



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) 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 \(36 ページ\)](#)
- [スマート ソフトウェア ライセンスのガイドライン \(37 ページ\)](#)
- [スマート ソフトウェア ライセンスのデフォルト \(37 ページ\)](#)
- [ASA 仮想：スマート ソフトウェア ライセンスの設定 \(38 ページ\)](#)
- [Firepower 4100/9300：スマート ソフトウェア ライセンシングの設定の設定 \(59 ページ\)](#)
- [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 \(60 ページ\)](#)
- [モデルごとのライセンス \(76 ページ\)](#)
- [モデルごとのライセンス PID \(93 ページ\)](#)
- [スマート ソフトウェア ライセンシングのモニタリング \(100 ページ\)](#)
- [Smart Software Manager 通信 \(100 ページ\)](#)
- [スマート ソフトウェア ライセンスの履歴 \(103 ページ\)](#)

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 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 (スマートライセンス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](#)（11 ページ）を参照）。

シスコでは、ASA 仮想に2つの永続ライセンス予約モードを用意しています。

- メモリおよび vCPU に基づく永続ライセンス予約モード
- 柔軟な永続ライセンス予約モード

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 ASA v30 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：ASA v5 (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、ASA v10 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、ASA v5 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 ASA v5 ではなく ASA v10 であると判断していたため、この増加により、ASA v5 の永続ライセンスが機能しなくなっています。ASA v5 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：ASA v10 (1G)
- 8 GB、4 vCPU：ASA v30 (2G)
- 16 GB、8 vCPU：ASA v50 (10G)
- 32 GB、16 vCPU：ASA v100 (20G)
- 64 GB、32 vCPU：ASA vU
- 128 GB、64 vCPU：ASA vU

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。

柔軟な永続ライセンス予約モード

ASA 仮想に割り当てられた RAM および vCPU に関係なく、モデル固有のライセンスを設定できます。

指定するモデルライセンスにより、ASA 仮想のスループットレベルが設定されます。ASA 仮想のメモリにより、最大セキュアクライアントセッション、TLS プロキシセッション、最大同時ファイアウォール接続数および VLAN が決定されます（モデルライセンスではありません）。ただし、ASA 仮想メモリプロファイルを小さくすると、セッションと機能の実際の数が制限されます。

たとえば、ASA 仮想に 8 GB の RAM があり、ASAV_50_UNIVERSAL に登録されている場合、セキュアクライアントに割り当てられる最大セッション数は 750 です。セッションがこの制限を超えると、接続はドロップされます。

永続ライセンスの予約ライセンスモードのその他の利点は次のとおりです。

- ASA 仮想に割り当てられたメモリに関係なく、永続ライセンスの予約ライセンスを切り替えることができます。ただし、ASA 仮想に 16 を超える vCPU がある場合は、ASA vU（無制限）ライセンスのみを設定できます。
- モデルライセンスを変更せずに、ASA 仮想に割り当てられたメモリと vCPU を変更できます。

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。

Secure Firewall 200 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
- 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（11 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 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 \(11 ページ\)](#) 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 \(11 ページ\)](#) 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 1210/1220 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
- 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 \(11 ページ\)](#) 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 1230/1240/1250 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
- 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 \(11 ページ\)](#) 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 3100/4200/6100 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 \(11 ページ\)](#) 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](#)（11 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ス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、Cisco Secure Firewall 1200/3100/4200

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ります。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スアカウントから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、輸出管理機能が無効になります。その場合、IPSec 暗号化が有効になっていると、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：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ス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。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。評価ライセンスを保有している場合や、高度暗号化が有効になっていない場合は、**crypto permit-weak-ciphers** コマンドを使用して弱い暗号化暗号を有効にした場合にのみ DES を使用できます。

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があります。

- 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

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。

Secure Firewall 200 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。

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。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。
- 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 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ス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ス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。スマートライセンスングサーバに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ス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ス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ス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（スプリットブレイク）。

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、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、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。

Cisco Secure Firewall 1210/1220 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。

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。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 1210 ユニットの場、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5Context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9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Cisco Secure Firewall 1220 ユニットの場、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5Context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9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4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9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。9 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。

Cisco Secure Firewall 1230/1240/1250 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。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 1230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25 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29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25であるため、結合されたライセンスでは最大25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21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Cisco Secure Firewall 1230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25であるため、結合されたライセンスでは最大25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 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。

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100Context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 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シングを設定できます。アクティブ/A

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。

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。

Cisco Secure Firewall 6100 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。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。2つのCisco Secure Firewall 6160ユニットの場合、これらのライセンスは最大20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。2つのCisco Secure Firewall 6160ユニットの場合、これらのライセンスは最大10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せん。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 ユニットの状況、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 ユニットの状況、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。シャーン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となります。

- 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となります。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ー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ー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ーライセンスは32のコンテキストを含みます。シャージ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ーライセンスは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。

Secure Firewall 6100 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。

- クラスタ内に4つのCisco Secure Firewall 6100があります。Essentialsライセンスは10のコンテキストを含みます。4つユニットの場合、合計で40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60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。60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60コンテキストを設定できます。各データユニットも、設定の複製を介して60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 6100があります。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。
- 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。

ASA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となります。
 - 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となります。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。
- 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（[モデルごとのライセンス PID \(93 ページ\)](#) を参照）。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時、「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 \(11 ページ\)](#)」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。



(注) VMware または KVM で 32 または 64 コア展開を使用している場合、**throughput level** コマンドで使用できるのは **unlimited** オプションのみです。

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。

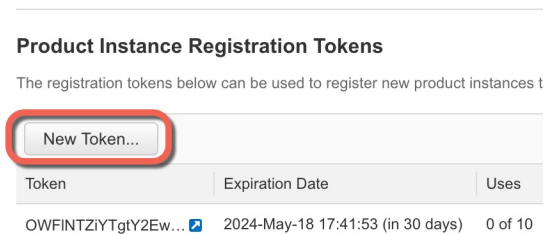
- a) [Inventory] をクリックします。

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

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

ステップ 2 (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) ASA 仮想 で、[設定 (Configuration)] > [デバイス管理 (Device Management)] > [Smart Call-Home] の順に選択します。
- b) (任意) [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て、[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。
(注)
認証を使用する HTTP プロキシはサポートされません。
- c) [Apply] をクリックします。
- d) [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)] の順に選択します。
- e) [トランスポート (Transport)] では、[Call Home] オプションボタンをクリックします。

ステップ 3 (任意) Smart Transport の HTTP プロキシを指定します。

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 2 \(41 ページ\)](#) を参照してください。

- a) [トランスポート (Transport)] で、[Smart Transport] オプションボタンをクリックします。
- b) [プロキシ URL (Proxy URL)] および [プロキシポート (Proxy Port)] フィールドに、IP アドレスまたは FQDN とプロキシポート番号を入力します。

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)] > [ライセンス (Licensing)] > [スマートライセンス (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]、[無制限 (unlimited)] 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
- 無制限：ASAvU

- 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 5 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)] > [ライセンスング (Licensing)] > [スマートライセンスング (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 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) 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) ASA 仮想 では、**[構成 (Configuration)] > [デバイス管理 (Device Management)] > [Smart Call-Home]** を選択します。
- b) (任意) **[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て、**[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。

(注)

認証を使用する HTTP プロキシはサポートされません。

- c) **[サブスクリプションプロファイルの設定 (Configure Subscription Profiles)]** 領域で、**[ライセンス (License)]** プロファイルを編集し、Smart Software Manager オンプレミスに移動するようにライセンスサーバー URL を編集します。
- d) **[Deliver Subscriptions Using HTTP transport]** 領域で、**[Subscribers] URL** を選択し、**[Edit]** をクリックします。
- e) **[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

- f) **[OK]** をクリックします。
- g) **[Apply]** をクリックします。

- h) [設定 (Configuration)] > [デバイス管理 (Device Management)] > [ライセンスング (Licensing)] > [スマートライセンスング (Smart Licensing)] の順に選択します。
- i) [トランスポート (Transport)] では、[Call Home] オプションボタンをクリックします。

ステップ 3 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)] > [ライセンスング (Licensing)] > [スマートライセンスング (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
- 無制限 : ASAvU

- 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 4 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、任意に HTTP プロキシを指定します。

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 2 \(43 ページ\)](#) を参照してください。

- a) [トランスポート (Transport)] で、[**Smart Transport**] オプションボタンをクリックします。
- b) [カスタム URL (Custom URL)] オプションボタンをクリックして、次の形式で Smart Software Manager オンプレミス URL を設定します。

https://on-prem_ip_address/SmartTransport

- c) (任意) [プロキシURL (Proxy URL)] の IP アドレスまたは FQDN と [プロキシポート (Proxy Port)] の番号を設定します。

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)] > [ライセンスング (Licensing)] > [スマートライセンスング (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スの設定

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スングでは、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スングモードでは、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スングでは、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。

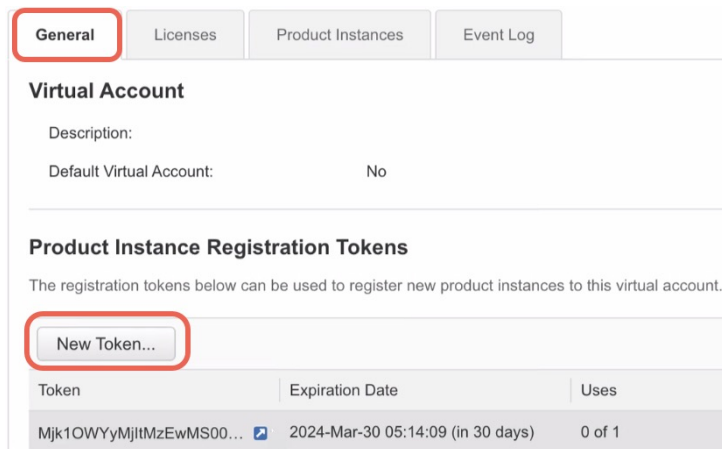
- a) [Inventory] をクリックします。

図 6: インベントリ



- 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。

- [最大使用数 (Max. Number of Uses)] : トークンの最大使用数。

トークンは、有効期限または最大使用回数で期限切れになります。

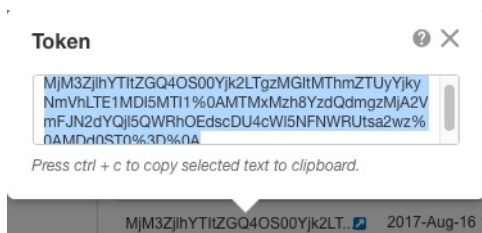
図 8: 登録トークンの作成

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)]>[ライセンスング (Licensing)]>[スマートライセンスング (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
- 無制限 : ASAvU

- 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 \(49 ページ\)](#)
- ステップ2** (オプション) [ASA 仮想の永続ライセンスの返却 \(54 ページ\)](#)
-

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 \(54 ページ\)](#) 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、非柔軟なライセンスング) 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 (オプション) 次のコマンドを実行して、RAM および vCPU に関係なく、永続ライセンス予約を手動で構成します (柔軟な永続ライセンスの予約モード)。

license smart flex-model { asav5_plr | asav10_plr | asav30_plr | asav50_plr | asav100_plr | asavu_plr }

(注)

ASA 仮想 に 16 を超える vCPU がある場合は、Cisco ASAvU (無制限) ライセンスのみを構成できます。

柔軟な永続ライセンス予約を無効にするには、**no license smart reservation** コマンドを使用して永続ライセンスの予約モードを無効にした後、このコマンドの **no** 形式を使用します。

柔軟な永続ライセンスの予約モードでは、ライセンス予約を有効にする前に任意の数で権限を変更できます。ライセンス予約を有効にした後に権限を変更するには、永続ライセンス予約を無効にし、新しい権限で有効にしてから、ライセンス予約を有効にする必要があります。

たとえば、ASA 仮想 に Cisco ASAv30 の権限があり、永続ライセンス予約が有効になっているとします。

```
asav1# license smart flex-model asav30_plr
asav1# license smart reservation
```

ここで、権限付与を Cisco ASAv50 に変更すると、エラーが発生します。

```
asav1# license smart flex-model asav50_plr
ERROR: Flexible PLR CLI is disabled when license reservation is enabled
```

権限付与を Cisco ASAv50 に変更するには、次のコマンドを実行する必要があります。

```
asav1# no license smart reservation
asav1# license smart flex-model asav50_plr
asav1# license smart reservation
```

ステップ 3 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。

ステップ 4 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/ljRDaSp3w8uG1feQ{53C13E
ciscoasa#
```

柔軟なライセンスの場合：モデルライセンスを変更せずに、Cisco ASA Virtual に割り当てられたメモリと vCPU を変更できます。

非柔軟なライセンスの場合：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 (54 ページ) を参照してください。

ステップ 5 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 6 [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 7 [次へ (Next)] をクリックします。

[予約するライセンス (Licenses to Reserve)] の下に表示される永続ライセンスの予約資格を確認します。これは、**ステップ 2** で設定した権限付与である必要があります。

ステップ 8 [次へ (Next)] をクリックします。

ステップ 9 情報を確認し、[承認コードの生成 (Generate Authorization Code)] 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。

ステップ 10 [閉じる (Close)] をクリックします。

ステップ 11 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 12 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 13 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

ステップ 14 ライセンスのステータスと権限付与の制限を確認します。

• **show license all**

```
asav1# show license all

Smart Licensing Status
=====
```

```
Smart Licensing is ENABLED
License Reservation is ENABLED

Registration:
  Status: REGISTERED - UNIVERSAL LICENSE RESERVATION
  Export-Controlled Functionality: ALLOWED
  Initial Registration: SUCCEEDED on Nov 12 2024 06:40:36 UTC

License Authorization:
  Status: AUTHORIZED - RESERVED on Nov 12 2024 06:27:23 UTC

Export Authorization Key:
  Features Authorized:
    <none>

Utility:
  Status: DISABLED

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

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

Miscellaneous:
  Custom Id: <empty>

License Usage
=====

No licenses in use

Product Information
=====
UDI: PID:ASAv,SN:9A9PJLLB849

Agent Version
=====
Smart Agent for Licensing: 5.7.25_asav/5

Reservation Info
=====
License reservation: ENABLED

Overall status:
  Active: PID:ASAv,SN:9A9PJLLB849
  Reservation status: UNIVERSAL INSTALLED on Nov 12 2024 06:27:23 UTC
```

- **show license features**

```
asav1# show license features
Serial Number: 9AEJMLUP4D4
Export Compliant: YES
```

(オプション) ASA 仮想の永続ライセンスの返却

```

License mode: Smart Licensing
License reservation: Enabled
ASAv Platform License State: Licensed
Active entitlement: ASAv50_PLR, enforce mode: Authorized
Firewall throughput limited to 10 Gbps
Licensed features for this platform:
Maximum VLANs                : 50
Inside Hosts                  : Unlimited
Failover                      : Active/Standby
Encryption-DES                : Enabled
Encryption-3DES-AES          : Enabled
Security Contexts             : 0
Carrier                       : Enabled
AnyConnect Premium Peers     : 250
AnyConnect Essentials        : Disabled
Other VPN Peers               : 250
Total VPN Peers               : 250
AnyConnect for Mobile        : Enabled
AnyConnect for Cisco VPN Phone : Enabled
Advanced Endpoint Assessment  : Enabled
Shared License                : Disabled
Total TLS Proxy Sessions     : 500
Botnet Traffic Filter         : Enabled
Cluster                       : Enabled

```

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(config)# license smart reservation return
WARNING: ASAv platform license state is Limited functionality.

Enter this return code in Cisco Smart Software Manager portal:
UDI: PID:ASAv,SN:9A6ST9AXQ24
Return code: DrTlpZ-8cRT2N-xxxxxx-64ABCD-xXYZeM-qD1
```

ステップ 2 ユニバーサルデバイス識別子 (UDI) をコピーして、Smart Software Manager でこの ASA 仮想インスタンスを見つけることができます。

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 [予約の削除 (Remove Reservation)] 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、柔軟な永続ライセンス予約を無効にします。

```
no license smart flex-model {asav5_plr | asav10_plr | asav30_plr | asav_50_plr |
asav100_plr | asavu_plr }
```

c) 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
```

非柔軟な PLR モードから柔軟な PLR モードへの切り替え

手順

ステップ 1 スマートアカウントから非柔軟な永続ライセンスの予約ライセンスの登録を解除します。

- a) 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(config)# license smart reservation return
WARNING: ASAv platform license state is Limited functionality.

Enter this return code in Cisco Smart Software Manager portal:
UDI: PID:ASAv,SN:9A6ST9AXQ24
Return code: DrT1pZ-8cRT2N-xxxxxx-64ABCD-xXYZeM-qD1
```

- b) ユニバーサルデバイス識別子 (UDI) をコピーして、Smart Software Manager でこの ASA 仮想 インスタンスを見つけることができます。
- c) 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。

- d) ライセンスを解除する ASA 仮想 を UDI を使用して検索します。
- e) [アクション (Actions)] > [削除 (Remove)] を選択し、ASA 仮想 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。
- f) [Remove Reservation] 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。

ステップ 2 永続ライセンスの予約ライセンスを ASA 仮想 から無効にします。

- 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

ステップ 3 ASA 仮想 を柔軟な永続ライセンスの予約ライセンスに登録します。詳細については、[ASA 仮想 永続ライセンスのインストール \(49 ページ\)](#) を参照してください。

柔軟な PLR モードから非柔軟な PLR モードへの切り替え

手順

ステップ 1 スマートアカウントから柔軟な永続ライセンスの予約ライセンスの登録を解除します。

- a) 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(config)# license smart reservation return
WARNING: ASAv platform license state is Limited functionality.

Enter this return code in Cisco Smart Software Manager portal:
UDI: PID:ASAv,SN:9A6ST9AXQ24
Return code: DrT1pZ-8cRT2N-xxxxxx-64ABCD-xXYZeM-qD1
```

- b) ユニバーサルデバイス識別子 (UDI) をコピーして、Smart Software Manager でこの ASA 仮想 インスタンスを見つけることができます。
- c) 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。

- d) ライセンスを解除する ASA 仮想 を UDI を使用して検索します。
- e) [アクション (Actions)] > [削除 (Remove)] を選択し、ASA 仮想 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。
- f) [Remove Reservation] 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。

ステップ 2 永続ライセンスの予約ライセンスを ASA 仮想 から無効にします。

- 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、柔軟な永続ライセンス予約を無効にします。

```
no license smart flex-model {asav5_plr | asav10_plr | asav30_plr | asav_50_plr |
asav100_plr | asavu_plr}
```

ステップ 3 ASA 仮想 を非柔軟な永続ライセンスの予約ライセンスに登録します。詳細については、[ASA 仮想 永続ライセンスのインストール \(49 ページ\)](#) を参照してください。

(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。ライセンス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。

- Cisco Secure Firewall 200
- Firepower 1010
- Firepower 1100
- Cisco Secure Firewall 1200
- Cisco Secure Firewall 3100
- Cisco Secure Firewall 4200
- Cisco Secure Firewall 6100

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（60 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）（75 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）（75 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（66 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）（75 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）（75 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（70 ページ）](#)

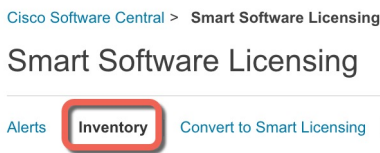
その他のモデル：定期スマートソフトウェアライセンスの設定

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

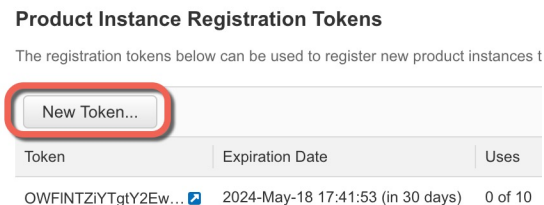
手順

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 ⓘ

- 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。

- 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

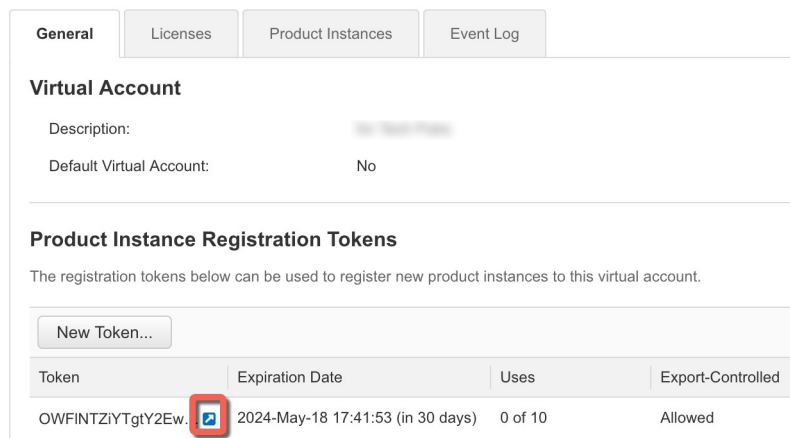
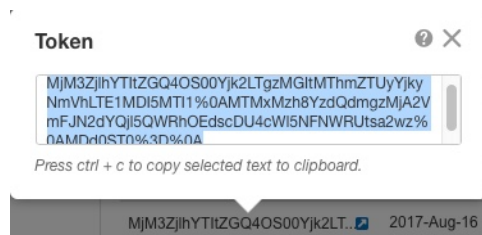


図 12: トークンのコピー



ステップ 2 (任意) 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。

- Cisco ASA で、[構成 (Configuration)] > [デバイス管理 (Device Management)] > [Smart Call-Home] を選択します。
- (任意) [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て、[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。

(注)

認証を使用する HTTP プロキシはサポートされません。

- c) [Apply] をクリックします。
- d) [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)] の順に選択します。
- e) [トランスポート (Transport)] では、[Call Home] オプションボタンをクリックします。

ステップ 3 (任意) Smart Transport の HTTP プロキシを指定します。

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 2 \(62 ページ\)](#) を参照してください。

- a) [トランスポート (Transport)] で、[Smart Transport] オプションボタンをクリックします。
- b) [プロキシ URL] および [プロキシポート (Proxy port)] フィールドにプロキシの IP アドレスまたは FQDN とポート番号を入力します。

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)] > [ライセンス (Licensing)] > [スマートライセンス (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

- Cisco Secure Firewall 1210 : 5 コンテキスト
- Cisco Secure Firewall 1220 : 10 コンテキスト
- Cisco Secure Firewall 1230 : 25 コンテキスト
- Cisco Secure Firewall 1240 : 25 コンテキスト

- Cisco Secure Firewall 1250 : 25 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
- Cisco Secure Firewall 6100 : 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。

- 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 5 [登録 (Register)] をクリックします。

Configuration > Device Management > Licensing > Smart Licensing

To configure an HTTP proxy for Smart Licensing using Call Home, go to [Smart Call-Home](#). If you are using Smart Transport, configure the following:

Enable Smart license configuration

Feature Tier:

Context:

Enable strong-encryption protocol

For a more detailed overview on Cisco Licensing, go to cisco.com/go/licensingguide

Transport Call Home Smart Transport

Configure Transport URL

Default Custom URL

Registration

Proxy URL

Proxy Port

Registration Status:

Effective Running Licenses

License Feature	License Value	License Duration
Maximum Physical Interfaces	Unlimited	
Maximum VLANs	512	
Inside Hosts	Unlimited	
Failover	Active/Active	
Encryption-DES	Enabled	
Encryption-3DES-AES	Disabled	
Security Contexts	5	
Carrier	Disabled	
Secure Client Premium Peers	150	
Secure Client Essentials	Disabled	
Other VPN Peers	150	
Total VPN Peers	150	
Secure Client for Mobile	Enabled	
Secure Client for Cisco VPN Phone	Enabled	
Advanced Endpoint Assessment	Enabled	
Shared License	Disabled	
Total TLS Proxy Sessions	220	

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。

Smart License Registration

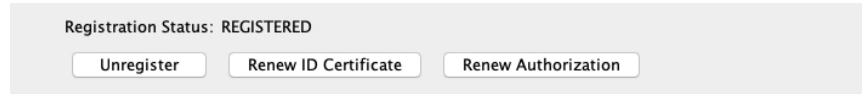
ID Token:

Force registration

(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、ライセンスステ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 : 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](http://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) 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) Cisco ASA で、[設定 (Configuration)] > [デバイス管理 (Device Management)] > [Smart Call-Home]の順に選択します。
- b) (任意) [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て、[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。

(注)

認証を使用する HTTP プロキシはサポートされません。

- c) [サブスクリプションプロファイルの設定 (Configure Subscription Profiles)] 領域で、[ライセンス (License)] プロファイルを編集し、Smart Software Manager オンプレミスに移動するようにライセンスサーバー URL を編集します。
- d) [Deliver Subscriptions Using HTTP transport] 領域で、[Subscribers] URL を選択し、[Edit] をクリックします。
- e) [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`

- f) [OK] をクリックします。
- g) [Apply] をクリックします。
- h) [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)] の順に選択します。
- i) [トランスポート (Transport)] では、[Call Home] オプションボタンをクリックします。

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)] > [ライセンス (Licensing)] > [スマートライセンス (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
- Cisco Secure Firewall 1210 : 5 コンテキスト
- Cisco Secure Firewall 1220 : 10 コンテキスト
- Cisco Secure Firewall 1230 : 25 コンテキスト
- Cisco Secure Firewall 1240 : 25 コンテキスト
- Cisco Secure Firewall 1250 : 25 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
- Cisco Secure Firewall 6100 : 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。

- 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 4 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、任意に HTTP プロキシを指定します。

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 2 \(66 ページ\)](#) を参照してください。

- a) [トランスポート (Transport)] で、[**Smart Transport**] オプションボタンをクリックします。
- b) [カスタム URL (Custom URL)] オプションボタンをクリックして、次の形式で Smart Software Manager オンプレミス URL を設定します。

https://on-prem_ip_address/SmartTransport

- c) (任意) [プロキシ URL (Proxy URL)] の IP アドレスまたは FQDN と [プロキシポート (Proxy Port)] の番号を設定します。

ステップ 5 [登録 (Register)] をクリックします。

Configuration > Device Management > Licensing > Smart Licensing

To configure an HTTP proxy for Smart Licensing using Call Home, go to [Smart Call-Home](#). If you are using Smart Transport, configure the following:

Enable Smart license configuration

Feature Tier:

Context:

Enable strong-encryption protocol

For a more detailed overview on Cisco Licensing, go to cisco.com/go/licensingguide

Transport Call Home Smart Transport

Configure Transport URL

Default Custom URL

Registration

Proxy URL

Proxy Port

Registration Status:

Effective Running Licenses

License Feature	License Value	License Duration
Maximum Physical Interfaces	Unlimited	
Maximum VLANs	512	
Inside Hosts	Unlimited	
Failover	Active/Active	
Encryption-DES	Enabled	
Encryption-3DES-AES	Disabled	
Security Contexts	5	
Carrier	Disabled	
Secure Client Premium Peers	150	
Secure Client Essentials	Disabled	
Other VPN Peers	150	
Total VPN Peers	150	
Secure Client for Mobile	Enabled	
Secure Client for Cisco VPN Phone	Enabled	
Advanced Endpoint Assessment	Enabled	
Shared License	Disabled	
Total TLS Proxy Sessions	220	

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。

Smart License Registration

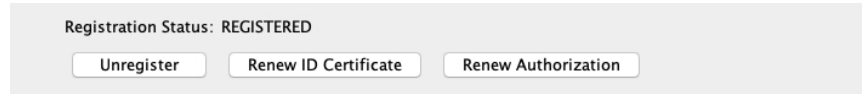
ID Token:

Force registration

(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、ライセンスステ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 [1000/1200/3100/4200/6100/200 永続ライセンスのインストール \(70 ページ\)](#)。

ステップ 2 (任意) [その他のモデル：永続ライセンスの返却 \(74 ページ\)](#)。

1000/1200/3100/4200/6100/200 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 \(74 ページ\)](#) 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 (74 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 AAu3431rGRS00Iq5HQ12vpzg{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) 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
- Cisco Secure Firewall 1210 : 5 コンテキスト
- Cisco Secure Firewall 1220 : 10 コンテキスト
- Cisco Secure Firewall 1230 : 25 コンテキスト

- Cisco Secure Firewall 1240 : 25 コンテキスト
- Cisco Secure Firewall 1250 : 25 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
- Cisco Secure Firewall 6100 : 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:
Au3431rGRS00Iq5HQ12vpcg{uXiTRfVrp7M/zDpirLwYCaq8oSv60yZJuFDVBS2Q1iQ=
```

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（101 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
- Cisco Secure Firewall 1200/3100/4200/6100/200

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 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 [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。または、柔軟な永続ライセンス予約の場合は、モデルを指定します。これにより Smart Software Manager から要求されるライセンスの種類が決定されます。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
- 無制限 : ASAvU

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	<p>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。または、柔軟な永続ライセンス予約の場合は、モデルを指定します。このレベルにより、必要なライセンスが決定されます。</p> <p>100M : ASAv5 1G : ASAv10 2G : ASAv30 10G : ASAv50 20G : ASAv100 無制限 : ASAvU</p>
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	<p>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。</p> <p>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</p> <p>ASAvU : 64 GB の最小メモリを使用する ASAvU を使用している場合、ファイアウォール接続の最大数は 8,000,000 です。</p>
通信事業者	イネーブル

ライセンス	説明
Total TLS Proxy Sessions	<p>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。</p> <p>100M スループット + 任意のメモリ：500</p> <p>1G スループット + 任意のメモリ：500</p> <p>2G スループット：</p> <ul style="list-style-type: none"> • 2 GB ～ 7.9 GB のメモリ：500 • 8 GB 以上のメモリ：1000 <p>10G スループット：</p> <ul style="list-style-type: none"> • 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 <p>20G スループット：</p> <ul style="list-style-type: none"> • 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 <p>無制限のスループット：64GBの最小メモリを使用する ASA vU を使用している場合、TLS プロキシセッションの最大数は 40,000 です。</p>
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	<p>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。</p> <p>オプション <i>Secure Client Advantage</i> または <i>Secure Client Premier</i> ライセンス、最大 :</p> <p>100M スループット + 任意のメモリ : 50</p> <p>1G スループット + 任意のメモリ : 250</p> <p>2G スループット :</p> <ul style="list-style-type: none"> • 2 GB ~ 7.9 GB のメモリ : 250 • 8 GB 以上のメモリ : 750 <p>10G スループット :</p> <ul style="list-style-type: none"> • 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 <p>20G スループット :</p> <ul style="list-style-type: none"> • 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 <p>無制限のスループット : 64GB の最小メモリを使用する ASA vU を使用している場合、セキュアクライアントピアの最大数は 40,000 です。</p>

ライセンス	説明
その他の VPN ピア	<p>(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。</p> <p>100M スループット + 任意のメモリ：50</p> <p>1G スループット + 任意のメモリ：250</p> <p>2G スループット：</p> <ul style="list-style-type: none"> • 2 GB ～ 7.9 GB のメモリ：250 • 8 GB 以上のメモリ：750 <p>10G スループット：</p> <ul style="list-style-type: none"> • 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 <p>20G スループット：</p> <ul style="list-style-type: none"> • 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 <p>無制限のスループット：64GBの最小メモリを使用する ASA vU を使用している場合、他の VPN ピアの最大数は40,000です。</p>

ライセンス	説明
合計VPNピア。全タイプの合計	<p>(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。</p> <p>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 :</p> <ul style="list-style-type: none"> • 2 GB ~ 7.9 GB のメモリ : 250 • 8 GB 以上のメモリ : 750 <p>10G スループット :</p> <ul style="list-style-type: none"> • 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 <p>20G スループット :</p> <ul style="list-style-type: none"> • 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 <p>無制限のスループット : 64GBの最小メモリを使用するASAvUを使用している場合、VPNピアの最大数は40,000です。</p>
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

ライセンス	説明
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

Cisco Secure Firewall 200

次の表に、Secure Firewall 200 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 220 : 30,000	
キャリア	サポートなし。	
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	CSF220 のオプションの <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 50
その他の VPN ピア	Cisco Secure Firewall 220 : 50	
合計 VPN ピア。全タイプの合計	Cisco Secure Firewall 220 : 50	
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	サポートなし	
クラスタ	サポートなし	
VLAN、最大	60	

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 <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 : 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 <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 1120 : 150</i> <i>Firepower 1140 : 400</i> <i>Firepower 1150 : 800</i>
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</i> : 5 <i>Firepower 1140</i> : 10 <i>Firepower 1150</i> : 25
クラスタ	サポートしない	
VLAN、最大	1024	

Cisco Secure Firewall 1210 および 1220

次の表に、Cisco Secure Firewall 1210 および 1220 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 1210 : 200,000 Cisco Secure Firewall 1220 : 300,000	
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	Cisco Secure Firewall 1210 : 320 Cisco Secure Firewall 1220 : 320	
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 1210 : 200 Cisco Secure Firewall 1220 : 300
その他の VPN ピア	Cisco Secure Firewall 1210 : 200 Cisco Secure Firewall 1220 : 300	

ライセンス	Essentials ライセンス	
合計 VPN ピア。全タイプの合計	Cisco Secure Firewall 1210 : 200 Cisco Secure Firewall 1220 : 300	
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 : Cisco Secure Firewall 1210 : 5 Cisco Secure Firewall 1220 : 10
クラスタ	サポートしない	
VLAN、最大	1024	

Cisco Secure Firewall 1230、1240、1250

次の表に、Cisco Secure Firewall 1230、1240、1250 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 1230 : 400,000 Cisco Secure Firewall 1240 : 600,000 Cisco Secure Firewall 1250 : 1,000,000
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。	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	Cisco Secure Firewall 1230 : 1000 Cisco Secure Firewall 1240 : 1000 Cisco Secure Firewall 1250 : 1000
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 : Cisco Secure Firewall 1230 : 500 Cisco Secure Firewall 1240 : 1000 Cisco Secure Firewall 1250 : 1500
その他の VPN ピア	Cisco Secure Firewall 1230 : 500 Cisco Secure Firewall 1240 : 1000 Cisco Secure Firewall 1250 : 1500	
合計 VPN ピア。全タイプの合計	Cisco Secure Firewall 1230 : 500 Cisco Secure Firewall 1240 : 1000 Cisco Secure Firewall 1250 : 1500	
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 : Cisco Secure Firewall 1230 : 25 Cisco Secure Firewall 1240 : 25 Cisco Secure Firewall 1250 : 25
クラスタ	イネーブル	
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	

ライセンス	Essentials 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 <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 3105 : 3,000</i> <i>Cisco Secure Firewall 3110 : 3,000</i> <i>Cisco Secure Firewall 3120 : 7,000</i> <i>Cisco Secure Firewall 3130 : 15,000</i> <i>Cisco Secure Firewall 3140 : 20,000</i>

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 <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 : <i>Firepower 4112</i> : 10,000 <i>Firepower 4115</i> : 15,000 <i>Firepower 4125</i> : 20,000 <i>Firepower 4145</i> : 20,000
その他の VPN ピア	<i>Firepower 4112</i> : 10,000 <i>Firepower 4115</i> : 15,000 <i>Firepower 4125</i> : 20,000 <i>Firepower 4145</i> : 20,000	
合計 VPN ピア。全タイプの合計	<i>Firepower 4112</i> : 10,000 <i>Firepower 4115</i> : 15,000 <i>Firepower 4125</i> : 20,000 <i>Firepower 4145</i> : 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 : 90,000,000 Cisco Secure Firewall 4245 : 180,000,000	
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

Cisco Secure Firewall 6100 シリーズ

次の表に、Secure Firewall 6100 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 6160 : 80,000,000 Cisco Secure Firewall 6170 : 120,000,000	
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 <i>Secure Client Advantage</i> 、 <i>Secure Client Premier</i> 、 <i>Secure Client VPN</i> 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	Cisco Secure Firewall 6160 : 45,000 Cisco Secure Firewall 6170 : 60,000	
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	

Firepower 9300

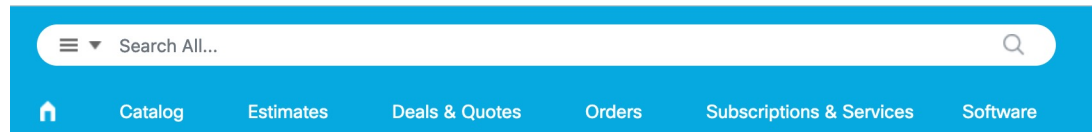
次の表に、Firepower 9300 のライセンス機能を示します。

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 <i>Secure Client Advantage</i> 、 <i>Secure Client Premier</i> 、 <i>Secure Client VPN</i> 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	

モデルごとのライセンス PID

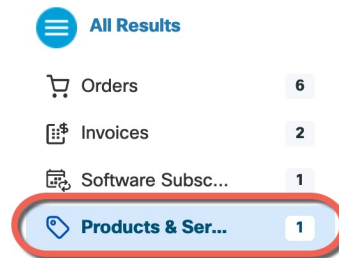
自身でライセンスを追加する必要がある場合は、[Cisco Commerce Workspace](#) で [すべて検索 (Search All)] フィールドを使用します。

図 13: ライセンス検索



結果から、[製品とサービス (Products & Services)] を選択します。

図 14: 結果



ASA 仮想 PID

ASA 仮想 Smart Software Manager 定期およびオンプレミス PID :

- ASAv5 license—L-ASAV5S-K9=
- ASAv10 license—L-ASAV10S-K9=
- ASAv30 license—L-ASAV30S-K9=
- ASAv50 license—L-ASAV50S-K9=
- ASAv100 license—L-ASAV100S-1Y=
- ASAv100 license—L-ASAV100S-3Y=
- ASAv100 license—L-ASAV100S-5Y=
- ASAvU license—L-ASA-V-U-K9=



(注) ASAv100 はサブスクリプションベースのライセンスで、期間は1年、3年、または5年です。

ASA 仮想 永続ライセンス予約 PID :

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 \(11 ページ\)](#) を参照)。

- ASAv5 license—L-ASAV5SR-K9=

- ASAv10 license—L-ASAV10SR-K9=
- ASAv30 license—L-ASAV30SR-K9=
- ASAv50 license—L-ASAV50SR-K9=
- ASAv100 license—L-ASAV100SR-K9=
- ASAvU license—ASA-V-U-ULR-K9=

Cisco Secure Firewall 200 シリーズ PID

Cisco Secure Firewall 200 シリーズ Smart Software Manager 定期およびオンプレミス PID :

- Essentials : CSF_220_BASE_STD。必須。
- 強力な暗号化 (3DES/AES) : CSF_200_ASA_ENC。アカウントに強力な暗号が承認されていない場合にのみ必要です。

Cisco Secure Firewall 200 シリーズ永続ライセンスの予約 PID :

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 \(11 ページ\)](#) を参照)。

- CSF_200_ASA_PLR

Firepower 1010 PID

Firepower 1010 Smart Software Manager 定期およびオンプレミス PID :

- Essentials : L-FPR1000-ASA=。必須。
- Security Plus : L-FPR1010-SEC-PL=。Security Plus ライセンスによってフェールオーバーが有効になります。
- 高度暗号化 (3DES/AES) : L-FPR1K-ENC-K9=。アカウントに強力な暗号が承認されていない場合にのみ必要です。

Firepower 1010 永続ライセンス予約 PID :

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 \(11 ページ\)](#) を参照)。

- L-FPR1K-ASA-BPU=

Firepower 1100 PID**Firepower 1100 Smart Software Manager 定期およびオンプレミス PID：**

- Essentials：L-FPR1000-ASA=。必須。
- 5 コンテキスト：L-FPR1K-ASASC-5=。コンテキストライセンスは追加的です。複数のライセンスを購入します。
- 10 コンテキスト：L-FPR1K-ASASC-10=。コンテキストライセンスは追加的です。複数のライセンスを購入します。
- 高度暗号化（3DES/AES）：L-FPR1K-ENC-K9=。アカウントに強力な暗号が承認されていない場合にのみ必要です。

Firepower 1100 永続ライセンス予約 PID：

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（11 ページ）](#)を参照）。

- L-FPR1K-ASA-BPU=

Secure Firewall 1210/1220 PID**Cisco Secure Firewall 1210/1220 Smart Software Manager 定期およびオンプレミス PID：**

- Essentials：自動的に含まれます。
- 5 コンテキスト：CSF1200-ASASC-5=。コンテキストライセンスは追加的です。複数のライセンスを購入します。
- 高度暗号化（3DES/AES）：L-CSF1200-ENCK9=。アカウントに強力な暗号が承認されていない場合にのみ必要です。

Cisco Secure Firewall 1210/1220 永続ライセンスの予約 PID：

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（11 ページ）](#)を参照）。

- L-CSF1200-ASA-BPU=

Cisco Secure Firewall 1230/1240/1250 PID**Cisco Secure Firewall 1230/1240/1250 Smart Software Manager 定期およびオンプレミス PID：**

- Essentials：自動的に含まれます。

- 5 コンテキスト : CSF1200-ASASC-5=。コンテキストライセンスは追加的です。複数のライセンスを購入します。
- 10 コンテキスト : CSF1200-ASASC-10=。コンテキストライセンスは追加的です。複数のライセンスを購入します。
- 高度暗号化 (3DES/AES) : L-CSF1200-ENCK9=。アカウントに強力な暗号が承認されていない場合にのみ必要です。

Cisco Secure Firewall 1230/1240/1250 永続ライセンスの予約 PID :

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 \(11 ページ\)](#) を参照)。

- L-CSF1200-ASA-BPU=

Secure Firewall 3100 PID

Secure Firewall 3100 Smart Software Manager 定期およびオンプレミス PID :

- Essentials : 自動的に含められます。
- 5 コンテキスト : L-FPR3K-ASASC-5=。コンテキストライセンスは追加的です。複数のライセンスを購入します。
- 10 コンテキスト : L-FPR3K-ASASC-10=。コンテキストライセンスは追加的です。複数のライセンスを購入します。
- キャリア (Diameter、GTP/GPRS、M3UA、SCTP) : L-FPR3K-ASA-CAR=
- 高度暗号化 (3DES/AES) : L-FPR3K-ENC-K9=。アカウントに強力な暗号が承認されていない場合にのみ必要です。

Firepower 3100 永続ライセンス予約 PID :

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 \(11 ページ\)](#) を参照)。

- L-FPR3K-ASA-BPU=

Firepower 4100 PID

Firepower 4100 Smart Software Manager 定期およびオンプレミス PID :

- Essentials : L-FPR4100-ASA=。必須。

- 10 コンテキスト：L-FPR4K-ASASC-10=。コンテキストライセンスは追加的です。複数のライセンスを購入します。
- 230 コンテキスト：L-FPR4K-ASASC-230=。コンテキストライセンスは追加的です。複数のライセンスを購入します。
- 250 コンテキスト：L-FPR4K-ASASC-250=。コンテキストライセンスは追加的です。複数のライセンスを購入します。
- キャリア（Diameter、GTP/GPRS、M3UA、SCTP）：L-FPR4K-ASA-CAR=
- 高度暗号化（3DES/AES）：L-FPR4K-ENC-K9=。アカウントに強力な暗号が承認されていない場合にのみ必要です。

Firepower 4100 永続ライセンス予約 PID：

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](#)（11 ページ）を参照）。

- L-FPR4K-ASA-BPU=

Secure Firewall 4200 PID

Secure Firewall 4200 Smart Software Manager 定期およびオンプレミス PID：

- Essentials：自動的に含められます。
- 5 コンテキスト：L-FPR4200-ASASC-5=。コンテキストライセンスは追加的です。複数のライセンスを購入します。
- 10 コンテキスト：L-FPR4200-ASASC-10=。コンテキストライセンスは追加的です。複数のライセンスを購入します。
- キャリア（Diameter、GTP/GPRS、M3UA、SCTP）：L-FPR4200-ASA-CAR=
- 高度暗号化（3DES/AES）：L-FPR4200-ENC-K9=。アカウントに強力な暗号が承認されていない場合にのみ必要です。

Firepower 4200 永続ライセンス予約 PID：

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](#)（11 ページ）を参照）。

- L-FPR4200-ASA-BPU=

Cisco Secure Firewall 6100 シリーズ PID**Secure Firewall 6100 Smart Software Manager 定期およびオンプレミス PID：**

- Essentials：自動的に含まれます。
- 10 コンテキスト：CSF_6100_ASA_CONTEXT コンテキストライセンスは追加的です。複数のライセンスを購入します。
- キャリア（Diameter、GTP/GPRS、M3UA、SCTP）：CSF_6100_ASA_CARRIER
- 強力な暗号化（3DES/AES）：CSF_6100_ASA_ENCアカウントに強力な暗号が承認されていない場合にのみ必要です。

Cisco Secure Firewall 6100 シリーズ永続ライセンスの予約 PID：

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（11 ページ）](#)を参照）。

- CSF_6100_ASA_PLR

Firepower 9300 PID**Firepower 9300 Smart Software Manager 定期およびオンプレミス PID：**

- Essentials：L-F9K-ASA=。必須。
- 10 コンテキスト：L-F9K-ASA-SC-10=。コンテキストライセンスは追加的です。複数のライセンスを購入します。
- キャリア（Diameter、GTP/GPRS、M3UA、SCTP）：L-F9K-ASA-CAR=
- 高度暗号化（3DES/AES）：L-F9K-ASA-ENCR-K9=。アカウントに強力な暗号が承認されていない場合にのみ必要です。

Firepower 9300 永続ライセンス予約 PID：

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（11 ページ）](#)を参照）。

- L-FPR9K-ASA-BPU=

スマートソフトウェアライセンス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スング、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、ASA の UDI の例を示します。

```
ciscoasa# show license udi
UDI: PID:ASA,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

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、**[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、輸出管理機能が無効になります。その場合、IPSec暗号化が有効になっていると、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
Secure Firewall 4200 の最大接続数の引き上げ	9.23(1)	最大接続数が引き上げられました。 <ul style="list-style-type: none"> • 4225 : 80M → 90M • 4245 : 80M → 180M
ASA 仮想 柔軟な永続ライセンス予約	9.23(1)	柔軟な永続ライセンス予約では、ASA 仮想に割り当てられたRAM および vCPU に関係なく、モデル固有のライセンスを設定できます。 モデルライセンスはASA 仮想のスループットレベルを設定し、ASA 仮想のメモリは最大セキュアクライアントセッション、TLSプロキシセッション、最大同時ファイアウォール接続、およびVLANを決定します。ただし、ASA 仮想メモリプロファイルを小さくすると、セッションと機能の実際の数制限されます。

機能名	プラットフォームリリース	説明
すべての Cisco Secure Firewall 1200 モデルでマルチコンテキストをサポート	9.23(1)	<p>Cisco Secure Firewall 1210/1220 のマルチコンテキストモードのサポートが追加されました。</p> <ul style="list-style-type: none"> • Cisco Secure Firewall 1210CE : 5 コンテキスト。 • Cisco Secure Firewall 1210CP : 5 コンテキスト。 • Cisco Secure Firewall 1220CX : 10 コンテキスト。 <p>スイッチポートはマルチコンテキストモードではサポートされていません。マルチコンテキストモードに変換する前に、すべてのインターフェイスをルーターインターフェイスに変換する必要があります。</p> <p>Cisco Secure Firewall 1230/1240/1250 も最初のリリースでマルチコンテキストモードをサポートしています。</p> <ul style="list-style-type: none"> • Cisco Secure Firewall 1230 : 25 コンテキスト。 • Cisco Secure Firewall 1240 : 25 コンテキスト。 • Cisco Secure Firewall 1250 : 25 コンテキスト。
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)	<p>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。</p> <p>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)]。</p>
ASAvU ライセンス	9.22(1)	<p>ASAvU ライセンスは、32 コアおよび 64 コアの展開で最大のスループットを実現します。このライセンスは、VMware および KVM でのみサポートされています。</p> <p>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)]。</p>
Secure Firewall 4200 の最大接続数の引き上げ	9.20(2)	<p>最大接続数が引き上げられました。</p> <ul style="list-style-type: none"> • 4215 : 15M → 40M • 4225 : 30M → 80M • 4245 : 60M → 80M

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)]。
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。

機能名	プラットフォームリリース	説明
ASA 仮想 のサテライトサーバーのサポート	9.6(2)	<p>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。</p> <p>変更された画面はありません。</p>
Firepower 4100/9300 シャーシ 上の ASA の永続ライセンス予約	9.6(2)	<p>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。</p> <p>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。</p>
ASA 仮想 の永続ライセンス予約	9.5(2.200) 9.6(2)	<p>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。</p> <p>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</p> <p>ASDM サポートはありません。</p>
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)	<p>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。</p> <p>(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。</p> <p>変更された画面はありません。</p>

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)	<p>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。</p> <p>(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。</p> <p>この機能には、FXOS 1.1.3 が必要です。</p> <p>次の画面が変更されました。[Configuration] > [Device Management] > [Licensing] > [Smart License]</p>
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)	<p>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。</p> <p>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]</p>
新しいキャリアライセンス	9.5(2)	<p>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。</p> <p>次の画面が変更されました。[Configuration] > [Device Management] > [Licensing] > [Smart License]</p>
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)	<p>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。</p> <p>次の画面が変更されました。[Configuration] > [Device Management] > [Licensing] > [Smart License]</p>

機能名	プラットフォームリリース	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)	<p>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。</p> <p>次の画面が導入または変更されました。</p> <p>[Configuration] > [Device Management] > [Licensing] > [Smart License] [Configuration] > [Device Management] > [Smart Call-Home] [Monitoring] > [Properties] > [Smart License]</p>

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。