UCSB Identity and LDAP

The central campus directory and authentication system

UCSB Identity System

UCSBnetID authentication

UCSB-wide student and employee info

http://www.identity.ucsb.edu/

LDAP Overview

Lightweight Directory Access Protocol

Based on the X.500, created in the 80s

You can

- Authenticate: Bind
- Lookup Information: Search
- Manage: Add, Modify, Delete

LDAP Overview

Servers:

- Apache Directory Server
- Apple Open Directory
- Microsoft Active Directory
- Novell eDirectory
- OpenLDAP

LDAP Schema

ou = Organizational Unit

cn = Common Name (Full Name)

dc = Domain Component

sn = Surname (Last Name)

givenName = Given Name (First Name)

https://tools.ietf.org/html/rfc4519

LDAP Structure

Information is stored in a folder structure.

The “path” is quite different than a filesystem.

Name=Value pairs, separated by commas.

Spaces are ok! This is called a DN (more later).

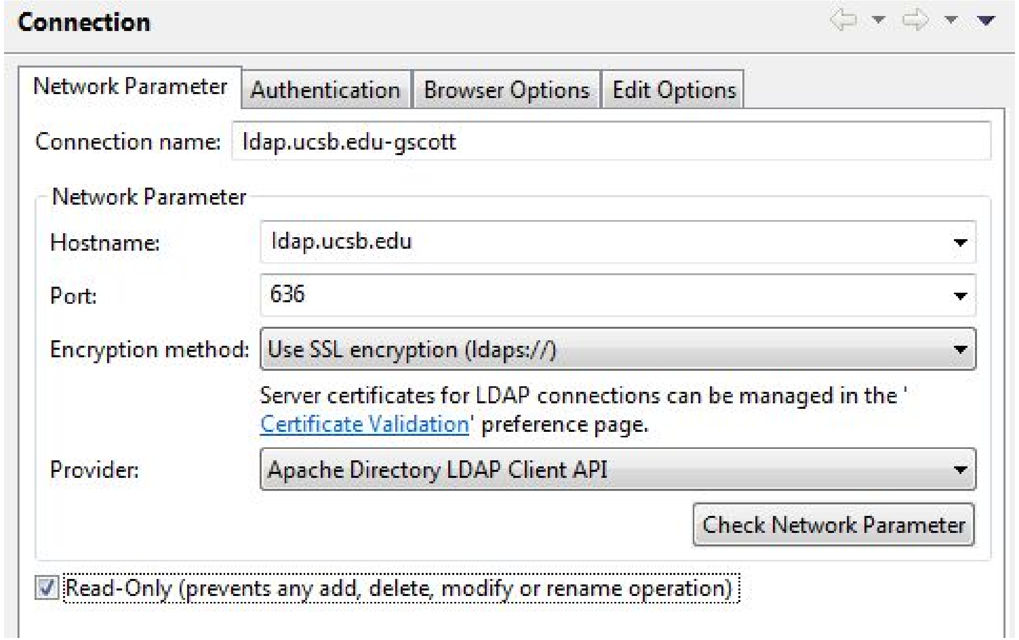
```
ou=People,o=ucsb
cn=Leroy,ou=Super Dept,dc=arit,dc=com
```

Connect to UCSB LDAP

Host: ldap.ucsb.edu

Port: 636

Security: Yes!



Connection name: ldap.ucsb.edu-gscott

Network Parameter

Hostname: ldap.ucsb.edu

Port: 636

Encryption method: Use SSL encryption (ldaps://)

Server certificates for LDAP connections can be managed in the ' Certificate Validation' preference page.

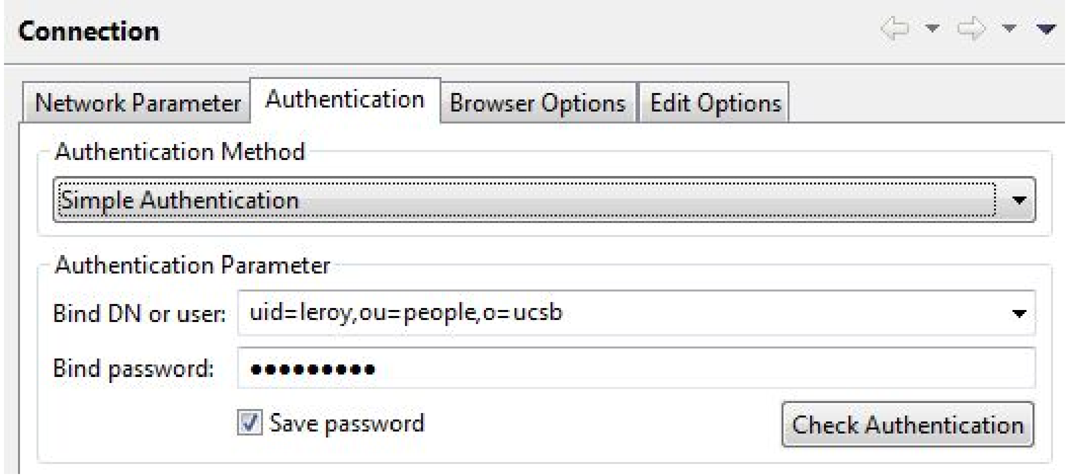
Provider: Apache Directory LDAP Client API

☑ Read-Only (prevents any add, delete, modify or rename operation)

Login

You login with a DN (distinguished name).

```
uid=leroy,ou=people,o=ucsb
```



Connection

Network Parameter | Authentication | Browser Options | Edit Options

Authentication Method

Simple Authentication

Authentication Parameter

Bind DN or user: uid=leroy,ou=people,o=ucsb

Bind password: ●●●●●●●●●●

☑ Save password

Login

Authenticating is called Binding.

Tip: LDAP will accept a blank password and connect **anonymously**. Your application should not allow blank user passwords, otherwise it will get a “success” on bind!

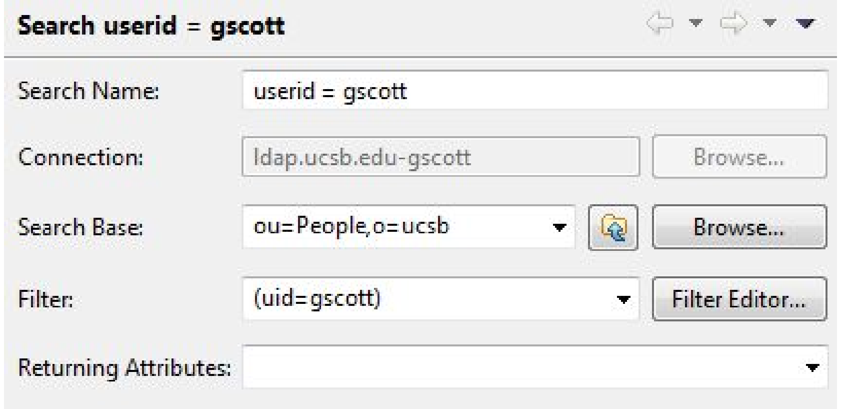
A false positive and possible security issue.

Search

Search Base: root folder to search from

Filter: query parameters

Returning Attributes: list of fields to return



Search userid = gscott

Search Name: userid = gscott

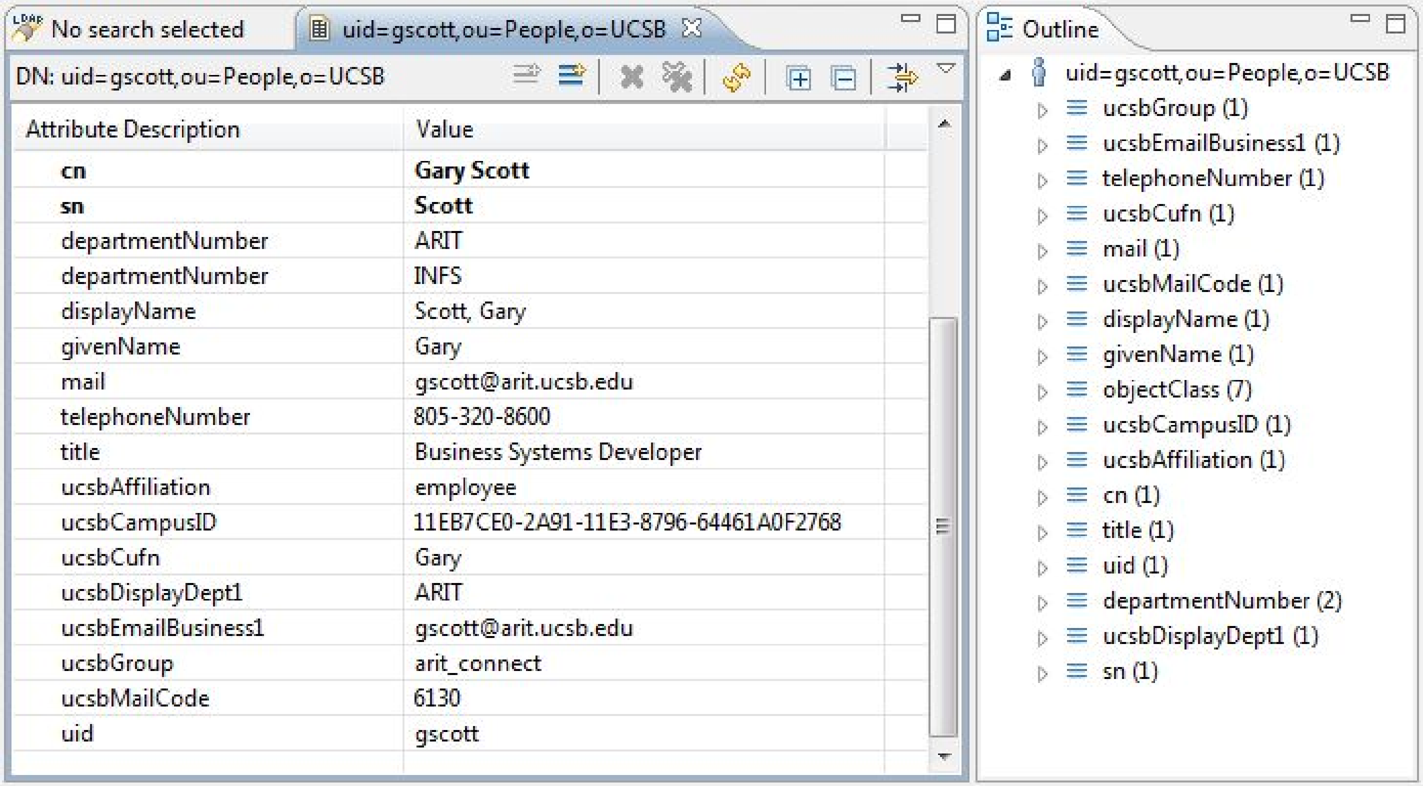
Connection: ldap.ucsb.edu-gscott

Search Base: ou=People,o=ucsb

Filter: (uid=gscott)

Returning Attributes:

Search Results



DN: uid=gscott,ou=People,o=UCSB

Attribute Description	Value
cn	**Gary Scott**
sn	**Scott**
departmentNumber	ARIT
departmentNumber	INFS
displayName	Scott, Gary
givenName	Gary
mail	gscott@arit.ucsb.edu
telephoneNumber	805-320-8600
title	Business Systems Developer
ucsbAffiliation	employee
ucsbCampusID	11EB7CE0-2A91-11E3-8796-64461A0F2768
ucsbCufn	Gary
ucsbDisplayDept1	ARIT
ucsbEmailBusiness1	gscott@arit.ucsb.edu
ucsbGroup	arit_connect
ucsbMailCode	6130
uid	gscott

- uid=gscott,ou=People,o=UCSB
  - ucsbGroup (1)
  - ucsbEmailBusiness1 (1)
  - telephoneNumber (1)
  - ucsbCufn (1)
  - mail (1)
  - ucsbMailCode (1)
  - displayName (1)
  - givenName (1)
  - objectClass (7)
  - ucsbCampusID (1)
  - ucsbAffiliation (1)
  - cn (1)
  - title (1)
  - uid (1)
  - departmentNumber (2)
  - ucsbDisplayDept1 (1)
  - sn (1)

Search Syntax

Search filters are done with parentheses in a name=value format: **`(attribute=value)`**

Asterisk is the wildcard: **`(attribute=value*)`**

Spaces are ok: **`(attribute=v a l u e)`**

Search Syntax: AND/OR

AND: is the “&” in front

(& (givenName=Leroy) (sn=Jackson))

(& (givenName=Leroy) (sn=Jackson) (ucsbAffliation=employee) (departmentNumber=ARIT))

OR: is the “pipe” in front

(| (sn=Scott) (sn=Jackson))

(| (sn=a*) (sn=b*) (sn=c*) (sn=d*) (sn=e*) (sn=f*))

Be careful on your logic here. Make sure it is correct.

LDAP Client Tool

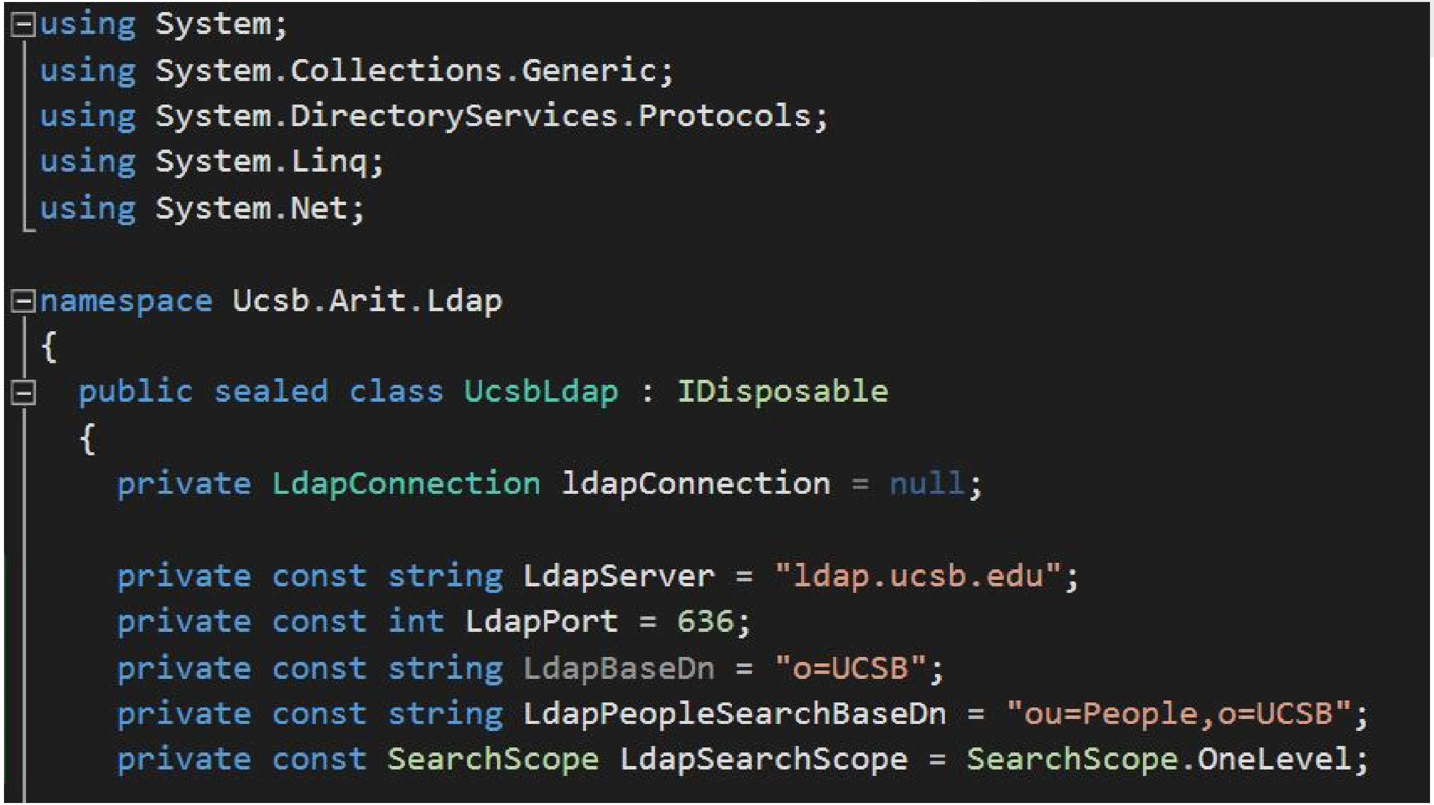
Apache Directory Studio

https://directory.apache.org/studio/

Free, works well. Must have Java installed!

Use to help debug your application or system.

Code - Connect/Auth

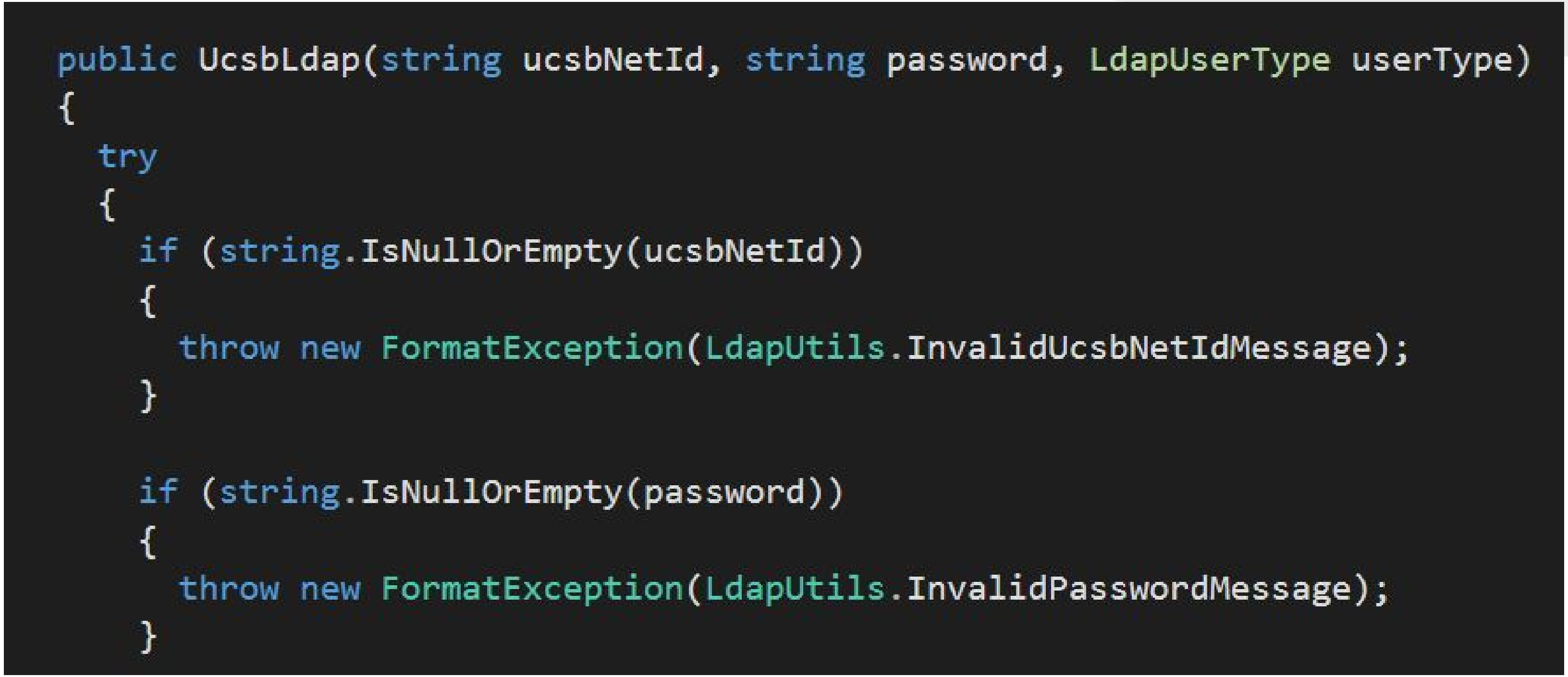


```
using System;
using System.Collections.Generic;
using System.DirectoryServices.Protocols;
using System.Linq;
using System.Net;

namespace Ucsb.Arit.Ldap
{
  public sealed class UcsbLdap : IDisposable
  {
    private LdapConnection ldapConnection = null;

    private const string LdapServer = "ldap.ucsb.edu";
    private const int LdapPort = 636;
    private const string LdapBaseDn = "o=UCSB";
    private const string LdapPeopleSearchBaseDn = "ou=People,o=UCSB";
    private const SearchScope LdapSearchScope = SearchScope.OneLevel;
```

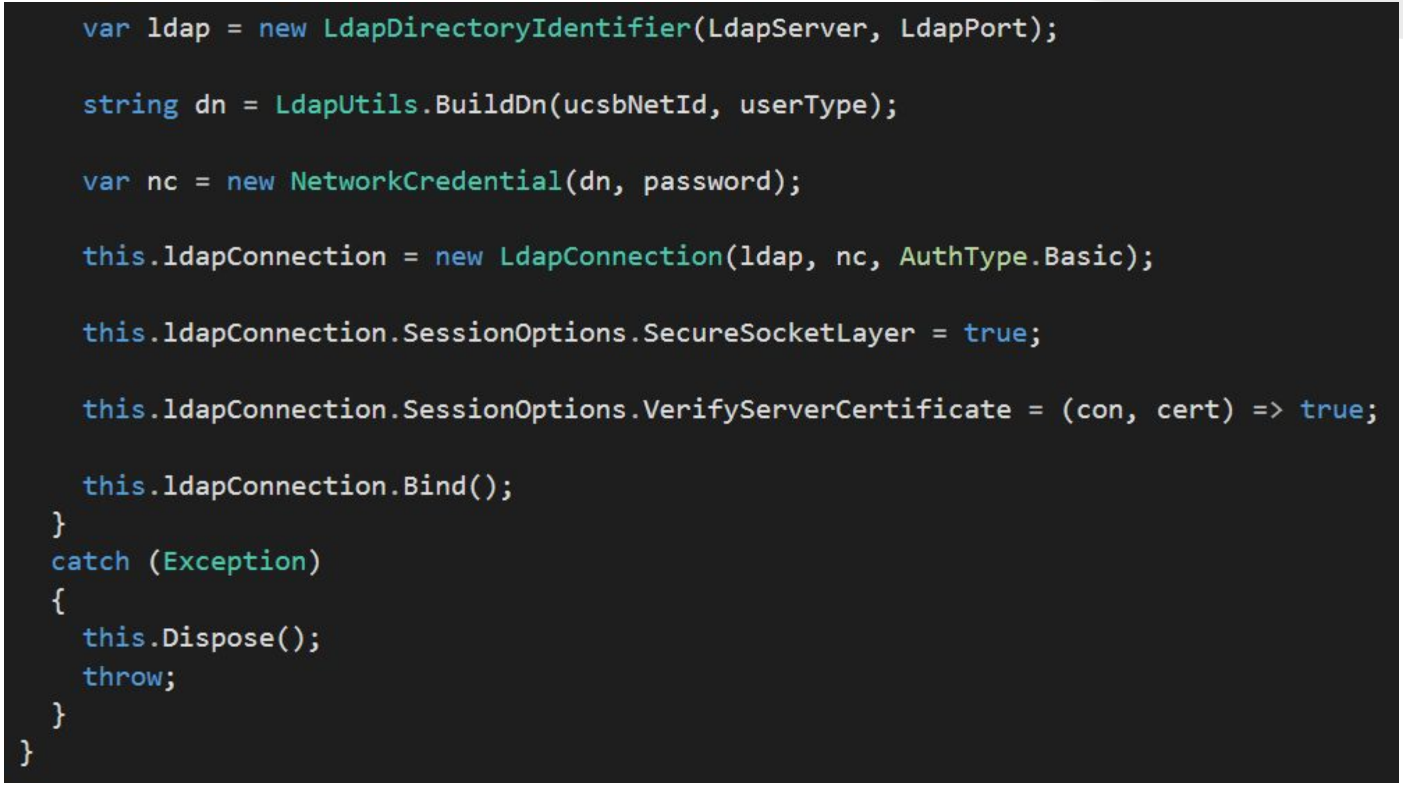
Code - Connect/Auth



```
public UcsbLdap(string ucsbNetId, string password, LdapUserType userType)
{
  try
  {
    if (string.IsNullOrEmpty(ucsbNetId))
    {
      throw new FormatException(LdapUtils.InvalidUcsbNetIdMessage);
    }

    if (string.IsNullOrEmpty(password))
    {
      throw new FormatException(LdapUtils.InvalidPasswordMessage);
    }
```

Code - Connect/Auth



```
    var ldap = new LdapDirectoryIdentifier(LdapServer, LdapPort);

    string dn = LdapUtils.BuildDn(ucsbNetId, userType);

    var nc = new NetworkCredential(dn, password);

    this.ldapConnection = new LdapConnection(ldap, nc, AuthType.Basic);

    this.ldapConnection.SessionOptions.SecureSocketLayer = true;

    this.ldapConnection.SessionOptions.VerifyServerCertificate = (con, cert) => true;

    this.ldapConnection.Bind();
  }
  catch (Exception)
  {
    this.Dispose();
    throw;
  }
}
```

Ucsb.Arit.Ldap

Have a .NET application? Need UCSBnetID authentication and lookup?

Get **Ucsb.Arit.Ldap** library as a Nuget package from http://code.arit.ucsb.edu

Get the source code from https://github.com/arit-ucsb/Arit.Common

(Your access may vary, talk to me)

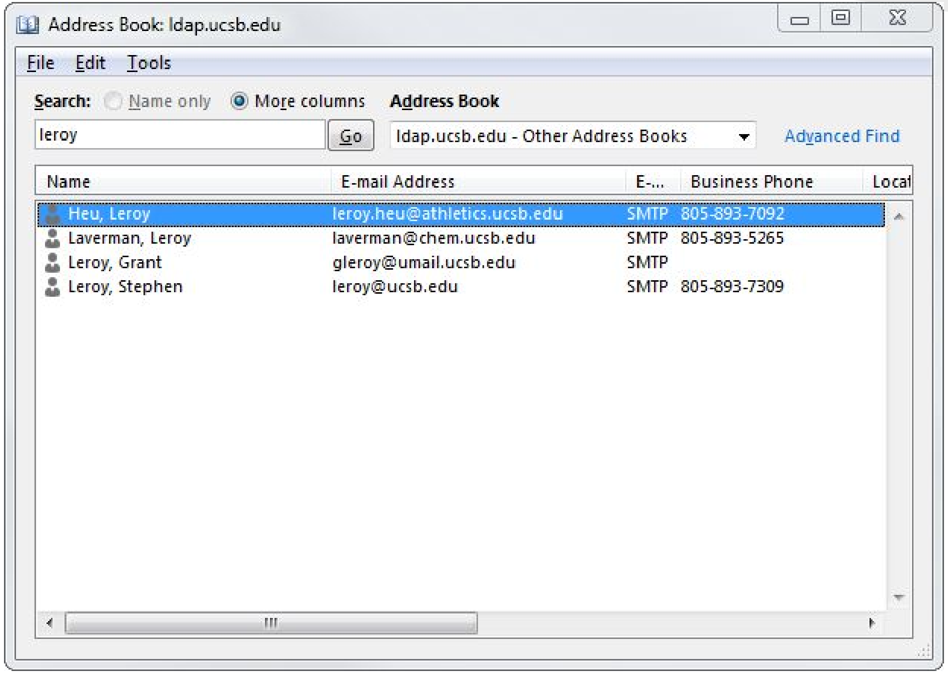
Apps that use Ucsb.Arit.Ldap

- ISDesk (ServiceNow) Data Import
- UCSB Learning Center
- Housing Room Prefs/Applications
- UCen Access Card Account Center
- RMS Mercury Portal Auth
- HRS Student Employment

Outlook Address Book

You can add the UCSB LDAP as an address book in Outlook.

Look up all UCSB people directly!



Search: ○ Name only ● More columns

leroy

Address Book: ldap.ucsb.edu - Other Address Books

Name	E-mail Address	E-...	Business Phone	Locat
Heu, Leroy	leroy.heu@athletics.ucsb.edu	SMTP	805-893-7092	
Laverman, Leroy	laverman@chem.ucsb.edu	SMTP	805-893-5265	
Leroy, Grant	gleroy@umail.ucsb.edu	SMTP		
Leroy, Stephen	leroy@ucsb.edu	SMTP	805-893-7309	

Access Issues - Account

Login with your personal account? You can only query a small set of fields.

Request an “Application” account from ETS for your system and you can query all the data.

Access Issues - Network

The UCSB LDAP system can only be accessed from an on-campus network.

If your system is externally hosted there are other methods for authentication.

See “shibboleth” on www.identity.ucsb.edu.

Get Help

Talk to me! I banged my head on the wall so you don’t have to!

http://www.identity.ucsb.edu/technologists/

ETS Support is very good for LDAP.

Thank you

Questions?

Let’s talk later.

Demo!

Gary Scott: gscott@arit.ucsb.edu