

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 （2 ページ）
- スマート ソフトウェア ライセンスの前提条件 （25 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 （26 ページ）
- スマート ソフトウェア ライセンスのデフォルト （27 ページ）
- ASA 仮想：スマート ソフトウェア ライセンスの設定 （27 ページ）
- ASA 仮想：永続ライセンス予約の設定 （37 ページ）
- （オプション）ASA 仮想 の登録解除（定期およびオンプレミス） （42 ページ）
- （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） （42 ページ）
- Firepower 4100/9300：スマート ソフトウェア ライセンシングの設定 （43 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 （44 ページ）
- モデルごとのライセンス （59 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 （71 ページ）
- Smart Software Manager 通信 （72 ページ）
- スマート ソフトウェア ライセンスの履歴 （75 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、組織全体で使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 License Central でスマートアカウントを設定する必要があります。

シスコライセンスの詳細な概要については、Licensing Hub 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。

デフォルトでは、ライセンスはマスターアカウントの下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。

オフラインライセンス管理：永続ライセンス予約モード

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 （7 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 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 （37 ページ）を参照してください。

Cisco Secure Firewall および Firepower デバイスの永続ライセンス機能の可用性

すべての機能を有効にするライセンスを取得できます。次の表に、ファイアウォールデバイスで使用可能な永続ライセンス機能を示します。

表 *1*：デバイス全体に適用可能な永続ライセンス機能

機能	Essentials 階層	Security Plus ライセンス	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（適格の場合）	Secure Client 機能が有効
Firepower 1010	対応	対応	非対応	非対応	対応	対応
Firepower 1100	対応	非対応	対応	非対応	対応	対応
Cisco Secure Firewall 3100/4200/6100	対応	非対応	対応	対応	対応	対応
Firepower 4100/9300 シャーシ	対応	非対応	対応	対応	対応	対応

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 （7 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。

Firepower 4100/9300 シャーシ のライセンスを管理するには、『FXOS configuration guide』を参照してください。

ライセンスの使用を停止する場合は、デバイス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。

オフラインライセンス管理：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 1000/2100 および Secure Firewall 3100 の評価ライセンス

ファイアウォールデバイスは、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、デバイス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 の評価ライセンス

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AnyConnect 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AnyConnect 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

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。このルールの例外は、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でき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。

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

構成要件とフェールオーバーの動作については、「ハイアベイラビリティのためのフェールオーバー」を参照してください。このセクションでは、フェールオーバーおよびクラスタリングに関するスマートライセンスの要件と権限付与の動作のみについて説明します。

ASAv 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。アカウントに充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 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。

（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 ライセンシング 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 ライセンシング 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シング 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 ライセンシング 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。アカウントに充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 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。

（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 ライセンシング 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 ライセンシング 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シング 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 ライセンシング 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 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 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。アカウントに充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。

  Secure Firewall 3130 の例：

  - 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。アカウントに充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。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。アカウントに充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 3100/4200 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。

  Secure Firewall 3100 の例：

  - 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 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、集約されたクラスタライセンスは 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。

Secure Firewall 4200 の例：

- 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。

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：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 クラスタライセンス

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

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。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：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と、「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 （7 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 は非準拠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

Smart Call Home プロファイル

Firepower4100/9300（シャーシレベルでスマート ソフトウェア ライセンス通信を有効にする）を除くすべてのモデルのデフォルト構成には、Smart Software Manager の URL を指定する、「ライセンス」と呼ばれる Smart Call Home プロファイルが含まれます。

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。

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。

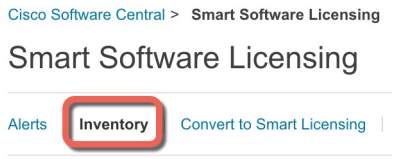
（注） ASA 仮想 を展開したときに、HTTP プロキシとライセンス権限付与が事前に設定されている可能性があります。また、ASA 仮想 を展開したときに Day0 設定で登録トークンが含まれている可能性があります。その場合は、この手順を使用して再登録する必要はありません。

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。

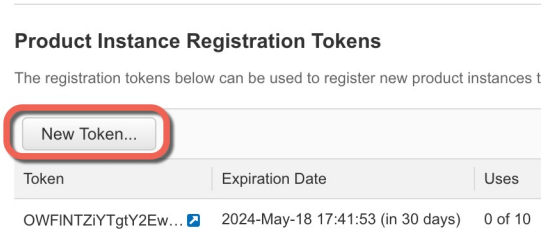
a) [Inventory] をクリックします。

図 *1*：インベントリ



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

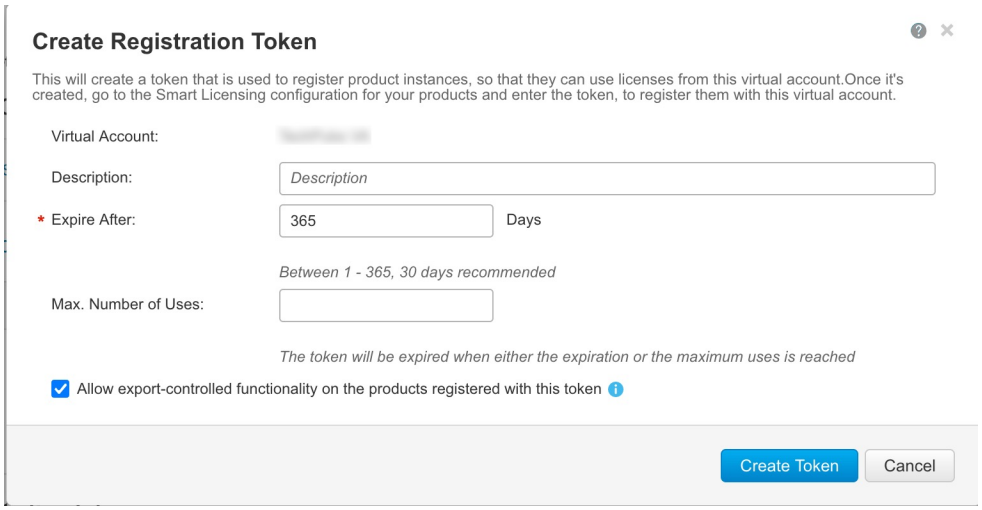
図 *2*：新しいトークン



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



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

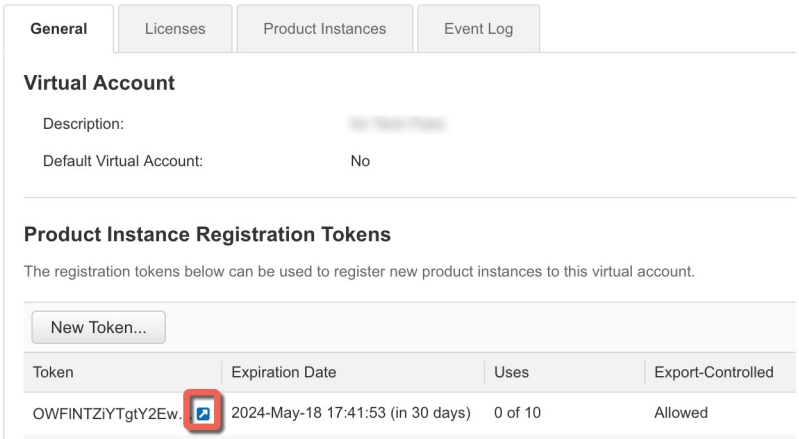
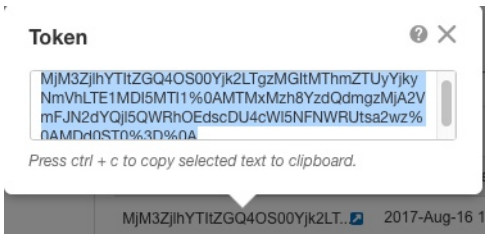


図 5：トークンのコピー



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

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、スマート ソフトウェア ライセンシング用のプロキシ アドレスを設定する必要があります。このプロキシは、一般に Smart Call Home にも使用されます。

（注） 認証を使用する HTTP プロキシはサポートされません。

a) [設定（Configuration）] > [デバイス管理（Device Management）] > [Smart Call-Home] の順に選択します。
b) [Enable HTTP Proxy] をオンにします。
c) [Proxy server] および [Proxy port] フィールドにプロキシの IP アドレスとポートを入力します。たとえば、HTTPS サーバーのポート 443 を入力します。
d) [Apply] をクリックします。

ステップ 3 ライセンス権限付与を設定します。

a) [設定（Configuration）] > [デバイス管理（Device Management）] > [ライセンシング（Licensing）] > [スマートライセンシング（Smart Licensing）] の順に選択します。
b) [スマートライセンス構成の有効化（Enable Smart license configuration）] をオンにします。
c) [機能階層（Feature Tier）] ドロップダウンリストから **Essentials** を選択します。

Essentials 階層のみが有効ですが、構成で有効にする必要があります。

d) [スループットレベル（Throughput Level）] ドロップダウンメニューから [100M]、[1G]、[2G]、[10G]、[20G] を選択します。

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

e) （任意）[強力な暗号化プロトコルの有効化（Enable strong-encryption protocol）] チェックボックスはオンにしてください。強力な暗号化トークンを受け取った場合は、このチェックボックスを**オンにしないでください**。

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。

f) [Apply] をクリックします。

ステップ 4 Smart Software Manager で ASA 仮想 を登録します。

a) [設定（Configuration）] > [デバイス管理（Device Management）] > [ライセンシング（Licensing）] > [スマートライセンシング（Smart Licensing）] の順に選択します。
b) [Register] をクリックします。
c) [ID Token] フィールドに登録トークンを入力します。
d) （オプション）[登録を強制（Force registration）] チェックボックスをオンにして、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 registration** を使用します。

e) [Register] をクリックします。

   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、後で ASA 仮想 の再登録が必要になる場合があります。たとえば、通信の問題により ID 証明書が期限切れになった場合です。

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

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 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。
- 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、Call Home の HTTP プロキシ URL を指定します。

（注） 認証を使用する HTTP プロキシはサポートされません。

a) [設定（Configuration）] > [デバイス管理（Device Management）] > [Smart Call-Home] の順に選択します。
b) [Enable HTTP Proxy] をオンにします。
c) [Proxy server] および [Proxy port] フィールドにプロキシの IP アドレスとポートを入力します。たとえば、HTTPS サーバーのポート 443 を入力します。
d) [Apply] をクリックします。

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。

a) **[設定（Configuration）] > [デバイス管理（Device Management）] > [Smart Call-Home] の順に選択します。**
b) [Configure Subscription Profiles] 領域で、[License] プロファイルを編集します。
c) [Deliver Subscriptions Using HTTP transport] 領域で、[Subscribers] URL を選択し、[Edit] をクリックします。
d) [Subscribers] URL を次の値に変更し、[OK] をクリックします。

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

e) [OK] をクリックし、さらに [Apply] をクリックします。

ステップ 4 ASA 仮想 では、ライセンス権限付与を構成します。

a) [設定（Configuration）] > [デバイス管理（Device Management）] > [ライセンシング（Licensing）] > [スマートライセンシング（Smart Licensing）] の順に選択します。
b) [Enable Smart license configuration] をオンにします。
c) [Feature Tier] ドロップダウンメニューから**Essentials**を選択します。

Essentials 階層のみが有効ですが、構成で有効にする必要があります。

d) Smart Software Manager から要求されるライセンスを決定するには、[スループットレベル（Throughput Level）] ドロップダウンリストから、[100M]、[1G]、[2G]、[10G]、[20G]、[無制限（unlimited）] のうちの 1 つを選択します。

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

e) （任意） [強力な暗号化プロトコルの有効化（Enable strong-encryption protocol）] チェックボックスはオンにしてください。強力な暗号化トークンを受け取った場合は、このチェックボックスを**オンにしないでください**。

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。

f) [適用（Apply）] をクリックします。

ステップ 5 ASA を Smart Software Manager に登録します。

a) [設定（Configuration）] > [デバイス管理（Device Management）] > [ライセンシング（Licensing）] > [スマートライセンシング（Smart Licensing）] の順に選択します。

b) [Register] をクリックします。

c) [ID Token] フィールドに登録トークンを入力します。

d) （オプション）[登録を強制（Force registration）] チェックボックスをオンにして、Smart Software Manager と同期されていない可能性がある登録済みの Cisco ASA を登録します。

たとえば、Smart Software Manager から誤って ASA を削除した場合に [Force registration] を使用します。

e) [登録（Register）] をクリックします。

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 ステータスを確認する場合は、[Monitoring] > [Properties] > [Smart License] の順に選択します。

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。

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

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、ライセンシ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

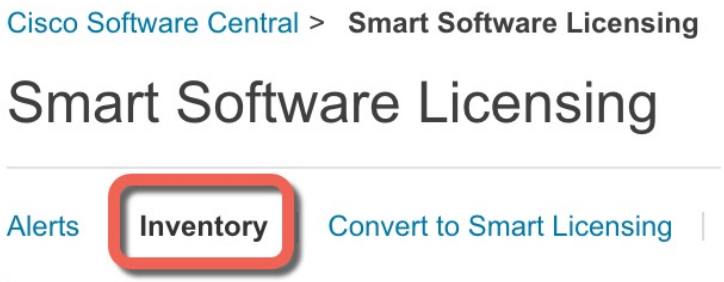
Download the Smart Software Manager オンプレミス OVA ファイルを Cisco.com からダウンロードし、VMware ESXi サーバーにインストールして構成します。詳細については、『*Cisco Smart Software Manager On-Prem Data Sheet*』を参照してください。

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。

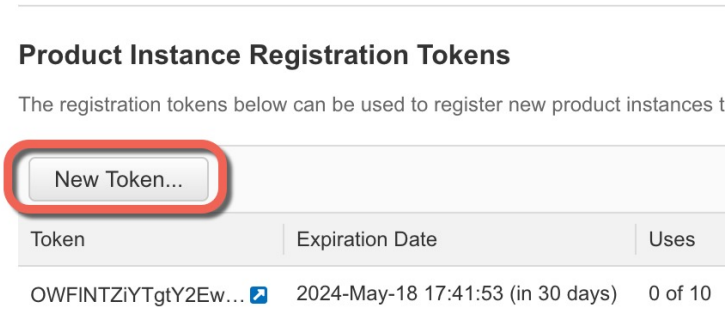
a) [Inventory] をクリックします。

図 *6*：インベントリ



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

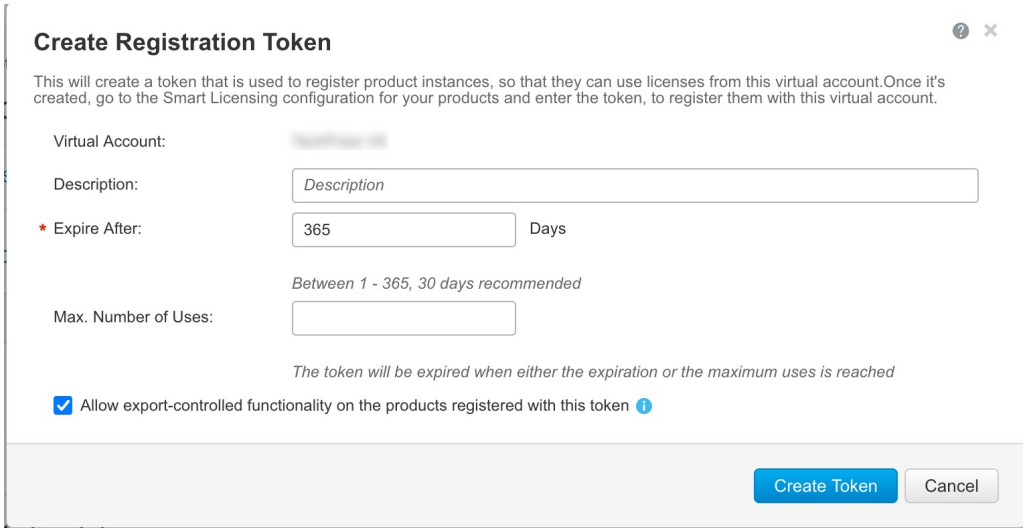
図 *7*：新しいトークン



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。
- [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



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

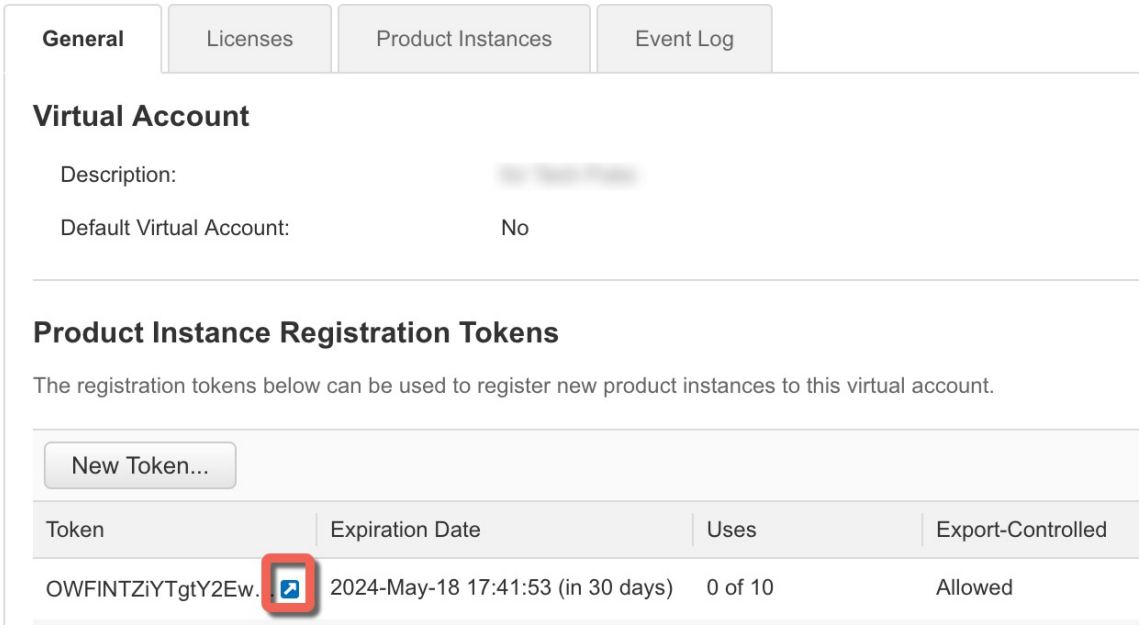
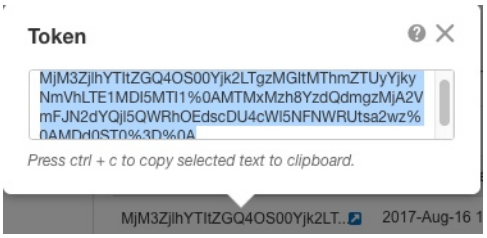


図 *10*：トークンのコピー



ステップ 2 [設定（Configuration）]>[デバイス管理（Device Management）]>[ライセンシング（Licensing）]>[スマートライセンシング（Smart Licensing）] の順に選択します。

ステップ 3 ライセンス権限付与を設定します。

a) [スマートライセンス構成の有効化（Enable Smart license configuration）] をオンにします。

b) [Feature Tier] ドロップダウンメニューから**Essentials**を選択します。

Essentials 階層のみが有効ですが、構成で有効にする必要があります。

c) Smart Software Manager から要求されるライセンスを決定するには、[スループットレベル（Throughput Level）] ドロップダウンリストから、[100M]、[1G]、[2G]、[10G]、[20G]、[無制限（unlimited）] のうちの 1 つを選択します。

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

d) （任意）[強力な暗号化プロトコルの有効化（Enable strong-encryption protocol）] チェックボックスはオンにしてください。

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。

ステップ 4 （任意）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する場合、次のチェックボックスをオンにします。

a) ホスト名（Host Name）。

b) バージョン（Version）。

ステップ 5 [Smart Transport] オプションボタンをクリックします。

ステップ 6 Smart Transport の URL を設定します。

a) [カスタムURL（Custom URL）]オプションボタンをクリックし、[URL]フィールドにURLを入力します。
b) [登録（Registration）]フィールドに、Smart Software Manager 定期またはオンプレミスの登録トークンを貼り付けます。
c) [ユーティリティ（Utility）]フィールドで、Smart Software Manager 定期またはオンプレミスの URL を指定します。
d) （任意）[**プロキシ url（proxy url**）]フィールドで、ライセンスサーバーまたはサテライトがプロキシ経由でのみ到達可能な場合は、プロキシの url を指定します。

（注） 認証を使用する HTTP プロキシはサポートされません。

e) （任意） [Proxy Port] フィールドで、プロキシポート番号を指定します。

ステップ 7 [標準ユーティリティモードを有効にする（Enable Standard Utility Mode）] チェックボックスをオンにします。

ステップ 8 ユーティリティライセンス情報を設定します。これには、課金のために必要な顧客情報が含まれます。

a) [Custom ID] フィールドで、一意のカスタマーIDを指定します。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。
b) お客様プロファイルを作成するには、残りの項目に適切な情報を入力してください。具体的には、[お客様会社ID（Customer Company Identifier）]、[お客様会社名（Customer Company Name）]、[お客様住所（番地）（Customer Street）]、[お客様住所（市区町村）（Customer City）]、[お客様住所（都道府県）（Customer State）]、[お客様住所（国名）（Customer Country）]、[お客様郵便番号（Customer Postal Code）] などです。

ステップ 9 [Apply] をクリックします。

ステップ 10 [登録（Register）] をクリックし、Smart Software Manager 定期またはオンプレミスに ASA 仮想を登録します。

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。ライセンス ステータスを確認する場合は、[Monitoring] > [Properties] > [Smart License] の順に選択します。

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 （38 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 （40 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 （40 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。Day 0 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 （40 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 AAu3431rGRS00Ig5HQl2vpzg{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

（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:
Au3431rGRS00Ig5HQl2vpcg{uXiTRfVrp7M/zDpirLwYCaq8oSv60yZJuFDVBS2QliQ=
```

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

ステップ 1 **[Configuration]** > **[Device Management]** > **[Licensing]** > **[Smart Licensing]** の順に選択します。

ステップ 2 [登録解除（Unregister）] をクリックします。

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 ヵ月ごと、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 **[Configuration]** > **[Device Management]** > **[Licensing]** > **[Smart Licensing]** の順に選択します。

ステップ 2 アイデンティティ証明書を更新するには、[Renew ID Certificate] をクリックします。

ステップ 3 ライセンス資格を更新するには、[Renew Authorization] をクリックします。

Firepower 4100/9300：スマート ソフトウェア ライセンシングの設定

この手順は、Smart Software Manager、Smart Software Manager オンプレミスを使用するシャーシ、または永続ライセンス予約に適用されます。ライセンシング通信を事前設定するには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、ASA がこれらの機能を使用することを「認識する」ためには、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ノードにアクセスする必要があります。Firewall Chassis Manager でどのノードが制御ノードなのかを確認してください。

手順

ステップ 1 ASDM で、**[Configuration]** > **[Device Management]** > **[Licensing]** > **[Smart Licensing]** の順に選択します。

ステップ 2 [機能層（Feature Tier）] ドロップダウン リストから [標準（Standard）] を選択します。

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 3 （任意）[強力な暗号化プロトコルの有効化（Enable strong-encryption protocol）] チェックボックスはオンにしてください。強力な暗号化トークンを受け取った場合は、このチェックボックスを**オンにしないでください**。

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。

ステップ 4 （任意）**[キャリア（Carrier）]** チェックボックスをオンにします。

ステップ 5 （任意）[コンテキスト（Context）] ドロップダウンリストから、必要なコンテキストの番号を選択します。

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。

ステップ 6 [Apply] をクリックします。

ステップ 7 ASDM を終了し、再起動します。

ライセンスを変更する場合、更新された画面を表示するには ASDM を再起動する必要があります。

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

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 ライセンシング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

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 ライセンシングの設定 （44 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） （58 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） （58 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シングの設定 （49 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） （58 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） （58 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 （53 ページ）

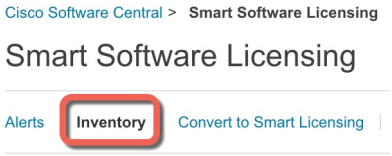
その他のモデル：定期スマート ソフトウェア ライセンシングの設定

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

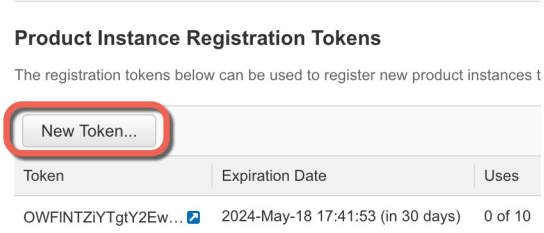
手順

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。

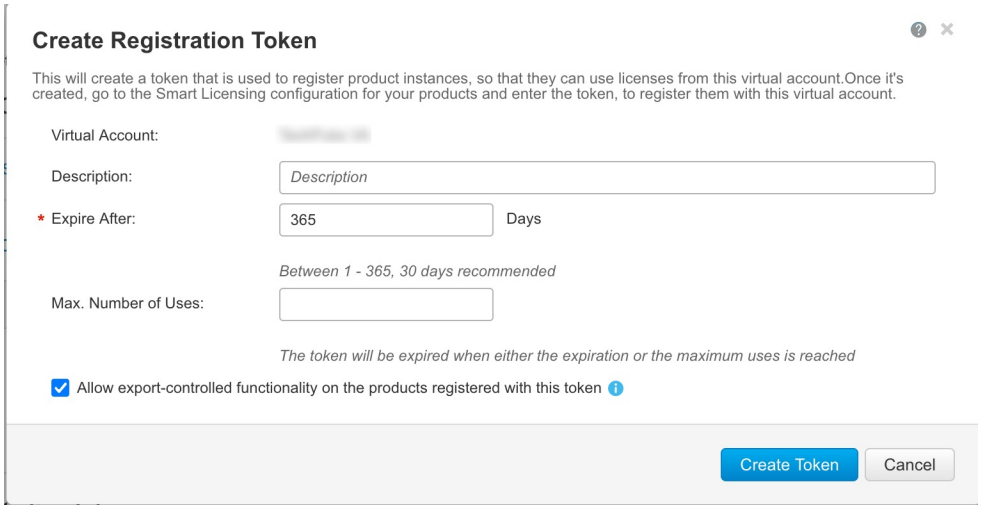
a) [Inventory] をクリックします。



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。



- **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

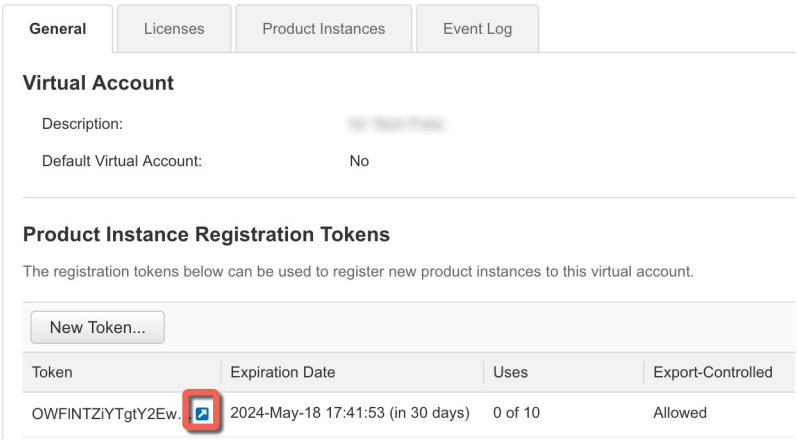
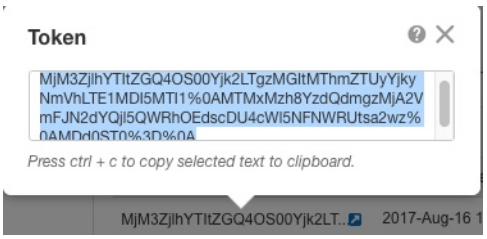


図 *12* : トークンのコピー



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

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、スマート ソフトウェア ライセンシング用のプロキシ アドレスを設定する必要があります。このプロキシは、一般に Smart Call Home にも使用されます。

（注） 認証を使用する HTTP プロキシはサポートされません。

a) [設定（Configuration）] > [デバイス管理（Device Management）] > [Smart Call-Home] の順に選択します。
b) [HTTPプロキシの有効化（Enable HTTP Proxy）] チェックボックスをオンにします。
c) [プロキシサーバー（Proxy server）] および [プロキシポート（Proxy port）] フィールドにプロキシの IP アドレスとポートを入力します。たとえば、HTTPS サーバーのポート 443 を入力します。
d) [Apply] をクリックします。

ステップ 3 ライセンス権限付与を設定します。

a) [設定（Configuration）] > [デバイス管理（Device Management）] > [ライセンシング（Licensing）] > [スマートライセンシング（Smart Licensing）] の順に選択します。
b) [スマートライセンス構成の有効化（Enable Smart license configuration）] をオンにします。

c) [機能層（Feature Tier）] ドロップダウンメニューから **[Essentials]** を選択します。

使用できるのは **[Essentials]** 階層のみですが、構成でこれを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です。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。

d) （任意）（Firepower 1010）[Security Plusの有効化（Enable Security Plus）] をオンにします。

Security Plus 階層によってフェールオーバーが有効になります。

e) （任意）（サポートされるモデル）[コンテキスト（Context）] ライセンスの場合、コンテキストの数を入力します。

デフォルトでは、ASA は 2 つ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 2 つのデフォルト コンテキストを差し引いたもの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

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。

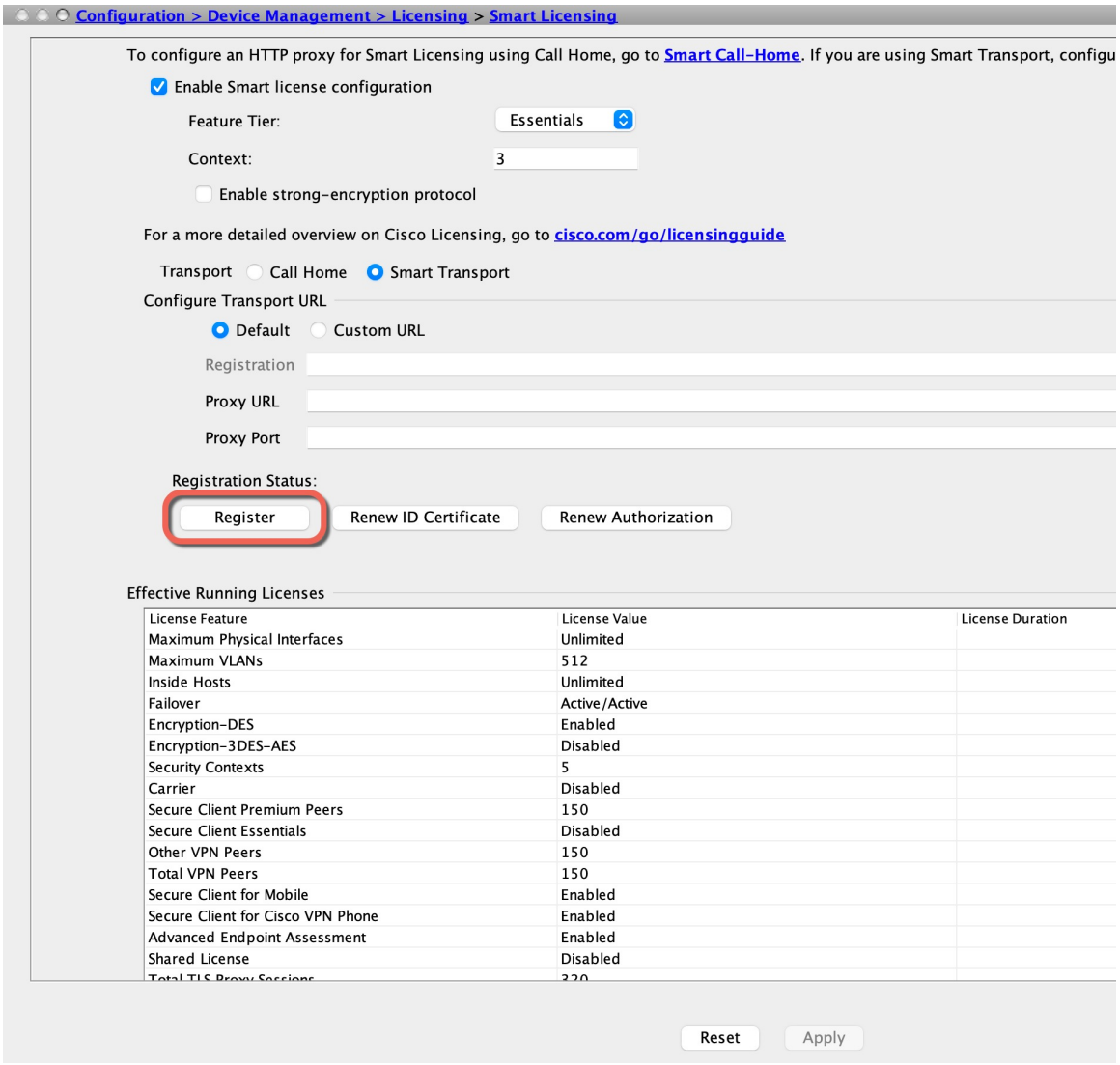
f) （任意）[強力な暗号化プロトコルの有効化（Enable strong-encryption protocol）] チェックボックスはオンにしてください。強力な暗号化トークンを受け取った場合は、このチェックボックスを**オンにしないでください**。

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。

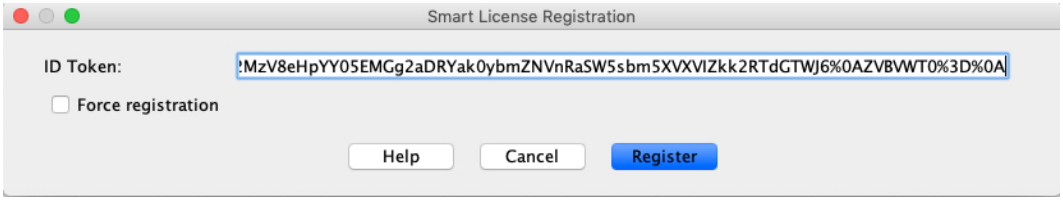
g) （任意）（サポートされるモデル）Diameter、GTP/GPRS、SCTP 検査に対して [キャリアを有効化（Enable Carrier）] をオンにします。

h) [Apply] をクリックします。

ステップ 4 [登録（Register）] をクリックします。



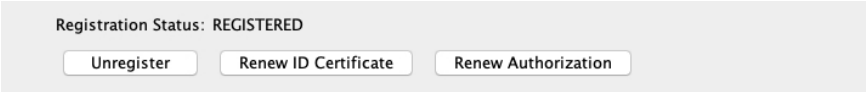
ステップ 5 [IDトークン（ID Token）] フィールドの [Cisco Smart Software Manager] に登録トークンを入力します。



（オプション）[登録を強制（Force registration）] チェックボックスをオンにして、Smart Software Manager と同期されていない可能性がある登録済みの ASA を登録します。たとえば、Smart Software Manager から誤って ASA を削除した場合に [Force registration] を使用します。

ステップ 6 [登録（Register）] をクリックします。

ライセンス ステータスが更新されると、ASDM によってページが更新されます。また、登録が失敗した場合などには、**[モニタリング（Monitoring）] > [プロパティ（Properties）] > [スマートライセンス（Smart License）]** の順に選択して、ライセンスステータスを確認できます。



ステップ 7 ASDM を終了し、再起動します。

ライセンスを変更する場合、更新された画面を表示するには ASDM を再起動する必要があります。

その他のモデル：Smart Software Manager オンプレミスライセンシングの設定

この手順は、Smart Software Manager オンプレミスを使用する ASA 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 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。
- 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） ASA 仮想 で、Call Home の HTTP プロキシ URL を指定します。

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、スマート ソフトウェア ライセンシング用のプロキシ アドレスを設定する必要があります。このプロキシは、一般に Smart Call Home にも使用されます。

（注） 認証を使用する HTTP プロキシはサポートされません。

a) [設定（Configuration）] > [デバイス管理（Device Management）] > [Smart Call-Home] の順に選択します。

b) [HTTPプロキシの有効化（Enable HTTP Proxy）] チェックボックスをオンにします。
c) [Proxy server] および [Proxy port] フィールドにプロキシの IP アドレスとポートを入力します。

たとえば、HTTPS サーバーのポート 443 を入力します。

d) [Apply] をクリックします。

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。

a) **[設定（Configuration）] > [デバイス管理（Device Management）] > [Smart Call-Home] の順に選択します。**
b) [Configure Subscription Profiles] 領域で、[License] プロファイルを編集します。
c) [Deliver Subscriptions Using HTTP transport] 領域で、[Subscribers] URL を選択し、[Edit] をクリックします。
d) [Subscribers] URL を次の値に変更し、[OK] をクリックします。

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

e) [OK] をクリックし、さらに [Apply] をクリックします。

ステップ 4 ライセンス権限付与を設定します。

a) [設定（Configuration）] > [デバイス管理（Device Management）] > [ライセンシング（Licensing）] > [スマートライセンシング（Smart Licensing）] の順に選択します。
b) [スマートライセンス構成の有効化（Enable Smart license configuration）] をオンにします。
c) [機能層（Feature Tier）] ドロップダウンメニューから **[Essentials]** を選択します。

使用できるのは **[Essentials]** 階層のみですが、構成でこれを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です。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。

d) （任意）（Firepower 1010）[Security Plusの有効化（Enable Security Plus）] をオンにします。

Security Plus 階層によってフェールオーバーが有効になります。

e) （任意）（サポートされるモデル）[コンテキスト（Context）] ライセンスの場合、コンテキストの数を入力します。

デフォルトでは、ASA は 2 つ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 2 つのデフォルト コンテキストを差し引いたもの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

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。

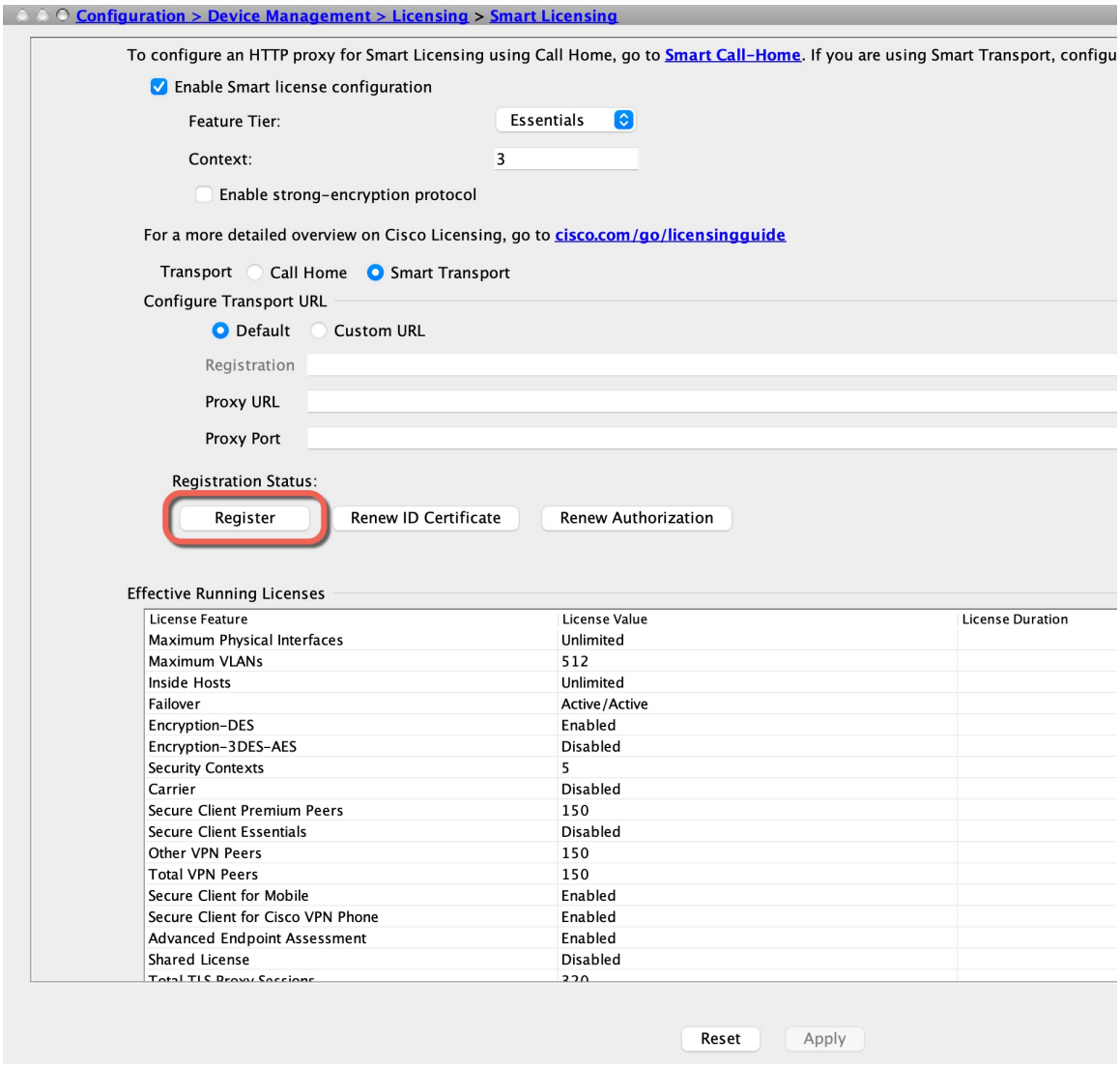
f) （任意）[強力な暗号化プロトコルの有効化（Enable strong-encryption protocol）] チェックボックスはオンにしてください。強力な暗号化トークンを受け取った場合は、このチェックボックスを**オンにしないでください**。

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。

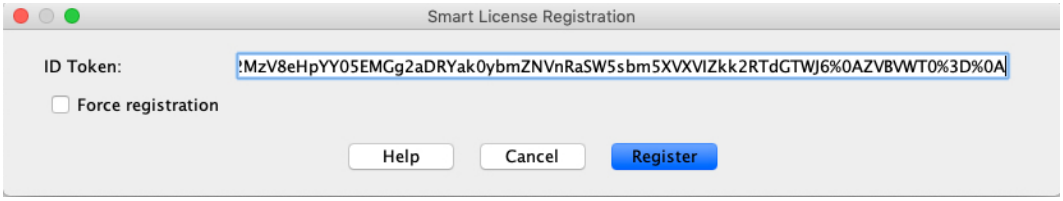
g) （任意）（サポートされるモデル）Diameter、GTP/GPRS、SCTP 検査に対して [キャリアを有効化（Enable Carrier）] をオンにします。

h) [適用（Apply）] をクリックします。

ステップ 5 [登録（Register）] をクリックします。



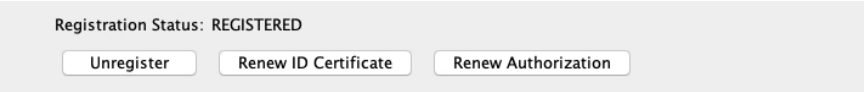
ステップ 6 [IDトークン（ID Token）] フィールドの [Cisco Smart Software Manager] に登録トークンを入力します。



（オプション）[登録を強制（Force registration）] チェックボックスをオンにして、Smart Software Manager と同期されていない可能性がある登録済みの ASA を登録します。たとえば、Smart Software Manager から誤って ASA を削除した場合に [Force registration] を使用します。

ステップ 7 [登録（Register）] をクリックします。

ライセンス ステータスが更新されると、ASDM によってページが更新されます。また、登録が失敗した場合などには、**[モニタリング（Monitoring）] > [プロパティ（Properties）] > [スマートライセンス（Smart License）]** の順に選択して、ライセンススタータスを確認できます。



ステップ 8 ASDM を終了し、再起動します。

ライセンスを変更する場合、更新された画面を表示するには ASDM を再起動する必要があります。

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 永続ライセンスのインストール （53 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 （57 ページ）。

1000/2100/3100 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 （57 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 （57 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 AAu3431rGRS00Ig5HQl2vpzg{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 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

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:
Au3431rGRS00Ig5HQl2vpcg{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 （73 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

手順

ステップ 1 **[Configuration]** > **[Device Management]** > **[Licensing]** > **[Smart Licensing]** の順に選択します。

ステップ 2 [登録解除（Unregister）] をクリックします。

（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 ヵ月ごと、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 **[Configuration]** > **[Device Management]** > **[Licensing]** > **[Smart Licensing]** の順に選択します。

ステップ 2 アイデンティティ証明書を更新するには、[Renew ID Certificate] をクリックします。

ステップ 3 ライセンス資格を更新するには、[Renew Authorization] をクリックします。

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、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	
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、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	有効。

ライセンス	説明
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	有効。
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

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	Base（DES）または Strong（3DES/AES）（アカウントのエクスポート コンプライアンス設定による）。
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	サポートしない
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	サポートしない	
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	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	Base（DES）または Strong（3DES/AES）（アカウントのエクスポート コンプライアンス設定による）。	
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	サポートしない	
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	Base（DES）または Strong（3DES/AES）（アカウントのエクスポート コンプライアンス設定による）。	

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： *Firepower 1120：5* *Firepower 1140：10* *Firepower 1150：25*
クラスタ	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	サポートしない
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 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*Secure Client Advantage*、*Secure Client Premier*、または*Secure Client VPN* のみライセンス、最大： *Firepower 2110：1,500* *Firepower 2120：3,500* *Firepower 2130：7,500* *Firepower 2140：10,000*
その他の VPN ピア	Firepower 2110：1,500 Firepower 2120：3,500 Firepower 2130：7,500 Firepower 2140：10,000	
合計 VPN ピア。全タイプの合計	Firepower 2110：1,500 Firepower 2120：3,500 Firepower 2130：7,500 Firepower 2140：10,000	
一般ライセンス		
暗号化	Base（DES）または Strong（3DES/AES）（アカウントのエクスポート コンプライアンス設定による）。	
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： *Firepower 2110：25* *Firepower 2120：25* *Firepower 2130：30* *Firepower 2140：40*
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	サポートしない	
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	Base（DES）または Strong（3DES/AES）（アカウントのエクスポート コンプライアンス設定による）。	
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	有効。	
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	サポートしない	
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	Base（DES）または Strong（3DES/AES）（アカウントのエクスポート コンプライアンス設定による）。	
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	有効。	
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	サポートしない	
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	Base（DES）または Strong（3DES/AES）（アカウントのエクスポート コンプライアンス設定による）。	
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	有効。	
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 画面を参照してください。

- [Configuration] > [Device Management] > [Licensing] > [Smart Licensing] ペインで、[Effective Running Licenses] 領域を表示します。

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。

- ：**[Monitoring] > [Properties] > [Smart License]**

  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。

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#
```

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り、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：デバイスが使用可能なライセンス数よりも多くのライセンスを使用している。
- 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。
- 通信の欠落：デバイスが再承認を得るためにライセンス認証局に到達することができず、承認期限が切れている。

デバイスがコンプライアンス違反なのか、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。

デバイスがコンプライアンス違反の場合、モデルによっては操作が制限されることがあります。

- ASA 仮想：システムは、同時 AnyConnect セッションを 2 つに制限し、合計スループットを 100 Kbps にスロットリングする制限状態に入ります。このレート制限により、有効な

ライセンスがインストールされるまで、デバイスは大幅に削減されたキャパシティで動作し続けます。この動作は、ASA 仮想モデルに固有です。

- 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、**[構成（Configuration）] > [リモートアクセスVPN（Remote Access VPN）] > [証明書管理（Certificate Management）] > [信頼できる証明書プール（Trusted Certificate Pool）] > [信頼できる証明書プールポリシーの編集（Edit Trusted Certificate Pool Policy）]** 画面の [自動インポート（Automatic Import）] エリアを構成します。

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。

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
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/変更された画面：**[設定（Configuration）] > [デバイス管理（Device Management）] > [ライセンス（Licensing）] > [スマートライセンス（Smart Licensing）]**。
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。
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/変更された画面：**[設定（Configuration）] > [デバイス管理（Device Management）] > [ライセンス（Licensing）] > [スマートライセンス（Smart Licensing）]**。

機能名	プラットフォームリリース	説明
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/メモリ構成で使用でき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/変更された画面：**[設定（Configuration）] > [デバイス管理（Device Management）] > [ライセンス（Licensing）] > [スマートライセンス（Smart Licensing）]**。
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 の短か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。 変更された画面はありません。
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。 変更された画面はありません。
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。

機能名	プラットフォームリリース	説明
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** ASDM サポートはありません。
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。[Configuration] > [Device Management] > [Licensing] > [Smart Licensing] ページで [Force registration] オプションを指定して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。 変更された画面はありません。
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。 次の画面が変更されました。**[Configuration]** > **[Device Management]** > **[Licensing]** > **[Smart License]**

機能名	プラットフォームリリース	説明
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。 次の画面が変更されました。**[Configuration]** > **[Remote Access VPN]** > **[Certificate Management]** > **[Trusted Certificate Pool]** > **[Edit Trusted Certificate Pool Policy]**
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 インスペク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。 次の画面が変更されました。**[Configuration]** > **[Device Management]** > **[Licensing]** > **[Smart License]**
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。 次の画面が変更されました。**[Configuration]** > **[Device Management]** > **[Licensing]** > **[Smart License]**
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。 次の画面が導入または変更されました。 **[Configuration] > [Device Management] > [Licensing] > [Smart License] [Configuration] > [Device Management] > [Smart Call-Home] [Monitoring] > [Properties] > [Smart License]**

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。

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。