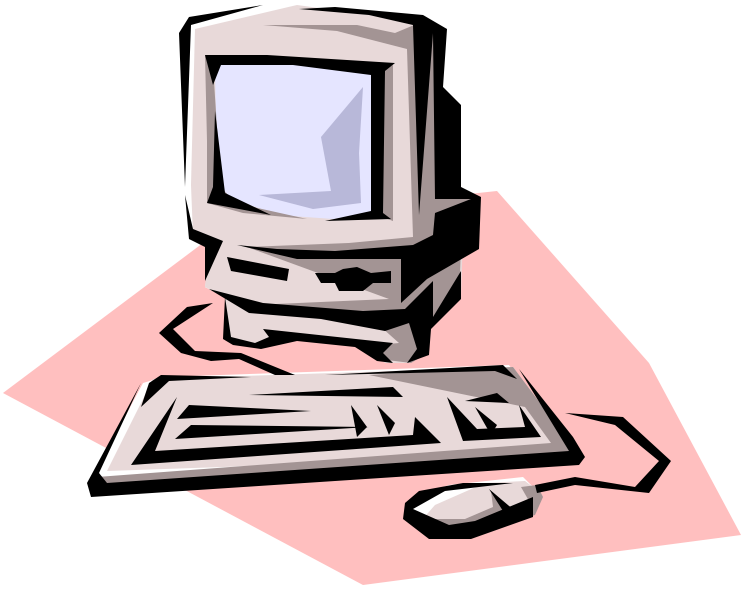
United States Department of Agriculture

SAMS
TRAINING GUIDE
FOR THE FLEET CARD



JUNE 2000

Table Of Contents

Page

INTRODUCTION

LOGGING ON/OFF SAMS

To access SAMS,

1. Double-click on the **SAMSv2 Prod** icon located on your desktop.

   Or

   From 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]**.

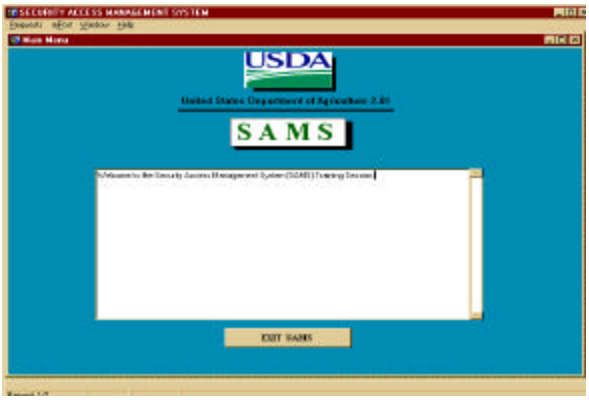
   NOTE: Every 90 days your password expires and must be changed.

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 users access in PCMS. Refer to the *Request* in *Establishing and Updating User Ids* for complete details.

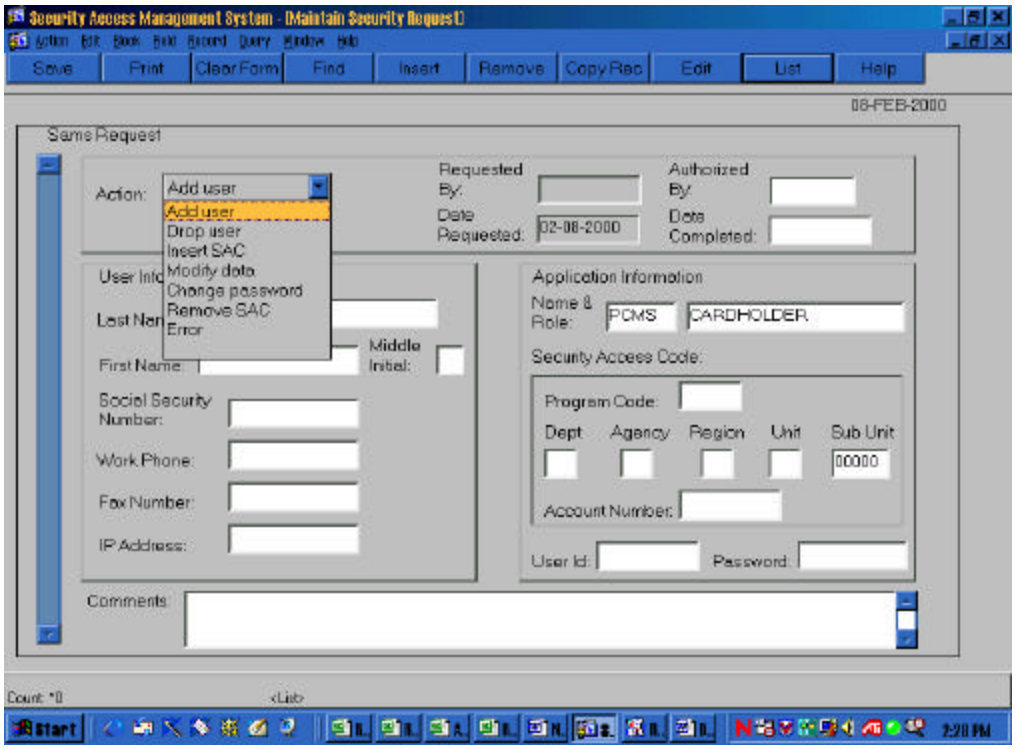
Reports

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.

ESTABLISHING AND UPDATING USER IDS

REQUESTS

Use the Request option to input security requests for access to PCMS and the data query tool (Discoverer). 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

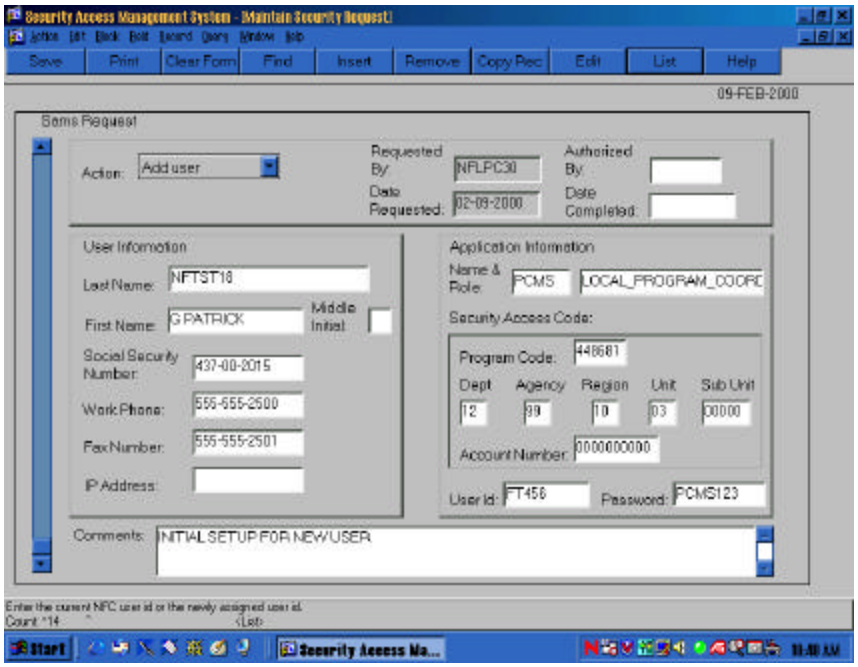
M - Modify data

P - Change Password

V - Remove SAC

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 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 fleet NAME & ROLE is selected (or if you accept the default and tab past these fields), the PROGRAM CODE field is populated with the fleet 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 DFPC 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 LFPC could have a SAC of Department Code 12, Agency Code 11, Region 03, Unit 01, Sub Unit 00000 which would only allow him/her to see his/her records).

An LFPC 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. 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. NOTE: If zeroes are entered in this field, zeroes must be entered in UNIT and SUB UNIT.
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. NOTE: If zeroes are entered in this field, zeroes must be entered in SUB UNIT.
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.
7. A default of **0000000000** will be entered in the **ACCOUNT NUMBER** field. Do not enter anything else in this field.
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 a 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 "F" at the end of it to differentiate it as Fleet. This is mandatory.

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

   NOTE: If you enter a user id that has already been assigned in SAMS or that already belongs to a PCMS user you will get a message indicating that. 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.

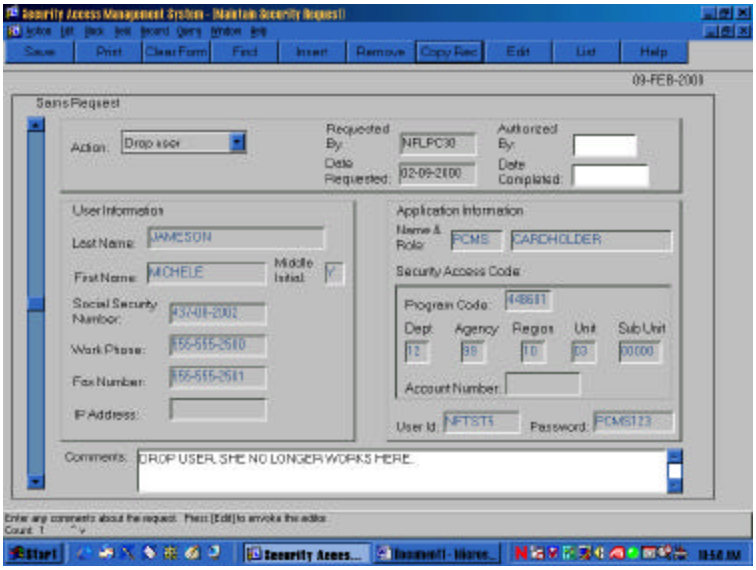
Drop User

Use this option to drop the user's access to PCMS. For AFHC's, ensure that all equipment records have been transferred from the LFPC 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.

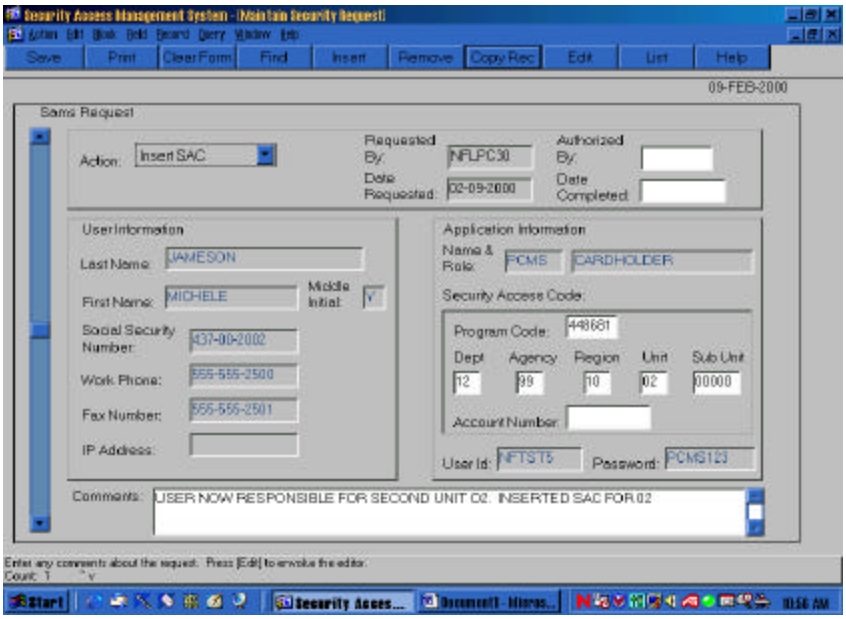
c. Press the **[Find]** button again and the record(s) will be displayed. If more than one record exists for that user the scroll bar on the left of the screen will be highlighted. It doesn't matter which record you choose to copy as long as the DATE COMPLETED field is not blank.

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 LFPC 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**.

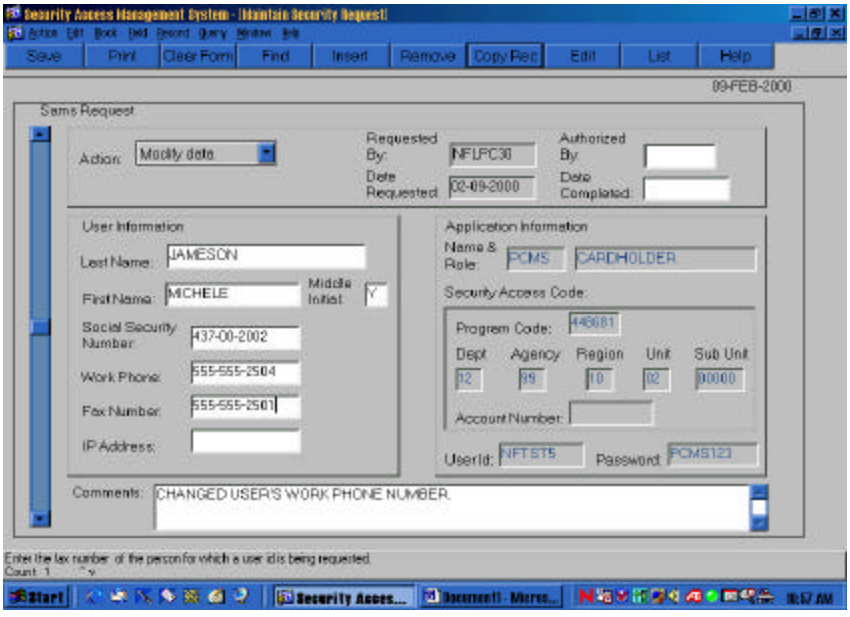
NOTE: You may query on any field on the screen like the Name or Social Security Number, but it is recommend that you use User Id for precise results.

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.). An example of a completed Modify Data request follows:



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.

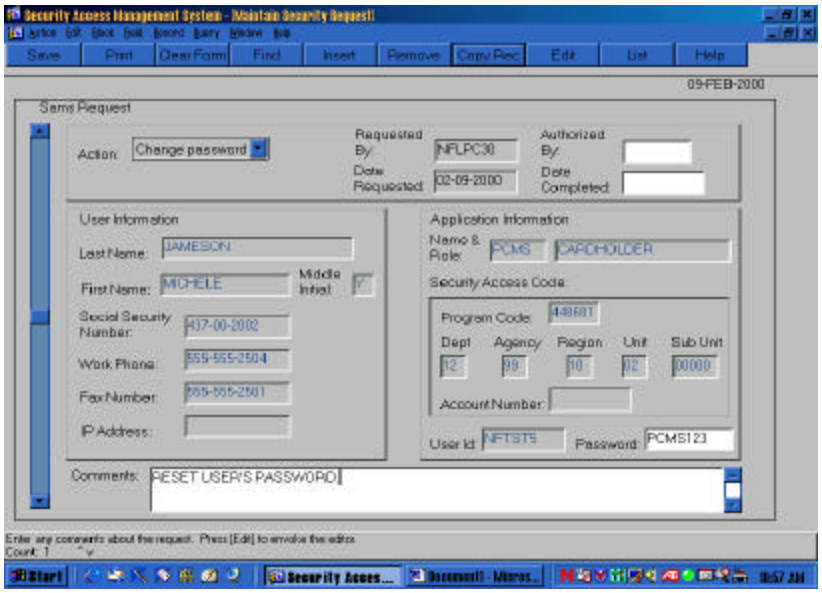
4. Modify data in the User Information region of the screen.

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

6. Press **[Save]**.

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. An example of a completed Change Password request follows:



To change a user's password, do the following:

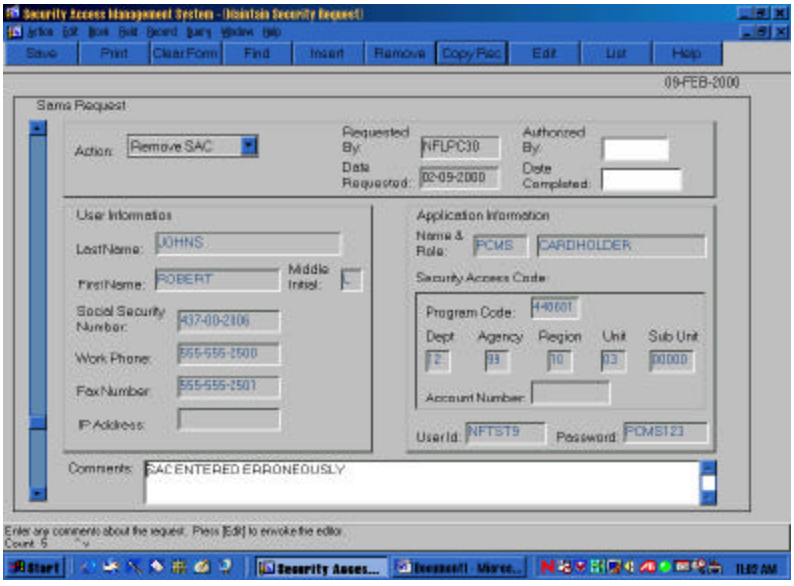
1. Query up a record that was previously processed for the user (e.g., the Add user record).
   a. Press the **[Find]** button on the toolbar and a blank screen will be displayed. The system is waiting for you to indicate what to find.
   b. Enter the user's **user id**.

      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]**.

Remove SAC

Use this option to remove a SAC that may have been entered erroneously or that is no longer needed. An example of a completed Remove SAC request follows:



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 (i.e., 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, i.e., 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.

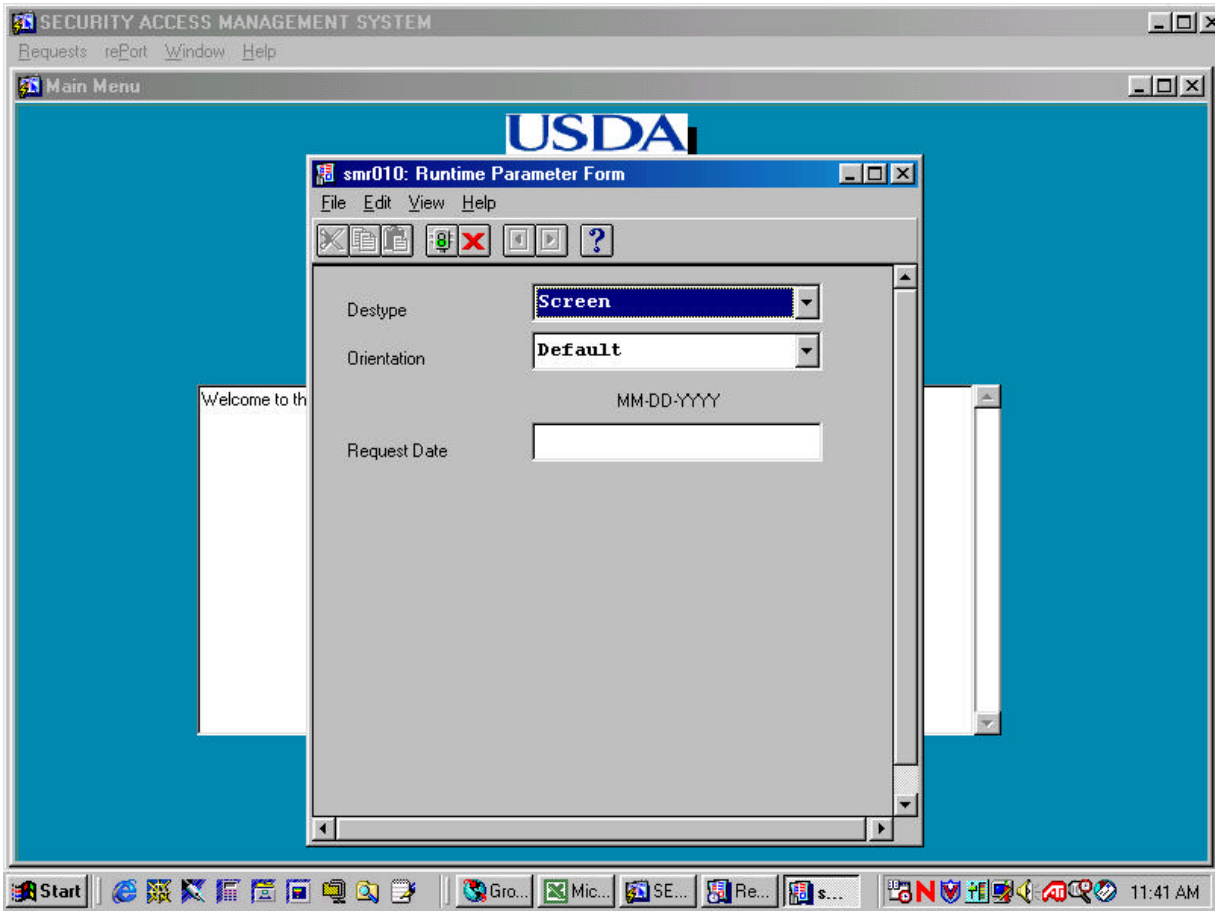
4. Enter data in the **AUTHORIZED BY** field, if applicable. Enter comments regarding the changes made in the **COMMENTS** field.

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 LFPC but that LFPC is attached to equipment records in PCMS, then you will not be able to remove that SAC. All of the equipment must be transferred to another LFPC 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].

REPORTS

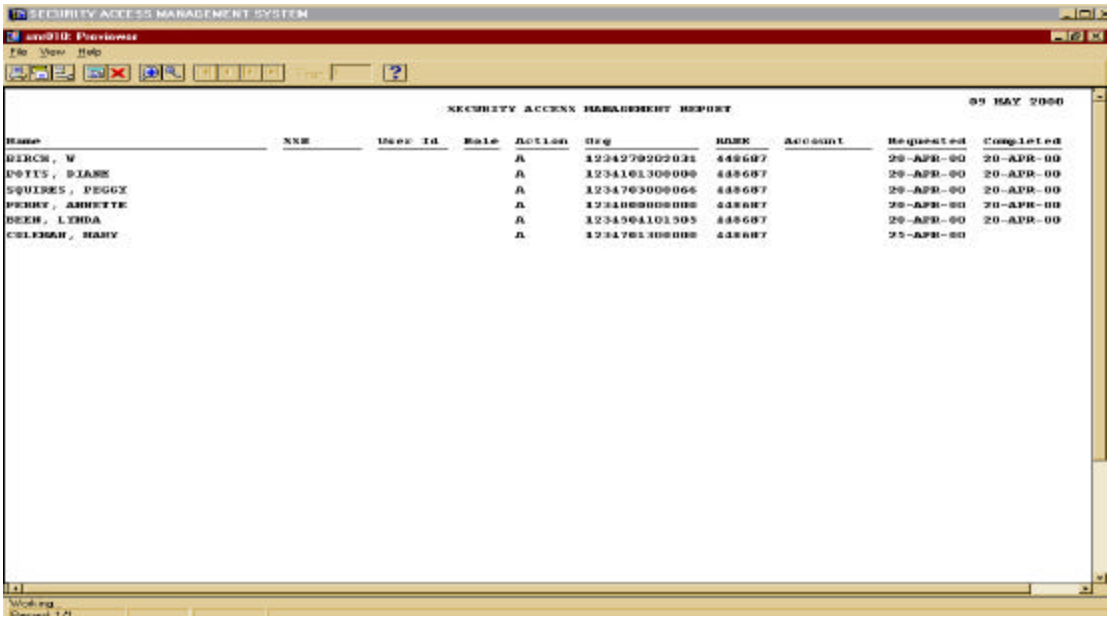
After you select the Reports option, the smr010: Runtime Parameter form window appears.



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 is 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.



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 AFHC contacts the Security Office at NFC for access to SAMS via fax (504-255-4131) or e-mail (nfc.securityofc@usda.gov).
2. The AFHC will receive a user id and password to access SAMS.
3. The AFHC will utilize on-line SAMS to establish AFPCs, LFPCs, and LFMs.
4. The SAMS batch program that runs at 12:00 noon CST and 8:00pm CST will process each request.
5. 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.
6. The AFHC 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.
7. 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.

APPENDIX A: PCMS ROLES

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

- The **Agency Fleet Headquarters Coordinator (AFHC)** is the person designated, in each USDA agency operating fleet equipment, who is responsible for the program within each agency. This person will also coordinate the implementation of the program within the agency through the DFPC. The **AFHC** will coordinate and assign responsibilities of the AFPC. All documentation needed to establish security access for PCMS related to the establishment of office, location, or area will be processed through the **AFHC**. The **AFHC** has access and update capability to all records within their agency and use of the Discoverer Ad Hoc Reporting Tool. The **AFHC** will use SAMS to set up AFPCs and/or LFPCs.

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

- The **Agency Fleet Program Coordinator (AFPC)** is responsible for monitoring the fleet management program under their specific organizational level. The **AFPC** assigns an individual to be the LFPC and to receive alerts from PCMS.

  Role to be assigned in SAMS: **FLEET_PROGRAM_COORDINATOR ONLY**

- The **Local Fleet Program Coordinator (LFPC)** is responsible for ordering, maintaining, deleting fleet credit cards and filing any billing disputes. The **LFPC** will also be responsible for receiving and distributing all fleet credit cards from the vendor. The **LFPC** will be responsible for assuring that all lost or stolen fleet credit cards are reported immediately to the vendor and deleted from PCMS to stop all charges and agency liability. The **LFPC** will use also receive system alerts for action when necessary and will have access to the Discoverer Ad Hoc Reporting Tool to access all data within their responsibility.

  Role to be assigned in SAMS: **FLEET_PROGRAM_COORDINATOR ONLY**

- The **Local Fleet Manager/Fleet Finance Manager (LFM)** is responsible for retrieving all fleet management and financial management credit card data from PCMS via the Discoverer Ad Hoc Reporting Tool.

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

APPENDIX B: USER IDS AND PASSWORDS

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

- If the user already has a PCMS user id, enter the PCMS user id with an "F" on the end of it to differentiate it as Fleet. This is mandatory.
- The AFHC will contact NFC in order to populate the drop-down listing of user ids in SAMS. For example: When an AFHC needs additional user ids, he/she will send an e-mail to NFC requesting user ids for the specific number of new users. NFC will populate the user id drop-down list with the specified number of user ids requested.

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.