

Configurazione dell'antivirus sul router serie RV34x

Obiettivo

L'obiettivo di questo documento è mostrare come configurare la funzionalità antivirus sui router serie RV34x.

Introduzione

L'antivirus protegge gli utenti della rete da infezioni e contenuto malware ricevuto tramite e-mail o dati. La funzionalità antivirus supporta i protocolli SMTP (Simple Mail Transfer Protocol), HTTP (Hypertext Transfer Protocol), FTP (File Transfer Protocol), POP3 (Post Office Protocol versione 3) e IMAP (Internet Message Access Protocol).

Il motore antivirus utilizza due componenti importanti: un classificatore che sa dove cercare e il database dei virus che sa cosa cercare. Il modulo classifica il file per tipo anziché basandosi sull'estensione. Il motore antivirus cerca i virus nel corpo e negli allegati dei messaggi ricevuti dal sistema; il tipo di file di un allegato consente di determinarne l'analisi.

Per informazioni sul malware, visita questo link: [Che cos'è il malware?](#).

Per informazioni su come configurare Umbrella, fare clic sul collegamento: [Configurazione di Cisco Umbrella RV34x](#).

Nota importante: Se il router è attualmente sottoposto a un carico di lavoro pesante, il problema potrebbe essere aggravato.

La tabella seguente fornisce le statistiche previste per le prestazioni nelle varie configurazioni. Questi valori devono essere utilizzati come guida, in quanto le prestazioni reali possono variare a causa di una serie di fattori.

	Connessioni simultanee	Velocità di connessione	Throughput HTTP	Throughput FTP
Impostazioni predefinite	40000	3000	982 MB/sec	981 MB/sec
Abilita controllo APP	15000-16000	1300	982 MB/sec	981 MB/sec
Abilita antivirus	16000	1500	982 MB/sec	981 MB/sec
Abilita IPS	17000	1300	982 MB/sec	981 MB/sec
Abilita Antivirus e IPS di App	15000-16000	1000	982 MB/sec	981 MB/sec

Control				
---------	--	--	--	--

I campi seguenti sono definiti come:

Connessioni simultanee - Il numero totale di connessioni simultanee. Ad esempio, se si sta scaricando un file da un sito, si tratta di una connessione, lo streaming audio da Spotify sarà un'altra connessione, rendendola due connessioni simultanee.

Frequenza di connessione: il numero di richieste di connessione al secondo che è possibile elaborare.

Throughput HTTP/FTP: il throughput HTTP e FTP corrisponde alla velocità di download in MB/sec.

Le licenze di protezione sono state aggiornate per includere antivirus oltre alle applicazioni e ai filtri Web esistenti. Per ottenere una licenza di protezione, è necessario uno smart account. Se non si dispone di uno smart account attivo, sarà necessaria la sezione 1 di questo documento.

per informazioni su come configurare Intrusion Prevention System su RV34x, fare clic [qui](#).

Dispositivi interessati

- RV34x

Versione del software

- 1.0.03.5

Sommario

1. [Struttura delle licenze](#)
2. [Configurazione antivirus](#)
3. [Stato minacce/IPS](#)
4. [Aggiornamento delle definizioni antivirus](#)
5. [Conclusioni](#)

Struttura delle licenze - Firmware versione 1.0.3.15 e successive

Inoltre, AnyConnect sarà a pagamento solo per le licenze client.

Per ulteriori informazioni sulle licenze AnyConnect sui router serie RV340, consultare l'articolo su: [Licenze AnyConnect per i router serie RV340](#).

Configurazione antivirus

Passaggio 1. Se non è stato effettuato l'accesso al router, accedere alla pagina di configurazione Web.



Router

Username

Password

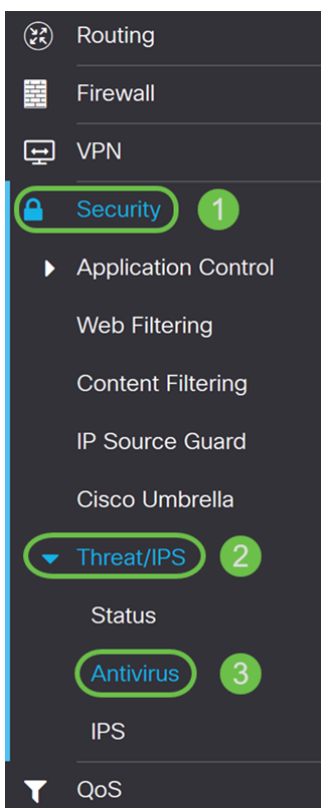
English ▾

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.

Passaggio 2. Selezionare **Security > Threat/IPS > Antivirus**.



Passaggio 3. Fare clic sul pulsante di opzione **On** per attivare la funzione antivirus.

Antivirus

Enable

On Off

Applications To Scan:	Protocol	Enable	Action
	HTTP:	<input type="checkbox"/>	None
	FTP:	<input type="checkbox"/>	None
	SMTP Email Attachments:	<input type="checkbox"/>	None
	POP3 Email Attachments:	<input type="checkbox"/>	None
	IMAP Email Attachments:	<input type="checkbox"/>	None
	<input type="checkbox"/> Enable File Size Threshold		
	AV scan when file size is less than	<input type="text" value="1"/>	MB (Range: 1-100)

Passaggio 4. Selezionare le caselle di controllo **Abilita** per abilitare *le applicazioni da analizzare* nei protocolli. In questo esempio sono stati abilitati tutti i protocolli (**HTTP, FTP, SMTP, POP3 e IMAP**). Selezionare quindi l'azione appropriata. Le opzioni seguenti sono definite come:

- **Log:** selezionare questa opzione per generare il log solo (con informazioni sul client, ID firma, ecc.) quando vengono identificate le minacce. Non influisce sulla connessione.
- **Eliminazione registro** - Selezionare questa opzione per eliminare la connessione quando vengono identificate minacce e il messaggio viene registrato per l'eliminazione.

Nota: In caso di minaccia identificata in un allegato, il file verrà troncato durante il processo di download.

Applications To Scan:	Protocol	Enable	Action
	HTTP:	<input checked="" type="checkbox"/>	Log Destroy
	FTP:	<input checked="" type="checkbox"/>	Log
	SMTP Email Attachments:	<input checked="" type="checkbox"/>	Log Destroy
	POP3 Email Attachments:	<input checked="" type="checkbox"/>	Log Destroy
	IMAP Email Attachments:	<input checked="" type="checkbox"/>	Log Destroy

Passaggio 5. Se si desidera che l'antivirus disponga di una dimensione di file necessaria per la scansione, controllare la **Soglia dimensioni file abilitata**. Immettere quindi le dimensioni del file che possono essere analizzate dall'antivirus. L'intervallo è compreso tra 1 e 100 MB.

Nell'esempio, sono stati immessi **50 MB**.

Enable File Size Threshold

1 AV scan when file size is less than 2 MB (Range: 1-100)

Passaggio 6. Nella sezione *Database virus*, l'*ultimo aggiornamento* mostra la data e l'ora dell'ultima firma aggiornata. *Versione file* indica la versione della firma in uso.

Virus Database

Last Update: 2019-Mar-06, 18:44:31 GMT

File Version: 2.5.0.1003

Passaggio 7. Fare clic sul pulsante **Applica** per salvare le modifiche.

Antivirus

On Off

Applications To Scan:	Protocol	Enable	Action
	HTTP:	<input checked="" type="checkbox"/>	Log Destroy
	FTP:	<input checked="" type="checkbox"/>	Log
	SMTP Email Attachments:	<input checked="" type="checkbox"/>	Log Destroy
	POP3 Email Attachments:	<input checked="" type="checkbox"/>	Log Destroy
	IMAP Email Attachments:	<input checked="" type="checkbox"/>	Log Destroy
<input checked="" type="checkbox"/> Enable File Size Threshold			
	AV scan when file size is less than	<input type="text" value="50"/>	MB (Range: 1-100)

Se si preme **Applica**, la configurazione viene salvata solo nella configurazione in esecuzione. Per mantenere la configurazione tra un riavvio e l'altro, è necessario copiarla nella configurazione di avvio.

Passaggio 8. Fare clic sull'icona **Disco floppy (Salva)** nella parte superiore della pagina. In questo modo si verrà reindirizzati alla *gestione della configurazione* per copiare la configurazione in esecuzione nella configurazione di avvio.



Passaggio 9. In *Gestione configurazione*, scorrere verso il basso fino alla sezione *Copia/Salva configurazione*. Verificare che l'*origine* stia **eseguendo la configurazione** e che la *destinazione* sia la **configurazione di avvio**. Fare clic su **Apply** (Applica). Il file della configurazione in esecuzione verrà copiato nel file della configurazione di avvio per conservare la configurazione tra un riavvio e l'altro.

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

Stato minaccia/IPS

Passaggio 1. Passare a **Sicurezza > Minaccia/IPS > Stato**.


The screenshot shows a dark-themed navigation menu with the following items: Routing, Firewall, VPN, Security (1), Application Control, Web Filtering, Content Filtering, IP Source Guard, Cisco Umbrella, Threat/IPS (2), Status (3), Antivirus, IPS, and QoS. The 'Security' item is highlighted with a green circle and a '1' in a green circle. The 'Threat/IPS' item is highlighted with a green circle and a '2' in a green circle. The 'Status' item is highlighted with a green circle and a '3' in a green circle.

Passaggio 2. Nella pagina *Stato*, è possibile visualizzare la data e l'ora del sistema, le minacce rilevate e analizzate e gli attacchi della scheda selezionata. Per impostazione predefinita, è possibile visualizzare lo stato della scheda Totale.

Status

System Date & Time: 2019-Mar-06, 22:44:55 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-Mar-06, 18:41:53 GMT 

Total

Virus

IPS

Last 24 Hours

Events over time




Passaggio 3. Nell'elenco a discesa della scheda *Totale* è possibile selezionare **Ultime 24 ore**, **Settimana** o **Mese** per visualizzare gli eventi.

Status

System Date & Time: 2019-Mar-06, 22:44:55 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-Mar-06, 18:41:53 GMT 

Total

Virus

IPS

Last 24 Hours

Events over time



Passaggio 4. Fare clic sulla scheda **Virus**. Nella scheda *Virus*, viene visualizzato quanto segue:


- **Primi 10 client interessati** - elenco di indirizzi MAC interessati.
- **Primi 10 virus rilevati** - l'elenco delle minacce rilevate.

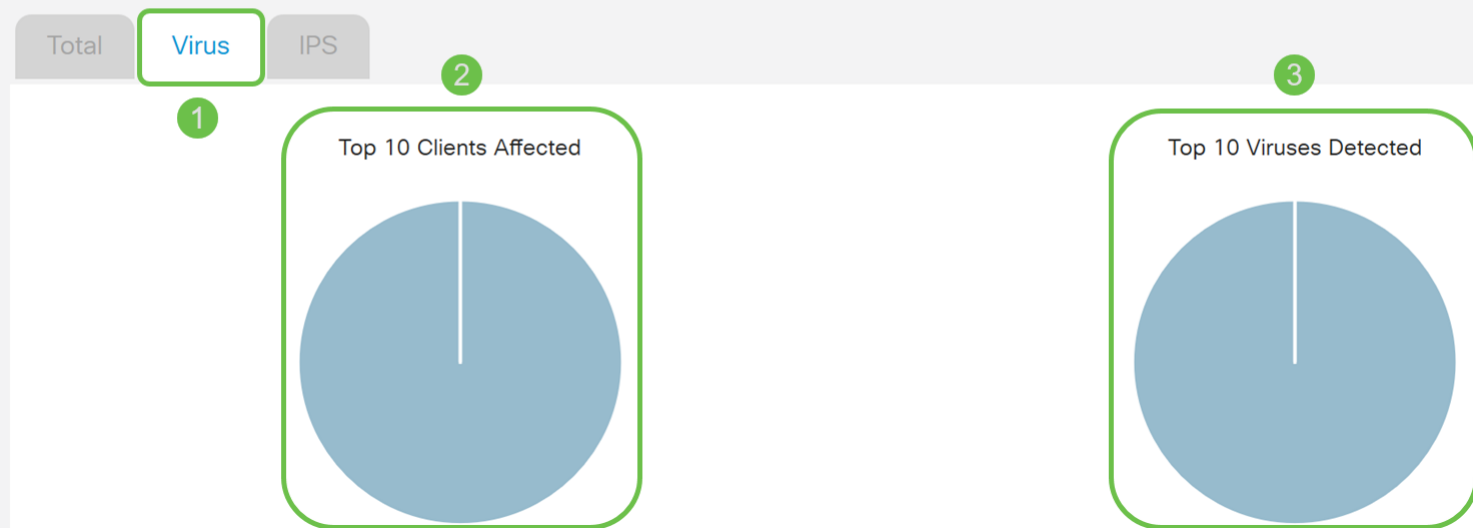
Nota: È possibile passare il mouse sul grafico a torta per visualizzare ulteriori dettagli.

Status

System Date & Time: 2019-Mar-06, 22:35:48 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-Mar-06, 18:41:53 GMT 

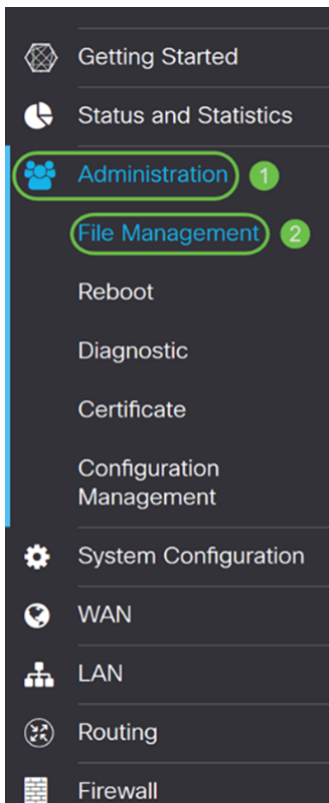


Aggiornamento delle definizioni antivirus

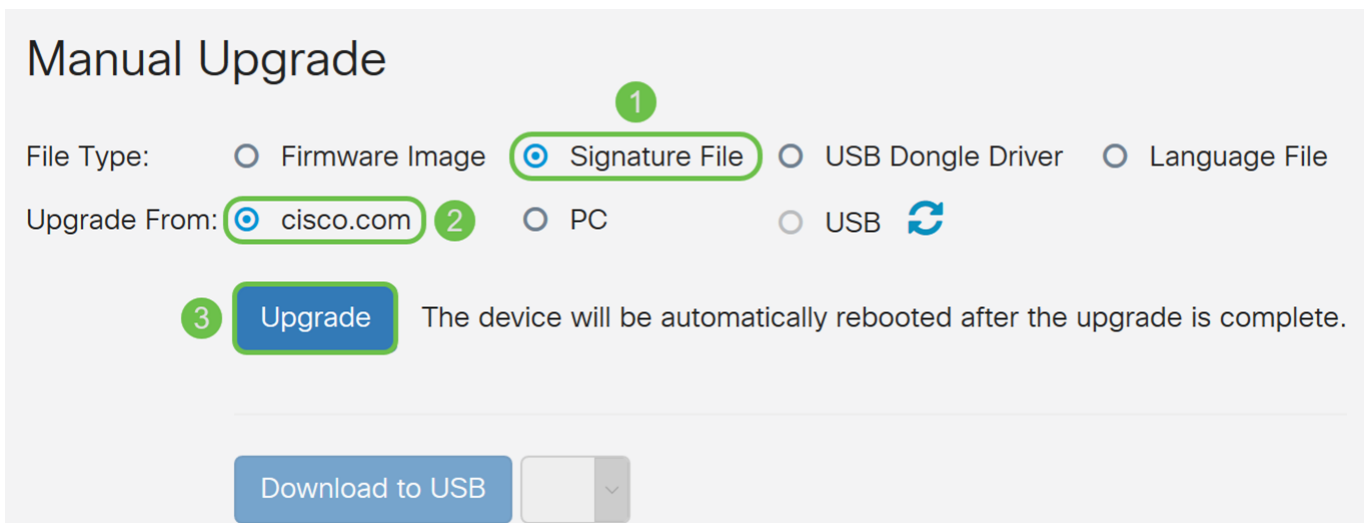
È possibile aggiornare il database antivirus manualmente o automaticamente. I passaggi da 1 a 2 mostrano come aggiornare il database antivirus manualmente, mentre i passaggi da 3 a 6 mostrano come aggiornare il database antivirus automaticamente.

Procedure ottimali: Si consiglia di aggiornare automaticamente le firme di protezione ogni settimana.

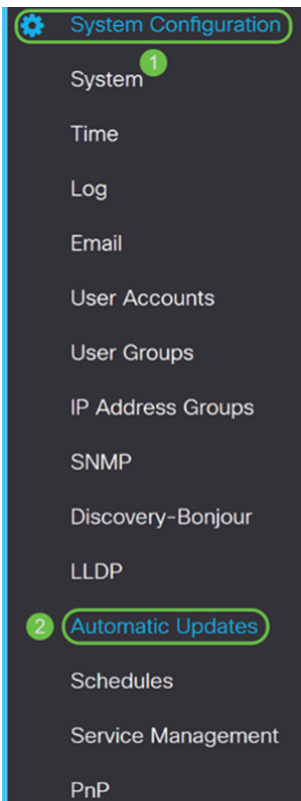
Passaggio 1. Per aggiornare manualmente il database antivirus, passare ad **Amministrazione > Gestione file**.



Passaggio 2. Scorrere fino alla sezione *Aggiornamento manuale* della pagina *Gestione file*. Selezionare **Signature File** per *File Type* (Tipo file) e **cisco.com** per *Upgrade da* (*Aggiorna da*). Quindi premere **Aggiorna**. Verrà scaricata la firma di protezione più recente e installata.



Passaggio 3. Per aggiornare automaticamente il database antivirus, selezionare **Configurazione di sistema > Aggiornamenti automatici**.



Passaggio 4. Viene visualizzata la pagina *Aggiornamenti automatici*. È possibile verificare la disponibilità di aggiornamenti su base settimanale o mensile. È possibile impostare la notifica del router tramite posta elettronica o interfaccia utente Web. In questo esempio verrà selezionato un controllo ogni settimana.

Nota: Si consiglia di aggiornare automaticamente le firme di protezione ogni settimana.

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.

Passaggio 5. Scorrere verso il basso fino alla sezione *Aggiornamento automatico* e cercare il campo *Firma di sicurezza*. Nell'elenco a discesa *Aggiornamento firma di sicurezza*, selezionare l'ora che si desidera aggiornare automaticamente. In questo esempio, la selezione verrà eseguita **immediatamente**.

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, ...

Passaggio 6. Fare clic su **Apply** (Applica) per salvare le modifiche nel file di configurazione in esecuzione.

Nota: Ricordarsi di fare clic sull'icona **Disco floppy** nella parte superiore per accedere alla pagina *Gestione configurazione* e copiare il file di configurazione in esecuzione nel file della configurazione di avvio. In questo modo, le configurazioni verranno mantenute tra un riavvio e l'altro.

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, ...

Conclusioni

A questo punto, è necessario configurare l'antivirus sul router serie RV34x.

Per ulteriori informazioni, consultare le seguenti risorse.

- **Community router:** [Community di supporto Cisco Small Business](#)
- **Domande frequenti sulla serie RV34x:** [Serie RV34x Router: domande frequenti](#)