تكوين نظام منع الاقتحام على موجه من السلسلة RV34x

الهدف

الهدف من هذا المستند هو توضيح كيفية تكوين نظام منع التسلل (IPS) على موجهات من السلسلة RV34x.

المقدمة

يقوم "نظام منع التسلل" بفحص حركة المرور للبحث عن أنماط الهجمات المعروفة التي يتم منعها. يراقب هو ربط وجلسات بينما هم يتدفق من خلال المسحاج تخديد ويمسح كل ربط أن تلاءم any of the cisco ips توقيع. وعندما يكتشف أي نشاط مريب، فإنه مصمم لتسجيل أو منع حدوثه. من المهم تحديث قواعد بيانات وتعريفات IPS ومكافحة الفيروسات. يمكن تحديث هذه الملفات يدويا أو تلقائيا.

اطلع على مقاطع الفيديو هذه على نظام Cisco لمنع الاقتحام:

ومع ذلك، يمكن أن يؤثر بروتوكول IPS على أداء الموجه. بشكل عام، لا يؤثر هذا على سعة المعالجة الإجمالية لحركة مرور بروتوكول نقل النص التشعبي (HTTP) وبروتوكول نقل الملفات (FTP)، ولكن يمكنه إسقاط الحد الأقصى لعدد الاتصالات المتزامنة بشكل كبير إلى حد ما.

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، سيتم دفق الصوت من Spotify وسيكون اتصال آخر، مما يجعله إتصالين متزامنين.

معدل الاتصال - عدد طلبات الاتصالات/الثانية التي يمكن معالجتها.

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

تم تحديث تراخيص الأمان لتضمين حماية نظام منع الاختراقات (IPS) 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 برنامج AntiVirus على RV34x، انقر هنا.

الأجهزة القابلة للتطبيق

- RV34x

إصدار البرامج

- x.1.0.03

جدول المحتويات

الترخيص الذكي

إذا لم يكن لديك حساب ذكي نشط، فستحتاج إلى متابعة الخطوات أدناه.

إذا صادفتك أية مشكلات أو مشكلات أثناء تكوين حساب "الترخيص الذكي"، فسيقوم فريق الدعم التابع لنا بالمساعدة في حل المشكلات المحتملة ويمكن الوصول إليها من خلال طرق متعددة. لا تتردد في إستخدام طريقتك المفضلة للوصول إلى الآخرين.

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

- **نظرة عامة على الترخيص Smart:** ترخيص البرامج الذكية

- **الأسئلة المتداولة حول التراخيص الذكية:** الأسئلة المتداولة حول الترخيص الذكي والحسابات الذكية للشركاء والموزعين والعملاء

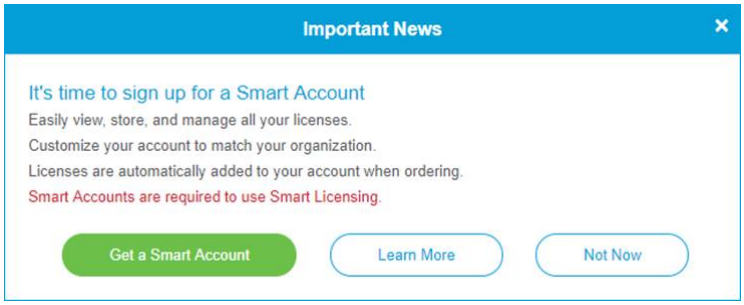
- **إرسال حالة:** Support Case Manager (مدير حالة الدعم)

- **رقم هاتف الدعم الخاص بالولايات المتحدة/كندا:** جهات اتصال TAC للأنشطة التجارية الصغيرة 1-866-606-1866

- **البريد الإلكتروني للترخيص:** licensing@cisco.com

الخطوة 1. إذا كنت قد قمت بإنشاء حساب Cisco.com الخاص بك أو قمت بزيارته مؤخرا، فسيتم الترحيب بك برسالة لإنشاء حساب الترخيص الذكي الخاص بك. إذا لم تقم بذلك، يمكنك النقر هنا لاخذك إلى صفحة إنشاء حساب الترخيص الذكي. قد تحتاج إلى تسجيل الدخول.

ملاحظة: للحصول على تفاصيل إضافية حول الخطوات المتعلقة بطلب حسابك الذكي، انقر هنا.



الخطوة 2. عند شراء ترخيص ذكي لمسحاج تخديد، يحتاج المورد إلى إجراء عملية ينقل معرف الترخيص الفريد إلى حساب الترخيص الذكي الخاص بك. في ما يلي جدول بالمعلومات الضرورية التي سيطلب منها عند شراء الحزم.

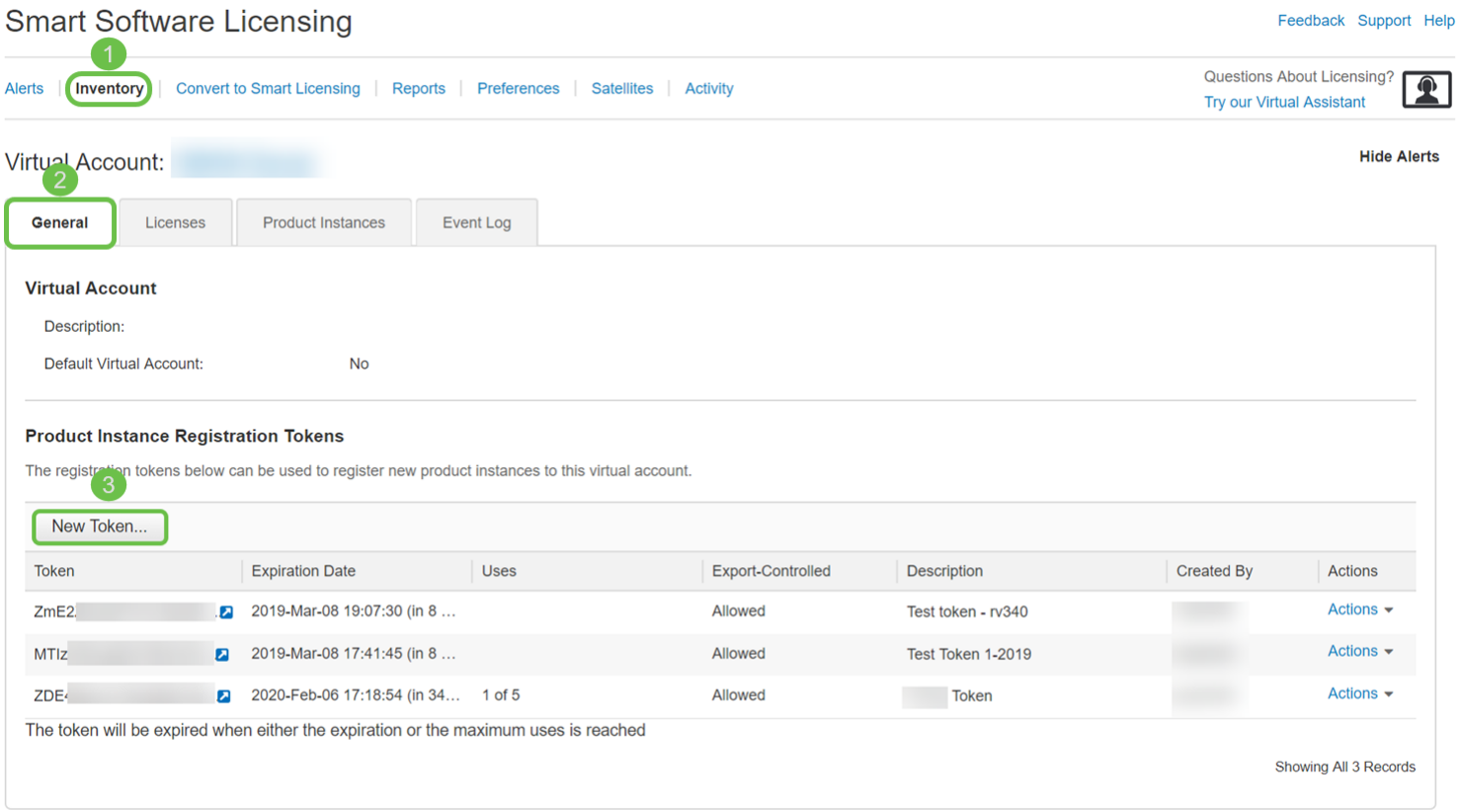
ملاحظة: يعد كل من IPS و AntiVirus جزءا من ترخيص الأمان المستخدم لتصفية الويب وتصفية التطبيقات.

المعلومات المطلوبة	تحديد موقع المعلومات
معرف Cisco.com المستخدم	موجود في ملف تعريف حسابك، أو يمكنك النقر هنا.
اسم حساب الترخيص الذكي	من الأفضل إنشاء حسابك الذكي قبل شراء الترخيص. يجب أن تكون هذه الخطوة 8 من مقال إنشاء حساب الترخيص الذكي".
وحدة الاحتفاظ بالمخزون (SKU) للترخيص الذكي	كود تعريف المنتج للجهاز. مثال. RV340-K9-NA

ملاحظة: إذا كنت قد اشتريت ترخيصا ولم يظهر في حسابك الظاهري، فعليك إما المتابعة مع بائع التجزئة لطلب التحويل أو التواصل معنا.

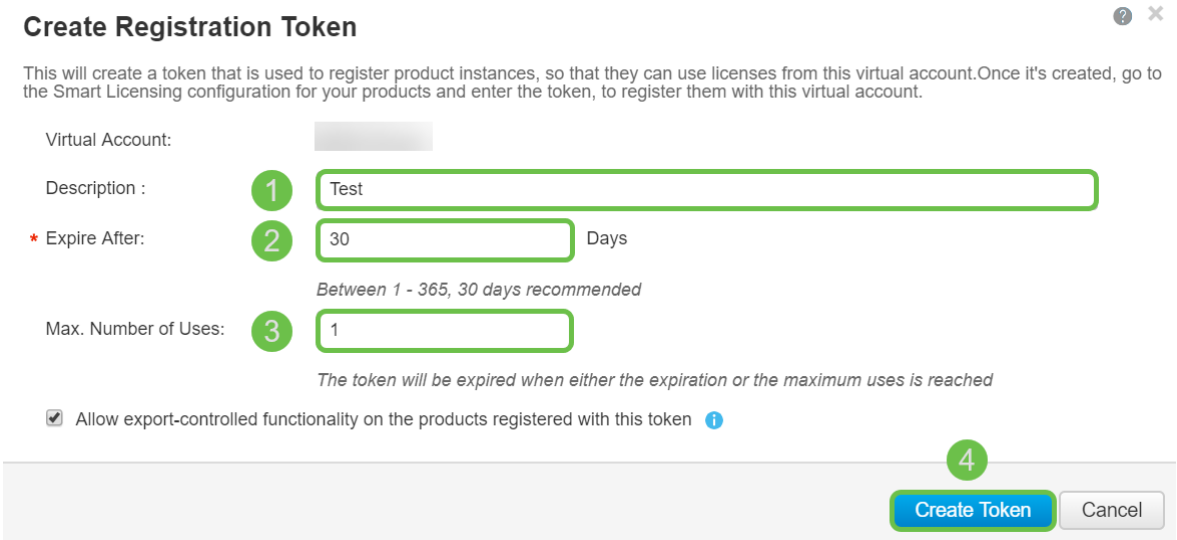
لجعل العملية مناسبة قدر الإمكان، يجب أن يكون لديك فاتورة الترخيص ورقم أمر المبيعات من Cisco ولقطة شاشة لصفحة ترخيص الحساب الذكي (للمشاركة مع فريقنا).

الخطوة 3. لإنشاء رمز مميز، انتقل إلى حساب ترخيص برنامج Smart الخاص بك. ثم انقر فوق **المخزون > علامة التبويب العامة**. انقر فوق الزر **رمز مميز جديد...**

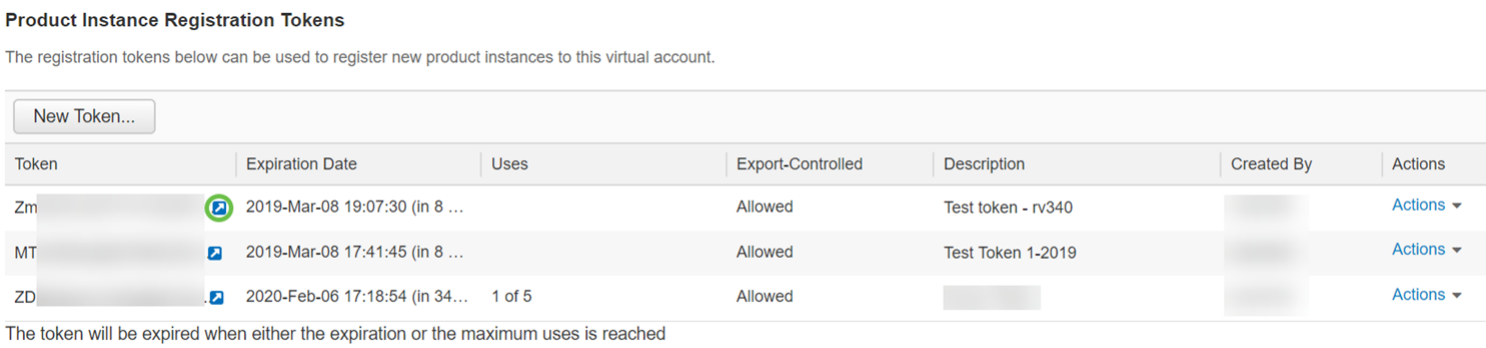


الخطوة 4. يتم فتح نافذة *إنشاء رمز تسجيل مميز*. أدخل *الوصف*، *وتنتهي الصلاحية بعد*، *والحد الأقصى. عدد الاستخدامات*. ثم اضغط على الزر **إنشاء رمز مميز**.

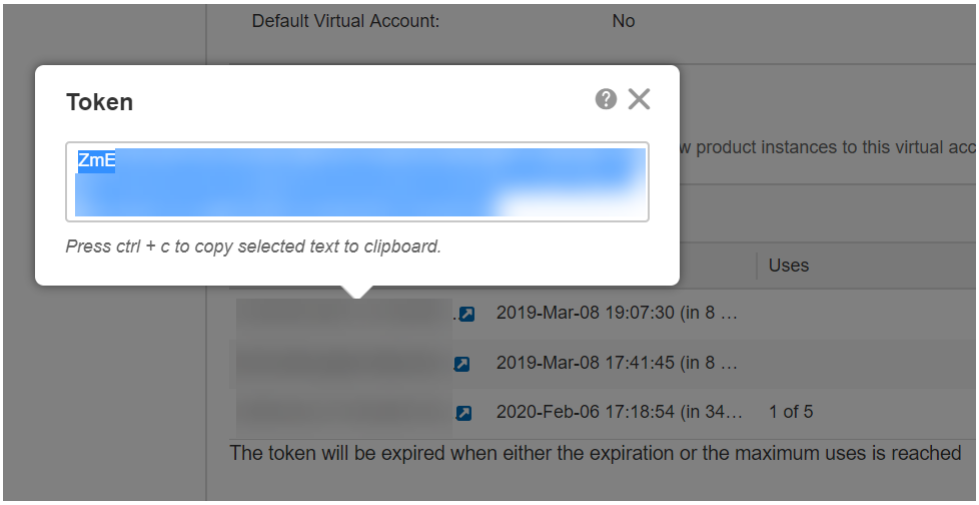
ملاحظة: 30 يوما *لانتهاء الصلاحية بعد* التوصية بها.



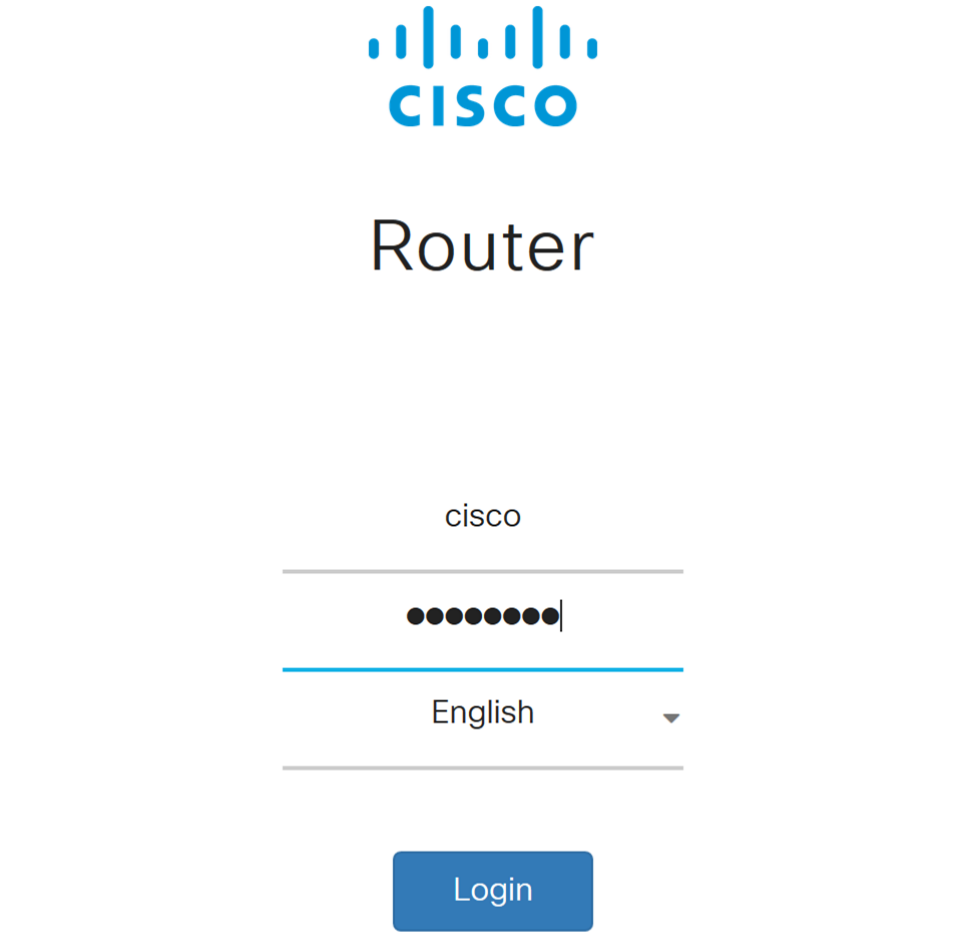
الخطوة 5. بمجرد إنشاء الرمز المميز، يمكنك النقر فوق **إرتباط الرمز المميز (مربع أزرق بسهم أبيض)** زر الموجود على يمين الرمز المميز الذي تم إنشاؤه مؤخرا.



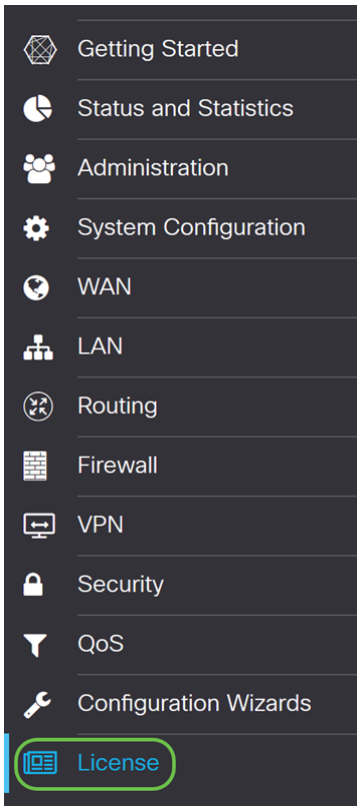
الخطوة 6. يجب أن تظهر نافذة *الرمز المميز* مع الرمز المميز الكامل للنسخ. ركزت الرمز المميز، انقر بزر الماوس الأيمن فوق الرمز المميز وانقر فوق **نسخ** أو يمكنك الضغط مع الاستمرار على زر **ctrl** على لوحة المفاتيح وانقر فوق **C** في نفس الوقت لنسخ النص.



الخطوة 7. بمجرد نسخ الرمز المميز، ستحتاج إلى تسجيل الدخول إلى الجهاز وتحميل مفتاح الرمز المميز. قم بتسجيل الدخول إلى صفحة تكوين الويب للموجه.

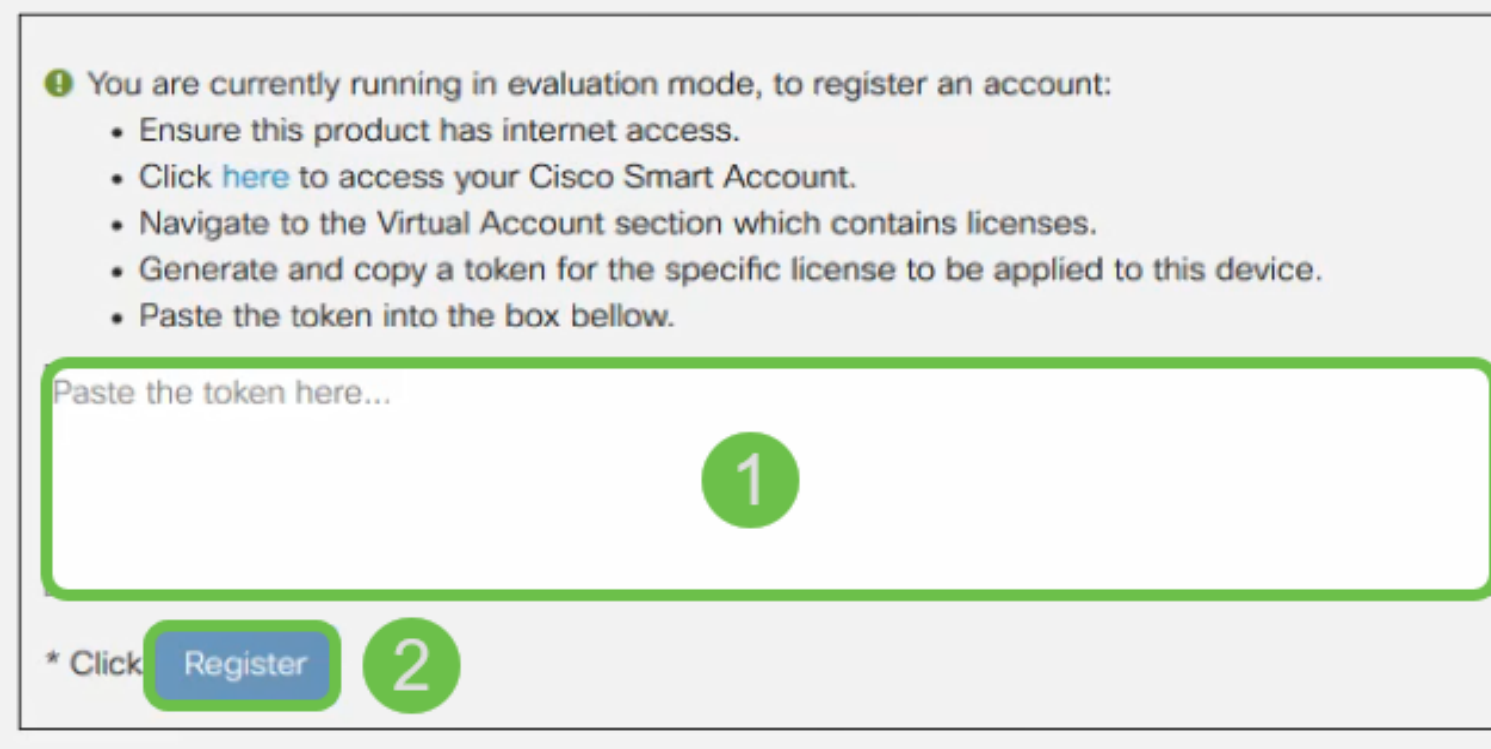


الخطوة 8. انتقل إلى **الترخيص**.

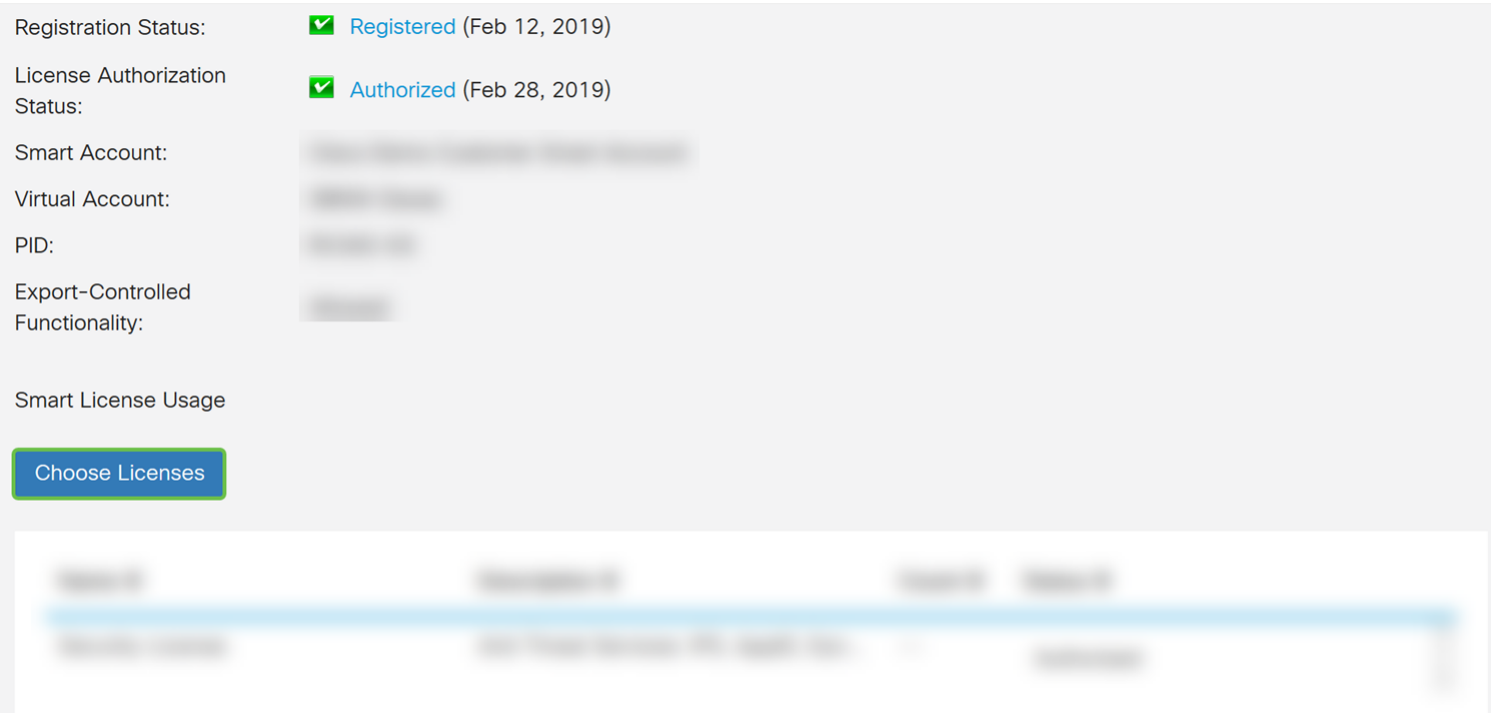


الخطوة 9. إذا كان جهازك غير مسجل، فسيتم إدراج *حالة تخويل الترخيص* الخاصة بك كوضع *تقييم*. الصق الرمز المميز (الخطوة 6 من هذا القسم) الذي قمت بتكوينه من صفحة *مدير الترخيص الذكي*. ثم انقر فوق **تسجيل**.

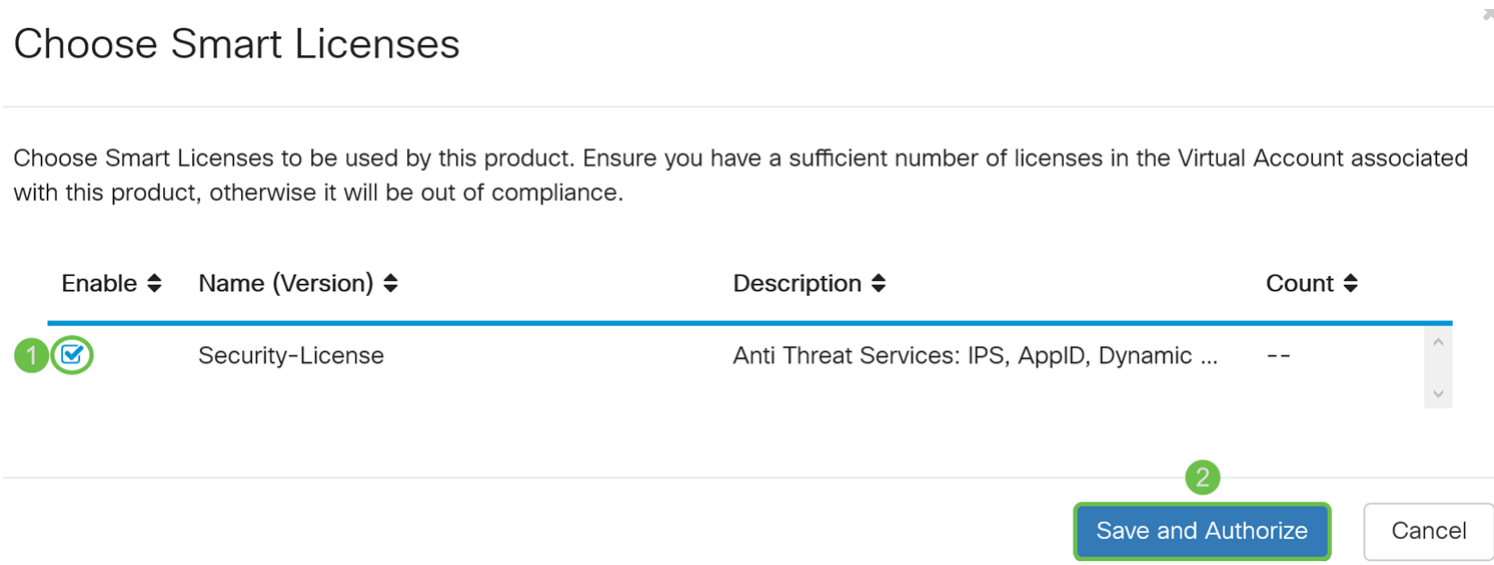
ملاحظة: قد تستغرق عملية التسجيل بعض الوقت، يرجى الانتظار حتى تنتهي.



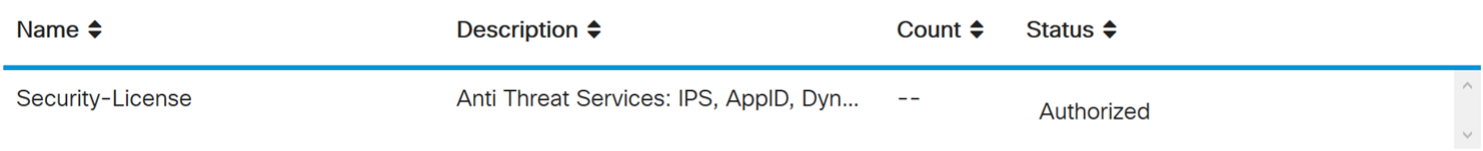
الخطوة 10. بمجرد تسجيل الرمز المميز، ستحتاج إلى تخصيص الترخيص. انقر فوق الزر **إختيار التراخيص**.



الخطوة 11. يجب أن يظهر إطار *إختيار التراخيص الذكية*. تحقق من **ترخيص الأمان** ثم اضغط على **حفظ والتخويل**.



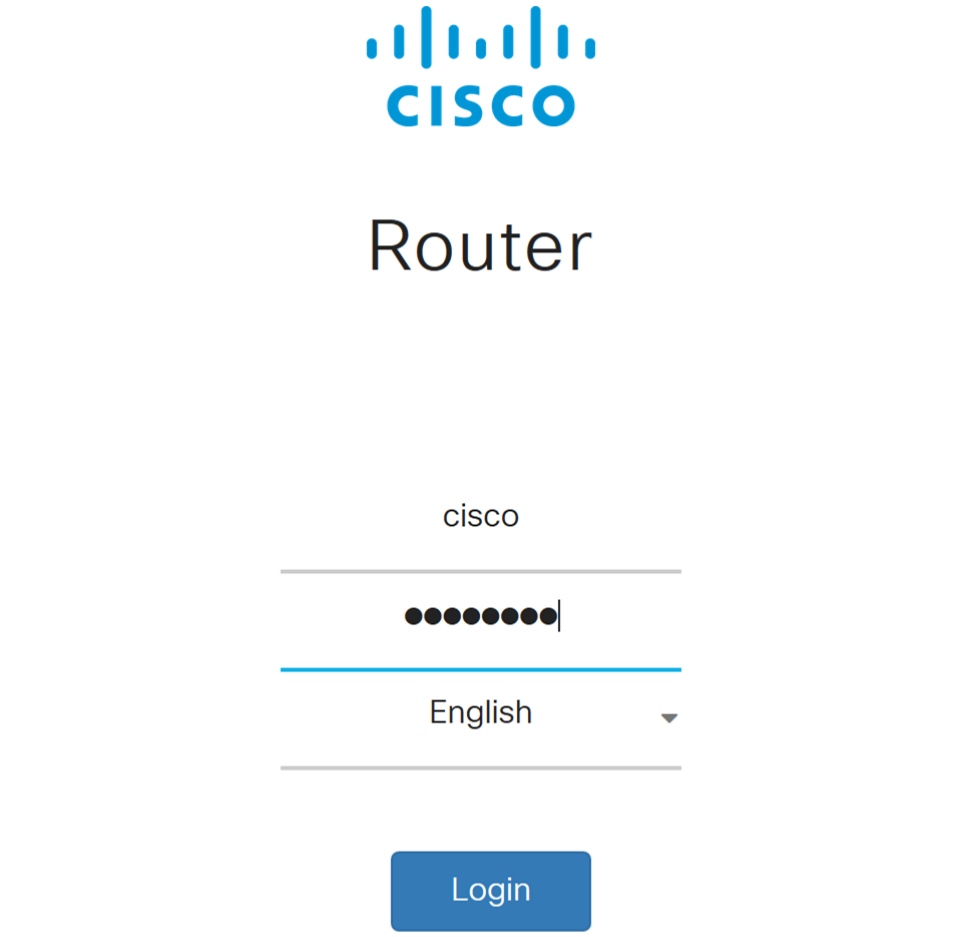
الخطوة 12. يجب اعتماد *حالة* ترخيص الأمان الآن.



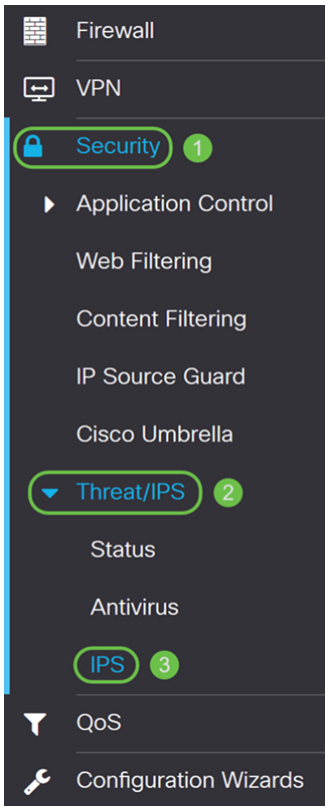
يجب أن تكون الآن قادرا على المضي قدما في تكوين نظام منع الاقتحام.

تهيئة نظام منع الاقتحام

الخطوة 1. إذا لم تسجل دخولك إلى الموجه بعد، فسجل الدخول إلى صفحة تكوين الويب الخاصة بالموجه.

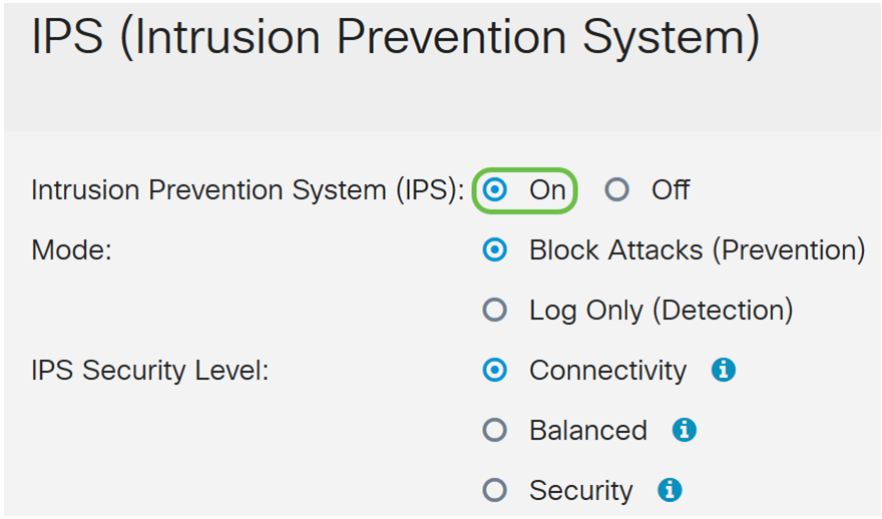


الخطوة 2. انتقل إلى **الأمان > التهديد/IPS > IPS**.



الخطوة 3. حدد **تشغيل** لتمكين ميزة نظام منع التسلل. إذا كنت تريد إيقاف تشغيله، حدد **إيقاف** التشغيل.

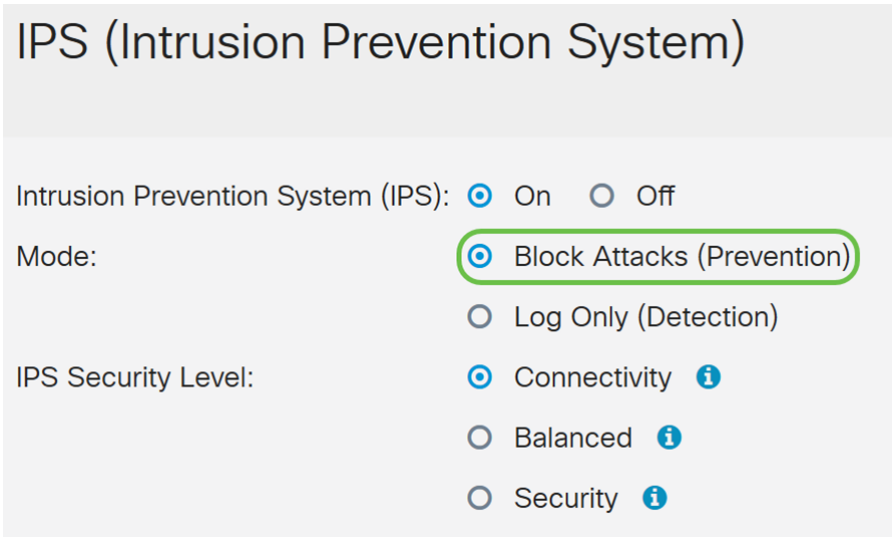
سنقوم باختيار **تشغيل** في هذا المثال.



الخطوة 4. حدد إما **حظر الهجمات (منع)** أو **السجل فقط**. في هذا المثال، سنختار **منع الهجمات (منع)**. يتم تحديد الخيارات التالية أدناه.

- **منع الهجمات (منع)** - حدد لحظر كافة الهجمات. ويسجل أيضا حالة الشذوذ.

- **السجل فقط** - سيقوم هذا الخيار بإنشاء السجل فقط (باستخدام معلومات العميل، ومعرف التوقيع، وما إلى ذلك) عند تحديد الحالات الشاذة. لا يؤثر على الاتصال.



الخطوة 5. حدد مستوى أمان IPS الذي تريد إستخدامه. يتم تعريف الخيارات التالية على أنها:

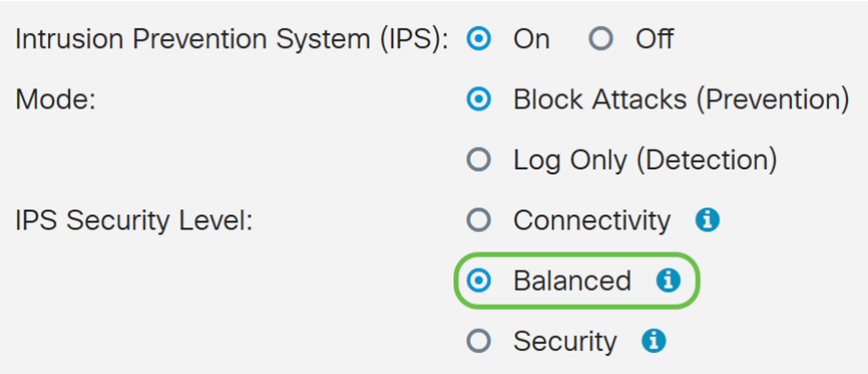
- **الاتصال** - سيقوم هذا الوضع باكتشاف الهجمات الأكثر خطورة. وهذا يوفر أقل قدر من الحماية: يتم اكتشاف هجمات المخاطر (عالية الخطورة) فقط. هذا هو الخيار الأقل أمانا.

- **متوازن** - . وهذا يوفر حماية متوسطة: (عالية + متوسطة الخطورة) يتم فحصها عن طريق تمرير توقيعات منخفضة المخاطر. هذا هو مستوى الأمان المتوسط ل IPS.

- **الأمان** - سيكتشف وضع الأمان الهجمات العادية بالإضافة إلى الهجمات الشديدة والخطيرة. يوفر ذلك أقصى حماية: يتم فحص جميع القواعد (عالية + متوسطة + منخفضة الخطورة). هذا هو أعلى مستوى أمان ل IPS.

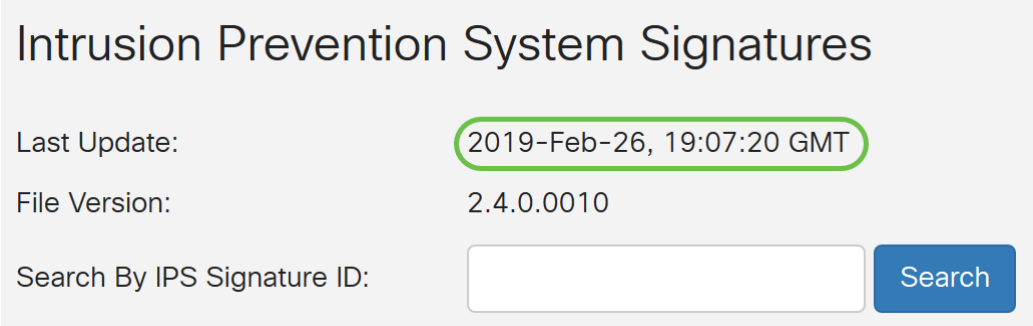
ملاحظة: كلما ارتفع مستوى الأمان الذي تختاره، كلما زاد عدد الهجمات التي يتم رصدها، كلما زاد التأثير على أداء النظام الذي قد يحدث.

سنختار **متوازن** لهذا العرض التوضيحي.

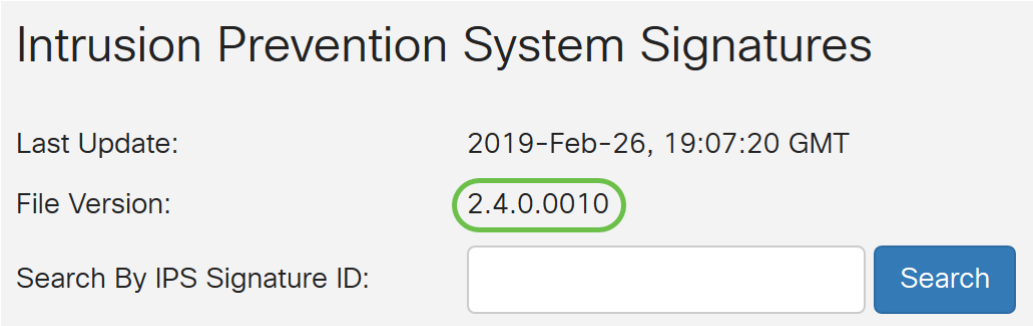


توقيعات نظام منع التسلل

الخطوة 6. في حقل *آخر تحديث*، سيعرض تاريخ ووقت آخر توقيع تم تحديثه.



الخطوة 7. يعرض *إصدار الملف* إصدار التوقيع الذي يتم إستخدامه.



الخطوة 8. للبحث عن معرف توقيع، أدخل **معرف التوقيع** في حقل *البحث بواسطة معرف توقيع IPS* وانقر فوق **بحث** للتحقق مما إذا كان التوقيع مدعوما أم لا. إذا كان معرف التوقيع مدعوما، سيتم تحديث الجدول بالنتيجة كما هو موضح أدناه.

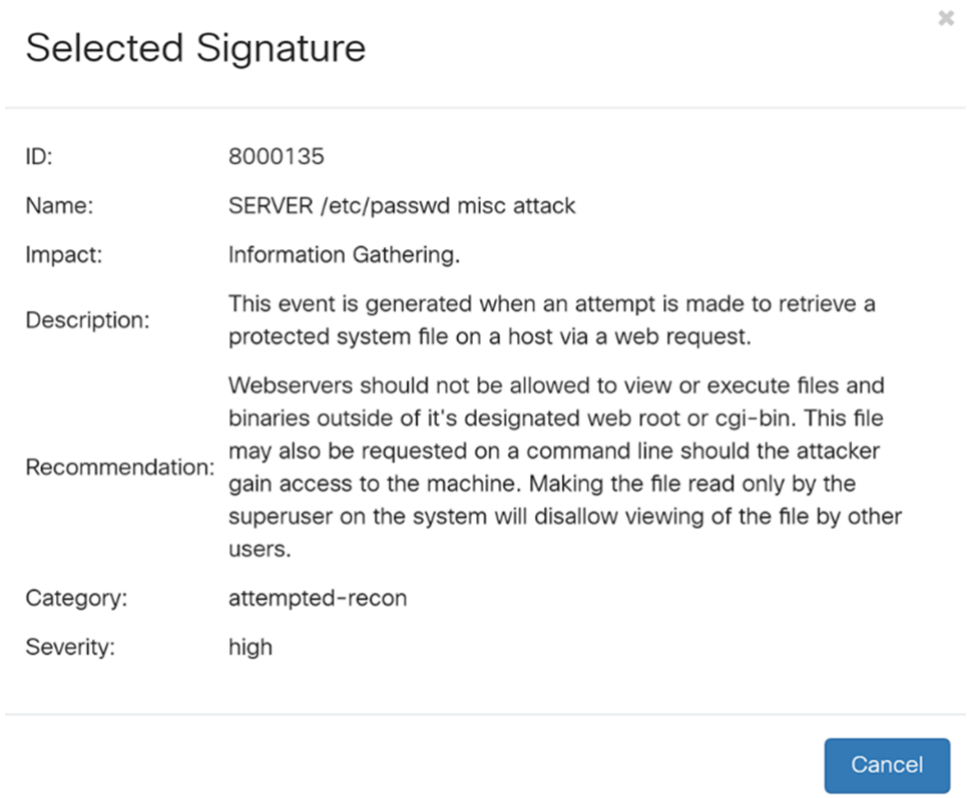
ملاحظة: إذا لم يكن معرف التوقيع مدعوما، فلن يظهر أي شيء في الجدول.

جدول توقيع نظام منع الاقتحام

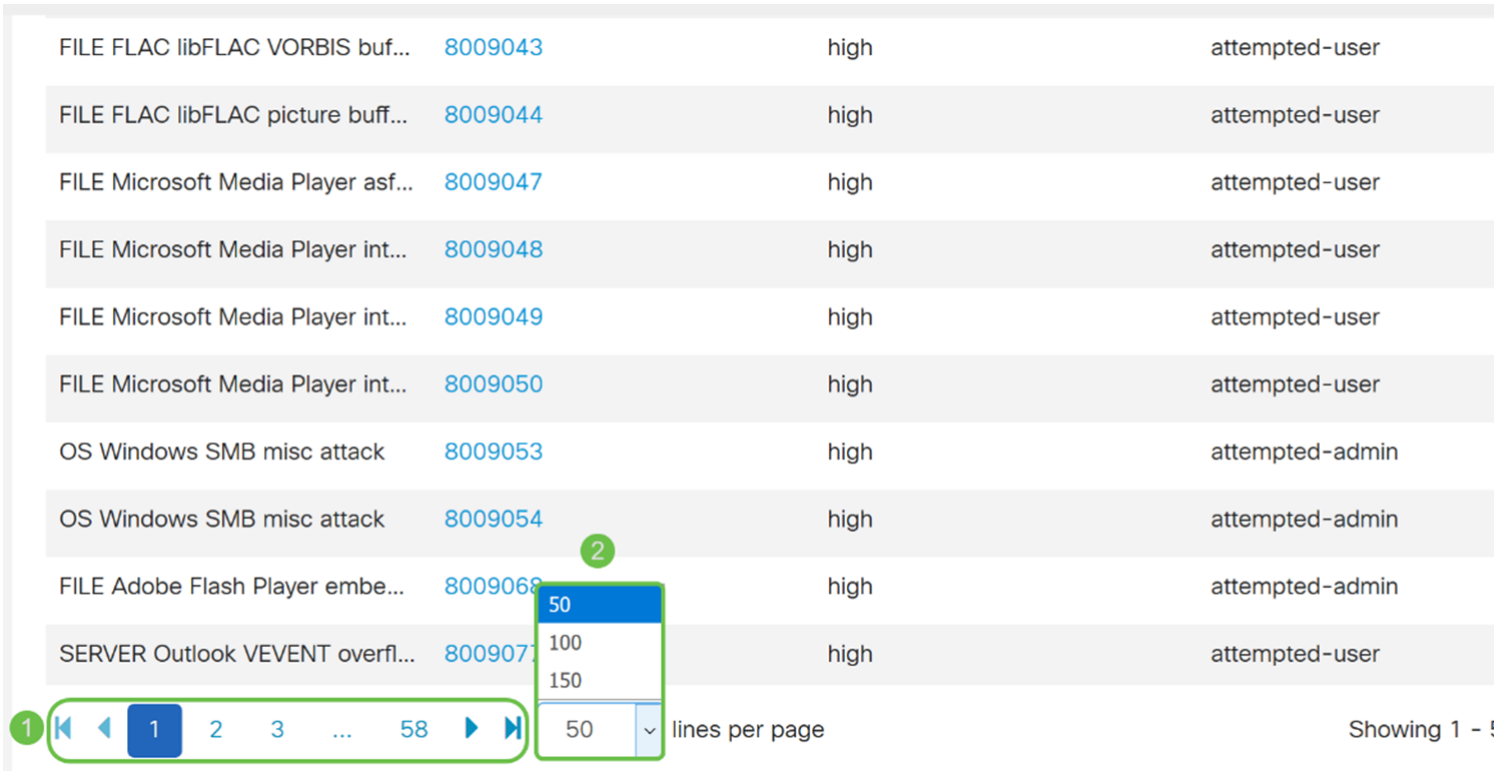
الخطوة 9. في *جدول توقيع IPS*، يتم تعريف الحقول التالية على أنها:

- **الاسم** - اسم التوقيع.
- **المعرف** - المعرف الفريد للتوقيع. سيؤدي النقر فوق المعرف إلى فتح نافذة لعرض التفاصيل الكاملة للتوقيع المحدد.
- **الخطورة** - .
- **الفئة** - .

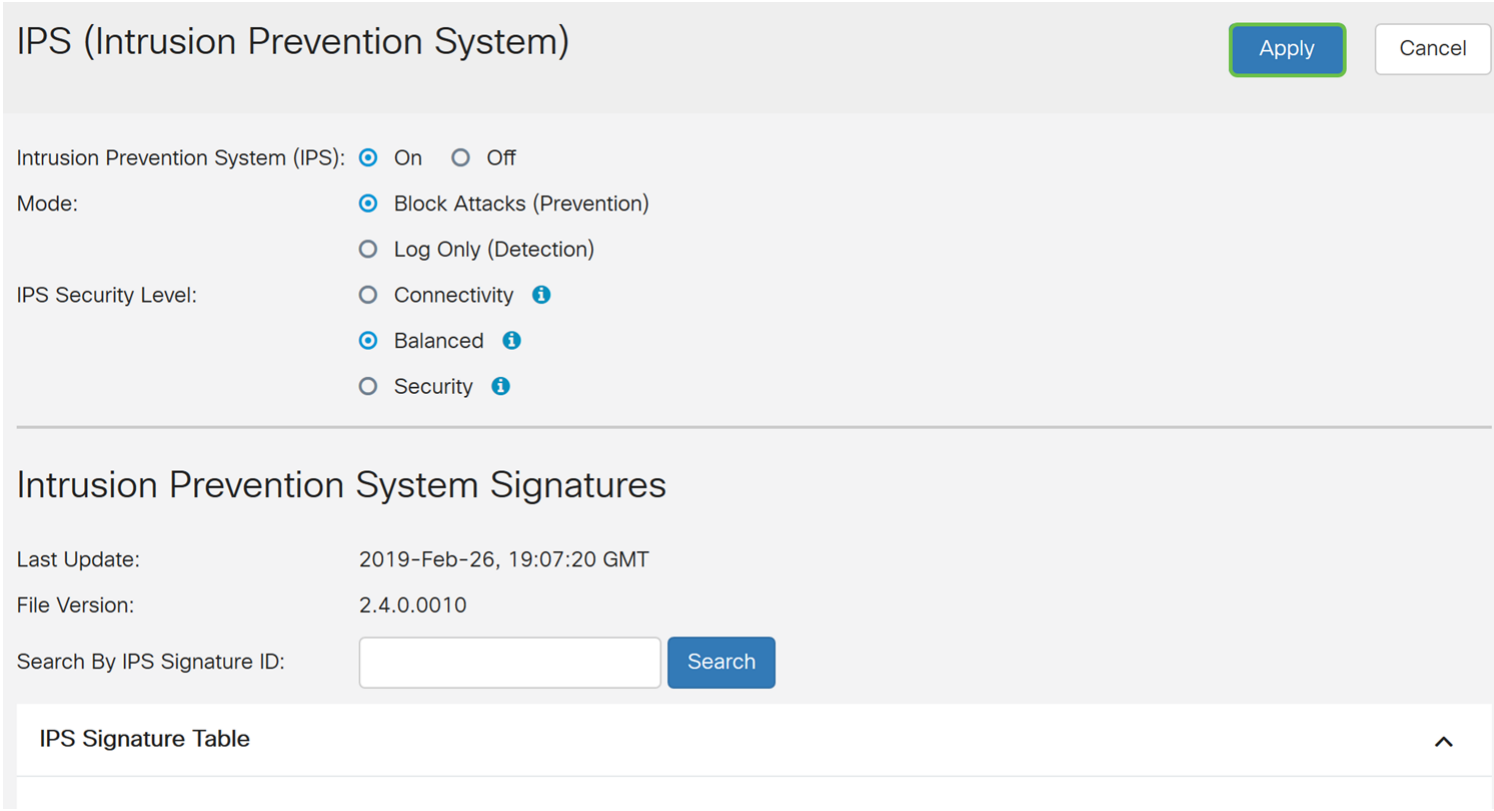
الخطوة 10. (إختياري) إذا قمت بالنقر فوق معرف التوقيع في *جدول توقيع IPS*، ستظهر نافذة لتظهر لك التفاصيل الكاملة للتوقيع المحدد.



الخطوة 11. في أسفل جدول *توقيع IPS*، حدد الأسهم وكذلك الأرقام التي تريد الانتقال بها إلى الأمام والخلف على الجدول. يمكنك أيضا تحديد مقدار الخطوط (**50**، **100**، أو **150**) لكل صفحة في **السطور لكل صفحة** في القائمة المنسدلة.



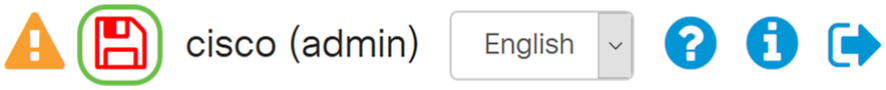
الخطوة 12. انقر فوق **تطبيق** لحفظ التغييرات التي أجريتها على ملف التكوين الجاري تشغيله.



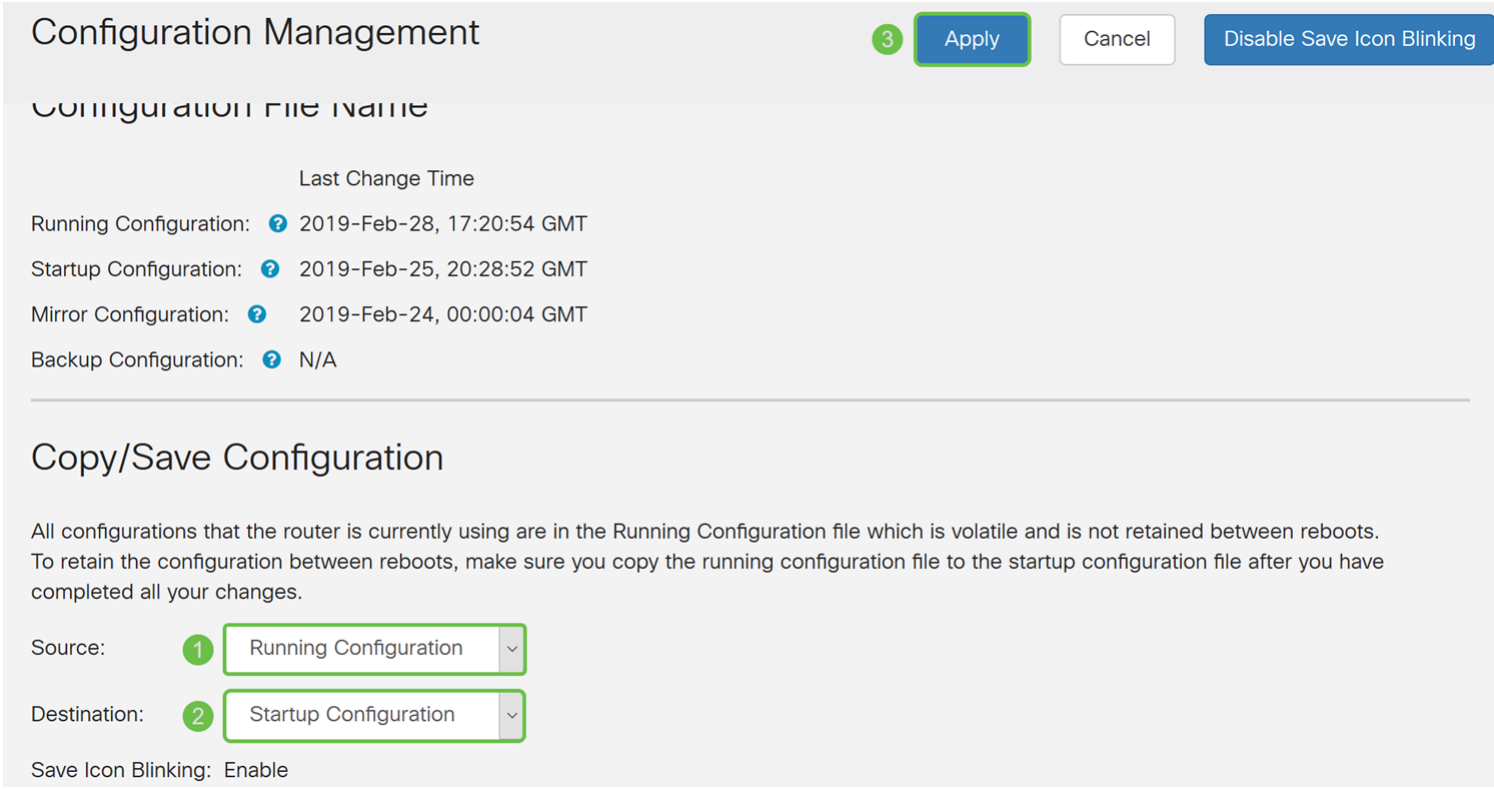
ملاحظة: توجد جميع التكوينات التي يستخدمها الموجه حاليا في ملف التكوين الجاري تشغيله والذي يكون متطايرا ولا يتم الاحتفاظ به بين عمليات إعادة التمهيد. للحفاظ على التكوين الخاص بك بين عمليات إعادة التمهيد، انسخ ملف التكوين الجاري تشغيله إلى ملف تكوين بدء التشغيل.

في الخطوات القليلة التالية، سنعرض لك كيفية نسخ التكوين الجاري تشغيله إلى تكوين بدء التشغيل.

الخطوة 13. انقر أيقونة **القرص المرن (حفظ)** في أعلى الصفحة. وهذا سيقوم بإعادة توجيهك إلى *إدارة التكوين* لحفظ التكوين الجاري تشغيله إلى تكوين بدء التشغيل.

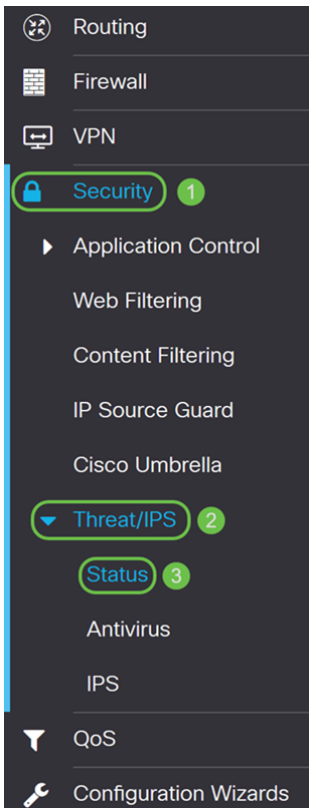


الخطوة 14. في *إدارة التكوين*، قم بالتمرير إلى قسم *نسخ/حفظ التكوين*. تأكد من أن *المصدر* يشغل التكوين *والوجهة* هي **بدء التشغيل**. طقطقة **يطبق**. سيؤدي هذا إلى نسخ ملف التكوين الجاري تشغيله إلى ملف تكوين بدء التشغيل للاحتفاظ بالتكوين بين عمليات إعادة التمهيد.

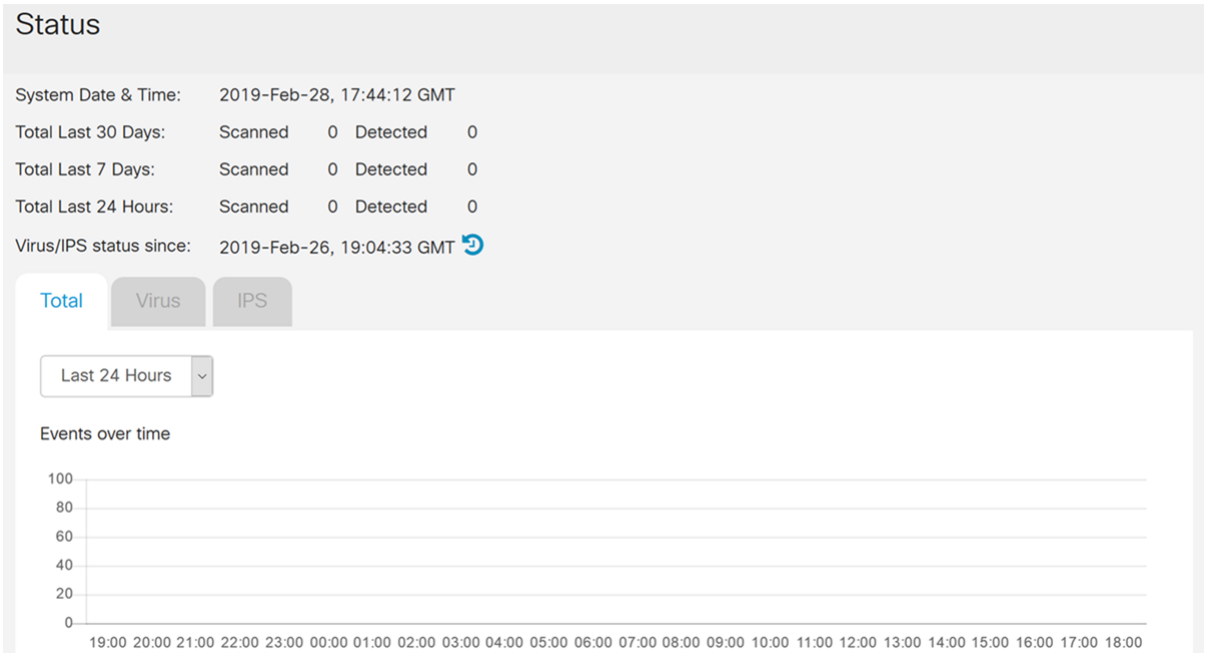


حالة IPS

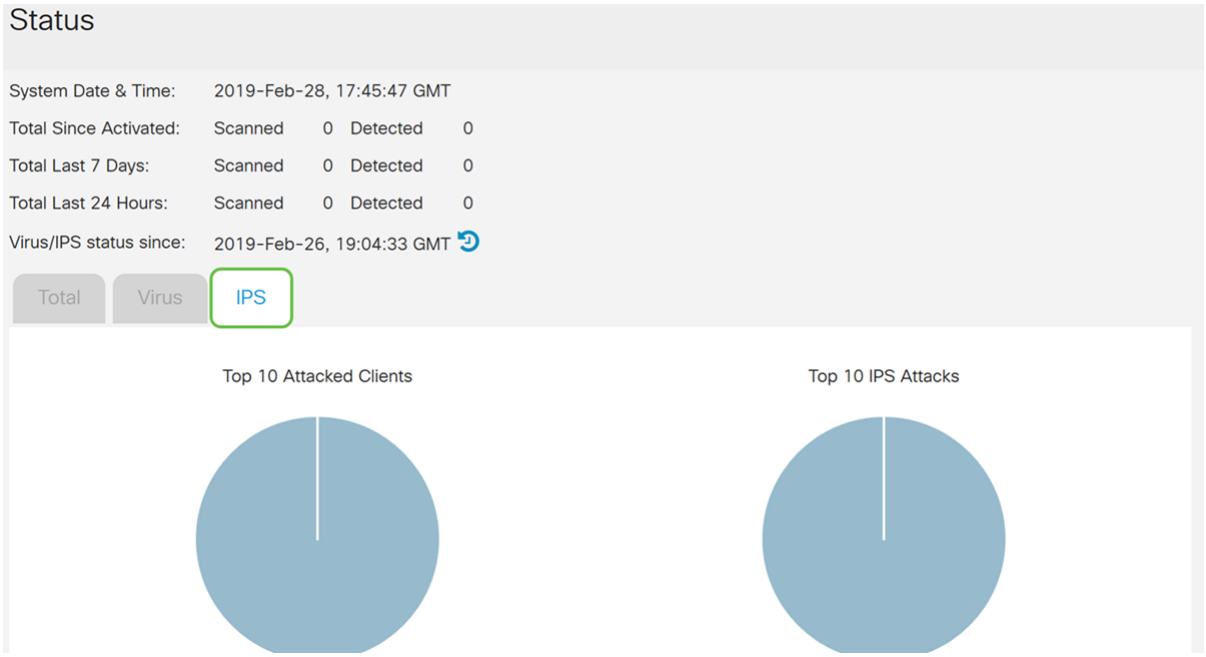
الخطوة 1. انتقل إلى **الأمان > التهديد/IPS > الحالة**.



الخطوة 2. تعرض صفحة *الحالة* تفاصيل التهديدات والهجمات عند تكوين ميزات الحماية من التهديد وبروتوكول الإنترنت (IPS). توفر لك لوحة المعلومات عرضا لملخص الأحداث بالكامل ومعلومات مفصلة عن التهديدات والهجمات التي تم الكشف عنها وفقا للتحديد مثل اليوم والأسبوع والشهر.



الخطوة 3. انقر فوق علامة التبويب **IPS**. وسيعرض هذا أفضل 10 عملاء مهاجمين بالإضافة إلى أكبر 10 هجمات ضمن خطة الحماية الدولية.

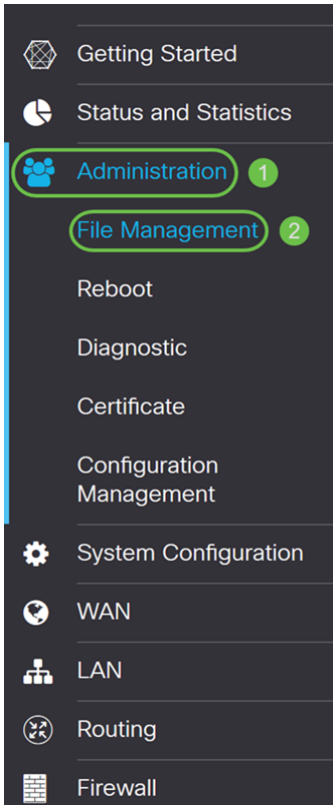


تحديث تعريفات IPS

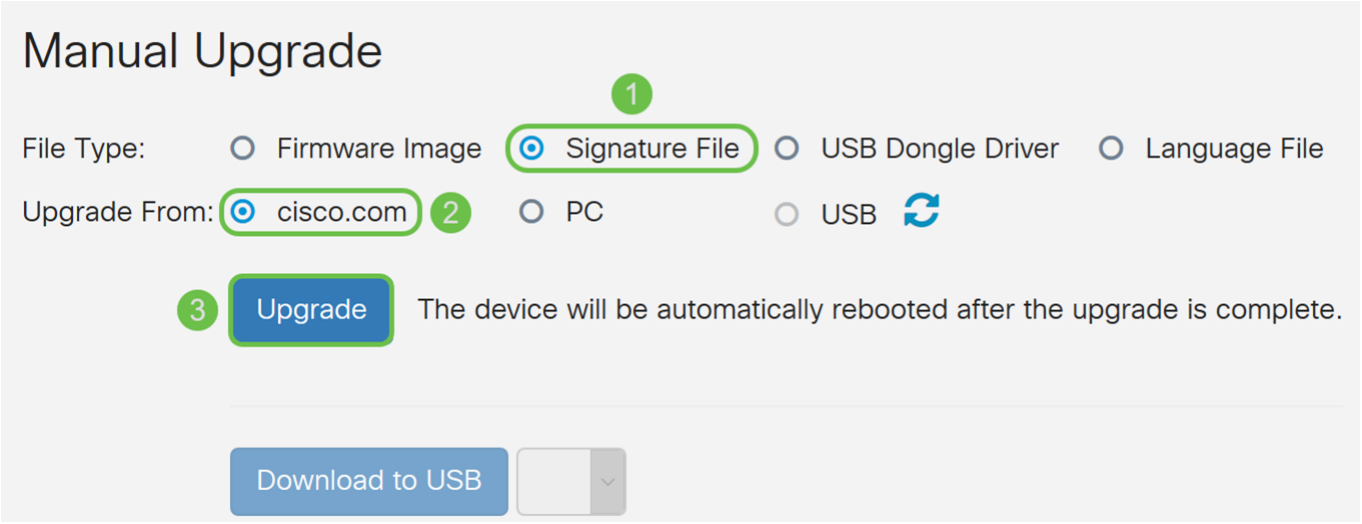
يمكنك تحديث تعريف IPS يدويا أو تلقائيا. توضح الخطوات من 1 إلى 2 كيفية تحديث تعريف IPS يدويا بينما تظهر لك الخطوات 3-6 كيفية تحديث تعريف IPS تلقائيا.

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

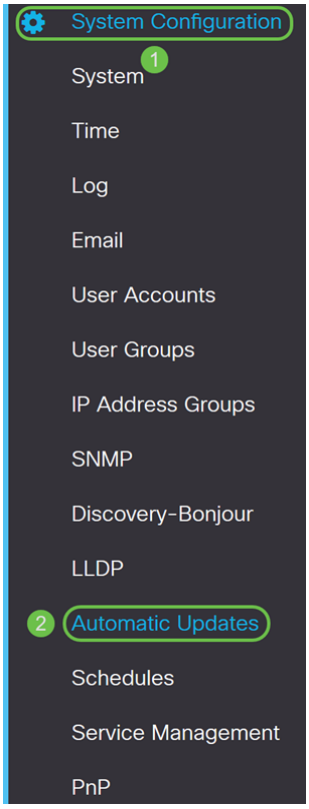
الخطوة 1. لتحديث تعريفات IPS يدويا، انتقل إلى **إدارة > إدارة الملفات**.



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.

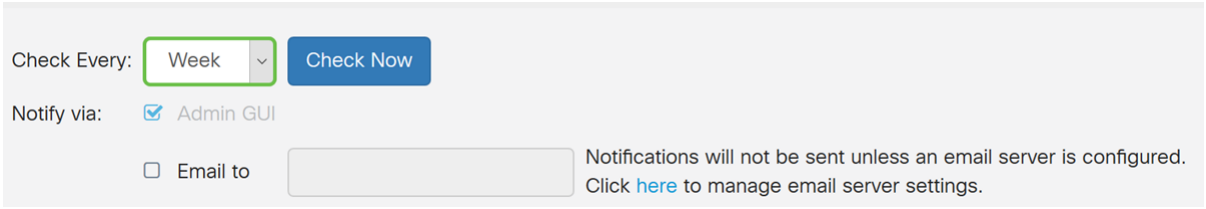


الخطوة 3. لتحديث تعريفات IPS تلقائيا، انتقل إلى **تكوين النظام > التحديثات التلقائية**.

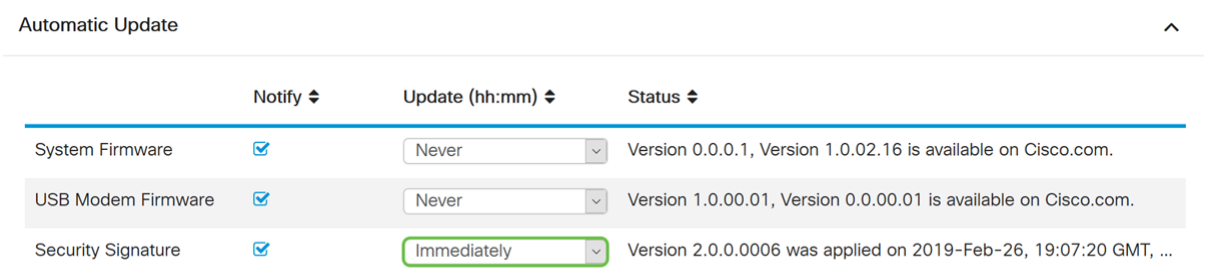


الخطوة 4. يتم فتح صفحة *التحديثات التلقائية*. لديك خيار التحقق من وجود تحديثات إما بشكل أسبوعي أو شهري. يمكنك أن تقوم بإخطار الموجه عبر البريد الإلكتروني أو واجهة مستخدم ويب. في هذا المثال، سنختار التحقق كل أسبوع.

ملاحظة: يوصى بتحديث توقيعات التأمين تلقائيا على أساس أسبوعي.

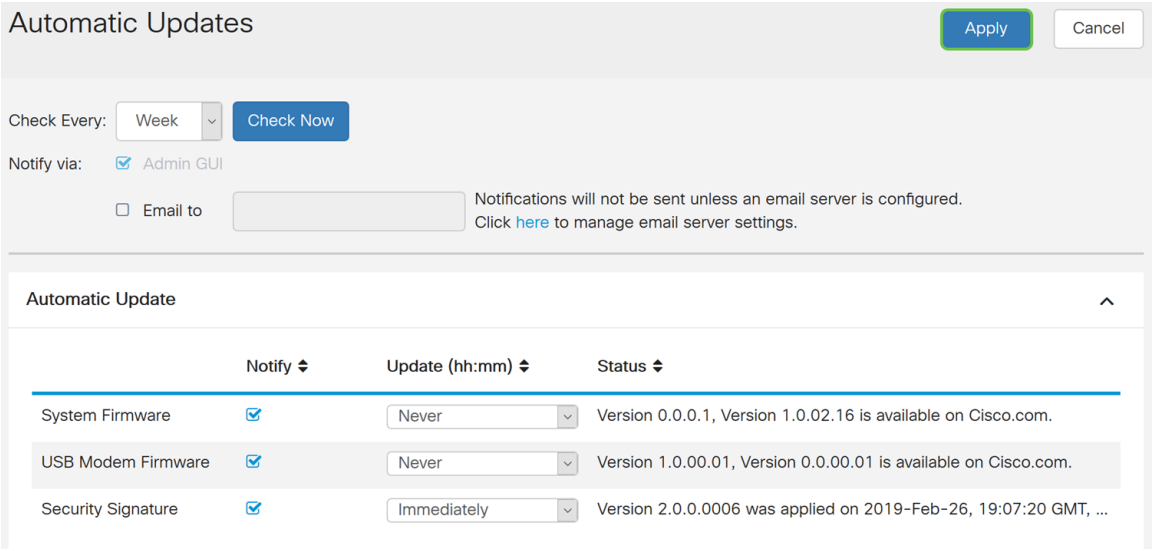


الخطوة 5. قم بالتمرير إلى قسم *التحديث التلقائي* وابحث عن حقل *توقيع الأمان*. في القائمة المنسدلة *تحديث توقيع الأمان*، حدد الوقت الذي تريد تحديثه تلقائيا. في هذا المثال، سنختار **فورا**.



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 نظام منع الاقتحام بنجاح على موجه من السلسلة RV34x.

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).