OpenSSL for IIS / Apache on Windows 2003

Enable LDAPS on Windows IIS / Apache

This guide is assuming that PHP and IIS / Apache has been installed and setup.

will need to generate a stand alone CA (you will need permission to do this by the enterprise admin) generate keys and change:
Properties
Select any CSP but strong certificate and the key length to 1024
Click next and add the name of the computer to the server info i.e. ActiveDIR
Select the output path to c:/
Click next to finish…
Go to run
Type mmc
Open the snap-in Certificates and select computer account.
Local account for computer and click on:
Personal > Certificates
There will be a certificate in there under ActiveDIR
Right click on the folder Certificates > all tasks and request new certificate.
Run thought the wizard to create new certificate.
You can double click on the certificate (do both to see the difference)
The new one will say in general proves your identity to a remote computer
This is the certificate that we need.
Right click on the new certificate and export.
Export as Base 64.
Give it a file name (anything you want but without spaces, for this example SSL)
And save to the c:
Open up c:/ you will have 2 certificates one called ActiveDIR.domain and the other call other openssl.cer

You will need to install OpenSSL or jump on a unix box (OSX).

openssl x509 –in drag the export1 file from the desktop –out drag the export1 file from the desktop and rename openssl.pem

So the path in our case will be:

```
openssl x509 –in /private/root/Desktop/ldaps.cer –out
/private/root/Desktop/openssl.pem
```

(assuming you are logged in as root)

(Note When copying the certificate around insure that it is safe as the Domain Controller will assume that anything that comes from the certificate is trusted)

Delete the openssl.cer from the unix box.

On the Windows web server create the following folder structure in the root of C:

C:\OpenLDAP\sysconf\

With text pad (or word pad) create a file called ldap.conf

Add the following text

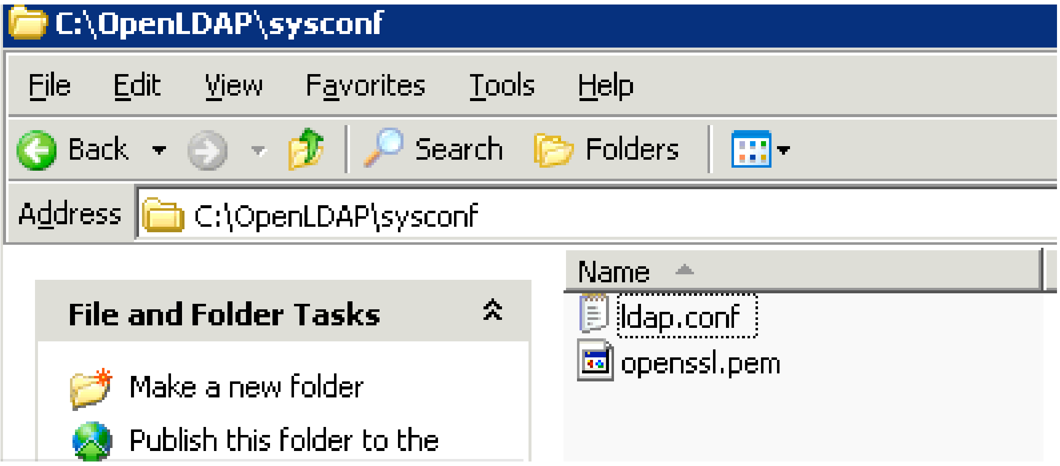
TLS_REQCERT never

#define location of CA certificate
TLS_CACERT C:\OpenLDAP\sysconf\openssl.pem
TLS_CACERTDIR C:\OpenLDAP\sysconf\

Save the file to your newly created path:

C:\OpenLDAP\sysconf\open.ssl.conf

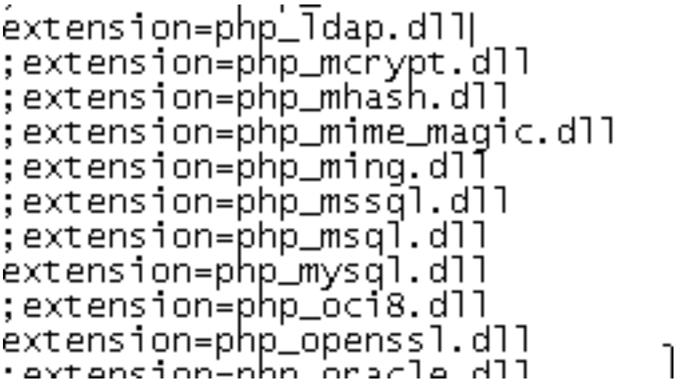
Your new pem certificate will need to go into the same place.



ldap.conf
openssl.pem

(remember to delete any cases of the pem file if copying the file around)

open up the php.ini file



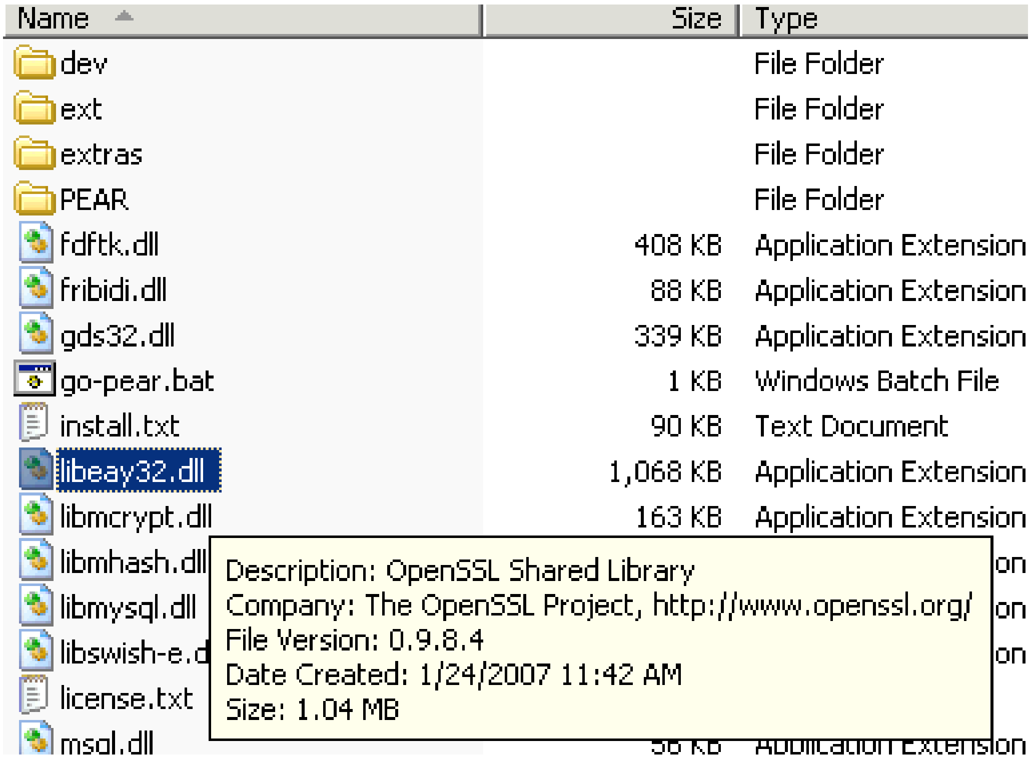
```
extension=php_ldap.dll
;extension=php_mcrypt.dll
;extension=php_mhash.dll
;extension=php_mime_magic.dll
;extension=php_ming.dll
;extension=php_mssql.dll
;extension=php_msql.dll
extension=php_mysql.dll
;extension=php_oci8.dll
extension=php_openssl.dll
;extension=php_oracle.dll
```

check that the two extentions ;

extension=php_ldap.dll

```
extension=php_openssl.dll
```

are switched on.



Name	Size	Type
dev		File Folder
ext		File Folder
extras		File Folder
PEAR		File Folder
fdftk.dll	408 KB	Application Extension
fribidi.dll	88 KB	Application Extension
gds32.dll	339 KB	Application Extension
go-pear.bat	1 KB	Windows Batch File
install.txt	90 KB	Text Document
libeay32.dll	1,068 KB	Application Extension
libmcrypt.dll	163 KB	Application Extension
libmhash.dll		on
libmysql.dll		on
libswish-e.d		on
license.txt		
msql.dll	56 KB	Application Extension

Description: OpenSSL Shared Library
Company: The OpenSSL Project, http://www.openssl.org/
File Version: 0.9.8.4
Date Created: 1/24/2007 11:42 AM
Size: 1.04 MB

copy the libeay32.dll file (from the PHP installed location i.e. c:\php)

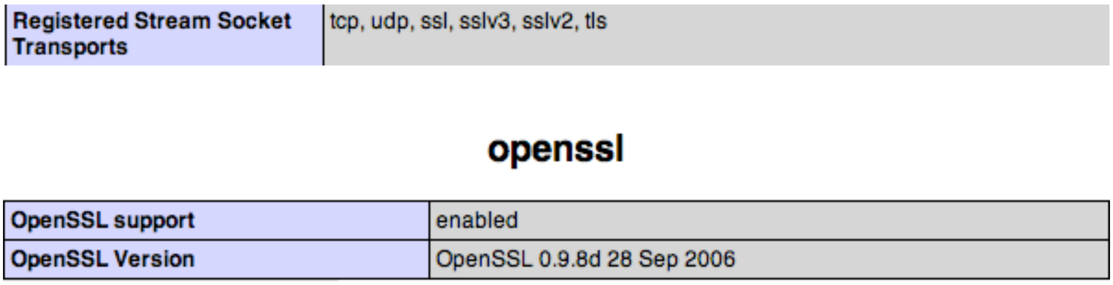
to C:\Windows\System32 or C:\WINNIT\System32 folder

Restart your web services.

Use

```
<?php
 phpinfo()
?>
```

to check that OpenSSL is running.

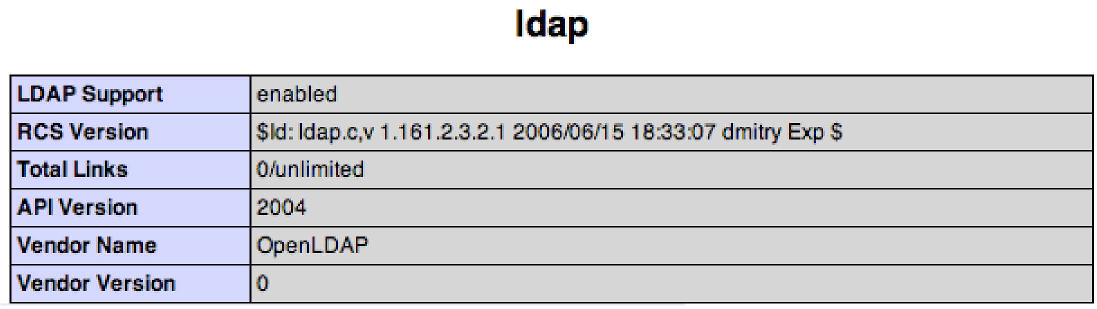


Registered Stream Socket Transports	tcp, udp, ssl, sslv3, sslv2, tls

openssl

OpenSSL support	enabled
OpenSSL Version	OpenSSL 0.9.8d 28 Sep 2006

Check that LDAP is also running.



ldap

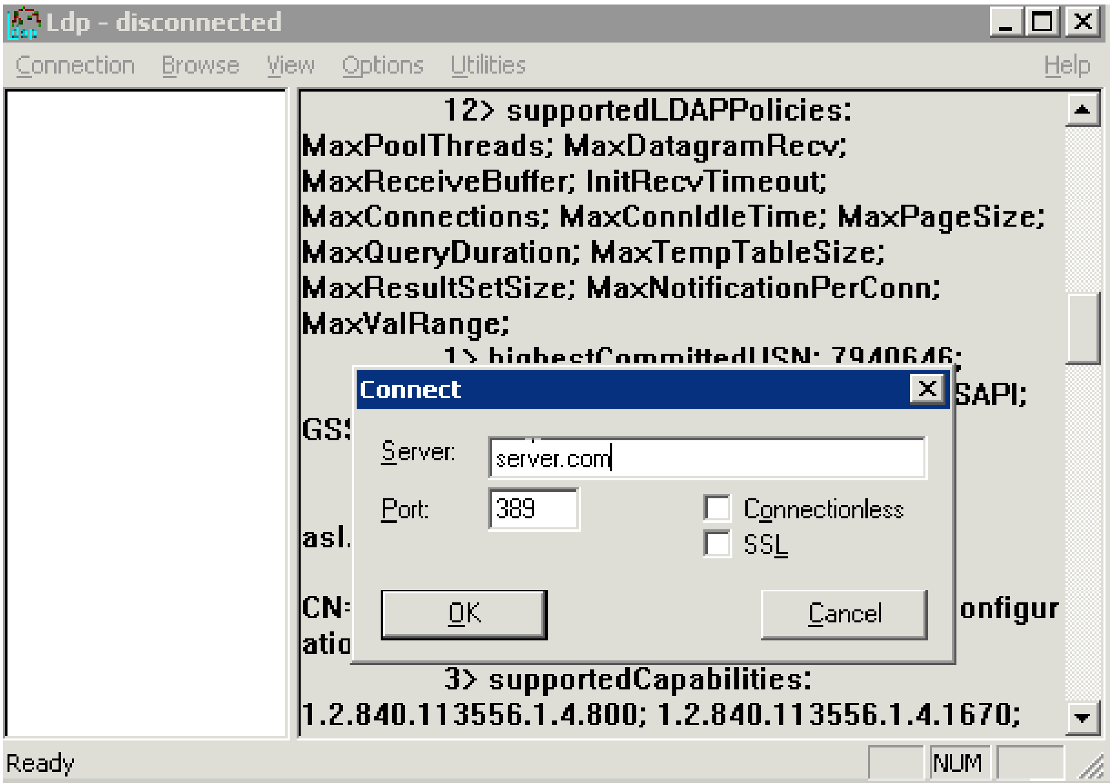
LDAP Support	enabled
RCS Version	$Id: ldap.c,v 1.161.2.3.2.1 2006/06/15 18:33:07 dmitry Exp $
Total Links	0/unlimited
API Version	2004
Vendor Name	OpenLDAP
Vendor Version	0

Create a quick ldaps script to check your conections

```
<?php

$ad = “ldaps://domain”
//i.e. ldaps://dc1.server.com or ldaps://asl.org

$au = “username@domain
//i.e. username of a domain admin (it would be worth creating a limited admin
//for this)
$pass = “password” //Password of the above username

$Connect = ldap_connect($ad)
or die(“Could not connect);

ldap_set_option($Connect,  LDAP_OPT_PROTOCOL_VERSION, 3)
or die (“Could not set ldap protocol”);

$Bind = ldap_bind($Connect, $au, $pass);
if ($Bind) echo “You have a ldaps connection);

else echo “No ldaps connection please check settings”;

?>
```

If you do have problems please check that you can connect to the remote server with LDAP.

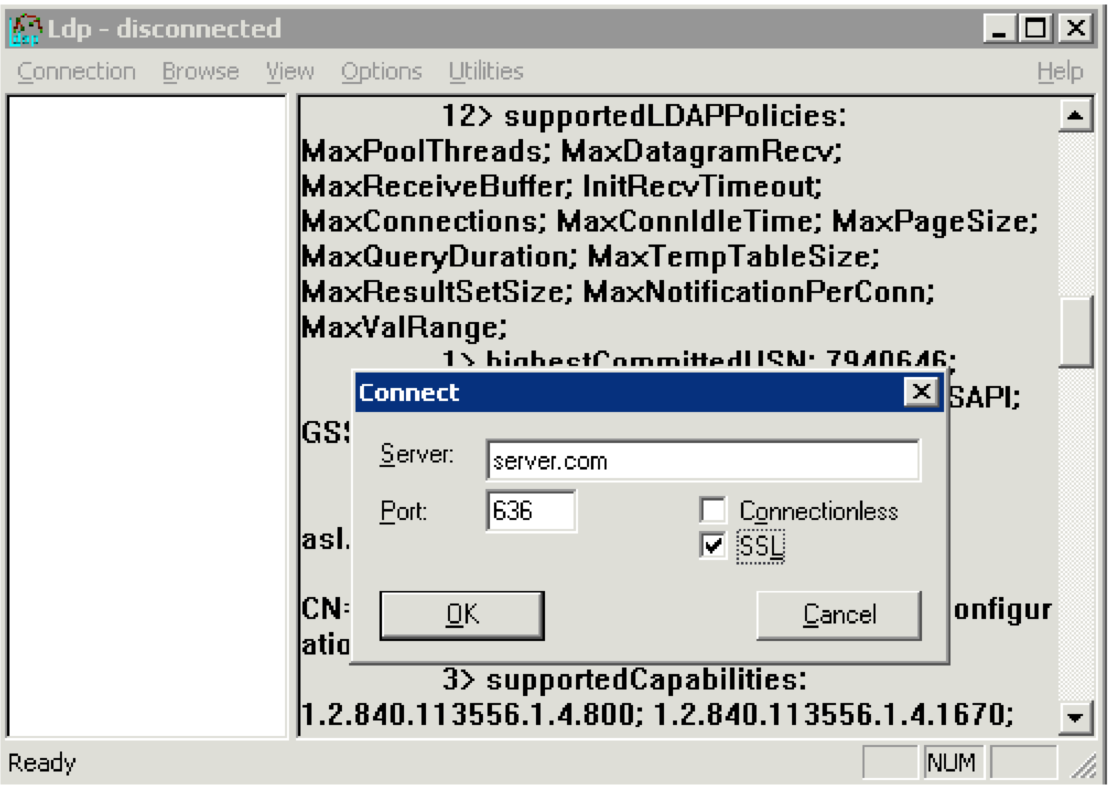
Use Microsoft’s ldp.exe to check your connections



```
          12> supportedLDAPPolicies:
MaxPoolThreads; MaxDatagramRecv;
MaxReceiveBuffer; InitRecvTimeout;
MaxConnections; MaxConnIdleTime; MaxPageSize;
MaxQueryDuration; MaxTempTableSize;
MaxResultSetSize; MaxNotificationPerConn;
MaxValRange;
          1> highestCommittedUSN: 7940646;
                                              SAPI;
GS
asl.
CN=                                           onfigur
atio
          3> supportedCapabilities:
1.2.840.113556.1.4.800; 1.2.840.113556.1.4.1670;
```

Server: server.com

Port: 389 □ Connectionless □ SSL



```
          12> supportedLDAPPolicies:
MaxPoolThreads; MaxDatagramRecv;
MaxReceiveBuffer; InitRecvTimeout;
MaxConnections; MaxConnIdleTime; MaxPageSize;
MaxQueryDuration; MaxTempTableSize;
MaxResultSetSize; MaxNotificationPerConn;
MaxValRange;
          1> highestCommittedUSN: 7940646;
                                              SAPI;
GS
asl.
CN=                                           onfigur
atio
          3> supportedCapabilities:
1.2.840.113556.1.4.800; 1.2.840.113556.1.4.1670;
```

Server: server.com

Port: 636 □ Connectionless ☑ SSL

By Dominic Carpenter
www.apple-scripts.com