تكوين سياسة ملف AMP واختباراه عبر FDM

المحتويات

المقدمة

يوضح اذه المستند كيفية تكوين سياسة ملف "الحماية المتقدمة من البرامج الضارة" (AMP) واختباراه عبر برنامج Firepower Device Manager (FDM).

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- مدير جهاز Firepower (FDM)
- Firepower Threat Defense (FTD)

المكونات المستخدمة

- برنامج FTD الظاهري الإصدار 7.0 من Cisco المدار من خلال FDM
- ترخيص التقييم (يستخدم ترخيص التقييم لأغراض العرض التوضيحي. تتمثل توصية Cisco في الحصول على ترخيص صالح واستخدامه)

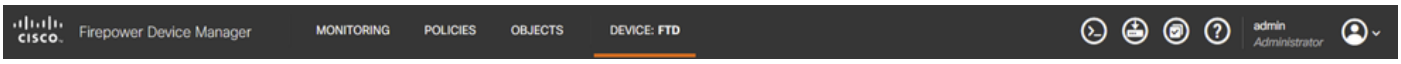
تم إنشاء المعلومات الواردة في اذه المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في اذه المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

تعليمات

الترخيص

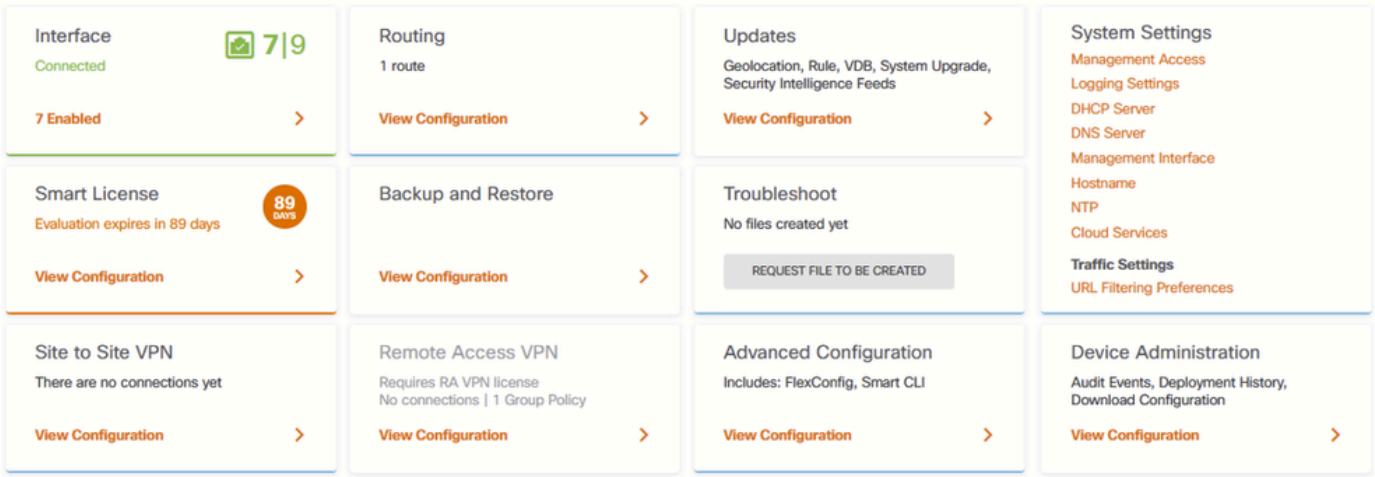
1. لتمكين ترخيص البرامج الضارة، انتقل إلى صفحة الجهاز على واجهة المستخدم

الرسومية (GUI) ل FDM.



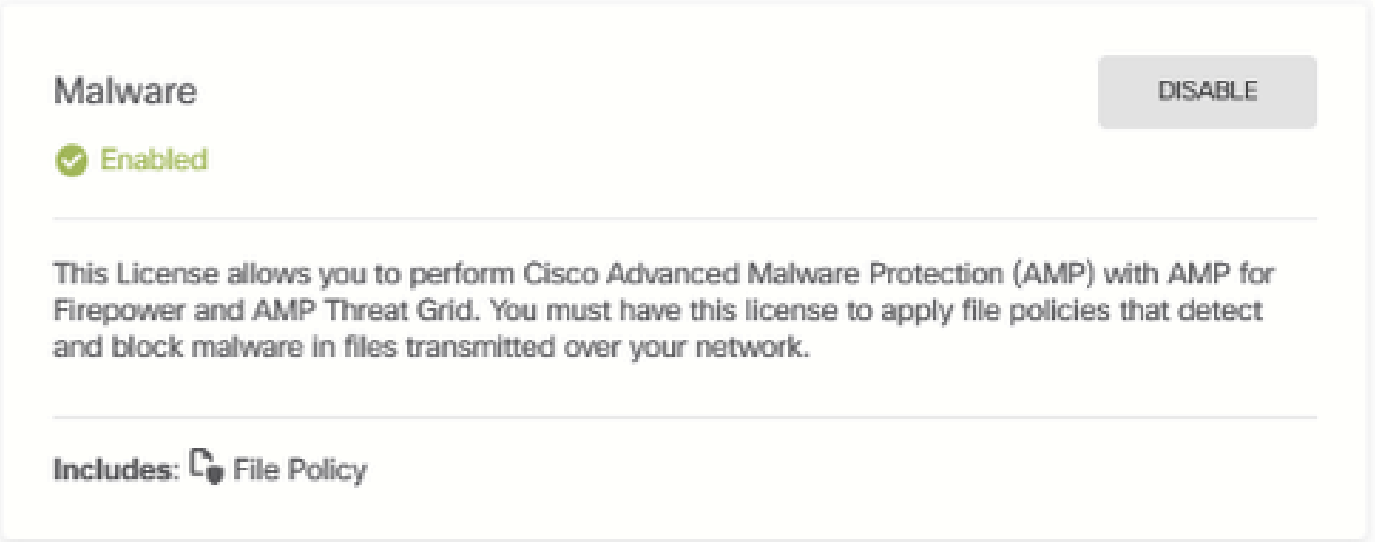
علامة تبويب جهاز FDM

2. حدد مكان المربع المسمى Smart License وانقر فوق عرض التكوين.



صفحة جهاز FDM

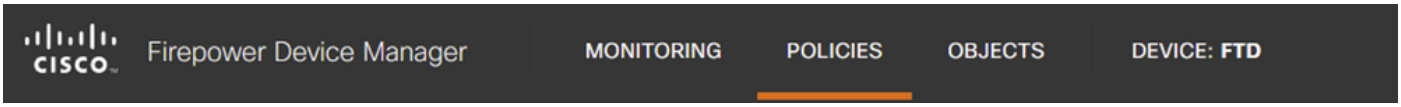
3. قم بتمكين الترخيص المسمى البرامج الضارة.



ترخيص البرامج الضارة

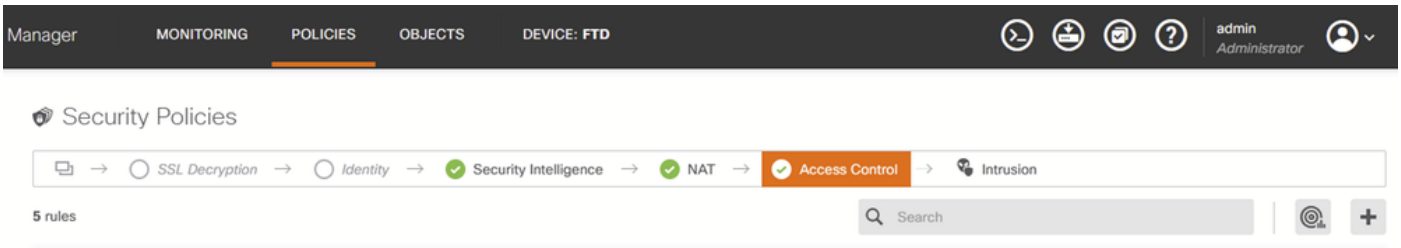
التكوين

1. انتقل إلى صفحة السياسات في FDM.



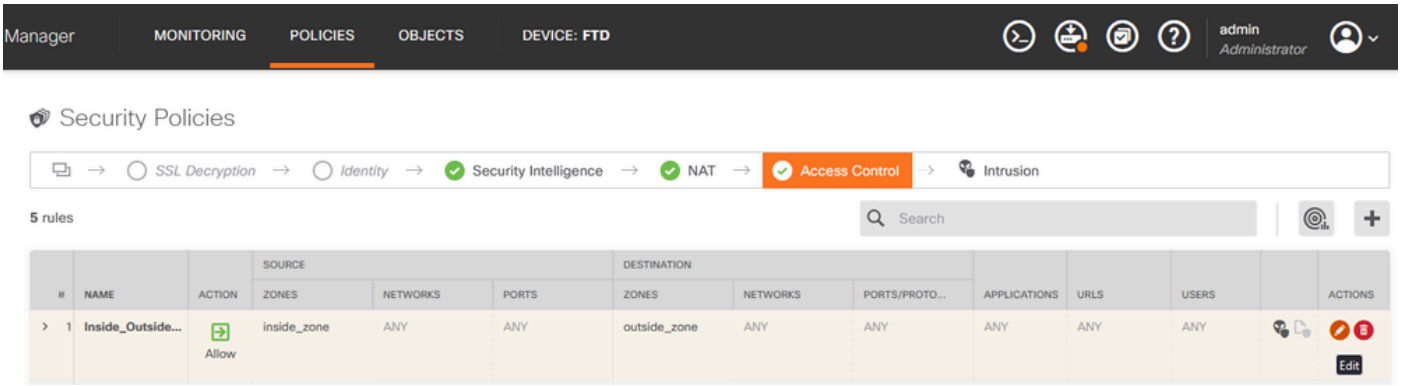
علامة التبويب سياسات FDM

2. تحت سياسات الأمان، انتقل إلى قسم التحكم في الوصول.



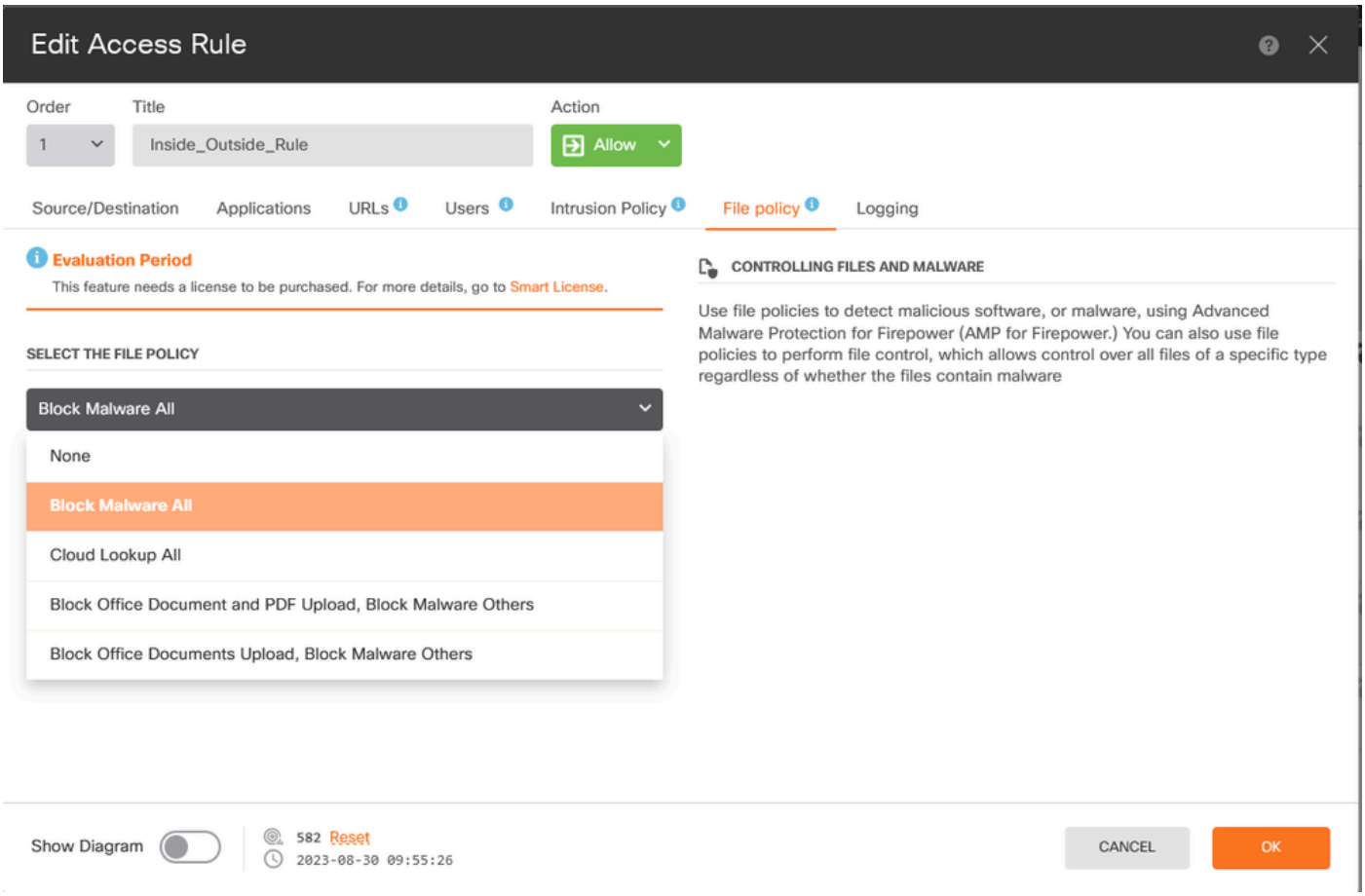
علامة تبويب التحكم في الوصول إلى FDM

3. البحث عن قاعدة وصول أو إنشاؤها لتكوين نهج الملف. انقر فوق محرر قاعدة الوصول. للحصول على تعليمات حول كيفية إنشاء قاعدة وصول، ارجع إلى هذا الارتباط.



قاعدة التحكم في الوصول إلى FDM

4. انقر فوق قسم نهج الملف في قاعدة الوصول وحدد الخيار نهج الملف المفضل من القائمة المنسدلة. انقر فوق موافق لحفظ التغييرات التي تم إجراؤها على القاعدة.



عالمة التبويب "سياسة ملف قاعدة التحكم بالوصول ل FDM"

5. تأكد من تطبيق نهج الملف على قاعدة الوصول عن طريق التحقق من تمكين أيقونة نهج الملف.

تم تمكين رمز نهج ملف

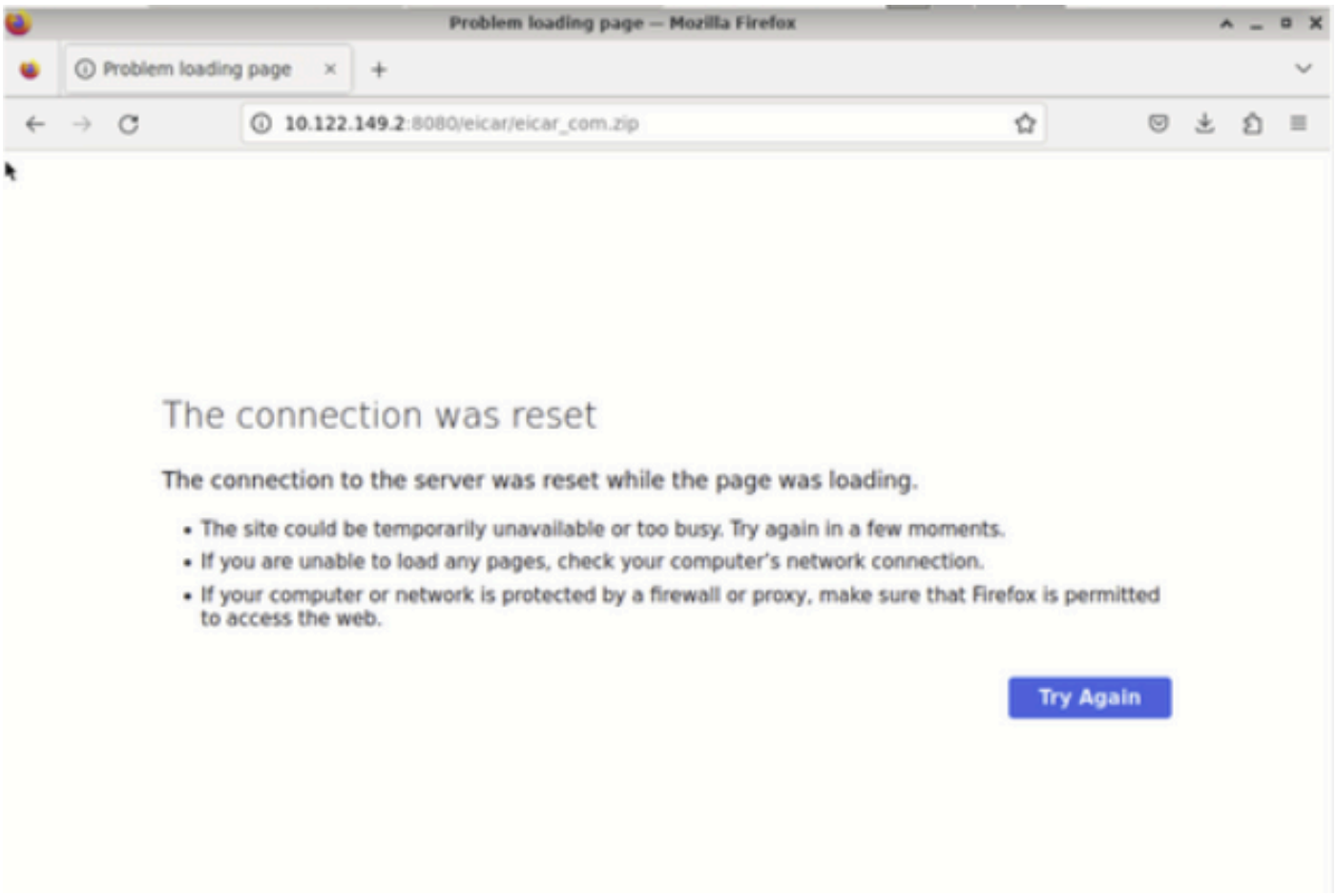
الملف

6. حفظ ونشر التغييرات على الجهاز المدار.

إختبار

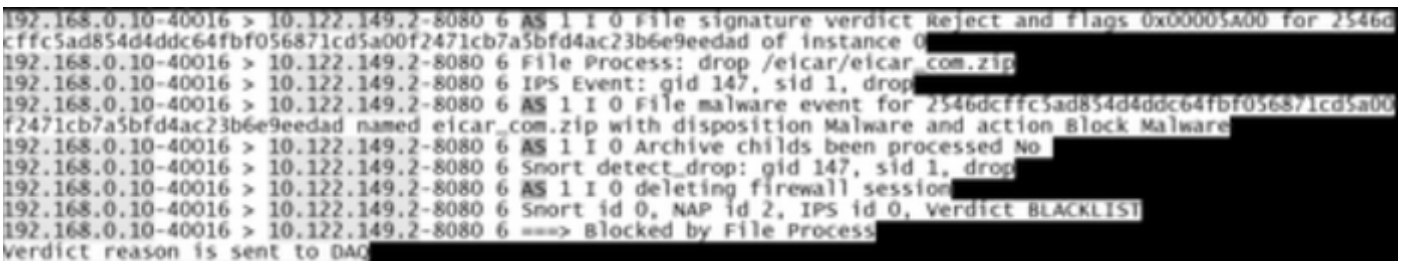
للتحقق من أن نهج الملف الذي تم تكوينه لحماية البرامج الضارة يعمل، أستخدم محاولات سيناريو الاختبار هذه لتنزيل ملف إختبار برنامج ضار من مستعرض ويب الخاص بمضيف نهائي.

كما هو معروض في لقطة الشاشة هذه، فإن محاولة تنزيل ملف إختبار برنامج ضار من مستعرض الويب غير ناجحة.



اختبار تنزيل المستعرض

من واجهة سطر أوامر (CLI) لـ FTD، يظهر تتبع دعم النظام أن تنزيل الملف تم حظره بواسطة عملية الملف. للحصول على تعليمات حول كيفية تشغيل تتبع دعم النظام عبر واجهة سطر الأوامر (CLI) الخاصة بـ FTD، ارجع إلى هذا الارتباط.



اختبار تتبع دعم النظام

هذا يؤكد نجاح تكوين نهج الملف في حظر البرامج الضارة.

استكشاف الأخطاء وإصلاحها

في حالة عدم حظر البرامج الضارة بنجاح عند إستخدام التكوينات السابقة، ارجع إلى اقتراحات أستكشاف الأخطاء وإصلاحها التالية:

1. التحقق من عدم انتهاء صلاحية ترخيص البرامج الضارة.

2. تأكد من أن قاعدة التحكم بالوصول تستهدف حركة مرور صحيحة.

3. تأكد من أن خيارات المجال المحددة صحيحة لحركة المرور المستهدفة والحماية المطلوبة من البرامج الضارة.

إذا كانت المشكلة لا تزال غير قابلة للحل، فاتصل بـ TAC من Cisco للحصول على دعم إضافي.

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).