تكوين خوادم TACACS الخارجية واستكشاف أخطائها وإصلاحها على ISE

المحتويات

المقدمة

يصف هذا المستند المزايا لاستخدام خادم TACACS+ الخارجي في عملية نشر باستخدام Identity Service Engine (ISE) كوكيل.

المتطلبات الأساسية

المتطلبات

- الفهم الأساسي لإدارة الأجهزة على ISE.
- يستند هذا المستند إلى الإصدار 2.0 من Identity Service Engine، القابل للتطبيق على أي إصدار من Identity Service Engine أعلى من 2.0.

المكونات المستخدمة

> **ملاحظة**: يمكن تفسير أي مرجع إلى ACS في هذا المستند ليكون مرجعا إلى أي خادم TACACS+ خارجي. ومع ذلك، قد يختلف التكوين على ACS والتكوين على أي خادم TACACS آخر.

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

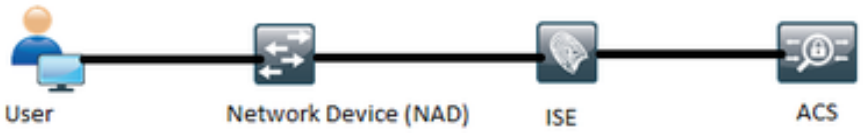
- Identity Service Engine 2.0
- نظام التحكم بالوصول (ACS) 5.7

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 تغيير في التكوين.

التكوين

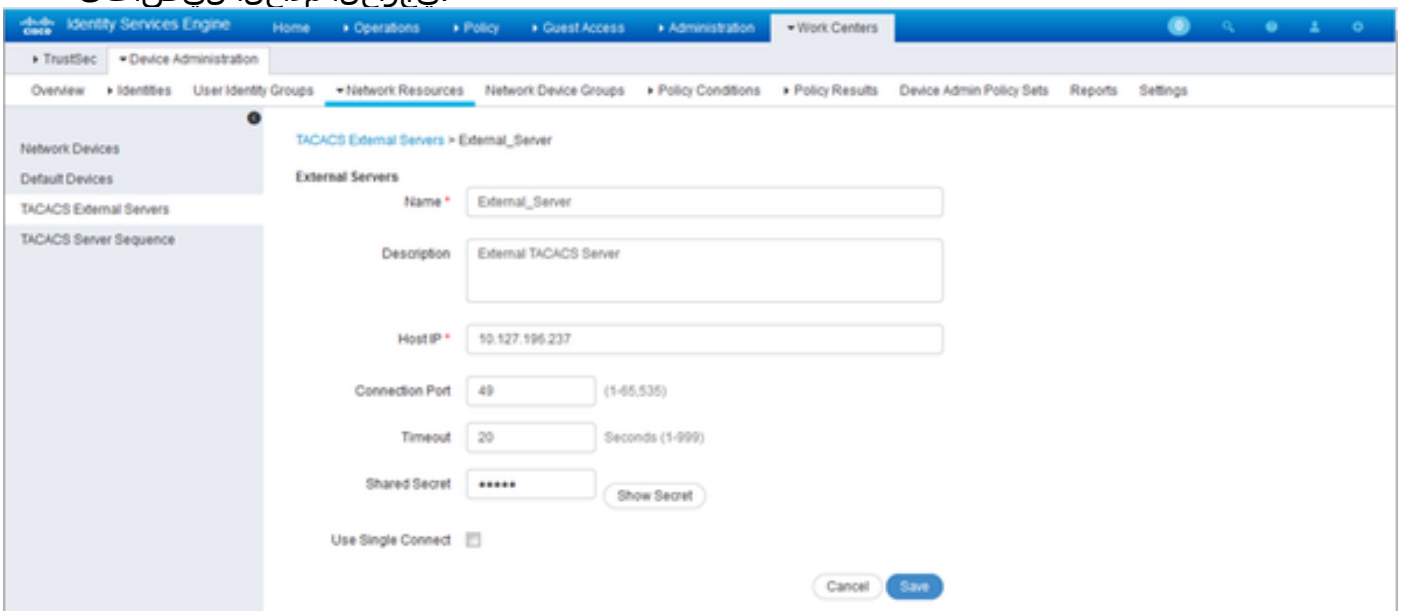
يساعد هذا القسم على تكوين ISE لطلبات TACACS+ للوكيل إلى ACS.

الرسم التخطيطي للشبكة



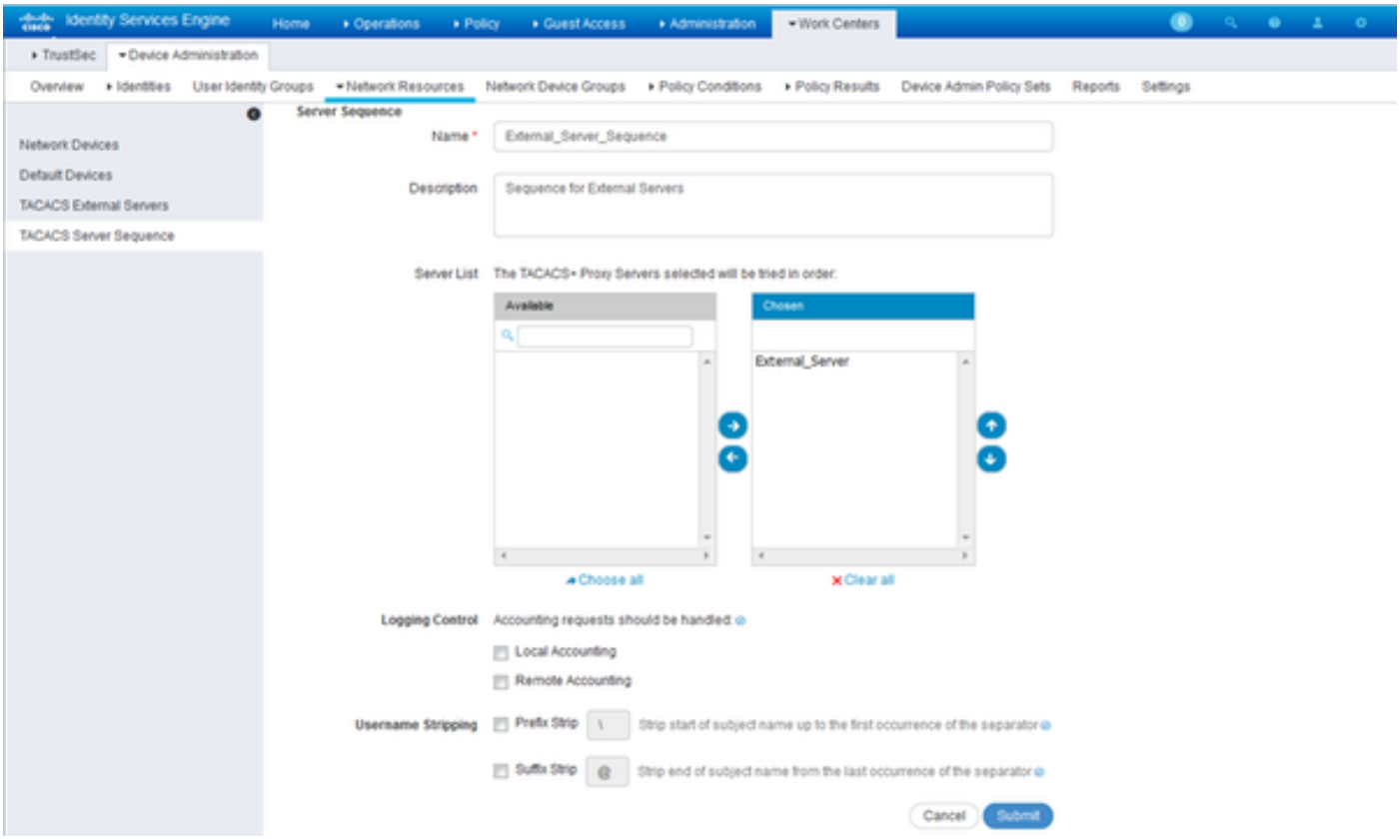
تكوين ISE

1. يمكن تكوين خوادم TACACS الخارجية المتعددة على ISE ويمكن إستخدامها لمصادقة المستخدمين. من أجل تكوين خادم TACACS+ الخارجي على ISE، انتقل إلى **مراكز العمل > إدارة الأجهزة > موارد الشبكة > خوادم TACACS الخارجية. انقر فوق إضافة** وتعبئة تفاصيل الخادم الخارجي.



يجب أن يكون السر المشترك المتوفر في هذا القسم هو نفسه السر المستخدم في ACS.

2. لاستخدام خادم TACACS الخارجي الذي تم تكوينه، يجب إضافته في تسلسل خادم TACACS الاستخدامه في مجموعات النهج. in order to شكلت TACACS نادل تسلسل، **انتقل** إلى **مراكز عمل > أداة إدارة > شبكة مورد > TACACS نادل تسلسل. انقر فوق إضافة**، قم بتعبئة التفاصيل واختر الخوادم المطلوبة لاستخدامها في هذا التسلسل.

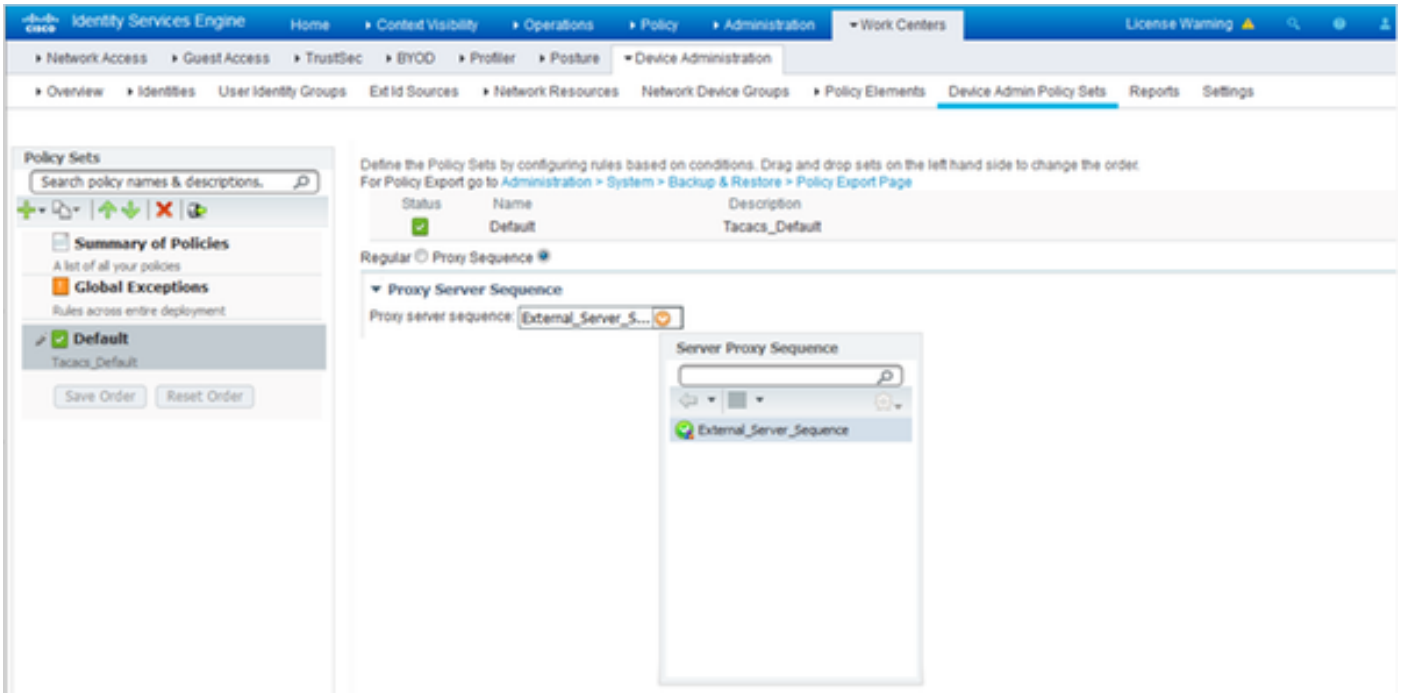


باإلضافة إلى تسلسل الخادم، تم توفير خيارين آخرين. التحكم في التسجيل وتعريف اسم المستخدم.

يعطي التحكم في التسجيل خيارا إما لتسجيل طلبات المحاسبة محليا على ISE أو لتسجيل طلبات المحاسبة إلى الخادم الخارجي الذي يتعامل مع المصادقة أيضا.

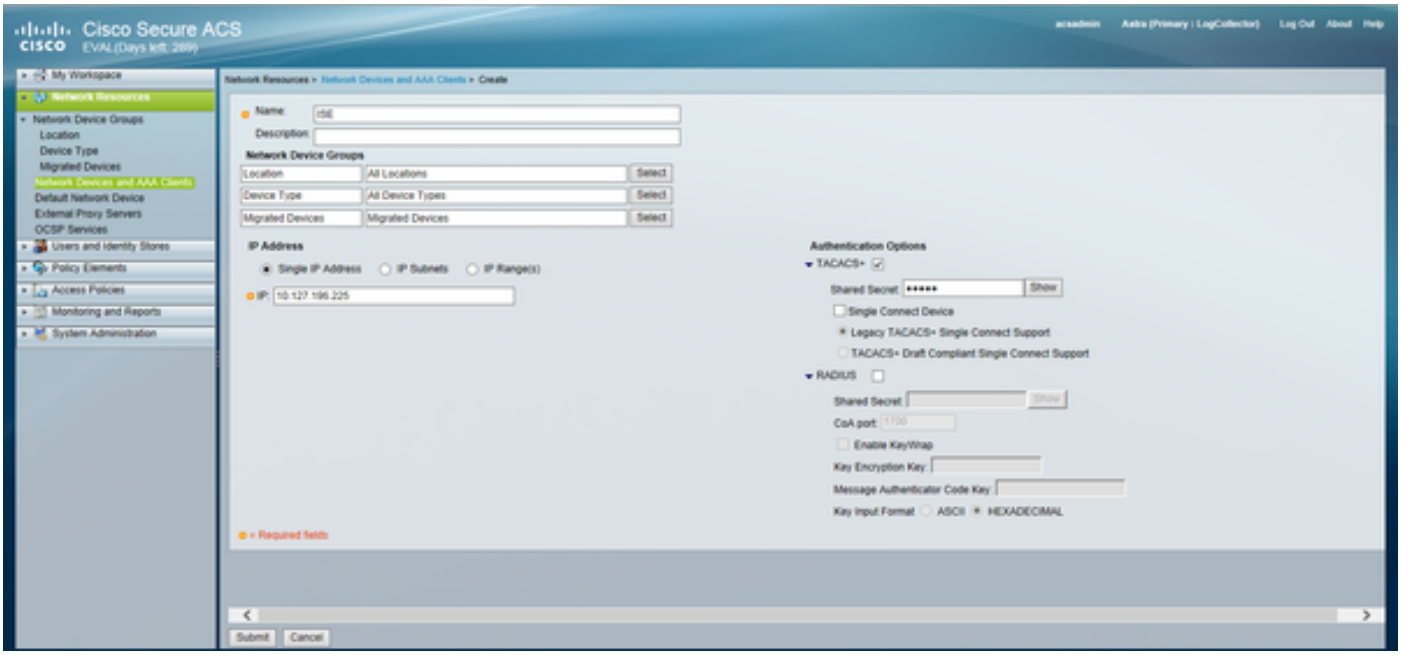
يتم إستخدام تجريد اسم المستخدم لشطب البادئة أو اللاحقة عن طريق تحديد محدد قبل إعادة توجيه الطلب إلى خادم TACACS خارجي.

3. لاستخدام تسلسل خادم TACACS الخارجي الذي تم تكوينه، يجب تكوين مجموعات النهج لاستخدام التسلسل الذي تم إنشاؤه. لتكوين مجموعات السياسات لاستخدام تسلسل الخادم الخارجي، انتقل إلى **مركز العمل > إدارة الأجهزة > مجموعات سياسات إدارة الأجهزة > [حدد مجموعة السياسات].** تبديل الزر اللاسلكي الذي يقول **تسلسل الوكيل.** أختر تسلسل الخادم الخارجي الذي تم إنشاؤه.

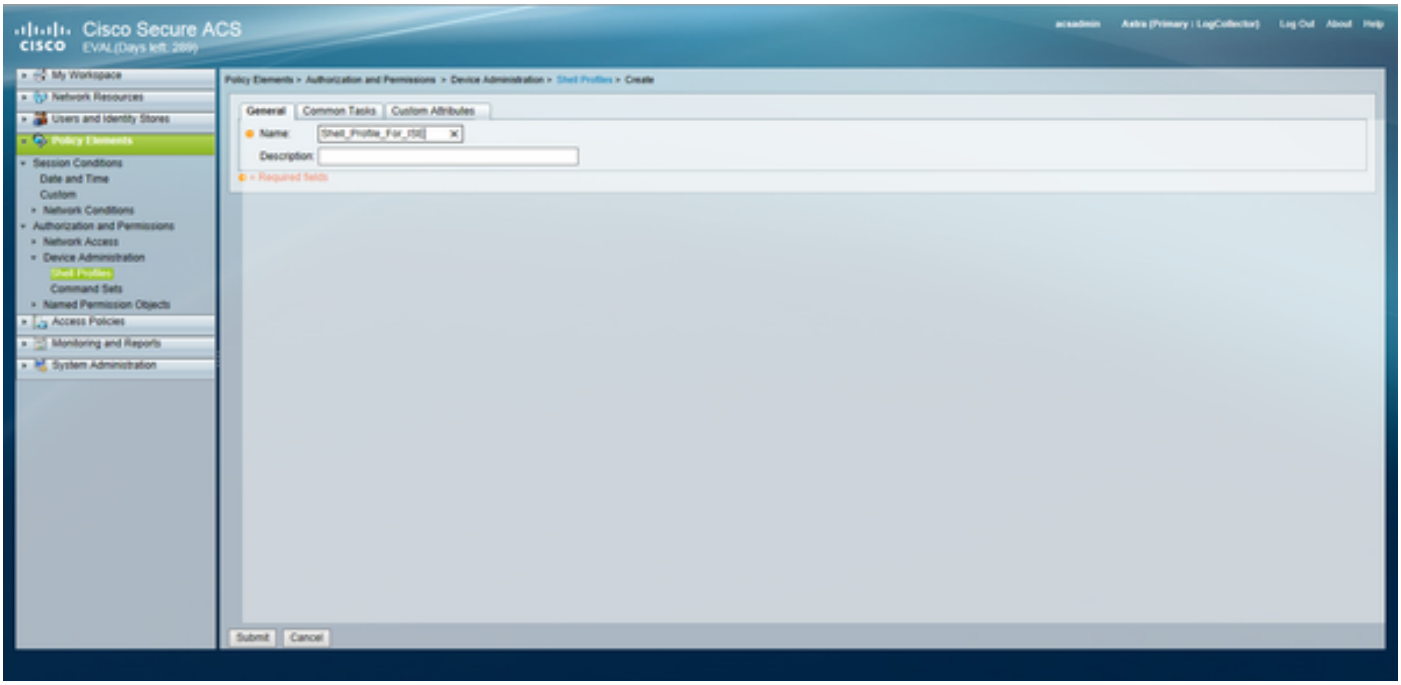


تكوين ACS

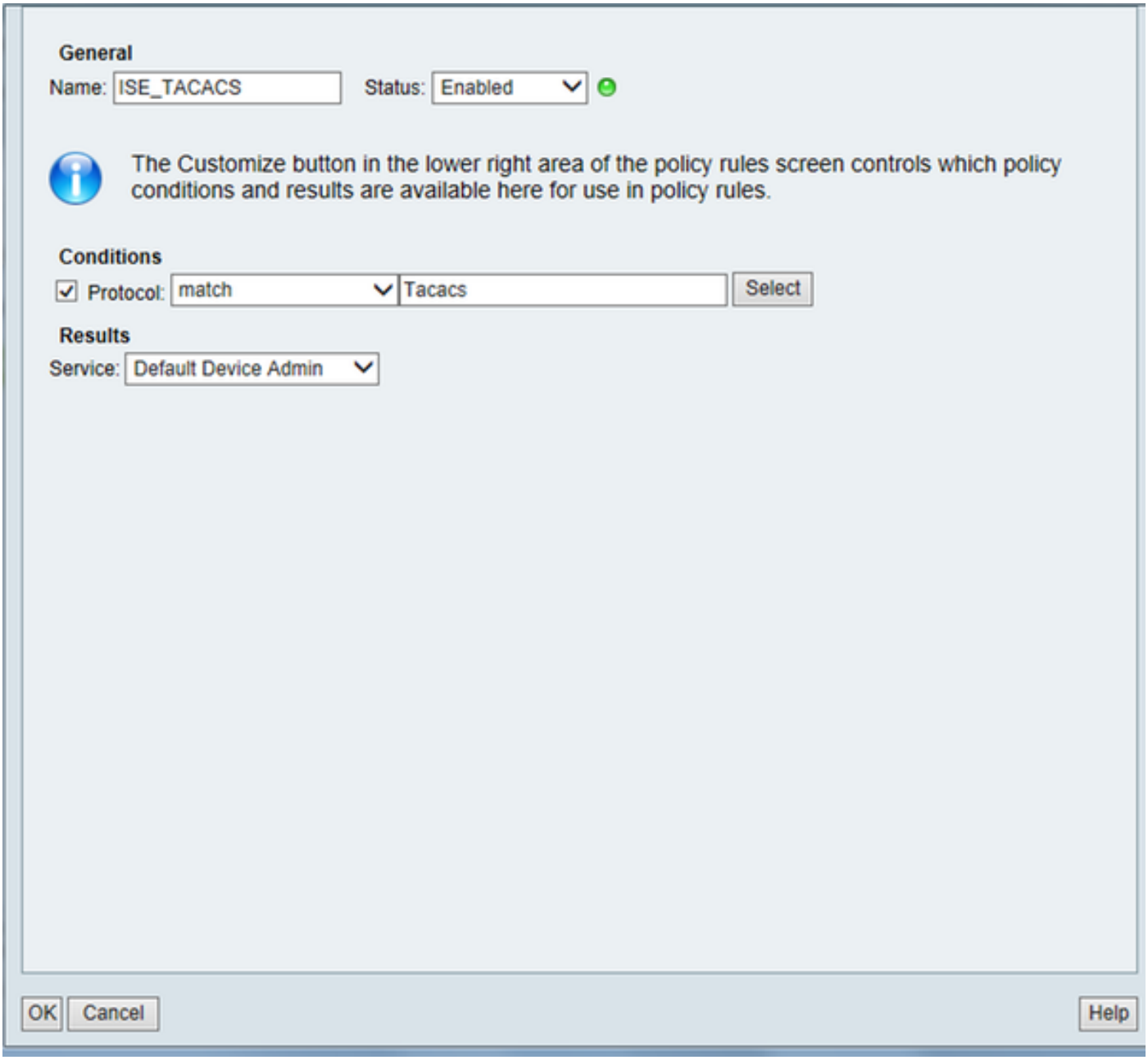
بالنسبة ل ACS، يعد ISE مجرد جهاز شبكة آخر سيقوم بإرسال طلب TACACS. لتكوين ISE كجهاز شبكة في ACS، انتقل إلى **موارد الشبكة > أجهزة الشبكة ومجموعات AAA. انقر فوق إنشاء** وتعبئة تفاصيل خادم ISE باستخدام نفس السر المشترك كما تم تكوينه على ISE.



قم بتكوين معلمات إدارة الأجهزة على ACS الموجودة وتوصيفات shell ومجموعات الأوامر. لتكوين توصيفات Shell، انتقل إلى **عناصر النهج > التخويل والأذونات > إدارة الأجهزة > توصيفات Shell. انقر فوق إنشاء** وتكوين الاسم والمهام المشتركة والسمات المخصصة وفقا للمتطلبات.



لتكوين مجموعات الأوامر، انتقل إلى **عناصر النهج > التخويل والأذونات > إدارة الجهاز > مجموعات الأوامر**. انقر فوق **إنشاء** وتعبئة التفاصيل حسب المتطلب.



قم بتكوين خدمة الوصول المحددة في قاعدة تحديد الخدمة وفقا للمتطلبات.لتكوين قواعد خدمة الوصول، انتقل إلى **سياسات الوصول > خدمات الوصول >مسؤول الجهاز الافتراضي > الهوية** حيث يمكن تحديد مخزن الهوية الذي يلزم إستخدامه للمصادقة. يمكن تكوين قواعد التخويل من خلال الانتقال إلى **سياسات الوصول > خدمات الوصول >مسؤول الجهاز الافتراضي > التفويض.**

> **ملاحظة**: قد يختلف تكوين سياسات التخويل وواجهات shell الخاصة بأجهزة معينة وذلك خارج نطاق هذا المستند.

التحقق من الصحة

أستخدم هذا القسم للتأكد من أن التكوين يعمل بشكل صحيح.

ويمكن التحقق من الصحة على كل من ISE و ACS. وأي خطأ في تكوين ISE أو ACS سيؤدي إلى فشل المصادقة. ACS هو الخادم الأساسي الذي سيتولى معالجة طلبات المصادقة والتفويض، ويتحمل ISE المسؤولية تجاه خادم ACS ومنه، كما يعمل وكيل للطلبات. بما أن الحزمة تعبر من خلال كل الخادمين، فإن التحقق من المصادقة أو طلب التخويل يمكن أن

يتم على كل الخادمين.

يتم تكوين أجهزة الشبكة باستخدام ISE كخادم TACACS وليس ACS. وبالتالي يصل الطلب إلى ISE أولا، واستادا إلى القواعد التي تم تكوينها، يقرر ISE ما إذا كان الطلب بحاجة إلى إعادة توجيهه إلى خادم خارجي. يمكن التحقق من هذا الإجراء في سجلات TACACS Live على ISE.

لعرض السجلات المباشرة على ISE، انتقل إلى **العمليات > TACACS > السجلات المباشرة.** يمكن مشاهدة التقارير المباشرة على هذه الصفحة ويمكن مراجعة تفاصيل طلب معين بالنقر فوق رمز العدسة المكبرة المتعلق بذلك الطلب المحدد ذي الأهمية.

Steps

13020	Get TACACS+ default network device setting
13013	Received TACACS+ Authentication START Request
15049	Evaluating Policy Group
15008	Evaluating Service Selection Policy
15048	Queried PIP - Network Access.Protocol
15006	Matched Default Rule
13064	TACACS proxy received incoming request for forwarding.
13065	TACACS proxy received valid incoming authentication request.
13063	Start forwarding request to remote TACACS server.
13074	Finished to process TACACS Proxy request.
13020	Get TACACS+ default network device setting
13014	Received TACACS+ Authentication CONTINUE Request
13064	TACACS proxy received incoming request for forwarding.
13065	TACACS proxy received valid incoming authentication request.
13071	Continue flow (seq_no > 1).
13063	Start forwarding request to remote TACACS server.
13074	Finished to process TACACS Proxy request.

لعرض تقارير المصادقة على ACS، انتقل إلى **المراقبة والتقارير > مراقبة بدء التشغيل (AAA) والمحاسبة والتفويض والمصادقة بروتوكول المراقبة والتقارير > وعارض التقارير > مصادقة TACACS.** مثل ISE، يمكن مراجعة تفاصيل طلب معين بالنقر فوق أيقونة العدسة المكبرة المتعلقة بذلك الطلب المحدد الذي له أهمية

استكشاف الأخطاء وإصلاحها

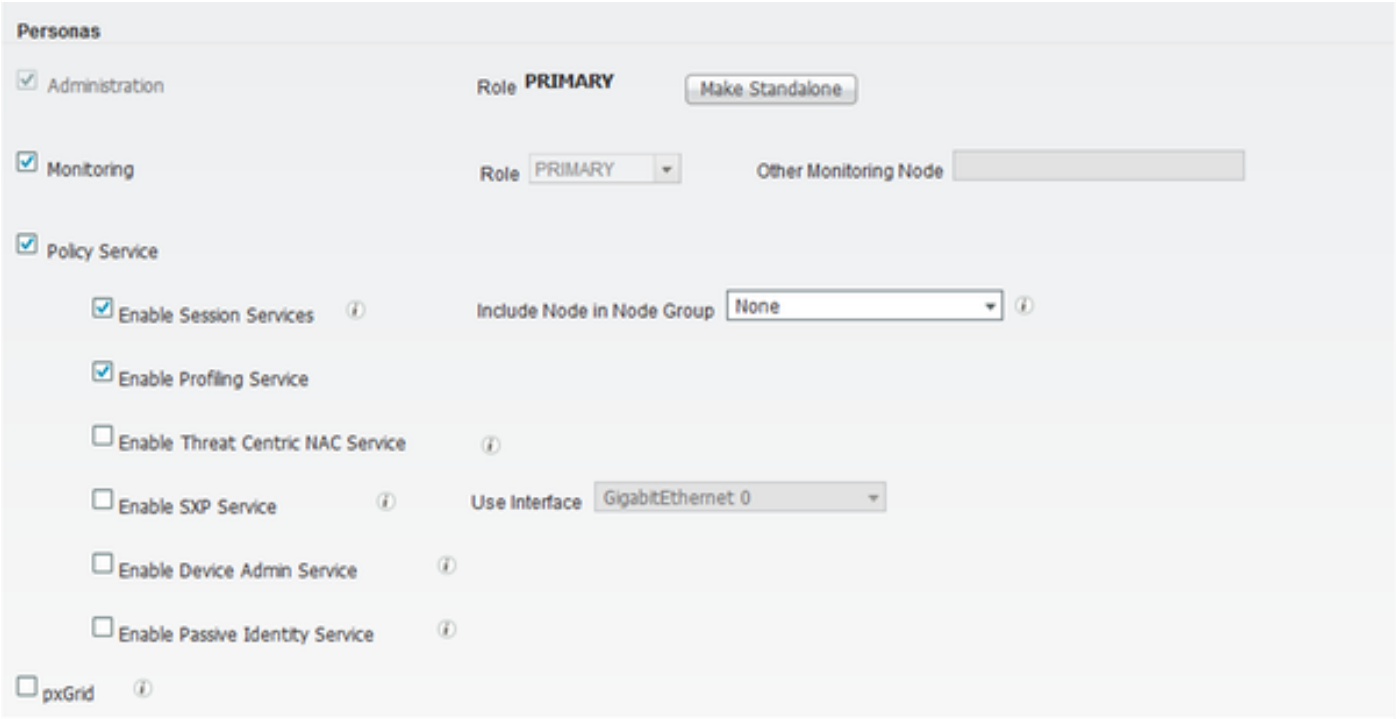
يوفر هذا القسم معلومات يمكنك استخدامها لاستكشاف أخطاء التكوين وإصلاحها

1. إذا أظهرت تفاصيل التقرير على ISE رسالة الخطأ الموضحة في الشكل، فإنها تشير إلى سر مشترك غير صالح تم تكوينه على ISE أو جهاز الشبكة (NAD).

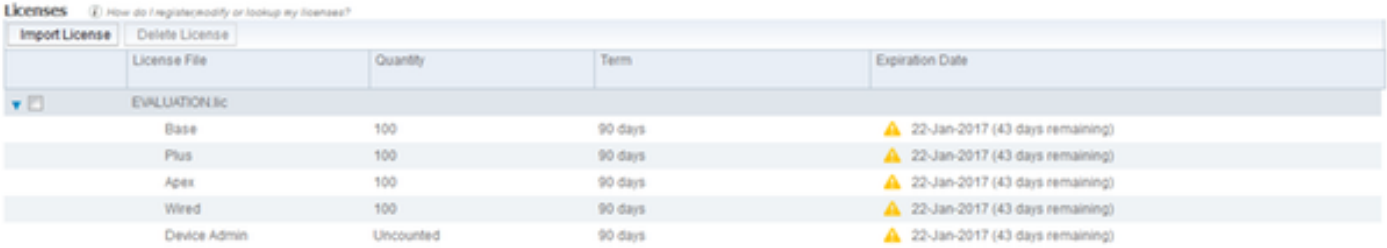
Message Text	TACACS: Invalid TACACS+ request packet - possibly mismatched Shared Secrets

2. في حالة عدم وجود تقرير مصادقة لطلب على ISE ولكن يتم رفض وصول المستخدم النهائي إلى جهاز الشبكة، يشير ذلك عادة إلى عدة أمور.

- لم يصل الطلب نفسه إلى خادم ISE.
- إذا تم تعطيل خدمة إدارة الأجهزة على ISE، فسيتم إسقاط أي طلب من TACACS+ إلى ISE بصمت. لن يتم عرض أي سجلات تشير إلى نفس ذلك في التقارير أو سجلات Live. للتحقق من ذلك، انتقل إلى **إدارة > نظام > نشر > [حدد العقدة]. انقر فوق تحرير** ولاحظ خانة الاختيار **تمكين خدمة إدارة الأجهزة** أسفل علامة التبويب **الإعدادات العامة** كما هو موضح في الشكل. يجب التحقق من خانة الاختيار هذه لكي تعمل "إدارة الأجهزة" على ISE.



- إذا لم يكن ترخيص إدارة الجهاز موجودا بعد انتهاء مدة صلاحيته، فسيتم إسقاط جميع طلبات TACACS+ بصمت. لا يتم عرض أي سجلات في واجهة المستخدم الرسومية لنفسه. انتقل إلى **إدارة > نظام > ترخيص** للتحقق من ترخيص إدارة الجهاز.



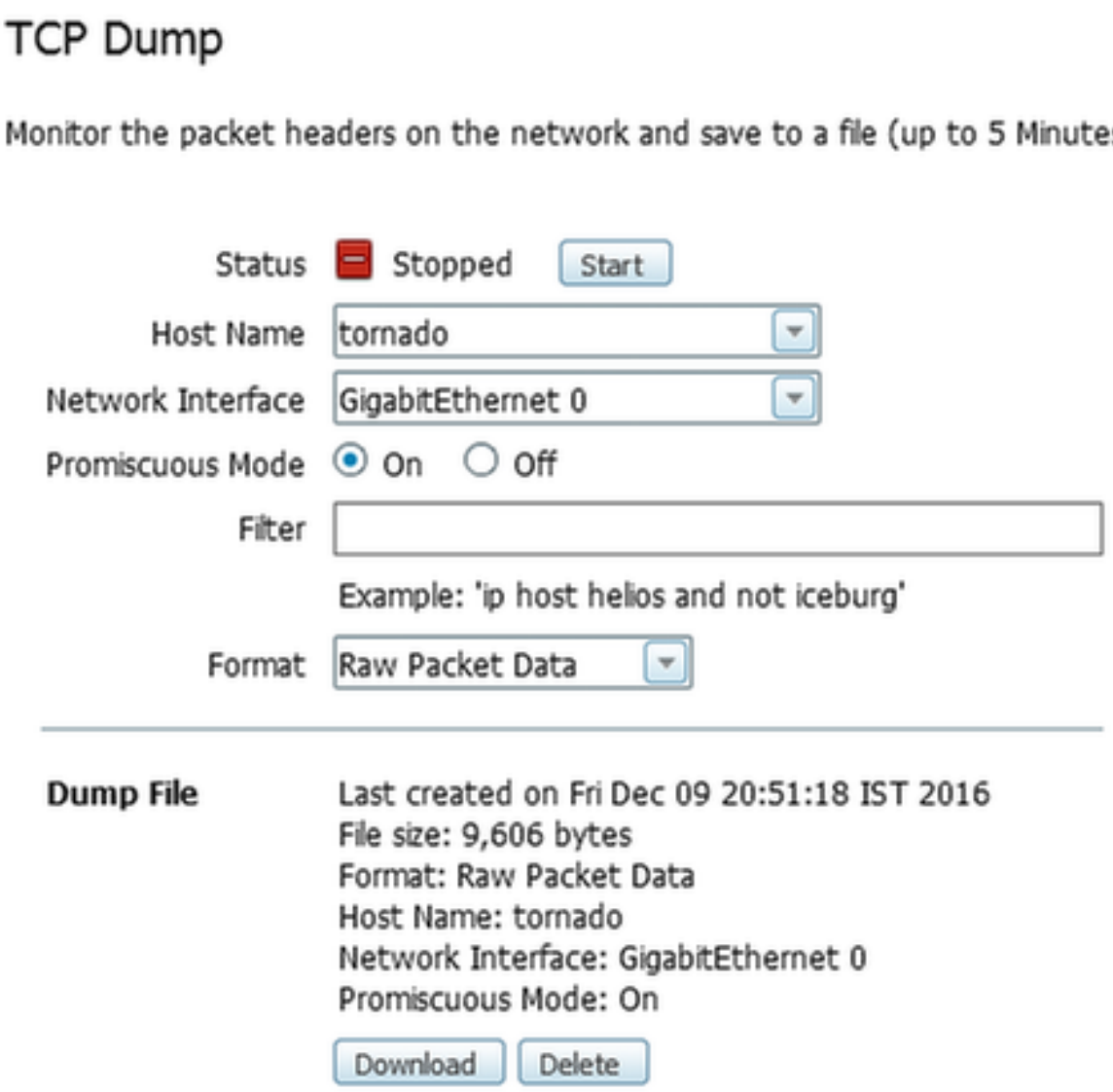
- إذا لم يتم تكوين جهاز الشبكة أو إذا تم تكوين IP لجهاز شبكة غير صحيح على ISE، فسيقوم ISE بإسقاط الحزمة بصمت. لم يتم إرسال أي إستجابة إلى العميل ولا يتم عرض أي سجلات في واجهة المستخدم الرسومية. وهذا تغير في سلوك ISE لـ TACACS+ عند مقارنته بسلوك ACS الذي يعلم بأن الطلب جاء من جهاز شبكة غير معروف أو عميل AAA.

- وصل الطلب إلى ACS ولكن الاستجابة لم تعد إلى ISE. يمكن التحقق من هذه السيناريو من التقارير المتعلقة بمصدر المحتوى الإضافي كما هو موضح في الشكل. وعادة ما يكون ذلك بسبب سر مشترك غير صالح إما على ACS الذي تم تكوينه لـ ISE أو على ISE الذي تم تكوينه لـ ACS.

- لن يتم إرسال الاستجابة حتى إذا لم يتم تكوين ISE أو لم يتم تكوين عنوان IP الخاص بواجهة إدارة ISE على ACS في تكوين جهاز الشبكة. في مثل هذا القطاع، يمكن ملاحظة الرسالة في الشكل على الـ ACS.

- إذا تم الاطلاع على تقرير مصادقة ناجح على ACS ولكن لا يتم مشاهدة أي تقارير على

ISE ويتم رفض المستخدم، فقد يكون ذلك مشكلة في الشبكة. يمكن التحقق من هذه الإجراء من خلال التقاط حزمة على ISE باستخدام عوامل التصفية الضرورية. لتجميع التقاط حزمة على ISE، انتقل إلى **العمليات > أستكشاف الأخطاء وإصلاحها > أدوات التشخيص > أدوات عامة > تفريغ TCP.**



3. إذا كان يمكن عرض التقارير على ISE ولكن ليس على ACS، فقد يعني ذلك إما أن الطلب لم يصل إلى ACS بسبب تكوين خاطئ لمجموعات السياسات على ISE والتي يمكن أستكشاف الأخطاء وإصلاحها استنادا إلى التقرير التفصيلي عن ISE أو بسبب مشكلة في الشبكة يمكن تحديدها بواسطة التقاط حزمة على ACS.

4. إذا تم الاطلاع على التقارير على كل من ISE و ACS ولكن لا يزال المستخدم ممنوعا من الوصول، فإنها تكون في الغالب مشكلة في تكوين سياسات الوصول على ACS والتي يمكن أستكشاف الأخطاء وإصلاحها استنادا إلى التقرير التفصيلي حول ACS. كما يجب السماح بحركة المرور العائدة من ISE إلى جهاز الشبكة.

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).