



UNIVERSITY OF UTAH
STUDENT COMPUTING LABS

Mac OS X Authentication

Kerberos and LDAP Issue

Darren R. Davis
Macintosh Specialist
University of Utah
Student Computing Labs

System Implementation

- Kerberos
- Enterprise Directory
 - Using LDAP to search
- Mac OS X Client Setup
 - Kerberos
 - Directory Access

Kerberos

- Ticket based authentication developed at MIT (many web sites)
- Many applications support it for authentication and authorization
- Realm = UTAH.EDU
- Three KDCs
 - Secured and replicated
 - Configured for fail-over



LDAP Directory

- Lightweight Directory Access Protocol
- Directories are special network databases optimized for searching
 - Think of a phone book
 - You have name, search, and find number
 - Used for storing user information
 - SCL does not store passwords in the Directory

Mac OS X 10.2.x Clients

- All Mac OS X clients running Jaguar
- Kerberos client (built in)
- Directory configuration (built in)
 - Apple Directory Access Utility

Enabling Kerberos Login

- Must edit XML document
 - /etc/authorization
- Several configuration options
 - Kerberos authentication required for login
 - Post-login Kerberos authentication
- Apple support documents
 - 107153
 - 107154



Mac OS X Directory Setup

- Apple supplied utility
- “Directory Access”
- Configure LDAPv3



Mac OS X Login Process

Login passes user name to Directory Server

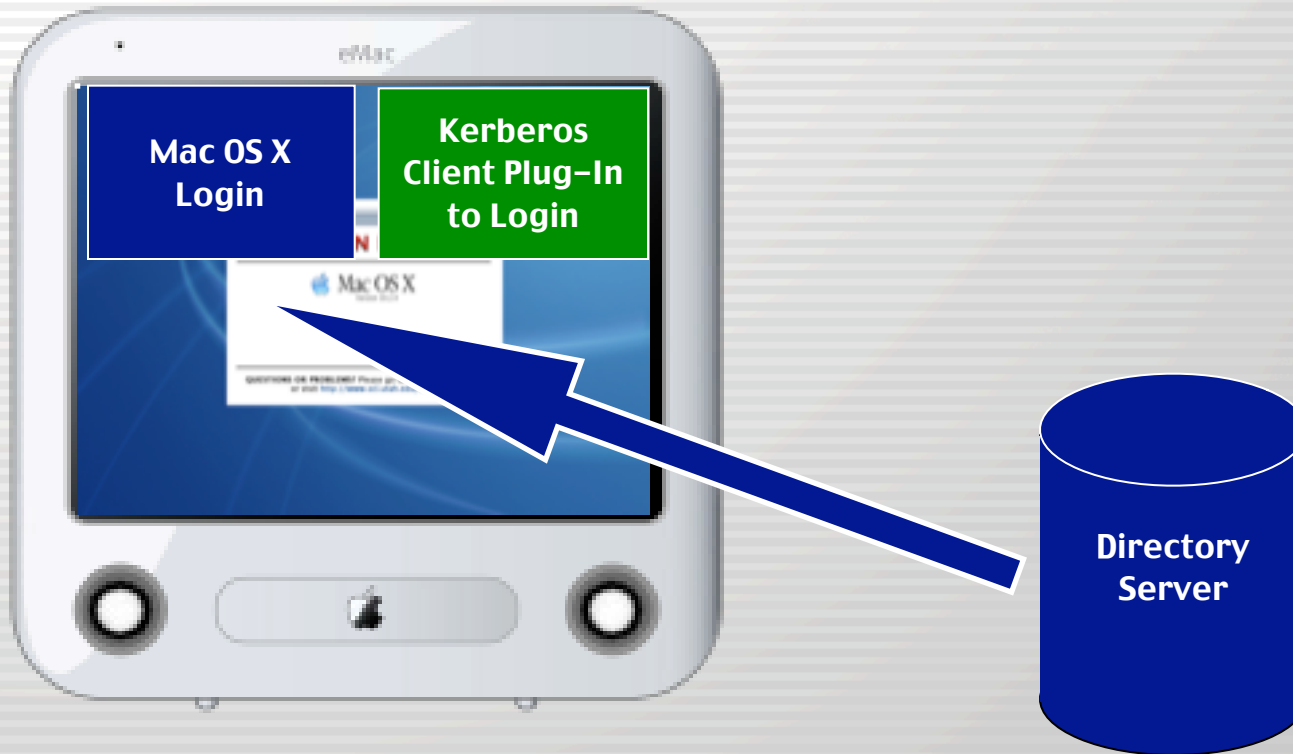


A default user created just for LDAP is used to authenticate to Directory to get user information.



Mac OS X Login Process

If user is in the Directory, user attributes are returned



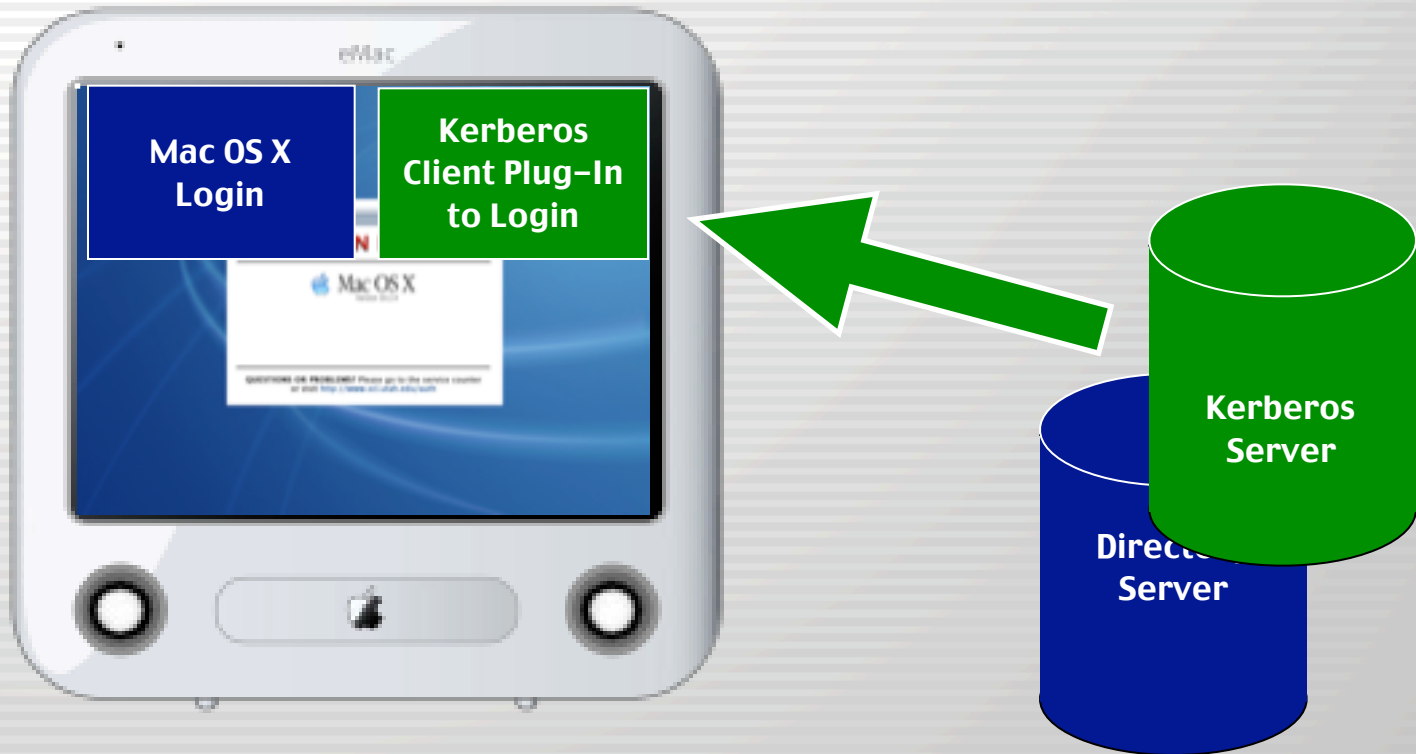
Mac OS X Login Process

Kerberos Client has user info, so authenticate



Mac OS X Login Process

Yes! user is authentic



Mac OS X Login Process

Directory searched again for user attributes

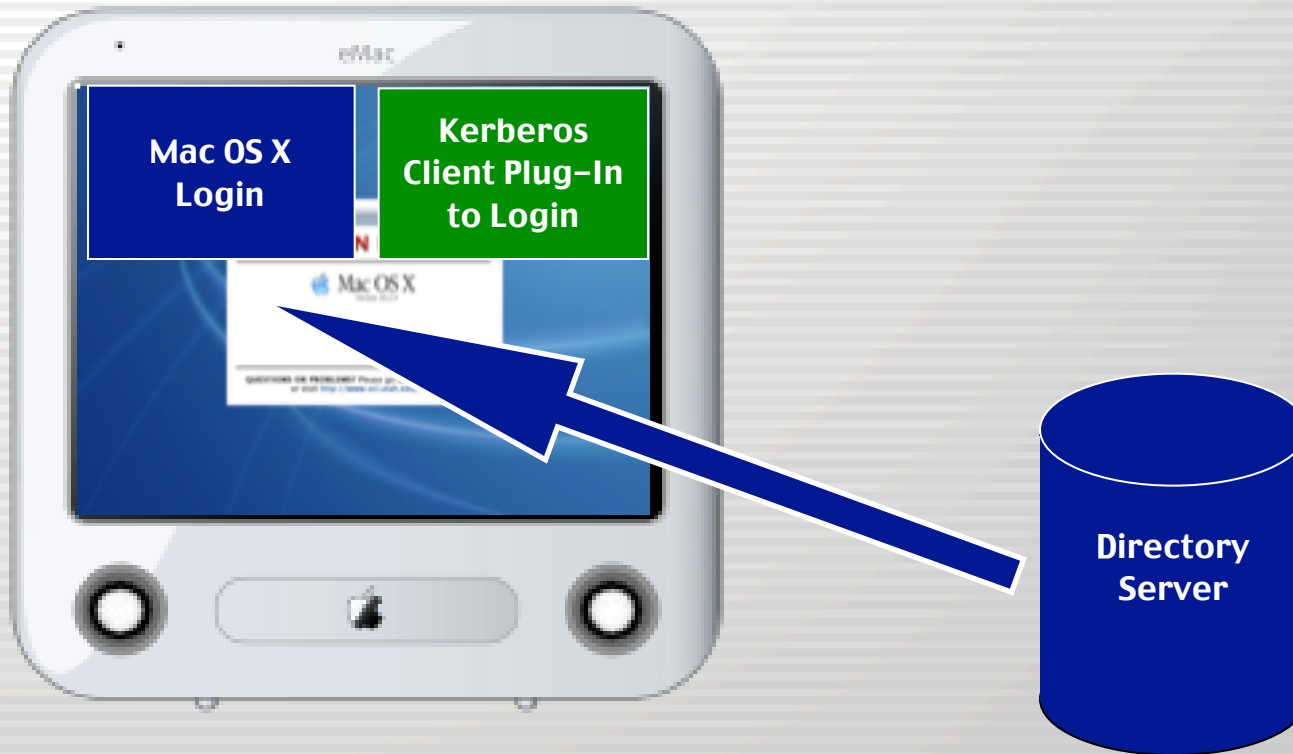


**LDAP BIND Attempted!
Meaning the Username
and Kerberos Password
sent to Directory Server.**



Mac OS X Login Process

Login gets remaining user attributes



Mac OS X Login Process

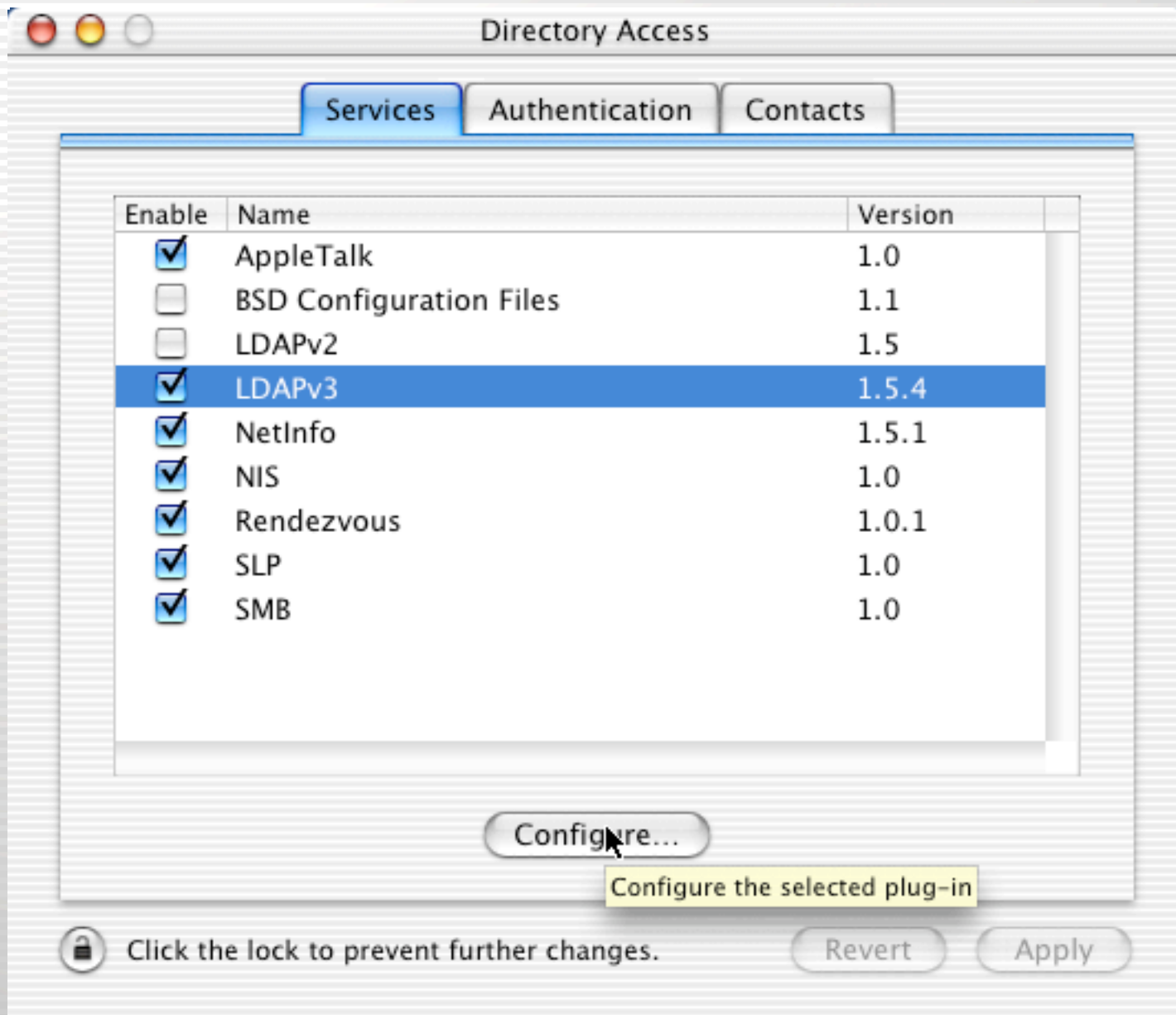
User is logged in and attributes used for user identity



Solutions

- Use SSL for all LDAP information
 - Everything is encrypted so OK
- Configure Directory Access to use AuthenticationAuthority attribute
 - Set to an existing Directory attribute that always has a value!

Directory Access



Directory Access

Directory Access

Location:

Use DHCP-supplied LDAP Server

Hide Options

Enable	Configuration Name	Server Name or IP Address	LDAP Mappings	SSL
<input checked="" type="checkbox"/>	SCL	dc1-mmcc.scl.utah.edu	<input type="text" value="Custom"/>	<input type="checkbox"/>

Directory Access

SCL

Connection Search & Mappings

Configuration Name: SCL

Server Name or IP Address: dc1-mmcscl.utah.edu

Open/close times out in: 120 seconds

Connection times out in: 120 seconds

Use authentication when connecting

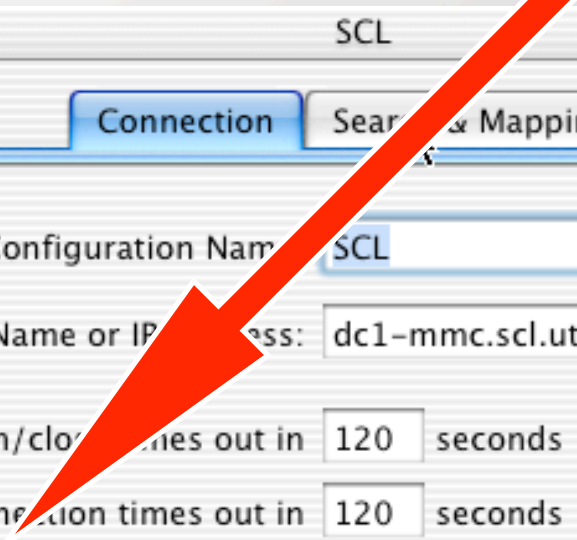
Distinguished Name: cn=ldapaccess,cn=users,dc=scl,

Password:

Encrypt using SSL

Use custom port: 389

Cancel OK



Directory Access

SCL

Connection Search & Mappings

Configuration Name: SCL

Server Name or IP Address: dc1-m...scl.utah.edu

Open/close times out in 30 seconds

Connection times out 120 seconds

Use authentication when connecting

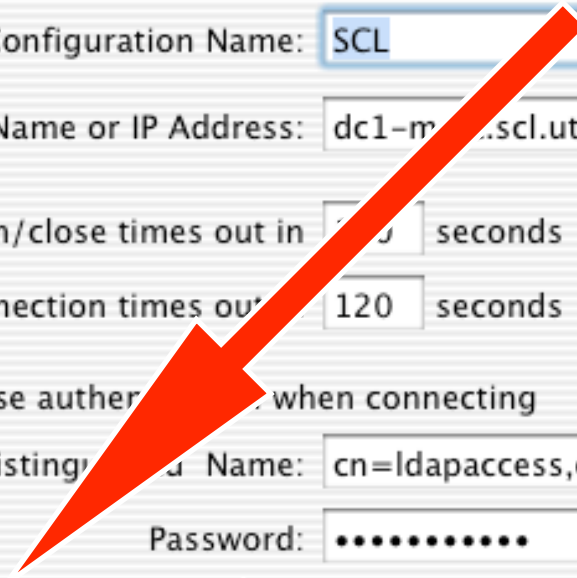
Distinguished Name: cn=ldapaccess,cn=users,dc=scl,

Password:

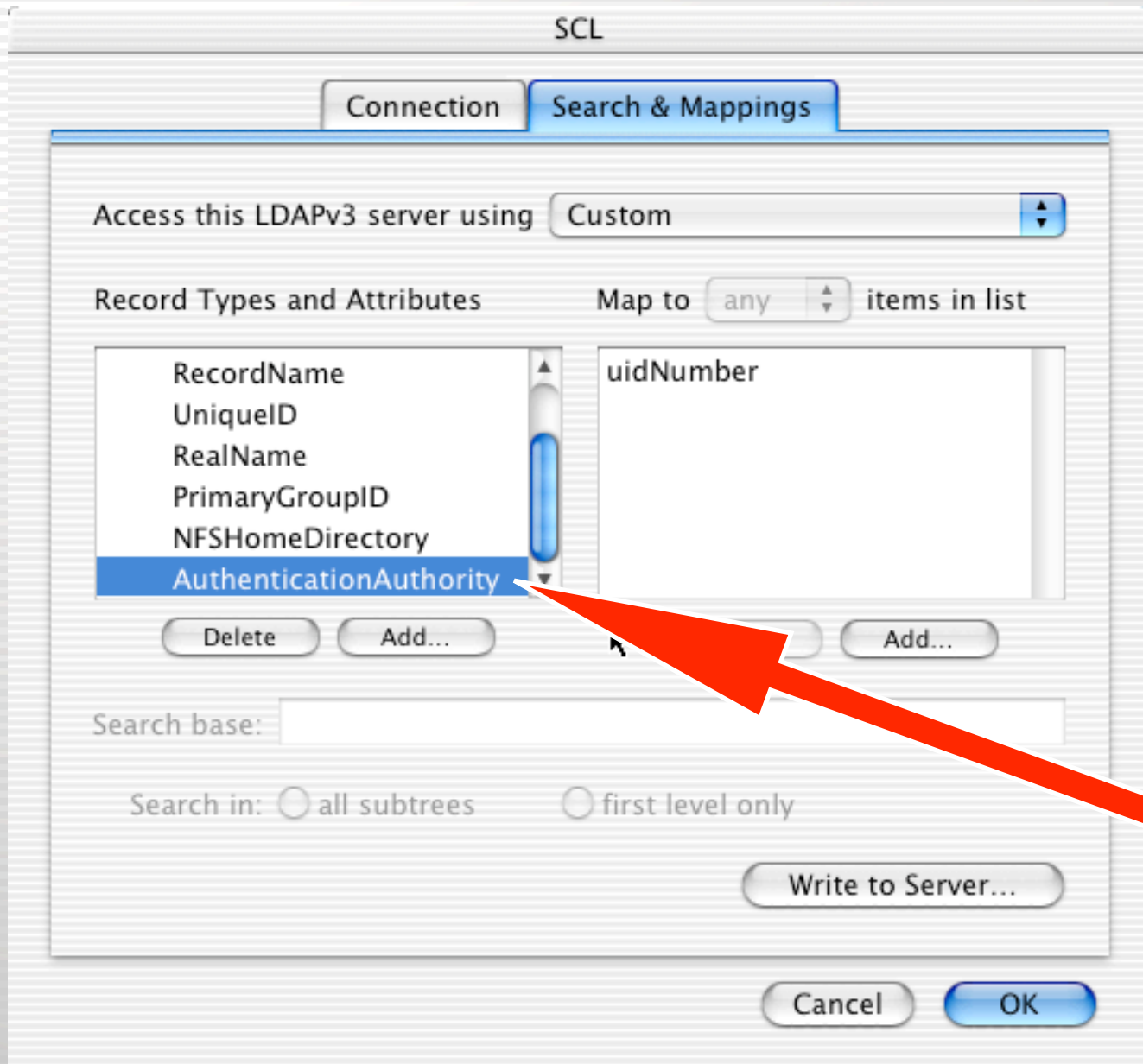
Encrypt using SSL

Use custom port 636

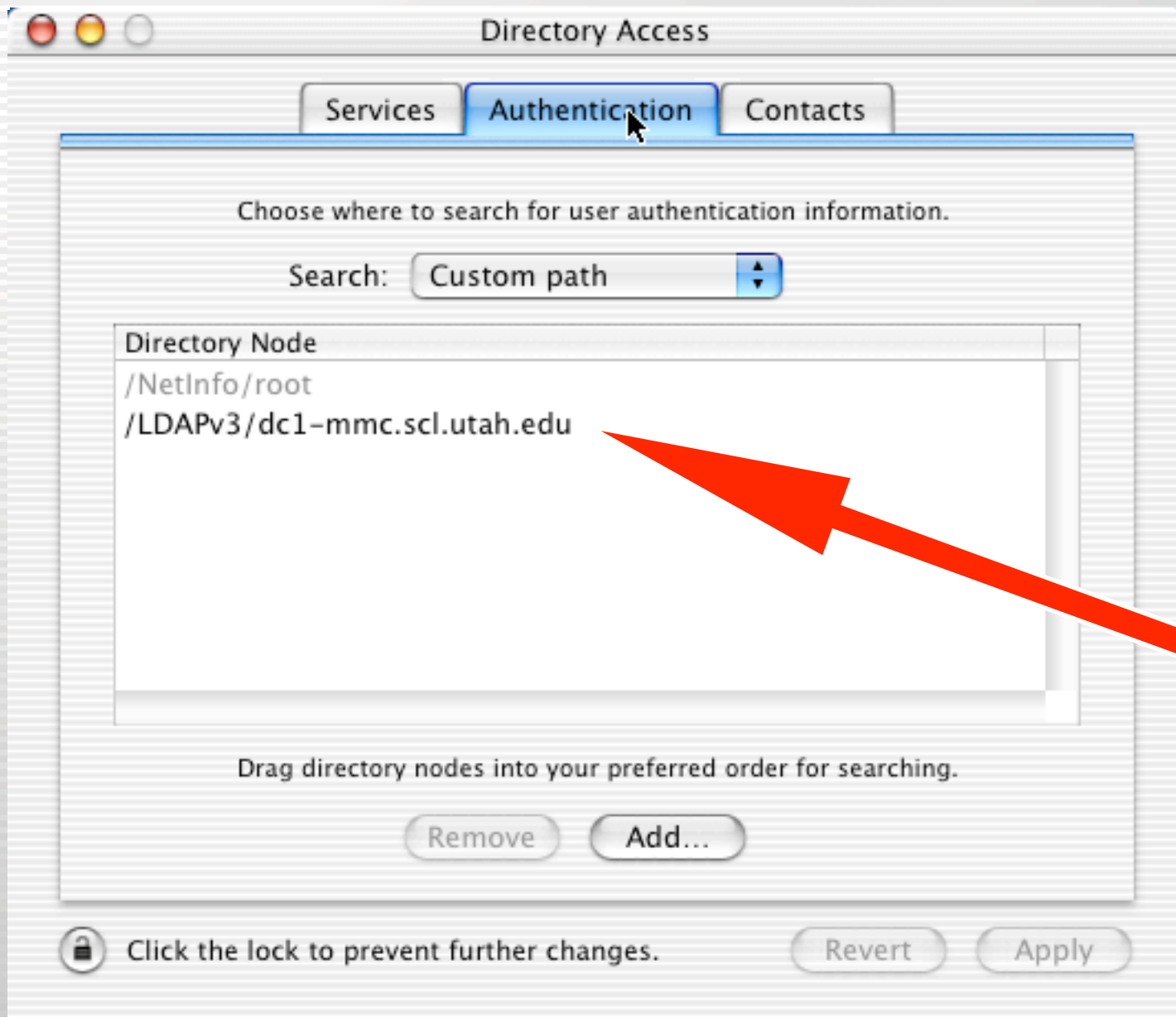
Cancel OK



Directory Access



Directory Access



Questions and Answers

