Configuring Intrusion Prevention System on the RV34x Series Router

Objective

The objective of this document is to show you how to configure the Intrusion Prevention System (IPS) on RV34x series routers.

Introduction

The Intrusion Prevention System scans traffic to look for known attack patterns to block. It watches packets and sessions as they flow through the router and scans each packet to match any of the Cisco IPS signatures. When it detects suspicious activity, it is designed to log or block it. It is important to update the IPS and Antivirus databases and definitions. These can be updated manually or automatically.

Check out these videos on Cisco Intrusion Prevention System:

However, IPS can impact the router's performance. In general, it doesn't impact the total throughput for Hypertext Transfer Protocol (HTTP) and File Transfer Protocol (FTP) traffic, but it can drop the maximum number of concurrent connections somewhat dramatically.

Important Note: If the router is currently under a heavy workload, this may exacerbate the issue.

The table below gives expected statistics for performance under various configurations. These values should be used as a guide, as real world performance may differ due to a number of factors.

	Concurrent Connections	Connection Rate	HTTP throughput	FTP throughput
Default Settings	40000	3000	982MB/sec	981MB/sec
Enable APP control	15000-16000	1300	982MB/sec	981MB/sec
Enable Antivirus	16000	1500	982MB/sec	981MB/sec
Enable IPS	**17000**	**1300**	**982MB/sec**	**981MB/sec**
Enable App Control Antivirus & IPS	15000-16000	1000	982MB/sec	981MB/sec

The following fields are defined as:

Concurrent Connections – The total number of concurrent connections. For example, if you are downloading a file from one site, that's one connection, streaming audio from Spotify that will be another connection, making it two concurrent connections.

Connection Rate – The number of connections request / second it can process.

HTTP/FTP Throughput – The HTTP and FTP throughput are the download rates in MB/sec.

Security licenses have been updated to include IPS protection in addition to existing application and web filtering. A smart account is required in order to have a security license. If you do not already have an active smart account, section 1 of this document will be required.

To learn how to configure Antivirus on RV34x, click here.

Applicable Devices

- RV34x

Software Version

- 1.0.03.x

Table of Contents

Smart Licensing

If you do not have an active smart account, you will need to proceed with the steps below.

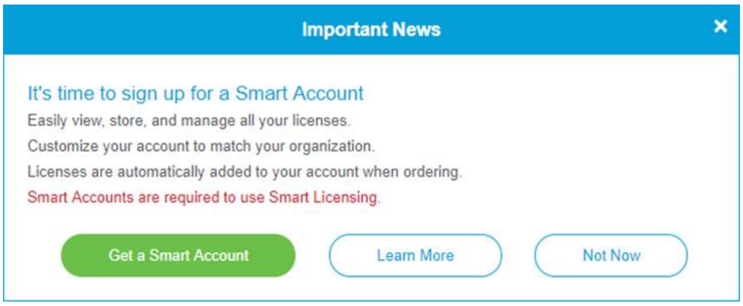
If you run into any troubles or issues while configuring your Smart License account, our support team will help sort out potential issues and can be reached through multiple methods. Feel free to use your preferred method to reach out.

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

- **FAQ about RV34x Series:** RV34x Series Router FAQs
- **Smart License Overview:** Smart Software Licensing
- **FAQ about Smart Licenses:** Smart Licensing and Smart Accounts FAQ for Partners, Distributors and Customers
- **Submit a case:** Support Case Manager
- **US/Canada Support Phone Number:** 1-866-606-1866 or Small Business TAC Contacts
- **Licensing Email:** licensing@cisco.com

Step 1. If you have created or visited your Cisco.com account recently, you're greeted by a message to create your own Smart License account. If you haven't, you can click here to be taken to the Smart License account creation page. You may need to log in.

Note: For additional details on the steps involved in requesting your Smart Account, click here.



Important News

It's time to sign up for a Smart Account

Easily view, store, and manage all your licenses.

Customize your account to match your organization.

Licenses are automatically added to your account when ordering.

Smart Accounts are required to use Smart Licensing.

Step 2. When purchasing a smart license for a router, the vendor needs to make a process which moves the unique license ID to your Smart License account. The below is a table of the necessary information that will be asked for when purchasing the bundles.

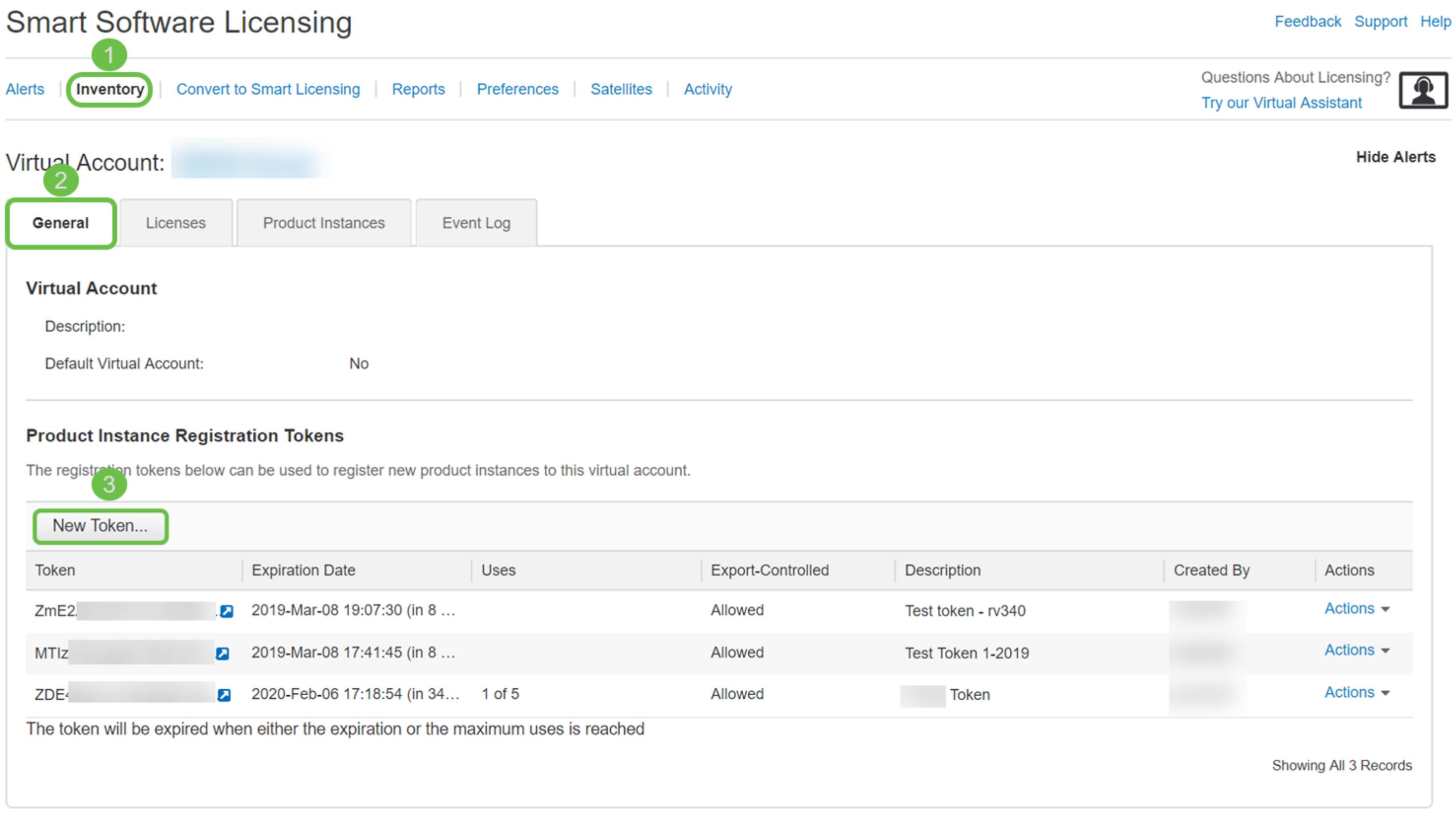
Note: IPS and Antivirus are part of the security license used for Web Filtering and Application Filtering.

Information Required	**Locating the information**
Cisco.com User ID	Located in your account profile, or you can click here.
Smart License Account Name	It is best to have created your smart account prior to purchasing the license. This should be step 8 of the Smart License Account Creation article.
Smart License SKU	The product identification code for the device. Ex. RV340-K9-NA

Note: If you have purchased a license and it's not appearing in your virtual account, you should either follow up with the reseller to request they make the transfer or reach out to us.

To make the process as expedient as possible, you should have your License Invoice, Cisco Sales Order Number, and a screenshot of your Smart Account License page (to share with our team).

Step 3. To generate a token, navigate to your Smart Software License account. Then click **Inventory > General Tab**. Click on the **New Token…** button.


Smart Software Licensing
Feedback Support Help
Alerts | Inventory | Convert to Smart Licensing | Reports | Preferences | Satellites | Activity
Questions About Licensing?
Try our Virtual Assistant
1
2
3
Hide Alerts
General
Licenses
Product Instances
Event Log
New Token...
Actions
Actions
Actions

Virtual Account: [redacted]

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.

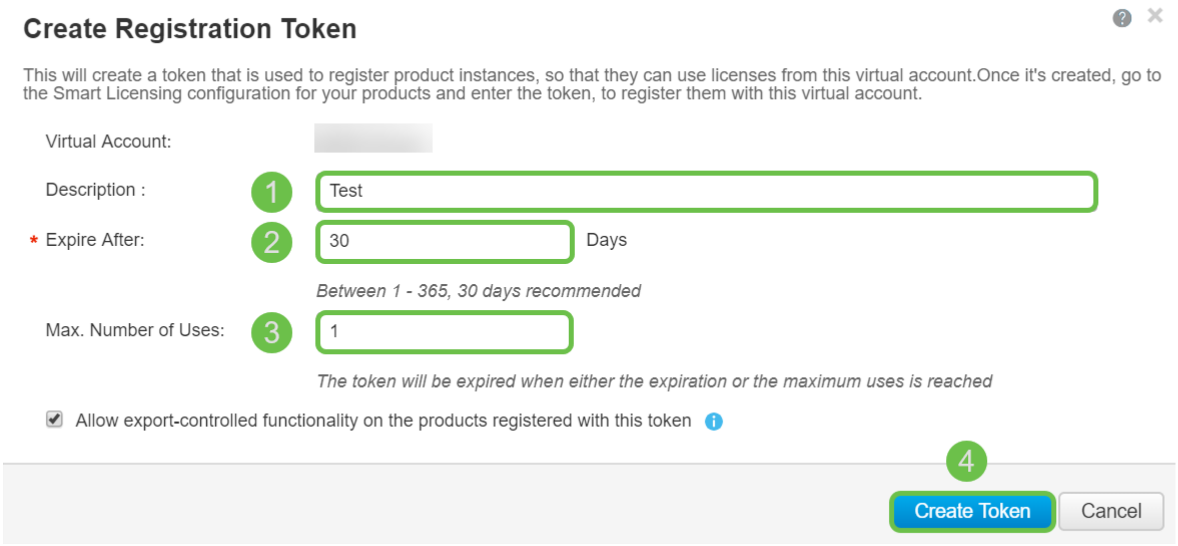
Token	Expiration Date	Uses	Export-Controlled	Description	Created By	Actions
ZmE2[redacted]	2019-Mar-08 19:07:30 (in 8 …		Allowed	Test token - rv340	[redacted]	Actions
MTIz[redacted]	2019-Mar-08 17:41:45 (in 8 …		Allowed	Test Token 1-2019	[redacted]	Actions
ZDE[redacted]	2020-Feb-06 17:18:54 (in 34…	1 of 5	Allowed	[redacted] Token	[redacted]	Actions

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

Showing All 3 Records

Step 4. A *Create Registration Token* window opens. Enter a *Description*, *Expire After*, and *Max. Number of Uses*. Then press the **Create Token** button.

Note: 30 days for *Expire After* is recommended.



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: [redacted]

Description : Test

* Expire After: 30 Days

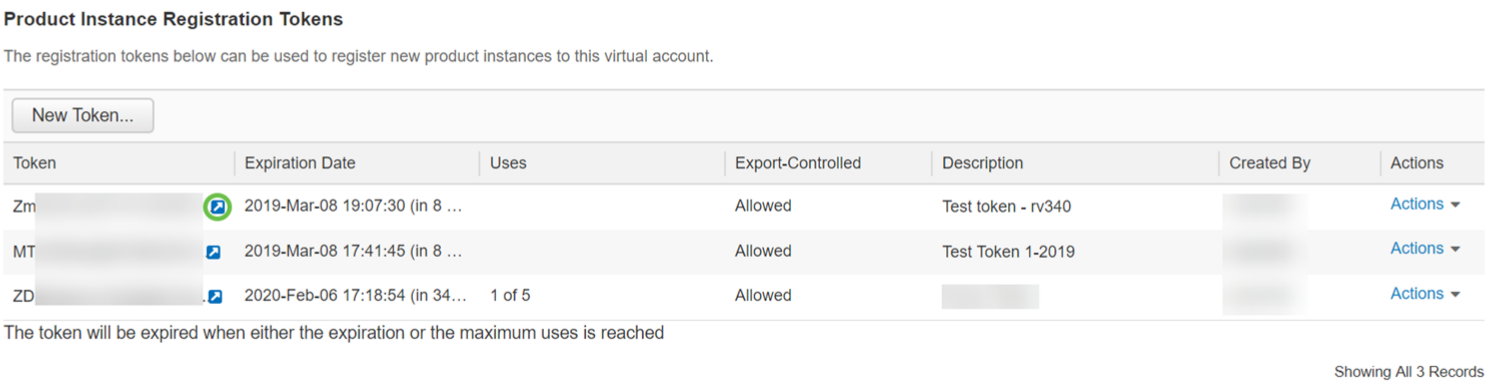
Between 1 - 365, 30 days recommended

Max. Number of Uses: 1

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

Step 5. Once the token is generated, you can click the **Token link (blue box with a white arrow)** button to the right of your recently created token.



Product Instance Registration Tokens

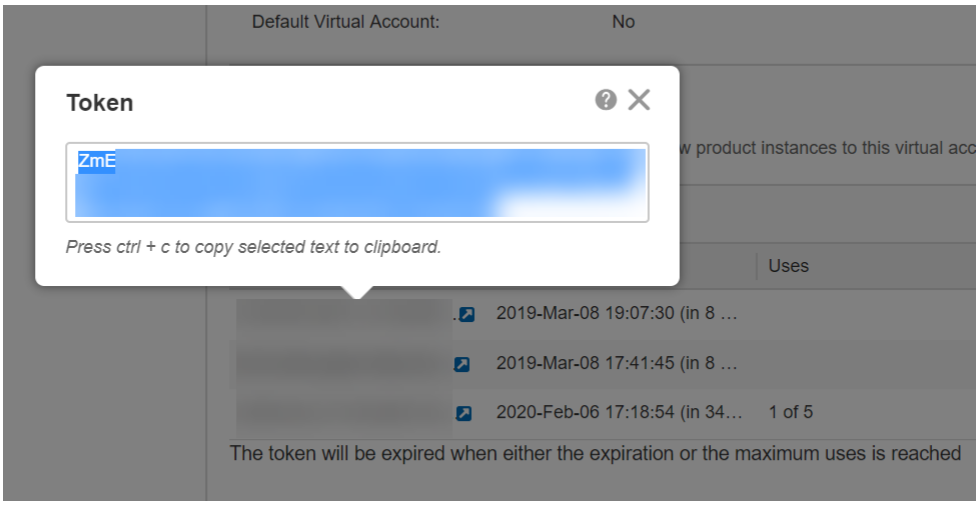
The registration tokens below can be used to register new product instances to this virtual account.

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

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

Showing All 3 Records

Step 6. A *Token* window should appear with the full token for you to copy. Highlight the token, right click the token and click **Copy** or you can hold down the **ctrl** button on your keyboard and click **c** at the same time to copy the text.



Default Virtual Account: No

Token

ZmE[redacted]

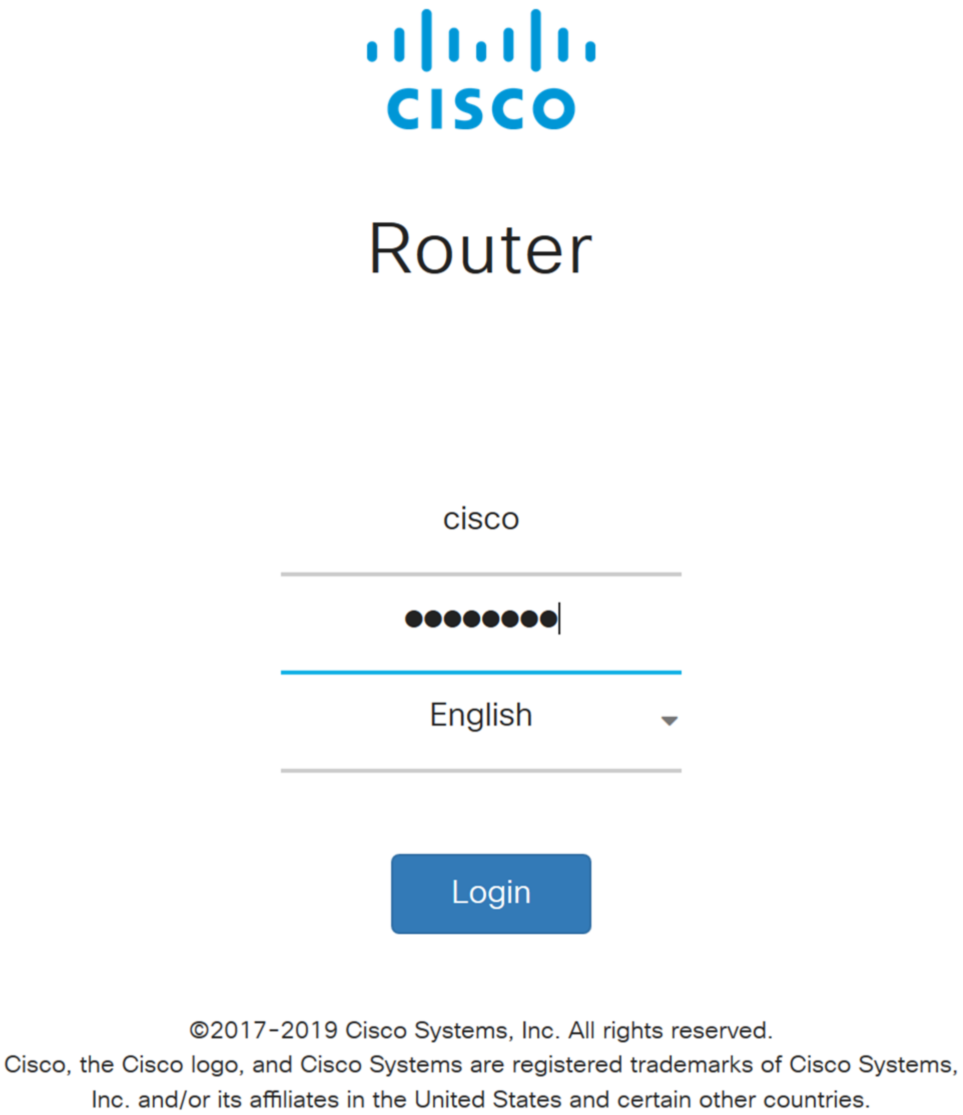
Press ctrl + c to copy selected text to clipboard.

w product instances to this virtual acc

	Uses
[redacted] 2019-Mar-08 19:07:30 (in 8 ...	
[redacted] 2019-Mar-08 17:41:45 (in 8 ...	
[redacted] 2020-Feb-06 17:18:54 (in 34...	1 of 5

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

Step 7. Once you have copied your token, you will need to log into the device and upload the token key. Log in to the web configuration page of the router.


Router

cisco

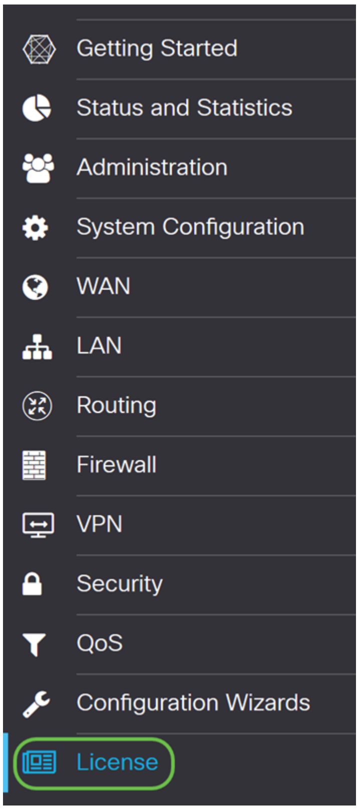
●●●●●●●●

English

Login

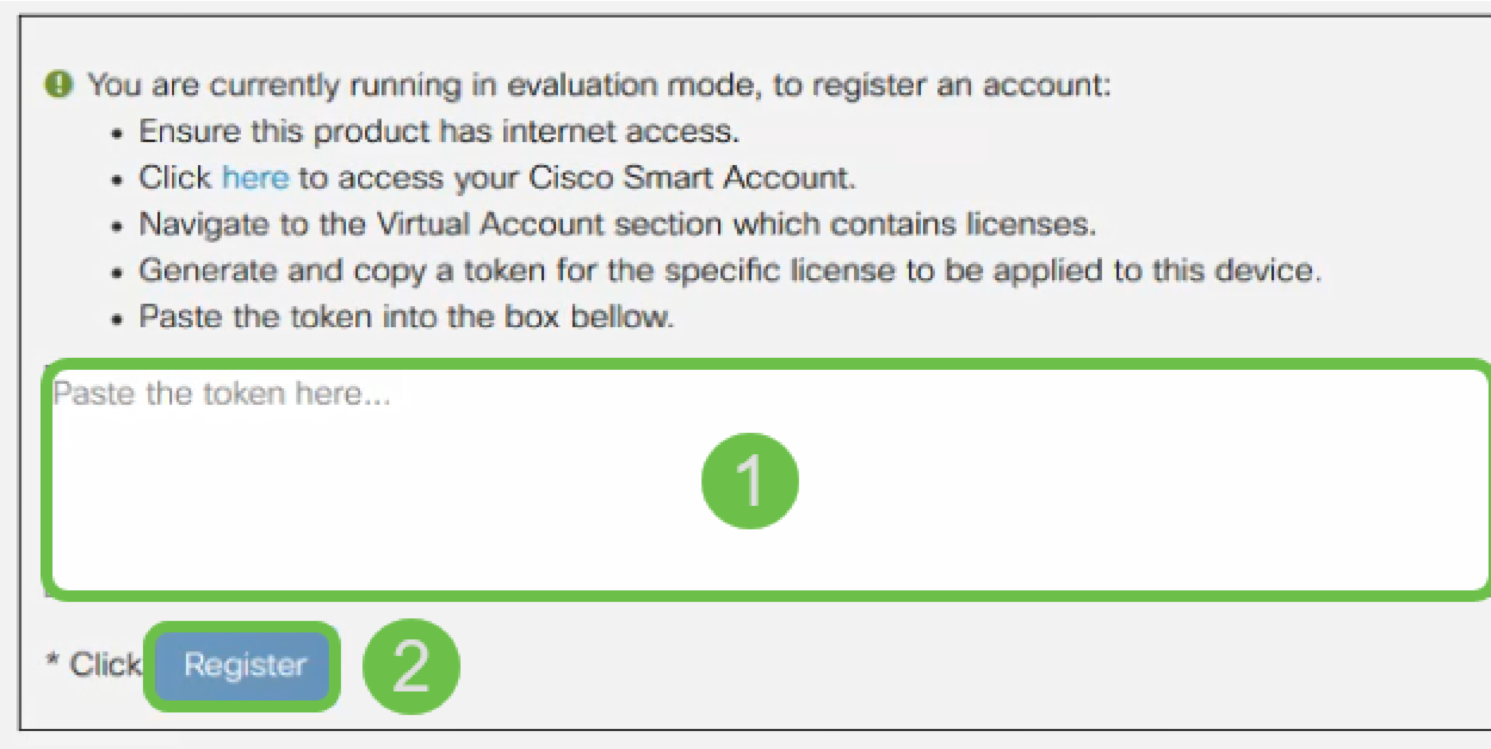
©2017-2019 Cisco Systems, Inc. All rights reserved.
Cisco, the Cisco logo, and Cisco Systems are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

Step 8. Navigate to **License.**



Step 9. If your device is unregistered, your *License Authorization Status* will be listed as *Evaluation Mode*. Paste the token (Step 6 of this section) that you have generated from the *Smart Licensing Manager* page. Then click **Register**.

Note: The registration process may take some time, please wait for it to finish.



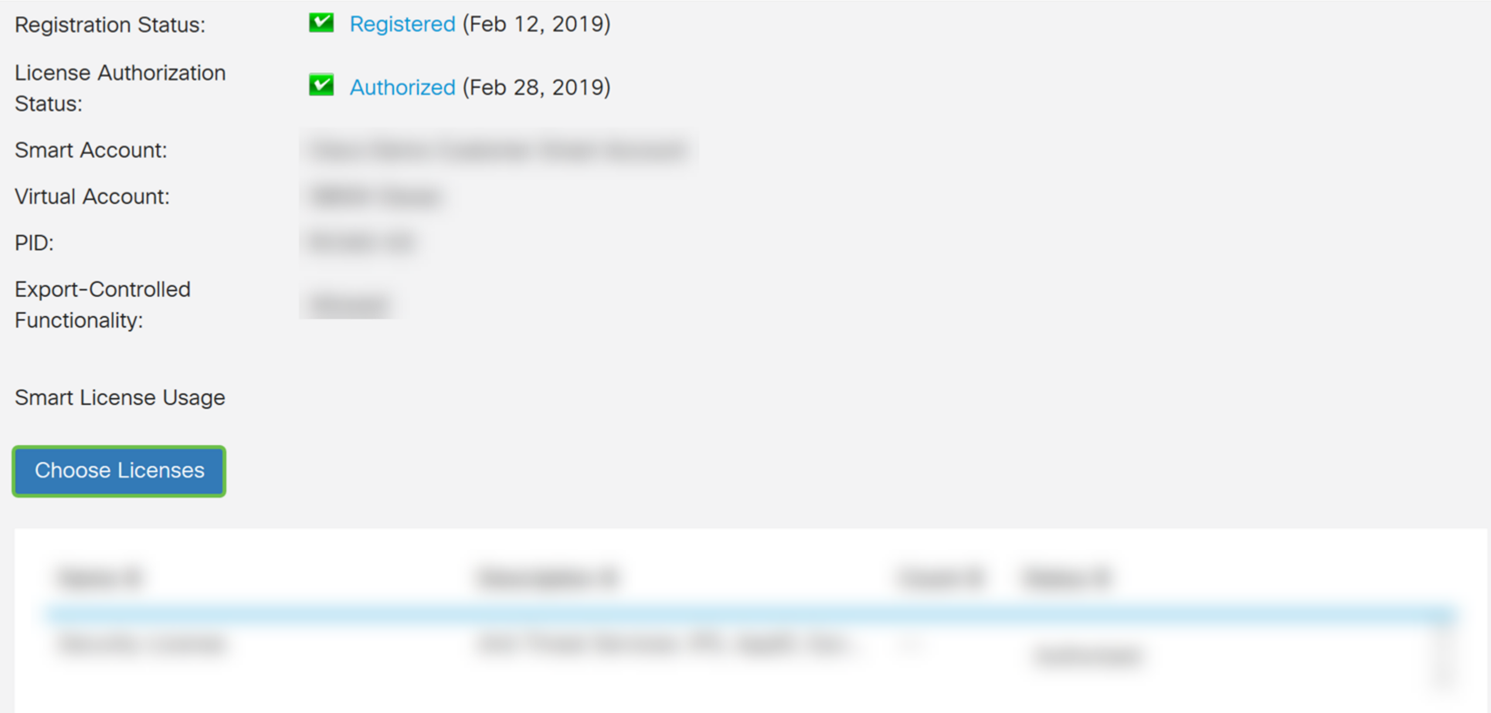
You are currently running in evaluation mode, to register an account:

- 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.
- Paste the token into the box bellow.

Paste the token here...

* Click Register

Step 10. Once the token is registered, you will need to allocate the license. Click the **Choose Licenses** button.



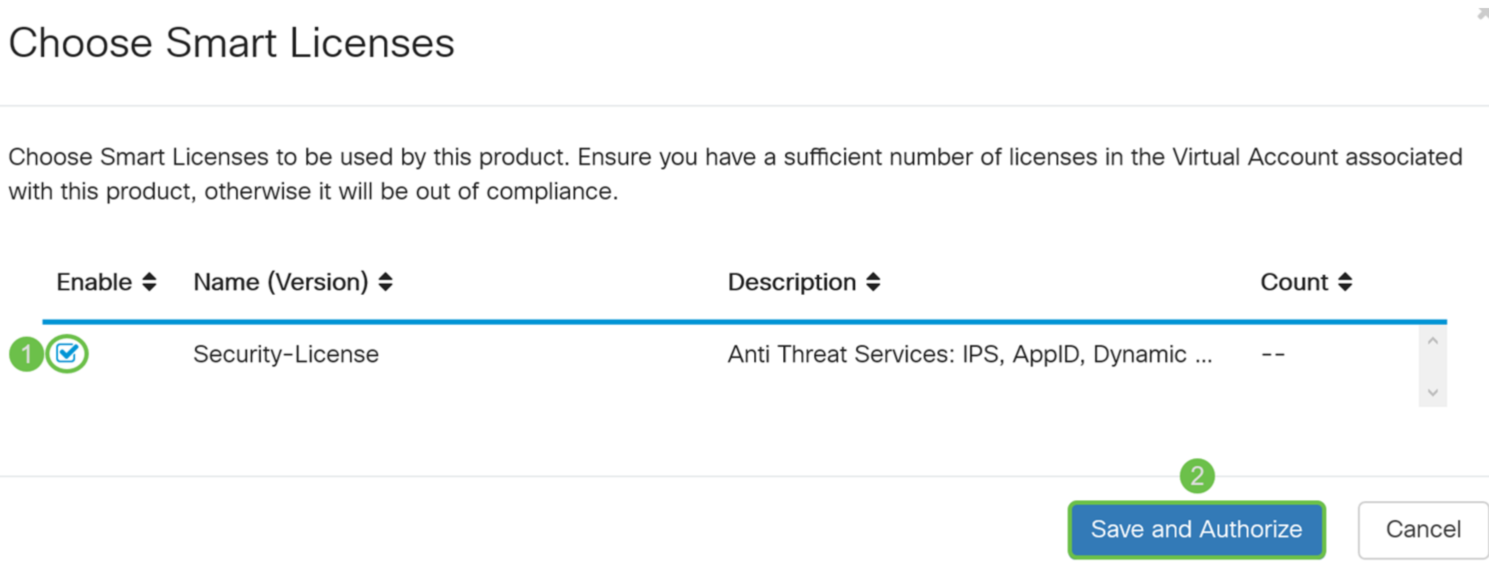
Registration Status:	✓ Registered (Feb 12, 2019)
License Authorization Status:	✓ Authorized (Feb 28, 2019)
Smart Account:	[redacted]
Virtual Account:	[redacted]
PID:	[redacted]
Export-Controlled Functionality:	[redacted]

Smart License Usage

Choose Licenses

[redacted]

Step 11. The *Choose Smart Licenses* window should appear. Check the **Security-License** and then press **Save and Authorize**.

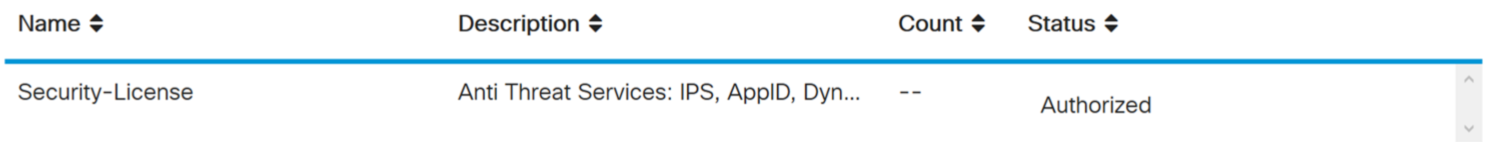


Choose Smart Licenses

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
☑	Security-License	Anti Threat Services: IPS, AppID, Dynamic ...	--

Step 12. The *Status* of your Security-License should be *Authorized* now.

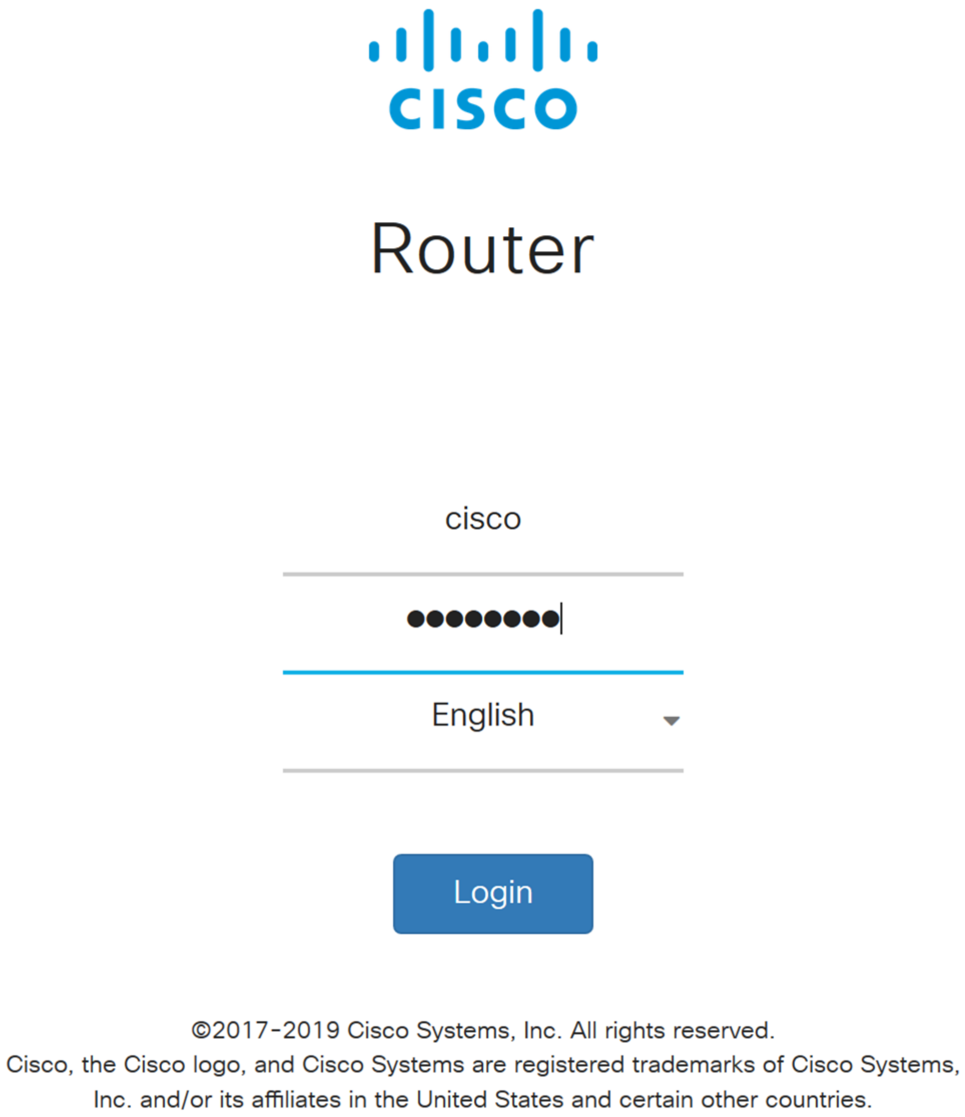


Name	Description	Count	Status
Security-License	Anti Threat Services: IPS, AppID, Dyn...	--	Authorized

You should now be able to proceed with configuring Intrusion Prevention System.

Configuring Intrusion Prevention System

Step 1. If you haven’t logged into the router yet, log in to the web configuration page of the router.



Router

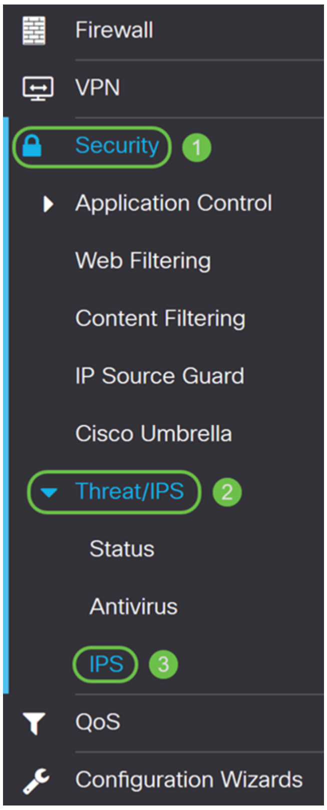
cisco

●●●●●●●●

English

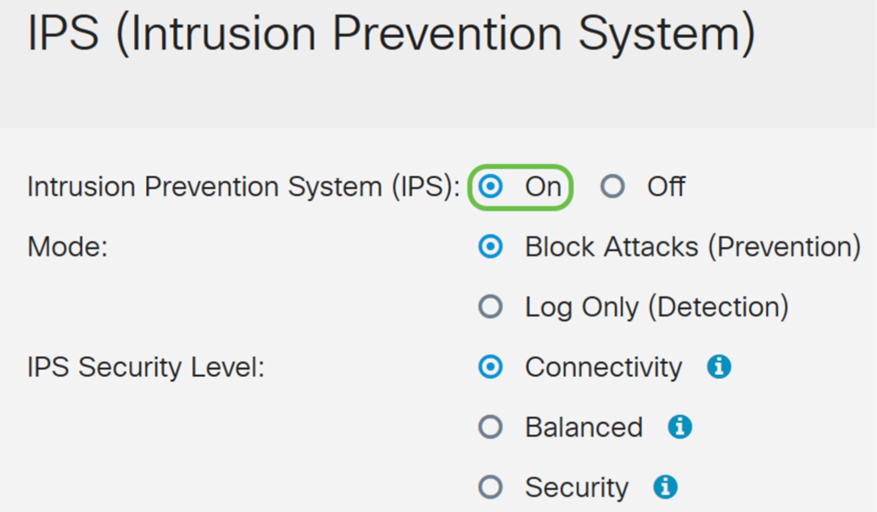
©2017-2019 Cisco Systems, Inc. All rights reserved.
Cisco, the Cisco logo, and Cisco Systems are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

Step 2. Navigate to **Security > Threat/IPS > IPS**.



Step 3. Select **On** to enable the Intrusion Prevention System feature. If you want to turn it off, select **Off**.

We will be selecting **On** in this example.



IPS (Intrusion Prevention System)

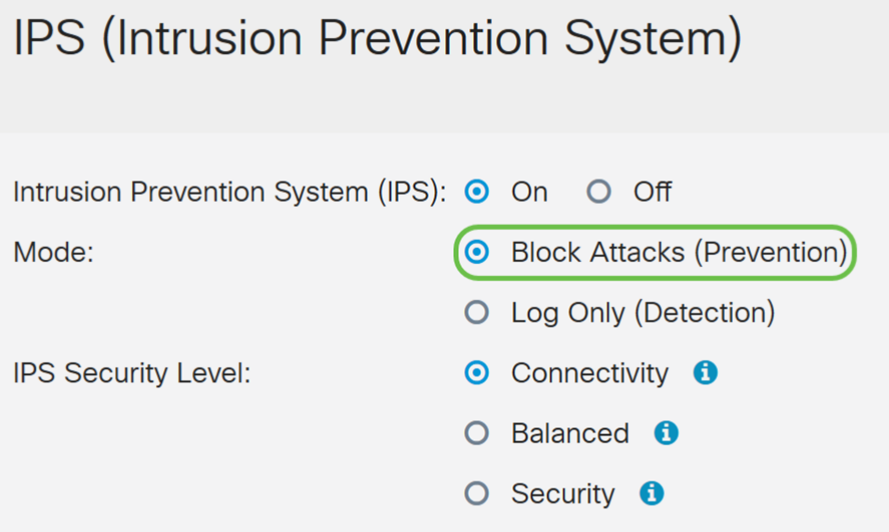
Intrusion Prevention System (IPS): ● On ○ Off

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

IPS Security Level: ● Connectivity ○ Balanced ○ Security

Step 4. Select either **Block Attacks (Prevention)** or **Log Only**. In this example, we will be selecting **Block Attacks (Prevention)**. The following options are defined below.

- **Block Attacks (Prevention)** – Select to block all the attacks. It also logs the anomaly.
- **Log Only** – This option will generate the log only (with client information, signature ID, etc.) when the anomalies are identified. It does not impact the connection.



IPS (Intrusion Prevention System)

Intrusion Prevention System (IPS): ● On ○ Off

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

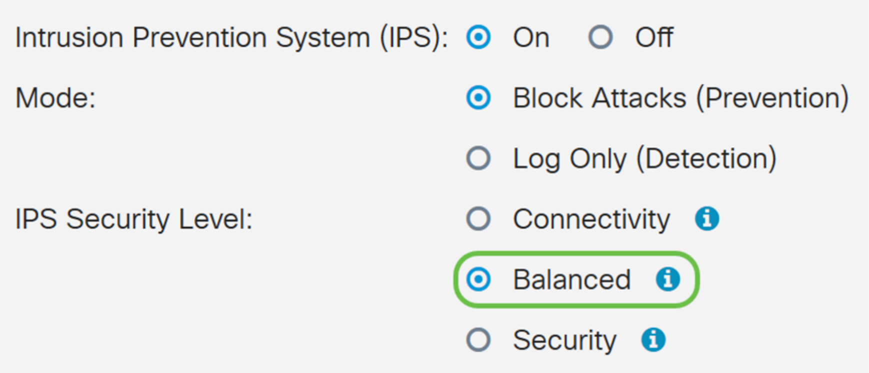
IPS Security Level: ● Connectivity ○ Balanced ○ Security

Step 5. Select the IPS security level that you want to use. The following options are defined as:

- **Connectivity** – This mode will detect the most critical attacks. This provides the least protection: only (high severity) risk attacks are detected. This is the least secure option.
- **Balanced** – The selected mode will detect severe attacks along with the critical attacks. This provides medium protection: (high + medium severity) are inspected, by passing low risk signatures. This is mid-level security for IPS.
- **Security** – Security mode will detect the normal attacks along with the severe and critical attacks. This provides the most protection: All rules (high + medium + low severity) are inspected. This is the highest security level for IPS.

Note: The higher security level you choose, the more attacks are being monitored, the bigger the impact on system performance that may be experienced.

We will be selecting **Balanced** for this demonstration.



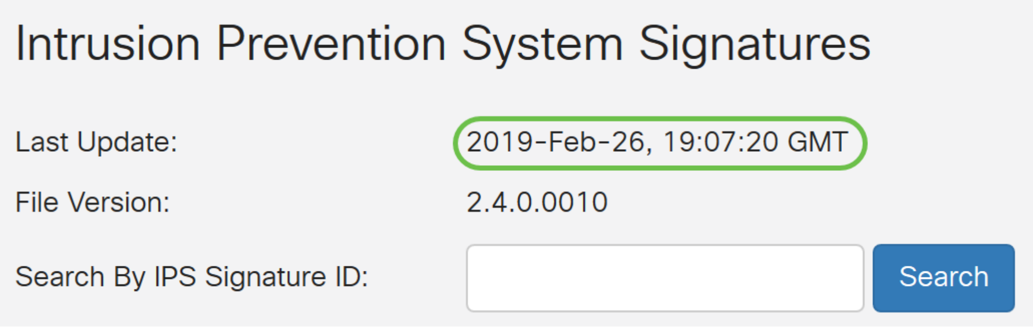
Intrusion Prevention System (IPS): ● On ○ Off

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

IPS Security Level: ○ Connectivity ● Balanced ○ Security

Intrusion Prevention System Signatures

Step 6. In the *Last Update* field, it will display the date and time of the last updated signature.



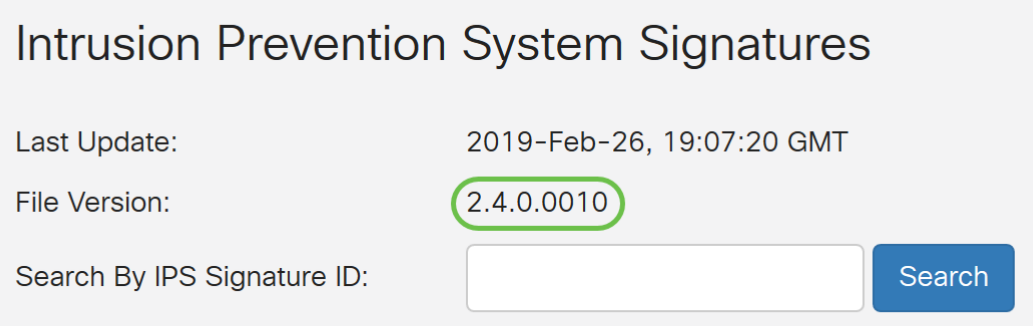
Intrusion Prevention System Signatures

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

File Version: 2.4.0.0010

Search By IPS Signature ID:

Step 7. The *File Version* displays the signature version which is being used.



Intrusion Prevention System Signatures

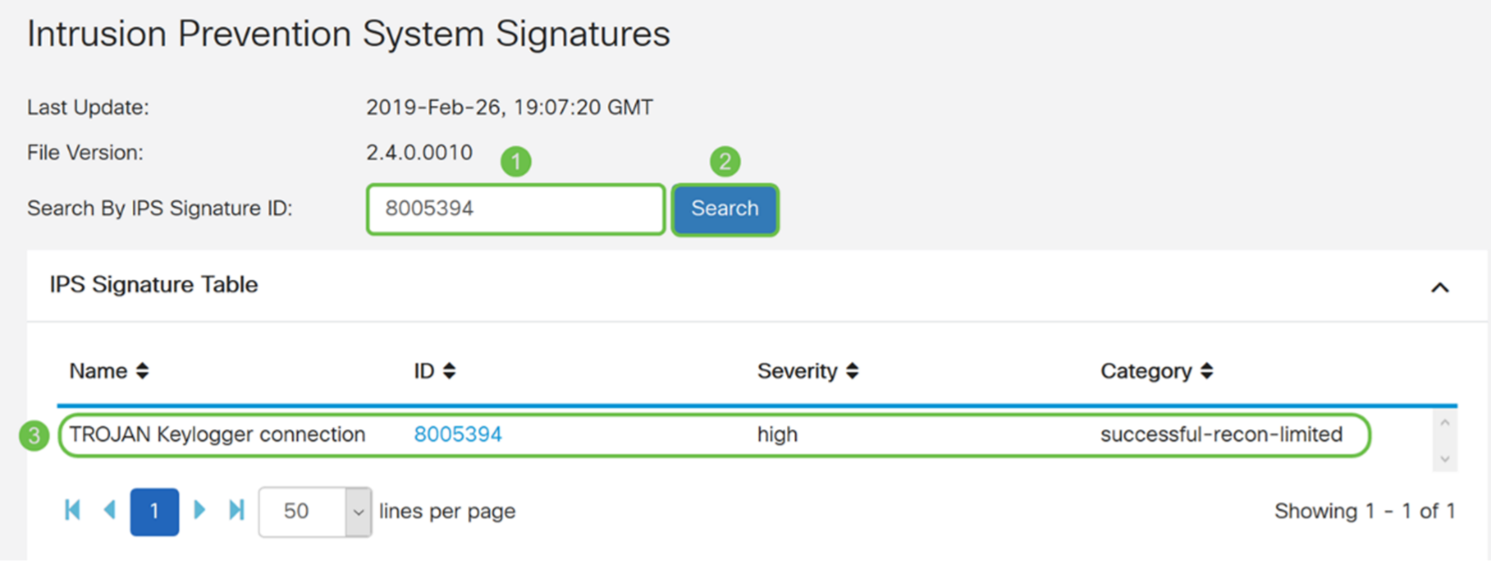
Last Update: 2019-Feb-26, 19:07:20 GMT

File Version: 2.4.0.0010

Search By IPS Signature ID:

Step 8. To search for a signature ID, enter the **Signature ID** in the *Search by IPS Signature ID* field and click **Search** to check whether the signature is supported or not. If the signature ID is supported, the table will update with the result like shown below.

Note: If the signature ID is not supported, nothing will appear in the table.



Intrusion Prevention System Signatures

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

File Version: 2.4.0.0010

Search By IPS Signature ID: 8005394

IPS Signature Table

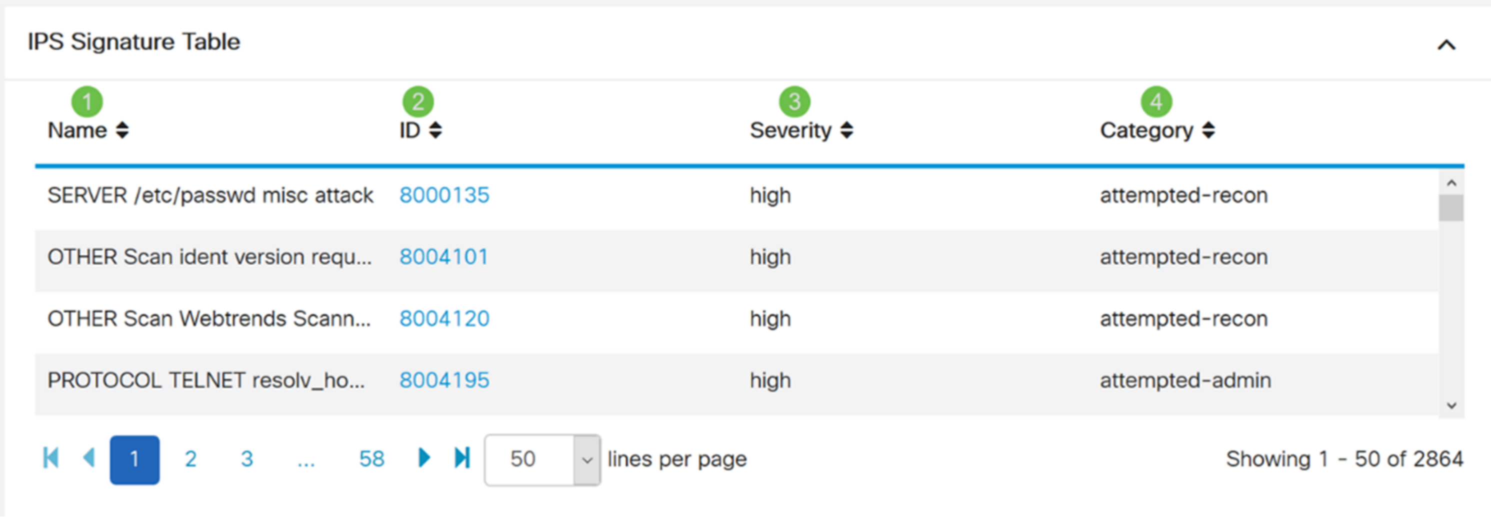
Name	ID	Severity	Category
TROJAN Keylogger connection	8005394	high	successful-recon-limited

1 · 50 lines per page · Showing 1 - 1 of 1

Intrusion Prevention System Signature Table

Step 9. In the *IPS Signature Table*, the following fields are defined as:

- **Name** – Name of the signature.
- **ID** – The unique identifier of the signature. Clicking the ID will open a window for you to view the complete details for the selected signature.
- **Severity** – Severity level denotes the security impact.
- **Category** – The category that the signature belongs to.

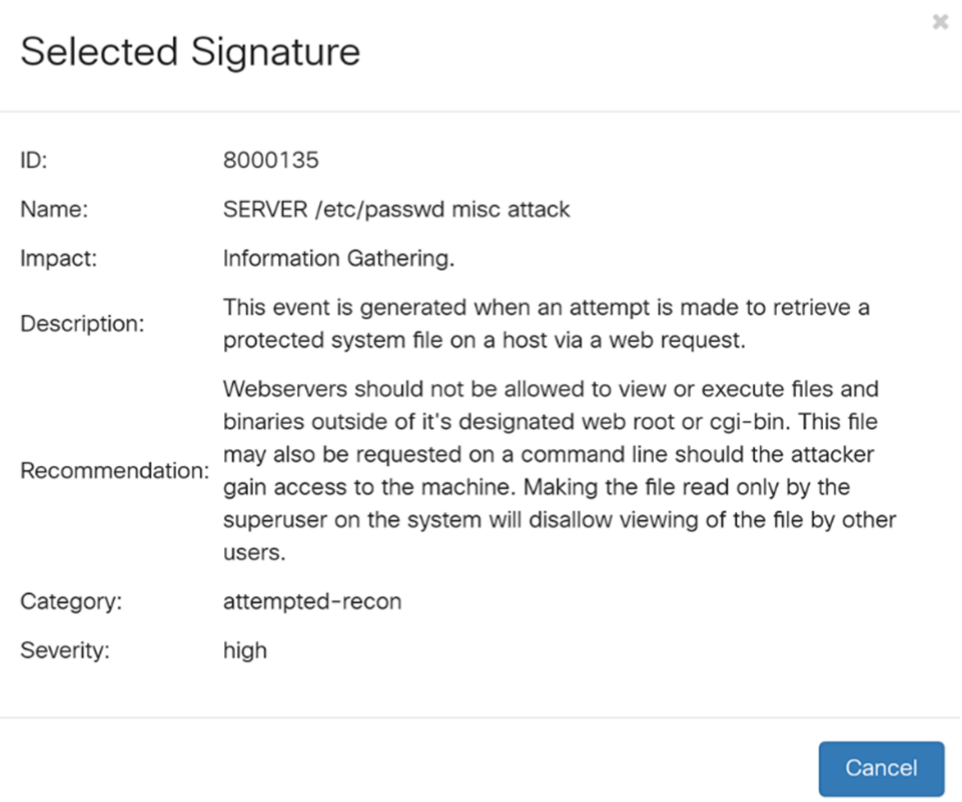


IPS Signature Table

Name	ID	Severity	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

1 2 3 ... 58 · 50 lines per page · Showing 1 - 50 of 2864

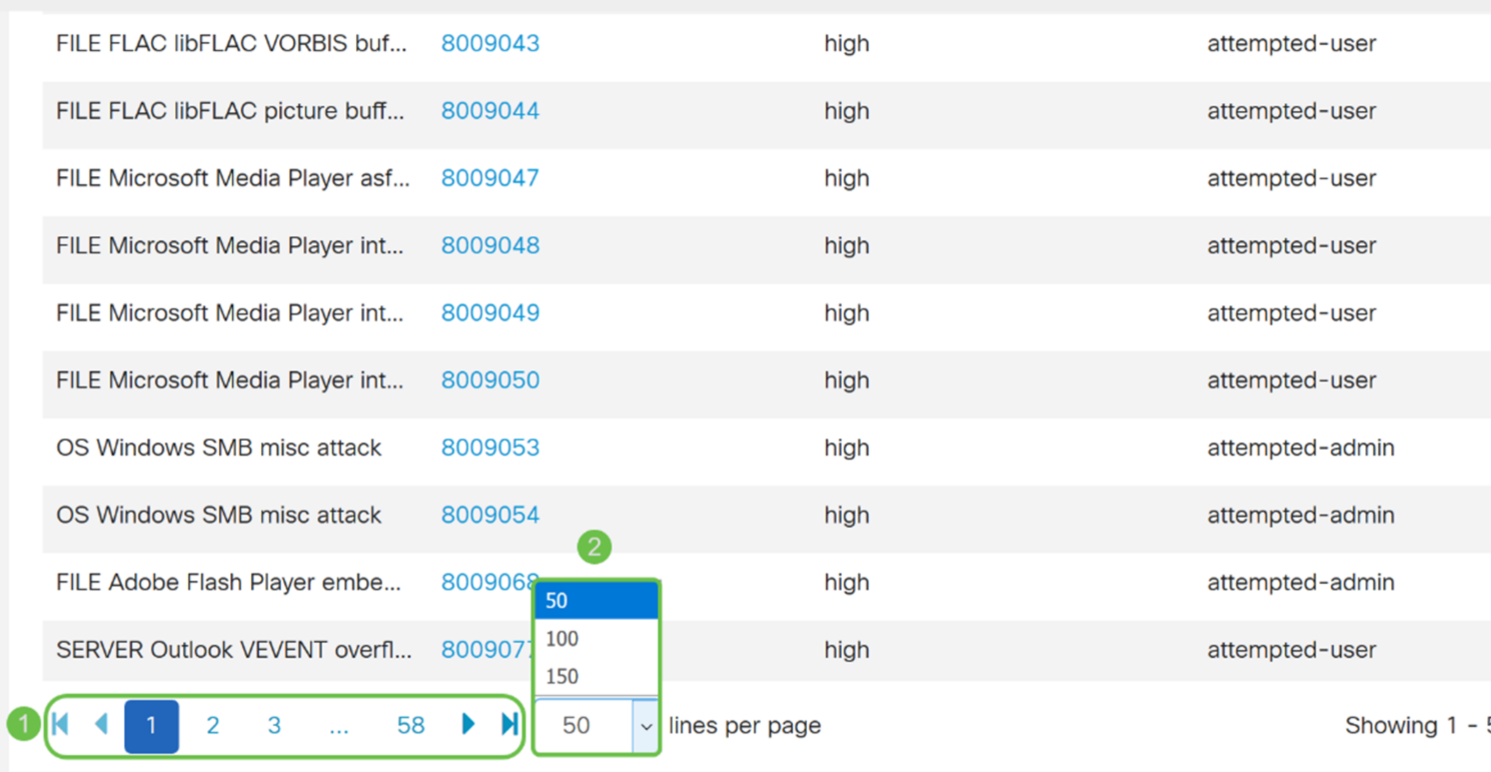
Step 10. (Optional) If you clicked on the signature ID in the *IPS Signature Table*, a window will appear to show you the complete details for the selected signature.



Selected Signature

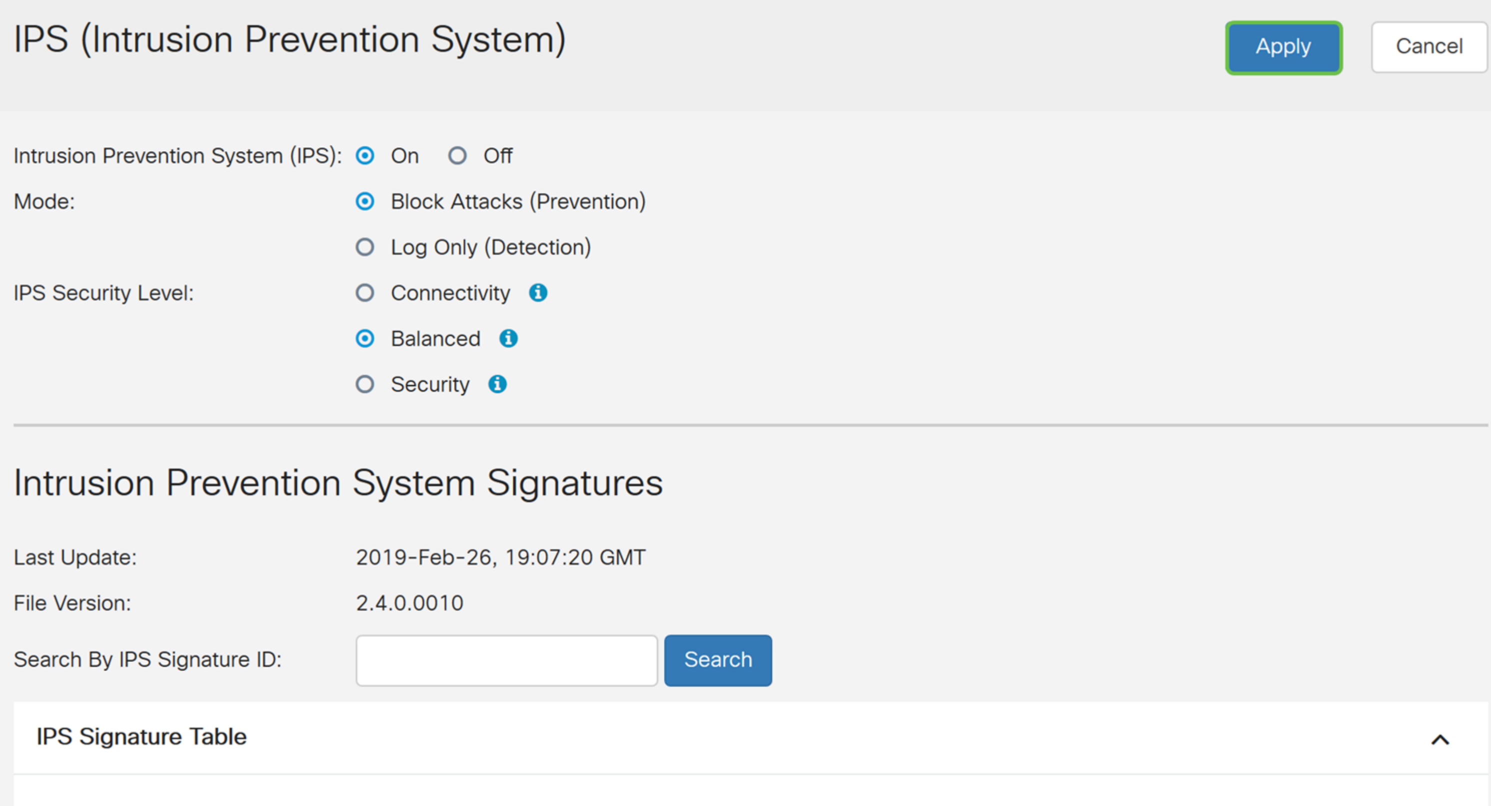
ID:	8000135
Name:	SERVER /etc/passwd misc attack
Impact:	Information Gathering.
Description:	This event is generated when an attempt is made to retrieve a protected system file on a host via a web request.
Recommendation:	Webservers should not be allowed to view or execute files and binaries outside 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

Step 11. At the bottom of the *IPS Signature Table*, select the arrows as well as the numbers to navigate back and forth on the table. You can also select the amount of lines (**50**, **100**, or **150**) per page in the *lines per page* drop-down list.



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

Step 12. Click **Apply** to save your changes to the running configuration file.



IPS (Intrusion Prevention System)

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

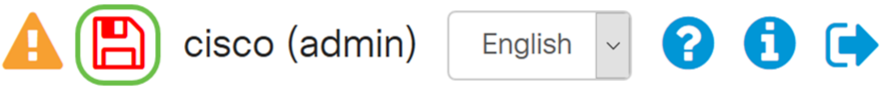
File Version: 2.4.0.0010

Search By IPS Signature ID:

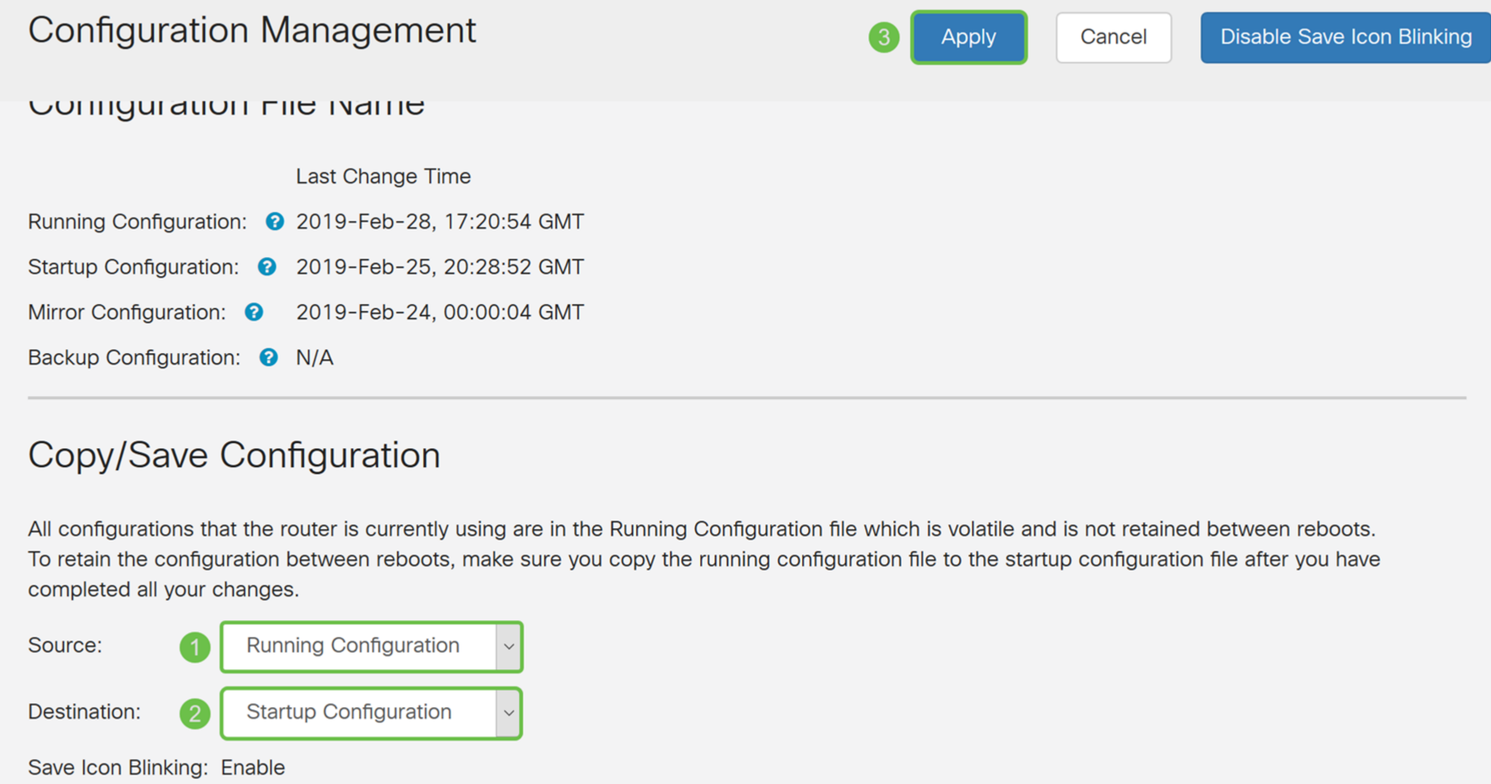
Note: All configurations that the router is using are currently in the running configuration file which is volatile and is not retained between reboots. In order to retain your configuration between reboots, copy your running configuration file to the startup configuration file.

In the next few steps, we will show you how to copy your running configuration to the startup configuration.

Step 13. Click the **Floppy Disk (Save)** icon at the top of the page. This will redirect you to the *Configuration Management* to save your running configuration to the startup configuration.



Step 14. In the *Configuration Management*, scroll down to the *Copy/Save Configuration* section. Ensure that the *Source* is **Running Configuration** and the *Destination* is **Startup Configuration**. Click **Apply**. This will copy the running configuration file to the startup configuration file to retain the configuration between reboots.



Configuration Management

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.

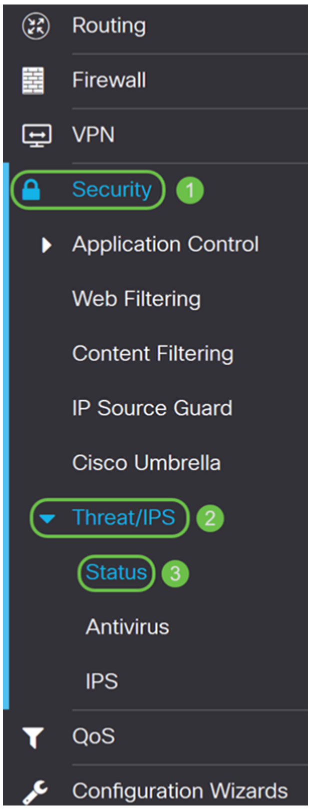
Source: 1 Running Configuration

Destination: 2 Startup Configuration

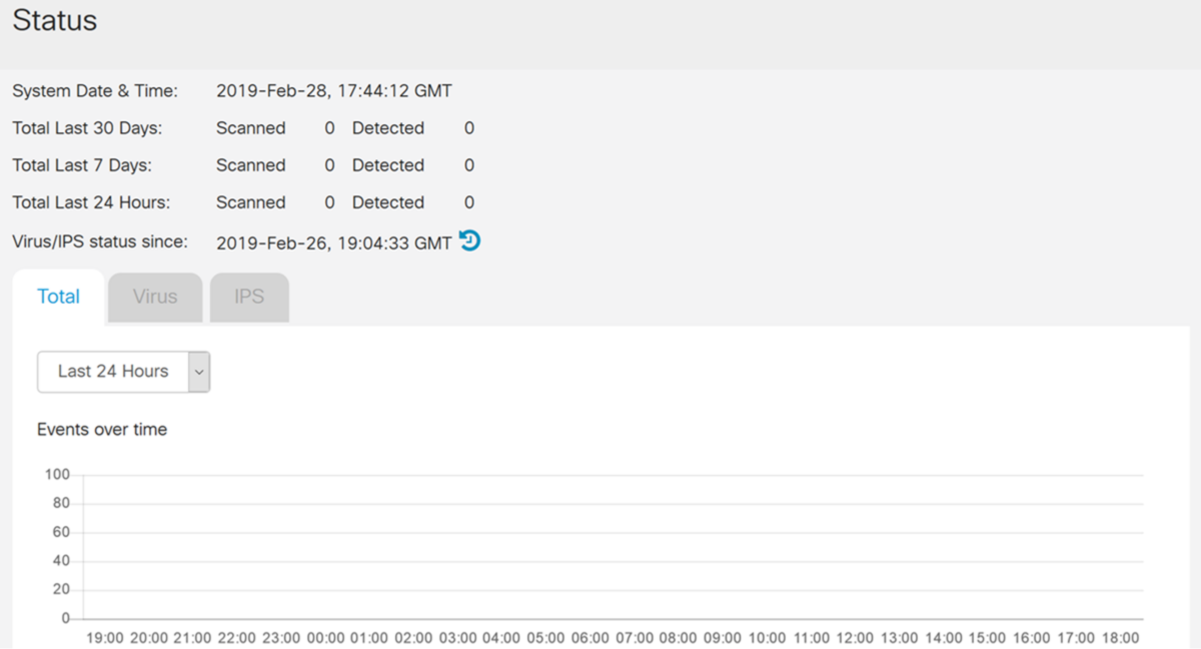
Save Icon Blinking: Enable

IPS Status

Step 1. Navigate to **Security > Threat/IPS > Status**.



Step 2. The *Status* page displays the details of the threats and attacks when the Anti Threat and IPS features are configured. The dashboard gives you a view of the entire events summary, and detailed information of threats and attacks detected as per selection such as day, week, and month.



Status

System Date & Time: 2019-Feb-28, 17:44:12 GMT

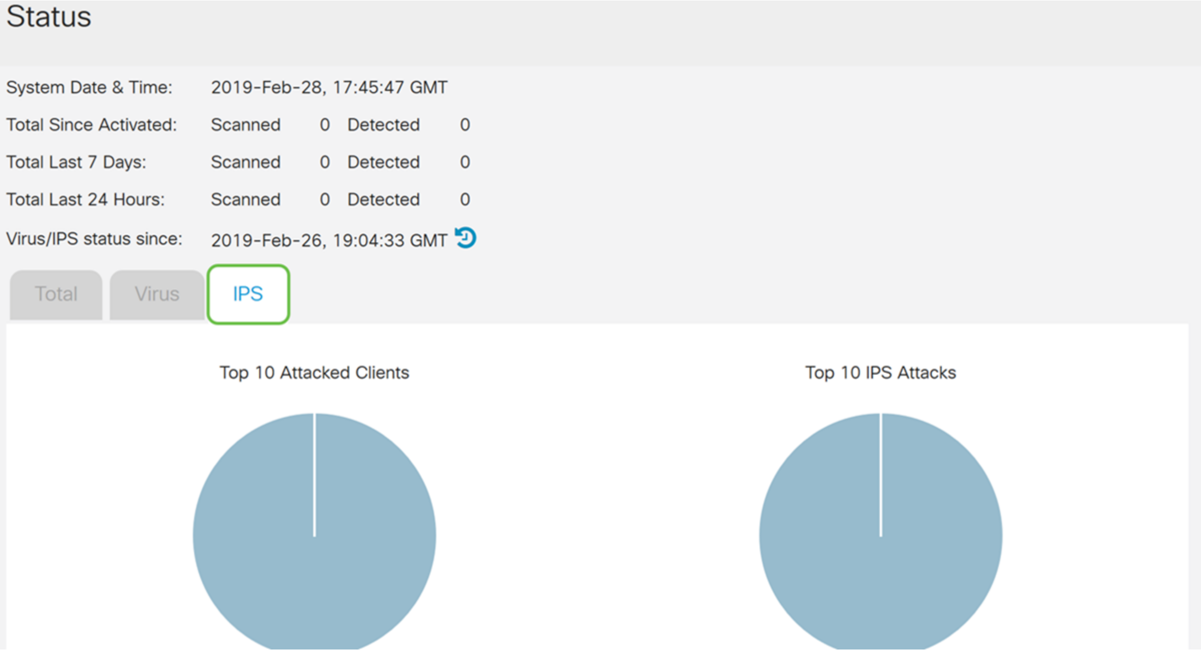
Total Last 30 Days: Scanned 0 Detected 0

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

Step 3. Click the **IPS** tab. This will display the top 10 attacked clients as well as the top 10 IPS attacks.



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

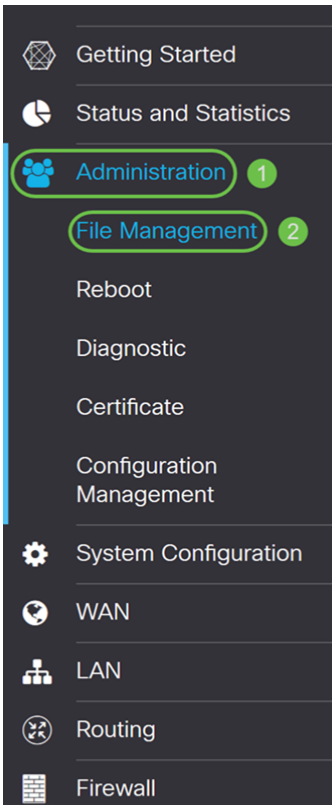
Virus/IPS status since: 2019-Feb-26, 19:04:33 GMT

Updating IPS Definitions

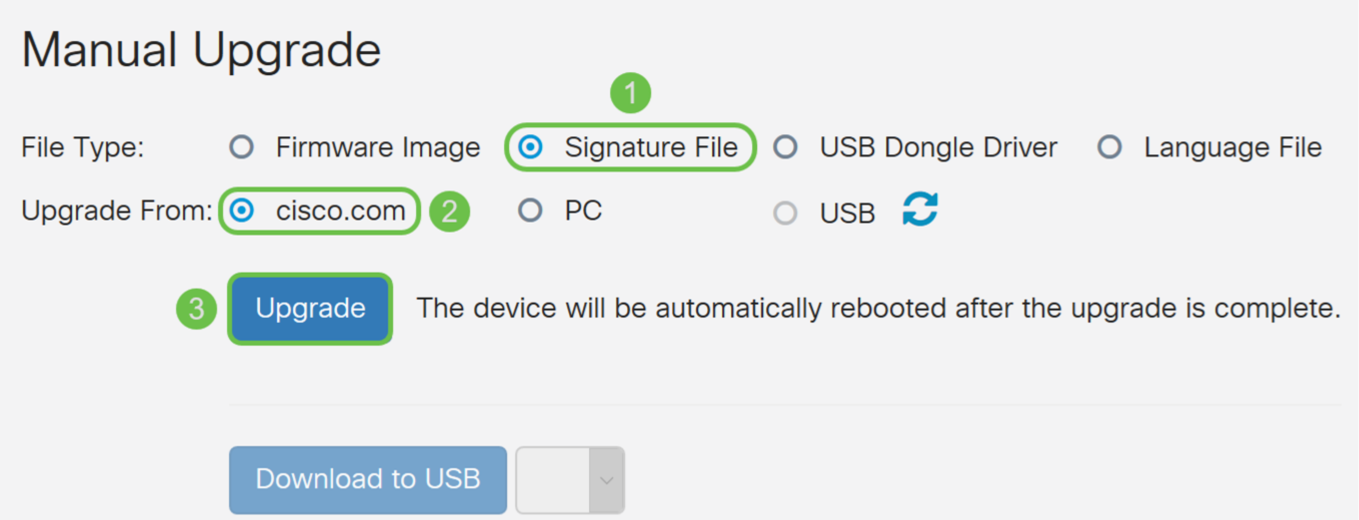
You can update the IPS definition either manually or automatically. Steps 1-2 will show you how to update the IPS definition manually while Steps 3-6 will show you how to update the IPS definition automatically.

Best Practice: It is recommended to update the security signatures automatically on a weekly basis.

Step 1. To manually update IPS definitions, navigate to **Administration > File Management**.



Step 2. Scroll down to the *Manual Upgrade* section in the *File Management* page. Choose **Signature File** for *File Type* and **cisco.com** for *Upgrade From*. Then press **Upgrade**. This will download the latest security signature and install it.


Manual Upgrade

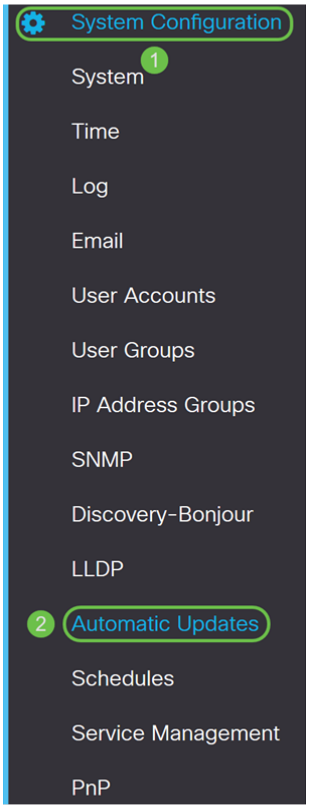
File Type: ○ Firmware Image ● Signature File ○ USB Dongle Driver ○ Language File

Upgrade From: ● cisco.com ○ PC ○ USB

Upgrade The device will be automatically rebooted after the upgrade is complete.

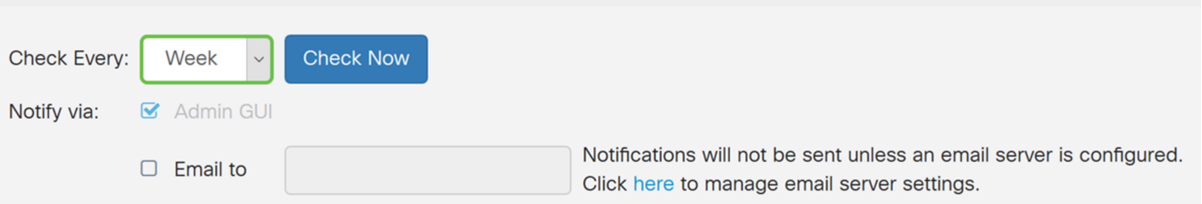
Download to USB

Step 3. To automatically update the IPS definitions, navigate to **System Configuration > Automatic Updates**.



Step 4. The *Automatic Updates* page opens. You have the option of checking for updates either on a weekly or monthly basis. You can have the router notify via email or the Web UI. In this example, we will be selecting to check every week.

Note: It is recommended to update security signatures automatically on a weekly basis.



Check Every: Week

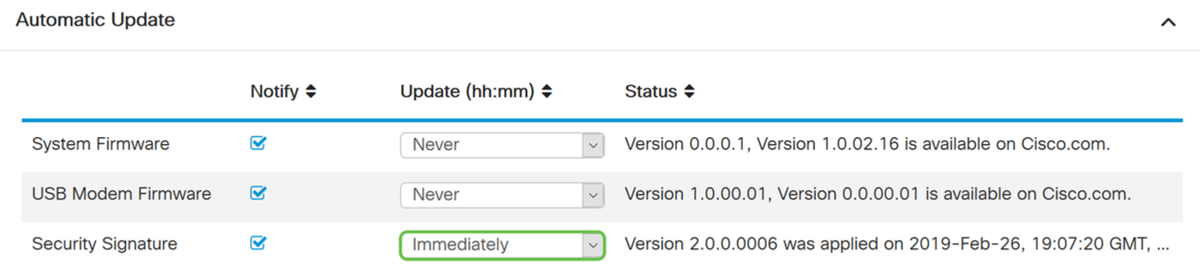
Check Now

Notify via: ☑ Admin GUI

□ Email to

Notifications will not be sent unless an email server is configured.
Click here to manage email server settings.

Step 5. Scroll down to the *Automatic Update* section and look for the *Security Signature* field. In the *Security Signature Update* drop-down list, select the time that you want to automatically update. In this example, we will be selecting **Immediately**.

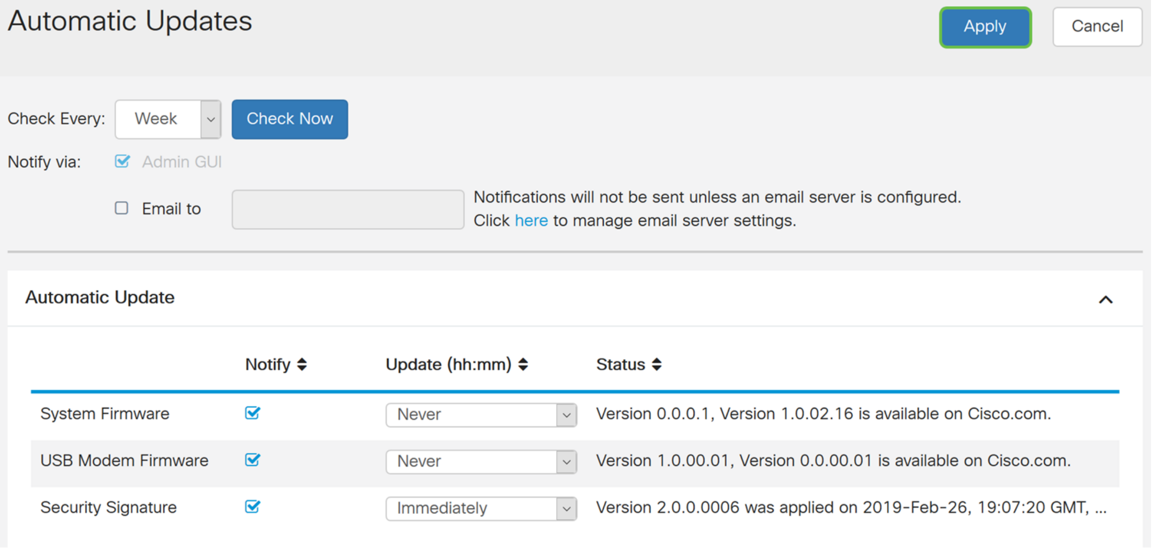


Automatic Update

	Notify	Update (hh:mm)	Status
System Firmware	☑	Never	Version 0.0.0.1, Version 1.0.02.16 is available on Cisco.com.
USB Modem Firmware	☑	Never	Version 1.0.00.01, Version 0.0.00.01 is available on Cisco.com.
Security Signature	☑	Immediately	Version 2.0.0.0006 was applied on 2019-Feb-26, 19:07:20 GMT, ...

Step 6. Click **Apply** to save the changes to the running configuration file.

Note: Remember to click the **Floppy Disk** icon on the top to navigate to the *Configuration Management* page to copy your running configuration file to the startup configuration file. This will help retain your configurations between reboots.



Check Every: Week

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	☑	Never	Version 0.0.0.1, Version 1.0.02.16 is available on Cisco.com.
USB Modem Firmware	☑	Never	Version 1.0.00.01, Version 0.0.00.01 is available on Cisco.com.
Security Signature	☑	Immediately	Version 2.0.0.0006 was applied on 2019-Feb-26, 19:07:20 GMT, ...

Conclusion

You should now have successfully configured Intrusion Prevention System on the RV34x series router.