



## **NeoAccel SSL VPN-Plus (2.0)**

### **Active Directory Integration**

# Contents

<b>NEOACCEL SSL VPN-PLUS (2.0)</b> .....	<b>1</b>
<b>ACTIVE DIRECTORY INTEGRATION</b> .....	<b>1</b>
<b>INTRODUCTION</b> .....	<b>3</b>
PURPOSE.....	3
<b>PART-I: CONFIGURING AUTH SERVER</b> .....	<b>3</b>
STEP 1: ADD AUTH SERVER .....	3
STEP 2: CREATE MATCHING GROUP.....	4
STEP 3: APPLY AUTH SERVER .....	5
STEP 4: TEST AUTHENTICATION .....	5

# Introduction

## Purpose

Provide directions for integrating SSL VPN-Plus™ with Microsoft Active Directory.

## PART-I: Configuring Auth Server

Open the NeoAccel SSL VPN-Plus NMC and navigate to Users/Groups

### Step 1: Add Auth Server

Click on Add button in NMC to Add the Active Directory domain controller that you will be authenticating against. Select AD from drop down list.

The screenshot shows a window titled "Add Authentication Server" with a close button in the top right corner. Inside the window, there is a "Create Server" section with two sub-sections: "Basic Configuration" and "Advanced Configuration".

**Basic Configuration:**

- Server type: AD (dropdown menu)
- Server alias name: (empty text box)
- Server IP address: (empty text box with three dots)
- Server port: 389 (text box)
- Server timeout: 10 (text box) sec

**Advanced Configuration:**

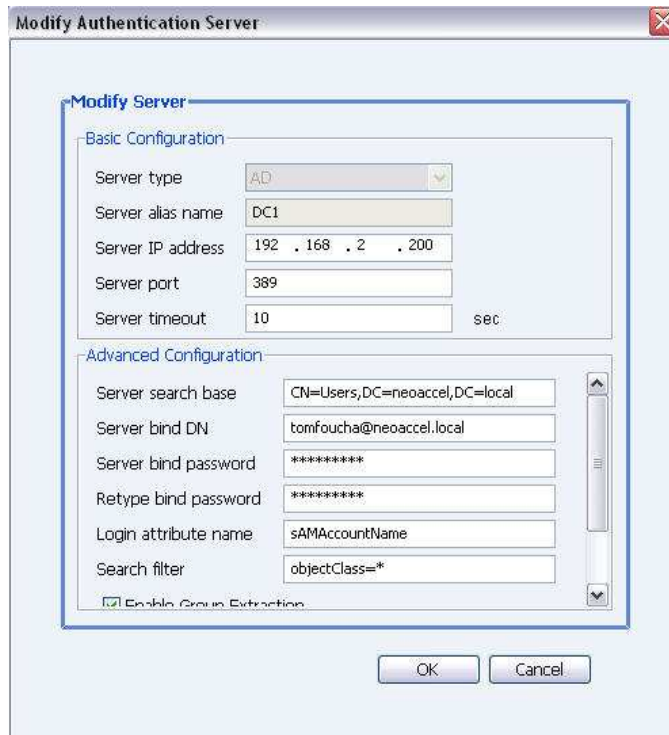
- Server search base: (empty text box)
- Server bind DN: (empty text box)
- Server bind password: (empty text box)
- Retype bind password: (empty text box)
- Login attribute name: sAMAccountName (text box)
- Search filter: objectClass=\* (text box)

At the bottom of the "Advanced Configuration" section, there is a checkbox labeled "Enable Group Extraction" which is checked. At the very bottom of the dialog are "OK" and "Cancel" buttons.

- a. provide Server alias name, this is simply descriptive text
- b. enter the IP Address of the AD Domain Controller
- c. Server port 389 is the standard LDAP port
- d. Server timeout is 10 sec. (no need to change in most cases)
- e. Server search base
  - a. This should be the full AD path where your user accounts are stored, example: CN=Users,DC=neoaccel,DC=com
- f. Server bind DN
  - a. Specify an account that has permissions to bind and read the directory structure in the form of [user@domain.com](#) (this is the UserPrincipalName setting)
- g. Enter the password for the above configured user in both places for verification

h. Click OK

## Completed example



## Step 2: Create matching Group

Using Active Directory Authentication does not require that users be configured on the SSL VPN-Plus gateway.

The SSL VPN-Plus will perform Group Extraction, as long as the Enable Group Extraction option is enabled in the gateway. This is the default configuration.

Either create a new group in Active Directory or use an existing group, enter that as a Group name under Users/Groups in the Group section.

We recommend that you create a group called VPNUUsers in Active Directory and assign those individuals that you want to use the SSL VPN. Next create a matching group on the SSL VPN gateway with the same name (case is important).

List of Groups		
Group Name	Group Policy	Group Users
default_group	deny-all	
Fulltunnel		tomtest
VPNUUsers	deny-rdp	
VPNAdmin		sandeep
VPNIndia		

You may create multiple groups in AD and the gateway and assign different Network Policies and Portal Configurations to those groups.

### **Step 3: Apply Auth Server**

Open NMC and go to SSL VPN-Plus, Gateways, select your gateway and click Modify. On the Authentication tab add the newly created Active Directory Authentication server and adjust the priority so that this server is a lower priority than other servers.

### **Step 4: Test Authentication**

Test logging in using the Active Directory username and password. It is NOT necessary to use domain\username.

Helpful resources

LDAP Browser from Softerra

<http://www.ldapbrowser.com/download/index.php>