تنفيذ عمليات مسح IOC لنقطة النهاية باستخدام AMP لنقاط النهاية أو FireAMP

المحتويات

المقدمة

يصف هذا وثيقة كيف أن يخلق إشارة إلى التسوية (IOC) توقيع مبرد من خلال مدير تحرير IOC، كيف أن يرفع هو إلى ال cisco FireAMP لوحة معلومات، وكيف أن يبدأ نقطة نهاية IOC مسح.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن يكون لديك على الأقل جيجابايت واحد من مساحة محرك الأقراص الحرة قبل أن تحاول تشغيل عمليات المسح الضوئي IOC لنقطة النهاية.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى ماسح IOC لنقطة النهاية، والذي يتوفر في إصدارات Cisco FireAMP Windows Connector 4.0.2 والإصدارات الأحدث.

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

معلومات أساسية

إن ميزة ماسح IOC الضوئي لنقطة النهاية هي أداة قوية للاستجابة للحوادث يتم إستخدامها من أجل مسح مؤشرات ما بعد التسوية عبر أجهزة كمبيوتر متعددة.

ملاحظة: على الرغم من أن FireAMP يدعم اللجنة الأوقيانوغرافية الحكومية الدولية بلغة الإدارة، إلا أن برنامج محرر اللجنة الأوقيانوغرافية الحكومية الدولية المسؤول نفسه لم يطوره أو يدعمه Cisco. لا يقوم دعم Cisco باستكشاف أخطاء IOCs التي أنشأها المستخدم أو التي قامت بإنشائها جهة خارجية وإصلاحها.

ملفات توقيع IOC

ملف توقيع IOC هو مخطط XML قابل للتوسيع لوصف الخصائص التقنية التي تحدد التهديد المعروف، منهجية المهاجم، أو دليل آخر على التسوية.

يمكنك إستيراد IOCs لنقطة النهاية من خلال وحدة التحكم من الملفات المستندة إلى OpenIOC والتي تتم كتابتها لتشغيل خصائص الملف مثل الاسم والحجم والتجزئة، بالإضافة إلى سمات أخرى وخصائص النظام مثل معلومات العملية والخدمات قيد التشغيل وإدخالات سجل Microsoft Windows. يمكن إستخدام اللجنة الأوقيانوغرافية الحكومية الدولية من قبل المستجيبين للحوادث من أجل العثور على قطع أثرية معينة أو من أجل إستخدام المنطق لإنشاء عمليات كشف معقدة ومترابطة لعائلات البرامج الضارة.

تشغيل المسح الضوئي على ملف توقيع IOC

هناك ثلاث خطوات يجب عليك إكمالها لتشغيل المسح الضوئي على ملف توقيع IOC:

1. إنشاء ملف توقيع IOC.
2. تحميل ملف توقيع IOC.
3. ابدأ الفحص.

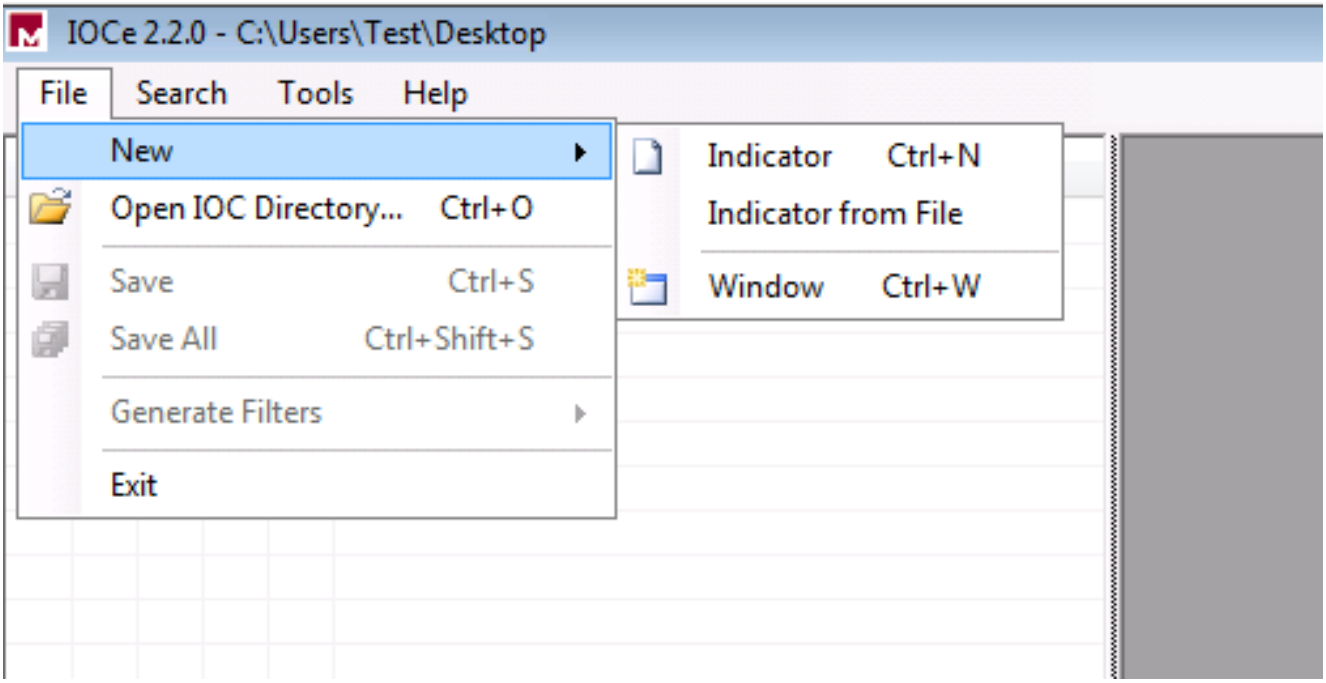
ويجري توسيع نطاق هذه الخطوات في الأقسام التالية.

إنشاء ملف توقيع IOC

ملاحظة: في هذا المثال، يتم إستخدام محرر IOC المتنقل لإنشاء ملف توقيع IOC لملف نصي يسمى **test.txt**.

أكمل الخطوات التالية لإنشاء ملف توقيع IOC:

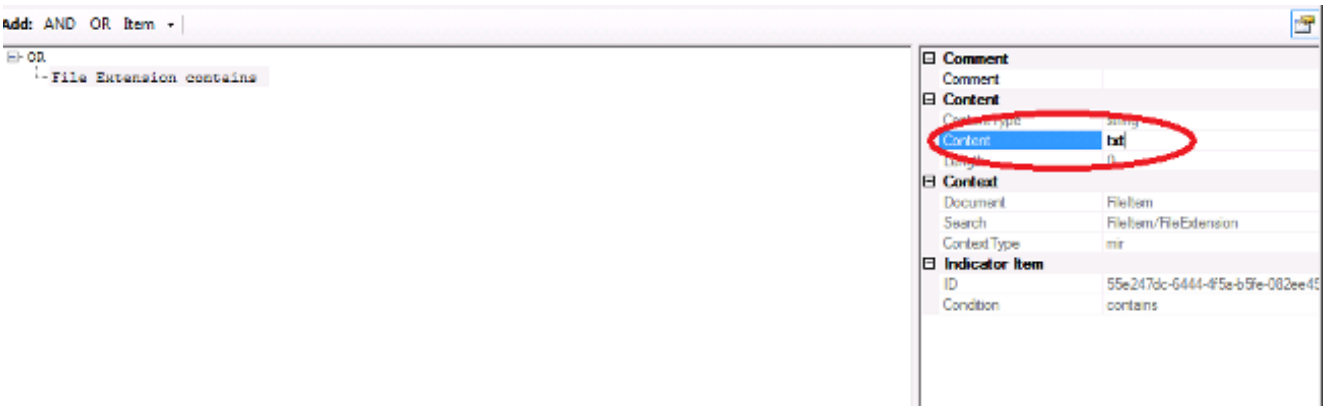
1. افتح **IOCe** وتصفح إلى **ملف > جديد > مؤشر**. يوفر ذلك مساحة عمل فارغة بحيث يمكنك البدء في بناء IOC.



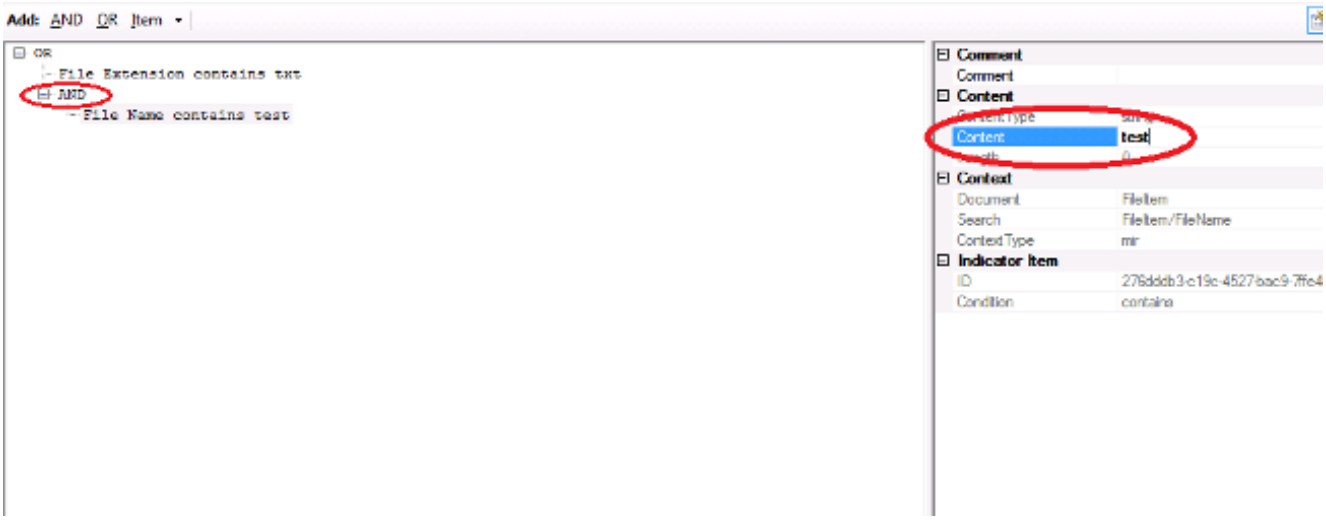
ملاحظة: من أجل إنشاء IOC لشئ محدد، أستخدم المنطق الثنائي مع الخصائص. المشغل الأولي هو OR، وهو أبسط قاعدة للعمل من. وهذا يسمح للوظيفة الأولية للجنة الأوقيانوغرافية الحكومية الدولية بالعمل، لذلك لا يطلب منك تغييرها. من المطلوب أن يحتوي ملف توقيع IOC على خصائص أو شروط على الأقل لاستخدامها بنجاح في المسح الضوئي.

2. انقر فوق القائمة المنسدلة **العناصر** لإضافة عوامل تشغيل. الخاصية الأولى التي يجب إضافتها هي **File Extension (ملحق الملف)**. ابحث عن الخاصية في قائمة شجرة **العناصر** وانقر فوقها.

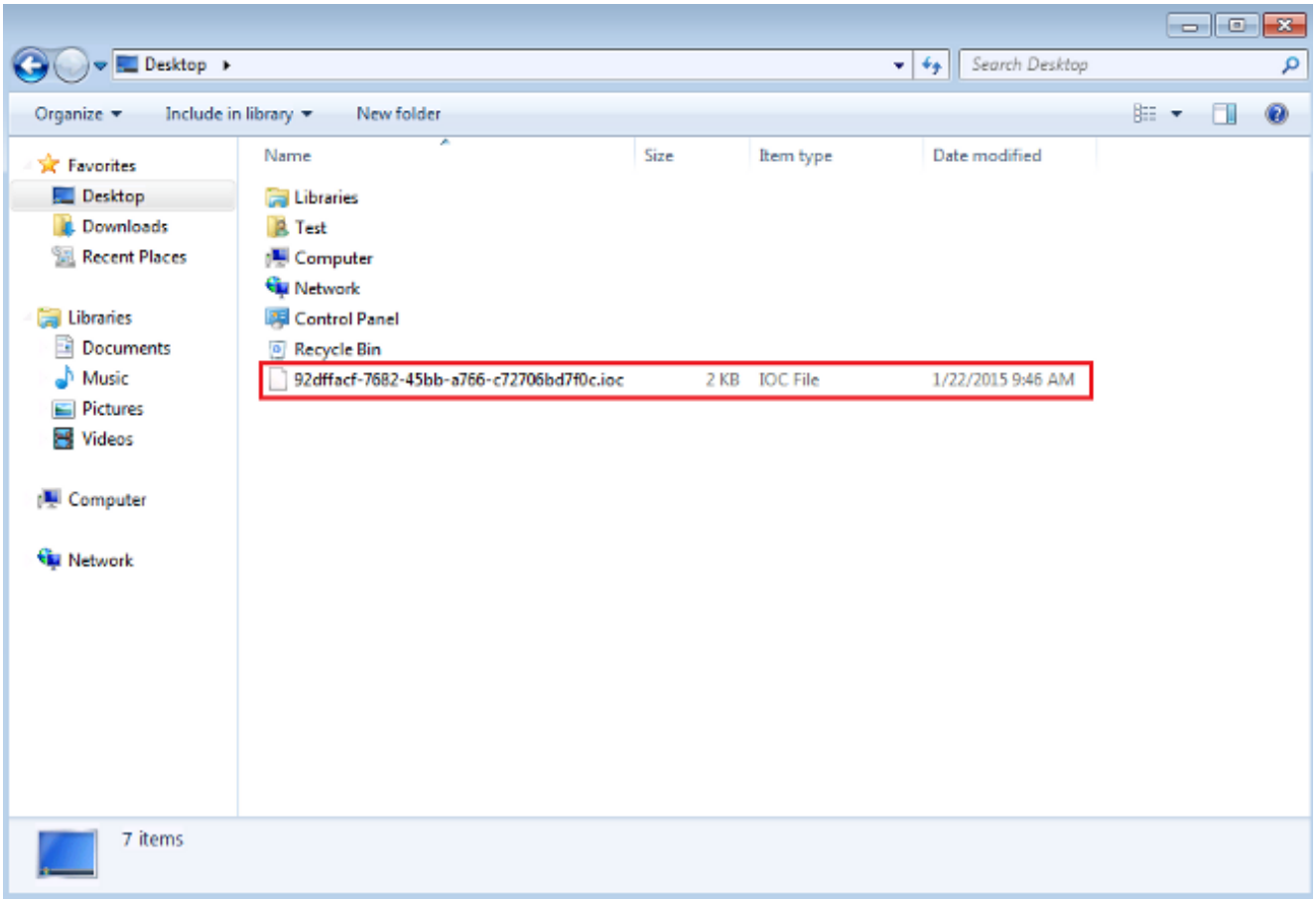
3. بعد إضافة خاصية، انقر فوق الأيقونة الصغيرة الموجودة في أقصى الجانب الأيمن من الشاشة لفتح جزء التكوين. ضمن هذا الجزء، أستخدم حقل **المحتوى** لمطابقة ملحق ملف. على سبيل المثال، أضف **txt** لمطابقة الملف النصي **test.txt**:



4. يجب أن تقوم الآن بإضافة عامل تشغيل منطق. في هذا المثال، ستطابق ملف **إختبار** النص. ولمطابقة هذا الأمر، أستخدم مشغل *AND* وأضف الخاصية التالية. حدد مكان اسم الملف وحدده من قائمة شجرة **العناصر**. في جزء "الخصائص"، قم بإضافة اسم الملف الذي تريد البحث عنه. على سبيل المثال، أضف **إختبار** في حقل المحتوى:



5. بما أنه لا توجد خصائص إضافية لازمة للجنة الأوقيانوغرافية الحكومية الدولية البسيطة، يمكنك الآن حفظ الملف. انقر فوق **ملف > حفظ**، ويتم حفظ ملف توقيع بملحق **.ioc** على النظام:



تحميل ملف توقيع IOC

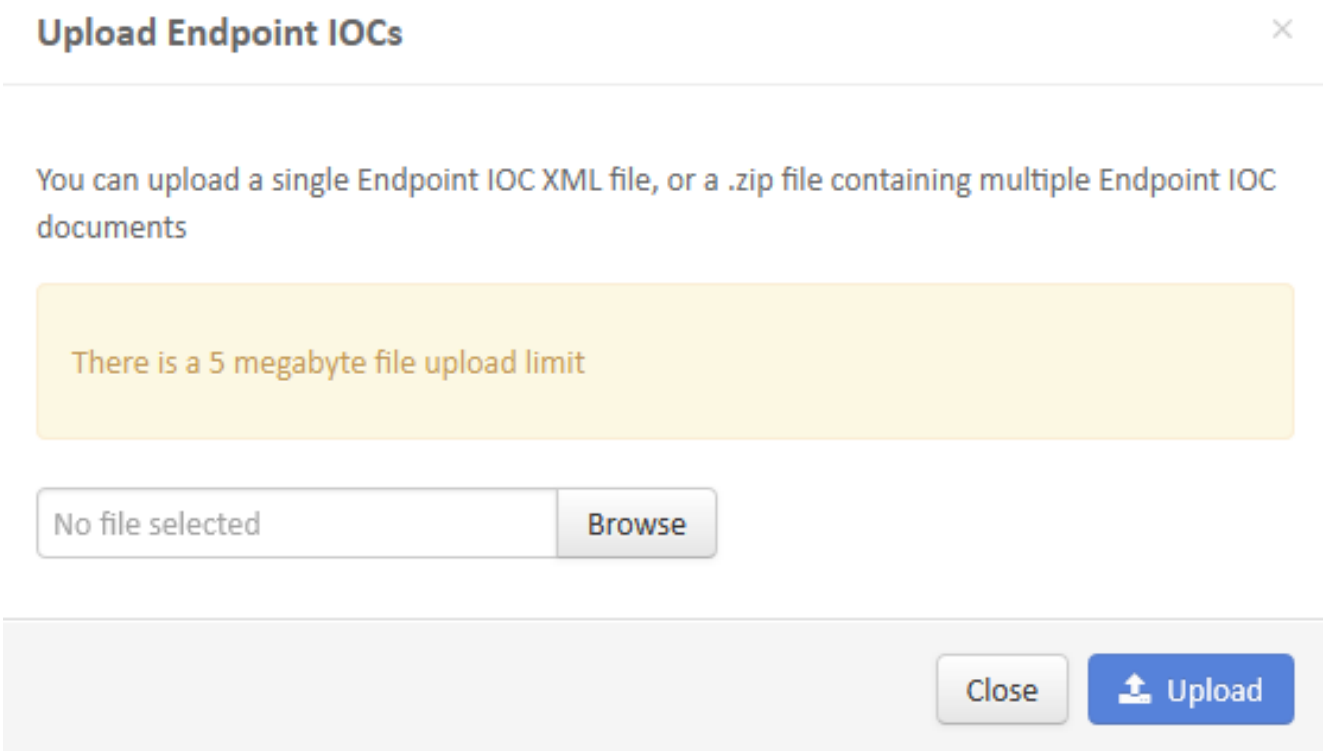
لإجراء مسح ضوئي، يجب تحميل ملف IOC إلى لوحة معلومات FireAMP. يمكنك إستخدام ملف توقيع IOC، ملف XML، أو أرشيف ZIP يحتوي على ملفات IOC متعددة. تقوم لوحة المعلومات بإلغاء ضغط الملف وتحليله باستخدام توقيعات IOC. يتم إخطارك في حالة إستخدام بناء جملة غير صحيح أو خاصية غير مدعومة.

تلميح: يمكنك تحميل الملفات التي يصل حجمها إلى 5 ميغابايت.

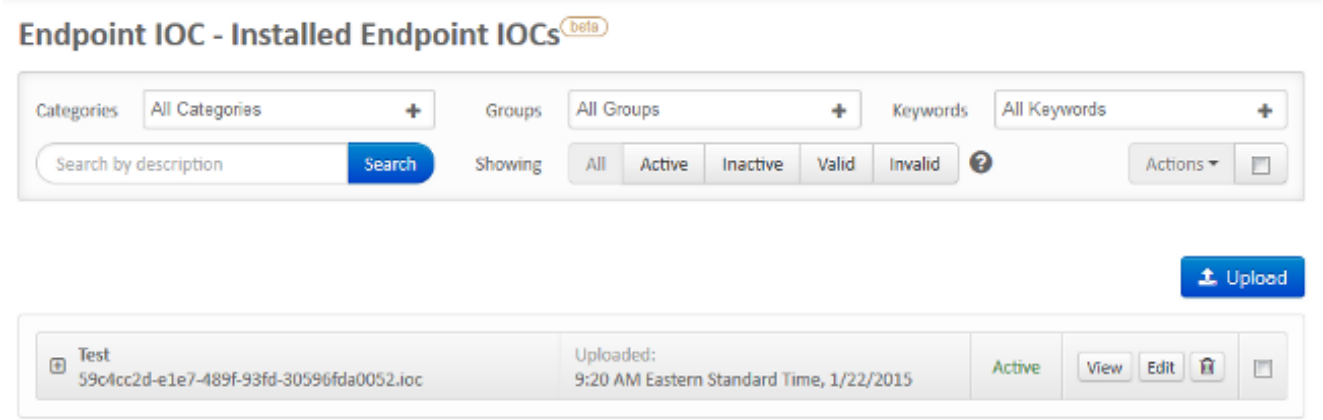
أكمل الخطوات التالية لتحميل ملف توقيع IOC إلى لوحة معلومات FireAMP:

1. قم بتسجيل الدخول إلى وحدة تحكم سحابة FireAMP وانتقل إلى **التحكم في التفشي > نقطة النهاية المثبتة**. **IOC**.

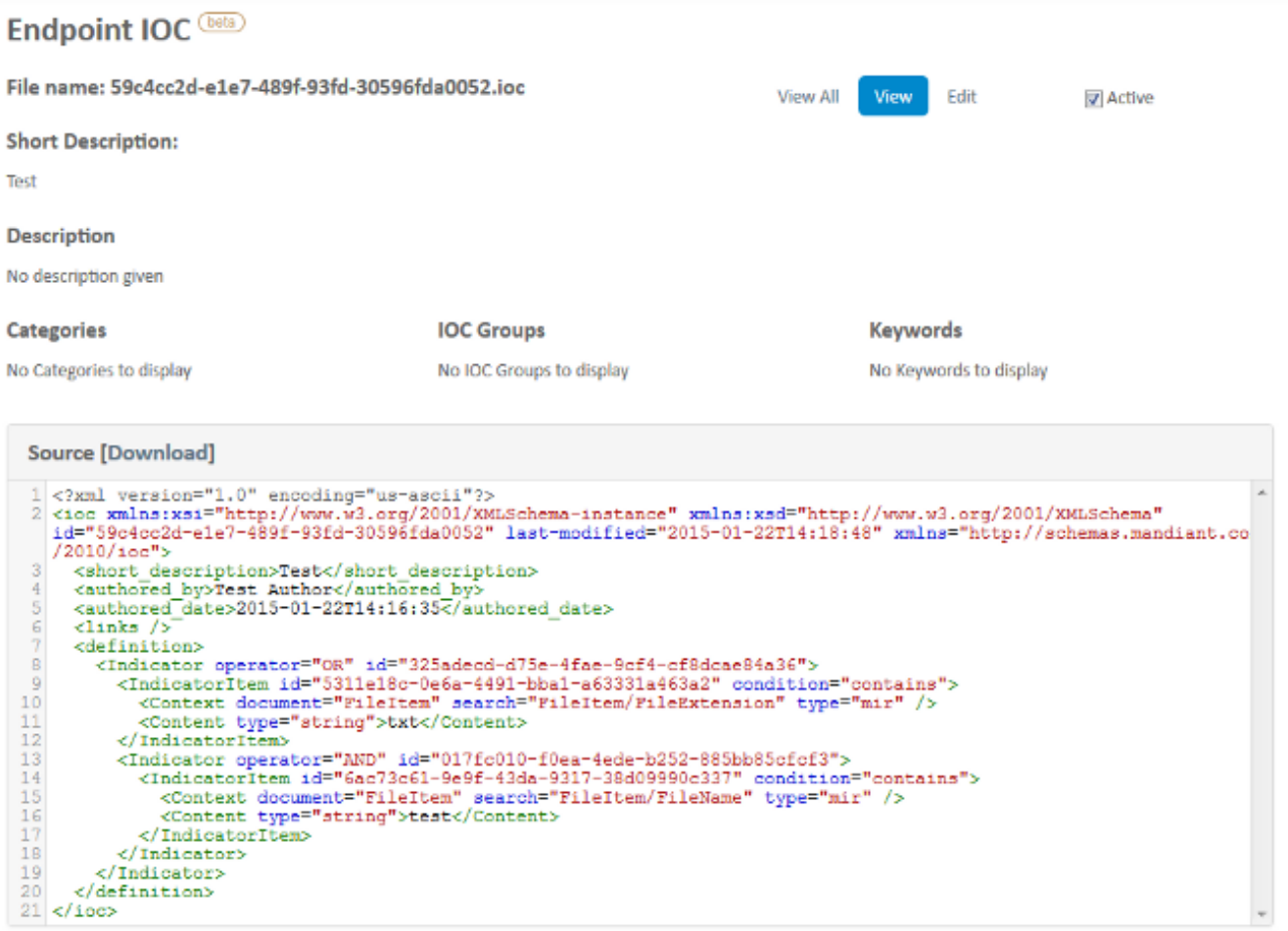
2. انقر **تحميل**، وتظهر نافذة **تحميل نقطة النهاية IOCs**:



بعد تحميل ملف توقيع IOC بنجاح، يظهر التوقيع على القائمة:



3. انقر فوق **عرض** لعرض بيانات XML الفعلية للتوقيع:



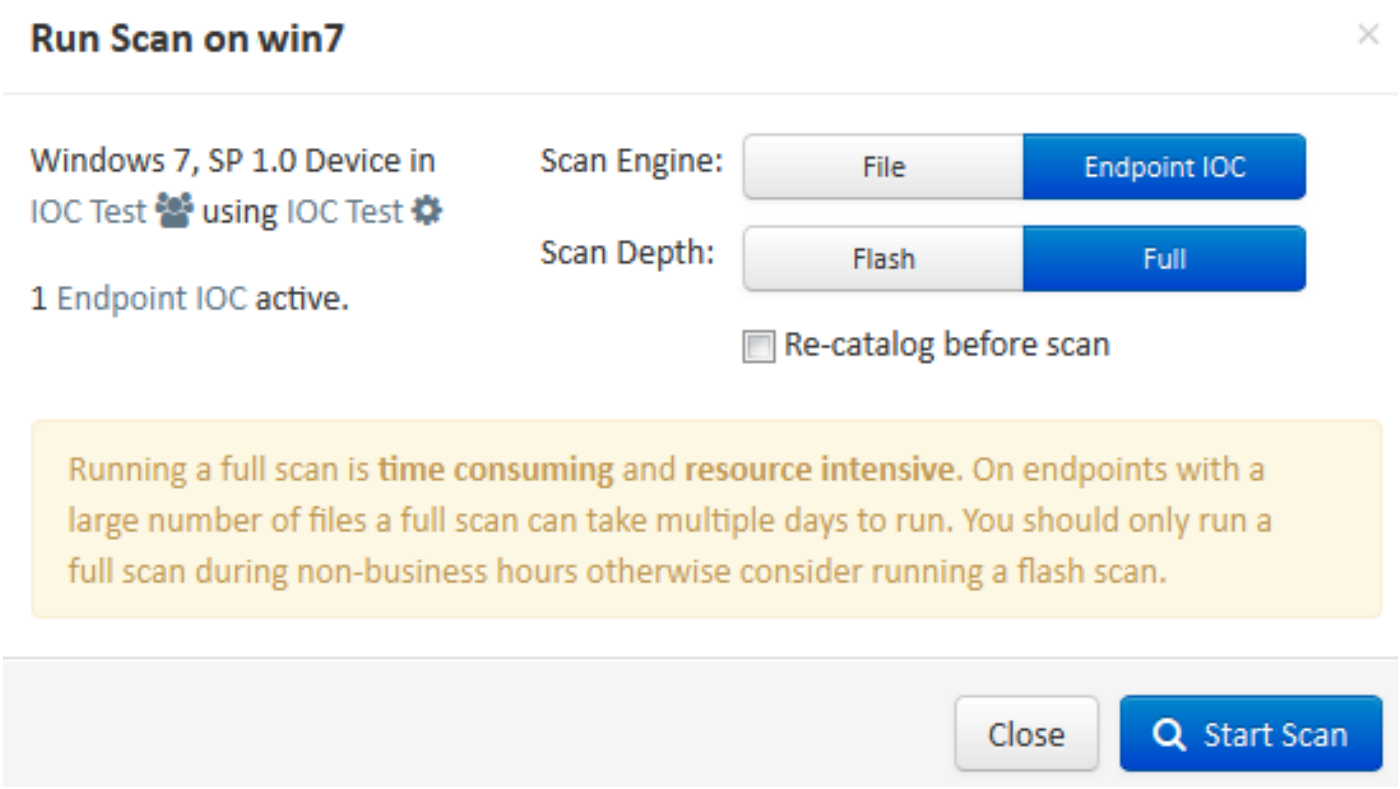
بدء الفحص

بعد تحميل ملف توقيع، قم بإجراء فحص *كامل*. يجب أن يكون الفحص الأول مسحا ضوئيا كاملا لأنه يجب أن يقوم بإنشاء كتالوج بيانات تعريف للكمبيوتر بأكمله، والذي قد يستغرق من ساعة إلى ساعتين. يمكنك إجراء مسح *فلاش* بعد فهرسة النظام من خلال مسح كامل.

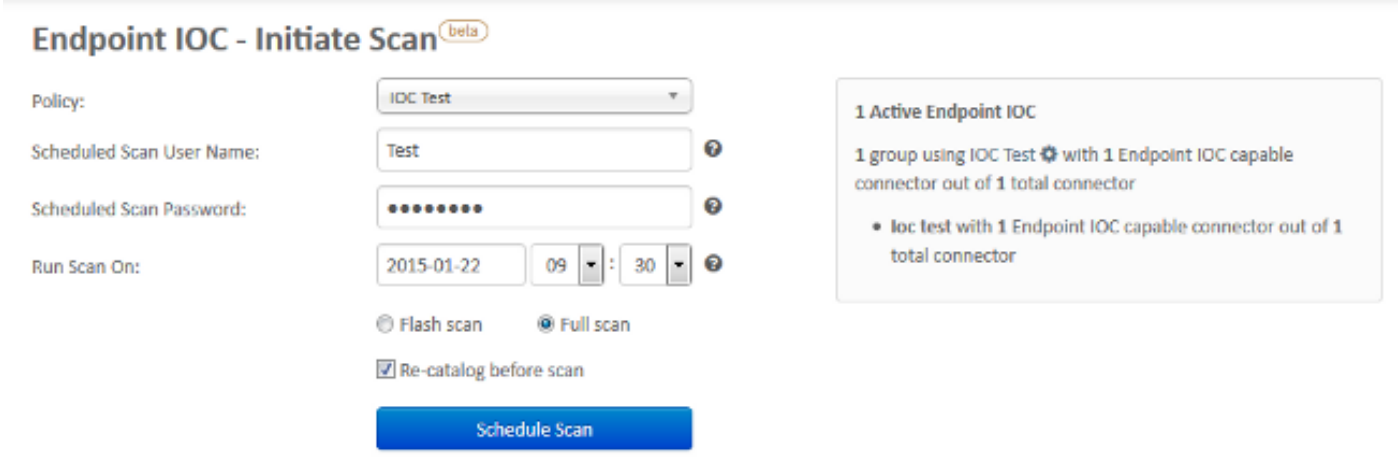
ملاحظة: يعد الفحص الكامل مكثفا جدا لوحدة المعالجة المركزية. توصي Cisco بعدم تشغيل فحص كامل على جهاز كمبيوتر أثناء إستخدامه. إذا كنت تخطط لاستخدام الميزة بشكل منتظم، فيمكنك إجراء فحص كامل مرة في الشهر لإعادة إنشاء الكتالوج.

هناك طريقتان مختلفتان يمكنك إستخدامهما لتشغيل مسح IOC. تتمثل الطريقة الأولى في إجراء فحص فوري للحدث أو من لوحة المعلومات. يتم تشغيل هذا في المرة التالية التي يرسل فيها جهاز كمبيوتر نبضات القلب إلى السحابة.

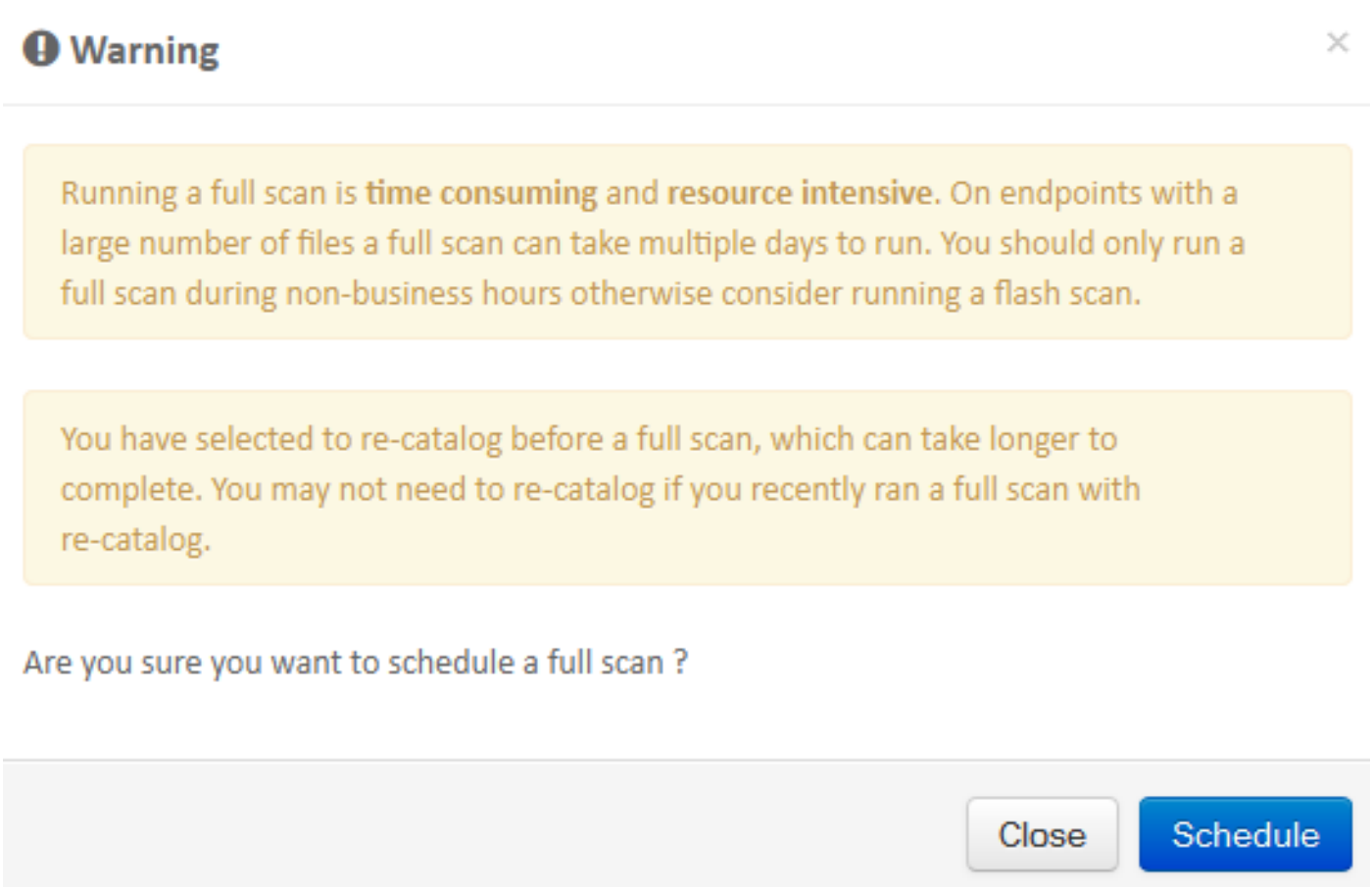
ملاحظة: إذا كانت هذه هي المرة الأولى التي تقوم فيها بتشغيل الفحص الكامل، فلن يطلب منك التحقق من **إعادة الكتالوج قبل** خيار **المسح الضوئي**.



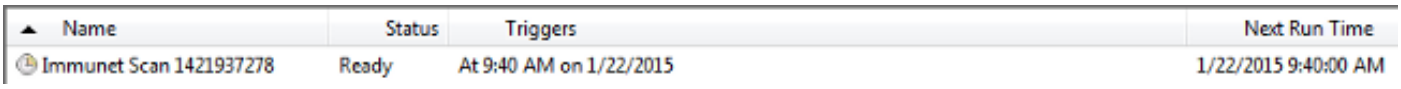
الطريقة الثانية هي إنشاء نقطة نهاية مجدولة مسح IOC من قائمة **التحكم في التفشي** الخاصة بلوحة المعلومات. قد يكون هذا الخيار مثاليا عندما ترغب في إجراء عمليات مسح ضوئي أثناء ساعات غير الذروة. يجب توفير بيانات اعتماد حساب لديه إذن على الكمبيوتر المحدد لإنشاء مهام مجدولة والسماح **بتسجيل الدخول** ك إذن نهج مجموعة **دفعات**.



عندما تقوم بجدولة نقطة نهاية مسح IOC، تظهر رسالة التحذير هذه:

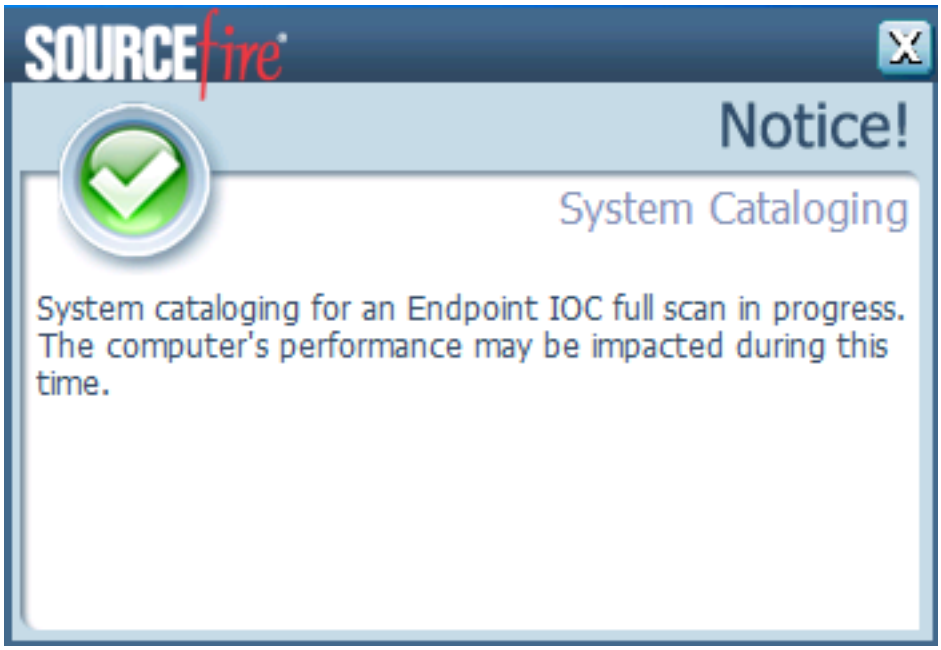


في المرة التالية التي يرسل فيها جهاز الكمبيوتر الخاص بك ضربات القلب، وإذا كانت بيانات اعتمادك صالحة، فيجب أن ترى مهمة مماثلة لهذه في "مجدول مهام Windows":

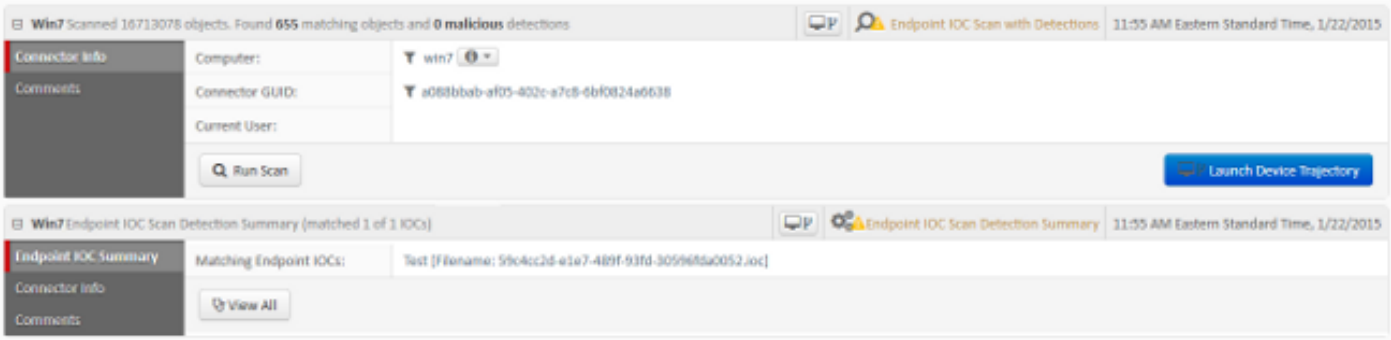


عندما يبدأ الفحص، تظهر هذه الرسالة:

ملاحظة: إذا تم تكوين واجهة المستخدم الرسومية (GUI) لتكون مخفية، فلن ترى إشعار **فهرسة النظام**.



عند اكتمال المسح، يمكنك عرض *ملخص اكتشاف المسح الضوئي ل Endpoint IOC*. يوضح هذا المثال تطابقا لملف توقيع IOC **Test.txt**:



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).