

White Paper: Securing aeSLAPD with Stunnel

Overview

Encryption support for aeSLAPD can be provided via “**stunnel**” the multi-platform SSL Tunnel that uses OpenSSL. Stunnel is a “wrapper” that allows TCP messages to be encapsulated in SSL for secure exchange between an SSL-capable client and the non-encrypted server. In the example, aeSLAPD is running on port 389, and SSL is setup on port 636., with a BaseDN of o=Airius.com..

References

- STUNNEL.ORG
<http://stunnel.org>
- HP Paper: Securing LDAP with Stunnel
http://h21007.www2.hp.com/dspp/tech/tech_TechDocumentDetailPage_IDX/1,1701,4002,00.html

Steps:

1. Obtain **stunnel** from <http://stunnel.mirt.net> and **OpenSSL**. Both can be downloaded from: <http://stunnel.mirt.net/downloads.html>
2. Setup the **stunnel.conf** configuration file. An example of the Windows configuration is:

```
service = stunnel
cert = stunnel.pem.txt

[ldaps]
connect = 127.0.0.1:389
accept = localhost:636
```

3. Note that the **stunnel.pem.txt** file is a certificate that can be generated with the “openssl” program, or online at: <http://www.stunnel.org/pem/>
4. Run stunnel (or on Windows, install it as a service).
5. Make a query to the clear port 389. For example, with Internet Explorer:
`ldap://localhost:389/o=Airius.com??sub?(cn=Dir*)`

6. Make the same query over the secure port 636, with an “ldaps” URL capable utility, or, with Internet Explorer, for example.:

```
ldap://localhost:636/o=Airius.com??sub?(cn=Dir*)
```

7. In both 5 and 6, the results should show the default Directory Manager output:

```
dn: cn=Directory Manager, o=Airius.com
objectclass: top
objectclass: person
objectclass: organizationalPerson
objectclass: inetOrgPerson
cn: Directory Manager
cn: Directory
cn: Manager
givenname: Directory
sn: Manager
mail: manager@localhost
telephonenumber: 411
```