

# *Headquarters Air Mobility Command*

---



# **G081 User Accounts**

CREATION & MANAGEMENT

---

*Enabling the "Global" in "Global Vigilance, Reach and Power!"*

**BLANK PAGE**

<b>TABLE OF CONTENTS</b>	<b>Page #</b>
<b>INTRODUCTION</b>	<b>5</b>
<b>ACCESSING TSO THROUGH MIAP</b>	<b>7</b>
<b>BUILDING NEW ACCOUNTS</b>	
• <b>ON THE MAINFRAME (TSO)</b>	<b>11</b>
• <b>IN USER MANAGER</b>	<b>14</b>
<b>IMPORTANT NOTES ABOUT G081 PASSWORDS</b>	<b>28</b>
<b>MANAGING USER ACCOUNTS IN TSO</b>	
• <b>RESET PASSWORDS</b>	<b>28</b>
• <b>UNSUSPEND ACCOUNTS</b>	<b>30</b>
• <b>UPDATE USER INFORMATION</b>	<b>32</b>
• <b>DELETE ACCOUNTS</b>	<b>36</b>
<b>MANAGING USER ACCOUNTS IN USER MANAGER</b>	
• <b>RESET PASSWORDS</b>	<b>38</b>
• <b>ENABLE/DISABLE ACCOUNTS</b>	<b>39</b>
• <b>UPDATE USER INFORMATION</b>	<b>41</b>
• <b>DELETE ACCOUNTS</b>	<b>43</b>
<b>USER MANAGER ACCOUNTS FOR GLOBAL REACH ACCESS ONLY</b>	<b>45</b>

**BLANK PAGE**

## **INTRODUCTION**

This guide has been developed to aid G081 Managers in creating and managing user accounts in the new Web environment of G081. This guide will cover creating new user accounts in TSO. We've also incorporated the processes outlined in the "Web Account Creating -User Manager" instructions published by the FAO.

The following pages will walk you through all tasks required to create, manage and maintain user accounts as a G081 Manager.

If you have any questions, suggestions or other constructive comments regarding this guide, please contact us.

Ms. Penny Young                      DSN: 779-4511                      [Penny.Young.2.ctr@us.af.mil](mailto:Penny.Young.2.ctr@us.af.mil)

Ms. Noella Clark                      DSN: 779-2731                      [Noella.Clark.ctr@us.af.mil](mailto:Noella.Clark.ctr@us.af.mil)

## **AREAS OF INTEREST**

WebG081                      [Click Here For The WebG081 Log-In Page](#)

MIAP                      [Click Here For The MIAP Log-In Page](#)

User Manager                      [Click Here For The User Manager Log-In Page](#)

G081 Manuals                      [Click Here For The G081 User Manuals Web Page](#)

G081 CoP                      [Click Here For The G081 Community of Practice \(CoP\)](#)

Global Reach                      [Click Here For The Global Reach Log-In Page](#)

**BLANK PAGE**

# G081 User Accounts

---

The information in this guide was obtained from the G081 Program Management Office at HQ AMC and the Functional Assistance Office at DISA OKC.

Creating new accounts in G081 has always been a 2-step process... 1) Create an account in G081 and 2) Create an account in User Manager. However, you could by-pass the second step by synchronizing the new G081 account to User Manager as part of step 1.

Currently, this is no longer possible and these accounts must now be created individually. The intent of this product is to provide key processes you, the G081 Manager, need to know about creating, managing and maintaining G081 user accounts in both TSO and User Manager.

=====

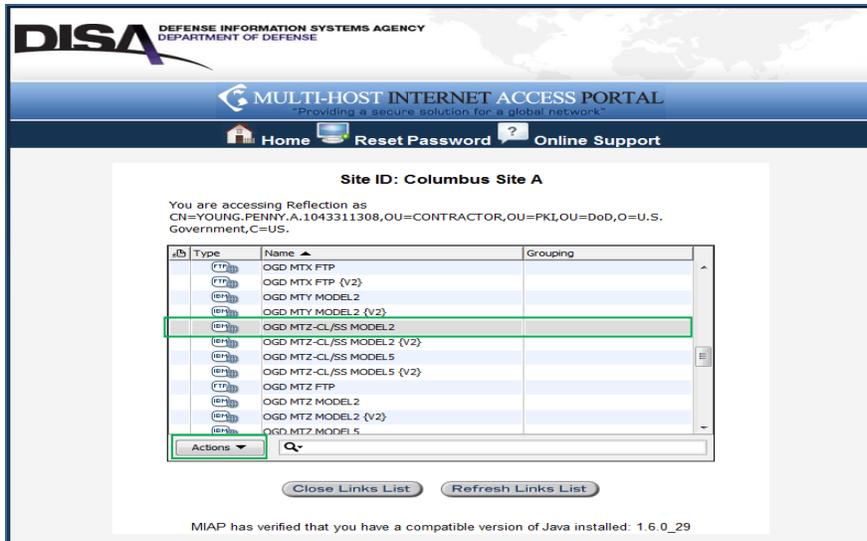
One of the changes brought about by the transition to Web G081 is that new accounts for routine users must be created in User Manager ONLY! Once created, you will then need to use Program 9057 to assign the USERID in Web G081. The exception to this will be G081 Managers and, in some cases, Maintenance Management Analyst performing dual roles (generally found in Guard and Reserve units). For these users, you will need to create an account in both TSO and User Manager.

**IMPORTANT NOTE:** The following steps are presented under the assumption that you, the G081 Manager, already have an active MIAP account. If this is not the case, you will need to get one set up before proceeding. Instructions for setting up a MIAP account are located on the [G081 CoP in the FAO folder](#).

## **ACCESSING TSO VIA MIAP**

The first step in creating an account for a new G081 Manager is to build the USERID and associated information in TSO. This area is now accessible through the [MIAP](#) interface.

Once you have entered the portal and are directed to the Program List page, you want to select the **OGD MTZ-CL/SS MODEL2** option from the menu.

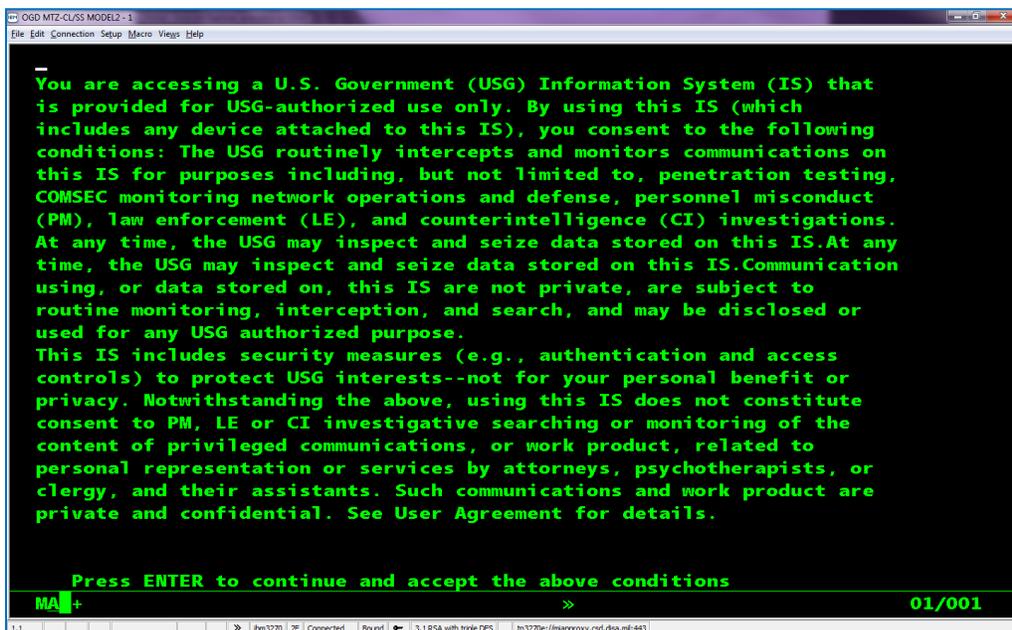


To open TSO, you can DOUBLE click the menu option

OR

Select OPEN from the Actions menu in the bottom left hand corner

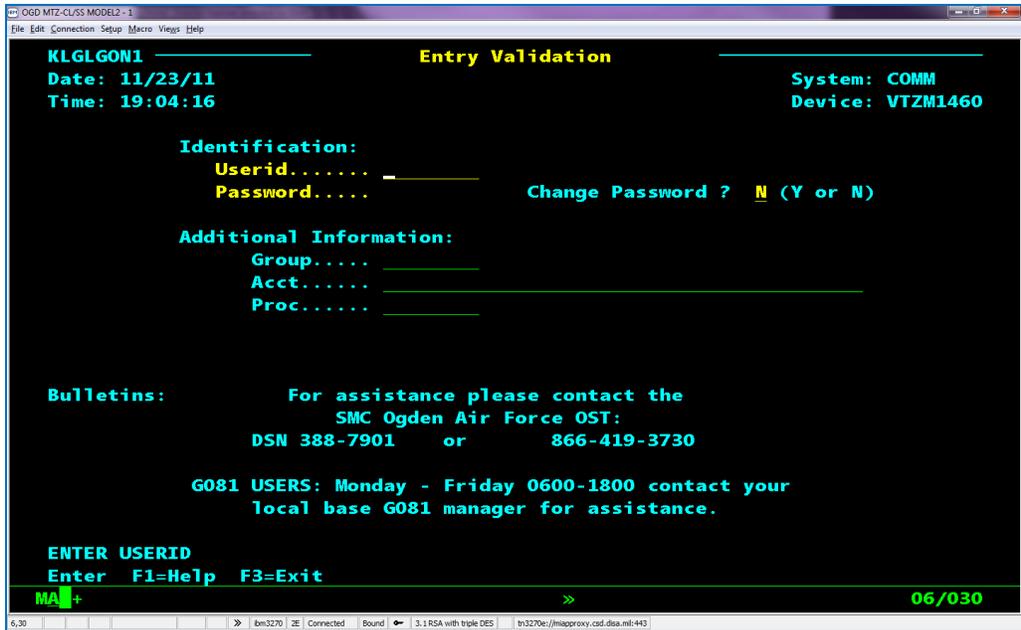
Once you are in TSO, you will see the familiar green-screen view you are familiar with from selecting the TEXT (green screen) view in GUI.



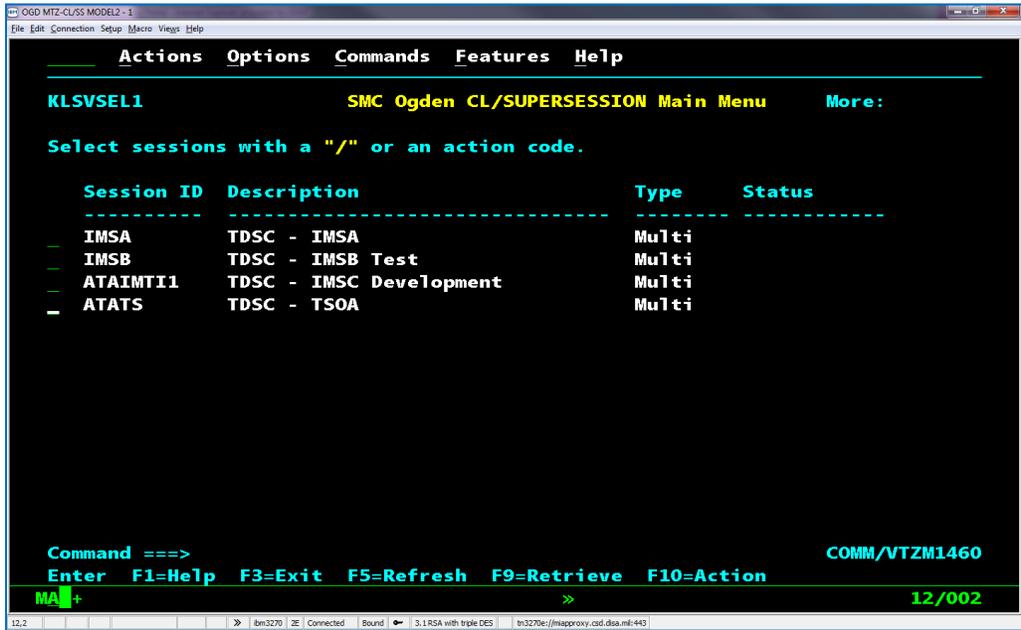
Press enter to log-in with your USERID/Password.

**Change Password** should default to "N". If not, be sure you input "N".

**NOTE:** As a G081 Manager, you **MUST** keep your manual log-in account current. This means you **MUST** log in at least once every 30-days (AD, ART, ANG Tech) or every 90-days (Traditional Reserve/Guard members).

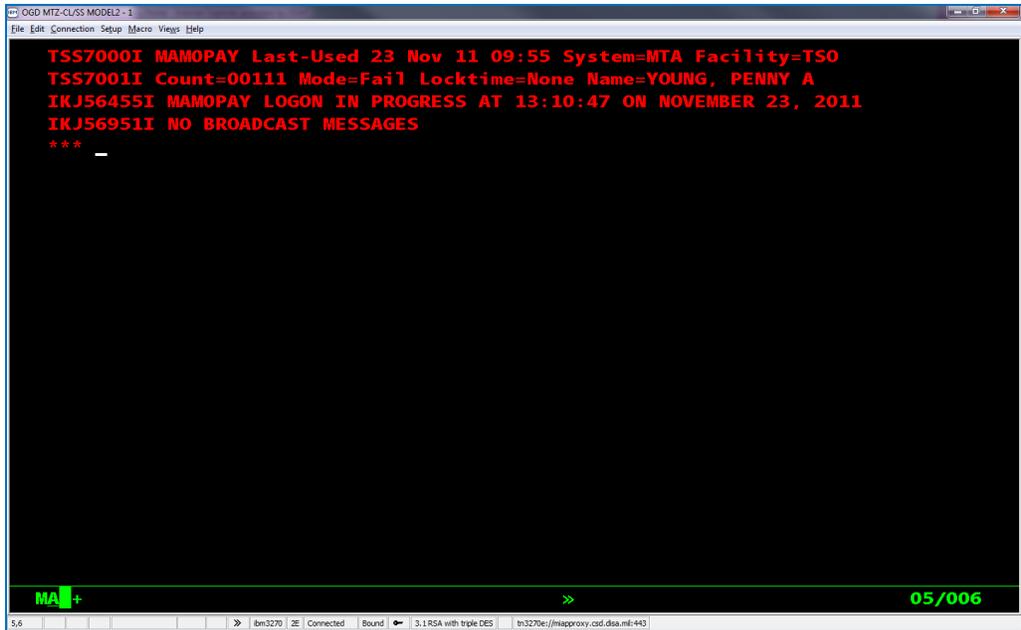


You will then be taken to the site selection page.



Select the **ATATS** option and hit ENTER.

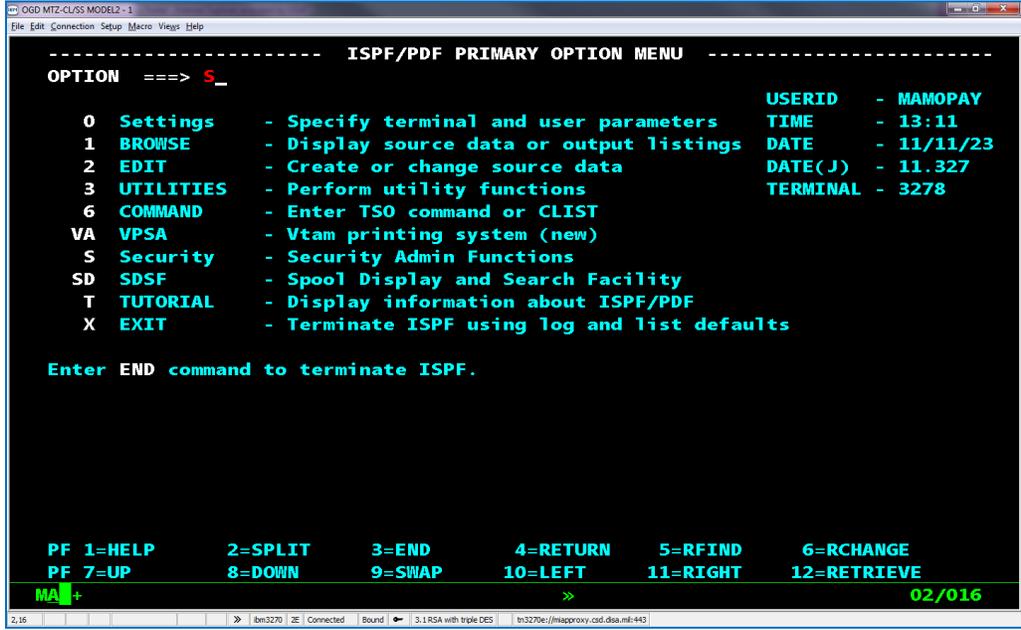
This will take you to the account access review page.



**REVIEW** your log-on history as presented on this page. This could be your first indication that your account has been compromised.

Once you have verified your log-in information, hit ENTER to proceed to the **ISPF/PDF Primary Option Menu**.

For the **OPTION**, input “S” for **Security Admin Functions** and hit ENTER



This will take you to the **G081 User ID Maintenance Facility** page.

You can create, reset, modify and delete user accounts from this location.

```
----- G081 User ID Maintenance Facility -----
COMMAND ==>
TIME - 13:16
DATE - 11/11/23

OPTION ==> _ User ID==> _

1 - Add New User ID
2 - Reset User ID
3 - Display User ID
4 - Modify User ID
5 - Delete Existing User ID
6 - List All Users (as of approx 0215 Central Time)
7 - List All Inactive Deleted G081 Users
F - Add or Remove IMS Facilities
M - Manage CITRIX/RUMBA Connection for this User ID
B - Manage CITRIX/RUMBA Connection for an entire Base
R - List Users Overriding the CITRIX Connection

X - Exit

For a list of userids with various select & sort options, use
batch program 67041
PF 1=HELP 2=SPLIT 3=END 4=RETURN 5=RFIND 6=RCHANGE
PF 7=UP 8=DOWN 9=SWAP 10=LEFT 11=RIGHT 12=RETRIEVE
MA+ >> 05/014
```

## CREATING NEW USER ACCOUNTS IN TSO

Remember, you only need to create an account in TSO if the user is a G081 Manager or will be performing G081 Management duties. Now that you are in the TSO area of G081, we can proceed to creating an account for a new user by inputting “1” as the **OPTION** and the **USERID** that you want to assign the person in the **User ID** section, then hitting ENTER.

```
----- G081 User ID Maintenance Facility -----
COMMAND ==>
TIME - 13:16
DATE - 11/11/23

OPTION ==> 1 User ID==> _

1 - Add New User ID
2 - Reset User ID
3 - Display User ID
4 - Modify User ID
5 - Delete Existing User ID
6 - List All Users (as of approx 0215 Central Time)
7 - List All Inactive Deleted G081 Users
F - Add or Remove IMS Facilities
M - Manage CITRIX/RUMBA Connection for this User ID
B - Manage CITRIX/RUMBA Connection for an entire Base
R - List Users Overriding the CITRIX Connection

X - Exit

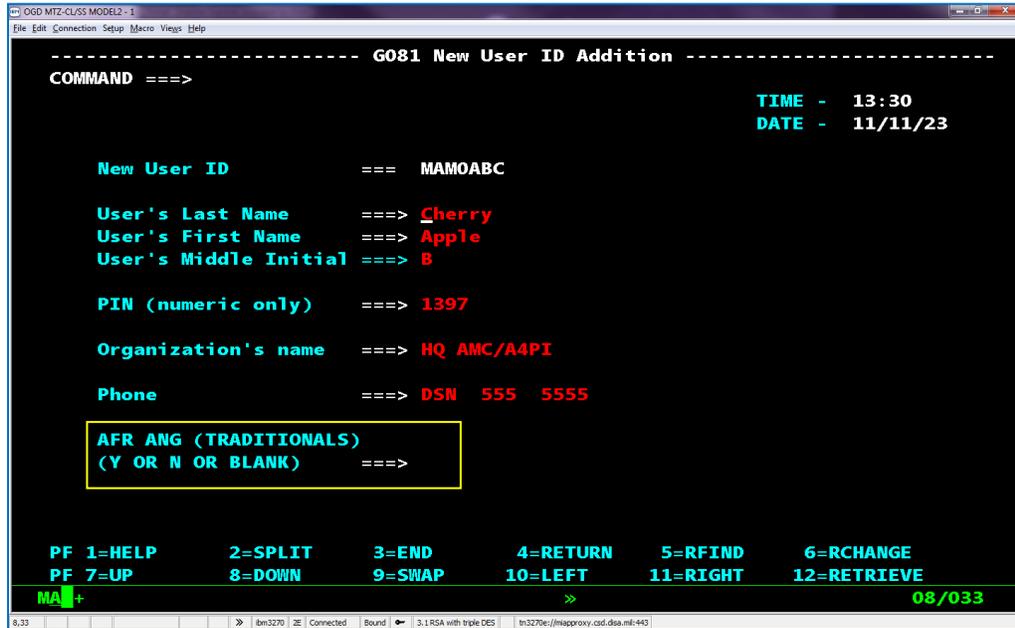
For a list of userids with various select & sort options, use
batch program 67041
PF 1=HELP 2=SPLIT 3=END 4=RETURN 5=RFIND 6=RCHANGE
PF 7=UP 8=DOWN 9=SWAP 10=LEFT 11=RIGHT 12=RETRIEVE
MA+ >> 05/054
```

User IDs are 7-character alpha-numeric, base specific designations

They begin with MA, followed by the 2-character designation assigned to the base or user group, and ending with the new user's initials.

In cases where the initials are already assigned, the first and last name initials are generally used, followed by a number.

This will take you to the **G081 New User ID Addition** page. Input the appropriate information for the user as shown in the below example.



**AFR ANG (TRADITIONALS)  
(Y OR N OR BLANK)**

G081 user accounts are suspended after 30-days of inactivity.

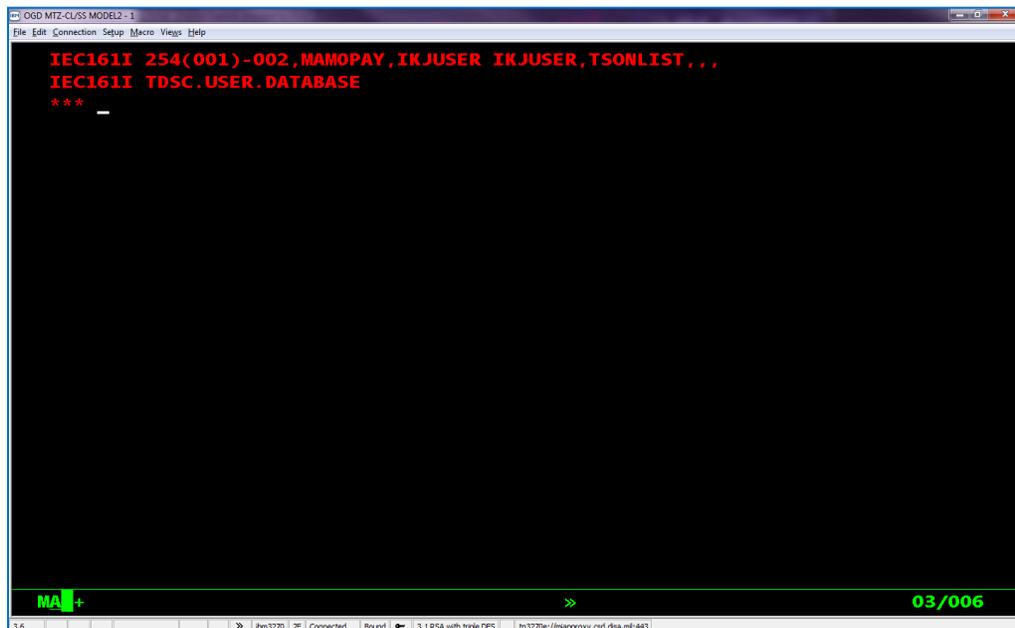
This can pose a serious issue for traditional Reserve and Guard members.

Input "Y" in this area to bypass the 30-day auto-suspension protocol.

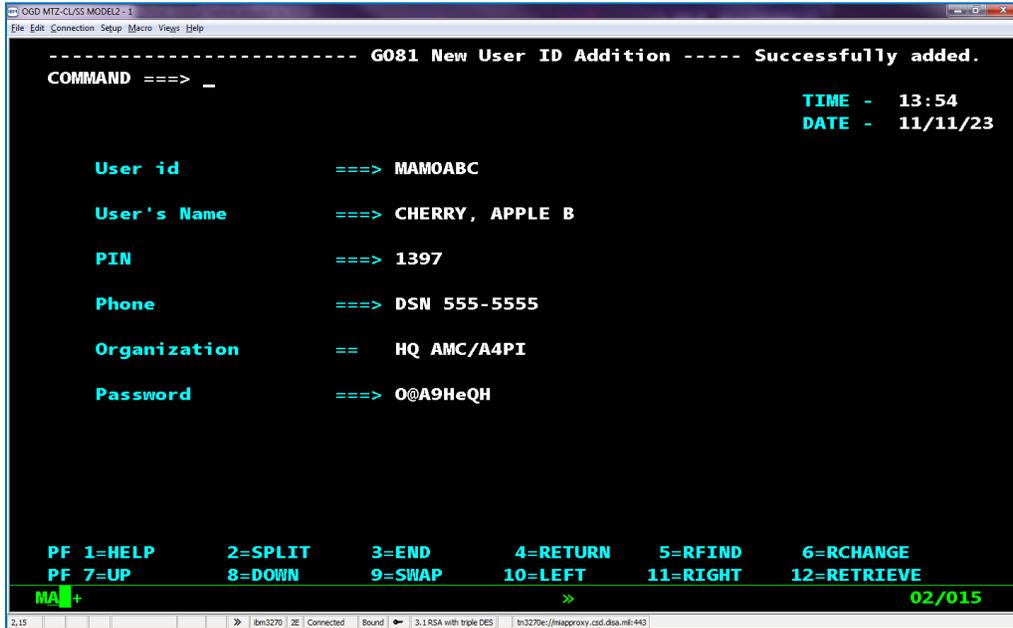
Traditional Reserve and Guard member accounts will be suspended after 90-days of inactivity.

Once you have input all the required information and reviewed it for accuracy, hit ENTER to build the account.

The first page you will be taken to is shown below. If there were any issues in creating the account, they would be shown here. Hit ENTER to proceed.



You will now be taken back to the **G081 New User ID Addition** page. In the upper right hand corner you should see “**Successfully added**” and also, a password will now be assigned to the account.



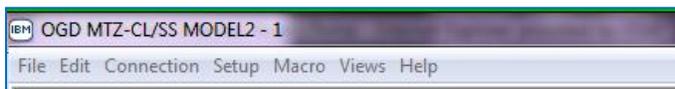
Make note of the password for use when building the account in User Manager. I recommend annotating the password on the member’s DD Form 2875.

And... You are now done with the first portion of creating a new user account.

If you have more accounts to create, hit ENTER to go back to the **G081 User ID Maintenance Facility** page. Then, simply repeat the process for the next person.

Once you are finished building new accounts, input “**END**” in **COMMAND** to return to the **ISPF/PDF Primary Option Menu** page and then input “**X**” in **COMMAND** to exit the system.

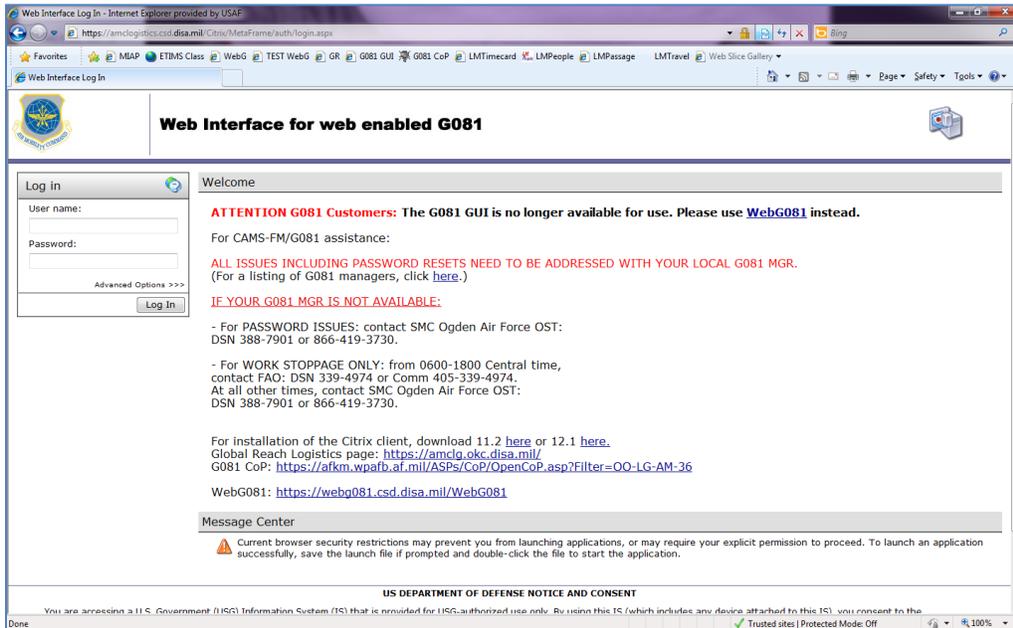
OR... Select **File** from the header menu and **Exit** from the drop down list



Once you have successfully established new users in TSO, you must create their accounts in User Manager to complete the process.

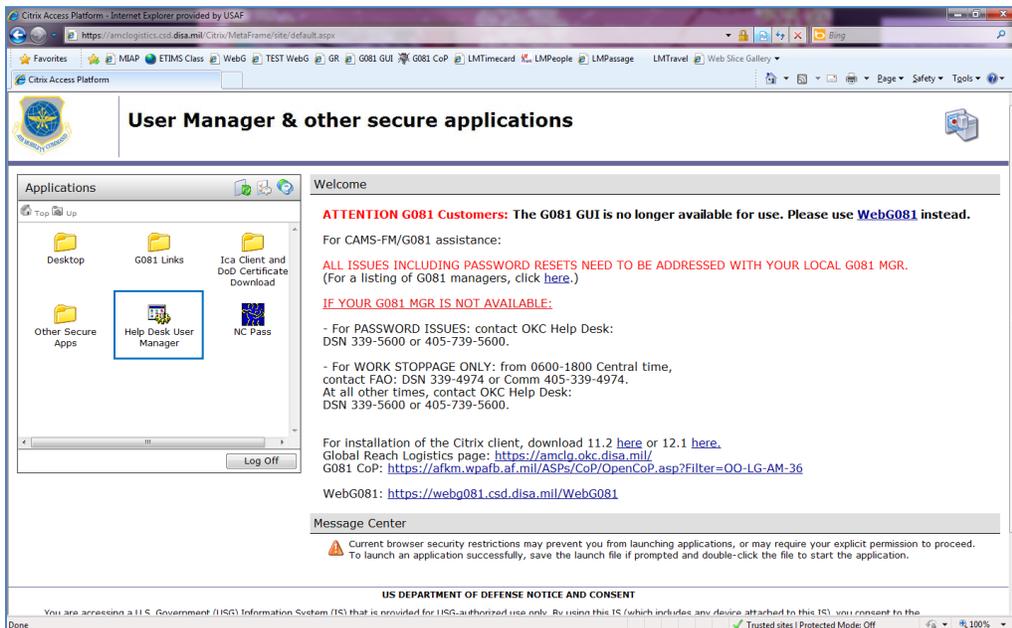
## CREATING NEW USER ACCOUNTS IN USER MANAGER

User Manager resides within the CITRIX environment and can only be accessed using the Web Interface page used previously for G081 GUI access. If you did not keep it, the GUI link is available on the [Introduction](#) page of this guide.



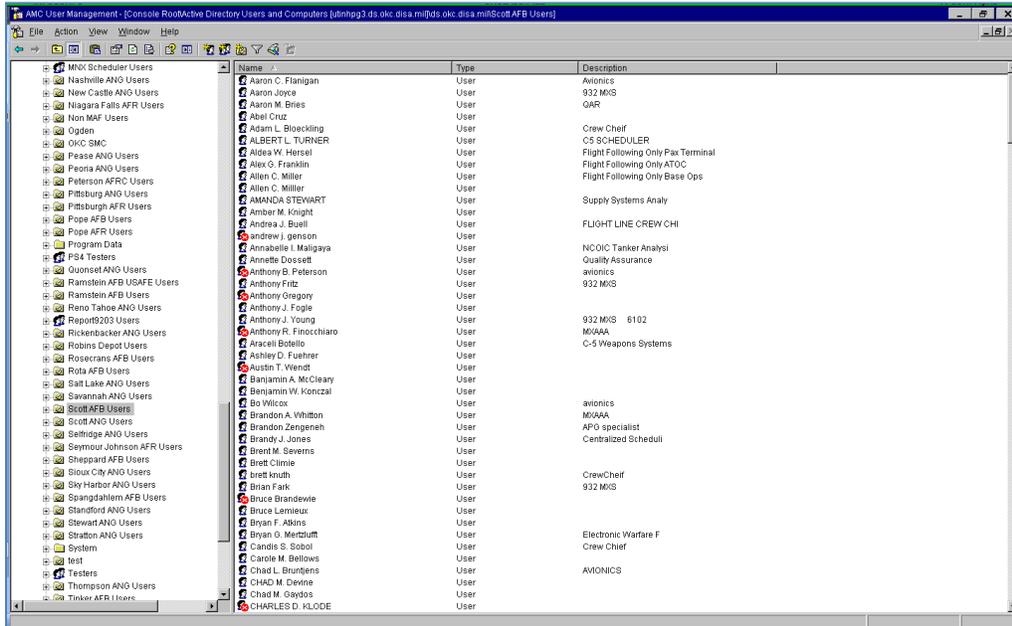
Input your G081 USERID/Password combination and click **Log In**

This will open up the **Applications** window. You should see the icon for **Help Desk User Manager** as one of your options



Select **Help Desk User Manager** from the Applications window to open the **AMC User Manager Console**.

When the console opens, it should default to your base user folder. If this is not the case, scroll down the menu on the left and manually select your base.

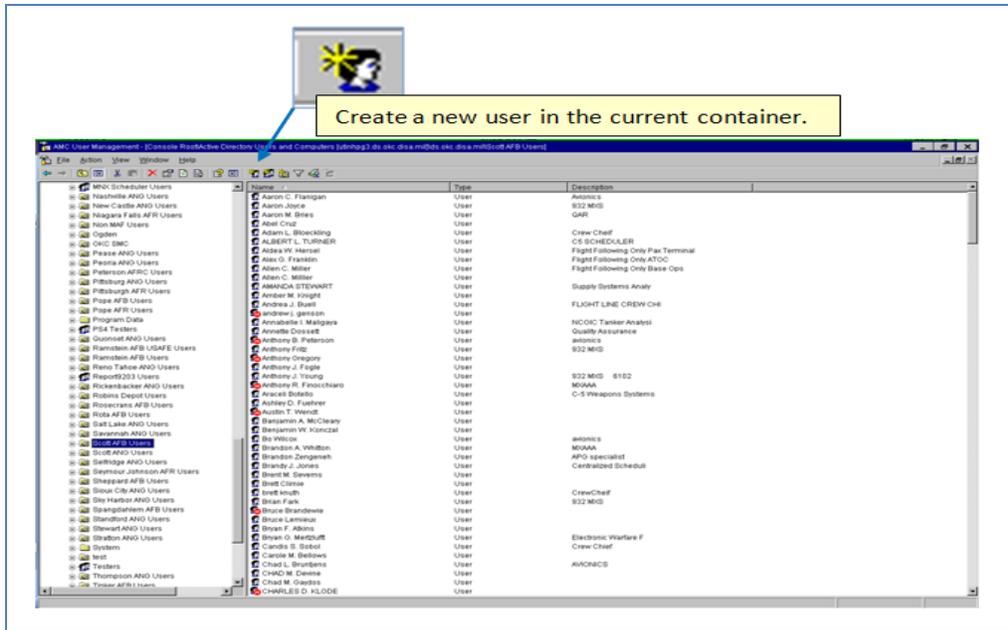


**NOTE:** Some bases have more than one group (Users, ANG Users, Depot Users, etc). Be sure to select the appropriate group for the individual you are adding.

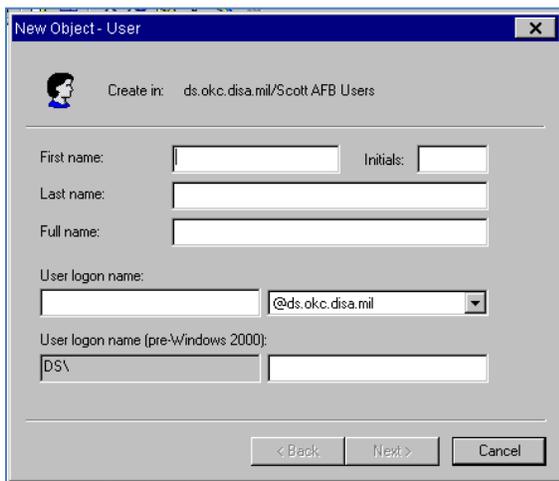
There are two methods for adding a new user in User Manager. You can copy a current user's accounts and make the applicable changes to reflect the new user's information, or you can start with a blank slate. We'll cover both in this guide.

### ◆ Create A New User From Scratch

From the icon menu at the top of the screen, select the individual head.



This will open the **New Object – User** window



Input the user’s information as requested. You will notice that the **Full name** section will automatically update. **DO NOT** alter this information.

In first half of the **User logon name** field, input the G081 USERID you assigned the user. You will notice that the USERID will automatically update in the second portion of the **User logon name (pre-Windows 2000)** field as you type.

The second portion of the **User logon name** field should be pre-filled with **@ds.okc.disa.mil**. If this is not the case, it should be available from the dropdown menu.

Once you have input the required information, select **Next>**.

This will take you to the password page where will input the password generated for the user when you created the account in TSO.

### Password Parameters

Must be EXACTLY 8-characters in length  
*\*\*size may increase in the near future\*\**

Must contain at least 1 of each character type  
 -Uppercase  
 -Lowercase  
 -Number  
 -Special Character (**ONLY @, #, \$ are allowed**)

Characters cannot be consecutively repeated  
 (22, mm, AA, @@)

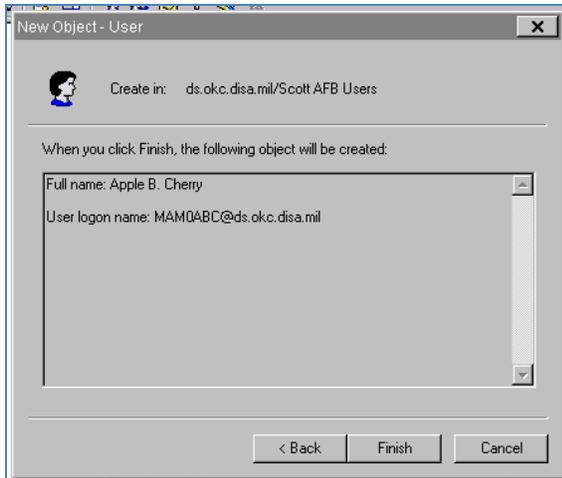
System recalls previous 10 passwords and will reject if input

Rejects may occur for using common words/names in your password

Ensure **User must change password at next logon** is **UNCHECKED**

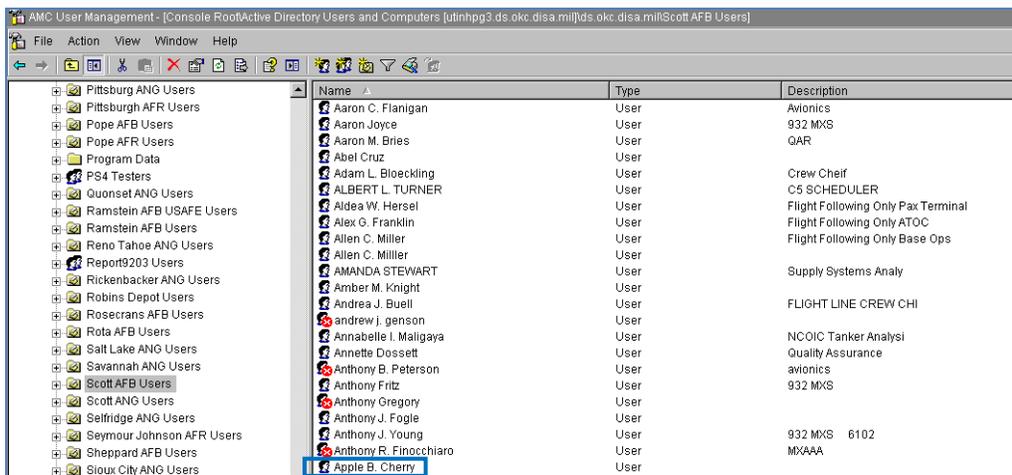
Ensure **Password never expires** is **CHECKED** and hit **Next>**.

You should see the below letting you know the user has been successfully added.



If you do not get this message, you should be given an error message specifying what needs to be corrected. Fix and re-submit.

Now that you have added the new user successfully, select **Finish**. You should see the new user in your group.



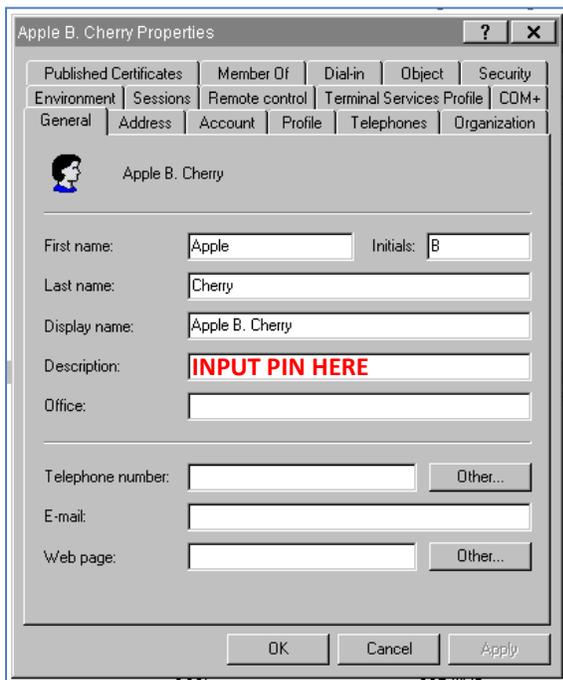
Now that you have added the user, you must make some additional annotations to the account for future reference.

Right mouse click on the user name and from the pop-up window, select **Properties**.

This will bring up the properties assigned to the users account. Most of the items will be updated by inputs made during the account creation or are pre-determined by the group where the user has been added.

But there are some key pieces of information you will want to add to the user properties. Most importantly, you need to annotate the members PIN. This

information is required when requesting a password reset from the help desk and this is the area they will look for the information.



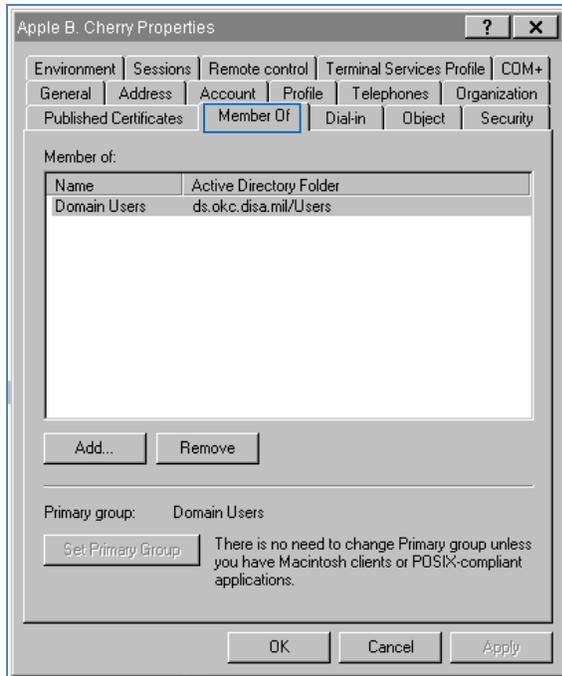
The PIN **must be input in the Telephone number field.**

All other field updates are at the G081 Manager's discretion. If you want to include the member's phone number, select the **Other** button to add it to the properties.

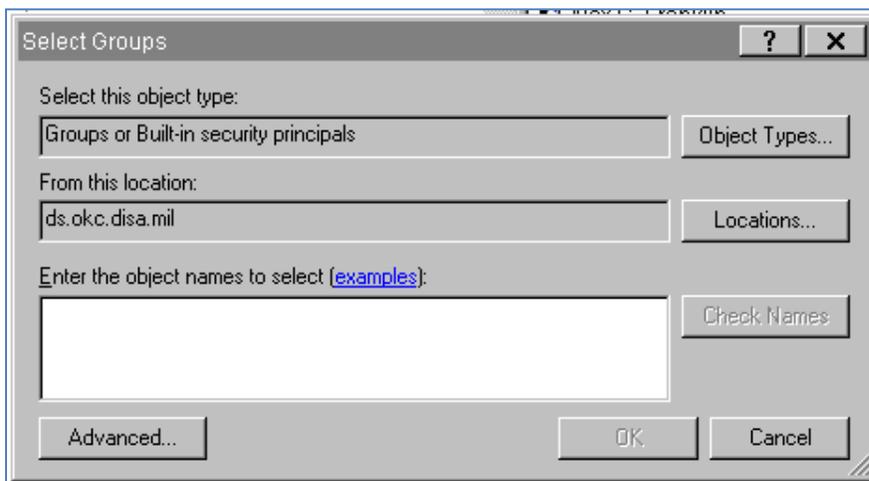
**Recommendation:** Use the Description field to input the member's unit affiliation (Civ, ART, Traditional ANG, etc). This can assist when reviewing a member's account suspension/disabled status as circumstantial or neglect.

Next, you need to ensure that the user is a member of all required groups. All new users will automatically have the *Domain Group* assigned. There is also a *User Group* (basic user) and a *Functional Group* (G081 Managers – only AMC has access to add/remove this group) for each base. All users will require the *Global Reach Group* and a few select users may require the *Flight Following Group*.

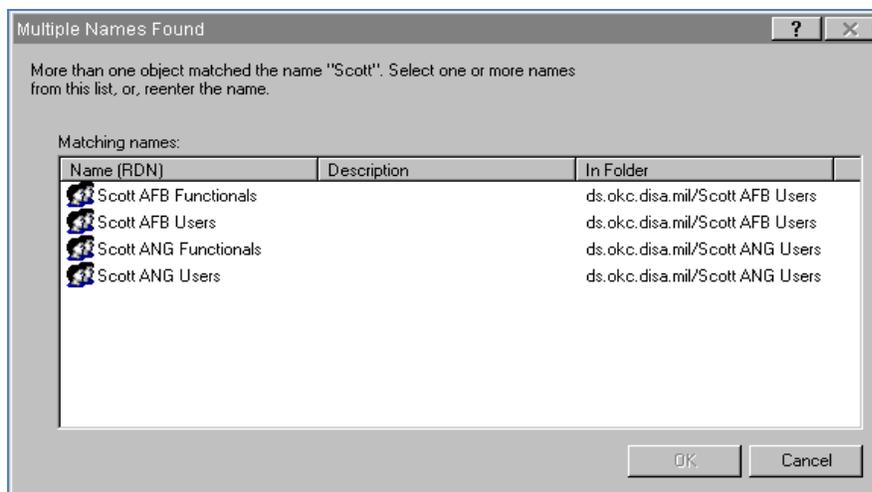
To review and/or add the required group(s) to a new user, select the Member of tab in the **Properties** window.



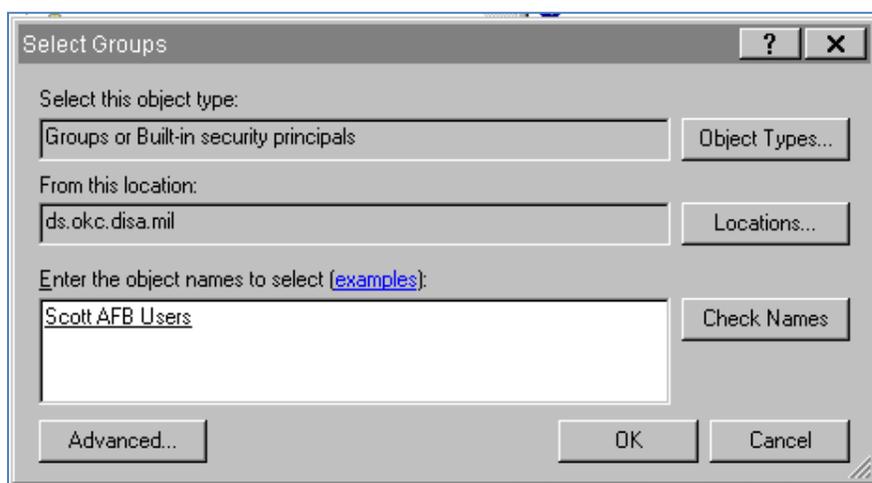
To add additional groups to the user, select the **Add...** button to bring up the **Select Groups** window.



In the **Enter the object names to select** box, type in the first part of the group name (i.e. Scott, GRL). Then select **Check Name** to pull up a list of available groups that match your input.



Select the group you need from the list and click **OK**. You will see that the domain group has been added to the **Enter the object names to select** box as a link.



If this is correct, hit **OK**. If not, hit **Cancel** and begin again to make the correct selection.

You will now see the added group in the users **Member of** window. Repeat the process to add additional groups, as needed.

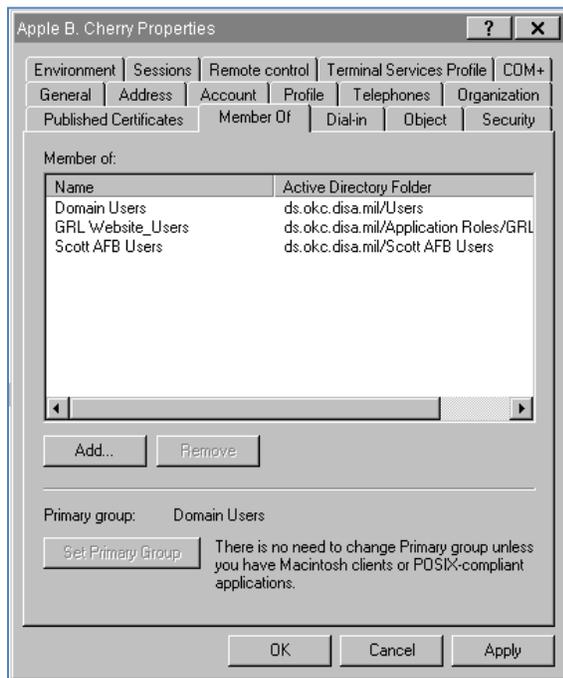
Groups which all users should have:

- Domain Users
- GRL Website\_Users
- <Base name> Users

Additional group(s) select users may require:

- FlightFollowing\_Users

Once you have finished adding groups, hit **Apply** and then **OK** to update the user profile and exit the **Properties** window.



You have now added a new user from scratch and updated their profile for all required user access to both G081 and Global Reach.

### ◆ Create A New User Using The Copy Feature

The process for adding a new user through the copy feature is almost exactly the same except for how you begin the process.

**DO NOT** select a member with a white “X” in a red circle on their icon (👤). This means their account has been disabled. You want to copy from an active member in the desired group.

Once you have selected the copy from account, right mouse-click on the name. This will bring up a pop-up and you want to select the **Copy...** option.

This will bring up the **Copy Object – User** window.

Input the user's information as requested. You will notice that the **Full name** section will automatically update. **DO NOT** alter this information.

In first half of the **User logon name** field, input the G081 USERID you assigned the user. You will notice that the USERID will automatically update in the second portion of the **User logon name (pre-Windows 2000)** field as you type.

The second portion of the **User logon name** field should be pre-filled with **@ds.okc.disa.mil**. If this is not the case, click the dropdown menu from this field to make the correct selection.

Once you have input the required information, select **Next>**.

This will take you to the password page where will input the password generated for the user when you created the account in TSO.



### Password Parameters

Must be EXACTLY 8-characters in length  
*\*\*size may increase in the near future\*\**

Must contain at least 1 of each character type  
-Uppercase  
-Lowercase  
-Number  
-Special Character (**ONLY @, #, \$ are allowed**)

Characters cannot be consecutively repeated  
(22, mm, AA, @@)

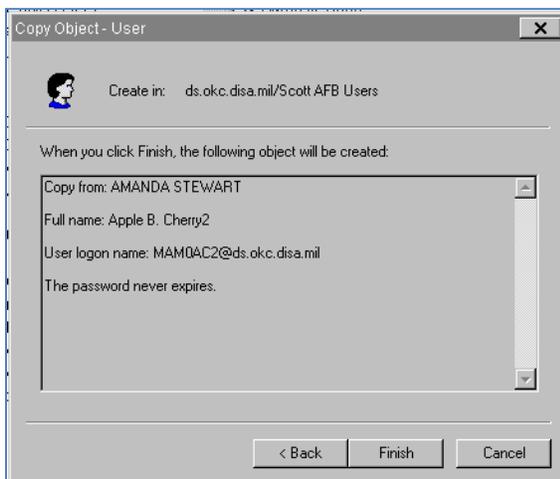
System recalls previous 10 passwords and will reject if input

Rejects may occur for using common words/names in your password

Ensure **User must change password at next logon** is **UNCHECKED**

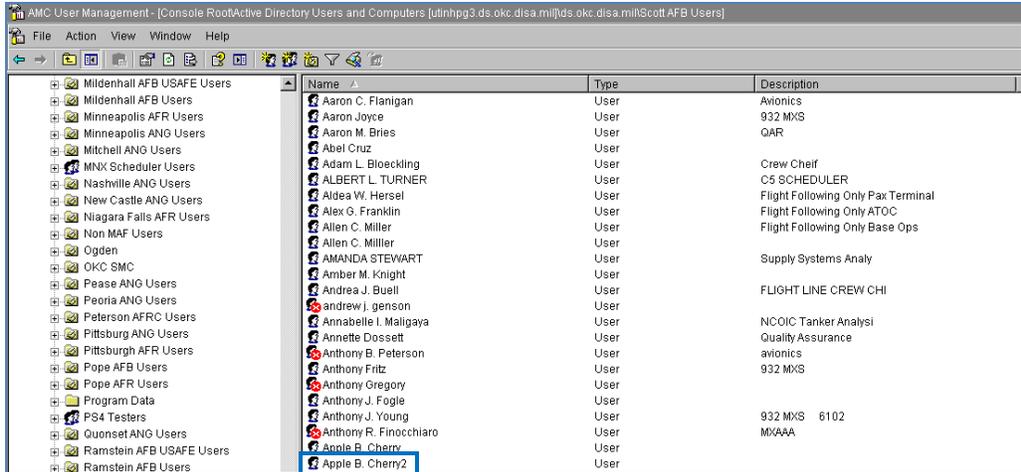
Ensure **Password never expires** is **CHECKED** and hit **Next>**.

You should see the below letting you know the user has been successfully copied from the user account you selected.



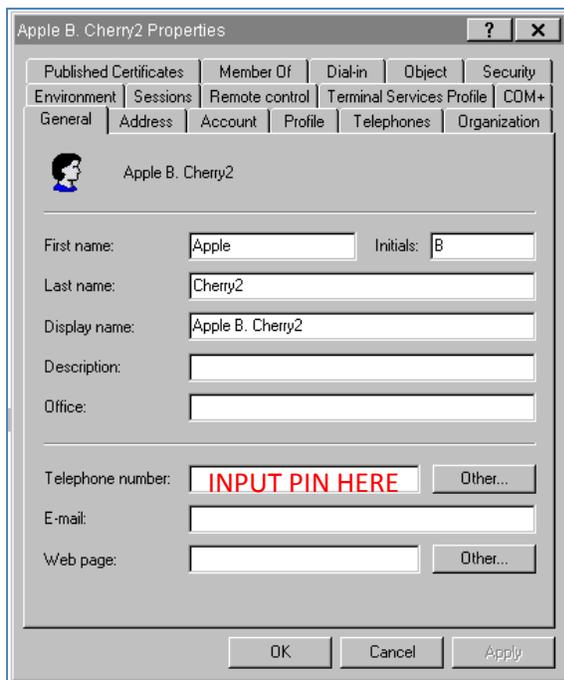
If you do not get this message, you should be given an error message specifying what needs to be corrected. Fix and re-submit.

Now that you have added the new user successfully using the copy feature, select **Finish**. You should see the new user in your group.



As with creating an account from scratch, when copying you must add the users PIN to the account properties. Right mouse click on the user name and from the pop-up window, select **Properties** to bring up the account properties.

The PIN **must** be input in the **Telephone number** field.

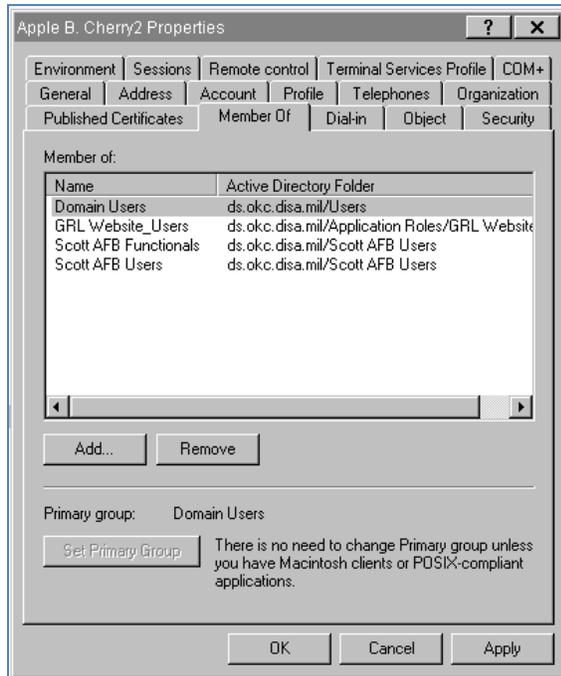


All other field updates are at the G081 Manager's discretion. If you want to include the member's phone number, select the **Other** button to add it to the properties.

**Recommendation:** Use the Description field to input the member's unit affiliation (Civ, ART, Traditional ANG, etc). This can assist when reviewing a member's account suspension/disabled status as circumstantial or neglect.

Next, select the **Member of** tab to review the assigned groups for the new user. Since you copied the account, these will update to match the original account you used to make the copy.

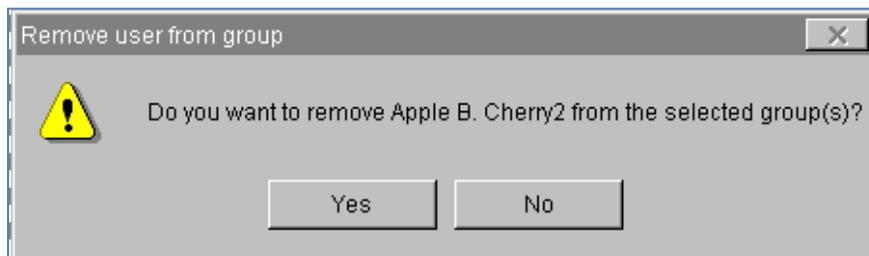
Basically, you want to make sure that the new user has the proper groups assigned. In the example below, the new user has a *Functional Group* assigned. For “how-to” sake, we are going to say this person is NOT a G081 Manager, and therefore should not have this group in their profile.

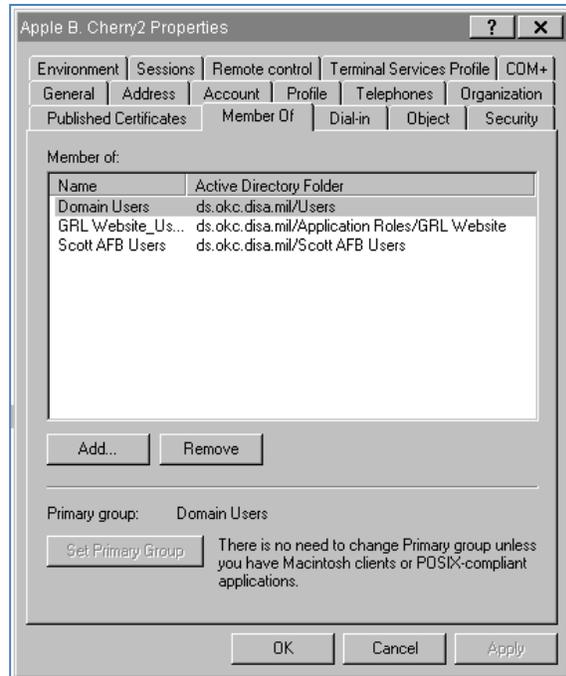
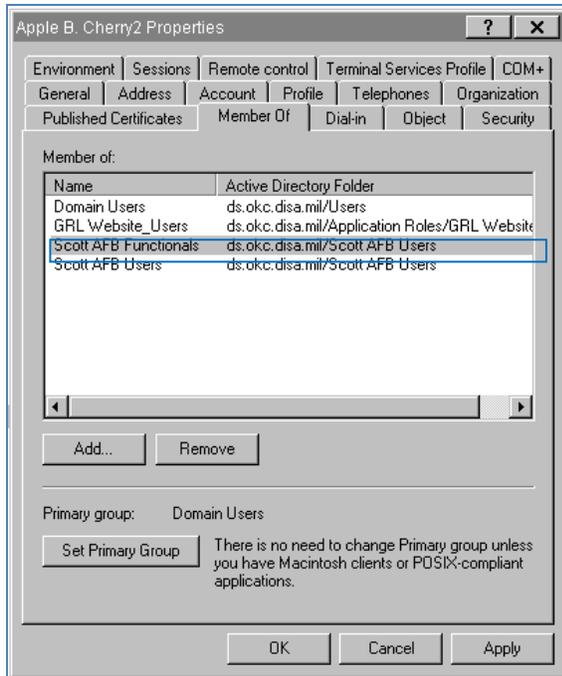


To remove the unnecessary group, select it from the list and click **Remove**.

**NOTE:** The **Member of** tab will always default to the first group on the list, so be sure to select the one you really want to remove.

You will have the opportunity to review/verify your selection from the **Remove user from group** pop-up. Be sure you highlighted the correct group, then hit **Yes**.





You will immediately see that the group has been removed from the user's **Member of** list. Hit **Apply** and then **OK** to update the user's profile and exit the **Properties** window.

## **ALL DONE... !?**

We have now covered all aspects of assigning new members access to G081. Once accounts are created, they must be maintained. This includes everything from password resets to account deletions.

As with creating new accounts, managing existing accounts must be accomplished in both TSO and User Manager.

## **IMPORTANT NOTES ABOUT G081 PASSWORDS**

The password used to register your CAC card will **NOT** expire.

- Users will only need to change this password if/when they change their USERID as a result of PCS

- CAC card replacements should retain log-in information, but if the data does not carry over, a reset and new password may be necessary

**G081 Managers MUST** keep their manual log-in passwords current

- Mainframe passwords expire every 65-days

- Mainframe password expiration will **NOT** affect your CAC log-in accessibility

  - Suspended, Locked or Disabled accounts WILL affect your CAC log-in

- Password expiration **WILL** affect your TSO log-in accessibility

  - Recommend you log into TSO at least once every 30-days to ensure your manual log-in remains active and you receive timely notification when it is time to reset your password

  - Traditional Guardsmen and Reservist should log into TSO at least once every drill

Now that we have answered the 2 biggest questions up front, let's talk about managing G081 user accounts in TSO and User Manager.

## **MANAGING USER ACCOUNTS IN TSO**

In the past, the two most frequently used account management features in TSO were resetting passwords and unsuspending accounts. In the WebG081 environment, you will reset passwords for general users in User Manager, but other account management actions will still be performed in TSO.

### **◆ Reset Passwords**

Why are we covering it here? Because you, the G081 Manager, Maintenance Management Analysts and anyone who needs to use the MIAP connection process require mainframe access and will occasionally need to be reset.

Log-in to TSO as described in the "[ACCESSING TSO VIA MIAP](#)" section of this guide.

Once you reach the **G081 User ID Maintenance Facility** page, you can reset the user's G081 password by inputting "2" for the **OPTION**, entering the user's G081 USERID in the **User ID** field and hitting ENTER.

```

OGD MTZ-CLASS MODEL2 - 1
File Edit Connection Setup Macro Views Help
----- G081 User ID Maintenance Facility -----
COMMAND ==>>
                                     TIME - 12:34
                                     DATE - 11/12/07

OPTION ==> 2                          User ID==> MAMOABC

1 - Add New User ID
2 - Reset User ID
3 - Display User ID
4 - Modify User ID
5 - Delete Existing User ID
6 - List All Users (as of approx 0215 Central Time)
7 - List All Inactive Deleted G081 Users
F - Add or Remove IMS Facilities
M - Manage CITRIX/RUMBA Connection for this User ID
B - Manage CITRIX/RUMBA Connection for an entire Base
R - List Users Overriding the CITRIX Connection

X - Exit

For a list of userids with various select & sort options, use
batch program 67041
PF 1=HELP      2=SPLIT      3=END      4=RETURN      5=RFIND      6=RCHANGE
PF 7=UP        8=DOWN       9=SWAP     10=LEFT      11=RIGHT     12=RETRIEVE
MAM+ >> 05/014
5,14 >> bin3270 | ZE | Connected | Bound | 3,1 RSA with triple DES | tn3270c:/maproxy.csd.dsa.mf-443

```

This will take you to the **G081 Reset User ID** page.

```

OGD MTZ-CLASS MODEL2 - 1
File Edit Connection Setup Macro Views Help
----- G081 Reset User ID -----
COMMAND ==>>
                                     TIME - 12:40
                                     DATE - 11/12/07

User ID == MAMOABC
Name == CHERRY, APPLE B

Change Password ==>> N
Un-Suspend ==>> N

PF3 - Exit

PF 1=HELP      2=SPLIT      3=END      4=RETURN      5=RFIND      6=RCHANGE
PF 7=UP        8=DOWN       9=SWAP     10=LEFT      11=RIGHT     12=RETRIEVE
MAM+ >> 09/038
9,38 >> bin3270 | ZE | Connected | Bound | 3,1 RSA with triple DES | tn3270c:/maproxy.csd.dsa.mf-443

```

The **Change Password** field will always default to "N", as shown. Verify that the **Name** of the individual you need to reset before proceeding. Occasionally a user may give you an incorrect USERID, especially if it has a number at the end and they give you their full initials.

Once you have verified the **User ID** and **Name**, input “**Y**” in the **Change Password** field and hit ENTER.

```
----- G081 Reset User ID -----
COMMAND ==>

                                TIME - 12:41
                                DATE - 11/12/07

User ID == MAMOABC
Name == CHERRY, APPLE B

Change Password ==> Y      New password = q@C1JuRY
Un-Suspend ==> N

PF3 - Exit

PF 1=HELP      2=SPLIT      3=END      4=RETURN      5=RFIND      6=RCHANGE
PF 7=UP        8=DOWN        9=SWAP     10=LEFT      11=RIGHT     12=RETRIEVE
MAM+ >>> 09/038
```

TSO will auto-generate a temporary password for the user. When the user logs in the first time, they will be prompted to change the password.

**Temporary passwords are only valid for 24-hours.** Once reset, the user should log in immediately to set-up their personal password.

### ◆ **Unsuspend Accounts**

G081 accounts are suspended after 30-days of inactivity. Although this suspension will occur on the mainframe, it **WILL** also affect your CAC log-in. If this happens, the accounts can only be unsuspended in TSO.

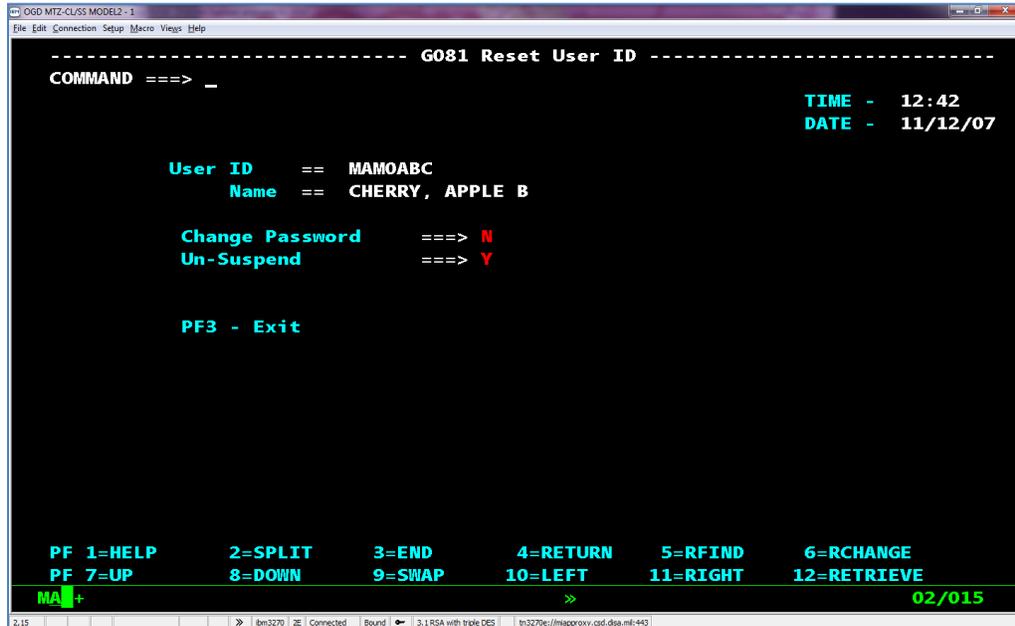
NOTE: Traditional Guard and Reserve member accounts should be set up for a 90-day inactivity bypass (*See page 11*).

In order to unsuspend an account, you must first log-in to TSO as described in the [“ACCESSING TSO VIA MIAP”](#) section of this guide.

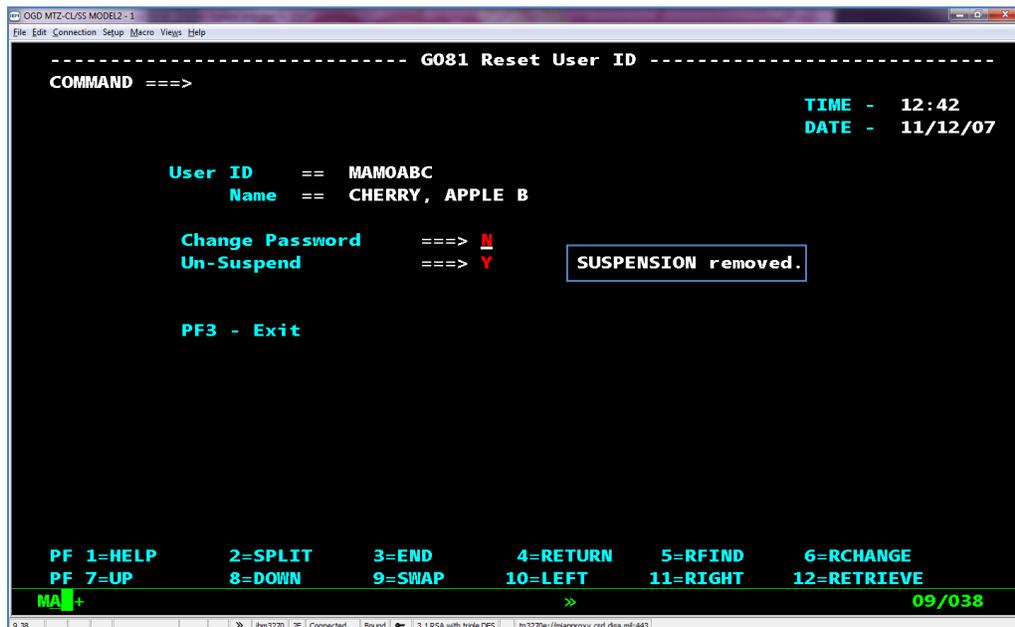
Once you reach the **G081 User ID Maintenance Facility** page, input “**2**” for the **OPTION**, enter the user’s G081 USERID in the **User ID** field and hit ENTER.

This will take you to the **G081 Reset User ID** page. You DO NOT have to reset the users account.

NOTE: For traditional guard/reserve members, the password will have expired by this point and should be reset as well.



Input "Y" in the **Un-Suspend** field and hit ENTER. You should see a message stating the suspension has been removed and the user can now log-in manually or using their CAC card. If you are also resetting the password, the auto-generated temporary password will also be shown.



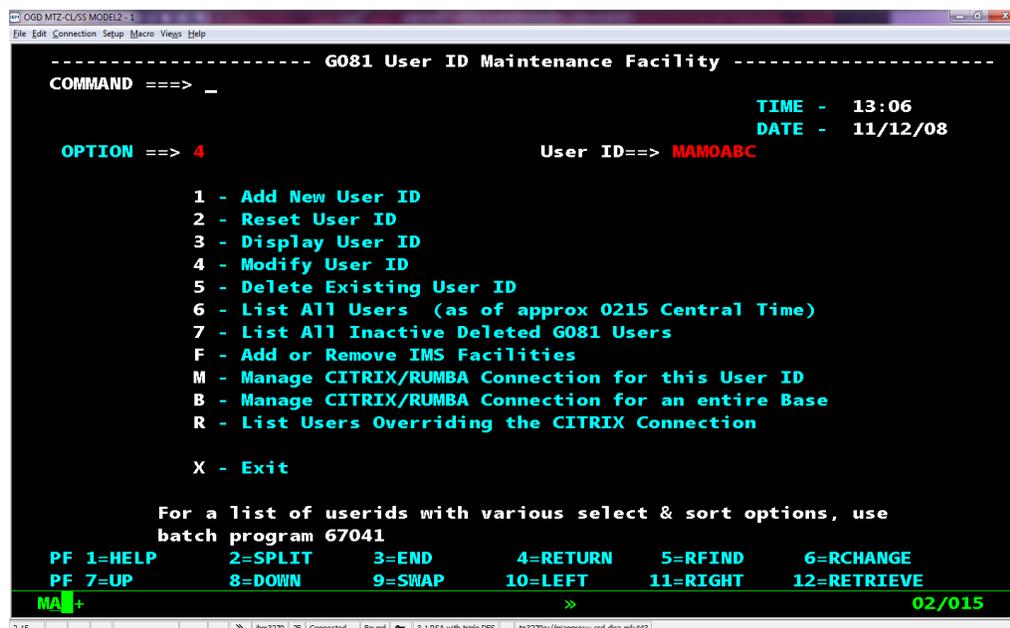
## ◆ Update User Information

The most obvious reason you would need to update user information would be for a name change. But, occasionally a user will change work centers or organizations (ie MSL moved from the MXG to the LRS).

In these situations, the user information MUST be updated on the DD Form 2875 as well as in TSO and User Manager.

To begin, log-in to TSO as described in the [“ACCESSING TSO VIA MIAP”](#) section of this guide.

Once you reach the **G081 User ID Maintenance Facility** page, input “4” for the **OPTION**, enter the user’s G081 USERID in the **User ID** field and hit ENTER.



```
----- G081 User ID Maintenance Facility -----
COMMAND ==> _
                                     TIME - 13:06
                                     DATE - 11/12/08
OPTION ==> 4                          User ID==> MAMOABC

 1 - Add New User ID
 2 - Reset User ID
 3 - Display User ID
 4 - Modify User ID
 5 - Delete Existing User ID
 6 - List All Users (as of approx 0215 Central Time)
 7 - List All Inactive Deleted G081 Users
 F - Add or Remove IMS Facilities
 M - Manage CITRIX/RUMBA Connection for this User ID
 B - Manage CITRIX/RUMBA Connection for an entire Base
 R - List Users Overriding the CITRIX Connection

 X - Exit

For a list of userids with various select & sort options, use
batch program 67041
PF 1=HELP   2=SPLIT   3=END     4=RETURN   5=RFIND   6=RCHANGE
PF 7=UP     8=DOWN    9=SWAP   10=LEFT    11=RIGHT  12=RETRIEVE
MAM+ >>> 02/015
```

This will take you to the **G081 User ID Modify** page.

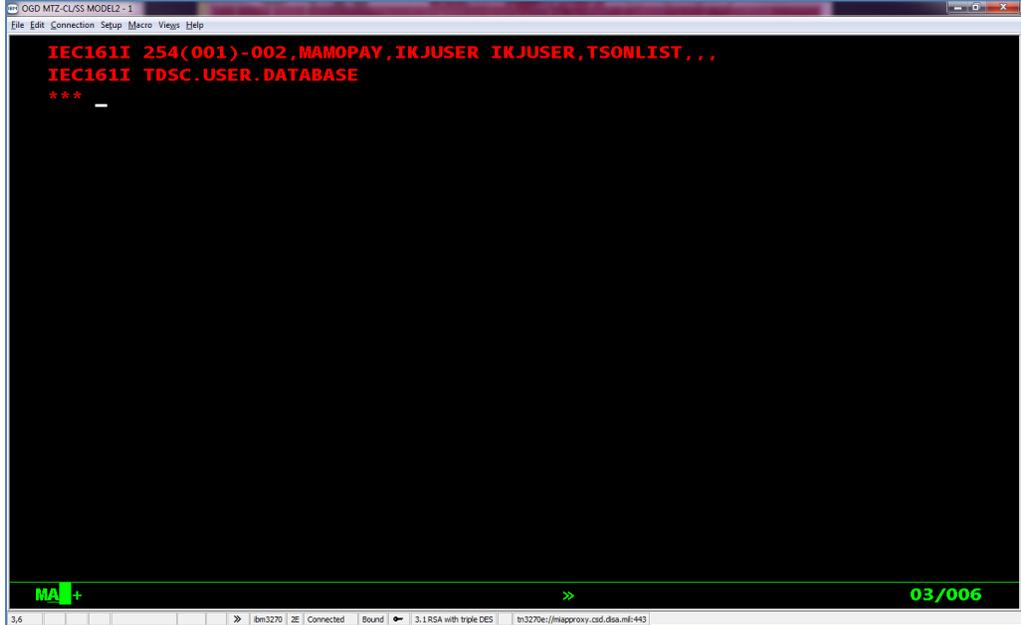
The member’s G081 USERID should be pre-filled in the **User ID** field.

Input “1” for the **OPTION** and hit ENTER.

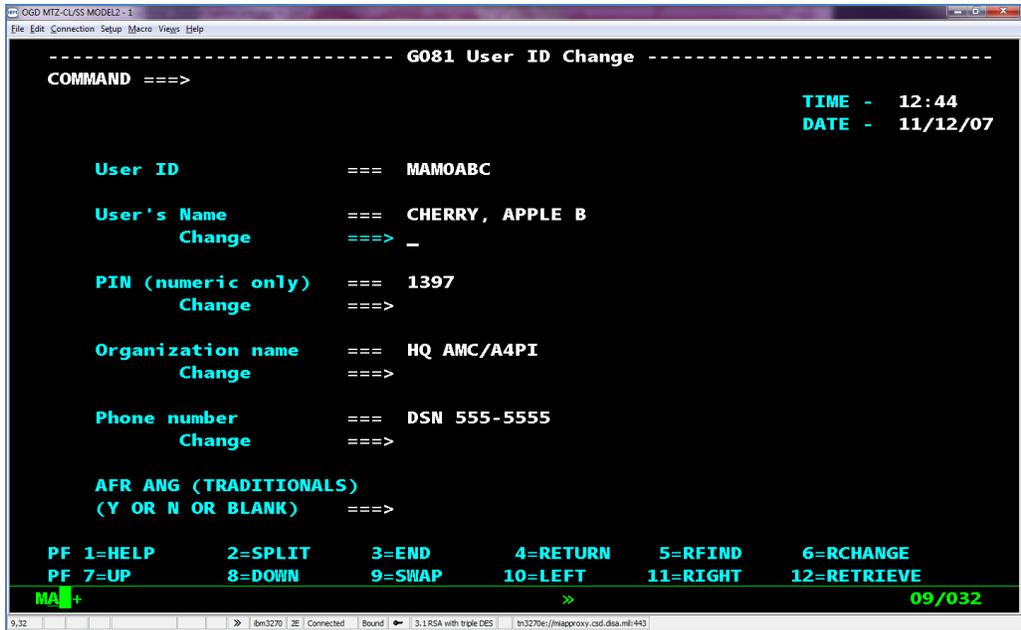


The first screen you will see is a verification of YOUR user information and access.

Hit ENTER to bring up the user's current account data.



Once you reach the **G081 User ID Change** screen, you can update/change key pieces of information for the user.



Below each current data field is a **Change** field. Input the updated information in this area. You can change one item or all using this transaction.

After all the changes have been made, hit ENTER.



NOTE: There is no option to change the **User ID**. If the user or you wish to assign a new USERID, you must delete the old account and create a new one. You should get a message as shown below stating that the process was successful and showing YOUR user data.

```

OGD MTZ-CLASS MODEL2 -1
File Edit Connection Setup Macro Views Help
TSS0300I REPLACE FUNCTION SUCCESSFUL
TSS0423I FROM: COMM
TSS0300I REPLACE FUNCTION SUCCESSFUL

IEC161I 254(001)-002,MAMOPAY,IKJUSER IKJUSER,TSOONLIST,,,
IEC161I TDSC.USER.DATABASE
***
-

MA + >> 07/006
7,6 |>| bin3270 | Z | Connected | Bound | 3.1.RSA with triple DES | bin3270e://mapproxy.csd.dsa.mil-443

```

Hit ENTER to return to the **G081 User ID Maintenance Facility** page.

The members **User ID** should be pre-filled.

Input “3” for the **OPTION** and hit ENTER to verify any name changes were saved.

```

OGD MTZ-CLASS MODEL2 -1
File Edit Connection Setup Macro Views Help
ACCESSORID = MAMOABC NAME = CASTLE, APPLE B
TYPE = USER SIZE = 512 BYTES
FACILITY = IMSPROD
ADMIN BY= BY(MAMOPAY ) SMFID(MTA ) ON(11/23/2011) AT(13:54:21)
FACILITY = QTA1MSTR
ADMIN BY= BY(MAMOPAY ) SMFID(MTA ) ON(11/23/2011) AT(13:54:21)
DEPT ACID = MAMODEPT DEPARTMENT = SCOTT AFB (AFRC), HQAMC (AMC)
DIV ACID = VG081 DIVISION = G081 USER DIVISION
ZONE ACID = ZUSERS ZONE = TDSC END USERS AND RES ZONE
CREATED = 11/23/11 13:54 LAST MOD = 12/27/11 15:10
PROFILES = MAMOIMSP PBYPASS
ATTRIBUTES = ASUSPEND
INSTDATA = HQ AMC/A4MMT #1397
PASSWORD = EXPIRES = 01/01/80 INTERVAL = 060

TSS0300I LIST FUNCTION SUCCESSFUL
***
-

MA + >> 17/006
17,6 |>| bin3270 | Z | Connected | Bound | 3.1.RSA with triple DES | bin3270e://mapproxy.csd.dsa.mil-443

```

Repeat the steps outlined in this section to verify all other changes.

## ◆ Delete A User Account

As members leave the organization or move to positions where G081 access is no longer required, their accounts should be deleted. You should ensure that the G081 Management office is annotated on your units out-processing checklist.

To delete users, log-in to TSO as described in the “[ACCESSING TSO VIA MIAP](#)” section of this guide.

Once you reach the **G081 User ID Maintenance Facility** page, input “**5**” for the **OPTION**, enter the user’s G081 USERID in the **User ID** field and hit ENTER.

```
----- G081 User ID Maintenance Facility -----
COMMAND ==>> _
                                     TIME - 12:45
                                     DATE - 11/12/07
OPTION ==>> 5                        User ID==>> MAMOAB1

1 - Add New User ID
2 - Reset User ID
3 - Display User ID
4 - Modify User ID
5 - Delete Existing User ID
6 - List All Users (as of approx 0215 Central Time)
7 - List All Inactive Deleted G081 Users
F - Add or Remove IMS Facilities
M - Manage CITRIX/RUMBA Connection for this User ID
B - Manage CITRIX/RUMBA Connection for an entire Base
R - List Users Overriding the CITRIX Connection

X - Exit

For a list of userids with various select & sort options, use
batch program 67041
PF 1=HELP      2=SPLIT      3=END      4=RETURN      5=RFIND      6=RCHANGE
PF 7=UP        8=DOWN       9=SWAP     10=LEFT      11=RIGHT     12=RETRIEVE
MA+                                                    02/015
```

This will bring up the user’s account information page where you will be prompted to verify that you want to delete the account.

Input “**1**” for YES or “**2**” for NO, as shown below, and hit ENTER.

```

OGD MTZ-CLASS MODEL2 - 1
File Edit Connection Setup Macro Views Help
ACCESSORID = MAMOAB1   NAME       = BOTELLO, ARACELI
TYPE       = USER     SIZE       = 512 BYTES
FACILITY   = IMSPROD
  ADMIN BY= BY(MAMODAT )   SMFID(MTA )   ON(03/17/2011) AT(08:38:55)
FACILITY   = QTA1MSTR
  ADMIN BY= BY(MAMODAT )   SMFID(MTA )   ON(03/17/2011) AT(08:38:55)
DEPT ACID = MAMODEPT DEPARTMENT = SCOTT AFB (AFRC), HQAMC (AMC)
DIV ACID  = VG081   DIVISION   = G081 USER DIVISION
ZONE ACID = ZUSERS  ZONE       = TDSC END USERS AND RES ZONE
CREATED   = 03/17/11 09:38 LAST MOD = 11/17/11 02:20
PROFILES  = MAMOIMSP
ATTRIBUTES = ASUSPEND
LAST USED = 10/17/11 12:20 CPU(MTA ) FAC(IMSPROD ) COUNT(00009)
INSTDATA  = 435 SCOS/GWL #2210

TSS0300I LIST      FUNCTION SUCCESSFUL

>>> DO YOU REALLY WANT TO DELETE MAMOAB1 ? (1)YES (0)NO

1_
MA +
20/002

```

Once you hit ENTER, you will see a message at the bottom of the screen stating that the account has been deleted from the database.

```

OGD MTZ-CLASS MODEL2 - 1
File Edit Connection Setup Macro Views Help
ACCESSORID = MAMOAB1   NAME       = BOTELLO, ARACELI
TYPE       = USER     SIZE       = 512 BYTES
FACILITY   = IMSPROD
  ADMIN BY= BY(MAMODAT )   SMFID(MTA )   ON(03/17/2011) AT(08:38:55)
FACILITY   = QTA1MSTR
  ADMIN BY= BY(MAMODAT )   SMFID(MTA )   ON(03/17/2011) AT(08:38:55)
DEPT ACID = MAMODEPT DEPARTMENT = SCOTT AFB (AFRC), HQAMC (AMC)
DIV ACID  = VG081   DIVISION   = G081 USER DIVISION
ZONE ACID = ZUSERS  ZONE       = TDSC END USERS AND RES ZONE
CREATED   = 03/17/11 09:38 LAST MOD = 11/17/11 02:20
PROFILES  = MAMOIMSP
ATTRIBUTES = ASUSPEND
LAST USED = 10/17/11 12:20 CPU(MTA ) FAC(IMSPROD ) COUNT(00009)
INSTDATA  = 435 SCOS/GWL #2210

TSS0300I LIST      FUNCTION SUCCESSFUL

>>> DO YOU REALLY WANT TO DELETE MAMOAB1 ? (1)YES (0)NO

1
IEC161I 254(001)-002,MAMOPAY,IKJUSER,IKJUSER,FT09K01,,
IEC161I TDSC.USER.DATABASE
MAMOAB1 DELETED FROM DATABASE
***
MA +
24/006

```

To verify that the account has been removed from the database, return to the **G081 User ID Maintenance Facility** page, input “3” as the OPTION and the USERID you deleted in the **USER ID** field.

When you hit ENTER, you should be directed to a screen stating the below:

```

TSS0314E ACID DOES NOT EXIST
TSS0301I LIST      FUNCTION FAILED, RETURN CODE = 8

```

## MANAGING USER ACCOUNTS IN USER MANAGER

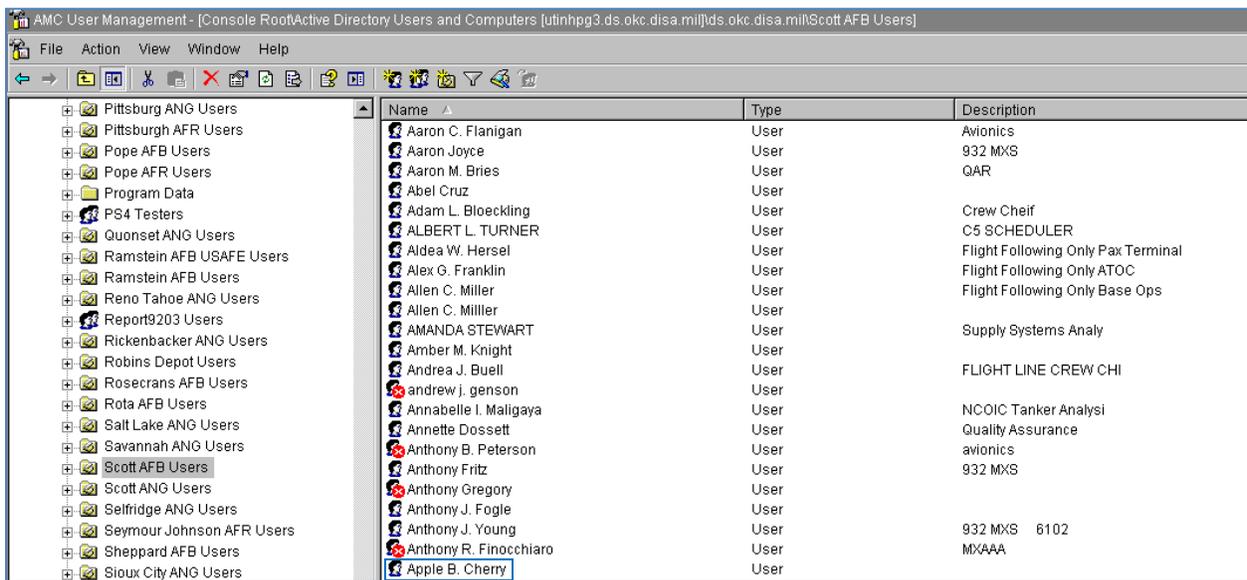
Just like creating new user accounts, any updates/changes to the users account information should be mirrored in both TSO and User Manager. The only

### ◆ Reset Passwords

As a rule, once a user registers their CAC for access to G081, they shouldn't need to have their password reset. The log-on credentials used when registering the CAC **WILL NOT** expire. However, there are exceptions to every rule.

Resetting passwords in User Manager is very easy. Log-in to User Manager as outlined in the [CREATING NEW USER ACCOUNTS IN USER MANAGER](#) section of this guide.

Once you have the **AMC User Management Console** open, right click on the name of the user you need to reset.



Select **Reset Password...** from the pop-up window to access the **Reset Password** feature.



### Password Parameters

Must be EXACTLY 8-characters in length  
*\*\*size may increase in the near future\*\**

Must contain at least 1 of each character type  
-Uppercase  
-Lowercase  
-Number  
-Special Character (**ONLY @, #, \$ are allowed**)

Characters cannot be consecutively repeated  
(22, mm, AA, @@)

System recalls previous 10 passwords and will reject if input

Rejects may occur for using common words/names in your password

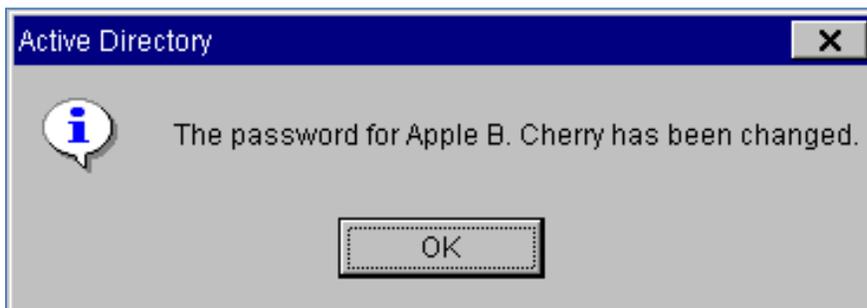
Input the user's new password.

**DO NOT** check **User must change password at next logon**

*Currently, there is no auto-generate capability in User Manager. This feature is being reviewed for a future update, but in the meantime, you must manually create and input the passwords. You can choose to have the user create their own for you to input.*

Once you have input the information in the **New password:** and **Confirm password:** areas, hit **OK**.

You will then get a confirmation pop-up telling you that the password for the user has been changed.



If there were any issues with the selected password, you will receive a pop-up letting you know what needs to be resolved. Fix and re-submit.

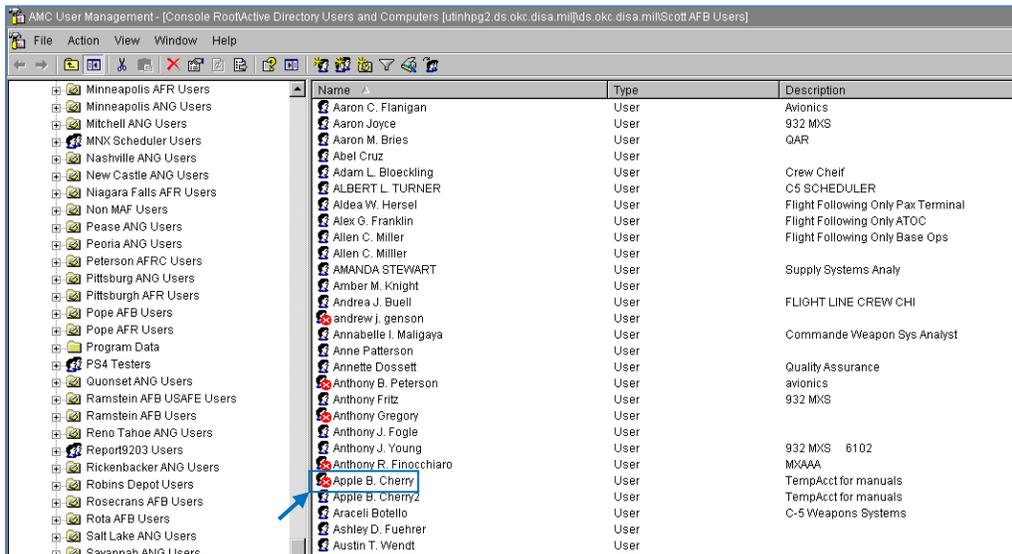
### ◆ **Enable Disabled Accounts**

Although most users will no longer be worried with resetting their passwords “every 5 minutes”, the responsibility to maintain a current account still applies.

Users must log-in to G081 (via CAC or manually) at least once every 65-days to ensure their User Manager account is not DISABLED. If this occurs, they will not be able to access G081 using their CAC or manually.

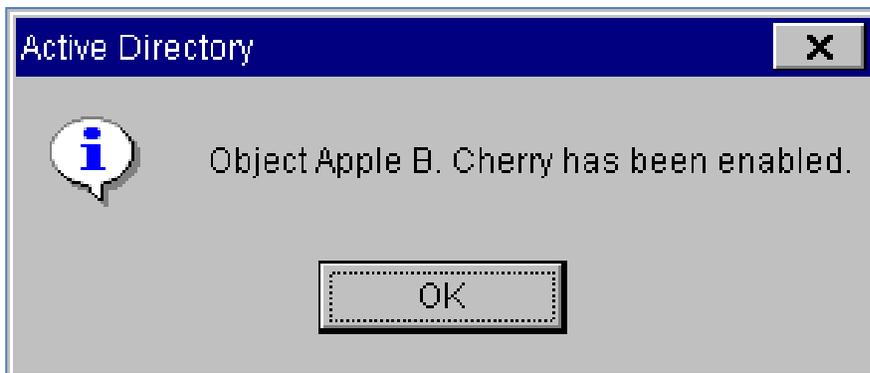
If a user account is DISABLED, you will need to log into User Manager as outlined in the [CREATING NEW USER ACCOUNTS IN USER MANAGER](#) section of this guide.

When you have the **AMC User Management Console** open, you will see a very distinctive mark (  ) on the user icon for the member.



Right click on the user's name and select **Enable Account** from the pop-up window.

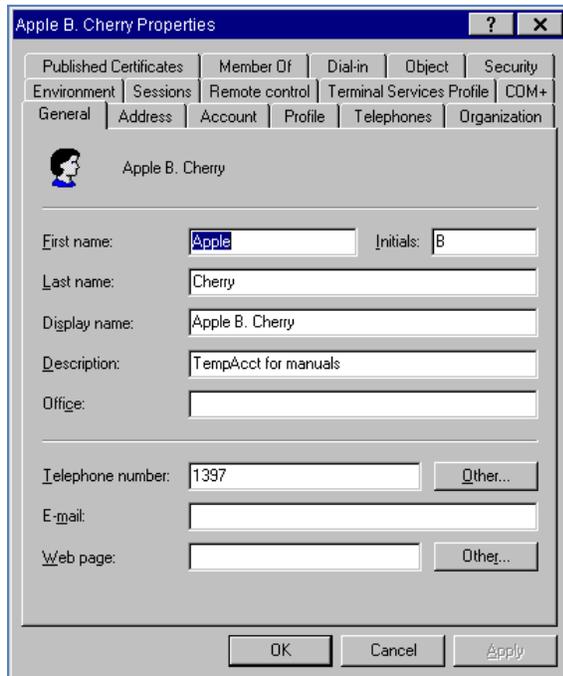
You should get a pop-up verifying that the account has been enabled.



## ◆ Updating User Information

All changes to user account information can be made in the user's Properties window in User Manager. Follow the log-in instructions specified in the [CREATING NEW USER ACCOUNTS IN USER MANAGER](#) section of this guide to get to the **AMC User Management Console**.

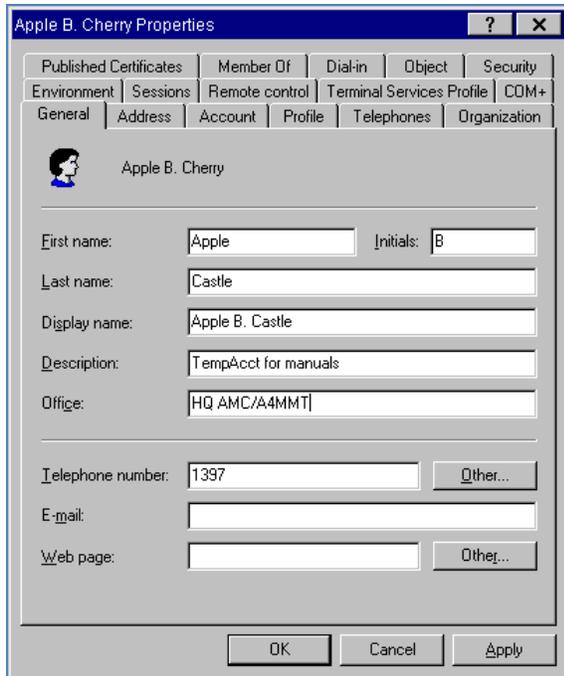
Once there, right mouse click on the user you need to update and select **Properties** from the pop-up window.



Over-type the information you need to update, or add in any additional information you want to include in the user's profile.

**NOTE:** When changing the user's name, be sure to update the **Display Name** as well to update the information that is shown in the user list.

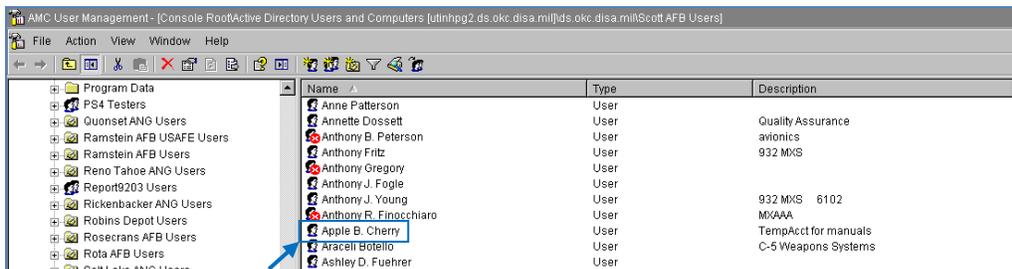
Once you have made all the necessary changes, hit **APPLY** to update the user's account information.



Verify that the information updated and hit **OK**.

You may have to refresh the user list, but you should see the name updated here as well.

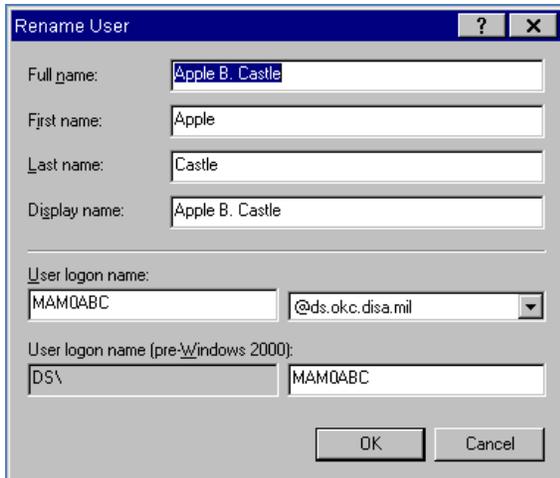
NOTE: If the name does not update on the user list, you can do it manually.  
 -- Right mouse click on the user name



-- Select **Rename** from the pop-up

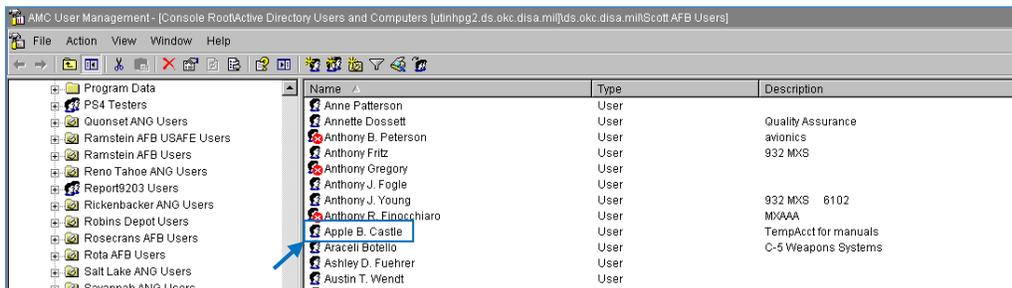
-- Type in the corrections and hit ENTER

-- Next you will get a **Rename User** pop-up



-- Verify the updated name is correct and hit **OK**.

-- You should now see that the user name on the user list matches the changes you made to the account properties



### ◆ Deleting User Accounts

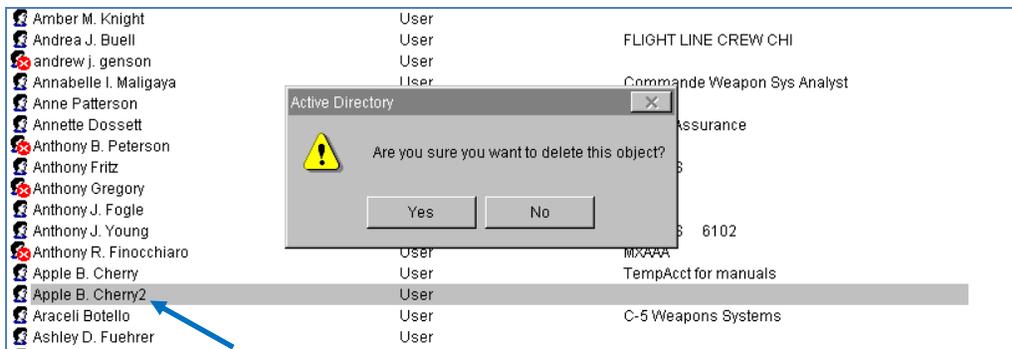
When a user leaves the unit or no longer has a need to access G081, you should delete their account immediately.

Log-in to User Manager as outlined in the [CREATING NEW USER ACCOUNTS IN USER MANAGER](#) section of this guide.

Locate the user in the list and right mouse click on the name.

From the pop-up window, click **Delete**.

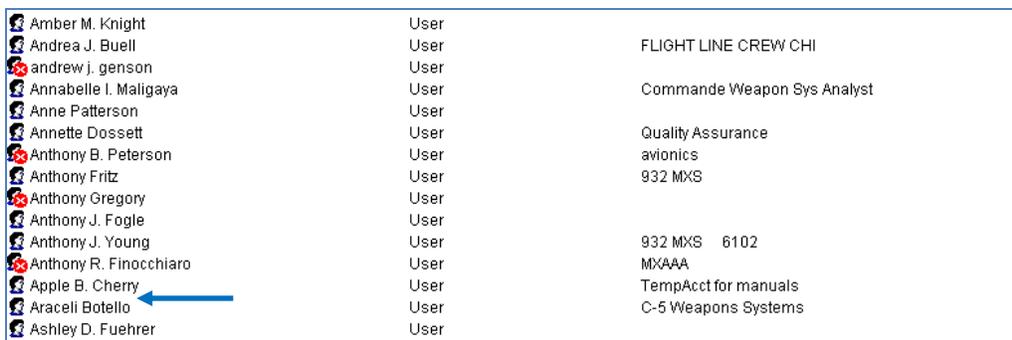
This will bring up an **Active Directory** pop-up asking you to verify the requested action.



You will notice that the user name is not shown in the **Active Directory** box. Before making your selection, check to be sure that the correct user name is highlighted on the list.

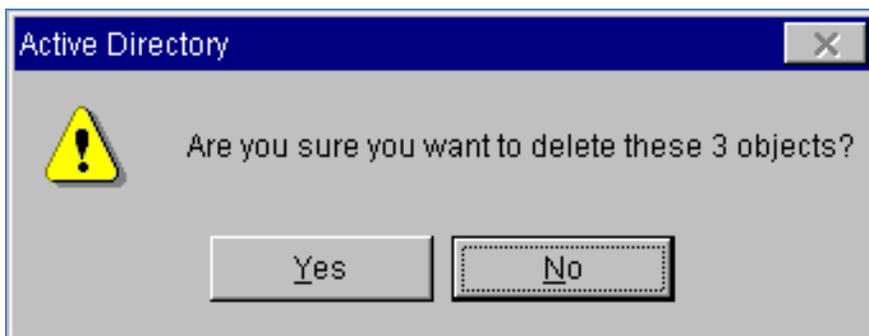
If everything is correct, click **Yes**.

You should immediately see the user name removed from the list



NOTE: If you have multiple users to delete, you can do so by holding down the CTRL key and selecting all of the accounts you want to remove.

Once you have finished making your selections, right mouse click on any of the highlighted names and select **Delete** from the pop-up.



The **Active Directory** will specify the number of names selected. Be sure this number is accurate and that the correct names are highlighted before selecting **Yes**.

## **CREATING ACCOUNTS FOR GLOBAL REACH (GR) ACCESS ONLY**

In the past, all maintenance and aircraft related reports were only available through G081. This meant that supervisors and commanders were dependent upon the G081 Management/Analysis office to provide them the data or keeping their G081 accounts current just to run an occasional report themselves.

Now, most of these same reports are available in the Global Reach environment. GR is a CAC accessible website where users can run real-time reports on anything from aircraft to member training status. Users with a CAC enabled G081 account automatically have access to the GR environment.

However, there will be cases where a member will want/need GR access but not have a need to use G081 (i.e. Commanders, Superintendants, etc.) In these cases, the G081 Manager must create a GR Only account in User Manager.

NOTE: Before you ask, regardless of whether or not the user falls under the Maintenance umbrella, the G081 Manager is responsible for creating ALL new user accounts in User Manager. This means if someone from Ops, at the Wing level or any other unit organization needs it... YOU are the OPR!

To get started, log-in to User Manager as outlined in the [\*\*CREATING NEW USER ACCOUNTS IN USER MANAGER\*\*](#) section of this guide.

### **◆ Create A Global Reach ONLY Account Using the Copy Feature**

The only way to create a GR Only account is to copy a current user account and make the required changes for the new account.

**DO NOT** select a member with a white “X” in a red circle on their icon (). This means their account has been disabled. You want to copy from an active member in the desired group.

Once you have selected the copy from account, right mouse-click on the name. This will bring up a pop-up and you want to select the **Copy...** option.

This will bring up the **Copy Object – User** window.

Input the user's information as requested. You will notice that the **Full name** section will automatically update. **DO NOT** alter this information.

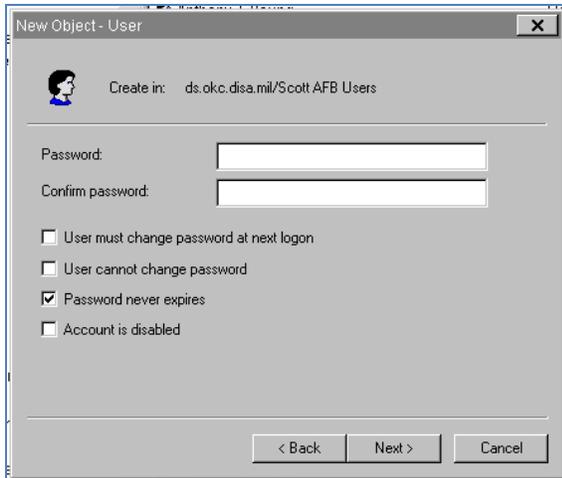
In first half of the **User logon name** field, you will create the users logon name in the format of **FirstName.LastName**.

You will notice that the logon name will automatically update in the second portion of the **User logon name (pre-Windows 2000)** field as you type.

The second portion of the **User logon name** field may be pre-filled. Ensure that it shows **@mil**. If not, use the dropdown menu to select this option.

Once you have input the required information, select **Next>**.

This will take you to the password page where will create a password for the user. To ensure security, you may want to have the user select a password prior to building the account.



### Password Parameters

Must be EXACTLY 8-characters in length  
*\*\*size may increase in the near future\*\**

Must contain at least 1 of each character type  
-Uppercase  
-Lowercase  
-Number  
-Special Character (**ONLY @, #, \$ are allowed**)

Characters cannot be consecutively repeated  
(22, mm, AA, @@)

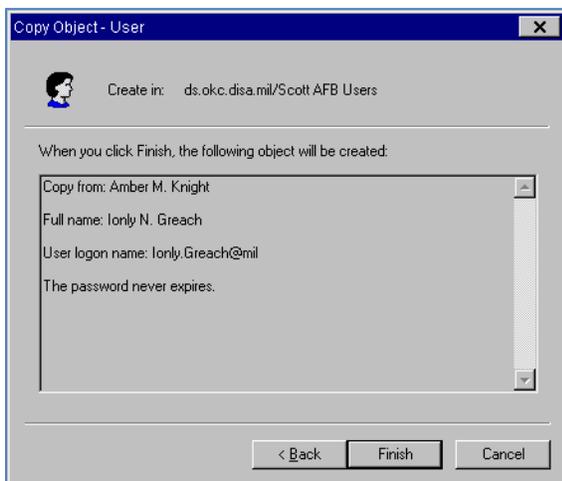
System recalls previous 10 passwords and will reject if input

Rejects may occur for using common words/names in your password

Ensure **User must change password at next logon** is **UNCHECKED**

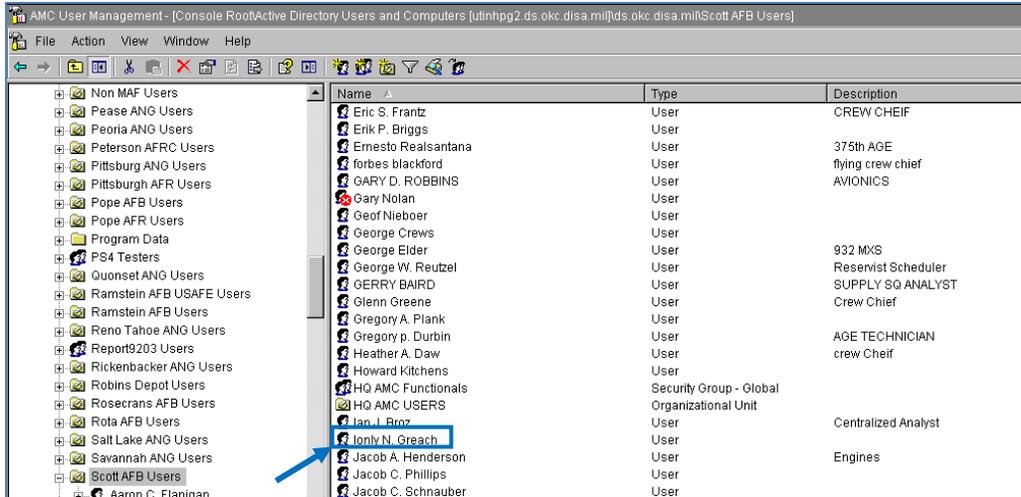
Ensure **Password never expires** is **CHECKED** and hit **Next>**.

You should see the below letting you know the user has been successfully copied from the user account you selected.



If you do not get this message, you should be given an error message specifying what needs to be corrected. Fix and re-submit.

Now that you have added the new user successfully, select **Finish**. You should see the new user in your group.

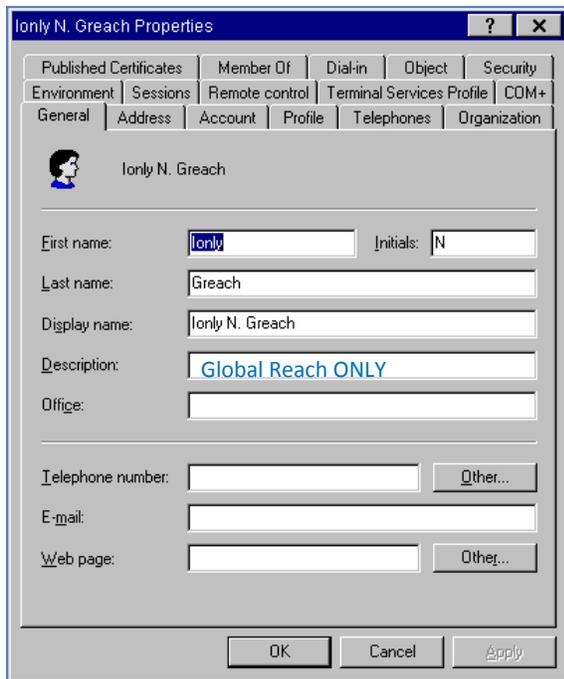


Now that you have added the user, you must make some additional annotations to the account for GR access and future reference.

Right mouse click on the user name and from the pop-up window, select **Properties**.

This will bring up the properties assigned to the users account. Most of the items will be updated by inputs made during the account creation or are pre-determined by the group where the user has been added.

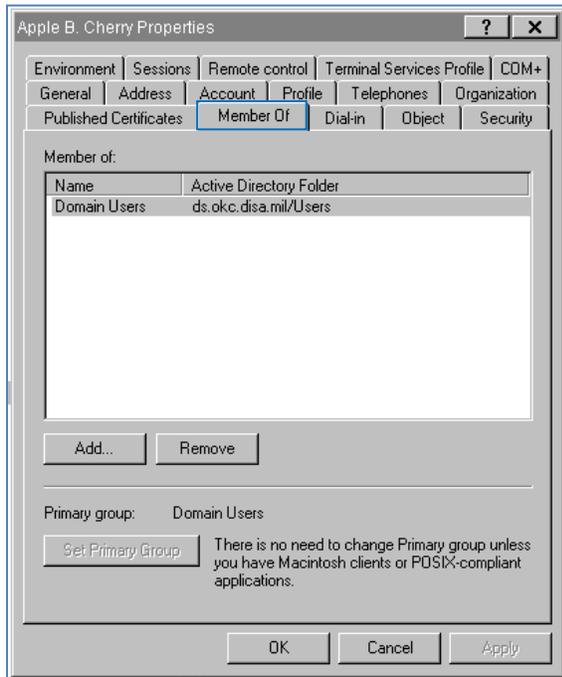
But there are some key pieces of information you will need to add to the user properties, as well as some recommended reference items.



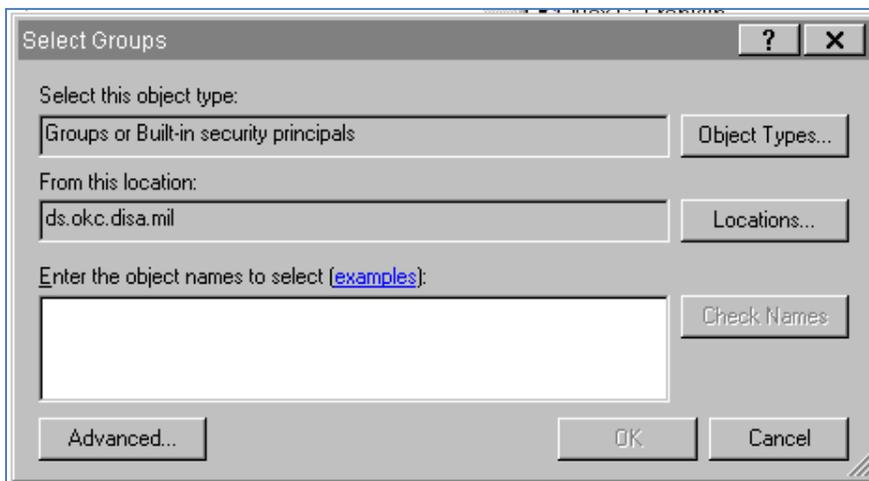
**Recommendation:** Use the Description field to input “Global Reach ONLY” for quick identification.

Next, you need to ensure that the user is a member of only the required groups for GR access, not G081. All new users will automatically have the *Domain Group* assigned but you will have to add the *Global Reach Group*.

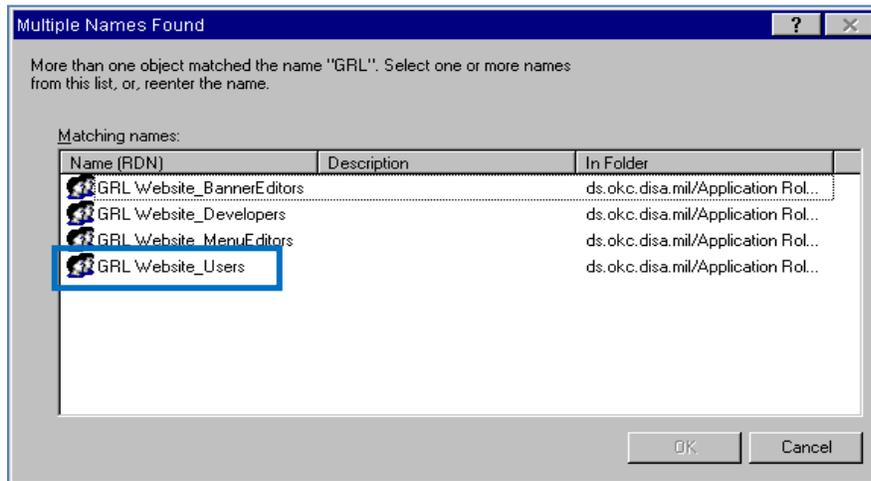
To review and/or add the required group(s) to a new user, select the Member of tab in the **Properties** window.



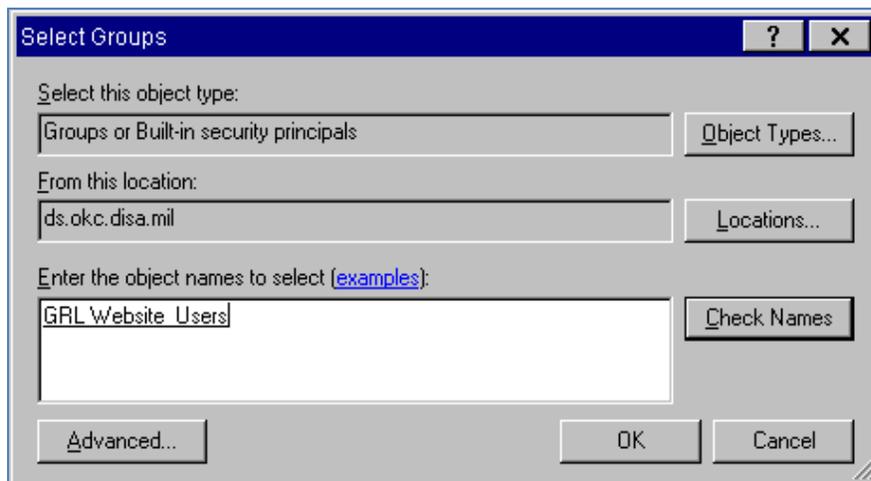
To add additional groups to the user, select the **Add...** button to bring up the **Select Groups** window.



In the **Enter the object names to select** box, type in **GRL**, then select **Check Name** to pull up a list of available groups that match your input.

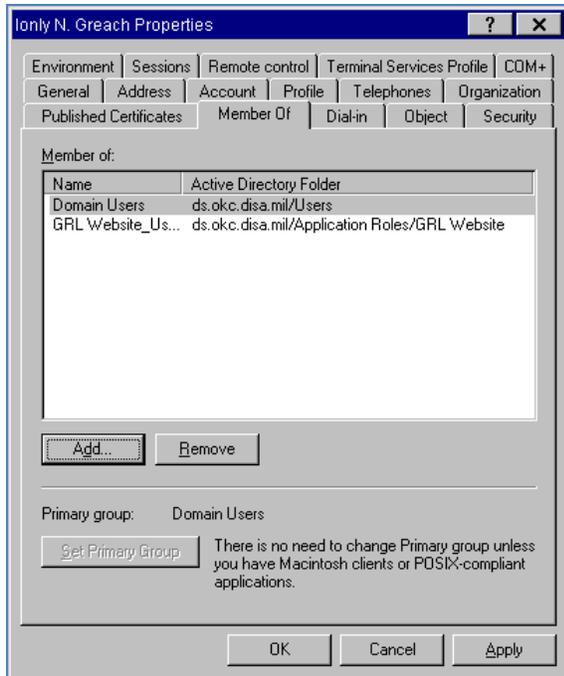


Select **GRL Website\_Users** and click **OK**. You will see that the domain group has been added to the **Enter the object names to select** box as a link.



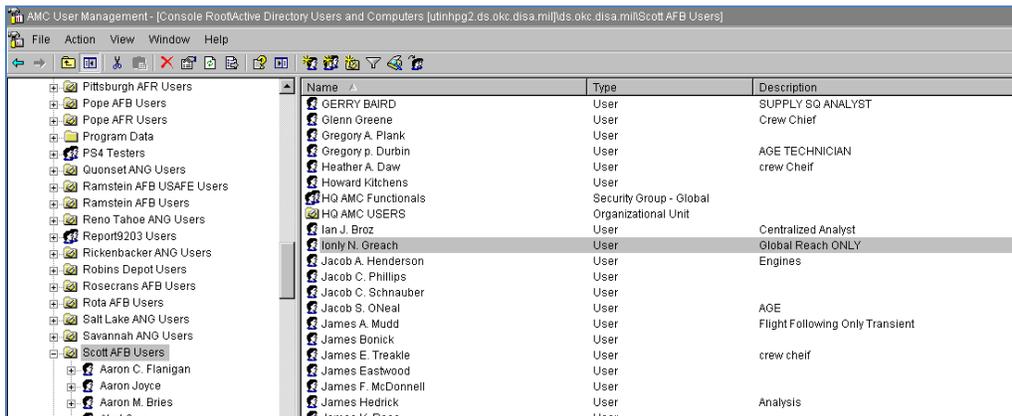
If this is correct, hit **OK**. If not, hit **Cancel** and begin again to make the correct selection.

You will now see the added group in the users **Member of** window.



Once you have finished, hit **Apply** and then **OK** to update the user profile and exit the **Properties** window.

You have now added a new user account for access to Global Reach and should see them in the user list.



**THE END...** At least until they create new stuff for us to do!