

Configurar o ISE para integração com um servidor LDAP

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Configurar](#)

[Diagrama de Rede](#)

[Configurar OpenLDAP](#)

[Integrar o OpenLDAP com o ISE](#)

[Configurar o WLC](#)

[Configurar EAP-GTC](#)

[Verificar](#)

[Troubleshooting](#)

Introdução

Este documento descreve como configurar um Cisco Identity Services Engine (ISE) para integração com um servidor LDAP da Cisco.

Pré-requisitos

Requisitos


Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações deste documento são baseadas nestas versões de software e hardware:

- Cisco ISE versão 1.3 com patch 2
- Microsoft Windows versão 7 x64 com OpenLDAP instalado
- Cisco Wireless LAN Controller (WLC) versão 8.0.100.0
- Cisco AnyConnect versão 3.1 para Microsoft Windows

- Editor de perfis do Cisco Network Access Manager

 Observação: este documento é válido para configurações que usam LDAP como a origem de identidade externa para a autenticação e autorização do ISE.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

Estes métodos de autenticação são suportados com LDAP:

- Protocolo de autenticação extensível - placa de token genérica (EAP-GTC)
- Protocolo de autenticação extensível - Transport Layer Security (EAP-TLS)
- Protocolo de autenticação extensível protegido - Transport Layer Security (PEAP-TLS)

Configurar

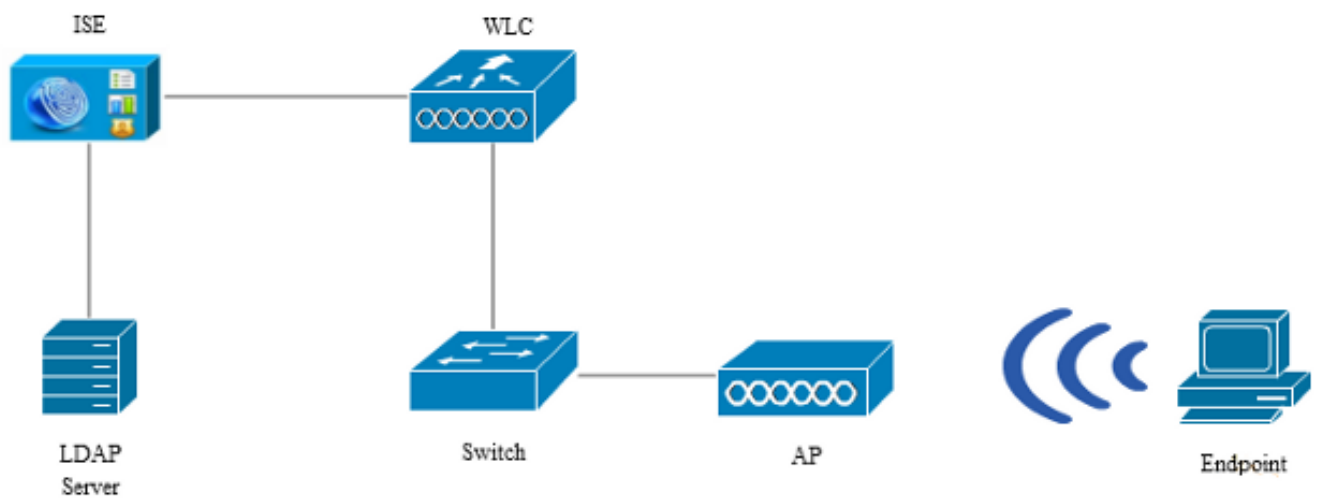
Esta seção descreve como configurar os dispositivos de rede e integrar o ISE com um servidor LDAP.

Diagrama de Rede

Neste exemplo de configuração, o endpoint usa um adaptador sem fio para associar-se à rede sem fio.





























A Wireless LAN (WLAN) na WLC está configurada para autenticar os usuários através do ISE. No ISE, o LDAP é configurado como um armazenamento de identidade externo.

Esta imagem ilustra a topologia de rede que é usada:



Configurar OpenLDAP

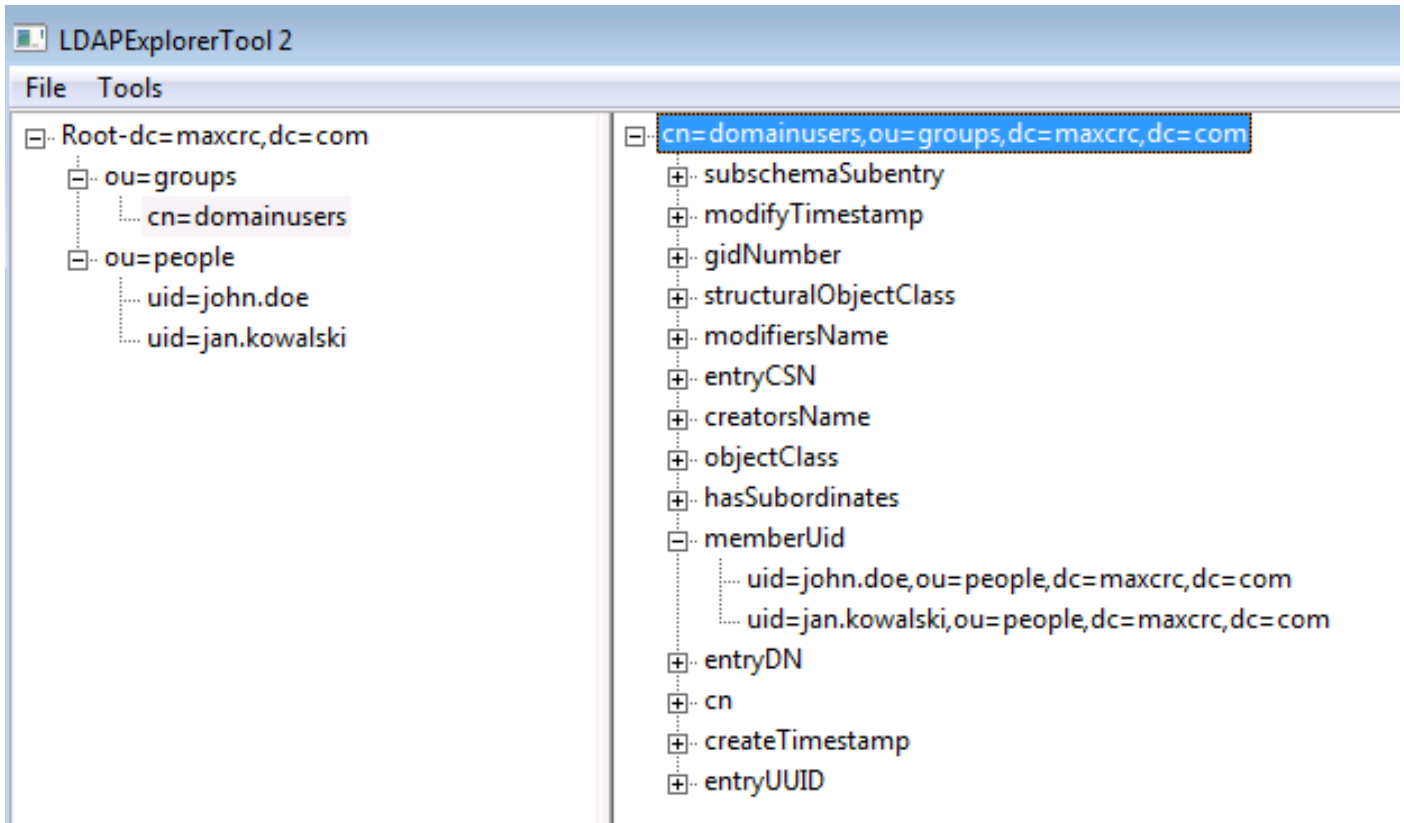
A instalação do OpenLDAP para Microsoft Windows é concluída via GUI e é simples. O local padrão é C: > OpenLDAP. Após a instalação, você deverá ver este diretório:

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

Tome nota de dois diretórios em particular:

- ClientTools - Este diretório inclui um conjunto de binários usados para editar o banco de dados LDAP.
- Idifdata - Este é o local no qual você deve armazenar os arquivos com objetos LDAP.

Adicione esta estrutura ao banco de dados LDAP:



No diretório Root, você deve configurar duas OUs (Organizational Units, unidades organizacionais). A OU OU=groups deve ter um grupo filho (cn=domainusers neste exemplo).

A OU OU=people define as duas contas de usuário que pertencem ao grupo cn=domainusers.

Para preencher o banco de dados, você deve criar o arquivo ldif primeiro. A estrutura mencionada anteriormente foi criada a partir deste arquivo:

```
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
```

Para adicionar os objetos ao banco de dados LDAP, use o binário ldapmodify:

```
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"

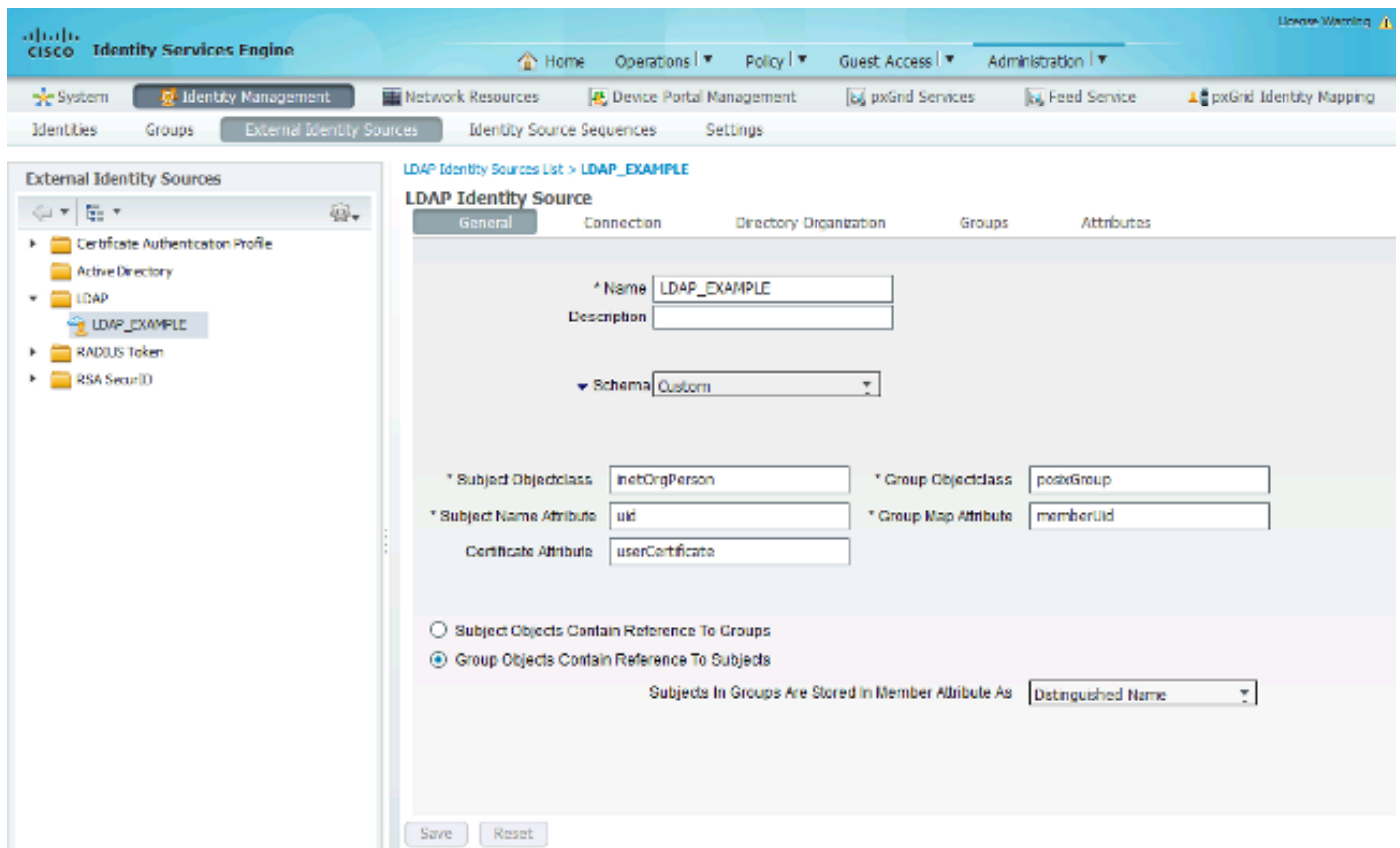
adding new entry "uid=john.doe,ou=people,dc=maxcrc,dc=com"

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

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

Integrar o OpenLDAP com o ISE

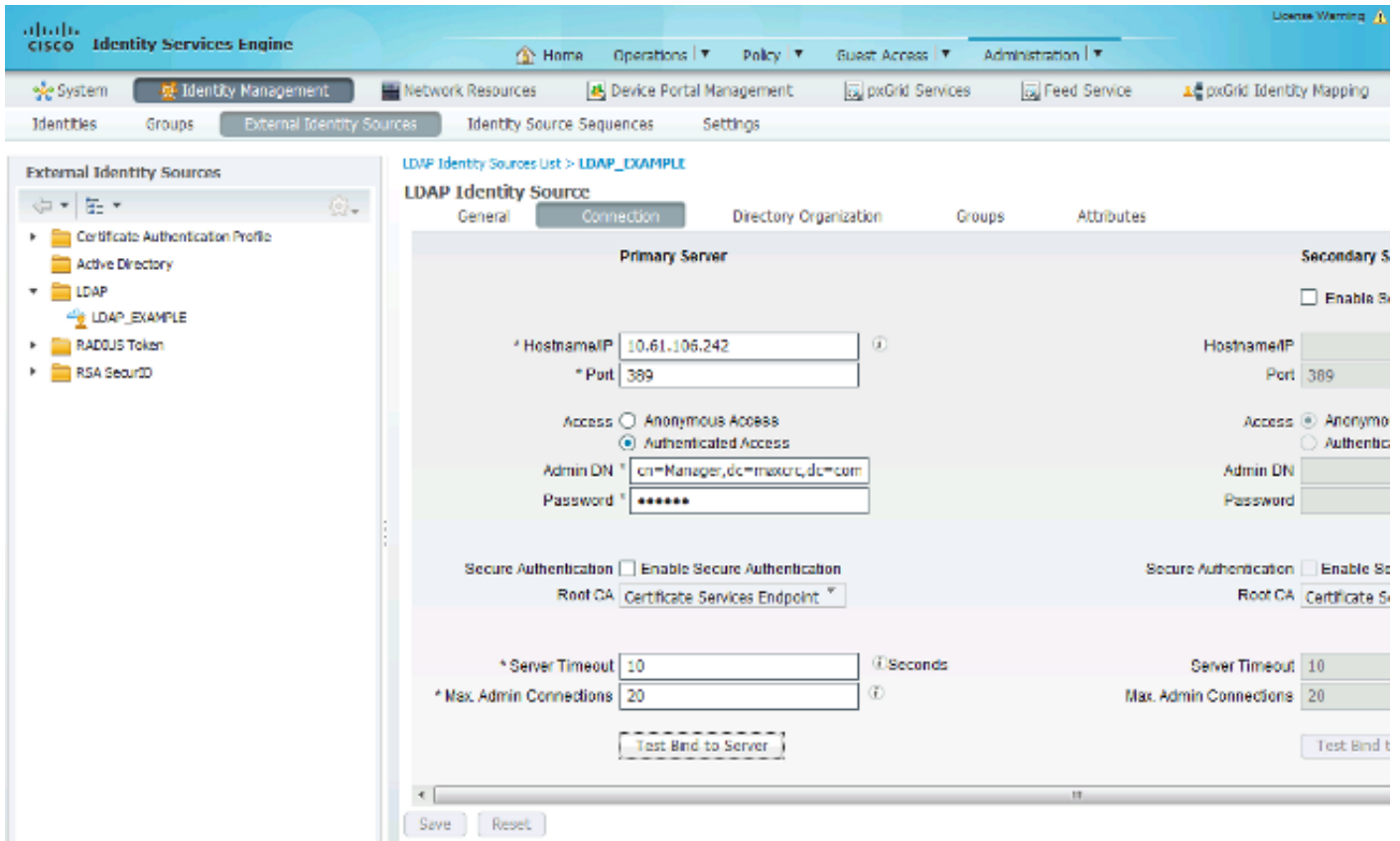
Use as informações fornecidas nas imagens ao longo desta seção para configurar o LDAP como um armazenamento de identidade externo no ISE.



Você pode configurar esses atributos na guia Geral:

- Subject Objectclass - Este campo corresponde à classe de objeto das contas de usuário no arquivo ldif. De acordo com a configuração LDAP, use uma destas quatro classes:
 - Superior
 - Pessoa
 - PessoaOrganizacional
 - InetOrgPerson
- Atributo do nome do assunto - Este é o atributo recuperado pelo LDAP quando o ISE consulta se um nome de usuário específico está incluído em um banco de dados. Neste cenário, você deve usar john.doe ou jan.kowalski como o nome de usuário no ponto final.
- Group Objectclass - Este campo corresponde à classe de objeto de um grupo no arquivo ldif. Neste cenário, a classe de objeto para o grupo cn=domainusers é posixGroup.
- Atributo de mapa de grupo - Este atributo define como os usuários são mapeados para os grupos. No grupo cn=domainusers no arquivo ldif, você pode ver dois atributos memberUid que correspondem aos usuários.

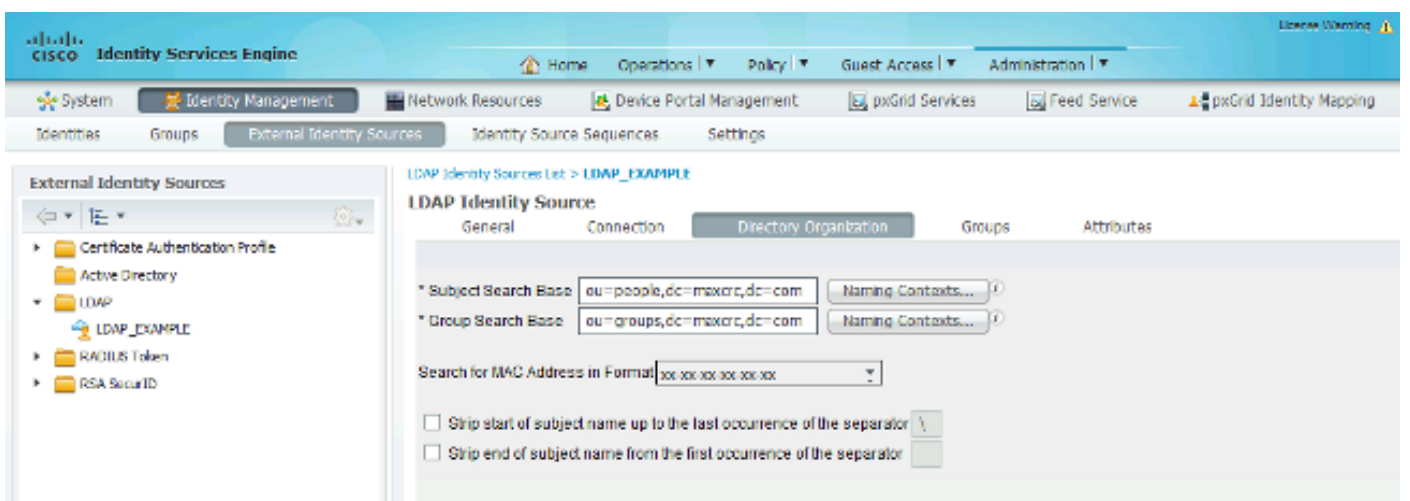
O ISE também oferece alguns esquemas pré-configurados (Microsoft Active Directory, Sun, Novell):



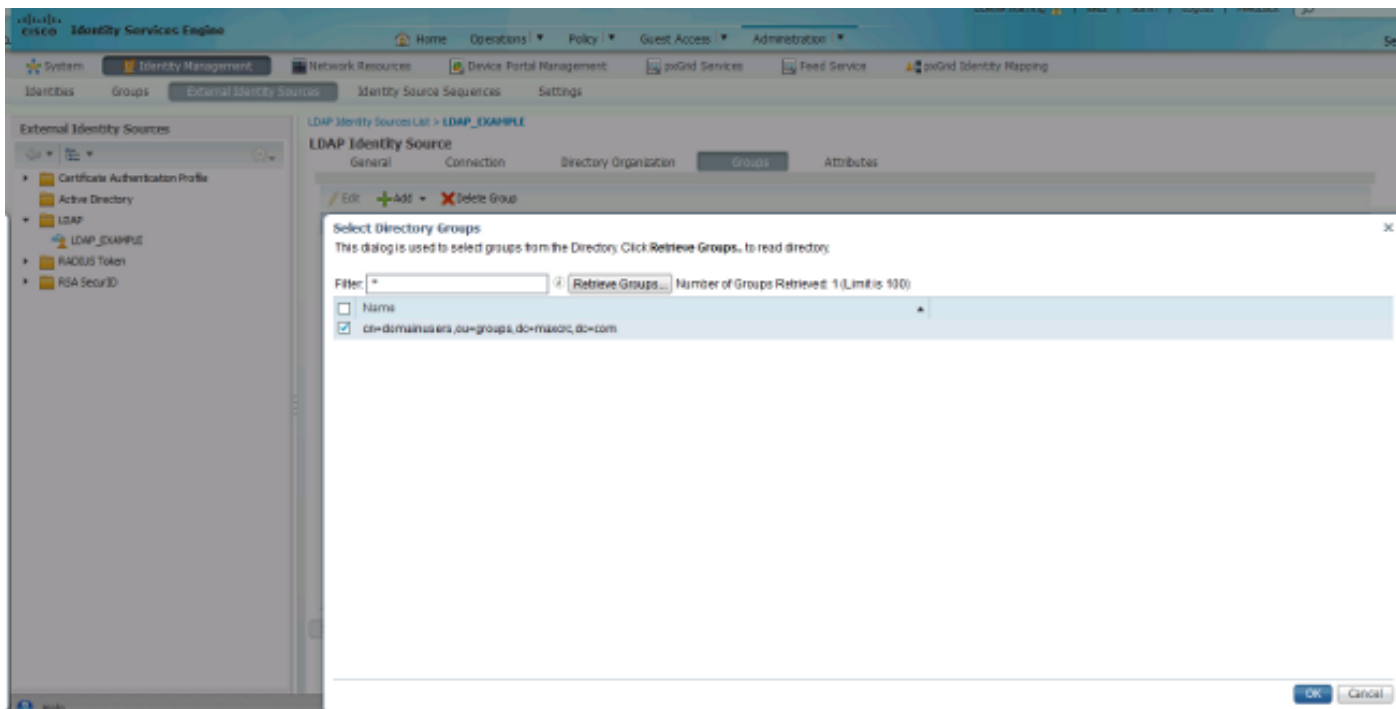
Depois de definir o endereço IP e o nome de domínio administrativo corretos, você pode Testar associação ao servidor. Neste ponto, você não recupera nenhum assunto ou grupo porque as bases de pesquisa ainda não estão configuradas.

Na próxima guia, configure a Base de pesquisa de assunto/grupo. Este é o ponto de junção do ISE para o LDAP. Você pode recuperar apenas assuntos e grupos que sejam filhos do seu ponto de junção.

Neste cenário, os assuntos de OU=people e os grupos de OU=groups são recuperados:

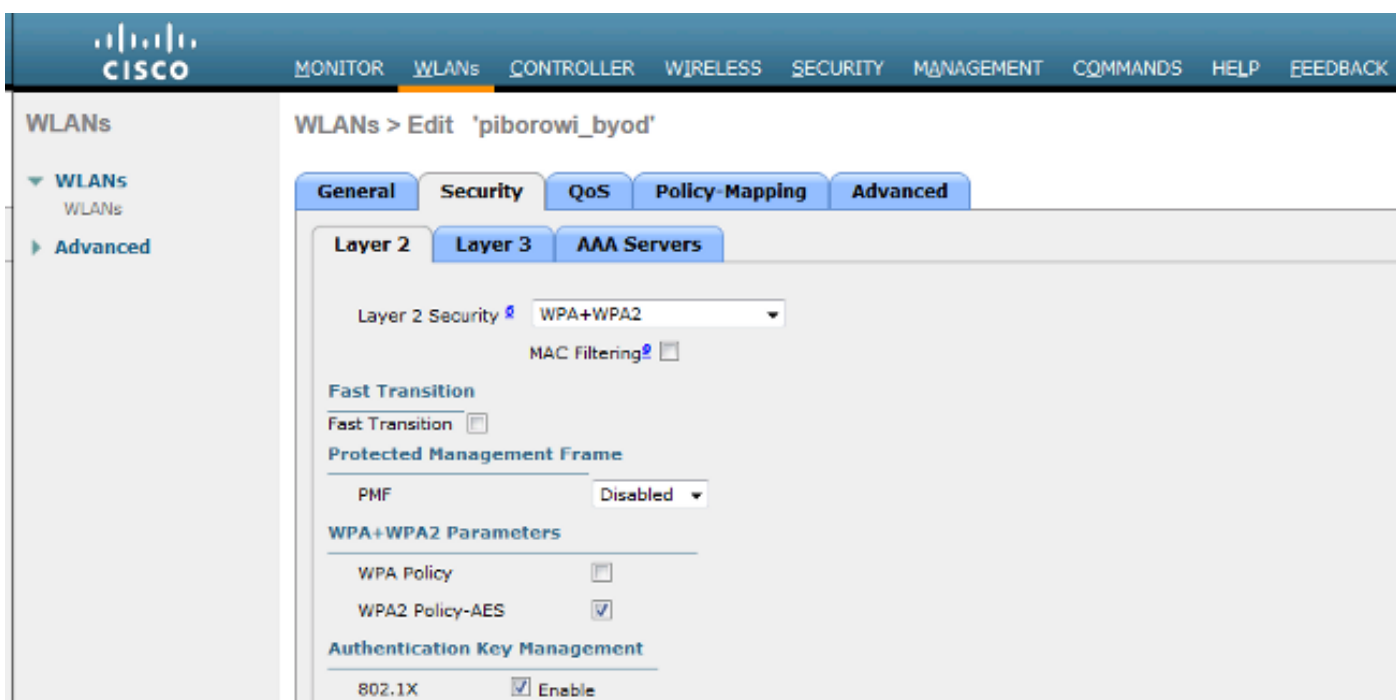


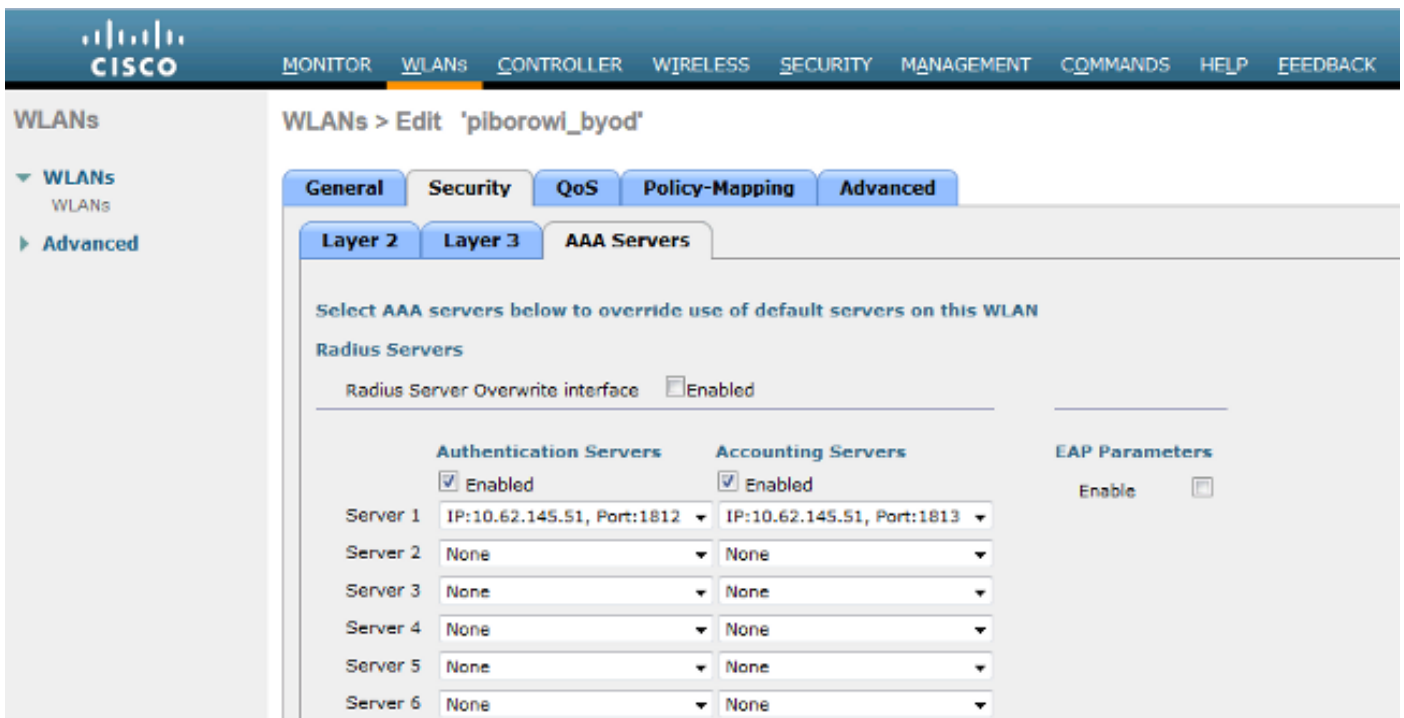
Na guia Groups, você pode importar os grupos do LDAP no ISE:



Configurar o WLC

Use as informações fornecidas nestas imagens para configurar a WLC para a autenticação 802.1x:





Configurar EAP-GTC

Um dos métodos de autenticação suportados para LDAP é EAP-GTC. Ele está disponível no Cisco AnyConnect, mas você deve instalar o Editor de perfis do gerenciador de acesso à rede para configurar o perfil corretamente.

Você também deve editar a configuração do Network Access Manager, que (por padrão) está localizada aqui:

C: > ProgramData > Cisco > Cisco AnyConnect Secure Mobility Client > Network Access Manager > sistema > arquivo configuration.xml

Use as informações fornecidas nessas imagens para configurar o EAP-GTC no endpoint:

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 '...ility Client\Network Access Manager\system\configuration.xml'. The configuration is divided into several sections:

- Name:** eap_gtc
- Group Membership:** Radio buttons for 'In group:' (set to 'Local networks') and 'In all groups (Global)'. The 'In all groups (Global)' option is selected.
- Choose Your Network Media:** Radio buttons for 'Wired (802.3) Network' and 'Wi-Fi (wireless) Network'. The 'Wi-Fi (wireless) Network' option is selected. Below this, there is a text box for 'SSID (max 32 chars):' containing 'pborowi_byod', and checkboxes for 'Hidden Network' and 'Corporate Network', both of which are unchecked. An 'Association Timeout' of '5 seconds' is also specified.
- Common Settings:** A section for 'Script or application on each user's machine to run when connected.' with an empty text box and a 'Browse Local Machine' button. Below this, a 'Connection Timeout' of '40 seconds' is set.

On the right side of the window, there is a vertical list of tabs: 'Media Type', 'Security Level', 'Connection Type', 'User Auth', and 'Credentials'. The 'Media Type' tab is currently selected.

At the bottom of the window, there are 'Next' and 'Cancel' buttons.

- 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.

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

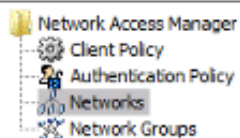
802.1X Settings

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

Next

Cancel



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

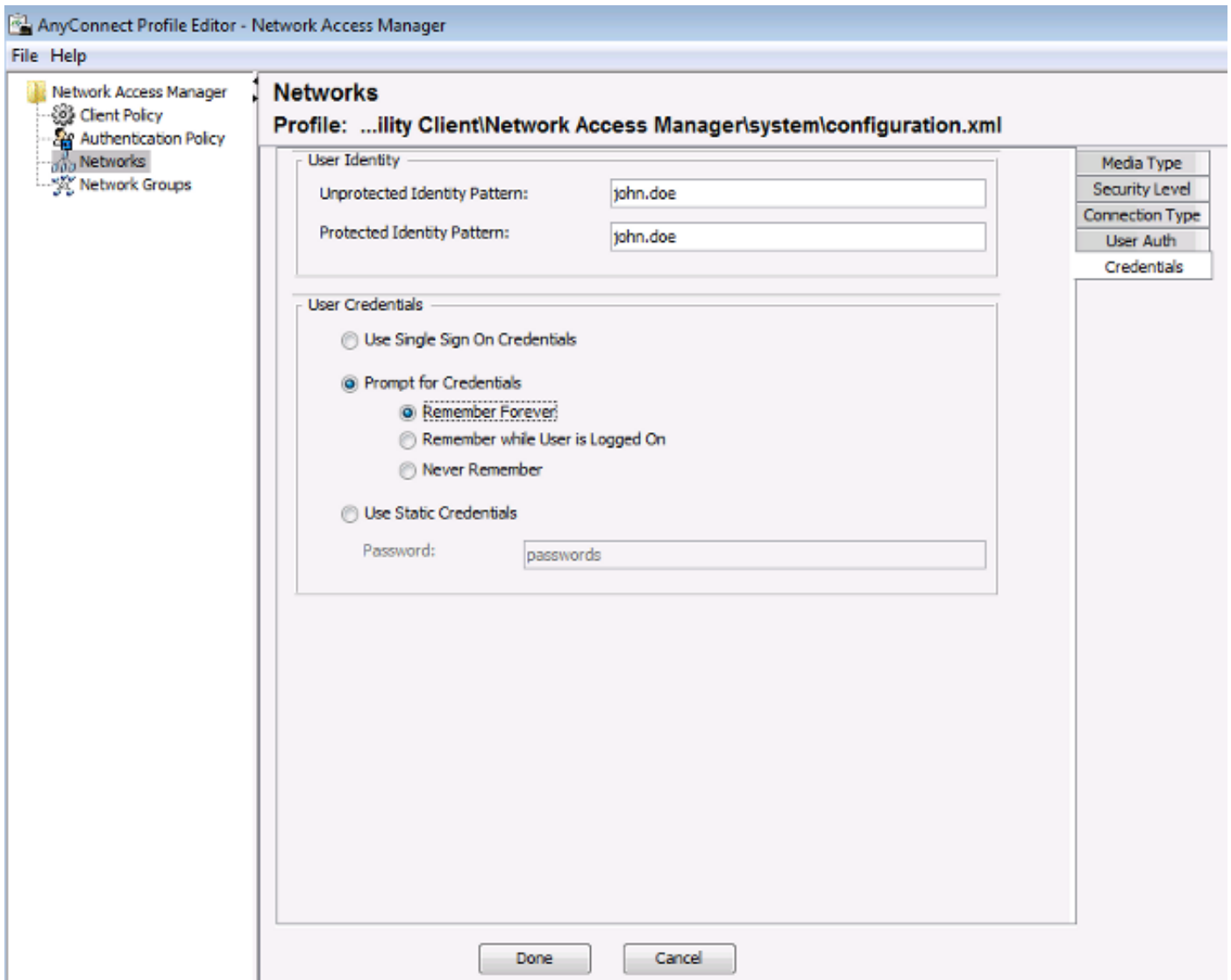
EAP-TLS, using a Certificate

Authenticate using a Token and EAP-GTC

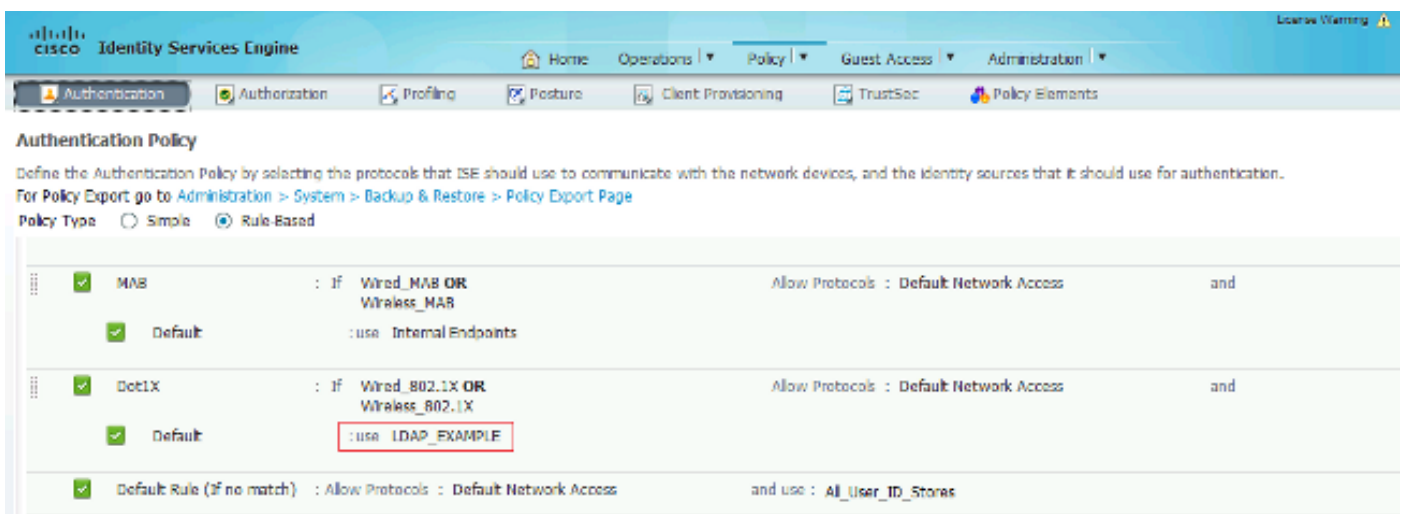
- Media Type
- Security Level
- Connection Type
- User Auth
- Credentials

Next

Cancel



Use as informações fornecidas nessas imagens para alterar as políticas de autenticação e autorização no ISE:



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

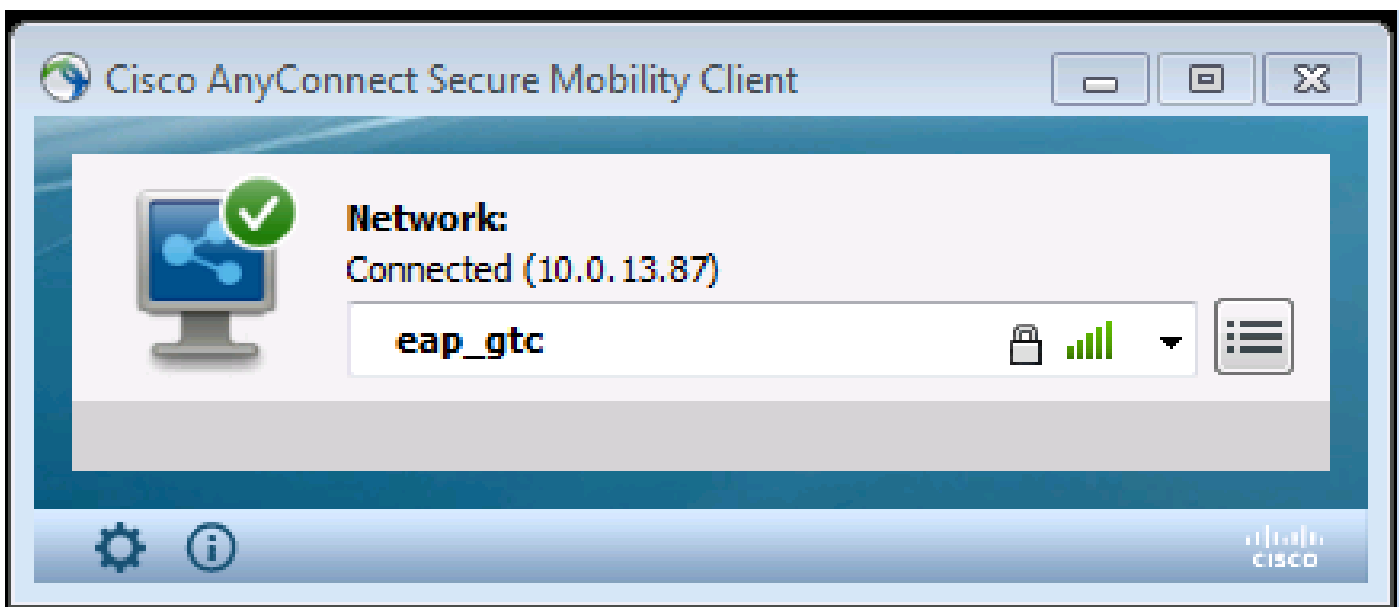
First Matched Rule Applies

Exceptions (0)

Standard

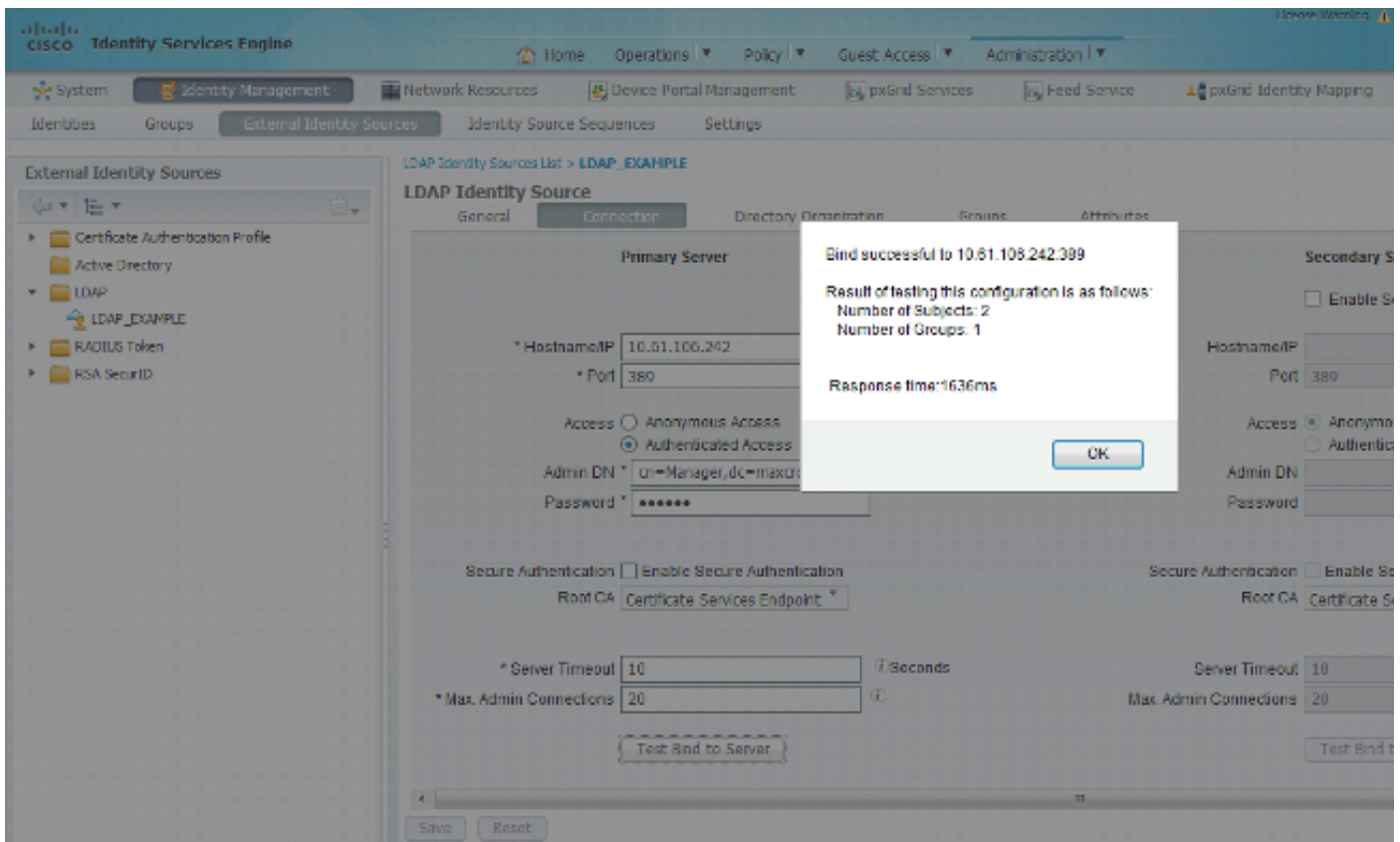
Status	Rule Name	Conditions (Identity groups and other conditions)	Permissions
✓	Users in LDAP store	if (Wireless_802.1X AND LDAP_EXAMPLE:ExternalGroups EQUALS cn=domainusers,ou=groups,dc=mxcorp,dc=com)	then PermitAccess
✓	Wireless Black List Default	if Blacklist AND Wireless_Access	then Blackhole_Wireless_Access
✓	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

Depois de aplicar a configuração, você poderá se conectar à rede:

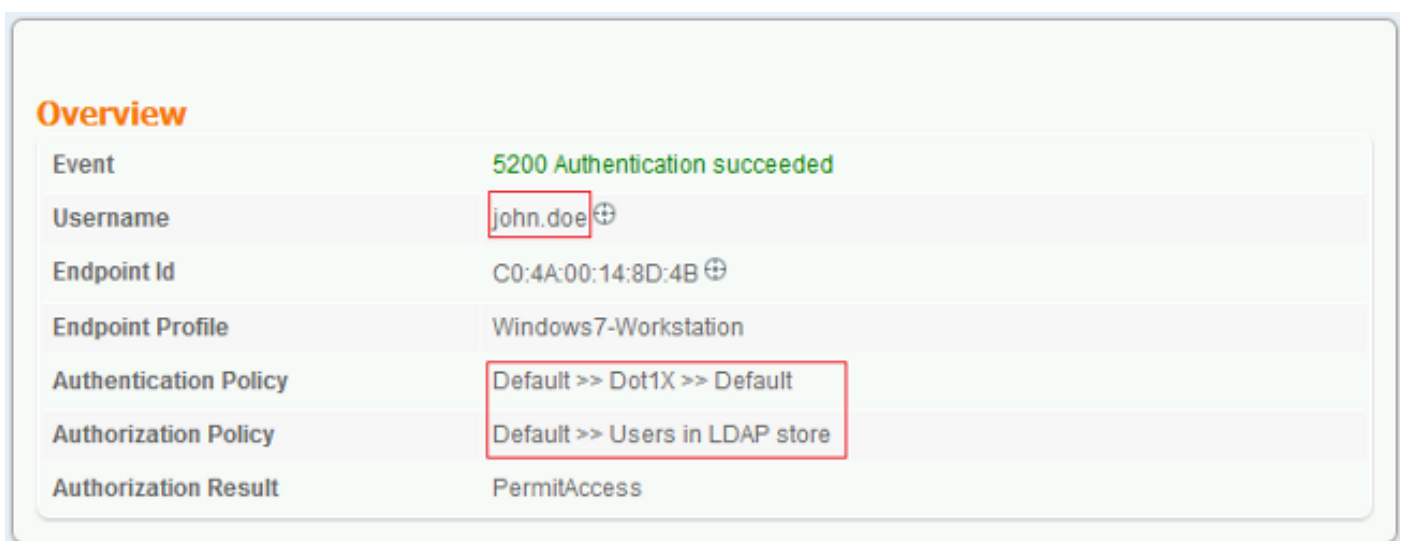
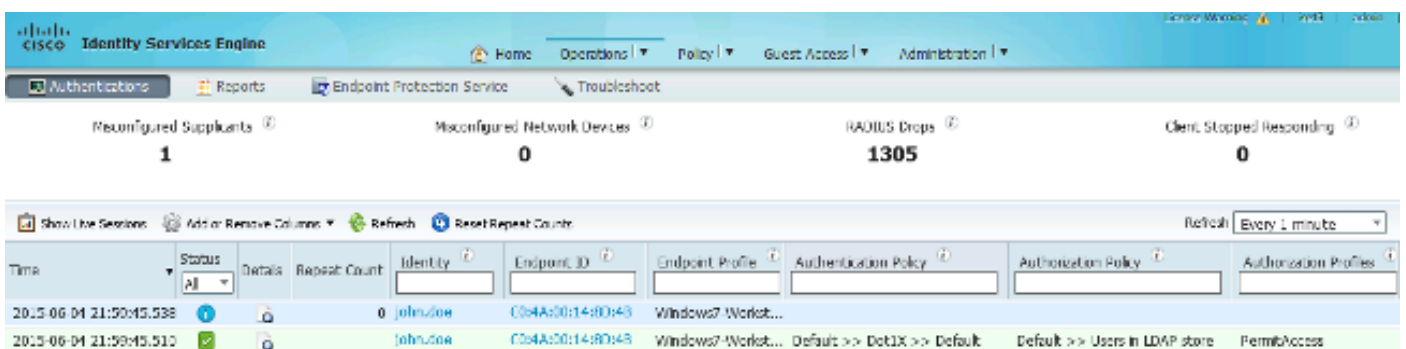


Verificar

Para verificar as configurações LDAP e ISE, recupere os assuntos e grupos com uma conexão de teste ao servidor:



Essas imagens ilustram um relatório de exemplo do ISE:



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

Troubleshooting

Esta seção descreve alguns erros comuns encontrados com esta configuração e como solucioná-los:

- Após a instalação do OpenLDAP, se você encontrar um erro para indicar que um gssapi.dll está ausente, reinicie o Microsoft Windows.
- Talvez não seja possível editar o arquivo configuration.xml diretamente para o Cisco AnyConnect. Salve a nova configuração em outro local e use-a para substituir o arquivo antigo.
- No relatório de autenticação, há esta mensagem de erro:

```
<#root>
```

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

Esta mensagem de erro indica que o método selecionado não é suportado pelo LDAP.

Verifique se o protocolo de autenticação no mesmo relatório mostra um dos métodos suportados (EAP-GTC, EAP-TLS ou PEAP-TLS).

- No relatório de autenticação, se você observar que o assunto não foi encontrado no armazenamento de identidades, o nome de usuário do relatório não corresponde ao atributo de nome de assunto para qualquer usuário no banco de dados LDAP.

Nesse cenário, o valor foi definido como uid para esse atributo, o que significa que o ISE procura os valores uid para o usuário LDAP quando ele tenta encontrar uma correspondência.

- Se os assuntos e grupos não forem recuperados corretamente durante um teste vincular ao servidor, é uma configuração incorreta para as bases de pesquisa.

Lembre-se de que a hierarquia LDAP deve ser especificada de folha para raiz e dc (pode consistir em várias palavras).



Dica: para solucionar problemas de autenticação EAP no lado da WLC, consulte o documento [Exemplo de Configuração de Autenticação EAP com Controladoras WLAN \(WLC\)](#) da Cisco.

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.