

Contrôle d'accès basé sur les rôles ISE avec LDAP

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Configurations](#)

[Rejoindre ISE à LDAP](#)

[Activer l'accès administratif pour les utilisateurs LDAP](#)

[Mapper le groupe Admin au groupe LDAP](#)

[Définir les autorisations d'accès au menu](#)

[Définir les autorisations d'accès aux données](#)

[Définir les autorisations RBAC pour le groupe Admin](#)

[Vérification](#)

[Accéder à ISE avec les identifiants AD](#)

[Dépannage](#)

[Informations générales](#)

[Analyse de capture de paquets](#)

[Analyse des journaux](#)

[Vérifier le fichier prrt-server.log](#)

[Vérifier le fichier ise-psc.log](#)

Introduction

Ce document décrit un exemple de configuration pour l'utilisation du protocole LDAP (Lightweight Directory Access Protocol) comme magasin d'identité externe pour l'accès administratif à l'interface utilisateur graphique de gestion de Cisco Identity Services Engine (ISE).

Conditions préalables

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Configuration de Cisco ISE version 3.0
- LDAP (Lightweight Directory Access Protocol)

Conditions requises

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Cisco ISE version 3.0
- Windows Server 2016

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Configurations

Utilisez la section ci-dessous pour configurer un utilisateur LDAP afin d'obtenir l'accès administratif / personnalisé à l'interface utilisateur graphique ISE . La configuration ci-dessous utilise les requêtes de protocole LDAP afin de récupérer l'utilisateur à partir d'Active Directory pour effectuer l'authentification.

Rejoindre ISE à LDAP

1. Accédez à **Administration > Identity Management > External Identity Sources > Active Directory > LDAP**.
2. Sous l'onglet **Général**, entrez le nom du LDAP et choisissez le schéma Active Directory.

The screenshot shows the Cisco ISE Administration interface. At the top, there is a navigation bar with 'Cisco ISE' on the left, 'Administration · Identity Management' in the center, and an 'Evaluation' warning icon on the right. Below the navigation bar, there are tabs for 'Identities', 'Groups', 'External Identity Sources' (which is selected), 'Identity Source Sequences', and 'Settings'. On the left side, there is a sidebar menu for 'External Identity Sources' with a list of categories: Certificate Authentication F, Active Directory, LDAP (selected), ODBC, RADIUS Token, RSA SecurID, SAML Id Providers, and Social Login. The main content area shows the configuration for an 'LDAP Identity Source' named 'LDAP_Server'. The breadcrumb path is 'LDAP Identity Sources List > LDAP_Server'. The configuration is displayed in a tabbed interface with 'General' selected. The 'General' tab shows the following fields: '* Name' with the value 'LDAP_Server', 'Description' (empty), and 'Schema' with a dropdown menu set to 'Active Directory'.

Configurer le type de connexion et la configuration LDAP

1. Accédez à **ISE > Administration > Identity Management > External Identity Sources > LDAP**.
2. Configurez le nom d'hôte du serveur LDAP principal avec le port 389(LDAP)/636 (LDAP-Secure).
3. Entrez le chemin d'accès du nom unique d'administrateur (DN) avec le mot de passe admin pour le serveur LDAP .
4. Cliquez sur Test Bind Server pour tester l'accessibilité du serveur LDAP à partir d'ISE .

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 *

Configurer l'organisation, les groupes et les attributs du répertoire

1. Choisissez le groupe Organisation correct de l'utilisateur en fonction de la hiérarchie des utilisateurs stockés dans le serveur LDAP .

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

* 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

Activer l'accès administratif pour les utilisateurs LDAP

Complétez ces étapes afin d'activer l'authentification basée sur un mot de passe.

1. Accédez à ISE > Administration > System > Admin Access > Authentication.
2. Sous l'onglet Authentication Method, sélectionnez l'option Password-Based.
3. Sélectionnez LDAP dans le menu déroulant Source d'identité.
4. Cliquez sur Enregistrer les modifications.

The screenshot shows the Cisco ISE Administration interface. The top navigation bar includes 'Administration - System' and 'Evaluation Mode 64 Days'. The main navigation menu has 'Admin Access' selected. On the left, a sidebar contains 'Authentication', 'Authorization', 'Administrators', and 'Settings'. The main content area is titled 'Authentication Method' and includes sub-sections for 'Password Policy', 'Account Disable Policy', and 'Lock/Suspend Settings'. Under 'Authentication Type', the 'Password Based' option is selected. Below this, the 'Identity Source' is set to 'LDAP:LDAP_Server' via a dropdown menu, and the 'Client Certificate Based' option is unselected. At the bottom right, there are 'Save' and 'Reset' buttons.

Mapper le groupe Admin au groupe LDAP

Configurez le groupe Admin sur l'ISE et associez-le au groupe AD. Cela permet à l'utilisateur configuré d'obtenir un accès en fonction des stratégies d'autorisation en fonction des autorisations RBAC configurées pour l'administrateur en fonction de l'appartenance au groupe.

The screenshot shows the Cisco ISE Administration interface for configuring an Admin Group. The top navigation bar includes 'Administration - System' and 'Evaluation Mode 64 Days'. The main navigation menu has 'Admin Access' selected. On the left, a sidebar contains 'Authentication', 'Authorization', 'Administrators', and 'Settings'. The 'Administrators' section is expanded to show 'Admin Users' and 'Admin Groups', with 'Admin Groups' selected. The main content area is titled 'Admin Group' and shows the configuration for 'LDAP_User_Group'. The 'Name' field is 'LDAP_User_Group'. The 'Description' field is empty. The 'Type' is set to 'External'. The 'External Identity Source' is 'LDAP_Server'. Under 'External Groups', a group is selected: 'CN=employee,CN=Users,DC=a'. Below this, there is a 'Member Users' section with 'Users' listed. There are '+ Add' and 'Delete' buttons. At the bottom, there is a table with columns: 'Status', 'Email', 'Username', 'First Name', and 'Last Name'. The table is currently empty, with the text 'No data available' below it.

Définir les autorisations d'accès au menu

1. Accédez à ISE > Administration > System > Authorization > Permissions > Menu access.

2. Définissez l'accès au menu pour que l'utilisateur administrateur puisse accéder à l'interface utilisateur graphique ISE. Nous pouvons configurer les sous-entités à afficher ou masquer sur l'interface utilisateur graphique pour qu'un utilisateur puisse accéder à un jeu d'opérations uniquement si nécessaire.

3. Cliquez sur Enregistrer.

The screenshot shows the Cisco ISE Administration interface for the 'System' section. The left sidebar contains navigation options: Authentication, Authorization, Permissions, Menu Access (selected), Data Access, RBAC Policy, Administrators, and Settings. The main content area is titled 'Edit Menu Access Permission' and shows the configuration for 'LDAP_Menu_Access'. The 'Name' field is filled with 'LDAP_Menu_Access' and the 'Description' field is empty. Below this, the 'Menu Access Privileges' section displays a tree view of the 'ISE Navigation Structure' with the following items: Operations, Policy, Administration, Work Centers, Wizard, Settings, Home, and Context Visibility. To the right of the tree, there are radio buttons for 'Show' (selected) and 'Hide'.

Définir les autorisations d'accès aux données

1. Accédez à ISE > Administration > System > Authorization > Permissions > Data access.

2. Définissez l'accès aux données pour que l'utilisateur administrateur dispose d'un accès complet ou en lecture seule aux groupes d'identité sur l'interface utilisateur graphique ISE.

3. Cliquez sur Enregistrer.

The screenshot shows the Cisco ISE Administration interface for the 'System' section. The left sidebar contains navigation options: Authentication, Authorization, Permissions, Menu Access, Data Access (selected), RBAC Policy, Administrators, and Settings. The main content area is titled 'Edit Data Access Permission' and shows the configuration for 'LDAP_Data_Access'. The 'Name' field is filled with 'LDAP_Data_Access' and the 'Description' field is empty. Below this, the 'Data Access Privileges' section displays a tree view of the 'Data Access Privileges' with the following items: Admin Groups, User Identity Groups, Endpoint Identity Groups, and Network Device Groups. To the right of the tree, there are radio buttons for 'Full Access' (selected), 'Read Only Access', and 'No Access'.

Définir les autorisations RBAC pour le groupe Admin

1. Accédez à ISE > Administration > System > Admin Access > Authorization > Policy.

2. Dans le menu déroulant **Actions** à droite, sélectionnez **Insérer une nouvelle stratégie ci-dessous** afin d'ajouter une nouvelle stratégie.
3. Créez une nouvelle règle appelée LDAP_RBAC_policy et mappez-la avec le groupe d'administration défini dans la section Activer l'accès administratif pour AD, et affectez-lui des autorisations pour l'accès au menu et aux données.
4. Cliquez sur **Enregistrer les modifications**, et la confirmation des modifications enregistrées s'affiche dans le coin inférieur droit de l'interface utilisateur graphique.

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
<input checked="" type="checkbox"/> Customization Admin Policy	If Customization Admin +	then Customization Admin Menu ... + Actions ▾
<input checked="" type="checkbox"/> Elevated System Admin Poli	If Elevated System Admin +	then System Admin Menu Access... + Actions ▾
<input checked="" type="checkbox"/> ERS Admin Policy	If ERS Admin +	then Super Admin Data Access + Actions ▾
<input checked="" type="checkbox"/> ERS Operator Policy	If ERS Operator +	then Super Admin Data Access + Actions ▾
<input checked="" type="checkbox"/> ERS Trustsec Policy	If ERS Trustsec +	then Super Admin Data Access + Actions ▾
<input checked="" type="checkbox"/> Helpdesk Admin Policy	If Helpdesk Admin +	then Helpdesk Admin Menu Access + Actions ▾
<input checked="" type="checkbox"/> Identity Admin Policy	If Identity Admin +	then Identity Admin Menu Access... + Actions ▾
<input checked="" type="checkbox"/> LDAP_RBAC_Rule	If LDAP_User_Group +	then LDAP_Menu_Access and L... X Actions ▾
<input checked="" type="checkbox"/> MnT Admin Policy	If MnT Admin +	then LDAP_Menu_Access ▾ +
<input checked="" type="checkbox"/> Network Device Policy	If Network Device Admin +	then LDAP_Data_Access ▾ +
<input checked="" type="checkbox"/> Policy Admin Policy	If Policy Admin +	then RBAC Admin Menu Access ... + Actions ▾
<input checked="" type="checkbox"/> RBAC Admin Policy	If RBAC Admin +	then RBAC Admin Menu Access ... + Actions ▾

Vérification

Accéder à ISE avec les identifiants AD

Complétez ces étapes afin d'accéder à ISE avec des informations d'identification AD :

1. Ouvrez l'interface utilisateur ISE pour vous connecter à l'utilisateur LDAP.
2. Sélectionnez LDAP_Server dans le menu déroulant **Source d'identité**.
3. Saisissez le nom d'utilisateur et le mot de passe de la base de données LDAP, puis connectez-vous.



Vérifiez la connexion de l'administrateur dans Rapports d'audit. Accédez à ISE > Operations > Reports > Audit > Administrators Logins.

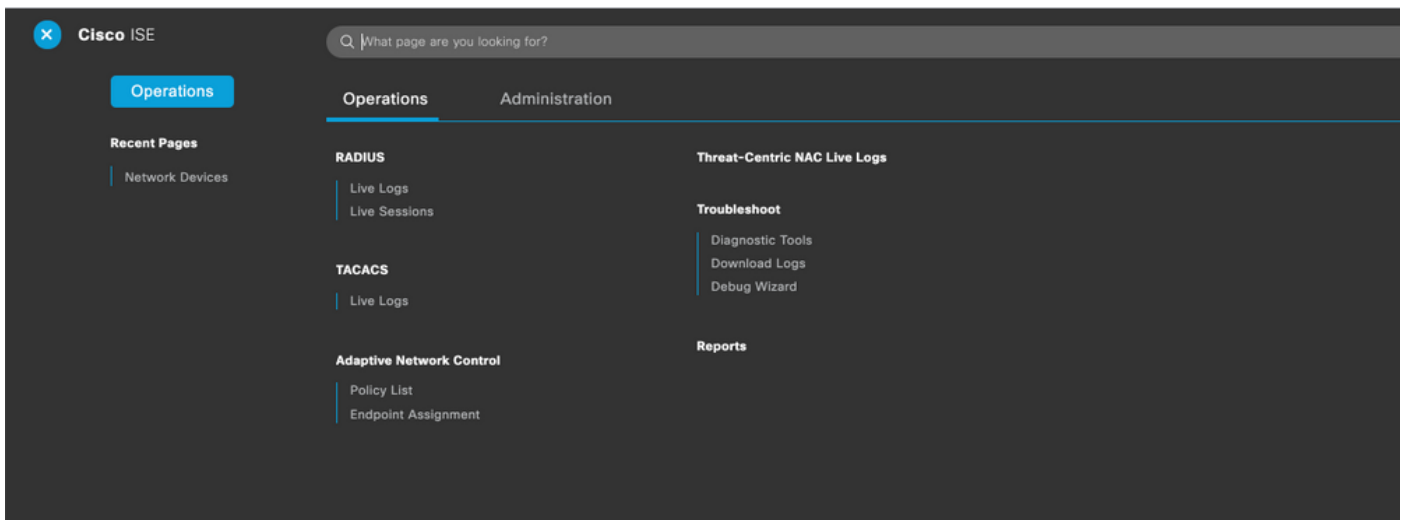
Cisco ISE Operations - Reports Evaluation Mode 64 Days

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

Afin de vérifier que cette configuration fonctionne correctement, vérifiez le nom d'utilisateur authentifié dans le coin supérieur droit de l'interface utilisateur graphique ISE. Définissez un accès personnalisé dont l'accès au menu est limité, comme indiqué ici :



Dépannage

Informations générales

Afin de dépanner le processus RBAC, ces composants ISE doivent être activés dans debug sur le noeud d'administration ISE :

RBAC - Ce message s'affiche lorsque nous tentons de nous connecter (ise-psc.log).

access-filter - Permet d'imprimer l'accès au filtre de ressources (ise-psc.log)

runtime-AAA - Les journaux seront imprimés pour les messages d'interaction LDAP et de connexion (prtt-server.log)

Analyse de capture de paquets

No.	Time	Source	Destination	Protocol	Length	User-Name	Op.
579	2028-09-30 01:21:00.848523	10.106.32.184	10.127.197.188	LDAP	73		unbindRequest(4)
1040	2028-09-30 01:21:13.346421	10.106.32.184	10.127.197.188	LDAP	140		bindRequest(1) "CN=Administrator,CN=Users,DC=anshsinh,DC=local" simple
1041	2028-09-30 01:21:13.348424	10.127.197.188	10.106.32.184	LDAP	88		bindResponse(1) success
1042	2028-09-30 01:21:13.349233	10.127.197.188	10.106.32.184	LDAP	475		searchRequest(2) "dc=anshsinh,dc=local" wholeSubtree
1048	2028-09-30 01:21:13.351026	10.106.32.184	10.127.197.188	LDAP	127		searchResEntry(2) "CN=admin2,CN=Users,DC=anshsinh,DC=local" searchRes
1049	2028-09-30 01:21:13.352089	10.127.197.188	10.106.32.184	LDAP	88		bindRequest(1) "CN=admin2,CN=Users,DC=anshsinh,DC=local" simple
15320	2028-09-30 01:21:40.068100	10.106.32.184	10.127.197.188	LDAP	191		bindResponse(1) success
15325	2028-09-30 01:21:40.069045	10.127.197.188	10.106.32.184	LDAP	475		searchRequest(3) "dc=anshsinh,dc=local" wholeSubtree
15330	2028-09-30 01:21:40.069756	10.106.32.184	10.127.197.188	LDAP	127		searchResEntry(3) "CN=admin2,CN=Users,DC=anshsinh,DC=local" searchRes
15337	2028-09-30 01:21:40.071004	10.127.197.188	10.106.32.184	LDAP	88		bindRequest(2) "CN=admin2,CN=Users,DC=anshsinh,DC=local" simple
							bindResponse(2) success

Analyse des journaux

Vérifier le fichier prtt-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
```

Vérifier le fichier ise-psc.log

À partir de ces journaux, vous pouvez vérifier la stratégie RBAC utilisée pour l'utilisateur admin2 lors d'une tentative d'accès à la ressource Périphérique réseau -

```
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
```