Establishing User Ids

SAMS is used to create and manage system user ids through the user's role, security profile (e.g., name, SSN), and Security Access Code (SAC) information. The role (e.g., Local Agency Program Coordinators (LAPC), Cardholder) defines the Purchase Card Management System (PCMS) options to which a user has access. The SAC is made up of the Department Code, Agency Code, Region, Unit, and Subunit. It defines the amount of information a user can see.

The Agency Program Coordinator (APC) will use SAMS to request access to PCMS for their 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. See No. 3 under *SAMS Process Flow*.

SAMS Process Flow

1. The APC will utilize SAMS to establish LAPCs.
2. The LAPC will establish Cardholder's, additional LAPCs, and FMs.
3. The SAMS batch program that runs at 1:00pm CST and 8:00pm CST will process each request.
4. 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. Refer to the *SAMS User's Guide for the Purchase Card* for complete details on error messages.

    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.
5. After a request has processed successfully, the results of the request will be evident to the user (e.g., 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).

Security Access Maintenance

When updating records in SAMS (D, I, M, P, V), proceed with the following steps:

1. Find the user record;
2. Click on [Copy Rec];
3. Select an ACTION and proceed to update record.

Refer to the *SAMS User's Guide for the Purchase Card* for complete details for adding LAPCs and in managing a user's security access in SAMS. SAMS and PCMS user guides can be viewed and downloaded at:
http://www.usda.gov/procure/pcard/pcguide.htm

Departing Cardholders

1. If the Cardholder voluntarily leaves the agency or USDA, excluding death, the LAPC will ensure that the Cardholder reconciles all transactions before leaving. All transactions must be reconciled before removing a Cardholder's system access; otherwise, a message will appear and the system will not allow the action. If the Cardholder died or was dismissed, skip to step 2.
2. Drop user access to PCMS when the Cardholder has either left the agency or USDA.
3. If transactions appear after dropping the Cardholder's user id, add the departing Cardholder back into SAMS through the Add user Action. The APC/LAPC should use their SSN and the Cardholder's original user id with an alpha character added at the end when re-establishing this access. Add note in Comments field explaining why this id was created.
4. Reconcile the remaining transactions. If after 30 days no additional transactions appear, Drop User access for this id.

Action Codes

NOTE for Actions D, I, M, P, and V: Unlike CAMS, all records created in SAMS are separate records that can be viewed to troubleshoot access problems. It is advisable to always use the last record to copy when creating a new record (e.g., Change Password, Insert SAC).

Add User (A) – Request access to PCMS.

Drop User (D) – Drop 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, 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 a user id is mistakenly dropped, either call NFC to re-establish it or add a new user id.

Insert SAC (I) – Insert an additional SAC for a user. For example, use this option when an LAPC is responsible for 2 of the 10 units in a region. When the LAPC was originally set up, it was with a SAC of Dept 12, Agency 11, Region 03, Unit 01 and now the LAPC is also responsible for unit 02. Insert another SAC for Department Code 12, Agency 11, Region 03, Unit 02.

Modify Data (M) – Modify the user profile information (name, social security number, etc.).

Change Password (P) – This action code is used to reset a user's password (i.e., receive a call from a user saying they have forgotten their password or that it has expired.)

Remove SAC (V) – Remove a SAC that may have been entered erroneously or that is no longer needed.

Error – Batch processing detected an error in the record. Details of the error are entered in the COMMENTS field. Correct the error and press [Save] to reprocess the record. Details for resolving errors are in the *SAMS User's Guide for the Purchase Card*.

Purchase Card
QUICK GUIDE
to using the
Security Access Management System (SAMS)
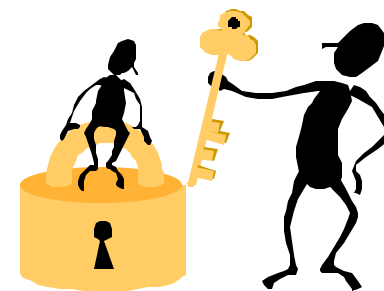
Originated: May 2001

Prepared by:
Office of Procurement and Property Management
Procurement Systems Division

Cardholder Setup and SAMS

SAMS and the PCMS Cardholder Setup process are fully integrated. When new Cardholder records are saved in PCMS using the Cardholder Setup option (CAMS), a skeleton record is simultaneously created in SAMS. Batch processing sends the record to the Bank. After the Bank sends back an acknowledgment that the account has been established, the account number is inserted into CAMS and then fed to the SAMS record. The LAPC then completes the skeletal SAMS record, giving the Cardholder access to PCMS.

Completing SAMS Records for New Cardholders

When an acknowledgment from the Bank is received (i.e., DATE RETURNED FROM BANK and ACCOUNT NUMBER are entered in the Cardholder's record in CAMS):

1. In SAMS, click on **REQUEST** to open the *Maintain Security Request* screen (refer to screen below);

2. Query the Cardholder record;

3. Select ACTION **Add user**. (Do not click on [Copy Rec] first, see *Security Access Maintenance*.)

    NOTE: When errors occur in batch processing, *Error* will appear in this field. Refer to the COMMENTS field for an explanation of the error.

    NOTE: Refer to the back panel of this tri-fold for complete description of all Action codes.

4. The **AUTHORIZED BY** field is optional. Note the user id of the person who authorized the request.

5. Once the request has been processed, the batch program completes the **DATE COMPLETED** field. This field will remain blank until the record is successfully processed.

    Changes to a request can be made, as long as the DATE COMPLETED field is null (blank). A new request can also be deleted from the system by pressing the

[Remove] button, as long as the DATE COMPLETED field is null. Once the record is processed by the SAMS batch program (DATE COMPLETED field is not null), changes can no longer be made without selecting a record, copying it, and selecting an Action.

6. Enter in the **COMMENTS** field notes pertaining to the action taken on this request (e.g., initial setup for new user).

    NOTE: Error messages generated by batch processing when the request was processed are shown in this field.

7. Complete the fields in the Application Information block and Security Access Code (see below).

Application Information Block

1. In the **NAME & ROLE** fields, "PCMS" and "CARDHOLDER" are defaulted. Click the mouse in the **NAME** field and press the [List] button to see a valid list of applications and roles.

    i.e., Agency_Coordinator (APC)
    Local_Program_Coordinator (LAPC)
    Cardholder
    Finance_MGR_Role (FM)

    Make a selection and press [Tab] to move to the **PROGRAM CODE** field.

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

2. If the person requesting access already has an NFC user id, enter that id in the **USER ID** field. If not, press [List] to select from a list of available user ids. The cursor moves to the PASSWORD field. If the user already has a PCMS user id, enter the existing PCMS user id and add an alpha character at the end.

    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 a user id selected has already been assigned in SAMS or already belongs to a PCMS user.

3. Enter a **PASSWORD** that is eight positions long and contains both alpha and numeric characters. The password must begin with an alpha character.

    NOTE: Passwords cannot be reused. For example: The old password was "Faith001". Cannot reuse "Faith001" again but can use "Faith002".

Security Access Code (SAC) Block

The SAC defines the user's level of access. Cardholder's should have a SAC allowing them to see only their record.

Defining a SAC:

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 units of a particular region 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**, which should be populated after having selected NAME & ROLE.

2. Enter the 2 digit **DEPARTMENT CODE** (e.g. 12 for USDA) and the cursor will move to the AGENCY field.

3. Enter the 2 digit **AGENCY** (e.g. 11 for Forest Service) and the cursor will move to the REGION field.

4. Enter the 2 digit **REGION** and the cursor will move to the UNIT field. If there is not a region to enter, enter 00.

5. Enter the 2 digit **UNIT** and the cursor will move to the sub unit field. If there is not a unit to enter, enter 00.

6. Enter the 5 digit **SUB UNIT** (with leading zeros if necessary) and the cursor will move to the account number field. If there is not a sub unit to enter, leave "00000" in the field.

    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. When entering a request for a role other than Cardholder, the ACCOUNT NUMBER field is to remain blank. When the Bank acknowledgment is received in CAMS, the Cardholder's ACCOUNT NUMBER is entered in both CAMS and SAMS.

    NOTE: If the system has not entered ACCOUNT NUMBER in SAMS, enter the credit card account number for the Cardholder.

Removing SAMS Records

If a SAMS record (other than Cardholder) is mistakenly created and saved, it can be deleted by pressing [Remove] as long as the batch process has not run (no date appears in the DATE COMPLETED field).

Lost/Stolen Purchase Cards

After a lost/stolen purchase card is reported to the Bank, NFC deletes the Cardholder's CAMS record in PCMS and adds a new record. When the Bank acknowledgment is received for the new CAMS record (DATE RETURN FROM BANK and ACCOUNT NUMBER are inserted), the NFC updates the Cardholder's record in SAMS (i.e., inserts new ACCOUNT NUMBER and enters into COMMENTS that the record was updated by NFC).