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付与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

Cisco Smart Licensing 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使用すると、ライセンスの使用状況と要件をひと目で確認できます。

また、スマート ライセンスでは、まだ購入していない製品の機能を使用できます。Cisco Smart Software Manager に登録すると、すぐにライセンスの使用を開始できます。また、後でライセンスを購入することもできます。これによって、機能の展開および使用が可能になり、発注書の承認による遅延がなくなります。

Cisco Smart Software Manager

Firepower Threat Defense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/#SmartLicensing-InventoryCisco Smart Software Manager では、組織のマスター アカウントを作成できます。

デフォルトでは、ライセンスはマスター アカウントの下のデフォルトの仮想アカウントに割り当てられます。アカウントの管理者として、たとえば、地域、部門、または子会社ごとに、追加の仮想アカウントを作成できます。複数の仮想アカウントを使用することで、多数のライセンスおよびアプライアンスの管理を行うことができます。

ライセンスとアプライアンスは仮想アカウントごとに管理されます。つまり、その仮想アカウントのアプライアンスのみが、そのアカウントに割り当てられたライセンスを使用できます。追加のライセンスが必要な場合は、別の仮想アカウントから未使用のライセンスを転用できます。また、仮想アカウント間でのアプライアンスの譲渡も可能です。

Cisco Smart Software Manager にデバイスを登録するとき、そのマネージャで製品インスタンス登録トークンを作成し、Firepower Device Manager にそのトークンを入力します。登録済みデバイスが、使用されているトークンに基づいて仮想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、マネージャのオンライン ヘルプを参照してください。

ライセンス認証局との定期通信

Firepower Threat Defenseデバイスの登録に製品インスタンス登録トークンを使用すると、デバイスはシスコのライセンス認証局に登録されます。ライセンス認証局は、デバイスとライセンス認証局の間の通信用に 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 証明書の期限が切れた場合（通常は、9 ヵ月または 1 年間通信がない状態）、デバイスは登録が解除された状態になり、ライセンスされた機能は使用停止になります。

デバイスは、定期的にライセンス認証局と通信します。Cisco Smart Software Manager に変更を加えた場合は、すぐに変更が有効になるようにデバイス上で認証を更新できます。また、スケジュールどおりにデバイスが通信するのを待つこともできます。通常のライセンス通信は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 日が経過する前にライセンス認証局と連絡を取る必要があります。

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ています。その他すべての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 ライセンスに含まれないすべての機能。 [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）] かどうかも指定する必要があります。国が輸出管理標準を満たしている場合にのみ、このオプションを選択できます。このオプションは、高度な暗号化および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	期間ベース	侵入検知および防御（Intrusion detection andprevention）：侵入ポリシーが、侵入およびエクスプロイトのネットワーク トラフィックを分析します。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（Filecontrol）：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）をブロックします。マルウェア ライセンスが必要な Firepower の AMP を使用すると、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	期間ベース	マルウェアを確認するファイルポリシー。Cisco Advanced Malware Protection（AMP）を Firepower の AMP（ネットワークベースの高度なマルウェア防御）および AMP Threat Gridとともに使用します。 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の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）	期間ベース	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、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

オプションのライセンスが期限切れになっても、そのライセンスを必要とする機能を使用し続けることはできます。ただし、ライセンスは非準拠とマークされます。ライセンスを準拠状態に戻すには、ライセンスを購入してアカウントに追加する必要があります。

オプションのライセンスを無効にすると、システムは次のように反応します。

- [マルウェア ライセンス（Malware license）]：システムは AMP クラウドへの問い合わせを停止し、AMP レトロスペクション クラウドから送信されたレトロスペクティブ イベントの認証も停止します。既存のアクセス コントロール ポリシーにマルウェア検出を適応ファイル ポリシーが含まれている場合、このアクセス コントロール ポリシー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極めて短時間のみであることに注意してください。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。

- [脅威（Threat）]：システムは侵入またはファイル制御ポリシーを適用しなくなります。ライセンスを必要とする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 カテゴリ条件が指定されたアクセス コントロール ルールは URL のフィルタリングをただちに停止し、システムは URL データへ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 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。

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 ステータスを表示するには、[スマート ライセンス（Smart License）] ページを使用します。システムにはライセンスが必要です。

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、または Cisco Smart Software Manager に登録済み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、および各ライセンス タイプのステータスを確認できます。

使用認証により、スマート ライセンス エージェントのステータスが特定されます。

- 承認済み（Authorized）（「接続/接続中」、「十分なライセンス」）：デバイスは、アプライアンスのライセンス権限を承認した License Authority に正常に登録されています。このデバイスはインコンプライアンス（In-Compliance）の状態です。
- アウトオブコンプライアンス（Out-of-Compliance）：デバイスで使用可能なライセンス権限がありません。ライセンスされた機能は動作を継続します。ただし、インコンプライアンス（In-Compliance）にするためには、追加の権限を購入するか、または解放する必要があります。
- 認証期限切れ（Authorization Expired）：デバイスは 90 日以上ライセンス認証局と通信していません。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、スマート ライセンス エージェントは認証要求を再試行します。再試行に成功すると、エージェントはアウトオブコンプライアンス（Out-of-Compliance）または承認済み（Authorized）状態になり、新たな承認期間が始まります。手動でデバイスの同期を試します。

（注） スマート ライセンスのステータスの横にある [i]ボタンをクリックすると、バーチャル アカウント、輸出管理機能を確認でき、Cisco Smart Software Manager を開くリンクが表示されます。輸出管理機能により、国家安全保障、外交ポリシー、反テロリズム法令を対象としたソフトウェアが制御されます。

次の手順では、システム ライセンスの管理方法の概要について説明します。

手順

ステップ 1 [デバイス（Device）]メニューのデバイス名、[スマート ライセンス（Smart License）] サマリで [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 ライセンスを割り当てる前に、Cisco Smart Software Manager に登録する必要があります。評価期間の終了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 オプション機能のライセンスをリクエストして管理します。
ライセンスによって制御される機能を使用するためには、オプション 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 ライセンスを維持します。
次の作業を実行できます。

- 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デバイスを購入すると、自動的に基本ライセンスが付いてきます。基本ライセンスは、オプション ライセンスではカバーされないすべての機能をカバーしています。これは永久ライセンスです。

システムの初期設定時に、Cisco Smart Software Manager にデバイスを登録するように求められます。登録せずに90日間の評価ライセンスを使用する場合、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、バーチャル アカウントからデバイスにライセンスが割り当てられます。デバイスを登録すると、有効にしている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（Device）]メニューのデバイス名、[スマート ライセンス（Smart License）] サマリで [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）]をクリックして、手順に従います。

a) リンクをクリックして Cisco Smart Software Manager を開いて自分の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) 新しいトークンを生成します。

トークンを作成する際に、トークンの有効使用期間を指定します。推奨の有効期間は 30 日です。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るため、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。使用前にトークンが期限切れになった場合は、簡単に新しいトークンを生成できます。

[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）]を選択するかどうかも指定する必要があります。このオプションは、自国が輸出管理の標準規格に適合している場合のみ選択できます。このオプションは、高度な暗号化および高度な暗号化を必要とする機能の使用を制御します。

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（Device）]メニューのデバイス名し、[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、定期的に Cisco Smart Software Manager と同期されます。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。

しかし、Smart Software Manager に変更を加えた場合は、デバイス上で認証を更新し、即座に変更を有効にすることができます。

同期により、ライセンスの現在のステータスが取得され、認証と ID 証明書が更新されます。

手順

ステップ 1 [デバイス（Device）]メニューのデバイス名クリックし、[スマート ライセンス サマリ（Smart License summary）] の [設定の表示（View Configuration）] をクリックします。

ステップ 2 ギア 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、そのデバイスを Cisco Smart Software Manager から登録解除できます。登録解除すると、基本ライセンス、およびデバイスに関連付けられたすべてのオプション ライセンスがバーチャル アカウントで解放されます。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（Device）]メニューのデバイス名クリックし、[スマート ライセンス サマリ（Smart License summary）] の [設定の表示（View Configuration）] をクリックします。

ステップ 2 ギア 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 実際にデバイスの登録を解除するには、警告を読み、[登録解除（Unregister）]をクリックします。