

Tech Note

SSL-VPN

Using LDAP Groups with Microsoft Windows 2003 Active Directory

This technote provides procedures to configure an LDAP group for an LDAP authentication domain in Windows 2003 Active Directory.

Windows 2003 Active Directory

In this example, an LDAP group called 'Sales' has been created in the Active Directory tree. 'User1' is a member of this group.

The screenshot shows the 'Active Directory Users and Computers' console. The left pane shows the tree structure with 'Users' expanded. The main pane displays a list of 28 objects. The 'Sales' group is highlighted. The 'User1 Properties' dialog box is open, showing the 'Member Of' tab. The 'Member Of' list includes 'Sales' with the path 'examplecompany.com/Users'. The 'Primary group' is set to 'Domain Users'.

Name	Type	Description
DnsUpdateProxy	Security Group ...	DNS clients who are permi...
Domain Admins	Security Group ...	Designated administrators...
Domain Computers	Security Group ...	All workstations and serve...
Domain Controllers	Security Group ...	
Domain Guests	Security Group ...	
Domain Users	Security Group ...	
Enterprise Admins	Security Group ...	
Group Policy Creator Ow...	Security Group ...	
Guest	User	
HelpServicesGroup	Security Group ...	
Internet Access	Security Group ...	
IS	Security Group ...	
Marketing	Security Group ...	
No Adult	Security Group ...	
RAS and IAS Servers	Security Group ...	
Sales	Security Group ...	
Schema Admins	Security Group ...	
SUPPORT_388945a0	User	
TelnetClients	Security Group ...	
User1	User	
User2	User	
User3	User	
User4	User	

Name	Active Directory Folder
Domain Users	examplecompany.com/Users
Internet Access	examplecompany.com/Users
No Adult	examplecompany.com/Users
Sales	examplecompany.com/Users
VPN Group 1	examplecompany.com/VPN Users

Tech Note

SonicWALL SSL-VPN Appliance

1. Create the LDAP authentication domain.

The BaseDN is the root of the directory tree. DN stands for Distinguished Name, which identifies and describes an object in the LDAP directory. In the **LDAP BaseDN** field, enter the DN for the folder which contains the user objects. In this example, our Users folder is at examplecompany.com/Users, whose BaseDN is cn=users,dc=examplecompany,dc=com.

2. Enter a valid username and password, then link the LDAP domain to a portal.

Edit Domain

Authentication Type: LDAP

Domain Name: LDAP domain

Server Address: 192.168.168.111

LDAP BaseDN*: cn=users,dc=examplecor

Login user name: Administrator

Login password: ●●●●●●●●

Portal Layout Name: LocalDomain

Require client digital certificates

3. Create the LDAP Group.

In our Active Directory tree, we had a group object called 'Sales', and 'User1' is a member of this group. The DN for the 'Sales' group object is 'cn=sales,cn=users,dc=examplecompany,dc=com'. Therefore, an attribute of User1 is that he's a member of that DN. This is expressed as **memberOf="cn=sales,cn=users,dc=examplecompany,dc=com"**.

Note: When creating the 'LDAP Domain' authentication domain, an 'LDAP Domain' group is automatically created. In this example, the 'LDAP Domain' group was not modified with the addition of specific LDAP attributes. Therefore, the 'LDAP Domain' group will serve as the less-specific group for all successfully authenticating 'LDAP Domain' users, who are not explicit members of the 'sales' group.

General Group Settings

Group Name: Sales

Domain Name: LDAP domain

LDAP Attribute (name="value"): memberOf="cn=sales,cn=use

LDAP Attribute (name="value"):

LDAP Attribute (name="value"):

LDAP Attribute (name="value"):

Inactivity Timeout (Minutes): 0

* Set the Inactivity Timeout to 0 to use the Global timeout setting.

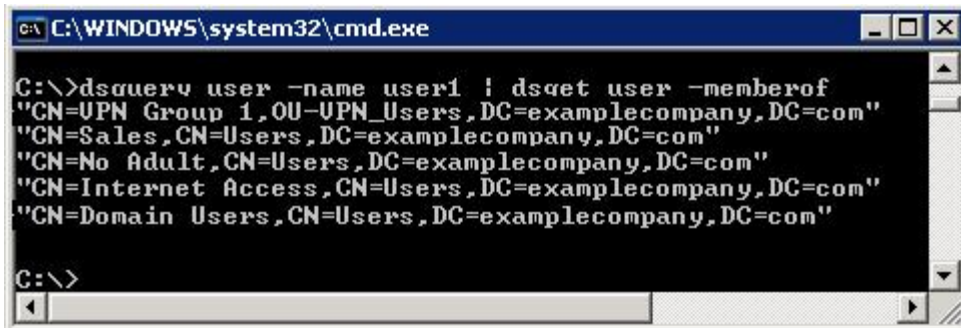


Tech Note

If you are unsure of the LDAP group's DN or need to verify the user's 'memberOf' attribute, enter at a command prompt on the server:

```
dsquery user -name username | dsget user -memberof
```

This will give you the DN for the LDAP groups that the user belongs to. See the example below:



```
C:\WINDOWS\system32\cmd.exe
C:\>dsquery user -name user1 | dsget user -memberof
"CN=UPN Group 1,OU=UPN_Users,DC=examplecompany,DC=com"
"CN=Sales,CN=Users,DC=examplecompany,DC=com"
"CN=No Adult,CN=Users,DC=examplecompany,DC=com"
"CN=Internet Access,CN=Users,DC=examplecompany,DC=com"
"CN=Domain Users,CN=Users,DC=examplecompany,DC=com"
C:\>
```

To test, log into the LDAP domain as the user. Open a separate browser, log in as **Admin**, and go to **Users > Status**. The user should appear in the list of Active User Sessions, and the Group column should say 'Sales'.



The screenshot shows the SonicWall SSL-VPN web interface. The left sidebar contains navigation options: System, Network, Portal, NetExtender, Users, Status, Local Users, and Local Groups. The main content area is titled 'Users > Status' and displays a table of 'Active User Sessions'.

Name	Group	IP Address	Login Time	Logged in	Idle Time	Logout
admin	LocalDomain	1.1.1.1	Sat Dec 17 07:52:03 2005	0 Days 00:00:15	0 Days 00:00:00	
user1	Sales	1.1.1.1	Sat Dec 17 07:52:15 2005	0 Days 00:00:04	0 Days 00:00:03	