A guide to using Account Management for associating end user login accounts to Windows based applications in the WCTCS environment.
## CONTENTS

1. OVERVIEW ................................................................................................................................. 3
2. LOGGING IN TO ACCOUNT MANAGEMENT .................................................................................. 4
3. USING THE SELECT USER SCREEN ........................................................................................... 5
4. USING THE EDIT USER SCREEN .................................................................................................. 8
   - Adding a User .............................................................................................................................. 9
   - Associating a User with a College ............................................................................................ 11
   - Associating a User with a Group ............................................................................................ 12
   - Making a User a College Administrator .................................................................................. 13
   - Assigning College Administrator Levels .................................................................................. 14
   - Assigning Financial Aid Groups ............................................................................................. 15
   - Editing a User .......................................................................................................................... 17
   - Changing a User’s Password .................................................................................................... 17
   - Deleting a User ....................................................................................................................... 18
5. USING PROCESS AUTHORIZATION ............................................................................................... 20
   - Assigning Process IDs to a User ............................................................................................. 22
   - Viewing a User’s Process IDs ................................................................................................ 24
   - Modifying a User’s Process IDs .............................................................................................. 25
   - Deleting a User’s Process IDs ................................................................................................ 27
   - Copying a User’s Process IDs to Another User ...................................................................... 28
6. APPENDIX: FIELD ENTRY DEFINITIONS ...................................................................................... 30
   - Select User ............................................................................................................................... 30
   - Edit User .................................................................................................................................. 30
   - Process Authorization ............................................................................................................. 34
Account Management is a web-based application that allows administrators in the Washington Community and Technical College (WCTC) system to manage user information and user access to web-based applications.

Account Management exchanges data with Microsoft Windows Active Directory, Microsoft SQL Server and its numerous databases, and the WCTC applications.

Account Management allows for three types of administrators:

- State Board for Community and Technical Colleges (SBCTC) administrators who manage all college users.
- District administrators who manage all users at all colleges within a district.
- College administrators who manage users at their college only.

Using this application, administrators can:

- Create new users.
- Modify or delete existing users.
- Control users’ access to applications, and assign user access levels for applications, for example, inquire only or inquire and change.
- Create other administrators.
LOGGING IN TO ACCOUNT MANAGEMENT

To log in to Account Management, follow the steps below:

1. From your web browser, go to https://www.wctcs.ctc.edu/wctcs/.
2. From the Login screen, type your account name and password and click the OK button or press return.
3. A FERPA message will be displayed. The message is standard for all colleges and cannot be customized by college. Click the Continue button.
4. From the List of Colleges screen, click on a college. (This screen only appears if you are associated with more than one college.)
5. From the List of Applications screen, click on Account Management. (This option only appears if you are authorized to access Account Management.) Account Management launches and the Select User screen is displayed.

**Note:** In order to run Account Management, you may need to turn off pop-up blocker software.

Administrative rights within Account Management are determined by user access level. The possible user access levels are:

- 0 = Inquire only
- 1 = Change password/Deactivate/Reactivate/Unlock
- 2 = Change
- 3 = Add
- 4 = Delete

To log out of Account Management, click the Exit button on the Select User screen. If, for a period of 20 minutes, you do not perform an action that sends a signal to the server, such as modifying a user’s settings, Account Management will automatically time out and you will be logged out of the application.
Based on your administrative level, the Select User screen allows you to:

- View all the users within your district, if you are a district administrator.
- View all the users at a specific college.
- View a group of users, for example, North Seattle Community College administrators.
- View a specific user.
- Access a specific user’s Account Management attributes.
- Add a user.

Access Process Authorization to give users access to applications.
The Select User screen provides the following filters for narrowing down the list of users:

**College filter**: If you are the administrator for a district college, use this filter to view all of the users at a specific college in your district. If you are the administrator for a non-district college, such as Bellevue College, you will see only your college in this filter. Note that administrators for non-district colleges will see a district title in the District Users field, for example, Bellevue District.

**Group filter**: Use this filter to view a specific group of users within your district or at your college. For example, if you are a Seattle district administrator you will see groups for North Seattle Community College (NSCC) administrators or South Seattle Community College (SSCC) administrators.

**Last name filter**: Use this filter to locate a specific user by last name. This filter allows you to enter free text which progressively matches the users’ last names from left to right. There are no minimum characters required; one character will generate matches.

**Note**: You can use an asterisk symbol (*) wildcard for any number of characters in your search string. For example, if you type b*, you will see names such as Baker, James or Bottenberg, Joannie. You can also use wildcards in the middle of your search string. For example, if you type b*k*r, you will see names such as Baker, James or Biker, Jane.

To view all the users within your district or college, leave the default values in the filtering fields and click the Find button. If you are a district administrator, you will see a list of all users within your district. If you are a college administrator, you will see only the users at your college.

To apply filters, follow the steps below:

1. Click the drop-down arrows for the College or Group filters.
2. From the drop-down lists, select a college, a group or both.
3. To narrow your search to an individual user, enter text in the Last name filter.
4. Click the Find button at any point during this process. A list of users is displayed.
Click on the name of the user whose information you want to view or update.

The Edit User screen is displayed. For more information, see Chapter 4, “Using the Edit User Screen.”

From the Select User screen you can also:

Add a new user. To do so, click the Add User button before or after you initiate a search. The Edit User screen is displayed. For more information, see “Adding a User” on page 9.

Control a user’s access to applications such as Degree Audit. To do so, click the Process Authorization link. For more information, see Chapter 5, “Using Process Authorization.”
The Edit User screen allows you to:

- Add a user.
- Associate a user with a college.
- Associate a user with a group.
- Create an administrator.
- Edit a user.
- Change a user’s password.
- Delete a user.

Access Process Authorization and User Report which lists the applications and permissions assigned to a user.
ADDING A USER

To add a user, follow the steps below:

1. From the Select User screen, click the Add New User button. The Edit User screen is displayed, now with the New User pane.

2. Enter the user’s information in the fields shown.

For detailed information about the fields, such as required length, format, and special edits, see the “Edit User” section in the Appendix.

3. Type the 9-character employee SID in the field provided. The employee SID must be valid in the EMP_M table. If the employee SID is not valid, an error message is displayed when you click OK to add the record and you cannot proceed.

If the employee SID is found but the first and last names do not match the employee SID in the EMP-M table, a warning message is displayed when you click OK to add the record. If you click OK, you accept the mismatch of the employee’s name and SID.
4 Enter the employee’s valid email address. This information is required for Financial Aid users.

5 Type the same temporary password in both the Password and Confirm password fields.

6 Check the User must change password next login check box to force the user to change his or her password the next time he or she attempts to log in. This step is not required but is recommended.

7 If appropriate for the user, use the Account expires field or the Account disabled, Account locked out, and User must change password next login check boxes.

These function as follows:

<table>
<thead>
<tr>
<th>Field or Check box</th>
<th>Function</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Account expires field</td>
<td>Use this to indicate the date an account expires and becomes inactive. If you are creating a temporary account, type a date. The format is MM/DD/YYYY but single digits for month and day are acceptable, for example, 09/02/2006 or 9/2/2006.</td>
<td>The default is Never. If you clear the field and leave it blank, the Never value is automatically used.</td>
</tr>
<tr>
<td>Account disabled check box</td>
<td>Check this to inactivate an account and to prevent the user from logging in.</td>
<td>The default is unchecked.</td>
</tr>
<tr>
<td>Account locked out check box</td>
<td>When checked, it indicates a user cannot log in. This is automatically (and only) checked by the system when the user makes several unsuccessful attempts to log in by, for example, repeatedly entering an incorrect password. You can uncheck this setting, but you cannot check it.</td>
<td>The default is unchecked.</td>
</tr>
<tr>
<td>User must change password next login check box</td>
<td>Check this to force a user to change his or her password the next time he or she attempts to log in.</td>
<td>The default is checked.</td>
</tr>
</tbody>
</table>
To add the user and return to the Select User screen, click the OK button.

To cancel the operation and return to the Select User screen, click the Cancel button.

To remain on the Edit User screen and associate the user with a college, click the Apply button. For more information, see “Associating a User with a College.”

ASSOCIATING A USER WITH A COLLEGE

If you clicked the Apply button after you entered the user’s information, the Edit User screen is redisplayed, now with the Add/Remove College pane which lists the colleges the user can be associated with. A user can be associated with more than one college; however, you will only see the college or colleges for which you are an administrator. District and college administrators from the other available colleges can associate the user with their colleges.

Note: You can add new users to the system without associating them with a particular college. Users not associated with a college can log in to the system but will not be able to launch any applications.
To associate a user with a college, follow the steps below:

1. To activate the Add/Remove College pane, click the Edit User Details button.

2. To associate the user with a college, click the Add button next to the college. A tab for that college is added to the pane.

3. To remove the user from a college, click the Remove button next to the college. The college tab is removed from the pane.

4. To add the user and return to the Select User screen, click the OK button.

To cancel the operation and return to the Select User screen, click the Cancel button.

To remain on the Edit User screen and associate the user with groups, click the Apply button. For more information, see “Associating a User with a Group.”

ASSOCIATING A USER WITH A GROUP

If you clicked the Apply button after you associated the user with a college or colleges, the Edit User screen is redisplayed, now with the Group Memberships pane. Group Memberships associate a user with a specified Active Directory group, thereby granting certain privileges in various applications. For example, creating administrators in Account Management or assigning permissions to perform various functions in Financial Aid.

If a user is associated with more than one college, several college tabs appear above the Group Memberships pane. The active college tab is dimmed or “grayed out.” In the following screenshot, the Seattle Central Community College tab is active. Any groups associated with the user account will only apply to SCCC. To apply the same (or different) groups at another college, click the appropriate college tab.
MAKING A USER A COLLEGE ADMINISTRATOR

A college administrator is given access to Account Management for the purpose of creating and managing user accounts at various levels. For more information, see “Assigning College Administrator Levels.”

Each college has a single administrators group defined in Active Directory. The group membership name appears in the Available Groups box with the college acronym followed by “Administrators.” For example, SCCC Administrators represents Seattle Central Community College Administrators.

To make a user a college administrator, follow the steps below:

1. To activate the Group Membership pane, click the Edit User Details button.
   
   The active college tab is dimmed or “grayed out.”

2. From the Available Groups box, click on an administrator group. For example, an SCCC administrator will see SCCC Administrators in the Available Groups box.

3. Click the button.
   
   The group is removed from the Available Groups box and appears in the Group Memberships box.
4 To accept the administrator group and remain on the Edit User screen to set the appropriate administrator level, click the Apply button. For more information, see “Assigning College Administrator Levels.”

To accept the administrator group and return to the Select User screen, click the OK button.

To cancel the operation and return to the Select User screen, click the Cancel button.

5 To remove a user from a group, in the Group Memberships box, click on a group and then click the button.

The group is removed from the Group Memberships box and appears in the Available Groups box.

ASSIGNING COLLEGE ADMINISTRATOR LEVELS

If you clicked the Apply button after you associated the user with a college administrator group or groups, the Edit User screen is redisplayed, now with the Administrator user access level drop-down list in the Group Memberships pane.

Note that administrators can create other administrators as follows:

SBCTC administrators can create SBCTC, district and college administrators.

District administrators with a user access level of 3 or greater can create district or college administrators in their district. The district administer must first be made a college administrator for each college in their district.

College administrators with a user access level of 3 or greater can create college administrators for their particular college.

To assign college administrator levels, follow the steps below:

1 To activate the Group Memberships pane, click the Edit User Details button.

2 From the Administrator user access level drop-down list, select the appropriate level.

The available levels are:

   0 = Inquire only (default)
   1 = Change password/Deactivate/Reactivate/Unlock
   2 = Change
   3 = Add
   4 = Delete
3 To accept the administrator level for the user at the active college, and remain on the Edit User screen, click the Apply button.

To accept the administrator level and return to the Select User screen, click the OK button.

To cancel the operation and return to the Select User screen, click the Cancel button.

ASSIGNING FINANCIAL AID GROUPS

Financial Aid System (FAS) groups allow you to manage users’ activity within FAS. Financial aid relies on Active Directory to create user groups. The groups are associated with various permissions inside the financial aid application. The groups are then assigned to a user via Account Management.

The available groups are:

- FAS Director
- FAS View Only
- FAS Prg Assist
- FAS Prg Coord
- FAS Role Admin
While it is more common to assign a user to a single FAS role, you can assign a user to multiple roles.

Remember that all FAS users must have a valid, formatted email address in the E-mail field in the Edit User screen. If this field is blank, an “Adding to FAS Group requires an email” error message appears at the bottom of the screen.

To assign financial aid groups, follow the steps below:

1. To activate the Group Membership pane for assigning FAS groups, click the Edit User Details button.

   The active college tab is dimmed or “grayed out.”

2. From the Available Groups box, click on a FAS group. For example, an SCCC administrator will see 062 FAS [group name] in the Available Groups box.

3. Click the > button.

   The group is removed from the Available Groups box and appears in the Group Memberships box.

4. To accept the FAS group and remain on the Edit User screen, click the Apply button.

   To accept the FAS group and return to the Select User screen, click the OK button.

   To cancel the operation and return to the Select User screen, click the Cancel button.

5. To remove the user from a group, in the Group Memberships box, click on a group and then click the << button.
The group is removed from the Group Memberships box and appears in the Available Groups box.

EDITING A USER

To modify a user’s existing information, follow the steps below:

1. From the Select User screen, apply filters to search for a specific user.
2. Click on the user’s name.

   The Edit User screen is displayed with the user’s information dimmed or “grayed out.”

   If you are a college administrator within a multiple-college district and click on a user who is not associated with your college, the only details you can edit are the user’s college membership details. For example, if you are an SSCC administrator and you click on an NSCC user, the only action you will be able to perform is to associate the user with SSCC.

3. To edit the user’s information, click the Edit User Details button.
4. Edit the information.

   For detailed information about the fields, such as the required length, format, and special edits, see the “Edit User” section in the Appendix.

   You cannot change the Account name or User ID.

5. If appropriate for the user, use the Account expires field or the Account disabled, Account locked out, and User must change password next login check boxes. For definitions of these fields, see page 10.

6. To add the changes but remain on the Edit User screen, click the Apply button.

   To add the changes and return to the Select User screen, click the OK button.

   To cancel the operation and return to the Select User screen, click the Cancel button.

CHANGING A USER’S PASSWORD

To change a user’s password, follow the steps below:

1. From the Select User screen, apply filters to search for a specific user.
2. Click on the user’s name.

   The Edit User screen is displayed with the user’s information dimmed or “grayed out.”
3 To edit the user’s information, click the Edit User Details button.

4 To change the user’s password, type a new, temporary, Active Directory-compliant password in the Password and Confirm password fields. For more information, see the “Edit User” section in the Appendix.

5 Check the User must change password next login check box to force the user to change his or her password the next time he or she attempts to log in. This step is not required but is recommended.

   If you check this option but do not create a new, temporary password, the user must type his or her old password and a new password the next time he or she attempts to log in.

6 To add the changes but remain on the Edit User screen, click the Apply button.

To add the changes and return to the Select User screen, click the OK button.

To cancel the operation and return to the Select User screen, click the Cancel button.

You can only change passwords for user at the college or colleges for which you are an administrator.

DELETING A USER

To delete a user, follow the steps below:

1 In the Select User screen, apply filters to search for a specific user.

2 Click on the user’s name.

   The Edit User screen is displayed.

3 Click the Delete button.

   A prompt asks if you want to delete the user.
To delete the user and return to the Select User screen, click the OK button.

To cancel the operation and return to the Select User screen, click the Cancel button.

You can only delete users from the college or colleges for which you have a level 4 administrator user access level.

**Note:** To optimize performance, SQL Server utilizes connection pooling, sometimes keeping an account active in the database for as long as 30 minutes after a user logs out. This means that if you delete a user account within 30 minutes of the user’s last connection, that account may still be active in the database. This situation is rare; however, the workaround is to immediately disable the account and then delete it after 30 minutes. Again, this is only necessary if a user was logged in within 30 minutes prior to you deleting the user’s account.
Process Authorization allows administrators to control user access to the following:

**Application Logging:** Provides a searchable log history of user activity, such as failed log-ons, time of activity, and successful application access. By assigning Application Logging to a user via Process Authorization, you create a “List of Applications” menu that displays the applications along with other assignments such as Financial Aid or Account Management.

**CEIS – Central Employee Inquiry System:** Allows human resources (HR) and payroll staff to look up employment records for employees, such as part-time faculty, who work (or have worked) at more than one college or campus across the state. The employee information is extracted from the Employee database using job group PG660R. College employment staff can obtain the information required for processing benefits for these employees at their college.

**Degree Audit:** A web-based advising module developed at SBCTC-IT. With Degree Audit, students and advisors have access to a set of integrated tools that assist in the evaluation and planning of a student’s academic or professional/technical goals.

**OneLookUp (SMS):** To coincide with the 2011 implementation of the system-wide Common SID, this Windows based application was developed that allows you to view certain student data at other colleges based on the entry of a SID or SSN. The application is designed to help research SID/SSN errors when receiving a student’s request to be assigned a SID used at a previously attended college.

**Web Admissions Center:** From the college user perspective, the Web Admissions Center is used to review student admissions applications and enter any codes/data that are required. Data entered by the student and college is entered into the SMS and/or ADM databases.

By assigning one of the applications noted above to a user via Process Authorization, you create a “List of Applications” menu that displays links to the applications along with other assignments such as Financial Aid or Account Management.

For the purposes of Process Authorization, the processes are referred to by process identification codes (IDs). Application Logging’s process ID is LOGING, the CEIS process ID is CR5910, Degree Audit’s process ID is SD4007, OneLookUp’s process ID is SM5036, and Web Admissions process ID is SM2011.
With Process Authorization, administrators can:

- Assign process IDs to a user.
- Modify a user’s process IDs.
- Delete a user’s process IDs.
- Copy a user’s process IDs to another user.

For every process ID you assign to a user, you must also assign:

- A process group which assigns the process to a particular page in the user’s process menu, for example, page 1 or 2. Because Process Authorization is being used for just a handful of applications that all fit on a single page, the default of 0 is an appropriate setting at this time.
- A user access level which indicates the functions the user can perform when accessing the processes. The generic definitions for the user access levels are as follows:

  0 = Inquire only
  1 = Change
  2 = Add
  3 = Delete
  4 = WCCCC

Because Application Logging, CEIS, and OneLookUp are inquiry only based applications, the default user access level setting of 0 is appropriate.

User access levels for Degree Audit include two categories: one for advisors and one for administrators. Advisors can run audits on students, create notes on a student’s account and create academic plans for a student. Administrators have the same capabilities as advisors, but can also create, modify and delete degree definitions and configure the Degree Audit application. The levels should be assigned as follows:

- 0, 1, 2 = Advisor (all levels function the same)
- 3, 4 = Administrator (both levels function the same)

The Web Admissions Center does not utilize the user access level settings. The value can be left at the default of 0.
ASSIGNING PROCESS IDS TO A USER

To assign process IDs to a user, follow the example of assigning Application Logging below:

1. From the Select User screen, apply filters to search for a specific user.

2. Click on the user’s name.
   The Edit User screen is displayed.

3. Click the Edit User Details button.

4. Click the Process Authorization link.
   The Process Authorization screen is displayed. The user’s information appears in the College, Account name, and User Id fields, but cannot be edited.

You can access the Process Authorization screen directly from the Select User screen without first selecting a user. If you do, on the Process Authorization screen, use the College and Account name drop-down lists to select a user.

5. Click the Add button.
   The Process Authorization—Add Process screen is displayed. For detailed information about the fields, such as the required length, format, and special edits, see the “Process Authorization” section in the Appendix.
6 From the Application Area drop-down list, select Application Logging.

7 From the Process ID drop-down list, select the process ID LOGING | Application Logging.

8 In the Process Group field, use the default value of 0.

To prevent blank pages from being created in the user’s process menu, the maximum value that you can type in the Process Group field is determined by the value in the Hi Process Group field displayed on the Process Authorization screen. The value in the Process Group field must be less than or equal to the value in the Hi Process Group field plus 1. For example, if the Hi Process Group value is 3, the maximum value you can type in the Process Group field is 4.

9 In the User Access Level field, use the default value or type a new value. The default value is 0.

10 To save the changes and return to the Process Authorization screen, click the OK button. The Process Authorization screen is redisplayed, now with the new process ID.

To add more processes to the user account, repeat above steps on the next line.

To cancel the operation and return to the Process Authorization screen, click the Cancel button.

11 If you clicked OK, you must complete the operation in the Process Authorization screen by doing one of the following:
To complete the operation and remain on the Process Authorization screen, click the Apply button.

To complete the operation and return to the screen from which you accessed Process Authorization, click the OK button.

To restore the original settings and remain on the Process Authorization screen, click the Reset button.

To cancel the operation and return to the screen from which you accessed Process Authorization, click the Cancel button.

**VIEWING A USER’S PROCESS IDS**

To view the process IDs assigned to a user, from the Edit User screen, click the User Report link. Note that you can only see a user’s authorization details at the college or colleges for which you are an administrator.

A printable report will show:

- The user’s associated college or colleges.
- The applications assigned to the user.
- Account Management appears if the user was assigned to the college administrator group.
- FAS appears if the user was associated with any of the FAS groups.
- Application Logging, CEIS, Degree Audit, OneLookUp, and/or Web Admissions appear if the user was assigned any of these functions in Process Authorization.
- The processes to which the user has access.
- The user’s access level relative to those processes.
MODIFYING A USER’S PROCESS IDS

To modify a user’s process IDs, follow the steps below:

1. From the Select User screen, apply filters to search for a specific user.

2. Click on the user’s name.
   The Edit User screen is displayed.

3. Click the Edit User Details button.

4. Click the Process Authorization link.
   The Process Authorization screen is displayed. The user’s information appears in the College, Account name, and User Id fields, but cannot be edited.

   You can access the Process Authorization screen directly from the Select User screen without first selecting a user. If you do, on the Process Authorization screen, use the College and Account name drop-down lists to select a user.

5. Select a process ID and click the Edit link next to it.
   The Process Authorization—Edit Process screen is displayed. For detailed information about the fields, such as the required length, format, and special edits, see the “Process Authorization” section in the Appendix.
6 Type new values in the Process Group and User Access Level fields.

To prevent blank pages from being created in the user’s process menu, the maximum value that you can type in the Process Group field is determined by the value in the Hi Process Group field displayed on the Process Authorization screen. The value in the Process Group field must be less than or equal to the value in the Hi Process Group field plus 1. For example, if the Hi Process Group value is 3, the maximum value you can type in the Process Group field is 4.

7 To add the changes and return to the Process Authorization screen, click the OK button. The Process Authorization screen is redisplayed with the changes you made.

To cancel the operation and return to the Process Authorization screen, click the Cancel button.

8 If you clicked OK, you must complete the operation in the Process Authorization screen by doing one of the following:

To complete the operation and remain on the Process Authorization screen, click the OK button.

To complete the operation and return to the screen from which you accessed Process Authorization, click the OK button.

To restore the original settings and remain on the Process Authorization screen, click the Reset button.
To cancel the operation and return to the screen from which you accessed Process Authorization, click the Cancel button.

DELETING A USER’S PROCESS IDS

To delete a user’s process IDs, follow the steps below:

1. From the Select User screen, apply filters to search for a specific user.
2. Click on the user’s name.
   The Edit User screen is displayed.
3. Click the Edit User Details button.
4. Click the Process Authorization link.
   The Process Authorization screen is displayed. The user’s information appears in the College, Account name, and User Id fields, and is display-only.

You can access the Process Authorization screen directly from the Select User screen without first selecting a user. If you do, on the Process Authorization screen, use the College and Account name drop-down lists to select a user.

5. Select a process ID and click the Delete link next to it.
   A prompt asks if you want to delete the selected process ID.

   ![Prompt image]

6. To delete the process ID, click the OK button in the prompt.
7. If you clicked OK, you must complete the operation in the Process Authorization screen by doing one of the following:
   To add the changes and remain on the Process Authorization screen, click the Apply button.
   To add the changes and return to the screen from which you accessed Process Authorization, click the OK button.
To restore the original settings and remain on the Process Authorization screen, click the Refresh button.

To cancel the operation and return to the screen from which you accessed Process Authorization, click the Cancel button. Note that you can still cancel the operation even if you clicked the OK button in the prompt. To do so, click the Cancel button in the Process Authorization screen.

**COPYING A USER’S PROCESS IDS TO ANOTHER USER**

To copy a user’s process IDs to another user, follow the steps below:

1. From the Select User screen, apply filters to search for a specific user.
2. Click on the user’s name.
   The Edit User screen is displayed.
3. Click the Edit User Details button.
4. Click the Process Authorization link.
   The Process Authorization screen is displayed. The user’s information appears in the College, Account name, and User Id fields, and is display-only.
   You can access the Process Authorization screen directly from the Select User screen without first selecting a user. If you do, on the Process Authorization screen, use the College and Account name drop-down lists to select a user.
5. From the Copy Authorization from a User drop-down list, click on a user’s name.
   The names that appear in the list are determined by the college with which the first user is associated. For example, if the first user is associated with SCCC, only users associated with SCCC will appear in the list.
6 Click the Copy button.

The process IDs assigned to the user listed in the Copy Authorization from a User drop-down list are copied to the user account name appearing at the top of the screen. Existing assigned processes are replaced.

7 To add the changes and remain on the Process Authorization screen, click the Apply button.

To add the changes and return to the screen from which you accessed Process Authorization, click the OK button.

To restore the original settings and remain on the Process Authorization screen, click the Reset button.

To cancel the operation and return to the screen from which you accessed Process Authorization, click the Cancel button.
The following tables provide detailed information, such as the length, format, and special edits, about the data in fields in Account Management.

### SELECT USER

<table>
<thead>
<tr>
<th>Field</th>
<th>Edits</th>
</tr>
</thead>
<tbody>
<tr>
<td>College filter</td>
<td>From the drop-down list, select a college.</td>
</tr>
<tr>
<td>Group filter</td>
<td>From the drop-down list, select a group.</td>
</tr>
</tbody>
</table>
| Last name filter | Required: Optional  
Character Classes: Alphabetic, space, hyphen, apostrophe  
Length: 0 - 16 characters  
Format: No special requirements  
Special Edits: The application is designed to handle single quotation marks in names, for example, O’Leary.  
Default: None |

### EDIT USER

<table>
<thead>
<tr>
<th>Field</th>
<th>Edits</th>
</tr>
</thead>
</table>
| First name | Required: Yes  
Character Classes: Alphabetic, space, hyphen, apostrophe  
Length: 1 - 30 characters  
Format: No special requirements  
Special Edits: The application is designed to handle single quotation marks in names, for example, O’Leary.  
Default: None |
<table>
<thead>
<tr>
<th>Field</th>
<th>Edits</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initial</td>
<td>Required: Optional</td>
</tr>
<tr>
<td></td>
<td>Character Classes: Alphabetic</td>
</tr>
<tr>
<td></td>
<td>Length: 0 - 1 character</td>
</tr>
<tr>
<td></td>
<td>Format: No special requirements</td>
</tr>
<tr>
<td></td>
<td>Special Edits: None</td>
</tr>
<tr>
<td></td>
<td>Default: None</td>
</tr>
<tr>
<td>Last name</td>
<td>Required: Yes</td>
</tr>
<tr>
<td></td>
<td>Character Classes: Alphabetic, numeric, space, hyphen, apostrophe</td>
</tr>
<tr>
<td></td>
<td>Length: 1 - 30 characters</td>
</tr>
<tr>
<td></td>
<td>Format: No special requirements</td>
</tr>
<tr>
<td></td>
<td>Special Edits: The application is designed to handle single quotation marks in names, for example, O’Leary.</td>
</tr>
<tr>
<td></td>
<td>Default: None</td>
</tr>
<tr>
<td>Account name</td>
<td>Required: Yes</td>
</tr>
<tr>
<td></td>
<td>Character Classes: Alphabetic, numeric</td>
</tr>
<tr>
<td></td>
<td>Length: 5 - 20 characters</td>
</tr>
<tr>
<td></td>
<td>Format: 999aaaaa... The first 3 digits are the 2-digit district code and a “0” followed by an alphabetic string, for example, 060khwewitt.</td>
</tr>
<tr>
<td></td>
<td>Special Edits: Must be unique across the entire WCTC system.</td>
</tr>
<tr>
<td></td>
<td>Default: The first 3 digits are automatically generated when a new user is added.</td>
</tr>
<tr>
<td>User ID</td>
<td>Required: Yes</td>
</tr>
<tr>
<td></td>
<td>Character Classes: alphabetic, numeric</td>
</tr>
<tr>
<td></td>
<td>Length: 1 - 8 characters</td>
</tr>
<tr>
<td></td>
<td>Format: No special requirements</td>
</tr>
<tr>
<td></td>
<td>Special Edits: Must be unique across the entire district. Once entered and applied, the user ID cannot be modified.</td>
</tr>
<tr>
<td></td>
<td>Default: None</td>
</tr>
<tr>
<td>Field</td>
<td>Edits</td>
</tr>
<tr>
<td>---------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Employee SID</td>
<td>Required: Yes</td>
</tr>
<tr>
<td></td>
<td>Character Classes: Alphabetic, numeric</td>
</tr>
<tr>
<td></td>
<td>Length: 1 - 9 characters</td>
</tr>
<tr>
<td></td>
<td>Format: Typically 9 digits, but alphabetic characters are allowed.</td>
</tr>
<tr>
<td></td>
<td>Special Edits: Must be valid in the Emp_M table with a matching first and last name.</td>
</tr>
<tr>
<td></td>
<td>If an employee SID is not found, an error message is displayed.</td>
</tr>
<tr>
<td></td>
<td>If an SID is found, and the first and last names do not match the SID, a warning message is displayed.</td>
</tr>
<tr>
<td></td>
<td>Default: None</td>
</tr>
<tr>
<td>E-mail</td>
<td>Required: Only for FAS users.</td>
</tr>
<tr>
<td></td>
<td>Character Classes: Alphabetic, numeric, “at” sign (@), hyphen, underscore, period</td>
</tr>
<tr>
<td></td>
<td>Length: 1 - 60 characters</td>
</tr>
<tr>
<td></td>
<td>Format: &lt;character string&gt; &lt;@&gt; &lt;alphanumeric and periods&gt;</td>
</tr>
<tr>
<td></td>
<td>Special Edits: Enter an email address only if the user is an FAS user. Be careful when using quotation marks with all non-alphanumeric characters.</td>
</tr>
<tr>
<td></td>
<td>Default: None</td>
</tr>
<tr>
<td>Password,</td>
<td>Required: Only for adding new users.</td>
</tr>
<tr>
<td>Confirm password</td>
<td>Character Classes: Standard alphanumeric and special characters (punctuation).</td>
</tr>
<tr>
<td></td>
<td>Length: 8 - 100 characters</td>
</tr>
<tr>
<td></td>
<td>Format: Character string</td>
</tr>
<tr>
<td></td>
<td>Special Edits: Must also pass Active Directory (AD) and group policies (GP) edits. The value must be at least 8 characters and contain a mix of alphanumeric and special characters, for example, 3at$Rgre8t!. A password recently used cannot be reused.</td>
</tr>
<tr>
<td></td>
<td>Default: None</td>
</tr>
<tr>
<td>Account expires</td>
<td>Required: Optional</td>
</tr>
<tr>
<td></td>
<td>Character Classes: Numeric, forward slash</td>
</tr>
<tr>
<td></td>
<td>Length: 8 - 10 characters</td>
</tr>
<tr>
<td></td>
<td>Format: MM/DD/YYYY</td>
</tr>
<tr>
<td></td>
<td>Special Edits: Must be a valid date. Month and day can be expressed.</td>
</tr>
<tr>
<td>Field</td>
<td>Edits</td>
</tr>
<tr>
<td>-----------------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>Field</td>
<td>as a single digit. NULL and Never (also indicated by a blank) are allowed and indicate there is no expiration date defined. Default: Never</td>
</tr>
<tr>
<td>Account disabled</td>
<td>Required: Yes</td>
</tr>
<tr>
<td></td>
<td>Character Classes: Boolean (set to true or false)</td>
</tr>
<tr>
<td></td>
<td>Length: NA</td>
</tr>
<tr>
<td></td>
<td>Format: NA</td>
</tr>
<tr>
<td></td>
<td>Special Edits: NA</td>
</tr>
<tr>
<td></td>
<td>Default: Set to false</td>
</tr>
<tr>
<td>Account lockout</td>
<td>Required: Yes</td>
</tr>
<tr>
<td></td>
<td>Character Classes: Boolean (set to true or false)</td>
</tr>
<tr>
<td></td>
<td>Length: NA</td>
</tr>
<tr>
<td></td>
<td>Format: NA</td>
</tr>
<tr>
<td></td>
<td>Special Edits: Allow edits only if field is set to true (a “true” setting can be changed to “false,” but not the inverse); the field will be disabled or “grayed out” if retrieved from the database as false. Default: Set to false</td>
</tr>
<tr>
<td>User must change password next login</td>
<td>Required: Yes</td>
</tr>
<tr>
<td></td>
<td>Character Classes: Boolean (set to true or false)</td>
</tr>
<tr>
<td></td>
<td>Length: NA</td>
</tr>
<tr>
<td></td>
<td>Format: NA</td>
</tr>
<tr>
<td></td>
<td>Special Edits: NA</td>
</tr>
<tr>
<td></td>
<td>Default: Set to false</td>
</tr>
<tr>
<td>Job Scheduler</td>
<td>Required: Yes</td>
</tr>
<tr>
<td></td>
<td>Character Classes: Boolean (set to true or false)</td>
</tr>
<tr>
<td></td>
<td>Length: NA</td>
</tr>
<tr>
<td></td>
<td>Format: NA</td>
</tr>
<tr>
<td></td>
<td>Special Edits: NA</td>
</tr>
<tr>
<td></td>
<td>Default: Set to false</td>
</tr>
<tr>
<td>Group Memberships</td>
<td>From the list, select a group.</td>
</tr>
</tbody>
</table>
## PROCESS AUTHORIZATION

<table>
<thead>
<tr>
<th>Field</th>
<th>Edits</th>
</tr>
</thead>
<tbody>
<tr>
<td>User ID</td>
<td>Required: Yes</td>
</tr>
<tr>
<td></td>
<td>Character Classes: Alphabetic, numeric</td>
</tr>
<tr>
<td></td>
<td>Length: 1-8 characters</td>
</tr>
<tr>
<td></td>
<td>Format: No special requirements</td>
</tr>
<tr>
<td></td>
<td>Special Edits: Must complete a valid lookup against User_M.User_ID.</td>
</tr>
<tr>
<td></td>
<td>Default: The User ID is taken from Edit User screen.</td>
</tr>
<tr>
<td>Process ID</td>
<td>Required: Yes</td>
</tr>
<tr>
<td></td>
<td>Character Classes: Alphabetic, numeric</td>
</tr>
<tr>
<td></td>
<td>Length: 1-8 characters</td>
</tr>
<tr>
<td></td>
<td>Format: No special requirements</td>
</tr>
<tr>
<td></td>
<td>Special Edits: Must complete a valid lookup against Process_M.Process_ID.</td>
</tr>
<tr>
<td></td>
<td>Default: None</td>
</tr>
<tr>
<td>Process Group</td>
<td>Required: Yes</td>
</tr>
<tr>
<td></td>
<td>Character Classes: Numeric (range 0-99)</td>
</tr>
<tr>
<td></td>
<td>Length: 1-2 digits</td>
</tr>
<tr>
<td></td>
<td>Format: No special requirements</td>
</tr>
<tr>
<td></td>
<td>Special Edits: The maximum value that you can type in this field is determined by the value in the Hi Process Group field displayed on the Process Authorization screen. The value in the Process Group field must be less than or equal to the value in the Hi Process Group field plus 1. For example, if the Hi Process Group value is 3, the maximum value you can type in the Process Group field is 4. This prevents blank pages from being created in the user’s process menu.</td>
</tr>
<tr>
<td></td>
<td>Default: 0</td>
</tr>
<tr>
<td>User Access Level</td>
<td>Required: Yes</td>
</tr>
<tr>
<td></td>
<td>Character Classes: Numeric (range 0-4)</td>
</tr>
<tr>
<td></td>
<td>Length: 1 digit</td>
</tr>
<tr>
<td></td>
<td>Format: No special requirements</td>
</tr>
<tr>
<td></td>
<td>Special Edits: None</td>
</tr>
<tr>
<td></td>
<td>Default: 0</td>
</tr>
</tbody>
</table>