



Lesson 8: *SAMS*

Lesson Description

In Lesson 8 the APC and LAPC will learn to provide and maintain security access to PCMS. This is the final lesson in the APC\LAPC PCMS training course.

Training Objectives

At the conclusion of this lesson, APC's and LAPC's will be able to:

1. Add or Drop Users
2. Insert or Remove Security Access Code (SAC) information
3. Modify Data
4. Change Passwords

Methodology

This lesson will be delivered using a combination of lecture and presentation, and discussion. Group discussion and trainee interaction will be used to stimulate recall of policy information and establish a knowledge base on which to build in subsequent lessons.

References

- (1) SAMS User's Guide for the Purchase Card, OPP&EP\PMT, Rev. September 2000
- (2) APC/LAPC PCMS Quick Guide for Managing Purchase Cardholder Accounts, OPP&EP\PMT, December 2000
- (3) APC/LAPC PCMS User's Guide, OPP&EP\PMT, September 2005

Enclosures

None.

I. SAMS Overview



Please turn off your monitor and give your attention to the instructor.

a. What is SAMS?

The Security Access Management System (SAMS) is a Web-based application used to establish user access to the Purchase Card Management System (PCMS) at the National Finance Center (NFC). SAMS provides a graphical user interface for entering security access requests online.

b. Workflow

When a new record is created in CAMS, a skeletal record for the Cardholder is concurrently established in SAMS. Once the bank establishes a Cardholder's account, SAMS is updated with the Cardholder's account number. The LAPC can then enter SAMS, complete the record, and establish PCMS access for the Cardholder.

c. Software Installation

SAMS Web is a web-based application and does not require any software installation.

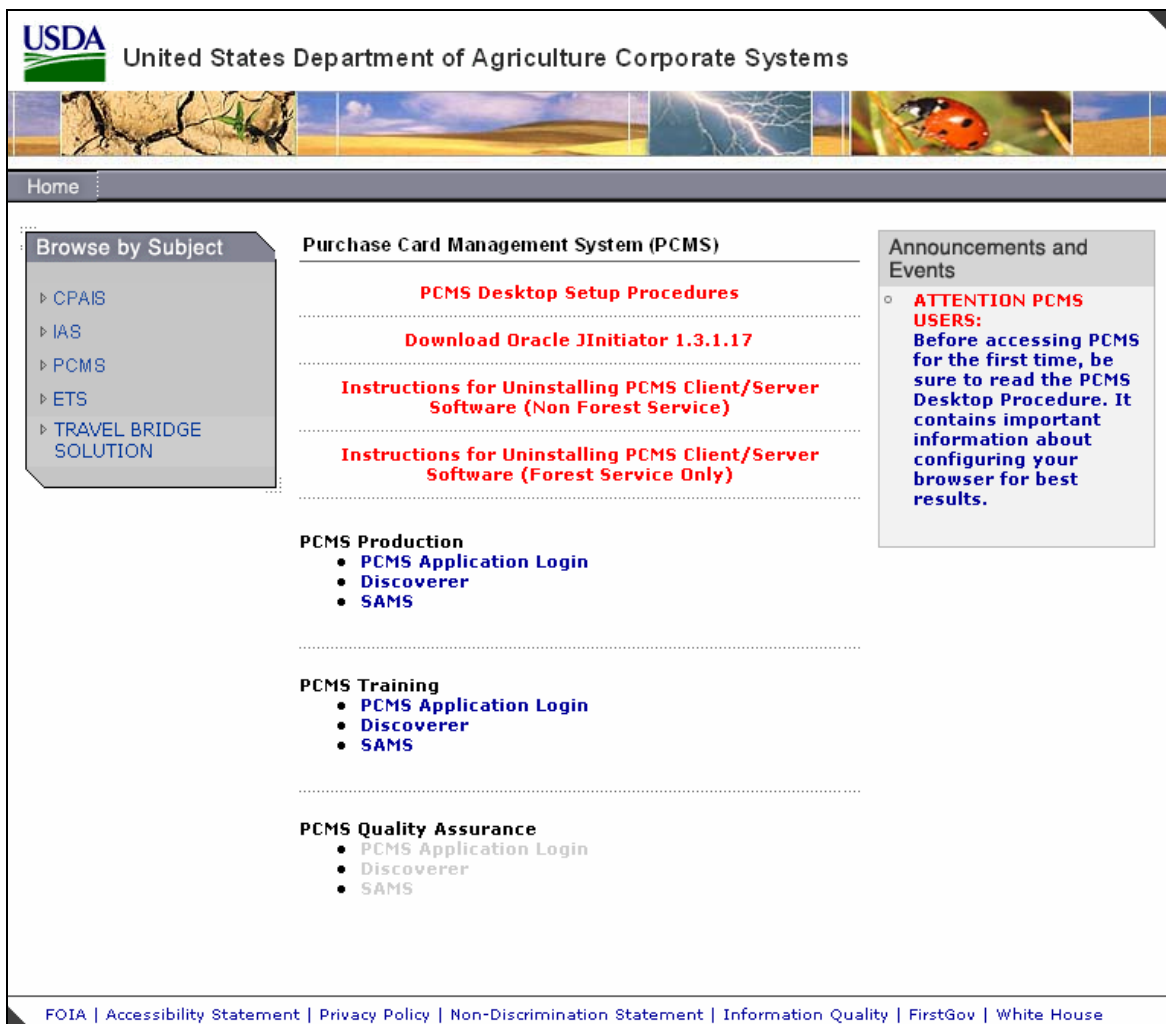
Notes:

II. Logging On to SAMS



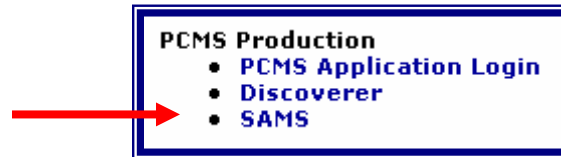
Please turn off your monitor and give your attention to the instructor.

To Log in to the PCMS Web application, access the USDA PCMS web page at <http://www.nfc.usda.gov/corporate/PCMS.htm>



The screenshot shows the USDA PCMS web page. At the top, the USDA logo and the text "United States Department of Agriculture Corporate Systems" are visible. Below this is a navigation bar with "Home" and a "Browse by Subject" menu. The menu includes links for CPAIS, IAS, PCMS, ETS, and TRAVEL BRIDGE SOLUTION. The main content area is titled "Purchase Card Management System (PCMS)" and contains several sections: "PCMS Desktop Setup Procedures" with links for "Download Oracle JInitiator 1.3.1.17", "Instructions for Uninstalling PCMS Client/Server Software (Non Forest Service)", and "Instructions for Uninstalling PCMS Client/Server Software (Forest Service Only)"; "PCMS Production" with links for "PCMS Application Login", "Discoverer", and "SAMS"; "PCMS Training" with links for "PCMS Application Login", "Discoverer", and "SAMS"; and "PCMS Quality Assurance" with links for "PCMS Application Login", "Discoverer", and "SAMS". On the right side, there is an "Announcements and Events" section with a red heading "ATTENTION PCMS USERS: Before accessing PCMS for the first time, be sure to read the PCMS Desktop Procedure. It contains important information about configuring your browser for best results." At the bottom of the page, there is a footer with links for FOIA, Accessibility Statement, Privacy Policy, Non-Discrimination Statement, Information Quality, FirstGov, and White House.

1. Click the active **SAMS** link under the **PCMS Production** heading.



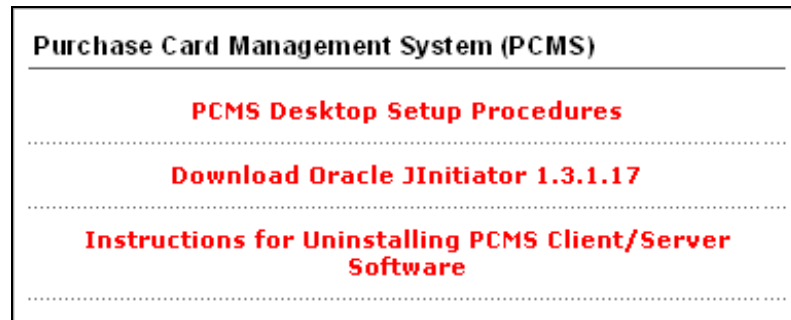
An Oracle Forms Runtime window will open in another browser.



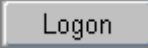
You may need to update your version of Oracle JInitiator to access the PCMS Web application. If a message displays asking to download JInitiator, click Yes.

Or

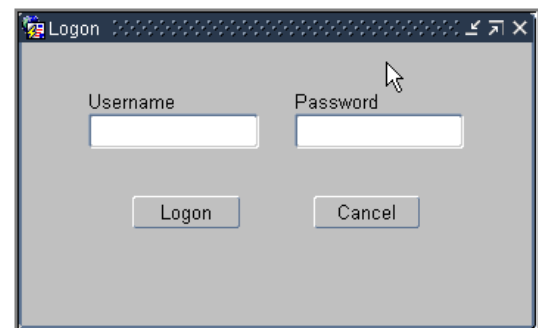
If the page does not load when you click on the **SAMS** link, use the back button to return to the USDA PCMS web page and click the link to Download Oracle JInitiator 1.3.1.17.



2. When the Logon dialog box opens, enter your

Username and password and click .

The Main Window will then open.



III. Main Menu



Please turn off your monitor and give your attention to the instructor.

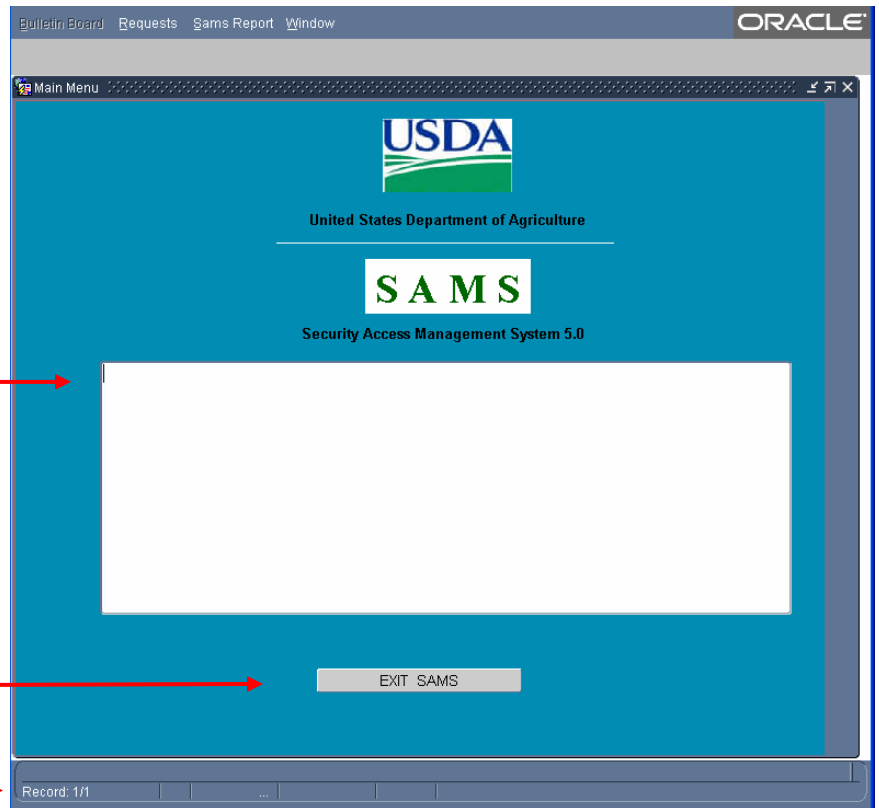
a. Main Window & Bulletin Board

Main Menu. Provides access to main functions in SAMS.

Bulletin Board. Displays news and messages about SAMS.

Exit Button. Closes application

Status Bar. Displays messages about the status of the current window.



This is the main window in SAMS. The bulletin board located in the center of the window provides up-to-date news about SAMS.



The Bulletin Board function is only available to the DPC and system administrators. The Departmental Program Administrator (DPC) and System Administrators will utilize the *Bulletin Board* to provide current system-related information to SAMS users.

b. Main Menu

The main menu provides access to the major functions of SAMS.

Bulletin Board Requests Sams Report Window ORACLE	
Bulletin Board	The Departmental Program Administrator and System Administrators will utilize the Bulletin Board to provide current system-related information to SAMS users.
Requests	Use to add new users or modify or drop existing users to PCMS.
Sams Report	Generate a report of PCMS users with a specific date search.
Window	Move between open windows in SAMS.

Notes:

IV. Establishing Usernames



Please turn off your monitor and give your attention to the instructor.

The information entered into SAMS is used to create a *Username* or *User Id*, role(s), security profile, and *Security Access Code* (SAC) information. The role (e.g. APC, LAPC, Cardholder, etc.) defines the PCMS options to which a user has access. The SAC, which defines the amount of information a user can see, may consist of any of the following: *Department Code*, *Agency Code*, *Region*, *Unit*, and *Sub Unit*.



If a PCMS user has a valid NFC System ID, he/she must provide existing User ID to be used in establishing any roles within PCMS.

DPC's use SAMS to request access to PCMS for Area Program Coordinators (APCs). APCs use SAMS to request access to PCMS for Local Agency Program Coordinators (LAPCs). LAPCs use SAMS to request access to PCMS for other LAPCs, Cardholders, and Financial Managers (FM). The process used by APCs and LAPCs to enter requests for access in SAMS will be discussed in greater detail in the subsequent section.

a. Requests

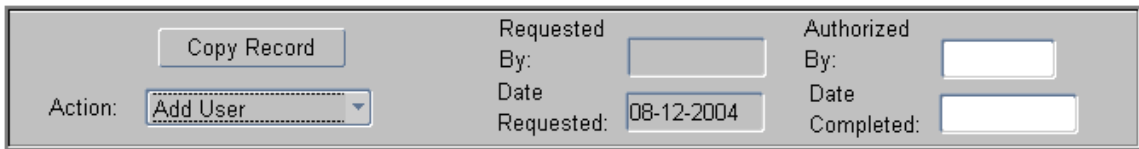
To access the Maintain Security Request window, request click **Requests** on the main menu.

Enter details to initiate an access request.

b. Add a User


ACTION REQUEST

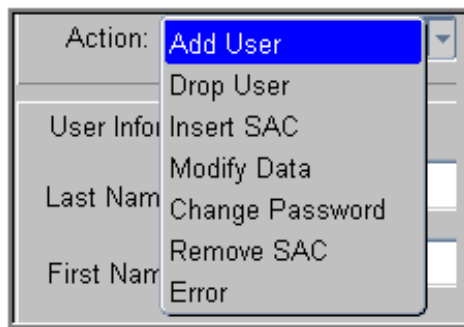
The first area of the window is the Action block. This contains information about the action requested.



The screenshot shows a form with the following fields and values:

- Action:** A dropdown menu with "Add User" selected.
- Copy Record:** A button.
- Requested By:** An empty text box.
- Date Requested:** A text box containing "08-12-2004".
- Authorized By:** An empty text box.
- Date Completed:** An empty text box.

The first entry field in this section is **Action**. *Add user* is the default action. Click  to open the drop-down list and review other options.



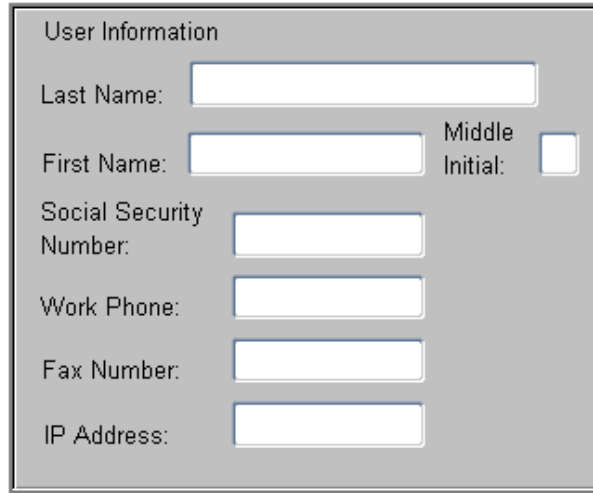
The screenshot shows the dropdown menu for the Action field, with the following options listed:

- Add User (highlighted in blue)
- Drop User
- Insert SAC
- Modify Data
- Change Password
- Remove SAC
- Error

Requested By and **Date Requested** are automatically populated. **Authorized By** is an optional field where you may record the User Id of the authorizing individual. **Date Completed** will be entered automatically once the request is processed and accepted as part of a batch process.

USER INFORMATION

This block of the window is used to enter identifying and contact information on the subject of the request.



The screenshot shows a window titled "User Information" with the following fields:

- Last Name: [Text Input]
- First Name: [Text Input]
- Middle Initial: [Text Input]
- Social Security Number: [Text Input]
- Work Phone: [Text Input]
- Fax Number: [Text Input]
- IP Address: [Text Input]

The following provides a brief description of the fields in the User Information block.

Fieldname	Required	Description
Last Name	Yes	The User's last name.
First Name	Yes	The User's first name.
Middle Initial	No	The User's middle initial.
Social Security Number	Yes	The User's 9-digit Social Security Number with no dashes or breaks. This is verified against Payroll information
Work Phone	Yes	The User's 10-digit work phone number with no parentheses, dashes or breaks.
Fax Number	Yes	The User's 10-digit fax number with no parentheses, dashes or breaks.
IP Address	No	The User's Internet Protocol (IP) address (e.g. 199.145.120.67)

APPLICATION INFORMATION

The *Application Information* block allows the APC/LAPC to establish or change a PCMS user's **Name & Role, Security Access Code, User Id** and/or **Password**.

Application Information

Name & Role:

Security Access Code:

Program Code:

Dept	Agency	Region	Unit	Sub Unit
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text" value="00000"/>

Account Number:

User Id: Password:

i) Name & Role

The system displays the default name & role “PCMS / CARDHOLDER.” A *List of Values* is available for these fields.

Place your cursor in the **Name** field, where “PCMS” displays and click .

The Application and Roles selection box opens.

Applications and Roles

Find:

Name & Role	Role
PCMS	AGENCY_COORDINATOR
PCMS	CARDHOLDER
PCMS	FINANCE_MGR_ROLE
PCMS	LOCAL_PROGRAM_COORDINATOR
PCMS	FLEET_PROGRAM_COORDINATOR
PCMS	FLEET_PROGRAM_COORDINATOR ONLY
PCMS	FLEET_PBT_ROLE

Find OK Cancel

Scroll to select the correct Name & Role and click .



Apply the following rules when assigning user names:

- SAMS can only establish one (1) role per transaction. For more information on *Roles*, see Appendix A of Reference (2), *SAMS User’s Guide for the Fleet Card*.
- Assign LAPCs role as LOCAL_PROGRAM_COORDINATOR

ii) Security Access Code

APCs and LAPCs should only have access to those areas necessary for them to carry out their responsibilities. This access is governed by limiting PCMS users by appropriate **Department, Agency, Region, Unit, Sub Unit** and/or **Account Number**.

The screenshot shows a 'Security Access Code' form with the following fields:

- Program Code: [Empty text box]
- Dept: [Empty text box]
- Agency: [Empty text box]
- Region: [Empty text box]
- Unit: [Empty text box]
- Sub Unit: [Text box containing '00000']
- Account Number: [Empty text box]

The following provides a brief description of the fields in the SAC area of the Application Information block:

Fieldname	Required	Description
Program Code	Yes	A six-digit code automatically populated when <i>Name & Role</i> is selected.
Dept	Yes	A two-digit code that indicates the user’s department. USDA’s Dept code is 12 .
Agency	Yes	The two-digit Agency code.
Region	Yes	The two-digit Region code. If no Region is to be specified, enter 00 .
Unit	Yes	The two-digit Unit code. If no Unit is to be specified, enter 00 .

Fieldname	Required	Description
Sub Unit	Yes	The five-digit Sub Unit code. Use leading zeros if Sub Unit code is less than five-digits. If no Sub Unit is to be specified, enter 00000 .
Account Number	Yes	A default Account Number of 0000000000 will automatically be entered. Do not enter any other value in this field.

iii) User ID & Password

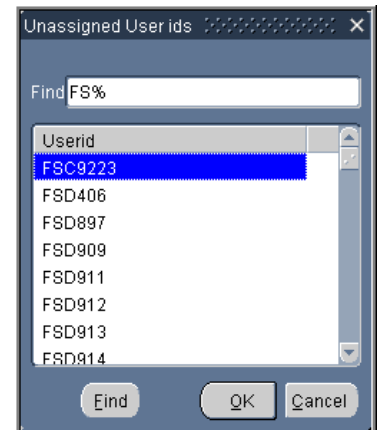
The combination of User ID and Password identify a unique system user and the functions the user can access. You can use the SAMS Security Request window to create a new user or assign a new role to an existing user.

A screenshot of a form with two input fields. The first field is labeled 'User Id:' and the second is labeled 'Password:'. Both fields are empty.

New User

Follow these steps to create a user id for a new user who does not have a PCMS user id.

- Place your cursor in the User ID field and click .
The Unassigned User Id list opens.
- Scroll to the desired User id and click .
The system enters the user id in the field.
- Tab or place your cursor in the Password field and enter a value.



Use the following rules when assigning passwords:



- A password must be at least 6 alphanumeric characters in length
- Must start with a letter.
- Must include at least one number.
- Cannot contain spaces.
- Must differ by at least 3 character from previous password.

New Role for Existing User

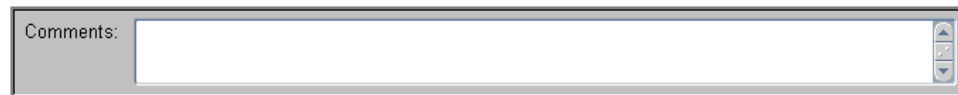
Follow these steps to assign a new role for a user who already has a PCMS user id.

1. Place your cursor in the User ID
2. Enter the user's existing PCSM user id with an *F* appended to the end (e.g. FS123F)
3. Tab or place your cursor in the Password field and enter a value.

Fieldname	Required	Description
User Id	Yes	An identification code that uniquely identifies the user in the PCMS system.
Password	Yes	A string of 6 - 8 characters used to verify that the user is authorized to access the system.

iv) Comments

The final section of the Security Request window is the Comments block at the bottom of the window.





Use this area to enter any comments that may be useful in establishing a clear record.

c. Drop User

Before you can terminate (or drop) access for an LAPC, you must ensure all equipment records are transferred to another LAPC.

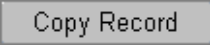
Follow these steps to drop a user

1. Click  on the command bar.
The record clears and you enter query mode.


2. Enter identifying information (such as user id, social security number, last name, etc.) for the user to delete and click  .

The user record displays.

3. Verify that the correct record displays.



4. Click  in the action block.

The Copied Record message displays.

5. Click  to create a copy of the retrieved record.





Note that the copied record now displayed is identical to the record retrieved, with two (2) exceptions: **Action** and **Date Completed** are now blank.

6. Click  on the **Action** dropdown box and select **Drop User**.
7. Enter values in **Authorized By** and/or **Comments** (this is optional for both fields) and click  .

d. Insert SAC




The **Insert SAC** action is used to provide the user with an additional SAC. This type of action may be utilized when, for example, an LAPC is assigned the oversight responsibility for an additional **Unit** or **Sub Unit**.

Follow these steps to insert SAC for an existing user.

1. Click  on the command bar.
The record clears and you enter query mode.
2. Enter identifying information (such as user id, social security number, last name, etc.) for the user to delete and click .
The user record displays.
3. Verify that the correct record displays.

4. Click  in the action block.

The Copied Record message displays.



5. Click  to create a copy of the retrieved record.
6. Click  on the **Action** dropdown box and select **Insert SAC**.
7. Enter the additional SAC.
8. Enter any values in **Authorized By** and/or **Comments** (this is optional for both fields) and click .



e. Remove SAC

The *Remove SAC* action is used to remove an SAC that is no longer required, or one that may have been erroneously assigned. This action will not affect other, existing SACs. Prior to undertaking a *Remove SAC* action, ensure all records related to this User and SAC are attached to another User.


Follow these steps to insert SAC for an existing user.

1. Click  on the command bar.
The record clears and you enter query mode.
2. Enter identifying information (such as user id, social security number, last name, etc.) for the user to delete and click .






For the best result, enter the user id and SAC information (e.g. Unit or Sub Unit) to be removed.

The user record displays.

3. Verify that the correct record displays.
4. Click  in the action block.



The Copied Record message displays.

5. Click  to create a copy of the retrieved record.
6. Click  on the **Action** dropdown box and select **Remove SAC**.
7. Enter any values in **Authorized By** and/or **Comments** (this is optional for both fields) and click .

f. Modify Data

The *Modify data* operation is used to modify *User Information* displayed on the *Sams Request* page, such as *Last Name, First Name, Social Security Number, or Work Phone*.


Follow these steps to modify data for an existing user.

1. Click  on the command bar.
The record clears and you enter query mode.
2. Enter identifying information (such as user id, social security number, last name, etc.) for the user to delete and click  .






For the best result, enter the user id.

The user record displays.

3. Verify that the correct, most current record copy of the record displays and that **Date Completed** is populated.
4. Click  in the action block.

The Copied Record message displays.

5. Click  to create a copy of the retrieved record.
6. Click  on the **Action** dropdown box and select **Modify Data**.
7. Make the desired updates.
8. Enter any values in **Authorized By** and/or **Comments** (this is optional for both fields) and click  .

g. Change Password

Periodically, Users will need assistance in changing their passwords. The *Change password* option in the *Action* field of the *Sams Request* page provides the ability to accomplish this necessary administrative task.

The screenshot shows a web application window titled "Maintain Security Request". Inside, there is a "Sams Request" form. At the top, there is a "Copy Record" button and an "Action" dropdown menu currently set to "Add User". To the right, there are fields for "Requested By" (FS2783S), "Date Requested" (02-26-1998), "Authorized By" (XXXXXXXX), and "Date Completed" (03-03-1998). Below this, the form is divided into two main sections: "User Information" and "Application Information".

User Information:



- Last Name: SMITH
- First Name: EDWARD
- Middle Initial:
- Social Security Number: 777-77-7777
- Work Phone: 555-555-5555
- Fax Number: 777-777-7777
- IP Address:

Application Information:

- Name & Role: PCMS LOCAL_PROGRAM_COORD
- Security Access Code:
 - Program Code: 471640
 - Dept: 12, Agency: 11, Region: 13, Unit: 01, Sub Unit: 00000
 - Account Number: 0020011820
- User Id: FS12345
- Password: *****

At the bottom of the form is a "Comments:" text area.

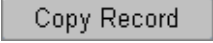
Follow these steps to modify data for an existing user.



1. Click  on the command bar.
The record clears and you enter query mode.
2. Enter identifying information (such as user id, social security number, last name, etc.) for the user to delete and click .



For the best result, enter the user id.

The user record displays.

3. Verify that the correct, most current record copy of the record displays and that **Date Completed** is populated.
4. Click  in the action block.
The Copied Record message displays.

5. Click  to create a copy of the retrieved record.
6. Click  on the Action dropdown box and select **Change Password**.
7. Make the desired updates.



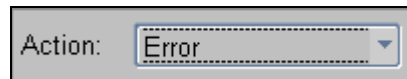
Use the following rules when assigning new passwords:

- A password must be at least 6 alphanumeric characters in length
- Must start with a letter.
- Must include at least one number.
- Cannot contain spaces.
- Must differ by at least 3 characters from previous password.

8. Enter any values in **Authorized By** and/or **Comments** (this is optional for both fields) and click .

h. Correct Error

In order to perform most of the operations listed in the **Action** field, it is necessary to first locate the most recent PCMS User record and then copy that record to perform an operation. When searching for most current PCMS User record for an action, if “*Error*” appears in the **Action** field, you may **NOT** proceed with a new operation until the *Error* is corrected.



The cause of the error is identified in **Comments** at the bottom of the window.

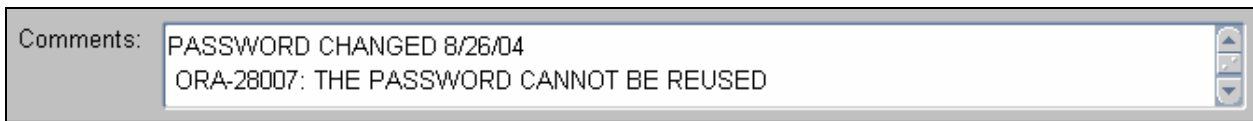


Figure 8-33

Correct the error by making a copy of the page, and then correcting the data entry that caused the error. Once the corrected transaction is complete and processed, the “*Error*” in the **Action** field will change to reflect the appropriate operation, e.g. “*Change password*” and the system will populate the **Date Completed** field.

v. Reports

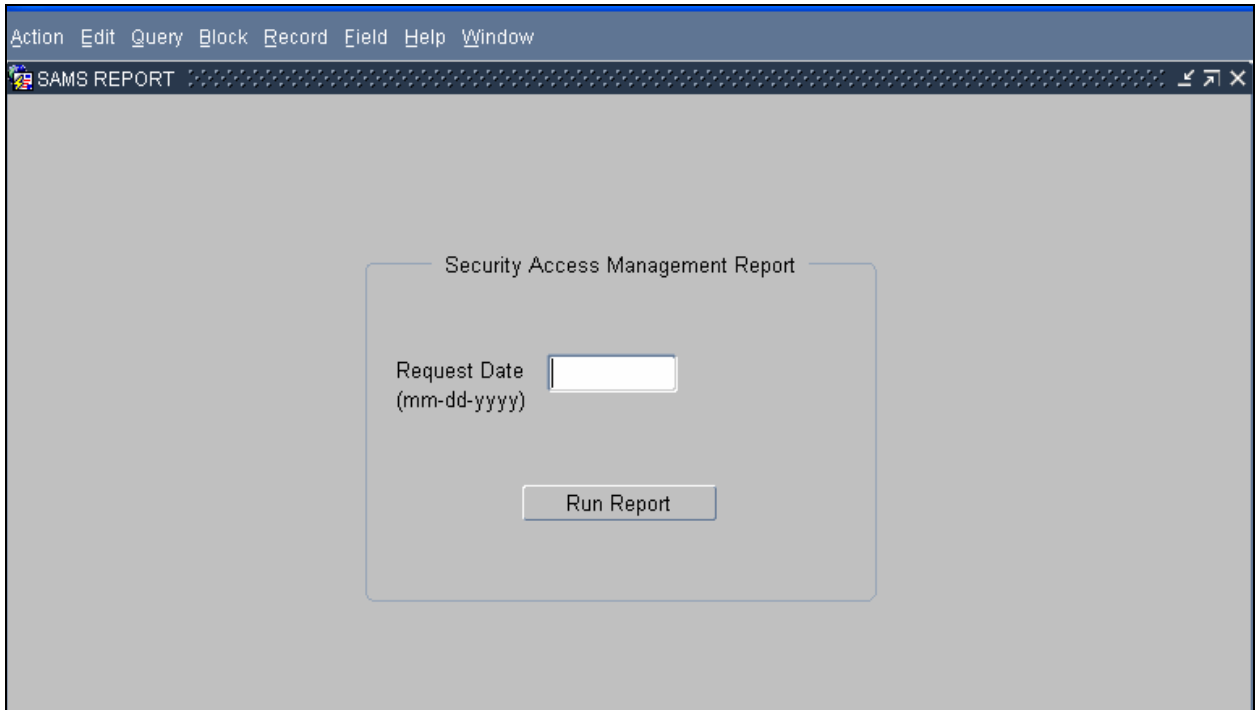


Please turn off your monitor and give your attention to the instructor.

To access SAMS' Report module click on  on the main menu bar.



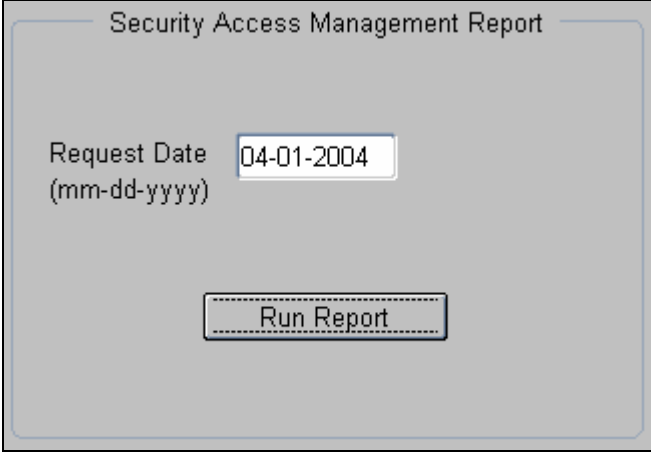
The SAMs Report window will appear.



SAMs Report Sub-menu:

Fieldname	Description
Action	Perform actions such as save, clear, print and exit.
Edit	Edit field values.
Query	Execute a query.
Block	Navigate between blocks of information. (Not used on this window)
Record	Navigate between records. (Not used on this window)
Field	Navigate between fields.
Help	View a hotkeys menu.
Window	Move between open windows in SAMS.

To generate a report enter a **Request Date** and click .



The screenshot shows a window titled "Security Access Management Report". Inside the window, there is a label "Request Date (mm-dd-yyyy)" followed by a text input field containing "04-01-2004". Below the input field is a button labeled "Run Report".

When your report is completed, your results should appear in a separate window. Use the scroll bar to navigate between pages. The report can be saved to your desktop or printed, using the **File** menu. The *SSN*, *User ID* and *Account* columns have been truncated for security.

Notes:

A description of each of the columns in the SAMS Report is shown in Table 8-D below:

Fieldname	Description
Name	The assigned username (e.g., da014).
SSN	The Social Security Number of the user.
User Id	The User's system identification.
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 ten (10) digits of the Cardholder's purchase card account number.
Requested	Date action requested.
Completed	Date request batch-processed and completed.



PRACTICAL EXERCISE

1. Logon to SAMS using your *Username* and *Password*. Note any messages on the *Main Menu Bulletin Board*.
2. Open the SAMS *Requests* module. Search for and locate the record of an individual under your cognizance, using *Last Name* (at a minimum) as the search criteria.
3. Open the SAMS *rePorts* module. Generate a report using a *Request Date* of the last day of the previous month.
4. Return to the *Main Menu*, and exit SAMS.

VI. Summary and Review



Please turn off your monitor and give your attention to the instructor.

1. What are the main functions the LAPC performs using SAMS?
2. What are the steps for an LAPC when setting up a new Cardholder account? (Walk the instructor through the steps)
3. What would prevent a new Cardholder record from being modified in SAMS?
4. How would an LAPC deactivate a Cardholder's Purchase Card?
5. If a Cardholder loses his/her *Password*, how would the LAPC provide a new one?