Overview and Steps to map pam.mapuser.*username*

This configuration parameter maps a local UNIX user account to an Active Directory account. Local user mapping allows you to set password policies in Active Directory even when a local UNIX account is used to log in. This parameter is most commonly used to map local system or application service accounts to an Active Directory account and password, but it can be used for any local user account. For more information about mapping local accounts to Active Directory users, see "Mapping local UNIX accounts to Active Directory" on page 159 in the *Centrify DirectControl Administrator's Guide*.

In most cases, you set this configuration parameter using the **Computer Configuration > Centrify Settings > DirectControl Settings > Set user mapping** group policy.

You can, however, set it manually in the configuration file if you aren't using group policy or want to temporarily override group policy.

If you are manually setting this parameter, you should note that the local account name you want to map to Active Directory is specified as the last portion of the configuration parameter name.

The parameter value is the Active Directory account name for the specified local user. For example, the following parameter maps the local UNIX account oracle to the Active Directory account

oracle_storm@acme.com if the host computer's name is storm:
pam.mapuser.oracle: oracle_$HOSTNAME@acme.com

You can specify the user name in the configuration file with any of the following valid formats:

Standard Windows format: domain\user_name
Universal Principal Name (UPN): user_name@domain
Alternate UPN: alt_user_name@alt_domain
UNIX user name: user

You must include the domain name in the format if the user account is not in the local computer's current Active Directory domain.

If this parameter is not defined in the configuration file, no local UNIX user accounts are mapped to Active Directory accounts.

Steps to map local user account to AD account (without GP):

1) Using root or any privileged account, create a normal local account called dluu (Daniel Luu) on Solaris 10 box using SMC or useradd method.

2) Login as dluu and verify if you can login with local credentials on the Centrify Server.

3) Now su to root on the Centrify/Solaris server. Navigate to /etc/centrifydc

4) cp centrifydc.conf centrifydc.conf.ori

5) vi centrifydc.conf

6) search for pam.map user and add the below line.

pam.mapuser.dluu: sfong@corp.contoso.com

where dluu is the local account and sfong@corp.contoso.com is the account in AD. It may or may not be zone-enabled in Centrify Zones.

7) run adreload (to run the config changes)

8) run adflush (to clear cache)

9) Now ssh to the Centrify/Solaris server and login as dluu

10) You have to type the AD password otherwise it will be rejected. This step tells AD password password policies can be applied to local accounts too

11) Now if you want to type the local account password for dluu, a few additional steps are needed.

12) Go to step 5) and search for pam.allow.override and add the local account next to root separated by space.

pam.allow.override: root dluu

13) Run adreload and adflush

14) Now login as dluu@**localhost** (the @localhost is very important) and type the local password set in step 1) and 2)

15) You should be to login in with local password. This will be handy when AD is down or Centrify is disconnected.