Experian Pandora
Using LDAP Help File

Version 5.9, 5.8

LDAP (Lightweight Directory Access Protocol)

Working with Microsoft Active Directory

Active Directory (AD) is Microsoft's implementation of an LDAP server. Its underlying authentication mechanism is Kerberos.
Note that Pandora only uses AD's authentication Mechanism, not its authorisation.
When you are using LDAP (or Kerberos) authentication and go to create a Pandora user, you do not set a password in Pandora as this is managed in LDAP itself.

The Pandora 'administrator' user must tell Pandora which LDAP users have access to Pandora. Pandora administrators still need to create Pandora users in the normal way, and during this process they link the Pandora username to the LDAP username.

The Pandora server associates the Pandora username and the AD username at the time a user logs in, as the relevent AD username and password are sent to AD for authentication checks.

Usernames

Usernames may be referred to by **Distinguished Name** (DN), **Universal Principal Name** (UPN) or **Service Principal Name** (SPN). For explanation of these terms refer to;
http://blogs.msdn.com/b/openspecification/archive/2009/07/10/understanding-unique-attributes-in-active-directory.aspx

Other vendor's LDAP servers use the DN to refer to username, however since AD uses Kerberos as its authentication mechanism, AD may also refer to username as a UPN (i.e. Internet email format).

Which format to use is site dependent and you should ask your LDAP system administrator for the relevant username format (DN or UPN – typically it will be the UPN format).

For the sake of convenience, the Pandora Client will allow you to select the authentication mechanism as 'LDAP and MS Active Directory Server'. These mechanisms are identical – the only difference between the two is the format in which you specify the username. If you are using LDAP you must specify a Distinguished Name, if you are using AD you must specify a UPN.

Security

A representation of the user's password is stored in the LDAP server. The mechanism (i.e. algorithm) that is used to create this representation is well defined, although its implementation is not. For this reason, the most common security mechanism is SIMPLE.
The mechanism may be defined on a per user basis, however the Pandora server assumes that all users have the same mechanism. You must ask your LDAP system administrator which one has been defined.

The SIMPLE mechanism expects you to authenticate by providing a username (DN or UPN) and a clear text password. Note that Pandora never stores this password. It is encrypted between the Pandora Client and Pandora Server then transmitted over a secure connection (using SSL) between the Pandora Server and the LDAP server.

Configuring

When you configure the LDAP server in Pandora you specify a URL that consists of a protocol, hostname and port. A typical URL may resemble;

- ldap://localhost:389
- ldaps://localhost:636

The first (protocol = “ldap”) is insecure and you must use the LDAP server’s insecure port.
The second is secure (protocol = “ldaps”) and you must use the LDAP server’s secure port.

Do not specify a URL that uses the insecure protocol (ldap) with the secure port or the secure protocol (ldaps) with the insecure port. If you use a secure port, then check with your LDAP system administrator that the LDAP server has been configured to use this port.

If you get “connection refused” errors then this implies that the URL is wrong (invalid host name, invalid port number or a combination of the two).

Under most circumstances, it is easiest to use the insecure protocol since the Pandora Server layers a secure connection on top of the insecure one (this means it is exactly equivalent to using the secure protocol).