Access Management – Gluu Server

This tutorial is for IT staff who are experienced in identity management, it requires insight into how the ActiveDirectory and LDAP work, and a working knowledge of Windows.

This tutorial will demonstrate some of the features of AMX, specifically:

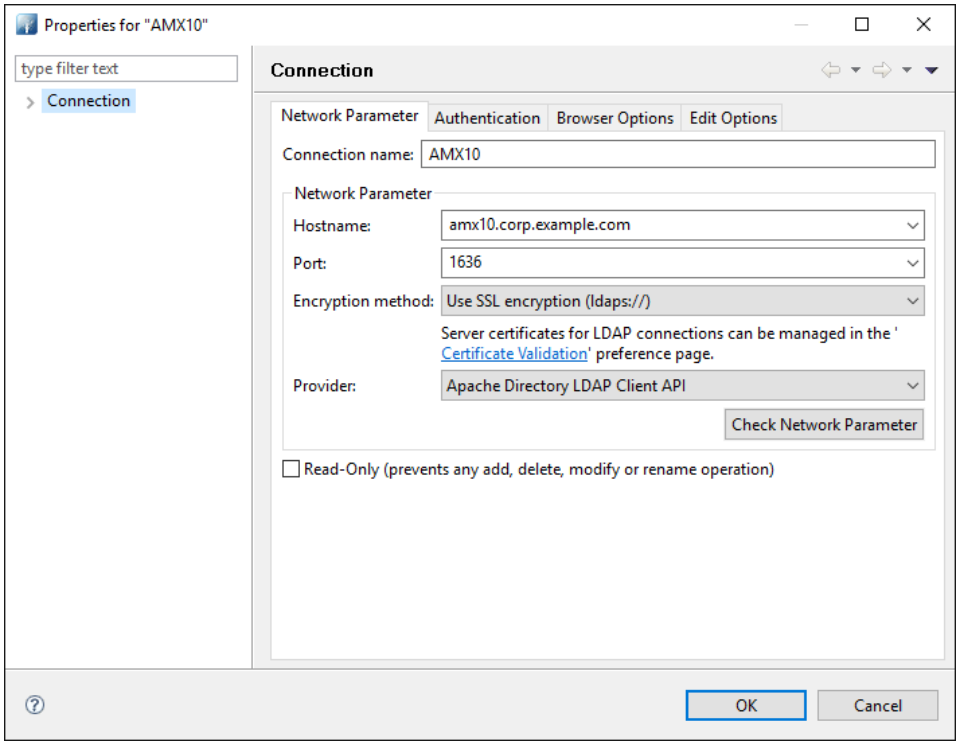
- Connecting to the Gluu OpenDj Ldap server
- Using IdentityReport to Extract accounts from the Ldap server
- Synchronising OpenDj with the Identity Report CSV File
- Synchronising OpenDj with the Active Directory

AMX runs on Windows and must be setup as shown in the AMX Tutorial Setup document.

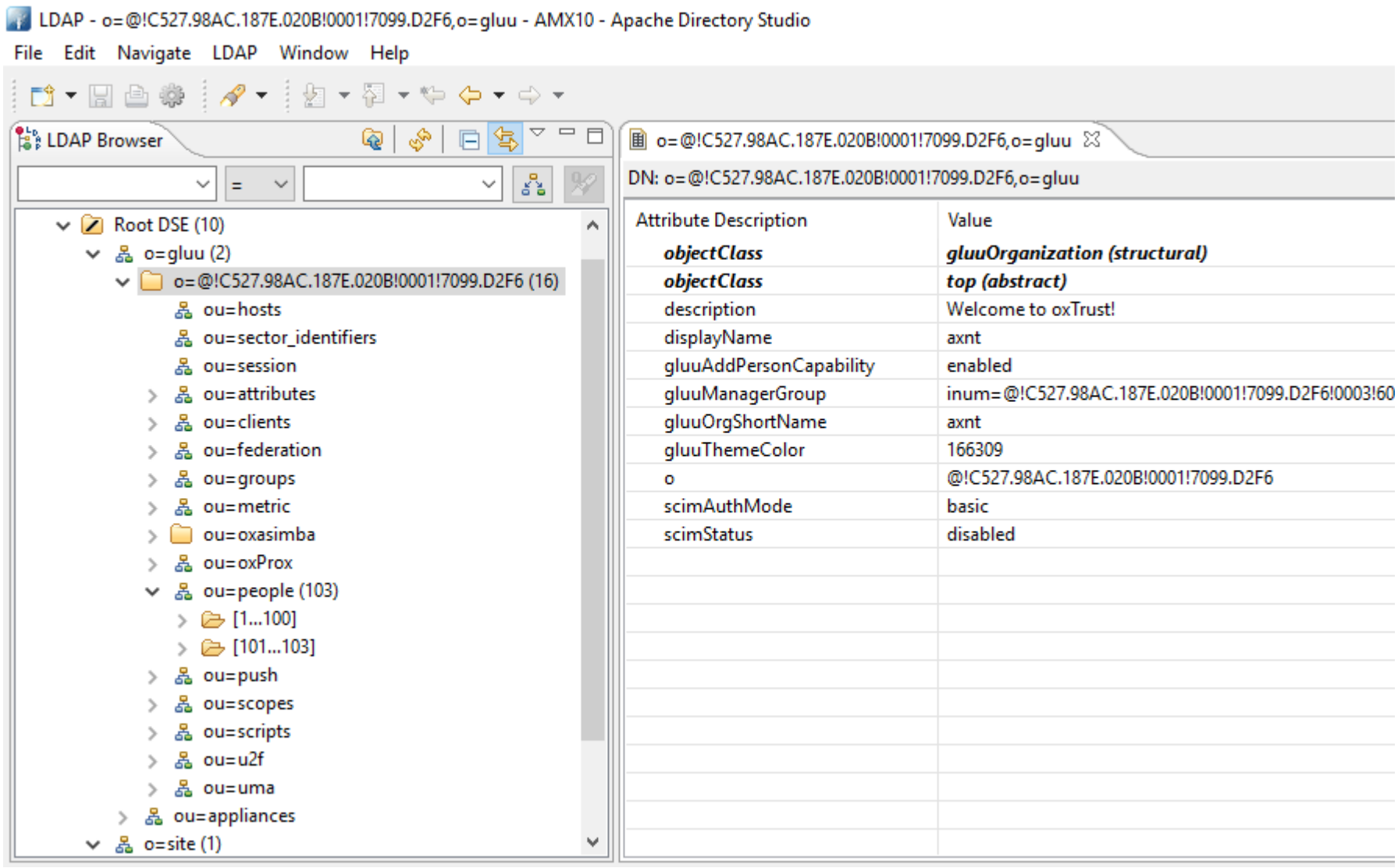
In this tutorial AMX is run from the Command Line, in production it is expected to be run by the Task Scheduler.

1. Connect to Gluu OpenDJ

The OpenDj exposes port 1636 as an Ldaps connection. Using a Ldap directory manager such as Apache Studio setup a connection to the directory



The user name is CN=Directory Manager and the password was set in the ./setup.py script when Gluu was installed. Details can be seen in the Gluu Configuration / Manage Authentication page.



Connect to the Gluu directory and copy the DN of the ou=people organisational unit.

2. identityReport

identityReport will read the Gluu directory and produce a report of accounts and their attributes. identityReport can be run with a non-privileged account.

Update Gluu1 Properties

Edit the Properties file Gluu1.properties, it is in the <installDirectory>\Tutorial1 directory. identityReport properties are consistent with identitySync and the same properties file is used for both applications.

The parameters that need to be updated are:

```
LdapResource1 = ldaps://amx10.corp.example.com:1636
LdapAccountContainer1 = ou=people,o=@!C527.98AC.187E.020B!0001!7099.D2F6,o=gluu
```

- LdapResource1 is the resolvable DNS name of the target Gluu server.
- LdapAccountContainer1 is the ou identified in the ldap browser in the previous step.

Update the ldap password

Create a GluuPasswd.txt file, add the password to the first line, it will be encrypted the first time that identityReport runs.

Run identityReport

Open a Command prompt and cd to the AMX Tutorial1 directory

```
C:\AMX\Tutorial1>..\identityReport.exe  Gluu1.properties
Begins Fri, 01 Jul 2016 16:06:35 GMT  identityReport
Total of 0 Identities

LDAP1 Gluu
Extracted 103 Accounts
LDAP Finished Fri, 01 Jul 2016 16:06:35 GMT
Finished Fri, 01 Jul 2016 16:06:35 GMT

C:\AMX\Tutorial1>
```

Check that the expected number of accounts were returned. In situations where the number of accounts is incorrect, open the debug file and check for errors.

After a successful run this will create identityReportGluu1.csv, open it and check the data. Notice that the first line is:

```
displayName,firstName,lastName,accountName,mail,status,distinguishedName
```

```
Default Admin User,Admin,User,admin,,active,
inum=@!C527.98AC.187E.020B!0001!7099.D2F6!0000!A8F2.DE1E.D7FB,ou=people,o=@!C527.98AC.187E.020B!0001!7099
.D2F6,o=gluu
```

This account should not be managed, it does not exist in any identity source. Edit Gluu1 and Gluu2 properties and add a filter to remove it

```
LdapFilterAttribute1 = displayName
LdapFilterValue1 = !Default Admin User
```

The filter is fully described in the reference manual, this will use the displayName to filter all records and filter out any one that has the value Default Admin User. You may need to filter out other records, in which case use the ActionFileDelimList string to delimit them. The default is ":".

```
LdapFilterValue1 = !Default Admin User:Other Admin User
```

Run identityReport again and check that the Admin user has been filtered out of the IdentityReportGluu1.csv report.

Errors

Error: LDAP Extract Create Connection The LDAP server is unavailable. For <host>:<port>

This can be caused by many issues, such as unresolvable hostname, firewalls, incorrect port etc. Troubleshoot using an LDAP client such as Apache LDAP Studio http://directory.apache.org/studio/ this will give better diagnostics concerning certificates and protocols.

Try using ldap:// on port 389 for attribute LdapServer1. This is not always available, but if this works:

- The server's certificate may not be trusted by the system running identitySync. Try running with the ldap property CertificateTrust = Yes. If this resolves the problem it is a certificate issue, try:
  - Export the certificate from Apache Directory Studio and install the certificate in the Trusted Root CA store.
  - Hostname must match the certificate and be resolvable with dns. Use nslookup to check.

Error: LDAP Extract. The object does not exist. For <adapterInstance>

Can be caused by a bad AccountContainer property value referring to a non-existent container.

Error: LDAP Extract. The server does not support the control. The control is critical. For <adapterInstance>

The AdapterInsatance does not support PagedRead. Set the PageSize property to 0.

3. IdentitySync with the IdentityReport CSV File

Syncronising the identity report extracted before will show no changes

```
C:\AMX\Tutorial1>..\identitySync.exe Gluu2.properties
Warning: Not run as administrator
Begins Tue, 19 Jul 2016 11:18:07 GMT  analyze
CSVIdentity1 C:\AMX\Tutorial1\IdentityReportGluu1.csv
Last updated 19/07/2016 11:18:01
Extracted 102 Identities
CSVIdentity Finished Tue, 19 Jul 2016 11:18:07 GMT
```

```
Total of 102 Identities

LDAP1 Gluu

Extracted 102 Accounts
Account joins    102
Account creates  0
Account updates  0
Account disables 0
Account deletes  0
LDAP Manual Update LDIF do File manual.ldf
LDAP Finished Tue, 19 Jul 2016 11:18:07 GMT
Finished Tue, 19 Jul 2016 11:18:07 GMT

C:\AMX\Tutorial1>
```

Update the Identity Report

Add some extra records and change some existing ones in the IdentityReport1.csv. For example add a new record:

```
,Y,Ailsa Sutherland,Ailsa,Sutherland,,
```

Run identitySync

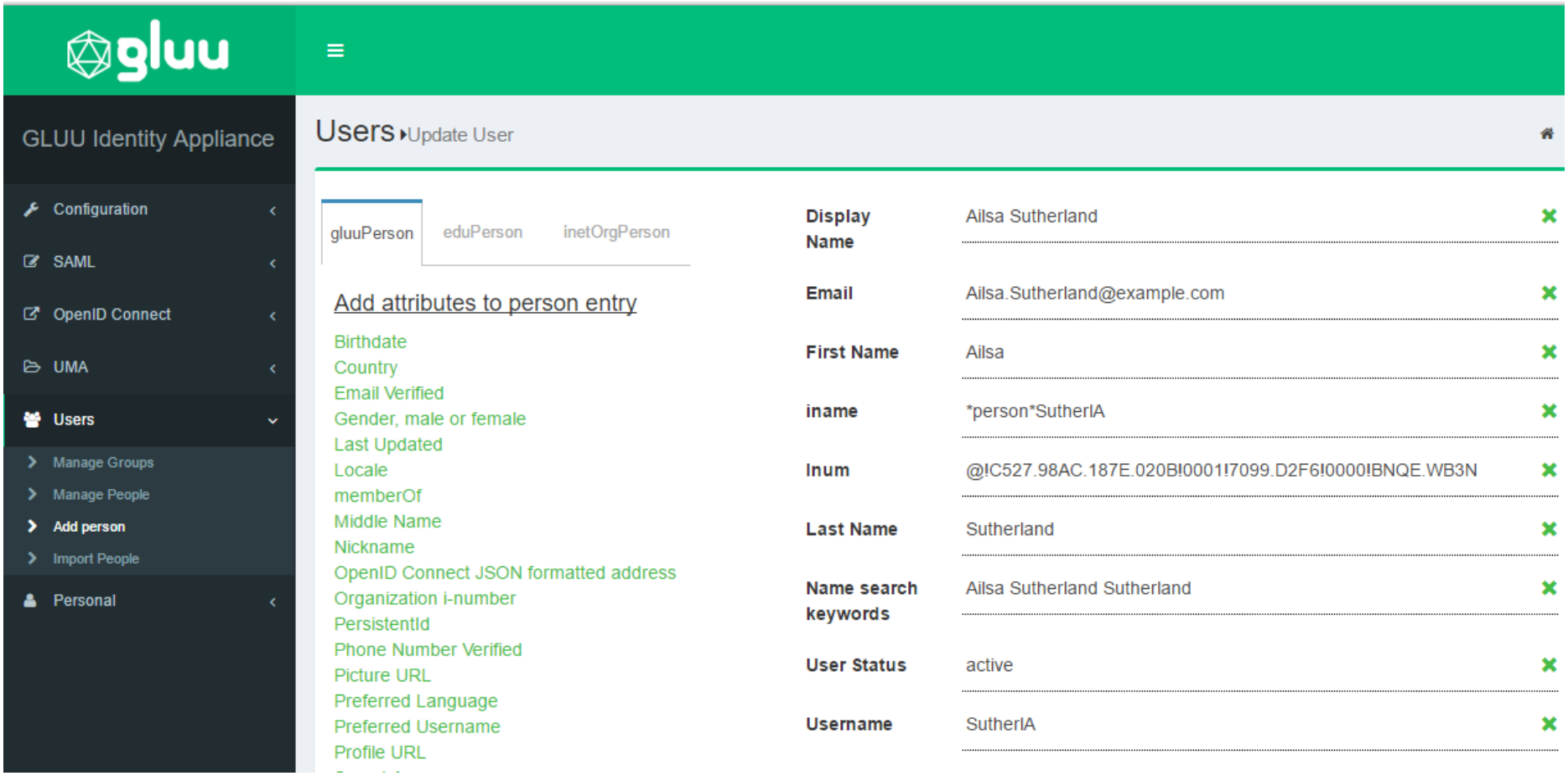
Run identitySync again and the transaction file ActionFile.txt will contain the changes. To make the changes to the LDAP directory run identitySync in the do mode. To undo the changes run it again in undo mode.

```
C:\AMX\Tutorial1>..\identitySync.exe Gluu2.properties do
Warning: Not run as administrator
Begins Tue, 19 Jul 2016 11:29:41 GMT  do
CSVIdentity 1 C:\AMX\Tutorial1\IdentityReportGluu1.csv
Last updated 19/07/2016 11:28:04
Extracted 103 Identities
CSVIdentityFinished Tue, 19 Jul 2016 11:29:41 GMT
Total of 103 Identities

LDAP1 Gluu

Extracted 102 Accounts
Account joins    102
```

```
Account creates  1
Account updates  0
Account disables 0
Account deletes  0
LDAP Manual Update LDIF do File manual.ldf
LDAP Finished Tue, 19 Jul 2016 11:29:42 GMT

LDAP1 Gluu
Number of Mandatory 1
LDAP Load Gluu Create do
inum=@!C527.98AC.187E.020B!0001!7099.D2F6!0000!GBP3.Z7U7,ou=people,o=@!C527.98AC.187E.020B!0001!7099.D2F6
,o=gluu
Finished Tue, 19 Jul 2016 11:29:42 GMT
```

Check the LDAP Directory Manager, this will need a refresh. Compare the new entry with an adjacent one to check all the attributes are present and correct.

Check the Gluu server, search for Sutherland



Run identitySync in the undo mode. This is the only situation where a resource account is deleted.

4. IdentitySync with the Active Directory

If you have been using Gluu's Cache Refresh facility and the Gluu accounts are well synchronised with the Active Directory, identitySync can be used to check it. It will be run in info mode so that the changes that it intends to make can be seen before actually making them.

Update Gluu2 Properties

Edit the Properties file Gluu2.properties, it is in the <installDirectory>\Tutorial1 directory. identityReport properties are consistent with identitySync and the same properties file is used for both applications.

Comment out the CSV identity file

```
// CSV File of Identities
// Tutorial AM3.3
//CSVIdentityResource1 = IdentityReportGluu1.csv
```

The parameters that need to be copied from Glu1.properties are:

```
LdapResource1 = ldaps://amx10.corp.example.com:1636
LdapAccountContainer1 = ou=people,o=@!C527.98AC.187E.020B!0001!7099.D2F6,o=gluu
LdapDNTemplate1 =
inum=@!C527.98AC.187E.020B!0001!7099.D2F6!0000!%random%.%random%,ou=people,o=@!C527.98AC.187E.020B!0001!7
099.D2F6,o=gluu
LdapObjectClasses1 = gluuPerson,ox-C52798AC187E020B00017099D2F6,top
```

- LdapResource1 is the resolvable DNS name of the target Gluu server.
- LdapAccountContainer1 is the ou identified in the ldap browser in the previous step. The same ou must be added to the DNTemplate
- ldapDNTemplate1, copy the preamble of the inum from an existing record, leaving the last two fields as random. A unique inum will be generated in the transaction file from this template.
- Check a record in the ou= people to see the objectClasses and add them to LdapObjectClasses1.

Update the ActiveDirectoryIdentity resource to suit your environment. Uncomment the ActiveDirectoryIdentityResource. other parameters that need to be updated are:

```
ActiveDirectoryIdentityResource1 = DC.corp.example.com
ActiveDirectoryIdentityAccountContainer1 = ou=accounts,DC=corp,DC=example,DC=com
ActiveDirectoryIdentityName1 = corp
ActiveDirectoryIdentityUser1 = corp\philn
```

The User does not need to be an administrative account, the Active Directory is being read which is a very low level privilege.

Update the Active Directory password

If the computer running identitySync is not in the same domain as the Active Directory, create an ActiveDirectoryPasswd1.txt file, add the password to the first line. It will be encrypted when identitySync first runs.

Run identitySync

The results should be no creates, updates, disables or deletes.

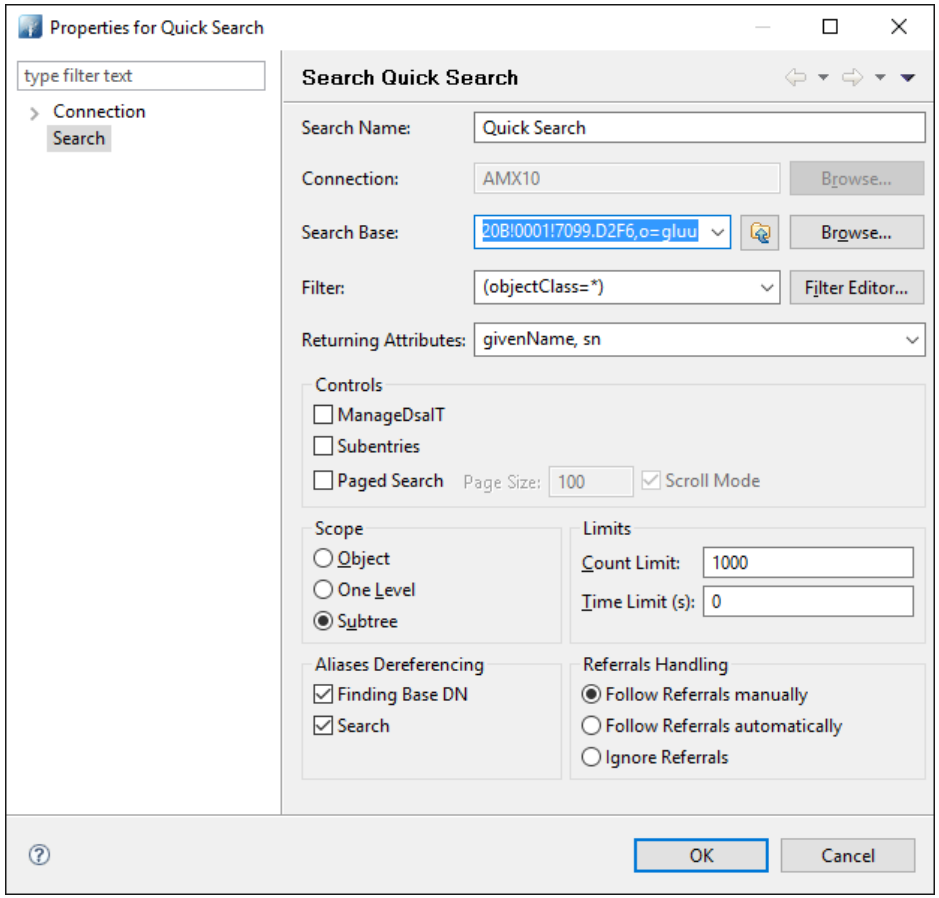
```
C:\AMX\Tutorial1>..\identitySync.exe Gluu2.properties
Warning: Not run as administrator
Begins Fri, 01 Jul 2016 16:16:15 GMT  analyze
ActiveDirectoryIdentity1 DC.corp.example.com
Extracted 103 Identities
ActiveDirectoryIdentity Finished Fri, 01 Jul 2016 16:16:15 GMT
Total of 103 Identities

LDAP1 Gluu

Extracted 102 Accounts
Account joins    102
Account creates  1
Account updates  1
Account disables 1
Account deletes  0
LDAP Finished Fri, 01 Jul 2016 16:16:15 GMT
Finished Sat, Fri, 01 Jul 2016 16:16:15 GMT

C:\AMX\Tutorial1>
```

The result is there is a create, an update and it's a disable. To find the account that is being updated, open the ActionFile.txt file. In this case it contained:

```
01/07/2016|Gluu;inum=@!C527.98AC.187E.020B!0001!7099.D2F6!0000!IVWA.EX4N,ou=people,o=@!C527.98AC.187E.020
B!0001!7099.D2F6,o=gluu|Create|firstName=Ailsa;accountName=SutherlA;lastName=Sutherland;passwdTemplate=Cv
cnCvcn
```

```
01/07/2016|Gluu;inum=@!C527.98AC.187E.020B!0001!7099.D2F6!0000!2414.FA88,ou=people,o=@!C527.98AC.187E.020
B!0001!7099.D2F6,o=gluu|Update|active=Y|active=N
```

The meaning of this is that the directory entry will be updated, the old value is active=Y, the new value is N. Both the old and the new values are written to the transaction log so that the update can be undone if required. The difficulty with the Gluu distinguishedName is it cannot be found in the Gluu GUI. It cannot even be pasted into the search field. Using Apache Directory Studio the entry can be found by pasting the distinguished name into the Search Base.



The alternative is to look in the IdentityReportGluu1.csv created in the first step.

As an example, this is the result of running identitySync in the update mode

```
C:\AMX\Tutorial1>..\identitySync.exe Gluu2.properties do
Warning: Not run as administrator
Begins Fri, 01 Jul 2016 16:17:10 GMT  do
ActiveDirectoryIdentity1 DC.corp.example.com
Extracted 102 Identities
ActiveDirectoryIdentity Finished Fri, 01 Jul 2016 16:17:10 GMT
Total of 102 Identities

LDAP1 Gluu
```

```
Extracted 102 Accounts
Account joins    102
Account creates  0
Account updates  1
Account disables 1
Account deletes  0
LDAP Finished Fri, 01 Jul 2016 16:17:10 GMT

LDAP1 Gluu
LDAP Load Gluu Update do
inum=@!C527.98AC.187E.020B!0001!7099.D2F6!0000!2414.FA88,ou=people,o=@!C527.98AC.187E.020B!0001!7099.D2F6
,o=gluu => active=N
Finished Fri, 01 Jul 2016 16:17:10 GMT

C:\AMX\Tutorial1>..\identitySync.exe Gluu2.properties undo
Warning: Not run as administrator
Begins Fri, 01 Jul 2016 16:17:25 GMT  undo

LDAP1 Gluu
LDAP Load Gluu Update undo
inum=@!C527.98AC.187E.020B!0001!7099.D2F6!0000!2414.FA88,ou=people,o=@!C527.98AC.187E.020B!0001!7099.D2F6
,o=gluu => active=Y
Finished Fri, 01 Jul 2016 16:17:25 GMT

C:\AMX\Tutorial1>
```