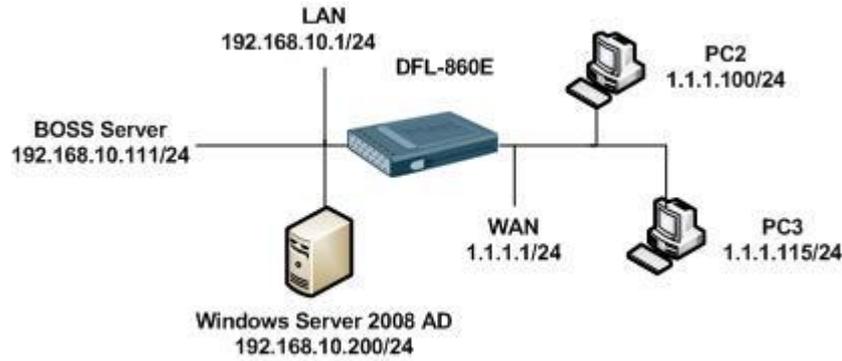


How to setup DFL PPTP authentication with Windows Server 2008 LDAP

[Topology]



Windows Server 2008 AD information

Domain: test.com

Group: boss, other,

Users: test in boss group and test2 in other group.

[DFL-860 Setup]

1. Objects > Address Book

#	Name	Address	User Auth Groups	Comments
1	InterfaceAddresses			
2	all-nets	0.0.0.0/0		All possible networks
3	pptp-ip	10.10.10.1		
4	pptp-pool	10.10.10.10-10.10.10.20		
5	to-boss-server	192.168.10.111		
6	to-ad	192.168.10.200		
7	pptp-auth-boss-group	10.10.10.10-10.10.10.20	boss	
8	pptp-auth-other-group	10.10.10.10-10.10.10.20	other	

2. Interfaces > PPTP/LTP Servers

#	Name	Tunnel protocol	Inner IP address	Outer interface	IP pool	Outer server IP	Comments
1	pptp-if	pptp	pptp-ip	wan1	pptp-pool	wan1_ip	

IP Pool

IPPool:

3. User Authentication > External User Databases

IP Address: Windows Server 2008 IP

Name Attribute: SAMAccountName

Base Object: DC=test, DC=com <Setup your domain here>

Administrator Account: administrator@test.com <Setup your domain administrator account>

Password: Setup your domain administrator password

Password Attribute: Description

ldap-2008
External LDAP server used to verify user names and passwords.

General

General

Name:

IP Address:

Port:

Timeout: seconds

Name Attribute:

Retrieve Group Membership

Membership Attribute:

Use Domain Name:

Database Settings

Base Object:

Administrator Account:

Password: Note! Existing passwords will always be shown with 8 characters to hide the actual length.

Confirm Password:

Domain Name:

Optional

Password Attribute:

Comments

Comments:

OK Cancel

4. User Authentication > User Authentication Rules

#	Name	Authentication agent	Authentication source	Interface	Comments
1	ptp-auth-rule	ppp	LDAP	pptp-if	

General | Log Settings | Authentication Options | Accounting | Agent Options | Restrictions

General

Name:

Authentication agent:

Authentication Source:

Interface:

Originator IP:

Terminator IP:

For XAuth and PPP, this is the tunnel originator IP.

Comments

Comments:

OK Cancel

LDAP servers

Available

Selected

>> <<<

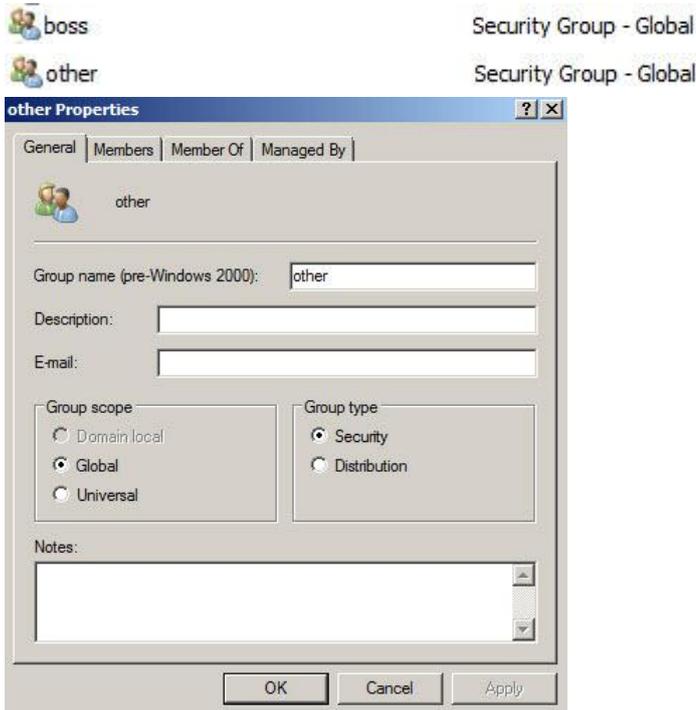
Move up Move down

5. Rules > IP Rules

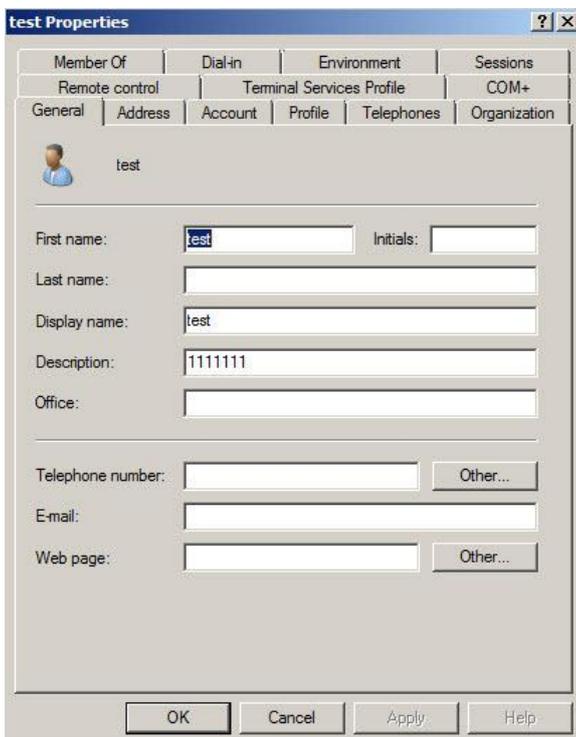
2		pptp-boss-in		Allow		pptp-if		pptp-auth-boss-group		lan		to-boss-server		all_services
3		pptp-user-in		Allow		pptp-if		pptp-auth-other-group		lan		to-ad		all_services

[Windows Server 2008 Setup]

1. Create Boss and other group

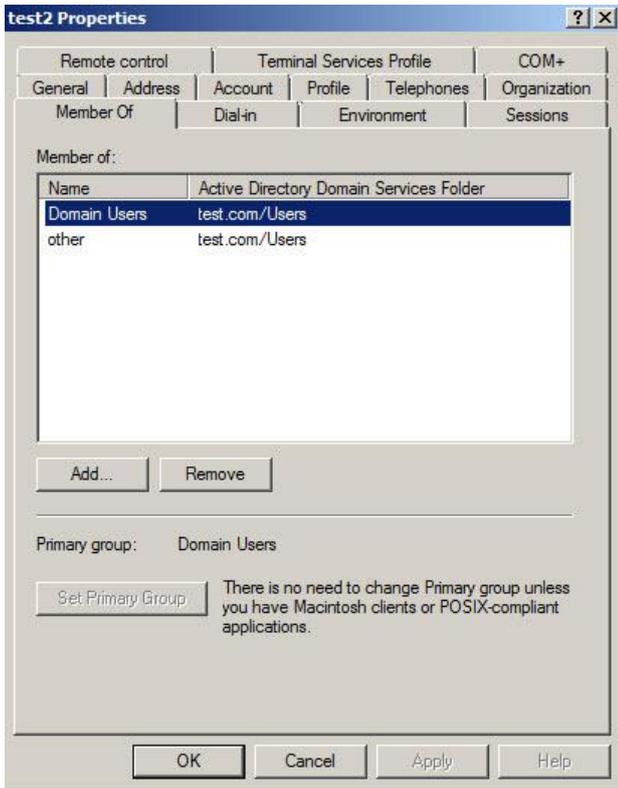


2. Setup user Description



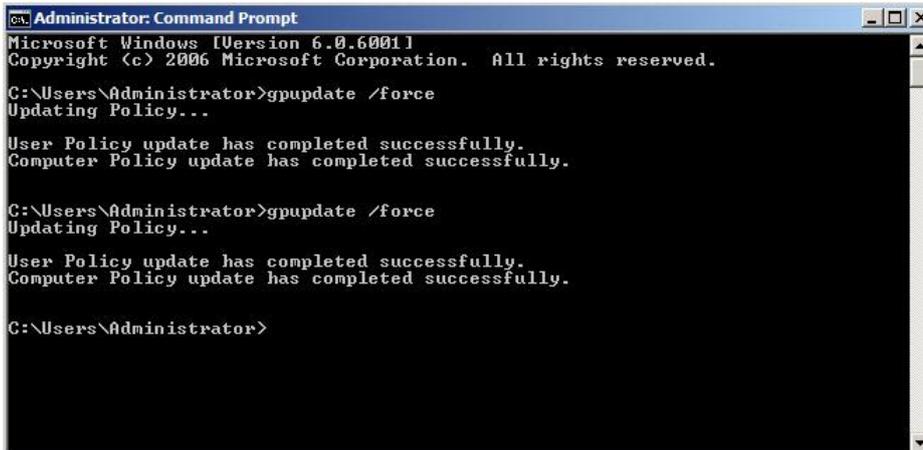
This setup is use for user dial-in password.
In this picture we setup 1111111 in user description.
This is user dial-in password.

3. Setup test in the Boss group and setup test2 in the other group.



Please set the "Domain Users" in the Primary Group.

4. Use cmd and run administrator and type in gpupdate /force to update the group policy.



[Test Result]

1. When test accounts dial-in it only can access boss server. (192.168.10.111)
2. When test2 accounts dial-in it only can access AD server. (192.168.10.200)

END