تكوين تدفق التخويل لجلسات عمل معرف الخامل في ISE 3.2

المحتويات

المقدمة

يوضح هذا المستند كيفية تكوين قواعد التخويل لأحداث معرف خامل لتخصيص الرقيب في الجلسات.

معلومات أساسية

ال تقوم خدمات الهوية السلبية (معرف خامل) بمصادقة المستخدمين مباشرة، ولكنها تجمع هويات المستخدمين وعناوين IP من خوادم المصادقة الخارجية مثل Active Directory (AD)، المعروفة باسم الموفرين، ثم تقوم بمشاركة تلك المعلومات مع المشتركين.

يقدم ISE 3.2 ميزة جديدة تسمح لك بتكوين سياسة تفويض لتعيين رقم مجموعة أمان (SGT) لمستخدم استنادا إلى عضوية مجموعة Active Directory.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- ISE 3.x من Cisco
- تكامل المعرف السلبي مع أي موفر
- إدارة Active Directory (AD)
- التقسيم (TrustSec)
- PxGrid (شبكة تبادل الأنظمة الأساسية)

المكونات المستخدمة

- برنامج محرك خدمة الهوية (ISE)، الإصدار 3.2
- Microsoft Active Directory
- Syslogs

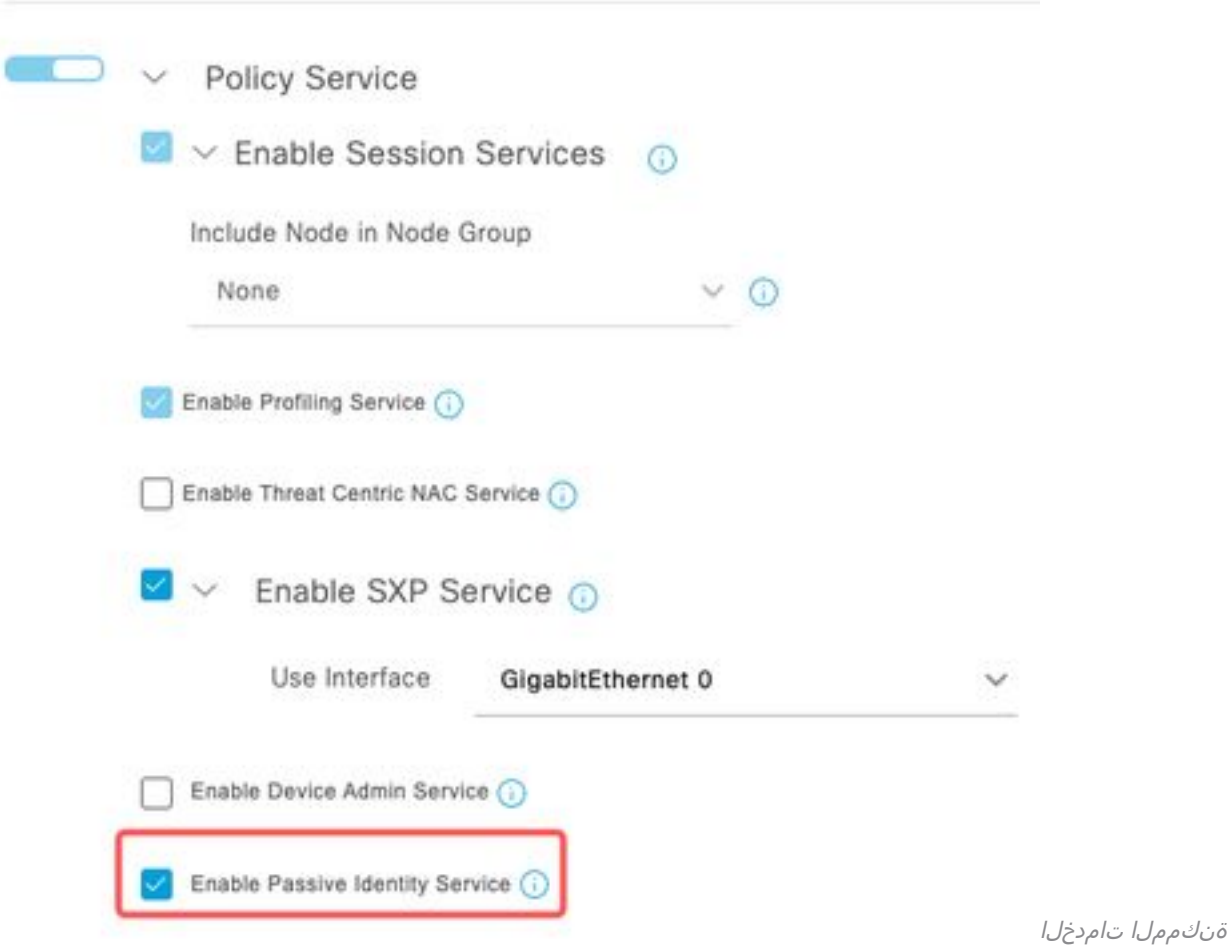
تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

التكوين

الخطوة 1. تمكين خدمات ISE.

1. في ISE، انتقل إلى إدارة > **نشر**، واختر عقدة ISE وانقر فوق **تحرير**، وقم بتمكين **خدمة** PxGrid و SXP يمكنك تمكين خدمة الهوية السلبية. إختياري، واختر تمكين خدمة **السياسة**. طقطقة **حفظ**.

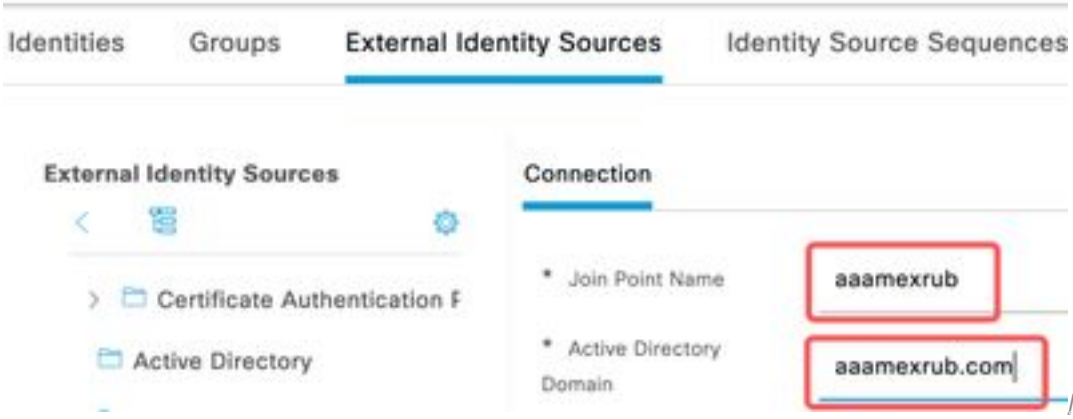
   تحذير: لا يمكن نشر تفاصيل SGT الخاصة بمستخدمي تسجيل دخول PassiveID الذين تم التصديق عليهم بواسطة موفر واجهة برمجة التطبيقات (API) في SXP. ومع ذلك، يمكن نشر تفاصيل الرقباء الخاصة بأولاء المستخدمين من خلال نظامي PXgrid و PXgrid.



الخدمات الممكنة

الخطوة 2. قم بتكوين Active Directory.

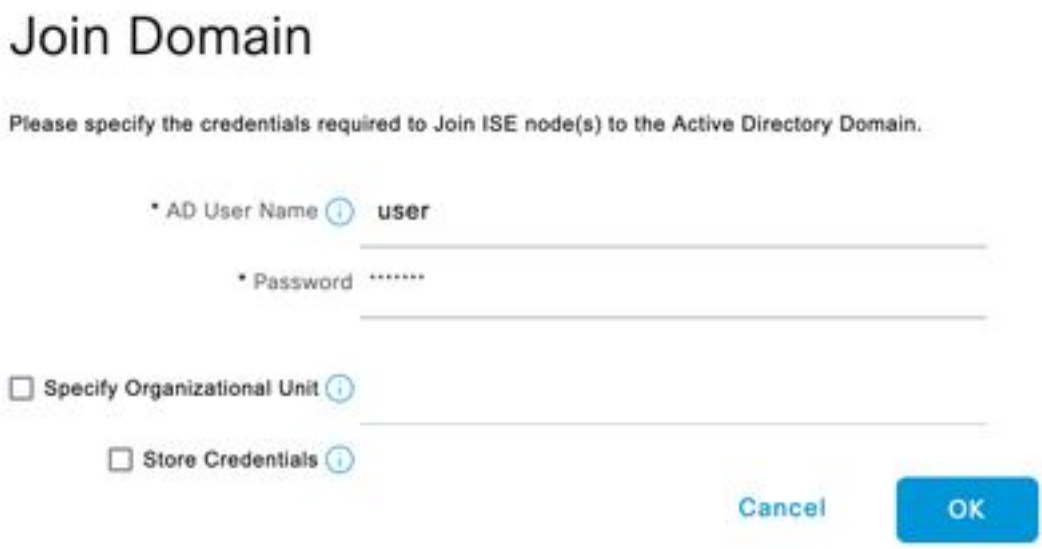
1. انتقل إلى إدارة > **إدارة الهوية > مصادر الهوية الخارجية** واختر **Active Directory** ثم انقر على زر **إضافة**.
2. أدخل **اسم نقطة الاتصال** و**مجال Active Directory**. انقر على **إرسال**.



إضافة Active Directory

3. يظهر أنه يمكنك الانضمام من ISE إلى AD. انقر فوق **نعم**. أدخل **اسم المستخدم** و**كلمة المرور**. ثم انقر فوق OK.

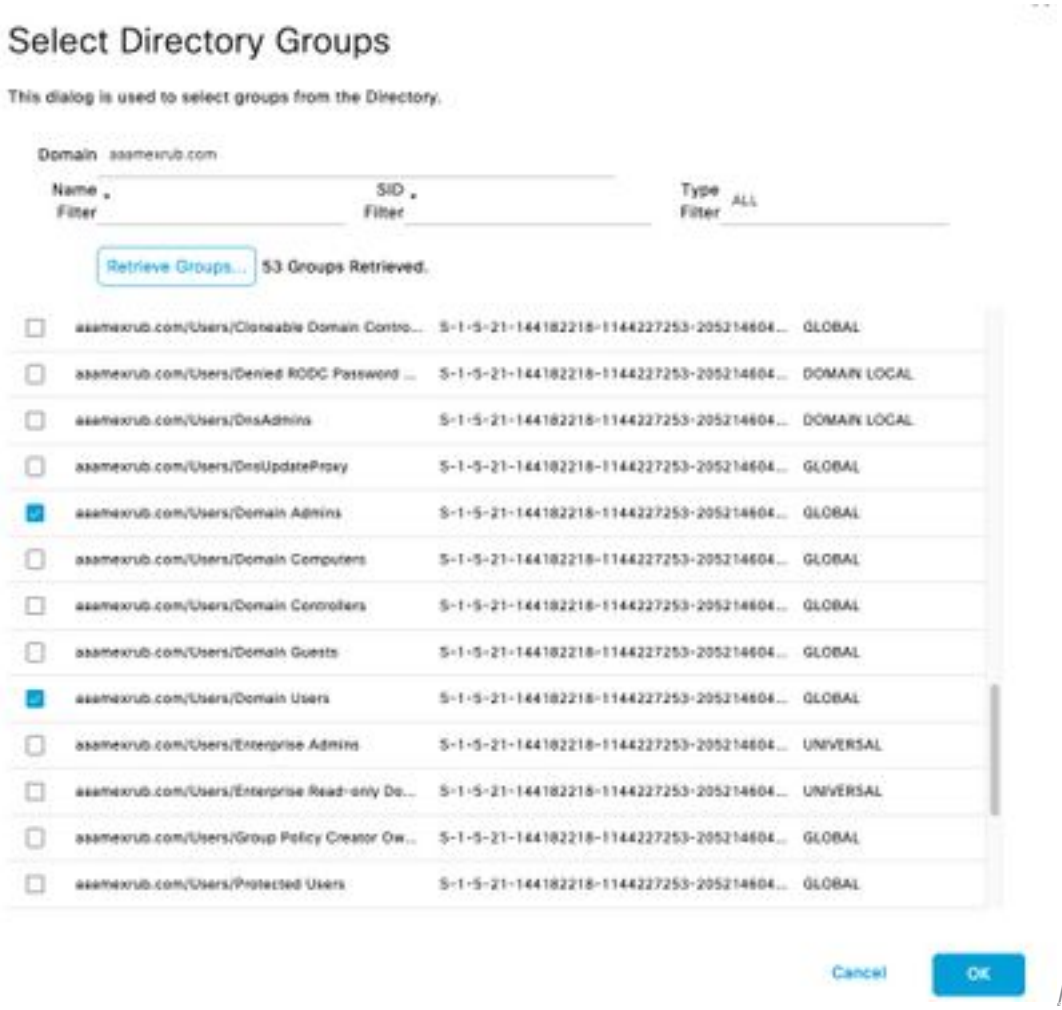
متابعة الانضمام إلى



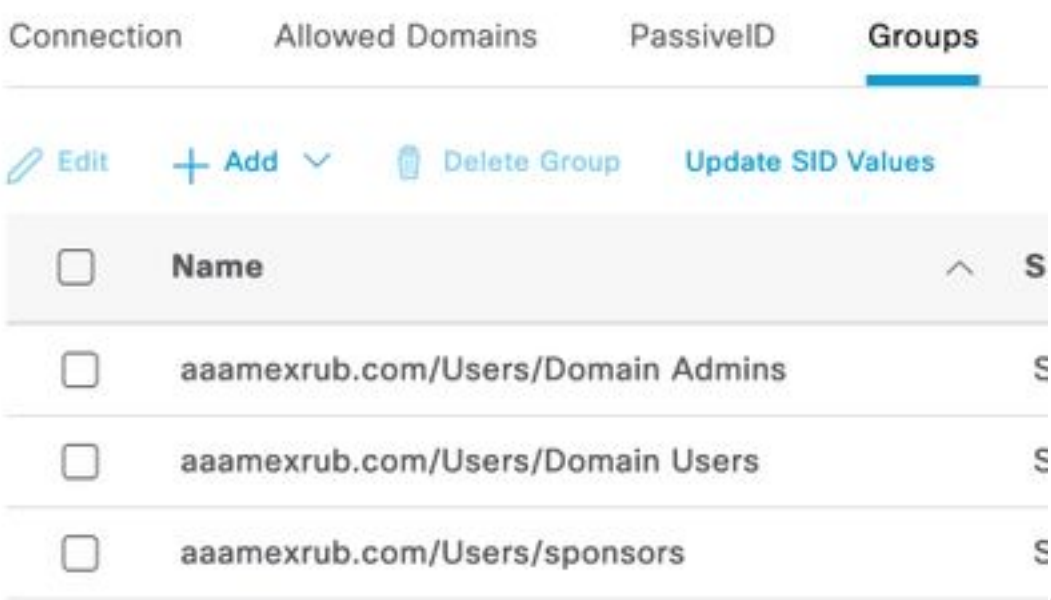
ISE

الانضمام إلى Active Directory

4. إستيراد مجموعات الإعلانات. انتقل إلى **مجموعات**، وانقر فوق **إضافة**، ثم انقر فوق **إستيراد المجموعات** واختر جميع المجموعات المهتمة وانقر فوق **موافق**.

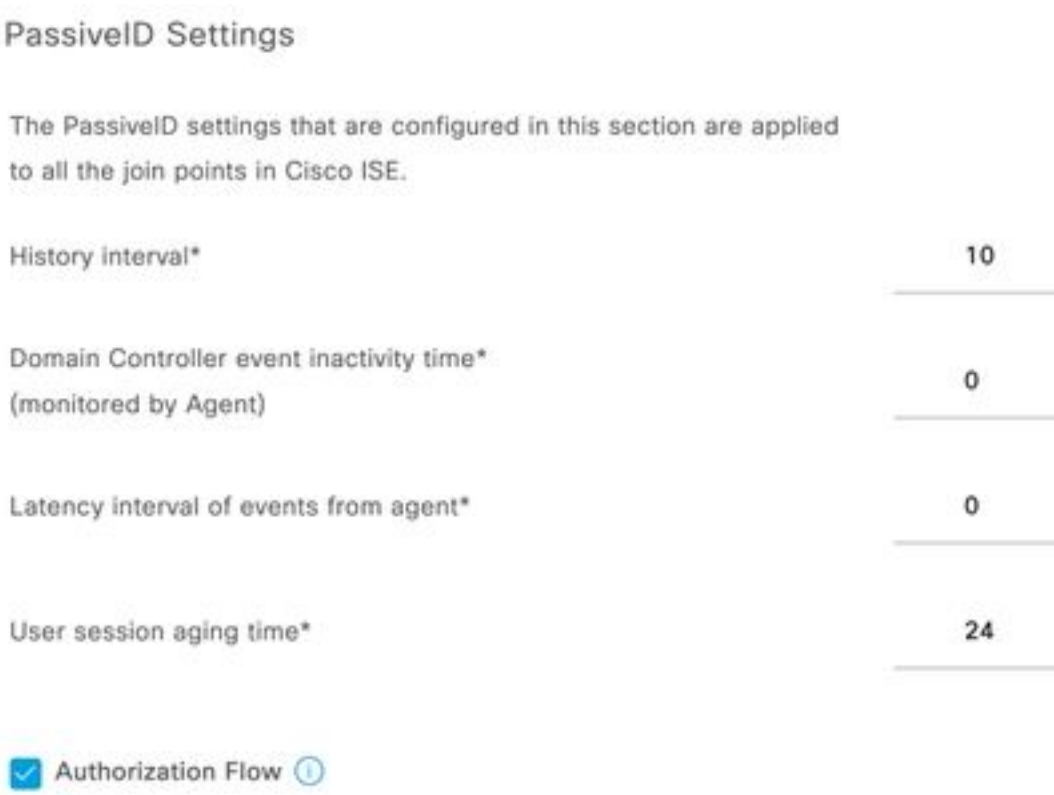


استيراد مجموعات الإعلانات



المجموعات التي تم استيرادها

5. تمكين تدفق التخويل. انتقل إلى **إعدادات متقدمة** وفي قسم **إعدادات PassiveID** حدد خانة الاختيار **تدفق التخويل**. طقطقة **حفظ**.

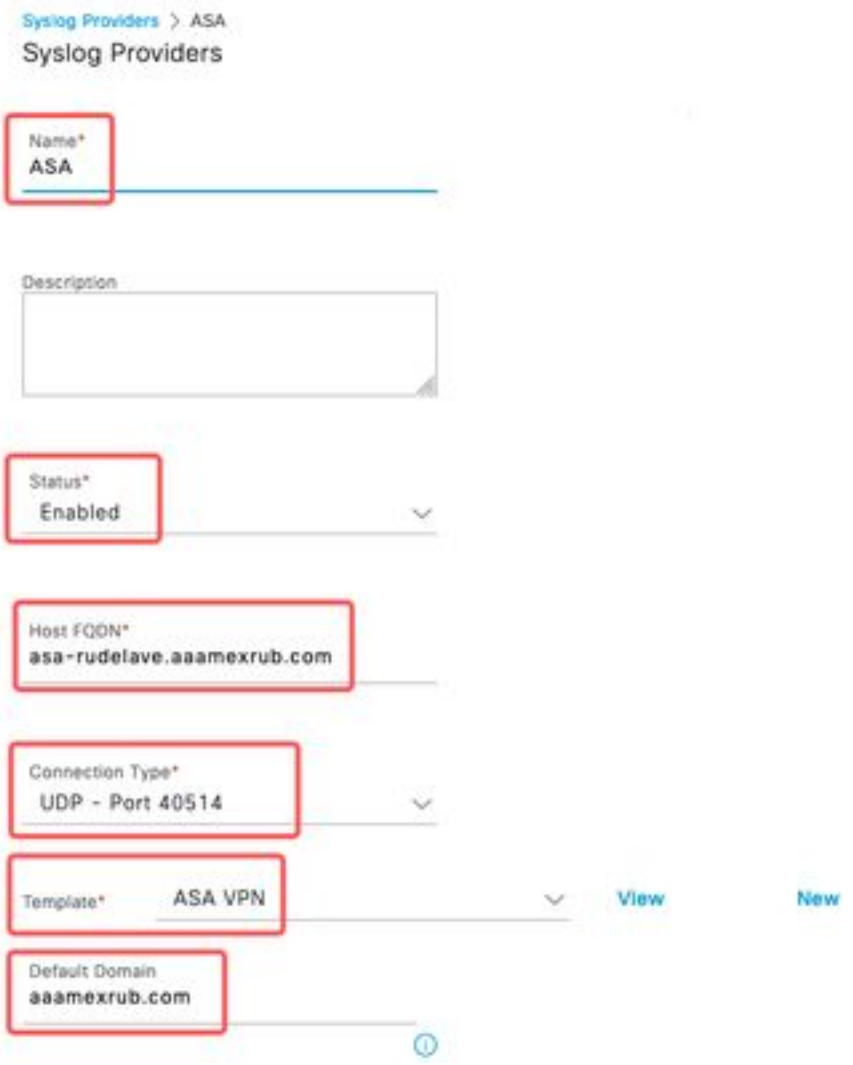


تمكين تدفق التخويل

الخطوة 3. قم بتكوين موفر syslog.

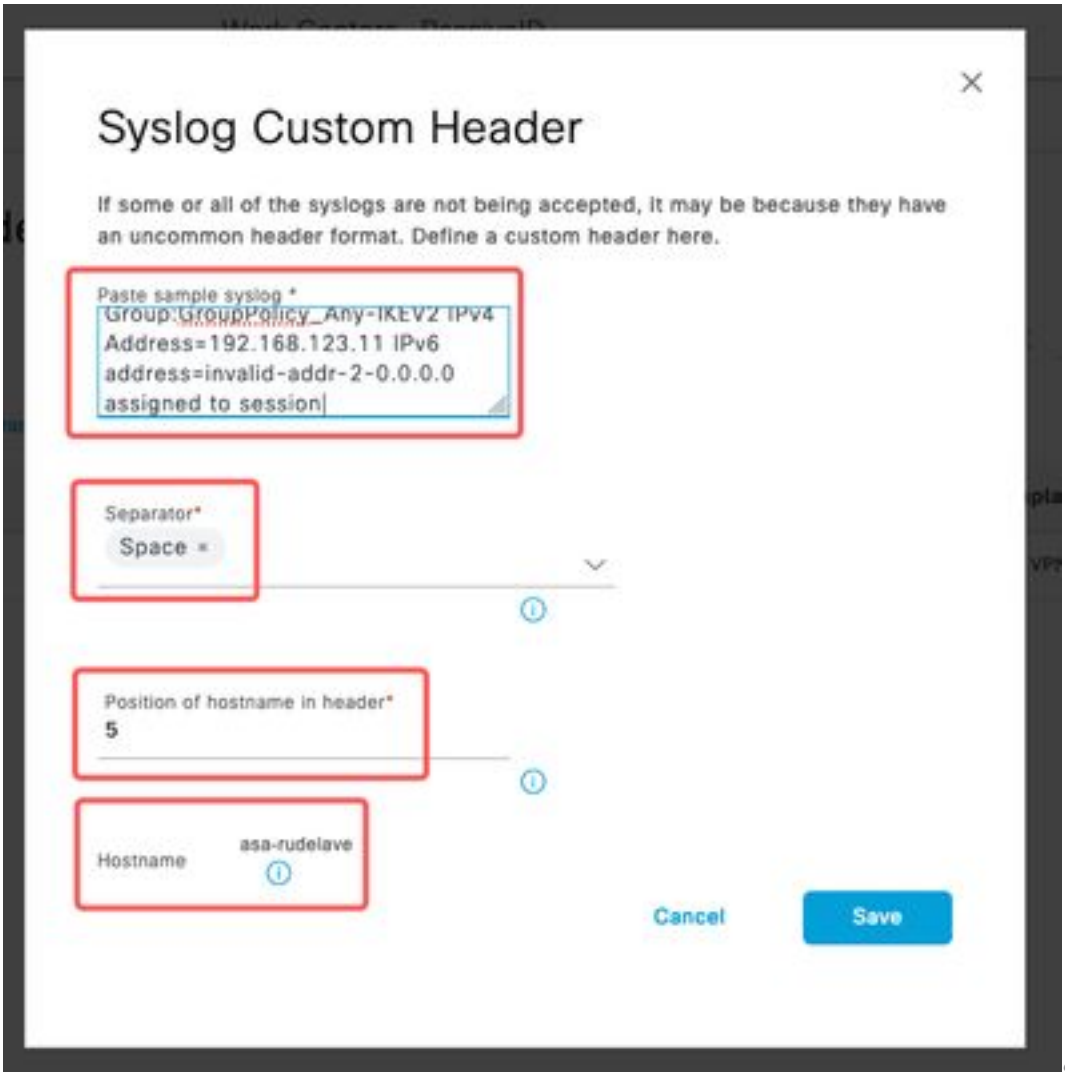
1. انتقل إلى مراكز العمل > PassiveID > **الموفرون**، واختر **موفري Syslog**، وانقر فوق **إضافة**، ثم أكمل المعلومات. طقطقة **حفظ**

   تحذير: في هذه الحالة، يستلم ISE رسالة syslog من اتصال VPN ناجح في ASA، ولكن لا يصف هذا المستند هذا التكوين.



تكوين موفر syslog

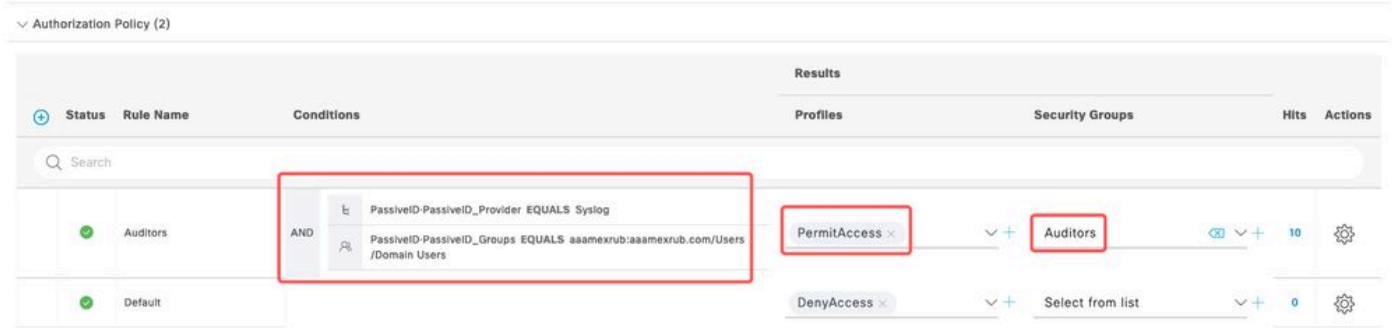
2. انقر **رأس مخصص**. الصق نموذج syslog واستخدم فاصل أو علامة تبويب للعثور على اسم مضيف الجهاز. إذا كان صحيحا، يظهر اسم المضيف. طقطقة **حفظ**



تكوين رأس مخصص

الخطوة 4. تكوين قواعد المصادقة

1. انتقل إلى **السياسة > مجموعات السياسات.** ولهذه الحالة، فإنه يستخدم النهج الافتراضي. انقر على النهج **الافتراضي**. في **نهج التخويل**، أضف قاعدة جديدة. في سياسات PassiveID، يحتوي ISE على جميع الموفرين. يمكنك دمج هذا مع مجموعة PassiveID. أختر **السماح بالوصول** كملف تعريف، **واختر في مجموعات الأمان** الحاجة لضابط تقنية المعلومات.



تكوين قواعد المصادقة

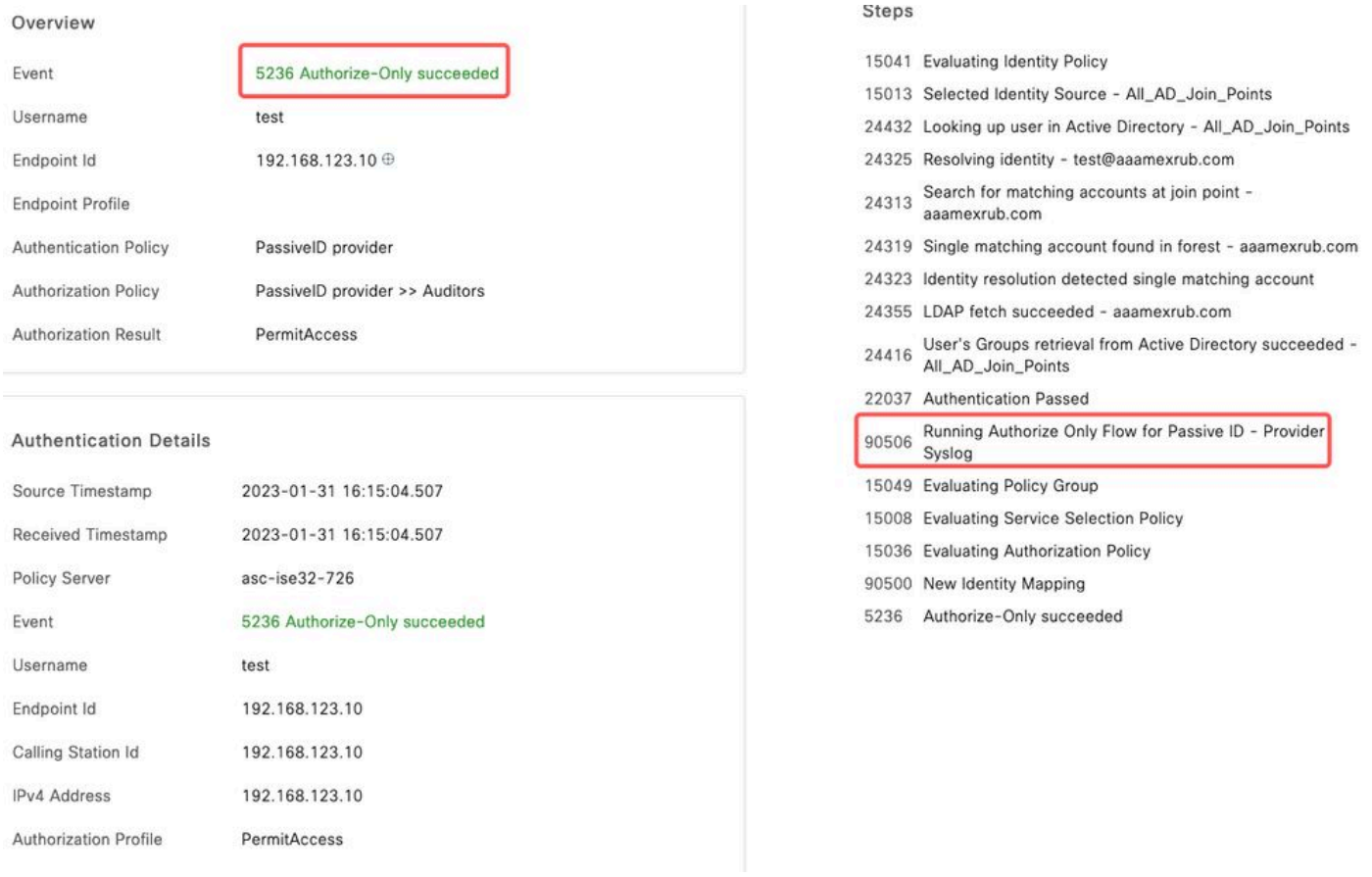
التحقق من الصحة

ما إن يستلم ISE ال syslog، أنت يستطيع فحصت ال radius حي سجل أن يرى تخويل تدفق. انتقل إلى **العمليات > RADIUS > السجلات المباشرة**.

في السجلات، يمكنك مشاهدة حدث التفويض. يحتوي هذا الرقم على اسم المستخدم ونوع التخويل وعلامة مجموعة الأمان المقترنة به.

سجل Radius Live

للتحقق من المزيد من التفاصيل، انقر فوق **تقرير التفاصيل**. هنا يمكنك مشاهدة تدفق السماح فقط الذي يقيم السياسات لتخصيص الرقيب.



تقرير السجل المباشر ل RADIUS

استكشاف الأخطاء وإصلاحها

بالنسبة لهذه الحالة، فإنه يستخدم دفعتين، جلسات PassiveID وتدفق Authoriation. لتمكين تصحيح الأخطاء، انتقل إلى **العمليات > أستكشاف الأخطاء وإصلاحها > معالج تصحيح الأخطاء>تكوين سجل تصحيح الأخطاء**، ثم أختر عقدة ISE.

بالنسبة ل PassiveID، قم بتمكين المكونات التالية من مستوى **تصحيح الأخطاء**:

- PassiveID

للتحقق من السجلات، استنادا إلى موفر المعرف الخامل، الملف الذي تريد التحقق من هذا السيناريو، يلزمك مراجعة **الملف** passiveid-syslog.log، للمزودين الآخرين:

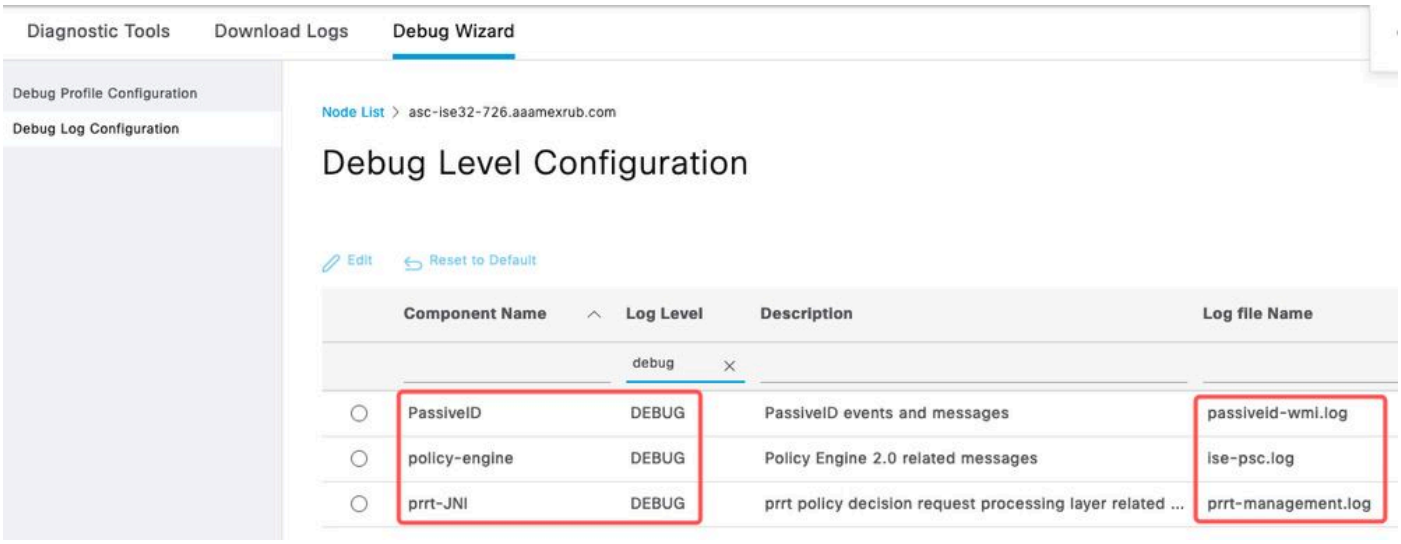
- عميل passiveid.log

- passiid-api.log
- passiid-endpoint.log
- passiid-span.log
- خوامل ومولوغ

لتدفق التخويل، قم بتمكين المكونات التالية من مستوى **تصحيح الأخطاء**:

- محرك السياسات
- بررت جني

مثال:



تم تمكين تصحيح الأخطاء

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).