The TxEIS "How To" Guide Series

Security Administration

How to:

MANAGE TXEIS ROLES AND USERS

Developed by the

TEXAS COMPUTER COOPERATIVE

1314 Hines Avenue
San Antonio, TX 78208-1899

Contents

Overview

The TxEIS Security Administration application provides security administrator rights to the TxEIS Business and Student systems to securely manage TxEIS users and roles (permissions). Additionally, the Security Administrator can run various reports to assist with assessing audit information.

This guide provides information about how to create and manage roles and users as well as assign campus rights, pay frequencies, and warehouses.

Prerequisites

- This guide assumes you are familiar with the basic features of the TxEIS Student or Business systems and have reviewed the TxEIS Student or Business Overview guide.
- For more detailed information about individual fields, please see the online Help in TxEIS Security Administration.
- This guide is based on TxEIS 2.0.0005.

Checklist Overview

The following steps are covered in this guide:

- [ ] Manage TxEIS roles.
- [ ] Manage TxEIS users.
- [ ] Review and purge audit log information.
- [ ] Review and print reports.

Manage Roles

The Manage Roles page allows you to create roles with specific permissions to various component, pay frequencies, campuses, and warehouses within TxEIS. Once roles have been established, you can assign the roles accordingly to each user.

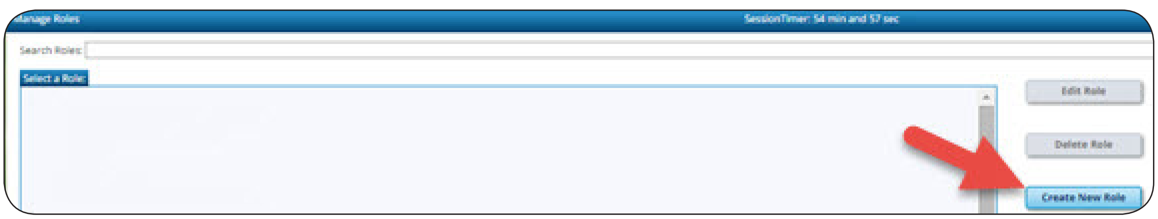
After creating users and performing other functions, you should exit any applications to which you are currently logged on, and log back in to refresh the updated security permissions.

Create a Role

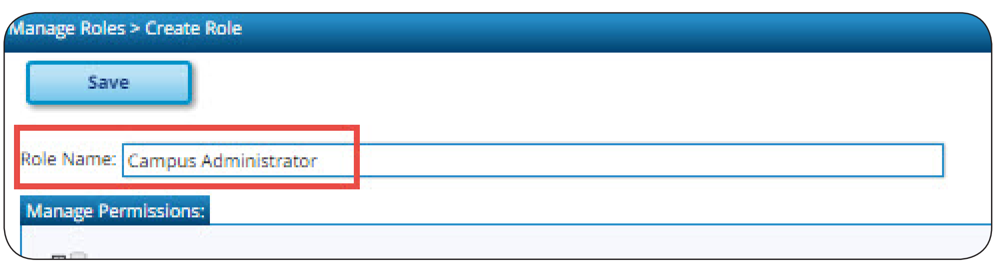
For new districts, log in to Security Administration as an admin user. If you have access, use your assigned login information to log in to Security Administration.

Security Administration > Manage Roles > Create New Role

1. Click **Create New Role**.



2. In the **Role Name** field, type a name for the new role.



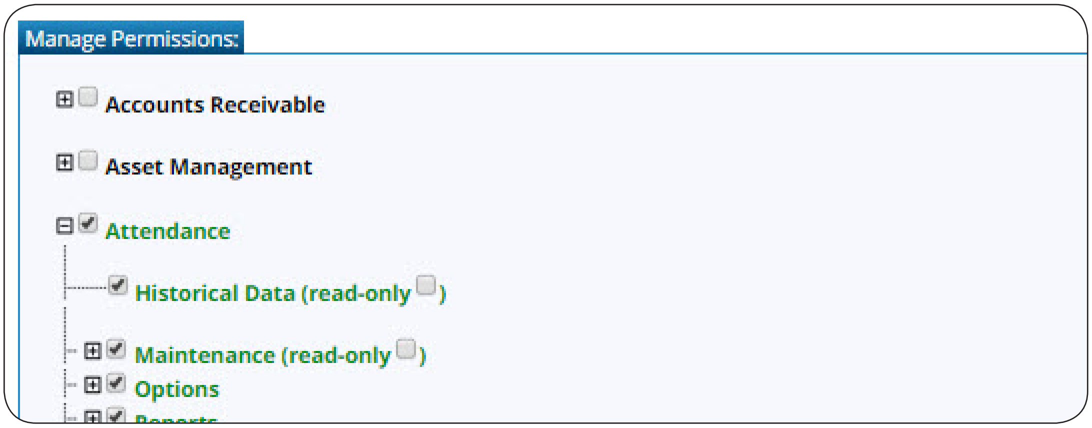
3. Under **Manage Permissions**, click ⊞ to expand an application title. All of the application components are displayed.

   - Select the necessary components to which you want to grant access. Once access is granted to a component, the title is displayed in green and the associated check box is selected.

- If you want to grant read-only access, select the read-only field where available. When selected the component title is displayed in orange. Read-only access limits the user to only be able to view data on a page.

  Notes:

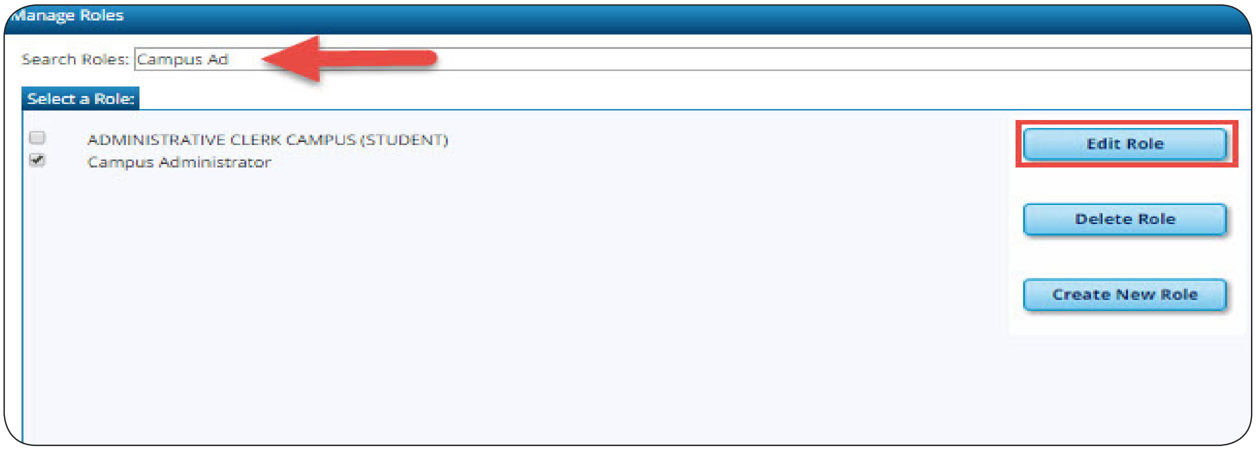
  - Multiple applications can be added to a role.
  - Multiple roles can be added to a user.



4. Click **Save**. The new role is displayed under **Select a Role**. You can continue creating roles as needed.

Edit a Role

Use the Manage Roles page to edit an existing role.



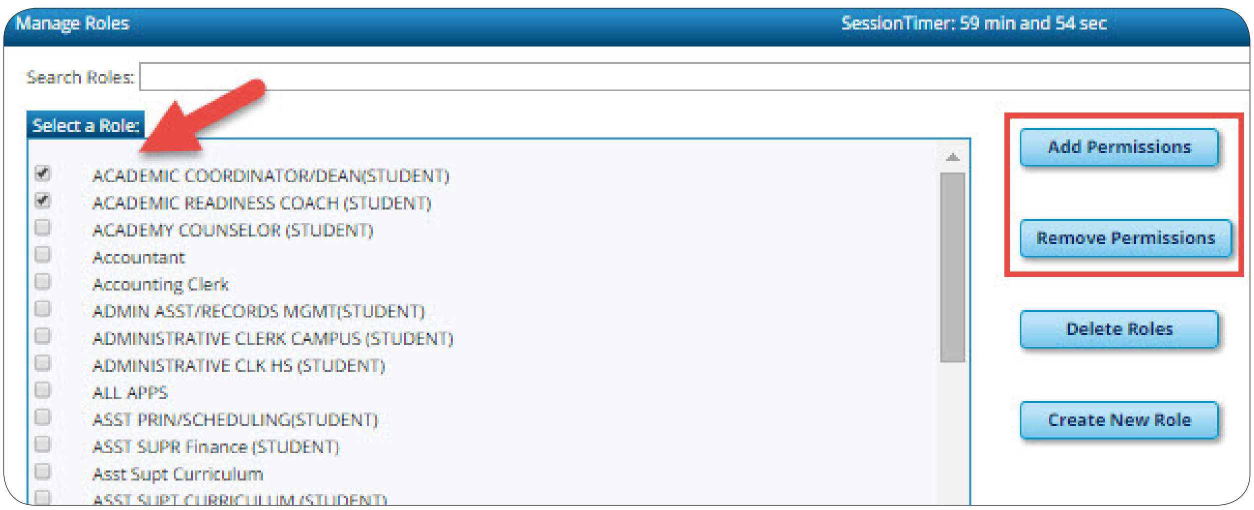
1. Type the role name in the **Search Roles** field. As you type a role name, the existing roles that match what you have typed are displayed under **Select a Role**.

NOTE: The **Edit Role** and **Delete Role** buttons are only enabled if a role is selected.

2. Under **Select a Role**, select the desired role.
3. Click **Edit Role**.
4. Under **Manage Permissions**, make the necessary changes.
5. Click **Save**.

Manage Permissions Across Multiple Roles

Use the Manage Roles page to add or remove permissions from multiple roles.

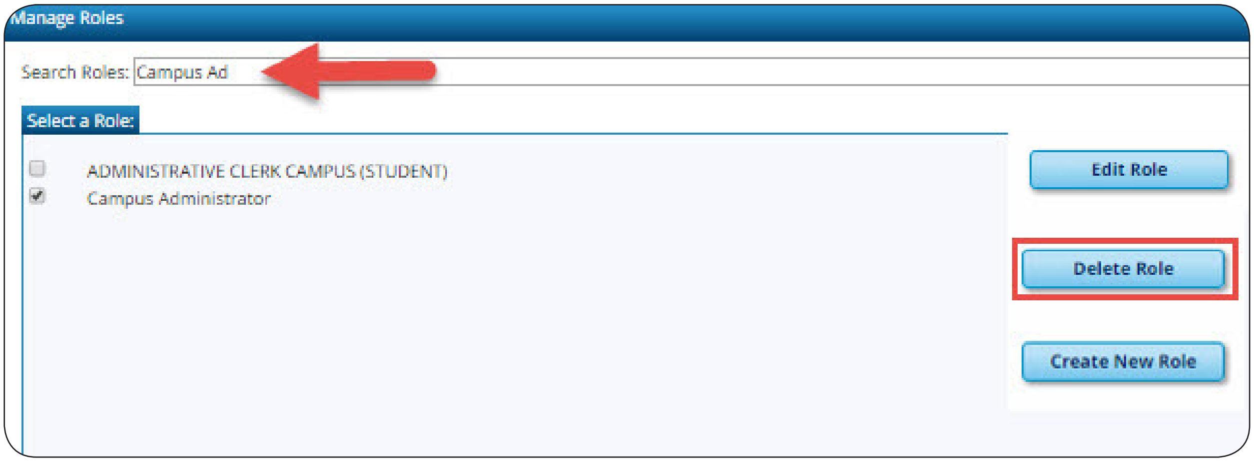


NOTE: If more than one role is selected, the **Edit Role** button is no longer displayed, and the **Add Permissions** and **Remove Permissions** buttons are displayed.

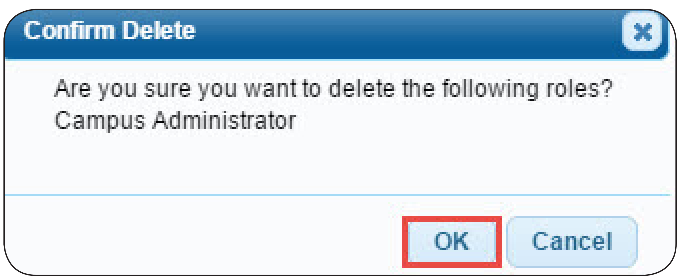
1. Click **Add Permissions** to add permissions across the selected roles.
2. Click **Remove Permissions** to remove permissions across the selected roles.
3. Click **Save**.

Delete a Role

After retrieving a role, you can delete a role if it is no longer needed.



1. Under **Select a Role**, select the desired role.
2. Click **Delete Role**. A message is displayed prompting you to confirm deletion.



- Click **OK** to delete.
- Click **Cancel** to close the dialog box and return to the Manage Roles page.

Manage Users

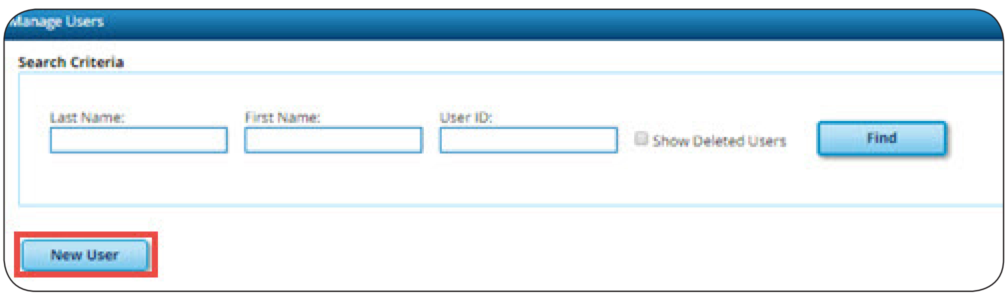
The Manage Users page allows you to create users and establish the roles and permissions associated with each user. You can assign each user a role along with pay frequencies (Business), campuses (Student), and warehouses (Business).

Create a New User

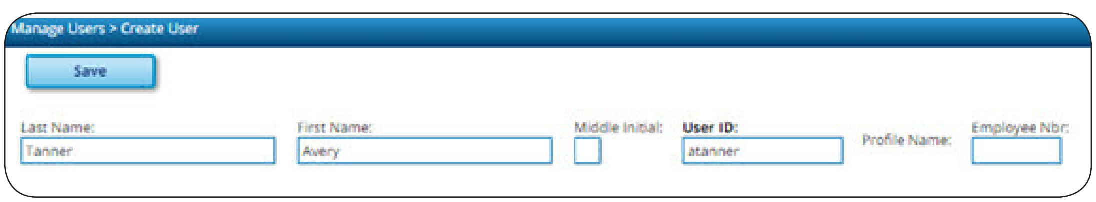
If you are a new user, stay logged in as an admin user to create another user. If not, then you can proceed with these steps under your assigned login information.

Manage Users > New User

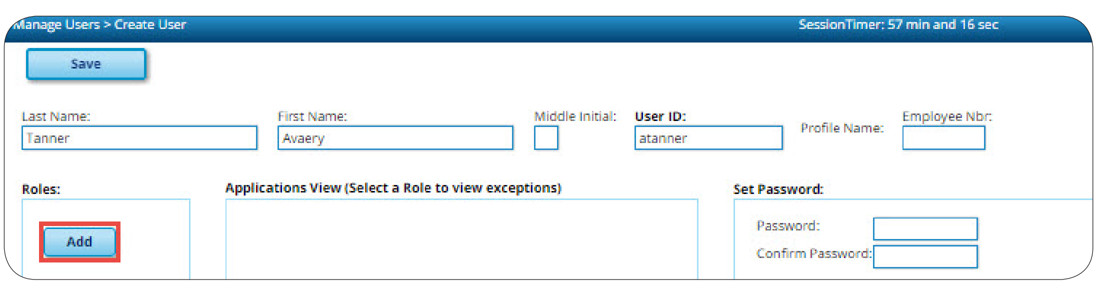
1. From the Manage Users page, click **New User**.



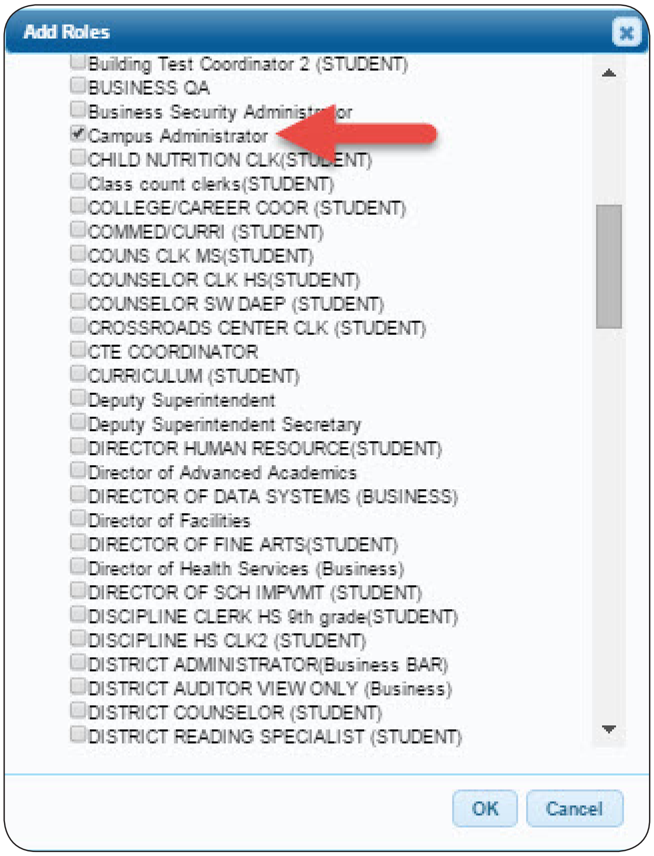
- Enter the user's first and last name, and a user ID to be used upon logging in to the TxEIS system.



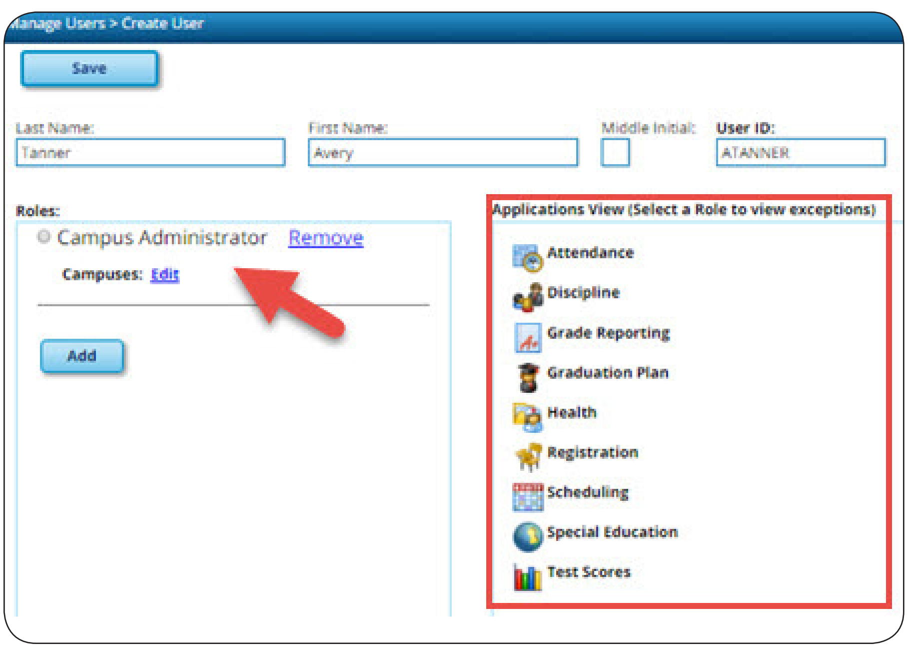
- Under **Roles**, click **Add**.



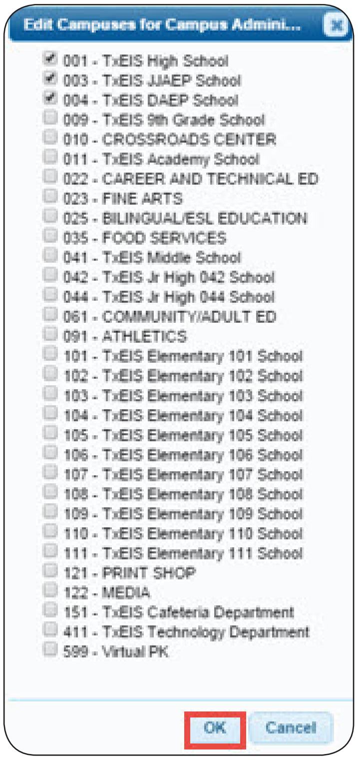
The Add Roles dialog box is displayed.



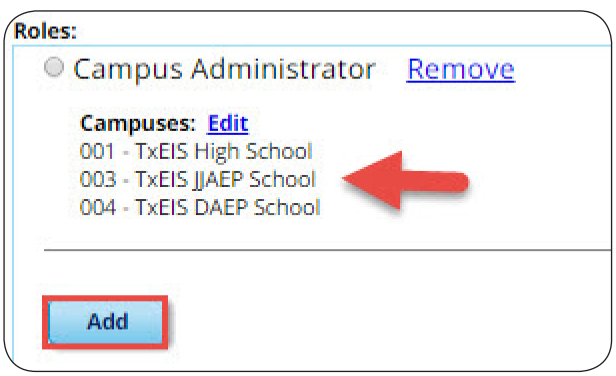
Select the role to be assigned to the user and click **OK**. The role is displayed under **Roles**, and the applications assigned to the role are displayed under **Applications View**.



2. For Student users, click **Edit** next to **Campuses** to display the Edit Campuses dialog box.



Select the campuses to which the user will have access and click **OK**. The campus information is displayed under the role title.

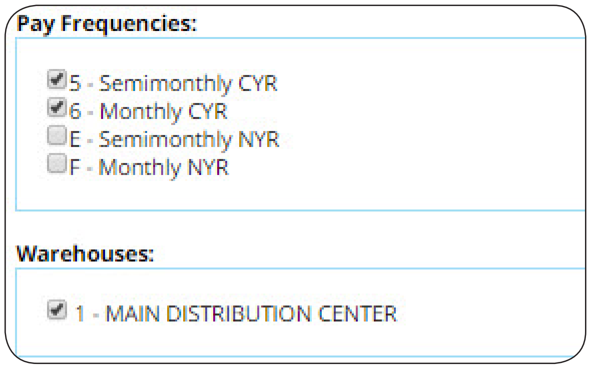


Click **Add** to add additional roles.

3. For Business users:

- Under **Pay Frequencies**, select the applicable pay frequencies to which you are granting the user access. Pay frequencies are necessary when using the Human Resources application.

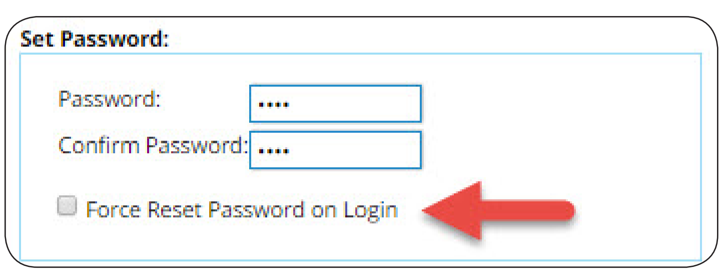
- Under **Warehouses**, select the applicable warehouses to which you are granting the user access. Warehouses are required when using the Warehouse application in the Business system.



4. For Business users, in the **Employee Nbr** field, type the employee's six-digit employee number. If you are creating a new user and he does not have an employee number, based on the employee type, use one of the following options to create an employee number.

   - On the Maintenance > Staff Demo tab in Human Resources:
     - Click **Add Emp**.
     - Enter the employee's demographic information.
     - Click **Save** to generate an employee number.
   - On the Maintenance > Non-Employee page in District Administration:
     - Click **Add**.
     - Enter the employee's demographic information.
     - Click **Save** to generate an employee number.

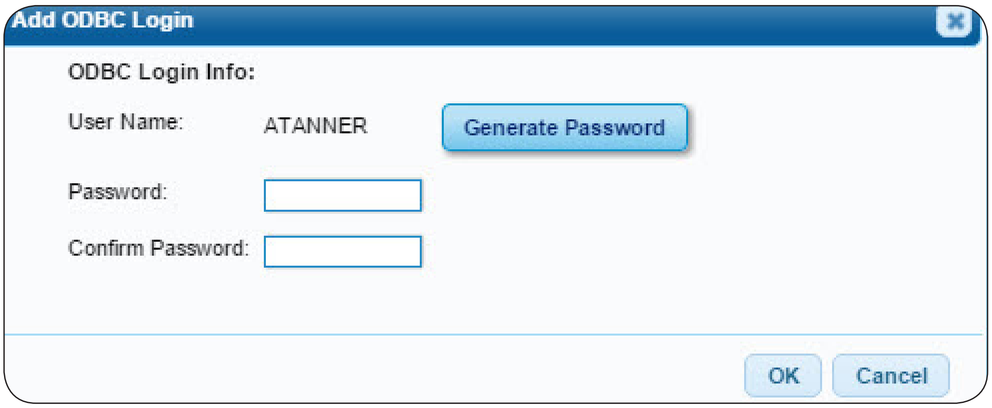
5. Under **Set Password**, in the **Password** field, type a password for the user. In the **Confirm Password** field, type the password again to confirm.



If you are setting a temporary password, select **Force Reset Password on Login** to prompt the user to enter a new password upon logging in to the system.

6. Under **ODBC Login**, click **Add**. A dialog box is displayed.

Note: A new user must be saved before adding an ODBC login.



- Enter and confirm a password, or click **Generate Password** to automatically generate a password for the user's ODBC login.
- Click **OK**.

7. Click **Save** to save the changes. Or, click **Save & Add New** to return to the Create User page and create another user.

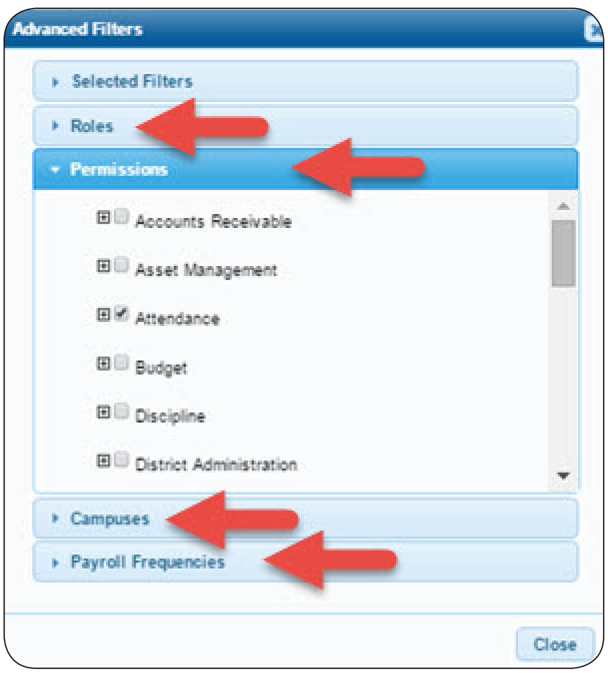
Edit a User

From the Edit User page, you can edit all of the preset functions that were saved while creating a user. Additionally, you can delete a user and update a user's password.

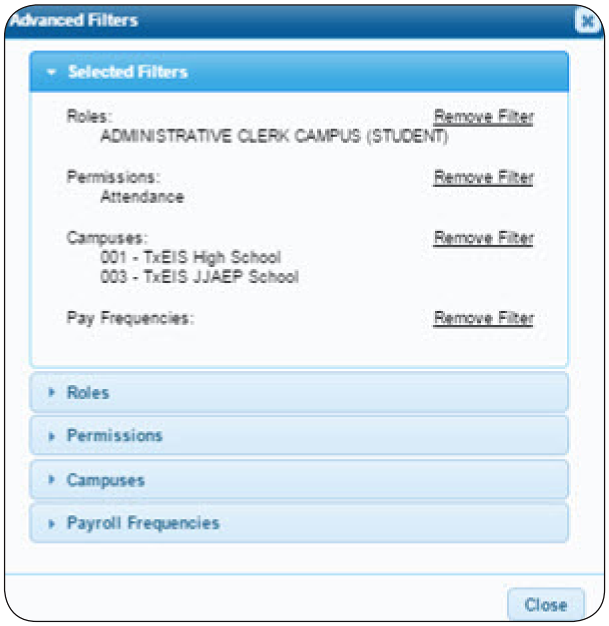
Security Administration > Manage Users > Edit User

1. Type the user's information in the **Last Name**, **First Name**, or **User ID** field.
2. To narrow your search results, click **Advanced Filters**. The Advanced Filters dialog box is displayed.

- Click the filter names to expand the list of available options.

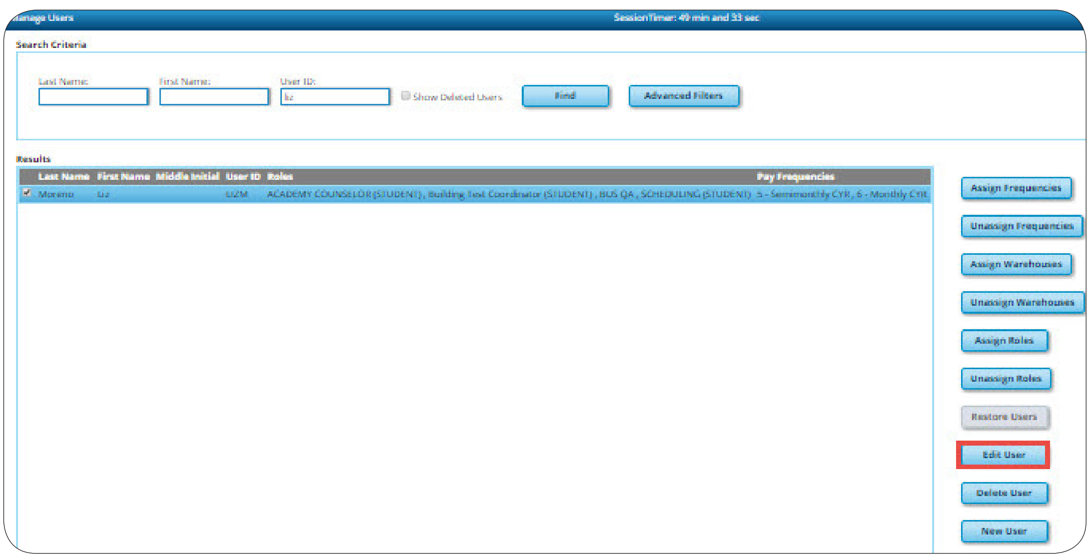


- Select the desired filters, and then click **Selected Filters** to display the selected filters.



- Click **Remove Filter** next to the filter selection that you want to remove.

3. Click **Find**. A list of user records matching the selected filters is displayed under **Results**.



4. Select the desired user and click **Edit**.

5. Make the necessary changes to the user's record and click **Save**.

Create an LDAP User

You can use the Edit User page to establish an LDAP ID association, which enables the user to use the same password associated with the LDAP ID in the TxEIS applications.

NOTE: Your database must be configured properly to enable the LDAP feature. Refer to the DBA Assistant online Help for information about setting up the LDAP preferences.

Security Administration > Manage Users > Edit User

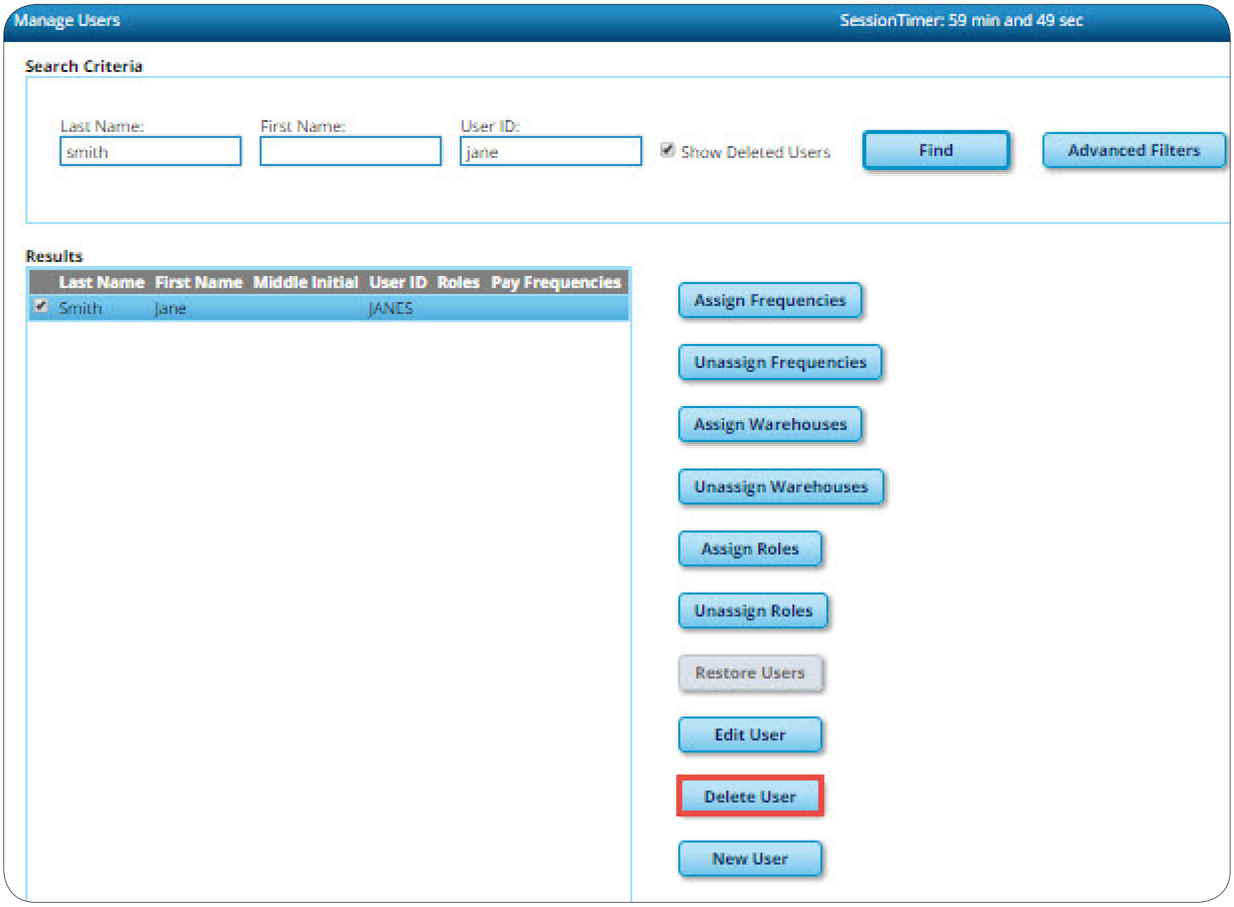
1. Click **LDAP Directory** to create an association between an established LDAP user ID and a user name.
2. Locate the LDAP user ID you wish to have associated with your user name. The password associated with the ID will be associated with your user name as well.
3. Click **Select** to select the LDAP user ID.
4. Click **Save** to add the association.

NOTE: Review the online Help for information about how to create an LDAP ID for a new user or for multiple users.

Delete a User

Use the Manage Roles page to delete a user.

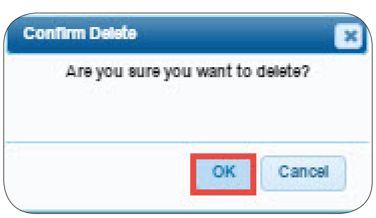
NOTE: Administrative users cannot be deleted. If an administrative user is selected, a dialog box is displayed indicating that the administrative user's properties cannot be changed.



1. Type the user's information in the **Last Name**, **First Name**, or **User ID** field.

2. Click **Find**. A list of users matching your search criteria is displayed.

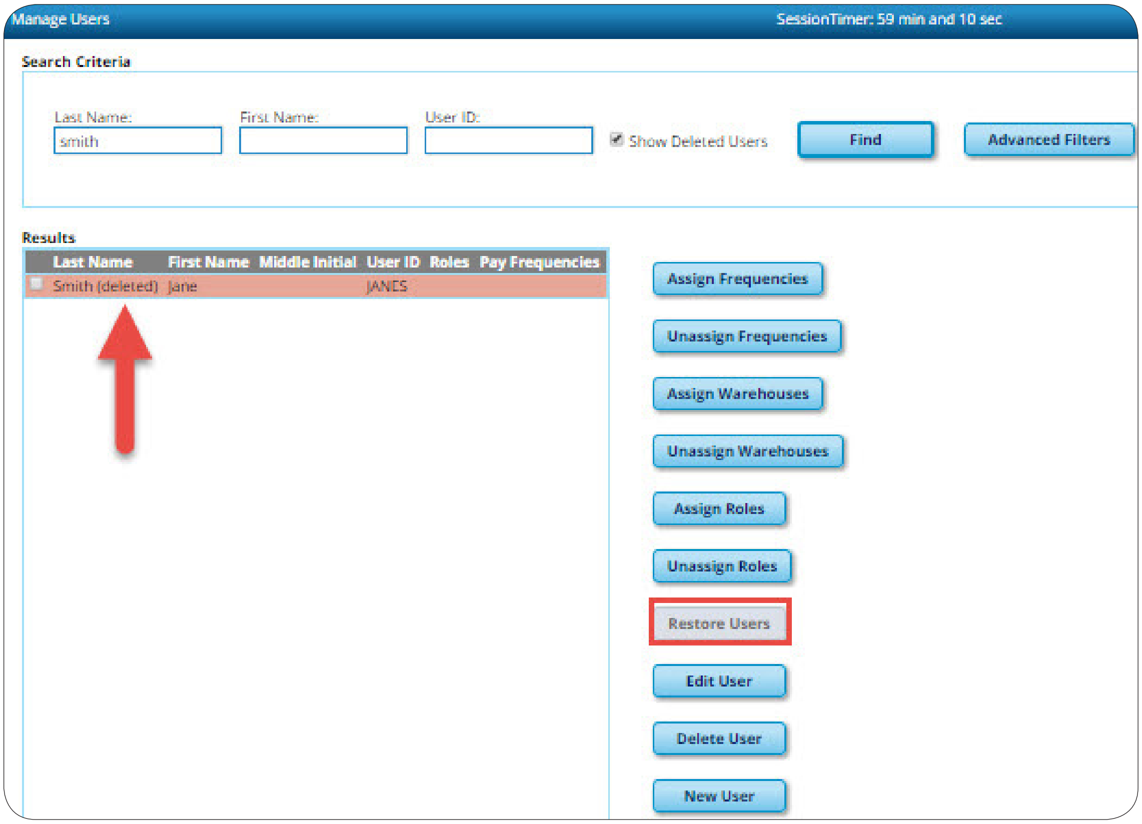
3. Select the user to be deleted and click **Delete User**. A message is displayed prompting you to confirm deletion.



- Click **OK** to delete.
- Click **Cancel** to close the dialog box and return to the Manage Users page.

Restore a User

The Manage Roles page also allows you to restore a deleted user.



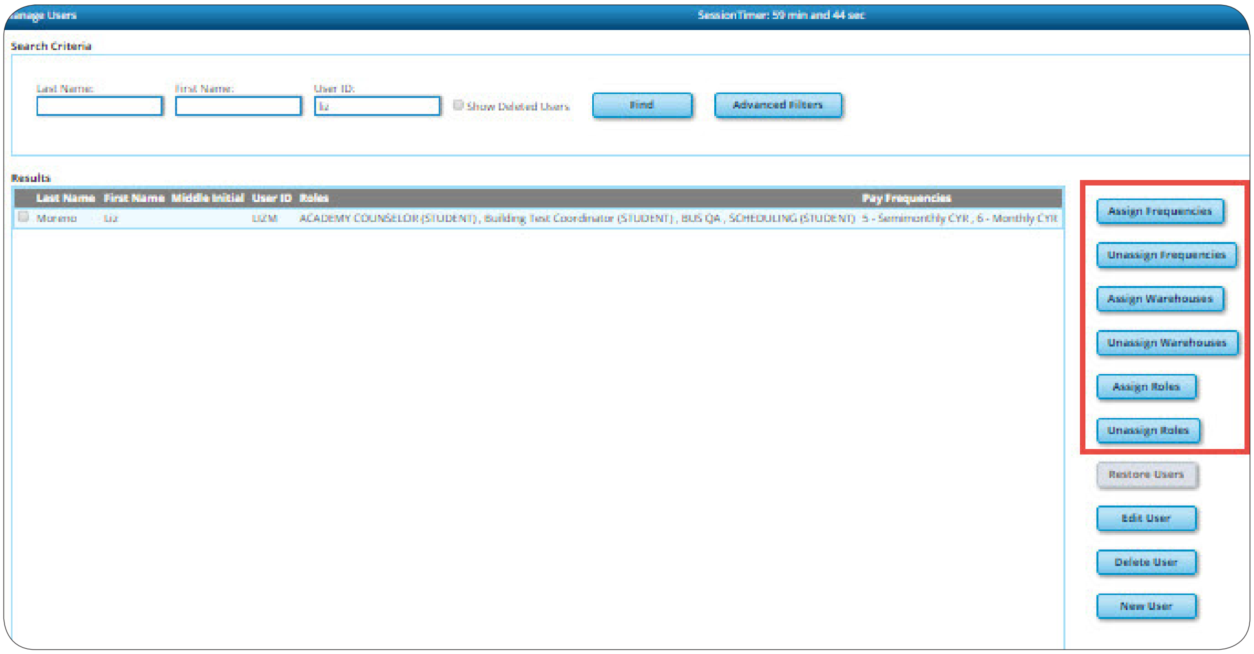
1. Type the user's information in the **Last Name**, **First Name**, or **User ID** field.
2. Select **Show Deleted Users** to include deleted users in the search.
3. Click **Find**. A list of users who match your search parameters is displayed.

   NOTE: Deleted users are highlighted in red.

4. Select the user to be restored and click **Restore User**. A "Save successful" message is displayed indicating that the user was restored.

Additional Features for Managing Users

From the Manage Users page, the following buttons are displayed on the right side of the page.



1. Select any of the buttons to display a dialog box with the applicable options to assign or unassign frequencies (Business users), warehouses (Business users), and roles for the selected user.

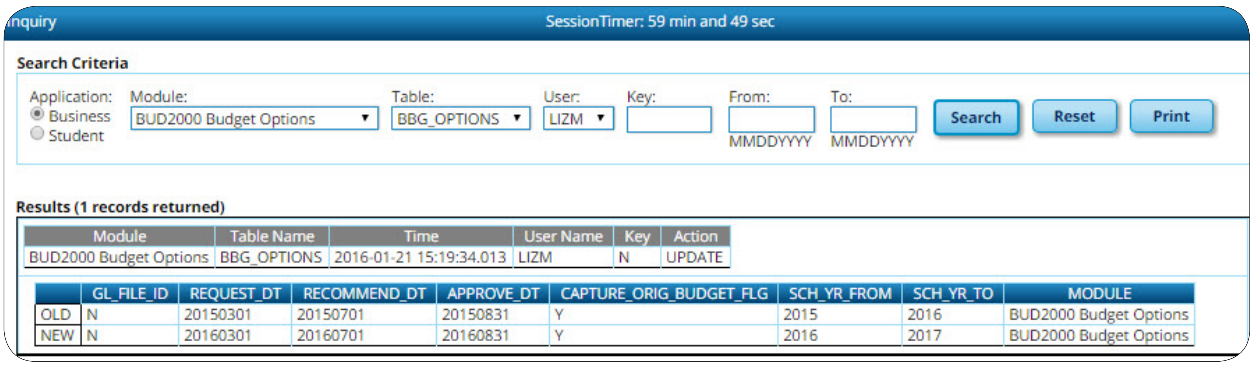
2. Click **OK** to save the changes.

Review the Audit Log

The Security Administration application allows you to search, view, and purge changes made in the Business or Student systems since the last audit log purge.

Perform an Audit Log Inquiry

Use the Audit Log Inquiry utility to search for and view changes made in the Business and Student systems.



Security Administration > Utilities > Audit Log Inquiry

1. Under **Application**, select **Business** or **Student**.

2. In the **Module** field, select the desired tab.

   Note: Only tabs that had changes are displayed.

3. In the **Table** field, select the table for which you would like to search.

4. In the **User** field, select the user name for which you would like to search.

5. In the **Key** field, type the key (i.e., employee number, vendor number, social security number, etc.) for which you would like to search.

   Note: Each table can only have one key field. In most cases, the key will include the employee number, the vendor number, or the student's social security number.

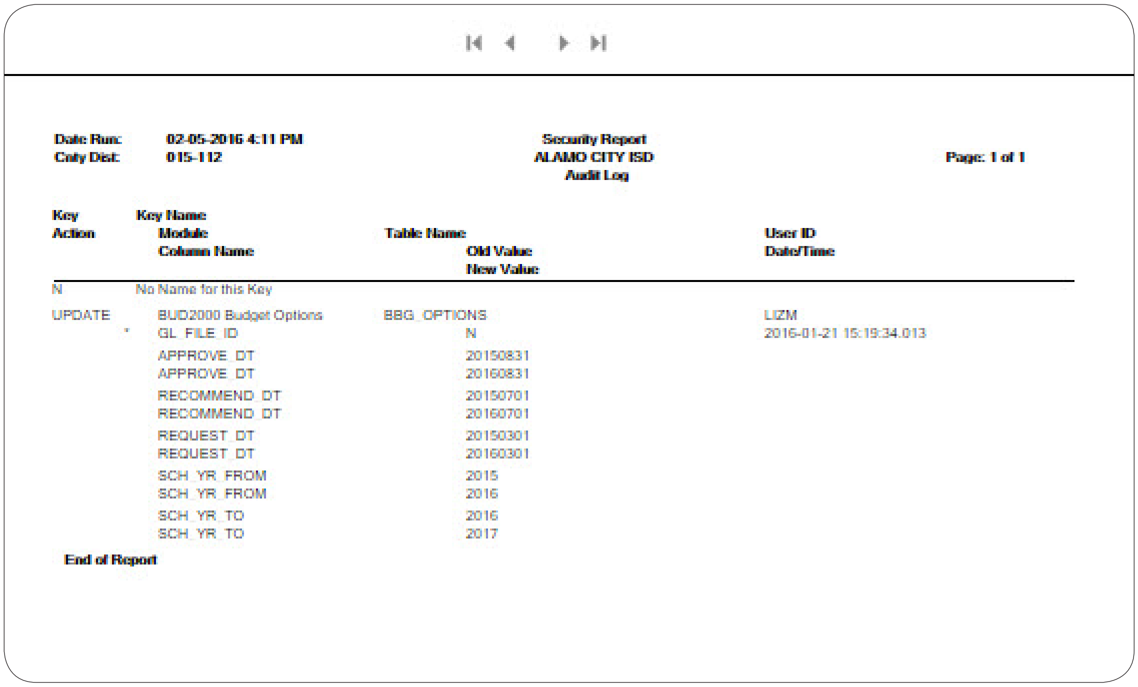
6. In the **From** and **To** fields, type the beginning and ending dates in the MMDDYYYY format for which you would like to search.

7. Click **Reset** to clear the inquiry criteria at any time. Enter new criteria to perform a new

inquiry.

8. Click **Search** to search the audit log. The results are displayed under **Results**.

9. Click **Print** to display and print a report of your search results. The report is displayed in a separate window.



Date Run: 02-05-2016 4:11 PM
Cnty Dist: 015-112

Security Report
ALAMO CITY ISD
Audit Log

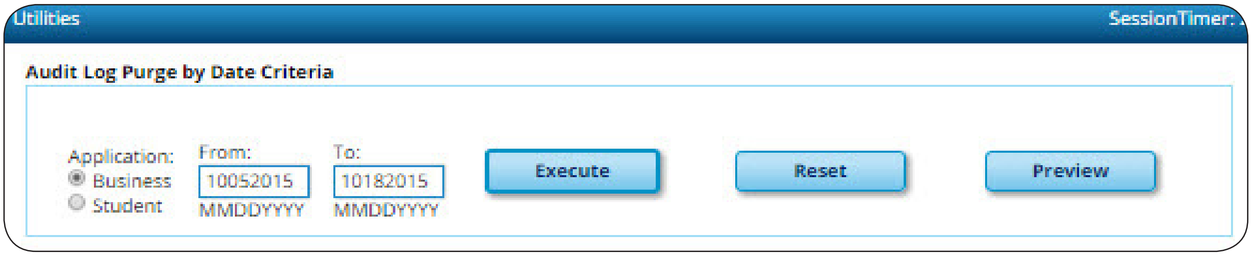
Page: 1 of 1

Key / Action	Key Name / Module / Column Name	Table Name	Old Value / New Value	User ID / Date/Time
N	No Name for this Key			
UPDATE	BUD2000 Budget Options	BBG_OPTIONS		LIZM
*	GL_FILE_ID		N	2016-01-21 15:19:34.013
	APPROVE_DT		20150831	
	APPROVE_DT		20160831	
	RECOMMEND_DT		20150701	
	RECOMMEND_DT		20160701	
	REQUEST_DT		20150301	
	REQUEST_DT		20160301	
	SCH_YR_FROM		2015	
	SCH_YR_FROM		2016	
	SCH_YR_TO		2016	
	SCH_YR_TO		2017	

End of Report

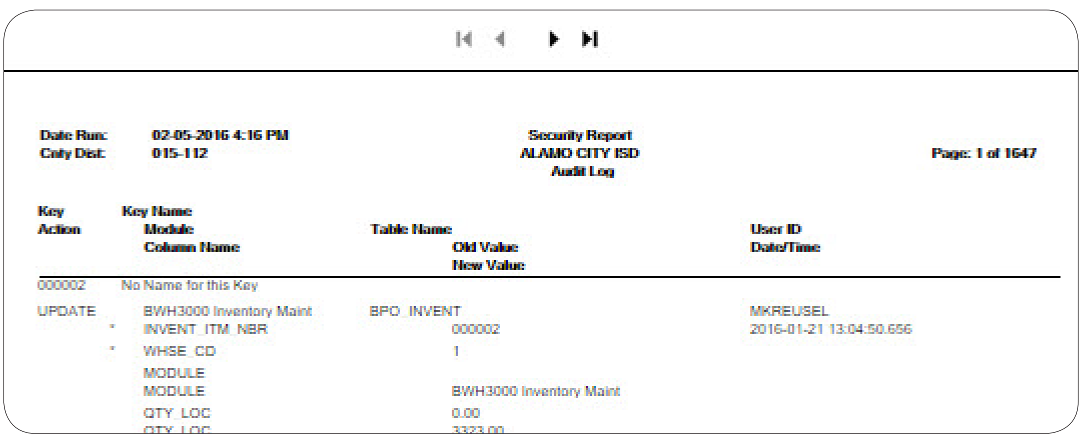
Purge Audit Log Data

Use the Audit Log Purge utility to purge Business or Student audit records for a selected date range, and to create, display, and print an Audit Log report.

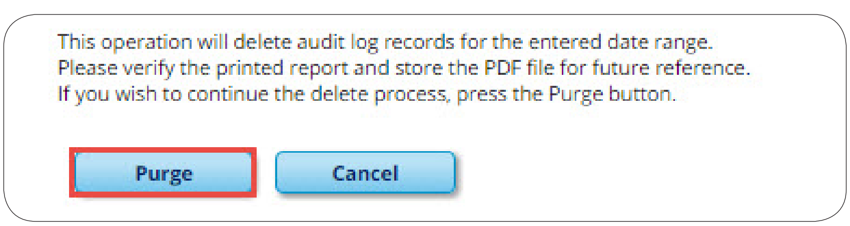


Security Administration > Utilities > Audit Log Purge

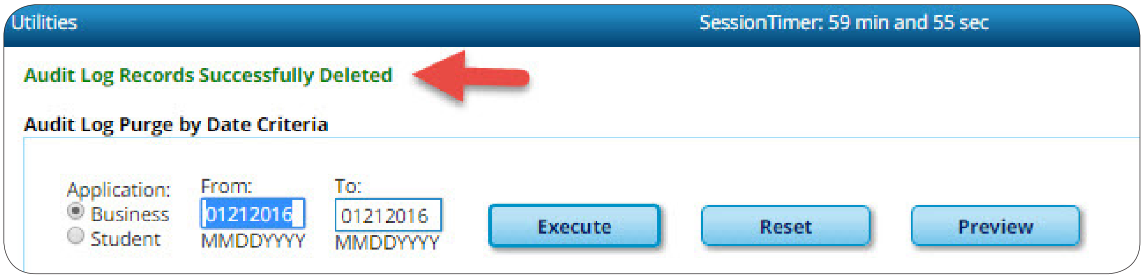
1. Under **Application**, select **Business** or **Student**.
2. In the **From** and **To** fields, type the beginning and ending dates in the MMDDYYYY format for which you would like to search.
3. Click **Reset** to clear the purge criteria at any time. Enter new criteria to perform a new purge.
4. Click **Preview** to display a report of the audit log items that will be purged.



Click **Execute** to process the purge. The following message is displayed.



Click **Purge** to purge the data. A message is displayed indicating that the process was successful.



Reports

There are several reports available in Security Administration to assist you in verifying user information such as roles, permissions, user names, and audit information. You can view and print the reports as needed. Please refer to the online Help for specific information about each report. The following reports are available from the Reports menu:

- List of Users by Permissions
- List of Tasks Associated With Roles
- List of Users With ODBC Login
- List of Security Users and Roles
- List of Security Users with Employee Numbers
- Audit Log
- Users Log

TxEIS™