Using Microsoft Active Directory for Checkpoint NG AI SecureClient

Dave Crowfoot
www.works4me.com
dave@works4me.com

This is the solution that I came up with to utilize MS Active directory to authenticate SecureClient users.

I do not extend the AD schema or use radius for this solution.

I do not use SmartDashboard to administer my AD users. I do not like the way it handles user maintenance and without extending the schema it doesn't work that well anyway. I only use the MS tools for this.

Environment used to create and test solution:

Compaq Proliant ML530
SecurePlatform NG AI
VPN-1 / FW-1 NG AI
Separate Management and Enforcement Point
Simplified Mode for policies

If you have any questions about this solution, please feel free to email at the above address

And as always, this works 4 me.

First I created a security group in Users called **VPN-Users** in the AD
cn=VPN-Users,cn=Users,dc=xxxx,dc=yyy

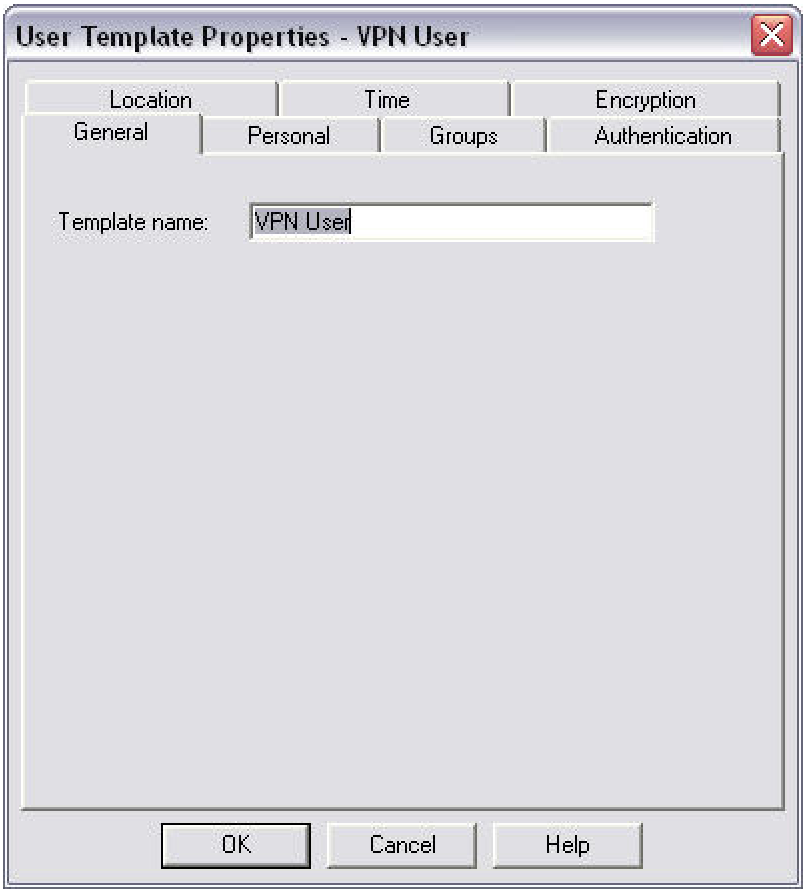
This is an AD group that I put all my allowed VPN users into. Also, this group serves as the one that maintains the amount of SecureClient licenses you own.

In SmartDashboard:

Go to the Policy Menu / Global Properties
From the **LDAP Account Management branch**, select **Use LDAP**, click OK

Create a host for your Active Directory Server: **MSADSrv**

Go to the **Users Icon**
Right click Templates and select New Template
(General Tab)
Template Name: **VPN User**

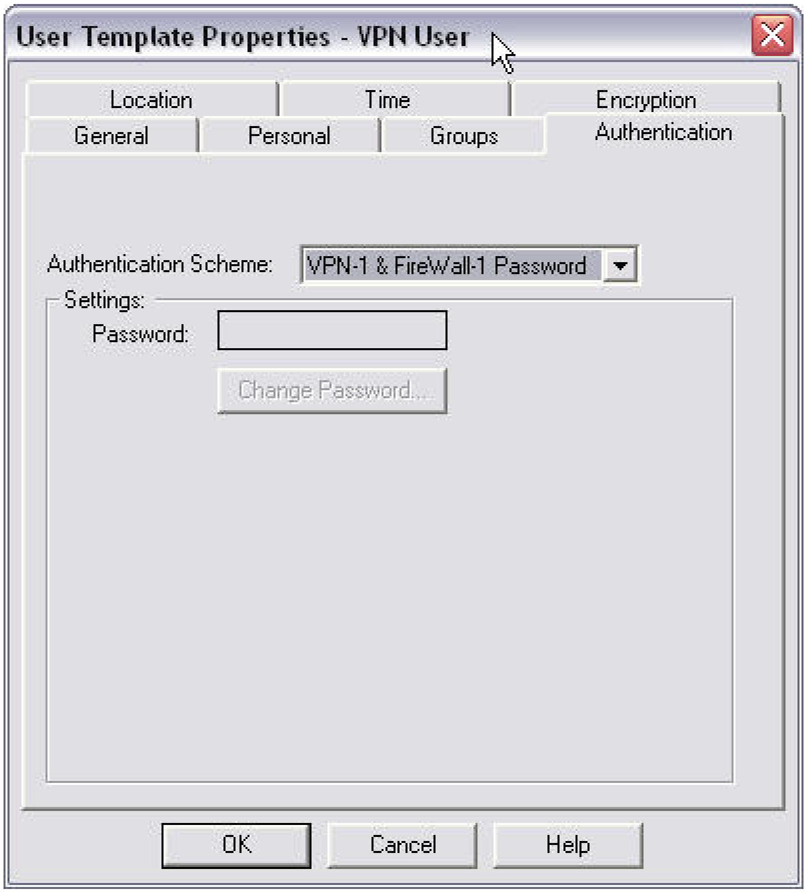


Template name: VPN User

(Authentication Tab)

Authentication Scheme: **VPN-1 & Firewall-1 Password**

Click OK



User Template Properties - VPN User

Authentication Scheme: VPN-1 & FireWall-1 Password

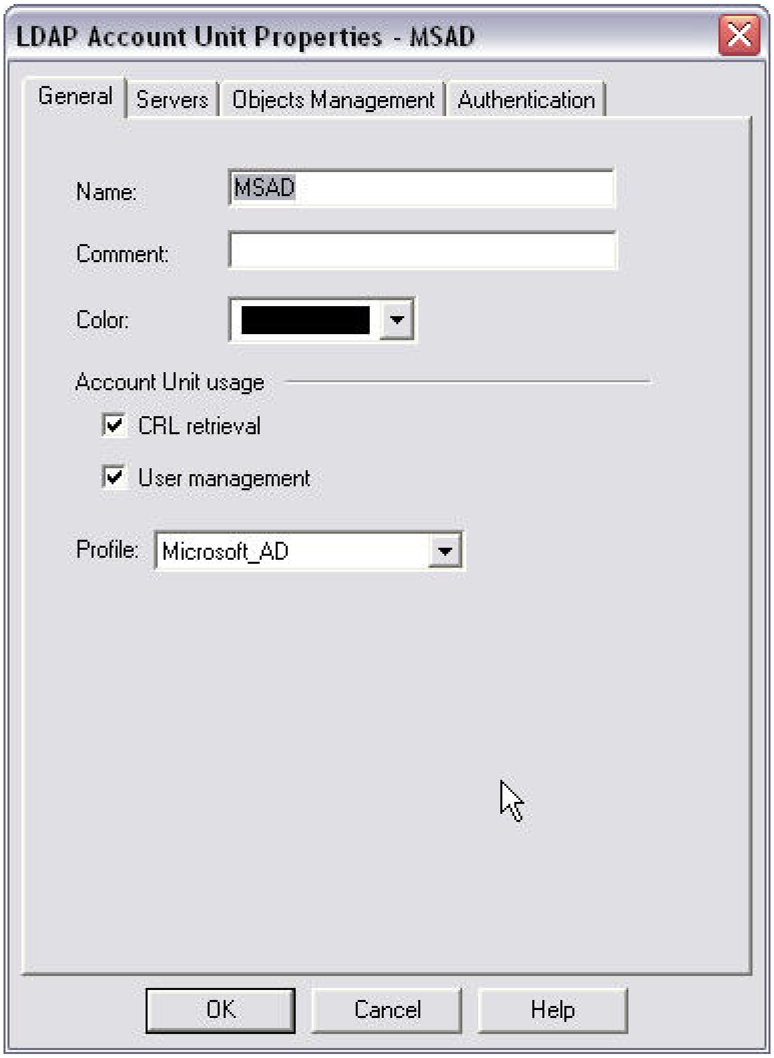
Settings:

Password:

Go to Manage Menu / Servers. Create a LDAP Account Unit object.

(General Tab)

Give it a name, i.e., **MSAD**
Check both boxes, **CRL retrieval** and **User management**
Set Profile to **Microsoft_AD**



LDAP Account Unit Properties - MSAD

Name: MSAD

Comment:

Color:

Account Unit usage

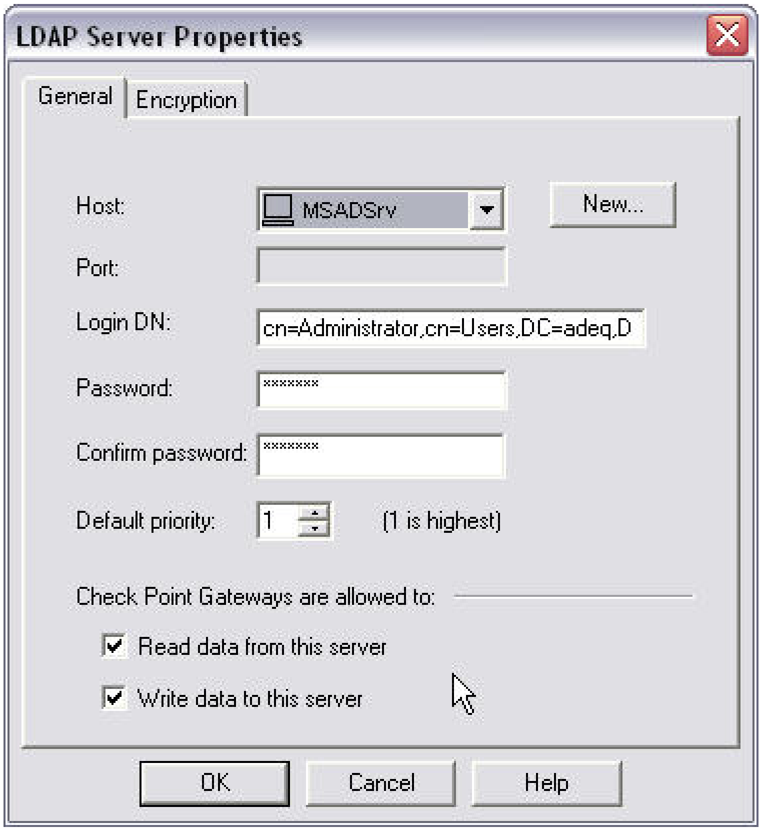
☑ CRL retrieval

☑ User management

Profile: Microsoft_AD

(Servers Tab)

Click Add
Choose the host that represents your AD Domain controller
Leave Port at 389
Login DN: cn=Administrator,cn=Users,dc=xxxx,dc=yyy
Enter administrator password twice
Check both boxes, **Read data from this server**, **Write data to this server**



Host: MSADSrv

Port:

Login DN: cn=Administrator,cn=Users,DC=adeq,D

Password: *******

Confirm password: *******

Default priority: 1 (1 is highest)

Check Point Gateways are allowed to:

☑ Read data from this server

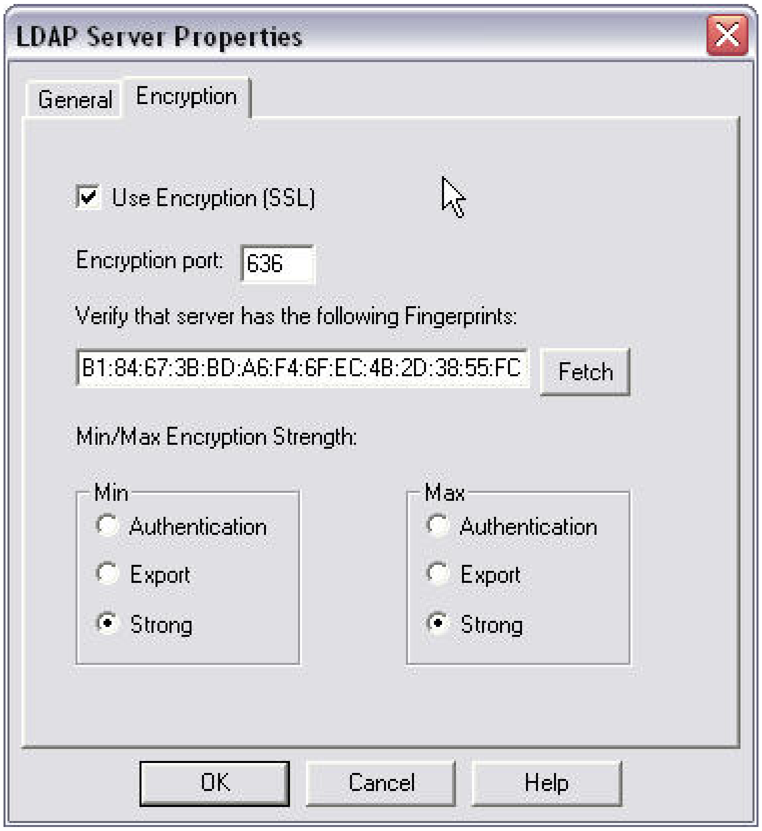
☑ Write data to this server

(Servers Tab / Encryption Tab)

Check **Use SSL**

Click **Fetch** for Fingerprint

Set Encryption to **strong** and **strong** for Min and Max



LDAP Server Properties

General | Encryption

☑ Use Encryption (SSL)

Encryption port: 636

Verify that server has the following Fingerprints:

B1:84:67:3B:BD:A6:F4:6F:EC:4B:2D:38:55:FC

Min/Max Encryption Strength:

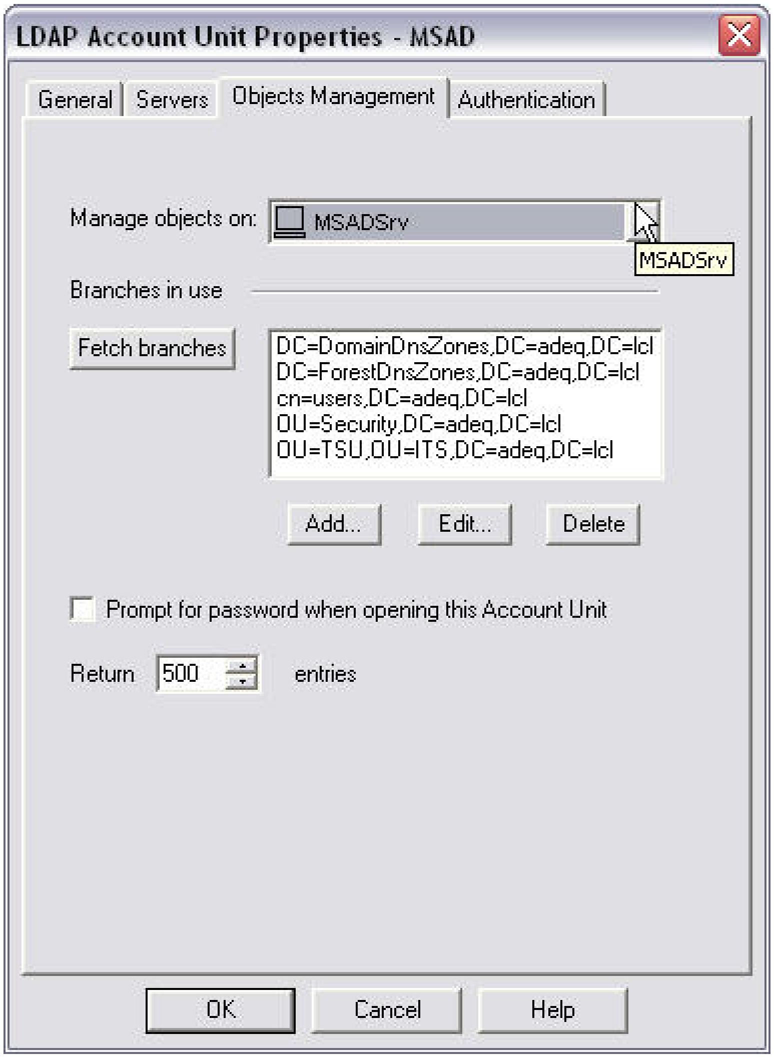
Min
○ Authentication
○ Export
● Strong

Max
○ Authentication
○ Export
● Strong

(Objects Management)

Select your AD object and fetch the branch
Click OK

Note: Active Directory only returns 'cn=users,dc=x" wher ex is the AD domain. When users are defined under separate organizational untis those units should Be manually added as branches. When doing so, they ***MUST*** *be in the format of OU=yyy,OU=yyy,DC=xxxx,DC=zzzz*



Manage objects on: MSADSrv

Branches in use

DC=DomainDnsZones,DC=adeq,DC=lcl
DC=ForestDnsZones,DC=adeq,DC=lcl
cn=users,DC=adeq,DC=lcl
OU=Security,DC=adeq,DC=lcl
OU=TSU,OU=ITS,DC=adeq,DC=lcl

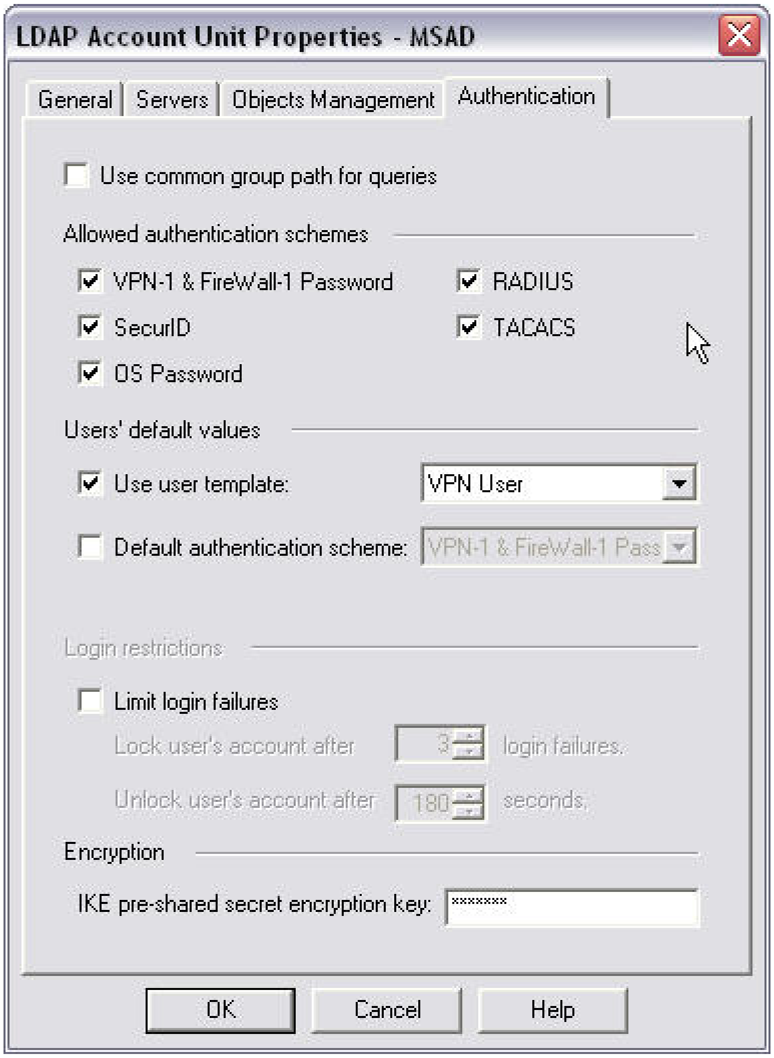
□ Prompt for password when opening this Account Unit

Return 500 entries

(Authentication)

Use user template: **VPN User**

IKE pre-shared secret encryption key: **AD Administrator password**



□ Use common group path for queries

Allowed authentication schemes

☑ VPN-1 & FireWall-1 Password ☑ RADIUS

☑ SecurID ☑ TACACS

☑ OS Password

Users' default values

☑ Use user template: VPN User

□ Default authentication scheme: VPN-1 & FireWall-1 Pass

Login restrictions

□ Limit login failures

Lock user's account after 3 login failures.

Unlock user's account after 180 seconds.

Encryption

IKE pre-shared secret encryption key: ********

Go to the **Users Icon**

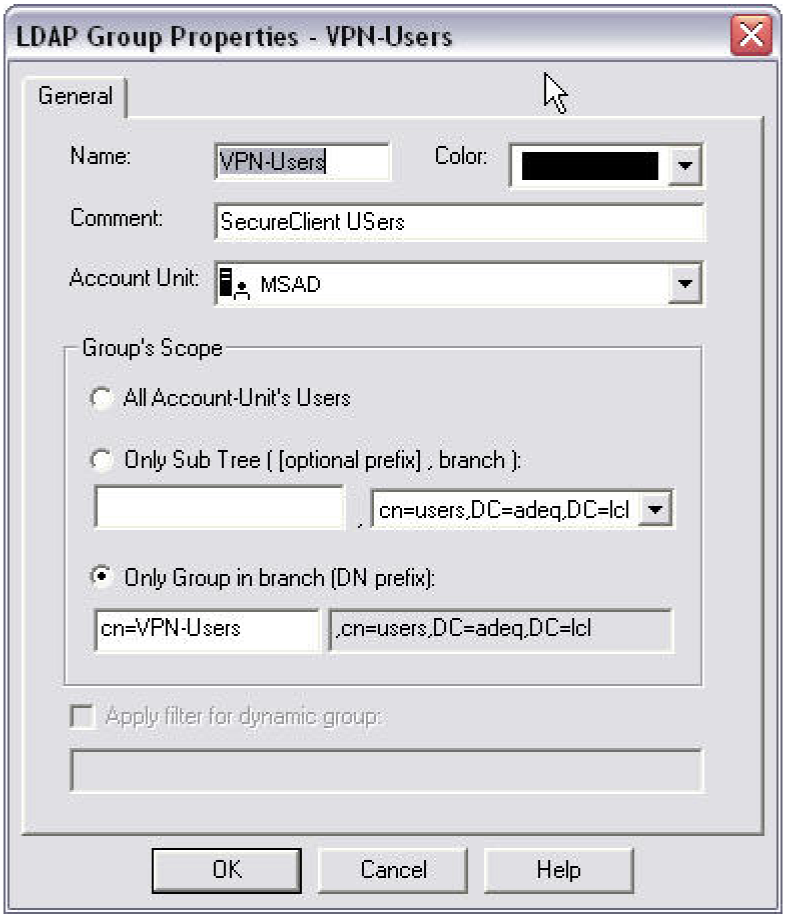
Right click on **LDAP Groups** and select **New LDAP Group**
Enter a name: **VPN-Users**
Select the account unit you created: **MSAD**

Group's Scope
First, select **Only Sub Tree** and select, cn=users,DC=xxxx,DC=yyy

Note: This has to be done first because it is the only way I found to make the next step work correctly.

Second, select **Only Group in branch** and put **cn=VPN-Users**

Note: This LDAP group will be used in the source of the ***Remote Access rule(s)***



LDAP Group Properties - VPN-Users

General

Name: VPN-Users
Color: ■
Comment: SecureClient USers
Account Unit: MSAD

Group's Scope

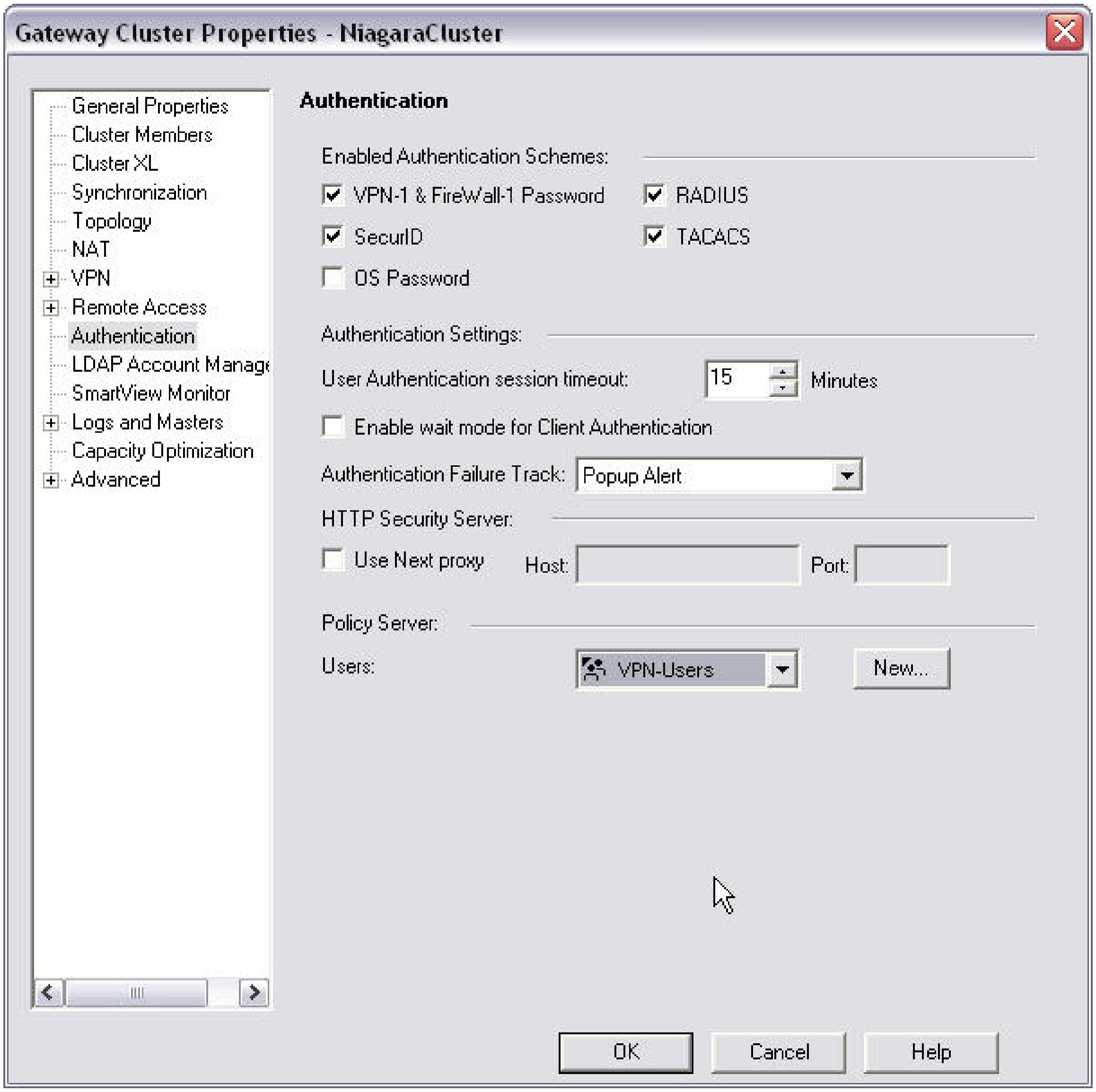
○ All Account-Unit's Users

○ Only Sub Tree ([optional prefix] , branch): , cn=users,DC=adeq,DC=lcl

● Only Group in branch (DN prefix): cn=VPN-Users ,cn=users,DC=adeq,DC=lcl

□ Apply filter for dynamic group:

Open your VPN-1 gateway object and click on the **Authentication** branch and set the Policy Server Users group to **VPN-Users**



Authentication

Enabled Authentication Schemes:

☑ VPN-1 & FireWall-1 Password ☑ RADIUS

☑ SecurID ☑ TACACS

☐ OS Password

Authentication Settings:

User Authentication session timeout: 15 Minutes

☐ Enable wait mode for Client Authentication

Authentication Failure Track: Popup Alert

HTTP Security Server:

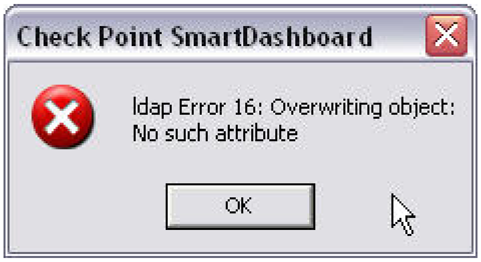
☐ Use Next proxy Host: Port:

Policy Server:

Users: VPN-Users New...

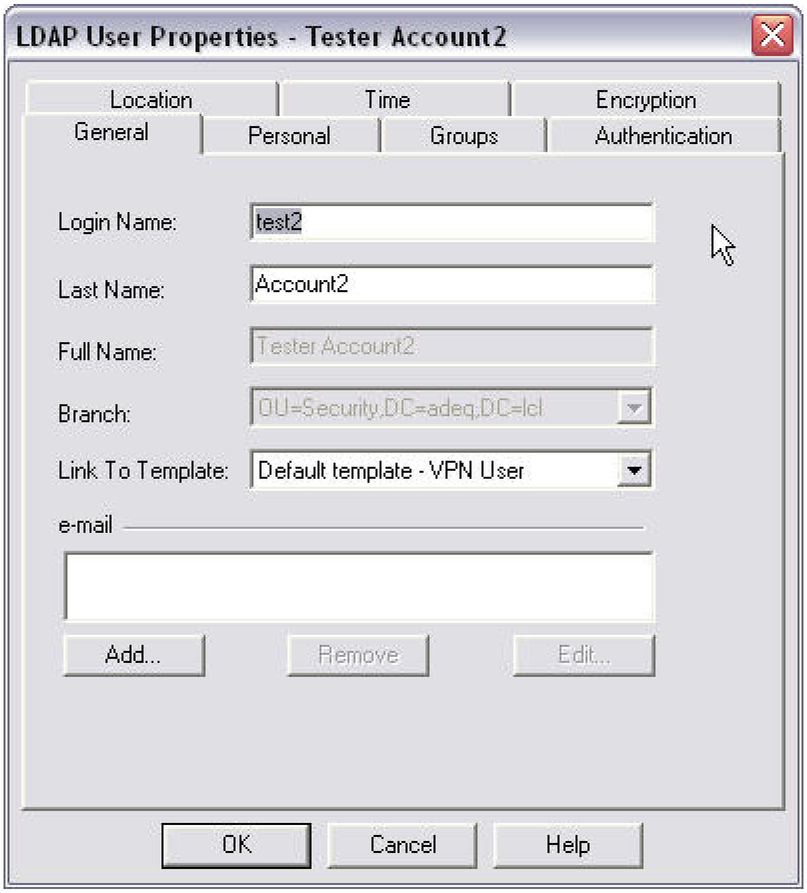
You can check the properties of a LDAP user by double clicking a user in the LDAP Account Unit. When using MS AD, the template is defined using **VPN-1 & Firewall-1 Password**

If you click OK on these screens, you might get the following because the MS Schema has not been extended. This is why I do not use these tools for user maintenance.



Check Point SmartDashboard

ldap Error 16: Overwriting object:
No such attribute



LDAP User Properties - Tester Account2

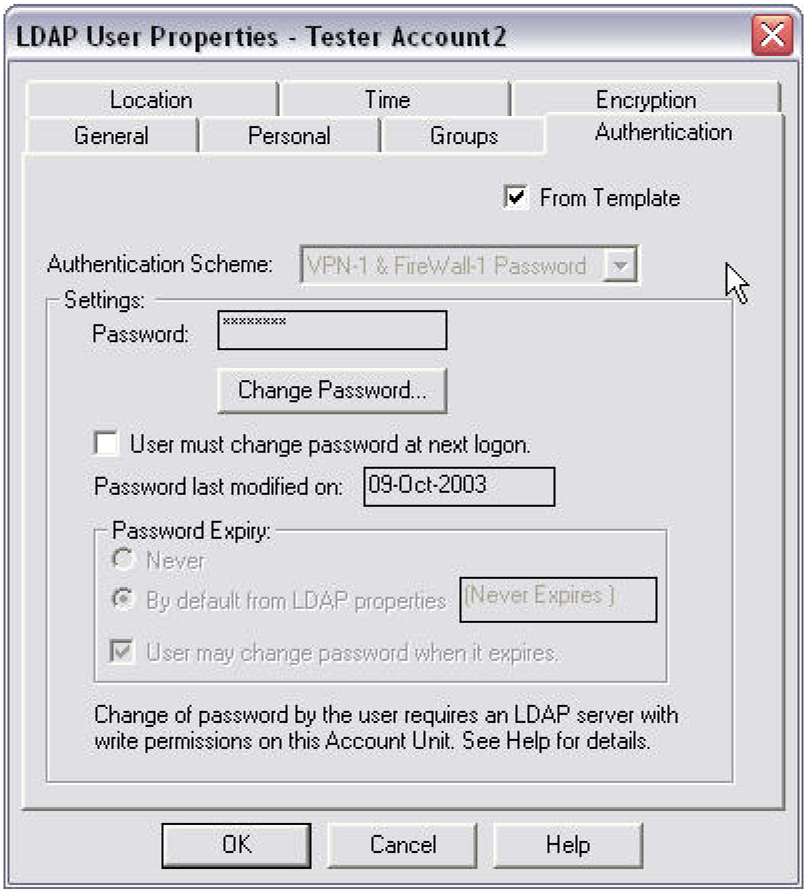
Login Name: test2

Last Name: Account2

Full Name: Tester Account2

Branch: OU=Security,DC=adeq,DC=lcl

Link To Template: Default template - VPN User



☑ From Template

Authentication Scheme: VPN-1 & FireWall-1 Password

Settings:

Password: *********

□ User must change password at next logon.

Password last modified on: 09-Oct-2003

Password Expiry:

○ Never

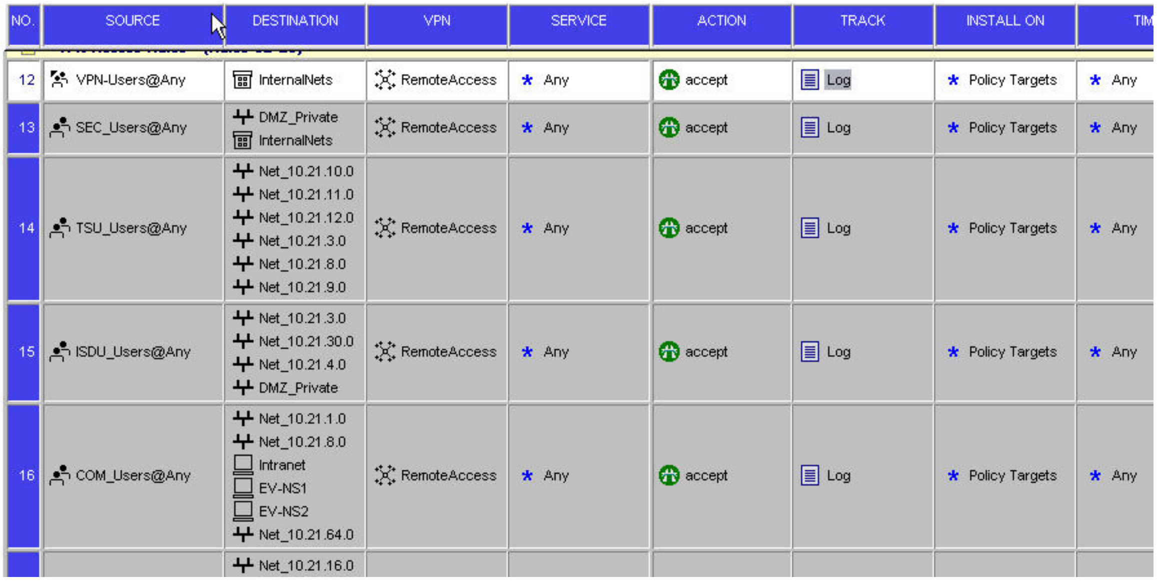
● By default from LDAP properties (Never Expires)

☑ User may change password when it expires.

Change of password by the user requires an LDAP server with write permissions on this Account Unit. See Help for details.

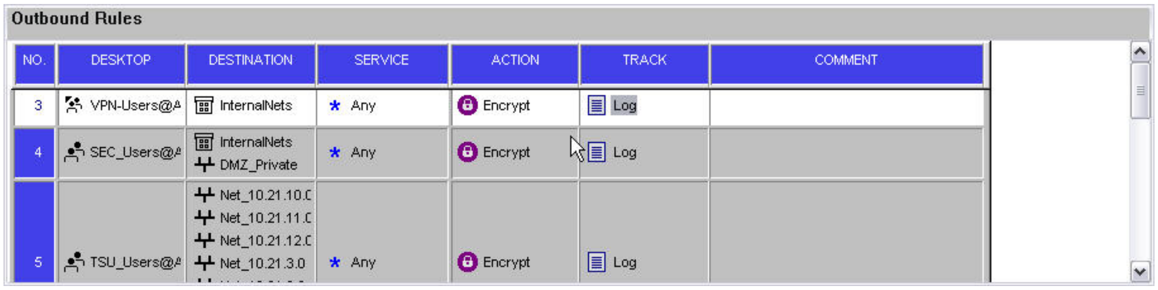
When creating Remote Access rules, you use the LDAP Group **VPN-Users**

Security



NO.	SOURCE	DESTINATION	VPN	SERVICE	ACTION	TRACK	INSTALL ON	TIM
12	VPN-Users@Any	InternalNets	RemoteAccess	* Any	accept	Log	* Policy Targets	* Any
13	SEC_Users@Any	DMZ_Private InternalNets	RemoteAccess	* Any	accept	Log	* Policy Targets	* Any
14	TSU_Users@Any	Net_10.21.10.0 Net_10.21.11.0 Net_10.21.12.0 Net_10.21.3.0 Net_10.21.8.0 Net_10.21.9.0	RemoteAccess	* Any	accept	Log	* Policy Targets	* Any
15	ISDU_Users@Any	Net_10.21.3.0 Net_10.21.30.0 Net_10.21.4.0 DMZ_Private	RemoteAccess	* Any	accept	Log	* Policy Targets	* Any
16	COM_Users@Any	Net_10.21.1.0 Net_10.21.8.0 Intranet EV-NS1 EV-NS2 Net_10.21.64.0	RemoteAccess	* Any	accept	Log	* Policy Targets	* Any
		Net_10.21.16.0						

Desktop Security



Outbound Rules

NO.	DESKTOP	DESTINATION	SERVICE	ACTION	TRACK	COMMENT
3	VPN-Users@A	InternalNets	* Any	Encrypt	Log	
4	SEC_Users@A	InternalNets DMZ_Private	* Any	Encrypt	Log	
5	TSU_Users@A	Net_10.21.10.C Net_10.21.11.C Net_10.21.12.C Net_10.21.3.0	* Any	Encrypt	Log	

In closing, the important notes are:

1. The MS AD group **VPN-Users MUST** contain all the users that you wish to allow VPN access too regardless of what resources that you wish them to access.

2. The LDAP group **VPN-Users** is associated with the Policy Server in the Gateway properties.

3. You can add more LDAP groups that are associated with MS AD groups for more granular control over with resources your users have access to. This is what you see in the rules figures above.

4. Using this method of authentication and access control, you never use Checkpoint Groups only LDAP Groups.