Configurando o sistema de prevenção de intrusão no roteador RV34x Series

Objetivo

O objetivo deste documento é mostrar a você como configurar o Sistema de Prevenção de Intrusão (IPS - Intrusion Prevention System) em roteadores da série RV34x.

Introduction

O sistema de prevenção de intrusão verifica o tráfego para procurar padrões de ataque conhecidos para bloquear. Ele observa pacotes e sessões à medida que fluem pelo roteador e verifica cada pacote para corresponder a qualquer uma das assinaturas do Cisco IPS. Quando detecta atividades suspeitas, é concebido para registrar ou bloquear a atividade. É importante atualizar as definições e os bancos de dados de IPS e antivírus. Eles podem ser atualizados manual ou automaticamente.

Confira estes vídeos no Cisco Intrusion Prevention System:

No entanto, o IPS pode afetar o desempenho do roteador. Em geral, não afeta o throughput total para o tráfego HTTP e FTP, mas pode diminuir drasticamente o número máximo de conexões simultâneas.

Nota importante: Se o roteador estiver atualmente sob uma carga de trabalho pesada, isso pode exacerbar o problema.

A tabela abaixo fornece as estatísticas esperadas para o desempenho em várias configurações. Esses valores devem ser usados como um guia, pois o desempenho real pode variar devido a vários fatores.

	Conexões simultâneas	Taxa de conexão	throughput de HTTP	throughput de FTP
Configurações padrão	40000	3000	982 MB/s	981 MB/s
Habilitar controle de APP	15000-16000	1300	982 MB/s	981 MB/s
Ativar antivírus	16000	1500	982 MB/s	981 MB/s
Habilitar IPS	**17000**	**1300**	**982 MB/s**	**981 MB/s**
Ativar antivírus e IPS de controle de aplicativos	15000-16000	1000	982 MB/s	981 MB/s

Os seguintes campos são definidos como:

Conexões simultâneas - O número total de conexões simultâneas. Por exemplo, se você estiver fazendo download de um arquivo de um site, essa é uma conexão, fazendo a transmissão de áudio do Spotify que será outra conexão, fazendo duas conexões simultâneas.

Connection Rate - O número de conexões solicitadas por segundo que podem ser processadas.

Throughput de HTTP/FTP - O throughput de HTTP e FTP são as taxas de download em MB/s.

As licenças de segurança foram atualizadas para incluir a proteção IPS, além da aplicação existente e da filtragem da Web. Uma Smart Account é necessária para ter uma licença de segurança. Se você ainda não tiver uma Smart Account ativa, a seção 1 deste documento será obrigatória.

Para saber como configurar o Antivírus no RV34x, clique aqui.

Dispositivos aplicáveis

- RV34x

Versão de software

- 1.0.03.x

Table Of Contents

Licenciamento inteligente

Se você não tiver uma Smart Account ativa, será necessário prosseguir com as etapas

abaixo.

Se você tiver problemas ou problemas ao configurar sua conta do Smart License, nossa equipe de suporte ajudará a resolver possíveis problemas e poderá ser encontrada por meio de vários métodos. Sinta-se à vontade para usar seu método preferido para sair.

- **Comunidade do roteador:** Comunidade de suporte Cisco Small Business

- **Perguntas frequentes sobre o RV34x Series:** Perguntas frequentes do roteador RV34x Series

- **Visão geral da Smart License:** Licenciamento de software inteligente

- **Perguntas frequentes sobre Smart Licenses:** Perguntas frequentes sobre Smart Licensing e Smart Accounts para parceiros, distribuidores e clientes

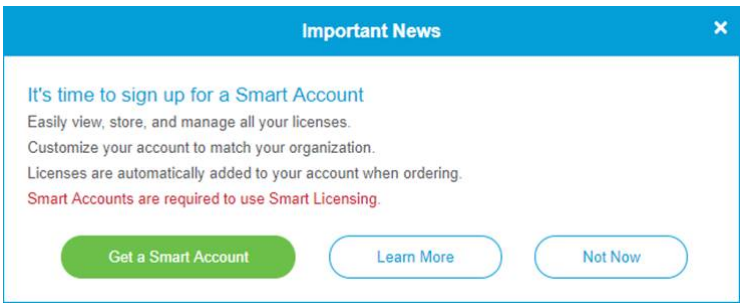
- **Envie um caso:** Support Case Manager

Número de telefone do suporte dos EUA/Canadá: 1-866-606-1866 ou Contatos do TAC para pequenas empresas

E-mail de licenciamento: licensing@cisco.com

Etapa 1. Se você criou ou visitou sua conta do Cisco.com recentemente, uma mensagem é recebida por você para criar sua própria conta Smart License. Caso contrário, você pode clicar aqui para ser levado à página de criação de conta da Smart License. Talvez seja necessário fazer login.

Note: Para obter mais detalhes sobre as etapas envolvidas na solicitação de sua Conta inteligente, clique aqui.



Etapa 2. Ao comprar uma licença inteligente para um roteador, o fornecedor precisa fazer um processo que mova a ID de licença exclusiva para sua conta do Smart License. A tabela a seguir contém as informações necessárias que serão solicitadas ao comprar os pacotes.

Note: IPS e antivírus fazem parte da licença de segurança usada para filtragem da Web e filtragem de aplicativos.

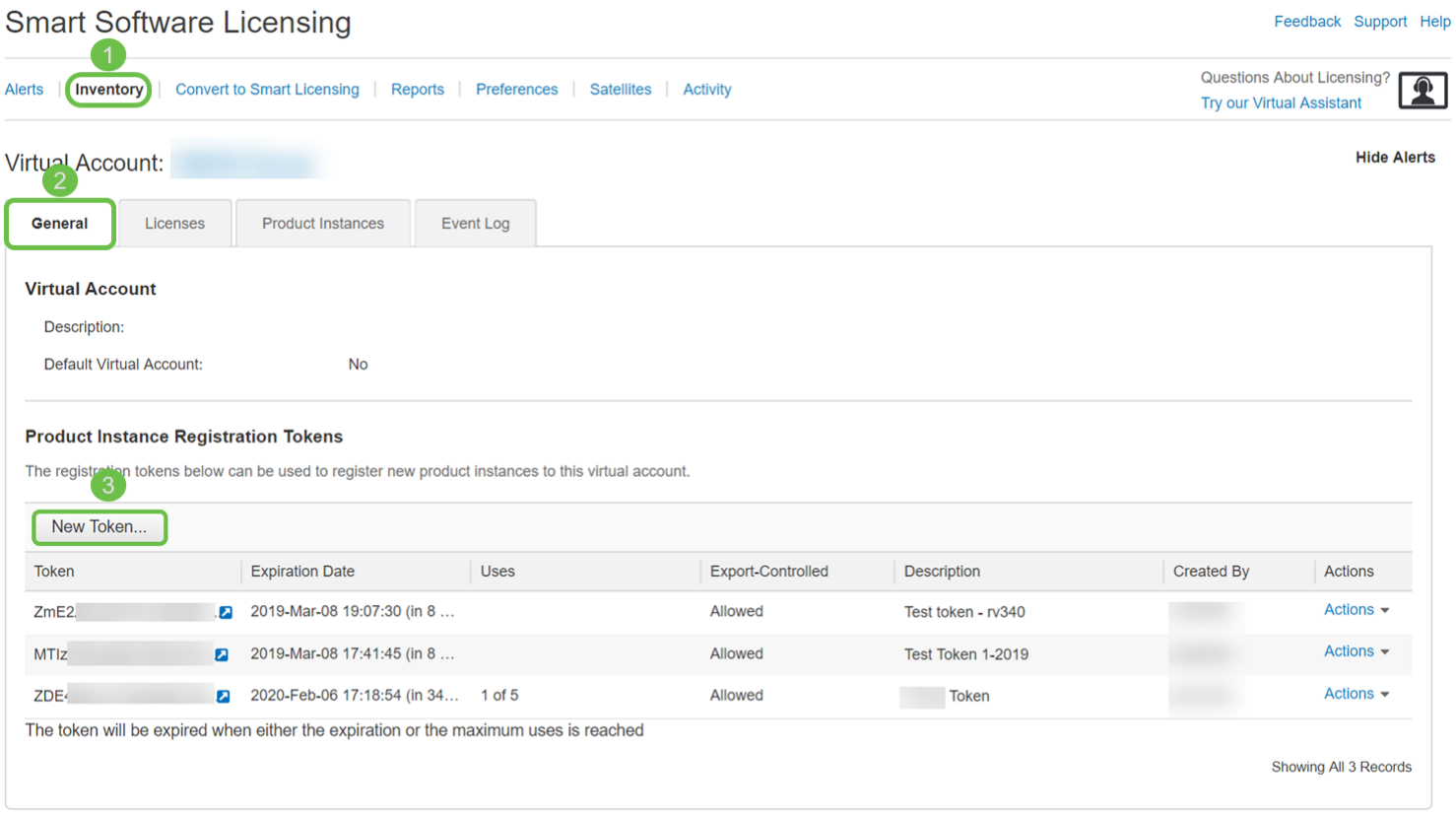
Informações necessárias	Localização das informações
ID de usuário do Cisco.com	Localizado no perfil da sua conta ou clique aqui.
Nome da Conta de Licença Inteligente	É melhor ter criado sua Smart Account antes de adquirir a licença. Esta

	deve ser a etapa 8 do artigo Criação de Smart License Account.
SKU de Smart License	O código de identificação do produto do dispositivo. Ex. RV340-K9-NA

Note: Se você adquiriu uma licença e ela não está aparecendo em sua conta virtual, você deve acompanhar o revendedor para solicitar que ele faça a transferência ou entre em contato conosco.

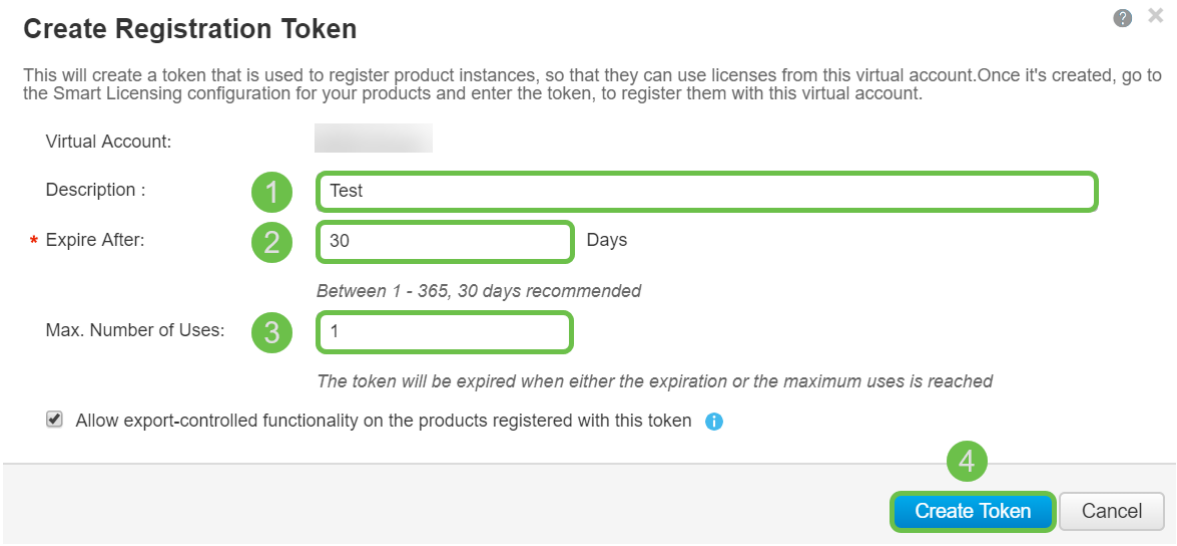
Para tornar o processo o mais rápido possível, você deve ter sua fatura de licença, o número do pedido de vendas da Cisco e uma captura de tela da sua página de licença da Smart Account (para compartilhar com nossa equipe).

Etapa 3. Para gerar um token, navegue até sua conta Smart Software License. Em seguida, clique em **Inventário > guia Geral**. Clique no botão **Novo token...**.

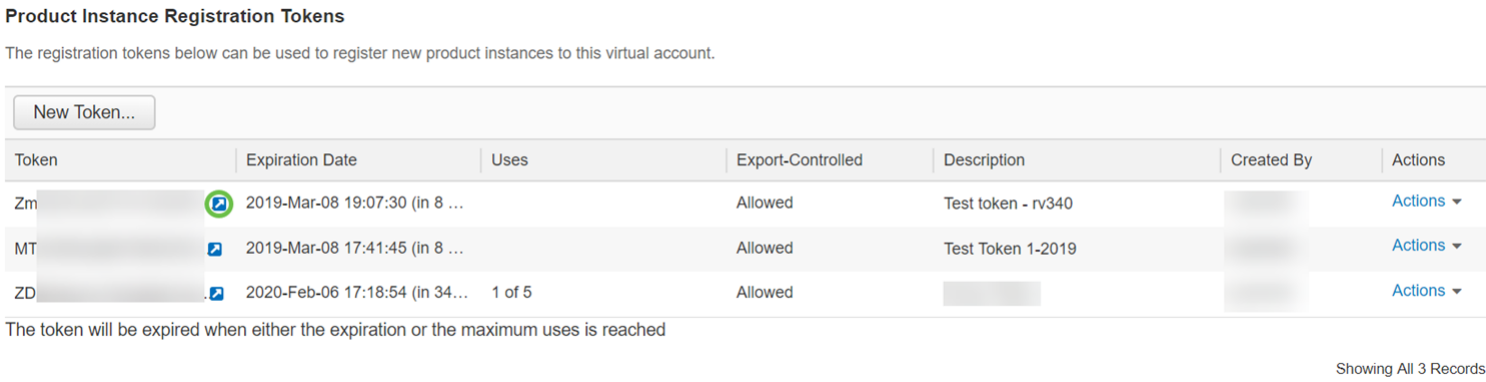


Etapa 4. Uma janela *Create Registration Token* é aberta. Insira uma *Descrição*, *Expirar Depois* e *Máx. Número de usuários*. Em seguida, pressione o botão **Create Token (Criar token)**.

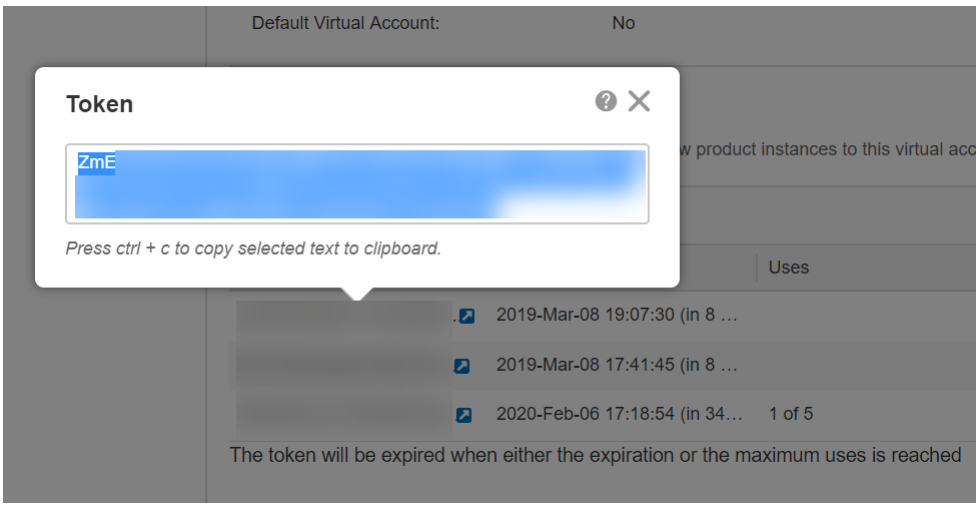
Note: 30 dias para *Expirar Depois* é recomendado.



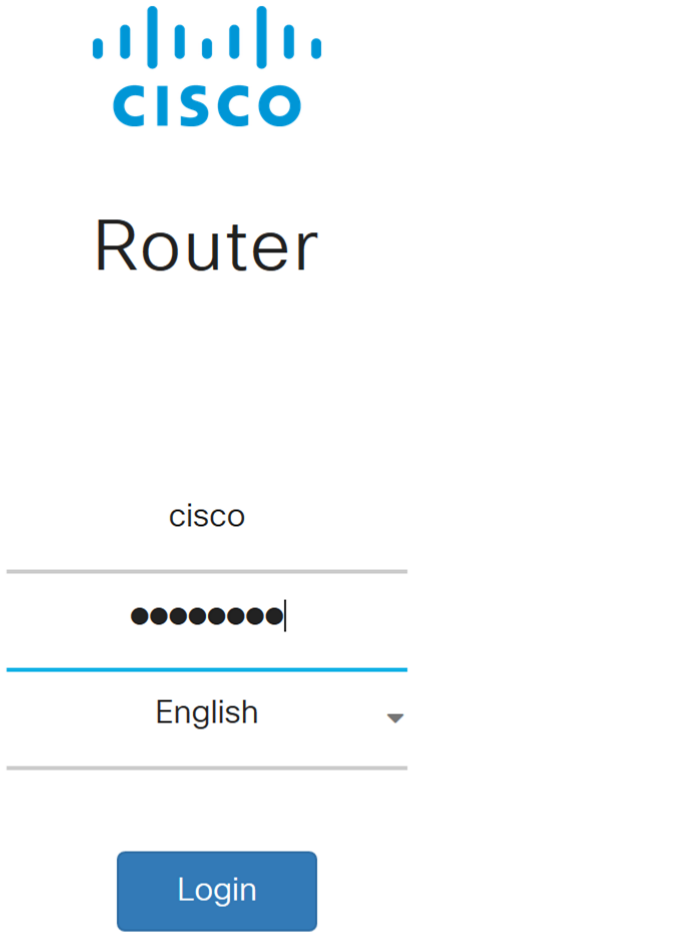
Etapa 5. Depois que o token for gerado, você poderá clicar no **link Token (caixa azul com uma seta branca)** à direita do token recém-criado.



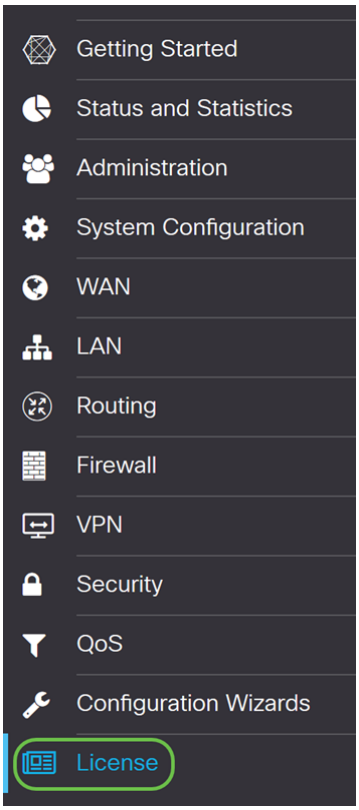
Etapa 6. Uma janela *Token* deve aparecer com o token completo para você copiar. Realce o token, clique com o botão direito do mouse no token e clique em **Copiar** ou mantenha pressionado o botão **ctrl** no teclado e clique em **c** ao mesmo tempo para copiar o texto.



Passo 7. Depois de copiar o token, você precisará fazer login no dispositivo e carregar a chave do token. Faça login na página de configuração da Web do roteador.

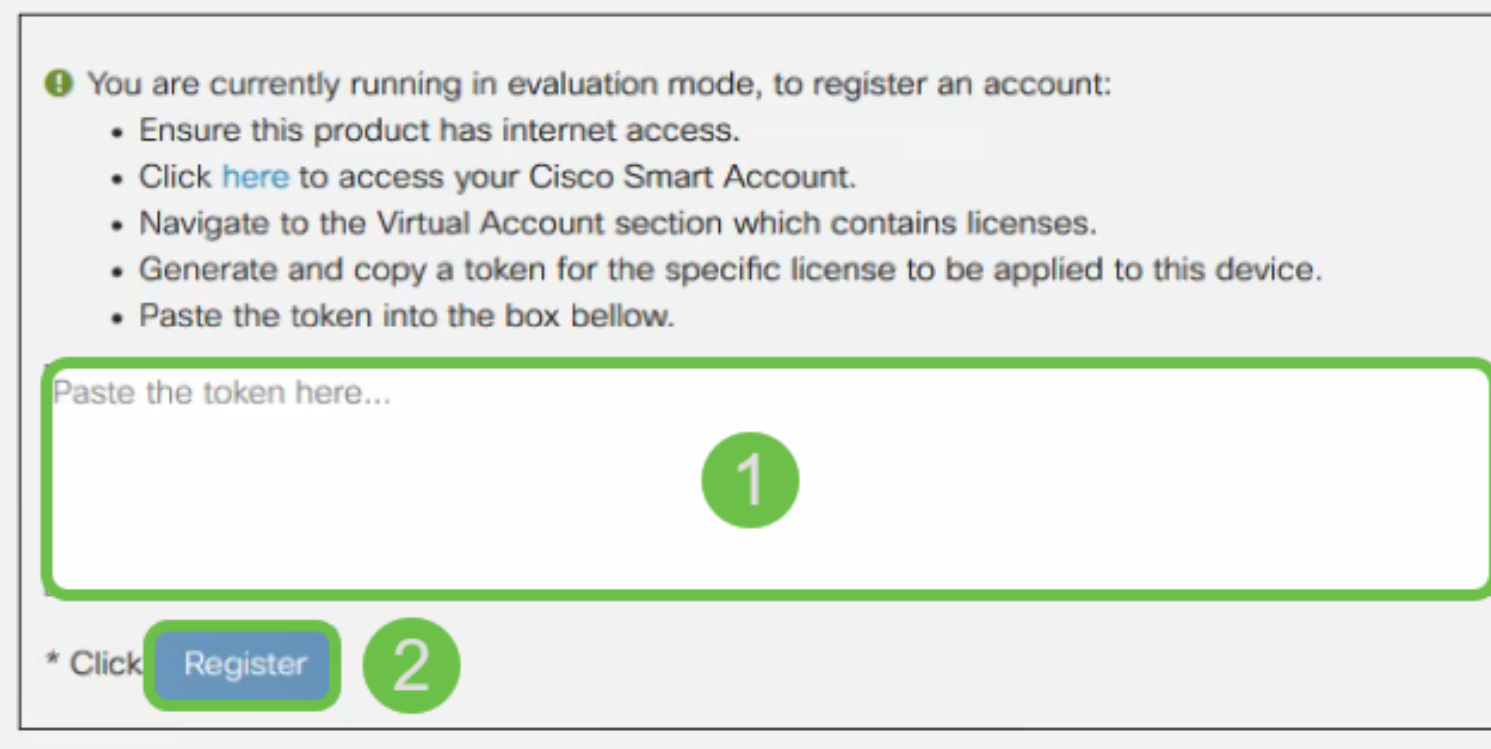


Etapa 8. Navegue até **Licença.**

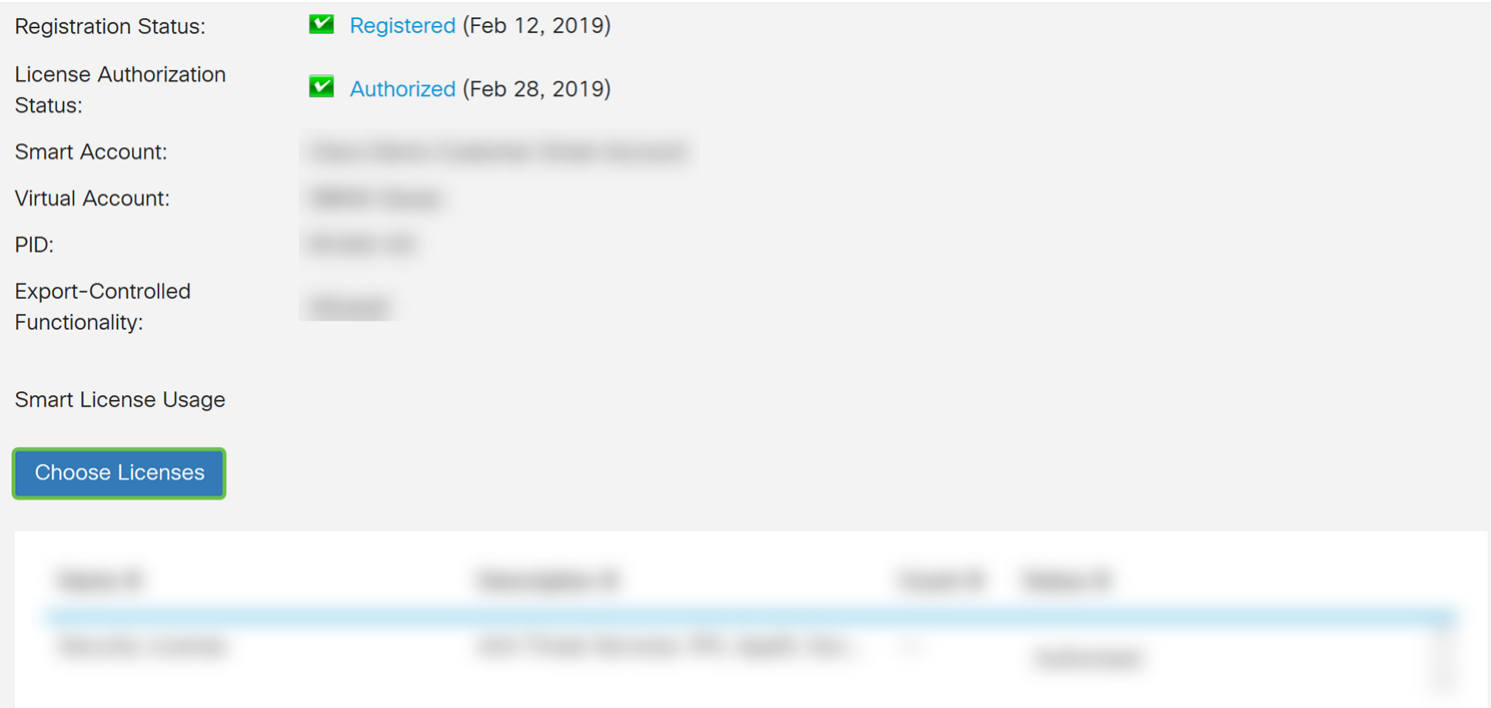


Etapa 9. Se o seu dispositivo não estiver registrado, o seu *Status de autorização de licença* será listado como *Modo de avaliação*. Cole o token (Etapa 6 desta seção) que você gerou na página *Smart Licensing Manager*. Em seguida, clique em **Registrar**.

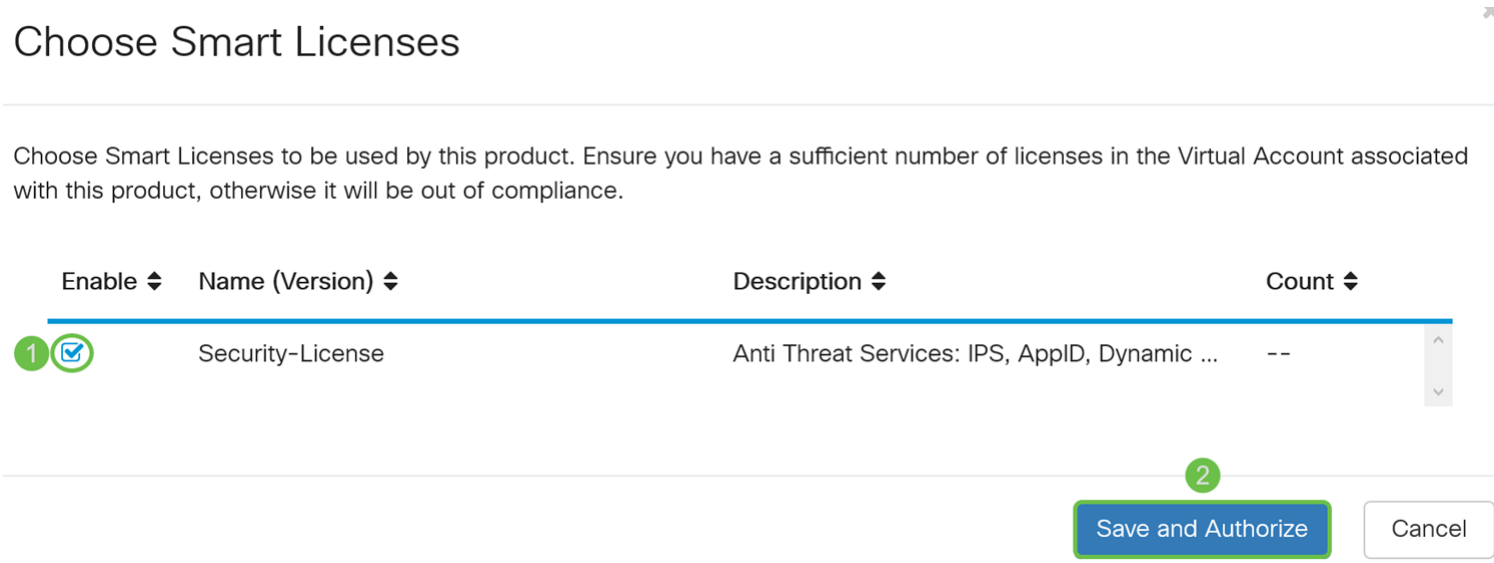
Note: O processo de registro pode levar algum tempo. Aguarde a conclusão.



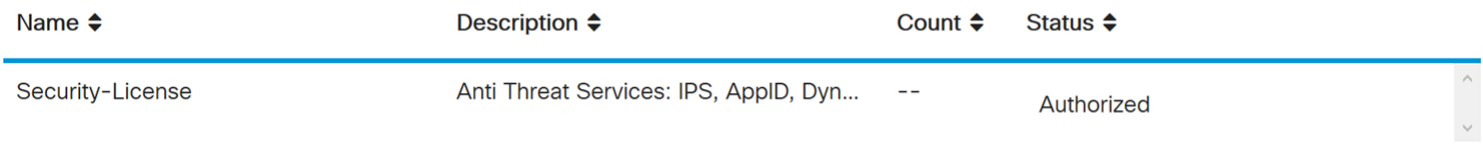
Etapa 10. Depois que o token for registrado, você precisará alocar a licença. Clique no botão **Escolher licenças**.



Etapa 11. A janela *Choose Smart Licenses (Escolher Smart Licenses)* será exibida. Verifique a **Licença de segurança** e pressione **Salvar e autorizar**.



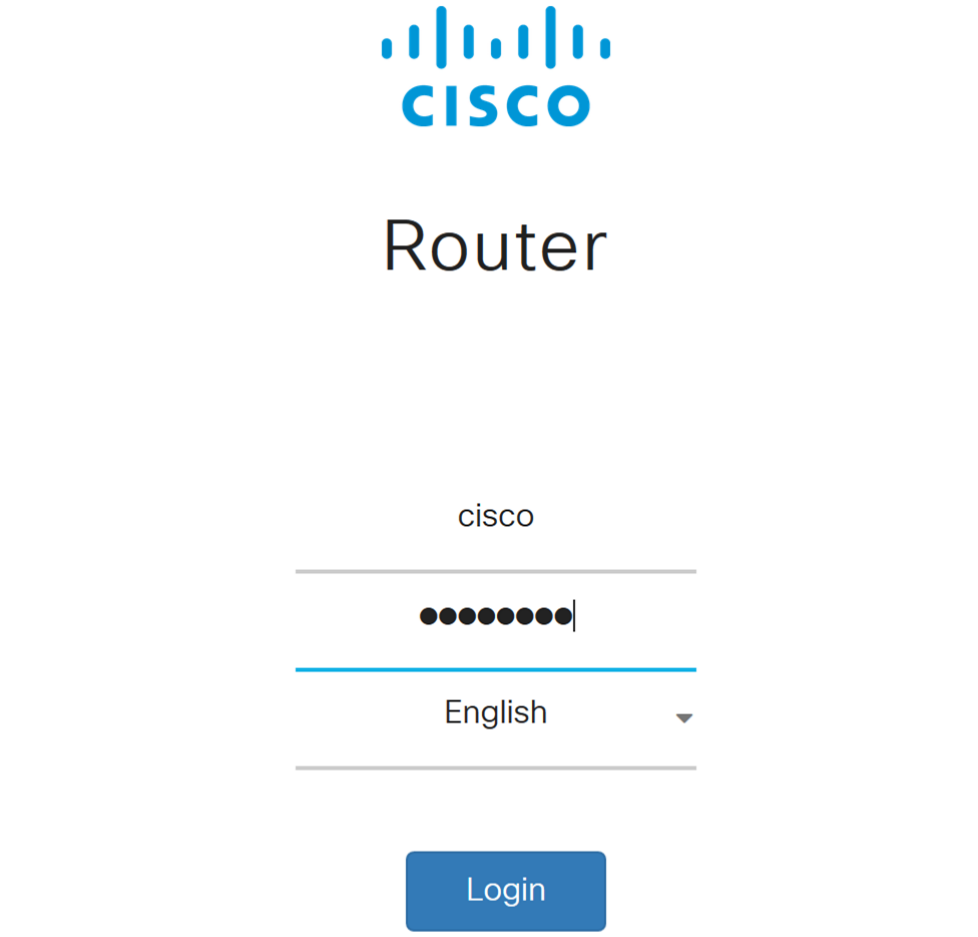
Etapa 12. O *Status* da Licença de Segurança deve ser *Autorizado* agora.



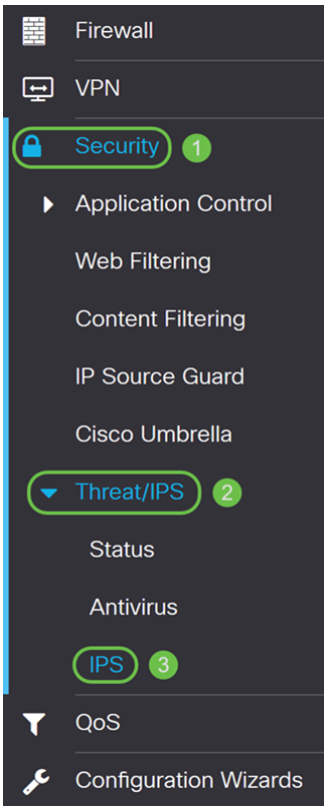
Agora você pode continuar a configurar o Sistema de prevenção de intrusão.

Configurando o sistema de prevenção de intrusão

Etapa 1. Se você ainda não fez login no roteador, faça login na página de configuração da Web do roteador.

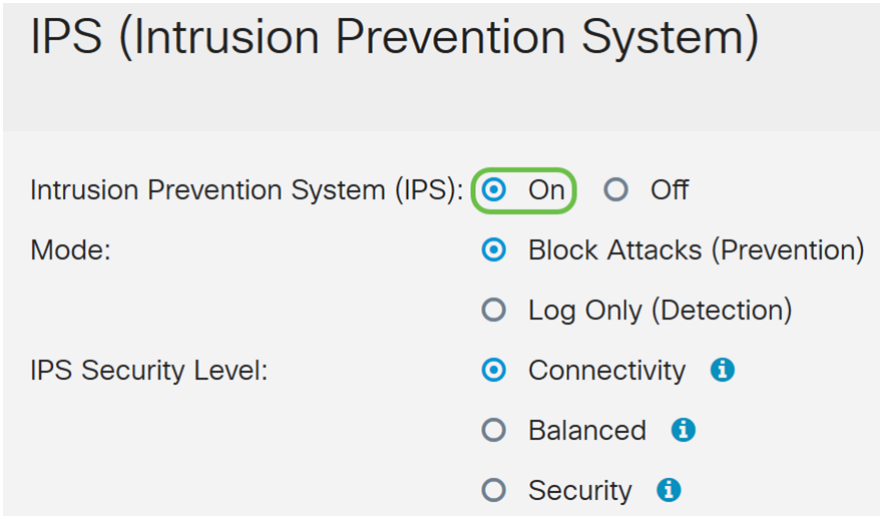


Etapa 2. Navegue até **Security > Threat/IPS > IPS**.



Etapa 3. Selecione **On** para habilitar o recurso Intrusion Prevention System (Sistema de prevenção de intrusão). Se quiser desligá-lo, selecione **Desligar**.

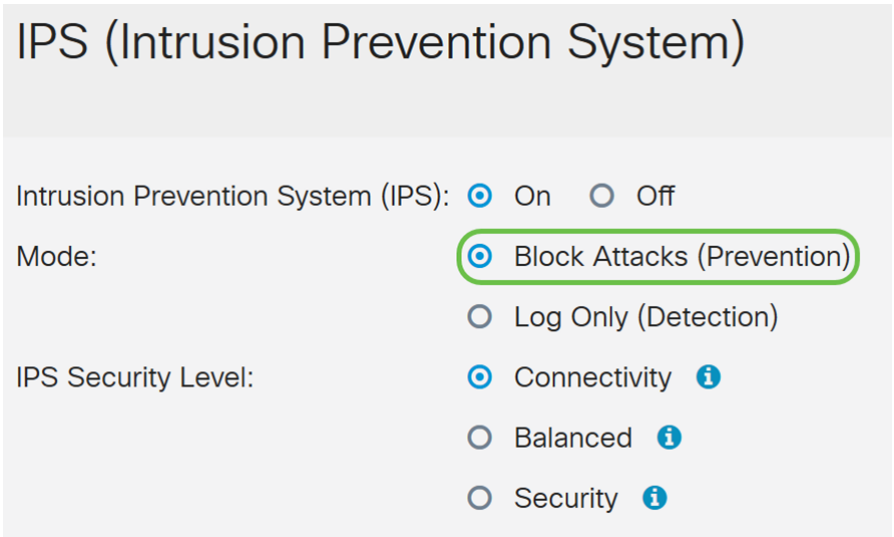
Vamos selecionar **On** neste exemplo.



Etapa 4. Selecione **Bloquear ataques (Prevenção)** ou **Somente registro**. Neste exemplo, selecionaremos **Bloquear Ataques (Prevenção)**. As opções a seguir estão definidas abaixo.

. **Bloquear ataques (Prevenção)** - Selecione para bloquear todos os ataques. Também registra a anomalia.

• **Log Only** - Essa opção gerará o log somente (com informações do cliente, ID de assinatura, etc.) quando as anomalias forem identificadas. Isso não afeta a conexão.



Etapa 5. Selecione o nível de segurança de IPS que deseja usar. As seguintes opções são definidas como:

• **Connectivity** - Este modo detectará os ataques mais críticos. Isso proporciona a menor proteção: somente ataques de risco (alta gravidade) são detectados. Esta é a opção menos segura.

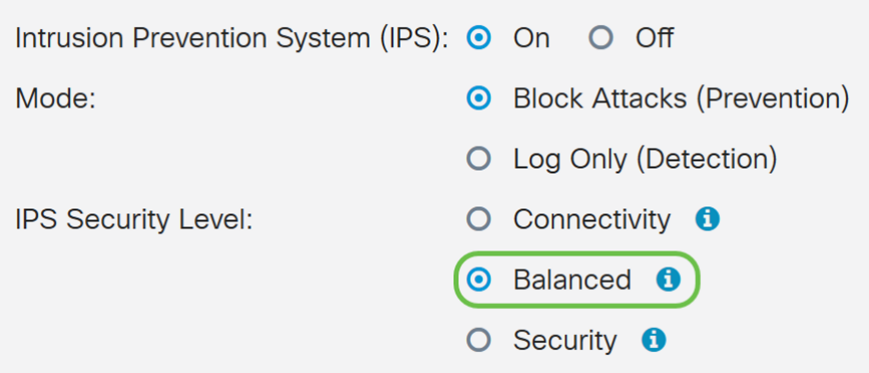
• **Equilibrado** - O modo selecionado detectará ataques graves juntamente com os ataques críticos. Isso fornece proteção de meio: (severidade alta + média) são inspecionadas, passando assinaturas de baixo risco. Essa é a segurança de nível intermediário para IPS.

. **Segurança** - O modo de segurança detectará os ataques normais, juntamente com os

ataques graves e críticos. Isso proporciona a maior proteção: Todas as regras (alta + média + baixa gravidade) são inspecionadas. Esse é o mais alto nível de segurança para IPS.

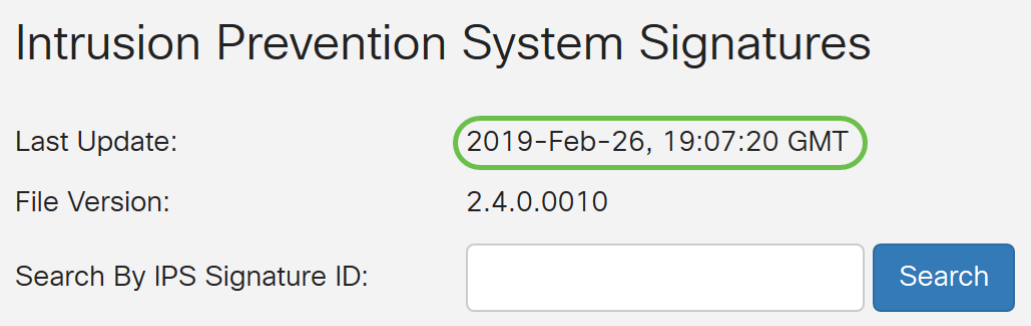
Note: Quanto maior o nível de segurança escolhido, mais ataques serão monitorados, maior será o impacto no desempenho do sistema.

Vamos selecionar **Equilibrado** para esta demonstração.

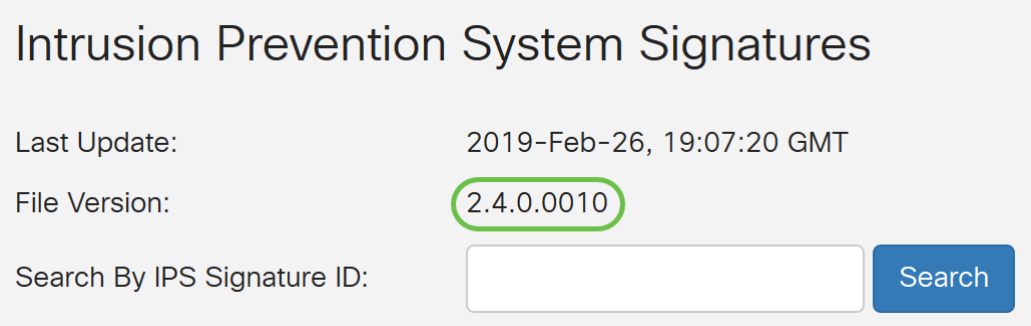


Assinaturas do sistema de prevenção de intrusão

Etapa 6. No campo *Última atualização*, ele exibirá a data e a hora da última assinatura atualizada.



Passo 7. A *versão do arquivo* exibe a versão da assinatura que está sendo usada.



Etapa 8. Para procurar um ID de assinatura, digite o **ID de assinatura** no campo *Pesquisar por ID de assinatura IPS* e clique em **Pesquisar** para verificar se a assinatura é suportada ou não. Se o ID de assinatura for suportado, a tabela será atualizada com o resultado como mostrado abaixo.

Note: Se o ID de assinatura não for suportado, nada aparecerá na tabela.

Tabela de assinatura do sistema de prevenção contra intrusão

Etapa 9. Na *Tabela de assinatura IPS*, os campos a seguir são definidos como:

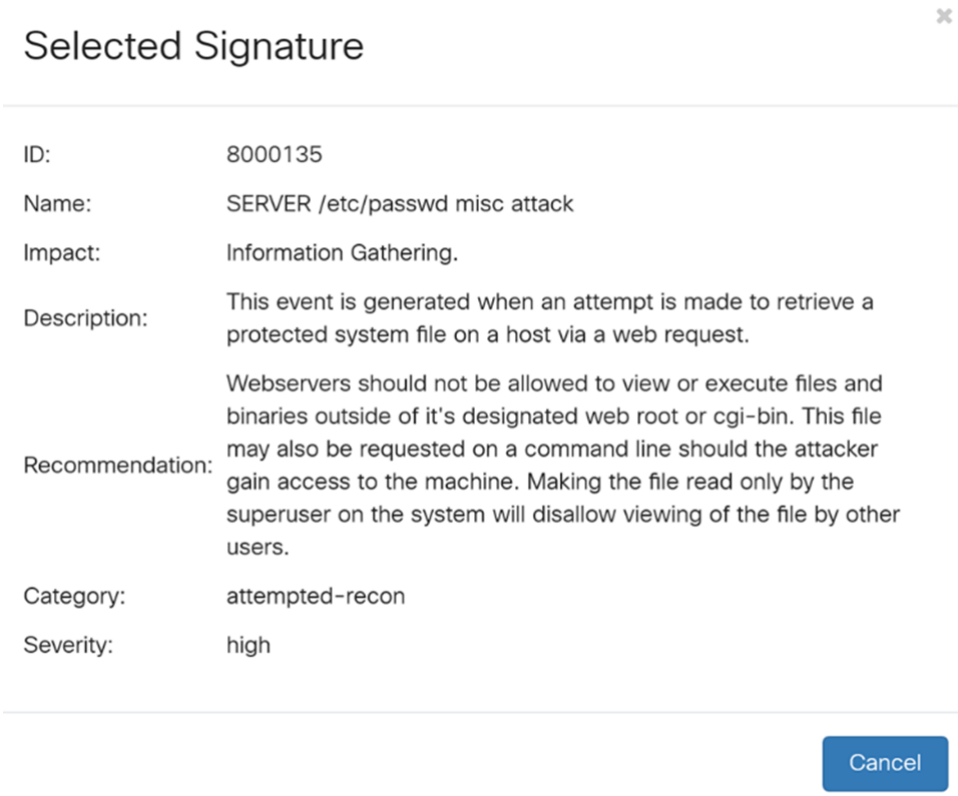
- **Nome** - Nome da assinatura.

. **ID** - O identificador exclusivo da assinatura. Clicar na ID abrirá uma janela para que você veja os detalhes completos da assinatura selecionada.

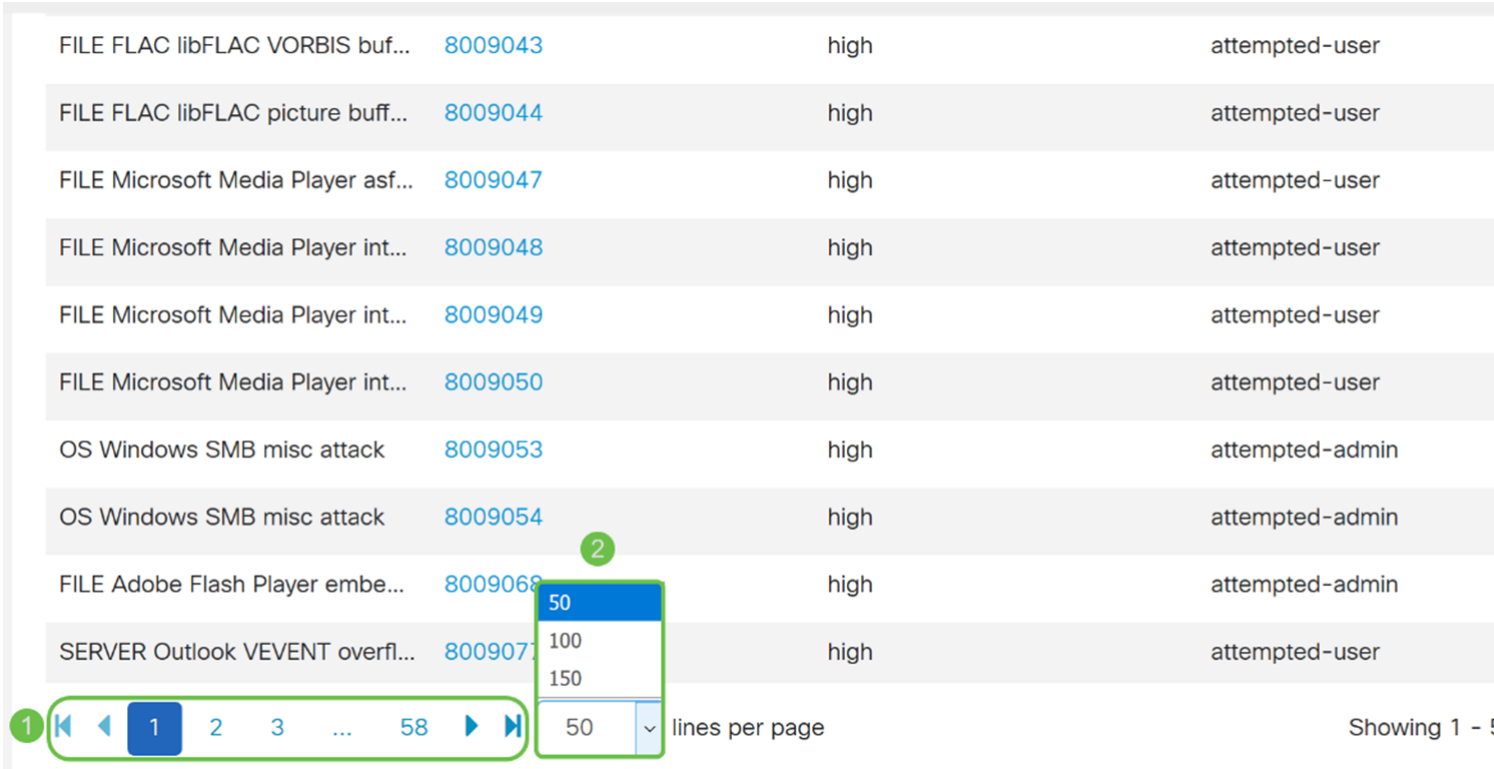
- **Gravidade** - O nível de gravidade indica o impacto na segurança.

- **Categoria** - A categoria à qual a assinatura pertence.

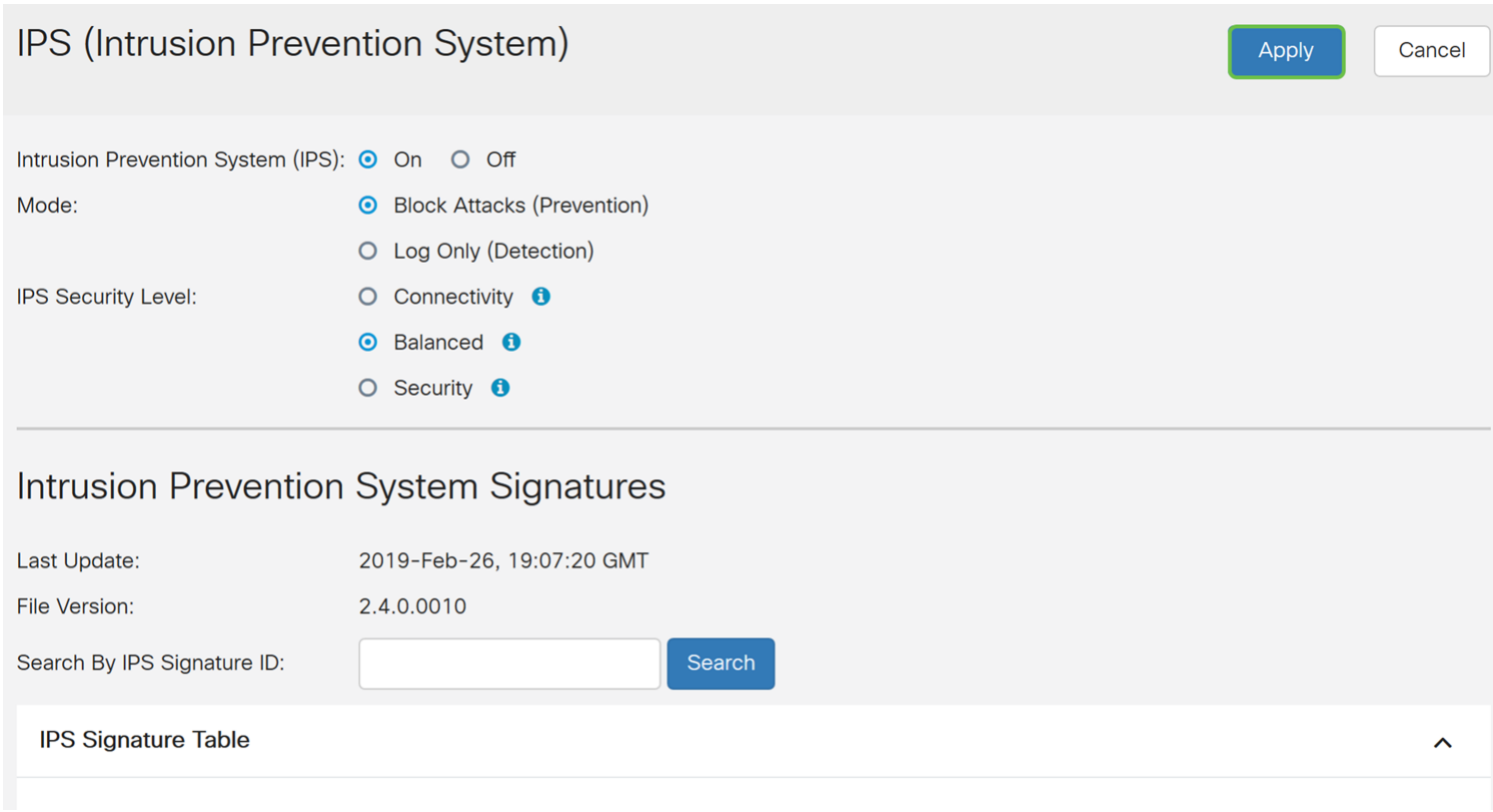
Etapa 10. (Opcional) Se você clicou na ID de assinatura na *Tabela de assinatura IPS*, uma janela será exibida para mostrar a você os detalhes completos da assinatura selecionada.



Etapa 11. Na parte inferior da *Tabela de assinatura IPS*, selecione as setas assim como os números para navegar para frente e para trás na tabela. Você também pode selecionar a quantidade de linhas (**50**, **100** ou **150**) por página na *lista suspensa* por página.



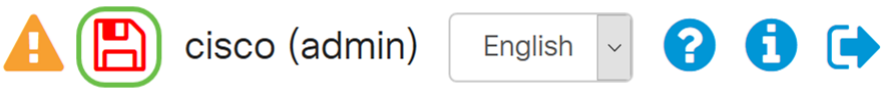
Etapa 12. Clique em **Apply** para salvar suas alterações no arquivo de configuração atual.



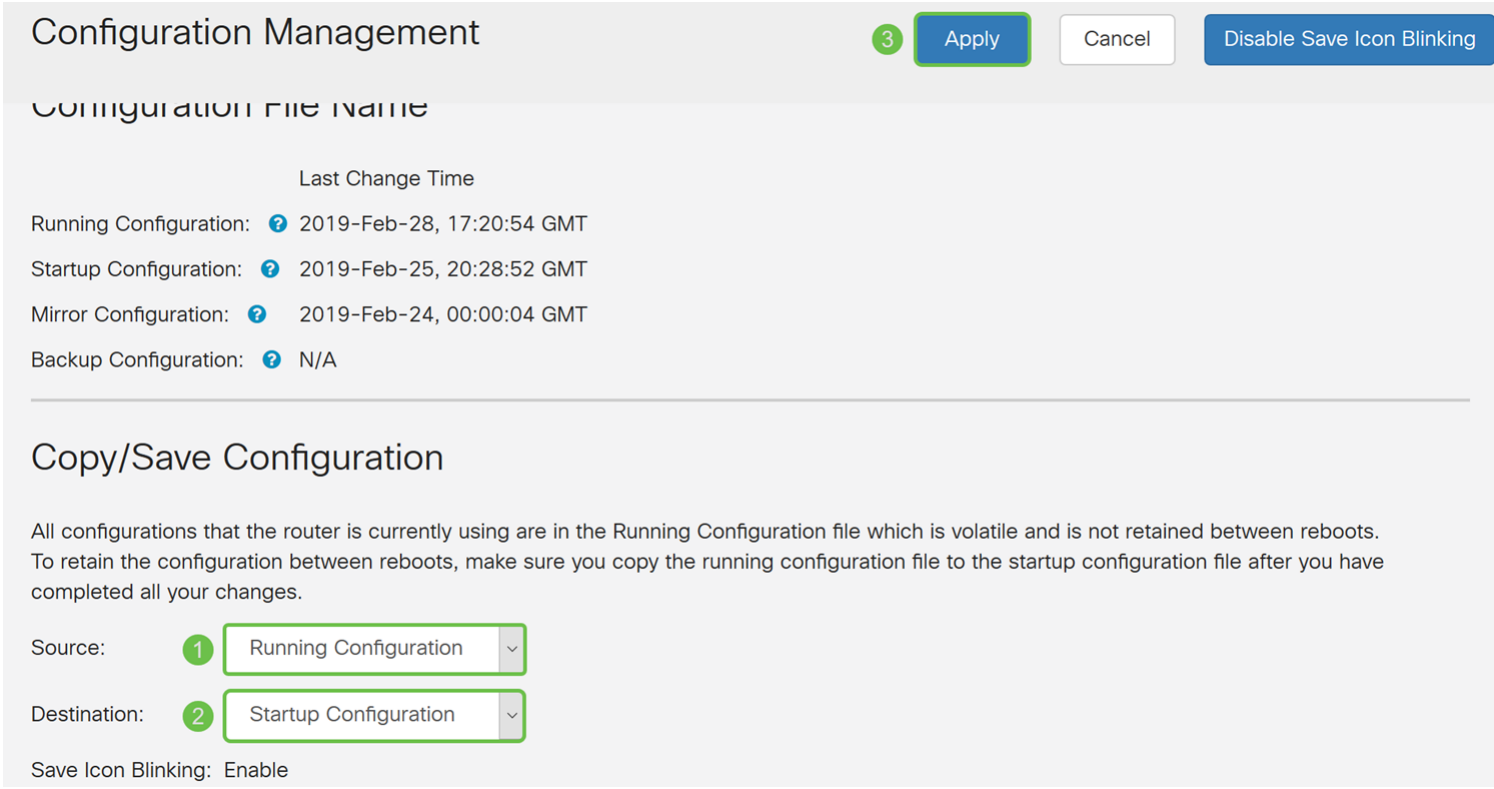
Note: Todas as configurações que o roteador está usando estão atualmente no arquivo de configuração atual, que é volátil e não é retido entre as reinicializações. Para manter sua configuração entre as reinicializações, copie seu arquivo de configuração atual no arquivo de configuração de inicialização.

Nas próximas etapas, mostraremos como copiar sua configuração atual para a configuração de inicialização.

Etapa 13. Clique no ícone **Disquete (Salvar)** na parte superior da página. Isso o redirecionará ao *Gerenciamento de configuração* para salvar sua configuração atual na configuração de inicialização.

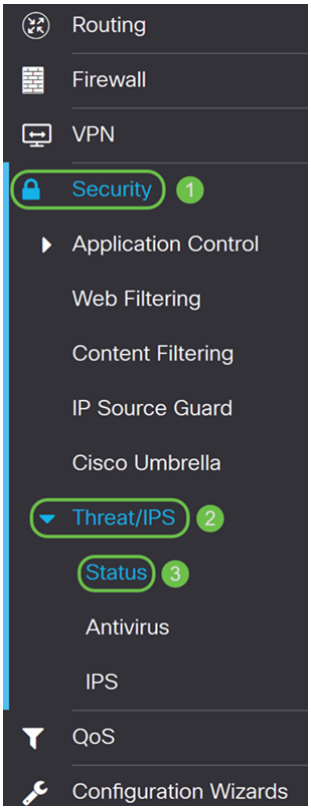


Etapa 14. No *Configuration Management*, role para baixo até a seção *Copy/Save Configuration*. Verifique se a *origem* está **executando a configuração** e se o *destino* está **iniciando a configuração**. Clique em Apply. Isso copiará o arquivo de configuração atual para o arquivo de configuração de inicialização para manter a configuração entre as reinicializações.

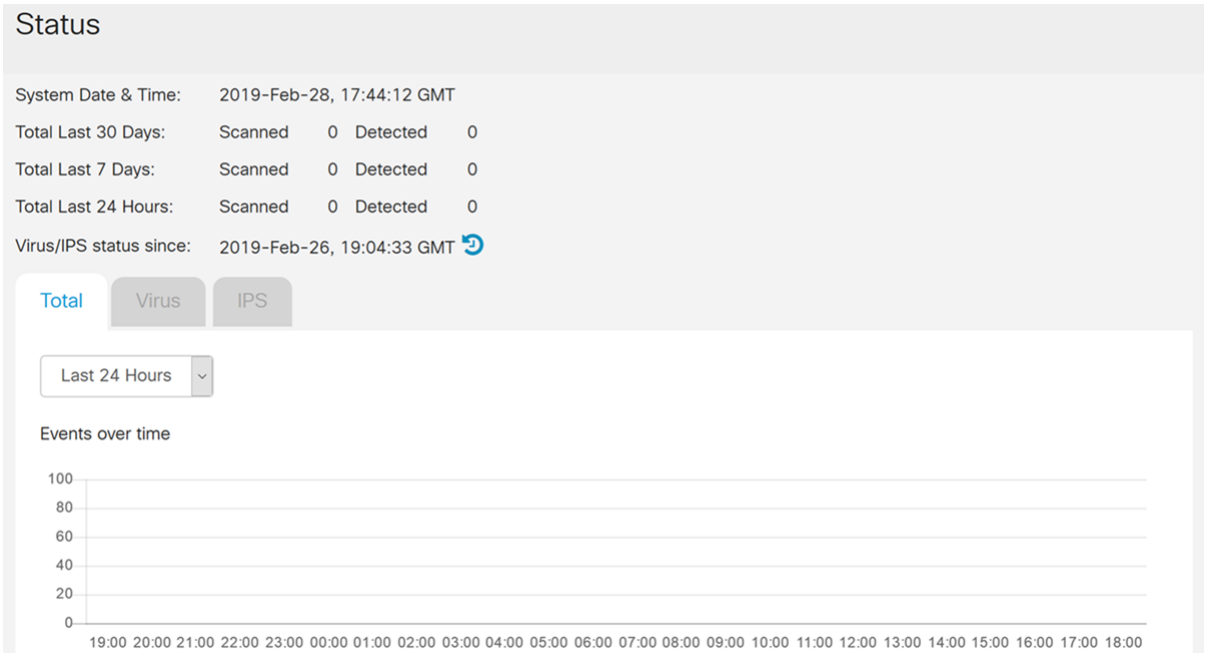


Status de IPS

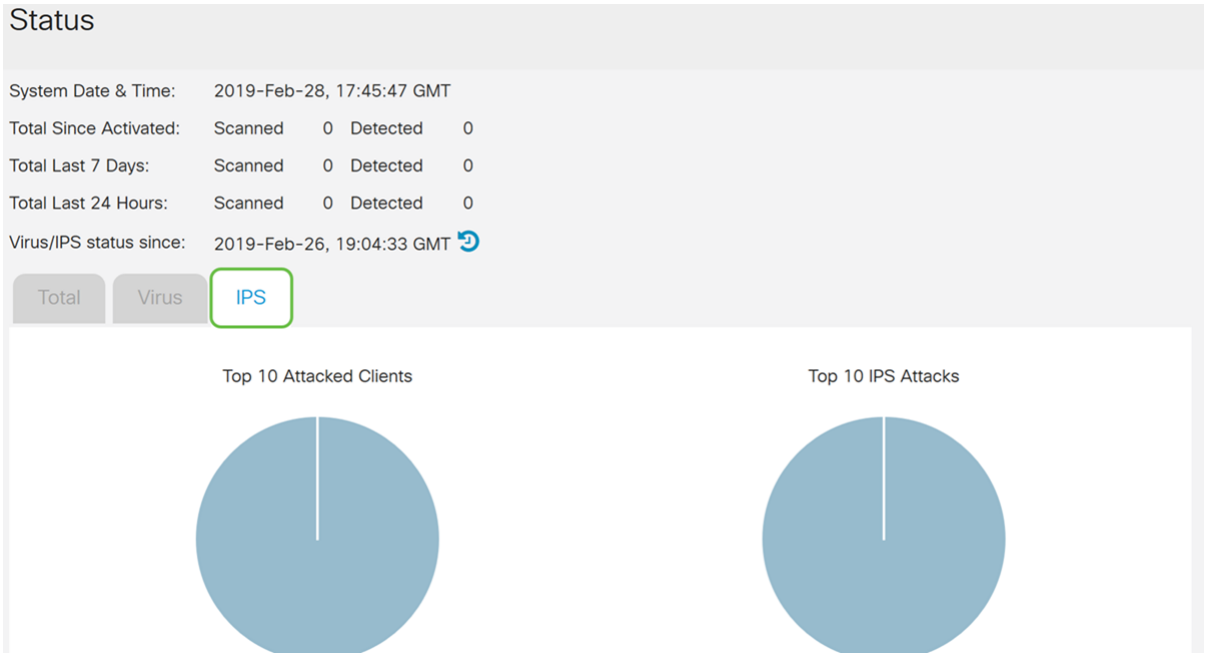
Etapa 1. Navegue até **Security > Threat/IPS > Status**.



Etapa 2. A página *Status* exibe os detalhes das ameaças e ataques quando os recursos Anti-Threat e IPS estão configurados. O painel fornece uma visão de todo o resumo de eventos e informações detalhadas sobre ameaças e ataques detectados de acordo com a seleção, como dia, semana e mês.



Etapa 3. Clique na guia **IPS**. Isso exibirá os 10 principais clientes atacados, bem como os 10 principais ataques IPS.

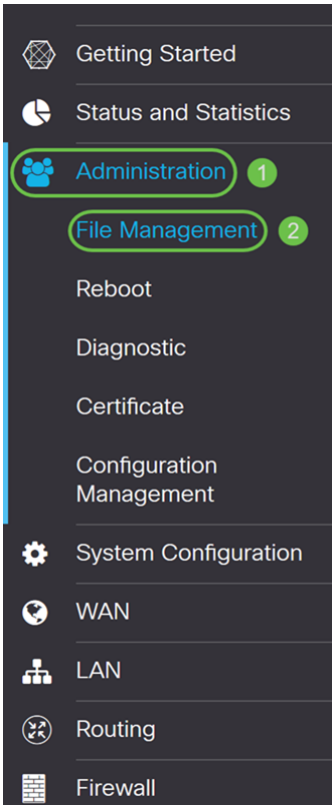


Atualizando definições de IPS

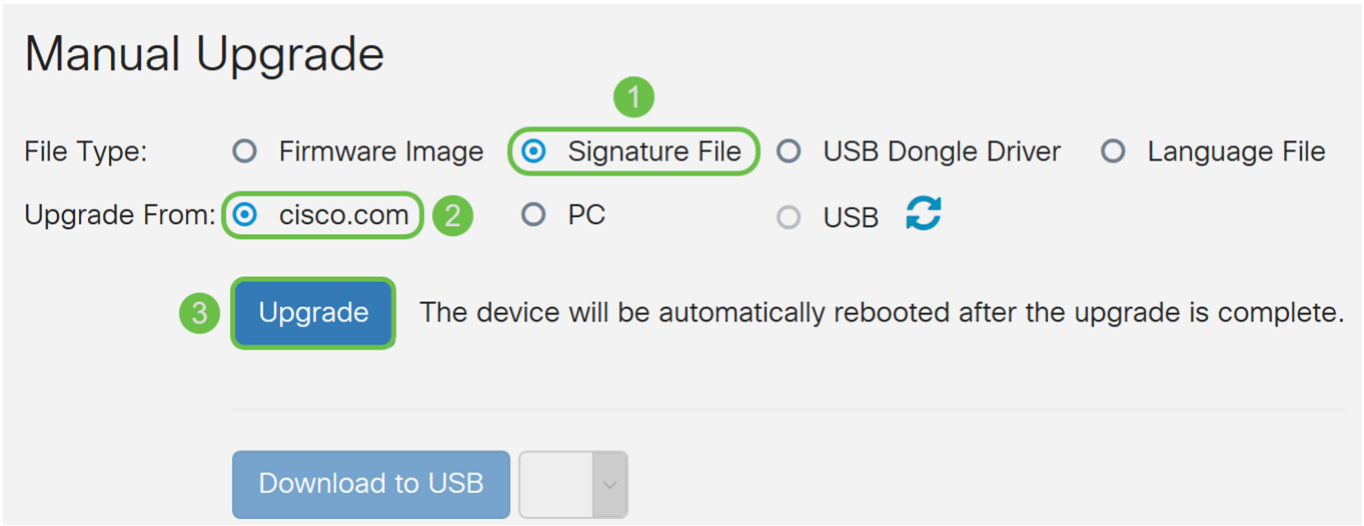
Você pode atualizar a definição de IPS manualmente ou automaticamente. As etapas 1 a 2 mostrarão como atualizar a definição de IPS manualmente, enquanto as etapas 3 a 6 mostrarão como atualizar a definição de IPS automaticamente.

Prática recomendada: Recomenda-se atualizar as assinaturas de segurança automaticamente semanalmente.

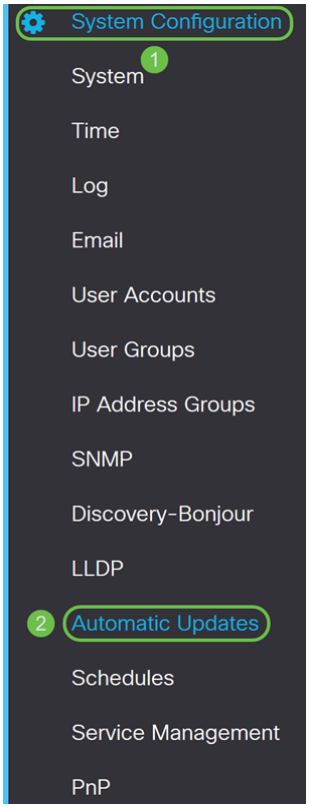
Etapa 1. Para atualizar manualmente as definições de IPS, navegue para **Administração > Gerenciamento de arquivos**.



Etapa 2. Role para baixo até a seção *Atualização manual* na página *Gerenciamento de arquivos*. Escolha **Arquivo de assinatura** para *Tipo de arquivo* e **cisco.com** para *atualização a partir*. Em seguida, pressione **Atualizar**. Isso fará o download da assinatura de segurança mais recente e a instalará.

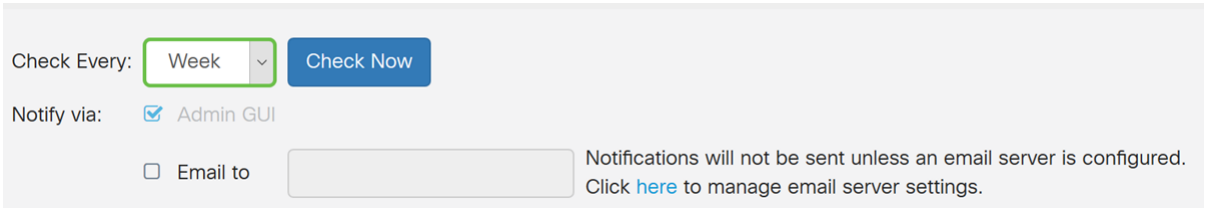


Etapa 3. Para atualizar automaticamente as definições de IPS, navegue para **Configuração do sistema > Atualizações automáticas**.

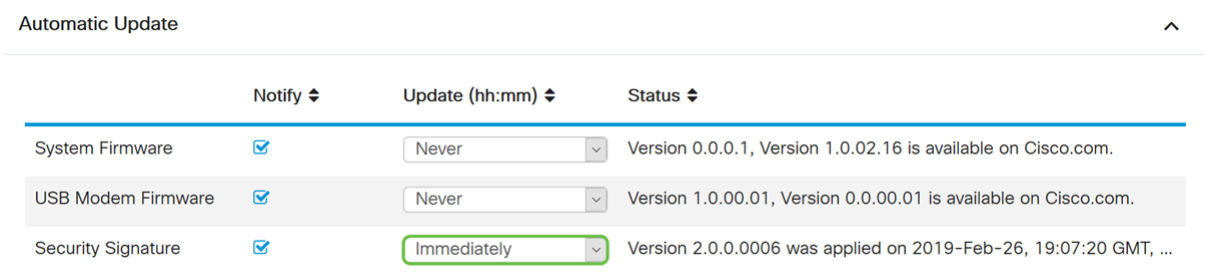


Etapa 4. A página *Atualizações automáticas* é aberta. Você tem a opção de verificar as atualizações semanalmente ou mensalmente. Você pode fazer com que o roteador notifique por e-mail ou pela IU da Web. Neste exemplo, selecionaremos para verificar todas as semanas.

Note: Recomenda-se atualizar as assinaturas de segurança automaticamente semanalmente.

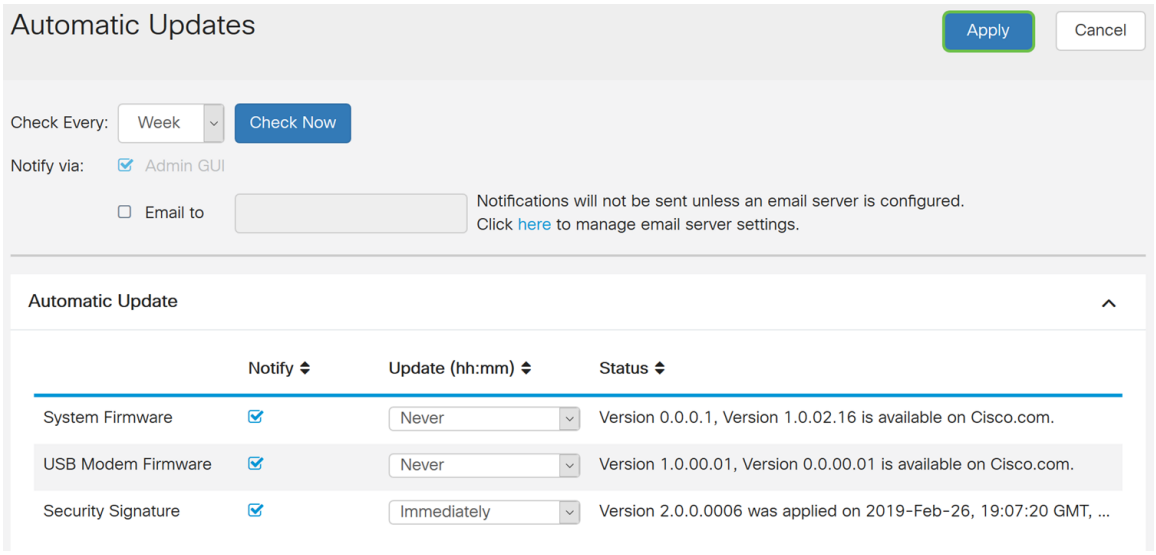


Etapa 5. Role para baixo até a seção *Atualização automática* e procure o campo *Assinatura de segurança*. Na lista suspensa *Atualização de assinatura de segurança*, selecione a hora que deseja atualizar automaticamente. Neste exemplo, selecionaremos **Imediatamente**.



Etapa 6. Clique em **Apply** para salvar as alterações no arquivo de configuração atual.

Note: Lembre-se de clicar no ícone **Disquete** na parte superior para navegar até a página *Gerenciamento de configuração* para copiar o arquivo de configuração atual para o arquivo de configuração de inicialização. Isso ajudará a manter suas configurações entre as reinicializações.



Conclusão

Agora você deve ter configurado com êxito o Sistema de prevenção de intrusão no roteador RV34x Series.