AD data source configuration

Contents

Overview

Swivel carries out a **Read Only** lookup of the AD server using LDAP so no information is written to the AD server and there is no software to install on the AD server. Each Swivel instance must be configured separately.

Also see the Active Directory FAQ

The following steps are required for AD Configuration:

- On the AD server create distribution or security groups and populate with users
- On the AD server create a service account for Swivel to use
- On the Swivel server create an AD Repository
- On the Swivel server configure the Repository Groups
- On the Swivel server configure Transport Attributes
- On the Swivel server configure Transport Groups
- On the Swivel server Synchronise the AD Users

Swivel reads users from Containers (CN), groups in AD, and nested groups, but not directly from containers (OU). It is not possible to traverse domains unless Global Catalog is used, or Swivel reads that domain.

For further information on LDAP data sources see the LDAP How to Guide

Prerequisites

Swivel 3.x system

Repository Configuration Importing users from External Sources

AD configuration checks

Ensure network connectivity from the Swivel server to the AD server for LDAP

Check AD Groups exist

Check Swivel error logs for messages

Check Service account username and password

Use and LDAP browser to confirm the LDAP path (Swivel 3.6 has a built in LDAP browser)

Ensure Transport Attribute is correct in Transport\Attributes, this is usually mail for SMTP and mobile for SMS by Cell Phone.

If SMTP is to be used, ensure SMTP gateway has been configured under Servers/SMTP

Swivel can read the Global Catalog if this is configured on the AD server, this saves each appliance having to be connected to individually. The Global Catalog port must be configured and the Swivel server must connect to the Global Catalog server.

Configuring A/A instances of Swivel

Each instance of Swivel should be configured separately. The following should be noted:

- Ensure Synchronisation with AD occurs at different times on each Swivel instance with a suitable gap between synchronisations.
- Ensure that the configuration of each virtual or hardware appliance is the same as incorrect configuration can lead to users being removed/added and PIN numbers resent. Specifically check Repository Groups and Transports are the same on the Primary and Standby.
- Under Transport General it is recommended to disable **Resend credentials if destination changes:** by setting it to No. (This option removed in Swivel 3.9.6).

Configuring multiple AD repositories

- Where multiple AD sources are used, ensure that the SAM account name (**sAMAccountName**) is different for the sources. It may be useful to use the User Principal name (**userPrincipalName**) instead.

Active Directory Server Configuration Steps

There is no software to install on the AD server, and Swivel reads AD groups. For multiple AD Domains create the required groups on each domain, or use a global catalog server.

Create the Active Directory Groups

Users are added to Active Directory (AD) groups to allow them access to differing authentication resources. By creating additional AD groups different configurations can be made to suit the required environment. Existing groups can be used. The following documentation assumes the following configuration:

Swivel Users - who have access to all authentication methods

Swivel Administrators ? who have access to all authentication methods and admin rights

On the AD server:

Create a Swivel Organizational Unit (OU) Right Click on the domain then select New and then OU, enter the name Swivel

Within the Swivel OU create a Swivel Admin Group (CN) Right click on the Swivel OU then select New Group, enter the name Swivel Admin

Within the Swivel OU create a Swivel Users Group (CN) Right click on the Swivel OU then select New Group, enter the name Swivel Users

Note: Ensure that Distribution or Security Groups are used and not an OU, as Swivel cannot directly read an OU. Swivel will not read users in CN=Users,DC=domain,DC=com

Add users to the Active Directory Groups

On the AD server:

Add users to the Swivel Users and Swivel Admin group as appropriate. Ensure users have the correct information for transport, i.e. an email address and mobile phone number. It is recommended to test with a small number of users first to ensure all settings such as transports etc are correct.

NOTE: Swivel cannot handle primary groups or group membership that refers to trusted domains. These relationships are handled by Active Directory in a non-standard way that standard LDAP queries cannot discover. Do not use groups that are configured as primary groups for any user within Swivel , and do not use groups that contain users from trusted domains. If you need to include user from other domains, use Global Catalog as described above.

Swivel Server Configuration Steps

Configure SMTP Server Settings

On the Swivel server:

Select Server then SMTP, enter the IP address/Hostname of the SMTP gateway

click Apply to save the settings

Add the AD Repository Servers

On the Swivel Server:

Select Repository/General and create an Active Directory Repository, the name is descriptive and must be unique and up to 32 characters in length, and when created it should appear on the left hand side below Repository. Create additional Swivel servers for each AD Domain, or use a global catalog server.

Click Apply to save settings

Configure the AD Repository Server Settings

On the Swivel Server Administration Console:

Select Repository then the required AD server, its name will be that defined in the step above for adding the AD repository.

The following information needs to be entered on each AD Repository Configuration

- Hostname/IP address of AD Server
- Service Account User Name
- Service Account Password

Do not configure Synchronization schedule at this stage.

For further details see AD Repository Configuration Settings below.

Click Apply to save settings.

For information on changing AD Credentials see AD Credential Change How to Guide

Create Swivel Groups

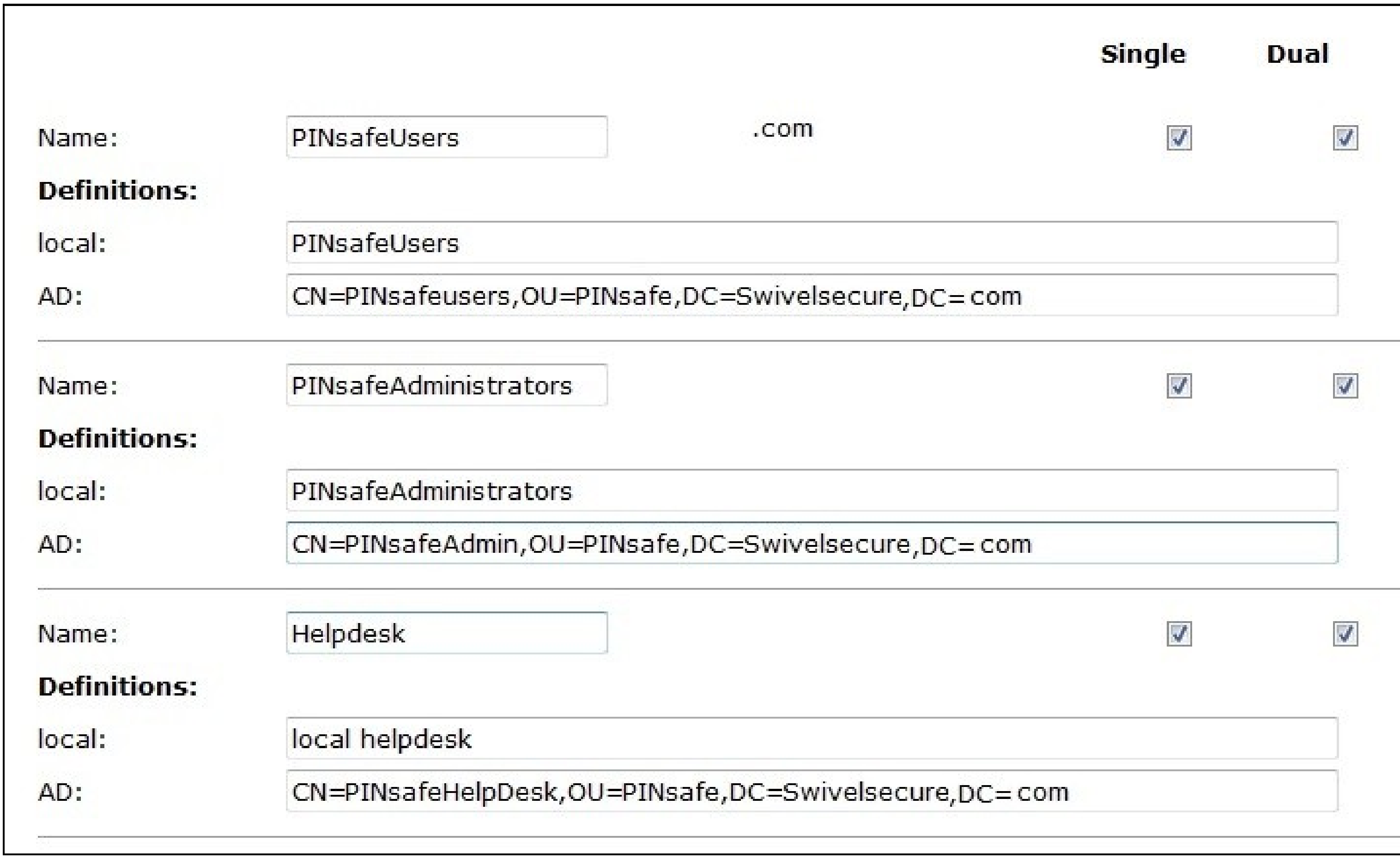
On the Swivel Server:

Select Repository/Groups and enter the Repository Group names corresponding to those created in Active Directory. Leave the fields blank that are not required. The input fields are case sensitive. Use an LDAP browser if unsure of the path, or if using Swivel 3.6 or higher use the inbuilt LDAP browser.

The format must be:

CN=<AD Container>,OU=<Organizational Unit>,DC=<mydomain>,DC=<com>

Example: CN=Swivel Admin,OU=Swivel,DC=swivelsecure,DC=com



			Single	Dual
Name:	PINsafeUsers	.com	☑	☑
Definitions:				
local:	PINsafeUsers			
AD:	CN=PINsafeusers,OU=PINsafe,DC=Swivelsecure,DC= com			
Name:	PINsafeAdministrators		☑	☑
Definitions:				
local:	PINsafeAdministrators			
AD:	CN=PINsafeAdmin,OU=PINsafe,DC=Swivelsecure,DC= com			
Name:	Helpdesk		☑	☑
Definitions:				
local:	local helpdesk			
AD:	CN=PINsafeHelpDesk,OU=PINsafe,DC=Swivelsecure,DC= com			

Configure Transport Attributes

On the Swivel Server:

Select Transport then Attributes. Ensure the settings are correct for each AD repository, usually:

- mobile for mobile phone
- mail for email

Other fields that are used may be telephoneNumber

For further information see Transport_Attribute

Configuring Transport Groups

Assign the AD groups to the required Transport class, the following Transport attributes are used for assigning groups:

- Group: Where security strings are sent to
- Alert Repository Group: Where information is sent regarding the user such as PIN numbers

For further information see Transport_Configuration

Sync the AD Database

On the Swivel Administration console, select User Admin and from the Repository drop down menu select the required AD server name then click on "User Sync". Users from the AD repository should appear. See also User Synchronisation.

Enable Automatic AD Synchronisation

If all the synchronisation is working as fully expected, the Swivel server can now be configured to automatically read the AD server at regular intervals. It is recommended that synchronisation should be configured once per hour. If an A/A pair is configured to synchronise then each Swivel instance must synchronise at differing times. See also User Synchronisation.

On the Swivel Server:

Select Repository then the required AD server. Set the required Synchronisation Schedule. For custom schedules see Schedule.

Click Apply to save the settings

AD Repository Configuration Settings

AD Import Information on the Swivel server is required as follows:

Repository Domain Qualifier: AD Domain name, this is used with the **Add domain qualifier:**

Reformat Phone Number: Yes No When the phone number is imported then Swivel will carry out some basic formatting as determined by the prefix to remove and add. Swivel will also remove extraneous characters and white spaces.

Prefix to remove: Swivel will remove a prefix from the phone number

Prefix to add: Swivel will add a prefix to the phone number, this could be for instance a country code.

Hostname/IP: AD server name, or entering an AD domain will pick up available AD server. If an AD replica is used, be aware that it may take some time for user information to be pushed out to replica AD servers. For redundancy an active directory with a Virtual IP or DNS can be used. Additionally two Swivel servers could be used, but ensure that they synchronise at differing times.

Username: AD service account, usually it is best to use a fully qualified domain name e.g. swivel@swivelsecure.com. The user needs to have permission to connect and bind using LDAP to the AD server.

Password: AD service account password, ensure that password ageing is not set or it is changed regularly

Allow self-signed certificates: Yes No Are certificates used on the AD server?

Username attribute: The username that the AD account reads. By default this is the SAM Account name, **sAMAccountName** for example; bob. It is possible to use the User Principle Name **userPrincipalName** so that the user has to enter their full username, for example bob@swivelsecure.com, users would need to enter this full address to authenticate. It is also possible to use the email address of a user by setting the Username attribute to **mail**. Note that this should be set during initial configuration, if the attribute is changed, then new users will be created with this different username and the old users deleted.

PIN attribute: Swivel can read an AD LDAP attribute that contains the users first PIN number, this AD LDAP attribute can be added here. It is not recommended to have a default PIN, but instead to use a randomly generated PIN that is sent to the user.

Password attribute: Swivel can read an AD LDAP attribute that contains the users first password, this AD LDAP attribute can be added here. It is not recommended to have a default password, but instead to use a randomly generated Password that is sent to the user. Note this is not the AD password but a Swivel password.

Import disabled state: Yes No Default: No. If the account is disabled in AD, should it be disabled or enabled when imported into Swivel. Contractors and 3rd parties can be configured as disabled so they cannot login to AD, but may still authenticate using Swivel.

Import disabled users: Yes No Default: No. If the account is disabled in AD, should it be imported into Swivel.

Ignore FQ name changes: Yes No Default: Yes. Changes to the AD infrastructure can lead to users account being deleted and re-created, users see this as new PIN numbers being generated. To stop this occurring Swivel can be set to ignore these changes.

Reformat Phone Number: Yes No Default: No. Reformat the mobile phone number using the fields **Prefix to remove:** or **Prefix to add:**

Mark missing users as deleted: Yes No If a user is deleted from the AD group that Swivel references, Swivel can mark it as deleted without actually deleting the account. If it is reinstated, then the user can be undeleted/restored in Swivel, and the user will retain their current PIN and security strings.

Port: 389 (Domain LDAP) 636 (Domain LDAP SSL) 3268 (Global Catalog LDAP) 3269 (Global Catalog LDAP SSL) Select the required port for communication.

Add domain qualifier: None Prefix Suffix When the user is imported from Active Directory into Swivel , the AD domain qualifier can be added either as a prefix or suffix to the username, or not used. For example a user imported from ad as *bob* may have the suffix @swivelsecure.com added and stored in Swivel as bob@swivelsecure.com.

Synchronization schedule: Choose how often Swivel will synchronise with the AD server. Note: an immediate synchronisation can be performed from the User Admin Screen

Check Password With Repository

It is possible for Swivel to check the AD password with some access devices. For Active Directory The username must be passed to AD as username@domain in order to authenticate via LDAP. This can be specified by using the the administrator or service account username for the repository configuration as administrator@domain.name, rather than just administrator or service account username, Swivel will automatically append the domain to the username when authenticating to AD, if one is not specified.

The AD domain used for Check Password with Repository is taken from the AD configuration. If it is authenticating with a different domain or sub domain the Check password with Repository may fail. Verify using the debug log. Also see Password How to Guide

Upgrading from Active Directory on a 2003 server to a 2008 server

Swivel supports Active Directory on 2008 Server

When upgrading from a 2003 to a 2008 server, ensure that the BaseDN remains the same. or you will encounter issues when attempting to sync. Specifically, it would be trying to look for the old FQDN and then abort. If you intend to change the BaseDN then you can avoid this issue by upgrading to the latest version of Swivel before migrating to AD 2008. The latest version would attempt to find the user elsewhere in the directory when performing a user sync if the BaseDN had changed, thus avoiding the abort issue.

Limiting users in a Repository

Swivel does not limit the number of users in a repository, but it may be possible to limit the number of users in the source group, see Active Directory Quotas

Additional Tools

Powershell commands

Powershell supports the use of commands to view AD details and may be of use in configuring Swivel, and are provided here for reference.

```
Import-Module activedirectory
```

```
get-aduser -Identity theadusername
```

```
get-aduser -Identity theadusername -properties *
```

Swivel log AD Error Messages

Repository "Active Directory", cannot be added to the database: possibly already exists.

This error can occur if the repository name already exists or the Database is still set to shipping mode. The repository "local" can be used but will also generate this error but can be ignored.

Exception occured during repository group member query, group: CN=SwivelUsers,OU=Groups,DC=swivelsecure,DC=com, exception 192.168.0.1:389; socket closed

A connection is being made but the socket is closed. This could be caused if the AD/LDAP server is restarted or if there is another AD/LDAP query in place. Check that the AD/LDAP synchronisations are set to occur at differing times and that they are not run too often. Typically synchronisation is set to occur every 60 or 120 minutes.

AcceptSecurityContext error, data 525, vece]

This is usually caused by when incorrect authentication is made against an AD domain. Check the username and password being used for the LDAP synchronisation, check the password has not been changed and the account is still active.

Test the user account with an LDAP browser.

Other possible errors for AcceptSecurityContext: *AcceptSecurityContect error, data xxx, vece* are as follows:

- 525 user not found
- 52e invalid credentials
- 530 not permitted to logon at this time
- 531 not permitted to logon at this workstation
- 532 password expired
- 533 account disabled
- 701 account expired
- 773 user must reset password
- 775 user account locked

Exception occurred: during repository attribute query, object: ERROR Exception occurred: during repository attribute query, object:<name>, attribute: sAMAccountName, exception:java.naming.InvalidNameException:<name>: [LDAP: error code 34 ? 000208F: NameErr: DSID-031001B3, problem 2006 (BAD_NAME), data 8350, best match of:?<name>?]; remaining name <name>

Names have failed to be found and existing names are not found. Check the AD paths and names.

No value for username attribute ?sAMAccountName?. The user "CN=x-x-x-x,CN=y,DC=z,DC=company,DC=com" has no value for username attribute "sAMAccountName". User not added.

A user has been added to a trusted domain where Swivel is looking for users within that group.

Java.net.NoRouteToHostException: No route to host? Exception occurred: during repository group member query, group: javax.naming.CommunicationException: xxx.xxx.xxx.xxx:389 [Root exception is java.net.NoRouteToHostException: No route to host],exception %2

or

Exception occured during repository group member query, group: CN=Swivel Users,OU=Groups,DC=swivelsecure,DC=com, exception javax.naming.CommunicationException: ad.swivelsecure.com:389 [Root exception is java.net.UnknownHostException: ad.swivelsecure.com]

Check the network connectivity to the AD server, ports, firewalls, routing, DNS, IP, etc.

ERROR 192.168.1.1 admin:Exception occurred during repository group member query, group: CN=Swivel users,OU=Swivel,DC=xxx,DC=swivelsecure,DC=com, exception ADserver1.xxx.swivelsecure.com:389

This can be caused by a user who is a member of the group Swivel users but is part of another domian. Swivel will not be able to read the attributes for that user. Swivel would need to connect to that AD domain or read a Global Catalogue Server.

No value for username attribute <attributeName> The user CN=x-x-x-x,CN=y,DC=z,DC=company,DC=com has no value for username attribute <AttributeName>. User not added
ERROR - Exception occured during repository attribute query, object: CN=something,OU=oux,offices,OU=Com,DC=bob,DC=corp, attribute: sAMAccountName, exception:javax.naming.NameNotFoundException: [LDAP: error code 32 -0000208D: NameErr: DSID-031001CD, problem 2001 (NO_OBJECT)

The user within the repository has no value set for the attribute that is configured to be used as the Swivel username; therefore an account cannot be created for that user. For example if Swivel was configured to use the Active Directory attribute for email address for the Swivel account name and this value was not set in AD for a given user.

This may happen when a user has been added to a trusted domain where Swivel is looking for users within that group, only the fact that the user is a member of the group is available, and not the attributes of that user.

admin:Sending alert to user "username" failed, error: The user does not have an associated alert transport.

A transport has not been defined for the user

Exception occured during repository group member query, group: CN=Swivel 2factor,CN=Users,DC=Swivel,DC=swivel,DC=secure, exception javax.naming.CommunicationException: 192.168.0.1:389 [Root exception is java.net.NoRouteToHostException: No route to host]

The error No Route to Host indicates a networking issue. Check to see if the Swivel server can Ping or Telnet on port 389 (or required port) to the AD or LDAP server.

Known Issues

Swivel cannot use the Active Primary Group as a Data Source of users, the effects of this are:

- A Swivel user must have a Primary Group (usually the Domain Users group), and a member of the group for which Swivel users are being read from.
- The Domain User group cannot be used as a group of Swivel users (unless another Primary Group is defined for the users)

Where AD groups are synced from Novell, combining multiple groups may create issues, remove the interlinking and retest.

User Sync Issues

Swivel 3.8 release 2 onwards, any error retrieving user details will skip over that user, but mark it as deleted (or actually delete the user, if mark as deleted is disabled).

Swivel 3.5 to 3.8 first release, if an error occurs trying to read a specific user?s details, it will only skip that particular user if the error is ?Not found?. Any other LDAP error will cause it to abort.

Group Sync Issues

Swivel 3.5 and later, Errors attempting to access LDAP or to read the group details will cause the user sync to abort. In earlier versions of Swivel, such errors could cause all users to be deleted.

<username> Failed to login. RADIUS: <86> Access-Request(1) LEN=57 <IP address>:12004 Access-Request by <username> Failed: AccessRejectException:

Swivel 3.8 userPrincipleName (UPN) fails, but using the sAMAccountName (SAM) account name authentication succeeds. This is caused by a bug and is resolved in Swivel 3.9

Note, this error can also be caused by other issues:

If RADIUS based auth attempt and RADIUS logging enabled. Possible options are: This indicates the user has failed to authenticate successfully. If no other errors are logged in relation to the authentication attempt then the cause is that the user entered the wrong credentials.

This can be caused when an SMS message is to be entered but a Single Channel Image is started, if so then it is expecting a single channel OTC login, until the image times out (default 120 seconds).

The wrong security string index was used (use OTC-String Index, Example 9381-01).

A previously used OTC was attempted to be used again.

Troubleshooting

Enable debugging in the Swivel Administration console under logging/XML and check for errors.

Cannot Sync with Active Directory

Use the LDAP browser under Repository/Groups or under the Repository/<AD repository>/Browse in window, and check for any errors.

If it is an existing system where synchronisation has been previously working, the sync may have stopped. Restart Tomcat and see if synchronisation works, if this is Swivel 3.7 or earlier, consider upgrading.

Cannot import users into AD

Is the AD Server accessible? Check by making a telnet connection from the Swivel server on port 389 or required port. Possible causes are firewalls, routing and network issues, SSL communications only to the AD server. AD server is down. Swivel Log will report an error.

Is DNS functioning? Check with a NSlookup. Swivel Log will report an error.

Does the AD group have any users in it?

License exceeded. Swivel Log will report an error.

Can the AD group be browsed through AD and does it show any users?

Are some users imported and not others?

Cannot import some users

Are users across multiple domains? Swivel can only read domains for AD domains that it is configured to read. Either create another AD domain or use Global Catalog.

If using the Global Catalog, is Swivel reading from the Global Catalog AD server? Is the Global Catalog port selected?

The same username exists on multiple AD servers? Use userPrincipalName

userPrincipalName is used but the user does not have a userPrincipalName set, this can occur with Administrator users where by default this is not set.

User Sync takes a long time

Swivel version 3.9.6 includes some enhancements to close LDAP connections and may improve performance for synchronizations.

If SSL is being used, try without SSL and see if User Sync time improves.

If domain name is beiing used, try sepcifying a specific hostname and see if User Sync time increases.

Network Troubleshooting

Can you ping the AD server?

Can you Telnet to the AD server?

Telnet using diagnostics or the command line of the virtual or hardware appliance to see if you can initiate a connection to port 389 (or port being used) of the ip address of the AD server?

Try the following:

```
[admin@primary ~]# telnet AD_Server_IP 389
```

If the connection succeeds you will get:

```
Trying 192.168.0.1...

Connected to 192.168.0.1(192.168.0.1).

Escape character is '^]'.

(You can press Ctrl-C to exit at this point) Connection closed by foreign host.
```

If the connection fails you will get:

```
Trying 192.168.0.1...

telnet: connect to address 192.168.0.1: Connection refused

telnet: Unable to connect to remote host: Connection refused
```

Null Values

If you try and read a user from an Active Directory but get a Null Value error message, it may be that there is no referential integrity. This means that a user can be deleted from AD but when you perform a get Members on the group that user will still be returned.

Prefix is not added to Telephone Number

See Phone Number Format incorrect

Error Messages

Abandoned User Sync for repository <repository name>

If a synchronisation encounters an error then the sync job will stop. Check the settings are correct, particularly LDAP group names, and check the logs for further associated errors. Has the AD infrastructure had any changes such as the renaming or move of an OU or CN?

LDAP: error code 49 and **AcceptSecurityContext error**

Swivel cannot authenticate to the AD server. Has the AD service account password Expired? Is the username/password correct? Try using different account details such as:

- userPrincipalName (username@domain) for the service account to login to AD
- domain\username
- CN=user,DC=domain,DC=local

Test the user account with an LDAP browser, and see if the LDAP can be browsed. We recommend the use of third-party software from Softerra called LDAP Browser. This is available as freeware and as a commercial paid-for product. Available here: http://www.ldapbrowser.com/

Membership of multiple alert transport group is not permitted for user

This occurs when users are member of more than one group that is assigned to a string transport entry or alert transport entry. The cause for this can be when users are added either purposely or accidentally to additional groups on the Active Directory or whichever repository type you are syncing with and a subsequent User Sync takes place in Swivel.

To resolve this issue, on the Swivel administration console select the User Administration screen. Find a user that is suffering from this problem. Change the View drop down on the User Administration screen to be 'Groups'. Make a note of the groups that the user is assigned to (represented by a tick/check mark). Then visit the Transport -> General screen. You now need to look for Transports you have defined, where these groups have a 'Alert repository group' drop down containing either of the groups you noted in the previous step. It is not possible to have a user assigned to more than one transport sting or transport alert. So you will need to remove the users from the offending group which has led to this situation.

No Transport Attribute found for User or **No Alert Transport Attribute found for User** Possible causes are:

Email Address (optional), if no value exists in AD a no transport attribute error message is logged

Phone Number (optional), if no value exists in AD a no transport attribute error message is logged

Transport has not been defined for user, see Transport_Configuration

Transport Attribute has bot been defined, see Transport_Attribute

Modifications have not been made but Swivel has not been Synchronised with Active Directory

The object "CN=swivel-users,OU=Groups,OU=Swivel,DC=swivel,DC=local" on repository "AD" is not a valid group.

This could be caused by:

- The swivel-users is actually a Container, rather than a group.
- swivel-users is not defined as a group, according to the LDAP standard. Swivel only looks for objects with objectClass=group.

- If it is a global group, it is possible that the account used to connect to AD does not have permission to read the group properties.
- Swivel cannot read primary groups.