
Vision

# Keeping Your NOS Clean

James La Brash
Practice Manager, Middleware
BTRG Inc.

# What to Take Away

- Network authentication, as a rule, is better than application authentication.
- Connecting apps to the NOS is not ideal – it creates strain and difficulty upgrading.
- ADLDS provides a simple way to "compartmentalize" a directory for use by a specific application, with nice tie-ins to AD.

# Agenda

- What to Take Away
- Back to Basics: Authentication in Enterprise Apps
- LDAP Directory Integration in PS
- Challenges of the Status Quo
- What is ADLDS?
- Emerging Architectures Leveraging ADLDS
- PS and Directories
- When to Use ADLDS User Proxy
- When Not to Use ADLDS User Proxy
- Demo
- What to Take Away
- Q&A

# Authentication in Enterprise Apps

- Authentication (in a nutshell):
  - Verifying that a user really is who he/she claims to be.
- Application authentication
- Single Sign-On
- Reduced Sign-On

# Authentication in Enterprise Apps

- Application Authentication
  - DB / dedicated directory
  - Pros: no reliance on outside infrastructure
  - Cons: security, password-per-app, password resets, password complexity standards

# Authentication in Enterprise Apps

- Single Sign-On
  - Trusts that an authentication challenge has already happened (successfully).
  - User passes seamlessly into target application
  - Two flavors:
    - Subordinated to the network.
      - Requires target application and application/web server to play ball.
    - Form fillers
      - Requires desktop client

# Authentication in Enterprise Apps

- Reduced Sign-On
  - User must re-enter network password
  - Authenticates directly against the network
  - Requires application support

# Authentication in Enterprise Apps

- Subordinating authentication to the network is always a better idea than letting apps handle it.

- Single Sign-On passes user straight through.
- Reduced Sign-On requires re-entry of the network password.
  - *Is Reduced Sign-On ever a better choice than SSO?* Yes! When the application contains sensitive data.

# LDAP Directory Integration in PS

- Authentication
- Profile import
- Profile export and provisioning (with PS Directory Interface or other user provisioning tool)

# Challenges of the Status Quo

- Schema imports slow your directory down
- A highly customized / extended directory is hard to upgrade.
- Some applications will not support authentication against different directories / domains / forests

# What is ADLDS?

- Active Directory Lightweight Directory Services (formerly ADAM – AD Application Mode)
- From Microsoft:

ADAM provides data storage and retrieval for directory-enabled applications, without the dependencies that are required for the Active Directory® directory service. ADAM provides much of the same functionality as Active Directory, but it does not require the deployment of domains or domain controllers. You can run multiple instances of ADAM concurrently on a single computer, with an independently managed schema for each ADAM instance.

# What is ADLDS?

- ADLDS is an LDAP v3-compliant directory service, available free from Microsoft.
- It comes with some good tools to integrate with AD proper:
  - Schema Analyzer
  - AD User Synchronizer
  - User Proxy support
- Many directory instances can be run from a single server.
- It’s FREE!

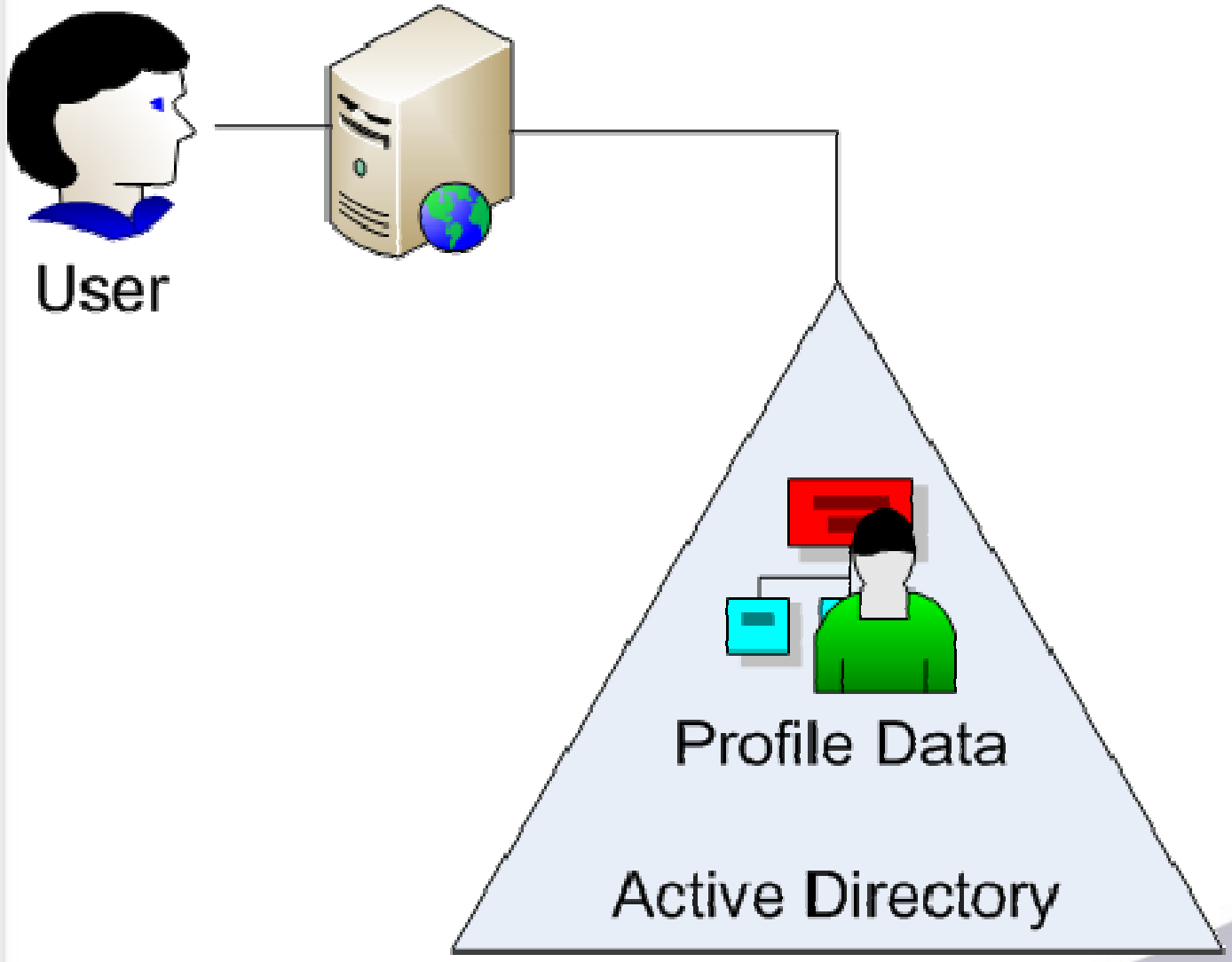
# Emerging Architectures Leveraging ADLDS

- Don’t use the NOS for anything but its main purposes:
  - User authentication
  - Basic user profile storage
  - Catalog of users and computers
  - Enterprise-wide group membership
- Applications should use their own profile/group storage, but authenticate to the network
  - The best of both worlds!

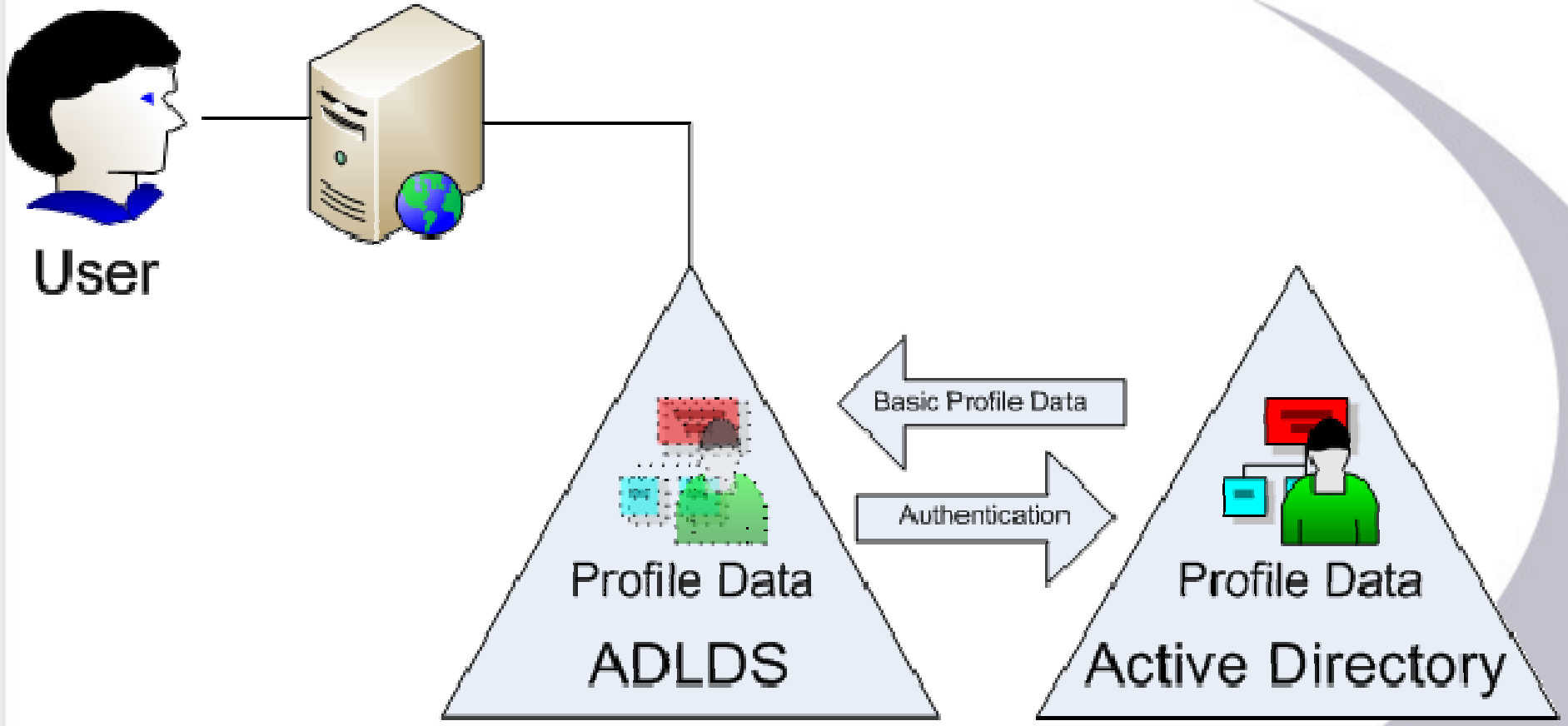
# Emerging Architectures Leveraging ADLDS

- User proxy objects can store profile information, and also point to the "real" AD object for all password activities.

# Emerging Architectures Leveraging ADLDS



# Emerging Architectures Leveraging ADLDS



# PS and Directories (revisited)

- Authentication
  - Use ADLDS with proxy NOS
- Profile import
  - Use ADLDS synched from NOS
- Profile export and provisioning (with PS Directory Interface)
  - Write directly to NOS

# When to Use ADLDS User Proxy

- Schema extensions
- Application-specific groups
- Multiple Active Directories without cross-domain / cross-forest trusts in place… M&A can tend to bring this on.
- Significant profile lookup activity

# When Not to Use ADLDS User Proxy

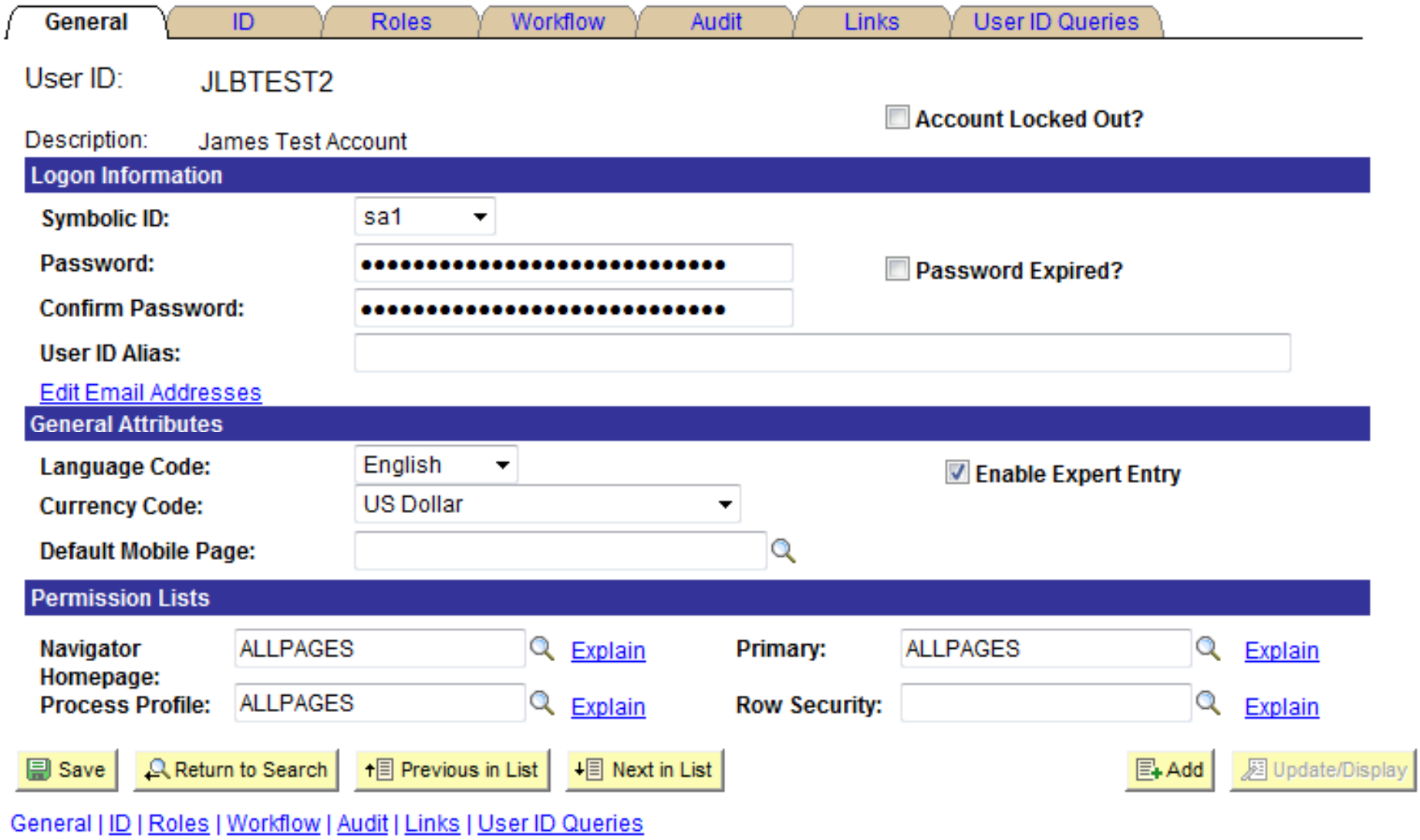
- No schema extensions
- No custom groups
- Single domain

# Demo

- What I've done beforehand:
  - Installed ADLDS: 5 minutes
  - Imported schema: 10 minutes
  - Set up directory in PS: 5 minutes
  - Cached schema into PS: 5 minutes

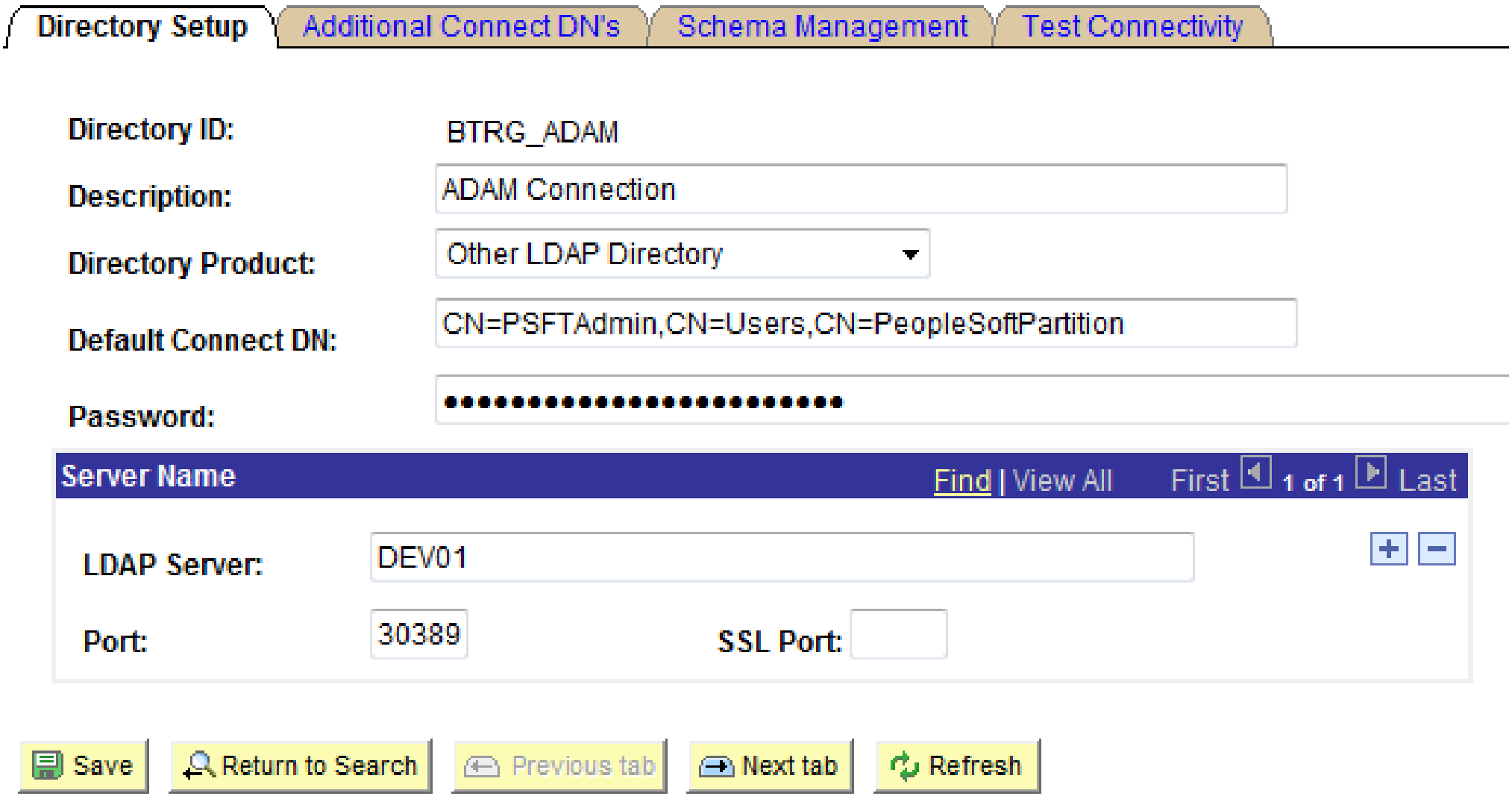
# Demo

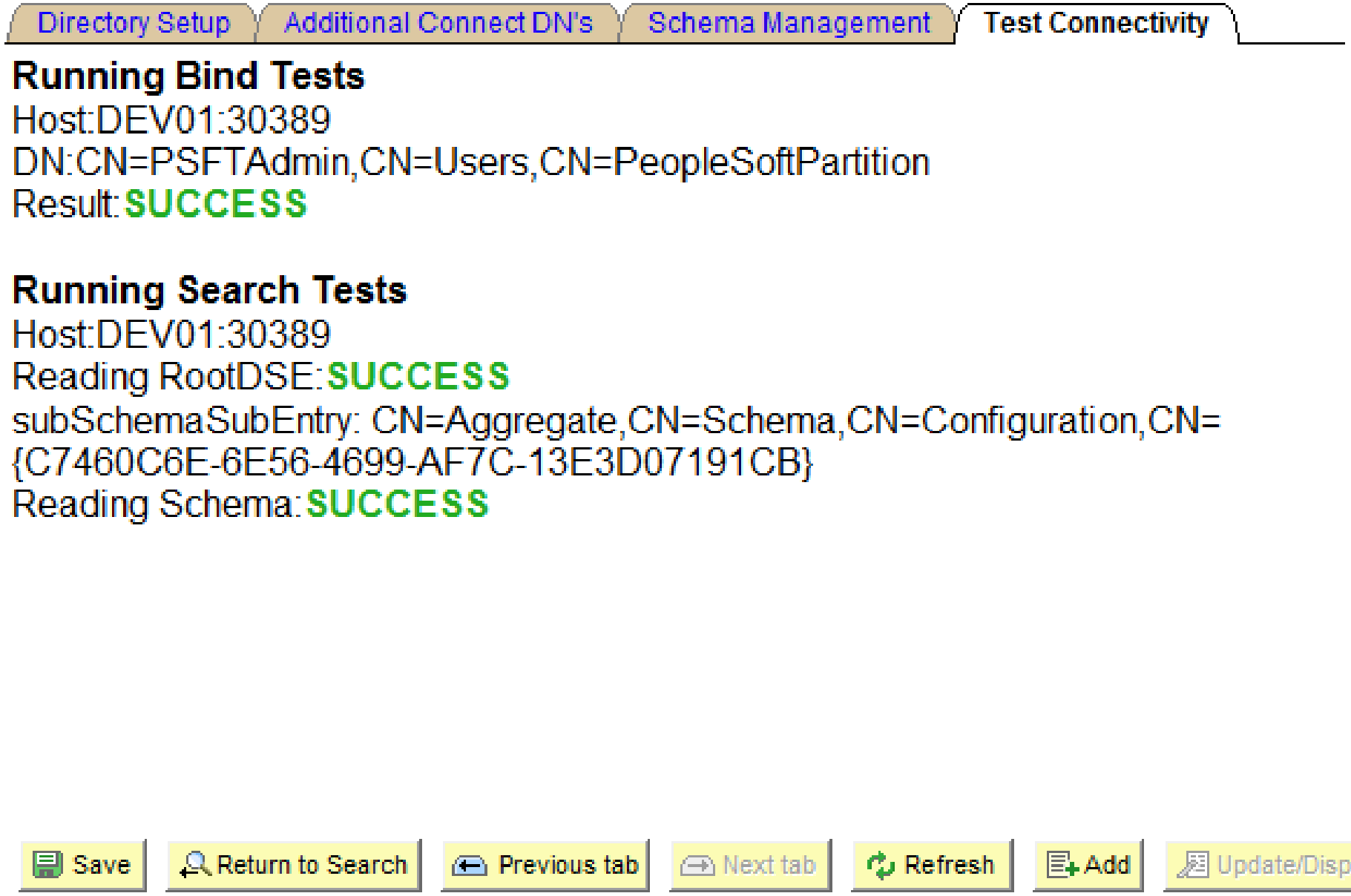
- Now:
  - **Set up a user in PS, log in**
  - Show the directory setup in PS
  - Connect to AD
  - Connect to an ADLDS instance
  - Set up a user proxy object
  - Log into PS with domain credentials


General
ID
Roles
Workflow
Audit
Links
User ID Queries
User ID: JLBTEST2
Account Locked Out?
Description: James Test Account
Logon Information
Symbolic ID: sa1
Password:
Password Expired?
Confirm Password:
User ID Alias:
Edit Email Addresses
General Attributes
Language Code: English
Enable Expert Entry
Currency Code: US Dollar
Default Mobile Page:
Permission Lists
Navigator Homepage: ALLPAGES Explain
Primary: ALLPAGES Explain
Process Profile: ALLPAGES Explain
Row Security: Explain
Save
Return to Search
Previous in List
Next in List
Add
Update/Display
General | ID | Roles | Workflow | Audit | Links | User ID Queries

# Demo

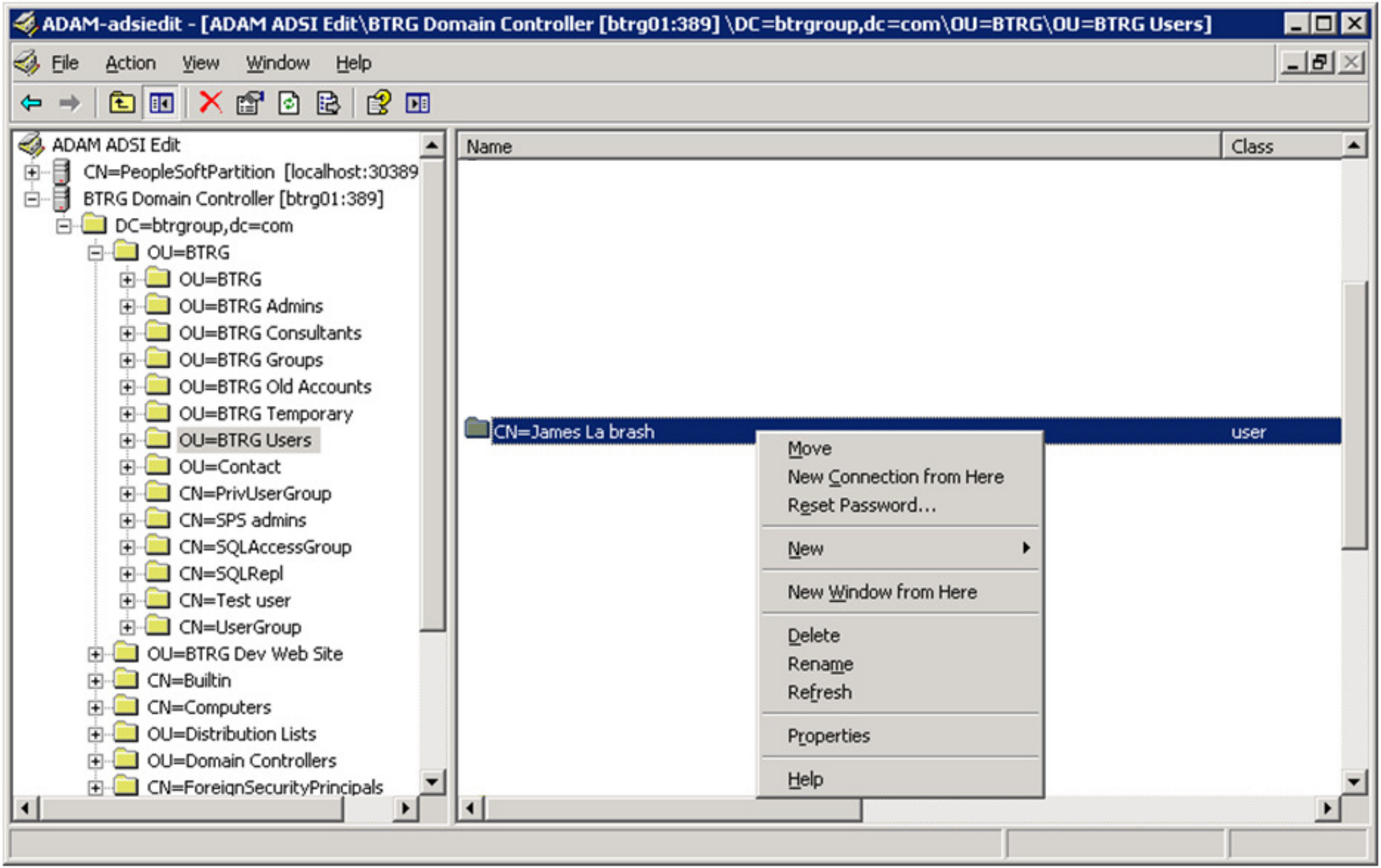
- Now:
  - Set up a user in PS, log in
  - **Show the directory setup in PS**
  - Connect to AD
  - Connect to an ADLDS instance
  - Set up a user proxy object
  - Log into PS with domain credentials

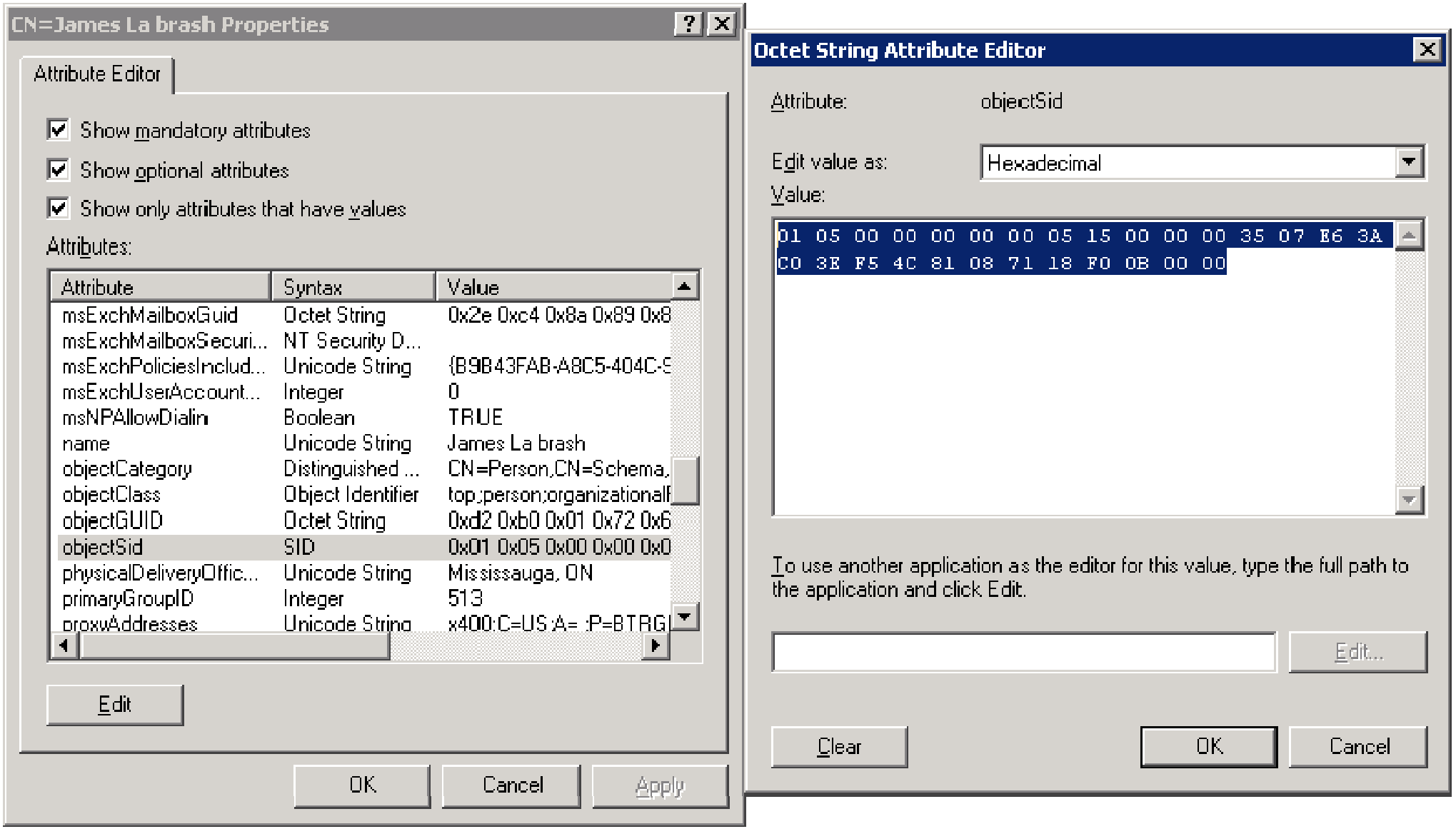

Directory Setup
Additional Connect DN's
Schema Management
Test Connectivity
Directory ID:
BTRG_ADAM
Description:
ADAM Connection
Directory Product:
Other LDAP Directory
Default Connect DN:
CN=PSFTAdmin,CN=Users,CN=PeopleSoftPartition
Password:
Server Name
Find | View All
First 1 of 1 Last
LDAP Server:
DEV01
Port:
30389
SSL Port:
Save
Return to Search
Previous tab
Next tab
Refresh
Directory Setup | Additional Connect DN's | Schema Management | Test Connectivity


Directory Setup
Additional Connect DN's
Schema Management
Test Connectivity
Running Bind Tests
Host:DEV01:30389
DN:CN=PSFTAdmin,CN=Users,CN=PeopleSoftPartition
Result:SUCCESS
Running Search Tests
Host:DEV01:30389
Reading RootDSE:SUCCESS
subSchemaSubEntry: CN=Aggregate,CN=Schema,CN=Configuration,CN=
{C7460C6E-6E56-4699-AF7C-13E3D07191CB}
Reading Schema:SUCCESS
Save
Return to Search
Previous tab
Next tab
Refresh
Add
Update/Display
Directory Setup | Additional Connect DN's | Schema Management | Test Connectivity

# Demo

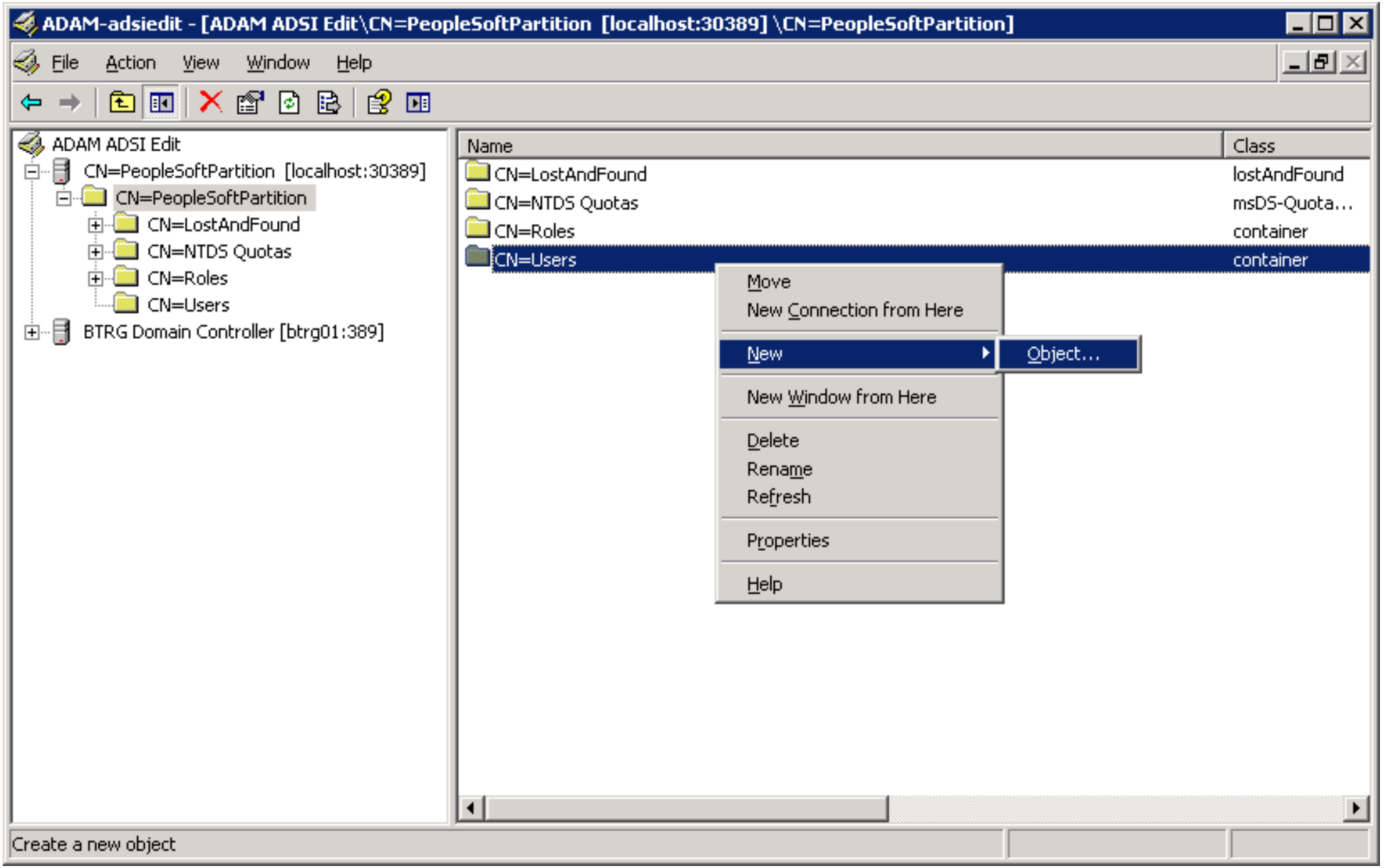
- Now:
  - Set up a user in PS, log in
  - Show the directory setup in PS
  - **Connect to AD**
  - Connect to an ADLDS instance
  - Set up a user proxy object
  - Log into PS with domain credentials

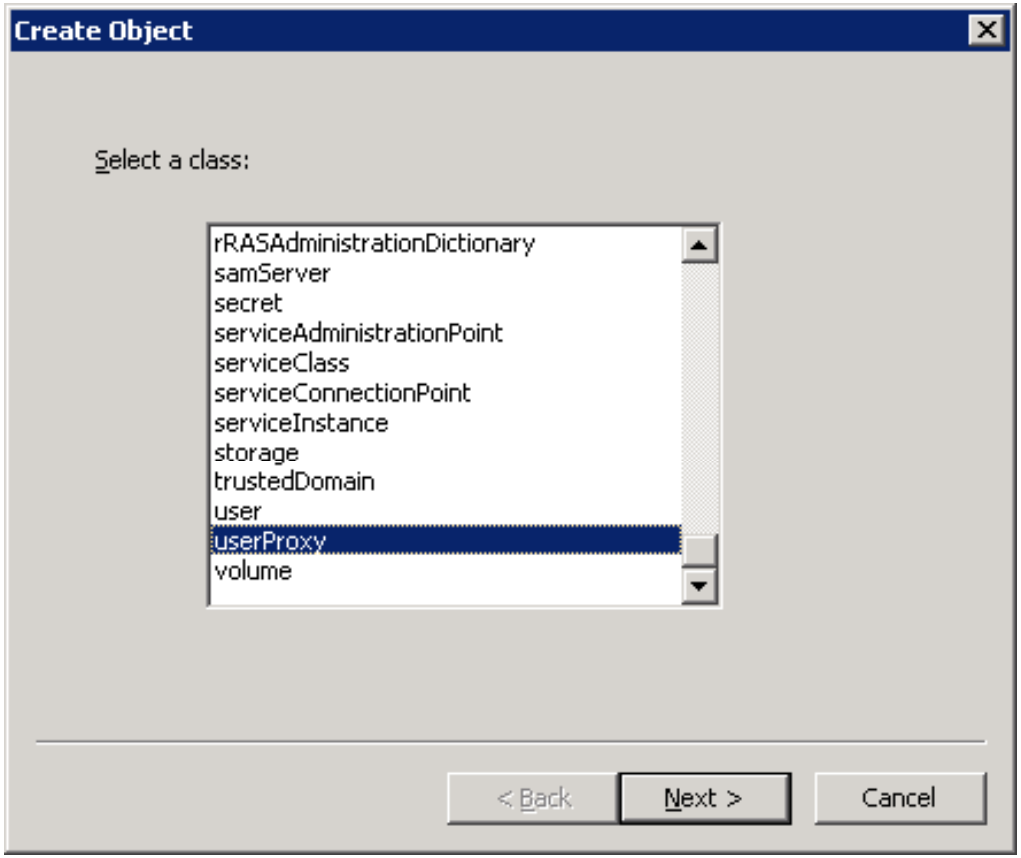

ADAM-adsiedit - [ADAM ADSI Edit\BTRG Domain Controller [btrg01:389] \DC=btrgroup,dc=com\OU=BTRG\OU=BTRG Users]
File Action View Window Help
ADAM ADSI Edit
CN=PeopleSoftPartition [localhost:30389
BTRG Domain Controller [btrg01:389]
DC=btrgroup,dc=com
OU=BTRG
OU=BTRG
OU=BTRG Admins
OU=BTRG Consultants
OU=BTRG Groups
OU=BTRG Old Accounts
OU=BTRG Temporary
OU=BTRG Users
OU=Contact
CN=PrivUserGroup
CN=SPS admins
CN=SQLAccessGroup
CN=SQLRepl
CN=Test user
CN=UserGroup
OU=BTRG Dev Web Site
CN=Builtin
CN=Computers
OU=Distribution Lists
OU=Domain Controllers
CN=ForeignSecurityPrincipals
Name
Class
CN=James La brash
user
Move
New Connection from Here
Reset Password...
New
New Window from Here
Delete
Rename
Refresh
Properties
Help

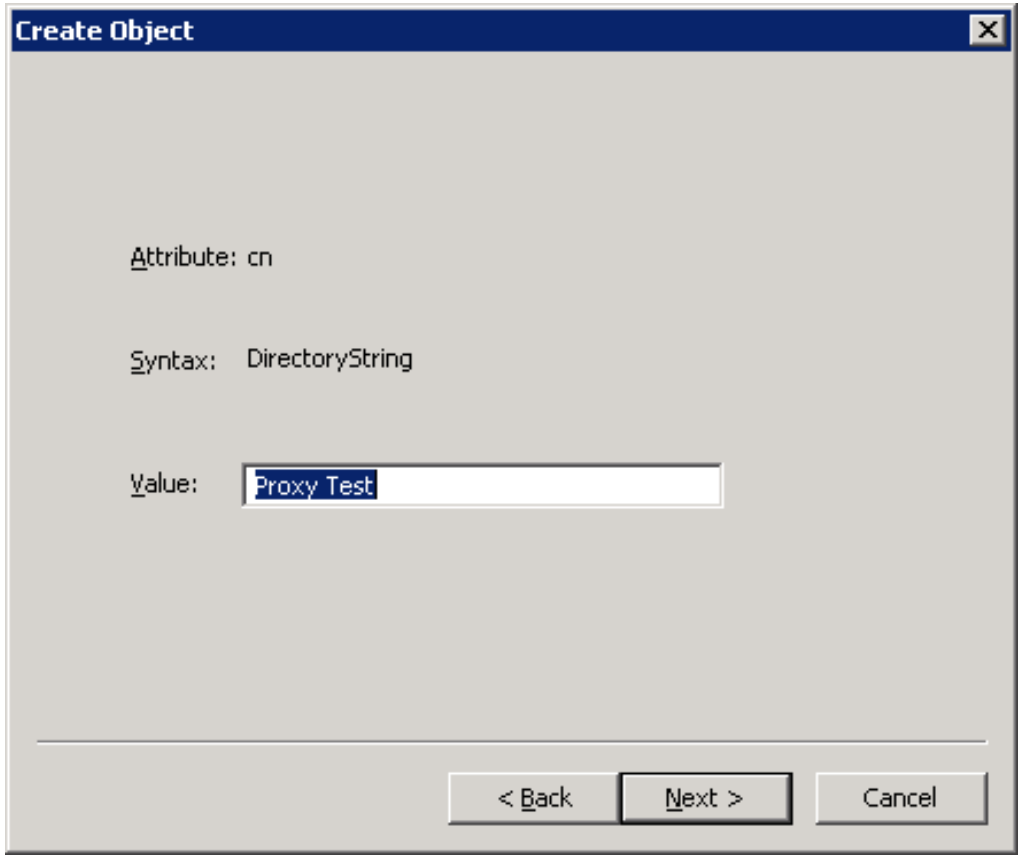

CN=James La brash Properties
Attribute Editor
Show mandatory attributes
Show optional attributes
Show only attributes that have values
Attributes:
Attribute
Syntax
Value
msExchMailboxGuid
Octet String
0x2e 0xc4 0x8a 0x89 0x8
msExchMailboxSecuri...
NT Security D...
msExchPoliciesInclud...
Unicode String
{B9B43FAB-A8C5-404C-9
msExchUserAccount...
Integer
0
msNPAllowDialin
Boolean
TRUE
name
Unicode String
James La brash
objectCategory
Distinguished ...
CN=Person,CN=Schema,
objectClass
Object Identifier
top;person;organizationalP
objectGUID
Octet String
0xd2 0xb0 0x01 0x72 0x6
objectSid
SID
0x01 0x05 0x00 0x00 0x0
physicalDeliveryOffic...
Unicode String
Mississauga, ON
primaryGroupID
Integer
513
proxyAddresses
Unicode String
x400:C=US;A= ;P=BTRG
Edit
OK
Cancel
Apply
Octet String Attribute Editor
Attribute:
objectSid
Edit value as:
Hexadecimal
Value:
01 05 00 00 00 00 00 05 15 00 00 00 35 07 E6 3A
C0 3E F5 4C 81 08 71 18 F0 0B 00 00
To use another application as the editor for this value, type the full path to the application and click Edit.
Edit...
Clear
OK
Cancel

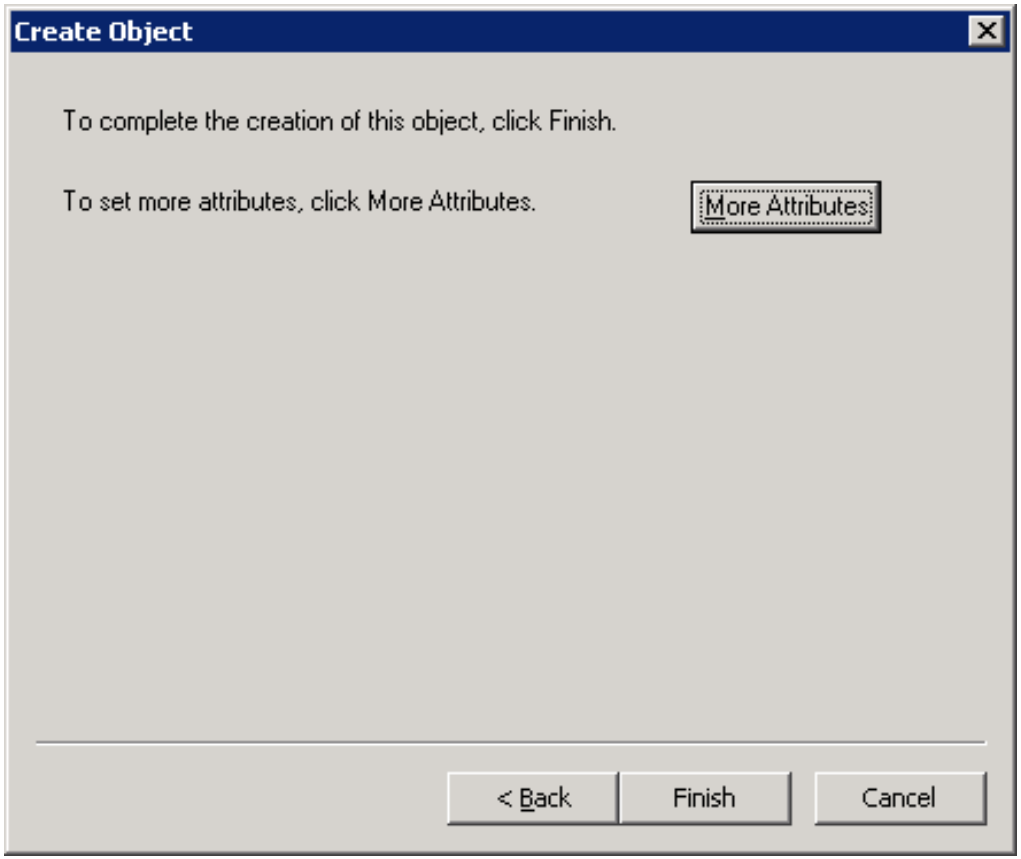
# Demo

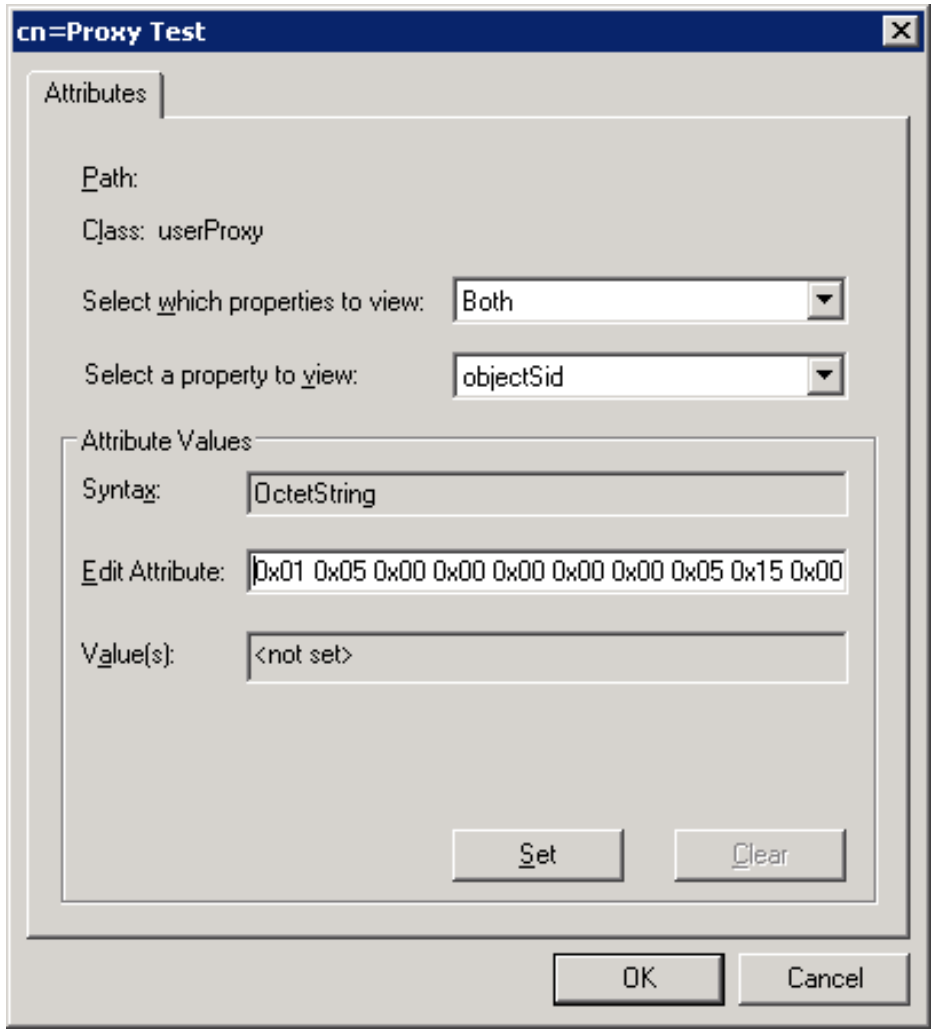
- Now:
  - Set up a user in PS, log in
  - Show the directory setup in PS
  - Connect to AD
  - **Connect to an ADLDS instance**
  - **Set up a user proxy object**
  - Log into PS with domain credentials

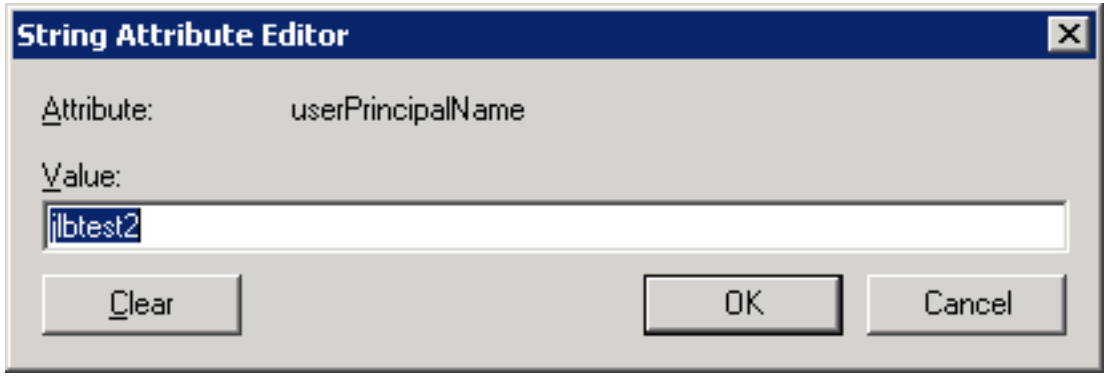

ADAM-adsiedit - [ADAM ADSI Edit\CN=PeopleSoftPartition [localhost:30389] \CN=PeopleSoftPartition]
File Action View Window Help
ADAM ADSI Edit
CN=PeopleSoftPartition [localhost:30389]
CN=PeopleSoftPartition
CN=LostAndFound
CN=NTDS Quotas
CN=Roles
CN=Users
BTRG Domain Controller [btrg01:389]
Name
Class
CN=LostAndFound
lostAndFound
CN=NTDS Quotas
msDS-Quota...
CN=Roles
container
CN=Users
container
Move
New Connection from Here
New
Object...
New Window from Here
Delete
Rename
Refresh
Properties
Help
Create a new object


Create Object
Select a class:
rRASAdministrationDictionary
samServer
secret
serviceAdministrationPoint
serviceClass
serviceConnectionPoint
serviceInstance
storage
trustedDomain
user
userProxy
volume
< Back
Next >
Cancel


Create Object
Attribute: cn
Syntax: DirectoryString
Value: Proxy Test
< Back
Next >
Cancel

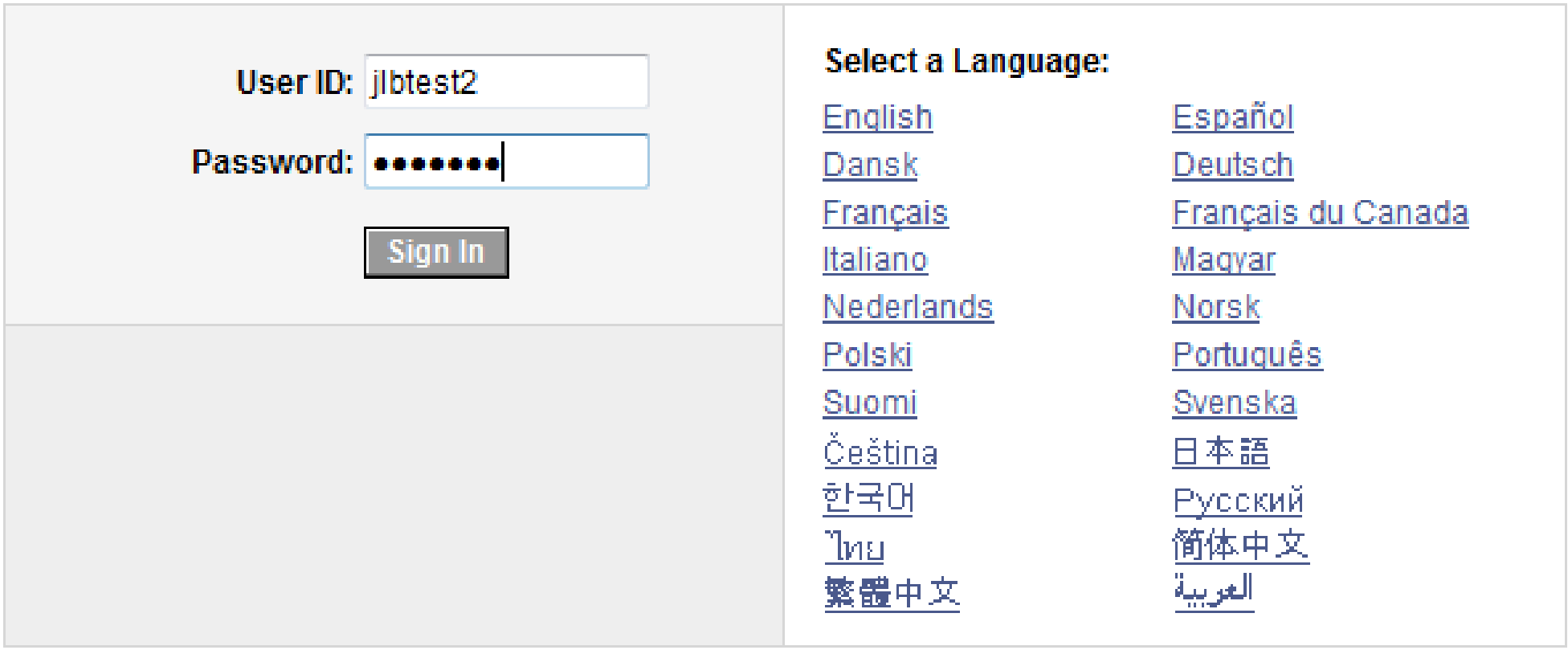

Create Object
To complete the creation of this object, click Finish.
To set more attributes, click More Attributes.
More Attributes
< Back
Finish
Cancel

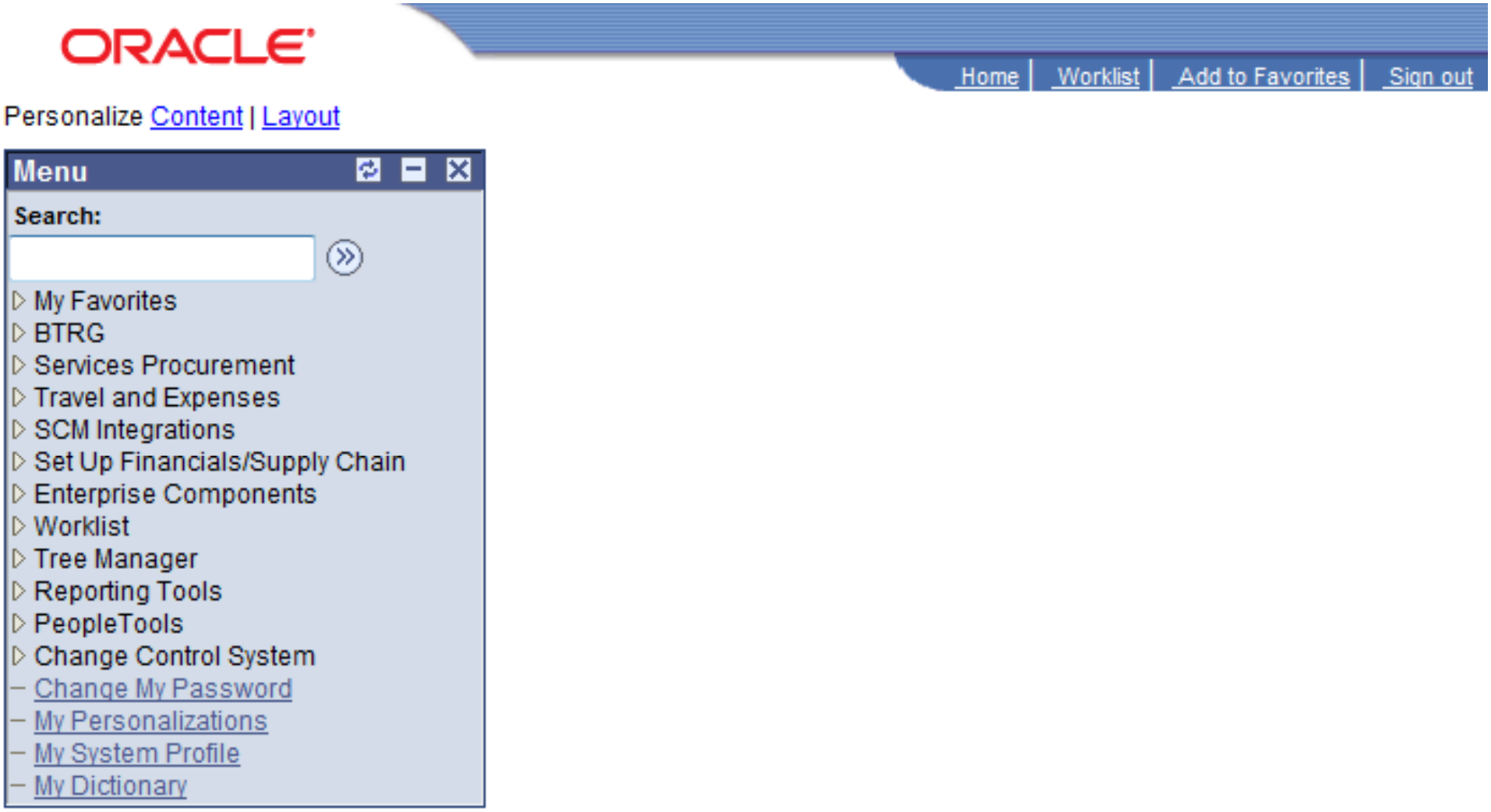

cn=Proxy Test
Attributes
Path:
Class: userProxy
Select which properties to view:
Both
Select a property to view:
objectSid
Attribute Values
Syntax:
OctetString
Edit Attribute:
0x01 0x05 0x00 0x00 0x00 0x00 0x00 0x05 0x15 0x00
Value(s):
<not set>
Set
Clear
OK
Cancel


String Attribute Editor
Attribute:
userPrincipalName
Value:
jlbtest2
Clear
OK
Cancel

# Demo

- Now:
  - Set up a user in PS, log in
  - Show the directory setup in PS
  - Connect to AD
  - Connect to an ADLDS instance
  - Set up a user proxy object
  - **Log into PS with domain credentials**


ORACLE
PEOPLESOFT ENTERPRISE
User ID: jlbtest2
Password:
Sign In
Select a Language:
English
Español
Dansk
Deutsch
Français
Français du Canada
Italiano
Magyar
Nederlands
Norsk
Polski
Português
Suomi
Svenska
Čeština
日本語
한국어
Русский
ไทย
简体中文
繁體中文
العربية


ORACLE
Home
Worklist
Add to Favorites
Sign out
Personalize Content | Layout
Menu
Search:
My Favorites
BTRG
Services Procurement
Travel and Expenses
SCM Integrations
Set Up Financials/Supply Chain
Enterprise Components
Worklist
Tree Manager
Reporting Tools
PeopleTools
Change Control System
Change My Password
My Personalizations
My System Profile
My Dictionary

# Demo

- What would happen if I changed the password on the domain account (but didn't touch PeopleSoft or the User Proxy object in ADLDS)? Would my first domain password still work or would my new, changed password work?
  - The new password would work immediately. Remember, PS is subordinating the password check to the User Proxy object in ADLDS, which in turn is referring back to the domain.
  - The password is always getting verified ***by the NOS*** against what is in the domain at the time of the check.

# What to Take Away

- Network authentication, as a rule, is better than application authentication.
- Connecting apps to the NOS is not ideal – it creates strain and difficulty upgrading.
- ADLDS provides a simple way to "compartmentalize" a directory for use by a specific application, with nice tie-ins to AD.

# Questions

- Do you have any questions about the presentation or any points you'd like me to explain or elaborate on? Feel free to contact me at: jlabrash@btrgroup.com
- It would help me a lot to find out which concepts made sense to you and which are still hazy.  Don't be shy!