# خطوات التكوين الأولية لنظام FireSIGHT

## المحتويات



## المقدمة

بعد إعادة تكوين مركز إدارة FireSIGHT أو جهاز FirePOWER، تحتاج إلى إكمال عدة خطوات لجعل النظام يعمل بشكل كامل ولإنشاء تنبيهات لأحداث التسلل، مثل تثبيت الترخيص وتسجيل الأجهزة وتطبيق سياسة الصحة وسياسة النظام وسياسة التحكم في الوصول وسياسة التسلل، وما إلى ذلك. هذا المستند هو ملحق لدليل تثبيت نظام FireSIGHT.

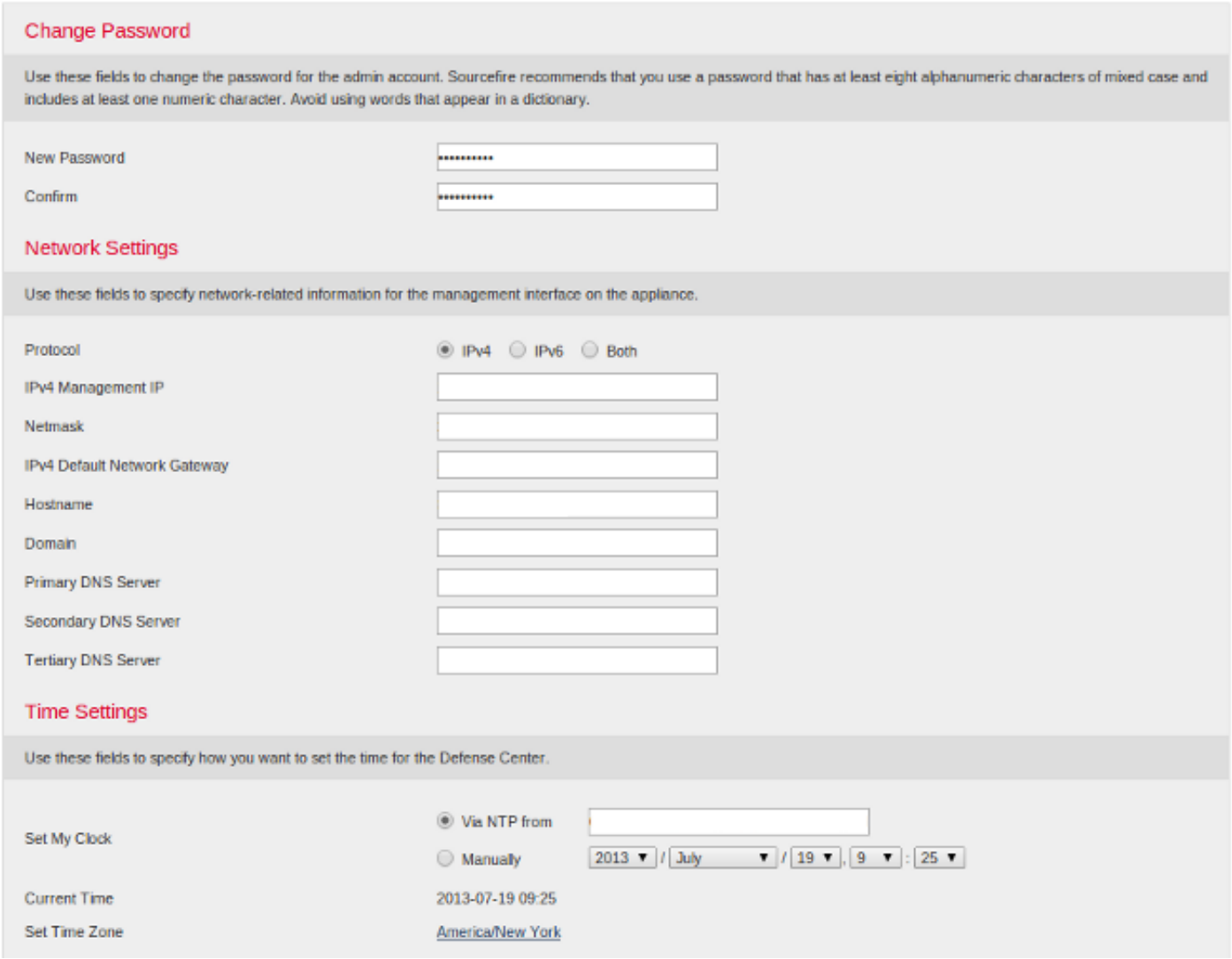
## المتطلبات الأساسية

يفترض هذا الدليل أنك قرأت بعناية دليل تثبيت نظام FireSIGHT.

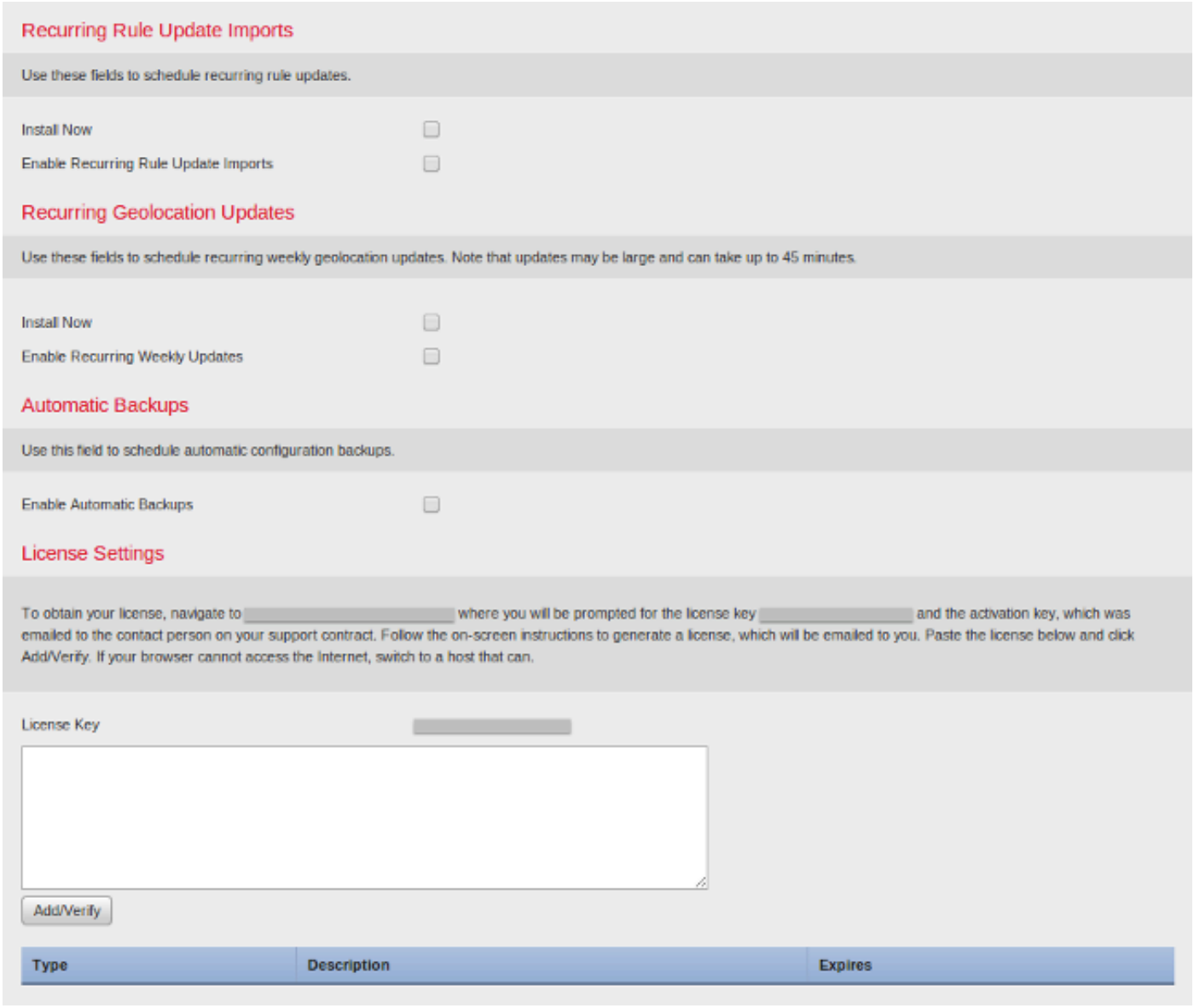
## التكوين

### الخطوة 1: الإعداد الأولي

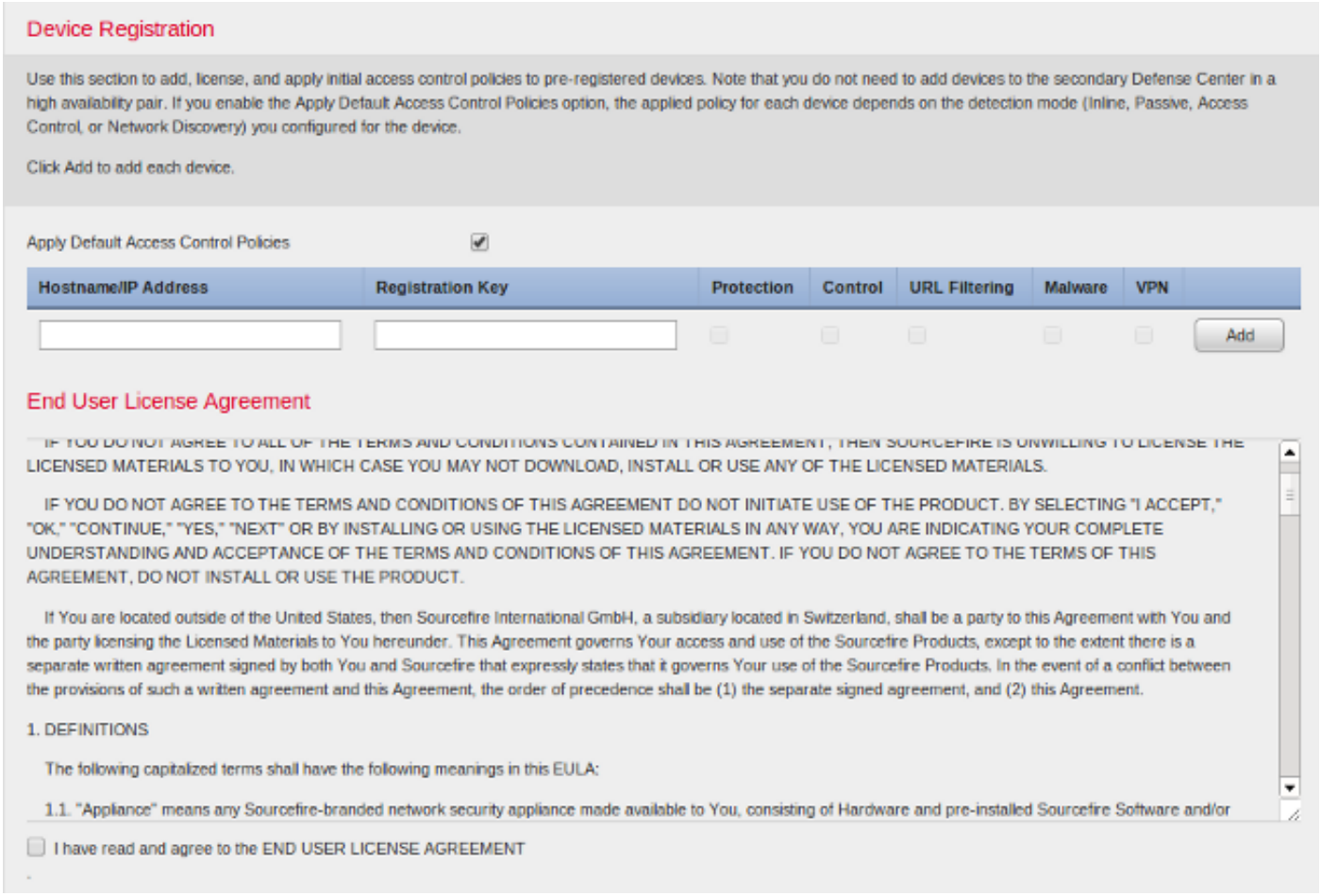
في مركز إدارة FireSIGHT الخاص بك، يجب عليك إكمال عملية الإعداد من خلال تسجيل الدخول إلى واجهة الويب وتحديد خيارات التكوين الأولية على صفحة الإعداد الموضحة أدناه. في هذه الصفحة، يجب عليك تغيير كلمة مرور المسؤول، كما يمكنك تحديد إعدادات الشبكة مثل خوادم Domain و DNS، وتكوين الوقت.




يمكنك بشكل إختياري تكوين تحديثات القواعد المتكررة والموقع الجغرافي بالإضافة إلى النسخ الاحتياطية التلقائية.
يمكن أيضا تثبيت أي تراخيص ميزات عند هذه النقطة.



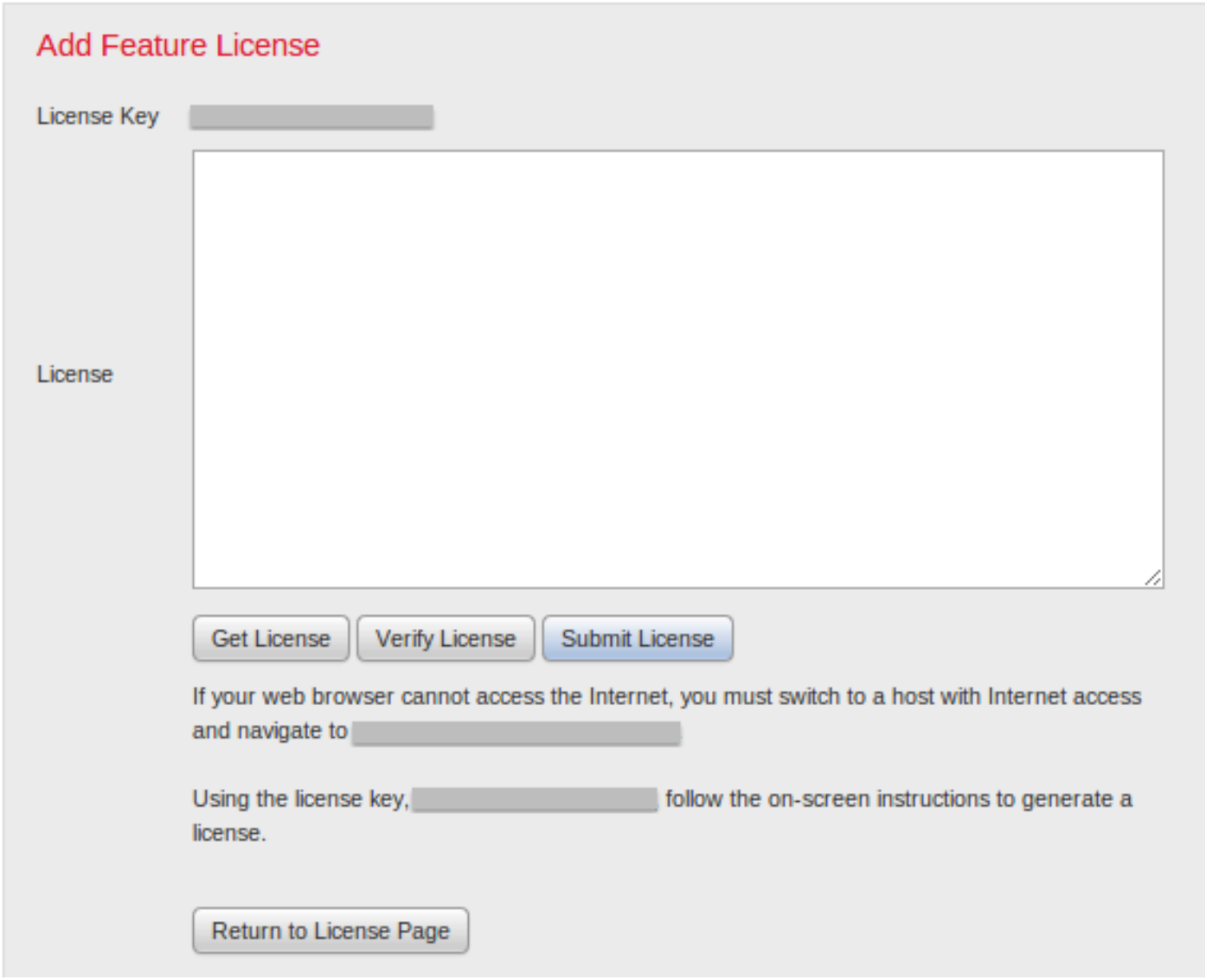

في هذه الصفحة، يمكنك أيضا تسجيل جهاز إلى مركز إدارة FireSIGHT وتحديد وضع اكتشاف. يحدد وضع الكشف والخيارات الأخرى التي تختارها أثناء التسجيل الواجهات الافتراضية والمجموعات المضمنة والمناطق التي ينشئها النظام، بالإضافة إلى النهج التي يطبقها في البداية على الأجهزة التي تتم إدارتها.




## الخطوة 2: تثبيت التراخيص

إذا لم تقم بتثبيت التراخيص أثناء صفحة الإعداد الأولي، فيمكنك إكمال المهمة باتباع الخطوات التالية:

- انتقل إلى الصفحة التالية: **النظام > التراخيص**.
- انقر على **إضافة ترخيص جديد**.




إذا لم تكن قد حصلت على ترخيص، فاتصل بمندوب المبيعات في حسابك.

## الخطوة 3: تطبيق سياسة النظام

يحدد نهج النظام تكوين ملفات تعريف المصادقة ومزامنة الوقت بين FireSIGHT Management Center والأجهزة المدارة. لتكوين سياسة النظام أو تطبيقها، انتقل إلى **النظام > محلي > نهج النظام**. يتم توفير نهج افتراضي للنظام ولكن يجب تطبيقه على أي أجهزة مدارة.

## الخطوة 4: تطبيق السياسة الصحية

يتم إستخدام "نهج الحماية" لتكوين كيفية قيام الأجهزة المدارة بالإبلاغ عن حالتها الصحية إلى "مركز إدارة FireSIGHT". لتكوين النهج الصحي أو تطبيقه، انتقل إلى **الصحة > النهج الصحي**. يتم توفير نهج صحة افتراضي ولكن يجب تطبيقه على أي أجهزة مدارة.

## الخطوة 5: تسجيل الأجهزة المدارة

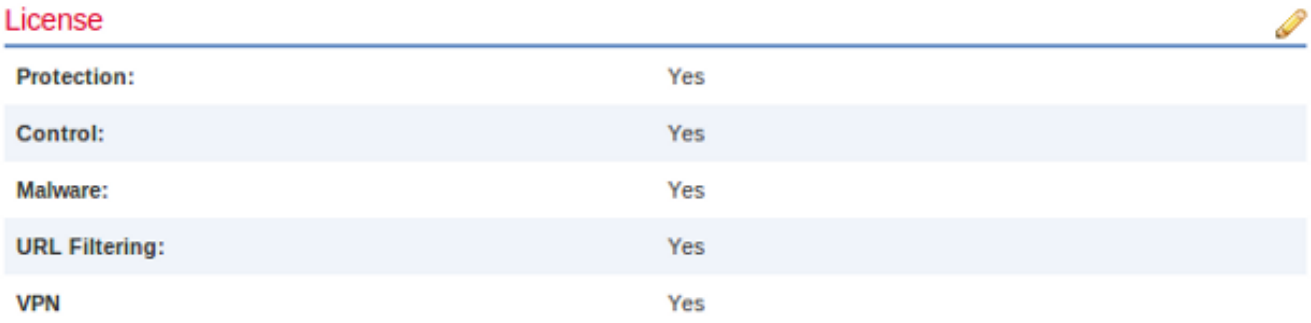
إذا لم تقم بتسجيل الأجهزة أثناء صفحة الإعداد الأولية، فقم بقراءة هذا المستند للحصول على تعليمات حول كيفية

تسجيل جهاز إلى مركز إدارة FireSIGHT.

## الخطوة 6: تمكين التراخيص المثبتة

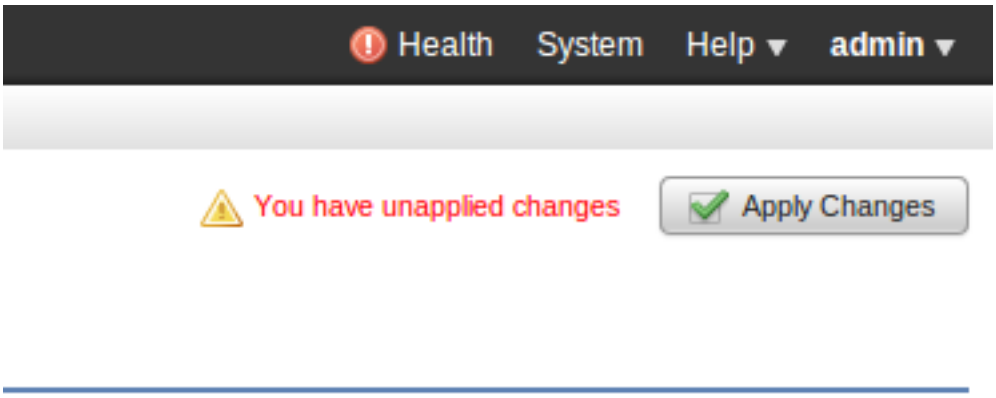
قبل أن تتمكن من إستخدام أي ترخيص ميزة على الجهاز الخاص بك، يلزمك تمكينه لكل جهاز تتم إدارته.

1. انتقل إلى الصفحة التالية: **الأجهزة > إدارة الأجهزة**.
2. انقر فوق الجهاز الذي تريد تمكين التراخيص له وإدخال علامة التبويب "الجهاز".
3. انقر فوق أيقونة **تحرير** (*قلم رصاص*) الموجودة بجوار الترخيص.



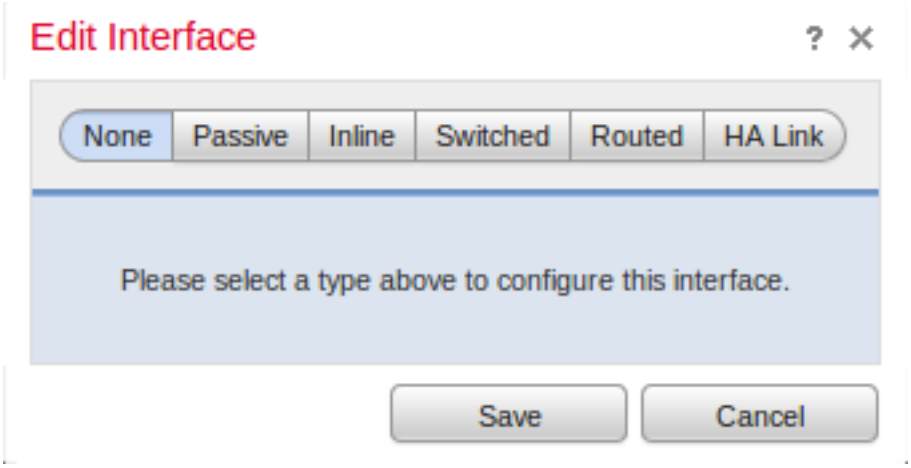

قم بتمكين التراخيص المطلوبة لهذا الجهاز وانقر فوق **حفظ**.

لاحظ الرسالة "*لديك تغييرات غير مطبقة*" في الركن الأيمن العلوي. يبقى هذا التحذير نشطا حتى إذا قمت بالتنقل بعيدا عن صفحة إدارة الأجهزة حتى تقوم بالنقر فوق الزر **تطبيق التغييرات**.




## الخطوة 7: تكوين واجهات الاستشعار

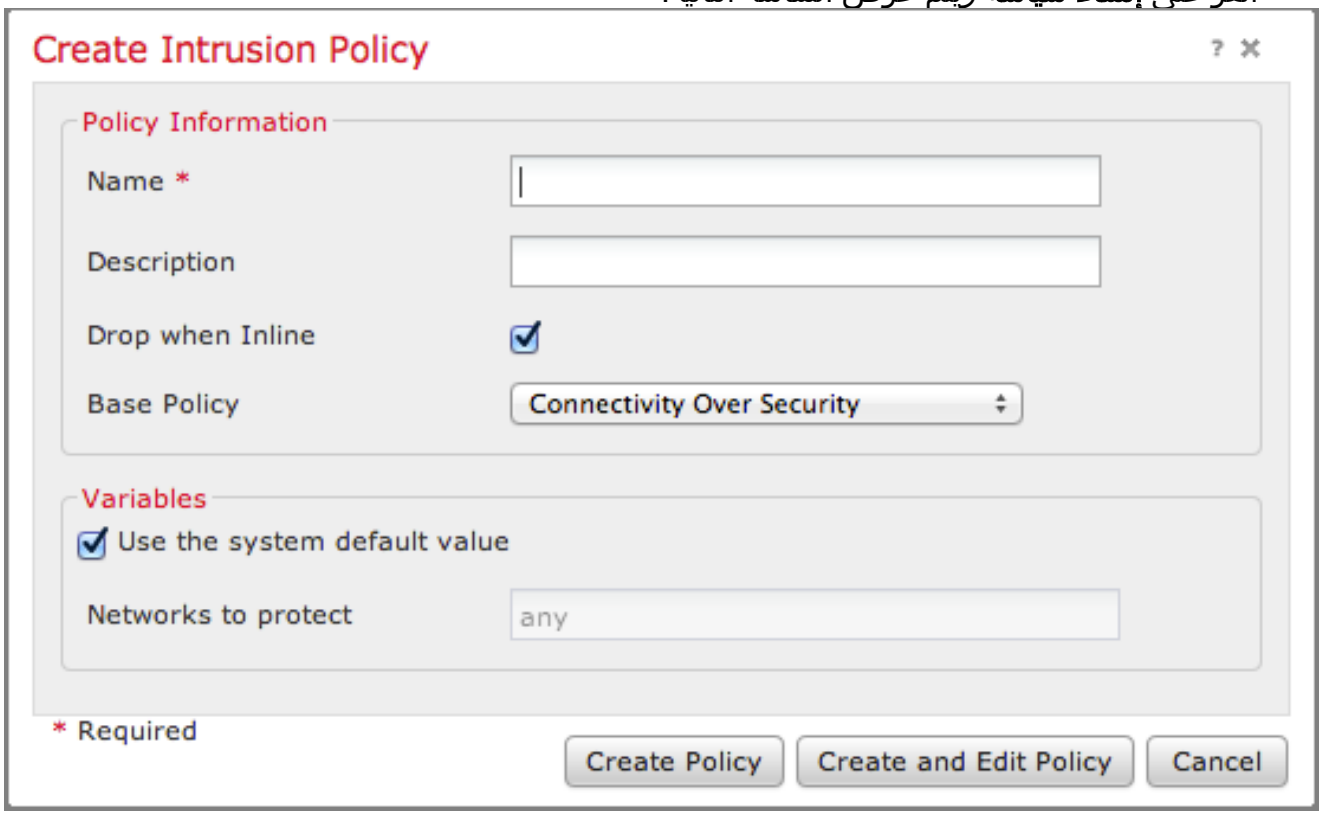
1. انتقل إلى **أجهزة** الصفحة التالية > **إدارة الأجهزة**.
2. انقر أيقونة **تحرير** (القلم الرصاص) للمستشعر الذي تختاره.
3. تحت علامة التبويب **الواجهات**، انقر فوق أيقونة **تحرير** للواجهة التي تختارها.




حدد تكوين واجهة خاملة أو مضمنة. الواجهات المحولة والموجهة خارج نطاق هذه المقالة.

## الخطوة 8: تكوين سياسة التسلل

- انتقل إلى الصفحة التالية: **السياسات > الاقتحام > سياسة الاقتحام.**
- انقر على **إنشاء سياسة** ويتم عرض الشاشة التالية:




يجب تعيين اسم وتحديد النهج الأساسي المراد إستخدامه. على حسب عملية النشر الخاصة بك، يمكنك إختيار خيار **الإسقاط عند** تمكين **الخط الداخلي**. قم بتعريف الشبكات التي تريد حمايتها لتقليل الإيجابيات الخاطئة وتحسين أداء النظام.

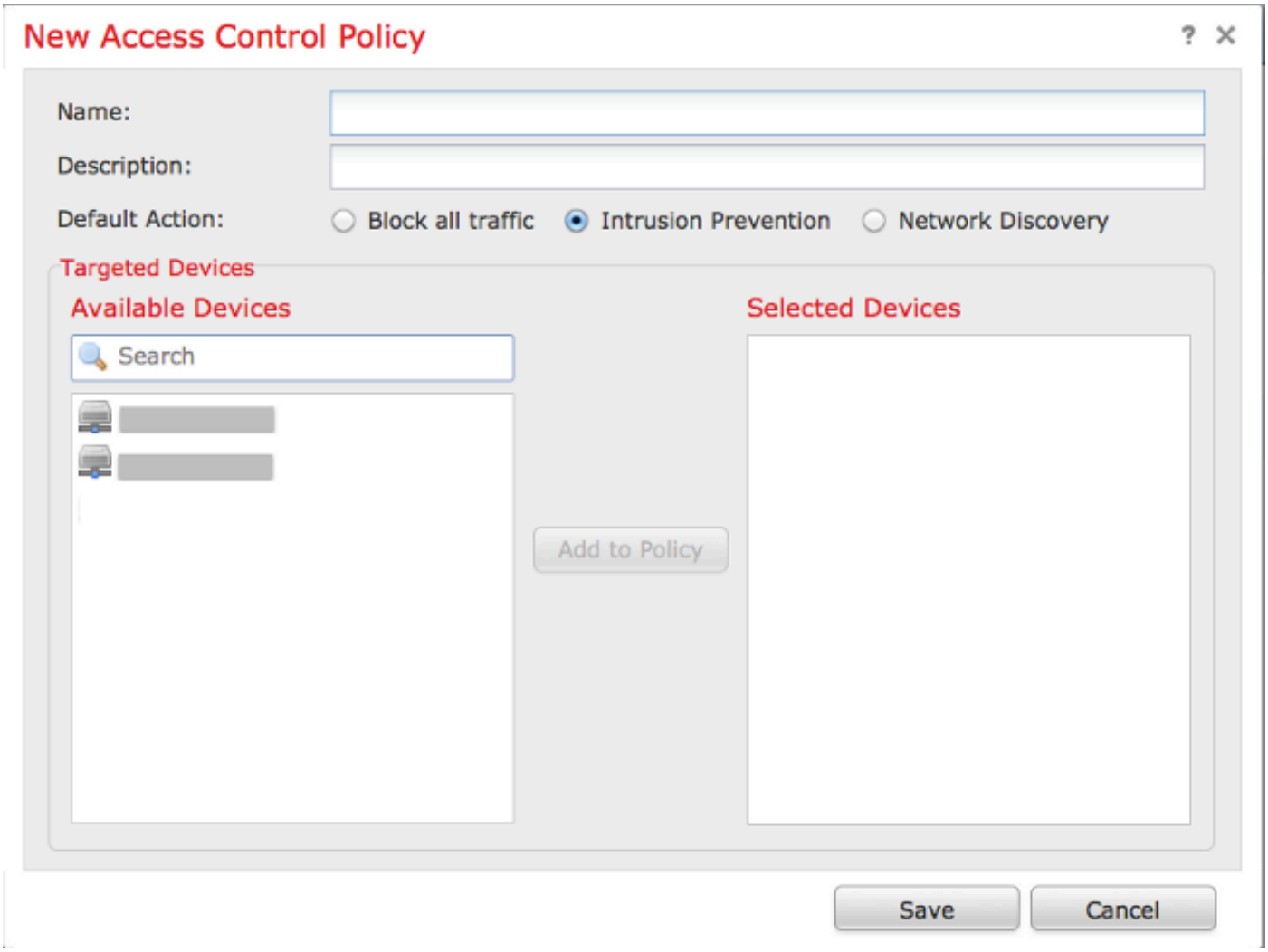
سيؤدي النقر فوق **إنشاء نهج** إلى حفظ الإعدادات وإنشاء نهج IPS. إذا كنت ترغب في إجراء أي تعديل على نهج التطفل، يمكنك إختيار **إنشاء نهج وتحريره** بدلا من ذلك.

**ملاحظة**: يتم تطبيق سياسات التسلل كجزء من سياسة التحكم بالوصول. بعد تطبيق سياسة التطفل، يمكن

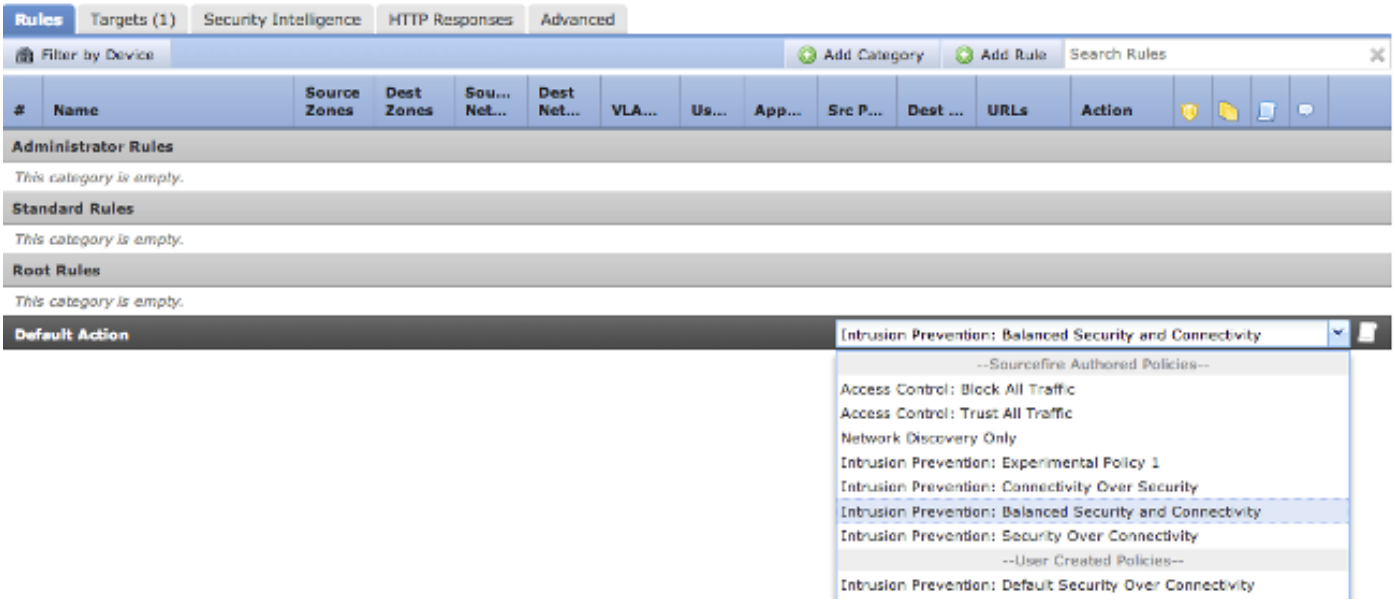
تطبيق أي تعديلات دون إعادة تطبيق سياسة التحكم بالوصول بالكامل عن طريق النقر فوق الزر **إعادة التطبيق**.

## الخطوة 9: تكوين سياسة التحكم في الوصول وتطبيقها

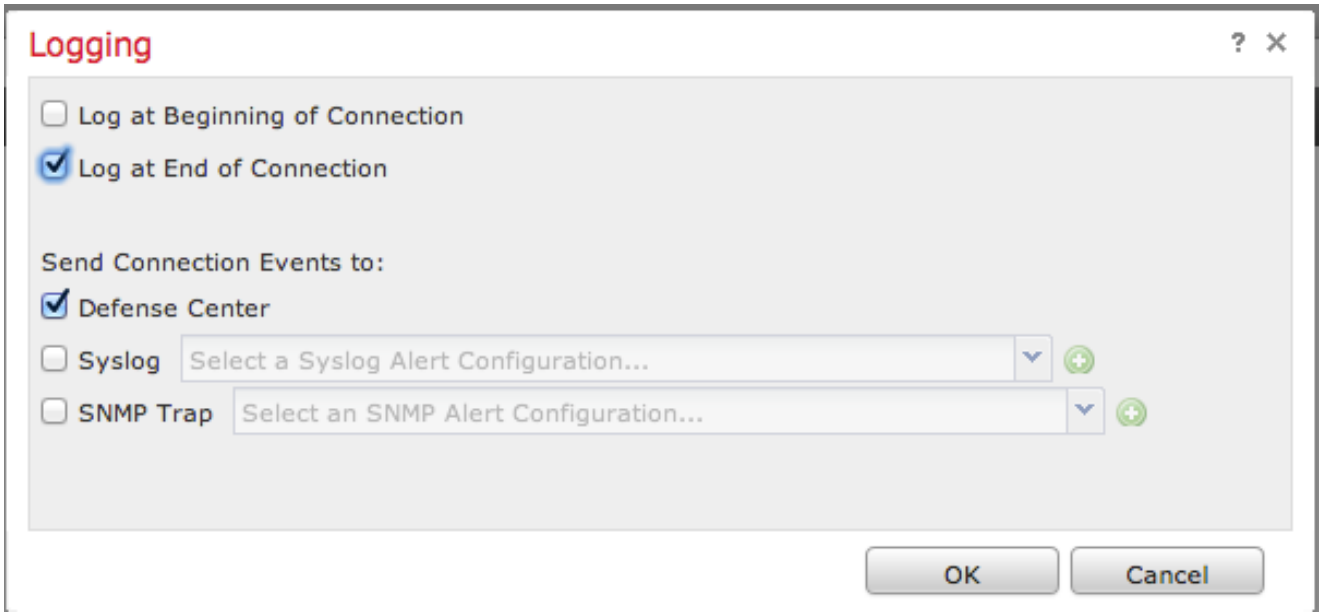
1. انتقل إلى **السياسات > التحكم في الوصول**.
2. انقر فوق **نهج جديد**.




3. قم بتوفير **اسم** للنهج و**الوصف**.
4. حدد **منع التسلل** على أنه **الإجراء الافتراضي** لسياسة التحكم بالوصول.
5. حدد أخيرا **الأجهزة المستهدفة** التي تريد تطبيق نهج التحكم في الوصول عليها، وانقر فوق **حفظ**.
6. حدد سياسة التطفل الخاصة بك للإجراء الافتراضي.




7. يجب تمكين تسجيل الاتصال لإنشاء أحداث الاتصال. انقر فوق القائمة المنسدلة التي تقع على يمين **الإجراء الافتراضي**.



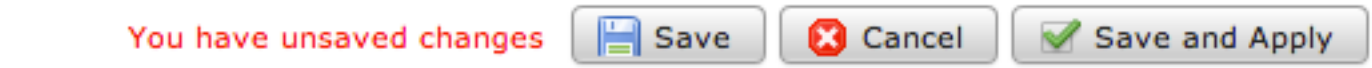

8. أختر تسجيل الاتصالات في بداية الاتصال أو نهايته. يمكن تسجيل الأحداث على FireSIGHT Management Center، أو موقع syslog، أو من خلال SNMP.

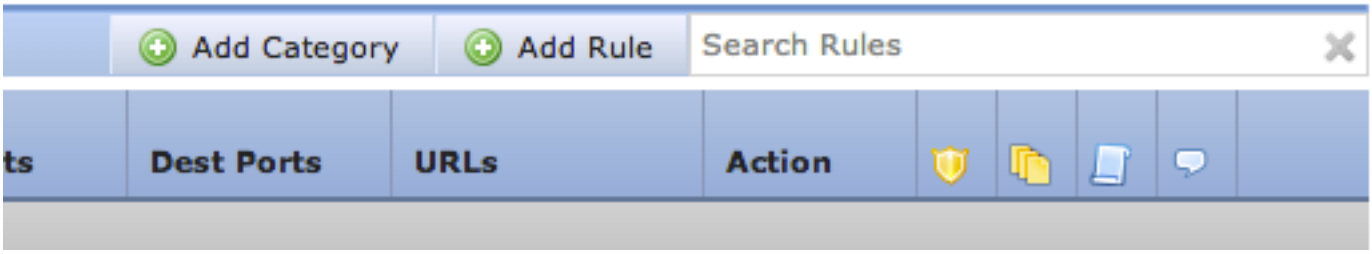
**ملاحظة**: لا يوصى بتسجيل الدخول في طرفي الاتصال لأن كل اتصال (باستثناء الاتصالات المحظورة) سيتم تسجيله مرتين. التسجيل في البداية مفيد للاتصالات التي سيتم حظرها، والتسجيل في النهاية مفيد لجميع الاتصالات الأخرى.

9. انقر فوق **OK**. لاحظ أن لون أيقونة التسجيل قد تغير.

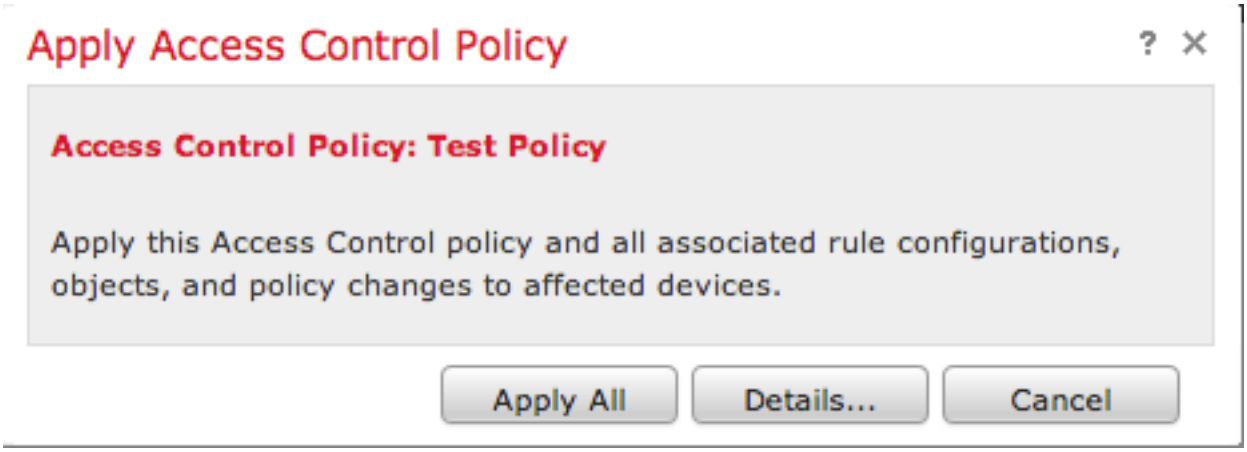
10. يمكنك إضافة **قاعدة التحكم بالوصول** في الوقت الحالي. تعتمد الخيارات التي يمكنك إستخدامها على نوع التراخيص التي قمت بتثبيتها.

11. عند الانتهاء من إجراء التغييرات. انقر فوق الزر **حفظ وتطبيق**. ستلاحظ رسالة تشير إلى أن لديك تغييرات غير محفوظة في النهج الخاص بك في الزاوية العلوية اليمنى حتى يتم النقر فوق الزر.



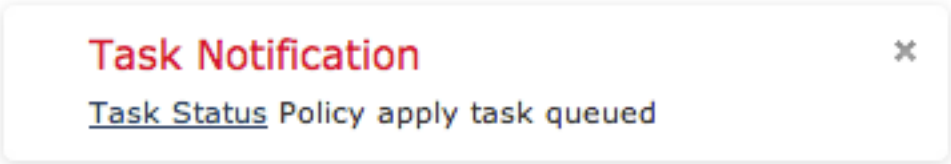

يمكنك إختيار **حفظ** التغييرات فقط أو النقر فوق **حفظ وتطبيق**. تظهر النافذة التالية إذا أخترت الأخيرة.




12. سيقوم **تطبيق الكل** بتطبيق سياسة التحكم في الوصول وأي سياسة (سياسات) إقتحام مرتبطة على الأجهزة المستهدفة.

**ملاحظة**: في حالة تطبيق سياسة التطفل لأول مرة، لا يمكن إلغاء تحديدها.

13. يمكنك مراقبة حالة المهمة التي تنقر فوق إرتباط **حالة المهمة** في الإعلام الموضح في أعلى الصفحة، أو بالانتقال إلى: **نظام > مراقبة > حالة المهمة**




14. انقر فوق الارتباط "حالة المهمة" لمراقبة تقدم تطبيق نهج التحكم بالوصول.

Job Summary

Remove Completed Jobs | Remove Failed Jobs

| | |
|---|---|
| Running | 0 |
| Waiting | 0 |
| Completed | 7 |
| Retrying | 0 |
| Failed | 0 |

Jobs

| Task Description | Message | Creation Time | Last Change | Status | |
|---|---|---|---|---|---|
| **Health Policy apply tasks**<br>0 Running 0 Waiting 1 Completed 0 Retrying 0 Failed | | | | | |
| **Health policy apply to appliance**<br>[redacted]<br>Health Policy Apply | Health Policy applied successfully | 2013-07-19 18:25:39 | 2013-07-19 18:26:42 | Completed | |
| **Policy apply tasks**<br>0 Running 0 Waiting 3 Completed 0 Retrying 0 Failed | | | | | |
| **Apply Default Access Control to**<br>[redacted]<br>Access Control Policy | Access Control Policy applied successfully | 2013-07-19 18:26:04 | 2013-07-19 18:27:12 | Completed | |

### الخطوة 10: التحقق مما إذا كان FireSIGHT Management Center يستقبل الأحداث

بعد اكتمال تطبيق سياسة التحكم بالوصول، يجب أن تبدأ في رؤية أحداث الاتصالات وتبعا لأحداث أختراق حركة المرور.

## توصية إضافية

يمكنك أيضا تكوين الميزات الإضافية التالية على النظام الخاص بك. يرجى الرجوع إلى دليل المستخدم للحصول على تفاصيل التنفيذ.

- النسخ الاحتياطية المجدولة
- التنزيل/التثبيتات التلقائية للبرامج و SRU و VDB و GeoLocation.
- مصادقة خارجية من خلال LDAP أو RADIUS

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).