تكوين Posture (وضعية) بدون برنامج

المحتويات

المقدمة

يصف هذه وثيقة كيفية أن يشكل Posture Without Agentless في ISE وهو مطلوب في نقطة نهاية أن يركض برنامج نصي البرنامج نصي.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- محرك خدمات الهوية (ISE).
- وضعية.
- الطرازان PowerShell و SSH
- نظام التشغيل Windows 10 أو إصدار أحدث.

المكونات المستخدمة

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

- إصدار Identity Services Engine (ISE) 3.3.
- حزمة Cisco AgentlessWindows 5.1.6.6
- نظام التشغيل Windows 10

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.

معلومات أساسية

توقوم وضعية محرك خدمات الهوية (ISE) بإجراء تقييم من جانب العميل. يتلقى العميل سياسة متطلبات الوضع من ISE، ويقارن النتائج مع بيانات الوضع، ويرسل نتائج التقييم مرة أخرى إلى ISE، ويرسل السياسة.

تحدد ISE بعد ذلك ما إذا كان الجهاز متوافق بناء على تقرير الوضع أو غير متوافق.

الوضع الخالي من أي برامج أو أدوات وهو أحد طرق الوضع التي تقوم بجمع معلومات الموقف من العملاء وتزيل نفسها تلقائيا عند الاكتمال دون الحاجة إلى أي إجراء من المستخدم النهائي. يتصل Posture (وضعية البرنامج) بالعميل باستخدام امتيازات إدارية.

الشروع في العمل

المتطلبات الأساسية:

- يجب أن يكون العميل قابل للوصول إليه من خلال عنوان IPv4 أو IPv6 الخاص به، كما يجب أن يكون عنوان IP هذا متوفرا في محاسبة RADIUS.
- يجب أن يكون العميل قابل للوصول إليه من محرك خدمات تعريف Cisco (ISE) من خلال

عنوان IPv4 أو IPv6 الخاص به. وبالإضافة إلى ذلك، يجب أن يكون عنوان IP هذا متوفرا في محاسبة RADIUS.

- عملاء Windows و Mac مدعومون حاليا:
    - لعملاء Windows، يجب أن يكون المنفذ 5985 للوصول إلى PowerShell على العميل مفتوحا. يجب أن يكون PowerShell v7.1 أو أحدث. يجب أن يحتوي العميل على cURL v7.34 أو إصدار أحدث.
    - لعملاء MacOS، يجب أن يكون المنفذ 22 للوصول إلى SSH مفتوحا للوصول إلى العميل. يجب أن يحتوي العميل على cURL v7.34 أو إصدار أحدث.
- يجب أن يكون لبيانات اعتماد العميل الخاصة بتسجيل الدخول إلى shell امتيازات مسؤول محلي.
- قم بتشغيل تحديث موجز ويب للوضع للحصول على أحدث العملاء، كما هو موضح في خطوات التكوين. يرجى التحقق من:
- بالنسبة لنظام التشغيل MacOS، تأكد من أن هذا الإدخال تم تحديثه في ملف Sudoers لتجنب فشل تثبيت الشهادة على نقاط النهاية:

<macadminusername> ALL = (ALL) NOPASSWD: /usr/bin/security, /usr/bin/osascript

•

بالنسبة لنظام التشغيل MacOS، يجب أن يكون حساب المستخدم الذي تم تكوينه حساب مسؤول. لا يعمل الوضع ≡ على أي نوع حساب آخر، حتى إذا قمت بإعطاء المزيد من الامتيازات.لعرض هذه الإطار، انقر على زر (Menuicon) واختر الإدارة > النظام > الإعدادات > البرامج النصية لنقطة النهاية > تسجيل الدخول التكوين > مستخدم Mac المحلي.

•

في حالة حدوث تغييرات في الأنشطة ذات الصلة بالمنفذ في عملاء Windows بسبب التحديثات من Microsoft، يجب إعادة تكوين سير عمل تكوين Windows دون حالة إستخدام لعملاء Windows.

شروط الوضع المدعومة

•

شروط الملف، ما عدا الشروط التي تستخدم مسارات ملف USER_PROFILE و USER_DESKTOP

•

شروط الخدمة، ما عدا عمليات التحقق من برنامج دايمن النظام أو برنامج دايمن أو وكيل المستخدم على نظام التشغيل MacOS

- شورط التطبيق
- شورط مصدر البيانات الخارجية
- ظروف مركبة
- حالات الحماية من البرامج الضارة
- شرط إدارة التصحيح، باستثناء عمليات التحقق من DateEnabenabled وUp
- شورط جدار الحماية
- شورط تشفير القرص، باستثناء التحقق من الحالة المستند إلى موقع التشفير
- شورط التسجيل، باستثناء الشورط التي تستخدم HCSK كمفتاح جذري

شورط الوضع غير المدعوم

- عالج
-

فترة سماح

- إعادة تقييم دورية

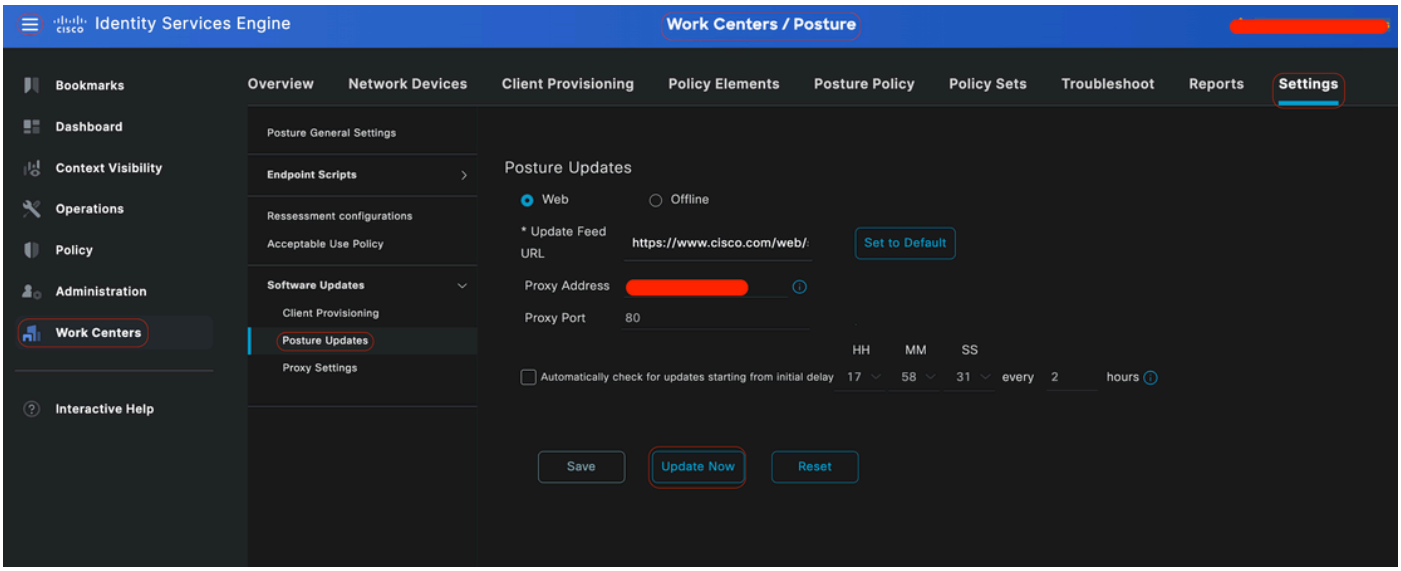
- سياسة إستخدام مقبولة

ISE التكوين

تحديث موجز ويب الوضع

من المستحسن تحديث موجز ويب للوضع قبل بدء تكوين الوضع.

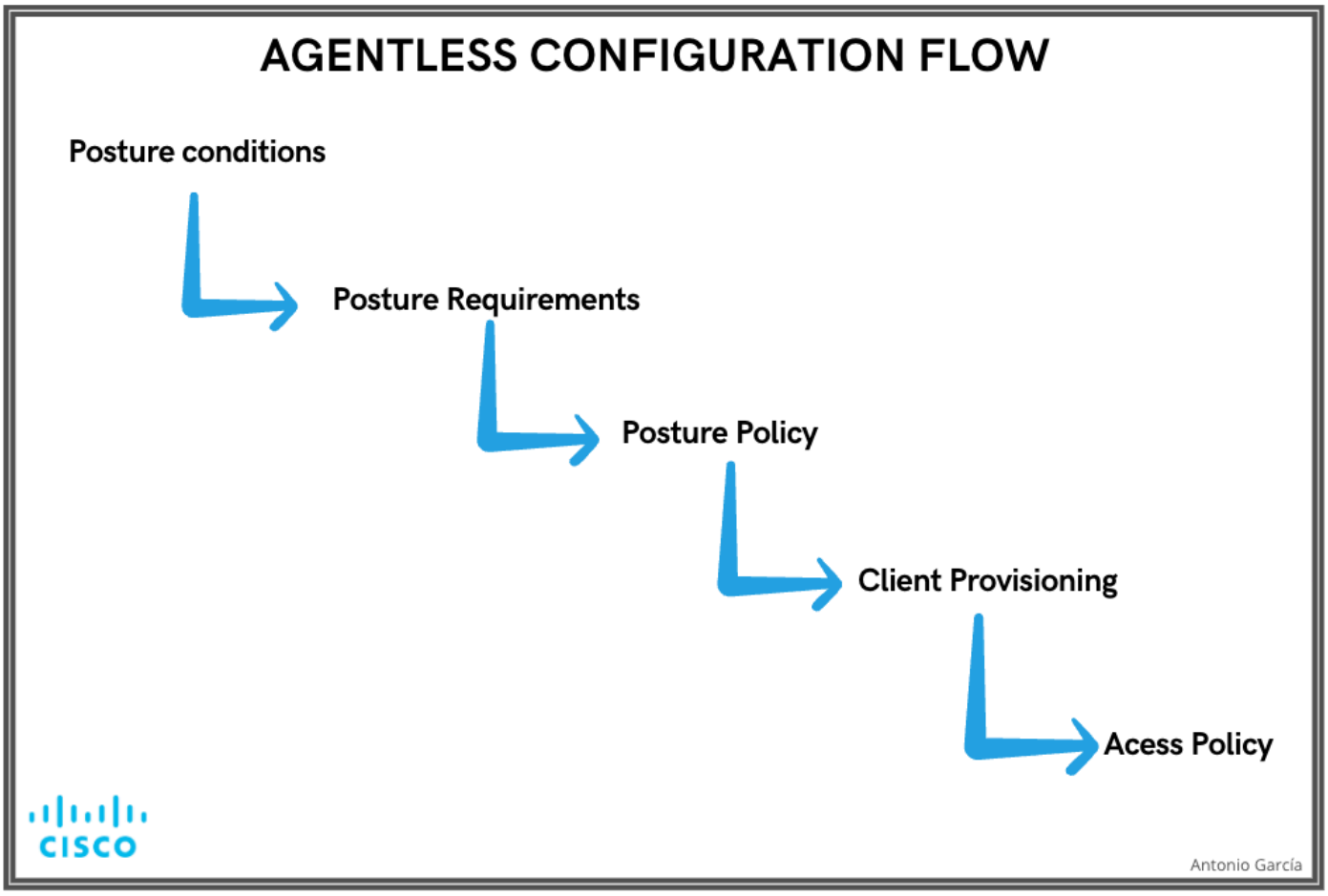
في واجهة المستخدم الرسومية Cisco ISE، انقر فوق Menuicon () واختر مراكز العمل > **Posture (وضعية) >** إعدادات > تحديثات البرامج> التحديث الآن.



تحديث موجز ويب الوضع

تدفق التكوين Posture Without Agentless

يجب تكوين Posture Agentless من أجل أن يكون التكوين الأول مطلوبا للتكوين التالي وهكذا. لاحظ أن الإصلاح ليس في التدفق؛ ومع ذلك، لاحقا، سيقوم هذا المستند بتغطية بديل لتكوين الإصلاح.



تدفق التكوين دون الحاجة إلى استخدام أية برامج

تكوين الوضع بدون برنامج

حالة الوضع

شروط الوضع هي مجموعة من القواعد في سياسة الأمان الخاصة بنا التي تحدد نقطة نهاية متوافقة. تتضمن بعض هذه العناصر تثبيت جدار حماية وبرامج مكافحة الفيروسات وبرامج مكافحة البرامج الضارة والإصلاحات العاجلة وتشفير الأقراص وغير ذلك الكثير.

في واجهة المستخدم الرسومية Cisco ISE، انقر فوق Menuicon () واختر مركز العمل > **Posture** > عناصر السياسة > الشروط، انقر فوق إضافة ، وقم بإنشاء واحدة أو أكثر من **تهيئة الوضع الذي يستخدم وضعية بلا برنامج لتحديد المتطلب.** بمجرد إنشاء الشرط، انقر **حفظ**.

في هذا السيناريو، تم تكوين شرط تطبيق باسم **"Agentless_Condition_Application"** باستخدام هذه المعلمات:

- **نظام التشغيل:** Windows All

ينطبق هذا الشرط على أي إصدار من نظام تشغيل Windows، مما يضمن التوافق الواسع عبر بيئات Windows المختلفة.

- **التحقق حسب:** العملية

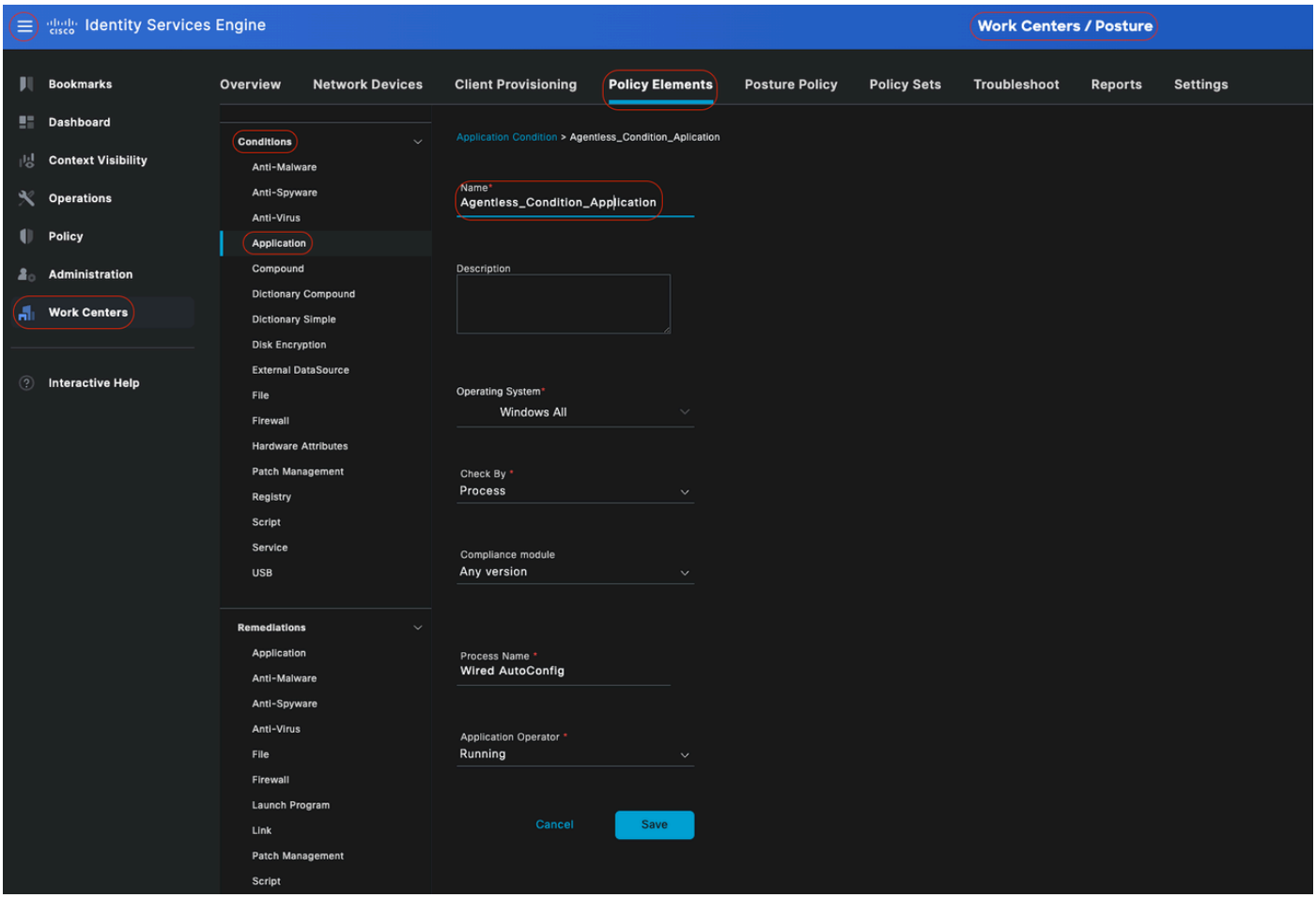
يراقب النظام العمليات داخل الجهاز. لديك الخيار لتحديد **العملية** أو **التطبيق**، وفي هذه الحالة، تم إختيار **العملية**.

- **اسم العملية:** التكوين التلقائي السلكي

عملية **التكوين التلقائي** السلكية هي أن الوحدة النمطية المتوافقة مع العملية سوف تقوم بإيداع الجهاز. هذه العملية مسؤولة عن تكوين إتصالات الشبكة السلكية وإدارتها، بما في ذلك مصادقة IEEE 802.1X.

- **عامل تشغيل التطبيق:** التشغيل

تتحقق الوحدة النمطية للتوافق مما إذا كانت عملية **التكوين التلقائي** السلكية قيد التشغيل حاليا على الجهاز. لديك الخيار لتحديد إما قيد **التشغيل** أو عدم **التشغيل**. في هذه الحالة، تم تحديد **التشغيل** لضمان أن العملية نشطة.



شرط دون الحاجة إلى استخدام أية أدوات

متطلب الوضع

متطلب الوضع هو مجموعة من الشروط المركبة أو شرط واحد فقط يمكن ربطه بدور ونظام تشغيل. يجب أن يفي جميع العملاء المتصلين بالشبكة بالمتطلبات الإلزامية أثناء تقييم الوضع لكي يصبحوا متوافقين مع الشبكة.

في واجهة المستخدم الرسومية Cisco ISE، انقر فوق Menuicon () واختر مراكز العمل > **Posture**>عناصر السياسة > متطلب. انقر فوق السهم لأسفل وحدد إدراج جديد متطلب، ثم قم بإنشاء **PostureRequirements** واحد أو أكثر يستخدم الوضع دون برنامج. بمجرد إنشاء المتطلب، انقر فوق تم ثم حفظ.

في هذه الحالة، تم تكوين أحد متطلبات التطبيق المسمى "**Agentless_Require_Application**" باستخدام هذه المعايير:

- **نظام التشغيل:** Windows All

ينطبق هذا المتطلب على أي إصدار من نظام تشغيل Windows، مما يضمن أنه قابل للتطبيق في جميع بيئات Windows.

- **نوع الوضع:** دون الحاجة إلى استخدام أية أدوات

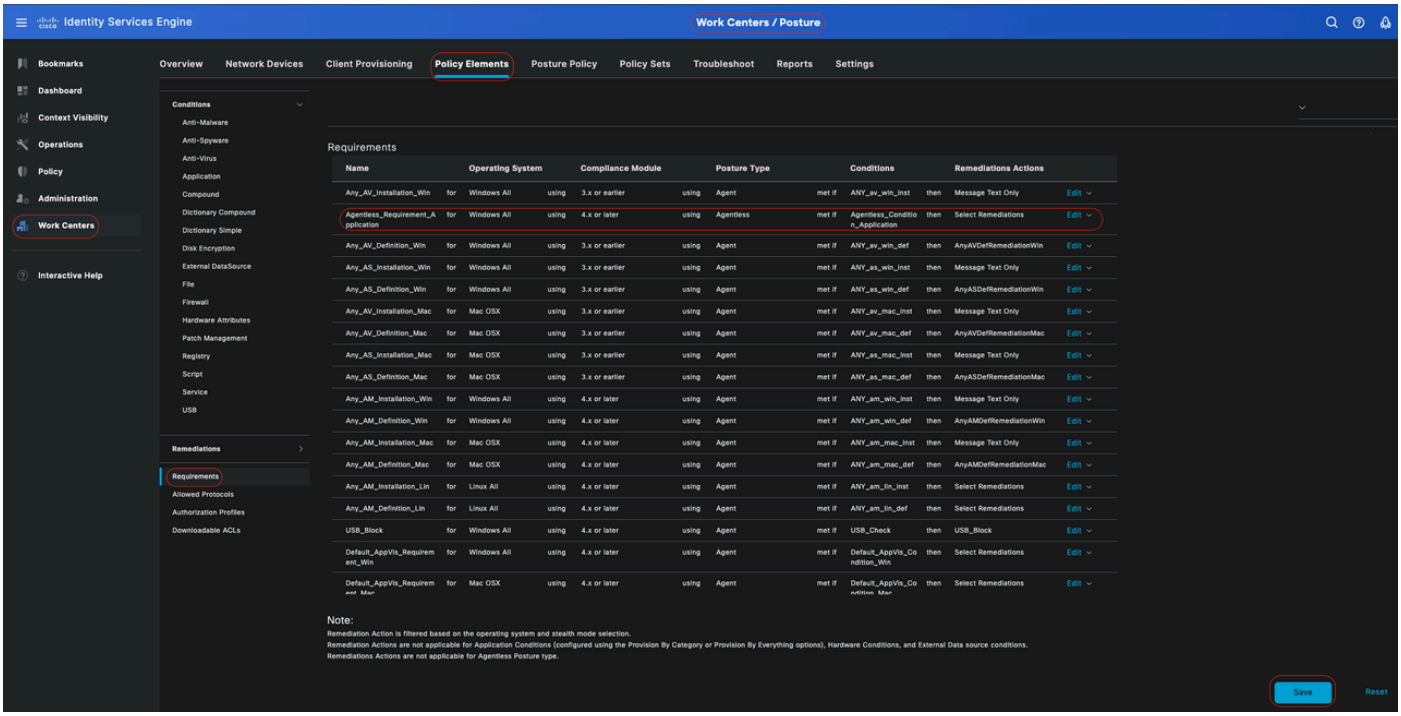
تم تعيين هذا التكوين لبيئة دون الحاجة إلى استخدام أية برامج. تتضمن الخيارات المتاحة الوكيل والوكيل **Stealth** والعامل المؤقت وعديم الحلقة. في هذا السيناريو، تم تحديد **بدون** استخدام أية برامج.

- **الشروط: Agentless_Condition_Application**

وهذا يحدد الشرط الذي تقوم به وحدة ISE Posture النمطية ووحدة التوافق بالتحقق من خلال عمليات الجهاز. الشرط المحدد هو **Agentless_Condition_Application**.

- **إجراءات الإصلاح:**

ونظرا لأن هذا التكوين خاص ببيئة لا تحتوي على أية برامج، فإن إجراءات الإصلاح غير مدعومة، ويتم مسح هذا الحقل.



متطلب بدون أدوات

نهج الوضع

في واجهة المستخدم الرسومية Cisco ISE، انقر فوق Menuicon (

) أو اختر مراكز العمل > **Posture** > Posture نهج. انقر فوق السهم لأسفل لوحدد إدراج متطلب جديد، ثم قم بإنشاء قاعدة **Posture** نهج واحد أو أكثر مدعومة التي تستخدم الوضع بدون برنامج لمتطلب الوضع هذا. بمجرد إنشاء نهج الوضع، انقر فوق تم ثم حفظ.

في هذا السيناريو، تم تكوين نهج الوضع المسمى "**Agentless_Policy_Application**" باستخدام هذه المعلمات:

- **اسم القاعدة:** Agentless_Policy_Application

هذا هو الاسم المعين لنهج الوضع في مثال التكوين هذا.

- **نظام التشغيل:** Windows All

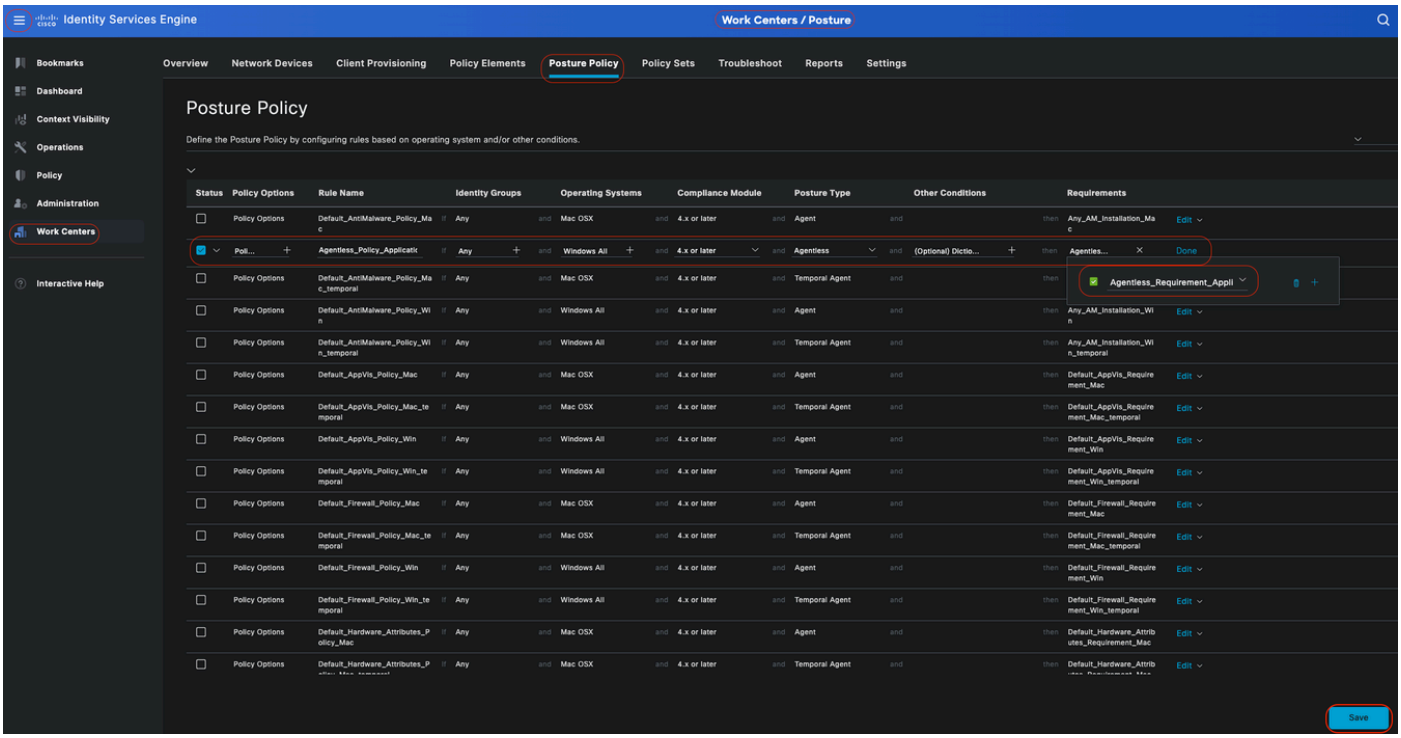
تم تعيين النهج للتطبيق على كافة إصدارات نظام التشغيل Windows، مما يضمن التوافق الواسع عبر بيئات Windows المختلفة.

- **نوع الوضع:** دون الحاجة إلى إستخدام أية أدوات

تم تعيين هذا التكوين لبيئة دون الحاجة إلى إستخدام أية برامج. تتضمن الخيارات المتاحة الوكيل والوكيل **Stealth** والعامل المؤقت وعدم التحقق. في هذا السيناريو، تم تحديد **بدون** إستخدام أية برامج عميل.

- **شروط أخرى:**

في مثال التكوين هذا، لم يتم إنشاء شروط إضافية. ومع ذلك، لديك خيار تكوين شروط محددة لضمان أن الأجهزة المستهدفة فقط هي التي تخضع لنهج الوضع هذا، بدلا من جميع أجهزة Windows على الشبكة. يمكن أن يكون هذا مفيدا بشكل خاص لتجزئة الشبكة.



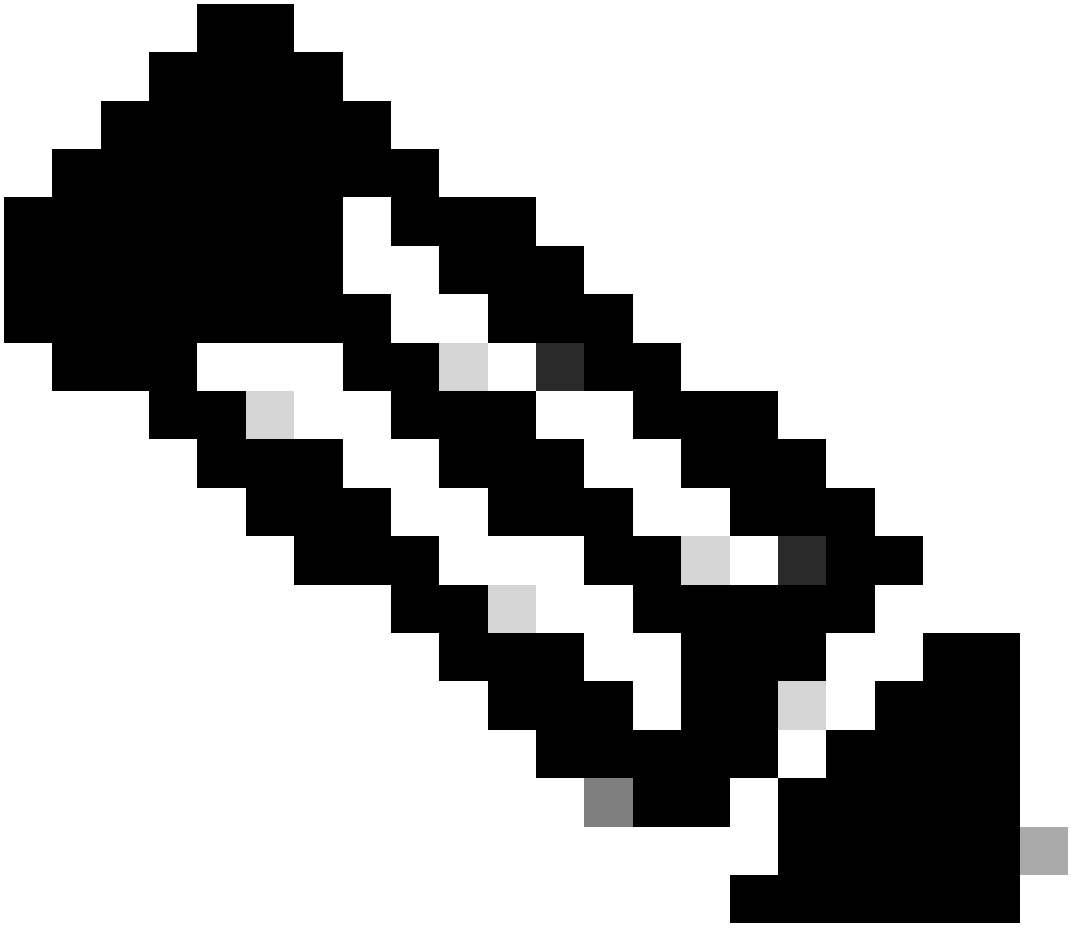
نهج *Posture WithoutEvent*

إمداد العميل

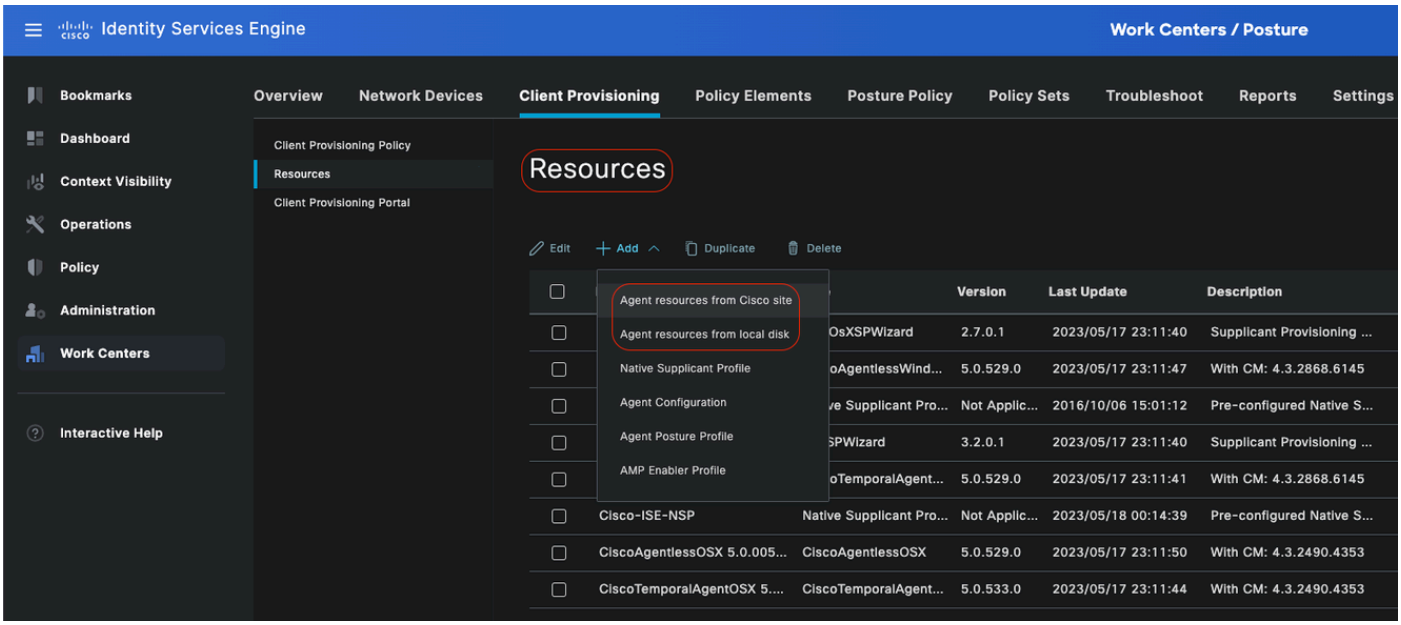
الخطوة 1- تنزيل المواد

لبدء تكوين "إمداد العميل"، يجب أولا تنزيل المواد المطلوبة وتوفيرها في ISE حتى يمكنك إستخدامها لاحقا في "نهج إمداد العميل".

هناك طريقتان لإضافة مواد إلى ISE، **ومواد الوكيل من موقع Cisco ومواد الوكيل من القرص المحلي**. بما أنك تقوم بتكوين دون الحاجة، فأنت مطالب بالمرور عبر مواد البرنامج من موقع **Cisco** للتنزيل.



ملاحظة: لاستخدام موارد الوكيل هذه من موقع **Cisco**، يجب أن يكون ISE PAN قادرًا على الوصول إلى الإنترنت.



الدواوين

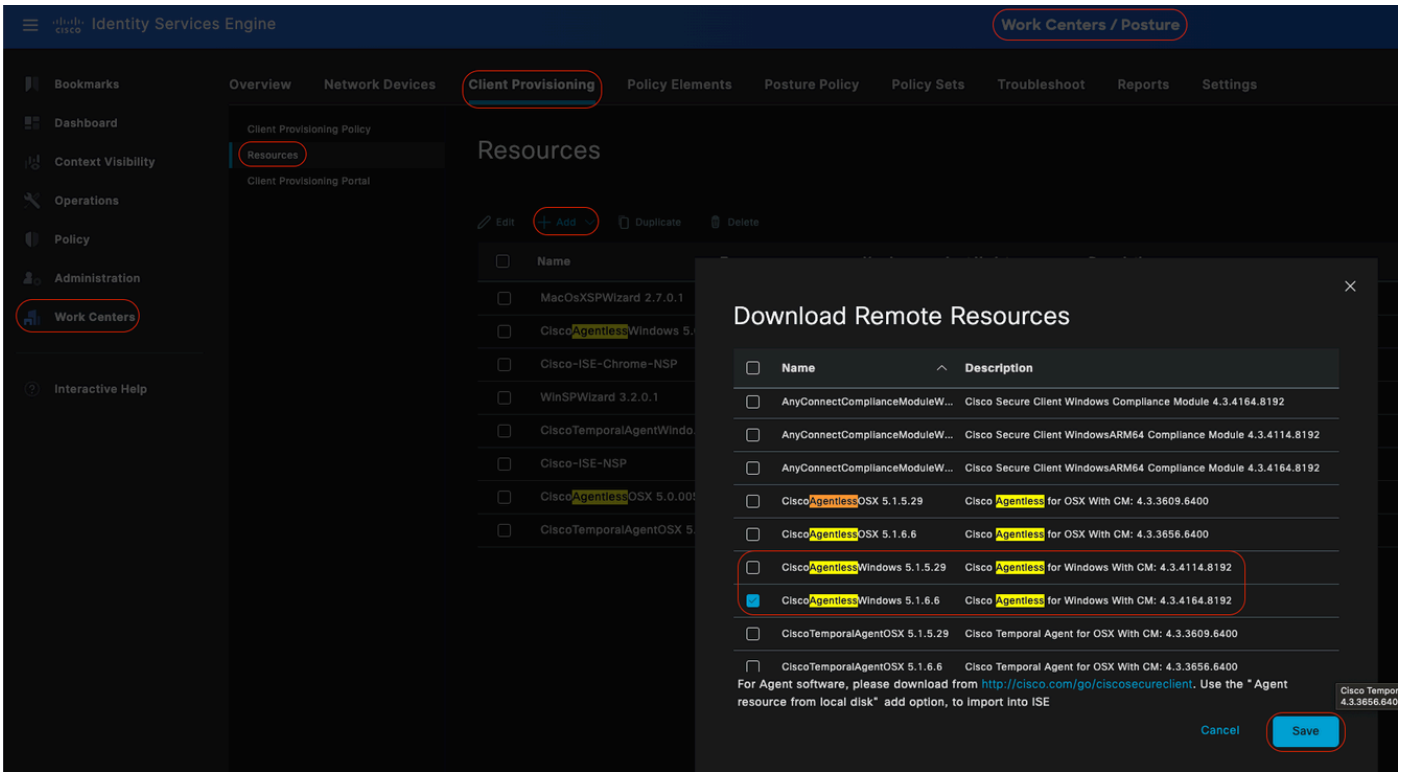
موارد الوكيل من موقع Cisco

في واجهة المستخدم الرسومية Cisco ISE، انقر فوق Menuicon () واختر مركز العمل > **Posture**>إمدادات العميل>الدواوين. انقر فوق إضافة ، حدد موارد الوكيل من موقع **Cisco**، انقر فوق حفظ.

من موقع Cisco، يمكنك فقط تحميل وحدة التوافق النمطية. يعرض النظام وحدتي التوافق الأخيرتين اللتين يجب تنزيلهما. يتم تحديد حزمة الدواوين **CiscoAgentlessWindows 5.1.6.6** لمثال التكوين هذا، وهذا مخصص لأجهزة Windows فقط.

.

دواوين



الوكيل من موقع *Cisco*

الخطوة 2- تكوين سياسة إمداد العميل

عند تكوين "عامل الوضع"، يلزمك موفرانِ مختلفانِ (**AnyConnect** أو **Secure Client** ووحدة التوافق)،

قم بتعيين كل الموارد ضمن تكوين العميل مع ملف تعريف وضعية العميل حتى يمكنك إستخدام تكوين العميل هذا في نهج توفير العميل لديك.

ومع ذلك، عند تكوين Posture Without Agentless، الحاجة لتكوين تكوين الوكيل أو ملف تعريف وضعية العميل، وبدلا من ذلك، تقوم فقط بتنزيل الحزمة غير المنفذة من موارد العميل من موقع **Cisco**.

في واجهة المستخدم الرسومية Cisco ISE، انقر فوق Menuicon () واختر مركز العمل > **Posture**>إمداد العميل > سياسة إمداد العميل. انقر فوق سهم القائمة وحدد إدراج نهج جديد أعلاه أو إدراج نهج جديد أدناه أو تكرار أعلاه أو تكرار أدناه:

- اسم القاعدة: **Agentless_Client_Provisioning_Policy**

يحدد هذا السمة نوع توفير العميل.

- **نظام التشغيل:** Windows All

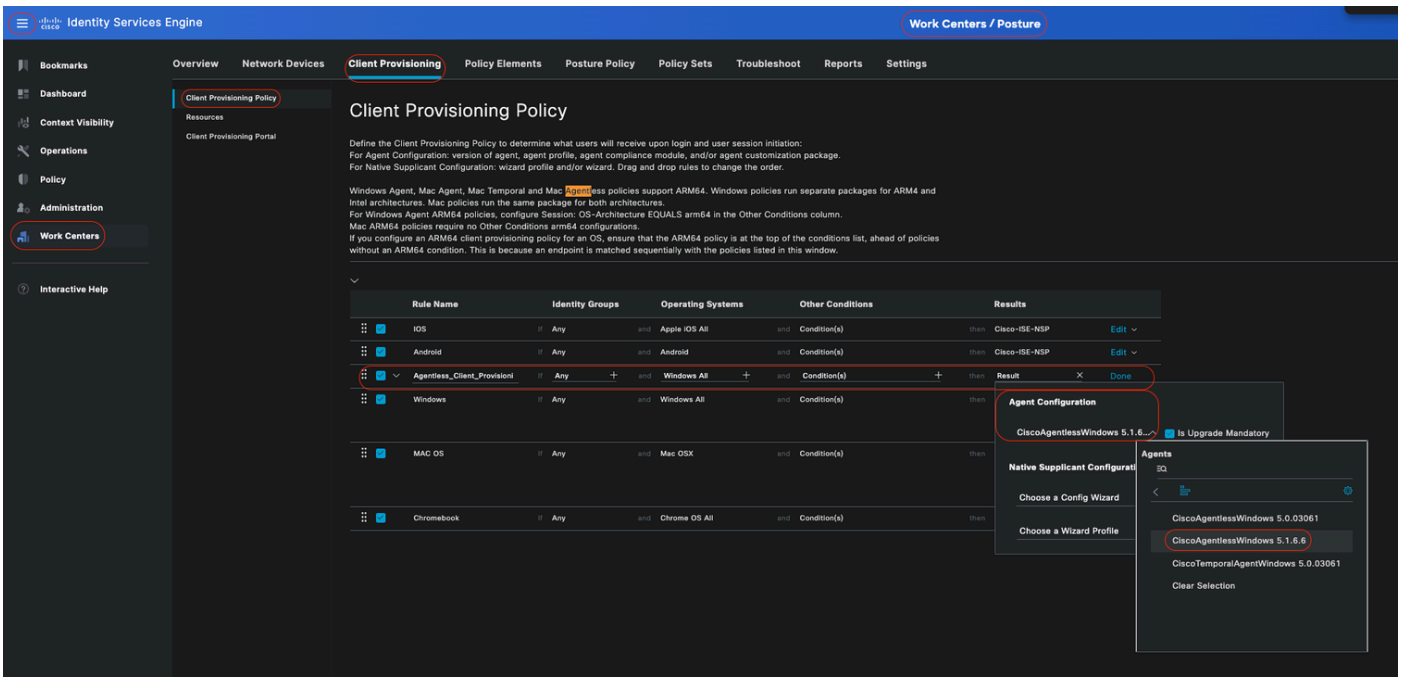
وهذا يضمن تطبيق السياسة على جميع إصدارات نظام التشغيل Windows.

- **شروط أخرى:** لم يتم تكوين شروط محددة في هذا المثال. ومع ذلك، يمكنك تكوين الشروط لضمان أن الأجهزة المطلوبة فقط تطابق سياسة إمداد العميل هذه، بدلا من جميع أجهزة Windows في الشبكة. وهذا مفيد بشكل خاص لتجزئة الشبكة.

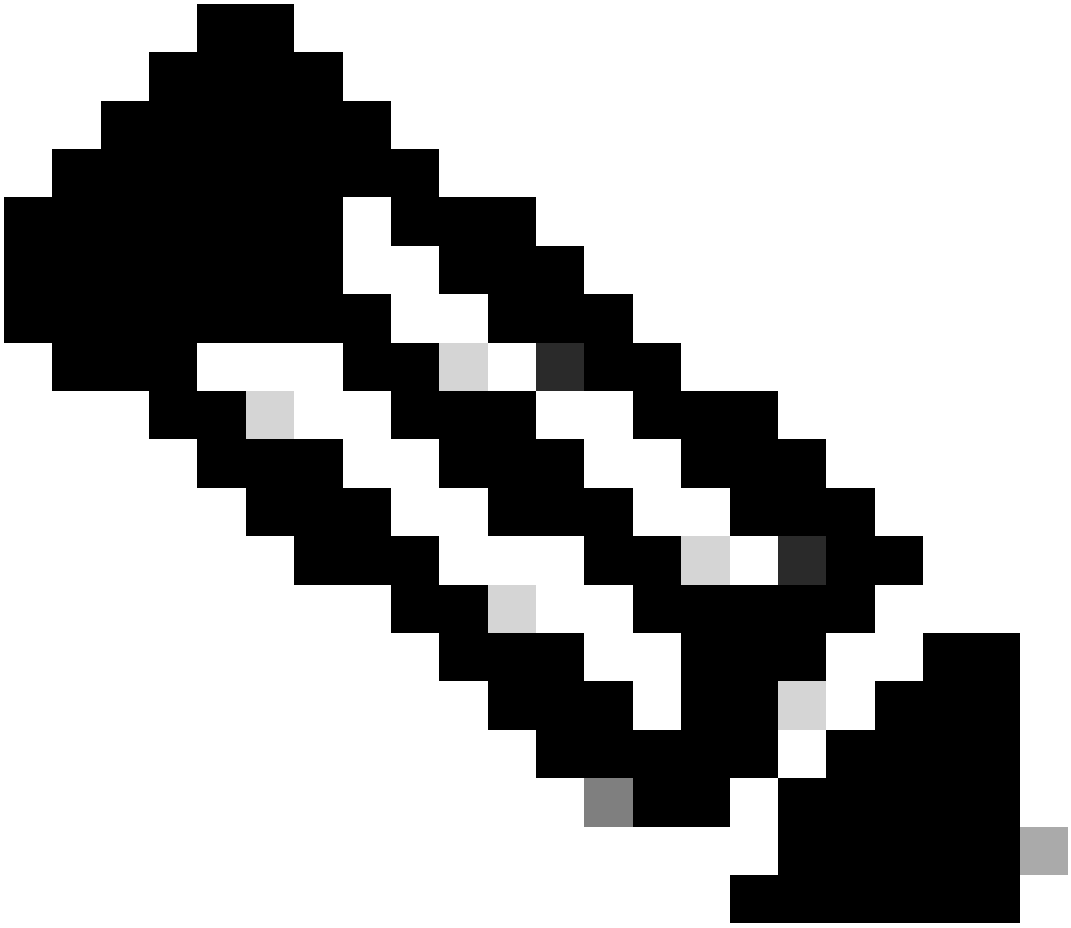
مثال: إذا كنت تستخدم Active Directory، يمكنك تضمين مجموعات Active Directory في النوع الخاص بك لتحسين الأجهزة التي تتأثر.

- **النتائج:** حدد عميل التكوين أو الحزمة المناسبة. بما أنك تقوم بالتكوين لبيئة لا تستخدم أي برامج، أختر الحزمة **CiscoAgentlessWindows 5.1.6.6**، والتي قمت بتنزيلها من قبل من موارد البرنامج العميل من موقع **Cisco**. تحتوي هذه الحزمة على الحزمة التي لا تحتاج إلى إستخدام أي برامج على جميع الموارد الضرورية (البرامج التي لا تحتاج إلى إستخدام أي برامج المطلوبة للتشغيل دون الحاجة إلى إستخدام برنامج Posture ووحدة التوافق).

•انقر فوق حفظ



نموذج توفير عميل بدون برامج عميل



ملاحظة: تأكد من أن سياسة إمداد عميل واحدة فقط تفي بالشروط اللازمة لأي محاولة مصادقة معينة. إذا تم تقييم سياسات متعددة في نفس الوقت، فقد يؤدي ذلك إلى سلوكيات غير متوقعة وتعارضات محتملة.

ملف تعريف التخويل بدون برامج وكيلة

في واجهة المستخدم الرسومية Cisco ISE، انقر فوق

المكون () واختر Policy > عناصر السياسة > النتائج > **Authorization** > **Authorization Profile** وقم بإنشاء ملف تعريف التفويض الذي يقيم النتائج من **Agentless Posture.**

- في مثال التكوين هذا، تم تسمية ملف تعريف التخويل باسم **Agentless_Authorization_Profile**.

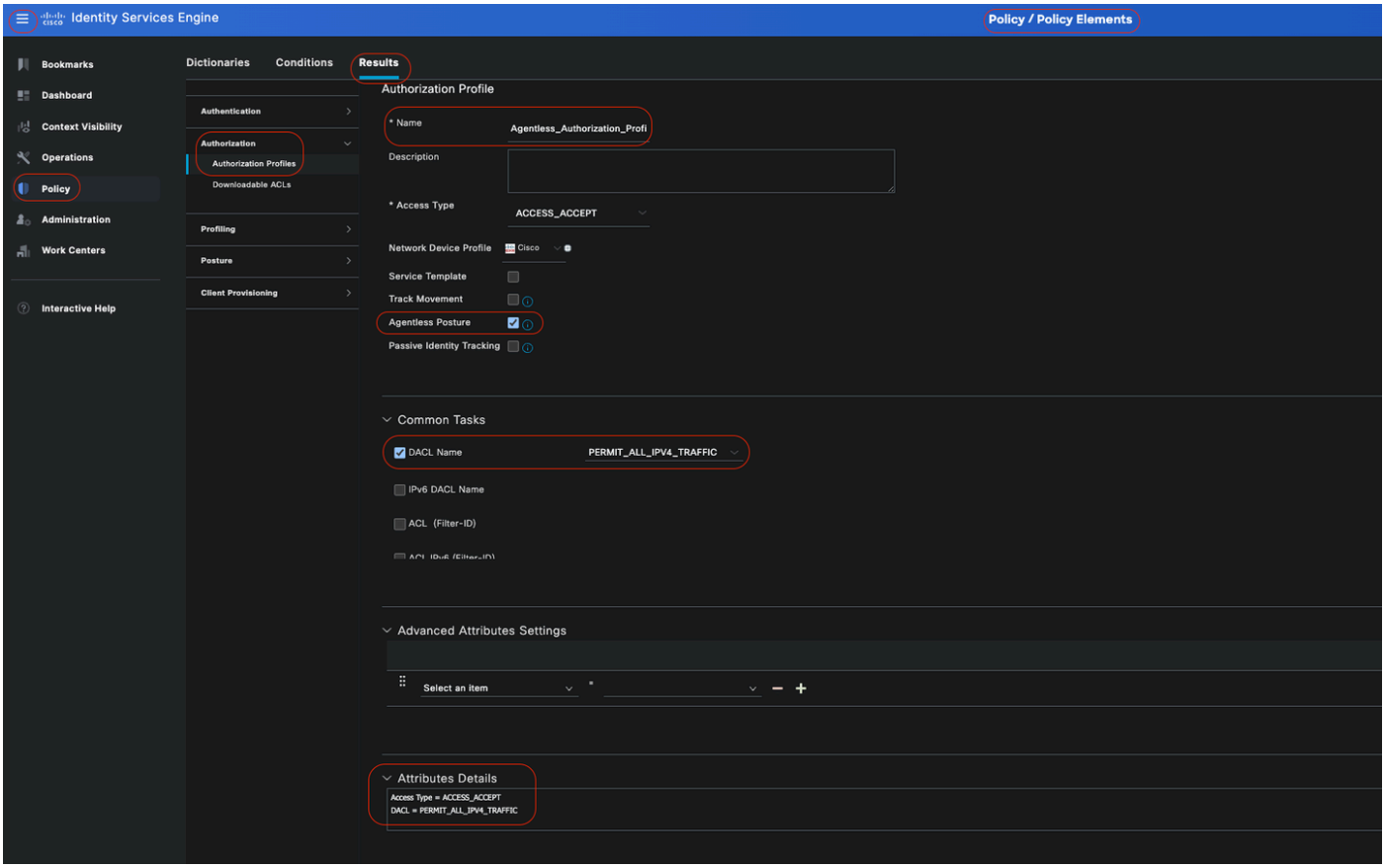
- تمكين الوضع دون الحاجة إلى استخدام أية برامج في ملف تعريف التخويل.

- أستخدم ملف التعريف هذا فقط من أجل **الوضع دون الحاجة إلى استخدام** برنامج. ال تستخدم هذا أيضا لأنواع الوضع الأخرى.

- ال يلزم توفر قائمة التحكم في الوصول (ACL) الخاصة ب CWA وقائمة التحكم في الوصول (ACL) المعاد توجيهها للوضع دون أية برامج. أنت يستطيع استعملت VLANs، DACLs، أو ACLs كجزء من ك قسم قاعدة. إلبقاء الأمر بسيطا، يتم تكوين قائمة تحكم في الوصول إلى البنية الأساسية (مما يسمح لجميع حركة مرور IPv4) فقط بجانب التحقق من الوضع دون الحاجة في مثال التكوين هذا.

-

انقر فوق **حفظ**.



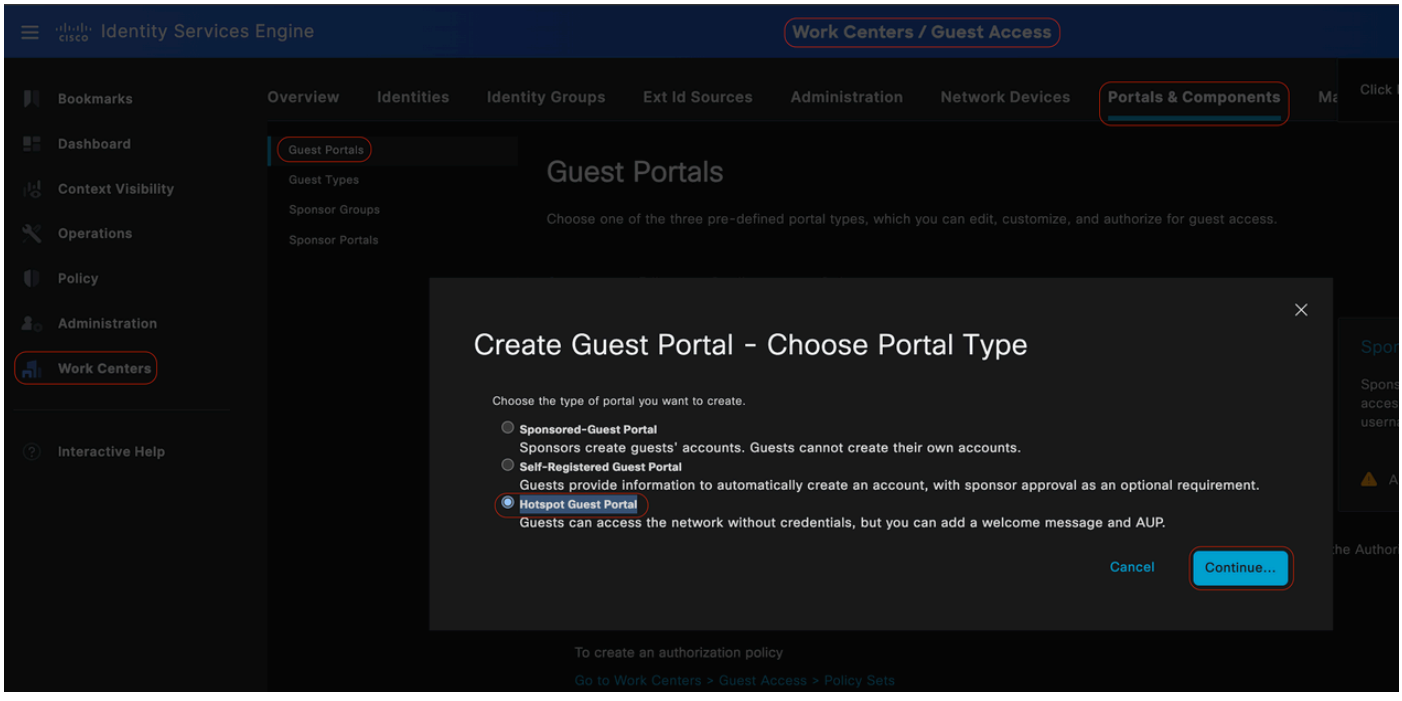
ملف تعريف التخويل بدون أدوات

حل بديل لاستخدام الإصلاح (إختياري)

لا يتوفر دعم الإصلاح في التدفق الخالي من العناوين. ولمعالجة هذا الأمر، يمكنك تنفيذ مدخل نقطة اتصال مباشر مخصص لتحسين وعي المستخدم فيما يتعلق بالتوافق مع نقطة النهاية. عندما يتم تعريف نقطة نهاية على أنها غير متوافقة، يمكن إعادة توجيه المستخدمين إلى هذه البوابة. ويكفل هذا النهج إبلاغ المستخدمين بحالة الامتثال لنقاط النهاية الخاصة بهم، ويمكنهم إتخاذ الإجراءات المناسبة لتصحيح أي مسائل.

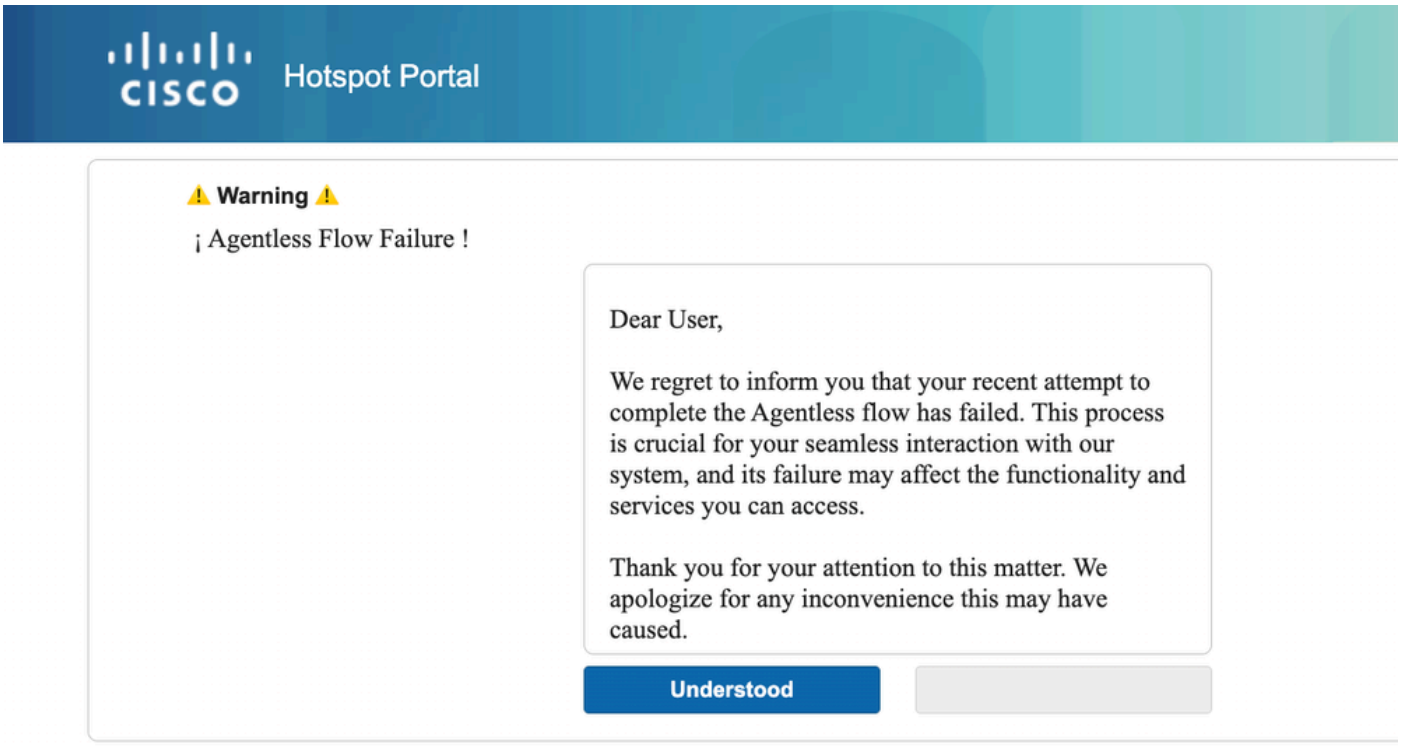
في واجهة المستخدم الرسومية Cisco ISE، انقر فوق

المينايكون () واختر مراكز العمل>وصول الضيف>المنافذ والمكونات>بوابات الضيف. انقر فوق إنشاء > تحديد مدخل ضيف النقطة الفعالة >متابعة: . في مثال التكوين هذا، يتم تسمية مدخل النقطة الساخنة باسم **Agentless_Warning**.



بوابة ضيف النقاط الساخنة

في إعدادات المدخل، لديك القدرة على تخصيص الرسائل المعروضة للمستخدمين النهائيين للتوافق مع متطلباتك الخاصة، هذا مجرد مثال على عرض المدخل المخصص:



فشل في الوضع دون الحاجة إلى إستخدام

ملف تعريف تفويض الإصلاح (إختياري)

في واجهة المستخدم الرسومية (GUI) Cisco ISE، انقر فوق Menuicon > عناصر السياسة > النتائج > التفويض > ملفات تعريف التخويل وقم بإنشاء ملف تعريف التخويل للإصلاح الخاص بك.

- في مثال التكوين هذا، تم تسمية ملف تعريف التخويل باسم **remediation_authorization_profile**.

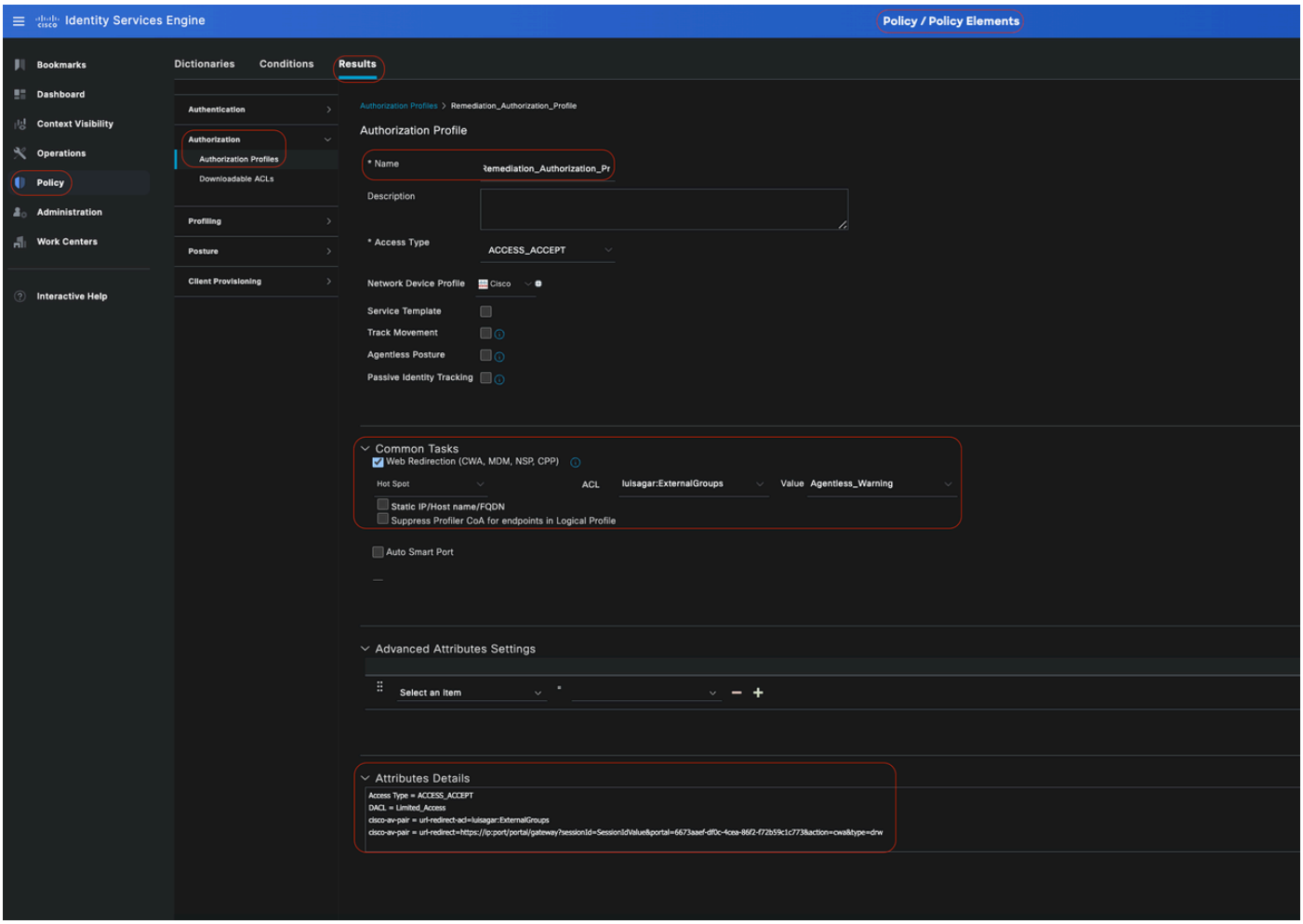
- من أجل البساطة، يتضمن مثال التكوين التالي فقط قائمة تحكم في الوصول (dACL) يمكن تنزيلها وتسمى **Limited_Access** (وصول محدود) تتيح وصولا محدودا، تم تخصيصها لتلبية الاحتياجات الخاصة لمؤسستك.

•

تم تكوين ميزة إعادة توجيه الويب بما في ذلك مجموعة خارجية والنقطة الساخنة، مما يزيد من وعي المستخدم فيما يتعلق بالتوافق مع نقطة النهاية.

•

انقر فوق **حفظ**.

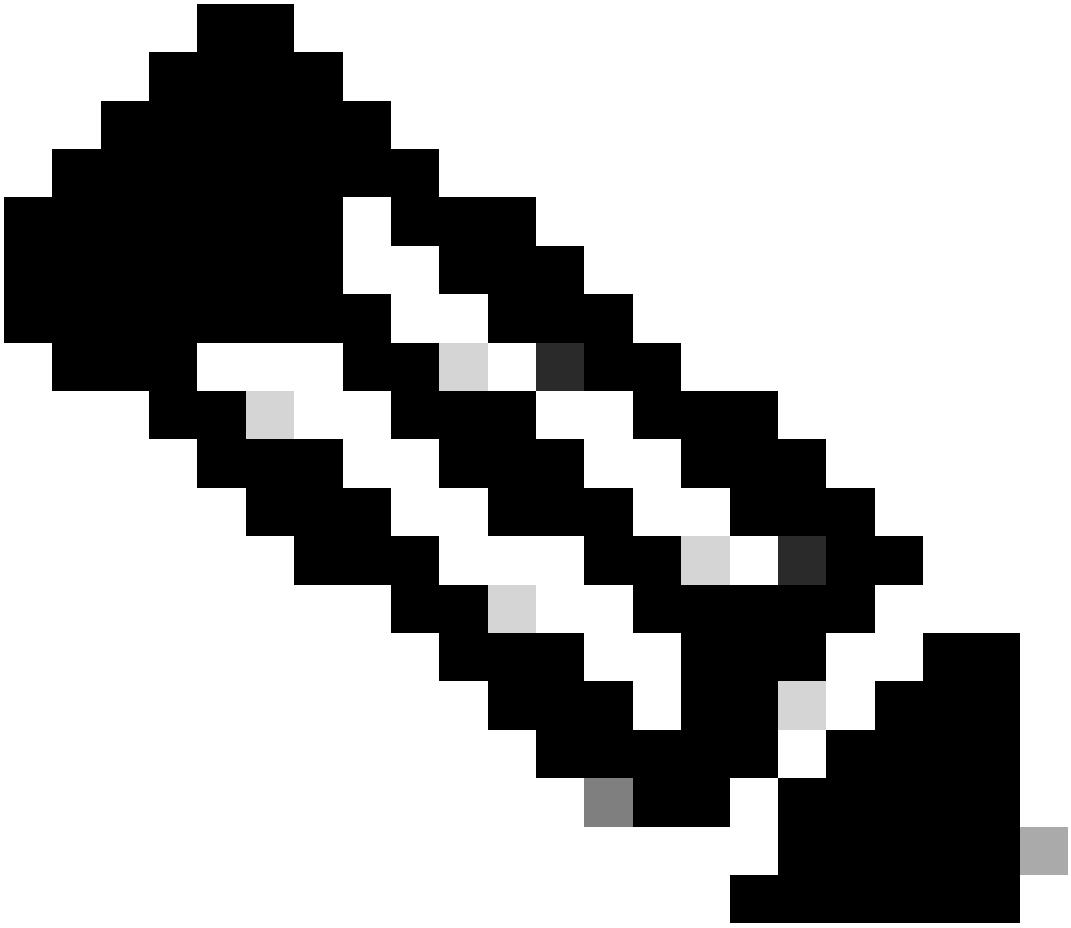


قاعدة تخويل الإصلاح

قاعدة تخويل بدون أدوات

في واجهة المستخدم الرسومية (GUI) Cisco ISE، انقر فوق (

) وأختر سياسة > سياسات وتوسيع سياسة التفويض. قم بتمكين نهج التخويل الثلاثة هذه وتكوينها:



ملاحظة: يجب تكوين قواعد التخويل هذه بالترتيب المحدد لضمان عمل تدفق الوضع بشكل صحيح.

Unknown_COMPLIANCE_REDIRECT:

•المعايير:

قم بتكوين network_access_authentication_pass و**compliance_unknown_devices** مع تعيين النتيجة على وضع دون فئات. تؤدي هذه الحالة إلى تشغيل التدفق بدون أدوات.

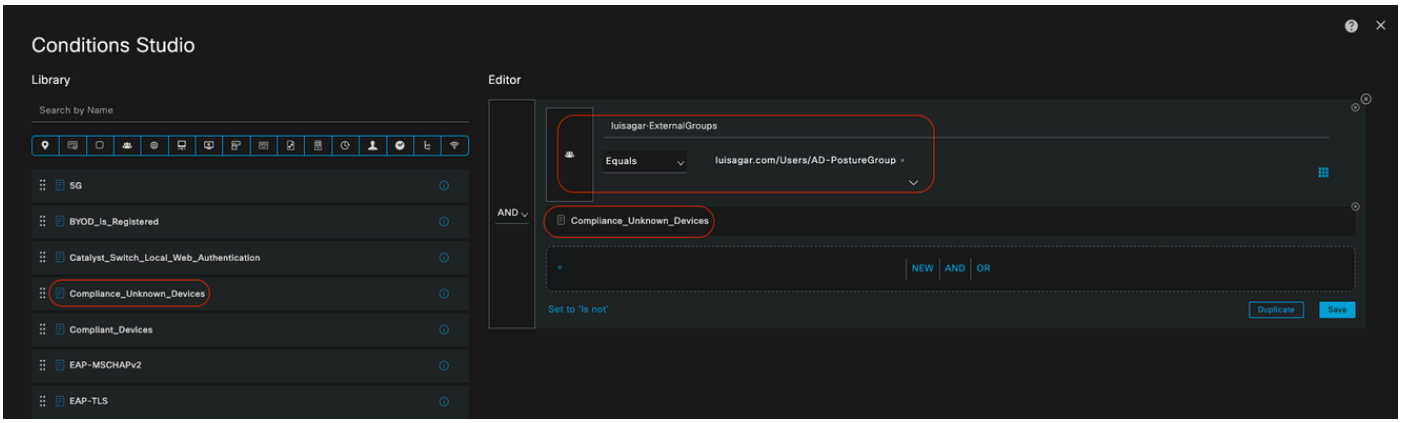
• مثال للشروط:

قم بتكوين حالة مجموعة Active Directory (AD) لحركة مرور المقطع.

يجب تكوين الشرط **compliance_unknown_devices** لأن حالة الوضع الأولي غير معروفة.

• ملف تعريف التخويل:

قم بتعيين **Agentless_Authorization_Profile** إلى قاعدة التخويل هذه للتأكد من مرور الأجهزة عبر تدفق الوضع دون الحاجة إلى إستخدام أية برامج. تحتوي هذه الحالة على تدفق بل حدود حتى تتمكن الأجهزة التي تصل هذا التوصيف من بدء تدفق بل حدود.



قاعدة تخويل غير معروفة

غير متوافق_Devices_Redirect:

• الشرط: قم بتكوين network_access_authentication_pass وnon_compliant_devices مع تعيين النتيجة على denyAccess. بدلا من ذلك، يمكنك إستخدام خيار الإصلاح، كما هو موضح في هذا المثال.

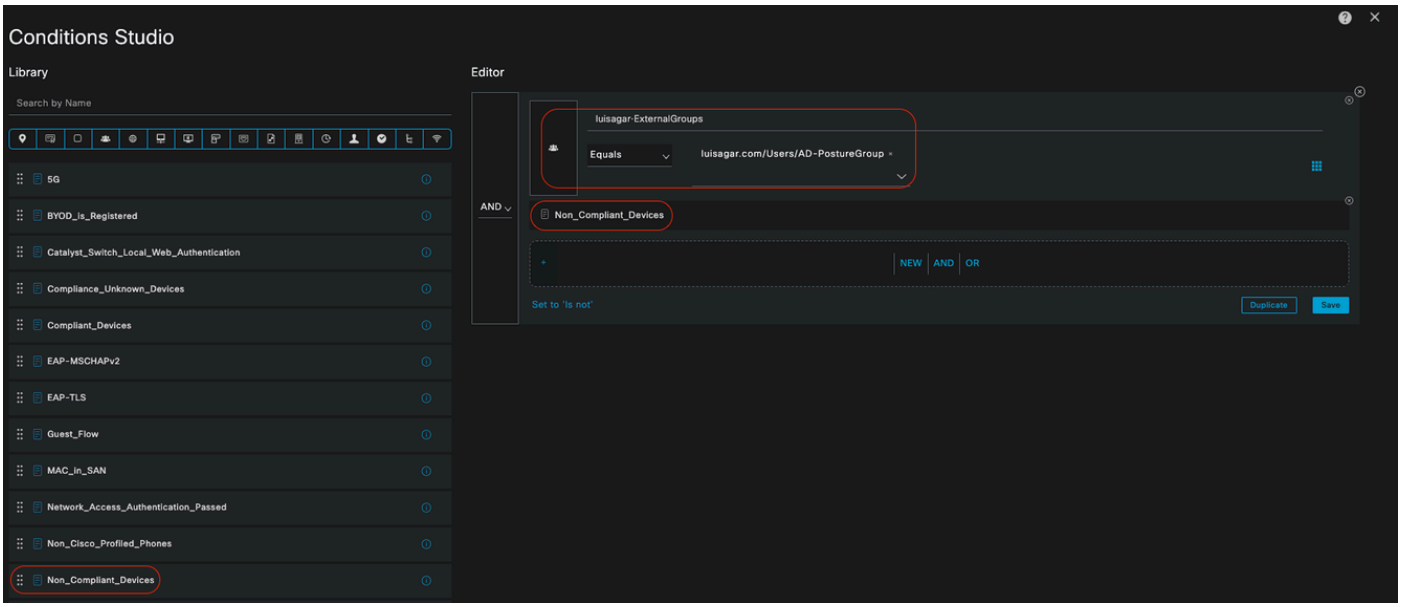
• مثال للشرط:

قم بتكوين حالة مجموعة AD لتقسيم حركة المرور.

يجب تكوين شرط **COMPLIANCE_UNKNOWN_DEVICES** لتخصيص موارد محدودة عندما تكون حالة الوضع غير متوافقة.

• ملف تعريف التخويل:

قم بتعيين **remediation_authorization_profile** لقاعدة التخويل هذه إلعلام الأجهزة غير المتوافقة بحالتها الحالية من خلال **مدخل نقطة الاتصال أو رفض الوصول.**



قاعدة تخويل غير متوافقة

compliant_devices_access:

•المعايير:

قم بتكوين network_access_authentication_pass و**compliant_devices** مع تعيين النتيجة إلى AllowedAccess.

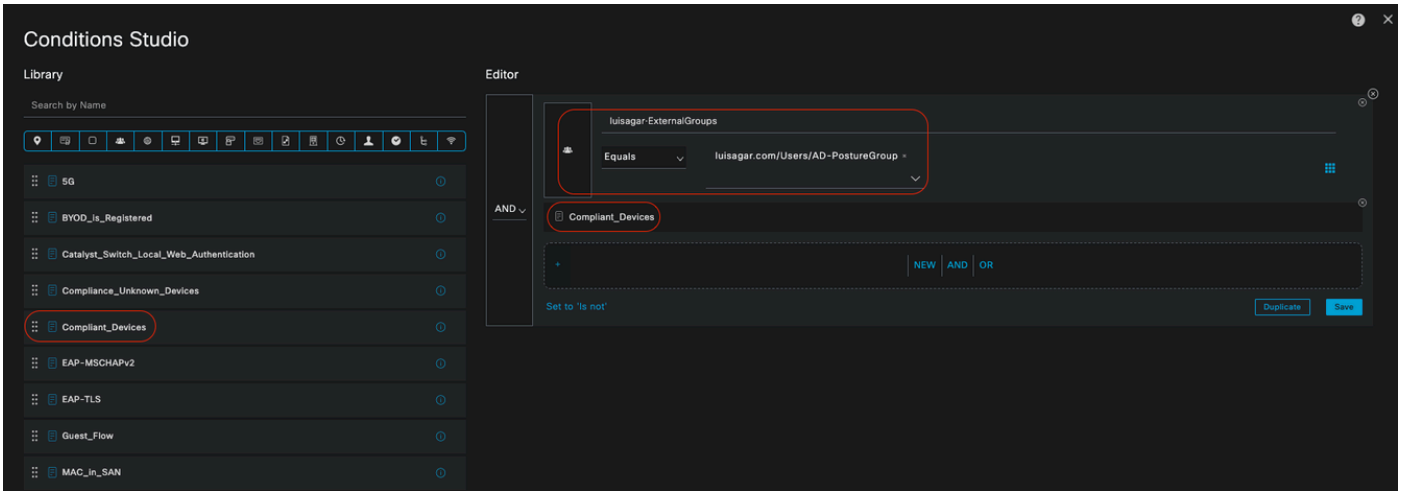
• مثال للشروط:

قم بتكوين حالة مجموعة AD لتقسيم حركة المرور.

يجب تكوين شرط **COMPLIANCE_UNKNOWN_DEVICES** بحيث يتم منح الأجهزة المتوافقة حق الوصول المناسب.

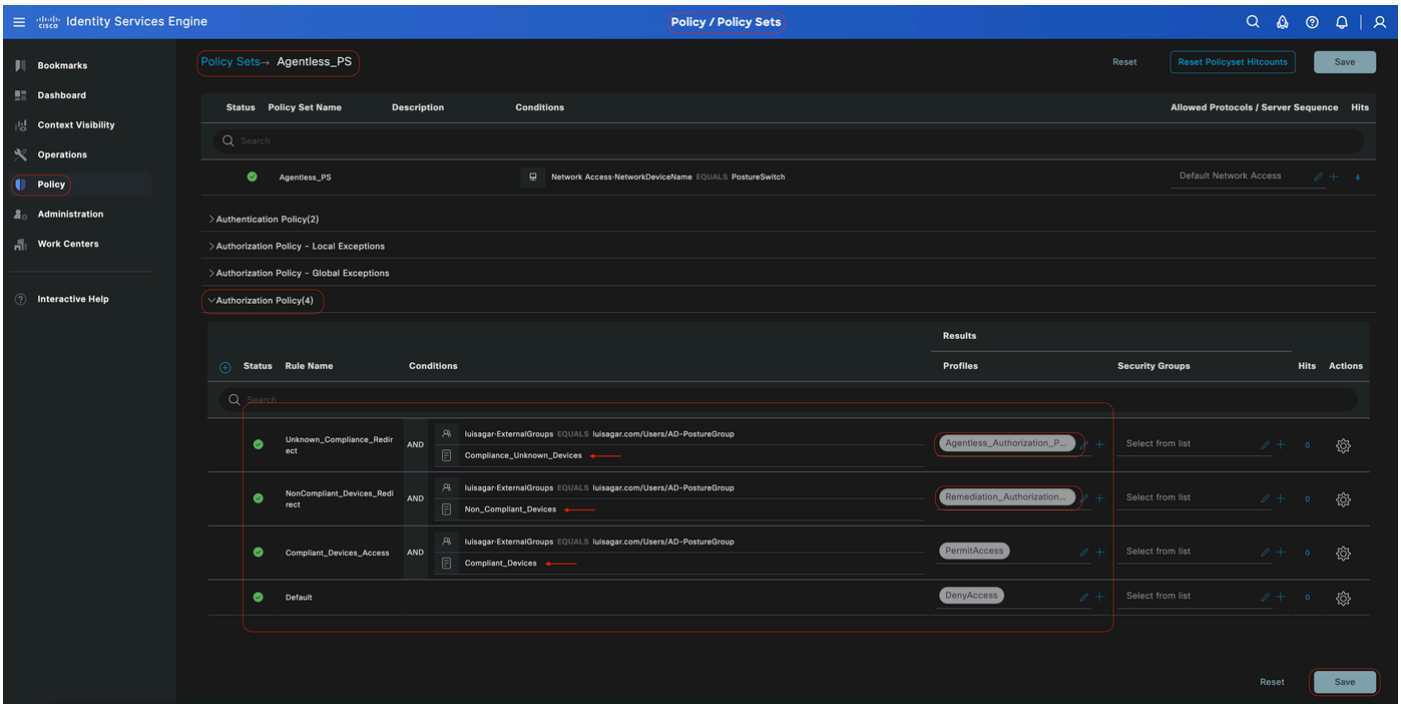
• ملف تعريف التخويل:

قم بتعيين **PermitAccess** لقاعدة التخويل هذه لضمان وصول الأجهزة المتوافقة. يمكن تخصيص ملف التعريف هذا لتلبية إحتياجات مؤسستك.



قاعدة تخويل متوافقة

كافة قواعد التخويل



قواعد التخويل

تكوين بيانات اعتماد تسجيل دخول نقطة النهاية

في واجهة المستخدم الرسومية Cisco ISE، انقر فوق Menuicon () واختر**Administration**>الإعدادات>البرامج النصية لنقطة النهاية>تكوين تسجيل الدخول، وقم بتكوين بيانات اعتماد العميل لتسجيل الدخول إلى العملاء.

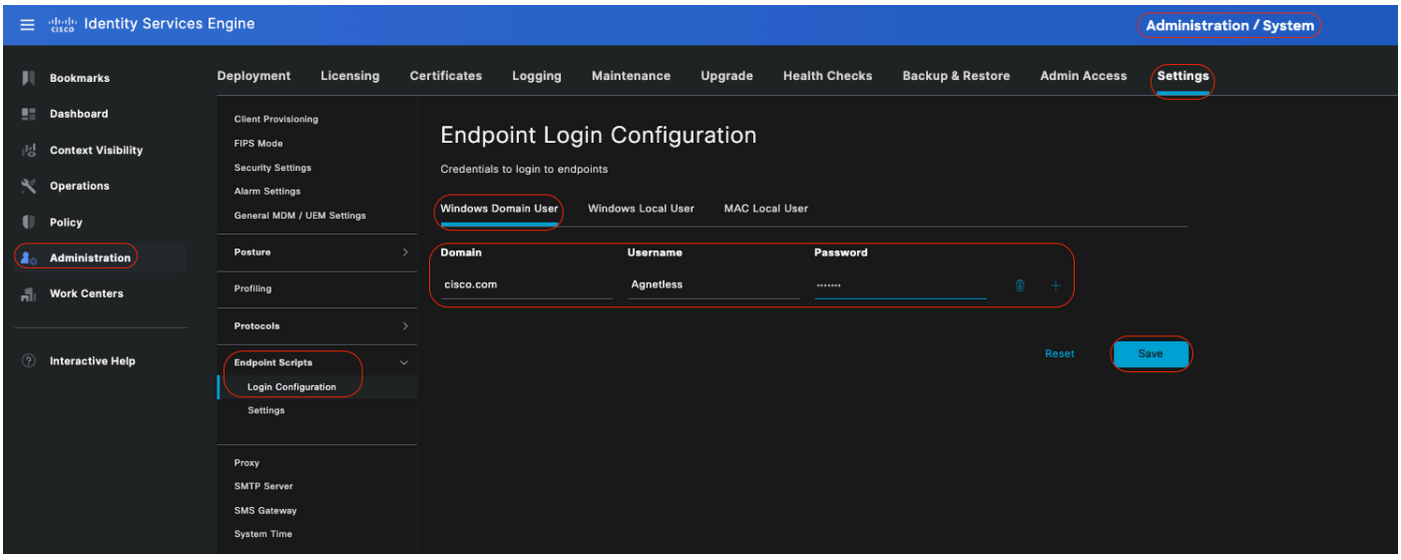
يتم إستخدام نفس بيانات الاعتماد هذه بواسطة البرامج النصية لنقطة النهاية حتى يمكن ل Cisco ISE تسجيل الدخول إلى العملاء.

بالنسبة لأجهزة Windows، تقوم فقط بتكوين علامتي التبويب الأوليين (مستخدم مجال **Windows** والمستخدم المحلي ل **Windows**

- **مستخدم مجال Windows:**

قم بتكوين بيانات اعتماد المجال التي يجب أن تستخدمها Cisco ISE لتسجيل الدخول إلى عميل عبر SSH. انقر على Plusicon وقم بإدخال كل ما تحتاجه من تسجيلات الدخول إلى Windows. لكل مجال، أدخل القيم المطلوبة في Domain وUsername وPasswordFields. إذا قمت بتكوين بيانات اعتماد المجال، سيتم تجاهل بيانات اعتماد المستخدم المحلي التي تم تكوينها في علامة تبويب مستخدم Windows المحلي.

إذا كنت تقوم بإدارة نقاط نهاية Windows التي تستخدم تقييم الوضع بدون برنامج من خلال مجال Active Directory، فتأكد من توفير اسم المجال مع بيانات الاعتماد التي تحتوي على امتيازات إدارية محلية.

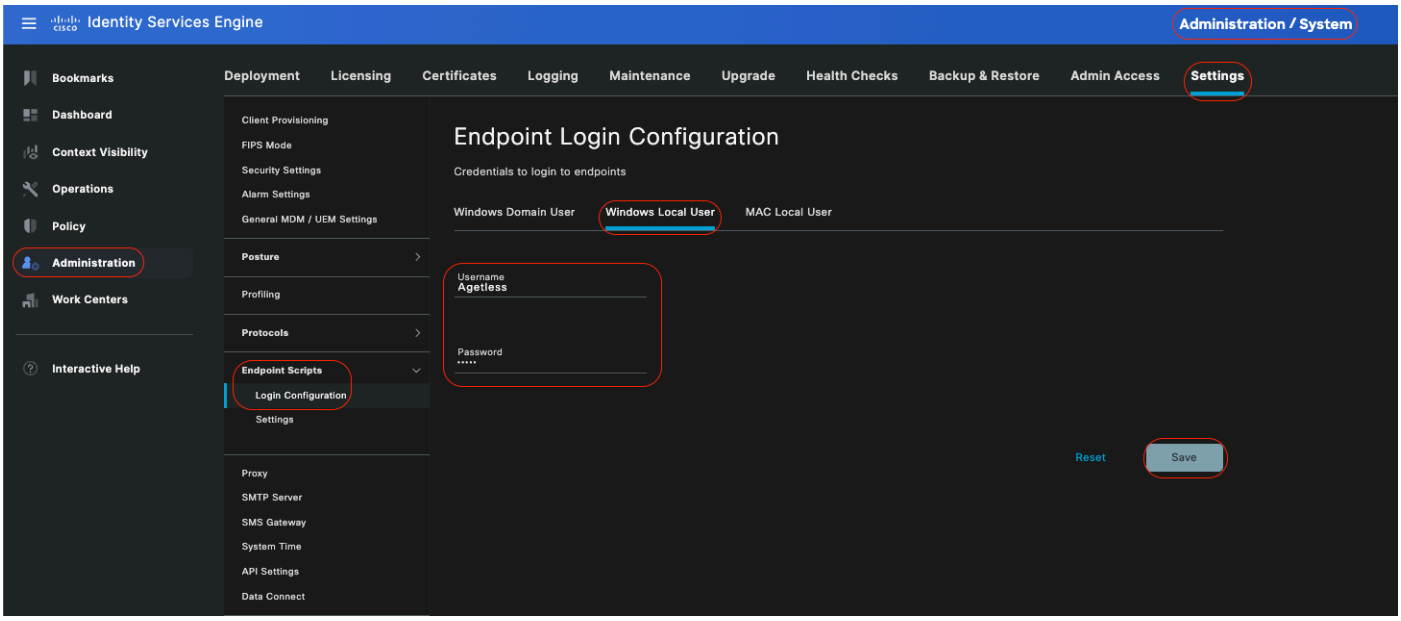


مستخدم مجال Windows

- **مستخدم Windows المحلي:**

قم بتكوين الحساب المحلي الذي يستخدمه Cisco ISE للوصول إلى العميل عبر SSH. يجب أن يكون الحساب المحلي قادرا على تشغيل PowerShell و PowerShell عن بعد.

إذا كنت لا تقوم بإدارة نقاط نهاية Windows التي تستخدم تقييم الوضع بدون برنامج من خلال مجال Active Directory، فتأكد من توفير بيانات الاعتماد التي لها امتيازات إدارية محلية.

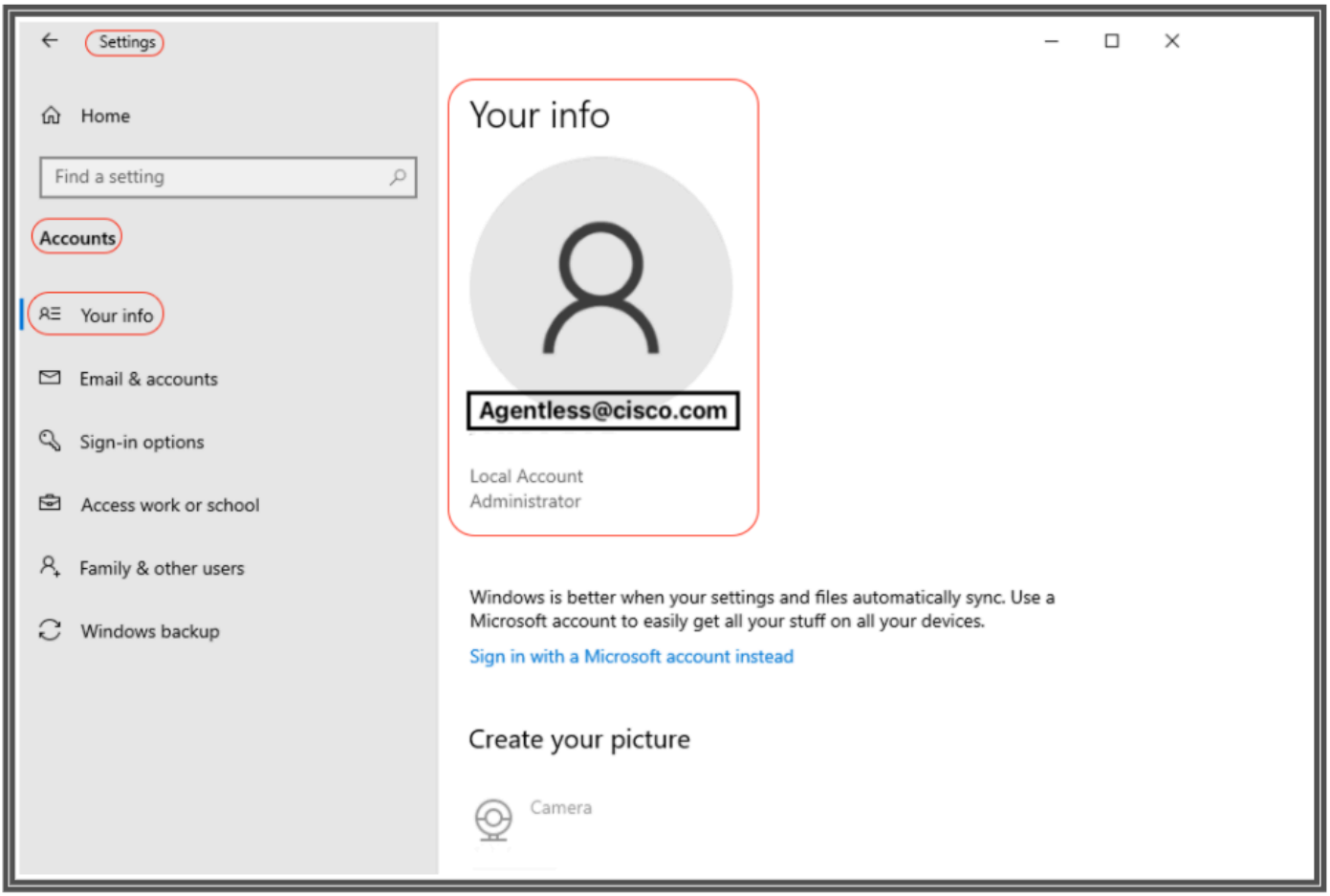


مستخدم *Windows* المحلي

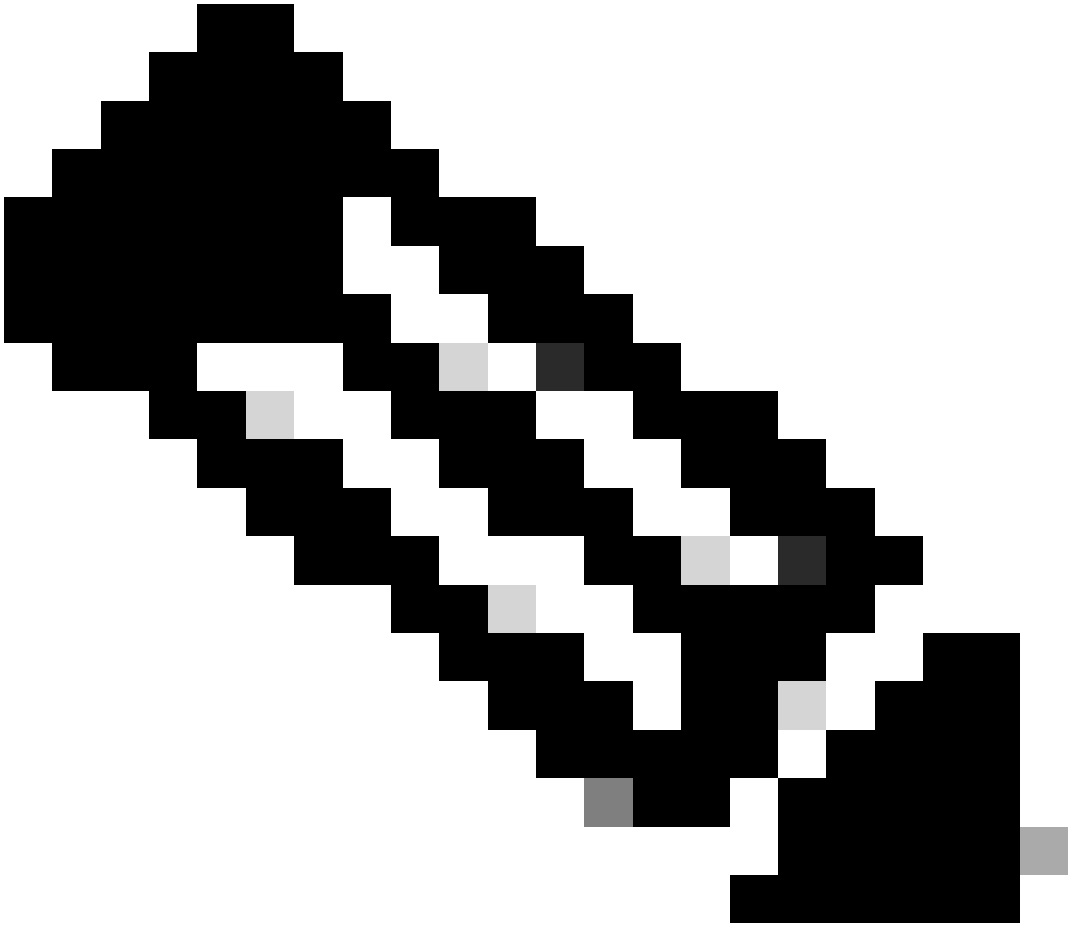
حسابات VEIFY

للتحقق من حساب مستخدم مجال Windows وحسابات مستخدمي Windows المحليين حتى يمكنك إضافة البيانات المناسبة بدقة تحت بيانات اعتماد تسجيل الدخول إلى نقطة النهاية، الرجاء إستخدام هذا الإجراء:

المستخدم المحلي ل Windows: باستخدام واجهة المستخدم الرسومية (تطبيق الإعدادات) انقر فوق الزر **WindowsStart**، ثم حدد الإعدادات (أيقونة العتاد)، ثم انقر فوق الحسابات، وحدد المعلومات الخاصة بك:



التحقق من الحسابات



ملاحظة: بالنسبة لنظام التشغيل MacOS، يمكنك الرجوع إلى **مستخدم Mac المحلي**. في مثال التكوين هذا، لن ترى تكوين MacOS.

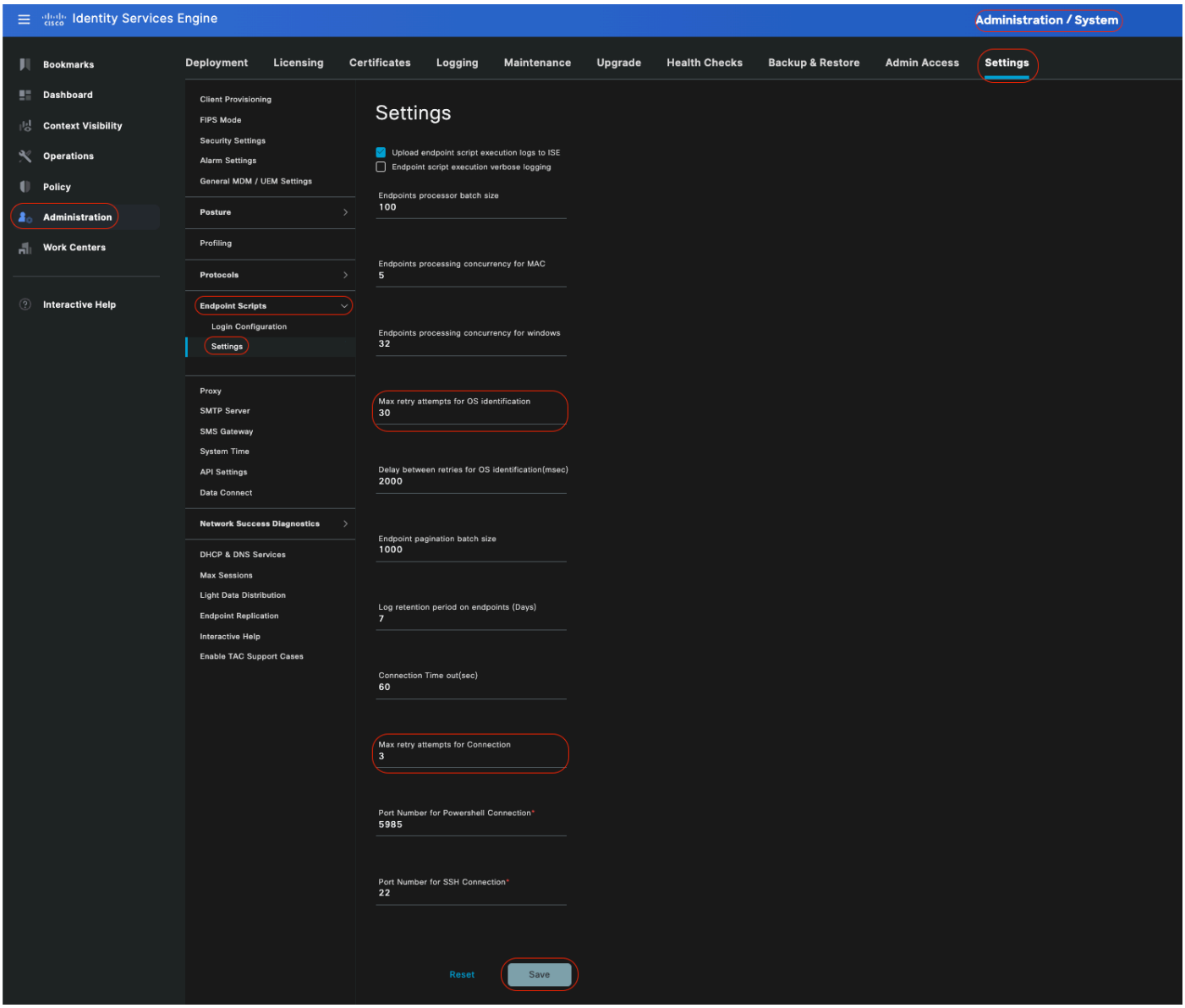
- **مستخدم MAC المحلي:** قم بتكوين الحساب المحلي الذي يستخدمه Cisco ISE للوصول إلى العميل عبر SSH. يجب أن يكون الحساب المحلي قادرا على تشغيل PowerShell و PowerShell عن بعد. في حقل UserNameField، أدخل اسم حساب الحساب المحلي.

لعرض اسم حساب Mac OS، قم بتشغيل الأمرwhoami في الطرفية:

الإعدادات

في واجهة المستخدم الرسومية Cisco ISE، انقر فوق Menuicon () واختر**Administration** > **الإعدادات** > **نصوص نقطة النهاية التفاعلية** > **الإعدادات**، وتكوين محاولات إعادة المحاولة القصوى لتعريف نظام التشغيل، والتأخير بين عمليات إعادة المحاولة لتعريف نظام التشغيل وما إلى ذلك. تحدد هذه الإعدادات مدى سرعة تأكيد مشاكل الاتصال. على سبيل المثال، حدث خطأ أثناء عدم فتح منفذ PowerShell في السجلات فقط بعد عدم استنفاد جميع عمليات إعادة المحاولة.

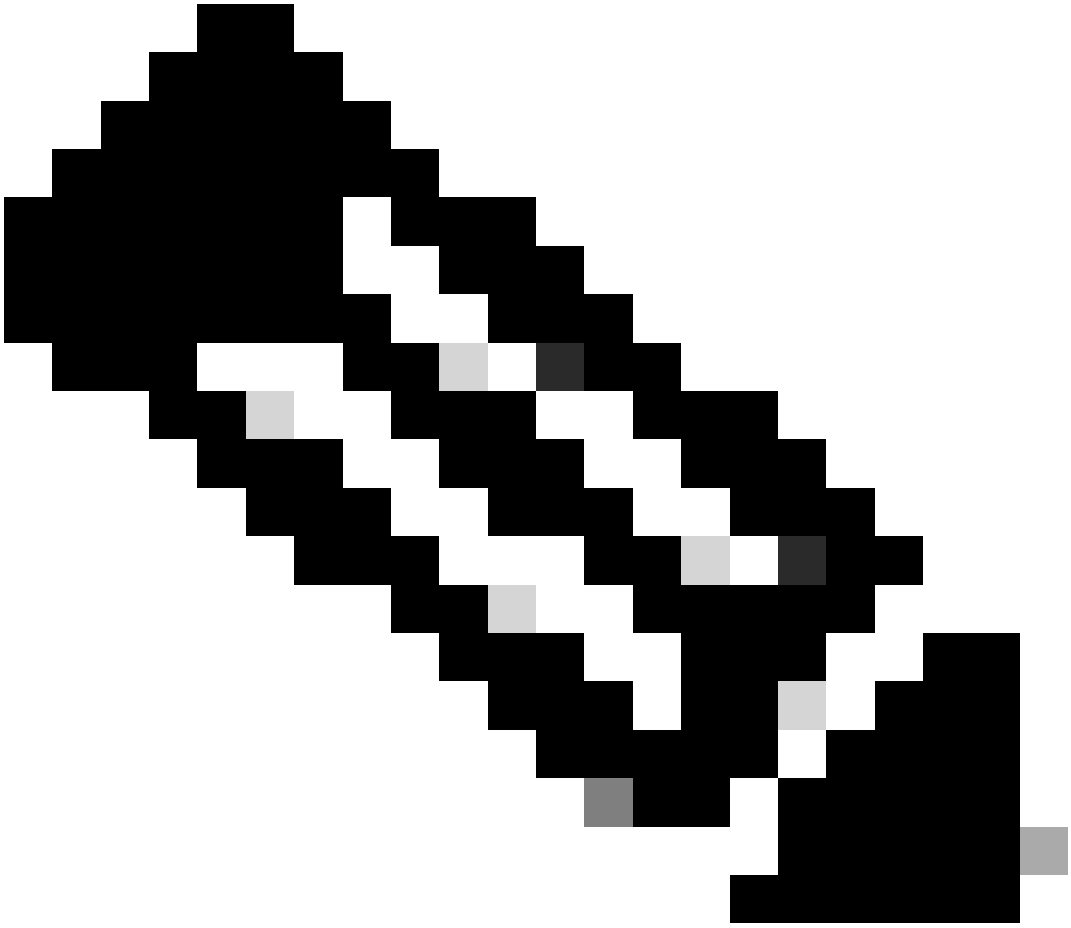
توضح لقطة الشاشة هذه إعدادات القيمة الافتراضية:



إعدادات البرنامج النصي لنقطة النهاية

مع اتصال العملاء بوضعية دون إستخدام أية أدوات، يمكنك رؤيتهم في سجلات Live.

تكوين نقطة نهاية Windows واستكشاف أخطائها وإصلاحها



ملاحظة: هذه بعض التوصيات للتحقق من أنها وتطبيقها على جهاز Windows، ومع ذلك، يجب الرجوع إلى وثائق Microsoft أو إلى ذلك أو PowerShell للوصول إلى المستخدم والامتيازات المتاحة لمثل هذه المشكلة في حالة الاتصال بدعم Microsoft...

التحقق من المتطلبات الأساسية واستكشاف الأخطاء وإصلاحها

إختبار اتصال TCP بالمنفذ 5985

لعملاء Windows، يجب فتح المنفذ 5985 للوصول إلى powershell على العميل. قم بتشغيل هذا الأمر لتأكيد اتصال TCP بالمنفذ 5985: **Test-NetConnection -ComputerName localhost -Port 5985**

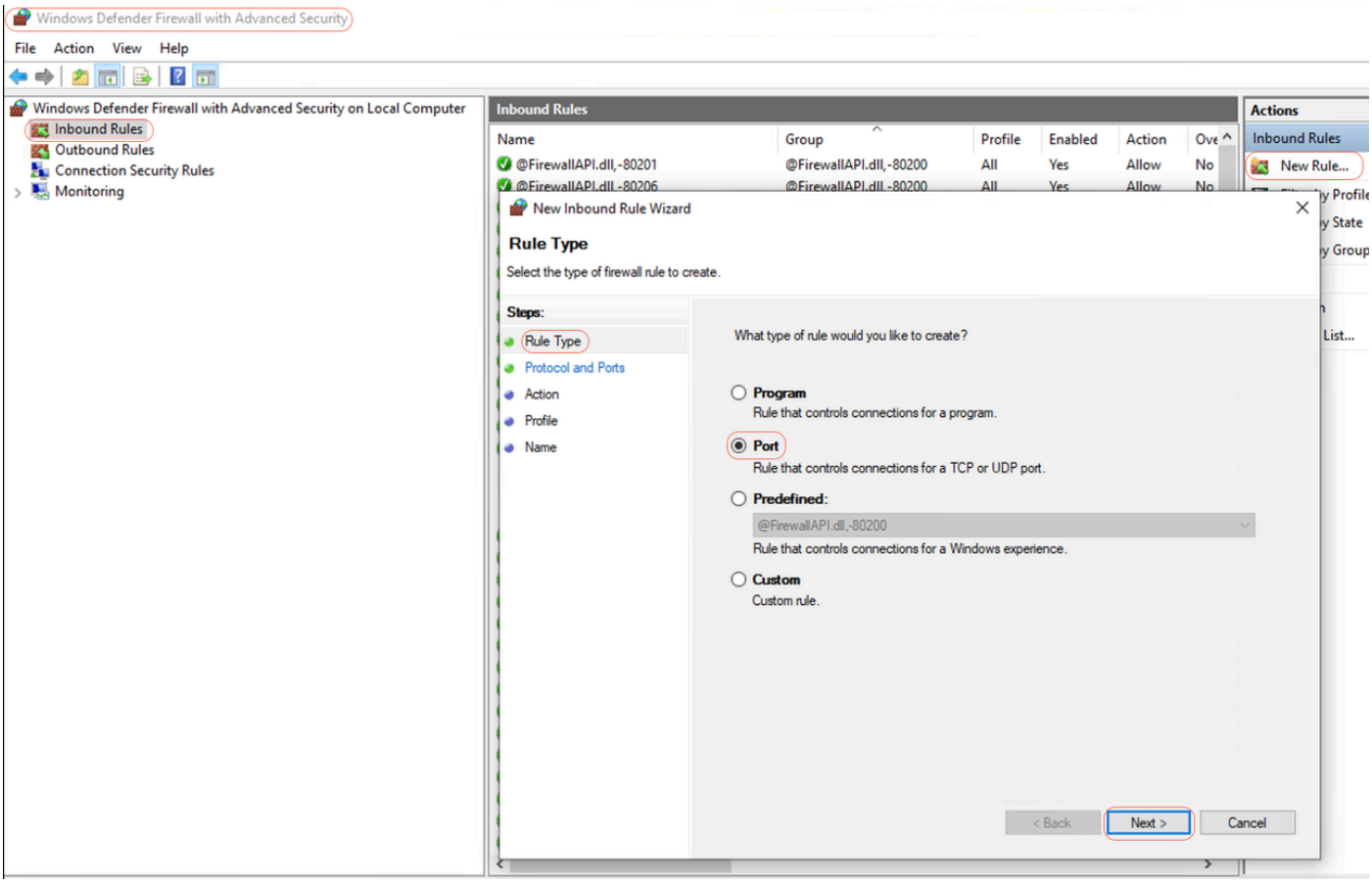
يشير الإخراج الموضح في لقطة الشاشة هذه إلى فشل اتصال TCP بالمنفذ 5985 على المضيف المحلي. هذا يعني أن خدمة WinRM (Windows Remote Management)، التي تستخدم المنفذ 5985، لا تعمل أو لم يتم تكوينها بشكل صحيح.

```
PS C:\Windows\system32> Test-NetConnection -Computer localhost -Port 5985
WARNING: TCP connect to (::1 : 5985) failed
WARNING: TCP connect to (127.0.0.1 : 5985) failed


ComputerName            : localhost
RemoteAddress           : ::1
RemotePort              : 5985
InterfaceAlias          : Loopback Pseudo-Interface 1
SourceAddress           : ::1
PingSucceeded           : True
PingReplyDetails (RTT) : 0 ms
TcpTestSucceeded        : False



PS C:\Windows\system32> ^C
```

Connection failed to WinRM

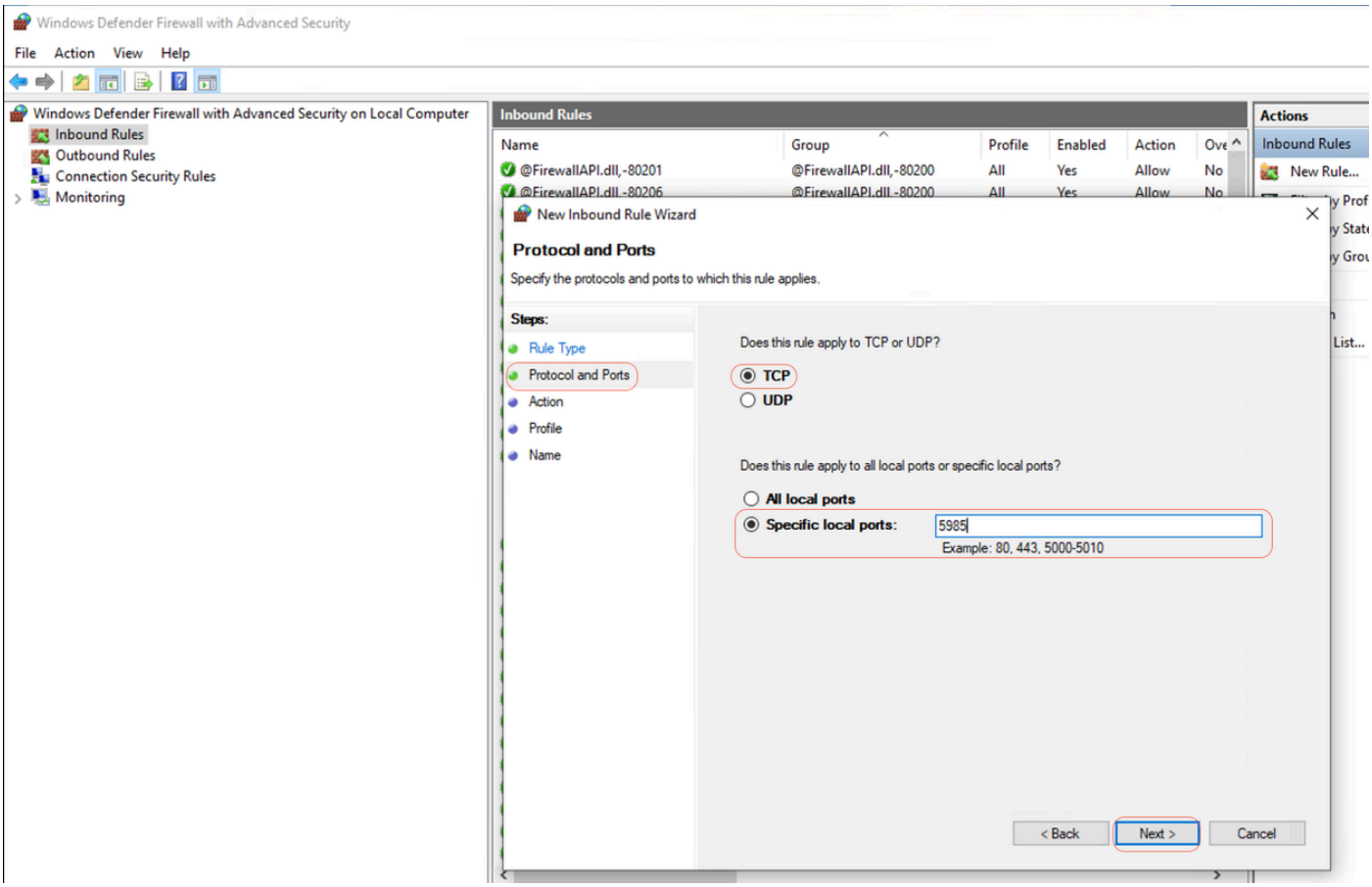
إنشاء قاعدة الوارد للسماح لـ PowerShell على المنفذ 5985

الخطوة 1- في واجهة المستخدم الرسومية (GUI) في Windows، انتقل إلى شريط البحث، واكتب جدار حماية Windows مع أمان متقدم، وانقر عليه وحدد تشغيل كمسؤول > قواعد الوارد > قاعدة جديدة > نوع القاعدة > المنفذ>التالي:



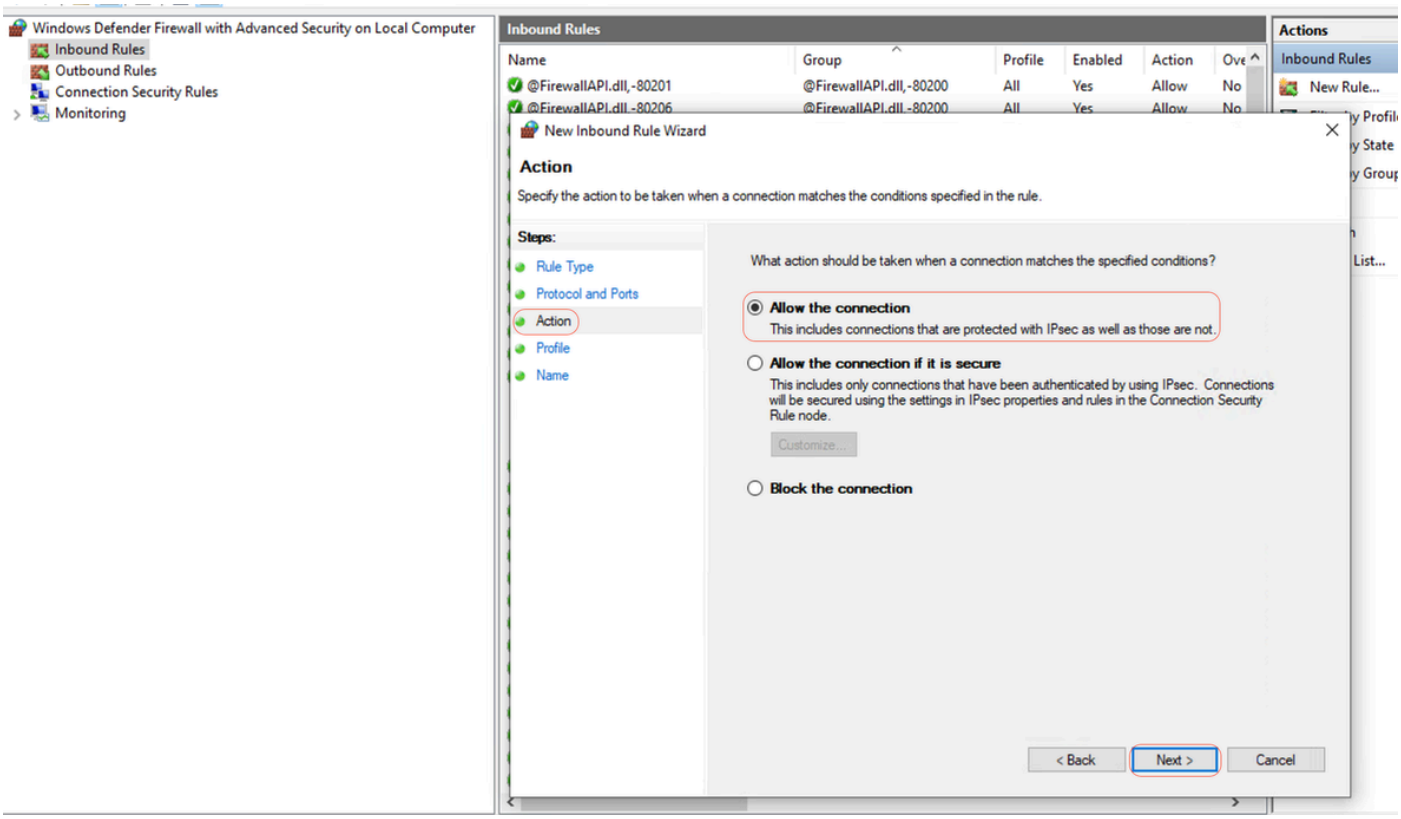
قاعدة الوارد الجديدة - المنفذ

الخطوة 2- تحت البروتوكولات والمنافذ، حدد TCP وحدد المنافذ المحلية، واكتب رقم المنفذ **5985** (المنفذ الافتراضي لـ PowerShell البعيد) وانقر فوق التالي:



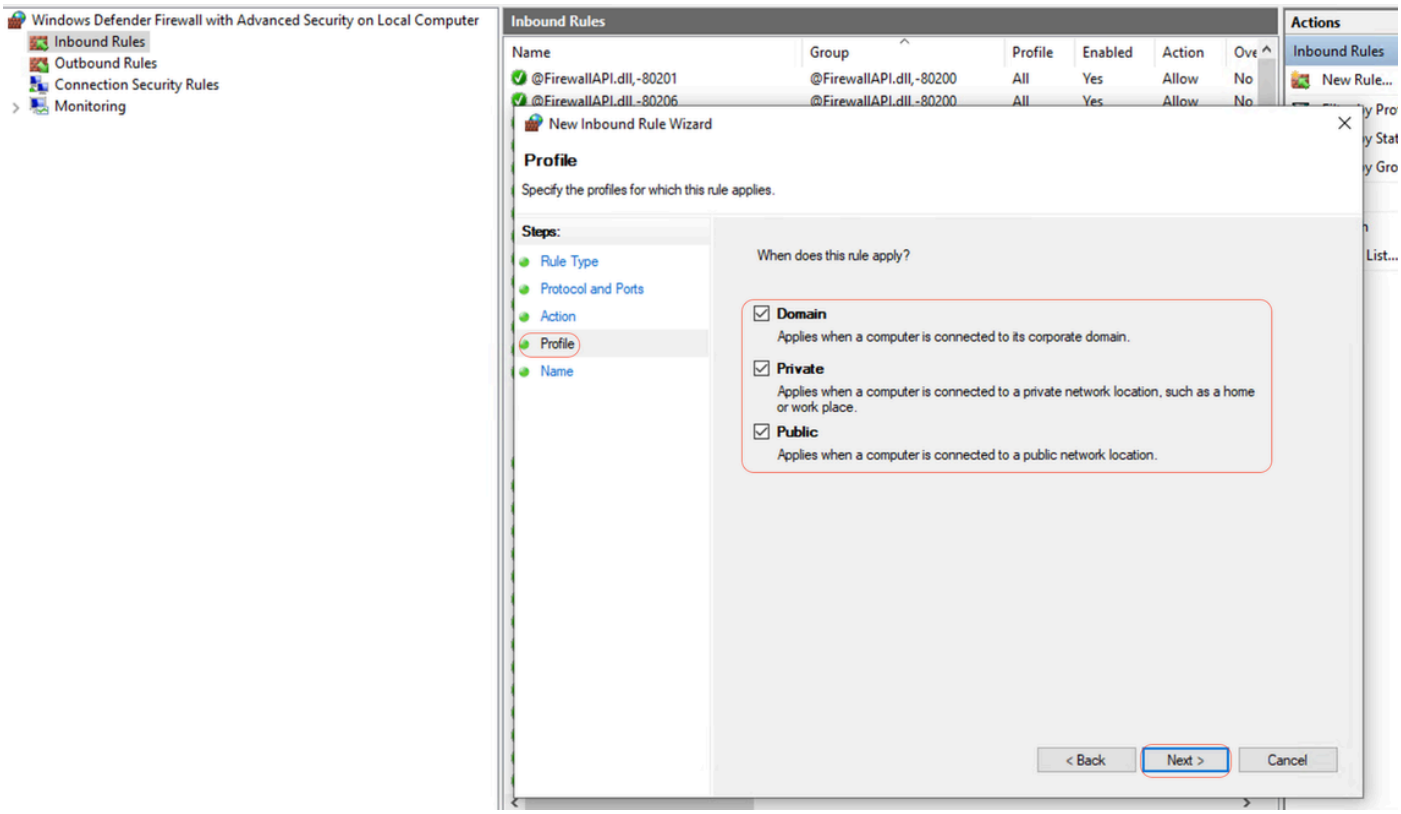
البروتوكولات والمنافذ

الخطوة 3- تحت الإجراء>تحديد السماح بالاتصال > التالي:



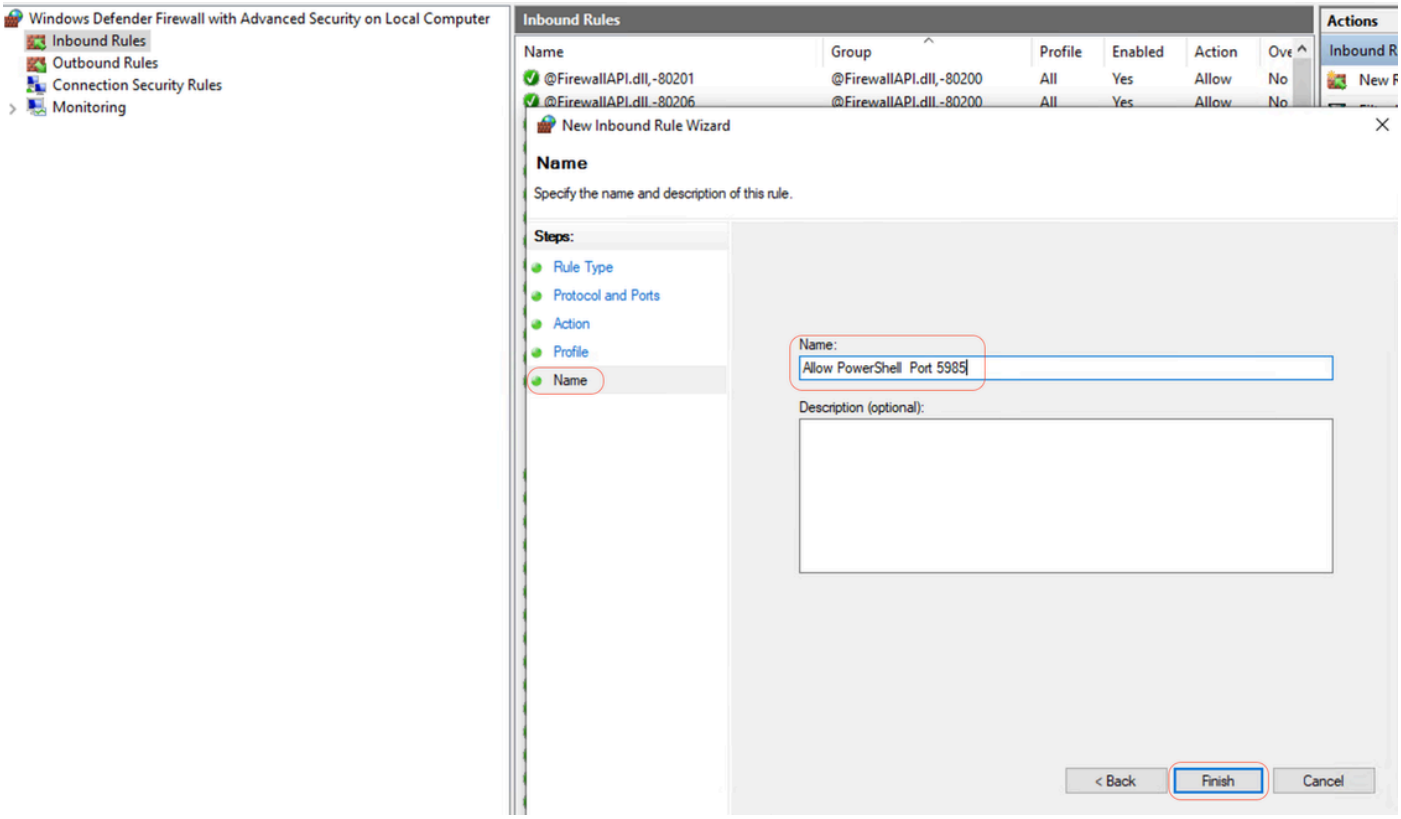
الإجراء

الخطوة 4- تحت ملف التعريف، حدد خانات الاختيار المجال، خاص، وعام وانقر بعد ذلك:



ملف التعريف

الخطوة 5- تحت الاسم، أدخل اسما للقاعدة، مثل السماح لـ PowerShell على المنفذ 5985 وانقر إنهاء:

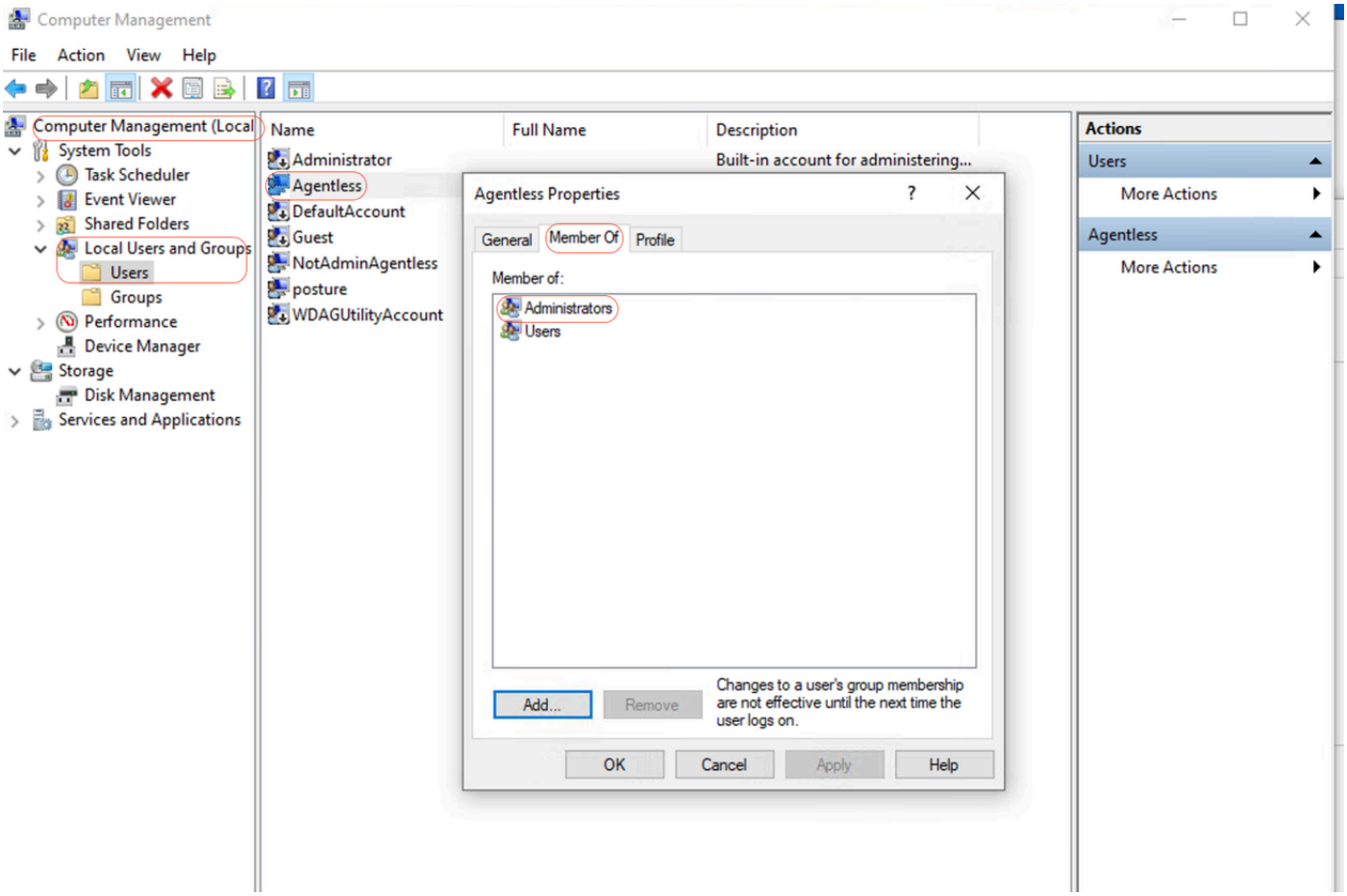


الاسم

بيانات اعتماد العميل الخاصة بتسجيل الدخول إلى shell يجب أن تحتوي على امتيازات مسؤول محلي

يجب أن يكون لبيانات اعتماد العميل الخاصة بتسجيل الدخول إلى shell امتيازات مسؤول محلي. لتأكيد ما إذا كان لديك امتيازات "مسؤول"، الرجاء التحقق من هذه الخطوات:

في واجهة المستخدم الرسومية Windows، انتقل إلى الإعدادات > إدارة الكمبيوتر > المستخدمون المحليون والمجموعات > المستخدمون > تحديد حساب المستخدم (في هذا المثال، يتم تحديد حساب بلا فئات) > يجب أن يحتوي الحساب على مجموعة المسؤولين.



امتيازات المسؤول المحلي

التحقق من صحة موزع رسائل WinRM

تأكد من تكوين وحدة إصغاء WinRM لـ **HTTP** على المنفذ **5985**:

C: \Windows\system32> **winrm enumerate winrm/config/listener** Listener Address = * **Transport = HTTP Port = 5985** Hostname Enabled = true URLPrefix = wsman CertificateThumbprint C: \Windows\system32>

تمكين WinRM لتقسيم PowerShell إلى بعيد

تأكد من تشغيل الخدمة وتكوينها للبدء تلقائيًا، انتقل عبر الخطوات التالية:

Enable the WinRM service **Enable-PSRemoting -Force** # Start the WinRM service **Start-Service WinRM** # Set the WinRM service to start automatically **Set-Service -Name WinRM -StartupType Automatic**

الناتج المتوقع:

C: \Windows\system32> **Enable-PSRemoting -Force** WinRM is already set up to receive requests on this computer. WinRM has been updated for remote management. WinRM firewall exception enabled. -Configured LocalAccountTokenFilterPolicy to grant administrative rights remotely to local users.

C: \Windows\system32> **Start-Service WinRM**

C: \Windows\system32> **Set-Service -Name WinRM -StartupType Automatic**

يجب أن يكون PowerShell الإصدار 7.1 أو إصدار أحدث. يجب أن يحتوي العميل على cURL v7.34 أو إصدار أحدث:

كيفية التحقق من إصدارات PowerShell و cURL على Windows

أحرص على ضمان استخدام الإصدارات المناسبة من PowerShell، حيث يعد cURL ضروريا لضمان عدم استخدام Posture (Posture) أية برامج عميلة:

التحقق من إصدار PowerShell

على Windows:

1. **افتح PowerShell:**

· اضغط على Win + X وحدد **Windows PowerShell** أو **Windows PowerShell (Admin)**.

2.قم بتنفيذ الأمر:$PSVersionTable.PSVersion

· يُنتج هذا الأمر تفاصيل إصدار PowerShell المثبت على النظام.

التحقق من إصدار cURL

على Windows:

1. افتح موجه أوامر:

· اضغط على Win + R، اكتب cmd، وانقر فوق **Enter**.

2. تنفيذ الأمر: curl --version

· يعرض هذا الأمر إصدار cURL المثبت على نظامك.

إخراج للتحقق من إصدارات PowerShell و cURL على أجهزة Windows

C: \Windows\system32> **$PSVersionTable.PSVersion** Major Minor Build Revision ----- ----- ----- ----- 7 1 19041 4291

C: \Windows\system32>

C: \Windows\system32>

C: \Windows \system32>**curl --version curl 8.4.0 (Windows) libcurl/8.4.0 Schannel WinIDN** Release-Date: 2023-10-11 Protocols: dict file ftp ftps http https imap imaps pop3 pop3s smtp smtps telnet tftp ftps http https Features: AsynchNS HSTS HTTPS-proxy IDN IPv6 Kerberos

Largefile NTLM SPNEGO SSL SSPI threadsafe Unicode UnixSockets c: \Windows\system32>

تهيئة إضافية

يقوم هذا الأمر بتكوين الجهاز لديك للثقة في مضيفين بعيدين محددين لاتصالات WinRM: Set-Item WSMan:\localhost\Client\TrustedHosts -Value <Client-IP>

C: \Windows\system32> **Set-Item WSMan:\localhost\Client\TrustedHosts -Value x.x.x.x** WinRM Security Configuration. This command modifies the TrustedHosts list for the WinRM client. The computers in the TrustedHosts list cannot be authenticated. The client can send credential information to these computers. Are you sure that you want to modify this list? [Y] Yes [N] No [S] Suspend [?] Help (default is "y"): **Y** PS C: \Windows \system32> -

يعد cmdlet الاختبار مع معلمات -Authentication Negotiate و-Credential أداة فعالة للتحقق من توفر خدمة WinRM وتكوينها على جهاز بعيد: test-wsman <Client-IP> -Authentication Negotiate -Credential <Accountname>

سإ وأ كام

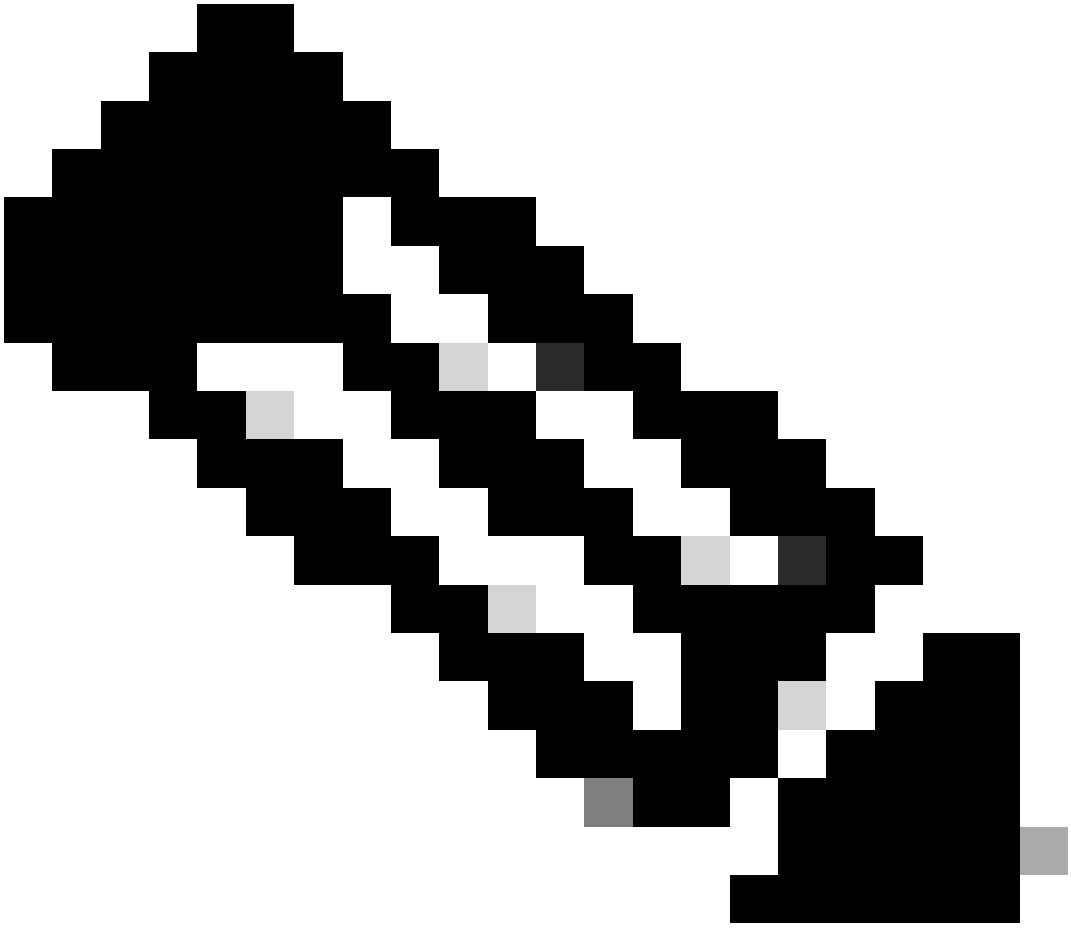
يجب أن يكون PowerShell الإصدار 7.1 أو إصدار أحدث. يجب أن يحتوي العميل على cURL v7.34 أو إصدار أحدث:

على MacOS:

1. **المحطة الطرفية المفتوحة:**

يمكنك العثور على وحدة طرفية في التطبيقات > الأدوات المساعدة.

2. تنفيذ الأمر: pwsh -Command '$PSVersionTable.PSVersion'



ملاحظة: ملاحظة: · تأكد من تثبيت PowerShell Core (pwsh). إذا لم تكن كذلك، فيمكنك تثبيته عبر Homebrew (تأكد من أنك قمت بتثبيت Himebrew): brew install --cask powershell

---

على MacOS:

1. **افتح المحطة الطرفية:**

· يمكنك العثور على وحدة طرفية في **التطبيقات > الأدوات المساعدة**.

2. تنفيذ الأمر: curl --version

· يجب أن يعرض هذا الأمر إصدار cURL المثبت على نظامك.

لعملاء MacOS، يجب أن يكون المنفذ 22 للوصول إلى SSH مفتوحا للوصول إلى العميل

الدليل بالتفصيل:

1. **تفضيلات النظام المفتوحة:**

· انتقل إلى **تفضيلات النظام** من قائمة Apple.

2. **تمكين تسجيل الدخول عن بعد:**

· انتقل إلى **المشاركة**.

· حدد المربع المجاور **لتسجيل الدخول عن بعد**.

· تأكد من تعيين خيار **السماح بالوصول إلى المستخدمين أو المجموعات المناسبة**. يسمح تحديد **جميع المستخدمين** لأي مستخدم لديه حساب صالح على Mac بتسجيل الدخول عبر SSH.

3. **التحقق من إعدادات جدار الحماية:**

· في حالة تمكين جدار الحماية، يلزمك التأكد من أنه يسمح باتصالات SSH.

· انتقل إلى **تفضيلات النظام > الأمان والخصوصية > جدار الحماية**.

· انقر فوق الزر **خيارات جدار الحماية**.

· تأكد من سرد **تسجيل الدخول عن بعد** أو **بروتوكول طبقة الأمان (SSH)** والسماح به. إذا لم يكن مدرجا، انقر فوق الزر **إضافة** (+) لإضافته.

4. **المنفذ المفتوح 22 عبر الوحدة الطرفية (إذا لزم الأمر):**

· فتح **التطبيق الطرفي** من **التطبيقات > الأدوات المساعدة**.

· أستخدم الأمر pfctl للتحقق من قواعد جدار الحماية الحالية والتأكد من أن المنفذ 22 مفتوح:sudo pfctl -sr | غروب 22

· إذا لم يكن المنفذ 22 مفتوحا، فيمكنك يدويا إضافة قاعدة للسماح لـ SSH:echo "تمرير بروتوكول TCP من أي إلى أي منفذ 22" | SUDO PFCTL -ef -

5. **إختبار وصول SSH:**

· من جهاز آخر، افتح عميل وحدة طرفية أو SSH.

· محاولة الاتصال بعميل MacOS باستخدام عنوان IP الخاص به:اسم مستخدم SSH@<macOS-client-IP>

· إستبدال اسم المستخدم بحساب المستخدم المناسب و<macOS-client-IP> بعنوان IP الخاص بعميل MacOS.

بالنسبة لنظام التشغيل MacOS، تأكد من أنه اذا تم تحديثه في حال فشل تثبيت الشهادة على نطاق النهاية لأجهزة تتجنب فشل:

عند إدارة نطاق نهاية MacOS، من المهم التأكد من أن أوامر إدارية معينة يمكن تنفيذها بدون طلب كلمة مرور.

المتطلبات الأساسية

• وصول المسؤول على جهاز MacOS.

• معرفة أساسية بأوامر المحطة الطرفية.

خطوات تحديث ملف المحسنين

1. **المحطة الطرفية المفتوحة:**

• يمكنك العثور على وحدة طرفية في **التطبيقات > الأدوات المساعدة**.

2. **قم بتحرير ملف المحسنين:**

• أستخدم الأمر visual لتحرير ملف المحسنين بأمان. وهذا يضمن التقاط أي أخطاء في بناء الجملة قبل حفظ الملف.sudo visual

• ستتم مطالبتك بإدخال كلمة مرور المسؤول.

3. **ابحث عن القسم المناسب:**

• في محرر المرئيات، انتقل إلى القسم حيث يتم تعريف القواعد الخاصة بالمستخدم. بشكل نموذجي، هذا هو الجزء السفلي من الملف.

4. **إضافة الإدخال المطلوب:**

• أضف هذا السطر لمنح المستخدم المحدد الإذن لتشغيل أوامر الأمان وتنسيق بدون كلمة مرور: <macadminusername> ALL = (ALL) NOPASSWD: /usr/bin/security, /usr/bin/osascript

• إستبدال <**macadminusername**> باسم المستخدم الفعلي لمسؤول MacOS.

5. **الحفظ والخروج:**

• إذا كنت تستخدم المحرر الافتراضي (النانو)، فاضغط على Ctrl+X للإنهاء، ثم اضغط على Y لتأكيد التغييرات، واضغط على Enter لحفظ الملف.

• إذا كنت تستخدم vi أو vim، اضغط على esc، اكتب **:wq**، واضغط على Enter للحفظ والخروج.

6. **تحقق من التغييرات:**

• لضمان سريان التغييرات، يمكنك تشغيل أمر يتطلب أذونات SUDO المحدثة. على سبيل المثال:

sudo /usr/bin/security find-certificate -a sudo /usr/bin/osascript -e 'tell application "Finder" to display dialog "Test"'

• يمكن تنفيذ هذه الأوامر دون المطالبة بكلمة مرور.

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).