ライセンス

この章では、さまざまなライセンスタイプ、サービスサブスクリプション、ライセンス要件などに関する詳細情報が提供されています。

（注） Firewall Management Center は、プラットフォームライセンスとして、スマートライセンスまたはレガシー PAK（製品アクティベーションキー）ライセンスをサポートしています。PAK ライセンスの使用についての詳細は、レガシー Firewall Management Center PAK ベースのライセンスの設定 （57 ページ）を参照してください。

ライセンスについて

シスコ スマート ライセンシングは、シスコ ポートフォリオ全体および組織全体でソフトウェアをより簡単かつ迅速に一貫して購入および管理できる柔軟なライセンスモデルです。また、これは安全です。ユーザーがアクセスできるものを制御できます。スマートライセンスを使用すると、次のことが可能になります。

- **簡単なアクティベーション**：スマートライセンスは、組織全体で使用できるソフトウェアライセンスのプールを確立します。PAK（製品アクティベーションキー）は不要です。

- **管理の統合**：My Cisco Entitlements（MCE）は、使いやすいポータルですべてのシスコ製品とサービスの完全なビューを提供するので、取得したもの、使用しているものを常に把握できます。
- **ライセンスの柔軟性**：ソフトウェアはハードウェアにノードロックされていないため、必要に応じてライセンスを簡単に使用および転送できます。

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

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

Smart Software Manager とアカウント

1 つ以上のライセンスを購入する場合は、それらのライセンスを Smart Software Manager（https://software.cisco.com/#module/SmartLicensing）で管理します。Smart Software Manager を使用すると、組織のプライマリアカウントを作成できます。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 を使用すると、組織のプライマリアカウントを作成できます。手順については、「Cisco アカウントの作成」を参照してください。

デフォルトでは、ライセンスはプライマリ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。アカウント管理者は、仮想アカウント（例：地域、部門、支社）を追加できます。複数のバーチャルアカウントは、多数のライセンスおよびデバイスを管理するために役立ちます。

ライセンスは、バーチャルアカウント別に管理します。バーチャルアカウントに割り当てられているライセンスを使用できるのは、そのバーチャル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。

エアギャップ展開のライセンスのオプション

次の表に、インターネットにアクセスできない環境で使用可能なライセンスオプションを比較して示します。特定の状況については、販売担当者が他のアドバイスをできる場合があります。

表 *1*: エアギャップ ネットワークのライセンス オプションの比較

Smart Software Manager オンプレミス	特定のライセンスの予約
大量の製品に対する拡張性	少数のデバイスに最適
ライセンス管理、使用状況、および資産管理の可視性を自動化	使用状況および資産管理の可視性の制限
デバイスを追加するための運用コストの増加なし	デバイスを追加するための経時的な運用コストが線形

Smart Software Manager オンプレミス	特定のライセンスの予約
柔軟性、使いやすさ、少ないオーバーヘッド	移動、追加、および変更の際の管理および手動によるオーバーヘッドの多さ
初期およびさまざまな期限切れ状態でコンプライアンス不適合ステータスが許可される	コンプライアンス不適合ステータスはシステムの動作に影響を与える
詳細については、「Firewall Management Center の Smart Software Manager オンプレミスへの登録 （33 ページ）」を参照してください。	詳細については、「特定ライセンス予約（SLR）の設定 （44 ページ）」を参照してください。

Management Center およびデバイスのライセンシングの仕組み

Firewall Management Center は Smart Software Manager に登録し、各管理対象デバイスにライセンスを割り当てます。デバイスは、Smart Software Manager に直接登録しません。

物理 Firewall Management Center は、それ自体の使用にはライセンスを必要としません。Firewall Management Center Virtual にはプラットフォームライセンスが必要です。

Smart Software Manager との定期的な通信

製品ライセンスの権限付与を維持するために、製品は Smart Software Manager と定期的に通信する必要があります。

製品インスタンス登録トークンを使用して、Firewall Management Center を Smart Software Manager に登録できます。Smart Software Manager は、Firewall Management Center と Smart Software Manager が通信するための ID 証明書を発行します。この証明書の有効期間は 1 年ですが、6 ヵ月ごとに更新されます。ID 証明書の有効期限が切れた場合（1 年間通信がなかった場合）、Firewall Management Center がアカウントから削除されることがあります。

Firewall Management Center は Smart Software Manager と定期的に通信します。Smart Software Manager で変更を加えた場合は、Firewall Management Center 上で認証を更新すると、その変更がすぐに適用されます。また、スケジュールどおりにFirewall Management Centerが通信するのを待つこともできます。

Firewall Management Center は、Smart Software Manager に直接インターネットアクセスできるか、エアギャップ展開のライセンスのオプション （2 ページ）で説明されているいずれかのオプションを使用する必要があります。非エアギャップ展開では、通常のライセンスに関する通信は 30 日ごとに行われますが、これには猶予期間があり、Firewall Management Centerは Smart Software Manager と通信することなく最大で 90 日間は動作します。90 日が経過する前に Firewall Management Center が Smart Software Manager と通信することを確認してください。そうでない場合、Firewall Management Center は未登録の状態に戻ります。

評価モード（Evaluation Mode）

Firewall Management Center は、Smart Software Manager への登録の前に 90 日間、評価モードで動作します。管理対象デバイスに機能ライセンスを割り当てることができ、評価モードの期間中はコンプライアンスに準拠した状態が維持されます。この期間が終了すると、Firewall Management Center は登録解除されます。

Firewall Management Center を Smart Software Manager に登録すると、評価モードが終了します。後で Firewall Management Center の登録を解除すると、最初に 90 日間すべてを使用していなくても、評価モードを再開することはできません。

未登録状態の詳細については、未登録状態 （5 ページ）を参照してください。

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

（注） Cisco Secure Firewall バージョン 7.6.0 の評価モード用 Talos 証明書は、2025 年 3 月 31 日に期限が切れるよう設定されています。この日以降、評価モードでの Talos ホスティングサービス（特に Web レピュテーション/分類ルックアップに関連するサービス）へのアクセスは中止されます。

コンプライアンス逸脱状態

Firewall Management Center 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。

- 使用超過：管理対象デバイスまたは Firewall Management Center Virtual が、利用できないライセンスを使用している場合。

  デバイスに対して 1 つのライセンスが利用できない場合でも、Firewall Management Center は**コンプライアンス逸脱**状態になることに注意してください。すべての構成の展開について成り立ちます。たとえば、2 つのマルウェア ライセンスと 3 台の管理対象デバイスがあるとします。3 つのデバイスすべてが**コンプライアンス違反**状態になり、マルウェア機能が動作しなくなります。

- ライセンスの有効期限切れ：管理対象デバイスの時間ベースライセンスの有効期限が切れている場合。

コンプライアンス違反状態になると、次のような影響が見られます。

- Firewall Management Center Virtual プラットフォームライセンス：動作は影響を受けません。

- すべての管理対象デバイスライセンス：動作は影響を受けません。

ライセンスの問題を解決すると、Firewall Management Center は、Smart Software Manager での定期的にスケジュールされた承認後に、コンプライアンス準拠状態になったことを示します。承認を強制するには、[システム（System）]（⚙）>**[ライセンス（Licenses）]**>**[スマートライセンス（Smart Licenses）]** ページで [再承認（Re-Authorize）] をクリックします。

未登録状態

Firewall Management Center は、次の状況で登録解除される可能性があります。

- 評価モードの有効期限：評価モードは 90 日後に期限切れになります。
- Firewall Management Center の手動登録解除
- Smart Software Manager との通信の欠如：Firewall Management Center は、Smart Software Manager と 1 年間通信していません。注：90 日後に Firewall Management Center 認証は期限切れになりますが、1 年以内に通信を正常に再開して自動的に再認証することができます。1 年後、ID 証明書の有効期限が切れ、Firewall Management Center はアカウントから削除されるため、手動で Firewall Management Center を再登録する必要があります。

未登録状態では、Firewall Management Center はライセンスを必要とする機能の設定変更をデバイスに展開できません。

エンドユーザーライセンス契約書

本製品の使用について規定するシスコ エンドユーザー ライセンス契約書（EULA）および適用される補足契約書（SEULA）は、http://www.cisco.com/go/softwareterms から入手できます。

ライセンスのタイプと制約事項

ここでは、使用可能なライセンスのタイプについて説明します。

表 *2:* スマート ライセンス

自分で割り当てるライセンス	期間	付与される機能
Essentials	永久かサブスクリプションか （注） Essentials サブスクリプション ライセンスは、Firewall Threat Defense Virtual でのみサポートされます。	特定のライセンス予約および Cisco Secure Firewall 1200/3100/4200 を除き、Essentials 永続的ライセンスは自動で、すべての Firewall Threat Defense い割り当てられます。 ユーザーおよびアプリケーション制御 スイッチングとルーティング NAT 詳細は、「Essentials ライセンス （8 ページ）」を参照してください。
IPS	サブスクリプション	侵入検知と防御 ファイル制御 セキュリティ インテリジェンス フィルタリング 詳細については、「IPS ライセンス （10 ページ）」を参照してください。
マルウェア防御	サブスクリプション	マルウェア防御 Secure Malware Analytics ファイル ストレージ （IPS ライセンスはマルウェア防御ライセンスの前提条件です）。 詳細については、マルウェア防御ライセンス （8 ページ） および Cisco Secure Firewall Management Center デバイス構成ガイドの「*License Requirements for File and Malware Policies*」を参照してください。
通信事業者	Firepower 4100/9300、Cisco Secure Firewall 3100/4200、および Firewall Threat Defense Virtual のサブスクリプション	Diameter、GTP/GPRS、M3UA、および SCTP インスペクション 詳細については、キャリア ライセンス （10 ページ）を参照してください。

自分で割り当てるライセンス	期間	付与される機能
URL フィルタリング	サブスクリプション	カテゴリとレピュテーションに基づく URL フィルタリング 詳細は、「URL フィルタリング ライセンス （12 ページ）」を参照してください。 （IPS ライセンスはURL フィルタリング ライセンスの前提条件です）。
Firewall Management Center Virtual	• 通常のスマートライセンス：永続 • 特定のライセンス予約：サブスクリプション	プラットフォームライセンスによって、Firewall Management Center Virtual が管理できるデバイスの数が決まります。 詳細は、「Firewall Management Center Virtual ライセンス （8 ページ）」を参照してください。
輸出管理機能	永続	国家安全保障、外交政策、反テロリズムに関する法律や規制の対象となる機能。「輸出規制対象の機能のライセンス （13 ページ）」を参照してください。
リモート アクセス VPN： • Secure Client Premier • Secure Client Advantage • Secure Client VPN のみ	サブスクリプションまたは永続	リモート アクセス VPN の設定リモート アクセス VPN を設定するには、アカウントによるエクスポート制御機能を許可する必要があります。デバイスを登録するときに、エクスポート要件を満たすかどうかを選択します。Firewall Threat Defense は、任意の有効な セキュアクライアント ライセンスを使用できます。使用できる機能はライセンス タイプによって異なります。 詳細については、セキュアクライアント ライセンス （12 ページ）およびCisco Secure Firewall Management Center デバイス構成ガイドの「*VPN Licensing*」 を参照してください。

（注） サブスクリプション ライセンスは、期間ベースのライセンスです。

Firewall Management Center Virtual ライセンス

Firewall Management Center Virtual には、管理できるデバイスの数に対応するプラットフォームライセンスが必要です。

Firewall Management Center Virtual は、スマートライセンスをサポートしています。

通常のスマートライセンスでは、これらのライセンスは永続的ライセンスです。

特定のライセンス予約では、これらのライセンスはサブスクリプションベースです。

（注） FMCv の新しいデバイスのアドオンライセンス要件がある場合は、追加のデバイスをサポートする上位の Firewall Management Center Virtual モデルに移行することをお勧めします。

Essentials ライセンス

Essentials ライセンスでは、次のことができます。

- スイッチングおよびルーティング（DHCP リレーおよび NAT を含む）を実行するようにデバイスを設定する
- デバイスをハイアベイラビリティペアとして設定する
- クラスタリングを設定する
- アクセスコントロールルールにユーザーとアプリケーションの条件を追加することで、ユーザーとアプリケーションの制御を実装する
- 脆弱性データベース（VDB）および地理位置情報データベース（GeoDB）を更新します。
- SRU/LSP などの侵入ルールをダウンロードします。ただし、IPS ライセンスが有効になっていない限り、アクセス コントロール ポリシーまたは侵入ポリシーを持つルールをデバイスに展開することはできません。

Cisco Secure Firewall 1200/3100/4200

Cisco Secure Firewall 1200/3100/4200 を購入時は、Essentials ライセンスを取得します。

他のモデル

特定のライセンス予約を使用する展開の場合を除き、Essentialsライセンスはデバイスを Firewall Management Center に登録したときに、アカウントに自動的に追加されます。特定のライセンス予約の場合、アカウントにEssentialsライセンスを追加する必要があります。

マルウェア防御ライセンス

マルウェア防御ライセンスでは、マルウェア防御およびSecure Malware Analyticsを実行できます。この機能では、デバイスを使用して、ネットワーク上で伝送されるファイルのマルウェアを検出してブロックできます。この機能ライセンスをサポートするために、スタンドアロンサ

ブスクリプションとしてマルウェア防御（AMP）サービスサブスクリプションを購入できます。また、IPS（TM）やIPSおよびURLフィルタリング（TMC）サブスクリプションと組み合わせて購入することもできます。IPSライセンスは、マルウェア防御ライセンスの前提条件です。

（注） マルウェア防御ライセンスが有効になっている管理対象デバイスは、動的分析を設定していない場合でも、定期的にSecure Malware Analytics Cloudへの接続を試行します。このため、デバイスの[インターフェイス トラフィック（Interface Traffic）]ダッシュボード ウィジェットには、送信済みトラフィックが表示されます。これは正常な動作です。

ファイル ポリシーの一部としてマルウェア防御を設定し、その後1つ以上のアクセス コントロール ルールを関連付けます。ファイル ポリシーでは、特定のアプリケーション プロトコルを介した特定のタイプのユーザーによるファイルのアップロードとダウンロードを検出できます。マルウェア防御では、ローカル マルウェア分析とファイルの事前分類を使用して、それらの限られた一連のファイルタイプを検査できます。特定のファイルタイプをダウンロードしてSecure Malware Analyticsクラウドにアップロードして、動的Spero分析でマルウェアが含まれているかどうかを判別することもできます。これらのファイルでは、ファイルがネットワーク内で経由する詳細なパスを示すネットワーク ファイル トラジェクトリを表示できます。マルウェア防御 ライセンスでは、ファイル リストに特定のファイルを追加し、そのファイル リストをファイルポリシー内で有効にすることもできます。これにより、検出時にこれらのファイルを自動的に許可またはブロックできます。

マルウェア防御ライセンスが必要なのは、マルウェア防御およびSecure Malware Analyticsを展開する場合のみであることに注意してください。マルウェア防御ライセンスがなければ、Firewall Management CenterはSecure Malware Analytics CloudからSecure Endpointマルウェアイベントおよび侵害の兆候（IOC）を受信できます。

Cisco Secure Firewall Management Center デバイス構成ガイド のファイルおよびマルウェアポリシーのライセンス要件で重要な情報も参照してください。

このライセンスを無効にすると、次の状況が発生します。

- システムはSecure Malware Analytics Cloudへの問い合わせを停止し、Secure Malware Analytics Cloudから送信される遡及的イベントの確認応答も停止します。
- 既存のアクセス コントロール ポリシーにマルウェア防御構成が含まれている場合は、それらのポリシーを再展開することができません。
- マルウェア防御ライセンスが無効にされた後、システムが既存のキャッシュファイルの性質を使用できるのはごく短時間のみです。この時間枠の経過後、システムは`Unavailable`という性質をこれらのファイルに割り当てます。

ライセンスの有効期限が切れると、前述の機能に対する利用資格が停止し、Firewall Management Centerはコンプライアンス違反の状態に移行します。

IPS ライセンス

IPS ライセンスでは、侵入の検出と防御、ファイル制御、およびセキュリティ インテリジェンスのフィルタリングを実行できます。

- 侵入検知および防御により、侵入とエクスプロイトを検出するためネットワーク トラフィックを分析できます。またオプションで違反パケットをドロップできます。
- ファイル制御により、特定のアプリケーションプロトコルを介した特定タイプのファイルを検出し、オプションでこれらのファイルのアップロード（送信）またはダウンロード（受信）をユーザーからブロックできます。マルウェア防御ライセンスが必要なマルウェア防御 では、マルウェアの性質に基づいて限られたファイルタイプを検査およびブロックすることもできます。
- セキュリティ インテリジェンス フィルタリングにより、トラフィックをアクセスコントロールルールによる分析対象にする前に、特定の IP アドレス、URL、および DNS ドメイン名をブロック（その IP アドレスとの間のトラフィックを拒否）できます。ダイナミックフィードにより、最新の情報に基づいて接続をただちにブロックできます。オプションで、セキュリティ インテリジェンス フィルタリングに「モニターのみ」設定を使用できます。

IPS ライセンスは、スタンドアロン サブスクリプション（T）として、または URL フィルタリング（TC）、マルウェア防御（TM）、あるいはその両方（TMC）と組み合わせて購入できます。

このライセンスを無効にすると、次の状況が発生します。

- Firewall Management Center で、影響を受けたデバイスからの侵入イベントとファイルイベントの確認応答が停止されます。結果として、トリガー条件としてこれらのイベントを使用する相関ルールがトリガーしなくなります。
- また、Firewall Management Center はシスコ提供またはサードパーティのセキュリティ インテリジェンス情報を取得するためにインターネットに接続しなくなります。
- IPS を再度有効にするまでは、既存の侵入ポリシーを適用し直すことができません。

ライセンスの有効期限が切れると、前述の機能に対する利用資格が停止し、Firewall Management Center はコンプライアンス違反の状態に移行します。

キャリア ライセンス

キャリアライセンスでは、以下のプロトコルのインスペクションが有効になります。

- Diameter：Diameter は、LTE（Long Term Evolution）および IMS（IP Multimedia Subsystem）用の EPS（Evolved Packet System）などの次世代モバイルと固定電気通信ネットワークで使用される認証、認可、およびアカウンティング（AAA）プロトコルです。RADIUS や TACACS がこれらのネットワークで Diameter に置き換えられます。
- GTP/GPRS：GPRS トンネリングプロトコル（GTP）は、General Packet Radio Service（GPRS）トラフィック用に GSM、UMTS、および LTE ネットワークで使用されます。GTP は、ト

ンネル制御および管理プロトコルを提供します。このプロトコルによるトンネルの作成、変更、および削除により、モバイル ステーションに GPRS ネットワーク アクセスが提供されます。GTP は、ユーザ データ パケットの伝送にもトンネリング メカニズムを使用します。

- M3UA：MTP3 User Adaptation（M3UA）は、Signaling System 7（SS7）Message Transfer Part 3（MTP3）レイヤと連動する IP ベースアプリケーション用の SS7 ネットワークへのゲートウェイを提供するクライアント/サーバープロトコルです。M3UA により、IP ネットワーク上で SS7 ユーザー パート（ISUP など）を実行することが可能になります。
- SCTP：Stream Control Transmission Protocol（SCTP）は、IP ネットワーク上で SS7 プロトコルをサポートするトランスポート層プロトコルです。4G LTE モバイル ネットワーク アーキテクチャをサポートしています。SCTP は、複数の同時ストリーム、多重化ストリームを処理でき、より多くのセキュリティ機能を提供します。

（注） デバイスでこのライセンスを有効にした後、FlexConfig ポリシーを使用してプロトコルインスペクションを有効にします。

キャリアライセンス PID は、デバイスモデルごとではなく、ファミリごとに利用できます。評価モードまたはスマートライセンスで、デバイスごとにこのライセンスを有効にすることができます。

Firepower 4100/9300、Cisco Secure Firewall 3100/4200、および Firewall Threat Defense Virtual のキャリアライセンスは期間ベースです。このライセンスは、特定のライセンス予約もサポートしています。

サポートされるデバイス

キャリアライセンスをサポートするデバイスは次のとおりです。

- Secure Firewall 3110
- Secure Firewall 3120
- Secure Firewall 3130
- Secure Firewall 3140
- Firepower 4112
- Firepower 4115
- Firepower 4125
- Firepower 4145
- Cisco Secure Firewall 4215
- Cisco Secure Firewall 4225
- Cisco Secure Firewall 4245

- Firepower 9300
- Firewall Threat Defense Virtual

URL フィルタリング ライセンス

URL フィルタリング ライセンスにより、モニター対象ホストにより要求される URL に基づいて、ネットワーク内を移動できるトラフィックを判別するアクセスコントロールルールを作成できます。この機能ライセンスをサポートするために、スタンドアロンサブスクリプションとして URL フィルタリング サービスサブスクリプションを購入できます。また、IPS （TC）や脅威およびマルウェア防御（TMC）サブスクリプションと組み合わせて購入することもできます。IPS ライセンスが、このライセンスの前提条件です。

ヒント URL フィルタリング ライセンスがない状態で、許可またはブロックする個別URL またはURL グループを指定できます。このオプションにより、Web トラフィックをカスタムできめ細かく制御できますが、URL カテゴリおよびレピュテーションデータをネットワークトラフィックのフィルタ処理に使用することはできません。

URL フィルタリング ライセンスがない状態でも、アクセスコントロールルールにカテゴリベースのURL 条件およびレピュテーションベースのURL 条件を追加できますが、Firewall Management Center はURL 情報をダウンロードしません。最初にURL フィルタリング ライセンスをFirewall Management Center に追加し、ポリシー適用対象デバイスで有効にするまでは、アクセス コントロール ポリシーを展開できません。

このライセンスを無効にすると、次の状況が発生します。

- URL カテゴリとレピュテーション ACP のルールに基づいたネットワークトラフィックのフィルタ処理にアクセスできなくなる場合があります。手動URL フィルタリングオプションは引き続きサポートされます。
- URL 条件によるアクセス コントロール ルールが、URL のフィルタリングをただちに停止します。
- Firewall Management Center で URL データの更新をダウンロードできなくなります。
- 既存のアクセス コントロール ポリシーに、カテゴリ ベースまたはレピュテーション ベースの URL 条件を含むルールが含まれている場合は、それらのポリシーを再展開することができません。

ライセンスの有効期限が切れると、前述の機能に対する利用資格が停止し、Firewall Management Center はコンプライアンス違反の状態に移行します。

セキュアクライアント ライセンス

セキュアクライアント および標準ベースの IPSec/IKEv2 を使用して、リモートアクセス VPN を設定できます。

リモートアクセス VPN を有効にするには、Secure Client Advantage、Secure Client Premier、または Secure Client VPN のみ のうちいずれかのライセンスを購入して有効にする必要があります。両方のライセンスがあり、そのどちらも使用する場合は、Secure Client Advantage と Secure Client Premier を選択できます。[Apex] または [Plus] と一緒に Secure Client VPN のみ ライセンスを使用することはできません。セキュアクライアントライセンスは、スマートアカウントと共有する必要があります。手順については、http://www.cisco.com/c/dam/en/us/products/collateral/security/anyconnect-og.pdfを参照してください。

指定されたデバイスに指定された セキュアクライアント ライセンスタイプの権限が 1 つ以上ない場合、リモートアクセス VPN 設定をそのデバイスに展開することはできません。登録されたライセンスがコンプライアンスに従っていない、または権限の有効期限が切れている場合は、システムにライセンス アラートとヘルス イベントが表示されます。

リモートアクセス VPN を使用する際は、スマートアカウントでエクスポート制御機能（高度な暗号化）を有効にしておく必要があります。セキュアクライアント とのリモートアクセス VPN 接続を確立するために、Firewall Threat Defense はより強力な暗号化を要求します（これは DES よりも高い暗号化です）。

次の条件に当てはまる場合、リモートアクセス VPN を展開できません。

- Firewall Management Center でスマート ライセンスが評価モードで実行されている。
- スマートアカウントがエクスポート制御機能（高度な暗号化）を使用するように設定されていない。

輸出規制対象の機能のライセンス

輸出規制対象の機能が必要な機能

特定のソフトウェア機能は、国家安全保障、外交政策、反テロリズムに関する法律や規制の対象となります。これらの輸出規制対象の機能は次のとおりです。

- セキュリティ認定コンプライアンス
- リモート アクセス VPN
- 強力な暗号化によるサイト間 VPN
- 強力な暗号化による SSH プラットフォーム ポリシー
- 強力な暗号化による SSL ポリシー
- 強力な暗号化による SNMPv3 などの機能

輸出規制対象の機能がシステムに対して現在有効になっているかどうかを判断する方法

輸出規制対象の機能がシステムに対して現在有効になっているかどうかを判断するには、[システム（System）]（⚙）>**[ライセンス（Licenses）]**>**[スマートライセンス（Smart Licenses）]** に移動し、**[輸出規制対象の機能（Export-Controlled Features）]** に **[有効（Enabled）]** と表示されているかどうかを確認します。

輸出規制対象の機能の有効化について

[輸出規制対象の機能（Export-Controlled Features）] に [無効（Disabled）] と表示されており、強力な暗号化が必要な機能を使用する場合、強力な暗号化機能を有効にする方法は2つあります。組織はどちらか一方を使用する（またはどちらも使用しない）ことができますが、両方を使用することはできません。

- Smart Software Manager で新しい製品インスタンス登録トークンを生成したときに輸出規制対象の機能を有効にするオプションがない場合は、アカウント担当者にお問い合わせください。

  シスコによって承認されたら、強力な暗号化ライセンスをアカウントに手動で追加して、輸出規制されている機能を使用できるようにすることができます。詳細については、グローバル権限のないアカウントの輸出規制機能の有効化 （35 ページ）を参照してください。

- Smart Software Manager で新しい製品インスタンス登録トークンを生成するときに、[このトークンを使用して登録した製品で輸出管理機能を許可（Allow export-controlled functionality on the products registered with this token）] オプションが表示される場合は、トークンを生成する前にそれを確認してください。

  Firewall Management Center の登録に使用した製品インスタンス登録トークンの輸出規制機能を有効にしなかった場合は、登録を解除してから、輸出規制機能を有効にした新しい製品インスタンス登録トークンを使用して Firewall Management Center を再登録する必要があります。

評価モードで、または Firewall Management Center で強力な暗号化を有効にする前にデバイスを Firewall Management Center に登録した場合は、各管理対象デバイスを再起動して、強力な暗号化を使用できるようにします。高可用性展開では、アクティブ デバイスとスタンバイ デバイスを一緒に再起動してアクティブ/アクティブの状態を回避する必要があります。

これは永続的な付与資格であり、サブスクリプションは必要ありません。

詳細情報

輸出規制に関する一般情報については https://www.cisco.com/c/en/us/about/legal/global-export-trade.html を参照してください。

Firewall Threat Defense Virtual ライセンス

このセクションでは、Firewall Threat Defense Virtual で使用可能なパフォーマンス階層ライセンスの権限について説明します。

すべての Firewall Threat Defense Virtual ライセンスを、サポートされているすべての Firewall Threat Defense Virtual vCPU/メモリ構成で使用できます。これにより、Firewall Threat Defense Virtual を使用しているお客様は、さまざまな VM リソースフットプリントで実行できるようになります。また、サポート対象の AWS および Azure インスタンスタイプの数も増えます。Firewall Threat Defense Virtual VM を設定する場合、サポートされる最大コア（vCPU）数は 16 個です。また、サポートされる最大メモリ容量は 32 GB RAM です。

Firewall Threat Defense Virtual スマートライセンスのパフォーマンス階層

RA VPN に対するセッション制限は、インストールされている Firewall Threat Defense Virtual プラットフォームの権限付与階層によって決定され、レートリミッタによって適用されます。次の表は、権限付与層とレート制限に基づくセッション制限をまとめたものです。

表 *3 : Firewall Threat Defense Virtual* 権限付与に基づくライセンス機能の制限

パフォーマンス階層	デバイス仕様（コア/RAM）	レート制限	RA VPN セッション制限
FTDv5、100Mbps	4 コア/8 GB	100Mbps	50
FTDv10、1Gbps	4 コア/8 GB	1Gbps	250
FTDv20、3Gbps	4 コア/8 GB	3 Gbps	250
FTDv30、5Gbps	8 コア/16 GB	5 Gbps	250
FTDv50、10Gbps	12 コア/24 GB	10 Gbps	750
FTDv100、16 Gbps	16 コア/32 GB	16 Gbps	10,000

FTDv パフォーマンス階層ライセンスのガイドラインと制限事項

Firewall Threat Defense Virtual デバイスのライセンスを取得する際は、次の注意事項と制限事項に注意してください。

- Firewall Threat Defense Virtual は、導入要件に基づいて異なるスループットレベルと VPN 接続制限を提供するパフォーマンス階層型ライセンスをサポートしています。
- すべての Firewall Threat Defense Virtual ライセンスを、サポートされているすべての Firewall Threat Defense Virtual コア/メモリ構成で使用できます。これにより、Firewall Threat Defense Virtual を使用しているお客様は、さまざまな VM リソースフットプリントで実行できるようになります。
- Firewall Threat Defense Virtual を展開する際、デバイスが評価モードであるか、すでに Cisco Smart Software Manager に登録されているかに関係なく、パフォーマンス階層を選択できます。

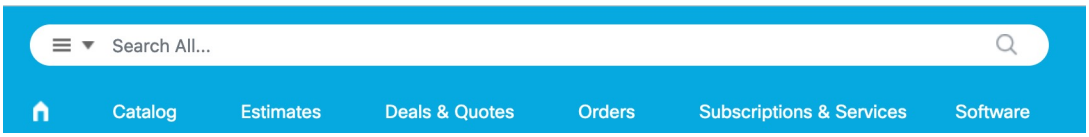
（注） お使いのスマート ライセンシング アカウントに、必要なライセンスが含まれていることを確認してください。使用アカウントにあるライセンスと一致する階層を選択することが重要です。Firewall Threat Defense Virtual をバージョン 7.0 にアップグレードする場合は、[FTDv - Variable] を選択して現在のライセンスコンプライアンスを維持できます。Firewall Threat Defense Virtual は、ご使用のデバイスの機能（コア/RAM の数）に基づいてセッション制限を引き続き実行します。

- REST API を使用して、新しい Firewall Threat Defense Virtual デバイスを展開する場合や Firewall Threat Defense Virtual をプロビジョニングする場合、デフォルトのパフォーマンス階層は FTDv50 です。
- Essentials ライセンスはサブスクリプションベースで、パフォーマンス階層にマッピングされます。バーチャルアカウントには、Firewall Threat Defense Virtual デバイスの Essentials ライセンス権限と、IPS 、マルウェア防御、および URL フィルタリング のライセンスが必要です。
- 各 HA ピアは 1 つの権限を消費します。各 HA ピアの権限は Essentials ライセンスを含めて一致している必要があります。
- HA ペアのパフォーマンス階層の変更は、プライマリピアに適用される必要があります。
- 個別のノードではなく、クラスタ全体に機能ライセンスを割り当てます。ただし、クラスタの各ノードは機能ごとに個別のライセンスを使用します。クラスタリング機能自体にライセンスは必要ありません。
- ユニバーサル PLR ライセンスは、HA ペアの各デバイスに個別に適用されます。セカンダリデバイスが、プライマリデバイスのパフォーマンス階層を自動的にミラーリングすることはありません。手動で更新する必要があります。

ライセンス PID

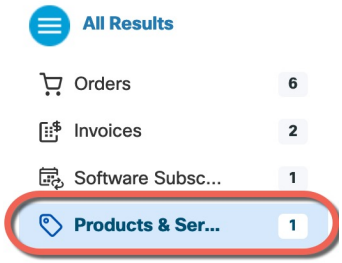
ライセンスは、シスコまたは販売代理店からデバイスを購入した際に、スマート ソフトウェア ライセンシング アカウントにリンクされています。ただし、自身でライセンスを追加する必要がある場合は、Cisco Commerce Workspace で [すべて検索（Search All）] フィールドを使用します。

図 *1*: ライセンス検索



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

図 *2*: 結果



Firewall Management Center Virtual PID

- VMware：
  - SF-FMC-VMW-2-K9—2 デバイス
  - SF-FMC-VMW-10-K9—10 デバイス
  - SF-FMC-VMW-K9—25 デバイス
  - SF-FMC-VMW-300-K9—300 デバイス
- KVM：
  - SF-FMC-KVM-2-K9—2 デバイス
  - SF-FMC-KVM-10-K9—10 デバイス
  - SF-FMC-KVM-K9—25 デバイス
- PAK ベースの VMware：
  - FS-VMW-2-SW-K9—2 デバイス
  - FS-VMW-10-SW-K9—10 デバイス
  - FS-VMW-SW-K9—25 デバイス

Firewall Threat Defense Virtual PID

FTDV-SEC-SUB を注文するときは、Essentialsライセンスとオプションの機能ライセンス（12ヵ月の期間）を選択する必要があります。

- Essentialsライセンス：
  - FTD-V-5S-BSE-K9
  - FTD-V-10S-BSE-K9
  - FTD-V-20S-BSE-K9
  - FTD-V-30S-BSE-K9
  - FTD-V-50S-BSE-K9
  - FTD-V-100S-BSE-K9
- IPS 、マルウェア防御および URL ライセンスの組み合わせ：
  - FTD-V-5S-TMC
  - FTD-V-10S-TMC
  - FTD-V-20S-TMC
  - FTD-V-30S-TMC

- FTD-V-50S-TMC
- FTD-V-100S-TMC

- キャリア：FTDV_CARRIER
- Cisco Secure Client：『Cisco Secure Client 発注ガイド』を参照してください。

Firepower 1010 PID

- IPS 、マルウェア防御および URL ライセンスの組み合わせ：
  - L-FPR1010T-TMC=

  上記の PID のいずれかを注文に追加すると、次のいずれかの PID に対応する期間ベースのサブスクリプションを選択できます。
  - L-FPR1010T-TMC-1Y
  - L-FPR1010T-TMC-3Y
  - L-FPR1010T-TMC-5Y

- Cisco Secure Client：『Cisco Secure Client 発注ガイド』を参照してください。

Firepower 1100 PID

- IPS 、マルウェア防御および URL ライセンスの組み合わせ：
  - L-FPR1120T-TMC=
  - L-FPR1140T-TMC=
  - L-FPR1150T-TMC=

  上記の PID のいずれかを注文に追加すると、次のいずれかの PID に対応する期間ベースのサブスクリプションを選択できます。
  - L-FPR1120T-TMC-1Y
  - L-FPR1120T-TMC-3Y
  - L-FPR1120T-TMC-5Y
  - L-FPR1140T-TMC-1Y
  - L-FPR1140T-TMC-3Y
  - L-FPR1140T-TMC-5Y
  - L-FPR1150T-TMC-1Y
  - L-FPR1150T-TMC-3Y
  - L-FPR1150T-TMC-5Y

- Cisco Secure Client：『Cisco Secure Client 発注ガイド』を参照してください。

Secure Firewall 1210/1220 PID

- Essential ライセンス：
  - 自動的に含める
- IPS 、マルウェア防御および URL ライセンスの組み合わせ：
  - L-CSF1210CET-TMC=
  - L-CSF1210CPT-TMC=
  - L-CSF1220CXT-TMC=

  上記の PID のいずれかを注文に追加すると、次のいずれかの PID に対応する期間ベースのサブスクリプションを選択できます。
  - L-CSF1210CE-TMC-1Y
  - L-CSF1210CE-TMC-3Y
  - L-CSF1210CE-TMC-5Y
  - L-CSF1210CP-TMC-1Y
  - L-CSF1210CP-TMC-3Y
  - L-CSF1210CP-TMC-5Y
  - L-CSF1220CX-TMC-1Y
  - L-CSF1220CX-TMC-3Y
  - L-CSF1220CX-TMC-5Y
- 強力な暗号化（3DES/AES）：
  - L-CSF1200TD-ENCK9=。アカウントに強力な暗号が承認されていない場合にのみ必要です。
- Cisco Secure Client：『Cisco Secure Client 発注ガイド』を参照してください。

Cisco Secure Firewall 1230/1240/1250 PID

- Essential ライセンス：
  - 自動的に含める
- IPS 、マルウェア防御および URL ライセンスの組み合わせ：
  - L-CSF1230T-TMC=
  - L-CSF1240T-TMC=

- L-CSF1250T-TMC=

上記の PID のいずれかを注文に追加すると、次のいずれかの PID に対応する期間ベースのサブスクリプションを選択できます。

- L-CSF1230-TMC-1Y
- L-CSF1230-TMC-3Y
- L-CSF1230-TMC-5Y
- L-CSF1240-TMC-1Y
- L-CSF1240-TMC-3Y
- L-CSF1240-TMC-5Y
- L-CSF1250-TMC-1Y
- L-CSF1250-TMC-3Y
- L-CSF1250-TMC-5Y

- 強力な暗号化（3DES/AES）：
  - L-CSF1200TD-ENCK9=。アカウントに強力な暗号が承認されていない場合にのみ必要です。

- Cisco Secure Client：『Cisco Secure Client Ordering Guide』を参照してください。

Secure Firewall 3100 PID

- Essentialsライセンス：
  - 自動的に含める

- IPS 、マルウェア防御および URL ライセンスの組み合わせ：
  - L-FPR3110T-TMC=
  - L-FPR3120T-TMC=
  - L-FPR3130T-TMC=
  - L-FPR3140T-TMC=

上記の PID のいずれかを注文に追加すると、次のいずれかの PID に対応する期間ベースのサブスクリプションを選択できます。

- L-FPR3105T-TMC-1Y
- L-FPR3105T-TMC-3Y
- L-FPR3105T-TMC-5Y
- L-FPR3110T-TMC-1Y

- L-FPR3110T-TMC-3Y
- L-FPR3110T-TMC-5Y
- L-FPR3120T-TMC-1Y
- L-FPR3120T-TMC-3Y
- L-FPR3120T-TMC-5Y
- L-FPR3130T-TMC-1Y
- L-FPR3130T-TMC-3Y
- L-FPR3130T-TMC-5Y
- L-FPR3140T-TMC-1Y
- L-FPR3140T-TMC-3Y
- L-FPR3140T-TMC-5Y

- キャリア：L-FPR3K-FTD-CAR=
- Cisco Secure Client：『Cisco Secure Client 発注ガイド』を参照してください。

Firepower 4100 PID

- IPS 、マルウェア防御および URL ライセンスの組み合わせ：
  - L-FPR4112T-TMC=
  - L-FPR4115T-TMC=
  - L-FPR4125T-TMC=
  - L-FPR4145T-TMC=

  上記の PID のいずれかを注文に追加すると、次のいずれかの PID に対応する期間ベースのサブスクリプションを選択できます。
  - L-FPR4112T-TMC-1Y
  - L-FPR4112T-TMC-3Y
  - L-FPR4112T-TMC-5Y
  - L-FPR4115T-TMC-1Y
  - L-FPR4115T-TMC-3Y
  - L-FPR4115T-TMC-5Y
  - L-FPR4125T-TMC-1Y
  - L-FPR4125T-TMC-3Y
  - L-FPR4125T-TMC-5Y
  - L-FPR4145T-TMC-1Y

- L-FPR4145T-TMC-3Y
- L-FPR4145T-TMC-5Y

- キャリア：L-FPR4K-FTD-CAR=
- Cisco Secure Client：『Cisco Secure Client 発注ガイド』を参照してください。

Secure Firewall 4200 PID

- Essentialsライセンス：
  - 自動的に含める
- IPS 、マルウェア防御および URL ライセンスの組み合わせ：
  - L-FPR4215T-TMC=
  - L-FPR4225T-TMC=
  - L-FPR4245T-TMC=

  上記の PID のいずれかを注文に追加すると、次のいずれかの PID に対応する期間ベースのサブスクリプションを選択できます。
  - L-FPR4215T-TMC-1Y
  - L-FPR4215T-TMC-3Y
  - L-FPR4215T-TMC-5Y
  - L-FPR4225T-TMC-1Y
  - L-FPR4225T-TMC-3Y
  - L-FPR4225T-TMC-5Y
  - L-FPR4245T-TMC-1Y
  - L-FPR4245T-TMC-3Y
  - L-FPR4245T-TMC-5Y
- キャリア：L-FPR4200-FTD-CAR=
- Cisco Secure Client：『Cisco Secure Client 発注ガイド』を参照してください。

Firepower 9300 PID

- IPS 、マルウェア防御および URL ライセンスの組み合わせ：
  - L-FPR9K-40T-TMC=
  - L-FPR9K-48T-TMC=
  - L-FPR9K-56T-TMC=

上記の PID のいずれかを注文に追加すると、次のいずれかの PID に対応する期間ベースのサブスクリプションを選択できます。

- L-FPR9K-40T-TMC-1Y
- L-FPR9K-40T-TMC-3Y
- L-FPR9K-40T-TMC-5Y
- L-FPR9K-48T-TMC-1Y
- L-FPR9K-48T-TMC-3Y
- L-FPR9K-48T-TMC-5Y
- L-FPR9K-56T-TMC-1Y
- L-FPR9K-56T-TMC-3Y
- L-FPR9K-56T-TMC-5Y

- キャリア：L-FPR9K-FTD-CAR=
- Cisco Secure Client：Cisco AnyConnect 発注ガイド [英語] を参照してください。

ISA 3000 PID

- IPS 、マルウェア防御および URL ライセンスの組み合わせ：
  - L-ISA3000T-TMC=

上記の PID のいずれかを注文に追加すると、次のいずれかの PID に対応する期間ベースのサブスクリプションを選択できます。

- L-ISA3000T-TMC-1Y
- L-ISA3000T-TMC-3Y
- L-ISA3000T-TMC-5Y

- Cisco Secure Client：Cisco AnyConnect 発注ガイド [英語] を参照してください。

ライセンスの要件と前提条件

特定ライセンス予約の要件については、特定ライセンス予約の要件および前提条件 （45 ページ）を参照してください。

一般的な前提条件

- Firewall Management Center と管理対象デバイスで NTP が設定されていることを確認します。登録を成功させるには、時刻を同期させる必要があります。

Firepower 4100/9300 シャーシの場合は、Firewall Management Center と同じ NTP サーバーをシャーシに使用してシャーシに NTP を設定する必要があります。

サポートされるドメイン

Global。明記されている場合を除きます。

ユーザの役割

- 管理者

高可用性、クラスタリング、マルチインスタンスのためのライセンシングの要件および前提条件

このセクションでは、高可用性（デバイス高可用性と Firewall Management Center Virtual 高可用性）、クラスタリング、およびマルチインスタンス展開のライセンス要件について説明します。

Firewall Management Center 高可用性のライセンシング

各デバイスには、単一の Firewall Management Center によって管理されているか、ハイアベイラビリティペア（ハードウェアまたは仮想）の Firewall Management Center によって管理されているかにかかわらず、同じライセンスが必要です。

例：Firewall Management Center ペアで管理されている 2 つのデバイスに対して高度なマルウェア防御を有効にする場合は、2 つの マルウェア防御 ライセンスと 2 つの TM サブスクリプションを購入し、アクティブ Firewall Management Center を Smart Software Manager に登録してから、ライセンスをアクティブ Firewall Management Center 上の 2 つのデバイスに割り当てます。

アクティブな Firewall Management Center のみが Smart Software Manager に登録されます。フェールオーバーが実行されると、システムは Smart Software Manager と通信して、ライセンスの付与資格を最初にアクティブだった Firewall Management Center から解放し、新たにアクティブになる Firewall Management Center に割り当てます。

特定ライセンス予約の展開では、プライマリ Firewall Management Center のみが特定ライセンス予約を必要とします。

ハードウェア（Hardware） Firewall Management Center

ハイアベイラビリティペア内のハードウェア Firewall Management Center に特別なライセンスは必要ありません。

Firewall Management Center Virtual

同じライセンスの Firewall Management Center Virtual が 2 つ必要です。

例：10 台のデバイスを管理する Firewall Management Center Virtual ハイアベイラビリティペアの場合は、以下を使用できます。

- 2 個の Firewall Management Center Virtual 10 エンタイトルメント
- 10 個のデバイスライセンス

ハイアベイラビリティペアを解除すると、セカンダリ Firewall Management Center Virtual に関連付けられた Firewall Management Center Virtual エンタイトルメントが解放されます。（この例では、2 個のスタンドアロン Firewall Management Center Virtual 10 があります。）

デバイス高可用性のライセンシング

高可用性構成の両方の Firewall Threat Defense ユニットは、ライセンスが同じである必要があります。

高可用性構成には 2 つのライセンス資格（ペアの各デバイスに 1 つずつ）が必要です。

高可用性を確立する前に、どのライセンスがセカンダリ/スタンバイデバイスに割り当てられているかどうかは問題にはなりません。高可用性の設定中に、Firewall Management Center はスタンバイユニットに割り当てられている不要なライセンスをすべて削除し、プライマリ/アクティブユニットに割り当てられているのと同じライセンスで置き換えます。たとえば、アクティブユニットに Essentials ライセンスと IPS ライセンスが割り当てられており、スタンバイユニットに Essentials ライセンスのみが割り当てられている場合、Firewall Management Center は Cisco Smart Software Manager と通信して、アカウントからスタンバイユニット用に使用可能な IPS ラインセンスを取得します。ライセンスアカウントで十分な数の資格が購入されていなければ、正しい数のライセンスを購入するまで、アカウントは非準拠の状態になります。

デバイスクラスタのライセンス

各 Firewall Threat Defense Virtual クラスタノードには、同じパフォーマンス階層ライセンスが必要です。すべてのメンバーに同じ数の CPU とメモリを使用することをお勧めします。そうしないと、パフォーマンスが最小能力のメンバーに一致するようにすべてのノードで制限されます。スループットレベルは、一致するように制御ノードから各データノードに複製されます。

個別のノードではなく、クラスタ全体に機能ライセンスを割り当てます。ただし、クラスタの各ノードは機能ごとに個別のライセンスを使用します。クラスタリング機能自体にライセンスは必要ありません。

制御ノードを Firewall Management Center に追加する際に、そのクラスタに使用する機能ライセンスを指定できます。クラスタを作成する前に、データノードにどのライセンスが割り当てられているのかは問題になりません。制御ノードのライセンス設定は、各データノードに複製されます。クラスタのライセンスは、[システム（System）]（⚙） > **[ライセンス（Licenses）]** > **[スマートライセンス（Smart Licenses）]** > **[ライセンスの編集（Edit Licenses）]** または**[デバイス（Devices）]** > **[デバイス管理（Device Management）]** > **[クラスタ（Cluster）]** > **[ライセンス（License）]** エリアで変更できます。

（注） Firewall Management Center にライセンスを取得する（および評価モードで実行する）前にクラスタを追加した場合、Firewall Management Center にライセンスを取得する際にポリシーの変更をクラスタに展開するとトラフィックの中断が発生することがあります。ライセンスモードを変更したことによって、すべてのデータユニットがクラスタをいったん離れてから再参加することになります。

複数インスタンス展開のライセンス

すべてのライセンスがコンテナ インスタンスごとではなく、セキュリティ エンジン/シャーシ（Firepower 4100 の場合）またはセキュリティ モジュール（Firepower 9300 の場合）ごとに使用されます。次の詳細情報を参照してください。

- Essentialsライセンスが セキュリティ モジュール/エンジン ごとに 1 つ自動的に割り当てられます。
- 機能ライセンスは各インスタンスに手動で割り当てますが、セキュリティ モジュール/エンジン につき機能ごとに 1 つのライセンスのみを使用します。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 の場合、使用中のインスタンスの数に関係なく、モジュールにつき 1 つの URL フィルタリング ライセンスが必要で、合計 3 つのライセンスが必要になります。

次に例を示します。

表 *4 : Firepower 9300* のコンテナインスタンスのサンプルライセンスの使用状況

Firepower 9300	インスタンス	ライセンス
セキュリティ モジュール 1	インスタンス 1	Essentials、URL フィルタリング、マルウェア防御
	インスタンス 2	Essentials、URL フィルタリング
	インスタンス 3	Essentials、URL フィルタリング
セキュリティ モジュール 2	インスタンス 4	Essentials、IPS
	インスタンス 5	Essentials、URL フィルタリング、マルウェア防御、IPS
セキュリティ モジュール 3	インスタンス 6	Essentials、マルウェア防御、IPS
	インスタンス 7	Essentials、IPS

表 *5:* ライセンスの総数

Essentials	URL フィルタリング	マルウェア防御	IPS
3	2	3	2

シスコアカウントの作成

スマートアカウントを要求し、シスコ製品のライセンスを取得するには、シスコアカウントが必要です。

手順

ステップ 1 URL https://id.cisco.com/signin/register を開き、新しいアカウントを作成します。

ステップ 2 アカウントを作成するには、すべての必須フィールドに入力します。

次の図は例を示しています。

ステップ 3 [登録（Register）] をクリックします。

電子メールアドレスを確認するために、アクティベーションコードが記載された電子メールが送信されます。

（注）
電子メールがまだ届いていない場合は、登録サポートチーム（web-help@cisco.com）に電子メールを送信してください。

ステップ 4 [電子メールでの確認（Verify with your email）] ページで、アクティベーションコードを入力して登録プロセスを完了し、[確認（Verify）] をクリックします。

登録が正常に完了すると、ログインページにリダイレクトされます。

次のタスク

ログインページで、新しく作成したアカウントの詳細を入力して、スマートアカウントを要求します。「スマートアカウントの作成とライセンスの追加 （27 ページ）」を参照してください。

スマートアカウントの作成とライセンスの追加

ライセンスを購入する前に、このアカウントを設定する必要があります。

始める前に

アカウント担当者または再販業者が、ユーザーのためにスマートアカウントを設定していることがあります。その場合は、この手順を使用するのではなく、その担当者からアカウントへのアクセスに必要な情報を取得してから、アカウントにアクセスできることを確認してください。

シスコアカウントをまだ作成していない場合は、新しいシスコアカウントを作成する必要があります。手順については、「シスコアカウントの作成」を参照してください。

スマート アカウントに関する一般情報については http://www.cisco.com/go/smartaccounts を参照してください。

手順

ステップ 1 [スマートアカウントの作成（Create a Smart Account）]https://software.cisco.com/software/csws/smartaccount/accountCreation/createSmartAccountページに移動します。シスコアカウントでログインするように求められます。

[スマートアカウントの作成（Create a Smart Account）] ページに、基本的なアカウント情報が表示されます。

ステップ 2 右上隅に表示される [マイアカウント（My Account）] アイコンをクリックし、[プロファイルの管理（Manage Profile）] をクリックします。

ステップ 3 [個人用（Personal）] をクリックします。

ステップ 4 [会社の詳細（Your Company Details）] セクションで、[編集（Edit）] をクリックします。

ステップ 5 [会社または組織（Company or organization）] フィールドに、組織名を入力します。

ステップ 6 会社の情報がすでにシスコのデータベースに存在する場合は、リストに表示されます。会社を選択できます。

[住所（Address）] ドロップダウンリストで、会社の住所を選択します。

ステップ 7 会社がシスコのデータベースに登録されていない場合は、引き続き [会社または組織（Company or organization）] フィールドに会社情報を入力できます。

a) [住所（Address）] ドロップダウンリストで、ドロップダウンの矢印をクリックして、[新しい住所の追加（Add New Address）] をクリックします。

b) 次のいずれかの [住所タイプ（Address Type）] オプションを選択できます。

- [会社/組織（Company/Organization）]：組織の住所を入力します。シスコは、この住所を確認します。住所と会社名がその国で確認できない場合は、続行できない可能性があります。そのため、正しい住所が入力されていることを確認する必要があります。
- [個人（Personal）]：個人の住所を入力します。

ステップ 8 会社に関連付けられているすべての必須フィールドに入力し、[更新（Update）] をクリックします。

[会社の詳細（Your Company Details）] セクションに、入力した会社の詳細が表示されます。

会社の詳細が確認されると、成功メッセージが表示されます。

ステップ 9 **[更新（Update）]**をクリックします。

会社の詳細が確認されると、成功メッセージが表示されます。

ステップ 10 前のタブで開いた [スマートアカウントの作成（Create a Smart Account）] ページを開きます。変更が反映されていない場合は、ページを更新してください。

または、URL「https://software.cisco.com/software/company/smartaccounts/home?route=module/accountcreation」を使用してこのページを開き、ログイン情報を使用してログインすることもできます。

ステップ 11 [アカウントの作成（Create Account）] をクリックします。

[アカウントサマリー（Account Summary）] ページにアカウントの詳細が表示されます。

ステップ 12 [完了（Done）] をクリックします。

ステップ 13 スマートアカウントの設定準備ができたことを知らせる電子メールが届くのを待ちます。電子メールが届いたら、指示に従って、メールに含まれているリンクをクリックします。

ステップ 14 お使いのスマート ライセンシング アカウントに、必要なライセンスが含まれていることを確認してください。

ライセンス PID については、ライセンス PID （16 ページ）を参照してください。

次のタスク

Smart Software Manager を使用してスマートライセンスを設定するには、スマート ライセンスの設定 （29 ページ）を参照してください。

スマート ライセンスの設定

ここでは、Smart Software Manager または Smart Software Manager On-Prem を使用してスマートライセンスを使用する方法について説明します。特定ライセンス予約を使用するには、特定ライセンス予約（SLR）の設定 （44 ページ）を参照してください。

スマートライセンシングに関する Firewall Management Center の登録

Firewall Management Center は、インターネット経由で Smart Software Manager に直接登録できます。また、エアギャップネットワークを使用している場合は、Smart Software Manager オンプレミスを使用して登録できます。

Smart Software Manager での Firewall Management Center の登録

Smart Software Manager で Firewall Management Center を登録します。

始める前に

- お使いのスマート ライセンシング アカウントに、必要なライセンスが含まれていることを確認してください。

  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 を参照します。ライセンス PID については、ライセンス PID （16 ページ）を参照してください。

- Firewall Management Center が smartreceiver.cisco.com で Smart Software Manager にアクセスできることを確認します。

- NTP を設定してください。登録時に、スマートエージェントと Smart Software Manager 間でキー交換が実行されるため、適切な登録には時刻の同期が必要です。

  Firepower 4100/9300 シャーシの場合は、Firewall Management Center と同じ NTP サーバーをシャーシに使用してシャーシに NTP を設定する必要があります。

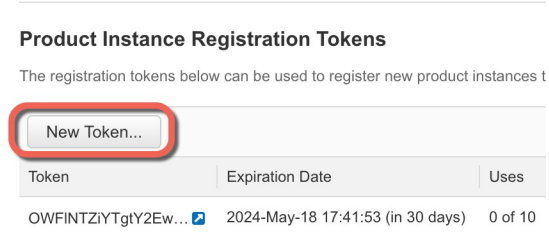
- 組織に複数の Firewall Management Center がある場合は、各 Firewall Management Center に明確に識別できる一意の名前が付いており、同じバーチャルアカウントに登録されている可能性がある他の Firewall Management Center と区別できることを確認します。この名前は、スマートライセンスの権限付与の管理にとって重要です。あいまいな名前だと後で問題が発生することがあります。

手順

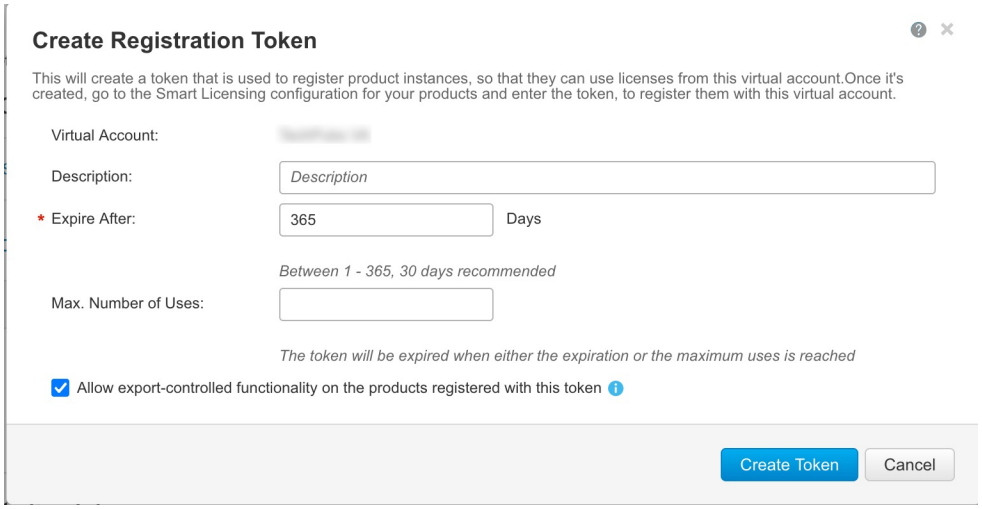
ステップ 1 Smart Software Manager で、このデバイスを追加する仮想アカウントの登録トークンを要求してコピーします。

a) [Inventory] をクリックします。

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



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



- **説明**
- [有効期限（Expire After）]：推奨値は 30 日です。
- 最大使用回数（Max. Number of Uses）
- [このトークンに登録された製品で輸出管理機能を許可する（Allow export-controlled functionality on the products registered with this token）]：高度暗号化が許可されている国の場合は輸出コンプライアンスフラグを有効にします。 この機能を使用する予定の場合、このオプションをここで選択する必要があります。後でこの機能を有効にする場合は、デバイスを新しいプロダクトキーで再登録し、デバイスをリロードする必要があります。このオプションが表示されない場合、アカウントは輸出規制機能をサポートしていません。

トークンはインベントリに追加されます。

d) トークンの右側にある矢印アイコンをクリックして [トークン（Token）] ダイアログボックスを開き、トークン ID をクリップボードにコピーできるようにします。Firewall Threat Defense 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 *3*: トークンの表示

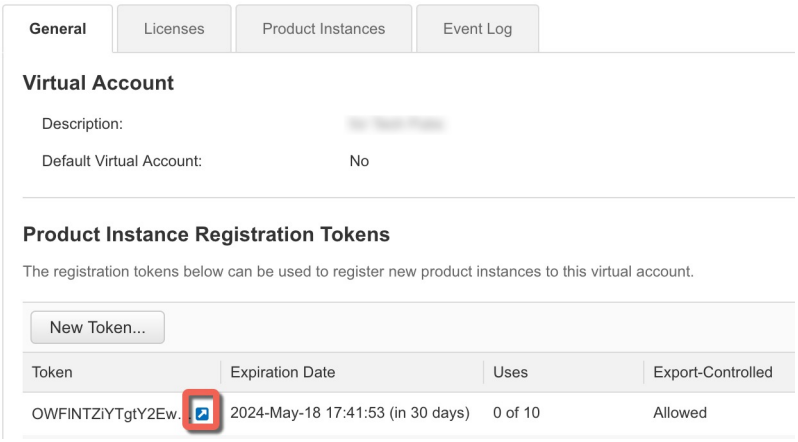
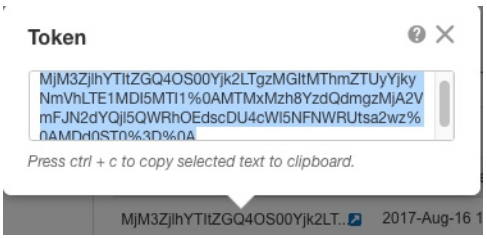


図 *4*: トークンのコピー



ステップ 2 Firewall Management Center で、[システム（System）]（⚙） > **[ライセンス（Licenses）]** > **[スマートライセンス（Smart Licenses）]** を選びます。

ステップ 3 [登録（Register）] をクリックします。

ステップ 4 Smart Software Manager から生成されたトークンを [製品インスタンス登録トークン（Product Instance Registration Token）] フィールドに貼り付けます。

テキストの前後にスペースや空白の行がないことを確認します。

ステップ 5 Management Center インスタンスがすでにスマートライセンスに登録されている場合は、[既存の登録済みManagement Centerインスタンスのオーバーライド（Override Existing Registered Management Center Instance）] チェックボックスをオンにして、スマートライセンスの既存の登録済み Management Center インスタンスをオーバーライドできます。

ステップ 6 使用状況データをシスコに送信するかどうかを決定します。

- シスコでは、Cisco Success Network の機能を通じて、シスコ製品のカスタマーエクスペリエンスを向上させるために、お客様の使用状況のメトリックと統計情報を収集しています。この機能は、デフォルトでイネーブルにされています。シスコへの Cisco Success Network テレメトリデータの送信をオプトアウトするには、使用状況のメトリックと統計をシスコと共有するための Firewall Management Center の設定を参照してください。シスコが収集するテレメトリデータの詳細については、[サンプルデータ（sample data）] をクリックしてください。

- Cisco Support Diagnostics の機能を通じて、シスコはお客様のデバイスから重要な情報を収集し、充実したサポートエクスペリエンスをお届けしています。この機能は、デフォルトでイネーブルにされています。シスコへの Cisco Support Diagnostics メトリックの送信をオプトアウトするには、デバイス正常性データをシスコと共有するための Firewall Management Center の設定を参照してください。

（注）
- Cisco Support Diagnostics を有効にすると、次の同期サイクルでデバイスに適用されます。Firewall Management Center とデバイスとの同期は、30 分ごとに 1 回実行されます。
- Cisco Support Diagnostics を有効にすると、この Firewall Management Center に登録される新しいデバイスに自動的に適用されます。

ステップ 7 [変更を適用（Apply Changes）] をクリックします。

次のタスク

- Firewall Management Center にデバイスを追加します。Cisco Secure Firewall Management Center デバイス構成ガイドの「Add a Device to the Firewall Management Center」を参照してください。
- ライセンスをデバイスに割り当てます。複数の管理対象デバイスへのライセンスの割り当て （37 ページ）を参照してください。

Firewall Management Center の Smart Software Manager オンプレミスへの登録

Smart Software Manager との定期的な通信 （3 ページ）で説明されているように、Firewall Management Center は、ライセンス権限を維持するためにシスコと定期的に通信する必要があります。次の状況のいずれかの場合、Smart Software Manager と接続するためのプロキシとして Smart Software Manager オンプレミス（旧称「Smart Software Satellite Server」）を使用できます。

- Firewall Management Center がオフラインである、接続が制限されている、または接続がない（つまり、エアギャップ ネットワークに展開されている）場合。

  （エアギャップネットワーク向けの代替ソリューションについては、エアギャップ展開のライセンスのオプション （2 ページ）を参照してください。）

- Firewall Management Center に固定接続があるが、ネットワークからの単一の接続によってスマート ライセンスを制御する場合。

Smart Software Manager オンプレミス を使用すると、同期スケジュールを設定、またはスマートライセンス認証を Smart Software Manager と手動で同期させることができます。

Smart Software Manager オンプレミス の詳細については、https://www.cisco.com/c/en/us/buy/smart-accounts/software-manager.html#~on-prem を参照してください。

手順

ステップ 1 Smart Software Manager オンプレミスを展開して設定します。

- Smart Software Manager オンプレミスのドキュメントを参照してください。https://www.cisco.com/c/en/us/buy/smart-accounts/software-manager.html#~on-prem から入手できます。
- Smart Software Manager オンプレミスの TLS/SSL 証明書の CN をメモします。
- http://www.cisco.com/security/pki/certs/clrca.cer に移動し、TLS/SSL 証明書の本文全体（"-----BEGIN CERTIFICATE-----" から "-----END CERTIFICATE-----" まで）を、設定中にアクセスできる場所にコピーします。

ステップ 2 Firewall Management Center を Smart Software Manager オンプレミス に登録します。

a) **[統合（Integration）] > [その他の統合（Other Integrations）]**を選択します。
b) [スマート ソフトウェア サテライト（Smart Software Satellite）] をクリックします。
c) [Cisco Smart Software Satellite Serverに接続（Connect to Cisco Smart Software Satellite Server）] を選択します。
d) この手順の前提条件で収集した CN 値を使用して、Smart Software Manager オンプレミスの **URL** を次の形式で入力します。

```
https://FQDN_or_hostname_of_your_SSM_On-Prem/SmartTransport
```

FQDN またはホスト名は、Smart Software Manager オンプレミスによって提示された証明書の CN 値と一致している必要があります。

e) 新しい [SSL 証明書（SSL Certificate）] を追加し、以前にコピーした証明書テキストを貼り付けます。
f) [適用（Apply）] をクリックします。
g) [システム（System）]>[ライセンス（Licenses）]>[スマートライセンス（Smart Licenses）] を選択し、[登録（Register）] をクリックします。
h) Smart Software Manager オンプレミスに新しいトークンを作成します。
i) トークンをコピーします。
j) トークンを管理センター ページのフォームに貼り付けます。
k) [変更を適用（Apply Changes）] をクリックします。

管理センターが Smart Software Manager オンプレミスに登録されました。

ステップ 3 デバイスにライセンスを割り当てた後、Smart Software Manager オンプレミス を Smart Software Manager に同期させます。

上記のSmart Software Manager オンプレミスのドキュメントを参照してください。

ステップ 4 継続的な同期時刻をスケジュールします。

グローバル権限のないアカウントの輸出規制機能の有効化

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

始める前に

- 展開でまだ輸出規制対象の機能がサポート**されていない**ことを確認します。

  展開で輸出規制対象の機能がサポートされている場合、Smart Software Manager の [登録トークンの作成（Create Registration Token）] ページに輸出規制対象の機能を有効にできるオプションが表示されます。詳細については、https://www.cisco.com/c/en/us/buy/smart-accounts/software-manager.htmlを参照してください。

- 展開で評価ライセンスが使用されていないことを確認します。
- Smart Software Manager の **[インベントリ（Inventory）]** > **[ライセンス（Licenses）]** ページで、Firewall Management Center に対応するライセンスがあることを確認します。

輸出規制ライセンス	Firewall Management Center モデル
Cisco Virtual FMC シリーズの強力な暗号化（3DES/AES）	すべての Firewall Management Center Virtual
Cisco FMC 1K シリーズの強力な暗号化（3DES/AES）	1000、 1600
Cisco FMC 2 K シリーズの強力な暗号化（3DES/AES）	2500、2600
Cisco FMC 4K シリーズの強力な暗号化（3DES/AES）	4500、4600

手順

ステップ 1 **[システム（System）]** > **[ライセンス（Licenses）]** > **[スマート ライセンス（Smart Licenses）]** を選択します。

（注）
[輸出キーの要求（Request Export Key）] が表示されている場合は輸出規制対象の機能がアカウントに承認されています。そのため、必要な機能の使用に進むことができます。

ステップ 2 [エクスポート キーの要求（Request Export Key）] をクリックして、エクスポート キーを生成します。

ヒント

エクスポート制御キーの要求に失敗した場合は、バーチャルアカウントに有効なエクスポート制御ライセンスがあることを確認します。

[輸出キーの返却（Return Export Key）] をクリックして、輸出規制ライセンスを無効にします

次のタスク

これで、輸出規制対象の機能を使用する設定またはポリシーを展開できるようになります。

メモ これによって有効にされた新しい輸出規制対象のライセンスとすべての機能は、Firewall Threat Defense デバイスが再起動されるまでそのデバイスでは有効になりません。それまでは、前のライセンスでサポートされていた機能のみがアクティブになります。

高可用性展開では、アクティブ/アクティブの状態を避けるために両方の Firewall Threat Defense デバイスを再起動する必要があります。

デバイスへのライセンスの割り当て

Firewall Management Center にデバイスを登録すると、ほとんどのライセンスを割り当てることができます。デバイスごと、または複数のデバイスにライセンスを割り当てることもできます。

単一のデバイスへのライセンスの割り当て

一部の例外はありますが、管理対象デバイスでライセンスを無効にすると、そのライセンスに関連づけられている機能は使用できなくなります。

（注） 同じ セキュリティ モジュール/エンジン のコンテナ インスタンスの場合は、ライセンスを各インスタンスに適用します。ただし、セキュリティ モジュール/エンジン のすべてのインスタンスについては、セキュリティ モジュール/エンジン は機能ごとに 1 つのライセンスのみを使用します。

（注） Firewall Threat Defense クラスタの場合は、クラスタ全体にライセンスを適用します。ただし、クラスタ内の各ユニットが機能ごとに個別のライセンスを使用します。

始める前に

このタスクを実行するには、管理者権限またはネットワーク管理者権限が必要です。複数のドメインを操作する場合は、このタスクをリーフドメインで実行する必要があります。

手順

ステップ 1 **[デバイス（Devices）]** > **[デバイス管理（Device Management）]**を選択します。

ステップ 2 ライセンスを割り当てまたは無効にするデバイスの横にある [編集（Edit）]（） をクリックします。

ステップ 3 [デバイス（Device）] をクリックします。

ステップ 4 [ライセンス（License）] セクションの横にある [編集（Edit）]（） をクリックします。

ステップ 5 適切なチェックボックスをオンまたはオフにして、デバイスのライセンスを割り当て、または無効にします。

ステップ 6 [保存（Save）] をクリックします。

ステップ 7 設定変更を展開します。Cisco Secure Firewall Management Center デバイス構成ガイドを参照してください。

次のタスク

ライセンスステータスの確認：[システム（System）]（） > **[ライセンス（Licenses）]** > **[スマートライセンス（Smart Licenses）]**に移動し、[スマートライセンス（Smart Licenses）] テーブル上部のフィルタにホスト名またはデバイスの IP アドレスを入力し、各デバイスおよび各ライセンスタイプに、**チェックマーク**（） のある緑色の円のみが表示されることを確認します。その他のアイコンが表示される場合は、アイコンにマウスオーバーすると詳細を確認できます。

複数の管理対象デバイスへのライセンスの割り当て

Firewall Management Center によって管理されるデバイスは、ライセンスを、Smart Software Manager から直接ではなく Firewall Management Center 経由で取得します。

複数のデバイスでライセンスを一度に有効にするには、次の手順を使用します。

（注） 同じ セキュリティ モジュール/エンジン のコンテナ インスタンスの場合は、ライセンスを各インスタンスに適用します。ただし、セキュリティ モジュール/エンジン のすべてのインスタンスについては、セキュリティ モジュール/エンジン は機能ごとに 1 つのライセンスのみを使用します。

（注） Firewall Threat Defense クラスタの場合は、クラスタ全体にライセンスを適用します。ただし、クラスタ内の各ユニットが機能ごとに個別のライセンスを使用します。

手順

ステップ 1 [システム（System）]（⚙）>**[ライセンス（Licenses）]**>**[スマートライセンス（Smart Licenses）]** または [特定のライセンス（Specific Licenses）] を選択します。

ステップ 2 [ライセンスの編集（Edit Licenses）] をクリックします。

ステップ 3 デバイスに追加するライセンスのタイプごとに、次の手順を実行します。

a) 該当するライセンスのタイプのタブをクリックします。

b) 左側のリスト内のデバイスをクリックします。

c) [追加（Add）] をクリックして、デバイスを右側のリストに移動させます。

d) 各デバイスが該当するタイプのライセンスを受信するまで、この手順をデバイスごとに繰り返します。

ここでは、追加するすべてのデバイスのライセンスをユーザが保持しているかどうかを気にする必要はありません。

e) 追加するライセンスのタイプごとに、この手順を繰り返します。

f) ライセンスを削除するには、デバイスの横にある [削除（Delete）]（🗑）をクリックします。

g) [適用（Apply）] をクリックします。

クラスタを選択し、クラスタのすべてのノードに任意のライセンスを割り当てることができます。

次のタスク

ライセンスが正しくインストールされていることを確認します。「スマートライセンスのモニタリング （40 ページ）」の手順に従います。

スマートライセンスの管理

このセクションでは、スマートライセンスを管理する方法について説明します。

の登録解除Firewall Management Center

Smart Software Manager から Firewall Management Center の登録を解除して、すべてのライセンス資格をスマートアカウントに戻し、他のデバイスで使用できるようにします。たとえば、Firewall Management Center を廃止または再イメージ化する必要がある場合は、登録を解除します。

未登録の状態でのライセンス施行の詳細については、未登録状態 （5 ページ）を参照してください。

手順

ステップ 1 [システム（System）]（⚙）>**[ライセンス（Licenses）]**>**[スマートライセンス（Smart Licenses）]**を選択します。

ステップ 2 **登録解除**（🔴）をクリックします。

Firewall Management Center の同期または再認証

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 [システム（System）]（⚙）>**[ライセンス（Licenses）]**>**[スマートライセンス（Smart Licenses）]**を選択します。

ステップ 2 アイデンティティ証明書を更新するには、**同期**（🔄）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、[再認証（Re-Authorize）] をクリックします。

スマートライセンスのステータスのモニタリング

[システム（System）]>[ライセンス（Licenses）]>[スマートライセンス（Smart Licenses）] ページの [スマートライセンスのステータス（Smart License Status）] セクションでは、次に示すとおり、Firewall Management Center でのライセンスの使用状況の概要が提供されます。

使用の認証

可能なステータス値は次のとおりです。

- **コンプライアンス適合**（✔）：管理対象デバイスに割り当てられているすべてのライセンスが要求を満たしており、Firewall Management Center が Smart Software Manager と正常に通信しています。
- **ライセンスは要求を満たしているが、ライセンス認証局との通信に失敗した**：デバイスのライセンスは要求を満たしていますが、Firewall Management Center がシスコのライセンス認証局と通信できません。
- **コンプライアンス不適合のアイコンまたはライセンス認証局と通信できない**：1 つ以上の管理対象デバイスがコンプライアンス不適合のライセンスを使用しているか、Firewall

Management Center が Smart Software Manager と通信していない期間が 90 日を超えています。

製品登録

Firewall Management Center が Smart Software Manager に連絡し登録された最終日を指定します。

割当済みの仮想アカウント

製品インスタンス登録トークンの生成に使用したスマートアカウントの下の仮想アカウントを指定し、Firewall Management Center を登録します。この展開がスマートアカウント内の特定の仮想アカウントに関連付けられていない場合は、この情報は表示されません。

輸出管理機能

このオプションが有効になっている場合、制限機能を展開できます。詳細は、「輸出規制対象の機能のライセンス （13 ページ）」を参照してください。

Cisco Success Network

Firewall Management Centerの Cisco Success Network を有効にしたかどうかを指定します。このオプションを有効にすると、テクニカルサポートを提供するために不可欠な使用状況に関する情報と統計がシスコに提供されます。また、この情報により、シスコは製品を向上させ、未使用の使用可能な機能を認識させるため、ネットワーク内にある製品の価値を最大限に生かすことができます。詳細については、使用状況のメトリックと統計をシスコと共有するための Firewall Management Center の設定を参照してください。

スマートライセンスのモニタリング

Firewall Management Center とその管理対象デバイスのライセンスステータスを表示するには、[スマートライセンス（Smart Licenses）] ページを使用します。

このページには、展開におけるライセンスのタイプごとに、使用されているライセンスの総数、そのライセンスのコンプライアンスの適合または不適合の状態、デバイスタイプ、およびデバイスが展開されているドメインとグループが表示されます。また、Firewall Management Center のスマートライセンス ステータスを表示できます。同じセキュリティ モジュール/エンジン 上のコンテナインスタンスは セキュリティ モジュール/エンジン ごとに 1 つのライセンスのみを使用します。したがって、ライセンスタイプごとに各コンテナライセンスが個別に Firewall Management Center に表示されても、機能ライセンスタイプに使用されているライセンスの数は 1 つのみです。

[スマートライセンス（Smart Licenses）] ページ以外にも、ライセンスを表示できる方法がいくつかあります。

- [製品ライセンス（Product Licensing）] ダッシュボードウィジェットはライセンスの概要を示します。

「ダッシュボードへのウィジェットの追加」、「ユーザー ロール別のダッシュボード ウィジェットの可用性」、および「[製品ライセンス（Product Licensing）] ウィジェット」を参照してください。

- [デバイス管理（Device Management）] ページ（**[デバイス（Devices）] > [デバイス管理（Device Management）]**）は、各管理対象デバイスに適用されているライセンスをリストします。
- ヘルスポリシーで使用される際に、[スマートライセンスモニター（Smart License Monitor）] のヘルスモジュールはライセンスステータスを伝達します。

手順

ステップ 1 [システム（System）]（⚙）> **[ライセンス（Licenses）] > [スマートライセンス（Smart Licenses）]** を選択します。

ステップ 2 [スマート ライセンス（Smart Licenses）] テーブルで、各 [ライセンス タイプ（License Type）] フォルダの左側にある矢印をクリックしてそのフォルダを展開します。

ステップ 3 各フォルダで、各デバイスの [ライセンスステータス（License Status）] 列に **チェックマーク**（✓）付きの緑の円が表示されていることを確認します。

（注）
Firewall Management Center Virtual ライセンスが重複している場合は、それぞれが 1 つの管理対象デバイスを表します。

すべてのデバイスに **チェックマーク**（✓）付きの緑の円が表示されている場合、デバイスには適切なライセンスがあり、使用できる状態にあります。

チェックマーク（✓）付きの緑の円以外のライセンスステータスが表示されている場合は、ステータスアイコンにマウスカーソルを合わせてメッセージを確認します。

次のタスク

- **チェックマーク**（✓）付きの緑の円が表示されているデバイスがない場合は、追加ライセンスの購入が必要な可能性があります。

スマート ライセンスのトラブルシューティング

予期していたライセンスがスマート アカウントに表示されません。

表示されると思っていたライセンスがスマート アカウントにない場合は、次を試してください。

- 他の仮想アカウントにないことを確認します。この問題について、組織のライセンス管理者によるサポートが必要な場合があります。

- ライセンスを販売した担当者と、アカウントへの譲渡が完了していることを確認します。

スマートライセンスサーバーに接続できない

最初に、明らかな原因を確認します。たとえば、Firewall Management Center に外部接続があることを確認します。インターネットリソースへのアクセス を参照してください。

予期していなかったコンプライアンス不適合の通知またはその他のエラー

- デバイスが別の Firewall Management Center にすでに登録されている場合は、新しい Firewall Management Center にデバイスのライセンスを付与する前に元の Firewall Management Center の登録を解除する必要があります。の登録解除Firewall Management Center （38 ページ）を参照してください。
- サブスクリプション ライセンスの有効期限が切れているかどうかを確認します。

その他の問題のトラブルシュート

その他の一般的な問題の解決方法については、https://www.cisco.com/c/en/us/support/docs/security/firepower-management-center/215838-fmc-and-ftd-smart-license-registration-a.html を参照してください

Firewall Threat Defense で使用するためのクラシックライセンスの変換

ライセンス登録ポータルまたは Smart Software Manager のいずれかを使用してライセンスを変換し、未使用の製品認証キー（PAK）またはデバイスにすでに割り当てられているクラシックライセンスに変換することができます。

（注） このプロセスは元に戻すことはできません。そのライセンスが元々はクラッシク ライセンスであっても、スマート ライセンスをクラッシク ライセンスに変換することはできません。

Cosco.com のドキュメントでは、クラッシック ライセンスは「従来型の」ライセンスとも呼ばれています。

始める前に

- 製品インスタンスにまだ割り当てられていない未使用の PAK がある場合、従来のライセンスからスマート ライセンスへの変換は最も簡単です。
- ハードウェアで Firewall Threat Defense を実行できる必要があります。https://www.cisco.com/c/en/us/support/security/defense-center/products-device-support-tables-list.html の『*Cisco Secure Firewall Threat Defense Compatibility Guide*』『』を参照してください。
- スマート アカウントが必要です。ない場合は作成します。「スマートアカウントの作成とライセンスの追加 （27 ページ）」を参照してください。

- 変換する PAK またはライセンスは、スマート アカウントに表示されている必要があります。
- Smart Software Manager ではなくライセンス登録ポータルを使用して変換する場合に変換プロセスを開始するには、スマート アカウント クレデンシャルを保有している必要があります。

手順

ステップ 1 実行する変換プロセスは、そのライセンスが使用されたことがあるかどうかによって異なります。

- 変換する PAK が使用されたことがない場合は、PAK の変換の手順を実行します。
- 変換する PAK がデバイスにすでに割り当てられている場合は、クラッシク ライセンスの変換の手順を実行します。

  既存の従来のライセンスがまだデバイスに登録されていることを確認します。

ステップ 2 次のドキュメントで変換のタイプ（PAK またはインストール済みのクラシック ライセンス）の手順を参照してください。

- ライセンス登録ポータルを使用して PAK またはライセンスを変換するには、次の手順を実行します。
  - スマートアカウントによる Cisco Classic Licensing Managementでの変換プロセスの License Registration Portal 部分を説明するビデオを表示します。
  - https://tools.cisco.com/SWIFT/LicensingUI/Home でライセンス登録ポータルにサインインし、上記のドキュメントの手順を実行します。
- Smart Software Manager を使用して PAK またはライセンスを変換するには、次の手順を実行します。
  - ハイブリッドライセンスをスマート ソフトウェア ライセンス *QRG* に変換するには、次の手順を実行します。

    https://community.cisco.com/t5/licensing-enterprise-agreements/converting-hybrid-licenses-to-smart-software-licenses-qrg/ta-p/3628609?attachment-id=134907
  - https://software.cisco.com/#SmartLicensing-LicenseConversion で Smart Software Manager にサインインし、上記のドキュメントの変換タイプ（PAK またはインストール済みのクラッシックライセンス）の手順を実行します。

ステップ 3 ハードウェアに Firewall Threat Defense を新たにインストールします。

インストールおよびアップグレードガイドにあるハードウェアに関する手順を参照してください。

ステップ 4 Firewall Device Manager を使用してこのデバイスをスタンドアロンデバイスとして管理するには、次の手順を実行します。

Secure Firewall Device Manager Configuration Guidesにある Firewall Device Manager の設定ガイドに含まれるデバイスのライセンシングに関する説明を参照してください。

この手順の残りは省略してください。

ステップ 5 Firewall Management Center でスマート ライセンスをすでに展開している場合は、次の手順を実行します。

a) 新しい Firewall Threat Defense でスマートライセンスを設定します。

複数の管理対象デバイスへのライセンスの割り当て （37 ページ）を参照してください。

b) 新しいスマート ライセンスがデバイスに正常に適用されていることを確認します。

スマートライセンスのモニタリング （40 ページ）を参照してください。

ステップ 6 Firewall Management Center でスマート ライセンスをまだ展開していない場合は、次の手順を実行します。

「スマート ライセンスの設定 （29 ページ）」を参照してください。（該当しないか、またはすでに完了しているステップはスキップします。）

特定ライセンス予約（SLR）の設定

特定のライセンスの予約機能を使用して、エアギャップ ネットワークにスマート ライセンスを展開できます。

（注） シスコでは、特定のライセンス予約に SLR、SPLR、PLR、永久ライセンス予約などのさまざまな名前を使用しています。シスコでは、これらの用語が、類似しているものの必ずしも同一ではないライセンスモデルを指すために使用される場合もあります。

特定のライセンスの予約が有効になっている場合、Firewall Management Center は、Smart Software Manager にアクセスせずに、または Smart Software Manager オンプレミス を使用せずに、バーチャルアカウントからライセンスを指定された期間予約します。

インターネットへのアクセスが必要なパブリック Web サイトに対する URL ルックアップや状況に応じた相互起動などの機能は動作しません。

シスコは、特定のライセンスの予約を使用する展開に関する Web 分析やテレメトリのデータを収集しません。

特定ライセンス予約の要件および前提条件

特定のライセンス予約への切り替え

現時点で通常のスマートライセンスを使用している場合、特定のライセンス予約を導入する前に Smart Software Manager から Firewall Management Center を登録解除します。「の登録解除 Firewall Management Center （38 ページ）」を参照してください。

Firewall Management Center に現在展開されているすべてのスマートライセンスがアカウントで使用可能なライセンスのプールに戻され、特定のライセンスの予約を実装すると再利用できるようになります。

特定のライセンス予約および高可用性

ライセンスを割り当てる前に高可用性を設定することを推奨します。セカンダリ Firewall Management Center のデバイスにすでにライセンスを割り当てている場合は、それらの割り当てを解除してください。

SLR ライセンスがプライマリ Firewall Management Center に割り当てられている場合、フェールオーバー後にセカンダリ Firewall Management Center がアクティブになると、SLR ライセンスをセカンダリ Firewall Management Center に追加できません。次のいずれかを実行する必要があります。

- フェールオーバーを実行して、プライマリ Firewall Management Center をアクティブにします。
- ライセンスの割り当てを解除し、セカンダリ Firewall Management Center に再割り当てします。

特定のライセンス予約を使用した脅威インテリジェンスのダウンロード

Security Services Exchange（SSE） の統合は、 へのセキュアな接続に必要です。ここではシステムは次を取得します。

- 侵入ルールの更新
- URL フィルタリングデータとルックアップ
- イベント エンリッチメント データ

Talos 接続ステータス正常性モジュールは、 との接続を監視します。

通常のスマートライセンスを使用している場合、Smart Software Manager で登録すると、SSE の統合が設定されます。ただし、エアギャップ以外の展開で特定のライセンス予約を使用している場合は、代わりに Cisco Security Cloud を有効にする必要があります：「Cisco Security Cloud 統合の有効化」。

データ共有に懸念がある場合は、イベントストレージ、Cisco Success Network、Cisco Support Diagnostics を含むすべての共有オプションを無効化します。ただし Firewall Management Center

は、インターネットリソースへのアクセスにリストされている地域クラウドに到達できる必要があります。

エアギャップ展開では、サポートされていないイベントエンリッチメントを除き、脅威インテリジェンスを手動で更新することに注意してください。

スマートアカウントが特定のライセンスの予約の展開の準備が整っているかどうかの確認

特定ライセンス予約の展開時の問題を防ぐため、Firewall Management Center に変更を加える前にこの手順を実行します。

始める前に

- 「特定ライセンス予約の要件および前提条件 （45 ページ）」で説明した要件を満たしていることを確認します。
- Smart Software Manager のクレデンシャルがあることを確認します。

手順

ステップ 1 Smart Software Manager にサインインします。

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

ステップ 2 該当する場合は、ページの右上隅から正しいアカウントを選択します。

ステップ 3 必要に応じて、[インベントリ（Inventory）] をクリックします。

ステップ 4 [ライセンス（Licenses）] をクリックします。

ステップ 5 次のことを確認してください。

- [ライセンスの予約（License Reservation）] ボタンが表示されている。
- 該当する場合は、デバイスの Firewall Management Center Virtual の付与資格を含めて展開するデバイスおよび機能に十分なプラットフォームライセンスと機能ライセンスがある。

ステップ 6 これらのアイテムがないか、または誤っている場合は、アカウント担当者に連絡して問題を解決します。

（注）
問題が修正されるまではこのプロセスは続行しないでください。

[特定のライセンス（Specific Licenses）] メニューオプションの有効化

この手順では、Firewall Management Center の [スマートライセンス（Smart Licenses）] メニュー オプションを [特定のライセンス（Specific Licenses）] に変更します。

手順

ステップ 1 USB キーボードと VGA モニターを使用して Firewall Management Center コンソールにアクセスするか、SSH を使用して管理インターフェイスにアクセスします。

ステップ 2 Firewall Management Center の CLI **管理者**アカウントにログインします。

ステップ 3 **expert** コマンドを入力して Linux シェルにアクセスします。

ステップ 4 特定のライセンスの予約のオプションにアクセスするには、次のコマンドを実行します。

sudo manage_slr.pl

例：

```
admin@fmc63betaslr: ~$ sudo manage_slr.pl
Password:


*************** Configuration Utility **************

1   Show SLR Status
2   Enable SLR
3   Disable SLR
0   Exit

************************************************************
Enter choice:
```

ステップ 5 オプション **2** を選択して、特定ライセンス予約を有効にします。

ステップ 6 オプション **0** を選択して、manage_slr ユーティリティを終了します。

ステップ 7 **exit** と入力し、Linux シェルを終了します。

ステップ 8 **exit** コマンドを入力してセキュアシェルのコマンドライン インターフェイスを終了します。

ステップ 9 Firewall Management Center の Web インターフェイスの [特定のライセンスの予約（Specific License Reservation）] ページにアクセスできることを確認します。

- [システム（System）]>[ライセンス（Licenses）]>[スマートライセンス（Smart Licenses）] ページが現在表示されている場合は、ページを更新します。
- それ以外の場合は、[システム（System）]>[ライセンス（Licenses）]>[特定のライセンス（Specific Licenses）] を選択します。

Firewall Management Center への特定のライセンス予約承認コードの入力

手順

ステップ 1 予約要求コードを生成します。

a) Firewall Management Center で、**[システム（System）]** > **[ライセンス（Licenses）]** > **[個別ライセンス（Specific Licenses）]** を選択します。
b) [生成（Generate）] をクリックします。
c) **予約要求コード**をメモします。

ステップ 2 予約承認コードを生成します。

a) Cisco Smart Software Manager に移動します：https://software.cisco.com/#SmartLicensing-Inventory
b) 必要に応じて、ページの右上から正しいアカウントを選択します。
c) 必要に応じて、[インベントリ（Inventory）] をクリックします。
d) [ライセンス（Licenses）] をクリックします。
e) [ライセンスの予約（License Reservation）] をクリックします。
f) 生成したコードを Firewall Management Center から [予約要求コード（Reservation Request Code）] ボックスに入力します。
g) [次へ（Next）] をクリックします。
h) [特定のライセンスの予約（Reserve a specific license）] を選択します。
i) 下にスクロールしてライセンス グリッド全体を表示します。
j) [予約する数量（Quantity To Reserve）] に、展開に必要な各プラットフォームと機能の数を入力します。

（注）
- 管理対象デバイスごとに（マルチインスタンス展開の場合はコンテナごとに）Essentials ライセンスを明示的に含める必要があります。
- Firewall Management Center Virtualを使用している場合は、各モジュール（マルチインスタンス展開において）または各管理対象デバイス（他のすべての展開において）にプラットフォームの資格を組み込む必要があります。
- 強力な暗号化機能を使用する場合は、次のとおりです。
  - スマート アカウント全体が輸出規制対象機能に対して有効になっている場合は、ここで何もする必要はありません。
  - 組織の資格が Firewall Management Center 単位の場合は、アプライアンス向けに適切なライセンスを選択する必要があります。

  Firewall Management Centerに適切なライセンス名を選択するには、「グローバル権限のないアカウントの輸出規制機能の有効化 （35 ページ）」の前提条件を参照してください。

k) [次へ（Next）] をクリックします。
l) [承認コードを生成（Generate Authorization Code）] をクリックします。

この時点で、ライセンスは、Smart Software Manager に従って使用中です。

m) Firewall Management Center に入力するための準備として承認コードをダウンロードします。

ステップ 3 Firewall Management Centerに承認コードを入力します。

a) Firewall Management Center で、[参照（Browse）] をクリックして、Smart Software Manager から生成した承認コードを含むテキストファイルをアップロードします。
b) [Install（インストール）] をクリックします。
c) [特定のライセンスの予約（Specific License Reservation）] ページに [使用の承認（Usage Authorization）] ステータスが [承認済み（authorized）] と表示されていることを確認します。
d)

ステップ 4 [予約済みライセンス（Reserved Licenses）] タブをクリックして、[承認コード（Authorization Code）] の生成時に選択したライセンスを確認します。

必要なライセンスが表示されていない場合は、必要なライセンスを追加します。詳細については、「Firepower Management Center の特定のライセンスの更新」を参照してください。

管理対象デバイスへの特定のライセンスの割り当て

この手順を使用して、複数の管理対象デバイスにライセンスを一度にすばやく割り当てます。

また、この手順を使用してライセンスを無効にするか、または1つのデバイスから別のデバイスにライセンスを移動できます。デバイスのライセンスを無効にすると、ライセンスに関連付けられた機能をそのデバイスで使用できません。

手順

ステップ 1 [システム（System）] > [ライセンス（Licenses）] > [個別ライセンス（Specific Licenses）] を選択します。
ステップ 2 [ライセンスの編集（Edit Licenses）] をクリックします。
ステップ 3 各タブをクリックし、必要に応じてデバイスにライセンスを割り当てます。
ステップ 4 [適用（Apply）] をクリックします。
ステップ 5 [割り当て済みのライセンス（Assigned Licenses）] タブをクリックし、各デバイスでライセンスが正しくインストールされていることを確認します。
ステップ 6 設定変更を展開します。Cisco Secure Firewall Management Center デバイス構成ガイドを参照してください。

特定ライセンス予約の管理

このセクションでは、特定ライセンス予約を管理する方法について説明します。

重要：特定ライセンス予約展開の維持

展開を有効に保つ脅威に関するデータとソフトウェアを更新するには、「エアギャップ展開の維持」を参照してください。

すべての機能が中断せずに動作し続けるようにするには、ライセンスの有効期限を（[予約済みライセンス（Reserved Licenses）] タブ）で監視します。いずれかのライセンスの有効期限が切れたときに使用数が使用可能数よりも大きいと、Firewall Management Center は [不適合（Out of Compliance）] 状態になります。

特定のライセンスの予約の更新

Firewall Management Center で特定のライセンスが正常に展開された後は、この手順を使用して付与資格をいつでも追加または削除できます。

ライセンスの有効期限が切れた後にライセンスを更新する必要がある場合は、この手順を使用します。必要なライセンスがない場合、次のアクションが制限されます。

- デバイス登録に使用
- ポリシーの展開

手順

ステップ 1 Firewall Management Center で、この Firewall Management Center の一意の製品インスタンス識別子を取得します。

a) **[システム（System）]>[ライセンス（Licenses）]>[特定のライセンス（Specific Licenses）]** を選択します。

b) [製品インスタンス（Product Instance）] の値をメモします。

この値はこのプロセス中に何度か必要になります。

ステップ 2 Smart Software Manager で、更新する Firewall Management Center を特定します。

a) Smart Software Manager に移動します。

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

b) 必要に応じて、[インベントリ（Inventory）] をクリックします。

c) [製品インスタンス（Product Instances）] をクリックします。

d) [タイプ（Type）] 列に **FP**、[名前（Name）] 列に一般的な SKU（ホスト名ではない）が設定されている製品インスタンスを探します。また他のテーブル列の値を使用すると、どの Firewall Management Center が正しい Firewall Management Center かを判断するのに役立ちます。名前をクリックします。

e) **UUID** を調べ、変更しようとしている Firewall Management Center の UUID かどうかを確認します。

違う場合は、正しい Firewall Management Center が見つかるまで、これらの手順を繰り返す必要があります。

ステップ 3 Smart Software Manager で適切な Firewall Management Center が見つかったら、予約したライセンスを更新し、新しい承認コードを生成します。

a) 正しい UUID が表示されているページで、**[アクション（Actions）]** > **[予約済みのライセンスの更新（Update Reserved Licenses）]** を選択します。

b) 必要に応じて、予約済みライセンスを更新します。

（注）
- 管理対象デバイスごとに（マルチインスタンス展開の場合はコンテナごとに）Essentials ライセンスを明示的に含める必要があります。
- Firewall Management Center Virtualを使用している場合は、各モジュール（マルチインスタンス展開において）または各管理対象デバイス（他のすべての展開において）にプラットフォームの資格を組み込む必要があります。
- 強力な暗号化機能を使用する場合は、次のとおりです。
  - スマートアカウント全体が輸出規制対象機能に対して有効になっている場合は、ここで何もする必要はありません。
  - 組織の資格が Firewall Management Center 単位の場合は、アプライアンス向けに適切なライセンスを選択する必要があります。

    Firewall Management Centerに適切なライセンス名を選択するには、「グローバル権限のないアカウントの輸出規制機能の有効化 （35 ページ）」の前提条件を参照してください。

c) [次へ（Next）] をクリックして詳細を確認します。

d) [承認コードを生成（Generate Authorization Code）] をクリックします。

e) Firewall Management Center に入力するための準備として承認コードをダウンロードします。

f) [予約の更新（Update Reservation）] ページを開いたままにしておきます。この手順の後半でこのページに戻ります。

ステップ 4 Firewall Management Center で個別ライセンスを更新します。

a) **[システム（System）]** > **[ライセンス（Licenses）]** > **[個別ライセンス（Specific Licenses）]** を選択します。

b) [SLR の編集（Edit SLR）] をクリックします。

c) [参照（Browse）] をクリックして、新たに生成された承認コードをアップロードします。

d) [インストール（Install）] をクリックしてライセンスを更新します。

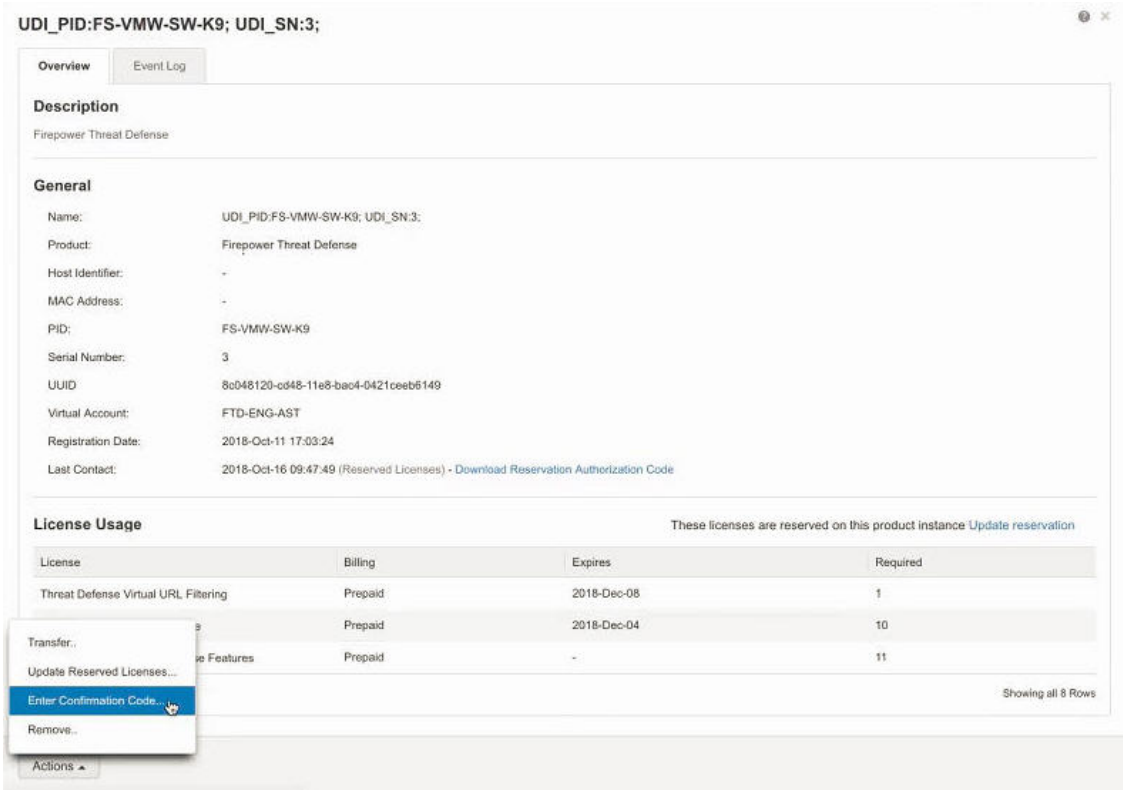
承認コードが正常にインストールされたら、Firewall Management Center の [予約済み（Reserved）] 列に表示されたライセンスが、Smart Software Manager で予約したライセンスと一致していることを確認します。

e) **確認コード**をメモします。

ステップ 5 Smart Software Manager に承認コードを入力するには、次の手順を実行します。

a) この手順の前半で開いたままにしておいた Smart Software Manager のページに戻ります。

b) **[アクション（Actions）]** > **[確認コードの入力（Enter Confirmation Code）]** を選択します。



c) Firewall Management Center から生成したコードを入力します。

ステップ 6 Firewall Management Center で、ライセンスが予期したとおりに予約されていること、および各管理対象デバイスの各機能に **チェックマーク**（✔） が付いた緑色の丸が表示されていることを確認します。

詳細については「特定ライセンス予約のステータスのモニタリング （55 ページ）」を必要に応じて参照してください。

ステップ 7 設定変更を展開します。Cisco Secure Firewall Management Center デバイス構成ガイドを参照してください。

特定のライセンスの予約の非アクティブ化と返却

特定のライセンスが不要になった場合は、そのライセンスをスマートアカウントに戻す必要があります。スマート ライセンシング アカウントを登録する場合は、[特定のライセンスの予約（Specific License Reservation）] を無効にする必要があります（以下の手順の手順 6）。

重要 この手順のすべてのステップを実行しないと、ライセンスは使用中の状態のままとなり、再利用できません。

この手順で、Firewall Management Center と関連付けられていたすべてのライセンス権限がバーチャルアカウントに戻されます。登録を解除すると、ライセンスが付与された機能への更新や変更が許可されなくなります。

手順

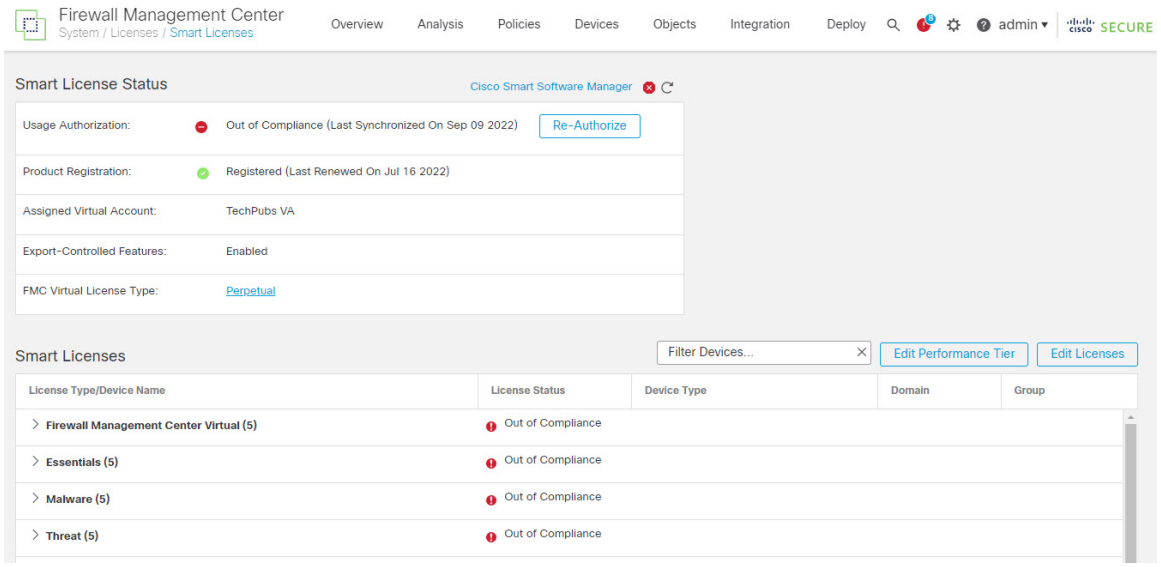
ステップ 1 Firewall Management Center の Web インターフェイスで、[システム（System）] > [ライセンス（Licenses）] > [特定のライセンス（Specific License）] を選択します。

ステップ 2 この Firewall Management Center の [製品インスタンス（Product Instance）] の識別子をメモします。

ステップ 3 Firewall Management Center からリターンコードを生成します。

a) [SLR の返却（Return SLR）] をクリックします。

次の図に、[SLR の返却（Return SLR）] を示します。



デバイスはライセンスのない状態になり、Firewall Management Center は登録解除状態に移行します。リターンコードが生成され、Firewall Management Center を SLR に再登録できます。

b) **返却コード**をメモします。

ステップ 4 Smart Software Manager で、登録解除する Firewall Management Center を特定します。

a) Smart Software Manager に移動します。

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

b) 必要に応じて、[インベントリ（Inventory）] をクリックします。
c) [製品インスタンス（Product Instances）] をクリックします。
d) [タイプ（Type）] 列に **FP**、[名前（Name）] 列に一般的な SKU（ホスト名ではない）が設定されている製品インスタンスを探します。また他のテーブル列の値を使用すると、どの Firewall Management Center が正しい Firewall Management Center かを判断するのに役立ちます。名前をクリックします。
e) **UUID** を調べ、変更しようとしている Firewall Management Center の UUID かどうかを確認します。

違う場合は、正しい Firewall Management Center が見つかるまで、これらの手順を繰り返す必要があります。

ステップ 5 正しい Firewall Management Center が特定されたら、ライセンスをスマートアカウントに戻します。

a) 正しい UUID が表示されたページで、[アクション（Actions）] > [削除（Remove）] を選択します。
b) Firewall Management Center から生成した予約リターンコードを [製品インスタンスの削除（Remove Product Instance）] ダイアログボックスに入力します。
c) [Remove Product Instance] をクリックします。

特定の予約済みライセンスがスマートアカウントの使用可能プールに戻り、この Firewall Management Center が Smart Software Manager の製品インスタンスリストから削除されます。

ステップ 6 Firewall Management Center の Linux シェルで、特定のライセンスを無効にします。

a) USB キーボードと VGA モニターを使用して Firewall Management Center コンソールにアクセスするか、SSH を使用して管理インターフェイスにアクセスします。
b) Firewall Management Center の CLI **管理者**アカウントにログインします。これにより、コマンドライン インターフェイスにアクセスできるようになります。
c) **expert** コマンドを入力して Linux シェルにアクセスします。
d) makecall ディレクトリで、次のコマンドを実行します。

sudo manage_slr.pl

例：

```
admin@fmc63betaslr: ~$ sudo manage_slr.pl
Password:


*************** Configuration Utility *************

1   Show SLR Status
2   Enable SLR
3   Disable SLR
0   Exit

************************************************************
Enter choice:
```

e) オプション **3** を選択して、特定のライセンスの予約を無効にします。

f) オプション **0** を選択して、manage_slr ユーティリティを終了します。
g) **exit** と入力し、Linux シェルを終了します。
h) **exit** コマンドを入力してセキュアシェルのコマンドライン インターフェイスを終了します。

特定ライセンス予約のステータスのモニタリング

次に示すように、[システム（System）]>[ライセンス（Licenses）]>[特定のライセンス（Specific Licenses）] ページには Firewall Management Center でのライセンスの使用状況の概要が表示されます。

使用の認証

可能なステータス値は次のとおりです。

- [承認済み（Authorized）]：Firewall Management Center は、アプライアンスのライセンスの付与資格を承認したライセンス認証局に準拠しており、正常に登録されています。
- [コンプライアンス不適合（Out-of-compliance）]：ライセンスの期限が切れているか、または Firewall Management Center が予約していないにもかかわらずライセンスを過剰に使用している場合、[コンプライアンス不適合（Out-of-Compliance）] がステータスに表示されます。[特定のライセンスの予約（Specific License Reservation）] にライセンスの付与資格が適用されるため、アクションを実行する必要があります。

製品登録

特定の登録ステータスと、Firewall Management Center で承認コードが最後にインストールされたか、または更新された日付を指定します。

輸出管理機能

Firewall Management Center の輸出規制対象機能を有効にしたかどうかを指定します。

輸出規制対象機能の詳細については、「輸出規制対象の機能のライセンス （13 ページ）」を参照してください。

製品インスタンス

この Firewall Management Center のユニバーサル一意識別子（UUID）。この値は Smart Software Manager でこのデバイスを識別します。

確認コード

特定のライセンスを更新するか、または非アクティブ化して返却する場合に [確認コード（Confirmation Code）] が必要です。

[割り当て済みライセンス（Assigned Licenses）] タブ

各デバイスとそれぞれのステータスに割り当てられているライセンスを表示します。

[予約済みライセンス（Reserved Licenses）] タブ

割当に使用されているライセンスと使用可能なライセンスの数、およびライセンスの有効期限を表示します。

特定のライセンスの予約のトラブルシューティング

Smart Software Manager の製品インスタンスリストから特定の Firewall Management Center を識別する方法を教えてください。

Smart Software Manager の [製品インスタンス（Product Instances）] ページで、テーブル内の列のいずれかの値に基づいて製品インスタンスが識別できない場合は、**FP** タイプの汎用製品インスタンスそれぞれの名前をクリックする必要があります。このページの **UUID** の値は 1 つの Management Center を一意に識別します。

Firewall Management Center の Web インターフェイスでは、Management Center の UUID は [システム（System）] > [ライセンス（Licenses）] > [特定のライセンス（Specific License）] ページに表示される [製品インスタンス（Product Instance）] の値です。

Smart Software Manager の [ライセンスの予約（License Reservation）] ボタンが表示されません。

[ライセンス予約（License Reservation）] ボタンが表示されない場合、お使いのアカウントでは特定のライセンスの予約が承認されていません。Linux シェルで特定のライセンスの予約をすでに有効にし、要求コードを生成している場合は、次の手順を実行します。

1. Management Center の Web インターフェイスですでに**要求コード**を生成している場合は、その要求コードをキャンセルします。
2. 「特定のライセンスの予約の非アクティブ化と返却 （52 ページ）」のセクションで説明しているように、Management Center の Linux シェルで特定のライセンスの予約を無効にします。
3. スマートトークンを使用して、通常モードで Management Center を Smart Software Manager に登録します。
4. Cisco TAC に連絡して、自分のスマート アカウントの個別ライセンスを有効にします。

ライセンス プロセスの最中に中断が発生しました。中断した場所を取得する方法を教えてください。

承認コードは生成したが、Smart Software Manager からまだダウンロードしていない場合は、Smart Software Manager の [製品インスタンス（Product Instance）] ページに移動し、製品インスタンスをクリックした後、[予約承認コードのダウンロード（Download Reservation Authorization Code）] をクリックします。

デバイスを Firewall Management Center Virtual に登録できません。

登録するデバイスをカバーするのに十分な Firewall Management Center Virtual の資格がスマートアカウントにあることを確認してから展開を更新し、必要な資格を追加します。

「特定のライセンスの予約の更新 （50 ページ）」を参照してください。

特定のライセンスを有効にしていましたが、[スマート ライセンス（Smart License）] ページが表示されなくなりました。

これは予期されている動作です。[特定のライセンス（Specific Licensing）] を有効にすると、スマート ライセンスは無効になります。[特定のライセンス（Specific License）] ページを使用してライセンスの操作を実行できます。

スマートライセンスを使用する場合は、特定のライセンスを返却する必要があります。詳細については、「特定のライセンスの予約の非アクティブ化と返却 （52 ページ）」を参照してください。

Firewall Management Center Virtual に [特定のライセンス（Specific License）] ページが表示されません。

[特定のライセンス（Specific License）] ページを表示するには、特定のライセンスを有効にする必要があります。詳細については、「[特定のライセンス（Specific Licenses）] メニュー オプションの有効化 （47 ページ）」を参照してください。

特定のライセンスを無効にしましたが、返却コードをコピーするのを忘れてしまいました。どうすればよいでしょうか。

リターンコードは Firewall Management Center Virtual に保存されています。Linux シェルから特定のライセンスをもう一度有効にし（「[特定のライセンス（Specific Licenses）] メニュー オプションの有効化 （47 ページ）」を参照）、Firewall Management Center Virtual の Web インターフェイスを更新します。[戻りコード（Return Code）] が表示されます。

レガシー Firewall Management Center PAK ベースのライセンスの設定

Firewall Management Center は、プラットフォームライセンスとしてスマートライセンスまたはレガシー PAK（製品アクティベーションキー）ライセンスをサポートします。この手順では、PAK ベースのライセンスを適用する方法について説明します。

スマートアカウントを再登録した後、すべての従来型デバイスのクラシックライセンスを手動で追加する必要があります。

始める前に

- ライセンス購入時にCiscoが提供したソフトウェア権利証明書にある製品アクティベーションキー（PAK）をお手元にご用意ください。レガシーの、以前のシスコのライセンスの場合は、サポートに問い合わせてください。

手順

ステップ 1 ライセンスキーは、Smart Software Manager で Firewall Management Center を一意に識別します。これは、Firewall Management Center の製品コード（66 など）と管理ポート（eth0）の MAC アドレスで構成されます（66:00:00:77:FF:CC:88 など）。

a) [システム（System）]（⚙）>**[ライセンス（Licenses）]**>**[クラシックライセンス（Classic Licenses）]** を選択します。
b) [新規ライセンスの追加（Add New License）] をクリックします。
c) [機能ライセンスの追加（Add Feature License）] ダイアログの上部にある [ライセンス キー（License Key）] フィールドの値をメモします。

ステップ 2 [システム（System）]（⚙）>**[ライセンス（Licenses）]**>**[クラシックライセンス（Classic Licenses）]** を選択します。

ステップ 3 [新規ライセンスの追加（Add New License）] をクリックします。

ステップ 4 必要に応じ、続いて以下を行います。

- ライセンステキストをすでに取得している場合は、ステップ 8 にスキップしてください。
- ライセンスのテキストを取得する必要がある場合は、次の手順を実行します。

ステップ 5 [ライセンス取得（Get License）] をクリックして、ライセンス登録ポータルを開きます。

（注）
ご使用のコンピュータからインターネットにアクセスできない場合は、アクセスできるコンピュータから http://cisco.com/go/licenseを探します。

ステップ 6 ライセンス登録ポータルで、PAK からライセンスを生成します：https://cisco.com/go/license。

この手順には、購入時に入手した PAK と、Firewall Management Center のライセンスキーが必要です。

このポータルの使用方法の詳細については、次を参照してください。

https://slexui.cloudapps.cisco.com/SWIFT/LicensingUI/Quickstart

これらのリンクにアクセスするには、アカウントのクレデンシャルが必要です。

ステップ 7 ライセンス登録ポータルの表示から、ないしはライセンス登録ポータルより送られてくるメールからライセンス テキストをコピーします。

重要

ポータルまたは電子メール メッセージ内のライセンス テキスト ブロックには、複数のライセンスを含めることができます。各ライセンスは、BEGIN LICENSE 行と END LICENSE 行で囲まれます。一度に 1 つのライセンスしかコピーして貼り付けることができません。

ステップ 8 Management Center Virtual の Web インターフェイスの [機能ライセンスの追加（Add Feature License）] ページに戻ります。

ステップ 9 [ライセンス（License）] フィールドにライセンス テキストを貼り付けます。

ステップ 10 [ライセンスの検証（Verify License）] をクリックします。

ライセンスが無効となる場合は、ライセンス テキストが正しくコピーされているか確認します。

ステップ 11 [ライセンスの提出（Submit License）] をクリックします。

ライセンスに関する追加情報

ライセンスに関するよくある質問の解決に役立つその他の情報については、次のドキュメントを参照してください。

- FAQ：ライセンスに関する FAQ
- ライセンスロードマップ

ライセンスの履歴

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
Secure Firewall Threat Defense 使用状況メトリック収集の改善	7.6.0	任意（Any）	Cisco Success Network 機能と Cisco Support Diagnostic 機能は、デフォルトで有効になりました。この機能拡張により、シスコは Cisco Secure Firewall Threat Defense 展開からテレメトリデータをより効率的に収集できるようになりました。 廃止された画面：[スマートライセンスの製品登録（Smart Licensing Product Registration）] ページ（**[システム（System）] > [ライセンス（Licenses）] > [スマートライセンス（Smart Licenses）] > [登録（Register）]**）の [Cisco Success Networkの有効化（Enable Cisco Success Network）] チェックボックスと [シスコのサポート診断の有効化（Enable Cisco Support Diagnostics）] チェックボックスは廃止されました。

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
スマートライセンスの標準化	7.3	任意（Any）	Firewall Management Center の GUI で以下のライセンス名が変更されました。 • Base は Essentials に変更 • Threat は IPS に変更 • Malware は Malware Defense に変更 • RA VPN/AnyConnect License は Cisco Secure Client に変更 • AnyConnect Plus は Secure Client Advantage に変更 • AnyConnect Apex は Secure Client Premier に変更 • AnyConnect Apex および Plus は Secure Client Premier および Advantage に変更 • AnyConnect VPN Only は Secure Client VPN Only に変更
キャリアライセンスのサポート	7.3	任意（Any）	キャリアライセンスは、Diameter、GTP/GPRS、SCTP および M3UA プロトコルを有効にします。 新規/変更された画面：**[システム（System）] > [スマートライセンス（Smart Licenses）]**。
Firewall Threat Defense Virtual のパフォーマンス階層ライセンス	7.0	任意（Any）	パフォーマンス階層型ライセンスでは、導入要件に基づいて異なるスループットレベルと VPN 接続制限を提供します。ライセンス階層は新しい Firewall Threat Defense Virtual モデルにマッピングされます。
Firepower 4100/9300 の Firewall Threat Defense に対する複数インスタンス機能のライセンス	6.3	任意（Any）	Firepower 4100/9300 に複数の Firewall Threat Defense コンテナ インスタンスを展開できるようになりました。セキュリティ モジュール/エンジンの機能ごとに必要なライセンスは 1 つのみです。基本ライセンスは、各インスタンスに自動的に割り当てられます。 新規/変更された画面：**[システム（System）] > [ライセンス（Licenses）] > [スマートライセンス（Smart Licenses）]**。 サポート対象プラットフォーム：Firepower 4100/9300 の Firewall Threat Defense

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
エアギャップ展開に対する特定のライセンスの予約	6.3	任意（Any）	展開でインターネットに接続してシスコのライセンス認証局と通信できない顧客は特定のライセンスの予約を使用できます。 新規/変更された画面：**[システム（System）]** > **[ライセンス（Licenses）]** > **[特定のライセンス（Specific Licenses）]**（このオプションはデフォルトでは使用できません。） サポートされるプラットフォーム：Firewall Management Center、Firewall Threat Defense
制限付きの顧客の輸出規制対象機能	6.3	任意（Any）	スマートアカウントで制限付き機能を使用する資格を持たない特定の顧客は、期間ベースのライセンスを承認を受けて購入することができます。 サポートされるプラットフォーム：Firewall Management Center、Firewall Threat Defense

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。