

TechNote

Objective

This document describes how to download, install and use the LDAP Browser as a troubleshooting tool for SonicWALL Email Security. Examples using Microsoft Active Directory are provided throughout this tech note.

Table of Contents

Recommended Version	1
Connecting the LDAP Browser to the LDAP Server	2
Obtaining Information from the LDAP Server	4
Using the LDIF File	5
Using Information from the LDIF File to Modify the LDAP Filter	5
Sample LDIF File	6

Recommended Version

The recommended version of the LDAP Browser is:

- Softerra™ LDAP Browser 2.6

This software is free and can be downloaded at <http://www.ldapadministrator.com/download.htm>

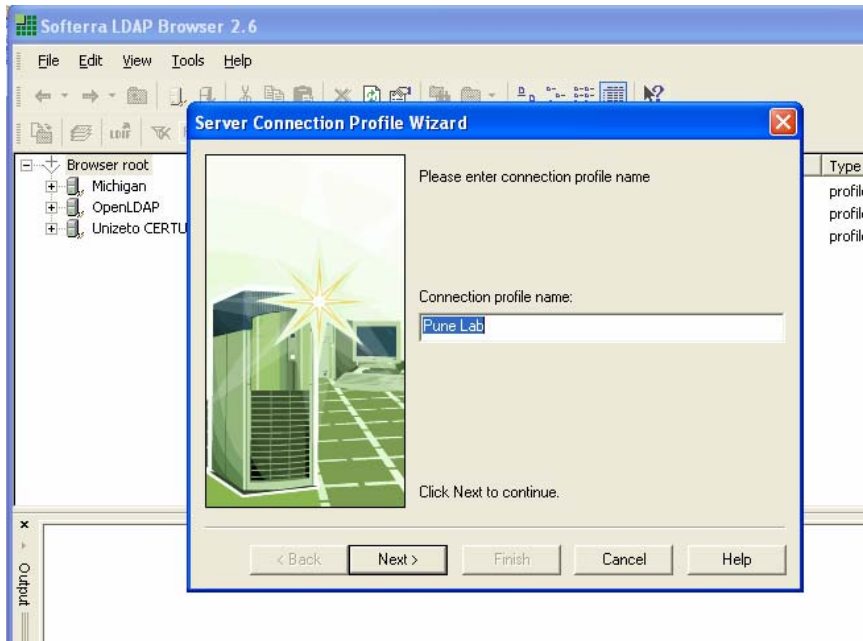


Tech Note

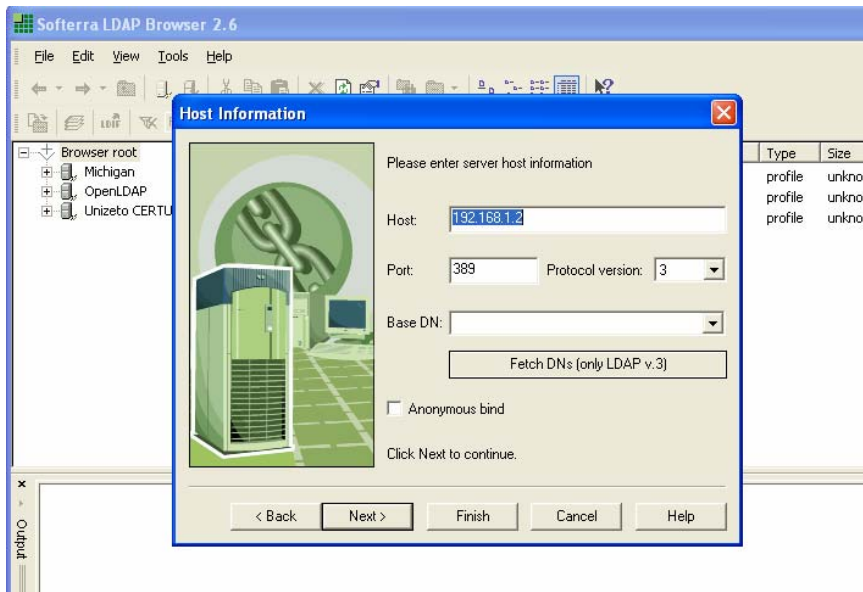
Connecting the LDAP Browser to the LDAP Server

The first step when using the LDAP Browser is to connect to the LDAP server.

1. Install and launch the LDAP Browser.
2. In the LDAP Browser, select **File > New Profile**. The Server Connection Profile Wizard launches.



3. Enter a descriptive name for the profile, and then click **Next**.
4. In the Host field, enter the IP address of the LDAP server.



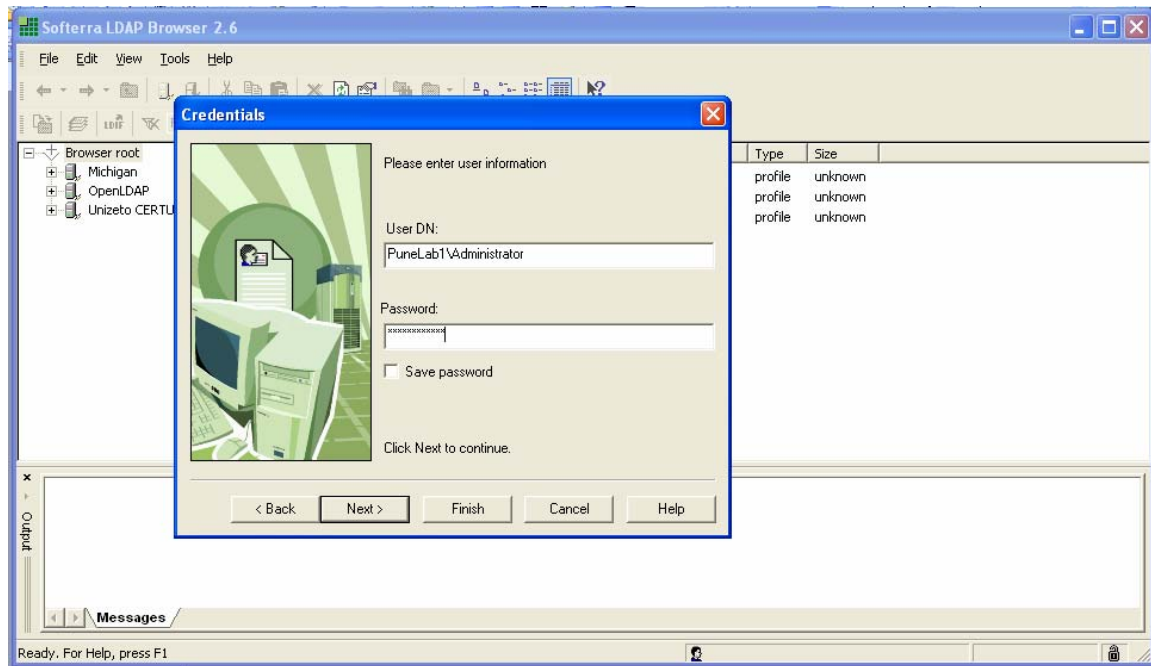
5. In the Port field, enter the port used by the LDAP server. The default LDAP port is **389**, the default LDAPS port is **636**, and the default Active Directory Global Catalog port is **3268**.

Note: Do not insert a base DN; let the software do it for you.

Tech Note

6. Click **Next**.
7. In the User DN field, enter the administrator account name. Some standard login credentials are as follows:
 - Active Directory login credentials: domainname\user_with_admin_rights_on_the_domain_controller
 - Exchange 5.5 login credentials: cn=admin_user_name
 - Domino login credentials: cn= admin_user_name
 - iPlanet/iMail login credentials: anonymous bind

Note: These are standards and are not always followed.



8. In the Password field, enter the administrator account password.
9. Click **Finish**.

Tech Note

Obtaining Information from the LDAP Server

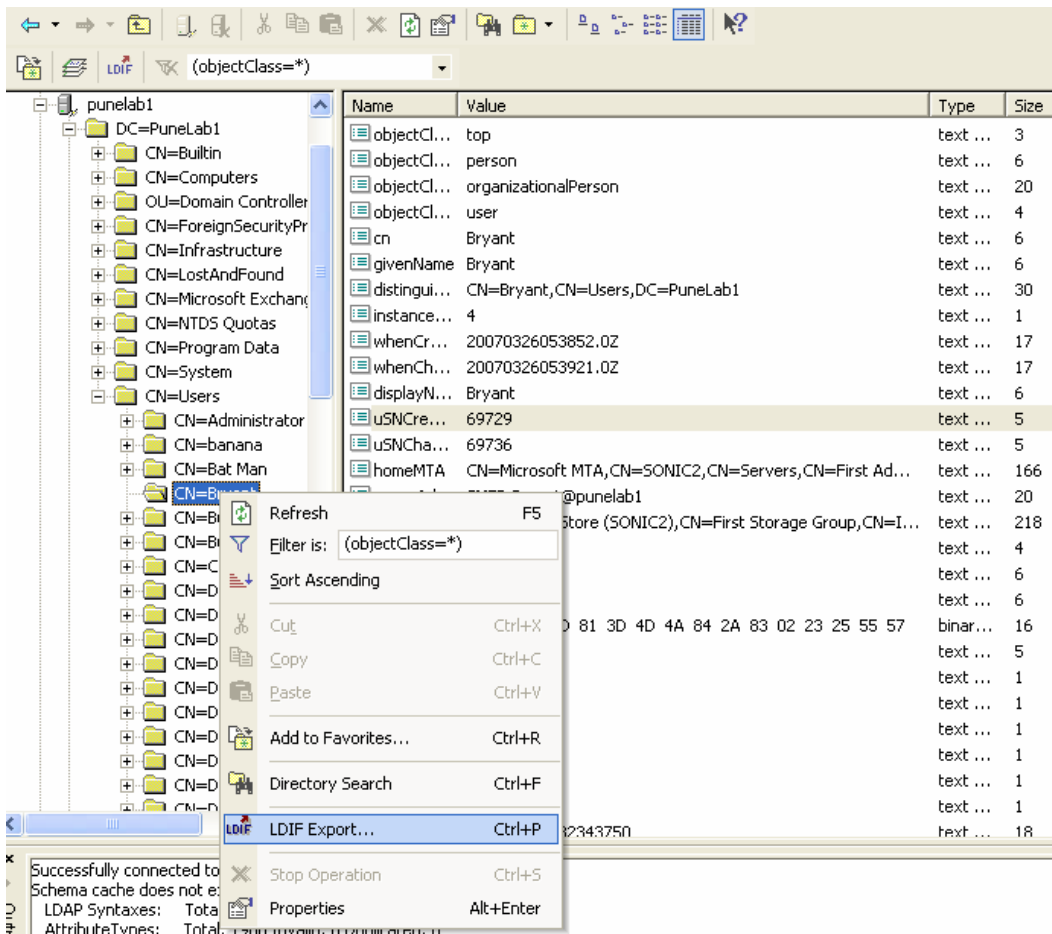
You can use the LDAP Browser to obtain attribute information from the LDAP Server.

The following attributes are available:

- Email attributes:
[mail:bugs.bunny@cartoon.net](mailto:bugs.bunny@cartoon.net)
- Proxy Address (Alias):
proxyaddress: bugs
proxyaddress: bunny
alias: bbunny
alias: bugsy
- Users
- Groups

To find the attributes, perform the following steps:

1. Right-click on a user's folder.
2. In the right-click menu, select **LDIF Export**.



3. In the LDIF Export dialog box, select the default search filter.
4. Click **OK** to export the LDIF file.

Tech Note

Using the LDIF File

Although there are standards, there are no absolute rules for setting up an LDAP server. The administrator may use non-standard labels for attributes or objectClasses.

For example, the administrator may have changed the label for the email attribute to "goofy". In this case,

`mail:bugs.bunny@cartoon.net`

would look like:

`goofy:bugs.bunny@cartoon.net`

By using the LDAP browser you would be able to see this and make the proper changes in the LDAP filter.

Instead of the usual filter such as:

```
(&( |objectClass=group)(objectClass=person)(objectClass=publicFolder))(mail=*)
```

You would change the search filter to:

```
(&( |objectClass=group)(objectClass=person)(objectClass=publicFolder))(goofy=*)
```

Using Information from the LDIF File to Modify the LDAP Filter

The example in this section illustrates how to use the LDIF file to obtain information for use in modifying an LDAP filter.

To view the LDIF file, open it with WordPad.

Scenario

After changes in the status of some employees, the administrator disables some email accounts in Active Directory. However, a SonicWALL LDAP query still lists them as users.

Cause

A Sonicwall Email Security LDAP client cannot tell the difference between an active account and a disabled account in a directory server such as **AD/exchange5.5/Domino**.

If the user is listed in the directory server, the information for that user will be included in the query results.

Investigation

To determine the best way to resolve this situation, perform the following steps:

1. On the client, run the Softerra LDAP Browser.
2. Right-click on the disabled user and export the LDIF file for that user.
3. Export an LDIF file from a user that is not disabled.
4. Compare the LDIF files and search for differences.

In this example, the userAccountControl values are different. The LDIF file shows a userAccountControl value of 66050 for the disabled user, and a userAccountControl of 512 for the active user.

```
userAccountControl: 66050  this is a disabled email account in AD
userAccountControl: 512   this is an enabled email account in AD
```

Resolution

To solve this problem, the search query must be modified.

The default search query is:

```
(&( | (objectClass=group)(objectClass=person)(objectClass=publicFolder))(mail=*)
```

The modified search query is:

```
(&( | (objectClass=group)(objectClass=person)(objectClass=publicFolder))(mail=*)
!(userAccountControl:1.2.840.113556.1.4.803:=(66050)))
```



Tech Note

Sample LDIF File

```
cn: Bryant
givenName: Bryant
distinguishedName: CN=Bryant,CN=Users,DC=PuneLab1
instanceType: 4
whenCreated: 20070326053852.0Z
whenChanged: 20070326053921.0Z
displayName: Bryant
uSNCreated: 69729
uSNChanged: 69736
homeMTA: CN=Microsoft MTA,CN=SONIC2,CN=Servers,CN=First Administrative Group,CN=Administrative
Groups,CN=PuneLab,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=PuneLab1
proxyAddresses: SMTP:Bryant@punelab1
homeMDB: CN=Mailbox Store (SONIC2),CN=First Storage
Group,CN=InformationStore,CN=SONIC2,CN=Servers,CN=First Administrative Group,CN=Administrative
Groups,CN=PuneLab,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=PuneLab1
mDBUseDefaults: TRUE
mailNickname: Bryant
name: Bryant
objectGUID:: f5fefYE9TUqEKoMClyVVVw==
userAccountControl: 66048
badPwdCount: 0
codePage: 0
countryCode: 0
badPasswordTime: 0
lastLogoff: 0
lastLogon: 0
pwdLastSet: 128193611332343750
primaryGroupID: 513
objectSid:: AQUAAAAAAAAUVAAAAZSPmHcpKwwQHlxbmhAQAAA==
accountExpires: 9223372036854775807
logonCount: 0
sAMAccountName: Bryant
sAMAccountType: 805306368
legacyExchangeDN: /o=PuneLab/ou=First Administrative Group/cn=Recipients/cn=Bryant
userPrincipalName: Bryant@PuneLab1
objectCategory: CN=Person,CN=Schema,CN=Configuration,DC=PuneLab1
mail: Bryant@punelab1
msExchHomeServerName: /o=PuneLab/ou=First Administrative Group/cn=Configuration/cn=Servers/cn=SONIC2
msExchMailboxSecurityDescriptor::
AQAEgHgAAACUAAAAAAAAABQAAAAEAGQAAQAAAAACFAADAAIAAQEAAAAAAAAUKAAAAAAAAAFMAYwBo
AGUAbQBhACwAQwAAAQAAAAEAAAEEAAAAGAAAAQByAGEAdABpAG8AbgAsAEQAQwA9AFAAdQBuAGUA
TABhAGIAAQUAAAAAAAAUVAAAAZSPmHcpKwwQHlxbm9AEAAAEFAAAAAAFFQAAAGUj5h3KSsMEByMW
5vQBAAA=
msExchMailboxGuid:: n5/tcl+uz0qEyoVYrzs0lw==
```

Last modified: 9/11/07

