

# 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
<b>IPS inschakelen</b>	<b>17000</b>	<b>1300</b>	<b>982 MB/sec</b>	<b>981 MB/sec</b>
Toepassingscontrole	15000-16000	1000	982 MB/sec	981 MB/sec

voor antivirus en IPS inschakele n				
--	--	--	--	--

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

1. [Smart Licensing](#)
2. [Inbraakpreventiesysteem configureren](#)
3. [Inbraakpreventiesysteem-handtekeningen](#)
4. [Signaaltabel met inbraakpreventiesysteem](#)
5. [IPS-status](#)
6. [IPS-definitie bijwerken](#)
7. [Conclusie](#)

# 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](#)

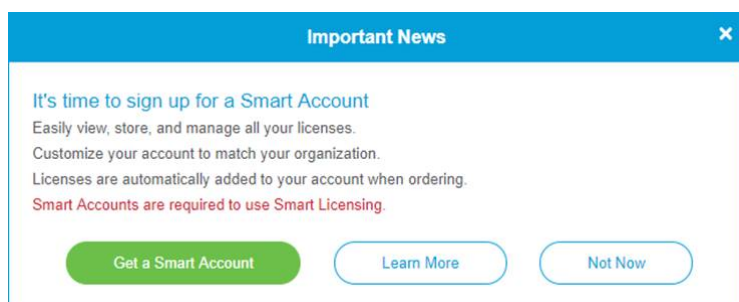
**Een case indienen:** [Support Case Manager](#)

**Telefoonnummer voor ondersteuning door de VS/Canada:** 1-866-606-1866 voor [contactgegevens](#) met [MKB TAC](#)

**E-mail met licenties:** [licensing@cisco.com](mailto: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 <a href="#">hier</a> 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 <a href="#">Smart License Account Creation</a> 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-verkoopordernummer 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...**

## Smart Software Licensing

[Feedback](#) [Support](#) [Help](#)

Alerts **Inventory** | [Convert to Smart Licensing](#) | [Reports](#) | [Preferences](#) | [Satellites](#) | [Activity](#)

Questions About Licensing?   
[Try our Virtual Assistant](#)

Virtual Account: [Redacted]

Hide Alerts

**General** | Licenses | Product Instances | Event Log

### Virtual Account

Description:

Default Virtual Account: No

### Product Instance Registration Tokens

The registration tokens below can be used to register new product instances to this virtual account.

**New Token...**

Token	Expiration Date	Uses	Export-Controlled	Description	Created By	Actions
ZmE2- <span style="background-color: #e0e0e0; padding: 2px;">[Redacted]</span>	2019-Mar-08 19:07:30 (in 8 ...)		Allowed	Test token - rv340	<span style="background-color: #e0e0e0; padding: 2px;">[Redacted]</span>	<a href="#">Actions</a> ▼
MTIz- <span style="background-color: #e0e0e0; padding: 2px;">[Redacted]</span>	2019-Mar-08 17:41:45 (in 8 ...)		Allowed	Test Token 1-2019	<span style="background-color: #e0e0e0; padding: 2px;">[Redacted]</span>	<a href="#">Actions</a> ▼
ZDE- <span style="background-color: #e0e0e0; padding: 2px;">[Redacted]</span>	2020-Feb-06 17:18:54 (in 34...)	1 of 5	Allowed	Token	<span style="background-color: #e0e0e0; padding: 2px;">[Redacted]</span>	<a href="#">Actions</a> ▼

The token will be expired when either the expiration or the maximum uses is reached

Showing All 3 Records

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.

## Create Registration Token



This will create a token that is used to register product instances, so that they can use licenses from this virtual account. Once it's created, go to the Smart Licensing configuration for your products and enter the token, to register them with this virtual account.

Virtual Account:

Description :

1

\* Expire After:

2

Days

*Between 1 - 365, 30 days recommended*

Max. Number of Uses:

3

*The token will be expired when either the expiration or the maximum uses is reached*

Allow export-controlled functionality on the products registered with this token

4

Create Token

Cancel

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.

### Product Instance Registration Tokens

The registration tokens below can be used to register new product instances to this virtual account.

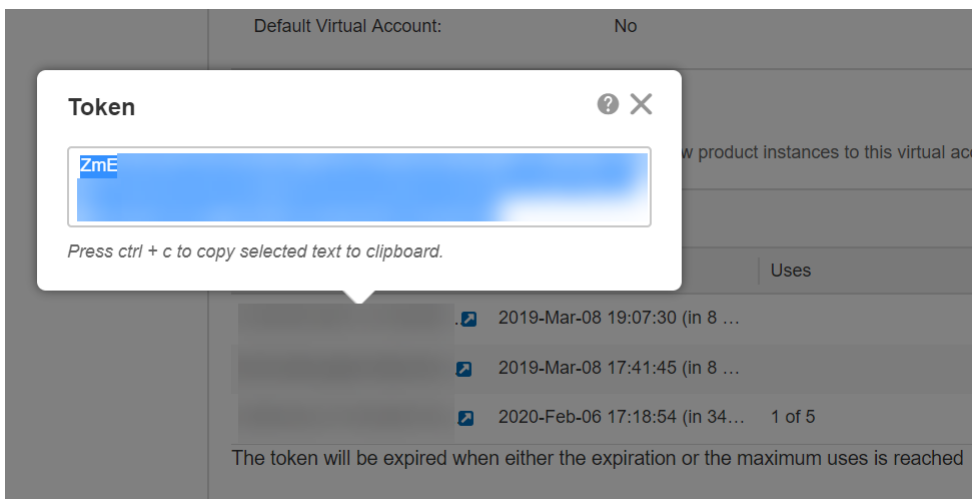
New Token...

Token	Expiration Date	Uses	Export-Controlled	Description	Created By	Actions
Zm	2019-Mar-08 19:07:30 (in 8 ...)		Allowed	Test token - rv340		Actions
MT	2019-Mar-08 17:41:45 (in 8 ...)		Allowed	Test Token 1-2019		Actions
ZD	2020-Feb-06 17:18:54 (in 34...)	1 of 5	Allowed			Actions

The token will be expired when either the expiration or the maximum uses is reached

Showing All 3 Records

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 pentopentoeets moeten uploaden. Meld u aan bij de webconfiguratie van de router.



# Router

cisco

---

●●●●●●●●|

---

English ▼

---

Login

©2017–2019 Cisco Systems, Inc. All rights reserved.

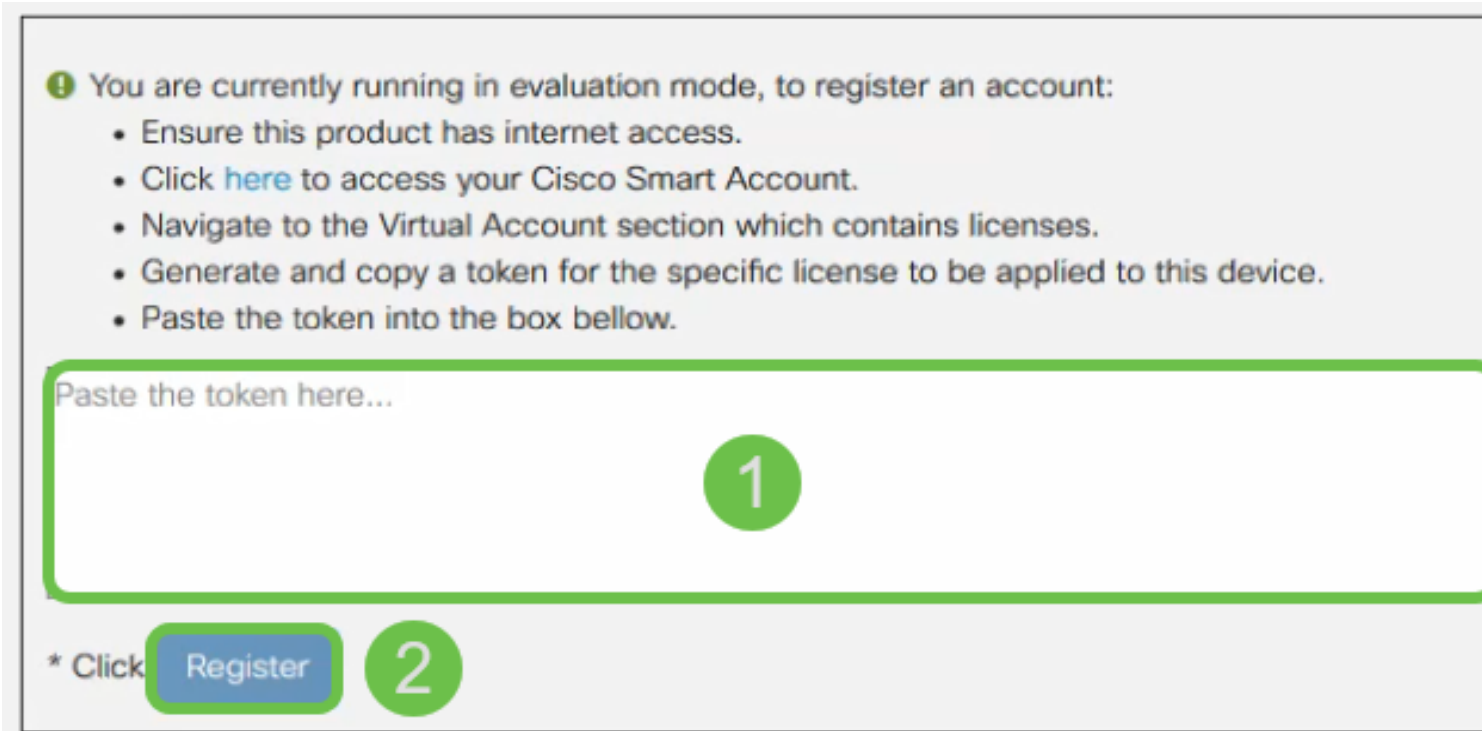
Cisco, the Cisco logo, and Cisco Systems are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

## Stap 8. Navigeer naar Licentie.

- Getting Started
- Status and Statistics
- Administration
- System Configuration
- WAN
- LAN
- Routing
- Firewall
- VPN
- Security
- QoS
- Configuration Wizards
- License**

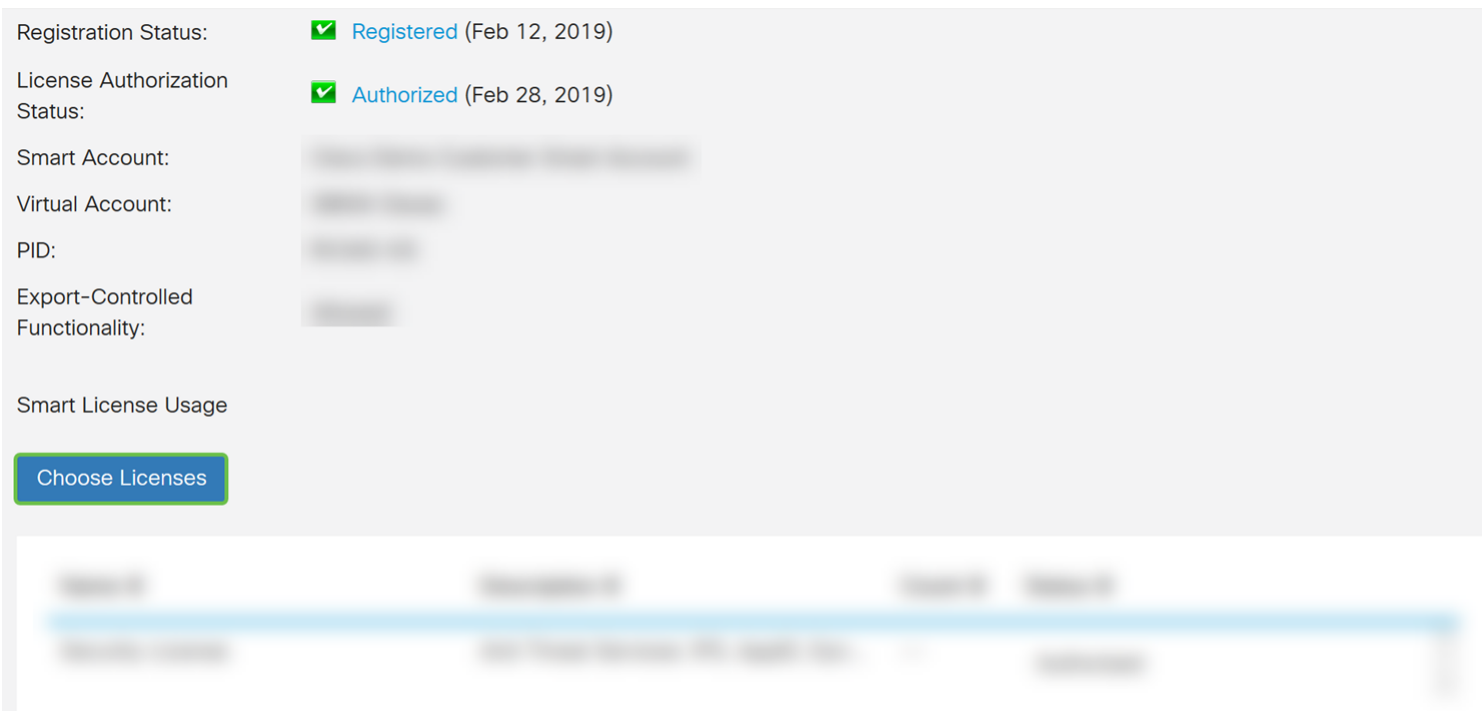
Stap 9. Als uw apparaat niet is geregistreerd, wordt de *licentiestatus* van uw *apparaat* weergegeven in de *evaluatiemodus*. Plakt het token ([Stap 6 van deze sectie](#)) die u gegenereerd hebt vanuit de pagina *Smart Licensing Manager*. Klik vervolgens op **Registreren**.

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



The screenshot shows a user interface for registration in evaluation mode. It includes an information icon and a heading: "You are currently running in evaluation mode, to register an account:". Below this is a list of instructions: "Ensure this product has internet access.", "Click here to access your Cisco Smart Account.", "Navigate to the Virtual Account section which contains licenses.", "Generate and copy a token for the specific license to be applied to this device.", and "Paste the token into the box below.". A large text input field is present with the placeholder text "Paste the token here...". A green circle with the number "1" is positioned over the input field. Below the input field, there is a blue button labeled "Register" with a green circle containing the number "2" next to it. The text "\* Click" is positioned to the left of the "Register" button.

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



The screenshot displays the registration status and license selection options. The registration status is "Registered (Feb 12, 2019)" with a green checkmark. The license authorization status is "Authorized (Feb 28, 2019)" with a green checkmark. Below this, there are fields for "Smart Account:", "Virtual Account:", "PID:", and "Export-Controlled Functionality:". A "Smart License Usage" section is visible, followed by a blue button labeled "Choose Licenses". Below the button, there is a table with columns for "License", "Status", and "Action". The table contains one row with a license name, a status of "Authorized", and an "Action" column with a dropdown menu.

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

## Choose Smart Licenses

Choose Smart Licenses to be used by this product. Ensure you have a sufficient number of licenses in the Virtual Account associated with this product, otherwise it will be out of compliance.

Enable	Name (Version)	Description	Count
<input checked="" type="checkbox"/>	Security-License	Anti Threat Services: IPS, AppID, Dynamic ...	--

2 Save and Authorize Cancel

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

Name	Description	Count	Status
Security-License	Anti Threat Services: IPS, AppID, Dyn...	--	Authorized

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.





# Router

cisco

---

●●●●●●●●|

---

English ▼

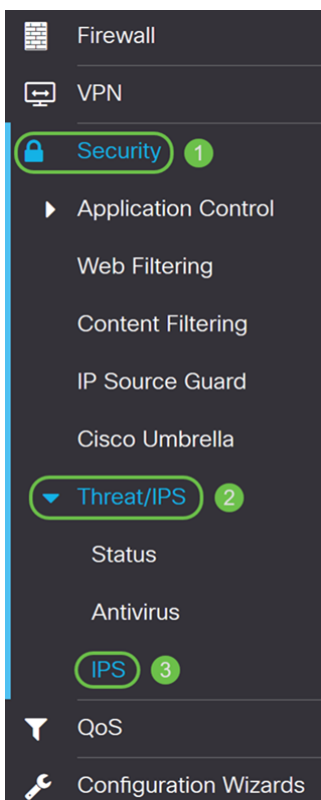
---

Login

©2017–2019 Cisco Systems, Inc. All rights reserved.

Cisco, the Cisco logo, and Cisco Systems are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

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.

## IPS (Intrusion Prevention System)

Intrusion Prevention System (IPS):  On  Off

Mode:  Block Attacks (Prevention)  
 Log Only (Detection)

IPS Security Level:  Connectivity **i**  
 Balanced **i**  
 Security **i**

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.

## IPS (Intrusion Prevention System)

Intrusion Prevention System (IPS):  On  Off

Mode:  Block Attacks (Prevention)  
 Log Only (Detection)

IPS Security Level:  Connectivity **i**  
 Balanced **i**  
 Security **i**

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**.

Intrusion Prevention System (IPS):  On  Off

Mode:  Block Attacks (Prevention)  
 Log Only (Detection)

IPS Security Level:  Connectivity   
 **Balanced**   
 Security 

## Inbraakpreventiesysteem-handtekeningen

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

### Intrusion Prevention System Signatures

Last Update:

File Version: 2.4.0.0010

Search By IPS Signature ID:

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

### Intrusion Prevention System Signatures

Last Update: 2019-Feb-26, 19:07:20 GMT

File Version:

Search By IPS Signature ID:

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.

# Intrusion Prevention System Signatures

Last Update: 2019-Feb-26, 19:07:20 GMT

File Version: 2.4.0.0010 1

Search By IPS Signature ID:

8005394 2

Search

## IPS Signature Table

Name	ID	Severity	Category
<span style="border: 1px solid green; border-radius: 50%; padding: 2px;">3</span> TROJAN Keylogger connection	8005394	high	successful-recon-limited

Navigation: ⏪ ⏩ 1 ⏪ ⏩  lines per page Showing 1 - 1 of 1

## 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.

<span style="border: 1px solid green; border-radius: 50%; padding: 2px;">1</span> Name	<span style="border: 1px solid green; border-radius: 50%; padding: 2px;">2</span> ID	<span style="border: 1px solid green; border-radius: 50%; padding: 2px;">3</span> Severity	<span style="border: 1px solid green; border-radius: 50%; padding: 2px;">4</span> Category
SERVER /etc/passwd misc attack	8000135	high	attempted-recon
OTHER Scan ident version requ...	8004101	high	attempted-recon
OTHER Scan Webtrends Scann...	8004120	high	attempted-recon
PROTOCOL TELNET resolv_ho...	8004195	high	attempted-admin

Navigation: ⏪ ⏩ 1 2 3 ... 58 ⏪ ⏩  lines per page Showing 1 - 50 of 2864

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.

## Selected Signature

ID: 8000135

Name: SERVER /etc/passwd misc attack

Impact: Information Gathering.

Description: This event is generated when an attempt is made to retrieve a protected system file on a host via a web request.

Recommendation: Webservers should not be allowed to view or execute files and binaries outside of it's designated web root or cgi-bin. This file may also be requested on a command line should the attacker gain access to the machine. Making the file read only by the superuser on the system will disallow viewing of the file by other users.

Category: attempted-recon

Severity: high

Cancel

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 vervolkeuzelijst pagina*.

FILE FLAC libFLAC VORBIS buf...	8009043	high	attempted-user
FILE FLAC libFLAC picture buff...	8009044	high	attempted-user
FILE Microsoft Media Player asf...	8009047	high	attempted-user
FILE Microsoft Media Player int...	8009048	high	attempted-user
FILE Microsoft Media Player int...	8009049	high	attempted-user
FILE Microsoft Media Player int...	8009050	high	attempted-user
OS Windows SMB misc attack	8009053	high	attempted-admin
OS Windows SMB misc attack	8009054	high	attempted-admin
FILE Adobe Flash Player embe...	8009068	high	attempted-admin
SERVER Outlook VEVENT overfl...	8009071	high	attempted-user

50 lines per page

Showing 1 - 5

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

## IPS (Intrusion Prevention System)

Apply

Cancel

Intrusion Prevention System (IPS):  On  Off

Mode:  Block Attacks (Prevention)

Log Only (Detection)

IPS Security Level:  Connectivity ⓘ

Balanced ⓘ

Security ⓘ

## Intrusion Prevention System Signatures

Last Update: 2019-Feb-26, 19:07:20 GMT

File Version: 2.4.0.0010

Search By IPS Signature ID:

Search

IPS Signature Table



**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.



cisco (admin)

English



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.

## Configuration Management

3

Apply

Cancel

Disable Save Icon Blinking

### Configuration File Name

Last Change Time

Running Configuration: ? 2019-Feb-28, 17:20:54 GMT

Startup Configuration: ? 2019-Feb-25, 20:28:52 GMT

Mirror Configuration: ? 2019-Feb-24, 00:00:04 GMT

Backup Configuration: ? N/A

### Copy/Save Configuration

All configurations that the router is currently using are in the Running Configuration file which is volatile and is not retained between reboots. To retain the configuration between reboots, make sure you copy the running configuration file to the startup configuration file after you have completed all your changes.

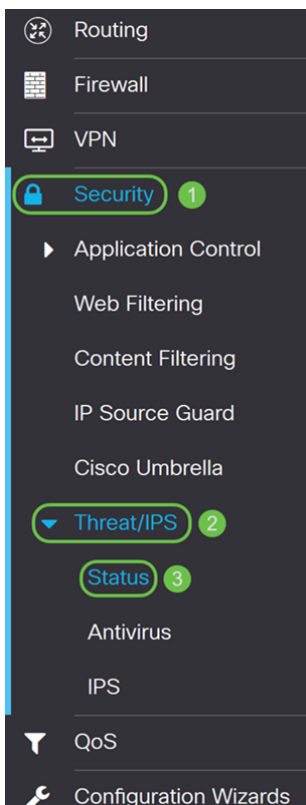
Source: 1 Running Configuration

Destination: 2 Startup Configuration

Save Icon Blinking: Enable

## 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.

## Status

System Date & Time: 2019-Feb-28, 17:44:12 GMT  
Total Last 30 Days: Scanned 0 Detected 0  
Total Last 7 Days: Scanned 0 Detected 0  
Total Last 24 Hours: Scanned 0 Detected 0  
Virus/IPS status since: 2019-Feb-26, 19:04:33 GMT ↻

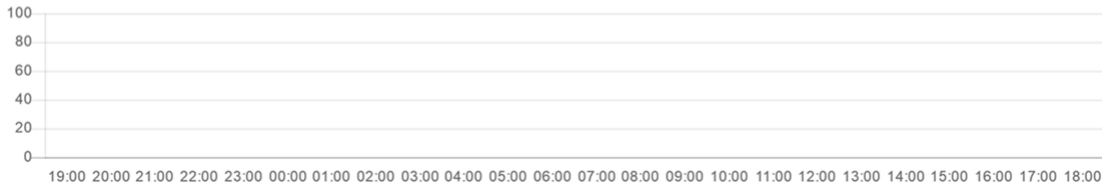
Total

Virus

IPS

Last 24 Hours ▾

Events over time



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

## Status

System Date & Time: 2019-Feb-28, 17:45:47 GMT  
Total Since Activated: Scanned 0 Detected 0  
Total Last 7 Days: Scanned 0 Detected 0  
Total Last 24 Hours: Scanned 0 Detected 0  
Virus/IPS status since: 2019-Feb-26, 19:04:33 GMT ↻

Total

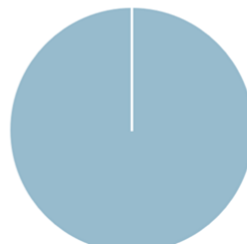
Virus

IPS

Top 10 Attacked Clients



Top 10 IPS Attacks



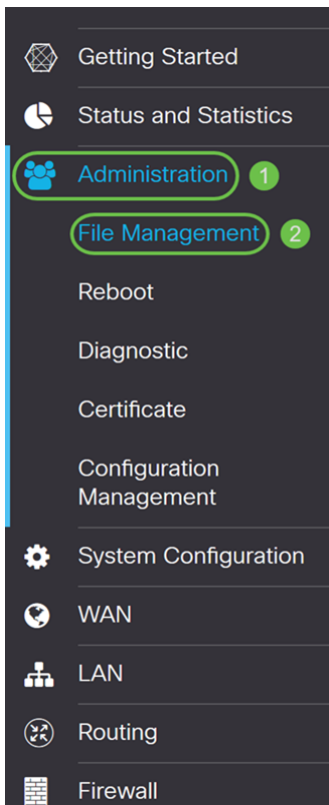
## IPS-definities bijwerken

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.

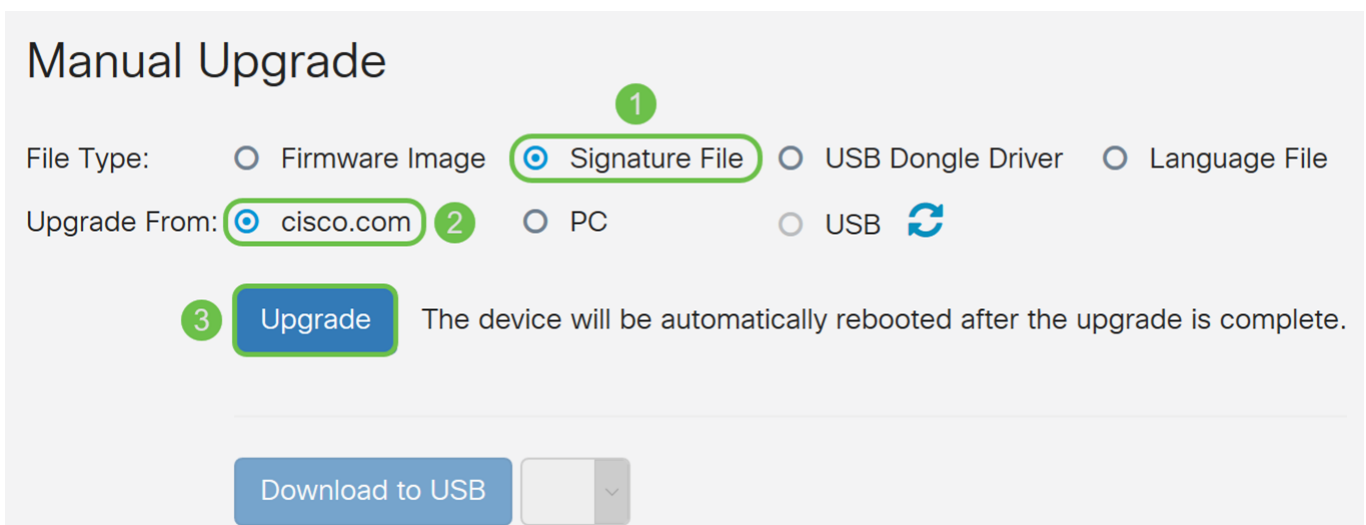
**Best Practice:** Aanbevolen wordt de veiligheidshandtekeningen wekelijks automatisch bij te werken.

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

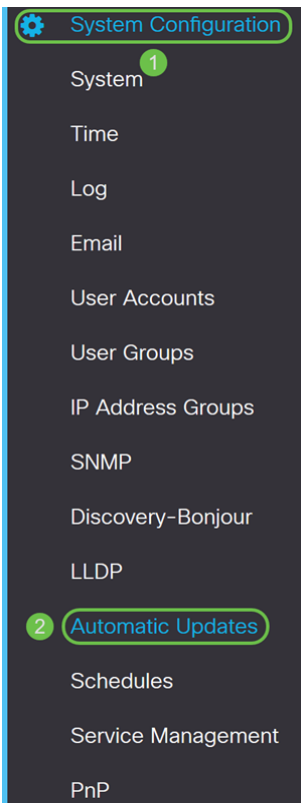




Stap 2. Scrollt naar het gedeelte *Handmatige upgrade* in de pagina *Bestandsbeheer*. Selecteer **Signaalbestand** voor *bestandstype* en **cisco.com** voor *upgrade vanaf*. Druk vervolgens op **upgrade**. Hierdoor kan de laatste veiligheidshandtekening worden gedownload en geïnstalleerd.



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

Check Every:

Notify via:  Admin GUI

Email to  Notifications will not be sent unless an email server is configured. Click [here](#) to manage email server settings.

Stap 5. Scrollt 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.

Automatic Update ^

	Notify <span>⌵</span>	Update (hh:mm) <span>⌵</span>	Status <span>⌵</span>
System Firmware	<input checked="" type="checkbox"/>	<input type="text" value="Never"/>	Version 0.0.0.1, Version 1.0.02.16 is available on Cisco.com.
USB Modem Firmware	<input checked="" type="checkbox"/>	<input type="text" value="Never"/>	Version 1.0.00.01, Version 0.0.00.01 is available on Cisco.com.
Security Signature	<input checked="" type="checkbox"/>	<input type="text" value="Immediately"/>	Version 2.0.0.0006 was applied on 2019-Feb-26, 19:07:20 GMT, ...

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.

### Automatic Updates

Apply Cancel

Check Every:

Notify via:  Admin GUI

Email to  Notifications will not be sent unless an email server is configured. Click [here](#) to manage email server settings.

---

#### Automatic Update

	Notify	Update (hh:mm)	Status
System Firmware	<input checked="" type="checkbox"/>	<input type="text" value="Never"/>	Version 0.0.0.1, Version 1.0.02.16 is available on Cisco.com.
USB Modem Firmware	<input checked="" type="checkbox"/>	<input type="text" value="Never"/>	Version 1.0.00.01, Version 0.0.00.01 is available on Cisco.com.
Security Signature	<input checked="" type="checkbox"/>	<input type="text" value="Immediately"/>	Version 2.0.0.0006 was applied on 2019-Feb-26, 19:07:20 GMT, ...

## Conclusie

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