

Controllo degli accessi basato sui ruoli ISE con LDAP

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Configurazioni](#)

[Unisci ISE a LDAP](#)

[Abilita accesso amministrativo per utenti LDAP](#)

[Mappare il gruppo amministrativo al gruppo LDAP](#)

[Imposta autorizzazioni per accesso menu](#)

[Impostare le autorizzazioni per l'accesso ai dati](#)

[Impostare le autorizzazioni RBAC per il gruppo Admin](#)

[Verifica](#)

[Accesso ad ISE con credenziali AD](#)

[Risoluzione dei problemi](#)

[Informazioni generali](#)

[Analisi acquisizione pacchetti](#)

[Analisi log](#)

[Verificare il file prrt-server.log](#)

[Verificare il file ise-psc.log](#)

Introduzione

Questo documento descrive un esempio di configurazione per l'uso del protocollo LDAP (Lightweight Directory Access Protocol) come archivio identità esterno per l'accesso amministrativo all'interfaccia utente di gestione di Cisco Identity Services Engine (ISE).

Prerequisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Configurazione di Cisco ISE versioni 3.0
- LDAP (Lightweight Directory Access Protocol)

Requisiti

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco ISE versione 3.0
- Windows Server 2016

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Configurazioni

Utilizzare la sezione seguente per configurare un utente basato su LDAP in modo da ottenere l'accesso amministrativo/personalizzato all'interfaccia grafica di ISE. La configurazione seguente utilizza le query del protocollo LDAP per recuperare l'utente da Active Directory per eseguire l'autenticazione.

Unisci ISE a LDAP

1. Passare a **Amministrazione > Gestione delle identità > Origini identità esterne > Active Directory > LDAP**.
2. Nella scheda **Generale**, immettere il nome del server LDAP e scegliere lo schema Active Directory.

The screenshot shows the Cisco ISE Administration interface. The breadcrumb navigation is "Administration > Identity Management". The main menu includes "Identities", "Groups", "External Identity Sources", "Identity Source Sequences", and "Settings". The "External Identity Sources" section is expanded, showing a list of sources: Certificate Authentication F, Active Directory, LDAP, ODBC, RADIUS Token, RSA SecurID, SAML Id Providers, and Social Login. The "LDAP" source is selected, and the configuration page for "LDAP Identity Source" is displayed. The "General" tab is active, showing the following fields: "Name" (LDAP_Server), "Description" (empty), and "Schema" (Active Directory). The "Evaluation" warning icon is visible in the top right corner.

Configura tipo di connessione e configurazione LDAP

1. Passare a **ISE > Amministrazione > Gestione delle identità > Origini identità esterne > LDAP**.
2. Configurare il nome host del server LDAP primario insieme alla porta 389(LDAP)/636 (LDAP-Secure).
3. Immettere il percorso per il nome distinto (DN) dell'amministratore con la password dell'amministratore per il server LDAP.
4. Fare clic su Test Bind Server per verificare la raggiungibilità del server LDAP da 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
<input type="checkbox"/> Specify server for each ISE node		<input type="checkbox"/> Enable Secondary Server	
Access	<input checked="" type="radio"/> Authenticated Access	Access	<input checked="" type="radio"/> Anonymous Access
Admin DN	* cn=Administrator,cn=Users,dc=	Admin DN	
Password	*	Password	

Configurare l'organizzazione della directory, i gruppi e gli attributi

1. Scegliere il gruppo di organizzazioni corretto dell'utente in base alla gerarchia degli utenti memorizzati nel server 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

Abilita accesso amministrativo per utenti LDAP

Completare questa procedura per abilitare l'autenticazione basata su password.

1. Selezionare **ISE > Amministrazione > Sistema > Accesso amministratore > Autenticazione**.
2. Nella scheda **Metodo di autenticazione** selezionare l'opzione **Basato su password**.
3. Selezionare **LDAP** dal menu a discesa **Origine identità**.
4. Fare clic su **Salva modifiche**.

The screenshot shows the Cisco ISE Administration interface. 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 includes sub-tabs for 'Password Policy', 'Account Disable Policy', and 'Lock/Suspend Settings'. Under 'Authentication Type', 'Password Based' is selected. The 'Identity Source' is set to 'LDAP:LDAP_Server'. There are 'Save' and 'Reset' buttons at the bottom right.

Mappare il gruppo amministrativo al gruppo LDAP

Configurare il gruppo Admin sull'ISE e mapparlo al gruppo AD. Ciò consente all'utente configurato di ottenere l'accesso in base ai criteri di autorizzazione basati sulle autorizzazioni RBAC configurate per l'amministratore in base all'appartenenza ai gruppi.

The screenshot shows the Cisco ISE Administration interface for configuring an Admin Group. The top navigation bar is the same as the previous screenshot. The left sidebar shows '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 'Type' is set to 'External'. The 'External Identity Source' is 'LDAP_Server'. Under 'External Groups', 'CN=employee,CN=Users,DC=a' is listed. There is an 'Add' button and a 'Delete' button. Below the configuration is a table for 'Member Users' with columns for 'Status', 'Email', 'Username', 'First Name', and 'Last Name'. The table is currently empty, showing 'No data available'.

Imposta autorizzazioni per accesso menu

1. Selezionare ISE > Amministrazione > Sistema > Autorizzazione > Autorizzazioni > Accesso al menu
2. Definire l'accesso al menu per l'utente amministratore per accedere all'interfaccia grafica di ISE. È possibile configurare le entità secondarie da visualizzare o nascondere sulla GUI per consentire a un utente di eseguire solo un insieme di operazioni, se necessario.

3. Fare clic su **Save** (Salva).

The screenshot shows the Cisco ISE Administration console. The top navigation bar includes 'Administration · System' and various tabs like 'Deployment', 'Licensing', 'Certificates', 'Logging', 'Maintenance', 'Upgrade', 'Health Checks', 'Backup & Restore', 'Admin Access', and 'Settings'. The left sidebar shows a menu with 'Menu Access' selected. 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'. Below it is a 'Description' text box. Underneath, the 'Menu Access Privileges' section shows a tree view of the 'ISE Navigation Structure' with options like 'Operations', 'Policy', 'Administration', 'Work Centers', 'Wizard', 'Settings', 'Home', and 'Context Visibility'. To the right of this tree, there are radio buttons for 'Show' (selected) and 'Hide'.

Impostare le autorizzazioni per l'accesso ai dati

1. Selezionare **ISE > Amministrazione > Sistema > Autorizzazione > Autorizzazioni > Accesso ai dati**

2. Definire l'accesso ai dati per l'utente amministratore in modo che abbia accesso completo o di sola lettura ai gruppi di identità sull'interfaccia grafica ISE.

3. Fare clic su **Save** (Salva).

The screenshot shows the Cisco ISE Administration console. The top navigation bar includes 'Administration · System' and various tabs like 'Deployment', 'Licensing', 'Certificates', 'Logging', 'Maintenance', 'Upgrade', 'Health Checks', 'Backup & Restore', 'Admin Access', and 'Settings'. The left sidebar shows a menu with 'Data Access' selected. 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'. Below it is a 'Description' text box. Underneath, the 'Data Access Privileges' section shows a tree view of the 'Data Access Privileges' with options like 'Admin Groups', 'User Identity Groups', 'Endpoint Identity Groups', and 'Network Device Groups'. To the right of this tree, there are radio buttons for 'Full Access' (selected), 'Read Only Access', and 'No Access'.

Impostare le autorizzazioni RBAC per il gruppo Admin

1. Selezionare **ISE > Amministrazione > Sistema > Accesso amministratore > Autorizzazione > Criteri**.
2. Dal menu a discesa **Azioni** a destra, selezionare **Inserisci nuovo criterio sotto** per aggiungere un nuovo criterio.
3. Creare una nuova regola denominata **LDAP_RBAC_policy** e mapparla al gruppo Admin definito nella sezione **Abilita accesso amministrativo per AD** e assegnarle le autorizzazioni per l'accesso ai menu e ai dati.
4. Fare clic su **Save Changes** (Salva modifiche). Nell'angolo inferiore destro dell'interfaccia grafica viene visualizzata la conferma delle modifiche salvate.

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

Verifica

Accesso ad ISE con credenziali AD

Per accedere ad ISE con le credenziali di AD, completare la procedura seguente:

1. Aprire ISE GUI per accedere con l'utente LDAP.
2. Selezionare LDAP_Server dal menu a discesa **Origine identità**.
3. Immettere il nome utente e la password dal database LDAP ed effettuare l'accesso.



Verificare l'accesso per gli account di accesso dell'amministratore nei report di verifica. Passare a ISE > Operazioni > Report > Audit > Login amministratori.

Cisco ISE Operations - Reports Evaluation Mode 64 Days

Export Summary

My Reports >

Reports >

Audit >

- Adaptive Network Cont...
- Administrator Logins
- Change Configuration ...
- Cisco Support Diagnost...
- Data Purging Audit
- Endpoints Purge Activit...
- Internal Administrator S...

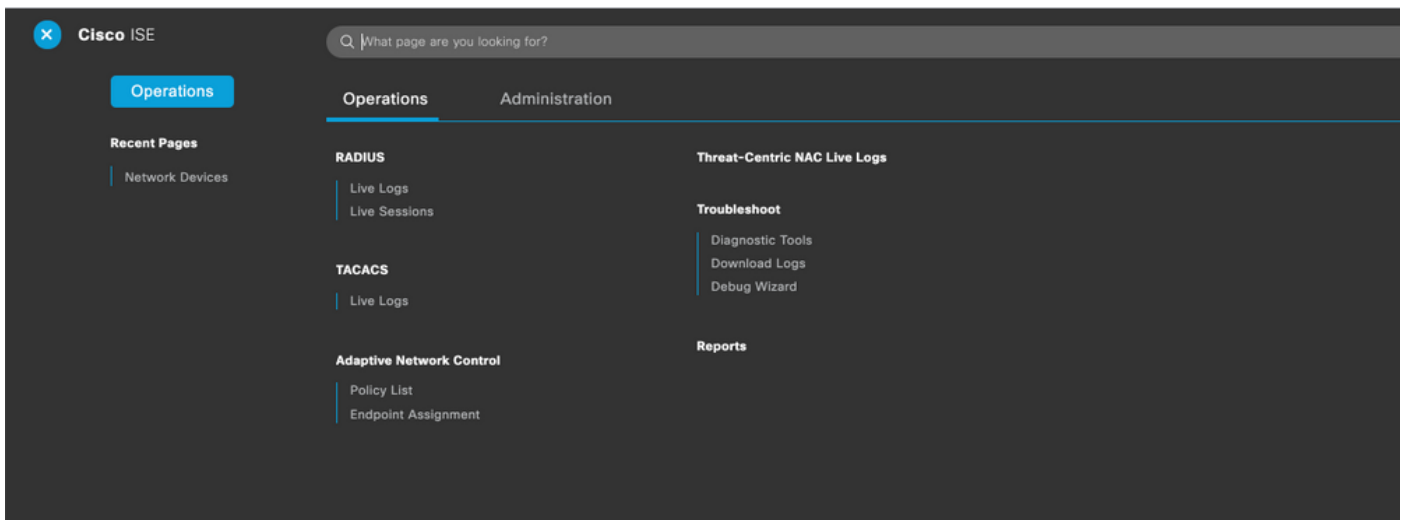
Administrator Logins

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

Filter Refresh

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

Per verificare che la configurazione funzioni correttamente, verificare il nome utente autenticato nell'angolo in alto a destra dell'interfaccia utente di ISE. Definire un accesso personalizzato con accesso limitato al menu, come illustrato di seguito:



Risoluzione dei problemi

Informazioni generali

Per risolvere i problemi relativi al processo RBAC, questi componenti ISE devono essere abilitati nel debug sul nodo ISE Admin:

RBAC - Stampa il messaggio relativo a RBAC quando si prova a eseguire il login (ise-psc.log)

access-filter - Stampa l'accesso al filtro risorse (ise-psc.log)

runtime-AAA - Stampa i log per i messaggi di accesso e interazione LDAP (prt-server.log)

Analisi acquisizione pacchetti

The image shows a network traffic capture window with several columns: No., Time, Source, Destination, Protocol, Length, User-Name, and Content. The content column shows LDAP protocol details. Three callout boxes highlight specific parts of the traffic:

- Bind Request and response using LDAP for the administrator.** Points to a bindRequest(1) and its corresponding bindResponse(1) success.
- Search request and response Entry for the username to the mapped LDAP group.** Points to a searchRequest(2) and its corresponding searchResEntry(2).
- Bind success for the username search** Points to a bindRequest(1) and its corresponding bindResponse(1) success.

Analisi log

Verificare il file prt-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
```

Verificare il file ise-psc.log

Da questi registri è possibile verificare il criterio RBAC utilizzato per l'utente admin2 quando tenta di accedere alla risorsa Dispositivo di rete -

```
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
```