قائمة التحكم في الوصول (ACL) القابلة للتنزيل في محولات Catalyst 1300 Switches

الهدف

الهدف من هذا المقال هو توضيح كيفية عمل قائمة التحكم في الوصول القابلة للتنزيل (DACL) على محولات Cisco Catalyst 1300 Switches باستخدام محرك خدمة الهوية (ISE) من Cisco.

الأجهزة القابلة للتطبيق | إصدار البرامج

- Catalyst 1300 Series | 4.1.6.54

المقدمة

قوائم التحكم في الوصول (ACL) الديناميكية هي قوائم التحكم في الوصول (ACL) التي تم تعيينها لمنفذ محول بناء على سياسة أو معايير مثل عضوية مجموعة حساب المستخدم، والوقت من اليوم، وغير ذلك. يمكن أن تكون قوائم تحكم في الوصول (ACL) محلية تم تحديدها بواسطة معرف عامل التصفية أو قوائم التحكم في الوصول (DACL) القابلة للتنزيل.

قوائم التحكم في الوصول (ACL) القابلة للتنزيل هي قوائم تحكم في الوصول (ACL) ديناميكية يتم إنشاؤها وتنزيلها من خادم Cisco ISE. وهم يطبقون بشكل ديناميكي قواعد التحكم في الوصول استنادا إلى هوية المستخدم ونوع الجهاز. تتمتع قائمة التحكم في الوصول الخاصة بالمنفذ (DACL) بميزة السماح لك بامتلاك مستودع مركزي واحد لقوائم التحكم في الوصول (ACL)، وبالتالي لا تحتاج إلى إنشاؤها يدويا على كل محول. عندما يتصل مستخدم بمحول، فإن يحتاج فقط إلى المصادقة، وسيقوم المحول بتنزيل قوائم التحكم في الوصول (ACL) القابلة للتطبيق من خادم Cisco ISE.

إستخدام حالات قوائم التحكم في الوصول (ACL) القابلة للتنزيل

1. سيتلقى المستخدمون المختلفون قوائم تحكم في الوصول (ACL) مختلفة عند إتصالهم بمحول (مستخدمو ISE المحليون).
2. يمكن للمستخدمين الذين لديهم اتصال محدود بالشبكة تسجيل الدخول إلى بوابة ويب مركزية للوصول الكامل إلى الشبكة (المصادقة المركزية للويب).
3. متقدم - إستخدام تجاوز مصادقة MAC (MAB) للسماح بالاتصال ب Windows Active Directory (AD) وبعض الخدمات ذات الصلة أثناء توصيل خادم ISE ب AD ومرافبة مصادقة المستخدم. قبل تسجيل الدخول إلى Windows AD، ستسمح الشبكة بالوصول إلى موارد محدودة جدا فقط، ولكن ستقوم مصادقة AD بتنزيل قوائم التحكم بالوصول (ACL) مختلفة استنادا إلى مجموعات Windows وتسمح بالوصول الكامل إلى الشبكة.

4 خيارات متقدمة - يتلقى المستخدمون قوائم تحكم في الوصول (ACL) مختلفة استنادا إلى يوم الأسبوع أو الوقت من اليوم أو أي عامل آخر بسبب السياسات على خادم ISE.

في هذه المقالة، ستناقش حالة الاستعمال الاول بالتفصيل.

جدول المحتويات

المتطلبات الأساسية

- تأكد من ترقية المحول Catalyst 1300 switch إلى أحدث البرامج الثابتة (يجب أن يكون البرنامج الثابت للمحول هو 4.1.6 أو أعلى).
- عينت ساكن إستاتيكي ip إلى المفتاح لأغراض الإدارة.

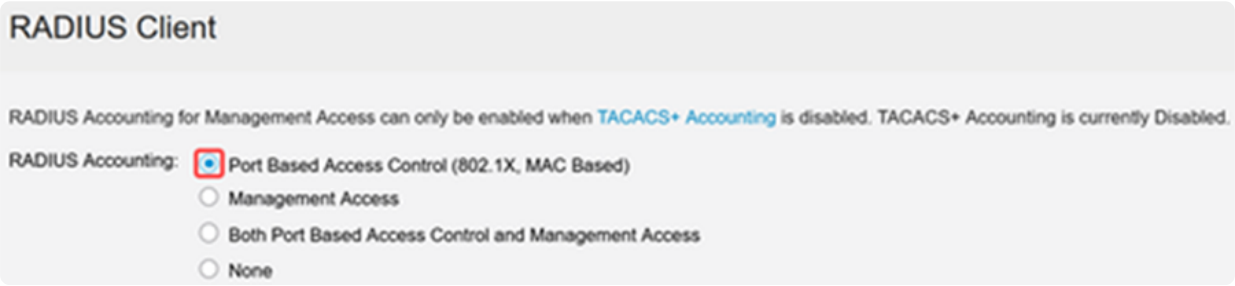
تكوين عميل RADIUS

الخطوة 1

قم بتسجيل الدخول إلى المحول Catalyst 1300 switch وانتقل إلى الأمان > قائمة عميل RADIUS.

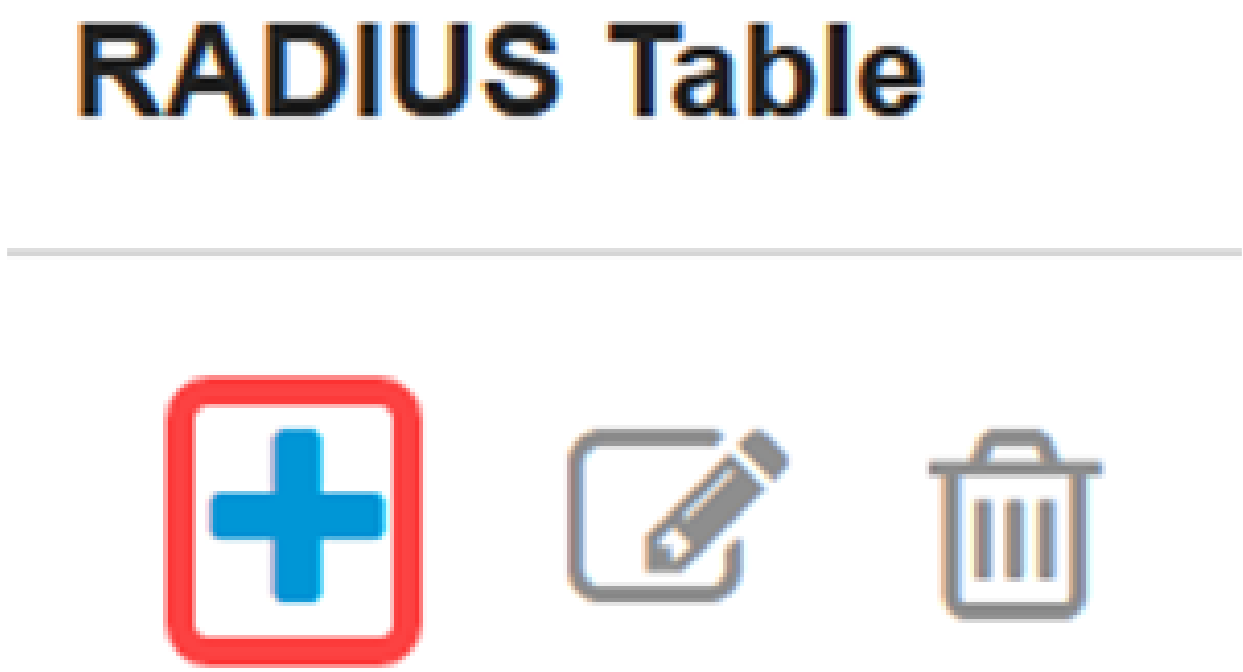
الخطوة 2

لمحاسبة RADIUS، حدد خيار التحكم في الوصول المستند إلى المنفذ.



الخطوة 3

تحت جدول RADIUS، انقر على أيقونة زائد لإضافة خادم Cisco ISE.



الخطوة 4

أدخل تفاصيل خادم Cisco ISE وانقر فوق تطبيق.

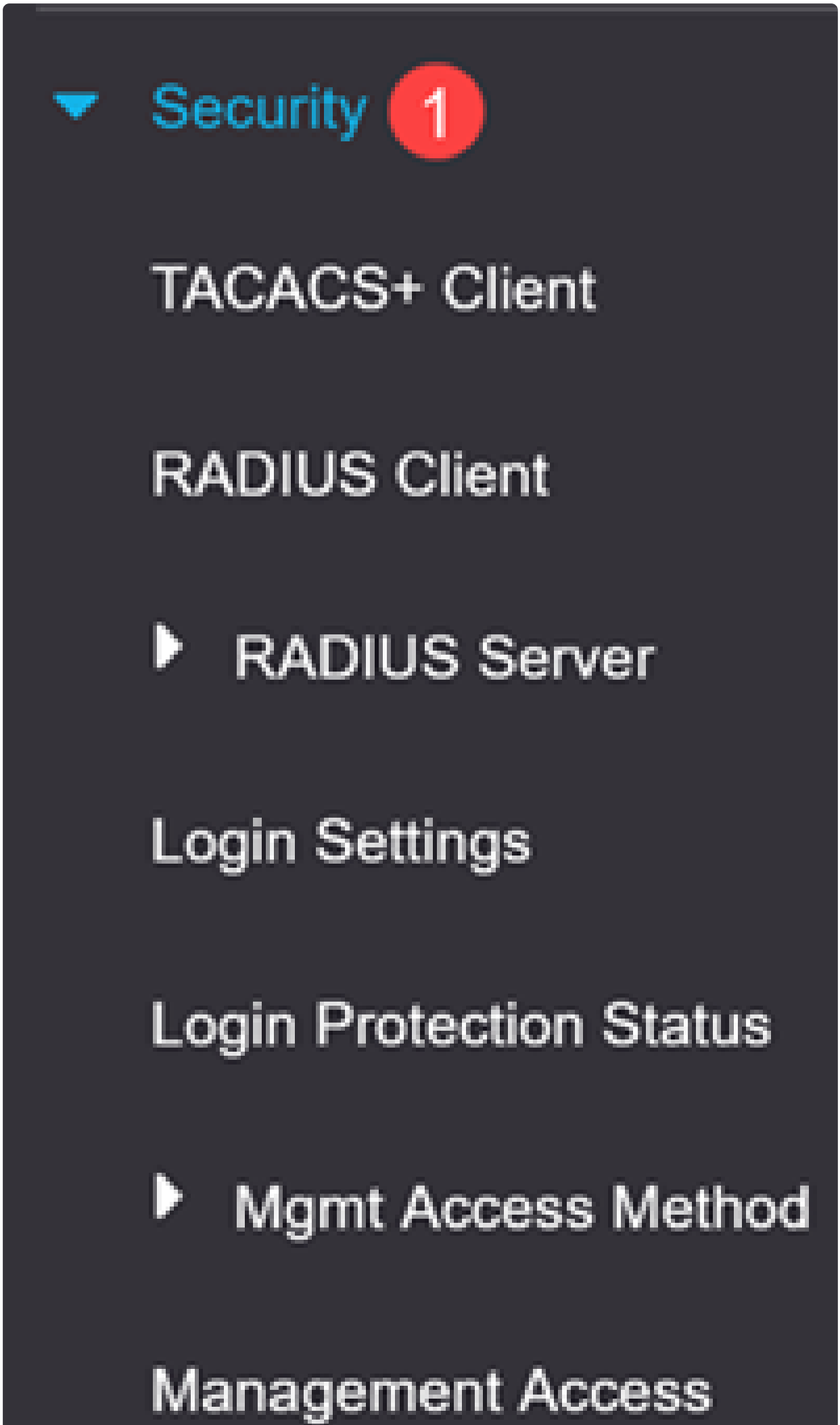
Note:

يجب تحديد نوع الاستخدام ك 802.1x.

تكوين مصادقة 802.1x

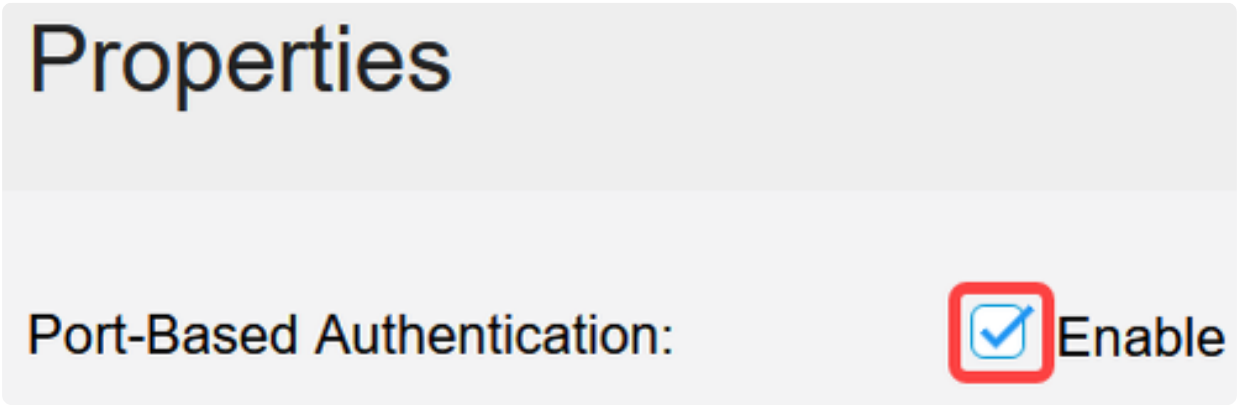
الخطوة 1

انتقل إلى التأمين > مصادقة 802. 1X > قائمة خصائص.


Security 1
TACACS+ Client
RADIUS Client
RADIUS Server
Login Settings
Login Protection Status
Mgmt Access Method
Management Access

الخطوة 2

انقر فوق خانة الاختيار لتمكين المصادقة المستندة إلى المنفذ.

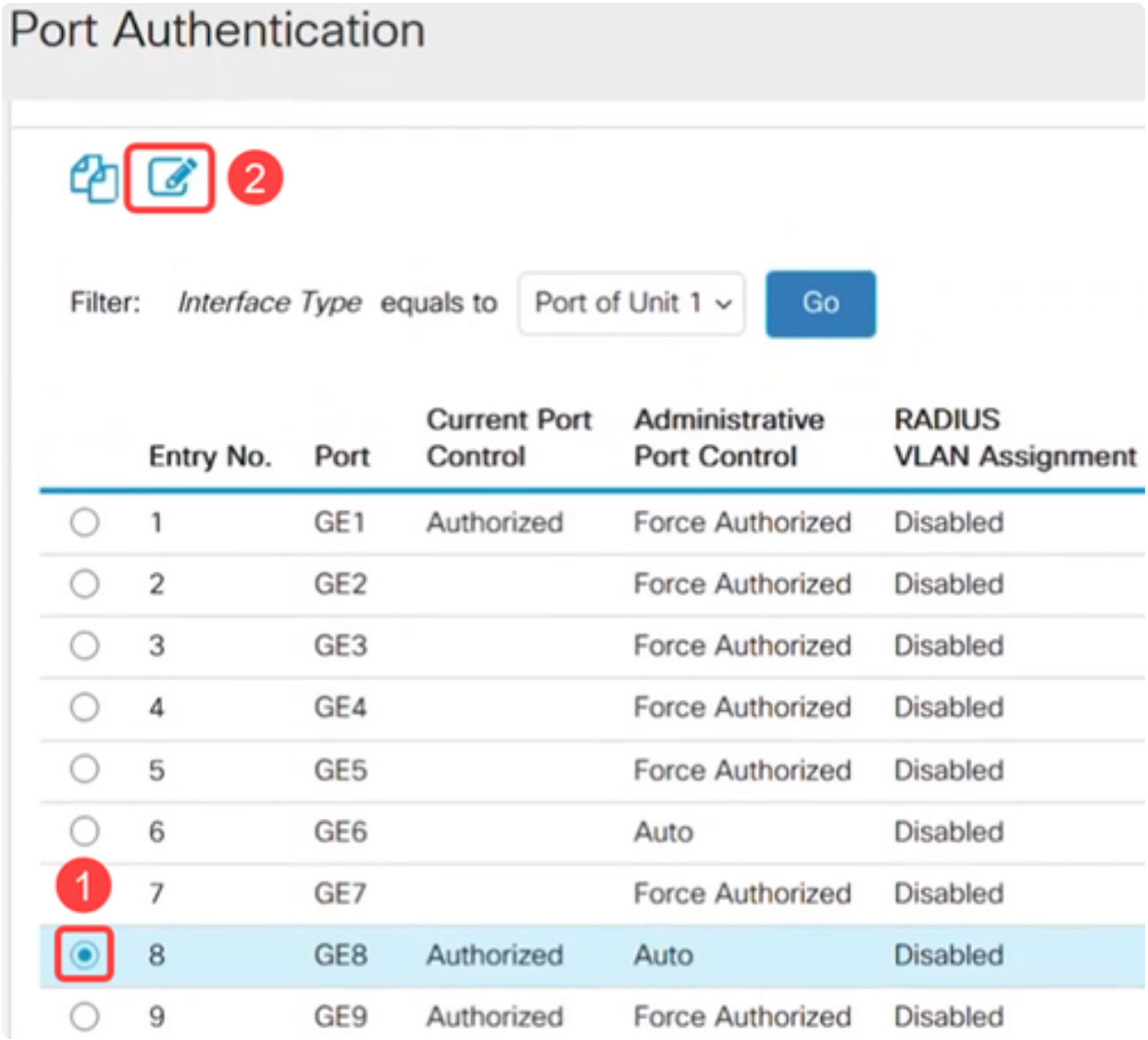


الخطوة 3

تحت أسلوب المصادقة، حدد RADIUS وانقر فوق تطبيق.

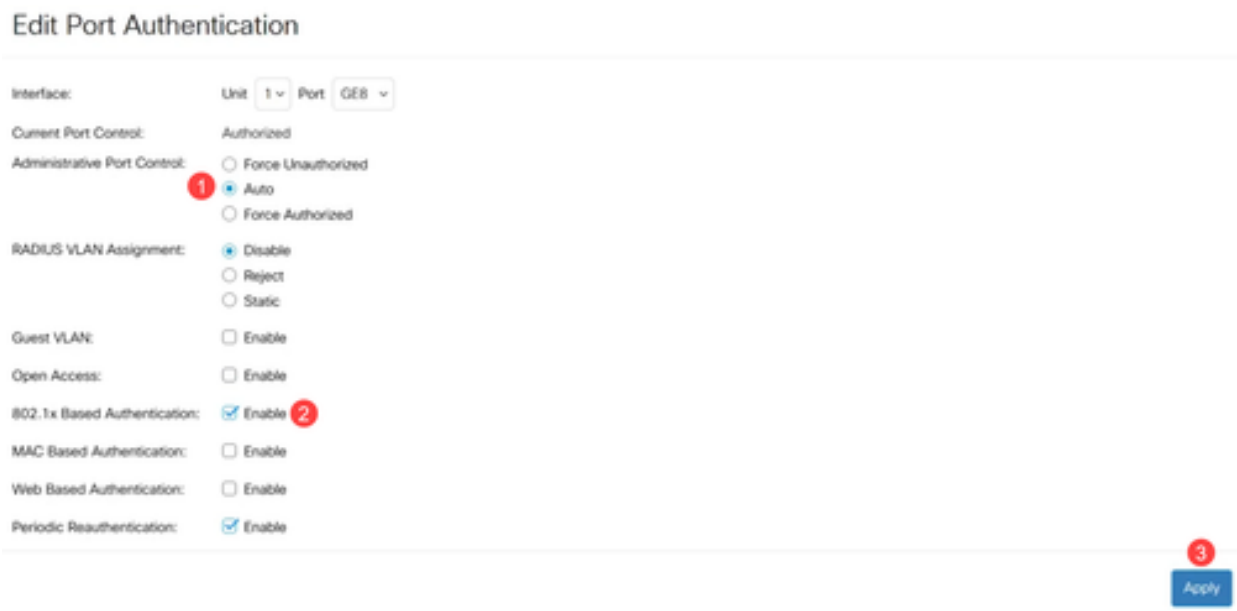
الخطوة 4

انتقل إلى الأمان > مصادقة 802.1X>قائمة مصادقة المنفذ. حدد المنفذ الذي يتم توصيل الكمبيوتر المحمول به ثم انقر على رمز تحرير. في هذا المثال، يتم تحديد GE8.



الخطوة 5

حدد التحكم في المنفذ الإداري على أنه تلقائي وقم بتمكين المصادقة المستندة إلى 802.1x. انقر فوق تطبيق.



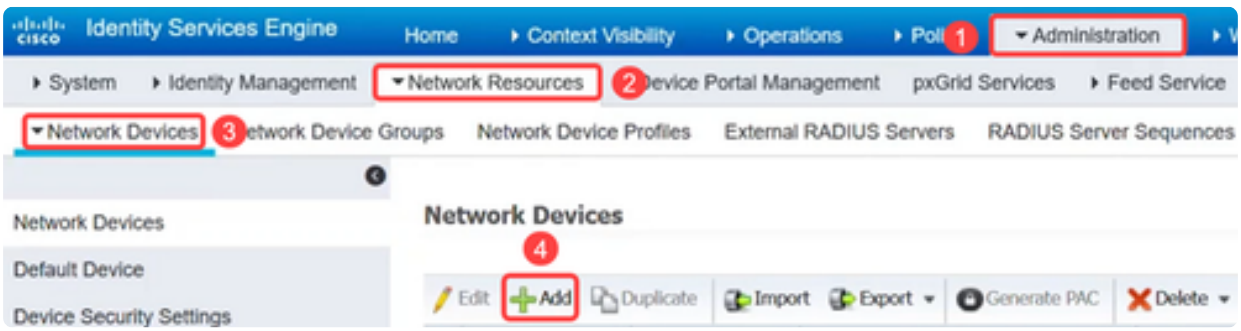
تكوين خادم Cisco ISE لقوائم التحكم في الوصول (ACL) القابلة للتنزيل

> **Note:**
> يتجاوز تكوين ISE نطاق دعم الأعمال من Cisco. راجع دليل مسؤول ISE للحصول على مزيد من المعلومات.

التكوينات الموضحة في هذه المقالة هي مثال لقائمة التحكم في الوصول (ACL) القابلة للتنزيل للعمل مع المحول Cisco Catalyst 1300 Series Switch.

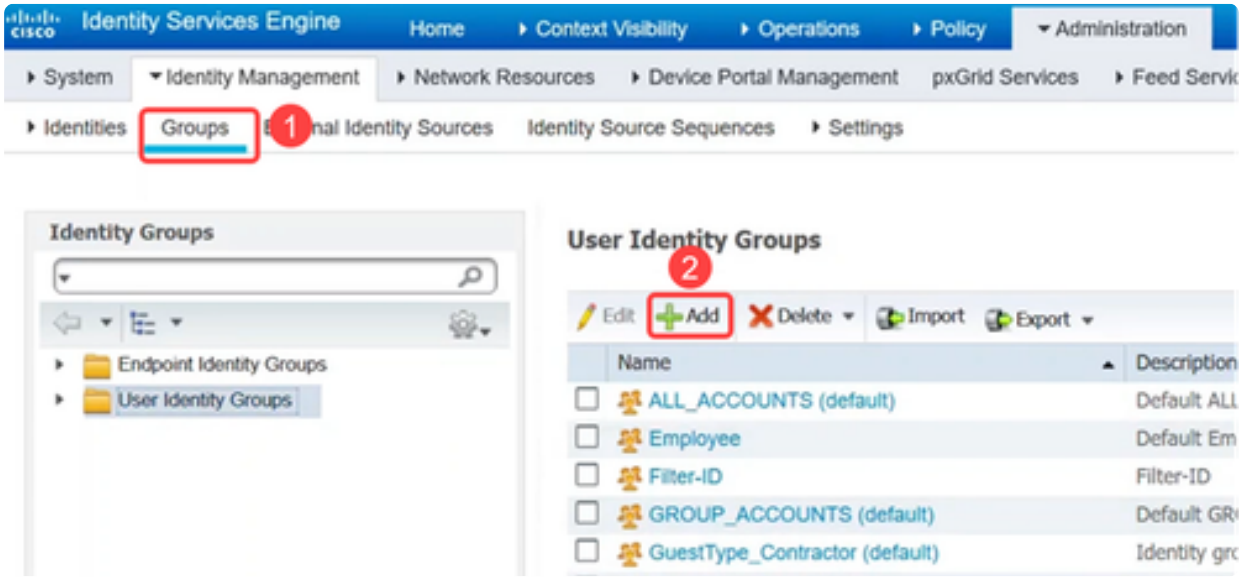
الخطوة 1

قم بتسجيل الدخول إلى خادم Cisco ISE الخاص بك وانتقل إلى إدارة > موارد الشبكة > أجهزة الشبكة وأضف جهاز المحول Catalyst switch.



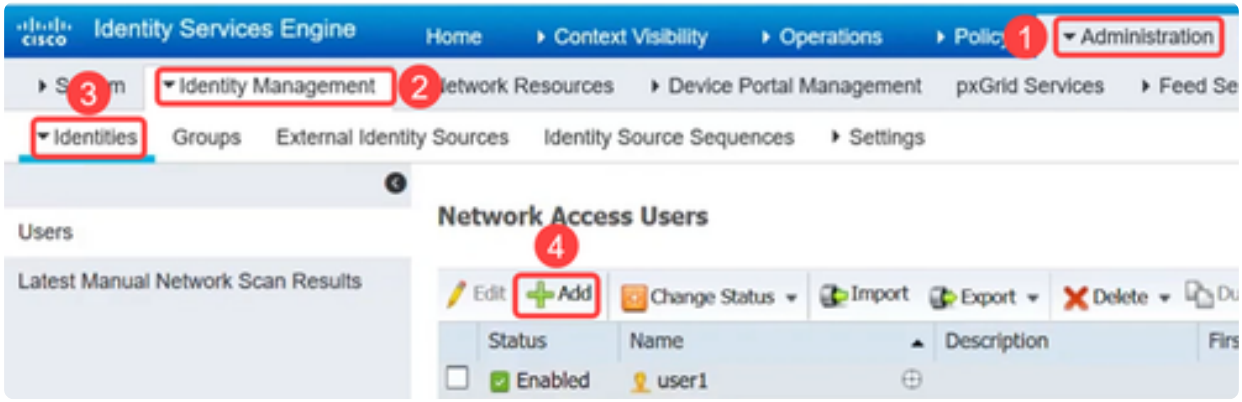
الخطوة 2

لإنشاء مجموعات هوية المستخدم، انتقل إلى علامة التبويب مجموعات أو ضف مجموعات هوية المستخدم.



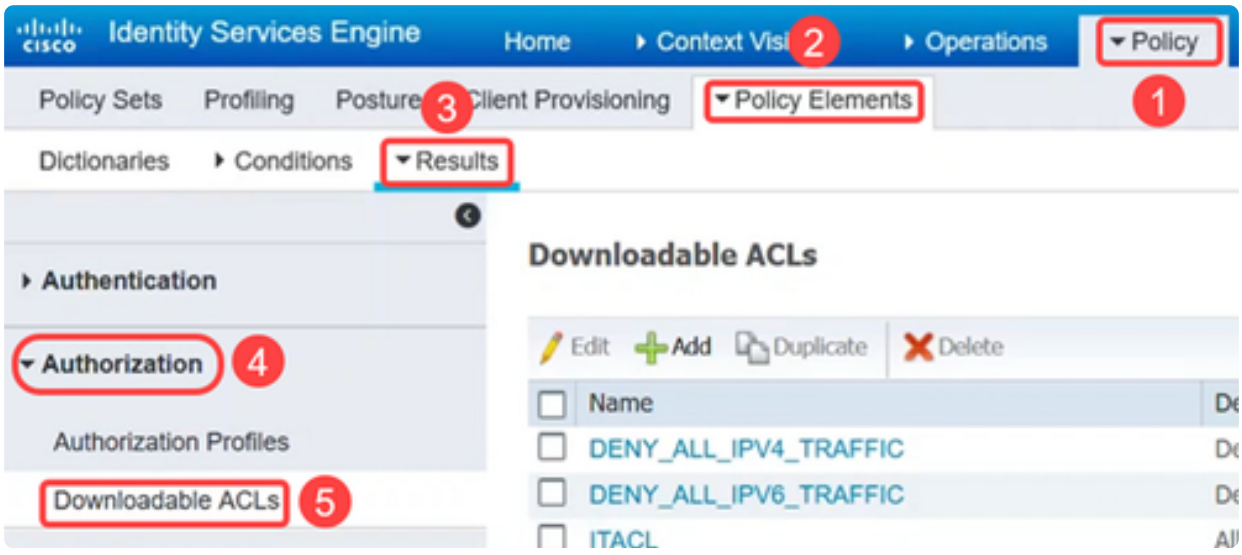
الخطوة 3

انتقل إلى قائمة الإدارة > إدارة الهوية > الهويات لتعريف المستخدمين ولتعيين المستخدمين إلى المجموعات.



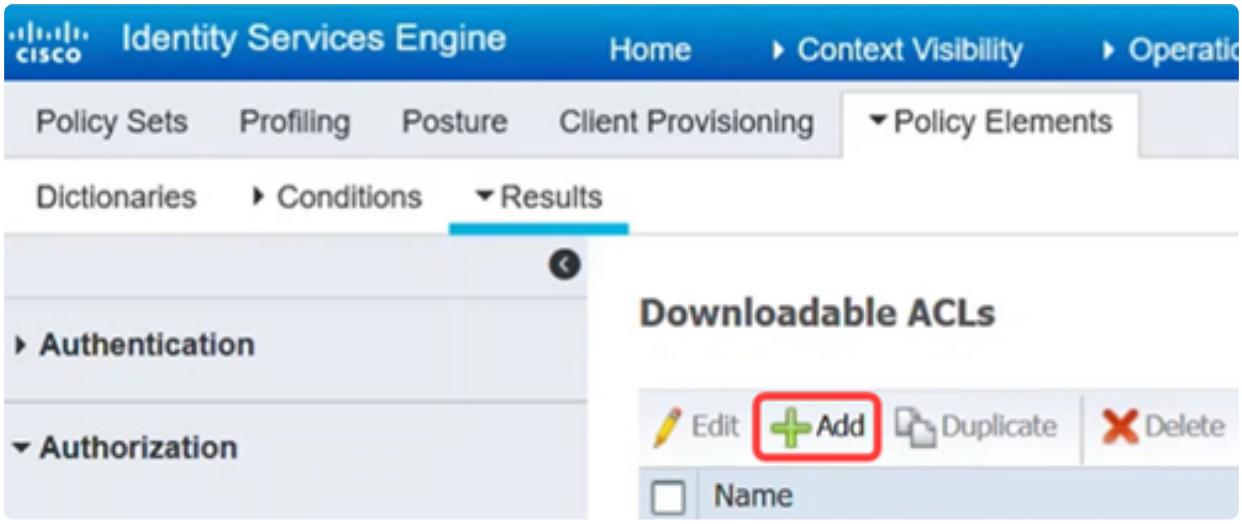
الخطوة 4

انتقل إلى السياسة > عناصر السياسة > قائمة النتائج. تحت التخويل، انقر على قوائم التحكم في الوصول (ACL) القابلة للتنزيل.



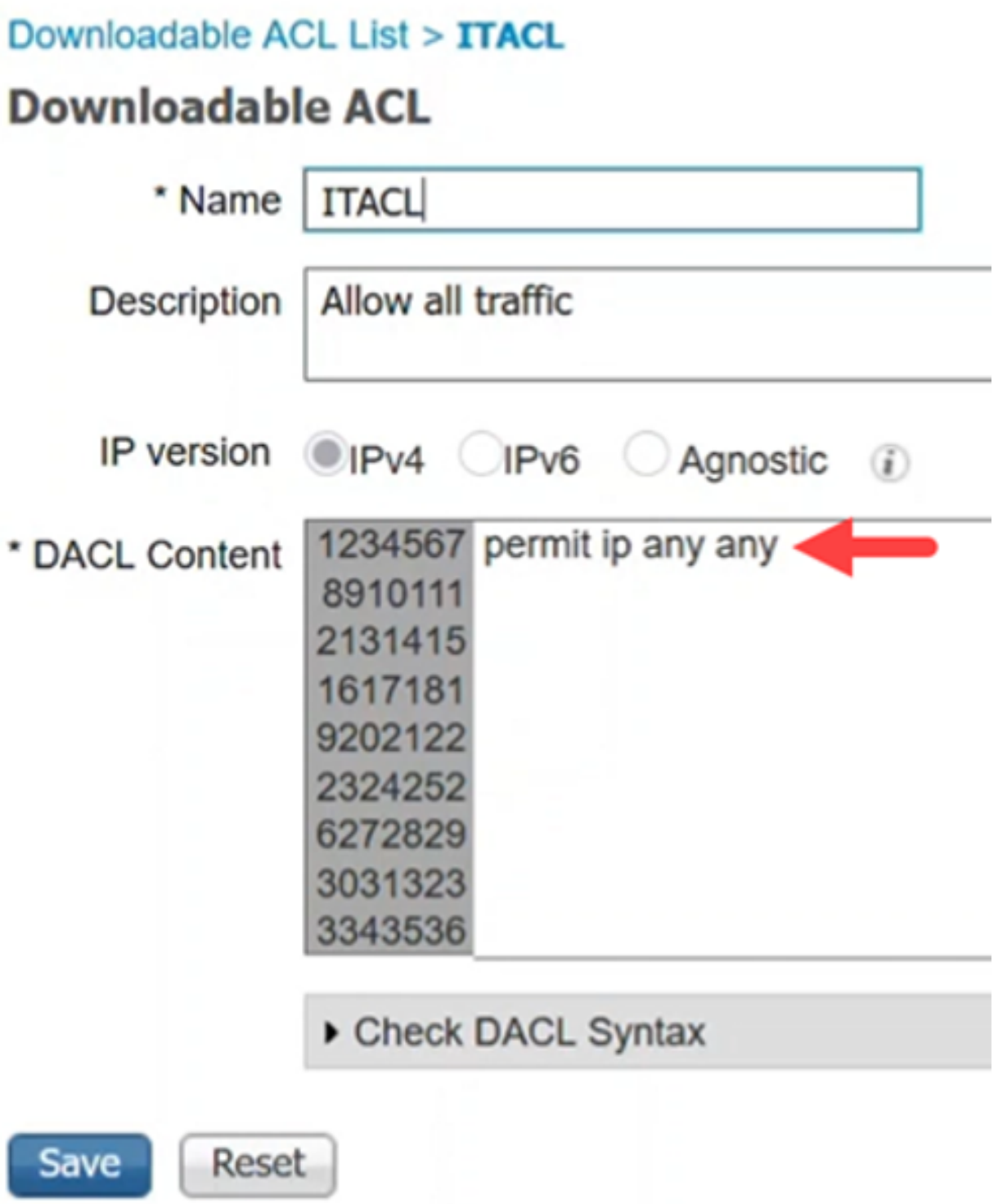
الخطوة 5

انقر فوق أيقونة الإضافة لإنشاء قائمة التحكم في الوصول (ACL) القابلة للتنزيل.



الخطوة 6

قم بتكوين الاسم والوصف، وحدد إصدار IP، وأدخل إدخالات التحكم في الوصول (ACEs) التي ستشكل قائمة التحكم في الوصول (ACL) القابلة للتنزيل في حقل محتوى قائمة التحكم في الوصول (DACL). انقر فوق حفظ.



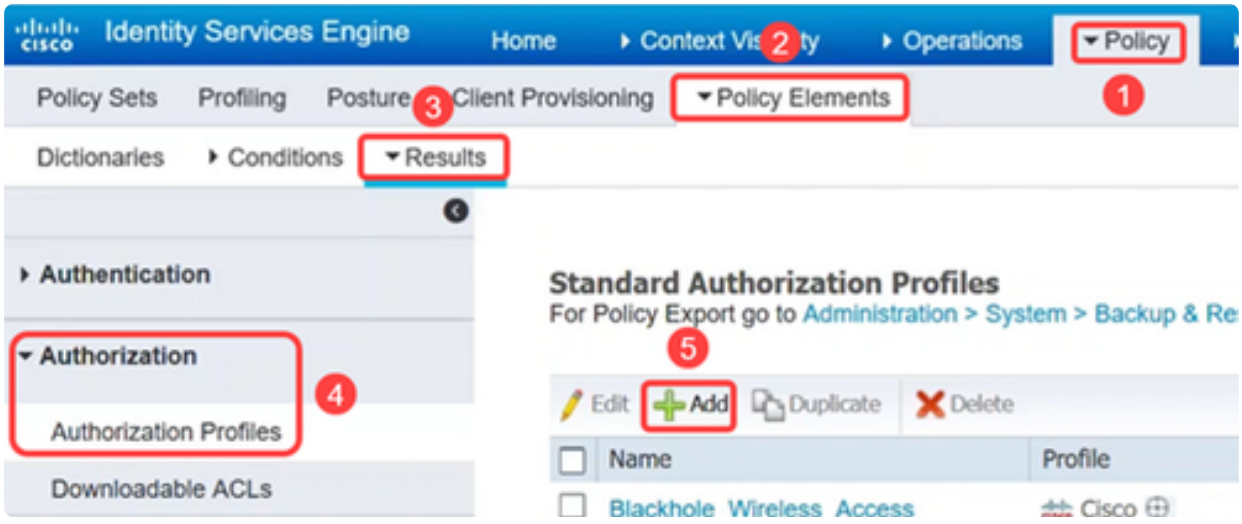
Note:

يتم دعم قوائم التحكم في الوصول إلى IP فقط، ويجب أن يكون المصدر أي. بالنسبة لقائمة التحكم في الوصول (ACL) على ISE، يتم دعم IPv4 فقط الآن. إذا تم إدخال قائمة التحكم في الوصول مع مصدر آخر، بينما قد تكون الصياغة جيدة بقدر ما يتعلق ISE، فإنها ستفشل عند تطبيقها على المحول.

الخطوة 7

إنشاء ملفات تعريف التفويض التي سيتم إستخدامها لربط قائمة التحكم في الوصول الخاصة بك (DACL) والنهج الأخرى معا بشكل منطقي داخل مجموعات نهج ISE.

للقيام بذلك، انتقل إلى السياسة > عناصر السياسة > النتائج > التخويل > ملفات تخصيص التخويل وانقر على إضافة.

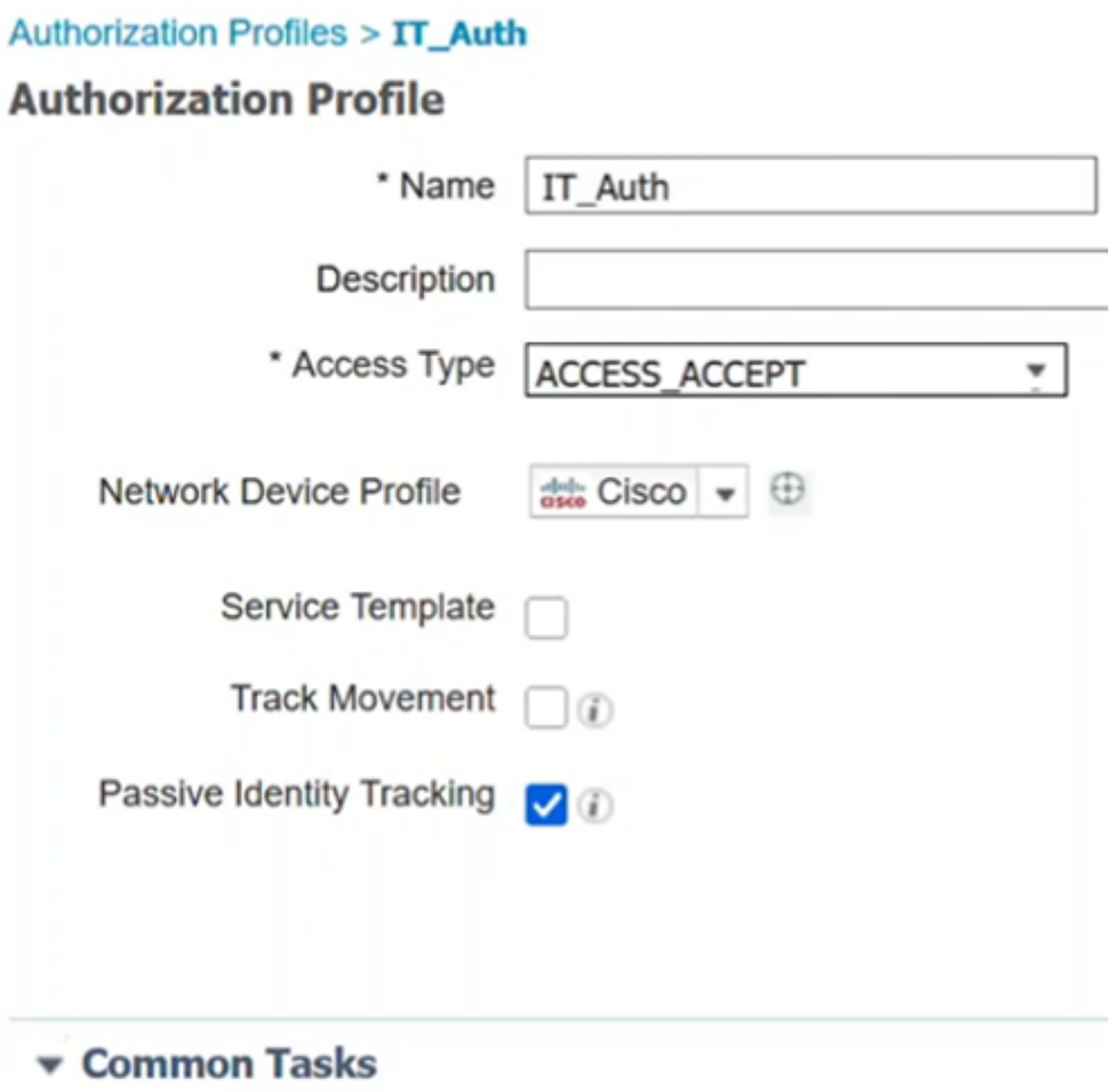


الخطوة 8

في صفحة ملف تعريف التخويل، قم بتكوين ما يلي:

- الاسم
- الوصف
- نوع الوصول - يجب تعيين هذا إلى ACCESS_ACCEPT. في حالة تعيينه إلى ACCESS_REJECT فإنه سيرفض المصادقة.
- ملف تعريف جهاز الشبكة - يجب تحديد هذا كشركة Cisco.
- تعقب الهوية السلبي - قد يلزم تمكينه لبعض سيناريوهات المصادقة. وهو مطلوب لسيناريوهات EasyConnect_PassiveID المرتبطة ب AD.
- مهام مشتركة - يحتوي هذا القسم على العديد من الخيارات. لهذا المثال، يتم تكوين اسم قائمة التحكم في الوصول إلى البيانات (DACL).

انقر فوق حفظ.



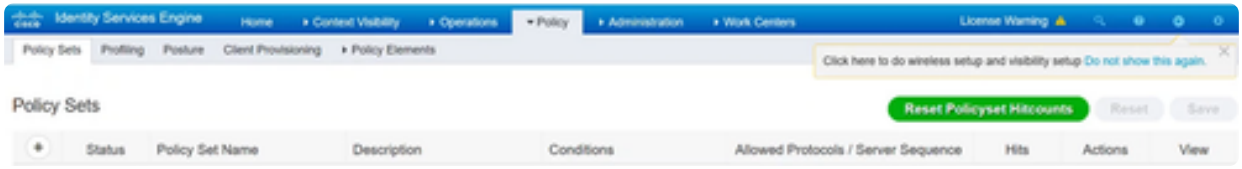
الخطوة 9

لتكوين مجموعات السياسات التي تعد تجميعا منطقيا لنهج المصادقة والتفويض، انقر فوق السياسة > قائمة مجموعات السياسات.

يمكنك عرض ما يلي عند النظر في قائمة بمجموعات النهج:

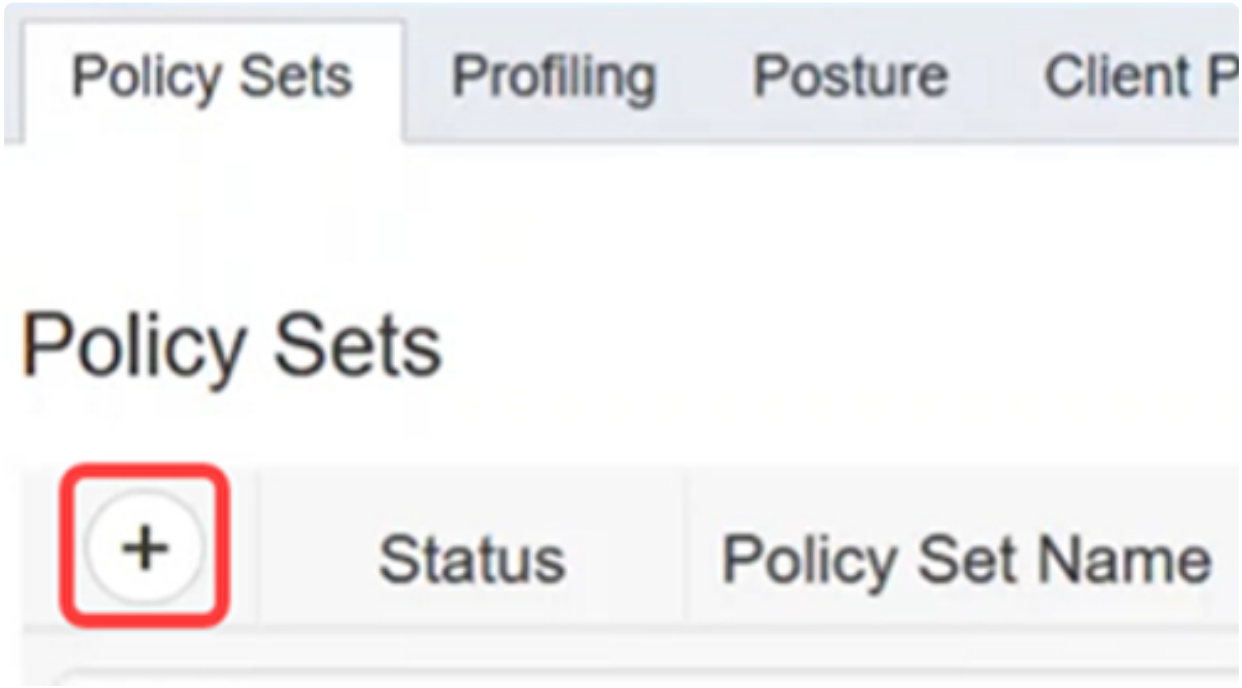
- الحالة - يشير التحقق الأخضر إلى تمكين، وتشير الدائرة البيضاء الفارغة إلى معطل، وتشير أيقونة العين إلى تكوين الشاشة فقط.
- اسم مجموعة النهج والوصف - توضيح ذاتي
- الشروط - قم بتعريف مكان تطبيق مجموعة السياسات.
- البروتوكولات/تسلسل الخادم المسموح به - يعمل على تعيين عناصر تحكم أكثر تقدما.
- Hits - إظهار عدد المرات التي تم فيها استخدام مجموعة النهج.
- الإجراءات - السماح لك بتغيير الترتيب الذي يمكن فيه تطبيق مجموعات النهج، أو نسخ مجموعة نهج موجودة، أو حذف مجموعة نهج موجودة.

- عرض - يسمح لك بتحرير تفاصيل مجموعة النهج.



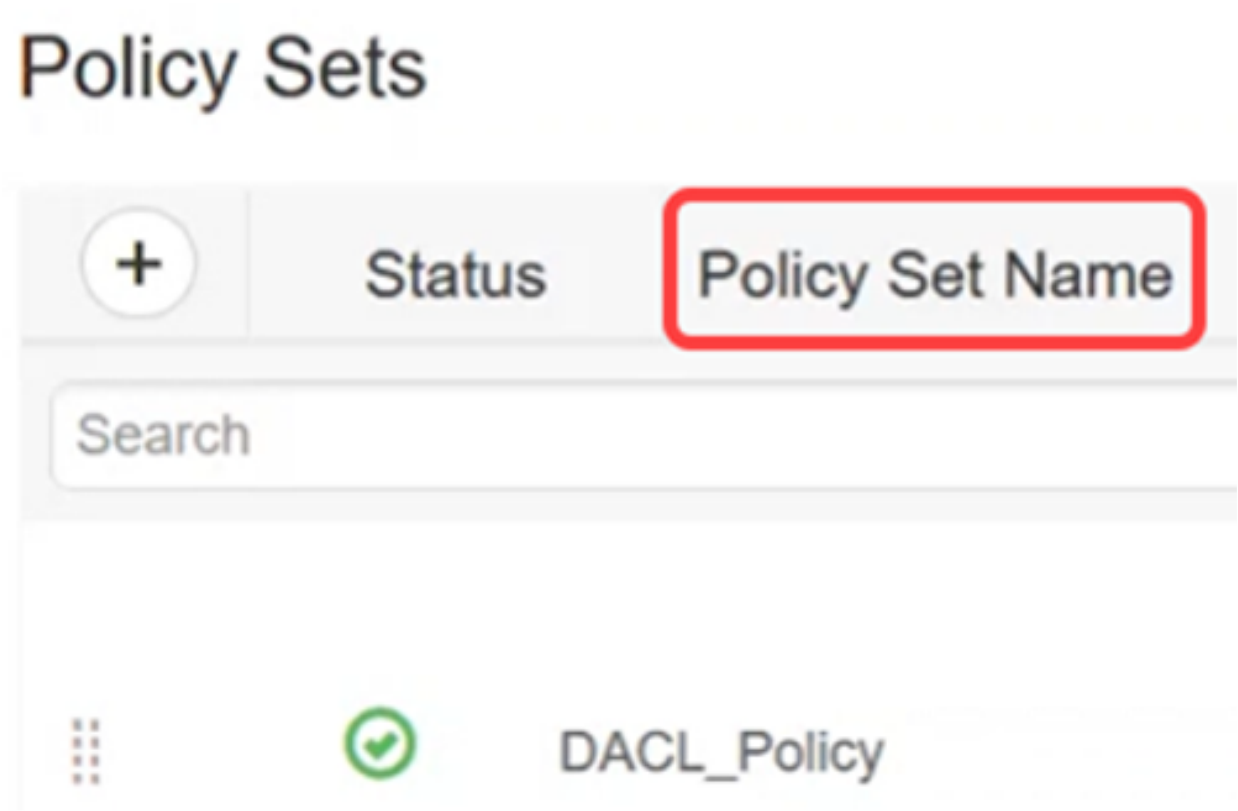
الخطوة 10

لإنشاء مجموعة نهج، انقر فوق الزر إضافة.



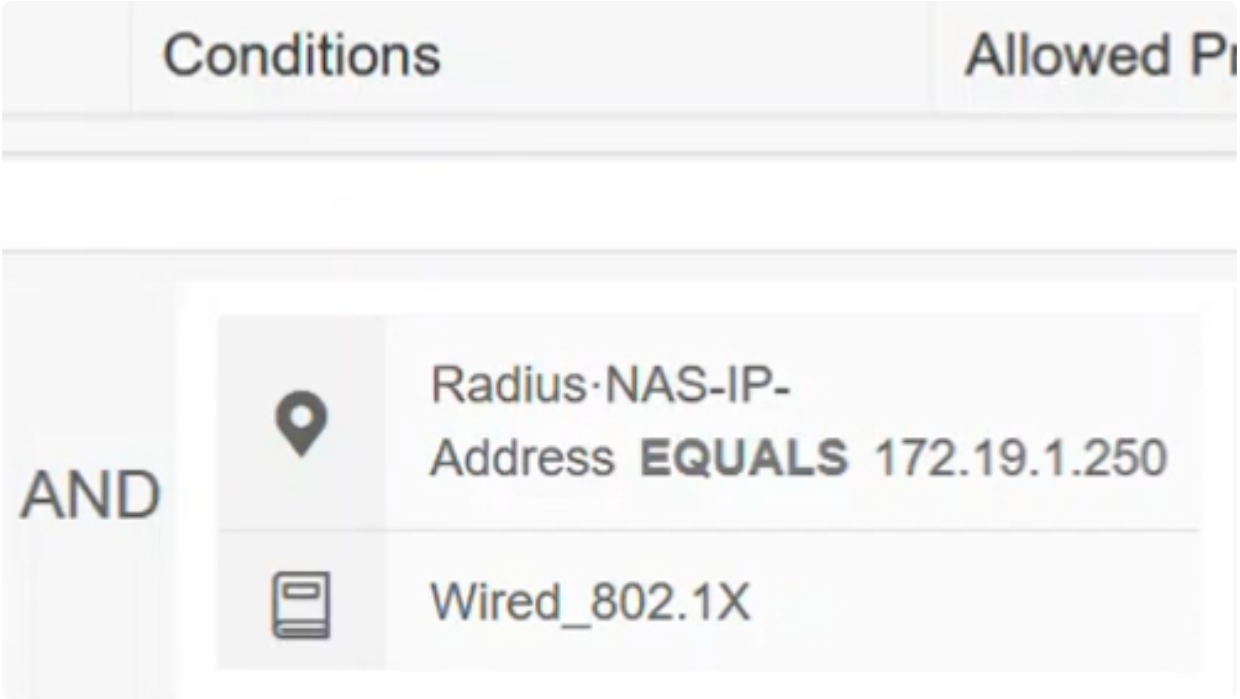
الخطوة 11

قم بتحديد اسم مجموعة نهج.



الخطوة 12

تحت الشروط، انقر فوق الزر إضافة. يؤدي هذا إلى فتح Conditions Studio حيث يمكنك تحديد المكان الذي سيتم إستخدام ملف تعريف المصادقة هذا فيه. في هذا المثال، تم تطبيقه على RADIUS-NAS-IP-Address (المحول) وهو حركة مرور wired_802.1x و 172.19.1.250.

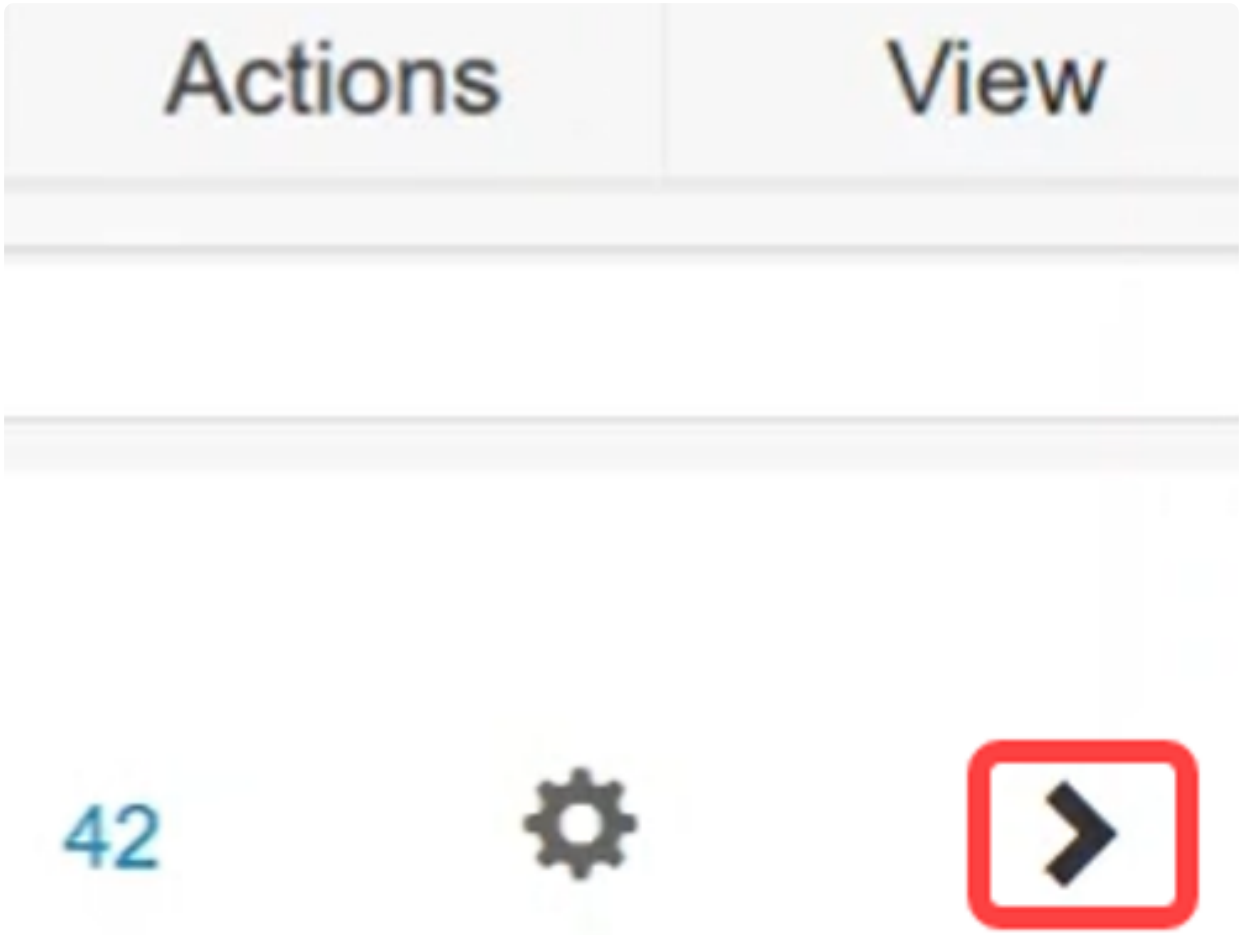


الخطوة 13

قم بتكوين البروتوكولات المسموح بها إلى الوصول الافتراضي إلى الشبكة وانقر فوق حفظ.

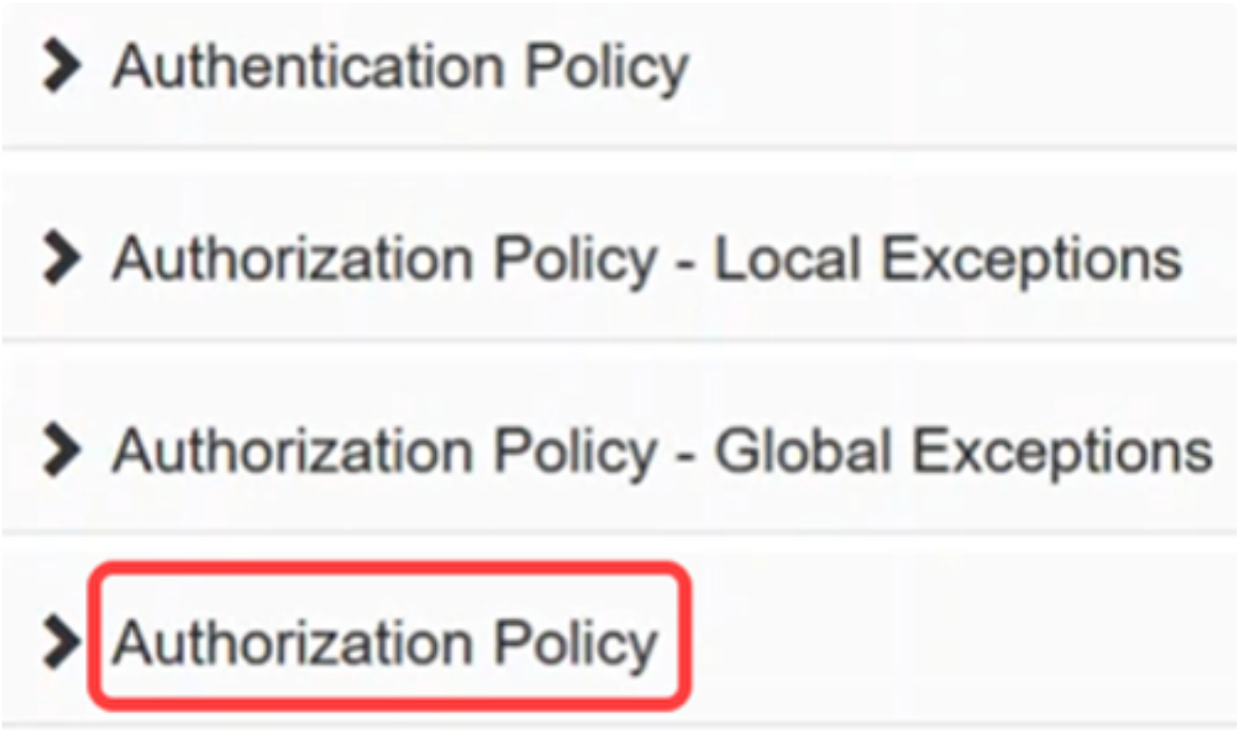
الخطوة 14

تحت عرض، انقر على أيقونة السهم لتكوين سياسات المصادقة والتفويض بناء على متطلبات إعداد الشبكة أو يمكنك إختيار الإعدادات الافتراضية. في هذا المثال، انقر فوق نهج التخويل.



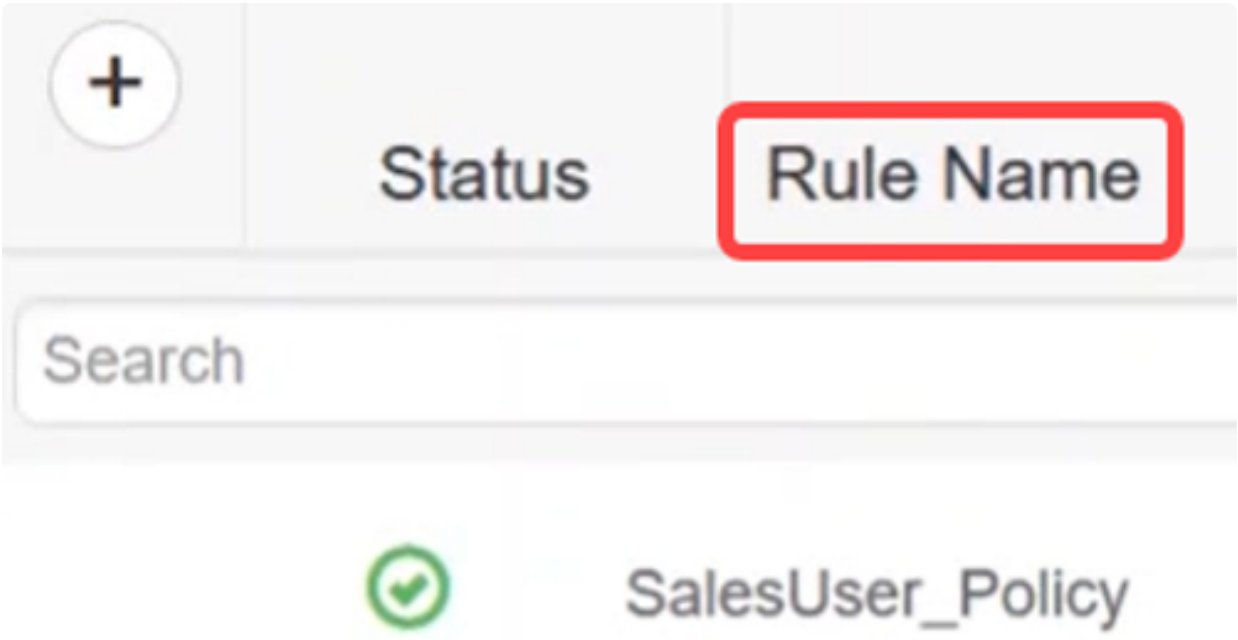
الخطوة 15

انقر على أيقونة الجمع لإضافة نهج.



الخطوة 16

أدخل اسم القاعدة.

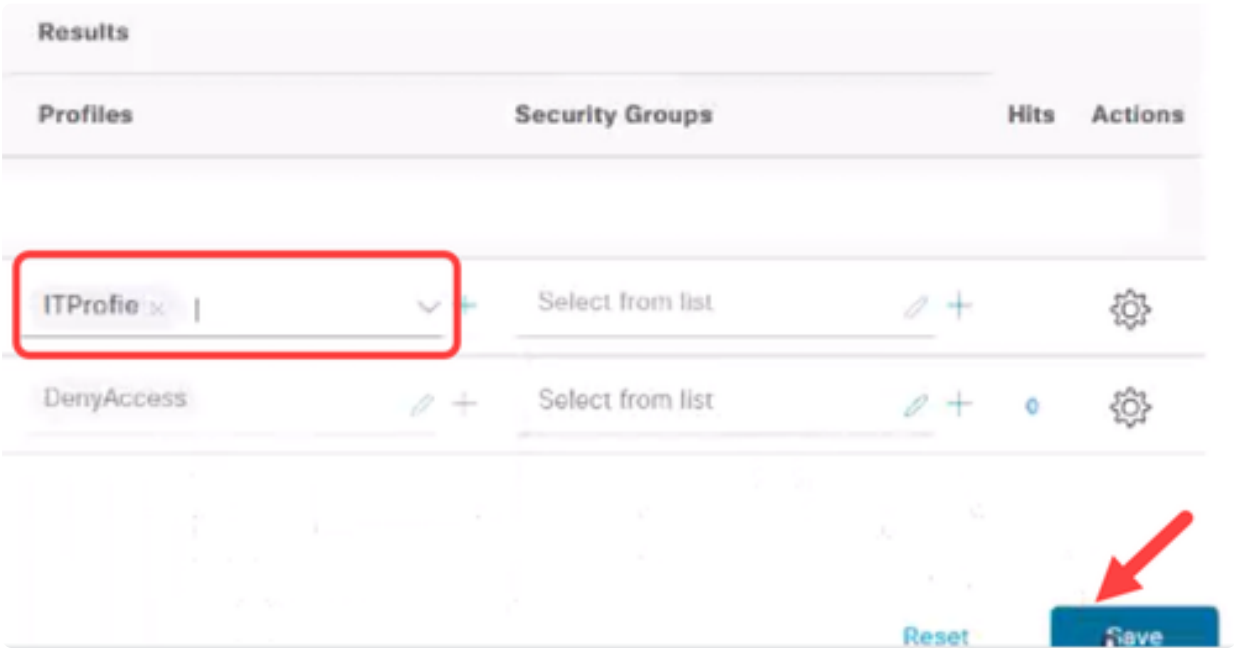


الخطوة 17

تحت الشروط، انقر على أيقونة زائد وحدد مجموعة الهوية. طقطقة إستعمال.

الخطوة 18

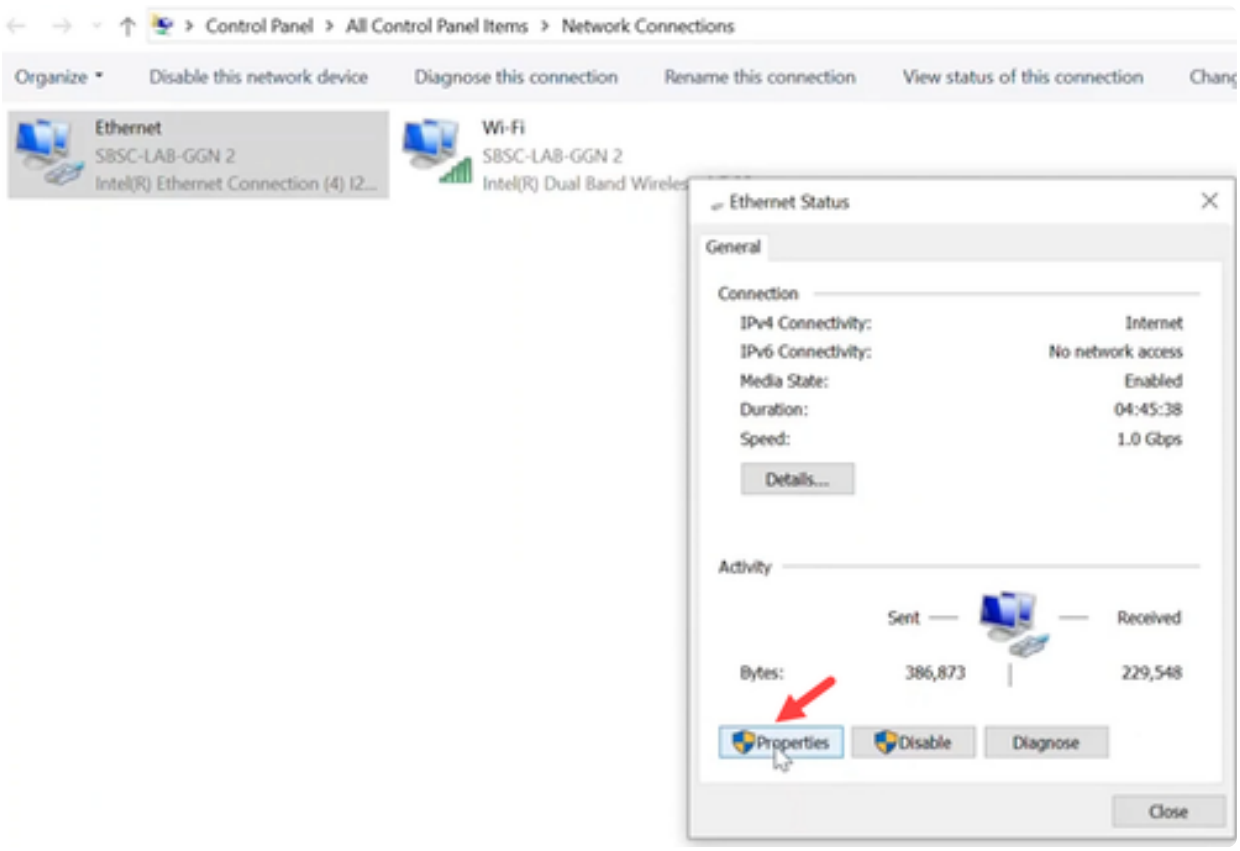
طبق التوصيف المطلوب وانقر على حفظ.



تكوينات العميل

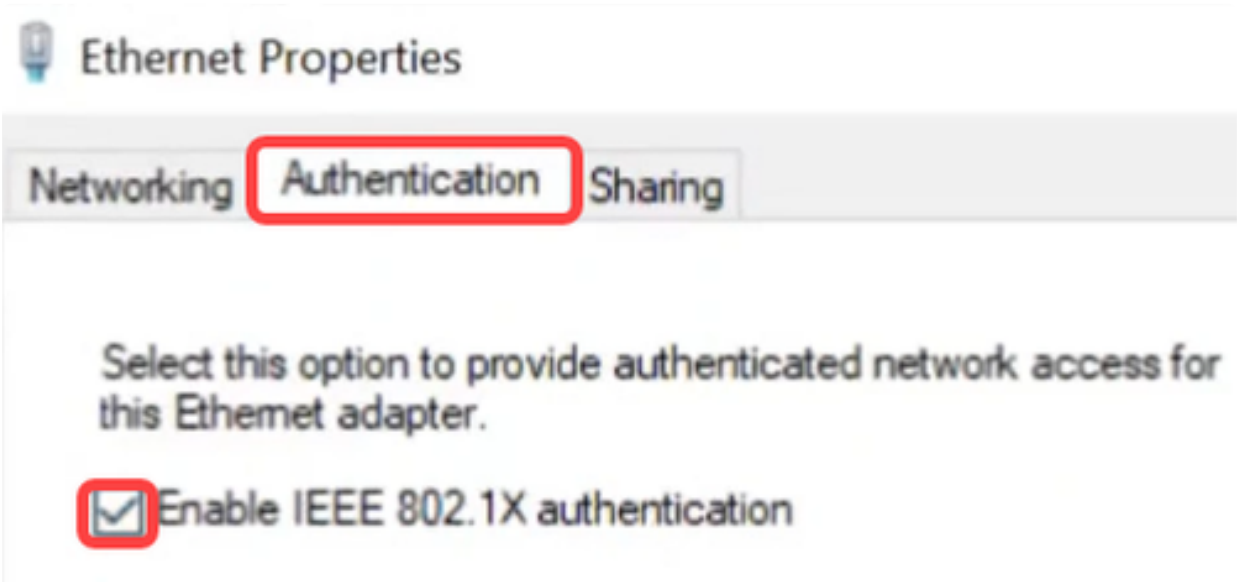
الخطوة 1

في الكمبيوتر المحمول العميل، انتقل إلى إتصالات الشبكة > إيثرنت وانقر فوق خصائص.



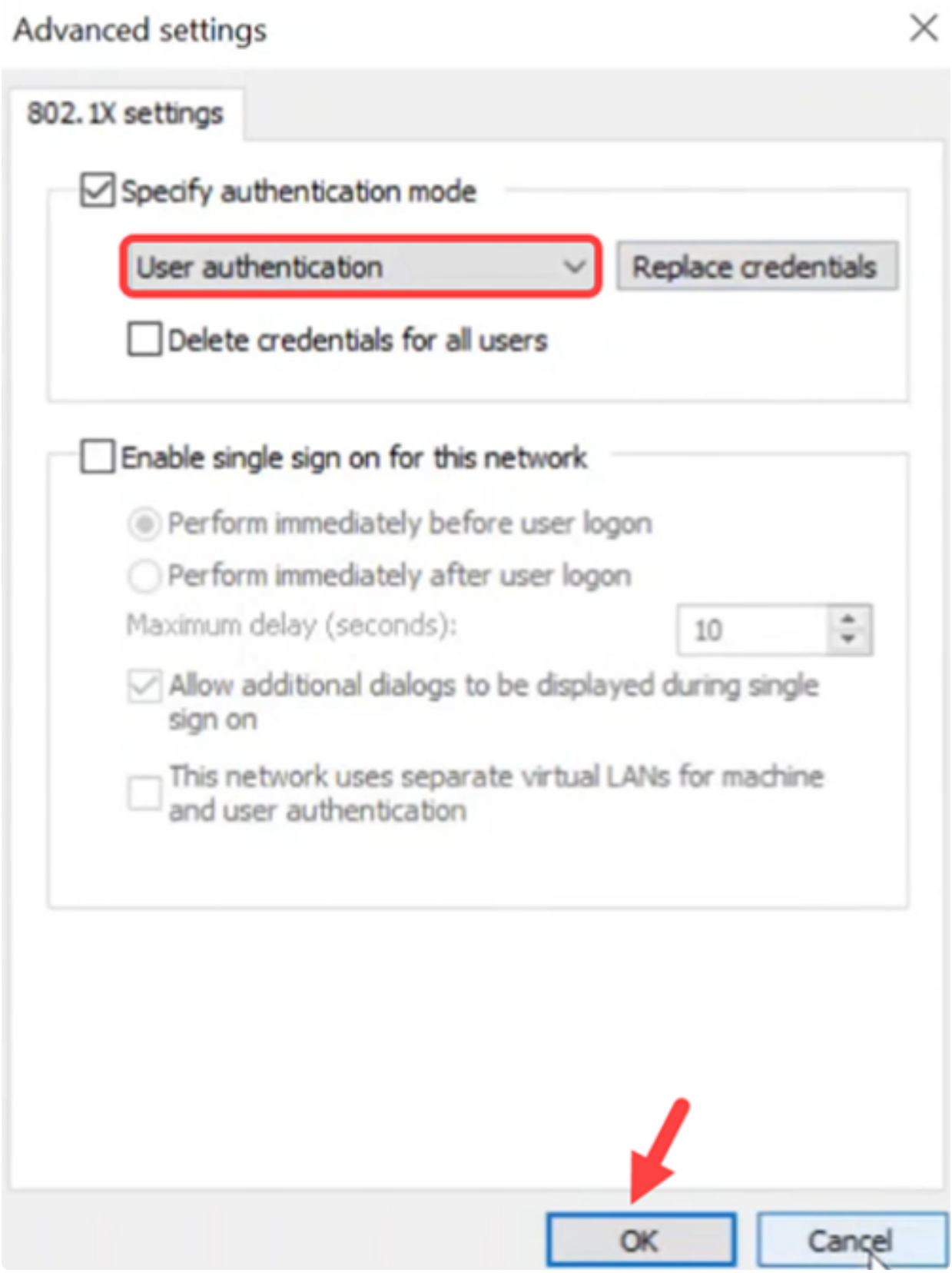
الخطوة 2

انقر على علامة التبويب المصادقة وتأكد من تمكين مصادقة 802.1X.



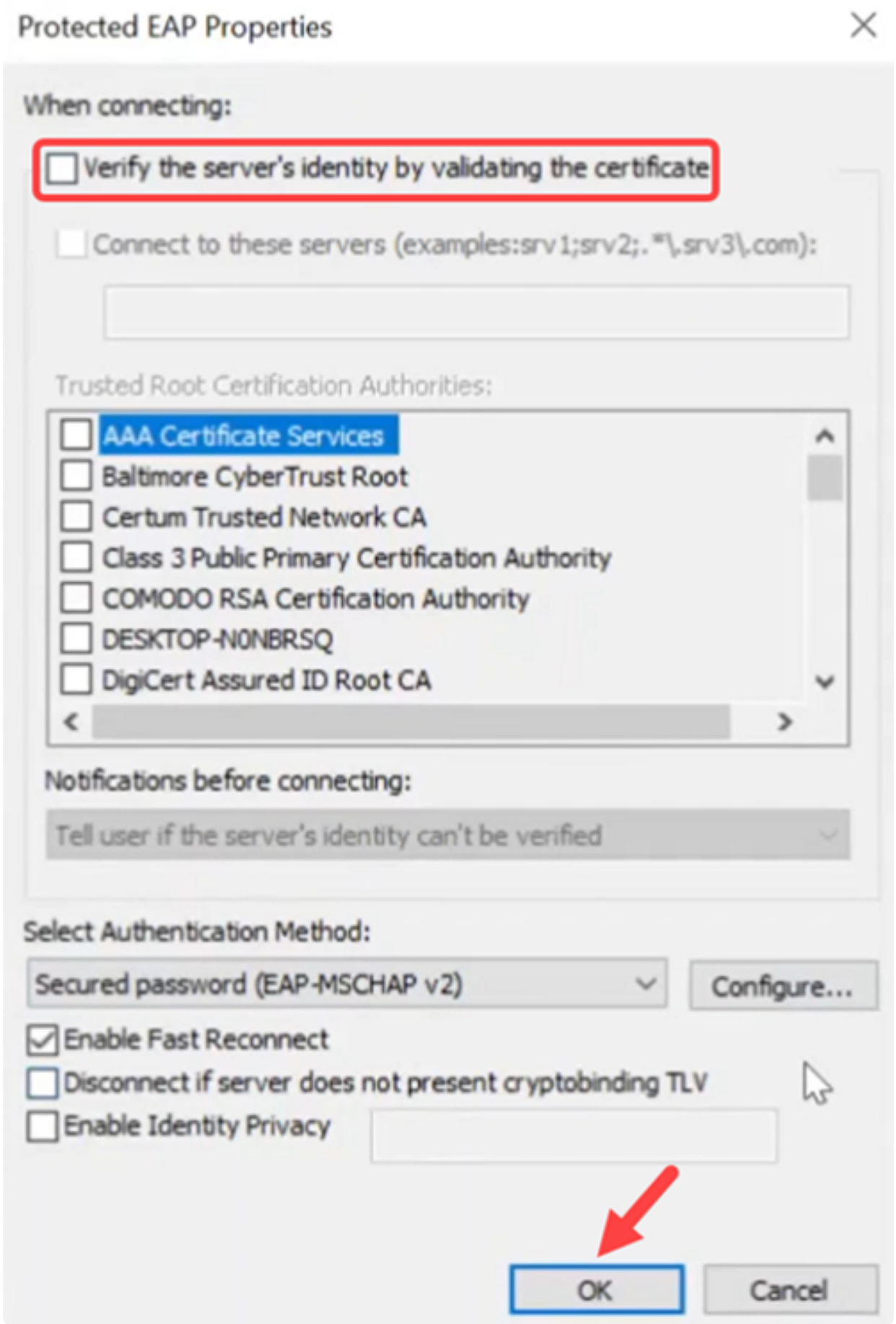
الخطوة 3

تحت إعدادات إضافية، حدد مصادقة المستخدم كوضع مصادقة. انقر فوق حفظ بيانات الاعتماد ثم موافق.



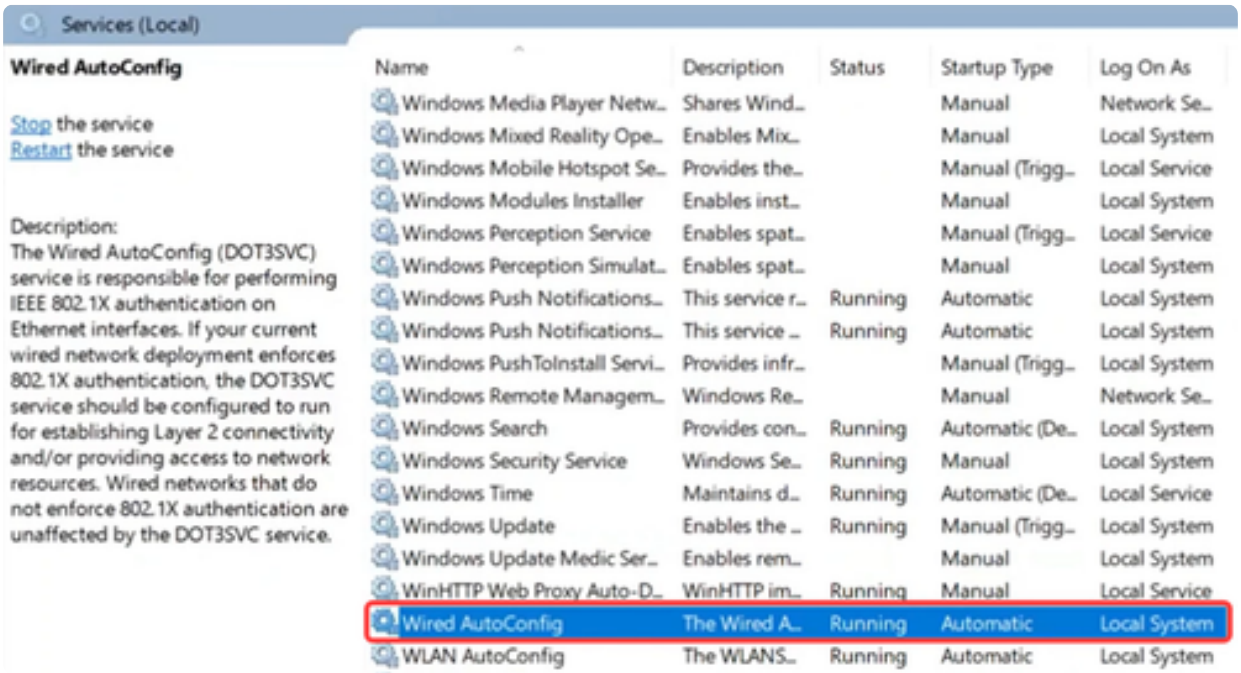
الخطوة 4

انقر على الإعدادات وتأكد من أن المربع المجاور للتحقق من هوية الخادم عن طريق التحقق من صحة الشهادة غير محدد. وانقر فوق OK.


Protected EAP Properties
When connecting:
Verify the server's identity by validating the certificate
Connect to these servers (examples:srv1;srv2;.*\.srv3\.com):
Trusted Root Certification Authorities:
AAA Certificate Services
Baltimore CyberTrust Root
Certum Trusted Network CA
Class 3 Public Primary Certification Authority
COMODO RSA Certification Authority
DESKTOP-N0NBRSQ
DigiCert Assured ID Root CA
Notifications before connecting:
Tell user if the server's identity can't be verified
Select Authentication Method:
Secured password (EAP-MSCHAP v2)
Configure...
Enable Fast Reconnect
Disconnect if server does not present cryptobinding TLV
Enable Identity Privacy
OK
Cancel

الخطوة 5

تحت الخدمات، قم بتمكين إعدادات التكوين التلقائي السلكية.

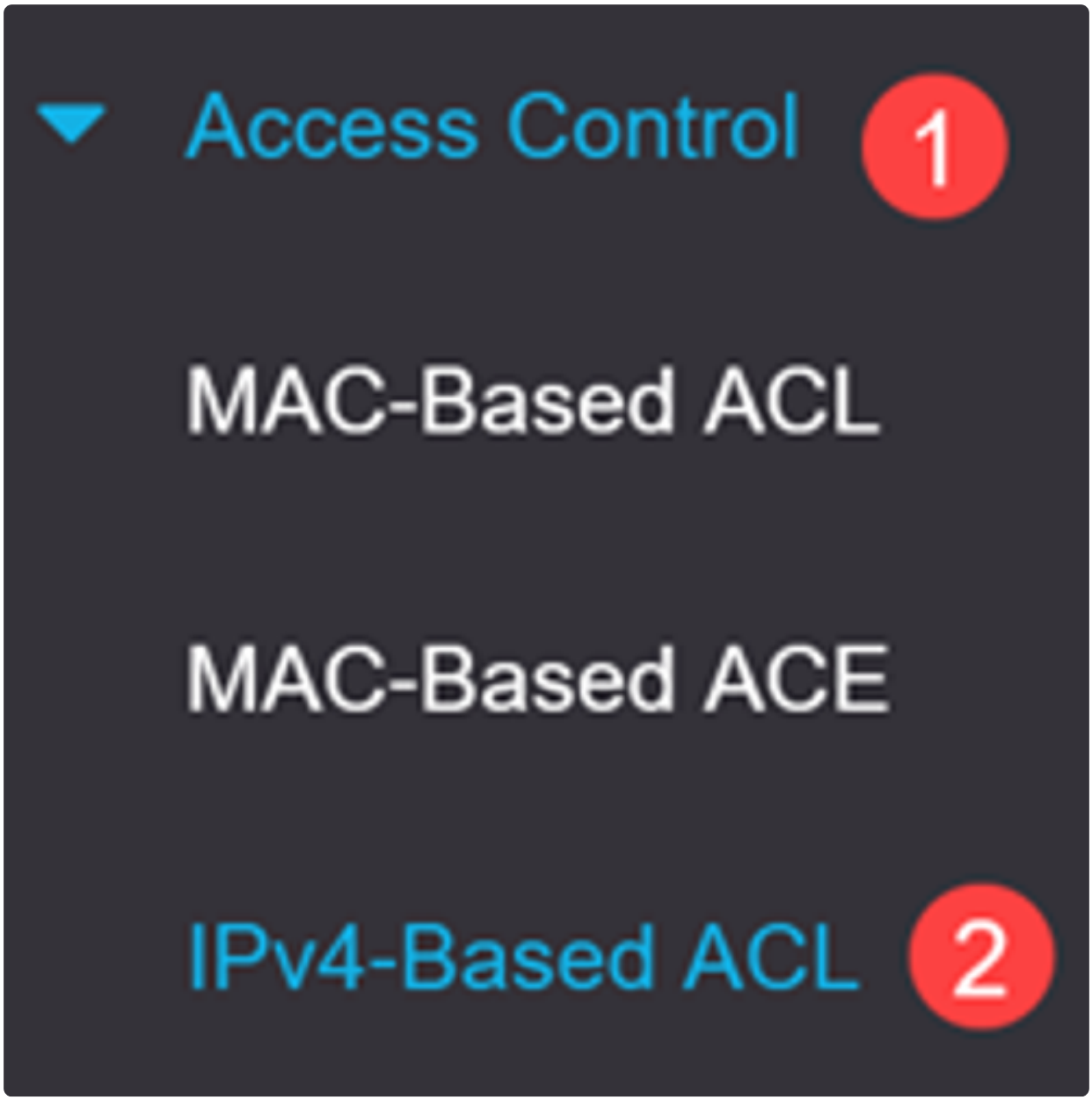


التحقق من DACL

بمجرد مصادقة المستخدم، يمكنك التحقق من قائمة التحكم في الوصول (ACL) القابلة للتنزيل.

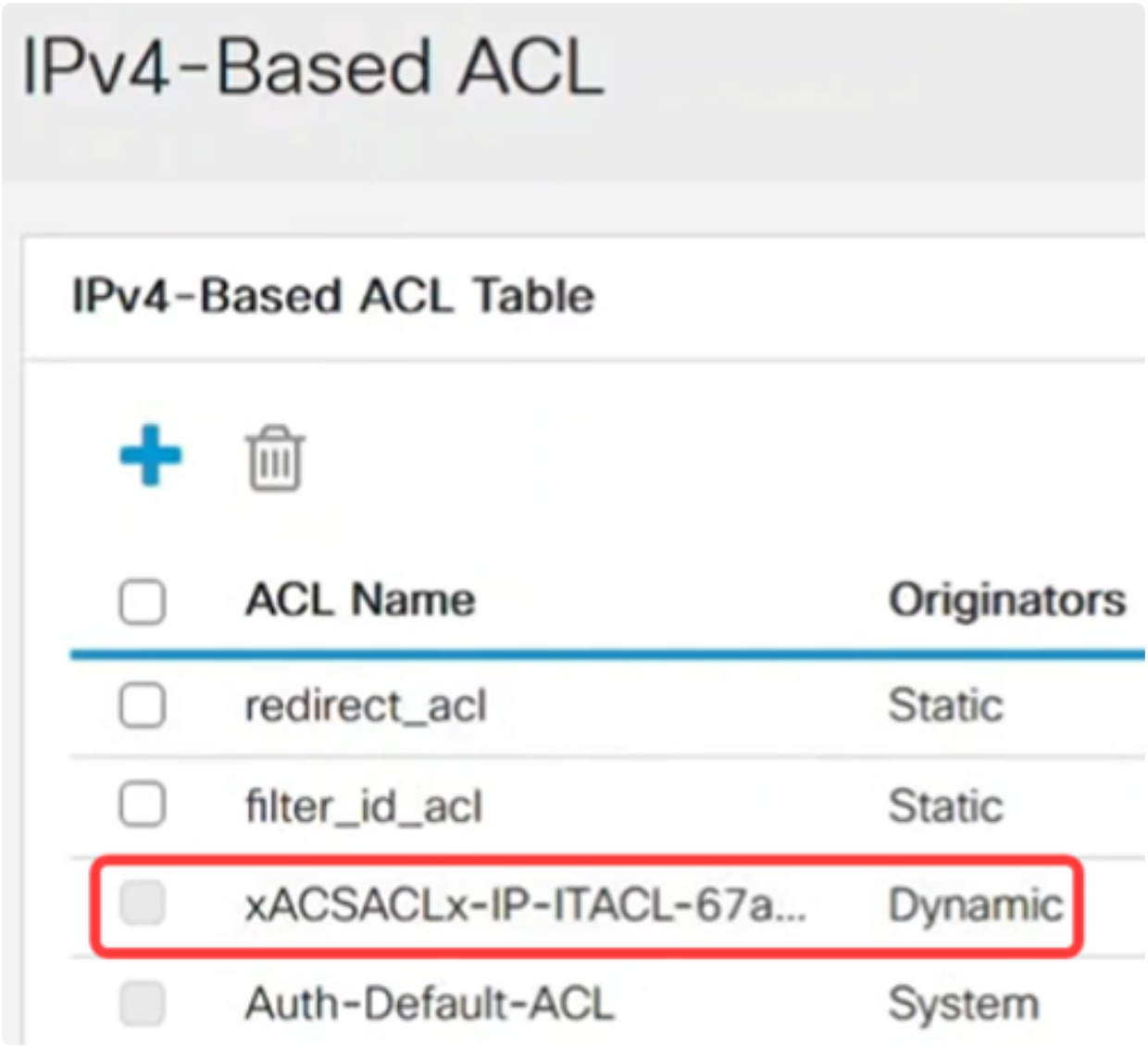
الخطوة 1

قم بتسجيل الدخول إلى المحول Catalyst 1300 switch وانتقل إلى التحكم في الوصول > قائمة التحكم في الوصول (ACL) المستندة إلى IPv4.



الخطوة 2

سيعرض جدول قائمة التحكم في الوصول (ACL) المستندة إلى IPv4 قائمة التحكم في الوصول (ACL) التي تم تنزيلها.

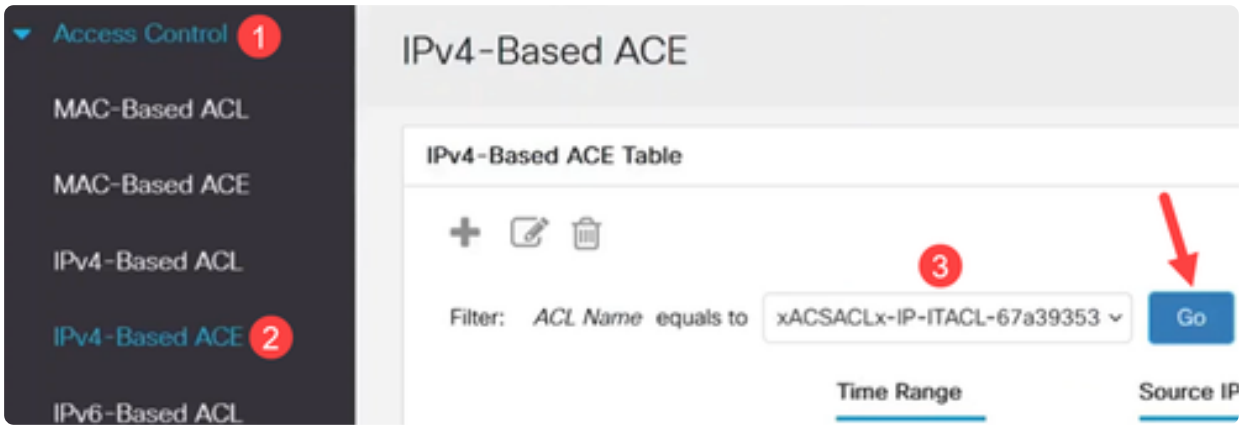


Note:

لا يمكن تحرير قوائم التحكم في الوصول (ACL) القابلة للتنزيل.

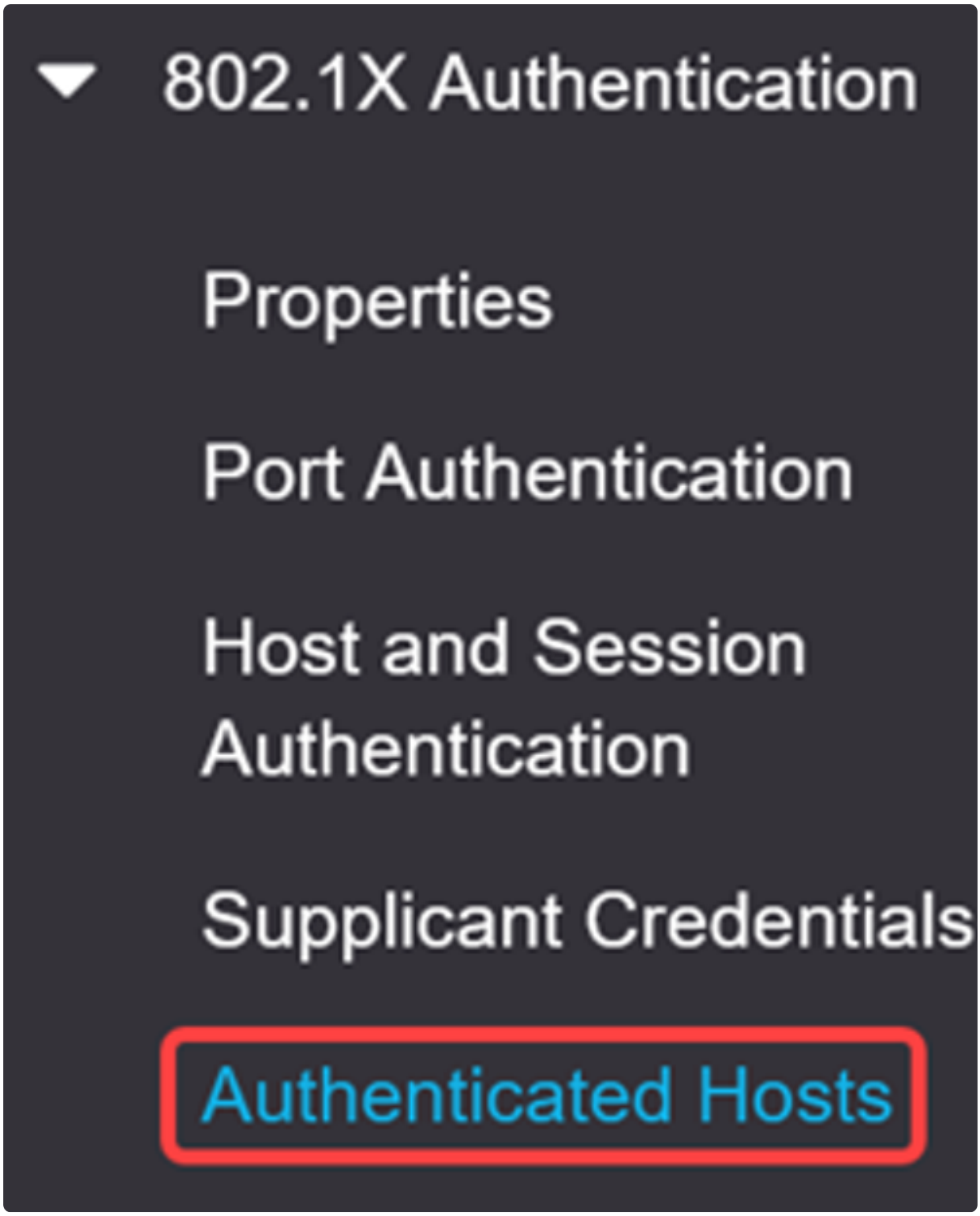
الخطوة 3

ثمة طريقة أخرى للتحقق منها تتمثل في التنقل إلى إدخال التحكم في الوصول (ACE) المستند إلى IPv4، وتحديد قائمة التحكم في الوصول (ACL) القابلة للتنزيل من القائمة المنسدلة اسم قائمة التحكم في الوصول (ACL)، وانقر فوق انتقال. سيتم عرض القواعد التي تم تكوينها في ISE.



الخطوة 4

انتقل إلى الأمان > مصادقة 802.1 >قائمة الأجهزة المضيفة التي تم مصادقتها. يمكنك التحقق من المستخدمين الذين تم مصادقتهم. انقر فوق جلسات العمل المصدق عليها للاطلاع على مزيد من التفاصيل.



الخطوة 5

من واجهة سطر الأوامر (CLI)، قم بتشغيل الأمر show ip access-lists interface الذي يتبعه معرف الواجهة.

في هذا المثال، يمكن رؤية قوائم التحكم في الوصول (ACL) وقوائم التحكم في الوصول (ACE) التي تم تطبيقها على إيثرنت جيجابت 3.

```
switch4a7d55#show ip access-lists interface ge1/0/3
ip access-list extended xACSACLx-IP-SalesACL-6760399d
    deny    ip any host 192.168.251.10 ace-priority 1
    permit  ip any any ace-priority 2
ip access-list extended Auth-Default-ACL
    permit  udp any any any domain ace-priority 20
    permit  tcp any any any domain ace-priority 40
    permit  udp any bootps any any ace-priority 60
    permit  udp any any any bootpc ace-priority 80
    permit  udp any bootpc any any ace-priority 100
    deny    ip any any ace-priority 120
```

الخطوة 6

يمكنك أيضا رؤية الإعدادات المتعلقة باتصال ISE وتنزيلات قائمة التحكم في الوصول باستخدام الأمر

show dot1x جلسة قارن <ID> مفصل. يمكنك عرض الحالة وحالة مصادقة 802.1x وقوائم التحكم في الوصول (ACL) التي تم تنزيلها.

```
switch4a7d55#show dot1x sessions interface ge1/0/3 detailed

          Interface: gi1/0/3
        MAC Address: e4:[redacted]:31
       IPv4 Address: 192.168.251.11
          User-Name: user5
             Status: Authorized
     Oper host mode: multi-host
    Session timeout: N/A
     Session Uptime: 196 sec
  Common Session ID: 14FBA8C00500032222C35D9E
    Acct Session ID: 0x05000322
 Server Policies:
            ACS ACL: xACSACLx-IP-SalesACL-6760399d

 Method status list:
    Method                  State
    802.1x                  Authentication success
```

القرار

اه أنت ذا! الآن تعرف كيفية عمل قائمة التحكم في الوصول (ACL) القابلة للتنزيل على محولات Cisco Catalyst 1300 Switches مع Cisco ISE.

لمزيد من المعلومات، راجع دليل مسؤول Catalyst 1300 وصفحة دعم Cisco Catalyst 1300 Series.

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).