LDAP105: Clients

If your find these documents useful and feel the need to express that opinion in a tangible way, consider selecting an item from my Amazon Wish List.
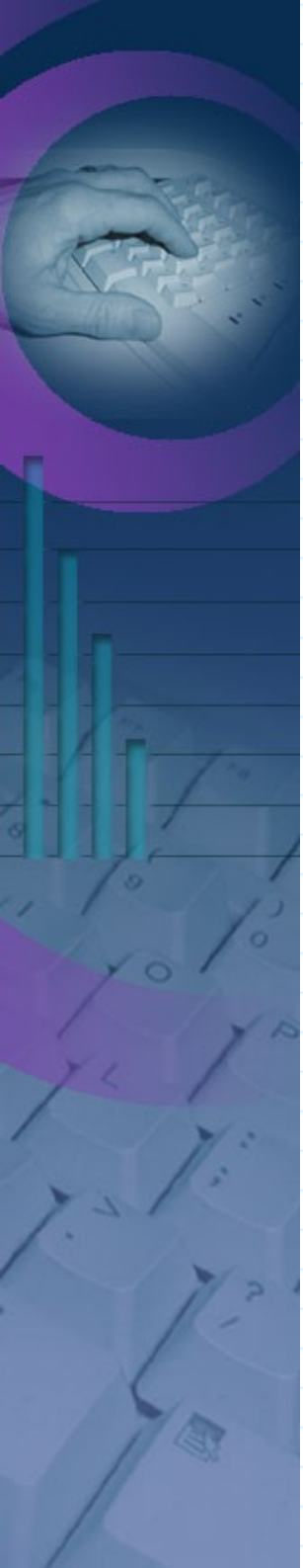
awilliam@whitemice.org

Copyright

If you find this document useful or further it's distribution we would appreciate you letting us know.

ldapsearch w/simple bind
(command line)

sardine:~ $ ldapsearch -x \   "simple" authentication
    -LLL \   less chatter to standard out
    -ZZ \   demand encryption
    -h throw.morrison.iserv.net \   DSA, FQDN if using SSL/TLS
    -b "o=Morrison Industries,c=US" \   search base
    -D "cn=Adam   bind dn
Williams,ou=People,ou=Entities,ou=SAM,o=Morrison
Industries,c=US" \
    -W \   prompt for password
    (&(objectclass=morrisonuser)(uid=adam)) \   search filter
     initials morrisonttymenu   attribute list
Enter LDAP Password: *******
dn: cn=Adam Williams,ou=People,o=Morrison Industries,c=US
initials: ATW
morrisonttymenu: 1103

ldapsearch w/SASL bind

```
sardine:~ $ ldapsearch  \
    -U adam \                          SASL user id
    -Y DIGEST-MD5 \                    SASL mechanism
    -ZZ \
    -LLL \
    -h throw.morrison.iserv.net \
    -b "o=Morrison Industries,c=US" \
    -W \                               prompt for password
    (&(objectclass=morrisonuser)(uid=adam)) \
     initials morrisonttymenu
Enter LDAP Password: *******
{some SASL noise here}
dn: cn=Adam Williams,ou=People,o=Morrison Industries,c=US
initials: ATW
morrisonttymenu: 1103
```

LDIF Modifications

dn: cn=Modify Me,dc=example,dc=com
changetype: modify
replace: mail
mail: modme@example.com
-
add: title
title: Grand Poobah
-
add: jpegPhoto
jpegPhoto:< file:///tmp/modme.jpeg
-
delete: description
-

dn: cn=Barbara Jensen,dc=example,dc=com
changetype: delete

Replace value of
the mail attribute.

Add a title attribute
with specified value.

Load value from file

Remove description attribute(s)

Delete this object.

ldapmodify

sardine:~ $ ldapmodify \
    -U adam \
    -Y DIGEST-MD5 \
    -ZZ \
    -f file.ldif   LDIF file to process.

-v Verbose mode, diagnostics to standard out.
-n Perform no modifications, report what would be done.

DSML
Directory Service Markup Language

- DSML is an OASIS standard that provides the ability to inter-operate with a directory via XML.
  - http://www.dsml.org/download/DSMLdatasheet.pdf
  - DSML has two versions
    - DSMLv1 represented the state of a directory
      - Read only
    - DSMLv2 represents LDAP operations and results
      - Read/Write
      - Also defines a SOAP specification of accessing directory as a traditional Web Service.

DSML: Query

```xml
<?xml version="1.0" encoding="UTF-8"?>
<dsml:batchRequest xmlns:dsml="urn:oasis:names:tc:DSML:2:0:core"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<dsml:searchRequest
 dn="ou=People,ou=Entities,ou=SAM,o=Morrison Industries,c=US"
 scope="wholeSubtree"
 derefAliases="neverDerefAliases"
 sizeLimit="5">
<dsml:filter>
  <dsml:and>
    <dsml:equalityMatch name="objectclass">
     <value>morrisonperson</value></dsml:equalityMatch>
    <dsml:equalityMatch name="title">
     <value>Service Manager</value></dsml:equalityMatch>
    <dsml:equalityMatch name="morrisonbranch">
     <value>BRT</value></dsml:equalityMatch>
  </dsml:and>
</dsml:filter>
<dsml:attributes>
 <dsml:attribute name="mail"/>
</dsml:attributes>
</dsml:searchRequest>
</dsml:batchRequest>
```

Search Specs →

Search Filter →

Search Elements →

DSML: Response

```xml
<?xml version="1.0" encoding="UTF-8"?>
<batchResponse xmlns="urn:oasis:names:tc:DSML:2:0:core"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<searchResponse requestID="6">
<searchResultEntry
dn="cn=************,ou=People,ou=Entities,ou=SAM,o=Morrison
Industries,c=US" requestID="6">
<attr name="mail">
<value>*******************</value>
</attr>
</searchResultEntry>
<searchResultDone requestID="6">
<resultCode code="0" descr="Success"/>
</searchResultDone>
</searchResponse>
</batchResponse>
```

DSML: Services

- DSML is broadly supported
  - DSML for eDirectory
    - http://developer.novell.com/ndk/dsml.htm
  - WDI's BIE (Business Integration Engine)
    - http://www.brunswickwdi.com/bie
  - Exolab's Castor
    - http://castor.codehaus.org/
  - DSML Tools
    - http://www.dsmltools.org/
      - DSML import, export, query, and bidirectional gateway.
  - DSML Services for M$-Windows
    - http://www.microsoft.com/windows2000/server/evaluation/news/bulletins/dsml.asp
  - Canada's Public Work's DSML to LDAP Gateway
    - http://fdis.srv.gc.ca/dsml/dsml_e.htm
      - Just requires a web server with CGI support & Perl

GQ

- gq is an LDAP v3 utility for GNOME/GTK:
  - Features/Advantages
    - DIT browseing and editing.
      - BLOB handling
        - Image rendering for JPEG formats.
      - X.509 Certificates and Certificate Revocation Lists
      - Password encryption
    - Connection encryption (TLS)
    - LDAPv3 schema browser.
      - Objectclasses, attribute types, matching rules, and ldapSyntaxes.
    - Simple, DIGEST-MD5, and Kerberos binds.
    - Exporting to LDIF.
  - Bugs/Problems
    - Development more-or-less stalled.
      - Is a GTK1 vs. GTK2 app.
    - Likes to crash during configuration
    - Hangs if connection to the DSA is lost.
    - No printing support.

GQ
Color Coding

cn=Sally Ward,ou=People,o=Morrison Industries,c=US

dn	cn=Sally Ward,ou=People,o=Morrison Ind
objectClass	top
	organizationalPerson
	inetOrgPerson
	morrisonperson
	posixAccount
	sambaAccount
	inetLocalMailRecipient
	morrisonuser
sn	Ward
cn	Sally Ward
userPassword	{crypt}A/uG3PgUfeHx6 Crypt
telephoneNumber	8102276311
seeAlso	
description	

Apply   Refresh   Close

• How the attribute of an object relates to the schema is presented to the user via the color of the attribute name.

- blue
  - An attribute required by one of the object's objectclass attributes.
- black
  - An attribute allowed, but not required by the object's objectclass attributes.
- red
  - Special attribues such as DSA meta-information or attributes allowed by the presence of an extensibleObject objectclass attribute.
- orange
  - An attribute that belonged to an objectclass that has been removed from the object. These will be deleted when Apply is clicked.
- purple
  - An attribute the user added to an object; applies only to extensibleObject objects.

GQ

BLOBS

- GQ has built in viewers for:
  - JPEG images
  - crypted passwords
  - X.509 certificates
  - X.509 certificate revocation lists.
- In GQ parlance these are called custom displaytypes.
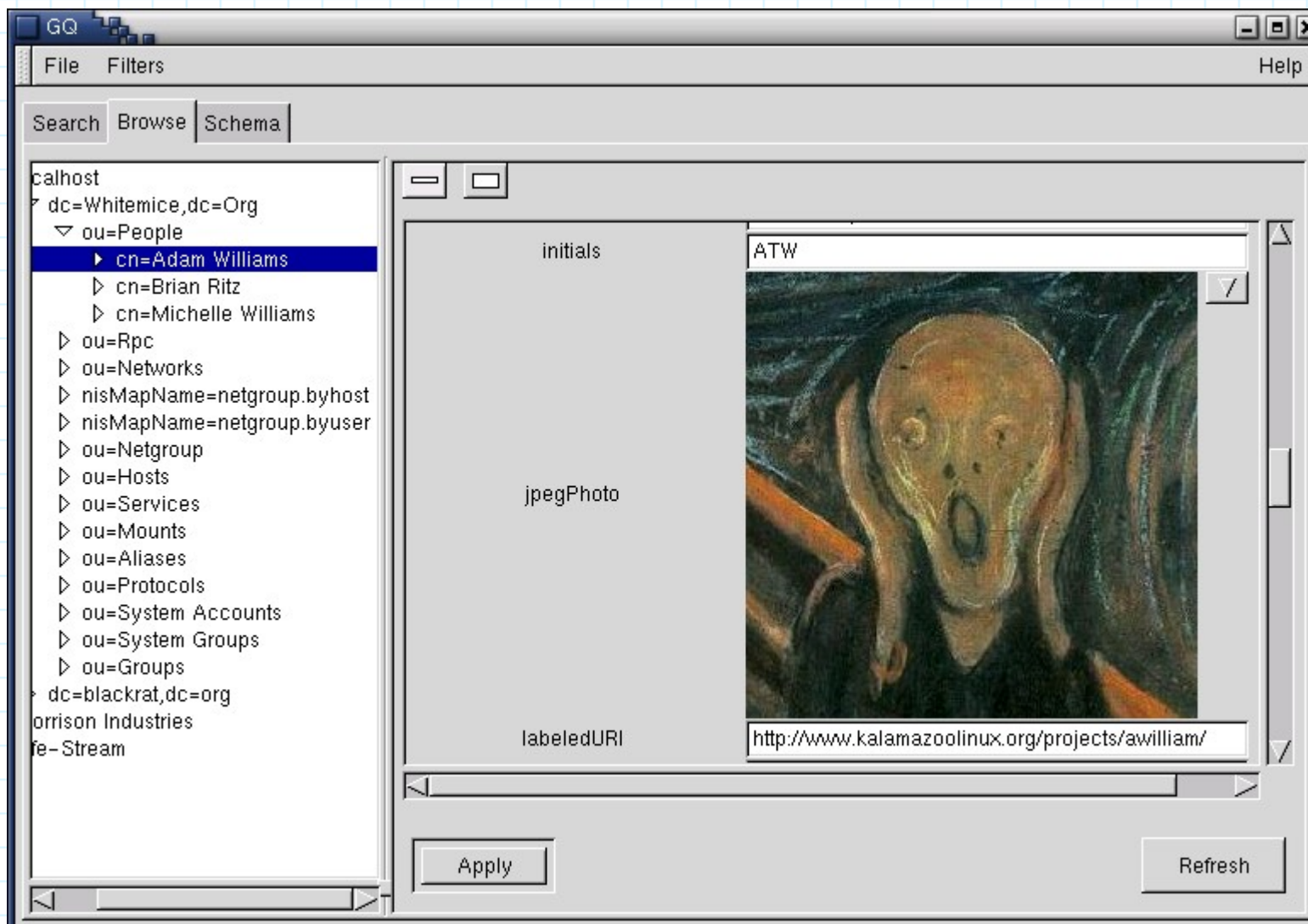
GQ
(Schema Browser)
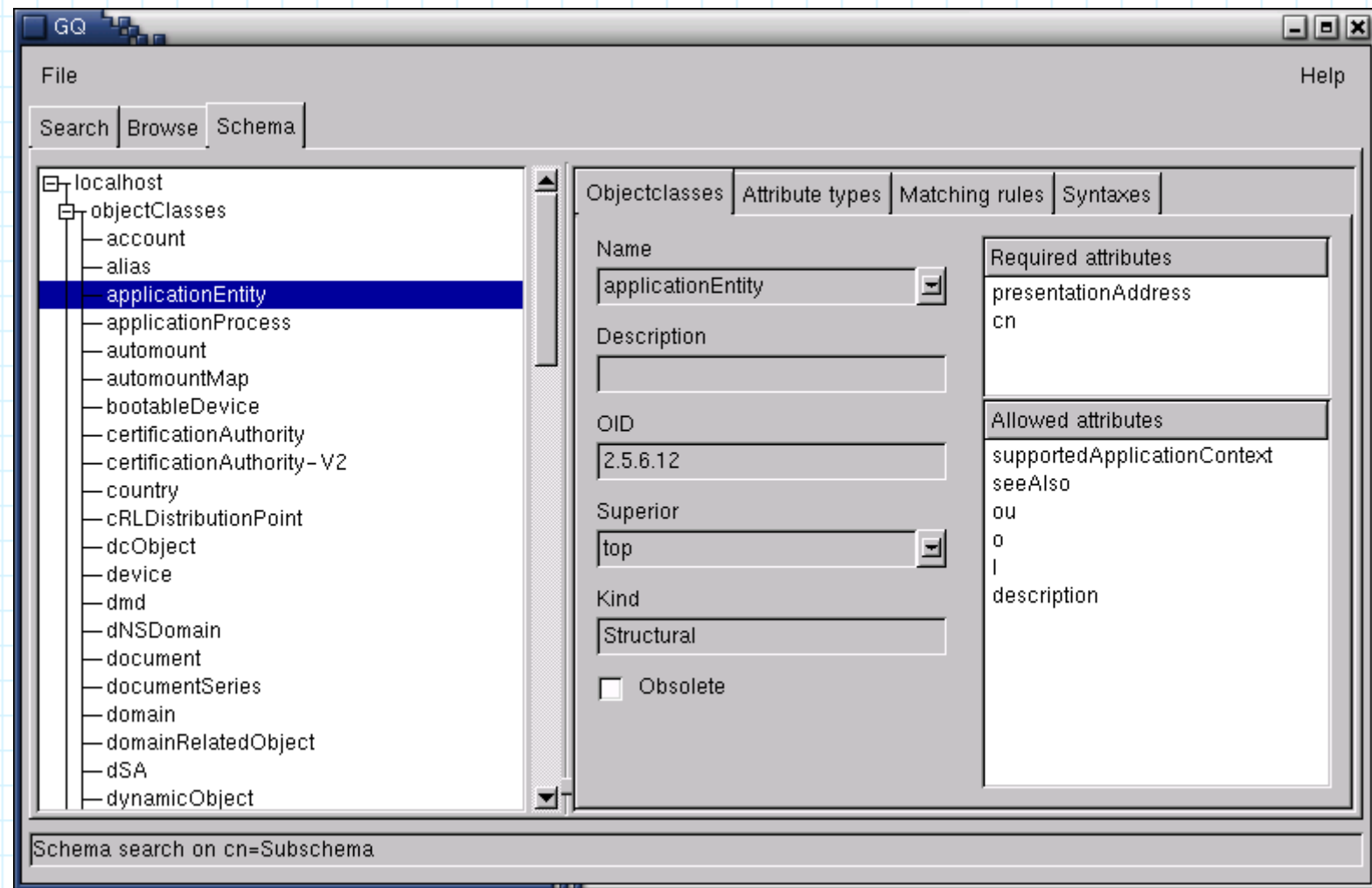
GQ

This zone is for loading and unloading only.

- Managing complex datatypes in a Dit is greatly facilitated by the GQ's object browser.
  - Non-string and numeric attribute values can be:
    - Displayed in various notations
      - Plain
      - Base64 encoded
      - Hexidecimal
    - Loaded from a file
    - Unloaded to a file

initials	ATW
jpegPhoto	
labeledURI	http://www.kalamazoolinux.org/projects/awilliam/
mail	awilliam@Whitemice.Org
manager	

Import
Export
Delete
___
Plain
Base64
Hex

KDirAdm

http://www.carillonis.com/kdiradm/

- KDE Directory Administrator is the equivalent of GNOME's gq
  - Including schema browsing
  - It does not support Kerberos V (GSSAPI) or SSL, so all communication with the DSA is performed in the clear.
  - Development equally stalled.

jXplorer

http://www.jxplorer.org/
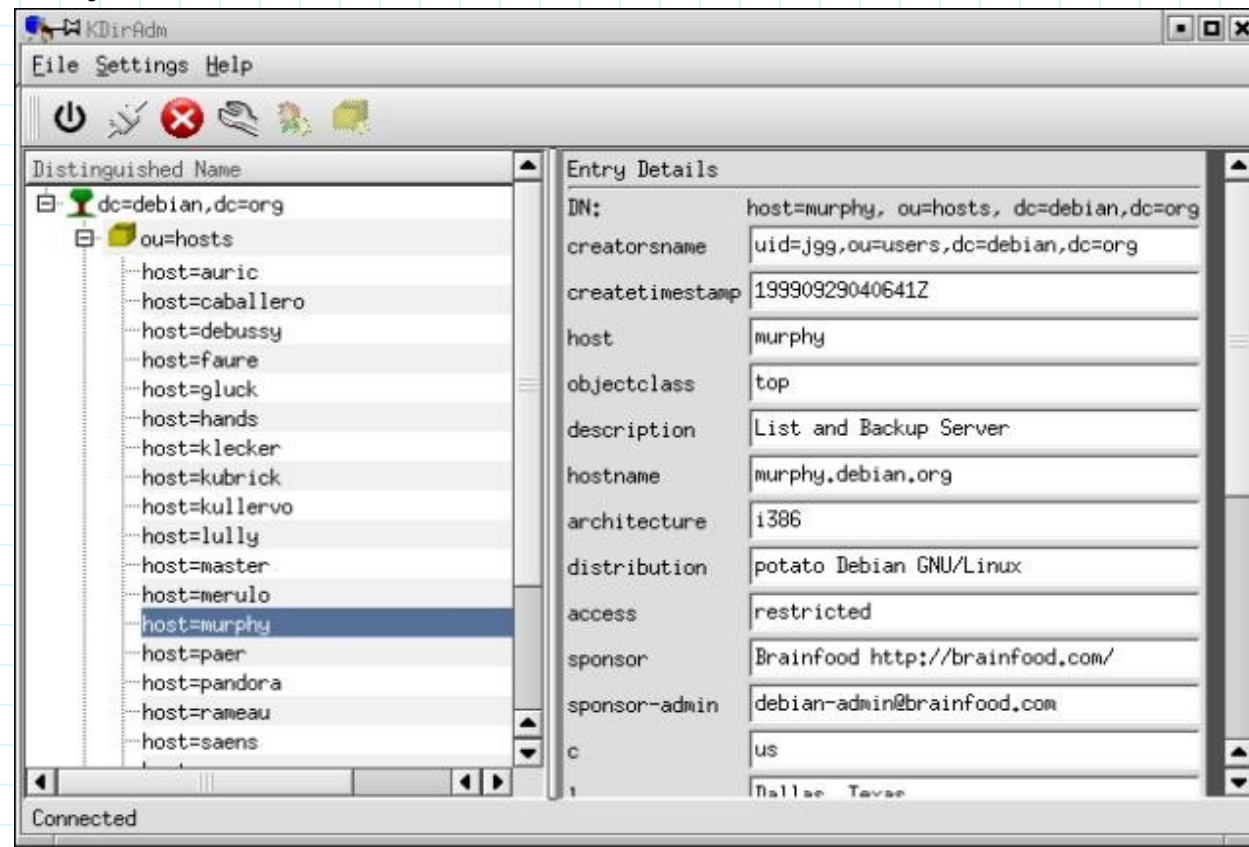
- jXplorer is a Java LDAP browser and management tool.
  - Supports SSL and SASL
  - BLOB & complex value management
    - Images
    - Certificates
    - Passwords
  - LDIF import and export
  - Anonymous DSML
  - Immensely customizable

MaXware' MDE
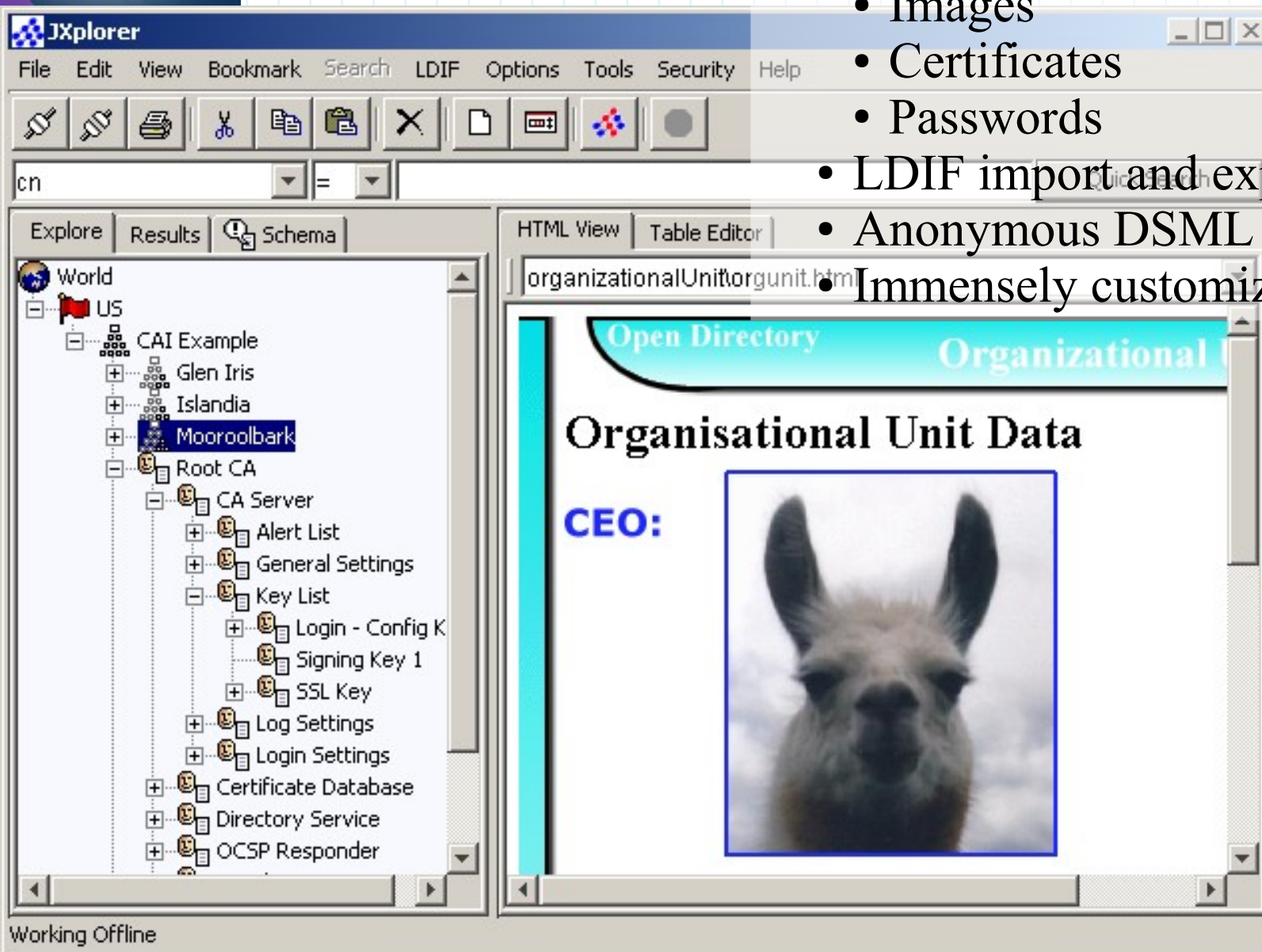
http://www.maxware.com/Products/MDE/
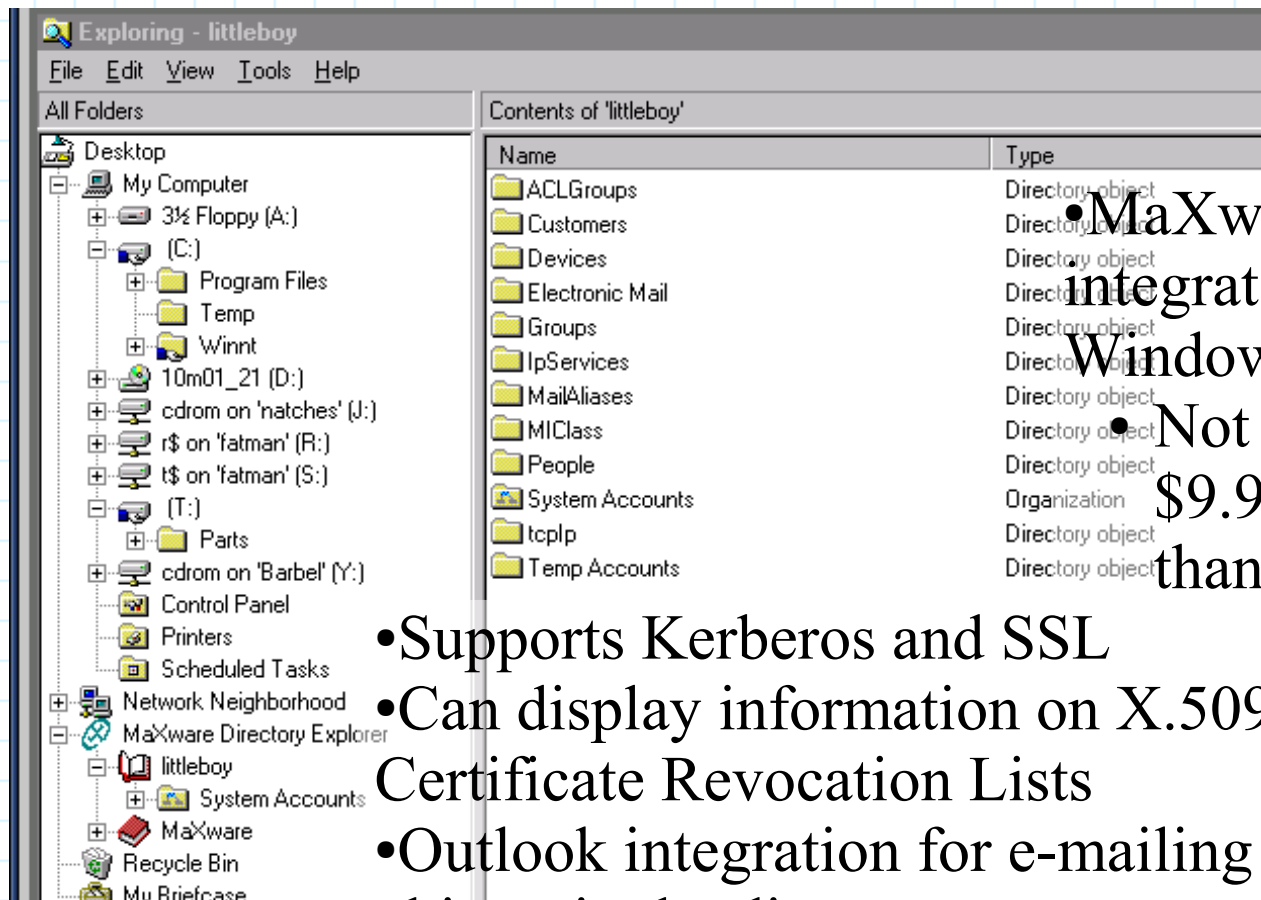
• MaXware's MDE integrates into Microsoft Windows Explorer.

• Not a FREE package; $9.95 a seat for less than 500 seats.

• Supports Kerberos and SSL
• Can display information on X.509 Certificates and Certificate Revocation Lists
• Outlook integration for e-mailing to groupOfNames objects in the directory.
• Runs on Windows 95/98, >NT4sp3, 2000, and XP.

phpLDAPadmin
http://phpldapadmin.sourceforge.net/

- phpLDAPadmin is a LDAP browser/editor for intranets.
  - Features/Advantages
    - DIT browseing and editing.
      - BLOB handling
        - Image rendering for JPEG formats.
      - Password encryption
    - Connection encryption (TLS)
    - LDAPv3 schema browser.
      - Objectclasses, attribute types, matching rules, and ldapSyntaxes.
    - LDIF (import and export) and DSML (export) support.
    - Wizard for creating, copying, and renaming objects.
    - Relevant attributes (mail, seeAlso, etc...) are rendered as hyperlinks.
  - Bugs/Problems
    - No SASL bind support
      - This is actually more PHP's fault than phpLDAPadmin's.
    - No certificate management support.

phpLDAPadmin

phpLDAPadmin - CVS - Mozilla

File Edit View Go Bookmarks Tools Window Help

http://raider/phpldapadmin/

phpLDAPadmin - CVS

💡 Request a new feature

🐞 Report a bug

🖥 Raider
(schema | search | refresh | create | info | import)

⊟ 🌐 dc=example , dc=com (9)

  ⊞ 👤 cn=admin

  ⊞ 👤 cn=dave test

  ⊞ 👥 cn=MyGroup

  ⊞ 👤 cn=test

  ⊞ 👤 cn=test smith2

  ⊞ 👥 ou=automount

  ⊟ 👥 ou=People (22)

    cn=Funk Bob

    ⊞ 👤 cn=Haberland felix

    ⊞ 👤 cn=Joe2

    ⊞ 👤 cn=Kazik Francuski

    ⊞ 👤 cn=Smith Dave

    ⊞ 👤 cn=thomas bob

    ⊞ 👤 cn=Verónica (1)

  ⊞ 👥 ou=People-copy8 (21)

DSA's schema can be browsed.

"Wizard" for creating new object.

Create Object

On server 'Raider', using template 'Custom'

Step 1 of 2: Name and ObjectClass(es)

RDN: `cn=new entry` (example: cn=MyNewPerson)

Container `dc=example,dc=com` 🔍
browse

ObjectClasses
```
oncRpc
OpenLDAProotDSE
organization
organizationalPerson
organizationalRole
organizationalUnit
person
pilotDSA
pilotOrganization
pilotPerson
posixAccount
posixGroup
qualityLabelledData
referral
residentialPerson
RFC822localPart
```

💡 Hint: You must choose at least one structural objectClass

[Proceed >>]

phpLDAPadmin

File Edit View Go Bookmarks Tools Window Help

http://raider/phpldapadmin/

phpLDAPadmin - CVS

Request a new feature
Report a bug

Raider

(schema | search | refresh | create | info | import)

- dc=example , dc=com (9)
  - cn=admin
  - cn=dave test
  - cn=MyGroup
  - cn=test
  - cn=test smith2
  - ou=automount
  - ou=People (22)
    - cn=Funk Bob
    - cn=Haberland felix
    - cn=Joe2
    - cn=Kazik Francuski
    - cn=Smith Dave
    - cn=thomas bob
    - cn=Verónica (1)
    - ou=People-copy8 (21)
    - uid=bäb
    - uid=dsmith
    - uid=esanford
    - uid=gsanford

Waiting for raider...

Sophisticated query tool.

Support for jpegPhoto attributes.

Advanced Search Form
(Simple Search Form | Predefined Searches)

Server	Raider
Base DN	dc=example,dc=com
Search Scope	Sub (entire subtree)
Search Filter	jpegPhoto=*
Show Attributes	cn, jpegPhoto, postalAddress

Search

Searching...
Entries found: **121** (1.67 seconds).
Showing results **1** through **50**.
« 1 2 3 »

cn=Haberland felix

dn   cn=Haberland felix,ou=People,dc=example,dc=com
cn   Haberland felix
jpegPhoto

mono::

cn=Joe2

dn   cn=Joe2,ou=People,dc=example,dc=com
cn   Joe2
jpegPhoto

LDAP Account Manager
http://lam.sourceforge.net/

- A web based interface loosely associated with the Samba project.
  - Supports the various NSS related objectclasses.
  - Supports the Samba v3 schema.

Evolution

- Of all the clients tested Novell's Evolution has the most complete and robust LDAP support.
  - Pros
    - Write support!
    - Lots of information exposed.
  - Cons
    - No support for SASL binds.
  - Notes
    - Requires the installation of the Evolution specific schema.
      - These objectclasses are structural, and thus create objectclass chaining problems.
      - Use the mHybridPerson objectclass.

Evolution

Creating an LDAP Addressbook

In the "Contacts" view right click in the sources pane and select "New Address Book".

Address Book Properties

General | Details

Display

Name: MI4 Enterprise Directory (Aliases)

Server Information

Server: littleboy.morrison.iserv.net

Port: 389

Use secure connection: Always

Authentication

Log in method: Using distinguished name (DN)

Login: cn=Adam Williams,ou=People,o=M

Cancel | OK

Address Book Properties

General | Details

Searching

Search base: stems,o=Morrison Industries,c=US

Find Possible Search Bases

Search scope: Sub

Downloading

Timeout: 1 ————————— 5 minutes

Download limit: 100 cards

Cancel | OK

No SASL support for DSA binding!

Evolution

Contact Search

Searching works the same as with a local address book.

Evolution
Contact Information

cn

fileAs*

displayName

Contact Editor

Contact | Personal Information | Mailing Address

Full Name... Adam Williams   Nickname: Adam Williams

File under: Williams, Adam   Where: MI4 Enterprise Directory (Users)

Categories

Email

mail

Work adam@morrison-ind.com   Other

Home   Other

Wants to receive HTML mail

facsimileTelephoneNumber

homePhone

telephoneNumber

Telephone

Business Fax 6163611124   Business Phone 6164473822

Home Phone 6164568931   Other Fax 6163611775

Assistant Phone 6164473820   Other Phone

mobile

Mobile Phone 6165818010   Other Phone

Instant Messaging

AIM   ICQ

Yahoo   GroupWise

Help   Cancel   OK

Evolution

Contact Information

Evolution

Contact Information

Contact Editor

Contact | Personal Information | Mailing Address

Home

Address: 537 Shirley St. NE
Grand Rapids, Mi.
49503

PO Box:

City:
Zip/Postal Code:
State/Province:
Country:

postalAddress

Work

Address: 1825 Monroe Ave NW
Grand Rapids, Mi.
49505

PO Box:

City:
Zip/Postal Code:
State/Province:
Country:

Other

Address:
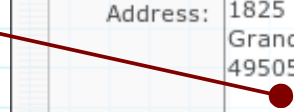
PO Box:

City:
Zip/Postal Code:
State/Province:
Country:

Help

Cancel

OK

Evolution

Autocompletion

Evolution
(Meetings)

Autocompletion sources are available for selecting as meeting attendees as well.

Evolution

(Search Dialog)

- ➢ (& and
  - ➢ (| or
    - ➢ (| or
      - ➢ (fileAs=rob)
      - ➢ (& and
        - ➢ (! not
          - ➢ (fileAs=*)
        - ➢)
        - ➢ (sn=rob)
      - ➢)
    - ➢)
    - ➢ (displayName=rob)
    - ➢ (| or
      - ➢ (cn=rob)
      - ➢ (sn=rob)
    - ➢)
    - ➢ (mail=rob)
  - ➢)
  - ➢ (mail=*)
- ➢)

Compose a message

File Edit Format View Insert Security

Send Attach Undo Redo Cut Copy Paste Find Replace Image Link Rule Table

From: Adam Tauno Williams <awilliam@whitemice.org>   Signa

To:

Cc:

Bcc:

Subject:

+0   N

Select Contacts from Address Book   ✕

Show Contacts

Address Book: MI4 Enterprise Directory (MVP Customers)

Category: All Categories

Search: rob   Find

Contacts

Cervantes, Robert
Conley, Robin
Cox, Robin
Daughtrey, Robert
Green, Robbie
Mann, Robert
May, Rob
Randall, Robert
Roberts, Chris
Robillard, Mark
Robinson, Butch
Robinson, Priscilla
Rodrigue, Robbie
Serfas, Robert
Topolski, Robert
Whitlock, Roberta

To:

Cc: ->

Bcc: ->

✕ Cancel   ✓ OK

WAB

Windows Address Book

- WAB is the address book integrated into most Microsoft Windows applications, including Microsoft Outlook.
  - Pros
    - Used by most Windows applications
    - Lots of information exposed.
    - Supports SSL
  - Cons
    - Read only.
    - No support for SASL binds.
  - Notes
    - Requires the installation of the Outlook specific schema.
      - These objectclasses are structural, and thus create objectclass chaining problems.
      - Use the mHybridPerson objectclass.

WAB
Creating an LDAP source
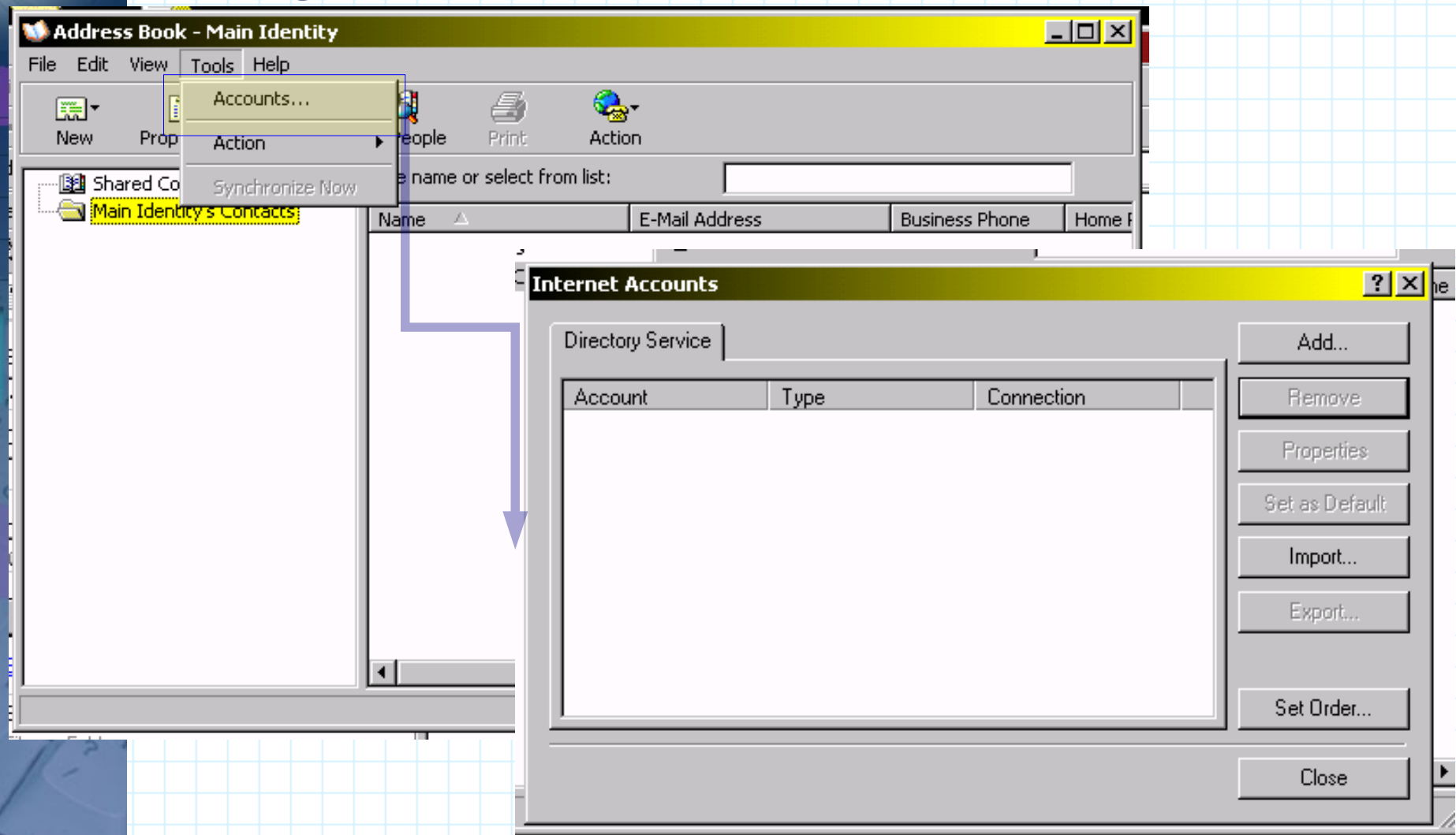
WAB
Configuration

Internet Accounts

Internet Connection Wizard

Internet Directory Server Name
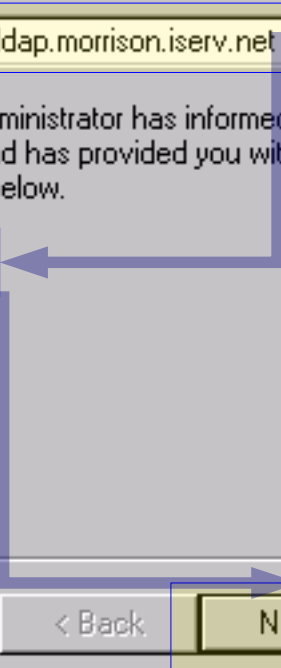
Type the name of the Internet directory (LDAP) server your Internet service provider or system administrator has given you.

Internet directory (LDAP) server: | ldap.morrison.iserv.net

If your Internet service provider or system administrator has informed you that they require you to log on to your LDAP server and has provided you with an LDAP account name and password, select the check box below.

☑ My LDAP server requires me to log on

< Back | Next > | Cancel

WAB
Configuration

Internet Connection Wizard

Internet Directory Server Logon

Type the LDAP account name and password your Internet service provider has given you.

Account name: `cn=Adam Williams,ou=People,o=Morrison Industries,c=US`

Password: `********`

If your Internet service provider requires you to use Secure Password Authentication (SPA) to access your LDAP account, select the 'Log On Using Secure Password Authentication (SPA)' check box.

☐ Log on using Secure Password Authentication (SPA)

< Back   Next >   Cancel

WAB
Configuration

Internet Connection Wizard

Check E-mail Addresses

Your e-mail program checks the e-mail addresses of your message recipients using one or more directory service address lists.

Using a directory service to check the e-mail addresses of your message recipients may slow down the performance of your e-mail program.

Do you want to check addresses using this directory service?

○ Yes

◉ No

required to set up your account.

< Back | Next > | Cancel

Back | Finish | Cancel

WAB

Viewing the configuration

If you thought you were done configuring WAB because you clicked "Finish", in typical Microsoft fashion – you're wrong.
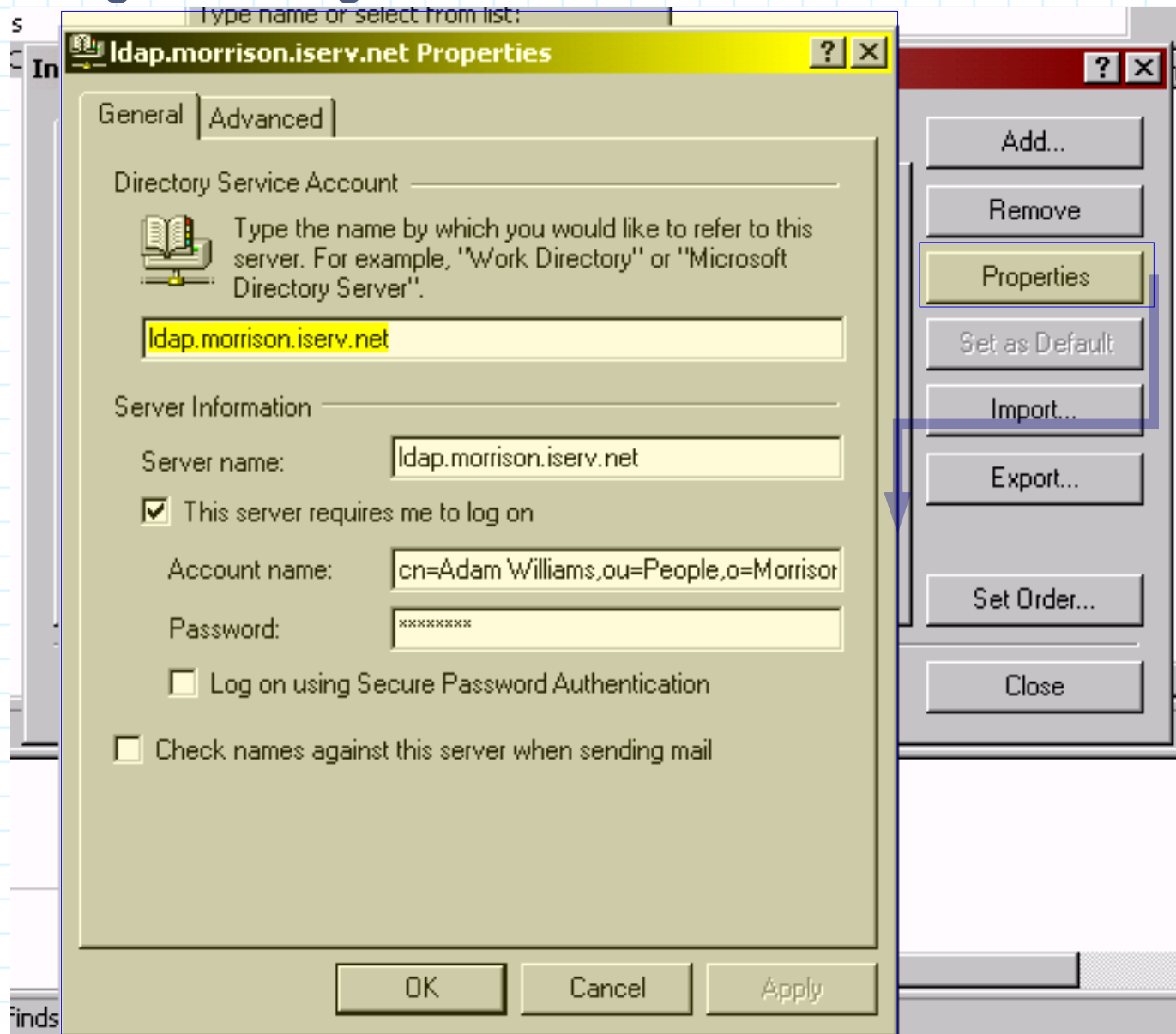
WAB

Setting the search base
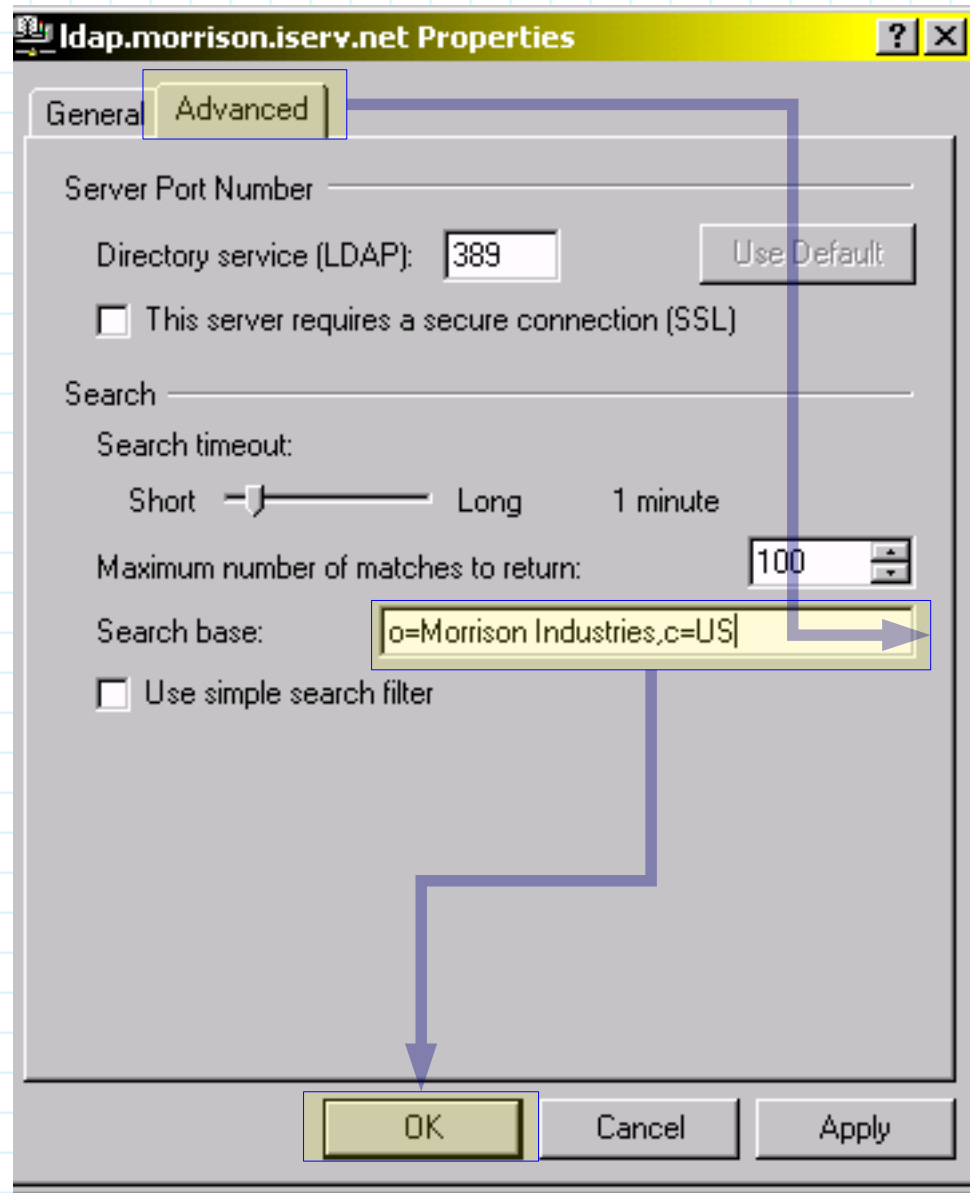
WAB
Simple Search
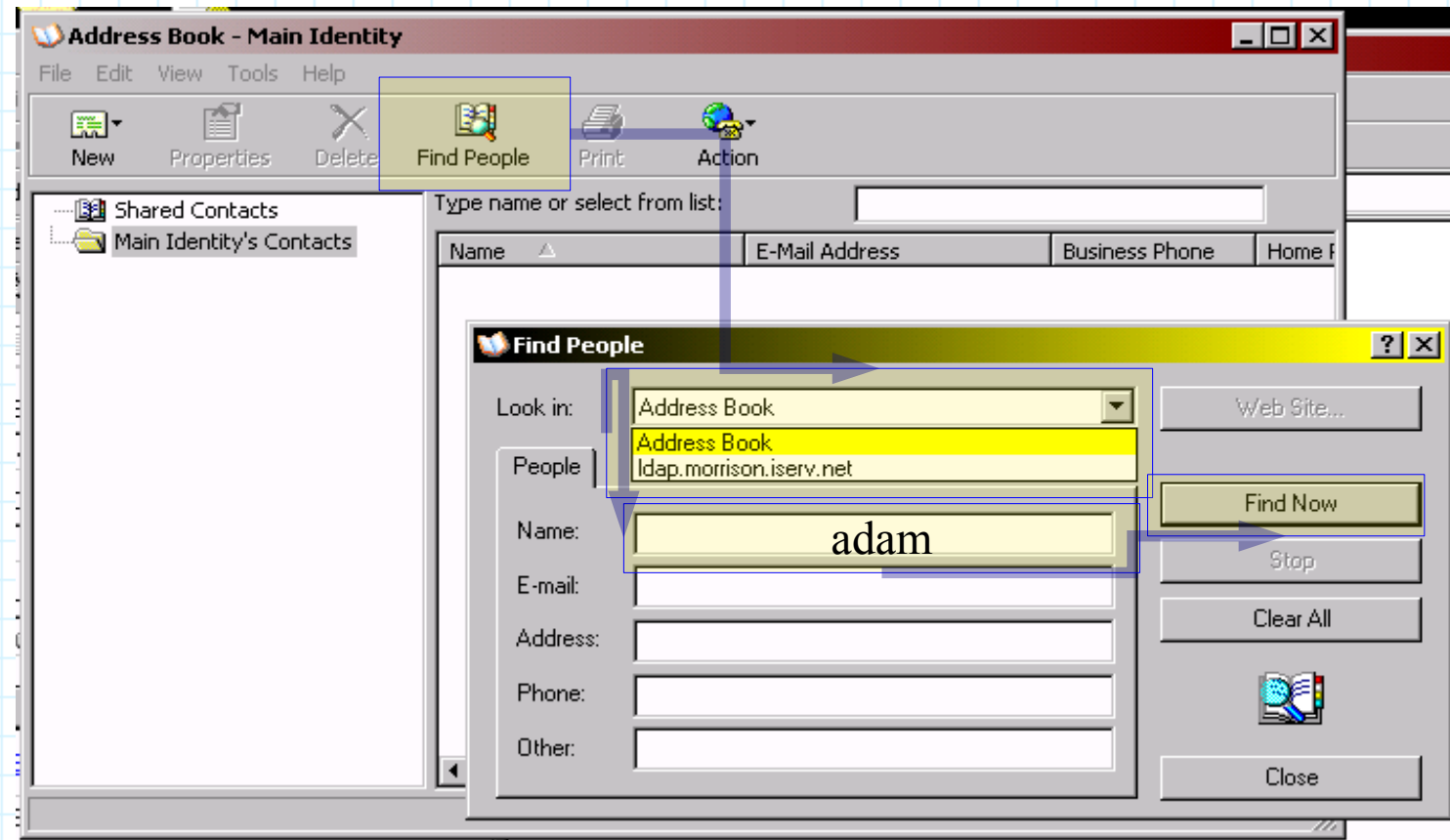
WAB
Simple Search

Find People - (1 entries found)

Look in: ldap.morrison.iserv.net

People | Advanced

Name: adam

E-mail:

Web Site...

Find Now

Stop

Clear All

Close

Properties

Delete

Add to Address Book

Name	E-Mail Address	E
Adam Williams	adam@morrison-ind.com	6

➢(& and
   ➢ (mail=*)
   ➢ (| or
      ➢ (mail=rqxwe*)
      ➢ (| or
         ➢ (cn=rqxwe*)
         ➢ (| or
            ➢ (sn=rqxwe*)
            ➢ (givenname=rqxwe*)
            ➢)
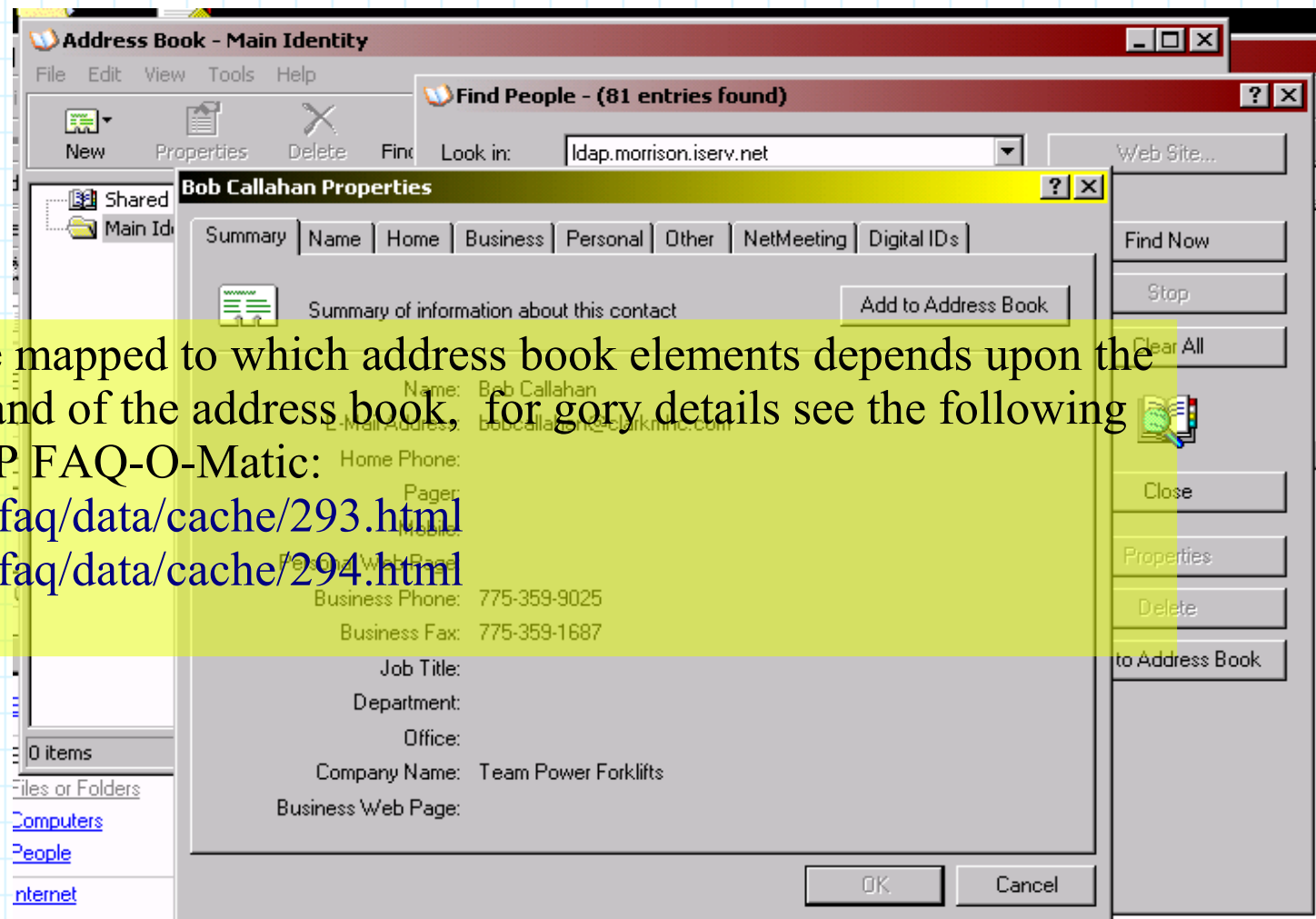   ➢)
   ➢)
➢)

WAB
Advanced Search

WAB
Contact Information

What LDAP attributes are mapped to which address book elements depends upon the version of M$-Windows and of the address book, for gory details see the following sections of the OpenLDAP FAQ-O-Matic:
http://www.openldap.org/faq/data/cache/293.html
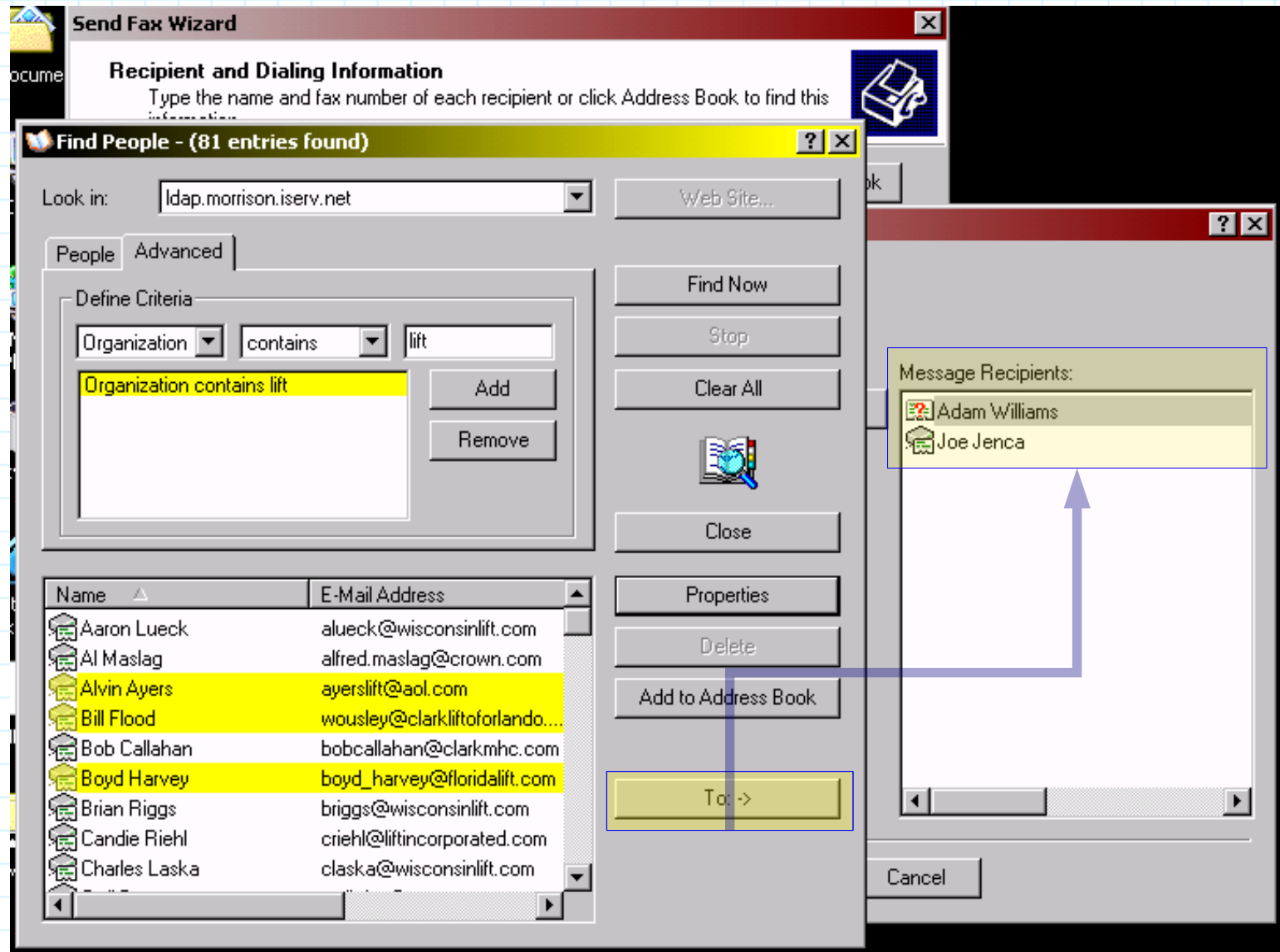http://www.openldap.org/faq/data/cache/294.html

WAB
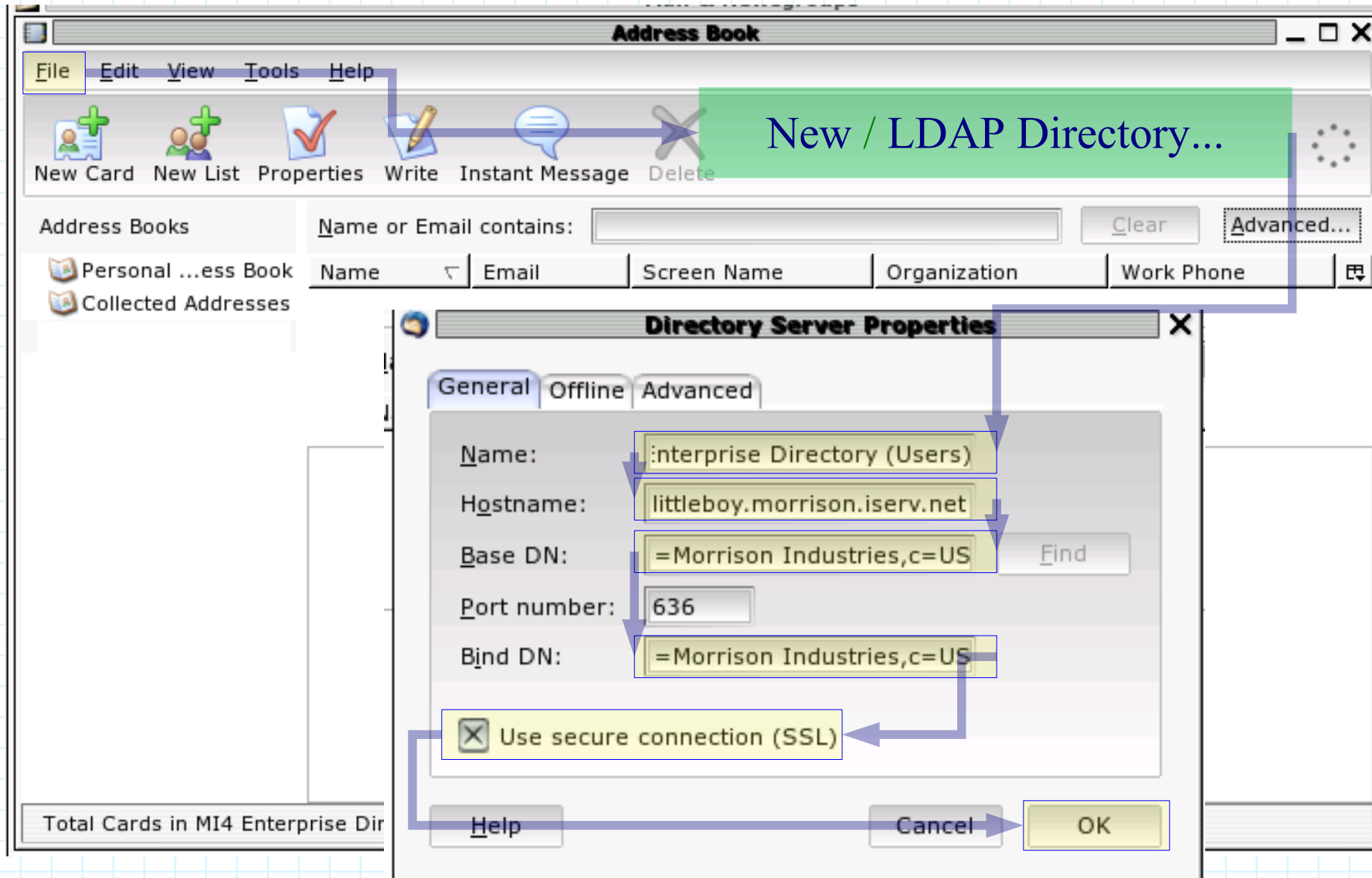## Called from another application

Thunderbird

- Thunderbird inherits its LDAP support (and its limitations) from the Mozilla project
  - Pros
    - Supports SSL
      - But apparently not TLS
    - Offline cache
  - Cons
    - Read only.
    - No support for SASL binds.
    - Limited information presented.
      - Thunderbird's address book is clearly an *e-mail client's address book* rather than a general purpose contact management interface.

Thunderbird

Configuration

New / LDAP Directory...

Address Book

File | Edit | View | Tools | Help

New Card | New List | Properties | Write | Instant Message | Delete

Address Books

Name or Email contains: | Clear | Advanced...

Name | Email | Screen Name | Organization | Work Phone

Personal ...ess Book

Collected Addresses

Directory Server Properties

General | Offline | Advanced

Name: | Enterprise Directory (Users)

Hostname: | littleboy.morrison.iserv.net

Base DN: | =Morrison Industries,c=US | Find

Port number: | 636

Bind DN: | =Morrison Industries,c=US

☒ Use secure connection (SSL)

Total Cards in MI4 Enterprise Dir

Help | Cancel | OK

Thunderbird

Addressbook

Thunderbird

Contact Details`

givenName

sn

cn

[Wrong!]

mail

telephoneNumber

homePhone

facsimileTelephoneNumber

pager

mobile

Edit Card for Adam Williams   ✕

| Contact | Address | Other |

Name

First: | Adam
Last: | Williams
Display: | Adam Williams
Nickname: |

Internet

Email: | Adam@morrison-ind.com
Additional Email: |
Prefers to receive messages formatted as: | Unknown ▼
Screen Name: |

Phones

Work: | 64473822
Home: | 64568931
Fax: | 63611124
Pager: |
Mobile: | 65818010

Cancel   OK

Thunderbird

Contact Details

Edit Card for Adam Williams

Contact | **Address** | **Other**

Home

Address:

City:

State/Province: ZIP/Postal Code:

Country:

Web Page:

Work

Title: _System and Network Administrator_ — title

Department: _IS/IT_ — organizationalUnitName

Organization: _Morrison Industries_ — organizationName

Address:

City: _Grand Rapids_ — l

State/Province: — st   ZIP/Postal Code: _4 605_ — postalCode

Country:

Web Page:
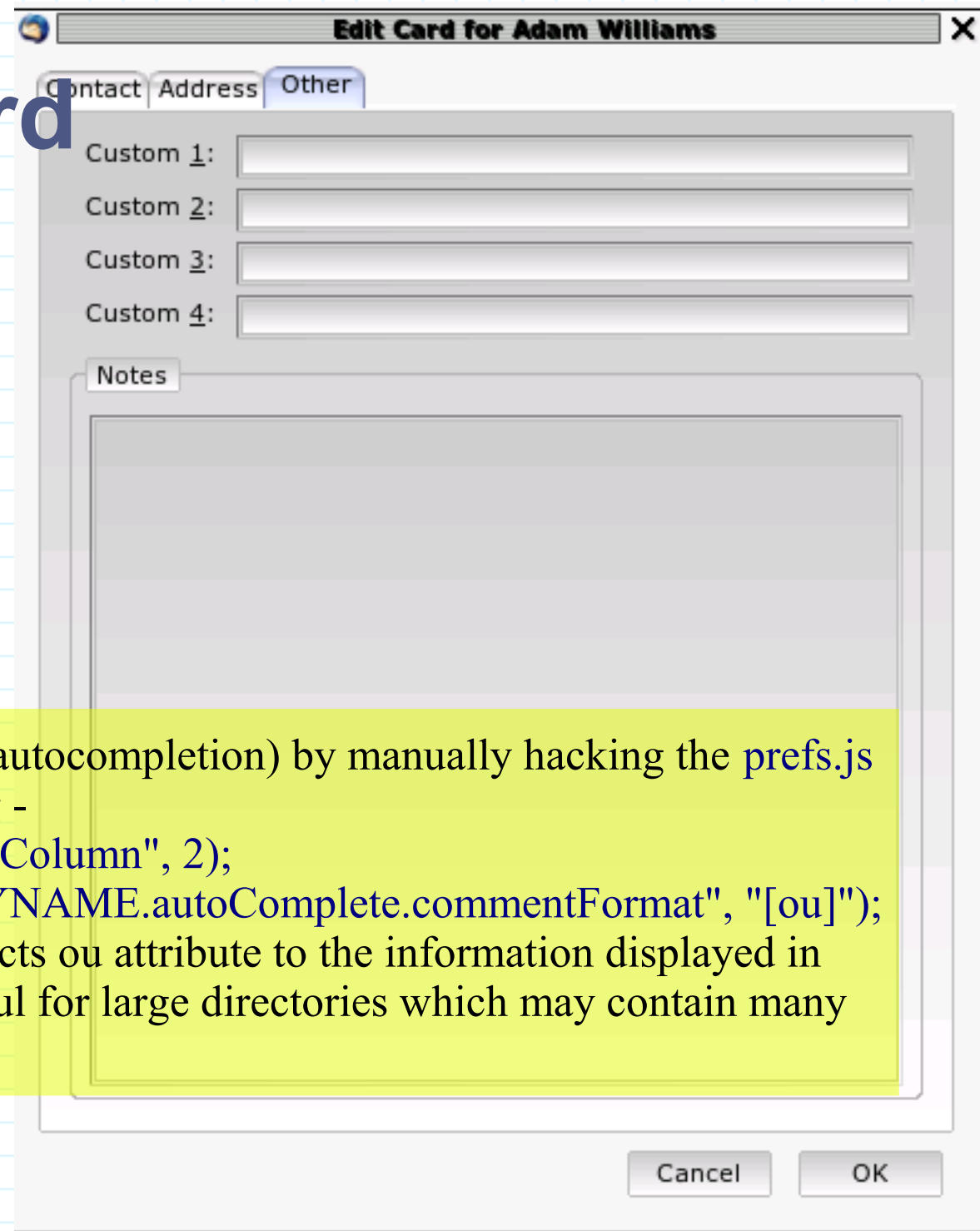
Cancel   OK

Thunderbird

Contact Details

Totally useless.

Contact | Address | Other

Custom 1:

Custom 2:

Custom 3:

Custom 4:

Notes

You can tweak the address 'typedown' (autocompletion) by manually hacking the prefs.js file in your Thunderbird profile; adding -
user_pref("mail.autoComplete.commentColumn", 2);
user_pref("ldap_2.servers.DIRECTORYNAME.autoComplete.commentFormat", "[ou]");
- for instance, adds the value of the objects ou attribute to the information displayed in the typedown pop-up. This is very useful for large directories which may contain many duplicate common names.

Cancel | OK

Thunderbird

Contact Details

Other Clients...

- Administrative Tools
  - LUMA
    - Platform: Python/Qt
    - http://luma.sourceforge.net/
  - lat
    - Platform: C#/GTK#
    - http://people.mmgsecurity.com/~lorenb/lat/
  - GOsa
    - Platform: PHP
    - https://gosa.gonicus.de/
  - Erudite
    - Platform: Python/GTK
    - http://edsadmin.sourceforge.net/
  - Eye Of Newt
    - Platform: Java
    - http://freshmeat.net/projects/eon/