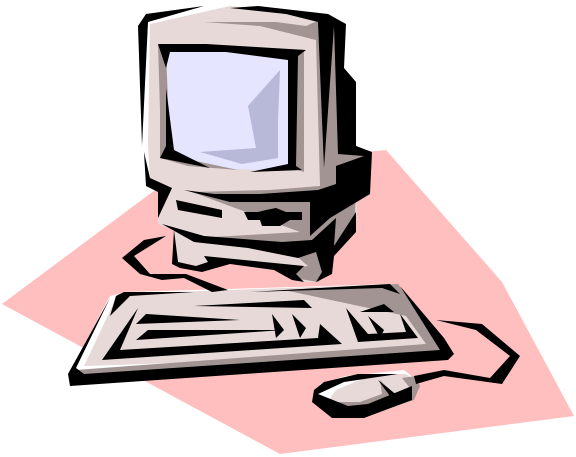
United States Department of Agriculture

SAMS
USER'S GUIDE
FOR THE PURCHASE CARD



Originated: JUNE 2000
Revised: SEPTEMBER 2000

Prepared by:

Office of Procurement, Property, and Emergency Preparedness
Procurement Modernization Team

Table of Contents

Page

INTRODUCTION **1**

SYSTEM OVERVIEW 1

SOFTWARE INSTALLATION 1

LOGGING ON/OFF SAMS 1

SAMS MAIN MENU 1

Menu Bar *2*

Requests 2

Reports 2

Window and Help 2

Bulletin Board *2*

USING FORMS, COMMAND BARS, AND MENU BARS 2

ESTABLISHING AND UPDATING USER IDS **4**

ESTABLISHING USER IDS 4

Establishing DPC and APC User Ids *4*

Establishing User Ids *4*

REQUESTS 5

Add user *6*

Drop User *8*

Insert SAC *9*

Modify Data *10*

Change Password *11*

Remove SAC *12*

REPORTS **14**

SAMS PROCESS FLOW **17**

CARDHOLDER SETUP & SAMS **18**

APPENDIX A: PCMS ROLES **19**

APPENDIX B: USER IDS AND PASSWORDS **20**

APPENDIX C: ERRORS **21**

INTRODUCTION

SYSTEM OVERVIEW

SAMS is a Windows-based system used to request access to applications and systems at the National Finance Center (NFC). This document will specifically cover the use of SAMS for requesting access to the Purchase Card Management System (PCMS). SAMS replaces a paper process by providing a graphical user interface front-end to enter security access requests online. The access requests are immediately stored in an NFC database. The requests are read and administered automatically by a batch program that runs twice a day, thus eliminating manual intervention and reducing turnaround time.

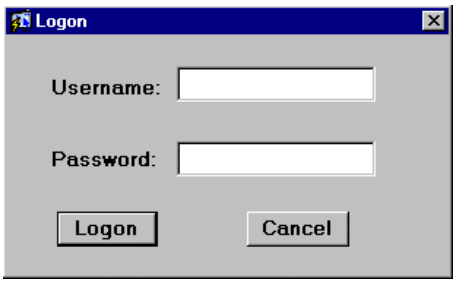
SOFTWARE INSTALLATION

SAMS software is part of the PCMS installation package. Refer to *Software Installation* in the *APC/LAPC PCMS User's Guide* for detailed instructions.

LOGGING ON/OFF SAMS

To access SAMS,

1. Double-click on the **SAMSv2 Prod** icon on your desktop. If you don't have the icon on your desktop, click on **Start>Programs>Purchase Card Management System Ver 4.0>SAMSv2 Prod**.
2. The WARNING popup window appears. Read the message and press **[OK]**.
3. The Logon popup window appears.



Enter your **USERNAME** and **PASSWORD** and press **[Logon]**.

Fieldname	Description
Username	Alphanumeric field, maximum of 20 positions (e.g., FS4003)
Password	Alphanumeric field, 6 to 20 positions (e.g., PCMS123)

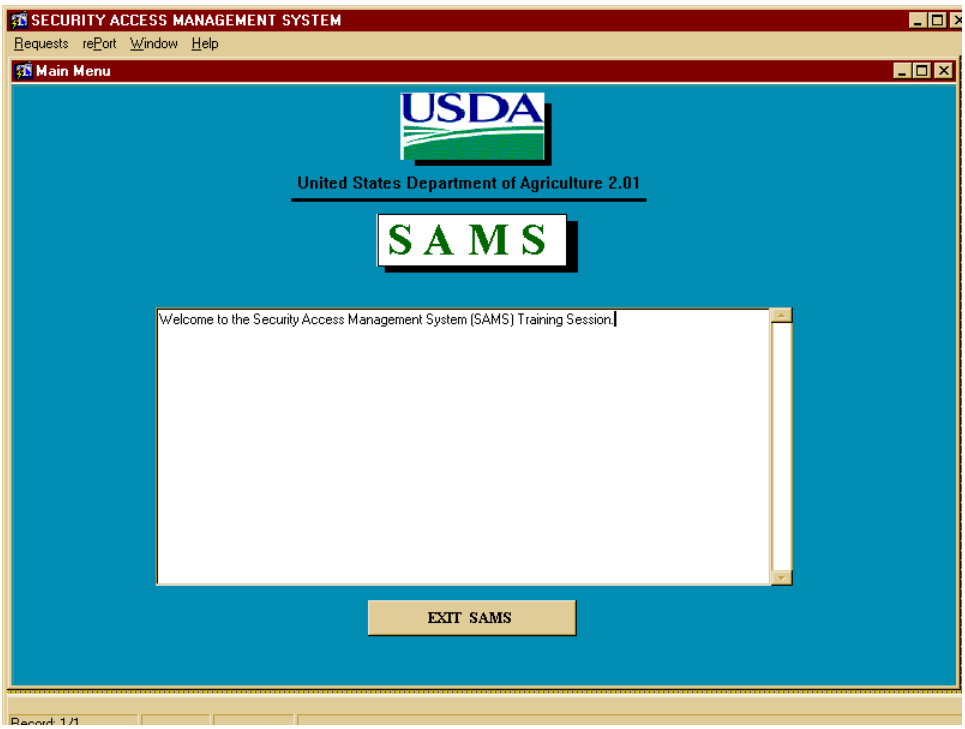
NOTE: Every 90 days your password expires and must be changed.

After you successfully log on, the SAMS Main Menu appears.

To exit SAMS, press **[Exit SAMS]** from the Main Menu.

SAMS MAIN MENU

After logging onto SAMS, the SAMS Main Menu appears:



Menu Bar

Requests

This option allows you to add or modify a user's access in PCMS. Refer to *Request* in *Establishing and Updating User Ids* for complete details.

Reports

This option is used to produce the Security Access Management Report. The report lists all records within your access that have either been added or had data changes prior to the date entered. Refer to the *Reports* section for complete details.

Window and Help

These two options are the same as in PCMS. Refer to *Introduction* in the *APC/LAPC PCMS User's Guide* for complete details.

Bulletin Board

The bulletin board, located in the center of the main menu screen, provides up-to-date news regarding security issues.

USING FORMS, COMMAND BARS, AND MENU BARS

SAMS uses data entry screens that are referred to as forms. Forms consist of an array of fields that are used to enter, update, and query data in the database. The command bars and menu bars located on forms windows provide options for you to perform the data query and entry functions. Moving around forms and using the command bars and menu bars in SAMS is the same as PCMS. Refer to the *Introduction* section of the *APC/LAPC PCMS User's Guide* for details.

ESTABLISHING AND UPDATING USER IDS

ESTABLISHING USER IDS

The information entered into SAMS is used to create a user id, if one does not already exist, set up the role, security profile (name, phone number, etc), and Security Access Code (SAC) information. SAMS is also used to change security information that was previously entered into SAMS. The role (APC, LAPC, etc.) defines the PCMS options to which a user has access. The SAC may be made up of any or all of the following: Department Code, Agency Code, Region, Unit, and Subunit. It defines the amount of information a user can see. For example a user with a SAC of Department Code 12, Agency Code 11, and Region 01 can see all credit card information for Region 01 of the Forest Service.

Establishing DPC and APC User Ids

When PCMS is initially implemented for an agency, the Departmental Program Coordinator (DPC) and Agency Program Coordinator (APC) will have to request SAMS access. A request must be sent via fax (504-255-4131) or e-mail (nfc.securityofc@usda.gov) to the Security Office at NFC including the following information:

1. Name
2. Phone number
3. SAC - Organizational structure (Department Code, Agency Code, Region, Unit, Sub Unit)
4. Your NFC user id, if you already have one

NFC will establish the SAMS record for the DPC and APC.

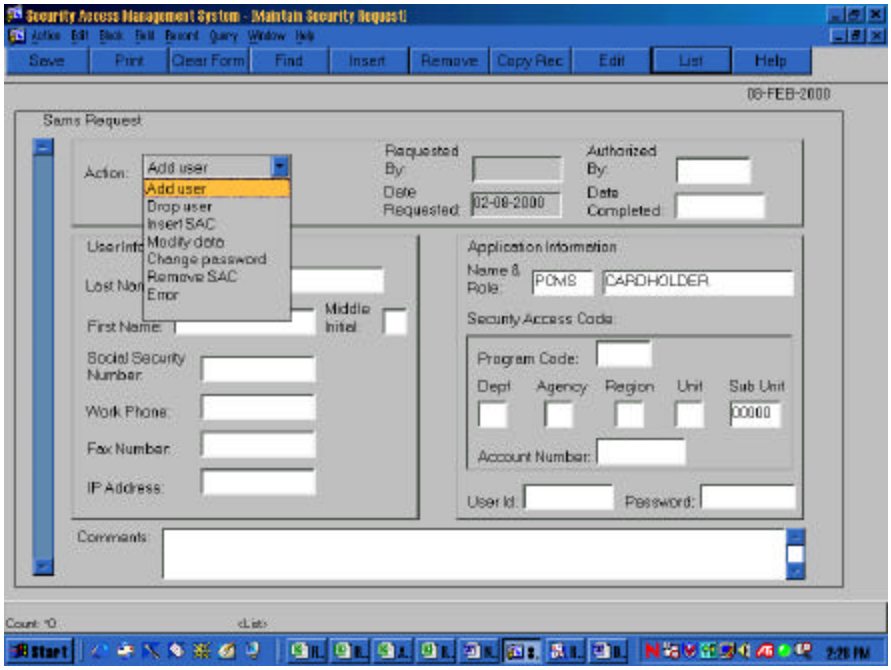
Establishing User Ids

The APC will use SAMS to request access to PCMS for their Local Agency Program Coordinators (LAPCs). The LAPC will then use SAMS to request access to PCMS for other LAPCs, Cardholders, and Financial Managers (FM) within their scope of responsibility. Access is automatically given to PCMS when the batch program runs. By the next business day, the LAPC, Cardholders, or FM can log on to PCMS.

The APC/LAPC will submit a request to NFC (using the fax or e-mail address listed above in *Establishing DPC and APC User Ids*) to request a block of user ids to be added to the USER ID drop-down list. Once this list has been populated, a user id can be established in SAMS by placing a cursor in the USER ID field, pressing [List], and selecting an id from the list provided. Refer to ***Requests*** for details in establishing a PCMS user in SAMS.

REQUESTS

Use the Request option to input security requests for access to PCMS. When you select this option, the following screen will be displayed:



The ACTION is the first field on the request screen. Press the **[Down Arrow]** to the right of the field to see a drop-down list of valid action codes:

A - Add user

D - Drop user

I - Insert SAC

M - Modify data

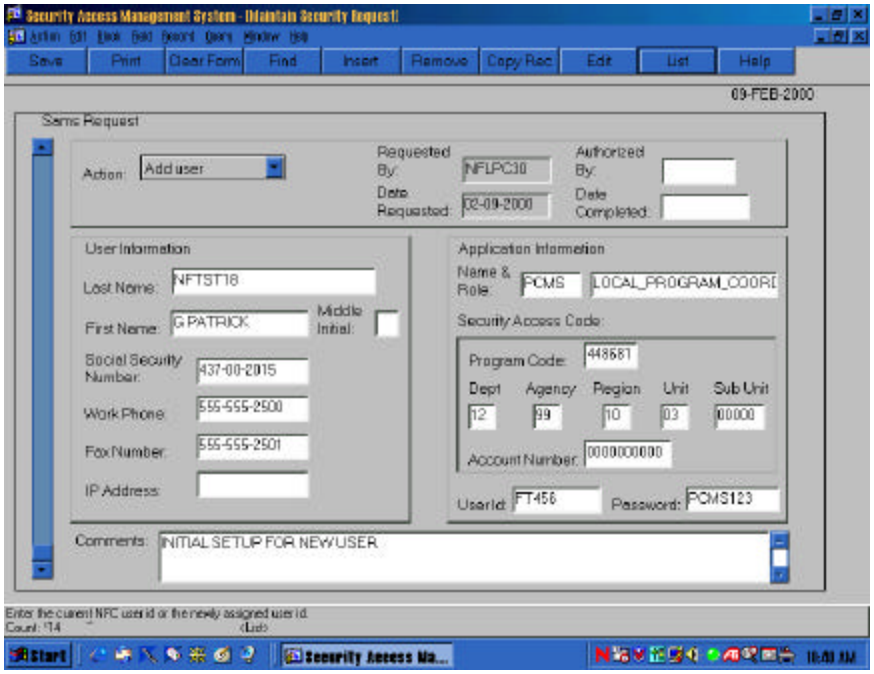
P - Change Password

V - Remove SAC

NOTE: If "Error" appears in this field, there has been a problem in processing this record. Refer to *Appendix C: SAMS Process Flow* later in this document to resolve errors.

Add user

Use this option to request access to PCMS for a user who does not currently have access. An example of a completed Add User request follows:



User Information and Application Information

The first region of the screen includes information about the person for which the request is being entered.

1. "Add user" will be defaulted in the **ACTION** field.
2. Click your mouse in the **LAST NAME** field, enter a last name and press **[Tab]**. This is mandatory.
3. Enter a **FIRST NAME** and press **[Tab]**. This is mandatory.
4. Enter a **MIDDLE INITIAL** and the cursor will move to the next field. This is optional.
5. Enter the **SOCIAL SECURITY NUMBER** without dashes (e.g., 434321254) and press **[Tab]**, the system will default in the dashes. This is mandatory.
6. Enter a **WORK PHONE** number without dashes (e.g., 5042525555) and press **[Tab]**, the system will default in the dashes. This is mandatory.
7. Enter a work **FAX NUMBER** without dashes (e.g., 5042558422) and press **[Tab]**, the system will default in the dashes. This is optional.
8. Enter an **IP** (Internet Provider) **ADDRESS** (e.g., 199.143.120) and press **[Tab]**. This is optional.
9. In the **NAME & ROLE** fields, "PCMS" and "CARDHOLDER" will be defaulted. Click in the **LAST NAME** field and press the **[List]** button to see a valid list of applications and roles. You must select one from the list by double-clicking it or by selecting it and pressing **[OK]**. Press **[Tab]** to move to the PROGRAM CODE field. This is mandatory. See Appendix A: PCMS Roles for a list and definition of each role.

NOTE: When a purchase card NAME &ROLE is selected (or if you accept the default and tab past these fields), the PROGRAM CODE field is populated with the appropriate program code.

Security Access Code

The next region of the screen includes the SAC information. It defines the user's level of access.

The following is a brief explanation of SAC's. A user who is at the top level of the organization would have the broadest access (e.g. a DPC could have a SAC of Department Code 12 which would allow him/her to see every record for every agency within the department). On the other hand, a user at the lowest level of the organization would have the most limited access (e.g. an LAPC could have a SAC of Department Code 12, Agency Code 11, Region 03, Unit 01, and Sub Unit 00000 which would only allow him/her to see his/her records).

An LAPC who needs to see several regions of a particular unit could have multiple SACs. If an LAPC in Agency 11 Region 03 needs to see all of Units 01, 02, and 03 then they could have the following three SACs: 12 11 03 01 00000, 12 11 03 02 00000, and 12 11 03 03 00000.

1. Enter the 6 digit **PROGRAM CODE** is populated when NAME & ROLE is selected. This is mandatory.
2. Enter the 2 digit **DEPARTMENT CODE** (e.g. 12 for USDA) and the cursor will move to the AGENCY field. This is mandatory.
3. Enter the 2 digit **AGENCY** (e.g. 11 for Forest Service) and the cursor will move to the REGION field. This is mandatory.
4. Enter the 2 digit **REGION** and the cursor will move to the UNIT field. If you don't have a region to enter, enter 00. This is mandatory.
5. Enter the 2 digit **UNIT** and the cursor will move to the sub unit field. If you don't have a unit to enter, enter 00. This is mandatory.
6. Enter the 5 digit **SUB UNIT** (with leading zeros if necessary) and the cursor will move to the account number field. If you don't have a sub unit to enter, leave **00000** in the field. This is mandatory.

   NOTE: Forest Service does not use sub units in PCMS for the purchase card.
7. When entering a request for an LAPC, a default of **0000000000** will be entered in the **ACCOUNT NUMBER** field. Do not enter anything else in this field if it is an LAPC. When entering a request for a role other than LAPC and Cardholder, the account number field is to remain blank. Enter the credit card account number if the role is Cardholder.
8. If the person you're requesting access for already has a NFC user id, you must enter that id in the **USER ID** field. If not, press **[List]** and a list of available user ids will be displayed. Select the next available user id by double-clicking on the user id or by selecting it and pressing **[OK]**. The cursor will move to the PASSWORD field. If the user already has a PCMS user id, enter the PCMS user id with an "A" or "B" at the end. This is mandatory.

   NOTE: To populate the drop-down listing of user ids, the APC needs to notify NFC requesting user ids for the specific number of new users.

   NOTE: The system will display a message if you enter a user id that has already been assigned in SAMS or that already belongs to a PCMS user. See *Appendix B: User Ids and Passwords* for additional information.
9. Enter a **PASSWORD** that is 6-8 positions long and contains both alpha and numeric characters. The password must begin with an alpha character. This is mandatory.
10. Enter any **COMMENTS** that you would like noted on the request. This is optional.

11. The **AUTHORIZED BY** field in the top right-hand corner of the screen is optional. If you would like to note the user id of the person who authorized the request, you may do so here.
12. Once the record has been processed, the DATE COMPLETED field will be completed by the SAMS batch program. This field will remain blank until the record is successfully processed.

You can make as many changes to this record as you need to, as long as the DATE COMPLETED field is null (blank). You may also delete the record if you decide you do not need it by pressing the **[Remove]** button, as long as the DATE COMPLETED field is null. Once the record has been processed by the SAMS batch program (DATE COMPLETED field is not null), you can no longer make any changes. Note that all fields on the screen are gray.

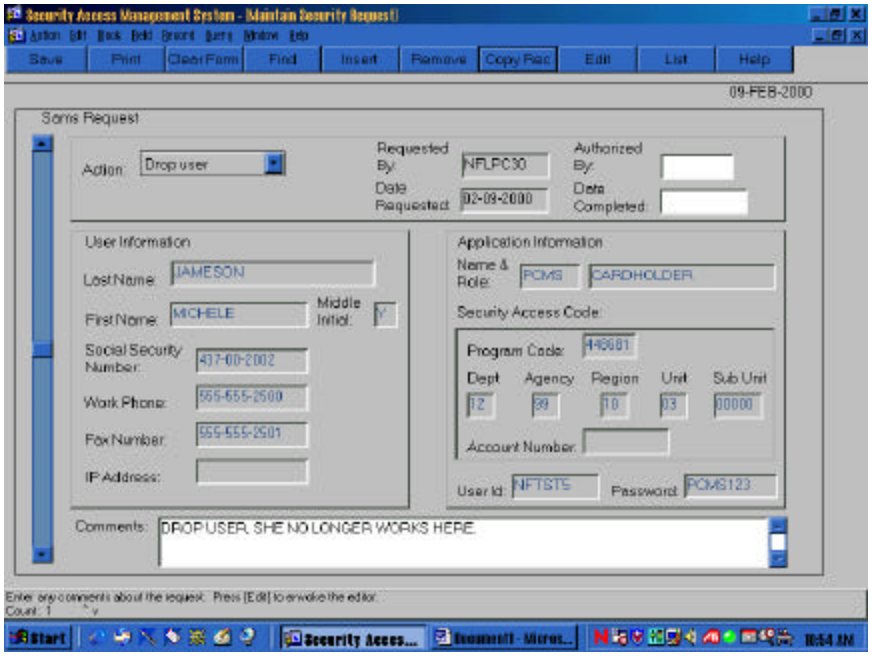
Drop User

Use this option to drop the user's access to PCMS. For LAPC's, ensure that all Cardholder records have been transferred from the LAPC before dropping their id and system access to PCMS.

NOTE: This will not revoke access to any other NFC applications or systems. To remove access to any other NFC systems from this id, you will need to contact the Security Office at NFC. Also, this option is not to be used to delete an erroneous SAC, use the Remove SAC action.

NOTE: If you mistakenly drop a user id, either call NFC to re-establish it or add a new user id.

An example of a completed Drop User request follows:



To drop access to PCMS, do the following:

1. Query up a record that was previously processed for the user (e.g. the Add user record).
   a. Press the **[Find]** button on the toolbar and a blank screen will be displayed. The system is waiting for you to indicate what to find.
   b. Enter the user's **USER ID**.

NOTE: You may query on any field on the screen like the NAME or SOCIAL SECURITY NUMBER, but it is recommend that you use USER ID for precise results.

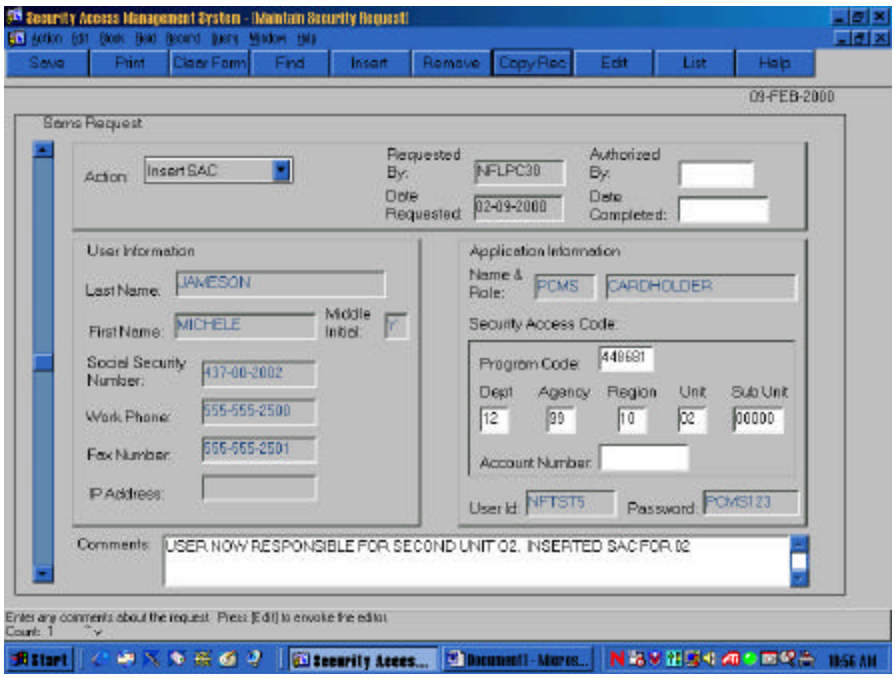
c. Press the **[Find]** button again and the record(s) will be displayed. If more than one record exists for that user the scroll bar on the left of the screen will be highlighted. It doesn't matter which record you choose to copy as long as the DATE COMPLETED field is not blank.

2. Press the **[Copy Rec]** button on the toolbar and the message "1 Record Copied" will be displayed. Press **[OK]**. When you press [OK], a copy of the record is displayed with the ACTION, AUTHORIZED BY and DATE COMPLETED fields blank. The AUTHORIZED BY and DATE COMPLETED fields will also appear white. This indicates that you may now make changes to those fields (all except the DATE COMPLETED field).
3. Select **Drop user** from the **ACTION** drop-down list.
4. Enter data in the **AUTHORIZED BY** field, if applicable. Enter comments regarding the changes made in the **COMMENTS** field.
5. Press **[Save]**.

Insert SAC

This option is used to insert an additional SAC for a user. For example, use this option when you have an LAPC who is responsible for 2 of the 10 units in a region. When they were originally set up, they were set up with a SAC of Dept 12, Agency 11, Region 03, Unit 01 and now they are also responsible for unit 02. You would insert another SAC for Department Code 12, Agency 11, Region 03, Unit 02.

An example of an Insert SAC request follows:



To insert an additional SAC, do the following:

1. Query up a record that was previously processed for the user (e.g., the Add user record).
   a. Press the **[Find]** button on the toolbar and a blank screen will be displayed. The system is waiting for you to indicate what to find.
   b. Enter the user's **USER ID**.

      NOTE: You may query on any field on the screen like the NAME or SOCIAL SECURITY NUMBER, but it is recommend that you use USER ID for precise results.

   c. Press the **[Find]** button again and the record(s) will be displayed. If more than one record exists for that user the scroll bar on the left of the screen will be highlighted. Make sure the DATE COMPLETED field is not blank and select the most current record to copy.
2. Press the **[Copy Rec]** button on the toolbar and the message "1 Record Copied" will be displayed. Press **[OK]**. When you press [OK], a copy of the record is displayed with the ACTION, AUTHORIZED BY and DATE COMPLETED fields blank. The AUTHORIZED BY and DATE COMPLETED fields will also appear white. This indicates that you may now make changes to those fields (all except the DATE COMPLETED field).
3. Select **Insert SAC** from the **ACTION** drop-down list and the fields in the *Security Access Code* region of the screen appear white.
4. Modify data in the ***Security Access Code*** region of the screen. In the example above you would change the unit from 01 to 02.
5. Enter data in the **AUTHORIZED BY** field, if applicable. Enter comments regarding the changes made in the **COMMENTS** field.
6. Press **[Save]**.

Modify Data

This option is used to modify the user profile information (name, social security number, etc.). To Modify data, do the following:

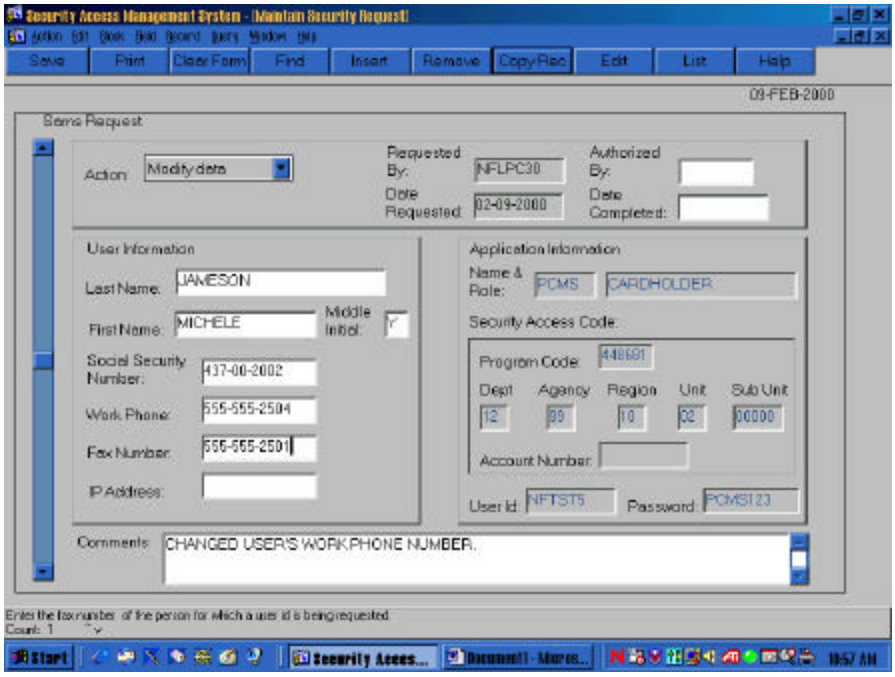
1. Query up a record that was previously processed for the user (e.g. the Add user record).
   a. Press the **[Find]** button on the toolbar and a blank screen is displayed. The system is waiting for you to indicate what to find.
   b. Enter the user's **USER ID**.

      NOTE: You may query on any field on the screen like the NAME or SOCIAL SECURITY NUMBER, but it is recommend that you use USER ID for precise results.

   c. Press the **[Find]** button again and the record(s) is displayed. If more than one record exists for that user the scroll bar on the left of the screen will be highlighted. Make sure the DATE COMPLETED field is not blank and select the most current record to copy.
2. Press the **[Copy Rec]** button on the toolbar and the message "1 Record Copied" will be displayed. Press **[OK]**. When you press [OK], a copy of the record is displayed with the ACTION, AUTHORIZED BY and DATE COMPLETED fields blank. The AUTHORIZED BY and DATE COMPLETED fields will also appear white. This indicates that you may now make changes to those fields (all except the DATE COMPLETED field).
3. Select **Modify Data** from the **ACTION** drop-down list and the fields in the *User Information* region of the screen will appear white.

4. Modify data in the ***User Information*** region of the screen.
5. Enter data in the **AUTHORIZED BY** field, if applicable. Enter comments regarding the changes made in the **COMMENTS** field.
6. Press **[Save]**.

An example of a completed Modify Data request follows:



Change Password

This option is used to reset a user's password. Use this option when you've received a call from a user saying they have forgotten their password or that it has expired. To change a user's password, do the following:

1. Query up a record that was previously processed for the user (e.g. the Add user record).
   a. Press the **[Find]** button on the toolbar and a blank screen will be displayed. The system is waiting for you to indicate what to find.
   b. Enter the user's **user id**.

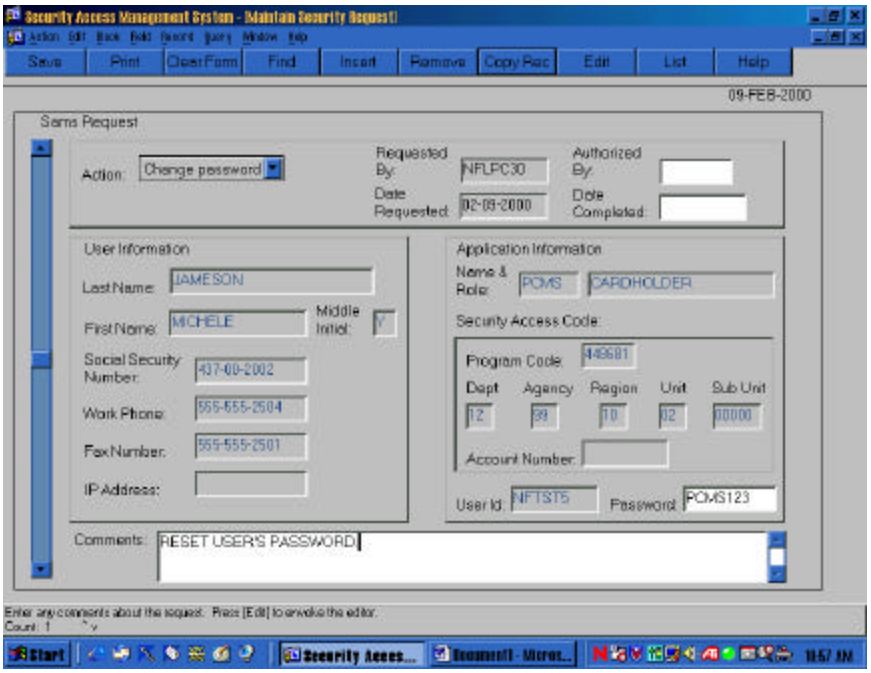
      NOTE: You may query on any field on the screen like the NAME or SOCIAL SECURITY NUMBER, but it is recommend that you use USER ID for precise results.

   c. Press the **[Find]** button again and the record(s) will be displayed. If more than one record exists for that user the scroll bar on the left of the screen will be highlighted. Make sure the DATE COMPLETED field is not blank and select the most current record to copy.
2. Press the **[Copy Rec]** button on the toolbar and the message "1 Record Copied" will be displayed. Press **[OK]**. When you press [OK], a copy of the record is displayed with the ACTION, AUTHORIZED BY and DATE COMPLETED fields blank. The AUTHORIZED BY and DATE COMPLETED fields will also

appear white. This indicates that you may now make changes to those fields (all except the DATE COMPLETED field).

3. Select **Change Password** from the **ACTION** drop-down list and the PASSWORD field will become white.
4. Change the **password** to something you haven't used before with that user id. Remember that the password should be 6-8 alphanumeric characters.
5. Enter data in the **AUTHORIZED BY** field, if applicable. Enter comments regarding the changes made in the **COMMENTS** field.
6. Press **[Save]**.

An example of a completed Change Password request follows:



Remove SAC

Use this option to remove a SAC that may have been entered erroneously or that is no longer needed.

To remove a user's SAC, do the following:

1. Query up the record that was used to Add the user or the one used to Insert another SAC for the user (e.g., if the user only has one SAC it would be the Add user record that you would query up. If the user has more than one SAC, then query up the record that contains the SAC you're trying to remove).
   a. Press the **[Find]** button on the toolbar and a blank screen will be displayed. The system is waiting for you to indicate what to find.
   b. Enter the user's **USER ID** and **SAC** information.

NOTE: You may query on any field on the screen like the NAME or SOCIAL SECURITY NUMBER, but it is recommend that you use USER ID and SAC information for precise results.

c. Press the **[Find]** button again and the record(s) will be displayed. If more than one record exists for that user the scroll bar on the left of the screen will be highlighted. Scroll down until you find the appropriate record, e.g., the record that contains the SAC you want removed. If you don't find a record that contains the SAC to be removed, copy the most current record and change the SAC information to correspond to the SAC you want removed.

2. Press the **[Copy Rec]** button on the toolbar and the message "1 Record Copied" will be displayed. Press **[OK]**. When you press [OK], a copy of the record is displayed with the ACTION, AUTHORIZED BY and DATE COMPLETED fields blank. The AUTHORIZED BY and DATE COMPLETED fields will also appear white. This indicates that you may now make changes to those fields (all except the DATE COMPLETED field).

3. Select **Remove SAC** from the **ACTION** drop-down list.

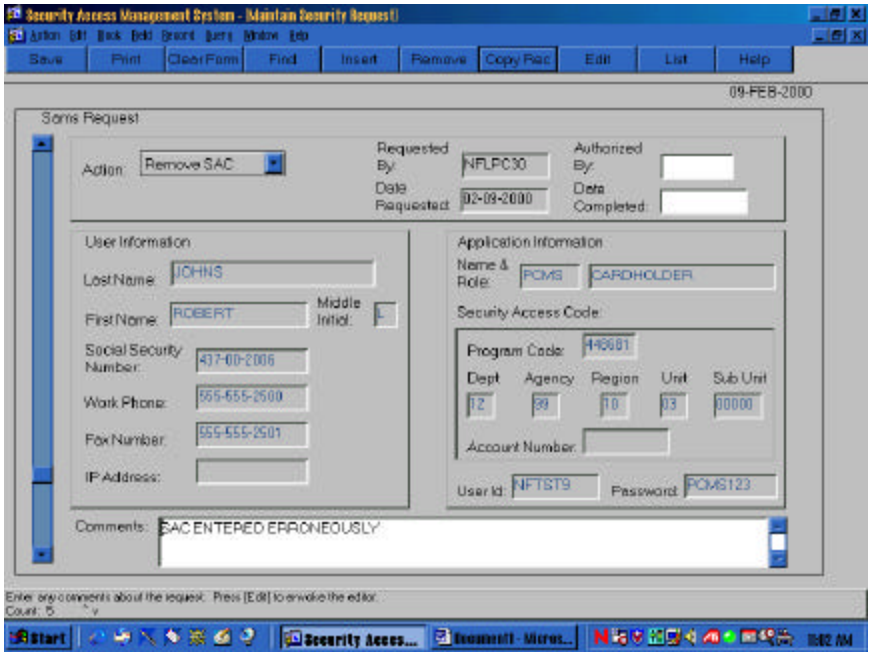
4. Enter data in the **AUTHORIZED BY** field, if applicable. Enter comments regarding the changes made in the **COMMENTS** field.

5. Press **[Save]**.

NOTE: You will not be able to remove a SAC if that SAC has records attached to it. For example, if you attempt to remove the SAC of an LAPC but that LAPC is attached to cardholder records in PCMS, then you will not be able to remove that SAC. All of the cardholders must be transferred to another LAPC before the SAC can be removed. An edit message will appear alerting you to this situation when you press [Save], "You cannot remove this SAC, there are transactions attached to it." Press [OK]. Then, press [Remove] to delete this request and press [Save].

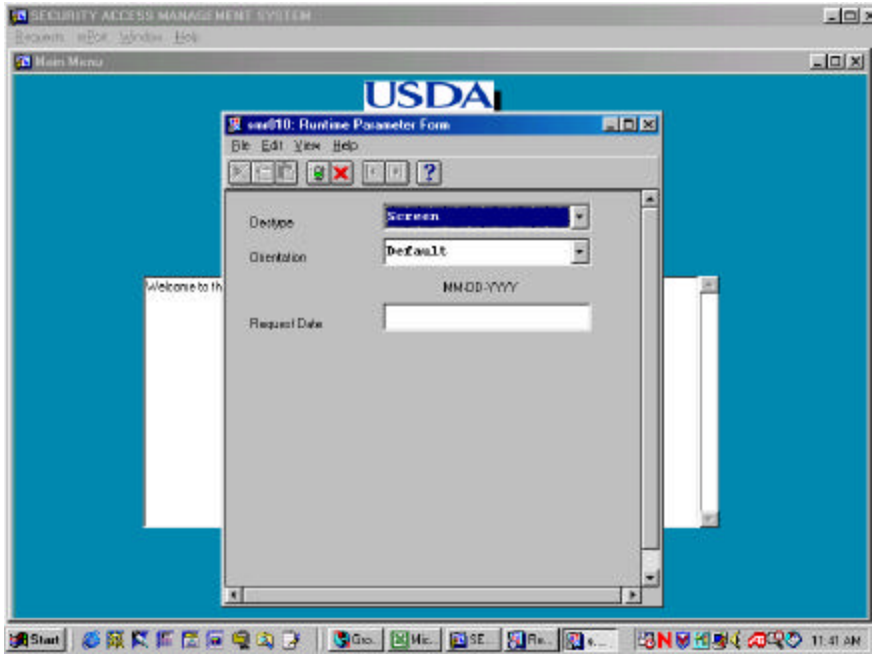
If the SAC information does not match the sac to be removed, change the SAC information to correspond to the one to be removed.

An example of a completed Remove SAC request follows:



REPORTS

After you select the Reports option, the smr010: Runtime Parameter form window appears.



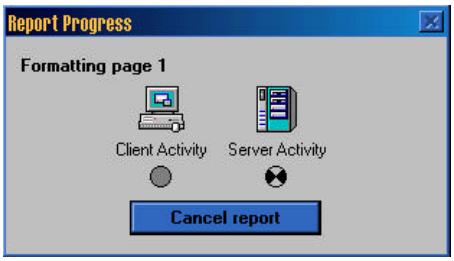
The report is created based on the DATE REQUESTED on the SAMS Requests. Complete the screen as follows:

Fieldname	Description
DESTYPE	Select an option from the drop-down menu. Screen is the default. *Screen* - Routes the output to the Previewer, truncates report if printed *File* – Saves the output to a file in DESNAME. *Printer* – Routes the output to a printer named in DESNAME. *Mail* – Sends the output to mail user specified in DESNAME. *Preview* – Routes the output to the Previewer, does not truncate report if printed.
ORIENTATION	Select an option from the drop-down menu. Default is the default. *Default* – Means use the current printer setting for orientation. *Landscape* – Means the pages are wider than they are tall. *Portrait* – Means the pages are taller than they are wide. Note: Select Landscape for the SAMS report.

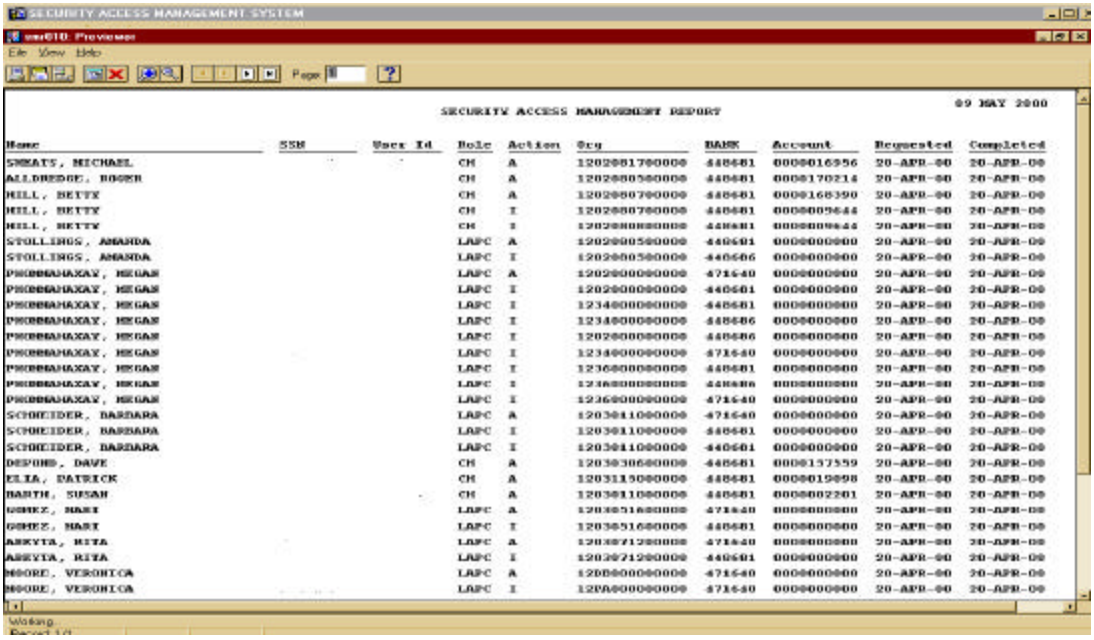
Fieldname	Description
REQUEST DATE	Type the date that you want the report to cover. The report returns all records with dates greater than or equal to the request date entered (e.g., if 03-13-1999 is entered, the report returns records where the date requested field is 03-13-1999 and greater.)

To run a report:

1. Select the **DESTYPE**.
2. Select the **ORIENTATION**.
3. Enter the **REQUESTED DATE** as MM-DD-YYYY (e.g., 10-01-1999)
4. Click **signal light icon** to generate the report to the requested destination type. The Report Progress window displays showing client and server activity. To cancel the report, press **[Cancel Report]**.



If you selected *Screen* or *Preview* in the DESTYPE field, the pfr010: Previewer window appears displaying the Security Access Management Report.



The following is a brief description of each field in the report:

Fieldname	Description
NAME	The assigned username (e.g., NFTST99, J Adams).
SSN	The Social Security Number of the user.
USER ID	The user's system identification number.
ROLE	User's role (e.g., CH = Cardholder).
ACTION	The Action Code: A – Add User D – Drop User I – Insert SAC M – Modify Data P – Change Password R – Remove SAC E - Error
ORG	User's SAC
BANK	Program Code
ACCOUNT	The last 10 digits of the cardholder's purchase card account number.
REQUESTED	Date action requested.
COMPLETED	Date NFC completed request.

5. Use the buttons at the top left of the Previewer window to view all pages of the report. Use the magnify buttons on the toolbar in the upper left of the window to adjust the size of the Previewer contents.

   For multipage reports, use the arrow command buttons at the top left side of the window to move through the pages. Note that to the right of the **Page:** field, you can enter the page number you want to go to and then press **[Enter]**.

   Press **printer icon** button if you want to print the report. You can either print the entire report or selected pages. If the report is going to print truncated, the system will notify you before printing.

6. Press **[X]** to return to the SAMS Main Menu.

SAMS PROCESS FLOW

1. The APC contacts the Security Office at NFC for access to SAMS via fax (504-255-4131) or e-mail (nfc.securityofc@usda.gov).
2. The APC will receive a user id and password to access SAMS.
3. The APC will utilize SAMS to establish LAPCs
4. The LAPC will establish Cardholder's, additional LAPCs, and FMs.
5. The SAMS batch program that runs at 1:00pm CST and 8:00pm CST will process each request.
6. After the batch program runs, the DATE COMPLETED field is updated on records which have processed successfully. The program updates the ACTION to "Error" and enters the error message in the COMMENTS field, if the record did not process successfully.
7. The LAPC should access SAMS after each batch run to check the status of requests. If any errors are encountered, refer to *Appendix C: Errors* for an explanation of the error and a solution. For additional help or information on an error message, contact NFC Customer Support at (504) 255-5230.

   Change the ACTION from "Error" to an appropriate action, correct the erroneous information according to the given solution, and remove the error information from the COMMENTS field and press [Save]. The corrected record will get processed the next time the SAMS batch program runs.

   NOTE: The batch program will not reprocess records with an "Error" action. Therefore, records that are in Error have to be corrected in order to reprocess.
8. After a request has processed successfully, the results of the request will be evident to the user. For example, after an Add User request has been successfully processed the user will be able to log on to PCMS with the new user id and password. Or, after a Change Password request has been successfully processed, the user will be able to log on to PCMS with his/her new password.

CARDHOLDER SETUP & SAMS

SAMS and the PCMS Cardholder Setup process are fully integrated. When you use the Cardholder Setup option (CAMS) to add new accounts, a skeleton record is simultaneously created in SAMS. When the account setup information is sent electronically to the bank and the bank sends back an acknowledgment that the account has been established, the account number is inserted into SAMS.

When you receive the card or an acknowledgment from the bank, go into SAMS and complete the skeleton security request that was generated when you created the cardholder setup record.

1. Select **Requests** from the SAMS Main Menu
2. Query up a record by **FIRST** and **LAST NAME** or **SOCIAL SECURITY NUMBER**.
3. Select **Add User** from the Action drop-down menu.
4. Make sure that the account number has been added, if not, enter it.

   If the bank acknowledgement has been received in CAMS, the account number will have been entered into SAMS. If the LAPC receives the cardholder's purchase card before receiving the bank acknowledgement in CAMS, the LAPC can go ahead and enter the account number into SAMS. The cardholder will then have access to PCMS but will not be able to view any transactions until the bank acknowledgement has been received in CAMS.
5. Click in the **USER ID** field and press **[List]** to retrieve a user id, or if the user already has an NFC user id, use that one.
6. Tab over to the **PASSWORD** field and enter a password.
7. Press **[Save]** on the toolbar.
8. When the SAMS batch program runs, it will grant access to PCMS for this cardholder. By the next business day the user can log onto PCMS.

APPENDIX A: PCMS ROLES

The following roles are used in PCMS for the Purchase Card Program and may be granted by entering a request in SAMS:

The **Department Coordinator (DPC)** is located in the Procurement Policy Division and is responsible for the implementation and oversight of the program. The DPC can not be set up in SAMS, they must request access via a request to Security Office at the NFC (refer to *Establishing DPC and APC User Ids* for details).

The **Agency Program Coordinator (APC)** is a person designated in each USDA agency or cross-serviced agency that is responsible for the program within the agency. This person also coordinates the implementation of the program within the agency through the DPC. The very first **APC** for an agency must request access to SAMS via a request to the Security Office at the NFC (refer to *Establishing DPC and APC User Ids* for details). Thereafter the **APC** is responsible for setting up other **APC**s and LAPCs in SAMS. They are also responsible for setting up Cardholders and Finance Managers in SAMS when there is no LAPC.

Role to be assigned in SAMS: **AGENCY_COORDINATOR**

The **Local Agency Program Coordinator (LAPC)** is responsible for the day-to-day operation of the purchase card program within their respective area, location, or office. They work directly with the Cardholder, bank contact person, APC and the NFC. The **LAPC** is responsible for setting up other LAPCs, Cardholders, and Finance Managers in SAMS.

Role to be assigned in SAMS: **LOCAL_PROGRAM_COORDINATOR**

The **Cardholder** is issued a card. No other person is authorized to use the card. The **Cardholder** is responsible for all purchases made with the card. Each Cardholder is responsible for reconciling their account using PCMS.

Role to be assigned in SAMS: **CARDHOLDER**

The **Finance Manager** is responsible for retrieving financial data from PCMS via the Discoverer Ad Hoc Reporting tool.

Role to be assigned in SAMS: **FINANCE_MGR**

APPENDIX B: USER IDS AND PASSWORDS

The following are the requirements for the **User Id**:

If a user already has an NFC user id, use that same id for access to PCMS. And, if the user has multiple roles in PCMS, you must assign a different user id for each role. For example, if a potential user already has an NFC user id and they need a Cardholder and LAPC role, assign the NFC user id as the Cardholder role and assign the same id with an "A" on the end to the LAPC role. If the user does not currently have an NFC user id, then select one from the pool of ids available from the List of Values on the application user id field on the SAMS screen. If the person is also an LAPC, then use the same user id with an "A" appended to the end of it.

The following are the requirements for the **Password**:

- Must be at least six positions long
- Must start with a character
- Must be alphanumeric
- Cannot contain spaces
- Must be different by at least three characters from previous password

APPENDIX C: ERRORS

Below is a list of errors that may appear in the COMMENTS field of the SAMS request screen when a request does not process successfully.

1. ERROR: ORA-28007: the password cannot be reused
   REASON: This user id/password combination has already been used.
   SOLUTION: Change the password to something that has not been used with that user id.
2. ERROR: ORA-0001: unique constraint (OPS$PCMS.SAC_PK) violated
   REASON: The record already exists in the PCMS SECURITY_ACCESS_CONTROL table.
   SOLUTION: Query up the record in SAMS and click the REMOVE button to remove it from SAMS, it's not needed.
3. ERROR: ORA-02291: integrity constraint OPS$PCMS.SAC_PCMS_USER_FK) violated
   REASON: The user is trying to insert into the PCMS SECURITY_ACCESS_CONTROL table and there's no record in PCMS_USER. In other words the user is trying to Insert a SAC and the Add User request was not processed.
   SOLUTION: See if an Add User record exists. If so, find out why it was not processed, and fix it. After looking at the Add User request and you determine you still need the Insert SAC request then simply change the action on the Insert SAC request from Error to Insert SAC. If an Add User record does not exist, then change the Insert SAC action to Add User action.
4. ERROR: ORA-01918: user 'AP8931' does not exist.
   REASON: The user is trying to change a password on a user id that was never created.
   SOLUTION: Remove the request because you cannot change a password on a user id that does not exist.
5. ERROR: ORA-01403: no data found.
   REASON: Generally this error occurs when trying to Modify data. The user is trying to modify data that does not exist. An Add user record is probably out there that was not processed successfully.
   SOLUTION: Press [Remove] to remove the request. If the Add User record is in SAMS and the DATE COMPLETED is null, then make the modifications on that record and press [Save].
6. ERROR: ORA-00988: missing or invalid password(s).
   REASON: The password is missing or invalid.
   SOLUTION: Enter a valid password.

7. ERROR: ORA-0001: unique constraint (OPS$PCMS.SAC_PK) violated

   REASON: If this error occurs on an Insert Sac record, this generally means the record already exists in the PCMS SECURITY_ACCESS_CONTROL table.

   SOLUTION: The record is not needed. Press [Remove] to remove the record.