

# Configuración del objeto de la autenticación LDAP en el sistema de FireSIGHT

## Contenido

[Introducción](#)

[Configuración de un objeto de la autenticación LDAP](#)

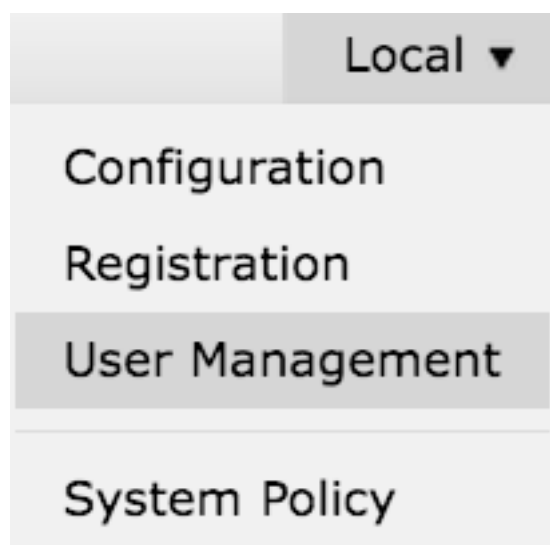
[Documento relacionado](#)

## Introducción

Los objetos de la autenticación son perfiles del servidor para los servidores externos de la autenticación, conteniendo las configuraciones de la conexión y las configuraciones del filtro de la autenticación para esos servidores. Usted puede crear, manejar, y suprimir los objetos de la autenticación en un centro de administración de FireSIGHT. Este documento describe cómo configurar el objeto de la autenticación LDAP en el sistema de FireSIGHT.

## Configuración de un objeto de la autenticación LDAP

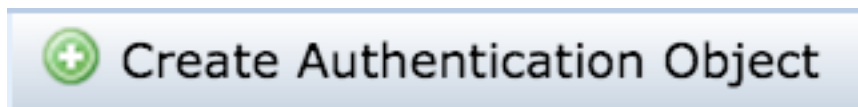
1. Ábrase una sesión al interfaz del Web User del centro de administración de FireSIGHT.
2. Navegue al **sistema** > al **Local** > **User Management (Administración de usuario)**.



Seleccione la **autenticación de inicio de sesión** cuadro.



Haga clic en **crean el objeto de la autenticación**.



3. Seleccione un **método de autenticación** y un **tipo de servidor**.

- **Método de autenticación:** LDAP
- **Nombre:** *Objeto Name* > del <*Authentication*
- **Tipo de servidor:** Active Directory ms

Nota: Los campos marcados con los asteriscos (\*) se requieren.

**Authentication Object**

Authentication Method	LDAP
Name *	<input type="text"/>
Description	<input type="text"/>
Server Type	MS Active Directory

4. Especifique el nombre de host o la dirección IP del servidor primario y de backup. Un servidor de reserva es opcional. Sin embargo, cualquier regulador del dominio dentro del mismo dominio se puede utilizar que un servidor de reserva.

Nota: Aunque el puerto LDAP sea valor por defecto al puerto **389**, usted puede utilizar un número del puerto no estándar en el cual el servidor LDAP esté escuchando.

5. Especifique los **parámetros LDAP-específicos** como se muestra abajo:

Consejo: El usuario, el grupo, y los atributos OU deben ser identificados antes de configurar los **parámetros LDAP-específicos**. Lea [este documento](#) para identificar los atributos de objeto del Active Directory LDAP para la configuración del objeto de la autenticación.

- **Base el DN** - Dominio u OU específico DN
- **Filtro bajo** - El grupo DN que los usuarios son miembro de.
- **Nombre de usuario** - La personificación explica DC
- **password:** <*password*>
- **Confirme la contraseña:** <*password*>

Opciones avanzadas:

- **Cifrado:** SSL, TLS o ninguno
- **Trayectoria de la carga por teletratamiento del certificado SSL:** Cargue por teletratamiento la certificación CA (opcional)
- **Plantilla del Nombre de usuario:** %s

- Descanso (segundos): 30

**LDAP-Specific Parameters**

Base DN \*   ex. dc=sourcefire,dc=com

Base Filter  ex. (cn=jsmith), (lcn=jsmith), (&(cn=jsmith)((cn=bsmith)(cn=csmith\*)))

User Name \*  ex. cn=jsmith,dc=sourcefire,dc=com

Password \*

Confirm Password \*

Show Advanced Options ▼

Encryption  SSL  TLS  None

SSL Certificate Upload Path   ex. PEM Format (base64 encoded version of DER)

User Name Template  ex. cn=%s,dc=sourcefire,dc=com

Timeout (Seconds)

En la configuración de la política de seguridad del dominio del ANUNCIO, si el **requisito de firma del servidor LDAP** se fija al **requerir firma**, el SSL o TLS debe ser utilizado.

### Requisito de firma del servidor LDAP

- **Ninguno:** La firma de los datos no se requiere para atar con el servidor. Si los datos de las solicitudes de cliente que firman, los soportes de servidor él.
- **Requerir firma:** A menos que se esté utilizando TLS \ SSL, la opción de firma de los datos LDAP debe ser negociada.

Nota: No requieren al lado del cliente o el certificado CA (CERT CA) para LDAPS. Sin embargo, sería un nivel de seguridad adicional de CERT CA se carga por teletratamiento al objeto de la autenticación.

### 6. Especifique la asignación del atributo

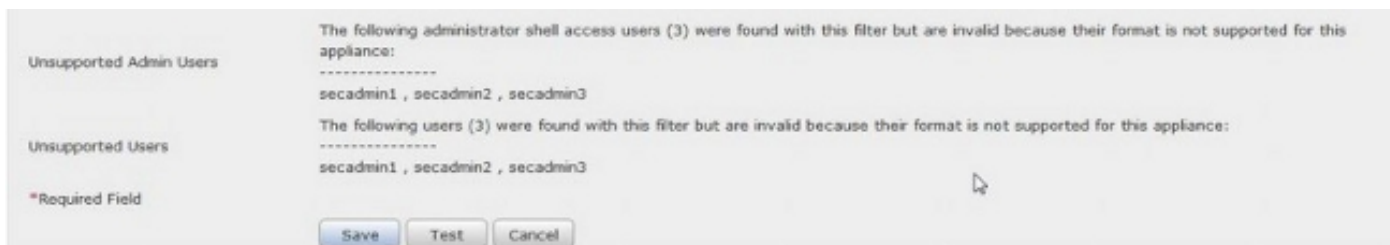
- **Atributo del acceso UI:** sAMAccountName
- **Atributo del acceso del shell:** sAMAccountName

**Attribute Mapping**

UI Access Attribute \*

Shell Access Attribute \*

Consejo: Si usted encuentra el mensaje **sin apoyo de los usuarios** en la salida de la prueba, cambie el **atributo del acceso UI** al **userPrincipalName** y asegúrese de que **plantilla del Nombre de usuario** está fijado a **%s**.



## 7. Configure los papeles del acceso controlado del grupo

En `ldp.exe`, hojee a cada grupos y copie al grupo correspondiente DN al objeto de la autenticación como se muestra abajo:

- **Grupo DN de Name>** del <Group: dn> del <group>
- **Atributo del miembro del grupo:** debe siempre estar el **miembro**

Ejemplo:

- **Grupo del administrador DN:** Admins CN=DC, grupos de CN=Security, DC=VirtualLab, DC=local
- **Atributo del miembro del grupo:** miembro

Un grupo de seguridad del ANUNCIO hace que un atributo del **miembro** sea seguido por los usuarios del DN del miembro. El atributo precedente del **miembro del** número indica el número de usuarios miembros.

```
3> member: CN=secadmin3,CN=Users,DC=VirtualLab,DC=local; CN=secadmin2,CN=Users,DC=VirtualLab,DC=local; CN=secadmin1,CN=Users,DC=VirtualLab,DC=local;
```


8. Seleccione **lo mismo que el filtro bajo** para el filtro del acceso del shell, o especifique el atributo del `memberOf` como se indica en el paso 5.

**Descasque el filtro del acceso:** (`memberOf=<group DN>`)

Como ejemplo,

**Filtro del acceso del shell:** (`usuarios del memberOf=CN=Shell, grupos de CN=Security, DC=VirtualLab, DC=local`)

9. Salve el objeto de la autenticación y realice una prueba. Un resultado de la prueba satisfactoria parece abajo:

 **Info** ✕


Administrator Shell Test:

3 administrator shell access users were found with this filter.  
See Test Output for details.

 **Info** ✕

User Test:

3 users were found with this filter.  
See Test Output for details.

 **Success** ✕

Test Complete: You may enter a test user name to further verify your Base Filter parameter.

Admin Users	The following administrator shell access users (3) were found with this filter: ----- secadmin1, secadmin2, secadmin3
Users	The following users (3) were found with this filter: ----- secadmin1, secadmin2, secadmin3

\*Required Field

10. Una vez que el objeto de la autenticación pasa la prueba, active el objeto en la política del sistema y reaplique la directiva a su dispositivo.

## Documento relacionado

- [Identifique los atributos de objeto del Active Directory LDAP para la configuración del objeto](#)

[de la autenticación](#)