NetIQ eDirectory

There are two eDirectory databases -- IDTREE and AUTHTREE. Use AUTHTREE for simple authentication needs (euid, password, employee/student status). More complex needs may require access to the IDTREE database.

Search Base: ou=people,o=unt

IDTREE: ldaps://ldap-id.untsystem.edu (load-balanced across both datacenters)

IMPORTANT: Clients within a datacenter **MUST** use their local LDAP service.

- GAB datacenter clients **must** use ldaps://ldap-id.gabdcn.unt.edu
- DP datacenter clients **must** use ldaps://ldap-id.dpdcn.unt.edu

AUTHTREE: ldaps://ldap-auth.untsystem.edu (load-balanced across both datacenters)

IMPORTANT: Clients within a datacenter **MUST** use their local LDAP service.

- GAB datacenter clients **must** use ldaps://ldap-auth.gabdcn.unt.edu
- DP datacenter clients **must** use ldaps://ldap-auth.dpdcn.unt.edu

Network Encryption Required

You are required to use a secure (encrypted) network connection. The IDTREE and AUTHTREE server farms use TLS certificates signed by the InCommon certificate authority. Windows, Mac, some Linux/UNIX systems (add the ca-certificates package), and most distributions of the Java runtime should already have the required self-signed "root" certificate.

If needed, you can obtain the InCommon (a.k.a. "Sectigo", "Comodo") self-signed "root" certificate from the InCommon web site. (Hint: You want the "USERTrust Secure" certificate).

Popular IDTREE/AUTHTREE attributes

- euid
- emplid
- sn
- givenname
- mail (not available from AUTHTREE)
- eduPersonScopedAffiliation

NOTE: Other attributes are available, but often require consultation to understand the limits of the available data and appropriate uses.

Microsoft Active Directory

UNT System maintains several Active Directory domains, all within the same Active Directory forest.

DNS domain name	LDAP Search Base	LDAP Connection URL	Use
ad.unt.edu	DC=ad,DC=unt,DC=edu	ldaps://ad.unt.edu:636	System-wide IT Services
its.ad.unt.edu	DC=its,DC=ad,DC=unt,DC=edu	ldaps://its.ad.unt.edu:636	System-wide IT Services
unt.ad.unt.edu	DC=unt,DC=ad,DC=unt,DC=edu	ldaps://unt.ad.unt.edu:636	Denton / Dallas / System employees
hsc.ad.unt.edu	DC=hsc,DC=ad,DC=unt,DC=edu	ldaps://hsc.ad.unt.edu:636	HSC employees
dallas.ad.unt.edu	DC=dallas,DC=ad,DC=unt,DC=edu	ldaps://dallas.ad.unt.edu:636	Abandoned, formerly Dallas employees
students.ad.unt.edu	DC=students,DC=ad,DC=unt,DC=edu	ldaps://students.ad.unt.edu:636	Denton / Dallas / HSC students

Please notice how the LDAP search base matches the fully-qualified DNS name of the domain. When you see the LDAP distingushed name for a user object, you call tell which domain it came from by looking at the end of the distingushed name.

Network Encryption Required

You are required to use a secure (encrypted) network connection. All our Active Directory domain controllers offer LDAP service over TLS. The certificates used for TLS are signed by the Active Directory forest's own certificate authority (not InCommon). Windows computers joined to any of our AD domains should already hold a copy of the required certificates. If your LDAP client is connecting from a computer that is not joined to one of our Active Directory domains, then you may need to import the following X.509 certificate into your application or operating system certificate database (sometimes called a "keystore").

TIP: Choose "binary" for Windows. Choose "text" for everything else (copy the text from your web browser into a plain text file, including the begin/end lines).

[binary] [text] "UNT AD Root CA" (self-signed "root" certificate, signed using SHA-256 (a.k.a. "SHA-2") hash algorithm)

Popular Active Directory attributes:

- employeeID - holds the EUID
- employeeNumber - holds the EMPLID
- sn
- givenname
- mail
- telephoneNumber
- eduPersonScopedAffiliation

NOTE: Other attributes are available, but often require consultation to understand the limits of the available data and appropriate uses.

Active Directory Global Catalog

Active Directory consists of separate directory databases called "domains". While there is some "trust" involved amongst the domains inside a forest, it is not possible to connect to one domain via LDAP to query another domain. This is just how Microsoft designed Active Directory. With the LDAP protocol, you must connect to the domain you wish to query.

If you have a need to query all domains in the forest, Microsoft provides a "global catalog" service. Use the global catalog **only when needed** to query all AD domains in our AD forest. The global catalog is a separate

LDAP service that handles LDAP over TLS on TCP port 3269. Some attributes from the Active Directory domains are **not** stored in the global catalog.

IMPORTANT:

- The TCP port number for the AD global catalog is **3269** (not 636).
- The LDAP search base is always an **empty string**.
- A DNS query for **gc._msdcs.ad.unt.edu** returns a list of servers running the global catalog service (then do a reverse DNS lookup on the IP address and **use the DNS name of that server** for TLS to work properly)

WARNING: Active Directory tends to be case-sensitive with some things like attribute names where a normal LDAP server would not care.

LDAP Encryption

This section should help you to properly configure your LDAP clients for TLS encryption. There is no valid excuse for not using encryption or not configuring it properly. If your system is not documented here, we are happy to work with you.

TLS encryption

Transport Layer Security (TLS) is a newer and more secure version of SSL. With TLS, it is possible (but not required) to initiate a non-encrypted connection and then issue a "STARTTLS" command to begin encryption. TLS can also operate with encryption from the beginning just like SSL did. TLS does **not** require you to start without encryption.

TLS vulnerabilities

By now, you should be using TLS 1.3. All systems should be configured to **ALLOW ONLY TLS 1.2 or higher** due to security weaknesses in earlier versions.

OpenLDAP

OpenLDAP may use one of two TLS code libraries -- OpenSSL or GNUTLS. In either case, you must configure encryption options in the OpenLDAP **ldap.conf** (LDAP client configuration) file. The **TLS_CACERT** directive tells OpenLDAP the location of your trusted root certificates (all trusted roots in a single file).

Distribution	Location of ldap.conf	Location of Trusted Certificates File	TLS library	Certs package
Debian	/etc/ldap/ldap.conf	TLS_CACERT /etc/ssl/certs/ca-certificates.crt	GNUTLS	ca-certificates
Ubuntu	/etc/ldap/ldap.conf	TLS_CACERT /etc/ssl/certs/ca-certificates.crt	GNUTLS	ca-certificates
Fedora	/etc/openldap/ldap.conf	TLS_CACERT /etc/ssl/certs/ca-bundle.crt	GNUTLS	ca-certificates
CentOS	/etc/openldap/ldap.conf	TLS_CACERT /etc/pki/tls/certs/ca-bundle.crt	GNUTLS	ca-certificates
RedHat	/etc/openldap/ldap.conf	TLS_CACERT /etc/pki/tls/certs/ca-bundle.crt	GNUTLS	ca-certificates
SuSE	/etc/openldap/ldap.conf	TLS_CACERTDIR /etc/ssl/certs	OpenSSL	openssl-certs

With Windows, C:\ldap.conf (PHP >= 5.3.1) or C:\OpenLDAP\sysconf\ldap.conf (earlier PHP versions) are the typical locations for this file.

RedHat / CentOS / Fedora

Copy the certificate authority's self-signed ("root") certificate to the /etc/pki/ca-trust/source/anchors/ directory and issue the update-ca-trust export command.

Java

For all implementations of LDAP based upon Java, you add trusted root certificate to the Java "keystore" (a file named **cacerts**). The location of the cacerts file varies and there is often more than one copy on the computer. You must install the correct root certificate in the correct cacerts file for the LDAP functions to verify the server certificates correctly.

```
keytool -import -trustcacerts -keystore $JAVA_HOME/jre/lib/security/cacerts -storepass changeit -alias
short-name-for-this-certificate -import -file file.cer
```

Special configuration notes for PHP LDAP on Windows

NOTE: These instructions for PHP on Windows are VERY old and may no longer work.

PHP uses the OpenLDAP library, which uses the OpenSSL library. You need to tell OpenLDAP where to find the trusted root certificates. This is the correct way to configure PHP LDAP for encryption on Windows.

1. Install PHP (recommended path is C:\php and version >= 5.3.1)
2. Make sure that libeay32.dll and ssleay32.dll are in the Windows path (typically C:\php)
3. Modify php.ini to tell PHP the location of the extensions directory (extension_dir = "c:\php\ext")
4. Modify php.ini to enable the LDAP extension (extension=php_ldap.dll)
5. Create C:\ldap.conf file (plain text, use Notepad or similar)
6. Add only the line TLS_CACERT c:\cacerts.pem to the C:\ldap.conf file
7. Create C:\cacerts.pem file (plain text, use Notepad or similar)
8. Obtain a copy of the USERTrust Secure certificate from InCommon
9. Add that certificate (in PEM/Base64 encoded format) to the C:\cacerts.pem file

NOTE: You do not need to enable the PHP OpenSSL extension. Yes, the LDAP module uses the OpenSSL code library, but that is not the same thing as the PHP extension for OpenSSL.

NOTE: The **cacerts.pem** file can contain multiple root certificates. You may wish to add the InCommon (a.k.a. Sectigo, Comodo) root ("USERTrust Secure") and the root certificate we use for Active Directory.

NOTE: Some of the comments on the PHP web site imply that PHP might look for the **ldap.conf** file on a drive other than the C: drive, especially if your web server is installed on another drive. It is not possible to relocate the **ldap.conf** file. In rare circumstances, it may be necessary to use the FileMon utility to find out where PHP is looking. Try these paths where X is the drive letter of any hard disk (starting with C:).

1. X:\ldap.conf
2. X:\OpenLDAP\sysconf\ldap.conf

OpenSSL command reference

View certificate details (if needed, add "-inform DER" or "-inform PEM"):

```
openssl x509 -in input-file.pem -text
```

Convert certificate file format from binary (".cer") to Base64 (".pem"):

```
openssl x509 -inform DER -in input-file.cer -outform PEM -out output-file.pem
```

Convert certificate file format from Base64 (".pem") to binary (".cer"):

```
openssl x509 -inform PEM -in input-file.pem -outform DER -out output-file.cer
```