تكوين برنامج AntiVirus على موجه من السلسلة RV34x

الهدف

الهدف من هذا المستند هو توضيح كيفية تكوين برنامج AntiVirus على موجهات سلسلة RV34x.

المقدمة

يحمي برنامج الحماية من الفيروسات مستخدمي الشبكة من حالات العدوى ومحتوى البرامج الضارة الذي يتم إستلامه في رسائل البريد الإلكتروني أو البيانات. تدعم ميزة مكافحة الفيروسات بروتوكولات بروتوكول نقل البريد البسيط (SMTP) وبروتوكول نقل النص التشعبي (HTTP) وبروتوكول نقل الملفات (FTP) وبروتوكول مكتب البريد الإصدار 3 (POP3) وبروتوكول الوصول إلى رسائل الإنترنت (IMAP).

يستخدم محرك الحماية من الفيروسات مكونين مهمين، هما مصنف يعرف أين يبحث، وقاعدة بيانات الفيروسات التي تعرف ما تبحث عنه. يقوم المحرك بتصنيف الملف حسب النوع بدلا من الاعتماد على الملحق. يقوم محرك الفيروسات بالبحث عن الفيروسات الموجودة في أجسام الرسائل التي تم تلقيها بواسطة النظام وملحقاتها، ويساعد نوع ملف المرفق في تحديد مسحها ضوئيا.

لمعرفة ما هي البرامج الضارة، راجع هذا الارتباط: ما هي البرامج الضارة؟.

لمعرفة كيفية تكوين Umbrella، انقر فوق الارتباط: تكوين Cisco Umbrella RV34x.

ملاحظة هامة: إذا كان الموجه يخضع حاليا لحمل عمل كبير، فقد يؤدي ذلك إلى تفاقم المشكلة.

ويتضمن الجدول أدناه إحصاءات متوقعة للأداء في إطار عمليات تهيئة مختلفة. وينبغي إستخدام هذه القيم كدليل، لأن الأداء العالمي الحقيقي قد يختلف بسبب عدد من العوامل.

	الاتصالات المتزامنة	معدل الاتصال	سعة معالجة HTTP	سعة معالجة FTP
الإعدادات الافتراضية	40000	3000	982 ميجابايت/ثانية	981 ميجابايت/ثانية
تمكين التحكم في التطبيق	15000-16000	1300	982 ميجابايت/ثانية	981 ميجابايت/ثانية
تمكين مكافحة الفيروسات	**16000**	**1500**	**982 ميجابايت/ثانية**	**981 ميجابايت/ثانية**
تمكين IPS	17000	1300	982 ميجابايت/ثانية	981 ميجابايت/ثانية
تمكين مكافحة الفيروسات و IPS للتحكم في التطبيقات	15000-16000	1000	982 ميجابايت/ثانية	981 ميجابايت/ثانية

يتم تعريف الحقول التالية على أنها:

الاتصالات المتزامنة - إجمالي عدد الاتصالات المتزامنة، على سبيل المثال، إذا كنت تقوم بتنزيل ملف من موقع واحد، فهذا اتصال واحد، يتم الآن دفق الصوت من Spotify ويكون اتصالا آخر، مما يجعله إتصالين متزامنين.

معدل الاتصال - عدد طلبات الاتصال في الثانية التي يمكن لهذا الاتصال معالجتها.

سعة معالجة HTTP/FTP - تعد سعة معالجة HTTP و FTP معدلات التنزيل بالميغابايت/الثانية.

تم تحديث تراخيص الأمان لتضمين برنامج الحماية من الفيروسات بالإضافة إلى التطبيق الحالي وتصفية الويب. يلزم وجود حساب ذكي للحصول على ترخيص أمان. إذا لم يكن لديك بالفعل حساب ذكي نشط، فسيلزم القسم 1 من هذا المستند.

لمعرفة كيفية تكوين نظام منع التسلل على RV34x، انقر هنا.

الأجهزة القابلة للتطبيق

- الطراز RV34x

إصدار البرامج

- 1.0.03.5

جدول المحتويات

1. بنية الترخيص
2. تكوين برنامج مكافحة الفيروسات
3. حالة التهديدات/IPS
4. تحديث تعريفات مكافحة الفيروسات
5. القرار

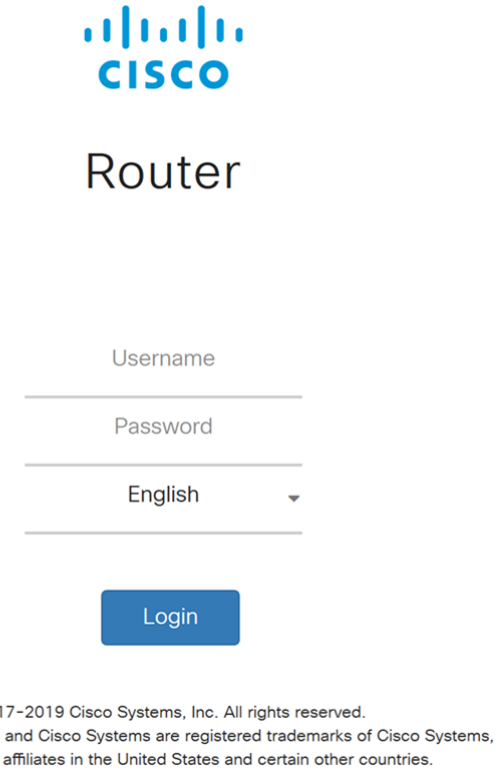
بنية الترخيص - إصدارات البرنامج الثابت 1.0.3.15 والإصدارات الأحدث

عند الانتقال إلى الأمام، سيتحمل AnyConnect رسوما لتراخيص العملاء فقط.

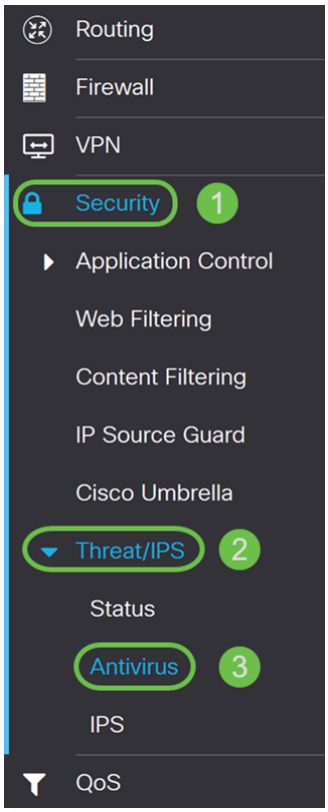
للحصول على معلومات إضافية حول ترخيص AnyConnect على موجهات سلسلة RV340، يرجى الاطلاع على المقالة المتعلقة بترخيص AnyConnect لموجهات سلسلة RV340.

تكوين برنامج مكافحة الفيروسات

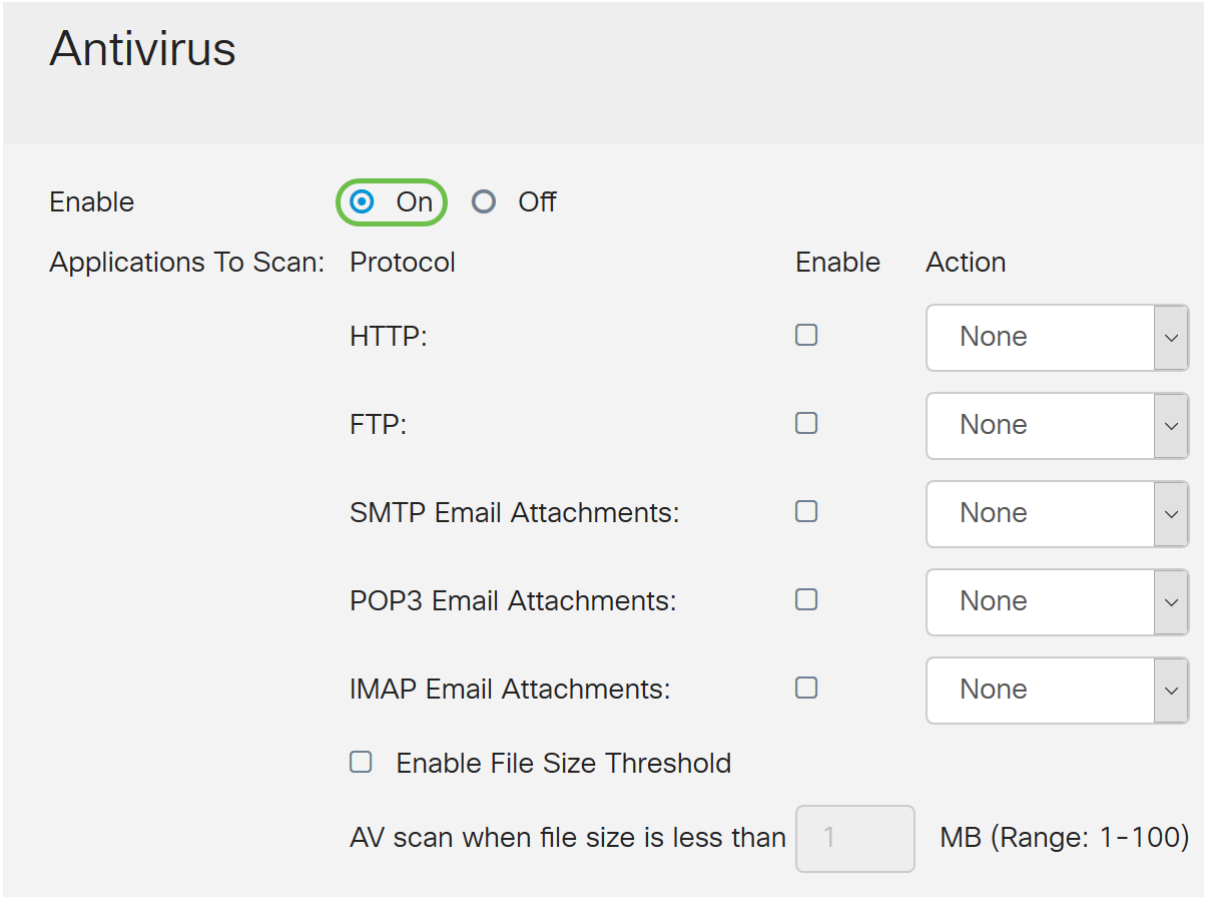
الخطوة 1. إذا لم تكن قد قمت بتسجيل الدخول إلى الموجه، فسجل الدخول إلى صفحة تكوين الويب.



الخطوة 2. انتقل إلى **الأمان > التهديد/IPS > مكافحة الفيروسات**.



الخطوة 3. انقر فوق الزر **تشغيل** الراديو لتمكين ميزة مكافحة الفيروسات.

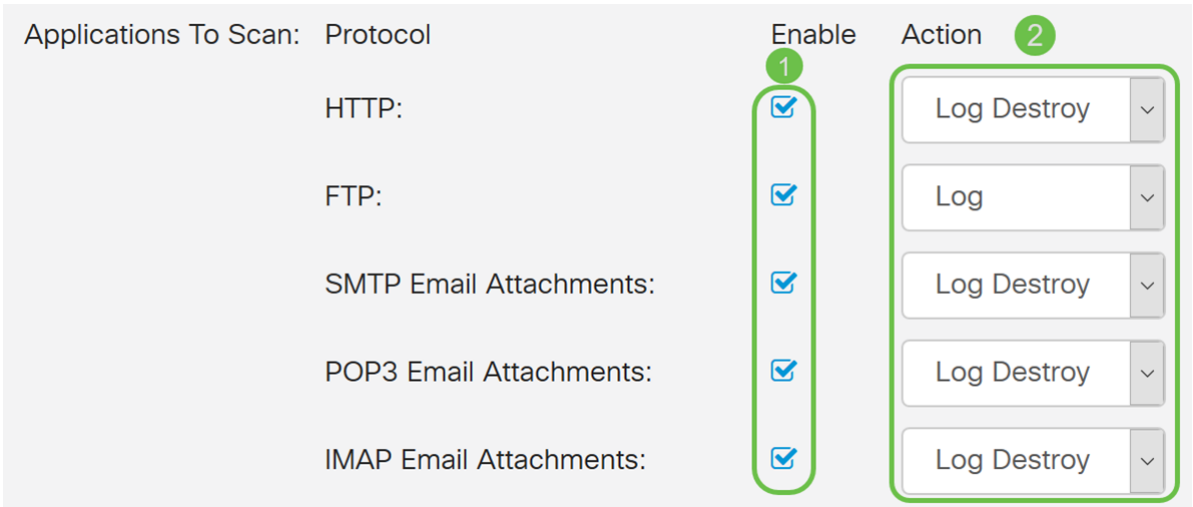


الخطوة 4. حدد خانة (خانات) **تمكين** لتمكين *التطبيقات من المسح الضوئي* على البروتوكولات. في هذا المثال، قمنا بتمكين جميع البروتوكولات (**HTTP و FTP و SMTP و POP3** و**IMAP**). ثم حدد الإجراء المناسب له. يتم تعريف الخيارات التالية على أنها:

- **السجل** - حدد هذا الخيار لإنشاء السجل فقط (باستخدام معلومات العميل ومعرف التوقيع، وما إلى ذلك) عند تعريف التهديدات. لا يؤثر على الاتصال.

- **تدمير السجل** - حدد هذا الخيار لإسقاط الاتصال عند تحديد التهديدات وتسجيل الرسالة للحذف.

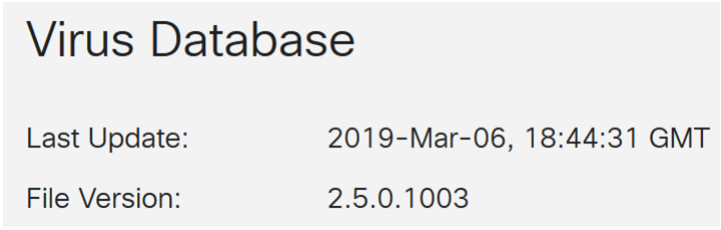
ملاحظة: في حالة وجود تهديد محدد في مرفق، سيتم اقتطاع الملف أثناء عملية التنزيل.



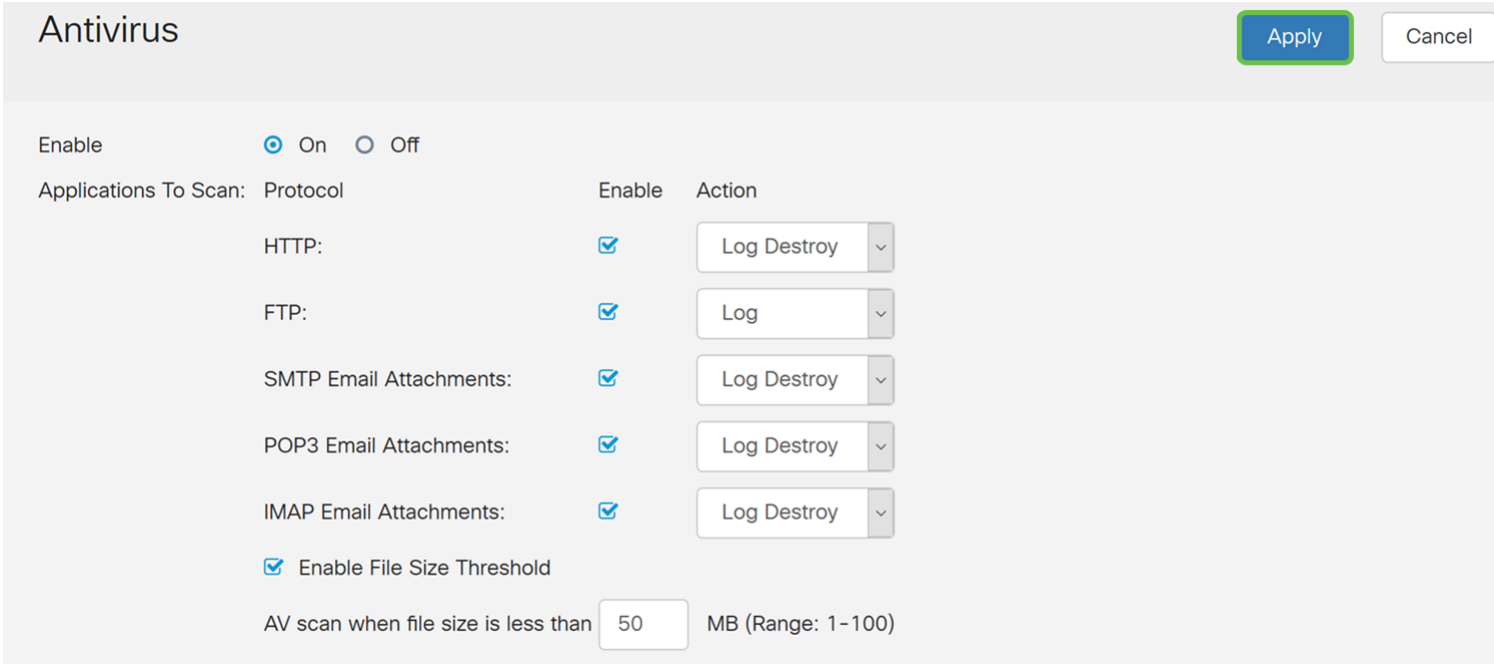
الخطوة 5. إذا كنت تريد أن يحتوي برنامج الحماية من الفيروسات على حجم ملف مطلوب للمسح الضوئي، فتحقق من **عتبة تمكين حجم الملف**. ثم قم بإدخال حجم الملف الذي يمكن أن يقوم برنامج مكافحة الفيروسات بمسحه. المدى 1-100 from ميغابايت.

في هذا المثال، تم إدخال **50** ميجابايت.

الخطوة 6. في قسم *قاعدة بيانات الفيروسات*، يظهر *التحديث الأخير* تاريخ ووقت آخر توقيع تم تحديثه. يعرض *إصدار الملف* إصدار التوقيع الذي يتم إستخدامه.

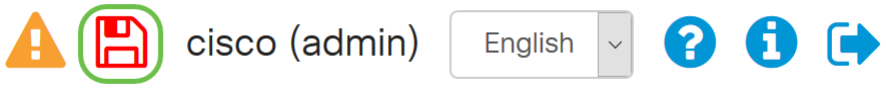


الخطوة 7. انقر فوق الزر **تطبيق** لحفظ التغييرات.

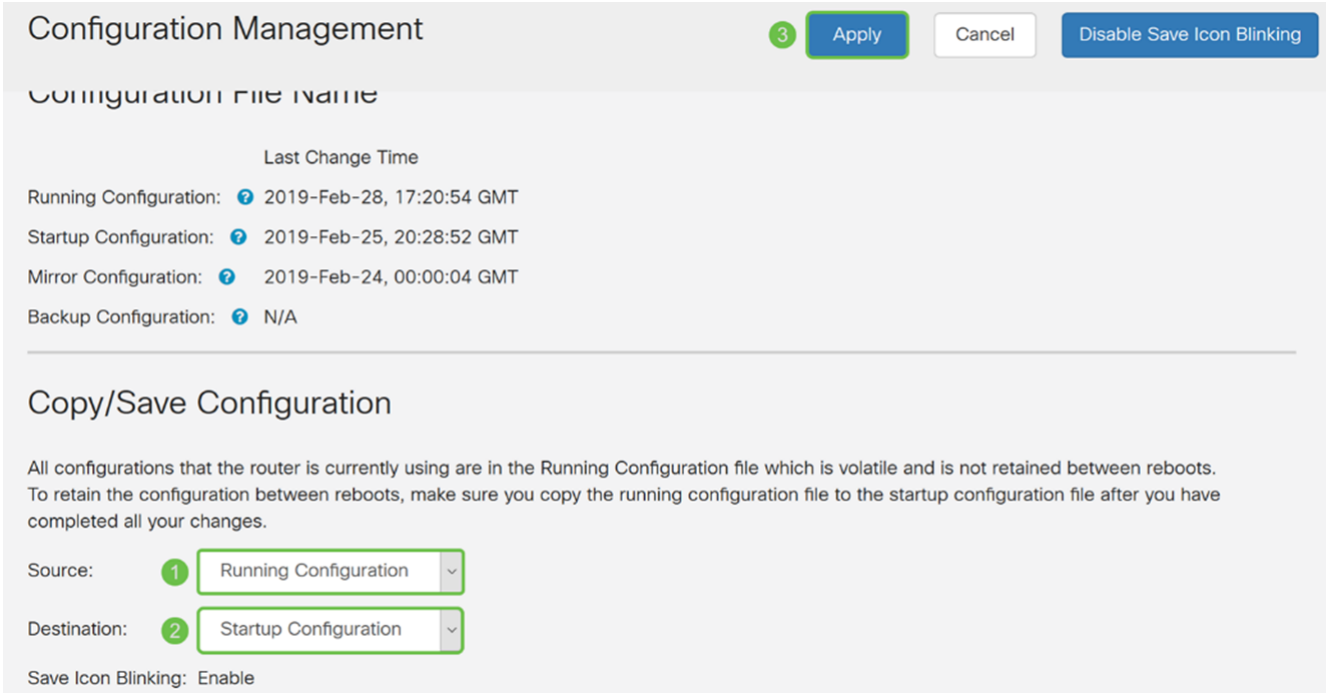


يؤدي الضغط على **تطبيق** فقط إلى حفظ التكوين الخاص بك في التكوين الجاري تشغيله. ستحتاج إلى نسخ التكوين الجاري تشغيله إلى تكوين بدء التشغيل إذا كنت ترغب في الاحتفاظ بالتكوين الخاص بك بين عمليات إعادة التشغيل.

الخطوة 8. انقر أيقونة **القرص المرن (حفظ)** في أعلى الصفحة. وهذا سيقوم بإعادة توجيهك إلى *إدارة التكوين* لنسخ التكوين الجاري تشغيله إلى تكوين بدء التشغيل.

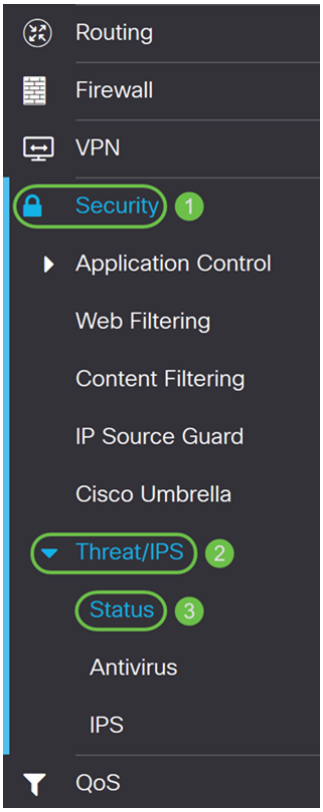


الخطوة 9. في *إدارة التكوين*، قم بالتمرير إلى قسم *نسخ/حفظ التكوين*. تأكد من أن *المصدر* يشغل التكوين *والوجهة* هي **بدء التشغيل**. طقطقة **يطبق**. سيؤدي هذا إلى نسخ ملف التكوين الجاري تشغيله إلى ملف تكوين بدء التشغيل للاحتفاظ بالتكوين بين عمليات إعادة التمهيد.

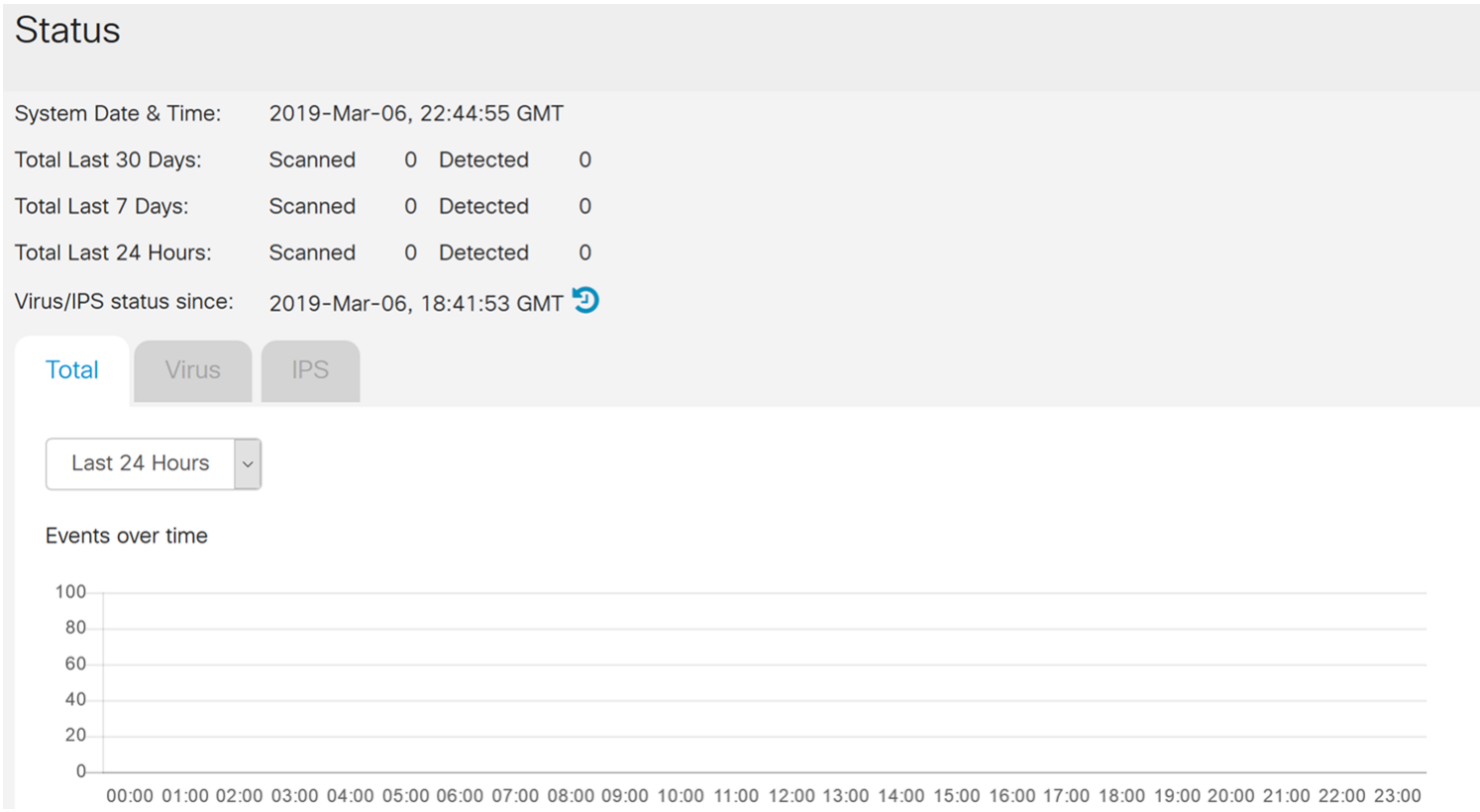


حالة التهديد/IPS

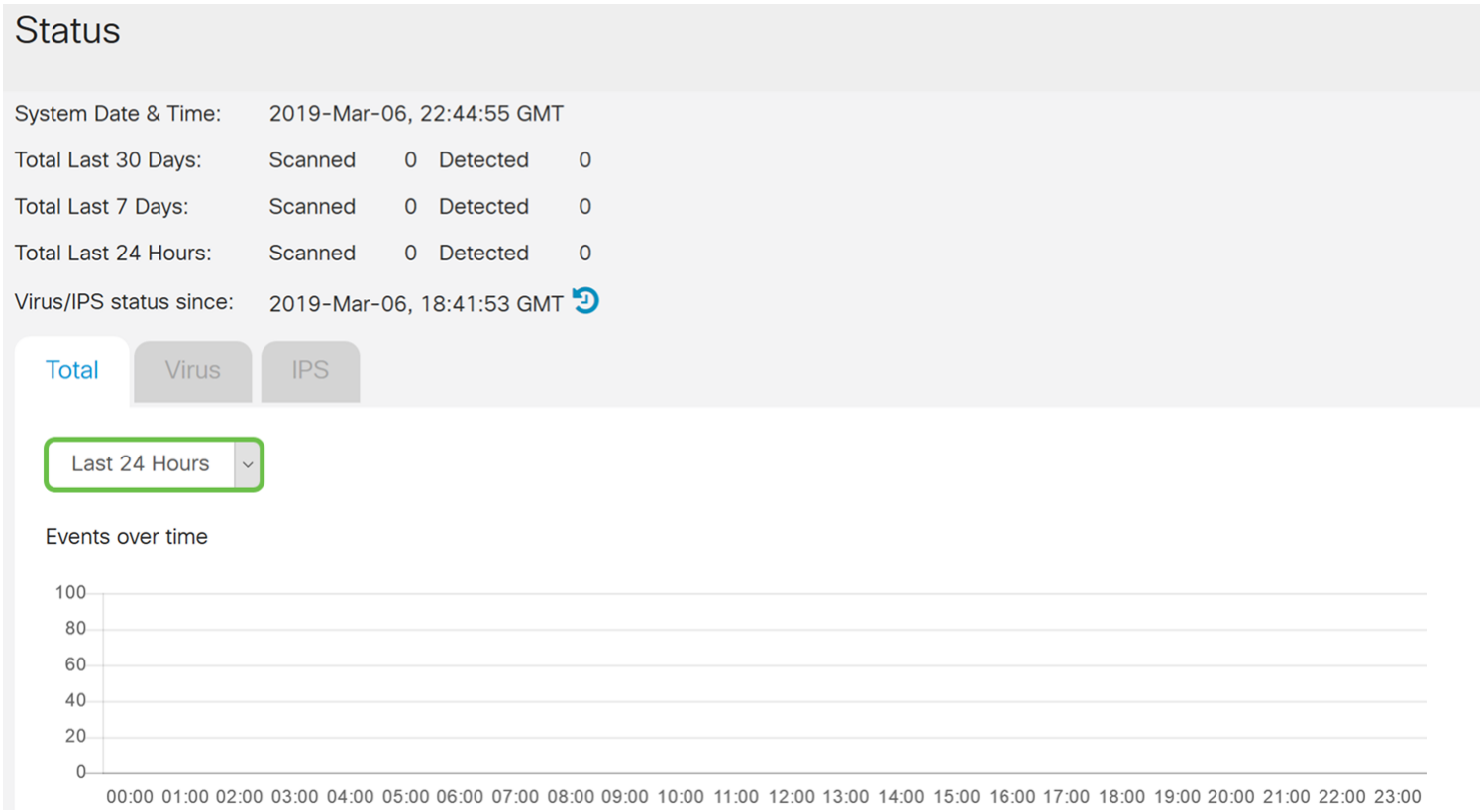
الخطوة 1. انتقل إلى **الأمان > التهديد/IPS > الحالة**.



الخطوة 2. في صفحة *الحالة*، يمكنك رؤية تاريخ ووقت النظام، والتهديدات التي تم مسحها ضوئيا أو كشفها، والهجمات من علامة التبويب المحددة. بشكل افتراضي، يمكنك أن ترى حالة علامة التبويب "إجمالي".



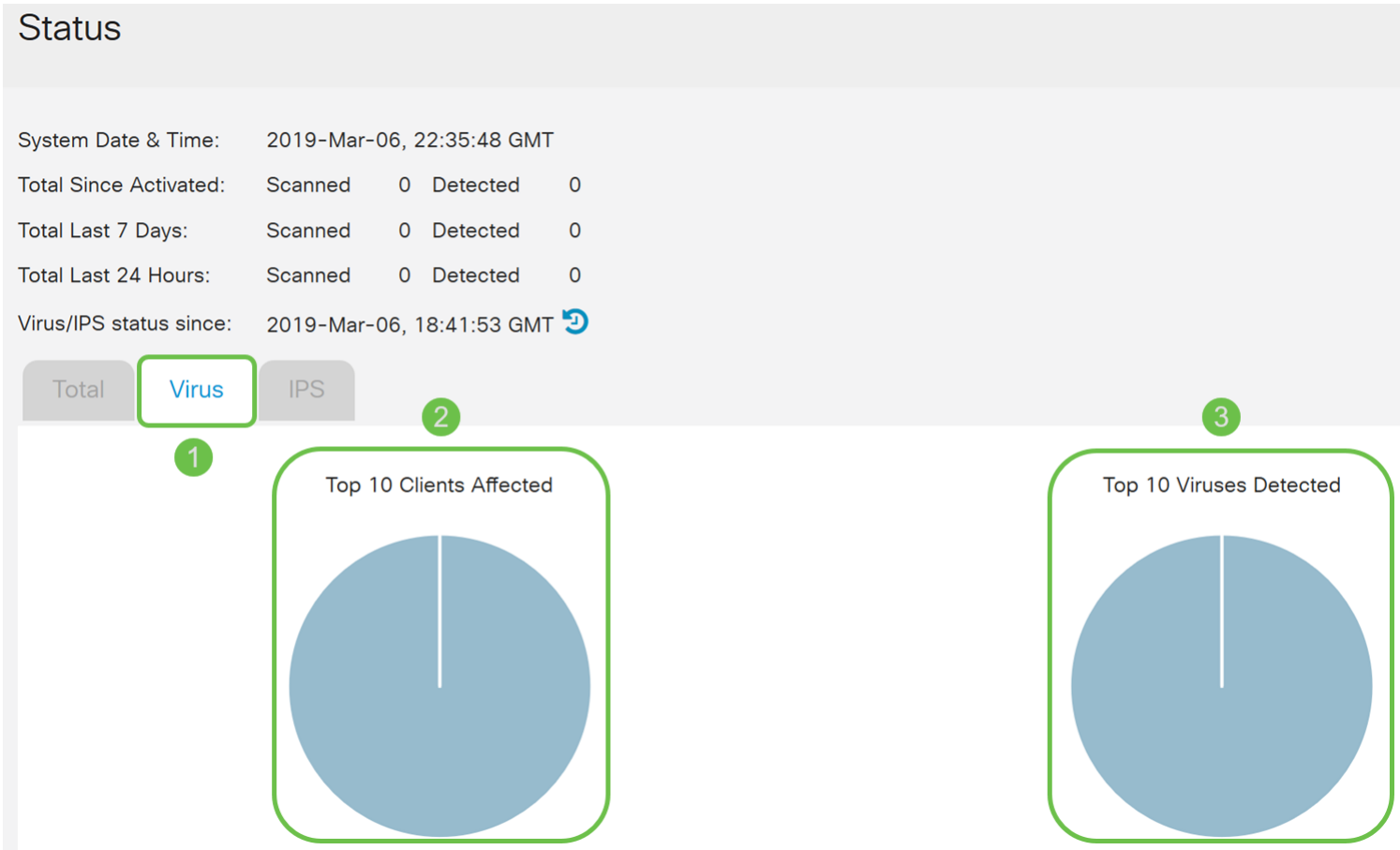
الخطوة 3. في القائمة المنسدلة تحت علامة التبويب *إجمالي* ، يمكنك تحديد **آخر 24 ساعة** أو **أسبوع** أو **شهر** لعرض الأحداث.



الخطوة 4. انقر فوق علامة التبويب **فيروس**. في علامة التبويب *فيروس*، سيعرض ما يلي:

- **أفضل 10 عملاء متأثرين** - قائمة عناوين MAC المتضررين.
- **أكثر 10 فيروسات تم اكتشافها** - قائمة التهديدات التي تم الكشف عنها.

ملاحظة: يمكنك تمرير الماوس عبر المخطط الدائري للحصول على مزيد من التفاصيل.

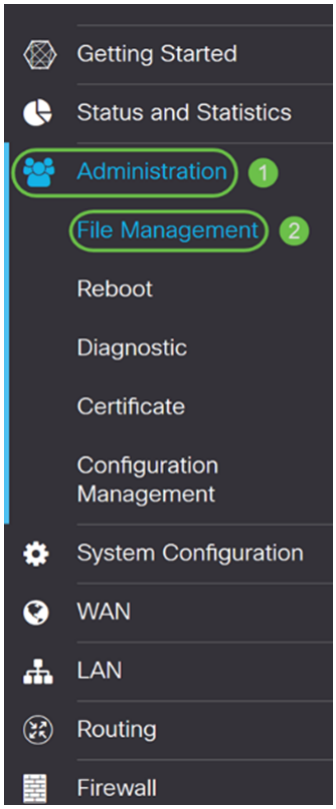


تحديث تعريفات مكافحة الفيروسات

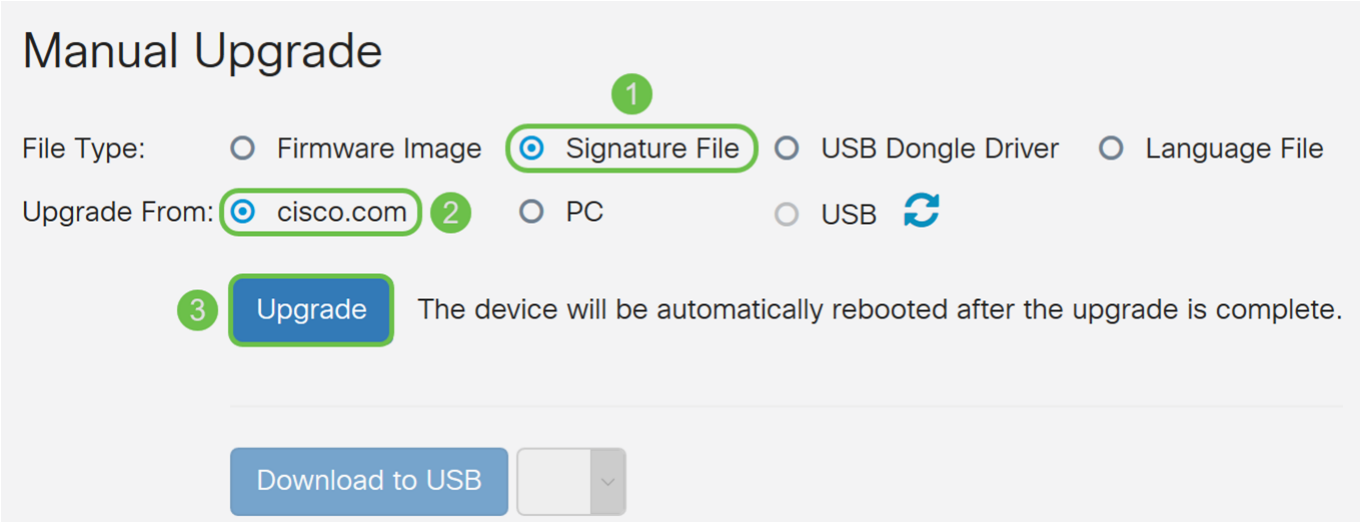
يمكنك تحديث قاعدة بيانات الحماية من الفيروسات يدويا أو تلقائيا. تظهر لك الخطوات من 1 إلى 2 كيفية تحديث قاعدة بيانات الحماية من الفيروسات يدويا بينما تظهر لك الخطوات من 3 إلى 6 كيفية تحديث قاعدة بيانات الحماية من الفيروسات تلقائيا.

أفضل ممارسة: يوصى بتحديث توقيعات الأمان تلقائيا على أساس أسبوعي.

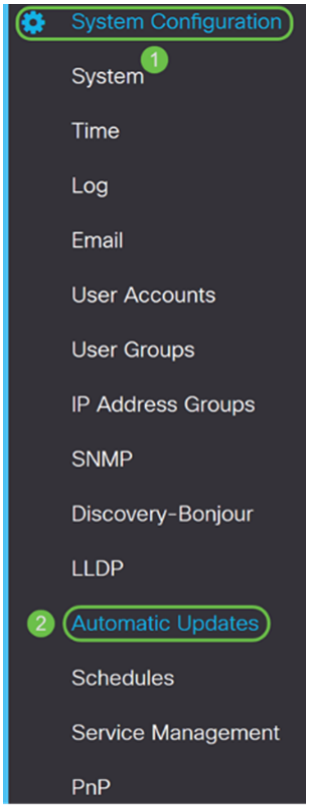
الخطوة 1. لتحديث قاعدة بيانات مكافحة الفيروسات يدويا، انتقل إلى **إدارة > إدارة الملفات**.



الخطوة 2. قم بالتمرير لأسفل إلى قسم *الترقية اليدوية* في صفحة *إدارة الملفات*. أختر **ملف توقيع** ل *نوع الملف* و**Cisco.com** ل *الترقية من*. ثم اضغط على **ترقية**. سيقوم هذا بتنزيل أحدث توقيع أمان وتثبيته.

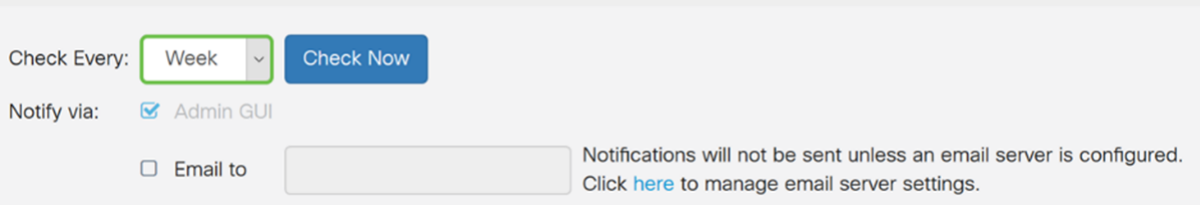


الخطوة 3. لتحديث قاعدة بيانات مكافحة الفيروسات تلقائيا، انتقل إلى **تكوين النظام > تحديثات تلقائية**.

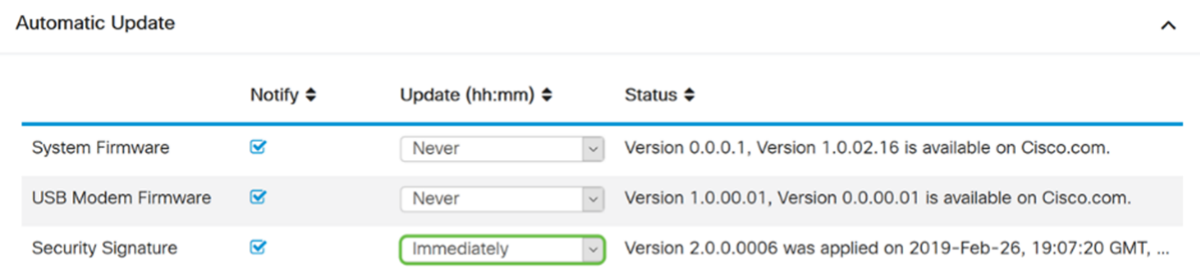


الخطوة 4. يتم فتح صفحة *التحديثات التلقائية*. لديك خيار التحقق من وجود تحديثات إما بشكل أسبوعي أو شهري. يمكنك أن تقوم بإخطار الموجه عبر البريد الإلكتروني أو واجهة مستخدم ويب. في هذا المثال، سنختار التحقق كل أسبوع.

ملاحظة: يوصى بتحديث توقيعات التأمين تلقائيا على أساس أسبوعي.

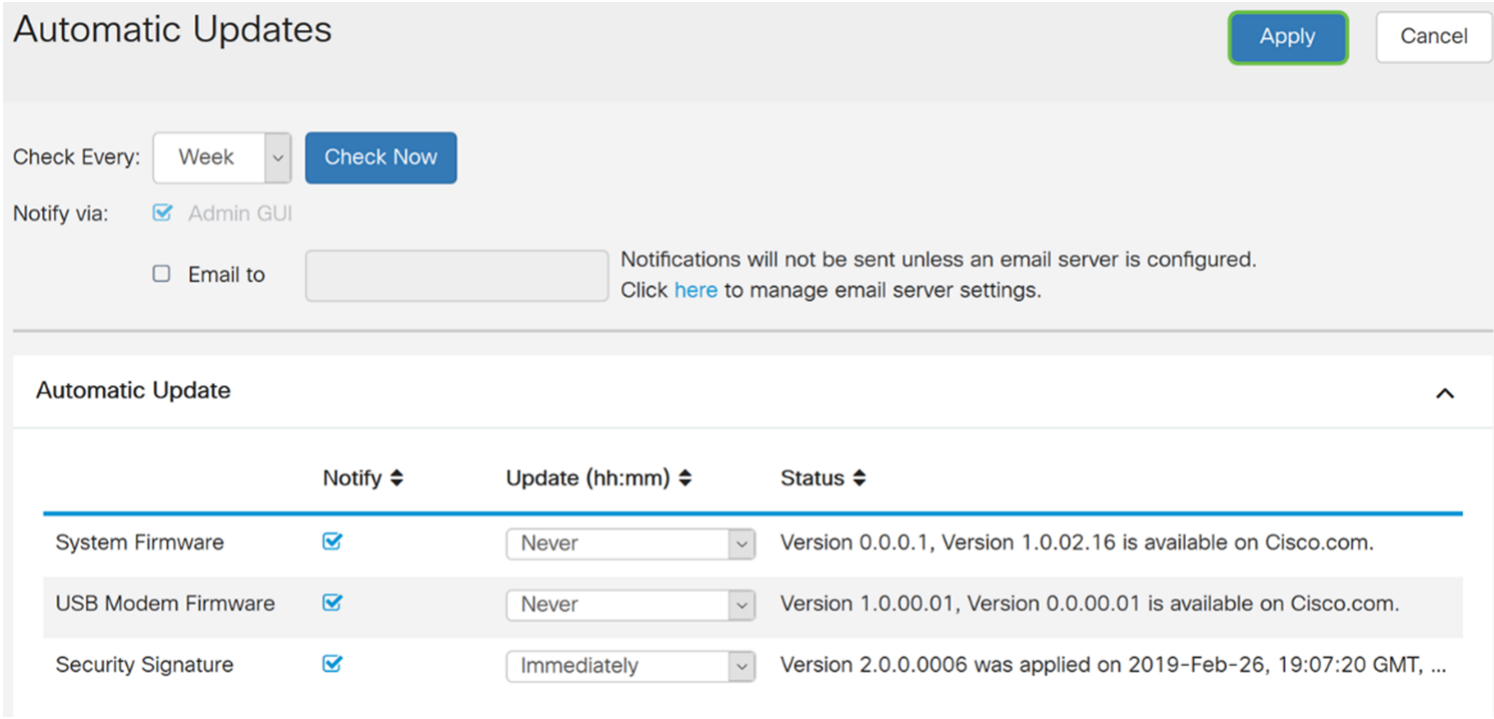


الخطوة 5. قم بالتمرير إلى قسم *التحديث التلقائي* وابحث عن حقل *توقيع الأمان*. في القائمة المنسدلة *تحديث توقيع الأمان*، حدد الوقت الذي تريد تحديثه تلقائيا. في هذا المثال، سنختار **فورا**.



الخطوة 6. انقر فوق **تطبيق** لحفظ التغييرات في ملف التكوين الجاري تشغيله.

ملاحظة: تذكر النقر فوق رمز **القرص المرن** الموجود بالأعلى للتنقل إلى صفحة *إدارة التكوين* لنسخ ملف التكوين الجاري تشغيله إلى ملف تكوين بدء التشغيل. سيساعد ذلك في الاحتفاظ بالتكوينات الخاصة بك بين عمليات إعادة التمهيد.



القرار

يجب أن تكون قد انتهيت الآن من تكوين برنامج AntiVirus على موجه من السلسلة RV34x لديك.

للحصول على معلومات إضافية، راجع الموارد التالية.

- **مجتمع الموجه:** مجتمع دعم الأعمال الصغيرة من Cisco
- **أسئلة متداولة حول السلسلة RV34x:** الأسئلة المتداولة حول الموجه RV34x Series

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).