



eDirectory and LDAP Authentication with PANOS

One of the most useful features of the Palo Alto firewall is its ability to map usernames to IP addresses. Once the firewall knows the names associated with IP addresses, the firewall can 1) log this information, and 2) control traffic based upon a particular username or group. Prior to PANOS 3.1, the following methods existed:

- **Transparent authentication:** the firewall can automatically retrieve username and IP mappings from Active Directory domain controllers, using the Active Directory User-ID agent. In this case, the user previously logged into the domain, and so is not prompted for credentials by the firewall.
- **Interactive authentication:** the firewall can prompt the user for their username, and then authenticate the user via RADIUS or a local user database. This would be the case in the following situations:
 - the users are running Mac or linux clients (called “captive portal”)
 - the users are connecting to the firewall over our SSL VPN
 - the users are trying to login to the firewall GUI as an administrator

With the release of PANOS 3.1 and the support for LDAP, the above methods are extended to include:

- **Transparent authentication:** the firewall can automatically retrieve username and IP mappings from Active Directory domain controllers (using the Active Directory User-ID agent) or from eDirectory servers (using the new eDirectory User-ID agent). **Please note the new User-ID agent is only compatible with eDirectory 8.8 and due to unique login information that eDirectory tracks.**
- **Interactive authentication:** the firewall can prompt the user for their username, and then authenticate the user via RADIUS, a local user database, or an LDAP server.

This document will cover configuring transparent authentication via an eDirectory server, as well as interactive authentication via an LDAP server. Thus this document has two parts:

- Part 1: Obtaining user authentication information from an eDirectory server transparently with the new User-ID agent.
- Part 2: Configuring LDAP authentication with an Active Directory server for use with captive portal, SSL VPN, or firewall GUI access.

Before we get into the actual setup I would suggest you have a local LDAP browser. This will help to verify the settings you will be using for the User-ID agent and the PA firewall.

Throughout this examples are done using JXplorer, a free cross platform LDAP browser that can be obtained here: <http://jxplorer.org/>.

Part 1: Transparently obtaining user authentication information from eDirectory

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 are stored in the directory in the fields: **networkAddress** (in a proprietary binary format) and **loginTime**. The new User-ID agent was developed to be able to specifically read this information so that we can transparently map users to their IP addresses.

One major difference between the Palo Alto LDAP agent and the Palo Alto 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.

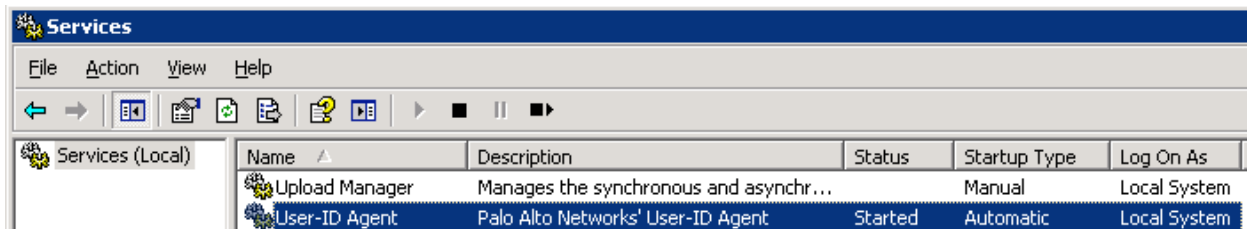
Part 1a: Installing and configuring the User-ID Agent

1. Make sure you are running Novell eDirectory 8.8 or higher. The User-ID Agent uses some LDAP functions that are not available in previous versions of eDirectory.
2. You will now install the new User-ID agent. Login to your support 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

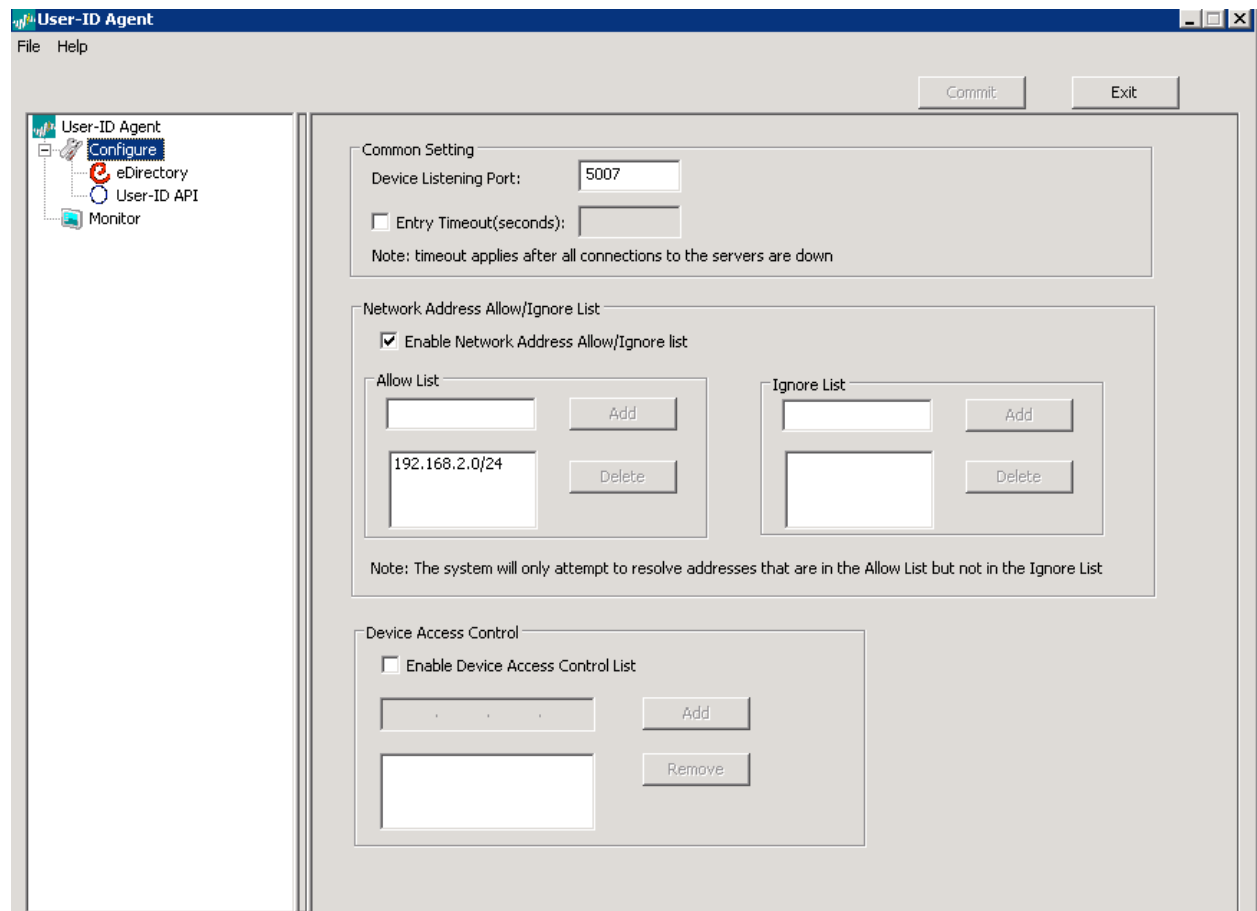
Version	Release Date	Release Notes	Download	Size	MD5
3.1.0-LDAP	15 Mar 10	PANOS-3.1.0-RN-revA.pdf	Download 	970 KB	Show MD5

Download this .msi file to the Windows server where the agent will run. Install the .msi file while logged in as an administrator. It will run as a local service under the local system account. The service name is "User ID Agent", as shown here in the Services management console.



3. Once installed launch the User-ID Agent and select Configure. Configure the following:

- Device Listening Port: use the default. This port number is used for communications between this agent and the PA firewall. Remember this port number, you will need it when configuring the PA firewall.
- Enable the Network Address Allow/Ignore list. Add the networks for which you want to monitor for user IDs. If there are terminal servers or other multi-user machines, add those IP addresses to the Ignore list as we need to use the Terminal Services Agent to track users on those systems.

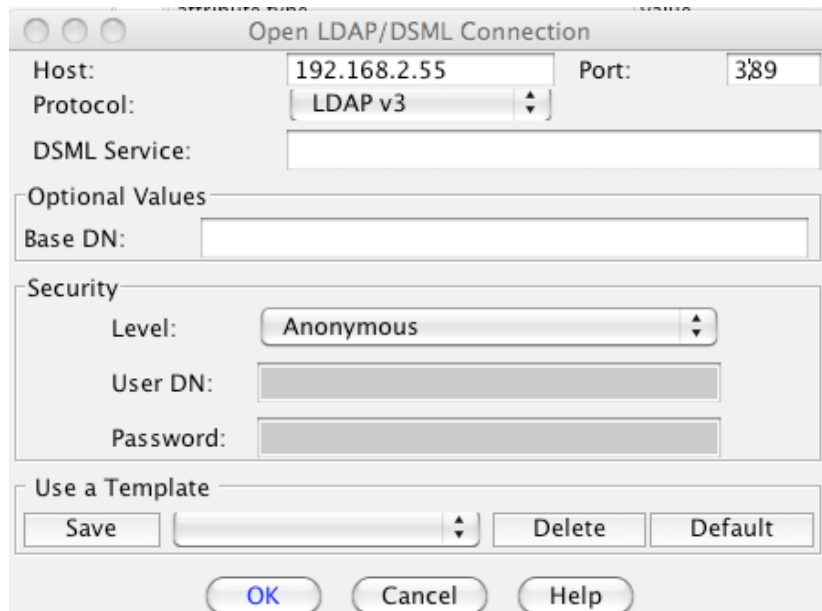


4. Next we need to configure our eDirectory settings. Select the eDirectory menu item on the left, and the screen below will appear.

The screenshot shows the 'User-ID Agent' configuration window. On the left is a tree view with 'Configure' selected, containing 'eDirectory', 'User-ID API', and 'Monitor'. The main area is titled 'LDAP Server Selection' and contains a 'Server' input field, an 'Add' button, a 'Server List' containing '192.168.2.55', a 'Remove' button, and a 'Copy Setting...' button. Below this are two panels: 'Basic Settings For 192.168.2.55' and 'Advanced Settings For 192.168.2.55'. The Basic Settings panel includes fields for 'Search Base' (o=lab), 'Bind Distinguished Name' (cn=Admin,o=lab), 'Bind Password' (masked), 'Confirm Bind Password' (masked), 'Server Domain Prefix' (mynds), and 'Search Interval(seconds)' (30). The Advanced Settings panel includes fields for 'Search Filter' ((objectClass=Person)), 'Login Address Attribute Name' (networkAddress), 'Login Time Attribute Name' (loginTime), 'Login ID Attribute Name' (uniqueID), and a 'Bind Port' section with radio buttons for '636 (SSL Enabled)' (selected) and 'Other' (with an empty input field), and a checkbox for 'SSL'. A 'Verify Server Certificate' checkbox is at the bottom right.

Complete the following fields:

- **Server** Enter the IP address of the eDirectory server you will be monitoring and hit “**Add**”. If you have multiple servers to monitor, you need to configure the settings at the bottom of the screen for EACH of the servers using the **Copy Setting** button can simplify the process. There are several instances where you will need to enter multiple eDirectory servers. If the directory is partitioned among servers you need to make sure that each partition has a server configured. Also depending on how quickly information is synchronized between servers you may want to add additional servers to insure that user/ip mappings show up more quickly.
- **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. In eDirectory this is typically in the form of **o=**. Using JXplorer you can connect to eDirectory anonymously and only specify the IP address and the default non SSL port as shown below.



Open LDAP/DSML Connection

Host: 192.168.2.55 Port: 389

Protocol: LDAP v3

DSML Service:

Optional Values

Base DN:

Security

Level: Anonymous

User DN:

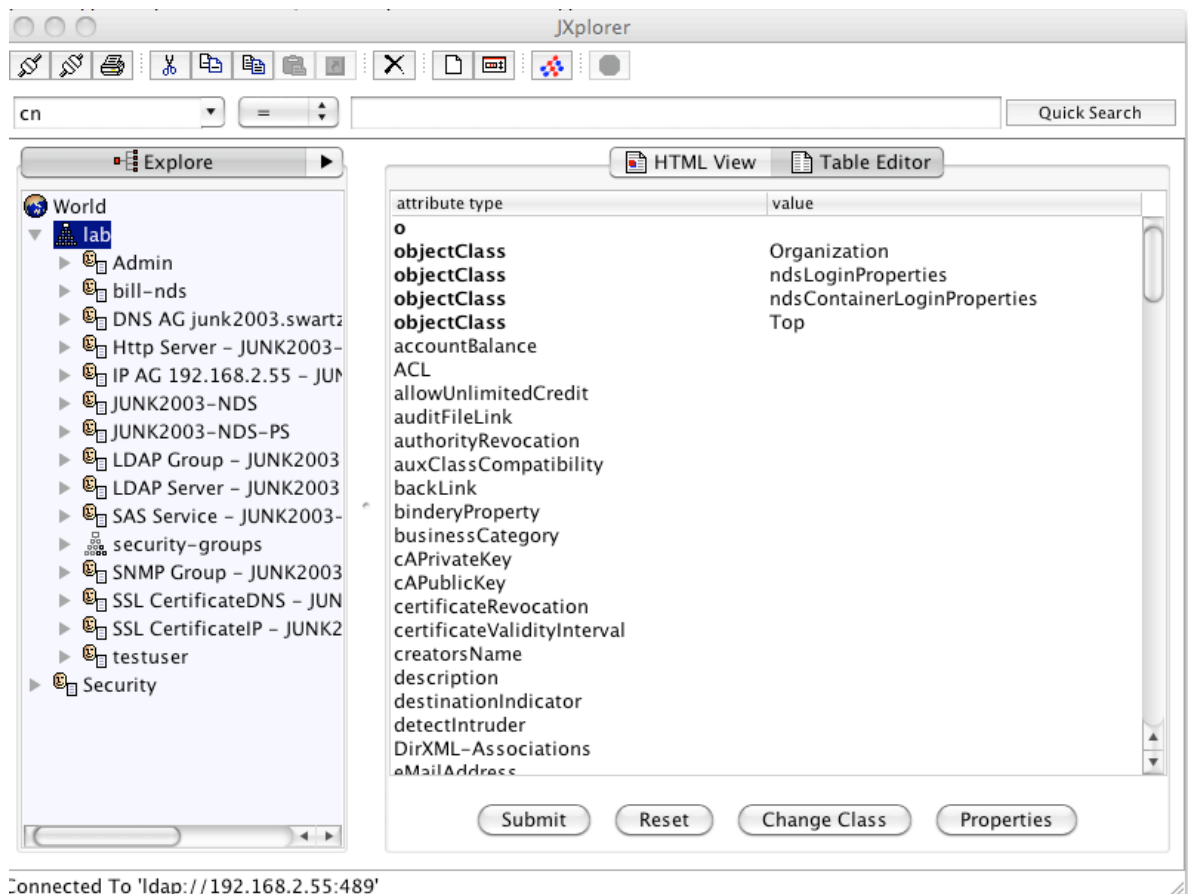
Password:

Use a Template

Save [] Delete Default

OK Cancel Help

Hit OK and you will get to the following where you can expand the root objects to determine your base DN. Also select Table Editor view to see the actual object type. In this example our base is **o=lab**.



JXplorer

cn

Quick Search

Explore

World

- lab
 - Admin
 - bill-nds
 - DNS AG junk2003.swartz
 - Http Server - JUNK2003-
 - IP AG 192.168.2.55 - JUN
 - JUNK2003-NDS
 - JUNK2003-NDS-PS
 - LDAP Group - JUNK2003
 - LDAP Server - JUNK2003
 - SAS Service - JUNK2003-
 - security-groups
 - SNMP Group - JUNK2003
 - SSL CertificateDNS - JUN
 - SSL CertificateIP - JUNK2
 - testuser
 - Security

HTML View Table Editor

attribute type	value
o	Organization
objectClass	ndsLoginProperties
objectClass	ndsContainerLoginProperties
objectClass	Top
accountBalance	
ACL	
allowUnlimitedCredit	
auditFileLink	
authorityRevocation	
auxClassCompatibility	
backLink	
binderyProperty	
businessCategory	
cAPrivateKey	
cAPublicKey	
certificateRevocation	
certificateValidityInterval	
creatorsName	
description	
destinationIndicator	
detectIntruder	
DirXML-Associations	
eMailAddress	

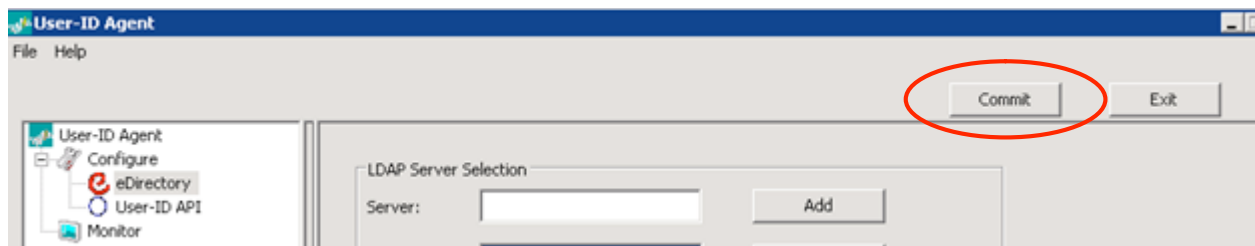
Submit Reset Change Class Properties

Connected To 'ldap://192.168.2.55:489'

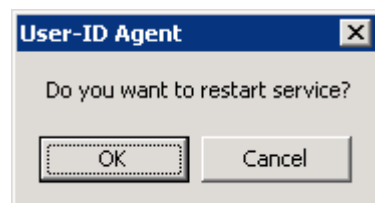
- **Bind Distinguished Name and Password** This is the fully distinguished name (FQDN) of the user you will use to query eDirectory. This account does not need any special privileges. You will need to enter the password for this account. You should be able to browse to this anonymously as we did to get the *BaseDN*. Remember that the fully distinguished name is built from using the entire hierarchy. In our example that would be cn=Admin, o=lab.
- **Server Domain Prefix** (optional) 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.
- **Search Interval** The default of 30 seconds should be fine but this can be adjusted if necessary. One point here: after the first query to build the list of all currently logged in users, subsequent queries only search for users entries that have been modified since the last query.

No other fields should need to be modified as they are set to specifically work with eDirectory.¹ Keep the bind port at 636, and SSL must be enabled, as eDirectory does not allow authenticated LDAP queries to be sent in the clear.

5. After entering the required information hit the **Commit** button to make our changes effective.

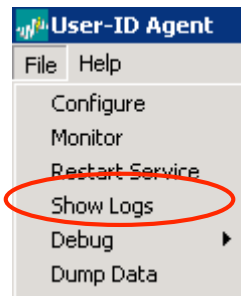


You will be prompted to restart the service.



6. Now, view the agent logs to see what is happening with the agent. File -> Show Logs will open a .txt file.

¹ Note that if they do need to be modified, you should use an LDAP browser to determine what to set the fields to.



At the bottom of that text file will be the latest debug information output from the agent, scroll down to that. Examine the output under the header labeled “Service is being started”. Here is an example log file:

```
debug.log - Notepad
File Edit Format View Help
04/16/10 09:30:40:812[Info 253]: -----Service is being started-----
04/16/10 09:30:40:812[Info 181]: Load debug log level Info .
04/16/10 09:30:40:812[Info 156]: Service version is 1.0.0.1.
04/16/10 09:30:40:812[Info 185]: Protocol version is 0x4.
04/16/10 09:30:40:812[Info 186]: Product version is 3.1.0.
04/16/10 09:30:40:828[Info 483]: LDAP Client thread 0 with server 1.1.1.9 is
started.
04/16/10 09:30:40:828[Info 212]: EDirectory gets started.
04/16/10 09:30:40:828[Info 1056]: Connect succeeds on server 1.1.1.9.
04/16/10 09:30:45:312[Info 585]: New connection 127.0.0.1:3667.
04/16/10 09:30:45:312[Info 630]: Client thread 0 with IP 127.0.0.1 is started.
04/16/10 09:30:45:437[Info 1031]: Client thread 0 accept finished
```

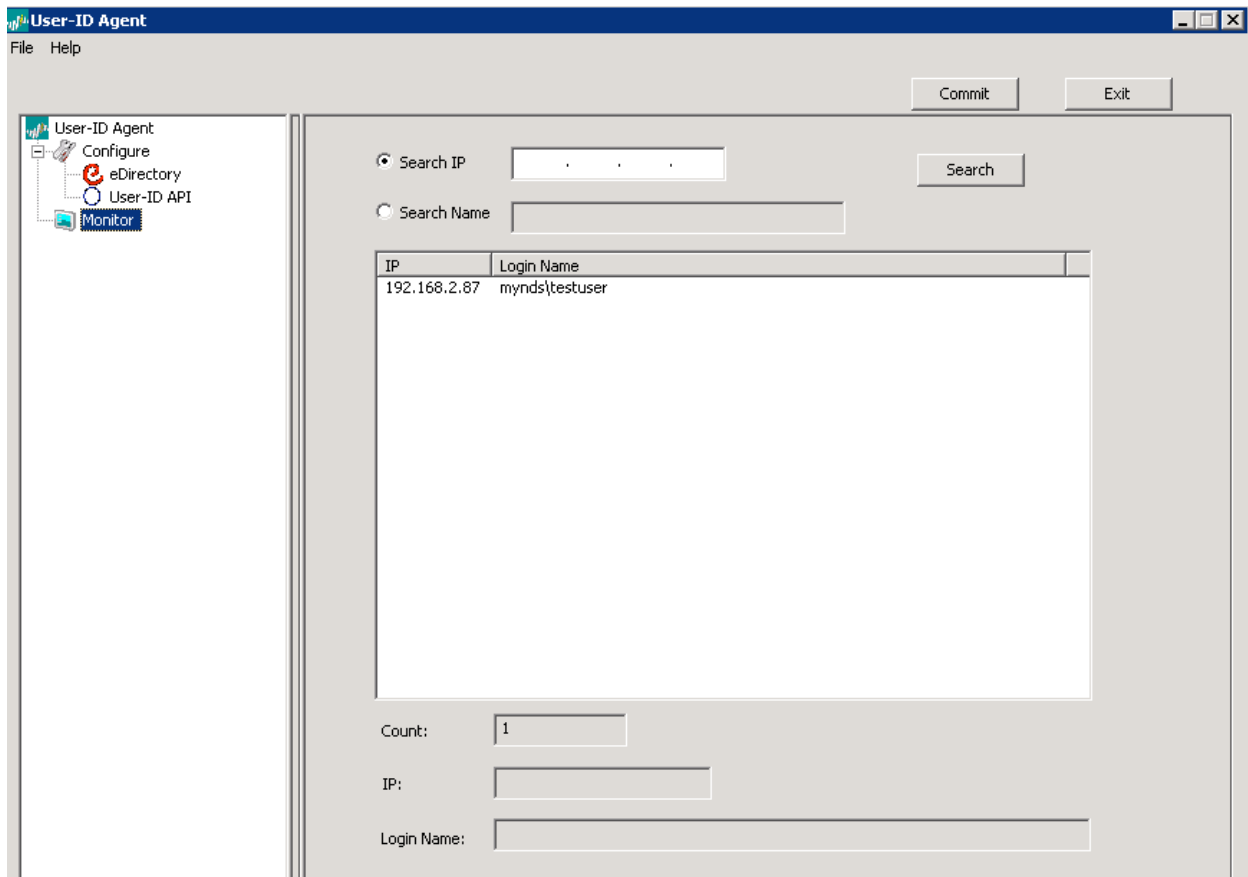
You want to see the message “Connect succeeds on server x.x.x.x”, as highlighted above. If you do not see that message, you will need to do some troubleshooting.

```
debug.log - Notepad
File Edit Format View Help
04/16/10 09:00:07:734[Info 253]: -----Service is being started-----
04/16/10 09:00:07:734[Info 181]: Load debug log level Debug.
04/16/10 09:00:07:734[Info 156]: Service version is 1.0.0.1.
04/16/10 09:00:07:734[Info 185]: Protocol version is 0x4.
04/16/10 09:00:07:734[Info 186]: Product version is 3.1.0.
04/16/10 09:00:07:734[Debug 531]: Server thread started.
04/16/10 09:00:07:750[Info 483]: LDAP Client thread 0 with server 1.1.1.9 is started.
04/16/10 09:00:07:750[Info 212]: EDirectory gets started.
04/16/10 09:00:07:750[Debug 728]: service started.
04/16/10 09:00:07:750[warn 140]: ldap_connect failed on error 81: server down(client thread 0, server 1.1.1.9)!
```

Helpful troubleshooting hints:

- If you see error 81 in the log, make sure that the bind port/SSL setting is configured as needed.
- If you see error 93 in the log that may mean that there is some kind of communication error. You may be running the wrong version of eDirectory, or the base DN is not correct.

- If you want to increase the amount of information logged, use File -> Debug menu to set the level to be more detailed (default level is “info”), and then restart the service (File -> Restart Service)
 - Note that this text file is not updated dynamically, so you will have to close it and use the menu to view it again to see new information.
7. To verify the configuration we can select the Monitor icon. On this screen we can see user to IP mappings. The number of mappings will increase as the agent reads more information from the LDAP server.

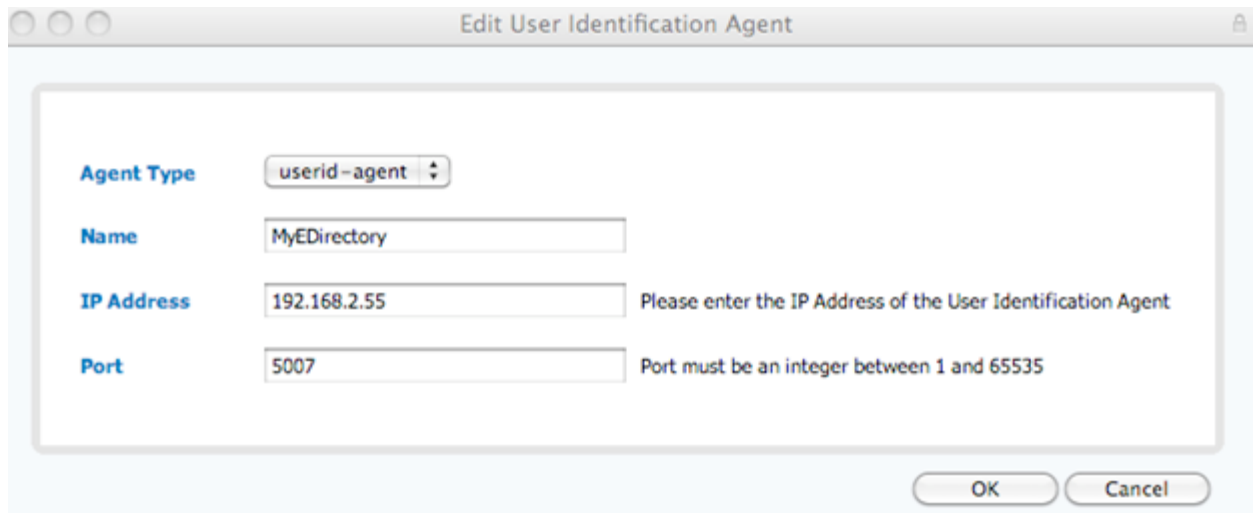


Once you see a list of users on this screen, that is confirmation that you have configured the agent properly. You can now move on to configuring the firewall to talk to this agent.

Part 1b: Configuring the firewall to talk to the User-ID agent

8. On the firewall GUI, 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 (default port is 5007).



Agent Type:

Name:

IP Address: Please enter the IP Address of the User Identification Agent

Port: Port must be an integer between 1 and 65535

OK Cancel

9. You will now enable User Identification on the appropriate zone. Choose the Network tab, select Zones from the list on the left, and click on the zone where users’ traffic originates. At the bottom of the screen check the box “**Enable User Identification**”.



Zone Protection Profile:

Log Setting:

Enable User Identification: ☒

Type here...

Select an address or address group or type in your own address (must be of the form Address (ex. 192.168.1.20) or IP Address/Mask (ex. 192.168.1.0/32))

OK

10. Commit your changes.

11. To confirm that the firewall is communicating with the agent, run this command:

```

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

```

12. To confirm that the user database was obtained from the agent, run this command:

```

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				

13. At this point, the user IDs will appear in the Monitor tab -> Traffic log in the source-user and target-user columns.

14. Now that 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”

LDAP Configuration

Name: NDS-LDAP

Admin Use Only: ☐

Base: o=lab

Bind DN: cn=Admin,o=lab

Bind Password: max 63 chars

Confirm Bind Password:

SSL: ☒

Time Limit: 30 (1 - 30) secs

Bind Time Limit: 30 (1 - 30) secs

Retry Interval: (1 - 3600) secs

	Name	IP Address	Port
#1	W2003-NDS	192.168.2.55	636
#2			
#3			
#4			

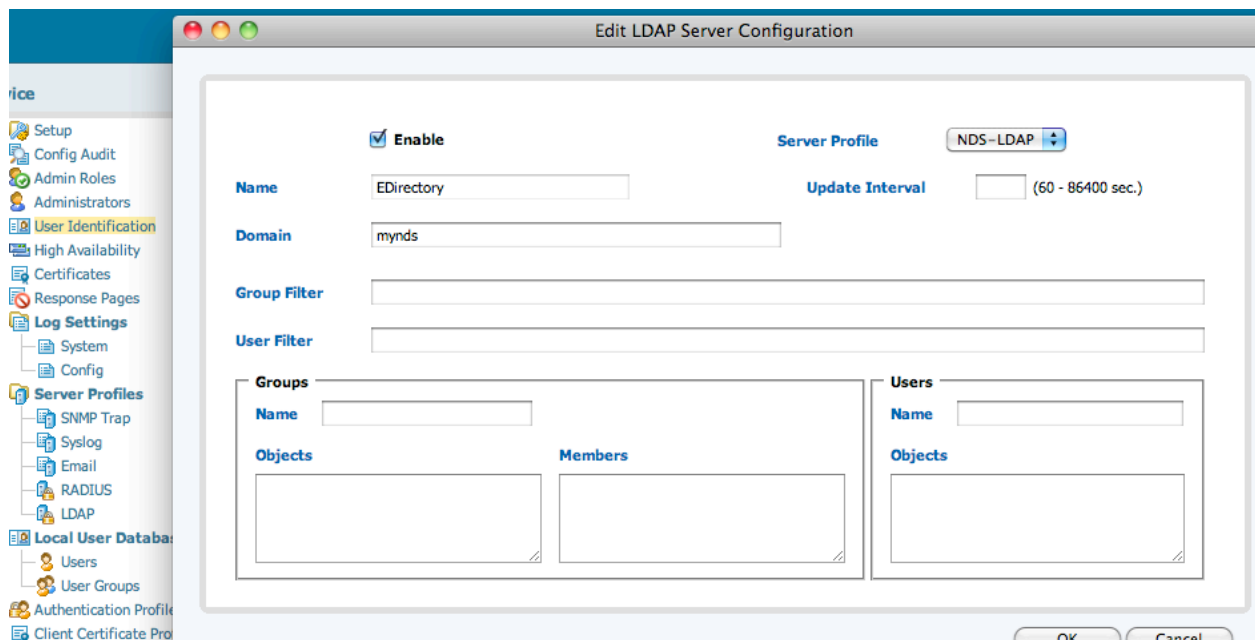
default 636

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.

15. For the final step we need to define the LDAP server to be able to retrieve the group information.² 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.

² The firewall will be retrieving object class cn=group.



16. Commit your changes. The group information is now being retrieved from the directory. It may take a while to populate the group and user information.

17. Confirm that the firewall is communicating with the LDAP server, and that group information was retrieved:

```
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
```

18. Once the group and user information is retrieved, then that information can be used in policy. To confirm, go to the Policies tab, click in the source-user column, and in the screen that appears, groups should appear.

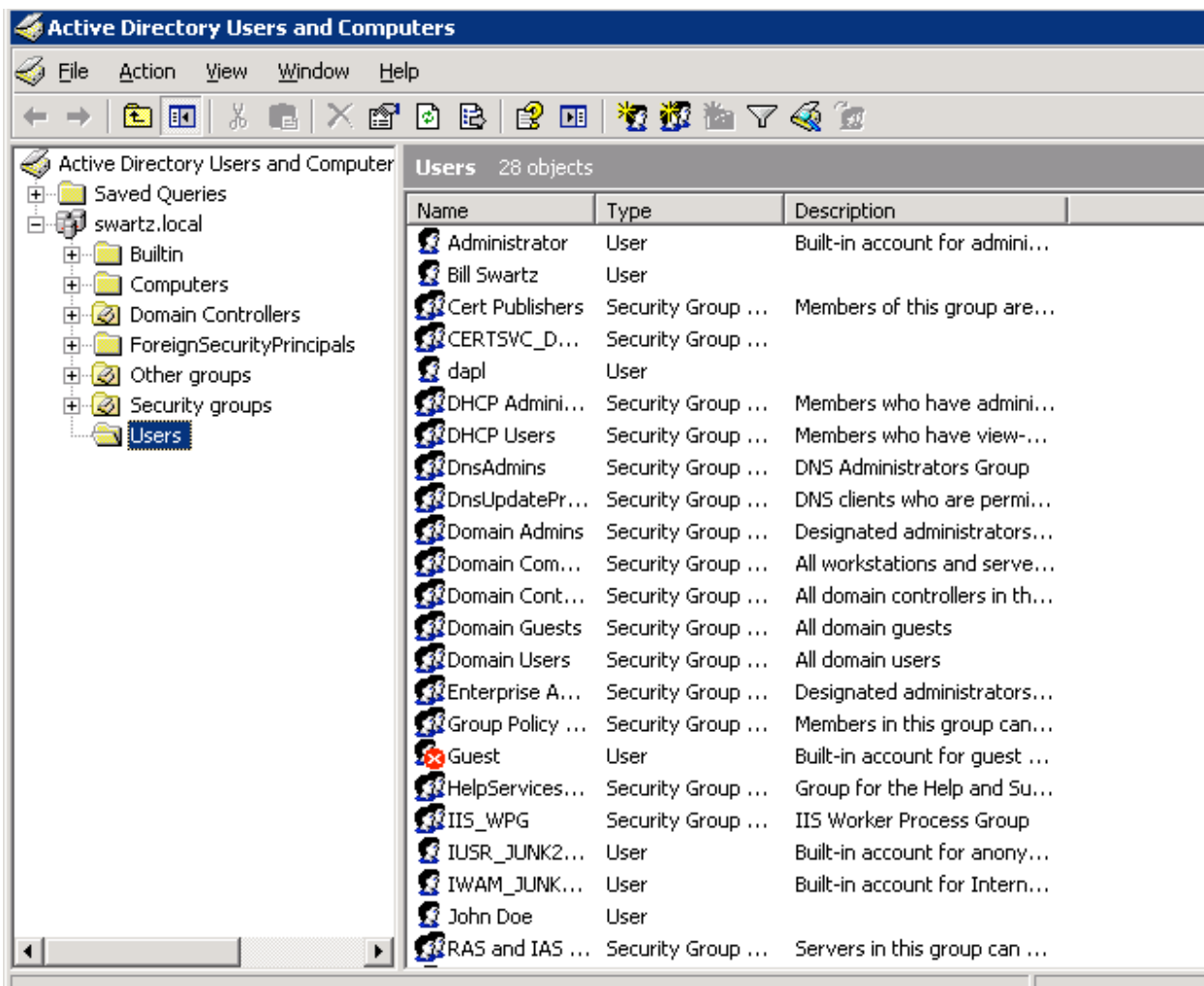
Part 2: Using the LDAP server for authentication with captive portal, SSL VPN, or firewall GUI access

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.

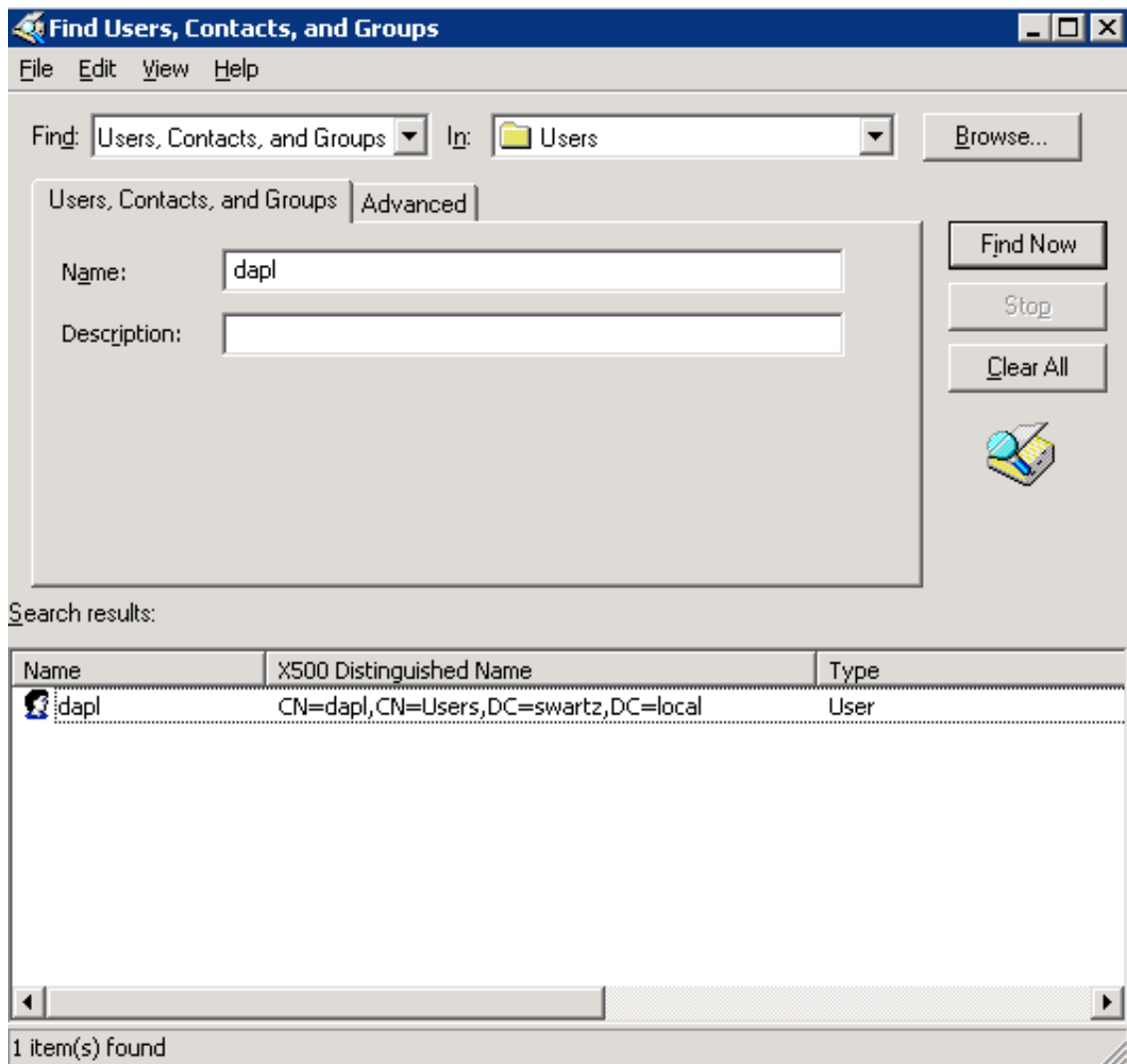
In this example we will connect to Active Directory using LDAP.

1. 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.

Unfortunately we cannot find the **Base** using the method we did for eDirectory. However if you go into Active Directory's Users and Computers you can see the base of the directory. In the example below the base would be **dc=swartz,dc=local**



In order to find **Bind DN** you can do a search for the User while still in Users and Computers then once you get your results from the **View** menu select **Choose Columns**. Add the **X500 distinguished name**. The results would look similar to the following:



With this information we can now finish our configuration.

Edit LDAP Server Profile

Name

Admin Use Only ☐

Base

Bind DN

Bind Password max 63 chars

Confirm Bind Password

SSL ☐

Time Limit (1 - 30) secs

Bind Time Limit (1 - 30) secs

Retry Interval (1 - 3600) secs

	Name	IP Address	Port
#1	NewADServer	192.168.2.55	389
#2	<input type="text"/>	<input type="text"/>	<input type="text"/>
#3	<input type="text"/>	<input type="text"/>	<input type="text"/>
#4	<input type="text"/>	<input type="text"/>	<input type="text"/>

default 389

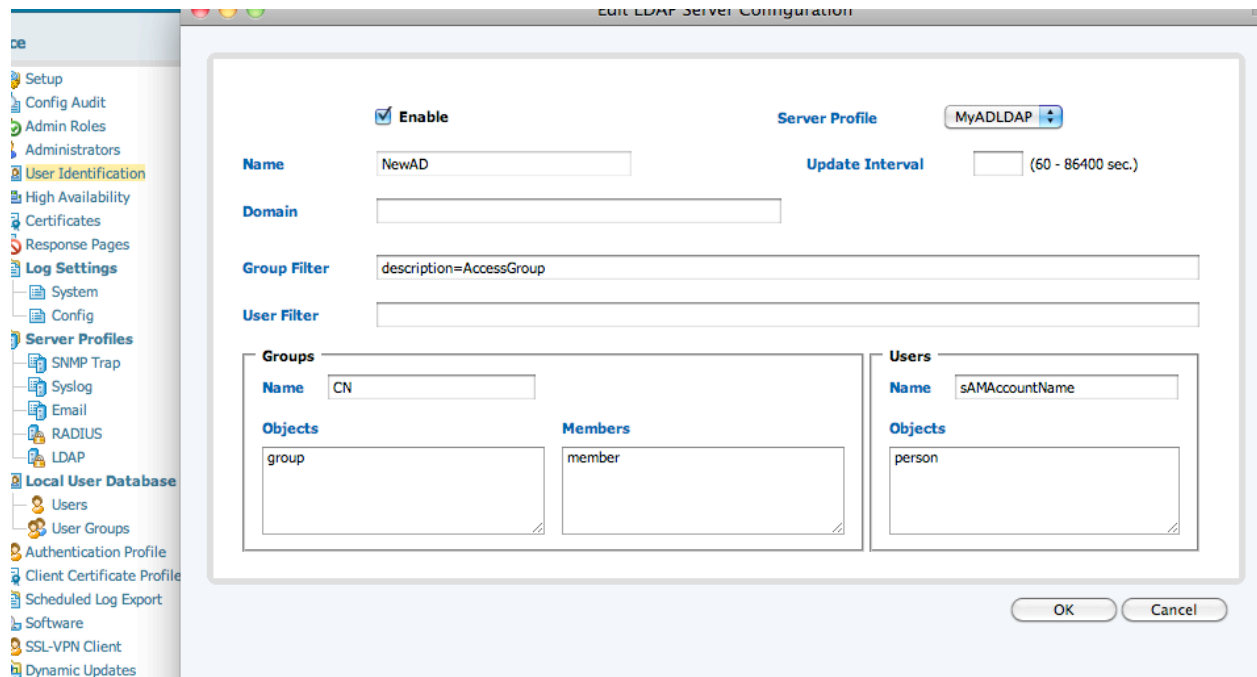
OK Cancel

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.

sAMAccountName corresponds to a user's login name in Active Directory.



Notice the 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

```

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

```

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.

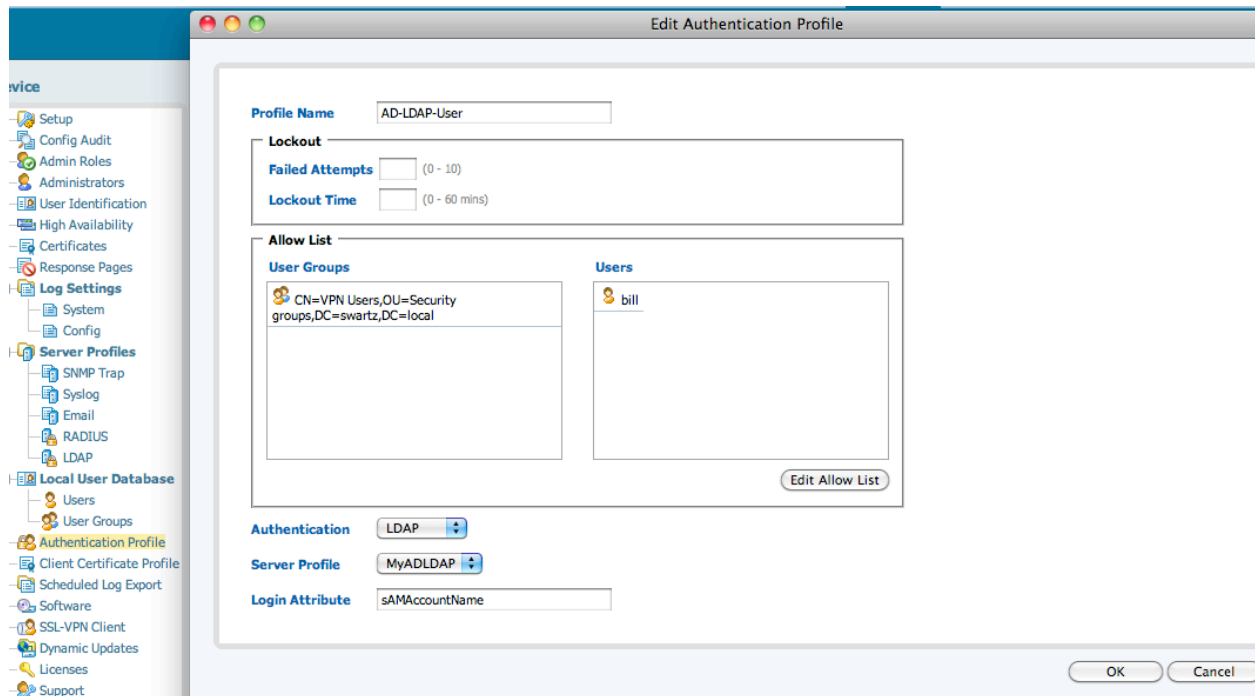
Note: Domain Users is a special group in Active Directory users are tied to it as part of the user schema with the attribute *primaryGroupID*. Members cannot be enumerated via an LDAP query, as the *member* attribute is not set for this group so it cannot be used to learn all of the usernames.

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>

3. 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*.
4. 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.

Appendix A

Overview of the Lightweight Directory Access Protocol

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 in 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

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.

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. Active Directory uses this format.

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

LDAP Browsers

Softerra LDAP Administrator is an excellent LDAP tool for Windows. It can be found at: <http://www.ldapadministrator.com/>. Note that after initial free use you will need to buy it to continue using it.

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

LdapBrowser by IIT Engineering is another free java based browser that can be found here: <http://www.brothersoft.com/ldap-browser-14779.html>