وأ ةداەشلا ىلإ ةدنتسملا ةقداصملا نيوكت ISE ةرادإل ةيكذلا ةقاطبلا

تايوتحملا

قمدق ملايا قمدق مل الماليا تابل طتمل تابل طتمل محدث سمل التانوكمل محدث سمل التانوكمل محدث سمل التانوكمل محدث من محدث محدث المال محدث المحدث محدث المال محدث المحدث محدث المال محدث المحدث محدث المال محدث المحدث محدث المحدث المحدث المحدث المحدث محدث المحدث المحدث المحدث المحدث المحدث المحدث محدث المحدث الم

ەمدقملا

ىلإ لوصولل ليمعلا ةداەش ىلإ ةدنتسملا ةقداصملا نيوكت ةيفيك دنتسملا اذه حضوي ةداەش لباقم ةقداصملاب ISE لوؤسم موقي ،لاثملا اذه يف (ISE) ةيوەلا تامدخ كرحم ةرادإ ةصاخلا (GUI) ةيموسرلا مدختسملا ةەجاو ىلإ لوؤسملا لوصو ىلع لوصحلل مدختسملا تم ةيوەلا تامدخ كرحم ةرادإب Cisco.

ةيساسألا تابلطتملا

تابلطتملا

:ةيلاتا عيضاوملاب ةفرعم كيدل نوكت نأب Cisco يصوت

- .ةداەشلاو رورملا ةملك ةقداصمل ISE نيوكت •
- Microsoft Active Directory (AD)

ةمدختسملا تانوكملا

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

- Cisco Identity Services Engine (ISE)، رادصإلا 2.6
- Windows Active Directory (AD) Server 2008 رادصإلاا
- ةداەش •

ةصاخ ةيلمعم ةئيب يف ةدوجوملا ةزهجألاا نم دنتسملا اذه يف ةدراولا تامولعملا ءاشنإ مت. تناك اذإ .(يضارتفا) حوسمم نيوكتب دنتسملا اذه يف ةمدختسُملا ةزهجألاا عيمج تأدب نيوكت يأل لمتحملا ريثأتلا مهف نم دكأتف ،ةرشابم ةكبشلا.

نيوكتلا

يرادإلا لوصولل ةيجراخ ةيوهك ةيكذلا ةقاطبلا وأ ليمعلا قداهش نيوكتل مسقلا اذه مدختساً قرادإل (GUI) ةيموسرلا مدختسملا ةهجاو يلإ

ةكبشلل يطيطختلا مسرلا



Active Directory ب ISE طبر

- 1. **مان المان ال**
- .Cisco ISE يف **AD لاجم**و **طبرلا ةطقن** مساب Active Directory ليثم ءاشنإب مق .2
- .ل**اسرا** ىلع رقنا .3

4. هجوم يف نيبسانملا **رورملا ةملك**و **مدختسملا مسا** مادختساب دقعلاا عيمج ىلإ مضنا رمألا.

cisco Identity Services Engine Home	→ Context Visibility → Ope	rations → Policy <mark>→</mark> Admi	inistration 🔹 Wor	< Centers		License Warning 🔺	Q,	0 0	¢
System Identity Management Network	> System								
+ Identities Groups External Identity Sources	Identity Source Sequence	s ▶ Settings							
External Identity Sources	Connection	Whitelisted Domains Pas	siveID Gro	ups Attributes Advanc	ced Settings				
🗇 * 🗄 * 🥹*	* Join Point Name	AD		Ð					-
AD	* Active Directory Domain	* Active Directory Domain mydomain.com							
LDAP	🕂 Join 🕂 Leave 🧕 Tes	t User 🛛 📸 Diagnostic Tool 🛛 🛞 R	Refresh Table						
RADIUS Token	ISE Node	▲ ISE Node Role	Status	Domain Controller	Site				
RSA SecurID	ise2.mydomain.com	STANDALONE	🖸 Operational	WIN-58UQFTHFNIP.mydomai	Default-First-Site-Name				
SAML Id Providers									
📻 Social Login	Join Domain X Please specify the credentials required to Join ISE node(\$) to the Active Directory Domain. * AD User Name @ [* Password Specify Organizational Unit @ Specify Organizational Unit @ Store Credentials @								
				(ok)	Cancel				

.**ظفح** ةقطقط .5

ليلدلا تاعومجم ديدحت

- 1. ما تعومجم علام المنييعتب مقو ةيجراخ لوؤسم ةعومجم ءاشنإب مق 1. Active Directory.
- ديدحت < تاعومجم < Active Directory < ةيجراخلا ةيوهلا رداصم < ةيوهلا قراداٍ< قراداٍ رتخأ .2 نم تاعومجم Directory.
- .لوؤسملا اهيلإ يمتني لقألا ىلع ةدحاو AD ةعومجم دادرتسإ .3

25	Identity Source Sequences + Settings		
	Select Directory Groups		×
-	This dialog is used to select groups from the Di	rectory.	
	Domain mydomain.com	Ψ	
	Name Filter *ISE-*	SID Filter * Type Filter ALL *	
	Retrieve Groups 2 Groups Retr	ieved.	
[✓ Name	Group SID Group Type	
	mydomain.com/ISE-Admin	S-1-5-21-4009324561-3650473562-621564990-1 GLOBAL	
	mydomain.com/Users/ISE-RO	S-1-5-21-4009324561-3650473562-621564990-11 GLOBAL	
			ancel

.**ظفح** ةقطقط .4

يرادإلا لوصولل Active Directory رورم ةملك ىلإ ةدنتسملا ةقداصملا نيكمت

- مضنا رورملا ةملك ىلإ دنتسم ةقداصم بولسأك Active Directory ليثم نيكمتب مق .1 قباس تقو يف ISE ىلإ.
- .ةروصلا يف حضوم وه امك ،**ةقداصملا < لوؤسملا لوصو < ماظن<ةرادإ** رتخأ .2

disco Identity Services Engine	Home Context Visibility Operations Policy Administration Work Centers
▼ System → Identity Management	Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC
Deployment Licensing + Certific	ates → Logging → Maintenance Upgrade → Backup & Restore →Admin Access → Settings
Authentication	Authentication Method Password Policy Account Disable Policy Lock/Suspend Settings
▶ Authorization	Authentication Type
Administrators	Password Based * Identity Source AD:AD *
 Settings 	
	O Client Certificate Based
	Save Reset

.**ظفح** ةقطقط .3

```
ةقداصملا نيكمتل رورملا ةملك ىلإ ةدنتسملا ةقداصملا نيوكت مزلي :ةظحالم
ةقداصملل حجان نيوكت دعب نيوكتلا اذه سكع بجي .ةداهشلا ىلإ ةدنتسملا
```

ةداەشلا ىلإ ةدنتسملا.

نيلوؤسملا تاعومجم ىلإ ةيجراخلا ةيوهلا تاعومجم نييعت

.ةيضارتفالا ةرادإلا ةعومجم ىلع ةيجراخلا AD ةعومجم نييعت متي ،لاثملا اذه يف

- ا. كوؤسملا تاعومجم< نولوؤسملا< لوؤسمل لوصو< ماظنلا< ةرادإ رتخأ .1 Super Admin.
- . **قيجراخ تاعومجم** نمض AD ةعومجم ددحو **يجراخ** عونك عونلا نم ققحت.

dentity Services Engine	lome → Context Visibility → Operations → Policy	←Administration	License W
▼ System → Identity Management	Network Resources Device Portal Management pxGrid	Services + Feed Service + Threat Centric N	AC
Deployment Licensing + Certifi	tes → Logging → Maintenance Upgrade → Backup & R	estore -Admin Access + Settings	
Authentication Authorization	Admin Groups > System Admin Admin Group		
▼ Administrators	Description Access permission for Operations tab. Inc	ludes System and data access permission for Admin	Groups. //
Admin Users	Type 🗹 External		
Admin Groups	External Identity Source		
	External Groups * mydomain.com/ISE-Admin O +		
	Status Email Usernar	me First Name Last Name	
	Save Reset	No data a	vailable

- .**ظفح** ةقطقط .3
- .لوؤسم طقف ةءارق < ةرادإلاا تاعومجم < نيلوؤسم < لوؤسملا لوصو < ماظن < ةرادإ رتخأ .4
- .ةروصلا يف حضوم وه امك ،**ةيجراخ تاعومجم** نمض AD ةعومجم ددحو **يجراخك** عونلا نم ققحت .5

disco Identity Services Engine	Home → Context Vi	sibility + Operations	→ Policy →Administ	tration 🔹 Work Cen	iters		License Wi
▼System → Identity Managemen	t 🕨 Network Resources	Device Portal Manag	ement pxGrid Services	Feed Service	Threat Centric NAC		
Deployment Licensing + Certi	icates ►Logging ►N	faintenance Upgrade	+ Backup & Restore 🔫	Admin Access + Sett	lings		
Authentication Authorization	Admin Groups > Read - Admin Group	Only Admin					
T Administration	* Name	Read Only Admin					
* Administrators	Description	Access Permission for a	dmin with read-only functiona	lity		11	
Admin Users	Туре	External					
Admin Groups	External Identity Sour	ce					
 Settings 	Name : AD	æ					
	* mydomain.com	n/Users/ISE-RO 🖸 🕂					
	Member Users Users						
	🕂 🕂 🕂 🕂 🕂 🕂 🕂						
	Status	 Email 	Username	First Name	Last Name		
					No data availa	ble	
	Save Reset						

.**ظفح** ةقطقط .6

اەب قوثوم ةداەش داريتسإ

- 1. ليمعلا ةداەش عقوت يتلا (CA) قدصملا عجرملا ةداەش داريتسإ.
- .داريتسإ < اهب قوثوم ةداهش < تاداهش < ماظن < ريدم راتخن .2
- .قدصملا عجرملا ةداەش رتخاو حفصت رقنا .3
- .ةروصلا يف حضوم وه امك ،**Syslog و ليمعلا ةقداصمب ةقثلا** رايتخالاا ةناخ ددح .4

-thati- tisco Identity Services Engine	Home + Context Visibility + Operations + Policy Administration + Work Centers	License Warning 🔺 🔍 \varTheta	• •
▼ System	Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC		
Deployment Licensing - Certifi	cates + Logging + Maintenance Upgrade + Backup & Restore + Admin Access + Settings		
Certificate Management System Certificates	Import a new Certificate into the Certificate Store * Certificate File Choose File DCcomDCmymainW.pem		
Trusted Certificates	Friendly Name		
OCSP Client Profile Certificate Signing Requests Certificate Periodic Check Setti	Trusted For: @ ☑ Trust for authentication within ISE		
Certificate Authority	 ✓ Trust for authentication of Cisco Services ✓ Trust for authentication of Cisco Services 		
	Description		
	Submit		

. **لاسرا** ىلع رقنا.

ةداەشلا ةقداصم فيرعت فلم نيوكت

ا قرادا رتخأ ،ليمعلا ةداەش ىلإ ةدنتسملا ةقداصملل ةداەشلا ةقداصم فيصوت ءاشنإل .1 قفاضا < قداەشلا ققداصم فيرعت فلم < قيجراخلا قيوەلا رداصم < قيوەلا قرادا<.

- .فيرعتلا فلم مسا فضاً .2
- ةداەشلا ةمس يف لوؤسملا مدختسم مسا ىلع يوتحت يتلا ةبسانملا ةمسلا ددح .3.
- ةنراقم ديريو مدختسملا ةداهش ىلع يوتحي مدختسملاب صاخلا AD لجس ناك اذإ .4 ققحتف ،AD يف ةدوجوملا ةداهشلا لباقم ضرعتسملا نم اهمالتسإ متي يتلا ةداهشلا مت يذلا Active Directory ليثم مسا ددحو ،**امئاد ةيئانث ةنراقم ذيفنت** رايتخالا ةناخ نم .اقبسم هديدحت

disco Identity Services Engine	Home	▶ Context Visibility	 Operations 	▶ Policy	→Administration	♦ Work	Centers
System Identity Managemen	nt ⊧Netwo	rk Resources 🕨 Devic	e Portal Managem	ent p×Grid	d Services 🕨 Feed	Service	Threat Centric NAC
▶ Identities Groups External I	dentity Sourc	es Identity Source Se	quences + Sett	ings			
	file	es Identify Source Se Certificate Authent Certificate Auth U: Match Client C Certificate In Submit Cance	iquenoes + Sett isoation Profiles Lis entication Profile Description Identity Store se Identity Store dentity Store ()	ings t > New Cert le CAC_Login AD Certificat AD Any Sub, Never Only to Always	Profile	en Profile	e ve Name - Other Name * (1) ves in the Certificate (for Active Directory Only) (1)

5. لاسرا ىلى رقىنا.

ةدنتسملا ةقداصملل ةداهشلا ةقداصم فيرعت فلم سفن كالهتسا نكمي :**قظحالم** اضيأ ةياهنلا ةطقن ةيوه يلإ.

ليمعلا ةداەش ىل قدنتسملا ةقداصملا نيكمت

اليمعلا ةداهش <mark>ةقداصملا بولسأ < ةقداصملا < لوؤسملا لوصو < ماظنلا < ةرادإلا</mark> راتخن . يلإ ةدنتسملا.

cisco Identity Services Engine	Home + Context Visibility + Oper	ations + Policy Administration + Work Centers
▼ System → Identity Management	Network Resources Device Portal 1	Management pxGrid Services + Feed Service + Threat Centric NAC
Deployment Licensing + Certific	ates + Logging + Maintenance	Enabling Client Certificate-Based Authentication will cause an application server restart on all deployment
0		nodes. This will result in significant downtime for the system.
Authentication	Authentication Method	
Authorization	Authentication Type	Cancel
✓ Administrators	O Password Based	
Admin Users		* Identity Source AD:AD *
Admin Groups		
▶ Settings	Client Certificate Based	
	Cours David	
	Save	

- .2 قوف رقناو .2 **OK**
- .اقبسم ەنيوكت مت يذلا **ةداەشلا ةقداصم فيرعت فلم** رتخأ
- 4. ليثم مسا ددح Active Directory.

dialb Identity Services Engine	Home Context Visibility Operations Policy Administration Work Centers
▼ System → Identity Management	Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC
Deployment Licensing + Certifi	cates → Logging → Maintenance Upgrade → Backup & Restore <mark>→</mark> Admin Access → Settings
O Authentication	Authentication Method Password Policy Account Disable Policy Lock/Suspend Settings
Authorization	Authentication Type
▼ Administrators Admin Users	O Password Based
Admin Groups	Client Certificate Based Certificate Authentication Profile CAC_Login_Profile T
	* Identity Source AD:AD
	Save Reset

- .**ظفح** ةقطقط .5
- 6. رشنلا ليغشت ةداعإ تايلمع يف دقعلا ةفاك ىلع ISE تامدخ.

dentity Services Engine	Home → Context Visibility → Operations	s + Policy -Administration + Work Centers	
▼ System → Identity Management	Network Resources Device Portal Manage	gement pxGrid Services + Feed Service + Threat Centric NAC	
Deployment Licensing + Certifi	cates + Logging + Maintenance	ne system will now restart.	
Q.	Authentication Method		
Authorization	Authentication Type		ок
▼ Administrators	O Password Based		
Admin Users			
Admin Groups			
▶ Settings	Client Certificate Based	* Certificate Authentication Profile CAC_Login	Profile -
		* Identity Source AD:AD	<u>*</u>
	Save Reset		

ةحصلا نم ققحتلا

ةمدخ ةلاح رييغت دعب ISE ب ةصاخلا (GUI) ةيموسرلا مدختسملا ةمجاو ىلإ لوصولا نم ققحت **ليغشتلا ديق** ىلإ **تاقيبطتال مداخ.**

كال لوخدلا ليجستل ةداهش رايتخاب مدختسملا ةبلاطم نم ققحت Super Admin: مدختسمل عزج نم ةداهشلا تناك اذا Super Admin تازايتما هئاطعاو (ISE) ةيموسرلا مدختسملا ةهجاو زيمتملا لوؤسملل ةيجراخلا ةيوهلا ةعومجم يف مدختسم





ةبلاطم متت ەنأ نم ققحت:(**طقف ةءارقلل لوؤسم مدختسم) Read-Only Admin User**

محنم متيو ،(ISE) ةيموسرلا مدختسملا ةمجاو ىلإ لوخدلا ليجستل قدامش رايتخاب مدختسملا ةيوملا ةعومجم يف مدختسم عزج نم قدامشلا تناك اذإ "طقف ةءارقلا لوؤسم" تازايتما طقف ةءارقلل لوؤسمل ةيجراخلا.

🗇 🔿 🥔 https://ise2.mydomain.com/	P → X O Waiting for ise2.mydomain X
----------------------------------	-------------------------------------





ةداهش Smartcard مدقت ،(CAC) كرتشملا لوصولا ةقاطب مادختسإ ةلاح يف :**قظحالم** لضفألا (PIN) يصخشلا فيرعتلا زمر مدختسملا لخدي نأ دعب ISE ىلإ مدختسملا حلاصلا.

اهحالصإو ءاطخألا فاشكتسا

- يف مكحتلاا ليطعتب حمسي نمآ عضو يف Cisco ISE ءدبل start ise safe رمألاا مدختسأ .1 اتامدخ ليغشت ةداعإو نيوكتلا حيحصتو لوؤسملا لخدم ىلا اتقۇم لوصول ISE تامدخ ليغشت مادع وي .
- لخدم ىلإ لوصولا نيمأتب لوؤسّملا ماق اذإ دادرتسالل ةليسو نمآلا رايخلا رفوي .2 لوؤسملا ماق اذإ ثدحلا اذه ثدحي دق .دصق نود نيمدختسملا عيمجل Cisco ISE لوؤسم **ةحفص < تادادعإ < لوؤسملا لوصو < ةرادإلا** يف ةحيحص ريغ **IP لوصو** ةمئاق نيوكتب مسا ىلإ عجريو **ةداهشلا ىل قدنتسملا ةقداصملا نمآلا** رايخلا زواجتي امك .**لوصول**ا Cisco Cisco لوغرا الاتفاد الاقسم لخدم ىلإ لوخدلا ليجستل رورملا ةملك ةقداصمو يضارتفالا مدختسمل الاقلام

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