP 検査のキャリアライセンスを要求します。

feature carrier

例：

```
ciscoasa(config-smart-lic)# feature carrier
```

- f) (任意) 高度暗号化を有効にします。強力な暗号化トークンを受け取った場合は、このコマンドを入力しないでください。

feature strong-encryption

Smart Software Manager から高度暗号化トークンを受け取った場合、このライセンスは必要ありません。ただし、スマートアカウントで高度暗号化が許可されていないものの、高度暗号化の使用が許可されているとシスコが判断した場合、高度暗号化ライセンスをアカウントに手動で追加できます。アクティブユニットのみがこのライセンスを要求し、ライセンスの集約により両方のユニットがこれを使用できます。

(注)

このコマンドを入力すると、必要かどうかに関係なく、強力な暗号化ライセンスを使用します。そのため、そのライセンスがアカウントに登録されていない場合、アカウントはコンプライアンス違反の状態になります。強力な暗号化トークンを使用する際にこのライセンスは不要なため、何のメリットもなく、偶発的にアカウントをコンプライアンス違反の状態にしてしまう場合があります。

例：

```
ciscoasa(config-smart-lic)# feature strong-encryption
```

ステップ4 （任意）スマートライセンスサーバーとの通信には、デフォルトの Smart Transport の代わりに Smart Call Home を使用します。

Smart Transport の代わりに Smart Call Home を使用する必要があることがわかっている場合は、次の手順を実行します。それ以外の場合は、デフォルトの Smart Transport を使用する必要があります。

- a) 転送タイプを [Smart Call Home] に設定します。

license smart

transport type callhome

構成には、Smart Software Manager の URL を指定する **ライセンス** と呼ばれる Smart Call Home のプロファイルが含まれます。

```
call-home
  profile License
    destination address http
    https://tools.cisco.com/its/service/oddce/services/DDCEService
```

例：

```
ciscoasa(config)# license smart
ciscoasa(config-smart-lic)#transport type callhome
```

- b) （任意）HTTP プロキシの URL を指定します。

call-home

http-proxy ip_address port port

（注）

認証を使用する HTTP プロキシはサポートされません。

例：

```
ciscoasa(config)# call-home
ciscoasa(cfg-call-home)# http-proxy 10.1.1.1 port 443
```

ステップ5 手順1でコピーしたトークンを使用して ASA を登録します。

license smart register idtoken id_token

例：

```
ciscoasa# license smart register idtoken YjE3Njc5MzYtMGQzMj00OTA4
LWJhODItNzBhMGQ5NGRlYjUxLTEOMTQ5NDAY%0AODQzNz18NXk2bzV3SDE0ZkgwQk
dYRmZlNTNCNGlvRnBHUFpjcm02WTB4TU4w%0Ac2NnMD0%3D%0A
```

ASA が Smart Software Manager に登録され、設定されたライセンス権限付与の承認を要求します。Smart Software Manager は、ご使用のアカウントが許可すれば高度暗号化（3DES/AES）ラ

イセンスも適用します。ライセンスのステータスと使用状況をチェックするには、**show license summary** または **show running-config license** コマンドを使用します。

例：

```
ciscoasa# show license summary

Smart Licensing is ENABLED

Registration:
  Status: REGISTERED
  Smart Account: Biz1
  Virtual Account: IT
  Export-Controlled Functionality: Allowed
  Last Renewal Attempt: None
  Next Renewal Attempt: Mar 19 20:26:29 2018 UTC

License Authorization:
  Status: AUTHORIZED
  Last Communication Attempt: SUCCEEDED
  Next Communication Attempt: Oct 23 01:41:26 2017 UTC

License Usage:
  License                               Entitlement tag                Count Status
  -----
  regid.2014-08.com.ci... (FP1010-ASA-Std)          1 AUTHORIZED
```

例：

```
ciscoasa(config)# show running-config license
license smart
feature tier standard
throughput level 1G
transport proxy proxy.esl.cisco.com port 80
```

その他のモデル：Smart Software Manager オンプレミスライセンスの設定

この手順は、Smart Software Manager オンプレミスを使用する ASA に適用されます。

始める前に

- Smart Software Manager オンプレミス OVA ファイルを [Cisco.com](https://www.cisco.com) からダウンロードし、VMware ESXi サーバーにインストールして設定します。詳細については、『[Cisco Smart Software Manager On-Prem Data Sheet](#)』を参照してください。
- バージョン 7.0 では、Smart Transport が Smart Software Manager オンプレミスに追加されました。それよりも古いバージョンを使用している場合、次の手順に従って、Cisco ASA で Smart Call Home を有効にします。

- デバイスをエアギャップネットワークに配置する前に、クリプト CA トラストプールをダウンロードします。このトラストプールは通常、自動的にダウンロードされますが、エアギャップネットワークでは失効している可能性があります。

crypto ca trustpool import url http://www.cisco.com/security/pki/trs/ios_core.p7b

手順

ステップ 1 Smart Software Manager オンプレミスサーバーで登録トークンを要求します。

ステップ 2 (任意) Cisco ASA で、Smart Transport の HTTP プロキシ URL を指定します。

license smart

transport proxy proxy_server_ip port port

Smart Transport の代わりに Smart Call Home を使用するには、ステップ [ステップ 7 \(66 ページ\)](#) を参照してください。

(注)

認証を使用する HTTP プロキシはサポートされません。

例：

```
ciscoasa(config)# license smart
ciscoasa(config-smart-lic)# transport proxy 10.1.1.1 port 10101
```

ステップ 3 ライセンスサーバーの URL を変更して、Smart Software Manager オンプレミスに移動します。

license smart

transport url https://on-prem_ip_address/SmartTransport

Smart Transport の代わりに Smart Call Home を使用するには、ステップ [ステップ 7 \(66 ページ\)](#) を参照してください。

例：

```
ciscoasa(config)# license smart
ciscoasa(config-smart-lic)# transport url https://10.1.5.5/SmartTransport
```

ステップ 4 (任意)

ステップ 5

ステップ 6 ASA でライセンス権限付与を要求します。

a) ライセンス スマート コンフィギュレーション モードを開始します。

license smart

例：

```
ciscoasa(config)# license smart
```

```
ciscoasa(config-smart-lic)#
```

- b) (Firepower 1000/2100) 機能階層を設定します。

feature tier standard

使用できるのは標準 (Essentials) 層のみですが、設定で有効にする必要があります。階層ライセンスは、他の機能ライセンスを追加するための前提条件になります。Essentials ライセンスは、以前は標準ライセンスと呼ばれていました。「標準」は引き続き CLI で使用されています。Cisco Secure Firewall モデルの場合、Essentials ライセンスは常に有効であり、無効にすることはできません。

- c) (任意) (サポートされるモデル) セキュリティ コンテキスト ライセンスを要求します。

feature context number

デフォルトでは、Cisco ASA は 2 または 10 のコンテキストをサポートしているため、必要なコンテキストの数からデフォルトコンテキスト数を差し引いた数を要求する必要があります。コンテキストの最大数は、モデルによって異なります。

- Firepower 1120 : 5 コンテキスト
- Firepower 1140 : 10 コンテキスト
- Firepower 1150 : 25 コンテキスト
- Firepower 2110 : 25 コンテキスト
- Firepower 2120 : 25 コンテキスト
- Firepower 2130 : 30 コンテキスト
- Firepower 2140 : 40 コンテキスト
- Secure Firewall 3100 : 100 コンテキスト
- Cisco Secure Firewall 4200 : 250 コンテキスト

たとえば、Firepower 1150 で最大 25 のコンテキストを使用するには、コンテキストの数として 23 を入力します。この値は、デフォルトの 2 に追加されます。

例 :

```
ciscoasa(config-smart-lic)# feature context 18
```

- d) (任意) (Firepower 1010) フェールオーバーを有効にするために Security Plus License を要求します。

feature security-plus

例 :

```
ciscoasa(config-smart-lic)# feature security-plus
```

- e) (任意) (サポートされるモデル) Diameter、GTP/GPRS、SCTP 検査のキャリアライセンスを要求します。

feature carrier

例：

```
ciscoasa(config-smart-lic)# feature carrier
```

- f) (任意) 高度暗号化を有効にします。強力な暗号化トークンを受け取った場合は、このコマンドを入力しないでください。

feature strong-encryption

Smart Software Manager から高度暗号化トークンを受け取った場合、このライセンスは必要ありません。ただし、スマートアカウントで高度暗号化が許可されていないものの、高度暗号化の使用が許可されているとシスコが判断した場合、高度暗号化ライセンスをアカウントに手動で追加できます。アクティブユニットのみがこのライセンスを要求し、ライセンスの集約により両方のユニットがこれを使用できます。

(注)

このコマンドを入力すると、必要かどうかに関係なく、強力な暗号化ライセンスを使用します。そのため、そのライセンスがアカウントに登録されていない場合、アカウントはコンプライアンス違反の状態になります。強力な暗号化トークンを使用する際にこのライセンスは不要なため、何のメリットもなく、偶発的にアカウントをコンプライアンス違反の状態にしてしまう場合があります。

例：

```
ciscoasa(config-smart-lic)# feature strong-encryption
```

ステップ 7 (任意) スマートライセンスサーバーとの通信には、デフォルトの Smart Transport の代わりに Smart Call Home を使用します。

Smart Transport の代わりに Smart Call Home を使用する必要があることがわかっている場合は、次の手順を実行します。それ以外の場合は、デフォルトの Smart Transport を使用する必要があります。

- a) 転送タイプを [Smart Call Home] に設定します。

license smart

transport type callhome

構成には、Smart Software Manager の URL を指定する **ライセンス** と呼ばれる Smart Call Home のプロファイルが含まれます。

```
call-home
  profile License
    destination address http
    https://tools.cisco.com/its/service/oddce/services/DDCEService
```

例：

```
ciscoasa(config)# license smart
ciscoasa(config-smart-lic)#transport type callhome
```

- b) (任意) HTTP プロキシの URL を指定します。

call-home

http-proxy ip_address port port

(注)

認証を使用する HTTP プロキシはサポートされません。

例：

```
ciscoasa(config)# call-home
ciscoasa(cfg-call-home)# http-proxy 10.1.1.1 port 443
```

- c) ライセンスサーバーの URL を変更して、Smart Software Manager オンプレミスに移動します。

call-home

profile License

destination address http

https://on-prem_ip_address/Transportgateway/services/DeviceRequestHandler

例：

```
ciscoasa(config)# call-home
ciscoasa(cfg-call-home)# profile License
ciscoasa(cfg-call-home-profile)#destination address http
https://10.1.5.5/Transportgateway/services/DeviceRequestHandler
```

ステップ 8 手順 1 で要求したトークンを使用して ASA を登録します。

license smart register idtoken id_token

例：

```
ciscoasa# license smart register idtoken YjE3Njc5MzYtMGQzMj00OTA4
LWJhODItNzBhMGQ5NGRlYjUxLTE0MTQ5NDAY%0AODQzNz18NXk2bzV3SDE0ZkgwQk
dYRmZlNTNCNGlVnBHUFPjcm02WTB4TU4w%0Ac2NnMD0%3D%0A
```

ASA が Smart Software Manager オンプレミスサーバーに登録され、設定されたライセンス権限付与の承認を要求します。Smart Software Manager オンプレミスサーバーは、お使いのアカウントで許可すれば高度暗号化（3DES/AES）ライセンスも適用します。ライセンスのステータスと使用状況をチェックするには、**show license summary** コマンドを使用します。

例：

```
ciscoasa# show license summary
```

```

Smart Licensing is ENABLED

Registration:
  Status: REGISTERED
  Smart Account: Biz1
  Virtual Account: IT
  Export-Controlled Functionality: Allowed
  Last Renewal Attempt: None
  Next Renewal Attempt: Mar 19 20:26:29 2018 UTC

License Authorization:
  Status: AUTHORIZED
  Last Communication Attempt: SUCCEEDED
  Next Communication Attempt: Oct 23 01:41:26 2017 UTC

License Usage:
  License                               Entitlement tag                Count Status
  -----
  regid.2014-08.com.ci... (FP1010-ASA-Std)                1 AUTHORIZED

```

その他のモデル：永続ライセンス予約の設定

永続ライセンスを割り当てることができます。この項では、ASAを廃止する場合にライセンスを返す方法についても説明します。

手順

- ステップ 1 [1000/2100/3100/4200 永続ライセンスのインストール（68 ページ）](#)。
- ステップ 2 [（任意）その他のモデル：永続ライセンスの返却（72 ページ）](#)。

1000/2100/3100/4200 永続ライセンスのインストール

インターネットアクセスを持たない ASA の場合は、Smart Software Manager から永続ライセンスを要求できます。永続ライセンスでは、すべての機能が有効になります（セキュリティコンテキストが最大の Essentials ライセンス）。



- (注) 永続ライセンスの予約については、ASA を廃棄する前にライセンスを戻す必要があります。ライセンスを正式に戻さないと、ライセンスが使用中の状態のままになり、新しい ASA に再使用できません。[（任意）その他のモデル：永続ライセンスの返却（72 ページ）](#) を参照してください。

始める前に

永続ライセンスを購入すると、Smart Software Manager でそれらのライセンスを使用できます。すべてのアカウントが永続ライセンスの予約について承認されているわけではありません。設定を開始する前にこの機能についてシスコの承認があることを確認します。

手順

ステップ 1 ASA CLI で、永続ライセンスの予約を次のように有効にします。

license smart reservation

例 :

```
ciscoasa (config)# license smart reservation
ciscoasa (config)#
```

ステップ 2 Smart Software Manager に入力するライセンス コードを次のように要求します。

license smart reservation request universal

例 :

```
ciscoasa# license smart reservation request universal
Enter this request code in the Cisco Smart Software Manager portal:
BB-ZFPR-2140:JAD200802RR-AzKmHcc71-2A
ciscoasa#
```

このコマンドを再入力すると、リロード後にも同じコードが表示されます。このコードをまだ Smart Software Manager に入力していない場合、要求をキャンセルするには、以下を入力します。

license smart reservation cancel

パーマネントライセンスの予約をディセーブルにすると、保留中のすべての要求がキャンセルされます。すでに Smart Software Manager にコードを入力している場合は、その手順を完了して ASA にライセンスを適用する必要があります。その時点から、必要に応じてライセンスを戻すことが可能になります。 [（任意）その他のモデル：永続ライセンスの返却（72 ページ）](#) を参照してください。

ステップ 3 Smart Software Manager インベントリ画面に移動して、[Instances] タブをクリックします。

<https://software.cisco.com/#SmartLicensing-Inventory>

[Licenses] タブにアカウントに関連するすべての既存のライセンスが、標準およびパーマネントの両方とも表示されます。

ステップ 4 [License Reservation] をクリックして、ASA のコードをボックスに入力します。[Reserve License] をクリックします。

Smart Software Managerが承認コードを生成します。コードをダウンロードまたはクリップボードにコピーできます。この時点で、ライセンスは、Smart Software Managerに従って使用中です。

[License Reservation] ボタンが表示されない場合、お使いのアカウントはパーマネントライセンスの予約について承認されていません。この場合、パーマネントライセンスの予約を無効にして標準のスマートライセンス コマンドを再入力する必要があります。

ステップ 5 ASA で、承認コードを次のように入力します。

license smart reservation install code

例：

```
ciscoasa# license smart reservation install AAu3431rGRS00Ig5HQ12vpzg{MEYCIQCBw$
ciscoasa#
```

ステップ 6 ASA でライセンス権限付与を要求します。

(注)

永続ライセンスにより、すべてのライセンスを完全に使用できますが、ASAがライセンスを使用できることをASAが認識できるように、ASA設定で権限をオンにする必要があります。

a) ライセンス スマート コンフィギュレーション モードを開始します。

license smart

例：

```
ciscoasa(config)# license smart
ciscoasa(config-smart-lic)#
```

b) (Firepower 1000/2100) 機能階層を設定します。

feature tier standard

使用できるのは標準 (Essentials) 層のみですが、設定で有効にする必要があります。階層ライセンスは、他の機能ライセンスを追加するための前提条件になります。Essentialsライセンスは、以前は標準ライセンスと呼ばれていました。「標準」は引き続きCLIで使用されています。Cisco Secure Firewall モデルの場合、Essentialsライセンスは常に有効であり、無効にすることはできません。

c) (任意) (サポートされるモデル) セキュリティ コンテキストライセンスを要求します。

feature context number

デフォルトでは、Cisco ASAは2または10のコンテキストをサポートしているため、必要なコンテキストの数からデフォルトコンテキスト数を差し引いた数を要求する必要があります。コンテキストの最大数は、モデルによって異なります。

- Firepower 1120 : 5 コンテキスト
- Firepower 1140 : 10 コンテキスト

- Firepower 1150 : 25 コンテキスト
- Firepower 2110 : 25 コンテキスト
- Firepower 2120 : 25 コンテキスト
- Firepower 2130 : 30 コンテキスト
- Firepower 2140 : 40 コンテキスト
- Secure Firewall 3100 : 100 コンテキスト
- Cisco Secure Firewall 4200 : 250 コンテキスト

たとえば、Firepower 1150 で最大 25 のコンテキストを使用するには、コンテキストの数として 23 を入力します。この値は、デフォルトの 2 に追加されます。

例：

```
ciscoasa(config-smart-lic)# feature context 18
```

- d) (任意) (Firepower 1010) フェールオーバーを有効にするために Security Plus License を要求します。

feature security-plus

例：

```
ciscoasa(config-smart-lic)# feature security-plus
```

- e) (任意) (サポートされるモデル) Diameter、GTP/GPRS、SCTP 検査のキャリアライセンスを要求します。

feature carrier

例：

```
ciscoasa(config-smart-lic)# feature carrier
```

- f) (任意) 高度暗号化を有効にします。強力な暗号化トークンを受け取った場合は、このコマンドを入力しないでください。

feature strong-encryption

Smart Software Manager から高度暗号化トークンを受け取った場合、このライセンスは必要ありません。ただし、スマートアカウントで高度暗号化が許可されていないものの、高度暗号化の使用が許可されているとシスコが判断した場合、高度暗号化ライセンスをアカウントに手動で追加できます。アクティブユニットのみがこのライセンスを要求し、ライセンスの集約により両方のユニットがこれを使用できます。

(注)

このコマンドを入力すると、必要かどうかに関係なく、強力な暗号化ライセンスを使用します。そのため、そのライセンスがアカウントに登録されていない場合、アカウントはコンプライアンス違反の状態になります。強力な暗号化トークンを使用する際にこのライセンスは不要なため、何のメリットもなく、偶発的にアカウントをコンプライアンス違反の状態にしてしまう場合があります。

例：

```
ciscoasa(config-smart-lic)# feature strong-encryption
```

（任意）その他のモデル：永続ライセンスの返却

永続ライセンスが不要になった場合（ASAを廃止する場合など）は、この手順を使用して正式に Smart Software Manager にライセンスを返却する必要があります。すべての手順を実行しないと、ライセンスが使用中のままになり、他の場所で使用するために容易に解除できなくなります。

手順

ステップ 1 ASA で返却コードを次のように生成します。

license smart reservation return

例：

```
ciscoasa# license smart reservation return
Enter this return code in the Cisco Smart Software Manager portal:
Au3431rGRS00Ig5HQ12vpccg{uXiTRfVrp7M/zDpirLwYCaq8oSv60yZJuFDVBS2QliQ=
```

ただちに ASA のライセンスがなくなり、評価状態に移行します。このコードを再度表示する必要がある場合は、このコマンドを再入力します。新しい永続ライセンス（**license smart reservation request universal**）を要求すると、このコードを再表示できなくなることに注意してください。必ず、コードをキャプチャして、戻す作業を完了してください。評価期間が終了すると、ASA は期限切れ状態に移行します。コンプライアンス違反状態の詳細については、[コンプライアンス逸脱状態（93 ページ）](#)を参照してください。

ステップ 2 ASA ユニバーサル デバイス識別子（UDI）が表示されるので、Smart Software Manager で ASA インスタンスを見つけることができます。

show license udi

例：

```
ciscoasa# show license udi
UDI: PID:FPR-2140,SN:JAD200802RR
ciscoasa#
```

ステップ 3 Smart Software Manager インベントリ画面に移動して、[Product Instances] タブをクリックします。

<https://software.cisco.com/#SmartLicensing-Inventory>

[Product Instances] タブに、ライセンスが付与されているすべての製品が UDI によって表示されます。

ステップ 4 ライセンスを解除する ASA を確認し、[Actions] > [Remove] を選択して、ASA の返却コードをボックスに入力します。[Remove Product Instance] をクリックします。

パーマネント ライセンスが使用可能なライセンスのプールに戻されます。

(任意) その他のモデル：Cisco ASA の登録解除（定期およびオンプレミス）

ASA の登録を解除すると、アカウントから ASA が削除されます。ASA のすべてのライセンス権限付与と証明書が削除されます。登録を解除することで、ライセンスを新しい ASA に利用することもできます。あるいは、Smart Software Manager (SSM) から ASA を削除できます。この手順は、次のデバイスモデルに適用されます。

- Firepower 1000/2100
- /3100/4200

手順

ASA の登録解除：

`license smart deregister`

(任意) その他のモデル：Cisco ASA ID 証明書またはソフトウェア利用資格の更新（定期およびオンプレミス）

デフォルトでは、アイデンティティ証明書は 6 ヶ月ごと、ライセンス資格は 30 日ごとに自動的に更新されます。インターネット アクセスの期間が限られている場合や、Smart Software Manager でライセンスを変更した場合などは、これらの登録を手動で更新することもできます。

手順

ステップ 1 アイデンティティ証明書を更新します。

license smart renew id

ステップ 2 Renew the license entitlement:

license smart renew auth

モデルごとのライセンス

このセクションでは、ASAv および Firepower 4100/9300 シャーシASA セキュリティ モジュールに使用可能なライセンス資格を示します。

ASA 仮想

Cisco ASA の構成設定でスループットレベルを設定するには、**throughput level** コマンドを使用します。次のスループットレベルとライセンスの関係を参照してください。

- 100M : ASAv5
- 1G : ASAv10
- 2G : ASAv30
- 10G : ASAv50
- 20G : ASAv100

このスループットレベルにより、最大セキュアクライアント および TLS プロキシセッションも決定されます。ただし、ASA 仮想 メモリプロファイルを小さくすると、実際のセッション数が制限されるため、セッションを決定するには、スループットレベルと搭載されているメモリの両方を確認する必要があります。

使用中の ASA 仮想 のメモリにより、最大同時ファイアウォール接続数と VLAN が決定されます（スループットレベルによっては決定されません）。

次の表に、ASA 仮想 シリーズのライセンス機能を示します。

ライセンス	説明
権限付与ライセンス	

ライセンス	説明
スループット レベル	Cisco ASA 設定でスループットレベルを指定するには、throughput level コマンドを使用します。。このレベルにより、必要なライセンスが決定されます。 100M : ASAv5 1G : ASAv10 2G : ASAv30 10G : ASAv50 20G : ASAv100
ファイアウォール ライセンス	
Botnet Traffic Filter	イネーブル
ファイアウォールの接続、同時	ファイアウォール接続数は、ASA 仮想のメモリによって決定されます。 2 GB ~ 7.9 GB : 100,000 8 GB ~ 15.9 GB : 500,000 16 GB ~ 31.9 GB : 2,000,000 32 GB ~ 64 GB : 4,000,000
通信事業者	イネーブル

ライセンス	説明
Total TLS Proxy Sessions	TLS プロキシセッション数は、スループットレベルと ASA 仮想のメモリによって決定されます。 100M スループット + 任意のメモリ : 500 1G スループット + 任意のメモリ : 500 2G スループット : • 2 GB ~ 7.9 GB のメモリ : 500 • 8 GB 以上のメモリ : 1000 10G スループット : • 2 GB ~ 7.9 GB のメモリ : 500 • 8 GB ~ 15.9 GB のメモリ : 1000 • 16 GB 以上のメモリ : 10,000 20G スループット : • 2 GB ~ 7.9 GB のメモリ : 500 • 8 GB ~ 15.9 GB のメモリ : 1000 • 16 GB ~ 31.9 GB のメモリ : 10,000 • 32 GB 以上のメモリ : 20,000
VPN ライセンス	

ライセンス	説明	
セキュアクライアントピア	Unlicensed	セキュアクライアントピア数は、スループットレベルとASA 仮想のメモリによって決定されます。 オプションSecure Client AdvantageまたはSecure Client Premierライセンス、最大： 100M スループット+任意のメモリ：50 1G スループット+任意のメモリ：250 2G スループット： 2 GB ～ 7.9 GB のメモリ：250 8 GB 以上のメモリ：750 10G スループット： 2 GB ～ 7.9 GB のメモリ：250 8 GB ～ 15.9 GB のメモリ：750 16 GB 以上のメモリ：10,000 20G スループット： 2 GB ～ 7.9 GB のメモリ：250 8 GB ～ 15.9 GB のメモリ：750 16 GB ～ 31.9 GB：10,000 32 GB 以上のメモリ：20,000

ライセンス	説明
その他の VPN ピア	(注) その他の VPN ピアの数、スループットレベルと ASA 仮想のメモリによって決定されます。 100M スループット + 任意のメモリ : 50 1G スループット + 任意のメモリ : 250 2G スループット : • 2 GB ~ 7.9 GB のメモリ : 250 • 8 GB 以上のメモリ : 750 10G スループット : • 2 GB ~ 7.9 GB のメモリ : 250 • 8 GB ~ 15.9 GB のメモリ : 750 • 16 GB 以上のメモリ : 10,000 20G スループット : • 2 GB ~ 7.9 GB のメモリ : 250 • 8 GB ~ 15.9 GB のメモリ : 750 • 16 GB ~ 31.9 GB : 10,000 • 32 GB 以上のメモリ : 20,000

ライセンス	説明
合計VPNピア。全タイプの合計	(注) VPNピアの合計数は、スループットレベルとASA仮想のメモリによって決定されます。 100M スループット + 任意のメモリ : 50 1G スループット + 任意のメモリ : 250 2G スループット : • 2 GB ~ 7.9 GB のメモリ : 250 • 8 GB 以上のメモリ : 750 10G スループット : • 2 GB ~ 7.9 GB のメモリ : 250 • 8 GB ~ 15.9 GB のメモリ : 750 • 16 GB 以上のメモリ : 10,000 20G スループット : • 2 GB ~ 7.9 GB のメモリ : 250 • 8 GB ~ 15.9 GB のメモリ : 750 • 16 GB ~ 31.9 GB : 10,000 • 32 GB 以上のメモリ : 20,000
一般ライセンス	
暗号化	アカウントのエクスポートコンプライアンス設定によって、Base (DES) または Strong (3DES/AES)
フェールオーバー	アクティブ/スタンバイ
セキュリティ コンテキスト	サポートなし
クラスタ	有効
VLAN、最大	VLAN 数は、ASA 仮想のメモリによって決定されます。 2 GB ~ 7.9 GB : 50 8 GB ~ 15.9 GB : 200 16 GB ~ 31.9 GB : 1,024 32 GB ~ 64 GB : 1,024

Firepower 1010

次の表に、Firepower 1010 のライセンス機能を示します。

ライセンス	Essentials ライセンス	
ファイアウォール ライセンス		
Botnet Traffic Filter	サポートなし。	
ファイアウォールの接続、同時	100,000	
通信事業者	サポートしないSCTP インспекション マップはサポートされていませんが、ACL を使用した SCTP ステートフルインспекションがサポートされています。	
合計 TLS プロキシセッション	4,000	
VPN ライセンス		
セキュアクライアントピア	Unlicensed	オプションSecure Client Advantage、Secure Client PremierまたはSecure Client VPNのみライセンス、最大：75
その他の VPN ピア	75	
合計 VPN ピア。全タイプの合計	75	
一般ライセンス		
暗号化	アカウントのエクスポート コンプライアンス設定によって、Base（DES）または Strong（3DES/AES）	
Security Plus（フェールオーバー、VPN ロードバランシング）	ディセーブル	オプション
セキュリティ コンテキスト	サポートしない	
クラスタ	サポートしない	
VLAN、最大	60	

Firepower 1100 シリーズ

次の表に、Firepower 1100 シリーズのライセンス機能を示します。

ライセンス	Essentials ライセンス	
ファイアウォール ライセンス		
Botnet Traffic Filter	サポートなし。	
ファイアウォールの接続、同時	Firepower 1120 : 200,000 Firepower 1140 : 400,000 Firepower 1150 : 600,000	
通信事業者	サポートしないSCTP インスペクション マップはサポートされていませんが、ACL を使用した SCTP ステートフルインスペクションがサポートされています。	
合計 TLS プロキシセッション	Firepower 1120 : 4,000 Firepower 1140 : 8,000 Firepower 1150 : 8,000	
VPN ライセンス		
セキュアクライアントピア	Unlicensed	オプションSecure Client Advantage、Secure Client Premier、またはSecure Client VPN のみライセンス、最大： Firepower 1120 : 150 Firepower 1140 : 400 Firepower 1150 : 800
その他の VPN ピア	Firepower 1120 : 150 Firepower 1140 : 400 Firepower 1150 : 800	
合計 VPN ピア。全タイプの合計	Firepower 1120 : 150 Firepower 1140 : 400 Firepower 1150 : 800	
一般ライセンス		
暗号化	アカウントのエクスポート コンプライアンス設定によって、Base (DES) または Strong (3DES/AES)	

ライセンス	Essentials ライセンス	
セキュリティ コンテキスト	2	オプションライセンス、最大： <i>Firepower 1120 : 5</i> <i>Firepower 1140 : 10</i> <i>Firepower 1150 : 25</i>
クラスター	サポートしない	
VLAN、最大	1024	

Firepower 2100 シリーズ

次の表に、Firepower 2100 シリーズのライセンス機能を示します。

ライセンス	Essentials ライセンス
ファイアウォール ライセンス	
Botnet Traffic Filter	サポートなし。
ファイアウォールの接続、同時	Firepower 2110 : 1,000,000 Firepower 2120 : 1,500,000 Firepower 2130 : 2,000,000 Firepower 2140 : 3,000,000
通信事業者	サポートしないSCTP インспекション マップはサポートされていませんが、ACL を使用した SCTP ステートフル インспекションがサポートされています。
合計 TLS プロキシセッション	Firepower 2110 : 4,000 Firepower 2120 : 8,000 Firepower 2130 : 8,000 Firepower 2140 : 10,000
VPN ライセンス	

ライセンス	Essentials ライセンス	
セキュアクライアントピア	Unlicensed	オプション <i>Secure Client Advantage</i> 、 <i>Secure Client Premier</i> 、または <i>Secure Client VPN</i> のみライセンス、最大： <i>Firepower 2110</i> ：1,500 <i>Firepower 2120</i> ：3,500 <i>Firepower 2130</i> ：7,500 <i>Firepower 2140</i> ：10,000
その他の VPN ピア	<i>Firepower 2110</i> ：1,500 <i>Firepower 2120</i> ：3,500 <i>Firepower 2130</i> ：7,500 <i>Firepower 2140</i> ：10,000	
合計 VPN ピア。全タイプの合計	<i>Firepower 2110</i> ：1,500 <i>Firepower 2120</i> ：3,500 <i>Firepower 2130</i> ：7,500 <i>Firepower 2140</i> ：10,000	
一般ライセンス		
暗号化	アカウントのエクスポート コンプライアンス設定によって、Base（DES）または Strong（3DES/AES）	
セキュリティ コンテキスト	2	オプションライセンス、最大： <i>Firepower 2110</i> ：25 <i>Firepower 2120</i> ：25 <i>Firepower 2130</i> ：30 <i>Firepower 2140</i> ：40
クラスタ	サポートしない	
VLAN、最大	1024	

Secure Firewall 3100 シリーズ

次の表に、Secure Firewall 3100 シリーズのライセンス機能を示します。

ライセンス	Essentials ライセンス	
ファイアウォール ライセンス		
Botnet Traffic Filter	サポートなし。	
ファイアウォールの接続、同時	Cisco Secure Firewall 3105 : 2,000,000 Cisco Secure Firewall 3110 : 2,000,000 Cisco Secure Firewall 3120 : 4,000,000 Cisco Secure Firewall 3130 : 6,000,000 Cisco Secure Firewall 3140 : 10,000,000	
通信事業者	ディセーブル	オプション ライセンス : 通信事業者
合計 TLS プロキシセッション	Cisco Secure Firewall 3105 : 10,000 Cisco Secure Firewall 3110 : 10,000 Cisco Secure Firewall 3120 : 15,000 Cisco Secure Firewall 3130 : 15,000 Cisco Secure Firewall 3140 : 15,000	
VPN ライセンス		
セキュアクライアントピア	Unlicensed	オプションSecure Client Advantage、Secure Client Premier、またはSecure Client VPN のみライセンス、最大 : Cisco Secure Firewall 3105 : 3,000 Cisco Secure Firewall 3110 : 3,000 Cisco Secure Firewall 3120 : 7,000 Cisco Secure Firewall 3130 : 15,000 Cisco Secure Firewall 3140 : 20,000

ライセンス	Essentials ライセンス	
その他の VPN ピア	Cisco Secure Firewall 3105 : 3,000 Cisco Secure Firewall 3110 : 3,000 Cisco Secure Firewall 3120 : 7,000 Cisco Secure Firewall 3130 : 15,000 Cisco Secure Firewall 3140 : 20,000	
合計 VPN ピア。全タイプの合計	Cisco Secure Firewall 3105 : 3,000 Cisco Secure Firewall 3110 : 3,000 Cisco Secure Firewall 3120 : 7,000 Cisco Secure Firewall 3130 : 15,000 Cisco Secure Firewall 3140 : 20,000	
一般ライセンス		
暗号化	アカウントのエクスポート コンプライアンス設定によって、Base (DES) または Strong (3DES/AES)	
セキュリティ コンテキスト	2	オプションライセンス、最大 : 100
クラスタ	イネーブル	
VLAN、最大	1024	

Firepower 4100

次の表に、Firepower 4100 のライセンス機能を示します。

ライセンス	Essentials ライセンス	
ファイアウォール ライセンス		
Botnet Traffic Filter	サポートなし。	
ファイアウォールの接続、同時	Firepower 4112 : 10,000,000	
	Firepower 4115 : 15,000,000	
	Firepower 4125 : 25,000,000	
	Firepower 4145 : 40,000,000	
通信事業者	ディセーブル	オプション ライセンス : 通信事業者

ライセンス	Essentials ライセンス	
合計 TLS プロキシセッション	15,000	
VPN ライセンス		
セキュアクライアントピア	Unlicensed	オプションSecure Client Advantage、Secure Client Premier、またはSecure Client VPN のみライセンス： Firepower 4112：10,000 Firepower 4115：15,000 Firepower 4125：20,000 Firepower 4145：20,000
その他の VPN ピア	Firepower 4112：10,000 Firepower 4115：15,000 Firepower 4125：20,000 Firepower 4145：20,000	
合計 VPN ピア。全タイプの合計	Firepower 4112：10,000 Firepower 4115：15,000 Firepower 4125：20,000 Firepower 4145：20,000	
一般ライセンス		
暗号化	アカウントのエクスポート コンプライアンス設定によって、Base（DES）または Strong（3DES/AES）	
セキュリティ コンテキスト	10	オプションライセンス：最大 250
クラスタ	イネーブル	
VLAN、最大	1024	

Cisco Secure Firewall 4200 シリーズ

次の表に、Secure Firewall 4200 シリーズのライセンス機能を示します。

ライセンス	Essentials ライセンス	
ファイアウォール ライセンス		
Botnet Traffic Filter	サポートなし。	
ファイアウォールの接続、同時	Cisco Secure Firewall 4215 : 40,000,000 Cisco Secure Firewall 4225 : 80,000,000 Cisco Secure Firewall 4245 : 80,000,000	
通信事業者	ディセーブル	オプション ライセンス : 通信事業者
合計 TLS プロキシセッション	15,000	
VPN ライセンス		
セキュアクライアントピア	Unlicensed	オプション <i>Secure Client Advantage</i> 、 <i>Secure Client Premier</i> 、または <i>Secure Client VPN</i> のみライセンス、最大 : <i>Cisco Secure Firewall 4215 : 20,000</i> <i>Cisco Secure Firewall 4225 : 25,000</i> <i>Cisco Secure Firewall 4245 : 30,000</i>
その他の VPN ピア	Cisco Secure Firewall 4215 : 20,000 Cisco Secure Firewall 4225 : 25,000 Cisco Secure Firewall 4245 : 30,000	
合計 VPN ピア。全タイプの合計	Cisco Secure Firewall 4215 : 20,000 Cisco Secure Firewall 4225 : 25,000 Cisco Secure Firewall 4245 : 30,000	
一般ライセンス		
暗号化	アカウントのエクスポート コンプライアンス設定によって、Base (DES) または Strong (3DES/AES)	
セキュリティ コンテキスト	10	オプションライセンス、最大 : 250
クラスタ	イネーブル	

ライセンス	Essentials ライセンス
VLAN、最大	1024

Firepower 9300

次の表に、Firepower 9300 のライセンス機能を示します。

ライセンス	Essentials ライセンス	
ファイアウォール ライセンス		
Botnet Traffic Filter	サポートなし。	
ファイアウォールの接続、同時	Firepower 9300 SM-56 : 60,000,000 Firepower 9300 SM-48 : 60,000,000 Firepower 9300 SM-40 : 55,000,000	
キャリア	無効	オプション ライセンス : 通信事業者
合計 TLS プロキシセッション	15,000	
VPN ライセンス		
セキュアクライアントピア	Unlicensed	オプションSecure Client Advantage、Secure Client Premier、Secure Client VPN のみライセンス : 最大 20,000
その他の VPN ピア	20,000	
合計 VPN ピア。全タイプの合計	20,000	
一般ライセンス		
暗号化	アカウントのエクスポート コンプライアンス設定によって、Base (DES) または Strong (3DES/AES)	
セキュリティ コンテキスト	10	オプションライセンス : 最大 250
クラスタ	イネーブル	
VLAN、最大	1024	

スマート ソフトウェア ライセンシングのモニタリング

デバッグメッセージをイネーブルにするだけでなく、ライセンスの機能、ステータス、および証明書をモニターすることもできます。

現在のライセンスの表示

ライセンスを表示するには、次の コマンドを参照してください。

- **show license features**

次に、Essentialsライセンスのみがある Cisco ASA の例を示します。

```
ciscoasa# show license features
Serial Number: JAD254312UA
Export Compliant: YES

License mode: Smart Licensing

Licensed features for this platform:
Maximum Physical Interfaces      : Unlimited
Maximum VLANs                   : 512
Inside Hosts                    : Unlimited
Failover                        : Active/Active
Encryption-DES                  : Enabled
Encryption-3DES-AES             : Enabled
Security Contexts               : 2
Carrier                         : Disabled
AnyConnect Premium Peers        : 150
AnyConnect Essentials           : Disabled
Other VPN Peers                 : 150
Total VPN Peers                 : 150
AnyConnect for Mobile           : Enabled
AnyConnect for Cisco VPN Phone  : Enabled
Advanced Endpoint Assessment    : Enabled
Shared License                  : Disabled
Total TLS Proxy Sessions        : 320
Cluster                         : Disabled
```

スマート ライセンス ステータスの表示

ライセンス ステータスを表示するには、次のコマンドを参照してください。

- **すべてのライセンスの表示**

スマート ソフトウェア ライセンシング、スマート エージェントのバージョン、UDI 情報、スマート エージェントの状態、グローバルコンプライアンスステータス、資格ステータス、使用許可証明書情報および予定のスマート エージェント タスクを表示します。

次の例は、ASA 仮想 ライセンスを示しています。

```
ciscoasa# show license all
Smart Licensing Status
```

```

=====

Smart Licensing is ENABLED

Registration:
  Status: REGISTERED
  Smart Account: ASA
  Virtual Account: ASAv Internal Users
  Export-Controlled Functionality: Not Allowed
  Initial Registration: SUCCEEDED on Sep 21 20:26:29 2015 UTC
  Last Renewal Attempt: None
  Next Renewal Attempt: Mar 19 20:26:28 2016 UTC
  Registration Expires: Sep 20 20:23:25 2016 UTC

License Authorization:
  Status: AUTHORIZED on Sep 21 21:17:35 2015 UTC
  Last Communication Attempt: SUCCEEDED on Sep 21 21:17:35 2015 UTC
  Next Communication Attempt: Sep 24 00:44:10 2015 UTC
  Communication Deadline: Dec 20 21:14:33 2015 UTC

License Usage
=====

regid.2014-08-com.cisco.ASAv-STD-1G,1.0_4fd3bdbd-29ae-4cce-ad82-45ad3db1070c
(ASAv-STD-1G):
  Description: This entitlement tag was created via Alpha Extension application
  Count: 1
  Version: 1.0
  Status: AUTHORIZED

Product Information
=====
UDI: PID:ASAv,SN:9AHV3KJBEKE

Agent Version
=====
Smart Agent for Licensing: 1.6_reservation/36

```

• show license status

スマートライセンスのステータスを表示します。

次に、通常のスマートソフトウェアライセンシングを使用するASA仮想のステータスの例を示します。

```

ciscoasa# show license status

Smart Licensing is ENABLED

Registration:
  Status: REGISTERED
  Smart Account: ASA
  Virtual Account: ASAv Internal Users
  Export-Controlled Functionality: Not Allowed
  Initial Registration: SUCCEEDED on Sep 21 20:26:29 2015 UTC
  Last Renewal Attempt: None
  Next Renewal Attempt: Mar 19 20:26:28 2016 UTC
  Registration Expires: Sep 20 20:23:25 2016 UTC

License Authorization:
  Status: AUTHORIZED on Sep 23 01:41:26 2015 UTC
  Last Communication Attempt: SUCCEEDED on Sep 23 01:41:26 2015 UTC

```

```
Next Communication Attempt: Oct 23 01:41:26 2015 UTC
Communication Deadline: Dec 22 01:38:25 2015 UTC
```

次に、永続ライセンス予約を使用する ASA 仮想 のステータスの例を示します。

```
ciscoasa# show license status

Smart Licensing is ENABLED
License Reservation is ENABLED

Registration:
  Status: REGISTERED - UNIVERSAL LICENSE RESERVATION
  Export-Controlled Functionality: Allowed
  Initial Registration: SUCCEEDED on Jan 28 16:42:45 2016 UTC

License Authorization:
  Status: AUTHORIZED - RESERVED on Jan 28 16:42:45 2016 UTC

Licensing HA configuration error:
  No Reservation Ha config error
```

• show license summary

スマート ライセンスのステータスと使用量のサマリーを表示します。

次に、通常のスマート ソフトウェア ライセンシングを使用する ASA 仮想 のサマリーの例を示します。

```
ciscoasa# show license summary

Smart Licensing is ENABLED

Registration:
  Status: REGISTERED
  Smart Account: ASA
  Virtual Account: ASAv Internal Users
  Export-Controlled Functionality: Not Allowed
  Last Renewal Attempt: None
  Next Renewal Attempt: Mar 19 20:26:29 2016 UTC

License Authorization:
  Status: AUTHORIZED
  Last Communication Attempt: SUCCEEDED
  Next Communication Attempt: Oct 23 01:41:26 2015 UTC

License Usage:
  License                               Entitlement tag                Count Status
  -----
  regid.2014-08.com.ci... (ASAv-STD-1G)                1 AUTHORIZED
```

次に、永続ライセンス予約を使用する ASA 仮想 のサマリーの例を示します。

```
ciscoasa# show license summary

Smart Licensing is ENABLED

Registration:
  Status: REGISTERED - UNIVERSAL LICENSE RESERVATION
  Export-Controlled Functionality: Allowed
```

```
License Authorization:
  Status: AUTHORIZED - RESERVED
```

- **show license usage**

スマート ライセンスの使用量を表示します。

次に、ASA 仮想 の使用状況の例を示します。

```
ciscoasa# show license usage

License Authorization:
  Status: AUTHORIZED on Sep 23 01:41:26 2015 UTC

regid.2014-08.com.cisco.ASAv-STD-1G,1.0_4fd3bdbd-29ae-4cce-ad82-45ad3db1070c
(ASAv-STD-1G):
  Description: This entitlement tag was created via Alpha Extension application
  Count: 1
  Version: 1.0
  Status: AUTHORIZED
```

UDI の表示

ユニバーサル製品識別子（UDI）を表示するには、次のコマンドを参照してください。

- **show license udi**

次に、ASAv の UDI の例を示します。

```
ciscoasa# show license udi
UDI: PID:ASAv,SN:9AHV3KJBEKE
ciscoasa#
```

スマート ソフトウェア ライセンスのデバッグ

クラスタリングのデバッグについては、次のコマンドを参照してください。

- **debug license agent {error | trace | debug | all}**

スマート エージェントからのデバッグをオンにします。

- **debug license level**

Smart Software Licensing Manager のデバッグの各種レベルをオンにします。

Smart Software Manager 通信

このセクションでは、デバイスが Smart Software Manager と通信する方法について説明します。

デバイス登録とトークン

各仮想アカウントに対し、登録トークンを作成できます。このトークンは、デフォルトで 30 日間有効です。各デバイスを導入するとき、または既存のデバイスを登録するときにこのトークン ID と権限付与レベルを入力します。既存のトークンの有効期限が切れている場合は、新しいトークンを作成できます。



(注) Firepower 4100/9300 シャーシ：デバイス登録は、ASA 論理デバイス上ではなく、シャーシで設定されます。

展開後の起動時、または既存のデバイスでこれらのパラメータを手動で設定した後、デバイスは Smart Software Manager に登録されます。トークンを使用してデバイスを登録すると、Smart Software Manager はデバイスと Smart Software Manager 間の通信用の ID 証明書を発行します。この証明書の有効期間は 1 年ですが、6 か月ごとに更新されます。

Smart Software Manager との定期的な通信

デバイスは、30 日ごとに Smart Software Manager と通信します。Smart Software Manager に変更を加えた場合は、デバイス上で許可を更新し、すぐに変更されるようにすることができます。または、スケジュールどおりにデバイスが通信するのを待ちます。

必要に応じて、HTTP プロキシを設定できます。

ASA 仮想

ASA 仮想では、少なくとも 90 日おきに、直接接続または HTTP プロキシを介したインターネットアクセスが必要です。通常のライセンス通信が 30 日ごとに行われますが、猶予期間によって、デバイスは Call Home なしで最大 90 日間遵守が維持されます。猶予期間終了後は、Smart Software Manager に連絡する必要があるため、そうしないと ASA 仮想がコンプライアンス違反の状態になります。その他の操作には影響ありません。

他のすべてのモデル

Cisco ASA は直接または HTTP プロキシ経由で少なくとも 90 日ごとにインターネットアクセスを行う必要があります。通常のライセンス通信が 30 日ごとに行われますが、猶予期間によって、デバイスは Call Home なしで最大 90 日間動作します。猶予期間後、Smart Software Manager に連絡しない限り、特別なライセンスを必要とする機能の設定変更を行えませんが、動作には影響ありません。

コンプライアンス逸脱状態

次の状況では、デバイスがコンプライアンスから逸脱している可能性があります。

- 使用超過：デバイスが利用できないライセンスを使用している場合。

- ライセンスの有効期限切れ：時間ベースのライセンスの有効期限が切れている場合。
- 通信の欠落：デバイスが再許可を得るために Licensing Authority に到達できない場合。

アカウントのステータスがコンプライアンス違反状態なのか、違反状態に近づいているのかを確認するには、デバイスで現在使用中の権限付与とスマートアカウントのものを比較する必要があります。

コンプライアンス違反状態では、モデルによってはデバイスが制限されている可能性があります。

- ASA 仮想：ASA 仮想 は影響を受けません。
- すべての他のモデル：特別なライセンスが必要な機能への設定変更はできなくなりますが、動作には影響ありません。たとえば、Essentialsのライセンス制限を超える既存のコンテキストは実行を継続でき、その構成を変更することもできますが、新しいコンテキストを追加することはできません。最初の登録時に十分なEssentialsライセンスがない場合、高度な暗号化機能を含むライセンス機能を設定できません。

Smart Call Home インフラストラクチャ

デフォルトでは、Smart Call Home のプロファイルは、Smart Software Manager の URL を指定する設定内にあります。このプロファイルは削除できません。ライセンスプロファイルの設定可能なオプションは、Smart Software Manager の宛先アドレス URL のみであることに注意してください。Cisco TAC に指示されない限り、Smart Software Manager の URL は変更しないでください。



(注) Firepower 4100/9300 シャーシの場合、ライセンスの Smart Call Home は ASA ではなく Firepower 4100/9300 シャーシ スーパーバイザで設定されます。

スマートソフトウェアライセンスの Smart Call Home をディセーブルにすることはできません。たとえば、**no service call-home** コマンドを使用して Smart Call Home を無効化しても、スマートソフトウェアライセンシングは無効化されません。

他の Smart Call Home の機能は、特に設定しない限り、有効になりません。

スマートライセンス証明書の管理

Cisco ASA はスマート転送または Smart Call Home サーバー証明書を発行した CA の証明書を含むトラストポイントを自動的に作成します。サーバー証明書を発行する階層が変更される場合、サービスの中断を防ぐため、定期的な **trustpool** バンドルの自動更新が有効になるように、**auto-update** コマンドを構成します。

スマートライセンスサーバーから受信したサーバー証明書は、[Extended Key Usage] フィールドに「ServAuth」が含まれていなければなりません。このチェックは、自己署名証明書以外の証明書にのみ実行されます。自己署名証明書の場合、このフィールドに値は表示されません。



(注) 1年以上ライセンス登録が期限切れのデバイスをリロードすると、輸出規制対象の機能が無効になります。IPSec 暗号化が有効になっている場合、VPN のダウンタイムやフェールオーバーのスプリットブレイクシナリオなどの重大な問題が発生する可能性があります。

スマートソフトウェアライセンスの履歴

機能名	プラットフォームリリース	説明
Smart Transport は、CSSM サーバーと通信するためのデフォルトのトランスポートメカニズムです	9.20(4)/9.22(1)	スマートライセンスでは現在、デフォルトの転送として Smart Transport を使用しています。必要に応じて、旧タイプの Smart Call Home を任意で有効にできます。 新規/変更されたコマンド： transport proxy 、 transport type 、 transport url
Secure Firewall 4200 の最大接続数の引き上げ	9.20(2)	最大接続数が引き上げられました。 • 4215 : 15M → 40M • 4225 : 30M → 80M • 4245 : 60M → 80M
キャリアライセンスの Secure Firewall 3100 サポート	9.18(1)	キャリアライセンスは、Diameter、GTP/GPRS、SCTP 検査を有効にします。 新規/変更されたコマンド： feature carrier
ASAv100 永続ライセンス予約	9.14(1.30)	ASAv100 で製品 ID L-ASAV100SR-K9= を使用した永続ライセンス予約がサポートされるようになりました。 注 ：すべてのアカウントが永続ライセンス予約について承認されているわけではありません。

機能名	プラットフォームリリース	説明
ASA 仮想 MSLA サポート	9.13(1)	ASA 仮想 は、シスコのマネージドサービス ライセンス契約 (MSLA) プログラムをサポートしています。このプログラムは、マネージドソフトウェア サービスをサードパーティに提供するシスコのお客様およびパートナー向けに設計された、ソフトウェアのライセンスおよび消費のフレームワークです。 MSLAはスマートライセンスの新しい形式で、ライセンス スマート エージェントは時間単位でライセンス権限付与の使用状況を追跡します。 新規/変更されたコマンド：license smart、mode、utility、custom-id、custom-info、privacy、transport type、transport url、transport proxy
ASA 仮想 柔軟なライセンス	9.13(1)	すべての ASA 仮想 ライセンスは、サポートされているすべての ASA 仮想 vCPU/メモリ構成で使えるようになりました。セキュアクライアント および TLS プロキシのセッション制限は、モデルタイプに関連付けられたプラットフォーム制限ではなく、インストールされた ASA 仮想 プラットフォームの権限付与によって決まります。 新規/変更されたコマンド：show version、show vm、show cpu、show license features
Firepower 4100/9300 シャーシのフェールオーバー ペアのライセンスの変更	9.7(1)	アクティブなユニットのみがライセンス権限を要求します。以前は、両方のユニットがライセンスの権限付与を要求していました。FXOS 2.1.1 でサポートされます。
ASA 仮想 の短い文字列の拡張機能向けの永続ライセンス予約	9.6(2)	スマート エージェント (1.6.4 への) の更新により、要求と認証コードには短い文字列が使用されます。 変更されたコマンドはありません。
ASA 仮想 のサテライトサーバーのサポート	9.6(2)	デバイスがセキュリティ上の理由でインターネットにアクセスができない場合、オプションで、仮想マシン (VM) としてローカル Smart Software Manager サテライト サーバーをインストールできます。 変更されたコマンドはありません。

機能名	プラットフォームリリース	説明
Firepower 4100/9300 シャーシ 上の ASA の永続ライセンス予約	9.6(2)	Cisco Smart Software Manager との通信が許可されていない非常にセキュアな環境では、FirePOWER 9300 および FirePOWER 4100 の ASA 用に永続ライセンスを要求できます。永続ライセンスには、標準層、高度暗号化（該当する場合）、セキュリティ コンテキスト、キャリア ライセンスをはじめ、使用可能なすべてのライセンス権限が含まれます。FXOS 2.0.1 が必要です。 すべての設定はFirepower 4100/9300 シャーシで実行され、ASA の設定は不要です。
ASA 仮想 の永続ライセンス予約	9.5(2.200) 9.6(2)	Cisco Smart Software Manager との通信が許可されていない非常にセキュアな環境では、ASA 仮想 用に永続ライセンスを要求できます。9.6(2) では、Amazon Web Services の ASA 仮想 向けに、この機能のサポートが追加されました。この機能はMicrosoft Azure ではサポートされません。 次のコマンドが導入されました。license smart reservation、license smart reservation cancel、license smart reservation install、license smart reservation request universal、license smart reservation return
スマートエージェントのv1.6へのアップグレード	9.5(2.200) 9.6(2)	スマート エージェントはバージョン 1.1 からバージョン 1.6 へアップグレードされました。このアップグレードは永続ライセンス予約をサポートするほか、ライセンス アカウントに設定された権限に従って、高度暗号化（3DES/AES）ライセンス権限の設定もサポートします。 （注） バージョン 9.5 （2.200）からダウングレードした場合、ASA 仮想 はライセンス登録状態を保持しません。license smart register idtoken id_token force コマンドを使用し、再登録する必要があります。Smart Software Manager から ID トークンを取得します。 次のコマンドが導入されました。show license status、show license summary、show license udi、show license usage 次のコマンドが変更されました。show license all、show tech-support license 次のコマンドが非推奨になりました。show license cert、show license entitlement、show license pool、show license registration

機能名	プラットフォームリリース	説明
FirePOWER 9300 の ASA に高度暗号化 (3DES) ライセンスを自動的に適用	9.5(2.1)	通常の Cisco Smart Software Manager (SSM) ユーザーの場合、FirePOWER 9300 で登録トークンを適用すると、対象となるお客様には強力な暗号化ライセンスが自動的に有効になります。 (注) スマートソフトウェアマネージャサテライトが導入されている場合、ASDM や他の高度暗号機能を使用するには、ASA の展開後に ASA CLI を使用して、高度暗号化ライセンスを有効にする必要があります。 この機能には、FXOS 1.1.3 が必要です。 サテライト以外の構成では、次のコマンドが除去されました。 feature strong-encryption
サーバー証明書の発行階層が変更された場合の Smart Call Home/スマート ライセンス証明書の検証	9.5(2)	スマートライセンスでは、Smart Call Home インフラストラクチャが使用されます。ASA はバックグラウンドで Smart Call Home 匿名レポートを最初に設定するときに、Call Home サーバー証明書を発行した CA の証明書を含むトラストポイントを自動的に作成します。ASA はサーバー証明書の発行階層が変更された場合の証明書の検証をサポートします。トラストプールバンドルの定期的な自動更新を有効にできます。 次のコマンドが導入されました。auto-import
新しいキャリア ライセンス	9.5(2)	新しいキャリア ライセンスは既存の GTP/GPRS ライセンスを置き換え、SCTP と Diameter インспекションもサポートします。Firepower 9300 上の ASA の場合、feature mobile-sp コマンドは feature carrier コマンドに自動的に移行します。 次のコマンドが導入または変更されました。feature carrier、show activation-key、show license、show tech-support、show version
FirePOWER 9300 の ASA のシスコ スマート ソフトウェア ライセンシング	9.4(1.150)	FirePOWER 9300 に ASA のシスコ スマート ソフトウェア ライセンシングが導入されました。 次のコマンドが導入されました。feature strong-encryption、feature mobile-sp、feature context

機能名	プラットフォーム	説明
ASA 仮想 のシスコ スマート ソフトウェア ライセンス	9.3(2)	Smart Software Licensing では、ライセンスのプールを購入して管理することができます。PAK ライセンスとは異なり、スマート ライセンスは特定のシリアル番号に関連付けられません。各ユニットのライセンスキーを管理しなくても、簡単に ASA 仮想 を展開したり使用を終了したりできます。スマート ソフトウェア ライセンスを利用すれば、ライセンスの使用状況と要件をひと目で確認することもできます。 clear configure license、debug license agent、feature tier、http-proxy、license smart、license smart deregister、license smart register、license smart renew、show license、show running-config license、throughput level 各コマンドが導入されました。

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。

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。