モニタリング

使用できる**モニタリング**オプションは、ユーザーロールによって異なります。

エージェントのモニタリング

このページには、現在選択されているルート範囲に基づいて、クラスタ内のすべての監視対象エージェントの数が表示されます。

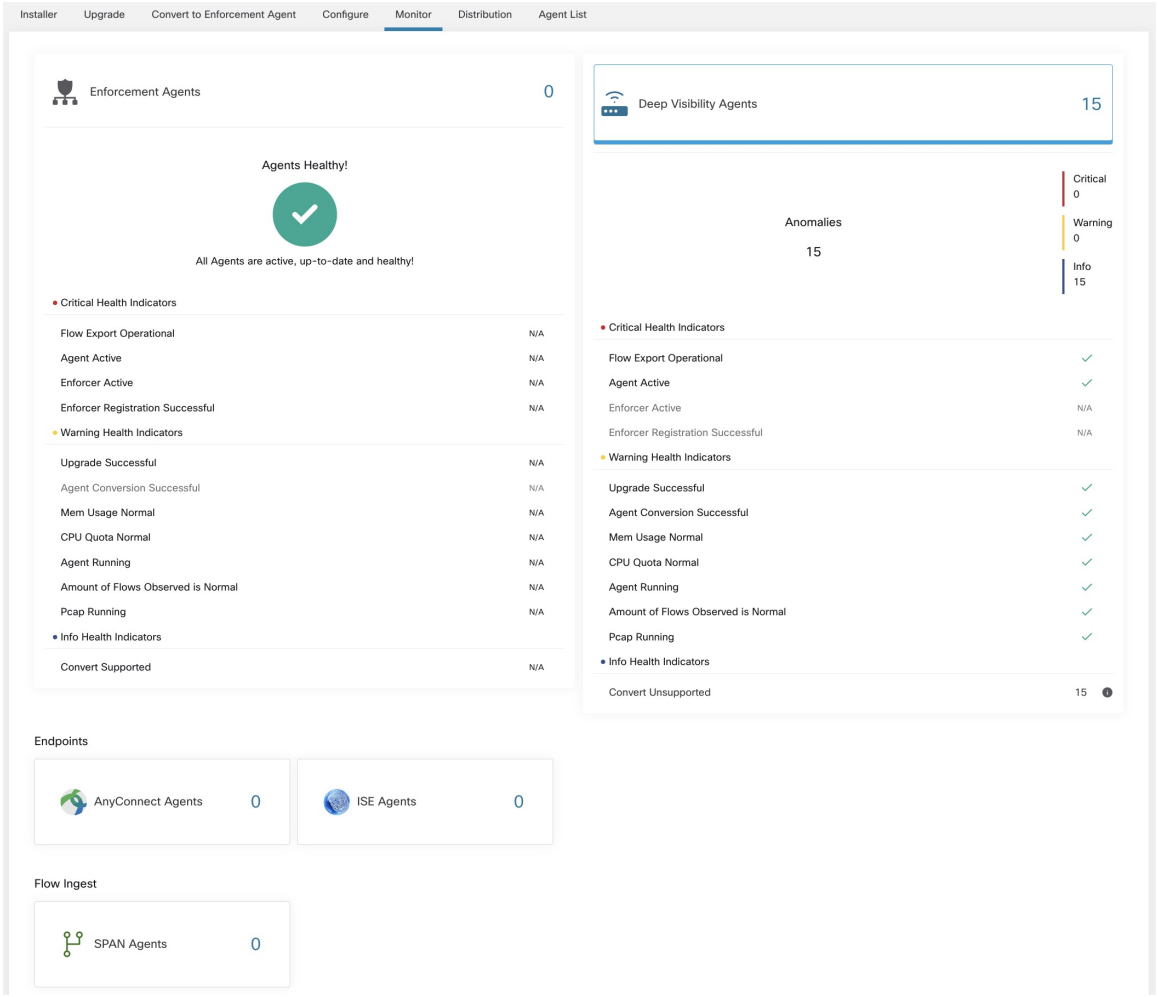
（注） インベントリの総数は、収集ルールを適用した後にネットワーク上で観察されたすべてのインベントリの合計です。

エージェントのモニタリング

エージェントを監視するには、左側のナビゲーションバーで**[管理（Manage）]** > **[エージェント（Agents）]**をクリックし、[監視（Monitor）] タブをクリックします。

このページは、**サイト管理者**および**カスタマーサポート**の役割を持つユーザーのみが利用できます。**範囲所有者**は、インベントリ、優れた可視性エージェント、および適用エージェントを表示できます。

図 *1:* インストールされているエージェントの総数



次の表は、エージェントタイプごとの違いを示しています。

Agent Type	説明
優れた可視性	時系列フローデータ、ホストで実行されるプロセスに関して最高の忠実度を提供します。ほとんどの Linux および Windows プラットフォームがサポートされています。sw_agents_deployment-label を参照してください。
施行	優れた可視性エージェントで使用可能なすべての機能を提供します。それに加えて、適用エージェントはインストールされているホストに対してファイアウォールルールを設定することができます。

AnyConnect	Network Visibility Module（NVM）を備えた AnyConnect セキュア モビリティ エージェントを実行しているエンドポイントで時系列フローデータを提供します。Cisco Secure Workload エージェントのインストールは必要ありません。NVM によって生成された IPFIX レコードは、Secure Workload AnyConnect プロキシコネクタに送信されます。Windows、Mac、および特定のスマートフォンのプラットフォームがサポートされています。
ISE	Cisco ISE に登録されているエンドポイントに関するメタデータを提供します。ISE コネクタは、ISE pxGrid を介してメタデータを収集し、ISE エージェントが ISE アプライアンスから取得した属性とエンドポイントにログインしたユーザーの LDAP 属性に基づいてラベルをプッシュするときに ISE エンドポイントを Secure Workload に登録します。
次の表は、Cisco Secure Workload が提供するさまざまなアプライアンスエージェントの概要を示しています。	
アプライアンスエージェント	説明
SPAN	ホストごとのエージェントのインストールを必要とせずに、フロー分析を提供します。Secure Workload ERSPAN VM アプライアンスで実行されます。任意の Cisco スイッチから発信された ERSPAN パケットを消費します。

（注） NetFlow、NetScaler、F5、AWS、AnyConnect Proxy などのアプライアンスエージェントが、コネクタとしてサポートされるようになりました。コネクタの詳細については、「コネクタとは」を参照してください。

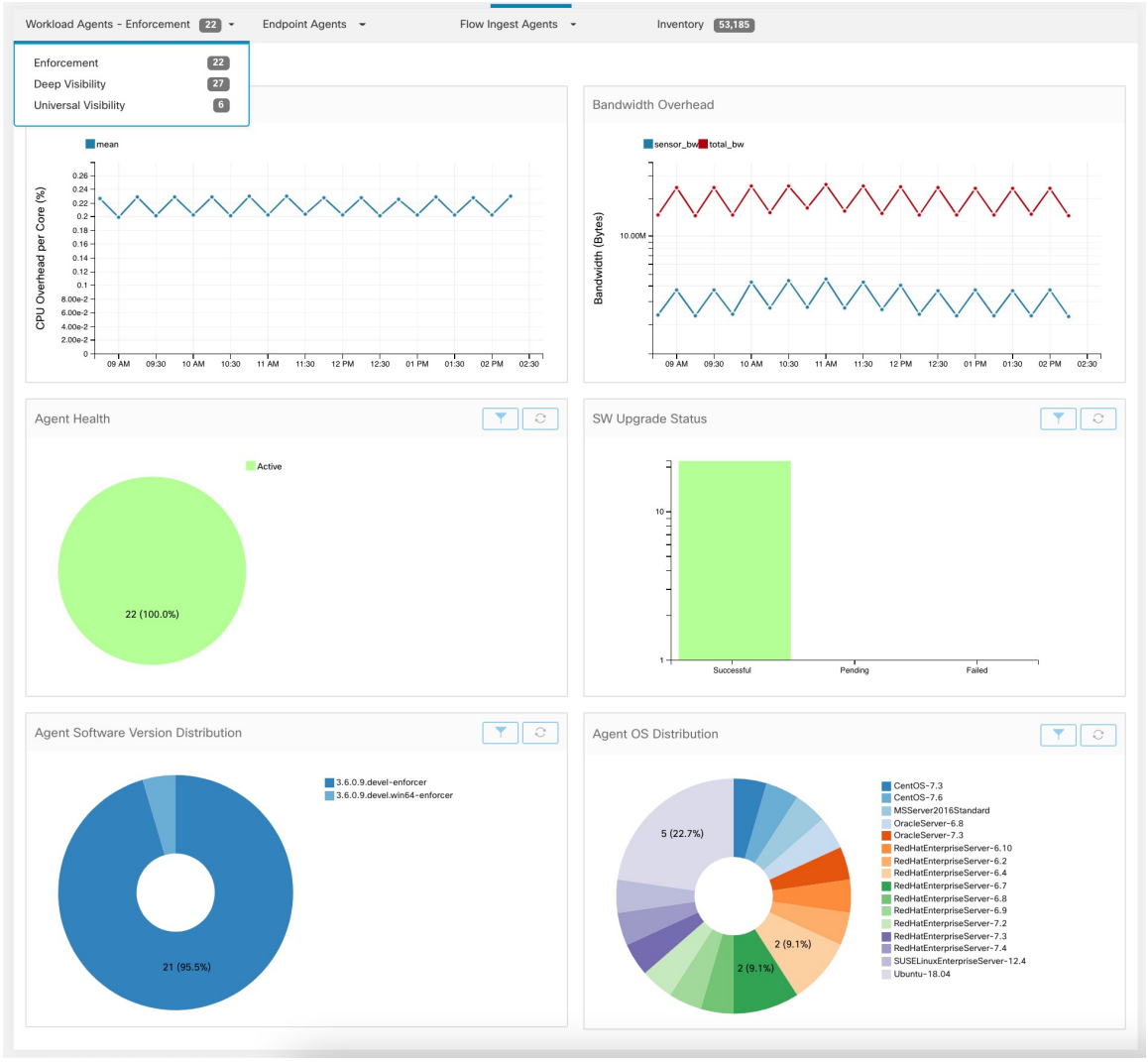
ゼロ以外のエージェントタイプのボタンを押すと、各エージェントタイプの分布にさらにドリルダウンできます。

エージェントのステータスと統計

このトピックで説明されているチャートを表示するには、[管理（Manage）] > [エージェント（Agents）] を選択し、[分布（Distribution）] タブをクリックします。

次のすべてのグラフは、詳細可視性タイプと適用エージェントタイプの両方で使用できます。

図 *2:* エージェントの分布



このページには、エージェントタイプごとに、全体的な CPU オーバーヘッド、帯域幅のオーバーヘッド、欠落したパケット、OS/バージョンの分布、エージェントのアップグレードステータスなど、登録されたエージェントの概要と正常性が表示されます。

[CPUオーバーヘッド（CPU Overhead）] チャート

[CPUオーバーヘッド（CPU Overhead）]チャートには、全エージェントからのコアごとのCPUオーバーヘッド集計ビューが表示されます。エージェントごとのCPUオーバーヘッドは、ワークロードプロファイルの一部として表示されます。このチャートは、詳細可視性タイプと適用エージェントタイプでのみ使用できます。

[帯域幅オーバーヘッド（Bandwidth Overhead）] チャート

[帯域幅オーバーヘッド（Bandwidth Overhead）] グラフには、総帯域幅とエージェントが使用する帯域幅の集約された統計が表示されます。エージェントごとの帯域幅オーバーヘッドは、

ワークロードプロファイルの一部として表示されます。このチャートは、詳細可視性タイプと適用エージェントタイプでのみ使用できます。

[エージェントの正常性（Agent Health）] チャート

[エージェントの正常性（Agent Health）] チャートには、アクティブ/非アクティブなエージェントの数が表示されます。アクティブなエージェントは、アップグレードのためにコンフィギュレーションサーバーに定期的にチェックインするエージェントです。チェックインの間隔は 30 分です。エージェントが 2 回を超えてチェックイン期間にチェックインしなかったことがわかった場合、そのエージェントは非アクティブなエージェントと宣言されます。

[最新のリビジョンへのソフトウェアエージェントの更新（Software Agent Updates to Latest Revision）] チャート

エージェントがコンフィギュレーションサーバーにチェックインするたびに、エージェントは現在の RPM バージョンも提示します。エージェントが特定のバージョンに設定されていて、2 回のチェックイン期間後に更新できていなかった場合、そのエージェントは最新バージョンにアップグレードできないと宣言されます。

[欠落エージェントパケット（Agent Packet Missed）] チャート

まれに、ホストを通過するトラフィック量がエージェントの検査できるレートよりも多い場合、一部のパケットが分析からスキップされます。欠落パケット数と対応するエージェント名がこのチャートに表示されます。

[エージェントのソフトウェアバージョン/OS分布（Agent Software Version/OS Distribution）] チャート

これらのグラフには、Secure Workload クラスタに登録されているすべてのエージェントのエージェントバージョン分布と親 OS プラットフォームが表示されます。

適用ステータス

適用ステータスを表示するには、ウィンドウの左側のナビゲーションバーの **[保護（Defend）]**> **[適用ステータス（Enforcement Status）]** をクリックします。

このページは、サイト管理者/カスタマーサポートユーザーと範囲所有者が、全適用エージェントの現在のステータス概要（ポリシーを適用しているクラウドコネクタを含む）を取得するために使用できます。

いずれかのチャートで赤またはオレンジが表示されている場合は、該当するトピックを参照してください。

表 *1*: 適用ステータスチャート

チャート（Chart）	結果	アクションの実行
適用が有効なエージェント（Agent Enforcement Enabled）	有効化されていない（Not Enabled）	エージェント設定で適用が有効になっていることを確認します。エージェント設定プロファイルの作成を参照してください。

チャート（**Chart**）	結果	アクションの実行
エージェントポリシーの設定（Agent Policy Config）	古いポリシー（Stale Policies）	一般的に、この状況は一時的なものであり、通常はアクションを必要としません。これは、ラベルに基づく Secure Workload 展開によってインベントリとポリシーが動的に更新されるために発生します。 ただし、個々のワークロードでこの状況が続く場合は、Cisco TAC にお問い合わせください。
エージェントの具体的なポリシー（Agent Concrete Policies）	スキップ（Skipped）	これは、ポリシーが一部のエージェントにプッシュされなかったことを示します。

ヒント

- 個々の範囲またはテナント全体のステータスを表示するには、ページの左上にある [範囲でフィルタ（Filter by Scope）] オプションを使用します。
- チャートに問題が示されている場合は、チャートの関連部分をクリックして、問題のあるワークロードを特定します。

  チャートの下のテーブルには、影響を受けるワークロードが表示されます。

  または、フィルタリングオプションを表示するには、チャートの下にある [フィルタ（Filter）] ボックス内の [(i)] ボタンをクリックします。
- 豊富な追加の詳細を表示するには、フィルタされたワークロードのリスト内で IP アドレスリンクをクリックして、[ワークロードプロファイル（Workload Profile）] ページを表示します。

次の表で、適用ステータステーブルに表示されるフィールドについて説明します。

フィールド	説明
[Host Name]	ワークロードのホスト名。
アドレス（Address）	ワークロード上のすべてのインターフェイスの IP アドレス。
[有効化された適用（Enforcement Enabled）]	エージェントで適用が有効になっているかどうかを示します。
[同期されている具体的なポリシー（Concrete Policies in Sync）]	必要なバージョンの具体的なポリシーが現在エージェントに適用されているかどうかを示します。

[具体的なポリシー（Concrete Polices）]	いずれかのホストでこの値が [スキップ（Skipped）] と表示されている場合は、そのホスト上のエージェントがポリシーの制限に達していることを意味します。（ポリシーに関連する制限 を参照。）
[ポリシー数（Policy Count）]	エージェントの具体的なポリシーの数。
ステータス（Status）	最新のポリシー設定適用のステータス。ステータスが [CONFIG_SUCCESS] の場合、現在のバージョンが問題なく適用されていることを示します。

クラウドコネクタの適用ステータス

AWS または Azure クラウドコネクタを設定している場合：

すべてのインターフェイスの適用ステータスを、適用ステータスページで確認できます。ポリシーが正常に適用された場合、ポリシーが同期していることがわかります。そうでない場合は、対応するエラーメッセージが表示されます。

適用ステータスページのポリシー数はSecure Workloadアカウンティングで、AWSまたはAzureルールアカウンティングではありません。

（AWS のみ）このページのホスト名フィールドは、パブリック DNS から取得されます。指定された VPC でパブリック DNS が有効になっていない場合、ホスト名フィールドは空になります。

ポリシー更新の一時停止

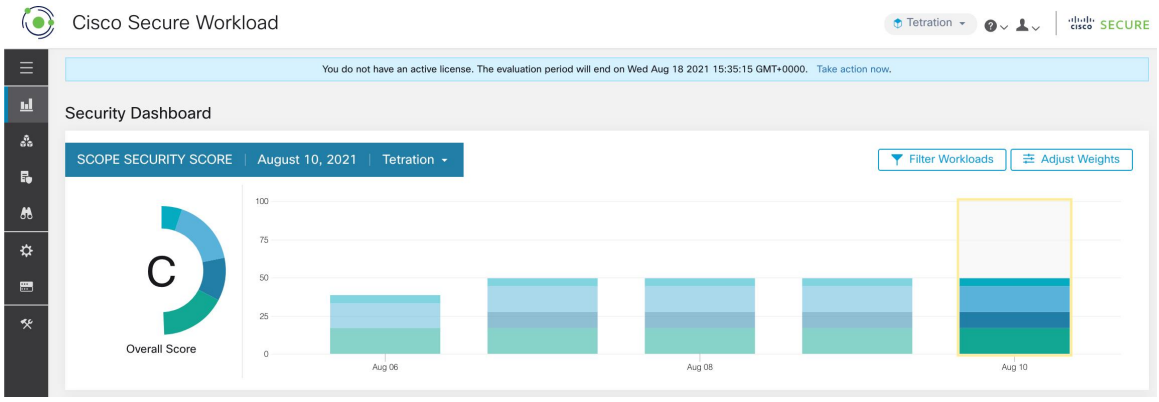
ポリシー更新の一時停止 を参照してください。

ライセンス

Secure Workload ライセンスのステータスを表示するには、ウィンドウの左側にあるナビゲーションバーで、**[管理（Manage）]** > **[ライセンス（Licenses）]** をクリックします。

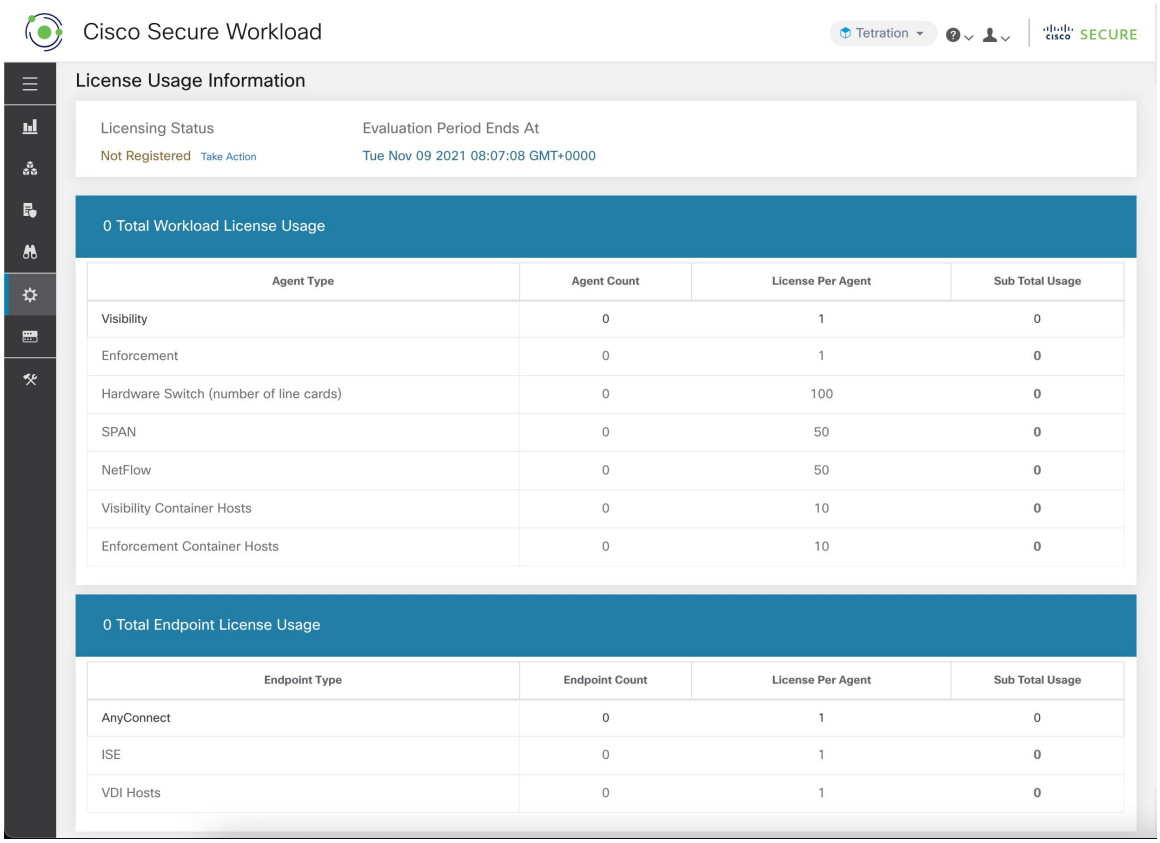
このページは、サイト管理者が現在のライセンスステータスとライセンス使用状況の概要を取得するために使用します。このリリース以降では、オンプレミスでの展開用にクラスタを登録する必要があります。このリリースで新しいクラスタにアップグレードするか、新しいクラスタを展開すると、ソフトウェアは自動的に 90 日間の評価モードに入ります。バナーが表示され、評価の有効期限が示されます。

図 *3:* ライセンスバナー



（注） 90 日以内に登録が正常に完了しなかった場合、バナーメッセージはコンプライアンス不適合に変わります。登録がないため、ブロックされる機能はありません。

図 *4:* [監視（*monitoring*）] - [ライセンス（*licenses*）] ページで表示される詳細なライセンス情報

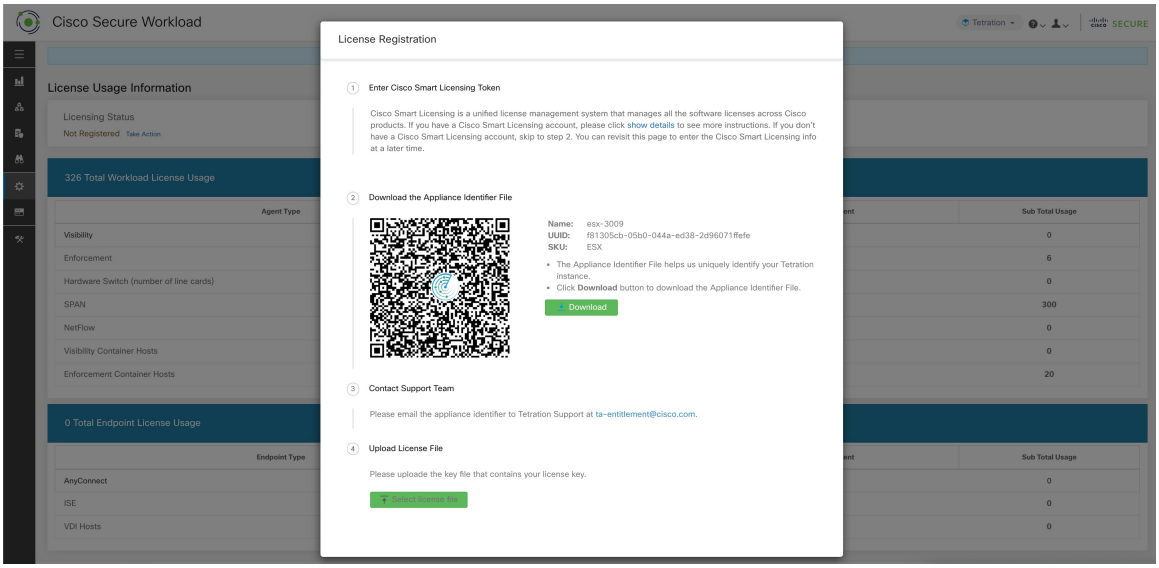


ライセンス登録

このセクションでは、ライセンスの取得方法について説明します。

ライセンスバナーまたは **[管理（Manage）]** > **[ライセンス（Licenses）]** ページで [アクションの実行（Take Action）] をクリックして、ライセンスを要求します。クラスタ識別ファイルをダウンロードする方法とライセンスを取得する方法についての説明が表示されます。

図 *5:* ライセンス登録モーダル：クラスタ識別ファイルのダウンロード



手順

ステップ 1 **ライセンス登録モーダル**を完了するには、CSSM スマート ソフトウェア ライセンス ポータルで生成された登録トークンが必要です。CSSM を使用してトークンを生成する手順は、ライセンスモーダル自体に表示されます。登録トークンを取得したら、トークンをコピーしてライセンスモーダルのテキストボックスに貼り付け、テキストボックスの横にある [送信（Submit）] ボタンをクリックします。

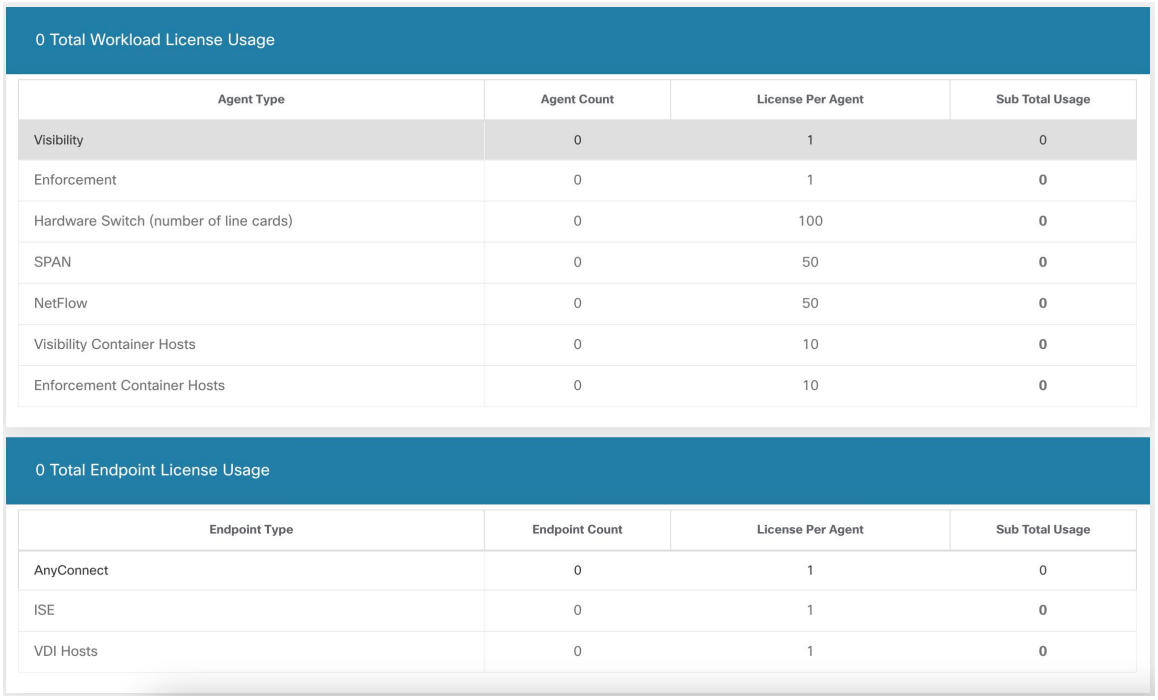
ステップ 2 次に、[Download] ボタンをクリックして、クラスタ識別ファイルをローカルストレージにダウンロードします。識別ファイルのファイル名形式は **reg_id_<cluster_name> _<cluster_uuid> .gz** です。ID ファイルには、IP アドレス情報、特定のワークロードの詳細、または PII 情報は含まれていません。この ID ファイルを ta-entitlement@cisco.com に送信する必要があります。**ライセンスキーファイル**を含む応答が、識別ファイルを受信したときと同じ電子メールアドレスに送信されます。

ステップ 3 この**ライセンスキーファイル**をライセンスモーダルからアップロードする必要があります。応答ファイルをアップロードするには、ライセンスモーダルの手順 4 を使用します。

ライセンス使用状況の確認

このセクションでは、詳細なライセンス使用状況を確認する方法について説明します。左側のナビゲーションバーで、**[管理（Manage）]** > **[ライセンス（Licenses）]** をクリックします。

図 *6:* ライセンステーブルと詳しい使用状況



0 Total Workload License Usage

Agent Type	Agent Count	License Per Agent	Sub Total Usage
Visibility	0	1	0
Enforcement	0	1	0
Hardware Switch (number of line cards)	0	100	0
SPAN	0	50	0
NetFlow	0	50	0
Visibility Container Hosts	0	10	0
Enforcement Container Hosts	0	10	0

0 Total Endpoint License Usage

Endpoint Type	Endpoint Count	License Per Agent	Sub Total Usage
AnyConnect	0	1	0
ISE	0	1	0
VDI Hosts	0	1	0

（注） 登録後、ライセンス使用量がエンタイトルメント（ワークロードまたはエンドポイント）を超えると、非準拠の警告バナーが UI に表示されます。ライセンス使用量を上回っても、追加センサーのインストールを含め、どの機能もブロックされることはありません。使用量がエンタイトルメントを下回ると、準拠に関する警告バナーは消えます。追加のライセンスを購入した場合は、ID 情報（ライセンスモーダルから再度ダウンロード）とともに ta-entitlement@cisco.com に連絡して、更新されたライセンスキーファイルを要求できます。

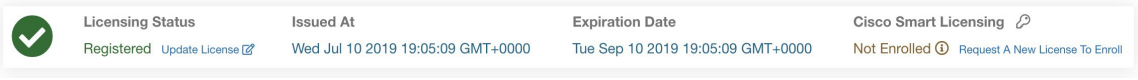
Cisco Smart Licensing の詳細

Cisco スマートライセンスは統合ライセンス管理システムであり、Cisco 製品のソフトウェアライセンスすべてを管理します。Cisco Smart Licensing アカウントを持っている場合は、Cisco Smart Licensing Token を Secure Workload ライセンスに関連付けることができます。Cisco Smart Licensing アカウントを持っていない場合は、Cisco Smart Licensing なしでライセンスを取得または更新できます。

手順

ステップ 1 有効な Secure Workload ライセンスをすでに持っている場合は、[登録する新しいライセンスをリクエスト（Request A New License To Enroll）] をクリックして、Cisco Smart Licensing Token を使用して新しいライセンスを取得できます。

図 *7:* 新しいライセンスを取得して、*Cisco Smart Licensing Token* をライセンスに *Secure Workload* に関連付ける



ステップ 2 有効な Secure Workload ライセンスがない場合は、前のセクションの説明に従い、[アクションの実行（Take Action）] をクリックして新しいライセンスを取得できます。

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。