Example - Create a User Database with Active Directory

https://campus.barracuda.com/doc/2458451/

On the Barracuda SSL VPN, you can use an external Active Directory server for a user database. If you are using multiple user databases, on the Barracuda SSL VPN 380 or above, each user database manages its own authentication server configuration, so you can configure multiple Active Directory servers on the same unit. If you are using a Barracuda SSL VPN 180 or 280 you must edit the default user database to configure the Active Directory server.

Before you begin

Before you begin, verify that your Barracuda SSL VPN can reach your Microsoft Active Directory server. If you deployed your Barracuda SSL VPN in a DMZ, open the necessary ports for read or read/write access to your Active Directory server.

You also need the following information:

- Domain controller hostname
- Domain
- Service account name
- Service account password

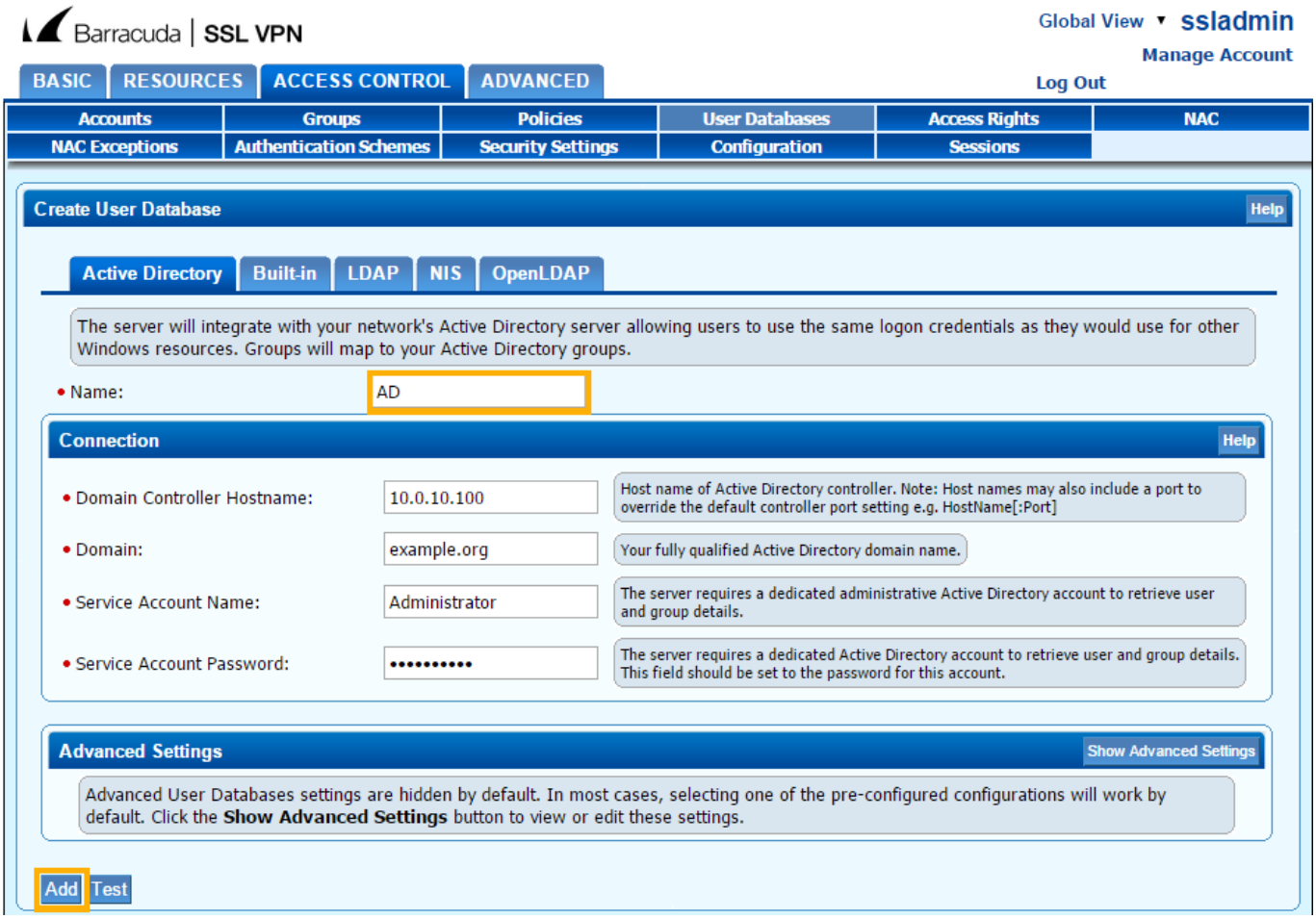
Configure the user database to use an Active Directory server

In the user database, provide the information required to connect with the Active Directory server.

1. Go to the **ACCESS CONTROL > User Databases** page.
2. In the **Create User Database** section, click the **Active Directory** tab.
3. In the **Connection** section, enter the following information:
   - **Domain Controller Hostname** – The name of the domain controller.
   - **Domain** – The domain.
   - **Service Account Name** – The user with permissions for read or read/write access to the Active Directory server. Write permissions must be configured in the Advanced Settings.
   - **Service Account Password** – The password for the user.
4. (Optional) Click **Show Advanced Settings** to configure Backup Domain Controller, SSL, read/write access, and OU Filters.
5. Click **Add**.

After you add the user database, it appears in the **User Databases** section on the bottom of the

page.


Barracuda | SSL VPN
Global View
ssladmin
Manage Account
Log Out
BASIC
RESOURCES
ACCESS CONTROL
ADVANCED
Accounts
Groups
Policies
User Databases
Access Rights
NAC
NAC Exceptions
Authentication Schemes
Security Settings
Configuration
Sessions
Create User Database
Help
Active Directory
Built-in
LDAP
NIS
OpenLDAP
The server will integrate with your network's Active Directory server allowing users to use the same logon credentials as they would use for other Windows resources. Groups will map to your Active Directory groups.
• Name:
AD
Connection
Help
• Domain Controller Hostname:
10.0.10.100
Host name of Active Directory controller. Note: Host names may also include a port to override the default controller port setting e.g. HostName[:Port]
• Domain:
example.org
Your fully qualified Active Directory domain name.
• Service Account Name:
Administrator
The server requires a dedicated administrative Active Directory account to retrieve user and group details.
• Service Account Password:
••••••••••
The server requires a dedicated Active Directory account to retrieve user and group details. This field should be set to the password for this account.
Advanced Settings
Show Advanced Settings
Advanced User Databases settings are hidden by default. In most cases, selecting one of the pre-configured configurations will work by default. Click the Show Advanced Settings button to view or edit these settings.
Add
Test

Figures

1. ad_db1.png