RV34xシリーズルータの侵入防御システムの設定

目的

このドキュメントの目的は、RV34xシリーズルータで侵入防御システム(IPS)を設定する方法を示すことです。

概要

侵入防御システム(IPS)はトラフィックをスキャンして、ブロックする既知の攻撃パターンを探します。ルータを通過するパケットとセッションを監視し、各パケットをスキャンして任意のCisco IPSシグニチャと一致させます。疑わしいアクティビティを検出すると、ログを記録またはブロックするように設計されています。IPSおよびウイルス対策データベースと定義を更新することが重要です。これらは手動または自動で更新できます。

Cisco Intrusion Prevention Systemの次のビデオをご覧ください。

ただし、IPSはルータのパフォーマンスに影響を与える可能性があります。一般に、ハイパーテキスト転送プロトコル(HTTP)トラフィックとファイル転送プロトコル(FTP)トラフィックの総スループットには影響しませんが、同時接続の最大数を大幅に減らすことができます。

特記事項：ルータの負荷が大きい場合は、問題が悪化する可能性があります。

次の表に、さまざまな設定でのパフォーマンスに関する予想される統計情報を示します。これらの値はガイドとして使用する必要があります。実際のパフォーマンスは多くの要因によって異なる場合があります。

	同時接続	接続レート	HTTPスループット	FTPスループット
デフォルト設定	40000	3,000	982 MB/秒	981 MB/秒
APP制御の有効化	15000-16000	1300	982 MB/秒	981 MB/秒
ウイルス対策を有効にする	16000	1,500	982 MB/秒	981 MB/秒
IPSの有効化	**17000**	**1300**	**982 MB/秒**	**981 MB/秒**
App Control Antivirus & IPSの有効化	15000-16000	1,000	982 MB/秒	981 MB/秒

次のフィールドは次のように定義されます。

同時接続数：同時接続数の合計。たとえば、あるサイトからファイルをダウンロードしている場合、つまり1つの接続であるSpotifyからオーディオをストリーミングして、別の接続を確立し、同時に2つの接続を確立します。

Connection Rate：処理できる接続要求の数/秒。

HTTP/FTPスループット:HTTPおよびFTPのスループットは、ダウンロード速度（MB/秒）です。

セキュリティライセンスが更新され、既存のアプリケーションやWebフィルタリングに加えてIPS保護が追加されました。セキュリティライセンスを取得するには、スマートアカウントが必要です。アクティブなスマートアカウントがない場合は、このドキュメントのセクション1が必要です。

RV34xでウイルス対策を設定する方法については、ここをクリックしてください。

該当するデバイス

RV34x

[Software Version]

1.0.03.x

目次

Smart Licensing

アクティブなスマートアカウントがない場合は、次の手順に進む必要があります。

スマートライセンスアカウントの設定中に問題が発生した場合は、サポートチームが潜在的な問題を解決し、複数の方法で問題を解決できます。ご希望の方法で連絡してください。

ルータコミュニティ： Cisco Small Business Support Community

RV34xシリーズに関するFAQ: RV34xシリーズルータに関するFAQ

スマートライセンスの概要： スマート ソフトウェア ライセンシング

スマートライセンスに関するFAQ: パートナー、ディストリビュータ、およびお客様向けのスマートライセンスおよびスマートアカウントに関するFAQ

ケースを送信します。 Support Case Manager

米国/カナダのサポート電話番号：1-866-606-1866またはSmall Business TACの連絡先

メール：licensing@cisco.com

ステップ1：最近Cisco.comアカウントを作成または閲覧した場合は、独自のスマートライセンスアカウントを作成するためのメッセージが表示されます。Smart Licenseアカウントの作成ページに移動するには、ここをクリックしてください。ログインが必要になる場合があります。

注：スマートアカウントのリクエスト手順の詳細については、ここをクリックしてください。

ステップ2：ルータのスマートライセンスを購入する際には、ベンダーが独自のライセンスIDをスマートライセンスアカウントに移動するプロセスを行う必要があります。次の表は、バンドルの購入時に必要な情報を示しています。

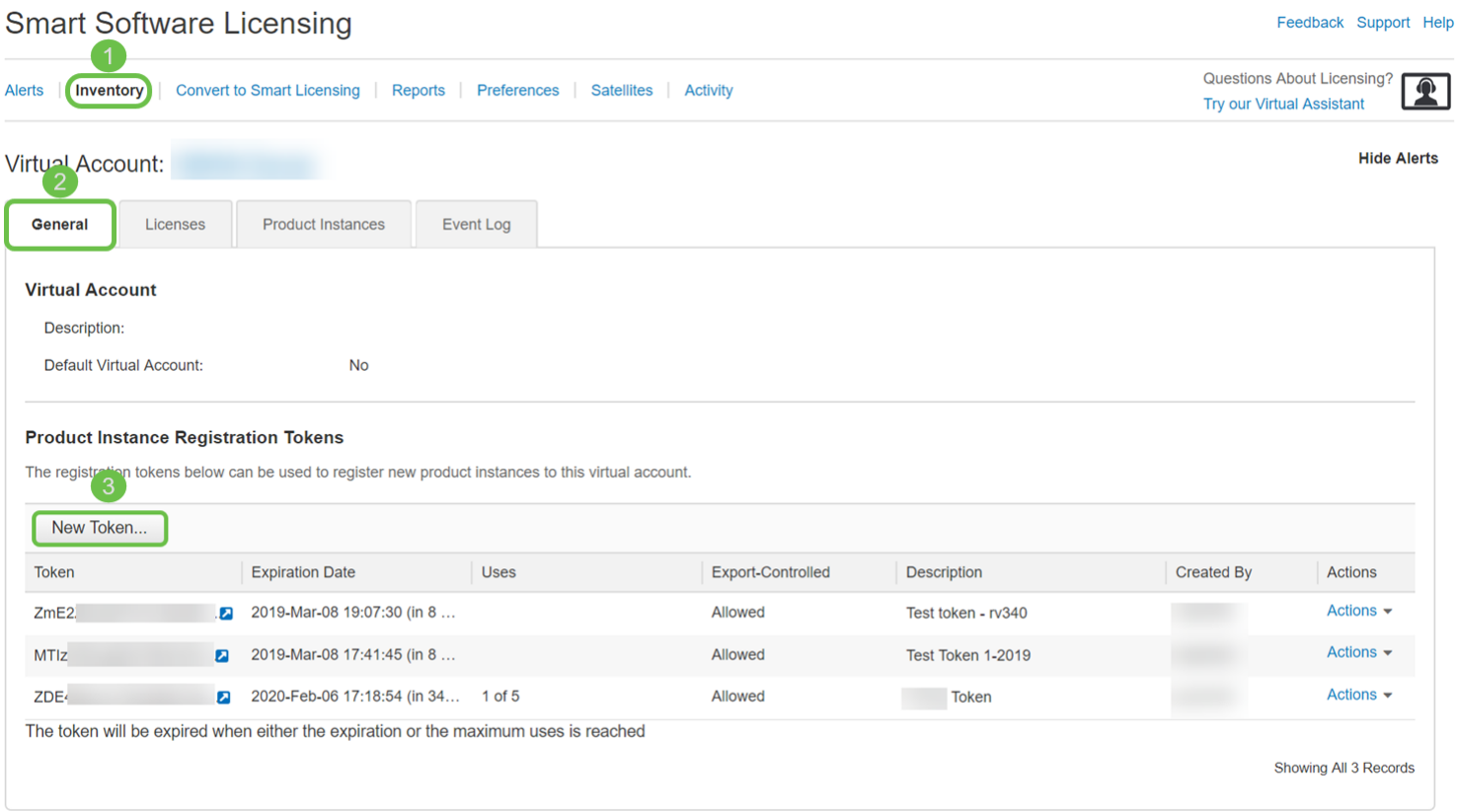
注：IPSとアンチウイルスは、Webフィルタリングとアプリケーションフィルタリングに使用されるセキュリティライセンスの一部です。

必要な情報	情報の検索
Cisco.comユーザID	アカウントプロファイルに配置するか、ここをクリックできます。
スマートライセンスアカウント名	ライセンスを購入する前にスマートアカウントを作成しておくことをお勧めします。 これは、「スマートライセンスアカウントの作成」の記事のステップ8でする。
スマートライセンスSKU	デバイスの製品識別コード。 例：RV340-K9-NA

注：ライセンスを購入していて、仮想アカウントに表示されない場合は、リセラーに連絡して転送を要求するか、または当社に連絡してください。

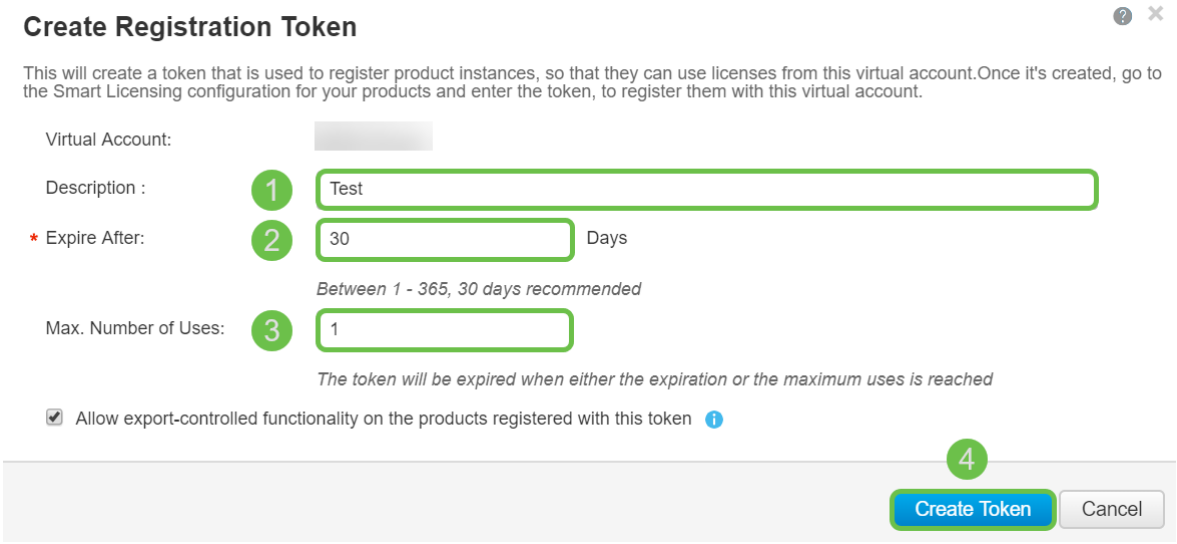
プロセスを適切に行うには、ライセンス請求書、シスコの販売注文番号、およびスマートアカウントライセンスページのスクリーンショットを用意する必要があります（チームと共有するため）。

ステップ3：トークンを生成するには、スマートソフトウェアライセンス[アカウントに移動](#)します。次に、[インベントリ] > **[全般]タブをクリックします。[New Token...]ボタンをクリックします。**

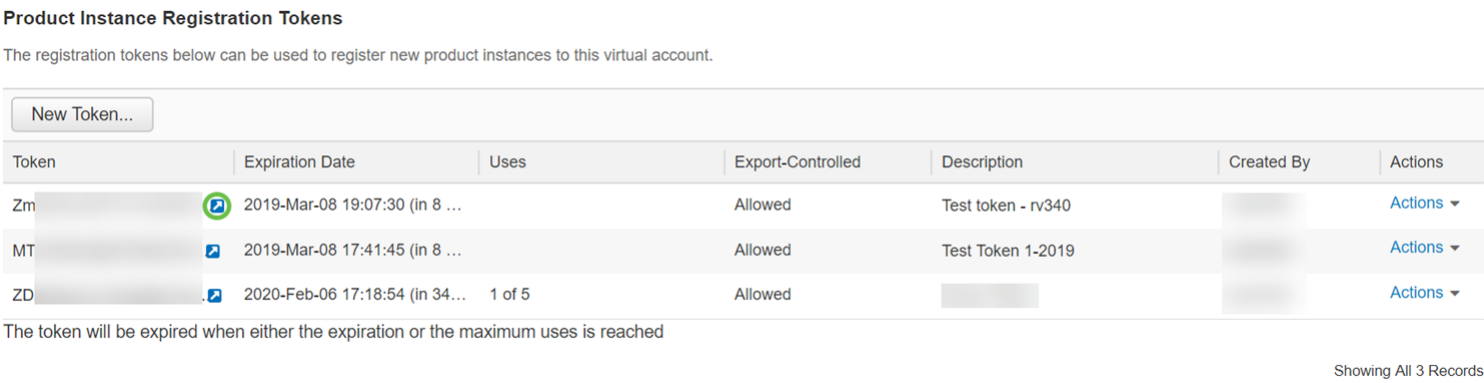


ステップ4:[Create Registration Token]ウィンドウが開きます。[説明]、*[期限切れ後]*、*[最大値]を入力します。使用回数*。次に、[トークンの作**成]ボタンを押**します。

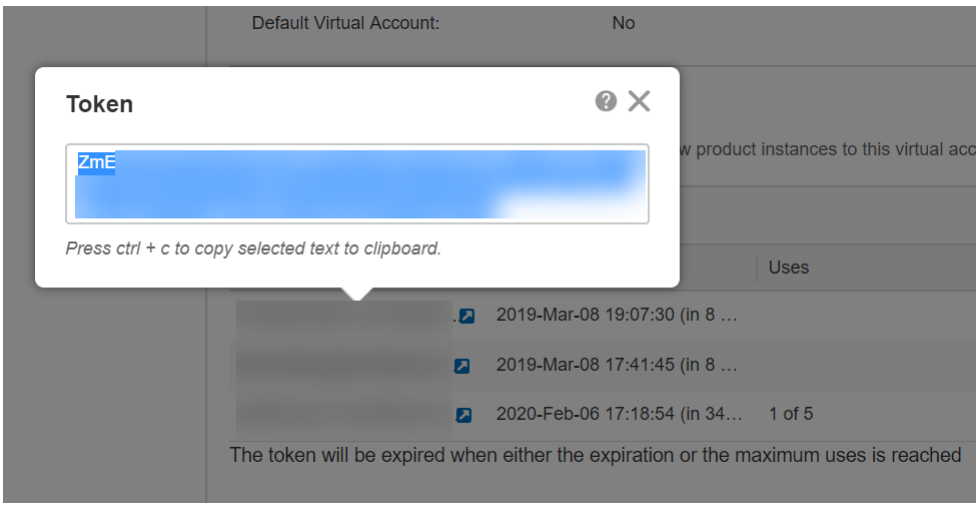
注：30日間の有効期限*が推奨*されます。



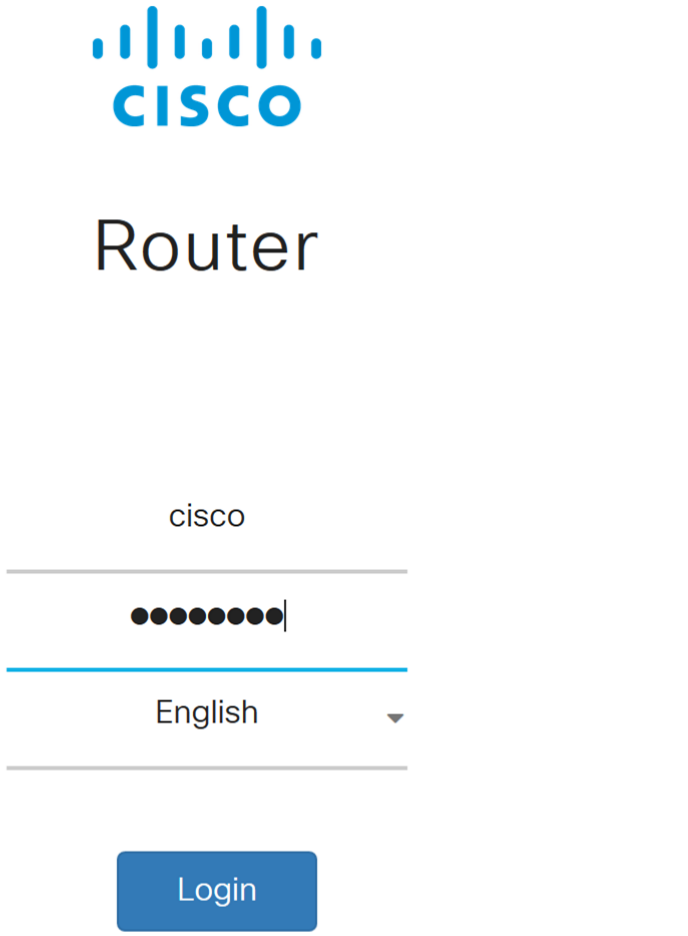
ステップ5：トークンが生成されたら、最近作成したトークンの右側にある**[Token]リンク（白い矢印の付いた青いボックス）ボタンをクリック**します。



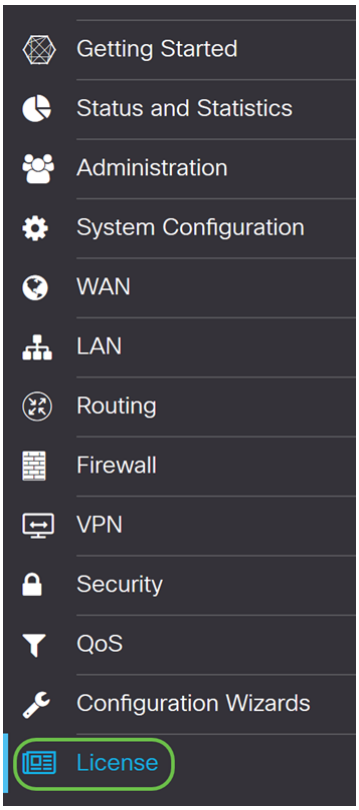
ステップ6：コピーする完全なトークンが含まれた[Token]ウィンドウが表示されます。トークンを強調表示し、トークンを右クリックして**[Copy]**をクリックするか、キーボードの**ctrlボタンを押したまま**cを同時にクリックしてテキストをコピーします。



ステップ7：トークンをコピーしたら、デバイスにログインし、トークンキーをアップロードする必要があります。ルータのWeb設定ページにログインします。

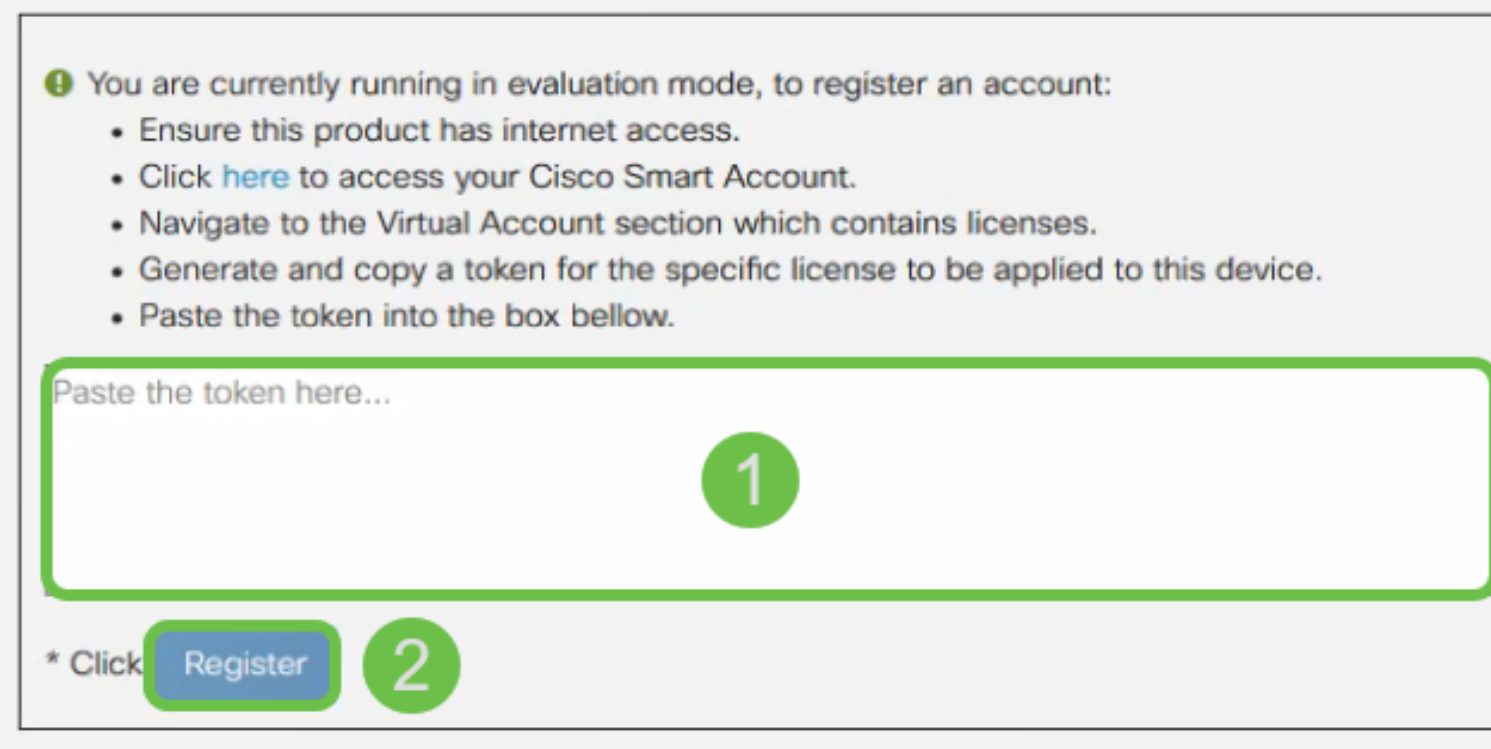


ステップ8:[License]に移動します。

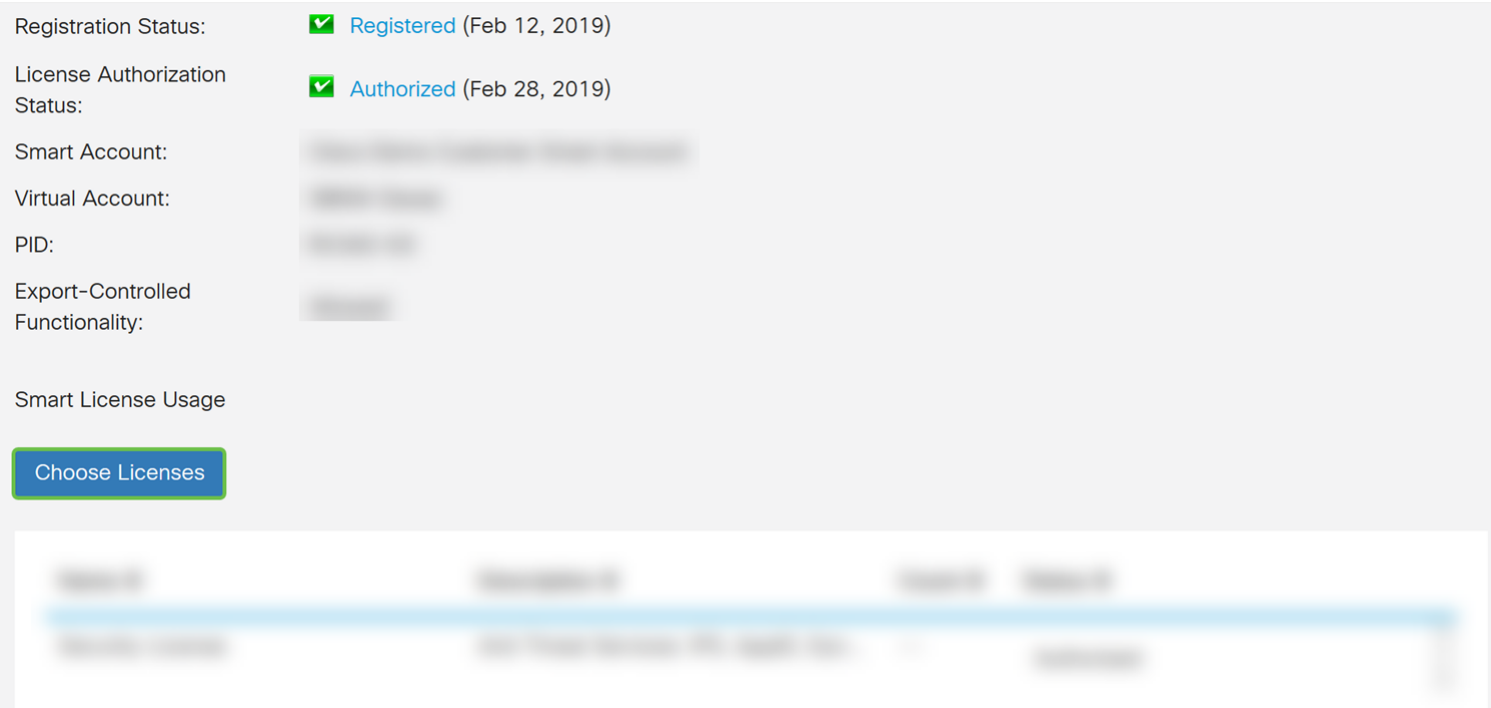


ステップ9：デバイスが登録解除されると、ライセンス認証ステータスが評価モードとして表示されます。[Smart Licensing Manager]ページから生成したトークン(このセクションのステップ6)を貼り付けます。次に、[登録]をクリックします。

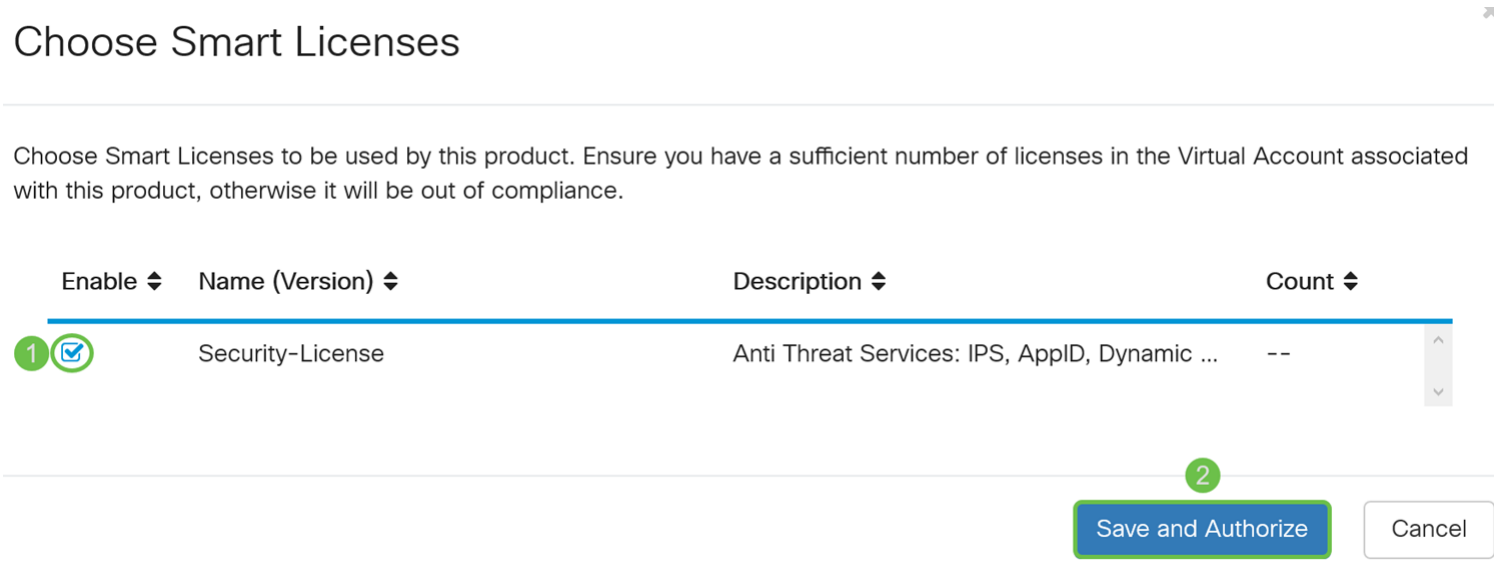
注：登録プロセスに時間がかかる可能性があります。完了するまでお待ちください。



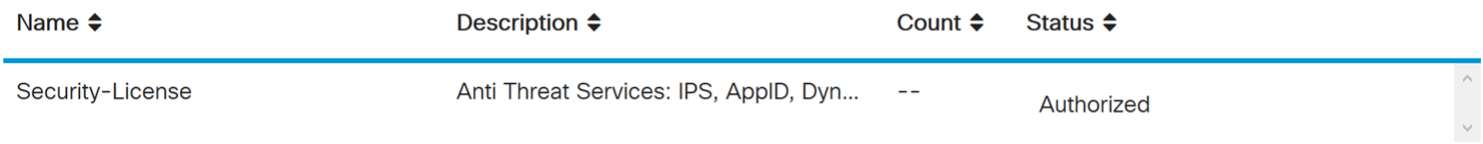
ステップ10：トークンを登録したら、ライセンスを割り当てる必要があります。[ライセンスの選択]ボタンをクリックします。



ステップ11:[スマートライセンスの選択]ウィンドウが表示されます。Security-Licenseを確認し、Save and Authorizeを押します。



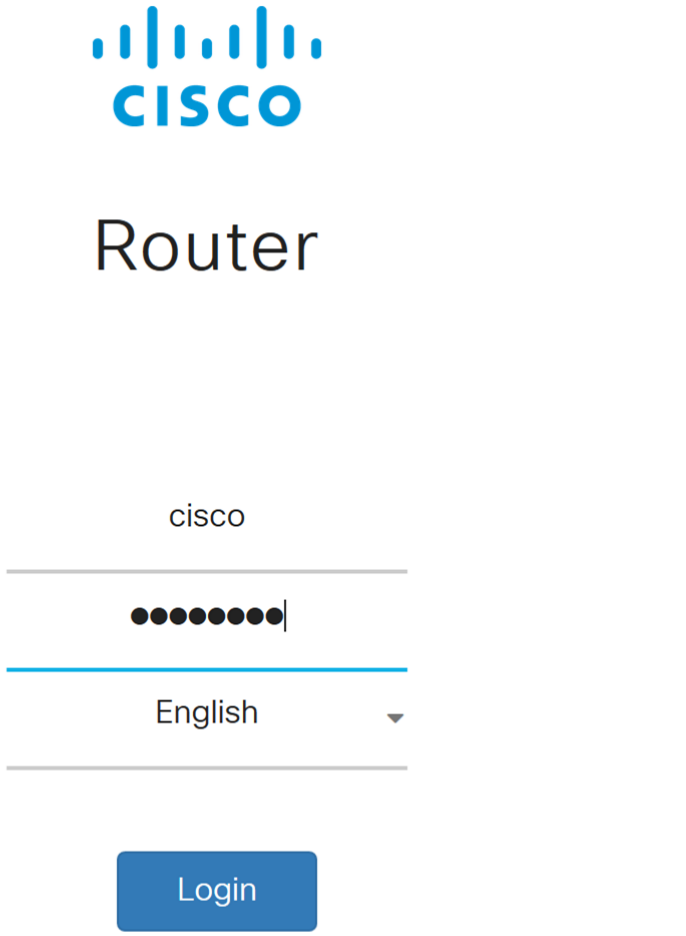
ステップ12：セキュリティライセンスのステータスは、今すぐ*承認され*ます。



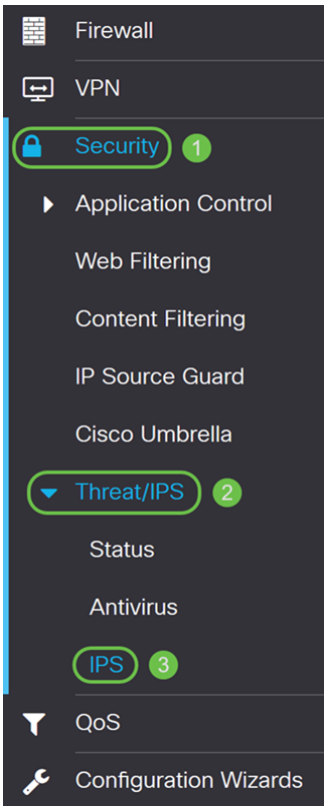
これで、侵入防御システムの設定に進むことができます。

侵入防御システムの設定

ステップ1：まだルータにログインしていない場合は、ルータのWeb設定ページにログインします。

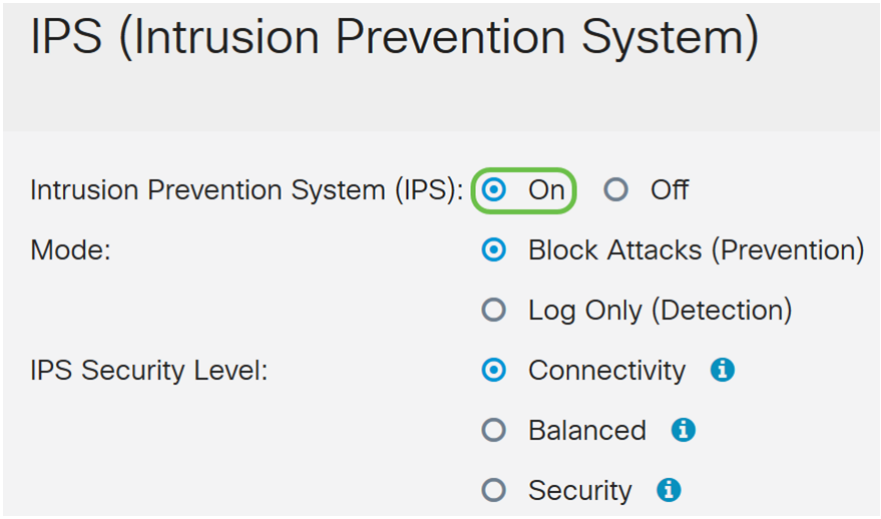


ステップ2:[Security] > [Threat/IPS] > [IPS]に移動します。



ステップ3：侵入防御システム(IPS)機能を有効にするには、[オン(On)]を選択します。オフにするには、[オフ]を選択します。

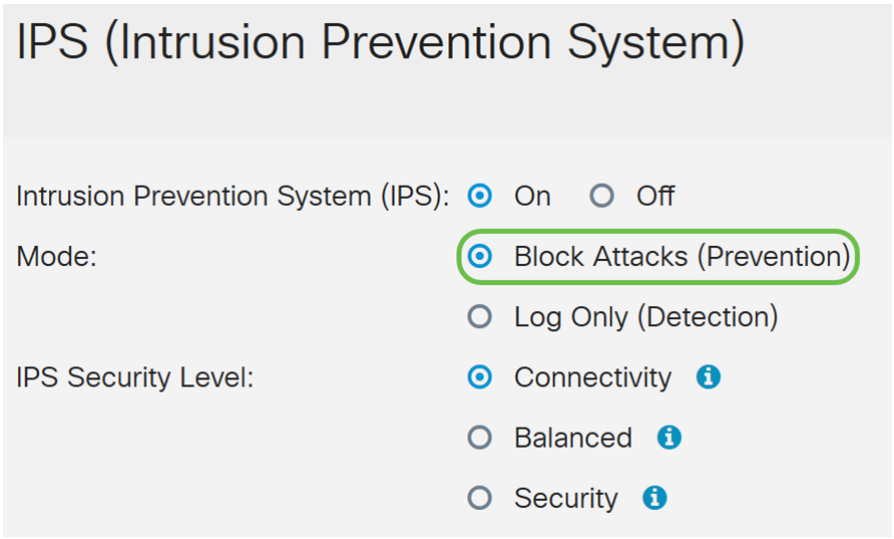
この例ではOnを選択します。



ステップ4:[Block Attacks (Prevention)]または[Log Only]を選択します。この例では、[Block Attacks (Prevention)]を選択します。 次のオプションを定義します。

Block Attacks (Prevention) -すべての攻撃をブロックします。また、異常も記録されます。

Log Only接続には影響しません。



ステップ5：使用するIPSセキュリティレベルを選択します。次のオプションを定義します。

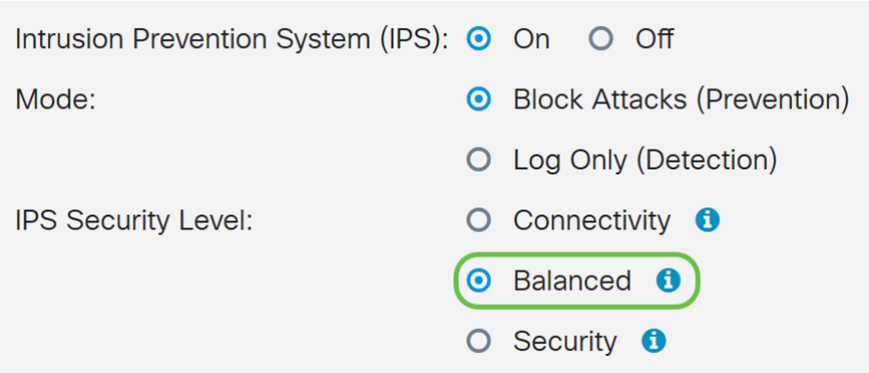
Connectivityこれにより、保護が最小限になります。（重大度が高い）リスク攻撃だけが検出されます。これは最もセキュアでないオプションです。

Balanced – 選択したモードは、重大な攻撃と同時に重大な攻撃を検出します。これは中程度の保護を提供します。（重大度の高+中）は、低リスクのシグニチャを渡すことによって検査されます。これは、IPSの中間レベルのセキュリティです。

セキュリティ：セキュリティモードは、重大および重大な攻撃とともに通常の攻撃を検出します。これにより、最も保護が強化されます。すべてのルール（高+中+低）が検査されます。これは、IPSの最高のセキュリティレベルです。

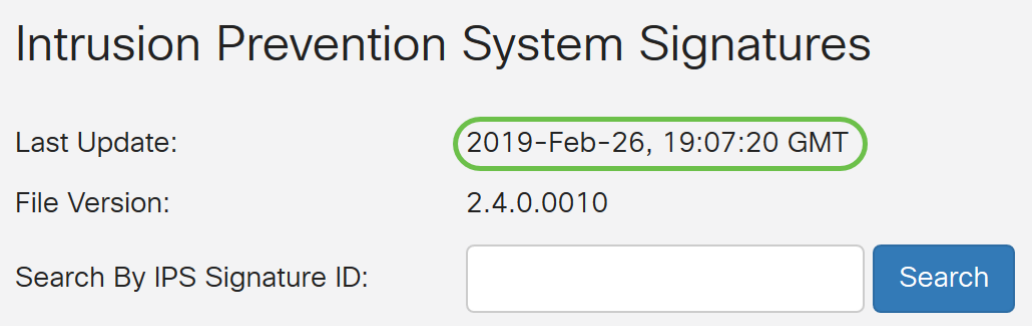
注：選択するセキュリティレベルが高いほど、モニタされる攻撃が多くなるため、システムパフォーマンスへの影響が大きくなります。

このデモンストレーションでは**[Balanced]**を選択します。

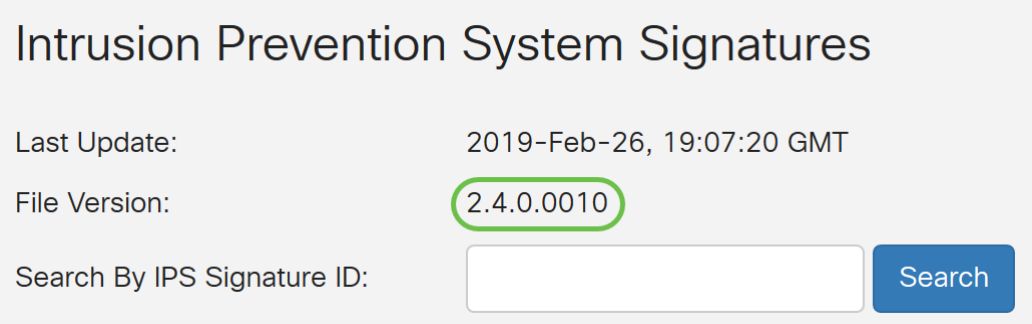


侵入防御システムシグニチャ

ステップ6:[*Last Update*]フィールドに、最後に更新された署名の日時が表示されます。



ステップ7:[ファイルのバージョン*(File Version)*]に、使用されている署名のバージョンが表示されます。



ステップ8：シグニチャIDを検索するには、[*Search by IPS Signature ID*]フィールドにシグニチャ**IDを入力し、**[Search*]をクリックしてシグニチャがサポートされているかどうかを確認します。*シグニチャIDがサポートされている場合、テーブルは次のような結果で更新されます。

注：シグニチャIDがサポートされていない場合、テーブルには何も表示されません。

侵入防御システムのシグニチャテーブル

ステップ9:[*IPS Signature Table*]で、次のフィールドを次のように定義します。

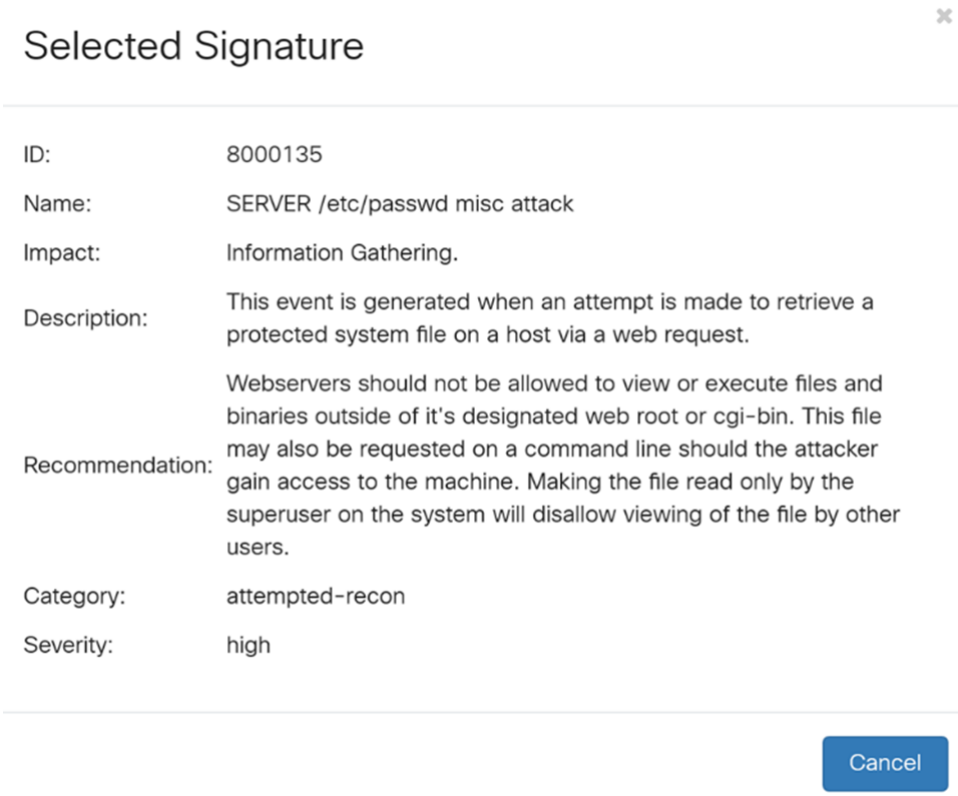
Name

ID：シグニチャの一意の識別子。IDをクリックすると、ウィンドウが開き、選択した署名の詳細が表示されます。

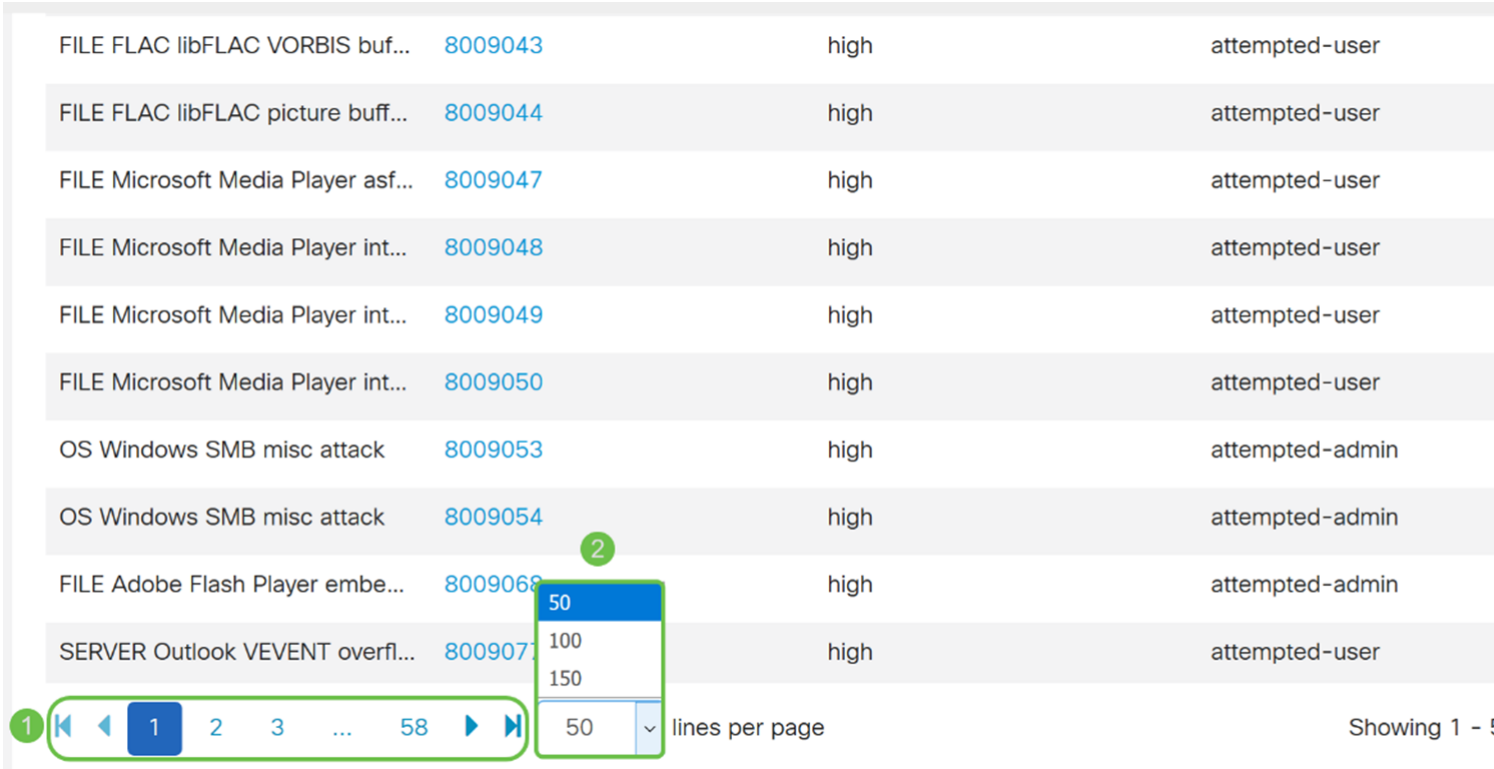
Severity ：重大度はセキュリティへの影響を示します。

Category

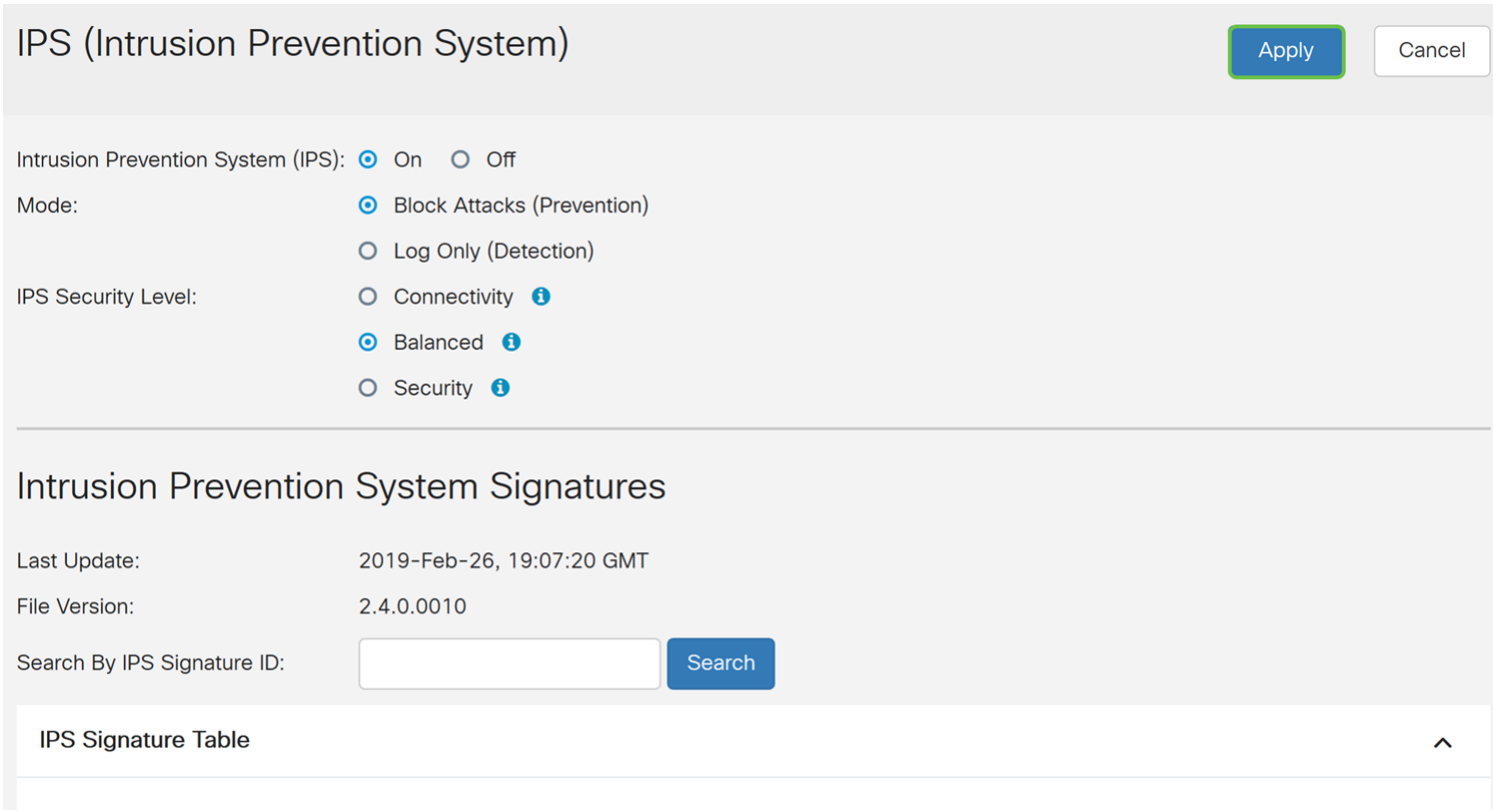
ステップ10:（オプション）*IPSシグニチャテーブルでシグニチャIDをクリックした場合は*、選択したシグニチャの完全な詳細を示すウィンドウが表示されます。



ステップ11:*IPS*シグニチャテーブルの下部で、矢印と番号を選択して、テーブルを前後に移動します。[ページあたりの行数(Lines per page)]ドロップダウンリストで、ページあたりの行数(**50**、**100**、または**150**)を選択することもできます。



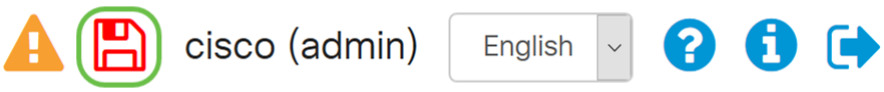
ステップ12:[**Apply**]をクリックして、実行コンフィギュレーションファイルに変更を保存します。



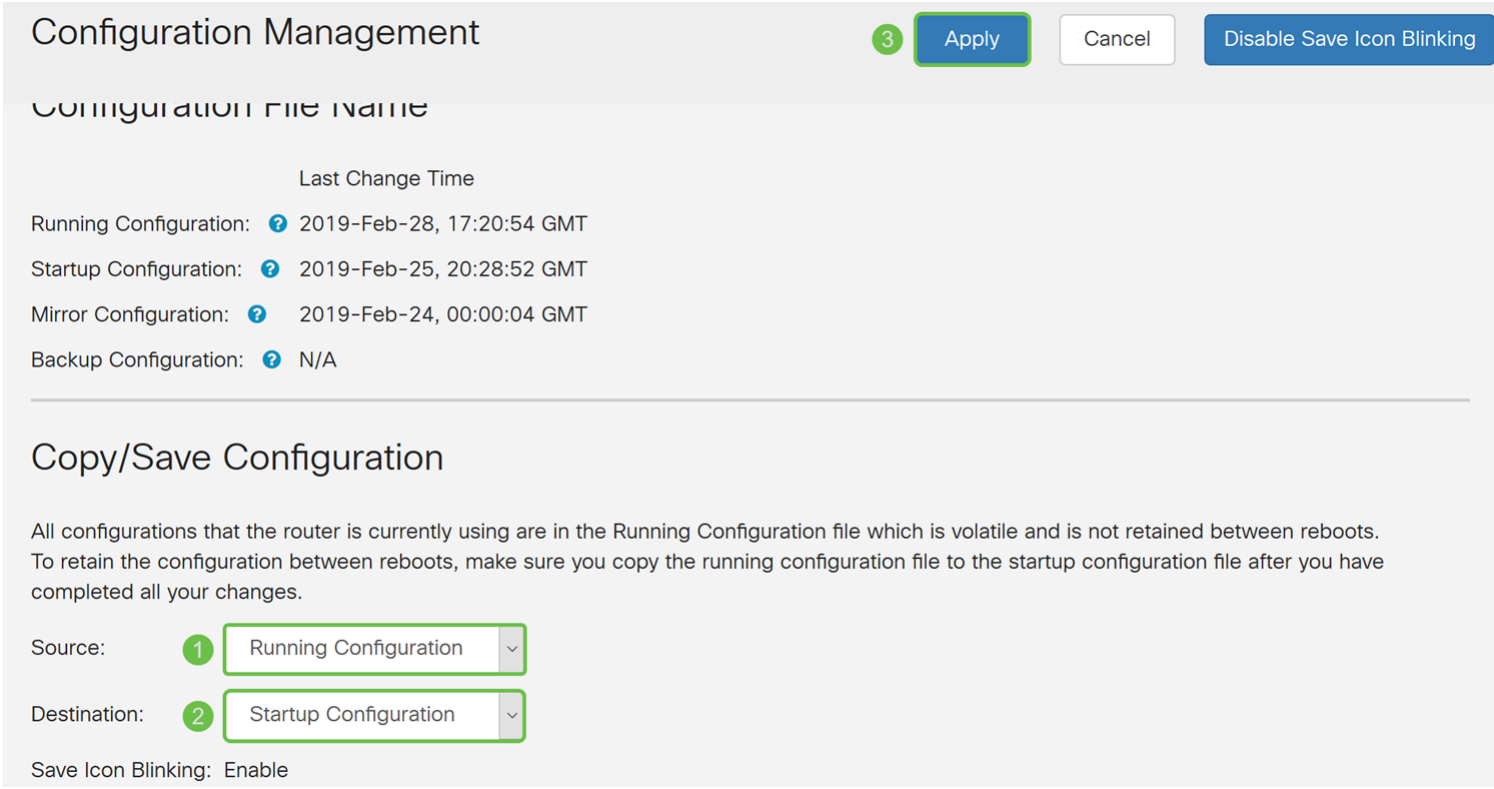
注：ルータが使用しているすべての設定は、現在実行コンフィギュレーションファイルに含まれています。このファイルは揮発性であり、リブートの間は保持されません。リブートの間も設定を保持するには、実行コンフィギュレーションファイルをスタートアップコンフィギュレーションファイルにコピーします。

次のいくつかの手順では、実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーする方法を示します。

ステップ13：ページ上部の**フッピーディスク(保**存)アイコンをクリックします。これにより、[構成管理]にリダイレクトされ、*実行*構成をスタートアップコンフィギュレーションに保存します。

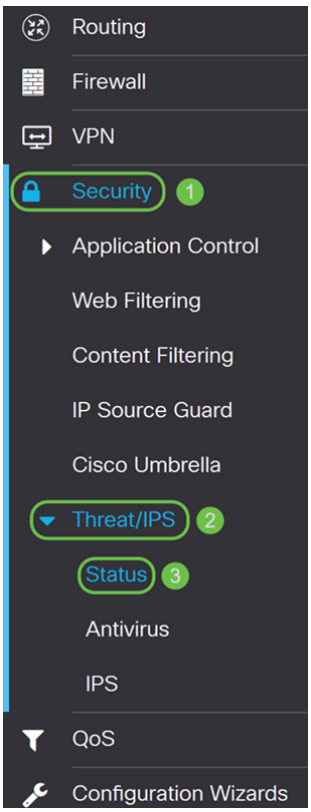


ステップ14:[Configuration Management]で、*[Copy*/Save Configuration]セクション*まで下にスクロール*します。[Source]が[**Running Configuration**]、[*Destination*]が[*Startup Configuration*]**であることを**確認してください。[Apply] をクリックします。これにより、実行コンフィギュレーションファイルがスタートアップコンフィギュレーションファイルにコピーされ、リブート間も設定が保持されます。

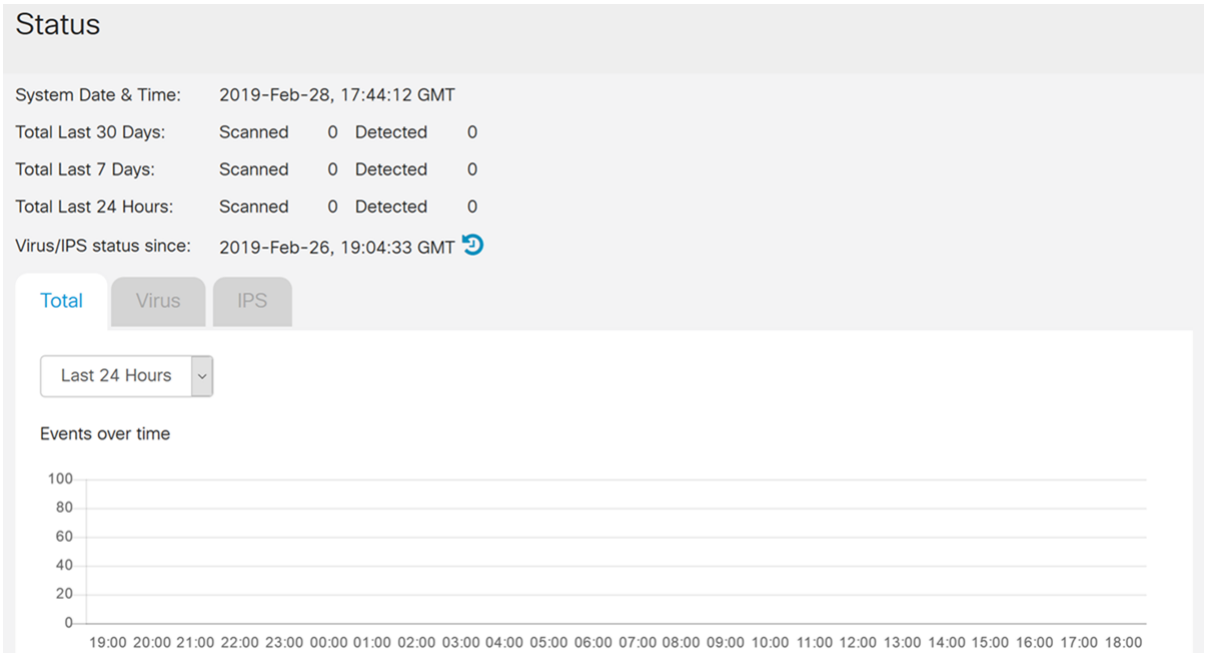


IPSステータス

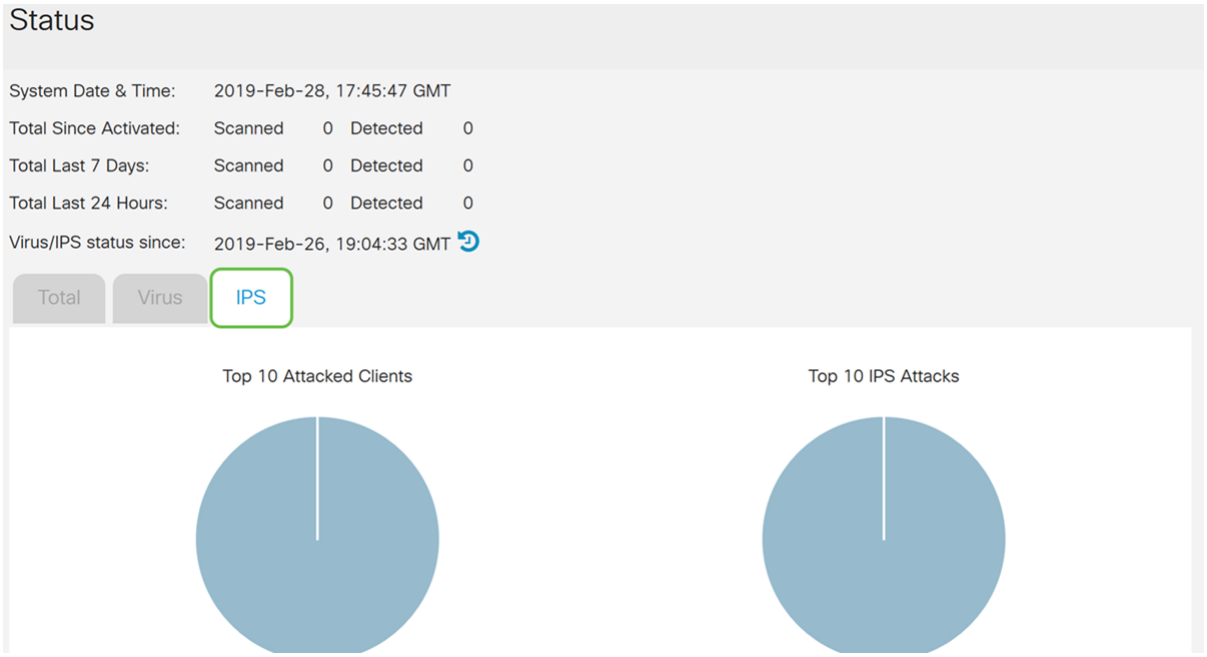
ステップ1:[Security] > **[Threat/IPS] > [Status]に移動します。**



ステップ2:[Status] ページに、脅威と攻撃に対する対策およびIPS機能が設定されている場合の詳細情報が表示されます。ダッシュボードには、イベント全体の概要と、選択した日、週、月ごとに検出された脅威と攻撃の詳細情報が表示されます。



ステップ3:[IPS]タブを**クリック**します。これにより、攻撃を受けたクライアントのトップ10とIPS攻撃のトップ10が表示されます。

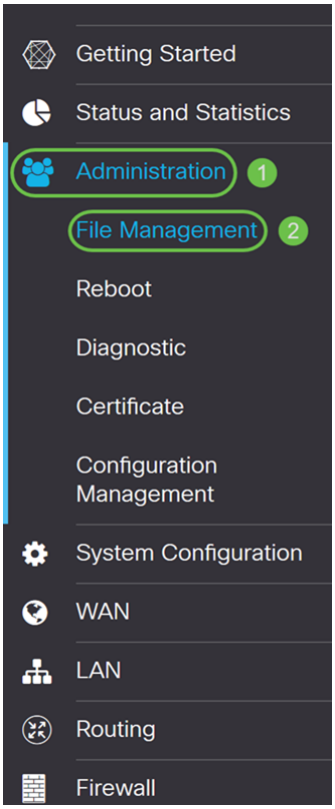


IPS定義の更新

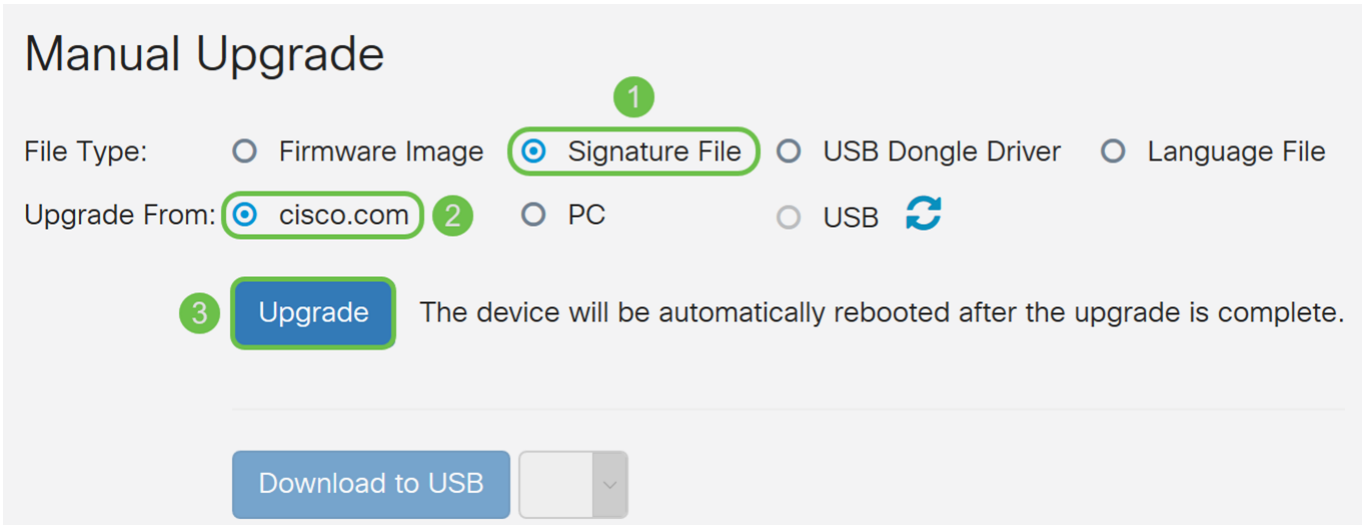
IPS定義は、手動または自動で更新できます。ステップ1 ~ 2ではIPS定義を手動で更新する方法を示し、ステップ3 ~ 6ではIPS定義を自動的に更新する方法を示します。

ベスト プラクティス:セキュリティシグニチャを毎週自動的に更新することをお勧めします。

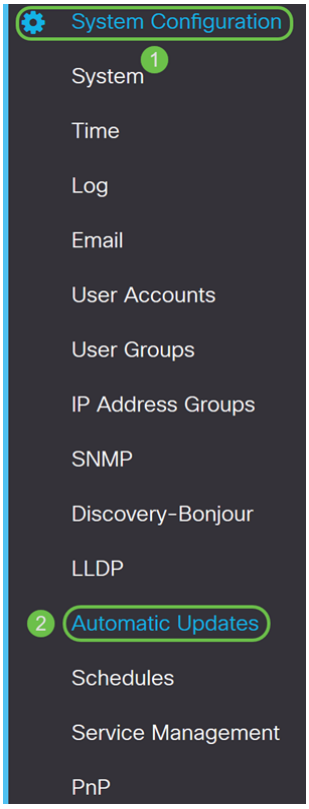
ステップ1:IPS定義を手動で更新するには、**[Administration] > [File Management]に移動します。**



ステップ2:[File Management]ページの[*Manual Upgrade*]セクションまで下にスクロールします。[File Type] に[Signature File] を、[Upgrade From] に[**cisco.com**]を選択します。次に、[アップグレード]を押します。これにより、最新のセキュリティ署名がダウンロードされ、インストールされます。

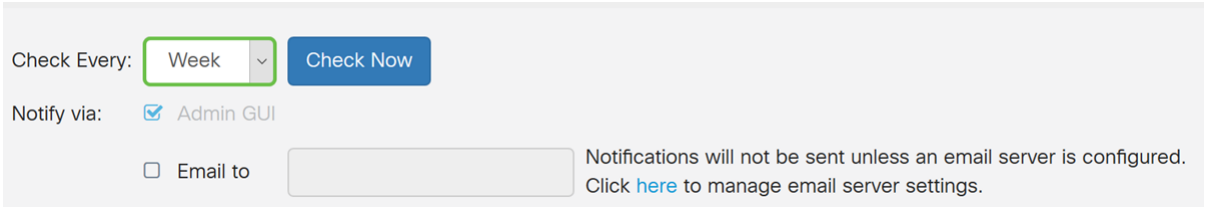


ステップ3:IPS定義を自動的に更新するには、[システムの構成] > [自動更新]に移動します。

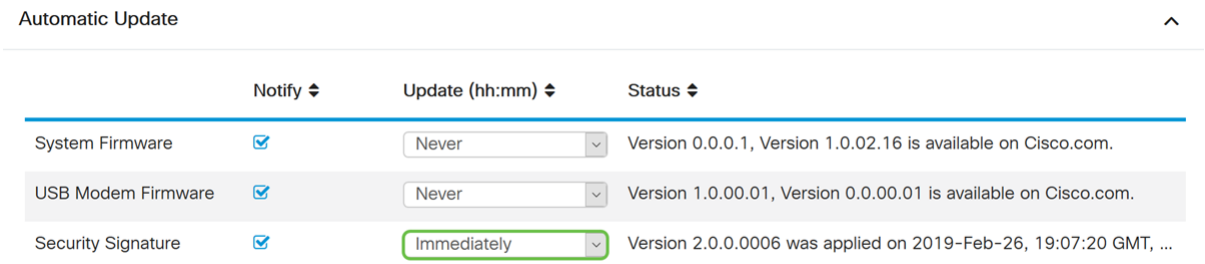


ステップ4:[自動更新]ページが開きます。更新を週ごとまたは月ごとに確認できます。ルータに電子メールまたはWeb UIで通知させることができます。この例では、毎週チェックを選択します。

注：セキュリティシグニチャを毎週自動的に更新することをお勧めします。

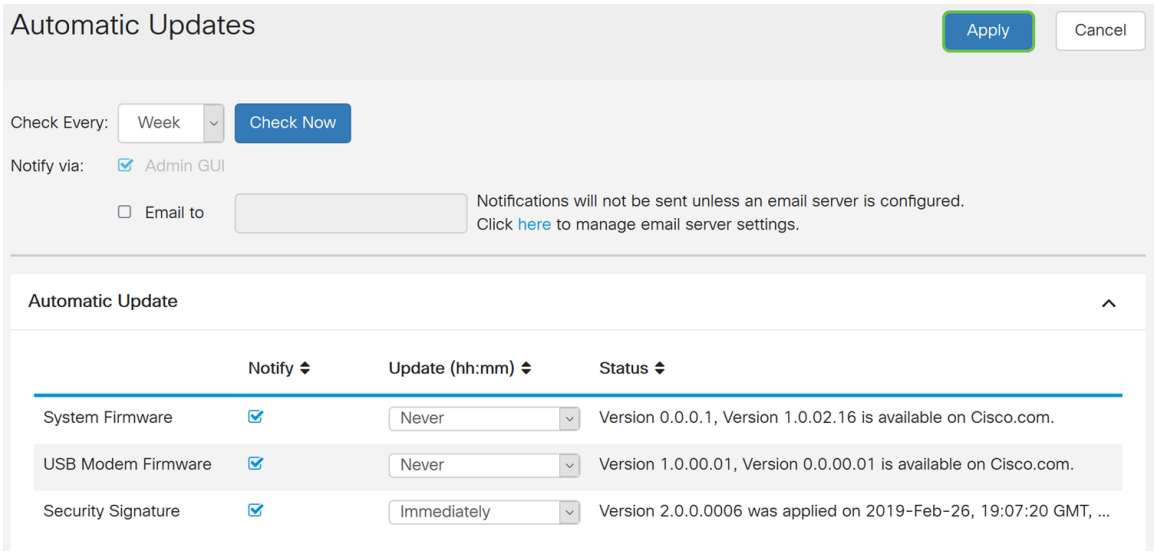


ステップ5:[Automatic Update]セクションまで下にスクロールし、[Security Signature]フィールドを*探*します。[セキュリティ*署名の更新*]ドロップダウンリストで、自動更新する時刻を選択します。この例では、[Immediately]を選択**します**。



ステップ6:[**Apply**]をクリックして、実行コンフィギュレーションファイルに変更を保存します。

注：上の[フロッピーディスク]**アイコンをクリック**して、[構成管理]ページ*に移動*し、実行コンフィギュレーションファイルをスタートアップコンフィギュレーションファイルにコピーしてください。これにより、リブート間の設定が維持されます。



結論

これで、RV34xシリーズルータで侵入防御システム(IPS)が正しく設定されたはずです。