تكوين حظر المعرفات باستخدام VMS IDS MC

المحتويات

المقدمة

يقدم هذا المستند عينة لتكوين نظام اكتشاف الاقتحام (IDS) من Cisco من خلال حل إدارة الأمان/الشبكة الخاصة الظاهرية (VPN)، وحدة تحكم إدارة نظام اكتشاف الاقتحام (IDS MC). في هذه الحالة، شكلت حجب من مستشعر IDS إلى موجه Cisco.

المتطلبات الأساسية

المتطلبات

قبل تكوين الحظر، تأكد من استيفاء هذه الشروط.

- يتم تركيب جهاز الاستشعار وتهيئته لاستشعار حركة المرور الضرورية.
- يتم تمديد واجهة sniffing إلى الموجه خارج الواجهة.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية.

- VMS 2.2 مع IDS MC ومراقبة الأمان 1.2.3
- مستشعر (Cisco IDS 4.1.3S(63
- موجه Cisco الذي يشغل برنامج Cisco IOS® الإصدار 12.3.5

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

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

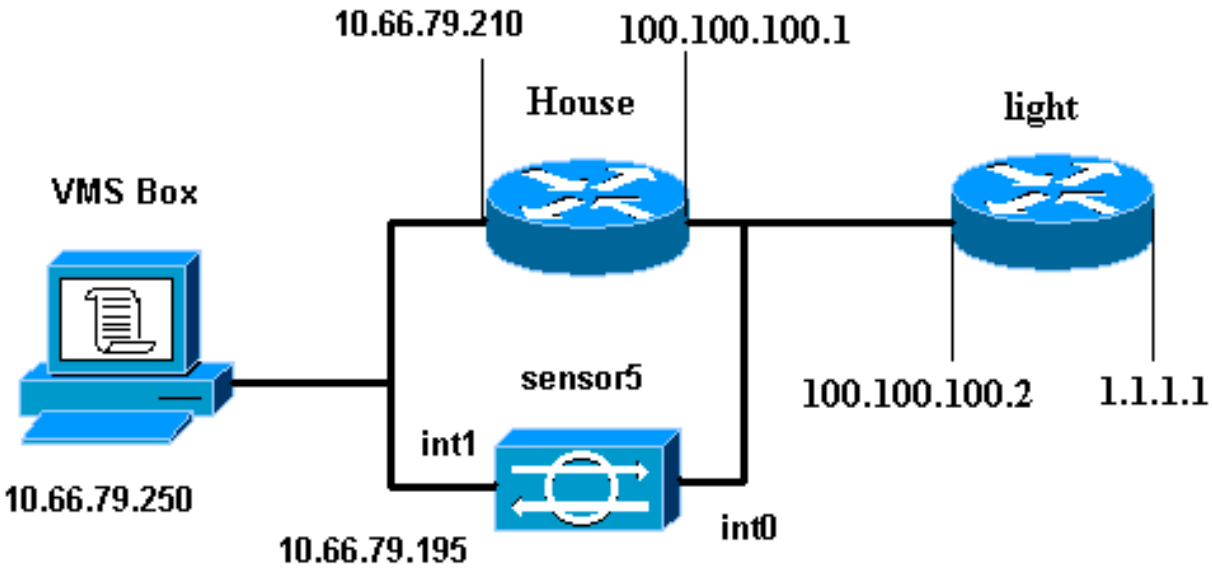
التكوين

في هذا القسم، تُقدّم لك معلومات تكوين الميزات الموضحة في هذا المستند.

ملاحظة: للعثور على معلومات إضافية حول الأوامر المستخدمة في هذا المستند، أستخدم أداة بحث الأوامر (للعملاء المسجلين فقط).

الرسم التخطيطي للشبكة

يستخدم هذا المستند إعداد الشبكة الموضح في هذا الرسم التخطيطي.



التكوينات

يستخدم هذا المستند التكوينات الموضحة هنا.

- ضوء الموجه
- منزل الموجه

ضوء الموجه

```
Current configuration : 906 bytes
!
version 12.3
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname light
!
enable password cisco
!
username cisco password 0 cisco
ip subnet-zero
!
!
!
ip ssh time-out 120
ip ssh authentication-retries 3
!
call rsvp-sync
!
!
!
fax interface-type modem
mta receive maximum-recipients 0
!
controller E1 2/0
!
!
!
interface FastEthernet0/0
ip address 100.100.100.2 255.255.255.0
duplex auto
speed auto
!
interface FastEthernet0/1
ip address 1.1.1.1 255.255.255.0
duplex auto
speed auto
!
interface BRI4/0
no ip address
shutdown
!
interface BRI4/1
no ip address
shutdown
!
interface BRI4/2
no ip address
shutdown
!
interface BRI4/3
no ip address
shutdown
!
ip classless
ip route 0.0.0.0 0.0.0.0 100.100.100.1
ip http server
ip pim bidir-enable
!
!
dial-peer cor custom
!
```

```
!
line con 0
line 97 108
line aux 0
line vty 0 4
 login
!
end
```

منزل الموجه

```
...Building configuration

Current configuration : 797 bytes
!
version 12.3
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname House
!
logging queue-limit 100
enable password cisco
!
ip subnet-zero
no ip domain lookup
!
!
interface Ethernet0
 ip address 10.66.79.210 255.255.255.224
 hold-queue 100 out
!
interface Ethernet1
 ip address 100.100.100.1 255.255.255.0
 !--- After Blocking is configured, the IDS Sensor !--- adds this access-group ip access-group
 IDS_Ethernet1_in_0 in
ip classless
ip route 0.0.0.0 0.0.0.0 10.66.79.193
ip route 1.1.1.0 255.255.255.0 100.100.100.2
ip http server
no ip http secure-server
!
 !--- After Blocking is configured, the IDS Sensor !--- adds this access list. ip access-list extended
 IDS_Ethernet1_in_0.
 permit ip host 10.66.79.195 any
 permit ip any any
!
line con 0
 stopbits 1
line vty 0 4
 password cisco
 login
!
scheduler max-task-time 5000
end
```

تكوين المستشعر الأولي

أكمل هذه الخطوات لتكوين المستشعر في البداية.

ملاحظة: إذا كنت قد قمت بتنفيذ الإعداد الأولي للمستشعر، فقم بالمتابعة إلى قسم إستيراد المستشعر إلى IDS MC.

1. وحدة تحكم في المستشعر.أنت حضضت ل username وكلمة. إذا كانت هذه هي المرة الأولى التي تقوم فيها بتوفير التحكم في المستشعر، فيجب عليك تسجيل الدخول باستخدام اسم المستخدم **Cisco** وكلمة المرور **Cisco**.
2. أنت حضضت أن يغير الكلمة وبعد ذلك أعدت الكلمة جديد أن يؤكد.
3. اكتب **setup** وأدخل المعلومات المناسبة في كل مطالبة لإعداد المعلمات الأساسية للمستشعر الخاص بك، كما هو موضح في هذا المثال:

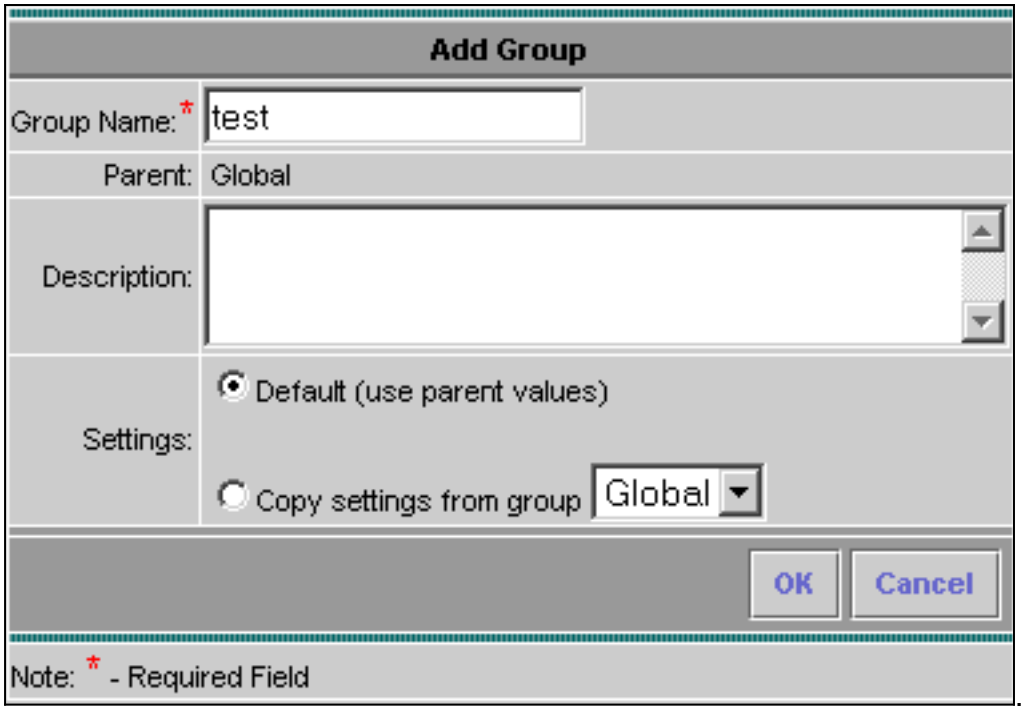
```
sensor5#setup

        --- System Configuration Dialog ---

.At any point you may enter a question mark '?' for help
.User ctrl-c to abort configuration dialog at any prompt
.'[]' Default settings are in square brackets

:Current Configuration

networkParams
ipAddress 10.66.79.195
netmask 255.255.255.224
defaultGateway 10.66.79.193
hostname sensor5
telnetOption enabled
accessList ipAddress 10.66.79.0 netmask 255.255.255.0
exit
timeParams
summerTimeParams
active-selection none
exit
exit
service webServer
general
ports 443
exit
exit
```

4. اضغط على **2** لحفظ التكوين الخاص بك.

إستيراد أداة الاستشعار إلى وحدة التحكم IDS MC

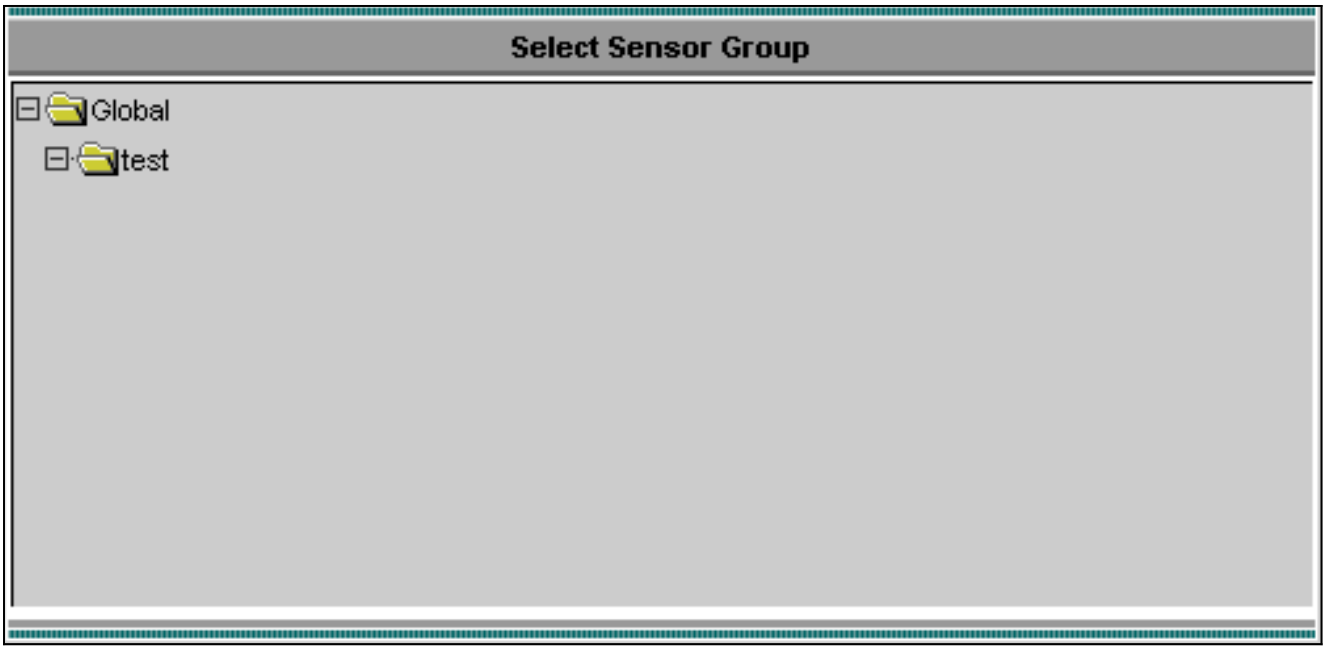
أتمت هذا steps أن يستورد المستشعر إلى ال IDS MC.

1. الاستعراض للوصول إلى جهاز الاستشعار الخاص بك.في هذه الحالة، استعرض للوصول إلى **http://10.66.79.250:1741** أو **https://10.66.79.250:1742**.
2. قم بتسجيل الدخول باستخدام اسم المستخدم وكلمة المرور الملائمين.في هذا المثال، تم إستخدام اسم المستخدم **admin** وكلمة المرور **cisco**.
3. حدد **VPN/حل إدارة الأمان>مركز الإدارة** واختر **أجهزة إستشعار IDS**.
4. انقر فوق علامة التبويب الأجهزة، وحدد **مجموعة المستشعر**، وقم بإبراز **عمومي**، وانقر فوق **إنشاء مجموعة فرعية**.
5. أدخل اسم المجموعة وتأكد من تحديد زر الاختيار **الافتراضي**، ثم انقر فوق **موافق** لإضافة المجموعة الفرعية إلى وحدة التحكم بالموجه الخاصة بالمعرف

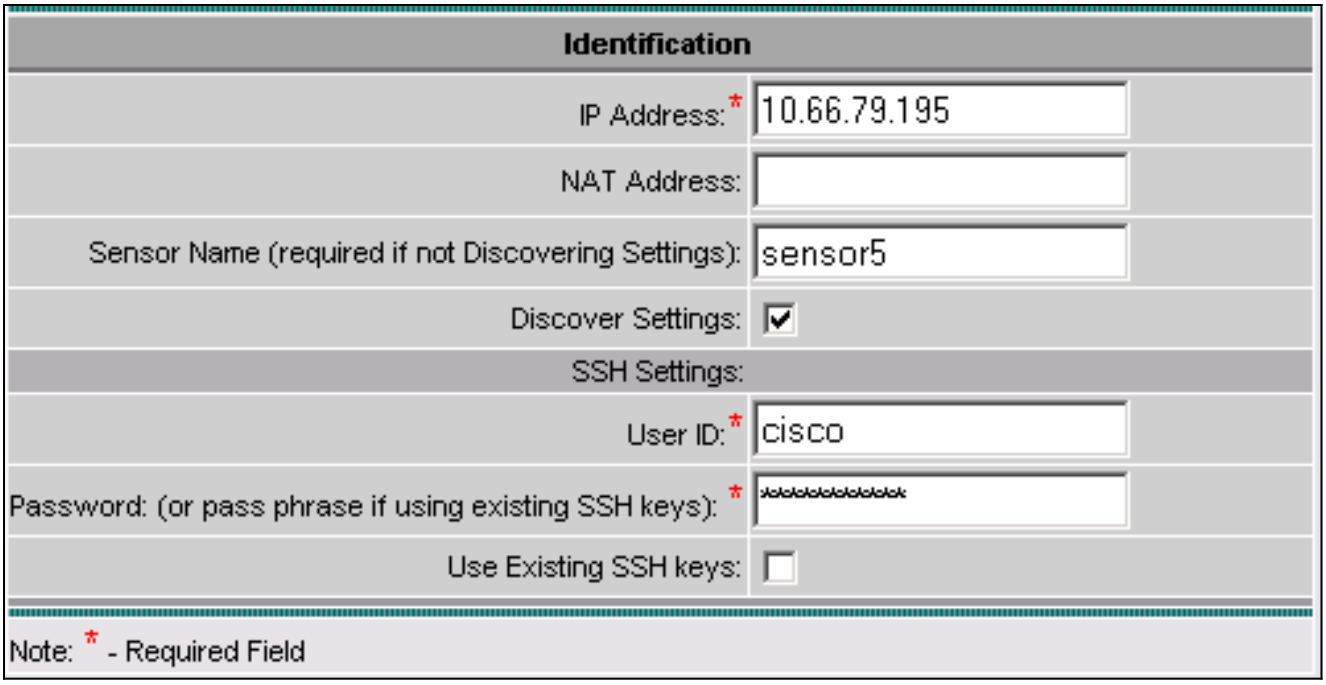


(IDS).

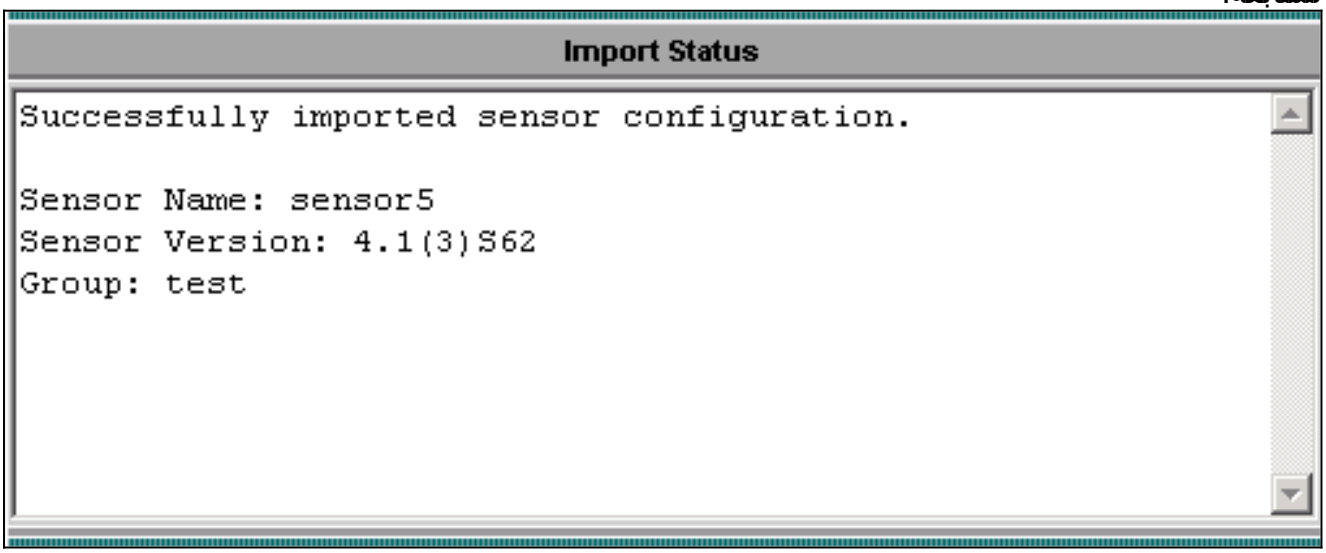
6. حدد **أجهزة** > **مستشعر**، أبرز المجموعة الفرعية التي تم إنشاؤها في الخطوة السابقة (في هذه الحالة، **إختبار**)، وانقر **إضافة**.
7. ركزت المجموعة الفرعية، وطقطقة **بعد ذلك**.



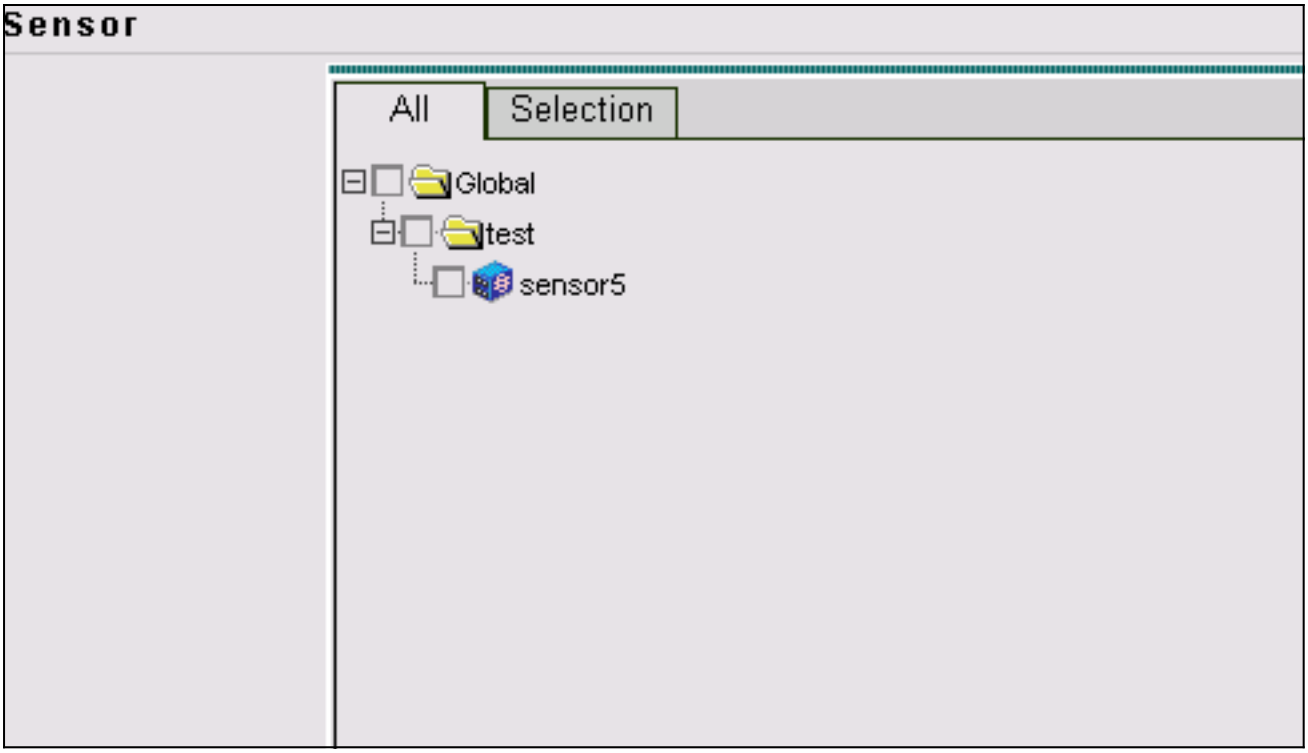
8. أدخل التفاصيل وفقا لهذا المثال، ثم انقر فوق **التالي** للمتابعة.



9. بعد تقديم رسالة إليك تفيد بأن ، انقر فوق **إنهاء** للمتابعة.



10. تم إستيراد جهاز الاستشعار إلى وحدة التحكم في إدارة IDS. في هذه الحالة، يتم إستيراد المستشعر5.



إستيراد المستشعر إلى مراقب الأمان

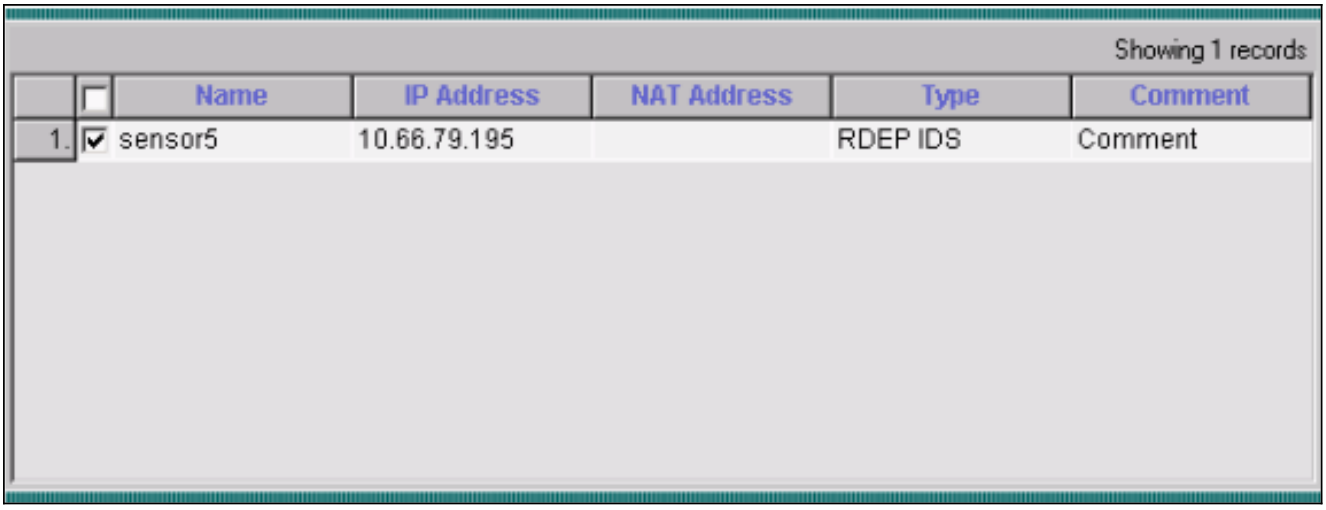
أكمل هذا الإجراء لاستيراد "المستشعر" إلى مراقبة الأمان.

1. في قائمة خادم VMS، حدد **حل إدارة الأمان/الشبكة الخاصة الظاهرية (VPN) > مركز المراقبة > مراقبة الأمان**.
2. حدد علامة التبويب "أجهزة"، ثم انقر فوق **إستيراد** وأدخل معلومات خادم IDS MC، طبقا لهذا المثال.

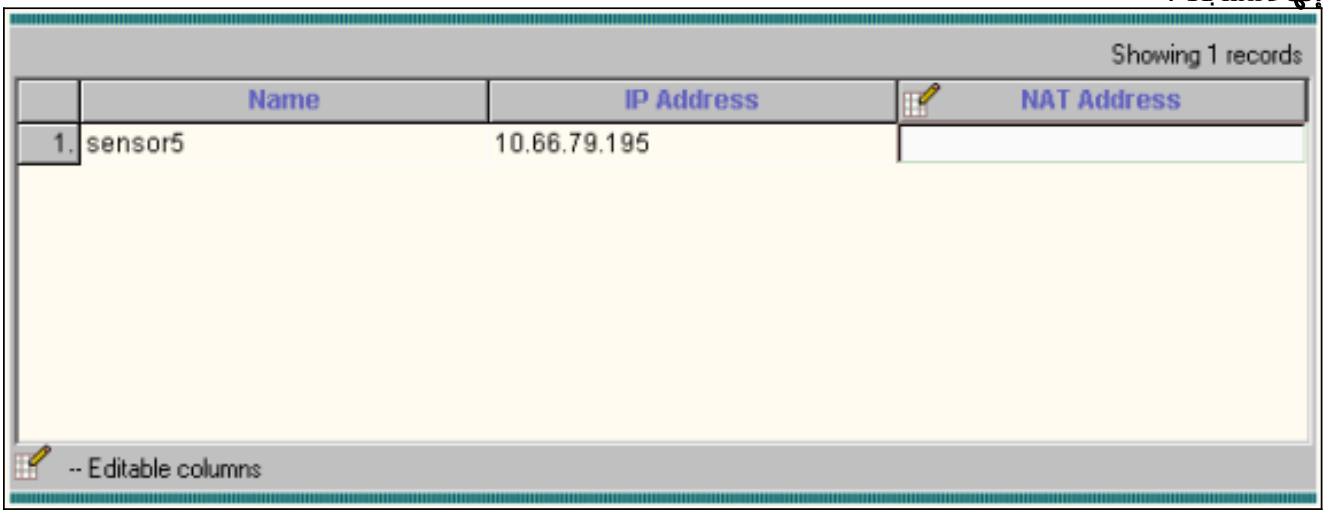
Enter IDS MC server contact information:	
IP Address/Host Name:*	10.66.79.250
Web Server Port:*	443
Username:*	admin
Password:*	•••••••

Note: * - Required Field

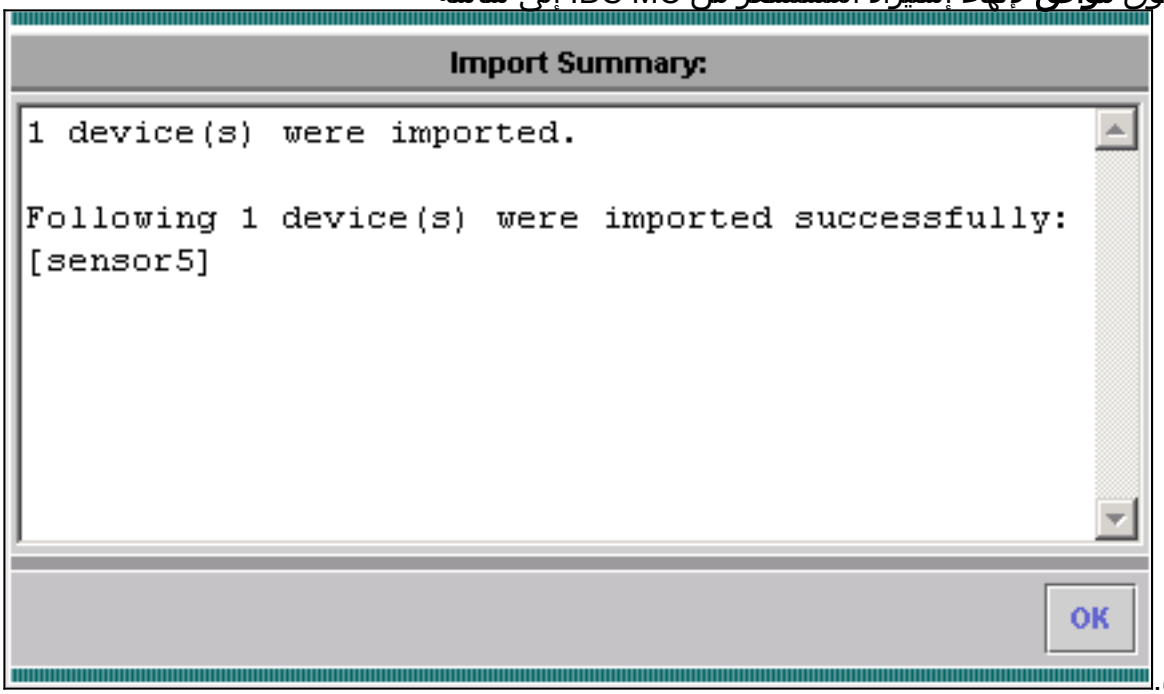
3. حدد المستشعر (في هذه الحالة، **المستشعر 5**) وانقر **التالي** للمتابعة.



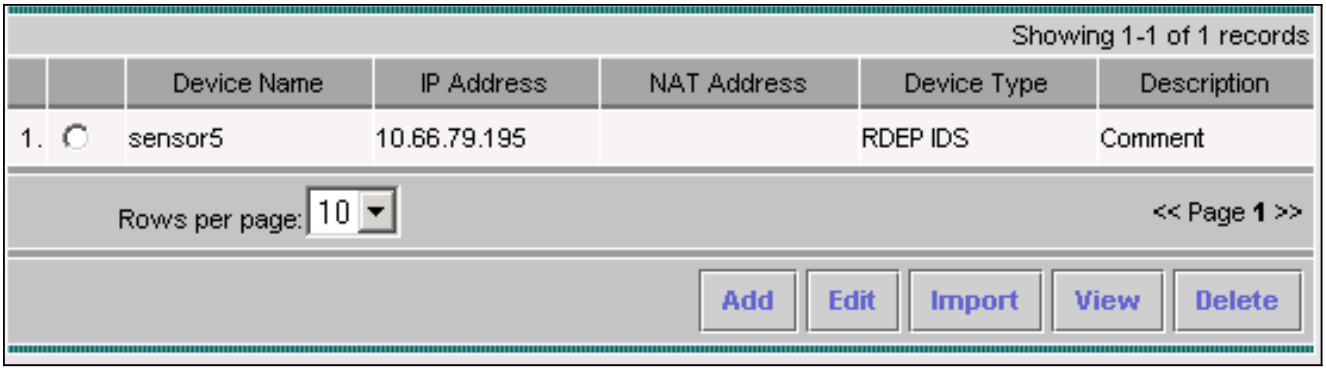
4. إن أمكن، حدث العنوان ترجمة عنوان الشبكة (NAT) للمستشعر الخاص بك، ثم انقر فوق **إنهاء**للمتابعة.



5. انقر فوق **موافق** لإنهاء إستيراد المستشعر من IDS MC إلى شاشة الأمان.



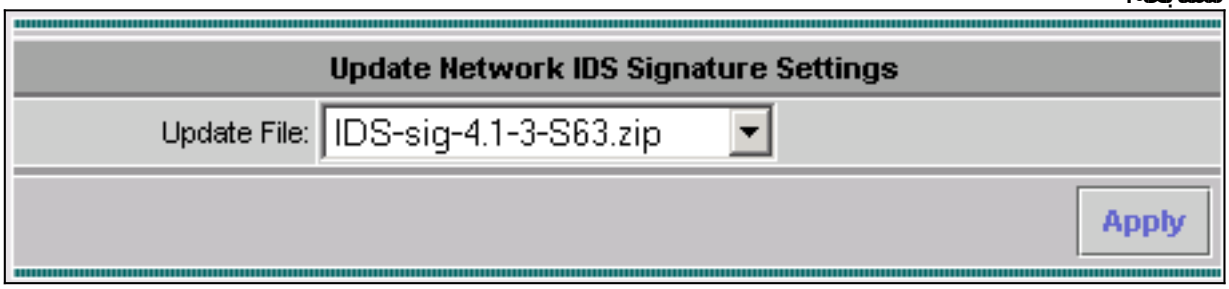
6. تم إستيراد جهاز الاستشعار بنجاح.



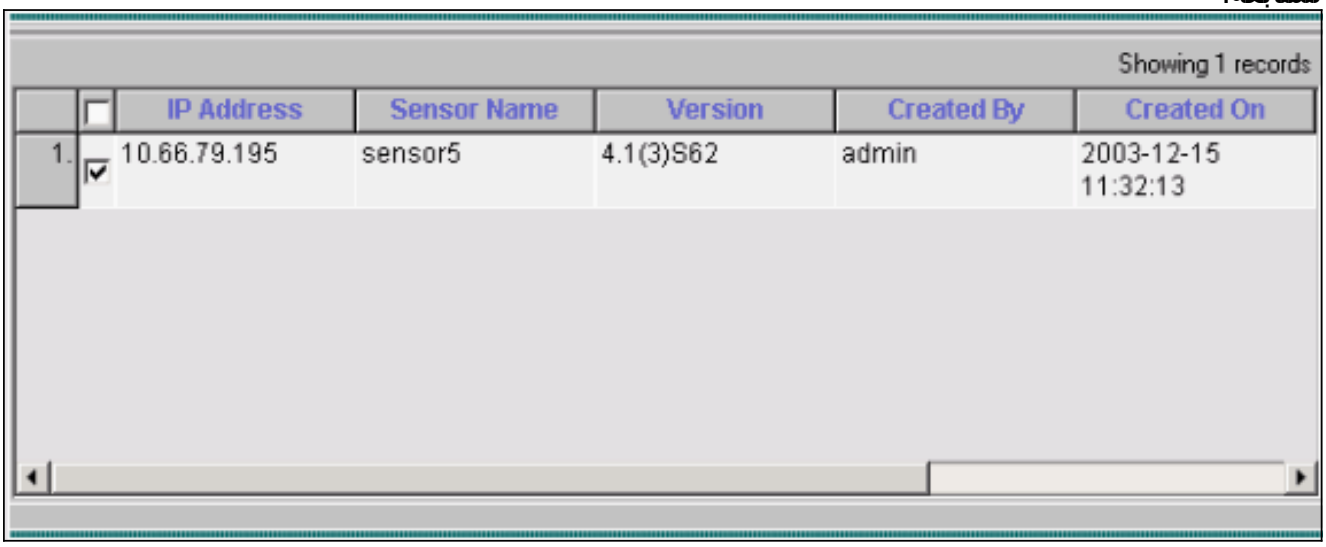
إستخدام IDS MC لتحديثات التوقيع

أكمل هذا الإجراء لاستخدام IDS MC لتحديثات التوقيع.

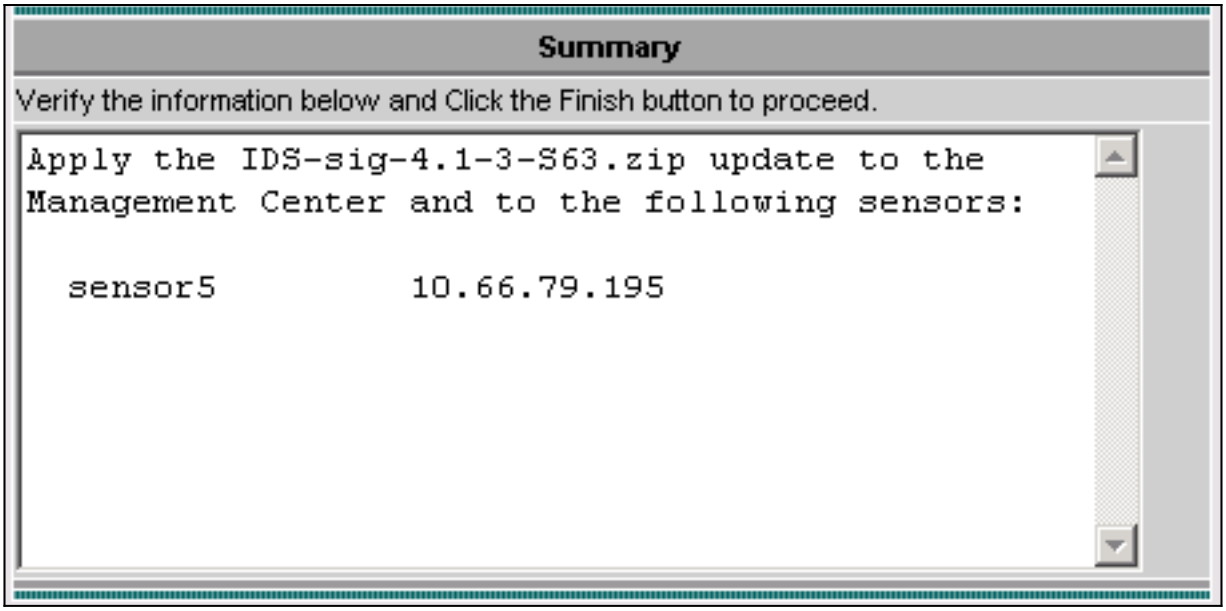
1. قم بتنزيل تحديثات توقيع معرفات الشبكة (للعملاء المسجلين فقط) من التنزيلات واحفظهم في دليل C:\PROGRA~1\CSCOpx\MDC\etc\ids\updates\ على خادم VMS الخاص بك.
2. في وحدة تحكم خادم VMS، حدد **حل إدارة الأمان/الشبكة الخاصة الظاهرية (VPN)** > **مركز الإدارة** > **أجهزة الاستشعار**.
3. انقر فوق علامة التبويب تكوين، وحدد **تحديثات**، وانقر فوق **تحديث توقيعات معرفات الشبكة**.
4. حدد التوقيع الذي تريد ترقيته من القائمة المنسدلة وانقر فوق **تطبيق** للمتابعة.



5. حدد أداة (أجهزة) الاستشعار المراد تحديثها، وانقر فوق **التالي** للمتابعة.



6. بعد مطالبتك بتطبيق التحديث على مركز الإدارة، بالإضافة إلى أداة الاستشعار، انقر فوق **إنهاء** للمتابعة.



7. برنامج Telnet أو وحدة التحكم في واجهة سطر أوامر المستشعر. تظهر معلومات مماثلة لهذا:

```
sensor5#
:(Broadcast message from root (Mon Dec 15 11:42:05 2003
.Applying update IDS-sig-4.1-3-S63
.This may take several minutes
.Please do not reboot the sensor during this update
:(Broadcast message from root (Mon Dec 15 11:42:34 2003
.Update complete
sensorApp is restarting
.This may take several minutes
```

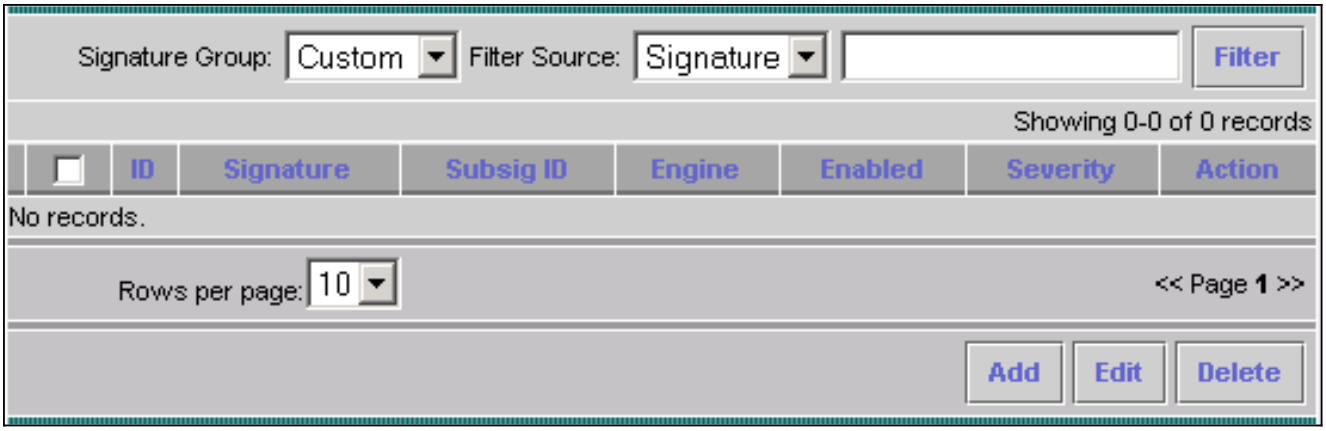
8. انتظر لبضع دقائق للسماح باستكمال الترقية، ثم أدخل **show version** للتحقق.

```
sensor5#show version
:Application Partition
Cisco Systems Intrusion Detection Sensor, Version 4.1(3)S63

:Upgrade History
 IDS-sig-4.1-3-S62           07:03:04 UTC Thu Dec 04 2003 *
IDS-sig-4.1-3-S63.rpm.pkg    11:42:01 UTC Mon Dec 15 2003
```

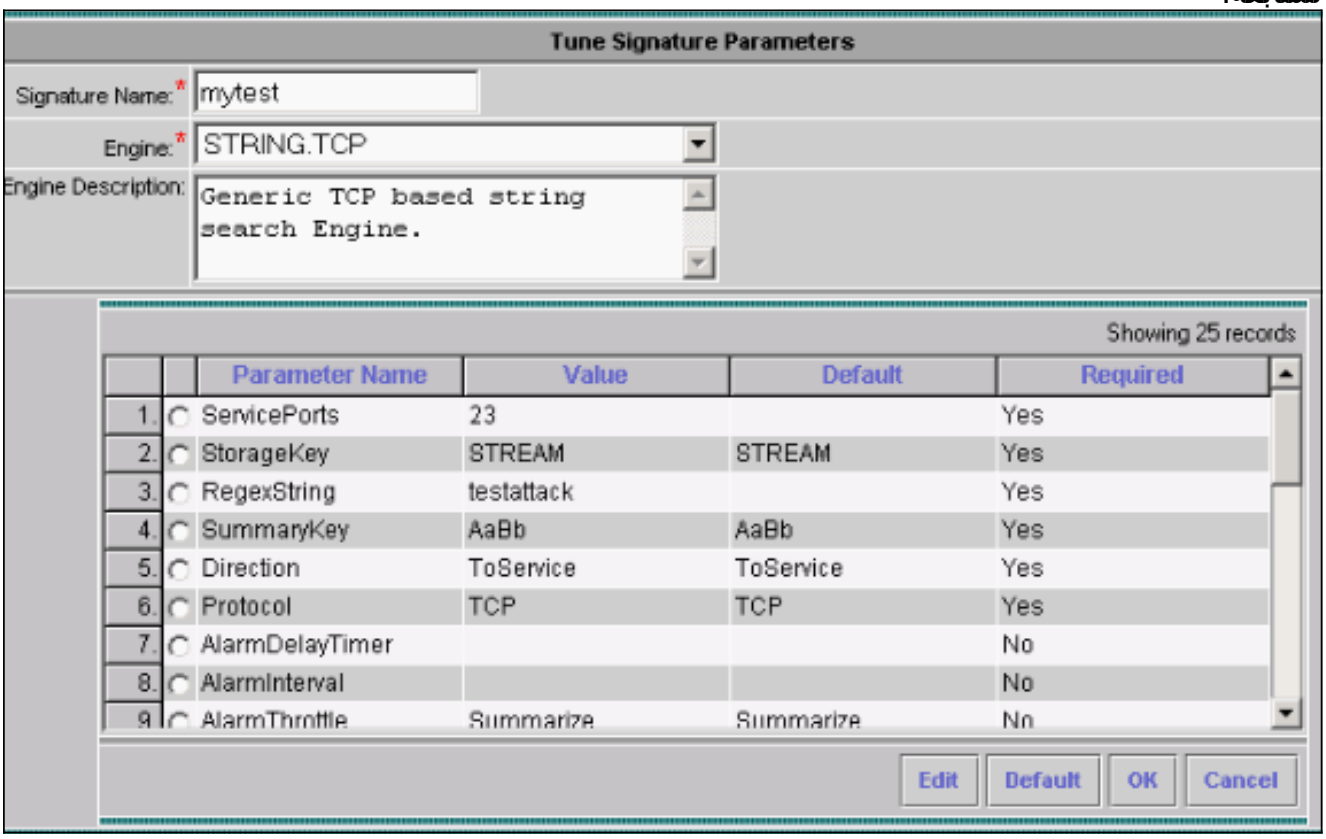
تكوين الحظر لموجه IOS

أكمل هذا الإجراء لتكوين الحظر لموجه IOS.

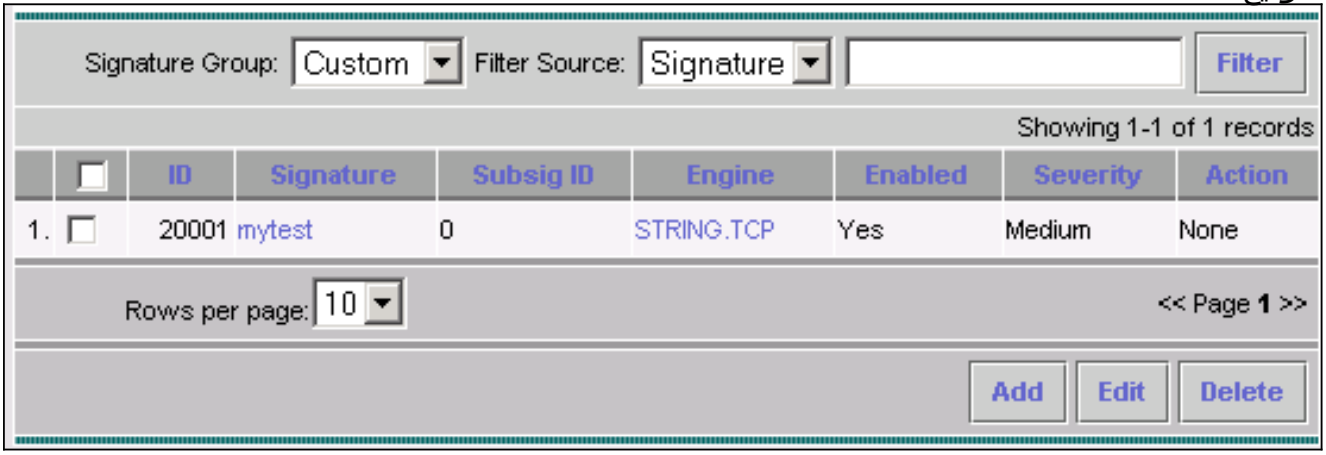
1. في وحدة تحكم خادم VMS، حدد **حل إدارة الأمان/الشبكة الخاصة الظاهرية (VPN) > مركز الإدارة > أجهزة إستشعار IDS**.
2. حدد علامة التبويب تكوين، وحدد أداة الاستشعار من أداة تحديد الكائن، وانقر فوق **إعدادات**.
3. حدد **توقيعات**، انقر **تخصيص**، ثم انقر **إضافة** لإضافة توقيع جديد.



4. أدخل اسم التوقيع الجديد، ثم حدد المحرك (في هذه الحالة، **STRING.TCP**).
5. يمكنك تخصيص المعلمات المتوفرة عن طريق التحقق من زر الاختيار المناسب والنقر فوق **تحرير**.في هذا المثال، يتم تحرير المعلمة ServicePorts لتغيير قيمتها إلى 23 (للمنفذ 23). تم تحرير المعلمة RegexString أيضا لإضافة **هجوم** إختبار القيمة. عند اكتمال هذا، انقر فوق **موافق"** للمتابعة.

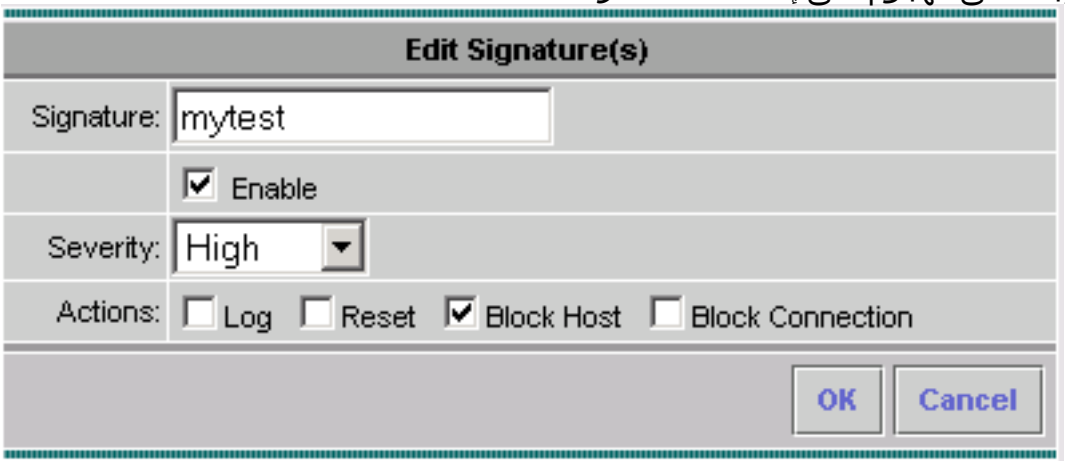


6. لتحرير خطورة وإجراءات التوقيع أو لتمكين/تعطيل التوقيع، انقر اسم التوقيع.



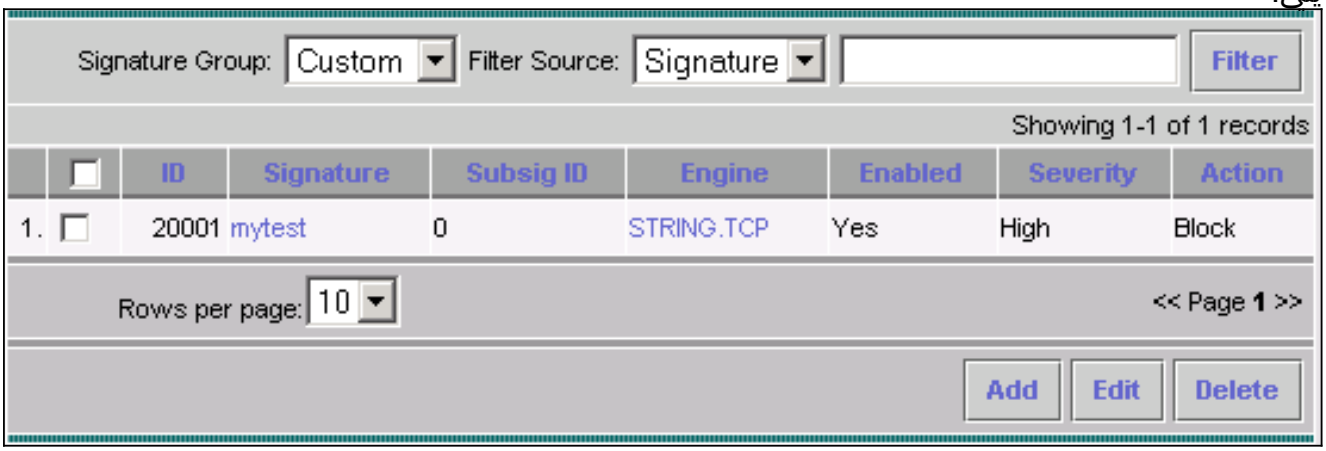
7. في هذه الحالة، يتم تغيير الخطورة إلى **عالي** ويتم تحديد الإجراء **حظر المضيف**. انقر فوق **موافق"**

للمتابعة.حظر المضيف الذي يهاجم مضيفات IP أو الشبكات الفرعية IP.يحظر اتصال الحظر منافذ TCP أو UDP (بناء على الهجوم على إتصالات TCP أو

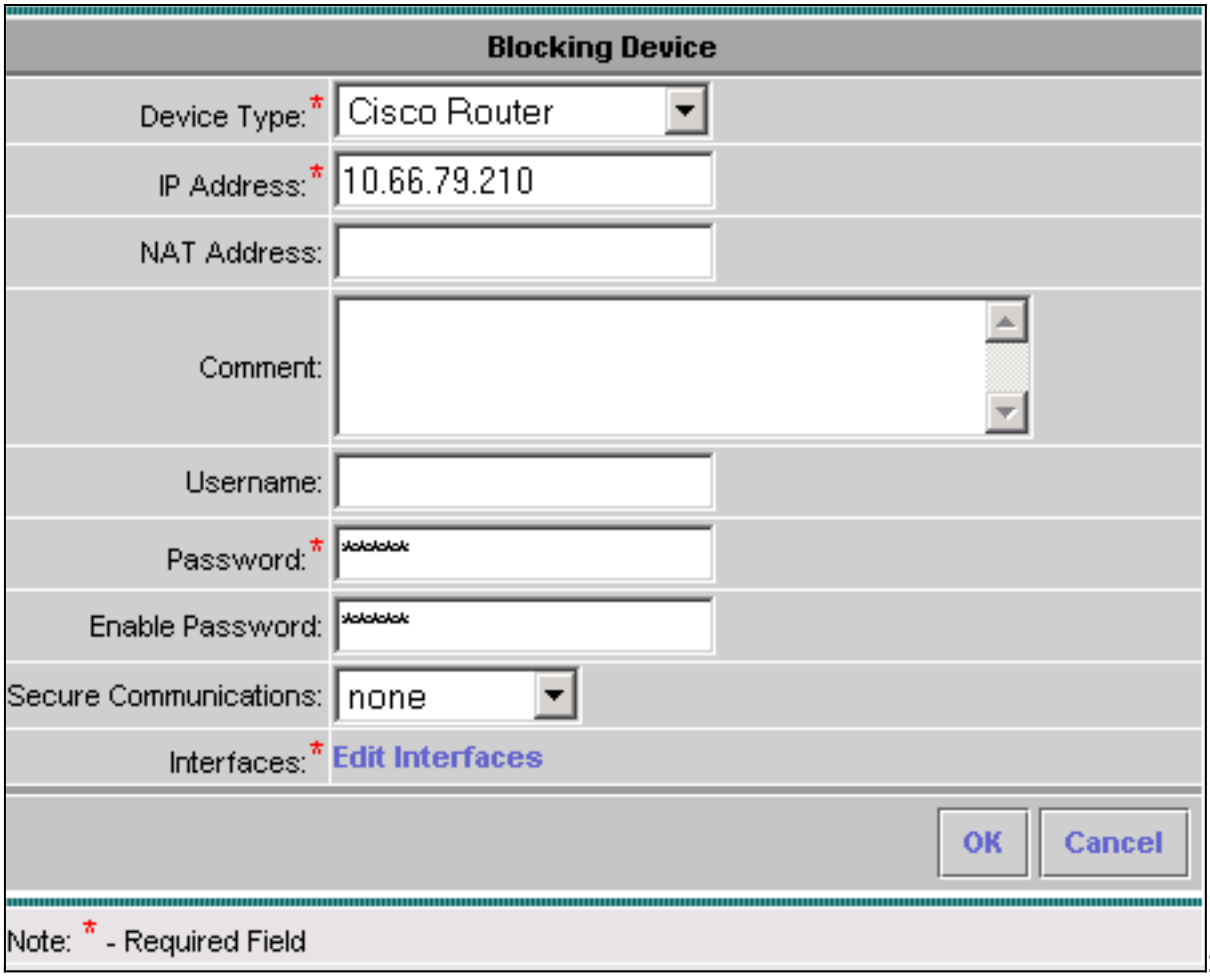


UDP).

8. يبدو التوقيع الكامل مشابها لما يلي:

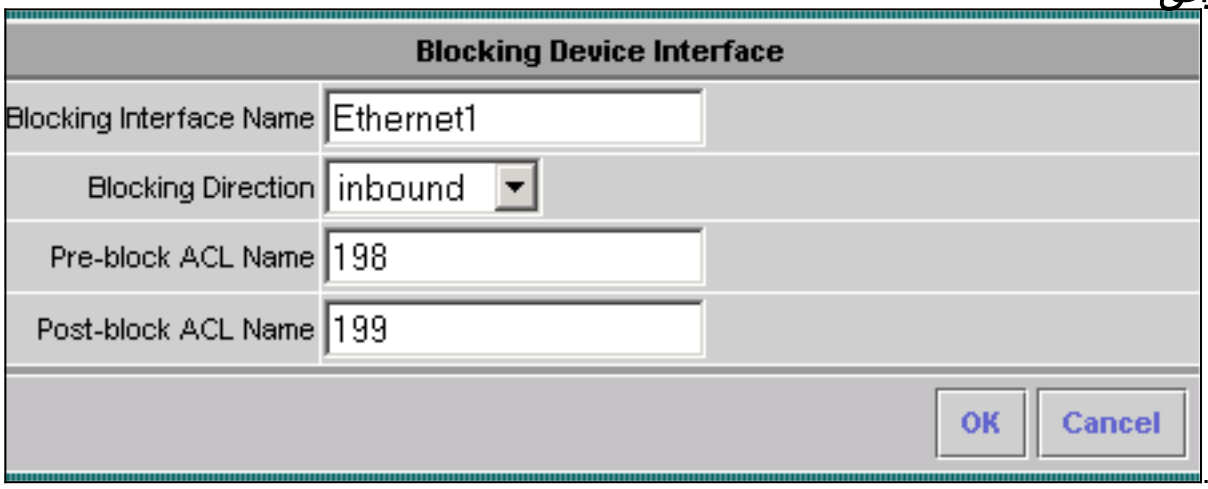


9. لتكوين جهاز الحظر، حدد **الحظر** > **أجهزة الحظر** من أداة تحديد الكائن (القائمة على الجانب الأيسر من الشاشة)، وانقر **إضافة** لإدخال المعلومات



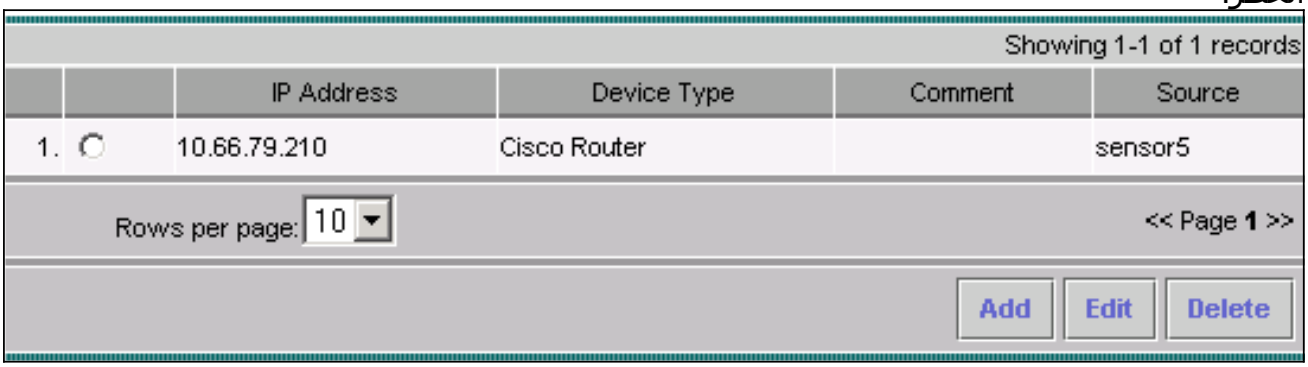
التالية:

10. انقر فوق **تحرير الواجهات** (راجع التقاط الشاشة السابق)، انقر فوق **إضافة**، وأدخل هذه المعلومات، ثم انقر فوق **موافق**



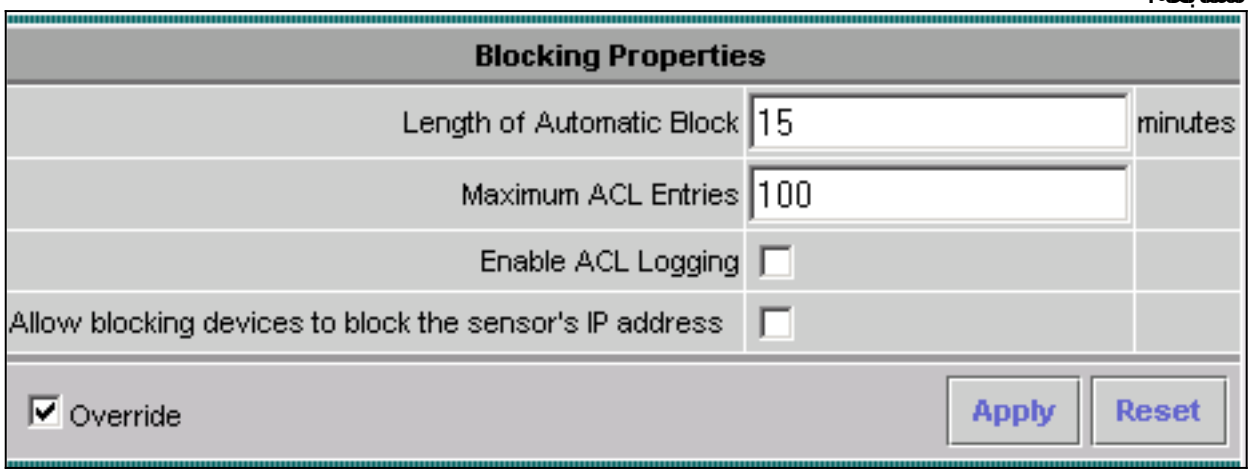
للمتابعة.

11. انقر فوق **موافق** مرتين لإكمال تكوين جهاز الحظر.

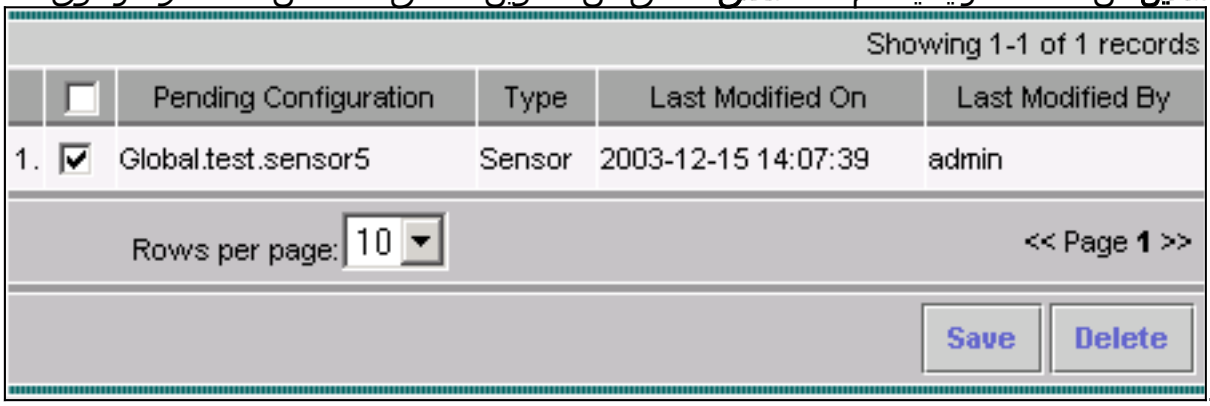


12. لتكوين خصائص الحظر، حدد **الحظر > خصائص الحظر**.يمكن تعديل طول "الحظر التلقائي". في هذه الحالة،

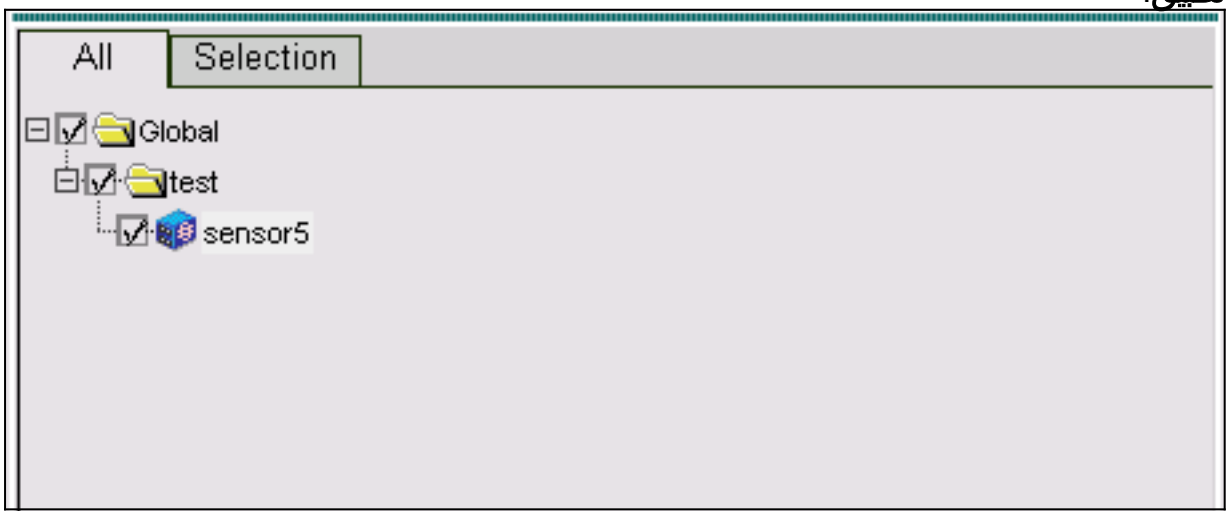
يتم تغييره إلى **15 دقيقة**. انقر فوق **تطبيق** للمتابعة.



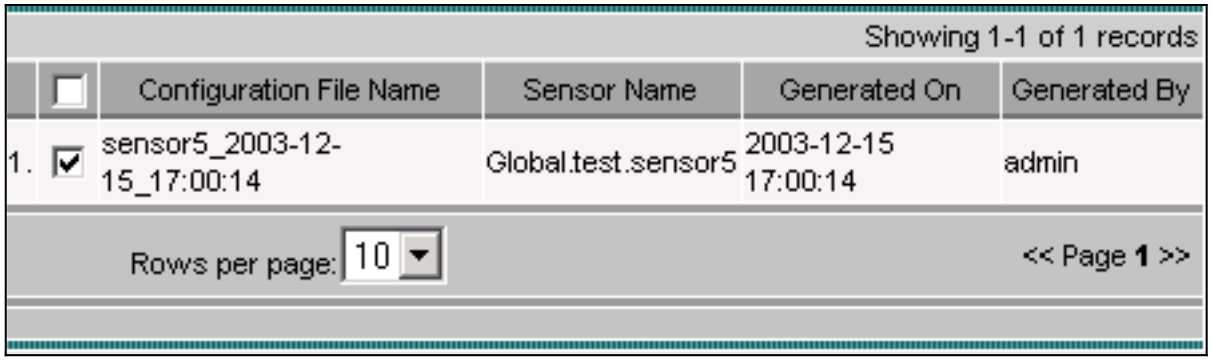
13. حدد **تشكيل** من القائمة الرئيسية، ثم حدد **معلق**، تحقق من التكوين المعلق للتأكد من صحته، وانقر فوق **حفظ**.



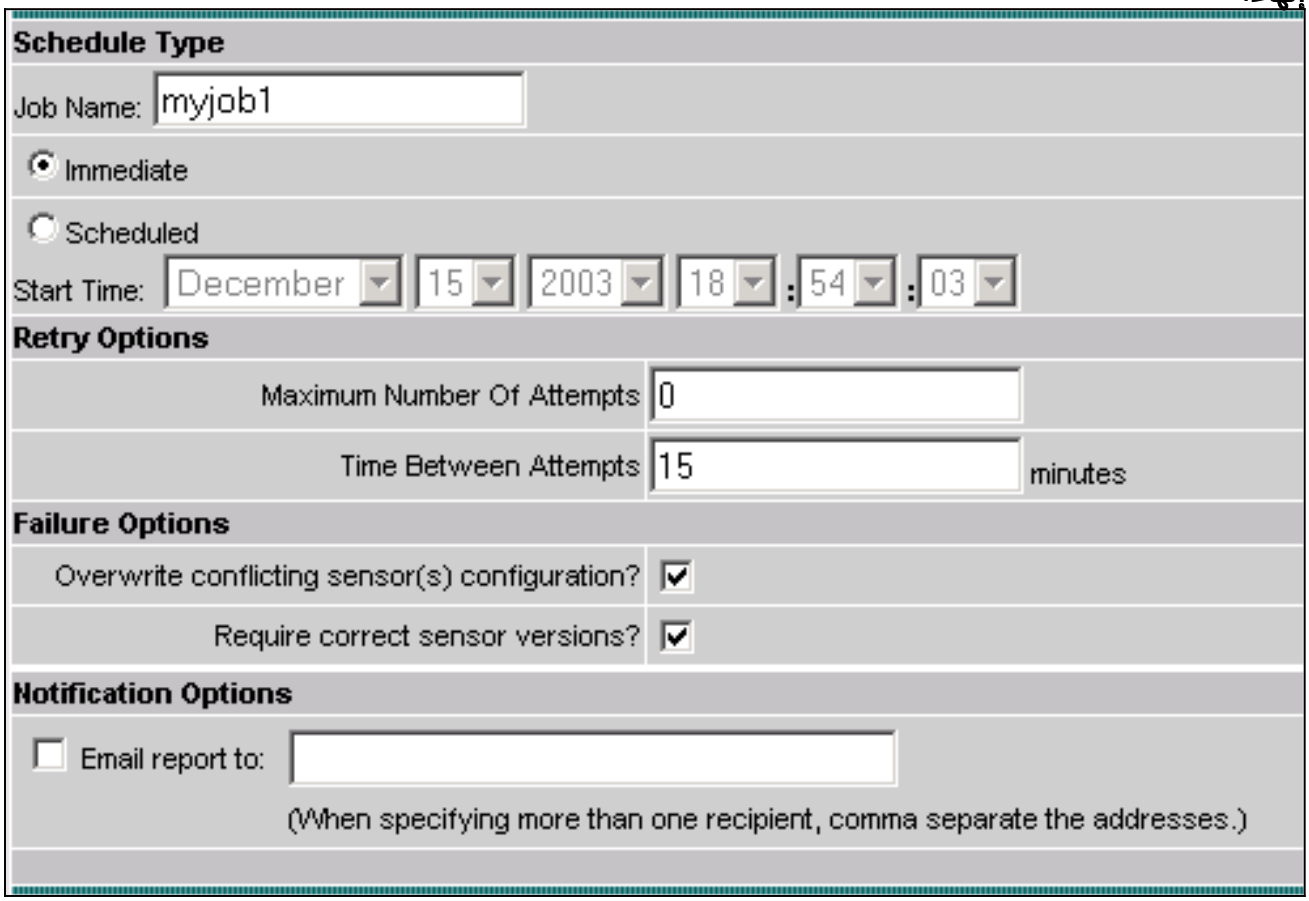
14. لدفع تغييرات التكوين إلى المستشعر، قم بإنشاء التغييرات ثم نشرها عن طريق تحديد **نشر** > **إنشاء** وانقر فوق **تطبيق**.



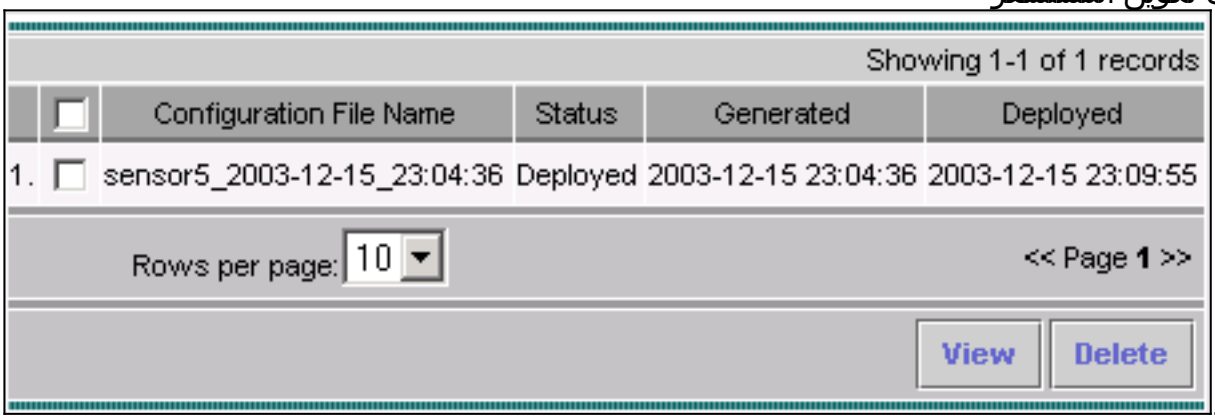
15. حدد **نشر** > **نشر**، ثم انقر فوق **إرسال**.
16. حدد خانة الاختيار المجاورة للمستشعر، ثم انقر فوق **نشر**.
17. حدد خانة الاختيار للمهمة في قائمة الانتظار، ثم انقر فوق **التالي** للمتابعة.



18. أدخل اسم الوظيفة وجدولة الوظيفة كفوري، ثم انقر فوق **إنهاء**.



19. حدد **نشر** > **نشر** > **تعليق**.انتظر بضع دقائق حتى يتم إكمال كافة المهام المعلقة. تكون قائمة الانتظار فارغة بعد ذلك.
20. لتأكيد النشر، حدد **Configuration**>**المحفوظات**.تأكد من عرض حالة التكوين كما هو **منشور**. هذا يعني أنه تم تحديث تكوين المستشعر بنجاح.



التحقق من الصحة

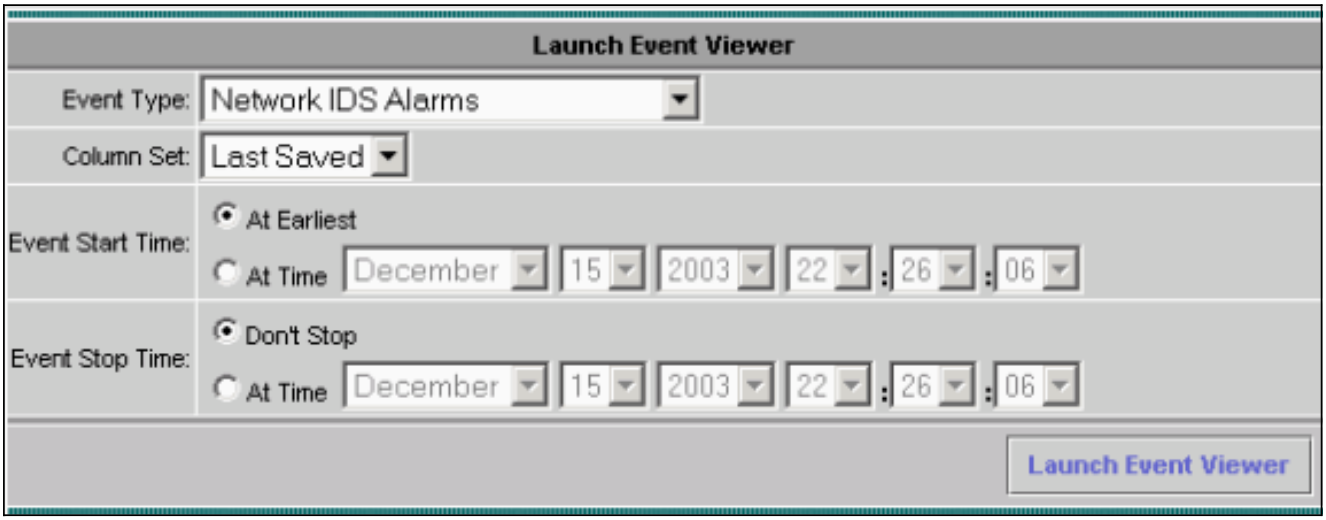
يوفر هذا القسم معلومات يمكنك إستخدامها للتأكد من أن التكوين يعمل بشكل صحيح.

يتم دعم بعض أوامر **العرض بواسطة** أداة مترجم الإخراج (العملاء المسجلون فقط)، والتي تتيح لك عرض تحليل إخراج أمر **العرض**.

شن الهجوم والعرقلة

للتحقق من أن عملية الحظر تعمل بشكل صحيح، قم بتشغيل هجوم إختبار وتحقق من النتائج.

1. قبل بدء الهجوم، حدد **حل إدارة الأمان/الشبكة الخاصة الظاهرية (VPN) > مركز المراقبة > مراقبة الأمان**.
2. أختر **شاشة** من القائمة الرئيسية، وانقر فوق **الأحداث** ثم انقر فوق **تشغيل عارض الأحداث**.



3. Telnet إلى الموجه (في هذه الحالة، Telnet إلى موجه المنزل)، للتحقق من الاتصال من المستشعر.

```
house#show user
  Line       User       Host(s)              Idle       Location
  con 0                 idle                 00:00:00 0  *
 vty 0                  idle                 00:00:17 10.66.79.195 226
house#show access-list
Extended IP access list IDS_Ethernet1_in_0
    permit ip host 10.66.79.195 any 10
    (permit ip any any (20 matches 20
#House
```

4. لبدء الهجوم، قم بتشغيل Telnet من موجه إلى آخر واكتب **هجوم** التجربة.في هذه الحالة، إستخدمنا Telnet للاتصال من موجه الضوء إلى موجه المنزل. بمجرد الضغط على **<space>** أو **<enter>**، بعد كتابة هجوم إختبار، يجب إعادة تعيين جلسة عمل برنامج Telnet.

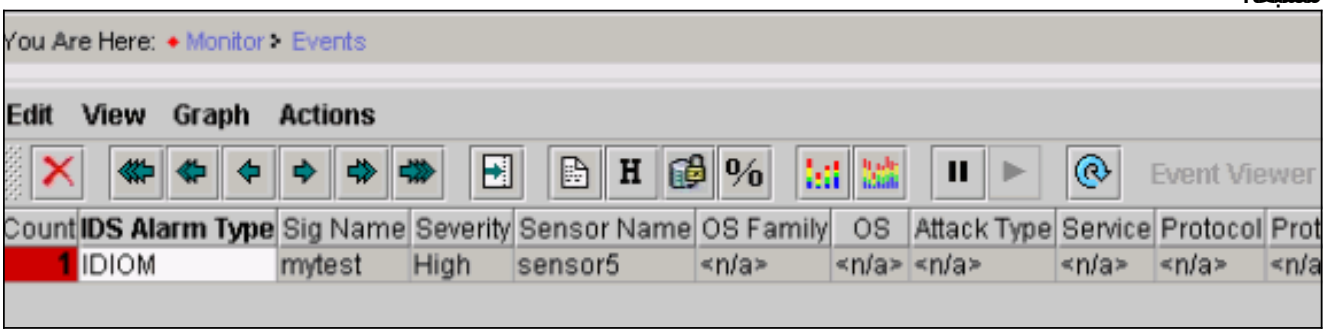
```
light#telnet 100.100.100.1
Trying 100.100.100.1 ... Open
User Access Verification
:Password
 house>en
:Password
house#testattack
Host 100.100.100.2 has been blocked due to the !--- signature "testattack" being ---!
[triggered. [Connection to 100.100.100.1 lost
```

5. Telnet إلى الموجه (المنزل) وأدخل الأمر **show access-list**.

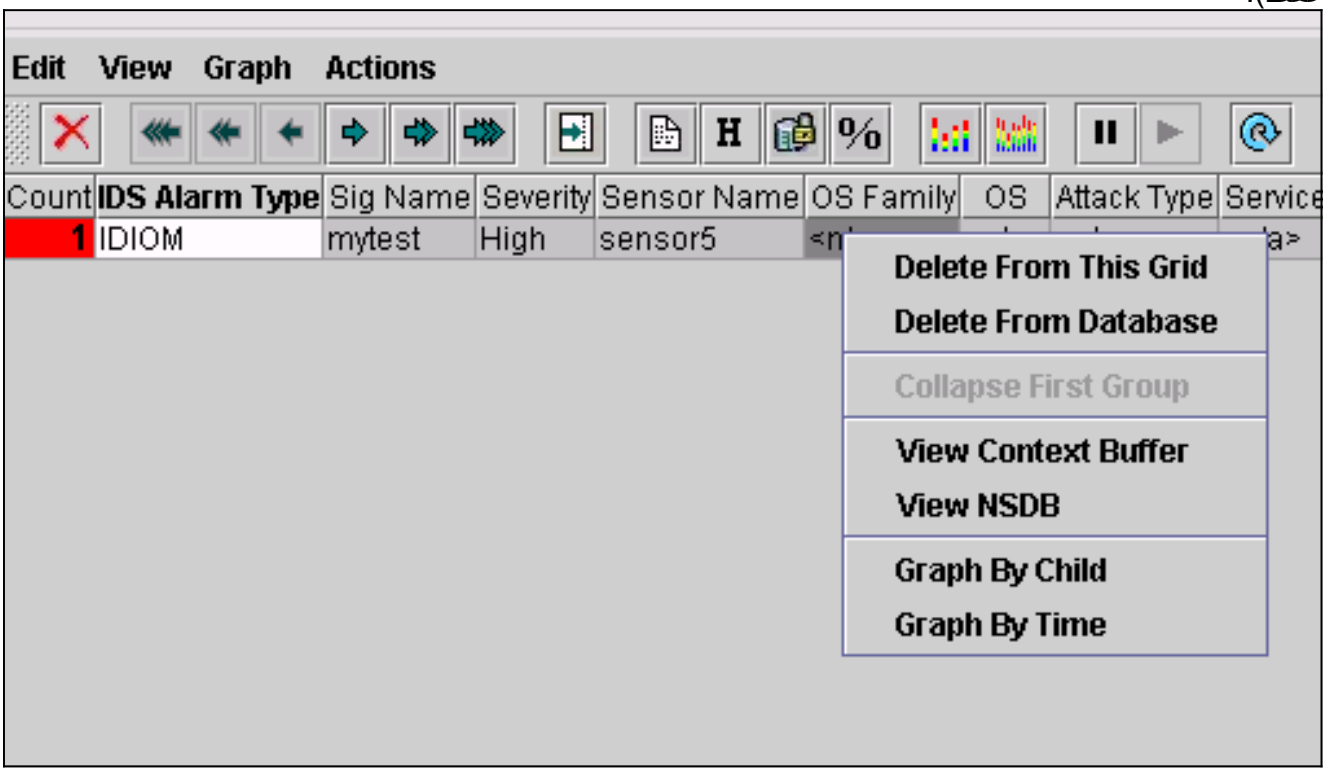
```
house#show access-list
Extended IP access list IDS_Ethernet1_in_1
    permit ip host 10.66.79.195 any 10
You will see a temporary entry has been added to !--- the access list to block the ---!
router from which you connected via Telnet previously. 20 deny ip host 100.100.100.2 any
((37 matches
```

```
permit ip any any 30
```

6. من عارض الأحداث، انقر فوق **قاعدة بيانات الاستعلام** للأحداث الجديدة الآن لعرض التنبيه للهجوم الذي تم تشغيله
مسبقا.



7. في عارض الأحداث، قم بإبراز التنبيه والنقر بزر الماوس الأيمن، ثم حدد **عرض المخزن المؤقت للسياق** أو **عرض NSDB** لعرض معلومات أكثر تفصيلا حول التنبيه.**ملاحظة:** يتوفر أيضا NSDB على الإنترنت في موسوعة Cisco Secure (العملاء المسجلون فقط).

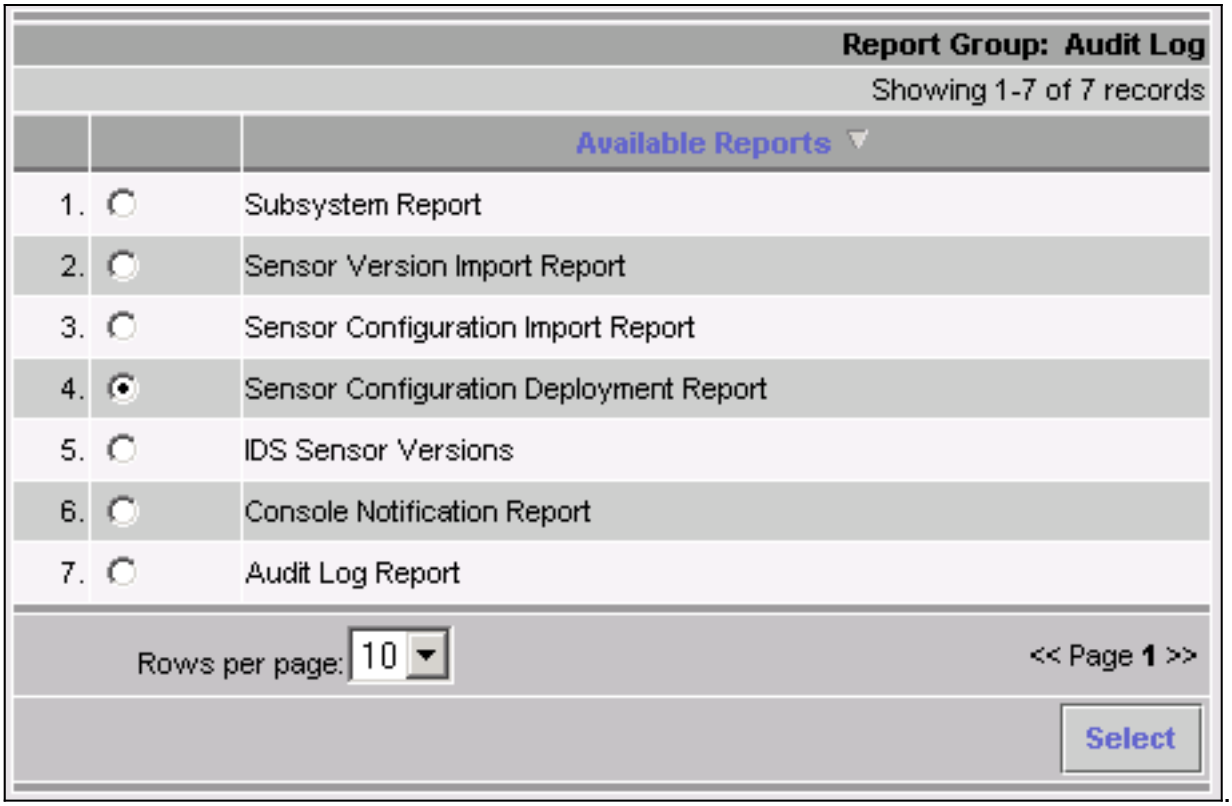


استكشاف الأخطاء وإصلاحها

إجراء استكشاف الأخطاء وإصلاحها

أستخدم الإجراء التالي لأغراض أستكشاف الأخطاء وإصلاحها.

1. في IDS MC، حدد **تقارير > إنشاء**.ورهنا بنوع المشكلة، ينبغي العثور على مزيد من التفاصيل في أحد التقارير السبعة



المتاحة.

2. دخلت في المستشعر وحدة طرفية للتحكم، الأمر **show statistics network access** وفحصت الإنتاج أن يضمن ال "حالة" نشط.

```
sensor5#show statistics networkAccess
                    Current Configuration
                AllowSensorShun = false
                   ShunMaxEntries = 100
                             NetDevice
                        Type = Cisco
                     IP = 10.66.79.210
                     NATAddr = 0.0.0.0
                Communications = telnet
                          ShunInterface
            InterfaceName = FastEthernet0/1
                   InterfaceDirection = in
                                        State
                      ShunEnable = true
                             NetDevice
                     IP = 10.66.79.210
            AclSupport = uses Named ACLs
                      State = Active
                           ShunnedAddr
                              Host
                IP = 100.100.100.2
                  ShunMinutes = 15
              MinutesRemaining = 12
                                    sensor5#
```

3. تأكد من أن معلمة الاتصال توضح أنه يتم إستخدام البروتوكول الصحيح، مثل Telnet أو SSH (Secure Shell) مع 3DES.يمكنك تجربة بروتوكول SSH أو Telnet يدويا من عميل SSH/Telnet على جهاز كمبيوتر للتحقق من صحة بيانات اعتماد اسم المستخدم وكلمة المرور. يمكنك بعد ذلك تجربة Telnet أو SSH من المستشعر نفسه، إلى الموجه، لضمان إمكانية تسجيل الدخول بنجاح.

معلومات ذات صلة

- صفحة دعم اكتشاف التسلل الآمن من Cisco

- دعم حل إدارة الأمان/الشبكة الخاصة الظاهرية (VPN) من CiscoWorks
- الدعم التقني والمستندات - Cisco Systems

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).