



## ライセンス：スマート ソフトウェア ライセンス（ASA<sub>v</sub>、ASA on Firepower）

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



（注） スマート ソフトウェア ライセンスは、ASA<sub>v</sub> および ASA Firepower シャーシでのみサポートされます。他のモデルは、PAK ライセンスを使用します。[PAK ライセンスについて](#)を参照してください。

- [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](#)（13 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](#)（14 ページ）
- [スマート ソフトウェア ライセンスのデフォルト](#)（15 ページ）
- [ASA<sub>v</sub>：スマート ソフトウェア ライセンシングの設定](#)（15 ページ）
- [Firepower 4100/9300 シャーシ：スマート ソフトウェア ライセンスの設定](#)（24 ページ）
- [モデルごとのライセンス](#)（28 ページ）
- [Smart Software Licensing のモニタリング](#)（32 ページ）
- [スマート ソフトウェア ライセンスの履歴](#)（32 ページ）

## スマート ソフトウェア ライセンスについて

ここでは、スマート ソフトウェア ライセンスの仕組みについて説明します。

## Firepower 4100/9300 シャーシの ASA のスマートソフトウェアライセンス

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スの設定は、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：License Authority 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ス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。



---

(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、ライセンスはマスターアカウントの下のデフォルト仮想アカウントに割り当てられます。アカウント管理者であれば、任意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、または子会社の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と、大量のライセンスおよびデバイスをより簡単に管理できます。

## 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、License Authority に登録できない場合は、オフラインライセンスを設定できます。

## 永続ライセンスの予約

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、License Authority への定期的なアクセスは必要ありません。PAK ライセンスのように、ライセンスを購入し、ASA のライ

センス キーをインストールします。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 を使用します。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。

#### ASAv 永続ライセンスの予約

すべての機能、つまりモデルの正しい最大スループットを備えた標準層を有効にする、モデル固有のライセンスを取得できます。

- ASAv5
- ASAv10
- ASAv30

ASAv 導入時に使用するモデルレベルを選択する必要があります。そのモデルレベルによって、要求するライセンスが決まります。ユニットのモデルレベルを後で変更したい場合は、現在のライセンスを返却し、正しいモデルレベルの新しいライセンスを要求する必要があります。導入済みの ASAv 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 の設定を変更できます。各値については、ASAv のクイックスタートガイドを参照してください。

ライセンスの使用を停止した場合、ASAv 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。

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。

#### Firepower 4100/9300 シャーシ 永続ライセンスの予約

すべての機能、すなわちモデルの正しい最大スループットを備えた標準ティアおよびキャリアライセンスを有効にするライセンスを取得できます。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。

## サテライトサーバ

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 サテライトサーバをインストールできます。サテライト (衛星) は、Smart Software Manager 機能のサブセットを提供し、これによりすべてのローカル デバイスに重要なライセンス サービスが提供可能になります。ライセンス使用を同期するために、定期的に衛星だけが License Authority と同期する必要があります。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。

サテライトサーバでは、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、『[Smart Software Manager satellite](#)』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。アカウントに割り当てられたライセンスを使用できるのは、その仮想アカウントのデバイスのみです。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

### ASAv

ASAv は、評価モードをサポートしていません。Licensing Authority への登録の前に、ASAv は厳しいレート制限状態で動作します。

### 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 シャーシによる Licensing Authority への登録の前に、評価モードで90日間（合計使用期間）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 Licensing Authority に登録をした後、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、License Authority に登録して永続ライセンスを取得する必要があります。

---

## Smart Software Manager 通信

このセクションでは、デバイスの Smart Software Manager に対する通信方法について説明します。

### デバイスの登録とトークン

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。各デバイスを展開するか、または既存のデバイスを登録する場合は、このトークン ID と権限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 Cisco License Authority に登録されます。デバイスがトークンにより登録されると、デバイスとライセンス機関との間の通信に使用する ID 証明書がライセンス機関により発行されます。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。

### License Authority との定期通信

デバイスは 30 日ごとに License Authority と通信します。Smart Software Manager に変更を行う場合、デバイスの認証を更新して変更をすぐに反映させることができます。またはスケジュール設定されたデバイスの通信を待つこともできます。

必要に応じて、HTTP プロキシを設定できます。

#### ASA v

ASA v 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 日間遵守が維持されます。猶予期間終了後は、Licensing Authority に連絡する必要があります、そうしないと ASA v がコンプライアンス違反の状態になります。

#### Firepower 4100/9300

Firepower 4100/9300 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 日間動作します。猶予期間後、Licensing Authority 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なえませんが、動作には影響ありません。

## 非適合状態

デバイスは、次の状況においてコンプライアンス違反になる可能性があります。

- 使用率超過：デバイスが使用不可の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。

- ASAv：ASAv は影響を受けません。
- Firepower 4100/9300：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、標準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。

## Smart Call Home インフラストラクチャ

デフォルトでは、Licensing Authority の URL を指定する Smart Call Home プロファイルがコンフィギュレーションに存在します。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唯一の設定可能なオプションが License Authority の宛先アドレス URL 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、License Authority 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

ASA は Smart Call Home サーバ証明書を発行した 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、**[Configuration] > [Remote Access VPN] > [Certificate Management] > [Trusted Certificate Pool] > [Edit Trusted Certificate Pool Policy]** 画面の **[Automatic Import]** 領域を設定します。

スマートライセンス サーバから受信したサーバ証明書は、[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。

## ライセンスに関する注意事項

次の表に、ライセンスに関する追加情報を示します。

### AnyConnect Plus および Apex ライセンス

AnyConnect Plus および Apex ライセンスは、ライセンスが指定するユーザプールを共有するすべての複数の ASA に適用できる同時使用ライセンスです。スマートライセンスを使用するデバイスでは、実際のプラットフォームに AnyConnect ライセンスを物理的に適用する必要はありません。ただし、同じライセンスを購入して、ソフトウェアセンターへのアクセスやテクニカルサポートを使用するために契約番号を Cisco.com ID に関連付ける必要があります。詳細については、以下を参照してください。

- [『Cisco AnyConnect Ordering Guide』](#)
- [AnyConnect Licensing Frequently Asked Questions \(FAQ\)](#)

### その他の VPN ライセンス

その他の VPN セッションには、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 セッション、全タイプ

- VPN セッションの最大数の合計が、VPN AnyConnect とその他の VPN セッションの最大数よりも多くなっても、組み合わせたセッション数が VPN セッションの制限を超えることはできません。VPN の最大セッション数を超えた場合、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。
- クライアントレス SSL VPN セッションを開始した後、ポータルから AnyConnect クライアントセッションを開始した場合は、合計1つのセッションが使用されています。これに対して、最初に AnyConnect クライアントを（スタンドアロンクライアントなどから）開始した後、クライアントレス SSL VPN ポータルにログインした場合は、2つのセッションが使用されています。

## 暗号化ライセンス

### 高度暗号化：ASAv

ライセンス認証局またはサテライト サーバに接続する前に、高度暗号化 (3DES/AES) を管理接続に使用できるので、ASDM を起動してライセンス認証局に接続することができます。through-the-box トラフィックの場合、License Authority 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 ASAv 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)。ASAv 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、ASAv 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。ASAv 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 ASAv 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。

最初に強力な暗号化なしで ASAv を登録し、後で強力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 ASAv をリロードする必要があります。

2.3.0 より前のサテライト サーバのバージョンでは、ASA 設定で高度暗号化ライセンスを手動で要求する必要があります (エクスポートコンプライアンストークンはサポートされていません)。この場合、ASAv がコンプライアンス違反になると、スループットは厳格に制限されます。

### 高度暗号化：Firepower 4100/9300 シャーシ

スマートソフトウェアライセンシングアカウントから Firepower シャーシ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 が論理デバイスとして展開されると、シャーシから高度暗号化ライセンスが継承されるため、ASDM を起動してスループットに他の機能をすぐに使用できます。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。

エクスポートコンプライアンストークンをサポートしていない 2.3.0 より前のサテライトサーバのバージョンの場合：ASDM には 3DES が必要なため、CLI を使用して ASA 設定で高度暗号化ライセンスを手動で要求する必要があります。ASA がコンプライアンス違反になると、管理トラフィックやこのライセンスを必要とするスループットは許可されません。

### DES : すべてのモデル

DES ライセンスはディセーブルにできません。3DES ライセンスをインストールしている場合、DES は引き続き使用できます。強力な暗号化だけを使用したい場合に DES の使用を防止するには、強力な暗号化だけを使用するようにすべての関連コマンドを設定する必要があります。

## 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
- GTP/GPRS
- SCTP

## 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。

## Firepower 4100/9300 シャーシの ASA のフェールオーバー ライセンス

各 Firepower 4100/9300 シャーシは、License Authority またはサテライト サーバに登録されている必要があります。セカンダリユニットに追加費用はかかりません。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する必要があります。

各 ASA に同じ暗号化ライセンスが必要です。通常の Smart Software Manager (SSM) ユーザの場合、強力な暗号化ライセンスは、Firepower 4100/9300 シャーシで登録トークンを適用すると、対象となるお客様の場合には自動的に有効化されます。古い Cisco Smart Software Manager サテライトが導入されている場合は、以下を参照してください。

ASA ライセンス設定では、その他のライセンスは各フェールオーバー ユニットで一致している必要はなく、各ユニットで別個にライセンスを設定できます。各ユニットには、サーバからの各自のライセンスが必要です。両方のユニットから要求される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。通常、プライマリユニットのみライセンスを設定すれば済みます。

各ライセンス タイプは次のように処理されます：

- **Standard**：デフォルトで各ユニットに **Standard** ライセンスが含まれています。したがって、フェールオーバーのペアでは、サーバから 2 つの標準ライセンスが要求されます。
- **Context**：各ユニットは自身の **Context** ライセンスを要求できます。ただし、デフォルトで **Standard** 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 **Standard** ライセンスの値と、両方のユニットにあるオプションの **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。
  - **Standard** ライセンスに 10 のコンテキストが含まれ、2 つのユニットでは 20 のコンテキストがあります。250 の **Context** ライセンスをアクティブ/スタンバイペアのプライマリユニットに設定した場合を考えます。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、プライマリの **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。
  - **Standard** ライセンスには 10 のコンテキストがあり、2 つユニットがあるため、合計で 20 のコンテキストがあります。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、セカンダリ ユニットにも 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 40 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 22 コンテキストを使用し、他方が 18 コンテキストを使用します (合計 40 の場合)。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。40 コンテキストは制限の範囲内です。
- **キャリア**：ユニット 1 つのみがこのライセンスを要求する必要があり、両方のユニットがこれを使用できます。

- 高度暗号化 (3DES) (2.3.0 より前の Cisco Smart Software Manager サテライト導入の場合のみ) : 各ユニットがサーバからの各自のライセンスを要求する必要があります。他のライセンス設定とは異なり、この設定はスタンバイユニットに複製されます。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、クラスタ展開後にプライマリユニットで ASA CLI を使い高度暗号化ライセンスを有効にする必要があります。高度暗号化 (3DES) ライセンスの評価ライセンスは一切ありません。

## Firepower 4100/9300 シャーシの ASA クラスタ ライセンス

各 Firepower 4100/9300 シャーシは、License Authority またはサテライトサーバに登録されている必要があります。スレーブユニットに追加費用はかかりません。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する必要があります。

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 設定で有効になっているオプションの高度暗号化 (3DES/AES) 機能の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、マスターユニットに対するスマートライセンスの設定のみを行います。設定はスレーブ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、スレーブ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、マスター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スレーブユニットにもキャッシュされ、その中の1つが将来マスター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:

- 標準 : マスターユニットのみがサーバから標準ライセンスを要求します。スレーブユニットにはデフォルトで有効になっている標準ライセンスがあります。そのライセンスを使用するため、サーバに登録を行う必要はありません。
- コンテキスト : マスターユニットのみがサーバからコンテキストライセンスを要求します。デフォルトで標準ライセンスは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。各ユニットの標準ライセンスの値と、マスター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。標準ライセンスは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。マスター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、マスターユニット上で最大80コンテキストを設定できます。各スレーブユニットも、コンフィギュレーションの複製を介して80コンテキストを持つことになります。

- クラスタに Firepower4110 が 3 台あるとします。標準ライセンスは 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。マスター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、マスターユニット上で最大 250 のコンテキストのみを設定できます。各スレーブユニットも、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、マスター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から各自のライセンスを要求します。このライセンスの設定はスレーブユニットに複製されます。
- 高度暗号化 (3DES) (2.3.0 以前の Cisco Smart Software Manager サテライト導入の場合、または追跡目的の場合) : 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から各自のライセンスを要求します。

新しいマスター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、マスター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。古いマスターユニットがスレーブユニットとしてクラスタに再度参加すると、マスター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、スレーブユニットがライセンスを解放する前に、マスター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、キャッシュされたマスター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。

## スマートソフトウェアライセンスの前提条件

- ASAv : デバイスからのインターネットアクセス、または HTTP プロキシアクセスを確保します。また、永続ライセンスの予約を使用することもできます。
- ASAv : デバイスが License Authority の名前を解決できるように DNS サーバを設定します。
- ASAv : デバイスのクロックを設定します。
- ASA v : 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。
- Firepower 4100/9300 シャーシ : 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。

- 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。

- ライセンスは、シスコまたは販売代理店からデバイスを購入した際に、スマート ソフトウェア ライセンシング アカウントにリンクされています。ただし、主導でライセンスを追加する必要がある場合は、[Cisco Commerce Workspace](#) で [Find Products and Solutions] 検索フィールドを使用します。次のライセンス PID を検索します。

図 1: ライセンス検索



#### ASAv PID :

- ASAv5 : L-ASAV5S-K9 =
- ASAv10 : L-ASAV10S-K9=
- ASAv30 : L-ASAV30S-K9=
- ASAv50 : L-ASAV50S-K9=

#### Firepower 4100 PID :

#### Firepower 9300 PID :

## 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。ASAv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ASAv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。ASAvをダウングレードすると、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。

# スマートソフトウェアライセンスのデフォルト

## ASA v

- ASA v のデフォルト設定には、認証局の URL を指定する Smart Call Home プロファイルが含まれています。
- ASA v を導入するときに、機能層とスループットレベルを設定します。現時点では、標準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。
- また、導入時に任意で HTTP プロキシを設定できます。

## Firepower 4100/9300 シャーシ上の ASA

デフォルト設定はありません。標準ライセンス階層、およびその他のオプションライセンスは手動で有効化する必要があります。

# ASA v : 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 v にスマートソフトウェアライセンスを設定する方法を説明します。次の方法の中から 1 つを選択してください。

## 手順

- ステップ 1 [ASA v : 定期スマートソフトウェアライセンスの設定 \(15 ページ\)](#)。
- ステップ 2 [ASA v : サテライト スマートソフトウェアライセンスの設定 \(18 ページ\)](#)。
- ステップ 3 [ASA v : 永続ライセンス予約の設定 \(20 ページ\)](#)。

# ASA v : 定期スマートソフトウェアライセンスの設定

ASA v を展開する場合は、デバイスを事前に設定し、License Authority 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スを有効にすることができます。HTTP プロキシサーバ、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 v を登録する必要がある場合 (Day0 コンフィギュレーションに 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) ASAv 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、ASAv を展開したときに Day0 コンフィギュレーション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** Smart Software Manager (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。

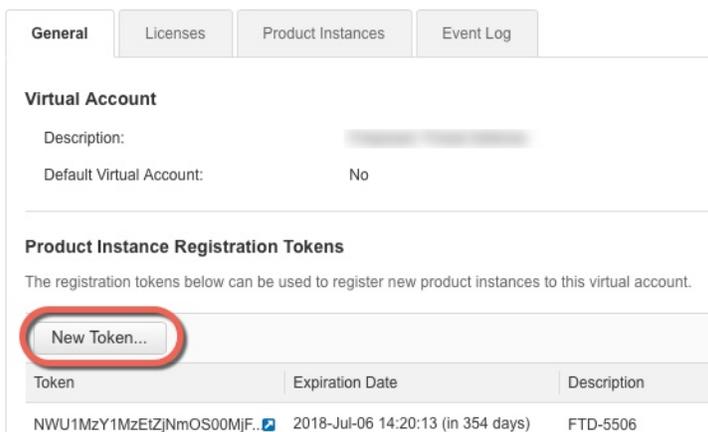
- a) [Inventory] をクリックします。

図 2: インベントリ



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

図 3: 新しいトークン



- c) [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 [Create Token] をクリックします。

- [説明 (Description) ]
- Expire After : 推奨値は 30 日です。
- 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 4: 登録トークンの作成

**Create Registration Token**

This dialog will generate the token required to register your product instances with your Smart Account.

Virtual Account: [Redacted]

Description: [Redacted]

\* Expire After: 30 Days

*Enter the value between 1 and 365, but Cisco recommends a maximum of 30 days.*

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

Create Token Cancel

トークンはインベントリに追加されます。

- d) トークンの右側にある矢印アイコンをクリックして [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 5: トークンの表示

General Licenses Product Instances Event Log

Virtual Account

Description: [Redacted]

Default Virtual Account: No

Product Instance Registration Tokens

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

New Token...

Token	Expiration Date	Description	Export-Controlled	Created By	Actions
MjM3ZjYhYTItZGQ4OS00Yjk2LT...	2017-Aug-16 19:41:53 (in 30 days)	ASA FP 2110 1	Allowed	[Redacted]	Actions

図 6: トークンのコピー

**Token**

MjM3ZjYhYTItZGQ4OS00Yjk2LTgzMGItMThmZTUyYjkyNmVhLTE1MDI5MTI1%0AMTMxMzh8YzdQdmgzMjA2VmFjN2dYQjI5QWRhOEEdscDU4cWI5NFNWRUtsa2wz%0AMFd0ST0%3D%0A

Press ctrl + c to copy selected text to clipboard.

MjM3ZjYhYTItZGQ4OS00Yjk2LT... 2017-Aug-16 1

**ステップ 2** (任意) HTTP プロキシの URL を指定します。

ネットワークでインターネットアクセスに HTTP プロキシを使用する場合、スマートソフトウェアライセンスのプロキシアドレスを設定する必要があります。このプロキシは、一般に Smart Call Home にも使用されます。

- a) [Configuration] > [Device Management] > [Smart Call-Home] を選択します。

- b) [Enable HTTP Proxy] をオンにします。
- c) [Proxy server] および [Proxy port] フィールドにプロキシの IP アドレスとポートを入力します。たとえば、HTTPS サーバのポート 443 を入力します。
- d) [Apply] をクリックします。

**ステップ 3** ライセンス権限付与を設定します。

- a) [Configuration] > [Device Management] > [Licensing] > [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 [Standard] を選択します。  
使用できるのは標準層だけです。

- d) [Throughput Level] ドロップダウンメニューから [100M]、[1G]、[2G]、[10G] を選択します。  
(注) [Enable strong-encryption protocol] チェックボックスはオンにしないでください。  
この設定は、2.3.0 より前のサテライトサーバ専用です。

- e) [Apply] をクリックします。

**ステップ 4** ASAv の License Authority への登録。

- a) [Configuration] > [Device Management] > [Licensing] > [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) [Force registration] チェックボックスをオンにして、License Authority と同期されていない可能性がある登録済みの ASAv を登録します。

たとえば、Smart Software Manager から誤って ASAv 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。

ASAv は、License Authority への登録を試み、設定されたライセンス資格の認証を要求します。

---

## ASAv : サテライトスマートソフトウェアライセンスの設定

この手順は、サテライトスマートソフトウェアライセンスサーバを使用する ASAv に適用されます。

始める前に

Smart Software Manager サテライト OVA ファイルを [Cisco.com](https://www.cisco.com) からダウンロードし、VMwareESXi サーバにインストールおよび設定します。詳細については、『[Smart Software Manager satellite](#)』を参照してください。

## 手順

**ステップ 1** サテライト サーバで登録トークンを要求します。

**ステップ 2** (任意) ASDM で、HTTP プロキシ URL を指定します。

ネットワークでインターネットアクセスに HTTP プロキシを使用する場合、スマートソフトウェアライセンスのプロキシアドレスを設定する必要があります。このプロキシは、一般に Smart Call Home にも使用されます。

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

**ステップ 3** ライセンス サーバの URL を変更して、サテライト サーバに移動します。

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

**https://satellite\_ip\_address/Transportgateway/services/DeviceRequestHandler**

- e) **[OK]** をクリックし、さらに **[Apply]** をクリックします。

**ステップ 4** ASA を License Authority に登録します。

- a) **[Configuration] > [Device Management] > [Licensing] > [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) **[Force registration]** チェックボックスをオンにして、License Authority 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。

- e) **[Register]** をクリックします。

ASA は、License Authority に登録し、設定されたライセンス権限付与の認証を要求します。License Authority は、ご使用のアカウントが許可すれば強力な暗号化 (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。

## ASAv : 永続ライセンス予約の設定

ASAv 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、ASAv の廃棄やモデル層の変更などにより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説明します。

### 手順

ステップ 1 [ASAv パーマネントライセンスのインストール \(20 ページ\)](#)

ステップ 2 (任意) [\(オプション\) ASAv のパーマネントライセンスの返却 \(22 ページ\)](#)

## ASAv パーマネント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 ASAvs の場合は、Smart Software Manager からパーマネントライセンスを要求できます。



(注) パーマネントライセンスの予約については、ASAv 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 ASAv に再使用できません。 [\(オプション\) ASAv のパーマネントライセンスの返却 \(22 ページ\)](#) を参照してください。



(注) 永久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** を使用するなど)、ステップ 1 に示すように、引数を指定せずに **license smart reservation** コマンドを使用して永久ライセンスの予約を再度有効にする必要があります。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

- パーマネントライセンスを購入すると、Smart Software Manager でそれらを使用できます。すべてのアカウントがパーマネント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。
- ASAv の起動後にパーマネントライセンスを要求する必要があります。第 0 日コンフィギュレーションの一部としてパーマネント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 ASAv CLI で、パーマネント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)#
```

次のコマンドが削除されます。

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

通常のスマートライセンスを使用するには、このコマンドの **no** 形式を使用し、上記のコマンドを再入力します。その他の Smart Call Home 設定はそのまま維持されますが、使用されないため、それらのコマンドを再入力する必要はありません。

**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:
ABP:ASAv,S:9AU5ET6UQHD{A8ug5/ljRDaSp3w8uG1feQ{53C13E
ciscoasa#
```

ASAv 導入時に使用するモデルレベル (ASAv5/ASAv10/ASAv30) を選択する必要があります。そのモデルレベルによって、要求するライセンスが決まります。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。既に導入されている ASAv のモデルを変更するには、ハイパーバイザから vCPU と DRAM の設定を新しいモデル要件に合わせて変更できます。これらの値については、ASAv 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 ASAv 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) [ASAv のパーマネントライセンスの返却 \(22 ページ\)](#) 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、ASAv 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** ASAv で、承認コードを次のように入力します。

**license smart reservation install code**

例 :

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

これで、ASAv ライセンスが完全に適用されました。

## (オプション) ASAv のパーマネントライセンスの返却

パーマネントライセンスが不要になった場合 (ASAv を廃棄する場合や ASAv の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)、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容易に解除できなくなります。

手順

**ステップ 1** ASAv 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:
Au3431rGRS00Ig5HQ12vpzg{uXiTRfVrp7M/zDpirLwYCaq8oSv6yZJuFDVBS2QliQ=
```

ただちに ASAv 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。新しいパーマネントライセンスを要求する (**license smart reservation request universal**) か、ASAv のモデルレベルを変更する (電源を切

り vCPU/RAM を変更する) と、このコードを再表示できなくなることに注意してください。必ず、コードをキャプチャして、戻す作業を完了してください。

- ステップ 2** ASA v ユニバーサルデバイス識別子 (UDI) を表示して、Smart Software Manager 内でこの ASA v インスタンスを見つけます。

**show license udi**

例 :

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

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

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

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

- ステップ 4** ライセンスを解除する ASA v を確認し、[Actions] > [Remove] を選択して、ASA v 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。

---

## (オプション) ASA v の登録解除 (定期およびサテライト)

ASA v の登録を解除すると、アカウントから ASA v が削除され、ASA v 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 v に利用することもできます。あるいは、Smart Software Manager (SSM) から ASA v を削除できます。

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** [Unregister] をクリックします。

ASA v がリロードされます。

---

## (オプション) ASAv ID 証明書またはライセンス権限付与の更新 (定期およびサテライト)

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。
- 

## Firepower 4100/9300 シャーシ : 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、Firepower 4100/9300 シャーシにスマートソフトウェアライセンスを設定する方法を説明します。

### 手順

- 
- ステップ 1 [Firepower 4100/9300 シャーシ : 2.3.0 より前のサテライトスマートソフトウェアライセンシングの設定 \(24 ページ\)](#)。事前 2.3.0 バージョンのサテライトサーバを使用して、シャーシを開始する必要があります; CLI で ASA のライセンスの設定事前のライセンスに関する通信を設定する FXOS 構成ガイドを参照してください。
  - ステップ 2 [Firepower 4100/9300 シャーシ : スマートソフトウェアライセンシングの設定の設定 \(27 ページ\)](#)
- 

## Firepower 4100/9300 シャーシ : 2.3.0 より前のサテライトスマートソフトウェアライセンシングの設定

事前 2.3.0 バージョンのサテライトサーバを使用して、シャーシを開始する必要があります; CLI で ASA のライセンスの設定事前のライセンスに関する通信を設定する FXOS 構成ガイドを参照してください。。



- (注) 2.3.0 より前の Smart Software Manager サテライト ユーザの場合 : 高度暗号化 (3DES/AES) ライセンスはデフォルトで有効になっていないため、ASA CLI を使用して高度暗号化ライセンスをリクエストするまで、ASA の設定に ASDM を使用することはできません。VPN を含む他の強力な暗号化機能も、このリクエストを行うまでは使用できません。

### 始める前に

ASA クラスタの場合は、設定作業のために標準出荷単位にアクセスする必要があります。Firepower Chassis Manager で、標準出荷単位を確認します。この手順に示すように、ASA CLI から確認できます。

### 手順

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

**connect module slot console connect asa**

例 :

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

asa>

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

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

- ステップ 2** ASA CLI で、グローバルコンフィギュレーションモードを入力します。デフォルトではインーブルパスワードは空白ですが。

**enable configure terminal**

例 :

```
asa> enable  
Password:  
asa# configure terminal  
asa(config)#
```

- ステップ 3** ASA クラスタの場合は、必要に応じて、このユニットが標準出荷単位であることを確認します。

**show cluster info**

例 :

```
asa(config)# show cluster info
Cluster stbu: On
  This is "unit-1-1" in state SLAVE
    ID : 0
    Version : 9.5(2)
    Serial No.: P3000000025
    CCL IP : 127.2.1.1
    CCL MAC : 000b.fcf8.c192
    Last join : 17:08:59 UTC Sep 26 2015
    Last leave: N/A
  Other members in the cluster:
    Unit "unit-1-2" in state SLAVE
      ID : 1
      Version : 9.5(2)
      Serial No.: P3000000001
      CCL IP : 127.2.1.2
      CCL MAC : 000b.fcf8.c162
      Last join : 19:13:11 UTC Sep 23 2015
      Last leave: N/A
    Unit "unit-1-3" in state MASTER
      ID : 2
      Version : 9.5(2)
      Serial No.: JAB0815R0JY
      CCL IP : 127.2.1.3
      CCL MAC : 000f.f775.541e
      Last join : 19:13:20 UTC Sep 23 2015
      Last leave: N/A
```

別のユニットが標準出荷単位の場合は、接続を終了し、正しいユニットに接続します。接続の終了については、以下を参照してください。

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

**license smart**

例 :

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

**ステップ 5** 機能層を設定します。

**feature tier standard**

使用できるのは標準層だけです。ティアライセンスは、他の機能ライセンスを追加するための前提条件です。

**ステップ 6** 次の機能の 1 つ以上をリクエストします。

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

**feature carrier**

- セキュリティ コンテキスト

**feature context <I-248>**

永続ライセンスの予約では、最大コンテキスト (248) を指定できます。

- 高度暗号化 (3DES/AES)

**feature strong-encryption**

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

## Firepower 4100/9300 シャーシ : 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、License Authority を使用するシャーシ、2.3.0 以降のサテライト サーバのユーザ、または永続ライセンスの予約に適用されます。ライセンス通信を事前設定するには FXOS 設定ガイドを参照してください。2.3.0 より前のサテライト サーバでは、最初に CLI でライセンスを設定する必要があります。サテライト サーババージョン 2.3.0 以降では、高度暗号化 (3DES/AES) エクスポート準拠トークンがサポートされているため、他のライセンス権限付与を要求する前に ASDM を実行できます。

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。



- (注) 2.3.0 より前のサテライト サーバユーザの場合は、[Firepower 4100/9300 シャーシ : 2.3.0 より前のサテライト スマートソフトウェアライセンシングの設定 \(24 ページ\)](#) を参照して CLI でライセンスを設定してください。

### 始める前に

ASA クラスタの場合は、設定作業のために標準出荷単位にアクセスする必要があります。Firepower Chassis Manager で、標準出荷単位を確認します。

### 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** **[Feature Tier]** ドロップダウンメニューから **[Standard]** を選択します。  
使用できるのは標準層だけです。
- ステップ 3** **2.3.0 より前のサテライトサーバユーザのみ** : **[Strong Encryption]** ライセンスを無効にしないでください。これは ASDM アクセスに必要です。

**ステップ4** (任意) [Mobile SP] [Carrier] を確認します。

**ステップ5** (任意) [Context] ドロップダウンメニューから、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。

## 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。

### ASAv

次の表に、ASAv シリーズのライセンス機能を示します。

ライセンス	Standard ライセンス
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	ASAv5 : 50,000 ASAv10 : 100,000 ASAv30 : 500,000
キャリア	イネーブル
合計 TLS プロキシセッション	ASAv5: 500 ASAv10 : 500 ASAv30 : 1000
VPN ライセンス	

ライセンス	Standard ライセンス	
AnyConnect ピア	ディセーブル	オプションの <i>AnyConnect Plus</i> または <i>Apex</i> ライセンス、最大 : <i>ASAv5</i> : 50 <i>ASAv10</i> : 250 <i>ASAv30</i> : 750
その他の VPN ピア	<i>ASAv5</i> : 50 <i>ASAv10</i> : 250 <i>ASAv30</i> : 1000	
合計 VPN ピア。全タイプの合計	<i>ASAv5</i> : 50 <i>ASAv10</i> : 250 <i>ASAv30</i> : 1000	
<b>一般ライセンス</b>		
スループット レベル	<i>ASAv5</i> : 100 Mbps <i>ASAv10</i> : 1 Gbps <i>ASAv30</i> : 2 Gbps	
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	サポートなし	
VLAN、最大	<i>ASAv5</i> : 25 <i>ASAv10</i> : 50 <i>ASAv30</i> : 200	
RAM、vCPUs	<i>ASAv5</i> : 1 GB、1 vCPU <i>ASAv10</i> : 2 GB、1 vCPU <i>ASAv30</i> : 8 GB、4 vCPU	

## Firepower 4100 シリーズ ASA アプリケーション

次の表に、Firepower 4100 シリーズ ASA アプリケーションのライセンス機能を示します。

ライセンス	Standard 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 4110 : 10,000,000 Firepower 4120 : 15,000,000 Firepower 4140 : 25,000,000 Firepower 4150 : 35,000,000	
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	Firepower 4110 : 10,000 その他すべて : 15,000	
VPN ライセンス		
AnyConnect ピア	ディセーブル	オプションの <i>AnyConnect Plus</i> または <i>Apex</i> ライセンス : <i>Firepower 4110 : 10,000</i> その他すべて : 20,000
その他の VPN ピア	Firepower 4110 : 10,000 その他すべて : 20,000	
合計 VPN ピア。全タイプの合計	Firepower 4110 : 10,000 その他すべて : 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、10 単位
クラスタ	イネーブル	
VLAN、最大	1024	

## Firepower 9300 ASA アプリケーション

次の表に、Firepower 9300 ASA アプリケーションのライセンス機能を示します。

ライセンス	Standard 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-44 : 60,000,000、最大 70,000,000 (3 モジュールを搭載したシャーシ) Firepower 9300 SM-36 : 60,000,000、最大 70,000,000 (3 モジュールを搭載したシャーシ) Firepower 9300 SM-24 : 55,000,000、最大 70,000,000 (3 モジュールを搭載したシャーシ)	
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		
AnyConnect ピア	ディセーブル	オプションの <i>AnyConnect Plus</i> または <i>Apex</i> 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、10 単位
クラスタ	イネーブル	
VLAN、最大	1024	

## Smart Software Licensing 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することもできます。

### 現在のライセンスの表示

ライセンスを表示するには、次の画面を参照してください。

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

### スマートライセンスステータスの表示

ライセンスステータスを表示するには、次のコマンドを参照してください。

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

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

### UDI の表示

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

**show license udi**

次に、ASA v の UDI の例を示します。

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

## 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
ASA v 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
ASAv のサテライト サーバのサポート	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>
ASAv 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、ASAv 用に永続ライセンスを要求できます。9.6(2) では、Amazon Web サービスの ASAv 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。</p> <p><b>license smart reservation、license smart reservation cancel、license smart reservation install、license smart reservation request universal、license smart reservation return</b></p> <p>ASDM サポートはありません。</p>

機能名	プラットフォーム リリース	説明
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、ASAv はライセンス登録状態を保持しません。 [Configuration] &gt; [Device Management] &gt; [Licensing] &gt; [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>
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] &gt; [Device Management] &gt; [Licensing] &gt; [Smart License]</p>

機能名	プラットフォーム リリース	説明
サーバ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。  <b>[Configuration] &gt; [Remote Access VPN] &gt; [Certificate Management] &gt; [Trusted Certificate Pool] &gt; [Edit Trusted Certificate Pool Policy]</b></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спекションもサポートします。Firepower 9300 上の ASA の場合、<b>feature mobile-sp</b> コマンドは <b>feature carrier</b> 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。  <b>[Configuration] &gt; [Device Management] &gt; [Licensing] &gt; [Smart License]</b></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。  <b>[Configuration] &gt; [Device Management] &gt; [Licensing] &gt; [Smart License]</b></p>

機能名	プラットフォーム リリース	説明
ASAv のシスコスマートソフトウェア ライセンスング	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 ASAv を導入したり導入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><b>[Configuration] &gt; [Device Management] &gt; [Licensing] &gt; [Smart License]</b>  <b>[Configuration] &gt; [Device Management] &gt; [Smart Call-Home] [Monitoring] &gt; [Properties] &gt; [Smart License]</b></p>