# Konfigurieren des Intrusion Prevention Systems auf dem Router der Serie RV34x

## Ziel

In diesem Dokument wird erläutert, wie Sie das Intrusion Prevention System (IPS) für Router der Serie RV34x konfigurieren.

## Einleitung

Das Intrusion Prevention System prüft den Datenverkehr, um bekannte Angriffsmuster zu erkennen, die blockiert werden sollen. Er überwacht Pakete und Sitzungen, die durch den Router fließen, und überprüft jedes Paket, um eine Übereinstimmung mit einer der Cisco IPS-Signaturen zu erhalten. Wenn verdächtige Aktivitäten erkannt werden, werden sie protokolliert oder blockiert. Es ist wichtig, die IPS- und Antivirus-Datenbanken und -Definitionen zu aktualisieren. Diese können manuell oder automatisch aktualisiert werden.

Sehen Sie sich die folgenden Videos auf dem Cisco Intrusion Prevention System an:

IPS kann jedoch die Leistung des Routers beeinträchtigen. Im Allgemeinen hat dies keine Auswirkungen auf den Gesamtdurchsatz für Hypertext Transfer Protocol (HTTP)- und File Transfer Protocol (FTP)-Datenverkehr, kann aber die maximale Anzahl gleichzeitiger Verbindungen etwas drastisch verringern.

**Wichtiger Hinweis:** Wenn der Router derzeit stark ausgelastet ist, kann dies das Problem noch verschärfen.

Die folgende Tabelle enthält erwartete Leistungsstatistiken für verschiedene Konfigurationen. Diese Werte sollten als Richtschnur dienen, da die tatsächliche Leistung aufgrund verschiedener Faktoren abweichen kann.

| | Gleichzeitige Verbindungen | Verbindungsrate | HTTP-Durchsatz | FTP-Durchsatz |
|---|---|---|---|---|
| Standardeinstellungen | 40000 | 3000 | 982 MB/s | 981 MB/s |
| APP-Steuerung aktivieren | 15000-16000 | 1300 | 982 MB/s | 981 MB/s |
| Antivirus aktivieren | 16000 | 1500 | 982 MB/s | 981 MB/s |
| **IPS aktivieren** | **17000** | **1300** | **982 MB/s** | **981 MB/s** |
| Aktivieren von Anwendungskontrolle Antivirus | 15000-16000 | 1000 | 982 MB/s | 981 MB/s |

| | | | | |
|---|---|---|---|---|
| und IPS | | | | |

Die folgenden Felder sind definiert als:

**Parallele Verbindungen** - Die Gesamtanzahl gleichzeitiger Verbindungen. Wenn Sie z. B. eine Datei von einer Site herunterladen, ist dies eine Verbindung, die Audio von Spotify streamt, eine andere Verbindung, wodurch es zwei gleichzeitige Verbindungen.

**Verbindungsrate** - Die Anzahl der Verbindungsanforderungen/Sekunde, die verarbeitet werden kann.

**HTTP/FTP-Durchsatz** - Der HTTP- und FTP-Durchsatz entspricht den Downloadraten in MB/s.

Security-Lizenzen wurden aktualisiert und umfassen neben der bestehenden Anwendungs- und Webfilterung auch IPS-Schutz. Für eine Sicherheitslizenz ist ein Smart Account erforderlich. Wenn Sie noch kein aktives Smart Account haben, ist Abschnitt 1 dieses Dokuments erforderlich.

Um zu erfahren, wie Antivirus auf RV34x konfiguriert wird, klicken Sie hier.

## Unterstützte Geräte

- RV34x

## Software-Version

- 1.0.03.x

## Inhalt



## Smart Licensing

Wenn Sie über kein aktives Smart Account verfügen, müssen Sie mit den nachfolgenden Schritten fortfahren.

Wenn bei der Konfiguration Ihres Smart License-Kontos Probleme oder Probleme auftreten, hilft unser Support-Team bei der Behebung potenzieller Probleme und kann auf verschiedene Weise erreicht werden. Nutzen Sie die von Ihnen bevorzugte Methode, um sich zu orientieren.

- **Router-Community:** Cisco Small Business Support Community

- **Häufig gestellte Fragen zur Serie RV34x:** Häufig gestellte Fragen zu Routern der Serie RV34x

- **Smart License im Überblick** Smart Software-Lizenzierung

- **Häufig gestellte Fragen zu Smart Licenses:** Häufig gestellte Fragen zu Smart Licensing und Smart Accounts für Partner, Distributoren und Kunden

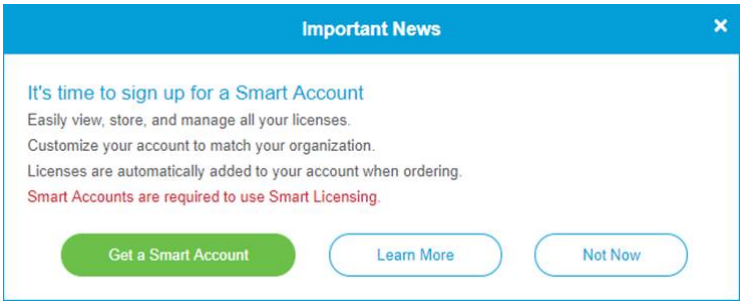
- **Ticket senden:** Support Case Manager

**Telefonnummer für den** • **USA/Kanada:** 1-866-606-1866 oder Small Business TAC-Kontakte

• **Lizenzierungs-E-Mail:** licensing@cisco.com

Schritt 1: Wenn Sie vor kurzem Ihr Cisco.com-Konto erstellt oder besucht haben, wird eine Nachricht angezeigt, in der Sie Ihr eigenes Smart License-Konto erstellen. Falls nicht, können Sie hier klicken, um zur Seite Smart License Account Creation (Smart-Lizenzkontoerstellung) zu gelangen. Sie müssen sich möglicherweise anmelden.

**Anmerkung:** Weitere Einzelheiten zu den Schritten für die Anforderung Ihres Smart Accounts finden Sie hier.




Schritt 2: Beim Kauf einer Smart-Lizenz für einen Router muss der Anbieter einen Prozess durchführen, bei dem die eindeutige Lizenz-ID auf Ihr Smart License-Konto übertragen wird. Im Folgenden finden Sie eine Tabelle mit den erforderlichen Informationen, die Sie beim Kauf der Pakete benötigen.

**Anmerkung:** IPS und Antivirus sind Teil der Sicherheitslizenz für die Webfilterung und Anwendungsfilterung.

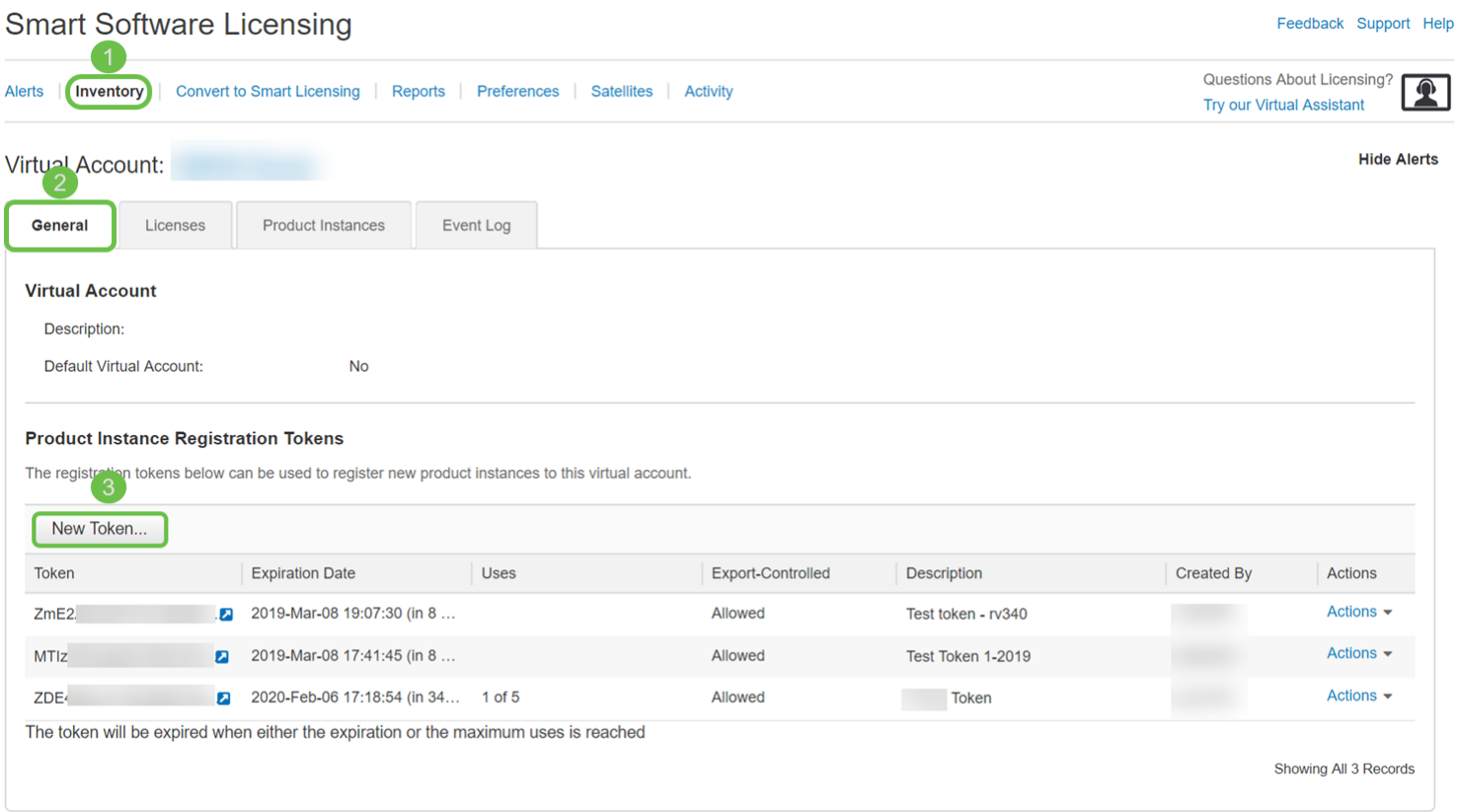
| Erforderliche Informationen | Suchen von Informationen |
|---|---|
| Cisco.com-Benutzer-ID | Befindet sich in Ihrem Kontoprofil, oder Sie können hier klicken. |
| Smart License | Es empfiehlt sich, vor |

| | |
|---|---|
| Account-Name | dem Erwerb der Lizenz Ihr Smart Account zu erstellen. Dies sollte Schritt 8 des Artikels Smart License Account Creation sein. |
| Smart License SKU | Der Produktkennzeichnungscode für das Gerät. Beispiel: RV340-K9-NA |

**Anmerkung:** Wenn Sie eine Lizenz erworben haben und diese nicht in Ihrem virtuellen Konto aufgeführt ist, sollten Sie sich entweder an den Händler wenden, um ihn zu bitten, die Übertragung vorzunehmen, oder uns kontaktieren.

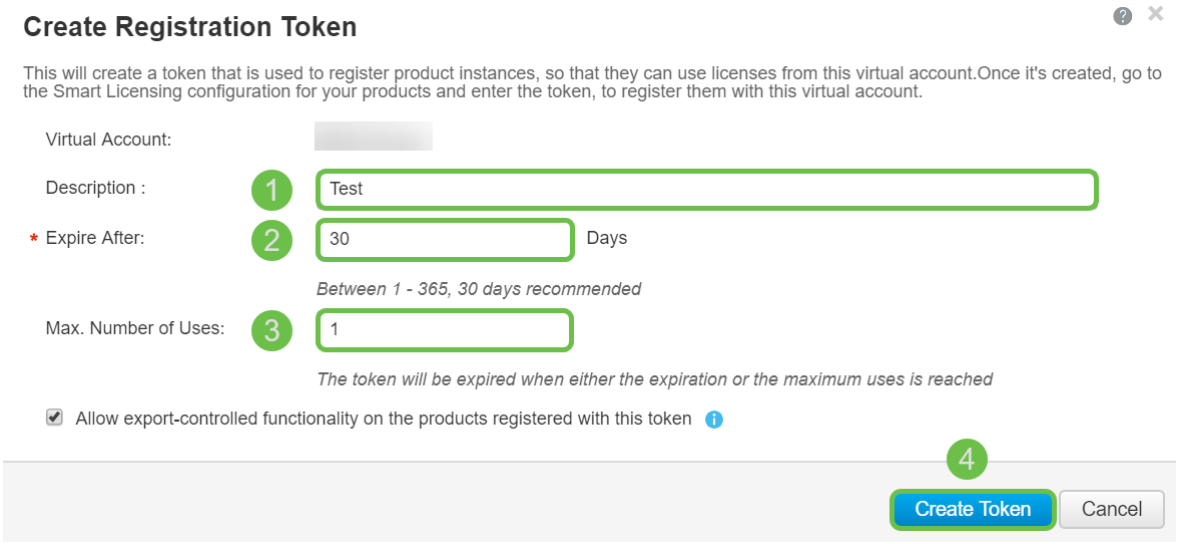
Um den Prozess so reibungslos wie möglich zu gestalten, sollten Sie Ihre Lizenzrechnung, die Cisco Verkaufsauftragsnummer und einen Screenshot Ihrer Smart Account-Lizenzseite (zur gemeinsamen Nutzung mit unserem Team) erstellen.

Schritt 3: Um ein Token zu generieren, navigieren Sie zu Ihrem Smart Software License-Konto. Klicken Sie anschließend auf die **Registerkarte Bestand > Allgemein**. Klicken Sie auf die Schaltfläche **Neues Token...**.

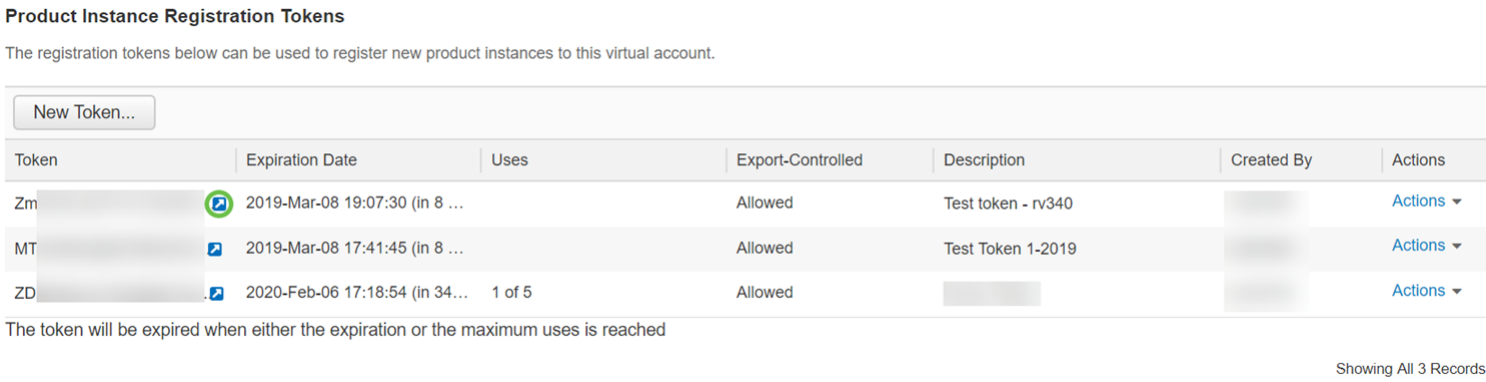



Schritt 4: Das Fenster *Registrierungstoken erstellen* wird geöffnet. Geben Sie eine *Beschreibung*, *Ablaufdatum* und *Max ein. Anzahl der Anwendungen*. Drücken Sie anschließend die Schaltfläche **Create Token (Token erstellen)**.

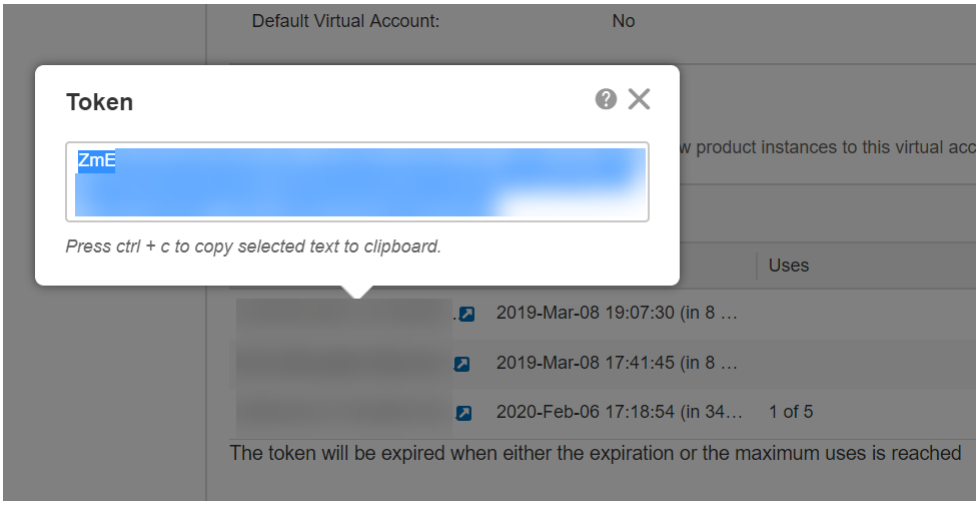
**Anmerkung:** 30 Tage für *Ablaufdatum Nach* Empfehlung



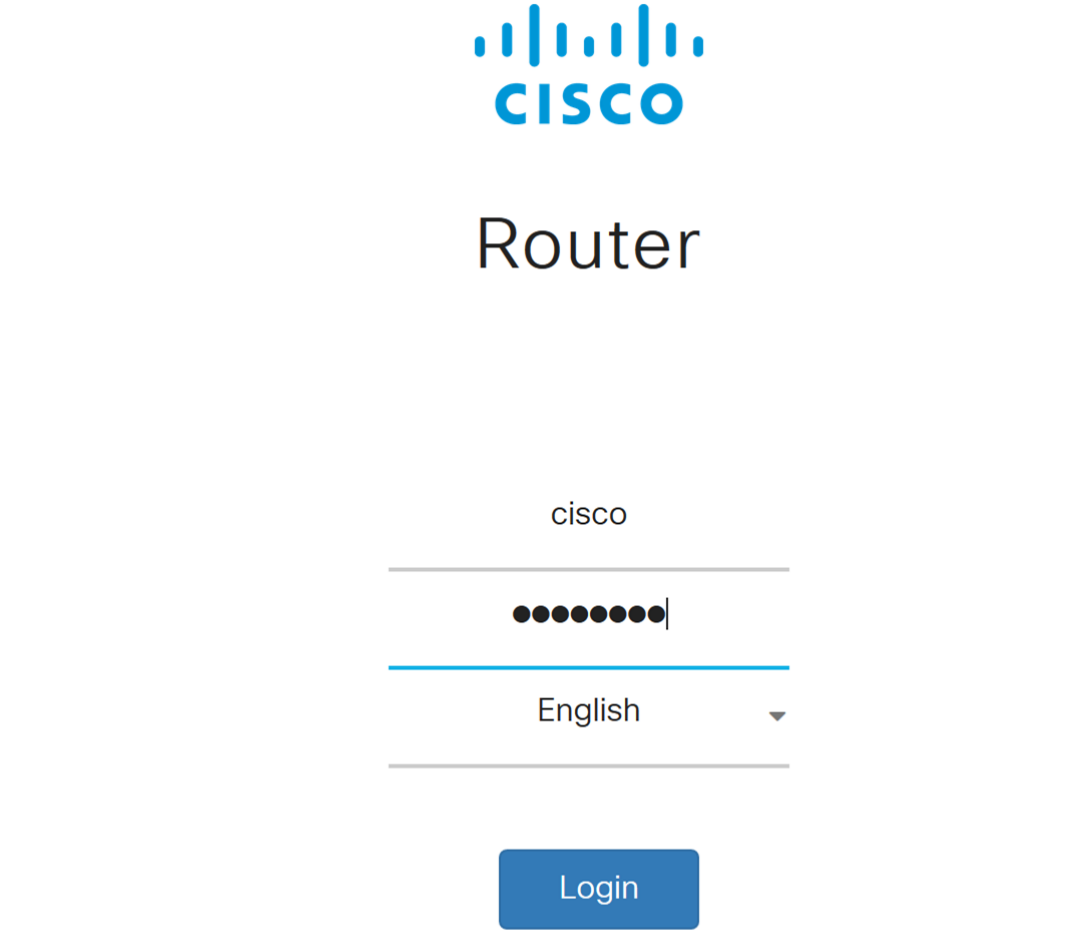

Schritt 5: Nachdem das Token generiert wurde, können Sie auf den **Token-Link (blaues Feld mit einem weißen Pfeil)** rechts neben dem kürzlich erstellten Token klicken.



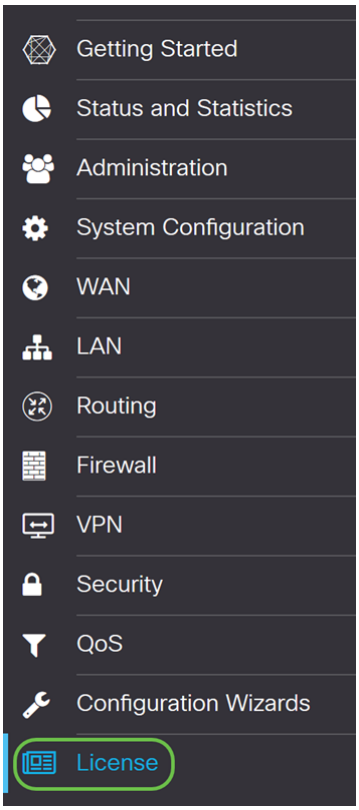

Schritt 6: Ein *Token*-Fenster mit dem vollständigen Token wird angezeigt, das Sie kopieren können. Markieren Sie das Token, klicken Sie mit der rechten Maustaste auf das Token, und klicken Sie auf **Kopieren**, oder Sie können die **Strg**-Taste auf der Tastatur gedrückt halten und **c** gleichzeitig klicken, um den Text zu kopieren.




Schritt 7: Nachdem Sie Ihr Token kopiert haben, müssen Sie sich beim Gerät anmelden und den Tokenschlüssel hochladen. Melden Sie sich auf der Webkonfigurationsseite des Routers an.

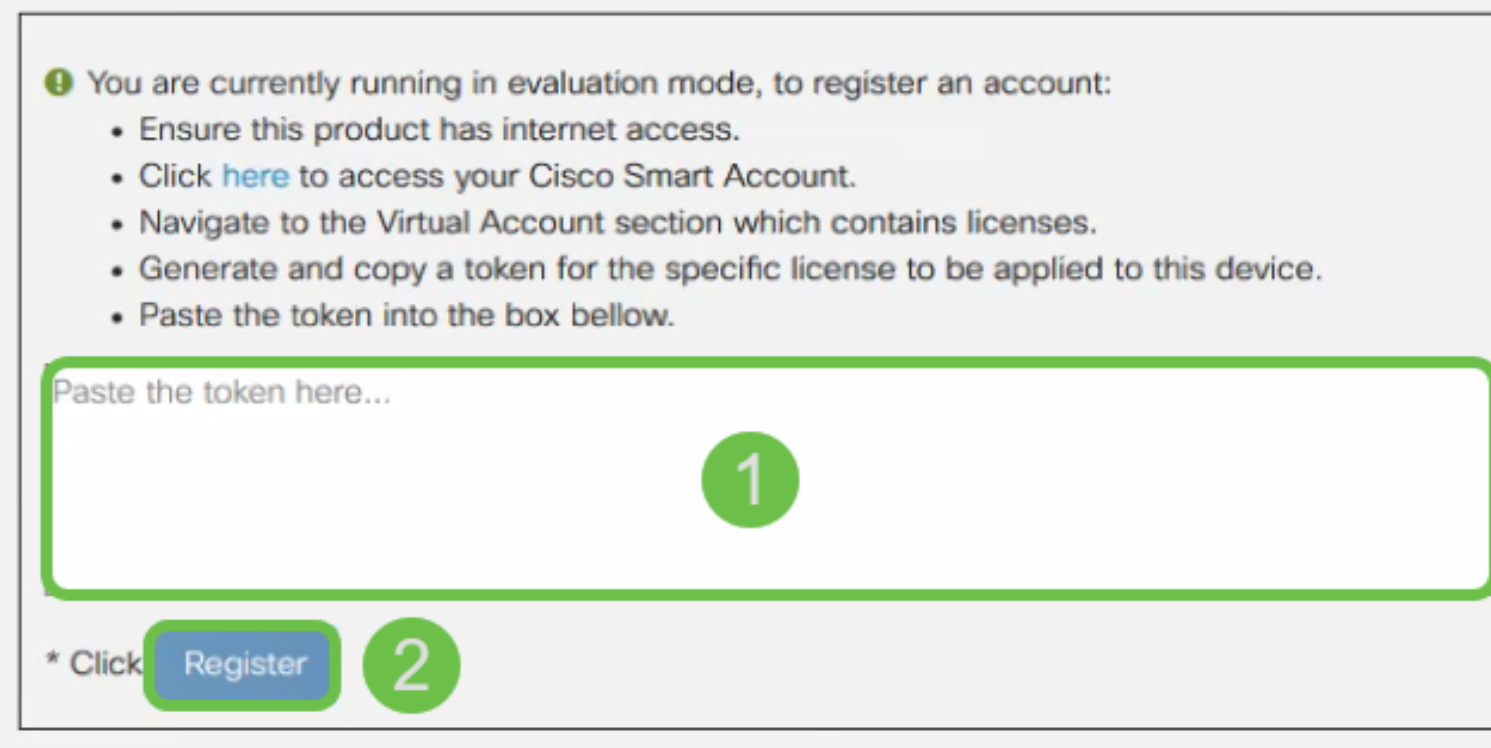



Schritt 8: Navigieren Sie zu **Lizenz.**

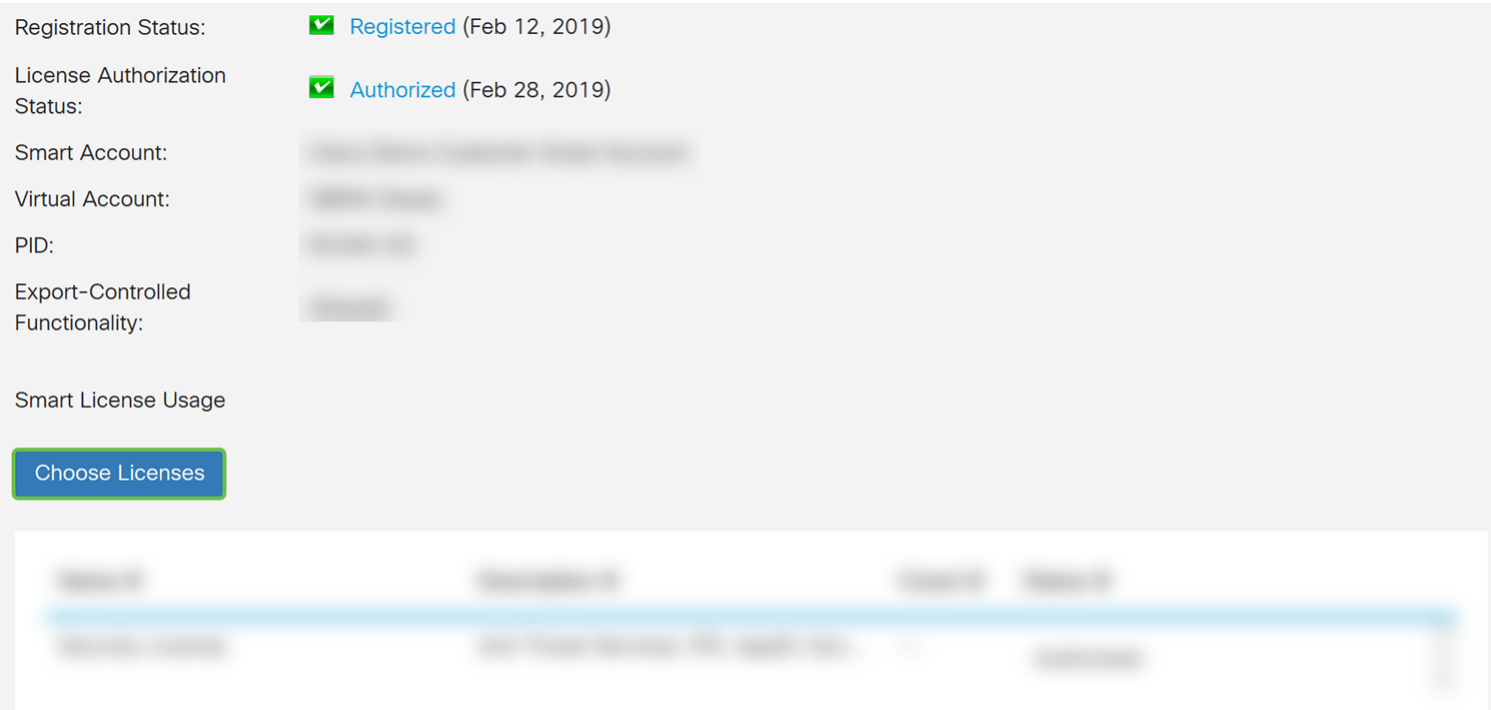


Schritt 9: Wenn Ihr Gerät nicht registriert ist, wird Ihr *Lizenzautorisierungsstatus* als *Evaluierungsmodus* angezeigt. Fügen Sie das Token (Schritt 6 dieses Abschnitts) ein, das Sie auf der Seite *Smart Licensing Manager* generiert haben. Klicken Sie anschließend auf **Registrieren**.

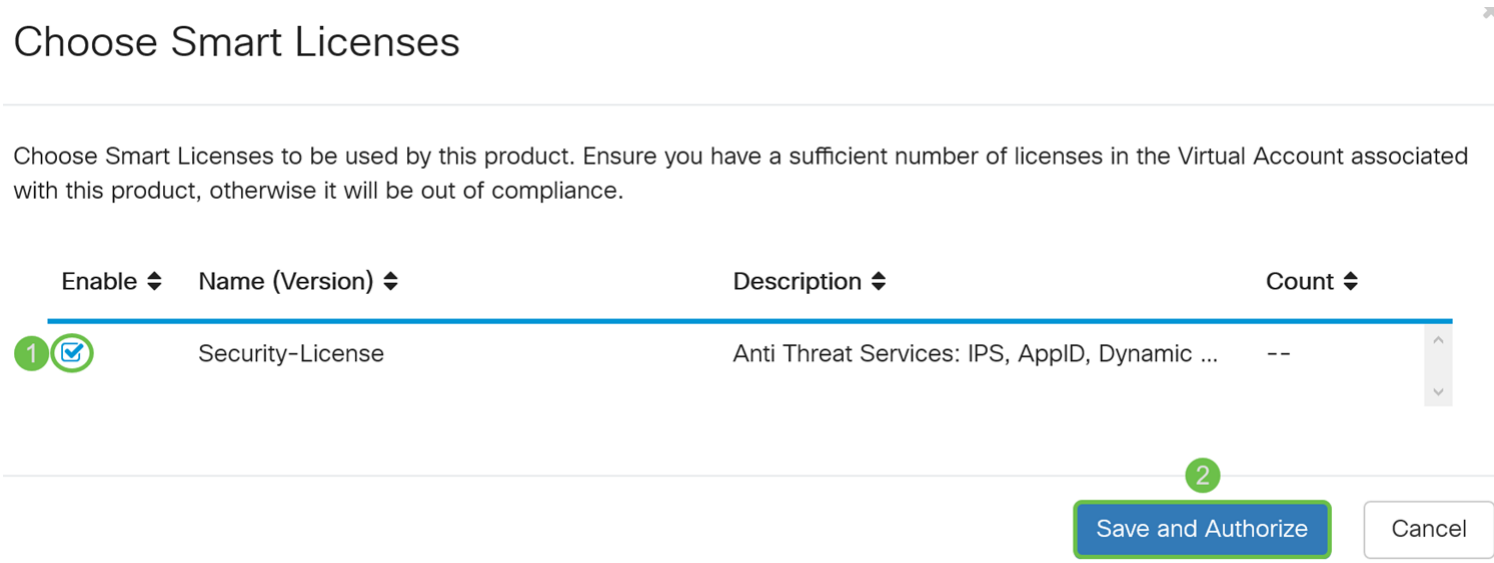
**Anmerkung:** Der Registrierungsvorgang kann einige Zeit in Anspruch nehmen. Warten Sie bitte, bis der Vorgang abgeschlossen ist.



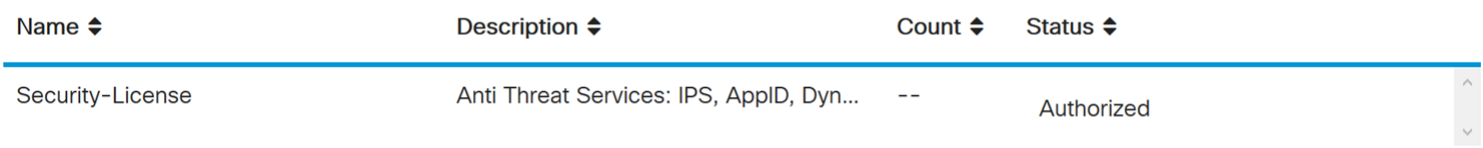

Schritt 10: Nach der Registrierung des Tokens müssen Sie die Lizenz zuweisen. Klicken Sie auf die Schaltfläche **Lizenzen auswählen**.




Schritt 11: Das Fenster *Smart Licenses (Smart Licenses auswählen*) sollte angezeigt werden. Aktivieren Sie die **Security-Lizenz** und drücken Sie dann **Save and Authorize (Speichern und Autorisieren)**.



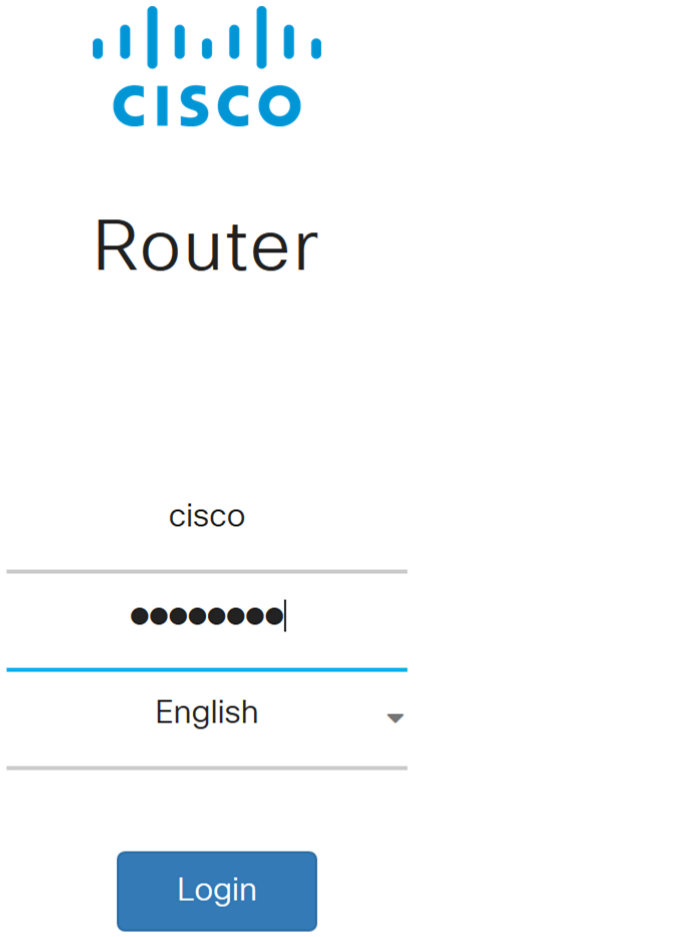

Schritt 12: Der *Status* Ihrer Security-Lizenz sollte jetzt *autorisiert* werden.



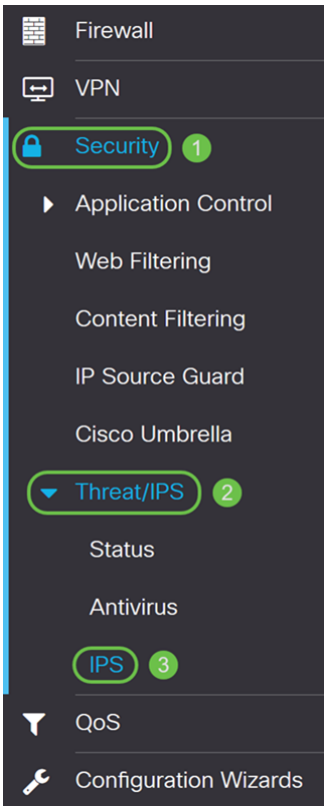

Sie sollten jetzt mit der Konfiguration des Intrusion Prevention Systems fortfahren können.

# Konfigurieren des Intrusion Prevention Systems

Schritt 1: Wenn Sie sich noch nicht beim Router angemeldet haben, melden Sie sich auf der Webkonfigurationsseite des Routers an.

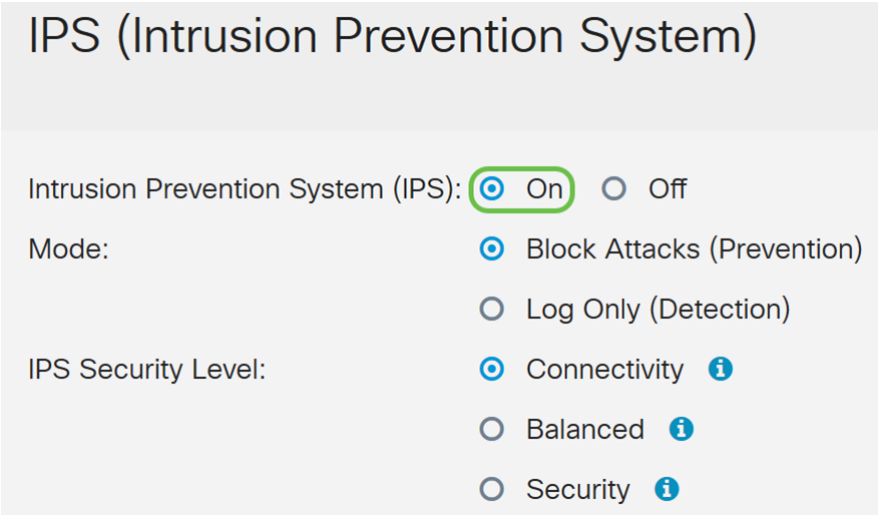



Schritt 2: Navigieren Sie zu **Security > Threat/IPS > IPS**.



Schritt 3: Wählen Sie **On** aus, um die Funktion Intrusion Prevention System (Intrusion Prevention System) zu aktivieren. Wenn Sie die Funktion deaktivieren möchten, wählen Sie **Aus**.

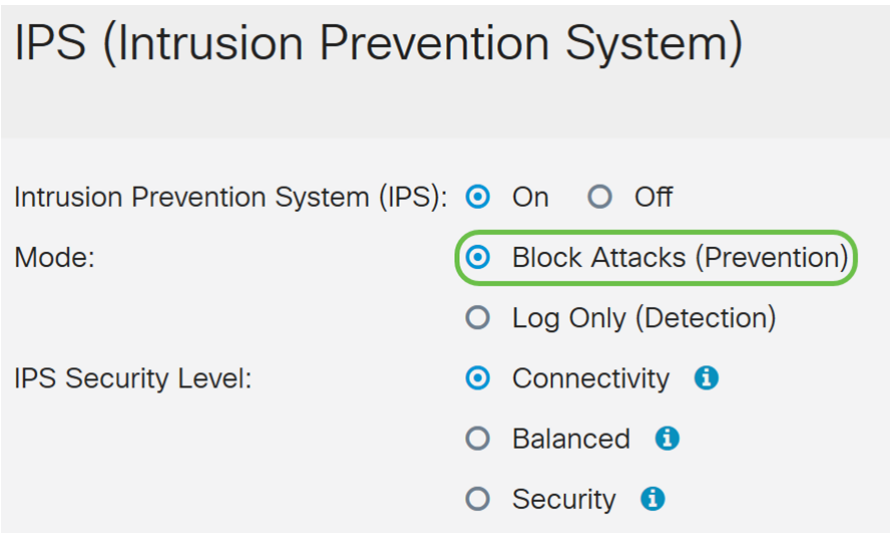
In diesem Beispiel wählen Sie **On (Ein) aus**.




Schritt 4: Wählen Sie entweder **Angriffe blockieren (Verhinderung)** oder **Nur Protokoll**. In diesem Beispiel wählen wir **Angriffe blockieren (Prävention)**. Die folgenden Optionen sind unten definiert.

- **Blockieren von Angriffen (Prävention)** - Wählen Sie diese Option aus, um alle Angriffe zu blockieren. Es protokolliert auch die Anomalie.

- **Log Only (Nur Protokoll)**: Diese Option generiert das Protokoll nur (mit Clientinformationen, Signatur-ID usw.), wenn die Anomalien identifiziert werden. Die Verbindung wird dadurch nicht beeinträchtigt.




Schritt 5: Wählen Sie die IPS-Sicherheitsstufe aus, die Sie verwenden möchten. Die folgenden Optionen sind definiert als:

- **Connectivity**: Dieser Modus erkennt die wichtigsten Angriffe. Dies bietet den geringsten Schutz: nur (mit hohem Schweregrad) Risikoangriffe erkannt werden. Dies ist die ungeschützte Option.

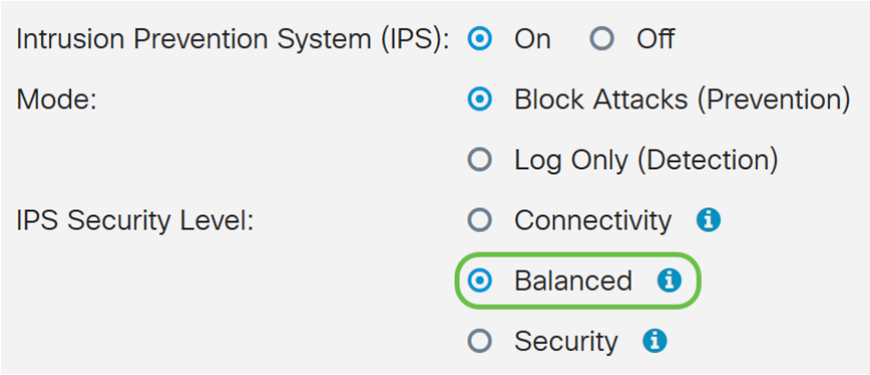
- **Balanced** - Der ausgewählte Modus erkennt schwere Angriffe zusammen mit den kritischen Angriffen. Dadurch wird ein mittlerer Schutz gewährleistet: (hoher + mittlerer Schweregrad)

durch Übergeben von Signaturen mit geringem Risiko überprüft werden. Dies ist die Midlevel-Sicherheit für IPS.

- **Sicherheit** - Der Sicherheitsmodus erkennt normale Angriffe sowie schwere und kritische Angriffe. Dies bietet den meisten Schutz: Alle Regeln (hoch + mittel + niedriger Schweregrad) werden geprüft. Dies ist die höchste Sicherheitsstufe für IPS.

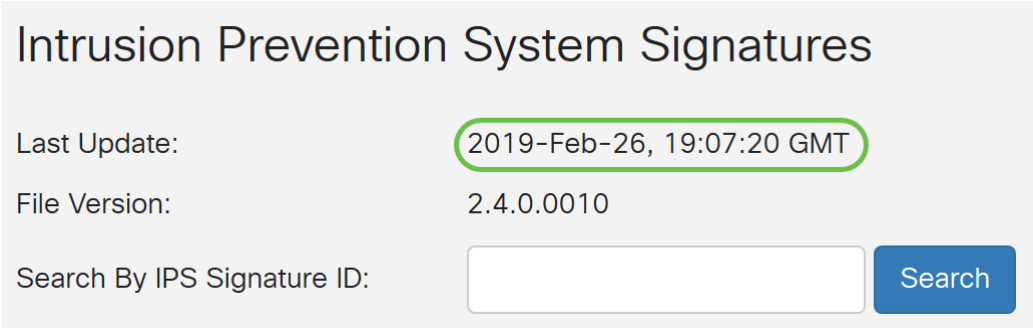
**Anmerkung:** Je höher die Sicherheitsstufe, desto mehr Angriffe werden überwacht, desto größer sind die Auswirkungen auf die Systemleistung.

Für diese Demonstration wählen Sie **Balanced** aus.

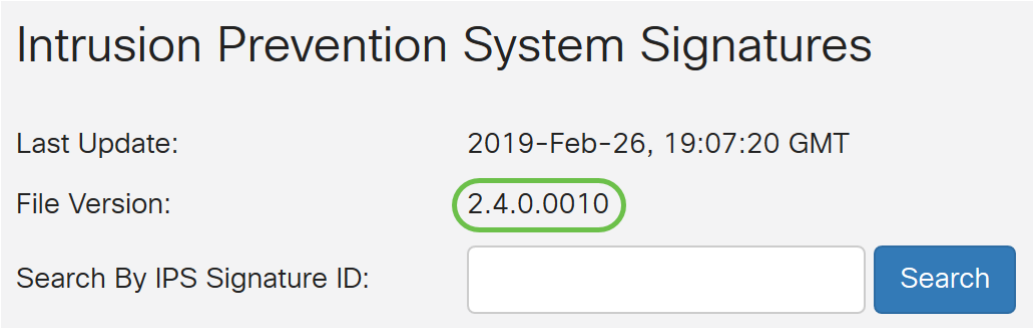



## Signaturen des Intrusion Prevention System

Schritt 6: Im Feld *Letzte Aktualisierung* werden Datum und Uhrzeit der letzten aktualisierten Signatur angezeigt.




Schritt 7: Die *Dateiversion* zeigt die verwendete Signaturversion an.




Schritt 8: Um nach einer Signature-ID zu suchen, geben Sie die **Signature-ID** in das Feld *Nach IPS-Signature-ID suchen ein,* und klicken Sie auf **Suchen**, um zu überprüfen, ob die Signatur unterstützt wird. Wenn die Signatur-ID unterstützt wird, wird die Tabelle mit dem unten gezeigten Ergebnis aktualisiert.

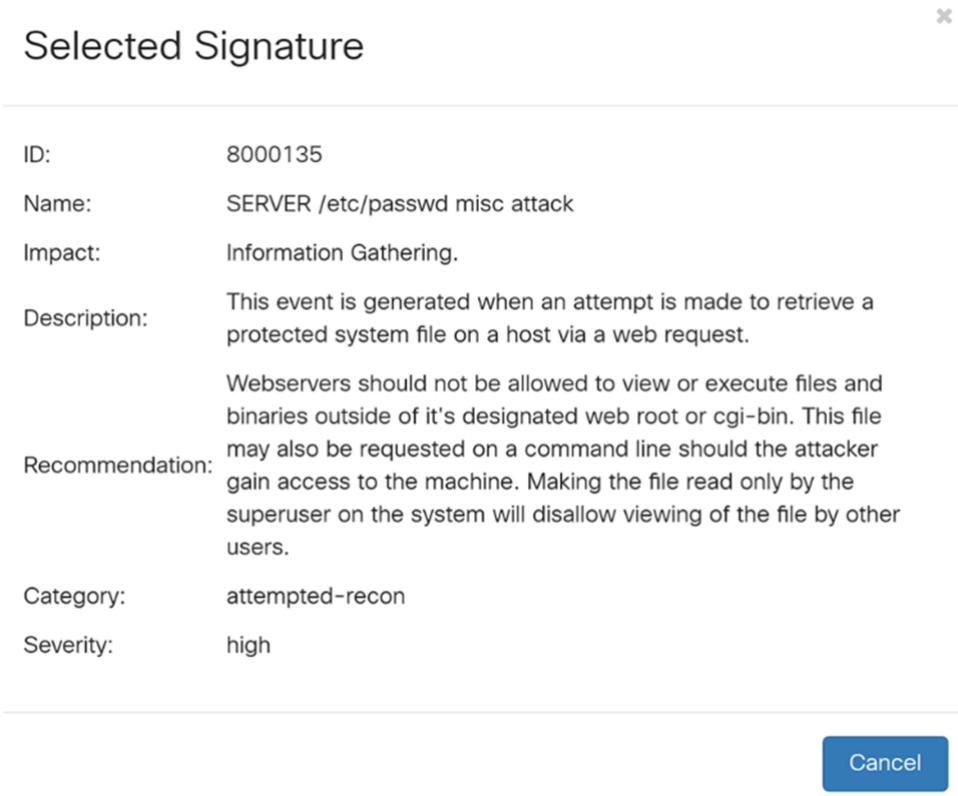
**Anmerkung:** Wenn die Signatur-ID nicht unterstützt wird, wird in der Tabelle nichts angezeigt.


## Signalisierungstabelle des Intrusion Prevention Systems

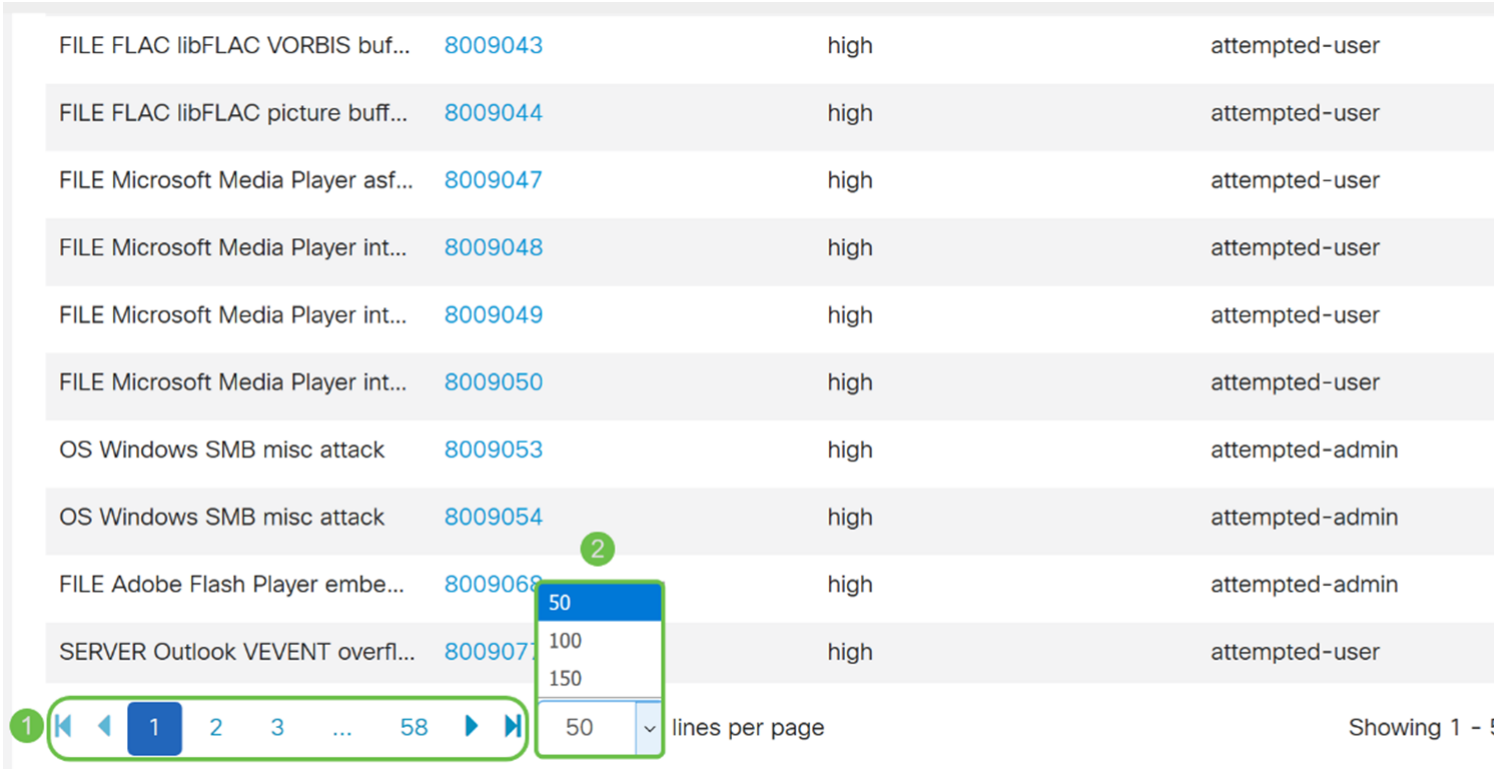
Schritt 9: In der *IPS-Signaturtabelle* sind die folgenden Felder definiert:

- **Name**: Name der Signatur.
- **ID** - Die eindeutige Kennung der Signatur. Wenn Sie auf die ID klicken, wird ein Fenster geöffnet, in dem Sie alle Details zur ausgewählten Signatur anzeigen können.
- **Schweregrad** - Schweregrad kennzeichnet die Sicherheitsauswirkungen.
- **Kategorie** - Die Kategorie, der die Signatur angehört.

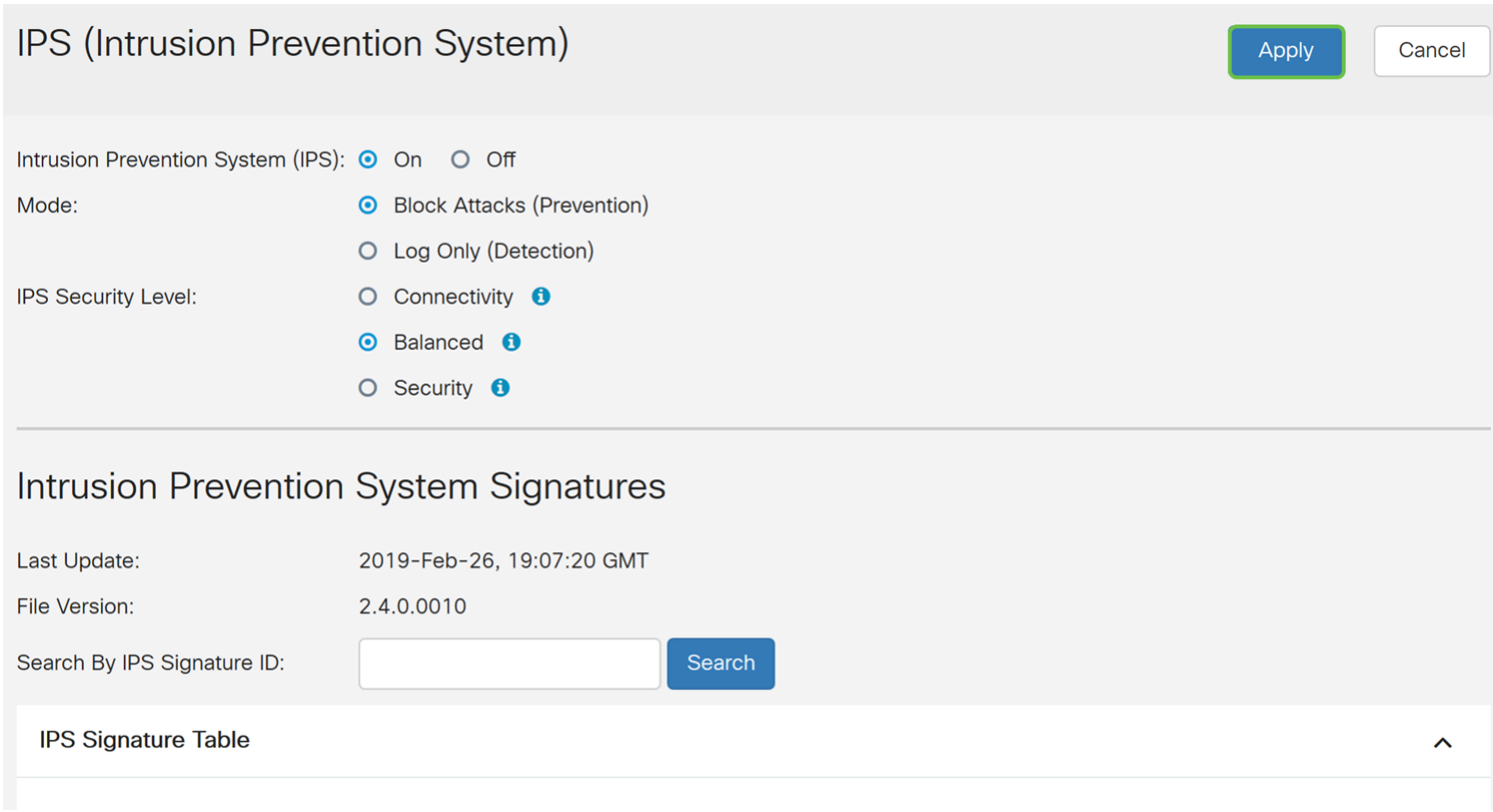

Schritt 10: (Optional) Wenn Sie in der *IPS-Signaturtabelle* auf die Signatur-ID geklickt haben, wird ein Fenster angezeigt, in dem alle Details zur ausgewählten Signatur angezeigt werden.




Schritt 11: Wählen Sie unten in der *IPS-Signaturtabelle* die Pfeile sowie die Nummern aus, die in der Tabelle hin und her navigieren sollen. Sie können auch die Anzahl der Zeilen (**50**, **100** oder **150**) pro Seite in der Dropdown-Liste Zeilen pro Seite auswählen.



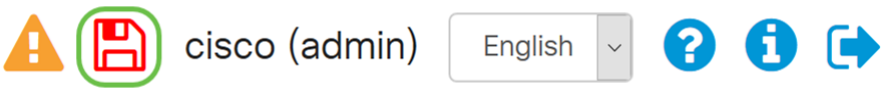

Schritt 12: Klicken Sie auf **Apply**, um die Änderungen in der aktuellen Konfigurationsdatei zu speichern.



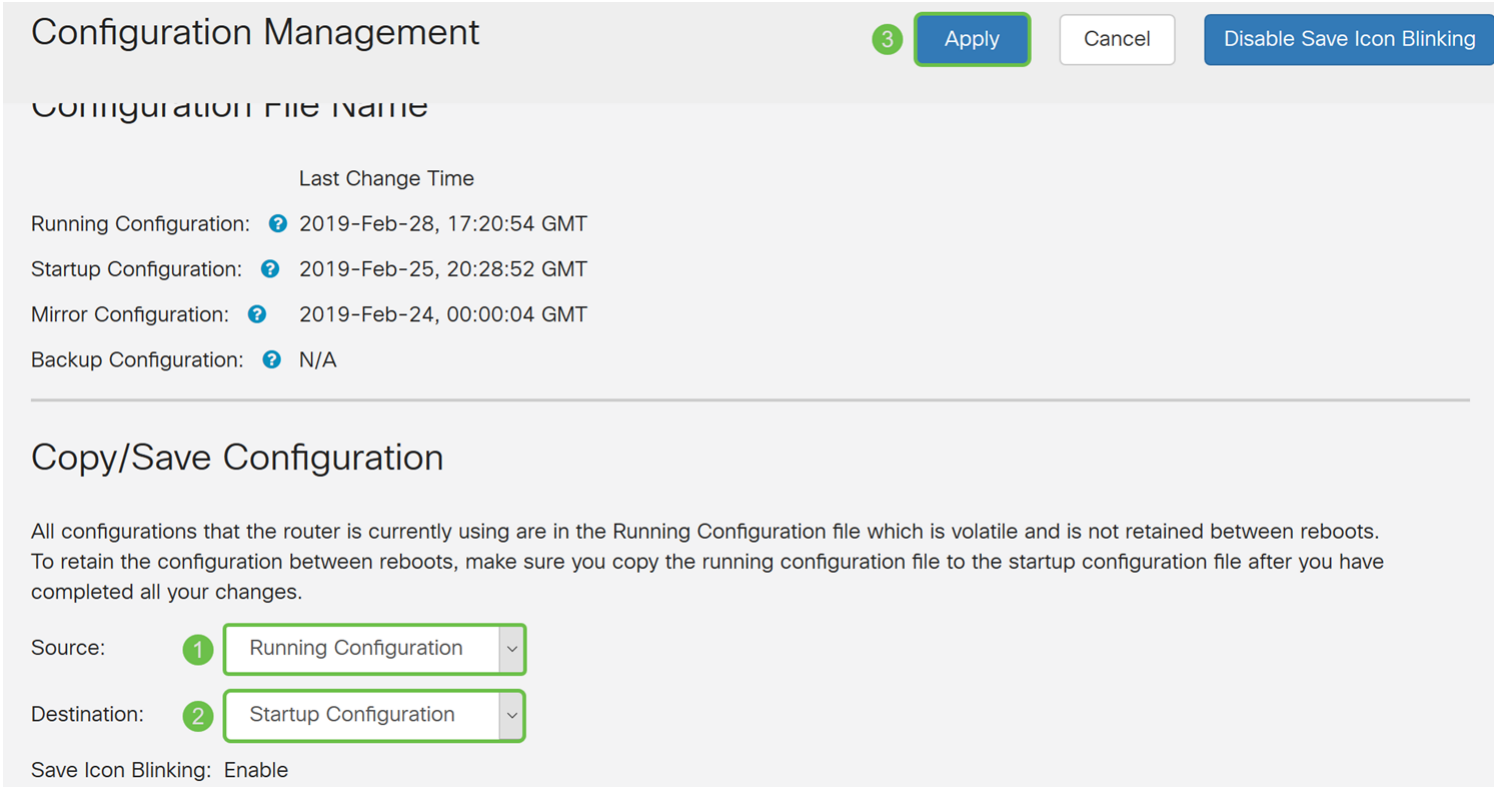

**Anmerkung:** Alle Konfigurationen, die der Router verwendet, befinden sich derzeit in der aktuellen Konfigurationsdatei, die flüchtig ist und zwischen Neustarts nicht beibehalten wird. Um die Konfiguration zwischen Neustarts beizubehalten, kopieren Sie die aktuelle Konfigurationsdatei in die Startkonfigurationsdatei.

In den nächsten Schritten wird gezeigt, wie Sie Ihre aktuelle Konfiguration in die Startkonfiguration kopieren.

Schritt 13: Klicken Sie oben auf der Seite auf das Symbol **Diskette (Speichern)**. Dadurch werden Sie zur *Konfigurationsverwaltung* umgeleitet, um Ihre aktuelle Konfiguration in der Startkonfiguration zu speichern.

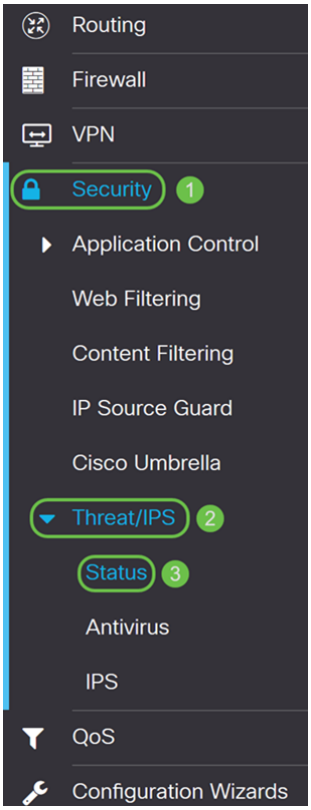



Schritt 14: Blättern Sie im *Konfigurationsmanagement* nach unten zum Abschnitt *"Konfiguration kopieren/speichern"*. Stellen Sie sicher, dass die *Quelle* die **Konfiguration ausführt** und das *Ziel die* **Startkonfiguration** ist. Klicken Sie auf **Apply** (Anwenden). Dadurch wird die aktuelle Konfigurationsdatei in die Startkonfigurationsdatei kopiert, um die Konfiguration zwischen Neustarts beizubehalten.

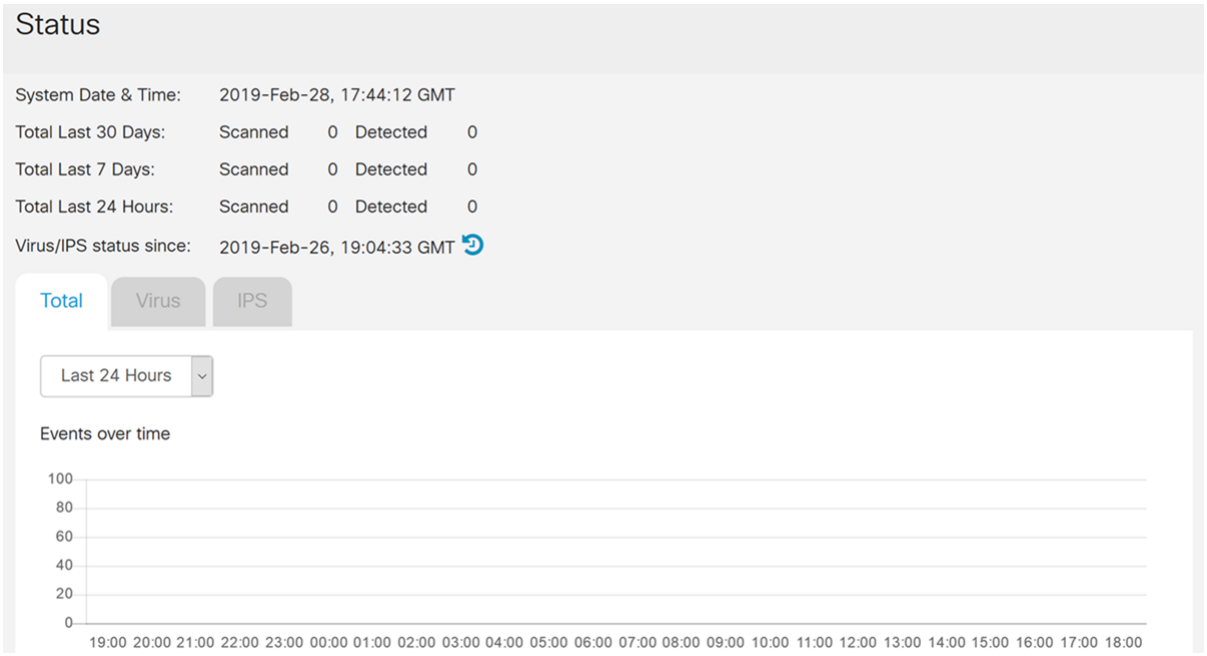



# IPS-Status

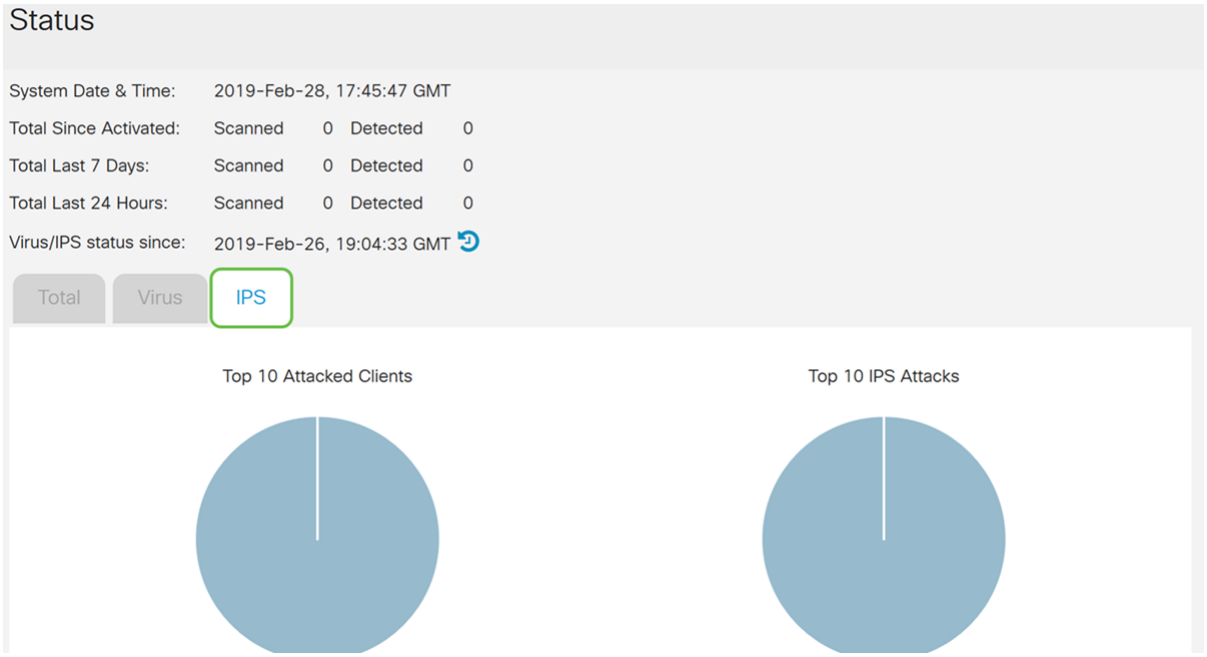
Schritt 1: Navigieren Sie zu **Sicherheit > Bedrohung/IPS > Status**.




Schritt 2: Auf der Seite "*Status*" werden Details zu Bedrohungen und Angriffen angezeigt, wenn die Funktionen für Anti-Bedrohungen und IPS konfiguriert sind. Das Dashboard bietet eine Übersicht über die gesamte Ereignisübersicht sowie detaillierte Informationen zu Bedrohungen und Angriffen, die je nach Auswahl erkannt werden, z. B. Tag, Woche und Monat.




Schritt 3: Klicken Sie auf die Registerkarte **IPS**. Dargestellt werden die 10 am häufigsten angegriffenen Clients sowie die zehn häufigsten IPS-Angriffe.

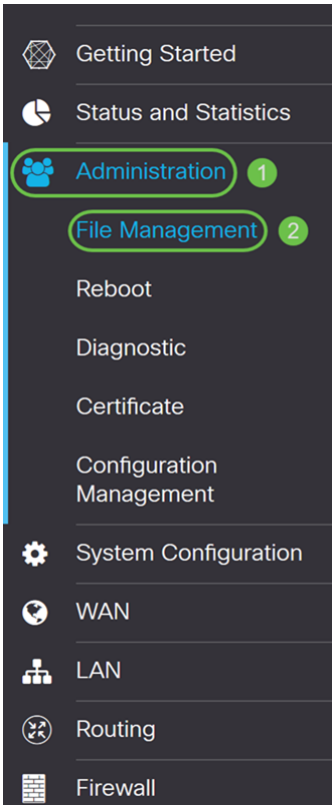



# IPS-Definitionen aktualisieren

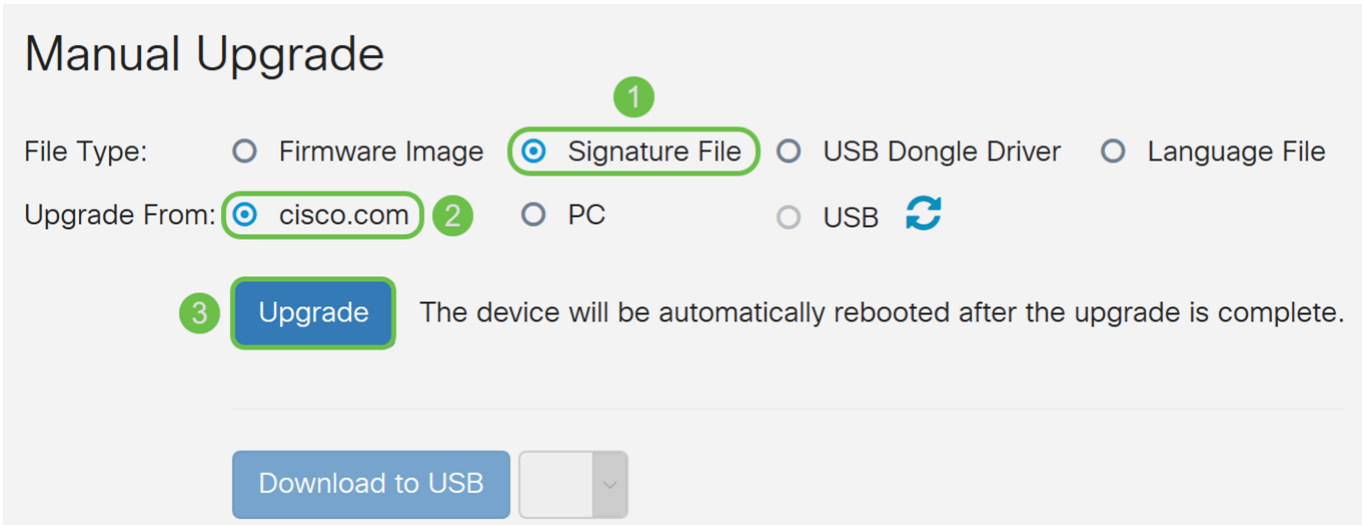
Sie können die IPS-Definition entweder manuell oder automatisch aktualisieren. In den Schritten 1-2 wird gezeigt, wie die IPS-Definition manuell aktualisiert wird, während in den Schritten 3-6 gezeigt wird, wie die IPS-Definition automatisch aktualisiert wird.

**Best Practice:** Es wird empfohlen, die Sicherheitssignaturen wöchentlich automatisch zu aktualisieren.

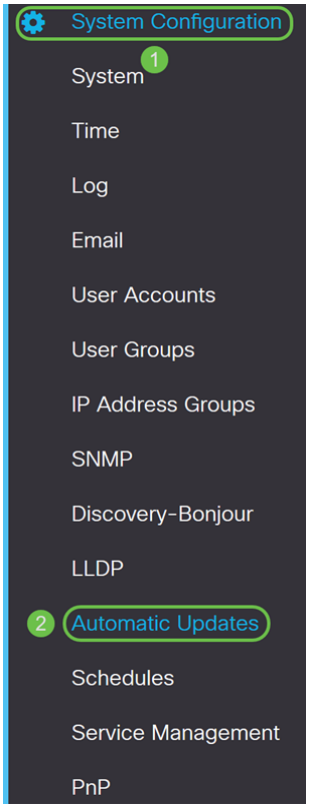
Schritt 1: Um IPS-Definitionen manuell zu aktualisieren, navigieren Sie zu **Administration > File Management**.




Schritt 2: Blättern Sie auf der Seite *Dateiverwaltung* nach unten zum Abschnitt *Manuelle Aktualisierung*. Wählen Sie **Signaturdatei** als *Dateityp* und **cisco.com** zum *Upgrade von aus*. Drücken Sie anschließend **Upgrade**. Dadurch wird die neueste Sicherheitssignatur heruntergeladen und installiert.

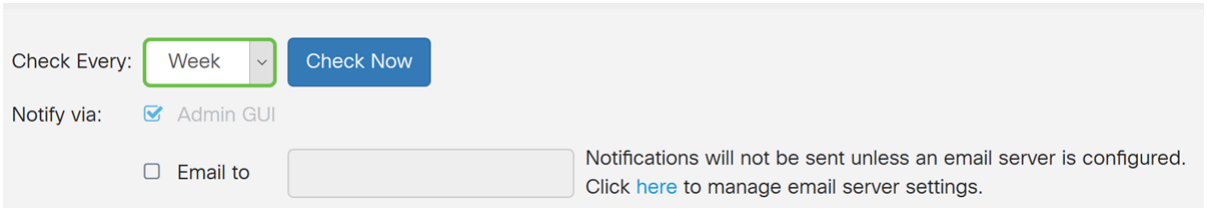



Schritt 3: Um die IPS-Definitionen automatisch zu aktualisieren, navigieren Sie zu **Systemkonfiguration > Automatische Updates**.

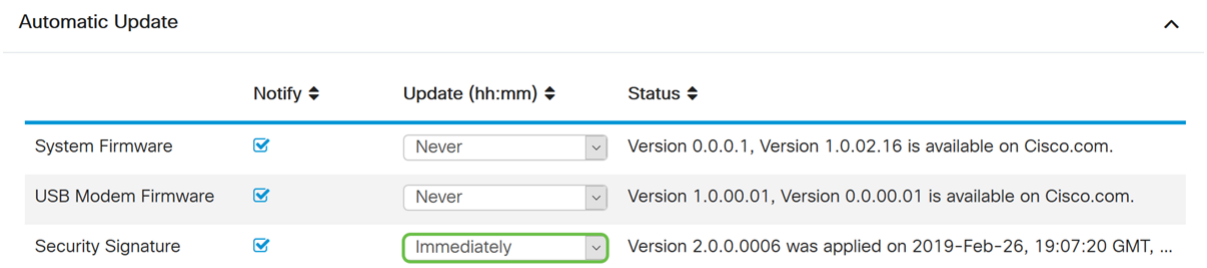



Schritt 4: Die Seite *Automatische Updates* wird geöffnet. Sie haben die Möglichkeit, wöchentlich oder monatlich nach Updates zu suchen. Sie können den Router per E-Mail oder über die Webbenutzeroberfläche benachrichtigen lassen. In diesem Beispiel wird jede Woche eine Überprüfung ausgewählt.

**Anmerkung:** Es wird empfohlen, Sicherheitssignaturen wöchentlich automatisch zu aktualisieren.



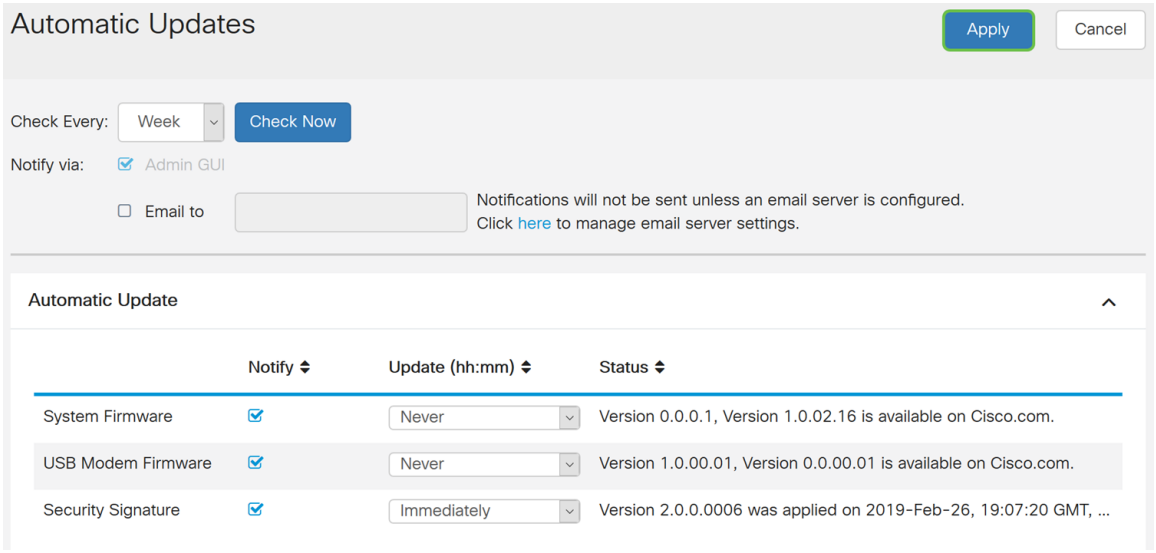

Schritt 5: Blättern Sie nach unten zum Abschnitt *Automatische Aktualisierung*, und suchen Sie das Feld *Sicherheitssignatur*. Wählen Sie in der Dropdown-Liste *Sicherheitssignaturaktualisierung* die Uhrzeit aus, zu der Sie die automatische Aktualisierung durchführen möchten. In diesem Beispiel wählen Sie **Sofort** aus.




Schritt 6: Klicken Sie auf **Apply**, um die Änderungen in der aktuellen Konfigurationsdatei zu speichern.

**Anmerkung:** Denken Sie daran, auf das Symbol **Diskette** oben zu klicken, um zur Seite *Konfigurationsverwaltung* zu navigieren, um die aktuelle Konfigurationsdatei in die Startkonfigurationsdatei zu kopieren. Dadurch können Sie Ihre Konfigurationen zwischen

Neustarts beibehalten.




# Schlussfolgerung

Sie sollten jetzt das Intrusion Prevention System auf dem Router der Serie RV34x erfolgreich konfiguriert haben.