

# Collecting Foreign Security Principals Via L&G Solution Guide.

Prepared for:  
**General Team Usage**

Version: **2.0**  
Issuance Date: 13<sup>th</sup> July 2016



**The Security Division of EMC**

Copyright © 2013 by EMC Corporation. All rights reserved.

## Contact Information

<b>RSA</b>	
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 .....	5
2. ISSUE .....	6
2.1. EXAMPLE.....	6
3. FIX .....	9
4. SOLUTION .....	10
4.1. UPDATE IDENTITY COLLECTOR .....	10
4.2. UPDATE ACCOUNT COLLECTORS.....	11
4.2.1. <i>Collect ObjectSID</i> .....	11
4.2.2. <i>Member Account Resolutions</i> .....	12
4.3. CREATE FSP ACCOUNT COLLECTORS .....	13
4.4. RUN COLLECTORS .....	13
4.5. END RESULT .....	14
5. PROCESS FLOW.....	15

## 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

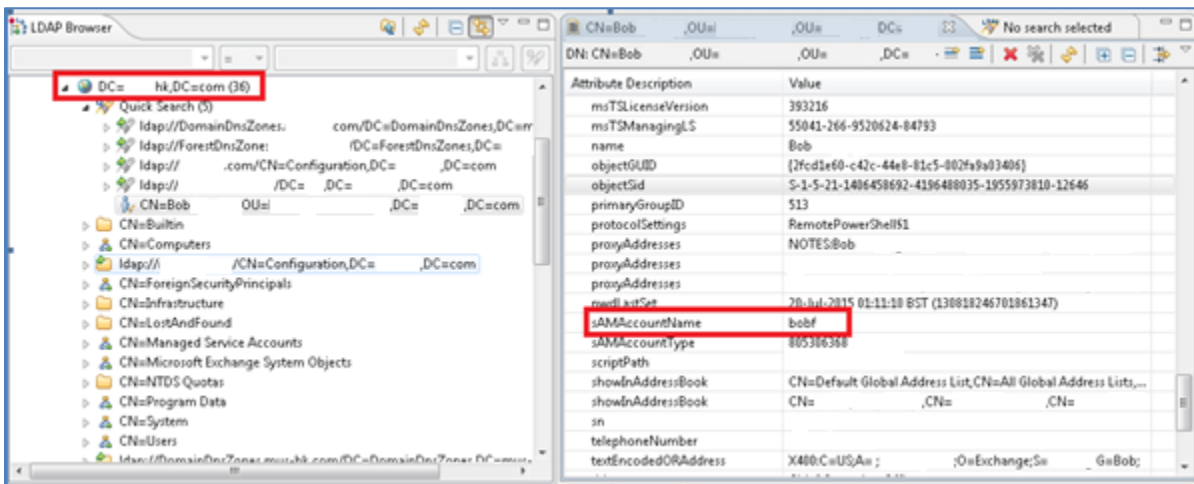
Customer has multiple domains and is using foreign security principals to give access across domains. In order to resolve the account to group relationship we need to collect the "objectSid" value on each account.

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.

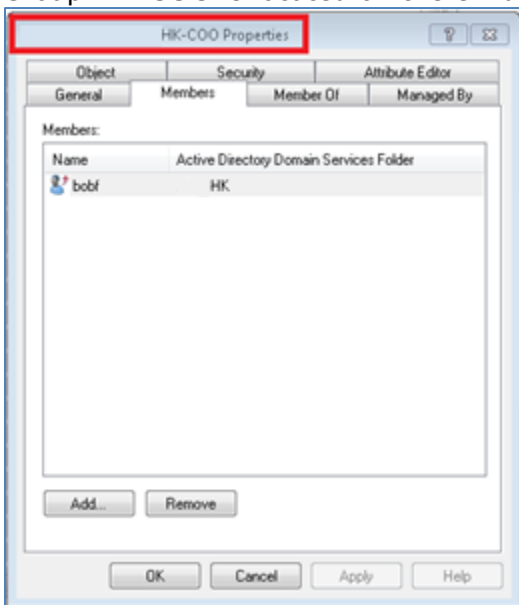
As a result, we aren't capturing accurate representation of group membership as FSPs are being excluded e.g. groups with FSP members were showing as empty.

### 2.1. Example

User **bobf** exists on the HK domain

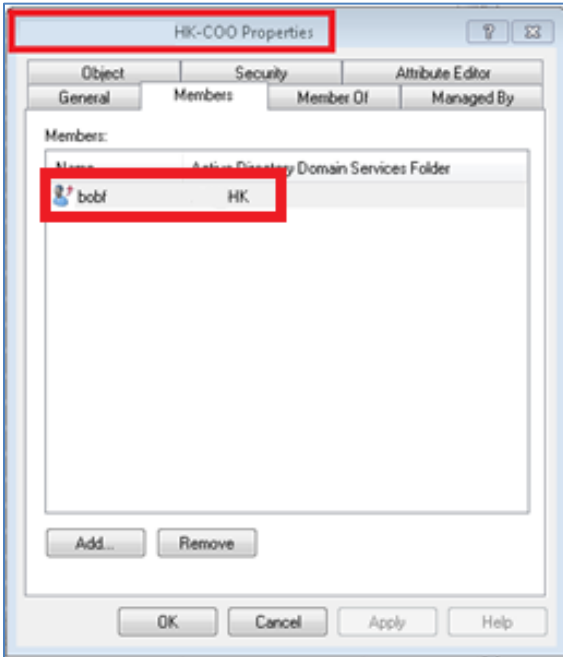


Group **HK-COO** is located on the UK domain



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 screenshot shows the Active Directory user properties for 'bobf'. The 'objectClass' is 'foreignSecurityPrincipal (structural)'. The 'objectCategory' is 'CN=Foreign-Security-Principal,CN=,CN=,DC= DC=...'. The 'objectSid' is 'S-1-5-21-1406458692-4196488035-1955973810-12646'. The 'cn' is 'S-1-5-21-1406458692-4196488035-1955973810-12646'. The 'distinguishedName' is 'CN=S-1-5-21-1406458692-4196488035-1955973810-12646,CN=ForeignSecurityP...'. The 'name' is 'S-1-5-21-1406458692-4196488035-1955973810-12646'. The 'objectGUID' is '{3cff724d-1257-4f7b-8b79-091bb425cab2}'. The 'showInAdvancedViewOnly' is 'TRUE'.

Attribute Description	Value
objectClass	foreignSecurityPrincipal (structural)
objectClass	top (abstract)
objectCategory	CN=Foreign-Security-Principal,CN=,CN=,DC= DC=...
objectSid	S-1-5-21-1406458692-4196488035-1955973810-12646
cn	S-1-5-21-1406458692-4196488035-1955973810-12646
distinguishedName	CN=S-1-5-21-1406458692-4196488035-1955973810-12646,CN=ForeignSecurityP...
name	S-1-5-21-1406458692-4196488035-1955973810-12646
objectGUID	{3cff724d-1257-4f7b-8b79-091bb425cab2}
showInAdvancedViewOnly	TRUE

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

The screenshot shows the Active Directory user properties for 'Bob'. The 'objectSid' attribute is highlighted with a red box. The table below represents the data shown in the screenshot.

Attribute Description	Value
msTSLicenseVersion	393216
msTSMManagingLS	55041-266-9520624-84793
name	Bob
objectGUID	{2fcd1e60-c42c-44e8-81c5-002fa9a03406}
objectSid	S-1-5-21-1406458692-4196488035-1955973810-12646
primaryGroupID	513
protocolSettings	RemotePowerShell\$1
proxyAddresses	NOTES:Bob
proxyAddresses	X400:C=US;A= ;P= ;O=Exchange;S= ;G=Bob;
pwdLastSet	20-Jul-2015 01:11:10 BST (130818246701861347)
sAMAccountName	bobf
sAMAccountType	805306368
scriptPath	users\bobf.bat
showInAddressBook	
showInAddressBook	
sn	
telephoneNumber	+852 28601405
textEncodedORAddress	X400:C=US;A= ;P= ;O=Exchange;S= ;G=Bob;



### 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.

Mapping for account and user account attributes

Search Configuration for Accounts

Accounts will be created by the User Account Mapping, unless the Accounts option is selected in this collector.

Account Base DN\*:

Account Search Scope\*:

Account Search Filter\*:

Account ID\*:

Account Attribute	Attribute in Ldap schema
Collect ObjectSID: <input type="checkbox"/>	The ObjectSID attribute is used for resolving groups' Foreign Security Principle members. Check this option to collect ObjectSID for any Account collected by this account collector.
Account Disabled: <input type="checkbox"/>	

Mapping for group attributes

Group Data

**Group attribute**    **Mapping**

Group Base DN\*:

Group Search Scope\*:

Group Search Filter\*:

Collect Primary Group:  Members

Collect Dynamic Group:  Members

Collect ObjectSID: <input checked="" type="checkbox"/>	The ObjectSID attribute is used for resolving groups' Foreign Security Principle members. Check this option to collect ObjectSID for any Group collected by this account collector.
--	---

Group ID/Name\*:

## 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.

**Edit Collector: IDC - SBM Identities**

Mapping for user attributes

Users Data Query\*: 

```
select iduniqueid, idtitle, idfirstname, IDLASTNAME, idterminated, idstatus, IDLASTWORKINGDAY, idmanageruniqueid, iddepartment, idemail, idlocation, uk_acc, uk_sid, hk_acc, hk_sid, us_acc, us_sid, sg_acc, sg_sid, idmaltransferdate, idmanageruniqueid as Current_Supervisor from
```

User attribute	DB column with value
User ID*	iduniqueid
Business Unit Id:	value is Business Unit <input type="text" value="Name"/>
Backup Supervisor:	value is User <input type="text" value="User ID"/>
Current Supervisor:	Current_Supervisor value is User <input type="text" value="User ID"/>
Department:	iddepartment
Domain:	
Email Address:	idemail
First Name:	idfirstname
Is Terminated:	idterminated
Job Status:	idstatus
Last Name:	IDLASTNAME
Location:	idlocation
SBM Transfer Date:	idmaltransferdate
SID:	
SID -	uk_sid
SID -	hk_sid
SID -	us_sid
SID -	sg_sid
Supervisor:	idmanageruniqueid
Termination Date:	IDLASTWORKINGDAY

## 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.

**Mapping for account and user account attributes** Search Configuration for Accounts

Accounts will be created by the User Account Mapping, unless the Accounts option is selected in this collector.

Account Base DN\*:  ⓘ

Account Search Scope\*:

Account Search Filter\*:

Account ID\*:

**Account Attribute** **Attribute in Ldap schema**

Collect ObjectSID:  The ObjectSID attribute is used for resolving groups' Foreign Security Principle members. Check this option to collect ObjectSID for any Account collected by this account collector.

Account Disabled:

Account Locked:

**Mapping for group attributes** Group Data

**Group attribute** **Mapping**

Group Base DN\*:  ⓘ

Group Search Scope\*:

Group Search Filter\*:

Collect Primary Group:  Members

Collect Dynamic Group:  Members

Collect ObjectSID:  The ObjectSID attribute is used for resolving groups' Foreign Security Principle members. Check this option to collect ObjectSID for any Group collected by this account collector.

### 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.

Target Collector	Account Attribute
AC - AD	UniqueID
AC UK - FSP	Display Name
AC HK - FSP	Display Name
AC USA - FSP	Display Name
AC SPR - FSP	Display Name

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).

Attribute Description	Value
objectClass	foreignSecurityPrincipal (structural)
objectClass	top (abstract)
objectCategory	CN=Foreign-Security-Principal,CN=Schema,CN=Configuration,DC=...
objectSid	S-1-5-21-1406458692-4196488035-1955973810-12646
cn	S-1-5-21-1406458692-4196488035-1955973810-12646
distinguishedName	CN=S-1-5-21-1406458692-4196488035-1955973810-12646,CN=ForeignSecurityP...
name	S-1-5-21-1406458692-4196488035-1955973810-12646
objectGUID	{3cff724d-1257-4f7b-8b79-091bb425cab2}
showInAdvancedViewOnly	TRUE

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.

Rejected	Group Name	Member Type	Member Name
	CN= HK-COO,OU= ,OU= ,DC= DC=local	account	S-1-5-21-1406458692-4196488035-1955973810-12646

### 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'

Mapping for account and user account attributes

Accounts will be created by the User Account Mapping, unless the Accounts option is selected in this collector.

Account Base DN\*: DC= ,DC=

Account Search Scope\*: Subtree

Account Search Filter\*: (&(ObjectClass=foreignsecurityprincipal))

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

Target Collector	User Attribute
Users	SID - HK
Users	SID - USA
Users	SID - SPR

### 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

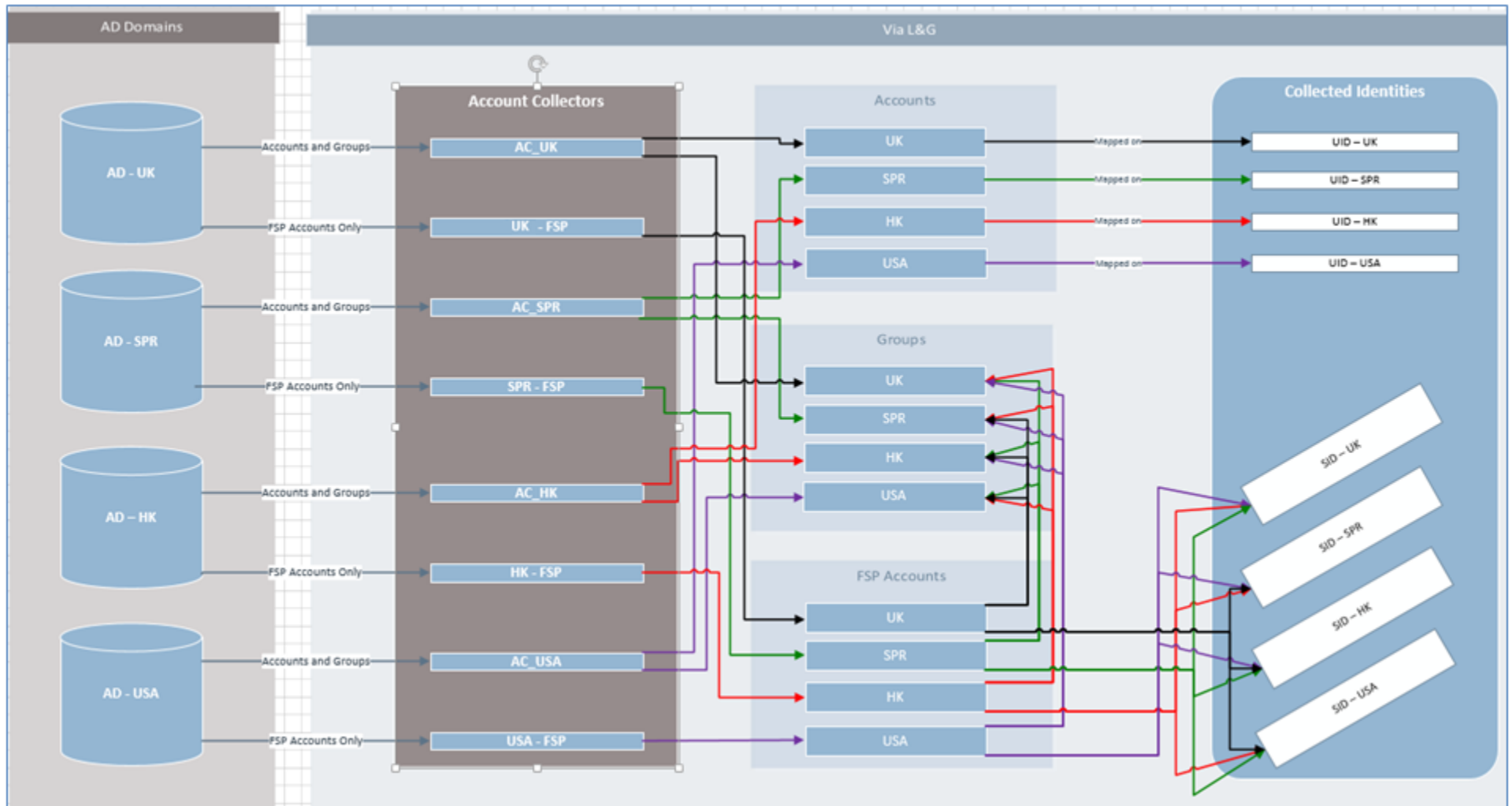
Once all collections have successfully completed, the groups containing FSP accounts which were previously empty will now contain members.

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.

Member Type	Member Name	Direct Member Of	Derived From Path	User ID	Display Name	Collector Name
user	Bob	CN=5-1-5-21-1406458692-4196488035-1955973810-12646.CN=ForeignSecurityPrincipal.s,DC=.DC=	CN=5-1-5-21-1406458692-4196488035-1955973810-12646.CN=ForeignSecurityPrincipal.s,DC=.DC=	1890	--	IDC - SEM Identities
account	CN=5-1-5-21-1406458692-4196488035-1955973810-12646.CN=ForeignSecurityPrincipal.s,DC=.DC=	HK-COO	--	1890	5-1-5-21-1406458692-4196488035-1955973810-12646	AC - FSP

2 items

## 5. PROCESS FLOW



**\*\* END OF DOCUMENT \*\***