LDAP Authentication on IIS

By Jan-Michael Ong (jmong@adobe.com)
10/6/2002 2:02PM

Instructions originally written by Ram Rajadhyaksha (ramr@inflectiontech.com). I then rewrote them, added snapshots and command line examples.

Summary:

The following is a step-by-step guide on installing and configuring an IIS LDAP module.

This document assumes that you have a fully functional LDAP server that allows you to do anonymous binds. (The IISLDAP_AUTH module itself allows you to bind as a specific user when connecting to the LDAP service using the BINDUSER directive in the ldapauth.ini properties file but that is not covered in this document.)

Very special thanks:

I am greatly indebted to Ram Rajadhyaksha's support and kindness. If it wasn't for his help and e-mails I'll still be banging my head on the monitor and you probably wouldn't be reading this document ☺

Getting started:

There are three major steps before we should get going on our journey to Never-never land.

- Identifying system requirements
- Checking for existing libraries
- Going grocery shopping

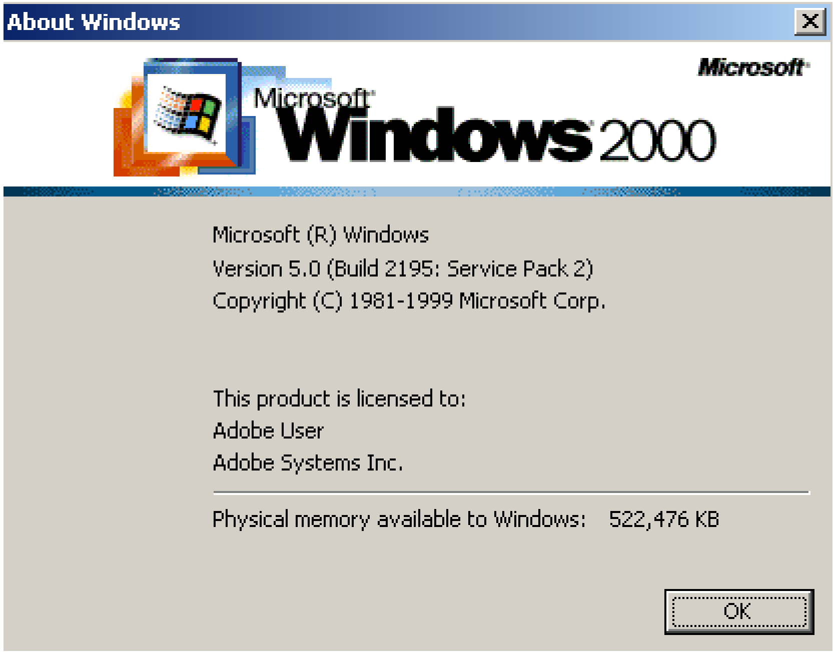
Identifying system requirements:
For the most part, I will assume that you have a similar environment to what I have (see below).

Build Environment:
Operating System
Microsoft Windows 2000 Professional
Version 5.0 (Build 2195: Service Pack 2)

LDAP Server
Solaris 2.7
OpenLDAP 2.0.25
DB 3.3.11

While the author has noted that it should work on Windows 2000 variants (Professional/Server/Advanced Server), I have yet to test it on either Server or Advanced Server. (So no guarantees okay? ☺)

For those Windoze-impared users (like myself), the fastest way to check your Windows version is by going Start → Run → and type winver. A window similar to image below will show up.



Microsoft (R) Windows
Version 5.0 (Build 2195: Service Pack 2)
Copyright (C) 1981-1999 Microsoft Corp.

This product is licensed to:
Adobe User
Adobe Systems Inc.

Physical memory available to Windows: 522,476 KB

To check your OpenLDAP server version, you can ask your LDAP administrator (which is me in our case) or bribe him with lots of cash to give you super user access ☺

One way to find out the OpenLDAP version is to start slapd with debug level 1 (most verbose).

```
root@pinnacle$ /etc/init.d/slapd debug
starting slapd in debug mode: 1
@(#) $OpenLDAP: slapd 2.0.25-Release (Tue Jul 30 15:10:19 PDT 2002) $
        @pinnacle:/work/openldap-2.0.25/servers/slapd
daemon_init: listen on ldap://pinnacle:389/
daemon_init: 1 listeners to open...
…
```

Checking for existing libraries

Now that we have the right system requirements, we have to make sure that there are no stray (read “old”) library files that may interfere with our installation.

The fastest ways to look for these guys is to just run a search on the following files:

```
lib*.dll
```

This will probably return gobs and gobs of DLLs. But make sure to pay attention to the following:

```
libnspr3.dll
libplc3.dll
libnspr4.dll
libplc4.dll
libplds4.dll
```

For the most part, you can safely ignore the lib*4.dll since these will be overwritten later. Also they should only appear once! If they appear more than once, make sure to keep the version in C:\WINNT\system32 (or change your PATH environment variable so that C:\WINNT\system32 is the first on the list)

However, for the lib*3.dll, these are old libraries and should be removed. (I spent a day on this trying to figure out why the ldap tools were complaining of old libraries … well duh, its because it was finding these on %PATH% and it was using this to run the searches… more on this later)

To remove them, you'll probably have to log onto Windows in Safe Mode. Check out this article on how to do that for Windows 2000:

http://www.quickbooks.com/support/faqs/qbw2000/118383.html

Going grocery shopping
Alright, you've made it this far so you must be

a.) a masochist
b.) really bored and have nothing better to do.

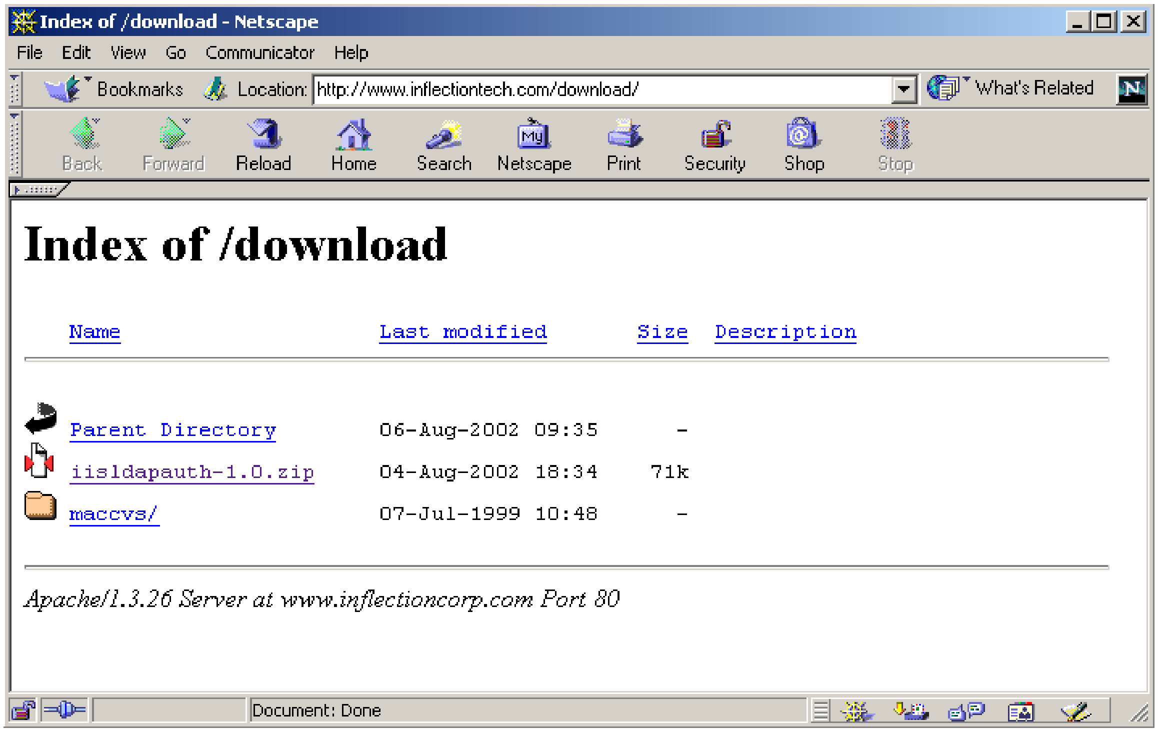
Well, assuming that you READ these instructions very carefully and that you have the same build/setup as I have then it should be a breeze.

We need to pick up a few things before we can actually get cranking.

First, you will need the IIS LDAP module from InflectionTech.

http://www.inflectiontech.com/download/

At the time of this writing, I downloaded iisldapauth-1.0.zip (see Figure 1)



Location: http://www.inflectiontech.com/download/

Index of /download

```
    Name                      Last modified       Size  Description

    Parent Directory          06-Aug-2002 09:35      -
    iisldapauth-1.0.zip       04-Aug-2002 18:34     71k
    maccvs/                   07-Jul-1999 10:48      -
```

Apache/1.3.26 Server at www.inflectioncorp.com Port 80

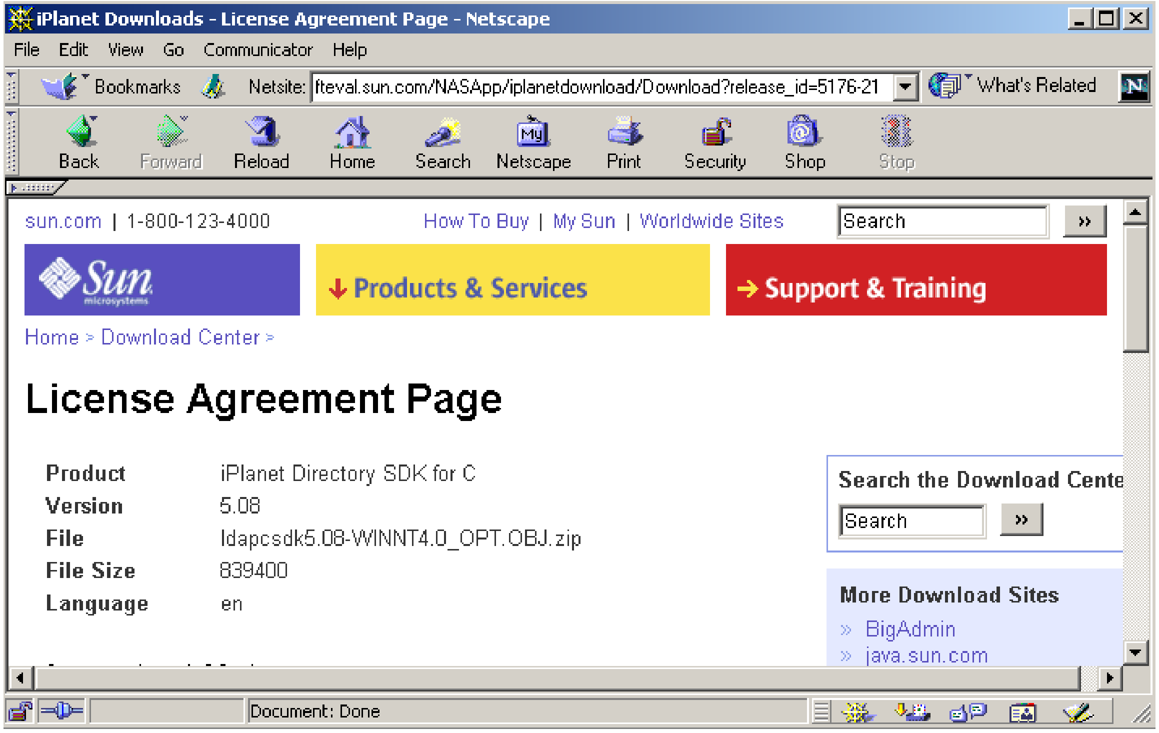
Document: Done

Figure 1 Download ldapauth.dll from inflectiontech.com

Next, you will need to visit Sun's website to pick up the iPlanet LDAP SDK. You probably will need to register first (if you haven't already), to pick up the files.

http://softeval.sun.com/NASApp/iplanetdownload/Download?release_id=5176-21

(see Figure 2)


iPlanet Downloads - License Agreement Page - Netscape
File Edit View Go Communicator Help
Bookmarks
What's Related
Back Forward Reload Home Search Netscape Print Security Shop Stop
sun.com | 1-800-123-4000
How To Buy | My Sun | Worldwide Sites
Search »
Sun microsystems
Products & Services
Support & Training
Home > Download Center >
Search the Download Cente
Search »
More Download Sites
» BigAdmin
» java.sun.com
Document: Done

Netsite: fteval.sun.com/NASApp/iplanetdownload/Download?release_id=5176-21

License Agreement Page

Product	iPlanet Directory SDK for C
Version	5.08
File	ldapcsdk5.08-WINNT4.0_OPT.OBJ.zip
File Size	839400
Language	en

Figure 2 Pick up the Netscape/iPlanet LDAP SDK 5.08 for WinNT 4.0

Preparing the IIS LDAP module

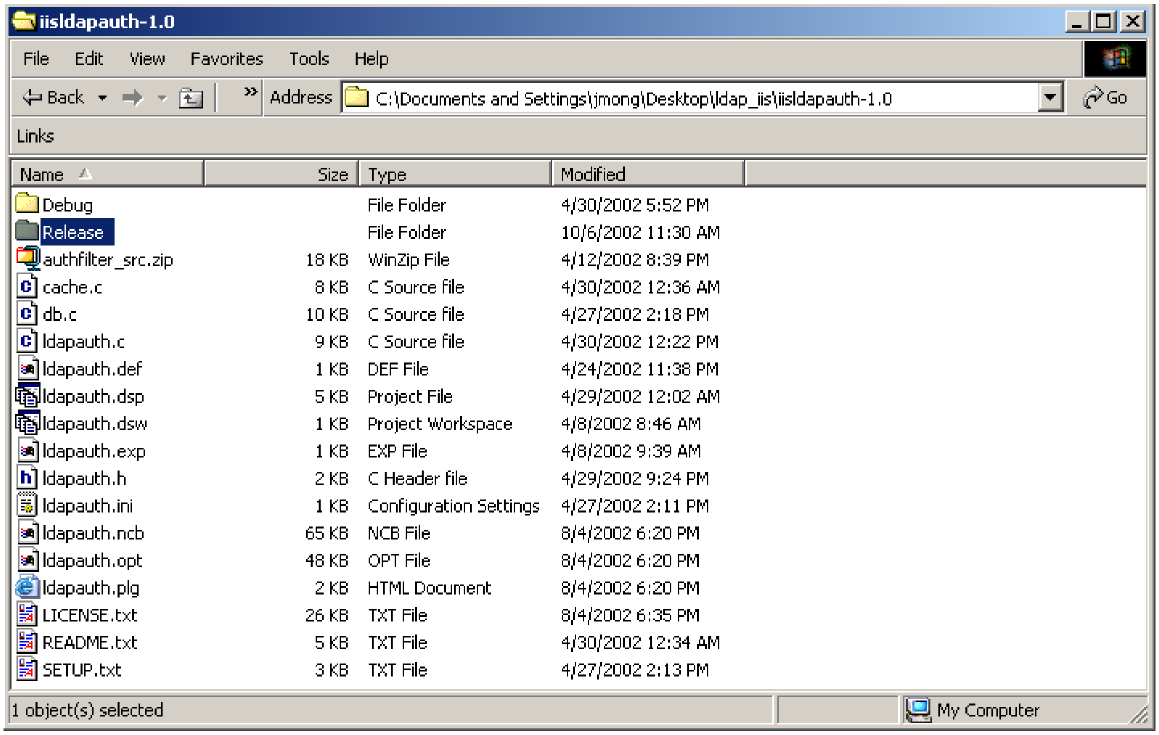
Once we've downloaded all the proper ingredients, we need to put the various components into their places.

1. Unzip the necessary files.

(Tip: Unzip the two zipped files onto your desktop and create separate directories for each of them. I called mine

```
ldap_iis\iisldapauth-1.0
ldap_iis\ldapcsdk5.08-Wint4.0
```

Also note, that I highlighted Release (Figure 3) and lib (Figure 4)on each of the images below. We will be working with these directories later)

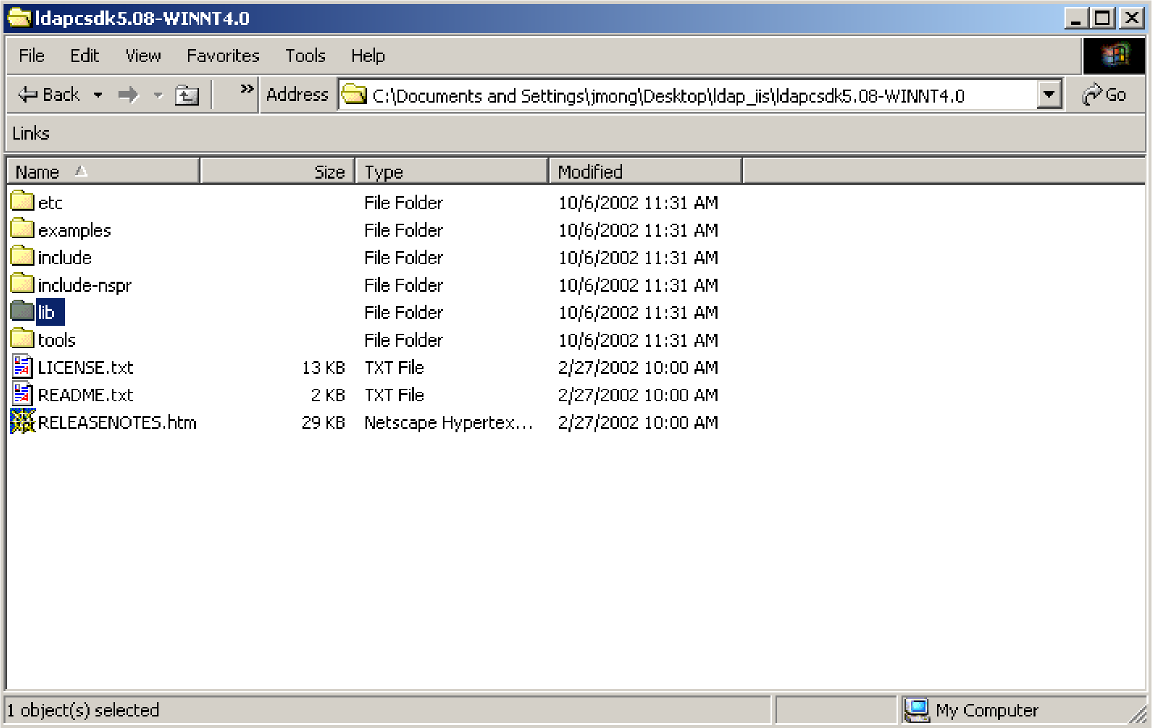


Address: C:\Documents and Settings\jmong\Desktop\ldap_iis\iisldapauth-1.0

Name	Size	Type	Modified
Debug		File Folder	4/30/2002 5:52 PM
Release		File Folder	10/6/2002 11:30 AM
authfilter_src.zip	18 KB	WinZip File	4/12/2002 8:39 PM
cache.c	8 KB	C Source file	4/30/2002 12:36 AM
db.c	10 KB	C Source file	4/27/2002 2:18 PM
ldapauth.c	9 KB	C Source file	4/30/2002 12:22 PM
ldapauth.def	1 KB	DEF File	4/24/2002 11:38 PM
ldapauth.dsp	5 KB	Project File	4/29/2002 12:02 AM
ldapauth.dsw	1 KB	Project Workspace	4/8/2002 8:46 AM
ldapauth.exp	1 KB	EXP File	4/8/2002 9:39 AM
ldapauth.h	2 KB	C Header file	4/29/2002 9:24 PM
ldapauth.ini	1 KB	Configuration Settings	4/27/2002 2:11 PM
ldapauth.ncb	65 KB	NCB File	8/4/2002 6:20 PM
ldapauth.opt	48 KB	OPT File	8/4/2002 6:20 PM
ldapauth.plg	2 KB	HTML Document	8/4/2002 6:20 PM
LICENSE.txt	26 KB	TXT File	8/4/2002 6:35 PM
README.txt	5 KB	TXT File	4/30/2002 12:34 AM
SETUP.txt	3 KB	TXT File	4/27/2002 2:13 PM

1 object(s) selected

Figure 3 We'll be working with Release\ldapauth.dll later



Address: C:\Documents and Settings\jmong\Desktop\ldap_iis\ldapcsdk5.08-WINNT4.0

Name	Size	Type	Modified
etc		File Folder	10/6/2002 11:31 AM
examples		File Folder	10/6/2002 11:31 AM
include		File Folder	10/6/2002 11:31 AM
include-nspr		File Folder	10/6/2002 11:31 AM
lib		File Folder	10/6/2002 11:31 AM
tools		File Folder	10/6/2002 11:31 AM
LICENSE.txt	13 KB	TXT File	2/27/2002 10:00 AM
README.txt	2 KB	TXT File	2/27/2002 10:00 AM
RELEASENOTES.htm	29 KB	Netscape Hypertex...	2/27/2002 10:00 AM

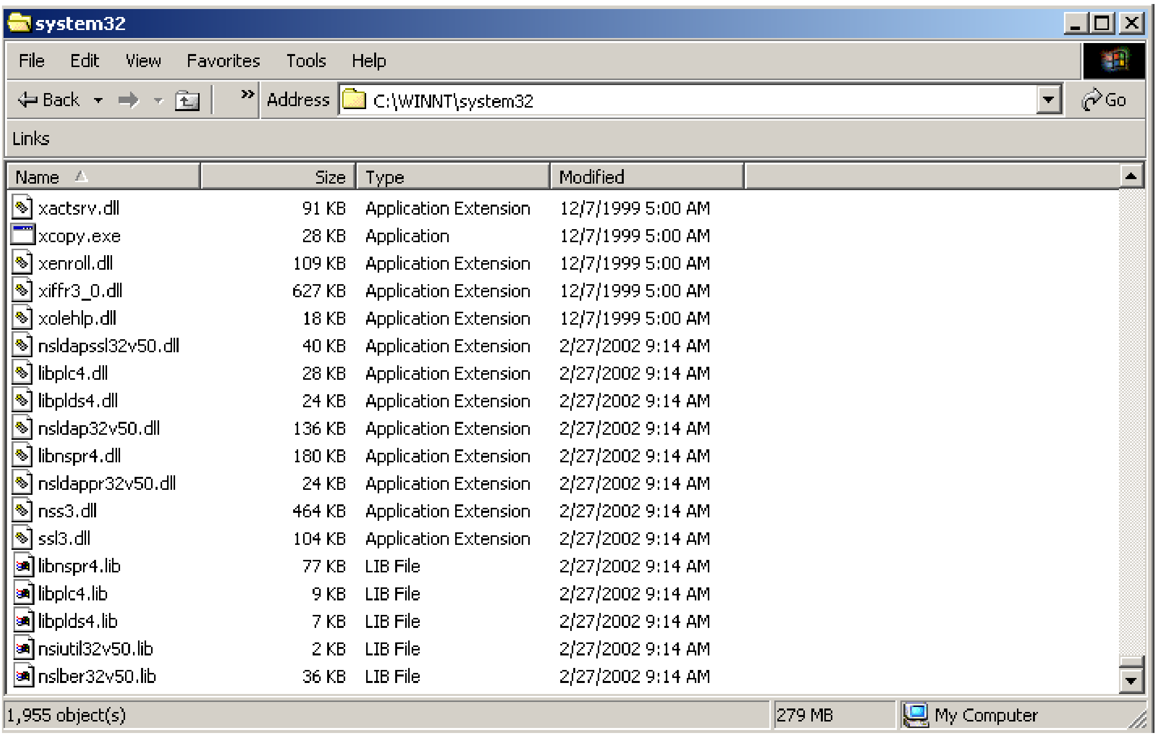
1 object(s) selected

Figure 4 We will copy lib* to C:\WINNT\System32\ in the next step

2. Copy everything from the Sun LDAP SDK’s lib directory into your WINNT\System32 folder.

```
copy c:\documents and settings\jmong\desktop\ldap_iis\ldapcsdk5.08-Wint4.0\lib\*
c:\winnt\system32
```

(I suspect that we don’t need to copy the *.lib stuff since that’s mostly UNIX but for the purposes of this guide, we’ll just leave them there). At this point your C:\WINNT\System32 directory should look like the figure below (Figure 5)



Name	Size	Type	Modified
xactsrv.dll	91 KB	Application Extension	12/7/1999 5:00 AM
xcopy.exe	28 KB	Application	12/7/1999 5:00 AM
xenroll.dll	109 KB	Application Extension	12/7/1999 5:00 AM
xiffr3_0.dll	627 KB	Application Extension	12/7/1999 5:00 AM
xolehlp.dll	18 KB	Application Extension	12/7/1999 5:00 AM
nsldapssl32v50.dll	40 KB	Application Extension	2/27/2002 9:14 AM
libplc4.dll	28 KB	Application Extension	2/27/2002 9:14 AM
libplds4.dll	24 KB	Application Extension	2/27/2002 9:14 AM
nsldap32v50.dll	136 KB	Application Extension	2/27/2002 9:14 AM
libnspr4.dll	180 KB	Application Extension	2/27/2002 9:14 AM
nsldappr32v50.dll	24 KB	Application Extension	2/27/2002 9:14 AM
nss3.dll	464 KB	Application Extension	2/27/2002 9:14 AM
ssl3.dll	104 KB	Application Extension	2/27/2002 9:14 AM
libnspr4.lib	77 KB	LIB File	2/27/2002 9:14 AM
libplc4.lib	9 KB	LIB File	2/27/2002 9:14 AM
libplds4.lib	7 KB	LIB File	2/27/2002 9:14 AM
nsiutil32v50.lib	2 KB	LIB File	2/27/2002 9:14 AM
nslber32v50.lib	36 KB	LIB File	2/27/2002 9:14 AM

Figure 5 After copying the Netscape SDKs into C:\WINNT\System32

3. After we’ve installed the necessary DLLs into C:\winnt\system32, we need to ensure that we can use these newly installed libraries to connection to our target LDAP server. This step is essential since IIS might not necessarily throw errors and we’ll be scratching our heads for days. As the author said [in an e-mail to me] “If there are any DLL dependency related problems, it will just fail to load and IIS will give no indication as to why”

The general usage for Netscape’s ldapsearch is:

```
ldapsearch –h target ldap server –b basedn “ldapfilter”
```

So in my case, I did the following:

```
cd C:\Documents and Settings\jmong\Desktop\ldap_iis>cd ldapcsdk5.08-WINNT4.0\tools

C:\Documents and Settings\jmong\Desktop\ldap_iis\ldapcsdk5.08-WINNT4.0\tools>ldapsearch -
h 153.32.2.92 -b "o=My Company" "cn=jmong"
version: 1
dn: cn=jmong,ou=Weird,ou=Engineer,o=My Company
```

```
…
```

Assuming that you've specified a valid filter, the search should return any viewable attributes as defined by your LDAP server. If you get something like the following:

```
C:\Documents and Settings\jmong\Desktop\ldap_iis\ldapcsdk5.08-WINNT4.0\tools>ldapsearch
ldapsearch: this program requires an LDAP library that implements revision
         2005 or greater of the LDAP API; running with revision 2004
```

You might want to check your PATH and run a search again for lib*.dll. It's possible that ldapsearch is still encountering old libraries somewhere.

(Note: If you want to increase your brain mass, you might want to read the following: http://docs.sun.com/source/816-5617-10/ that talks about the error noted above)

Whatever you do, do not proceed past this step until you get this working!

4. After our successful search, we will need to install the ldapauth.dll into our IIS ISAPI filters directory or C:\WINNT\System32\inetsrv.

```
Cd C:\Documents and Settings\jmong\Desktop\ldap_iis\iisldapauth-1.0\Release>dir
 Volume in drive C has no label.
 Volume Serial Number is 5489-6EB6

 Directory of C:\Documents and Settings\jmong\Desktop\ldap_iis\iisldapauth-1.0\Release

10/06/2002  11:30a      <DIR>          .
10/06/2002  11:30a      <DIR>          ..
08/04/2002  06:20p              45,056 ldapauth.dll
               1 File(s)         45,056 bytes
               2 Dir(s)   1,977,679,360 bytes free

C:\Documents and Settings\jmong\Desktop\ldap_iis\iisldapauth-1.0\Release>copy ld
apauth.dll c:\winnt\system32\inetsrv
```

We're almost done with MS-DOS/command line stuff so hang in there! ☺

5. Using your favorite text editor, create an appropriate ldapauth.ini file and save this in C:\WINNT\ldapauth.ini.

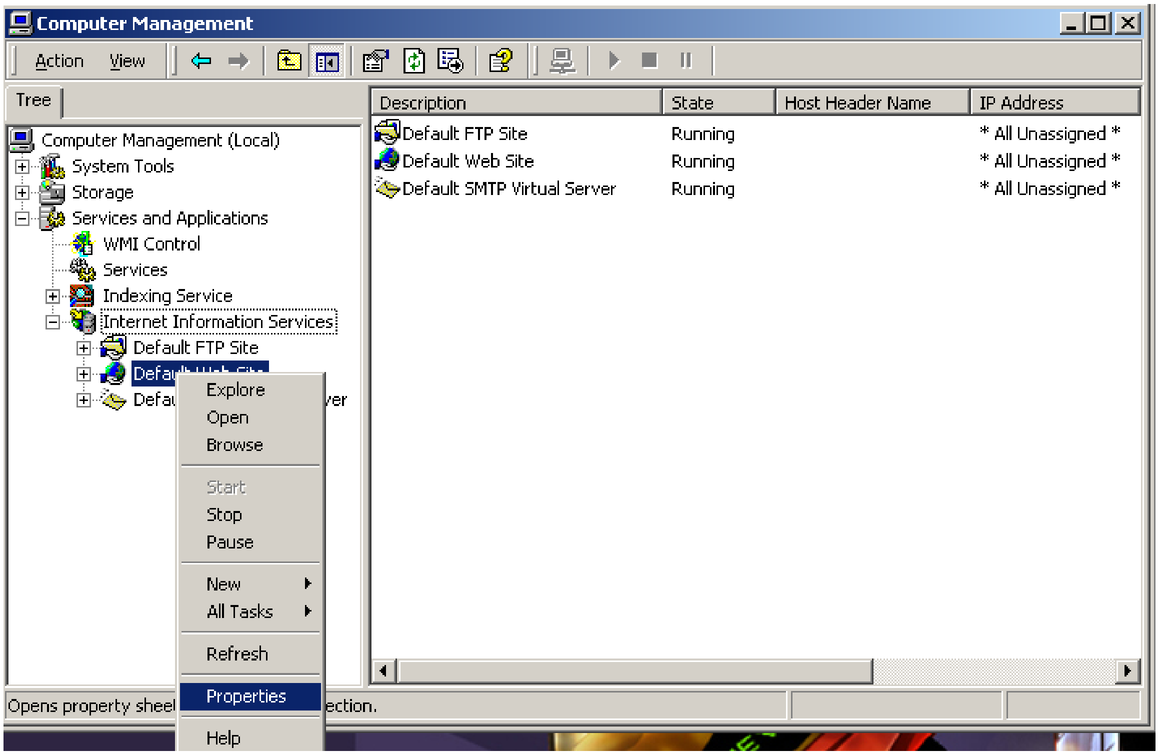
```
LDAPHOST       153.32.2.92
LDAPFILTER     (objectClass=*)
LDAPUID        cn
SEARCHBASE     o=My_Company
NTUSER         jmong
NTUSERPASSWORD secret
```

For details regarding the format, additional directives and other information regarding the ldapauth.ini file, please consult the INSTALL.TXT file. If there is an error in the configuration file, you will probably see an error in the eventlog:

```
The HTTP Filter DLL C:\WINNT\system32\inetsrv\ldapauth.dll failed to load.  The data is
the error.
For additional information specific to this message please visit the Microsoft Online
Support site located at: http://www.microsoft.com/contentredirect.asp.
```

6. Add the ldapauth module in IIS.

On your desktop, right click on “My Computer”
Select “Manage”
The “Computer Management” window will pop-up
Double-click on “Services and Applications”
Right click on “Default Web Site” (at this point your window should look somewhat like the Figure 6)



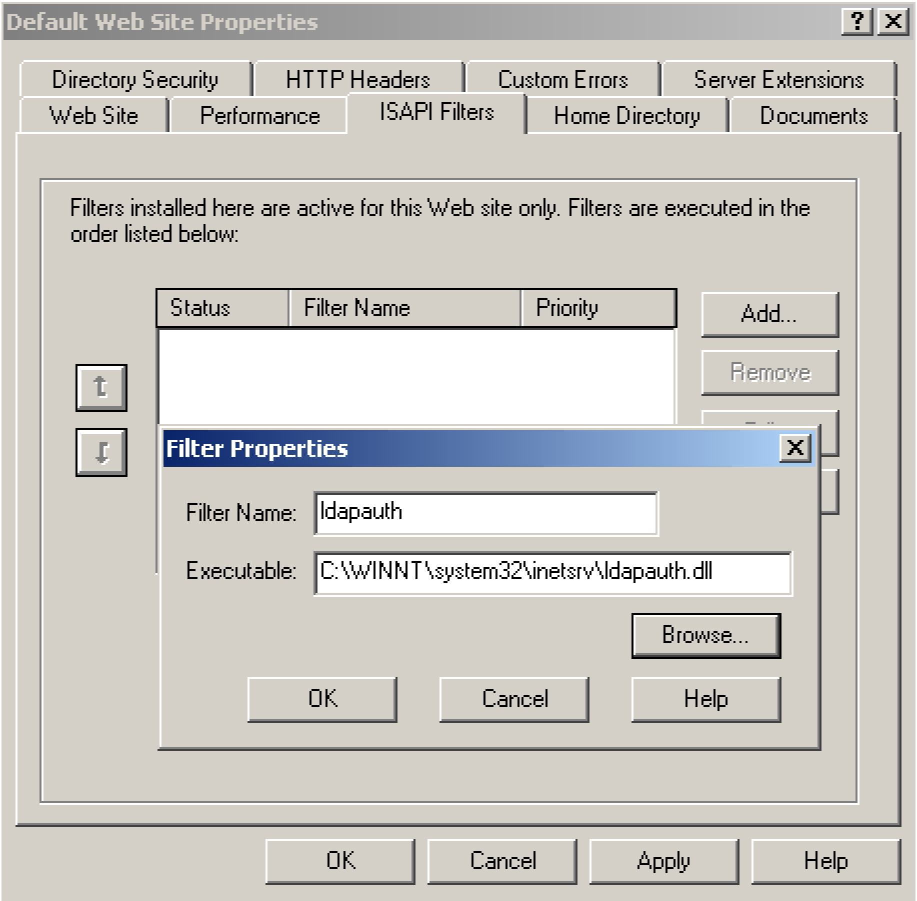
Description	State	Host Header Name	IP Address
Default FTP Site	Running		* All Unassigned *
Default Web Site	Running		* All Unassigned *
Default SMTP Virtual Server	Running		* All Unassigned *

Figure 6 After right-clicking on "Default Web Site"

Choose “Properties”
Click on the “ISAPI Filters” tab.
Click “Add”
The “Filter Properties” should pop up and enter the following information

Filter Name: ldapauth
Executable: C:\WINNT\System32\inetsrv\ldapauth.dll

(Figure 7)



Filters installed here are active for this Web site only. Filters are executed in the order listed below:

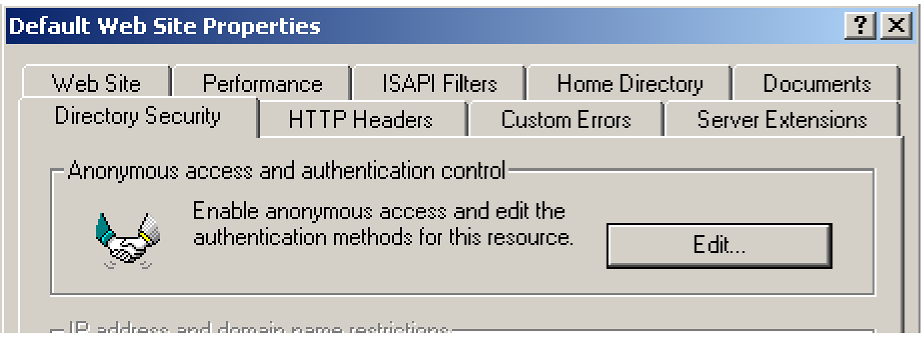
Filter Name: ldapauth

Executable: C:\WINNT\system32\inetsrv\ldapauth.dll

Figure 7 Creating the ldapauth filter for IIS

7. Enable Basic Authentication

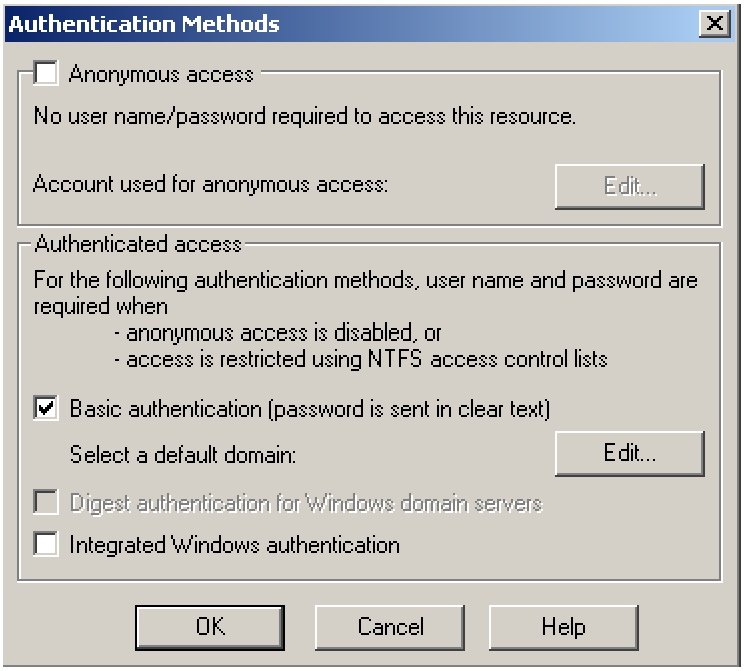
Click on the “Directory Security” tab
Select “Edit” in the “Anonymous access and authentication control” text panel. (Figure 8)



Enable anonymous access and edit the authentication methods for this resource.

Figure 8 Click on "Edit" button

Disable “Anonymous access” and “Integrated Windows authentication”
Check on “Basic authentication” and select “OK” when the warning about clear text passwords is displayed. (Figure 9)


Authentication Methods

☐ Anonymous access

No user name/password required to access this resource.

Account used for anonymous access:

Authenticated access

For the following authentication methods, user name and password are required when
- anonymous access is disabled, or
- access is restricted using NTFS access control lists

☑ Basic authentication (password is sent in clear text)

Select a default domain:

☐ Digest authentication for Windows domain servers

☐ Integrated Windows authentication

Figure 9 Disable Integrated Windows auth and anonymous access. Enable Basic auth!

8. Stop and restart the IIS web service

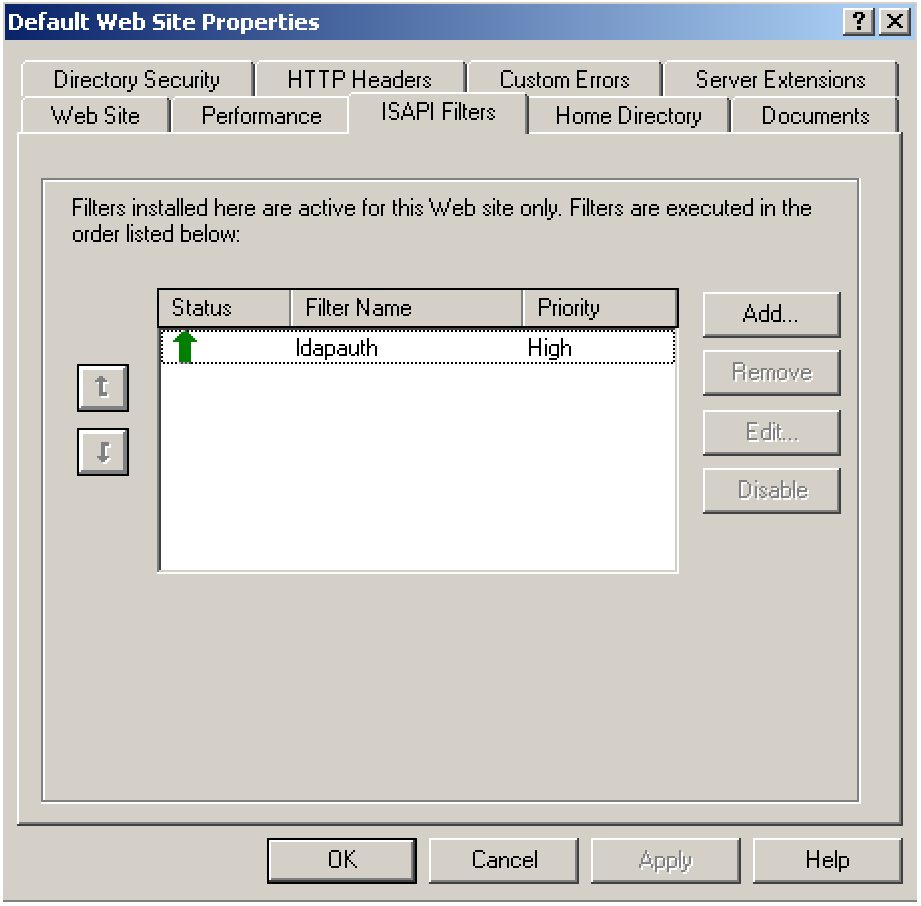
```
C:\Documents and Settings\jmong\Desktop\ldap_iis\iisldapauth-1.0\Release>net stop w3svc
The World Wide Web Publishing Service service is stopping.
The World Wide Web Publishing Service service was stopped successfully.

C:\Documents and Settings\jmong\Desktop\ldap_iis\iisldapauth-1.0\Release>net start w3svc
The World Wide Web Publishing Service service is starting..
The World Wide Web Publishing Service service was started successfully.
```

You can also do this from the IIS GUI but why? We already have a Command Shell window open so might as well put it into good use ☺

9. Check ldapauth filter

Verify that the ldapauth module loaded properly. It should display something similar to the figure below. (Figure 10)



Filters installed here are active for this Web site only. Filters are executed in the order listed below:

Status	Filter Name	Priority
🟩	ldapauth	High

Figure 10 ldapauth filter loaded successfully!!

If you get a "red arrow" (rather than a green one), check Event Viewer for clues. The following are likely culprits:

- spaces in ldapauth.ini
- you've specified an invalid location for ldapauth.dll
- the ldapauth.dll is corrupt
- the Sun/iPlanet/Netscape SDK libraries are not in your PATH somehow (if you specified a different location) or you have conflicting versions

10. Check to see everything is working

Once its loaded, you should be able to authenticate with your LDAP server. Here is a sample log snippet, from when I accessed a protected IIS directory

```
Oct  6 12:13:23 pinnacle slapd[6299]: daemon: conn=1 fd=10 connection from
IP=153.32.140.107:1174 (IP=0.0.0.0:389) accepted.
Oct  6 12:13:23 pinnacle slapd[6299]: conn=1 op=0 BIND dn="" method=128
Oct  6 12:13:23 pinnacle slapd[6299]: conn=1 op=0 RESULT tag=97 err=0 text=
Oct  6 12:13:23 pinnacle slapd[6299]: conn=1 op=1 SRCH base="o=My Company" scope=2
filter="(&(cn=jmong)(objectClass=*))"
Oct  6 12:13:23 pinnacle slapd[6299]: conn=1 op=1 SEARCH RESULT tag=101 err=0 text=
Oct  6 12:13:23 pinnacle slapd[6299]: conn=1 op=2 BIND
dn="CN=JMONG,OU=WEIRD,OU=ENGINEER,O=MY COMPANY" method=128
Oct  6 12:13:23 pinnacle slapd[6299]: conn=1 op=2 RESULT tag=97 err=0 text=
Oct  6 12:13:23 pinnacle slapd[6299]: conn=1 op=3 UNBIND
Oct  6 12:13:23 pinnacle slapd[6299]: conn=-1 fd=10 closed
```

That's it! (Pat yourself in the back and ask your manager for a raise ^_^)

Hopefully that wasn't too painful. Like the authors noted in README/SETUP, you probably want to do a lot of praying before, during and after the installation.

Good luck!

Additional notes:

(These are notes that I've picked out from my email correspondence with Ram Rajadhyaksha)

9/27/2002

1. SSL support does not work at this time. The SSL calls in the LDAP library fail for an unknown reason.
2. Make sure BASIC authentication is enabled, disable NTLM.
3. Try a NTUSER value on the NT box that is an administrator, if that works you have a permissions problem.

The NTUSER/NTPASSWORD are required because IIS still needs a valid account for handling permissions. So either you have to setup the same set of accounts in your NT environment as your LDAP server or you can have all LDAP accounts "transformed" to one NT account.

You don't have to specify the NTUSER value- if you omit it, the module will use whatever username was typed into the password challenge box.

If the module is loaded but users are still not authenticating, make sure the NT users are either part of the Administrator group OR you have enabled "Log On Locally" rights for that user.

http://support.microsoft.com/default.aspx?scid=KB;EN-US;q142868&