



システムのライセンス

ここでは、FirePOWER Threat Defenseデバイスにライセンスを適用する方法について説明します。

- [Firepower システムのスマート ライセンス, 1 ページ](#)
- [スマート ライセンスの管理, 4 ページ](#)

Firepower システムのスマート ライセンス

シスコスマート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することができます。製品認証キー（PAK）ライセンスとは異なり、スマート ライセンスは特定のシリアル番号またはライセンスキーに関連付けられません。スマート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。

加えて、スマートライセンスを使用しても、まだ購入していない製品機能を使用できなくなることはありません。Cisco Smart Software Managerに登録し、後でライセンスを購入する場合に限り、ライセンスの使用をすぐに開始できます。これにより、機能を展開して使用することができ、発注書の承認を待つて遅れることがなくなります。

Cisco Smart Software Manager

FirePOWER Threat Defenseデバイスに対する1つまたは複数のライセンスを購入する場合は、これらのライセンスをCisco Smart Software Manager (<https://software.cisco.com/#SmartLicensing-Inventory>)で管理します。Cisco Smart Software Managerでは、組織のマスター アカウントを作成できます。

デフォルトでは、マスター アカウントの下位のデフォルト バーチャル アカウントにライセンスが割り当てられます。アカウントの管理者は、たとえば地域、部署、子会社などに対し、追加のバーチャルアカウントを作成できます。複数のバーチャルアカウントを使用することで、大量のライセンスおよびアプライアンスを管理しやすくなります。

ライセンスおよびアプライアンスは、バーチャルアカウントごとに管理されます。各バーチャルアカウントのアプライアンスは、それぞれのアカウントに割り当てられたライセンスのみを使用できます。追加のライセンスが必要になった場合は、未使用のライセンスを別のバーチャルア

ウントから転送できます。バーチャル アカウント間でアプライアンスを転送することもできます。

Cisco Smart Software Manager にデバイスを登録する際、製品インスタンスの登録トークンを作成し、このトークンを Firepower Device Manager に入力します。使用するトークンに基づき、登録したデバイスがバーチャル アカウントに関連付けられます。

Cisco Smart Software Manager の詳細については、オンライン ヘルプを参照してください。

License Authority との定期通信

製品インスタンス登録トークンを使用して FirePOWER Threat Defense デバイスを登録すると、そのデバイスは Cisco License Authority に登録されます。License Authority は、デバイスと License Authority の間の通信に使用する 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 ヶ月ごとに更新されます。ID 証明書の期限が切れると（通常、9 ヶ月または 1 年間通信がない場合）、デバイスは登録解除状態に戻り、ライセンス機能の使用は中断されます。

デバイスは License Authority と定期的に通信します。Cisco Smart Software Manager で変更を加えた場合は、デバイス上の認証を更新し、変更がすぐに反映されるようにします。あるいは、デバイスがスケジュールどおりに通信するのを待つこともできます。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、デバイスはホームをコール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 License Authority に連絡する必要があります。

スマート ライセンスのタイプ

次の表に、FirePOWER Threat Defense デバイスで使用可能なライセンスを示します。

FirePOWER Threat Defense デバイスを購入すると、自動的に基本ライセンスが含まれます。すべての追加ライセンスはオプションです。

表 1: スマート ライセンスのタイプ

ライセンス	期間	付与される機能
基本（自動的に含まれる）	永久	オプションのタームライセンスでカバーされないすべての機能。 [このトークンに登録した製品でエクスポート制御機能を許可する（Allow export-controlled functionality on the products registered with this token）]かどうかも指定する必要があります。このオプションは、エクスポート制御基準に国が適合している場合のみ選択できます。このオプションは、高度な暗号化や、高度な暗号化を必要とする機能の使用を制御します。

ライセンス	期間	付与される機能
脅威 (Threat)	ターム ベース	侵入検知および防御：侵入ポリシーが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し、またオプションで違反パケットをドロップします。 ファイル制御：ファイルポリシーが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）をブロックできます。マルウェア ライセンスを必要とする AMP for Firepower は、マルウェアを含むファイルのインスペクションを実行してブロックすることができます。
マルウェア (Malware)	ターム ベース	マルウェアを確認するポリシーであり、Cisco Advanced Malware Protection (AMP) と一緒に AMP for Firepower（ネットワークベースの高度なマルウェア保護）と AMP Threat Grid を使用します。 ファイルポリシーは、ネットワーク上で伝送されるファイルに存在するマルウェアを検出してブロックすることができます。
URL フィルタリング (URL Filtering)	ターム ベース	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。 このライセンスなしでも、個々の URL で URL フィルタリングを実行できます。

期限切れまたは無効なオプション ライセンスの影響

オプション ライセンスの期限が切れた場合でも、引き続きライセンスを必要とする機能を使用できます。ただし、ライセンスはコンプライアンス違反としてマークされるため、ライセンスを購入してアカウントに追加し、ライセンスをコンプライアンスの状態に戻す必要があります。

オプション ライセンスを無効にすると、システムは次のように対応します。

- マルウェア ライセンス (Malware license)：システムは AMP クラウドのクエリを停止し、AMP クラウドから送信されるレトロスペクティブ 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 インスペクションを適用するファイル ポリシーが含まれている場合、それらを再展開することはできません。マルウェア ライセンスが無効化された後、ごく短時間のみ、システムが既存のキャッシュされた処理済みのファイル

を使用できる点に注意してください。その時間枠が経過すると、システムはそれらのファイルに使用不可 (Unavailable) の処理を割り当てます。

- 脅威 (Threat) : システムは侵入ポリシーまたはファイル制御ポリシーを適用しなくなります。ライセンスが必要な既存のポリシーを再展開することはできません。
- URL フィルタリング (URL Filtering) : URL カテゴリ条件付きのアクセスコントロールルールは、即座に URL のフィルタリングを停止し、システムは URL データの更新をダウンロードしなくなります。既存のアクセスコントロールポリシーにカテゴリおよびレピュテーションベースの URL 条件が含まれる場合、それらを再展開することはできません。

スマート ライセンスの管理

システムの現在のライセンスステータスを確認するには、[スマート ライセンス (Smart License)] ページを使用します。システムはライセンスされる必要があります。

このページには、90 日間の評価ライセンスを使用しているかどうかや、Cisco Smart Software Manager に登録しているかどうかが表示されます。登録すると、Cisco Smart Software Manager への接続のステータスと、各タイプのライセンスのステータスが表示されます。

[使用認証 (Usage Authorization)] では、Smart License Agent のステータスが識別されます。

- [承認済み (Authorized)] ([接続済み (Connected)]、[十分なライセンス (Sufficient Licenses)]) : デバイスはライセンス認証局に正常にアクセスして登録されており、ライセンス認証局によってそのアプライアンスのライセンス付与が承認されています。デバイスは、現在、[コンプライアンス適合 (In-Compliance)] 状態です。
- [コンプライアンス不適合 (Out-of-Compliance)] : デバイスに使用可能なライセンス付与がありません。ライセンスされた機能は動作を継続します。ただし、コンプライアンス適合状態になるには追加の権限付与を購入するか解除する必要があります。
- [認証期限切れ (Authorization Expired)] : デバイスがライセンス認証局と通信せずに 90 日以上が経過しています。ライセンスされた機能は動作を継続します。この状態の場合、Smart License Agent は認証要求を再試行します。再試行に成功すると、エージェントはコンプライアンス不適合状態または承認済み状態になり、新しい認証期間が開始されます。デバイスの同期を手動で試みてください。



(注) [スマート ライセンス (Smart License)] ステータスの横にある [i] ボタンをクリックして、仮想アカウントとエクスポート制御機能を表示し、Cisco Smart Software Manager を開くためのリンクを取得します。エクスポート規制機能により、国家安全保障、外交政策、および反テロリズムに関する法律と規制の対象となるソフトウェアが制御されます。

次の手順で、システムのライセンスを管理する方法の概要を示します。

手順

-
- ステップ 1** デバイスをクリックし、[スマート ライセンス (Smart License)] サマリの [設定の表示 (View Configuration)] をクリックします。
- ステップ 2** デバイスを登録します。
オプションのライセンスを割り当てるには、Cisco Smart Software Manager に登録する必要があります。評価期間が終了する前に登録してください。
[デバイスの登録, \(5 ページ\)](#) を参照してください。
- ステップ 3** オプションの機能ライセンスを要求して管理します。
ライセンスによって制御される機能を使用するには、オプションのライセンスを登録する必要があります。[オプション ライセンスの有効化と無効化, \(6 ページ\)](#) を参照してください。
- ステップ 4** システムのライセンス付与を保持します。
次のタスクを実行できます。
- [Cisco Smart Software Manager との同期, \(7 ページ\)](#)
 - [デバイスの登録解除, \(7 ページ\)](#)
-

デバイスの登録

FirePOWER Threat Defense デバイスの購入には自動的に基本ライセンスが含まれます。基本ライセンスの対象は、オプション ライセンスの対象になっていないすべての機能です。これは永久ライセンスです。

システムの初期セットアップ時に、Cisco Smart Software Manager によってデバイスを登録するように求められます。代わりに 90 日間の評価ライセンスの使用を選択した場合は、評価期間の終了前にデバイスを登録する必要があります。

デバイスを登録すると、仮想アカウントによってライセンスがデバイスに割り当てられます。また、デバイスの登録により、有効にしたすべてのオプション ライセンスも登録されます。

手順

-
- ステップ 1** デバイスをクリックし、[スマート ライセンス (Smart License)] サマリの [設定の表示 (View Configuration)] をクリックします。
- ステップ 2** [登録の要求 (Request Register)] をクリックし、画面の指示に従います。
- a) リンクをクリックして [Cisco Smart Software Manager](#) を開き、アカウントにログインするか、必要に応じて新しいアカウントを作成します。
 - b) 新しいトークンを作成します。

トークンを作成する際、トークンの有効な使用期間を指定します。推奨される有効期間は 30 日間です。この期間は、トークン自体の有効期限を定義するものであり、トークンを使用して登録するデバイスには影響しません。トークンを使用する前に期限切れになった場合は、単に新しいトークンを生成できます。

また、[このトークンで登録される製品でエクスポート制御機能を許可する (Allow export-controlled functionality on the products registered with this token)] かどうかを指定する必要があります。このオプションは、製品を使用する国がエクスポート制御基準を満たしている場合にのみ選択できます。このオプションにより、高度な暗号化と高度な暗号化を必要とする機能の使用が制御されます。

- c) トークンをコピーして、[スマートライセンスの登録 (Smart License Registration)] ダイアログボックスの編集ボックスに貼り付けます。
- d) [登録の要求 (Request Register)] をクリックします。

オプションライセンスの有効化と無効化

オプションのライセンスを有効化（登録）または無効化（リリース）することができます。ライセンスによって制御される機能を使用するには、ライセンスを有効にする必要があります。

オプションのタームライセンスの対象となる機能を使用しなくなった場合、ライセンスを無効化することができます。ライセンスを無効にすると、Cisco Smart Software Manager アカウントでライセンスがリリースされるため、別のデバイスにそのライセンスを適用できるようになります。

評価モードで動作させる場合は、これらのライセンスの評価バージョンを有効にすることもできます。評価モードでは、デバイスを登録するまでライセンスは Cisco Smart Software Manager に登録されません。

はじめる前に

ライセンスを無効にする前に、そのライセンスが使用中でないことを確認します。ライセンスを必要とするポリシーは書き換えるか削除します。

手順

- ステップ 1** デバイスし、[スマートライセンス (Smart License)] サマリで [設定を表示 (View Configuration)] をクリックします。
- ステップ 2** 必要に応じて、それぞれのオプションライセンスの [有効化/無効化 (Enable/Disable)] コントロールをクリックします。
 - [有効化 (Enable)] : Cisco Smart Software Manager アカウントにライセンスを登録し、制御された機能が有効になります。ライセンスによって制御されるポリシーを設定し、展開できるようになります。

- [無効化 (Disable)] : Cisco Smart Software Manager アカウントのライセンスを登録解除し、制御された機能が無効になります。新しいポリシーの機能を設定することも、その機能を使用するポリシーを展開することもできません。

Cisco Smart Software Manager との同期

ライセンス情報は、システムによって Cisco Smart Software Manager と定期的に同期されます。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、アップライアンスはホームをコールすることなく最大で 90 日間は動作します。

ただし、Cisco Smart Software Manager に変更を加えた場合は、デバイス上で許可を更新し、変更をすぐに反映させることができます。

同期では、ライセンスの現在のステータスを取得して、許可と ID 証明書を更新します。

手順

- ステップ 1 デバイス[スマート ライセンス (Smart License)] サマリの [設定の表示 (View Configuration)] をクリックします。
- ステップ 2 歯車ドロップダウンリストから [接続の再同期 (Resync Connection)] を選択します。

デバイスの登録解除

デバイスを使用しなくなった場合は、Cisco Smart Software Manager からデバイスの登録を解除できます。登録を解除すると、仮想アカウントでデバイスに関連付けられている基本ライセンスとすべてのオプションライセンスが解放されます。オプションライセンスは他のデバイスに割り当てることができます。

デバイスの登録を解除すると、デバイスの現在の設定とポリシーはそのまま機能しますが、変更を加えたり展開したりすることはできません。

手順

- ステップ 1 デバイス[スマート ライセンス (Smart License)] サマリの [設定の表示 (View Configuration)] をクリックします。
- ステップ 2 歯車ドロップダウンリストから [デバイスの登録解除 (Unregister Device)] を選択します。
- ステップ 3 警告を確認し、デバイスの登録を本当に解除する場合は [登録解除 (Unregister)] をクリックします。

