

# LDAP サーバと統合するための ISE の設定

## 内容

---

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[設定](#)

[ネットワーク図](#)

[OpenLDAP の設定](#)

[OpenLDAP と ISE の統合](#)

[WLC の設定](#)

[EAP-GTC の設定](#)

[確認](#)

[トラブルシューティング](#)

---

## はじめに

このドキュメントでは、Cisco LDAPサーバと統合するためにCisco Identity Services Engine(ISE)を設定する方法について説明します。

## 前提条件


### 要件

このドキュメントに関する固有の要件はありません。

### 使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- パッチ 2 が適用された Cisco ISE バージョン 1.3
- OpenLDAP がインストールされた Microsoft Windows 7 x64
- Cisco Wireless LAN Controller ( WLC ) バージョン 8.0.100.0
- Microsoft Windows 向け Cisco AnyConnect バージョン 3.1
- Cisco Network Access Manager プロファイル エディタ

 注：このドキュメントは、ISE認証および認可の外部アイデンティティソースとしてLDAPを使用する設定に有効です。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

## 背景説明

LDAP では、次の認証方式がサポートされます。

- 拡張認証プロトコル – 汎用トークンカード(EAP-GTC)
- Extensible Authentication Protocol - Transport Layer Security(EAP-TLS)
- Protected Extensible Authentication Protocol - Transport Layer Security(PEAP-TLS)

## 設定

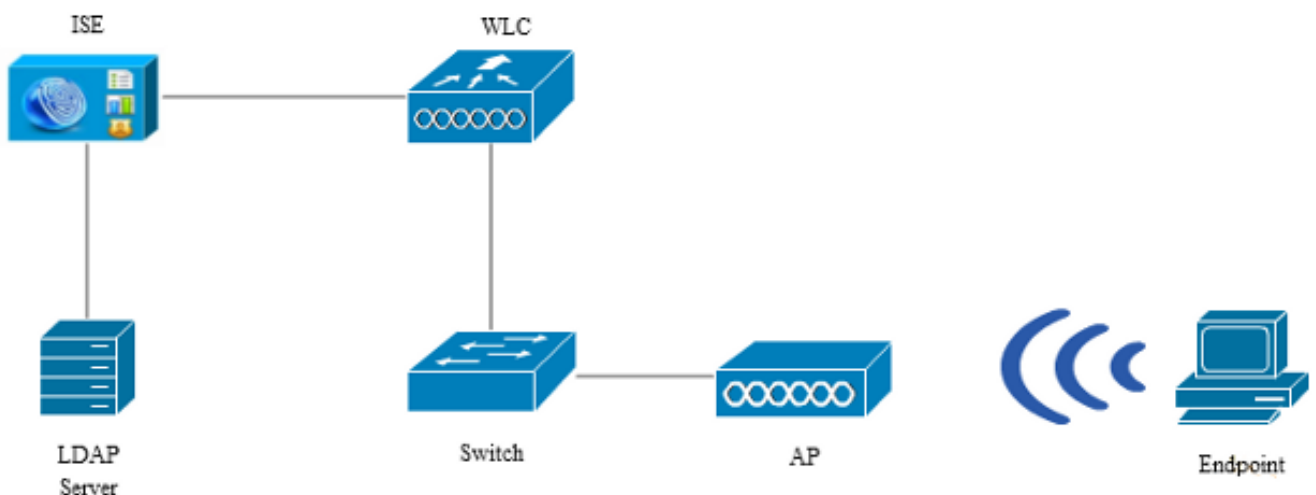
ここでは、ネットワーク デバイスを設定して ISE に LDAP サーバを統合する方法を説明します。

### ネットワーク図

この設定例では、エンドポイントでワイヤレス アダプタを使用してワイヤレス ネットワークに関連付けます。





























WLC 上のワイヤレス LAN ( WLAN ) は、ISE を介してユーザを認証するように設定します。ISE では、LDAP を外部 ID ストアとして設定します。

次の図に、使用するネットワーク トポロジを示します。



## OpenLDAP の設定

OpenLDAP for Microsoft Windows は、GUI を使用して簡単にインストールできます。デフォルトの場所はC: > OpenLDAPです。インストールが完了すると、このディレクトリは次のように表示されます。

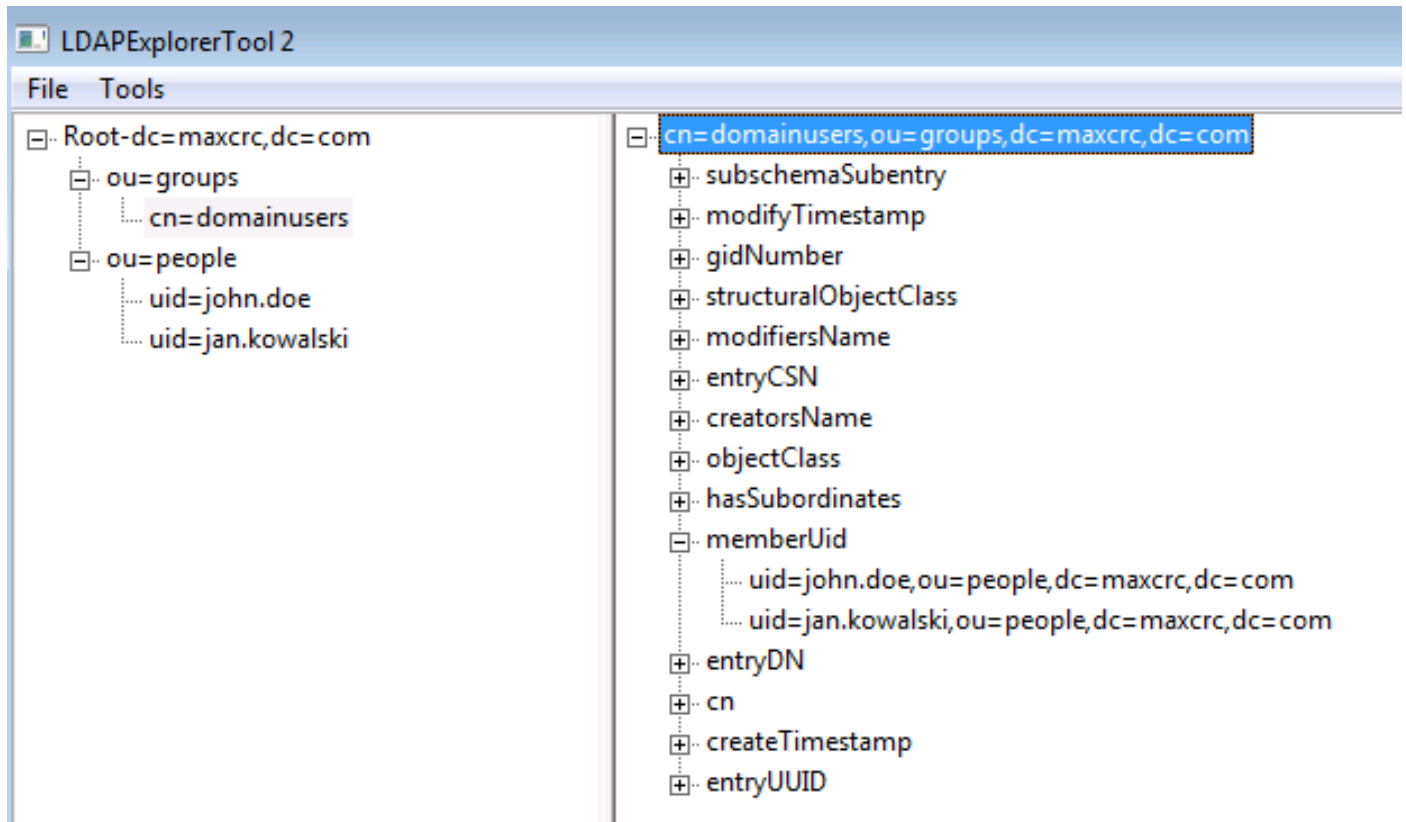
Name	Date modified	Type	Size
 BDBTools	6/3/2015 5:06 PM	File folder	
 ClientTools	6/3/2015 5:06 PM	File folder	
 data	6/4/2015 9:09 PM	File folder	
 Idifdata	6/4/2015 11:03 AM	File folder	
 Readme	6/3/2015 5:06 PM	File folder	
 replica	6/3/2015 5:06 PM	File folder	
 run	6/4/2015 9:09 PM	File folder	
 schema	6/3/2015 5:06 PM	File folder	
 secure	6/3/2015 5:06 PM	File folder	
 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

次の2つのディレクトリに注目してください。

- ClientTools : このディレクトリには、LDAPデータベースを編集するために使用されるバイナリのセットが含まれます。

- Idifdata : これは、LDAPオブジェクトとともにファイルを保存する場所です。

次に示す構造を LDAP データベースに追加してください。



ルート ディレクトリの下に、2 つの組織単位 ( OU ) を設定する必要があります。OU=groups OU には 1 つの子グループを持たせます ( この例では cn=domainusers )。

OU=people OU は、cn=domainusers グループに属する 2 つのユーザ アカウントを定義します。

データベースにデータを取り込むには、最初に Idif ファイルを作成する必要があります。前述の構造は、次のファイルを基に作成されたものです。

```
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
```

LDAPデータベースにオブジェクトを追加するには、ldapmodifyバイナリを使用します。

```
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_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"

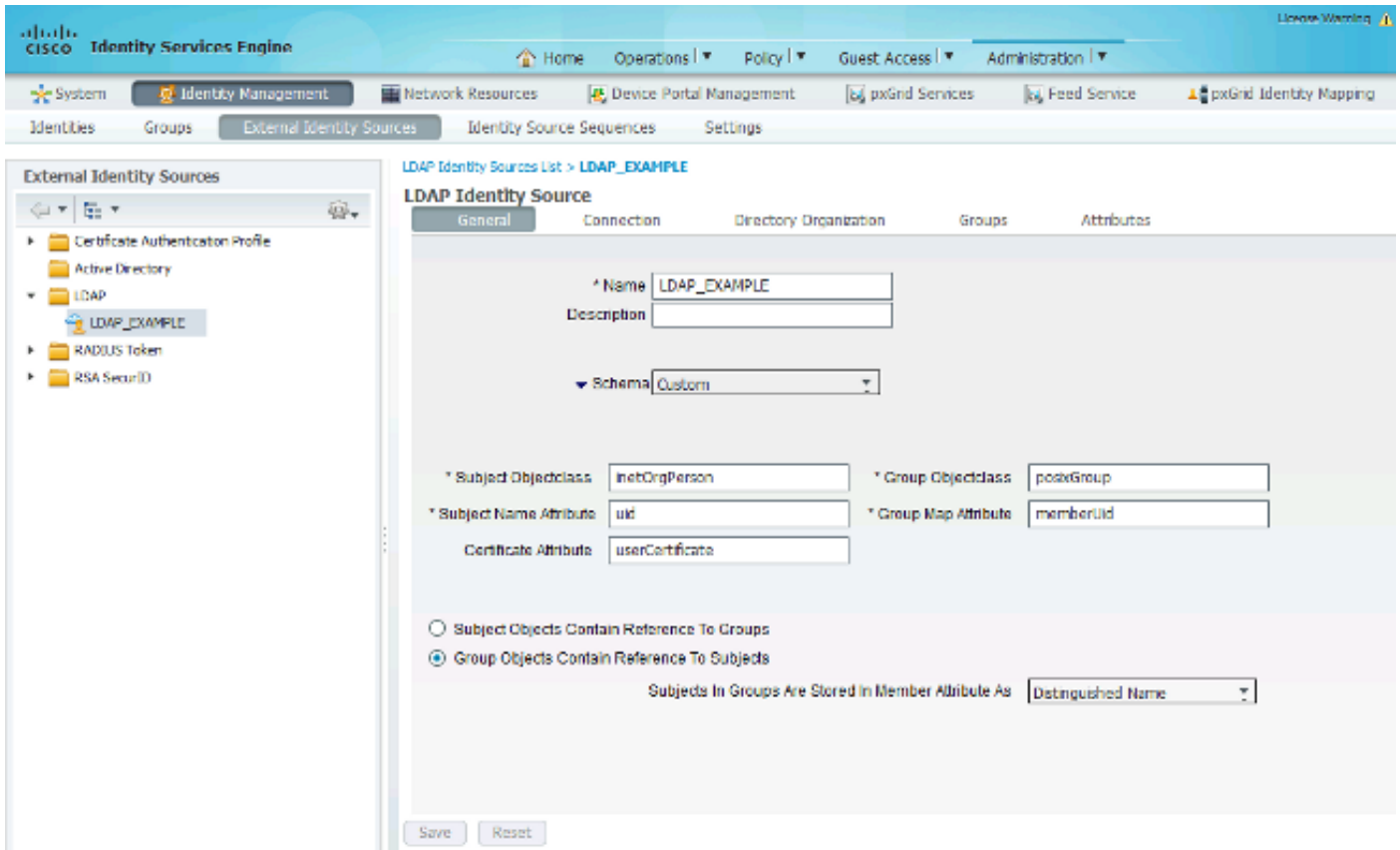
adding new entry "uid=john.doe,ou=people,dc=maxcrc,dc=com"

adding new entry "uid=jan.kowalski,ou=people,dc=maxcrc,dc=com"

adding new entry "cn=domainusers,ou=groups,dc=maxcrc,dc=com"
```

## OpenLDAP と ISE の統合

ISE に LDAP を外部 ID ストアとして設定するには、この項全体を通して記載する図を参考にしてください。

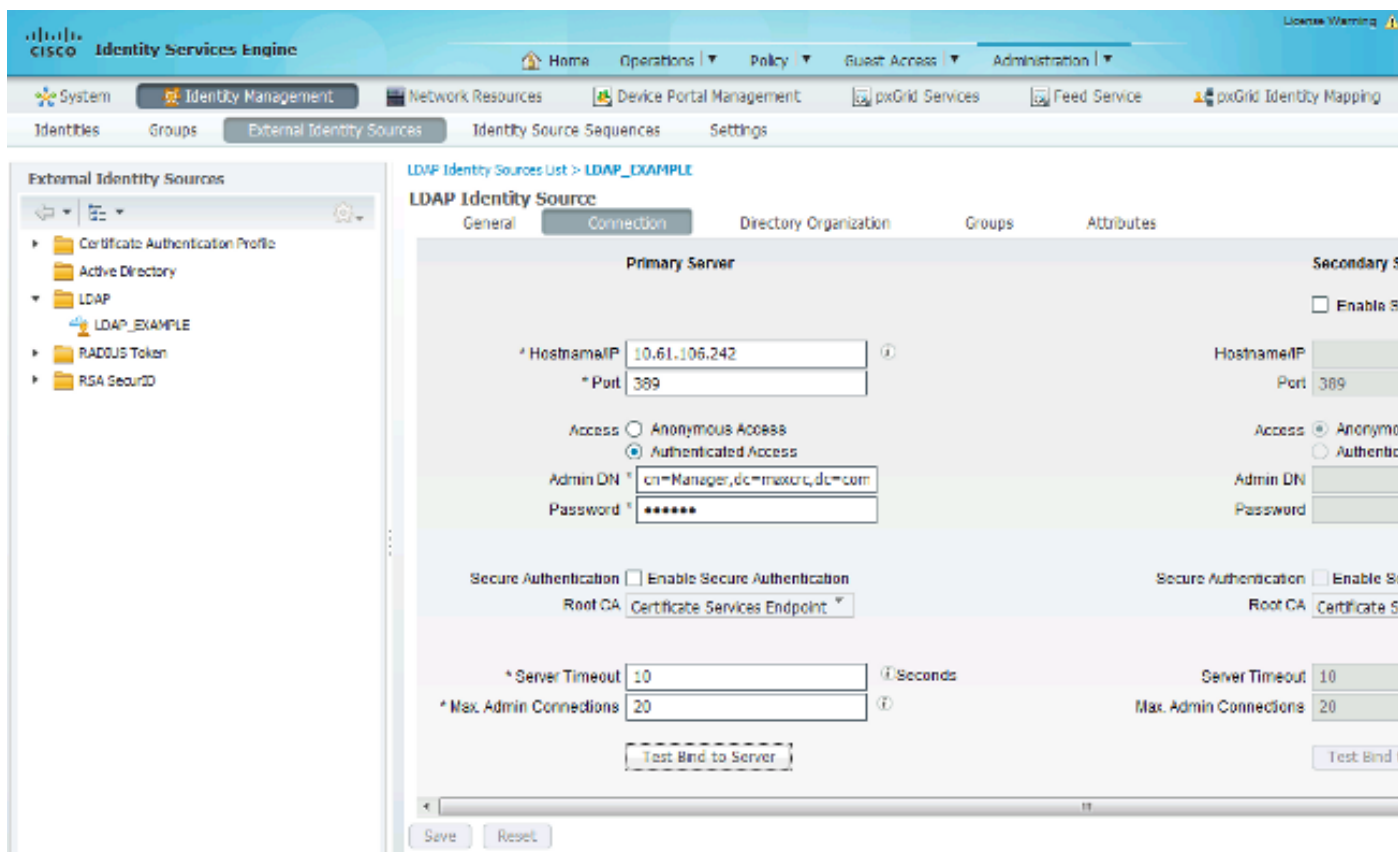


[General] タブで次の属性を設定します。:

- Subject Objectclass : このフィールドは、Idifファイル内のユーザアカウントのオブジェクトクラスに対応します。LDAP設定に従います。次の4つのクラスのいずれかを使用します。
  - Top
  - Person
  - OrganizationalPerson
  - InetOrgPerson
- サブジェクト名属性 : これは、ISEが特定のユーザ名がデータベースに含まれているかどうかを問い合わせたときにLDAPによって取得される属性です。このシナリオでは、エンドポイントのユーザ名としてjohn.doeまたはjan.kowalskiを使用する必要があります。
- Group Objectclass : このフィールドは、Idifファイル内のグループのオブジェクトクラスに対応します。このシナリオでは、cn=domainusers グループのオブジェクト クラスは posixGroup です。
- グループマップ属性 : この属性は、ユーザをグループにマッピングする方法を定義します。Idif ファイル内の cn=domainusers グループの下に、ユーザに対応する 2 つの memberUid 属性があります。

ISE には、事前設定されたスキーマ ( Microsoft Active Directory、Sun、Novell ) も用意されてい

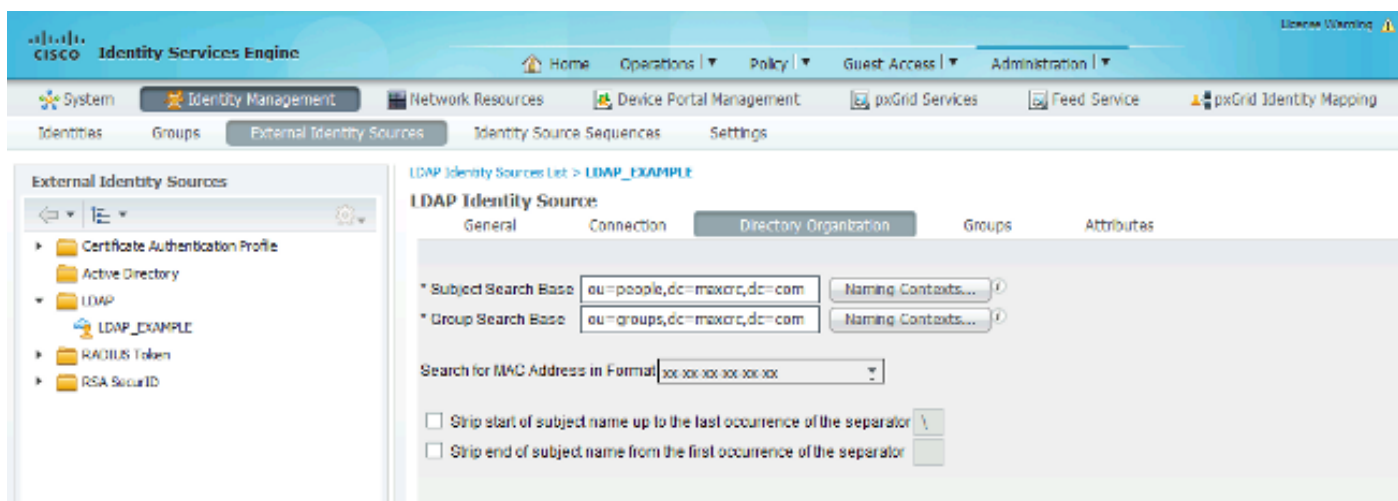
ます。



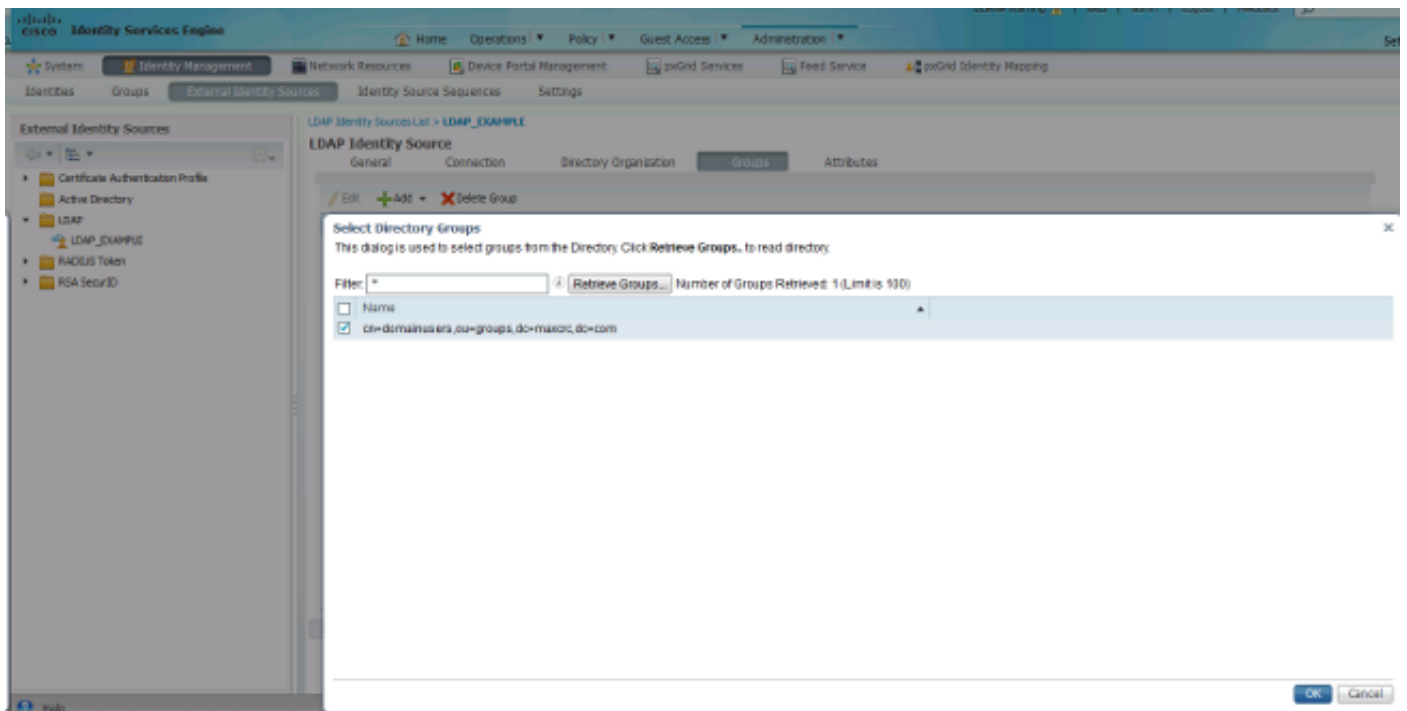
正しい IP アドレスと管理ドメイン設定した後、サーバとのバインディングのテスト を実行できます。この時点では、検索ベースがまだ設定されていないため、サブジェクトまたはグループは取得されません。

次のタブで、件名/グループ検索ベースを設定します。これが、ISE と LDAP の結合ポイントになります。取得できるサブジェクトとグループは、統合ポイントの子となっているものだけです。

このシナリオでは、サブジェクトは OU=people から取得され、グループは OU=groups から取得されます。

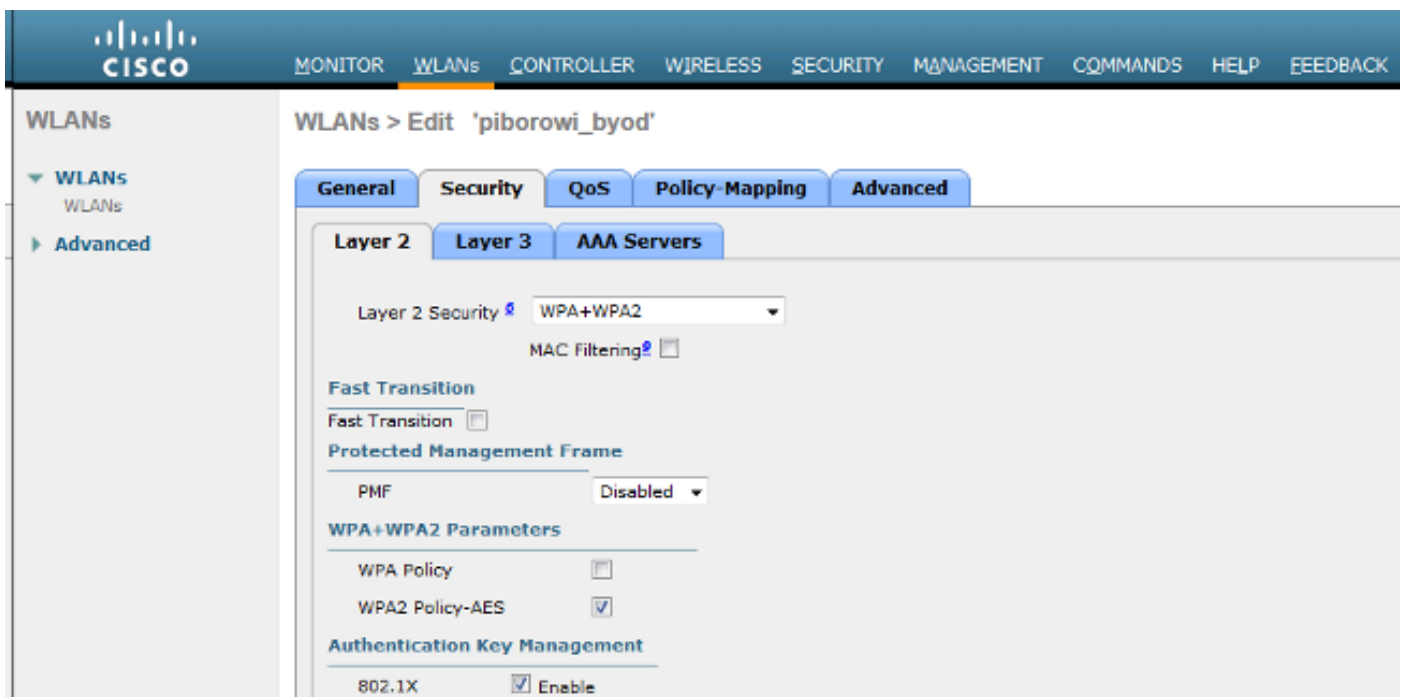


[Groups] タブで、LDAP から ISE にグループをインポートできます。、



## WLC の設定

以下の図を参考に、802.1x 認証に対応するよう WLC を設定してください。





The screenshot shows the Cisco AnyConnect configuration interface for the WLAN 'piborowi\_byod'. The 'Advanced' tab is selected, and the 'AAA Servers' sub-tab is active. The 'Radius Servers' section is visible, with the 'Radius Server Overwrite interface' checkbox disabled. The 'Authentication Servers' and 'Accounting Servers' sections are both enabled. The 'EAP Parameters' section has the 'Enable' checkbox disabled. The configuration table is as follows:

Server	Authentication Servers	Accounting Servers	EAP Parameters
Server 1	IP:10.62.145.51, Port:1812	IP:10.62.145.51, Port:1813	Enable <input type="checkbox"/>
Server 2	None	None	
Server 3	None	None	
Server 4	None	None	
Server 5	None	None	
Server 6	None	None	

This screenshot is identical to the one above, showing the same configuration for the WLAN 'piborowi\_byod' in the 'AAA Servers' section.

## EAP-GTC の設定

EAP-GTC は、LDAP でサポートされる認証方式の 1 つです。Cisco AnyConnect ではこの認証方式を使用できますが、それには Network Access Manager プロファイル エディタをインストールして、プロファイルを正しく設定する必要があります。

Network Access Manager の設定も編集する必要があります ( デフォルト )。この設定は次の場所にあります。

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

以下の図を参考に、エンドポイントに EAP-GTC を設定してください。

The screenshot shows the 'AnyConnect Profile Editor - Network Access Manager' interface. The main window is titled 'Networks' and shows the configuration for a profile named 'eap\_gtc'. The profile path is '...ility Client\Network Access Manager\system\configuration.xml'. The configuration is divided into several sections:

- Name:** eap\_gtc
- Group Membership:** In all groups (Global) is selected. The 'In group' dropdown is set to 'Local networks'.
- Choose Your Network Media:** 'Wi-Fi (wireless) Network' is selected. The 'Wired (802.3) Network' option is also visible with instructions: 'Select a wired network if the endstations will be connecting to the network with a traditional ethernet cable.' The 'Wi-Fi (wireless) Network' option has instructions: 'Select a WiFi network if the endstations will be connecting to the network via a wireless radio connection to an Access Point.' The SSID (max 32 chars) is 'pborowi\_byod'. There are checkboxes for 'Hidden Network' and 'Corporate Network', both of which are unchecked. The Association Timeout is set to 5 seconds.
- Common Settings:** A field for 'Script or application on each user's machine to run when connected.' is empty, with a 'Browse Local Machine' button next to it. The Connection Timeout is set to 40 seconds.

At the bottom of the window, there are 'Next' and 'Cancel' buttons. On the right side, there is a vertical list of tabs: 'Media Type', 'Security Level', 'Connection Type', 'User Auth', and 'Credentials'.

- Network Access Manager
  - Client Policy
  - Authentication Policy
  - Networks**
  - Network Groups

## Networks

Profile: ...ility Client\Network Access Manager\system\configuration.xml

### Security Level

- 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.)	<input type="text" value="30"/>	startPeriod (sec.)	<input type="text" value="30"/>
heldPeriod (sec.)	<input type="text" value="60"/>	maxStart	<input type="text" value="3"/>

### Association Mode

- Media Type
- Security Level
- Connection Type
- User Auth
- Credentials

Next

Cancel

- Network Access Manager
  - Client Policy
  - Authentication Policy
  - Networks**
  - Network Groups

## Networks

Profile: ...ility Client\Network Access Manager\system\configuration.xml

### Network Connection Type

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.

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.

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

- Network Access Manager
- Client Policy
- Authentication Policy
- Networks
- Network Groups

### Networks

Profile: ...ility Client\Network Access Manager\system\configuration.xml

EAP Methods

EAP-TLS  PEAP

EAP-TTLS  EAP-FAST

LEAP

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

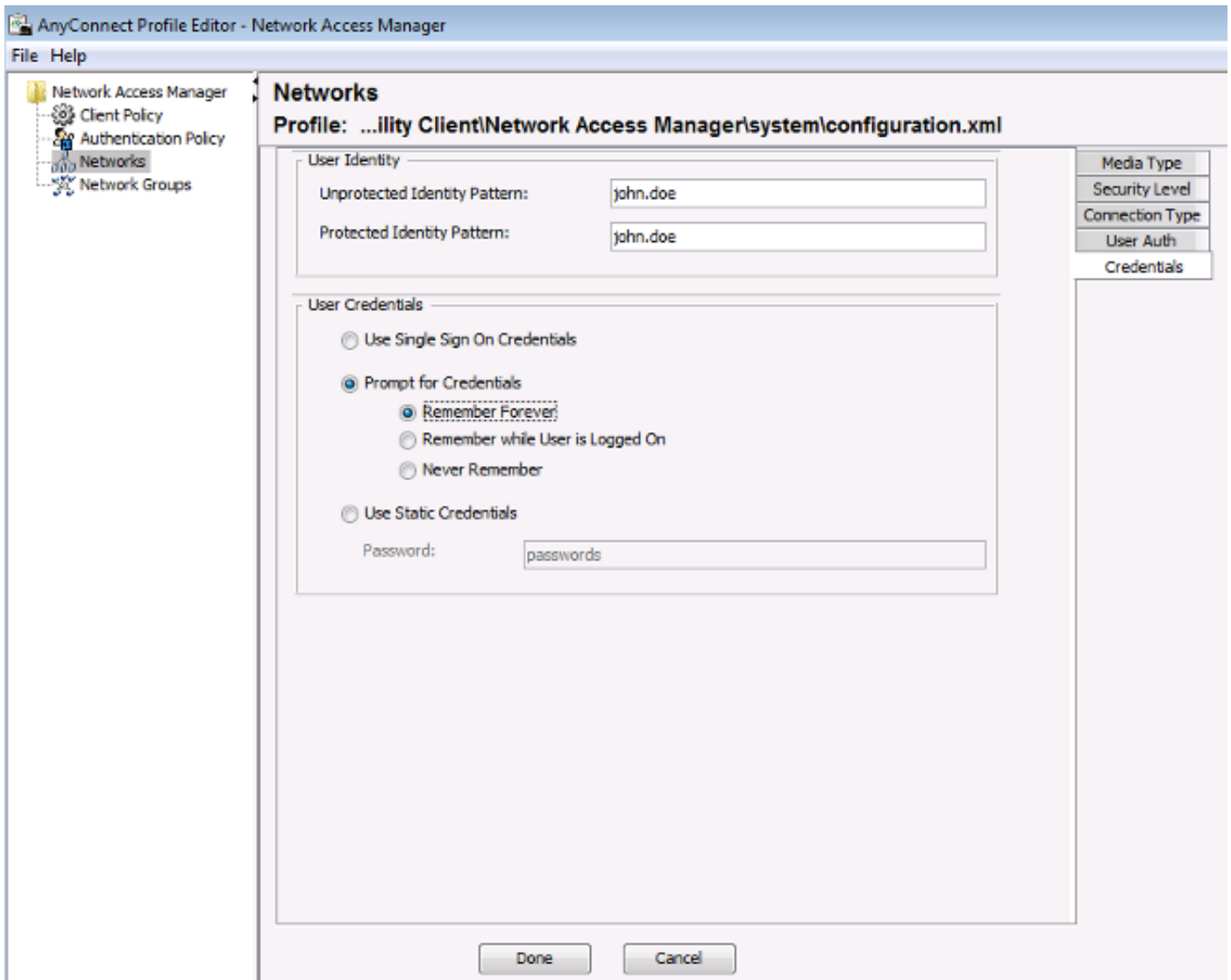
EAP-TLS, using a Certificate

Authenticate using a Token and EAP-GTC

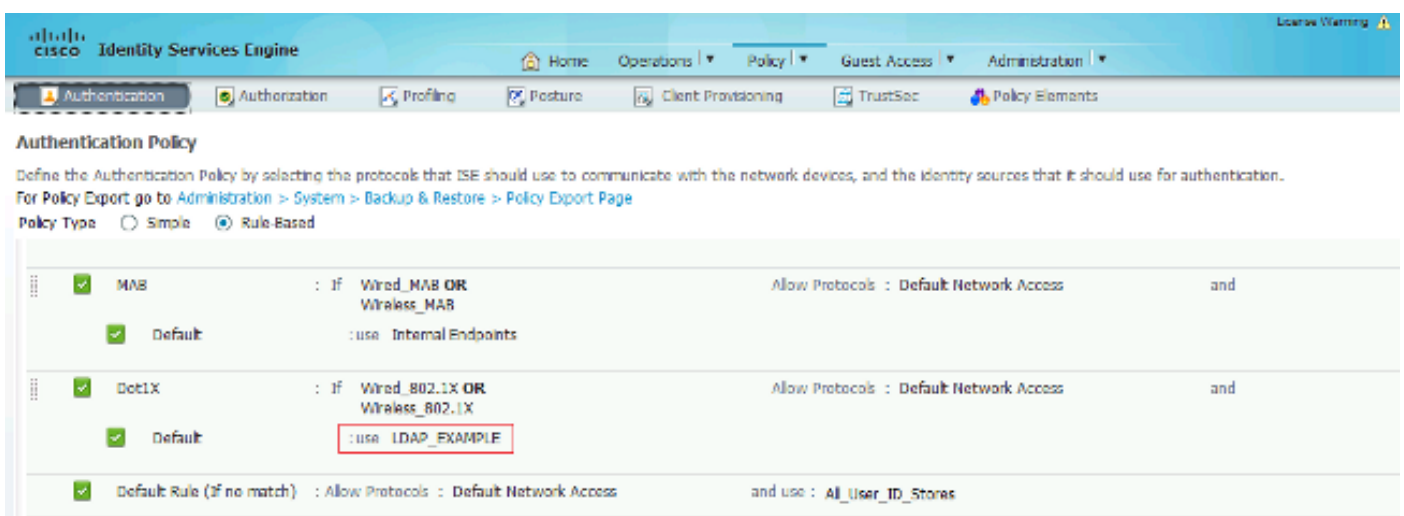
- Media Type
- Security Level
- Connection Type
- User Auth
- Credentials

Next

Cancel



以下の図を参考に、ISE の認証および承認ポリシーを変更してください。



**CISCO Identity Services Engine**

Home | Operations | **Policy** | Guest Access | Administration

Authentication | **Authorization** | Profiling | Posture | Client Provisioning | TrustSec | Policy Elements

### Authorization Policy

Define the Authorization Policy by configuring rules based on identity groups and/or other conditions. Drag and drop rules to change the order.  
 For Policy Export go to Administration > System > Backup & Restore > Policy Export Page

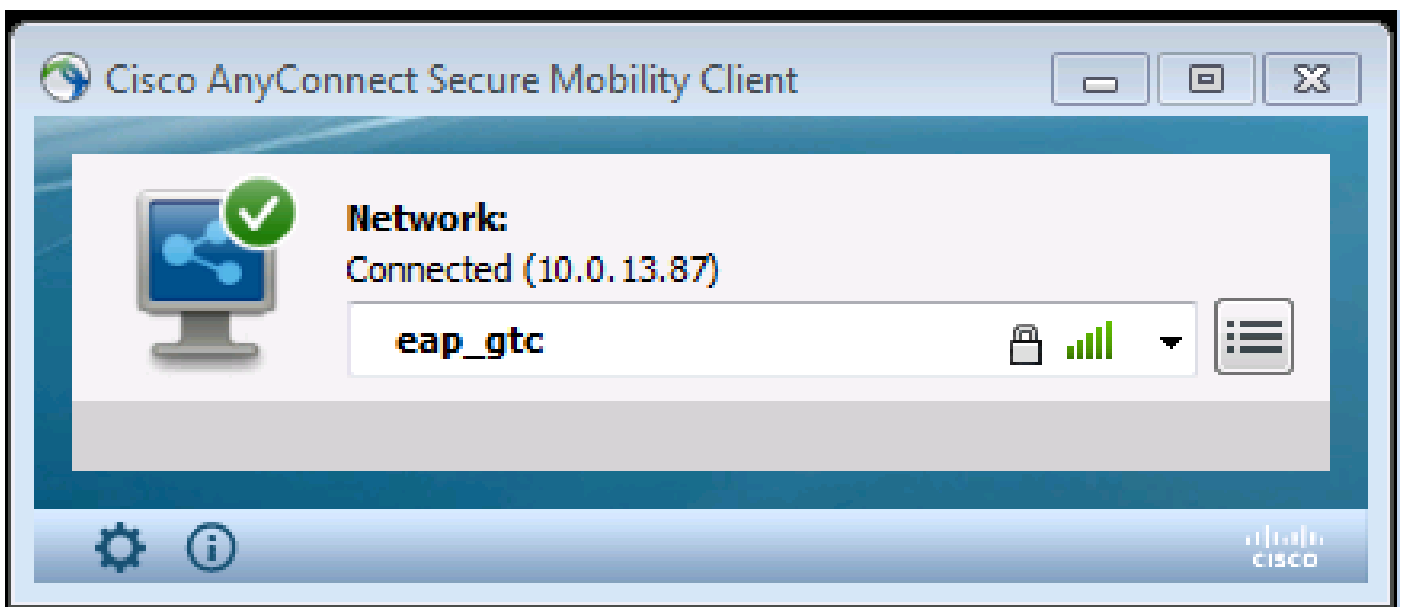
First Matched Rule Applies

Exceptions (0)

Standard

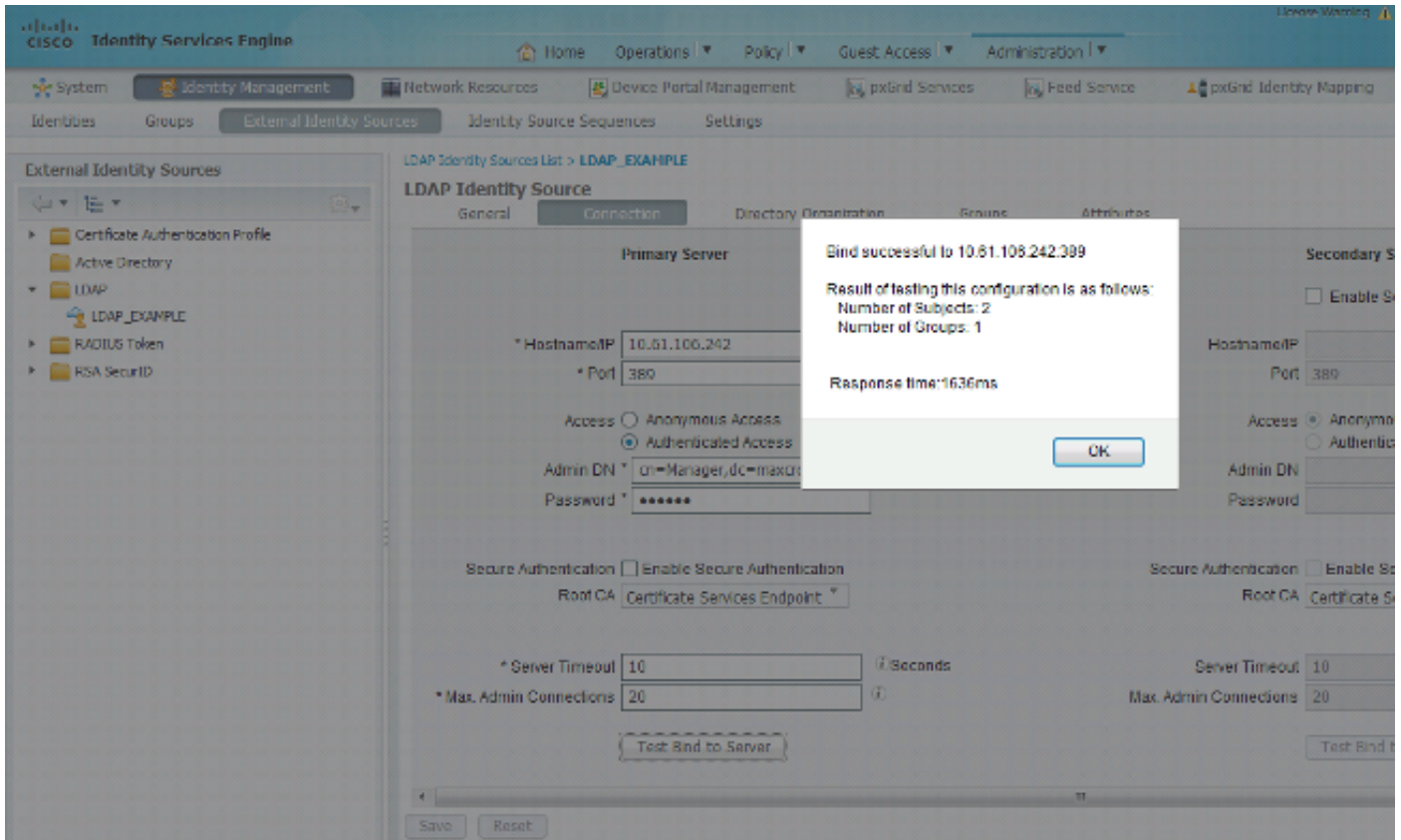
Status	Rule Name	Conditions (Identity groups and other conditions)	Permissions
✓	Users in LDAP store	if (Wireless_802.1X AND LDAP_EXAMPLE:ExternalGroups EQUALS cn=domainusers,ou=groups,dc=maxxc,dc=com )	then PermitAccess
✓	Wireless Black List Default	if Blacklist AND Wireless_Access	then Blackhole_Wireless_Access
✓	Profiled Cisco IP Phones	if Cisco-IP-Phone	then Cisco_IP_Phones
✓	Profiled Non Cisco IP Phones	if Non_Cisco_Profiled_Phones	then Non_Cisco_IP_Phones
✓	Basic_Authenticated_Access	if Network_Access_Authentication_Passed	then PermitAccess
✓	Default	if no matches, then	DenyAccess

以上の設定を適用すると、ネットワークに接続できるようになっているはずです。

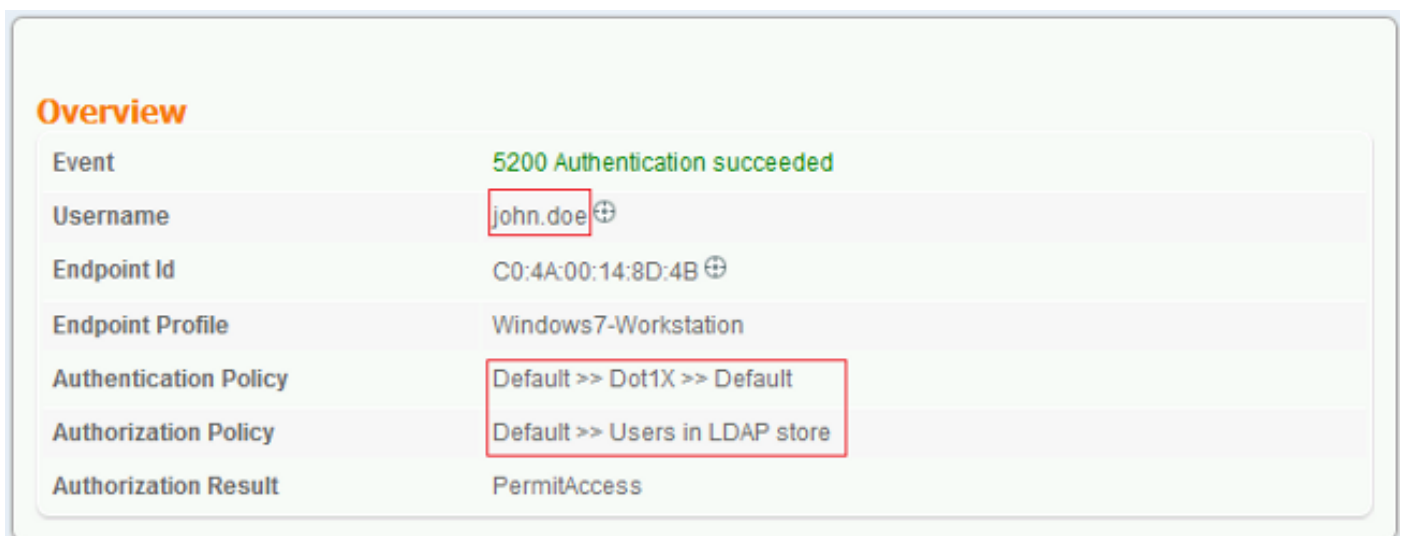
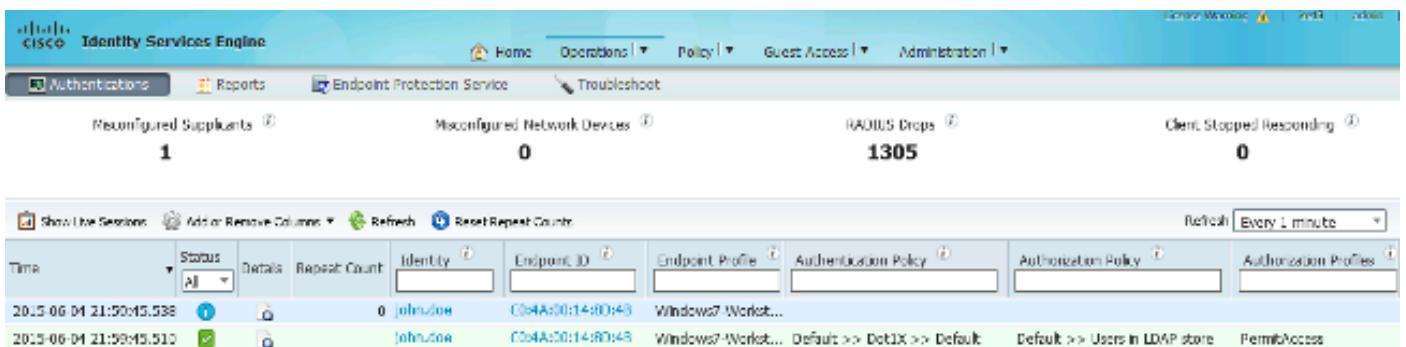


## 確認

LDAPとISEの設定を確認するには、サーバへのテスト接続を使用してサブジェクトとグループを取得します。



以下の図に、ISE からのレポート例を示します。





## 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

## トラブルシューティング

ここでは、この設定で発生する一般的なエラーと、そのトラブルシューティング方法を説明します。

- OpenLDAPのインストール後に、gssapi.dllがないことを示すエラーが発生した場合は、Microsoft Windowsを再起動します。
- Cisco AnyConnect の configuration.xml ファイルを直接編集できない場合があります。新しい構成を別の場所に保存してから、そのファイルで古いファイルを置き換えてください。
- 認証レポートに、次のエラーメッセージが表示されます。

```
<#root>
```

```
Authentication method is not supported by any applicable identity store
```

このエラーメッセージは、選択した認証方式がLDAPでサポートされないことを意味します。

同じレポート内に、認証プロトコルとしてサポートされている方式 ( EAP-GTC、EAP-TLS、PEAP-TLS ) のいずれかが示されていることを確認してください。


- 認証レポートで、サブジェクトがIDストアで見つからなかった場合、レポートからのユーザ名が、LDAPデータベース内のどのユーザのサブジェクト名属性とも一致しません。

このシナリオでは、この属性の値がuidに設定されているため、ISEは一致を見つけようとするときに、LDAPユーザのuid値を調べます。

- サーバへのバインドテスト中にサブジェクトとグループが正しく取得されなかった場合、検索ベースの設定が正しくありません。

LDAP階層は、リーフからルートの方角およびdc ( 複数の単語で構成可能 ) で指定する必要があることに注意してください。

---

 ヒント:WLC側でEAP認証のトラブルシューティングを行うには、シスコのドキュメント『[WLANコントローラ\(WLC\)でのEAP認証の設定例](#)』を参照してください。

---

## 翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。