NCAA Single-Source Sign-On System Administrator Guide

TABLE OF CONTENTS

GENERAL DESCRIPTION

What is Single-Source Sign-On?

The NCAA Single-Source Sign-On System (SSO) allows a user to access specific NCAA applications, forms and programs through a single login. It also provides the membership control over access privileges to NCAA applications, forms and programs by enabling members to specify which resources a user needs. The SSO system was developed in response to national office and membership concerns about data security and to increase ease of accessing NCAA business applications online through one login and in one centralized location.

How Does a User Access Single-Source Sign-On?

Users of the SSO system must have an individual account (user ID and password) created by the member's SSO administrator. Once a user account is established by the member institution's or conference's SSO administrator, the user may access programs made available to them via the "My Apps" link located on the top right of the homepage of ncaa.org. After logging in, the user will see the applications for which access privileges have been assigned. No additional login is needed to access the assigned applications.

NCAA MY APPS OVERVIEW

My Profile

- Provides access to individual users to update their password.

Tabs

- Tabs allow user to maneuver among different screens.
- The current tabs for the tool administrator(s) include: "Users," "Groups," "My Apps" and "Help."
  Note: Only administrators have access to "Users" and "Groups" tabs.

COMMON FEATURES

How to Log In

1. Go to ncaa.org.
2. Click the **"My Apps"** link found in the upper right hand corner of the page. (see fig. 1)

fig. 1

3. Enter Email and Password (Note: The email must be the email used to set up the account). (see fig. 2)
4. Click the **"Sign in"** button. (see fig. 2)

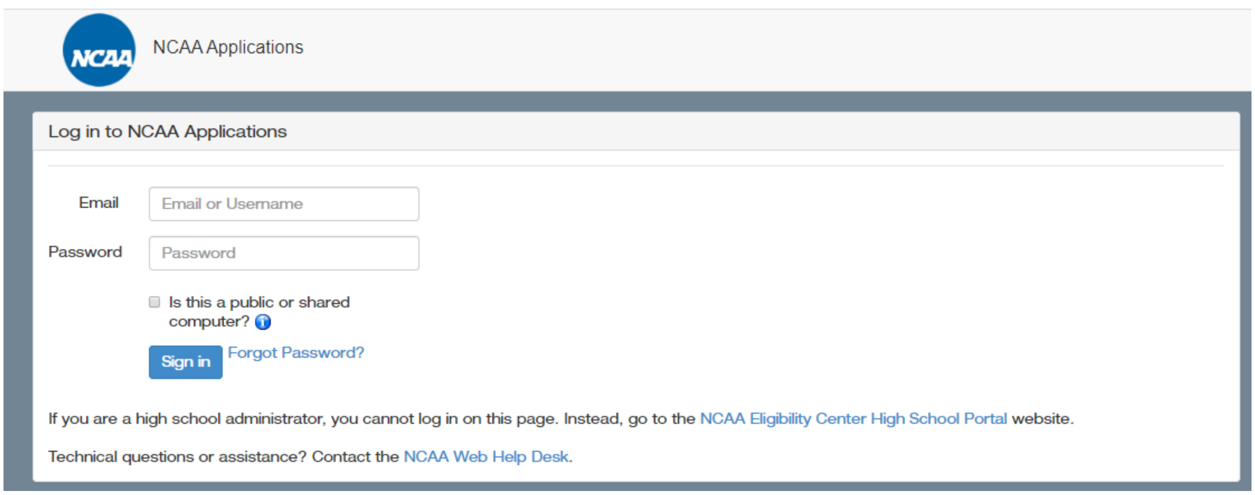


fig. 2

How to Update Passwords

Passwords may be updated either by the user or an SSO administrator.

Password Update by the User

1. Click the **“My Profile”** link in the “Welcome” tab. (see fig. 3)

fig. 3

2. Enter the new password in the data fields Password and Password confirmation. (see fig. 4)
3. Click the **“Submit”** button. (see fig. 4)

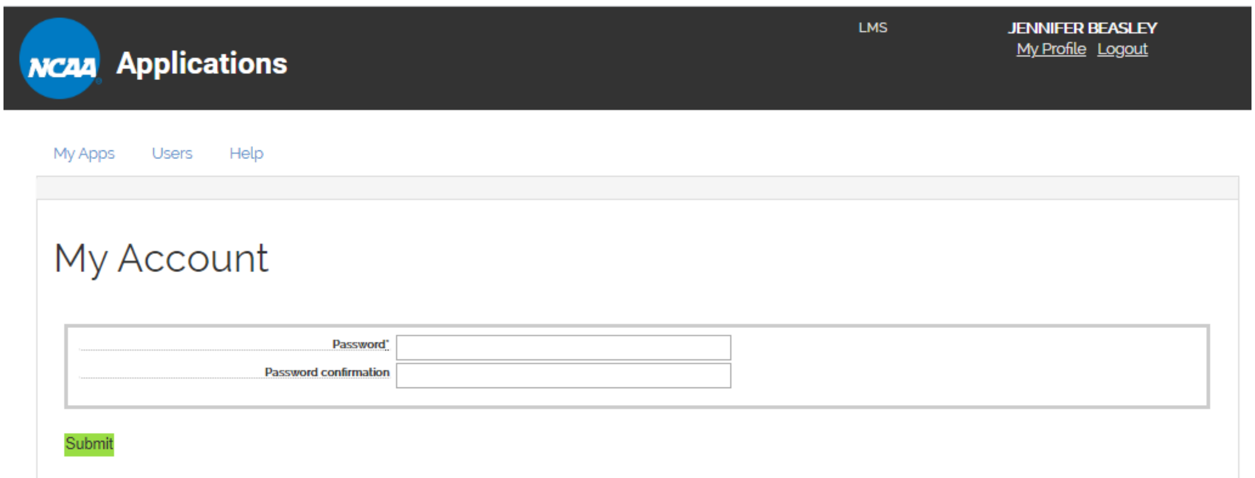


fig. 4

How to Find a Forgotten Password

1. If a password is forgotten, click the **"Forgot Password?"** link. (see fig. 5)

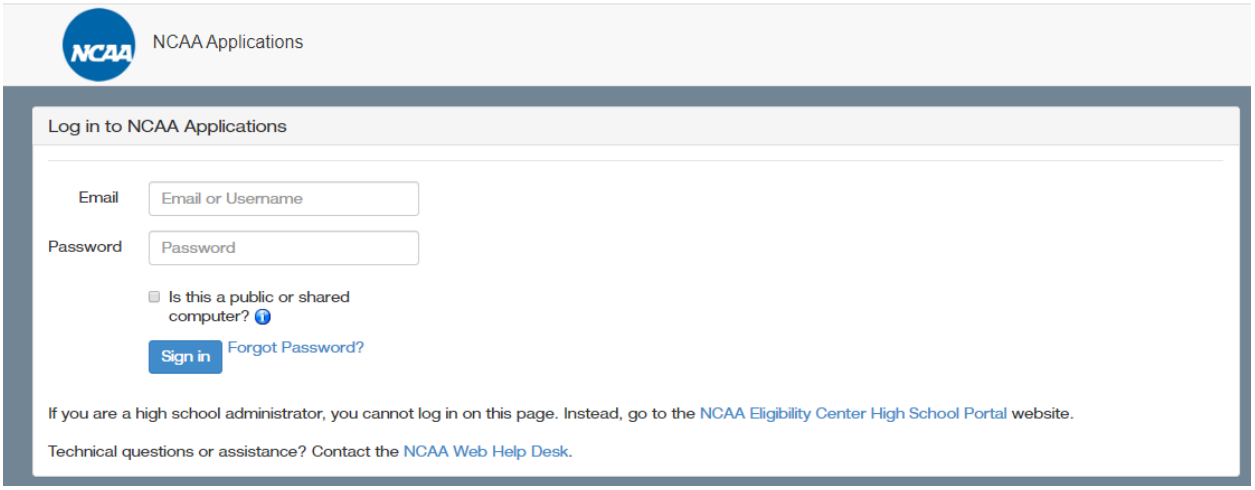


fig. 5

2. A screen will appear in which to enter the user's email address. (see fig. 6)

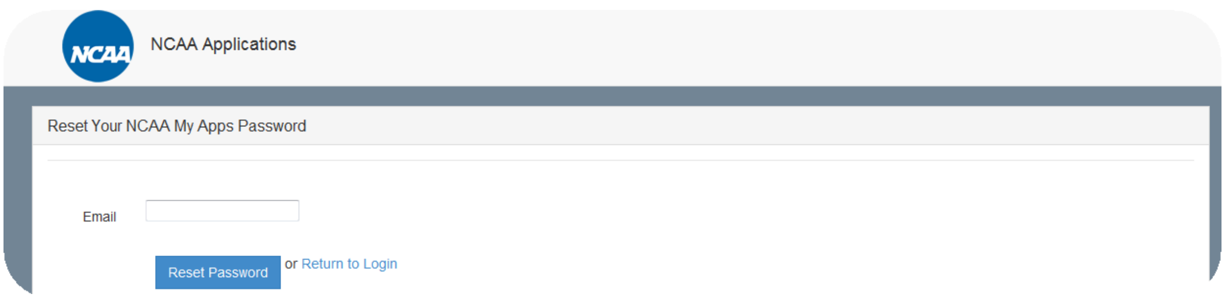


fig. 6

3. Type the email address used to create the account in the Email field and click the **"Reset Password"** button.

An email from nobody@ncaa.org will be sent to the email address entered with a new password.
Note: Users should check their junk email folder if they do not receive an email in their main inbox.

How to Log Out of the System

For data security purposes, it is important for users to log out of the NCAA My Apps/SSO system when all work is complete**. Note:** Closing a specific program does not log a user out of the overall NCAA My Apps/SSO system.

1. Click the **"Log Out"** link found under the user's name on the NCAA My Apps main screen. (see fig. 7)

fig. 7

Tabs

- Tabs allow the user to maneuver among different screens.
- The current tabs for administrators include: "Users," "Groups," "My Applications" and "Help."
- Only administrators will see the "Users" and "Groups" tabs.

MANAGEMENT AND MAINTENANCE

Access Levels

Users and Groups are used to define the applications available and the level of access for each user.

There are different levels of access based on the program or application. Some NCAA applications require a ***Yes*** or ***No*** while others require ***Full Access, Update Only, Read Only*** and ***None***. Still others allow full access to the application simply by being selected. More complete descriptions of these access levels are defined within the Groups Administration and Users Administration areas.

Groups Administration

The “Groups” tab is found at the top of the page. (see fig. 8) SSO administrators should consider using the groups function when establishing accounts for like users with similar responsibilities.

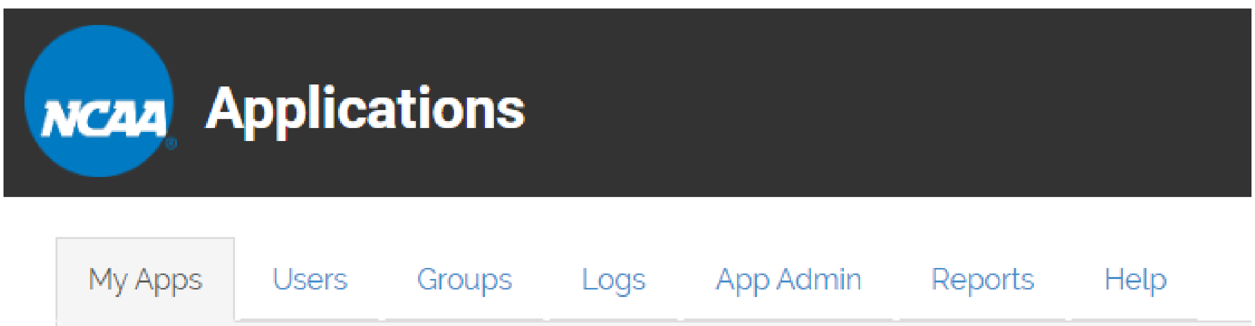


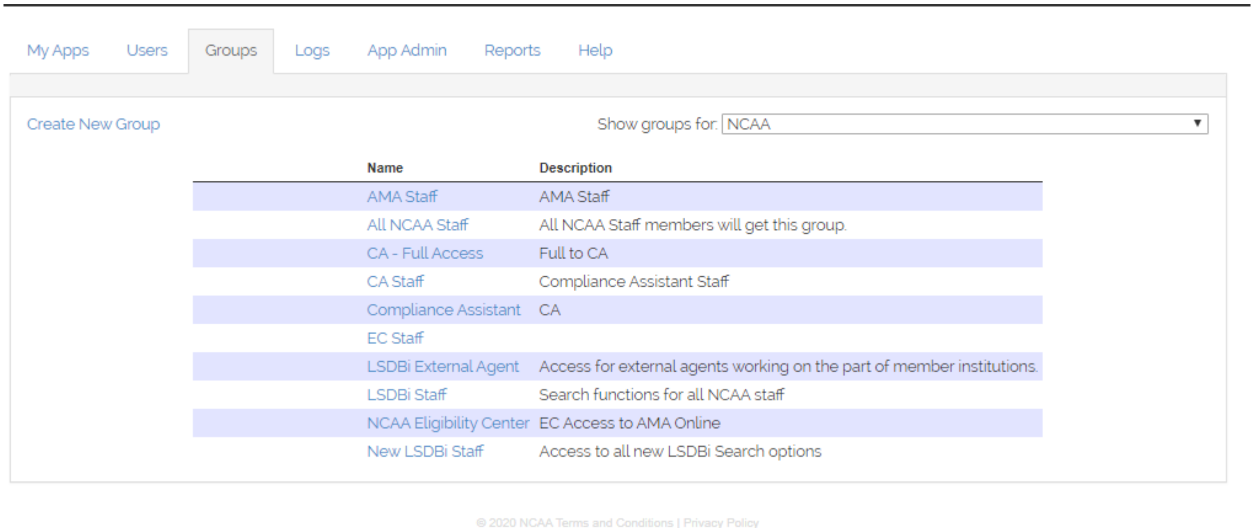
fig. 8

When setting up a group, there are a few things to remember:

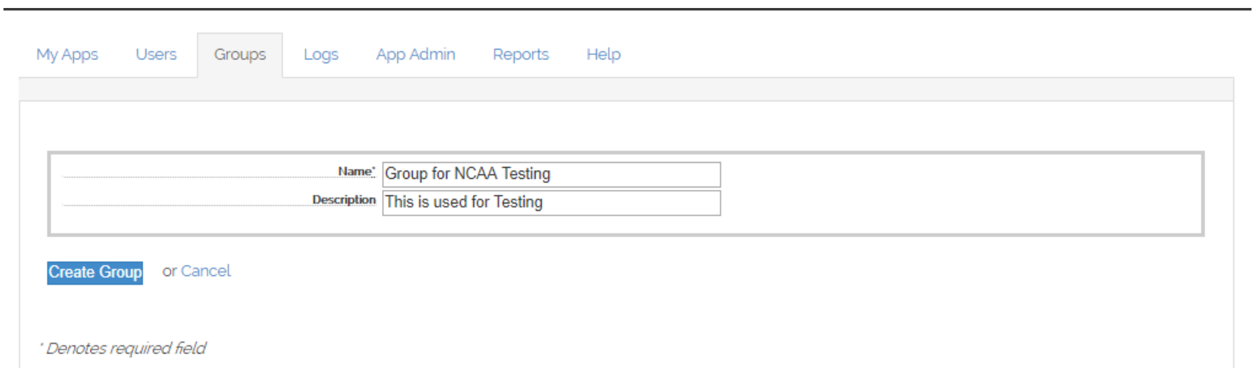
- Setting up groups is NOT required. Users can be given access and privileges individually and do not have to be assigned to a group.
- By selecting the “Groups” tab the system will display all groups created by the administrator.
- The SSO administrators are the only users that have access to the “Groups” tab and its functions.

How to Create a Group

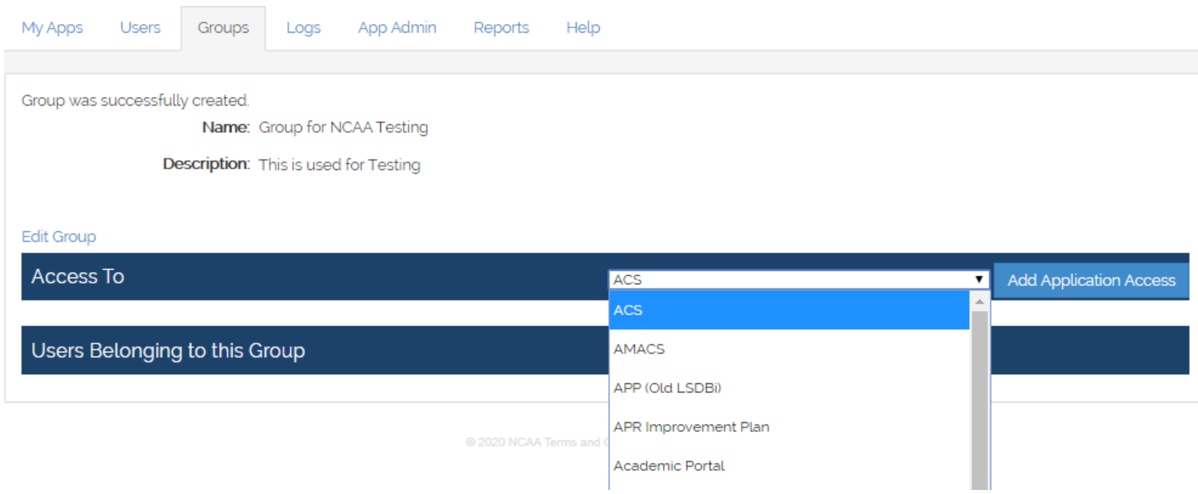
1. Click the “Groups” tab in the navigation bar.
2. A list of groups created by the SSO administrator appears. (**Note:** Administrators who are just starting to create groups may not see any groups in the list.)



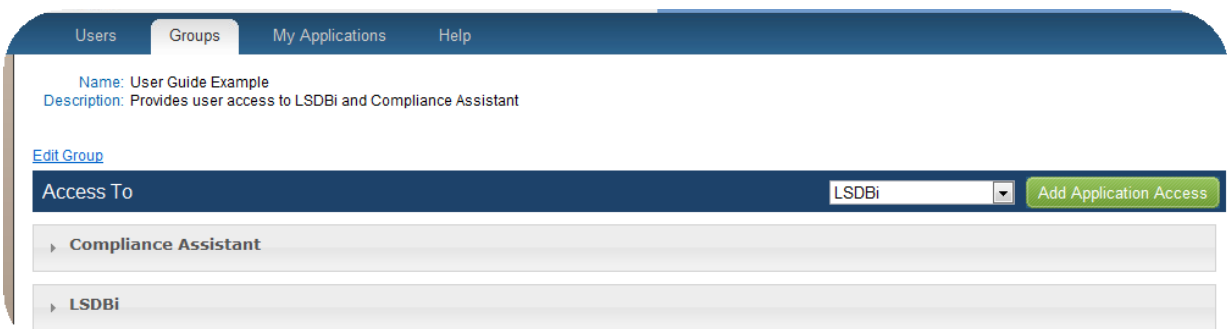
3. Click the “Create a New Group” link found on the left side of the page.
4. Enter a Name for the group (required) and a brief description.
5. Click the **“Create Group”** button.



6. Click the drop-down arrow to see the available applications.
7. Highlight the application to be added to the group via the drop-down menu.

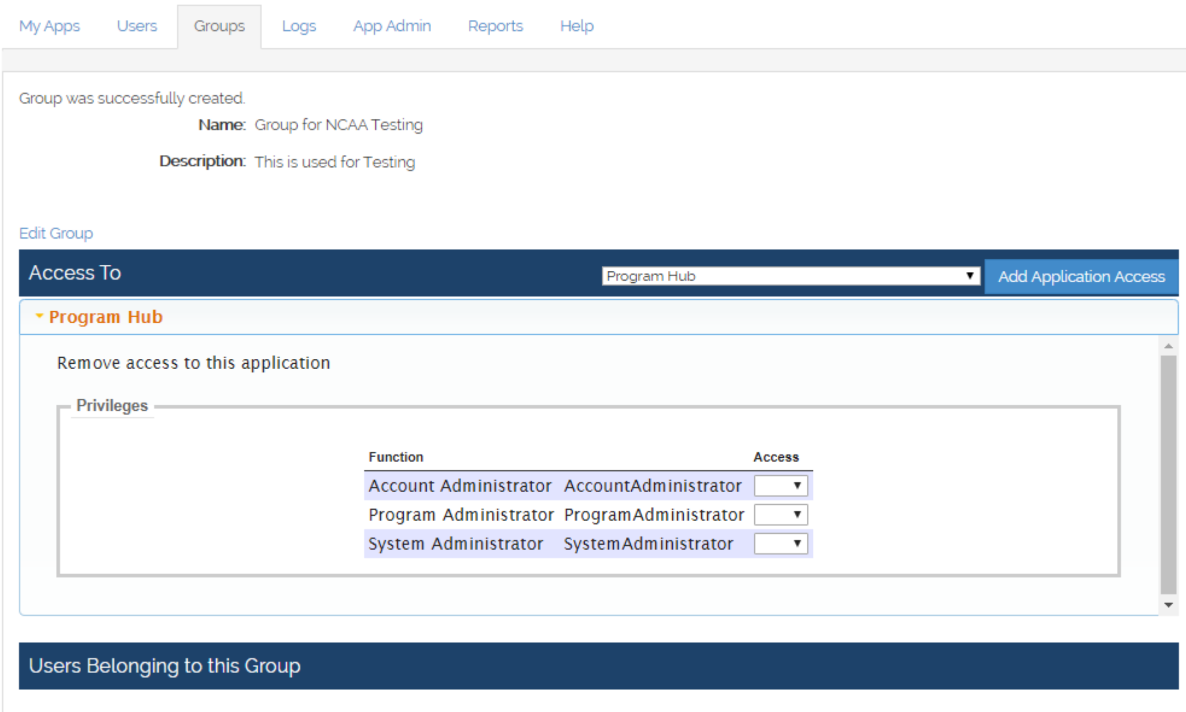


8. Click the **"Add Application Access"** button to add the application to the group.



9. Click the name of the application to define the roles and privileges and access types for each application. The access options are different depending on the application. Generally, the access options are ***Yes*** or ***No***. Others use differing levels of access including: ***Full Access, Update Only, Read Only*** and ***None***.
    a. The ***Yes*** option provides a user complete access to that program or area of the program and allows that user to add, edit, save and delete information.
    b. The ***No*** option would not provide a user any access to that program or area of the program.
    c. The ***Full Access*** option provides a user complete access to that area of the program and allows the user to add, edit, save and delete information.
    d. The ***Update Only*** option allows the user the ability to add, edit and save information.
    e. The ***Read Only*** option allows a user to view information on the screen but restricts the user from adding, deleting or saving information.

f. The ***None*** option causes that screen or area of the program not to be available to a user.



Example

Users assigned to the group in the example above would have access to the Compliance Assistant program and the Legislative Services Database for the Internet (LSDB*i*). They would all be assigned the same privileges and access levels as described by the administrator within each application.

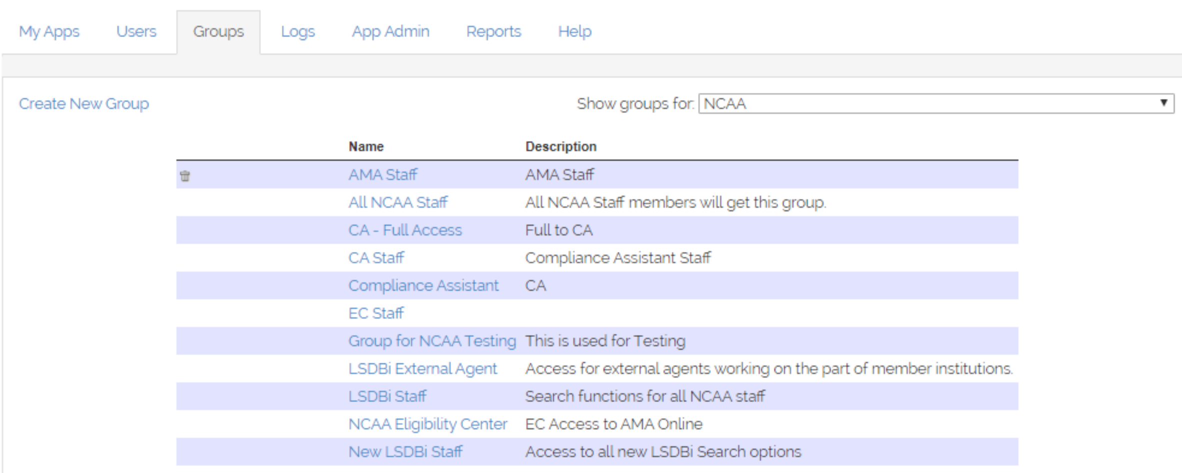
How to Delete an Application from the Group

1. Click the name of the application in the group to be deleted.
2. Click the “Remove access to this application” link.
3. Click the **“OK”** button, indicating that you “are sure you want to remove access to this application.”

How to Delete a Group from the List

1. Hover to the left of the name of the group to be deleted.
2. When the trash can icon appears, click the icon to delete the group.
3. Click the **“OK”** button, indicating that you “are sure you want to remove this group.”

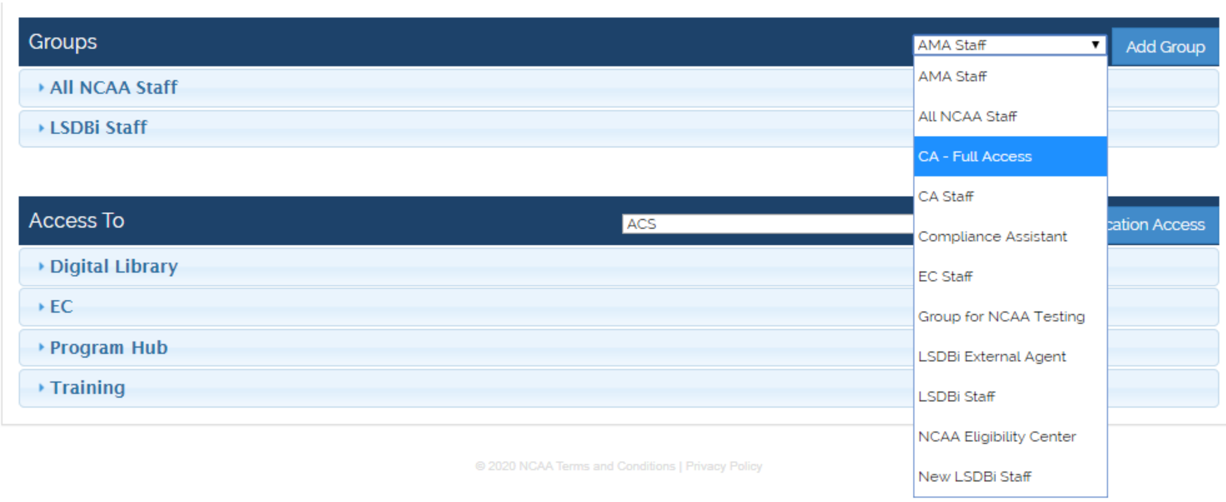
Note: If users were assigned to the deleted group, they no longer will have the access the group provided.



Name	Description
AMA Staff	AMA Staff
All NCAA Staff	All NCAA Staff members will get this group.
CA - Full Access	Full to CA
CA Staff	Compliance Assistant Staff
Compliance Assistant	CA
EC Staff	
Group for NCAA Testing	This is used for Testing
LSDBi External Agent	Access for external agents working on the part of member institutions.
LSDBi Staff	Search functions for all NCAA staff
NCAA Eligibility Center	EC Access to AMA Online
New LSDBi Staff	Access to all new LSDBi Search options

How to Add a Group to a User’s Profile

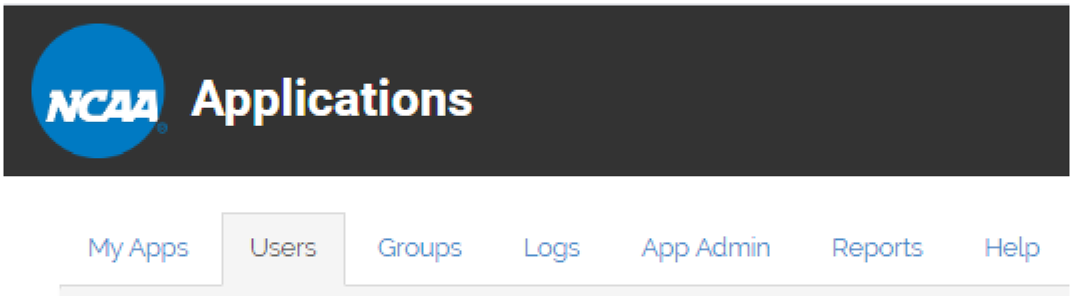
1. Click the “Users” tab in the tool bar.
2. Click the appropriate user’s name in the list.
3. Click the drop-down arrow to see the available groups.
4. Highlight the group to which the user should be assigned.
5. Click the **“Add Group”** button. The user will be granted access and privileges to the programs that were assigned to this group in the Groups Administration section.



How to Delete a Group from a User's Profile

1. Click the "Users" tab in the tool bar.
2. Click the appropriate user's name in the list.
3. Click the name of the group to be removed from the user's profile.
4. After the Group is expanded, the user may be removed from the group by selecting the "Remove Group" link.
5. Click the **"OK"** button, indicating that you "are sure you want to remove this group."

USERS ADMINISTRATION



- The “Users” tab is found at the top of the page.
- By selecting the “Users” tab, the system will display all currently active users.
- It is recommended that two (or more) people on campus be selected to administer the SSO system.
- The SSO administrators are responsible for assigning access and privileges to users on campus.
- Users are directed to the SSO administrators with questions and concerns about the access and privilege assignments.
- The SSO administrators and application administrators are the only users that have access to the “Users” tab and its functions.
- Unless otherwise stated, NCAA applications (e.g., Requests/Self-Reports Online, Compliance Assistant, etc.) were designed and are intended for use by NCAA members. The NCAA provides administrators the ability to determine and assign access to NCAA applications through SSO at prescribed access levels. Administrators should take care to protect data by providing only the access levels needed for each individual that has access to the system. Administrators are ultimately responsible for any access to information that is provided to an unintended user.

How to Add a User to the List

1. Click the “Users” tab in the tool bar.
2. A list of users created by the SSO administrator appears. (Note: New members will include administrators established by the national office.)
3. Click the “Create New User” link found on the left side of the page.
4. Complete the new user’s profile information.
5. The Email, First name, Last name, Password and Active fields are required. Other fields are available for the administrator’s convenience (e.g., title, department, phone number).
    a. To make a user an administrator of the SSO system, which allows the user to create user accounts and assign account privileges, select “Yes” from the drop-down for the field labeled “Administrator.” The users marked as an Administrator can be identified in the user list screen with a “true” in the “Administrator?” column.

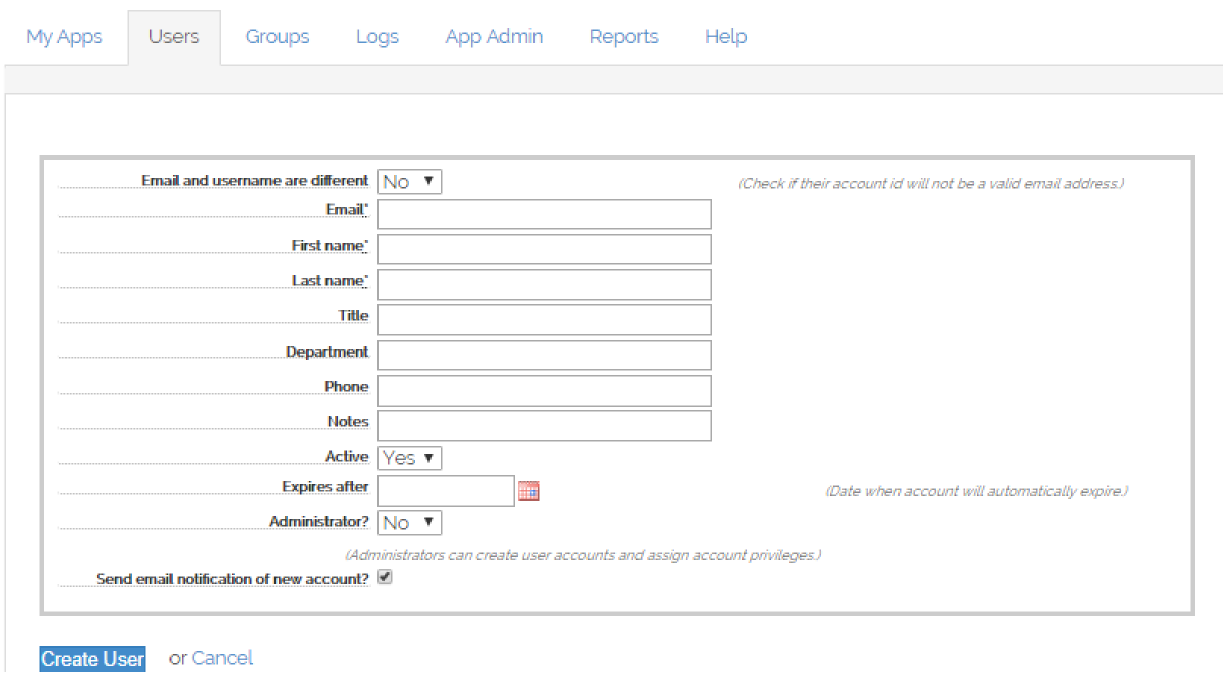
    b. Two email notifications are sent to the new user created when the check box labeled “Send email notification of new account” is selected.

Account username email:
You have been setup with an NCAA Business Applications Member Access Account by <%= @admin_user %>. Your username is <%= @user.email %>.

Account password email:
You have been setup with an NCAA Business Applications Member Access Account by <%= @admin_user %>. Your password is <%= @user.plain_password %>.

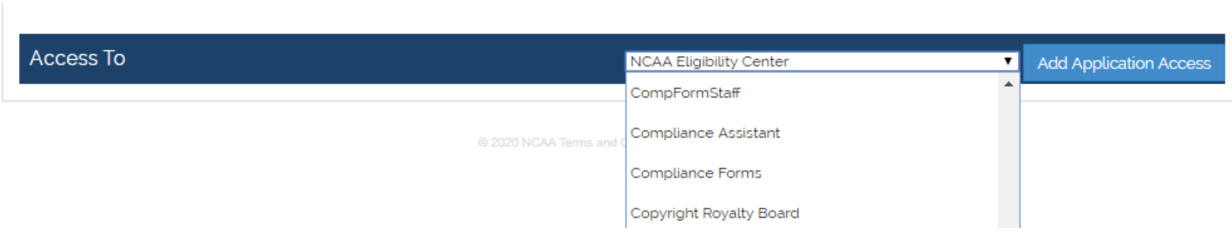
Note: Users have the ability to change their password (see the Password section of this user guide).

6. Click the **"Create User"** button to save the new user information.



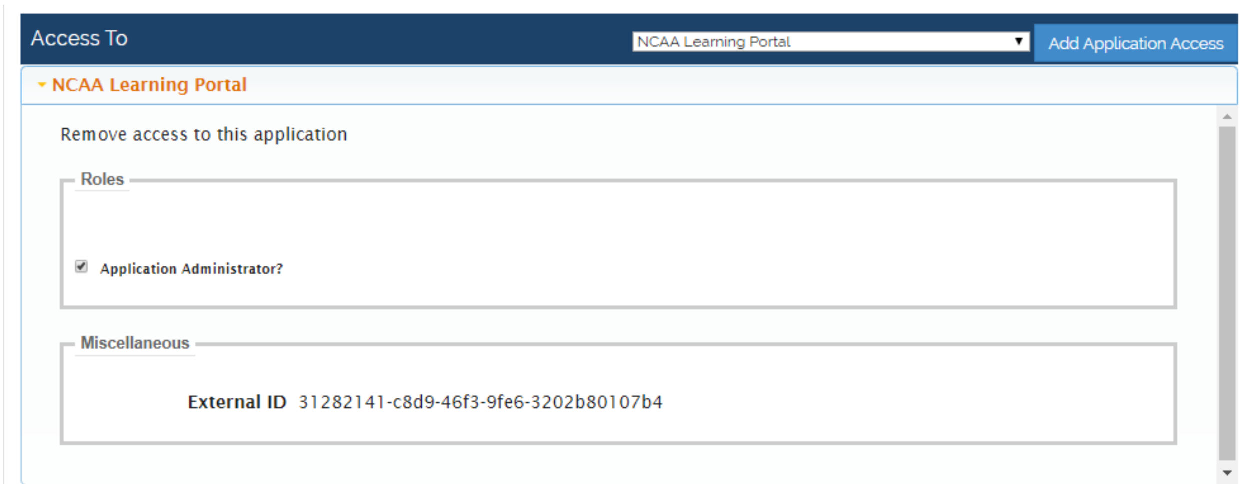
How to Add Access to a Specific Application

1. Click the "Users" tab in the tool bar.
2. Click the appropriate user's name in the list.
3. Click the drop-down arrow in the "Access To" tool bar to see the available applications.
4. Highlight the application to which the user should have access.
5. Click the **"Add Application Access"** button.



6. Once the application appears under the “Access To” tool bar, assign appropriate roles and privileges.

    a. To assign the role of Application Administrator, click the check box which allows the user to assign other users and privileges to that specific program. **Note:** An Application Administrator does not have access to create a group.



    b. Assign appropriate privileges to users, to allow or restrict access to perform their specified job functions. Generally, the access options are ***Group Default*** or ***None, Yes*** or ***No.*** Others use differing levels of access including: ***Full Access, Update Only, Read Only*** and ***None.***

    The ***Group Default*** or ***None*** option provides a user the access level allowed by the group the user is assigned to, or no access if the user is not assigned to a group that provides any access.

    1) The ***Yes*** option provides a user complete access to that program or area of the program and allows that user to add, edit, save and delete information.

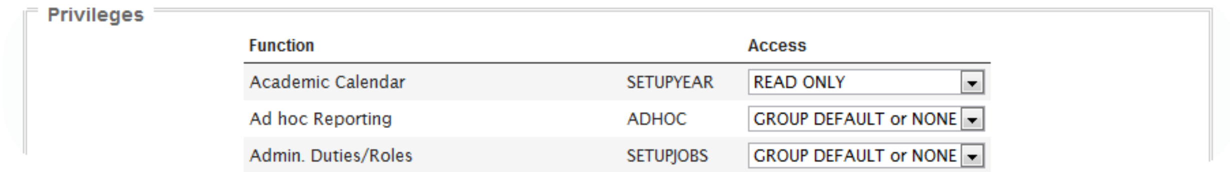
    2) The ***No*** option would not provide a user any access to that area of the program.

    3) The ***Full Access*** option provides a user complete access to that area of the program and allows the user to add, edit, save and delete information.

    4) The ***Update Only*** option allows the user the ability to add, edit and save information.

5) The ***Read Only*** option allows a user to view information on the screen but restricts the user from adding, deleting or saving information.

6) The ***None*** option causes that screen or area of the program not to be available to a user.



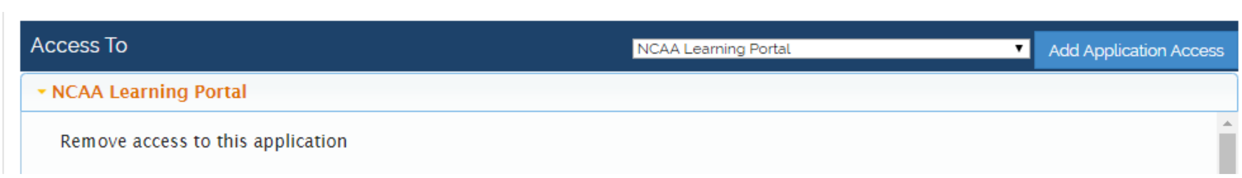
How to Change Assigned Access and Privileges for a Specific User

1. Click the "Users" tab in the tool bar.
2. Click the appropriate user's name in the list.
3. Click the name of the application for which access or privileges needs to be adjusted.
4. Select the drop-down arrow next to the access levels to see the available levels to be assigned.
5. Highlight and click the appropriate access level for the user for each function.

   a. Access assigned at the individual level will be more restrictive than access provided at the group level. For example, if ***Full Access*** is granted at the group level, but ***Read Only*** is granted for the same function at the user level, the user will have ***Read Only*** access.
   Note: There is no save button or confirmation message when changing access levels. As the user makes a selection the level is changed.

How to Delete Access to a Particular Application

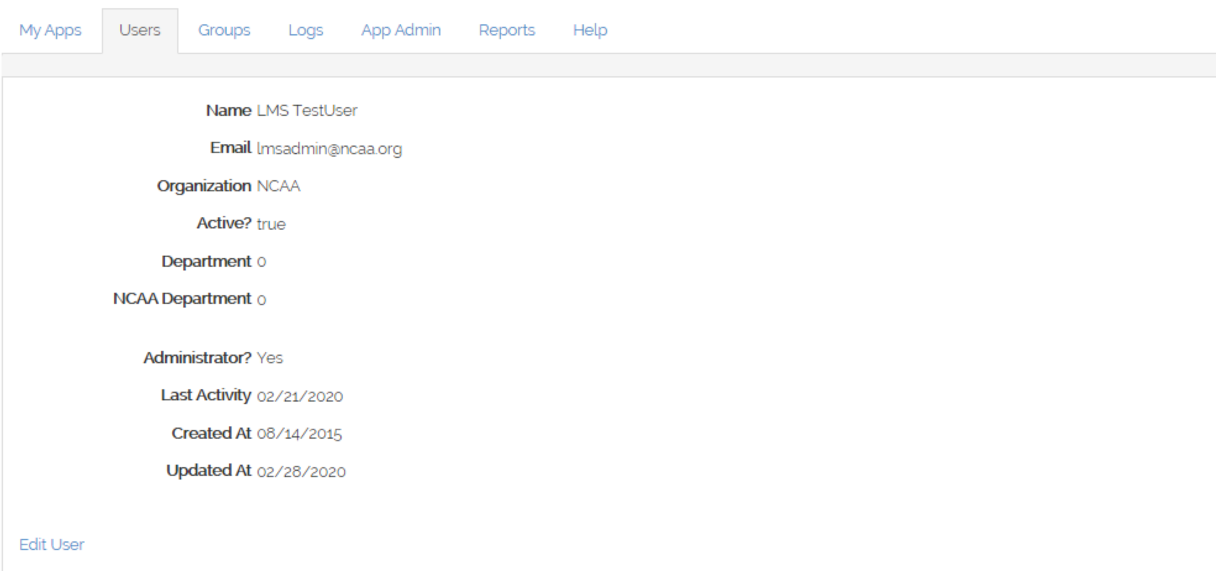
1. Click the "Users" tab in the tool bar.
2. Select the appropriate user's name from the list.
3. Click the name of the application to be removed from the user profile.
4. After the program has expanded, the user may remove the application by selecting the "Remove access to this application" link.



5. Click the **"OK"** button, indicating that you are sure "you want to remove access to this application."

How to Edit User Profile Information

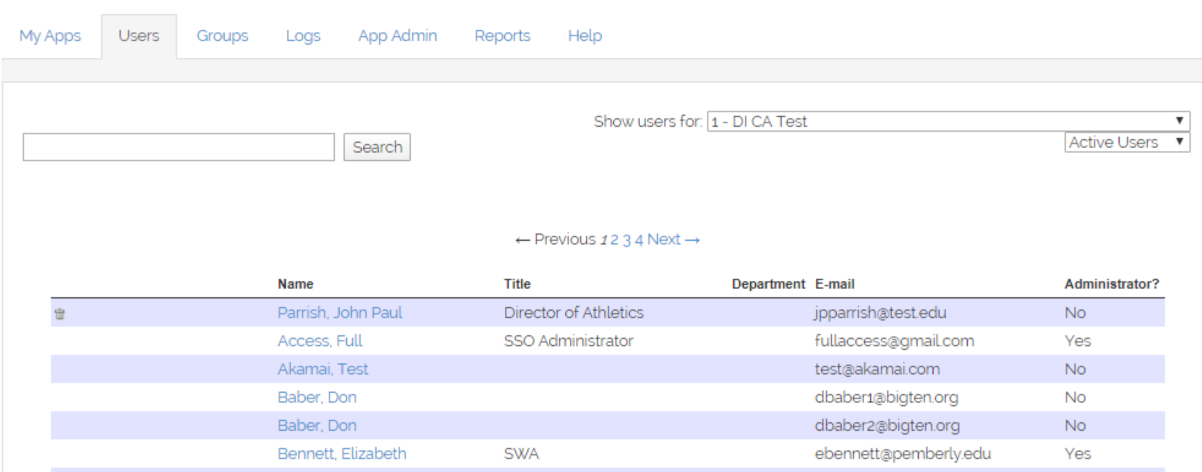
1. Click the “Users” tab in the tool bar.
2. Select the appropriate user’s name from the list.
3. Click the “Edit User” link for access to the previously saved profile information.



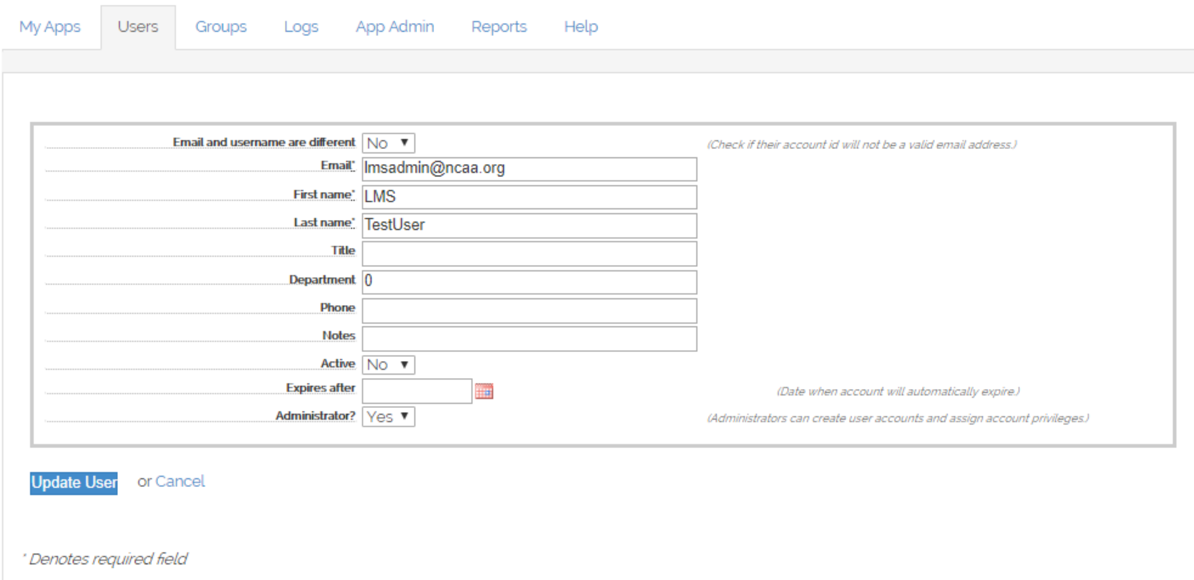
4. Make the necessary edits to the user’s profile.
5. Click the **“Update User”** button.

How to Remove a User from the Active Users List

1. Hover to the left of the name of the user to be removed from the list.
2. When the trash can icon appears, click the icon to remove the user from the list.



3. Click the **“OK”** button, indicating you “are sure you want to deactivate this user” or select “No” from the “Active” drop-down box in the User profile area.



This action removes the user from the active user list and marks the user as inactive. Administrators should promptly deactivate those users that have separated from employment to safeguard against access to information by an unintended user.

ADDITIONAL INFORMATION

System Security

The system security, or authentication, that takes place when a user logs into the system is designed for security purposes. User information is not to be shared. Users have been given appropriate access levels and privileges by the administrators of the system. It is important to note that users should understand the importance of logging out of the authentication system to protect the integrity of all NCAA business applications, forms and programs using the SSO system.

Unless otherwise stated, NCAA applications (e.g., Requests/Self-Reports Online, Compliance Assistant, etc.) were designed and are intended for use by NCAA members. The NCAA provides administrators the ability to determine and assign access to NCAA applications through SSO at prescribed access levels. Administrators should take care to protect data by providing only the access levels needed for each individual that has access to the system. Administrators are ultimately responsible for any access to information that is provided to an unintended user.

Help

Additional support and assistance can be reached at webhelpdesk@ncaa.org.

APPENDIX

Single-Source Sign-On System – The system in which a user is able to log in for access to all NCAA business applications, forms and programs necessary to perform the user's job functions.

NCAA Applications Account Maintenance Tool – The tool used by the membership to assign NCAA applications, forms and programs access and privileges to users and groups at appropriate levels.

My Apps Link – The link located on the top right of the homepage of ncaa.org that provides direct access to the login for NCAA business applications through the NCAA Applications Account Maintenance Tool.

Single-Source Sign-On Administrator – The person(s) designated by the institution to manage the users and group functions at the membership level.

Application Administrator – The person(s) designated by the SSO administrator to manage the users assigned to a specific application.