Collecting Foreign Security Principals

Via L&G Solution Guide.

Prepared for:
General Team Usage

Version: **2.0**
Issuance Date: 13th July 2016

The Security Division of EMC

Contact Information

RSA	
Professional Services Contact:	Clive Morrish
Mobile:	07732 880 186
E-mail:	Clive.Morrish@rsa.com

Revision History

Rev.	Date	Author(s)	Approver(s)	Description
1	04/02/2016	Clive Morrish		Document created
2				
3				

Table of Contents

1. WHAT ARE FOREIGN SECURITY PRINCIPALS

Within Active Directory (AD) any entity that can be authenticated by the system, such as a user account or computer account is referred to as a *Security Principal.*

Security Principals are directory objects with each being automatically assigned a security identifier (SID) upon creation. Objects with SIDs can log on to the network and can then access domain resources.

When using multiple trusted domains, Foreign Security Principals (FSPs) are created anytime a Security Principal from a trusted domain is added to the local domain. These FSPs are created in the special foreignSecurityPrincipals container and are represented in the directory by the *foreignSecurityPrincipal* objectClass.

The FSP serves as the local representation of a foreign user that can then be added to security groups or used as a local security principal.

Or, more simply, when you add a user from a trusted domain to a group in your domain, AD creates a local object – foreignSecurityPrincipal – to represent this external account. You can essentially think of this object as a pointer/shortcut to the actual account in a trusted domain

2. ISSUE

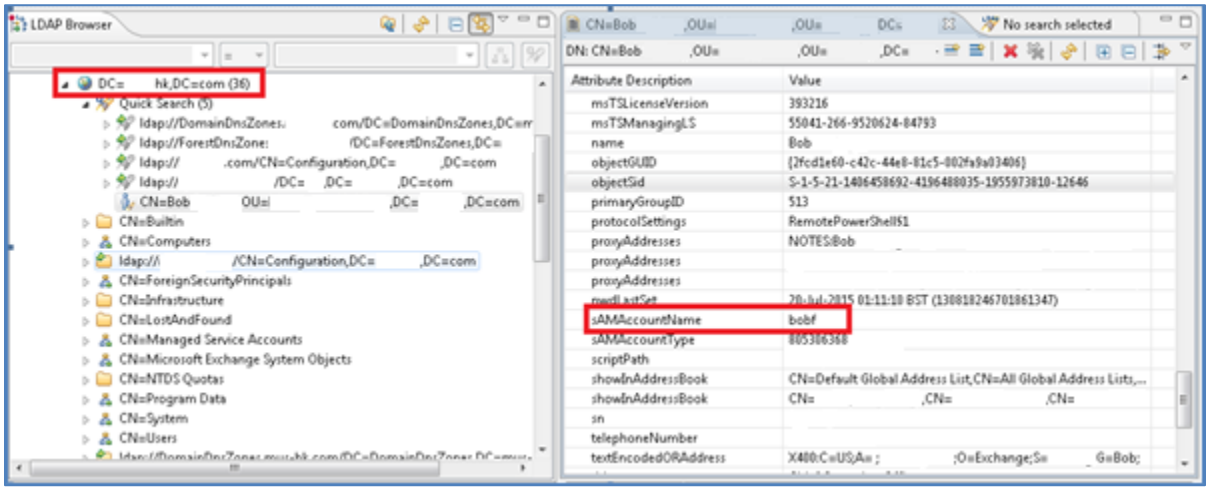
Customer has multiple domains and is using foreign security principals to give access across domains. In order to resolve the account to group relationship we need to collect the "objectSid" value on each account.

Currently, using the AD and LDAP collectors we're unable to collect the objectSID value. However, it does appear when running a 'test'. Without this value we're unable to create the relationship between FSP account and group.

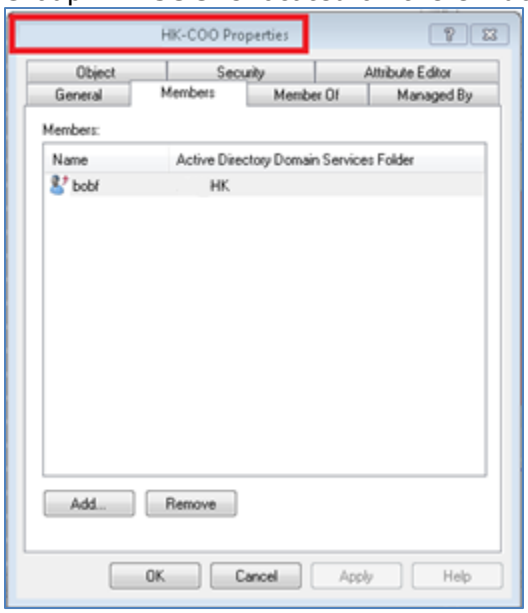
As a result, we aren't capturing accurate representation of group membership as FSPs are being excluded e.g. groups with FSP members were showing as empty.

2.1. Example

User **bobf** exists on the HK domain

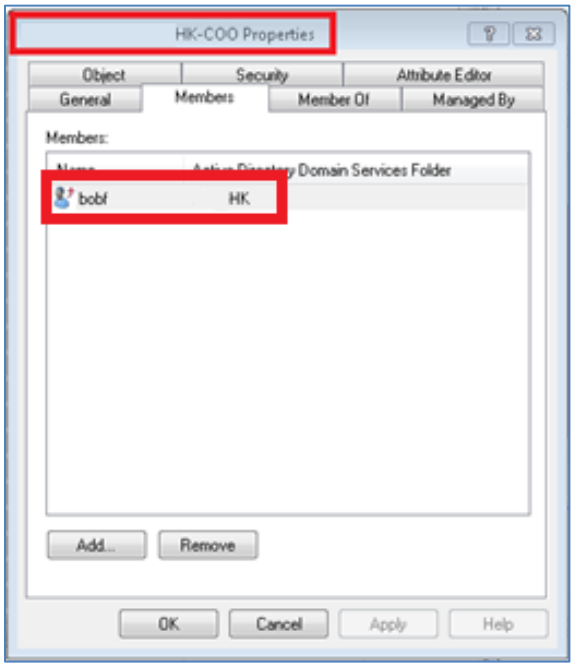


Group **HK-COO** is located on the UK domain

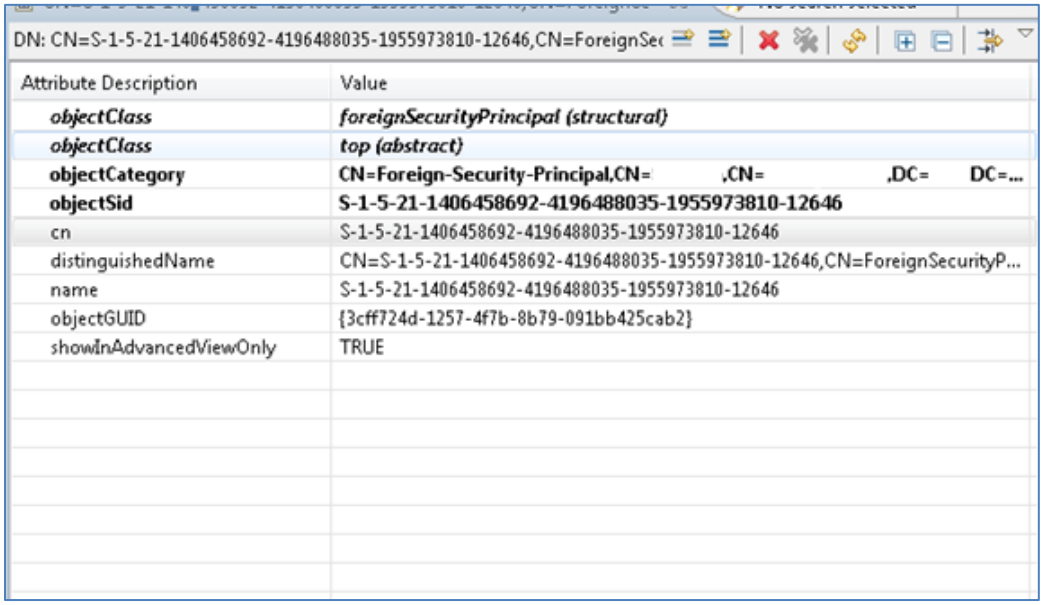


As the relationship between the UK and HK domain is trusted, **bobf** can be assigned membership of the **HK-COO** group

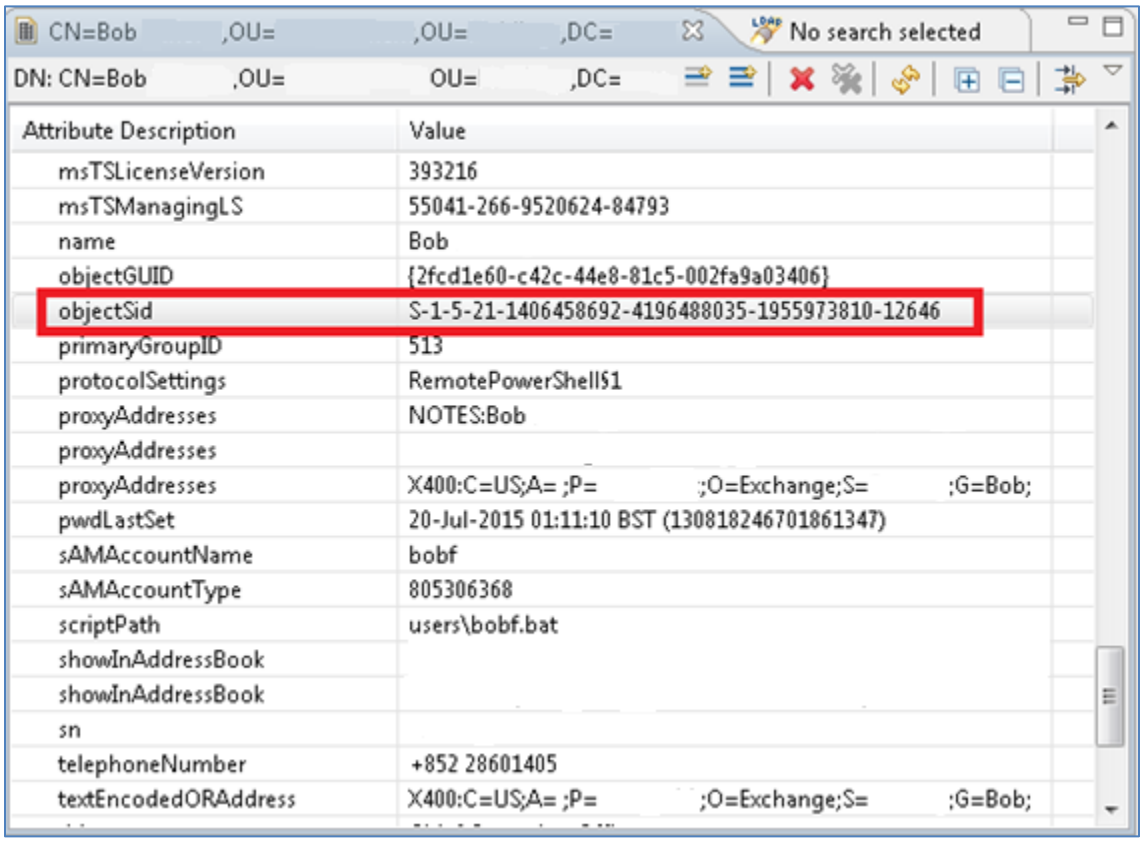
Note: The Red arrow next to the member indicates a foreignSecurityPrincipal



This creates a foreignSecurityPrincipal representing the external account.



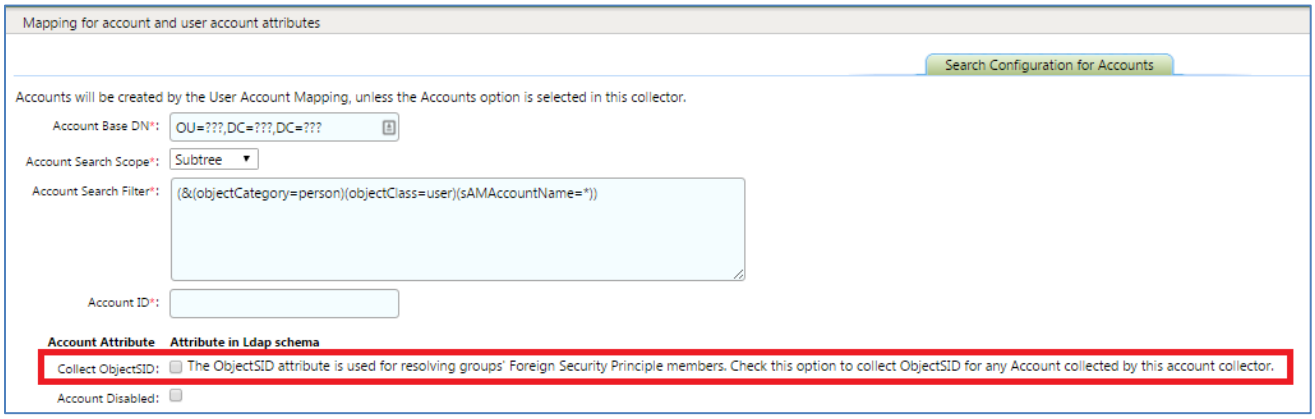
The objectSid can then be used to link the foreignSecurityPrincipal back to the account on the HK domain.

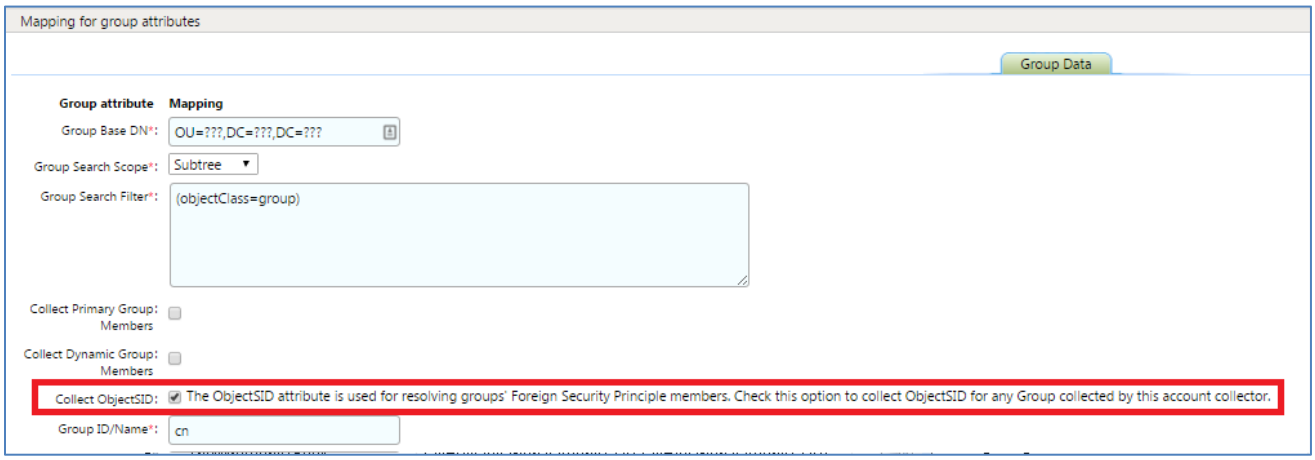


3. FIX

New functionality was added to the product which allows the processing of group members that are a Foreign Security Principal (FSP) within Active Directory.

This requires each Active Directory collector to collect the object SIDs for accounts and groups. To collect the object SIDs, simply select the Collect ObjectSID option.



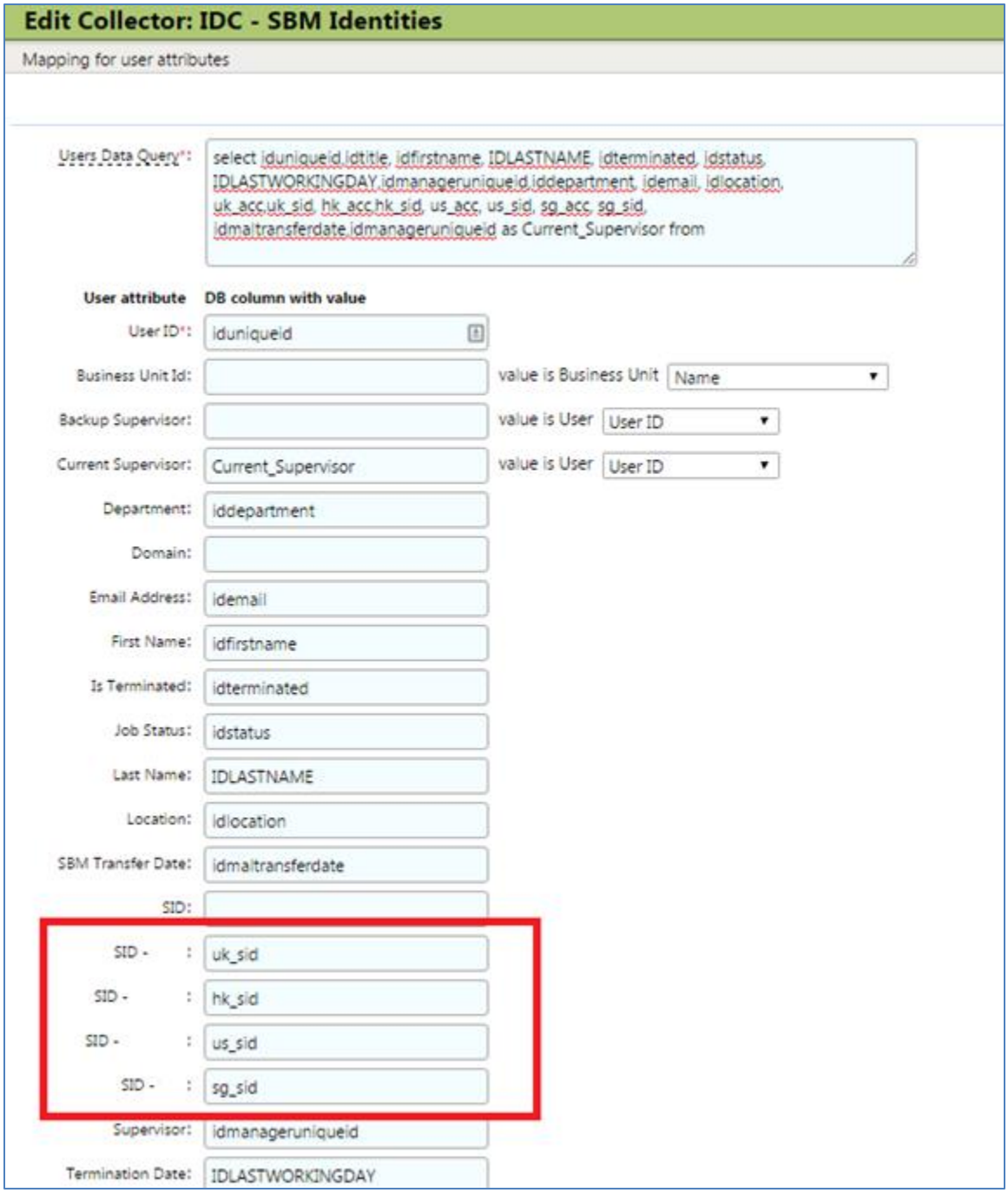


4. SOLUTION

4.1. Update Identity Collector

To enable mapping of the FSP account to an identity, we must collect the SID value at an Identity level.

Identity collector updated to collect SID for all 4 domains.

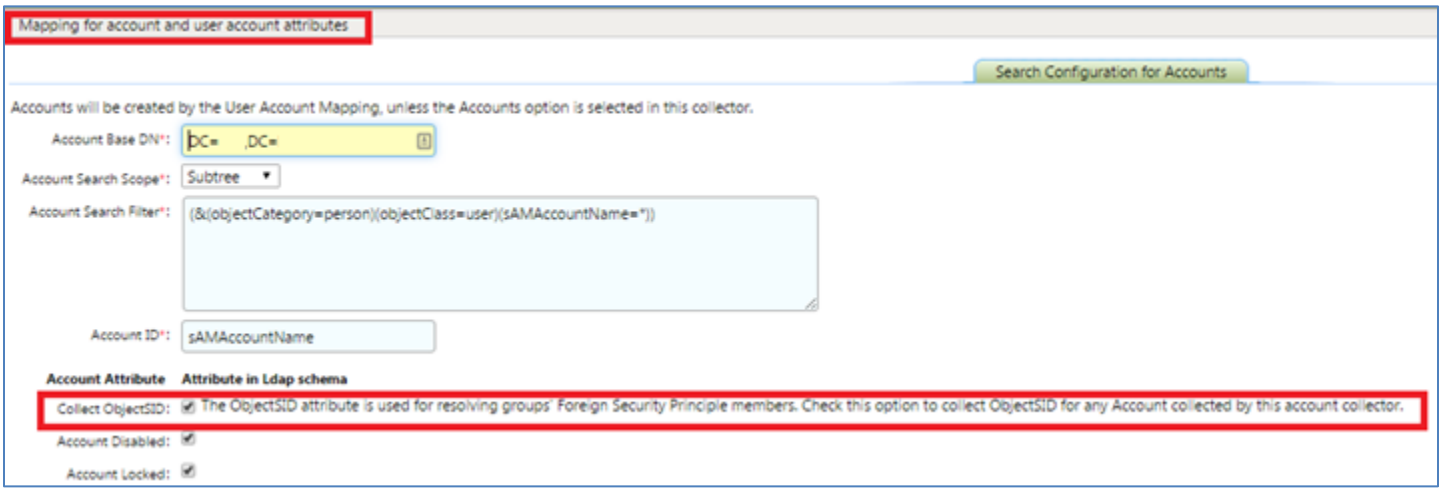


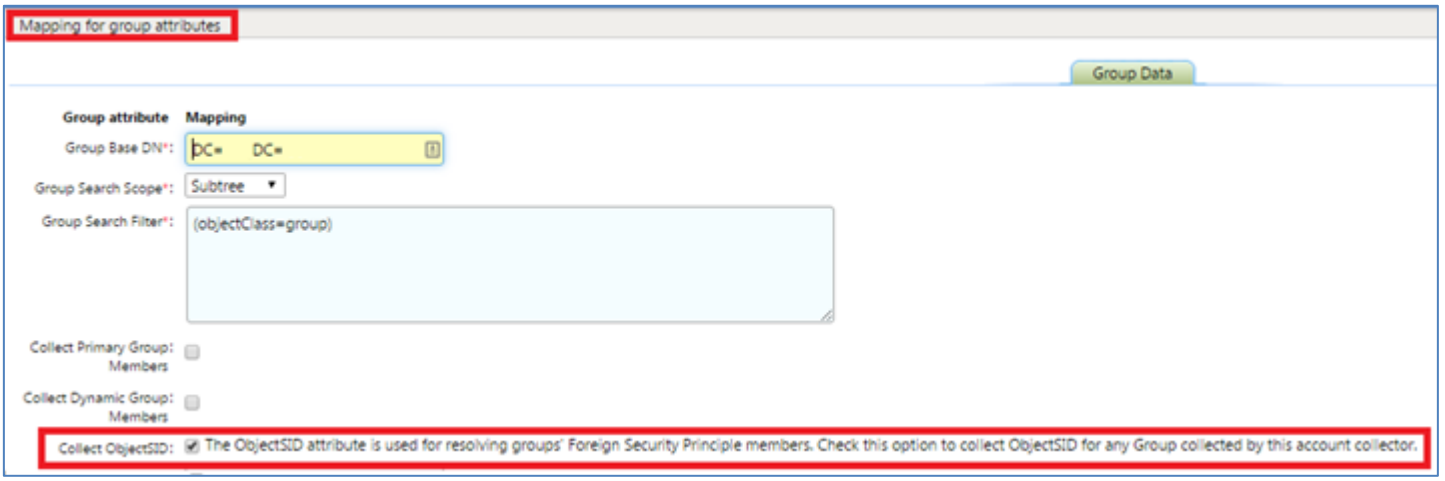
4.2. Update Account Collectors

4.2.1. Collect ObjectSID

For the Account Collectors collecting Accounts, User Account Mappings and Groups the 'Collect ObjectSID' option is selected.

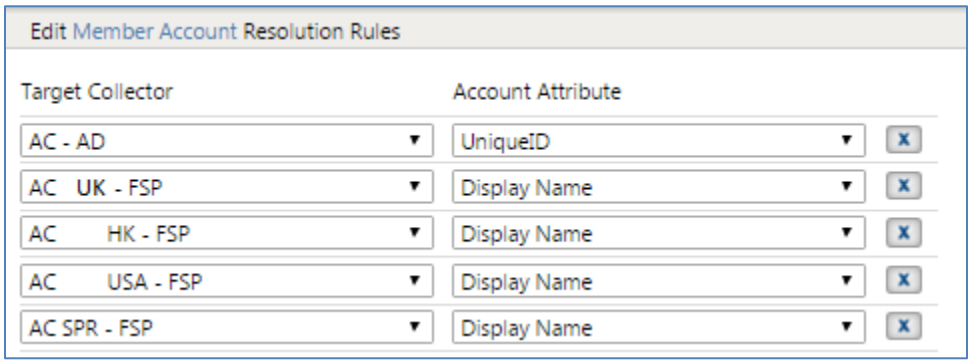
The ObjectSID value is used for resolving groups' Foreign Security Principal members.





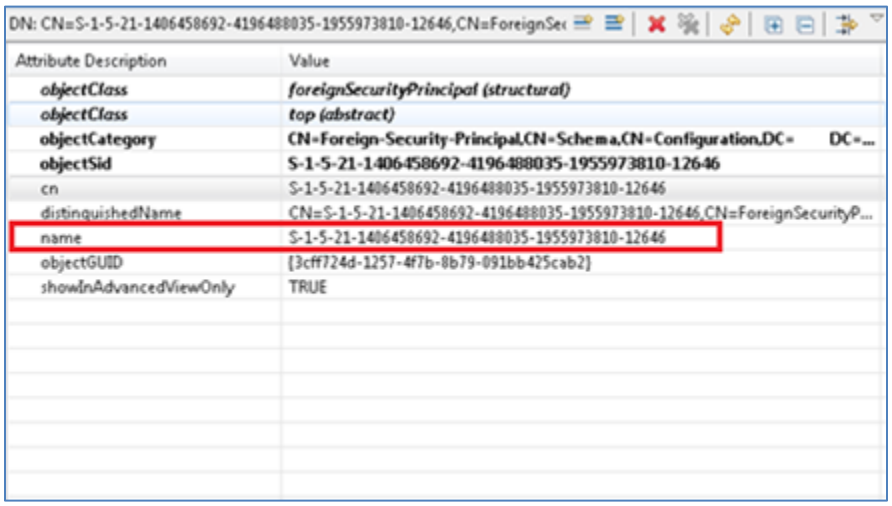
4.2.2. Member Account Resolutions

To correctly represent account memberships in groups, the Member Account Resolution rules are updated with account attributes that identify accounts.

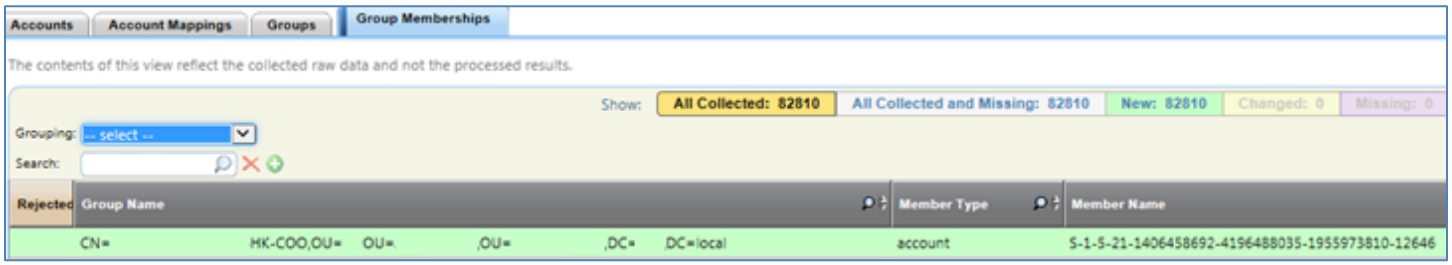


For the normal account collectors, we resolve the accounts on the UniqueID (distinguishedName).

The FSP account collectors (yet to be created) are resolved on the Display Name (name).



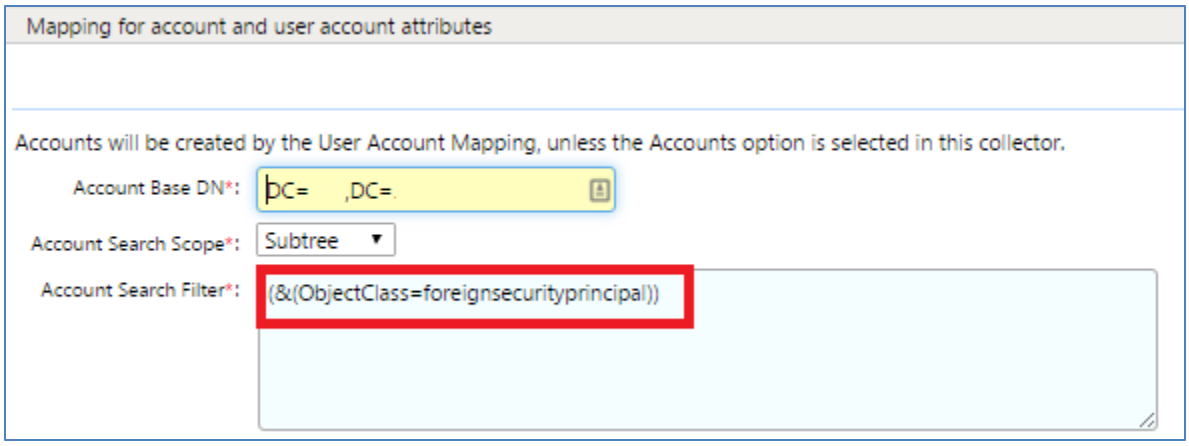
Although the collector has collected in the group membership, the mapping of the account to the group can't happen until the FSP accounts have been collected.



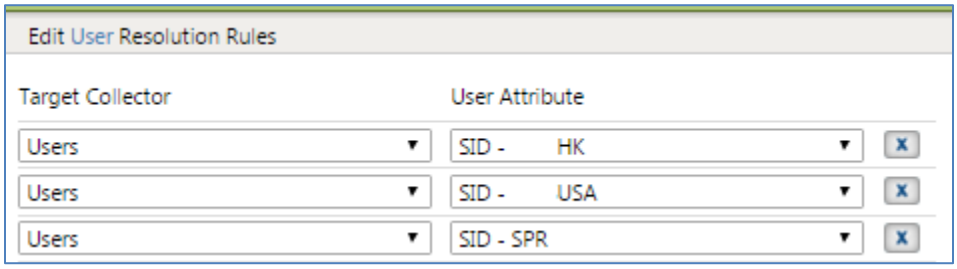
4.3. Create FSP Account Collectors

For each domain, an additional account collector was created just for collecting the FSP accounts. These collectors only collect Accounts and User Account Mappings.

The Account Search Filter is restricted to only those accounts with the ObjectClass 'foreignsecurityprincipal'



The FSP accounts are then linked back to the collected identities on the SID attribute.



4.4. Run Collectors

For the account mapping to be successful, the collectors need to be run in the correct order. For example, the FSP account to group membership can't occur if the groups haven't yet been collected.

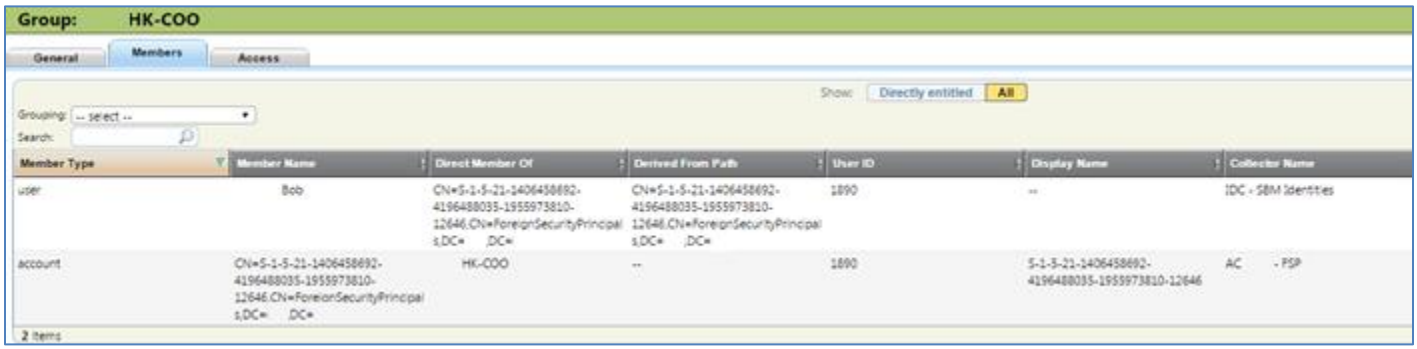
For this implementation, the collectors were required to be run in the following order:

- **Identity Collector**
- **Non FSP Account Collector (All)**
- **FS Account Collector (All)**

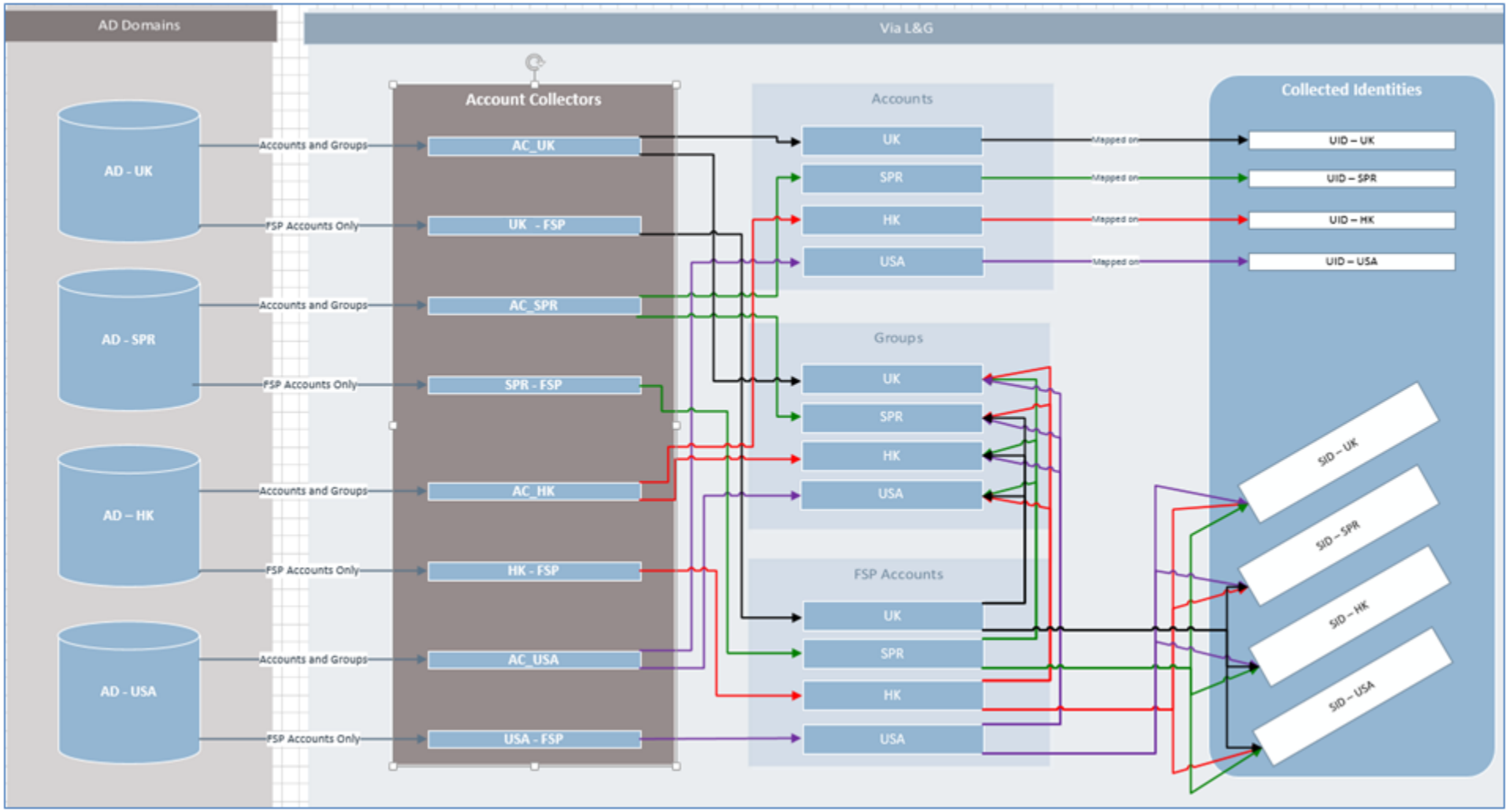
4.5. End Result

Once all collections have successfully completed, the groups containing FSP accounts which were previously empty will now contain members.

From the below screenshot, you can clearly see the FSP account (….12646) is a member of the group HK-COO and is linked to the user **Bob** as per the example set out in step 2.1.



5. PROCESS FLOW



**** END OF DOCUMENT ****