# Configurer l'ISE pour l'intégration à un serveur LDAP

# Table des matières

Introduction
Conditions préalables
Exigences
Composants utilisés
Informations générales
Configurer
Diagramme du réseau
Configurer OpenLDAP
Intégrer OpenLDAP à l'ISE
Configurer le WLC
Configurer EAP-GTC
Vérifier
Dépannage

# Introduction

Ce document décrit comment configurer un moteur Cisco Identity Services Engine (ISE) pour l'intégration à un serveur Cisco LDAP.

# Conditions préalables

## Exigences

Aucune exigence spécifique n'est associée à ce document.

## Composants utilisés

Les informations contenues dans ce document sont basées sur les versions logicielles et matérielles suivantes :

- Cisco ISE version 1.3 avec correctif 2
- Microsoft Windows Version 7 x64 avec OpenLDAP installé
- Contrôleur LAN sans fil Cisco (WLC) version 8.0.10.0
- Cisco AnyConnect version 3.1 pour Microsoft Windows

• Éditeur de profil Cisco Network Access Manager

Remarque : ce document est valide pour les configurations qui utilisent LDAP comme source d'identité externe pour l'authentification et l'autorisation ISE.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

# Informations générales

Ces méthodes d'authentification sont prises en charge avec LDAP :

- Extensible Authentication Protocol Carte à jeton générique (EAP-GTC)
- Protocole EAP-TLS (Extensible Authentication Protocol Transport Layer Security)
- Protocole PEAP-TLS (Protected Extensible Authentication Protocol Transport Layer Security)

## Configurer

Cette section décrit comment configurer les périphériques réseau et intégrer l'ISE à un serveur LDAP.

#### Diagramme du réseau

Dans cet exemple de configuration, le point d'extrémité utilise une carte sans fil afin de s'associer au réseau sans fil.

Le réseau local sans fil (WLAN) sur le WLC est configuré afin d'authentifier les utilisateurs via l'ISE. Sur ISE, LDAP est configuré en tant que magasin d'identités externe.

Cette image illustre la topologie de réseau utilisée :



## Configurer OpenLDAP

L'installation d'OpenLDAP pour Microsoft Windows est effectuée via l'interface graphique utilisateur, et c'est simple. L'emplacement par défaut est C: > OpenLDAP. Après l'installation, vous devriez voir ce répertoire :

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	
🌗 ldifdata	6/4/2015 11:03 AM	File folder	
\mu Readme	6/3/2015 5:06 PM	File folder	
🐌 replica	6/3/2015 5:06 PM	File folder	
퉬 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	
퉬 SQL	6/3/2015 5:06 PM	File folder	
🐌 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
📧 slapacl.exe	5/11/2015 10:59 PM	Application	3,711 KB

Prenez note de deux répertoires en particulier :

- ClientTools Cet annuaire inclut un ensemble de binaires qui sont utilisés afin de modifier la base de données LDAP.
- Idifdata II s'agit de l'emplacement dans lequel vous devez stocker les fichiers avec des objets LDAP.

Ajoutez cette structure à la base de données LDAP :



Dans le répertoire Root, vous devez configurer deux unités d'organisation (OU). L'unité d'organisation OU=groups doit avoir un groupe enfant (cn=domainusers dans cet exemple).

L'unité d'organisation OU=people définit les deux comptes d'utilisateur qui appartiennent au groupe cn=domainusers.

Pour remplir la base de données, vous devez d'abord créer le fichier ldif. La structure mentionnée précédemment a été créée à partir de ce fichier :

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

Afin d'ajouter les objets à la base de données LDAP, utilisez le binaire Idapmodify :

```
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_new_socket: 496
ldap_prepare_socket: 496
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 "uid=john.doe,ou=people,dc=maxcrc,dc=com"
adding new entry "uid=jan.kowalski,ou=people,dc=maxcrc,dc=com"
```

#### Intégrer OpenLDAP à l'ISE

Utilisez les informations fournies dans les images tout au long de cette section afin de configurer LDAP en tant que magasin d'identités externe sur l'ISE.

aluh		Liceose Warning 🔒
CISCO Identity Services Engine	Administration I▼ Policy I▼ Guest Access I▼ Administration I▼	
🔆 System 🛛 😥 Identity Management	🖬 Network Resources 🛛 🛃 Device Portal Management 🛛 🙀 pxGnd Services 🛛 🙀 Feed Service	LepxGrid Identity Mapping
Identities Groups External Identity S	urces Identity Source Sequences Settings	
Extended Lifentity Sources  External Identity Sources  Certificate Authenticaton Profile  Active Directory  CIDAP  DAP  DAP  DAP  RADUS Token  RSA SecuriD	LDAP Identity Source Settleres       Settleres         LDAP Identity Source       Connection         General       Connection         * Name       LDAP_EXAMPLE         Description	
	(Durigue is new	
	Save Reset	

Vous pouvez configurer ces attributs à partir de l'onglet Général :

- Subject Objectclass Ce champ correspond à la classe d'objet des comptes d'utilisateurs dans le fichier Idif. Selon la configuration LDAP. Utilisez l'une des quatre classes suivantes :
  - Haut
  - Personne
  - PersonneOrganisationnelle
  - PersonnelnetOrg
- Attribut de nom de sujet Attribut récupéré par le serveur LDAP lorsque l'ISE demande si un nom d'utilisateur spécifique est inclus dans une base de données. Dans ce scénario, vous devez utiliser john.doe ou jan.kowalski comme nom d'utilisateur sur le point d'extrémité.
- Group Objectclass Ce champ correspond à la classe d'objet d'un groupe dans le fichier ldif. Dans ce scénario, la classe d'objet pour le groupe cn=domainusers est posixGroup.
- Attribut de mappage de groupe Cet attribut définit la façon dont les utilisateurs sont mappés aux groupes. Sous le groupe cn=domainusers dans le fichier ldif, vous pouvez voir deux attributs memberUid qui correspondent aux utilisateurs.

ISE propose également des schémas préconfigurés (Microsoft Active Directory, Sun, Novell) :

aluh		License Warning 🚠
cisco Identity Services Engine	⚠ Home Operations I ▼ Policy I ▼ Guest Access I ▼ Administration I ▼	
🔆 System 🛛 💆 Identity Management	📲 Network Resources 🛛 🛃 Device Portal Management 🛛 😡 pxGrid Services 🖉 Feed Service	Reproductive Mapping
Identities Groups External Identity So	urces Identity Source Sequences Settings	
External Identity Sources	LDAP Identity Source:         LDAP_DAP Identity Source:           General         Connection         Directory Organization         Groups         Attributes	
Active Directory	Primary Server	Secondary S
🔻 🚞 LDAP		Enable Se
TOAP_EXAMPLE		
RADUS Token	* Hosmamel/P 10.61.106.242	Hostname/IP
	P011 309	Port 389
	Access O Anonymous Access	Access  Anonymo
	Authenticated Access	Authentic
	Parsword <sup>1</sup>	Password
		1 435/1014
	Basue Adhanishing Casula Secure Adhanishing Casu	un Authoritanian 🗌 Enable Ca
	Root CA Certificate Services Endnoted *	Root CA Cartificate Sc
		Cerdicate a
	A Descent Thread in a Descent of the second	Construct 10
	*Server Imeout 10 (Asconos	Server Timeout 10
	· Wax Admin Connections 20 Wax Ad	min Connections 20
	Test Brid to Server	Test Bind t
	Seve [ Reset ]	

Après avoir défini l'adresse IP et le nom de domaine administratif corrects, vous pouvez tester la liaison au serveur. À ce stade, vous ne récupérez aucun objet ou groupe, car les bases de recherche ne sont pas encore configurées.

Dans l'onglet suivant, configurez la base de recherche des sujets/groupes. Il s'agit du point de jonction entre l'ISE et le LDAP. Vous ne pouvez récupérer que les sujets et les groupes qui sont des enfants de votre point de jonction.

Dans ce scénario, les sujets de l'OU=people et les groupes de l'OU=groups sont récupérés :

abab		Lizense Warning A
CISCO Identity Services Engine	Home Operations I▼ Policy I▼ Guest Access I▼ Administration I▼	
System Zidentity Management Identities Groups External Identity Sour	Network Resources 🛃 Device Portal Management 💽 pxGrid Services 🗔 Feed Service 4 px	Grid Identity Mapping
External Identity Sources	LDAP Identity Sources Lot > LDAP_EXAMPLE LDAP Identity Source General Connection Directory Organization Groups Attributes  * Subject Search Base ou=people,dc=maxrc,dc=com Naming Contexts	
<ul> <li>EANP_CCAMPLE</li> <li>RACIUS Token</li> <li>RSA SocurID</li> </ul>	Search for MAC Address in Format Address in Format Address and Address in Format Address and Address in Format Address and Address and Address	

Dans l'onglet Groups, vous pouvez importer les groupes à partir du LDAP sur l'ISE :



## Configurer le WLC

Utilisez les informations fournies dans ces images afin de configurer le WLC pour l'authentification 802.1x :

սիսիս cisco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP EEEDBACK
WLANs	WLANs > Edit 'piborowi_byod'
WLANS	General Security QoS Policy-Mapping Advanced
Advanced	Layer 2 Layer 3 AAA Servers
	Layer 2 Security  WPA+WPA2 MAC Filtering?
	Fast Transition       Fast Transition
	Protected Management Frame PMF Disabled
	WPA+WPA2 Parameters
	WPA Policy
	WPA2 Policy-AES
	802.1X Enable

ပါပါပ cisco	<u>M</u> ONITOR <u>W</u> LANS <u>C</u> ONTROLLER WIRELESS <u>S</u> ECURITY MANAGEMENT C <u>O</u>	OMMANDS HELP FEEDBACK
WLANs	WLANs > Edit 'piborowi_byod'	
WLANS	General Security QoS Policy-Mapping Advanced	
Advanced	Layer 2 Layer 3 AAA Servers	
	Select AAA servers below to override use of default servers on this WLAN Radius Servers Radius Server Overwrite interface	
	Authentication Servers Accounting Servers EA	P Parameters
	✓ Enabled ✓ Enabled	Enable 🔲
	Server 1 IP:10.62.145.51, Port:1812    IP:10.62.145.51, Port:1813	
	Server 2 None VNone V	
	Server 3 None   None	
	Server 4 None V None V	
	Server 5 None   None	
	Server o None V None V	
uluulu cisco	<u>M</u> ONITOR <u>W</u> LANS <u>C</u> ONTROLLER W <u>I</u> RELESS <u>S</u> ECURITY M <u>A</u> NAGEMENT C <u>I</u>	<u>o</u> mmands he <u>l</u> p <u>e</u> eedback
WLANs	WLANs > Edit 'piborowi_byod'	
WLANS	General Security QoS Policy-Mapping Advanced	
Advanced	Layer 2 Layer 3 AAA Servers	
	Select AAA servers below to override use of default servers on this WLAN	

Radius Se	rver Overwrite interface 🛛 🗉 E	nabled	
	Authentication Servers	Accounting Servers	EAP Parameter
	Enabled	Enabled	Enable
Server 1	IP:10.62.145.51, Port:1812	<ul> <li>IP:10.62.145.51, Port:1813</li> </ul>	•
Server 2	None	<ul> <li>None</li> </ul>	•
Server 3	None	- None	•
Server 4	None	- None	*
Server 5	None	<ul> <li>None</li> </ul>	•
S		Nees	

## **Configurer EAP-GTC**

EAP-GTC est l'une des méthodes d'authentification prises en charge pour LDAP. Il est disponible dans Cisco AnyConnect, mais vous devez installer l'Éditeur de profil Network Access Manager pour configurer correctement le profil.

Vous devez également modifier la configuration du Gestionnaire d'accès réseau, qui (par défaut) se trouve ici :

C: > ProgramData > Cisco > Cisco AnyConnect Secure Mobility Client > Network Access Manager > system > fichier configuration.xml

Utilisez les informations fournies dans ces images afin de configurer l'EAP-GTC sur le terminal :

Local networks	Security Level Connection Typ User Auth Credentials
Local networks -	Connection Typ User Auth Credentials
Local networks v	User Auth Credentials
ς	Credentials
¢	-1
¢ .	
if the endstations will be connecting to the network	
net cable.	
rk	
f the endstations will be connecting to the network	
nnection to an Access Point.	
piborowi_byod	
Hidden Network	
Corporate Network	
5 seconds	
5 BECONDS	
	net cable. k f the endstations will be connecting to the network nection to an Access Point. piborowi_byod Hidden Network Corporate Network 5 seconds user's machine to run when connected.

🚰 AnyConnect Profile Editor - N	letwork Access Manager	
File Help		
Network Access Manager	Networks Profile:ility Client\Network Access Manager\system\configuration.xml Security Level	Media Type
Network Groups	<ul> <li>Open Network Open networks have no security, and are open to anybody within range. This is the least secure type of network.</li> <li>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.</li> <li>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.</li> <li>802. 1X Settings authPeriod (sec.) 30 startPeriod (sec.) 30 heldPeriod (sec.) 60 maxStart 3</li> </ul>	Security Level Connection Type User Auth Credentials
	Next Cancel	

🚰 AnyConnect Profile Editor - N	letwork Access Manager	
File Help		
AnyConnect Profile Editor - N File Help Network Access Manager Clent Policy Authentication Policy 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	

Authentication Policy Networks	EAP Methods -	Media Type
Network Groups	@ FAP-TLS @ PEAP	Security Level
	0	Connection Typ
	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	
	O 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.xm	1
Network Groups	User Identity — Unprotected Identity Pattern: Protected Identity Pattern: User Credentials © Use Single Sign On Credentials © Remember Forever) © Remember Forever) © Never Remember © Use Static Credentials Password: passwo	john.doe john.doe	Media Type Security Level Connection Type User Auth Credentials
	Done	Cancel	

Utilisez les informations fournies dans ces images afin de modifier les stratégies d'authentification et d'autorisation sur l'ISE :

ahaha										Loarse Warring 🚠
cisco	Identity Serv	rices Engine		🙆 Home	Operations   •	Policy   •	Guest Access	Administration -		
📕 Aut	hentication	S Authorization	🛃 Profiling	🖲 Posture	👸 Client Pro	visioning	🚉 TrustSec	🐴 Policy Elements		
Authent	ication Policy									
Define the	Authentication F	Policy by selecting th	e protocols that ISE sh	ould use to con	municate with th	e network de	vices, and the ident	ity sources that it should	i use for authenticatio	n.
For Policy Policy Typ	Export go to Adm e O Simple	<ul> <li>ninistration &gt; System</li> <li>Rule-Based</li> </ul>	I > Backup & Restore >	Policy Export P	age					
	МАВ	: 1f	Wired_MAB OR Wireless_MAB			Allow P	rotocols : Default	Network Access	and	
	🛃 Default		: use Internal Endpol	ints						
	Dot1X	: 1f	Wired_802.1X OR Wireless_802.1X			Allow P	rotocols : Default	Network Access	and	
	🔄 Default	[	USA LDAP_EXAMPLE							
	Default Rule	(If no match) : All	ow Protocols : Defaul	t Network Acces	25	and use :	Al_User_ID_Stores	i		

aha	dis anti-										License Warning A
cise	co Iden	tity Services Engine		🟠 Home	Operations I 🔻	Policy   •	Guest Access 🖛	Adm	inistration 🛛		
4	Authentica	ation 🕒 Authorization	🔣 Profiling	🖄 Posture	Gient Pro	visioning	🔁 TrustSec	🐥 Poli	cy Elements		
Auth	orization	Policy									
Define For Pol	the Autho icy Export	rization Policy by configuring rules $b = 0$ to Administration > System > B	ased on iden lackup & Rest	tity groups and/or of tore > Policy Export (	ther conditions. Dr	ag and drop i	rules to change the o	rder.			
100 000	cy copore	ge to namine accord is appendix o	to map or need	and a reacy capace							
First M	latched Ru	le Applies 🔻									
) Ex	ceptions	(0)									
Sta	ndard										
_	Status	Rule Name	(	Conditions (identity g	roups and other co	onditions)			Permissions		
1	2	Users in LDAP store	if (	Wireless_802.1X AN m=domainusers.ou=	D LDAP_EXAMPLE: groups,dc=maxtre	ExternalGrou ,dc=com )	ps EQUALS	then	PermitAccess		
ł	2	Wireless Black List Default	if t	Blacklist AND Wirele	ss_Access			then	Blackhole_Wire	less_Access	
Ĩ	2	Profiled Cisco IP Phones	iř. (	Cisco-IP-Phone				then	Cisco_IP_Phone	es	
Ī	~	Profiled Non Cisco IP Phones	f 1	Non_Cisco_Profiled_P	hones			then	Non_Osco_IP_	Phones	
÷	2	Basic_Authenticated_Access	if I	Network_Access_Aut	hentication_Passe	đ		then	PermitAccess		
	2	Default	if no	matches, then De	enyAccess						

Après avoir appliqué la configuration, vous devriez pouvoir vous connecter au réseau :

S Cisco AnyCor	nnect Secure Mobility Client	
	Network: Connected (10.0.13.87) eap_gtc	
<b>\$</b> (i)		بالبيل. cisco

# Vérifier

Afin de vérifier les configurations LDAP et ISE, récupérez les sujets et les groupes avec une connexion test au serveur :

CESCO Telentity Services Fagins  I home Operators * Poky * Guet Access * Anoministration *  Services Fagins  I home Operators * Poky * Guet Access * Anoministration *  Services Fagins  I home Operators * Poky * Guet Access * Anoministration *  Services Fagins  I home Operators * Poky * Guet Access * Anoministration *  Centered Identity Sources  I home Operators * Poky * Guet Access * Anoministration *  Centered Identity Sources  I home Operators * Poky * Guet Access * Anoministration *  Centered Identity Sources  I home Operators * Dental Management  I home Operators * Poky * Guet Access *  I home Operators * Poky * Guet Access *  I home Operators *  I home of Groups *  I home of Bugets *  I home	ախալիս						Liow	w Warning A
	cisco Identity Services En	igine	🏠 Home 🔇	Operations 💌 Policy 🖃	Guest Access	Administration 1 🔻		
Verticitis       Verticity Sources       Methy Sources       Settings         Consection       Consection </th <th>😽 System 🛛 🛃 Identity Ma</th> <th>inagement 🛛 🖬 Netwo</th> <th>ork Resources 🛛 🛃 D</th> <th>evice Portal Management</th> <th>😹 pxGrid Services</th> <th>Feed Service</th> <th>Le pxGnd Identit</th> <th>y Mapping</th>	😽 System 🛛 🛃 Identity Ma	inagement 🛛 🖬 Netwo	ork Resources 🛛 🛃 D	evice Portal Management	😹 pxGrid Services	Feed Service	Le pxGnd Identit	y Mapping
Deternal Identity Sources         Image: Source Authentication Profile         Image: Advector         Image: Source Authentication Profile         Image: Advector         Image: Source Authentication Profile         Image: Source Authentication         Image: Sour	Identities Groups	ctemal Identity Sources	Identity Source Seque	ences Settings				
Certificate Authentication Profile Active Directory Case Active Directory Case Data Economy Server Bind successful to 10.81.108.242.339 Result of fasting this configuration is as follows: Number of Subjects: 2 Number of Subj	External Identity Sources		dentity Sources List > LDAP, P Identity Source General Conn	EXAMPLE	cantration Sco	uns Attributes		
<ul> <li>Result of testing this configuration is as follows: Number of Stropes: 1 * RADIUS Token * Server Timeout 10 * Max. Admin Connections 20 * Tax Bind to Sarvar * Rest</li> </ul>	Certificate Authentication Prof     Actus Directory	file		Primary Server	Bind successful to 10.6	1.108.242.389		Secondary S
<ul> <li>* RADUS Token</li> <li>* HastnamedP</li> <li>* RSA Securit</li> <li>* HastnamedP</li> <li>* Port 380</li> <li>Access</li> <li>Anonymous Access</li> <li>Anonymous Accesters<td>* DAP_EXAMPLE</td><td></td><td></td><td></td><td>Result of testing this co Number of Subjects: 2 Number of Grouper, 1</td><td>nfiguration is as follows: 2</td><td></td><td>Enable S</td></li></ul>	* DAP_EXAMPLE				Result of testing this co Number of Subjects: 2 Number of Grouper, 1	nfiguration is as follows: 2		Enable S
Read	RADIUS Token		* Hostname/IP	10.61.106.242	Hamber of Groups. 1		Hostname/IP	
Access Anonymous Access Authenticated Access Authenticated Access Authenticated Access Authenticated Access Authenticated Access Admin DN Password Password Becure Authentication Enable Secure Authentication Root CA Certificate Services Endpoint * Secure Authentication Enable Sec Root CA Certificate Services Endpoint * Server Timeout 10 * Max. Admin Connections 20 Test End to Server Root CA Certificate Server Access Anonymo Access Anonymo Access Anonymo Authentic Authent	<ul> <li>RSA SecuriD</li> </ul>		* Port	389	Response time:1636m	15	Port	389
Password * ••••• Password * ••••• Password *			Access Admin DN	Anonymous Access     Authenticated Access     Ton=Manager,dc=maxore		ОК	Access Admin DN	<ul> <li>Anonymo</li> <li>Authentics</li> </ul>
Secure Authentication Enable Secure Authentication Root CA Certificate Services Endpoint *  * Server Timeout 10 * Max. Admin Connections 20  Test Root to Server  Test Root to Server  *  * * * * * * * * * * * * * * * * *			Password	* *****			Password	
Secure Authentication Enable Secure Authentication Secure Authentication Enable Secure Authentication E								
Root CA       Certificate Services Endpoint *       Root CA       Certificate Services Endpoint *         * Server Timeoul       10       Ø Boconds       Server Timeoul       10         * Max. Admin Connections       20       Ø       Max. Admin Connections       20         ( Test Bind to Server)       Test Bind to Server       Test Bind to Server       Test Bind to Server			Secure Authentication	Enable Secure Authentical	tion	Sec	ure Authentication	Enable Se
* Server Timeout 10 (FiSoconds Server Timeout 10 * Max. Admin Connections 20 (Test Bind to Server) * Test Bind to Server) * Test Bind to Server Timeout 10 Test Bind to Server Timeout 10 * Max. Admin Connections 20 Test Bind to Server Timeout 10 * Max. Admin Connections 20			Root CA	Certificate Services Endpoint	: *		Root CA	Certificate S
* Server Timeout 10  * Max. Admin Connections 20  * Max. Admin Connections 20  * Test Bind to Server  *  Save Reset								
* Max. Admin Connections 20 (Test Bind to Server) (Test Bind to Server) (Test Bind to Server) (Test Bind to Server)			* Server Timeput	10	0.Seconds		Server Timeout	10
Test Bind to Server			Max. Admin Connections	20	w	Max. A	dmin Connections	20
۲ Save Roset				Test Bind to Server				Test Bind t
Save Reset		75						
			e Reset					

Ces images illustrent un exemple de rapport de l'ISE :

cisco Identity Services Engine	The Operations Policy	Guest Access      Administration      T	Licrosz Waxnine, 🔥   Kretił   odnin
🔟 Authentications 📑 Reports 🔤 E	ndpoint Protection Service 💊 Troubleshoot		
Nisconfigured Supplicanta 🛞 1	Misconfigured Network Devices (8) 0	RAONUS Drops (C) 1305	Clent Stopped Responding (2) 0
🛃 Shaw Live Sessions – 🎡 Add ar Remove Columns 💌	🏀 Refrech 🛛 🔞 Reset Repeat Counts		Refresh Every 1 minute *
ime v Status Al v Detais Repeat	Count identity () Endpoint () () Endpoint ()	Authentication Policy (2) Author	Authorization Profiles
2015-06-04 21:50:45.538 🕚 🚡 2015-06-04 21:59:45.510 🛛 🚡	0 johnuloe         C0x4Ax00:14:80:48         Windows7-           johnuloe         C0x4Ax00:14:80:48         Windows7-	Workst Default >> Dot1X >> Default Default	t >> Users in LDAP store PermitAccess
Overview	5200 Authentication s	ucceeded	
Username	john.doe⊕		
Endpoint Id	C0:4A:00:14:8D:4B 🕀		
Endpoint Profile	Windows7-Workstatio	n	
Authentication Policy	Default >> Dot1X >> D	Default	
Authorization Policy	Default >> Users in L	DAP store	
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

# Dépannage

Cette section décrit quelques erreurs courantes rencontrées avec cette configuration et explique comment les résoudre :

- Après l'installation d'OpenLDAP, si vous rencontrez une erreur indiquant qu'un gssapi.dll est manquant, redémarrez Microsoft Windows.
- Il n'est peut-être pas possible de modifier le fichier configuration.xml pour Cisco AnyConnect directement. Enregistrez votre nouvelle configuration à un autre emplacement, puis utilisezla pour remplacer l'ancien fichier.
- Le rapport d'authentification contient le message d'erreur suivant :

#### <#root>

Authentication method is not supported by any applicable identity store

Ce message d'erreur indique que la méthode sélectionnée n'est pas prise en charge par LDAP.

Assurez-vous que le protocole d'authentification dans le même rapport affiche l'une des méthodes prises en charge (EAP-GTC, EAP-TLS ou PEAP-TLS).

• Dans le rapport d'authentification, si vous remarquez que l'objet n'a pas été trouvé dans le magasin d'identités, le nom d'utilisateur du rapport ne correspond pas à l'attribut Nom de l'objet pour tout utilisateur de la base de données LDAP.

Dans ce scénario, la valeur a été définie sur uid pour cet attribut, ce qui signifie que l'ISE recherche les valeurs uid pour l'utilisateur LDAP lorsqu'il tente de trouver une correspondance.

• Si les sujets et les groupes ne sont pas récupérés correctement lors d'un test de liaison au serveur, la configuration des bases de recherche est incorrecte.

N'oubliez pas que la hiérarchie LDAP doit être spécifiée de leaf à root et dc (peut être constituée de plusieurs mots).

Conseil : Afin de dépanner l'authentification EAP du côté du WLC, référez-vous au document <u>Exemple de configuration d'authentification EAP avec des contrôleurs WLAN (WLC)</u> Cisco.

### À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.