

# Controle de acesso baseado em função do ISE com LDAP

## Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Configurações](#)

[Ingressar ISE em LDAP](#)

[Habilitar acesso administrativo para usuários LDAP](#)

[Mapear o grupo de administração para o grupo LDAP](#)

[Definir permissões para acesso ao menu](#)

[Definir permissões para acesso a dados](#)

[Definir permissões RBAC para o grupo de administração](#)

[Verificar](#)

[Acesse o ISE com credenciais do AD](#)

[Troubleshoot](#)

[Informações gerais](#)

[Análise de Captura de Pacotes](#)

[Análise de log](#)

[Verifique o servidor da porta.log](#)

[Verifique o ise-psc.log](#)

## Introduction

Este documento descreve um exemplo de configuração para o uso do Lightweight Directory Access Protocol (LDAP) como um repositório de identidade externa para acesso administrativo à GUI de gerenciamento do Cisco Identity Services Engine (ISE).

## Prerequisites

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Configuração do Cisco ISE versões 3.0
- LDAP (Lightweight Directory Access Protocol)

## Requirements

As informações neste documento são baseadas nestas versões de software e hardware:

- Cisco ISE versão 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.

## Configurações

Use a seção abaixo para configurar um usuário baseado em LDAP para obter o acesso baseado em administração/personalizado à GUI do ISE . A configuração abaixo usa as consultas do protocolo LDAP para buscar o usuário do Ative Directory para executar a autenticação.

### Ingressar ISE em LDAP

1. Navegue até **Administration > Identity Management > External Identity Sources > Active Directory > LDAP**.
2. Na guia **Geral**, insira o nome do LDAP e escolha o esquema Active Directory.

The screenshot shows the Cisco ISE Administration interface. The breadcrumb navigation is Administration > Identity Management > External Identity Sources > LDAP\_Server. The left sidebar shows a tree view of External Identity Sources, with LDAP selected. The main content area displays the configuration for the LDAP Identity Source 'LDAP\_Server'. The 'General' tab is active, showing fields for Name (LDAP\_Server), Description, and Schema (Active Directory).

### Configurar o tipo de conexão e a configuração LDAP

1. Navegue até **ISE > Administration > Identity Management > External Identity Sources > LDAP**.
2. Configure o nome de host do servidor LDAP primário junto com a porta 389(LDAP)/636 (LDAP-Secure) .
3. Insira o caminho para o DN (Admin Distinguished Name, nome distinto de administrador) com a senha de administrador para o servidor LDAP .
4. Clique em **Test Bind Server** para testar a acessibilidade do servidor LDAP do ISE .

Cisco ISE Administration - Identity Management Evaluation Mode 64 Days

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: \*

## Configurar a organização, os grupos e os atributos do diretório

1. Escolha o grupo de Organização correto do usuário com base na hierarquia de usuários armazenados no servidor LDAP .

Cisco ISE Administration - Identity Management

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

## Habilitar acesso administrativo para usuários LDAP

Conclua estes passos para habilitar a autenticação baseada em senha.

1. Navegue até ISE > Administration > System > Admin Access > Authentication.
2. Na guia Authentication Method, selecione a opção Password-Based.
3. Selecione LDAP no menu suspenso Origem da identidade.
4. Clique em Salvar alterações.

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 'Authentication Type'. Under 'Authentication Method', 'Password Based' is selected. The 'Identity Source' is set to 'LDAP:LDAP\_Server'. There are 'Save' and 'Reset' buttons at the bottom right.

## Mapear o grupo de administração para o grupo LDAP

Configure o grupo Admin no ISE e mapeie-o para o grupo AD. Isso permite que o usuário configurado obtenha acesso com base nas políticas de autorização com base nas permissões de RBAC configuradas para o administrador com base na associação do grupo.

The screenshot shows the Cisco ISE Administration interface for configuring an Admin Group. 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 'Admin Groups' selected. The main content area is titled 'Admin Group' and 'LDAP\_User\_Group'. The 'Name' is 'LDAP\_User\_Group'. The 'Type' is 'External'. The 'External Identity Source' is 'LDAP\_Server'. The 'External Groups' section shows 'CN=employee,CN=Users,DC=a'. The 'Member Users' section is empty. There are 'Add' and 'Delete' buttons. A table with columns 'Status', 'Email', 'Username', 'First Name', and 'Last Name' is shown with 'No data available'.

## Definir permissões para acesso ao menu

1. Navegue até ISE > Administration > System > Authorization > Permissions > Menu access
2. Defina o acesso ao menu para que o usuário administrador acesse a GUI do ISE. Podemos configurar as subentidades a serem mostradas ou ocultadas na GUI para acesso personalizado para que um usuário execute apenas um conjunto de operações, se necessário.

### 3. Clique em **Salvar**.

The screenshot shows the Cisco ISE Administration interface. The top navigation bar includes 'Administration · System' and a menu with 'Admin Access' selected. The left sidebar shows 'Permissions' > 'Menu Access' selected. The main content area is titled 'Edit Menu Access Permission' for 'LDAP\_Menu\_Access'. It features a 'Description' text box and a 'Menu Access Privileges' section. This section contains a tree view of the 'ISE Navigation Structure' with items like Operations, Policy, Administration, Work Centers, Wizard, Settings, Home, and Context Visibility. To the right, 'Permissions for Menu Access' are set to 'Show'.

### Definir permissões para acesso a dados

1. Navegue até ISE > Administration > System > Authorization > Permissions > Data access

2. Defina o acesso aos dados para que o usuário administrador tenha acesso total ou somente leitura aos grupos de identidade na GUI do ISE.

### 3. Clique em **Salvar**.

The screenshot shows the Cisco ISE Administration interface. The top navigation bar includes 'Administration · System' and a menu with 'Admin Access' selected. The left sidebar shows 'Permissions' > 'Data Access' selected. The main content area is titled 'Edit Data Access Permission' for 'LDAP\_Data\_Access'. It features a 'Description' text box and a 'Data Access Privileges' section. This section contains a tree view of 'Data Access Privileges' with items like Admin Groups, User Identity Groups, Endpoint Identity Groups, and Network Device Groups. To the right, 'Permissions for Data Access' are set to 'Full Access'.

### Definir permissões RBAC para o grupo de administração

1. Navegue até ISE > Administration > System > Admin Access > Authorization > Policy.

- No menu suspenso **Ações** à direita, selecione **Inserir nova política abaixo** para adicionar uma nova política.
- Crie uma nova regra chamada LDAP\_RBAC\_policy e mapeie-a com o Grupo Admin definido na seção Ativar acesso administrativo para AD e atribua-lhe permissões para acesso a menu e acesso a dados.
- Clique em **Save Changes** e a confirmação das alterações salvas será exibida no canto inferior direito da GUI.

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 ▾

## Verificar

### Acesse o ISE com credenciais do AD

Conclua estes passos para acessar o ISE com credenciais do AD:

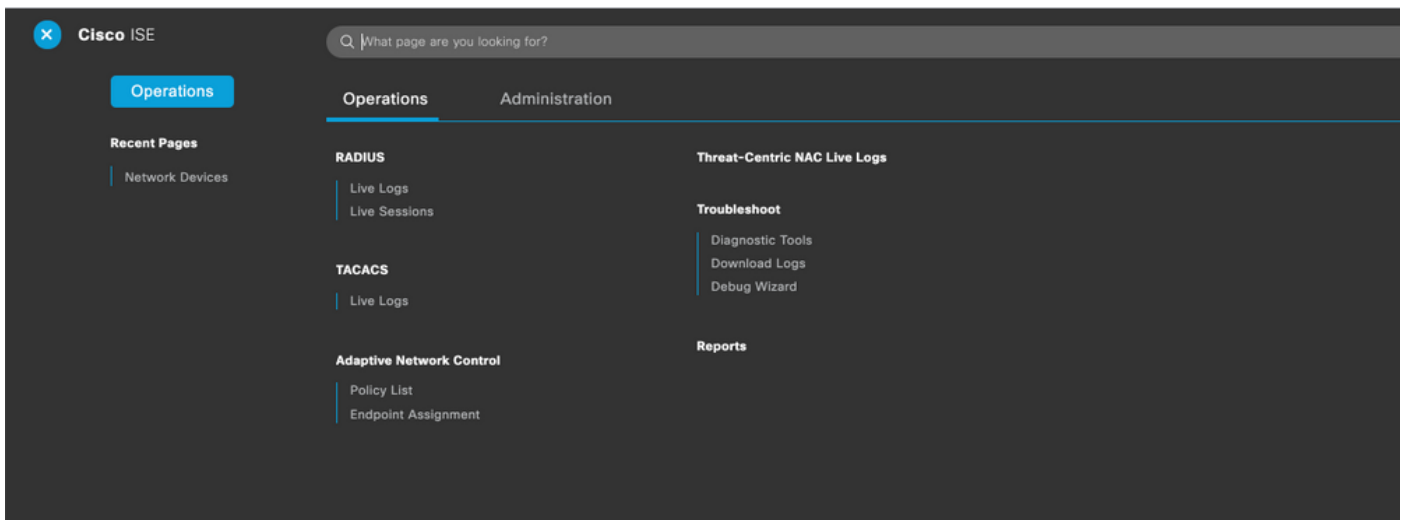
- Abra a GUI do ISE para fazer login com o usuário LDAP.
- Selecione LDAP\_Server no menu suspenso **Origem da identidade**.
- Insira o nome de usuário e a senha do banco de dados LDAP e faça login.



Verifique o login do administrador nos Relatórios de auditoria. Navegue até ISE > Operations > Reports > Audit > Administrators Logins.

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

Para confirmar se essa configuração funciona corretamente, verifique o nome de usuário autenticado no canto superior direito da GUI do ISE. Defina um acesso personalizado que tenha acesso limitado ao menu como mostrado aqui:





# Troubleshoot

## Informações gerais

Para solucionar problemas do processo de RBAC, esses componentes do ISE precisam ser ativados na depuração no nó de administração do ISE :

RBAC - Isso imprimirá a mensagem relacionada ao RBAC quando tentarmos fazer login ( ise-psc.log )

access-filter - Isso imprimirá o acesso ao filtro de recursos (ise-psc.log )

runtime-AAA - Isso imprimirá os logs para mensagens de interação de login e LDAP (prtt-server.log )

## Análise de Captura de Pacotes

The image shows a Wireshark packet capture analysis of LDAP traffic. A table of packets is visible on the left, and the packet details pane on the right shows the structure of the LDAP messages. Three callout boxes provide context:

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

No.	Time	Source	Destination	Protocol	Length	Username	Content
579	2020-09-30 01:21:08.848523	10.106.32.104	10.127.197.180	LDAP	73		unbindRequest(4)
1040	2020-09-30 01:21:13.346421	10.106.32.104	10.127.197.180	LDAP	140		bindRequest(1) "CN=Administrator,CN=Users,DC=anshsinh,DC=local" simple
1041	2020-09-30 01:21:13.348424	10.127.197.180	10.106.32.104	LDAP	88		bindResponse(1) success
1043	2020-09-30 01:21:13.348757	10.106.32.104	10.127.197.180	LDAP	191		searchRequest(2) "dc=anshsinh,dc=local" wholeSubtree
1044	2020-09-30 01:21:13.349581	10.127.197.180	10.106.32.104	LDAP	475		searchResEntry(2) "CN=admin2,CN=Users,DC=anshsinh,DC=local"   searchRes
1048	2020-09-30 01:21:13.351026	10.106.32.104	10.127.197.180	LDAP	127		bindRequest(1) "CN=admin2,CN=Users,DC=anshsinh,DC=local" simple
1049	2020-09-30 01:21:13.352009	10.127.197.180	10.106.32.104	LDAP	88		bindResponse(1) success
15320	2020-09-30 01:21:40.968100	10.106.32.104	10.127.197.180	LDAP	191		searchRequest(13) "dc=anshsinh,dc=local" wholeSubtree
15325	2020-09-30 01:21:40.968045	10.127.197.180	10.106.32.104	LDAP	475		searchResEntry(13) "CN=admin2,CN=Users,DC=anshsinh,DC=local"   searchRes
15330	2020-09-30 01:21:40.969756	10.106.32.104	10.127.197.180	LDAP	127		bindRequest(2) "CN=admin2,CN=Users,DC=anshsinh,DC=local" simple
15337	2020-09-30 01:21:40.972004	10.106.32.104	10.127.197.180	LDAP	88		bindResponse(2) success

## Análise de log

### Verifique o servidor da porta.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_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
```

## Verifique o ise-psc.log

Nesses registros, você pode verificar a política de RBAC usada para o usuário admin2 quando tentar acessar o recurso de dispositivo de rede -

```
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
```