

Configuración de ISE para la integración con un servidor LDAP

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Configurar](#)

[Diagrama de la red](#)

[Configurar OpenLDAP](#)

[Integre OpenLDAP con ISE](#)

[Configurar la WLC](#)

[Configuración de EAP-GTC](#)

[Verificación](#)

[Troubleshoot](#)

Introducción

Este documento describe cómo configurar Cisco Identity Services Engine (ISE) para la integración con un servidor LDAP de Cisco.

Prerequisites

Requirements


No hay requisitos específicos para este documento.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware:

- Cisco ISE versión 1.3 con parche 2
- Microsoft Windows versión 7 x64 con OpenLDAP instalado
- Cisco Wireless LAN Controller (WLC) versión 8.0.100.0
- Cisco AnyConnect versión 3.1 para Microsoft Windows

- Editor de perfiles de Cisco Network Access Manager

 Nota: este documento es válido para las configuraciones que utilizan LDAP como origen de identidad externo para la autenticación y autorización de ISE.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

Estos métodos de autenticación son compatibles con LDAP:

- Protocolo de autenticación extensible - Tarjeta de testigo genérica (EAP-GTC)
- Protocolo de autenticación extensible - Seguridad de la capa de transporte (EAP-TLS)
- Protocolo de autenticación extensible protegido - Seguridad de la capa de transporte (PEAP-TLS)

Configurar

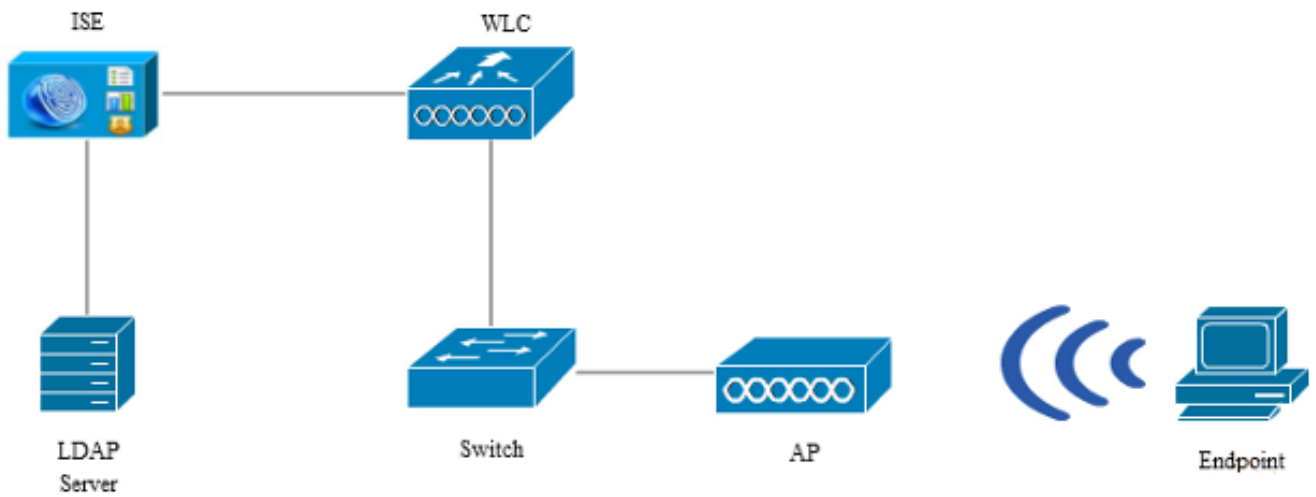
En esta sección se describe cómo configurar los dispositivos de red e integrar ISE con un servidor LDAP.

Diagrama de la red

En este ejemplo de configuración, el terminal utiliza un adaptador inalámbrico para asociarse con la red inalámbrica.





























La LAN inalámbrica (WLAN) en el WLC se configura para autenticar a los usuarios a través de ISE. En ISE, LDAP se configura como un almacén de identidades externo.

Esta imagen ilustra la topología de red que se utiliza:



Configurar OpenLDAP

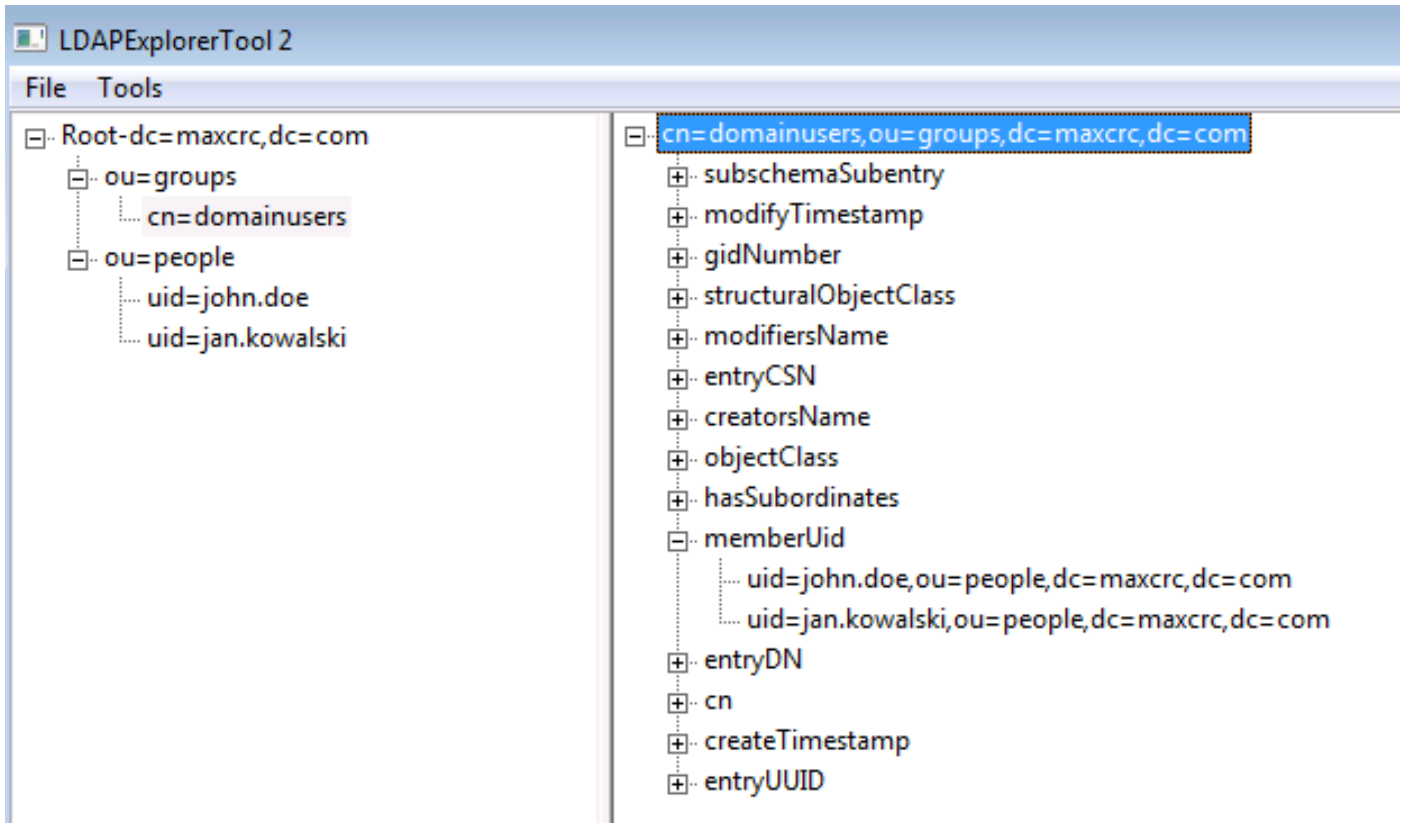
La instalación de OpenLDAP para Microsoft Windows se realiza a través de la GUI y es muy sencilla. La ubicación predeterminada es C: > OpenLDAP. Después de la instalación, debería ver este directorio:

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 dos directorios en particular:

- ClientTools - Este directorio incluye un conjunto de binarios que se utilizan para editar la base de datos LDAP.
- Idifdata - Esta es la ubicación en la que debe almacenar los archivos con objetos LDAP.

Agregue esta estructura a la base de datos LDAP:



En el directorio Root, debe configurar dos unidades organizativas (OU). La unidad organizativa OU=groups debe tener un grupo secundario (cn=domainusers en este ejemplo).

La unidad organizativa OU=people define las dos cuentas de usuario que pertenecen al grupo cn=domainusers.

Para rellenar la base de datos, primero debe crear el archivo ldif. La estructura mencionada anteriormente se creó a partir de este archivo:

```
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 agregar los objetos a la base de datos LDAP, utilice el binario `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"

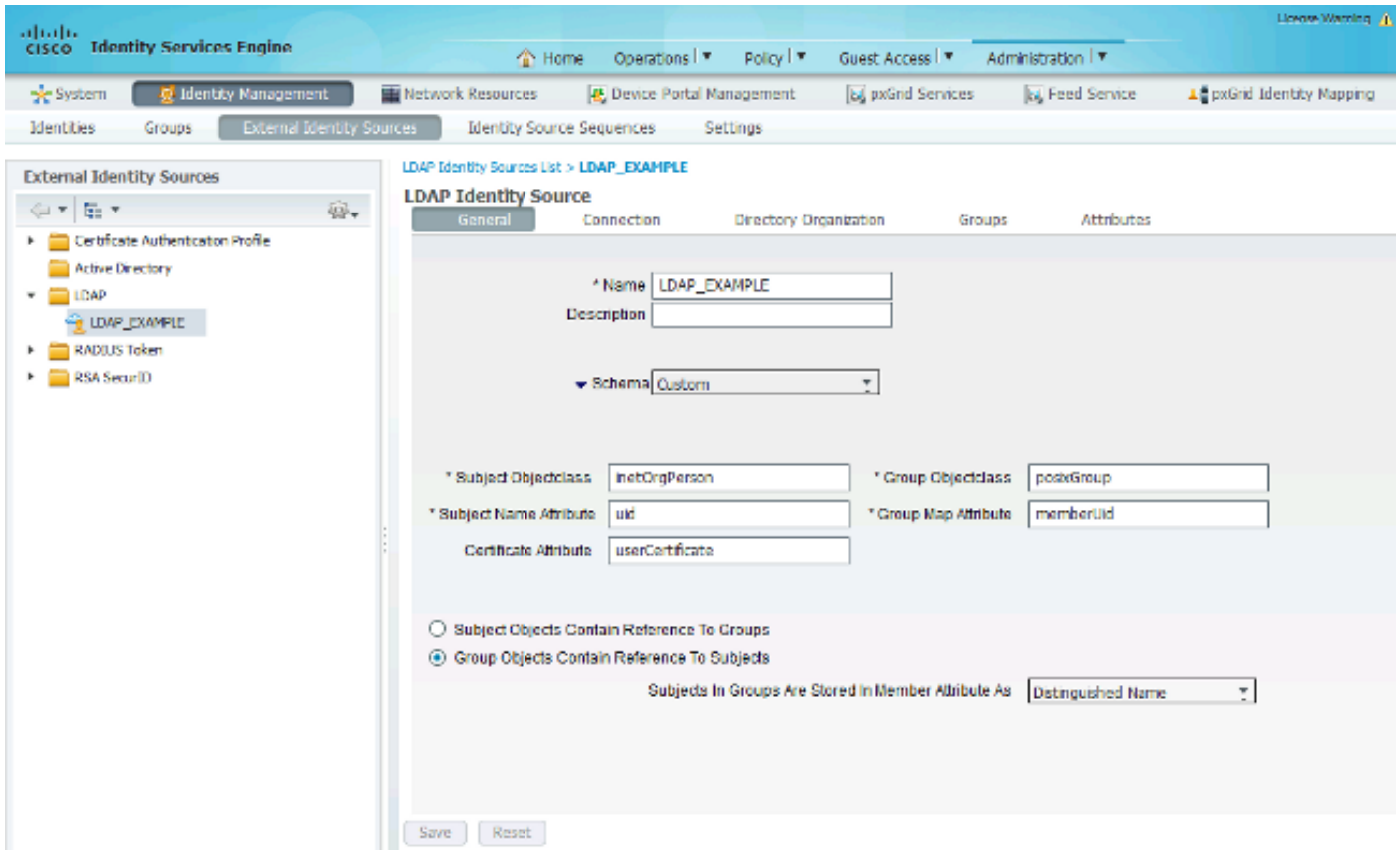
adding new entry "uid=john.doe,ou=people,dc=maxcrc,dc=com"

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

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

Integre OpenLDAP con ISE

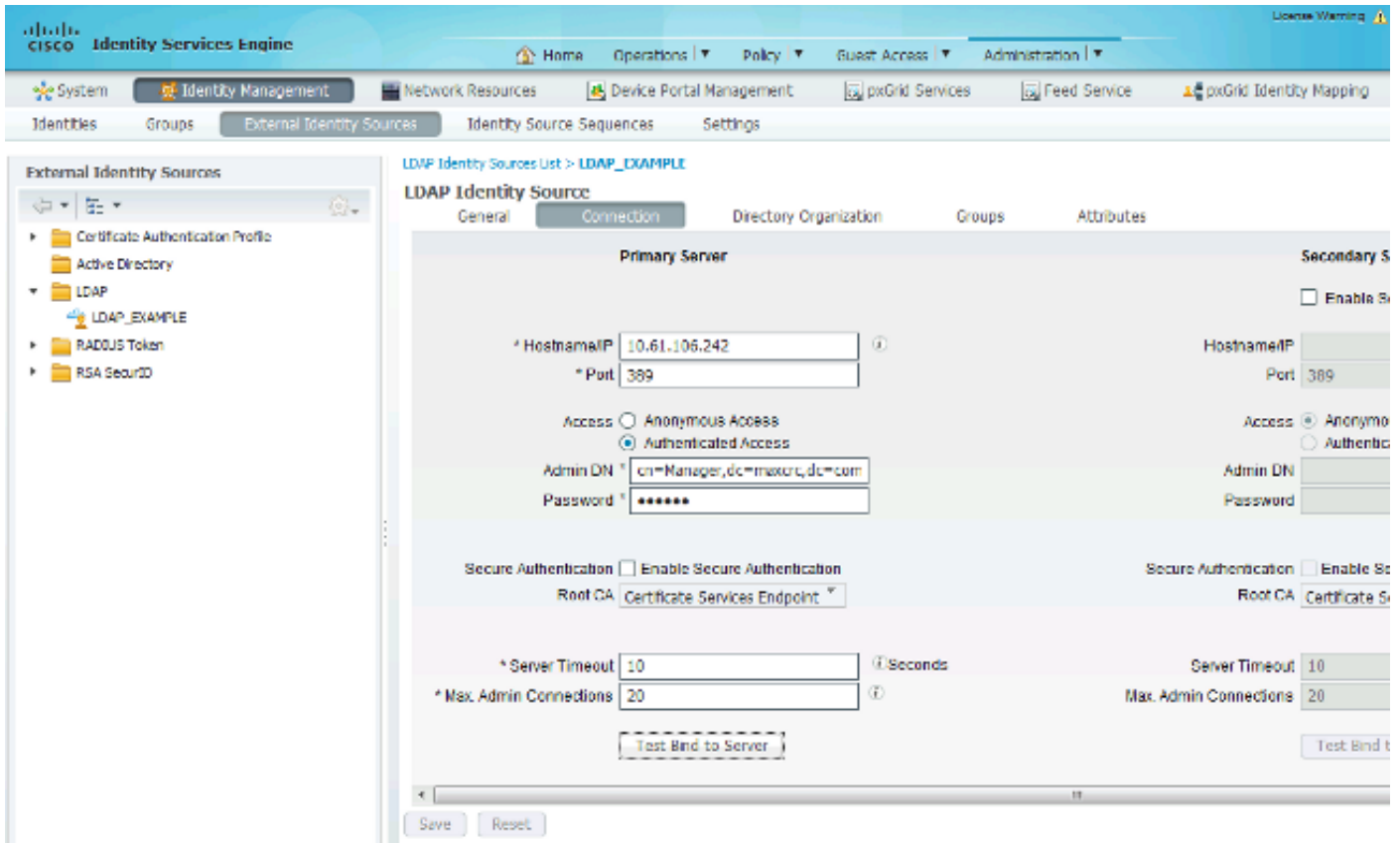
Utilice la información que se proporciona en las imágenes de esta sección para configurar LDAP como un almacén de identidades externo en ISE.



Puede configurar estos atributos desde la pestaña General:

- Subject Objectclass: este campo corresponde a la clase de objeto de las cuentas de usuario del archivo Idif. Según la configuración de LDAP, use una de estas cuatro clases:
 - Arriba
 - Persona
 - PersonaOrganizativa
 - InetOrgPerson
- Atributo de nombre de sujeto: atributo que recupera LDAP cuando ISE pregunta si un nombre de usuario específico está incluido en una base de datos. En este escenario, debe utilizar john.doe o jan.kowalski como el nombre de usuario en el terminal.
- Group Objectclass - Este campo corresponde a la clase de objeto para un grupo en el archivo Idif. En este escenario, la clase de objeto para el grupo cn=domainusers es posixGroup.
- Atributo de asignación de grupo: este atributo define cómo se asignan los usuarios a los grupos. En el grupo cn=domainusers del archivo Idif, puede ver dos atributos memberUid que corresponden a los usuarios.

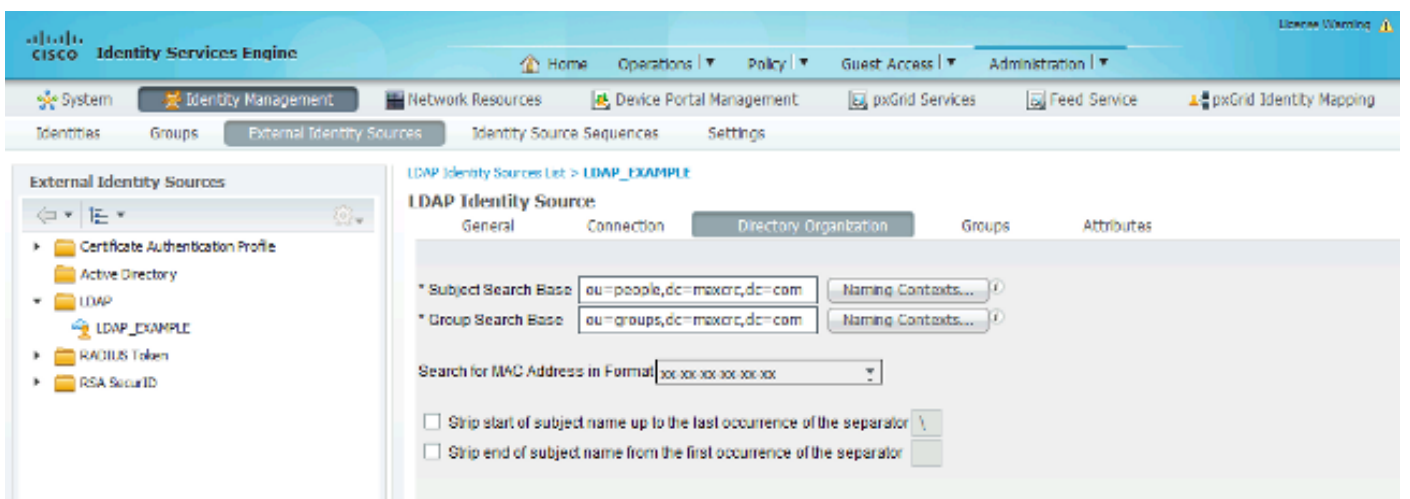
ISE también ofrece algunos esquemas preconfigurados (Microsoft Active Directory, Sun, Novell):



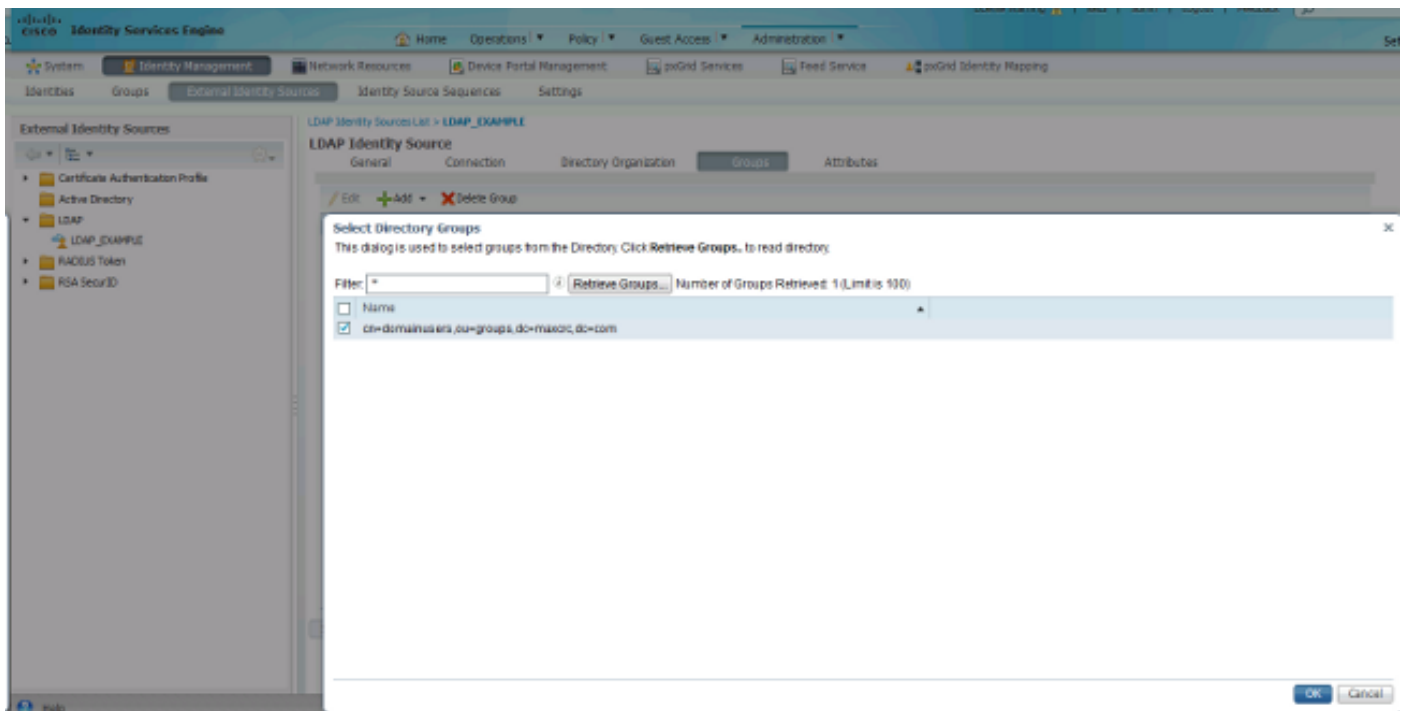
Después de establecer la dirección IP y el nombre de dominio administrativo correctos, puede Probar enlace con el servidor. En este momento, no se recupera ningún asunto o grupo porque las bases de búsqueda aún no están configuradas.

En la ficha siguiente, configure la base de búsqueda de sujetos/grupos. Este es el punto de unión para ISE a LDAP. Sólo podrá recuperar los sujetos y grupos que sean hijos del punto de unión.

En este escenario, se recuperan los sujetos de OU=people y los grupos de OU=groups:

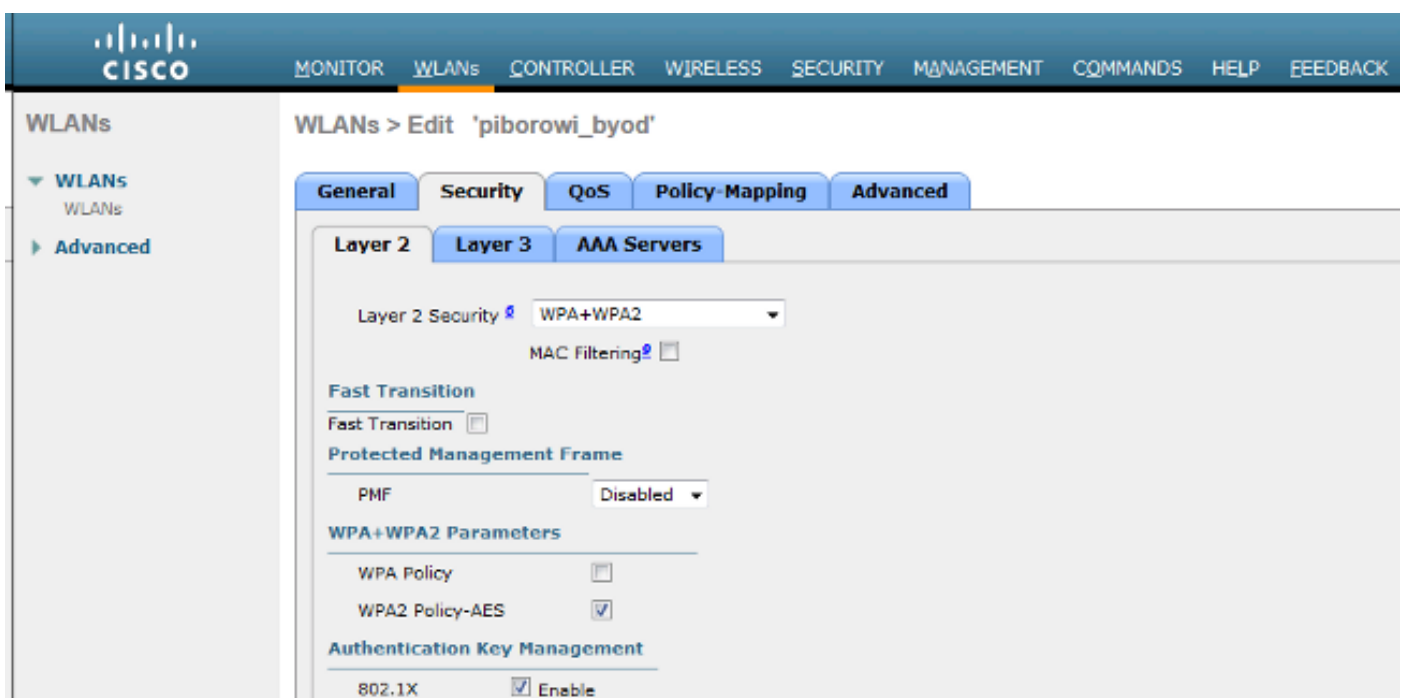


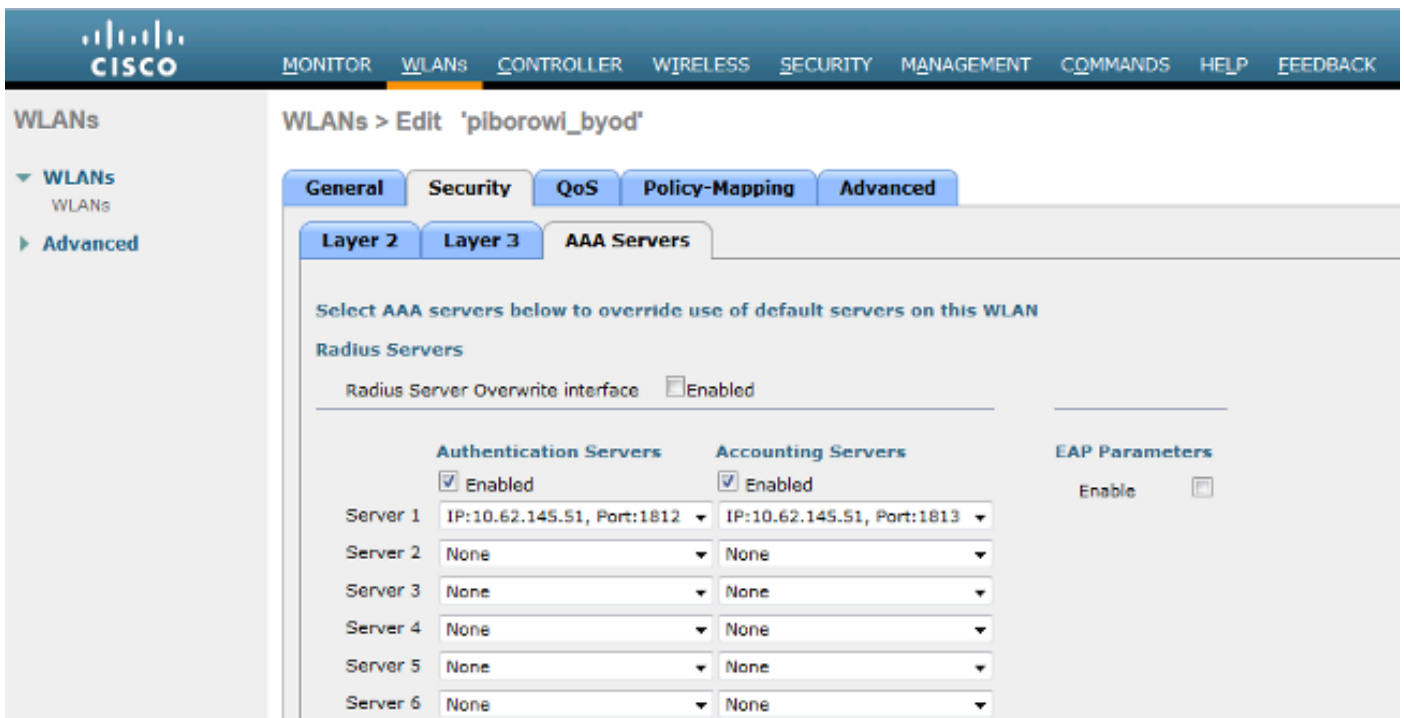
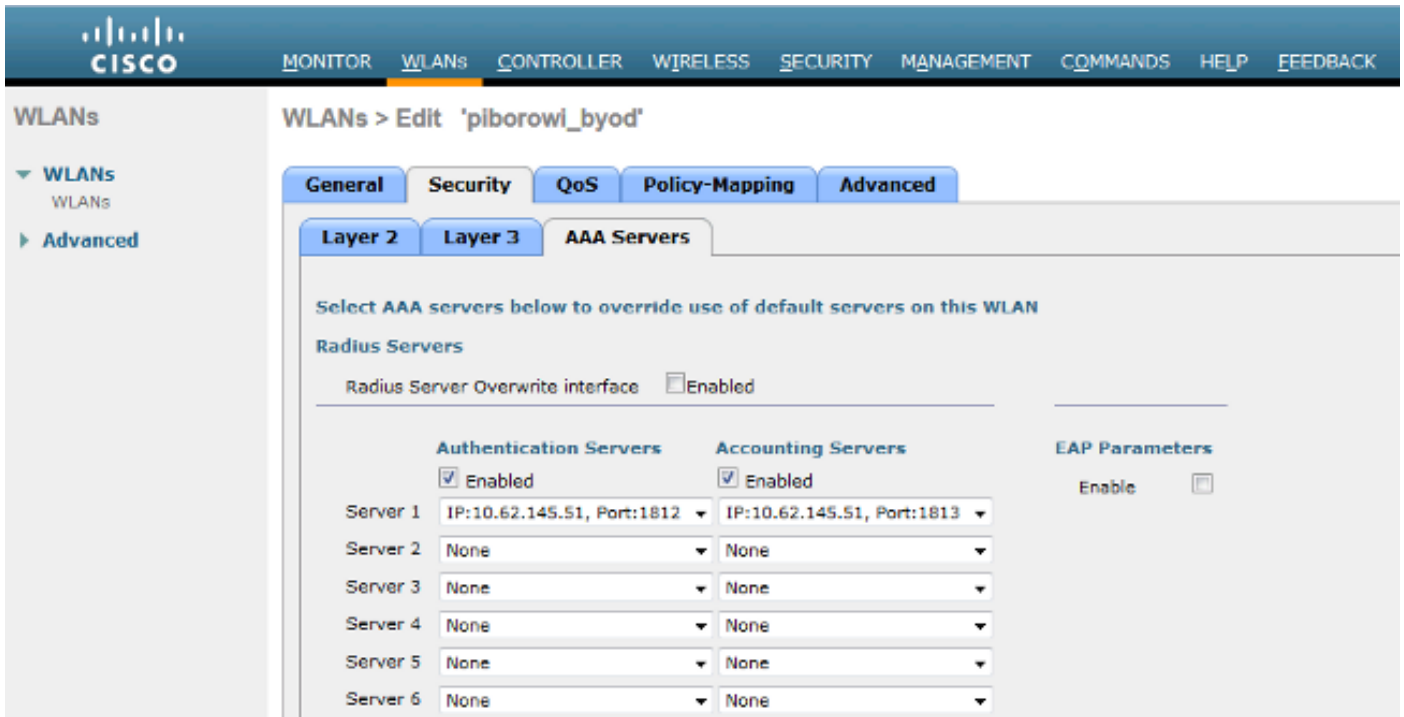
En la pestaña Groups, puede importar los grupos desde LDAP en ISE:



Configurar la WLC

Utilice la información que se proporciona en estas imágenes para configurar el WLC para la autenticación 802.1x:





Configuración de EAP-GTC

Uno de los métodos de autenticación compatibles con LDAP es EAP-GTC. Está disponible en Cisco AnyConnect, pero debe instalar el Editor de perfiles del Administrador de acceso de red para configurar el perfil correctamente.

También debe editar la configuración del Administrador de acceso de red, que (de forma predeterminada) se encuentra aquí:

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

Utilice la información que se proporciona en estas imágenes para configurar el EAP-GTC en el punto final:

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 'piborowi_byod', and checkboxes for 'Hidden Network' and 'Corporate Network', both of which are unchecked. An 'Association Timeout' of 5 seconds is also set.
- 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 'Media Type' sidebar with a list of options: Security Level, Connection Type, User Auth, and Credentials. 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

- 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

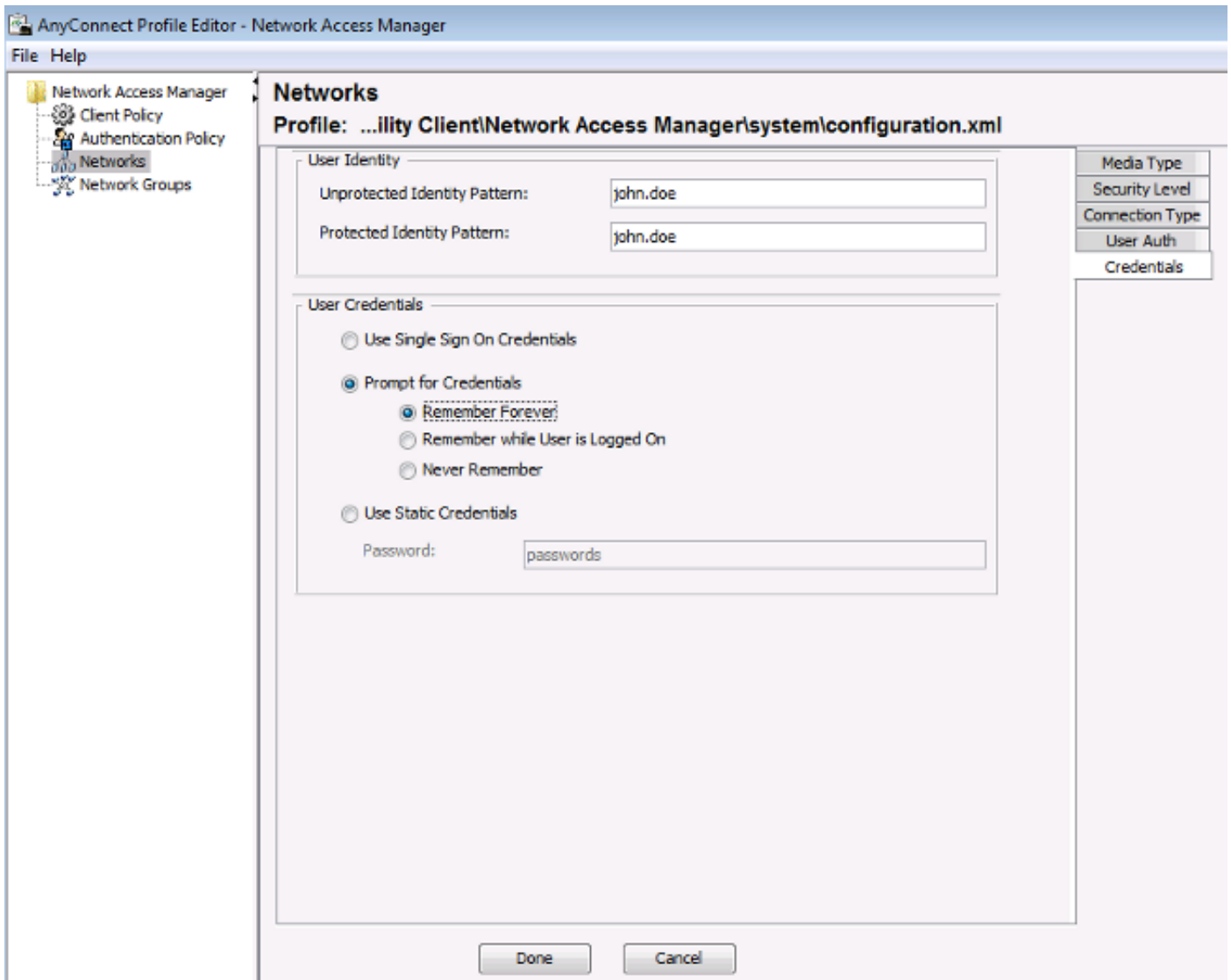
EAP-TLS, using a Certificate

Authenticate using a Token and EAP-GTC

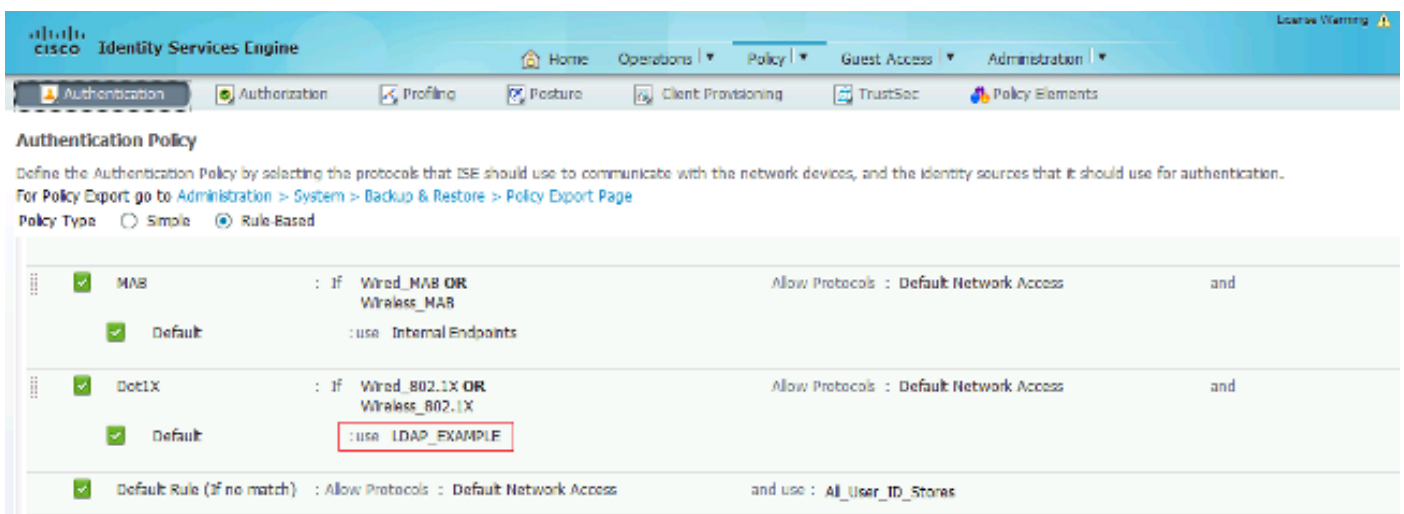
- Media Type
- Security Level
- Connection Type
- User Auth
- Credentials

Next

Cancel



Utilice la información que se proporciona en estas imágenes para cambiar las políticas de autenticación y autorización en 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

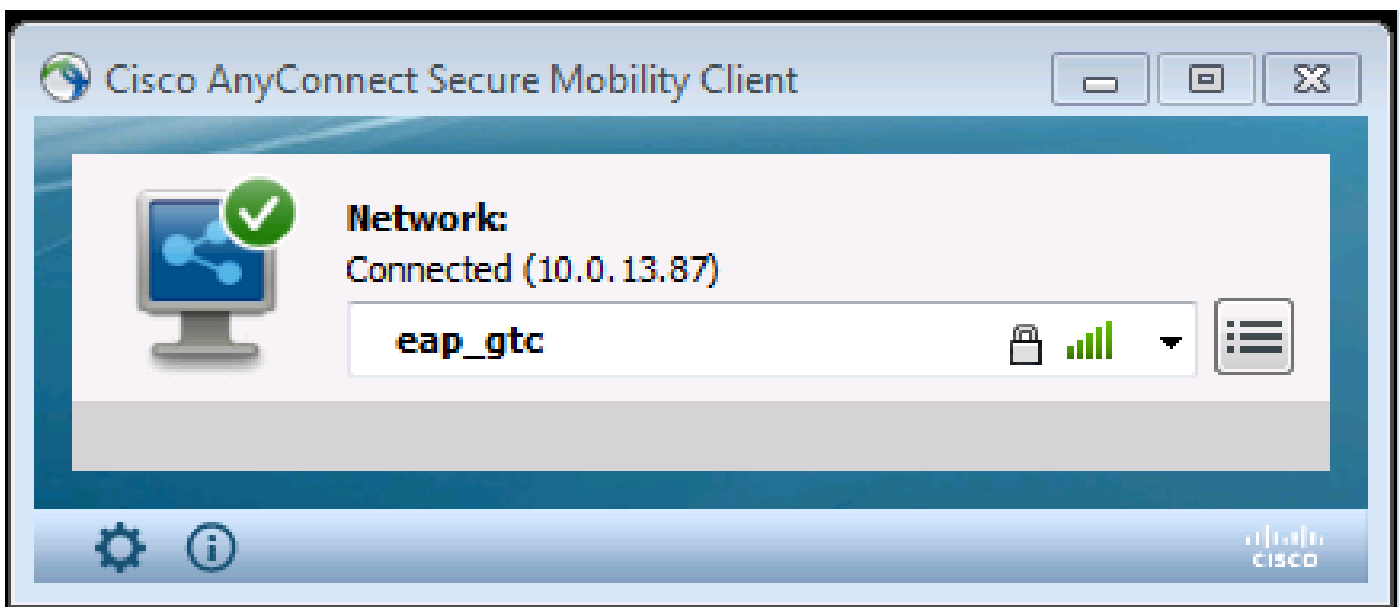
First Matched Rule Applies

Exceptions (0)

Standard

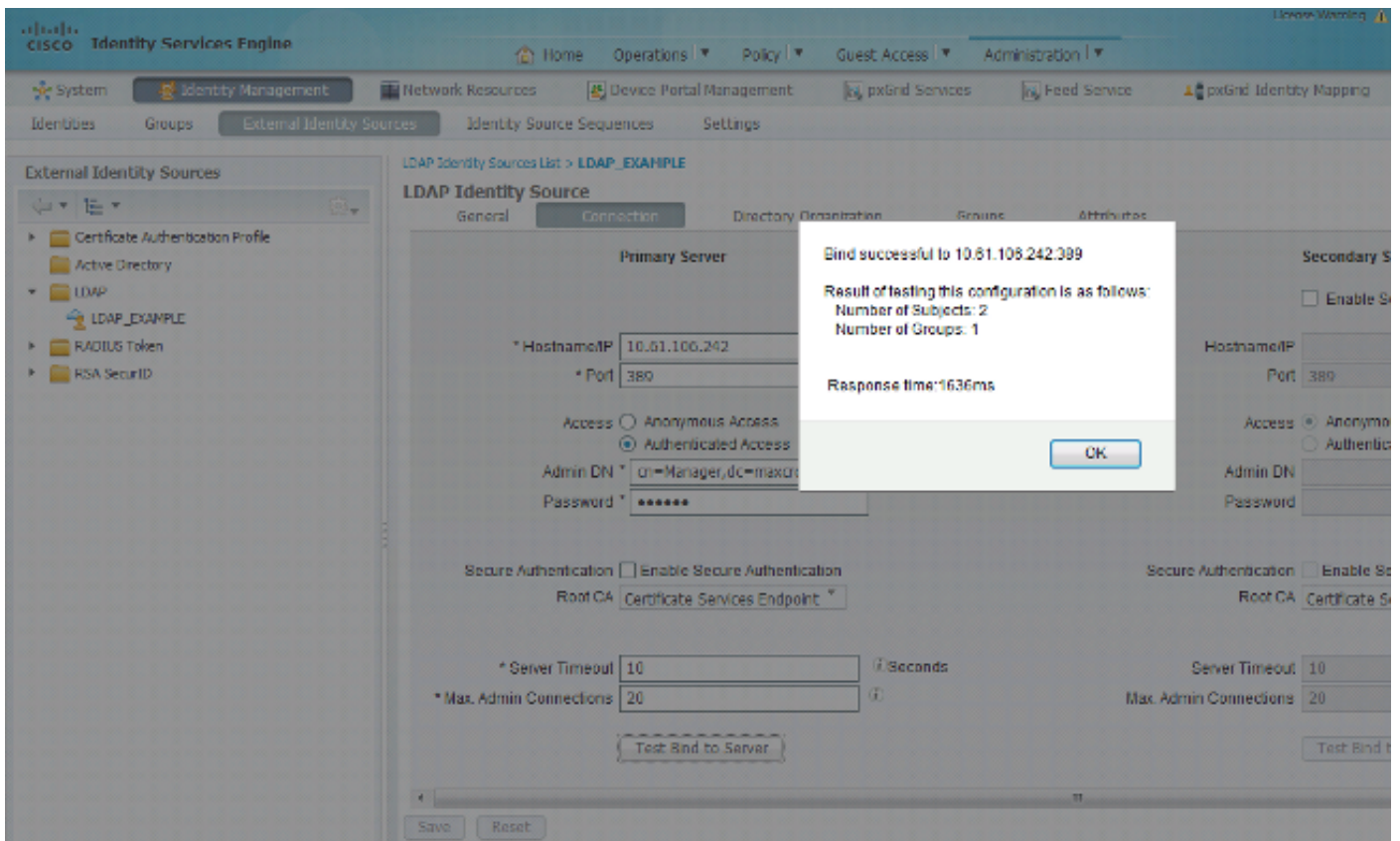
Status	Rule Name	Conditions (Identity groups and other conditions)	Permissions
✓	Users in LDAP store	if (Wireless_802.1X AND LDAP_EXAMPLE:ExternalGroups EQUALS cn=domainusers,ou=groups,dc=mxarc,dc=com)	then PermitAccess
✓	Wireless Black List Default	if Blacklist AND Wireless_Access	then Blackhole_Wireless_Access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

Después de aplicar la configuración, debería poder conectarse a la red:

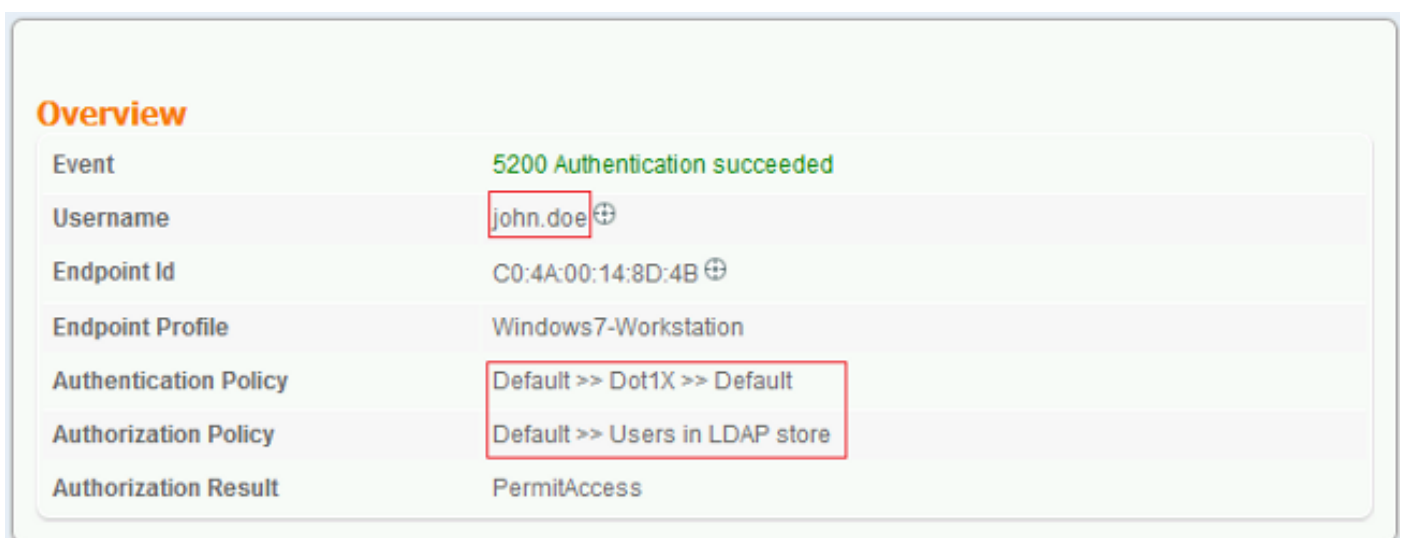
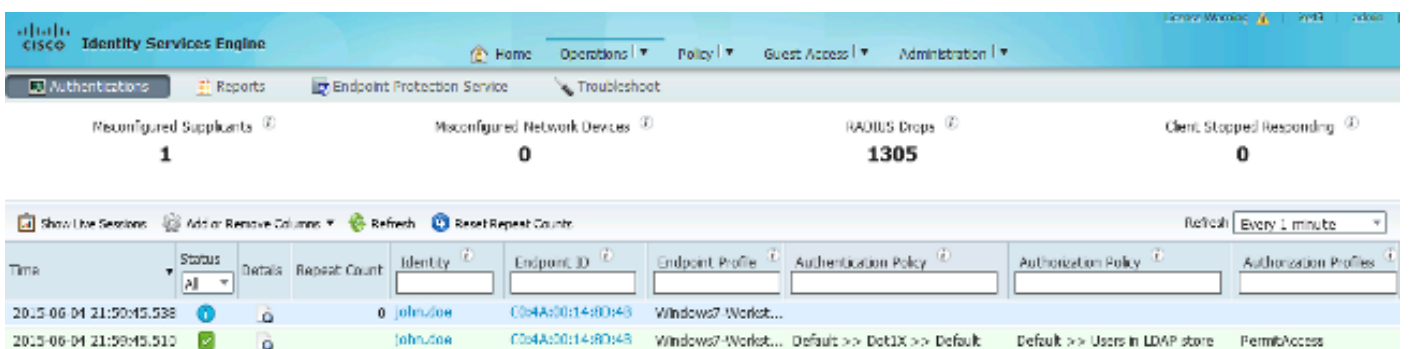


Verificación

Para verificar las configuraciones de LDAP e ISE, recupere los sujetos y grupos con una conexión de prueba con el servidor:



Estas imágenes ilustran un ejemplo de informe de 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

Troubleshoot

Esta sección describe algunos errores comunes que se encuentran con esta configuración y cómo solucionarlos:

- Después de la instalación de OpenLDAP, si encuentra un error que indique que falta un archivo gssapi.dll, reinicie Microsoft Windows.
- Puede que no sea posible editar el archivo configuration.xml para Cisco AnyConnect directamente. Guarde la nueva configuración en otra ubicación y, a continuación, utilícela para sustituir el archivo antiguo.
- En el informe de autenticación, aparece este mensaje de error:

```
<#root>
```

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

Este mensaje de error indica que el método seleccionado no es soportado por LDAP.


Asegúrese de que el protocolo de autenticación del mismo informe muestre uno de los métodos compatibles (EAP-GTC, EAP-TLS o PEAP-TLS).

- En el informe de autenticación, si observa que no se encontró el asunto en el almacén de identidades, el nombre de usuario del informe no coincide con el atributo de nombre de sujeto para ningún usuario de la base de datos LDAP.

En este escenario, el valor se estableció en uid para este atributo, lo que significa que ISE busca los valores uid para el usuario LDAP cuando intenta encontrar una coincidencia.

- Si los sujetos y grupos no se recuperan correctamente durante una prueba de enlace al servidor, es una configuración incorrecta para las bases de búsqueda.

Recuerde que la jerarquía de LDAP debe especificarse desde hoja a raíz y dc (puede constar de varias palabras).

 Sugerencia: Para resolver problemas de autenticación EAP en el lado del WLC, consulte el documento de [Ejemplo de Configuración de Autenticación EAP con Controladores WLAN \(WLC\) de Cisco](#).

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).