

Konfigurieren von Antivirus auf dem Router der Serie RV34x

Ziel

In diesem Dokument wird die Konfiguration von Antivirus auf Routern der Serie RV34x erläutert.

Einführung

Der Antivirus schützt Netzwerkbenutzer vor Infektionen und Malware-Inhalten, die in E-Mails oder Daten empfangen werden. Die Antivirus-Funktion unterstützt die Protokolle Simple Mail Transfer Protocol (SMTP), Hypertext Transfer Protocol (HTTP), File Transfer Protocol (FTP), Post Office Protocol Version 3 (POP3) und Internet Message Access Protocol (IMAP).

Die Antivirus-Engine verwendet zwei wichtige Komponenten: einen Klassifizierer, der weiß, wo er suchen soll, und die Virusdatenbank, die weiß, worauf er achten muss. Die Engine klassifiziert die Datei nach Typ und nicht nach der Erweiterung. Die Virusengine sucht in den Körpern und Anlagen der vom System empfangenen Nachrichten nach Viren. Der Dateityp eines Anhangs hilft dabei, dessen Prüfung zu bestimmen.

Unter dem folgenden Link erfahren Sie, was Malware ist: [Was ist Malware?](#).

Um zu erfahren, wie Umbrella konfiguriert wird, klicken Sie auf den Link: [Konfigurieren der Cisco Umbrella RV34x](#).

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

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

	Gleichzeitige Verbindungen	Verbindungsrate	HTTP-Durchsatz	FTP-Durchsatz
Standardeinstellungen	40000	3000	982 MB/s	981 MB/s
APP-Steuerung aktivieren	15.000-16.000	1300	982 MB/s	981 MB/s
Antivirus aktivieren	16.000	1500	982 MB/s	981 MB/s
IPS aktivieren	17.000	1300	982 MB/s	981 MB/s
Aktivieren von	15.000-16.000	1000	982 MB/s	981 MB/s

Anwendungs- kontr olle Antivirus und IPS				
--	--	--	--	--

Die folgenden Felder sind definiert als:

Parallele Verbindungen - Die Gesamtzahl gleichzeitiger Verbindungen Wenn Sie beispielsweise eine Datei von einer Site herunterladen, ist dies eine Verbindung, Audio von Spotify streamen, also eine andere Verbindung, wodurch es zwei gleichzeitige Verbindungen gibt.

Verbindungsrate - Die Anzahl der Verbindungsanforderungen pro Sekunde, die verarbeitet werden können.

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

Sicherheitslizenzen wurden aktualisiert und umfassen neben der vorhandenen Anwendungs- und Webfilterung auch Antivirus. Für eine Sicherheitslizenz ist ein Smart Account erforderlich. Wenn Sie noch kein aktives Smart Account haben, ist Abschnitt 1 dieses Dokuments erforderlich.

Um zu erfahren, wie Sie das Intrusion Prevention System auf RV34x konfigurieren, klicken Sie [hier](#).

Anwendbare Geräte

- RV34x

Softwareversion

- 1.0.03.5

Inhaltsverzeichnis

1. [Lizenzierungsstruktur](#)
2. [Konfigurieren von Antivirus](#)
3. [Bedrohungs-/IPS-Status](#)
4. [Aktualisieren der Virendefinitionen](#)
5. [Schlussfolgerung](#)

Lizenzierungsstruktur - Firmware-Versionen 1.0.3.15 und höher

Für AnyConnect wird künftig nur noch Client-Lizenzen berechnet.

Weitere Informationen zur AnyConnect-Lizenzierung für Router der Serie RV340 finden Sie in folgendem Artikel: [AnyConnect-Lizenzierung für Router der Serie RV340](#).

Konfigurieren von Antivirus

Schritt 1: Wenn Sie sich nicht beim Router angemeldet haben, melden Sie sich auf der Webseite für die Konfiguration an.



Router

Username

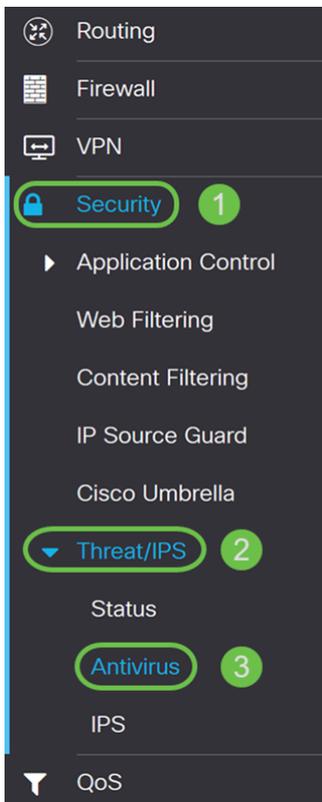
Password

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.

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



Schritt 3: Klicken Sie auf das Optionsfeld **Ein**, um die Virenschutzfunktion zu aktivieren.

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)

Schritt 4: Aktivieren Sie das bzw. die Kontrollkästchen **Enable (Aktivieren)**, um *Anwendungen für die Protokolle* zu aktivieren. In diesem Beispiel wurden alle Protokolle aktiviert (**HTTP, FTP, SMTP, POP3** und **IMAP**). Wählen Sie dann die entsprechende Aktion aus. Die folgenden Optionen sind definiert als:

- **Protokoll** - Wählen Sie diese Option aus, um das Protokoll nur dann zu generieren (mit Clientinformationen, Signatur-ID usw.), wenn die Bedrohungen identifiziert werden. Die

Verbindung wird dadurch nicht beeinträchtigt.

• **Log Destroy (Zerstören von Protokolldateien):** Wählen Sie diese Option aus, um die Verbindung beim Erkennen von Bedrohungen zu verwerfen und die Nachricht zum Löschen zu protokollieren.

Hinweis: Wenn eine Bedrohung in einem Anhang identifiziert wird, wird die Datei während des Download-Prozesses abgeschnitten.

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

Schritt 5: Wenn der Virenschutz eine erforderliche Dateigröße zum Scannen aufweisen soll, überprüfen Sie den **Schwellenwert Dateigröße aktivieren**. Geben Sie dann die Dateigröße ein, die der Virenschutz prüfen kann. Der Bereich liegt zwischen 1 und 100 MB.

In diesem Beispiel wurden **50 MB** eingegeben.

Enable File Size Threshold

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

Schritt 6: Im Abschnitt *Virendatenbank* zeigt das *letzte Update* das Datum und die Uhrzeit der letzten aktualisierten Signatur an. *Die Dateiversion* zeigt die verwendete Signaturversion an.

Virus Database	
Last Update:	2019-Mar-06, 18:44:31 GMT
File Version:	2.5.0.1003

Schritt 7: Klicken Sie auf die Schaltfläche **Übernehmen**, um die Änderungen zu speichern.

Antivirus

Apply

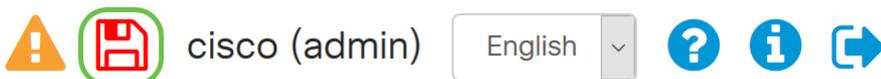
Cancel

Enable 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)

Durch Drücken von **Apply** wird die Konfiguration nur in der aktuellen Konfiguration gespeichert. Sie müssen die aktuelle Konfiguration in die Startkonfiguration kopieren, wenn Sie die Konfiguration zwischen Neustarts beibehalten möchten.

Schritt 8: Klicken Sie oben auf der Seite auf das Symbol **Diskette (Speichern)**. Dadurch werden Sie zur *Konfigurationsverwaltung* umgeleitet, um Ihre aktuelle Konfiguration in die Startkonfiguration zu kopieren.



Schritt 9: Blättern Sie im *Konfigurationsmanagement* nach unten zum Abschnitt "*Konfiguration kopieren/speichern*". Stellen Sie sicher, dass die *Quelle* die **Konfiguration ausführt** und das *Ziel* die **Startkonfiguration** ist. Klicken Sie auf **Übernehmen**. Dadurch wird die aktuelle Konfigurationsdatei in die Startkonfigurationsdatei kopiert, um die Konfiguration zwischen Neustarts beizubehalten.

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.

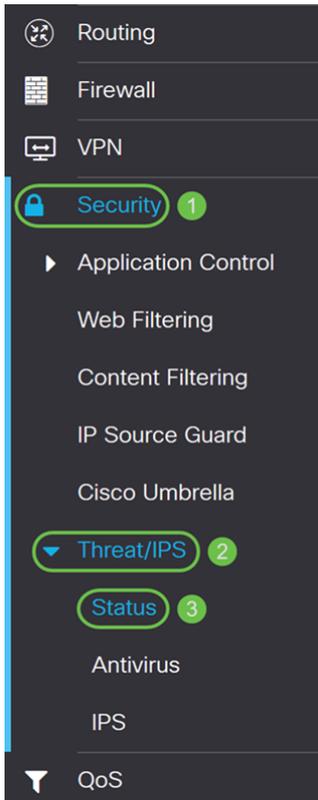
Source: **1** Running Configuration

Destination: **2** Startup Configuration

Save Icon Blinking: Enable

Bedrohungs-/IPS-Status

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



Schritt 2: Auf der Seite *Status* können Sie das Systemdatum und die Systemzeit, gescannte und erkannte Bedrohungen sowie Angriffe auf die ausgewählte Registerkarte anzeigen. Standardmäßig wird der Status der Registerkarte "Insgesamt" angezeigt.

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



Schritt 3: In der Dropdown-Liste unter der Registerkarte *Total (Gesamt)* können Sie die Ereignisse zur Anzeige der Ereignisse **Letzte 24 Stunden**, **Woche** oder **Monat** auswählen.

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



Schritt 4: Klicken Sie auf die Registerkarte **Virus**. Auf der Registerkarte *Virus* wird Folgendes angezeigt:

- **Die 10 wichtigsten betroffenen Clients** - die Liste der betroffenen MAC-Adressen.
- **Top 10 erkannte Viren** - Liste der erkannten Bedrohungen

Hinweis: Für weitere Informationen können Sie die Maus über das Tortendiagramm bewegen.

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 

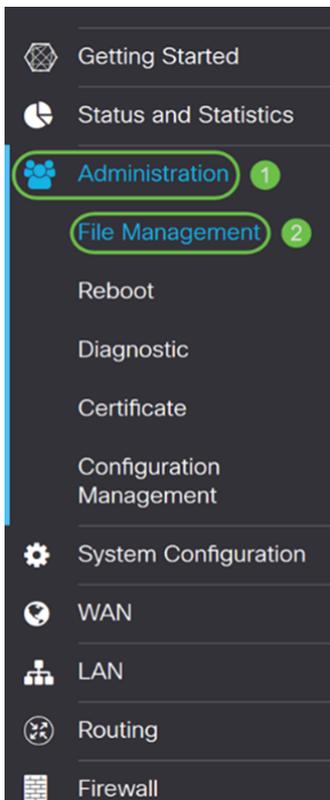


Aktualisieren der Virendefinitionen

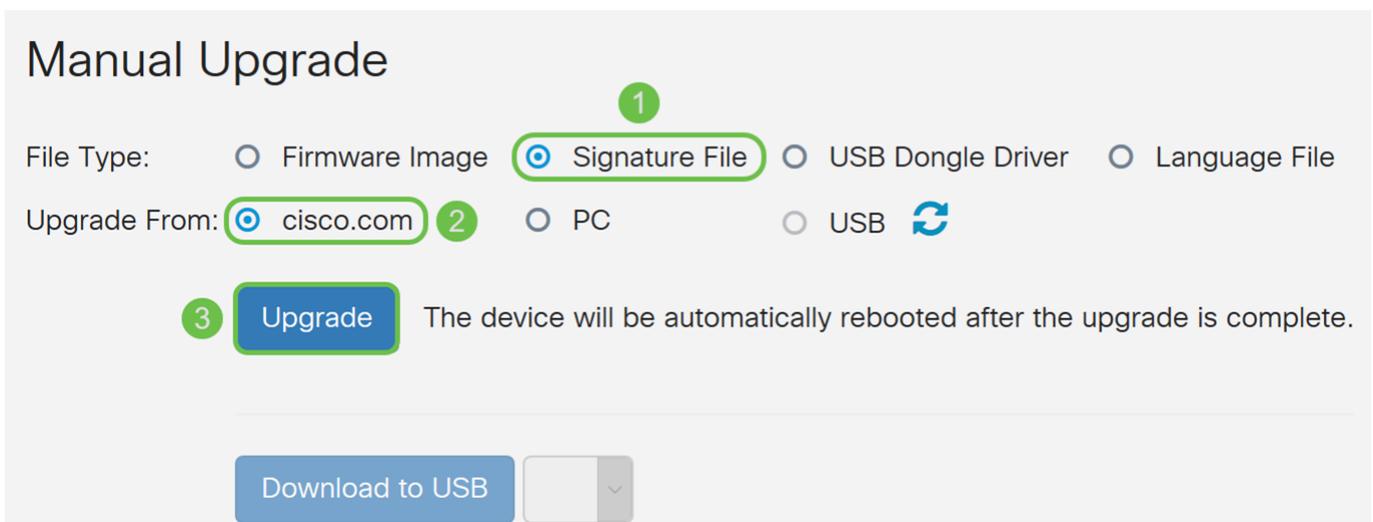
Sie können die Antivirus-Datenbank entweder manuell oder automatisch aktualisieren. Die Schritte 1-2 zeigen Ihnen, wie Sie die Antivirus-Datenbank manuell aktualisieren, während die Schritte 3-6 zeigen, wie Sie die Antivirus-Datenbank automatisch aktualisieren.

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

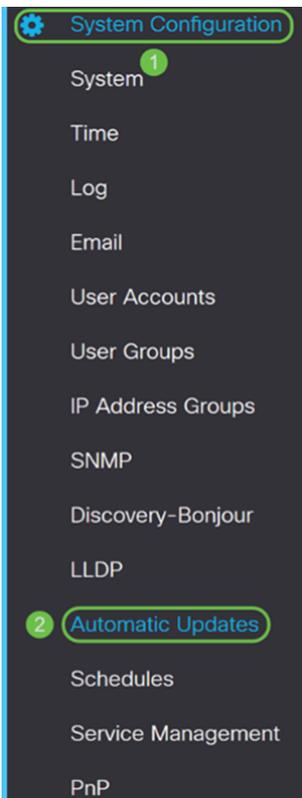
Schritt 1: Um die Antivirus-Datenbank manuell zu aktualisieren, navigieren Sie zu **Administration > File Management**.



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



Schritt 3: Um die Virenschutzdatenbank automatisch zu aktualisieren, wählen Sie **Systemkonfiguration > Automatische Updates** aus.



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

Hinweis: Es wird empfohlen, Sicherheitssignaturen wöchentlich automatisch zu aktualisieren.

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.

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

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, ...

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

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

Neustarts beibehalten.

Automatic Updates Apply Cancel

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.

Automatic Update ^

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

Schlussfolgerung

Sie sollten nun Virenschutz auf Ihrem Router der Serie RV34x konfiguriert haben.

Weitere Informationen finden Sie in den folgenden Ressourcen.

- Router-Community: [Cisco Small Business Support Community](#)
- Häufig gestellte Fragen zur Serie RV34x: [Häufig gestellte Fragen zu Routern der Serie RV34x](#)