

Setting up Multiple LDAP Domains in SonicWall 6.5 Firmware without Partitioning.

SonicWall 6.5 firmware now allows multiple LDAP servers for authentication, to set this up follow the guide below.

SonicWall OS 6.5 onwards is all available on all Gen6 Appliances from the SOHO wireless and up (not including the non-wireless SOHO as this runs 5.9 firmware).

Prerequisites:

- For this to work you will need to make sure each Domain is resolvable via the SonicWall DNS settings, e.g. in this example the SonicWall's DNS settings under Network\DNS are set to each of the Servers' IP addresses. The domain Netthreat.local resolves to 172.16.32.250 and the domain Test.local resolves to 172.16.32.60, they also each have A records in the forward look up zones to each domain for failover. If the name resolves to multiple IP addresses then use the name for the LDAP connection rather than IP address i.e. Test.local (not the server name) instead of 172.16.32.60.
- The Domains in the example are not in a Trust or the same forest.

1. Add Domains

Add the required Domains to use for LDAP Authentication under Users\Settings\Configure LDAP

2. Login/Bind settings

For the Login/Bind settings you can use any of the three methods below.

N.B. The Bind Usernames and Passwords don't have to be the same (this is only needed for Domains in a trust).

Method 1: Give Bind Distinguished Name (Domain\User). This is ideal if you don't know the exact location in AD of the Administrator account.

Edit server

Settings Login/Bind Schema Directory

☐ Anonymous login
 ☐ Give login name/location in tree
 ☒ Give bind distinguished name

Bind distinguished name: Netthreat\Administrator

User tree for login to server:

Password:

When referred to other servers:
 ☒ Bind with this account
 ☐ Bind with an equivalent account on that server (same password)

Method 2: Give Bind Distinguished Name (Using the distinguished Name).

To find these details if they are not visible in the Users Account in AD then go to View and select Advanced Features then in the Users Details you will now see the Attribute Editor, you can select the distinguishedName choose the View Tab and you can copy the details.

Edit server

Settings Login/Bind Schema Directory

☐ Anonymous login
 ☐ Give login name/location in tree
 ☒ Give bind distinguished name

Bind distinguished name: CN=Administrator,CN=Users,DC=Netthreat,DC=Local

User tree for login to server:

Password:

When referred to other servers:
 ☒ Bind with this account
 ☐ Bind with an equivalent account on that server (same password)

Method 3: Give Login name/location in tree (this must be where the User Account that you are using to bind is located in AD)

Edit server

Settings Login/Bind Schema Directory

☐ Anonymous login
 ☒ Give login name/location in tree
 ☐ Give bind distinguished name

Login user name: Administrator

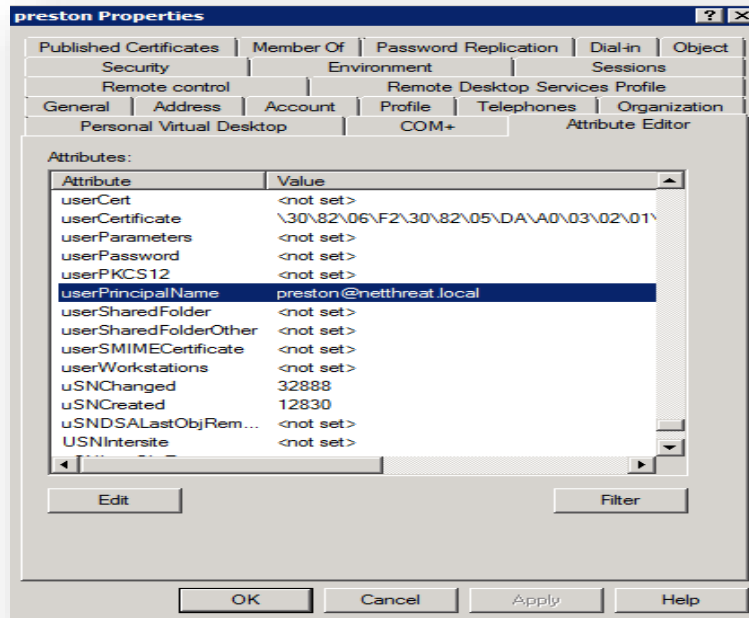
User tree for login to server: netthreat.local/Users

Password:

When referred to other servers:
 ☒ Bind with this account
 ☐ Bind with an equivalent account on that server (same password)

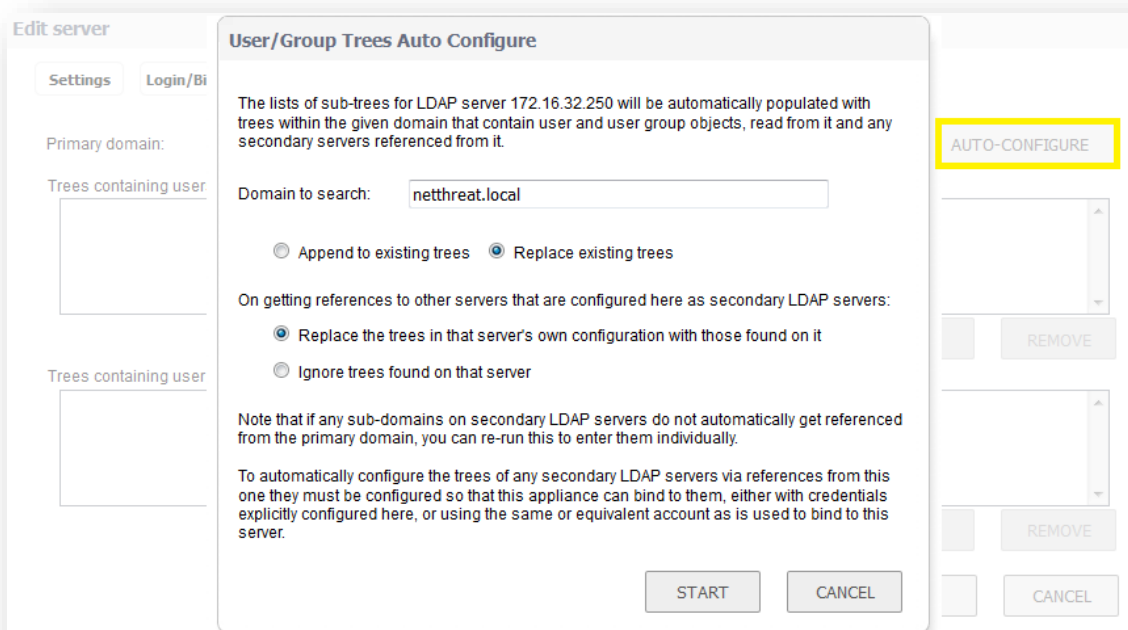
3. Schema Settings

For the Schema Settings, both Domains need to use the same Schema settings. If you have some usernames which are identical in both Domains then make sure that the Users in each Domain's Active Directory are set under userPrincipalName to the User@domain type as below:



4. Directory Settings

On the Directory settings select auto-configure, Replace existing trees and then Start.

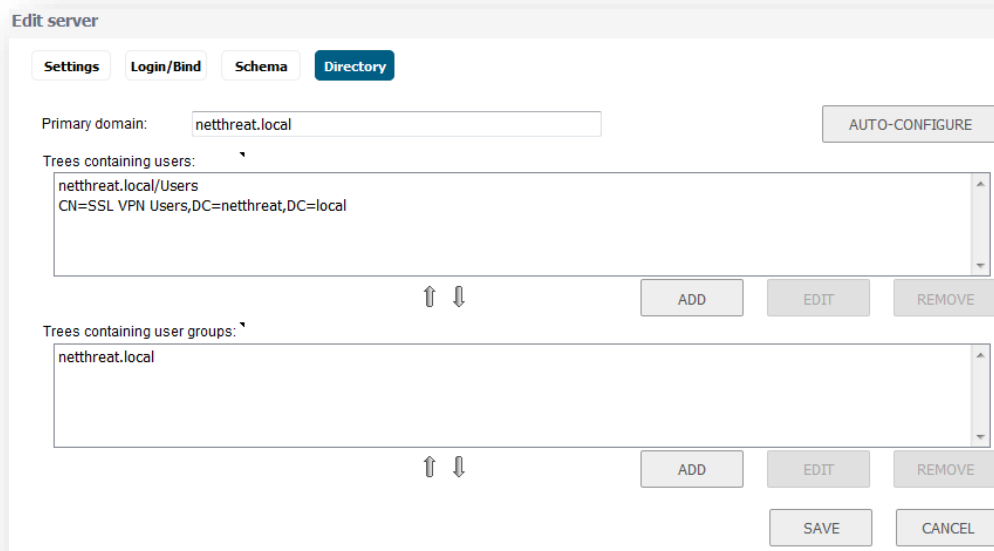


This should pull in your Trees with that include Users as below. You can manually add others if needed.

If the Users Trees don't pull in then go to the Test tab and check the Connectivity / bind test. If this succeeds then try the Directory Auto-configure again, otherwise check the Username and Password in the Bind Settings.

Also make sure you have un-ticked the Case Sensitive Usernames option in the User/Settings Menu.

Tip: If you have trouble with users being authenticated in a group add the distinguished name like in the example below for the SSL VPN Users Group.

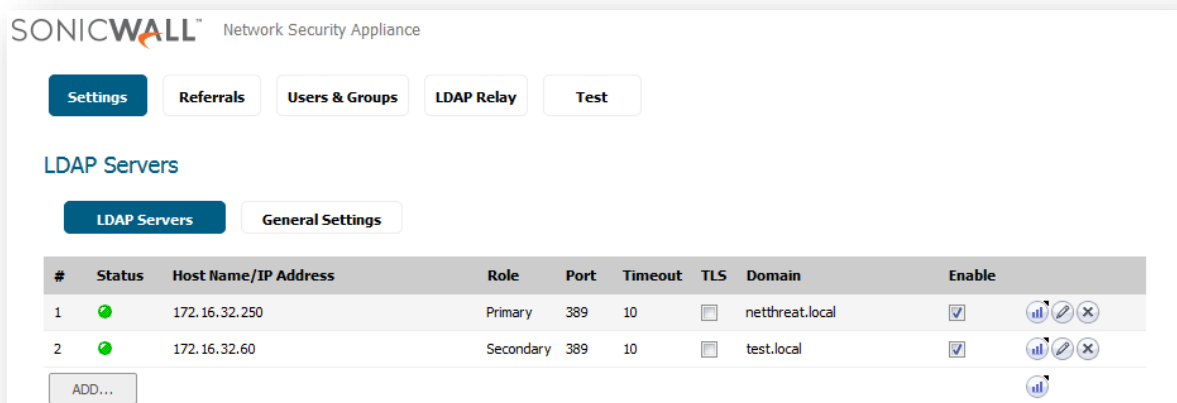








5. Add Secondary Domains

Repeat steps 2 to 4 to add the Secondary Domain.

You should now see both Domains connected as below.

You can add more Domains if needed by adding them as Secondary Domains.

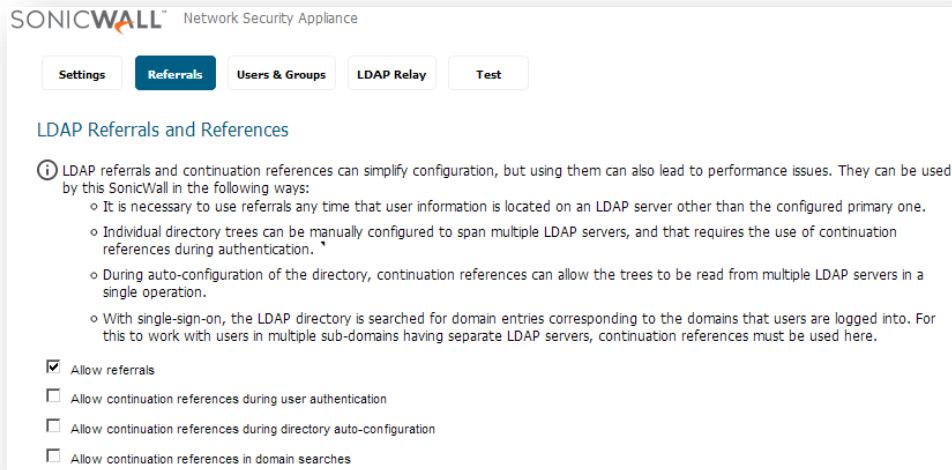


#	Status	Host Name/IP Address	Role	Port	Timeout	TLS	Domain	Enable	
1	OK	172.16.32.250	Primary	389	10	<input type="checkbox"/>	netthreat.local	<input checked="" type="checkbox"/>	  
2	OK	172.16.32.60	Secondary	389	10	<input type="checkbox"/>	test.local	<input checked="" type="checkbox"/>	  

ADD...

6. Referrals

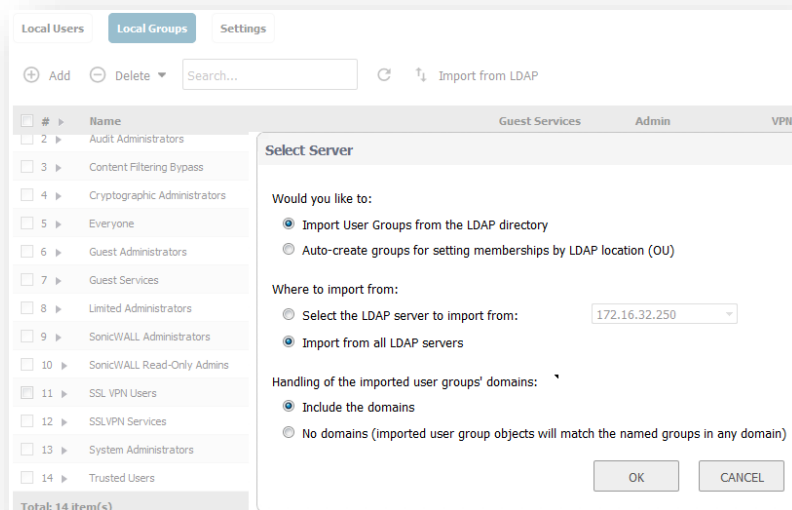
It is **important** that under the Referrals Menu, you only select **Allow Referrals** as below otherwise you will have issues with password caching.



7. Importing the User Groups

In both Domains for this example we have created the same group name called SSL VPN Users. With 6.5 firmware you can now import the Groups from both Domains simultaneously.

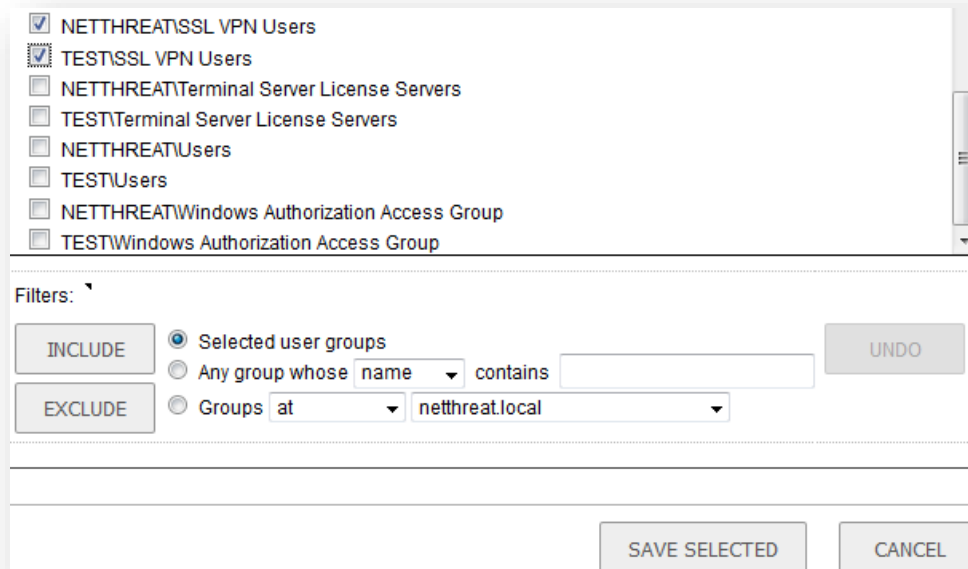
Go to Users/Local Groups and select Import from LDAP



Choose the Selected Groups to Import.

N.B. I've selected **Include the Domains**. Normally as you are using the same user group name from both Domains you could select **No Domains** and it would authenticate any user in the SSL VPN Users group in any of the Domains, see below example in section 8.

Once you have selected the Groups then Save.



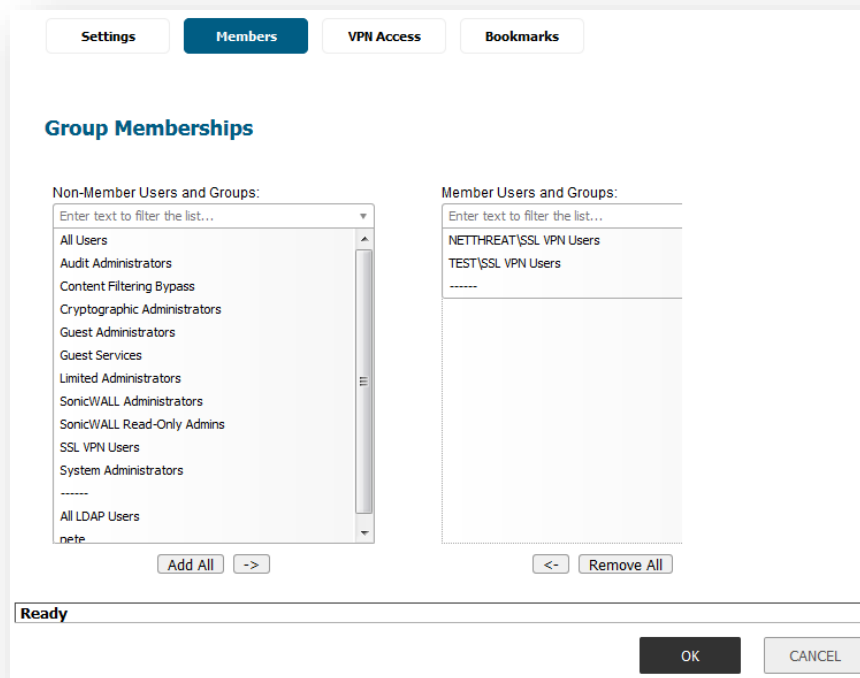
The screenshot shows a dialog box for selecting user groups. It features a list of groups with checkboxes: ☒ NETTHREAT\SSL VPN Users, ☒ TEST\SSL VPN Users, ☐ NETTHREAT\Terminal Server License Servers, ☐ TEST\Terminal Server License Servers, ☐ NETTHREAT\Users, ☐ TEST\Users, ☐ NETTHREAT\Windows Authorization Access Group, and ☐ TEST\Windows Authorization Access Group. Below the list is a 'Filters:' section with two main options: 'INCLUDE' and 'EXCLUDE'. Under 'INCLUDE', there are three radio buttons: 'Selected user groups' (selected), 'Any group whose name contains' (with an empty text field), and 'Groups at' (with a dropdown menu showing 'at' and a text field showing 'netthreat.local'). An 'UNDO' button is to the right of the 'INCLUDE' section. At the bottom right are 'SAVE SELECTED' and 'CANCEL' buttons.

For this example, we are going to add the groups in to the SSLVPN Services group and test with NetExtender but you could add any groups to use with other services like the Global VPN Clients or use with SSO, Content Filtering etc.

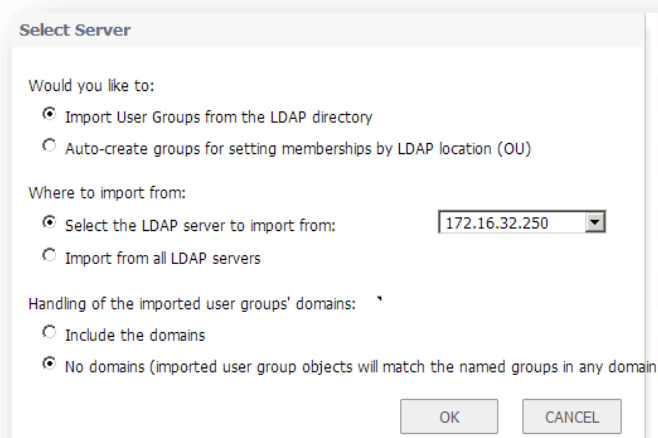
8. Adding the User Groups

Select the **SSLVPN Services** Group and edit. Then add the SSL VPN Users groups from both Domains.

Make sure in the VPN Access you have selected the desired Networks to access.



If you want to just use the one user group instead of two then import one of the groups from LDAP like below and select **No domains**.



☒ SSL VPN Users
☐ Terminal Server License Servers
☐ Users
☐ Windows Authorization Access Group

Filters:

☒ Selected user groups

☐ Any group whose contains

☐ Groups

ready

As you can see this will match both Domains. You can now add this to the SSLVPN Services or use for CFS etc.

Group Settings

☒ This can match a domain user group
 ☐ Members are set locally only

☐ Memberships are set by the user's location in the LDAP directory

Name:

Domain:

Comment:

LDAP Location:

☐ Require one-time passwords

9. Testing using NetExtender

If you are logging on with a username that is in both domains you need to enter the username followed by @domain.local or whatever your Domain is, see examples below.

We've used different passwords for each user from both Domains, just to check there isn't any password caching occurring.

SONICWALL | NetExtender

Server: 193.248.150.124:4433

Username: preston@Netthreat.local

Password:

Domain: LocalDomain

Connect

Save user name only if server allows

Log Details

General

Time	20:55:47 Mar 08
ID	1079
Category	SSL VPN
Group	General
Event	SSL VPN
Msg. Type	Simple Message String
Priority	Inform
Message	LDAP User preston@Netthreat.local login success through LDAP server
Src. Name	
Dst. Name	
Notes	

SONICWALL | NetExtender

Server: 193.248.150.124:4433

Username: preston@test.local

Password:

Domain: LocalDomain

Connect

Save user name only if server allows

Log Details

General

Time	21:01:58 Mar 08
ID	1079
Category	SSL VPN
Group	General
Event	SSL VPN
Msg. Type	Simple Message String
Priority	Inform
Message	LDAP User preston@test.local login success through LDAP server
Src. Name	
Dst. Name	
Notes	

If you are logging on with a username unique to that domain you can login just using the username and the Domain with that user will authenticate them. See examples below.

Server: 193.248.150.124:4433
 Username: izzy
 Password: ●●●●●●●●
 Domain: LocalDomain

Connect

Save user name only if server allows

Log Details

General

Time	21:07:52 Mar 08
ID	1080
Category	Users
Group	Authentication Access
Event	Successful SSL VPN User Login
Msg. Type	Standard String Service
Priority	Inform
Message	SSL VPN zone remote user login allowed
Src. Name	L'Puteaux-657-1-116-124.w193-248.abo.wanadoo.fr
Dst. Name	
Notes	izzy
User Name	izzy@test.local

Server: 193.248.150.124:4433
 Username: david
 Password: ●●●●●●●●
 Domain: LocalDomain

Connect

Save user name only if server allows

Log Details

General

Time	21:11:48 Mar 08
ID	1079
Category	SSL VPN
Group	General
Event	SSL VPN
Msg. Type	Simple Message String
Priority	Inform
Message	LDAP User david login success through LDAP server
Src. Name	
Dst. Name	
Notes	
User Name	david@netthreat.local