UNIVERSITY OF UTAH
STUDENT COMPUTING LABS

Mac OS X Authentication

Case Study

Darren R. Davis
M.S. Computer Science
Macintosh Specialist
University of Utah
Student Computing Labs

Presentation Overview

- Goals and History
- Authentication System Components
  - Student, Faculty and Staff Database
  - University Network ID System
  - Authentication with Kerberos
  - Enterprise Directory
- Client Setup and Operation

Definitions

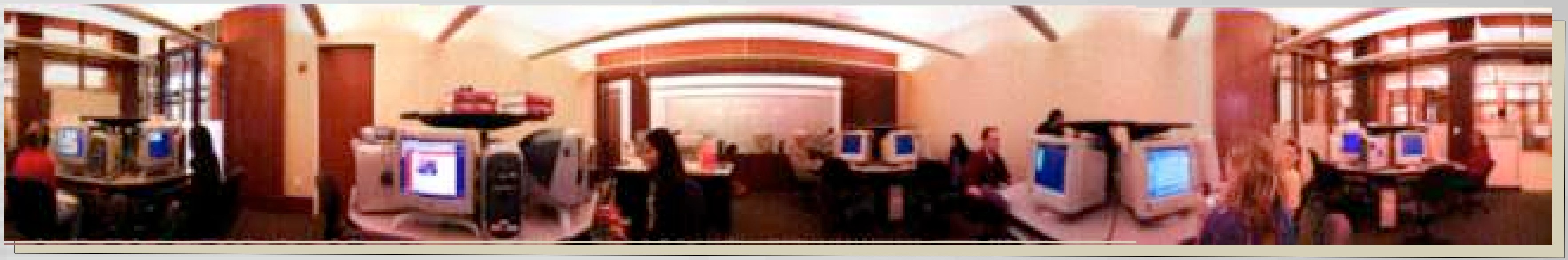
- Authentication
  - Process of verifying the identity of a user
- Authorization
  - Determining what the user can access
- Kerberos
  - A network authentication protocol
- Enterprise Directory
  - A network database optimized for searching and used to store identity

Definitions

- KDC
  - Kerberos Key Distribution Center
- LDAP
  - Lightweight Directory Access Protocol
- NID
  - Network Identification for user
    - name
    - password

Student Computing Labs

- Provides Computers for Student Use
  - Macintosh OS X Clients
  - Macintosh OS 9 Clients
  - Windows 2000 and XP Clients



UNIVERSITY OF UTAH
STUDENT COMPUTING LABS

Authentication Project Goals

- Need users to authenticate
  - Control access to computing resources
  - Problems with non-authorized use.
- Need to manage user information
  - Single identity and password
- Need to use existing University infrastructure
  - Campus NID (Network ID) system

Potential Issues

- Authenticated Classrooms
- Guest Users
- Network Disruption
- User Privacy
  - FERPA (Family Education Rights and Privacy Act)
- Integration with campus infrastructure

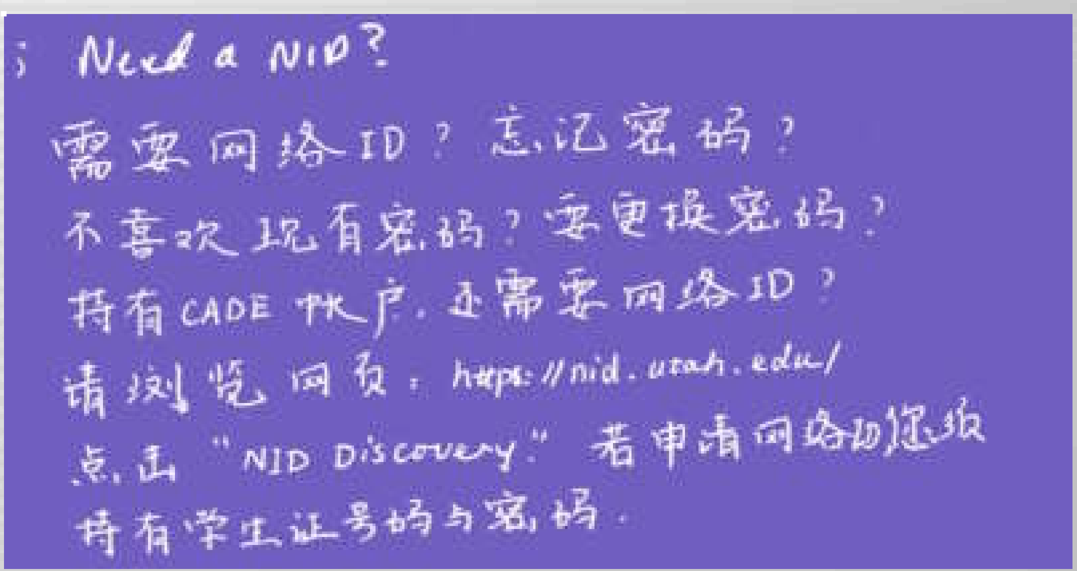
Timeline

- Project Started December 2001
  - Test environment to work out issues
- Student Computing Labs
  - Several lab locations
  - Set dates to convert labs
- Production Deployment
  - Gradual and incremental roll-out
  - Labs and one classroom Jun - Aug 02

UNIVERSITY OF UTAH
STUDENT COMPUTING LABS

Support Issues

- Consulting Staff Primary Support
  - Aided by full-time staff
- Documentation
  - web based
- Training
- Tools



Need a NID?

需要网络ID？忘记密码？

不喜欢现有密码？要更换密码？

持有CADE帐户，还需要网络ID？

请浏览网页：https://nid.utah.edu/

点击 "NID Discovery." 若申请网络ID您必须

持有学生证号码与密码。

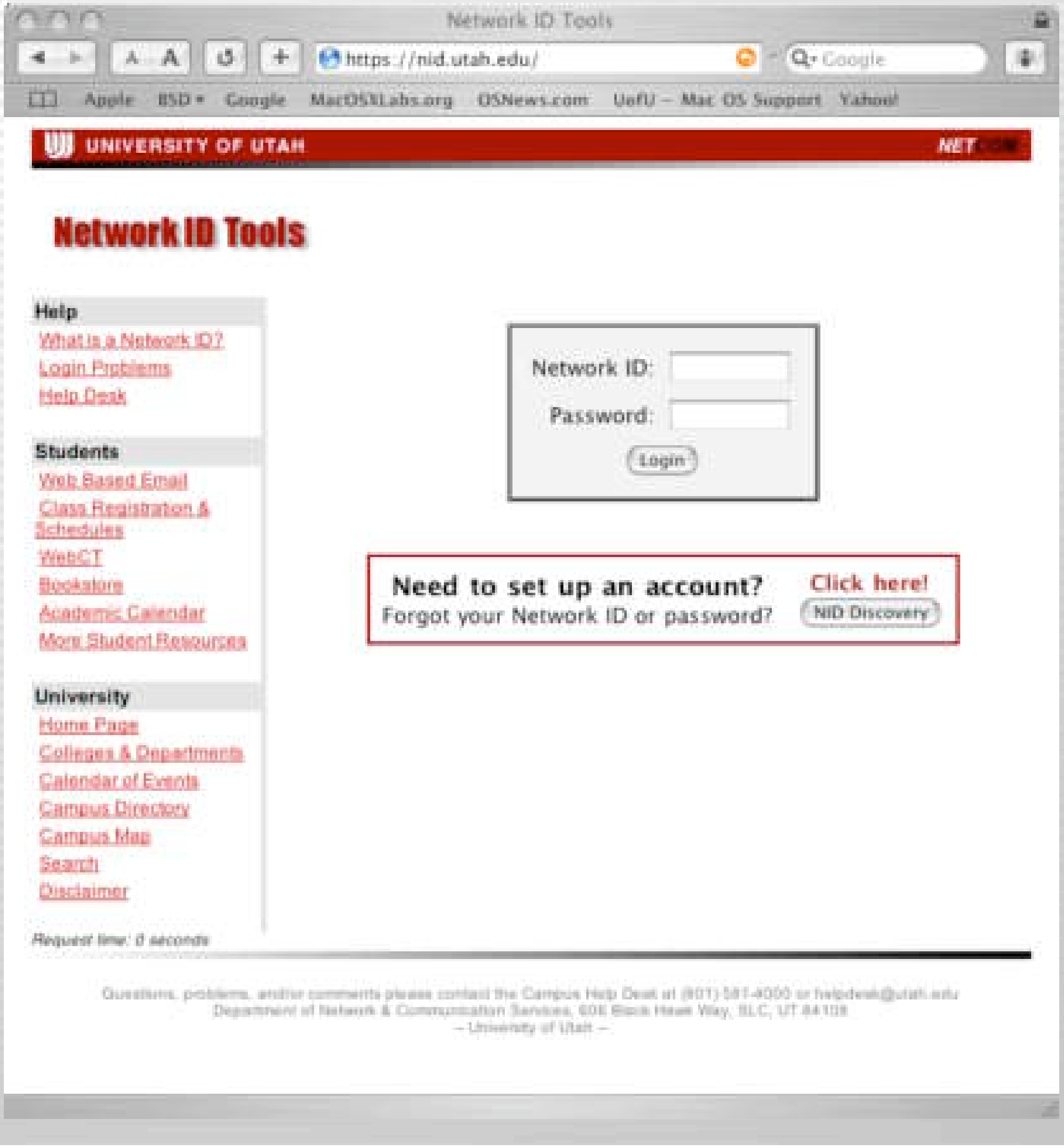
Staff Tools

- Password Reset
  - people forget their passwords
- Guest Accounts
  - Need to support temporary accounts

User Tools

- Do I have an account
  - NID Discovery
- Account Administration
  - Get NID Password
  - Change NID Password

Network ID Tools



Network ID Tools

Help

- What is a Network ID?
- Login Problems
- Help Desk

Students

- Web Based Email
- Class Registration & Schedules
- WebCT
- Bookstore
- Academic Calendar
- More Student Resources

University

- Home Page
- Colleges & Departments
- Calendar of Events
- Campus Directory
- Campus Map
- Search
- Disclaimer

Network ID:

Password:

Login

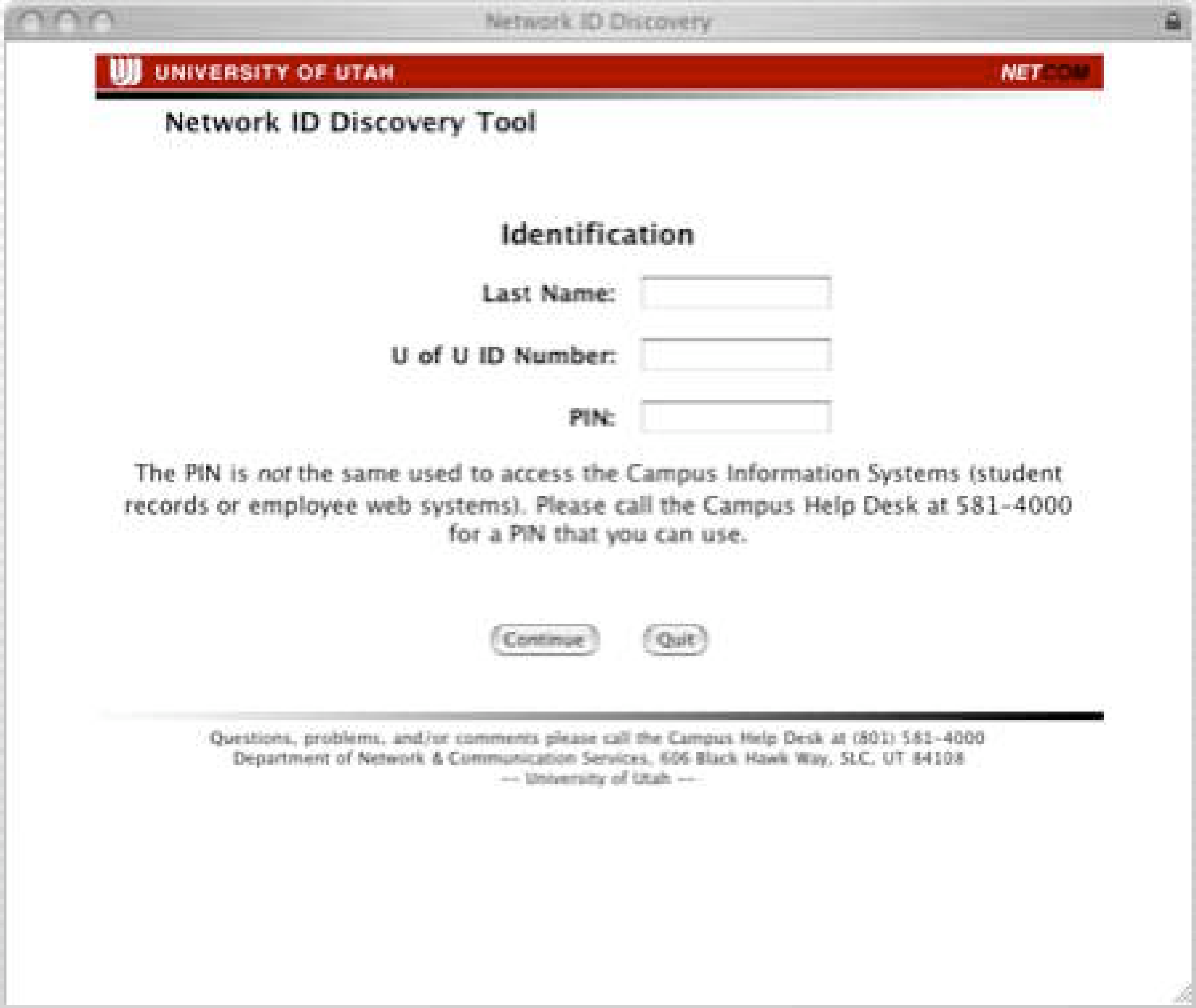
Need to set up an account? Click here!

Forgot your Network ID or password? NID Discovery

Request time: 0 seconds

Questions, problems, and/or comments please contact the Campus Help Desk at (801) 581-4000 or helpdesk@utah.edu
Department of Network & Communication Services, 606 Black Hawk Way, SLC, UT 84108
-- University of Utah --

NID Discovery



Network ID Discovery Tool

Identification

Last Name:

U of U ID Number:

PIN:

The PIN is *not* the same used to access the Campus Information Systems (student records or employee web systems). Please call the Campus Help Desk at 581-4000 for a PIN that you can use.

Questions, problems, and/or comments please call the Campus Help Desk at (801) 581-4000
Department of Network & Communication Services, 606 Black Hawk Way, SLC, UT 84108
--- University of Utah ---

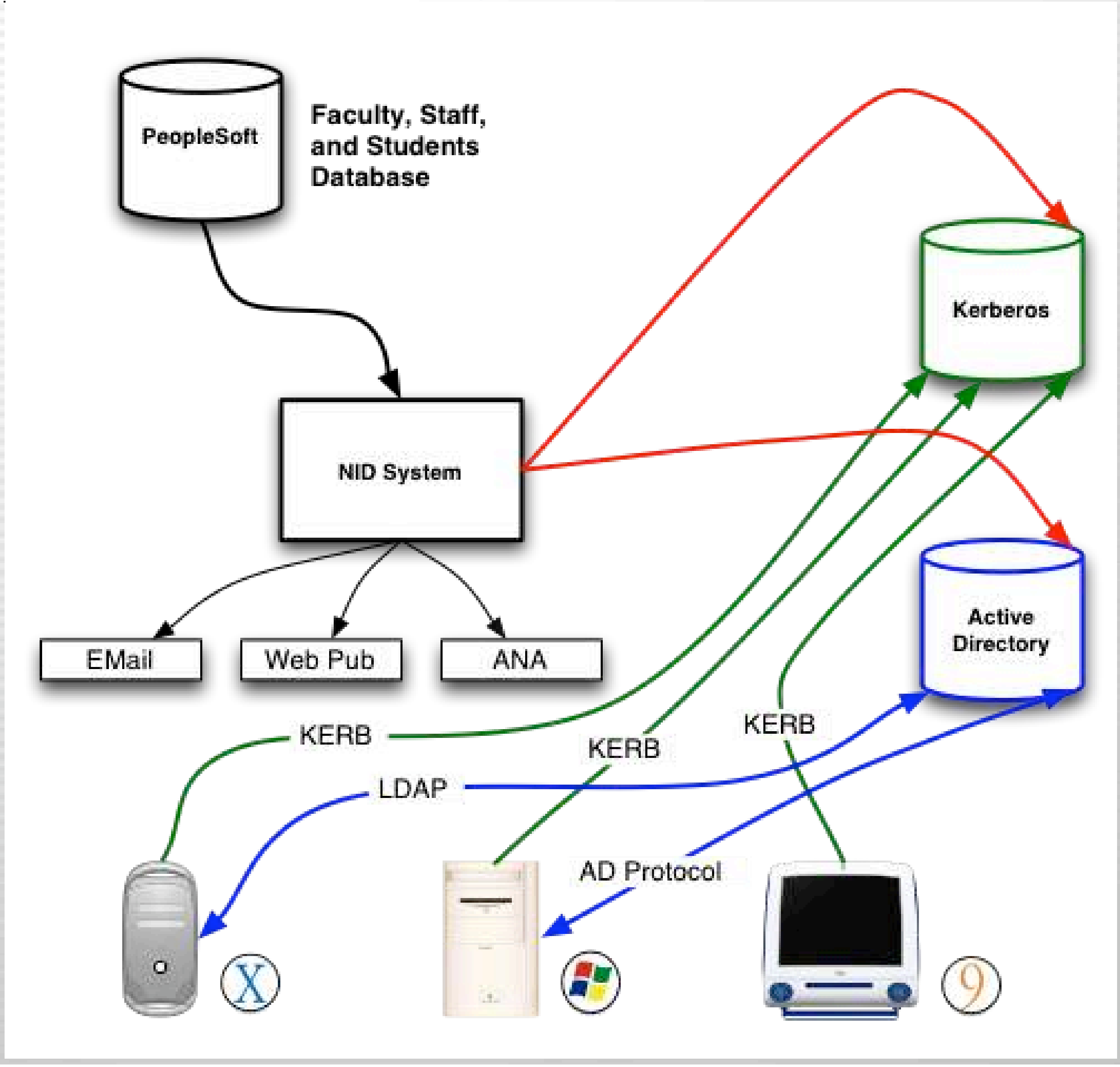
Publicity

- Signs
- Web Pages
- FAQs
- Complaint Handling

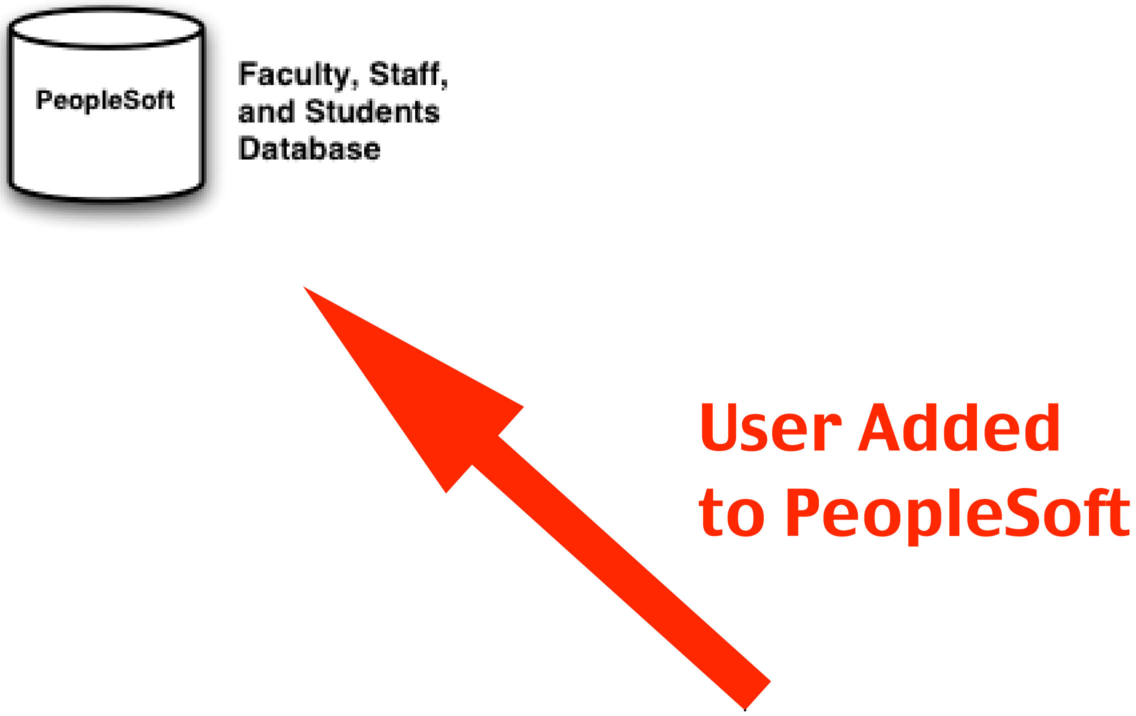
System Implementation

- Existing Infrastructure
  - Faculty, staff and student database
    - PeopleSoft
  - University Network ID system (NID)
    - Active Directory
- Kerberos
- Microsoft Active Directory
- Mac OS X Client Setup

Overview Diagram



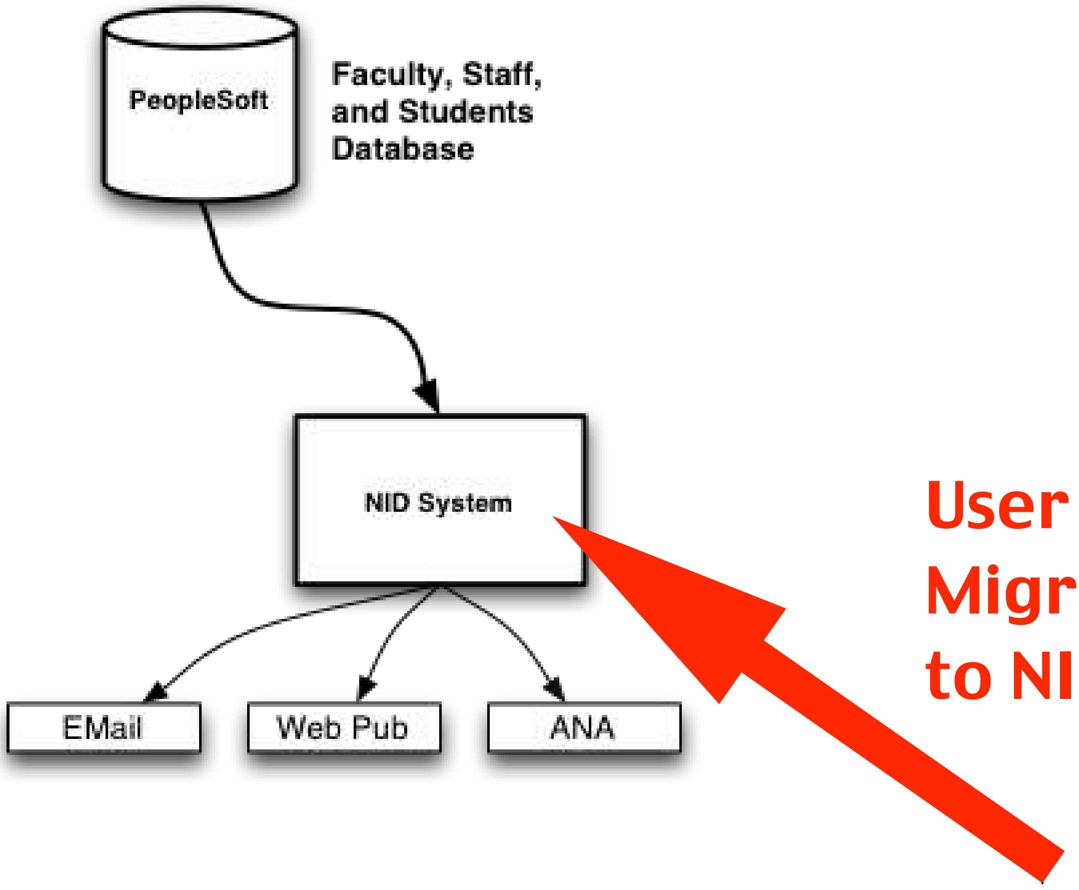
PeopleSoft Managed by HR



Faculty, Staff, and Students Database

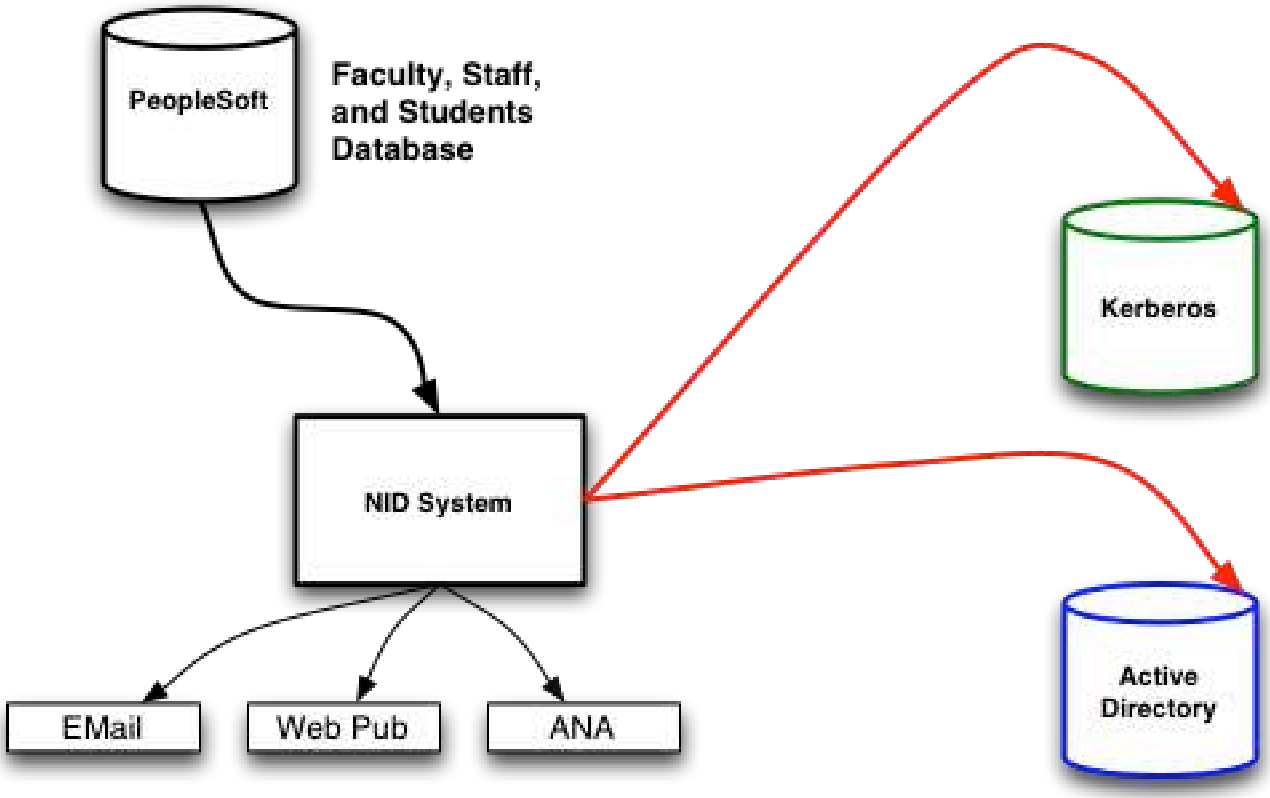
User Added to PeopleSoft

University NID System

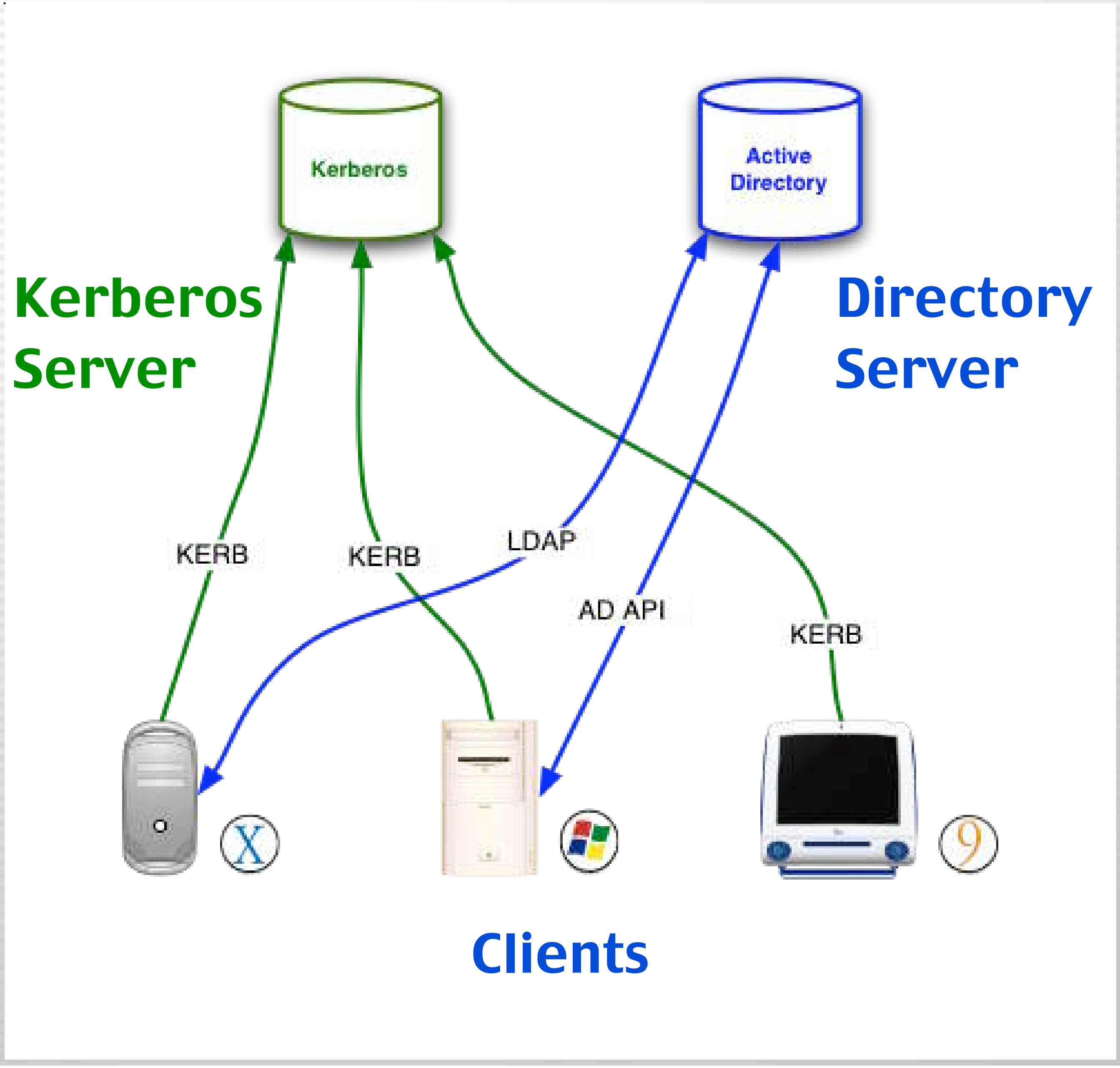


User Data Migrates to NID

NID Data Migrates to SCL



SCL Authentication Overview

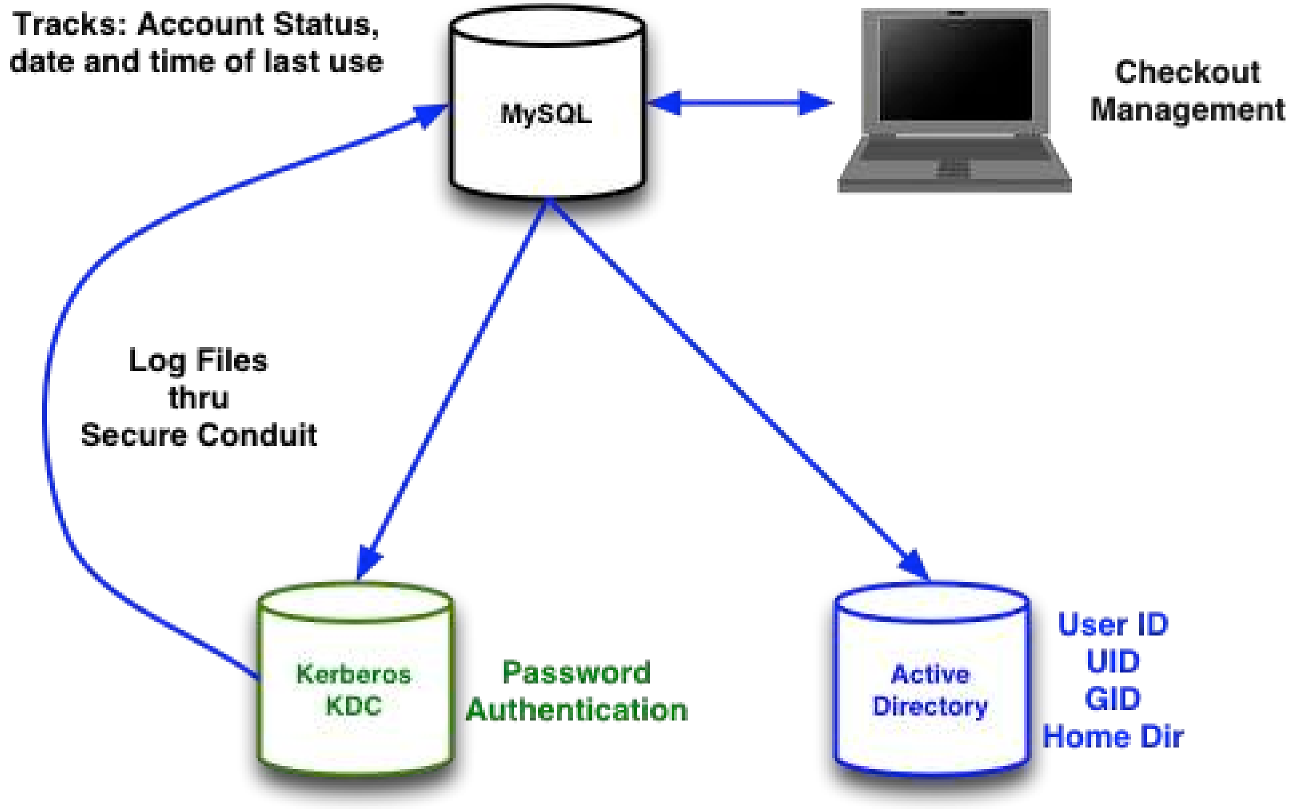


Kerberos Server

Directory Server

Clients

Guest System



Kerberos
Server

Directory
Server

Guest System

- To provide for one-day lab use
- MySQL Database
  - Management and Tracking
    - Account Status
    - Date and Time Data
- Data Migrates
  - Active Directory
  - Kerberos

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

Why Kerberos?

- Local authentication
- Kerberized applications
  - ssh, fetch, mail, printing, etc.
- Kerberized services
  - AFP, login, print accounting, etc.
- Kerberized OS integration
- Years of experience and use!

Enterprise Directory

- Microsoft Active Directory (AD)
  - Why Active Directory?
  - Because we manage Windows 2000 clients
  - Use the enterprise directory we have
- Could switch to another directory

Setting up Active Directory

- Install Windows 2000 Server
- Applied patches and updates
- Setup domain controller
- Extend directory schema
- Automated adding users
  - PERL script

Extend the Schema

- The schema represents the structure of the directory
  - We needed it to contain Mac OS X (UNIX) information
  - So, we added schema information for UNIX using AD4UNIX, but other schema extensions tools will work
    - Microsoft Windows Services for UNIX

Active Directory Management

- Five domain controllers
  - located adjacent to each lab
- User information updates
  - University NID system
  - Guest account system
- All users are populated in a single container

What is stored in AD?

- Minimally populated
  - User ID (’the-user’)
  - UID (Unique ID #)
  - GID (Group ID #)
  - Home Directory Path (/User/Home)
- We DO NOT store passwords in AD
  - For security reasons
  - Password field set to random value

Example Directory Entry

- gidNumber: 500
- loginShell: /bin/false
- msSFUHomeDirectory:
    - /Users/Authenticated User/
- msSFUName: the-user
- syncNisDomain: scl
- uidNumber: 1234567

Mac OS X 10.2.x Clients

- All Mac OS X clients running Jaguar
  - Currently Mac OS X 10.2.5
- 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

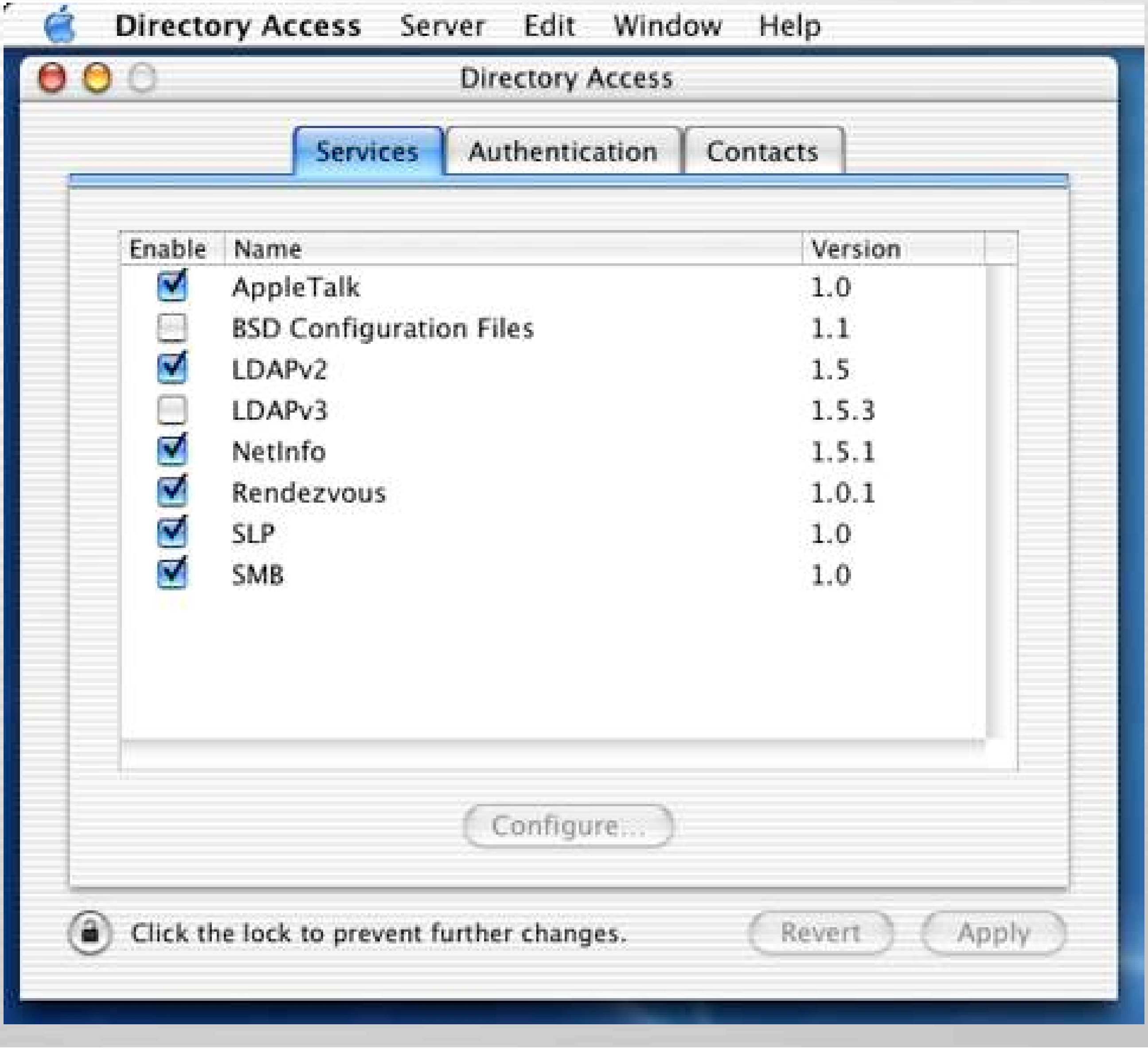
Kerberos Extras

- Apple does not include support for Kerberos-using applications like Eudora and Fetch
- Get Mac OS X 10.2 Kerberos Extras from MIT
  - This gives support for some applications to use the Kerberos authentication system
- No support for Screen Saver and Keychain, but coming from Apple

Mac OS X Directory Setup

- Apple supplied utility
- “Directory Access”

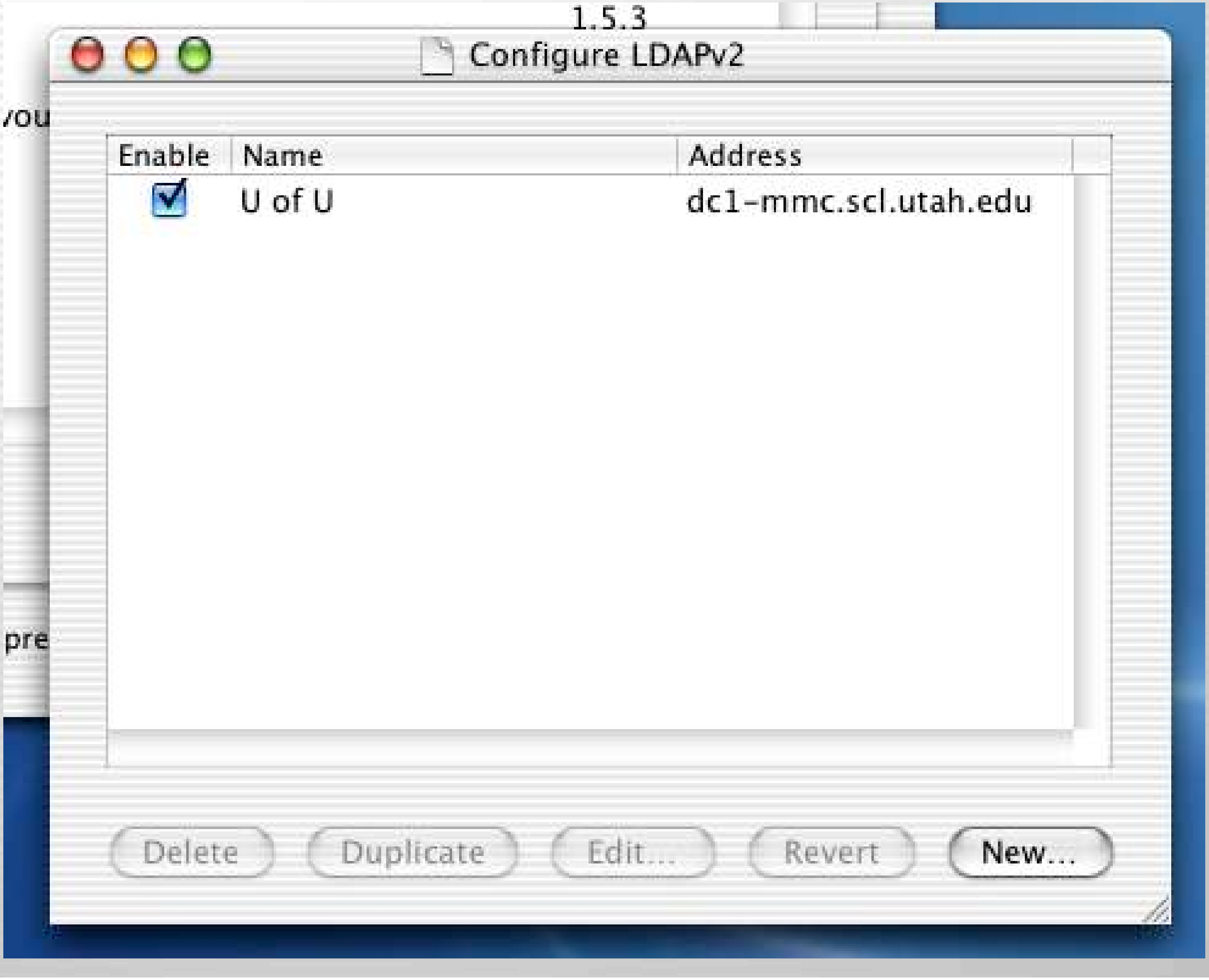
Directory Access



Enable	Name	Version
☑	AppleTalk	1.0
□	BSD Configuration Files	1.1
☑	LDAPv2	1.5
□	LDAPv3	1.5.3
☑	NetInfo	1.5.1
☑	Rendezvous	1.0.1
☑	SLP	1.0
☑	SMB	1.0

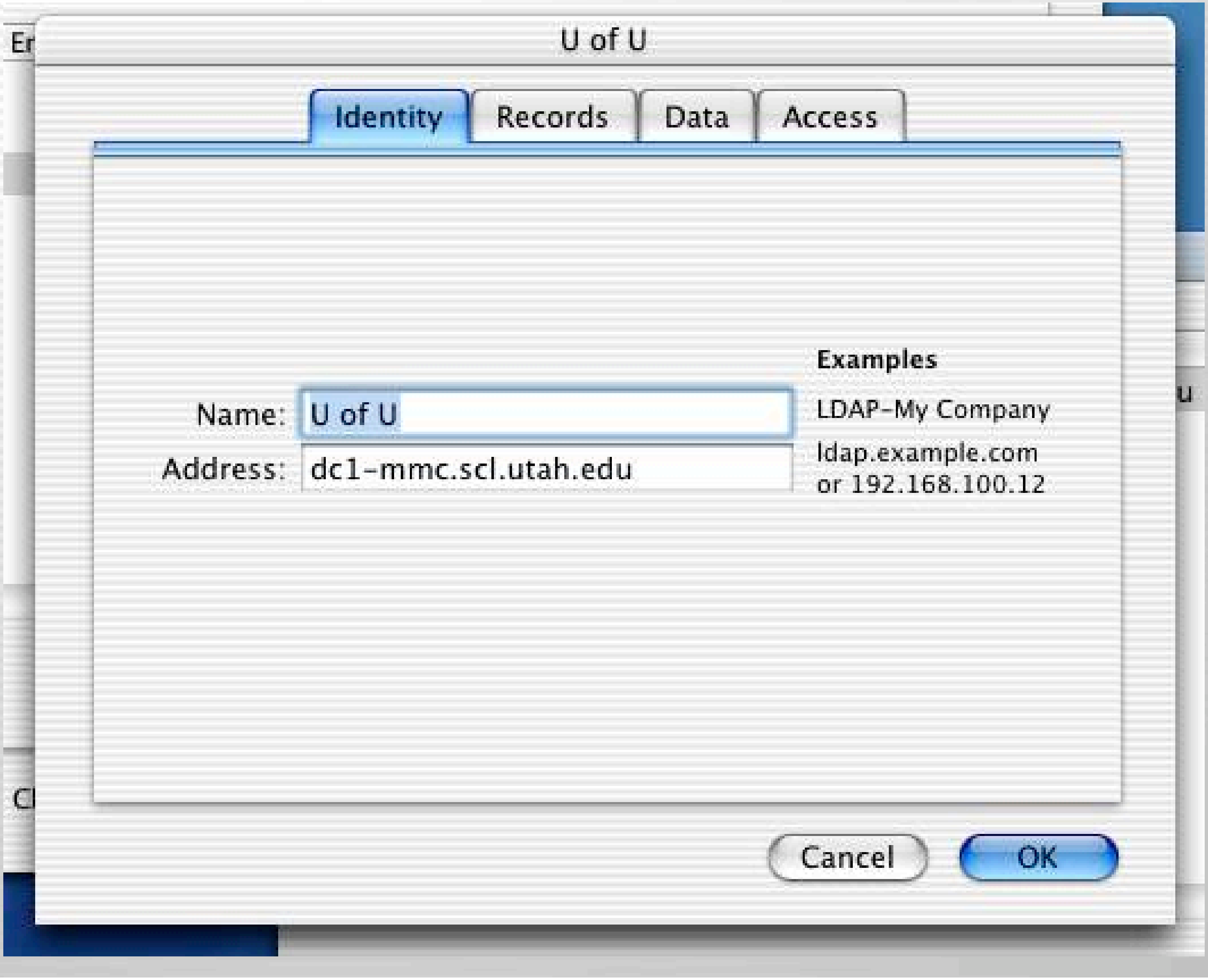
Click the lock to prevent further changes.

Configure LDAPv2



Enable	Name	Address
☑	U of U	dc1-mmc.scl.utah.edu

LDAPv2 - Identity



U of U

Name: U of U

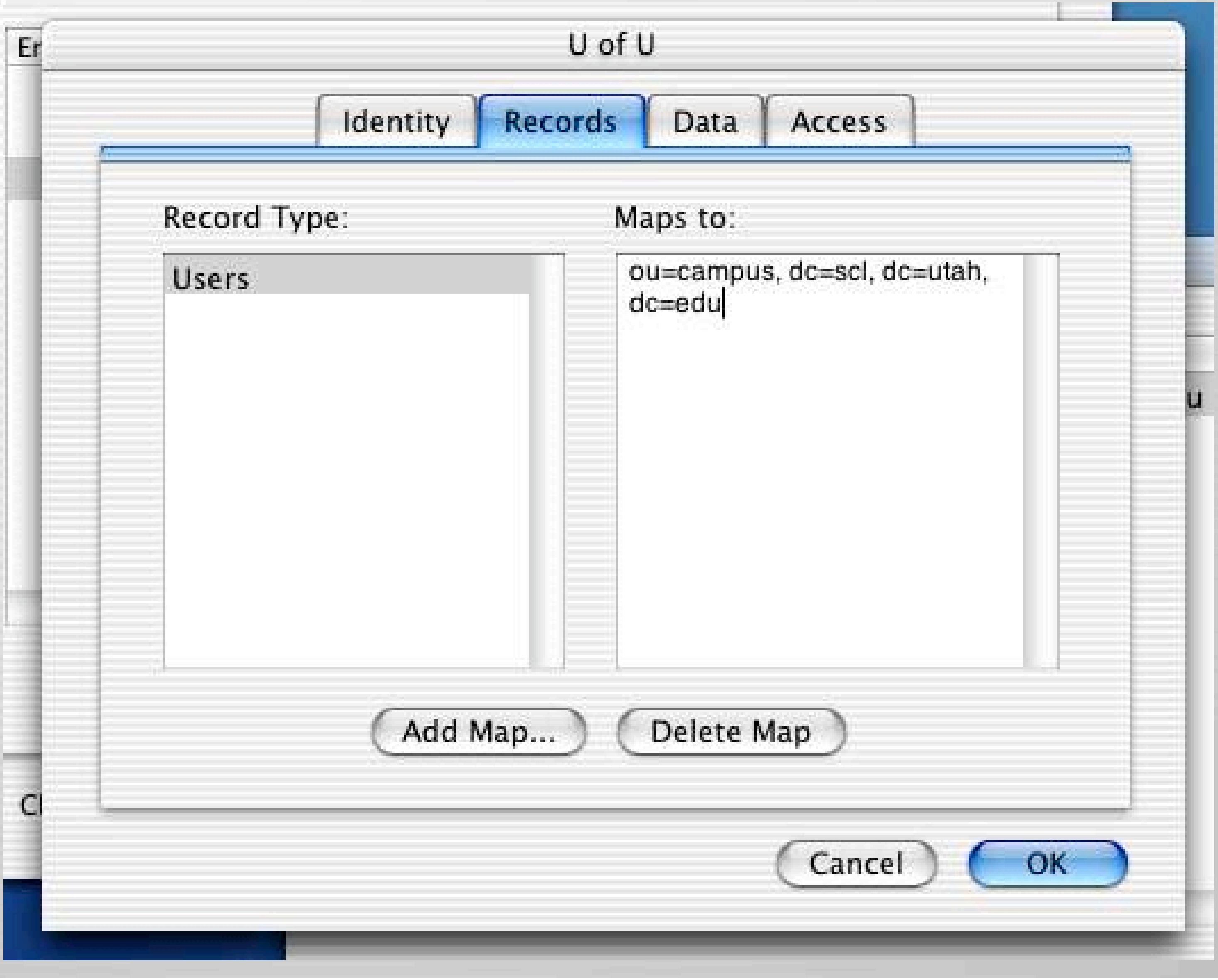
Address: dc1-mmc.scl.utah.edu

Examples

LDAP-My Company

ldap.example.com
or 192.168.100.12

LDAPv2 - Records



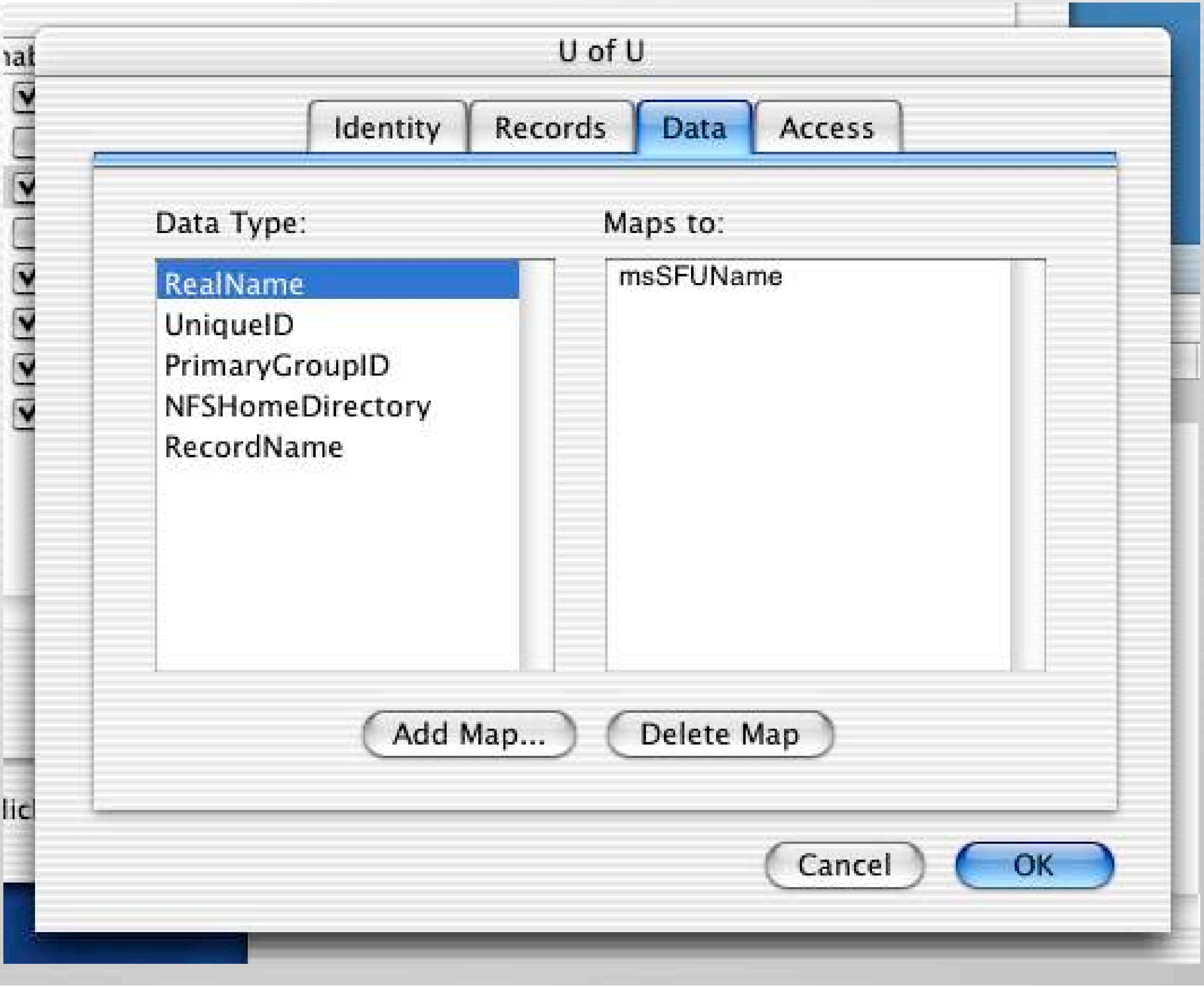
Record Type:

Users

Maps to:

ou=campus, dc=scl, dc=utah, dc=edu

LDAPv2 - Data



U of U

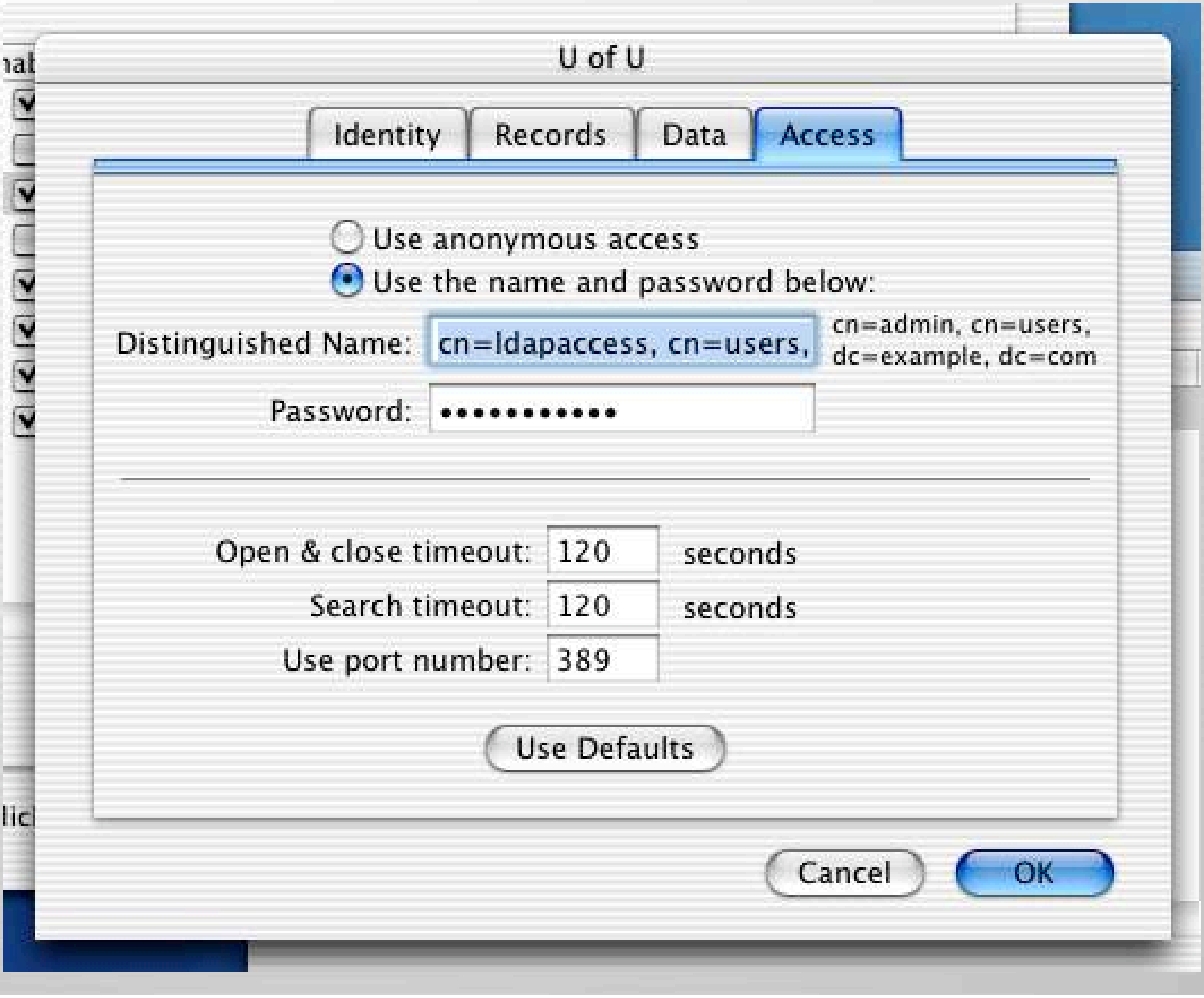
Data Type:

- RealName
- UniqueID
- PrimaryGroupID
- NFSHomeDirectory
- RecordName

Maps to:

msSFUName

LDAPv2 - Access



○ Use anonymous access
● Use the name and password below:

Distinguished Name: cn=ldapaccess, cn=users,

cn=admin, cn=users,
dc=example, dc=com

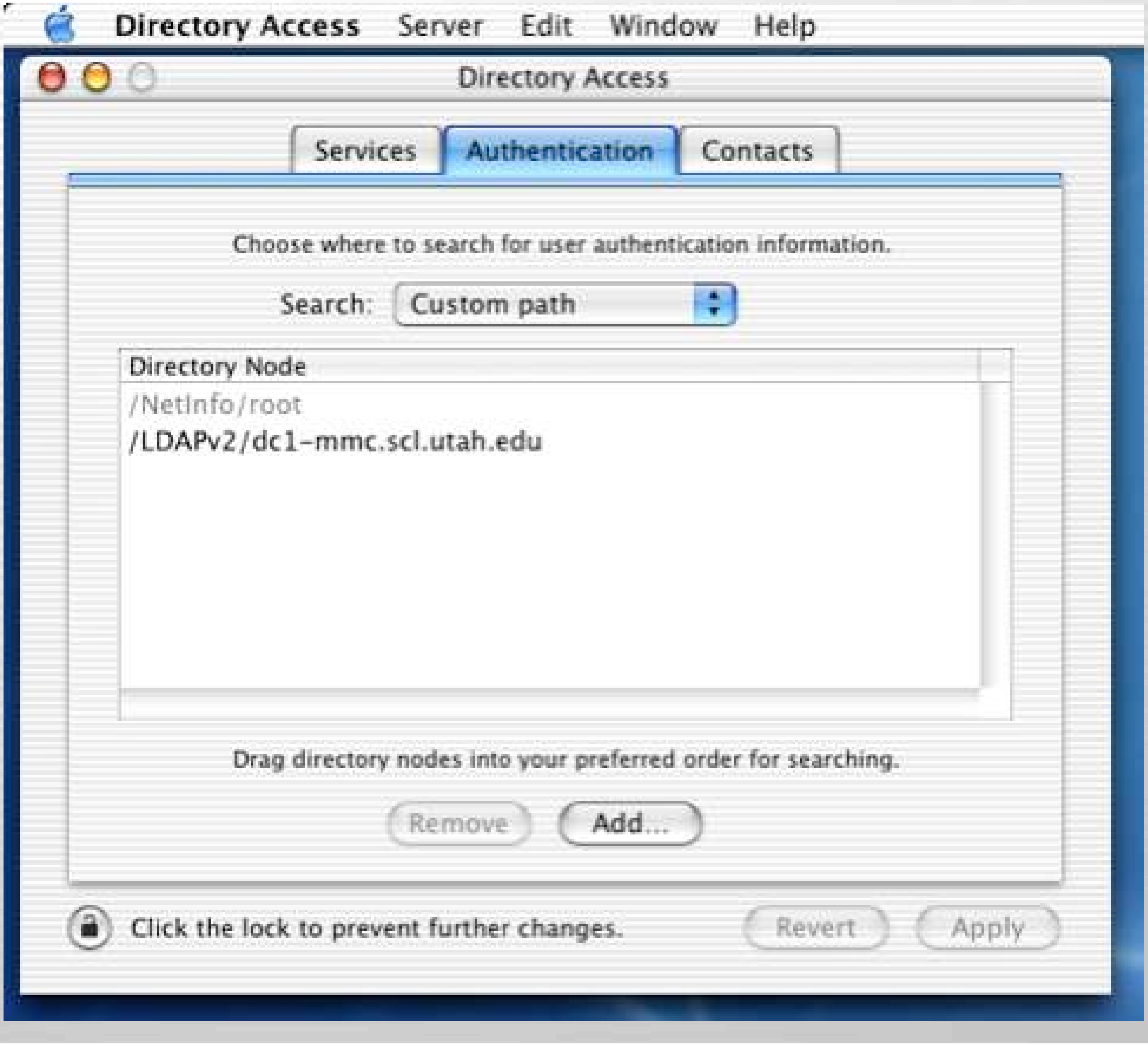
Password: ••••••••••••

Open & close timeout: 120 seconds

Search timeout: 120 seconds

Use port number: 389

Authentication



Choose where to search for user authentication information.

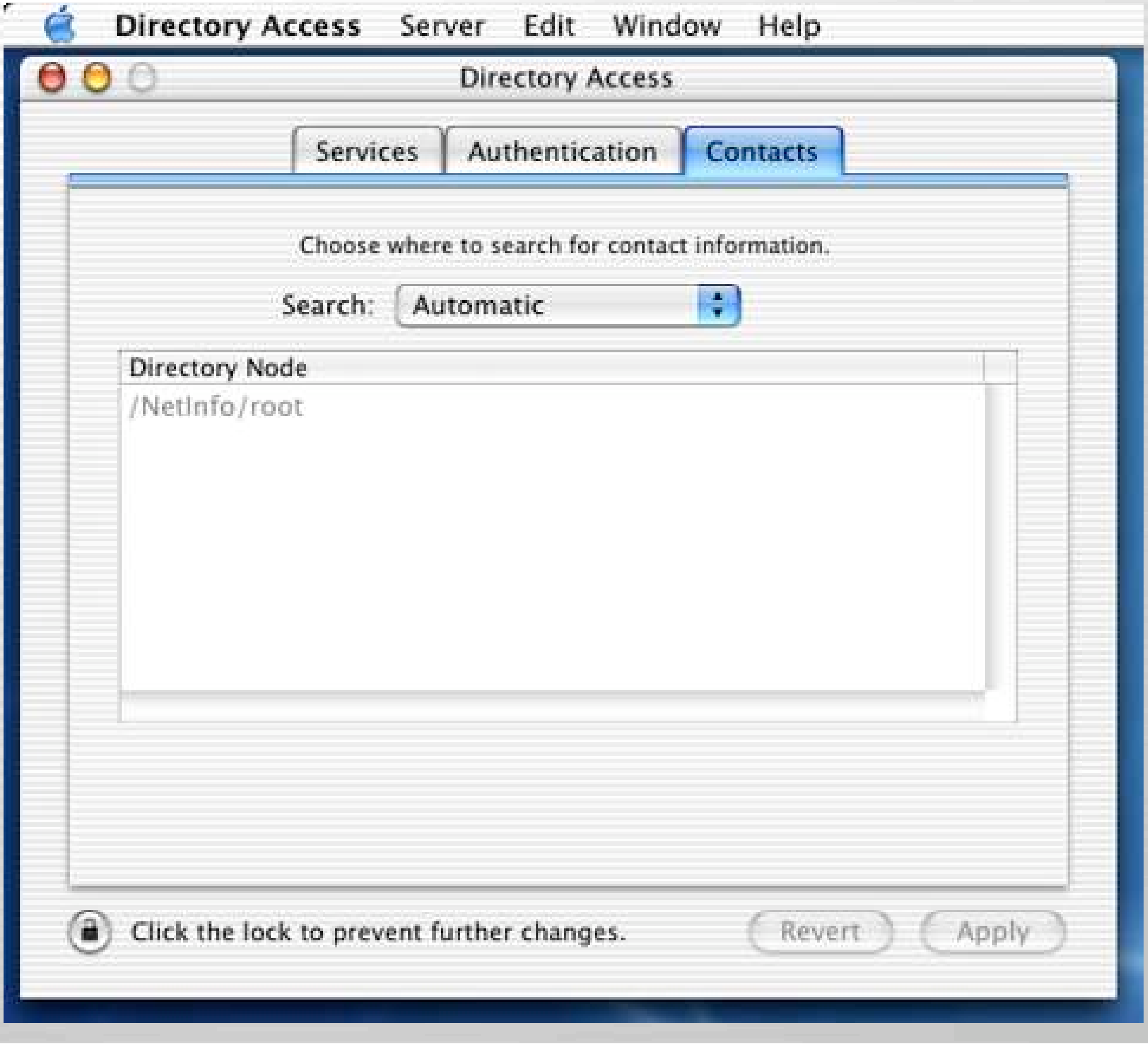
Search: Custom path

Directory Node
/NetInfo/root
/LDAPv2/dc1-mmc.scl.utah.edu

Drag directory nodes into your preferred order for searching.

Click the lock to prevent further changes.

Contacts



Choose where to search for contact information.

Search: Automatic

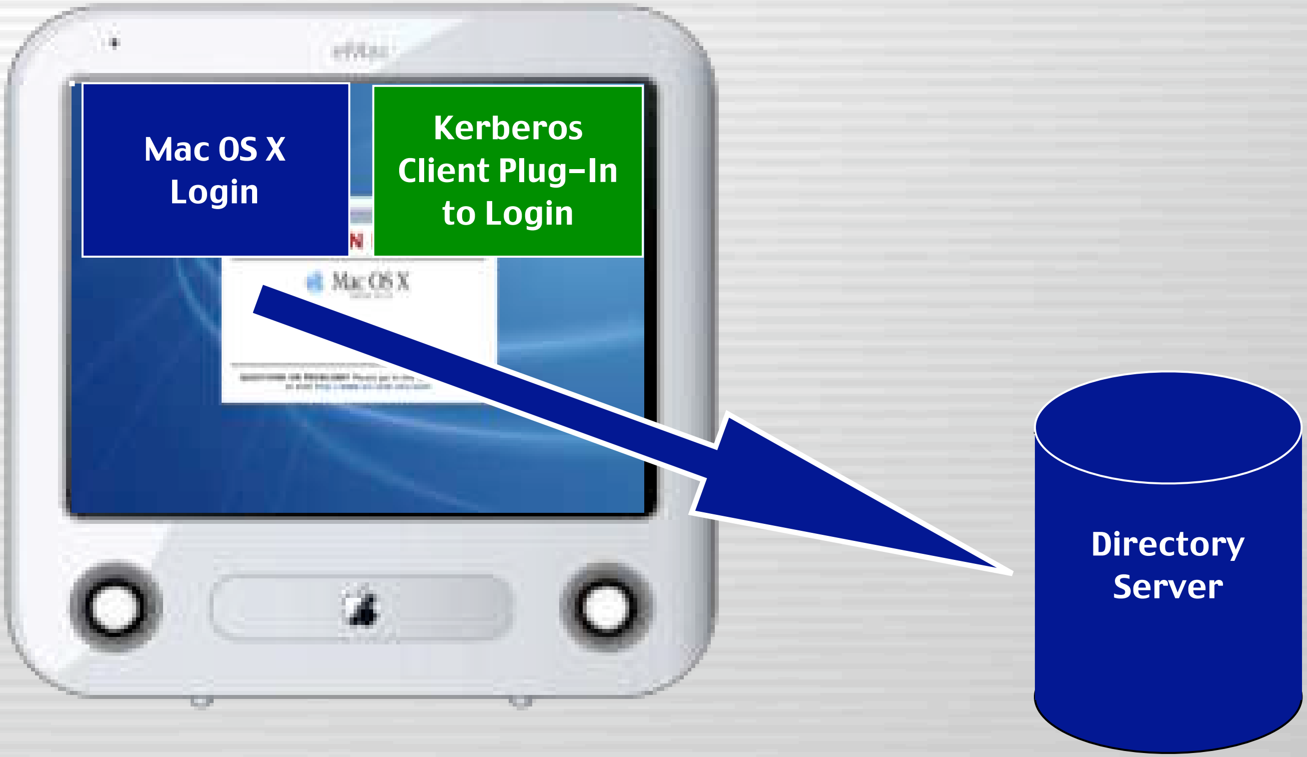
Directory Node

/NetInfo/root

Click the lock to prevent further changes.

Mac OS X Login Process

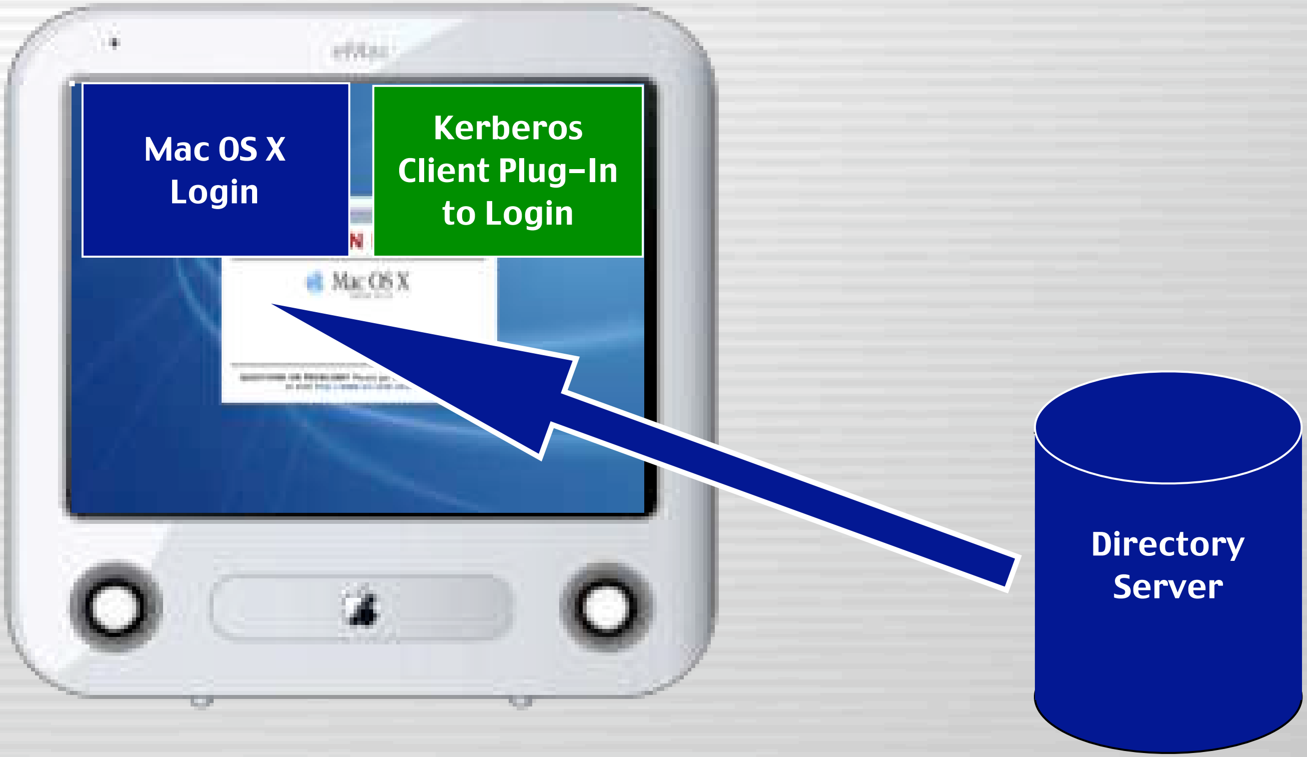
Login passes user name to Directory Server



UNIVERSITY OF UTAH
STUDENT COMPUTING LABS

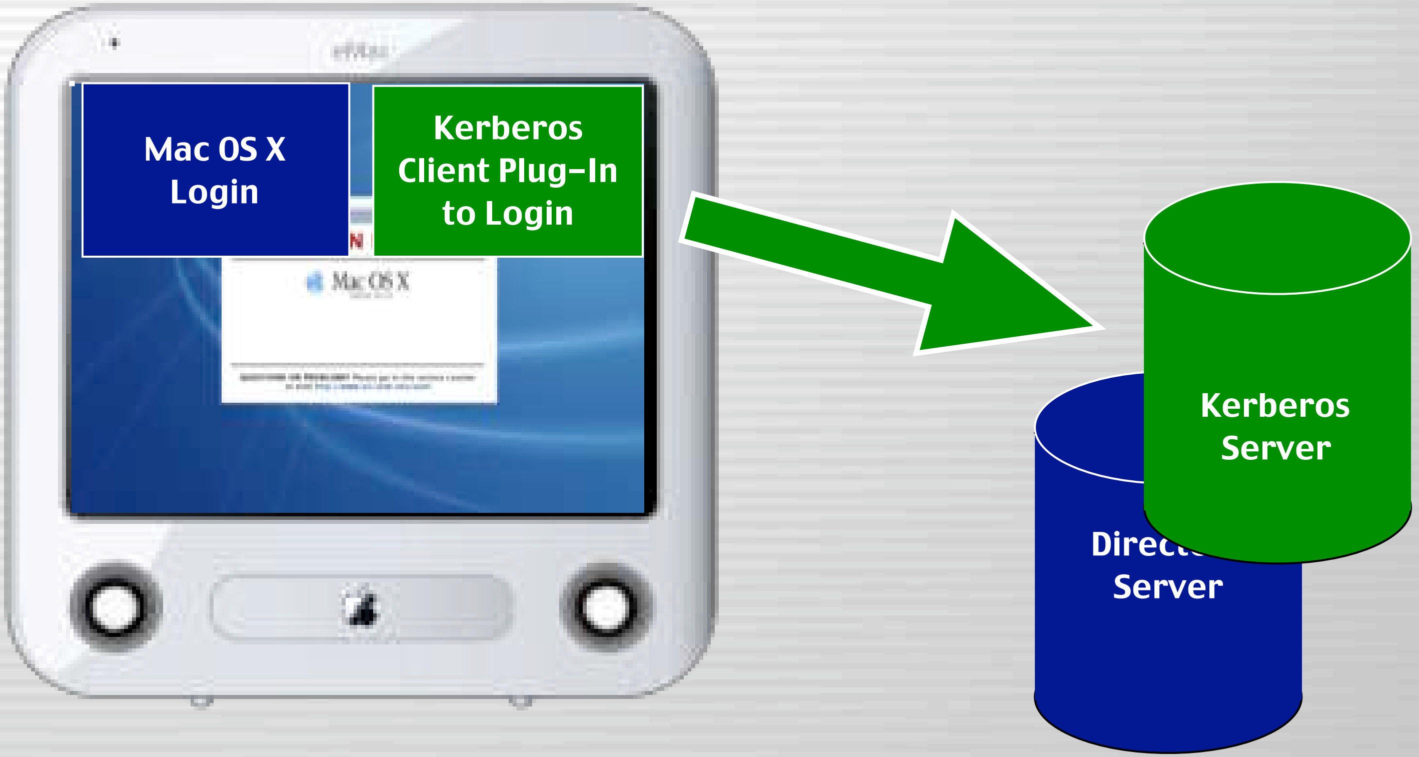
Mac OS X Login Process

If user is in the Directory, user attributes are returned



Mac OS X Login Process

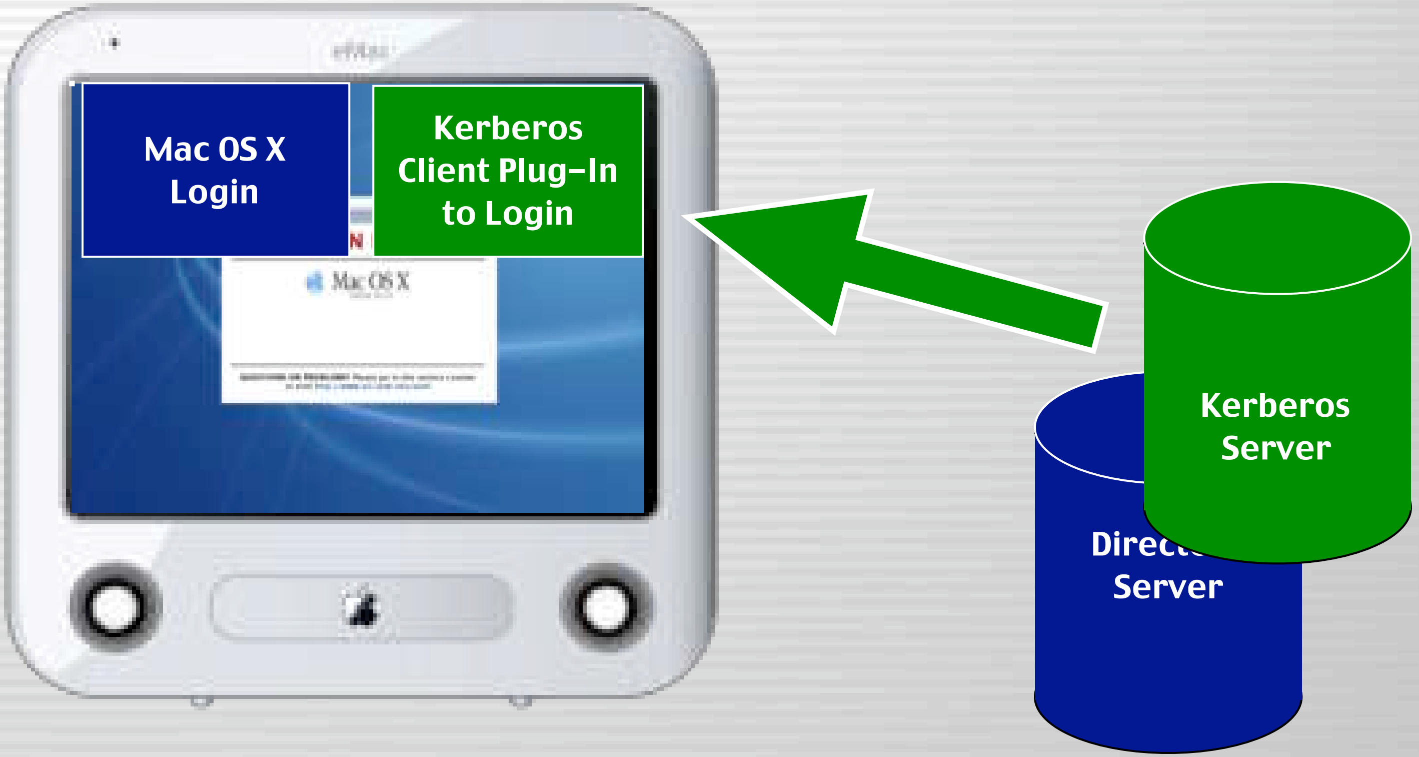
Kerberos Client has user info, so authenticate



UNIVERSITY OF UTAH
STUDENT COMPUTING LABS

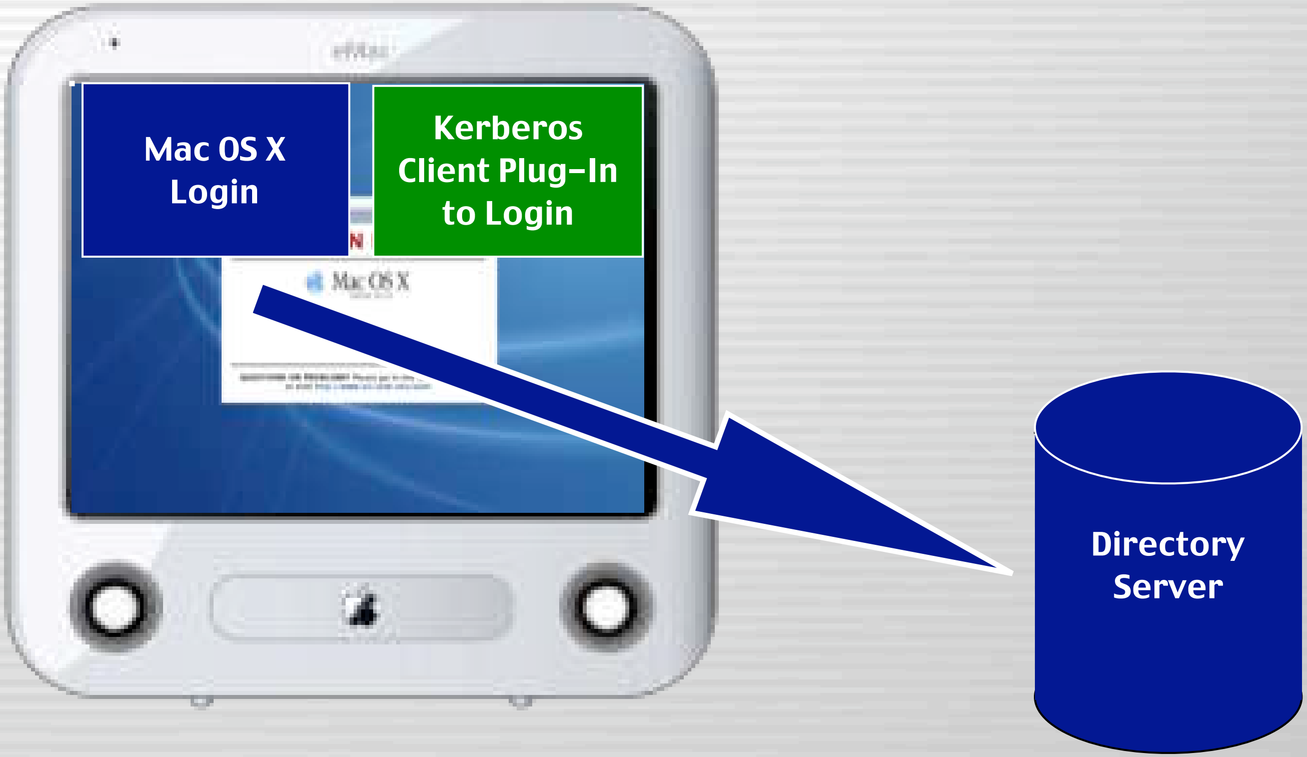
Mac OS X Login Process

Yes! user is authentic



Mac OS X Login Process

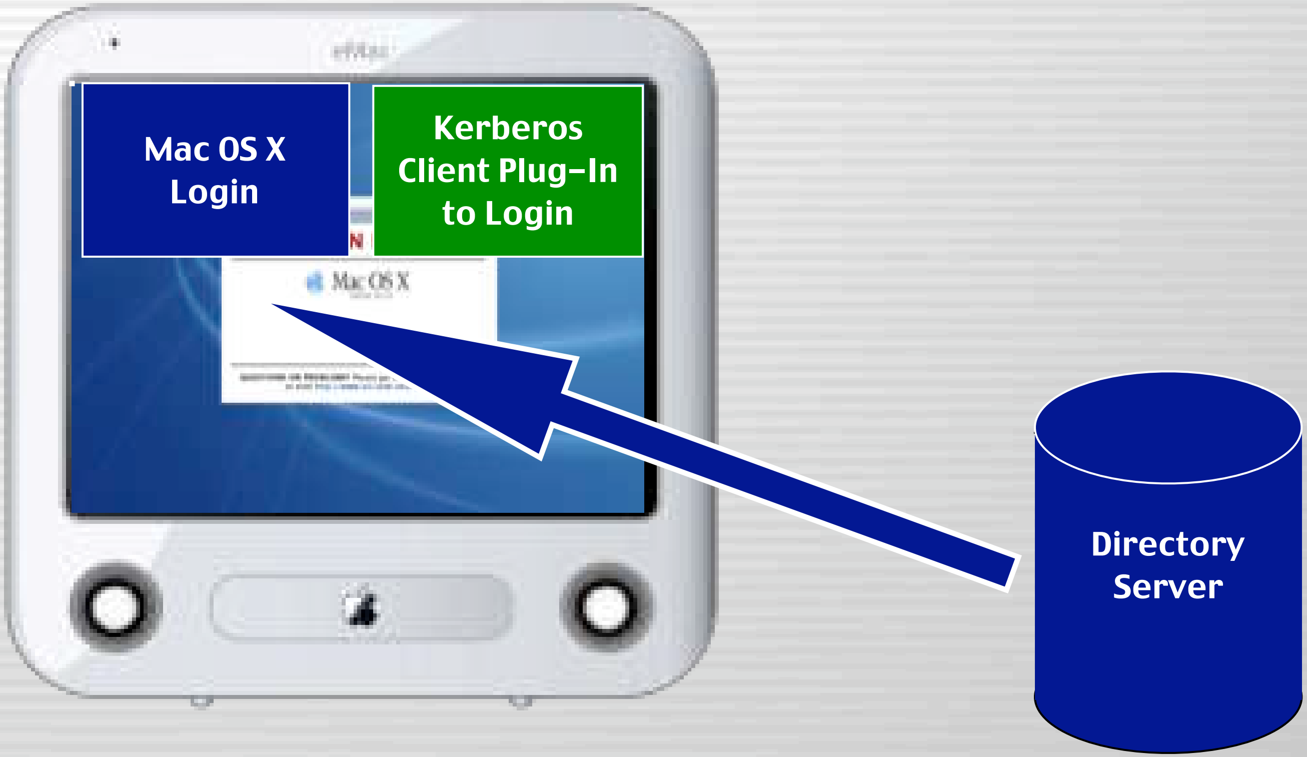
Directory searched again for user attributes



UNIVERSITY OF UTAH
STUDENT COMPUTING LABS

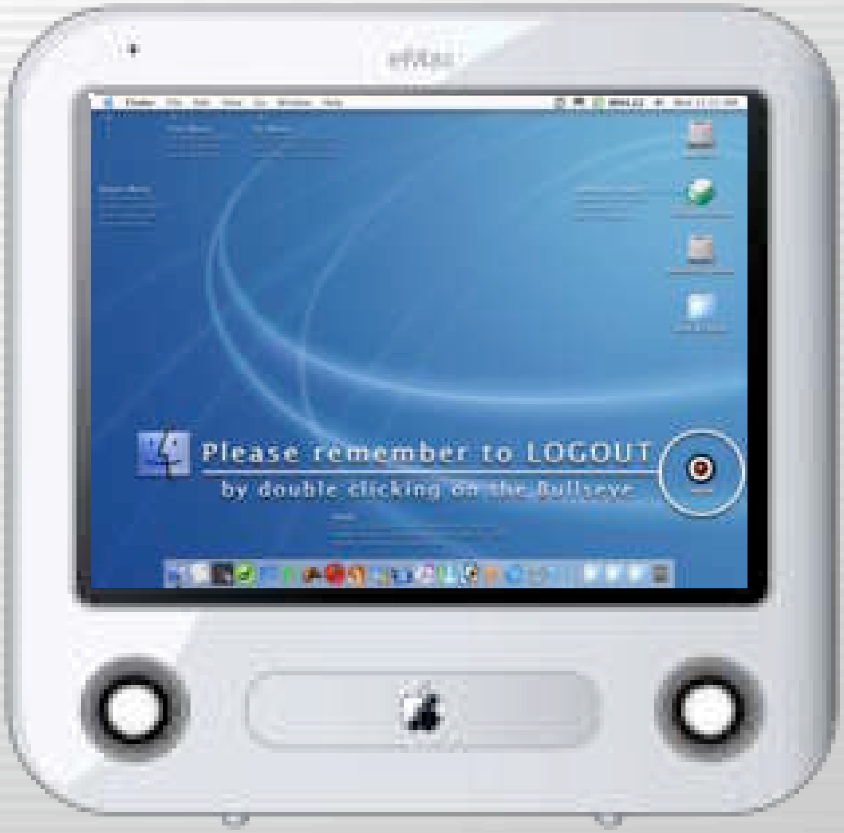
Mac OS X Login Process

Login gets remaining user attributes



Mac OS X Login Process

User is logged in and attributes used for user identity



Please remember to LOGOUT

by double clicking on the Bullseye

UNIVERSITY OF UTAH

STUDENT COMPUTING LABS

Future Goals

- Finer Control for Managed Groups
  - Restrict certain software
  - Restrict certain machines
  - Restrict user services
- Pay for Print based on Authentication
- Managed Disk Space for users
  - minimum fixed limit (quota)
  - lease for extra space

Questions and Answers

?

UNIVERSITY OF UTAH
STUDENT COMPUTING LABS