システムのライセンス

ここでは、Firewall 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。

ファイアウォール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**： Cisco License Central 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します。所有しているものと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**：ライセンス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。

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

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。

Cisco Smart Software Manager

Firewall 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（https://software.cisco.com/#SmartLicensing-Inventory）で管理します。Cisco 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。

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際は、製品インスタンスの登録トークンを Cisco Smart Software Manager で作成し、そのトークンを Firewall Device Manager に入力します。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

Firewall 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。通常のライセンスに関する通信は 12 時間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、Firewall Threat Defense デバイスで使用可能なライセンスを示します。

Firewall Threat Defense デバイスを購入すると、自動的にBase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
Base	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。 Base ライセンスは登録時にアカウントに自動的に追加されます。 [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、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、高度な暗号化や、高度な暗号化を必要とする機能の使用を制御します。
Threat	ターム ベース	次のポリシーを使用するために必要です。 • 侵入（Intrusion） • ファイル（File）（Malware も必要） • セキュリティ インテリジェンス（Security Intelligence）
Malware	ターム ベース	ファイルポリシー（Threat も必要）
URL	ターム ベース	URLポリシー：カテゴリおよびレピュテーションベースの URL フィルタリングまたは DNS ルックアップ要求フィルタリング。 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。

ライセンス	期間	付与される機能
RA VPN： • AnyConnect Plus • AnyConnect Apex • AnyConnect VPN Only	ライセンスタイプに基づきタームベースまたは永久	リモートアクセス VPN の設定RA VPN を設定するには、基本ライセンス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 Device Manager は、任意の有効な AnyConnect Client 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。まだ購入していない場合は、リモートアクセス VPN のライセンス要件を参照してください。 『*Cisco AnyConnect Ordering Guide*』（http://www.cisco.com/c/dam/en/us/products/collateral/security/anyconnect-og.pdf）も参照してください。

Firewall Threat Defense Virtual のライセンス

このセクションでは、FTDv 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 FTDv ライセンスを、サポートされているすべての FTDv vCPU/メモリ構成で使用できます。これにより、FTDv 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。FTDv 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 FTDv 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 *2 : 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

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
FTDv50、10Gbps	12 コア/24 GB	10 Gbps	750
FTDv100、16 Gbps	16 コア/32 GB	16 Gbps	10,000

Firewall Threat Defense Virtual 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

FTDv 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。

- FTDv 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 FTDv ライセンスを、サポートされているすべての FTDv コア/メモリ構成で使用できます。これにより、FTDv 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。
- FTDv 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。FTDv 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。FTDv 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 FTDv デバイスを展開する場合や FTDv 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。
- Base 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、FTDv デバイスの Base ライセンス権限と、Threat、Malware、および URL Filtering 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 Base 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。
- 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。

暗号化機能に対するエクスポート制御設定の影響

デバイスを登録する場合、**このトークンに登録された製品の輸出規制された機能を許可する**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、高度な暗号化や、高度な暗号化を必要とする機能の使用を制御します。

評価モードは、非輸出準拠アカウントを使用して登録する場合と同じように扱われます。つまり、評価モードで実行している場合、リモートアクセス VPN を設定したり、高度な暗号化アルゴリズムを使用したりはできません。

特に、DES 標準は評価モードまたは非輸出準拠モードでのみ使用できます。

したがって、サイト間 VPN などの暗号化機能を設定したり、高アベイラビリティグループのフェールオーバー接続を暗号化したりすると、輸出準拠アカウントに登録した後に接続の問題が発生する可能性があります。機能が評価モードで DES を使用していた場合、アカウントの登録後にその機能の設定が破損します。

暗号化関連の問題を回避するには、次の推奨事項を考慮してください。

- サイト間 VPN や暗号化されたフェールオーバー接続などの暗号化機能は、デバイスを登録するまで設定しないでください。
- 輸出準拠アカウントを使用してデバイスを登録した後、評価モードで設定したすべての暗号化機能を編集し、より安全な暗号化アルゴリズムを選択します。各暗号化機能をテストおよび検証して、正しく機能していることを確認します。

（注） 評価モードで HA フェールオーバー暗号化を設定した場合は、HA グループ内の両方のデバイスをリブートして、より強力な暗号化の使用を開始する必要もあります。両方のデバイスが自身をアクティブユニットと見なすスプリットブレイン状態を回避するために、最初に暗号化を削除することを推奨します。

期限切れまたは無効なオプション ライセンスの影響

次のいずれかのオプション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は引き続き使用できます。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。

- Malware：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。ファイルポリシーが含まれている既存のアクセス コントロール ポリシーは再展開できません。Malware 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。

- Threat：システムは、侵入ポリシーまたはファイルポリシーを適用しなくなります。セキュリティ インテリジェンス ポリシーの場合、システムはこのポリシーを適用せず、フィード更新のダウンロードを停止します。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]：URL カテゴリ条件を使用したアクセスコントロールルールは URL または DNS ルックアップ要求のフィルタリングを直ちに停止し、システムは URL データに対する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。
- [RA VPN]：リモート アクセス VPN 設定は編集できませんが、削除は可能です。ユーザーは引き続き RA VPN 設定を使用して接続できます。ただし、デバイスの登録を変更してシステムがエクスポートに準拠しなくなると、リモート アクセス VPN 設定はただちに停止し、リモート ユーザーは VPN に接続できなくなります。

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（「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の状態です。
- アウトオブコンプライアンス：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：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または承認済み状態になり、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。

始める前に

システムのインターネットへのパスがない場合は、スマートライセンスを使用できません。代わりに、パーマネントライセンス予約（PLR）モードに切り替えます。詳細については、永久ライセンスの適用 （13 ページ）を参照してください。

手順

ステップ 1 [デバイス（Device）] をクリックし、[スマートライセンス（Smart License）] のサマリーで [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 （8 ページ）を参照してください。

（注）
登録する際に、使用状況データをシスコに送信するかどうかを選択します。選択内容は、[歯車（gear）] アイコンの横にある [Cisco Success Networkにアクセス（Go To Cisco Success Network）] リンクをクリックすると変更できます。

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または無効化 （11 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 （12 ページ）
- デバイスの登録解除 （12 ページ）

デバイスの登録

Firewall Threat Defense デバイスを購入すると、自動的に Base ライセンスが含まれます。Base 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。

始める前に

デバイスの登録時には、そのデバイスだけが登録されます。高可用性のために設定されているデバイスの場合は、その装置を登録するために、高可用性ペアにあるその他の装置にログインする必要があります。

手順

ステップ 1 [デバイス（Device）] をクリックし、[スマートライセンス（Smart License）] のサマリーで [設定の表示（View Configuration）] をクリックします。

ステップ 2 **[Register Device]** をクリックして、説明に従います。

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、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、高度な暗号化や、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) FTDvデバイスのパフォーマンス階層（**Firewall Threat Defense Virtualのみ**）を選択するか、デフォルトの選択のままにします。

パフォーマンス階層が選択されていない場合、FTDv デバイスはレガシーモードで動作します。デフォルト設定は4 コア/8 GB です。詳細については、Firewall Threat Defense Virtual パフォーマンス階層の変更 （10 ページ）を参照してください。

e) シスコ クラウドサービスの登録リージョンを選択します。

登録後、このリージョンを変更する必要がある場合は、デバイスの登録を解除してから再度登録し、新しいリージョンを選択する必要があります。

f) 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。

Cisco Success Network ステップの情報を読み、[サンプルデータ（Sample Data）] をクリックして収集された実際のデータへのリンクを表示して、[Cisco Success Networkを有効にする（Enable Cisco Success Network）] オプションを選択したままにするかどうかを決定します。

g) **[デバイスの登録（Register Device）]** をクリックします。

Firewall Threat Defense Virtual パフォーマンス階層の変更

FTDv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FTDvライセンスを、サポートされているすべてのFTDvコア/メモリ構成で使用できます。これにより、FTDv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 スマートライセンスのパフォーマンス階層 （4 ページ）を参照してください。

FTDv をバージョン 7.0+ にアップグレードすると、デバイスは自動的に「FTDv 変数」 階層状態に移行し、権限付与レベルを選択するまで非階層化権限を使用し続けます。

次の点を考慮してください。

- スループットまたはRA VPNの要件に基づいて、導入ニーズに合わせてパフォーマンス階層を変更できます。FTDv は、調整可能なコアおよびメモリリソースを使用して展開することに注意してください。選択したパフォーマンス階層は、デバイスの仕様を超えることはできません。
- AWS では、パフォーマンス階層の変更はサポートされていません。

手順

ステップ 1 [デバイス（Device）] をクリックし、[スマートライセンス概要（Smart License summary）] の [設定の表示（View Configuration）] をクリックします。

ステップ 2 [パフォーマンス階層（Performance Tier）] ドロップダウンリストから目的のオプションを選択します。

- FTDv5（4 コア/8 GB）
- FTDv10（8 コア/8 GB）
- FTDv20（8 コア/8 GB）
- FTDv30（8 コア/16 GB）
- FTDv50（12 コア/24 GB）
- FTDv100（16 コア/24 GB）

（注）
現在のデバイス仕様に基づいて最適な階層が強調表示されます。

ステップ 3 選択内容とデバイスの仕様を確認します。

（注）
FTDv VM を設定する場合、サポートされる最大コア（vCPU）数は 12 個です（VMware および KVM での FTDv100 の場合は 16 個）。また、サポートされる最大メモリ容量は 24 GB RAM です。選択したパフォーマンス階層は、デバイスの仕様を超えることはできません。

ステップ 4 [はい（Yes）] をクリックして、パフォーマンス階層を変更します。

オプション ライセンスの有効化または無効化

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）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。ただし、評価モードでは RA VPNライセンスを有効化できません。

始める前に

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。

高可用性の設定で動作する装置の場合は、アクティブな装置でのみライセンスを有効化または無効化します。スタンバイ装置が必要なライセンスを要求（または解放）すると、次の設定の展開時にスタンバイ装置に変更内容が反映されます。ライセンスを有効にする際は、Cisco Smart Software Manager アカウントで十分な数のライセンスが使用可能であることを確認する必要があります。これを確認しないと、一方の装置が準拠、もう一方の装置が非準拠になる可能性があります。

手順

ステップ 1 [デバイス（Device）] をクリックし、[スマートライセンス（Smart License）] のサマリーで [設定の表示（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の設定も、その機能を使用するポリシーの展開もできません。

ステップ 3 RA VPNライセンスを有効にしている場合、アカウントで使用可能なライセンスタイプを選択します。

AnyConnect Client の任意のライセンス（Plus]、Apex]、[VPNのみ（VPN Only）]）を使用できます。両方のライセンスがあり、どちらも使用する場合は [PlusおよびApex（Plus and Apex）] を選択できます。

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）] をクリックし、[スマートライセンス（Smart License）] のサマリーで [設定の表示（View Configuration）] をクリックします。

ステップ 2 歯車の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Base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。また、デバイスはクラウドおよびクラウドサービスから登録解除されます。

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。

⚠

注意 デバイスの登録を解除するには、次の手順を使用する必要があります。代わりに Cisco Smart Software Manager アカウントから登録を解除すると、デバイスでのライセンス状態と Cisco Smart Software Manager でのライセンス状態の間に不一致が生じます。これにより、HA ペアを形成する場合など、デバイスのライセンス登録を再度試行したときにエラーが発生します。この失敗の症状を示すメッセージは、「Failed to generate token to enroll with Cisco Cloud using Smart License」と「Could not return the certificate for the given sn (*serial_number*) since it is REVOKED.」です。この場合は、この手順を使用してユニットの登録を解除し、再試行してください。

始める前に

デバイスの登録解除時には、そのデバイスだけが登録解除されます。ハイアベイラビリティのために設定されているデバイスの場合は、その装置を登録解除するために、ハイアベイラビリティ ペアにあるその他の装置にログインする必要があります。

手順

ステップ 1 [デバイス（Device）] をクリックし、[スマートライセンス（Smart License）] のサマリーで [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。

永久ライセンスの適用

非エアギャップネットワークとエアギャップネットワークの両方で永久ライセンスを適用できます。エアギャップネットワークは、インターネットへのパスがないネットワークです。これらは、外部からの侵入や攻撃の可能性を完全に防ぐことを目指した高セキュリティネットワークです。インターネットへのパスがないため、Cisco Smart Software Manager にデバイスを直接登録することはできません。代わりに、永久ライセンス予約（PLR）モードを使用して、デバイスに適用可能なライセンスを取得できます。

PLR モードを使用する必要がある場合は、次のことに注意してください。

- ファイルポリシー、URL ルックアップ、パブリック Web サイトへの状況に応じた相互起動といった、インターネットへのアクセスを必要とする機能は使用できません。
- Web 分析と Cisco Success Network を有効にしても、インターネットへのアクセスがないため、シスコは関連データを収集しません。
- 地理位置情報データベース、侵入ルール、および脆弱性データベース（VDB）に更新を手動でアップロードする必要があります。たとえば、更新をフラッシュドライブにダウン

ロードし、そのドライブをセキュリティ保護された建物に持ち込んで、セキュリティ保護されたワークステーションからアップロードすることができます。

（注） Cisco Smart Software Manager は、デバイスのシリアル番号を使用して永久ライセンスを割り当てます。デバイスの登録を解除する必要があるものの、通常の登録解除プロセスまたはキャンセルプロセスでライセンス割り当ての削除に失敗した場合、シスコテクニカルサポートに連絡して、Cisco Smart Software Manager から登録を削除する必要があります。デバイスを再イメージ化しても、ライセンス登録は削除されません。

次のトピックでは、各タイプの永久ライセンス、それらを適用する方法、およびデバイスの登録をキャンセルまたは解除する方法について詳しく説明します。

ユニバーサル永久ライセンスと特定ライセンス予約

ライセンス予約には、次の 2 つの異なるタイプがあります。

- ユニバーサル永久ライセンス予約（ユニバーサル PLR または UPLR）：ユニバーサル永久ライセンスでは、サポートされているファイアウォール製品（すべてのオプションライセンスを含む）を無期限かつ無制限で使用できます。ユニバーサル永久ライセンスを購入して適用すると、適用される機能ライセンスが、無期限に適用されます（通常は時間ベース）。ただし、スマート ライセンス アカウントで有効期限が切れた場合は、交換用ライセンスを購入する必要があります。ISA 3000 はユニバーサル PLR をサポートしていません。
- 特定ライセンス予約：特定ライセンス予約には、標準スマートライセンスと同じ数およびタイプのライセンスが必要です。このライセンスを取得する場合は、基本ライセンスに追加するオプションの機能ライセンスを選択します。このライセンスは有効期限があるため、定期的に更新する必要があります。

Firewall Device Manager ではユニバーサル PLR だけがサポートされています。

Cisco Smart Software Manager（CSSM）アカウントでユニバーサル永久ライセンス予約（PLR）モードを有効にする場合は、シスコの担当者と協同で作業する必要があります。

スマートアカウントがユニバーサルライセンスを提供できることの確認

永久ライセンスを取得して適用できることを確認するには、CSSMアカウントにログインし、**[スマート ソフトウェア ライセンシング（Smart Software Licensing）]** > **[インベントリ（Inventory）]** ページに移動して、[ライセンス（Licenses）] タブをクリックします。[ライセンスの予約（License Reservation）] ボタンが表示された場合は、永久ライセンス予約を取得する権限があります。

ただし、このボタンを使用すると、ユニバーサルライセンスと特定の永久ライセンスの両方に対して機能するウィザードが開始します。

また、デバイスのユニバーサルライセンスがあることを確認するには、使用可能なライセンスのリストを参照する必要があります。このライセンスは、[ライセンスの予約（License Reservation）] ボタンで起動するウィザードのステップ 2 で選択可能な項目として表示されます。

[ライセンスの予約（License Reservation）] ボタンが表示され、ユニバーサルライセンスを取得できる場合は、永久ライセンスを使用するためのシステムの変換に進めます。ボタンが表示されない場合、または特定のライセンスのみを予約できる場合は、シスコの担当者に連絡し、お客様のアカウントに対してユニバーサル PLR モードを有効にするように依頼してください。

PLR モードへの切り替えおよびユニバーサルライセンスの適用

スマートアカウントがユニバーサルライセンスを提供できることの確認 （14 ページ）の説明に従い、永久ライセンスを取得できることを確認し、必要なユニバーサルライセンスを購入したら、永久ライセンス予約（PLR）モードに切り替えてライセンスを適用できます。

⚠

注意 現在評価モードになっている場合、PLR モードに切り替えた後で評価モードに戻ることはできません。

始める前に

デバイスが高可用性用に設定されている場合は、HA グループ内の両方のデバイスに対して、このタスクを個別に実行する必要があります。

手順

ステップ 1 [デバイス（Device）] をクリックし、[スマート ライセンス概要（Smart License summary）] の [設定の表示（View Configuration）] をクリックします。

ステップ 2 スマートライセンスを使用してすでにデバイスを登録している場合は、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、登録解除を確認します。登録解除タスクが完了するのを待ってから、次に進みます。

ステップ 3 歯車 ドロップダウンリストから [ユニバーサルPLRに切り替え（Switch to Universal PLR）] を選択して、ユニバーサル永久ライセンス予約（PLR）モードに切り替えます。

警告を読み、[はい（Yes）] をクリックしてスイッチを確認します。

システムが PLR モードに切り替わり、PLR 登録プロセスが開始されます。

ステップ 4 PLR 登録を完了します。

a) [ユニバーサル永久ライセンス予約（Universal Permanent License Reservation）] ダイアログボックスが開いたら、最初のステップで必要な要求コードを含めます。テキストファイル

に保存する場合は [テキストで保存（Save AS TXT）] をクリックし、印刷する場合は [印刷（Print）] をクリックします。文字列を強調表示し、Ctrl+C を押してクリップボードにコピーすることもできます。

モードの切り替え後にプロセスをキャンセルした場合は、[ライセンス（Licensing）] ページの [予約の続行（Continue Reservation）] ボタンをクリックして、この時点から再開できます。

b) CSSM アカウントにログインし、**[スマート ソフトウェア ライセンシング（Smart Software Licensing）] > [インベントリ（Inventory）]** ページに移動して、[ライセンス（Licenses）] タブをクリックします。

c) [ライセンス予約（License Reservation）] ボタンをクリックし、ウィザードの指示に従います。生成した要求コードの入力を求められ、入力すると、承認コードを入手できます。

ウィザードには、次のステップが含まれています。

1. ライセンス要求コードを入力するか、コードを含むテキストファイルをアップロードして、[次へ（Next）] をクリックします。
2. ステップ 2 では、ライセンスを取得しているシステムの製品の詳細と、使用可能なライセンスの箇条書きリストが表示されます。ローカルで管理されている Firewall Threat Defense デバイスのユニバーサルライセンスを選択し、[次へ（Next）] をクリックします。
3. ステップ 3 では、適切なライセンスが選択されていることを確認し、[承認コードの生成（Generate Authorization Code）] をクリックします。
4. ステップ 4 では、承認コードが表示されます。必要に応じて、[ファイルとしてダウンロード（Download As File）] または [クリップボードにコピー（Copy to Clipboard）] をクリックして、コードを保存します。
5. [Close] をクリックしてウィザードを終了します。

d) Firewall Device Manager に戻り、承認コードを適切なフィールドに貼り付けます。

ユニバーサルライセンスの有効な承認コードの形式は次のとおりです。XXXXXX-XXXXXX-XXXXXX-XXXXXX-XXXXXX-XXXX。ここで X は英数字です。承認コードが XML ファイルである場合、特定のライセンスを保有していますが、このシステムでは使用できません。PLR 登録のキャンセル （17 ページ）の説明に従って登録をキャンセルし、CSSM で予約済みライセンスをリリースしてください。次に、シスコの担当者と協力して、スマートアカウントをユニバーサル PLR に変換します。

e) [登録（Register）] をクリックします。

登録プロセスが開始されます。[ライセンス（Licensing）] ページを更新して、登録ステータスを確認します。

ステップ 5 必要に応じて、オプションの機能ライセンスを有効にします。

ユニバーサルライセンスでは、Baseライセンスに対してのみデバイスが登録されます。必要な機能ライセンスごとに、[有効化（Enable）] をクリックできます。

PLR 登録のキャンセル

ユニバーサル永久ライセンス予約（PLR）要求は、完了する前にキャンセルできます。たとえば、PLR 登録プロセスを開始したが、Smart Software Manager アカウントが PLR に対して設定されていない場合は、PLR モードの承認を取得している間にプロセスをキャンセルし、スマート ライセンス アカウントを適切に設定できます。

PLR 登録プロセスが完了している場合は、キャンセルできません。代わりに、PLR モードでのデバイスの登録解除 （18 ページ）を参照してください。

手順

ステップ 1 [デバイス（Device）] をクリックし、[スマート ライセンス概要（Smart License summary）] 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 [PLRのキャンセル（Cancel PLR）] を選択して、キャンセルプロセスを開始します。

ステップ 3 状況に適したオプションを選択します。

- [CSSMにライセンスがあります（I have a license in CSSM）]：Cisco Smart Software Manager（CSSM）でライセンス登録ウィザードを実行し、承認コードを取得している場合は、このオプションを使用します。この時点で、CSSM に予約されているライセンスがあるため、それらのライセンスをリリースする必要があります。
- [CSSMにライセンスがありません（I do not have a license in CSSM）]：承認コードを取得した時点でCSSM ウィザードを完了していない場合は、このオプションを使用します。たとえば、Firewall Device Manager で PLR 登録を開始したが、自分のスマートアカウントに [ライセンス予約（License Reservation）] ボタンがないことに気付いた場合に使用します。

ステップ 4 （[CSSMにライセンスがあります（I have a license in CSSM）] を選択した場合）ライセンスが使用中としてマークされていないことを確認するには、CSSMからリリースコードを取得する必要があります。取得しないと、それらのライセンスは他のデバイスで使用可能な状態になりません。

a) （登録時に）CSSM から取得した承認コードを [キャンセル（Cancellation）] ダイアログボックスに貼り付け、[リリースコードの生成（Generate Release Code）] をクリックします。

b) [ライセンスコードのリリース（Release License Code）] フィールドにコードがある場合は、[テキストで保存（Save As TXT）] をクリックしてテキストファイルに保存するか、[印刷（Print）] をクリックして印刷します。コードを選択し、Ctrl+C を押してクリップボードにコピーすることもできます。

c) CSSM の **[スマート ソフトウェア ライセンシング（Smart Software Licensing）]** > **[インベントリ（Inventory）]** ページでデバイスを見つけ（[名前（Name）] はデバイスのシリアル番号）、**[アクション（Action）]** > **[削除（Remove）]** をクリックして、リリースコードを入力します。

CSSM に製品が正常に削除されたことが表示されるまで待ちます。

ステップ 5 [OK] をクリックしてキャンセルプロセスを完了します。

システムがスマートライセンスモードに戻ります。ただし、デバイスは登録解除されるため、評価モードは再開できません。この時点で、スマートライセンスを使用してデバイスを登録するか、PLR モードに切り替えて、使用するデバイスを再度登録する必要があります。

PLR モードでのデバイスの登録解除

デバイスの使用を停止する、別のファシリティに移動するなどによりデバイスのライセンスを必要としなくなった場合、デバイスの登録を解除できます。

デバイスの登録を解除すると、ライセンスが未使用の状態に戻ります。デバイスの登録を解除しない場合、ライセンスは使用中としてマークされたままになり、他の目的で使用することはできません。

手順

ステップ 1 [デバイス（Device）] をクリックし、[スマート ライセンス概要（Smart License summary）] 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 [ユニバーサルPLRの登録解除（Unregister Universal PLR）] を選択し、警告を読み、[はい（Yes）] をクリックしてプロセスを開始します。

ステップ 3 [ユニバーサル永久ライセンス予約の登録解除（Unregister Universal Permanent License Reservation）] ダイアログボックスが開くと、[リリースライセンスコード（Release License Code）] フィールドには、CSSM アカウントに現在割り当てられているライセンスを解放するために必要なコードが入力されます。このコードのコピーを保持するには、[テキストで保存（Save as TXT）] または [印刷（Print）] をクリックします。コードを選択し、Ctrl+C を押してクリップボードにコピーすることもできます。

ステップ 4 CSSM アカウントに移動し、**[スマート ソフトウェア ライセンシング（Smart Software Licensing）]** > **[インベントリ（Inventory）]** ページでデバイスを見つけ（[名前（Name）] はデバイスのシリアル番号）、**[アクション（Action）]** > **[削除（Remove）]** をクリックして、リリースコードを入力します。

CSSM に製品が正常に削除されたことが表示されるまで待ちます。

ステップ 5 Firewall Device Manager に戻り、[デバイスの登録解除（Unregister Device）] ダイアログボックスで [登録解除（Unregister）] をクリックします。

これでプロセスは完了です。この時点で、CSSMのライセンスは他のデバイスに自由に割り当てることができ、Firewall Threat Defense デバイスのライセンスは解除されます。

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。

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。