**Ascender Security Administration**



Introduction

Ascender Security Administration is intended to be used by those designated as database administrator(s). Through this system, roles are created (Business Manager, Nurse, Principal, etc…), then assigned to users. Roles include campuses and pay frequencies where applicable, along with applications (Attendance, Finance, Requisition, etc…). It is through Security Administration that usernames and passwords are created, and permissions are granted to applications, menus, and tabs.

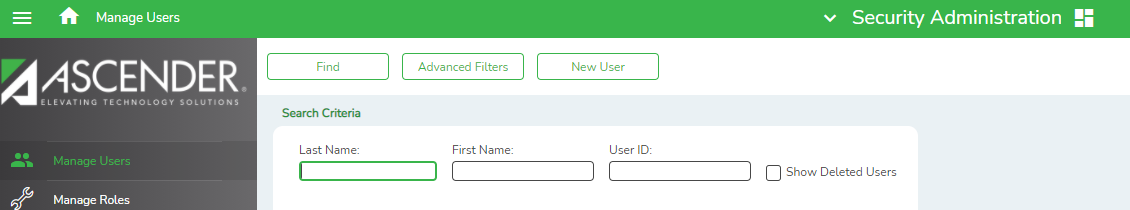
**Features**

The following features are provided by the Security Administration application.

* **Managing Roles**
  + Allows you to create new roles.
  + Allows you to modify permissions to applications for each role.
* **Managing Users**
  + Allows you to add users to the application.
  + Allows you to assign and manage existing roles for users.
  + Allows you to assign campuses and/or pay frequencies as needed.
  + Produces a list of users based on selection criteria.
* **Generating Reports**
  + Allows you to generate a report of users by permissions.
  + Allows you to generate a report of tasks associated with roles.

Main Menu

The Security Administration Main Menu includes the current application version; options to change to a different application, exit the current application, online help, and other menu options in the Security Administration application. A session timer ensures users will be automatically logged out after 60 minutes of inactivity.



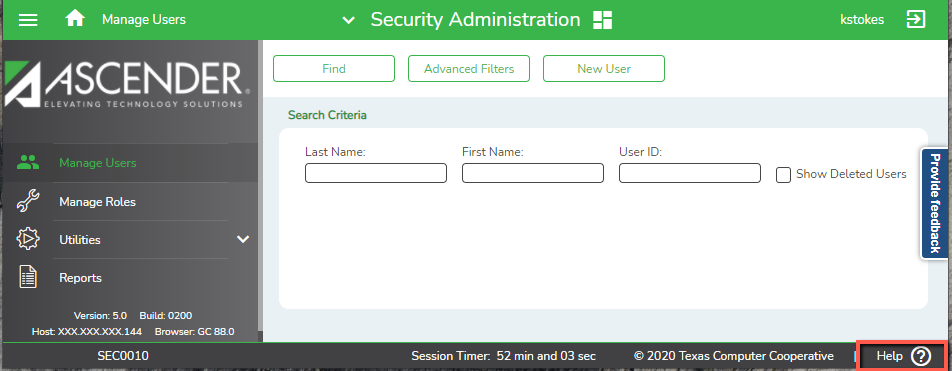
**Online Help**

The Ascender Security Administration application changes to meet ongoing needs. With every

system change that occurs, the online Help system is updated to reflect the change. Click Help in the lower-right hand corner of the application page at any time for information about the

individual fields on the pages. This ensures that you will be accessing the most up-to-date

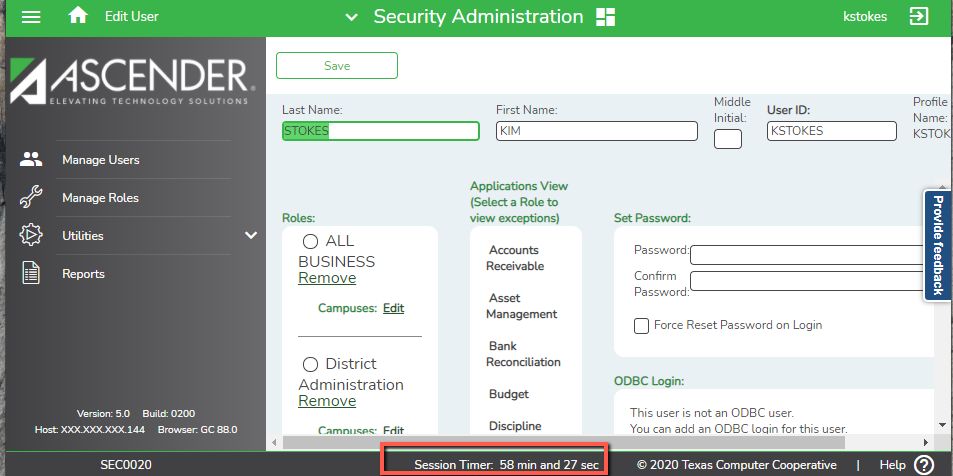
information for every field in the application.



# Session Timer

On each application page, along the bottom, a session time displays. Each time the user performs an action that makes a call back to the database, the timer resets. The session timer is automatically set to 60 minutes. The time counts down to 00 minutes before automatically logging the user out. A warning message displays at the two-minute mark.

* If you want to extend the session for another 30 minutes, click save
* After the 2 minute warning, if you do not click save, the application session automatically times out due to inactivity. Following a session timeout, the user will be returned to the main landing page of the application where the time out occurred. Any unsaved changes will be lost.

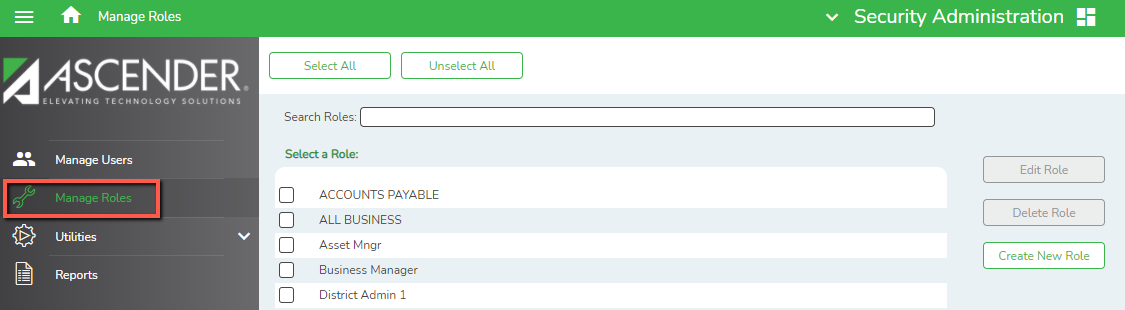


**Maintenance Functions**

The Security Administration application creates roles and users, then assigns users to the roles. Maintenance functions also include adding permissions within applications.

# Manage Roles

When you log on to the Security Administration application, the Security Administration page is displayed with Manage Users as the default tab. Click the Manage Roles on the left-hand side. The Manage Roles page is displayed.

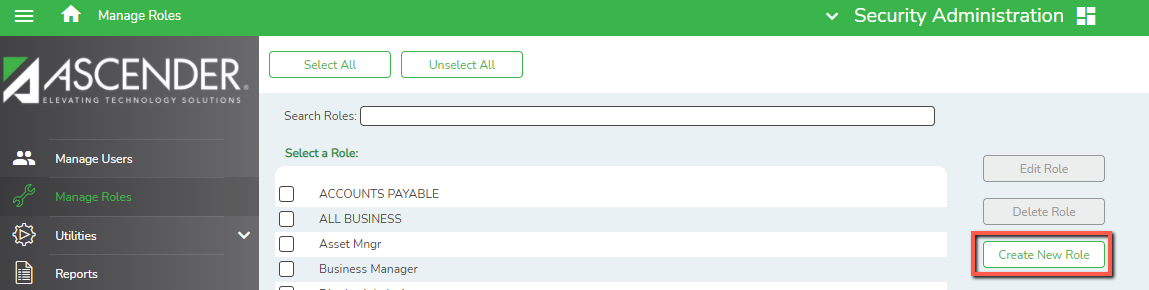


The Manage Roles tab is used to add, modify, or delete roles as needed. Roles allow users with similar duties to easily receive the same or similar permissions. For example, by creating a role for Principals and assigning permissions normally needed by someone in that role, multiple users can quickly be assigned to those permissions by simply assigning them to that role. Removing or editing permissions can be just as easily managed as the user’s responsibilities change. Users may be assigned more than one role as needed, however care must be taken to ensure no conflicts between roles exists. For example, if a user is assigned Role A that allows the user access to create TSDS Interchange files and Role B that gives the user access to State Reporting (TSDS) but Role B indicates the user cannot create those interchanges, a conflict exists.

In the Manage Roles tab, a list of existing roles is displayed. From this screen, roles can be created, edited or deleted.

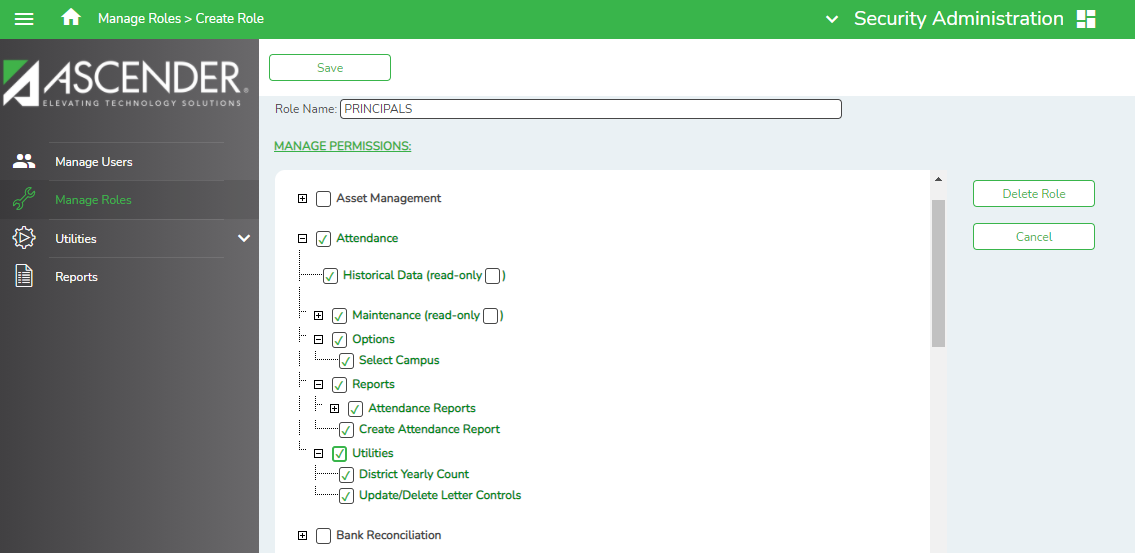
**Create New Roles**

To create a new role, click Create New Role. The Create Role page is displayed.



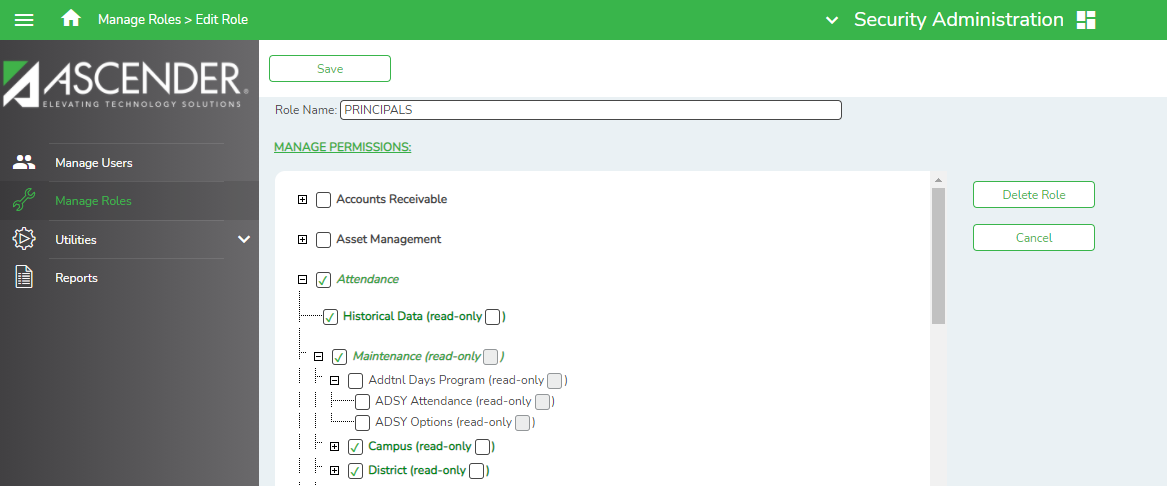
In the Role Name field, enter the name of the role you are creating. The field holds a maximum of 100 characters. (If you do not wish to assign permissions to the new role at this time, click Save to save the new role. You may add the permissions later through Edit.)

Assign permissions to applications, menus and tabs for the new role. Click the plus and minus boxes to expand or collapse submenus and view all components within each application. When available, Read Only Access may be given by selecting the Read Only box.



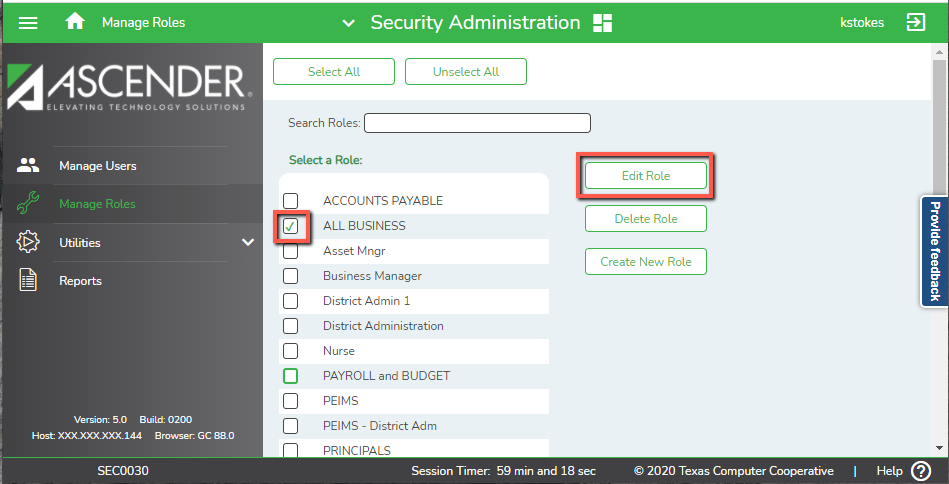
Once the appropriate permissions have been selected, click Save. The lists collapse to show only the highest level of each application.

* For any box selected, the title is displayed in green.
* For any level that has a sublevel that has not been selected, the upper-level title is displayed in green italics. For instance, our example below shows Principal has many sublevels, some of which have not been selected. Maintenance will appear in italics denoting that not everything beneath it has been granted permission for this role.
* Read Only permissions –
* **Note: Read Only permissions may prevent users from being able to select certain options on the screens. Contact Region 14 consultants for additional guidance when assigning Read Only permissions if needed.**



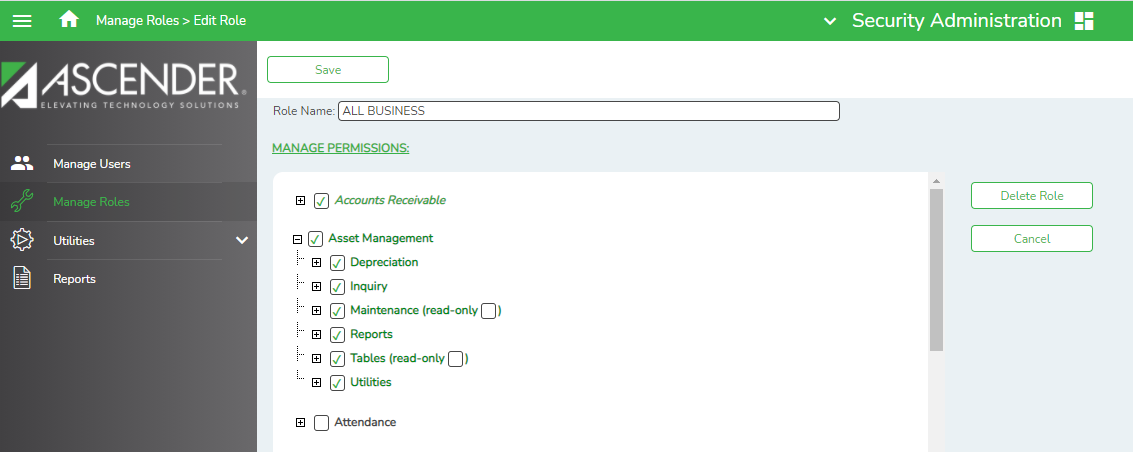
**Edit Roles**

To edit an existing role, select the role for which you wish to make changes in the Manage Roles tab and click on Edit Role



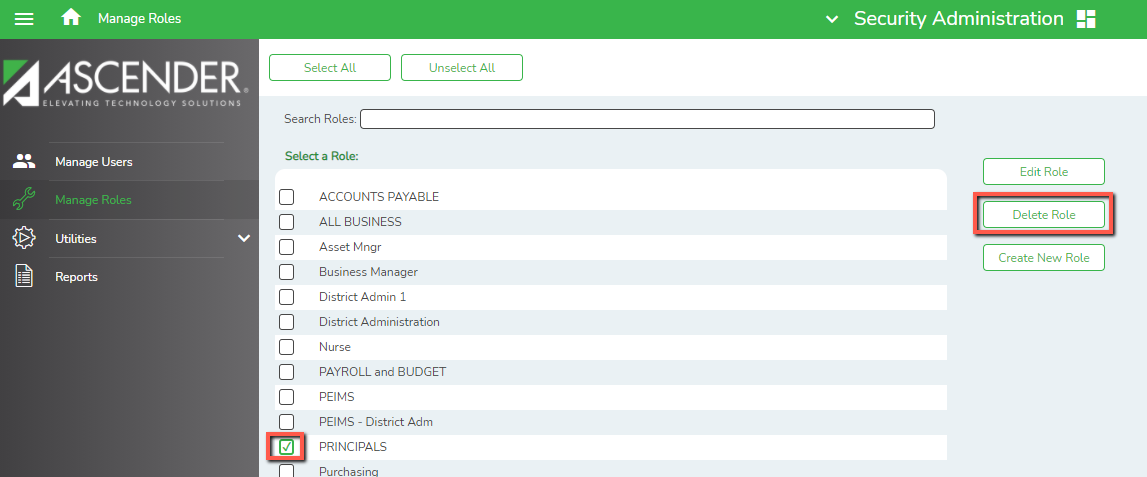
The Edit Role page is displayed, displaying a list of applications. Just as when creating, any application that has been selected displays the title in green. For any level that has a sublevel that has not been selected, the upper-level title is displayed in green italics. Select each application to grant or deny permissions, and then click Save.

**Note: Changes made at the role level will be applied to all users assigned to that role once Save is clicked.**



## Delete Roles

To delete an existing role, select the role you wish to delete in the Manage Roles tab and click on Delete.

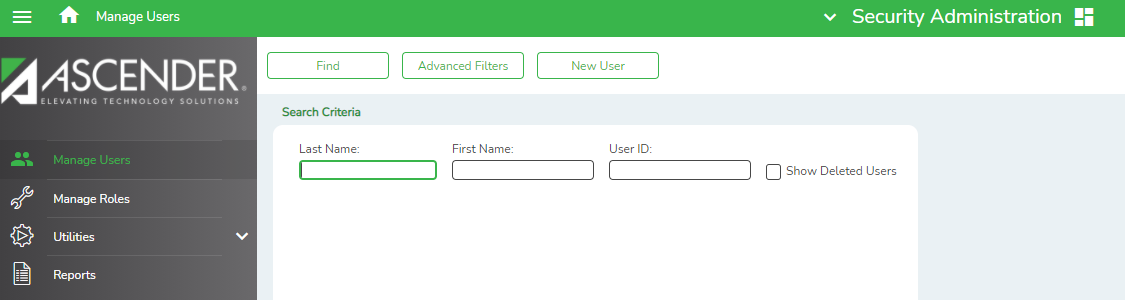


A dialog box asks if you are sure you want to delete the role. Click OK to delete the role.

**Note: Any user assigned to that role will lose those permissions once OK is selected.**

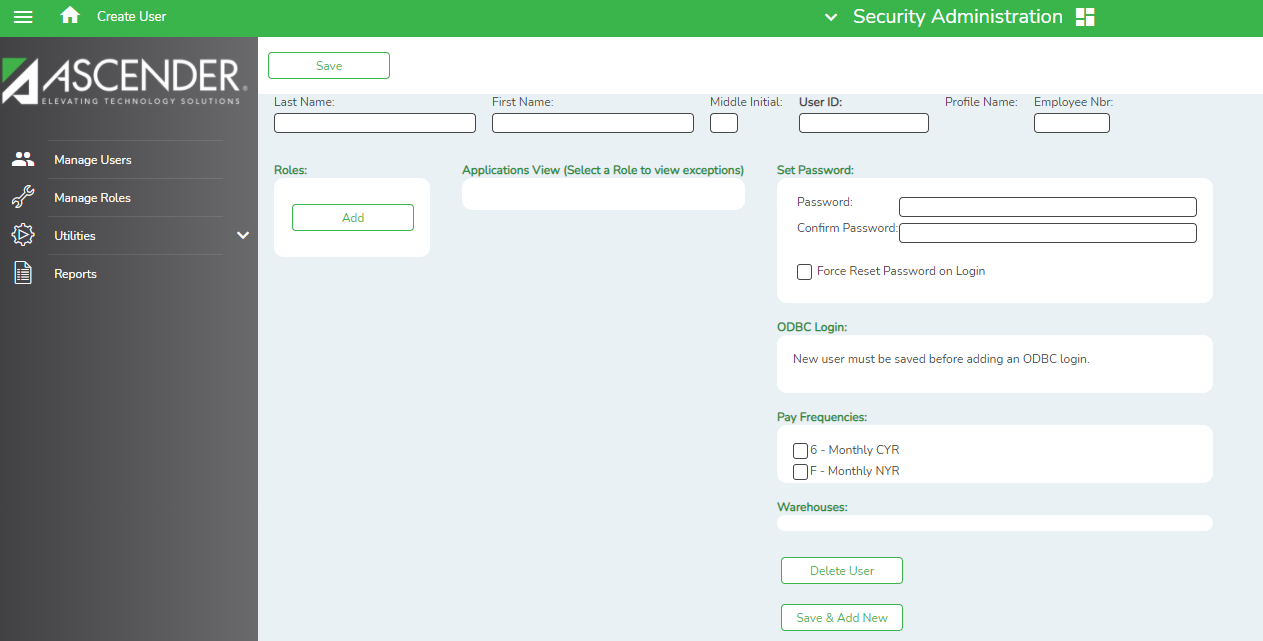
**Manage Users**

The Manage Users tab is used to create users and attribute the roles and permissions associated with each user. For each user, you can establish the role(s) he will play in addition to the campuses to which he will have access if appropriate. After creating or editing users or roles, users must log out and back into Ascender to refresh security permissions.



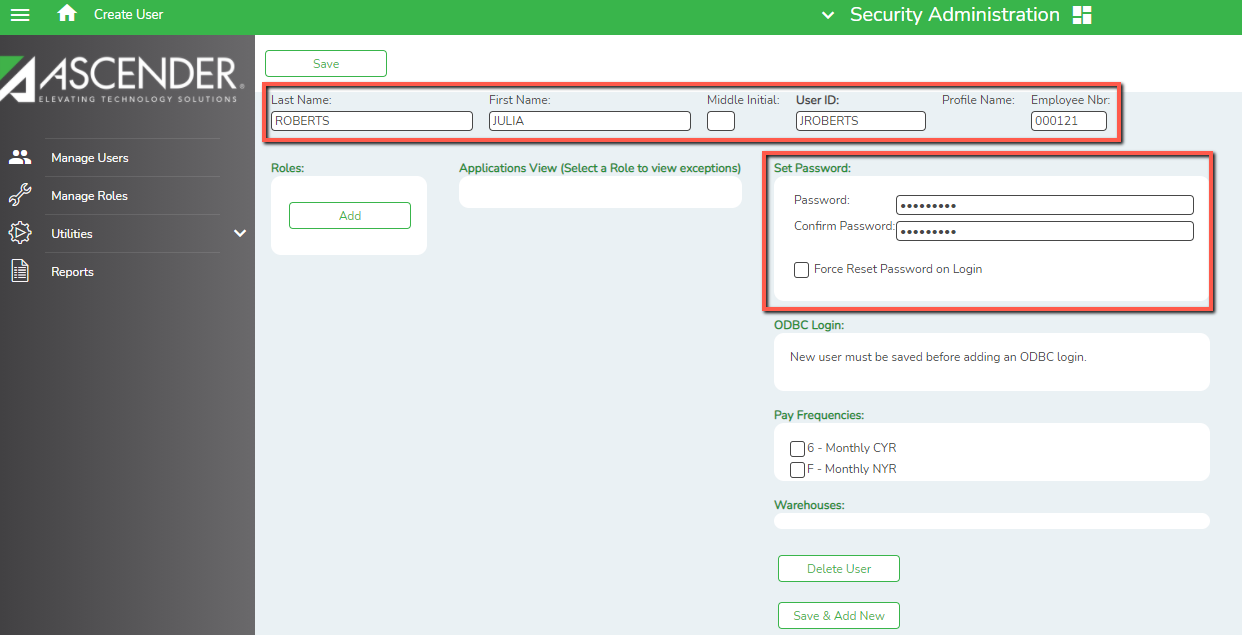
To Add a New User

When you log on to the Security Administration application, the Security Administration page is displayed with Manage Users as the default tab. Click New User to add the new user. The Edit User page is displayed.



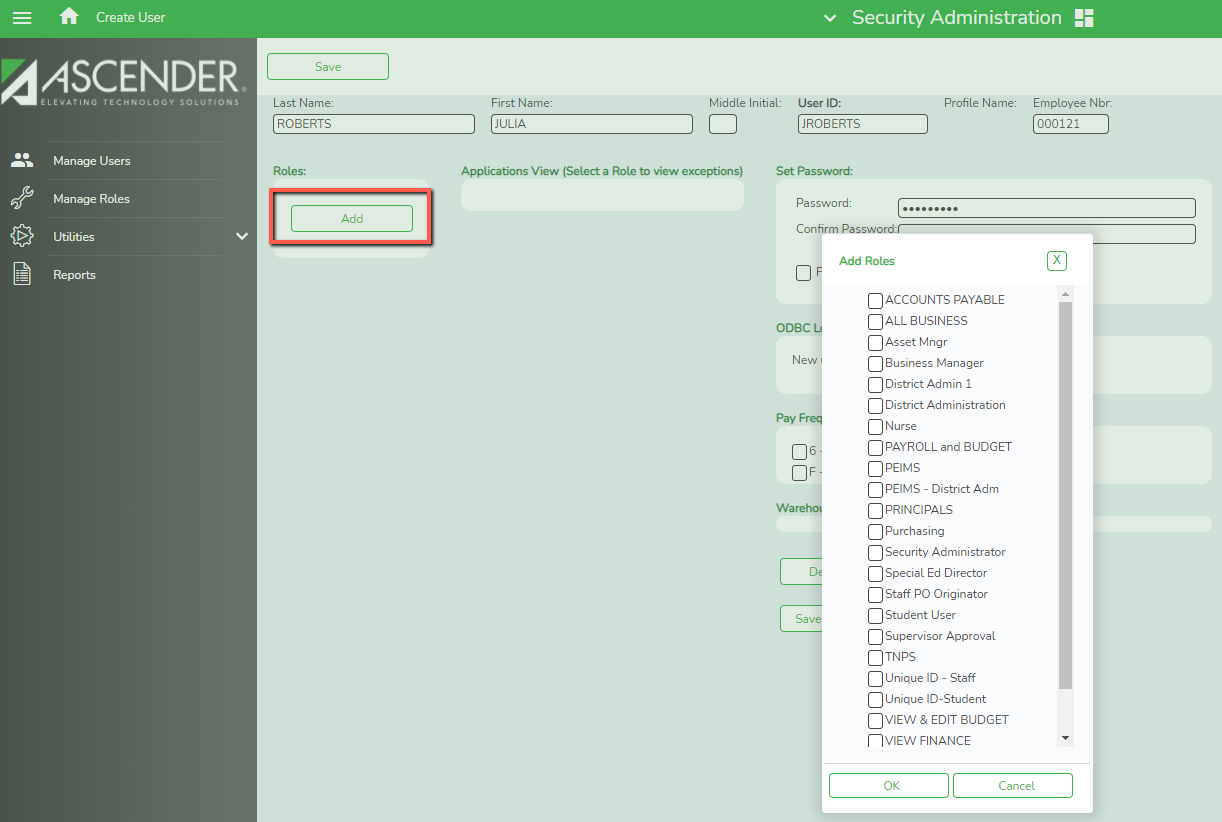
Enter the following and Save:

* Last Name (maximum of 30 characters)
* First Name (maximum of 30 characters)
* Middle Initial (optional)
* User ID (maximum of 29 characters)
* Employee number assigned in Human Resources
* Password (must be entered twice to confirm)
  + Passwords must be 8-12 characters and contain at least one upper case letter, one lower case letter, one special character, and one number.
  + Users will be prompted to change their password every 90 days. The system holds the two prior passwords in its memory so be prepared to choose a password that is different from the current plus the past two.
  + Users who forget their password must contact an Ascender Security User at their district to have their password reset. Three incorrect attempts at a password will lock the user out of the system for 15 minutes. After the 15 minutes are up, users may attempt their password again or contact their district’s Ascender Security user.
  + You may force the user to reset their password when they logon, rather than continuing to use the temporary password you assign at this time.



**To Grant Permissions to New Users**

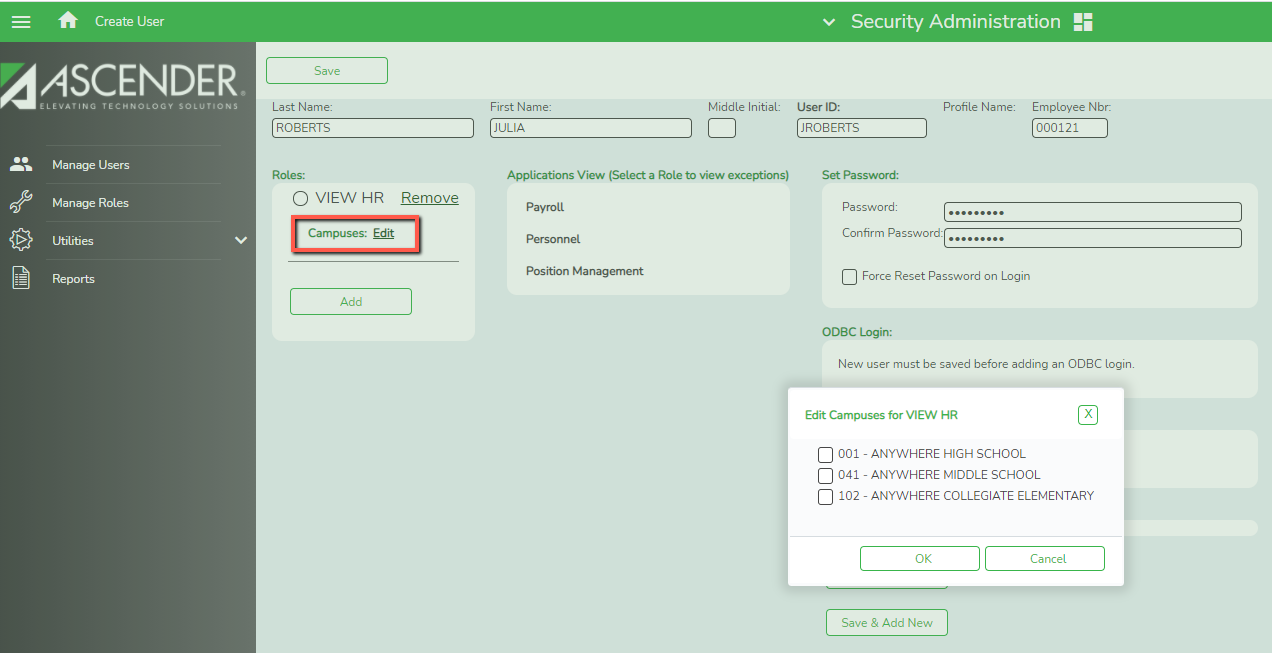
Once you have created a user, you may add role(s). In the **Roles** box, click **Add**. The Add Role dialog box displays existing roles from which to choose. You may need to scroll to view all roles.



Select each role to assign it to the user, and then click **OK**. **Save** your selections.

If campus assignment is required for the role, select **Edit** to the right of **Campuses**. The Select Campuses dialog box is displayed with existing campuses from which to choose.

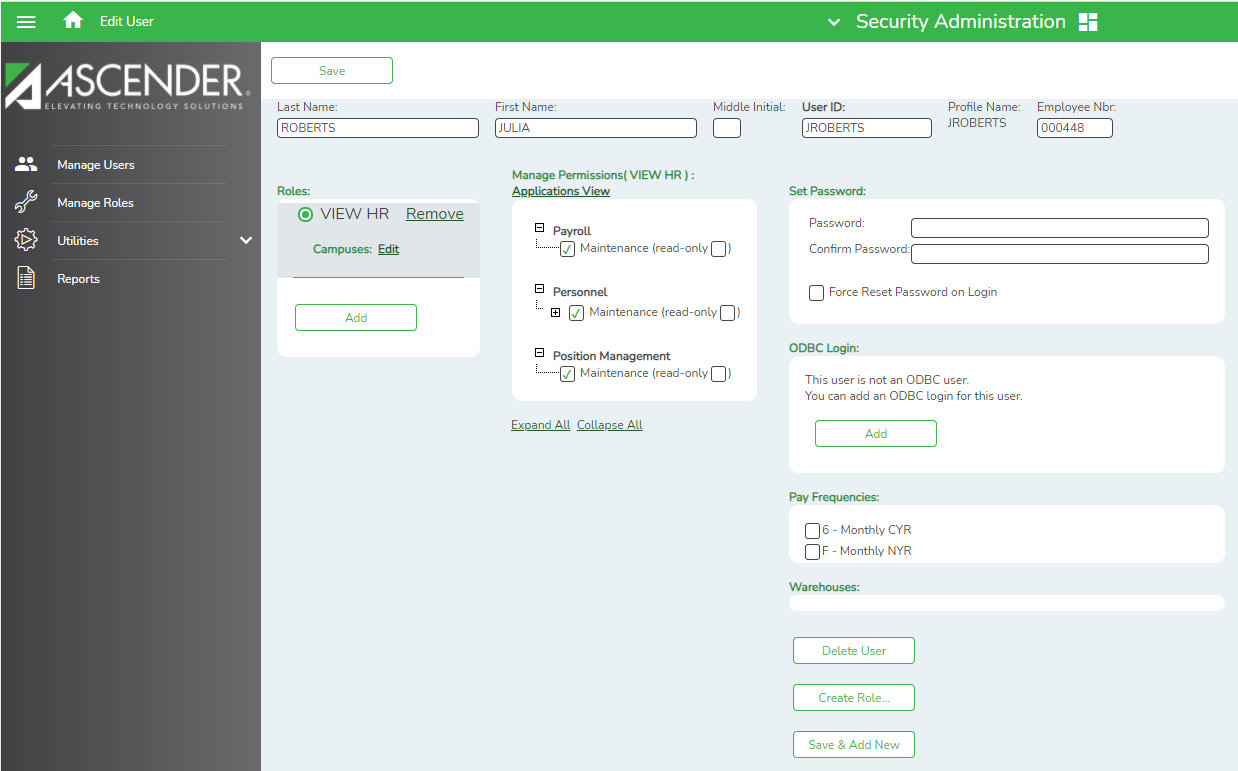
**Note: Campuses are not assigned to Business Roles.**



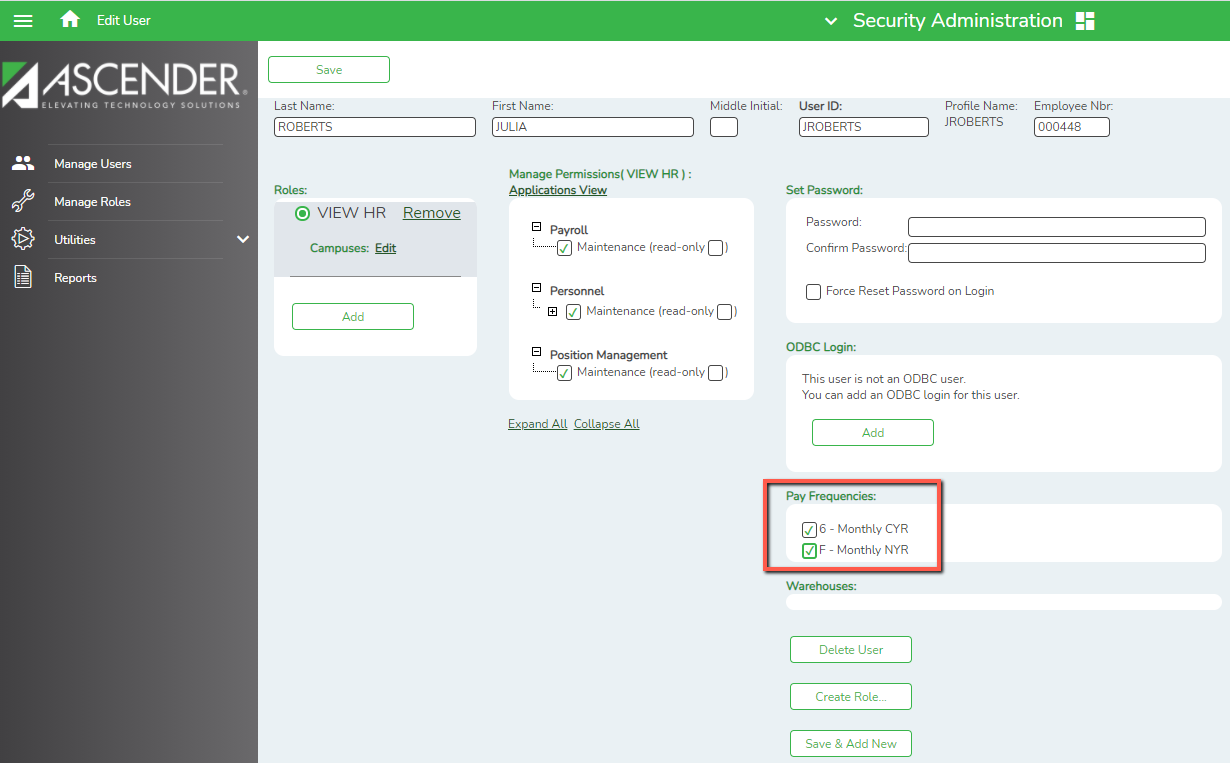
To update permissions assigned through the role(s), select the radio button for the desired role. The Applications view in the center of the screen will change to the **Manage Permissions** view. By default, permission is granted to all components as established by the role.

Click **Expand All** to show all lower-level pages available, or use the plus box to expand individual sections.

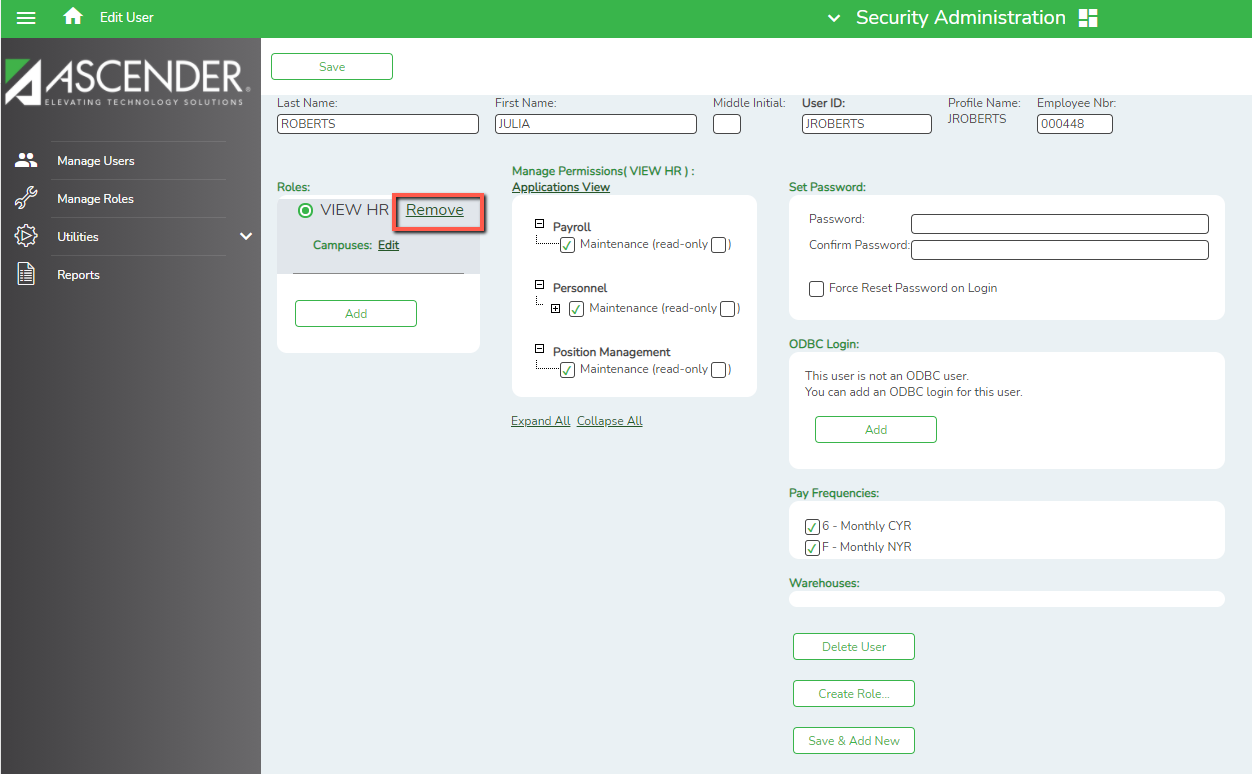
De-select to clear check box(es) as desired. A check box that has been cleared is displayed in red. For any level that has a sublevel that has been cleared, the upper-level title is displayed in italics. For instance, if Utilities has many sublevels, one of which has been cleared, Utilities will appear in italics denoting that not everything beneath Utilities has been granted permission. Click **Save** to save the changes and to show the highest level only of each application.



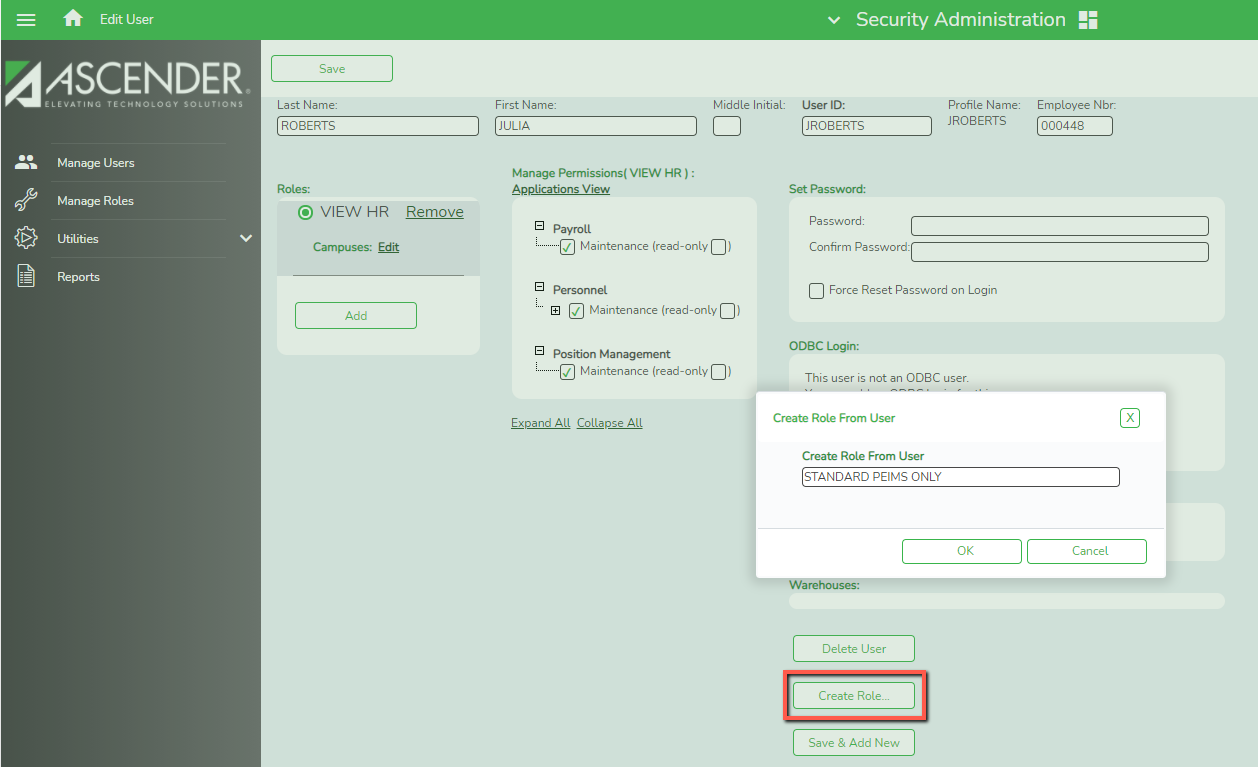
If pay frequencies are required for the role, select the desired Payroll Frequencies and save.



To remove a role once you have assigned it, click **Remove** to the right of the role you wish to remove. Removing the role will also remove the campuses to which you had granted permission.



The **Create Role** button on this screen allows you to create a new role based on the permissions assigned to the user ID displayed. Click Create Role and the Create Role from User dialog box is displayed. In the field, type the name of the new role.

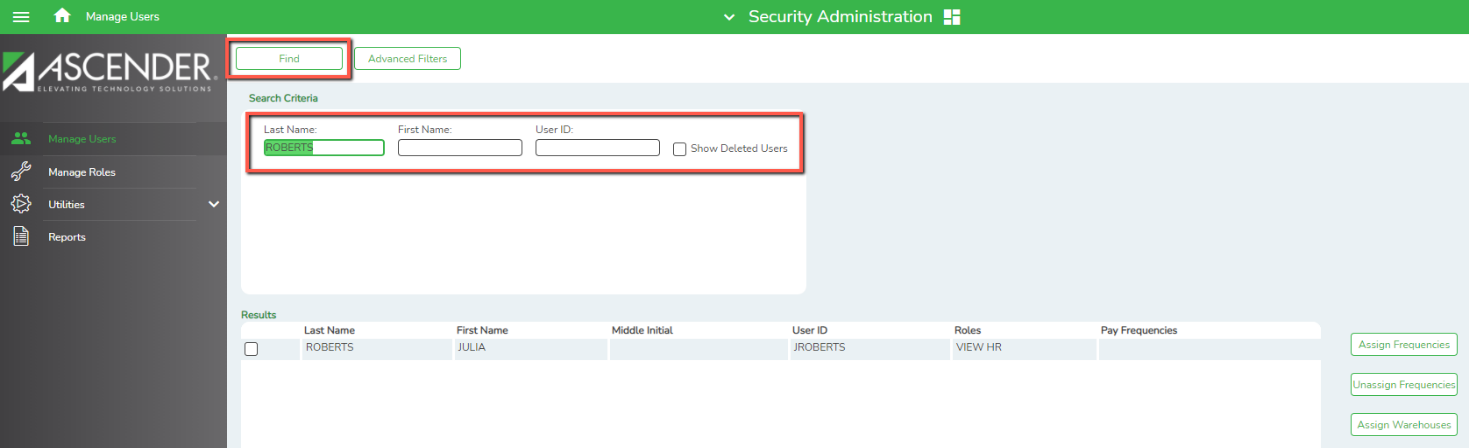


To Find an Existing User

When you log on to the Security Administration application, the Security Administration page is displayed with Manage Users as the default tab.

To perform a search, do one of the following:

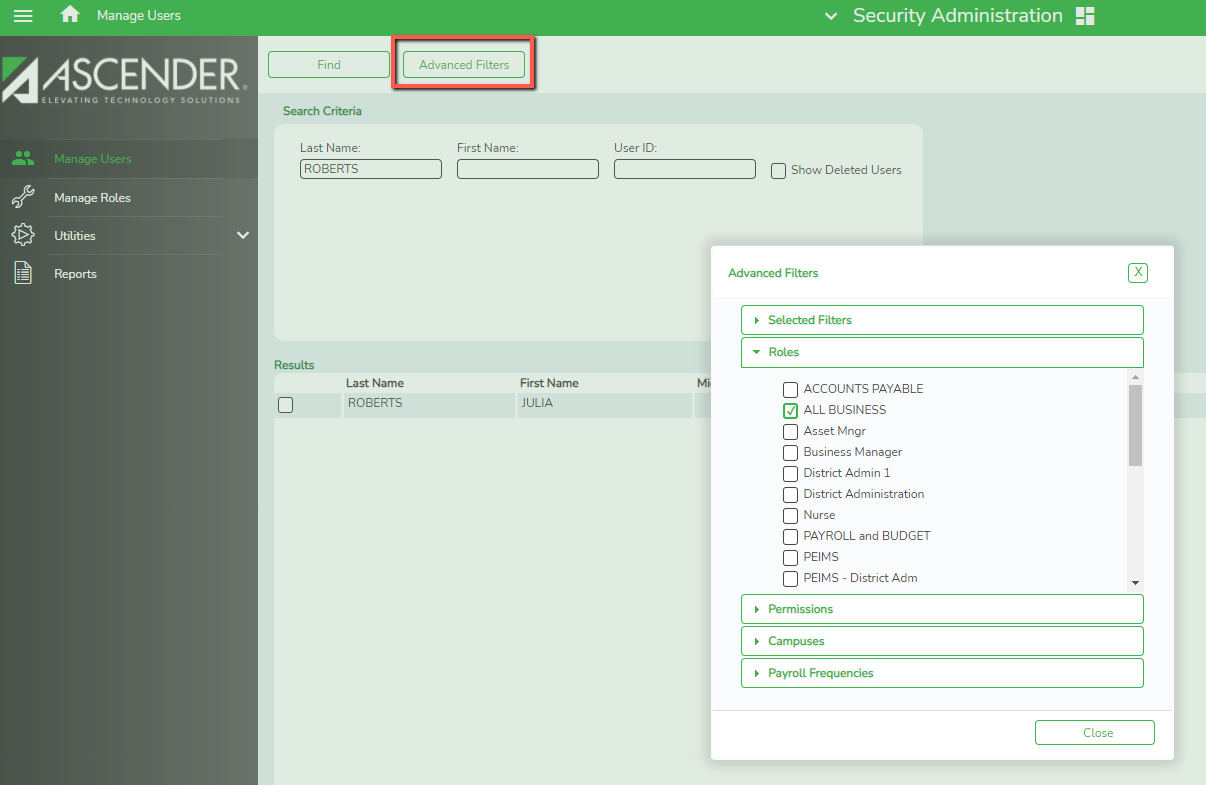
* To display all users, leave the search criteria (Last Name, First Name, User ID) blank and click Find. All existing users will be listed.
* To conduct a search for a specific user, under Search Criteria, enter the following:
  + In the Last Name field, type all or part of the last name of the user. The field can be a maximum of 30 characters.
  + In the First Name field, type all or part of the first name of the user. The field can be a maximum of 30 characters, or
  + In the User ID field, type all or part of the ID of the user. The field can be a maximum of 12 characters. The first character must be a letter.



* Click Find. (If a deleted user needs to be accessed, select Show Deleted Users, and then click Find.) Deleted usernames appear in red.

## Advanced Filters

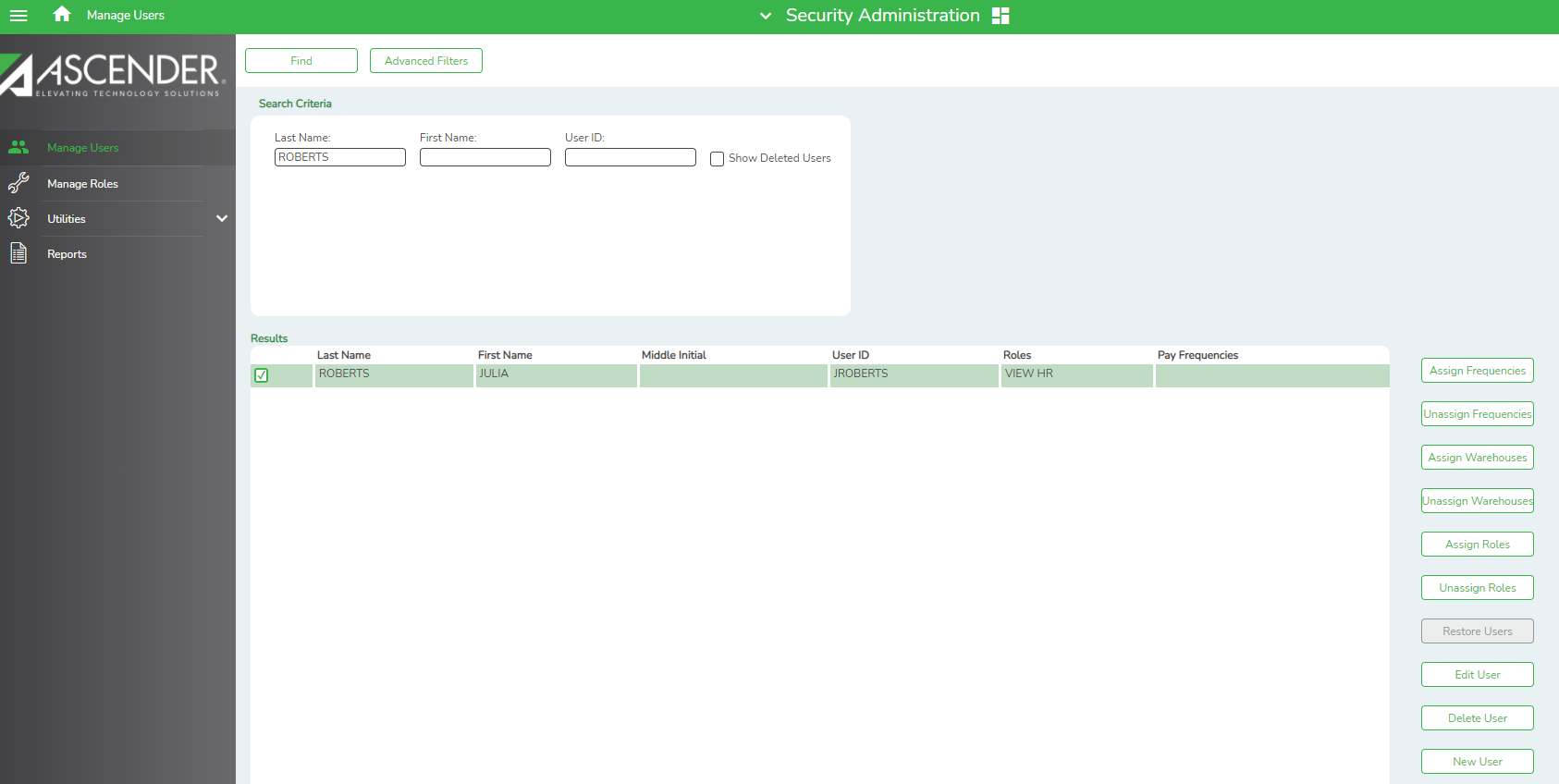
To produce a list of users based on specific roles, permissions, campuses, or payroll frequencies, click Advanced Filters. The advanced filters feature allows you to refine the list of users you produce through the search criteria.



* Roles displays all roles that have been established. Select desired role(s) to refine the search for users having that role.
* Permissions displays applications. Select applications desired. Use the + box to request more specific permissions and to refine the search for users having those permissions.
* Campuses displays all campuses. Select desired campus(es) to refine the search for users having that campus.
* Edit Payroll Frequencies displays all payroll frequencies that have been established. Select a payroll frequency to refine the search for users having that payroll frequency.
* Selected Filters allows you to remove filter(s) from the results. For example, by removing the role filter, all users regardless of the roles to which they are assigned will be displayed, etc…

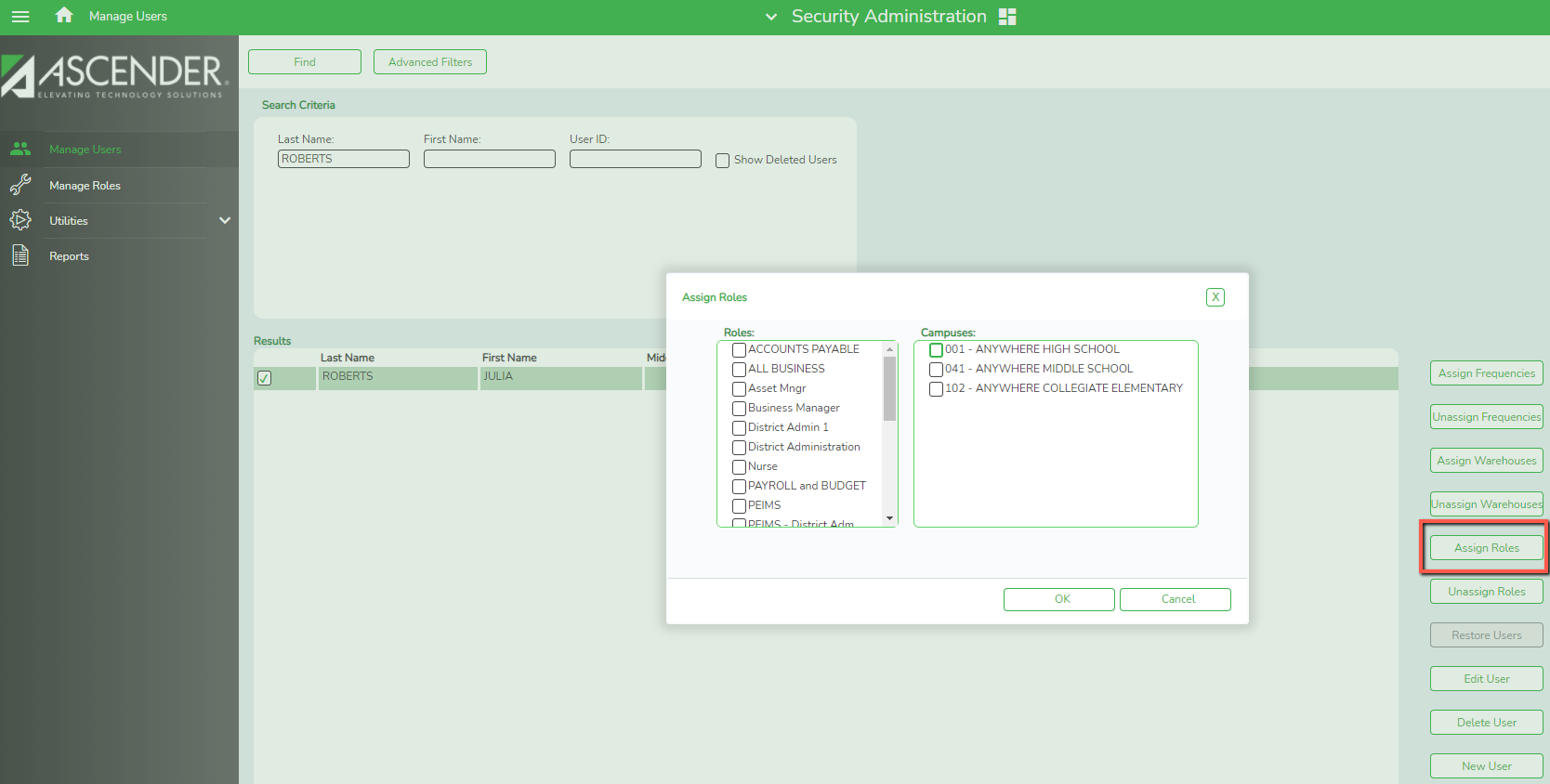
## To Edit an Existing User

Find the desired user and select the box to the left of their name. Once a user has been retrieved and selected, the Assign Frequencies, Un-assign Frequencies, Assign Roles, Un-assign Roles, Import Users, Restore Users, Edit User, Delete User, and New User buttons will display to the right, allowing you to edit permissions.

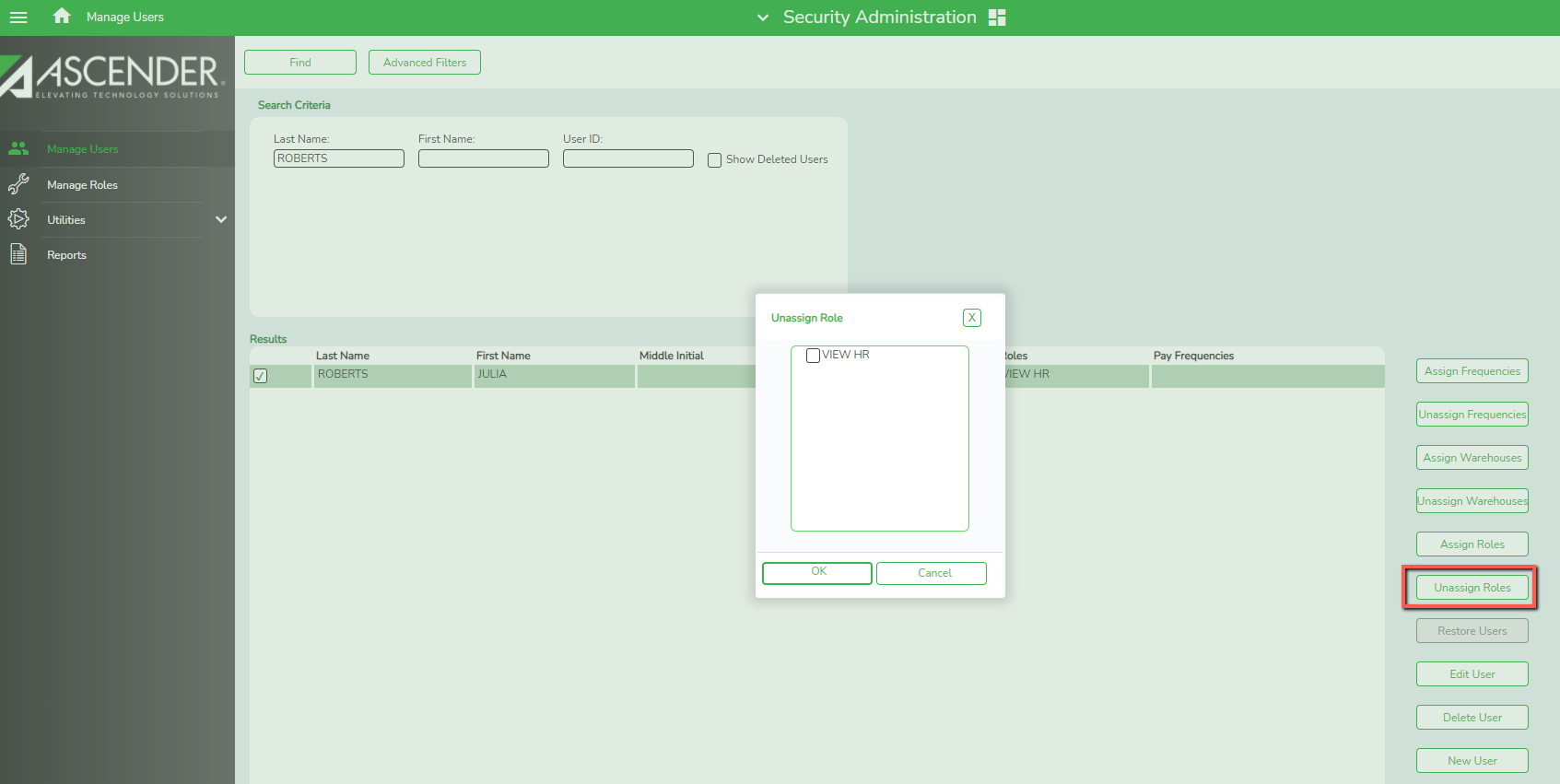


The Assign Frequencies and Un-assign Frequencies buttons allow to assign and un-assign payroll frequencies as needed. The **Assign Roles** button displays a dialog box with the already established roles from which to choose. Select a role and associated campuses to assign to the user. You may select multiple users to assign roles and campuses to.

**Note: If the role contains only Business applications, no campuses should be selected. Access is assigned in District Administration or the individual applications for business users.**



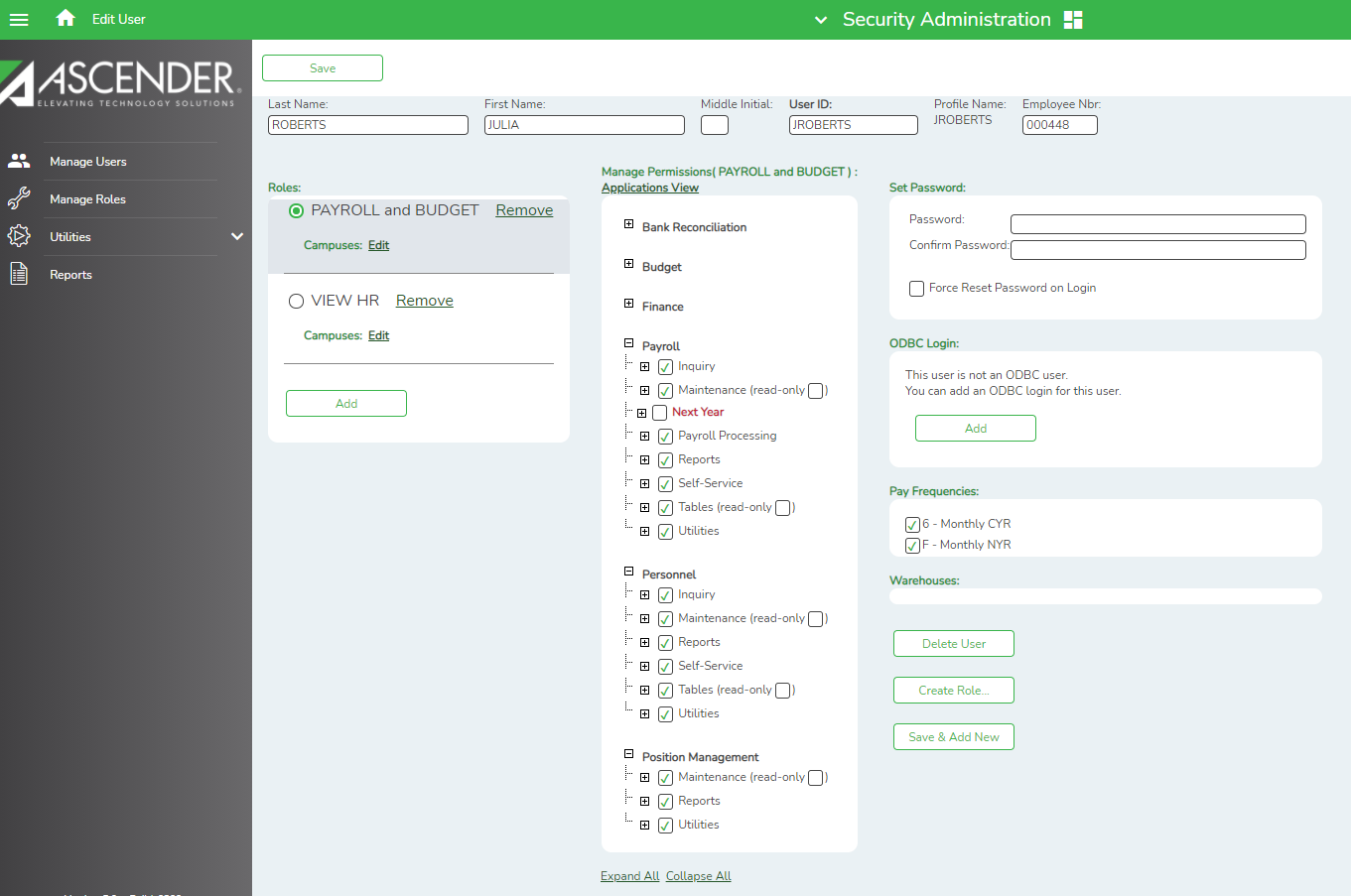
The **Unassign Roles** button displays a dialog box listing the roles currently assigned to the user. Select a role to un-assign from the user.



Use the **Edit User** button to change the roles and responsibilities associated with the user. When selected, the user’s roles and permissions are displayed.

* Passwords can be reset
* Roles may be added or removed
* To edit permissions, select a role and expand the access. Access may be further restricted by deselecting applications, menus and/or tabs.

**Note: Access may only be further restricted here. To add additional access, a change must be made to the role, or a new role with increased access must be created and assigned. Access that has not been granted to the role will not display at all in the Manage Permissions section.**



## Restoring Users Previously Deleted

From the Manage Users page, you may also elect to **Restore Users**. This feature allows you to

restore users that have been previously deleted. Conduct a search for the deleted user by selecting Show Deleted Users, populating the Search Criteria fields as desired, and clicking Find. Under Results, the deleted user name is displayed. Select the user. The Restore Users button is enabled.



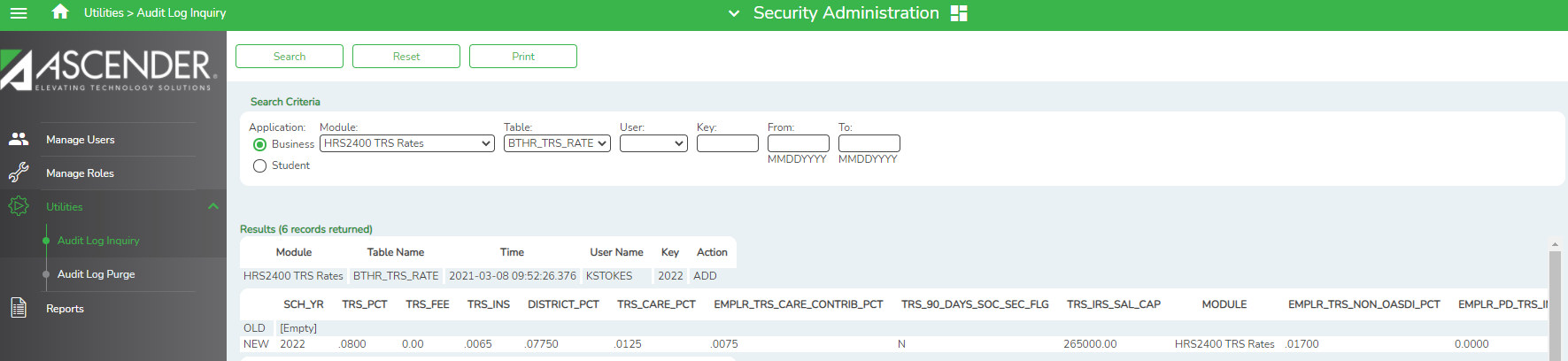
Click Restore Users and the user is restored. You will still need to assign roles and permissions, but the user will be able to use the same username they had before.

# ODBC Access

* ODBC is used in Ascender by programmers and advanced users. No ODBC access is granted to district users at this time. Contact Region 14 for additional details if desired.

Utilities

The Audit Log Inquiry utility allows you to view changes that have been made to the database. Select the Application and define the information you want to search for. In the example below, I can see that User KSTOKES changed info in the TRS Rates table on 03/08/2021. The Original data is displayed along with the new so you can see exactly what was changed.



Report Functions

The Security Administration provides a report printing capability.

# Reports

When you log on to the Security Administration application, the Security Administration page is displayed with Manage Users as the default tab. Click the Reports tab. The Reports page is displayed.

The following reports are available. Select the report to generate it. Reports may be saved as PDFs or in CSV format. Sort and Filter capabilities exist in these reports.

* List of Users by Permissions
* List of Tasks Associated with Roles
* List of Users with ODBC Login (not used at the district level.)
* List of Security Users and Roles
* List of Security Users with Employee Numbers
* Audit Log
* User Log