

Authentication

Authorization >

Administrators >

Settings >

GUI and CLI Password Policy

* Minimum Length: 4 characters (Valid Range 4 to 127)

Password must not contain:

- Admin name or its characters in reverse order
- *cisco* or its characters in reverse order
- This word or its characters in reverse order: _____
- Repeated characters four or more times consecutively
- Dictionary words, their characters in reverse order or their letters replaced with other characters ⓘ
 - Default Dictionary ⓘ
 - Custom Dictionary ⓘ No file selected.

The newly added custom dictionary file will replace the existing custom dictionary file.

Authentication

Authorization >

Administrators >

Settings >

Password must contain at least one character of each of the selected types:

- Lowercase alphabetic characters
- Uppercase alphabetic characters
- Numeric characters
- Non-alphanumeric characters

Password History

- Password must be different from the previous 3 versions [When enabled CLI remembers only last 1 password irrespective of value configured]

* Cannot reuse password within 15 days (Valid Range 0 to 365)

Password Lifetime

Admins can be required to periodically change their password

If Admin user is also configured as a network user, an expired enable password can cause the admin account to become disabled

- Administrator passwords expire 45 days after creation or last change (valid range 1 to 3650)
- Send an email reminder to administrators 30 days prior to password expiration (valid range 1 to 3650)

إلى لقتنا، اذه نيوكتل. طشن ريغ لوؤسم مدختسم ليطعتل ريفوت ىل ع ISE يوتحي
 Administration > System > Admin Access > Authentication و Account Disable Policy.

Admin Groups		
Name	External Groups Mapped	Description
Customization Admin	0	Access Permission to Guest Menu and Device Portal Management.
ERS Admin	0	Full access permission to External RESTful Services (ERS) APIs. Admins ...
ERS Operator	0	Read-only access permission to the External RESTful Services (ERS) API...
Elevated System Admin	0	Access permission for Operations tab. Includes System and data access ...
Helpdesk Admin	0	Access permission for Operations tab.
Identity Admin	0	Access permission for Operations tab. Includes Identity Management and...
MnT Admin	0	Access permission for Operations tab.
Network Device Admin	0	Access permission for Operations tab. Includes Network Resources and ...
Policy Admin	0	Access permission for Operations and Policy tabs. Includes System and I...
RBAC Admin	0	Access permission for Operations tab. Includes System and data access ...
Read Only Admin	0	Access Permission for admin with read-only functionality
SPOG Admin	0	This is the group for SPOG Admin to use the APIs for export and import
Super Admin	0	Access permission for Operations, Policy and Administration tabs. Includ...
System Admin	0	Access permission for Operations tab. Includes System and data access ...

كلت إلى ني يراد ني م دختسم ة فاضال ري رحت قوف رقن او ة ومجم ل ادح ، ة ومجم عاشن إدجم ب
 ISE إلى ني لوؤسم ل ة ومجم إلى ة ي ج راخ ال ة ي وه ل ة ومجم ني ع تل ريفوت كانه . ة ومجم ل
 عونك عون ل ادح ، اذه ني وكتل . ة بول طم ل ة ان و ذال إلى ع ي ج راخ لوؤسم م دختسم لصح ي شي ح ب
 م دختسم ل ة فاضال ة ان ة ي ج راخ .

Admin Group	
* Name	Super Admin
Description	Access permission for Operations, Policy and Administration tabs. Includes data access permission for Admin Groups, User Identity Groups, Endpoint Identity Groups, All Locations and All Device Types.
Type	<input checked="" type="checkbox"/> External
External Identity Source	Name :
External Groups	Select an item
Member Users	Users
	<input type="checkbox"/> <input checked="" type="checkbox"/> Enabled
	admin

لوؤسم ل ة ومجم ني وكت

ةديج ةسايس عاشنإ نكمي وأ اهصيصخت.

> لوؤسمل لوصول > ماطنل > ةرادإل ىلإ لقتنا ، ةمئاقلا ىلإ لوصول ةسايس نيوكتل
> ةمئاقلا لوصول > نوذأ > ليوختلا

Cisco ISE Administration • System

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

Authentication

Authorization

Permissions

Menu Access

Data Access

RBAC Policy

Administrators

Settings

Menu Access

Edit Add Duplicate Delete

<input type="checkbox"/>	Name	Description
<input type="checkbox"/>	Super Admin Menu Access	Access permission for Operations tab, Policy tab, Guest Access tab, Mobile Device Management tab
<input type="checkbox"/>	Policy Admin Menu Access	Access permission for Operations tab, Policy tab, Guest Access tab, Mobile Device Management tab,
<input type="checkbox"/>	Helpdesk Admin Menu Access	Access permission for Operations tab.
<input type="checkbox"/>	Identity Admin Menu Access	Access permission for Operations tab and Identity Management.
<input type="checkbox"/>	Network Device Menu Access	Access permission for Operations tab and Network Resources.
<input type="checkbox"/>	System Admin Menu Access	Access permission for Operations tab and System.
<input type="checkbox"/>	RBAC Admin Menu Access	Access permission for Operations tab and System.
<input type="checkbox"/>	MnT Admin Menu Access	Access permission for Operations tab.
<input type="checkbox"/>	Customization Admin Menu Access	Access Permission to Guest Menu and Device Portal Management.
<input type="checkbox"/>	TACACS+ Admin Menu Access	Access Permission to Operations, Administration and Workcenter

مئيل ISE ف لقتنلا تاراخي نم راخي لك نيوكتل نكمي (Add) ةفاضل قوف رقننا
جهن في هؤافخ/هضرع

Cisco ISE Administration • System

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

Menu Access List > New RBAC Menu Access

Create Menu Access Permission

* Name: Custom_Menu_Access

Description:

Menu Access Privileges

Permissions for Menu Access

Show Hide

ISE Navigation Structure

- > Policy
- > Administration
 - > System
 - Deployment
 - Licensing
 - > Certificates
 - > Certificate Manage
 - System Certificates
 - Trusted Certificates

لوؤسملال لوصولو > ماظنل > ةرادالال ل لقتنا، تانايبال ل لوصولو ةسايس نيوكت > تانايبال ل لوصولو > نوذا > ليوختل >

Cisco ISE Administration • System Evaluation Mode ?

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

Authentication

Authorization

Permissions

Menu Access

Data Access

RBAC Policy

Administrators

Settings

Data Access

Edit Add Duplicate Delete

Name	Description
Super Admin Data Access	Access permission for Admin Groups, User Identity Groups, Endpoint Identity Groups, All Locations and All Device Types.
Policy Admin Data Access	Access permission for User Identity Groups and Endpoint Identity Groups.
Identity Admin Data Access	Access permission for User Identity Groups and Endpoint Identity Groups.
Network Admin Data Access	Access permission for All Locations and All Device Types.
System Admin Data Access	Access permission for Admin Groups.
RBAC Admin Data Access	Access permission for Admin Groups.
Customization Admin Data Access	
TACACS+ Admin Data Access	Access permission for All Locations and All Device Types, User Identity groups and End point identity groups.
Read Only Admin Data Access	Access permission for All Locations and All Device Types, User Identity groups and End point identity groups.

ةيوه لوصولل تانوذال نيوكتو ديدج چهن ءاشنال ةفاضل قوف رقن ةكبشلل تاومجم/ةياهنل ةطقن ةيوه/مدختسملال/لوؤسملال

Cisco ISE Administration • System

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

Authentication

Authorization

Permissions

Menu Access

Data Access

RBAC Policy

Administrators

Settings

Create Data Access Permission

* Name Custom_Data_Access

Description

Data Access Privileges

Permissions for Data Access

- Full Access
- Read Only Access
- No Access

- Admin Groups
- User Identity Groups
- Endpoint Identity Groups
 - Blacklist
 - GuestEndpoints
 - RegisteredDevices
 - Unknown
 - Profiled
 - Network Device Groups

RBAC تاسايس نيوكت

(ةرادالال ةومجم) رودل نيوكت نكمي. راوذالال ل دنتسملال لوصولو يف مكحتل RBAC لثمي

ةبولطملا تانايبلا ىل لوصول او ةمئاقلا جهن مادختسا ل مدختسمل ا هيل يمتني يذلا نكمي ةددعتم راودأ وا دحاو رودل اهنويوكت مت ةددعتم RBAC تاسايس كانه نوكت نا نكمي تاسايسلا هذه عيجم مييقت متي . تانايبلا وا/و ةمئاقلا ىل لوصول دحاو جهن ي اهنويوكت عومجم وه يئاهنلا رارقلاو . عارج ذيفنت لوؤسم مدختسم لواحي امدنع قيبتلل ةلباقلا يفتن وحمست ةضقانتم دعاوق كانه تناك اذ . رودلا كلذ ىلع ةقبتنملا تاسايسلا عيجم لقتنا ، تاسايسلا هذه نيويوكتل . ضفرلا ةدعاوق يغلتي حيرصتلا ةدعاوق نإف تقولا سفن ي RBAC جهن > ضيوفتلا > لوؤسملا ىل لوصول > ماظنلا > ةرادلا ىل

Cisco ISE Administration • System Evaluation

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

Authentication

Authorization

Permissions >

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 element). Note that system-created and default policies cannot be deleted. For decision making, all applicable policies will be evaluated. The subject's permissions will be the aggregate of all permissions from each applicable policy.

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 Policy	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"/> MnT Admin Policy	If MnT Admin	+ then MnT Admin Menu Access + Actions
<input checked="" type="checkbox"/> Network Device Policy	If Network Device Admin	+ then Network Device Menu Access ... + Actions
<input checked="" type="checkbox"/> Policy Admin Policy	If Policy Admin	+ then Policy Admin Menu Access a... + Actions
<input checked="" type="checkbox"/> RBAC Admin Policy	If RBAC Admin	+ then RBAC Admin Menu Access a... + Actions

جهن فذح/جاردإ/ةفعاضملا تاءارجا قوف رقنا

الو ، ةيضا رتفال تاسايسلا او ماظنلا اهأش نا يتلا تاسايسلا شي دحت نكمي ال : ةظالم ةيضا رتفال تاسايسلا فذح نكمي .

ةدحاو ةدعاوق ي تانايبلا/ةمئاقلا ىل لوصول ةددعتم تانوذأ نيويوكت نكمي ال : ةظالم

لوؤسملا لوصول تاداعا نيويوكت

نوكت يتلا او اهنويوكت نكمي يتلا تاداعا ال ضعب كانه ، RBAC تاسايس ىل ةفاضل اب لوؤسملا يمدختسم عيجملا ةكرتشم .

in order to GUI و CLI ل ةيار post-login و pre-login ، حمسي ةسلج ىصقأ نم مقرلا تلكش ، بيوبتلا ةمالع نمض هذه نيويوكتب مق . ذفنم > تاداعا > > ذفنم Admin > ماظن > ةرادا ىل لقتنا لمعلا ةسلج .

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

Authentication
 Authorization >
 Administrators >
 Settings >
 Access
 Session
 Portal Customization

Session IP Access MnT Access

GUI Sessions

Maximum Concurrent Sessions: 10 (Valid Range 1 to 20)

Pre-login banner

Welcome to ISE

Post-login banner

CLI Sessions

Maximum Concurrent Sessions: 5 (Valid Range 1 to 10)

Pre-login banner

ةيموسرلا مدختسملا هجاو ىل اهل الخ نم لوصولو نكمي يتلا IP نيوانع ةمئاق نيوكتل > تاداع | > ةرادال ىل لوصولو > ماظنلا > ةرادال ىل لقتنا، (CLI) رماوال رطس هجاوو (GUI) > تاداع | > ةرادال ىل لوصولو > ماظنلا > ةرادال ىل لقتنا و لوصولو IP Access بيوبتل ةمالع ىل لقتنلا و لوصولو.

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

Authentication
 Authorization >
 Administrators >
 Settings >
 Access
 Session
 Portal Customization

Session **IP Access** MnT Access

Access Restriction

Allow all IP addresses to connect

Allow only listed IP addresses to connect

Configure IP List for Access Restriction

IP List

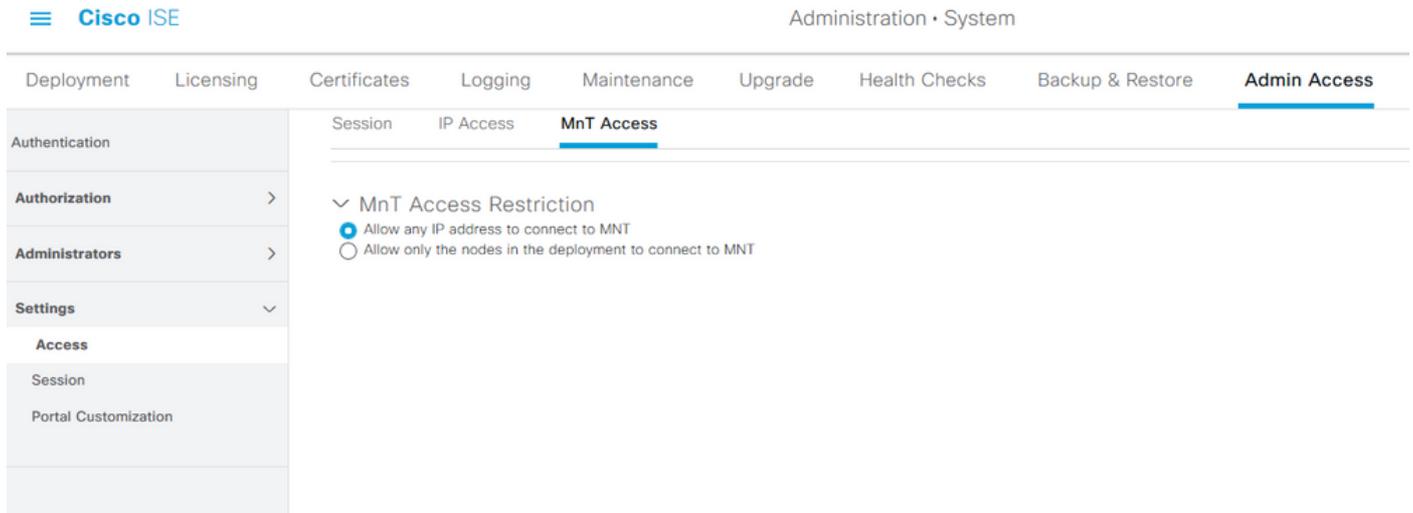
+ Add Edit Delete

IP	MASK
<input type="checkbox"/> 10.9.8.0	24

Cisco ISE يف اهنم MnT مسق ىل لوصولو ني لوؤسمل نكمي يتلا دقعلا نم ةمئاق نيوكتل ىل لقتنلا و لوصولو > تاداع | > لوؤسمل ىل لوصولو > ماظنلا > ةرادال ىل لقتنا، ISE، MnT لوصولو بيوبتل ةمالع.

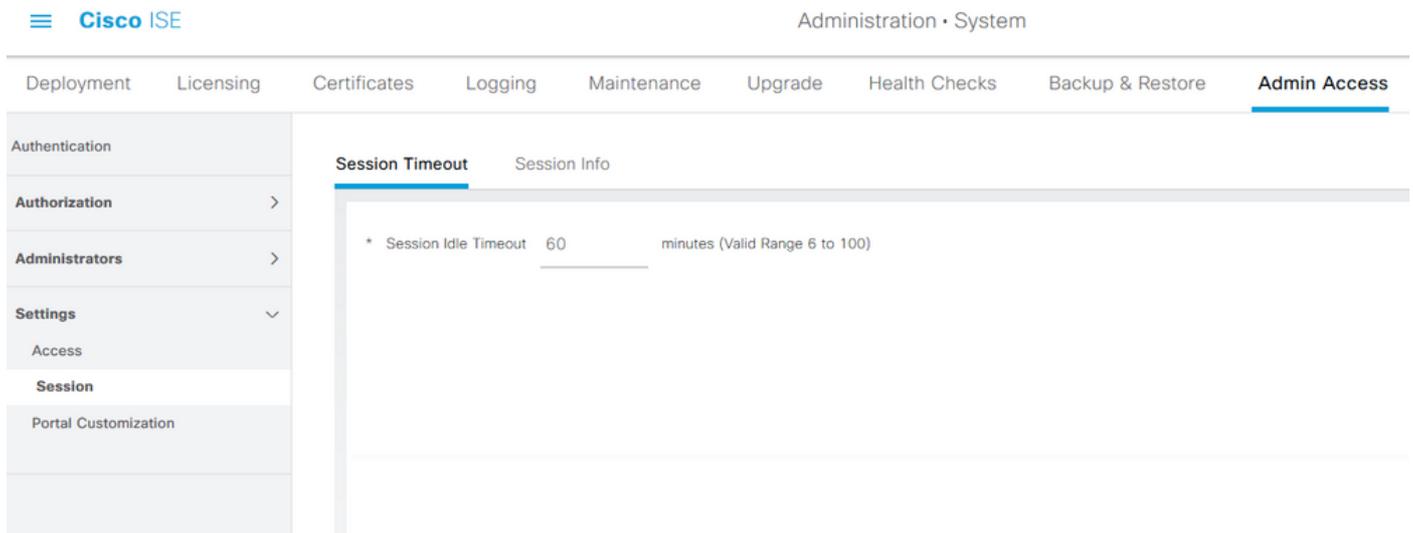
قوف رقنا، MnT ىل syslog لاسراب رشنلا جراخ و رشنلا لخاد اما تاناكلا و دقعلا حامس لل

ةدوجوملا تانايكلا وأ دقعلل طقف حامسلل MNT وي دار رزب لاصتالاب IP ناونع يأل حامسلل رشنلا يف ةدوجوملا دقعلل طقف حامسلل قوف رقنا ، MNT لىل syslog لاسراب رشنلا نمض MNT وي دار رزب لاصتالاب



ةمدخ" مادختسا لىل لغشت متي ، ثدحأل تارادصل او ISE 2.6 حى حصتلا ةبسنلاب :ةظحالم جم دب حمسي الام ، يضارتفا لكشب MNT لىل UDP Syslogs لىل صوتل "ISE ةلسارم رشنلا جراخ ىرخأ تانايك يا نم ةمداقلا syslog

ريدم >ماظن >ةرادا لىل لقتنا ، ةسلج نم طاشن مدع لىل بجاو ةميقي لىل طعتت لكش in order to لمعلا ةسلج ةلهم بيوبتلا ةمالع نمض ةميقيلا هذه نييعت ب مق . ةسلج >دادع لىل لمع >ذفنم



ةسلج > تادادع لىل لوؤسمل لوصو > ةرادا لىل لقتنا ، ةيلاحلا ةطاشنلا تاسلجلا لاطب لىل ضرع ل لمعلا ةسلج تامولعم بيوبتلا ةمالع قوف رقناو لمعلا

Authentication

Authorization >

Administrators >

Settings v

Access

Session

Portal Customization

Session Timeout

Session Info

Select session and terminate

Session Info

Invalidate

	UserID	IP Address	Session Creation Time	Session Last Accessed
<input type="checkbox"/>	admin	10.65.48.253	Fri Oct 09 01:16:59 IST 2020	Fri Oct 09 01:45:10 IST 2020

دامت عا تاناي ب مادختساب لوؤس م لا لخدم ى ل لوصول ني وكت AD

AD ى ل ISE مامضنا

> ةي ج راخ ل ةي و ه ل رداصم > ةي و ه ل ةراد > ةراد ى ل ل ق ت ن ا ، ةي ج راخ ل ا ج م ى ل ISE م ض ل ج ا ن م دامت عا تاناي ب ل خ د ا . Active Directory ل ا ج م و ة د ي د ج ل ط ب ر ل ا ة ط ق ن م س ا ل خ د ا . Active Directory قوف ر ق ن ا م ت ، ا ه ي ل ع ت ا ر ي ي غ ت ا ر ج ا و ر ت و ي ب م ك ل ل ت ا ن ئ ا ك ة ف ا ض ا ه ن ك م ي ي ذ ل ا AD با س ح ق ف ا و م .

Identities

Groups

External Identity Sources

Identity Source Sequences

Settings

External Identity Sources

<

📁

⚙️

> 📁 Certificate Authentication F

v 📁 Active Directory

👤 AD

📁 LDAP

📁 ODBC

📁 RADIUS Token

📁 RSA SecurID

📁 SAML Id Providers

📁 Social Login

Connection

Whitelisted Domains

PassiveID

Groups

Attributes

Advanced S

* Join Point Name

AD

📘

* Active Directory Domain

rinsantr.lab

📘

Join Domain

Please specify the credentials required to Join ISE node(s) to the Active Directory Domain.

* AD User Name 📘 Administrator

* Password ●●●●●●●●●●

 Specify Organizational Unit 📘 Store Credentials 📘

Cancel

OK

* Join Point Name	AD	i
* Active Directory Domain	rinsantr.lab	i

[+ Join](#) [+ Leave](#) [Test User](#) [Diagnostic Tool](#) [Refresh Table](#)

<input type="checkbox"/>	ISE Node	ISE Node R...	Status	Domain Controller	Site
<input type="checkbox"/>	rini-ise-30.gce.iselab.local	STANDALONE	<input checked="" type="checkbox"/> Operational	WIN-5KSMPOHEP5A.rinsantr.l...	Default-First-Site-Name

ليلدل تاعومجم دي دحت

مسا يلع رقنا **Active Directory** > ةي جراخلا ةي وهلا رداصم > ةي وهلا ةرادا > ةرادا يل لقتنا دي دحت > ةفاضل قوف رقنا. تاعومجم بيوبتلا ةمالع يل لقتناو ةبولطملا طبرلا ةطقن يمتني لقالا يلع ةدحاو AD ةومجم داري تساب مق. تاعومجم دادر تساب > ليلدلا نم تاعومجم طافح قوف رقنا م، قفاوم قوف رقنا م، لوؤسملا اهيلل

Identity Sources

Connection

Edit +

Na

No data available

Select Directory Groups

This dialog is used to select groups from the Directory.

Domain

Name Filter * SID Filter * Type Filter

<input type="checkbox"/>	Name	Group SID	Group Type
<input type="checkbox"/>	rinsantr.lab/Users/Enterprise Key Admins	S-1-5-21-1977851106-3699455990-29458652...	UNIVERSAL
<input type="checkbox"/>	rinsantr.lab/Users/Enterprise Read-only Domain ...	S-1-5-21-1977851106-3699455990-29458652...	UNIVERSAL
<input type="checkbox"/>	rinsantr.lab/Users/Group Policy Creator Owners	S-1-5-21-1977851106-3699455990-29458652...	GLOBAL
<input type="checkbox"/>	rinsantr.lab/Users/Key Admins	S-1-5-21-1977851106-3699455990-29458652...	GLOBAL
<input type="checkbox"/>	rinsantr.lab/Users/Protected Users	S-1-5-21-1977851106-3699455990-29458652...	GLOBAL
<input type="checkbox"/>	rinsantr.lab/Users/RAS and IAS Servers	S-1-5-21-1977851106-3699455990-29458652...	DOMAIN LOCAL
<input type="checkbox"/>	rinsantr.lab/Users/Read-only Domain Controllers	S-1-5-21-1977851106-3699455990-29458652...	GLOBAL
<input type="checkbox"/>	rinsantr.lab/Users/Schema Admins	S-1-5-21-1977851106-3699455990-29458652...	UNIVERSAL
<input checked="" type="checkbox"/>	rinsantr.lab/Users/Test Group	S-1-5-21-1977851106-3699455990-29458652...	GLOBAL

[Cancel](#) [OK](#)

[Edit](#) [+ Add](#) [Delete Group](#) [Update SID Values](#)

<input type="checkbox"/>	Name	SID
<input type="checkbox"/>	rinsantr.lab/Users/Test Group	S-1-5-21-1977851106-3699455990-2945865208-1106

AD ليرادال لوصول نيكم

Administration > System > Admin Access > Authentication. راڤيخ لادح، ةقداصم لبولسأ بيوبت ةمالع يف. ظفح قوف روناو ةيوهل رصم ةلدسنم لةمئاق ل نم AD دح. رورم لةمك لىل دننسم ل

The screenshot shows the Cisco ISE Administration console. The breadcrumb navigation is Administration > System > Admin Access > Authentication. The 'Authentication Method' is set to 'Password Based' (selected with a radio button). Below it, the 'Identity Source' is set to 'AD:AD' (selected in a dropdown menu). There is also an option for 'Client Certificate Based' which is not selected. A 'Save' button is visible at the bottom right.

AD ةومجم نييعة ل ISE لوؤسم ةومجم نيوك

رودل لىل ةدننسم ل (RBAC) لوصول ابم كحتل تانودأ ديحتب ليوختل لحمسي اذو نييعة و Cisco ISE لوؤسم ةومجم ديحتل AD. يف ةومجم لةيوضع لىل ادانتسا لوؤسم ل. ةرادال تاعومجم > نولوؤسم > لوؤسم لوصول > ماظن > ةراد لىل لقتنا، AD ةومجم لىل لك لذ رايتخال ةناخ دح، عون ل ل قح يف. "ةديجال ةرادال" ةومجم ل امسا لخداو ةفاصل قوف رونا ةومجم نييعة متيس لىل AD ةومجم دح، ةيخراخ تاعومجم ةلدسنم لةمئاق ل نم. يخراخ تاريغي لاسرا. (هالعل لىل دل تاعومجم ديحت مسق يف دحم وه امك) اهل هذه ني لوؤسم ل

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

Authentication

Authorization >

Administrators >

Admin Users

Admin Groups

Settings >

Admin Groups > ISE AD Admin Group

Admin Group

* Name ISE AD Admin Group

Description

Type External

External Identity Source
Name : AD

External Groups

* +

Member Users

Users

+ Add Delete

<input type="checkbox"/>	Status	Email	Username	First Name	Last Name
No data available					

ةرادإلا ةومجم RBAC تانوذأ نييعت

إلى لقتنا، قبا سلال مسقلا يف اهؤاشنإ مت يتلا ةرادإلا ةومجم إلى RBAC تانوذأ نييعت لتاءارجا ةلدسنملا ةمئاقلا نم RBAC جهن > ضيوفت > لوؤسمل لوصو > ماظن > ةرادإل مادختساب اهطيطختب مقو، ةديج ةدعاق عاشنإب مق. ديدج جهن چاردإ دح، نييمى إلى لىع ةدوجوملا ةمئاقلا إلى لوصولا تانوذأب انه نييعت مقو، هالع مسقلا يف ةفرعملا "ةرادإلا ةومجم" ظفح قوف رقنا م، ةبولطملا تاناي بلاو

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

Authentication

Authorization >

Permissions >

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 ci 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 Men... + Actions
<input checked="" type="checkbox"/> RBAC Policy 1	If ISE AD Admin Group	+ then Super Admin Menu Acces... X Actions
<input checked="" type="checkbox"/> Elevated System Admin Poli	If Elevated System Admin	+ then
<input checked="" type="checkbox"/> ERS Admin Policy	If ERS Admin	+ then
<input checked="" type="checkbox"/> ERS Operator Policy	If ERS Operator	+ then

Super Admin Menu Access +

Super Admin Data Access +

ةحصلال نم ققحتلاو AD دامتعا تانايب مادختساب ISE إلى لوصولا

نم طبرلا ةطقن مسا دح. ةيرادإلا (GUI) ةيموسرلا مدختسملا ةهجاو نم جورخلا ليجست AD، تانايب ةدعاق نم رورملا ةملكو مدختسملا مسا لخدأ. ةيوهال ردصم ةلدسنملا ةمئاقلا لوخدلا لىسو.



Identity Services Engine

Intuitive network security

Username
TestUser

Password
●●●●●●●●

Identity Source
AD

Login

نم هتقد اصم تم تي ذلا مدختسملا مسا نم ققحت، ححص لكشب لمعي نيوكتلنا أديكأتل لقتنا (ISE). ةيموسرلا مدختسملا ةهجاو نم نميال يولعل نكرلا يلع دوجوملا تاداعلا زمر مدختسملا مسا نم ققحتو مداخلا تامولعم لا

Server Information

Username: TestUser

Host: rini-ise-30

Personas: Administration, Monitoring, Policy
Service (SESSION,PROFILER)

Role: STANDALONE

System Time: Oct 27 2020 01:23:21 AM
Asia/Kolkata

FIPS Mode: Disabled

Version: 3.0.0.458

Patch Information: none

OK

LDAP مداخلتساب لوؤسملالخدمىلى لوصولانىوكت

LDAP لى ISE مامضنا

ةمالع تحت . Active Directory > LDAP > ةىجراخلاةوهلارداصم > ةىوهلارادا > ةرادىلى لقتنا
Active Directory ك ططخملالرتخاو LDAP ل مساللاخداب مق ،ماع بيوبتلا

External Identity Sources

- <  
- >  Certificate Authentication F
- ▼  Active Directory
 -  AD
 -  LDAP
 -  ODBC
 -  RADIUS Token
 -  RSA SecurID
 -  SAML Id Providers
 -  Social Login

LDAP Identity Sources List > New LDAP Identity Source

LDAP Identity Source

General

Connection

Directory Organization

Groups

Attribut

* Name

Description

▶ Schema ▼

لا تتبث، انه **لي صوت** بيوبت الة مالع ىل لقتنا، لاصت الة عون لى كشتل، كذ دعب راسم لخدأ 389(LDAP)/636 (LDAP-Secure) مانىم الة عم ياسا لدان LDAP ال نم hostname/IP LDAP م داخبة صاخ ال Admin رورم ةم لك مادختساب (DN) لوؤس ملل زيم ملل م س ال

- ▼  Active Directory
 -  AD
 -  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	<input type="text" value="10.127.196.131"/>	Hostname/IP	<input type="text"/>
* Port	<input type="text" value="389"/>	Port	<input type="text" value="389"/>
<input type="checkbox"/> Specify server for each ISE node			
Access	<input type="radio"/> Anonymous Access <input checked="" type="radio"/> Authenticated Access	Access	<input checked="" type="radio"/> Anonymous Access <input type="radio"/> Authenticated Access
Admin DN	<input type="text" value="* CN=Administrator,CN=Users,DC"/>	Admin DN	<input type="text" value="admin"/>
Password	<input password"="" type="password" value="*</td> <td>Password</td> <td><input type="/>		
Secure Authentication	<input type="checkbox"/> Enable Secure Authentication	Secure Authentication	<input type="checkbox"/> Enable Secure Authentication

رايتخال ةيمست الة اتا ايس قوف روناو لى لدل ةسسؤم بيوبت الة مالع ىل لقتنا، كذ دعب ني مدختس ملل لى لك يه الة لس لس الة ىل ادان س ا مدختس ملل لى ح ص الة اس سؤم الة ةوم جم LDAP م داخبة ي ف ةنخ ملل

General **Connection** Directory Organization Groups Attributes Advan

LDAP Server Root CA Cisco

Issuer CA of ISE Certificates Select

Ldap bind succeeded to 10.127.196.131:389
Number of Subjects 8
Number of Groups 50
Response time 7ms

OK

* Server Timeout 10 Seconds Server Tim

* Max. Admin Connections 20 Max. Adm

Force reconnect every Minutes

Test Bind to Server

> لېدلې نېم تاعومجم دېدحت > ؤفاضل قوف رقناو تاعومجم بېوېتلا ؤمالع ىل نآلا لقتنا
رقنا مٲ، لوؤس مالا هېلې ىم تنې ل قالا ىلع ؤدحاو ؤعومجم دارېت ساب مق. تاعومجم دادرتسا
ظفح قوف رقنا مٲ، قفاوم قوف

Select Directory Groups

This dialog is used to select groups from the Directory. Click **Retrieve Groups..** to read directory.

Filter: * Retrieve Groups... Number of Groups Retrieved: 50 (Limit is 100)

<input type="checkbox"/>	Name
<input type="checkbox"/>	CN=Server Operators,CN=Builtin,DC=rinsantr,DC=lab
<input type="checkbox"/>	CN=Storage Replica Administrators,CN=Builtin,DC=rinsantr,DC=lab
<input type="checkbox"/>	CN=System Managed Accounts Group,CN=Builtin,DC=rinsantr,DC=lab
<input type="checkbox"/>	CN=Terminal Server License Servers,CN=Builtin,DC=rinsantr,DC=lab
<input checked="" type="checkbox"/>	CN=Test Group,CN=Users,DC=rinsantr,DC=lab
<input type="checkbox"/>	CN=Users,CN=Builtin,DC=rinsantr,DC=lab
<input type="checkbox"/>	CN=Windows Authorization Access Group,CN=Builtin,DC=rinsantr,DC=lab

Cancel OK

Internal Identity Sources

- <
- > Certificate Authentication F
- > Active Directory
- ✓ LDAP
 - LDAPExample
 - ODBC
 - RADIUS Token
 - RSA SecurID

LDAP Identity Sources List > LDAPExample

LDAP Identity Source

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

Edit + Add Delete Group

<input type="checkbox"/>	Name
<input type="checkbox"/>	CN=Test Group,CN=Users,DC=rinsantr,DC=lab

LDAP يمدخستسمل يرا دال لوصول ني كمت

ىل لقتنا ، LDAP مادختساب رورملا ةملك ىل ةدنتسمل ISE ةقداصم ني كمتل
Administration > System > Admin Access > Authentication. ةقداصملا بولسا بيوبت ةمالع يف
رقناو ةيوهلا ردصم ةلدسنملا ةمئاقلا نم LDAP دح رورملا ةملك ىل دننتسمل راىخلا دح
ظفح ىل ع

Authentication

Authorization

Permissions

RBAC Policy

Administrators

Settings

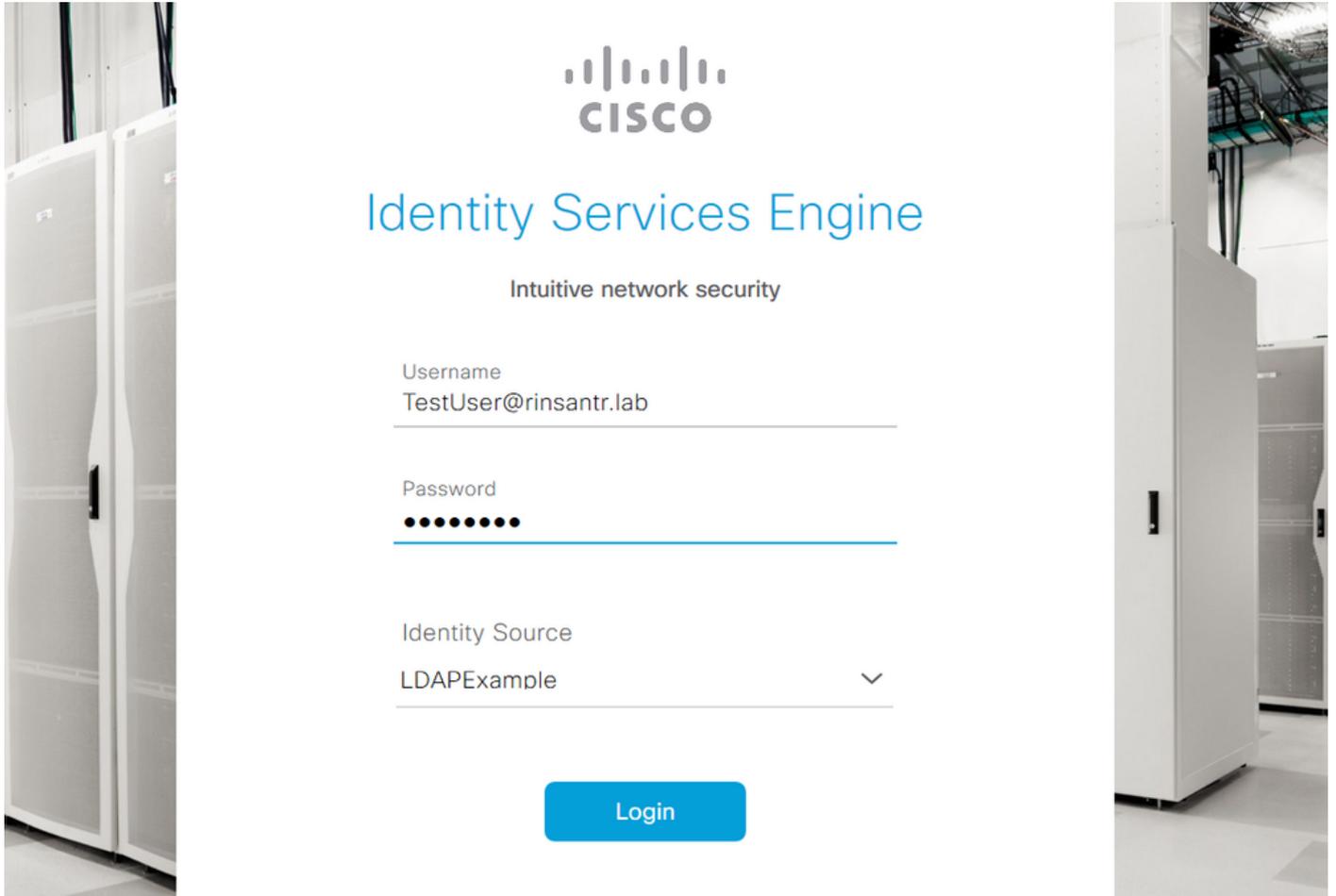
Create Role Based Access Control policies by configuring rules based on Admin groups, Menu Access permissions (menu items), Data Access permissions (identity group data element). Menu/Data Access permissions are not allowed on a single policy. You can copy the default policies shown below, then modify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

RBAC Policies

Rule Name	Admin Groups	Permissions
Customization Admin Policy	Customization Admin	Customization Admin Menu ...
RBAC Policy 2	ISE LDAP Admin Group	Super Admin Menu Access a...
Elevated System Admin Poli	Elevated System Admin	Super Admin Menu Access
ERS Admin Policy	ERS Admin	Read Only Admin Data Acces
ERS Operator Policy	ERS Operator	Super Admin Data Access
ERS Trustsec Policy	ERS Trustsec	Super Admin Menu Access
Healthsec Admin Policy	Healthsec Admin	Healthsec Admin Menu Access

تحصيل نام ققحت لاول LDAP دامتعا تانايب مادختساب ISE لى لوصول

ةمئاق لى نام LDAP مسا ددح .ةيرادلإا (GUI) ةيموسرلر مدختسمل ةهجاو نام جورخ لى لىجست لىجسو ، LDAP تانايب ةدعاق نام رورم لى ةم لك و مدختسمل مسا لىخدا .ةيوه لى ردىم ةلدىس نام لى لىل.



ةتقداصم تمت يذلى مدختسمل مسا نام ققحت ،حىحص لىكشب لمعى لىوكت لى نأ نام دكأت لى (ISE) .ةيموسرلر مدختسمل ةهجاو نام رىس لى لىل نىك رلى لىل دوجوم لى ادادع لى لى زمر نام مدختسمل مسا نام ققحت و مداخلى تامولعم لى لى لىل.



Server Information

Username: **TestUser@rinsantr.lab**

Host: **rini-ise-30**

Personas: **Administration, Monitoring, Policy
Service (SESSION,PROFILER)**

Role: **STANDALONE**

System Time: **Oct 27 2020 03:48:32 AM
Asia/Kolkata**

FIPS Mode: **Disabled**

Version: **3.0.0.458**

Patch Information: **none**

OK

ةمچرتل هذه لوج

ةللأل تاي نقتل نم ةومچم مادختساب دن تسمل اذه Cisco تچرت
ملاعلاء انءمچ يف نيمدختسمل معدى وتحم مي دقتل ةيرشبل او
امك ةقيد نوك تنل ةللأل ةمچرت لصف أن ةظحال مچرئ. ةصاغل مه تلبل
Cisco يلخت. فرتحم مچرت مامدقي يتل ةيفارتهال ةمچرتل عم لاعل وه
ىل إأمئاد ةوچرلاب يصوت وتامچرتل هذه ةقد نع اهتيلوئسم Cisco
Systems (رفوتم طبارل) يلصلأل يزىلچنل دن تسمل