eDirectory and LDAP Autheentication

With the release of PANOS 3.1 there are now have several new methods of identifying users. This document will cover configuring transparent eDirectory User-ID and LDAP authentication as they are closely related.

Novell's eDirectory is a directory service that fully supports LDAP queries. A useful feature of eDirectory is that when a user authenticates to it the source IP address and login time is stored in the directory in the fields: ***networkAddress*** (in binary) and ***loginTime***. A new User-ID agent was developed to be able to read this information so that we can transparently map users to their IP addresses.

One major difference between this agent and our Active Directory agent is that it does not handle pushing group information it merely maps users to IP addresses. Our new LDAP support in PANOS is used to query the directory, build list of groups for policies and map users to groups. Because of this, part of the process of implementing eDirectory support is configuring LDAP information on the PAN device.

Before we cover configuration lets do an overview on LDAP.

Overview of the Lightweight Directory Access Protocol

Before we get into the actual configuration of the SA, it is helpful to go over some basic information about LDAP.

Lightweight Directory Access Protocol (LDAP) is an open standard for providing directory services via IP networks. LDAP is based upon X.500, the OSI Directory Access Protocol, and was first described in RFC1487. The most recent version (version 3) is described in RFC2251.

There are two main components to an LDAP database that we must understand in order to use it for authentication, its structure and its contents.

LDAP is a hierarchical database structure that lends itself to defining organizations and their structures. It is incredibly flexible is design, because of this each organization's LDAP structure will differ.

The contents of the directory are defined in its schema that is highly extensible. Users can modify the database design to meet their needs. The directory schema defines the possible database objects and attributes that they can possess.

When viewing a directory, it is common to view it as a collection of container objects (organizations, organizational units) and leaf objects (people, computers).

RFC 2377 defines the basic schema for directory-enabled applications. Following is a list of some of the ones that are important to us.

Terminology

rdn Relative distinguished name is the name of an object without reference to its place within the tree. It is often based upon the object's common name.

dn Distinguished Name is the name that defines an object by indicating its location within the directory hierarchy. It is created by concatenating the relative distinguished names of the object and each of its ancestors up to the root of the directory partition. This name is unique across the entire directory

cn Common Name is typically used to reference objects, as it is an attribute that all leaf objects possess. The common name need only be unique within its own container (so it is possible to have two objects with the cn of Bob as long as they are in separate containers. This attribute can contain the users login name.

o Organization is many times the root of a directory. Below the organization will be the various organizational units, groups, and members. eDirectory uses this as the base of its structure.

ou Organizational Unit is used to help define the structure of the organization A directory can be comprised of multiple organizational units on any level of the tree.

dc Domain Component defines the top level portions of the directory and is based upon the organization's DNS domain name.

member Attribute of a group object that contains all of the members of a group. The SA uses this attribute to determine if a user is in a static group.

sAMAccountName This is the logon name used to support clients and servers from previous versions of Windows. Note that the sAMAccountName should be less than 20 characters to support these clients. This maps to the user login name.

One other term we will find useful is "base DN". Each directory is required to provide basic directory specific information so that clients can access them. One of these attributes is the list of base distinguished names (DN) that you can access on this server. Typically the base DN will be the various domain components of the directory.

When we are specifically working with Active Directory we have an additional challenge. Using the tools available on an Active Directory server, we can view the structure of the directory; however, it is not represented in LDAP format with fully qualified distinguished names. We need this information when configuring the Palo Alto Firewall; it is therefore helpful to use an LDAP browser when trying to setup LDAP authentication.

LDAP Browsers

Softerra LDAP Administrator is an excellent LDAP tool for Windows. It can be found at: http://www.ldapadministrator.com/.

JXplorer is a free Java based browser that works on Windows, Mac and Linux. It can be found at: http://jxplorer.org/.

With this basic information we can move to configuration. First we will cover setting up the new User-ID agent for eDirectory. Then we will cover the LDAP integration. Finally we will cover using LDAP with Active Directory for things like Captive Portal, SSL VPN or Administrative Access.

eDirectory User Identification

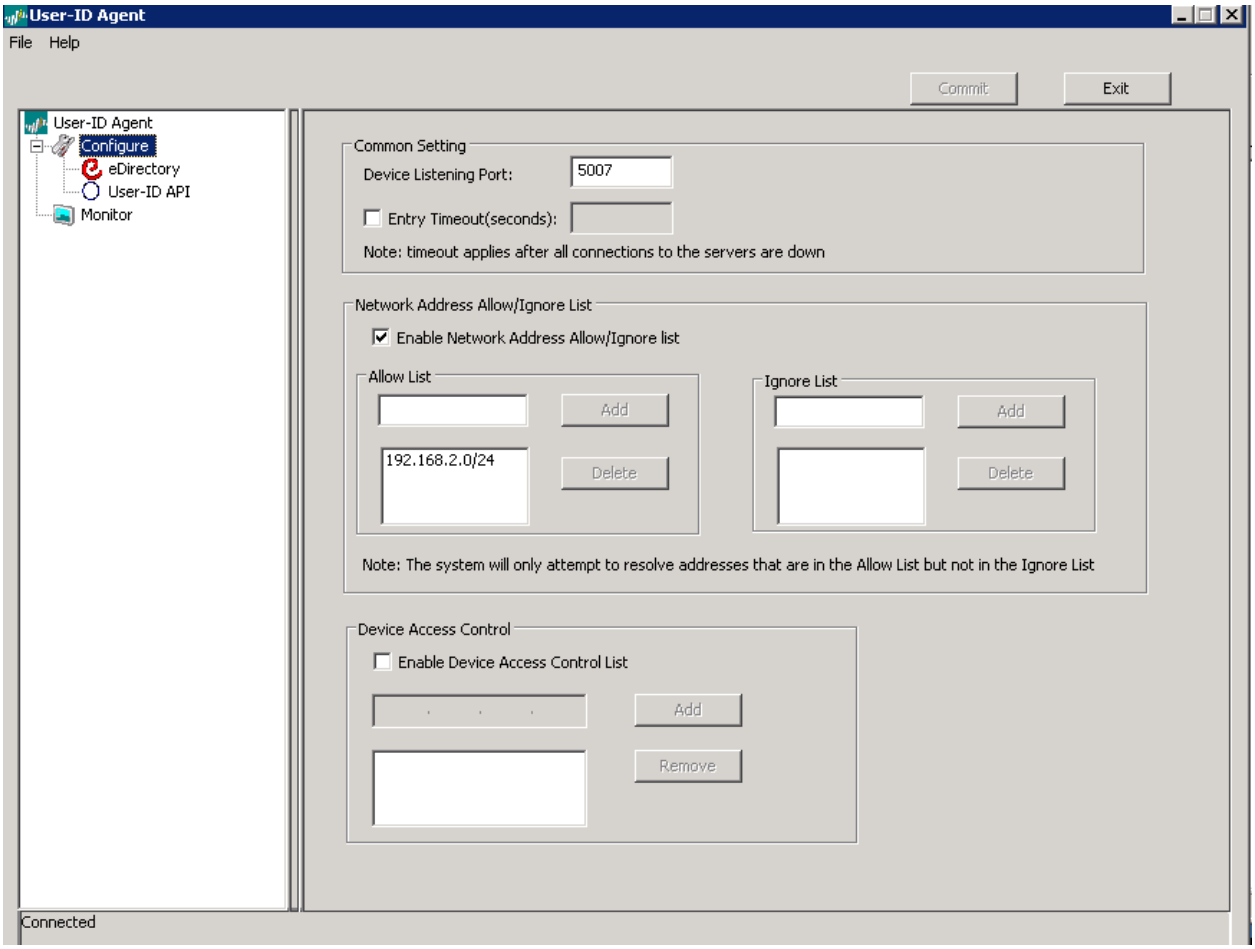
First we need to install the new User-ID agent. Login to your account at: https://support.paloaltonetworks.com. Go to the Software section and then find User Identification Agent section. You are looking for a version that ends in "-LDAP".

User Identification Agent

Version	Release Date	Release Notes	Download	Size	MD5
3.1.0-LDAP	15 Mar 10	PANOS-3.1.0-RN-revA.pdf	Download	970 KB	Show MD5

Download this to the server where the agent will run, it will run as a local service. Then follow the prompts for installation.

Once installed launch the User-ID Agent and select Configure. You will need to set a listening port and you will want to enable the Network Address Allow/Ignore list. Here you will add the networks for which you will be performing user identification.



Next we need to configure our eDirectory settings. Select the eDirectory icon, then in the Server field you will enter the IP address of the eDirectory server you will be monitoring and hit "**Add**". Note that many of the fields are already pre-populated but you will need to complete the following:

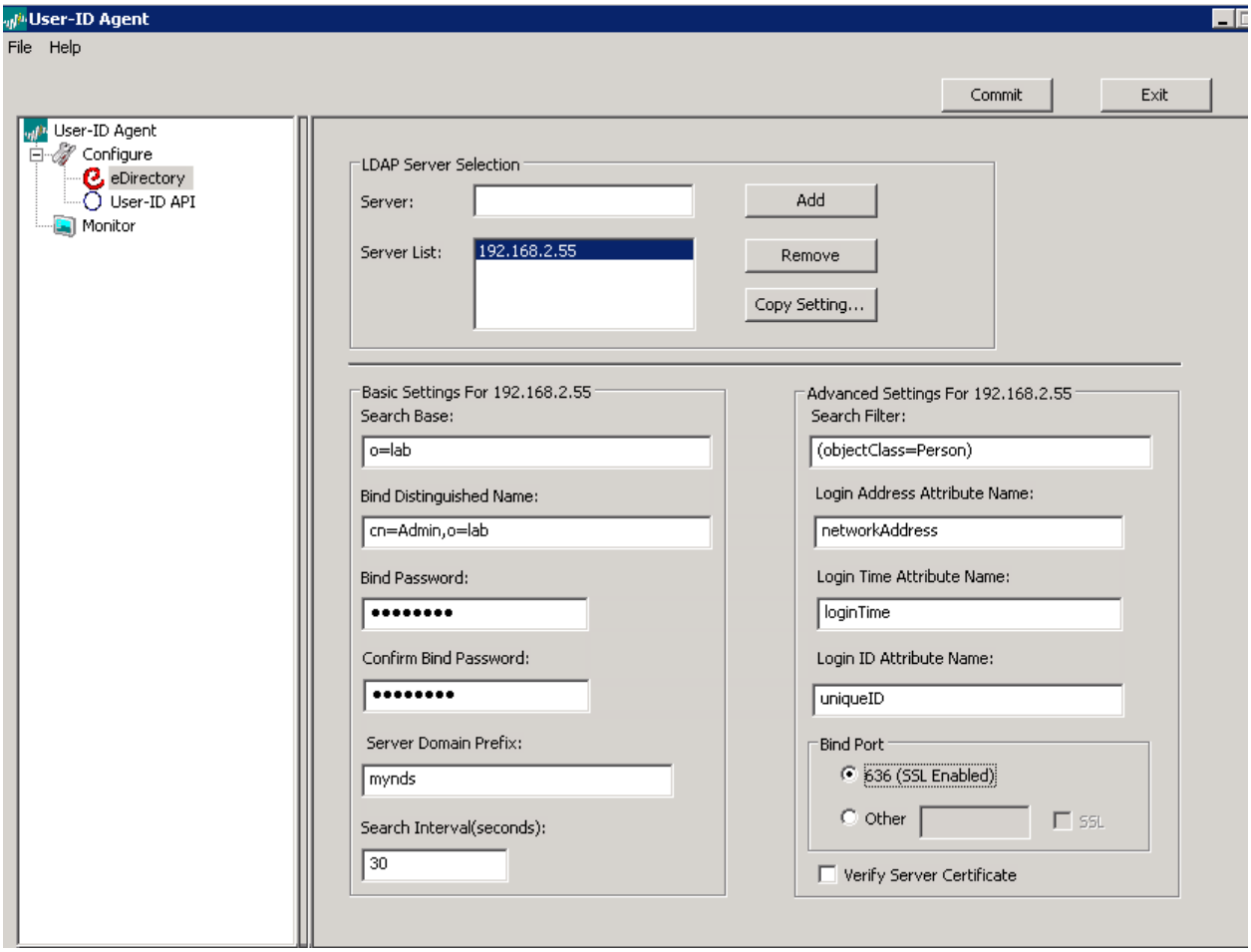
Search Base This is the base DN (or root) of the directory where the agent will look for users. In a very large deployment you can scope how much of the directory is searched by setting the search base appropriately.

Bind Distinguished Name This is the fully distinguished name (FQDN) of the user you will use to query eDirectory. This account does not need any special privileges.

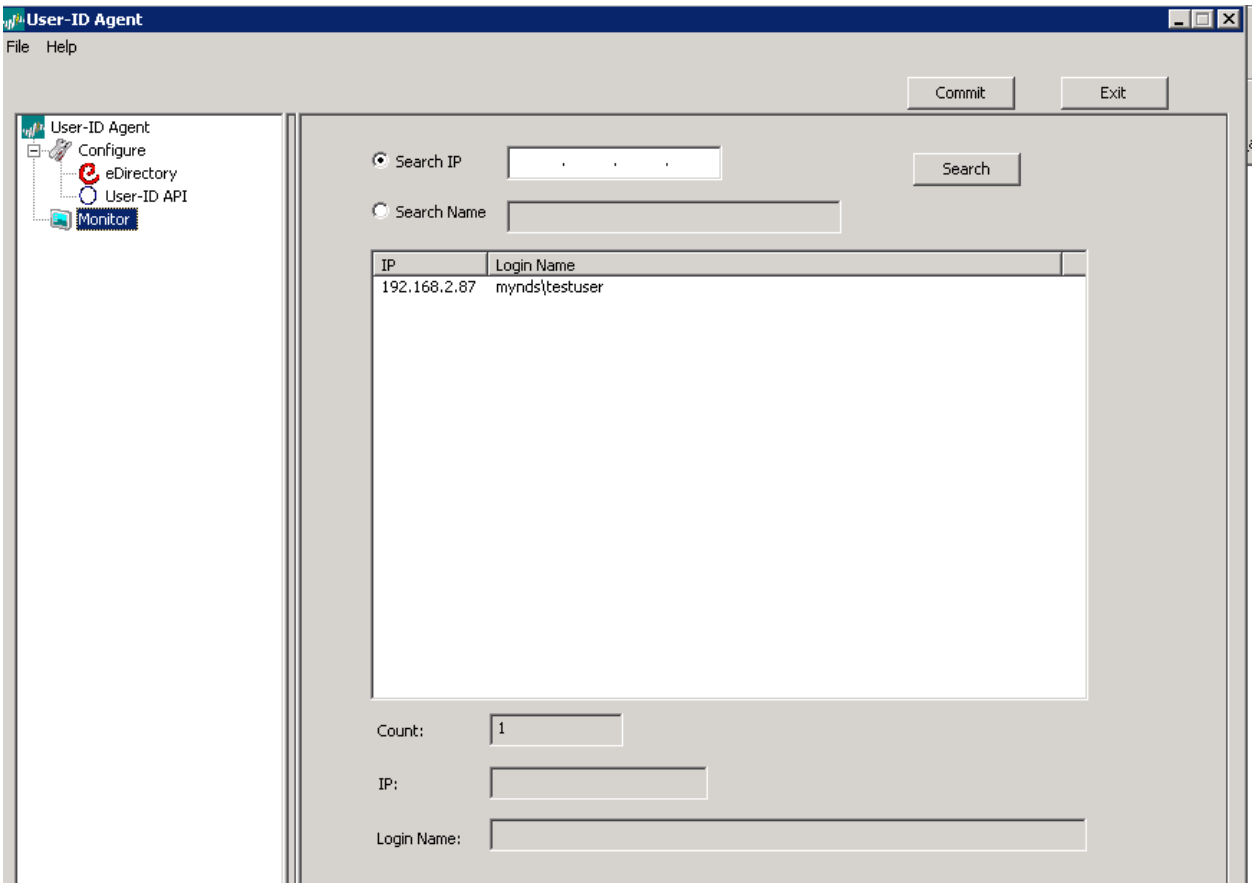
You will need to enter and reenter the password for the account you will be using. The only other field you may want to set is:

Server Domain Prefix This will be pre-pended to the user name and can be useful if you are using multiple authentication sources. In our example users would show up in the traffic logs as: mynds\username.

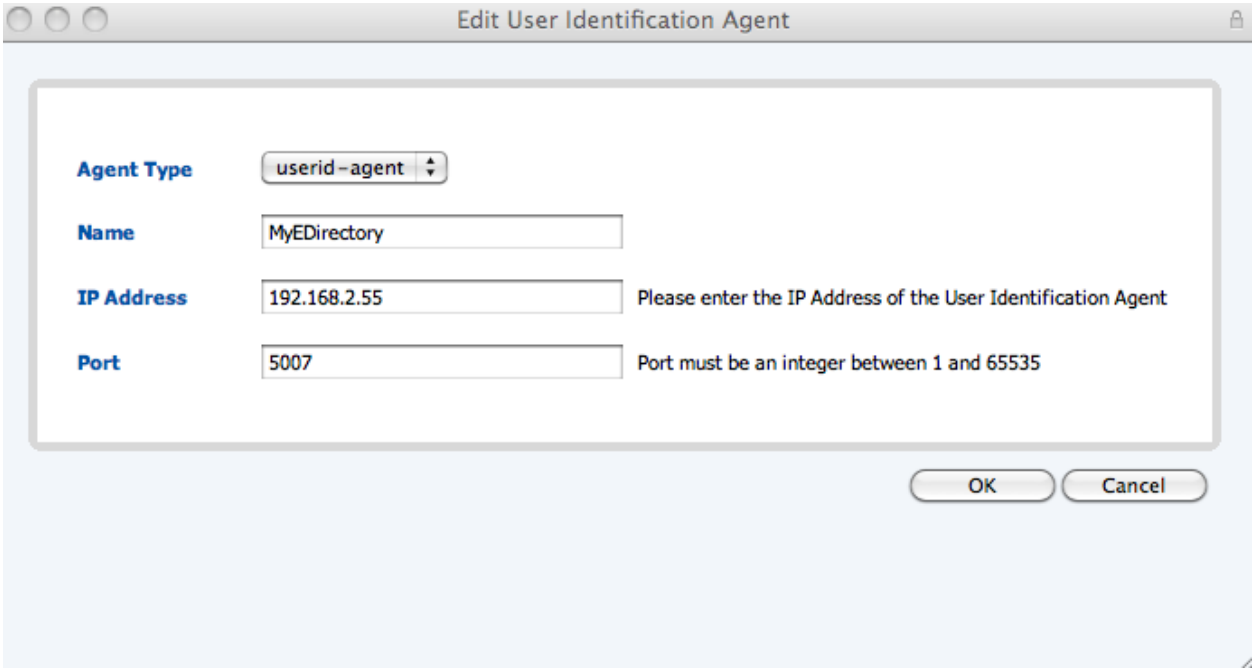
After entering the required information hit the commit button to make our changes effective.



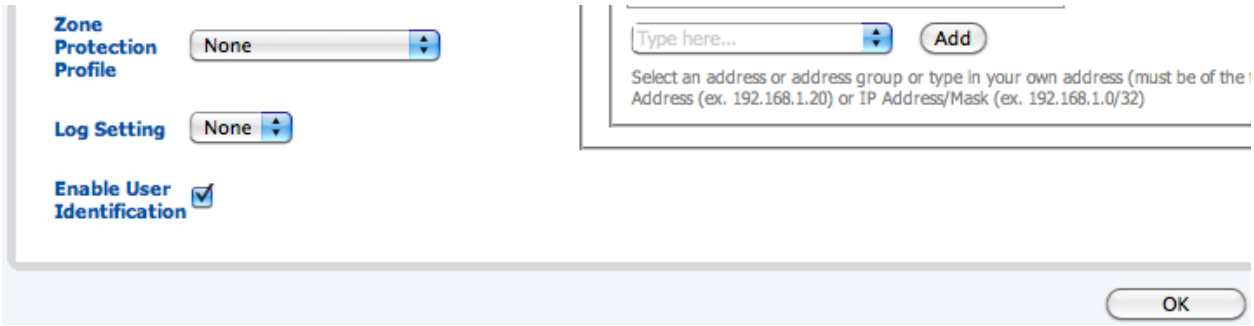
To verify the configuration we can select the Monitor icon. On this screen we can see user to IP mappings and perform searches.



Next we need to configure the Palo Alto Networks firewall to work with the agent. From the UI select the Device tab, then select User Identification from the list on the left. Under the User Identification Agent section hit the "**Add**" button. Set the Agent Type "***user-id-agent***". Give it a name set and fill in the IP address and the port you had configured the agent to listen on.



Our next step is to enable User Identification on the appropriate zone. Choose the Network tab, select Zones from the list on the left, and click on the zone you wish to use. At the bottom of the screen check the box " **Enable User Identification**".



Once we hit OK and commit our changes we should start to get some user information showing up in our logs.

We can use the CLI to gain some more useful statistics for troubleshooting. The command: ***show user user-id-agent statistics*** give us the following:

```
admin@PA-500> show user userid-agent statistics

uid-agent is running.

Server: MyEDirectory(vsys: vsys1) Address: 192.168.2.55:5007
        Connection                                        : Connected
        Version                                           : 3.1.0
        number of connection tried                        : 11773
        number of connection succeeded                    : 11735
        number of connection failed                       : 38
        number of user ip mapping messages received       : 2
        number of user ip mapping add entries received    : 2
        number of user ip mapping del entries received    : 0
        number of ip msgs rcvd but failed to process      : 0
        number of status messages received                : 1061
        number of request of ip mapping messages sent     : 0
        number of request of all ip mapping messages sent : 2
        number of request of status messages sent         : 1061
```

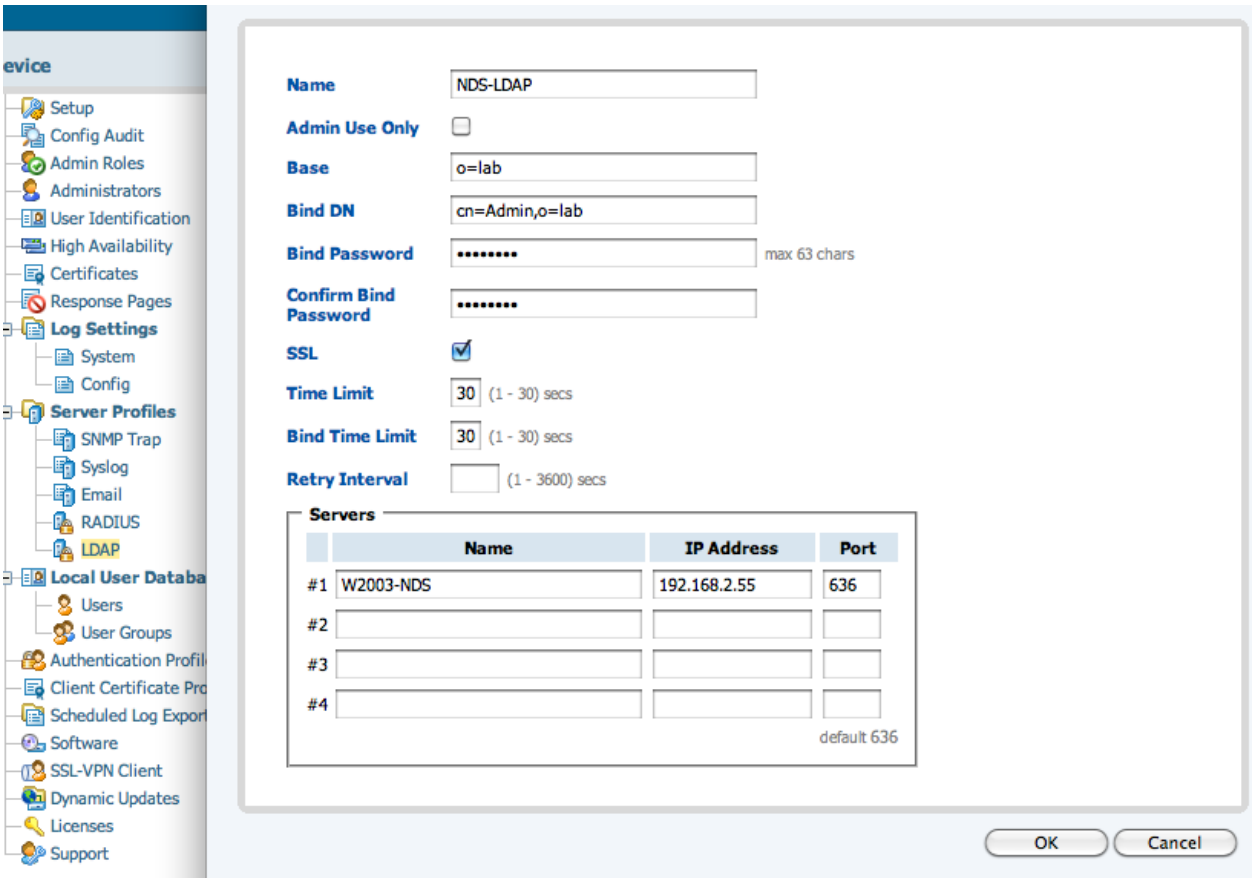
The "***show user ip-user-mapping***" can also provide useful information:

```
admin@PA-500> show user ip-user-mapping

IP              Ident. By User                            Idle Timeout (s) Max. Timeout (s)
--------------- --------- ------------------------------- ---------------- ----------------
192.168.2.87    AD        mynds\testuser                  3069             3069
Total: 1 users
```

Once we have gotten the basic User-ID working we next need to create an LDAP Server Profile we will use later for the User Identification LDAP server setup.

From the Device Tab, under Server Profiles, select LDAP and then click on "**New**"

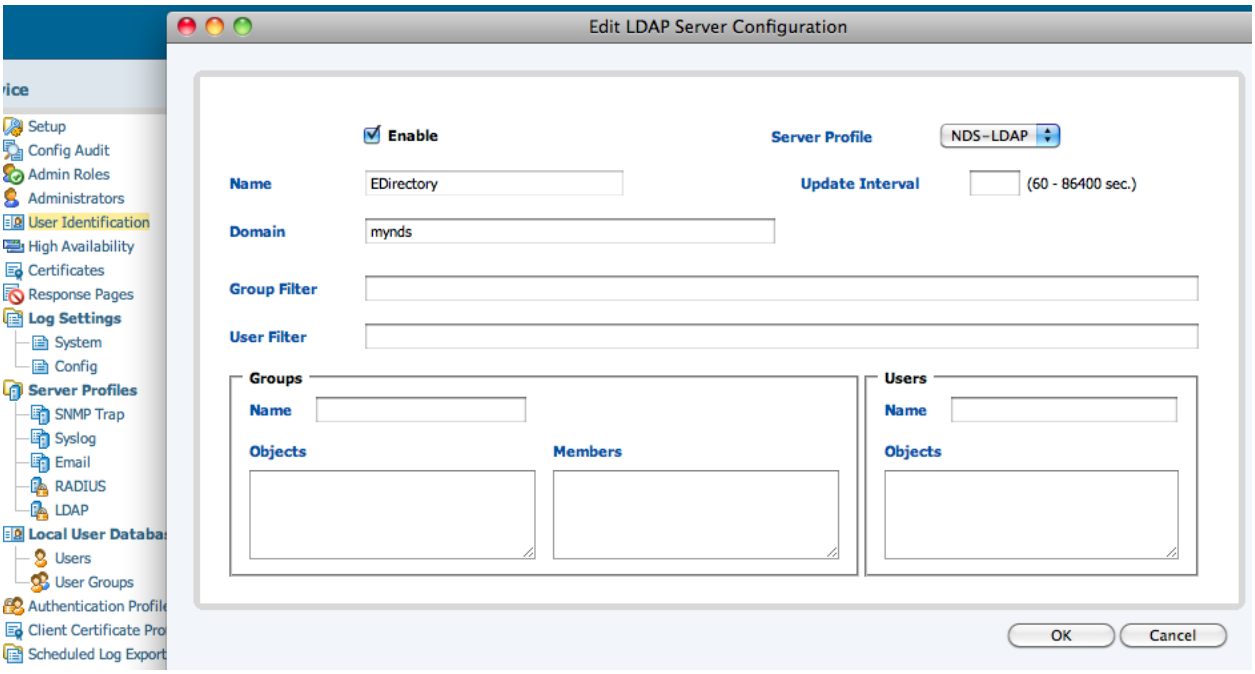
Fill in the same information that you did when setting up the User Agent. Make sure that SSL is enabled and the port is set to 636. eDirectory does not allow passwords to be sent in the clear.



For the final step we need to define the LDAP server for User Identification. Select the User Identification icon under the Device tab. Choose "**Add**", give the server a name and select the Server Profile you just created.

You can create a group or user profile if desired (we will give an example of this later). These limit the users and groups that the firewall learns about for use in policy.

For eDirectory we do not need to complete any of the other fields.



After you commit your changes you can verify the configuration from the CLI using the command '***show user ldap-server server <Server Name>***"

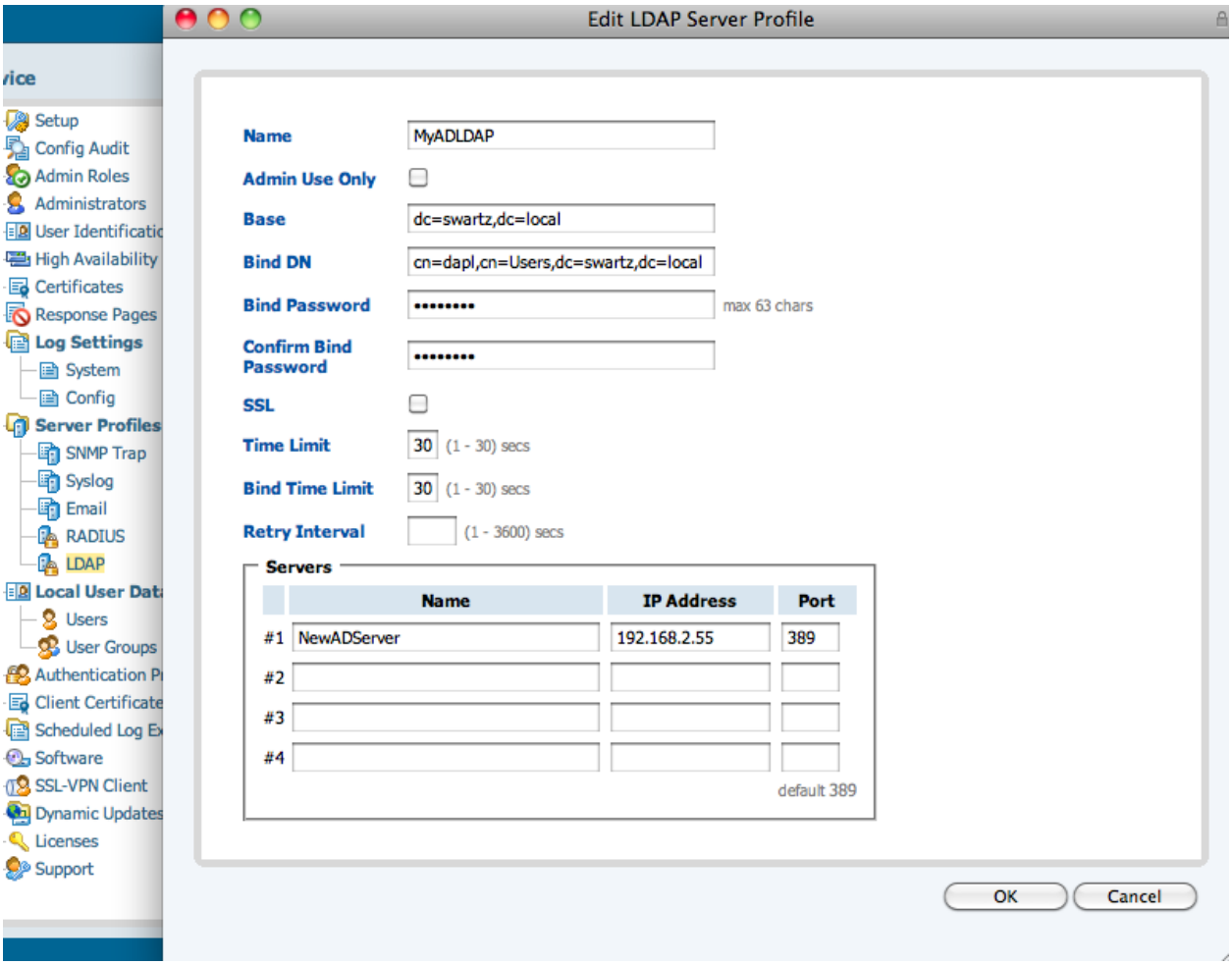
```
admin@PA-500> show user ldap-server server EDirectory


LDAP server EDirectory
        Bind DN    : cn=Admin,o=lab
        Base       : o=lab
        Group Filter: (None)
        User Filter: (None)
        Servers    : configured 1 servers
                192.168.2.55(736)
                        Last Action Time: 2779 seconds ago
                        Next Action Time: In 821 seconds
Groups:
GROUP: cn=internet-access,ou=security-groups,o=lab, member: 1
        mynds\testuser    cn=testuser,o=lab

admin@PA-500>
```

Note: it may take a while to populate the group and user information. Once the group and user information is available then they are available for use in policy. Next we will show how to use native LDAP for authenticating users and administrators.

LDAP Authentication Configuration

For situations where we need to actually challenge users for a username and password, we can now use LDAP. There are three basic steps involved: add an LDAP server under Server Profiles, add an LDAP server under the User Identification section, create an Authentication profile using the defined LDAP server.

In this example we will connect to Active Directory using LDAP. Under the Device tab select the LDAP option under Server Profiles. Click "New" to add the server. As in our previous example fill in all the necessary information.



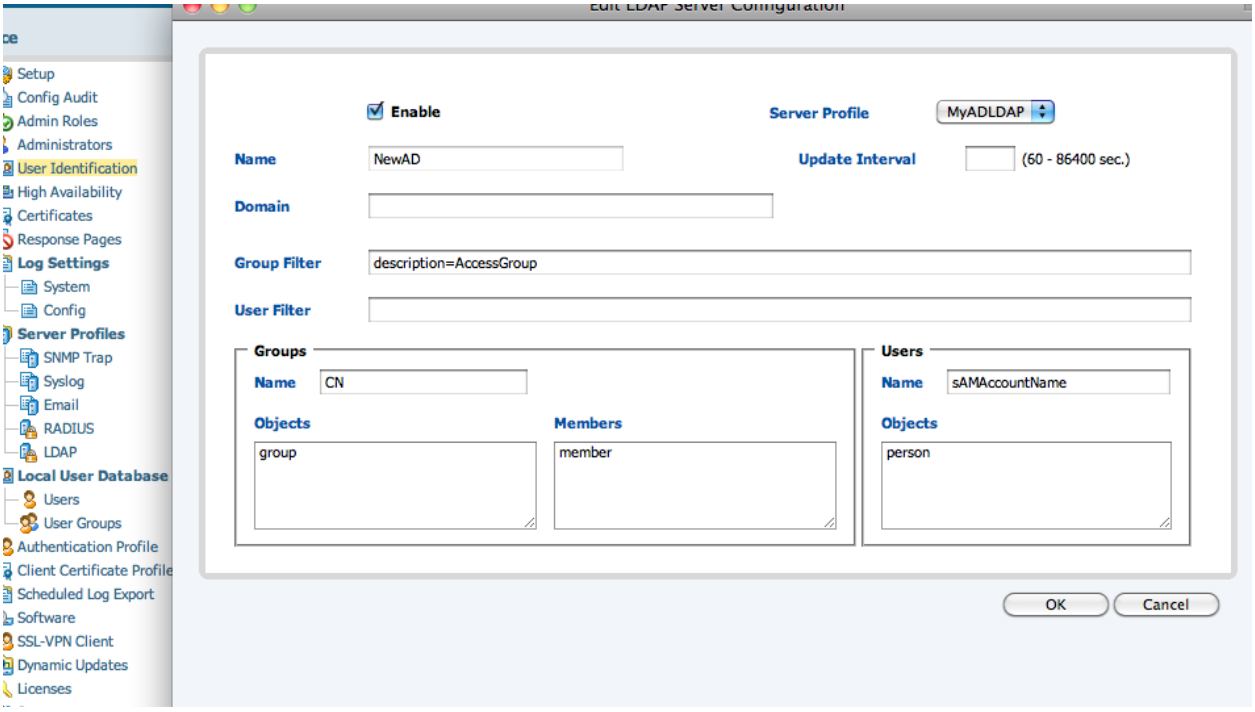
Note that in this example we are setting it up without SSL encryption over port 389. Active Directory does not require encryption and it is not available by default. If you want to enable

SSL for LDAP in Active Directory the following URL can prove helpful: http://www.linuxmail.info/enable-ldap-ssl-active-directory/.

Next we add the LDAP server in the User Identification section as we did before. There are a few differences. For Active Directory we need to specify how we determine group and user objects. For Active Directory you can set the fields as follows:

Groups: Name=CN, Objects:=group, Members=member

Users: Name=sAMAccountName, Objects=person.



Notice I have added a group filter: ***description=AccessGroup.*** This limits the number of groups and users that the firewall will learn about and therefore are available for use in creating policies.

In the following example I had set the description fields on the groups I wanted to use. Here is a before and after look at the effect of this setting (obviously I committed my changes before adding this setting and then after).

```
admin@PA-500> show user ldap-server server NewAD


LDAP server NewAD(job 790)
        Bind DN    : cn=dapl,cn=Users,dc=swartz,dc=local
        Base       : dc=swartz,dc=local
        Group Filter: (None)
        User Filter: (None)
        Servers    : configured 1 servers
           192.168.2.55(389)
                      Last Action Time: 402 seconds ago
                      Next Action Time: Now

Groups:
GROUP: CN=HelpServicesGroup,CN=Users,DC=swartz,DC=local, member: 1
        SUPPORT_388945a0 CN=SUPPORT_388945a0,CN=Users,DC=swartz,DC=local
GROUP: CN=TelnetClients,CN=Users,DC=swartz,DC=local, member: 0
GROUP: CN=IIS_WPG,CN=Users,DC=swartz,DC=local, member: 1
        IWAM_JUNK2003     CN=IWAM_JUNK2003,CN=Users,DC=swartz,DC=local
GROUP: CN=DHCP Users,CN=Users,DC=swartz,DC=local, member: 0
GROUP: CN=DHCP Administrators,CN=Users,DC=swartz,DC=local, member: 0
GROUP: CN=Administrators,CN=Builtin,DC=swartz,DC=local, member: 2
        Administrator     CN=Administrator,CN=Users,DC=swartz,DC=local
        bill              CN=Bill Swartz,CN=Users,DC=swartz,DC=local
GROUP: CN=Domain Admins,CN=Users,DC=swartz,DC=local, member: 2
        Administrator     CN=Administrator,CN=Users,DC=swartz,DC=local
        bill              CN=Bill Swartz,CN=Users,DC=swartz,DC=local
GROUP: CN=Enterprise Admins,CN=Users,DC=swartz,DC=local, member: 1
        Administrator     CN=Administrator,CN=Users,DC=swartz,DC=local
GROUP: CN=Users,CN=Builtin,DC=swartz,DC=local, member: 0
GROUP: CN=Domain Users,CN=Users,DC=swartz,DC=local, member: 0
GROUP: CN=Guests,CN=Builtin,DC=swartz,DC=local, member: 2
        Guest             CN=Guest,CN=Users,DC=swartz,DC=local
        IUSR_JUNK2003     CN=IUSR_JUNK2003,CN=Users,DC=swartz,DC=local
GROUP: CN=Domain Guests,CN=Users,DC=swartz,DC=local, member: 0
GROUP: CN=Print Operators,CN=Builtin,DC=swartz,DC=local, member: 0
GROUP: CN=Backup Operators,CN=Builtin,DC=swartz,DC=local, member: 0
GROUP: CN=Replicator,CN=Builtin,DC=swartz,DC=local, member: 0
GROUP: CN=Remote Desktop Users,CN=Builtin,DC=swartz,DC=local, member: 1
        bill              CN=Bill Swartz,CN=Users,DC=swartz,DC=local
GROUP: CN=Network Configuration Operators,CN=Builtin,DC=swartz,DC=local, member: 0
GROUP: CN=Performance Monitor Users,CN=Builtin,DC=swartz,DC=local, member: 0
GROUP: CN=Performance Log Users,CN=Builtin,DC=swartz,DC=local, member: 0
GROUP: CN=Domain Computers,CN=Users,DC=swartz,DC=local, member: 0
GROUP: CN=Domain Controllers,CN=Users,DC=swartz,DC=local, member: 0
GROUP: CN=Schema Admins,CN=Users,DC=swartz,DC=local, member: 1
        Administrator     CN=Administrator,CN=Users,DC=swartz,DC=local
```

```
admin@PA-500> show user ldap-server server NewAD


LDAP server NewAD
        Bind DN    : cn=dapl,cn=Users,dc=swartz,dc=local
        Base       : dc=swartz,dc=local
        Group Filter: description=AccessGroup
        User Filter: (None)
        Servers    : configured 1 servers
                192.168.2.55(389)
                        Last Action Time: 357 seconds ago
                        Next Action Time: In 3243 seconds
Groups:
GROUP: CN=VPN Users,OU=Security groups,DC=swartz,DC=local, member: 1
        bill              CN=Bill Swartz,CN=Users,DC=swartz,DC=local
GROUP: CN=Web Only,OU=Security groups,DC=swartz,DC=local, member: 0

admin@PA-500>
```

The User filter can be used to restrict the users that you will learn about.

These filters only control the groups you see or users you can search for when setting an Allow List in an Authentication Profile or when setting a source user or group in policy.

Note: Domain Users is a special group in Active Directory users are tied to it as part of the user schema with the attribute ***primaryGoupID*** . Members cannot be enumerated via an LDAP query, as the ***member*** attribute is not set for this group so it cannot be used to learn all of the usernames.

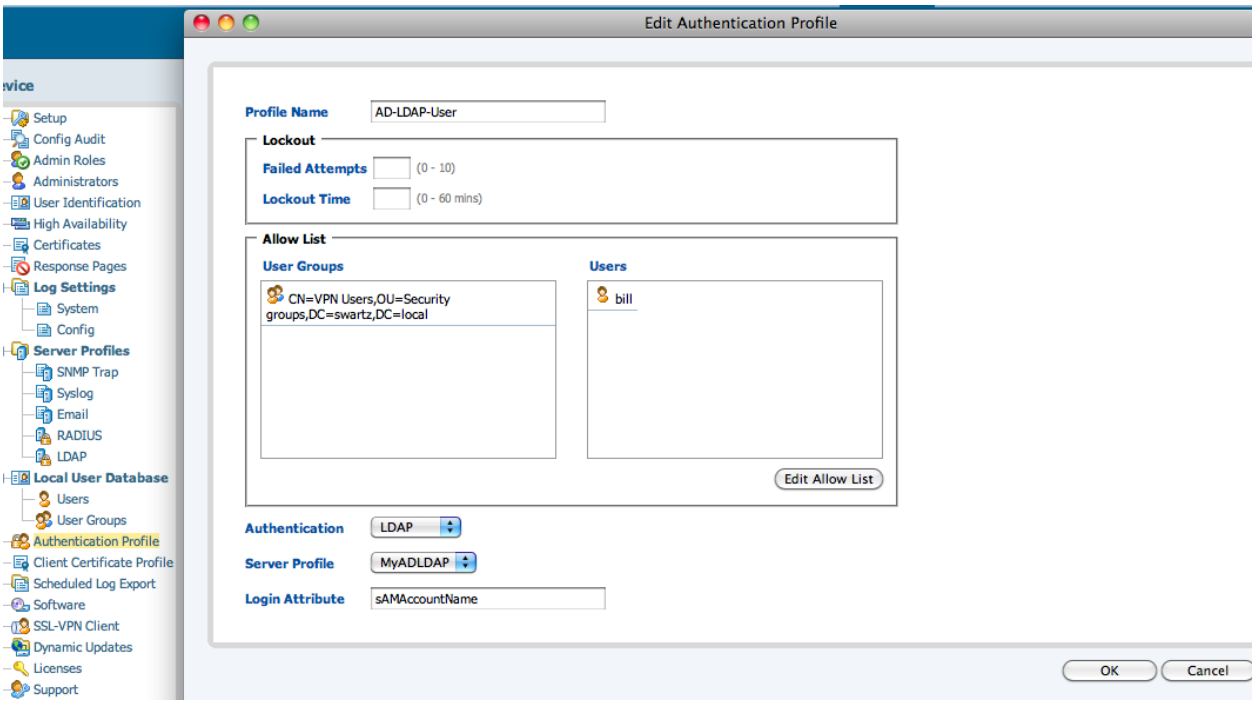
You can learn more about building LDAP queries at the following sites:

http://www.rfc-editor.org/rfc/rfc2254.txt

http://www.zytrax.com/books/ldap/apa/search.html

The final step is to create an Authentication Profile using our LDAP server. From the Device tab select the Authentication Profile icon and choose "**New**". Give the profile a name set Authentication to LDAP, select the Server Profile you created and set the login attribute. This maps the name entered by the user to an LDAP attribute. For AD we use ***sAMAccountName***.

Next you will want to edit the Allow List to specify the groups and users that can use this method of authentication. Note: as of this writing you must specify each user you want to provide administrative access for).



You can now use this profile for administrative access, Captive Portal or SSL VPN access as you previously could for RADIUS or a Local User Database.

Following is a screenshot of an SSL VPN profile using LDAP.

Edit SSL-VPN - MyNewSSLVPN

SSL VPN | Client Configuration

Portal Configuration

Portal Name: MyNewSSLVPN
Virtual System: vsys1
Tunnel Interface: tunnel.1 New ...
Max User:
Authentication Profile: AD-LDAP-User New ...
Client Certificate Profile: [empty] New ...
Server Certificate: myVPN
Import certificate ...
Generate self-signed certificate ...
☑ Enable IPSec encapsulation of client traffic
☑ Redirect HTTP traffic to HTTPS login page

Gateway Address

Interface: ethernet1/3
IP Address: 71.246.8.35/24

Timeout Configuration

Login Lifetime: [empty]
Inactivity Logout: [empty]

One advantage of using LDAP for authentication is that for most organizations already have a directory service that supports LDAP so nothing needs to be installed or configured. Also since we allow the user to define how to determine both groups and users it should work with almost any LDAP compatible directory.