## ىلع RBAC و لوؤسملا ىلا لوصولا جەن مەف ISE

## تايوتحملا

<u>ةمدقملا</u> <u>ةيساسألا تابلطتملا</u> تابلطتملا <u>ةمدختسملا تانوكملا</u> نىوكترا <u>ةقداصملا تادادعا</u> <u>ةرادالا تاعومجم نىوكت</u> لوؤسملا ىمدختسم نىوكت <u>تانوذألا نىوكت</u> <u>RBAC تاساىس نىوكت</u> <u>لوؤسملل لوصولا تادادعا نىوكت</u> <u>AD دامتعا تانایب مادختساب لوؤسملا لخدم یلا لوصولا نیوکت</u> AD <u>یل ISE مامضنا</u> <u>لىلدلا تاءومجم دىدحت</u> <u>AD ل يرادالا لوصولا نيكمت</u> <u>AD ةعومجم نييعتل ISE لوؤسم ةعومجم نيوكت</u> <u>ةرادإلا ةعومجمل RBAC تانوذاً نىىعت</u> <u>قحصلا نم ققحتلاو AD دامتعا تانايب مادختساب ISE ىلا لوصولا</u> LDAP مادختسات لوؤس مل الخدم <u>علا لوصولا نىوكت</u> LDAP <u>یل ISE</u> مامضنا LDAP <u>یمدختسمل یرادالا لوصولا نی</u>كم<u>ت</u> <u>LDAP ةعومجم ىلا ISE لوؤسم ةعومجم نېيعت</u> <u>ةرادالاا ةعومجمل RBAC تانوذا نىىعت</u> <u>قحصلا نم ققحتلاو LDAP دامتعا تانايب مادختساب ISE ىلا لوصولا</u>

## ةمدقملا

الف فصي Identity Services Engine (ISE). كان عيرادإل المصول المراد العالي المراجع المراجع العامي المراجع المراجع

## ةيساسألا تابلطتملا

### تابلطتملا

:عوضوم اذه نم ةفرعم تنأ ىقلتي نأ يصوي cisco

- (ISE) ةيوەلا فشك تامدخ كرحم •
- مدخ Active Directory
- (LDAP) ليلدلل لوصولل فيفخلا لوكوتوربلا •

### ةمدختسملا تانوكملا

ةيلاتلا ةيداملا تانوكملاو جماربلا تارادصإ ىلإ دنتسملا اذه يف ةدراولا تامولعملا دنتست

- Identity Services Engine 3.0
- كindows Server كيغشتال ماظن

ةصاخ ةيلمعم ةئيب يف ةدوجوملا ةزهجألاا نم دنتسملا اذه يف ةدراولا تامولعملا ءاشنإ مت. تناك اذإ .(يضارتفا) حوسمم نيوكتب دنتسملا اذه يف ةمدختسُملا ةزهجألا عيمج تأدب رمأ يأل لمتحملا ريثأتلل كمهف نم دكأتف ،ليغشتلا ديق كتكبش.

## نيوكتلا

#### ةقداصملا تادادعإ

نكمي .ISE لوح تامولعم يأ ىلإ لوصولل مەسفنأ ةقداصم ىلإ Admin ومدختسم جاتحي ةيوەلا نزخم وأ ISE يلخادلا ةيوەلا نزخم مادختساب لوؤسملا يمدختسم ةيوە نم ققحتلا ،تادادعإلا ەذە نيوكتل .ةداەش وأ رورم ةملك ةطساوب امإ ةلاصألا نم ققحتلا نكمي .يچراخلا نمض بولطملا ةقداصملا عون ددح .Admin Access > Authentication <ماظنلا > قرادإلا ىل قتنا .

≡ Cisco	ISE				Administration • System						
Deployment	Licensing	Certificates	Logging	Maintenance	Upgrade	Health Check	s Backup & Restore	Admin Access	Settings		
Authentication		Authentication	Method	Password Policy	Account Disat	le Policy Loc	ck/Suspend Settings				
Authorization	>	Authenticatio	on Type								
Administrators	>										
Settings	>	Password B	lased								
		* Identity Source	8								
		Internal		$\sim$							
		Client Certif	ficate Based								

مت اذإ .يضارتفا لكشب رورملا ةملك ىلإ ةدنتسملا ةقداصملا نيكمت متي :**قظحالم** ليغشت ةداعإ ىلإ كلذ يدؤيسف ،ليمعلا ةداهش ىلإ ةدنتسم ةقداصم ىلإ اذه رييغت رشنلا دقع ةفاك ىلع قيبطتلا مداخ.

نم (CLI) رماوألاا رطس ةەجاول رورملا ةملك ةسايس نيوكتب Identity Services Engine حمسي ال مدختسملا ةەجاو نم لكل رورملا ةملك ةسايس نيوكت نكمي .(رماوألاا رطس ةەجاو) CLI ىل لقتنا ،اذە نيوكتل .طقف (ISE) ةيموسرلا مدختسملا ةەجاو ربع CLI و (GUI) ةيموسرلا Administration (القرام الملائي الموصول System (الموتنا المائي الموتنا المائي) > Authentication (المولي الموتنا القتناو (قوداصمل) > Authentication (المولي المولي المولي المولي المولي المولي المولي المولي المولي المولي المولي

≡ Cisco	ISE	Administration • System								
Deployment	Licensing	Certificates Logging Maintenance Upgrade Health Checks Backup & Restore Admin Access	Settings							
Authentication		Authentication Method Password Policy Account Disable Policy Lock/Suspend Settings								
Authorization	>	GUL and CLI Password Policy								
Administrators	>									
Settings	>	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 ()         Browse No file selected.								
≡ Cisco	ISE	Administration • System	Evaluation Mode							
Deployment	Licensing	Certificates Logging Maintenance Upgrade Health Checks Backup & Restore Admin Access	Settings							
Authentication		Authentication Method Password Policy Account Disable Policy Lock/Suspend Settings								
Authorization	>	Password must contain at least one character of each of the selected types:								
Administrators	>	Lowercase alphabetic characters								
Settings	>	Uppercase alphabetic characters								
		Vumeric 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 config	ured]							
		Cannot reuse password within 15 days (Valid Range 0 to 365)								
		Password Lifetime								
		Admins can be required to periodically change their password								
		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								

ى الإلى القى الذى ني وكتل. طشن ريغ لوؤسم مدختسم ليطعتل ريفوت ىلع ISE ى الذى ني القتنا، اذه ني وكتل. Administration > System > Admin Access > Authentication بي وبتلا الم الع ىل Disable Policy.

days prior to password expiration (valid range 1 to 3650)

Send an email reminder to administrators 30

<b>≡</b> Cisco	ISE			Adm	inistration • S	ystem			4
Deployment	Licensing	Certificates	Logging	Maintenance	Upgrade	Health C	Checks	Backup & Restore	Admin Access
Authentication		Authenticatio	n Method	Password Policy	Account Disab	le Policy	Lock/Su	spend Settings	
Authorization	>	Account Di	isable Policy						
Administrators	>								
Settings	>	🗸 Dis	sable account after	r 30 days of ina	ctivity. (Valid range	1 to 365)			

ادانتسا اتقۇم ەفاقيإ وأ لوؤسم مدختسم باسح نيمأتل ةمزاللا تاليەستلا ISE رفوي امك لوصولا < ماظنلا < ةرادال ىل لوتنا ،اذە نيوكتل .ةلشافلا لوخدلا ليجست تالواحم ددع ىلإ تقۇملا فاقيال/لفقلا تادادعا بيوبتلا قمالع ىلإ لقتناو **ةقداصملا < لوؤسملا ىل** 

≡ Cisco	ISE	Administration • System
Deployment	Licensing	Certificates Logging Maintenance Upgrade Health Checks Backup & Restore Admin Access
Authentication		Authentication Method Password Policy Account Disable Policy Lock/Suspend Settings
Authorization	>	Suspend or Lock Account with Incorrect Login Attempts
Administrators	>	* Take action after 3 failed attempts (Valid Range 3 to 20)
Settings	>	<ul> <li>Suspend account for 15 minutes (Valid Range 15 to 1440)</li> </ul>
		C Lock account Email remediation message This account has been locked. For this account to become unlocked, please contact your IT helpdesk.

فلتخمو نيمدختسملاو ةيرادإلا تاعومجملل ةجاح كانه ،يرادإلا لوصولا ةرادإل اهترادإو مهتازايتما يف مكحتلل دعاوقلا/تاسايسلا.

#### ةرادإلا تاعومجم نيوكت

ىلإ لقتنا Administration (اماظنلا) > System (ماظنلا) > Admin Access (ماظنلا) > Administrators (نولوؤسملا) > Admin Groups (نولوؤسملا) > Administrators (تاعومجم نيوكتل اهفذح نكمي الو يضارتفا لكشب ةجمدم ةليلق تاعومجم كانه .نيلوؤسملا.

Administration · System

Deployment	Licensing	Certificates	Logging	Maintenance	Upgrade	Health Checks	Backup & Restore	Admin Access	Settings
Authentication		Adm	in Groups	6					
Authorization	>	2 Edit	LAM D. Dual	lianto 🛱 Doloto	Const All C	ut groups			
Administrators	~	e e e e e e e e e e e e e e e e e e e	- Add [] Dob	iicate 🖉 Delete	li Keset Ali E	xt. groups			
Admin Users			Name		External G	iroups Mapped	Description		
Admin Groups			8 Customization Ac	dmin	0		Access Permission to Guest Mer	u and Device Portal Manag	ement.
Sottings			8 ERS Admin		0		Full access permission to Externa	al RESTful Services (ERS) A	Pls. Admins
Jettinga	,		8 ERS Operator		0		Read-only access permission to	the External RESTful Servic	es (ERS) API
			B Elevated System	Admin	0		Access permission for Operation	s tab. Includes System and	data access
			8 Helpdesk Admin		0		Access permission for Operation	s tab.	
			🔱 Identity Admin		0		Access permission for Operation	s tab. Includes Identity Mar	nagement and
			🕵 MnT Admin		0		Access permission for Operation	s tab.	
			8 Network Device	Admin	0		Access permission for Operation	s tab. Includes Network Re	sources and
			8 Policy Admin		0		Access permission for Operation	s and Policy tabs. Includes	System and I
			8 RBAC Admin		0		Access permission for Operation	s tab. Includes System and	data access
			🔏 Read Only Admin	i	0		Access Permission for admin wit	h read-only functionality	
			SPOG Admin		0		This is the group for SPOG Admi	n to use the APIs for expor	t and import
			Super Admin		0		Access permission for Operation	s, Policy and Administration	tabs. Includ
			System Admin		0		Access permission for Operation	s tab. Includes System and	data access

كلت ىلإ نييرادإ نيمدختسم ةفاضإل ريرحت قوف رقناو ةعومجملا ددح ،ةعومجم ءاشنإ درجمب ISE ىلع نيلوؤسملا تاعومجم ىلإ ةيجراخلا ةيوهلا تاعومجم نييعتل ريفوت كانه .ةعومجملا عونك عونلا ددح ،اذه نيوكتل .ةبولطملا تانوذألا ىلع يجراخ لوؤسم مدختسم لصحي ثيحب مدختسملا ةفاضإ ءانثأ يجراخ.

	SE				Admi	nistration • System	n		
Deployment	Licensing	Certificates	Logging	Maintenance	Upgrade	Health Checks	Backup & Restore	Admin Access	Settings
Authentication		Admin Groups >	Super Admin						
Authorization	>	Admin Grou	q						
Administrators	~	* Name	Su	per Admin					
Admin Users Admin Groups		Description	Acce Adm	ss permission for Operati in Groups, User Identity G	ons, Policy and Adm roups, Endpoint Ider	inistration tabs. Includes dat itity Groups, All Locations an	a access permission for ad All Device Types.		
Settings	>	Type External Identity Name :	Source	External					
		✓ External	Groups						
		* <b>#</b> _s	Select an item	~	+				
		Member Us <sup>Users</sup> + Add ~	Gers Delete						
		Sta	itus	Email	Usernam	e First Nam	ne Last Name		
			Enabled		ä admin				

لوؤسملا يمدختسم نيوكت

# < لوؤسملا ىل لوصولا < ماظنلا < قرادال ىل لقتنا ،قرادال يمدختسم نيوكتل Administrators > Admin Users.

≡ Cisco	Cisco ISE Administration · System										
Deployment	Licensing	Certificates	Logging	Maintenance	Upgrade	Health Checks	Backup &	Restore	Admin Access	Settings	
Authentication		Admi	nistrator	rs							
Authorization	>										
Administrators	~	🖉 Edit	+ Add 🛞	Change Status	🛱 Delete 📋 Dup	licate					
Admin Users						_					
Admin Groups			Status N	ame	Description	First Name	Last Name	Email Add	ress Admin Gro	ups	
			🖌 Enabled	admin 🔋	Default Admin U	ser			Super Admir	1	
Settings	>										

ديدج مدختسم ةفاضإ وه لوألاا .امەنېب نم رايتخالل نارايخ كانە .**(Add) ةفاضإ** قوف رقنا يلخاد مدختسمك ەنيوكت مت مدختسم يأ) ةكبشلا ىلإ لوصولا مدختسم لعج وه رخآلاو .امامت الوؤسمك (قزەجألا/ةكبشلا ىلإ لوصول

≡ Cisco	SE		Administration • System										
Deployment	Licensing	Certificates	Logging	Maintenance	Upgrade	Health Checks	Backup & R	estore Adm	nin Access	Settings			
Authentication		Admi	nistrator	S									
Authorization	>												
Administrators	~	🖉 Edit -	+ Add 🛛 🛞 🤇	Change Status	Delete 📋 D	uplicate							
Admin Users													
Admin Groups			Create an Admi	n User	Description	First Name	Last Name	Email Address	Admin Gro	oups			
			Select from Net	work Access Users	Default Admin	User			Super Adm	'n			
Settings	>												

ادانتسا نيمدختسملا ةعومجم ديدحتو ةبولطملا ليصافتلا ريفوت بجي ،رايخ ديدحت دعب مدختسملل امحنم متي تازايتمالاو تانوذالا يأ ىلإ

#### 

#### Administration · System

Deployment	Licensing	Certificates Logging Maintenance	e Upgrade Health Checks	Backup & Restore	Admin Access	Settings
Authentication		Administrators List > New Administrator				
Authorization	>	✓ Admin User				
Administrators	~	* Name Test_Admin				
Admin Users		Status 🗹 Enabled 🗸				
Admin Groups		Email testadmin@abcd.com	Include system alarms in emails			
Settings	>	External 🧻 🤅				
		Read Only				
		Inactive account never disabled				
		<ul> <li>Password</li> <li>* Password</li> <li>* Re-Enter Password</li> <li>Generate Password</li> </ul>	0 0			
		✓ User Information First Name				
		Last Name	Admin Groups	_		
		V Account Options	Customization Admin     ERS Admin     ERS Operator	<b>^</b>		
		<ul> <li>✓ Admin Groups</li> <li>*</li> <li>#</li> </ul>	Elevated System Admin     Helpdesk Admin     Identitv Admin	~		

#### تانوذألا نيوكت

نيمدختسم ةعومجمل اەنيوكت نكمي يتلا تانوذألا نم ناعون كانە:

#### ةمئاقلا ىلإ لوصولا .1

تانايبلا يلإ لوصولا .2

ببيوبت لكل نارايخ كانه .ISE ىلع لقنتلا ةيؤر ةيناكمإ يف ةمئاقلا ىلإ لوصولا مكحتي، تامالع راهظإل ةمئاقلا ىلإ لوصولا ةدعاق نيوكت نكمي .هنيوكت نكمي ،ءافخإ وأ راهظإ اهئافخإ وأ ةددحملا بيوبتلا.

نكمي .ISE ىلع قېوەلا تانايب لېدعت/لوصولا/ةءارق قېناكمإ يف Data Access مكحتي قېوە تاعومجمو مدختسملا قېوە تاعومجمو نېلوؤسملا تاعومجمل طقف لوصولا نذإ نېوكت نكمي ISE ىلع تانايكلا ەذەل تارايخ قثالث كانە .قكبشلا قزەجأ تاعومجمو قېاەنلا قطقن اەيلإ لوصولا نكمي الو طقف قءارقلل لوصو قېناكماو قلماك لوصو قېناكمإ يەف .اەنيوكت قمالع لكل قثالثلا تارايخلا ەذە دحأ رايتخال تانايبلا ىلإ لوصولا قدعاق نيوكت نكمي ISE.

ةعومجم يأ ىلع اەقيبطت لـبق تانايبلا ىلإ لوصولاو ةمئاقلا ىلإ لوصولا جەن ءاشنإ بجي امئاد نكمي نكلو يضارتفا لكشب ةنمضم نوكت يتلا تاسايسلا ضعب كانە .لوؤسم ةديدج ةسايس ءاشنإ نكمي وأ اهصيصخت.

#### < **لوؤسملا لوصو < ماظنلا < ةرادالا** ىلإ لقتنا ،ةمئاقلا ىلإ لوصولا ةسايس نيوكتل **ةمئاقلا لوصو < نوذأ < ليوختلا**.

≡ Cisco IS	SE	Administration • System									
Deployment	Licensing	Certificates	Logging	Maintenance	Upgrade	Health Checks	Backup & Restore	Admin Access			
Authentication		Men	u Access	;							
Authorization	~										
Permissions	~	0 Edit	+ Add Du	plicate 🍵 Delete	9						
Menu Access			Name		Description						
Data Access			Super Admin Menu	Access	Access permission	for Operations tab, Policy	tab, Guest Access tab, Mobile	Device Management tab			
RBAC Policy			Policy Admin Menu	Access	Access permission	for Operations tab, Policy	tab, Guest Access tab, Mobile	Device Management tab,			
			Helpdesk Admin M	enu Access	Access permission	for Operations tab.					
Administrators	>		Identity Admin Mer	nu Access	Access permission	for Operations tab and Ide	ntity Management.				
Settings	>		Network Device M	enu Access	Access permission	for Operations tab and Ne	twork Resources.				
			System Admin Mer	nu Access	Access permission	for Operations tab and Sys	stem.				
			RBAC Admin Menu	Access	Access permission	for Operations tab and Sys	stem.				
			MnT Admin Menu	Access	Access permission	for Operations tab.					
			Customization Adm	nin Menu Access	Access Permission	to Guest Menu and Device	e Portal Management.				
			TACACS+ Admin N	lenu Access	Access Permission	to Operations, Administrat	ion and Workcenter				

#### متيل ISE يف لقنتلا تارايخ نم رايخ لك نيوكت نكمي .**(Add) ةفاضإ** قوف رقنا جەن يف مۇافخ<u>|</u>/ەضرع.

#### ■ Cisco ISE

Deployment	Licensing	Certificates	Logging	Maintenance	Upgrade	Health Checks	Backup & Restore	Admin Access
Authentication		Menu Access L Create Me	ist > New RBAC	Menu Access Permission				
Authorization	~	* Name	0					
Permissions	~		Custom_Men	u_Access				
Menu Access		Description:						
Data Access								-
RBAC Policy		Menu Ac	gation Structu Policy	ges	Permissions for Me	nu Access		
Administrators	>	~ d	Administratio	n	O Hide			
Settings	>		<ul> <li>♂ System</li> <li>♂ Deployment</li> <li>☆ Licensing</li> <li>√ ♂ Certificate</li> <li>√ ♂ Certificate</li> <li>√ ♂ System</li> <li>♂ Trusted</li> </ul>	ess ate Manage Certificates Certificates				

Administration • System

#### لوؤسملا ىل ل لوصولا < ماظنلا < قرادالا ىل ل قرتنا ،تانايبلا ىل ل وصولا ةسايس نيوكتل تانايبلا ىل لوصولا < نوذأ < ليوختلا <.

	SE			Adm	inistration • S	vstem		4	Evaluation Mode 78
Deployment	Licensing	Certificates	Logging	Maintenance	Upgrade	Health Checks	Backup & Restore	Admin Access	Settings
Authentication		Data	Access						
Authorization	~	Data	100000						:
Permissions Menu Access	~	/ Edit -	+ Add Dut	olicate 🍵 Delete					
Data Access			ame	De	escription				
RBAC Policy		□ St	uper Admin Data Ad	ccess A	ccess permission fo	r Admin Groups, User Ide	ntity Groups, Endpoint Identity (	Groups, All Locations and	All Device Types.
		D Po	olicy Admin Data Ad	ccess A	ccess permission fo	r User Identity Groups an	d Endpoint Identity Groups.		
Administrators	>	🗌 Id	entity Admin Data	Access A	ccess permission fo	r User Identity Groups an	d Endpoint Identity Groups.		
Settings	>		etwork Admin Data	Access A	ccess permission fo	r All Locations and All De	vice Types.		
		🗆 S)	ystem Admin Data /	Access A	ccess permission fo	r Admin Groups.			
			BAC Admin Data Ac	cess A	ccess permission fo	r Admin Groups.			
			ustomization Admin	Data Access					
		□ T/	ACACS+ Admin Dat	a Access A	ccess permission fo	r All Locations and All De	vice Types, User Identity group:	s and End point indentity g	roups.
		R	ead Only Admin Dat	ta Access A	ccess permission fo	r All Locations and All De	vice Types, User Identity group:	s and End point indentity g	roups.

#### ةيوه ىلإ لوصولل تانوذألا نيوكتو ديدج جهن ءاشنإل **ةفاضإ** قوف رقنا ةكبشلا تاعومجم/ةياهنلا ةطقن ةيوه/مدختسملا/لوؤسملا.

#### Administration · System Deployment Licensing Certificates Logging Maintenance Upgrade Health Checks Backup & Restore Admin Access Create Data Access Permission Authentication \* Name Custom\_Data\_Access Authorization Description Permissions Menu Access Data Access Data Access Privileges Permissions for Data Access RBAC Policy Full Access > 💪 Admin Groups of User Identity Groups O Read Only Access Administrators ♂ Endpoint Identity Groups O No Access Settings Blacklist GuestEndpoints ♂ RegisteredDevices 🔥 Unknown > of Profiled network Device Groups

#### RBAC تاسايس نيوكت

(ةرادإلا ةعومجم) رودلا نيوكت نكمي .راودألا ىلإ دنتسملا لوصولا يف مكحتلا RBAC لثمي

ةبولطملاا تانايبلا ىل لوصولاو ةمئاقلا جەن مادختسال مدختسملا ەيلإ يمتني يذلا. نكمي ةددعتم راودأ وأ دحاو رودل اەنيوكت مت ةددعتم RBAC تاسايس كانە نوكت نأ نكمي تاسايسلا ەذە عيمج مييقت متي .تانايبلا وأ/و ةمئاقلا ىل لوصولل دحاو جەن يف اەنيوكت عومجم وە يئاەنلا رارقلاو .ءارجإ ذيفنت لوؤسم مدختسم لواحي امدنع قيبطتلل ةلباقلا يفنت و حمست قضقانتم دعاوق كانە تناك اذإ .رودلا كلذ ىلع ةقبطنملا تاسايسلا عيمج لقتنا ،تاسايسلا ەذە نيوكتل .ضفرلا قدعاق يغلت حيرصتلا قدعاق ناف يف يفنت الا من يوكت . ماظنلا الا يول

≡ Cisco	ISE			Д	dministration • Sys	stem				🛕 E	ivalua
Deployment	Licensing	Certificates	Logging	Maintenan	ce Upgrade	Health Chec	:ks	Backup & Restore	Admin A	Access	Se
Authentication		Create Role Ba multiple Menu and default po	ased Access Control po /Data Access permissio plicies cannot be deleter	licies by configurir ns are not allowed d.For decision mak	ng rules based on Admin gro on a single policy. You can ing, all applicable policies w	oups,Menu Access p copy the default po vill be evaluated. The	permission licies show e subject's	s (menu items), Data Access perr vn below,then modify them as ner s permissions will be the aggrega	nissions (iden eded. Note the te of all permi	tity group data e at system-create ssions from eact	ed an h app
Authorization	~	policies are di	splayed in alphabetical	order of the policy	name).						
Permissions	>	∽ RBAC	Policies								
RBAC Policy			Rule Name	А	dmin Groups		Permis	sions			
		<b>~</b>	Customization Admin	n Policy If	Customization Admin	+	then	Customization Admin Menu	+	Actions ~	
Administrators	>	<b>~</b>	Elevated System Ad	min Poli If	Elevated System Admin	n +	then	System Admin Menu Access	+	Actions $\sim$	
Settings	>	<b>~</b>	ERS Admin Policy	If	ERS Admin	+	then	Super Admin Data Access	+	Actions ~	
		<b>~</b>	ERS Operator Policy	If	ERS Operator	+	then	Super Admin Data Access	+	Actions ~	
		V	ERS Trustsec Policy	If	ERS Trustsec	+	then	Super Admin Data Access	+	Actions $\vee$	
		<b>~</b>	Helpdesk Admin Pol	icy If	Helpdesk Admin	+	then	Helpdesk Admin Menu Acce	ss +	Actions ~	
		V	Identity Admin Polic	y If	Identity Admin	+	then	Identity Admin Menu Access	+	Actions $\checkmark$	
		V	MnT Admin Policy	If	MnT Admin	+	then	MnT Admin Menu Access	+	Actions $\vee$	
		<b>~</b>	Network Device Poli	cy If	Network Device Admin	+	then	Network Device Menu Acces	+	Actions ~	
		V	Policy Admin Policy	If	Policy Admin	+	then	Policy Admin Menu Access	+	Actions ~	
			RBAC Admin Policy	If	RBAC Admin	+	then	RBAC Admin Menu Access a	+	Actions ~	

جەن ڧذح/جاردإ/ةڧعاضمل **تاءارجإ** قوڧ رقنا.

الو ،ةيضارتفالا تاسايسلاو ماظنلا اهأشنأ يتلا تاسايسلا ثيدحت نكمي ال :**قظحالم** ةيضارتفالا تاسايسلا فذح نكمي.

.ةدحاو ةدعاق يف تانايبلا/ةمئاقلا ىلإ لوصولل ةددعتم تانوذأ نيوكت نكمي ال :**ةظحالم** 

#### لوؤسملل لوصولا تادادعإ نيوكت

نوكت يتلاو اەنيوكت نكمي يتلا تادادعإلا ضعب كانە ،RBAC تاسايس ىلإ ةفاضإلاب لوؤسملا يمدختسم عيمجل ةكرتشم.

in order to و GUI ل ةيار post-login و pre-login ،حمسي ةسلج ىصقأ نم مقرلاا تلكش GUI، بيوبتلا ةمالع نمض هذه نيوكتب مق .**ذفنم<تادادعإ<ذفنم Admin ماظن<قرادإ** ىلإ لقتنا ل**معلا قسلج**.

=	Ci	e	<b>c</b> 0	. 1	5	F
_		2	υU		0	

Deployment	Licensing	Certificates	Logging	Maintenar	nce	Upgrade	Health Checks	Backup & Resto	re	Admin Access
Authentication		Session	IP Access	MnT Access						
Authorization	>									
Administrators	>									
A	,	GUI S	essions							
Access	~									
Session		Maximum Co	oncurrent Sessions	10	(Valid Ra	inge 1 to 20)				
Portal Customizati	on	Pre-log	in banner	Welcome to ISE	Ę					
		<b>1</b> 10 103								
		Post-lo	gin banner							
		CLI Se	essions							
		Maximum Co	oncurrent Sessions	5	(Valid Ra	inge 1 to 10)			ł	
		Pre-log	in banner							

ةيموسرلا مدختسملا ةهجاو ىلإ اهلالخ نم لوصولا نكمي يتل IP نيوانع ةمئاق نيوكتل (GUI) ح الال المان (CLI)، حماظنلا ح قرادإلا عل القتنا (CLI) ماوألا رطس قهجاوو (GUI) المال عال القنتا و القريمة (CLI) بيوبتلا قمال عال القنتا و القريمة (GUI)

≡ Cisco IS	SE				Adm	inistration • System	1	
Deployment	Licensing	Certificates	Logging	Maintenance	Upgrade	Health Checks	Backup & Restore	Admin Access
Authentication		Session	IP Access	MnT Access				
Authorization	>	~ Acces	s Restriction					
Administrators	>	<ul> <li>Allow all</li> <li>Allow onl</li> </ul>	y listed IP address	es to connect				
Settings	~							
Access		X Config	uro ID Liet fr	or Access Postric	stion			
Session		IP List		DI ACCESS RESULC	,0011			
Portal Customizatio	on	$+ \operatorname{Add}$	🖉 Edit 🏾 📋 D	elete				
			IP			∨ MASK		
			10.9.8.0			24		

يف اەنم MnT مسق ىلإ لوصولا نيلوۇسملل نكمي يتلا دقعلا نم ةمئاق نيوكتل الال القنتلاو **لوصولا < تادادعإلا < لوؤسملا ىل لوصولا < ماظنلا < ةرادإلا</mark> ىل لقتنا ،ISE لو<b>صو** بيوبتلا ةمالع MnT.

قوف رقنا ،MnT ىلإ syslog لاسراب رشنلا جراخ وأ رشنلا لخاد امإ تانايكلا وأ دقعلل حامسلل

ةدوجوملا تانايكلا وأ دقعلل طقف حامسلل .MNT ويدار رزب **لاصتالاب IP ناونع يأل حامسلا** ر**شنلا يف ةدوجوملا دقعلل طقف حامسلا** قوف رقنا ،MnT ىلإ syslog لاسراب رشنلا نمض ويدار رزب **لاصتالاب** 

≡ Cisco 🗄	SE	Administration • System									
Deployment	Licensing	Certificates	Logging	Maintenance	Upgrade	Health Checks	Backup & Restore	Admin Access			
Authentication		Session	IP Access	MnT Access							
Authorization	>	∽ MnT A	ccess Restr	iction							
Administrators	>	<ul> <li>Allow any</li> <li>Allow only</li> </ul>	y the nodes in the	e deployment to connect t	o MNT						
Settings	~										
Access											
Session											
Portal Customizati	on										

ةمدخ" مادختسإ ليغشت متي ،ثدحألا تارادصإلاو ISE 2.6 حيحصتل ةبسنلاب :**قظحالم** جمدب حمسي ال امم ،يضارتفا لكشب *MnT يل UDP ل* Syslogs *ليصوتل "ISE قلسارم* syslog لي م ةمداقلا عمد العالي عن التابي ال

in order to **ريدم<ماظن<ةرادا** ىلإ لقتنا ،ةسلج نم طاشن مدع ىلإ بجاو ةميق ليطعت تلكش in order to لمعلا ةسلج قلهم بيوبتلا ةمالع نمض ةميقلا هذه نييعتب مق .**ةسلج<دادعا قيلمع<ذفنم**.

≡ Cisco IS	SE				Admi	inistration • System	1	
Deployment	Licensing	Certificates	Logging	Maintenance	Upgrade	Health Checks	Backup & Restore	Admin Access
Authentication		Session Time	out Sessio	n Info				
Authorization	>							
Administrators	>	* Session	Idle Timeout 60	minutes	Valid Range 6 to 1	00)		
Settings	~							
Access								
Session								
Portal Customization	on							

**ةسلج < تادادعإ < لوؤسملا لوصو < ةرادإ** ىلإ لقتنا ،ةيلاحلا ةطشنلا تاسلجلا لاطبإ/ضرعل **لمعلا ةسلج تامولعم** بيوبتلا ةمالع قوف رقناو **لمعل**ا.

					Adm	iinistration • System				
Deployment	Licensing	Certificates	Logging	Maintenance	Upgrade	Health Checks	Backup 8	& Restore	Admin Access	Settings
Authentication		Session Time	out Sessi	on Info						
Authorization	>									
Administrators	>	Selec	st sessi	on and ter	minate					
Settings	~	1 Invalidat	e							
Access			HearlD		troce	Section Creatio	on Timo	Socion Last	Accessed	
Session			OsenD		1622	Session creation	on mile	Session Last	Accessed	
Portal Customization			admin	10.65.	48.253	Fri Oct 09 01:16:5	59 IST 2020	Fri Oct 09 01:4	5:10 IST 2020	

## دامتعا تانايب مادختساب لوؤسملا لخدم ىلا لوصولا نيوكت AD

#### AD ىلإ ISE مامضنا

< قيجراخلا قيوهلا رداصم < قيوهلا قرادا < قرادا على القتنا ،يجراخ لاجم على ISE مض لجأ نم دامتعا تانايب لخداً Active Directory لاجمو قديدجلا طبرلا قطقن مسا لخداً قوف رقنا مث ،اهيلع تارييغت ءارجاو رتويبمكلا تانئاك قفاضا هنكمي يذلا AD باسح قوفاوم.

■ Cisco ISE		Administration • Identity Management
Identities Groups External Ide	ntity Sources Identit	ty Source Sequences Settings
External Identity Sources	Connection Whitelis	sted Domains PassivelD Groups Attributes Advanced S
> 🖹 Certificate Authentication F	* Join Point Name	AD
Active Directory	* Active Directory Domain	rinsantr.lab (j
<ul> <li>LDAP</li> <li>ODBC</li> </ul>	Join Doma	ain
RADIUS Token     RSA SecurID	Please specify the crede	entials required to Join ISE node(s) to the Active Directory Domain.
<ul> <li>SAML Id Providers</li> <li>Social Login</li> </ul>	AD 058	* Password
	Specify Organization	dentials () Cancel OK

Connection	Whiteliste	ed Domains	PassiveID	Groups	Attributes	Advanced Settings	
* Join Point	Name	AD			(i)		
* Active Dire Domain	ectory	rinsantr.lab			(i)		
+ Join +	- Leave 🛛	Test User 🛛 🕺	Diagnostic Tool	🖯 Refresh Ta	ble		
	E Node	^	ISE Node R	Status	Doma	in Controller	Site
ri	rini-ise-30.gce.iselab.loca		STANDALONE	Operational	WIN-5	KSMPOHEP5A.rinsantr.l	Default-First-Site-Name

#### ليلدلا تاعومجم ديدحت

مسا ىلع رقنا. Active Directory < **ةيجراخلا ةيوەلا رداصم < ةيوەلا ةرادإ < ةرادإ** ىلإ لقتنا د**يدحت < ةفاضا** قوف رقنا .**تاعومجم** بيوبتلا ةمالع ىلإ لقتناو ةبولطملا طبرلا ةطقن يمتني لقألا ىلع ةدحاو AD ةعومجم داريتساب مق .**تاعومجم دادرتسإ < ليلدلا نم تاعومجم** .**ظفح** قوف رقنا مث ،**قفاوم** قوف رقنا مث ،

dentity Sources	Select Directory G	iroups		
Connection	This dialog is used to select groups from t	he Directory.		
🖉 Edit 🕂	Domain rinsantr.lab			
🗌 Na	Name Filter *	SID * Filter	Type Filter	
No data availal	Name	A Group SID	)	Group Type
	rinsantr.lab/Users/Enterprise Ke	y Admins S-1-5-21-1	977851106-3699455990-29458652	UNIVERSAL
	rinsantr.lab/Users/Enterprise Re	ad-only Domain S-1-5-21-1	1977851106-3699455990-29458652	UNIVERSAL
	rinsantr.lab/Users/Group Policy	Creator Owners S-1-5-21-1	977851106-3699455990-29458652	GLOBAL
	rinsantr.lab/Users/Key Admins	S-1-5-21-1	977851106-3699455990-29458652	GLOBAL
	rinsantr.lab/Users/Protected Us	ers S-1-5-21-1	977851106-3699455990-29458652	GLOBAL
	rinsantr.lab/Users/RAS and IAS	Servers S-1-5-21-1	977851106-3699455990-29458652	DOMAIN LOCAL
	rinsantr.lab/Users/Read-only Do	omain Controllers S-1-5-21-1	977851106-3699455990-29458652	GLOBAL
<	rinsantr.lab/Users/Schema Adm	ins S-1-5-21-1	977851106-3699455990-29458652	UNIVERSAL
	rinsantr.lab/Users/Test Group	S-1-5-21-1	977851106-3699455990-29458652	GLOBAL
	<			

Cancel

Ok

Connecti	ion Whitelisted Domains	PassiveID Grou	ps Attributes	Advanced Settings
🖉 Edit	+ Add \vee 🍵 Delete Group	Update SID Values		
	Name	^	SID	
	rinsantr.lab/Users/Test Group		S-1-5-21-1977851	106-3699455990-2945865208-1106

#### AD ل يرادإلا لوصولا نيكمت

حمت العام الحالي الحقت العامين العام الحياي من العام العامي العامي العالي الحقت العامي العامي العامي العامي الع مرايخ ل الدام م**تي المراب المراب المراب الي التي التي التي الم Admin Access > Authentication. عنف المالي المراب الم** 

≡ Cisco	SE				Admi	inistration • System	1			A Evaluation Mode 60 I
Deployment	Licensing	Certificates	Logging	Maintenance	Upgrade	Health Checks	Backup & Restore	Admin Access	Settings	
Authentication		Authenticatio	n Method	Password Policy	Account Disat	ble Policy Lock/Su	ispend Settings			
Authorization	>	Authentica	tion Type							
Administrators	>									
Settings	>	Password	I Based							
		* Identity Sou AD:AD O Client Ce	rce rtificate Based	~						Save

#### AD ةعومجم نييعتل ISE لوؤسم ةعومجم نيوكت

≡ Cisco IS	SE				Admi	nistration • System	l.	
Deployment	Licensing	Certificates	Logging	Maintenance	Upgrade	Health Checks	Backup & Restore	Admin Access
Authentication		Admin Groups >	ISE AD Admin G	roup				
Authorization	>	Admin Grou	p					
Administrators	~	* Name	ISE	AD Admin Group				
Admin Groups		Description						
Settings	>	Type External Identity Name : AD	Source	External				
		<pre>     External     External </pre>	Groups Insantr.lab/User Gers Delete tus	rs/Test Group 🗸	+ Usernam	e First Nam	e Last Name	

### ةرادإلا ةعومجمل RBAC تانوذأ نييعت

ِىلِإِ لِقِتِنا ،قِباسِلا مسقِلا يف اهؤاشناٍ مت يتلا ةرادإلا ةعومجم ىلإ RBAC تانوذأ نييعتل ُتاءارجإ َةلدسَنمُلااَ ةمئاقُلا نم .RBAC ج**ەن < ضيوفتَ < لوؤسملا لوصو < ماظن < ةراد**ا مادختساب اهطيطختب مقو ،قديدج ةدعاق ءاشناب مق .**ديدج جهن جاردا** ددح ،نيميلاً يل ع قدوجوملاً ةمئاقلاا يلإ لوصولا تانوذأب اهنييعتب مقو ،هالعاً مسقلاً يف ةفرعملاً "قرادإلاً قعومجم" . ظفح قوف رقنا مث ،ةبولطملا تانايبلاو

≡ Cisco	ISE				Admir	nistration • Sy	/stem			
Deployment	Licensing	Certificates	Logging N	laintenan	ce Upgrade	Health Chee	cks	Backup & Restore	Admin Access	Settings
Authentication		Create Role Bas	ed Access Control policies	by configurir	ng rules based on Admin gr	oups,Menu Access	permission	s (menu items), Data Access pe	ermissions (identity group da	ata elements) and other c
Authorization	~	allowed on a sin evaluated. The s	gle policy. You can copy th subject's permissions will b	e default poli e the aggrega	cies shown below,then mod ate of all permissions from e	dify them as needed each applicable pol	<ol> <li>Note that icy.Permit c</li> </ol>	t system-created and default po overrides Deny. (The policies an	olicies cannot be updated, a e displayed in alphabetical o	nd default policies canno order of the policy name).
Permissions	~	✓ RBAC F	Policies							
RBAC Policy		R	ule Name	A	dmin Groups		Permis	ssions		
Administrators	>	V< C	Customization Admin Pol	icy If	Customization Admin	+	then	Customization Admin Men.	+ Actions	~
Settings	>	✓ _ R	RBAC Policy 1	lf	ISE AD Admin Group	+	then	Super Admin Menu Acces.	X Actions	~
			Elevated System Admin P	Poli If	Elevated System Admin	n +	then	Super Admin Menu	Access ~	+
		V E	RS Admin Policy	If	ERS Admin	+	then			
		✓ ✓ _E	RS Operator Policy	lf	ERS Operator	+	then	Super Admin Data	Access ~	0

### ةحصلا نم ققحتلاو AD دامتعا تانايب مادختساب ISE ىلإ لوصولا

نم طبرلا ةطقن مسا ددح .ةيرادإلا (GUI) ةيموسرلا مدختسملا ةهجاو نم جورخلا ليجست ، AD تأنايب ةدعاق نم رورملاً ةملكو مدختسملاً مُسا لخداً .**ةيوەلاً ردصّم** ةلدُسْنَملاً ةمَّئاقلاً لوخدلا لجسو.

cisco	
 Identity Services Engine	
 Intuitive network security	
Username TestUser	-
Password ••••	1
Identity Source	
AD	-
Login	/

نم ەتقداصم تمت يذلا مدختسملا مسا نم ققحت ،حيحص لكشب لمعي نيوكتلا نأ ديكأتل لقتنا .(ISE) ةيموسرلا مدختسملا ةەجاو نم نميألا يولعلا نكرلا ىلع دوجوملا **تادادعإلا** زمر مدختسملا مسا نم ققحتو **مداخلا تامولعم** ىلإ



## LDAP مادختساب لوؤسملا لخدم ىلإ لوصولا نيوكت

#### LDAP ىلإ ISE مامضنا

ةمالع تحت .Active Directory > LDAP **حتيجراخلا قيوهلا رداصم < قيوهلا قرادا < قرادا** ىلا لقتنا ل مسا لاخداب مق ،**ماع** بيوبتلا LDAP ل ططخملا رتخاو LDAP ل مسا ل

<b>E Cisco</b> ISE	Administration • Identity Management							
Identities Groups External Iden	ntity Sources	Identity Source Sequences	Settings					
External Identity Sources       <     E     Image: Second	LDAP Identity Source	es List > New LDAP Identity Source						
	General Co	onnection Directory Organizatio	on Groups Attribut					
👻 AD								
LDAP	* Name	LDAPExample						
CDBC	Description							
RADIUS Token								
C RSA SecurID	▶ Schema	Active Directory	<u></u>					
SAML Id Providers								
🔁 Social Login								

لا تتبث ،انه .**ليصوت** بيوبتلا ةمالع ىلإ لقتنا ،لاصتالا عون ليكشتل ،كلذ دعب مال مالخدأ .(LDAP-Secure) 389(LDAP)/636 عانيملا عم يساسأ لدان LDAP لا نم hostname/IP مداخب ةصاخلا Admin رورم ةملك مادختساب (DN) لوؤسملل زيمملا مسالا

A Evaluation Mode 60	A E		nt	E Cisco ISE							
				ettings	e Sequences S	Identity Sour	tity Sources	External Ident	Groups	tities	Iden
		Advanced Settings	Attributes	Groups	irectory Organization	Connection [	General	у	Active Directory	~ L A	
Server	Secondary Serve				ary Server	Prim			D	🔁 A	
ondary Server	Enable Secondary S								AP	🗖 LDA	
									BC	🗖 OD	
		Hostname/IP		<u> </u>	27.196.131	10.1	* Hostname/IP		DIUS Token	🗖 RAI	
	389	Port				389	* Port		A SecurID	🗖 RS/	
								rs	ML Id Providers	🗀 SAI	
									cial Login	🗖 Soc	
						ver for each ISE node	Specify ser				
nous Access	<ul> <li>Anonymous Act</li> </ul>	Access			Anonymous Access	C	Access				
ticated Access	Authenticated A				Authenticated Access	c					
	admin	Admin DN		sers,D(	CN=Administrator,CN=L		Admin DN				
		Password					Password				
								>		<	
	admin Enable	Admin DN Password Secure Authentication		isers,D(	CN=Administrator,CN=L	cation	Admin DN Password Secure Authenti	>		٢	

رايتخال **ةيمستلا تاقايس** قوف رقناو **ليلدلا ةسسؤم** بيوبتلا ةمالع ىلإ لقتنا ،كلذ دعب نيمدختسملل يلكيهلا لسلستلا ىلإ ادانتسا مدختسملل ةحيحصلا تاسسؤملا ةعومجم لمداخ يف ةنزخملا

E Cisco ISE	Administration • Identity Management
Identities Groups E	ternal Identity Sources Sequences Settings
External Identity Sources 〈 管	LDAP Identity Sources List > LDAPExample
<ul> <li>Certificate Authent</li> <li>Active Directory</li> </ul>	General Connection Directory Organization Groups Attributes Advanced Settings
<ul><li>AD</li><li>LDAP</li></ul>	* Subject Search Base DC=rinsantr,DC=lab ()
<ul><li>ODBC</li><li>RADIUS Token</li></ul>	* Group Search Base DC=rinsantr,DC=lab ()
<ul><li>RSA SecurID</li><li>SAML Id Providers</li></ul>	Search for MAC Address in Format xx-xx-xx-xx-xx-xx V
🗖 Social Login	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

لوصولا ةيناكمإ رابتخال **لاصتالا** بيوبتلا ةمالع نمض **مداخلاب طبرلا رابتخإ** قوف رقنا ISE. مداخب ةصاخلا



#### 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)	
	Name	
		^
	CN=Server Operators,CN=Builtin,DC=rinsantr,DC=Iab	
	CN=Storage Replica Administrators,CN=Builtin,DC=rinsantr,DC=lab	
	CN=System Managed Accounts Group,CN=Builtin,DC=rinsantr,DC=lab	
	CN=Terminal Server License Servers,CN=Builtin,DC=rinsantr,DC=lab	
	CN=Test Group,CN=Users,DC=rinsantr,DC=Iab	
	CN=Users,CN=Builtin,DC=rinsantr,DC=lab	
	CN=Windows Authorization Access Group,CN=Builtin,DC=rinsantr,DC=lab	
		~

Cancel

ternal Identity Sources	LDAP Identity Sources List > LDAPExample		
> 🖻 Certificate Authentication F			
> 🔁 Active Directory	General Connection Directory Organization	Groups Att	ributes Advanced Settings
LDAP			
😤 LDAPExample	🖉 Edit 🕂 Add 💛 📋 Delete Group		
C ODBC	□ Name		^
RADIUS Token	CN=Test Group,CN=Users,DC=rinsantr,DC=lab		
C RSA SecurID			

### LDAP يمدختسمل يرادإلا لوصولا نيكمت

ىلإ لقتنا، LDAP مادختساب رورملا ةملك ىلإ ةدنتسملا ISE ققداصم نيكمتل Administration> System > Admin Access > Authentication. مقالع يف مالع يف رقناو **ةيوهلا ردصم** قلدسنملا قمئاقلا نم LDAP ددح .**رورملا قملك ىلإ دنتسملا** رايخلا ددح ظفح ىلع.

≡ Cisco	SE	Administration • System								
Deployment	Licensing	Certificates	Logging	Maintenance	Upgrade	Health Checks	Backup & Restore	Admin Access	Settings	
Authentication		Authenticatio	on Method	Password Policy	Account Disab	le Policy Lock/S	uspend Settings			
Authorization	>	Authentica	tion Type							
Administrators	>									
Settings	>	Password	d Based							
		* Identity Sou LDAP:LDA Client Ce	rce IPExample	~					Save	

#### LDAP ةعومجم ىلإ ISE لوؤسم ةعومجم نييعت

جەن ضيوفت ىلع ءانب لوۇسملا ىلإ لوصولاب ەنيوكت مت يذلا مدختسملل حمسي اذەو لوۇسم ةعومجم ديدحتل .مدختسملل LDAP قعومجم ةيوضع ىلإ ەرودب دنتسي يذلاو .RBAC **نولوۇسم < لوۇسملا لوصو < ماظن < ةرادإ** ىلإ لقتنا ،LDAP قعومجم مىلإ اەطيطختو Cisco ISE ددح ،عونلا لقح يف ."ةديدجلا قرادإلاا" قعومجمل امسا لخدأو **قفاضا** قوف رقنا .**قرادإلاا تاعومجم <** متيس يتلا LDAP قعومجم ددح ،**قيجراخ تاعومجم** ةلدسنملا ةمئاقلاا نم .**يجراخ** رايتخالاا ةناخ .تارىيغتارا لەل ەندە ،قومجم دىرا مى المى الخرار قەرەر مى ال مى المى المى المى المى المى مى ال

	SE			Admi	nistration • S	ystem		
Deployment	Licensing	Certificates	Logging	Maintenance	Upgrade	Health Checks	Backup & Restore	Admin Access
Authentication		Admin Groups	> New Admin Gro	up				
Authorization	>	Admin Gro	up					
Administrators	~	* Name	ISE LDA	P Admin Group				
Admin Users								
Admin Groups		Description						
		Туре	Extern	al				
Settings	>	External Identit Name : LDAPE	y Source xample					
		✓ Externa	I Groups					
		* #	CN=Test Group,	CN=Users,DC= 🗸	÷			

## ةرادإلا ةعومجمل RBAC تانوذأ نييعت

ىلإ لقتنا ،قباسلا مسقلا يف اهؤاشنإ مت يتلا ةرادإلا ةعومجم ىلإ RBAC تانوذأ نييعتل تاءارجا قلدسنملا ةمئاقلا نم .**RBAC جهن < ضيوفت < لوؤسملا لوصو < ماظن < قرادا** مادختساب اهطيطختب مقو ،ةديدج ةدعاق ءاشنإب مق .**ديدج جهن جاردا** ددح ،نيميلا ىلع ةدوجوملا قمئاقلا ىلإ لوصولا تانوذأب اهنييعتب مقو ،هالعا مسقلا يف ةفرعملا "قرادإلا ةعومجم" .

E Cisco	ISE		Administration • System							Evaluate		
Deployment	Licensing	Certificates	Logging	Maintenanc	e Upgrade	Health Check	s	Backup & Restore	Admin A	Access	Set	
Authentication		Create Role Bas	sed Access Control policie	es by configuring	g rules based on Admin grou	ips,Menu Access pe	ermissions	(menu items), Data Access pe	rmissions (iden	itity group da	ata elemer	
Authorization	~	policies cannot displayed in alph	ess permissions are not a be deleted.For decision n habetical order of the pol	nowed on a sing naking, all applic icy name).	able policies will be evaluate	ed. The subject's pe	ermissions	will be the aggregate of all pe	rmissions from	each applica	able policy	
Permissions	~											
RBAC Policy		✓ RBAC F	Policies									
		R	ule Name	Ac	Imin Groups		Permis	sions				
Administrators	>	<b>v</b> v	Customization Admin P	olicy If	Customization Admin	+	then	Customization Admin Men	···· +	Actions	~	
Settings	>	<b>V</b> - <b>F</b>	RBAC Policy 2	If	ISE LDAP Admin Group	+	then	Super Admin Menu Access	a ×	Actions	~	
		<b>V</b> E	Elevated System Admin	Poli If	Elevated System Admin	+	then	Super Admin Menu	Access	× .	+	
		V	ERS Admin Policy	lf	ERS Admin	+	then					
		V	ERS Operator Policy	lf	ERS Operator	+	then	Read Only Admin D	ata Acces: `	~	0	
		<b>V</b> E	ERS Trustsec Policy	lf	ERS Trustsec	+	then	Super Admin Data Access	+	Actions	~	
			Helndesk Admin Policy	14	Helpdesk Admin	+	thee	Helpdesk Admin Menu Acc	Acc 1	Actions	0	

### ةحصلا نم ققحتلاو LDAP دامتعا تانايب مادختساب ISE ىلإ لوصولا

ةيموسرلا مدختسملا ةهجاو نم جورخلا ليجست (GUI) قيموسرلا مدختسملا قهجاو نم جورخلا ليجست لجسو ،LDAP تانايب ةدعاق نم رورملا ةملكو مدختسملا مسا لخدأ .**قيوملا ردصم** قلدسنملا لوخدلا.

	CISCO	
	Identity Services Engine	
	Intuitive network security Username TestUser@rinsantr.lab	-
-1	Password ●●●●●●●	1
	Identity Source	
	Login	

ەتقداصم تمت يذلا مدختسملا مسا نم ققحت ،حيحص لكشب لمعي نيوكتلا نأ نم دكأتلل is يموسرلا مدختسملا ةەجاو نم رسيألا يولعلا نكرلا ىلع دوجوملا **تادادعإلا** زمر نم (ISE). مدختسملا مسا نم ققحتو **مداخلا تامولعم** ىلإ لقتنا.



ةمجرتاا مذه لوح

تمجرت Cisco تايان تايانق تال نم قعومجم مادختساب دنتسمل اذه Cisco تمجرت ملاعل العامي عيمج يف نيم دختسمل لمعد يوتحم ميدقت لقيرشبل و امك ققيقد نوكت نل قيل قمجرت لضفاً نأ قظعالم يجرُي .قصاخل امهتغلب Cisco ياخت .فرتحم مجرتم اممدقي يتل القيفارت عال قمجرت اعم ل احل اوه يل إ أم اد عوجرل اب يصوُتو تامجرت الاذة ققد نع اهتي لوئسم Systems الما يا إ أم الا عنه يل الان الانتيام الال الانتيال الانت الما