CAMPS

ISR Procedural Guide

Version 6

Table of Contents

ISR PROCEDURAL GUIDE

As a designated Information Security Representative (ISR), you have been given authorization, by the Civil Service Commission, to create and maintain CAMPS Logon ID's for the employees in your jurisdiction.

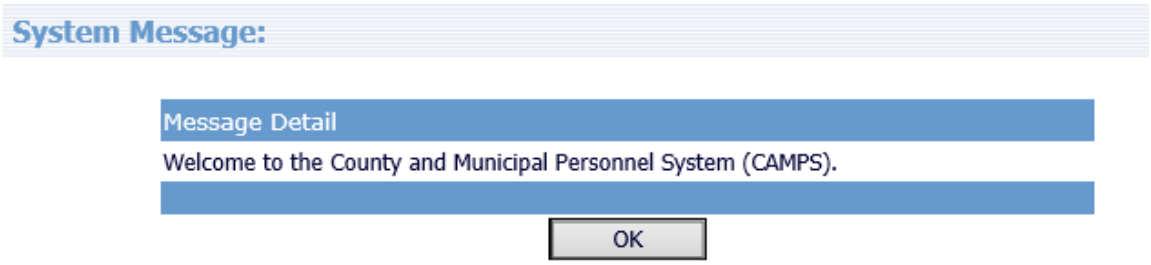
This security level includes the ability to create new Logon ID's, assign security levels, and designate the data groups (jurisdictions and/or departments) that each user within your jurisdiction may access. You may also grant ISR security rights to other users in your organization.

Your ISR Logon ID can be identified by the last byte – *all security id's must end with the number '8.'*

In addition to the administrative functions listed above, this id will also allow you to perform the regular data entry functions of CAMPS.

THE SYSTEM MESSAGE SCREEN

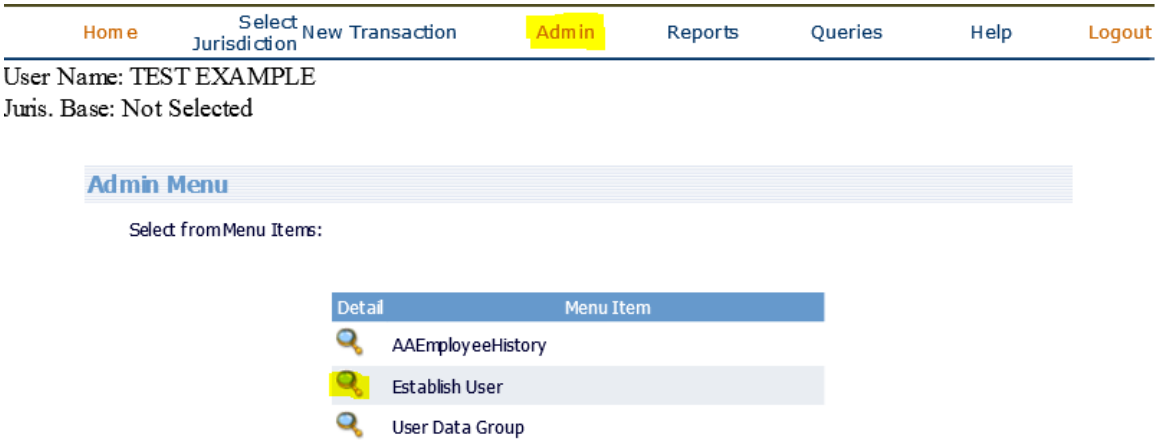
After a successful login to CAMPS, a *System Message* screen will display. If there have been recent changes to the system, or if there is general information of which you should be aware, a message will display here. Please take a moment to read this before proceeding. To continue, click OK.



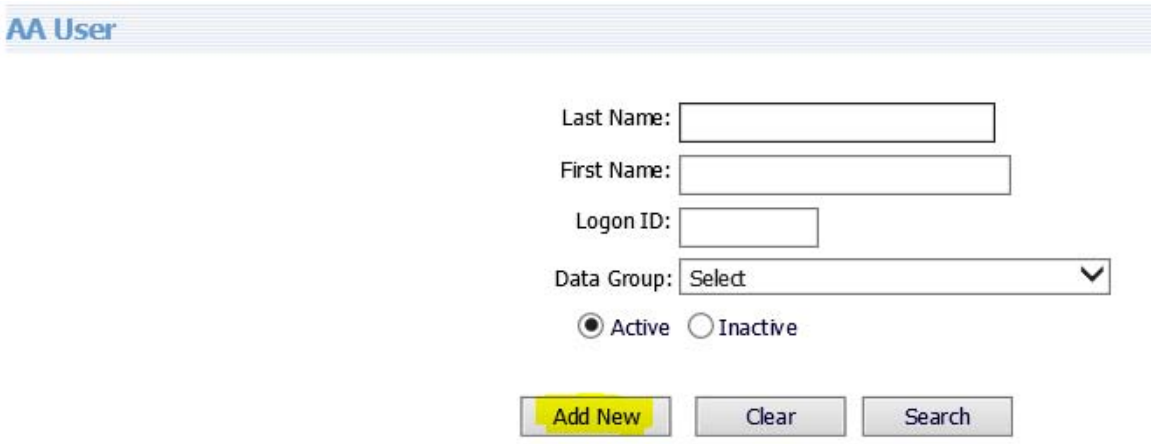
Following the System Message, the Inventory screen for your jurisdiction will display.

CREATING A NEW LOGON ID

To access the Administrative functions, click on "Admin" on the top menu bar. The following options will display:

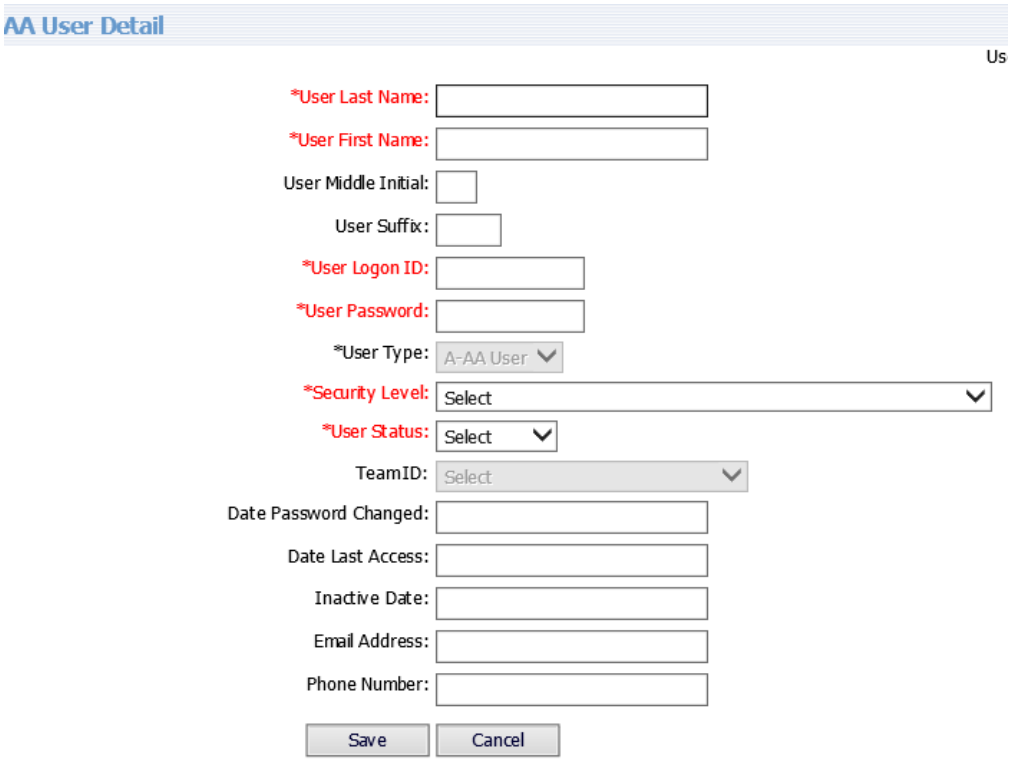


To create a new logon id, click on the magnifying glass icon in the "Detail" column next to the "Establish User" option. The AA USER screen will display:



This screen includes fields for Last Name, First Name, Logon ID, and Data Group. *When creating a new Logon ID, these four fields should be left blank.*

Click the **ADD NEW** button. The AA USER DETAIL screen will display.



You will notice that several fields on this screen (such as User Last Name, User First Name, User Logon ID) display in red, and are preceded by as asterisk. *These fields are required, and must be completed before the record will be accepted.*

Complete each applicable field, as indicated below:

EMPLOYEE NAME

Enter the full name of the employee in the appropriate fields: User Last Name, User First Name, User Middle Initial and, if applicable, User Suffix (Sr, Jr, Esq, etc.).

When entering a last name, embedded blanks and commas are not allowed; however, hyphens and apostrophes are acceptable. For example:

John R O'Hara – valid
Leigh R Van Der Veer – invalid
Leigh R VanDerVeer – valid
Mary Winston-Smith – valid
Mary Winston Smith – invalid

USER LOGON ID

Type the 7-character Logon ID that you are assigning to the user. If the employee has already been assigned a Logon ID to access mainframe systems such as RAPS or PMIS, it is recommended that the same Logon ID be used for the CAMPS system.

- The **first three bytes** of the ID must match the first three bytes of the ISR's id. This code identifies your jurisdiction. This is the system default and cannot be changed.

- The **last four bytes** should be the first four letters of the employee's last name (i.e. Mary Jones might be C9AJONE). In the case of duplicates, the accepted practice is to replace the last letter of the Logon ID with a number (i.e. C9AJON1).

Keep in mind that the Logon ID field is case-sensitive! We recommend that you create Logon ID's in ALL CAPS for consistency.

USER PASSWORD

Type a password for the employee. Passwords must be between 5-7 characters, and are *case-sensitive!* We recommend that you use the Logon ID as their initial password.

Users will be required to change their password the first time they log into CAMPS.

USER TYPE

The only option available to appointing authorities will be "A - AA User."

SECURITY LEVEL

From the drop-down menu, select the appropriate security level for the employee. Valid security levels are as follows:

0	**Data Entry** The user may submit transactions but not approve them. Upon submission, the status will be "*Pending AA App 1*."
1	**Data Entry and First Level AA Approval** The user may submit transactions and approve them. Upon submission, the status will be "*Pending AA App 2*."
2	**Data Entry and Both Levels of AA Approval** The user may submit and approve all transactions, including those requiring a second level of approval. *
8	**Security Administration** Also includes data entry, and both levels of AA Approval.
I	**Inquiry and Report Generation** The user may view the inventory screen but cannot "Select" individual inventory items. Access to Queries and Reports.
M	**Inquiry for Managers** The user may view the inventory AND "Select" individual transactions. Access to Queries and Reports.

*** NOTE**: Some actions, such as Leaves of Absence and Salary Adjustments, are automatically approved once they pass all validations.

USER STATUS

Valid options are "A-Active" or "I-Inactive." Select "A-Active" for a new employee.

TEAM ID

This option is not available to appointing authorities.

DATE PASSWORD CHANGED

This is a display-only field. It will show the date of the most recent password change. For a new Logon ID, the field will be blank.

DATE LAST ACCESS

This field will display the last date on which the user accessed CAMPS. Again, for a new Logon ID, the field will be blank.

INACTIVE DATE

This is a display-only field. If the USER STATUS field is set to "Inactive," the date of that change will be reflected in the Inactive Date field.

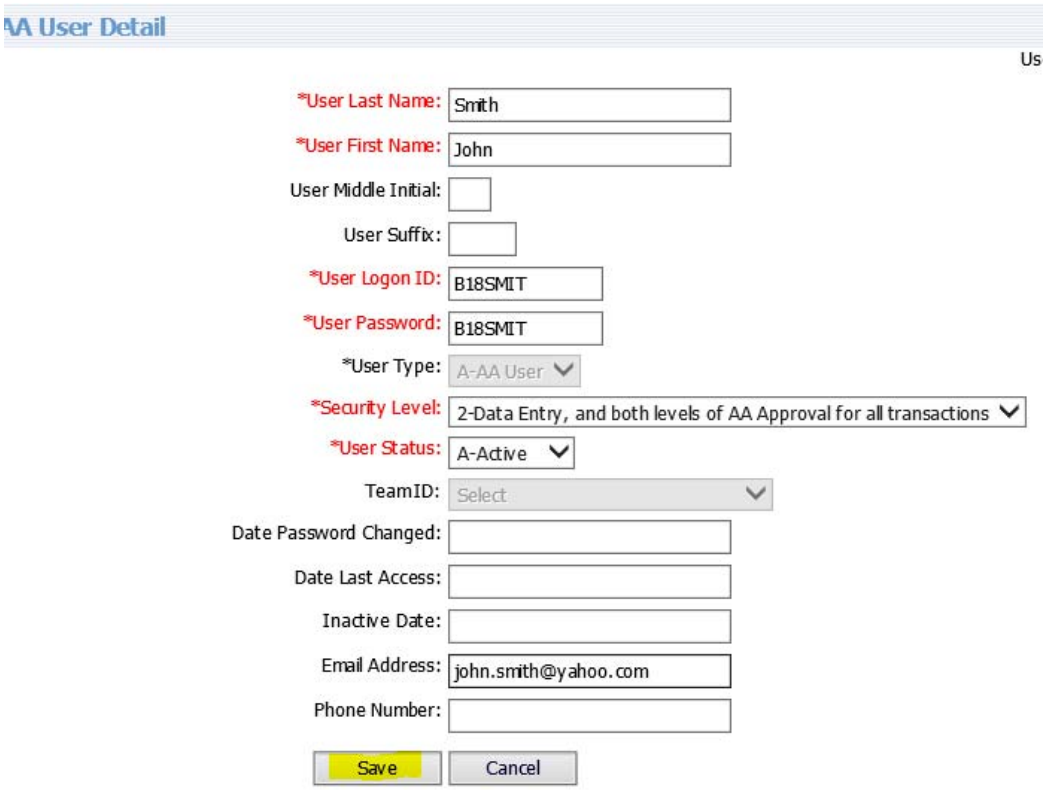
E-MAIL ADDRESS

This is a required field. It is used in conjunction with the "Forgot Password" link on the login screen. Enter the employee's e-mail address.

PHONE NUMBER

This is an optional field that may be used to record an employee's telephone number.

After completing all necessary fields, click **SAVE**.

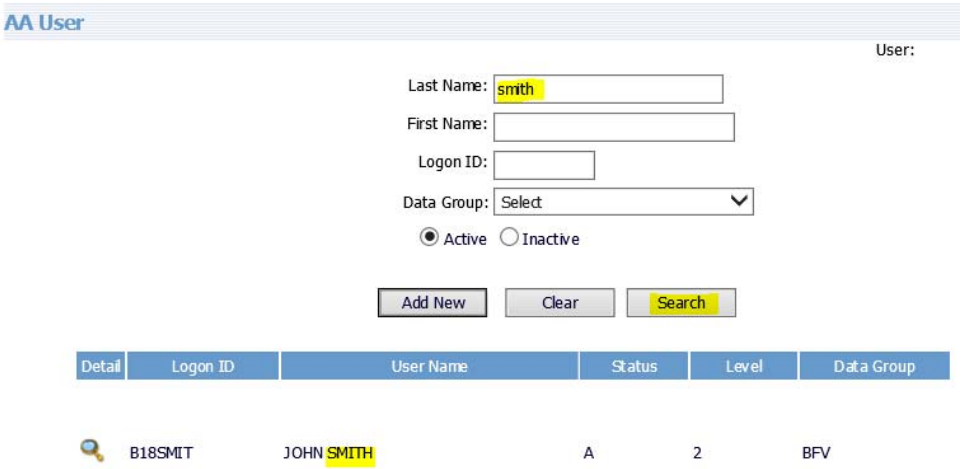


The message "*New User Successfully Added*" will display. After clicking OK, you will be returned to the AA USER screen.

VIEWING THE NEWLY CREATED LOGON ID

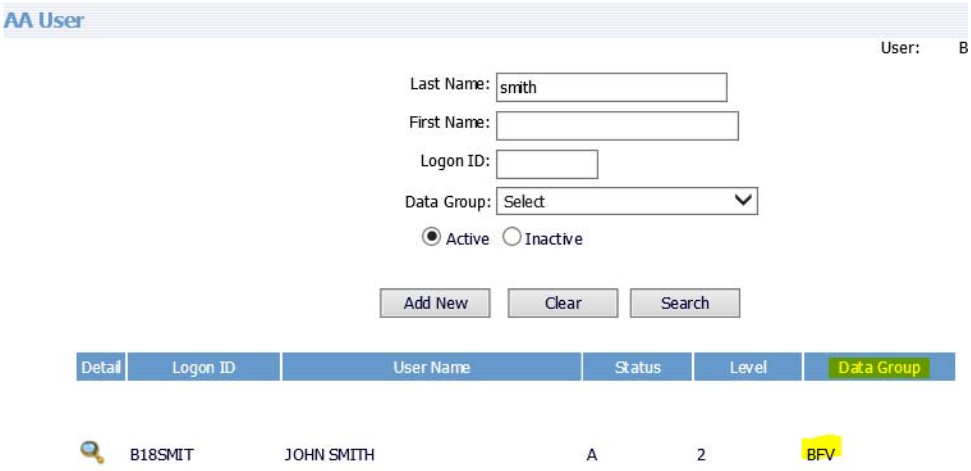
To ensure that the logon id has been created correctly, you may search for it using the AA USER screen.

The quickest method is by typing the user's last name in the Last Name field. Click SEARCH, and all users with that last name will display.



"DATA GROUPS"

You will notice a column on this screen called "Data Group."



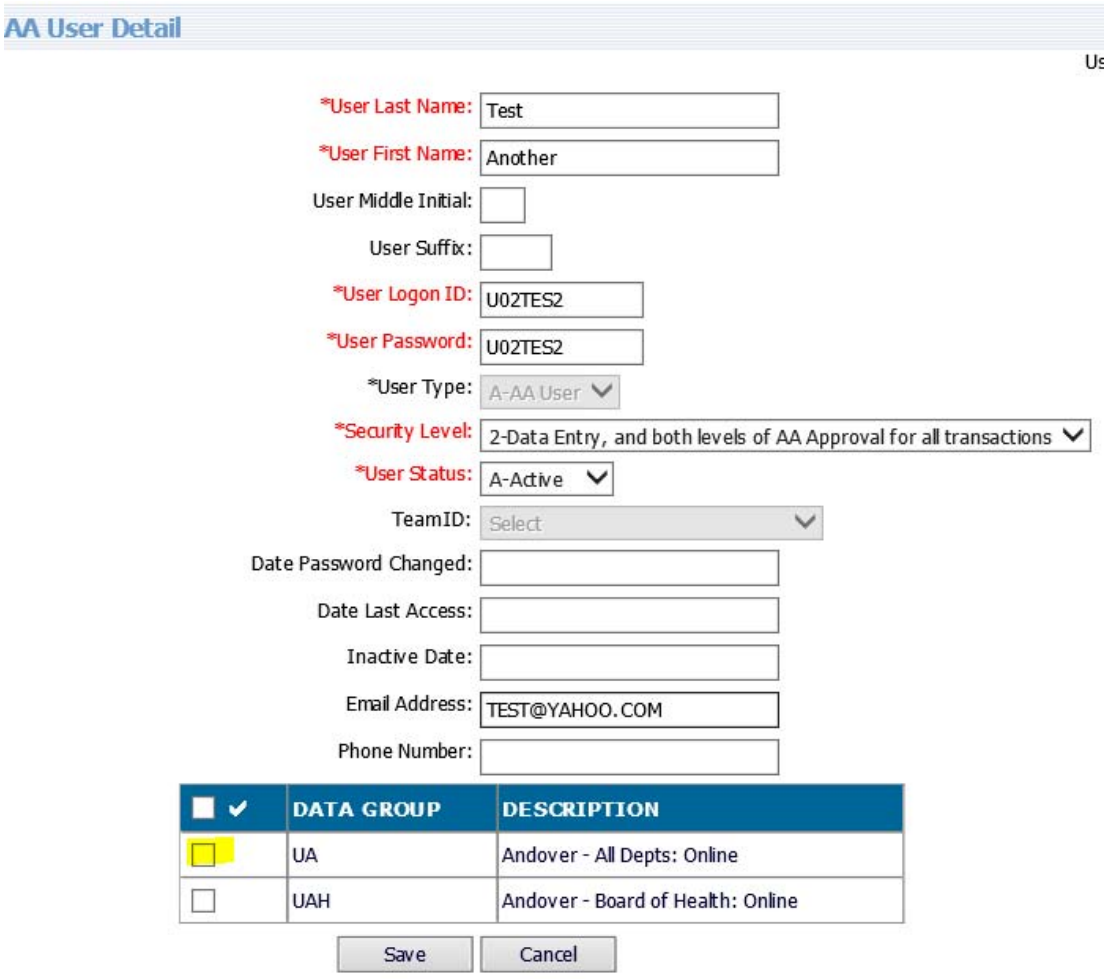
"Data Group" is a term used to define the data (employee information) contained within a specific jurisdiction. In the above example, BFV is the code for the Borough of Fairview. This code restricts the user's CAMPS access to only the data in that jurisdiction.

A data group will automatically be assigned to the new user, based on the data group already in the profile of the ISR (the employee who is creating the id).

MULTIPLE "DATA GROUPS"

In most cases, the ISR will only have access to one data group. Occasionally, however, the ISR may have rights to more than one; for example, the Central Office and the Board of Health.

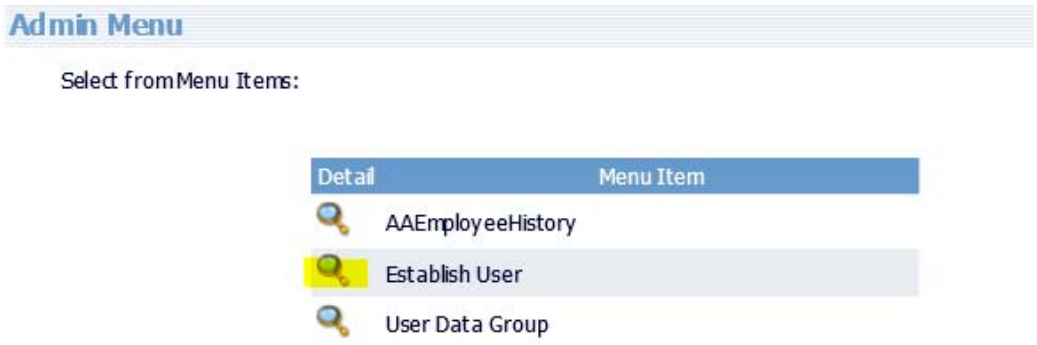
In these cases, both data groups will display at the bottom of the screen. The ISR must select the one (or more) which is appropriate for the new user. At least one data group must be checked before clicking SAVE.



MODIFYING AN EXISTING USER PROFILE

The ISR may modify any of the personal information within an employee's profile, to reset a password, change a security level, update an email address, etc.

From the Administration Menu, click on the magnifying glass icon in the "Detail" column next to the "ESTABLISH USER" option.



The AA USER screen will display, with blank fields for Last Name, First Name, Logon ID, and Data Group. One or more of these fields may now be used as search criteria to locate a specific record. *These fields are NOT case-sensitive*.

- **HINT**: It is NOT necessary to complete all of the following fields. When searching for one person, use Last Name or Logon ID. To see everyone in your jurisdiction, use the Data Group field.

LAST NAME – Type the employee's last name, or the first few characters of the last name.

To further refine the search, position the cursor on the FIRST NAME field, and type the employee's first name.

LOGON ID – Type the employee's Logon ID, or the first few characters of the ID.

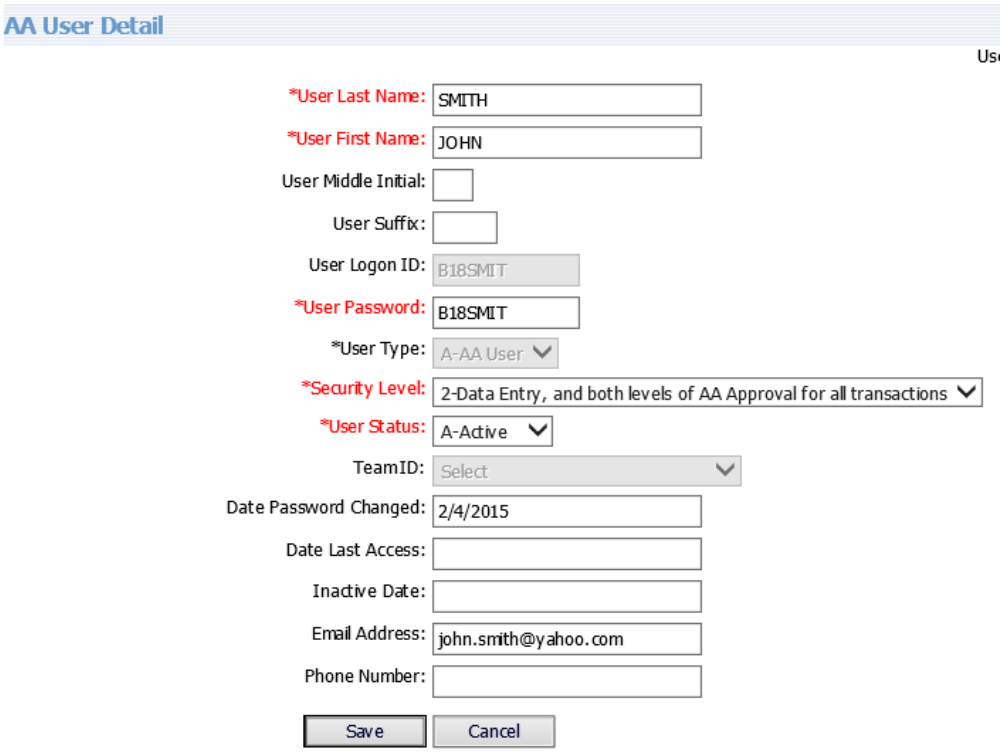
DATA GROUP - Selecting a jurisdiction from this menu will display everyone in that jurisdiction who has access to CAMPS.

After entering the necessary information, click SEARCH. A table will display at the bottom of the screen listing all those records that match the search criteria entered.

Select the appropriate record by clicking on the icon in the "Detail" column, next to the employee's Logon ID. The AA USER DETAIL screen will display.

THE AA USER DETAIL SCREEN

The AA User Detail screen will be populated with the employee's current profile information. Any of these fields may be changed by positioning the cursor on the appropriate field and either typing over the existing data, or making a new selection from the drop-down menu.



RESETTING A PASSWORD

One of the most common reasons for modifying an employee's record is to reset a password. This can easily be done by positioning the cursor on the USER PASSWORD field, and re-typing a new password over the old one. Keep in mind that *passwords are case-sensitive*; we recommend that all passwords be typed in upper-case.

General Password Guidelines

- The user will be forced to change their password the first time they login to CAMPS, and the first time they login after the password has been reset by the ISR.
- Once reset, a password cannot be changed by the user for 10 calendar days. If the password is forgotten, the employee may use the "Forgot Your Password?" link on the login screen, or it can be reset by the ISR.
- The user will be required to change their password every 60 days.
- If the user wishes to change their password between 10-60 days, they may do so by clicking on the "Change Password" link on the main login screen, and following the instructions either on the screen or in the User Manual.

INACTIVATING A RECORD

Once created, a Logon ID cannot be deleted. If for any reason a Logon ID is no longer needed (an employee may be on leave, may have resigned, etc.), it should be inactivated. This may be done on a temporary or a permanent basis.

- To *inactivate* an employee's Logon ID, open the USER STATUS drop-down menu, and select "I-Inactive." Click SAVE to save the change.

- A Logon ID may be *reactivated* at any time by changing the USER STATUS back to "A-Active."

When all changes have been made, click SAVE. The message "Successfully Updated" will display. After clicking OK, you will be returned to the AA USER screen.

To return to the Administration Menu at any time, click on "Admin" on the top Menu Bar

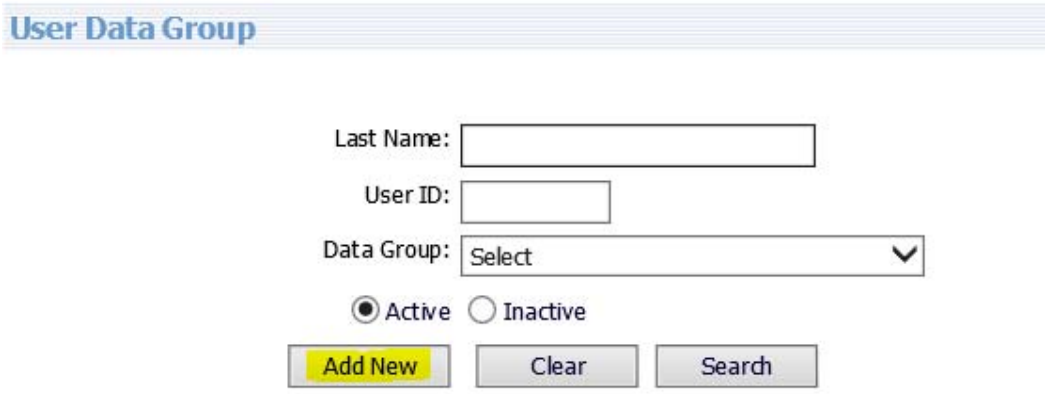
ADDING ADDITIONAL DATA GROUPS TO A LOGON ID

Occasionally an AA ISR may need to give an employee access to a second data group after the id has been created. For example, they may already have access to the Central Office, but now also need access to the Library's data.

- *Keep in mind that an AA ISR can only give access to the data groups that they themselves have access to.*

To grant an existing user access to an additional data group, do the following:

From the Administration Menu, click on the icon in the "Detail" column next to the USER DATA GROUP option. The USER DATA GROUP screen will display.



This screen functions in the same manner as the AA User screen. *To add an additional data group to a user's profile, leave all the fields blank and click **ADD NEW***. The USER DATA GROUP DETAIL screen will display.

THE USER DATA GROUP DETAIL SCREEN

LOGON ID

Type the user's 7-character Logon ID, and click NEXT. A "Data Group" drop-down box will display.

DATA GROUP

From the Data Group drop-down menu, select a data group.

NOTE: If the employee already has access to a data group, that group will not display in the drop-down menu.

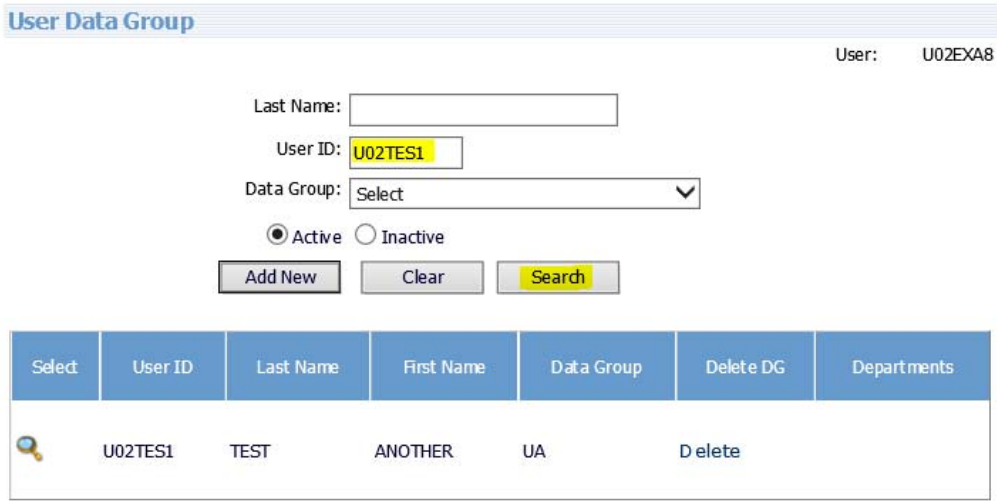
After selecting the appropriate data group, click SAVE. The employee is now authorized to view and/or enter data on the employees in that jurisdiction. The system will return to the USER DATA GROUP screen.

RESTRICTING ACCESS TO A SPECIFIC DEPARTMENT

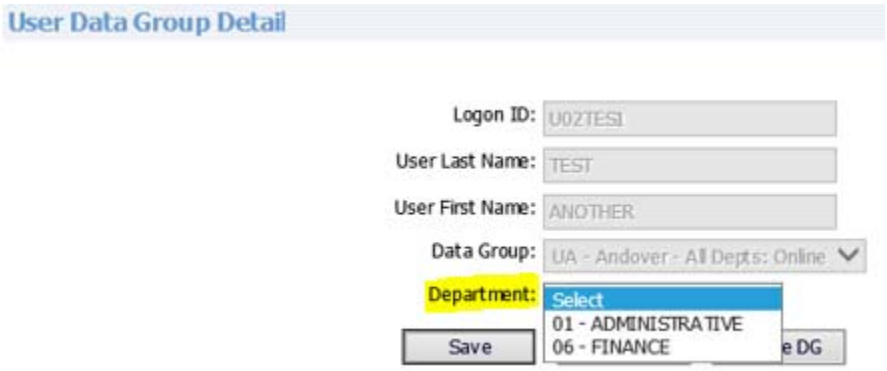
For those jurisdictions that contain multiple departments (such as at the County level), the user will be given access to all departments by default. However, an employee may be restricted to viewing / entering data for only one or more specific departments within a jurisdiction.

To restrict a user to one or more departments, ***you must first create the id and give the employee access to the "All Departments" level***, using the steps described earlier. Once that access is given, do the following:

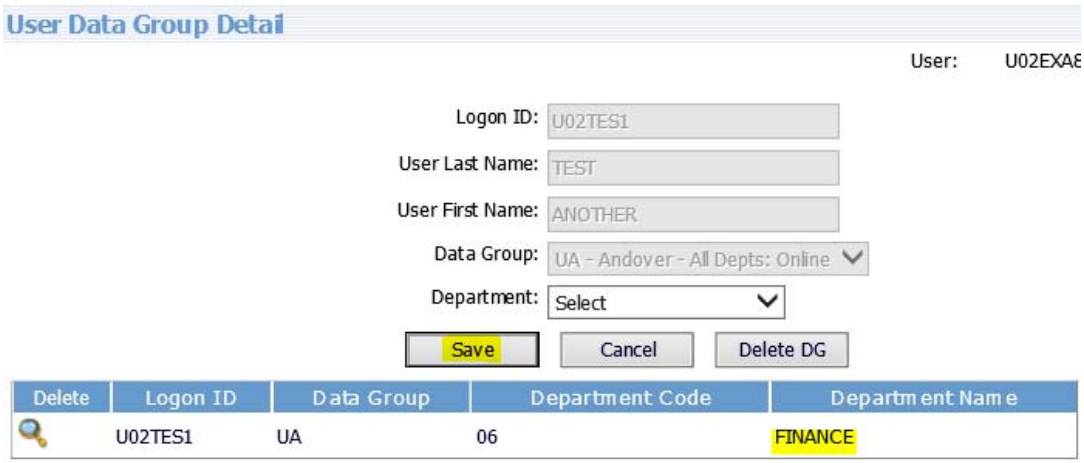
1) From the USER DATA GROUP screen, type the Logon ID of the user in the User ID field. Click SEARCH to display the data group(s) that they currently have access to.



2) Using the magnifying glass icon, select the appropriate data group. The USER DATA GROUP DETAIL screen will display, which will now include a drop-down box for Department.

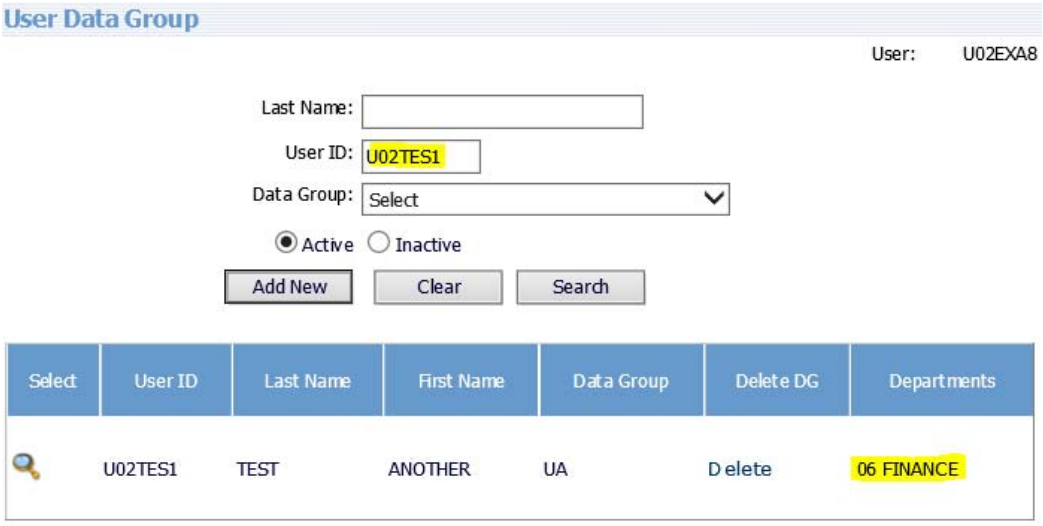


3) Open the Department drop-down menu, and select the department that the employee should have access to. Click SAVE. A grid will display at the bottom of the screen showing that the employee now has access to only that department. To add a second department, follow the same procedure.



4) After verifying that the correct department is displaying, click CANCEL to return to the previous screen.

5) To verify that the employee's access is restricted to one or more departments, enter their User ID on the USER DATA GROUP screen, and click SEARCH. A grid will display showing the employee's Name, User ID, and the department(s) that they are restricted to.



DELETING A USER'S DATA GROUP

To delete a data group from an employee's profile, access the USER DATA GROUP screen from the Administration menu. This screen will display blank fields for Last Name, User ID, and Data Group. One or more of these fields may be used to locate a specific employee.

LAST NAME – Type the employee's last name, or the first few characters of the last name.

USER ID – Type the employee's Logon ID, or the first few characters of the ID.

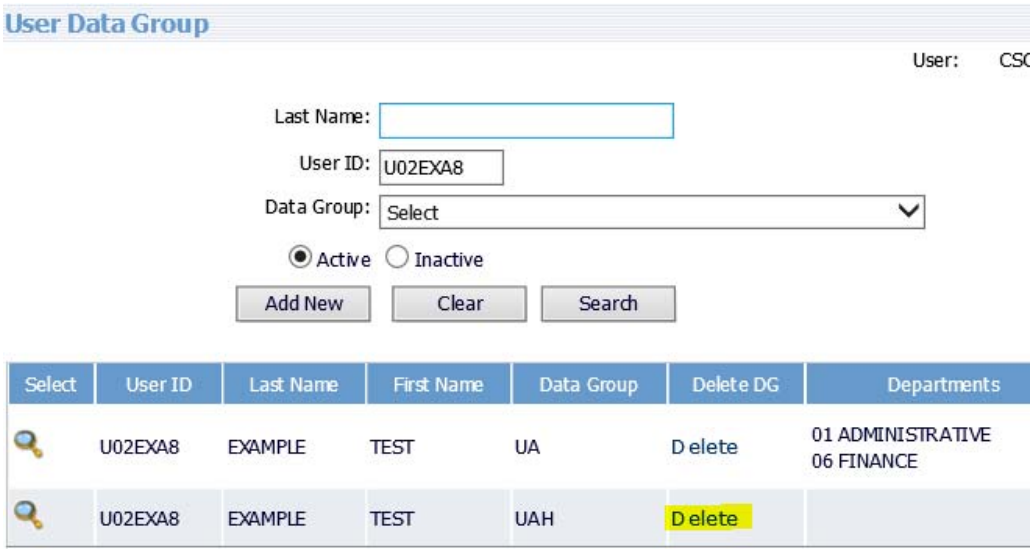
DATA GROUP – From the drop-down menu, select the data group (jurisdiction) that contains the records you wish to view.

After entering the necessary information, click SEARCH. A grid will display at the bottom of the screen listing all those records that match the search criteria entered.

If an employee has been authorized to access more than one data group, each data group will display on a separate line.

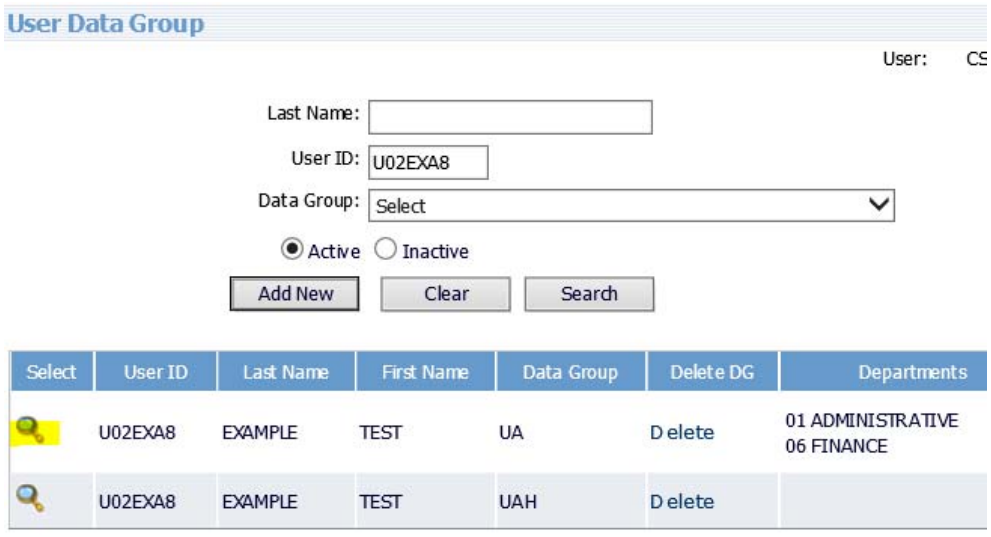
There are two ways to delete a data group from an employee's profile.

1) *To delete an entire data group* (including individual departments), click on the word "Delete" in the DELETE DG column.

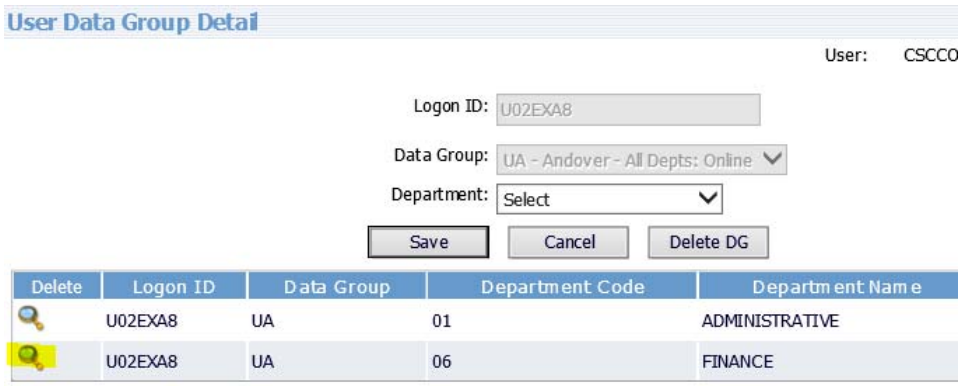


- OR -

2) *To delete only a specific department*, click on the magnifying glass icon in the SELECT column.



The USER DATA GROUP DETAIL screen will display, and each department that the employee has access to will display on a separate line. To delete one or more, click on the magnifying glass under the DELETE column. That department will then disappear from the grid.



NOTE: The DELETE DG button on this screen *will delete the entire data group*, not just a department. Please be sure that is your intention before selecting this button.

LOGGING OFF

To log out of the CAMPS system, click on the LOGOUT option on the right side of the top Menu Bar.

QUICK REFERENCE GUIDE

TO CREATE A NEW LOGON ID

- Click on ADMIN
- Click on ESTABLISH USER
- Click ADD NEW
- On the AA User Detail screen, complete all required fields.
- If a "Data Group" section displays at the bottom of the screen, select the Data Group(s) the employee should have access to.
- Click SAVE.

TO VERIFY THAT THE NEW ID HAS BEEN CREATED

- Click on ADMIN
- Click on ESTABLISH USER
- Enter a Last Name / Logon ID / or select your jurisdiction from the Data Group drop-down menu. (It is only necessary to complete one field.)
- Click SEARCH.
- A grid will display with the user's Logon ID, Name, Security Level, and Data Group(s).
- To view the AA User Detail screen again, click the icon in the "Detail" column.

TO LOOK UP A PASSWORD or MODIFY EXISTING INFORMATION

- Click on ADMIN
- Click on ESTABLISH USER
- Type the user's Last Name OR Logon ID
- Click SEARCH
- Click the DETAIL icon next to the appropriate person
- The AA User Detail screen displays. To change the password, type over it. The name, security level, status, or e-mail fields may also be changed.
- When finished, click SAVE.

TO INACTIVATE A USER

- Click on ADMIN
- Click on ESTABLISH USER
- Type the user's Last Name OR Logon ID
- Click SEARCH
- Click the DETAIL icon next to the appropriate person
- The AA User Detail screen displays. Change the USER STATUS field to I-Inactive.
- Click SAVE.