

## SSL For port 636

By Dominic Carpenter  
www.apple-scripts.com

### Secure connections

There is several ways to do this:

If you are a Enterprise Admin you can Create Enterprise root Certificate if you are not you 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 through 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 SSL.cer

Login as root on the OSX server (or your Unix server)

On OSX copy SSL.cer to the desktop.

Open the Terminal and type:

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

so the path in our case will be

```
openssl x509 -in /private/root/Desktop/ssl.cer -out /private/root/Desktop/ssl.pem
```

press enter

you will have a new file on the desktop called SSL.pem  
copy this file to system > library > openssl > certs folder

in the Terminal type:

c\_rehash

we can test the certificate by typing  
openssl verify and drag the file SSL.pem from the certs folder to terminal and press enter.  
You should get a message saying OK.

How ever if you get a message saying:

Error 20 at 0 depth lookup:unable to get local issuer certificate.

Don't worry.

Open up the folder private > etc > openldap > openldap.conf  
And make sure that the line

TLS\_REQCERT says never  
Type the following

```
#define location of CA certificate  
TLS_CACERT /System/Library/Openssl/certs/SSL.pem  
TLS_CACERTDIR /System/Library/Openssl/certs
```

**Openssl s\_client -connect 192.168.1.5:636**

We will have a page of results returned.  
Which at the bottom will confirm a SSL 128bit connection.  
Now we are ready to test the connection

Type:

**Ldapsearch -H ldaps://192.168.1.5**

And press enter

We will now be prompted for a password enter a password or press enter.  
The connection will fail as we are using a IP address in the ldapsearch as apposed  
to a name with out a bind.  
But it has asked us for a password so we know that the server has a connection.

If you had this error before

Error 20 at 0 depth lookup:unable to get local issuer certificate.

Type this:

**openssl s\_client -connect 1.1.1.1:636 -state**

\*\* 1.1.1.1 is a example IP please replace with you Active Directory IP

**ldapsearch -H ldaps://192.168.1.5**

**you should now have a secure conection.**

By Dominic Carpenter  
[www.apple-scripts.com](http://www.apple-scripts.com)