

在RV34x系列路由器上配置防病毒軟體

目標

本文檔旨在向您展示如何在RV34x系列路由器上配置防病毒軟體。

簡介

防病毒軟體可保護網路使用者免受電子郵件或資料中接收的感染和惡意軟體內容的侵害。防病毒功能支援簡單郵件傳輸協定(SMTP)、超文本傳輸協定(HTTP)、檔案傳輸協定(FTP)、郵局協定第3版(POP3)和網際網路消息訪問協定(IMAP)協定。

防病毒引擎使用兩個重要元件：一個是知道要查詢的分類器，另一個是知道要查詢什麼的病毒資料庫。引擎按型別而不是依靠副檔名對檔案進行分類。病毒引擎查詢系統接收的郵件正文和附件中的病毒；附件的檔案型別有助於確定其掃描方式。

要瞭解惡意軟體是什麼，請簽出以下連結：[什麼是惡意軟體？](#)。

要瞭解如何配置Umbrella，請按一下連結：[配置Cisco Umbrella RV34x](#)。

重要附註：如果路由器當前工作負荷過重，可能會使問題惡化。

下表給出了不同配置下的預期效能統計資訊。這些值應作為指導，因為實際績效可能因多種因素而不同。

	併發連線	連線速率	HTTP吞吐量	FTP吞吐量
預設設定	40000	3000	982MB/秒	981MB/秒
啟用APP控制	15000-16000	1300	982MB/秒	981MB/秒
啟用防病毒	16000	1500	982MB/秒	981MB/秒
啟用IPS	17000	1300	982MB/秒	981MB/秒
啟用App Control防病毒和IPS	15000-16000	1000	982MB/秒	981MB/秒

以下欄位定義為：

併發連線 — 併發連線的總數。例如，如果您從一個站點下載檔案，即一個連線，從Spotify流式傳輸音訊即另一個連線，從而使它成為兩個併發連線。

連線速率 — 每秒可處理的連線請求數。

HTTP/FTP吞吐量- HTTP和FTP吞吐量是下載速率 (MB/秒) 。

安全許可證已更新，除了現有的應用程式和Web過濾之外，還包含防病毒軟體。需要智慧帳戶才能獲得安全許可證。如果您尚未擁有活動的智慧帳戶，則需要本文檔的第1部分。

要瞭解如何在RV34x上配置入侵防禦系統，請按一下[此處](#)。

適用裝置

- RV34x

軟體版本

- 1.0.03.5

目錄

1. [許可結構](#)
2. [配置防病毒](#)
3. [威脅/IPS狀態](#)
4. [更新防病毒定義](#)
5. [結論](#)

許可結構 — 韌體版本1.0.3.15及更高版本

接下來，AnyConnect將只對客戶端許可證收費。

有關RV340系列路由器上的AnyConnect許可的其他資訊，請參閱以下文章：[RV340系列路由器的AnyConnect許可](#)。

配置防病毒

步驟1。如果您尚未登入路由器，請登入Web組態頁面。



Router

Username

Password

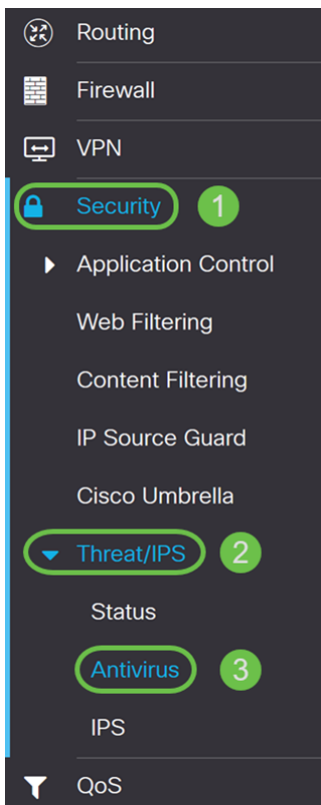
English ▾

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.

步驟2. 導覽至 **Security > Threat/IPS > Antivirus**。



步驟3. 按一下 **On** 單選按鈕啟用防病毒功能。

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)

步驟4. 勾選**Enable** 覆取方塊以啟用 *Applications to Scan on the protocols*。在本例中，我們啟用了所有協定(HTTP、FTP、SMTP、POP3和IMAP)。然後選擇適當的操作。以下選項定義為：

- **Log** — 選擇此選項僅在識別威脅時生成日誌 (包含客戶端資訊、簽名ID等)。不會影響連線。

Log Destroy

附註：如果附件中發現威脅，它將在下載過程中截斷檔案。

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

步驟5. 如果您希望防病毒軟體具有所需的檔案大小進行掃描，請選中**Enable File Size Threshold**。然後輸入防病毒程式可以掃描的檔案大小。範圍為1-100 MB。

在本例中，輸入了**50 MB**。

Enable File Size Threshold
1 AV scan when file size is less than 2 50 MB (Range: 1-100)

步驟6.在病毒資料庫部分，上次更新顯示上次更新簽名的日期和時間。檔案版本顯示正在使用的簽名版本。

Virus Database

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

File Version: 2.5.0.1003

步驟7.按一下Apply按鈕以儲存變更。

Antivirus

Apply

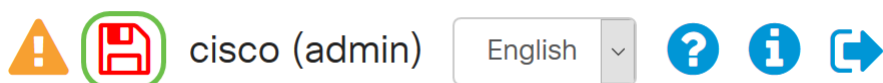
Cancel

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	50	MB (Range: 1-100)

按Apply僅將配置儲存到運行配置。如果要在重新啟動之間保留配置，則需要將運行配置複製到啟動配置。

步驟8.按一下頁面頂部的Floppy Disk(Save)圖示。這會將您重新導向至組態管理，將執行中的組態複製到啟動組態。



步驟9.在組態管理中，向下滾動到複製/儲存組態一節。請確認Source是Running Configuration，而Destination是Startup Configuration。按一下「Apply」。此操作會將運行配置檔案複製到啟動配置檔案中，以便在重新啟動之間保留配置。

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

威脅/IPS狀態

步驟1. 導覽至 Security > Threat/IPS > Status。


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 expanded, and its 'Status' sub-item is highlighted with a green circle and a '3' in a green circle.

步驟2. 在 Status 頁面中，您可以檢視選定頁籤的系統日期和時間、掃描和檢測到的威脅以及攻擊。預設情況下，您可以檢視「合計」頁籤的狀態。

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 

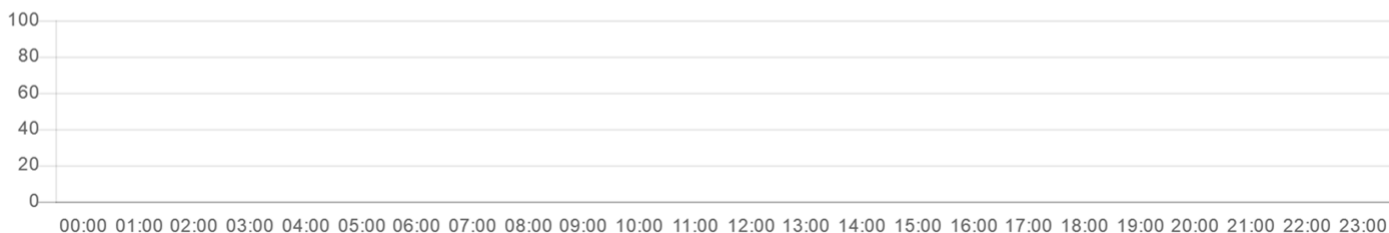
Total

Virus

IPS

Last 24 Hours

Events over time




步驟3.在 *Total* 索引標籤下的下拉式清單中，可以選擇 **Last 24 hours**、**Week**或**Month**以顯示事件。

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



步驟4.按一下 **Virus** 索引標籤。在 *Virus* 頁籤中，將顯示以下內容：


- 受影響的10大客戶端 — 受影響的mac地址清單。
- 檢測到的前10個病毒

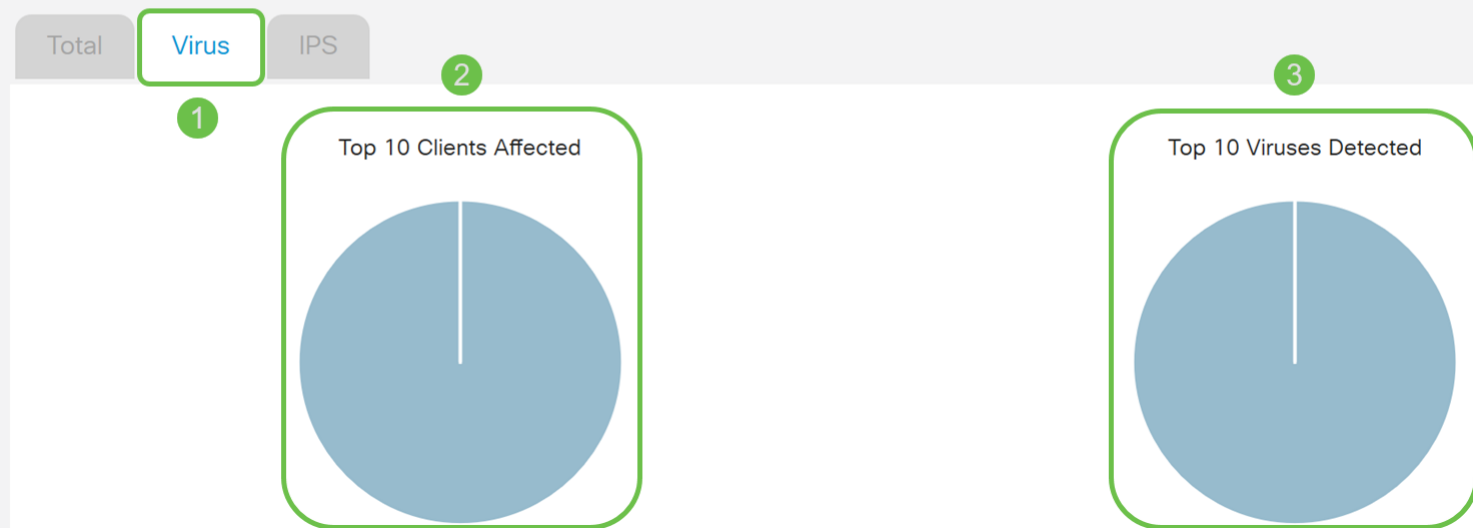
附註：您可以將滑鼠懸停在餅圖上以瞭解詳細資訊。

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 

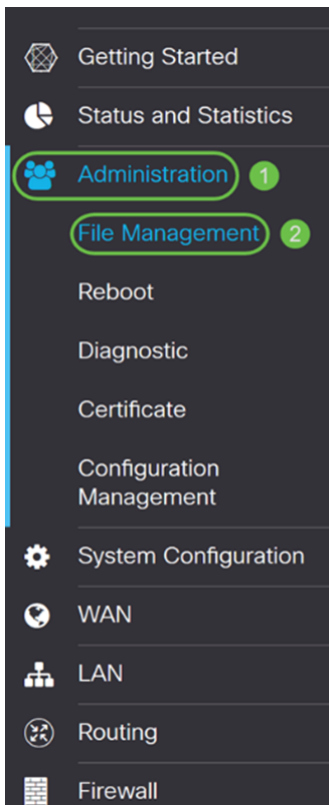


更新防病毒定義

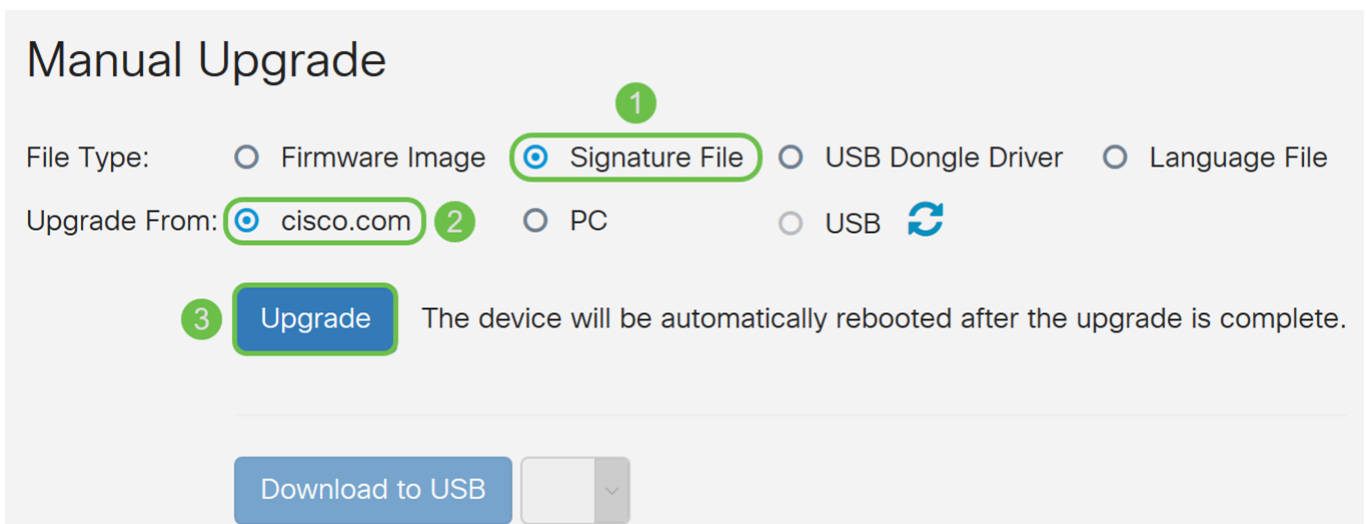
您可以手動或自動更新防病毒資料庫。第1-2步將向您顯示如何手動更新防病毒資料庫，而第3-6步將向您顯示如何自動更新防病毒資料庫。

最佳實踐：建議每週自動更新安全簽名。

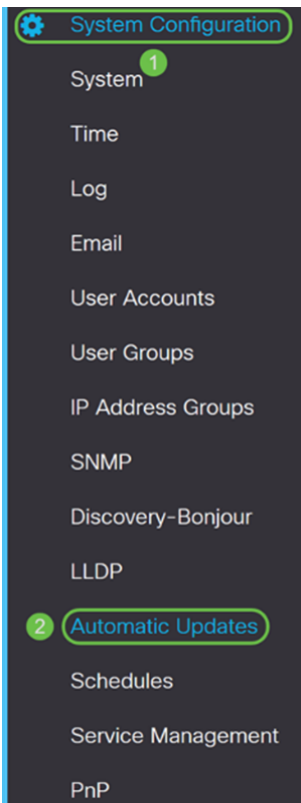
步驟1.要手動更新防病毒資料庫，請導航到**管理>檔案管理**。



步驟2. 向下滾動到 *File Management* 頁面的 *Manual Upgrade* 部分。為 *File Type* 選擇 **Signature File**，為 *Upgrade From* 選擇 **cisco.com**。然後按升級。這將下載並安裝最新的安全簽名。



步驟3. 要自動更新防病毒資料庫，請導航至 **系統配置 > 自動更新**。



步驟4. *Automatic Updates* 頁面隨即開啟。您可以選擇每週或每月檢查更新。您可以通過電子郵件或Web UI通知路由器。在此示例中，我們將選擇每週進行檢查。

附註：建議每週自動更新安全簽名。

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.

步驟5. 向下滾動到 *Automatic Update* 部分，並查詢 *Security Signature* 欄位。在「*Security Signature Update*」下拉選單中，選擇要自動更新的時間。在本例中，我們將選擇 **Immediate**。

	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, ...

步驟6. 按一下 **Apply**，將變更儲存到執行組態檔中。

附註：請記得按一下頂部的 **Floppy Disk** 圖示，導航到 *Configuration Management* 頁面，將運行配置檔案複製到啟動配置檔案。這將有助於在重新啟動後保留您的配置。

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, ...

結論

您現在應該已經在RV34x系列路由器上配置了防病毒軟體。

有關其他資訊，請訪問以下資源。

- 路由器社群：[思科小型企業支援社群](#)
- RV34x系列常見問題：[RV34x系列路由器常見問題](#)