تكوين معالجة Firepower 6.1 pxGrid باستخدام ISE

المحتويات

المقدمة

يوضح هذا المستند كيفية تكوين حل Firepower 6.1 pxGrid باستخدام محرك خدمات الهوية (ISE). يمكن إستخدام وحدة معالجة ISE Firepower 6.1+ مع خدمة حماية نقطة نهاية ISE (EPS) لأتمتة البطاقة/القائمة السوداء للمهاجمين على طبقة الوصول إلى الشبكة.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة أساسية بالمواضيع التالية:

- Cisco ISE
- Cisco Firepower

المكونات المستخدمة

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

- Cisco ISE، الإصدار 2.0 Patch 4
- Cisco Firepower 6.1.0
- وحدة التحكم في شبكة LAN اللاسلكية الظاهرية (vWLC) 8.3.102.0

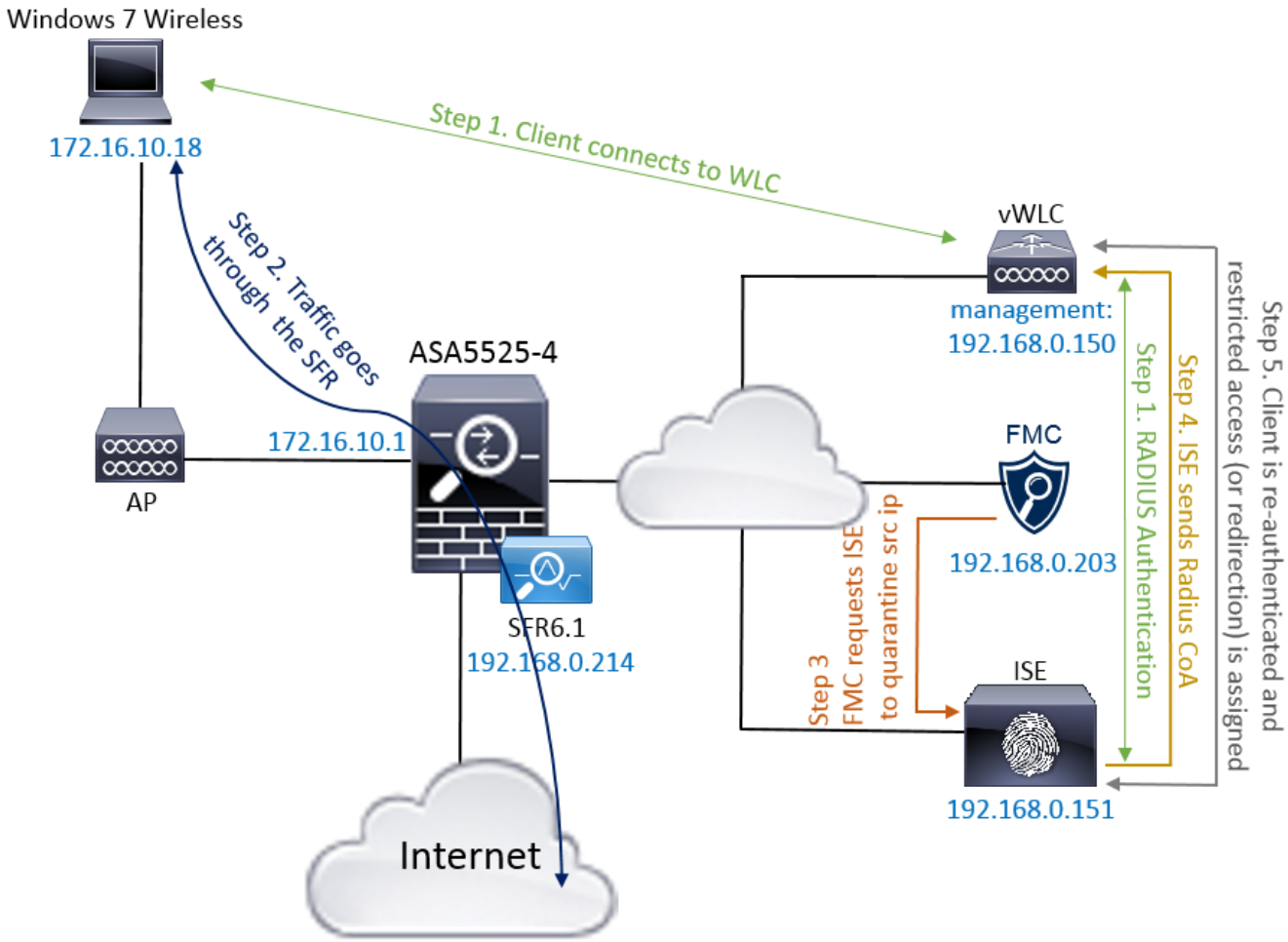
تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

التكوين

ال تغطي هذه المقالة التكوين الأولي لتكامل ISE مع FirePOWER وتكامل ISE مع Active Directory (AD) وتكامل Firepower مع AD. لهذه المعلومات انتقل إلى قسم المراجع. تسمح وحدة الإصلاح Firepower 6.1 لنظام FirePOWER باستخدام إمكانيات ISE EPS (الحجر الصحي، إلغاء الحجر الصحي، إيقاف تشغيل المنفذ) كعلاج عند مطابقة قاعدة الارتباط.

ملاحظة: لا يتوفر إيقاف تشغيل المنفذ لعمليات النشر اللاسلكية.

الرسم التخطيطي للشبكة



وصف التدفق:

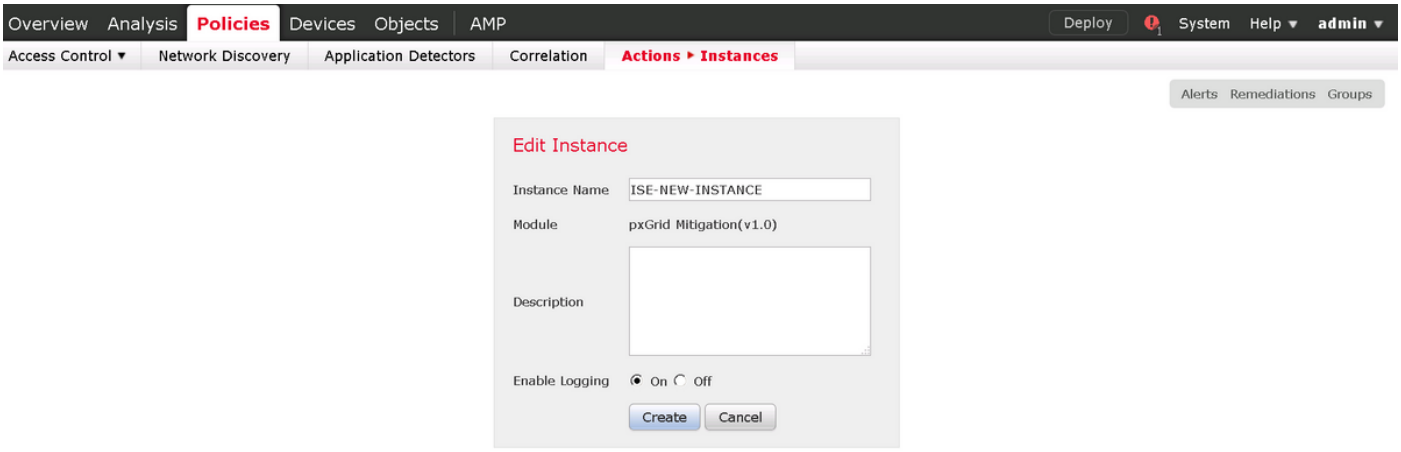
1. يتصل العميل بشبكة ويصادق مع ISE ويدخل على قاعدة تخويل بملف تعريف تخويل يمنح وصولا غير مقيد إلى الشبكة.
2. ثم تتدفق حركة المرور من العميل عبر جهاز FirePOWER.
3. يبدأ المستخدم في تنفيذ نشاط ضار ويضرب قاعدة ارتباط تقوم بدورها بتشغيل مركز إدارة FirePOWER (FMC) للقيام بمعالجة ISE عبر PXgrid.
4. يقوم ISE بتعيين عملية عزل EPSStatus إلى نقطة النهاية ويقوم بتشغيل تغيير تفويض RADIUS إلى جهاز وصول إلى الشبكة (WLC أو المحول).
5. يقوم العميل بتنفيذ سياسة ترخيص أخرى تعين وصولا مقيدا (يقوم بتغيير SGT أو إعادة التوجيه إلى البوابة أو رفض الوصول).

ملاحظة: يجب تكوين جهاز الوصول إلى الشبكة (NAD) لإرسال محاسبة RADIUS إلى ISE لتزويده بمعلومات عنوان IP التي يتم استخدامها لتعيين عنوان IP إلى نقطة نهاية.

تكوين Firepower

الخطوة 1. تكوين مثيل تخفيف pxGrid.

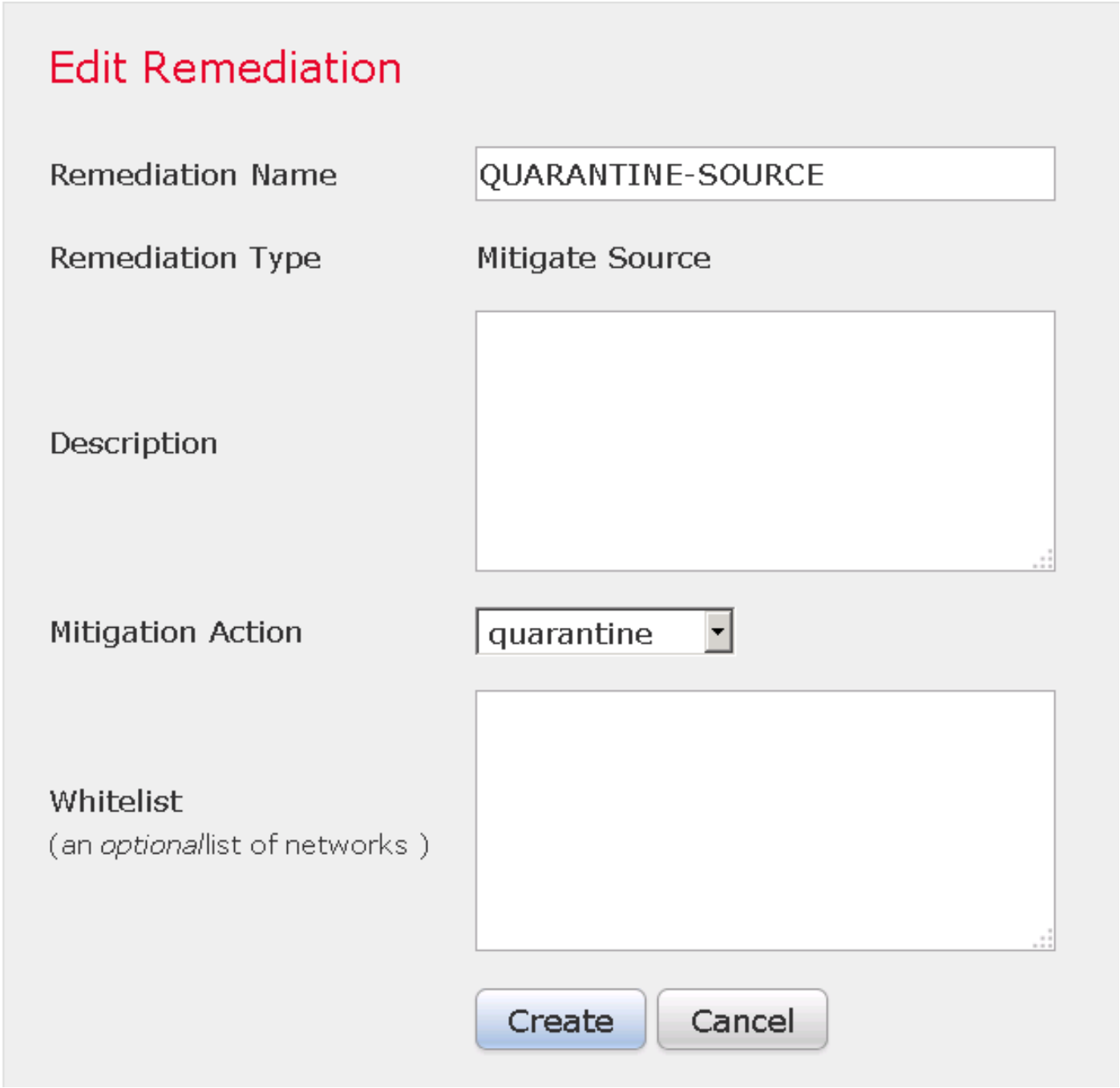
انتقل إلى **السياسات > الإجراءات > المثيلات** وإضافة مثيل تخفيف PxGrid كما هو موضح في الصورة.



الخطوة 2. تكوين حل.

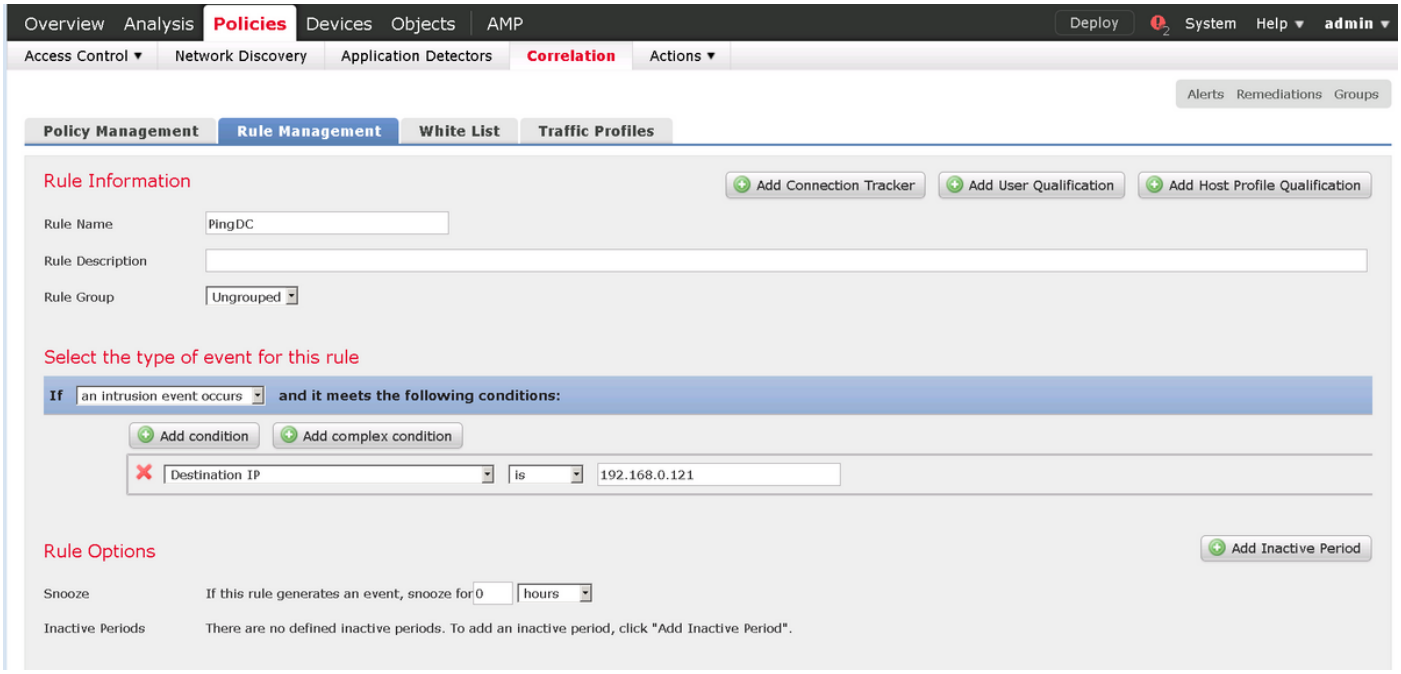
هناك نوعان متاحان: تخفيف الوجهة والحد من المصدر. في هذا المثال، يتم إستخدام تخفيف المصدر. أختر نوع المعالجة وانقر **إضافة** كما هو موضح في الصورة:

تعيين إجراء تخفيف إلى الإصلاح كما هو موضح في الصورة:



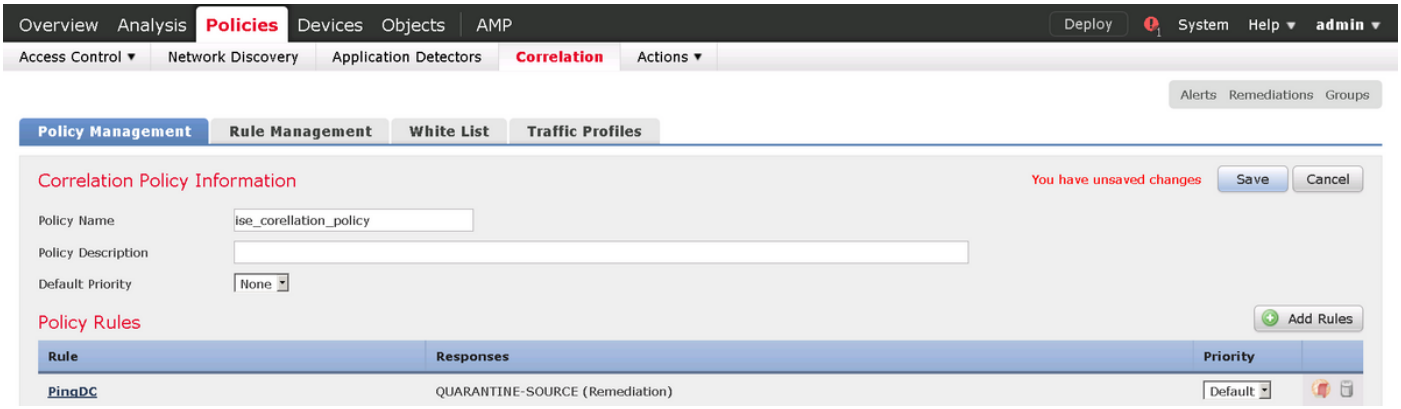
الخطوة 3. تكوين قاعدة إرتباط.

انتقل إلى **السياسات > الارتباط > إدارة القواعد** وانقر فوق **إنشاء** قاعدة إرتباط **القاعدة** وه المشغل لحصول عملية الإصلاح. يمكن أن تحتوي قاعدة الارتباط على عدة شروط. في هذا المثال، يتم الوصول إلى **قاعدة** الارتباط **PingDC** إذا حدث إقتحام وكان عنوان IP للوجهة 192.168.0.121. يتم تكوين قاعدة منع الوصول المخصصة المطابقة للرد على صدى بروتوكول ICMP لغرض الاختبار كما هو موضح في الصورة:

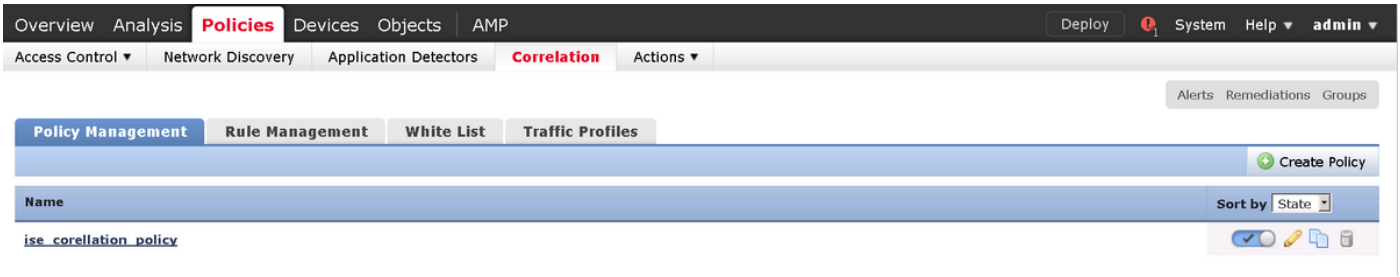


الخطوة 4. تكوين نهج إرتباط.

انتقل إلى **السياسات > الارتباط > إدارة السياسة** وانقر فوق **إنشاء سياسة**، وقم بإضافة قاعدة إلى السياسة وقم بتعيين الاستجابة لها كما هو موضح في الصورة:



قم بتمكين سياسة الارتباط كما هو موضح في الصورة:

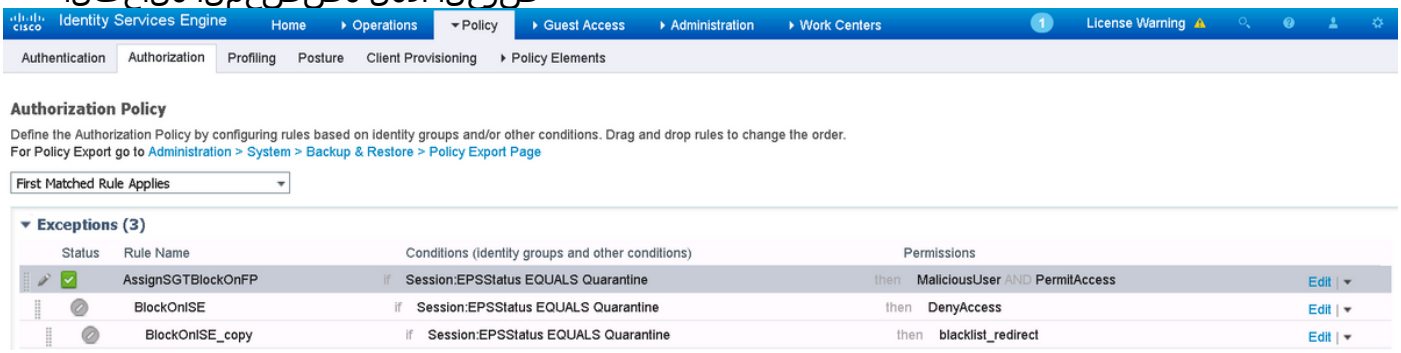


تكوين ISE

الخطوة 1. تكوين نهج التخويل.

انتقل إلى **النهج > التفويض** وأضف سياسة تخويل جديدة سيتم تنفيذها بعد إجراء الإصلاح. إستخدام **جلسة: EPSStatus يساوي عزل** كشرط. هناك عدة خيارات التي يمكن إستخدامها كنتيجة لذلك:

- السماح بالوصول وتعيين مساعد رقمي (فرض قيود التحكم في الوصول على أجهزة الشبكة)
- رفض الوصول (يجب طرد المستخدم من الشبكة والا يجب أن يكون قادرا على الاتصال مرة أخرى)
- إعادة التوجيه إلى بوابة **قائمة** سوداء (في هذا السيناريو، يتم تكوين بوابة النقاط الفعالة المخصصة لهذا الغرض

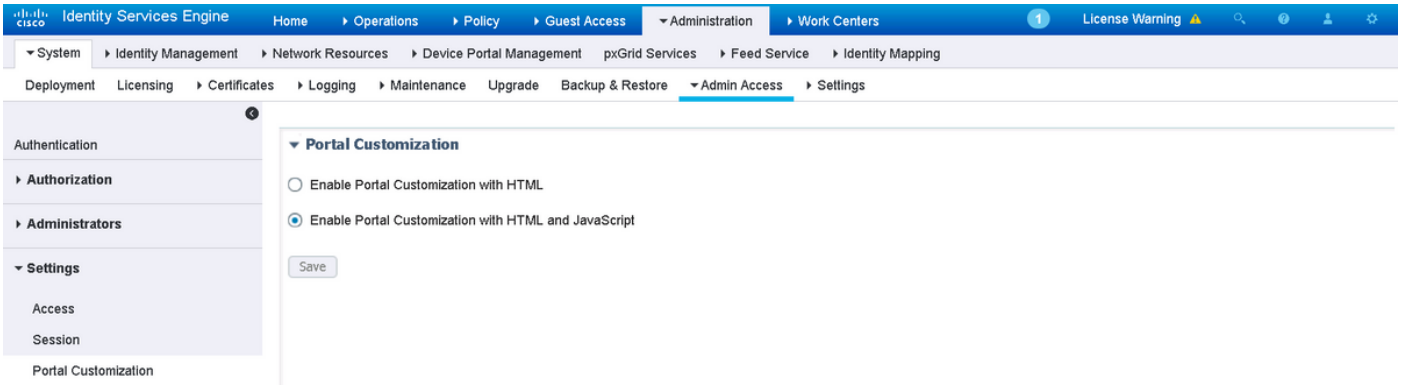


تكوين المدخل المخصص

في هذا المثال، تم تكوين بوابة النقاط الساخنة كقائمة **سوداء**. توجد فقط صفحة سياسة إستخدام مقبولة (AUP) بنص مخصص والا توجد إمكانية لقبول AUP (يتم ذلك باستخدام JavaScript). لتحقيق ذلك، تحتاج أولا إلى تمكين JavaScript ثم لصق رمز يخفي زر AUP وعناصر التحكم في تكوين تخصيص المدخل.

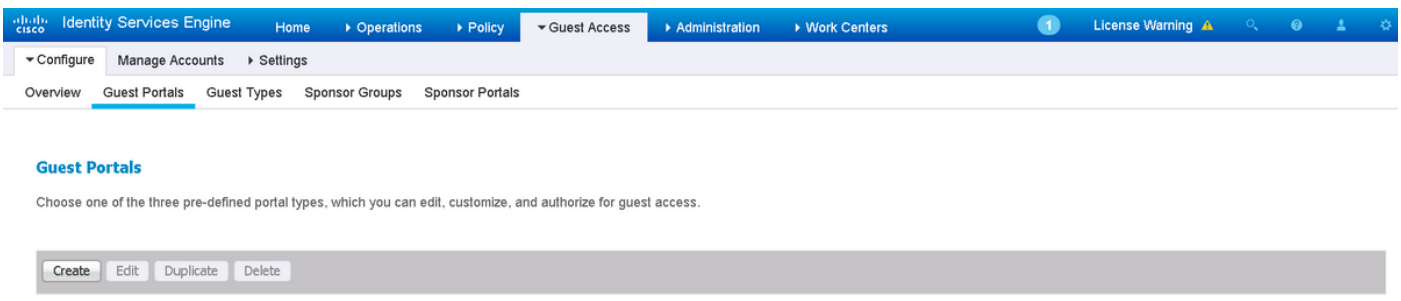
الخطوة 1. إتاحة JavaScript.

انتقل إلى **إدارة > نظام > Admin Access> إعدادات > تخصيص المدخل. أختر تمكين تخصيص المدخل باستخدام HTML و JavaScript** وانقر **حفظ**.



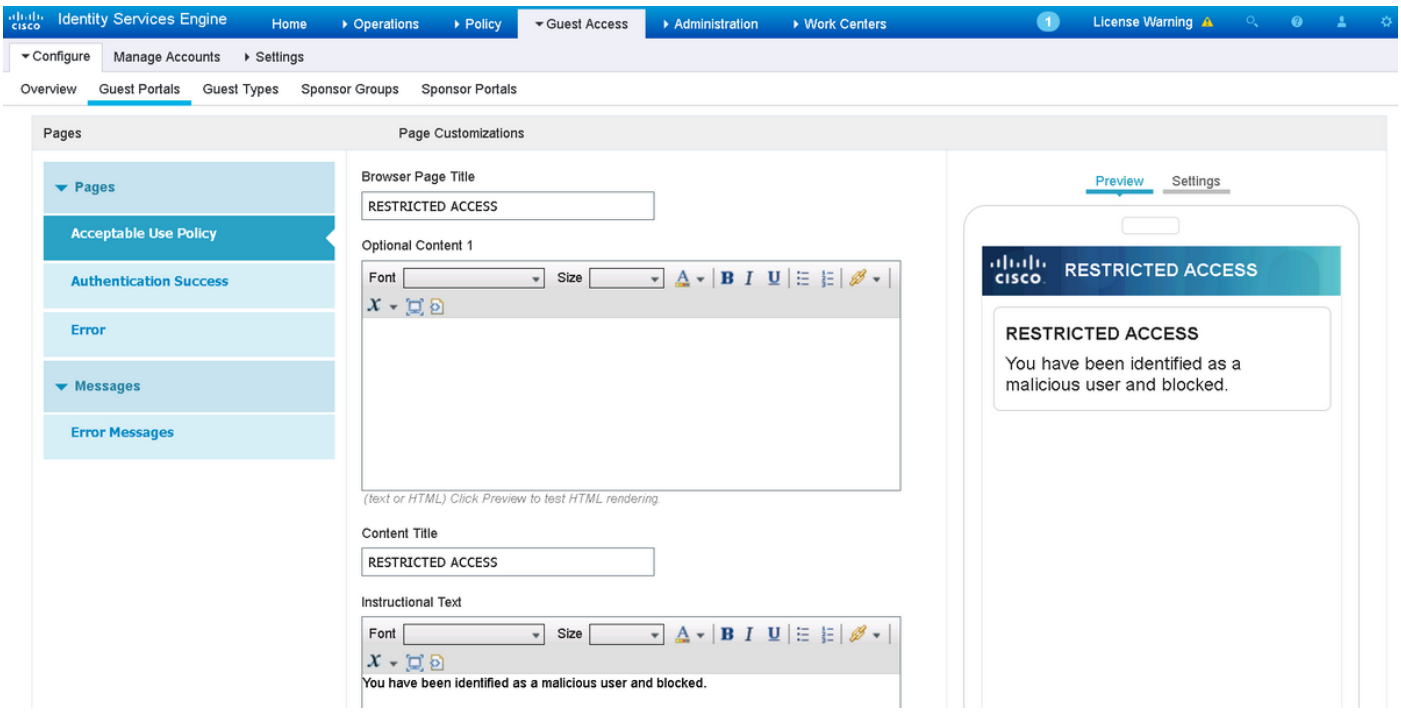
الخطوة 2. إنشاء مدخل نقطة اتصال.

انتقل إلى **Guest Access (وصول الضيف) > Configure (تكوين) > بوابات الضيف** وانقر فوق **Create** (إنشاء)، ثم أختر نوع النقطة الفعالة.



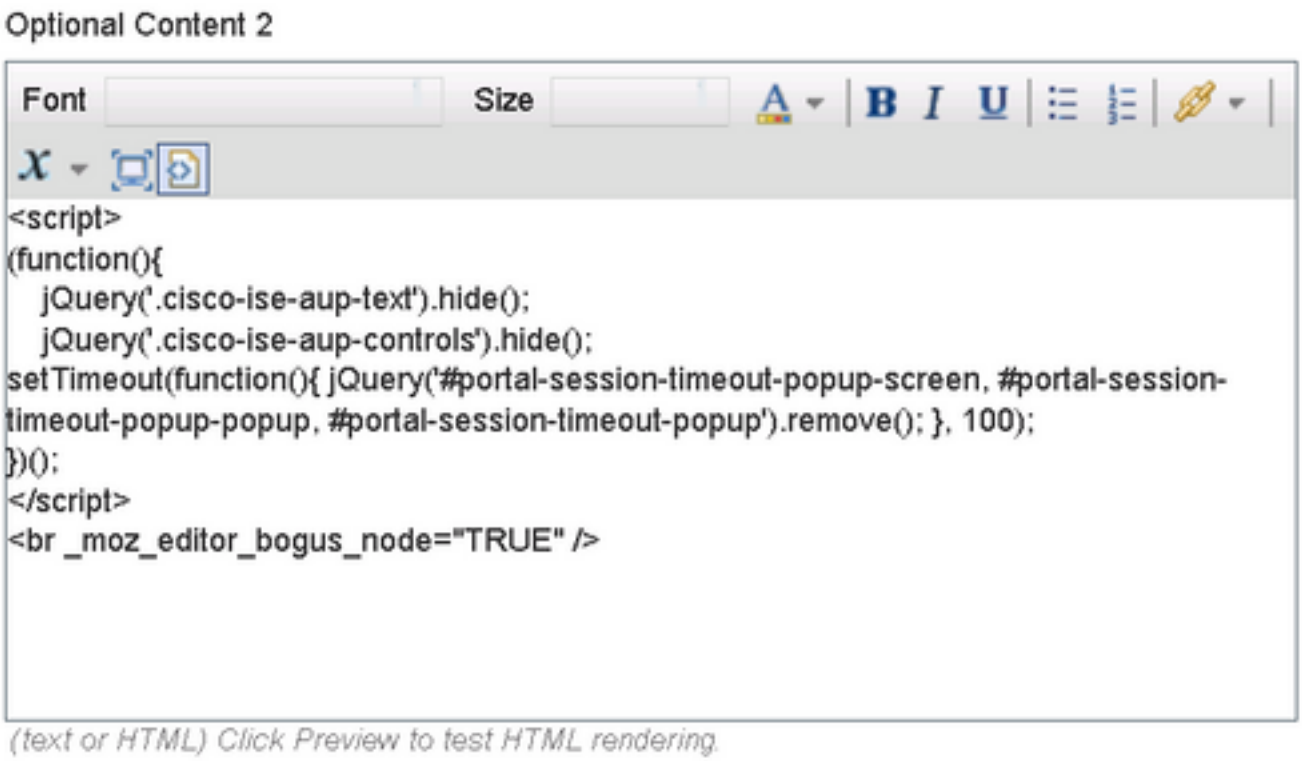
الخطوة 3. تكوين تخصيص المدخل.

انتقل إلى **تخصيص صفحة المدخل** وقم بتغيير العناوين والمحتوى لتوفير تحذير مناسب للمستخدم.



قم بالتمرير إلى **خيار محتوى 2**، انقر **تبديل مصدر HTML**، وقم بلصق النص التنفيذي بالداخل:

انقر **إلغاء تشغيل مصدر HTML**.



التحقق من الصحة

أستخدم المعلومات المقدمة في هذا القسم للتحقق من أن التكوين لديك يعمل بشكل صحيح.

قوة النيران

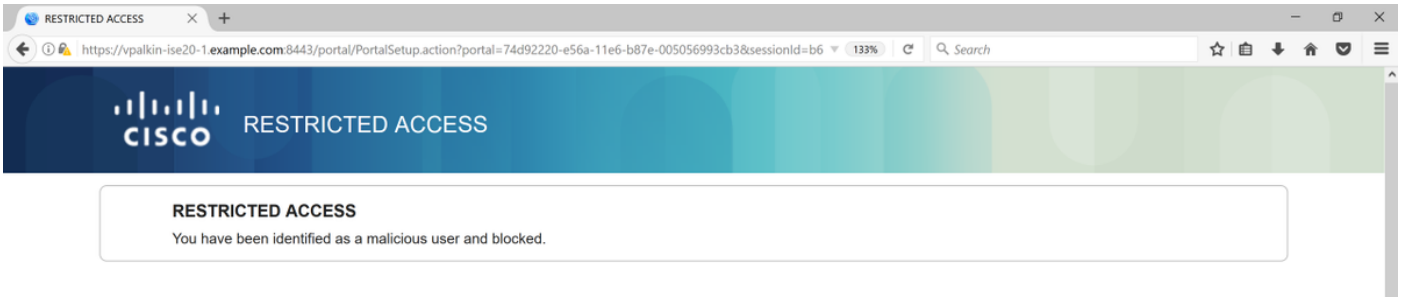
المشغل لحدوث الإصلاح هو ضرب من سياسة / قاعدة الارتباط. انتقل إلى **Analysis (التحليل) > Correlation > Correlation Events** وتحقق من حدوث حدث الارتباط.

محرك خدمات كشف الهوية (ISE)

بعد ذلك يجب أن يقوم ISE بتشغيل RADIUS: CoA وإعادة مصادقة المستخدم، ويمكن التحقق من هذه الأحداث في **العملية > RADIUS livelog.**

في هذا المثال، قام ISE بتعيين Sgt **MaliciousUser** مختلف إلى نقطة النهاية. في حالة رفض ملف تعريف تخويل **الوصول**، يفقد المستخدم الاتصال اللاسلكي ولا يمكنه الاتصال مرة أخرى.

الإصلاح باستخدام مدخل القائمة السوداء. إذا تم تكوين قاعدة تفويض الإصلاح لإعادة التوجيه إلى البوابة، فيجب أن تبدو هكذا من منظور المهاجم:



استكشاف الأخطاء وإصلاحها

يوفر هذا القسم معلومات يمكنك إستخدامها لاستكشاف أخطاء التكوين وإصلاحها.

انتقل إلى **Analysis (التحليل) > Correlation > Status (الحالة)** كما هو موضح في هذه الصورة.

يجب أن ترجع رسالة النتيجة إما **إكمال الإصلاح بنجاح** أو رسالة خطأ معينة. دققت syslog: **نظام > مراقبة > Syslog** ومرشح إنتاج مع **pxgrid**. يمكن التحقق من نفس السجلات في **/var/log/messages**.

معلومات ذات صلة

- https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/200319-Troubleshoot-ISE-and-FirePOWER-Integrati.html
- https://communities.cisco.com/docs/DOC-68284
- https://communities.cisco.com/docs/DOC-68285
- https://communities.cisco.com/thread/64870?start=0&tstart=0
- http://www.cisco.com/c/en/us/td/docs/security/ise/2-0/admin_guide/b_ise_admin_guide_20.html
- http://www.cisco.com/c/en/us/td/docs/security/firepower/610/configuration/guide/fpmc-config-guide-v61.html

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).