# Configuración del mapeo de atributos LDAP en ASA para VPN de cliente seguro

## Contenido



## Introducción

Este documento describe cómo configurar la asignación de atributos LDAP en Cisco ASA para asignar políticas de grupo VPN basadas en grupos de Active Directory.

### Requirements

#### Requisitos de Cisco ASA

- Cisco ASA con una versión de software compatible.
- Acceso administrativo al dispositivo ASA.

#### Requisitos de la red

- Dominio de Active Directory (AD) accesible para ASA.
- LDAP sobre SSL (LDAP) configurado en el servidor AD (puerto predeterminado 636).

Requisitos del cliente

- Secure Client instalado en los dispositivos cliente.

### Componentes Utilizados

La información de este documento no se limita a versiones específicas de software y hardware.

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.

## Configuration Steps

### Paso 1. Definición de Políticas de Grupo

Las directivas de grupo determinan los permisos y las restricciones para los usuarios de VPN. Cree las políticas de grupo necesarias que se ajusten a los requisitos de acceso de su organización.

Crear una directiva de grupo para usuarios autorizados

```
group-policy VPN_User_Policy internal
group-policy VPN_User_Policy attributes
  vpn-simultaneous-logins 3
  split-tunnel-policy tunnelspecified
  split-tunnel-network-list value SPLIT_TUNNEL_ACL
```

Cree una directiva de grupo predeterminada para denegar el acceso.

```
group-policy No_Access_Policy internal
group-policy No_Access_Policy attributes
  vpn-simultaneous-logins 0
```

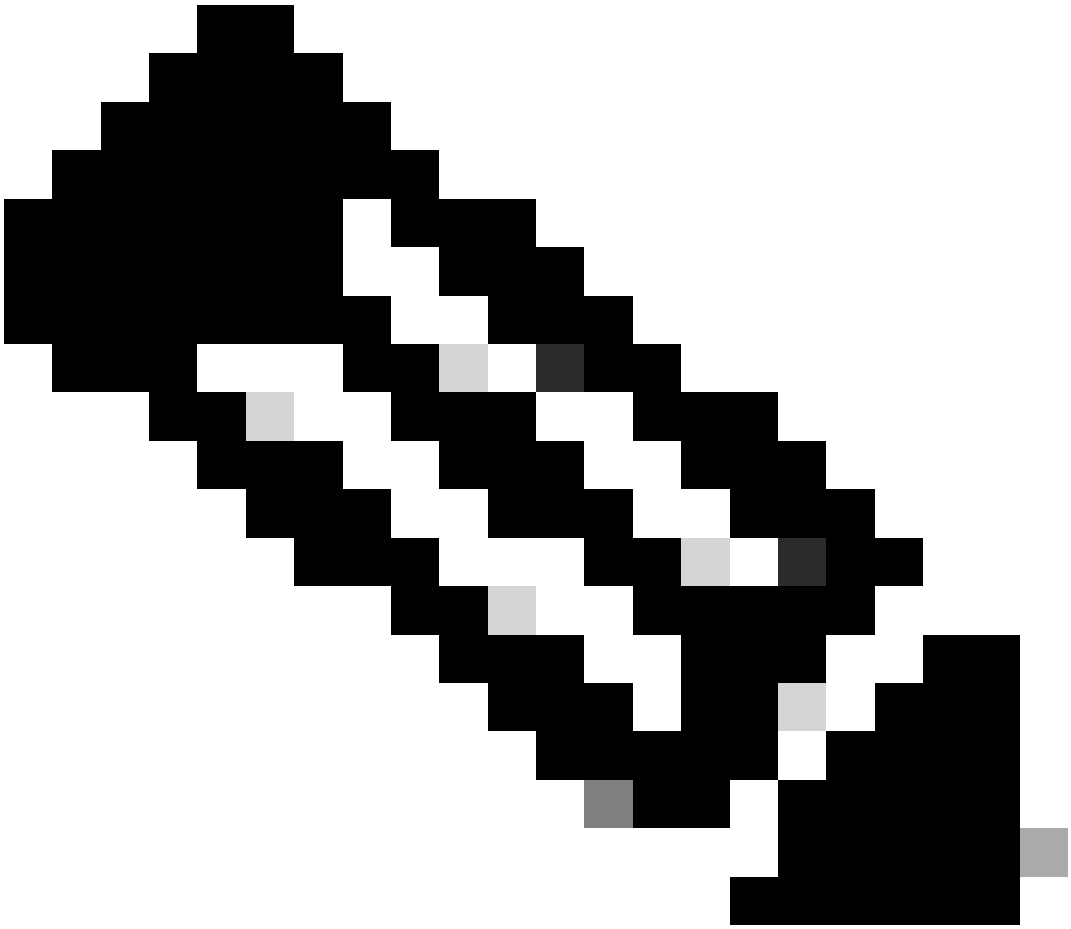
### Paso 2. Configure el Mapa de Atributos LDAP

El mapa de atributos traduce los atributos LDAP a atributos ASA, lo que permite al ASA asignar usuarios a la política de grupo correcta en función de sus pertenencias a grupos LDAP.

```
ldap attribute-map VPN_Access_Map
  map-name  memberOf Group-Policy
```

```
  map-value memberOf "CN=VPN_Users,OU=Groups,DC=example,DC=com" VPN_User_Policy
```

---



Nota: El nombre distinguido (DN) del grupo LDAP debe ir siempre entre comillas dobles (""). Esto garantiza que ASA interpreta correctamente los espacios y caracteres especiales en el DN.

---

## Paso 3. Configure el Servidor LDAP AAA

Configure ASA para comunicarse con el servidor AD para la autenticación y la asignación de grupos.

```
aaa-server AD_LDAP_Server protocol ldap
aaa-server AD_LDAP_Server (inside) host 192.168.1.10
  ldap-base-dn dc=example,dc=com
  ldap-scope subtree
  ldap-naming-attribute sAMAccountName
```

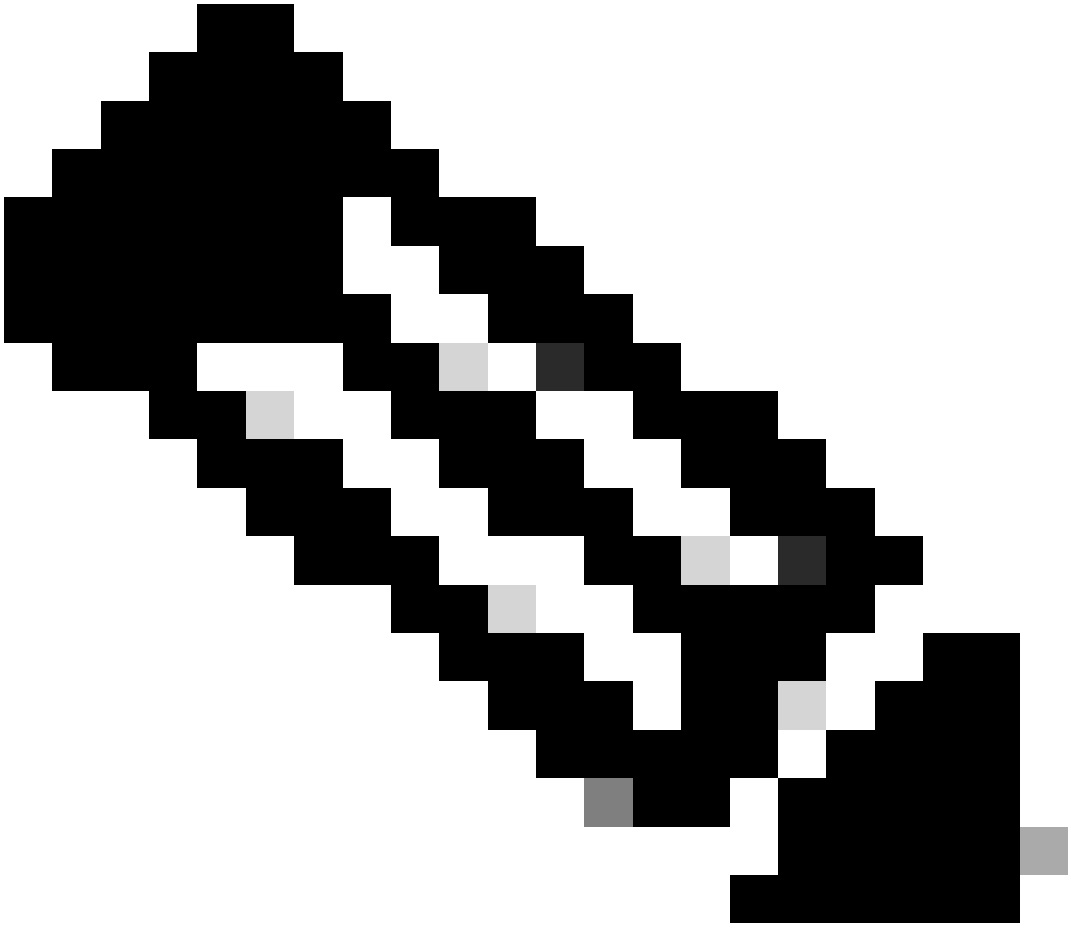
```
  ldap-login-password ********
  ldap-login-dn CN=ldap_bind_user,OU=Service Accounts,DC=example,DC=com
  ldap-over-ssl enable
  ldap-attribute-map VPN_Access_Map
```

## Paso 4. Defina el Grupo de Túnel

El grupo de túnel define los parámetros VPN y vincula la autenticación al servidor LDAP.

```
tunnel-group VPN_Tunnel type remote-access
tunnel-group VPN_Tunnel general-attributes
  address-pool VPN_Pool
  authentication-server-group AD_LDAP_Server
  default-group-policy No_Access_Policy

tunnel-group VPN_Tunnel webvpn-attributes
  group-alias VPN_Tunnel enable
```



Nota: El default-group-policy se configura en No_Access_Policy, denegando el acceso a los usuarios que no coincidan con ningún criterio de mapa de atributo LDAP.

## Verificación

Una vez finalizada la instalación, compruebe que los usuarios están correctamente autenticados y que se les han asignado las directivas de grupo adecuadas.

Verificar asignación de sesión VPN

```
show vpn-sessiondb anyconnect filter name
```

Reemplace <username> con la cuenta de prueba real.

# Troubleshoot

Use esta sección para resolver problemas de configuración.

Habilitar depuración LDAP

Si los usuarios no reciben las directivas de grupo esperadas, habilite la depuración para identificar problemas.

```
debug ldap 255
debug aaa common 255
debug aaa shim 255
```

Iniciar una conexión VPN

Haga que un usuario de prueba intente conectarse mediante Cisco Secure Client.

Revisar salida de depuración

Verifique los registros de Cisco ASA para asegurarse de que el usuario esté asignado a la política de grupo correcta en función de su pertenencia al grupo de Active Directory (AD).

Deshabilitar depuración después de la verificación

```
undebug all
```

## Problemas comunes

Las asignaciones de atributos LDAP distinguen entre mayúsculas y minúsculas. Asegúrese de que los nombres del grupo AD en las sentencias map-value coincidan exactamente, incluyendo la distinción entre mayúsculas y minúsculas.

Compruebe que los usuarios son miembros directos de los grupos AD especificados. No siempre se reconocen las pertenencias a grupos anidados, lo que provoca problemas de autorización.

Los usuarios que no coincidan con ningún criterio de valor de mapa recibirán la política de grupo predeterminada (No_Access_Policy en este caso), lo que impedirá el acceso.

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).