LDAP مداخ عم لماكتلل ISE نيوكت

تايوتحملا

الباحية البماحمم الباحيم الباحيم الباحيم الباحيم الباحيم الباحيم ا

ةمدقملا

مداخ عم لماكتلل Cisco نم (ISE) ةيوهلا تامدخ كرحم نيوكت ةيفيك دنتسملا اذه فصي Cisco LDAP.

ةيساسألا تابلطتملا

تابلطتملا

دنتسملا اذهل ةصاخ تابلطتم دجوت ال.

ةمدختسملا تانوكملا

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

- Cisco ISE رادصإلا 1.3 حيحصت عم
- Microsoft Windows تيبثت عم x64 7 رادصإلا OpenLDAP
- 8.0.100.0 رادصإلا، Cisco نم (WLC) ةيكلساللاا LAN ةكبش يف مكحتلا ةدجو •
- Cisco AnyConnect، ل 3.1 رادصإلا Microsoft Windows
- دم قكبشلا ىلإ لوصولا ريدم فيرعت فلم ررحم

🔌 ةيجراخلا ةيوەلا ردصمك LDAP مدختست يتلا تاودألل حلاص دنتسملا اذه :ةظحالم اەب صاخلا ضيوفتلاو ISE ةقداصمل.

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.

ةيساسأ تامولعم

LDAP: عم ةموعدم هذه ةقداصملا بيلاسأ

- (EAP-GTC) ماعلا زيمملا زمرلا ةقاطب عسوتملا ةقداصملا لوكوتورب •
- القنابة الما الما القنابة الما يمحمل عسوتما القاداصمل الوكوتورب (PEAP-TLS)

نيوكتلا

.LDAP مداخ عم ISE جمدو ةكبشلا ةزهجأ نيوكت ةيفيك مسقلا اذه فصي

ةكبشلل يطيطختلا مسرلا

ةكبشلاب نارتقالل يكلسال لوحم ةياەنلا ةطقن مدختست ،اذە نيوكتلا لاثم يف ةيكلساللا.

لا قيرط نع لمعتسملاً تقداص WLC in order to لا يلع (WLAN) يكلسال LAN لا تلكش. يجراخ ةيوه نزخمك LDAP نيوكت مت ،ISE يف

همادختسإ متي يذلا ةكبشلا ططخم ةروصلا اذه حضوي:



OpenLDAP نيوكت

ل OpenLDAP تيبثت لمتكا Microsoft Windows ل OpenLDAP تيبثت لمتكا اذه ىرت نأ بجي ،تيبثتلا دعب .C: > OpenLDAP وه يضارتفالاا عضوملا .ةرشابمو ةحضاو يهو ليلدلا

Name	Date modified	Туре	Size
BDBTools	6/3/2015 5:06 PM	File folder	
ClientTools	6/3/2015 5:06 PM	File folder	
퉬 data	6/4/2015 9:09 PM	File folder	
퉬 ldifdata	6/4/2015 11:03 AM	File folder	
🐌 Readme	6/3/2015 5:06 PM	File folder	
🐌 replica	6/3/2015 5:06 PM	File folder	
\mu run	6/4/2015 9:09 PM	File folder	
퉬 schema	6/3/2015 5:06 PM	File folder	
퉬 secure	6/3/2015 5:06 PM	File folder	
🐌 SQL	6/3/2015 5:06 PM	File folder	
퉬 ucdata	6/3/2015 5:06 PM	File folder	
🚳 4758cca.dll	2/22/2015 5:59 PM	Application extens	18 KB
🚳 aep.dll	2/22/2015 5:59 PM	Application extens	15 KB
🚳 atalla.dll	2/22/2015 5:59 PM	Application extens	13 KB
🚳 capi.dll	2/22/2015 5:59 PM	Application extens	29 KB
🚳 chil.dll	2/22/2015 5:59 PM	Application extens	21 KB
🚳 cswift.dll	2/22/2015 5:59 PM	Application extens	20 KB
🚳 gmp.dll	2/22/2015 5:59 PM	Application extens	6 KB
🚳 gost.dll	2/22/2015 5:59 PM	Application extens	76 KB
🚳 hs_regex.dll	5/11/2015 10:58 PM	Application extens	38 KB
InstallService.Action	5/11/2015 10:59 PM	ACTION File	81 KB
💼 krb5.ini	6/3/2015 5:06 PM	Configuration sett	1 KB
🚳 libeay32.dll	2/22/2015 5:59 PM	Application extens	1,545 KB
🚳 libsasl.dll	2/5/2015 9:40 PM	Application extens	252 KB
maxcrc.ldif	2/5/2015 9:40 PM	LDIF File	1 KB
🚳 nuron.dll	2/22/2015 5:59 PM	Application extens	11 KB
🗟 padlock.dll	2/22/2015 5:59 PM	Application extens	7 KB
slapaci.exe	5/11/2015 10:59 PM	Application	3,711 KB

صوصخلا هجو ىلع نيلالدب املع ةطاحإلا:

- ClientTools ريرحتل اهمادختسإ متي يتلا تايئانثلا نم ةعومجم ليلدلا اذه نمضتي تانايب ةدعاق LDAP.
- Idifdata تانئاك عم هيف تافلملا نيزخت بجي يذلا ناكملا وه اذه LDAP.

LDAP: تانايب ةدعاق ىلإ لكيەلا اذه ةفاضإ



يوتحت نأ بجي .(OUs) نيتيسسؤم نيتدحو نيوكت بجي ،رذجلا ليلدلاا تحت OU=groups OU يوتحت نأ بجي .(لااثملا اذه يف cn=domainUsers) ةدحاو ةيعرف ةعومجم ىلع

cn=domainUsers. ةعومجم ىلإ نايمتني نيذللا مدختسملا يباسح OU=people فرعت

نم اقباس ةروكذملا ةينبلا ءاشنإ مت .الوأ ldif فلم ءاشنإ كيلع بجي ،تانايبلا ةدعاق علمل فلملا اذه:

dn: ou=groups,dc=maxcrc,dc=com changetype: add ou: groups description: All groups in organisation objectclass: organizationalunit dn: ou=people,dc=maxcrc,dc=com changetype: add ou: people description: All people in organisation objectclass: organizationalunit dn: uid=john.doe,ou=people,dc=maxcrc,dc=com changetype: add objectClass: top objectClass: person objectClass: organizationalPerson objectClass: inetOrgPerson uid: john.doe givenName: John sn: Doe

cn: John Doe
mail: john.doe@example.com
userPassword: password

dn: uid=jan.kowalski,ou=people,dc=maxcrc,dc=com changetype: add objectClass: top objectClass: person objectClass: organizationalPerson objectClass: inetOrgPerson uid: jan.kowalski givenName: Jan sn: Kowalski cn: Jan Kowalski mail: jan.kowalski@example.com userPassword: password

dn: cn=domainusers,ou=groups,dc=maxcrc,dc=com changetype: add objectClass: top objectClass: posixGroup gidNumber: 678 memberUid: uid=john.doe,ou=people,dc=maxcrc,dc=com memberUid: uid=jan.kowalski,ou=people,dc=maxcrc,dc=com

:Idapmodify binary رمألا مدختسأ ،LDAP تانايب ةدعاق ىلٍ تانئاكلا ةفاضإل

C:\OpenLDAP\ClientTools>ldapmodify.exe -a -x -h localhost -p 389 -D "cn=Manager, dc=maxcrc,dc=com" -w secret -f C:\OpenLDAP\ldifdata\test.ldif ldap_connect_to_host: TCP localhost:389 ldap_prepare_socket: 496 ldap_connect_to_host: Trying ::1 389 ldap_pvt_connect: fd: 496 tm: -1 async: 0 attempting to connect: connect success adding new entry "ou=groups,dc=maxcrc,dc=com" adding new entry "ou=people,dc=maxcrc,dc=com" adding new entry "uid=john.doe,ou=people,dc=maxcrc,dc=com" adding new entry "uid=jan.kowalski,ou=people,dc=maxcrc,dc=com"

ISE عم OpenLDAP جمد

ا مسق اذہ لالخ نم روصلا يف تدوز نوكي نأ ةمولعملا تلمعتسا LDAP تلكش in order to مسق اذہ لاخ نم روصل يف تدوز نوكي ا لا ىل ع نزخم ةيوەك ISE.

ahah		Liceose Warning 🔒
CISCO Identity Services Engine	Home Operations I▼ Policy I▼ Guest Access I▼ Administration I▼	
🔆 System 🛛 😥 Identity Management	Network Resources 🛛 Device Portal Management 🛛 🙀 pxGnd Services 🕅 Feed Service	L pxGrid Identity Mapping
Identities Groups External Identity So	urces Identity Source Sequences Settings	
External Identity Sources	LDAP Identity Sources General Connection Directory Organization Groups Attributes * Name LDAP_DXAMPLE Description * * Schema v Custorn v * Subject Objectclass inetOrgPerson * Group Objectclass poskGroup * Subject Name Attribute uid * Group Nap Attribute memberUid	
	Save Reset	Y

ماع بيوبتلا ةمالع نم تامسلا هذه نيوكت كنكمي:

- SubjectClass اقبط الله ل فالم يف مدختسملا تاباسحل نئاكلا ةئف لقحلا اذه لثامي المامي القري الفاجي القربط ال تيوكتل LDAP. نيوكتل
 - ىلعأ ∘
 - صخش ∘
 - يميظنت فظوم ⊸
 - InetOrgPerson
- امدنع LDAP ةطساوب اهدادرتسإ متي يتلا ةمسلا يه هذه عوضوملا مسا ةمس يف .ال مأ تانايب ةدعاق يف نمضم ددحم مدختسم مسا كانه ناك اذإ امع ISE رسفتسي ةطقن ىلع مدختسم مساك jan.kowalskski وأ John.doe مادختسإ بجي ،ويرانيسلا اذه .ةياهنلا
- اذه يف النه الفالي في الم يف قعومجمل نئاكلا ةئف لقحلا اذه لثامي ObjectClass قعومجم ويرانيسلا مي الفات ،ويرانيسل وposixGroup.
- .تاعومجملا ىل ان يمدختسملا نييعت ةيفيك ةمسلا هذه ددحت ةعومجملا ططخم ةمس. نانثإ تيأر عيطتسي تنأ ،دربم اdif لا يف ةعومجم cn=domainUsers لا تحت لمعتسمل فداري نأ قمس.

:(Novell) و Sun و Sun و Novell و Microsoft Active Directory) اقبسم ةأيهملا تاططخمل ضعب ISE مدقي امك

alada	La	case Warning 🛕
cisco Identity Services Engine	Home Operations Policy Guest Access Administration	
🔆 System 🛛 👰 Identity Management	🞬 Network Resources 🛛 😹 Device Portal Management 🛛 😡 pxGrid Services 🖉 Feed Service 💶 pxGrid Ident	ity Mapping
Identities Groups External Identity S	turces Identity Source Sequences Settings	
External Identity Sources	LDAP Identity Source Lat > LDAP_EXAMPLE LDAP Identity Source General Connection Directory Organization Groups Attributes	
Active Directory	Primary Server	Secondary S
* 🚞 LDAP		Enable Se
LDAP_EXAMPLE		
 KADUJS TOKEN RSA SequeD 	* Hosmamell* 10.01.100.242 0 Hosmamell*	200
	- Dit 309	209
	Access O Anonymous Access Access	Anonymo
	Automicated Access	 Authentics
	Parenaver Annu Div	
	Secure Authentication Enable Secure Authentication Secure Authentication	Enable Sc
	Root CA Certificate Services Endpoint *	Certificate Se
	* Server Timeout 10 @Soconds Server Timeout	10
	* Max. Admin Connections 20 (1) Max. Admin Connections	20
	Test Bind to Server	Test Bind t
	۲	
	Save Reset	

مداخلا ىلإ طبر رابتخإ كنكمي ،يرادإلا لاجملا مساو حيحصلا IP ناونع طبضب موقت نأ دعب. اەنيوكت متي مل ثحبلا دعاوق نأل تاعومجم وأ عيضاوم يأ دادرتسإ كنكمي ال ،ةطقنلا ەذە دنع دعب.

ةطقن يه هذه .ةعومجملا/عوضوملا ثحب ةدعاق نيوكتب مق ،ةيلاتلا بيوبتلا ةمالع يف ةطقنل الافطأ دعت يتلا تاعومجملاو تاعوضوملا دادرتسإ كنكمي LDAP. ىلإ ISE ل طبرلا طقف كمامضنا.

تاعومجم نم تاعومجملاو OU=People نم تاعوضوملا دادرتسإ متي ،ويرانيسلا اذه يف OU=Groups:

abab		Libecae Warning 👖
Cisco Identity Services Engine	Administration I▼ Policy I▼ Guest Access I▼ Administration I▼	
🔆 System 🛛 💆 Identity Management 🔰	🖥 Network Resources 🛛 😹 Device Portal Management 🛛 🖳 pxGrid Services 🕞 Feed Service	Le pxGrid Identity Mapping
Identities Groups External Identity Sou	rces Identity Source Sequences Settings	
External Identity Sources	LDAP Identity Sources Let > LDAP_EXAMPLE LDAP Identity Sources General Connection Directory Organization Groups Attributes * Subject Search Base ou=people,dc=maxcrc,dc=com Naming Contexts 0 * Group Search Base ou=groups,dc=maxcrc,dc=com Naming Contexts 0 Search for MAC Address in Formation xxx xxx xxx xxx xxx xxx T Strip start of subject name up to the last occurrence of the separator	

ا:ISE ىلع LDAP نم تاعومجملا داريتسإ كنكمي ،تاعومجم بيوبتلا ةمالع نم



(WLC) ةيكلساللا ةيلحملا ةكبشلا يف مكحتلا رصنع نيوكت

ةيلحملا ةكبشلا يف مكحتلا رصنع نيوكتل روصلا هذه يف ةمدقملا تامولعملا مدختساً قيكلساللاا (WLC) قوداصمل (WLC) قيكلساللا



սիսիս cisco	MONITOR WLAN	s <u>C</u> ONTROLLER W <u>I</u> F	ELESS <u>S</u> ECURITY M	MANAGEMENT	C <u>O</u> MMANDS	HELP FEEDBACK
WLANs	WLANs > Edit	'piborowi_byod'				
WLANs WLANs	General Sec	curity QoS Polic	y-Mapping Advanc	ced		
P Advanced	Radius Servers Radius Servers Radius Server Server 1 IF Server 2 No Server 3 No Server 4 No Server 5 No	vers below to override r Overwrite interface	t:1813 • •	EAP Parameter Enable	rs	
	Server 6 No	one	▼ None	•		
uluili. cisco	MONITOR WLAN:	s <u>c</u> ontroller W <u>i</u> r	ELESS <u>s</u> ecurity M	MANAGEMENT	C <u>O</u> MMANDS	HELP FEEDBACK
WLANs	WLANs > Edit	'piborowi_byod'				
WLANs WLANs Advanced	General Sec	curity QoS Polic	y-Mapping Advanc	ced		

	ers				
Radius Se	rver Overwrite interface 📃	Ena	abled		
	Authentication Servers		Accounting Servers		EAP Parameter
	Enabled		Enabled		Enable
Server 1	IP:10.62.145.51, Port:1812	•	IP:10.62.145.51, Port:1813	•	
Server 2	None	٠	None	•	
Server 3	None	•	None	•	
Server 4	None	Ŧ	None	•	
Server 5	None	•	None		
		_		_	

EAP-GTC نيوكت

وه LDAP ل ةموعدملا ةقداصملا بيلاسأ دحأ EAP-GTC يف رفوتم وهو Cisco AnyConnect، فلم نيوكتل ةكبشلا ىلإ لوصولا ريدم فيرعت فلم ررحم تيبثت كيلع بجي نكلو جيحص لكشب فيرعتلا.

انه (يضارتفا لكشب) دوجوملا "ةكبشلا ىلإ لوصولا ريدم" نيوكت ريرحت كيلع بجي امك:

C: > ProgramData > Cisco > Cisco AnyConnect Secure Mobility Client > Network Access Manager (ماظنلا < (مَكْبِشْلَا يَلْإِلُوصُولَا رِيدُم) > Configuration.xml file

:ةياەنلا ةطقن ىلع EAP-GTC نيوكتل روصلا ەذە يف ةمدقملا تامولعملا مدختسأ

Client Policy	Profile:ility Client\Ne	twork Access M	anager\system\configuration.xm	1
Networks	Nome:	eap otc		Media Type
-3% Network Groups	Group Membership			Security Level
	To group:	Local networks		Connection Typ
				Credentials
	 In all groups (Global) 			Credentida
	Choose Your Network Media			
	Wired (802.3) Network			
	Select a wired network	if the endstations will be	connecting to the network	
	with a traditional ethern	net cable.		
	Wi Ei (wirdoor) Notword	4		
	WHY (Wreless) Network	ĸ		
	Select a WiFi network if	f the endstations will be	connecting to the network	
	via a wireless radio con	nection to an Access Po	int.	
	SSID (max 32 chars):	piborowi_byod		
		Hidden Netv	vork	
		Corporate N	etwork	
	Association Timeout	5	seconds	
		-	BECONDO	
	Common Settings			
	Script or application on each u	user's machine to run wh	en connected.	
			Browse Local Machine	
	Connection Timeout	40	seconds	

🚰 AnyConnect Profile Editor - N	letwork Access Manager						
File Help							
Network Access Manager	Networks Profile:ility Client\Network Access Manager\system\configuration.xml Security Level						
Network Groups	 Open Network Open networks have no security, and are open to anybody within range. This is the least secure type of network. Shared Key Network Shared Key Networks use a shared key to encrypt data between end stations and network access points. This medium security level is suitable for small/home offices. Authenticating Network Authenticating networks provide the highest level of security and are perfect for enterprise level networks. Authentication networks require radius servers, and other network infrastructure. 802. 1X Settings authPeriod (sec.) 30 startPeriod (sec.) 30 heldPeriod (sec.) 60 maxStart 3 	Security Level Connection Type User Auth Credentials					
	Next Cancel						

🚰 AnyConnect Profile Editor - N	letwork Access Manager	
File Help		
AnyConnect Profile Editor - File Help Network Access Manager Clent Policy Authentication Policy add Networks Network Groups	Network Access Manager Profile:ility Client\Network Access Manager\system\configuration.xml Network Connection Type Image: Machine Connection This should be used if the end station should log onto the network before the user logs in. This is typically used for connecting to domains, to get GPO's and other updates from the network before the user has access. Image: User Connection The user connection should be used when a machine connection is not needed. A user connection will make the network available after the user has logged on. Image: Machine and User Connection This type of connection will be made automatically when the machine boots. It will then be brought down, and back up again with different credentials when the user logs in.	Media Type Security Level Connection Type User Auth Credentials
	Next Cancel	

Client Policy Authentication Policy FAD Methods FAD Me	\configuration.xml
Network Groups	Media Type
© EAP-TLS	Connection Type
C EAP-TTLS C EAP-FAST	User Auth
© LEAP	Credentials
Extend user connection beyond log off	
EAP-PEAP Settings	
Validate Server Identity	
Enable Fast Reconnect	
Disable when using a Smart Card	
Inner Methods based on Credentials Source	
Authenticate using a Password	
EAP-MSCHAPv2	
EAP-GTC	
EAP-TLS, using a Certificate	
Authenticate using a Token and EAP-GTC	

🚰 AnyConnect Profile Editor - N	letwork Access Manager						
File Help							
Network Access Manager	Networks Profile:ility Client\Network Access Manager\system\configuration.xml						
Authentication Policy	User Identity Unprotected Identity Pattern: Protected Identity Pattern: User Credentials Use Single Sign On Credentials Prompt for Credentials Remember Foreve Remember while U Use Static Credentials	john.doe john.doe	Media Type Security Level Connection Type User Auth Credentials				
	Password: par	e Cancel					

ىلع ضيوفتلاو ةقداصملا تاسايس رييغتل روصلا هذه يف ةمدقملا تامولعملا مدختسأ ISE:

ahaha									Loarse Warring 🚠
cisco	Identity Serv	rices Engine		🙆 Home	Operations •	Policy •	Guest Access	Administration 💌	
📕 Aut	hentication	Authorization	🔀 Profiling	🖲 Posture	👸 Client Pro	ntsioning	🛃 TrustSec	🐴 Policy Elements	
Authent	ication Policy								
Define the	Authentication I	olicy by selecting th	ne protocols that ISE sh	hould use to co	mmunicate with th	ne network de	vices, and the iden	ity sources that it should	use for authentication.
For Policy I Rollog Typ	Export go to Adr	ninistration > System	n > Backup & Restore >	Policy Export	Page				
Party 199	a () shipa	() National							
	МАВ	: 1	f Wired_MAB OR Wireless_MAB			Alow I	rotocols : Default	Network Access	and
	🛃 Default		: use - Internal Endpoi	nts					
	Dot1X	: 1	f Wired_802.1X OR Wireless_802.1X			Allow I	Protocols : Default	Network Access	and
	🔄 Default		:USE LDAP_EXAMPLE						
	Default Rule	(If no match) : Al	low Protocols : Defaul	t Network Aco	055	and use :	Al_User_ID_Stores		

ahaha									License Warning A
CISCO Identity Services Engine			🟠 Home	Operations 🔻 Policy 🔻		Guest Access	Administration 💌		
🛓 Authen	tication 🛛 🙆 Authorization	🔀 Profiling	🗷 Posture	Gient Pro	visioning	🚊 TrustSec	🐥 Poli	ky Elements	
Authorization Policy									
Define the Aut	thorization Policy by configuring rules in the sector of depictment of the sector of t	based on identity	groups and/or o	ther conditions. Dr	rag and drop r	rules to change the o	der.		
FOIL POILLY EXDO	incigo to Administración > System > 1	oschup or nescure	> Porcy Export	raye					
First Matched	First Matched Rule Apples +								
• Exception	Exceptions (0)								
Standard									
0.000									
Status	Rule Name	Con	ditions (identity g	roups and other o	onditions)			Permissions	
. 🗹	Users in LDAP store	if (Without an	eless_802.1X AN domainusers, ou=	D LDAP_EXAMPLE groups,dc=maxcro	:ExternalGroup ;,dc=com)	ps EQUALS	then	PermitAccess	
1	Wireless Black List Default	if Blac	klist AND Wirele	ss_Access			then	Blackhole_Wireless_Acces	15
	Profiled Cisco IP Phones	if Cisc	o-IP-Phone				then	Cisco_IP_Phones	
	Profiled Non Cisco IP Phones	if Non	Cisco_Profiled_P	hones			then	Non_Osco_IP_Phones	
1	Basic_Authenticated_Access	if Net	work_Access_Aut	thentication_Passe	d		then	PermitAccess	
	Default	if no ma	tches, then D	enyAccess					

ةكبشلاب لاصتالا ىلع ارداق نوكت نأ بجي ،نيوكتلا قيبطت دعب:

S Cisco AnyCo	nnect Secure Mobility Client	
	Network: Connected (10.0.13.87) eap_gtc	e ili -
¢ (i)		a judu cisco

ةحصلا نم ققحتلا

لاصتا مادختساب تاعومجملاو تاعوضوملا دادرتساب مق ،ISE و LDAP تانيوكت نم ققحتلل مداخلاب رابتخإ:

ahaha						Licen	es Warning A
cisco Identity Services	: Engine	🙆 Home 🛛 C	operations 💌 Policy 🔍	Guest Access	iministration 1 🔻		
😽 System 🛛 👹 Identit	y Management	Network Resources 🛛 🛃 D	evice Portal Management	🙀 pxGrid Services	Feed Service	1 pxGnd Identit	y Mapping
Identities Groups	External Identity Sour	Identity Source Seque	moes Settings				
External Identity Sources	©	LDAP Identity Sources List > LDAP LDAP Identity Source General Connect	EXAMPLE ection Directory Or	nanitation Group	s Attrivitos		
Certificate Authentication	Profile		Primary Server	Bind successful to 10.61.1	105.242.389		Secondary S
* COAP				Result of festing this conf Number of Subjects: 2 Number of Groups: 1	guration is as follows:		Enable S
RADIUS Token		* Hostname/IP	10.61.106.242			Hostname/IP	
 RSA SecuriD 		* Port	389	Response time:1636ms		Port	.389
		Access Admin DN	Anonymous Access Authenticated Access Ton=Manager.dc=maxgs		ок	Access Admin DN	 Anonymo Authentics
		Password	* *****			Password	
		Secure Authentication	Enable Secure Authentica	lion	re Authentication	Enable Se	
		Root CA	Certificate Services Endpoint	t.*		Root CA	Certificate Se
		* Server Timeout	10	ØSeconds		Server Timeout	10
		* Max. Admin Connections	20	æ	Max. Adr	min Connections	20
		1	Test Bind to Server				Test Bind t
		•			"		
		Save					

:ISE لا نم ايجذومن اريرقت روصلا هذه حضوت

i 1. to Identity Services	Engine	Barne Decretions	Point & Guest Acress	 Administration 	Timer W	anning 🔥 Andā s
Authentications 🚊 👖	Reports 🛛 🙀 Endp	aint Protection Service 💦 Troubleshoot				
Misconfigured Suppli 1	kanta 🗹	Misconfigured Network Devices (3) 0	U	0105 Drops © 1305	Clent St	opped Responding ⁽²⁾ O
haw Live Sessions – 🎡 Add a	r Remove Columns 💌 🍪	Refrech 🔯 Reset Repeat County			Refre	sh Every 1 minute
• Status Al	Details Repeat Con	Int Identity C Endpoint ID C	Indpoint Profile T Authentic	ition Policy 🛞	Authorization Policy	Authorization Pro
06-04 21:50:45.538	à	0 johnudoe C0:4A:00:14:80:48 W	Vindows7-Workst			
)verview						
)verview Event		5200 Authentica	ition succeeded			
)verview Event Username		5200 Authentica john.doe⊕	ition succeeded			
)verview Event Username Endpoint Id		5200 Authentica john.doe C0:4A:00:14:8D:	tion succeeded :4B⊕			
)verview Event Username Endpoint Id Endpoint Profile	e	5200 Authentica john.doe C0:4A:00:14:8D: Windows7-Work	tion succeeded :4B⊕ kstation			
Dverview Event Username Endpoint Id Endpoint Profile Authentication	e Policy	5200 Authentica john.doe € C0:4A:00:14:8D: Windows7-Work Default >> Dot1)	tion succeeded :4B⊕ kstation X >> Default			

Authorization Result PermitAccess

Authentication Details	
Source Timestamp	2015-06-04 21:59:45.509
Received Timestamp	2015-06-04 21:59:45.51
Policy Server	ise13
Event	5200 Authentication succeeded
Failure Reason	
Resolution	
Root cause	
Username	john.doe
User Type	
Endpoint Id	C0:4A:00:14:8D:4B
Endpoint Profile	Windows7-Workstation
IP Address	
Authentication Identity Store	LDAP_EXAMPLE
Identity Group	Workstation
Audit Session Id	0a3e9465000010035570b956
Authentication Method	dot1x
Authentication Protocol	PEAP (EAP-GTC)
Service Type	Framed
AD ExternalGroups	cn=domainusers,ou=groups,dc=maxcrc,dc=com
IdentityDn	uid=john.doe,ou=people,dc=maxcrc,dc=com
RADIUS Username	john.doe

اهحالصإو ءاطخألا فاشكتسا

ةيفيكو نيوكتلا اذه عم اهتفداصم متت يتلا ةعئاشلا ءاطخألا ضعب مسقلا اذه فصي اهحالصإو ءاطخألا فاشكتسأ:

- ليغشت ةداعإب مق ،gssapi.dll نادقف ىلإ ةراشإلل أطخ تەجاو اذإ ،OpenLDAP تيبثت دعب Microsoft Windows.
- ظفحا .ةرشابم Cisco AnyConnect ل configuration.xml فلم ريرحت انكمم نوكي ال دق ميدقلا فلملا لادبتسال ممدختسا مث رخآ عقوم يف ديدجلا نيوكتلا.
- هذه أطخلا ةلاسر دجوت ،ةقداصملا ريرقت يف

<#root>

Authentication method is not supported by any applicable identity store

LDAP. ةطساوب دمتعم ريغ هترتخإ يذلا بولسألا نأ ىلإ هذه أطخلا ةلاسر ريشت

ا EAP-GTC) ةموعدملا قرطلا ىدحإ حضوي ريرقتلا سفن يف ةقداصملا لوكوتورب نأ نم دكأت وأ EAP-TLS وأ PEAP-TLS وأ

ال ،تايوهلا نزخم يف عوضوملا ىلع روثعلا مدع تظحال اذإ ،ةقداصملا ريرقت يف
 قدعاق يف مدختسم يأل عوضوملا مسا قمس عم ريرقتلا نم مدختسملا مسا قباطتي
 LDAP.

رظني ISE نأ ينعي امم ،ةمسلا هذهل ديرف فرعم ىلإ ةميقلا نييعت مت ،ويرانيسلا اذه يف قباطت ىلع روثعلا لواحي امدنع LDAP مدختسمب ةصاخلا مدختسملا فرعم ميق ىلإ.

، مداخلاب طبر رابتخإ ءانثأ حيحص لكشب تاعومجملاو تاعوضوملا دادرتسإ متي مل اذإ ثحبلا دعاوقل حيحص ريغ نيوكت اذهف.

نأ نكمي) dc و رذجلا ىلإ ةيفرطلا ةدحولا نم LDAP ل يمرهلا جردتلا ديدحت بجي هنأ ركذت (ةددعتم تاملك نم نوكتي).

المات كي المات WLC، <u>ققداصم</u> ىل عجرا WLC، <u>ققداصم</u> ىل عجرا الانتسم (WLC<u>) قيكل سال ل المي لعمل المكين المكوت تادحو نيوكت ل اثم مادخت ساب EAP</u> Cisco.

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