# Inbraakpreventiesysteem configureren op de RV34x Series router

## Doel

Het doel van dit document is om u te tonen hoe u het Inbraakpreventiesysteem (IPS) op RV34x Series routers kunt configureren.

## Inleiding

Het Inbraakpreventiesysteem scant verkeer om bekende aanvalspatronen te zoeken om te blokkeren. Het kijkt pakketten en sessies terwijl zij door de router lopen en scant elk pakje om een van de IPS-handtekeningen van Cisco aan te passen. Wanneer verdachte activiteit wordt gedetecteerd, wordt deze ontworpen om te loggen of te blokkeren. Het is belangrijk de IPS- en antivirusdatabases en -definities bij te werken. Deze kunnen handmatig of automatisch worden bijgewerkt.

Bekijk deze video's op Cisco Inbraakpreventiesysteem:

IPS kan echter van invloed zijn op de prestaties van de router. In het algemeen heeft dit geen invloed op de totale doorvoersnelheid voor Hypertext Transfer Protocol (HTTP)- en File Transfer Protocol (FTP)-verkeer, maar het kan het maximale aantal gelijktijdige verbindingen ietwat dramatisch verminderen.

**Belangrijke opmerking:** Als de router momenteel onder een zware werklast ligt, kan dit de kwestie verscherpen.

De onderstaande tabel geeft de verwachte prestaties in verschillende configuraties. Deze waarden dienen als leidraad te worden gebruikt, aangezien de reële prestaties in de wereld kunnen verschillen als gevolg van een aantal factoren.

| | Gelijktijdige verbindingen | verbindingssnelheid | HTTP-doorvoersnelheid | FTP-doorvoersnelheid |
|---|---|---|---|---|
| Standaard instellingen | 40000 | 3000 | 982 MB/sec | 981 MB/sec |
| APP-regeling inschakelen | 15000-16000 | 1300 | 982 MB/sec | 981 MB/sec |
| Antivirus inschakelen | 16000 | 1500 | 982 MB/sec | 981 MB/sec |
| **IPS inschakelen** | **17000** | **1300** | **982 MB/sec** | **981 MB/sec** |
| Toepassingscontrole | 15000-16000 | 1000 | 982 MB/sec | 981 MB/sec |

| | | | | |
|---|---|---|---|---|
| voor antivirus en IPS inschakelen | | | | |

De volgende velden zijn gedefinieerd als:

**Gelijktijdige verbindingen** - het totale aantal gelijktijdige verbindingen. Als u bijvoorbeeld een bestand van één site downloaden, is dat één verbinding, streaming audio van Spotify die een andere verbinding zal zijn, maakt het twee gelijktijdige verbindingen.

**verbindingssnelheid** - Het aantal aansluitingen verzoek / seconde dat het kan verwerken.

**HTTP/FTP-doorvoersnelheid** - de HTTP- en FTP-doorvoersnelheid zijn de downloadsnelheden in MB/sec.

Security licenties zijn bijgewerkt om IPS-bescherming te bieden naast bestaande toepassing en webfiltering. Om een beveiligingslicentie te hebben, is een slimme account vereist. Als u nog geen actieve slimme account hebt, is sectie 1 van dit document vereist.

Klik hier om te leren hoe u Antivirus op RV34x kunt configureren.

## Toepasselijke apparaten

RV34x

## Softwareversie

1.0.03.x

## Inhoud

# Smart Licensing

Als u geen actieve slimme account hebt, dient u de onderstaande stappen te volgen.

Als u problemen of problemen hebt bij het configureren van uw Smart License account, helpt ons ondersteuningsteam potentiële problemen op te lossen en kan dit via meerdere methoden worden bereikt. Voel je vrij om je favoriete methode te gebruiken om te proberen.

**Routercommunity:** Cisco-ondersteuningscommunity voor MKB

**FAQ over RV34x Series:** RV340x Series routerPAQ's

**Smart License Overzicht:** Smart Software Licensing

**FAQ over slimme licenties:** Smart Licensing en Smart Account FAQ voor partners, distributeurs en klanten

**Een case indienen:** Support Case Manager

**Telefoonnummer voor ondersteuning door de VS/Canada:** 1-866-606-1866 voor contactgegevens met MKB TAC

**E-mail met licenties:** licensing@cisco.com

Stap 1. Als u uw Cisco.com-account onlangs hebt gemaakt of bezocht, wordt u door een bericht begroet om uw eigen Smart License account te maken. Als u dat niet hebt gedaan, kunt u hier klikken om naar de pagina met de maken van de Smart Licentie-account te gaan. Mogelijk moet u inloggen.

**Opmerking:** Klik hier voor meer informatie over de stappen die nodig zijn om uw slimme account aan te vragen.


Stap 2. Wanneer u een slimme licentie voor een router aanschaft, moet de verkoper een proces uitvoeren om de unieke licentie-ID naar uw Smart Licentieaccount te verplaatsen. Hieronder volgt een overzicht van de noodzakelijke informatie die zal worden gevraagd bij de aankoop van de bundels.

**Opmerking:** IPS en Antivirus maken deel uit van de beveiligingslicentie die wordt gebruikt voor webfiltering en toepassingsfiltering.

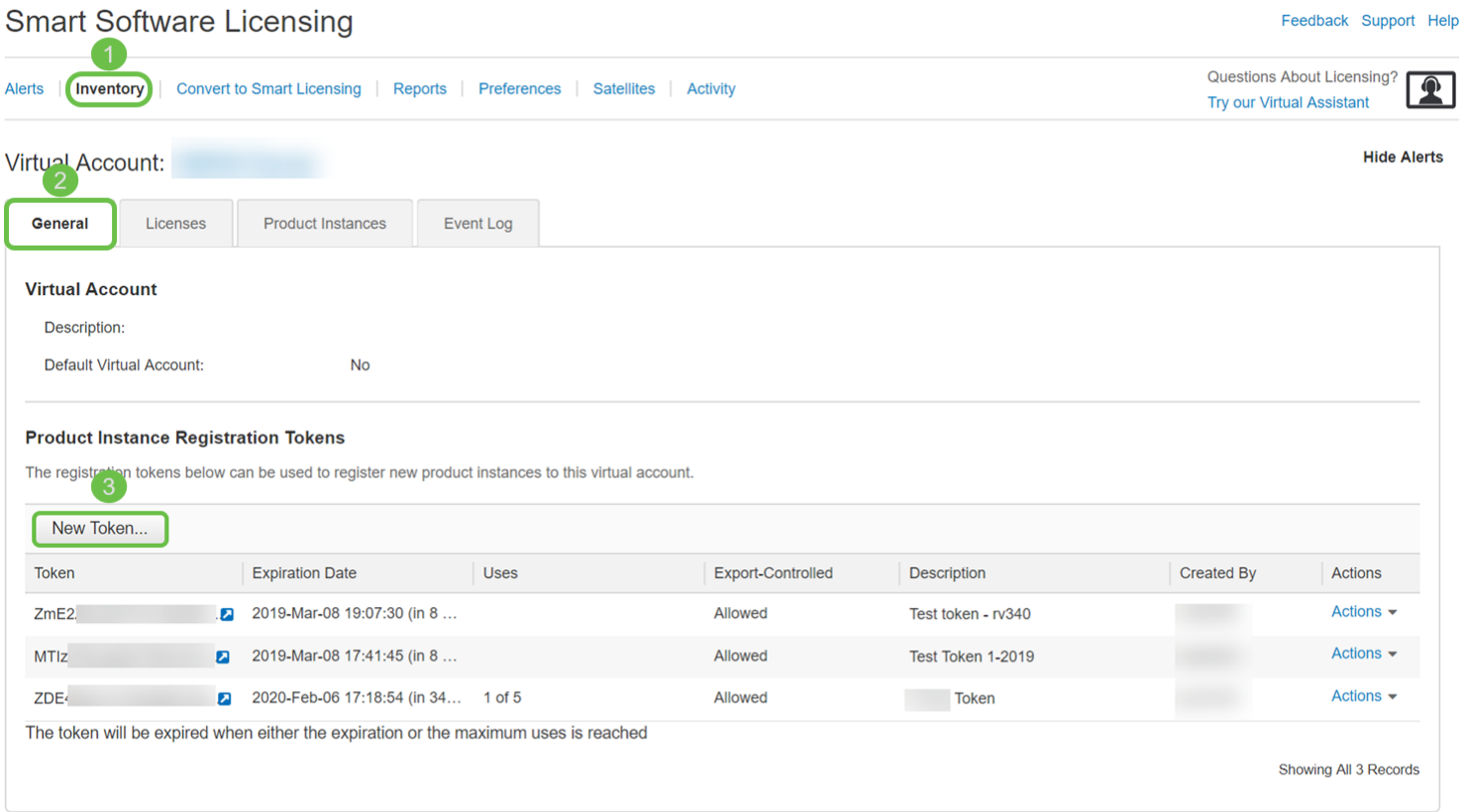
| Vereiste informatie | De informatie lokaliseren |
|---|---|
| Cisco.com gebruikers-id | Plaatsing in uw accountprofiel, of u kunt hier klikken. |

| | |
|---|---|
| Naam van slimme licentieserver | U kunt het beste uw slimme account maken voordat u de licentie aanschaft. Dit dient stap 8 van het artikel Smart License Account Creation te zijn. |
| Smart License SKU | De productidentificatiecode van het hulpmiddel. Ex. RV340-K9-NA |

**Opmerking:** Als u een licentie hebt aangeschaft en deze niet op uw virtuele account voorkomt, dient u contact op te nemen met de wederverkoper om te vragen of u de overdracht wilt uitvoeren of ons te bereiken.

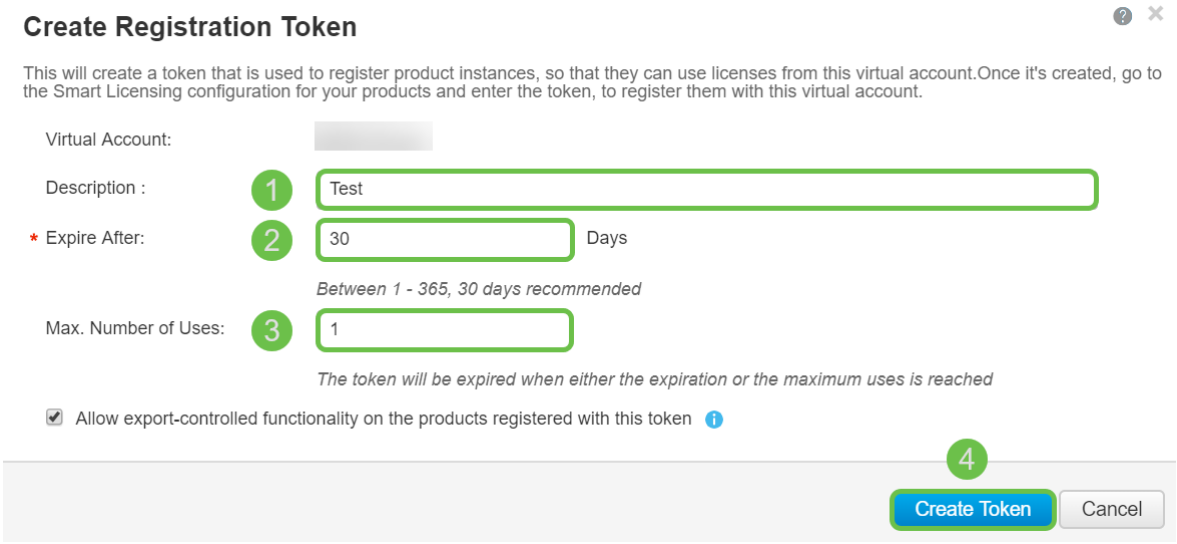
Als u het proces zo snel mogelijk wilt maken, moet u uw Licentienummer, Cisco-verkooporder nummer en een screenshot van uw pagina met Licentie voor slimme account (om met ons team te delen) hebben.

Stap 3. Voor het genereren van een token, dient u te navigeren naar uw Smart Software License account. Klik vervolgens op **Voorwas > tabblad Algemeen**. Klik op de knop **New Token...**.

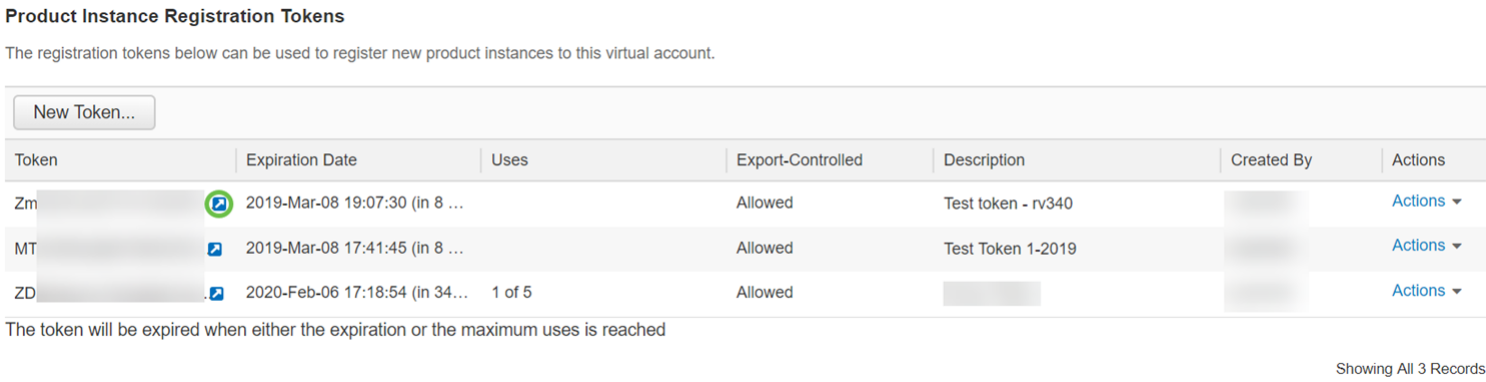



Stap 4. Het venster *Registratie Token maken* wordt geopend. Voer een *omschrijving in*, *verlopen na*, en *Max. Aantal gebruikers*. Druk vervolgens op de knop **Token maken**.

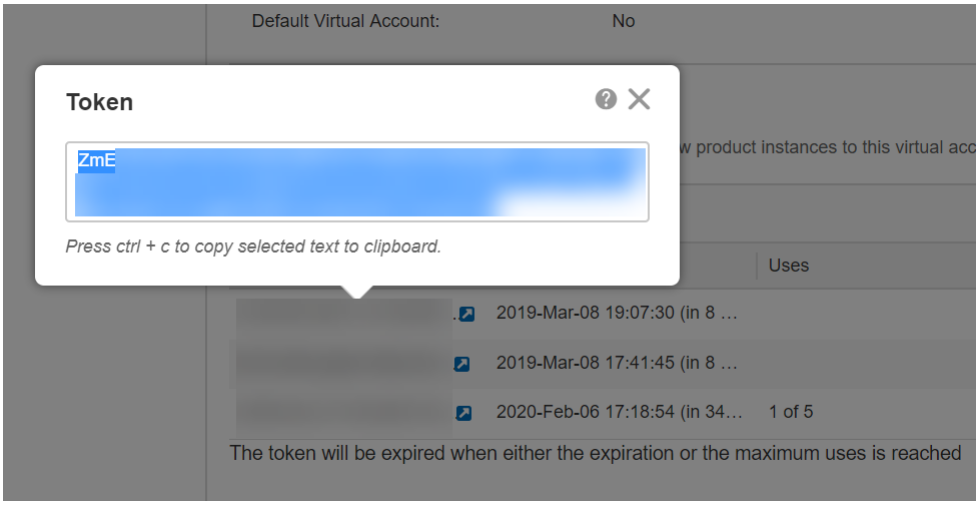
**Opmerking:** 30 dagen voor *verloop Na* aanbevolen.



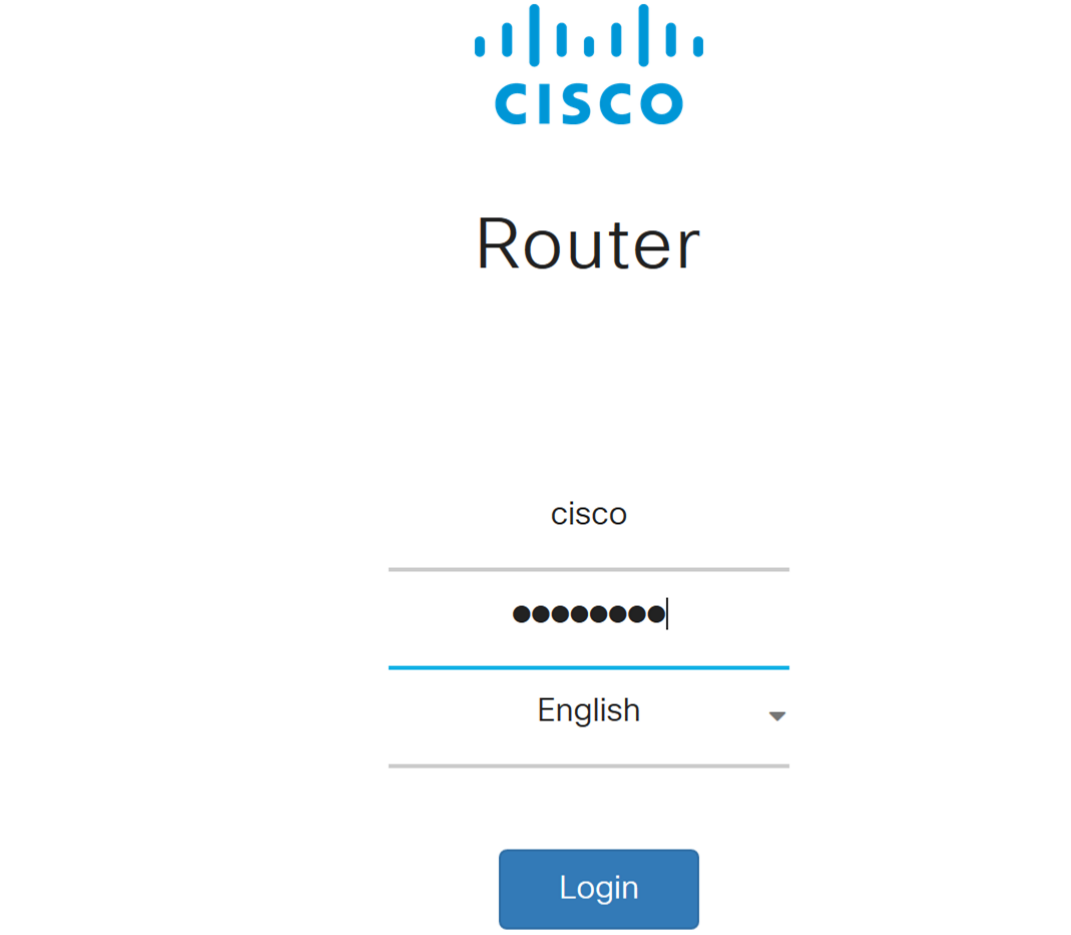

Stap 5. Zodra het token gegenereerd is, kunt u op de knop **Token Link (Blauw-vakje met een witte pijl)** rechts van uw recent gemaakte token klikken.



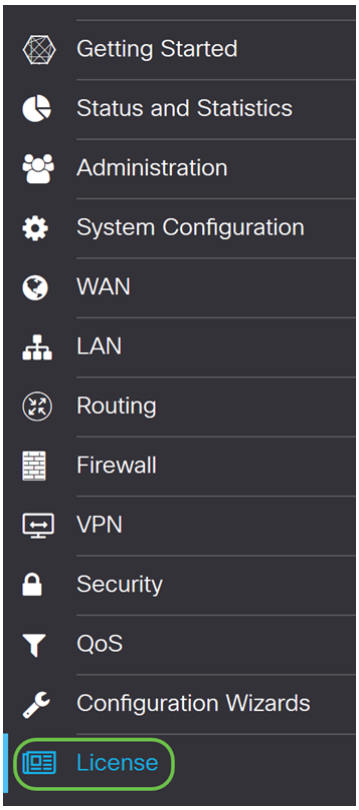

Stap 6. Een *Token*-venster moet met het volledige token worden weergegeven zodat u het kunt kopiëren. Markeer het token, klik met de rechtermuisknop op het token en klik op **Kopie** of u kunt de knop Ctrl op het toetsenbord ingedrukt houden en **c** tegelijkertijd klikken om de tekst te kopiëren.




Stap 7. Zodra u uw token hebt gekopieerd, zult u in het apparaat moeten loggen en de pentopentoets moeten uploaden. Meld u aan bij de webconfiguratie van de router.

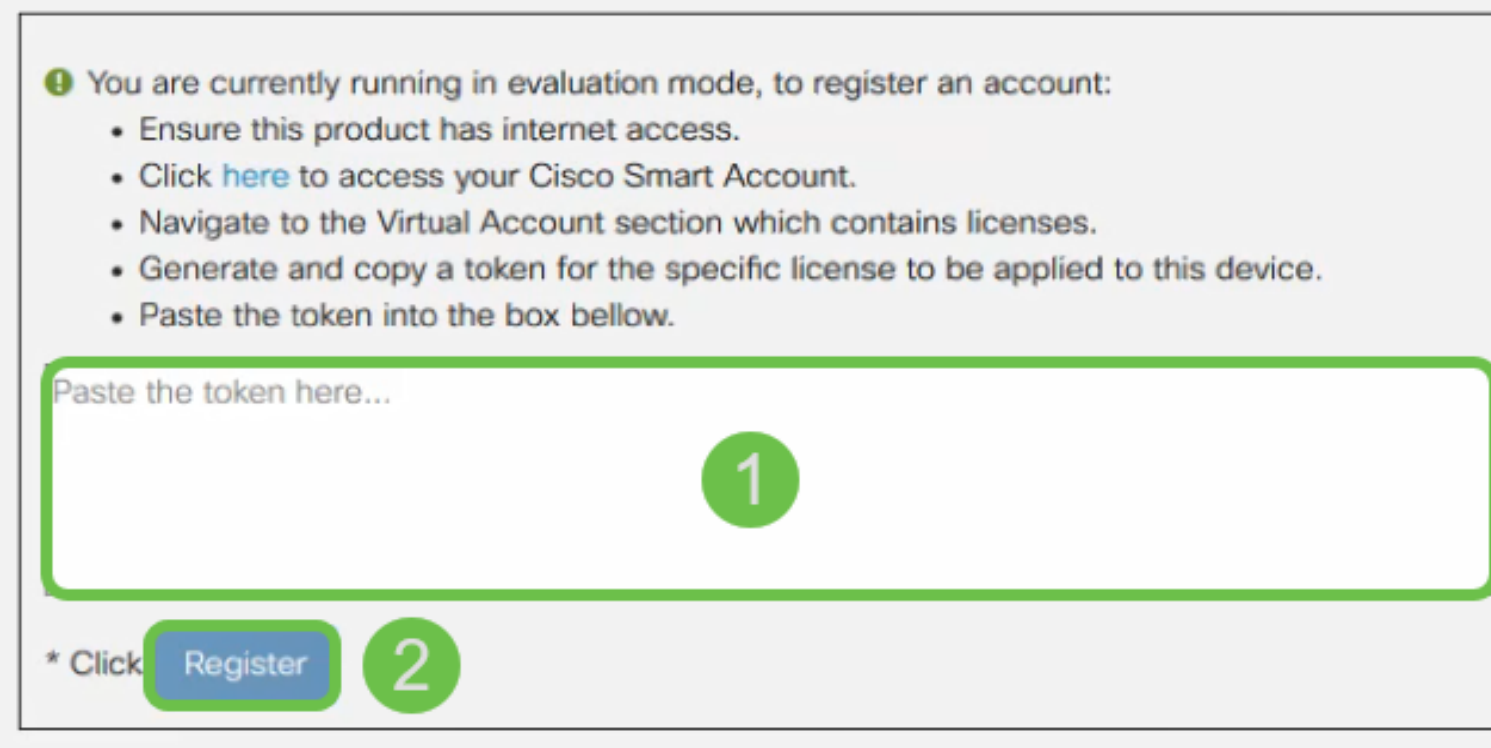



Stap 8. Navigeer naar **Licentie.**

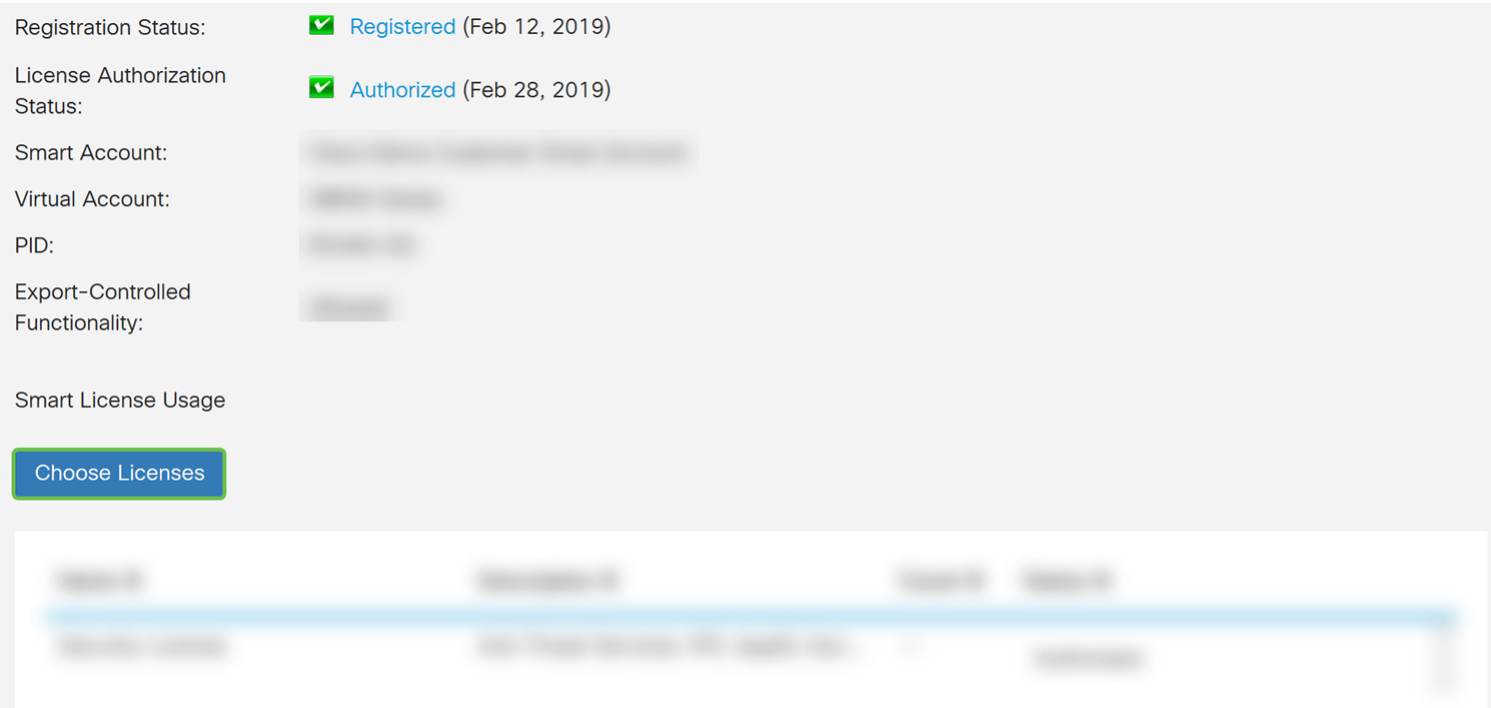


Stap 9. Als uw apparaat niet is geregistreerd, wordt de *licentiestatus* van uw *apparaat* weergegeven in de *evaluatiemodus*. Plakt het token (Stap 6 van deze sectie) die u gegenereerd hebt vanuit de pagina *Smart Licensing Manager*. Klik vervolgens op **Registreren**.

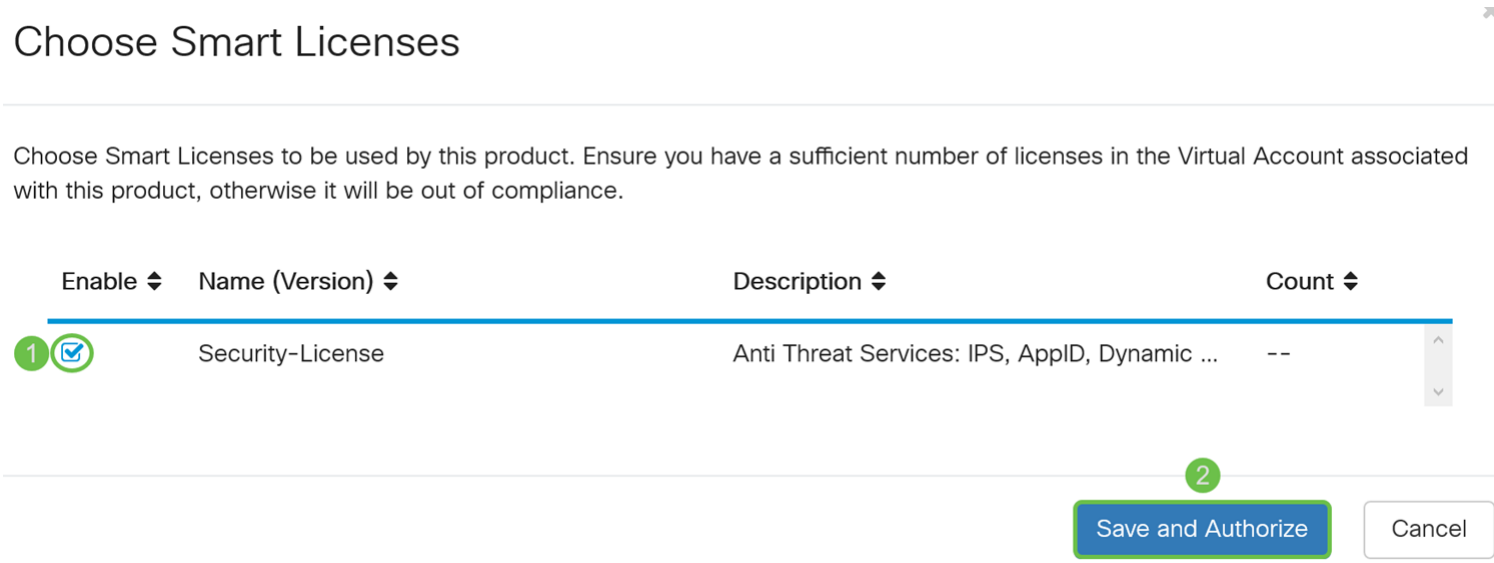
**Opmerking:** Het registratieproces kan enige tijd in beslag nemen. Wacht tot het proces is voltooid.



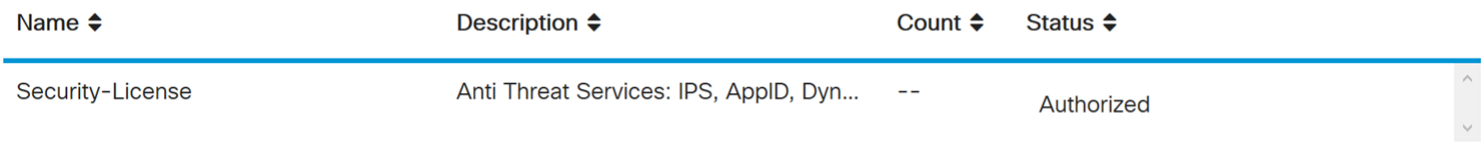

Stap 10. Zodra het token is geregistreerd, moet u de licentie toewijzen. Klik op de knop **Licenties kiezen**.




Stap 1. Het venster *Smart Licenties* kiezen moet worden weergegeven. Controleer de **Security-licentie** en druk vervolgens op **Opslaan en autoriseren**.



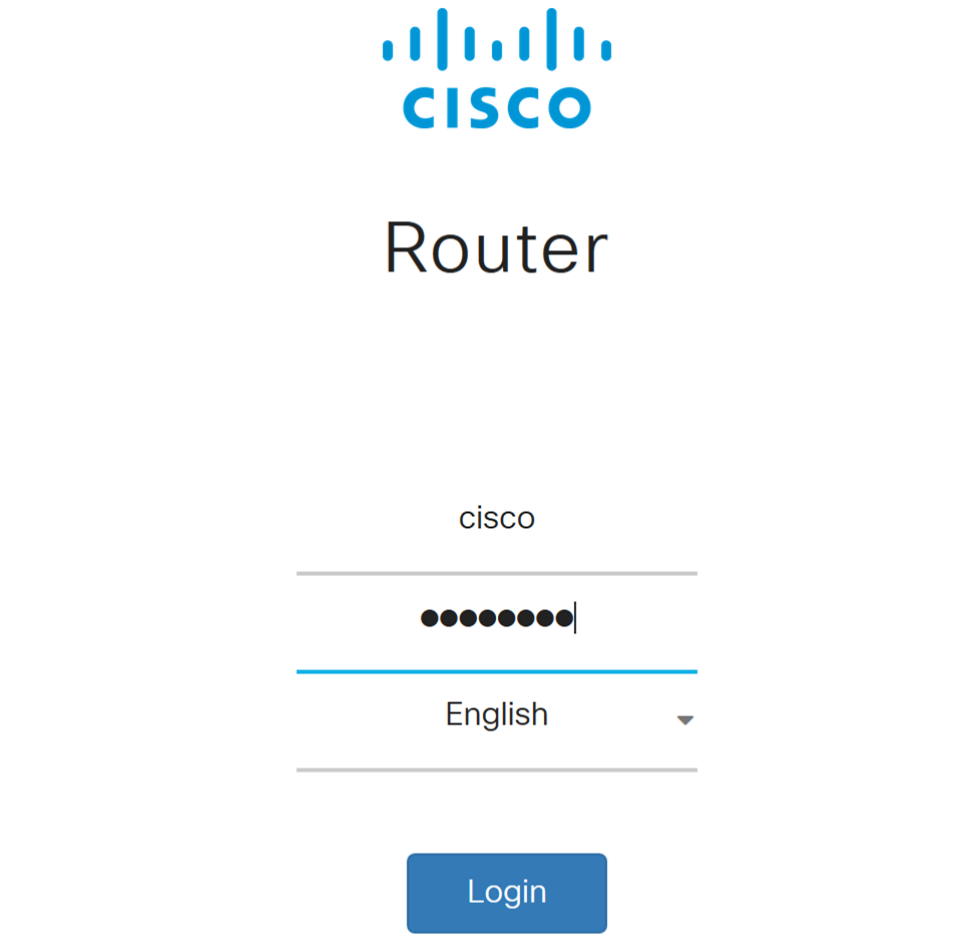

Stap 12. De *status* van uw security-licentie moet nu *worden* geautoriseerd.



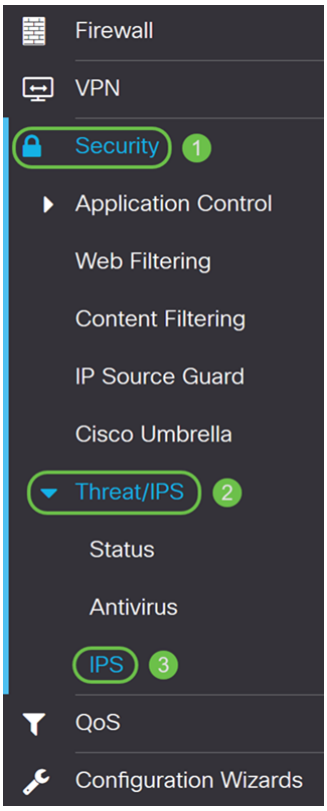

U moet nu kunnen doorgaan met het configureren van inbraakpreventiesysteem.

# Inbraakpreventiesysteem configureren

Stap 1. Als u nog niet in de router hebt ingelogd, logt u in op de webconfiguratie van de router.

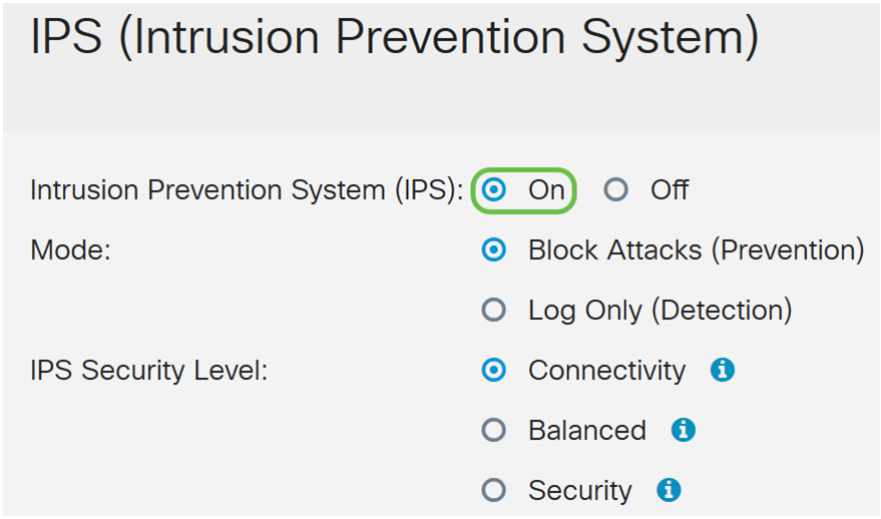



Stap 2. Navigeer naar **security > bedreigingen/IPS > IPS**.



Stap 3. Selecteer **Aan** om de functie Inbraakpreventiesysteem in te schakelen. Als u de functie wilt uitschakelen, selecteert u **Uit**.

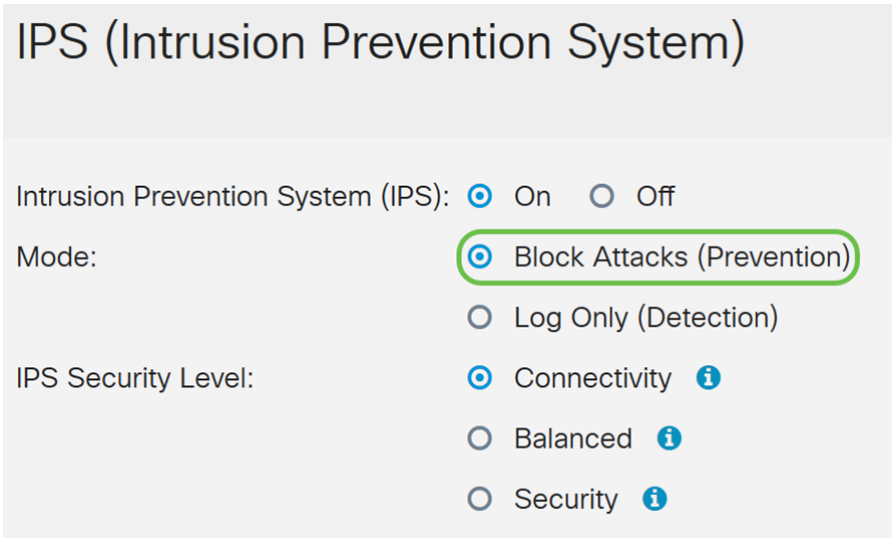
We zullen in dit voorbeeld **On** selecteren.




Stap 4. Selecteer **Blokkingsaanvallen (preventie)** of **alleen** voor **Log**. In dit voorbeeld selecteren we **Blokaanvallen (Preventie)**. De volgende opties worden hieronder gedefinieerd.

**Blokaanvallen (preventief)** - selecteer dit om alle aanvallen te blokkeren. Het registreert ook de anomalie.

**Alleen loggen** - Met deze optie wordt alleen het logbestand gegenereerd (met informatie over de client, handtekening, enzovoort) wanneer de anomalieën worden geïdentificeerd. Het heeft geen invloed op de verbinding.




Stap 5. Selecteer het IPS-beveiligingsniveau dat u wilt gebruiken. De volgende opties zijn gedefinieerd als:

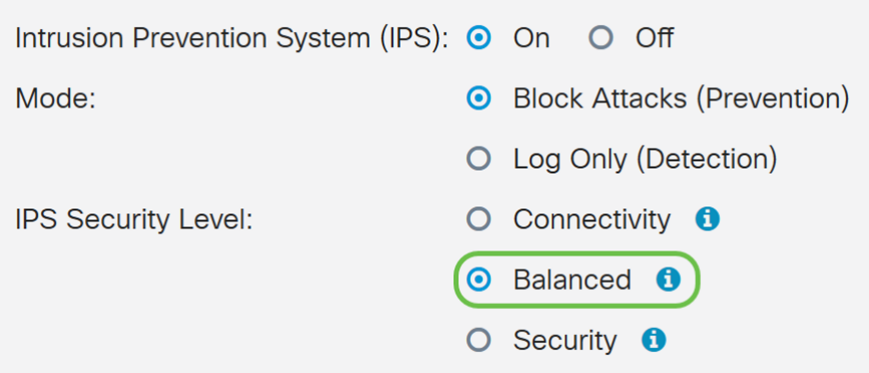
**Connectiviteit** - In deze modus worden de meest kritische aanvallen gedetecteerd. Dit biedt de minste bescherming: alleen (hoge ernst) risicoaanvallen worden gedetecteerd. Dit is de minst veilige optie.

Balanceerd - De geselecteerde modus detecteert ernstige aanvallen samen met de kritische aanvallen. Dit biedt middelmatige bescherming: (hoge + gemiddelde ernst) worden geïnspecteerd door middel van handtekeningen met een laag risico. Dit is beveiliging halverwege voor IPS.

**Beveiliging** - Beveiliging zal de normale aanvallen tegelijkertijd met de ernstige en kritieke aanvallen detecteren. Dit biedt de meeste bescherming: Alle regels (hoog + middelhoog + laag) worden geïnspecteerd. Dit is het hoogste veiligheidsniveau voor IPS.

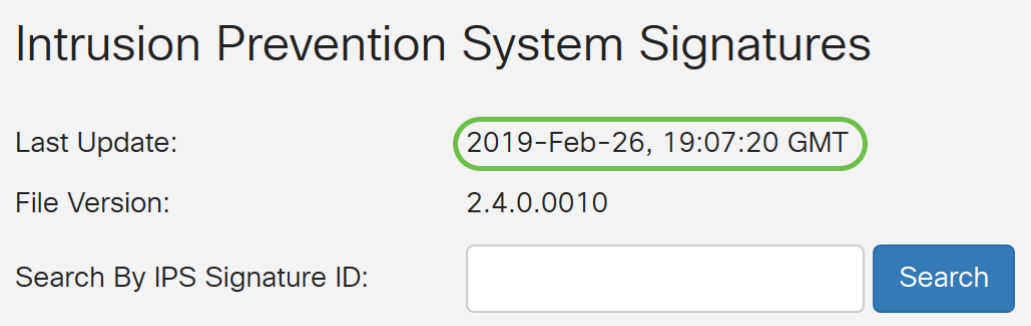
**Opmerking:** Hoe hoger het beveiligingsniveau dat u kiest, hoe meer aanvallen worden bewaakt, hoe groter de impact op de systeemprestaties die mogelijk wordt ervaren.

We kiezen voor deze demonstratie **gebalanceerd**.

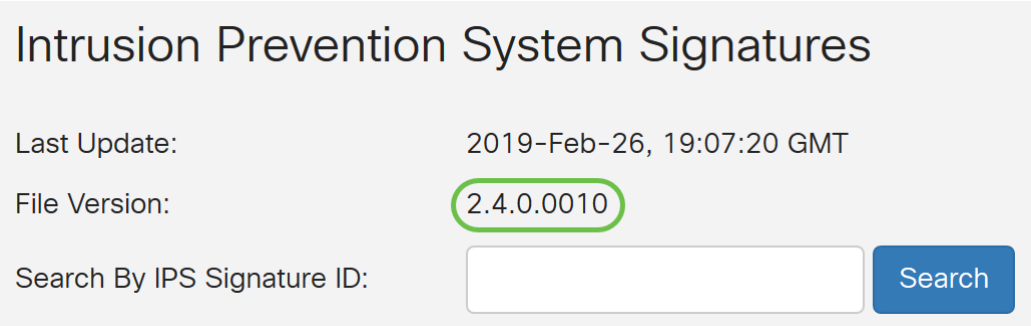



## Inbraakpreventiesysteem-handtekeningen

Stap 6. In het veld *Laatste update* geeft u de datum en het tijdstip van de laatste bijgewerkte handtekening weer.




Stap 7. De *versie van het bestand* geeft de handmatige versie weer die wordt gebruikt.




Stap 8. Om naar een handtekening-ID te zoeken, voert u de **handtekening-ID** in het veld *Zoeken met IPS-handtekeningen* en klikt u op **Zoeken** om te controleren of de handtekening wordt ondersteund. Als de handtekening ID wordt ondersteund, wordt in de tabel het resultaat bijgewerkt zoals hieronder wordt weergegeven.

**Opmerking:** Als de handtekening-ID niet wordt ondersteund, verschijnt er niets in de tabel.


## Signaaltabel met inbraakpreventiesysteem

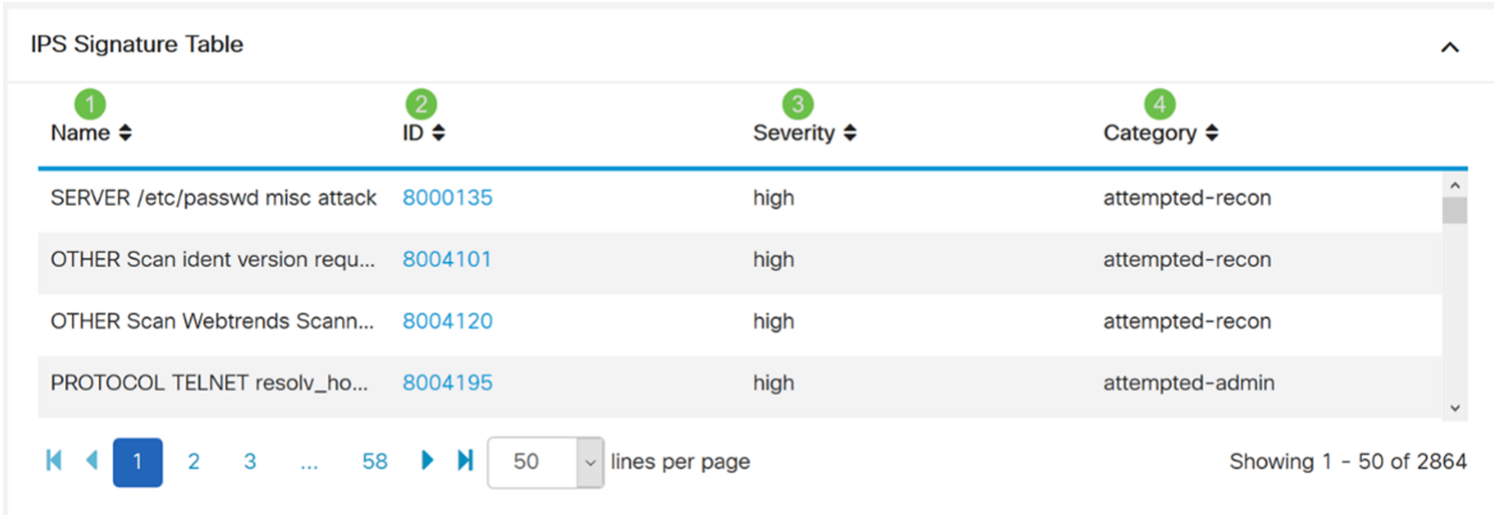
Stap 9. In de *tabel met IPS-handtekeningen* zijn de volgende velden gedefinieerd als:

**Naam** - Naam van de handtekening.

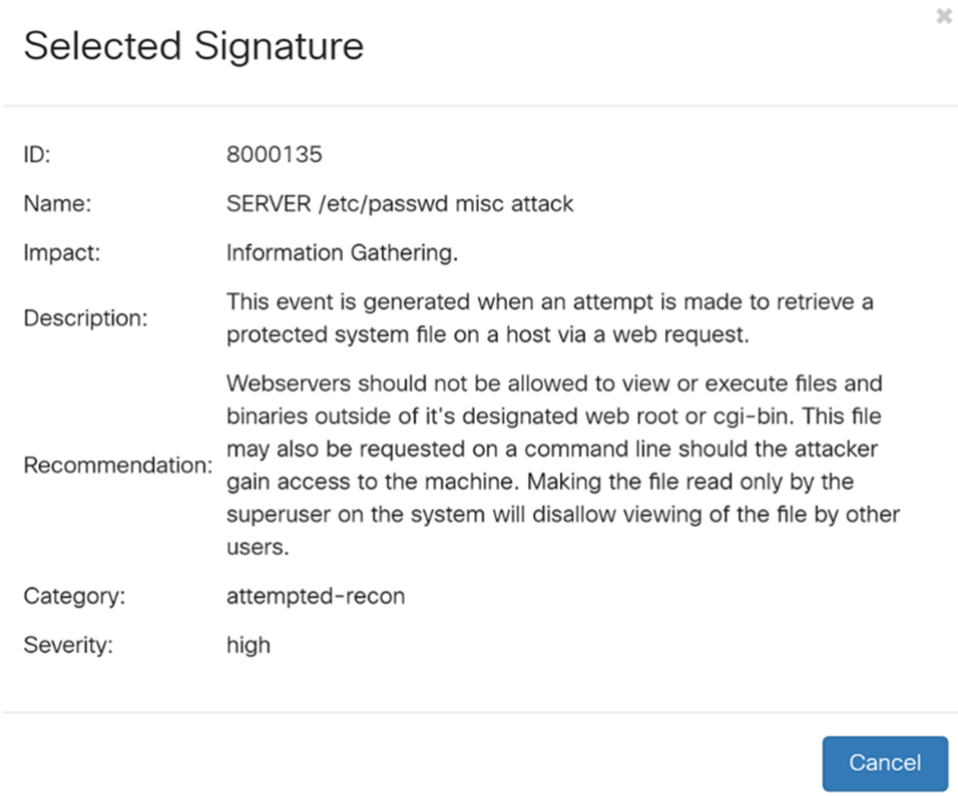
**ID** - het unieke identificatienummer van de handtekening. Als u op de ID klikt, wordt een venster geopend waarmee u de volledige gegevens voor de geselecteerde handtekening kunt bekijken.

**Severity** - Severity Level duidt op de impact op de beveiliging.

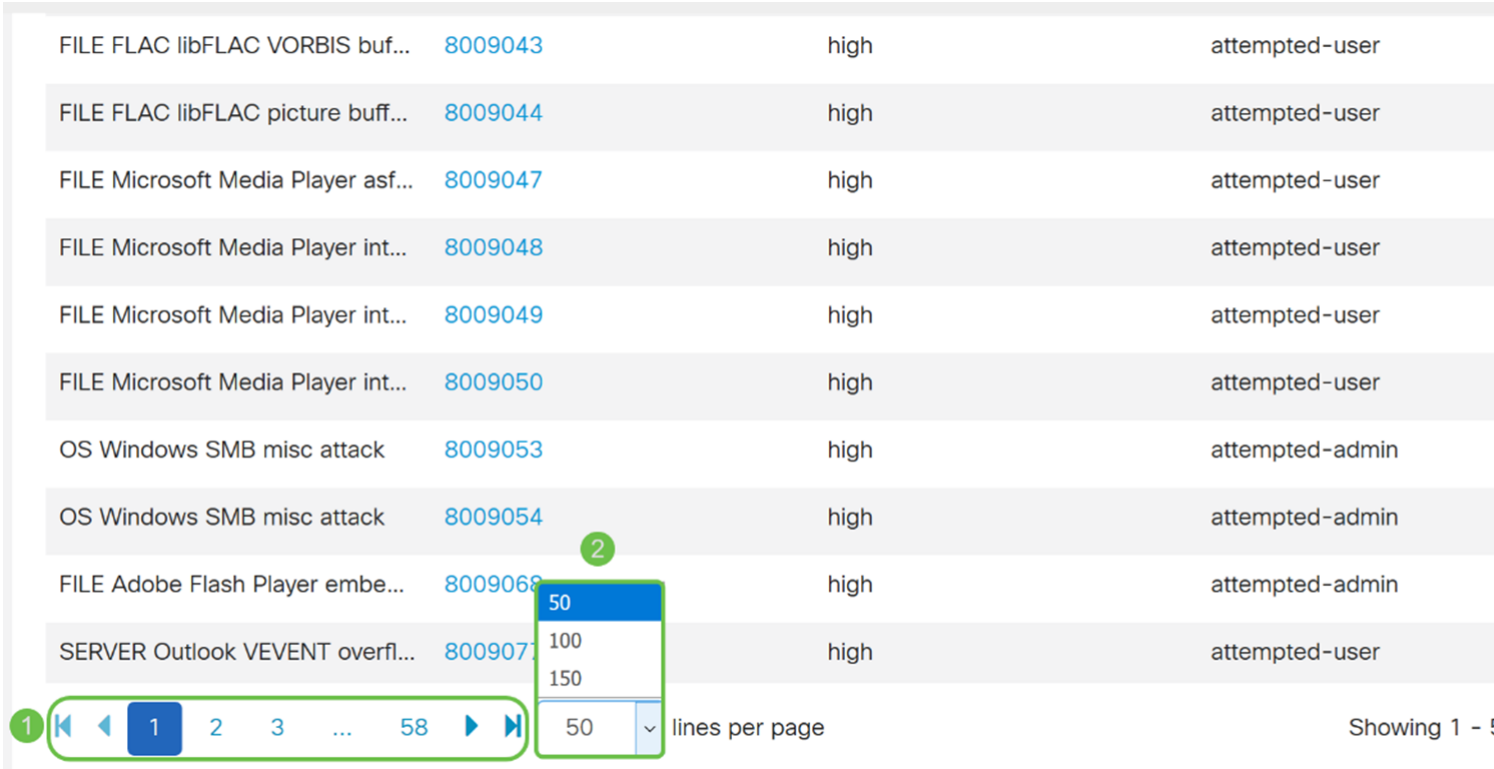
**Categorie** - De categorie waartoe de handtekening behoort.



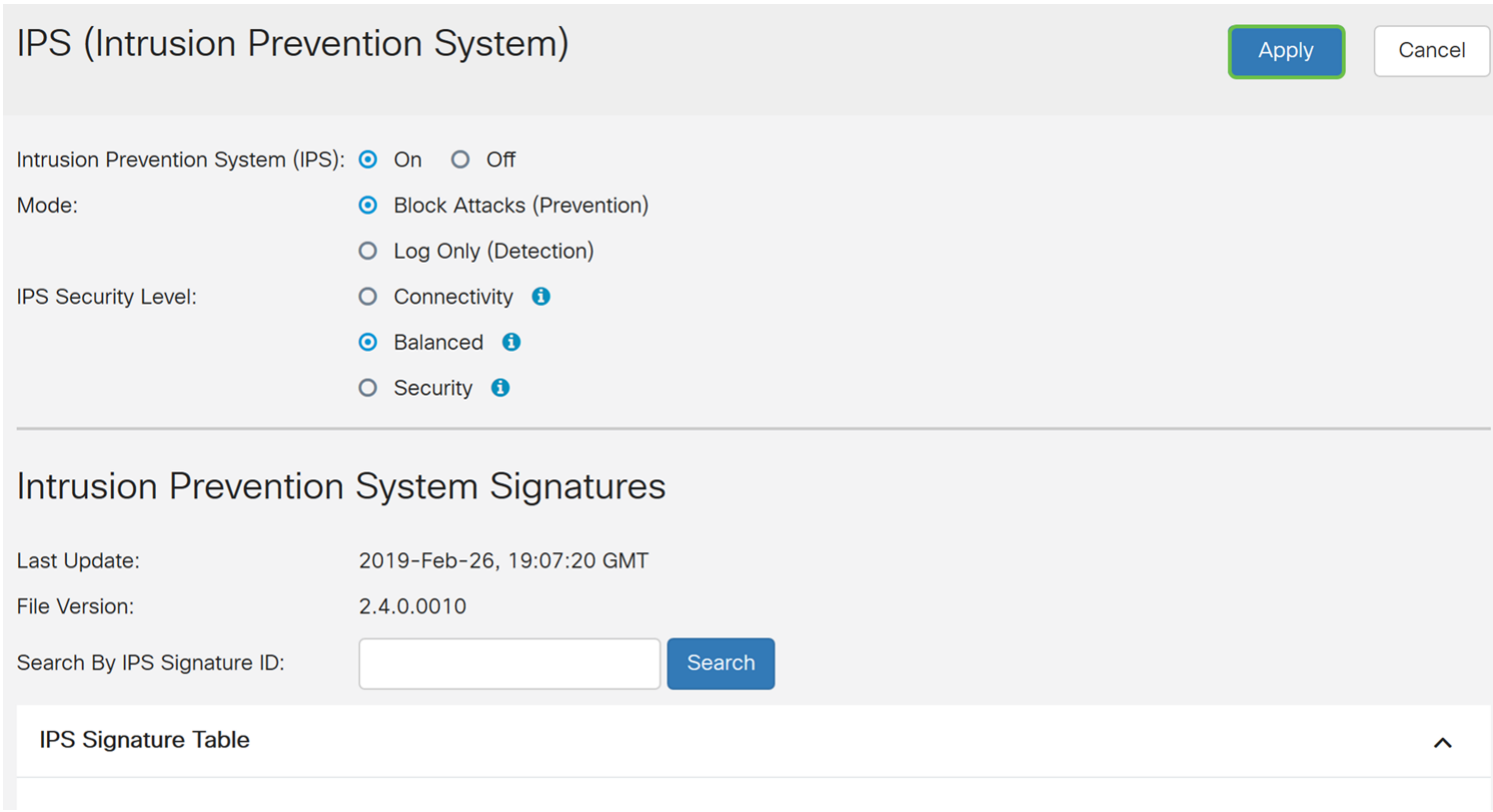

Stap 10. (Optioneel) Als u op de handtekening-ID hebt geklikt in de *tabel met IPS-handtekeningen*, verschijnt een venster om u de volledige details voor de geselecteerde handtekening te tonen.




Stap 1. Onder in de *IPS-handgreep* selecteert u de pijlen en de nummers die u in de tabel wilt navigeren. U kunt ook de hoeveelheid lijnen (**50**, **100** of **150**) per pagina selecteren in de *regels per* vervolgkeuzelijst *pagina*.



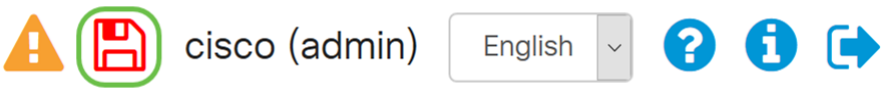

Stap 12. Klik op **Toepassen** om uw wijzigingen in het actieve configuratiebestand op te slaan.



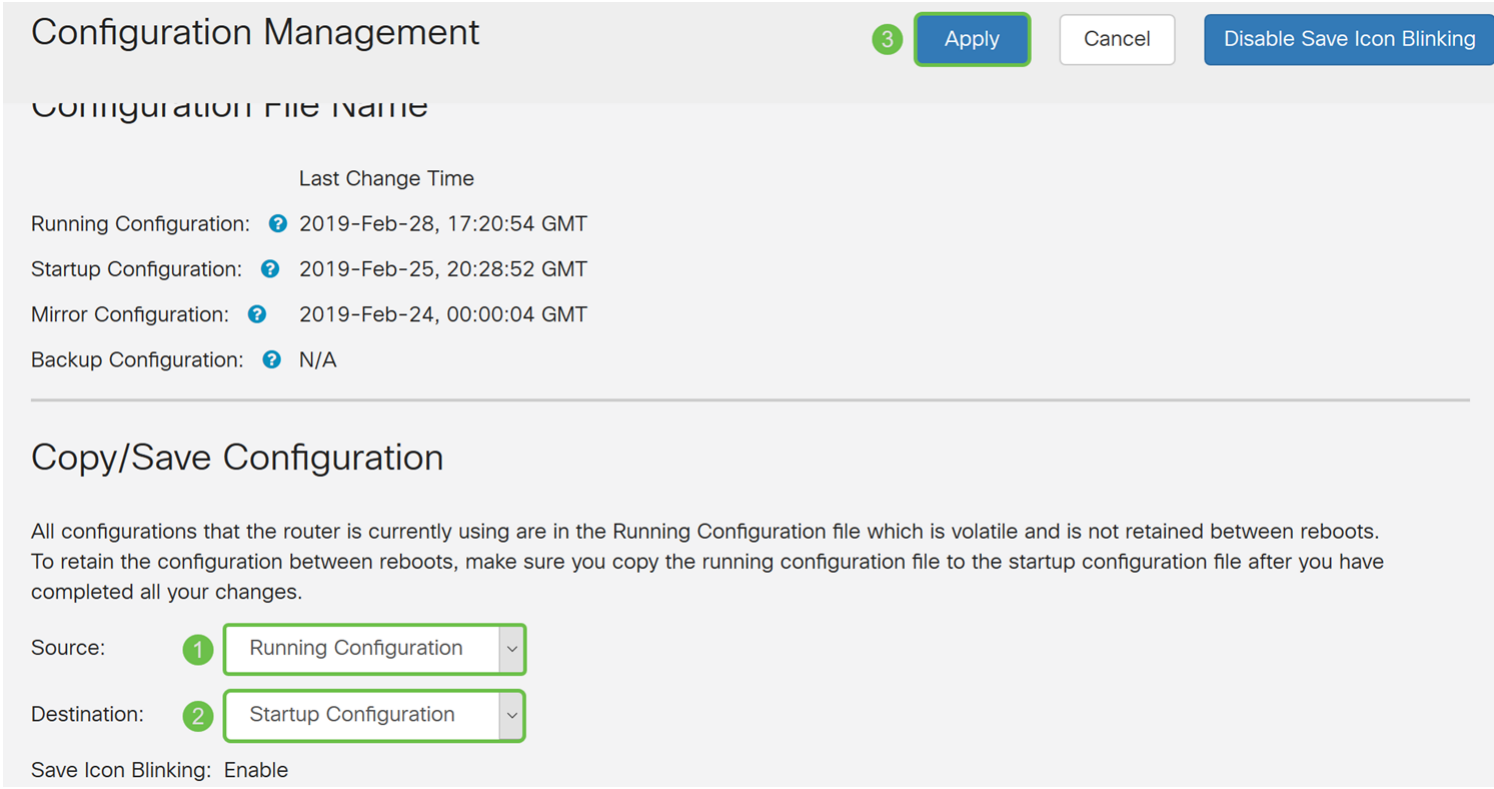

**Opmerking:** Alle configuraties die de router gebruikt zijn momenteel in het actieve configuratiebestand dat vluchtig is en niet tussen reboots behouden blijft. Om de configuratie tussen de herstart te behouden, kopieert u het configuratiebestand van uw actieve configuratie naar het opstartconfiguratiebestand.

In de volgende stappen zullen we u tonen hoe u uw actieve configuratie aan de opstartconfiguratie kunt kopiëren.

Stap 13. Klik op het pictogram **Floppy Disk (Opslaan)** boven op de pagina. Hiermee richt u de *Configuration Management* om uw actieve configuratie in de opstartconfiguratie op te slaan.

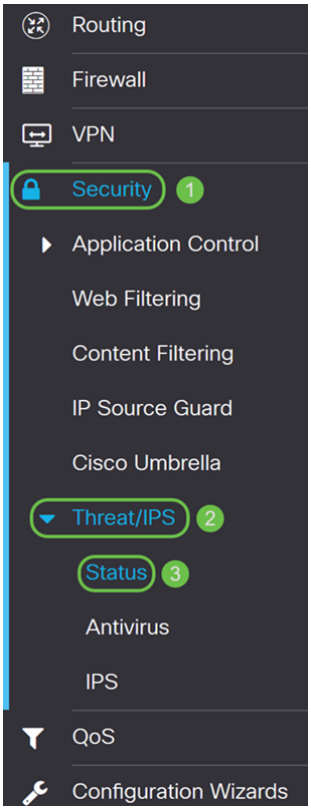



Stap 14. Bij het *Configuratiebeheer* gaat u naar het gedeelte *Kopie/Configuratie opslaan*. Zorg ervoor dat de *bron* **Configuratie** is **uitgevoerd** en dat de *bestemming* **opstartconfiguratie** is. Klik op **Apply** (Toepassen). Dit kopieert het configuratie-bestand naar het opstartconfiguratiebestand om de configuratie tussen de herstart te behouden.

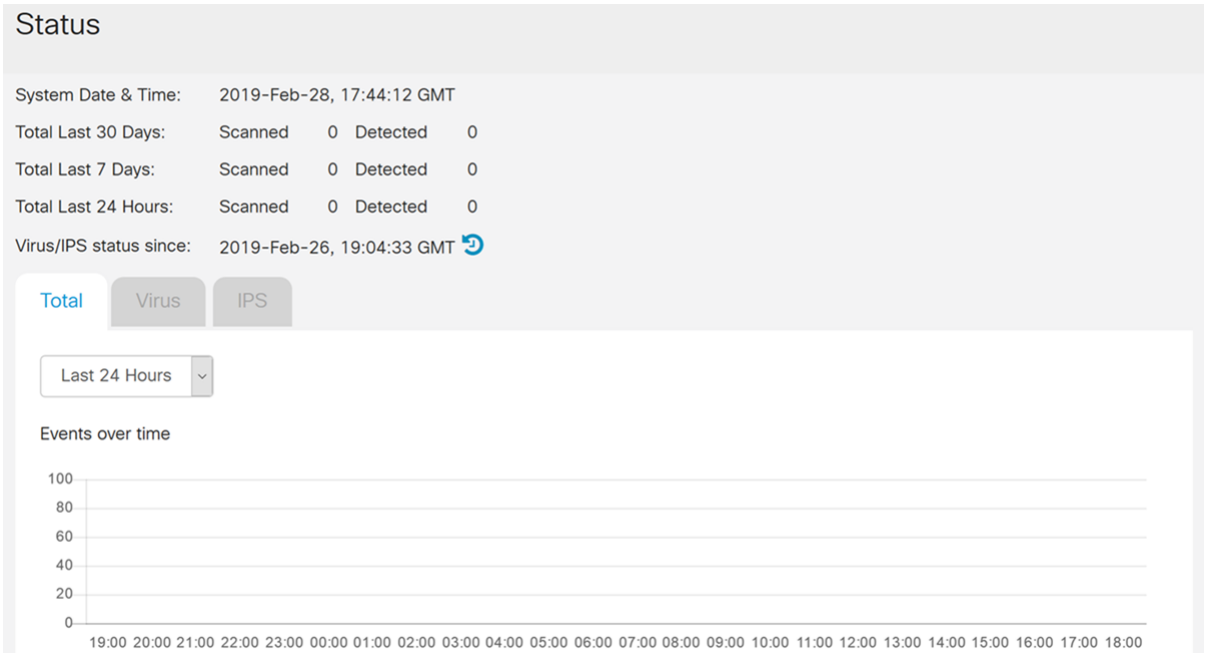



# IPS-status

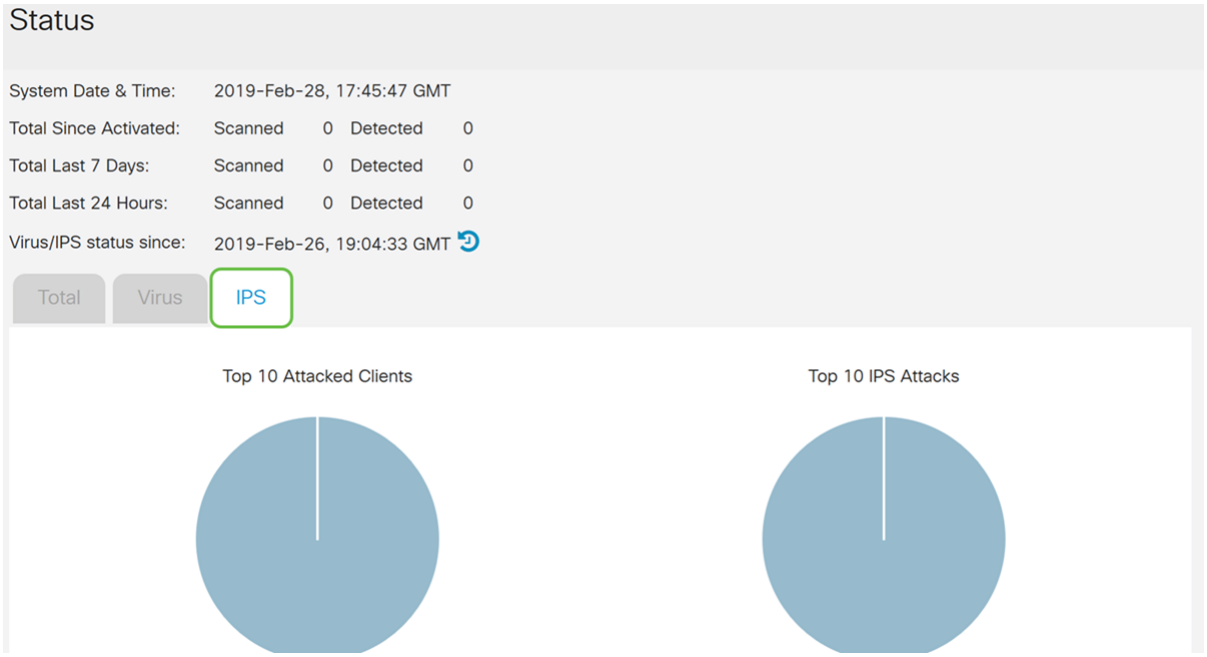
Stap 1. Navigeer naar **Security > Threat/IPS > Status**.




Stap 2. De pagina *Status* geeft de details van de bedreigingen en aanvallen weer wanneer de functies Anti-Threat en IPS zijn geconfigureerd. Het dashboard geeft u een overzicht van de gehele gebeurtenissen, samen met gedetailleerde informatie over bedreigingen en aanvallen die gedetecteerd zijn per selectie zoals dag, week en maand.




Stap 3. Klik op het tabblad **IPS**. Dit zal de top 10 aangevallen cliënten evenals de top 10 IPS aanvallen tonen.

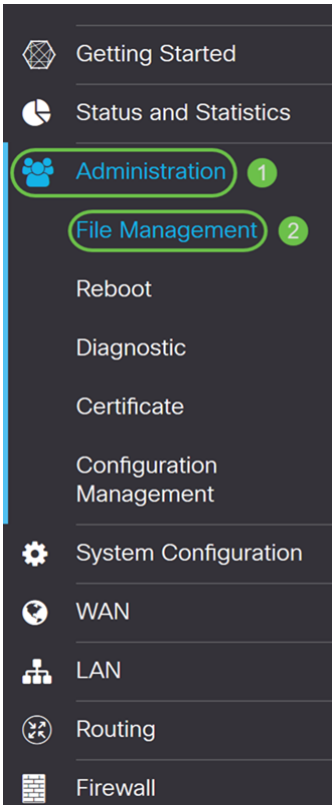



# IPS-definities bijwerken

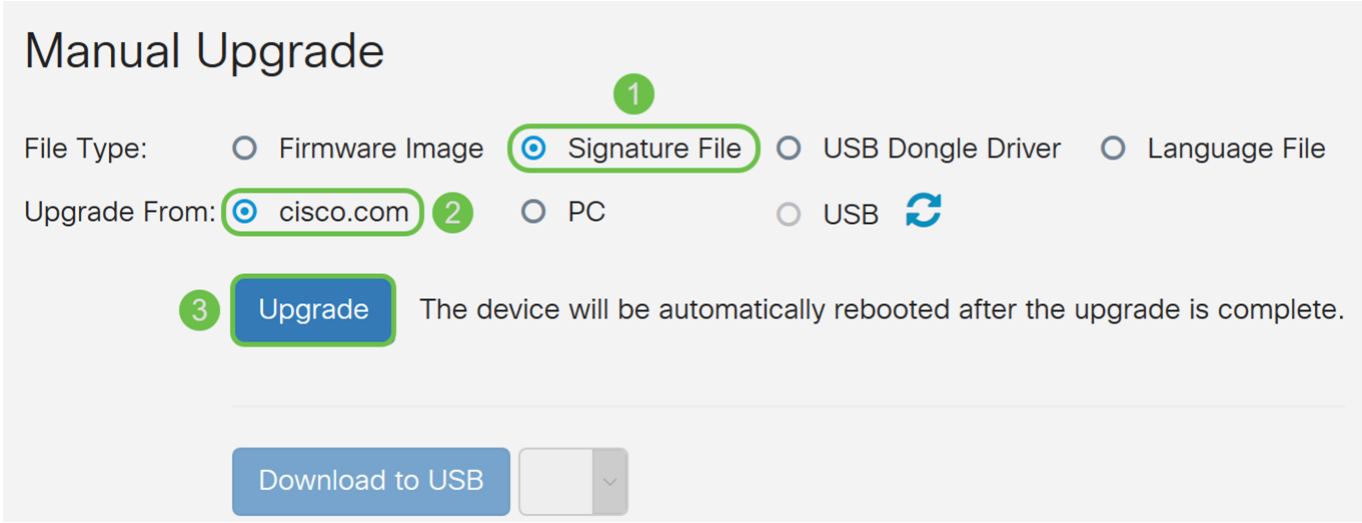
U kunt de IPS-definitie handmatig of automatisch bijwerken. De stappen 1-2 zullen u tonen hoe u de IPS definitie handmatig kunt bijwerken terwijl de Stappen 3-6 u zullen tonen hoe u de IPS definitie automatisch bijwerken.

**Best Practice:** Aanbevolen wordt de veiligheidshandtekeningen wekelijks automatisch bij te werken.

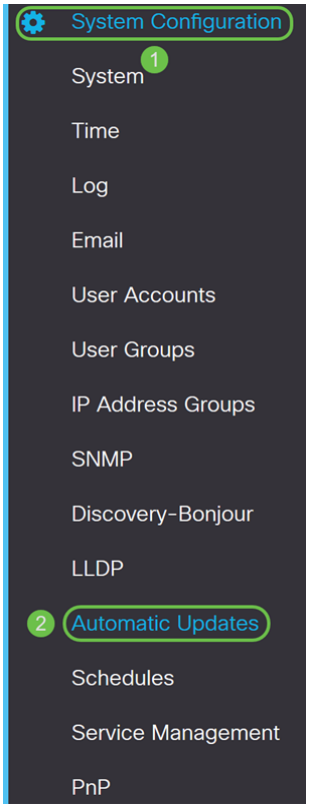
Stap 1. Om IPS-definities handmatig bij te werken, navigeer naar **Beheer > Bestandsbeheer**.




Stap 2. Scrolt naar het gedeelte *Handmatige upgrade* in de pagina *Bestandsbeheer*. Selecteer **Signaalbestand** voor *bestandstype* en **cisco.com** voor *upgrade vanaf*. Druk vervolgens op **upgrade**. Hierdoor kan de laatste veiligheidshandtekening worden gedownload en geïnstalleerd.

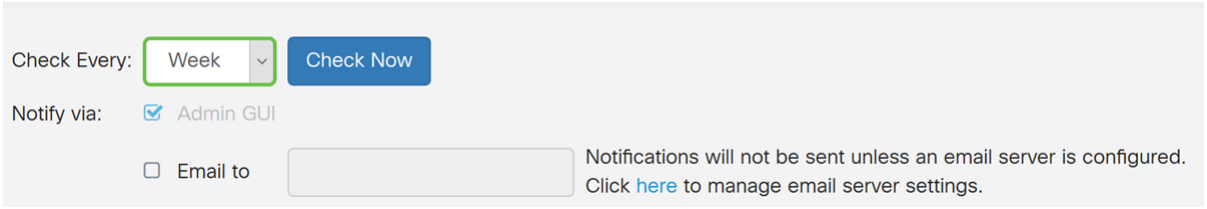



Stap 3. Om de IPS-definities automatisch bij te werken, navigeer dan naar **systeemconfiguratie > Automatische updates**.

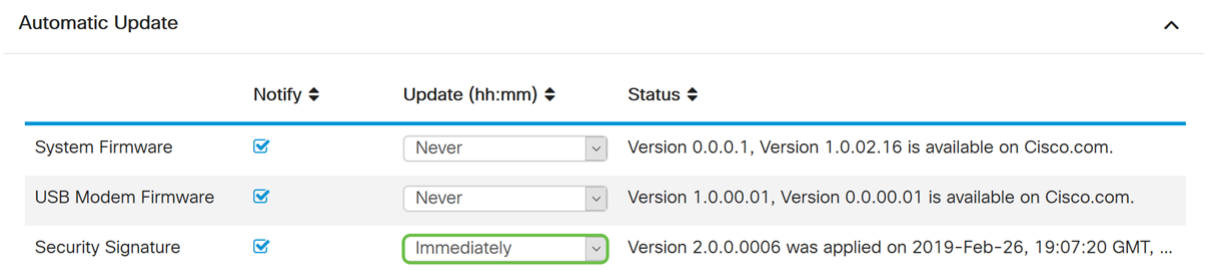



Stap 4. De pagina *Automatische updates* wordt geopend. U hebt de mogelijkheid om de actualiseringen wekelijks of maandelijks te controleren. U kunt de router hebben om via e-mail of het Web UI te melden. In dit voorbeeld zullen wij elke week een controle uitvoeren.

**Opmerking:** Aanbevolen wordt de veiligheidshandtekeningen wekelijks automatisch bij te werken.

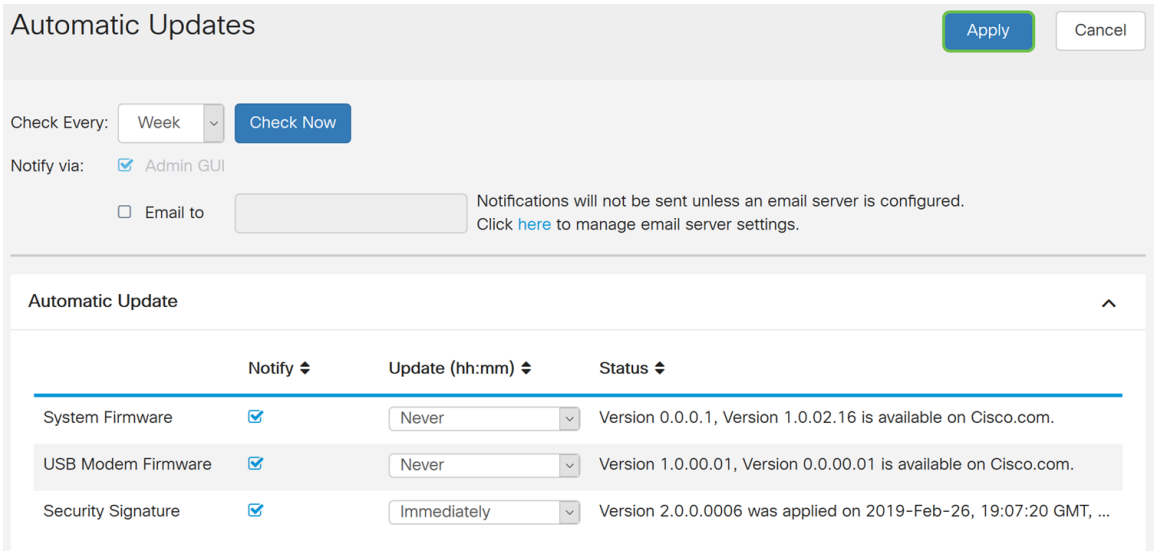



Stap 5. Scrolt naar het gedeelte *Automatische update* en kijk naar het veld *Security Signature*. Selecteer in de vervolgkeuzelijst Security Signature Update de tijd die u automatisch wilt bijwerken. In dit voorbeeld zullen wij **onmiddellijk** kiezen.




Stap 6. Klik op **Toepassen** om de wijzigingen in het actieve configuratiebestand op te slaan.

**Opmerking:** Vergeet niet bovenaan het pictogram **diskette** te klikken om naar de pagina *Configuration Management* te navigeren om uw actieve configuratiebestand naar het opstartconfiguratiebestand te kopiëren. Dit zal helpen om uw configuraties tussen herstart's te behouden.




# Conclusie

U had nu met succes het Inbraakpreventiesysteem op de RV34x-Series router moeten configureren.