التحكم في الوصول المستند إلى دور ISE باستخدام LDAP

المحتويات

المقدمة

يصف هذا المستند مثال للتكوين باستخدام بروتوكول الوصول إلى الدليل (LDAP) في الوضع Lightweight كمخزن هوية خارجي للوصول الإداري إلى واجهة المستخدم الرسومية (GUI) لإدارة محرك خدمات الهوية من Cisco.

المتطلبات الأساسية

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- تكوين Cisco ISE، الإصدار 3.0
- LDAP (البروتوكول الخفيف للوصول للدليل)

المتطلبات

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

- ISE الإصدار 3.0 من Cisco
- نظام التشغيل Windows Server 2016

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة.

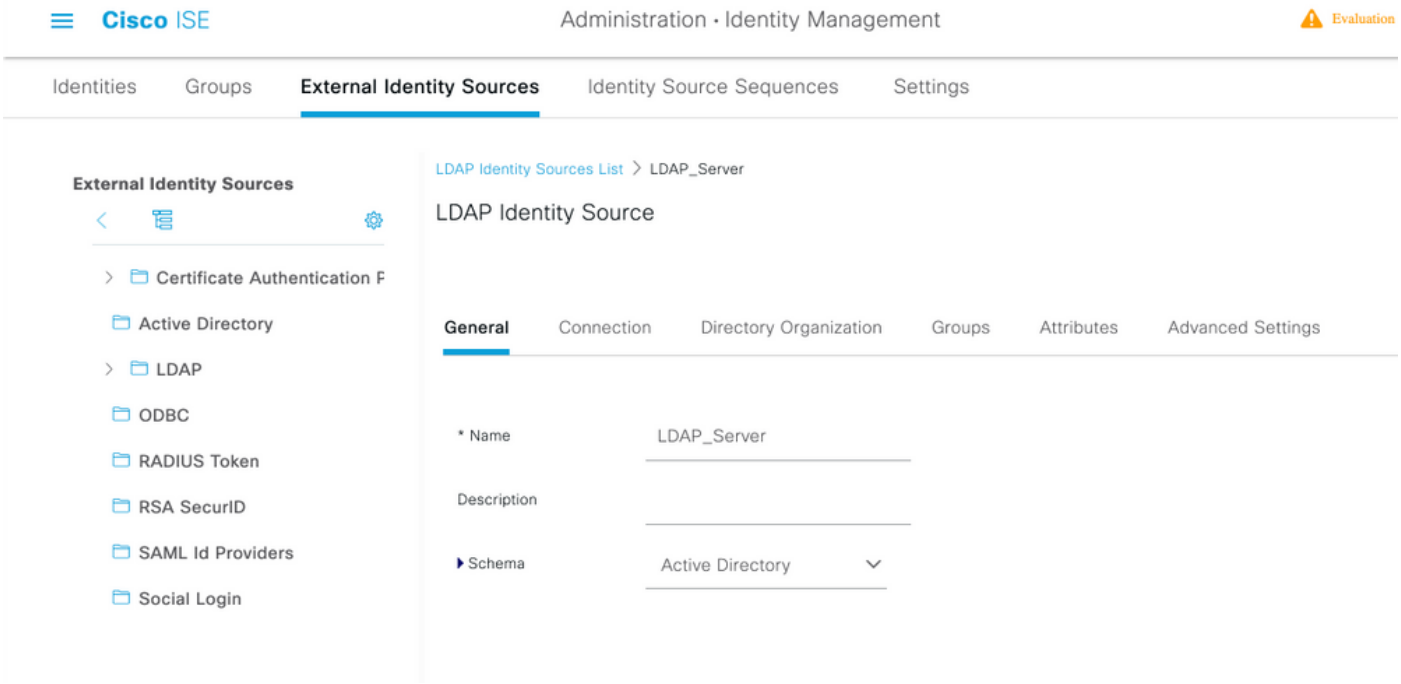
بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

التكوينات

أستخدم القسم التالي لتكوين مستخدم يستند إلى LDAP للحصول على الوصول الإداري / المستند إلى مخصص إلى واجهة المستخدم الرسومية (GUI) الخاصة ب ISE . يستخدم التكوين التالي استعلامات بروتوكول LDAP لجلب المستخدم من Active Directory لتنفيذ المصادقة.

انضمام ISE إلى LDAP

1. انتقل إلى **إدارة > إدارة الهوية > مصادر الهوية الخارجية > Active Directory > LDAP.**
2. تحت علامة التبويب **عام**، أدخل اسم LDAP واختر المخطط Active Directory.



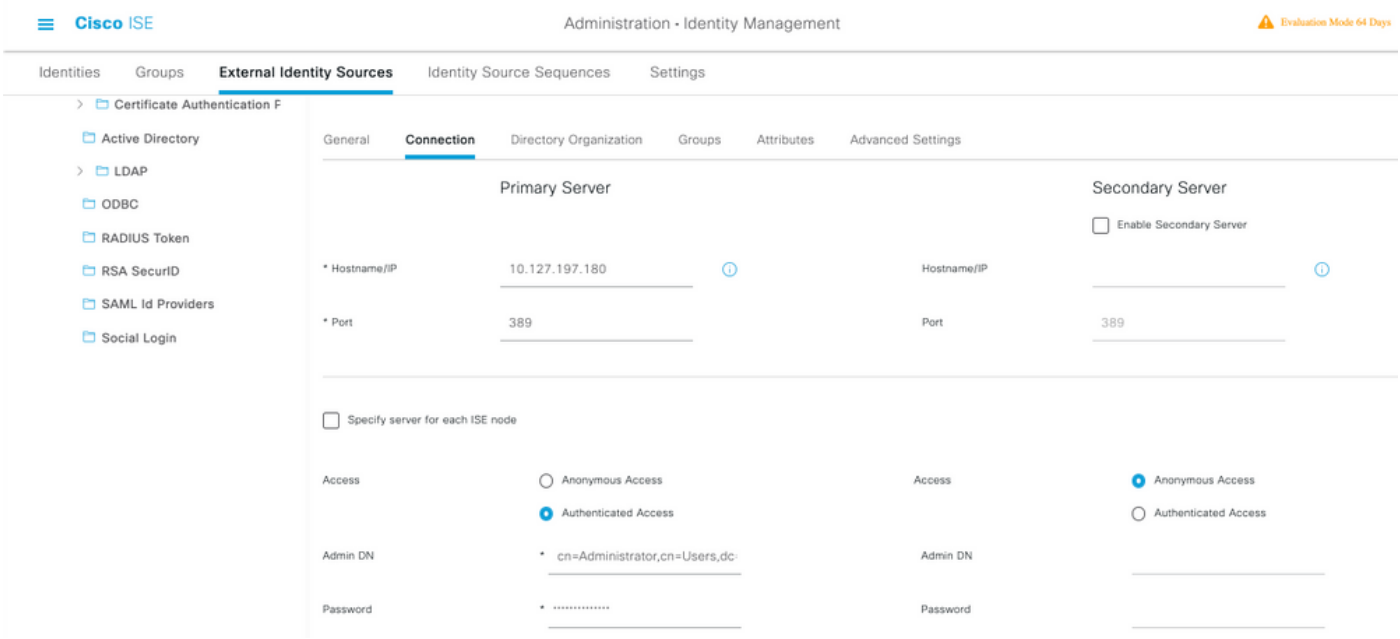
تكوين نوع الاتصال وتكوين LDAP

1. انتقل إلى **ISE > إدارة > إدارة الهوية > مصادر الهوية الخارجية > LDAP.**

2. قم بتكوين اسم المضيف لخادم LDAP الأساسي مع المنفذ 389(LDAP)/636 (LDAP-Secure) .

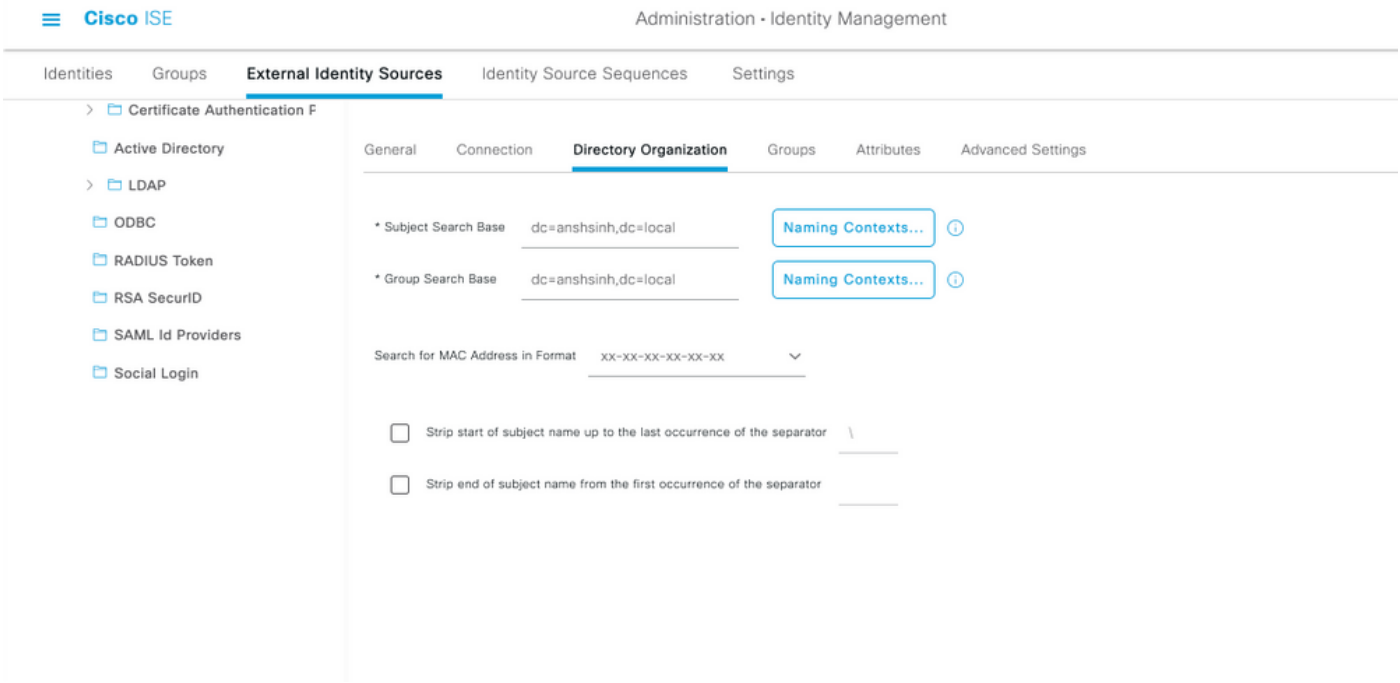
3. أدخل مسار الاسم المميز للمسؤول (DN) باستخدام كلمة مرور المسؤول لخادم LDAP .

4. انقر فوق Test Bind Server لاختبار إمكانية الوصول إلى خادم LDAP من ISE .



تكوين مؤسسة الدليل والمجموعات والسمات

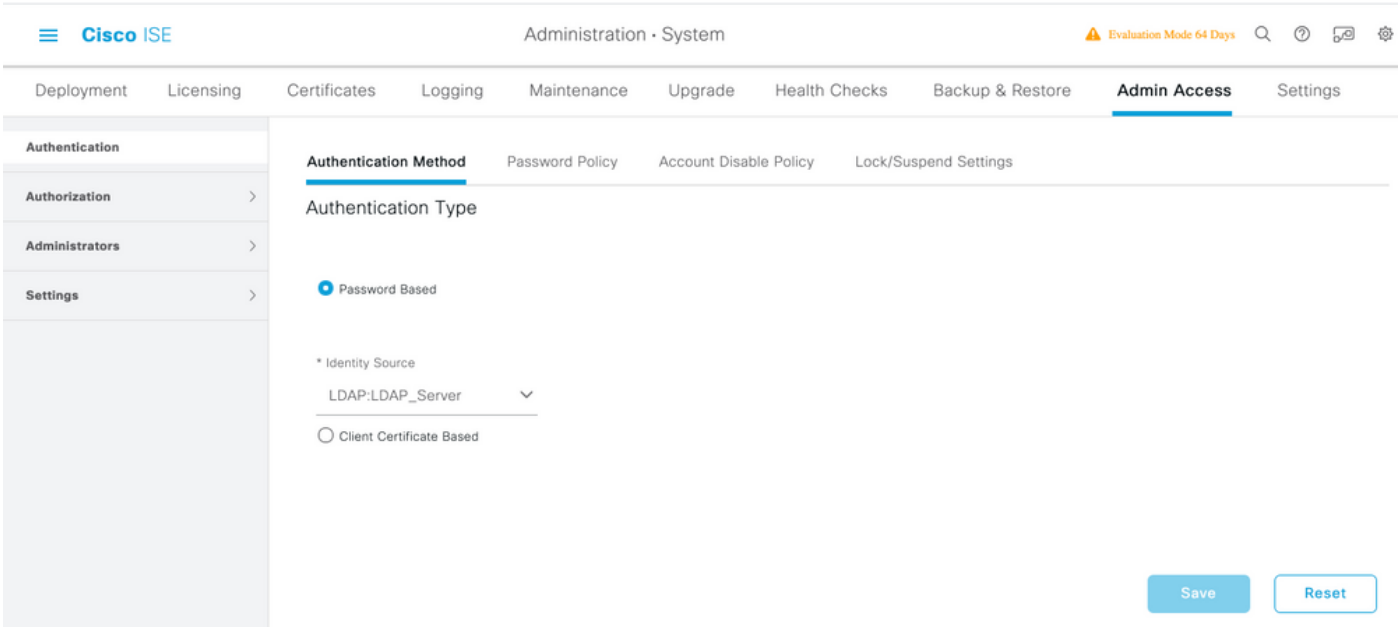
1. أختر مجموعة المؤسسات الصحيحة للمستخدم استنادا إلى التسلسل الهيكلي للمستخدمين المخزنين في خادم LDAP .



تمكين الوصول الإداري لمستخدمي LDAP

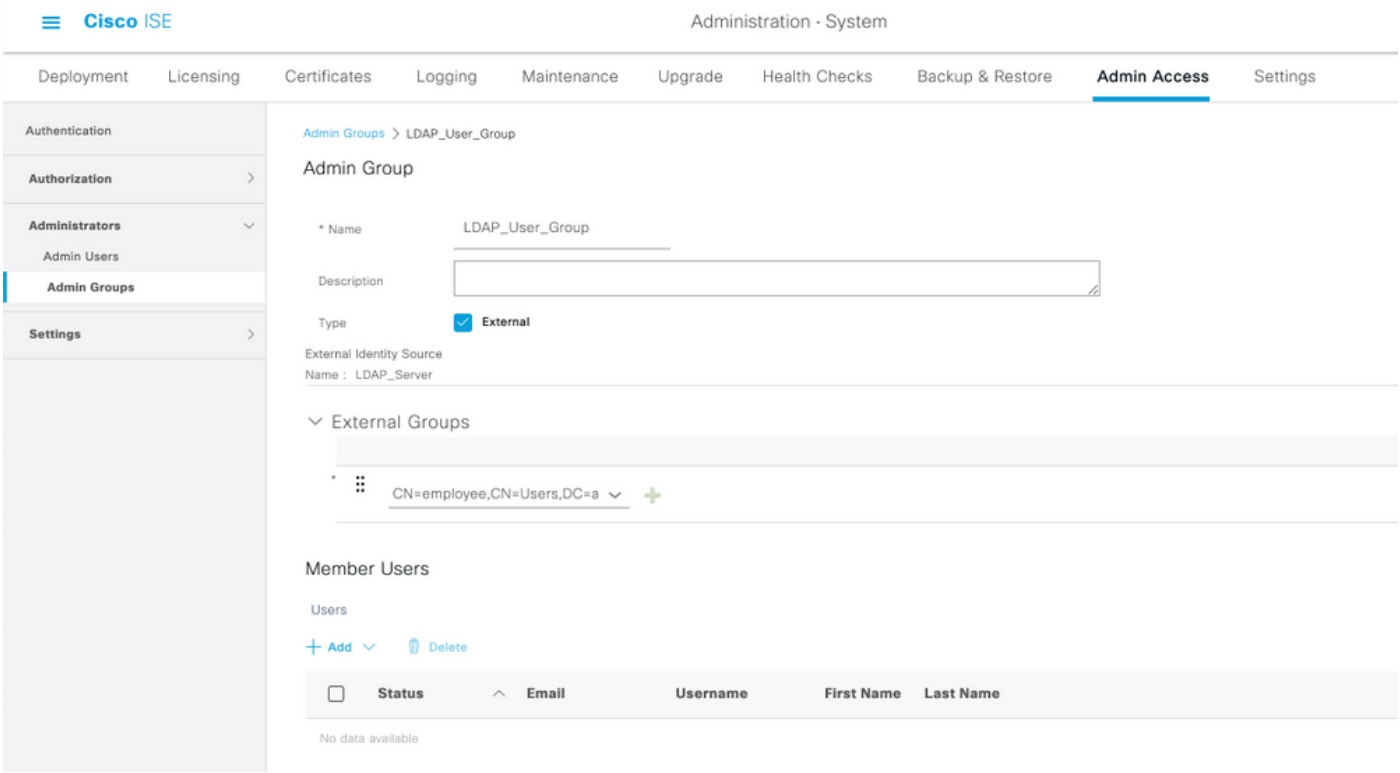
أكمل هذه الخطوات لتمكين المصادقة المستندة إلى كلمة المرور.

1. انتقل إلى **ISE > الإدارة > النظام > الوصول إلى المسؤول > المصادقة**.
2. تحت علامة التبويب **أسلوب المصادقة**، حدد الخيار **المستند إلى كلمة المرور**.
3. حدد **LDAP** من القائمة المنسدلة **مصدر الهوية**.
4. انقر فوق **حفظ التغييرات**.



تعيين مجموعة الإدارة إلى مجموعة LDAP

قم بتكوين مجموعة الإدارة على ISE وقم بتعيينها إلى مجموعة AD. وهذا يسمح للمستخدم الذي تم تكوينه بالوصول بناء على سياسات التخويل بناء على أذونات RBAC التي تم تكوينها للمسؤول استنادا إلى عضوية المجموعة.

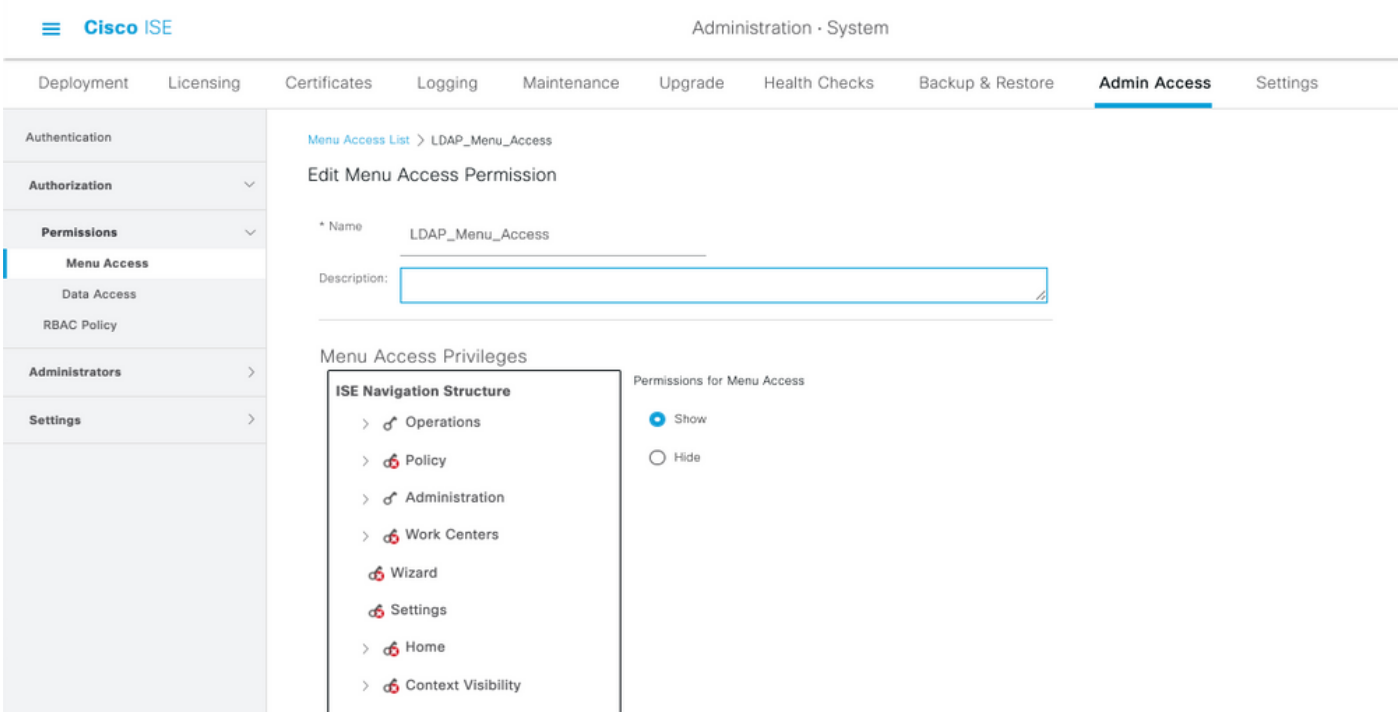


تعيين أذونات للوصول إلى القائمة

1. انتقل إلى **ISE > الإدارة > النظام > التخويل > الأذونات > الوصول إلى القائمة**

2. قم بتحديد وصول القائمة للمستخدم المسؤول للوصول إلى واجهة المستخدم الرسومية (GUI) ل ISE. يمكنك تكوين الكيانات الفرعية ليتم عرضها أو إخفاءها على واجهة المستخدم الرسومية (GUI) للوصول المخصص للمستخدم لإجراء مجموعة من العمليات فقط إذا لزم الأمر.

3. انقر فوق **حفظ**.

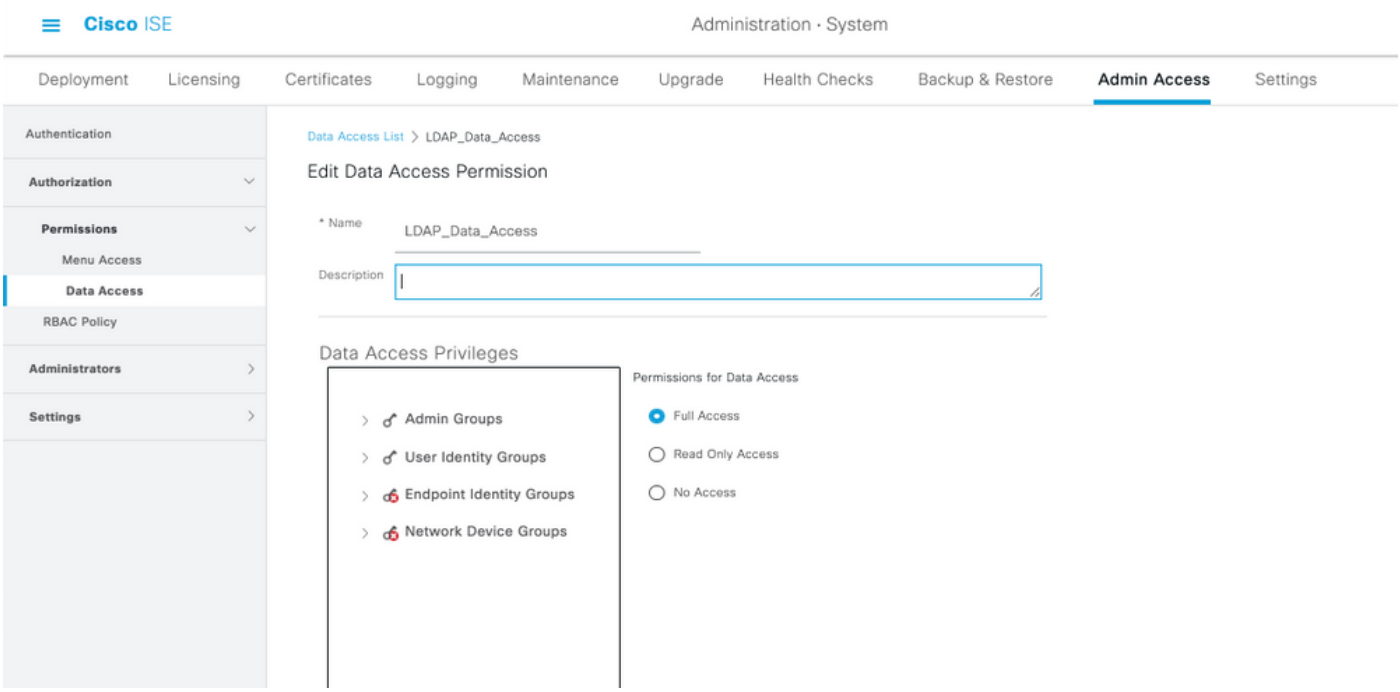


تعيين أذونات للوصول إلى البيانات

1. انتقل إلى **ISE > الإدارة > النظام > التخويل > الأذونات > الوصول إلى البيانات**

2. تحديد الوصول إلى البيانات لمستخدم المسؤول للحصول على وصول كامل أو وصول للقراءة فقط إلى مجموعات الهوية على واجهة المستخدم الرسومية (GUI) الخاصة ب ISE.

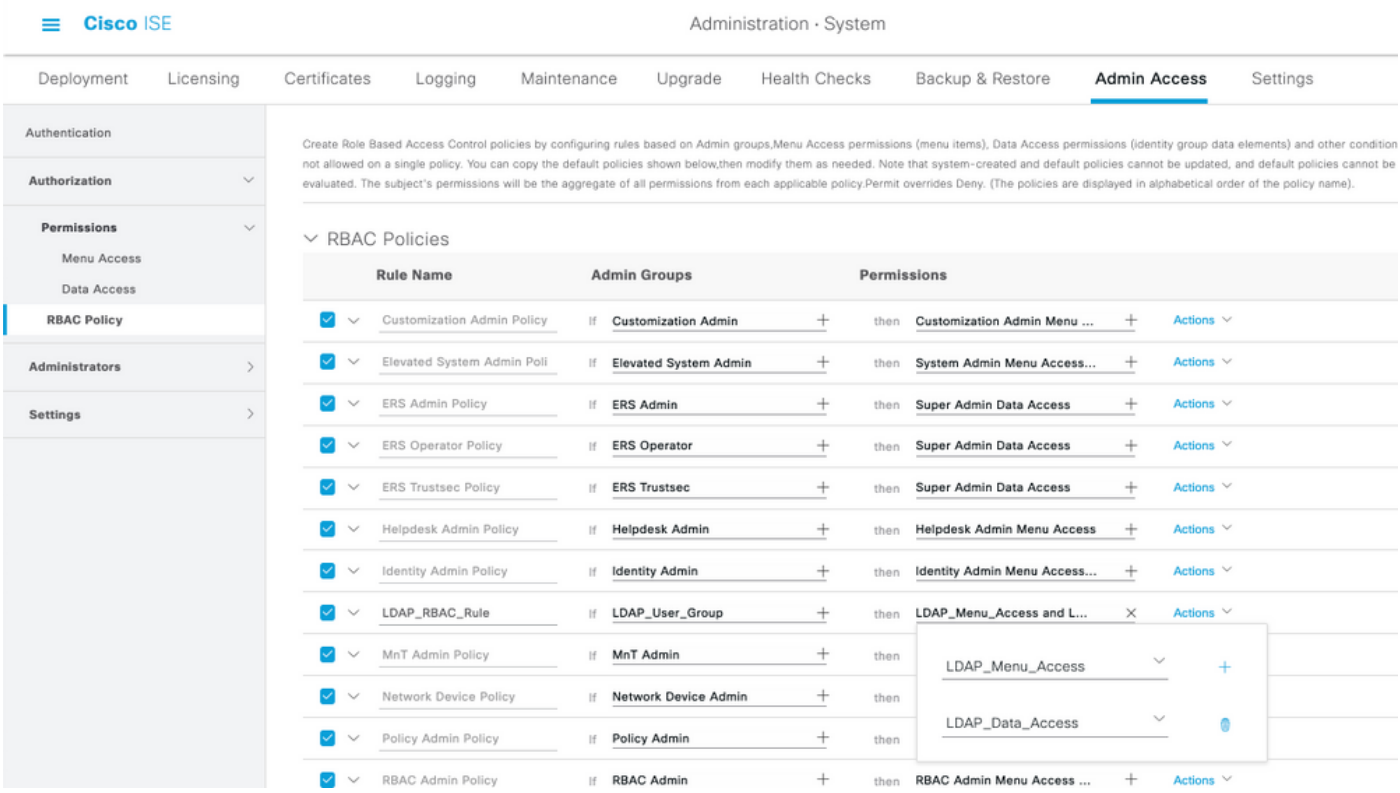
3. انقر فوق **حفظ**.



تعيين أذونات RBAC لمجموعة الإدارة

1. انتقل إلى **ISE > الإدارة > النظام > وصول المسؤول > التفويض > السياسة**.

2. من القائمة المنسدلة **إجراءات** على اليمين، حدد **إدراج نهج جديد أدناه** لإضافة نهج جديد.
3. قم بإنشاء قاعدة جديدة تسمى LDAP_RBAC_POLICY وقم بتخطيطها مع مجموعة الإدارة المعرفة في قسم تمكين الوصول الإداري لـ AD، وقم بتعيين أذونات لها للوصول إلى القائمة والوصول إلى البيانات.
4. انقر فوق **حفظ التغييرات**، ويتم عرض تأكيد التغييرات المحفوظة في الزاوية السفلى اليمنى من واجهة المستخدم الرسومية.

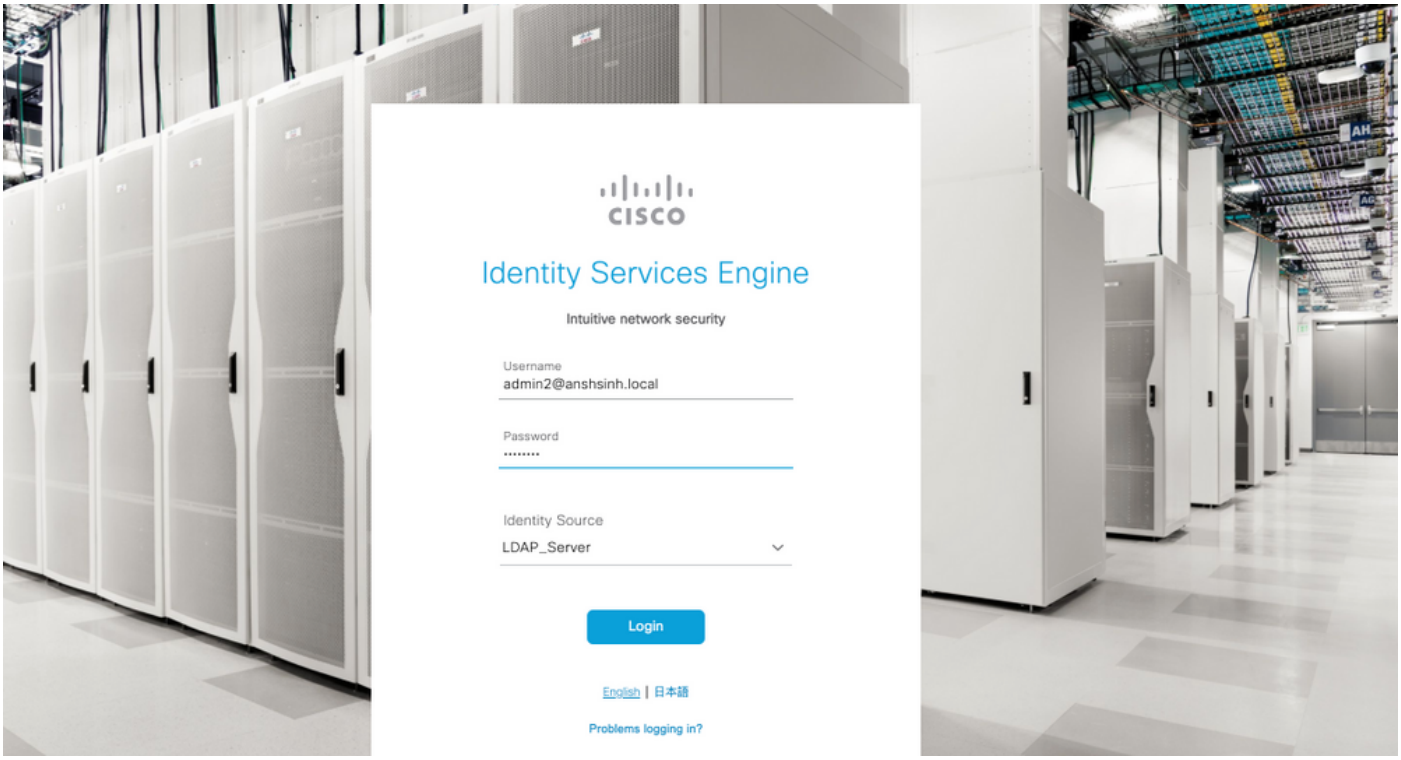


التحقق من الصحة

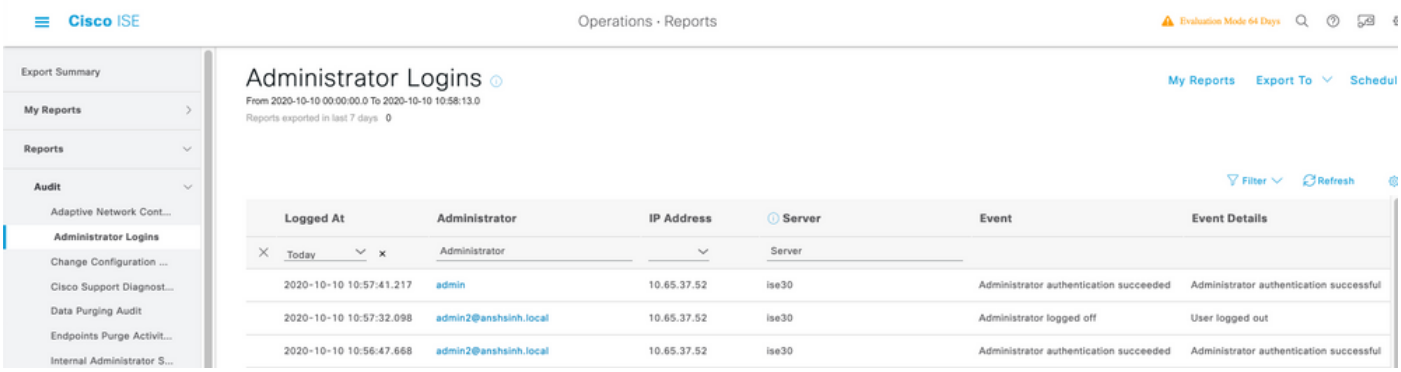
الوصول إلى ISE باستخدام بيانات اعتماد AD

أكمل الخطوات التالية للوصول إلى ISE باستخدام مسوغات AD:

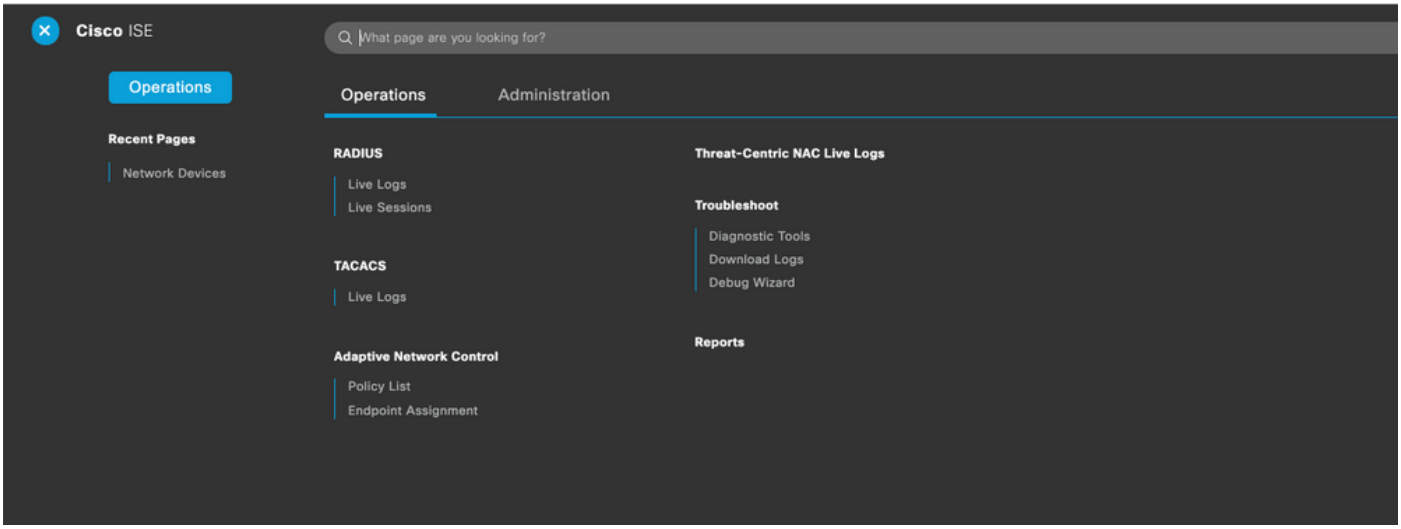
1. افتح واجهة المستخدم الرسومية (GUI) ISE لتسجيل الدخول باستخدام مستخدم LDAP.
2. حدد LDAP_Server من القائمة المنسدلة **مصدر الهوية**.
3. أدخل اسم المستخدم وكلمة المرور من قاعدة بيانات LDAP، وسجل الدخول.



تحقق من تسجيل الدخول للمسؤول في تقارير التدقيق. انتقل إلى **ISE > العمليات > التقارير > التدقيق > عمليات تسجيل دخول المسؤولين.**



للتأكد من أن هذا التكوين يعمل بشكل صحيح، تحقق من اسم المستخدم الذي تمت مصادقته في الزاوية العليا اليمنى من واجهة المستخدم الرسومية (ISE). قم بتحديد وصول مخصص يستند إلى إمكانية وصول محدودة إلى القائمة كما هو موضح هنا:



استكشاف الأخطاء وإصلاحها

معلومات عامة

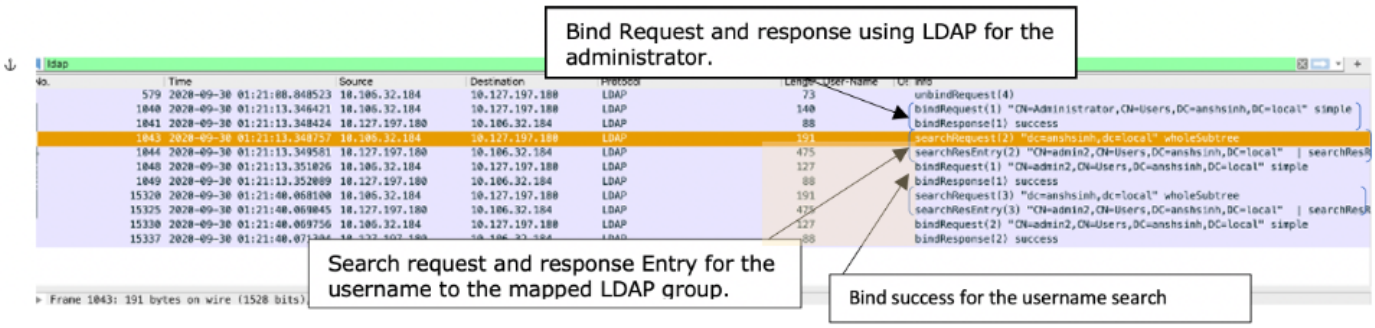
لاستكشاف أخطاء عملية RBAC وإصلاحها، يجب تمكين مكونات ISE هذه في تصحيح الأخطاء على عقدة مسؤول ISE :

RBAC - سيقوم هذا بطباعة الرسالة ذات الصلة RBAC عند محاولة تسجيل الدخول (ise-psc.log)

الوصول-filter - سيقوم هذا بطباعة الوصول إلى عامل تصفية الموارد (ise-psc.log)

Runtime-AAA - سيقوم هذا بطباعة السجلات الخاصة بتسجيل الدخول ورسائل تفاعل LDAP (prrt-server.log)

تحليل التقاط الحزمة



تحليل السجل

التحقق من صحة prrt-server.log

```
PAPAuthenticator,2020-10-10
08:54:00,621,DEBUG,0x7f852bee3700,cntx=0002480105,sesn=ise30/389444264/3178,CPMSessionID=ise30:u
serauth286,user=admin2@anshsinh.local,validateEvent: Username is [admin2@anshsinh.local]
bIsMachine is [0] isUtf8Valid is [1],PAPAuthenticator.cpp:86 IdentitySequence,2020-10-10
08:54:00,627,DEBUG,0x7f852c4e9700,cntx=0002480105,sesn=ise30/389444264/3178,CPMSessionID=ise30:u
serauth286,user=admin2@anshsinh.local,******* Authen
IDStoreName:LDAP_Server,IdentitySequenceWorkflow.cpp:377 LDAPIDStore,2020-10-10
08:54:00,628,DEBUG,0x7f852c4e9700,cntx=0002480105,sesn=ise30/389444264/3178,CPMSessionID=ise30:u
serauth286,user=admin2@anshsinh.local,Send event to LDAP_Server_924OqzxSbv_199_Primary
server,LDAPIDStore.h:205 Server,2020-10-10
08:54:00,634,DEBUG,0x7f85293b8700,cntx=0002480105,sesn=ise30/389444264/3178,CPMSessionID=ise30:u
serauth286,user=admin2@anshsinh.local,LdapServer::onAcquireConnectionResponse: succeeded to
acquire connection,LdapServer.cpp:724 Connection,2020-10-10
08:54:00,634,DEBUG,0x7f85293b8700,LdapConnectionContext::sendSearchRequest(id = 1221): base =
dc=anshsinh,dc=local, filter =
(&(objectclass=Person)(userPrincipalName=admin2@anshsinh.local)),LdapConnectionContext.cpp:516
Server,2020-10-10
08:54:00,635,DEBUG,0x7f85293b8700,cntx=0002480105,sesn=ise30/389444264/3178,CPMSessionID=ise30:u
serauth286,user=admin2@anshsinh.local,LdapSubjectSearchAssistant::processAttributes: found
CN=admin2,CN=Users,DC=anshsinh,DC=local entry matching admin2@anshsinh.local
subject,LdapSubjectSearchAssistant.cpp:268 Server,2020-10-10
```

```
08:54:00,635,DEBUG,0x7f85293b8700,cntx=0002480105,sesn=ise30/389444264/3178,CPMSessionID=ise30:u
serauth286,user=admin2@anshsinh.local,LdapSubjectSearchAssistant::processGroupAttr: attr =
memberOf, value = CN=employee,CN=Users,DC=anshsinh,DC=local,LdapSubjectSearchAssistant.cpp:389
Server,2020-10-10
08:54:00,636,DEBUG,0x7f85293b8700,cntx=0002480105,sesn=ise30/389444264/3178,CPMSessionID=ise30:u
serauth286,user=admin2@anshsinh.local,LdapServer::onAcquireConnectionResponse: succeeded to
acquire connection,LdapServer.cpp:724 Server,2020-10-10
08:54:00,636,DEBUG,0x7f85293b8700,cntx=0002480105,sesn=ise30/389444264/3178,CPMSessionID=ise30:u
serauth286,user=admin2@anshsinh.local,LdapServer::authenticate: user = admin2@anshsinh.local, dn
= CN=admin2,CN=Users,DC=anshsinh,DC=local,LdapServer.cpp:352 Connection,2020-10-10
08:54:00,636,DEBUG,0x7f85293b8700,LdapConnectionContext::sendBindRequest(id = 1223): dn =
CN=admin2,CN=Users,DC=anshsinh,DC=local,LdapConnectionContext.cpp:490 Server,2020-10-10
08:54:00,640,DEBUG,0x7f85293b8700,cntx=0002480105,sesn=ise30/389444264/3178,CPMSessionID=ise30:u
serauth286,user=admin2@anshsinh.local,LdapServer::handleAuthenticateSuccess: authentication of
admin2@anshsinh.local user succeeded,LdapServer.cpp:474 LDAPIDStore,2020-10-10
08:54:00,641,DEBUG,0x7f852c6eb700,cntx=0002480105,sesn=ise30/389444264/3178,CPMSessionID=ise30:u
serauth286,user=admin2@anshsinh.local,LDAPIDStore::onResponse:
LdapOperationStatus=AuthenticationSucceeded -> AuthenticationResult=Passed,LDAPIDStore.cpp:336
```

دقق ال ise-psc.log

من هذه السجلات، يمكنك التحقق من سياسة RBAC المستخدمة للمستخدم admin2 عند محاولة الوصول إلى موارد جهاز الشبكة -

```
2020-10-10 08:54:24,474 DEBUG [admin-http-pool51][] com.cisco.cpm.rbacfilter.AccessUtil -
:admin2@anshsinh.local::- For admin2@anshsinh.local on /NetworkDevicesLPInputAction.do --
ACCESS ALLOWED BY MATCHING administration_networkresources_devices 2020-10-10 08:54:24,524 INFO
[admin-http-pool51][] cpm.admin.ac.actions.NetworkDevicesLPInputAction -
:admin2@anshsinh.local::- In NetworkDevicesLPInputAction container method 2020-10-10
08:54:24,524 DEBUG [admin-http-pool51][] cisco.ise.rbac.authorization.RBACAuthorization -
:admin2@anshsinh.local::- :::::::::Inside RBACAuthorization.getDataEntityDecision::::::
userName admin2@anshsinh.local dataType RBAC_NETWORK_DEVICE_GROUP permission ALL 2020-10-10
08:54:24,526 DEBUG [admin-http-pool51][] ise.rbac.evaluator.impl.DataPermissionEvaluatorImpl -
:admin2@anshsinh.local::- In DataPermissionEvaluator:hasPermission 2020-10-10 08:54:24,526
DEBUG [admin-http-pool51][] ise.rbac.evaluator.impl.DataPermissionEvaluatorImpl -
:admin2@anshsinh.local::- Data access being evaluated:LDAP_Data_Access 2020-10-10 08:54:24,528
DEBUG [admin-http-pool51][] cisco.ise.rbac.authorization.RBACAuthorization -
:admin2@anshsinh.local::- :::::::::Inside RBACAuthorization.getDataEntityDecision::::::
permission retrieved false 2020-10-10 08:54:24,528 INFO [admin-http-pool51][]
cpm.admin.ac.actions.NetworkDevicesLPInputAction -:admin2@anshsinh.local::- Finished with rbac
execution 2020-10-10 08:54:24,534 INFO [admin-http-pool51][]
cisco.cpm.admin.license.TrustSecLicensingUIFilter -:admin2@anshsinh.local::- Should TrustSec be
visible :true 2020-10-10 08:54:24,593 DEBUG [admin-http-pool51][]
cisco.ise.rbac.authorization.RBACAuthorization -:admin2@anshsinh.local::- :::::::::Inside
RBACAuthorization.getPermittedNDG:::::: userName admin2@anshsinh.local 2020-10-10 08:54:24,595
DEBUG [admin-http-pool51][] ise.rbac.evaluator.impl.DataPermissionEvaluatorImpl -
:admin2@anshsinh.local::- In DataPermissionEvaluator:getPermittedNDGMap 2020-10-10 08:54:24,597
DEBUG [admin-http-pool51][] ise.rbac.evaluator.impl.DataPermissionEvaluatorImpl -
:admin2@anshsinh.local::- processing data Access :LDAP_Data_Access 2020-10-10 08:54:24,604 INFO
[admin-http-pool51][] cisco.cpm.admin.license.TrustSecLicensingUIFilter -
:admin2@anshsinh.local::- Should TrustSec be visible :true
```

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).