وحدة التحكم في إدارة اللوحة الأساسية CiscoWorks IPS Mc في مثال تكوين Cisco IOS IPS

المحتويات

المقدمة
المتطلبات الأساسية
المتطلبات
المكونات المستخدمة
الاصطلاحات
التكوين
فهم أساسي لمهام التكوين
التكوين الأولي لموجهات Cisco IOS IPS
إستيراد موجه Cisco IOS IPS إلى وحدة التحكم في الوصول الخاصة ب IPS
تكوين موجه Cisco IOS IPS لاستخدام ملفات التوقيع المعينة مسبقا
تعديل توقيعات SDF المضبوطة مسبقا
إختيار توقيعات مخصصة
إنشاء قاعدة لتطبيقها على الواجهة (الواجهات)
نشر التكوين
التنزيل التلقائي لتحديثات التوقيع
تحديث موجه Cisco IOS IPS بملفات SDF الجديدة
معلومات ذات صلة

المقدمة

يعد مركز إدارة CiscoWorks لأجهزة إستشعار IPS (IPS MC) وحدة التحكم في الإدارة لأجهزة Cisco IPS. يدعم الإصدار 2.2 من IPS MC توفير ميزة نظام منع التسلل (IPS) على موجهات برامج Cisco IOS®. يصف هذا المستند كيفية إستخدام IPS MC 2.2 لتكوين Cisco IOS IPS.

للحصول على مزيد من المعلومات حول كيفية إستخدام وحدة التحكم في الوصول الخاصة ببروتوكول IPS (والتي تتضمن كيفية إستخدامها لتكوين الأجهزة التي لا تستند إلى برنامج Cisco IOS)، ارجع إلى مركز إدارة CiscoWorks لوثائق أجهزة إستشعار IPS في عنوان URL هذا:

http://www.cisco.com/en/US/products/sw/cscowork/ps3990/index.html

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى مركز إدارة CiscoWorks لأجهزة إستشعار IPS (IPS MC)، الإصدار 2.2.

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

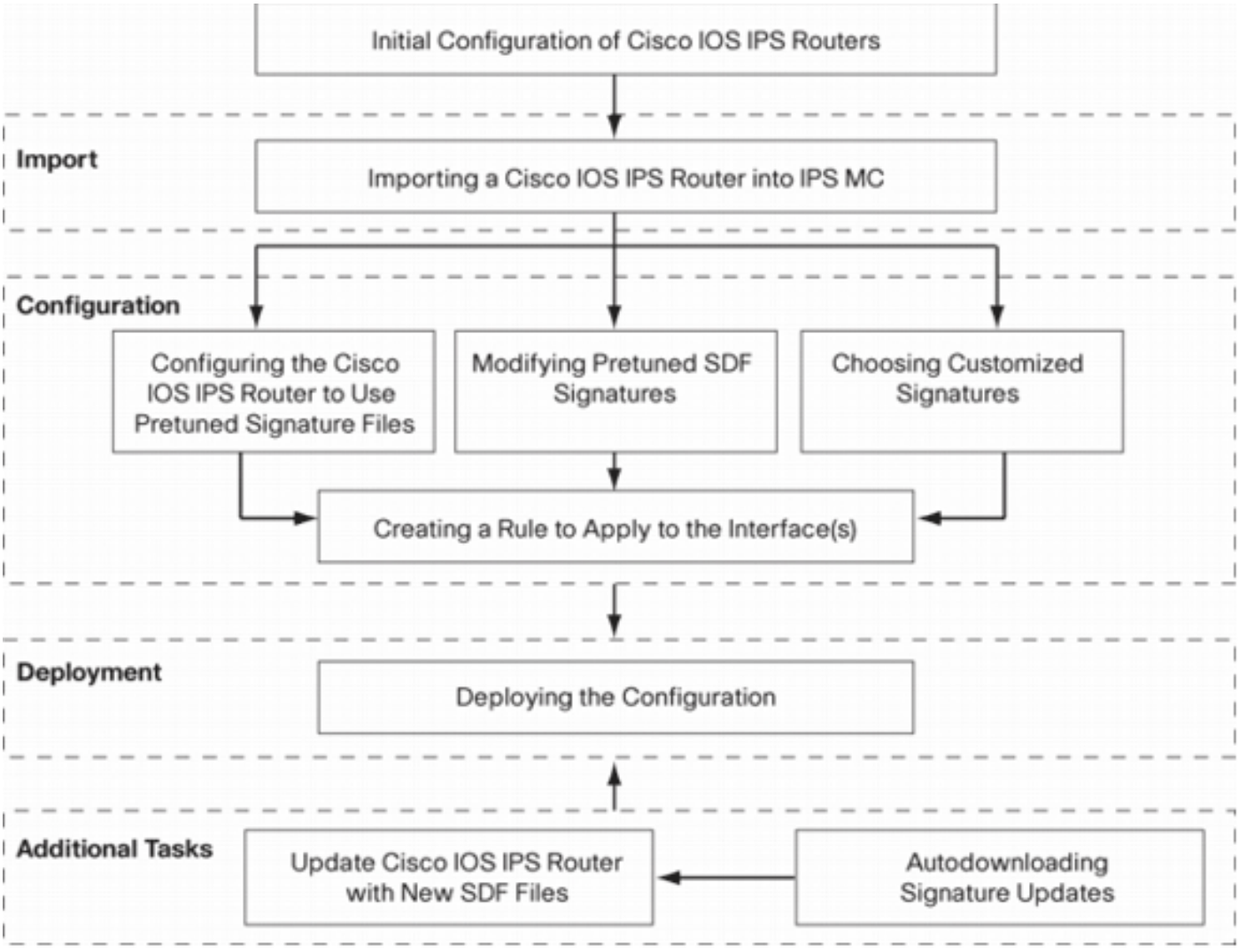
الاصطلاحات

راجع اصطلاحات تلميحات Cisco التقنية للحصول على مزيد من المعلومات حول اصطلاحات المستندات.

التكوين

فهم أساسي لمهام التكوين

يتم إستخدام وحدة التحكم في الوصول الخاصة ببروتوكول IPS لإدارة تكوين مجموعة من موجهات Cisco IOS IPS. لاحظ أن وحدة التحكم في الوصول الخاصة ببروتوكول IPS لا تقوم بإدارة التنبيهات من الموجهات التي تقوم بتشغيل IPS. توصي Cisco بنظام Cisco لمراقبة الأمان والتحليل والاستجابة (Cisco Security MARS) لمراقبة بروتوكول الإنترنت (IPS). تتألف إدارة التكوين من سلسلة من المهام الموضحة في هذا المستند. يمكن تقسيم هذه المهام إلى ثلاث مراحل: الاستيراد والتكوين والنشر كما هو موضح في هذه الصورة.



ولكل مرحلة مجموعة خاصة بها من المسؤوليات والمهام:

- *الاستيراد*—إستيراد موجه إلى وحدة التحكم في إدارة اللوحة الأساسية (MC) ل IPS. يجب إستيراد موجه إلى وحدة التحكم في إدارة الشبكة (MC) من IPS قبل أن تتمكن من إستخدام وحدة التحكم في الشبكة (IPS) لتكوينها. لا يمكن إستيراد موجه ما لم يكن هناك تكوين IPS أولي موجود على الموجه (يتم توفير التفاصيل لاحقا في هذا المستند).
- *تشكيل*— يشكل الجهاز. على سبيل المثال، يمكنك تكوين موجه Cisco IOS IPS لاستخدام واحد من ملفات التوقيع المسبقة الموصى بها من Cisco. يتم تخزين تغييرات التكوين في وحدة التحكم في الوصول الخاصة ببروتوكول IPS، ولكنها لا يتم إرسالها إلى الموجه في هذه المرحلة.
- *النشر*—قم بتسليم تغييرات التكوين إلى الجهاز الفعلي. خلال هذه المرحلة، تقوم بتنفيذ التغييرات التي تم إجراؤها في مهام التكوين للموجهات.
- *مهام إضافية*—يوفر IPS MC وظيفة تنزيل تلقائي لتنزيل تحديثات التوقيع تلقائيا من Cisco.com.

يجب عليك فهم هذا النهج المرحلي من أجل الاستخدام الفعال لوحدة التحكم في الإنترنت IPS. هو مختلف من أداة baser إدارة guiS، مثل cisco مسحاج تخديد وأمان أداة مدير (SDM). تعمل شبكات GUI المستندة إلى الأجهزة مباشرة على موجه واحد، في حين تم تصميم وحدة التحكم في الوصول الخاصة ببروتوكول IPS للعمل على مجموعات الموجهات (وأجهزة IPS الأخرى مثل أجهزة إستشعار Cisco IPS 4200 Series) على مستوى الشبكة.

يوفر هذا المستند معلومات حول كل مهمة من المهام الموجودة في المخطط لمساعدتك في إستخدام وحدة التحكم في الإنترنت (IPS) لإدارة موجهات Cisco IOS IPS.

التكوين الأولي لموجهات Cisco IOS IPS

من أجل إستيراد موجه Cisco IOS IPS أو إضافته بنجاح إلى وحدة التحكم في الإنترنت (IPS)، يجب عليك تنفيذ بعض خطوات التكوين الأولية على موجهات Cisco IOS IPS. يصف هذا القسم هذه الخطوات.

يجب تمكين بروتوكول طبقة الأمان (SSH) في موجه Cisco IOS IPS للتكوين والاستيراد والنشر من خلال Cisco IPS MC. بالإضافة إلى ذلك، يجب تمكين بروتوكول "تبادل أحداث أجهزة الأمان" (SDEE) لأغراض إعداد تقارير الأحداث (على الرغم من عدم إرسال هذه التنبيهات إلى وحدة التحكم الإدارية ل IPS لأنه يتم إستخدام وحدة التحكم في الوصول الخاصة ب IPS فقط للتوفير، وليس إعداد التقارير). أخيرا، يلزمك التأكد من مزامنة إعداد الساعة على موجه IPS مع IPS MC.

أكمل الخطوات التالية لتكوين موجهات IOS IPS لديك:

1. قم بإنشاء اسم مستخدم وكلمة مرور محليين للموجه.

```
Router#config terminal
Router(config)#username <username> password <password>
```

2. قم بتمكين تسجيل الدخول المحلي على واجهة خطوط vty.

```
Router#config terminal
Router(config)#line vty 0 15
Router(config-line)#login local
Router(config-line)#exit
```

إذا تم تكوين واجهة سطر الأوامر (CLI) للنقل input أو transport output تحت تكوين سطر vty، فتأكد من تمكين SSH. على سبيل المثال:

```
Router#conf terminal
Router(config)#line vty 0 15
Router(config-line)#transport input ssh telnet
Router(config-line)#exit
```

3. قم بإنشاء مفتاح -RSA 1024بت (إذا لم يكن هناك مفتاح بالفعل).يتم تمكين SSH تلقائيا بعد إنشاء مفتاح التشفير.

```
Router#conf terminal
.Enter configuration commands, one per line. End with CNTL/Z
Router(config)#crypto key generate rsa
The name for the keys will be: Router.cisco.com
Choose the size of the key modulus in the range of 360 to 2048 for your General Purpose
.Keys
.Choosing a key modulus greater than 512 may take a few minutes
How many bits in the modulus [512]: 1024
[Generating 1024 bit RSA keys, keys will be non-exportable...[OK %
#(Router(config
Jan 23 00:44:40.952: %SSH-5-ENABLED: SSH 1.99 has been enabled*
#(Router config
```

4. قم بتمكين SDEE على الموجه.

```
Router(config)#ip ips notify sdee
```

5. تمكين HTTPS.يتطلب HTTP أو HTTPS لكي تتصل IPS MC بالموجه باستخدام SDEE لتجميع معلومات الحدث.

```
Router(config)#ip http authentication local
Router(config)#ip http secure-server
```

6. أستخدم خادم بروتوكول وقت الشبكة الخارجي (NTP) أو الأمر clock لتكوين إعداد الساعة على موجه IPS.

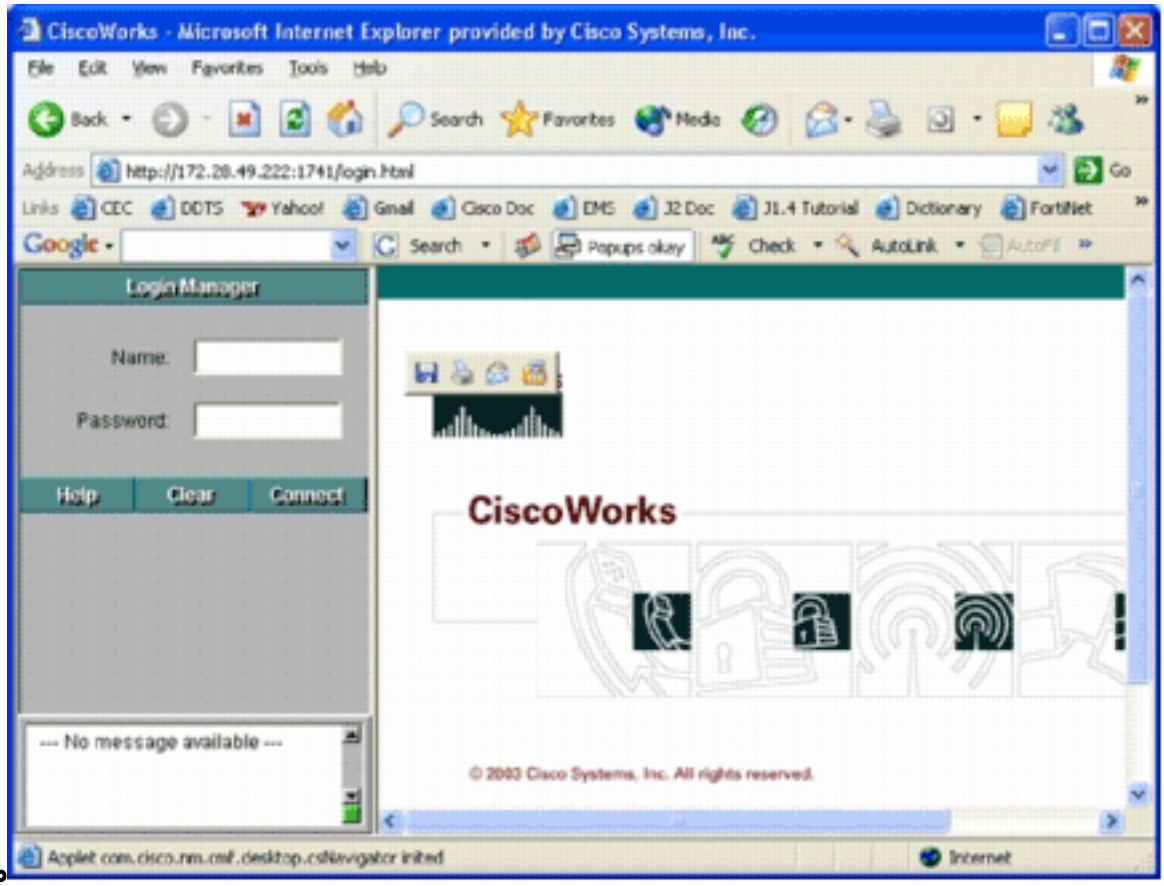
```
Router(config)#clock set hh:mm:ss day month year
```

يعد موجه Cisco IOS IPS الآن جاهزا ويمكن إستيراده إلى وحدة التحكم في إدارة النظام الأساسي ل IPS للحصول على مزيد من التهيئة والإدارة.

إستيراد موجه Cisco IOS IPS إلى وحدة التحكم في الوصول الخاصة ب IPS

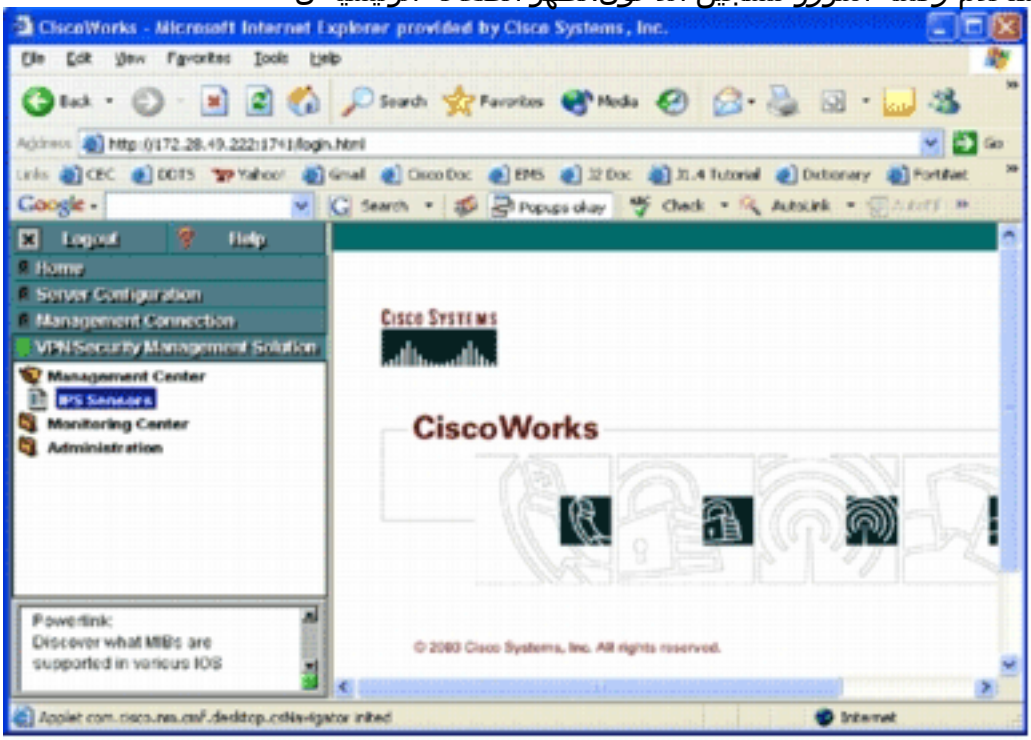
بمجرد اكتمال التكوين الأولي على الموجه، يمكنك إضافته (أو إستيراده) إلى وحدة التحكم في الوصول الخاصة ب IPS.

1. قم بتشغيل مستعرض الويب الخاص بك، وأشر إلى خادم CiscoWorks.يظهر مدير تسجيل الدخول إلى CiscoWorks.



ملاحظة: رقم المنفذ الافتراضي لخادم الويب هو 1741؛ لذلك، يجب إستخدام عنوان URL مماثل ل http://<*server ip address*>:1741/.

2. أدخل اسم المستخدم وكلمة المرور لتسجيل الدخول.تظهر الصفحة الرئيسية ل CiscoWorks.

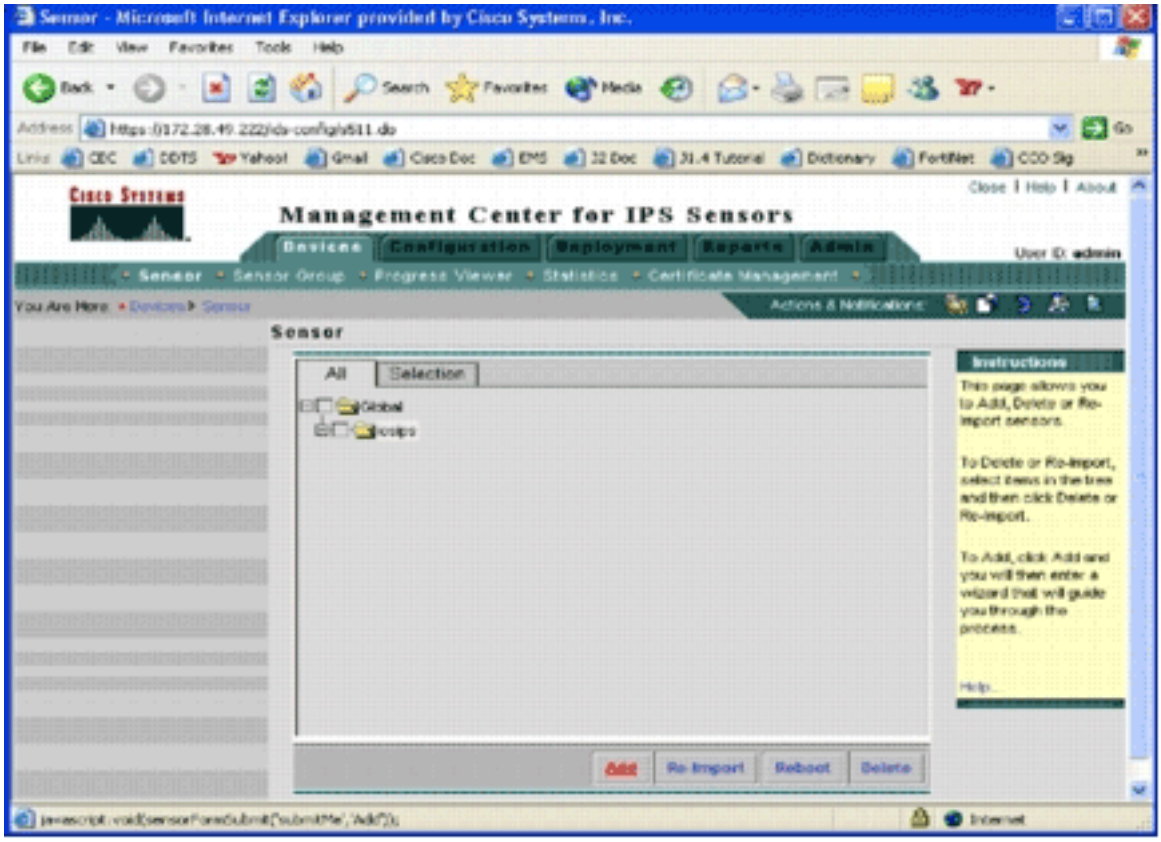


3. في لوحة التنقل اليسرى، أختر **حل إدارة الأمان/الشبكة الخاصة الظاهرية (VPN)**، ثم أختر **مركز الإدارة**.سوف تظهر صفحة "مركز إدارة أجهزة إستشعار

تعرض "IPS".

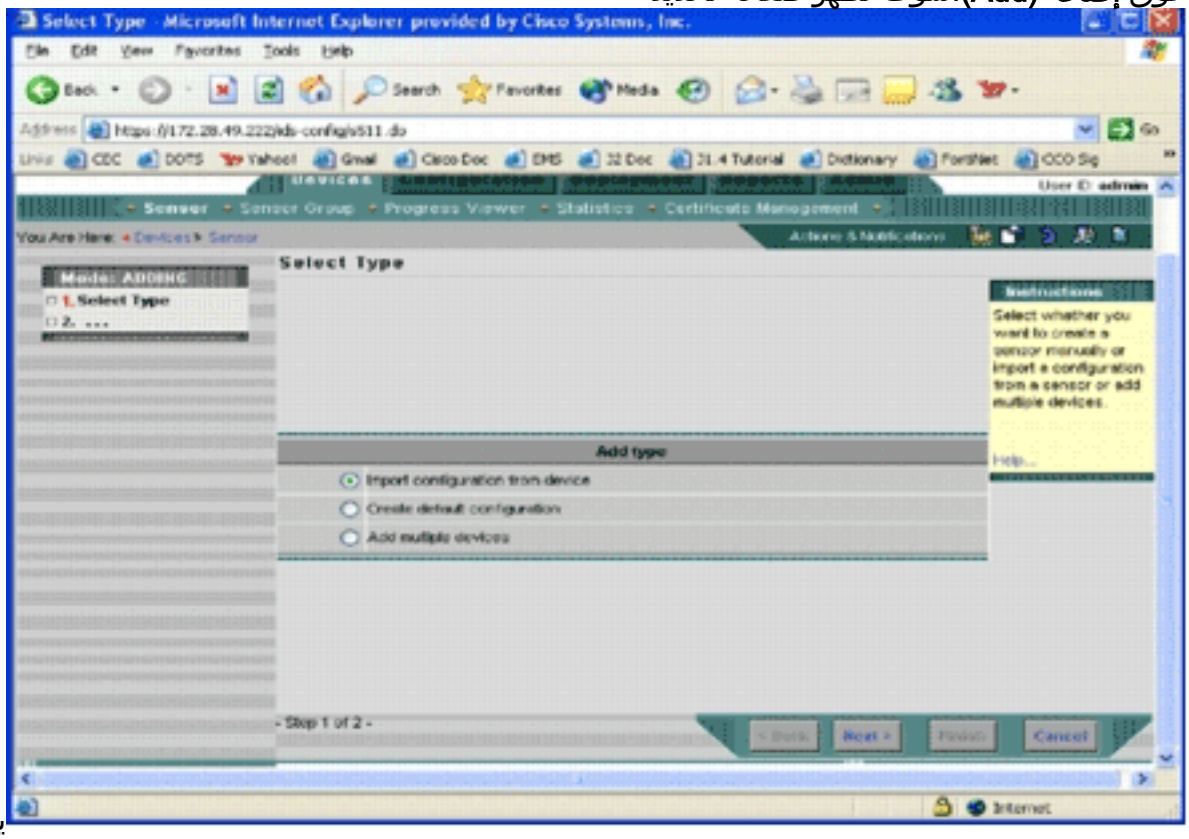
هذه الصفحة علامات التبويب الخمس التالية:*الأجهزة*—في علامة التبويب "الأجهزة"، يمكنك تنفيذ الإعداد الأولي لكافة الأجهزة وإدارتها على النظام.*التكوين*—في علامة التبويب "التكوين"، يمكنك تنفيذ وظائف الإمداد. يمكنك تكوين الأجهزة على مستوى الأجهزة الفردية أو على مستوى المجموعة. يمكن أن تحتوي مجموعة أجهزة واحدة على أجهزة متعددة. يجب حفظ كافة التغييرات التي تم إجراؤها من خلال مهام التكوين. لا تقوم وظيفة التكوين بإجراء تغييرات على الأجهزة على الفور. يجب إستخدام وظيفة النشر لنشر التغييرات.*النشر*—في علامة التبويب النشر، يمكنك نشر تغييرات التكوين الخاصة بك إلى الأجهزة. توفر إمكانية الجدولة إمكانية تحكم مرنة في الوقت الذي يجب أن تدخل فيه تغييرات التكوين حيز التنفيذ.*التقارير*—في علامة التبويب "التقارير"، يمكنك إنشاء تقارير متنوعة حول عمليات النظام.*admin*—في علامة التبويب "الإدارة"، يمكنك تنفيذ مهام إدارة النظام، مثل إدارة قاعدة البيانات وتهيئة النظام وإدارة الترخيص.

4. انقر فوق علامة التبويب **الأجهزة** لإضافة جهاز جديد.تظهر صفحة



المستشعر.

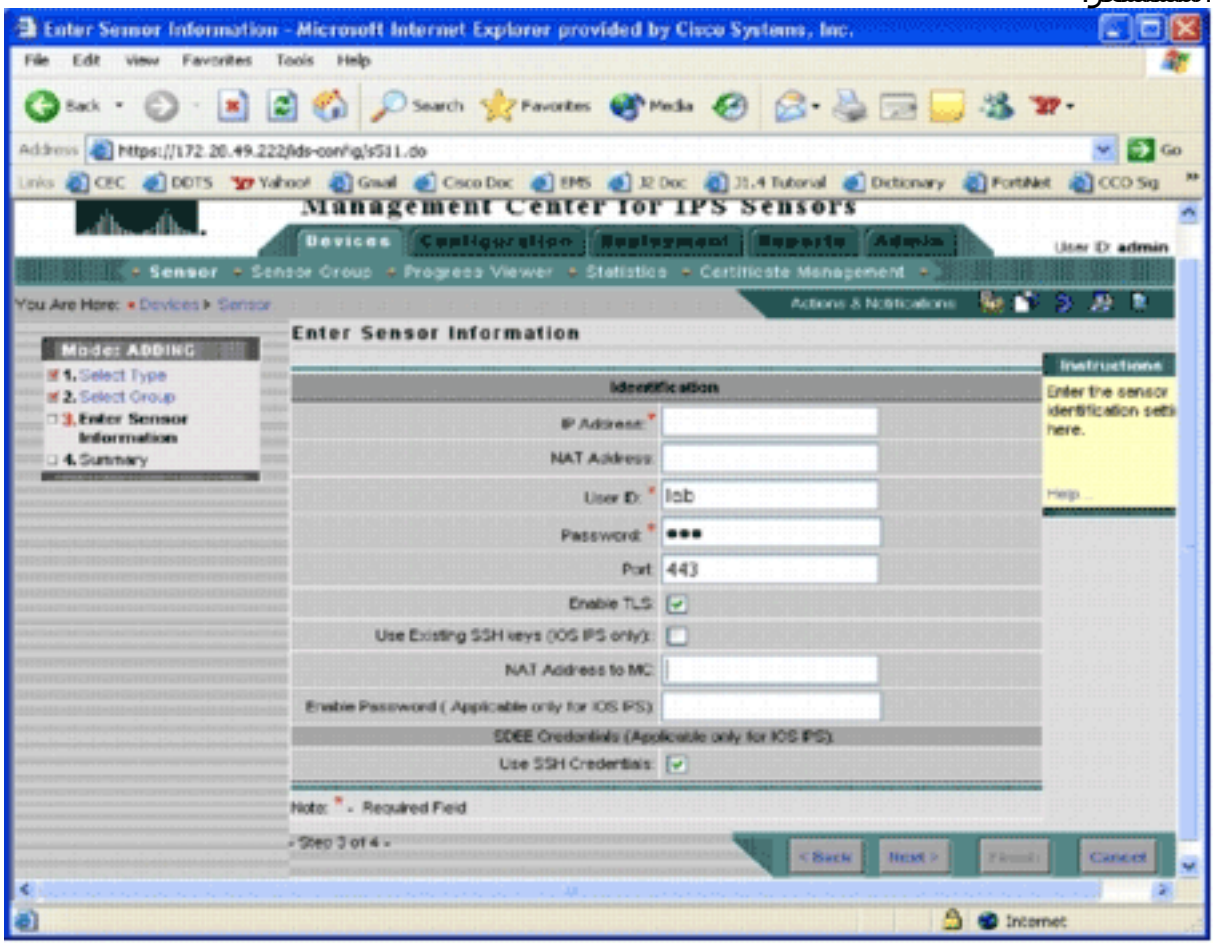
5. انقر فوق **إضافة (Add)**.سوف تظهر صفحة تحديد



نوع. يجب إعلام IPS MC بنوع وظيفة الإضافة التي تريد تنفيذها. تصف هذه القائمة كل خيار:*إستيراد التكوين من الجهاز*—أستخدم هذا الخيار لإضافة أجهزة IPS MC التي يتم تشغيلها حاليا على الشبكة.*إنشاء تكوين افتراضي*—أستخدم هذا الخيار لإضافة الأجهزة التي لا تعمل حاليا على الشبكة حتى الآن.*إضافة أجهزة متعددة*-أستخدم هذا الخيار لإضافة أجهزة متعددة. يمكنك إنشاء ملف csv. أو .xml يحتوي على جميع معلومات الجهاز ثم إستيرادها إلى وحدة التحكم في الوصول الخاصة ب IPS لإضافة الأجهزة في وقت واحد.**تلميح:** توجد ملفات تنسيق .csv و .xml العينة في: \InstallDirectory\MDC\etc\ids ويطلق عليها اسم -MultiAddDevices format.csv و MultiAddDevices-format.xml، على التوالي.

6. أختر خيار إضافة نوع مناسب، وانقر **التالي**.

7. حدد المجموعة التي تريد إضافة موجه Cisco IOS IPS إليها، أو أستخدم المجموعة العمومية الافتراضية، ثم انقر فوق **التالي**.سوف تظهر صفحة إدخال معلومات المستشعر.



8. في صفحة التعريف، أدخل معلومات تعريف الجهاز.**ملاحظة:** إذا لم يكن للمستخدم حقوق وصول إلى مستوى الامتياز 15، فيجب عليك توفير كلمة مرور enable. في الصف الأخير من صفحة التعريف، حدد خانة الاختيار **إستخدام بيانات اعتماد SSH**.
9. انقر فوق **Next (التالي)**.يظهر ملخص إضافة مستشعر.
10. انقر فوق **إنهاء**.تمت إضافة الجهاز بنجاح إلى IPS MC.**ملاحظة:** إذا واجهت أخطاء أثناء عملية الاستيراد، تأكد من التحقق من هذه العناصر:*تكوين المتطلب الأساسي*— يلزم توفر هذه التكوينات ل IPS MC للاتصال بموجهات Cisco IOS IPS.*الاتصال*— تأكد من أن وحدة التحكم في إدارة اللوحة الأساسية (IPS) يمكنها الوصول إلى موجهات Cisco IOS IPS.*الساعة* — تحقق من الوقت الموجود على وحدة التحكم في IPS وموجه Cisco IOS IPS. يمثل الوقت مكونا هاما لشهادة HTTPS التي يتم إستخدامها للمصادقة. يجب أن يكون الوقت في غضون 12 ساعة من بعضها البعض. (أفضل الممارسات بضع ساعات على الأكثر).*شهادة Cisco IOS IPS*—أحيانا تكون شهادة Cisco IOS IPS المخزنة غير صحيحة. لحذف شهادة من Cisco IOS IPS، يجب عليك إزالة TrustPoint من موجه Cisco IOS IPS.*تكوين إضافي*— إذا تم تكوين **ip http timeout-policy** باستخدام عدد قليل من الحد الأقصى للطلبات، مثل **ip http timeout-policy idle 600 life 86400 طلب 1**، فيجب عليك زيادة الحد الأقصى لعدد الطلبات. على سبيل المثال: **ip http timeout-policy idle 600 Life 86400 طلبات 8400**

تكوين موجه Cisco IOS IPS لاستخدام ملفات التوقيع المعينة مسبقا

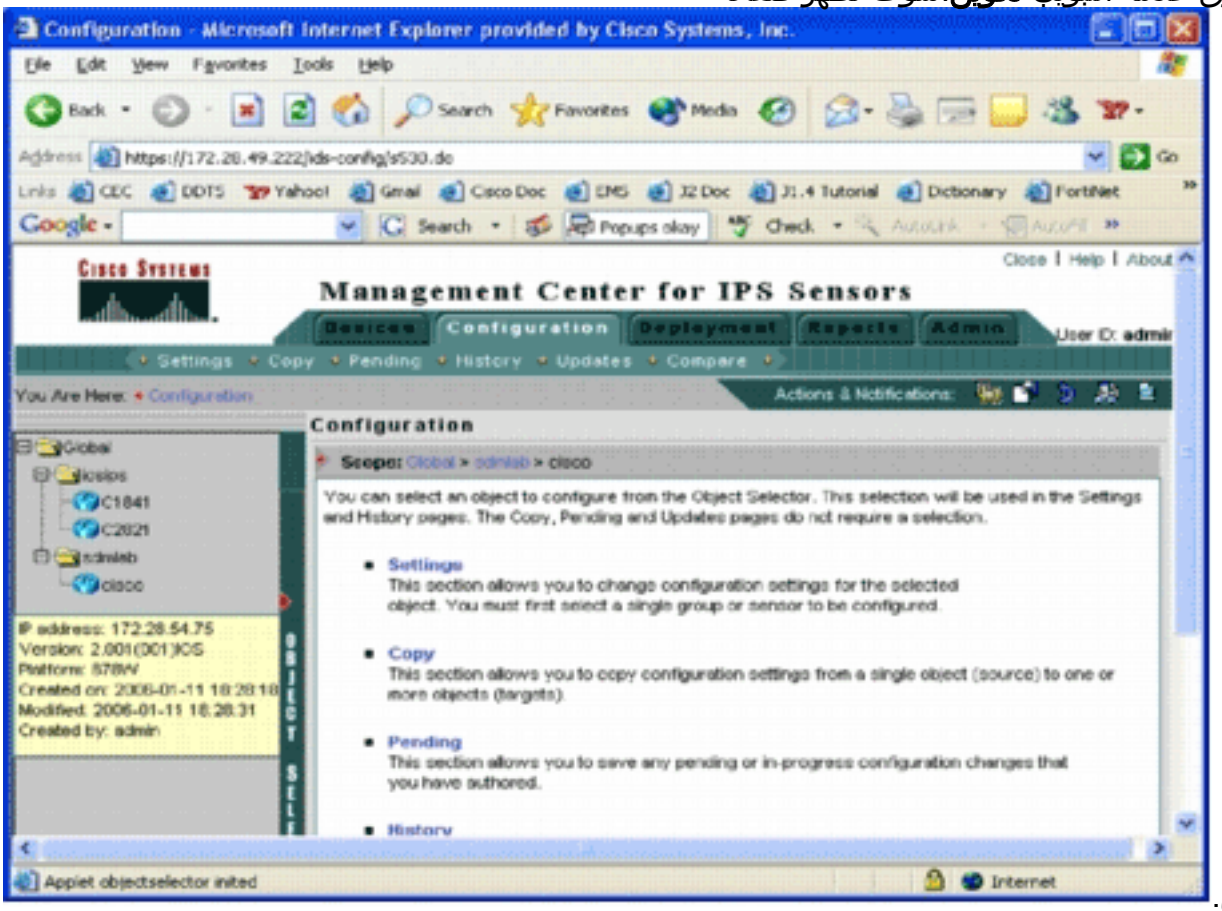
بعد إستيراد الموجه إلى وحدة التحكم في إدارة اللوحة الأساسية (IPS)، يجب عليك تحديد ملف تعريف التوقيع (SDF) (ملف مستند إلى نص يتضمن توقيعات التهديد التي سيستخدمها موجه IPS) والإجراء الذي يجب إتخاذه عند تشغيل كل توقيع (على سبيل المثال، إسقاط وإعادة ضبط بروتوكول TCP والتنبيه).

توصي Cisco Systems® باستخدام ملفات SDF مسبقة الضبط من Cisco. وتوجد حاليا ثلاثة ملفات من هذا القبيل

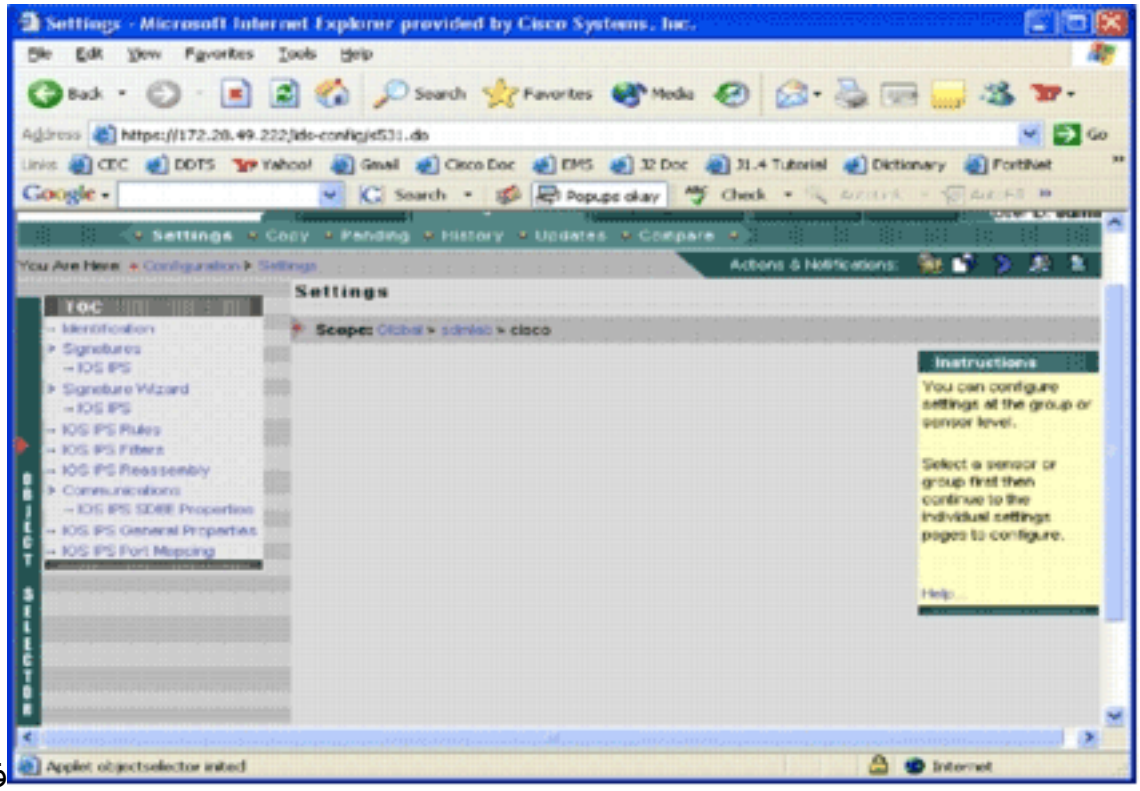
هي: وحدة الهجوم-drop.SDF، وحدة التحكم 128 ميجابايت.SDF، ووحدة التحكم 256 ميجابايت. يمكن ل IPS MC تنزيل هذه الملفات تلقائيا من Cisco.com. راجع تحديثات توقيع التنزيل التلقائي للحصول على مزيد من المعلومات.

يستخدم هذا الإجراء جهازا فرديا كمثال ويبدأ باستخدام موجه بدون تكوين IPS. يمكنك أيضا إستخدام هذا الإجراء لأجهزة متعددة على مستوى مجموعة.

1. انقر فوق علامة التبويب **تكوين**.سوف تظهر صفحة التكوين.



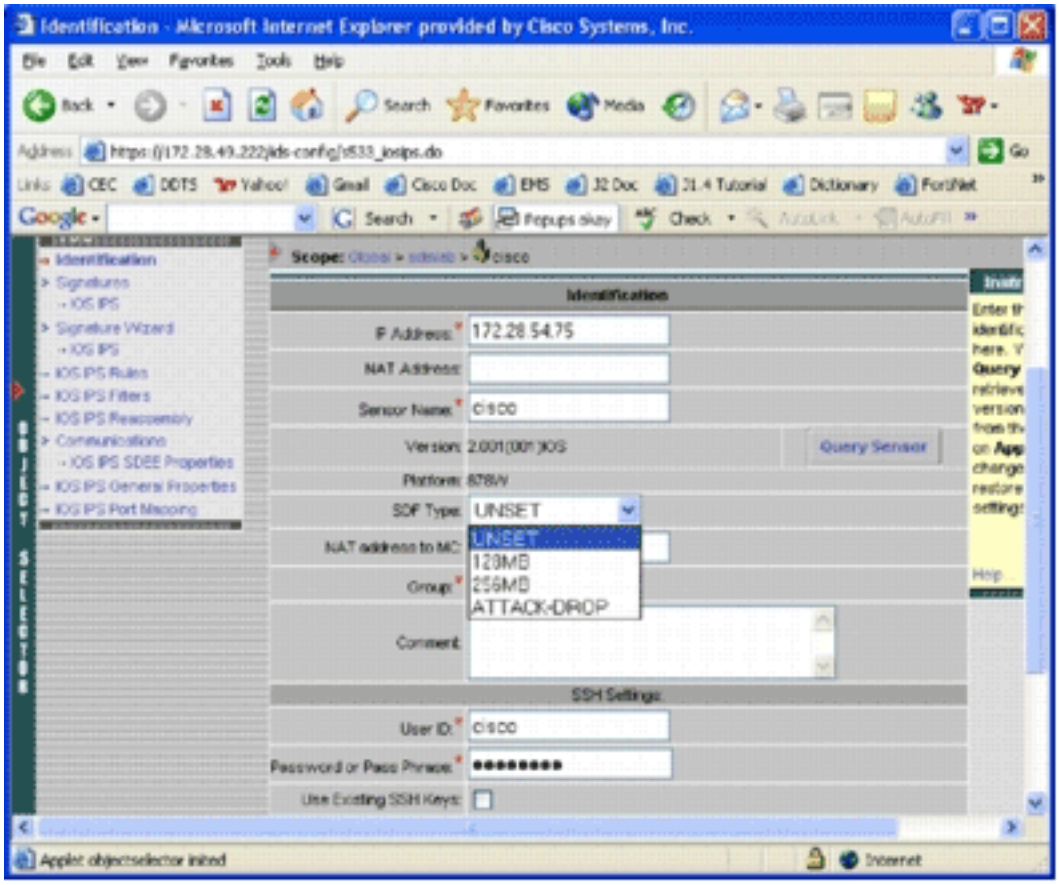
2. من محدد الكائن الموجود على الجانب الأيسر من الصفحة، أختر موجه Cisco IOS IPS الذي تريد تكوينه.**ملاحظة:** يمكن تكوين معظم إعدادات التكوين في IPS MC 2.2 على مستوى المجموعة وكذلك على مستوى الجهاز الفردي. على سبيل المثال، مجموعات العناصر العامة و ioSIPS و sdmlab هي جميع مجموعات الكائنات القابلة للتكوين. يستخدم هذا المثال أداة فردية-cisco لمجموعة sdmlab.بمجرد تحديد الموجه الذي تريد تكوينه، يعرض شريط المسار الموجود في أعلى صفحة التكوين النطاق الحالي للتكوين. على سبيل المثال، النطاق لهذا المثال هو *global > sdmlab > cisco*. *cisco* هو كائن التكوين الحالي (أي الموجه الذي تم تحديده من محدد الكائن).
3. من شريط قائمة التكوين، انقر فوق **إعدادات**.تظهر صفحة



في الإعدادات.

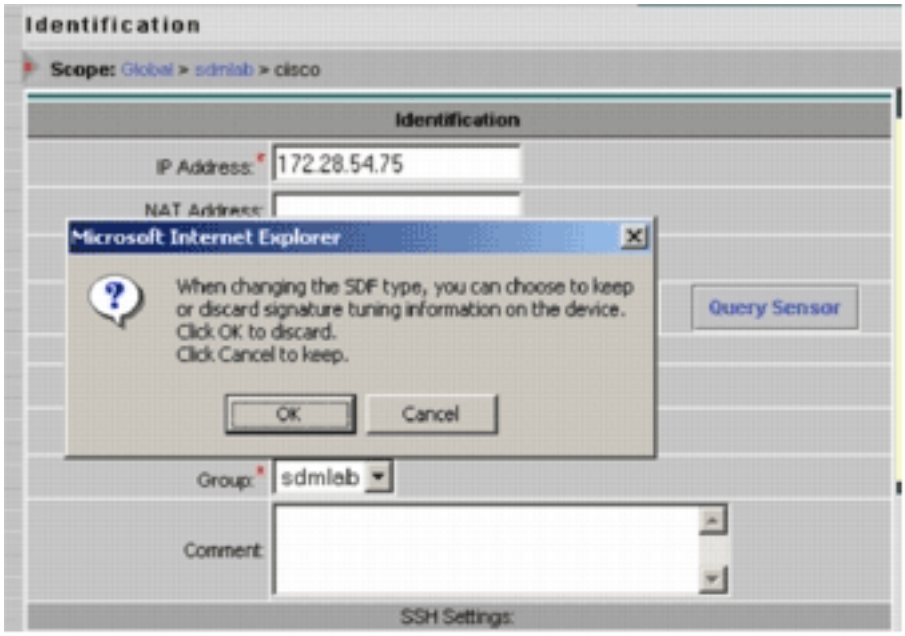
صفحة الإعدادات، يمكنك تغيير إعدادات التكوين للكائن المحدد. توجد إعدادات التكوين الخاصة بموجهات Cisco IOS IPS في قسم جدول المحتويات الموجود على الجانب الأيسر من الصفحة. فيما يلي قائمة بالمهام المتوفرة تحت قسم مركز العمليات التكتيكية:*التعريف*—المعلومات الأساسية لموجه Cisco IOS IPS؛ يمكنك تحديد ملف SDF تم ضبطه مسبقا هنا*التوقيع*—توقيعات موجه IPS من Cisco IOS*معالج التوقيع*- معالج توقيع لإضافة توقيعات مخصصة*قواعد Cisco IOS IPS*—لتكوين قواعد Cisco IOS IPS التي يتم إستخدامها للتطبيق على الواجهات*عوامل تصفية Cisco IOS IPS* — عوامل تصفية Cisco IOS IPS*إعادة تجميع Cisco IOS IPS*—تكوين إعادة التجميع الظاهري لبروتوكول الإنترنت (IP) للواجهة*خصائص CISCO IOS IPS SDEE*—لتكوين إعدادات SDEE*الخصائص العامة لنظام منع التسلل* (IPS) *من Cisco IOS*—التكوينات الإضافية المتعلقة بنظام منع التسلل (IPS) من Cisco IOS

4. أخترت **تعريف** in order to شكلت سابق تشكيل مبرد يحول.سوف تظهر صفحة



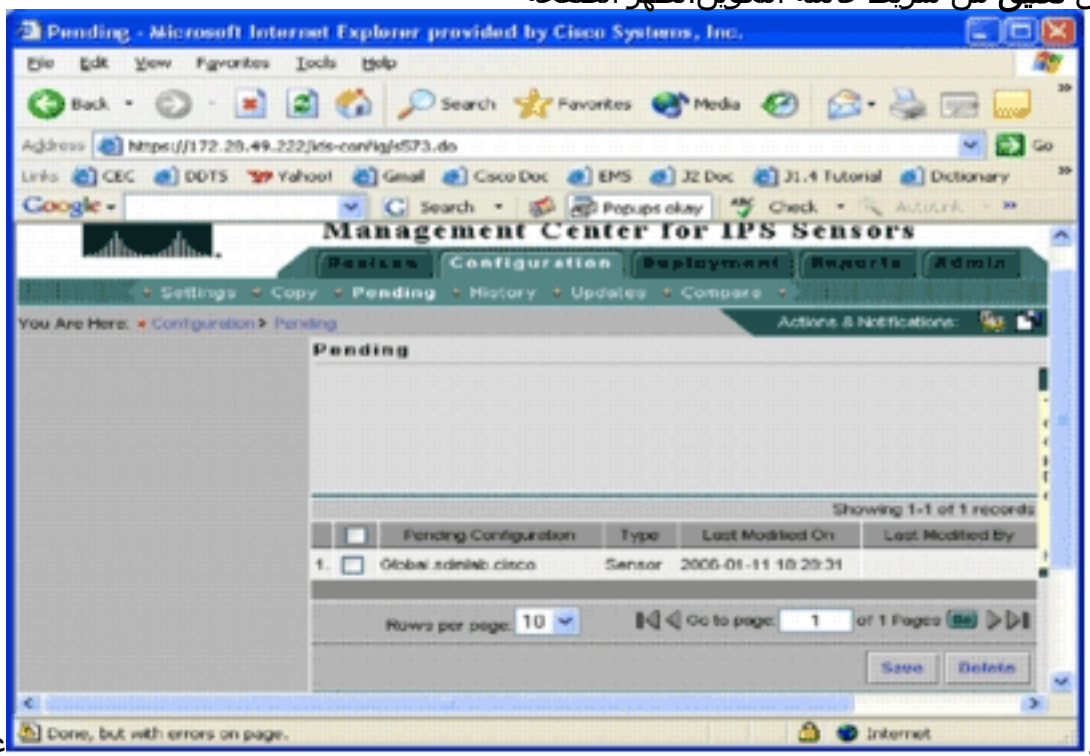
التعريف.

5. من القائمة المنسدلة نوع SDF، أختر SDF المناسب الذي تم ضبطه مسبقا، ثم انقر فوق **تطبيق** لتطبيق التغييرات.يدعم نظام منع التسلل (IPS) IOS من Cisco أكثر من 1600 توقيع، وهو ما يتجاوز سعة ذاكرة الموجهات التي يمكن قبولها. وقد تم تطوير قوات الدفاع الذاتى كطريقة ملائمة لاختيار وتحميل أكثر التوقيعات اهمية. حاليا، يمكنك الاختيار من بين ثلاثة SDFs. وهي تختلف في الحجم لتمكينك من تحديد ملف SDF وفقا لسعة DRAM الخاصة بالموجهات لديك. والخيارات المتاحة موصوفة هنا:UNSET — لم يتم تعيين نوع SDF.إسقاط الهجوم — تستخدم أداة SDF هذه كموجه مع ذاكرة DRAM سعة 64 ميجابايت.256 ميجابايت—هذه هي وحدات التحكم من Dell (المعروفة إختصارا باسم SDF) للموجهات التي تحتوي على ذاكرة DRAM سعة 256 ميجابايت.128 ميجابايت—هذه هي وحدات SDF للموجهات التي تحتوي على ذاكرة DRAM سعة 128 ميجابايت.**ملاحظة:** تتطلب وحدات الدفاع عن الذات بسعة 128 و 256 ميجابايت توفر محرك 2.001 أو أكثر. تتوفر هذه المعلومات في حقل **الإعدادات > واجهة مستخدم التعريف > الإصدار.تحذير:** لا تتضمن وحدة التحكم في إدارة الذاكرة (IPS) وظائف إدارة الذاكرة لموجهات Cisco IOS IPS. كن حذرا عند تحديد ملفات SDF لموجه Cisco IOS IPS. تأكد من أن موجه Cisco IOS IPS يحتوي على ذاكرة كافية لتشغيل ملف SDF المحدد.**ملاحظة:** عند تغيير نوع SDF، قد تتلقى هذه الرسالة: *عند تغيير نوع SDF، يمكنك إختيار الاحتفاظ بمعلومات توليف التوقيع على الجهاز أو تجاهلها. انقر موافق للتجاهل. انقر فوق "إلغاء الأمر"*



للاحتفاظ به.

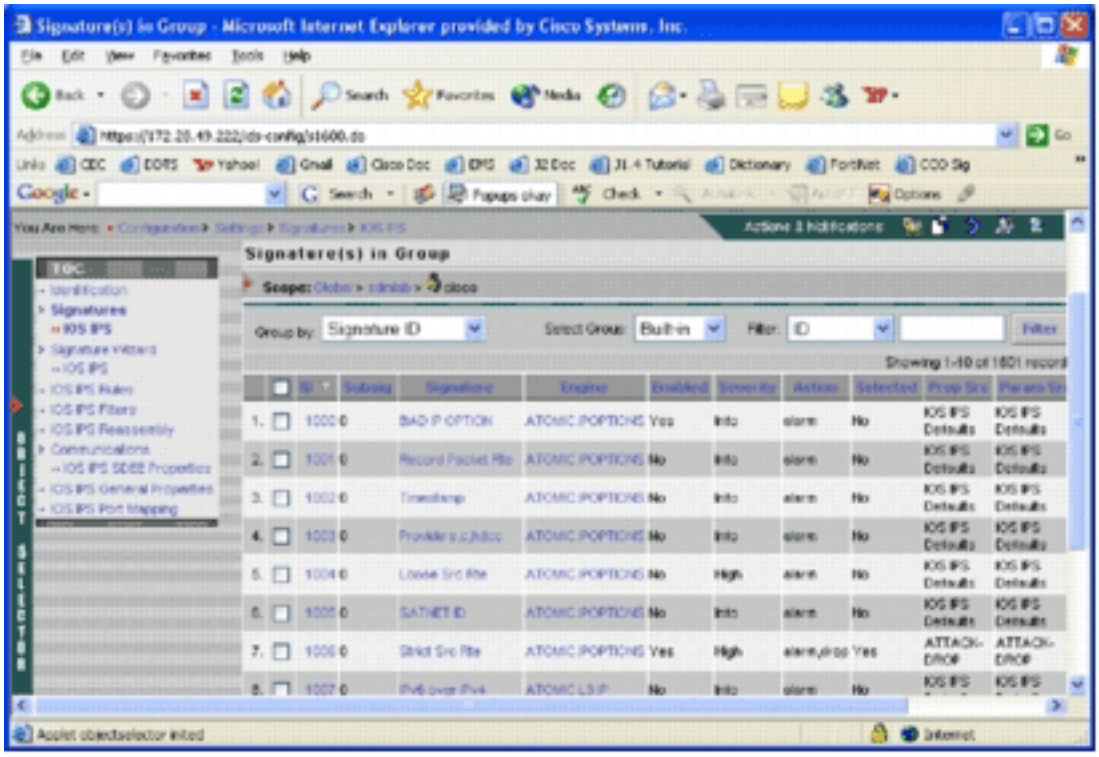
6. انقر فوق **إلغاء الأمر** للإبقاء على معلومات توليف توقيعك.الآن بعد أن أخترت بنجاح SDF تم ضبطه مسبقا للموجه-cisco، يمكنك تنفيذ توليف توقيع إضافي مثل إضافة أو تحرير، أو حتى إنشاء توقعاتك الخاصة، أو يمكنك تخطي مهام توليف التوقيع والتوجه مباشرة إلى إنشاء قاعدة لتطبيقها على الواجهة (الواجهات).
7. انقر فوق **تعليق** من شريط قائمة التكوين.تظهر الصفحة



المعلقة. عند هذه النقطة، يتم إكمال مهمة التكوين. ومع ذلك، يجب عليك إكمال مهمة النشر لنشر التغييرات التي أجريتها على الجهاز الهدف.

تعديل توقيعات SDF المضبوطة مسبقا

بعد تحديد ملف SDF تم ضبطه مسبقا للموجه، يمكنك تنفيذ مهام إضافية لتوليف التوقيع. يمكنك إضافة، تحرير، حذف، وتعديل التوقيعات لتلائم إحتياجاتك بشكل أفضل، أو يمكنك إنشاء توقعاتك الخاصة عند الضرورة. يستخدم هذا المثال وحدة التحكم في إدارة اللوحة الأساسية (IPS) لإضافة توقيعات إضافية وتعديل العمليات. تعرض هذه الصورة واجهة تكوين التوقيع.



يمكنك إستخدام تكوين التوقيع لتمكين أو تعطيل، تحديد أو إلغاء تحديد، إضافة توقيع، حذف توقيع، تغيير إجراءات التوقيع، وتحرير معلمات التوقيع. أستخدم معالج التوقيع الموجود على اليسار لإنشاء توقيعات مخصصة.

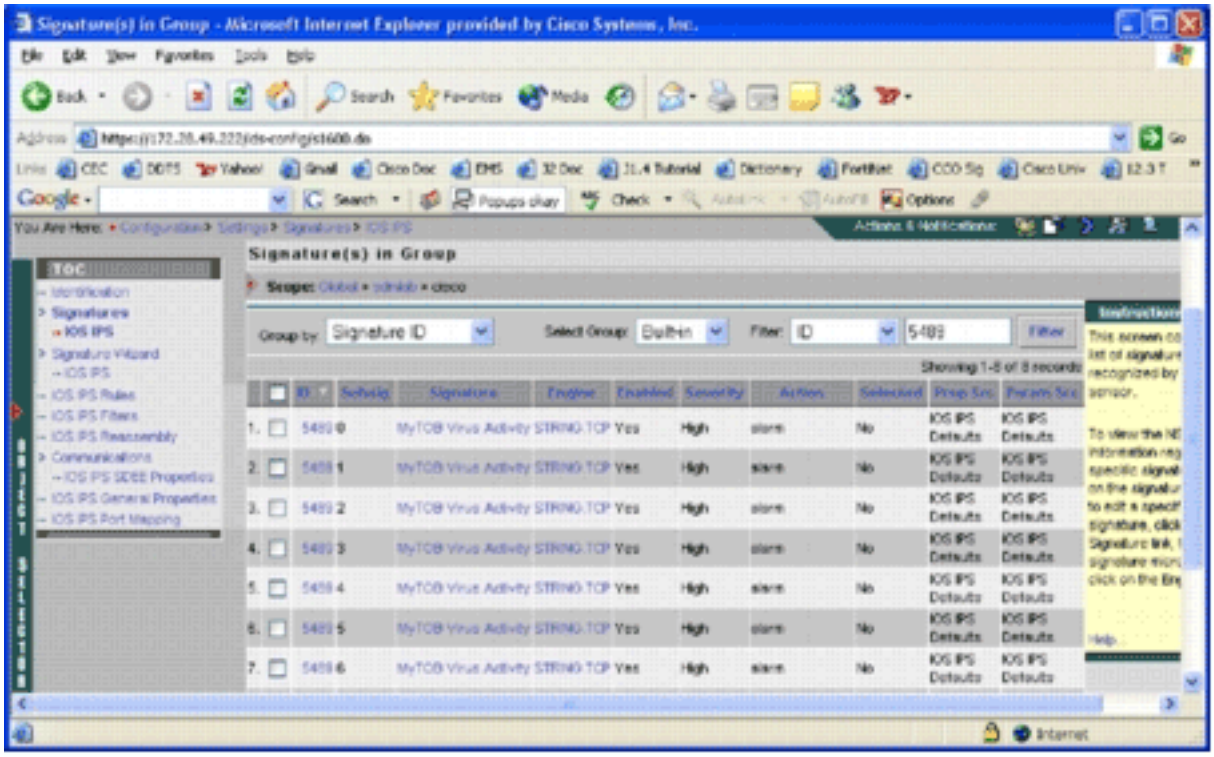
في واجهة مستخدم تكوين التوقيع، يتم عرض بعض المعلومات بشكل افتراضي. يشير المحدد إلى ما إذا كان التوقيع سيتم تضمينه في ملف SDF الذي تم إرساله إلى الموجه. إذا لم يتم تحديد توقيع، فلن تتم إضافته. يمكن تطبيق فقط إذا كان التوقيع محددا. عندما يتم تعطيل توقيع، لن ترسل محركات IPS أحداث لهذا التوقيع المحدد. إذا كان التوقيع غير محدد، فإنه يكون أيضا معطلا تلقائيا.

يخبرك العمودان الأخيران (Prop Src و Param Src) من أين يأتي التوقيع ومعلمته، على التوالي. يمكن أن يكون التوقيع قد تم أخذه من ملفات SDF التي تم ضبطها مسبقا أو من إعدادات المصنع الافتراضية التي يمكنك العثور عليها في تحديثات ملف IOS-SXXX.zip (يتم عرضه كإعدادات IOS IPS الافتراضية). تنطبق هذه القيم أيضا على عمود المعلمة.

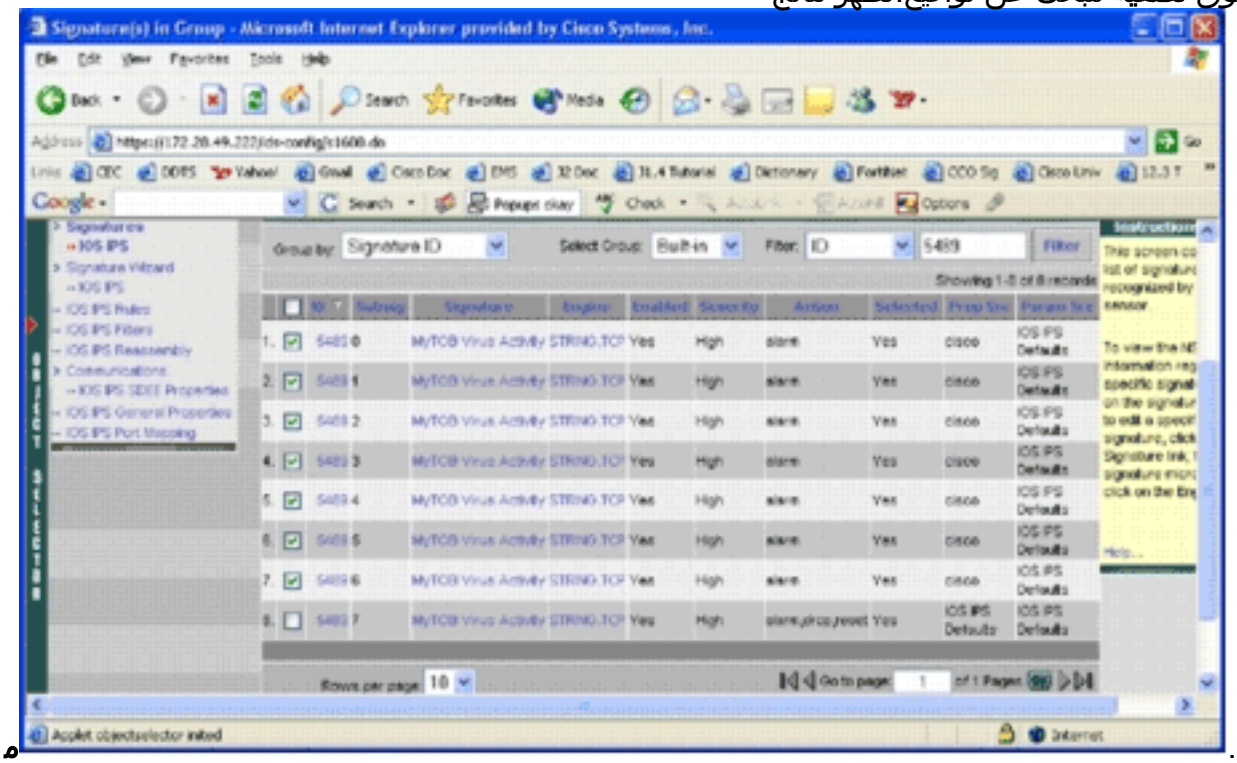
بينما تقوم بإضافة تواقيع إلى موجهات Cisco IOS IPS، يجب حساب اعتبارات الذاكرة. إذا قمت بإضافة المزيد من التوقيعات التي لا يمكن لموجه Cisco IOS IPS معالجتها، فسيفشل IPS MC في نشر تغييرات التكوين على الأجهزة.

أكمل الخطوات التالية لإضافة التوقيعات x/5489 إلى موجه IPS من Cisco IOS:

1. حدد **التكوين**، ثم أستخدم أداة تحديد الكائن لتحديد موجه Cisco IOS IPS الذي تريد تكوين توقيعات IPS له.
2. أختر **التكوين > الإعدادات > التوقيعات > IOS IPS**.يظهر التوقيع (التوقيعات) في صفحة المجموعة.



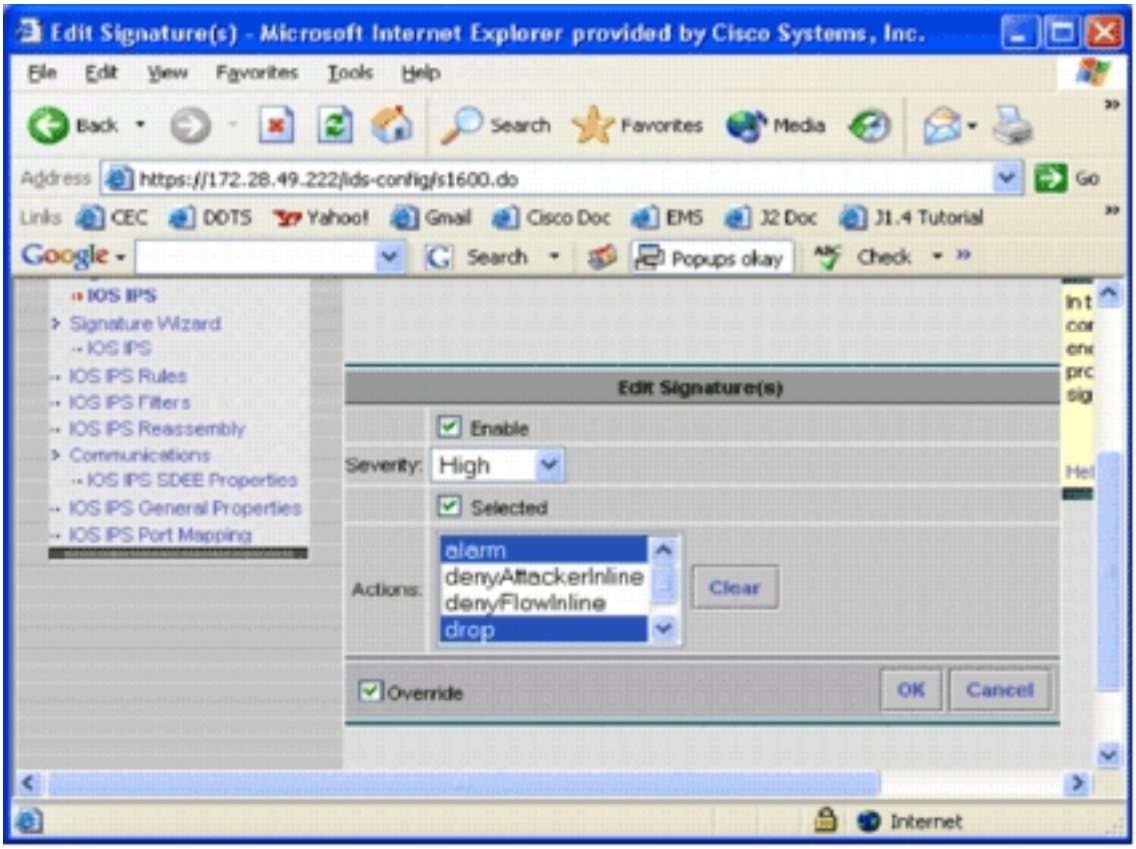
3. في قائمة التوقيع التي تنتج، حدد مرشح حسب المعرف، واكتب معرف التوقيع 5489.
4. انقر فوق **تصفية** للبحث عن تواقيع.تظهر نتائج



البحث.

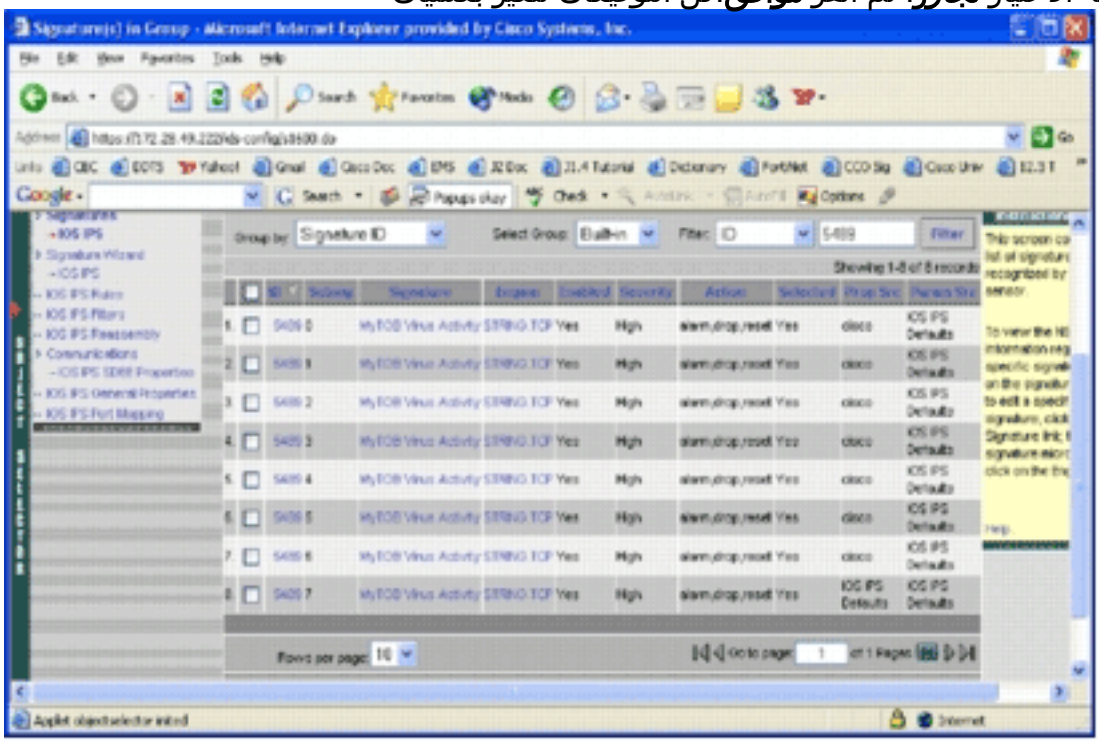
ملاحظة: لا تدعم وحدة التحكم في الإدارة (MC) ل IPS التصنيف الجديد المتاح في إدارة قاعدة بيانات المحول (SDM) من Cisco.

5. حدد خانة الاختيار المجاورة للتواقيع التي لم يتم تحديدها، وانقر **تحديد** في شريط الأدوات السفلي.
6. انقر فوق **تحرير** لتغيير إجراءات التوقيع.تظهر صفحة تحرير التوقيع



(التوقيعات).

7. حدد خانة الاختيار **المحددة**، وحدد **تنبيه**، و**إسقاط**، و**إعادة ضبط** من قائمة الإجراءات.
8. حدد خانة الاختيار **تجاوز**، ثم انقر **موافق**.كل التوقيعات تتغير بعمليات



مرغوبة.

9. انتقل إلى المهمة المعلقة وقم بحفظ كافة التغييرات. يؤدي هذا إلى اكتمال مهمة التكوين.**تلميح:** انتبه جيدا لعمود Prop Src. بعد التعديل، تغير المصدر إلى الجهاز المسمى *cisco*، مما يعني أن جميع معلومات التوليف يتم حفظها بشكل منفصل عن ملفات SDF الافتراضية التي تم ضبطها مسبقا. تمنح هذه الآلية IPS MC القدرة على الاحتفاظ بتغييرات التوقيع المخصصة.

في القسم السابق عند تغيير أنواع ملفات SDF، سألك IPS MC ما إذا كنت تريد الاحتفاظ بمعلومات توليف التوقيع. هذه هي معلومات توليف التوقيع المشار إليها.

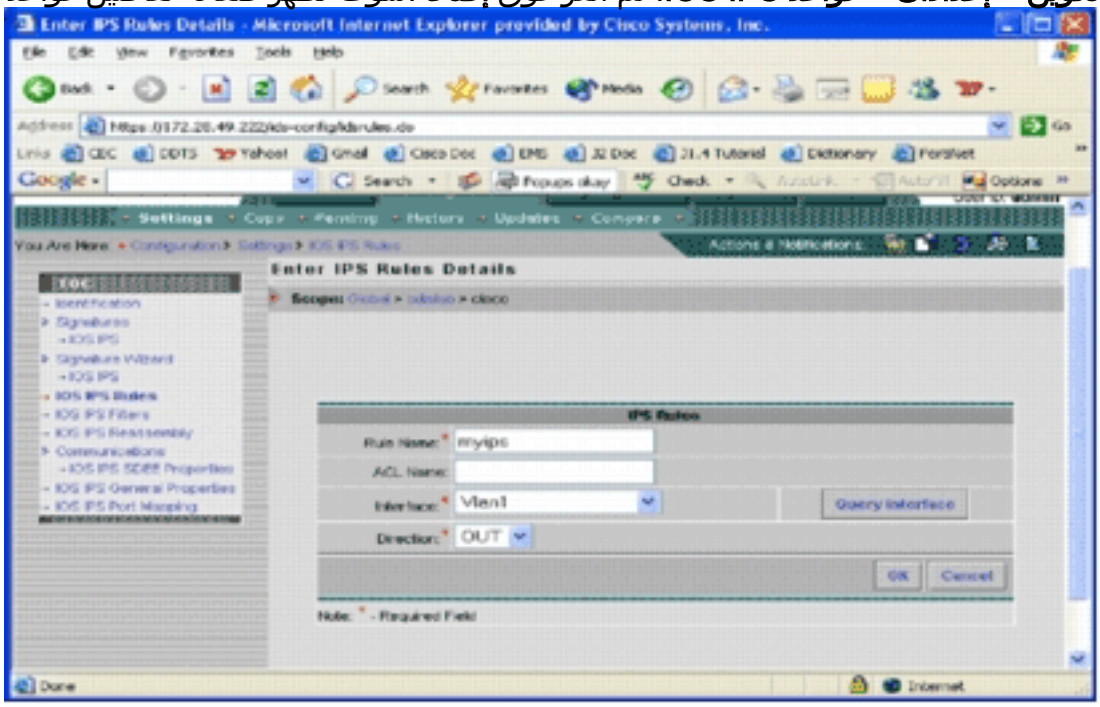
إختبار توقيعات مخصصة

إذا كنت لا ترغب في إستخدام ملفات SDF الافتراضية التي تم ضبطها مسبقا، يمكنك إستخدام الخطوات المحددة في القسم تعديل توقيعات SDF التي تم ضبطها مسبقا لتحديد ضبط التوقيعات الخاصة بأجهزتك. في صفحة التعريف، تحتاج إلى التأكد من عدم تعيين نوع SDF. ارجع إلى الخطوة 3 في تكوين موجه Cisco IOS IPS لاستخدام ملفات التوقيع التي تم ضبطها مسبقا.

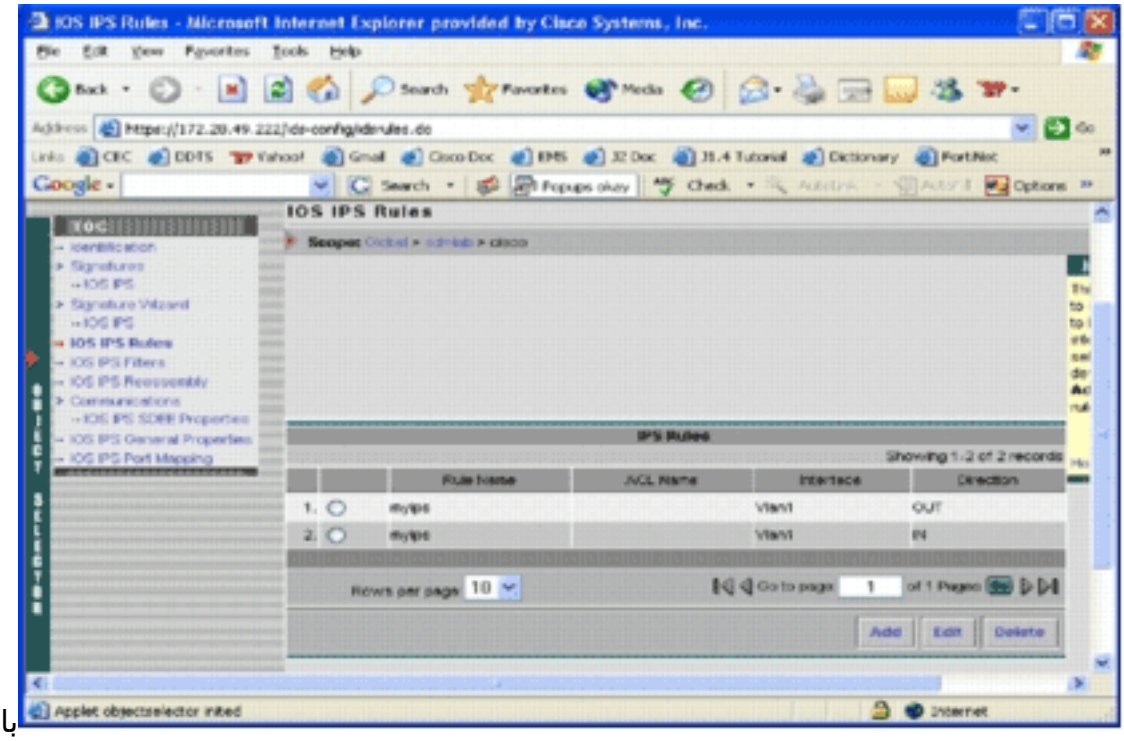
إنشاء قاعدة لتطبيقها على الواجهة (الواجهات)

بعد ضبط التوقيع، يلزمك تمكين IPS على موجهات Cisco IOS. لتمكين IPS على الموجه، يجب عليك إنشاء قاعدة IPS وتطبيقها على واجهة واحدة على الأقل.

1. حدد **التكوين**، ثم أستخدم أداة تحديد الكائن لتحديد موجه Cisco IOS IPS الذي تريد تكوينه. تحقق في شريط المسار من أن النطاق الخاص بك موجود على مستوى الجهاز، وليس على مستوى المجموعة.
2. حدد **تكوين > إعدادات > قواعد IOS IPS**، ثم انقر فوق **إضافة**.سوف تظهر صفحة تفاصيل قواعد Enter IPS.



3. قم بإدخال معلومات لاسم القاعدة والواجهة التي تريد تطبيق القاعدة والاتجاه عليها.
4. وانقر فوق **OK**.تظهر صفحة قواعد IOS



بالمثل، IPS.

يمكنك إنشاء قواعد لكلا الاتجاهين لواجهة.

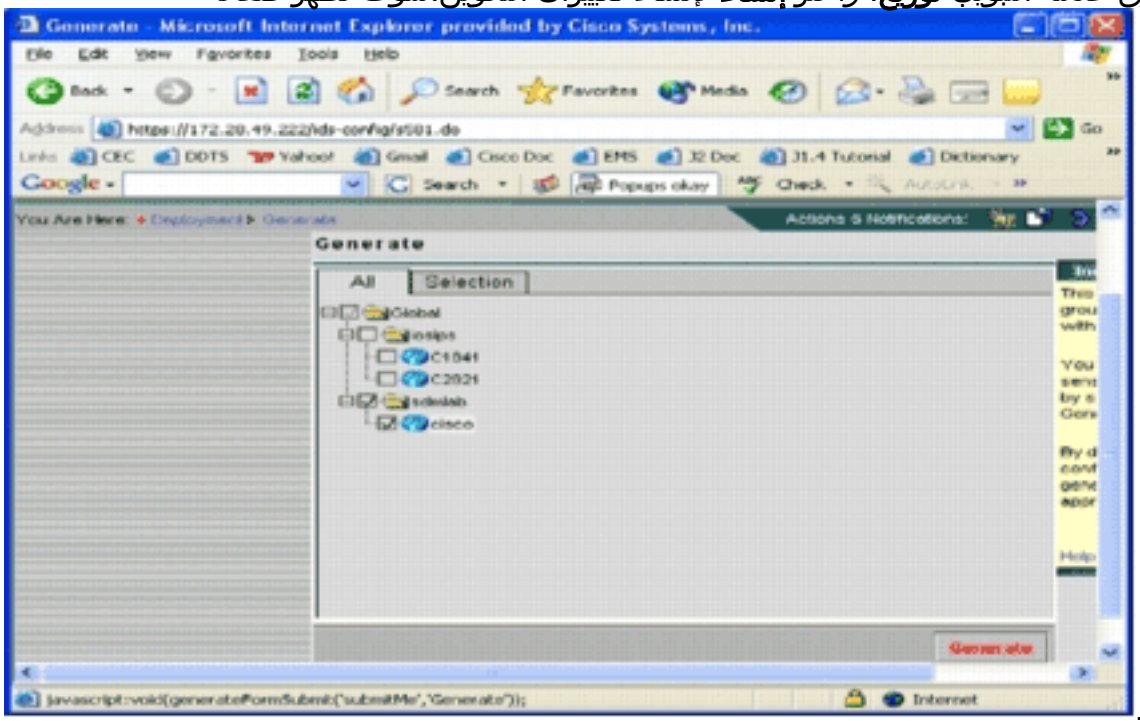
5. يجب حفظ تغييرات التكوين والانتقال خلال عملية النشر لتقديم التغييرات إلى الجهاز أو مجموعة الأجهزة المتأثرة.يمكنك تنفيذ التكوينات الأخرى المتعلقة ب IPS أيضا، ولكن جميع المهام الأخرى إختيارية وغير مطلوبة. أنت يستطيع وجدت all the خيار إلى يسار التشكيل مستعمل قارن. لا يغطي هذا المستند خيارات التكوين الاختيارية.

نشر التكوين

بعد إجراء جميع تغييرات التكوين، يجب إستخدام مهمة النشر لتنفيذ التغييرات على الأجهزة. يتم حفظ جميع التكوينات التي قمت بها حتى الآن محليا على خادم IPS MC.

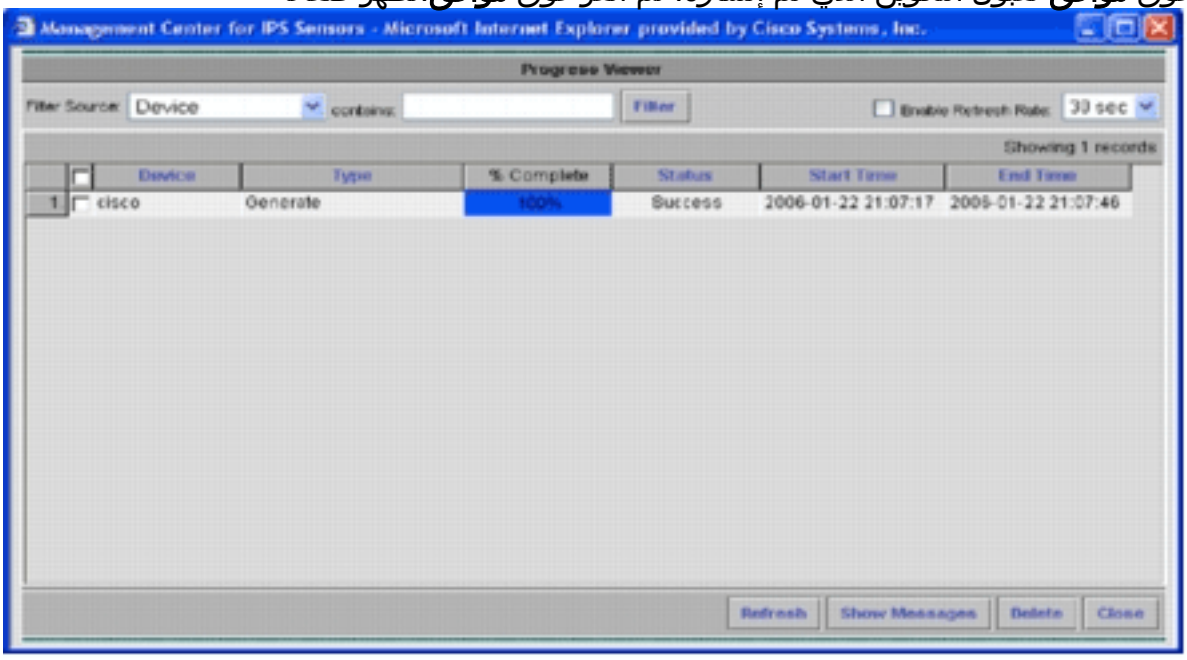
لنشر تغييرات التكوين، انتقل إلى صفحة النشر، ثم أكمل الخطوات التالية:

1. انقر فوق علامة التبويب **توزيع**، واختر **إنشاء** لإنشاء تغييرات التكوين.سوف تظهر صفحة



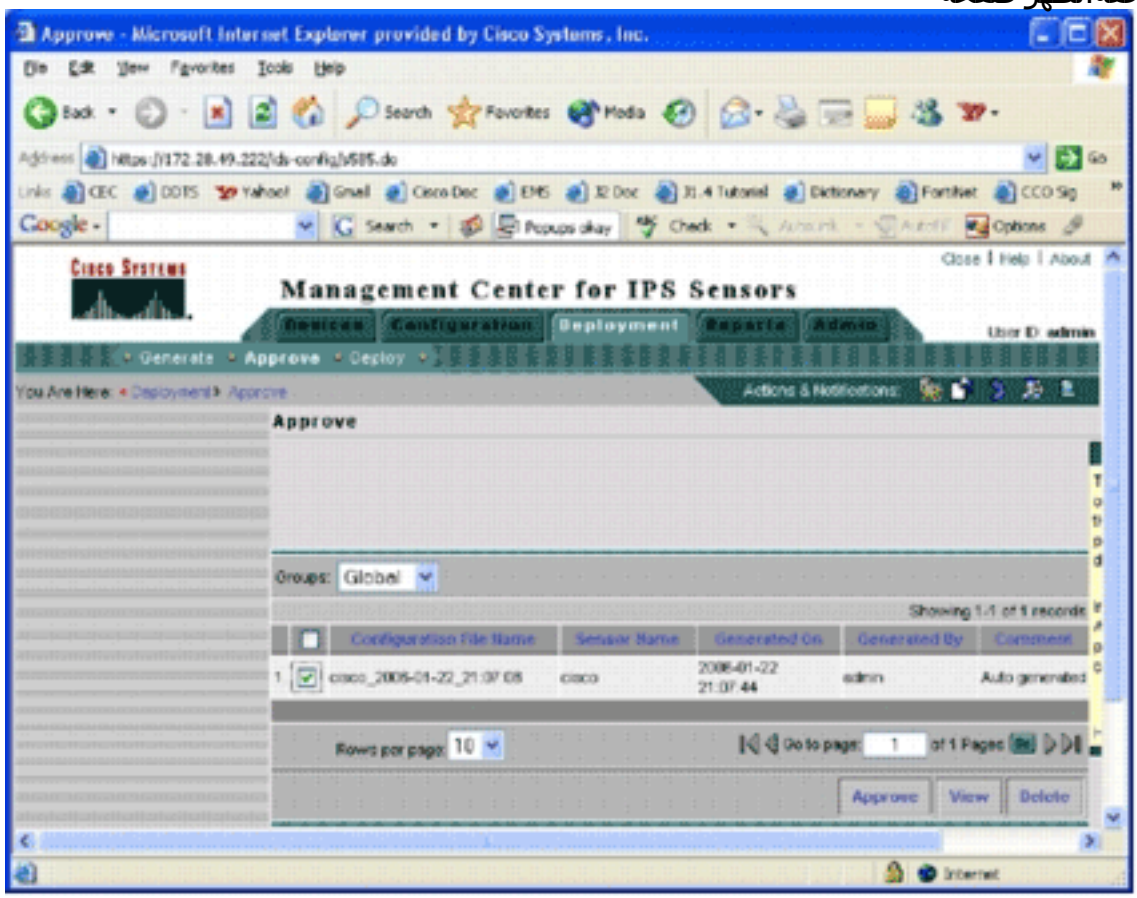
الإنشاء.

2. أختر *ال cisco* أداة أن أنت تشكل، وطقطقة **يلد**.
3. انقر فوق **موافق** لقبول التكوين الذي تم إنشاؤه، ثم انقر فوق **موافق**.تظهر صفحة



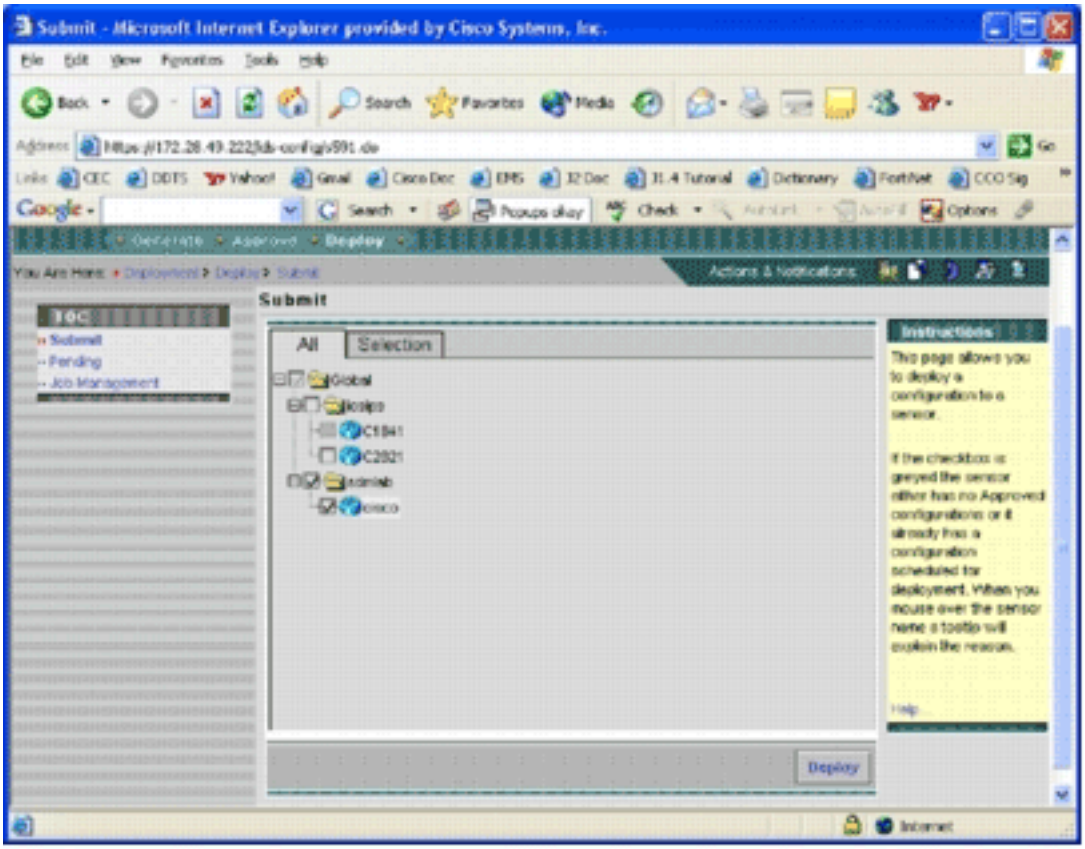
حالة.

4. انقر فوق **تحديث** حتى تكتمل مهمة الإنشاء بنجاح.
5. انقر فوق **الموافقة** الموجودة في شريط قائمة النشر ومجموعة sdmlab لعرض قائمة التكوينات التي تحتاج إلى الموافقة.تظهر صفحة



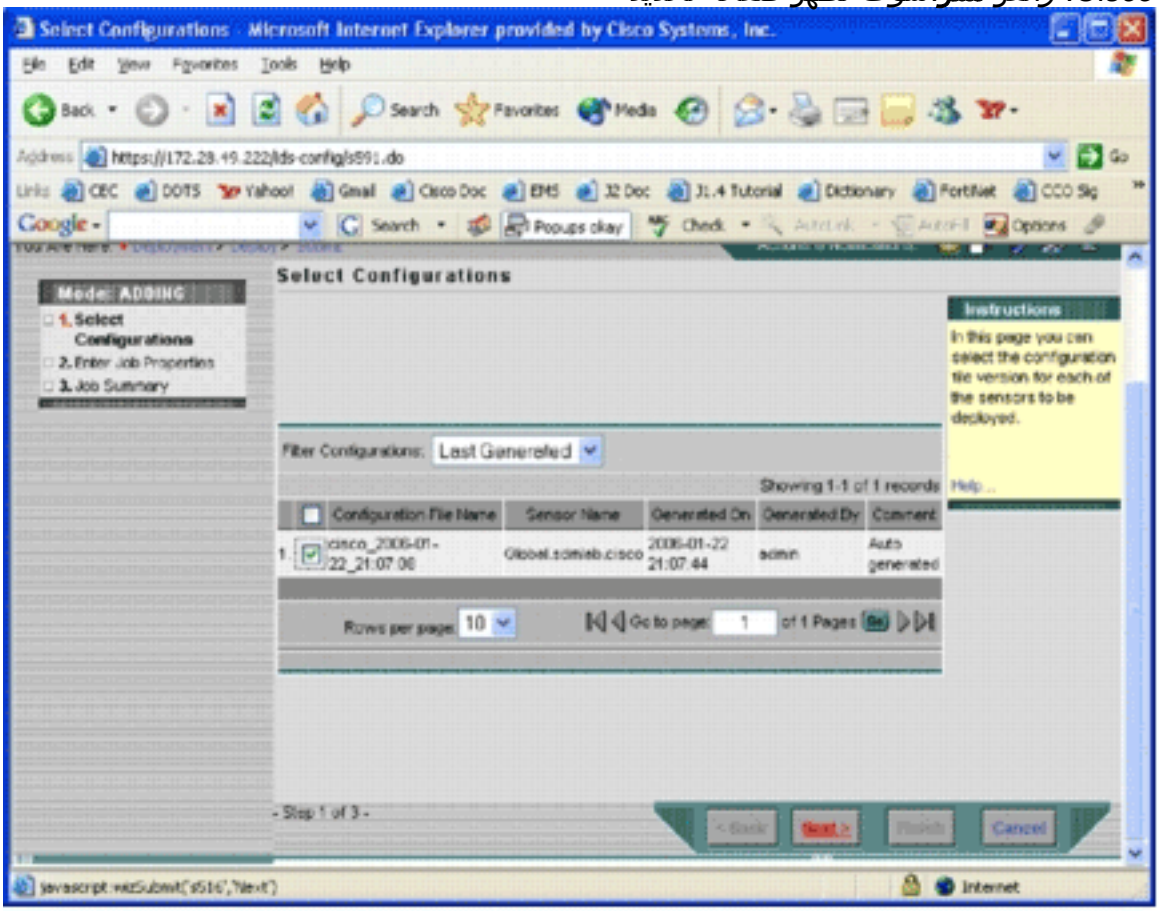
الموافقة.

6. أختر المهمة (المهام)، وانقر فوق **موافقة**.انقر فوق **توزيع** الموجود في شريط قائمة النشر، ثم انقر فوق **إرسال**.تظهر صفحة



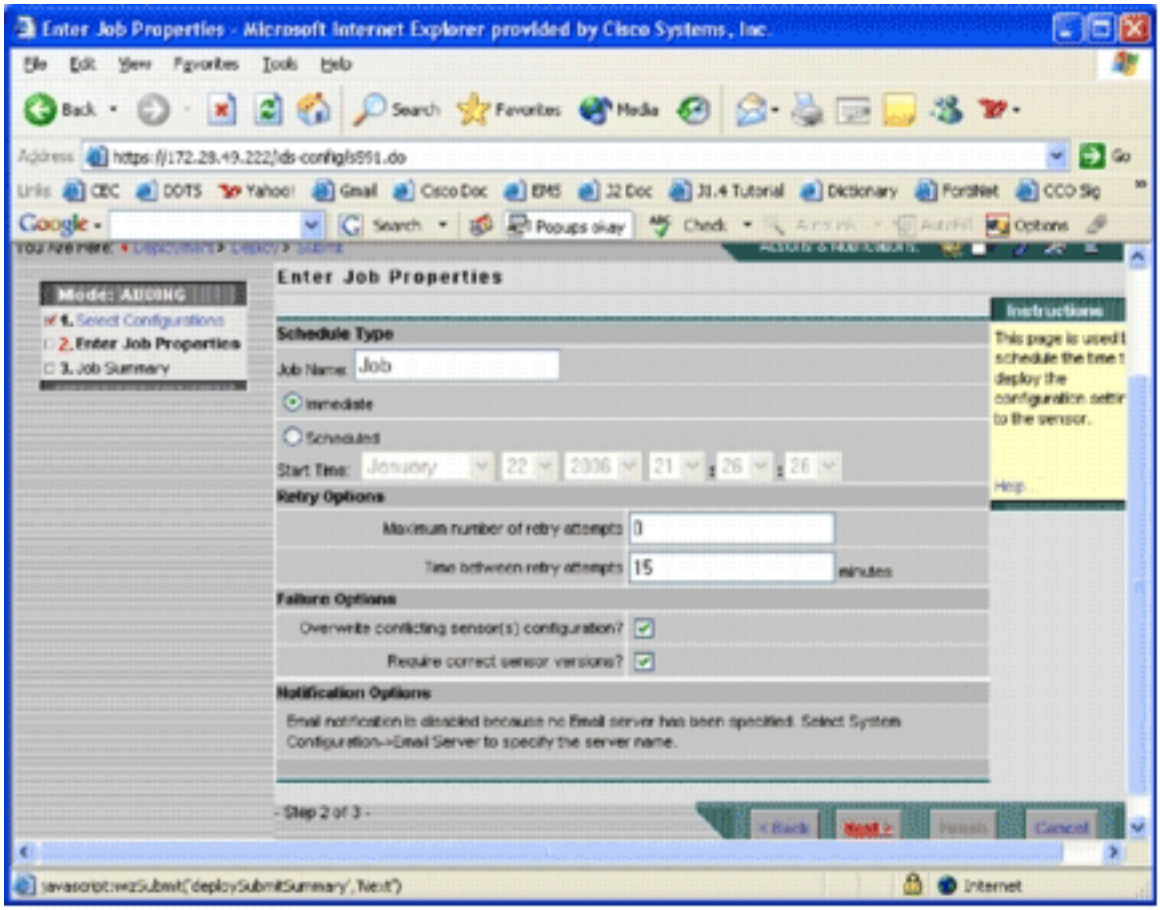
التسليم.

7. أختر الأجهزة التي تريد إرسال مهمة النشر لها.
8. حدد جهاز *Cisco*، وانقر **نشر**.سوف تظهر صفحة تحديد



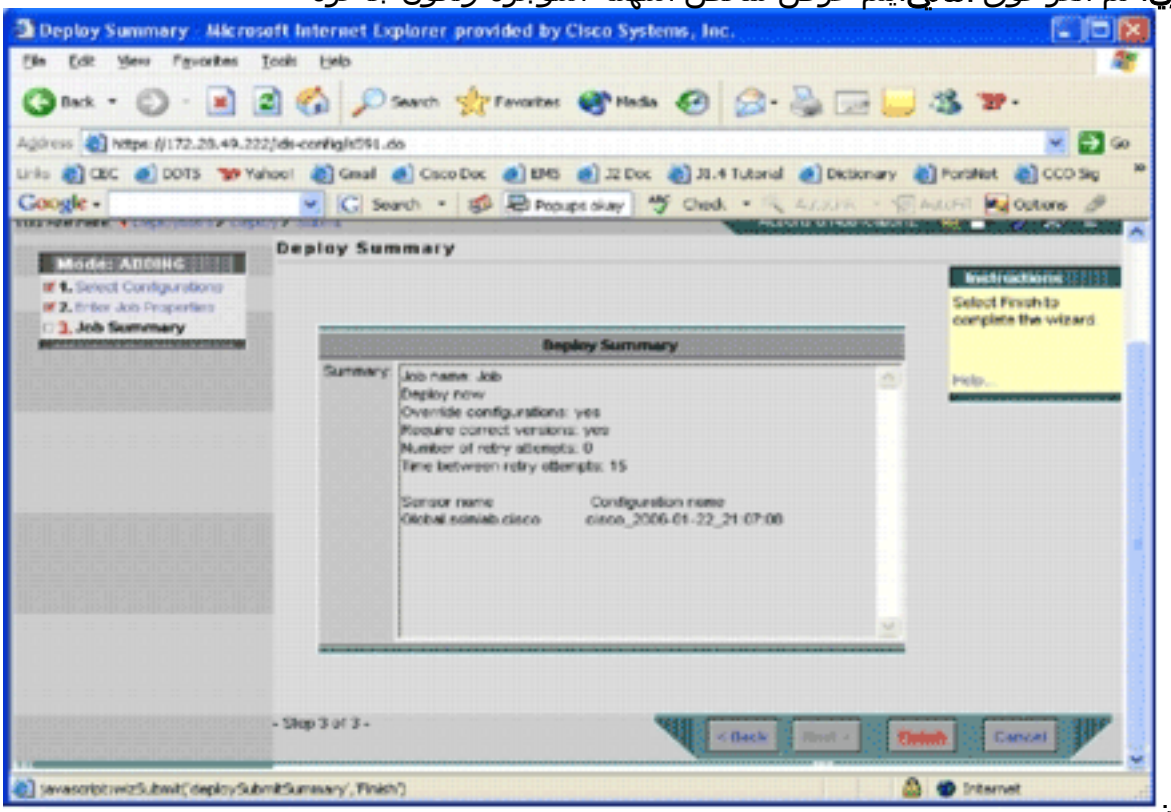
التكوينات.

9. أخترت التشكيل أنت فقط جعلت إلى *ال cisco* أداة، وطقطقة **بعد ذلك**.تظهر الصفحة إدخال خصائص



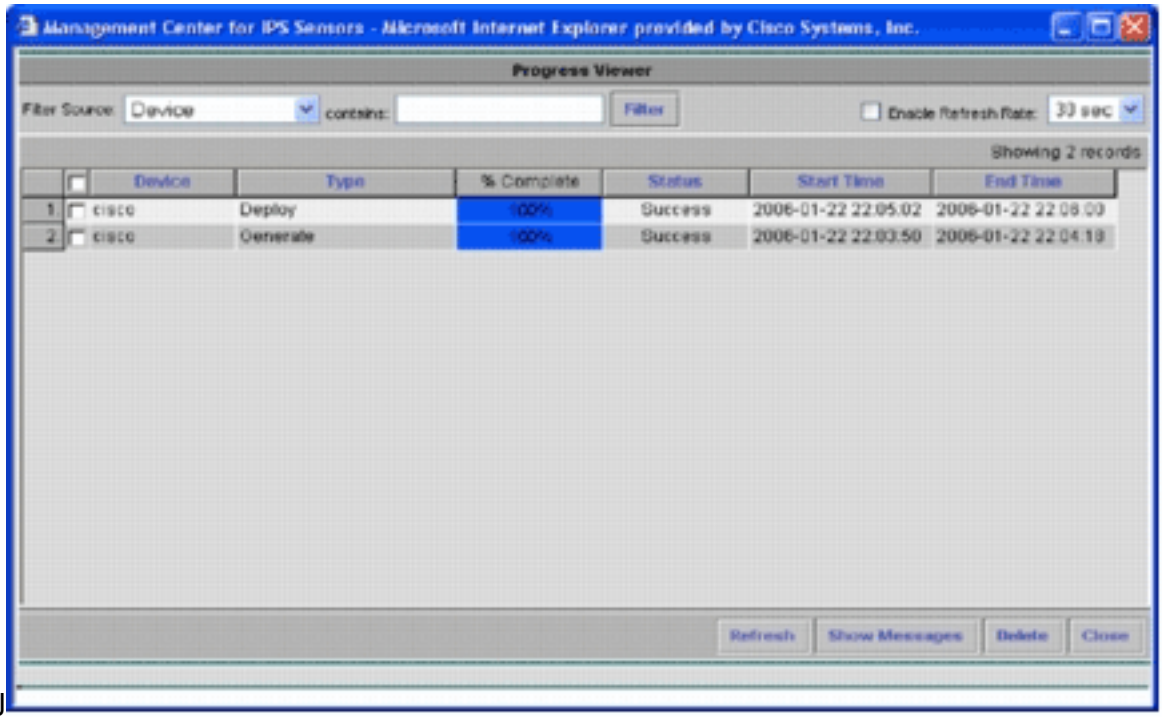
المهمة.

10. يمكنك إما نشر التغييرات مباشرة أو جدولة مهمة للقيام بذلك في وقت لاحق. في هذا المثال، أختر الخيار **الفوري**، ثم انقر فوق **التالي**.يتم عرض ملخص المهمة الموجزة وتكون جاهزة

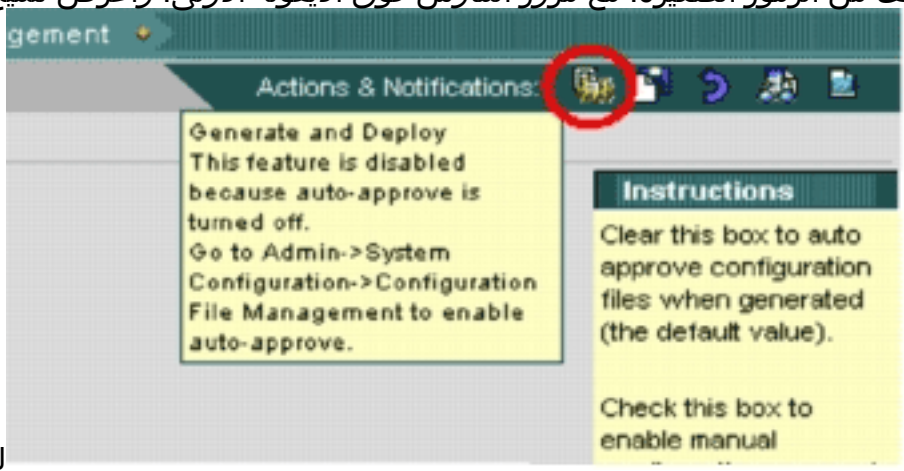


للنشر.

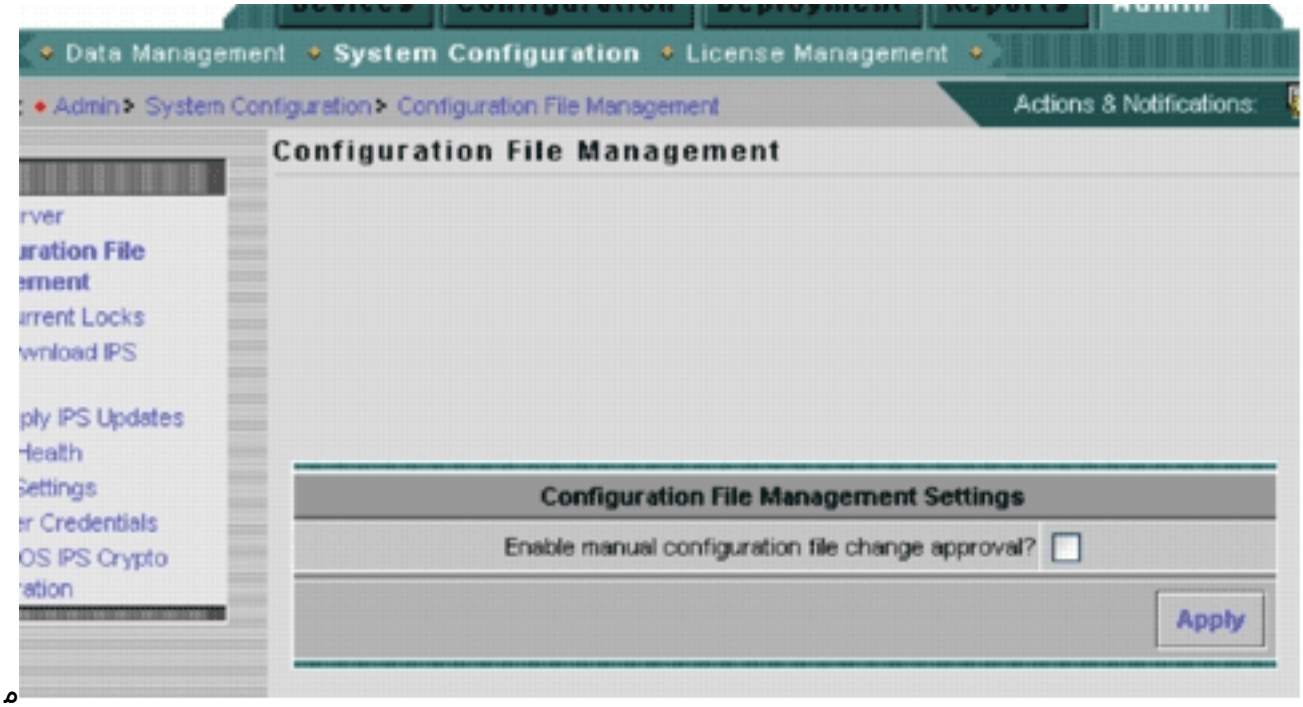
11. انقر فوق **إنهاء**.في نهاية النشر، يظهر مربع حوار حالة عملية



لقد قمت بنشر تكوينات Cisco IOS IPS بنجاح إلى الجهاز. عند تكوين أجهزة متعددة، يمكنك إجراء تغييرات التكوين على مستوى المجموعة ثم تطبيق التغييرات على جميع موجهات Cisco IOS IPS التي تنتمي إلى المجموعة نفسها.**تلميح:** هذه العملية طويلة، ولكن ميزة التسليم السريع متوفرة. عندما تستخدم هذه الميزة، لا يجب عليك المرور عبر عملية **إنشاء > اعتماد > نشر**. أتمت هذا steps in order to استعملت السمة:يوجد في أعلى واجهة المستخدم صف من الرموز الصغيرة. مع مرور الماوس فوق الأيقونة الأولى، وأعرض تلميح الأداة

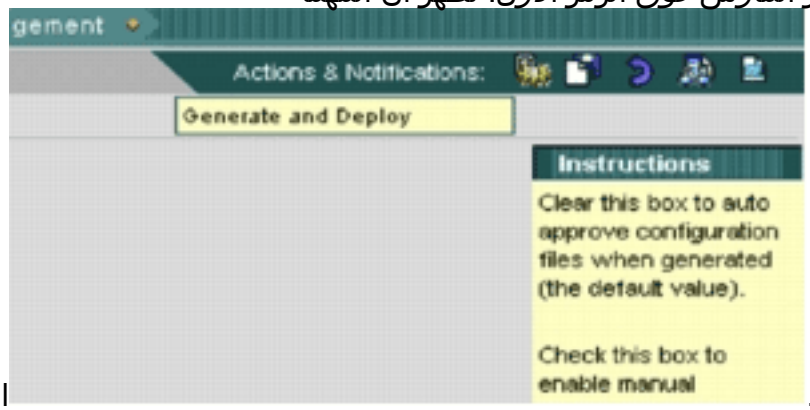


الظاهر في هذه الصورة: لتمكين مهمة "الإنشاء والنشر"، انتقل إلى **المسؤول > تكوين النظام > إدارة ملف التكوين**، وقم بإلغاء تحديد خانة الاختيار **تمكين الموافقة اليدوية على تغيير ملف التكوين**.



م

ع مرور الماوس فوق الرمز الأول، تظهر أن المهمة

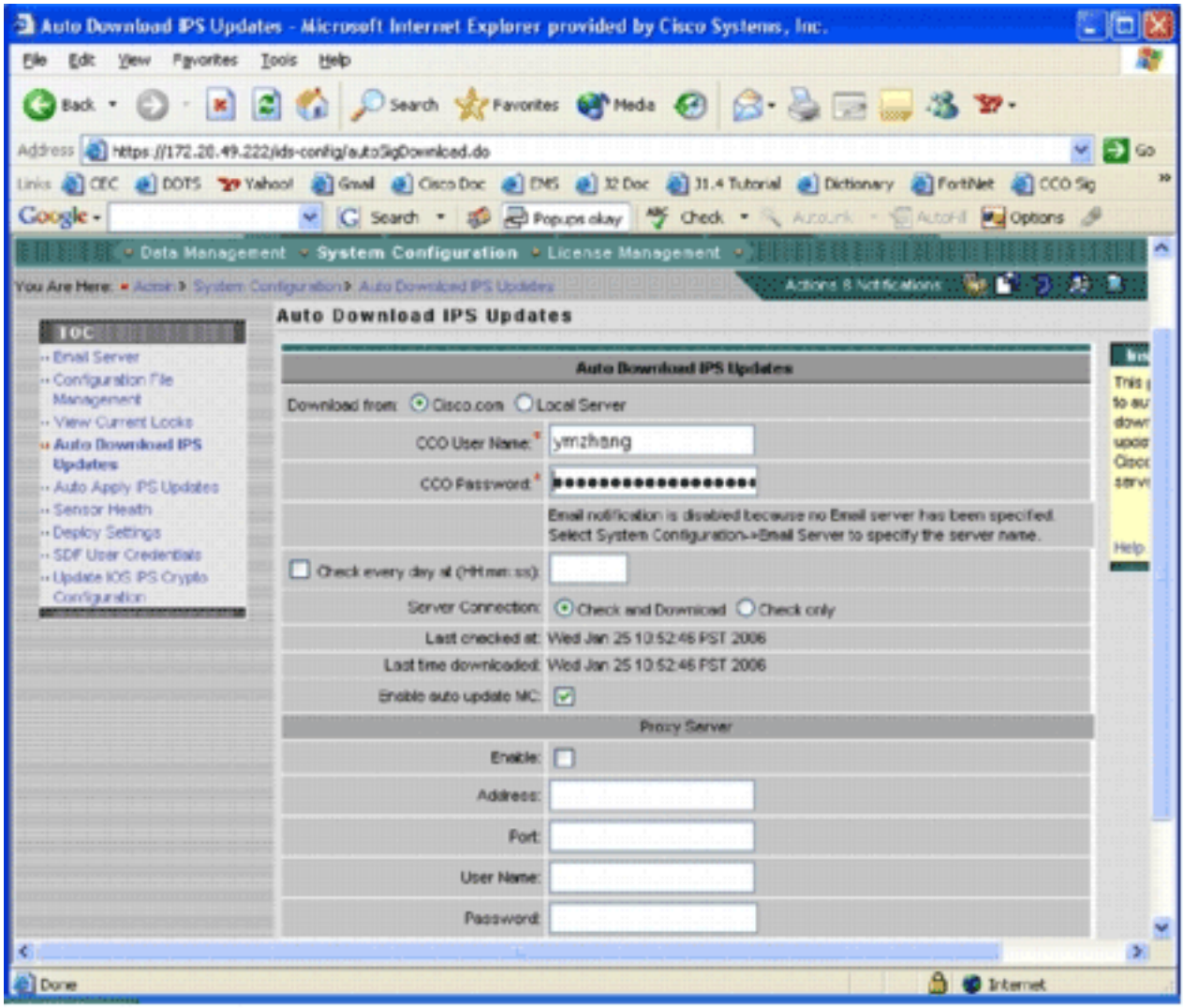


ممكنة. انقر فوق هذه الأيقونة.تعمل وحدة التحكم في الإنترنت (IPS) على إنشاء تغييرات التكوين ونشرها على الأجهزة تلقائيا.

التنزيل التلقائي لتحديثات التوقيع

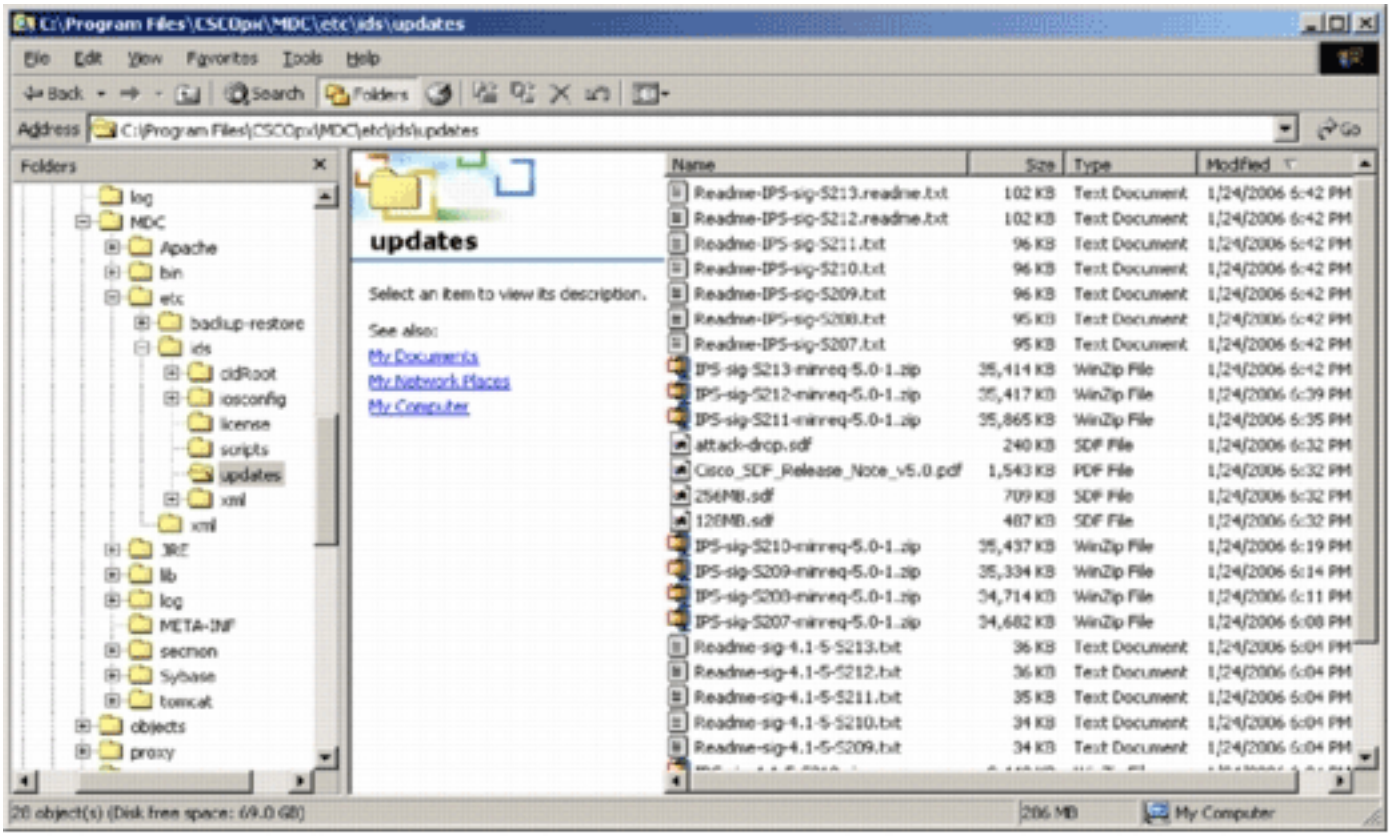
يدعم IPS MC تحديثات توقيع التنزيل التلقائي من Cisco.com. يمكنه تنزيل تحديثات التوقيع لأنظمة المستشعر، وكذلك لأنظمة Cisco IOS IPS الأساسية. لتكوين هذه الميزة، انتقل إلى **admin > تكوين النظام > التنزيل التلقائي لتحديثات IPS**.

تظهر صفحة التنزيل التلقائي لتحديث IPS.



يجب أن يكون لديك حساب Cisco.com صالح لتنزيل تحديث التوقيع هذا. للتحقق من الملفات التي تم تنزيلها تلقائيا، انتقل إلى الدليل الرئيسي لتثبيت IPS MC. في الوضع الافتراضي، يكون \program files\CSCOpx\MDC\etc\ids\updates.

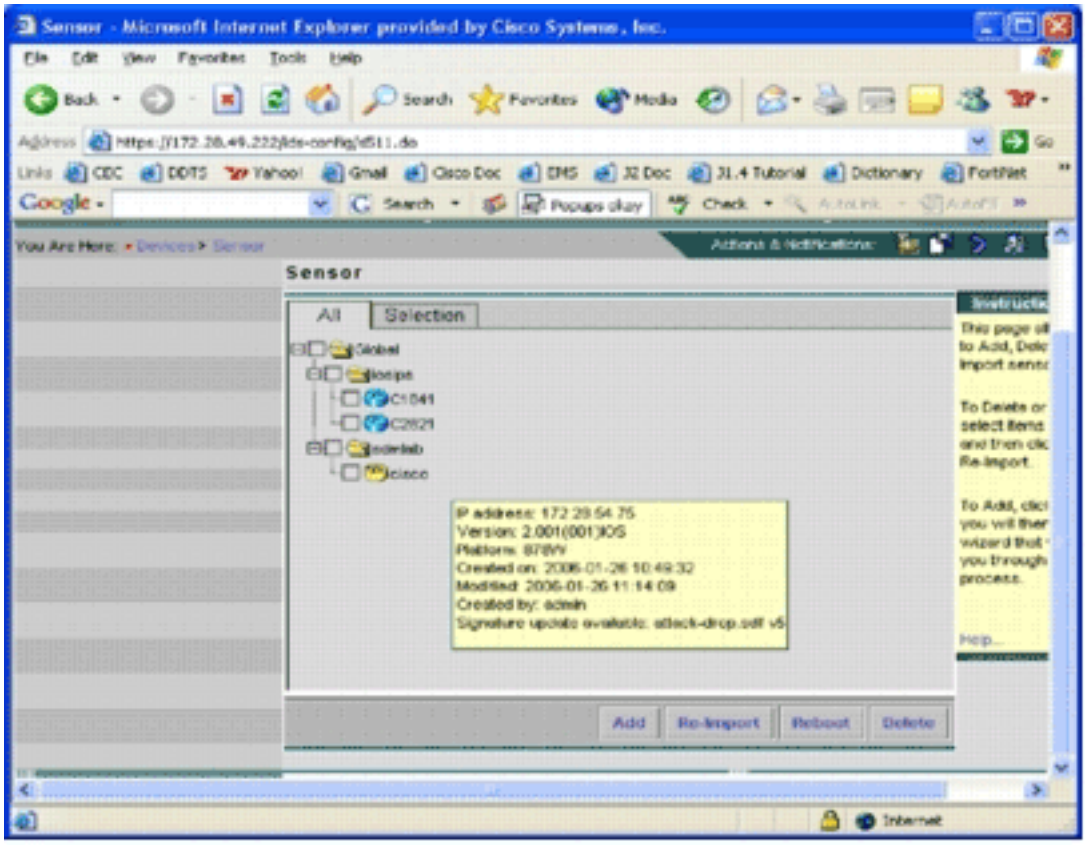
تعرض هذه الصورة صورة للملفات التي تم تنزيلها في هذا الدليل.



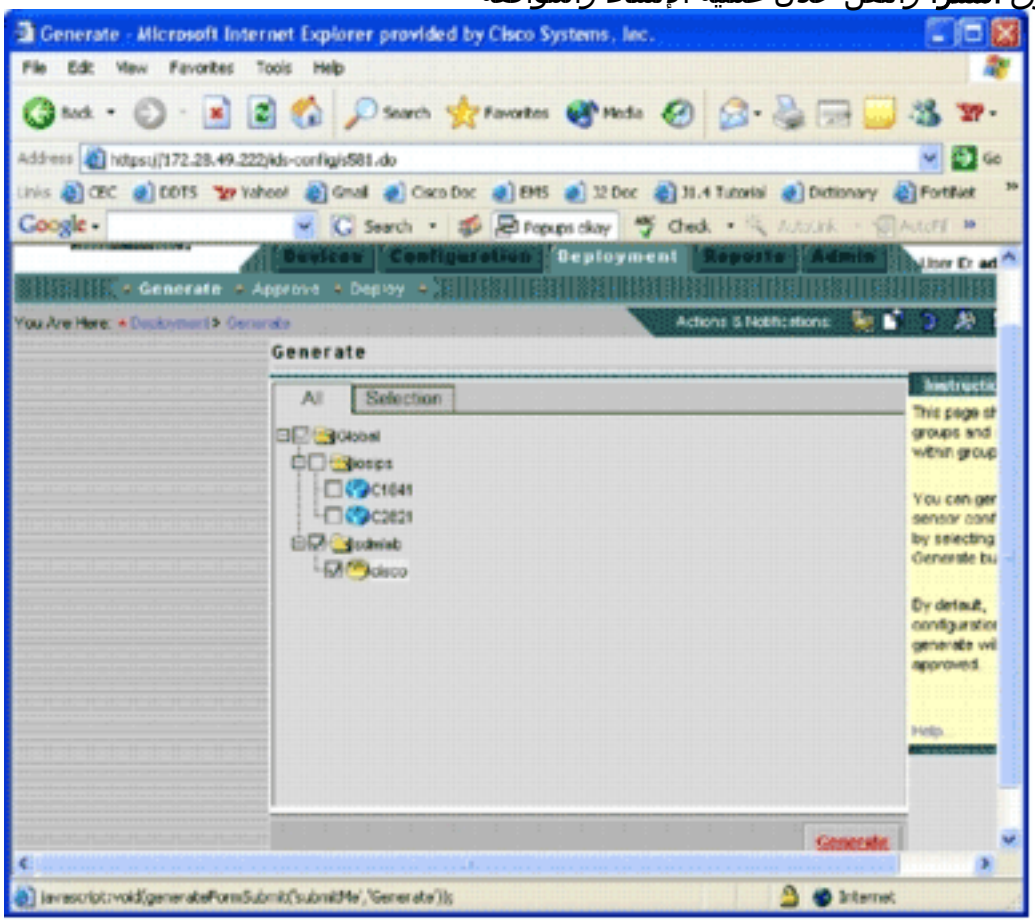
يمكنك أن ترى ملفات تحديث أداة الاستشعار تلك. يتم تنزيل ملف تحديث برنامج Cisco IOS Software وملفات SDF السابقة الضبط.

تحديث موجه Cisco IOS IPS بملفات SDF الجديدة

بالنسبة لموجهات Cisco IOS IPS التي تم نشرها مع ملفات SDF السابقة الضبط، بمجرد توفر إصدار جديد من ملفات SDF من خلال التنزيل التلقائي أو النسخ إلى دليل التحديثات، يتعرف وحدة التحكم الإدارية Cisco IPS على الإصدار الجديد. بعد تحديث واجهة المستخدم، تتحول رموز الأجهزة للأجهزة القابلة للتطبيق إلى اللون الأصفر.



1. انقر فوق **النشر**، وانتقل خلال عملية الإنشاء والموافقة



والنشر.

2. بعد النشر الناجح، يستخدم موجه Cisco IOS IPS إصدارا جديدا من ملفات SDF.

معلومات ذات صلة

- نظام Cisco لمنع الاقتحام

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).