ライセンス：スマート ソフトウェア ライセンス（ASAv、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、ASAv 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

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。

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

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

- Firepower 4100/9300 シャーシ：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。

（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できます。

ASAv 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
- ASAv50

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。モデル レベルは、要求するライセンスを決定します。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。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。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。

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 2100 永続ライセンスの予約

すべての機能を有効にするライセンス（セキュリティ コンテキストが最大の標準ティア）を取得できます。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。

Firepower 2100 および Firepower 4100/9300 シャーシ のサテライト 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、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 2100

Licensing Authority への登録の前に、Firepower 210 は評価モードで 90 日間（合計使用時間）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、License Authority 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 タイプ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。

ASAv 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、そうしないとASAvがコンプライアンス違反の状態になります。

Firepower 4100/9300 シャーシ 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。
- 通信の不足：デバイスが再認証のためにライセンス機関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 2100 の ASA：特別なライセンスが必要な機能への設定変更は行えなくなりますが、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。
- Firepower 4100/9300 シャーシの ASA：特別なライセンスが必要な機能への設定変更は行えなくなりますが、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 からの指示がない限り、ライセンス認証局の URL を変更しないでください。

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

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

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

スマート ライセンス証明書の管理

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、 **auto-update** コマンドを設定します。

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

License Authority 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 License Authority 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。

高度暗号化：Firepower 2100

License Authority 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 を起動できます。ASDM アクセスは、デフォルトの暗号化を適用する管理専用インターフェイスでのみ使用できることに注意してください。高度暗号化ライセンスに接続して取得するまで、through the box トラフィックは許可されません。

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

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、ASA がコンプライアンス違反になると、スルートラフィックは許可されません。

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 を起動してスルートラフィック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。

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トラフィックは許可されません。

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もあります。

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

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

VLAN、最大

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

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

ボットネット トラフィック フィルタ ライセンス

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

フェールオーバーまたは ASA クラスタ ライセンス

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 2100 のフェールオーバー ライセンス

各 Firepower 2100 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。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。2.3.0 より前の 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。

アクティブ/スタンバイ フェールオーバーでは、アクティブ装置にのみスマートライセンシングを設定できます。アクティブ/アクティブ フェールオーバーでは、フェールオーバー グループ 1 がアクティブになっている装置にのみスマートライセンシングを設定できます。設定はスタンバイ ユニットに複製されますが、スタンバイ ユニットは設定を使用しません。この設定はキャッシュの状態のままになります。アクティブな装置のみサーバ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:

- Standard：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 Stardard 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 Standard 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 Standard 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。
  - Standard ライセンスには 2 つのコンテキストが含まれています。2 つの Firepower 2130 ユニットの場合、これらのライセンスは最大 4 つのコンテキストを追加します。アクティブ/スタンバイペアのアクティブな装置に 30 Context ライセンスを設定します。この場合、集約されたフェールオーバーライセンスには 34 のコンテキストが含まれています。しかし、ユニットごとのプラットフォームの制限が 30 であるため、結合されたライセンスでは最大 30 のコンテキストが許容されます。この場合では、アクティブな Context ライセンスとして 25 のコンテキストのみを設定できます。
  - Standard ライセンスには 2 つのコンテキストが含まれています。2 つの Firepower 2130 ユニットの場合、これらのライセンスは最大 4 つのコンテキストを追加します。アクティブ/アクティブペアのプライマリユニットに 10 Context ライセンスを設定します。この場合、集約されたフェールオーバーライセンスには 14 のコンテキストが含まれています。たとえば、一方のユニットが 9 コンテキストを使用し、他方が 5 コンテキストを使用します（合計 14 の場合）。ユニットごとのプラットフォームの制限が 30 であるため、結合されたライセンスでは最大 30 のコンテキストが許容されます。14 コンテキストは制限の範囲内です。
- 高度暗号化（3DES/AES）（2.3.0 より前の Cisco Smart Software Manager サテライト導入の場合のみ）：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。Smart Software Manager 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、アクティブユニットで ASA CLI を使用して高度暗号化（3DES）ライセンスを有効にする必要があります。高度暗号化（3DES/AES）ライセンスの評価ライセンスは一切ありません。

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

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。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。

アクティブ/スタンバイ フェールオーバーの ASA ライセンス設定では、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シングを設定できます。設定はスタンバイ ユニットに複製されますが、スタンバイ ユニットは設定を使用しません。この設定はキャッシュの状態のままになります。アクティブな装置のみサーバ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:

- Standard：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 Stardard 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 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、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。
  - 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/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。
  - 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（合計 30 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。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）：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、クラスタ展開後にアクティブな装置で 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。

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

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。

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、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えます。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のみ）：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。Smart Software Manager 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、クラスタ展開後にマスター ユニットで ASA CLI を使用して高度暗号化（3DES）ライセンスを有効にする必要があります。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）ライセンスの評価ライセンスは一切ありません。

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。

Smart Software Licensing 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、このリンクをクリックして新しいアカウントをセットアップしてください。Smart Software Manager では、組織のマスター アカウントを作成できます。

- Cisco Commerce Workspace から 1 つ以上のライセンスを購入します。ホーム ページの [Find Products and Solutions] 検索フィールドで、ライセンス PID を検索します。一部のライセンスは無料ですが、スマート ソフトウェア ライセンス アカウントにそれらを追加する必要があります。

- ASAv および Firepower 2100：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、またはサテライト サーバへの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 および Firepower 2100：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 および Firepower 2100：デバイスのクロックを設定します。 Firepower 2100 では、FXOS でクロックを設定します。

- ASA□：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。

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

ASAv

- ASAv 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。

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

- ASAv 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。

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

- また、導入時に任意で HTTP プロキシを設定できます。

```
call-home
  http-proxy ip_address port port
```

Firepower 2100

Firepower 2100 のデフォルト設定には、Licensing Authority の URL を指定する「License」という Smart Call Home プロファイルが含まれています。

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

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。

ASAv：スマート ソフトウェア ライセンシングの設定

このセクションでは、ASAv 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 ASAv：定期スマート ソフトウェア ライセンシングの設定 （18 ページ）。

ステップ 2 ASAv：永続ライセンス予約の設定 （22 ページ）.

ASAv：定期スマート ソフトウェア ライセンシングの設定

ASAv 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 ライセンシング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 ASAv 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、次の作業を行います。

手順

ステップ 1 ライセンスの設定と ASAv の登録 （18 ページ）。展開時に設定した HTTP プロキシまたは権限付与を変更する必要がある場合、または ASAv を展開したときに ID トークンを含めなかった場合は、この手順を完了します。

ステップ 2 （オプション）ASAv の登録解除 （22 ページ） または （オプション）ASAv アイデンティティ証明書またはライセンス資格の更新 （22 ページ） も可能です。

ライセンスの設定と ASAv の登録

オプションの HTTP プロキシを設定し、ライセンス権限付与を要求し、ASAv を登録するには、次の手順を実行します。

（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

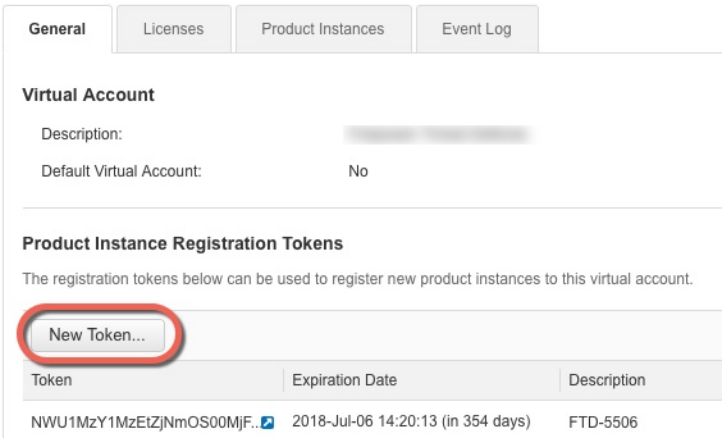
ステップ 1 Smart Software Manager（Cisco Smart Software Manager）で、このデバイスを追加するバーチャル アカウントの登録トークンを要求してコピーします。

a) [Inventory] をクリックします。

図 *1*：インベントリ

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

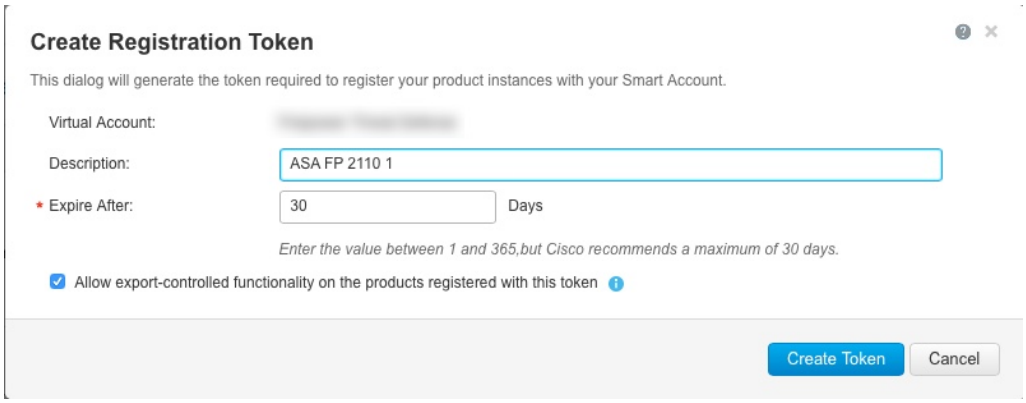
図 *2*：新しいトークン



c) [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。

- **Description**
- Expire After：推奨値は 30 日です。
- Allow export-controlled functionaility 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 [Token] ダイアログボックスを開き、トークン ID をクリップボードにコピーできるようにします。ASA の登録が必要なときに後の手順で使用するために、このトークンを準備しておきます。

図 *4*: トークンの表示

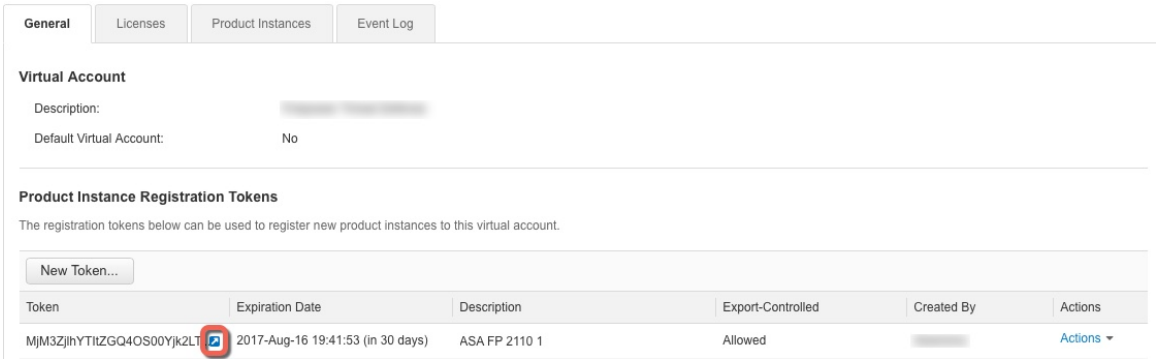
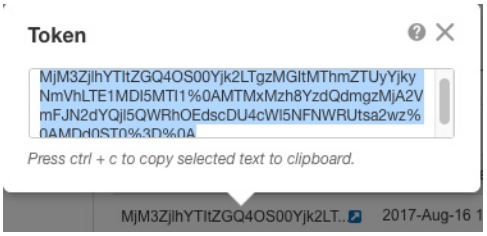


図 *5*: トークンのコピー



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

call-home

http-proxy *ip_address* **port** *port*

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。

例：

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

ステップ 3 ライセンス権限付与を設定します。

a) ライセンス スマート コンフィギュレーション モードを開始します。

license smart

例：

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

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

b) 機能層を設定します。

feature tier standard

使用できるのは標準層だけです。

c) スループット レベルを設定します。

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

例：

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

a) ライセンス スマート モードを終了して、変更を適用します。

exit

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

例：

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

ステップ 4 ASAv の License Authority への登録.

License Authority に ASAv を登録すると、ASAv と License Authority の間の通信に使用する ID 証明書が発行されます。また、該当する仮想アカウントに ASAv が割り当てられます。通常、この手順は 1 回で済みます。ただし、通信の問題などが原因でアイデンティティ証明書の期限が切れた場合は、ASAv の再登録が必要になります。

a) ASAv の登録トークンを入力します。

license smart register idtoken *id_token* [**force**]

例：

force キーワードを使用すると、License Authority と同期されていない可能性がある登録済みの ASAv を登録できます。たとえば、Smart Software Manager から誤って ASAv を削除した場合に **force** を使用します。

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。

例：

```
ciscoasa# license smart register idtoken YjE3Njc5MzYtMGQzMi00OTA4
LWJhODItNzBhMGQ5NGRlYjUxLTE0MTQ5NDAy%0AODQzNzl8NXk2bzV3SDE0ZkgwQk
```

```
dYRmZ1NTNCNGlvRnBHUFpjcm02WTB4TU4w%0Ac2NnMD0%3D%0A
```

（オプション）ASAv の登録解除

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

手順

ASAv の登録解除

license smart deregister

ASAv がリロードされます。

（オプション）ASAv アイデンティティ証明書またはライセンス資格の更新

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 アイデンティティ証明書を更新します。

license smart renew id

ステップ 2 Renew the license entitlement:

license smart renew auth

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 （23 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 （25 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 （25 ページ）を参照してください。

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 | 10G}
```

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{A8ug5/1jRDaSp3w8uGlfeQ{53C13E
ciscoasa#
```

ASAv 導入時に使用するモデル レベル（ASAv5/ASAv10/ASAv30/ASAv50）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（25 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 AAu3431rGRS00Ig5HQl2vpzg{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:
Au3431rGRS00Ig5HQl2vpcg{uXiTRfVrp7M/zDpirLwYCaq8oSv60yZJuFDVBS2QliQ=
```

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 ASAv 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 ASAv インスタンスを見つけます。

show license udi

例：

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

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

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

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

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

Firepower 2100：スマート ソフトウェア ライセンシングの設定

この項では、Firepower 2100 にスマート ソフトウェア ライセンシング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 Firepower 2100：定期スマート ソフトウェア ライセンシングの設定 （26 ページ）。

（オプション）Firepower 2100 の登録解除（定期およびサテライト） （35 ページ） または （オプション）Firepower 2100 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） （36 ページ） も可能です。

ステップ 2 Firepower 2100：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 （30 ページ）。

（オプション）Firepower 2100 の登録解除（定期およびサテライト） （35 ページ） または （オプション）Firepower 2100 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） （36 ページ） も可能です。

ステップ 3 Firepower 2100：永続ライセンス予約の設定 （32 ページ）。

Firepower 2100：定期スマート ソフトウェア ライセンシングの設定

この手順は、License Authority を使用した ASA に適用されます。

手順

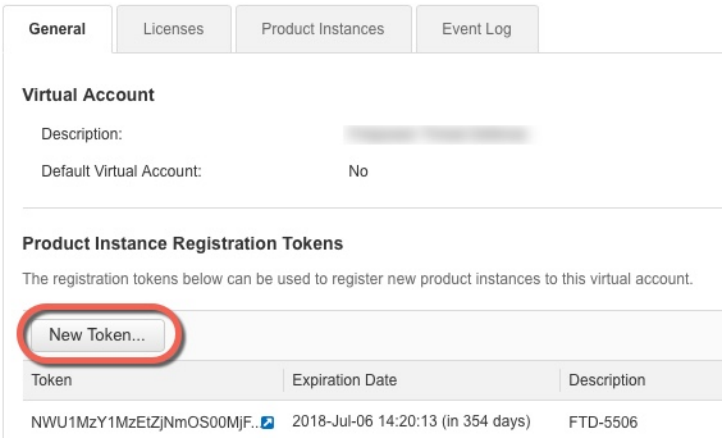
ステップ 1 Smart Software Manager（Cisco Smart Software Manager）で、このデバイスを追加するバーチャル アカウントの登録トークンを要求してコピーします。

a) [Inventory] をクリックします。

図 *6*：インベントリ

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

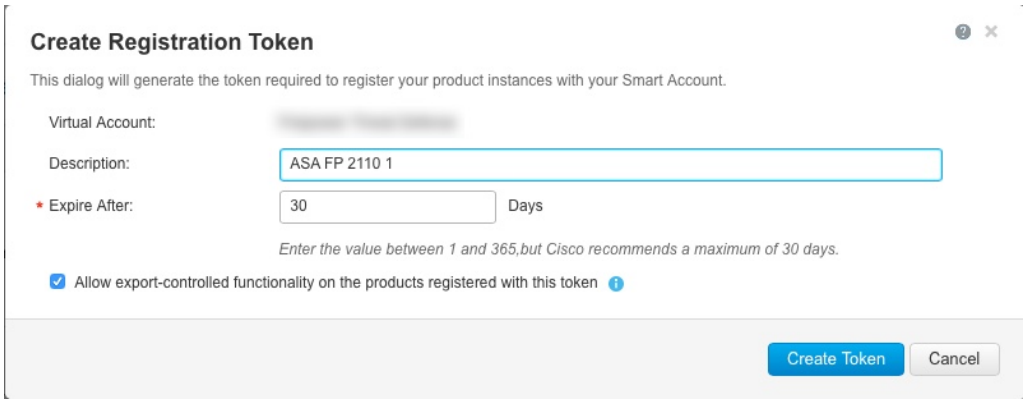
図 *7*：新しいトークン



c) [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。

- **Description**
- Expire After：推奨値は 30 日です。
- Allow export-controlled functionaility on the products registered with this token：輸出コンプライアンス フラグを有効にします。

図 *8*：登録トークンの作成



トークンはインベントリに追加されます。

d) トークンの右側にある矢印アイコンをクリックして [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

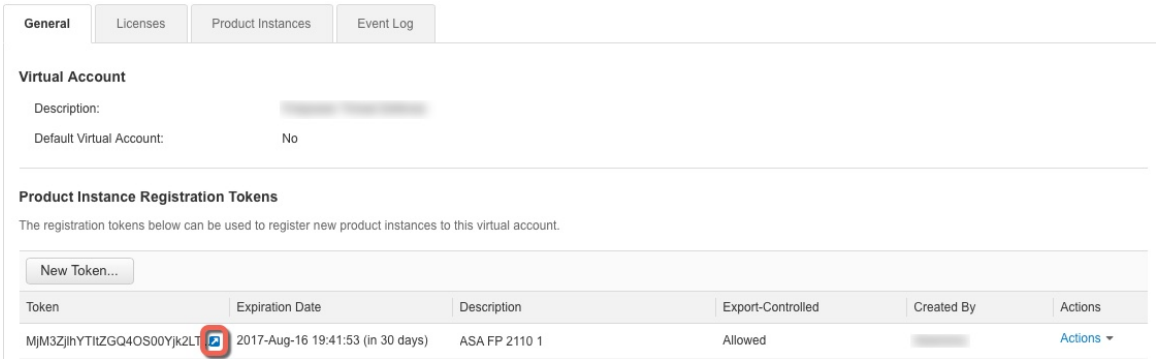
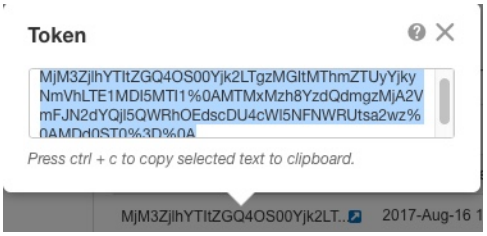


図 *10*：トークンのコピー



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

call-home

http-proxy *ip_address* **port** *port*

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。

例：

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

ステップ 3 ASA でライセンス権限付与を要求します。

a) ライセンス スマート コンフィギュレーション モードを開始します。

license smart

例：

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

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

b) 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。

c) セキュリティ コンテキストのライセンスを要求します。

feature context *number*

コンテキストの最大数は、モデルによって異なります。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。

例：

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

ステップ 4 手順 1 でコピーしたトークンを使用して ASA を登録します。

license smart register idtoken *id_token*

例：

```
ciscoasa# license smart register idtoken YjE3Njc5MzYtMGQzMi00OTA4
LWJhODItNzBhMGQ5NGRlYjUxLTE0MTQ5NDAy%0AODQzNzl8NXk2bzV3SDE0ZkgwQk
dYRmZ1NTNCNGlvRnBHUFpjcm02WTB4TU4w%0Ac2NnMD0%3D%0A
```

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

例：

```
ciscoasa# show license summary

Smart Licensing is ENABLED

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

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

License Usage:
  License                Entitlement tag              Count Status
```

```
------------------------------------------------------------------------
regid.2014-08.com.ci... (FP2110-ASA-Std)                    1 AUTHORIZED
```

Firepower 2100：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

この手順は、サテライト スマート ソフトウェア ライセンシング サーバを使用する ASA 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 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） ASA で、HTTP プロキシ URL を指定します。

call-home

http-proxy *ip_address* **port** *port*

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。

例：

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

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。

call-home

profile License

destination address http https://*satellite_ip_address***/Transportgateway/services/DeviceRequestHandler**

例：

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

ステップ 4 ASA でライセンス権限付与を要求します。

a) ライセンス スマート コンフィギュレーション モードを開始します。

license smart

例：

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

b) 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。

c) セキュリティ コンテキストのライセンスを要求します。

feature context *number*

コンテキストの最大数は、モデルによって異なります。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。

例：

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

ステップ 5 手順 1 で要求したトークンを使用して ASA を登録します。

license smart register idtoken *id_token*

例：

```
ciscoasa# license smart register idtoken YjE3Njc5MzYtMGQzMi00OTA4
LWJhODItNzBhMGQ5NGRlYjUxLTE0MTQ5NDAy%0AODQzNzl8NXk2bzV3SDE0ZkgwQk
dYRmZ1NTNCNGlvRnBHUFpjcm02WTB4TU4w%0Ac2NnMD0%3D%0A
```

ASA は、サテライト サーバに登録し、設定されたライセンス権限付与の認証を要求します。サテライト サーバは、ご使用のアカウントが許可すれば高度暗号化（3DES/AES）ライセンスも適用します。ライセンスのステータスと使用状況をチェックするには、**show license summary** コマンドを使用します。

例：

```
ciscoasa# show license summary

Smart Licensing is ENABLED

Registration:
  Status: REGISTERED
  Smart Account: Biz1
  Virtual Account: IT
  Export-Controlled Functionality: Allowed
```

```
  Last Renewal Attempt: None
  Next Renewal Attempt: Mar 19 20:26:29 2018 UTC

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

License Usage:
  License                 Entitlement tag               Count Status
  -----------------------------------------------------------------------------
  regid.2014-08.com.ci... (FP2110-ASA-Std)                    1 AUTHORIZED
```

Firepower 2100：永続ライセンス予約の設定

Firepower 2100 に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 Firepower 2100 永続ライセンスのインストール （32 ページ）。

ステップ 2 （任意） （オプション）Firepower 2100 永続ライセンスの返却 （34 ページ）.

Firepower 2100 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標準ティア）。

（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。（オプション）Firepower 2100 永続ライセンスの返却 （34 ページ）を参照してください。

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。

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。（オプション）Firepower 2100 永続ライセンスの返却 （34 ページ）を参照してください。

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

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

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

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

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

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

ステップ 5 ASA で、承認コードを次のように入力します。

license smart reservation install *code*

例：

```
ciscoasa# license smart reservation install AAu3431rGRS00Ig5HQl2vpzg{MEYCIQCBw$
ciscoasa#
```

ステップ 6 ASA でライセンス権限付与を要求します。

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。

a) ライセンス スマート コンフィギュレーション モードを開始します。

license smart

例：

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

b) 機能層を設定します。

feature tier standard

使用できるのは標準層だけです。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。

c) セキュリティ コンテキストのライセンスを要求します。

feature context *number*

コンテキストの最大数はモデルによって異なります。これは、永続ライセンスには最大数のコンテキストが含まれているためで、最大数から 2 つのデフォルト コンテキストを除いたものを要求する必要があります。

例：

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

（オプション）Firepower 2100 永続ライセンスの返却

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

手順

ステップ 1 ASA で返却コードを次のように生成します。

license smart reservation return

例：

```
ciscoasa# license smart reservation return
Enter this return code in the Cisco Smart Software Manager portal:
Au3431rGRS00Ig5HQl2vpcg{uXiTRfVrp7M/zDpirLwYCaq8oSv60yZJuFDVBS2QliQ=
```

ただちに ASA のライセンスがなくなり、評価状態に移行します。このコードを再度表示する必要がある場合は、このコマンドを再入力します。新しい永続ライセンス（**license smart reservation request universal**）を要求すると、このコードを再表示できなくなることに注意してください。必ず、コードをキャプチャして、戻す作業を完了してください。

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

show license udi

例：

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

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

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

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

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

パーマネント ライセンスが使用可能なライセンスのプールに戻されます。

（オプション）Firepower 2100 の登録解除（定期およびサテライト）

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。

手順

ASA の登録解除：

license smart deregister

その後、ASA はリロードします。

（オプション）Firepower 2100 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 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 アイデンティティ証明書を更新します。

license smart renew id

ステップ 2 Renew the license entitlement:

license smart renew auth

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

この手順は、License Authority を使用するシャーシ、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。方法を前提条件として設定するには、FXOS 設定ガイド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。

（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 からも確認できます。

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。デフォルトではイネーブル パスワードは空白です。

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 インスペクション）

  feature carrier

- セキュリティ コンテキスト

  feature context *<1-248>*

永続ライセンスの予約では、最大コンテキスト（248）を指定できます。

- **2.3.0 より前のサテライト サーバ ユーザのみの場合**：高度暗号化（3DES/AES）

  feature strong-encryption

例：

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

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

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。

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 ASAv50：2,000,000
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 ASAv50：10,000
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 *AnyConnect Plus* または *Apex* ライセンス、最大： *ASAv5: 50* *ASAv10：250* *ASAv30：750* *ASAv50：10,000*
その他の VPN ピア	ASAv5：50 ASAv10：250 ASAv30：1000 ASAv50：10,000	
合計 VPN ピア。全タイプの合計	ASAv5：50 ASAv10：250 ASAv30：1000 ASAv50：10,000	
一般ライセンス		
スループット レベル	ASAv5：100 Mbps ASAv10：1 Gbps ASAv30：2 Gbps ASAv50：10 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	ASAv5：25 ASAv10：50 ASAv30：200 ASAv50：1024	

ライセンス	Standard ライセンス
RAM、vCPUs	ASAv5：1 GB、1 vCPU （オプション）ASAv5：1.5 GB、1 vCPU（9.8(2) 以降）。ASAv5 でメモリの枯渇が発生する場合は、追加のメモリを割り当てることができます。 ASAv10：2 GB、1 vCPU ASAv30：8 GB、4 vCPU ASAv50：16 GB、8 vCPU

Firepower 2100 シリーズ

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

ライセンス	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 2110：1,000,000 Firepower 2120：1,500,000 Firepower 2130：2,000,000 Firepower 2140：3,000,000
通信事業者	サポートしないSCTP インスペクション マップはサポートされていませんが、ACL を使用した SCTP ステートフル インスペクションがサポートされています。
合計 TLS プロキシセッション	Firepower 2110：4,000 Firepower 2120：8,000 Firepower 2130：8,000 Firepower 2140：10,000
VPN ライセンス	

ライセンス	Standard ライセンス	
AnyConnect ピア	ディセーブル	オプションの *AnyConnect Plus* または *Apex* ライセンス、最大： *Firepower 2110：1,500* *Firepower 2120：3,500* *Firepower 2130：7,500* *Firepower 2140：10,000*
その他の VPN ピア	Firepower 2110：1,500 Firepower 2120：3,500 Firepower 2130：7,500 Firepower 2140：10,000	
合計VPNピア。全タイプの合計	Firepower 2110：1,500 Firepower 2120：3,500 Firepower 2130：7,500 Firepower 2140：10,000	
一般ライセンス		
暗号化	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 *5* または *10* の増分： *Firepower 2110：25* *Firepower 2120：25* *Firepower 2130：30* *Firepower 2140：40*
クラスタ	サポートしない	
VLAN、最大	1024	

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	10,000	
VPN ライセンス		
AnyConnect ピア	ディセーブル	オプションの *AnyConnect Plus* または *Apex* ライセンス：最大 *10,000*
その他の VPN ピア	10,000	
合計 VPN ピア。全タイプの合計	10,000	
一般ライセンス		
暗号化	アカウントのエクスポート コンプライアンス設定によって、Base（DES）または Strong（3DES/AES）	
セキュリティ コンテキスト	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。

ライセンス	Standard ライセンス	
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 *AnyConnect Plus* または *Apex* 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	

スマート ソフトウェア ライセンスのモニタリング

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 コマンドを参照してください。

- **show license features**

  次に、基本ライセンスのみの ASAv の例を示します（現在のライセンス権限なし）。

```
Serial Number:  9AAHGX8514R

ASAv Platform License State: Unlicensed
No active entitlement: no feature tier configured

Licensed features for this platform:
Maximum Physical Interfaces       : 10             perpetual
Maximum VLANs                     : 50             perpetual
Inside Hosts                      : Unlimited      perpetual
Failover                          : Active/Standby perpetual
Encryption-DES                    : Enabled        perpetual
Encryption-3DES-AES               : Enabled        perpetual
Security Contexts                 : 0              perpetual
GTP/GPRS                          : Disabled       perpetual
AnyConnect Premium Peers          : 2              perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 250            perpetual
Total VPN Peers                   : 250            perpetual
Shared License                    : Disabled       perpetual
AnyConnect for Mobile             : Disabled       perpetual
AnyConnect for Cisco VPN Phone    : Disabled       perpetual
Advanced Endpoint Assessment      : Disabled       perpetual
UC Phone Proxy Sessions           : 2              perpetual
Total UC Proxy Sessions           : 2              perpetual
Botnet Traffic Filter             : Enabled        perpetual
Intercompany Media Engine         : Disabled       perpetual
Cluster                           : Disabled       perpetual
```

スマート ライセンス ステータスの表示

ライセンス ステータスを表示するには、次のコマンドを参照してください。

- **すべてのライセンスの表示**

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

  次の例では、ASAv ライセンスを表示します。

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

Smart Licensing is ENABLED

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

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

License Usage
==============

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

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

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

- **show license status**

  スマート ライセンスのステータスを表示します。

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

```
ciscoasa# show license status

Smart Licensing is ENABLED

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

License Authorization:
  Status: AUTHORIZED on Sep 23 01:41:26 2015 UTC
  Last Communication Attempt: SUCCEEDED on Sep 23 01:41:26 2015 UTC
  Next Communication Attempt: Oct 23 01:41:26 2015 UTC
  Communication Deadline: Dec 22 01:38:25 2015 UTC
```

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

```
ciscoasa# show license status

Smart Licensing is ENABLED
License Reservation is ENABLED

Registration:
```

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

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

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

- **show license summary**

  スマート ライセンスのステータスと使用量のサマリーを表示します。

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

```
ciscoasa# show license summary

Smart Licensing is ENABLED

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

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

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

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

```
ciscoasa# show license summary

Smart Licensing is ENABLED

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

License Authorization:
  Status: AUTHORIZED - RESERVED
```

- **show license usage**

  スマート ライセンスの使用量を表示します。

  次に、ASAv の使用量の例を示します。

```
ciscoasa# show license usage
```

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

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

UDI の表示

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

show license udi

次に、ASAv の UDI の例を示します。

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

スマート ソフトウェア ライセンスのデバッグ

クラスタリングのデバッグについては、次のコマンドを参照してください。

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

  スマート エージェントからのデバッグをオンにします。

- **debug license** *level*

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

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
ASAvのシスコ スマート ソフトウェア ライセンシング	9.3(2)	Smart Software Licensing では、ライセンスのプールを購入して管理することができます。PAKライセンスとは異なり、スマートライセンスは特定のシリアル番号に関連付けられません。各ユニットのライセンスキーを管理しなくても、簡単にASAv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。 **clear configure license**、**debug license agent**、**feature tier**、**http-proxy**、**license smart**、**license smart deregister**、**license smart register**、**license smart renew**、**show license**、**show running-config license**、**throughput level** 各コマンドが導入されました。
FirePOWER 9300 の ASA のシスコ スマート ソフトウェア ライセンシング	9.4(1.150)	FirePOWER 9300 に ASA のシスコ スマート ソフトウェア ライセンシングが導入されました。 次のコマンドが導入されました。**feature strong-encryption**、**feature mobile-sp**、**feature context**

機能名	プラットフォーム 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)	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。 次のコマンドが導入されました。**auto-import**
新しいキャリア ライセンス	9.5(2)	新しいキャリア ライセンスは既存の GTP/GPRS ライセンスを置き換え、SCTP と Diameter インスペクションもサポートします。Firepower 9300 の ASA の場合、**feature mobile-sp** コマンドは **feature carrier** コマンドに自動的に移行します。 次のコマンドが導入または変更されました。**feature carrier**、**show activation-key**、**show license**、**show tech-support**、**show version**

機能名	プラットフォーム リリース	説明
FirePOWER 9300 の ASA に高度暗号化（3DES）ライセンスを自動的に適用	9.5(2.1)	通常の Cisco Smart Software Manager（SSM）ユーザの場合、FirePOWER 9300 で登録トークンを適用すると、対象となるお客様には強力な暗号化ライセンスが自動的に有効になります。 （注） スマート ソフトウェア マネージャ サテライトが導入されている場合、ASDM や他の高度暗号機能を使用するには、ASA の展開後に ASA CLI を使用して、高度暗号化ライセンスを有効にする必要があります。 この機能には、FXOS 1.1.3 が必要です。 サテライト以外の構成では、次のコマンドが除去されました。**feature strong-encryption**
ASAv の永続ライセンス予約	9.5(2.200) 9.6(2)	Cisco Smart Software Manager との通信が許可されていない非常にセキュアな環境では、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。 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**

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)	スマート エージェントはバージョン 1.1 からバージョン 1.6 へアップグレードされました。このアップグレードは永続ライセンス予約をサポートするほか、ライセンス アカウントに設定された権限に従って、高度暗号化（3DES/AES）ライセンス権限の設定もサポートします。 （注） バージョン 9.5（2.200）からダウングレードした場合、ASAv はライセンス登録状態を保持しません。**license smart register idtoken** *id_token* **force** コマンドを使用し、再登録する必要があります。Smart Software Manager から ID トークンを取得します。 次のコマンドが導入されました。**show license status**、**show license summary**、**show license udi**、**show license usage** 次のコマンドが変更されました。**show license all**、**show tech-support license** 次のコマンドが非推奨になりました。**show license cert**、**show license entitlement**、**show license pool**、**show license registration**
ASAv の短かい文字列の拡張機能向けの永続ライセンス予約	9.6(2)	スマート エージェント（1.6.4 への）の更新により、要求と認証コードには短い文字列が使用されます。 変更されたコマンドはありません。

機能名	プラットフォーム リリース	説明
Firepower 4100/9300 シャーシ 上の ASA の永続ライセンス予約	9.6(2)	Cisco Smart Software Manager との通信が許可されていない非常にセキュアな環境では、FirePOWER 9300 および FirePOWER 4100 の ASA 用に永続ライセンスを要求できます。永続ライセンスには、標準層、高度暗号化（該当する場合）、セキュリティ コンテキスト、キャリア ライセンスをはじめ、使用可能なすべてのライセンス権限が含まれます。FXOS 2.0.1 が必要です。 すべての設定はFirepower 4100/9300 シャーシで実行され、ASA の設定は不要です。
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。