تكوين VPN (الشبكة الافتراضية الخاصة) متعددة المصادقة مع ASA AnyConnect من خلال SAML (لغة ترميز تأكيد الأمان) من Microsoft Azure من العوامل

المحتويات

المقدمة

يوضح هذا المستند كيفية تكوين لغة ترميز تأكيد الأمان (SAML) مع التركيز على ASA AnyConnect من خلال Microsoft Azure MFA.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- معرفة أساسية بتكوين RA VPN على جهاز الأمان القابل للتكيف (ASA).
- معرفة أساسية ب SAML و Microsoft Azure.
- تم تمكين ترخيص AnyConnect (APEX أو VPN فقط).

المكونات المستخدمة

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

- اشتراك Microsoft Azure AD.
- Cisco ASA 9.7+ و AnyConnect 4.6+
- عميل ملف تعريف AnyConnect VPN

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

SAML هو إطار عمل يستند إلى XML لتبادل بيانات المصادقة والتفويض بين مجالات الأمان. وهو يعمل على إنشاء دائرة من الثقة بين المستخدم ومزود الخدمة (SP) ومزود الهوية (IDp) مما يسمح للمستخدم بتسجيل الدخول مرة واحدة لعدة خدمات. يتم دمج Microsoft Azure MFA بسلاسة مع جهاز VPN ASA من Cisco لتوفير أمان إضافي لتسجيل دخول شبكة VPN من Cisco AnyConnect.

مكونات SAML

بيانات التعريف: المستند المستند إلى XML وهو الذي يضمن معاملة آمنة بين مقدم P ومقدم SP. وهو يسمح للمقدم والمرفق الاستراتيجي بالتفاوض على الاتفاقيات.

الأدوار المدعومة بواسطة الأجهزة (IdP، SP)

يمكن أن يدعم الجهاز أكثر من دور واحد وقد يحتوي على قيم لكل من SP و IDp. تحت حقل EntityDescriptor يكون IDPSSODescriptor، إذا كانت المعلومات الواردة تخص مقدم تسجيل دخول أحادي أو محدد SPSSODescriptor إذا كانت المعلومات الواردة تخص SP لتسجيل دخول واحد. وهذا مهم لأنه يجب أخذ القيم الصحيحة من الأقسام المناسبة لإعداد SAML بنجاح.

مقدم الكيان: هذا الحقل وهو مقدم فريد ل SP أو IDp. يمكن أن يحتوي الجهاز الواحد على عدة خدمات ويمكنه استخدام مقدمات كيانات مختلفة للتفريق بينها. على سبيل المثال، يحتوي ASA على مقدمات كيان مختلفة لمجموعات النفق المختلفة التي يلزم مصادقتها. تحتوي مقدم الهوية الذي يقوم بمصادقة كل مجموعة نفق على إدخالات مقدم كيان منفصلة لكل مجموعة نفق لتحديد هذه الخدمات بدقة.

يمكن أن يدعم ASA مقدمات متعددة وله مقدم كيان منفصل لكل مقدم للتمييز بينها. إذا تلقى أي من الجانبين رسالة من جهاز ال يحتوي على مقدم كيان تم تكوينه مسبقا، فمن المحتمل أن يسقط الجهاز هذه الرسالة، وتفشل مصادقة SAML. يمكن العثور على مقدم الكيان داخل حقل EntityDescriptor بجانب EntityID.

عناوين URL للخدمة: تعرف هذه عناوين URL لخدمة SAML التي يتم توفيرها بواسطة SP أو IdP. بالنسبة لمعرف الخدمة (IdPs)، تكون هذه الخدمة هي خدمة تسجيل الخروج الأحادي وخدمة تسجيل الدخول الأحادي. بالنسبة لمزودي الخدمات الاجتماعية، عادة ما تكون هذه الخدمة هي خدمة العملاء الموكدة وخدمة تسجيل الخروج الأحادي.

يستخدم SP عنوان URL لخدمة تسجيل الدخول الأحادي الذي تم العثور عليه في بيانات تعريف IdP لإعادة توجيه المستخدم إلى IdP للمصادقة. في حالة تكوين هذه القيمة بشكل غير صحيح، لا يتلقى IdP طلب المصادقة المرسل بواسطة SP أو يتعذر عليه معالجته بنجاح.

يتم إستخدام عنوان URL لخدمة العملاء لتأكيد الهوية الذي تم العثور عليه في بيانات تعريف SP بواسطة IDp لإعادة توجيه المستخدم مرة أخرى إلى SP وتوفير معلومات حول محاولة مصادقة المستخدم. في حالة تكوين هذا بشكل غير صحيح، لا يتلقى SP التأكيد (الاستجابة) أو يتعذر معالجته بنجاح.

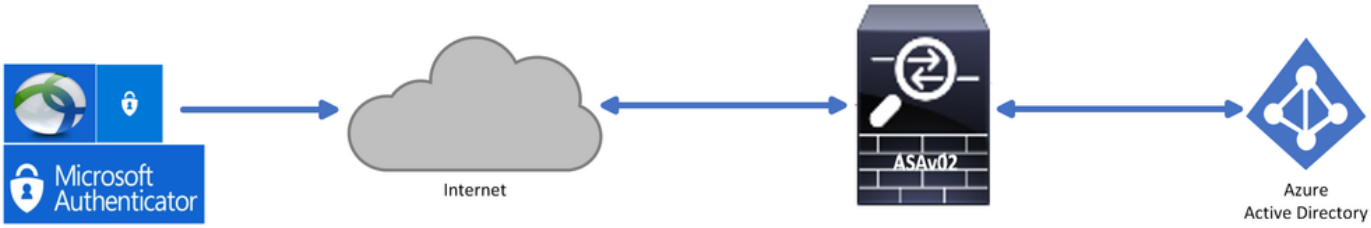
يمكن العثور على عنوان URL لخدمة تسجيل الخروج الأحادي على كل من SP و IDp. ويتم إستخدامه لتسهيل تسجيل الخروج من جميع خدمات SSO من SP وهو إختياري على ASA. عندما يتم تكوين عنوان URL لخدمة SLO من بيانات تعريف IdP على SP، عندما يقوم المستخدم بتسجيل الخروج من الخدمة على SP، يرسل SP الطلب إلى IdP. بمجرد أن يقوم IdP بتسجيل خروج المستخدم من الخدمات بنجاح، فإنه يعيد توجيه المستخدم مرة أخرى إلى SP ويستخدم عنوان URL لخدمة SLO الموجود ضمن بيانات تعريف SP.

روابط SAML لعناوين URL الخاصة بالخدمة: الروابط هي الطريقة التي يستخدمها SP لنقل المعلومات إلى IdP والعكس بالعكس للخدمات. ويتضمن ذلك إعادة توجيه HTTP و HTTP POST و Artifact. ولكل طريقة طريقة طريقة طريقة مختلفة لنقل البيانات. يتم تضمين طريقة الربط التي تدعمها الخدمة ضمن تعريف هذه الخدمات. على سبيل المثال: SingleSignOnService Binding="urn:oasis:names:tc:saml:2.0:bindings:http-redirect" location= خدمة SSO >. الدعم ASA ربط Artifact. يستخدم ASA دائما طريقة إعادة توجيه HTTP لطلبات مصادقة SAML، لذلك من المهم إختيار عنوان URL لخدمة SSO الذي يستخدم ربط HTTP لإعادة التوجيه بحيث يتوقع IdP هذا.

شهادات لعمليات التوقيع والتشفير

لتوفير السرية والنزاهة للرسائل المرسلة بين SP و IDp، يتضمن SAML القدرة على تشفير البيانات وتوقيعها. يمكن تضمين الشهادة المستخدمة لتشفير البيانات و/أو توقيعها ضمن بيانات التعريف بحيث يمكن للطرف الذي يستلم التحقق من رسالة SAML والتأكد من أنها تأتي من المصدر المتوقع. يمكن العثور على الشهادات المستخدمة للتوقيع والتشفير ضمن بيانات التعريف ضمن KeyDescriptor use=signature و KeyDescriptor use=encryption، بكل إحترام، ثم X509Certificate. الدعم ASA تشفير رسائل SAML.

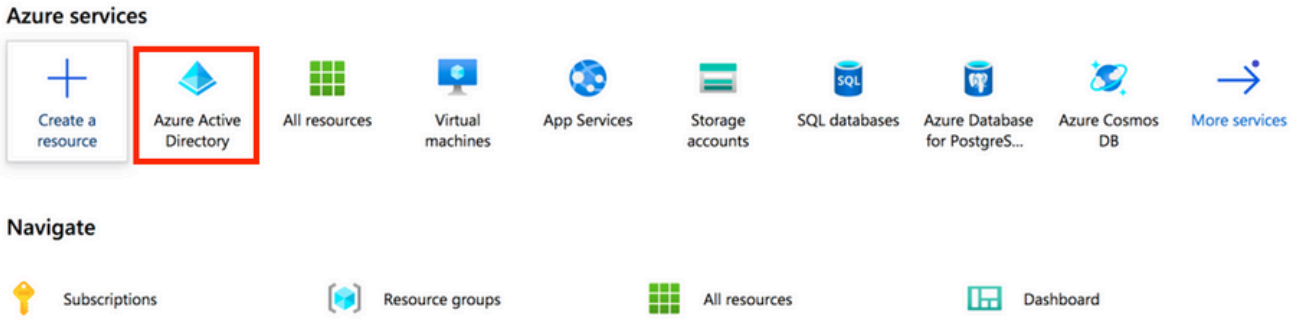
الرسم التخطيطي للشبكة



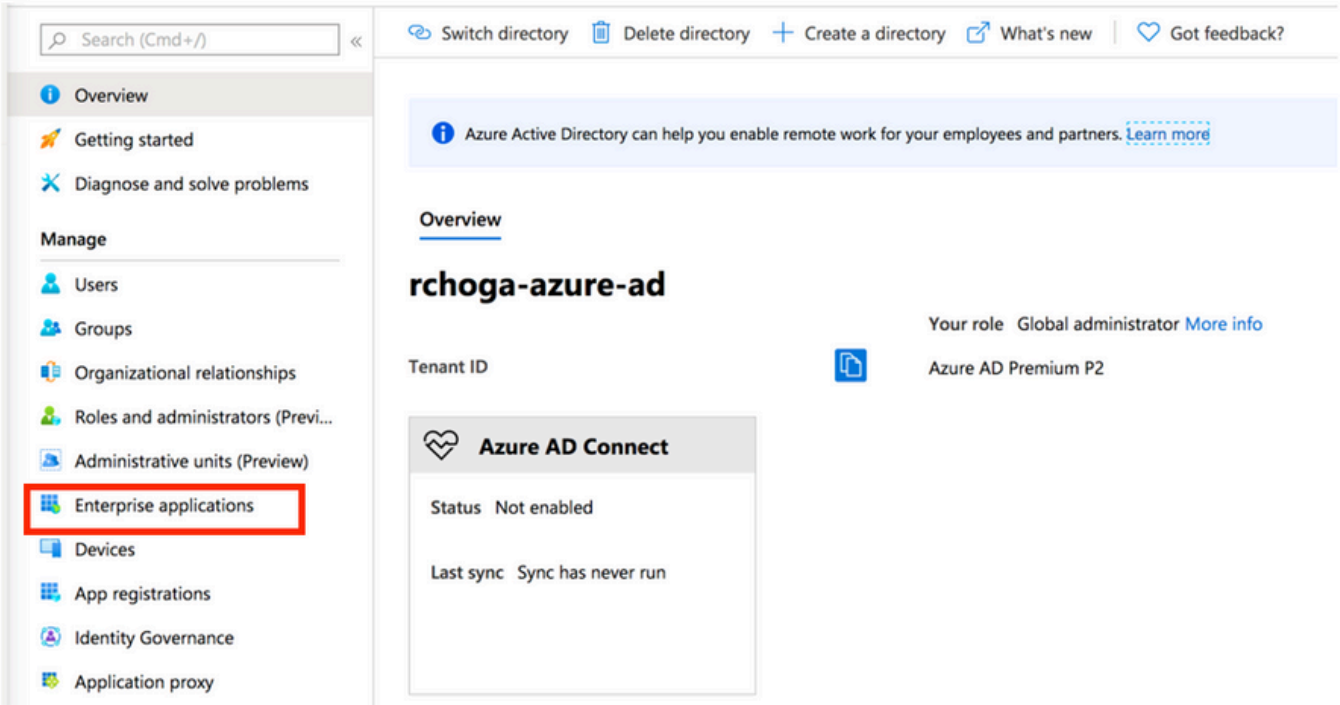
التكوين

إضافة Cisco AnyConnect من معرض تطبيقات Microsoft

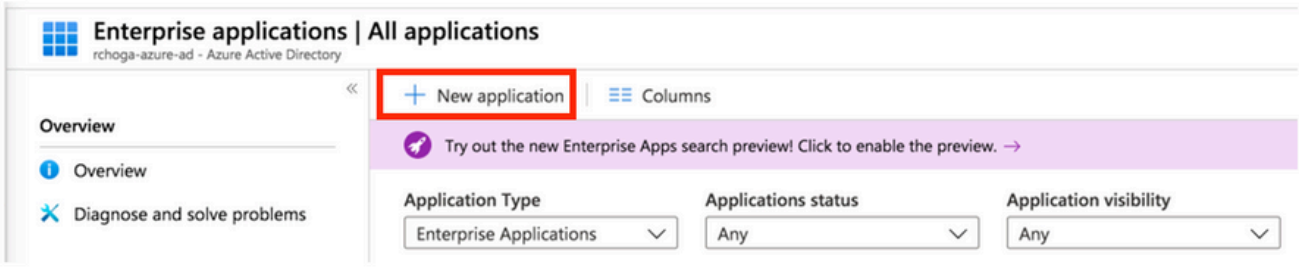
الخطوة 1. سجل الدخول إلى مدخل Azure واختر Azure Active Directory.



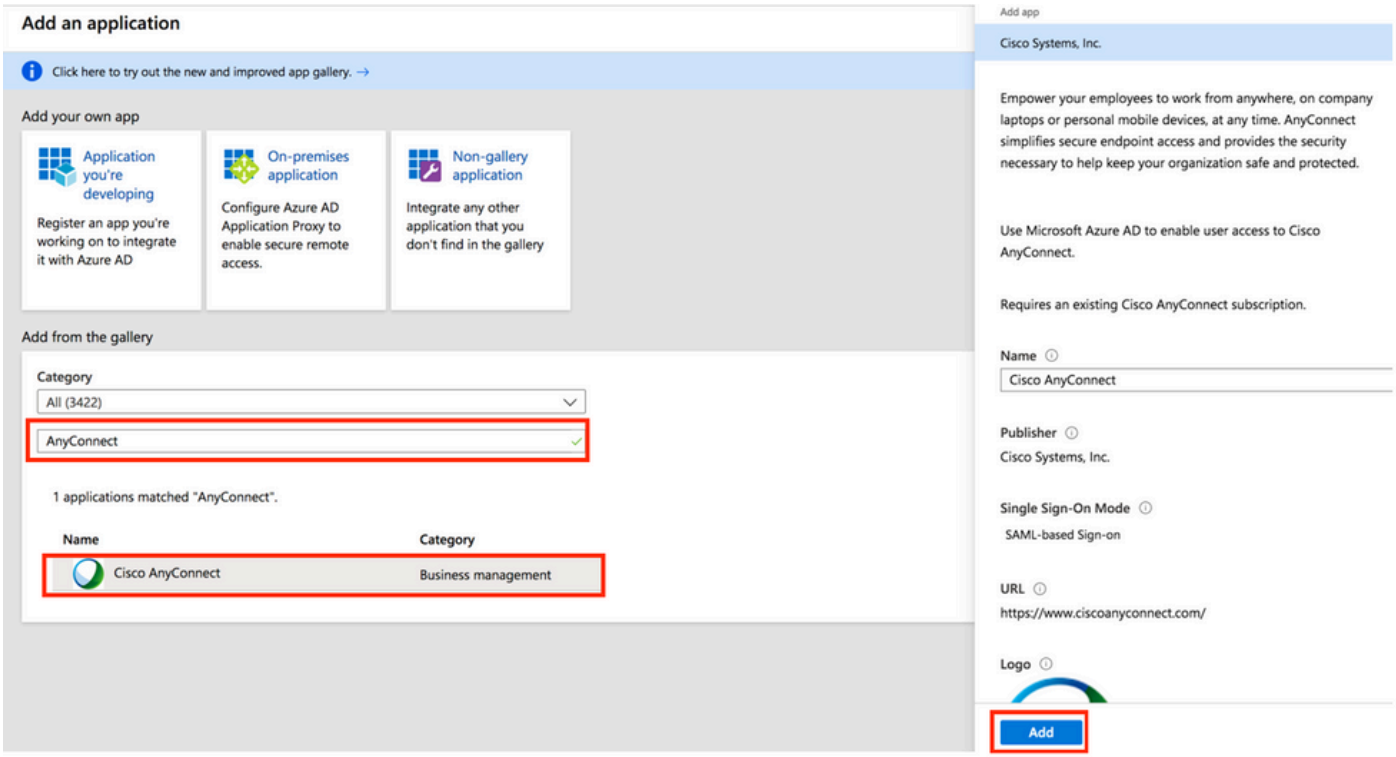
الخطوة 2. كما هو موضح في هذه الصورة، أختر تطبيقات المؤسسات.



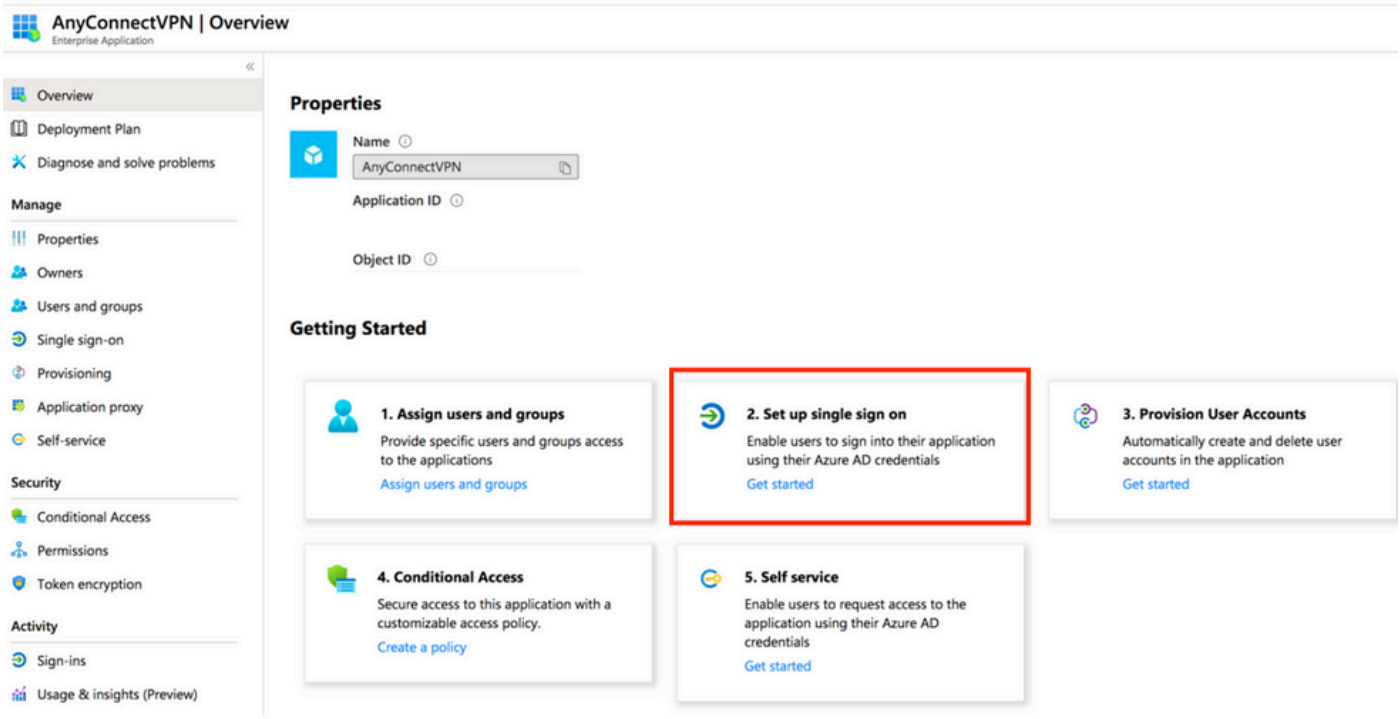
الخطوة 3. الآن، أختر تطبيق جديد، كما هو موضح في هذه الصورة.



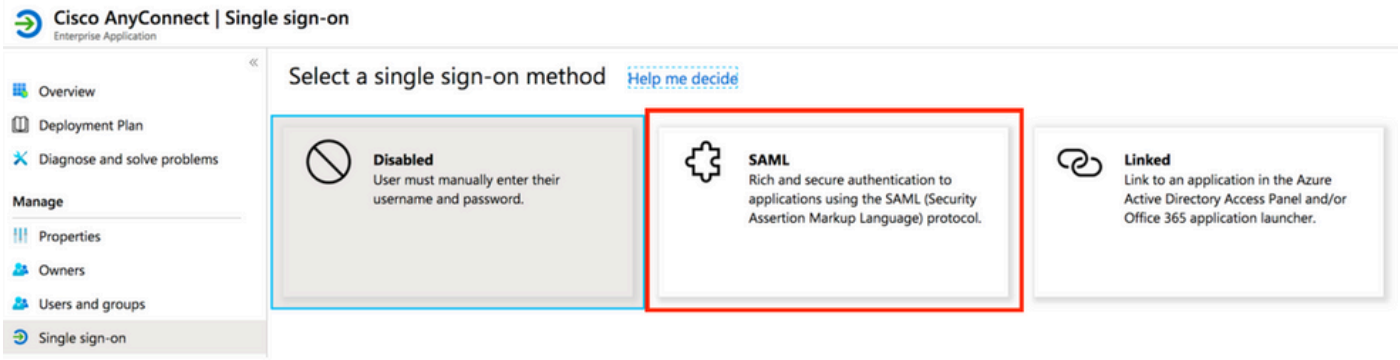
الخطوة 4. في قسم الإضافة من المعرض، اكتب AnyConnect في مربع البحث، واختر Cisco AnyConnect من لوحة النتائج، ثم أضف التطبيق.



الخطوة 5. أختر عنصر قائمة تسجيل الدخول الأحادي، كما هو موضح في هذه الصورة.



الخطوة 6. أختر SAML، كما هو موضح في الصورة.



الخطوة 7. قم بتحرير القسم 1 بهذه التفاصيل.

<#root>

a. Identifier (Entity ID) - https://<VPN URL>/saml/sp/metadata/<TUNNEL-GROUP NAME>

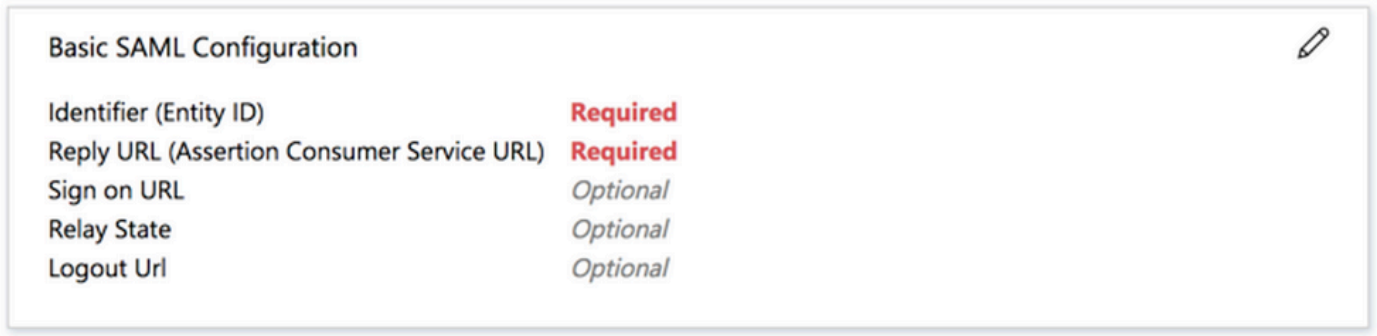
b. Reply URL (Assertion Consumer Service URL) - https://<VPN URL>/+CSCOE+/saml/sp/acs?tgname=<TUNNEL-G

Example: vpn url called

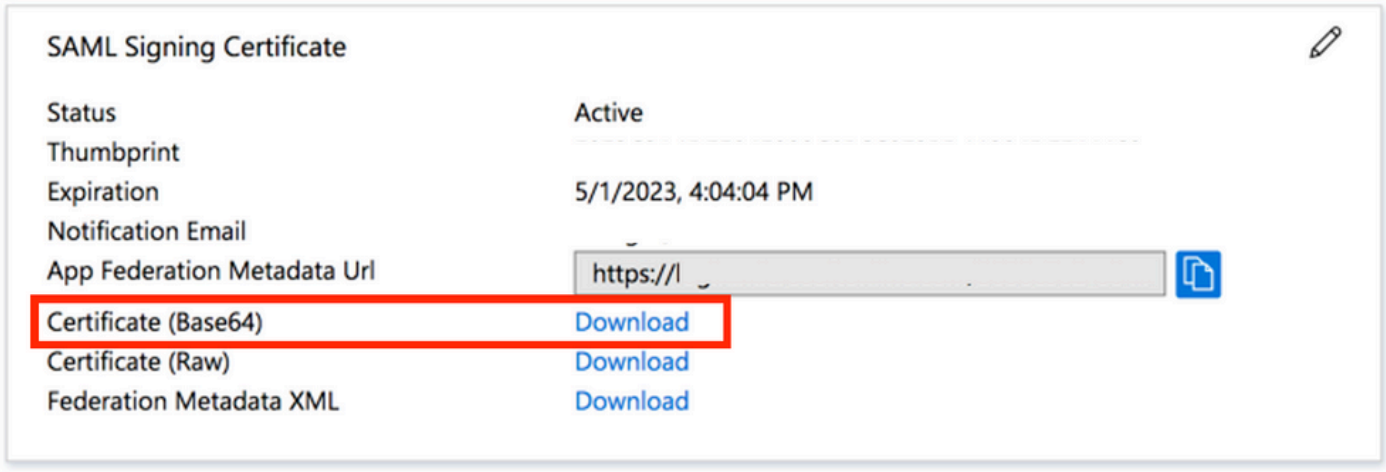
asa.example.com

and tunnel-group called

AnyConnectVPN-1

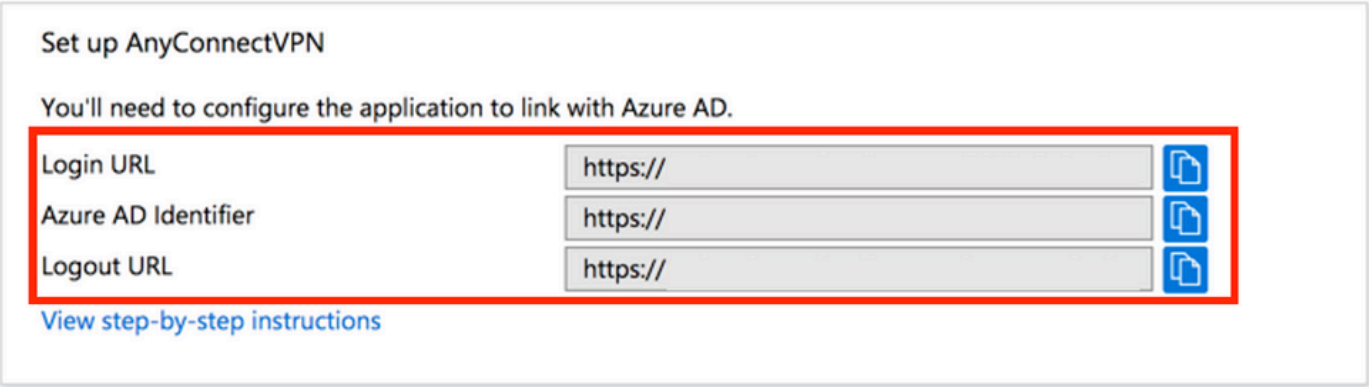


الخطوة 8. في قسم شهادة توقيع SAML، أختر تنزيل لتنزيل ملف الترخيص، وحفظه على حاسبك.



الخطوة 9. هذا مطلوب لتكوين ASA.

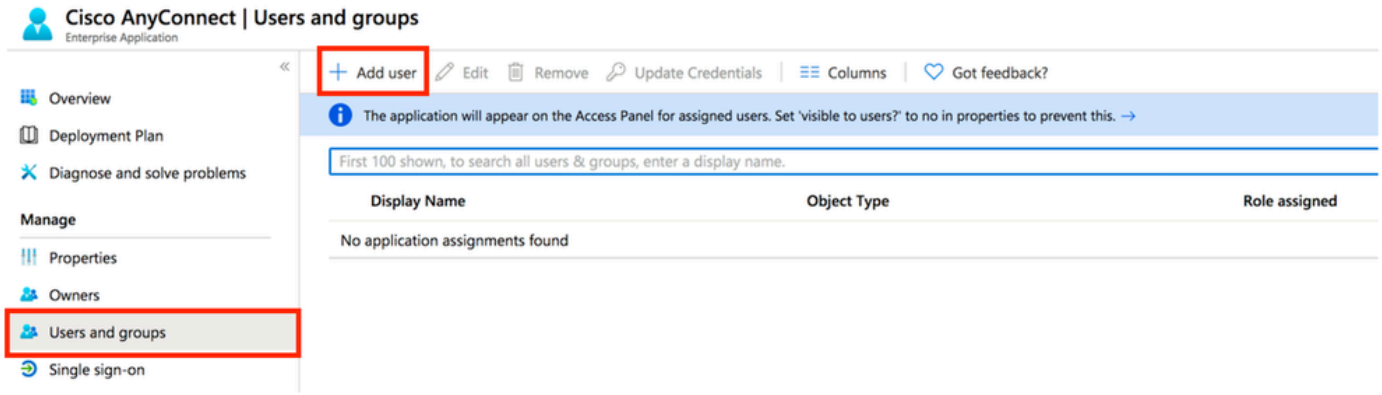
- Azure AD Identifier - هذا هو SAML idp في تكوين VPN الخاص بنا.
- عنوان URL لتسجيل الدخول - هذا هو تسجيل دخول URL.
- عنوان URL لتسجيل الخروج - هذا هو تسجيل خروج URL.



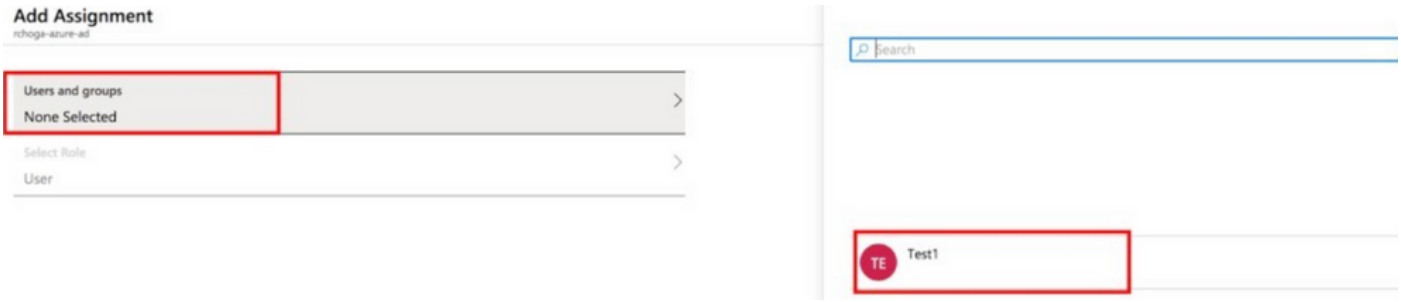
تعيين مستخدم Azure AD للتطبيق

في هذا القسم، يتم تمكين Test1 الاستخدام تسجيل الدخول الأحادي ل Azure، نظرا لأنك تمنح الوصول إلى تطبيق Cisco AnyConnect.

الخطوة 1. في صفحة نظرة عامة على التطبيق، أختر المستخدمون والمجموعات، ثم إضافة مستخدم.



الخطوة 2. أختر مستخدمين ومجموعات في شاشة إضافة مهمة.



الخطوة 3. في شاشة إضافة مهمة، انقر زر تعيين.

تكوين ASA ل SAML عبر CLI

الخطوة 1. قم بإنشاء TrustPoint واستيراد شهادة SAML الخاصة بك.

```
config t

 crypto ca trustpoint AzureAD-AC-SAML
   revocation-check none
```

```
   no id-usage
   enrollment terminal
   no ca-check
 crypto ca authenticate AzureAD-AC-SAML
 -----BEGIN CERTIFICATE-----
 …
 PEM Certificate Text you downloaded goes here
 …
 -----END CERTIFICATE-----
 quit
```

الخطوة 2. توفر هذه الأوامر تعريف SAML الخاص بك.

```
webvpn

 saml idp https://xxx.windows.net/xxxxxxxxxxxx/ - [Azure AD Identifier]
 url sign-in https://login.microsoftonline.com/xxxxxxxxxxxxxxxxxxxxxx/saml2 - [Login URL]
 url sign-out https://login.microsoftonline.com/common/wsfederation?wa=wsignout1.0 – Logout URL
 trustpoint idp AzureAD-AC-SAML - [IdP Trustpoint]
 trustpoint sp ASA-EXTERNAL-CERT - [SP Trustpoint]
 no force re-authentication
 no signature
 base-url https://asa.example.com
```

الخطوة 3. تطبيق مصادقة SAML على تكوين نفق VPN.

```
tunnel-group AnyConnectVPN-1 webvpn-attributes
  saml identity-provider https://xxx.windows.net/xxxxxxxxxxxx/
  authentication saml
end

write memory
```

ملاحظة: إذا قمت بإجراء تغييرات على تكوين IdP، فأنت بحاجة إلى إزالة تكوين موفر هوية saml من مجموعة النفق، وإعادة تطبيقه لكي تصبح التغييرات فعالة.

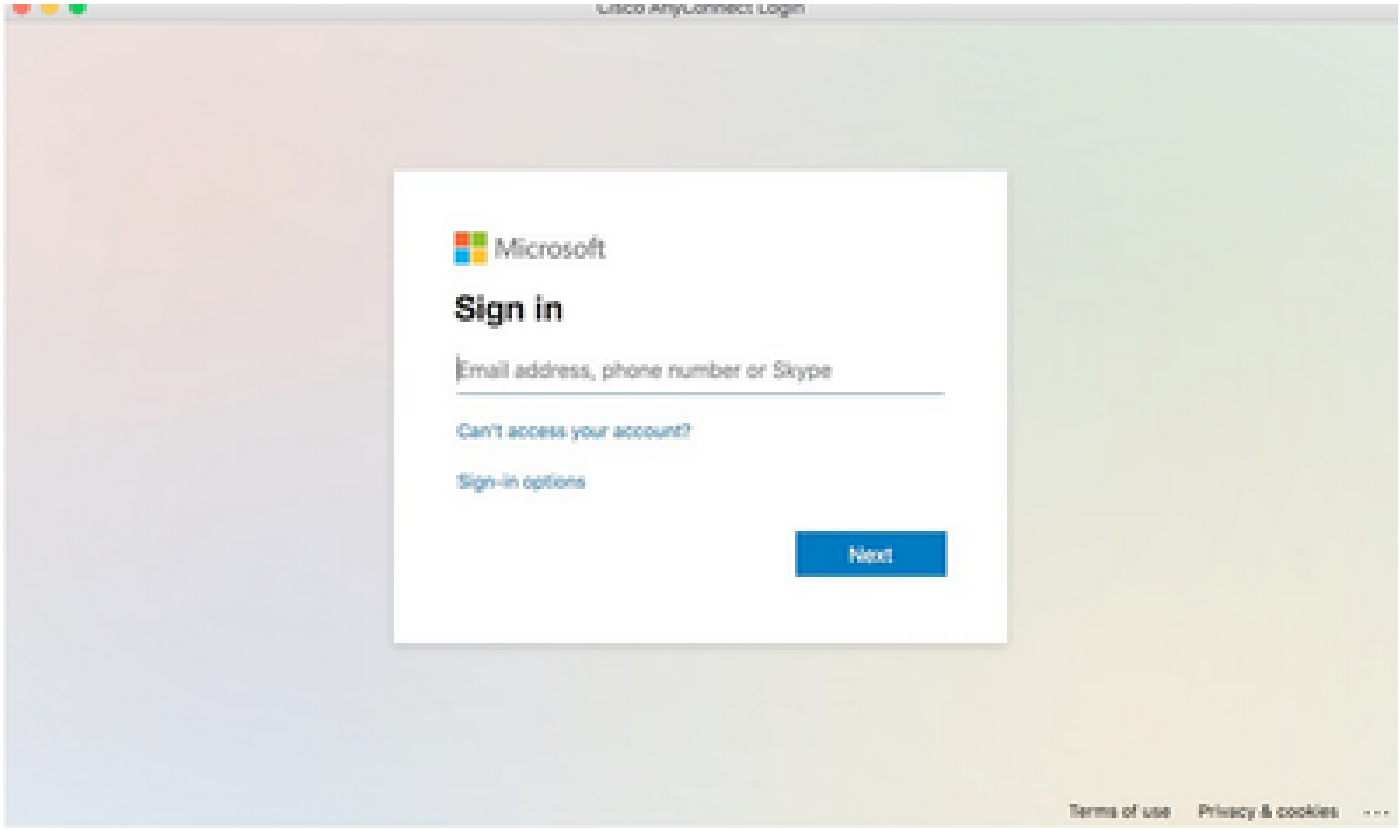
التحقق من الصحة

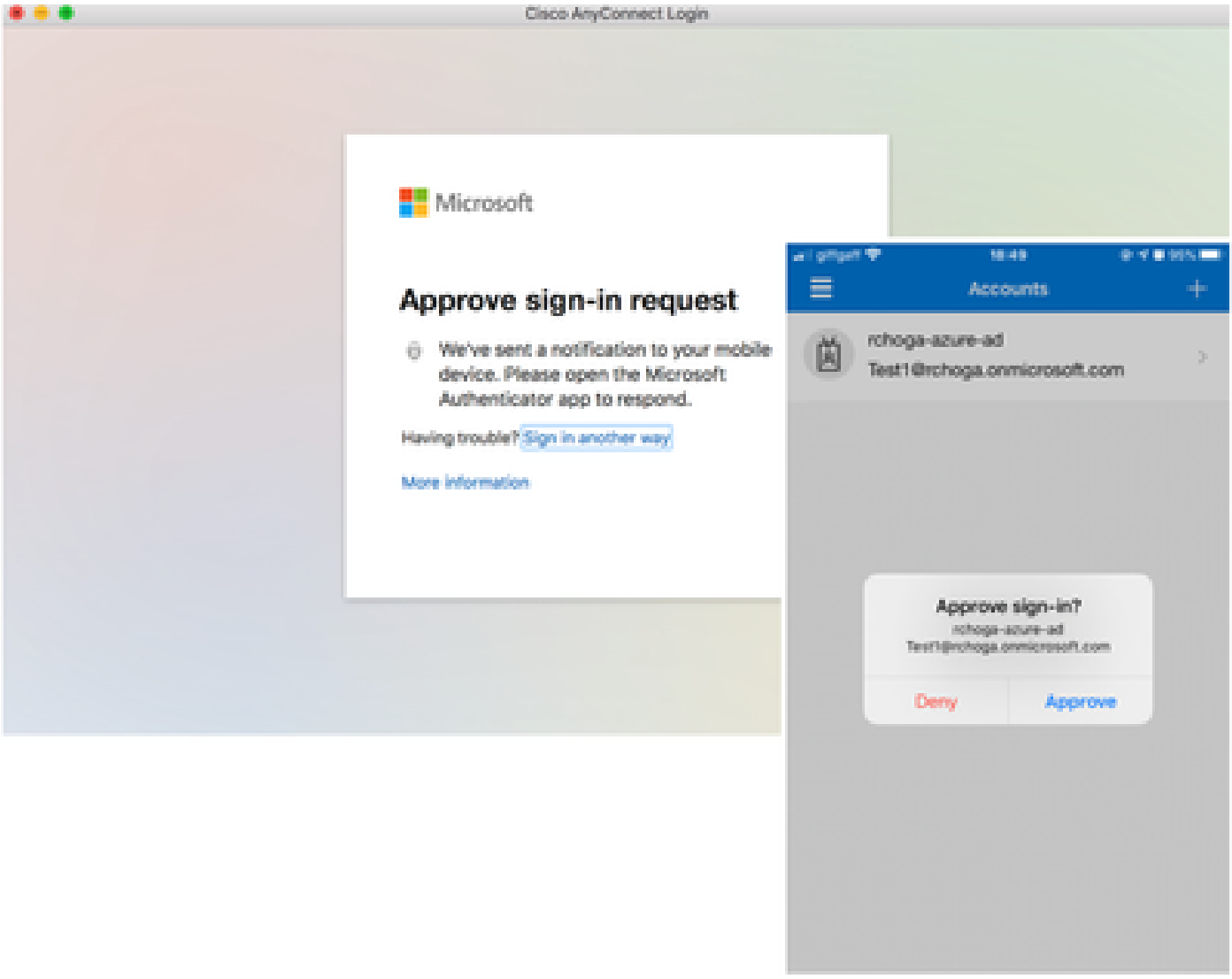
إختبار AnyConnect باستخدام مصادقة SAML

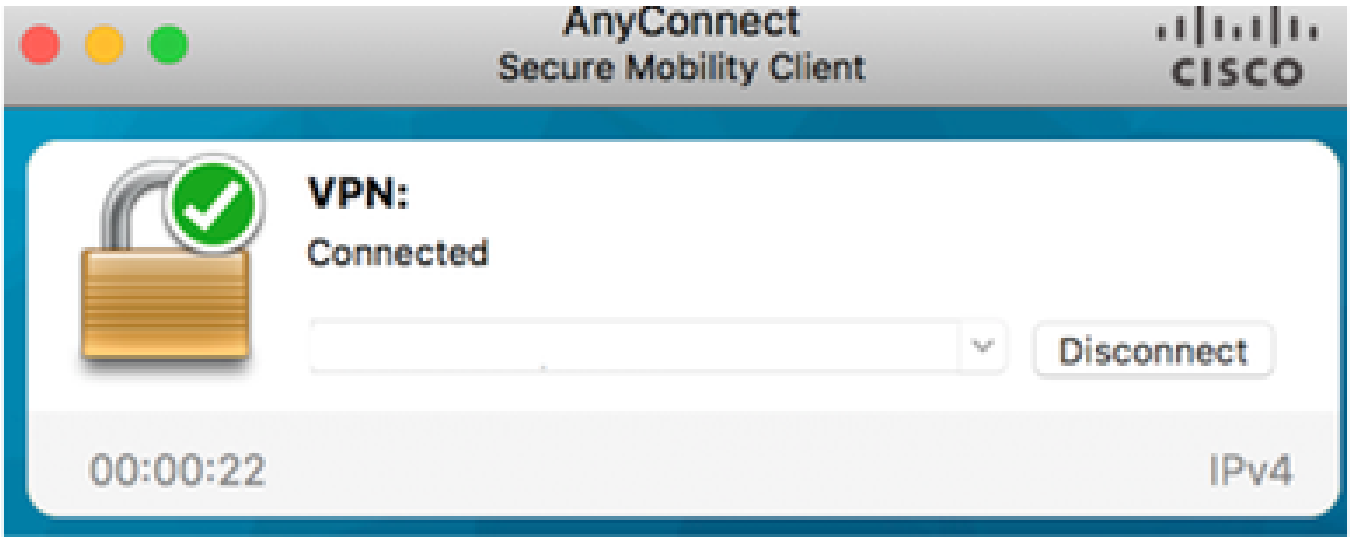
الخطوة 1. اتصل بعنوان URL الخاص بالشبكة الخاصة الظاهرية (VPN) وأدخل تفاصيل Azure AD.

الخطوة 2. الموافقة على طلب تسجيل الدخول.

الخطوة 3. يتم توصيل AnyConnect.







المشكلات الشائعة

معرف الكيان غير متطابق

مثال تصحيح الأخطاء:

[SAML] consumption_confirmation: معرف المورد غير معروف #LassoServer. لتسجيل مورد في #LassoServer، يجب إستخدام الأسلوب lasso_server_add_provider() أو lasso_server_add_provider_from_buffer().

المشكلة: بشكل عام، تعني أن الأمر saml idp [entityID] المضمن تكوين WebVPN الخاص ب ASA لا يتطابق مع معرف كيان IdP الذي تم العثور عليه في بيانات تعريف IdP'.

الحل: تحقق من معرف الكيان الخاص بملف بيانات تعريف IdP وقم بتغيير الأمر saml idp [entity id] ليطابق هذا الأمر.

عدم تطابق الوقت

مثال تصحيح الأخطاء:

[SAML] ليست قبل:2017-09-05T23:59:01.896z NotOnOrAfter:2017-09-06T00:59:01.896Z المدة: 0

[SAML] Consumption_Confirmation: التأكيد منتهي الصلاحية أو غير صالح

المشكلة 1. لم تتم مزامنة وقت ASA مع وقت IdP.

الحل 1. قم بتكوين ASA باستخدام خادم NTP نفسه المستخدم من قبل IdP.

المشكلة 2. التأكيد غير صالح بين الوقت المحدد.

الحل 2. قم بتعديل قيمة المدة التي تم تكوينها على ASA.

تم إستخدام شهادة توقيع IDp غير صحيحة

مثال تصحيح الأخطاء:

[Lasso] func=xmlSecOpenSSLEvpSignatureVerify:file=signatures.c:line=493:obj=rsa-sha1:subj=EVP_VerifyFinal:error=18:data تطابق ال:signature تطابق ال

[SAML] Consumption_Confirmation: لا يمكن للملف التعريفي التحقق من توقيع على الرسالة

مشكلة: تعذر على ASA التحقق من الرسالة الموقعة من قبل IdP أو لا يوجد توقيع ل ASA للتحقق.

الحل: تحقق من شهادة توقيع IdP المثبتة على ASA للتأكد من مطابقتها لما يتم إرساله بواسطة IdP. إذا تم تأكيد ذلك، فتأكد من تضمين التوقيع في إستجابة SAML.

جمهور التأكيد غير صالح

مثال تصحيح الأخطاء:

[SAML] Consumption_Confirmation: تأكيد الجمهور غير صالح

المشكلة: يعرف IdP الجمهور غير الصحيح.

الحل: تصحيح تكوين الجمهور على IDp. يجب أن تطابق معرف كيان ASA.

عنوان URL خاطئ لتأكيد خدمة المستهلك

مثال تصحيح الأخطاء: يتعذر تلقي أي تصحيح أخطاء بعد إرسال طلب المصادقة الأولي. يمكن للمستخدم إدخال بيانات الاعتماد في IdP ولكن IdP ال يعيد التوجيه إلى ASA.

المشكلة: تم تكوين IdP لعنوان URL غير صحيح ل Confirmation Consumer Service.

الحل (الحلول): تحقق من URL الأساسي في التكوين وتأكد من صحته. تحقق من بيانات تعريف ASA مع إظهار للتأكد من صحة URL خدمة المستهلك للتأكيد. الاختبار هو، تصفح إلى ASA، فحص ال idP أن ال url صحيح. هو، إن يكون الكل صحيح على ال ASA.

تغييرات تكوين SAML التي لا تدخل حيز التنفيذ

مثال: بعد تعديل أو تغيير عنوان URL أحادي لتسجيل الدخول، شهادة SP، ال يزال SAML ال يعمل ويرسل التكوينات السابقة.

المشكلة: يحتاج ASA إلى إعادة إنشاء بيانات التعريف الخاصة به عندما يكون هناك تغيير في التكوين يؤثر عليه. وهو ال يفعل ذلك تلقائيا.

الحل: بعد إجراء التغييرات، تحت أمر إزالة SAML idp [entity-id] المنطبق على مجموعة النفق المتأثرة وإعادة تطبيقه.

استكشاف الأخطاء وإصلاحها

تتضمن معظم أدوات أستكشاف أخطاء SAML وإصلاحها تكوين غير صحيح يمكن العثور عليه عند التحقق من تكوين SAML، أو تشغيل تصحيح الأخطاء. يمكن إستخدام debug webVPN saml 255 ال في السيناريوهات التي ال، ومع ذلك، يمكن أستكشاف أخطاء معظم المشاكل وإصلاحها. هذا مع علومات مفيدة، يمكن تشغيل مزيد من أدوات تصحيح الأخطاء في وقت تصحيح الأخطاء:

```
debug webvpn saml 255
debug webvpn 255
debug webvpn session 255
debug webvpn request 255
```

معلومات ذات صلة

- تسجيل دخول أحادي SAML للتطبيقات المحلية باستخدام وكيل التطبيق

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).