EXACT IDENTITY

XID

User Manual

2012.2.320.6 Rev B

Table of Contents

Glossary and terms

Item	Description
IDM|IdM	Identity management (IDM) describes the management of individual identifiers, their authentication, authorization, and privileges/permissions within or across system and enterprise boundaries with the goal of increasing security and productivity while decreasing cost, downtime, and repetitive tasks. *(Reference Wikipedia)*
IAM, IdAM	Identity and Access Management.
IDV or ID Vault (XID primary application)	Identity Vault. Central repository for IDM Identities.
Application (App), Connected System (XID secondary application)	A system that connects to the ID Vault for purposes of Identity Management.
Application (App), Entity or System (XID)	An XID reference for a repository where an extraction file has been configured for analysis.
LDAP	Lightweight Directory Access Protocol. An application protocol for accessing and maintaining distributed directory information services over an Internet Protocol (IP) network. *(Reference Wikipedia)*
LDIF	LDAP Data Interchange Format (LDIF) is a standard plain text data interchange format for representing LDAP directory content and update requests. *(Reference Wikipedia)*
CSV	Comma-separated values (CSV) file stores data in plain-text form and represents columns using a delimiter character.
XML	Extensible Markup Language (XML) is a markup language created to structure, store, and transport data by defining a set of rules for encoding documents in a format that is both human-readable and machine-readable. *(Reference Wikipedia)*
Attribute/Field	Attribute may be used generically to describe either an attribute (e.g. LDAP object) or field (e.g. database). Attribute may be shortened to 'attr'.
Input or Extract file	Data is extracted from a repository for use as an input into XID. Terms Input and Extract can be used interchangeably.

XID

Overview

XID is a Business Intelligence Data Analytics Solution that performs data integration simulation to quantify data readiness challenges at any stage of a project or to analyse integrated data as an audit function.

Out of the box XID provides the following:

- Comparison between different data systems providing a report on account matching and orphaned accounts.
- Attribute level comparison with business rule injection to determine authoritative attribute anomalies.
- Active Directory, LDAP and Unix group analysis for elevated privileged accounts.
- Manager analysis identifying accounts without managers. This is for resolving accounts without managers at an early stage of the project for products dependant on manager population such as SailPoint.
- Rectification script generation that provides a means to bulk update attribute anomalies in systems.
- Summary Report: Graphical report quantifying the anomalies found by the business analytics.
- Detailed Report: Identifies each account and account attribute highlighting the anomaly found.

XID can be part of the Identity Management professional and Data Analyst software toolkit so that early data issue resolution can begin right at the outset of a project.

XID fits in any market where there is a need to have data analysed for one or many systems whereby business rules can be injected into the analysis process for information arbitration.

The value of XID is that it can predict success or failure of integrating data from an Identity Management perspective. Poor data quality can be an obstacle to completing a project on time or at all if issues arise from anomalies with this data.

Rapid repeatable data analysis expedites this process and alleviates the need to employ multiple analysts to perform analysis from the ground up with discrete electronic tools.

Concepts

Project data readiness analysis can begin right at the outset, identifying data anomalies even before installation of the big vendor IDM/IAM solution. While many solutions have their own data analytics tools, often these tools cannot be utilised until the main product is installed which can take time. This time can be put to good use with XID, getting data ready so that the main IDM/IAM solution can get on with the task of managing Identities once installed and not rectifying data issues.

XID is enabler product for Identity Management projects. The product looks holistically at data in different systems and correlates merge points for data items common between systems.

XID is designed to analyze data at a fixed point in time. This is achieved by gathering extracts of data in LDIF, CSV or XML formats and creating a model on the production system.

As data issues (once located) cannot be rectified in real time, there is limited benefit from reading or extracting the data in real time. A reasonably current extract is sufficient in data rectification when applying the concept of data rendering.

Data rendering looks at a snapshot in time and attempts to rectify at least 80% of issues in the first error detection/rectification pass that may take weeks, depending upon the clients' inertia in changing production data.

The 2nd and subsequent renders should work on a smaller error pool until an error level is reached that the project can accept. The remaining errors can be handled as exceptions.

XID also remains abstracted from production systems for the following reasons:

- Difficult to obtain account to access data directly.
- Difficult to obtain authorisation level to extract all relevant data.
- Live data changes during processing can create a variant in the result set.
- Potential performance and/or operational impact to live systems.
- XID processes an agreed data set sanctioned by data owner.

Self-analysis of each application is also possible and an anomaly report is produced for the application.

Basic entitlements can be analysed for each application with a report produced detailing users without managers, elevated group privileges

Match modes

There are two modes for matching:

- Parallel
- Cascade

Parallel mode matches all Apps centric to primary Application (App) 1. Each Application is compared against App1 in its entirety from App1 to App then in the reverse direction App to App1. Any account in the secondary App that cannot be matched to the primary App1 will be logged as an Orphan 'App -> App1'.

Cascade matching will begin from App1 to the next downstream App. Once a match is found XID searches the next selected App.

Any account that cannot be matched from App1 to any other App will be logged as an Orphan 'App1 -> App'

Project

An XID Project is a representation of a physical Data project that encompasses Apps, Matching & Business Rules.

An Application (App) is a reference for a repository where an extraction file has been configured for analysis.

App 1 is the primary entity and can also be referenced as an Identity Vault (IDV) if this exists in the architecture. Other Applications are secondary App.

If there is no designated primary App in the architecture then App 1 should be the App deemed as most authoritative.

App 1 is represented as the central entity in the XID architecture tab.

Matching rules: Matching is performed from the App 1 to each secondary App selected for analysis.

The business rules allow comparison of Apps at an attribute/field level. Attribute(s) may be used as a global reference to attributes and fields.

XID Demo Data

XID is shipped with demonstration data that emulates a sample company. Data represents extracts from the following applications:

- Novell/NetIQ ™ eDirectory ™ [Primary App 1]
- SAP ™ HR
- Oracle ™ Database
- Sun ONE LDAP
- Microsoft ™Active Directory (AD)

XID has been preconfigured so that the 5 applications can be run “out of the box” and produce results right away.

The XID full version has the following limitations:

- Program will expire biannually.
- Registered users will have access to a password that is used to login as admin. Full detailed reports can be generated without limitation if authenticated.
- A user without the admin password can still use XID but the detailed reports are limited.

The XID demonstration version has the following limitations:

- Program will expire quarterly.
- Detailed reports are limited to 10 rows per application. The reports used to be encrypted and decrypted by request.
- Cascade wide report is not available.

Download

The XID full package can be downloaded from the following URL:
http://www.automation.co.nz/download/xid.zip

The file is an encrypted zip archive and the password will be supplied by Exact Identity.

The XID demo package can be downloaded from the following URL:

http://www.automation.co.nz/download/xidemo.zip

XID Files

Extract the zip file to a folder on a Windows computer, for example, C:\XID. The zip program may let you create a directory and it is best to have the files in their own directory. The 'Image', 'input', 'output' and 'output\xrecycle' subdirectories are needed; please do not remove them.

File	Type	Purpose
Application Files		
xid.zip | xidemo.zip	Zip archive	XID archive prod distribution file.
xid.exe	.exe	Main XID prod executable program file.
xid.ico, xid1.ico	Icon file .ico	XID icon files.
xid_setup_proj.xml	XML config	XID configuration file. This file must be located with xid.exe.
XID_Test_Project_1_Ent_1_conf.xml XID_Test_Project_1_Ent_2_conf.xml XID_Test_Project_1_Ent_3_conf.xml XID_Test_Project_1_Ent_4_conf.xml XID_Test_Project_1_Ent_5_conf.xml	XML config	Contains the configuration for each application XID has been configured to analyse. The naming convention is: `<XID Project Name>_<Project Number>_Ent_<Application Number>_conf.xml`
Project Schema Files: XID_Test_Project_1_*_sch.xml ** = Application Name* Schema Templates: IDV_sch.xml JDBC2_sch.xml, JDBC2b_sch.xml LDAP2_sch.xm, LDAP2b_sch.xml SAP2_sch.xml, SAP2b_sch.xml AD2_sch.xml, AD2b_sch.xml	XML config	Each application has a schema file with the following naming convention: `<project name>_<project no>_<application name>_sch.xml` Additional template schema files have been included for the workshop exercise.
XID_Test_Project_1_match.xml	XML config	Contains the matching rules configuration for all applications. Naming convention: `<XID Project Name>_<Project Number>_match.xml`
XID_Test_Project_1_schmap.xml	XML config	Contains the Schema Mapping rules configuration for all applications. Naming convention: `<XID Project Name>_<Project Number>_schmap.xml`
Application Input Files – subdirectory: \input		
xtcoad.csv, xtcoadb.csv xtcoidvault.ldif xtcojdbc.xml, xtcojdbc2.xml xtcoldap.ldif, xtcoldap2.ldif xtcosap.csv, xtcosapb.csv	Input .csv Input ldif Input .xml Input ldif input csv	Active Directory CSV file 1 & 2 ID Vault – eDirectory LDIF file Oracle XML file 1 & 2 LDAP application LDIF file 1 & 2 SAP application CSV file 1 & 2
Application Output Files		
XID_Test_Project_1_syslog.txt	txt file	XID sample project general log. `<Project Name>_syslog.txt`

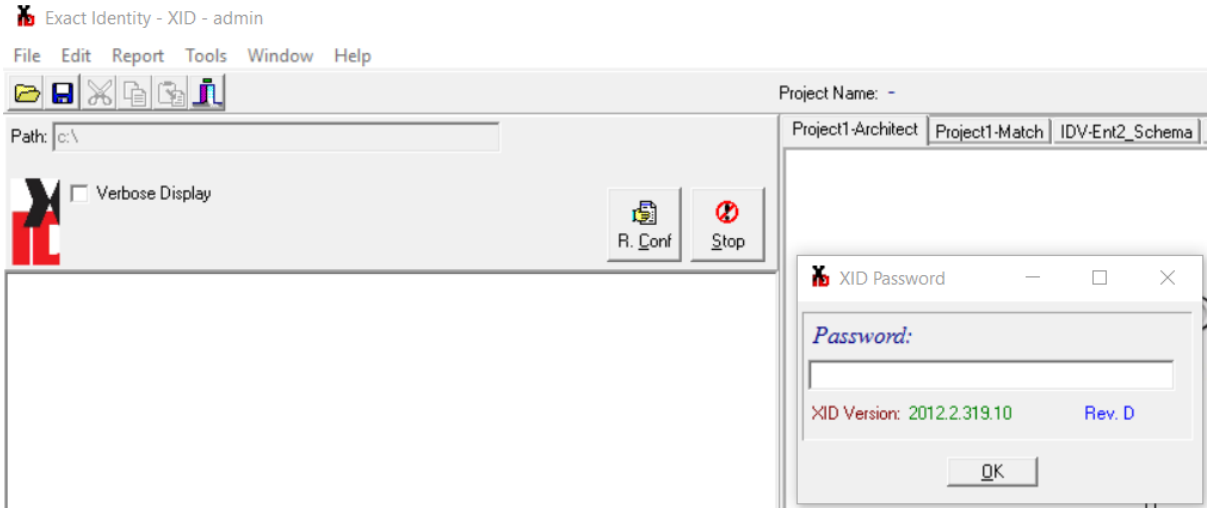
File	Type	Purpose
Application Output Files – subdirectory: \output		
XID_Test_Project_1_reportlogen.csv <Project Name>_reportlogen.csv	Report csv	General information such as successful matching.
XID_Test_Project_1_matchorpans.csv <Project Name>_matchorphans.csv	Report csv	Matching, Orphan and Duplicate Match report.
XID_Test_Project_1_busrulegen.csv <Project Name>_busrulegen.csv	Report csv	Business Rules report.
XID_Test_Project_1_busrulegenwide.csv <Project Name>_busrulegenwide.csv	Report csv	Business Rules Wide report. Cascade mode only.
XID_Test_Project_1_repstats.txt <Project Name>_repstats.csv	Report Txt	Report statistics and encryption key file.
XID_Test_Project_1_Ent*X*_Rect_*ENme*.txt *X* = Application Number - *ENme* = Application Name	text files	Application Rectification Files.
XID_Test_Project_1_Ent*X*_Rect_RollBack_*ENme*.txt *X* = Application Number - *ENme* = Application Name	text files	Application Rectification Rollback Files.
XID_Test_Project_1_Ent*X*_Rect_Control_*ENme*.txt *X* = Application Number - *ENme* = Application Name	text files	Application Rectification SQL Loader compatible control files.
XID_Test_Project_1_Ent*X*_Rect_Control_Rollback_*ENme*.txt *X* = Application Number - *ENme* = Application Name	text files	Application Rectification SQL Loader compatible rollback control files.
zentsysdmp*X*.txt X = application number	text files	The application dump memory files are for troubleshooting purposes and provide an indication of the translation of input file to XID.
zentmemdmp*X*.txt X = application number	text files	The application dump schema memory files are for troubleshooting purposes the same as the system dump files.
Key Generation Files \output directory		
<ReportUID>_reportlogen_crypt.csv	Report csv	General information such as successful matching. Encrypted
<ReportUID>_matchorphans_crypt.csv	Report csv	Matching, Orphan and Duplicate Match report. Encrypted
<ReportUID>_repstats_crypt.csv	Report Txt	Report statistics. Encrypted
<ReportUID>_Ent*X*_Rect_*ENme*_crypt.txt *X* = Application Number - *ENme* = Application Name	text files	Application Rectification Files.
<ReportUID>_Ent*X*_Rect_RollBack_*ENme*_crypt.txt *X* = Application Number - *ENme* = Application Name	text files	Application Rectification Rollback Files.
<ReportUID>_Ent*X*_Rect_Control_*ENme*_crypt.txt *X* = Application Number - *ENme* = Application Name	text files	Application Rectification SQL Loader compatible control files.
<ReportUID>_Ent*X*_Rect_Control_Rollback_*ENme*_crypt.txt *X* = Application Number - *ENme* = Application Name	text files	Application Rectification SQL Loader compatible rollback control files.
The <ReportUID> is comprised of the computer name + login name with an appended unique identifier.		
The encrypted key generation files are moved to the 'xrecycle' folder and replaced by the decrypted '<ReportUID>*_dcypt.*' file for each encrypted file.		
\output\sample_detailed_reports	folder	Decrypted detailed report sample from demo input data.

Run XID

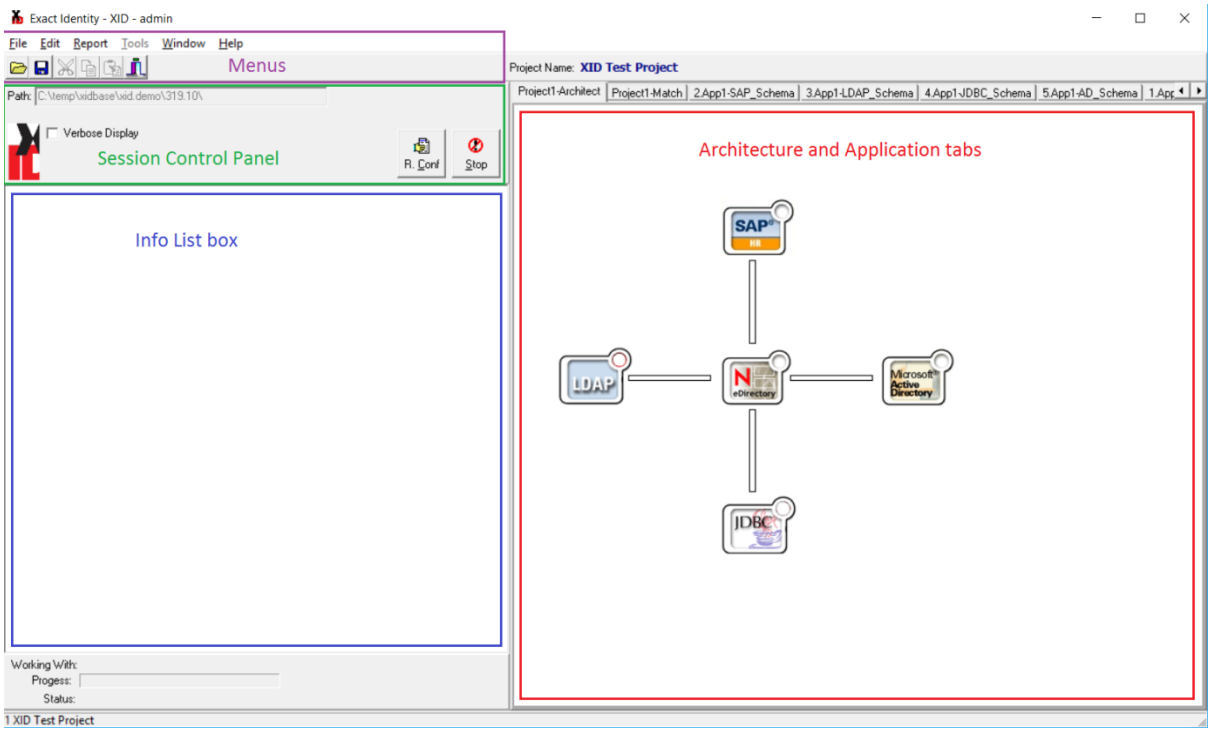
The full XID version will be used for this manual.

Once extracted, the program can be run by double clicking the executable program in Windows explorer.

- Run: **`xid.exe`**
- The XID Password box is displayed. A password is supplied when purchasing XID. If the password is known, enter the password and click 'OK' or press <enter>. If the password is correct then XID runs in admin mode.
- If the password is not known or XID is being evaluated then do not enter a password and click 'OK'. A box is displayed indicating the password is not correct. Once the box is closed XID continues in user mode. User mode is fully functional but the detailed reports are limited. Note that the cascade wide report is not available for the demo mode.



XID starts and opens the last open project. The system architect tab displays the applications configured.



XID initial configuration

The global configuration file `xid_setup_proj.xml` should reside in the same folder as the XID program.

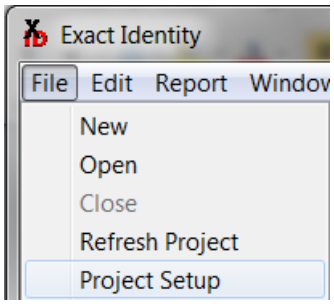
The global configuration file stores the project name, project number and the location method for application input files.

The output file delimiter needs to be set to match that of your system. The shipping configuration is set to use the comma. If the computer system running XID uses a character other than a comma for the CSV delimiter then XID can be updated as follows.

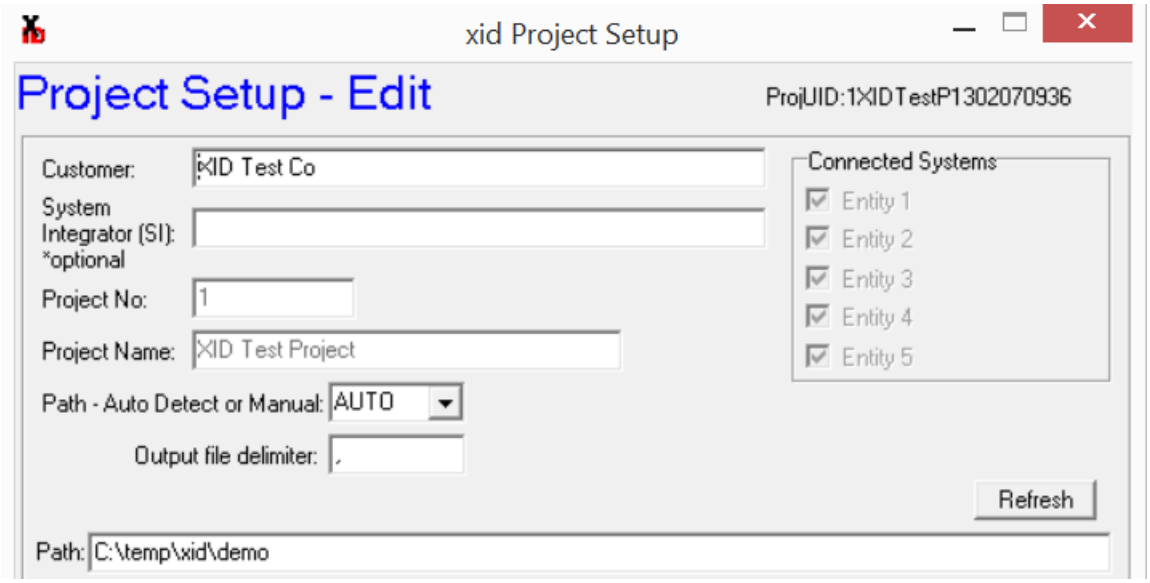
Output File CSV delimiter setting

The following shows how to update XID to accommodate a computer system that does not use comma as the CSV delimiter character.

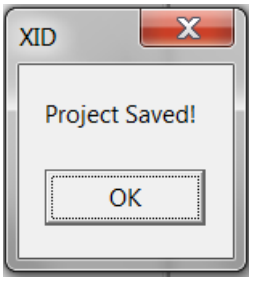
1. Run XID.
2. Click 'File' and select 'Project Setup'.



3. Change the 'Output file delimiter' to match that of your system. Note: Enter '#9' without quotes for a 'tab' delimiter.



4. Click OK.
5. Save the Project by clicking the 'Save' icon  or by clicking 'File' then selecting 'Save'.



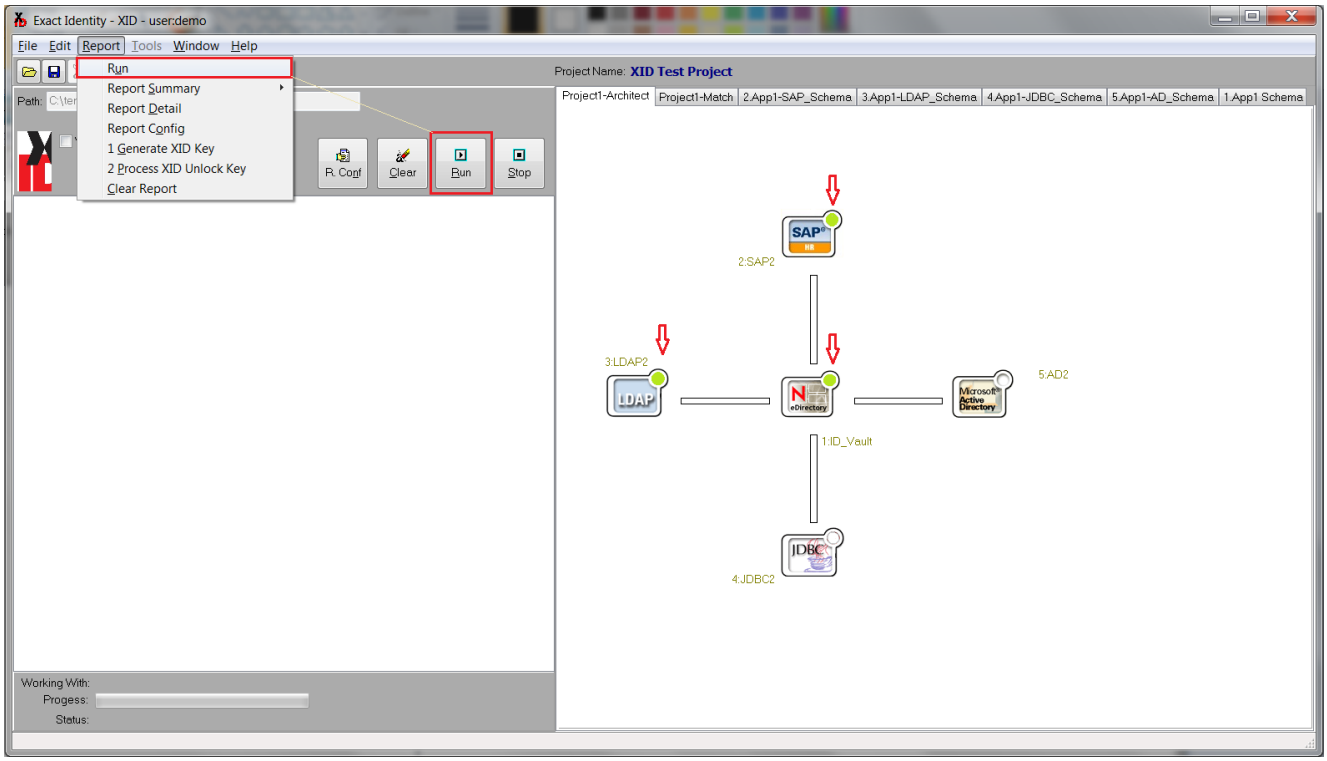
6. Click 'OK' to close the 'Project Saved!' message.

Note: It is recommend that the path is not changed. The path will be set automatically to where XID was extracted and will possibly be different for each XID installation. The 'Path – Auto Detect or Manual' setting should remain set to 'AUTO'. XID will reference the application input files from the detected path when set to auto and the value in the 'Path' edit box is ignored.

Reporting

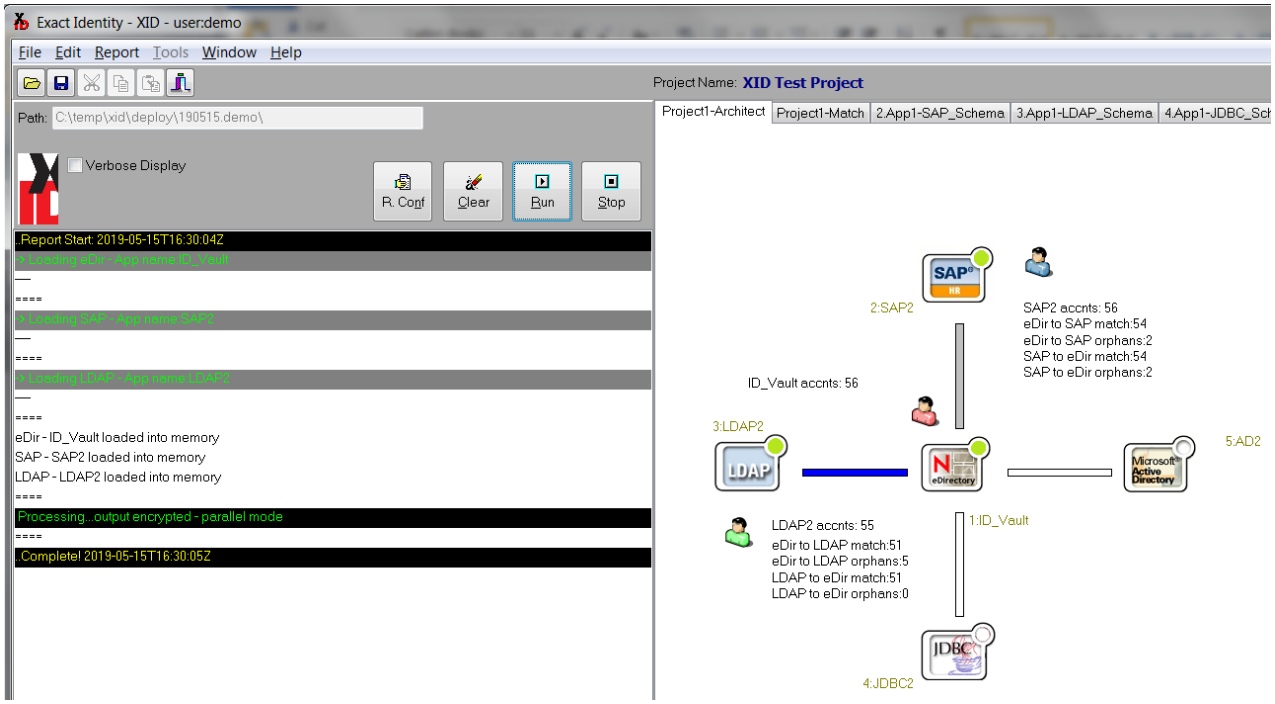
The sample demo system is preconfigured to run "out-of-the-box". A report can be run as follows:

1. Select the "Architect" Page.
2. Click on the applications to be included in the report. To compare one or more applications, the central application 1 *must* be selected together with at least one other application. The following shows the ID Vault eDirectory, SAP and LDAP selected. The green indicator appears when an application is selected. Click again to deselect.
3. Click the 'Run' button or click 'Report' and select 'Run'.

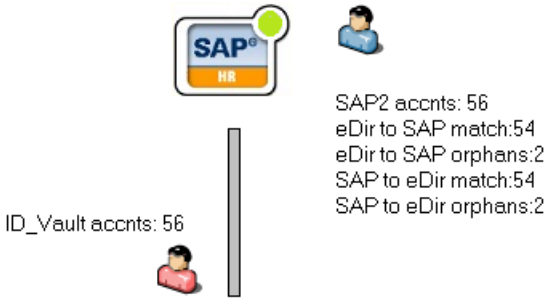


Report Results

The report window displays the processing during the report and the results build in the architect section.

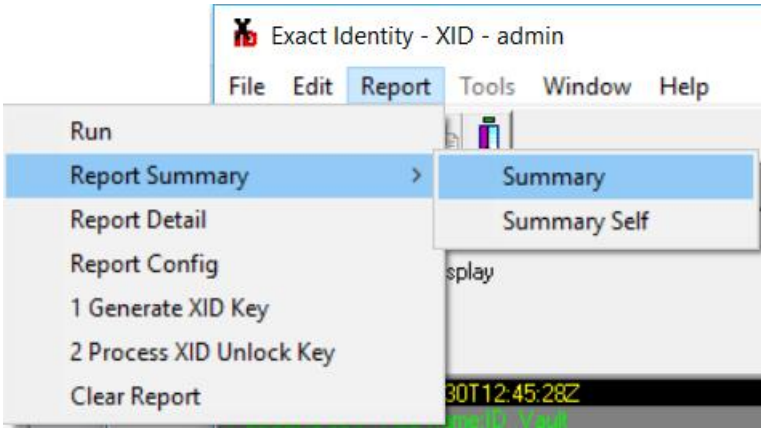


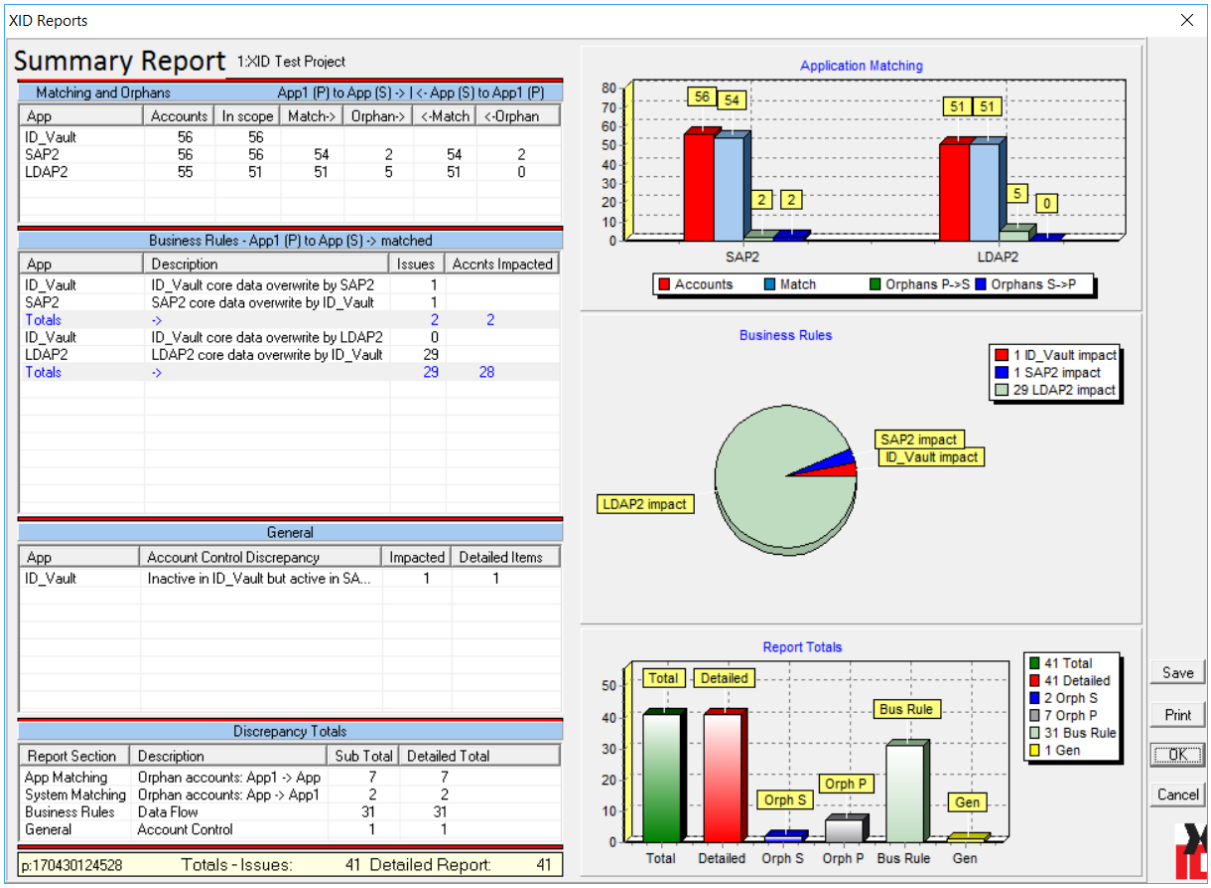
The results for total accounts, matches and orphans are displayed as each application is processed. The list box will display the loading of applications.



Report Summary

To display the report summary click ‘Report’ then select ‘Summary’.





The summary shows the Application Matching, Business Rule and Account Control totals with corresponding graphs to the right.

The Application Matching and Business Rules for parallel mode display only the matches from the lifecycle primary application (ID Vault) to the secondary system. Refer to the appendix section “Match Modes” for a description of “Parallel” and “Cascade” Modes.

The report can be saved to a bitmap file by clicking ‘Save’. The file will be saved in the ‘output’ folder with the name ‘*<ReportUID>_summary_report.BMP*’.

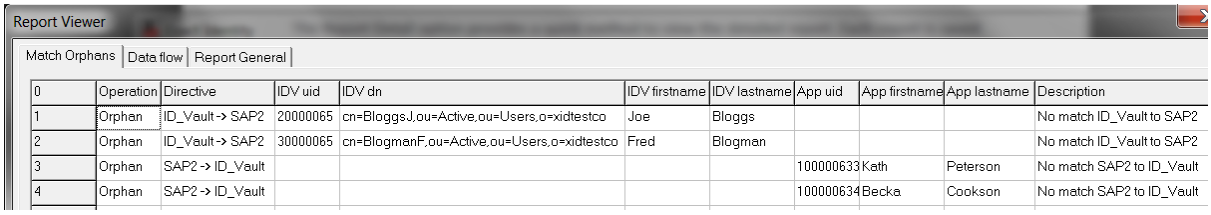
Report Detail

The Report Detail option provides a quick method to view the detailed report. Each report is saved as a CSV file that can be opened using a spread sheet such as Microsoft Excel.

To access the report detail, click ‘Report’ and select ‘Report Detail’.

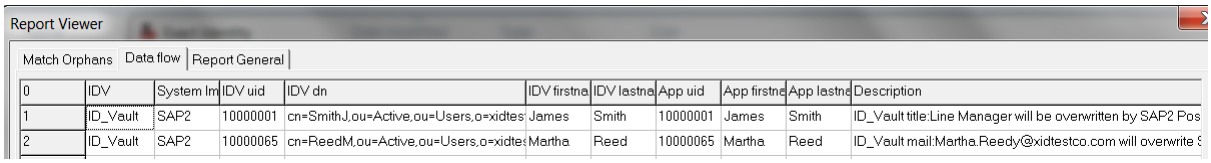
The Report Detail comprises ‘Match Orphans, ‘Data Flow’ and ‘Report General’ tabs and are encrypted if in user mode or if using the demo program.

The following shows the decrypted detailed reports. The full sample files are located ‘..**\output\sample_detailed_reports’**.



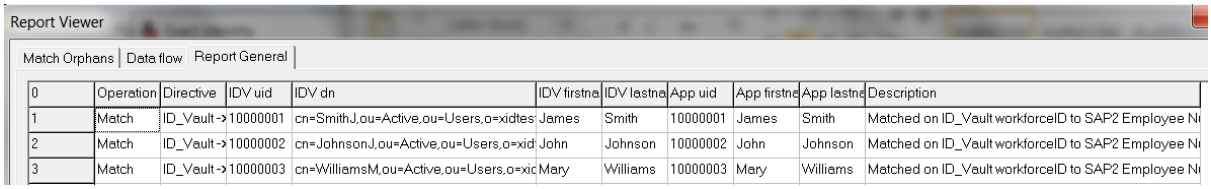
0	Operation	Directive	IDV uid	IDV dn	IDV firstname	IDV lastname	App uid	App firstname	App lastname	Description
1	Orphan	ID_Vault -> SAP2	20000065	cn=BloggsJ,ou=Active,ou=Users,o=xidtestco	Joe	Bloggs				No match ID_Vault to SAP2
2	Orphan	ID_Vault -> SAP2	30000065	cn=BlogmanF,ou=Active,ou=Users,o=xidtestco	Fred	Blogman				No match ID_Vault to SAP2
3	Orphan	SAP2 -> ID_Vault					100000633	Kath	Peterson	No match SAP2 to ID_Vault
4	Orphan	SAP2 -> ID_Vault					100000634	Becka	Cookson	No match SAP2 to ID_Vault

Match Orphans tab - XID_Test_Project_1_matchorphans.csv



0	IDV	System Im	IDV uid	IDV dn	IDV firstna	IDV lastna	App uid	App firstna	App lastna	Description
1	ID_Vault	SAP2	10000001	cn=SmithJ,ou=Active,ou=Users,o=xidtes	James	Smith	10000001	James	Smith	ID_Vault title:Line Manager will be overwritten by SAP2 Pos
2	ID_Vault	SAP2	10000065	cn=ReedM,ou=Active,ou=Users,o=xidtes	Martha	Reed	10000065	Martha	Reed	ID_Vault mail:Martha.Reedy@xidtestco.com will overwrite S

Data flow based on business rules tab - XID_Test_Project_1_busrulegen.csv



0	Operation	Directive	IDV uid	IDV dn	IDV firstna	IDV lastna	App uid	App firstna	App lastna	Description
1	Match	ID_Vault ->	10000001	cn=SmithJ,ou=Active,ou=Users,o=xidtes	James	Smith	10000001	James	Smith	Matched on ID_Vault workforceID to SAP2 Employee N
2	Match	ID_Vault ->	10000002	cn=JohnsonJ,ou=Active,ou=Users,o=xid	John	Johnson	10000002	John	Johnson	Matched on ID_Vault workforceID to SAP2 Employee N
3	Match	ID_Vault ->	10000003	cn=WilliamsM,ou=Active,ou=Users,o=xic	Mary	Williams	10000003	Mary	Williams	Matched on ID_Vault workforceID to SAP2 Employee N

Report General - XID_Test_Project_1_reportlogen.csv

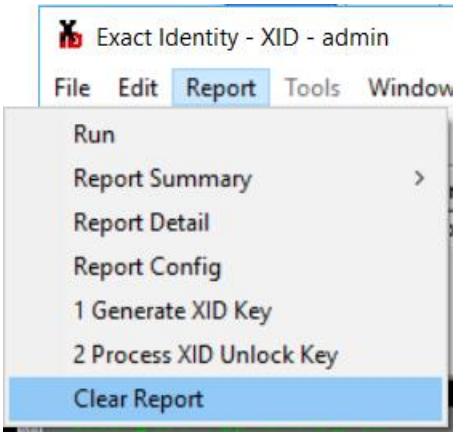
The business rule wide report is generated in cascade mode is only available to view in a spreadsheet for registered users. The file is located in the '..\output' directory and is named:

<*Unique identifier*>_busrulegenwide_dcrypt.csv

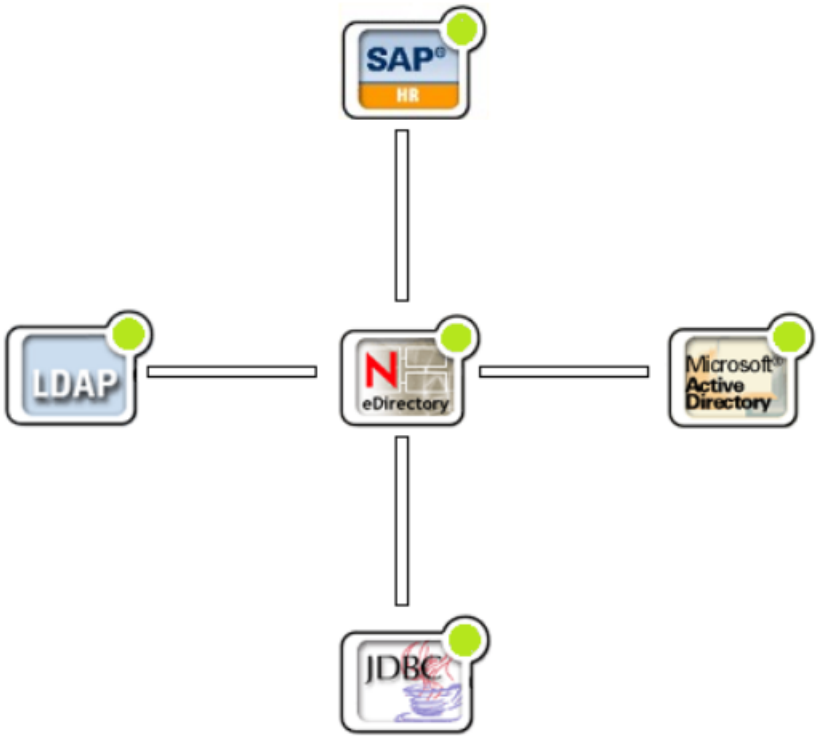
Run a new report

A new report can be run after clearing the existing report.

1. Click ‘Report’ and select ‘Clear Report’.

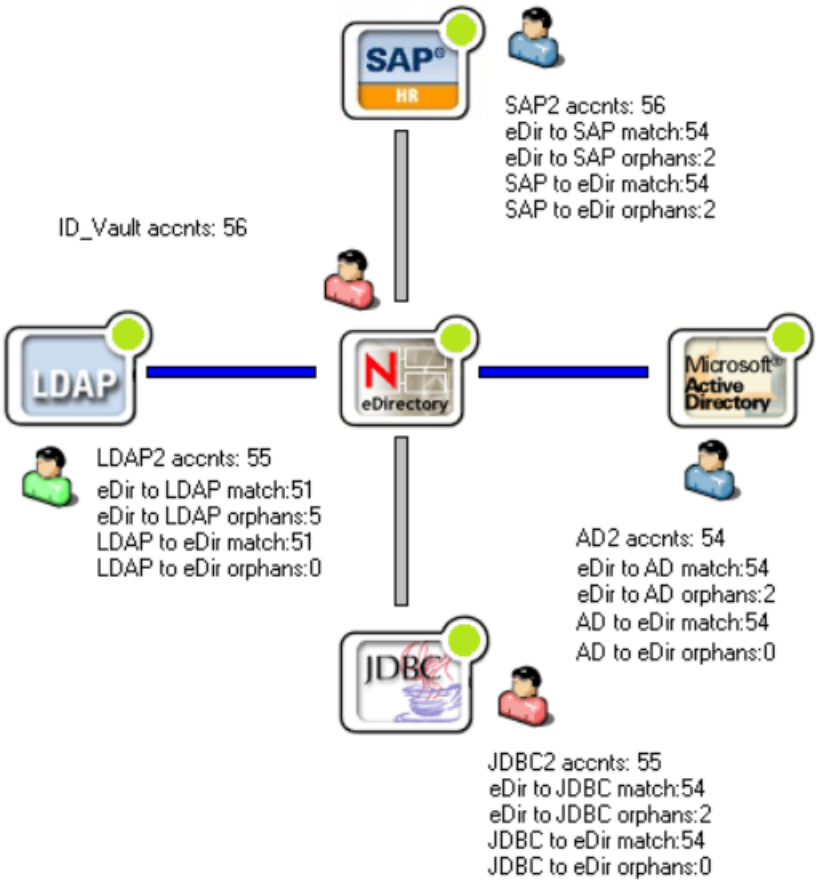


2. Click ‘Yes’ to confirm the action.
3. In the architect tab, select the applications to be included in the report.

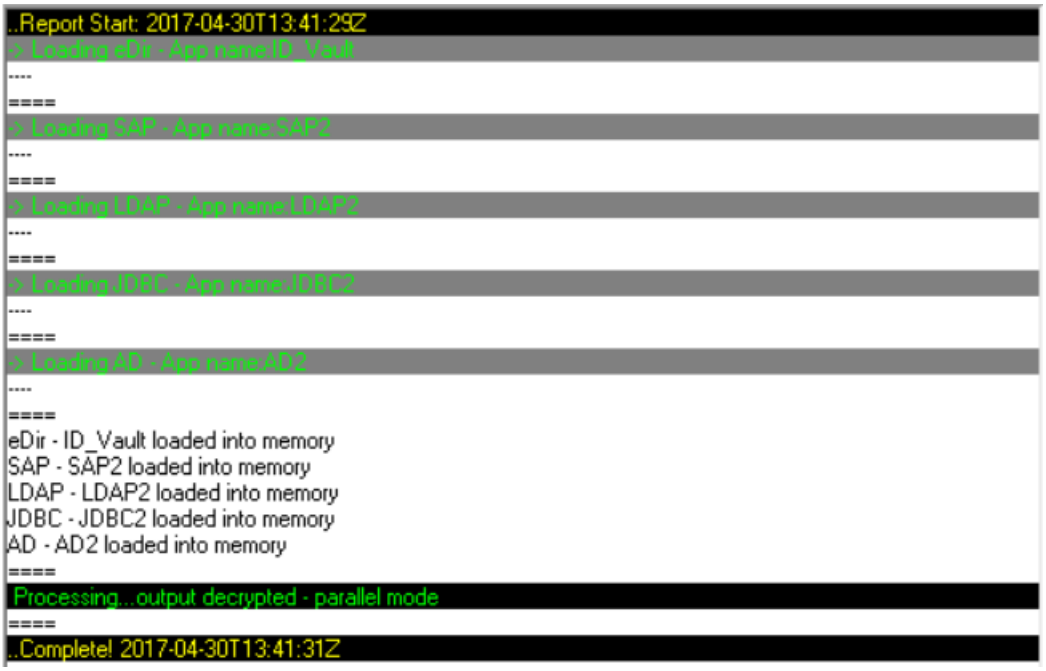


4. Click the ‘Report’ menu and select ‘Run’.

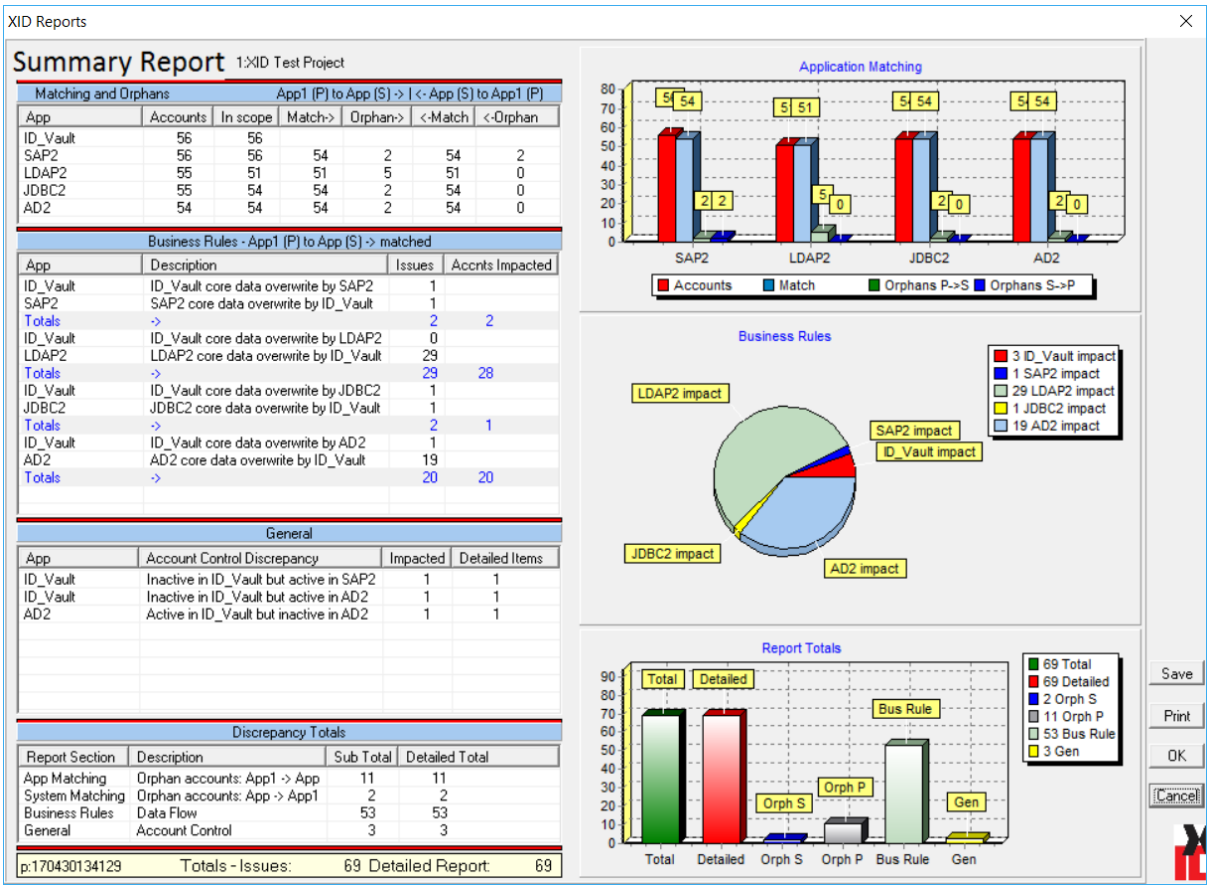
5. The architect tab shows the results summary for each application.



6. The list box displays a summary of the report process.



7. View the report summary by clicking ‘Report’ and selecting ‘Summary’.

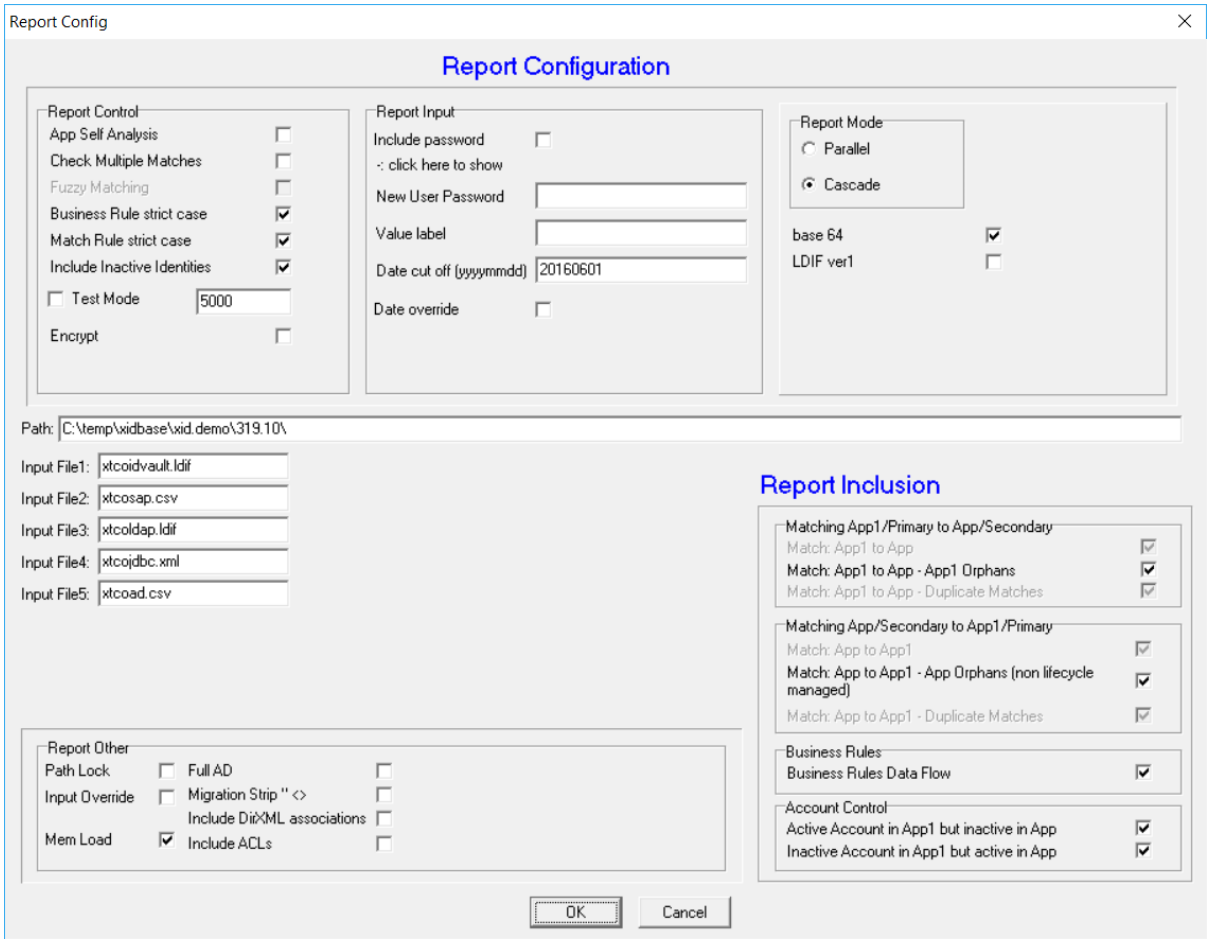


8. Click ‘OK’ to close the report summary.

Report Configuration

1. Click ‘Report’ then select ‘Report Config’ or click the 'R. Conf' button.

2. The 'Report Config' window is displayed providing options that impact the report output.



Report Priority Controls

Report Mode - Parallel	All Apps centric to primary Application (App) 1.
Report Mode - Cascade	Wide business rule report is produced.
Check Multiple Match	Parallel mode only: Duplicate accounts are searched.

Report Control

Setting	Values	Description
App Self Analysis	true/false	This looks at the individual application(s) individually checking information such as missing managers, elevated privileges if entitlements are configured. If only one application is selected for a report then the App Self Analysis checkbox is selected automatically.
Check Multiple Matches	true/false	Parallel mode only: Duplicate accounts are searched if selected.
Fuzzy Matching	true/false	When set to true data transformation rules are applied that allow dissimilar formatted attributes from different applications to be converted and compared.
Business Rule strict case	true/false	True: The attribute comparison must exactly match between apps regardless of case. False: The attribute comparison is case independent.
Match Rule strict case	true/false	True: The match attribute comparison must exactly match between apps regardless of case. False: The match attribute comparison is case independent.
Include Inactive Identities	true/false	If the LDAP datasource has an 'Inactive' Identity store then this can be configured on the Application. Inactive Identities can be included or excluded depending on the requirement.
Report Mode	Parallel	All Apps centric to primary Application (App) 1.
	Cascade	Cascade matches App1 to the next downstream App. Once a match is found XID searches the next selected App. The wide business rule report is produced.

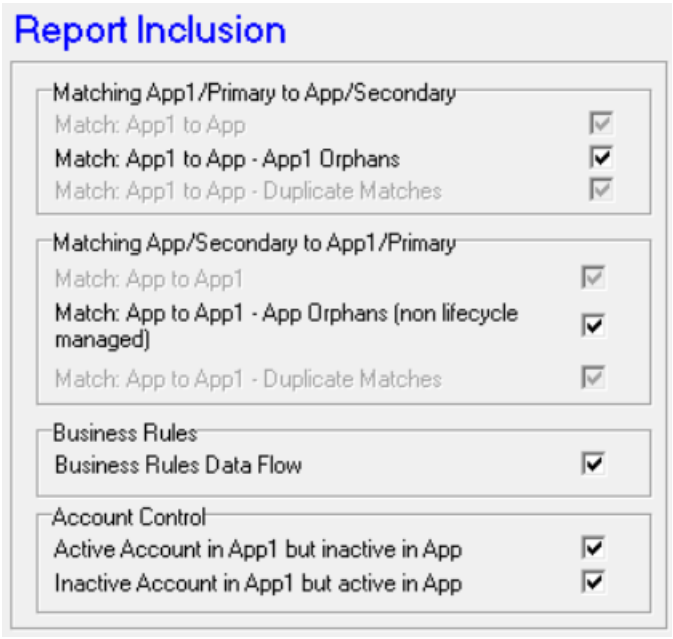
Report Inclusion

The report inclusion can be changed to select or deselect items that are to be included in the report. This allows customisation of what detail will be highlighted. If, for example, only orphans are to be included then ‘Business Rules’ and ‘Account Control’ information can be excluded.

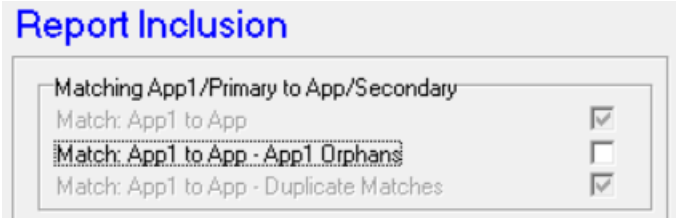
The primary use for making the report configuration change is to ensure only required items are selected for line item or per issue billing.

The configuration can be updated and a summary re-displayed without having to re-run the report.

1. Click ‘Report’ then select ‘Report Config’ or click the 'R. Conf' button.
2. The following displays the default settings for the demo version. The greyed items cannot be changed in this version of XID.

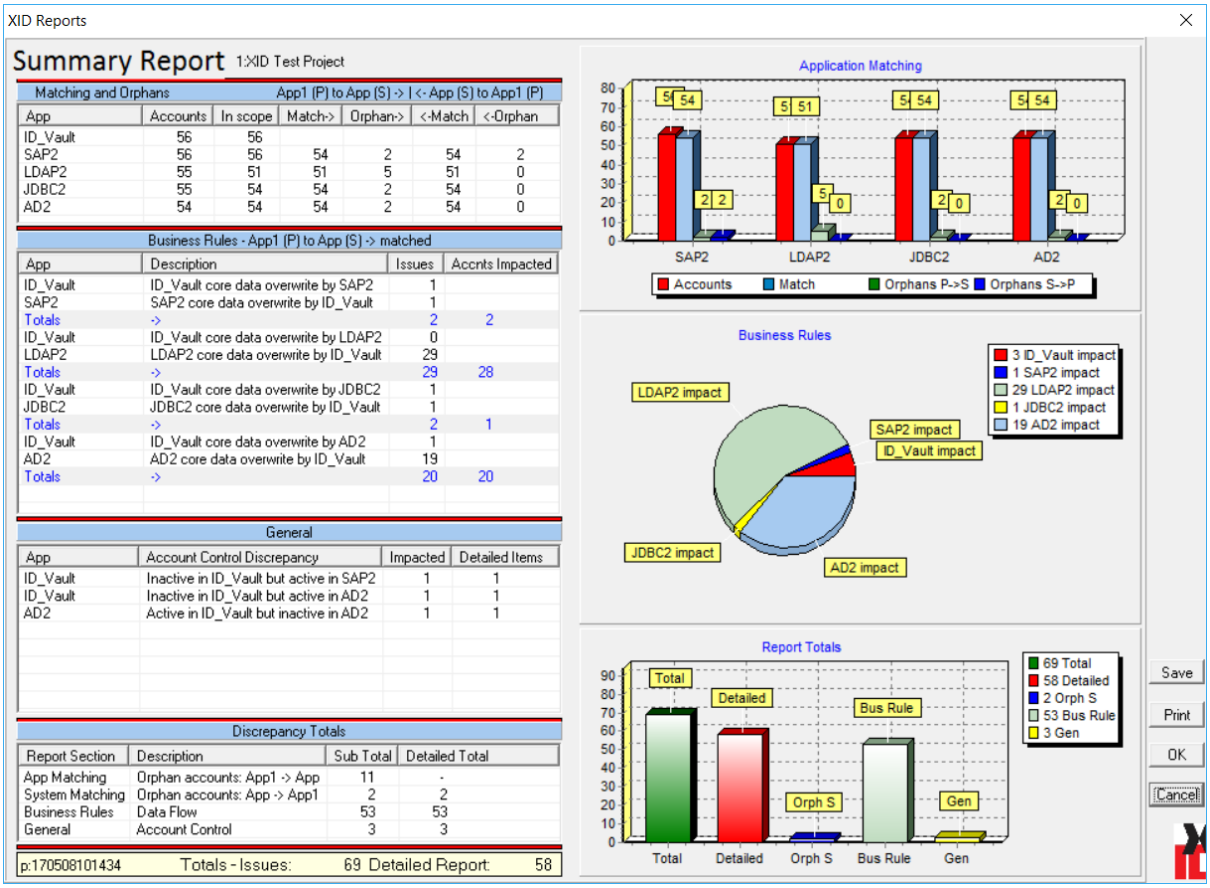


3. To exclude the ‘App1 to App’ orphans for example, click the ‘Match App1 to App – App1 Orphans’ check box. Note that the ‘Application to IDV’ orphans are the non-lifecycle managed orphans that cannot be matched by the ID Vault.



4. Click ‘OK’ to update the report configuration. The change will be reflected in the report summary without the need to re-run another report.

5. Click ‘Report’ then select ‘Show Summary’. Orphan accounts ‘App1 -> App’ are now excluded in the Detailed Report Total.

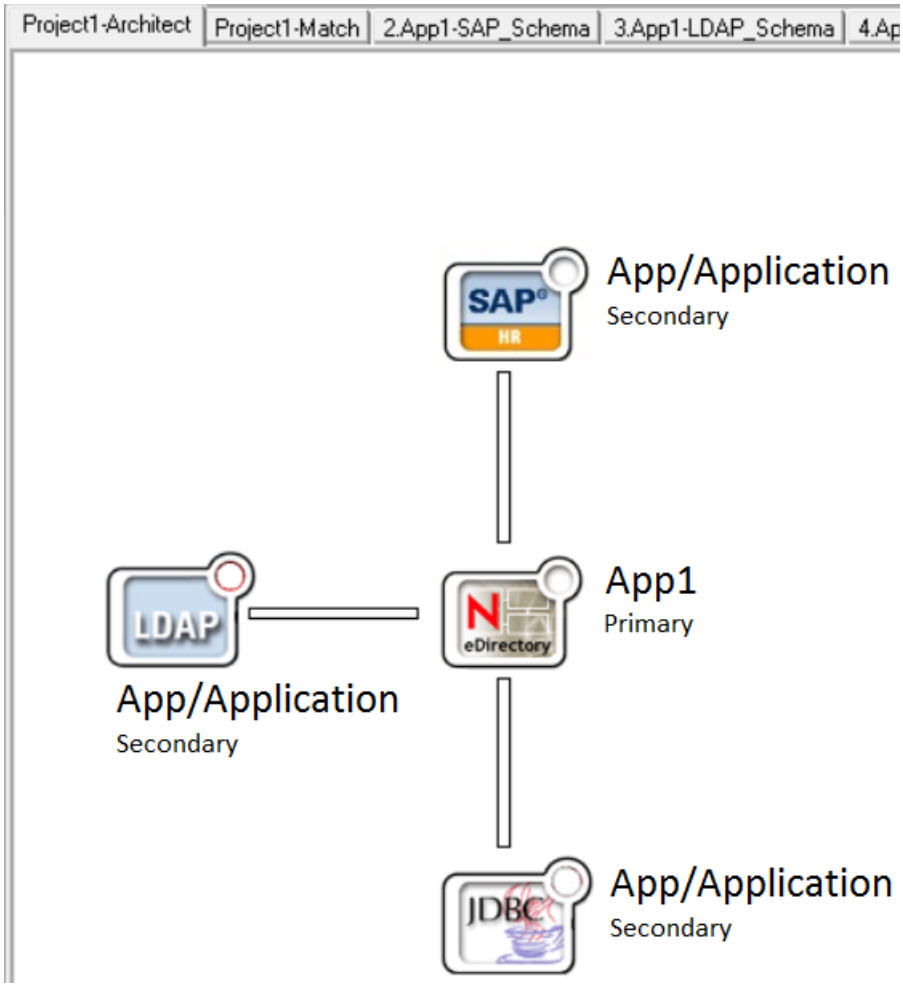


6. Click ‘OK’ to close the report summary.

XID Architecture

XID Architect

The architect screen displays configured applications and will update during reporting to indicate application totals, matches and orphans.

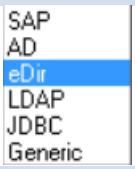
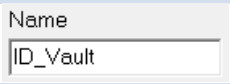
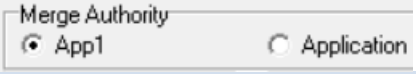


The Primary App1 is always located in the centre with the secondary Applications (Apps) displayed in a hub and spoke configuration.

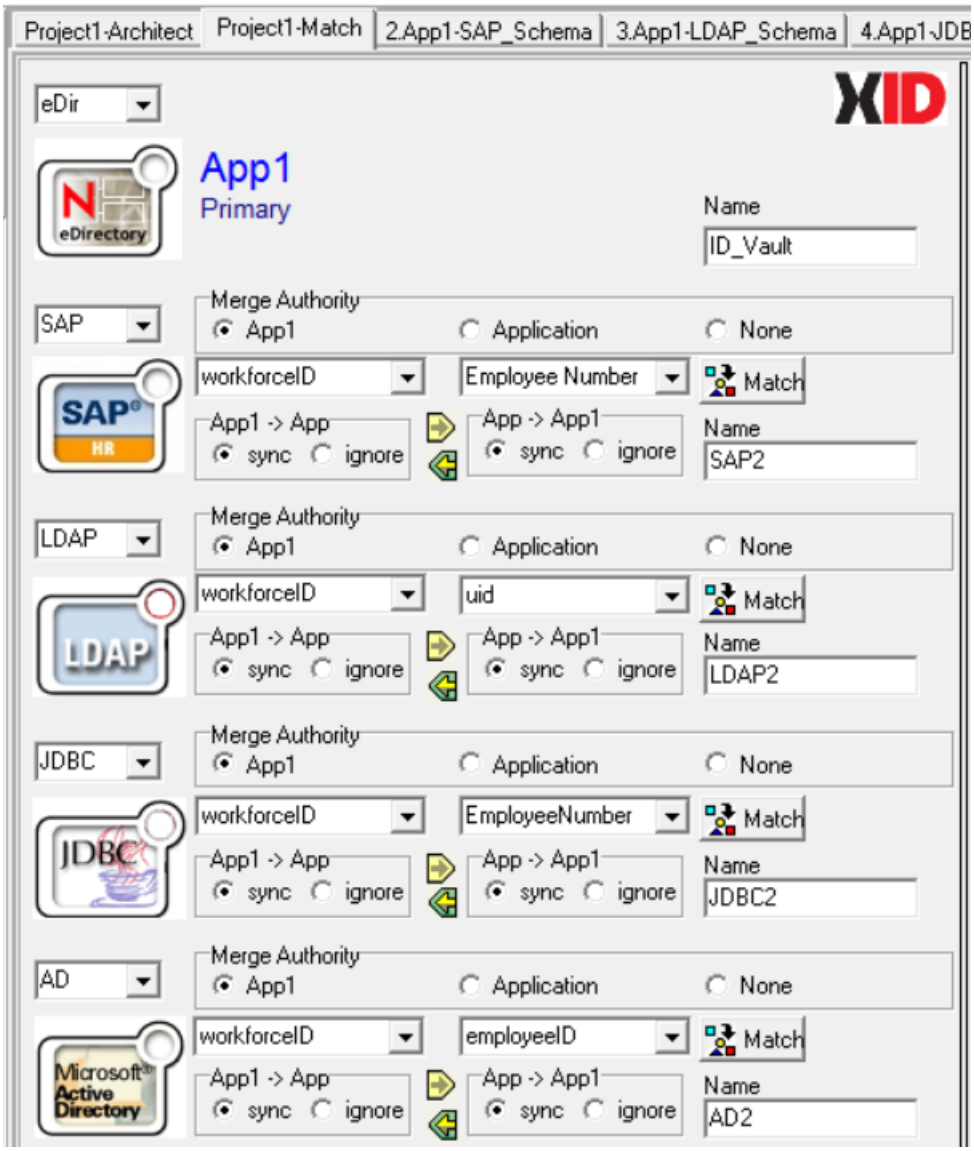
An App can be edited by double clicking the application image.

Match

The Match tab is where the following is configured:

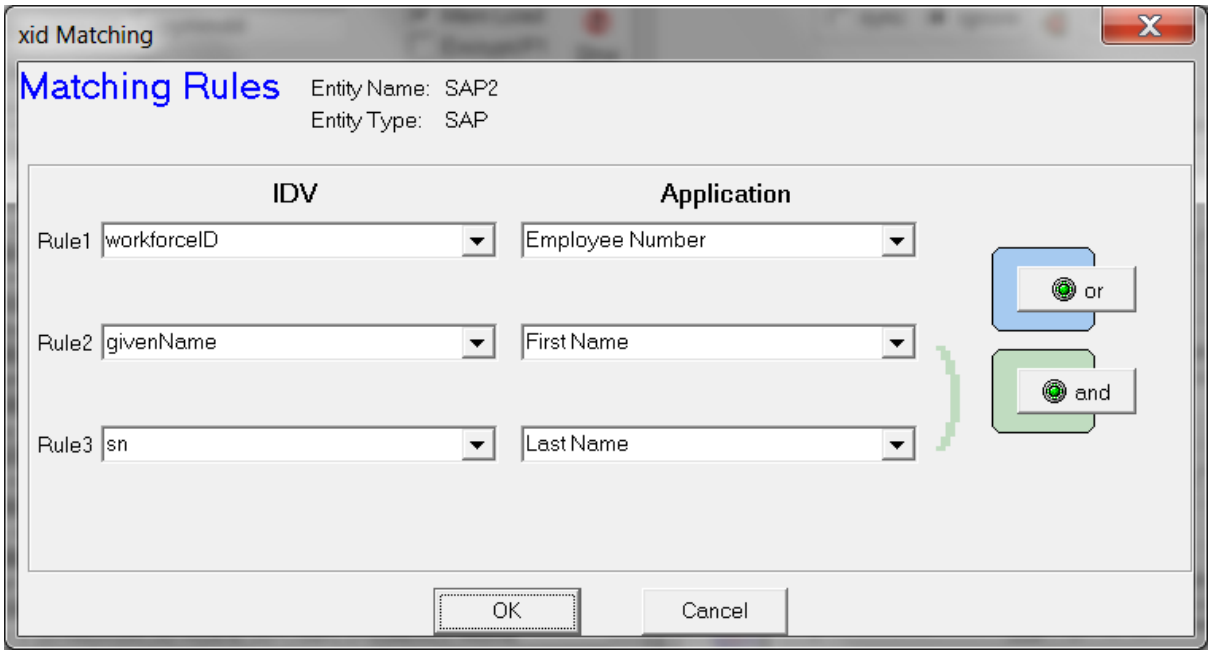
Item		
Application Type	Sets the application type using the combo box. The primary App1 must always be the first application in the list.	
Application Name	Set the name of the application	
Global Merge Authority	Determines the account lifecycle creation point for the company	
Matching Rules	Sets the matching attributes used to match accounts between systems	

The following shows the sample application Match tab configuration.



Each Application has a match button to the right of the match pair. 

The match button displays a Windows that provides further options for application matching.

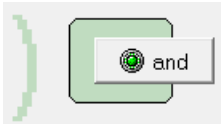


Rule 1 is the primary rule specified in the main matching tab. Rule 1, in this example, specifies that App1 ‘workforceID’ will be used as the attribute to match the Application ‘Employee Number’ attribute.

The combo boxes in Rule 2 and Rule 3 allow the selection of further attributes for matching purposes.

In addition to defining matching rules there are operator buttons that define operator functions between Rule 1 and Rule 2 and Rule 2 and Rule 3. The default operator rule ‘and’ can be changed to ‘or’ by clicking the button. The above example shows that the operator for the top button (blue surround) has been changed to ‘or’ for Rule 1 and Rule 2.

The lower button with the green surround is set to ‘and’ for Rule 2 and Rule 3. This rule has an additional bracket surrounding Rule 2 and Rule 3. The bracket will force Rule 2 and Rule 3 to be processed first. The result will then be “or’d” with Rule 1.



To activate a bracket for Rule 1 and 2, click the blue shaded area next to the operator button.

To activate a bracket for Rule 2 and 3, click the green shaded area next to the operator button.

To deselect the bracket, click the bracket graphic. 

Rules must be defined sequentially so that Rule 3 cannot be defined without having Rule 2 defined.

To clear a rule, select hyphen from the combo list. This action will clear the rule set pair.

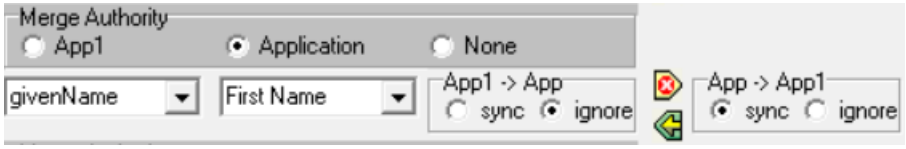
Click ‘OK’ in the matching rule window to save the changes or ‘Cancel’ to abandon the changes. Although the matching rule changes are updated for the session, the project will need to be saved to update the changes permanently.

Business Rules Schema Map

The application configured in the match tab is allocated a Schema Map tab page. The schema map page allows mapping of App1 attribute values to the Application attribute values. For each mapping a Merge Authority and authoritative rule set can be configured. XID also applies the term 'Business Rules' to these settings.

The combo boxes are populated with the schema values specified in the Application configuration page. The left combo box displays attributes from App1. The right combo box displays attributes for the Application.

The following example shows the App1 ‘givenName’ attribute mapped to the ‘First Name’ attribute in the SAP Application.

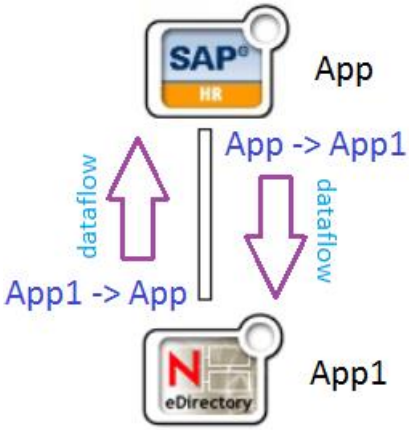


The Merge Authority is set to ‘Application’ which indicates that in the event of attribute overwrite arbitration, the Application will always overwrite unless the business rules set in ‘App1 -> App’ and ‘App -> App1’ indicate otherwise.

- **App1 -> App:** Data flows from the primary App1 to the Application.

Sync: Data can flow from App1 to the Application.

Ignore: Data does not flow from App1 to the Application.



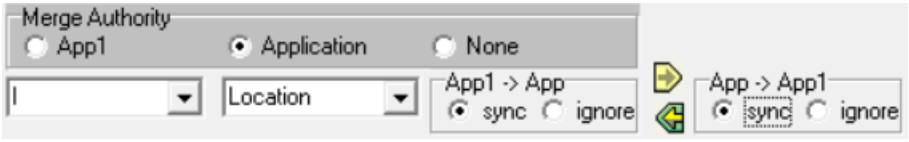
- **App -> App1:** Data flows from the Application to the primary App1.

Sync: Data can flow from the Application to App1.

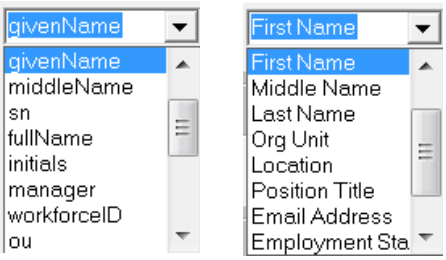
Ignore: Data does not flow from the Application to App1.

For the [‘givenName’ -> ‘First Name’] mapping, the business rules have been configured so that changes from App1 (eDirectory) are ignored and the changes from the App (SAP) are synchronised.

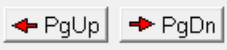
For the [‘l’ -> ‘Location’] mapping, the business rules have been configured so that changes from App1 and the App are synchronised. The Merge Authority in this example dictates that the Application will be authoritative in a situation whereby App1 and App values differ.



The following shows the ‘givenName’ attribute selected for App1 and the ‘First Name’ attribute (that corresponds to the App1 attribute) selected for the Application (SAP).



The Merge Authority and business rules can then be set for the attribute as required.

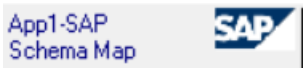
The Page Up and Page Down buttons allow access to more pages so that more attributes can be configured if required. 

Subsequent pages show similar settings but for the Application type specified in the Matching page.

To delete a rule; highlight a rule and press the delete key or select ’-‘ from the App1 and/or Application combo boxes.

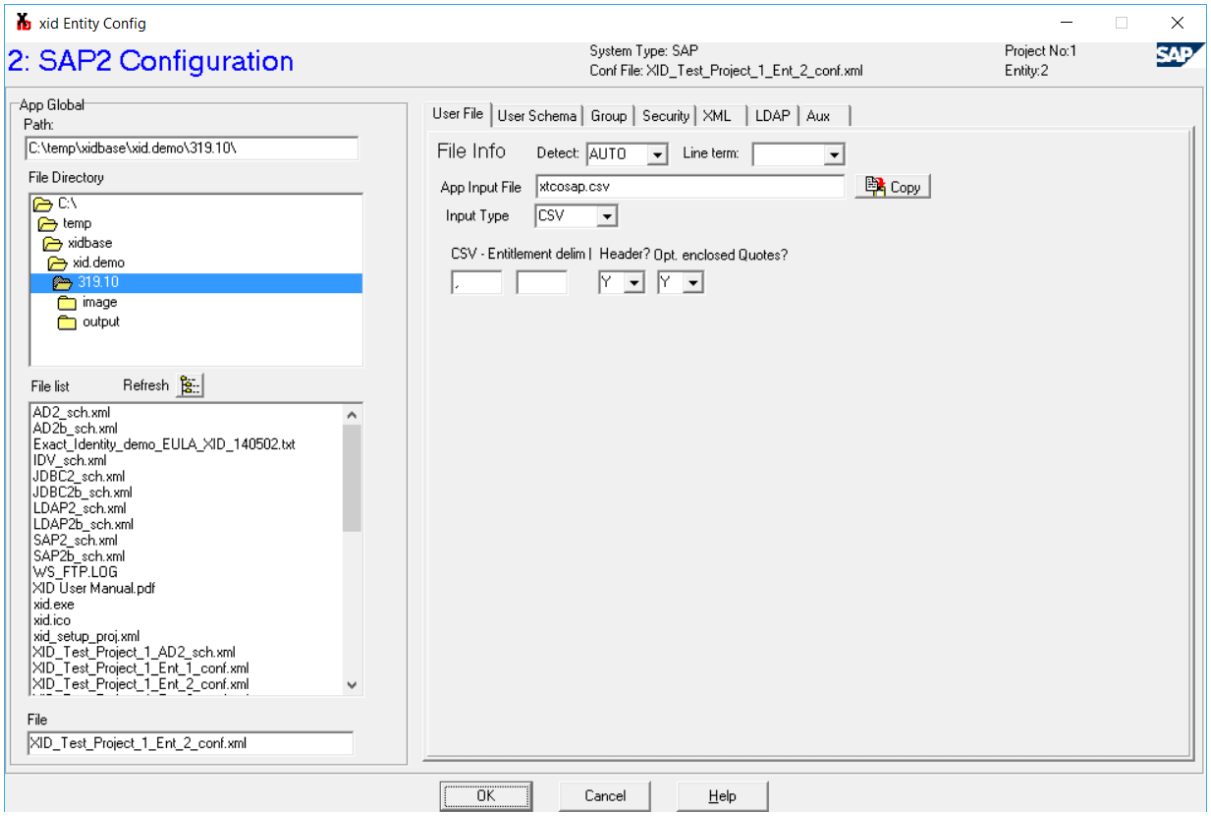
The following is the LDAP Application schema map. The attributes in the LDAP schema are different and are reflected in the combo boxes.

Application Configuration

Application configuration can be accessed by clicking the application graphic in the schema map which is SAP in this example. 

Note that the application configuration can also be accessed by clicking the system graphic in the matching tab. 

The application configuration specifies details for the Application such as file input information, schema, account security and special account masking.



Click ‘Cancel’ to exit the configuration if no changes have been made.

XID Data Analysis Manipulation

Scenarios can be created by changing the input data or by changing the business rules in XID.

Input data change

The sample data is supplied in LDIF, CSV and XML formats and is located in the 'input' folder.

The files can be edited to change data or to remove or add complete records to a maximum of 60 for the demo version.

Care must be taken not to alter the format so the data no longer matches the standard input format. The files are also Windows Carriage Return Line Feed (CR LF) format. While this can be changed to LF, the configuration will have to be changed in XID to indicate that system has changed input file format. The last record for all files must have a CR LF after the final row.

Only a text editor can be used to alter the data. Suitable text editors include Windows Notepad, Notepad++, UltraEdit, EmEditor etc. Applications such as Microsoft Word, WordPad are not suitable.

- ID Vault – `xtcoidvault.ldif`
  - The ID Vault App1 uses the 'LDAP Data Interchange Format' (LDIF). The first two records are shown below.
  - Each record begins with `dn: cn=<distinguished name of object>`
  - Each attribute begins with the attribute name, colon, space then the attribute value.
  - The record completes with a blank row then the next record begins. The final record finishes with a carriage return – line feed (CR LF).
  - Attribute values can be altered in the file then the file can be saved.

```
dn: cn=SmithJ,ou=Active,ou=Users,o=xidtestco
givenName: James
middleName: null
sn: Smith
fullName: James Smith
initials: null
manager: null
workforceID: 10000001
ou: HR
l: Paris
title: Line Manager
mail: James.Smith@xidtestco.com
telephoneNumber: 33110102
mobile: 33120103
loginDisabled: FALSE
cn: SmithJ

dn: cn=JohnsonJ,ou=Active,ou=Users,o=xidtestco
givenName: John
middleName: null
sn: Johnson
fullName: John Johnson
initials: null
manager: cn=SmithJ,ou=Active,ou=Users,o=xidtestco
workforceID: 10000002
ou: Drafting
```

```
l: Seattle
title: Line Manager
mail: John.Johnson@xidtestco.com
telephoneNumber: 20610103
mobile: 20620104
loginDisabled: FALSE
cn: JohnsonJ
```

- SAP – `xtcosap.csv`
  - SAP uses the Comma-separated values (CSV) format. Attributes have been optionally enclosed with quotes that enable information with commas to be imported without the creation of extra columns by applications that read the CSV file.
  - Records can be deleted or added (to a maximum of 60 for the demo) by deleting or adding a row. The last row must be terminated by a CR LF.
  - Data in each row and column can be changed using a text editor.

```
"Employee Number","First Name","Middle Name","Last Name","Org Unit"
```

```
"10000001","James","null","Smith","HR","Paris","Area Manager"
"10000002","John","null","Johnson","Drafting","Seattle","Line Manager"
```

- JDBC – `xtcojdbc.xml`
  - The JDBC (Oracle Database) data is stored in XML format.
  - Each record has an opening tag of <Record> and a closing tag of </Record> that encapsulates the record fields.
  - Field names have an opening field name tag such as <EmployeeNumber>, <LoginName> etc.
  - The field values are contained within the opening and close field value tag.
  - A text editor can be used to change the values for each field. The field will not be recognised if the field name is changed as these values map to the schema settings in the XID configuration for the connected system.
  - Entire records can be removed or added (to a maximum of 60 for the demo) using the format used by the records that are in existence.
  - The final row must have a CR LF.

```
<?xml version="1.0" standalone="yes" ?>
<User>
<Record>
<EmployeeNumber>10000001</EmployeeNumber>
<LoginName>SmithJ</LoginName>
<FirstName>James</FirstName>
<LastName>Smith</LastName>
<Location>Paris</Location>
<Department>HR</Department>
<Title>Line Manager</Title>
<EmailAddress>James.Smith@xidtestco.com</EmailAddress>
<PhoneNumber>33110102</PhoneNumber>
<Mobile>33120103</Mobile>
```

```
<AccountStatus>Active</AccountStatus>
</Record>
<Record>
<EmployeeNumber>10000002</EmployeeNumber>
<LoginName>JohnsonJ</LoginName>
<FirstName>John</FirstName>
<LastName>Johnson</LastName>
<Location>Seattle</Location>
<Department>Drafting</Department>
<Title>Line Manager</Title>
<EmailAddress>John.Johnson@xidtestco.com</EmailAddress>
<PhoneNumber>20610103</PhoneNumber>
<Mobile>20620104</Mobile>
<AccountStatus>Active</AccountStatus>
</Record>
```

- LDAP – `xtcoldap.ldif`
  - The LDAP system uses the 'LDAP Data Interchange Format (LDIF). The first two records of the LDIF are show below.
  - Each record begins with `dn: cn=<distinguished name of object>`
  - Each attribute begins with the attribute name, colon, space then the attribute value.
  - The record completes with a blank row then the next record begins. The final record finishes with a carriage return – line feed (CR LF).
  - Attribute values can be altered in the file then the file can be saved.

```
dn: cn=SmithJ,ou=Paris,ou=FR,o=xidtestco
givenName: James
sn: Smith
fullName: James Smith
uid: 10000001
ou: HR
l: Paris
mail: James.Smith@xidtestco.com
telephoneNumber: 33110102
mobile: 33120103
title: Line Manager
loginDisabled: FALSE
cn: SmithJ

dn: cn=JohnsonJ,ou=Seattle,ou=US,o=xidtestco
givenName: John
sn: Johnson
fullName: John Johnson
uid: 10000002
ou: Drafting
l: Seattle
mail: John.Johnson@xidtestco.com
telephoneNumber: 20610103
mobile: 20620104
title: Line Manager
loginDisabled: FALSE
cn: JohnsonJ
```

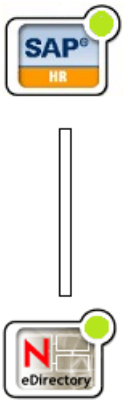
- AD – `xtcoad.csv`
    - AD uses the Comma-separated values (CSV) format. Some attributes have been optionally enclosed with quotes that enable information with commas to be imported without the creation of extra columns by applications that read the CSV file.
    - Records can be deleted or added (to a maximum of 60 for the demo) by deleting or adding a row. The last row must be terminated by a CR LF.
    - Data in each row and column can be changed using a text editor.

```
dn,sAMAccountName,sAMAccountType,..
"cn=SmithJ,ou=HR,ou=Paris,ou=FR,DC=xidtestco,DC=com",SmithJ,..
"cn=JohnsonJ,ou=Drafting,ou=Seattle,ou=US,DC=xidtestco,DC=com",JohnsonJ,..
```

XID Business Rules change

The following example shows a report run with the business rules set as per the shipped XID package. The business rules will be changed and the report will reflect this in the report.

1. Run a report selected SAP and ID Vault only.
    a. In the architect section, select the primary centre App1 (eDirectory) and SAP by clicking the Application icons.
    b. Click ‘Report’ and select ‘Run’.



2. Click ‘Report Summary’ then 'Summary’.
3. Click the ‘Data flow’ tab. The following are the decrypted results for the detailed report.

Report General Log | Data flow

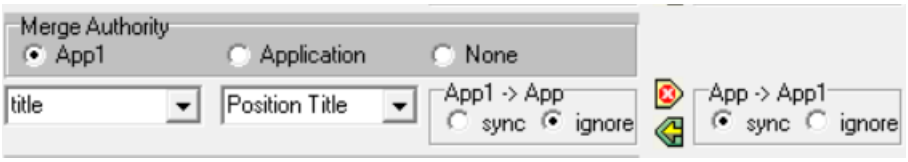
0	IDV	System Im	IDV uid	IDV dn	IDV firstname	IDV lastname	Description
1	ID_Vault	SAP2	10000001	cn=SmithJ,ou=A(	James	Smith	ID_Vault title:Line Manager will be overwritten by SAP2 Position Title
2	ID_Vault	SAP2	10000065	cn=ReedM,ou=A	Martha	Reed	ID_Vault mail:Martha.Reedy@xidtestco.com will overwrite SAP2 Em

4. The description indicates the following:

- James Smith ID Vault title attribute ‘Line Manager’ will be overwritten by SAP Position Title.
- Martha Reed ID Vault attribute will mail will overwrite SAP email.

5. Close the report detail window by clicking ‘Cancel’.

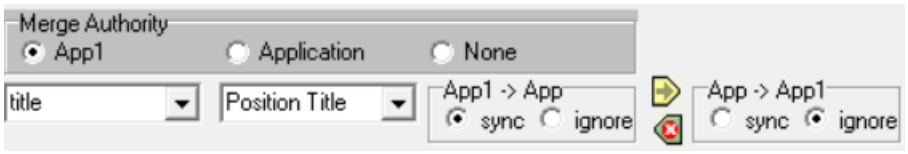
6. Click the '2.App1-SAP_Schema' tab.



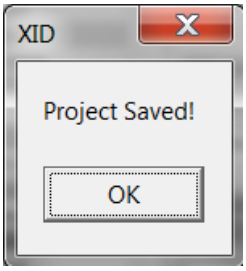
Note that the App1 'title' to App (SAP) 'Position Title' mapping indicates that changes from App1 will be ignored (App1->App set to ignore) and changes from SAP will update the ID Vault (App->App1 set to sync). This will override the merge authority set to App1.

The following will reverse the business rules to make the App1 ID Vault authoritative for the title attribute.

1. To change the business rules click the 'sync' radio button in the Subscribe section of the title attribute. Click the 'ignore' radio button in the Publish section of the title attribute. The business rules should look as follows:

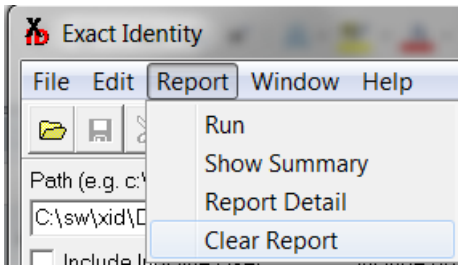


2. Save the project by clicking the save icon or by clicking the 'File' menu and selecting 'Save'.
3. Click 'OK' to close the save confirmation box.



4. Select the architect tab of the project.

5. Clear the previous report by clicking the ‘Report’ menu and selecting ‘Clear Report’.



6. Reselect the ID Vault and SAP for reporting as per step 1.
7. Click ‘Report’ and select ‘Run’.
8. Click ‘Report’ and select ‘Report Detail’.
9. Click the ‘Data flow’ tab. The following shows the decrypted results for the detailed report.

Report General Log | Data flow

0	IDV	System Im	IDV uid	IDV dn	IDV firstname	IDV lastname	Description
1	ID_Vault	SAP2	10000001	cn=SmithJ,ou=Active,	James	Smith	ID_Vault title:Line Manager will overwrite SAP2 Position Title:Area Manager
2	ID_Vault	SAP2	10000065	cn=ReedM,ou=Active	Martha	Reed	ID_Vault mail:Martha.Reedy@xidtestco.com will overwrite SAP2 Email Address:

The description has changed to reflect the business rule update so that James Smith ID Vault title attribute ‘Line Manager’ will overwrite SAP Position Title. Previously SAP was authoritative and the ID Vault attribute was being overwritten.

Click ‘Cancel’ to exit the report detail.

Rectification/Remediation Files

Disclaimer: *The Rectification/Remediation files are to be used with caution and are should be tested in a Development/Staging environment before applying to any system that could impact production. The files follow the detailed report modifications made by enforcing the business rules on the data. The updates need to be checked to ensure that the authoritative repositories had the correct data in the first place. It is that reason that the rectification files act as an assistance tool for experienced administrators only and should not be used without first ensuring that the update is authorised with the updated data being checked as correct.*

XID generates a rectification and rollback file. The files are encrypted and will be decrypted with the detailed report.

LDAP Applications, such as Novell eDirectory, Sun ONE LDAP and Active Directory, can utilise the Lightweight Directory Access Protocol (LDAP) Data Interchange Format or LDIF.

There are many tools that can be used to process the LDIF file and update the target directory. OpenLDAP, for example, has a suite of cross platform tools and 'ldapmodify' can be used to import the LDIF files into Novell eDirectory and most LDAP compliant directories such as Sun ONE.

Novell eDirectory also has its own tool called 'Import Convert Export' (ICE) with options as follows:

- Novell iManager (Web based management tool) Import Convert Export Wizard.
- ConsoleOne (Cross-platform Java application) Novell eDirectory Import/Export Wizard.
- Command Line Interface (CLI). Support for Windows, Linux, Solaris, and AIX systems.

Active Directory employs its own tool called LDIFDE that can be used for Import/Export of LDIF files.

Multiple changes can be made per object but XID employs only one update per changetype or object. This is by design so that updates can be easily segregated in the event that staging of updates is to be rolled out.

All LDIF files have a comment line denoted by a '#' character. The first item of the comment is the line item number of the detailed report. This enables correlation between the rectification entry and the XID Detailed Report.

The JDBC in the XID demo is representative of an Oracle database. XID produces an 'SQL*Loader' control file with a corresponding data file. There is also a roll back control and data file. There are limitations with SQL*Loader in that existing tables cannot be modified. The process is to load the rows into a staging table that can later be merged with the tables to be updated. This can also be done for the roll back.

For Microsoft SQL Server a CSV file is created to support 'Bulk Insert'.

For MySQL a CSV file is created to support 'LOAD DATA INFILE'.

Rectification File Samples

ID Vault Rectification LDIF:

```
# 1 ID_Vault title:Line Manager will be overwritten by SAP2 Position Title:Area
Manager
dn: cn=SmithJ,ou=Active,ou=Users,o=xidtestco
changetype: modify
replace: title
title: Area Manager
-

# 54 ID_Vault givenName:Martha will be overwritten by SAP2 First Name:Martha1
dn: cn=ReedM,ou=Active,ou=Users,o=xidtestco
changetype: modify
replace: givenName
givenName: Martha1
-

# 54 ID_Vault telephoneNumber:852710166 will be overwritten by JDBC2
PhoneNumber:952710166
dn: cn=ReedM,ou=Active,ou=Users,o=xidtestco
changetype: modify
replace: telephoneNumber
telephoneNumber: 952710166
-

# 54 ID_Vault mail:Martha.Reedy@xidtestco.com will be overwritten by AD2
mail:Martha.Reed@xidtestco.com
dn: cn=ReedM,ou=Active,ou=Users,o=xidtestco
changetype: modify
replace: mail
mail: Martha.Reed@xidtestco.com
-
```

ID Vault Rollback LDIF:

```
# 1 rollback ID_Vault title:Line Manager will be overwritten by SAP2 Position
Title:Area Manager
dn: cn=SmithJ,ou=Active,ou=Users,o=xidtestco
changetype: modify
replace: title
title: Line Manager
-

# 54 rollback ID_Vault givenName:Martha will be overwritten by SAP2 First
Name:Martha1
dn: cn=ReedM,ou=Active,ou=Users,o=xidtestco
changetype: modify
replace: givenName
givenName: Martha
-

# 54 rollback ID_Vault telephoneNumber:852710166 will be overwritten by JDBC2
PhoneNumber:952710166
dn: cn=ReedM,ou=Active,ou=Users,o=xidtestco
changetype: modify
replace: telephoneNumber
telephoneNumber: 852710166
-
```

```
# 54 rollback ID_Vault mail:Martha.Reedy@xidtestco.com will be overwritten by AD2
mail:Martha.Reed@xidtestco.com
dn: cn=ReedM,ou=Active,ou=Users,o=xidtestco
changetype: modify
replace: mail
mail: Martha.Reedy@xidtestco.com
-
```

AD Rectification LDIF:

```
# 1 ID_Vault title:Line Manager will overwrite AD2 title:Line Mgr
dn: cn=SmithJ,ou=HR,ou=Paris,ou=FR,DC=xidtestco,DC=com
changetype: modify
replace: title
title: Line Manager
-

# 4 ID_Vault telephoneNumber:020710105 will overwrite AD2 telephoneNumber:20710105
dn: cn=BrownR,ou=HR,ou=London,ou=UK,DC=xidtestco,DC=com
changetype: modify
replace: telephoneNumber
telephoneNumber: 020710105
-

# 10 ID_Vault telephoneNumber:093410114 will overwrite AD2 telephoneNumber:93410114
dn: cn=TaylorR,ou=Engineering,ou=Auckland,ou=NZ,DC=xidtestco,DC=com
changetype: modify
replace: telephoneNumber
telephoneNumber: 093410114
-

# 16 ID_Vault telephoneNumber:020410121 will overwrite AD2 telephoneNumber:20410121
dn: cn=WhiteL,ou=Marketing,ou=Sydney,ou=AU,DC=xidtestco,DC=com
changetype: modify
replace: telephoneNumber
telephoneNumber: 020410121
-

# 19 ID_Vault telephoneNumber:020410126 will overwrite AD2 telephoneNumber:20410126
dn: cn=ClarkK,ou=Call Centre,ou=Sydney,ou=AU,DC=xidtestco,DC=com
changetype: modify
replace: telephoneNumber
telephoneNumber: 020410126
-

# 46 ID_Vault telephoneNumber:020710157 will overwrite AD2 telephoneNumber:20710157
dn: cn=MorrisM,ou=Communication,ou=London,ou=UK,DC=xidtestco,DC=com
changetype: modify
replace: telephoneNumber
telephoneNumber: 020710157
-
```

AD Rollback LDIF:

```
# 1 rollback ID_Vault title:Line Manager will overwrite AD2 title:Line Mgr
dn: cn=SmithJ,ou=HR,ou=Paris,ou=FR,DC=xidtestco,DC=com
changetype: modify
replace: title
title: Line Mgr
-

# 4 rollback ID_Vault telephoneNumber:020710105 will overwrite AD2
telephoneNumber:20710105
dn: cn=BrownR,ou=HR,ou=London,ou=UK,DC=xidtestco,DC=com
changetype: modify
replace: telephoneNumber
telephoneNumber: 20710105
-

# 10 rollback ID_Vault telephoneNumber:093410114 will overwrite AD2
telephoneNumber:93410114
dn: cn=TaylorR,ou=Engineering,ou=Auckland,ou=NZ,DC=xidtestco,DC=com
changetype: modify
replace: telephoneNumber
telephoneNumber: 93410114
-

# 16 rollback ID_Vault telephoneNumber:020410121 will overwrite AD2
telephoneNumber:20410121
dn: cn=WhiteL,ou=Marketing,ou=Sydney,ou=AU,DC=xidtestco,DC=com
changetype: modify
replace: telephoneNumber
telephoneNumber: 20410121
-

# 19 rollback ID_Vault telephoneNumber:020410126 will overwrite AD2
telephoneNumber:20410126
dn: cn=ClarkK,ou=Call Centre,ou=Sydney,ou=AU,DC=xidtestco,DC=com
changetype: modify
replace: telephoneNumber
telephoneNumber: 20410126
-

# 46 rollback ID_Vault telephoneNumber:020710157 will overwrite AD2
telephoneNumber:20710157
dn: cn=MorrisM,ou=Communication,ou=London,ou=UK,DC=xidtestco,DC=com
changetype: modify
replace: telephoneNumber
telephoneNumber: 20710157
-
```

JDBC (Oracle Database):

Rectification Control File: Replace <staging_table_name> with the actual target table name.

```
load data
infile 'XID_Test_Project_1_Ent4_Rect_JDBC2.txt'
append into table <replace_with_Staging_Table_Name>
fields terminated by ";" optionally enclosed by '"'
trailing NULLCOLS
(
"EmployeeNumber";"LoginName";"FirstName";"LastName";"Location";"Department";"Title"
;"EmailAddress";"PhoneNumber";"Mobile";"AccountStatus" )
```

JDBC Rectification Data File:

```
"10000065";"ReedM";"Martha";"Reed";"Hong
Kong";"Marketing";"Manager";"Martha.Reedy@xidtestco.com";"952710166";"852720167";""
```

Rectification Control File rollback: Replace <staging_table_name> with the actual target table name.

```
load data
infile 'XID_Test_Project_1_Ent4_Rect_Rollback_JDBC2.txt'
append into table <replace_with_Staging_Table_Name>
fields terminated by ";" optionally enclosed by '"'
trailing NULLCOLS
(
"EmployeeNumber";"LoginName";"FirstName";"LastName";"Location";"Department";"Title"
;"EmailAddress";"PhoneNumber";"Mobile";"AccountStatus" )
```

JDBC Rectification Data Rollback File:

```
"10000065";"ReedM";"Martha";"Reed";"Hong
Kong";"Marketing";"Manager";"Martha.Reed@xidtestco.com";"952710166";"852720167";""
```

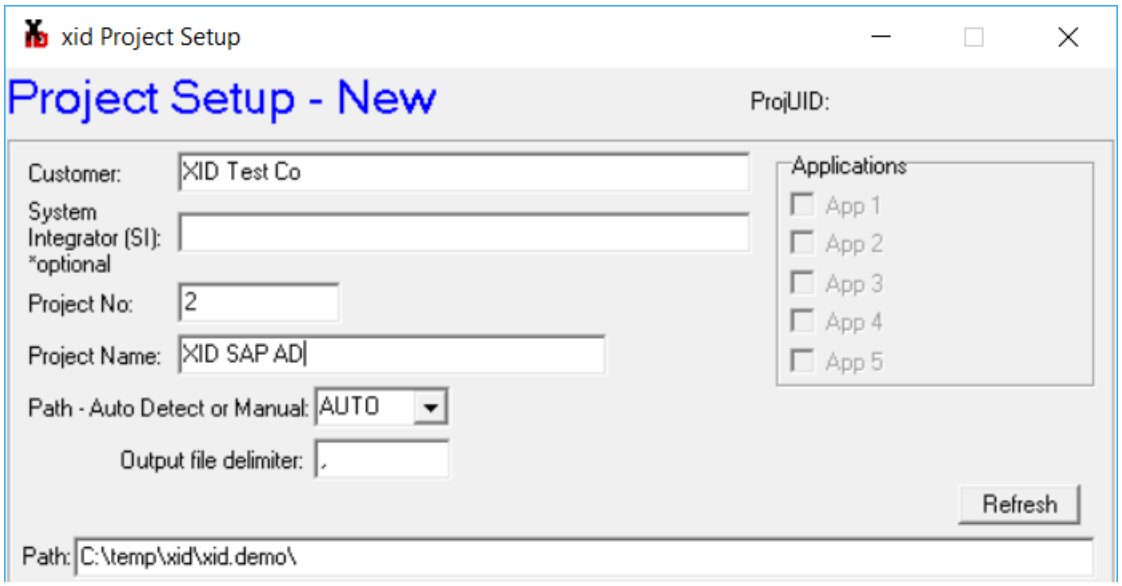
New Project Workshop

The following is a guide for setting up a new project in XID. The new project will comprise a SAP application at the core (primary/ID Vault) with Active Directory (AD) as the second application.

The following process uses the sample XID data. For this workshop it is recommended to use the same names as used in the documentation.

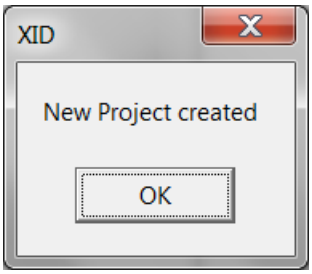
Create New Project

1. Run XID: **`xid.exe`**
2. Click the 'File' menu and select 'New'.
3. Click 'Yes' if prompted to clear the current project.
4. The 'Customer' (mandatory) is the name of the company who is undertaking the XID project.
5. The 'System Integrator (SI)' (optional) is the name of the SI or 3rd party performing the work for the customer.
6. The 'Project No' (number) and 'Project Name' (both mandatory) should reflect the project but can be any value set by the user. Avoid leading/trailing spaces and using more than a single space between words. Once these values are set they cannot be changed once the project has been created.



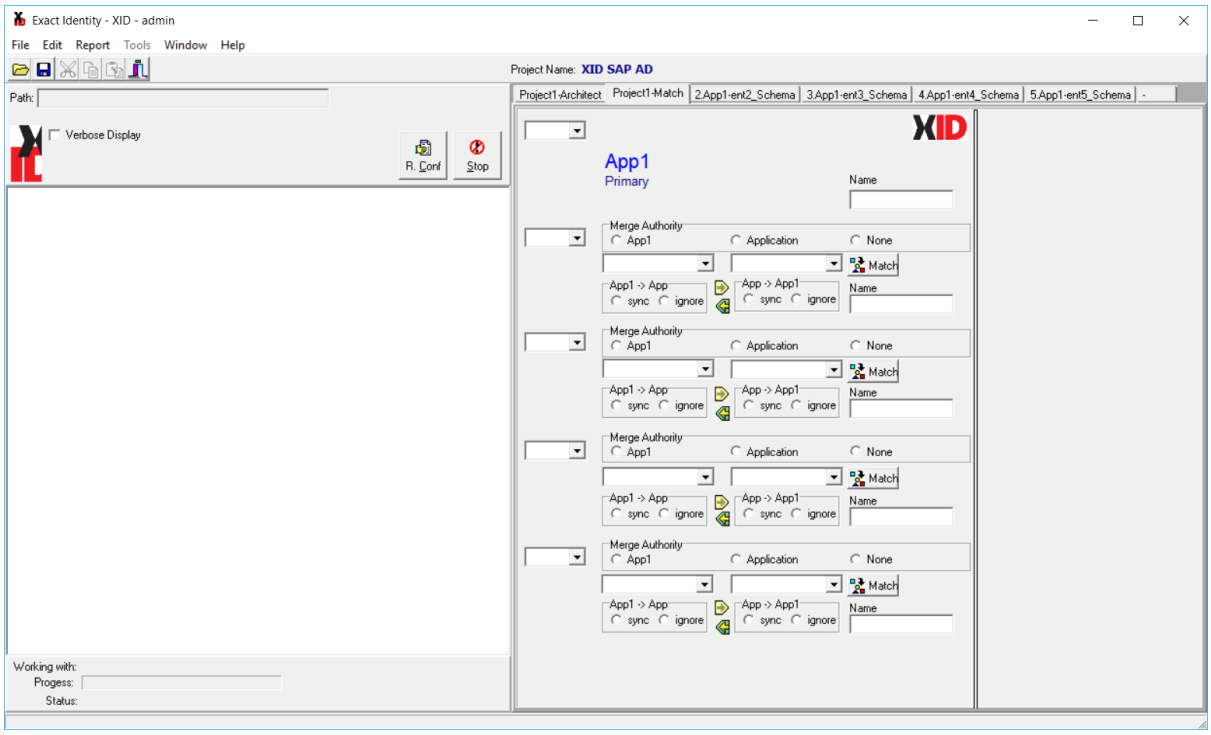
7. Path detection is automatic and is the location where XID is run from. The value should not be changed.
8. Do not change the 'Path' setting from 'AUTO' unless the data files have been separated from the executable program.
9. If required, change the 'Output file delimiter' from the default comma to the 'Windows List Separator' defined by the Windows Operating system running XID. If the delimiter is 'tab' then enter '#9' without the quotes.

10. Click ‘OK’ then click ‘OK’ again to close the ‘New Project created’ message box.

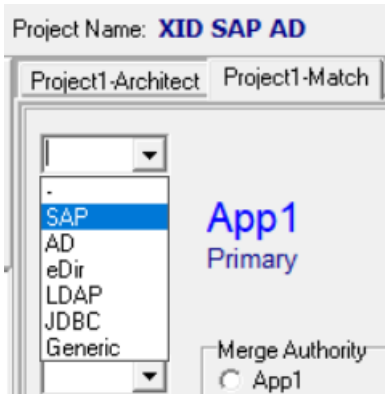


Create New Applications

1. Click the ‘Project1-Match’ tab.

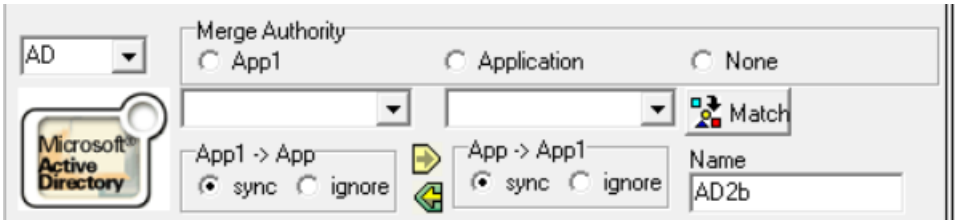


2. The first application position denotes application 1 or the ID Vault if it exists. For this project SAP is the primary application. From the application combo box select ‘SAP’.



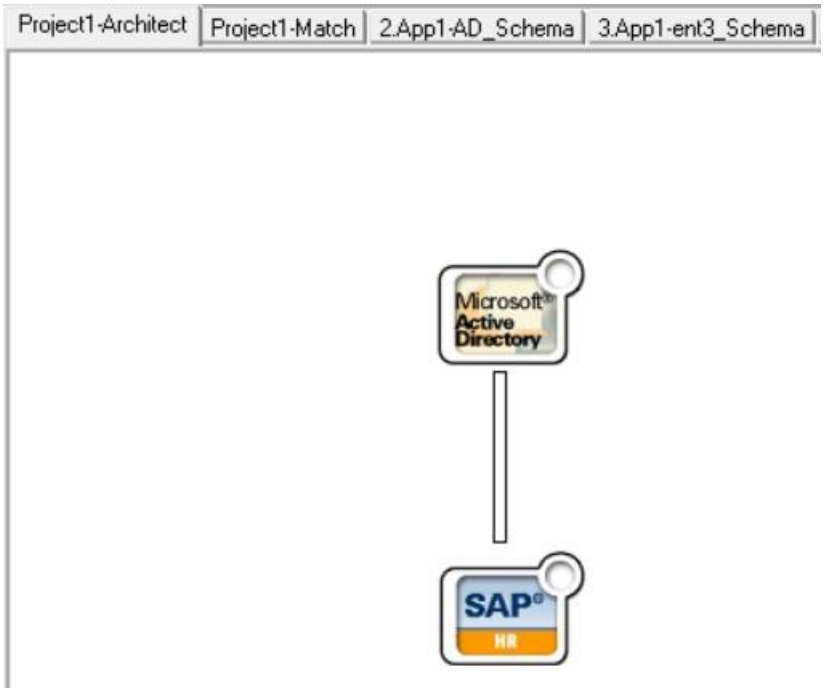
3. Enter a name for the application. Avoid using spaces for the application name if possible. This example uses ‘SAP2b’ for the application name.

4. Select ‘AD’ from the application combo box in the second application position.
5. Enter a name for the application. The name ‘AD2b’ for the application name.



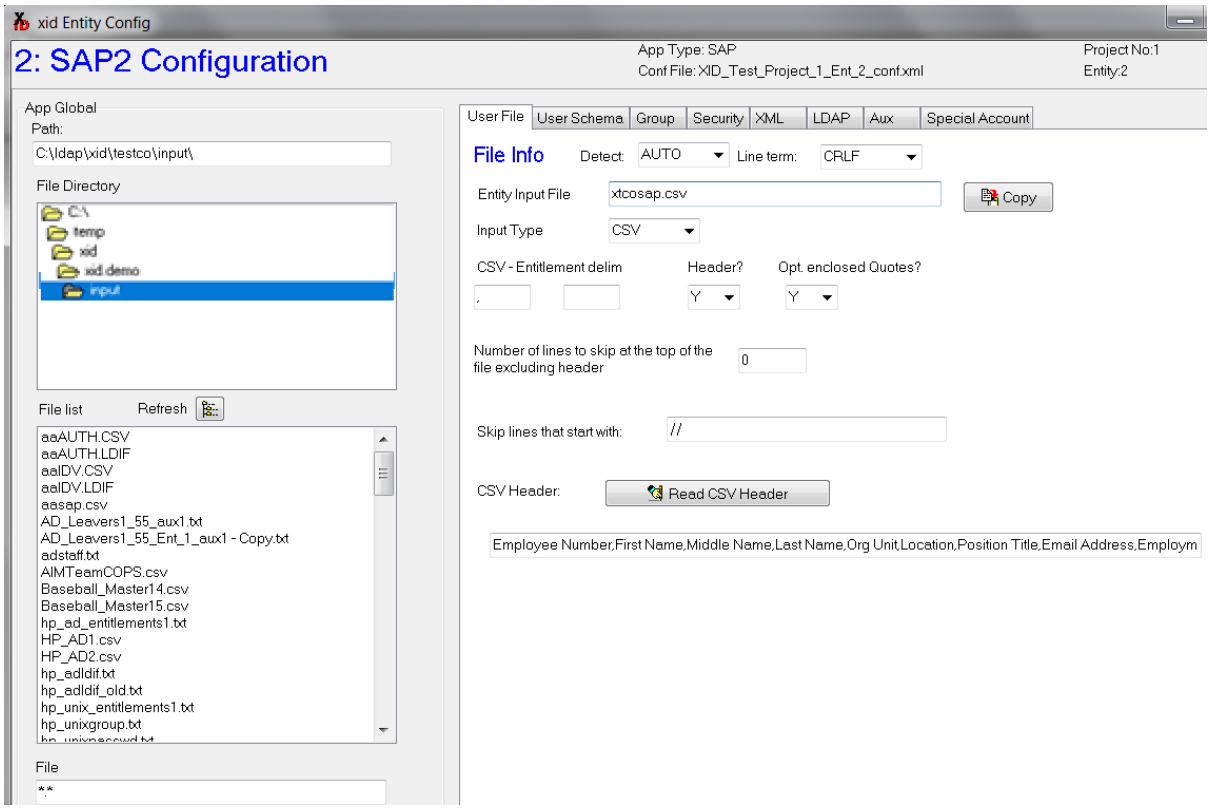
6. Click ‘sync’ in the AD Subscribe box.
7. Click ‘sync’ in the AD Publish box.
8. Save the Project by clicking the ‘Save’ icon  or by clicking ‘File’ then selecting ‘Save’.
9. Click ‘OK’ to close the save confirmation box.
    - Note that the project application is only partly created and the application file information must be completed as per the ‘Application Configuration’ section.

10. Click the ‘Project1-Architect’ tab. The applications should be displayed as follows.



Application Configuration: SAP

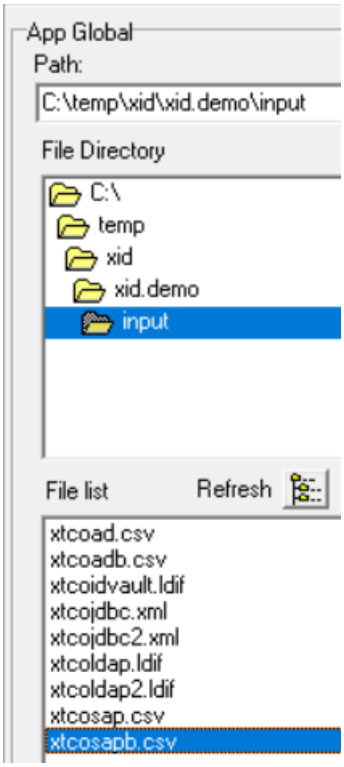
1. Load SAP application configuration by clicking the ‘SAP’ icon in ‘Project1-Match’. For a new configuration the 'User File' tab is selected. Once the information on this tab is completed then the 'User Schema' will be the landing tab.



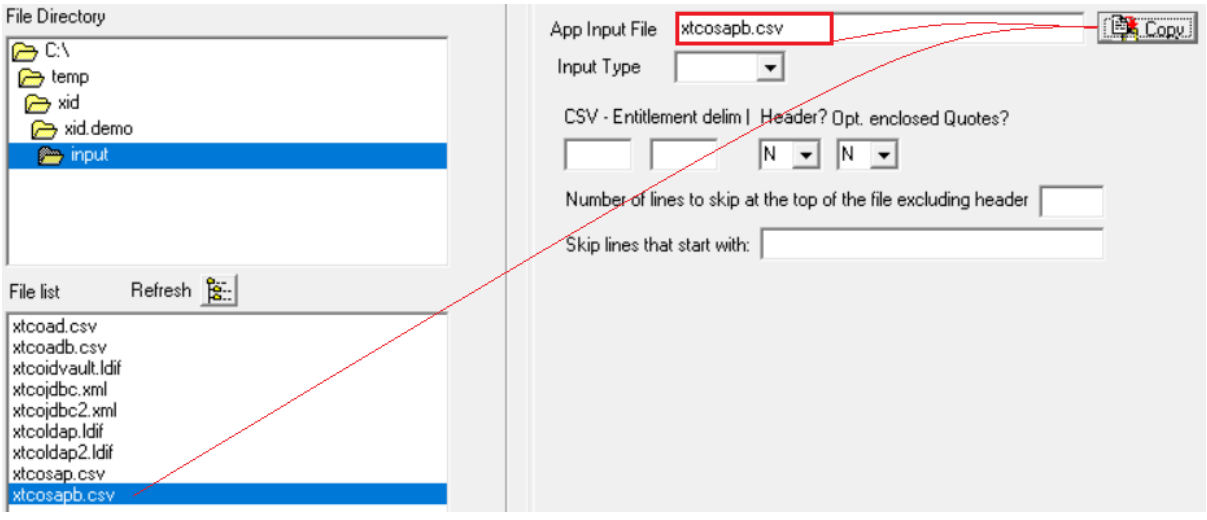
File Info

1. Change ‘Detect’ to ‘AUTO’. This setting will use the XID file detection process.
2. Select ‘CRLF’ for ‘Line term’. For Windows systems ‘Carriage Return Line Feed’ is used for terminating text file lines. Text files sourced from Unix/Linux systems can be Line Feed ‘LF’ only. Select ‘LF’ if this is the line termination character.

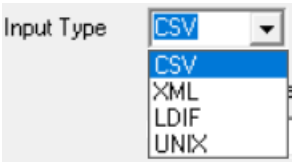
3. Select the SAP input file extracted for this project in the ‘File list’ box. For this example the file is ‘xtcosapb.csv’ and represents a data extract from SAP. The File Directory should be set to the 'input' folder from where XID was executed.



4. Click the ‘Copy’ button to populate the ‘App Input File’ edit box.

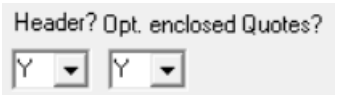


5. Select the extract file type from the ‘Input Type’ drop down box. The sample SAP extraction file is of type ‘CSV’.



6. Enter the CSV delimiter that is used in the application input file. The sample SAP extraction uses a comma as the CSV delimiter. Enter the comma character ‘,’ (without the quotes) in the ‘CSV delim’ edit box. If the delimiter is 'tab' then enter '#9' without the quotes.
7. If entitlements (such as groups for example) are included in the row then enter the entitlement delimiter. Set this to semi-colon for this example.

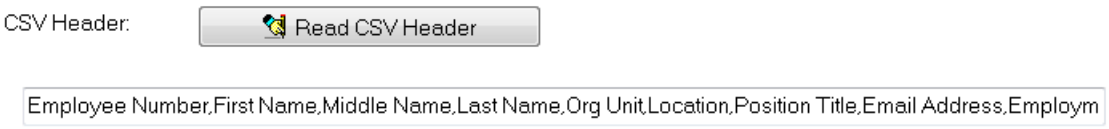
8. If the extraction CSV file has a header row then select ‘Y’ from the ‘Header Row?’ combo box. The sample SAP extraction file uses a header row therefore ‘Y’ should be selected for this sample.



9. If the CSV attributes use enclosed quotes then select ‘Y’ from the ‘Opt. enclosed Quotes?’ combo box. Select ‘Y’ for this sample application.
10. If the file contains initials rows that are to be excluded at the beginning of the file then enter the number of lines to skip. Enter the number of rows to skip but do not count the header row if this exists.

11. If there are lines to skip that are identified by a pattern at the beginning of the row then enter this pattern in the edit box 'Skip lines that start with:'.

12. For a CSV file, the CSV header can be read by clicking 'Read CSV Header'.



13. The CSV results are displayed in the edit box. A prompt is displayed requesting if the schema is to be created or recreated based on the CSV header. Caution this will overwrite an existing schema if it already exists. If the original schema is to be preserved, click 'No' to prevent the overwrite. Click 'Yes' to create a new schema. The new schema is created but needs to be edited to assign the correct, UID, GN (Given Name) and SN (Surname) as a minimum.

SAP CSV Schema

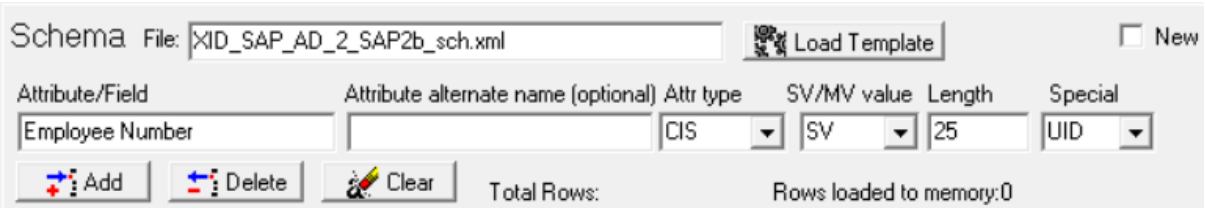
A default schema file will be created based on the application name with a '_sch.xml' suffix. The schema file name can be changed and alternatively an existing template schema file can be loaded. Loading a template will be discussed later in this section. The following will demonstrate creating a new schema from the CSV extract.

1. Click on the 'User Schema' tab.

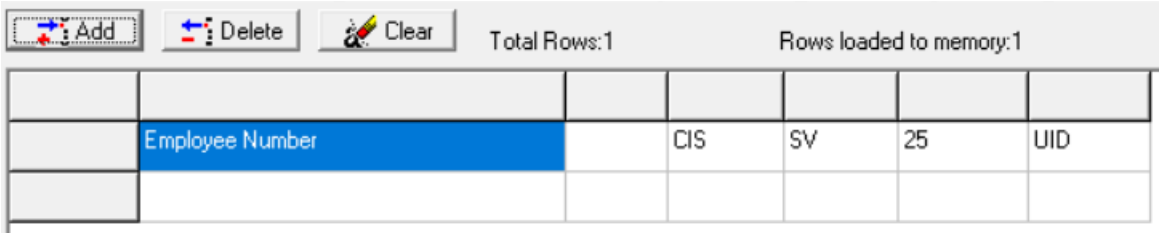
2. The attribute list must follow the CSV attribute order. If there is a header row then it is advised to name the attributes the same as those in the header. The following are the first two rows of the sample SAP extract file. Note that the lines wrap in this document.

```
"Employee Number","First Name","Middle Name","Last Name","Org
Unit","Location","Position Title","Email Address","Employment
Status","TEL_NUMBER","MOB_NUMBER"
"10000001","James","null","Smith","HR","Paris","Area
Manager","James.Smith@xidtestco.com","Active","33110102","33120103"
```

   - The first attribute is 'Employee Number' which will be entered into the schema first.
   - Enter 'Employee Number' into the 'Attribute' edit box.
   - The 'Attribute alternate name' is optional. This is for LDAP schema types that can have naming for LDAP compliance in addition to proprietary naming. Ignore the alternate name.
   - The 'Attr type' provides alternate selections for LDAP schemas. For SAP the value will be set to 'CIS' which is case ignore string. Alternatively the value could be set to 'Number' if it was sure that all of the values for the attribute were strictly numeric.
   - Select 'SV' to indicate the attribute is single valued.
   - The Length value indicates the maximum number of characters for the attribute.
   - Special: The special selection denotes attribute significance to XID. As XID cannot assume significance of the attribute then this must be bestowed. The appendix has the full description for all of the combo box items. The 'Employee Number' is the unique value that will be used for primary matching to other applications. Select 'UID' from the Special combo box.
   - *The appendix has a list of the expanded values for the combo boxes.*

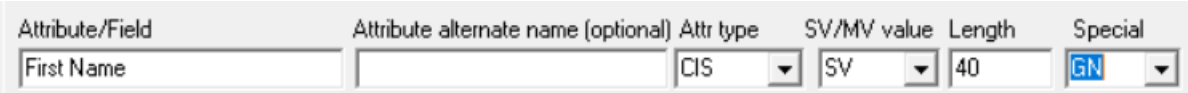


3. Click the ‘Add’ button. The value is populated in the schema list.



- A blank row is intentionally added below the last attribute in the schema.

4. The next attribute in the CSV extract is ‘First Name’.
   - Enter ‘First Name’ in the ‘Attribute’ edit box.
   - Set the ‘Attr type’ to ‘CIS’.
   - Set the ‘Single/Multi Valued’ to ‘SV’.
   - Set the ‘Length’ to the character length value for the First Name. For this example the value is ‘40’.
   - Set the ‘Special’ value to ‘GN’.



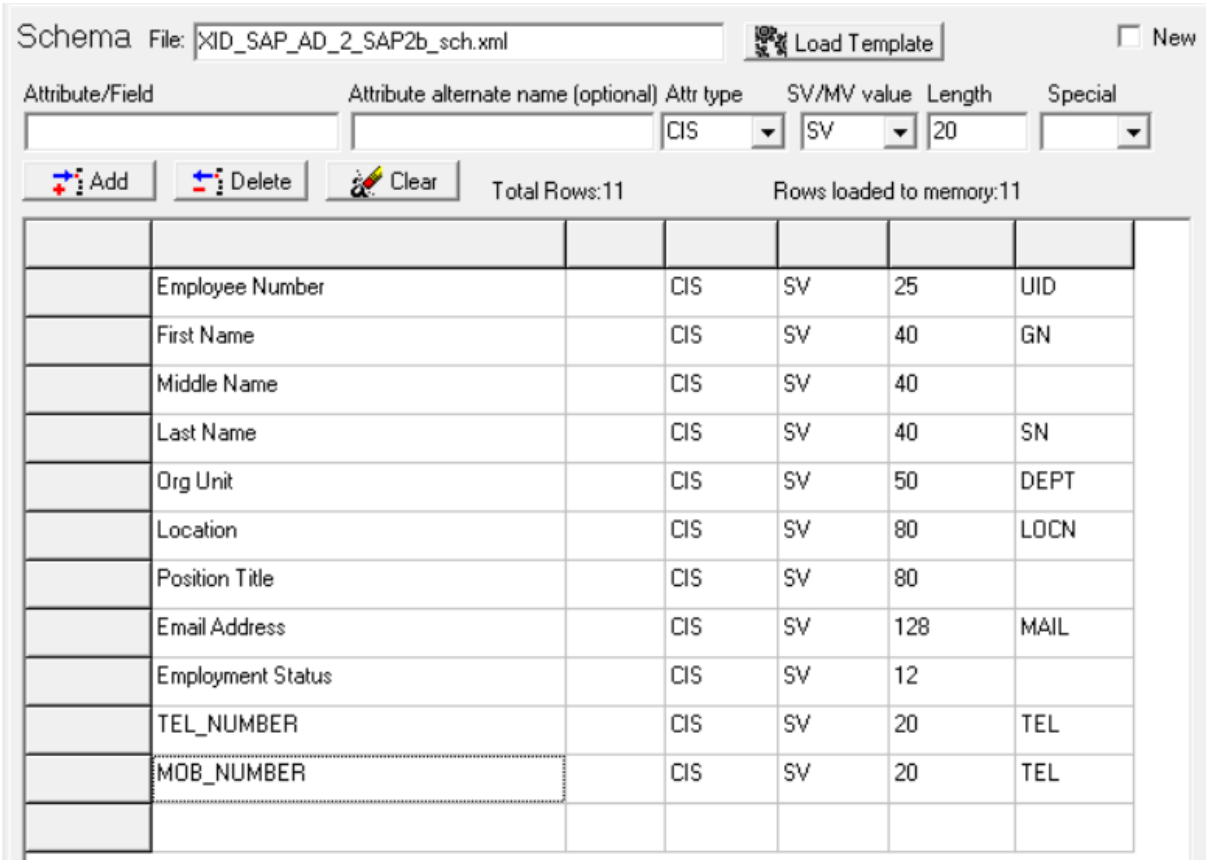
5. Click ‘Add’ to add First Name to the schema.
6. The next attribute in the CSV extract is ‘Middle Name’.
   - Enter ‘Middle Name’ in the ‘Attribute’ edit box.
   - Set the ‘Attr type’ to ‘CIS’.
   - Set the ‘Single/Multi Valued’ to ‘SV’.
   - Set the ‘Length’ to the character length value for the First Name. For this example the value is ‘40’.
   - Click ‘Add’.

7. The next attribute in the CSV extract is ‘Last Name’.
   - Enter ‘Last Name’ in the ‘Attribute’ edit box.
   - Set the ‘Attr type’ to ‘CIS’.
   - Set the ‘Single/Multi Valued’ to ‘SV’.
   - Set the ‘Length’ to the character length value for the First Name. For this example the value is ‘40’.
   - Set the ‘Special’ value to ‘SN’.
   - Click ‘Add’.

8. Repeat the action as per the previous step for the remaining attributes in the following table:

Attribute	Attr type	Single/Multi valued	Length	Special
Employee Number	CIS	SV	25	UID
First Name	CIS	SV	40	GN
Middle Name	CIS	SV	40	
Last Name	CIS	SV	40	SN
Org Unit	CIS	SV	50	DEPT
Location	CIS	SV	80	LOCN
Position Title	CIS	SV	80	
Email Address	CIS	SV	128	MAIL
Employment Status	CIS	SV	12	
TEL_NUMBER	CIS	SV	20	TEL
MOB_NUMBER	CIS	SV	20	TEL

9. The resultant schema will look in XID as follows:



Schema table editing

Edit Cell

Changes can be made to the schema table. Click into a cell of the schema table that requires update. Use the up|down|left|right arrow keys if required to access the cell to be updated.

Click the cell an additional time to change the cell mode to edit and change the value as required. Press Enter to action the update.

Change Special information

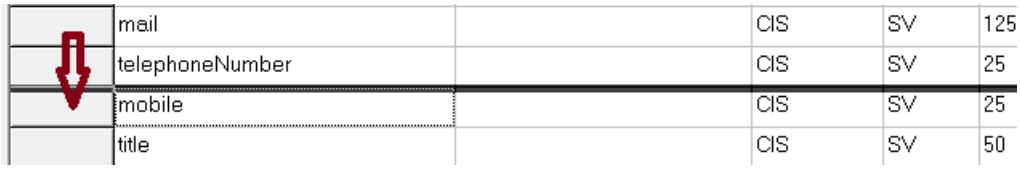
If a cell requires information to be changed in the 'Special' column then access the special cell and change the cell mode to edit. Delete or Add information as required. If adding special information ensure the text matches the value from the Special combo box without leading or trailing spaces.

It is easier to double click the row to edit the information in the edit window. The edit row function is shown below.

Move Row

XID schema row order must match the CSV extract files. If the CSV changes or if a row was defined at an incorrect location then the row can be moved.

Click the shaded cell to the left of the 'Attribute' cell and drag the row up or down to the correct location. The following shows the 'mobile' attribute being moved LDAP application.

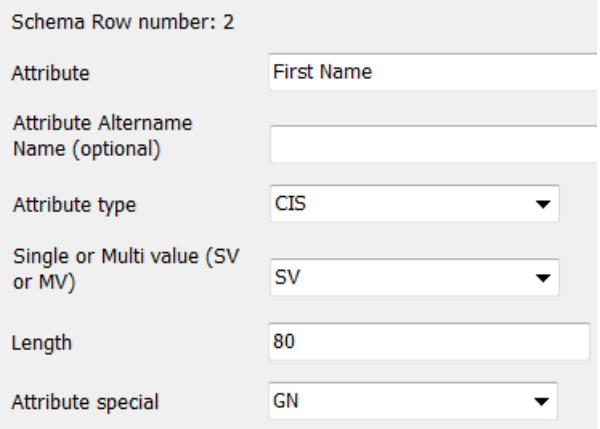


Delete Row

Click into the row to be deleted and click the 'Delete' button above the schema table.

Edit Row

Double click a row to open the edit schema row window.

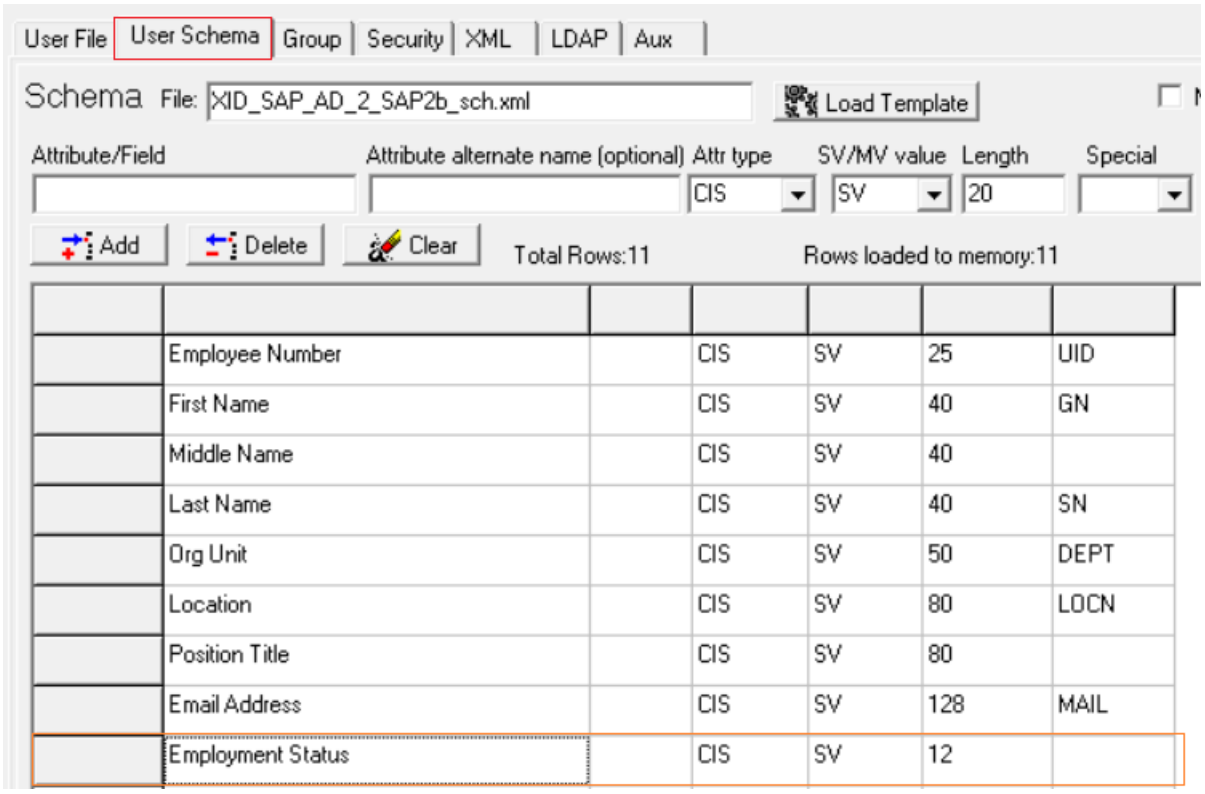


Make changes to the schema entry then click 'OK' to save or 'Cancel' to abort

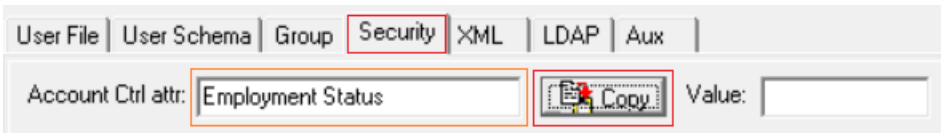
Account Control

The optional account control attribute defines the attribute used to determine if an account is active. The value specified is for the account enabled state. The following will set the account enabled information for the sample SAP application.

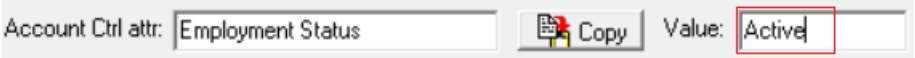
1. Remain in the 'User Schema' tab or click the 'User Schema' tab to return.
2. Click and highlight the attribute in the schema table used for account control. For this example, the SAP attribute is ‘Employment Status’.



3. Click the 'Security' tab.
4. Click the ‘Copy’ button to populate the ‘Account Ctrl attr:’ edit box with the account control attribute selected in the schema.



5. Enter the value used to determine the value that determines that the account is active. In this sample the value is ‘Active’.

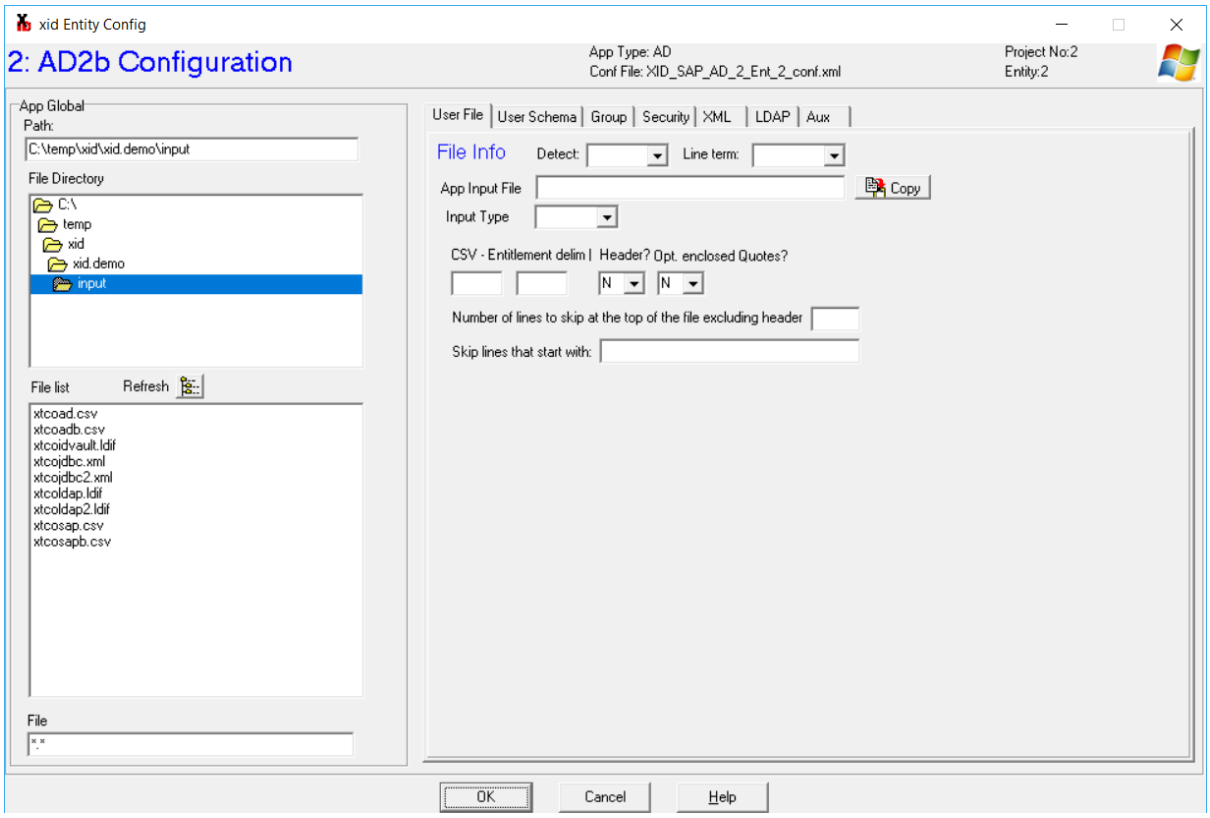


Save Application

1. Click ‘OK’ to save the application selection. At this stage the information is saved to a memory cache and will not be committed to disk until the project is saved.
2. Save the Project by clicking the ‘Save’ icon  or by clicking ‘File’ then selecting ‘Save’.
3. Click ‘OK’ to close the save confirmation box.

Application Configuration: AD

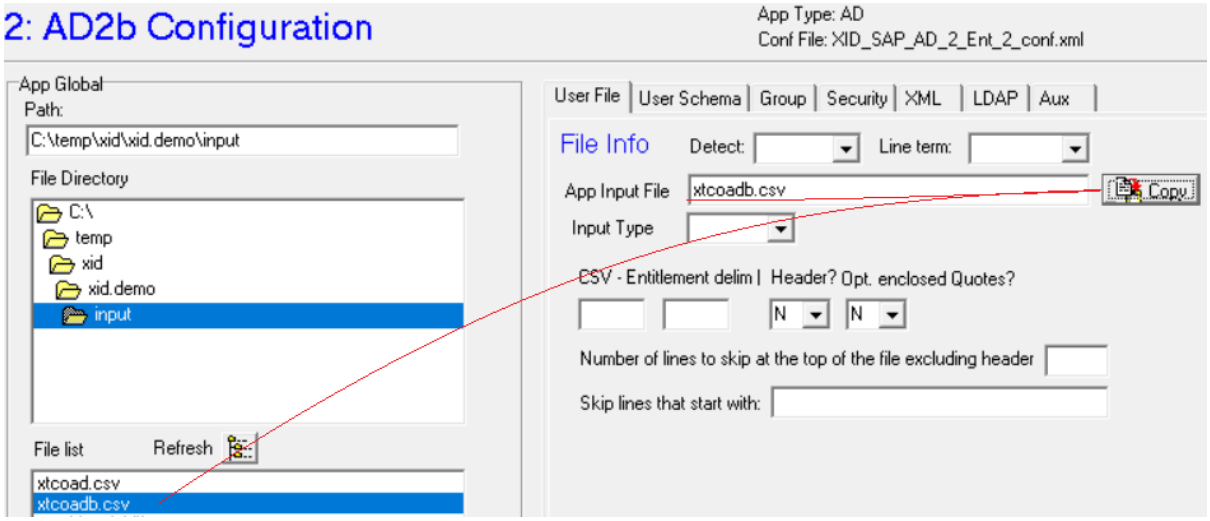
1. Load AD application configuration by clicking the ‘AD’ icon in ‘Project1-Match’.



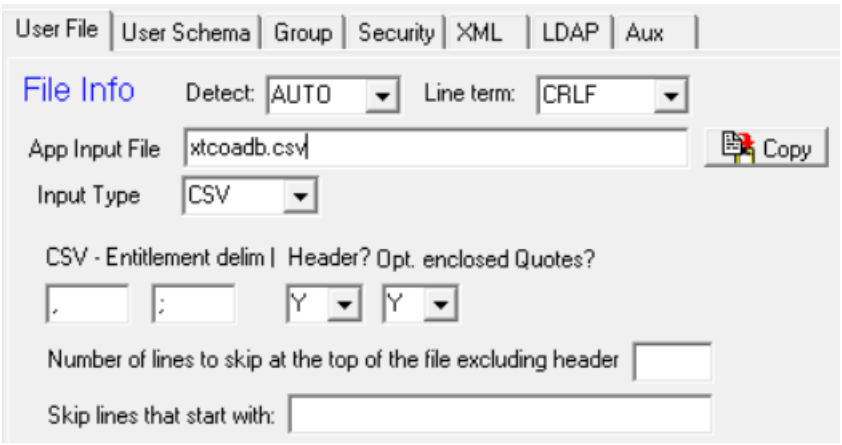
File Info

1. Set ‘Detect’ to ‘AUTO’. This setting will use the XID file detection process.
2. Select ‘CRLF’ for ‘Line term’. For Windows systems ‘Carriage Return Line Feed’ is used for terminating text file lines. Text files sourced from Unix/Linux systems can be Line Feed ‘LF’ only. Select ‘LF’ if this is the line termination character.
3. Select the AD input file extracted for this project in the ‘File list’ box. For this example the file is ‘xtcoadb.csv’ and represents a data extract from AD. The File Directory should be set to the 'input' folder where XID was executed.

4. Click the ‘Copy’ button to populate the ‘App Input File’ edit box.



5. Select the extract file type from the ‘Input Type’ drop down box. The sample AD extraction file is of type ‘CSV’.
6. Enter the CSV delimiter that is used in the application input file. The sample AD extraction uses a comma as the CSV delimiter. Enter the comma character ‘,’ (without the quotes) in the ‘CSV delim’ edit box. If the delimiter is 'tab' then enter '#9' without the quotes.
7. If entitlements (such as groups for example) are included in the row then enter the entitlement delimiter. Set this to semi-colon for this example.
8. If the extraction CSV file has a header row then select ‘Y’ from the ‘Header Row?’ combo box. The sample AD extraction file uses a header row therefore ‘Y’ should be selected for this sample.
9. If the CSV attributes use enclosed quotes then select ‘Y’ from the ‘Opt. enclosed Quotes?’ combo box. Select ‘Y’ for this sample application.
10. If the file contains initials rows that are to be excluded at the beginning of the file then enter the number of lines to skip. Enter the number of rows to skip but do not count the header row if this exists.
11. If there are lines to skip that are identified by a pattern at the beginning of the row then enter this pattern in the edit box 'Skip lines that start with:'.



AD CSV Schema

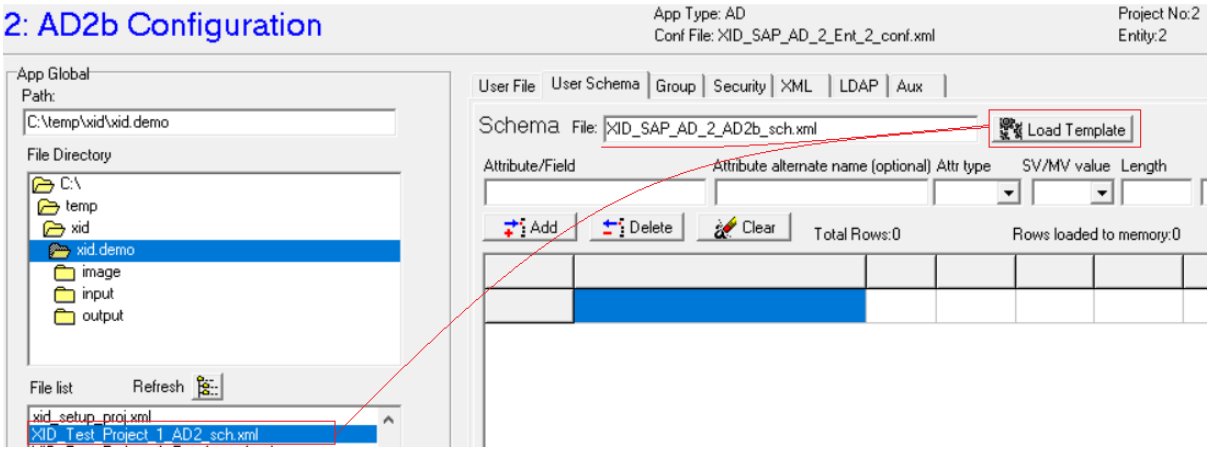
A default schema file will be created based on the application name with a '_sch.xml' suffix. The schema file name can be changed and alternatively an existing template schema file can be loaded.

⇨ It is recommended to use the template method to load the AD schema. Once the template is loaded return to complete the 'Account Control' section in this chapter skipping the subsequent steps.

Template Method: See the 'Schema Templates' section further on in this manual if required.

The following example will demonstrate the use of templates using an Active Directory (AD) application and will use the same information from the training workshop. The templates used in this example are those shipped with XID.

1. Click the 'User Schema' tab.
2. Scroll to the top of the 'File list' scroll box and locate the schema files for AD. The files will end with '_sch.xml'. The 'XID_Test_Project_1_AD2_sch.xml' template file contains the AD schema shipped with XID which is a good base schema for the AD workshop application. Note that this could be any previously created schema file.
3. Select 'XID_Test_Project_1_AD2_sch.xml' in the File list box.



4. Click 'Load Template' load the schema.

Manual Schema creation

Skip this section if the template method has been used and go to 'Account Control'.

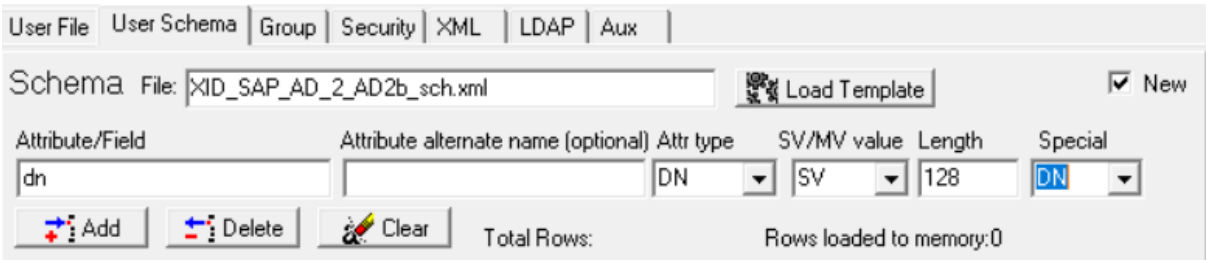
The following details the manual schema creation excluding the template usage.

1. Click the 'User Schema' tab.
2. The attribute list must follow the CSV attribute order. If there is a header row then it is advised to name the attribute names the same as those in the header. The following are the first two rows of the sample AD extract file. Note that the lines wrap in this document.

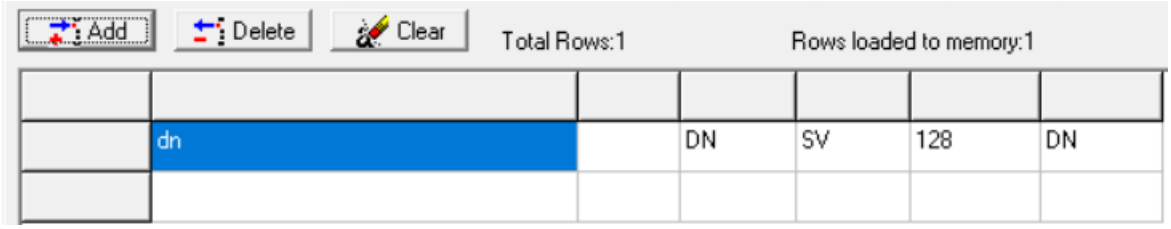
```
dn,sAMAccountName,sAMAccountType,givenName,middleName,sn,displayName,initial
s,manager,employeeID,employeeNumber,l,title,Department,mail,userPrincipalNam
e,telephoneNumber,mobile,cn,name,userAccountControl,lastLogon,lastLogonTimes
tamp,homeDirectory,profilePath
"cn=SmithJ,ou=HR,ou=Paris,ou=FR,DC=xidtestco,DC=com",SmithJ,805306368,James,
null,Smith,James Smith,null,null,10000001,10000001,Paris,Line
Mgr,HR,James.Smith@xidtestco.com,James.Smith@xidtestco.com,33110102,33120103
,SmithJ,SmithJ,514,null,null,\\xidtestcoParis\userdata$\SmithJ,\\xidtestcoPa
ris\profiles$\SmithJ
```

- The first attribute is ‘dn’ which will be entered into the schema first.
- Enter ‘dn’ into the ‘Attribute’ edit box.
- The ‘Attribute alternate name’ is optional. This is for LDAP schema types that can have naming for LDAP compliance in addition to proprietary naming. Ignore the alternate name.
- The ‘Attr type’ provides alternate selections for LDAP schemas. For AD the value will be set to ‘DN’ which is ‘Distinguished Name’.
- Select ‘SV’ to indicate the attribute is single valued.
- The Length value indicates the maximum number of characters for the attribute. Set the value to ‘128’ for this example.
- Special: The special selection denotes attribute significance to XID. As XID cannot assume significance of the attribute or field then this must be bestowed. The appendix has the full description for all of the combo box items. The ‘dn’ is significant as the LDAP object is referenced by its distinguished name (DN). Select ‘DN’ from the Special combo box.
- *The appendix has a list of the expanded values for the combo boxes.*

3. Once the details have been entered, click the ‘Add’ button. The value is populated in the schema list.

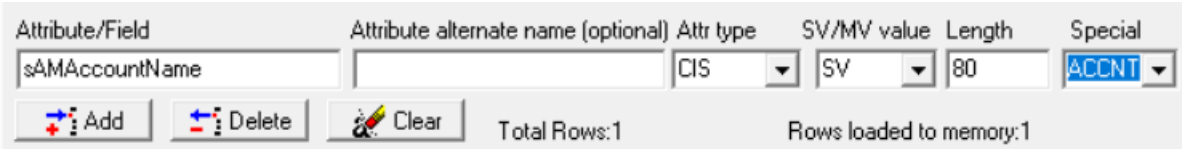


The attribute row is added. Note that a blank row is intentionally added below the last attribute in the schema.



The next attribute in the CSV extract is ‘sAMAccountName’.

- Enter ‘sAMAccountName’ in the ‘Attribute’ edit box.
- Set the ‘Attr type’ to ‘CIS’ (Case Ignore String).
- Set ‘Single/Multi Valued’ to ‘SV’.
- Set the ‘Length’ to the character length value for the First Name. For this example the value is ‘80’.
- Set the ‘Special’ value to ‘ACCNT’. This indicates to XID that this attribute is the account name specifier.

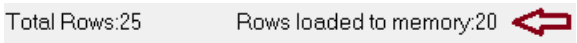


4. Click ‘Add’ to add sAMAccountName to the schema.

5. Repeat the action as per the previous step for the remaining attribute in the following table: Note that 'l' is the lowercase letter 'L' as in location.

Attribute	Attr type	Single/Multi valued	Length	Special
dn	DN	SV	128	DN
sAMAccountName	CIS	SV	80	ACCNT
sAMAccountType	CIS	SV	20	
givenName	CIS	SV	40	GN
middleName	CIS	SV	40	
sn	CIS	SV	40	SN
displayName	CIS	SV	80	
Initials	CIS	SV	12	X
manager	CIS	SV	80	
employeeID	CIS	SV	25	UID
employeeNumber	CIS	SV	12	
l	CIS	SV	50	LOCN
Title	CIS	SV	50	
department	CIS	SV	40	DEPT
mail	CIS	SV	125	MAIL
userPrincipalName	CIS	SV	125	
telephoneNumber	CIS	SV	25	TEL
mobile	CIS	SV	25	TEL
cn	CIS	SV	80	
name	CIS	SV	80	
userAccountControl	CIS	SV	25	
lastLogon	CIS	SV	25	X
lastLogonTimestamp	CIS	SV	25	X
homeDirectory	CIS	SV	125	X
profilePath	CIS	SV	125	X

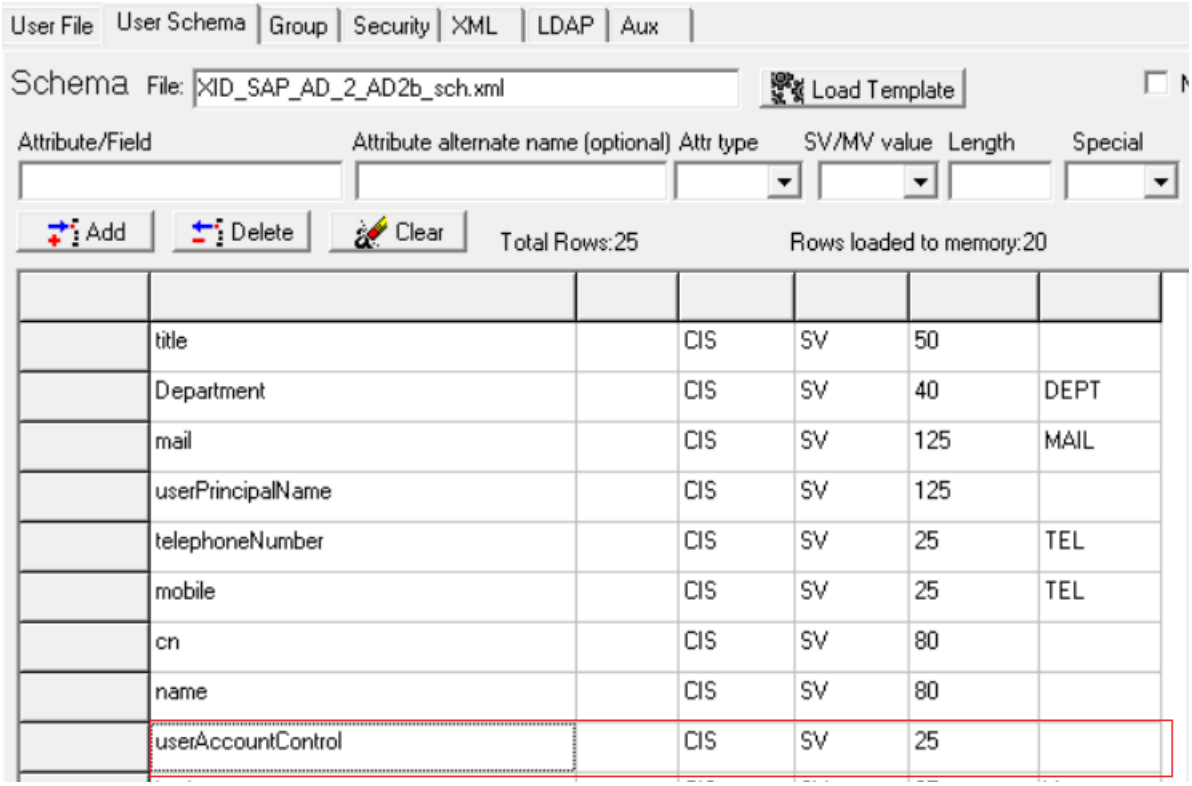
The 'Rows loaded to memory' must not exceed 20 attributes/fields. Total rows are limited to 50. An 'X' in the Special cell excludes attributes/fields from memory.



Account Control

The optional account control attribute defines the attribute used to determine if an account is active. The value specified is for the account enabled state. The following will set the account enabled information for the sample AD application.

1. Remain in the 'User Schema' tab or click the 'User Schema' tab to return.



2. Click and highlight the attribute in the schema table used for account control. For the sample AD this attribute is ‘userAccountControl’.
3. Click the 'Security' tab.
4. Click the ‘Copy’ button to populate the ‘Account Ctrl attr:’ edit box with the account control attribute selected in the schema.

5. Enter the value used to determine the value that determines that the account is active. In this sample the value is ‘512’.

Save Application

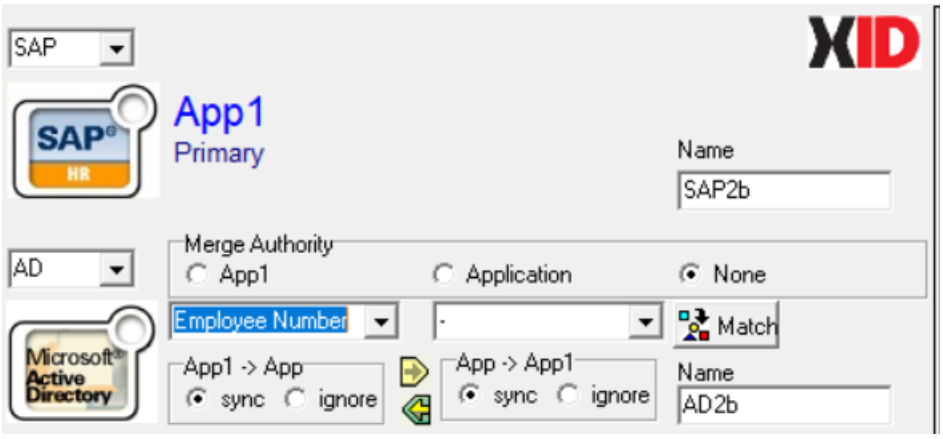
1. Click ‘OK’ to save the application selection. At this stage the information is saved to a memory cache and will not be committed to disk until the project is saved.
2. Save the Project by clicking the ‘Save’ icon  or by clicking ‘File’ then selecting ‘Save’.
3. Click ‘OK’ to close the save confirmation box.

AD Matching Rules

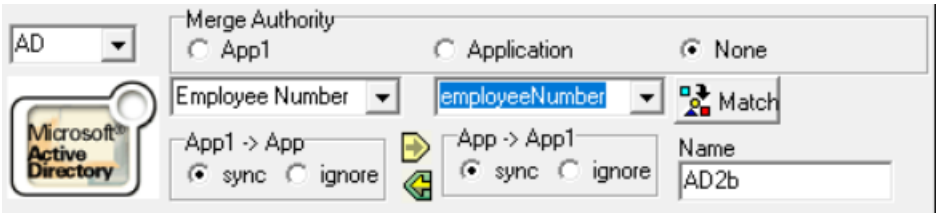
The matching rules will be set at the second application. The first application or ID Vault does not require the matching rule set.

The matching combo boxes are populated with the information from the application schema. The left combo box is the primary application 1 or ID Vault. The right combo box is the application represented by the application position.

1. Select the 'Project1-Match' tab.
2. Click the left combo box on application 2 which is the AD application AD2b.



3. Select the application 1 attribute used for matching. For SAP (application 1) select 'Employee Number'.
4. Click the right combo box and select the application 2 matching attribute. For AD (application 2) select 'employeeID'.



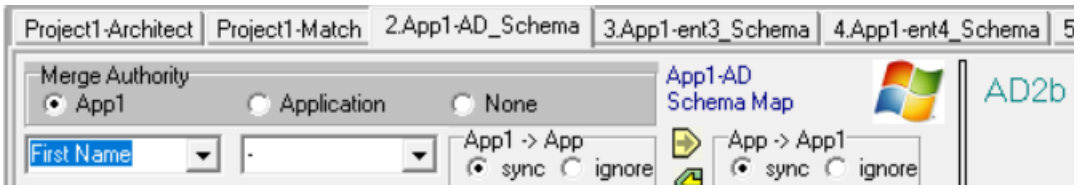
5. Save the Project by clicking the 'Save' icon  or by clicking 'File' then selecting 'Save'.
6. Click 'OK' to close the save confirmation box.

AD Business Rules

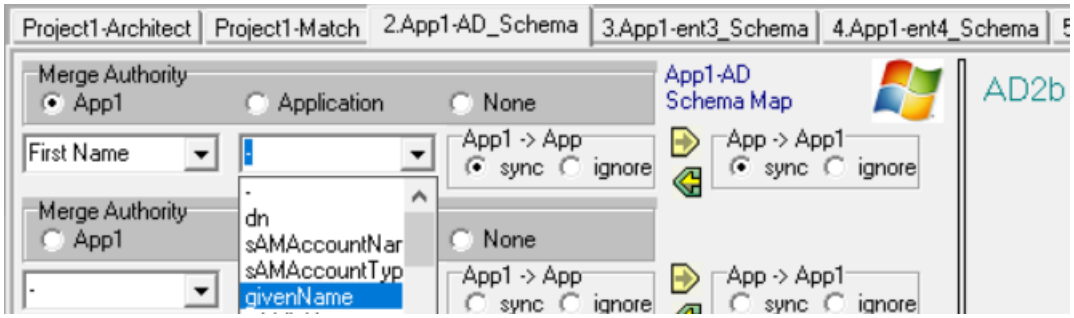
The business rules section allows comparison of applications at an attribute level. Although 50 items can be added to the schema, there is a limit of 30 business rules that can be defined. Not all of the attributes need to be added and it is recommended to compare only relevant attributes for this analysis phase.

The business rule combo boxes are populated with the information from the application schema. The left combo box is application 1 or the ID Vault (IDV). The right combo box is the application represented by the tab selected. This is also referred to as the Application.

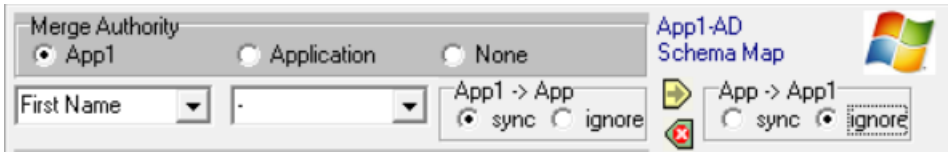
1. Click the '2. App1-AD_Schema' tab.
2. Click the left combo box which contains the schema for application 1 or the ID Vault. Select the 'First Name' attribute from SAP.



3. Click the right combo box which contains the schema for application 2. Select the 'givenName' attribute from AD.



4. For this example SAP 'First Name' is authoritative for this attribute. AD will subscribe from changes from SAP but SAP will ignore changes from AD. Set this rule scenario as follows:
   - Click 'sync' in 'App1 -> App' (Subscribe) to allow data from application 1 (SAP) to application 2 (AD).
   - Click 'ignore' in 'App -> App1' (Publish) to block data from application 2 (AD) to application 1 (SAP).



5. Set the global merge authority to be ‘App1’ by clicking ‘App1’ in ‘Merge Authority’. In the absence of a defined 'sync'/'ignore' (‘Subscribe’/’Publish’) rule the merge authority will arbitrate to determine which application is authoritative. The merge authority will also determine authority if both attribute authoritative (‘Subscribe’ and ‘Publish’) rules are set to ‘sync’.
6. Repeat the previous steps to add attributes as per the following table. When ‘TEL_NUMBER’ is entered click ‘PgDn’ to continue entering rules on the next page. ‘PgUp’ will return the focus to the first page of schema mappings.

Application 1 (IDV)	**Application 2** (Application)	**Subscribe** Application 1 to Application 2	**Publish** Application 2 to Application 1	**Merge Authority**
First Name	**givenName**	sync	ignore	App1
Middle Name	**middleName**	sync	ignore	App1
Last Name	**sn**	sync	ignore	App1
Org Unit	**Department**	sync	ignore	App1
Location	**l**	sync	ignore	App1
Position Title	**title**	sync	ignore	App1
Email Address	**mail**	ignore	sync	Application
TEL_NUMBER	**telephoneNumber**	sync	sync	App1
MOB_NUMBER	**mobile**	sync	sync	App1

Page 1 of the schema map should look as follows:

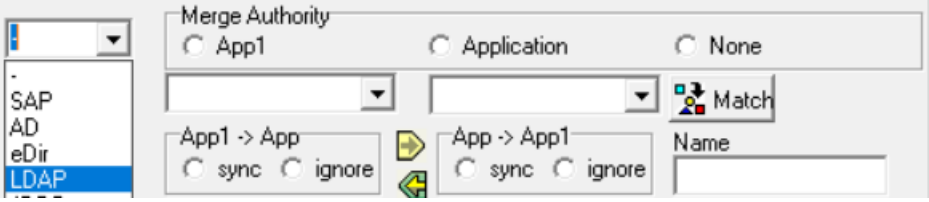
7. Save the Project by clicking the 'Save' icon  or by clicking 'File' then selecting 'Save'. Click 'OK' to close the dialog box.

New Project Additional Application: LDAP

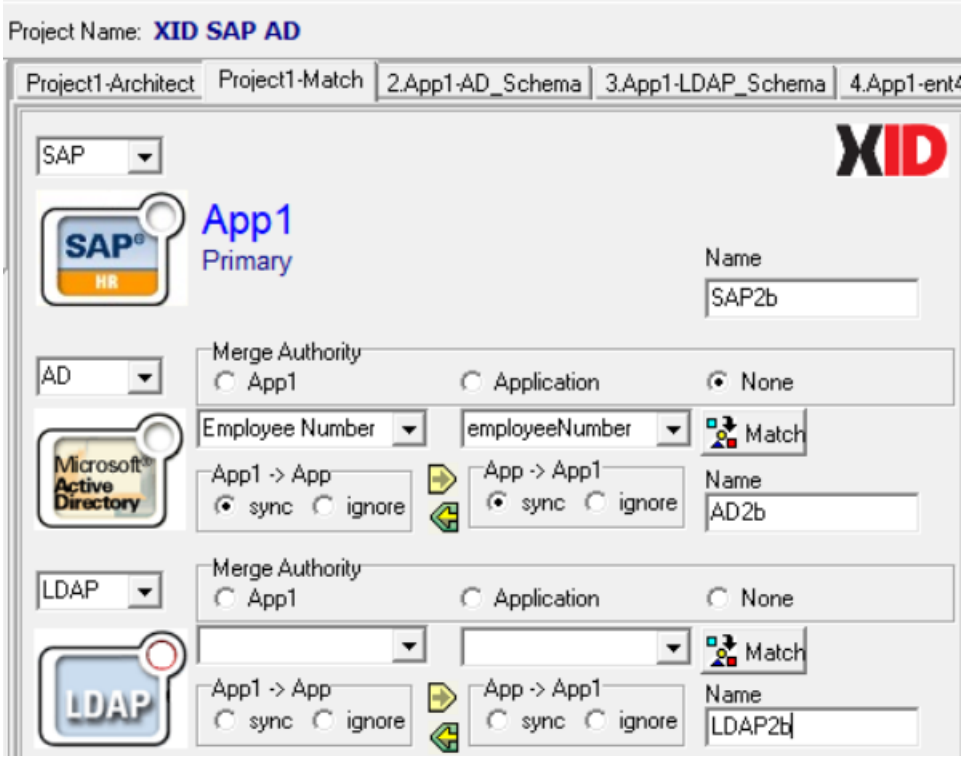
The following will cover the addition of a new application to the existing project.

Add LDAP Application

1. Click the 'Project1-Match tab.
2. Select 'LDAP' from the application combo box in the next available application row.



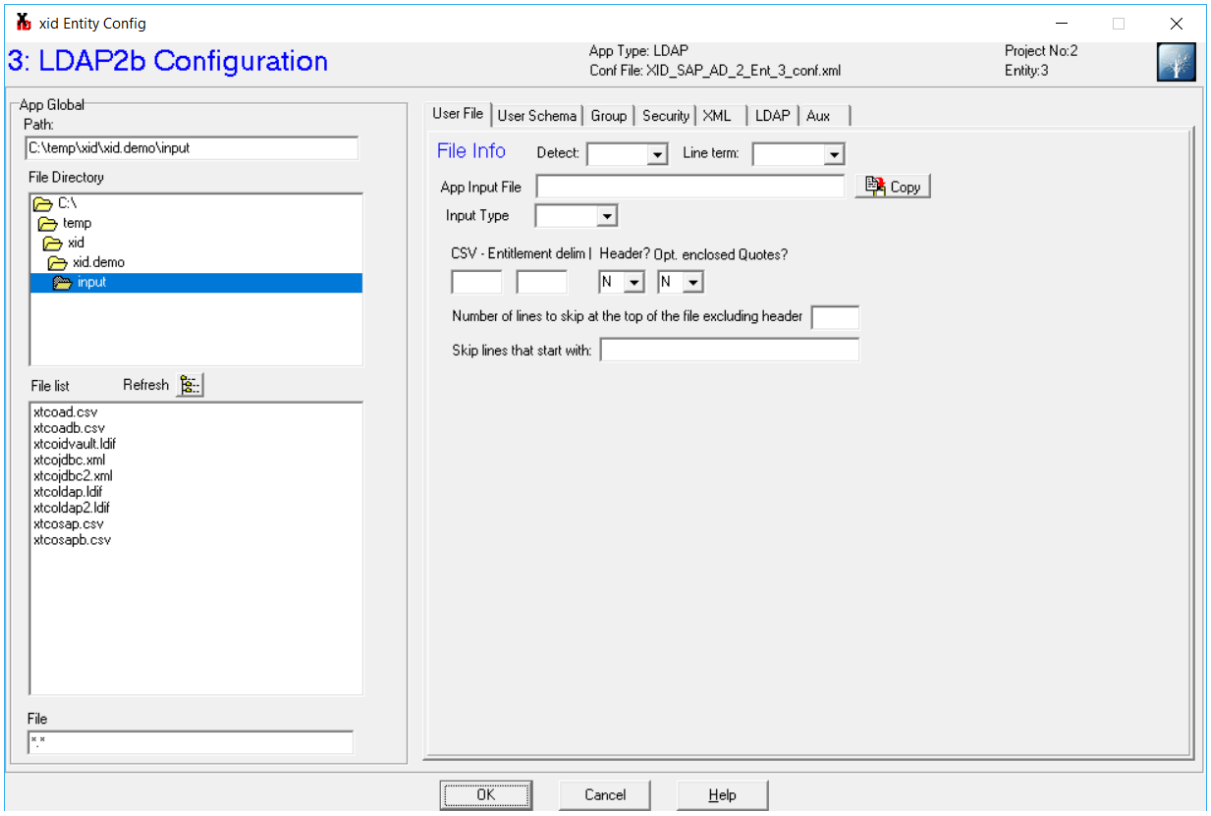
3. Enter the 'Name' for the new application. 'LDAP2b' is the name for the new application.



4. Save the Project by clicking the 'Save' icon  or by clicking 'File' then selecting 'Save'. Click 'OK' to close the dialog box.

Application Configuration: LDAP

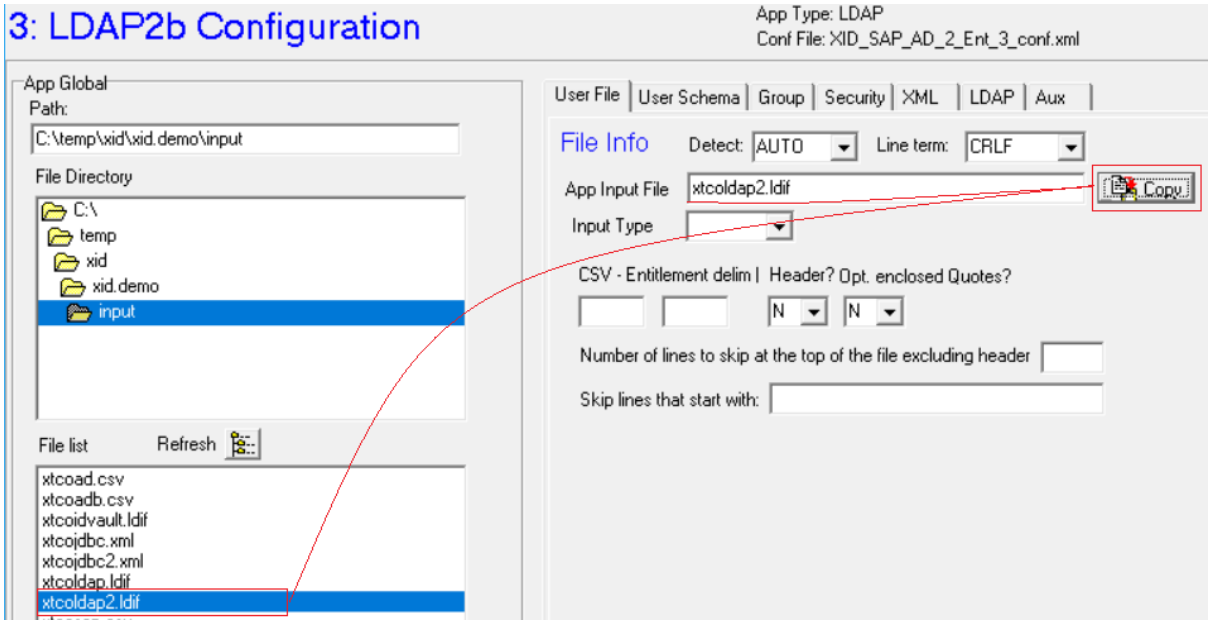
1. Load LDAP application configuration by clicking the ‘LDAP’ icon in ‘Project1-Match’.



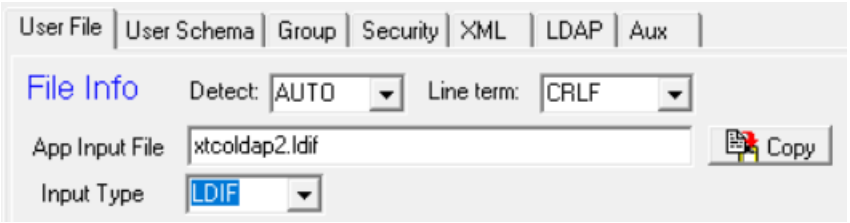
File Info

1. Click the 'User File' tab if not already selected.
2. Set ‘Detect’ to ‘AUTO’. This setting will use the XID file detection process.
3. Select ‘CRLF’ for ‘Line term’. For Windows systems ‘Carriage Return Line Feed’ is used for terminating text file lines. Text files sourced from Unix/Linux systems can be Line Feed ‘LF’ only. Select ‘LF’ if this is the line termination character.

4. Select the LDAP input file extracted for this project in the ‘File list’ box. For this example the file is ‘xtcoldap2.ldif’ and represents a data extract from LDAP.
5. Click 'Copy' to populate the 'App Input File' edit box.



6. Select the extract file type from the ‘Input Type’ drop down box. The sample LDAP extraction file is of type ‘LDIF’. Do not enter CSV details as they do not apply to LDIF files.



LDAP Schema

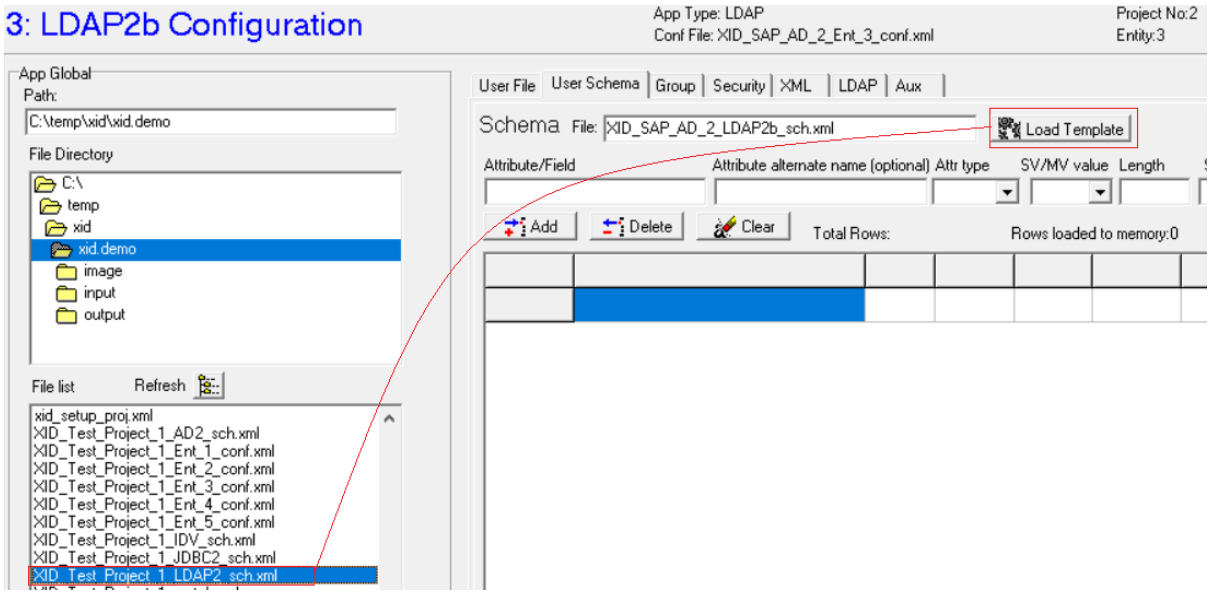
The schema attribute has to match that of its LDIF attribute counterpart. Although attribute spelling is important, the case does not have to be exact. Attribute order is not a requirement and not all attributes have to be entered into the XID schema. It is best to only load necessary attributes into the XID schema. The following is the first User object in the sample LDAP LDIF file.

```
dn: cn=SmithJ,ou=Paris,ou=FR,o=xidtestco
givenName: James
sn: Smith
fullName: James Smith
uid: 10000001
ou: HR
l: Paris
mail: James.Smith@xidtestco.com
telephoneNumber: 33110102
mobile: 33120103
title: Line Manager
loginDisabled: FALSE
cn: SmithJ
```

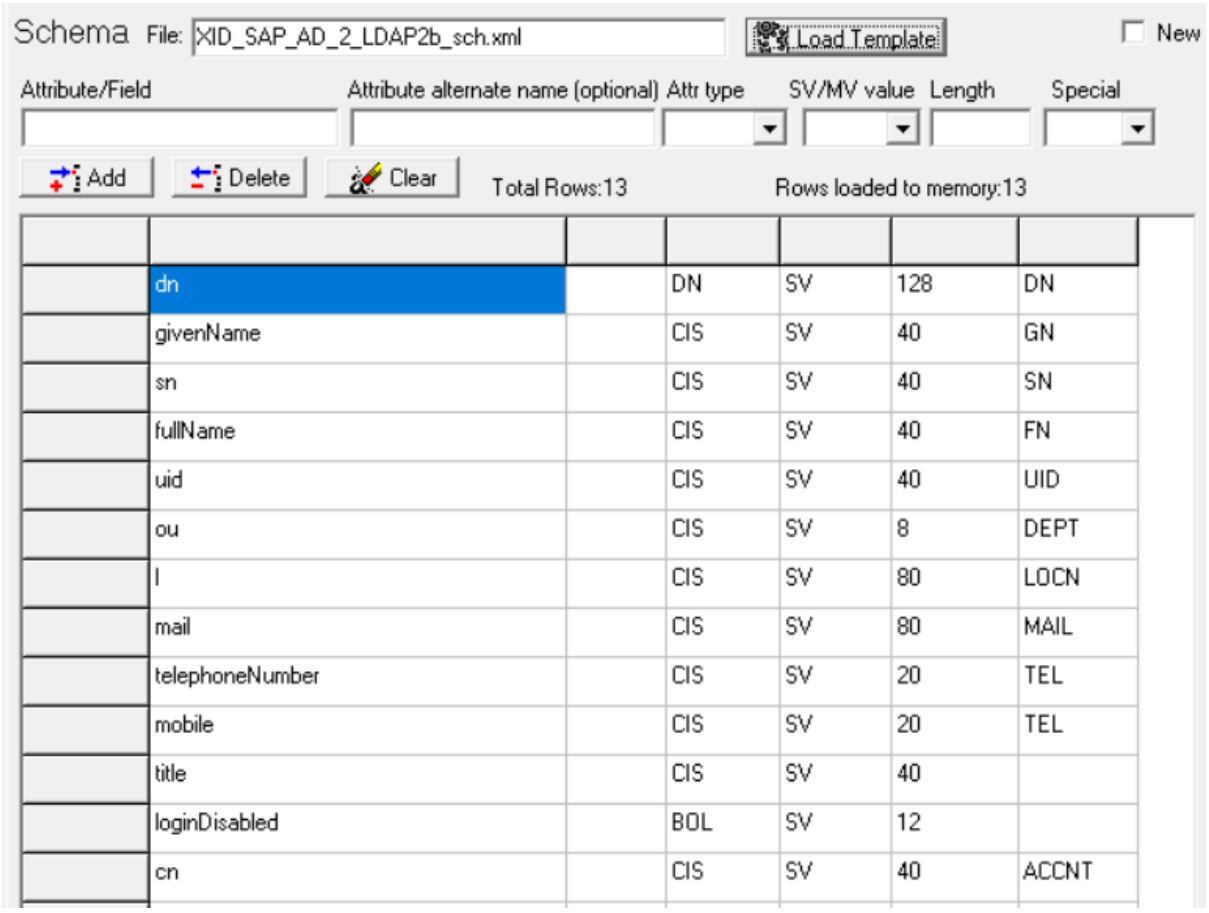
Template Method:

The following example will demonstrate the use of templates. The templates used in this example are those shipped with XID.

1. Click the 'User Schema' tab.
2. Scroll through the 'File list' scroll box and locate the schema files for LDAP. The files will end with '_sch.xml'. The 'XID_Test_Project_1_LDAP2_sch.xml' template file contains the LDAP schema shipped with XID.
3. Select 'XID_Test_Project_1_LDAP2_sch.xml' in the File list box.



4. Click 'Load Template'.
5. The schema will be loaded with the following details.



	dn		DN	SV	128	DN
	givenName		CIS	SV	40	GN
	sn		CIS	SV	40	SN
	fullName		CIS	SV	40	FN
	uid		CIS	SV	40	UID
	ou		CIS	SV	8	DEPT
	l		CIS	SV	80	LOCN
	mail		CIS	SV	80	MAIL
	telephoneNumber		CIS	SV	20	TEL
	mobile		CIS	SV	20	TEL
	title		CIS	SV	40	
	loginDisabled		BOL	SV	12	
	cn		CIS	SV	40	ACCNT

Manual Schema creation

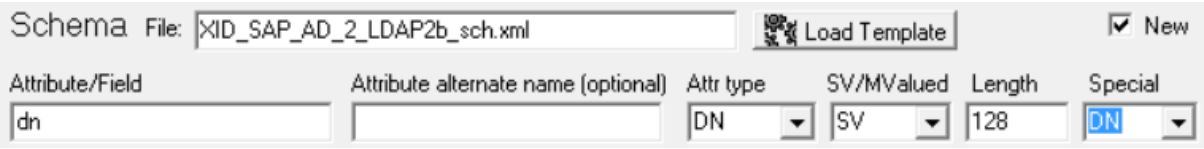
Skip this section if the template method has been used and go to 'Account Control'.

The following details the manual schema creation excluding the template usage.

1. Click the 'User Schema' tab.

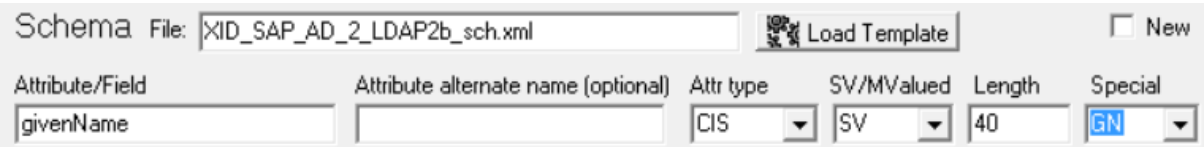
- The first attribute is ‘dn’ which will be entered into the schema first.
- Enter ‘dn’ into the ‘Attribute’ edit box.
- The ‘Attribute alternate name’ is optional. This is for LDAP schema types that can have naming for LDAP compliance in addition to proprietary naming. Ignore the alternate name.
- The ‘Attr type’ provides alternate selections for LDAP schemas. For LDAP the value will be set to ‘DN’ which is ‘Distinguished Name’.
- Select ‘SV’ to indicate the attribute is single valued.
- The Length value indicates the maximum number of characters for the attribute. Set the value to ‘128’ for this example.

- Special: The special selection denotes attribute significance to XID. As XID cannot assume significance of the attribute then this must be bestowed. The appendix has the full description for all of the combo box items. The 'dn' is significant as the LDAP object is referenced by its distinguished name (DN). Select 'DN' from the Special combo box.
- *The appendix has a list of the expanded values for the combo boxes.*



2. Click the 'Add' button. The value is populated in the schema list.A blank row is intentionally added below the last attribute in the schema.
3. The next attribute in the LDIF extract is 'givenName'.
   - Enter 'givenName' in the 'Attribute'.
   - Set the 'Attr type' to 'CIS' (Case Ignore String).
   - Set 'Single/Multi Valued' to 'SV'.
   - Set the 'Length' to the character length value for the First Name. For this example the value is '40'.
   - Set the 'Special' value to 'GN'. This indicates to XID that this attribute is the Given Name specifier.

4. Click 'Add' to add givenName to the schema.



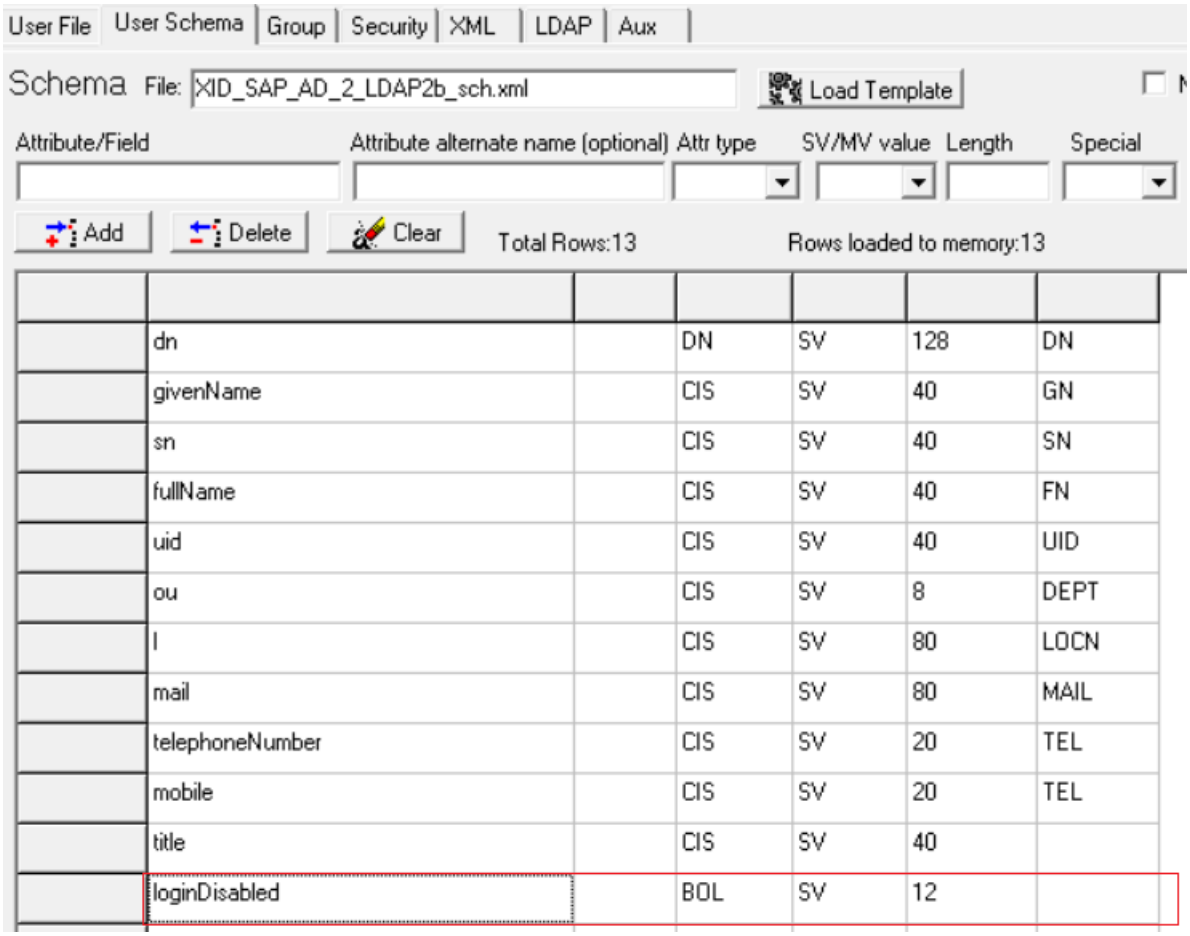
5. Repeat the action as per the previous step for the remaining attributes in the following table. Note that 'l' is the lowercase letter 'L' as in location.

Attribute	Attr type	Single/Multi valued	Length	Special
dn	DN	SV	128	DN
givenName	CIS	SV	40	GN
sn	CIS	SV	40	SN
fullName	CIS	SV	80	FN
uid	CIS	SV	25	UID
ou	CIS	SV	80	DEPT
l	CIS	SV	50	LOCN
mail	CIS	SV	125	MAIL
telephoneNumber	CIS	SV	25	TEL
mobile	CIS	SV	25	TEL
title	CIS	SV	50	
loginDisabled	CIS	SV	25	
cn	CIS	SV	80	ACCNT

Account Control

The account control attribute defines the attribute used to determine if an account is active. The value specified is for the account enabled state. The following will set the account enabled information for the sample AD application.

1. Click the 'User Schema' tab if not already selected.
2. Click and highlight the attribute in the schema table used for account control. For the sample LDAP this attribute is ‘loginDisabled’.



	dn		DN	SV	128	DN
	givenName		CIS	SV	40	GN
	sn		CIS	SV	40	SN
	fullName		CIS	SV	40	FN
	uid		CIS	SV	40	UID
	ou		CIS	SV	8	DEPT
	l		CIS	SV	80	LOCN
	mail		CIS	SV	80	MAIL
	telephoneNumber		CIS	SV	20	TEL
	mobile		CIS	SV	20	TEL
	title		CIS	SV	40	
	loginDisabled		BOL	SV	12	

3. Click the 'Security' tab.
4. Click the ‘Copy’ button to populate the ‘Account Ctrl attr:’ edit box with the account control attribute selected in the schema.
5. Enter the value used to determine the value that determines that the account is active. In this sample the value is ‘false’.

Save Application

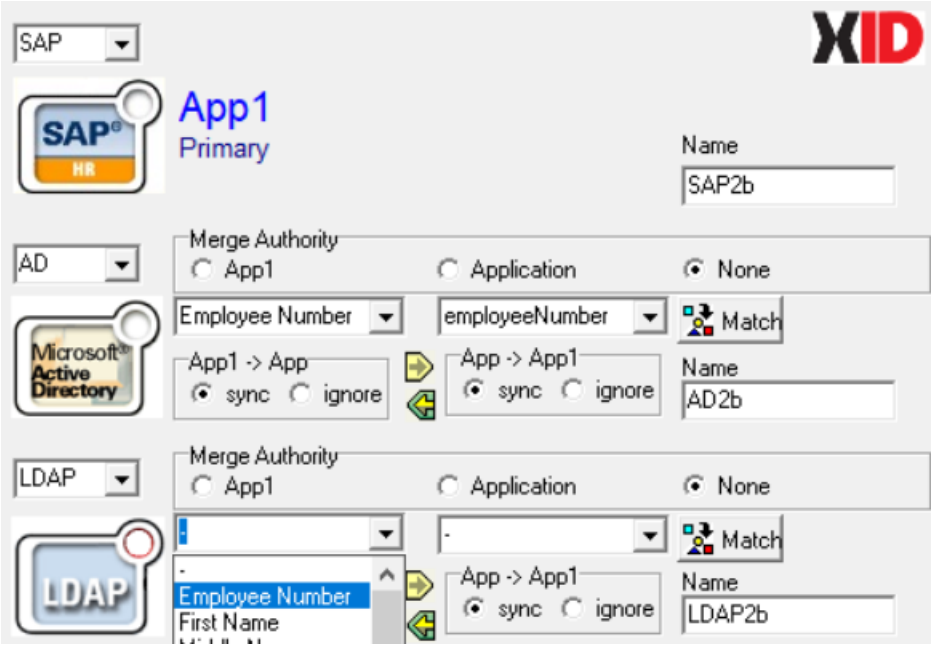
1. Click ‘OK’ to save the application selection. At this stage the information is saved to a memory cache and will not be committed to disk until the project is saved.
2. Save the Project by clicking the ‘Save’ icon  or by clicking ‘File’ then selecting ‘Save’.
3. Click ‘OK’ to close the save confirmation box.

LDAP Matching Rules

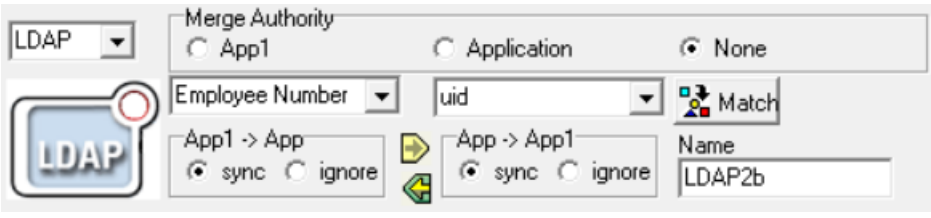
The matching rules will be set at the third application for this example.

The matching combo boxes are populated with the information from the application schema. The left combo box is application 1 or the ID Vault. The right combo box is the application represented by the application position.

1. Select the ‘Project1-Match’ tab.
2. Click the left combo box on application 3 which is the LDAP application LDAP2b.
3. Select the application 1 attribute used for primary matching. For SAP (application 1) select ‘Employee Number’.



4. Click the right combo box and select the application 3 primary matching attribute. For LDAP (application 3) select ‘uid’.



5. Save the Project by clicking the ‘Save’ icon  or by clicking ‘File’ then selecting ‘Save’.
6. Click ‘OK’ to close the save confirmation box.

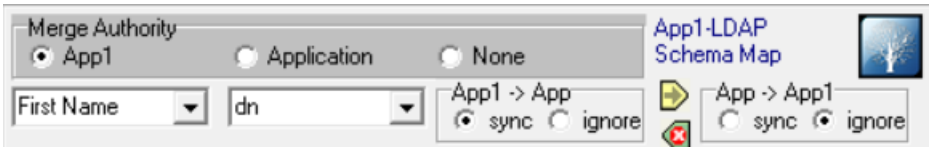
LDAP Business Rules

The business rules section allows comparison of applications at an attribute level. Although 50 items can be added to the schema, there is a limit of 30 business rules that can be defined.

The business rule combo boxes are populated with the information from the application schema. The left combo box is application 1 or the ID Vault (IDV). The right combo box is the application represented by the tab selected. This is also referred to as the Application.

1. Click the ‘3. App1-LDAP_Schema’ tab.
2. Click the left combo box which contains the schema for application 1 or the ID Vault. Select the ‘First Name’ attribute from SAP.
3. Click the right combo box which contains the schema for application 3. Select the ‘givenName’ attribute from LDAP.
4. For this example SAP ‘First Name’ is authoritative for this attribute. LDAP will subscribe from changes from SAP but SAP will ignore changes from LDAP. Set this rule scenario as follows:
    - Click ‘sync’ in 'App1 -> App' (Subscribe) to allow data from application 1 (SAP) to application 3 (LDAP).
    - Click ‘ignore’ in 'App -> App1' (Publish) to block data from application 3 (LDAP) to application 1 (SAP).

5. Set the global merge authority to be ‘App1’ by clicking ‘App1’ in ‘Merge Authority’. In the absence of a defined authoritative attribute (‘Subscribe’/’Publish’) rule the merge authority will arbitrate to determine which application is authoritative. The merge authority will also determine authority if both ‘Subscribe’ and ‘Publish’ are set to ‘sync’.

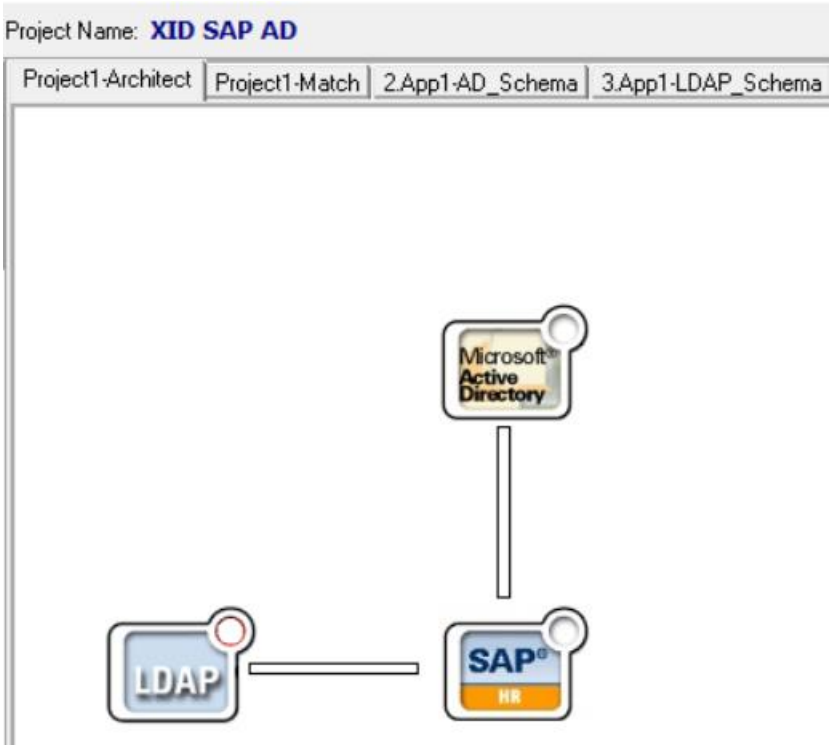


6. Repeat the previous steps to add attributes per the following table. The last schema mapping is 'MOB_NUMBER'. The business rules will fit on the first page of the schema map.

Application 1 (IDV)	Application 3 (Application)	Subscribe Application 1 to Application 3	Publish Application 3 to Application 1	Merge Authority
First Name	givenName	Sync	Ignore	App1
Last Name	sn	Sync	Ignore	App1
Org Unit	ou	Sync	Ignore	App1
Location	l	Sync	Ignore	App1
Position Title	title	Sync	Ignore	App1
Email Address	mail	Sync	Ignore	App1
TEL_NUMBER	telephoneNumber	Sync	Sync	App1
MOB_NUMBER	mobile	Sync	Sync	App1

The schema map should look as follows:

7. Save the Project by clicking the ‘Save’ icon  or by clicking ‘File’ then selecting ‘Save’. Click ‘OK’ to close the dialog box.
8. Click the 'Project1-Architect' tab. The project will contain three applications:

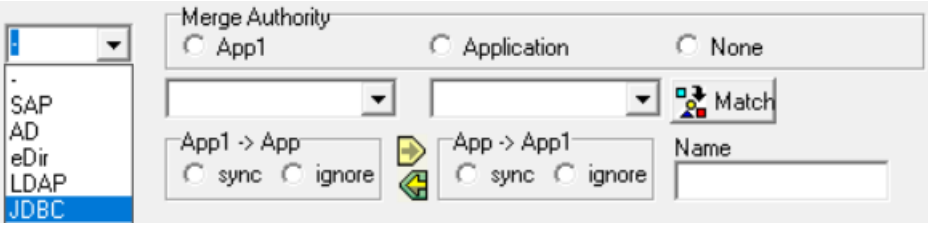


New Project Additional Application: JDBC

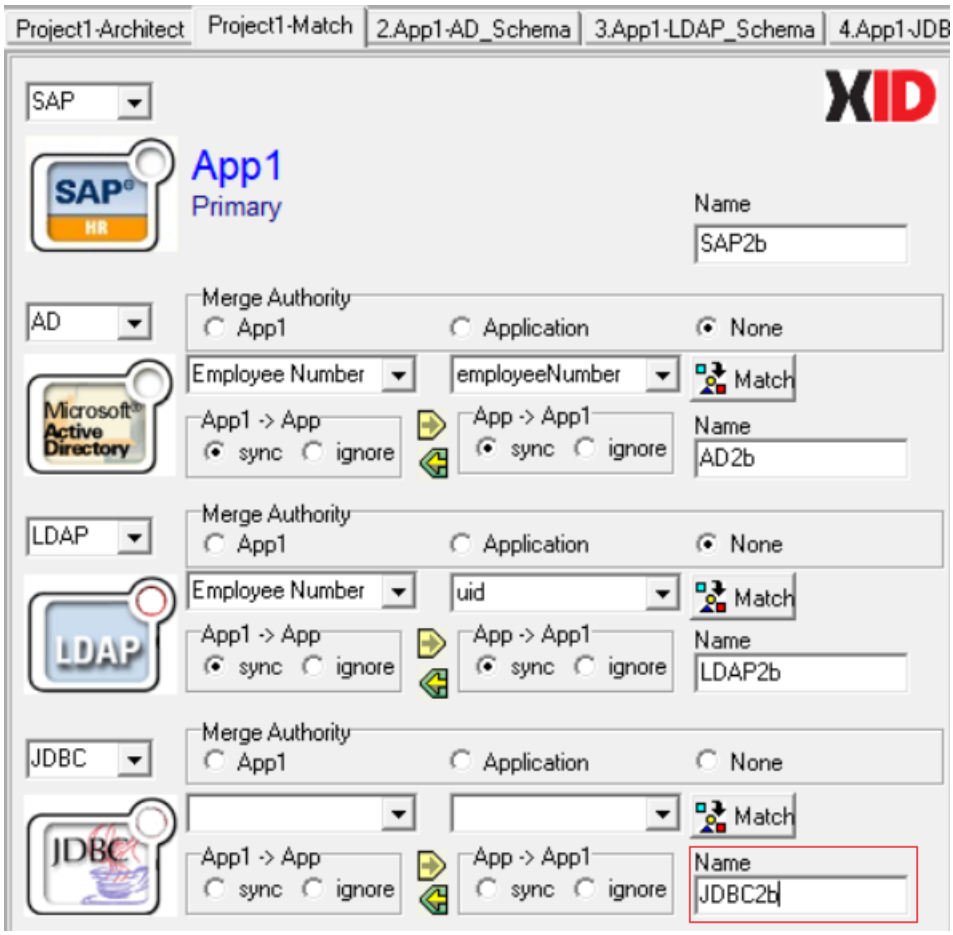
The following will cover the addition of a new JDBC application to the existing project. JDBC covers databases such as MS SQL, Oracle and MySQL.

Add JDBC Application

1. Click the 'Project1-Match tab.
2. Select 'JDBC' from the application combo box in the next available application row.



3. Enter the 'Name' for the new application. 'JDBC2b' is the name for the new application.



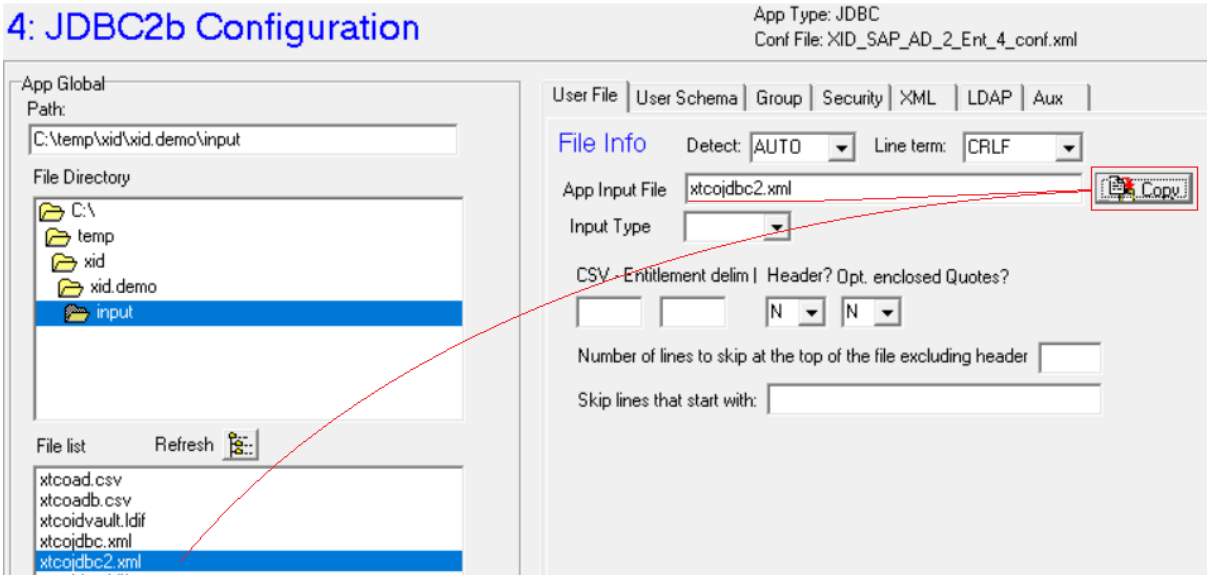
4. Save the Project by clicking the ‘Save’ icon  or by clicking ‘File’ then selecting ‘Save’. Click ‘OK’ to close the dialog box.

Application Configuration: JDBC

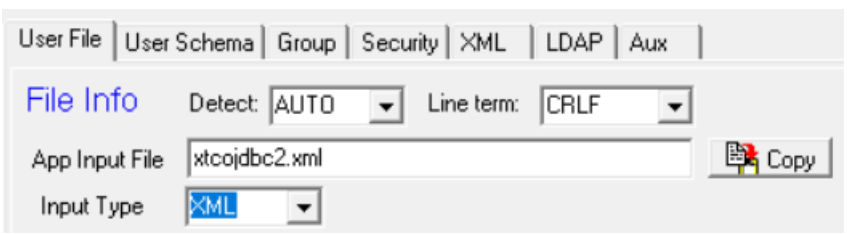
1. Load JDBC application configuration by clicking the ‘JDBC’ icon in ‘Project1-Match’.

File Info

1. Click the 'User File' tab if not already selected.
2. Set ‘Detect’ to ‘AUTO’. This setting will use the XID file detection process.
3. Select ‘CRLF’ for ‘Line term’. For Windows systems ‘Carriage Return Line Feed’ is used for terminating text file lines. Text files sourced from Unix/Linux systems can be Line Feed ‘LF’ only. Select ‘LF’ if this is the line termination character.
4. Select the JDBC input file extracted for this project in the ‘File list’ box. For this example the file is ‘xtcojdbc2.xml’ and represents a data extract from JDBC.
5. Click 'Copy' to populate the 'App Input File' edit box.



6. Select the extract file type from the ‘Input Type’ drop down box. The sample JDBC extraction file is of type ‘XML’. Do not enter CSV details as they do not apply to XML files.



XML Headers

The XML Headers define the encapsulating elements for the user object and identity record. Not all of the elements have to be configured but the common element that encapsulates the user class attributes/fields must be.

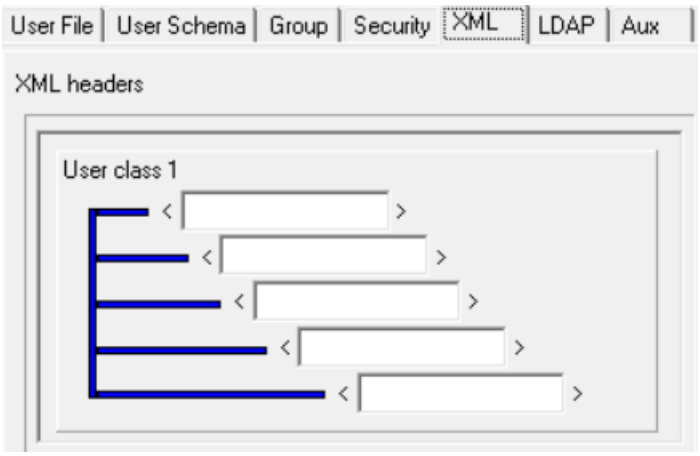
In the JDBC sample extract the common element that encapsulates the user class XML field elements which begins with the <record> tag. The <record> start tag must be defined in the XML Headers section. It is advised to configure the field type definition for a user class if there are other class types defined in the JDBC XML extract file. In this example the user class definition element is <User> and this can be entered in the XML Header configuration in the hierarchical order defined in the JDBC XML extract file.

```
<User>
      <Record>
            <EmployeeNumber>10000001</EmployeeNumber>
            .
      </Record>
</User>
```

The field elements are not entered in the XML Header section as these elements are represented in the XID schema.

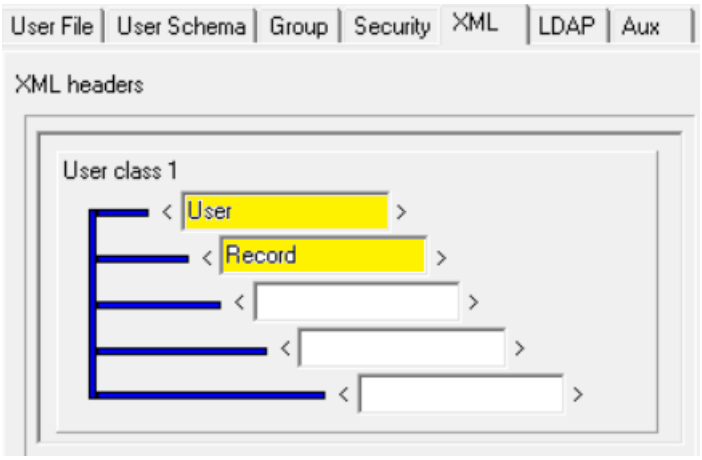
Only the start tag definition is required. The end tag will be applied automatically and is not to be added to the XML Header configuration.

1. Click the 'XML' tab.



2. Click into the first element definition edit box under ‘XML Headers’ -> ‘User class 1’.
3. Optional: Enter the class definition element which is ‘User’ in this example. Do not enter opening or closing characters (‘<’,’>’,’/’) and avoid spaces before and after the elements definition.

4. Click into the second element definition edit box and enter the next record encapsulating element. In this example the second and final encapsulating element is ‘Record’. As the user class fields are encapsulated directly by the ‘Record’ element then no other XML element can follow ‘Record’ in the ‘XML Headers’ section. *There is provision for five XML elements. If an extract has more than five elements it is recommended to have at least two elements defined in sequence up to and including the element directly encapsulating the user class field elements.*



JDBC Schema

The schema attribute/field name has to match that of its XML field element counterpart. Although field spelling is important, the case does not have to be exact. Field order is not a requirement and not all fields have to be entered into the XID schema. It is best to only load necessary fields into the XID schema. The following are the header elements and the first two records in the sample JDBC XML file.

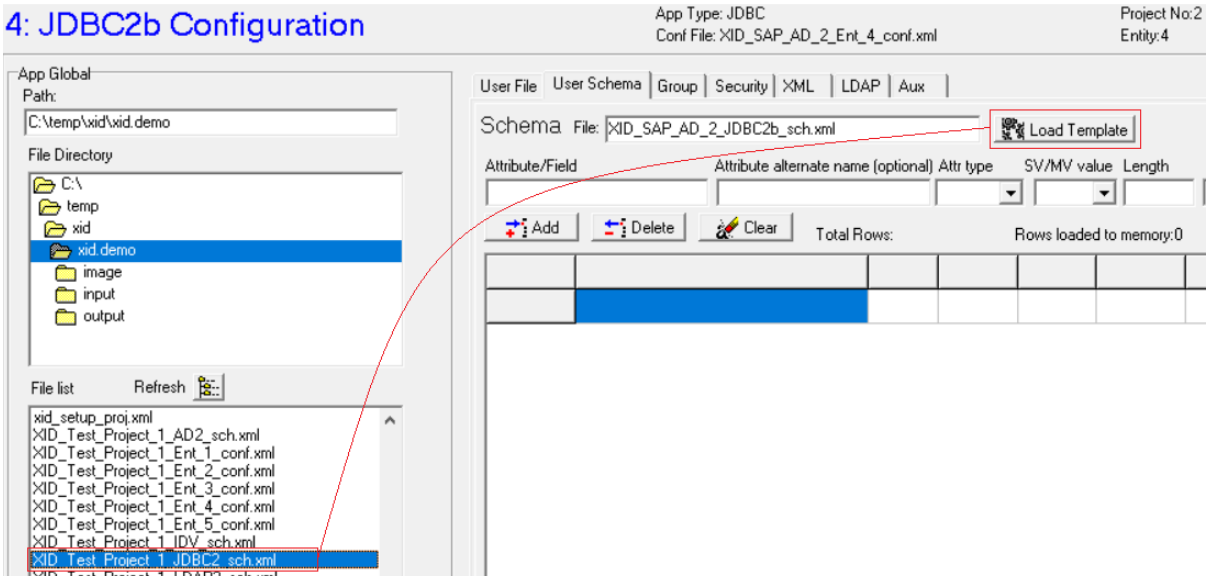
```
<?xml version="1.0" standalone="yes" ?>
<User>
<Record>
<EmployeeNumber>10000001</EmployeeNumber>
<LoginName>SmithJ</LoginName>
<FirstName>James</FirstName>
<LastName>Smith</LastName>
<Location>Paris</Location>
<Department>HR</Department>
<Title>Line Manager</Title>
<EmailAddress>James.Smith@xidtestco.com</EmailAddress>
<PhoneNumber>33110102</PhoneNumber>
<Mobile>33120103</Mobile>
<AccountStatus>Active</AccountStatus>
</Record>
<Record>
<EmployeeNumber>10000002</EmployeeNumber>
<LoginName>JohnsonJ</LoginName>
<FirstName>John</FirstName>
<LastName>Johnson</LastName>
<Location>Seattle</Location>
<Department>Drafting</Department>
<Title>Line Manager</Title>
<EmailAddress>John.Johnson@xidtestco.com</EmailAddress>
<PhoneNumber>20610103</PhoneNumber>
<Mobile>20620104</Mobile>
<AccountStatus>Active</AccountStatus>
</Record>
```

A default schema file will be created based on the application name with a '_sch.xml' suffix. The schema file name can be changed and alternatively an existing template schema file can be loaded.

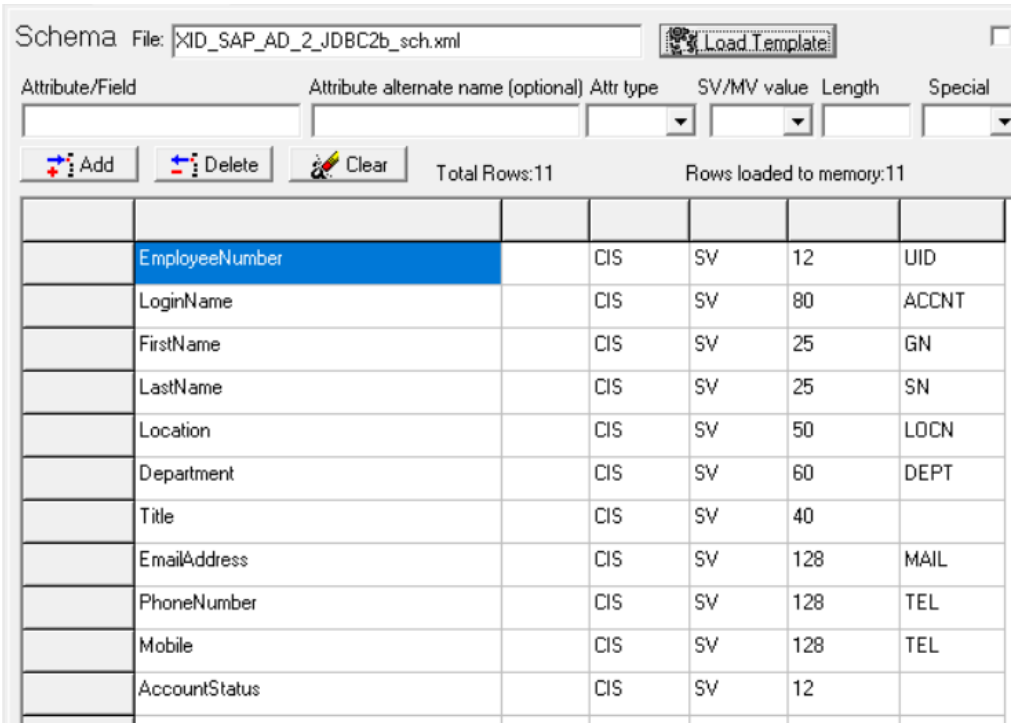
Template Method:

The following example will demonstrate the use of templates. The templates used in this example are those shipped with XID.

1. Click the 'User Schema' tab.
2. Scroll through the 'File list' scroll box and locate the schema files for LDAP. The files will end with '_sch.xml'. The 'XID_Test_Project_1_LDAP2_sch.xml' template file contains the LDAP schema shipped with XID.
3. Select 'XID_Test_Project_1_LDAP2_sch.xml' in the File list box.
4. Click 'Load Template'.



5. The schema will be loaded with the following details.



	EmployeeNumber		CIS	SV	12	UID
	LoginName		CIS	SV	80	ACCNT
	FirstName		CIS	SV	25	GN
	LastName		CIS	SV	25	SN
	Location		CIS	SV	50	LOCN
	Department		CIS	SV	60	DEPT
	Title		CIS	SV	40	
	EmailAddress		CIS	SV	128	MAIL
	PhoneNumber		CIS	SV	128	TEL
	Mobile		CIS	SV	128	TEL
	AccountStatus		CIS	SV	12	

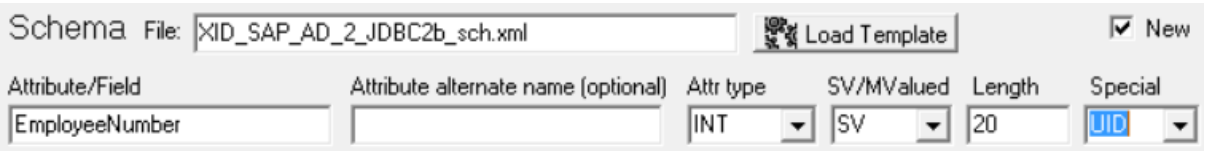
Manual Schema creation

Skip this section if the template method has been used and go to 'Account Control'.

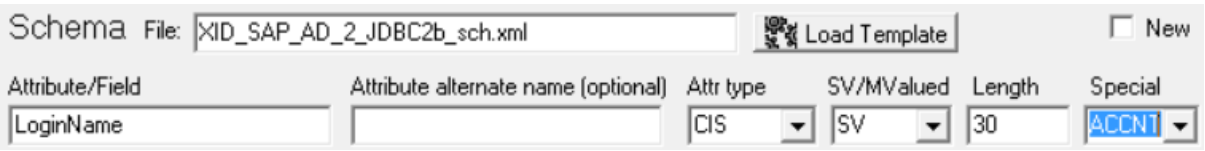
The following details the manual schema creation excluding the template usage.

1. Click the 'User Schema' tab.

- The first field is ‘EmployeeNumber’ which will be entered into the schema first.
- Enter ‘EmployeeNumber’ into the ‘Attribute/Field’ edit box.
- The ‘Attribute alternate name’ is optional.
- The ‘Attr type’ provides alternate selections for schemas. For JDBC the value will be set to ‘INT’ which is an integer number.
- Select ‘SV’ to indicate the field is single valued.
- The Length value indicates the maximum number of characters for the attribute or field. Set the value to ‘20’ for this example.
- Special: The special selection denotes attribute/field significance to XID. As XID cannot assume significance of the attribute or field then this must be bestowed. The appendix has the full description for all of the combo box items. The ‘EmployeeNumber’ is significant as this is the JDBC unique identifier that will be used for matching. Select ‘UID’ from the Special combo box.
- *The appendix has a list of the expanded values for the combo boxes.*



1. Click the ‘Add’ button. The value is populated in the schema list. A blank row is intentionally added below the last attribute or field in the schema.
2. The next field in the XML extract is ‘LoginName’.
   - Enter ‘LoginName’ in the ‘Attribute/Field’.
   - Set the ‘Attr type’ to ‘CIS’ (Case Ignore String).
   - Set ‘Single/Multi Valued’ to ‘SV’.
   - Set the ‘Length’ to the character length value for the First Name. For this example the value is ‘30’.
   - Set the ‘Special’ value to ‘ACCNT’. This indicates to XID that this attribute is the account name specifier.
   -



3. Click ‘Add’ to add 'LoginName' to the schema.

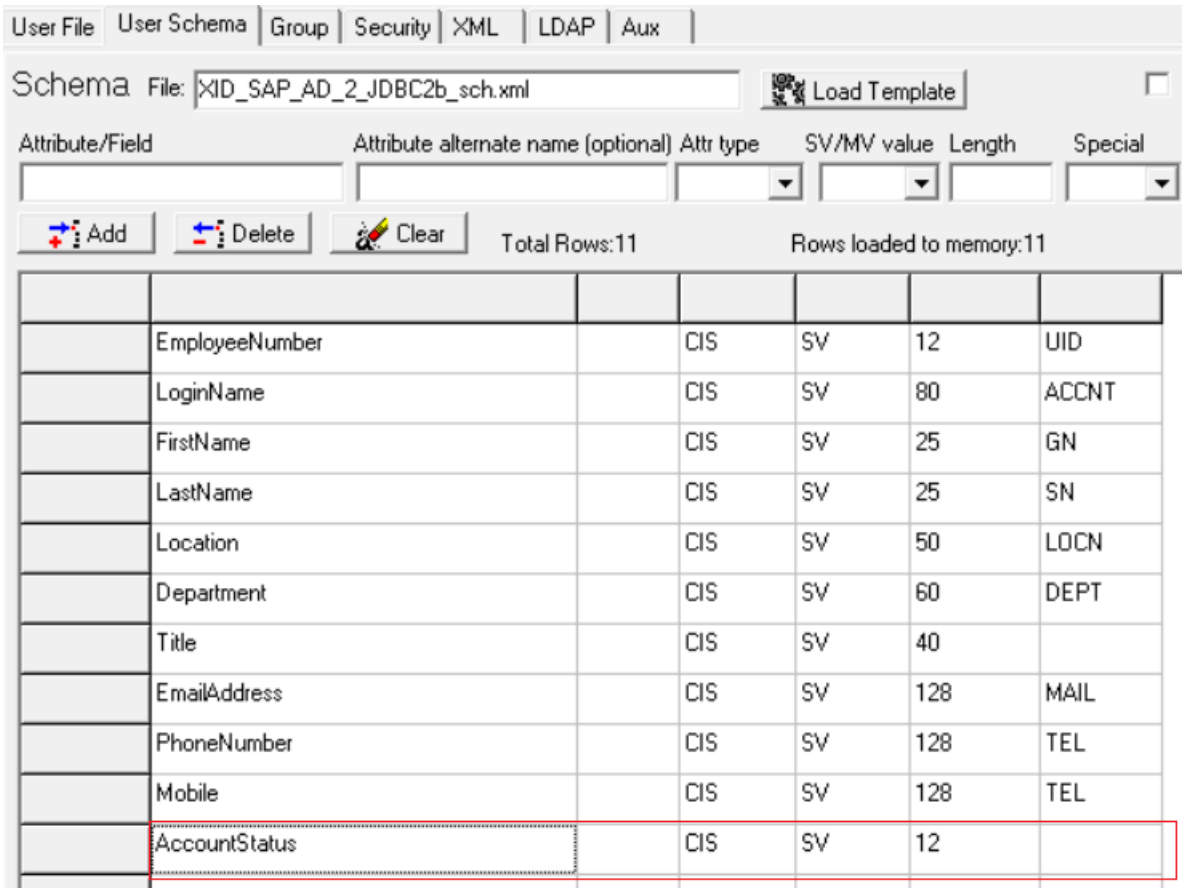
4. Repeat the action as per the previous step for the remaining fields in the following table:

Attribute/Field	Attr type	Single/Multi valued	Length	Special
EmployeeName	INT	SV	20	UID
LoginName	CIS	SV	30	ACCNT
FirstName	CIS	SV	40	GN
LastName	CIS	SV	40	SN
Location	CIS	SV	80	LOCN
Department	CIS	SV	80	DEPT
Title	CIS	SV	50	
EmailAddress	CIS	SV	125	MAIL
PhoneNumber	CIS	SV	25	TEL
Mobile	CIS	SV	25	TEL
AccountStatus	CIS	SV	12	

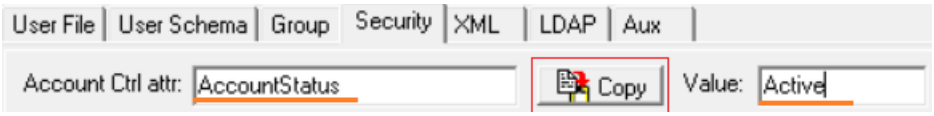
Account Control

The account control attribute/field defines the attribute/field used to determine if an account is active. The value specified is for the account enabled state. The following will set the account enabled information for the sample JDBC application.

1. Click or remain in the 'User Schema' tab.
2. Highlight the attribute in the schema table used for account control. For the sample JDBC this attribute is ‘AccountStatus’.



3. Click the 'Security' tab.
4. Click the ‘Copy’ button to populate the ‘Account Ctrl attr:’ edit box with the account control field selected in the schema.
5. Enter the value used to determine the value that determines that the account is active. In this sample the value is ‘Active’.



Save Application

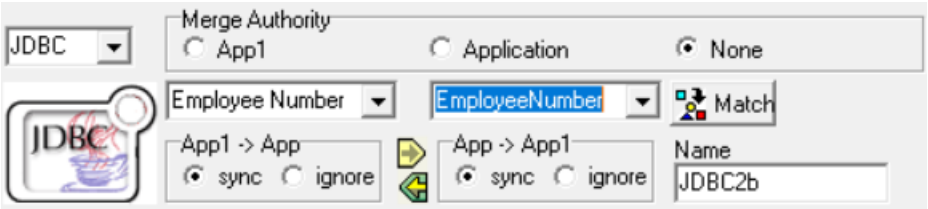
1. Click ‘OK’ to save the application selection. At this stage the information is saved to a memory cache and will not be committed to disk until the project is saved.
2. Save the Project by clicking the ‘Save’ icon  or by clicking ‘File’ then selecting ‘Save’.
3. Click ‘OK’ to close the save confirmation box.

JDBC Matching Rules

The matching rules will be set at the third application for this example.

The matching combo boxes are populated with the information from the application schema. The left combo box is application 1 or the ID Vault. The right combo box is the application represented by the application position.

1. Select the 'Project1-Match' tab.
2. Click the left combo box on application 4 which is the JDBC application JDBC2b.
3. Select the application 1 attribute used for primary matching. For SAP (application 1) select 'Employee Number'.
4. Click the right combo box and select the application 4 primary matching attribute. For JDBC (application 4) select 'EmployeeNumber'.



5. Save the Project by clicking the 'Save' icon  or by clicking 'File' then selecting 'Save'.
6. Click 'OK' to close the save confirmation box.

JDBC Business Rules

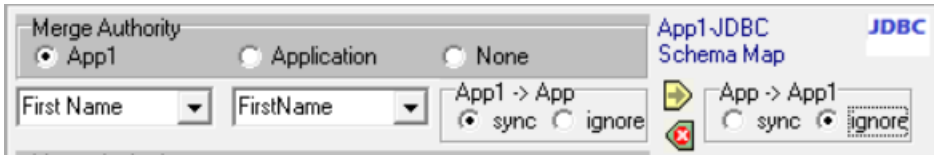
The business rules section allows comparison of applications at an attribute level. Although 50 items can be added to the schema, there is a limit of 30 business rules that can be defined. Not all of the fields and attributes need to be added but there must be at least one rule defined before running a report.

The business rule combo boxes are populated with the information from the application schema. The left combo box is application 1 or the ID Vault (IDV). The right combo box is the application represented by the tab selected. This is also referred to as the Application.

1. Click the '4. App1-JDBC_Schema' tab.
2. Click the left combo box which contains the schema for application 1 or the ID Vault. Select the 'First Name' attribute from SAP.
3. Click the right combo box which contains the schema for application 4. Select the 'FirstName' field from JDBC.
4. For this example SAP 'First Name' is authoritative for this attribute. JDBC will subscribe from changes from SAP but SAP will ignore changes from JDBC. Set this rule scenario as follows:
    - Click 'sync' in 'App1 -> App' (Subscribe) to allow data from application 1 (SAP) to application 4 (JDBC).

- Click ‘ignore’ in 'App -> App1' (Publish) to block data from application 4 (JDBC) to application 1 (SAP).

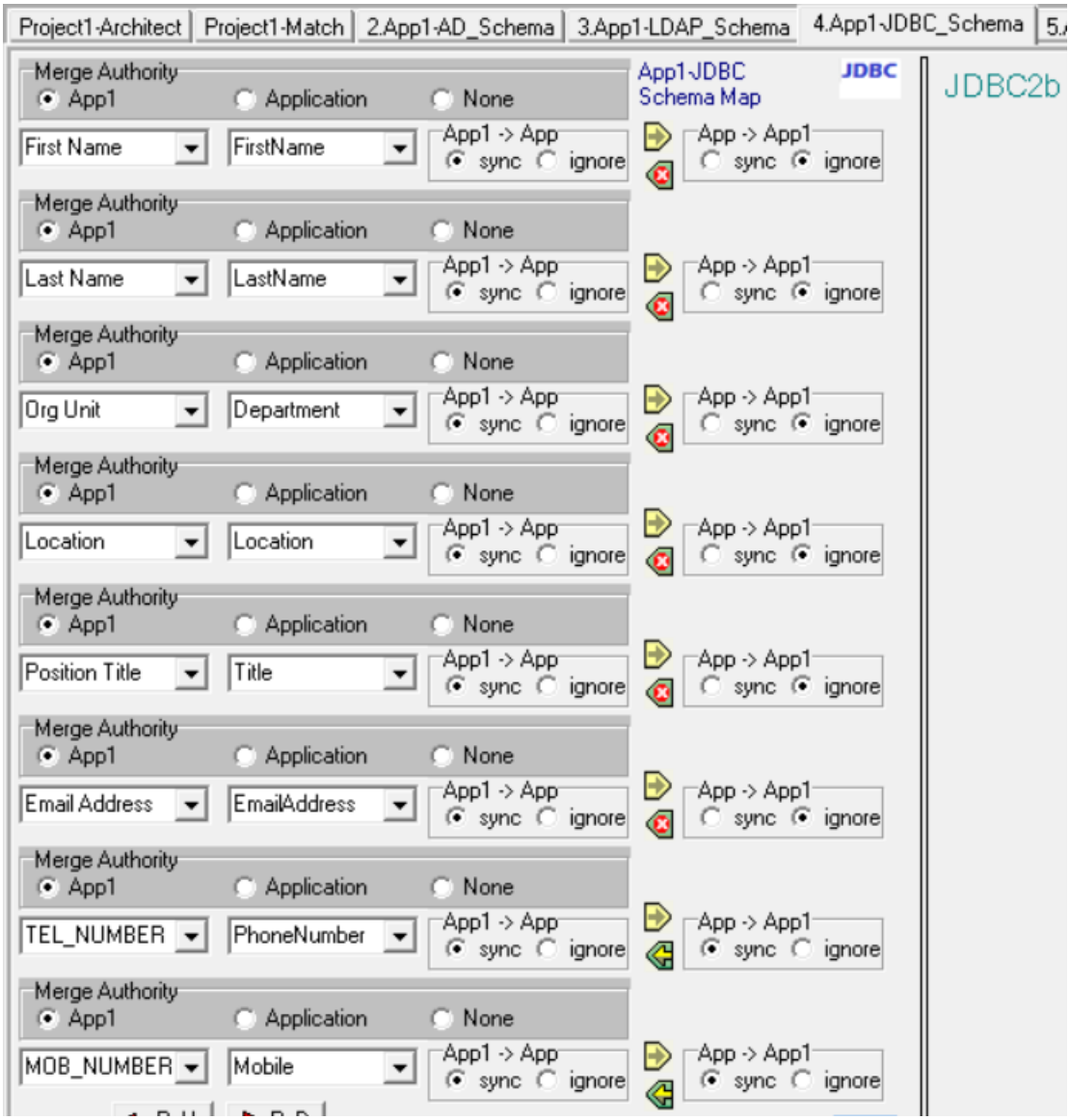
5. Set the global merge authority to be ‘App1’ by clicking ‘App1’ in ‘Merge Authority’. In the absence of a defined authoritative attribute (‘Subscribe’/’Publish’) rule the merge authority will arbitrate to determine which application is authoritative. The merge authority will also determine authority if both ‘Subscribe’ and ‘Publish’ are set to ‘sync’.



6. Repeat the previous steps to add attributes as per the following table. The last schema mapping is ‘MOB_NUMBER’. The business rules will fit on the first page of the schema map.

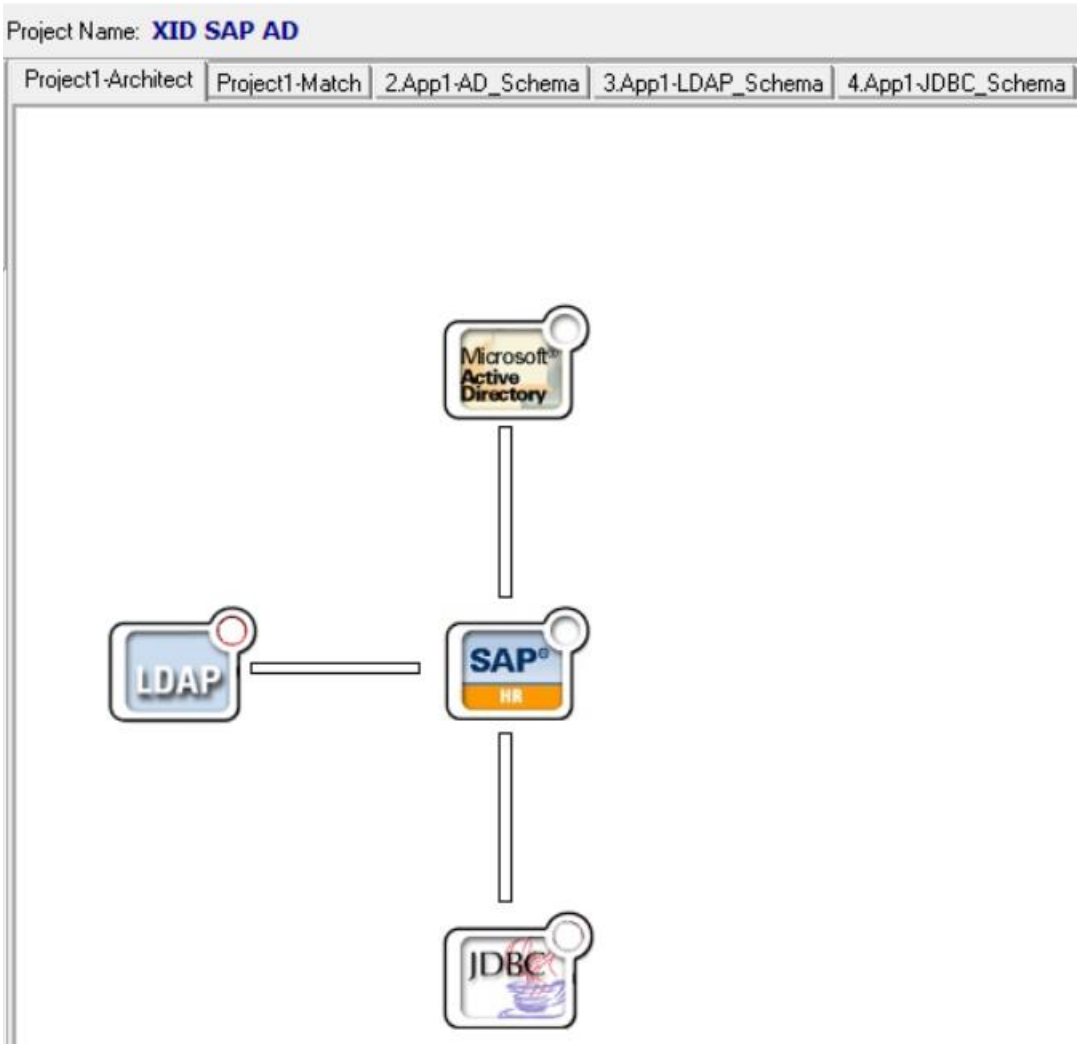
Application 1 (IDV)	Application 4 (Application)	Subscribe Application 1 to Application 4	Publish Application 4 to Application 1	Merge Authority
First Name	FirstName	sync	ignore	App1
Last Name	LastName	sync	ignore	App1
Org Unit	Department	sync	ignore	App1
Location	Location	sync	ignore	App1
Position Title	Title	sync	ignore	App1
Email Address	EmailAddress	sync	ignore	App1
TEL_NUMBER	PhoneNumber	sync	sync	App1
MOB_NUMBER	Mobile	sync	sync	App1

The schema map should look as per the following image.



7. Save the Project by clicking the 'Save' icon  or by clicking 'File' then selecting 'Save'. Click 'OK' to close the dialog box.

8. Click the 'Project1-Architect' tab. The JDBC application is displayed.



Schema Templates

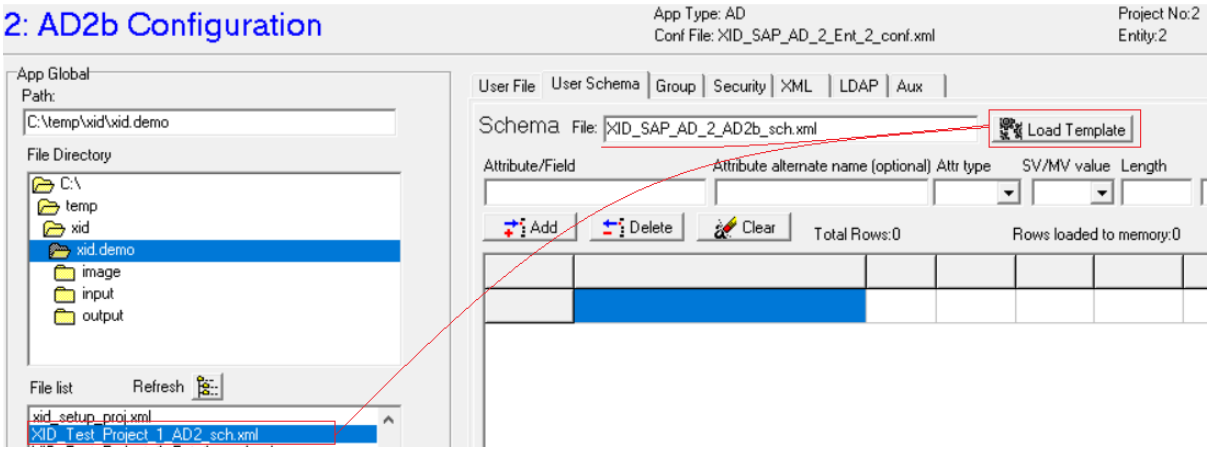
A schema template can be an existing schema file whose content can be copied into the current application schema. Once the schema is loaded it can be modified if necessary to include attributes from the new application.

For systems such as Active Directory or eDirectory, the base schema can be a useful starting point for a new application. Additional attributes can be added and attributes removed where needed.

The following example will demonstrate the use of templates using an Active Directory (AD) application and will use the same information from the training workshop. The templates used in this example are those shipped with XID.

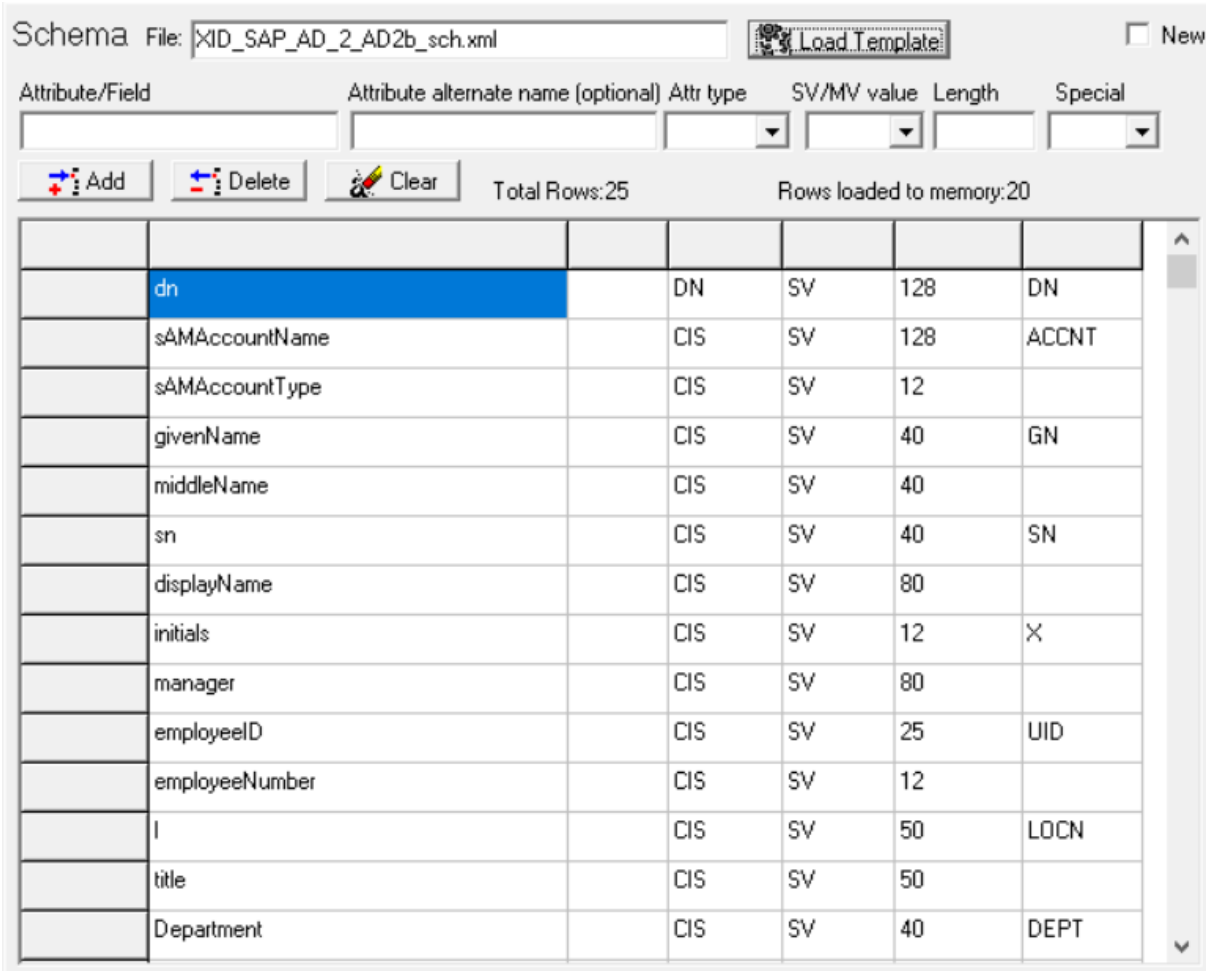
1. Open the Application configuration and click the 'User Schema' tab.
2. Scroll to the top of the 'File list' scroll box and locate the schema files for AD. The files will end with '_sch.xml'. The 'XID_Test_Project_1_AD2_sch.xml' template file contains the AD schema shipped with XID which is a good base schema for the AD workshop application. Note that this could be any previously created schema file.

3. Select 'XID_Test_Project_1_AD2_sch.xml' in the File list box.



4. Click the 'Load Template' button in the Schema section.

The schema grid populates with the attributes and settings from the template.

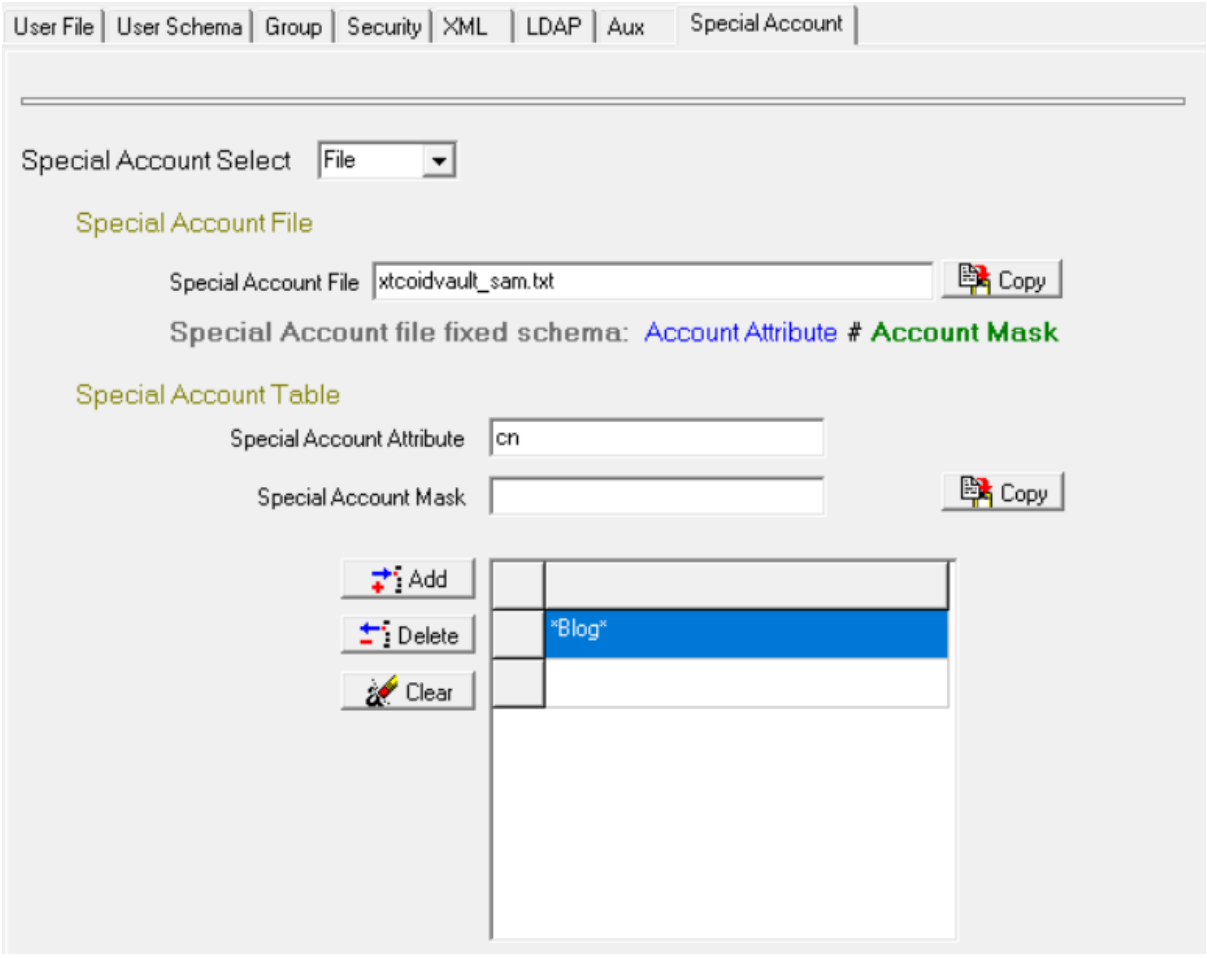


	dn		DN	SV	128	DN
	sAMAccountName		CIS	SV	128	ACCNT
	sAMAccountType		CIS	SV	12	
	givenName		CIS	SV	40	GN
	middleName		CIS	SV	40	
	sn		CIS	SV	40	SN
	displayName		CIS	SV	80	
	initials		CIS	SV	12	X
	manager		CIS	SV	80	
	employeeID		CIS	SV	25	UID
	employeeNumber		CIS	SV	12	
	l		CIS	SV	50	LOCN
	title		CIS	SV	50	
	Department		CIS	SV	40	DEPT

5. Complete any other configuration required then click 'OK' to close the application configuration preserving settings. Ensure the project is saved to permanently save the application configuration.

Special Account Mask

Special Account Mask allows service/admin etc accounts to be excluded at application load time. This configuration is located on the 'Special Account' tab of the Application configuration.



The 'Special Account Select' combo box is used to select the following:

- Off The Special Account Mask is ignored.
- Table Account Attribute and Mask are used in the 'Special Account Table' section.
  - Only a single attribute can be used to define all masks.
  - There is a 40 item limit.

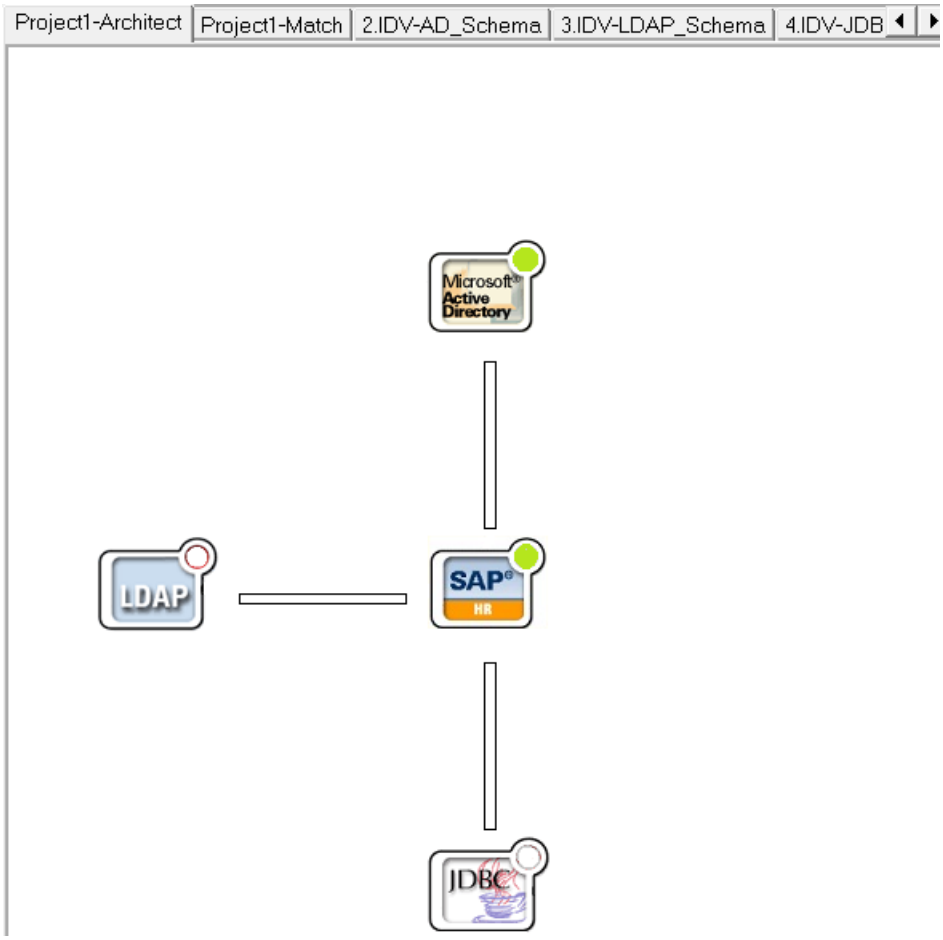
- File The File with delimited special accounts is used.
  - The file rows are comprised of attribute/mask pairs delimited by the hash '#' character.
  - The limit is attributed to system memory and performance impact.

New Project Report

The following will demonstrate the generation of an encrypted detailed report. The process involves generating a key that will be decrypted by Exact Identity Ltd (EID). The unlock key supplied by EID will be used to decrypt the detailed report.

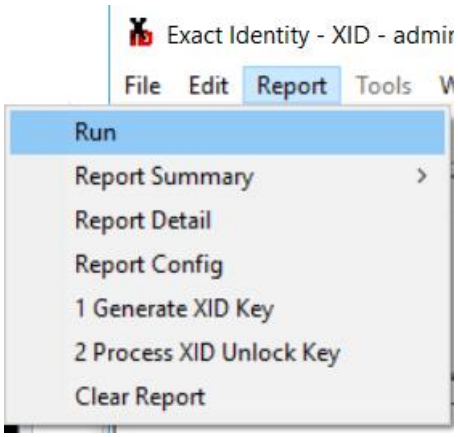
Run Report

1. Click the 'Project1-Architect' tab. Use the left arrow control  if necessary.
2. Select the 'SAP' and 'AD' applications by clicking the application icons. The application icon will update with a green circle once selected.

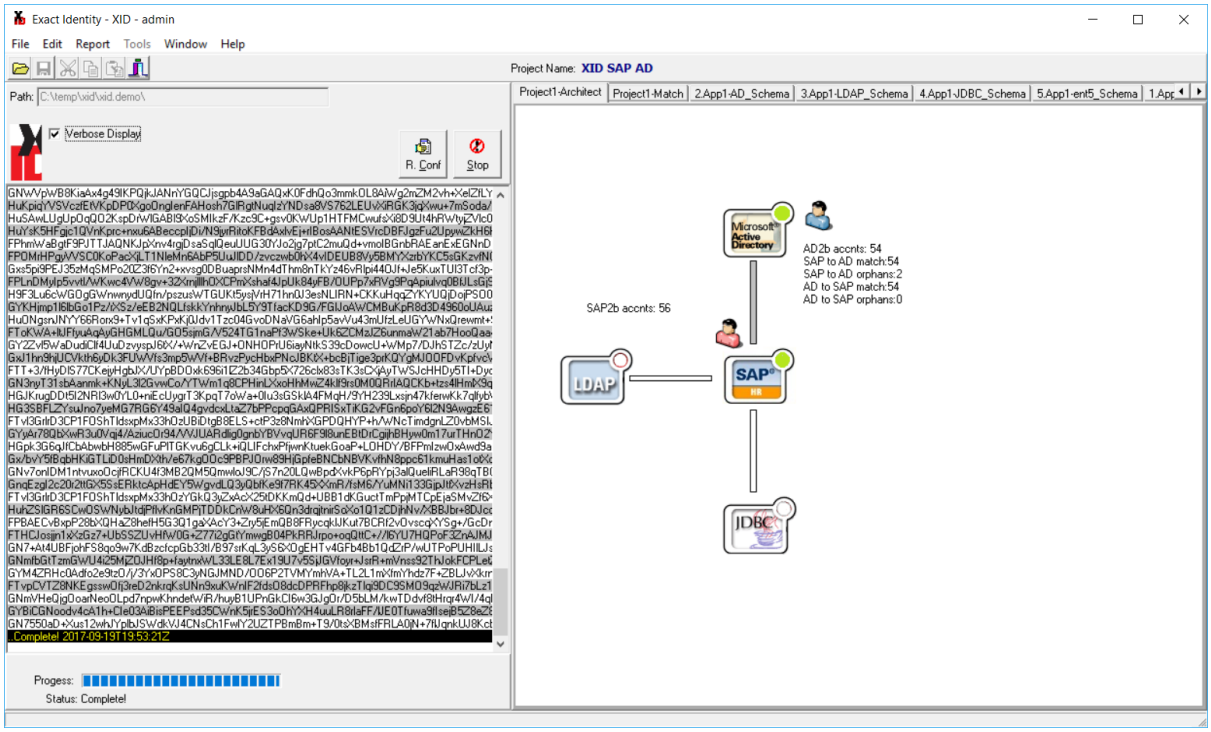


3. Click the 'Verbose Display' checkbox to select this mode. Note Verbose Display is set for test purposes only. For large reports it is recommended to set 'Verbose Display' to off.

4. Click the ‘Report’ menu and select ‘Run’.

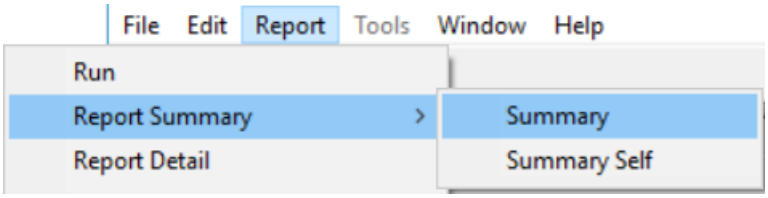


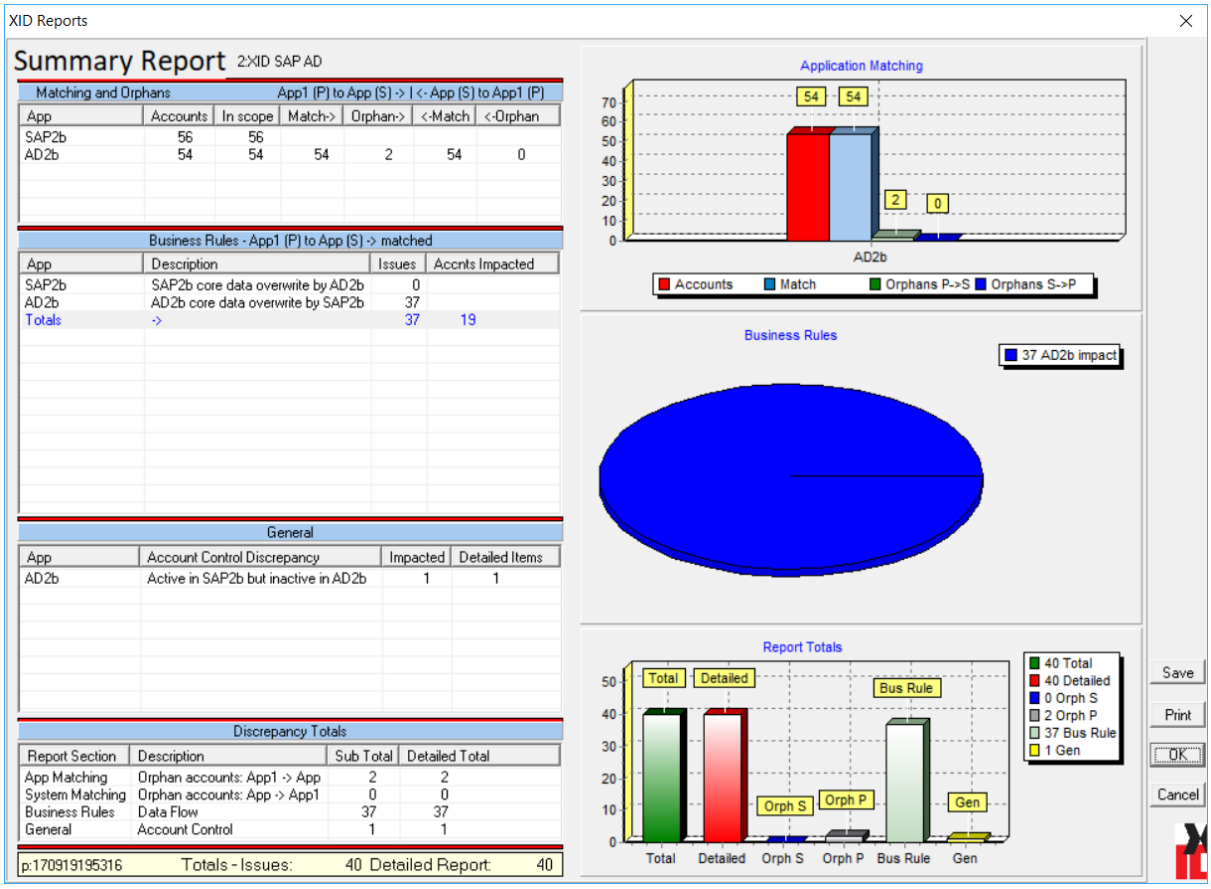
The following shows the completed report with 'Verbose Display' activated.



Report Summary

1. View the report summary by clicking ‘Report Summary’ and selecting ‘Summary’.

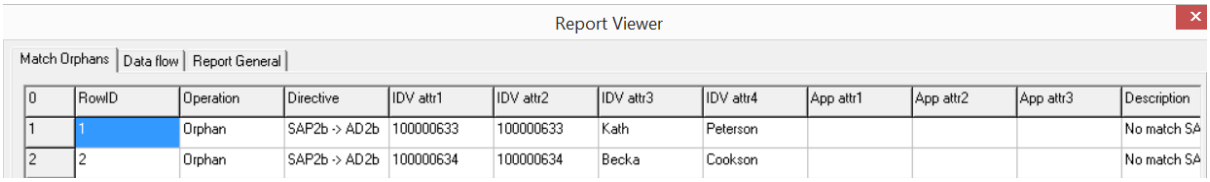




2. Print the report to the printer or file using the ‘Print’ button. Save the report to a file using the ‘Save’ button.
3. Close the summary report by clicking ‘Cancel’.

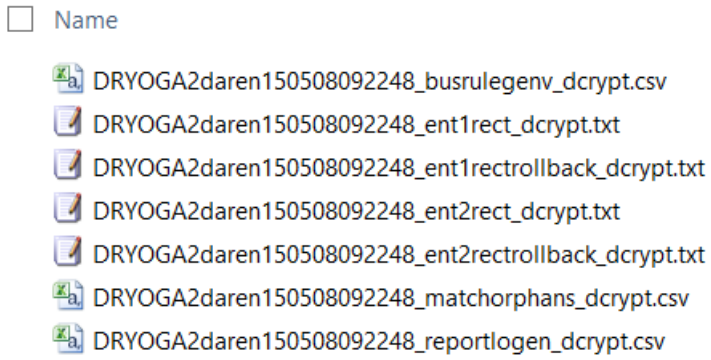
Detailed Report

1. The detailed report can be viewed in the current XID session by clicking 'Report' and selecting 'Report Detail'. Note the report will be limited if in demo mode or not authenticated.
2. The report information is available on three tabs: 'Match Orphans' [matching information], 'Data flow' [business rules] and 'Report General' [general information]. Use the horizontal and vertical scroll bars to view more columns/records.



0	RowID	Operation	Directive	IDV attr1	IDV attr2	IDV attr3	IDV attr4	App attr1	App attr2	App attr3	Description
1	1	Orphan	SAP2b -> AD2b	100000633	100000633	Kath	Peterson				No match SA
2	2	Orphan	SAP2b -> AD2b	100000634	100000634	Becka	Cookson				No match SA

The decrypted report files will be available in the output directory. The report name suffix has the '_dcrypt' suffix.



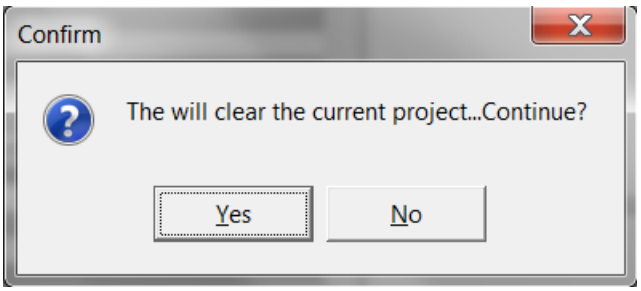
- Spread sheet tools should now be used for further analysis of the decrypted files.

XID Functions

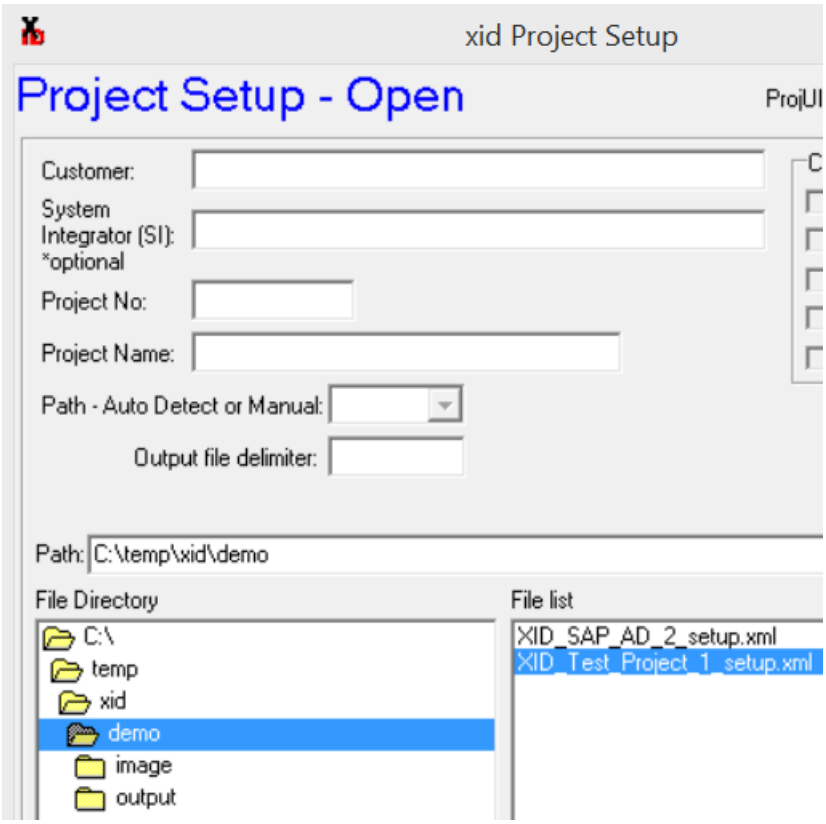
Open XID Project

Upon XID start, XID will open the last saved project. The following will demonstrate how to open another XID project.

1. Save the existing project if changes have been made.
2. Click the 'File' menu and select 'Open'.
3. Click 'Yes' when informed about clearing the existing project.

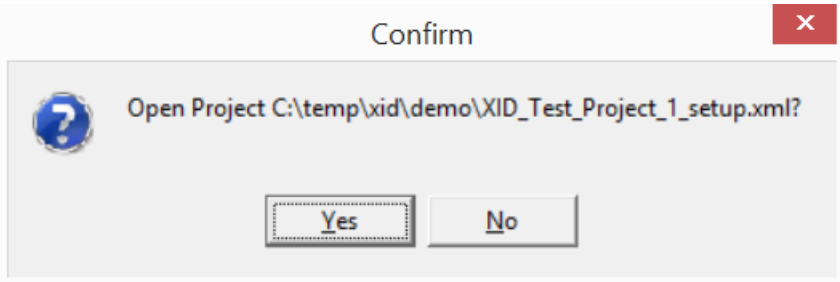


A list of existing XID projects is displayed in the 'File list' box.



4. Select the project to open from the project 'File list'. The example will select 'XID_Test_Project_1_setup.xml'.

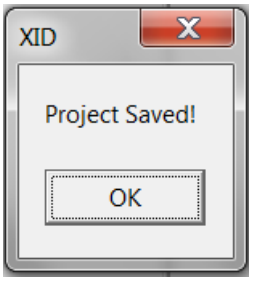
5. The following dialog box requests confirmation to open the project. Click 'Yes' to open the project.



6. Click 'OK' to close the Project Setup window and to open the selected project.

Save XID Project

1. Save the Project by clicking the 'Save' icon  or by clicking 'File' then selecting 'Save'.



2. Click 'OK' to close the save confirmation box.

Exit XID

To exit XID click 'File' and select 'Exit' or click the exit icon  .

XID Desktop Controls

Check Multiple Matches.

Checked: When running a report XID will continue searching for further matches after the first match. Further matches are recorded as duplicates.

Business Rule strict case.

Checked: When running a report, XID will invoke case sensitivity when comparing attribute items.

Match Rule strict case.

Checked: When running a report, XID will invoke case sensitivity when comparing matching rule items.

Test Mode.

Checked: Will process a sample of the input files for test purposes. The edit box to the right of the check box contains the value of the maximum number of records to sample. This value can be changed to raise or lower the sample.

Verbose Display.

Checked: When running a report, XID will display all report processing information.

Unchecked: XID will display minimal report processing information.

LDIF ver1.

Checked: LDIF input uses '=' instead of ':' to distinguish name/value pairs.

Unchecked: LDIF uses ':' to distinguish name/value pair (default).

Base 64.

Checked: Enable XID to process base 64 information from LDIF files.

Unchecked: Do not convert to base 64 information to text.

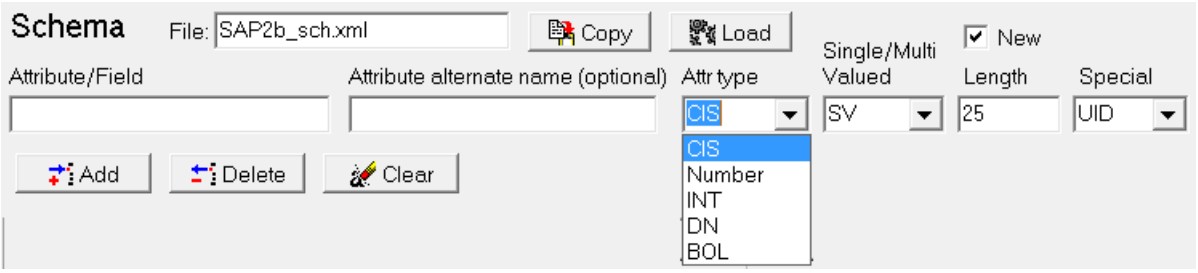
Appendix

Windows List Separator

The Windows system List Separator impacts how Windows references CSV files. The setting can be checked as follows if unsure:

1. Access the Windows Control Panel.
2. Open 'Region and Language'.
3. Select 'Additional Settings' from the 'Formats' tab (Windows 7) or 'Customize' from the 'Regional Options' tab (Windows XP, Windows Server 2003).
4. The 'List Separator' details the value used by Windows for CSV files. Note that Microsoft Excel and other spread sheet applications will utilise this value when opening files from Windows Explorer.

Schema Combo Box content



Attribute/Field Type:

Attribute or Field Type (Attr type)	Description
CIS	Case Ignore String: A string that can be comprised of any character and is not case sensitive.
Number	An integer or floating point number.
INT	Strictly and integer number.
DN	Distinguished Name: An LDAP object is referenced by its distinguished name (DN). A DN is a sequence of relative distinguished names (RDN) connected by commas. An RDN is an attribute with an associated value in the form attribute=value; normally expressed in a UTF-8 string format. The following table lists typical RDN attribute types.
BOL	Boolean: True or False | TRUE or FALSE | 1 or 0

Single or Multi Valued Attribute Type: An LDAP attribute can be single (SV) or multi valued (MV) per object.

Special: The special selection denotes attribute/field significance to XID. As XID cannot assume significance of the attribute or field then this must be bestowed. The following table describes the special combo box values that can be assigned to an attribute or field in the schema.

Special Combo Value	Description
ACCNT	Specifies the attribute/field value is the account name.
GN	Given Name.
SN	Surname.
FN	Full Name.
DN	Distinguished Name.
UID	Unique Identifier. This identifies the primary unique attribute/field used for matching.
DEPT	Department.
LOCN	Location.
MAIL	Email.
TEL	Telephone/Mobile/Facsimile etc. number.
X	The field is in the LDIF, XML or CSV file but will not be processed by XID. The value will also be excluded in the memory load.
- or blank	No special attribute significance.

Reserved Characters

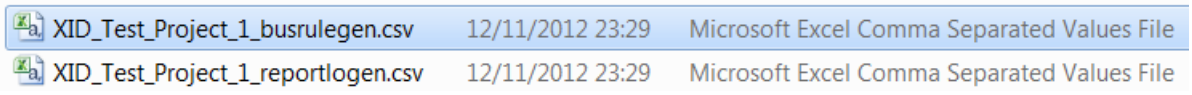
The following table lists reserved characters that cannot be used in an attribute value without being escaped.

Note See the guidance below the table about using the escape character with these reserved characters.

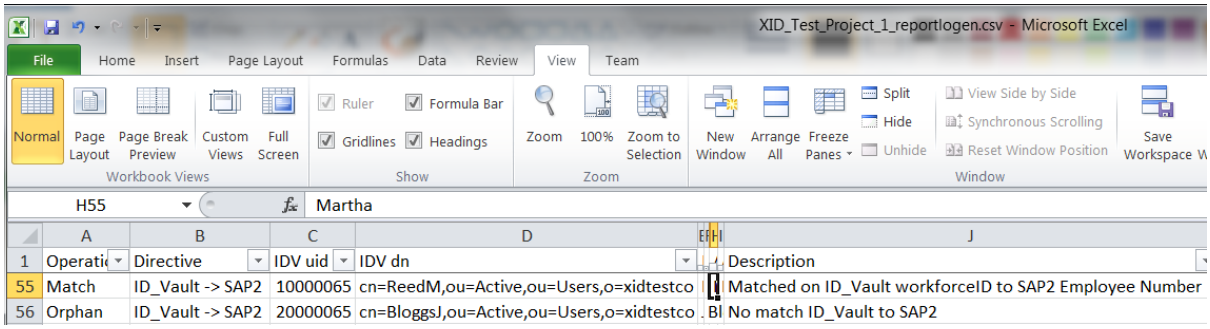
Reserved character	Description	Hex value
	space or # character at the beginning of a string	
	space character at the end of a string	
,	comma	0x2C
+	plus sign	0x2B
"	double quote	0x22
\	backslash	0x5C
<	left angle bracket	0x3C
>	right angle bracket	0x3E
;	semicolon	0x3B
LF	line feed	0x0A
CR	carriage return	0x0D
=	equals sign	0x3D
/	forwards slash	0x2F

XID reports in Microsoft Excel

The output report files can be opened by double clicking the file using Windows Explorer.



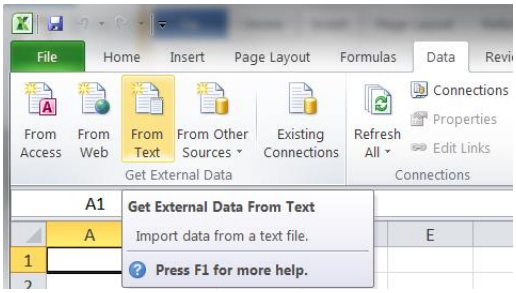
If the delimiter value set in XID matches the list separator in Windows then the report will be displayed with each field occupying a row and column in the spreadsheet application.



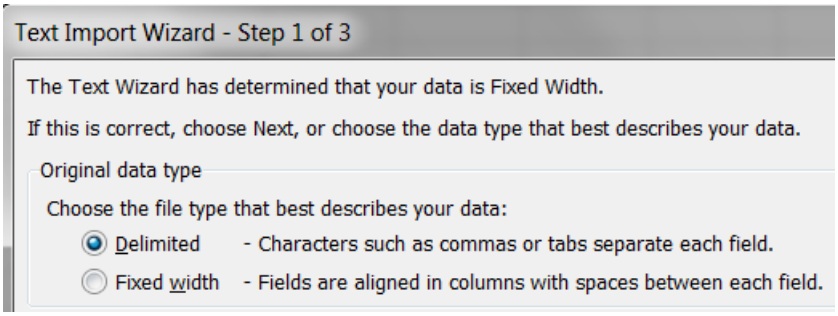
Important: Please ensure to **close** the report spreadsheet before running a new report in XID.

If the XID report is not loading correctly into the spreadsheet application then use the following method to load the information:

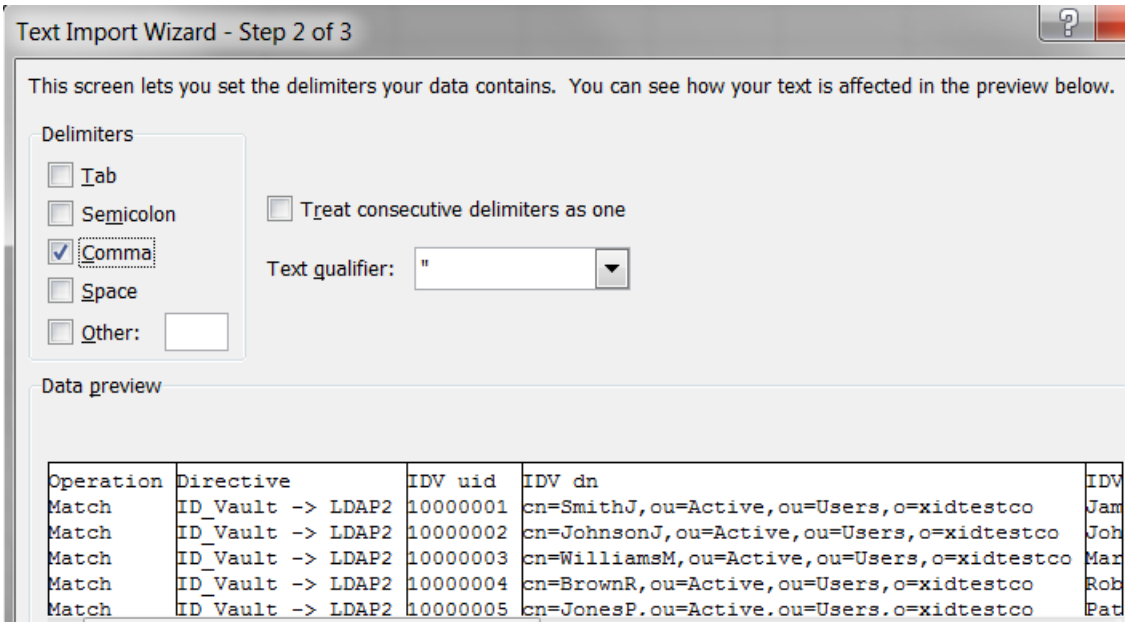
1. Open the spreadsheet application. This example will use Microsoft Excel.
2. Click 'Data' and select 'From Text'.



3. Select the report then click 'Import'.
4. Select 'Delimited' then click 'Next'.



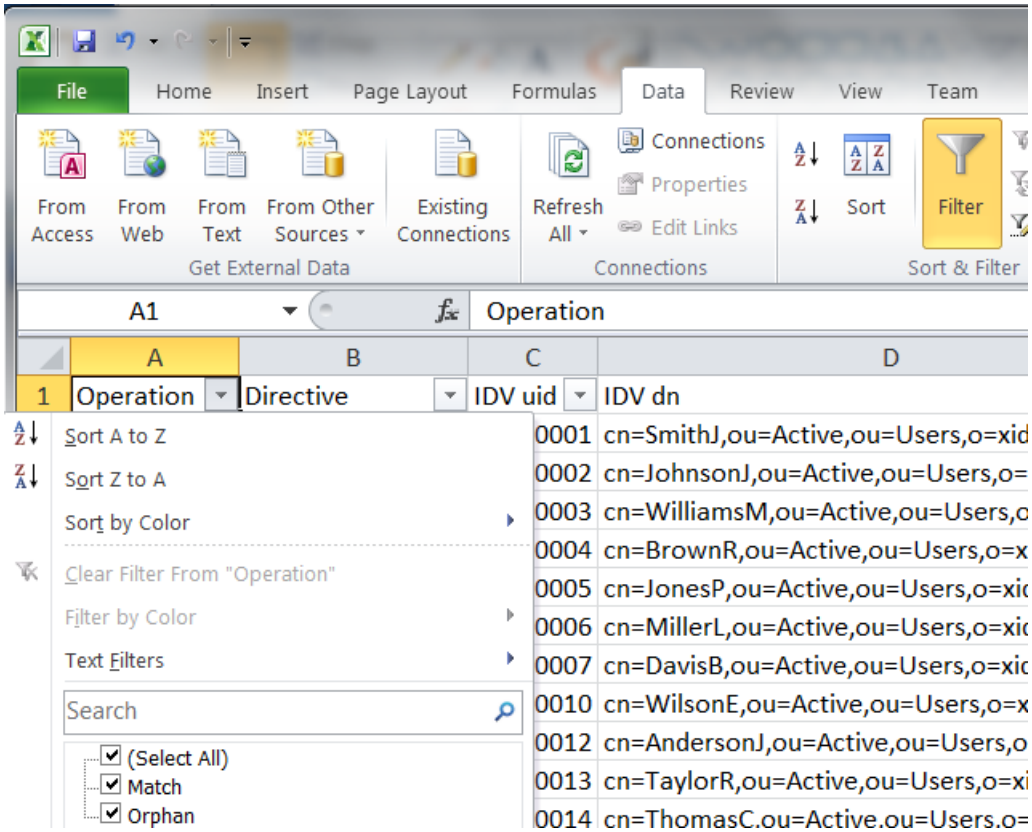
5. Select the delimiter set in XID. The Data preview should display the information in columns as shown in the example.



6. Click ‘Finish’.

Further analysis using Excel

With the report loaded, click 'Filter' in the 'Data' tab.



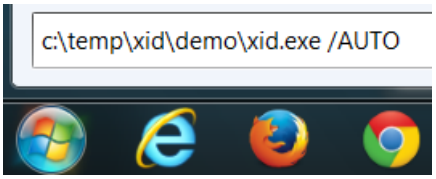
Each report field has a combo box that can be used to select items to be analysed further.

The above example shows that the Orphan rows can be selected exclusively by deselecting 'Match' in the filter drop down of the 'Operation' column.

Important: Please ensure to **close** the report spreadsheet before running a new report in XID.

Starting XID forcing AUTO file detection.

There may be certain circumstances where the XID needs to be started using auto file detection if the project is set to manual detection. A command line parameter '`/AUTO`' can be set to force this condition either at the command prompt or the Windows Start -> Run option as follows:



Troubleshooting

Issue starting XID

Blank Architect Screen

Application configuration not completed

After configuring and saving a project, the applications are not present when restart XID.

If the Application was defined in the matching screen without further configuration in the application configuration to define 'File Info', the project will be aborted and XID will start without that application or applications defined.

Redefine the application and complete at least the 'File Info' section in the application configuration.

Applications disappeared in an existing project

If this is an existing project and the applications have now gone then there could have been an issue with the setup file.

Future versions will have a recovery in this case. A workaround for now is to edit to the 'xid_setup_proj.xml' file as follows:

1. Close XID.
2. Open the 'xid_setup_proj.xml' using a text editor such as Windows notepad. Do not use a Word Processor or Spreadsheet application for this task.

   The XML elements <xid-application-1> to <xid-application-5> will contain a value of 0 for no application configured or 1 to indicate an application has been configured for the corresponding application position in XID.

   The following shows a project for four applications but the xid setup file is indicating that no applications are configured.

```
<xid_version>1</xid_version>
<default_project>1</default_project>
<xid_project projno="2">
<xid_project_Name>XID SAP AD</xid_project_Name>
<xid_cust_Name>XID Test Co</xid_cust_Name>
<xid-proj-path-automan>AUTO</xid-proj-path-automan>
<xid-proj-repout-delim>,</xid-proj-repout-delim>
<xid-proj-file>xid_setup_proj.xml</xid-proj-file>
<xid-application-1>0</xid-application-1>
<xid-application-2>0</xid-application-2>
<xid-application-3>0</xid-application-3>
<xid-application-4>0</xid-application-4>
<xid-application-5>0</xid-application-5>
</xid_project>
```

3. Up the XML elements <xid-application-1> to <xid-application-5> (only update those necessary) changing the value of 0 to a 1 for the application that has been configured for the corresponding application position in the XID project.

```
<xid_version>1</xid_version>
<default_project>1</default_project>
<xid_project projno="2">
<xid_project_Name>XID SAP AD</xid_project_Name>
<xid_cust_Name>XID Test Co</xid_cust_Name>
<xid-proj-path-automan>AUTO</xid-proj-path-automan>
<xid-proj-repout-delim>,</xid-proj-repout-delim>
<xid-proj-file>xid_setup_proj.xml</xid-proj-file>
<xid-application-1>1</xid-application-1>
<xid-application-2>1</xid-application-2>
<xid-application-3>1</xid-application-3>
<xid-application-4>1</xid-application-4>
<xid-application-5>0</xid-application-5>
</xid_project>
```

4. Save the setup file and exit the file editor.
5. Run XID. If the applications have not returned then contact XID support: support@exactidentity.com

Error when running a Report

General I/O error

Check to ensure that all XID files are closed in other applications such as a text editor or spreadsheet. Restart XID.

Error 77

Error 77 is displayed when loading an application when there are an excess of 20 attributes/fields specified to load to memory in the application schema configuration. Edit the application and place an 'X' in the special cell of attributes/fields that are not required for matching or business rule comparison. Continue excluding attributes/fields until the 'Rows Loaded to Memory' value reaches 20 or below.

Error 102, 103

Edit the application and ensure the following are set and correct:

File Info:

- Detect
- Line term
- Input Type
- System File
- CSV delim (if CSV Input Type)

Check that the schema table matches the input file extract.

Contacts

Exact Identity Limited

www.exactidentity.com

Email technical: support@exactidentity.com