

# LDAPによるISEロールベースアクセスコントロール

## 内容

[概要](#)

[前提条件](#)

[要件](#)

[設定](#)

[ISEからLDAPへの参加](#)

[LDAPユーザの管理アクセスの有効化](#)

[管理グループをLDAPグループにマッピングします。](#)

[メニューアクセス権限の設定](#)

[データアクセスの権限の設定](#)

[管理グループの RBAC アクセス許可の設定](#)

[確認](#)

[AD クレデンシャルでの ISE へのアクセス](#)

[トラブルシューティング](#)

[一般情報](#)

[パケットキャプチャ分析](#)

[ログ分析](#)

[prrt-server.logを確認します](#)

[ise-psc.logを確認します](#)

## 概要

このドキュメントでは、Cisco Identity Services Engine(ISE)管理GUIへの管理アクセス用の外部IDストアとしてLightweight Directory Access Protocol(LDAP)を使用するための設定例について説明します。

## 前提条件

次の項目に関する知識があることが推奨されます。

- Cisco ISEバージョン3.0の設定
- LDAP(Lightweight Directory Access Protocol)

## 要件

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco ISE バージョン 3.0
- Windows Server 2016

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド

キュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

## 設定

ISE GUIへの管理/カスタムベースのアクセスを取得するようにLDAPベースのユーザを設定するには、次のセクションを使用します。次の設定では、LDAPプロトコルクエリを使用して、Active Directoryからユーザを取得し、認証を実行します。

### ISEからLDAPへの参加

1. [Administration] > [Identity Management] > [External Identity Sources] > [Active Directory] > [LDAP]に移動します。
2. [General]タブで、LDAPの名前を入力し、スキーマの[Active Directory]を選択します。

The screenshot shows the Cisco ISE Administration console. The breadcrumb navigation is Administration > Identity Management > External Identity Sources > LDAP Identity Sources List > LDAP\_Server. The left sidebar shows the navigation tree with 'External Identity Sources' expanded to 'LDAP'. The main content area shows the configuration for the 'LDAP Identity Source' with the 'General' tab selected. The configuration fields are: Name (LDAP\_Server), Description (empty), and Schema (Active Directory).

Field	Value
* Name	LDAP_Server
Description	
Schema	Active Directory

### 接続タイプとLDAP設定の設定

1. [ISE] > [Administration] > [Identity Management] > [External Identity Sources] > [LDAP]に移動します。
2. プライマリLDAPサーバのホスト名を、ポート389(LDAP)/636(LDAP-Secure)とともに設定します。
3. LDAPサーバの管理パスワードを使用して、管理識別名(DN)のパスを入力します。
4. [Test Bind Server]をクリックして、ISEからのLDAPサーバの到達可能性をテストします (LDAPサーバの到達可能性をテストします)。

Identities Groups **External Identity Sources** Identity Source Sequences Settings

> Certificate Authentication F

- Active Directory
- LDAP
- ODBC
- RADIUS Token
- RSA SecurID
- SAML Id Providers
- Social Login

General **Connection** Directory Organization Groups Attributes Advanced Settings

Primary Server		Secondary Server	
* Hostname/IP	10.127.197.180	Hostname/IP	
* Port	389	Port	389

Enable Secondary Server

Specify server for each ISE node

Access  Anonymous Access  Authenticated Access

Admin DN \* cn=Administrator,cn=Users,dc=

Password \* .....

## ディレクトリの編成、グループ、および属性の設定

1. LDAPサーバに保存されているユーザの階層に基づいて、ユーザの正しい組織グループを選択します ( 図2を参照 )。

Identities Groups **External Identity Sources** Identity Source Sequences Settings

> Certificate Authentication F

- Active Directory
- LDAP
- ODBC
- RADIUS Token
- RSA SecurID
- SAML Id Providers
- Social Login

General **Directory Organization** Connection Groups Attributes Advanced Settings

\* Subject Search Base dc=anshsinh,dc=local [Naming Contexts...](#)

\* Group Search Base dc=anshsinh,dc=local [Naming Contexts...](#)

Search for MAC Address in Format xx-xx-xx-xx-xx-xx

Strip start of subject name up to the last occurrence of the separator \

Strip end of subject name from the first occurrence of the separator

## LDAPユーザの管理アクセスの有効化

パスワードベースの認証を有効にするには、次の手順を実行します。

1. [ISE] > [Administration] > [System] > [Admin Access] > [Authentication]に移動します。
2. [Authentication Method]タブで、[Password-Based]オプションを選択します。
3. [IDソース]ドロップダウンメニューから[LDAP]を選択します。
4. [Save Changes] をクリックします。

The screenshot shows the Cisco ISE Administration console. The top navigation bar includes 'Cisco ISE', 'Administration · System', and 'Evaluation Mode 64 Days'. The main navigation menu has 'Admin Access' selected. The left sidebar shows 'Authentication' selected. The main content area is titled 'Authentication Method' and 'Authentication Type'. Under 'Authentication Type', 'Password Based' is selected with a radio button. Below it, the 'Identity Source' is set to 'LDAP:LDAP\_Server' via a dropdown menu. There is also an option for 'Client Certificate Based' which is not selected. At the bottom right, there are 'Save' and 'Reset' buttons.

## 管理グループをLDAPグループにマッピングします。

ISEで管理グループを設定し、ADグループにマッピングします。これにより、設定されたユーザは、グループメンバーシップに基づいて管理者に設定されたRBAC権限に基づいて、許可ポリシーに基づいてアクセスできるようになります。

The screenshot shows the Cisco ISE Administration console for configuring an Admin Group. The breadcrumb is 'Admin Groups > LDAP\_User\_Group'. The main title is 'Admin Group'. The 'Name' field contains 'LDAP\_User\_Group'. The 'Description' field is empty. The 'Type' is set to 'External' with a checked checkbox. The 'External Identity Source' is 'LDAP\_Server'. Under the 'External Groups' section, there is a list of groups with one entry: 'CN=employee,CN=Users,DC=a' with a plus sign to add more. Below this is the 'Member Users' section, which is currently empty with a table header: 'Status', 'Email', 'Username', 'First Name', 'Last Name'. The table shows 'No data available'.

## メニューアクセス権限の設定

1. [ISE] > [Administration] > [System] > [Authorization] > [Permissions] > [Menu access]に移動します

2. ISE GUIにアクセスするadminユーザのメニューアクセスを定義します。ユーザが必要に応じて一連の操作のみを実行できるように、GUIで表示または非表示になるようにサブエンティティを設定できます。

### 3. [Save]をクリックします。

The screenshot shows the Cisco ISE Administration console. The breadcrumb navigation is 'Administration > System > Admin Access > Menu Access List > LDAP\_Menu\_Access'. The main heading is 'Edit Menu Access Permission'. The 'Name' field contains 'LDAP\_Menu\_Access'. The 'Description' field is empty. Below this, the 'Menu Access Privileges' section is expanded to show the 'ISE Navigation Structure'. The structure includes: Operations, Policy, Administration, Work Centers, Wizard, Settings, Home, and Context Visibility. To the right, under 'Permissions for Menu Access', the 'Show' radio button is selected, and the 'Hide' radio button is unselected.

### データアクセスの権限の設定

1. [ISE] > [Administration] > [System] > [Authorization] > [Permissions] > [Data access]に移動します

2. ISE GUIでアイデンティティグループへのフルアクセスまたは読み取り専用アクセス権を持つ管理者ユーザのデータアクセスを定義します。

3. 「保存」をクリックします。

The screenshot shows the Cisco ISE Administration console. The breadcrumb navigation is 'Administration > System > Admin Access > Data Access List > LDAP\_Data\_Access'. The main heading is 'Edit Data Access Permission'. The 'Name' field contains 'LDAP\_Data\_Access'. The 'Description' field is empty. Below this, the 'Data Access Privileges' section is expanded to show a list of groups: Admin Groups, User Identity Groups, Endpoint Identity Groups, and Network Device Groups. To the right, under 'Permissions for Data Access', the 'Full Access' radio button is selected, while 'Read Only Access' and 'No Access' are unselected.

### 管理グループの RBAC アクセス許可の設定

1. [ISE] > [Administration] > [System] > [Admin Access] > [Authorization] > [Policy]に移動します。
2. 右側にある [Actions] ドロップダウン メニューから [Insert New Policy Below] を選択して、新しいポリシーを追加します。
3. LDAP\_RBAC\_policyという名前の新しいルールを作成し、[Enable Administrative Access for AD]セクションで定義した管理グループにマッピングし、メニューアクセスとデータアクセスに権限を割り当てます。
4. [Save Changes] をクリックすると、保存された変更の確認が GUI の右下隅に表示されます。

Cisco ISE Administration · System

Deployment Licensing Certificates Logging Maintenance Upgrade Health Checks Backup & Restore **Admin Access** Settings

Authentication

Authorization

Permissions

Menu Access

Data Access

**RBAC Policy**

Administrators

Settings

Create Role Based Access Control policies by configuring rules based on Admin groups, Menu Access permissions (menu items), Data Access permissions (identity group data elements) and other condition not allowed on a single policy. You can copy the default policies shown below, then modify them as needed. Note that system-created and default policies cannot be updated, and default policies cannot be evaluated. The subject's permissions will be the aggregate of all permissions from each applicable policy. Permit overrides Deny. (The policies are displayed in alphabetical order of the policy name).

RBAC Policies

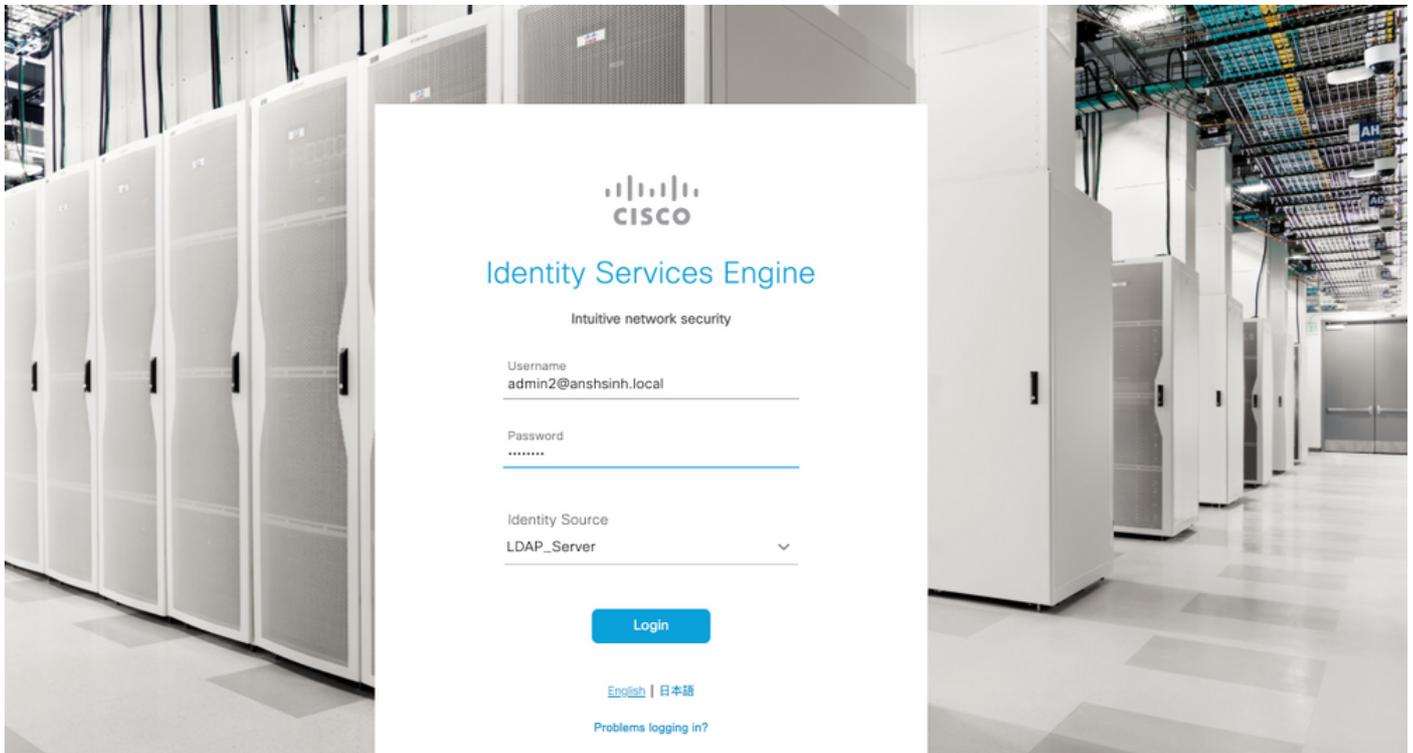
Rule Name	Admin Groups	Permissions
Customization Admin Policy	Customization Admin	Customization Admin Menu ...
Elevated System Admin Poli	Elevated System Admin	System Admin Menu Access...
ERS Admin Policy	ERS Admin	Super Admin Data Access
ERS Operator Policy	ERS Operator	Super Admin Data Access
ERS Trustsec Policy	ERS Trustsec	Super Admin Data Access
Helpdesk Admin Policy	Helpdesk Admin	Helpdesk Admin Menu Access
Identity Admin Policy	Identity Admin	Identity Admin Menu Access...
LDAP_RBAC_Rule	LDAP_User_Group	LDAP_Menu_Access and L...
MnT Admin Policy	MnT Admin	LDAP_Menu_Access
Network Device Policy	Network Device Admin	LDAP_Data_Access
Policy Admin Policy	Policy Admin	
RBAC Admin Policy	RBAC Admin	RBAC Admin Menu Access ...

## 確認

### AD クレデンシャルでの ISE へのアクセス

AD クレデンシャルを使用して ISE にアクセスするには、次の手順を実行してください。

1. ISE GUIを開き、LDAPユーザでログインします。
2. [IDソース]ドロップダウンメニューからLDAP\_Serverを選択します。
3. LDAPデータベースからユーザ名とパスワードを入力し、ログインします。



監査レポートで管理者ログインのログインを確認します。[ISE] > [Operations] > [Reports] > [Audit] > [Administrators Logins]に移動します。

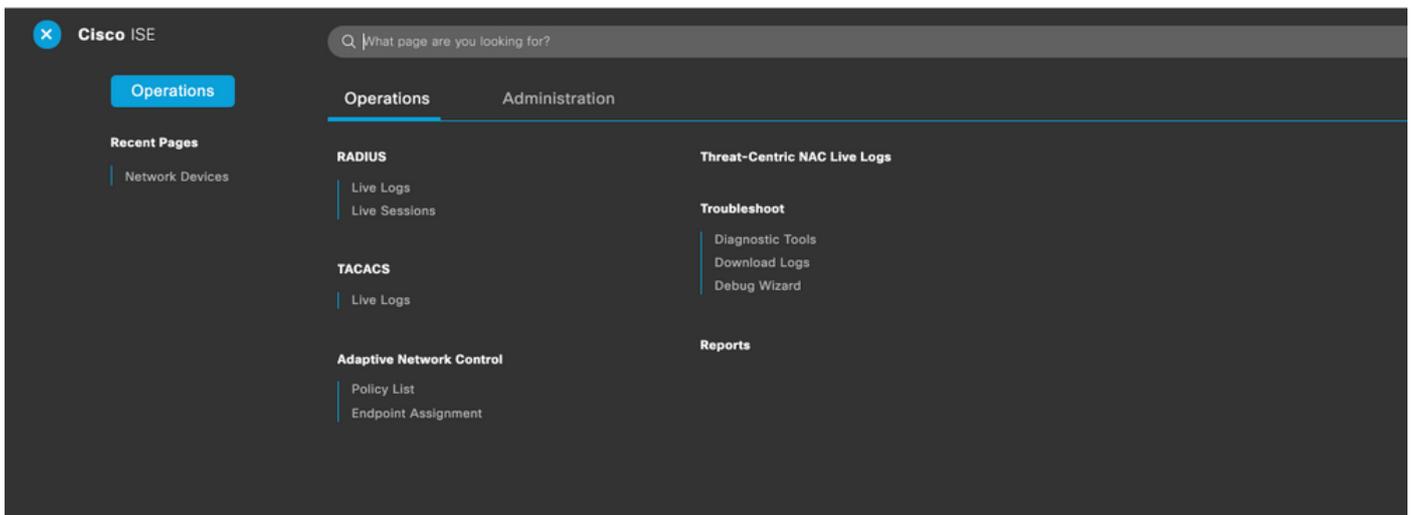
Cisco ISE Operations - Reports

Administrator Logins

From 2020-10-10 00:00:00.0 To 2020-10-10 10:58:13.0  
Reports exported in last 7 days 0

Logged At	Administrator	IP Address	Server	Event	Event Details
Today	Administrator		Server		
2020-10-10 10:57:41.217	admin	10.65.37.52	ise30	Administrator authentication succeeded	Administrator authentication successful
2020-10-10 10:57:32.098	admin2@anshsinh.local	10.65.37.52	ise30	Administrator logged off	User logged out
2020-10-10 10:56:47.668	admin2@anshsinh.local	10.65.37.52	ise30	Administrator authentication succeeded	Administrator authentication successful

この設定が正しく動作していることを確認するには、ISE GUIの右上隅にある認証済みユーザ名を確認します。次に示すように、メニューへのアクセスが制限されているカスタムベースのアクセスを定義します。



# トラブルシューティング

## 一般情報

RBACプロセスのトラブルシューティングを行うには、ISE管理ノードのデバッグで次のISEコンポーネントを有効にする必要があります ( ISEのデバッグはISE管理ノードで有効にする必要があります )。

RBAC : ログインを試みると、RBAC関連のメッセージが表示されます( ise-psc.log )

access-filter : リソースフィルタアクセス(ise-psc.log)を印刷します

runtime-AAA : ログインおよびLDAPインタラクションメッセージ(prrt-server.log)のログが出力されます

## パケットキャプチャ分析

The image shows a Wireshark packet capture analysis of LDAP traffic. The main window displays a list of packets with columns for No., Time, Source, Destination, Protocol, Length, Username, and Content. Three specific packets are highlighted with callout boxes:

- Packet 1843:** A bind request for the administrator. The callout box says: "Bind Request and response using LDAP for the administrator." The content shows a bindRequest(1) for "CN=Administrator,CN=Users,DC=anshsinh,DC=local" and a successful bindResponse(1).
- Packet 1844:** A search request for the username. The callout box says: "Search request and response Entry for the username to the mapped LDAP group." The content shows a searchRequest(2) for "dc=anshsinh,dc=local" with a wholeSubtree filter, and a searchResEntry(2) for "CN=admin2,CN=Users,DC=anshsinh,DC=local".
- Packet 1845:** A bind success for the username search. The callout box says: "Bind success for the username search." The content shows a bindRequest(1) for "CN=admin2,CN=Users,DC=anshsinh,DC=local" and a successful bindResponse(1).

## ログ分析

prrt-server.logを確認します

```
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_9240qzxSbv_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
```

## ise-psc.logを確認します

これらのログから、ネットワークデバイスのリソースにアクセスしようとしたときにadmin2ユーザに使用されるRBACポリシーを確認できます。

```
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
```