Security Administration Overview

Table of Contents

Security Administration Overview

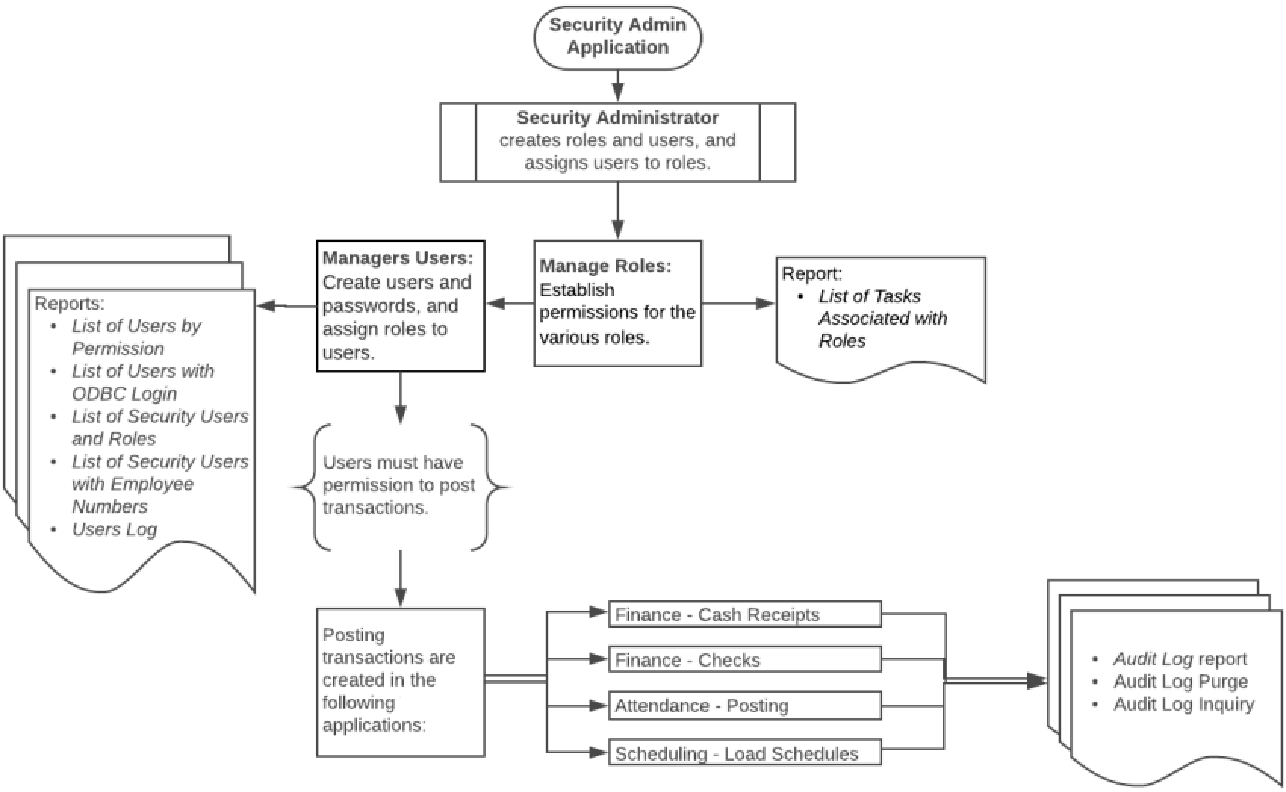
ASCENDER Security Administration provides security administrators or designated users the rights to securely manage roles and permissions for ASCENDER Business and Student users. Additionally, various reports are available to assist with assessing audit information.

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

Before You Begin:

Review the Security Administration flow chart and terminology in order to understand the relationship between roles, users, and permissions and how they integrate into the ASCENDER Business and Student systems.

Security Administration flow chart



Review Security Administration terms.

Term	Description
User	An individual who has access to log on to ASCENDER with a valid user name and password.
Authentication	Determines a user's identity via a user name and password that is entered on the ASCENDER Login page.
Authorization	Determines the user's system permissions (access) after the user's identity is authenticated.
Task	Represents each page or tab within ASCENDER.
User Role	Represents the association of a user with a role. The user role provides campus, payroll frequency, and warehouse permissions.
Role	A group of tasks (page or tab) to which a user has access.
Permission	Determines the relationship between a role and a task in order to extend the appropriate access to the user in ASCENDER.
Component	Refers to an application, page, or tab when managing ASCENDER roles and users.

What is the purpose of a role?

The Security Administration application is structured to assign roles to users instead of individual tasks, which simplifies the designated security administrator's duty of managing user permissions.

For example, if a new page (task) is added to the Attendance application and only the Attendance Clerks require access to the page, the security administrator can provide page permission to only the Attendance Clerk role, which grants access to all users who are assigned the Attendance Clerk role.

If roles did not exist, each individual user profile would have to be manually updated with access to the new page.

Why use permissions?

In most cases, roles cover all user access; however, special cases may exist. For example, if a user is assigned to a role but this particular user should not have access to a specific page within that role, you can manually update the user's profile to set the exclude permission to that specific page. The user would still have access to the other role permissions with the exception of the excluded page. You can exclude a permission by simply unselecting a task (page or tab) from the user's profile permissions.

What is a user role?

For Student users, the user role provides campus access. For example, a user may be assigned the Attendance Clerk role for a high school campus but may also have the Discipline Advisor role for the middle school campus. Based on the campus permissions in the user role, the user cannot modify attendance information for the middle school campus, only the high school campus.

For Business users, the user role provides access to payroll frequencies and warehouses. For example, if a user only has access to a specific payroll frequency, the user can only run Human Resources processes for that specific payroll frequency.

Manage Roles

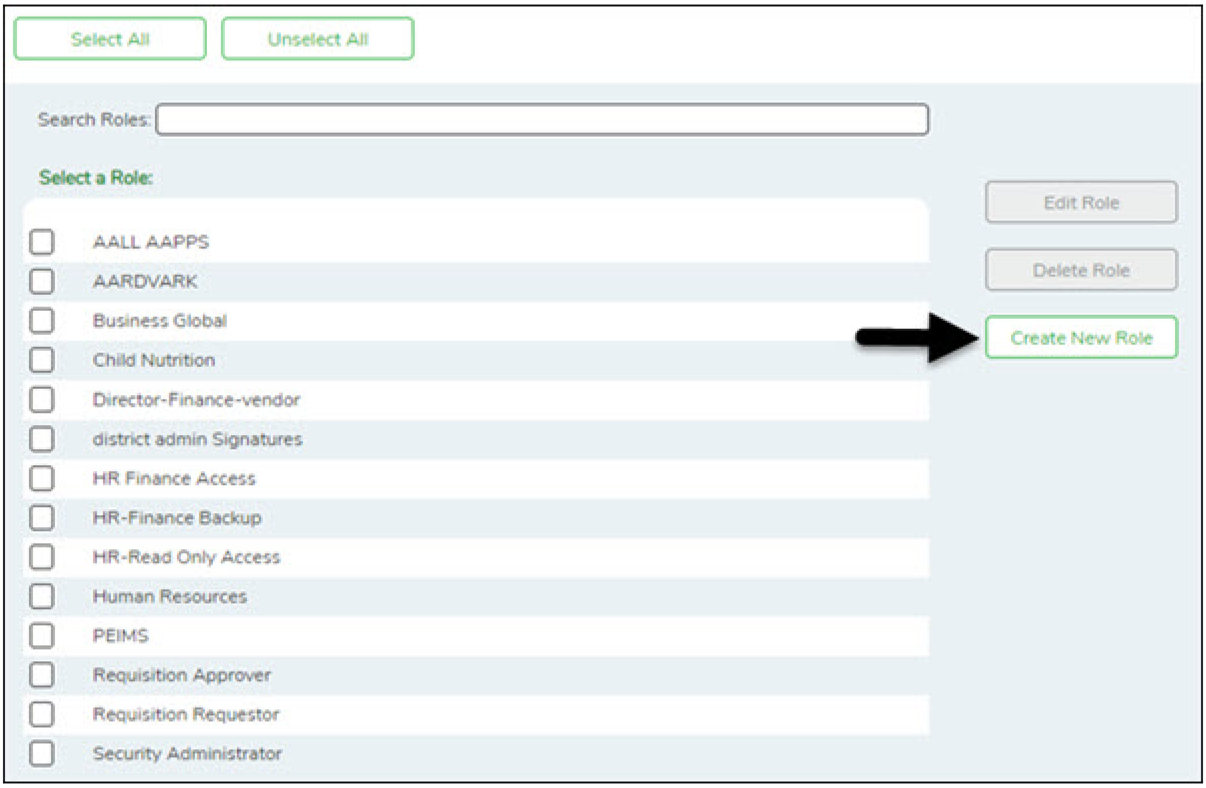
Manage roles.

Security Administration > Create/Edit Roles

This page is used to create new roles or edit existing roles. You can add or edit roles for which a security component is required. Additionally, you can establish permissions for the various roles; for example, you can assign a database administrator permission to the Finance application.

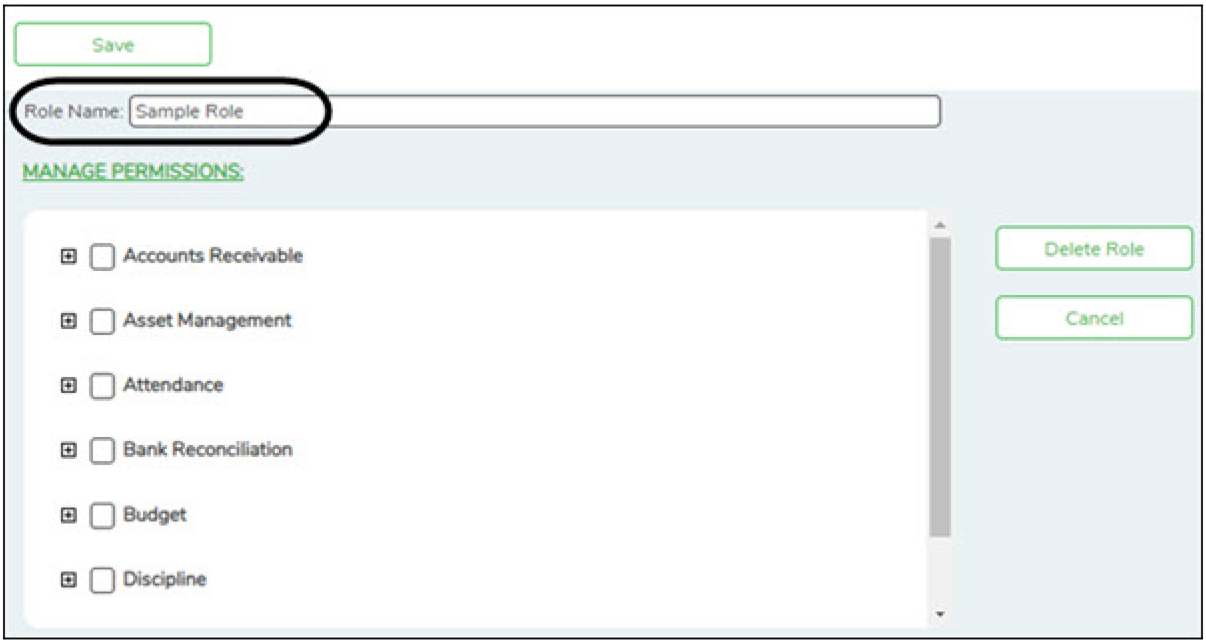
Create a role:

❏ From the Manage Roles page, click **Create New Role**.



The Create Role page is displayed.

Role Name	Type the name of the role to be created.

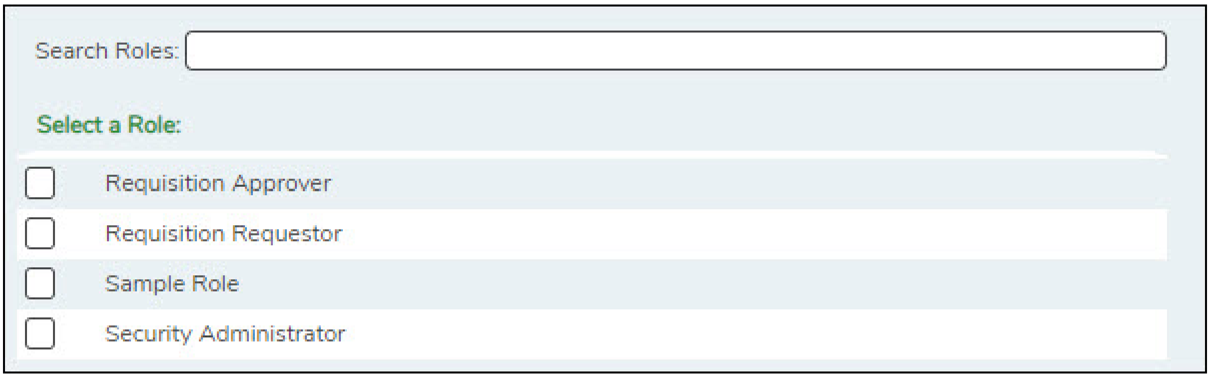


❑ Under **Manage Permissions**:

- Click + - to expand or collapse available role permissions.
- Select the permissions to be added to the role. Once permission is granted to a component, the title is displayed in green and the associated check box is selected.

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

❑ Click **Save**. The new role is displayed under **Select a Role**.

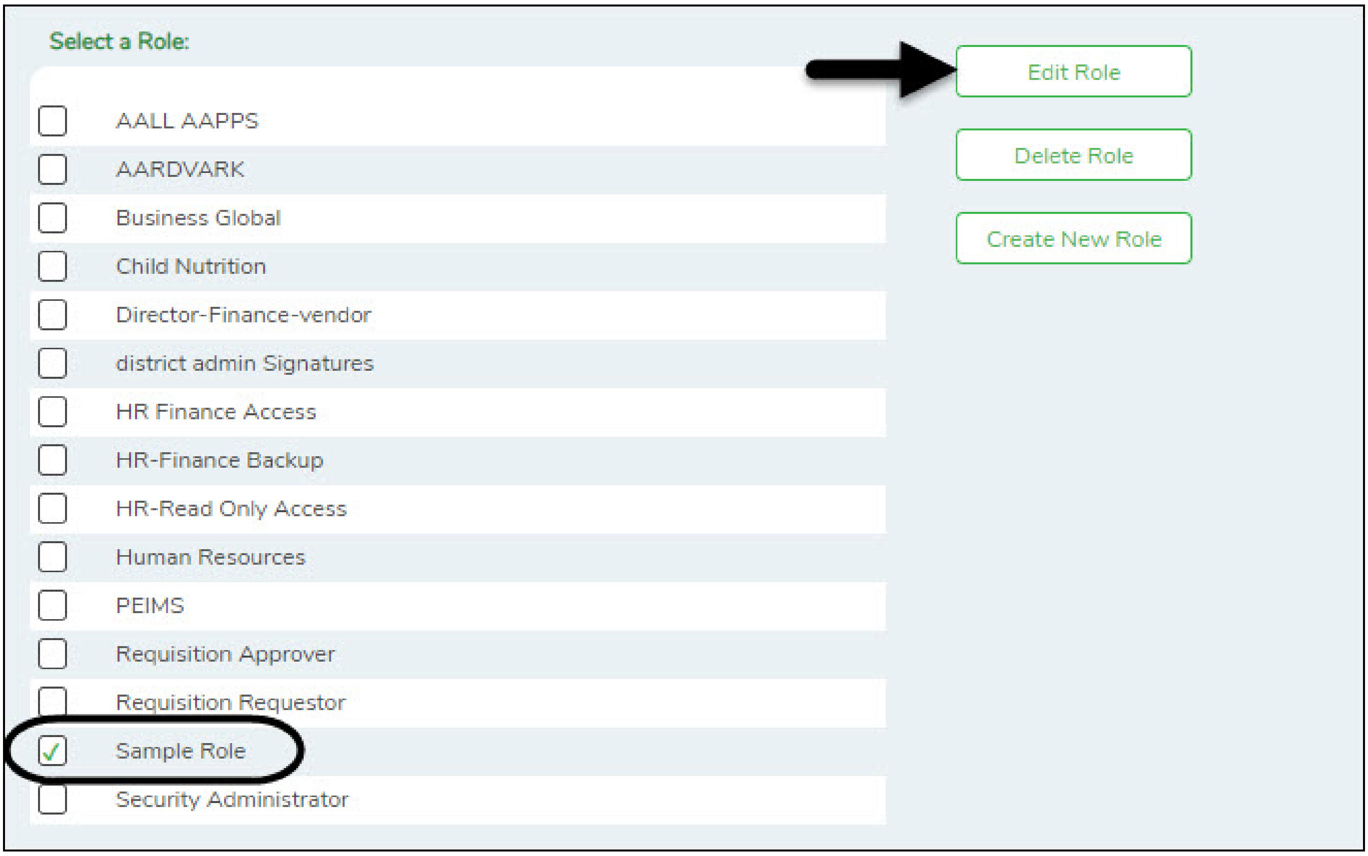


You can continue creating roles as needed.

Edit a role:

❑ From the Manage Roles page, you can type a role name in the **Search Roles** field. As you type the role name, the existing roles that match the typed data are displayed under **Select a Role**. The **Edit Role** and **Delete Role** buttons are enabled.

❑ Select the role to be edited.



❑ Click **Edit Role** to edit the selected role. The Edit Role page is displayed with the selected role name in the **Role Name** field and the existing role permissions.

❑ Under **Manage Permissions**, add or remove components (i.e., permissions to a page/menu). Any changes made to a role are effective to all users who are assigned to that role.

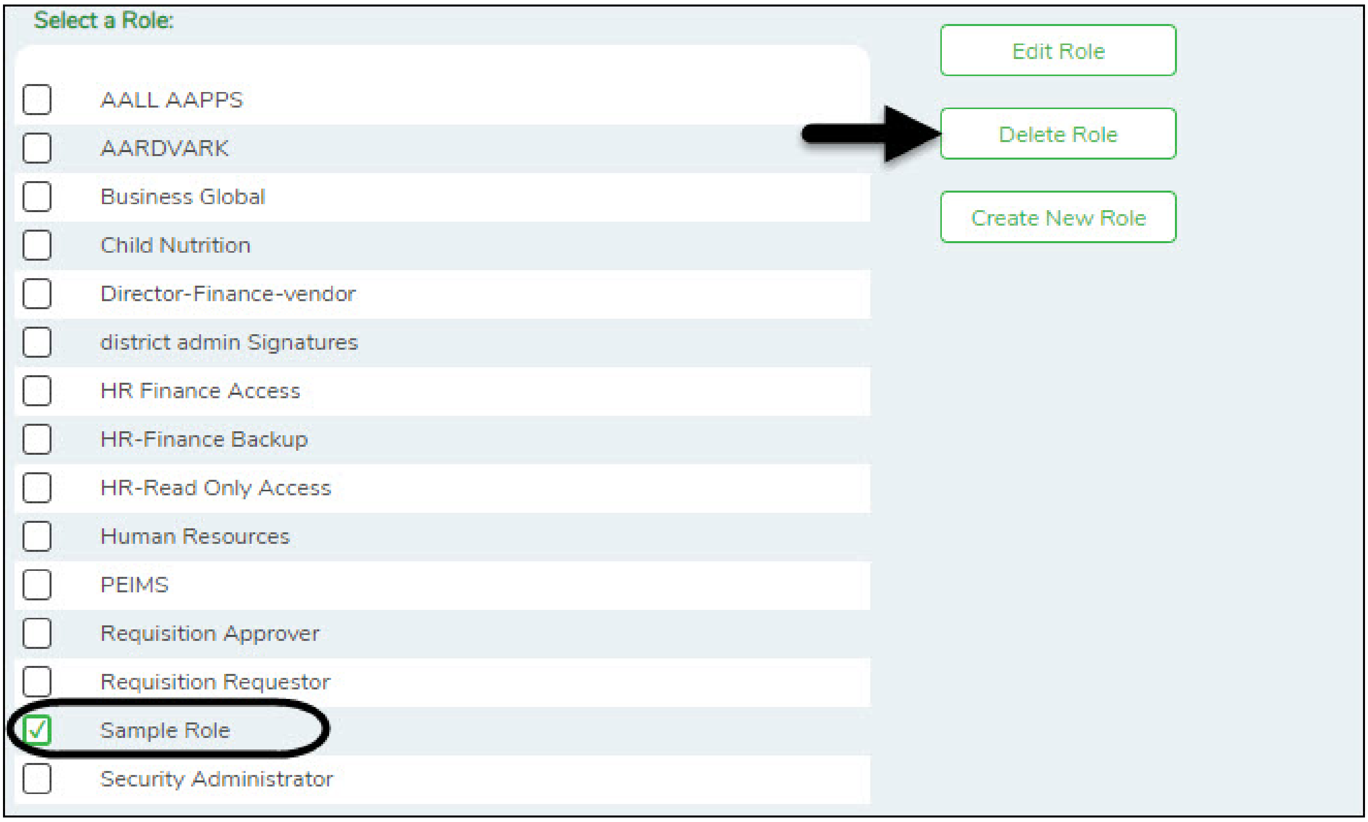
Notes:

- Selected components are displayed in green.
- An application with a component that is not selected is displayed in green italics. For example, if a component under Test Scores is not selected, then Test Scores is displayed in italics denoting that not everything under Test Scores has been granted permission.
- For those components with a read-only capability and **read-only** is selected, the component is displayed in orange. Read-only access limits the user to only be able to view data on a page. The component must be selected along with the read-only option.
- For Budget and Finance, an All Historical File IDs read-only option is available allowing users to view all file IDs when logged on to the application if the option is selected. If the option is not selected, the user can only view the current year.

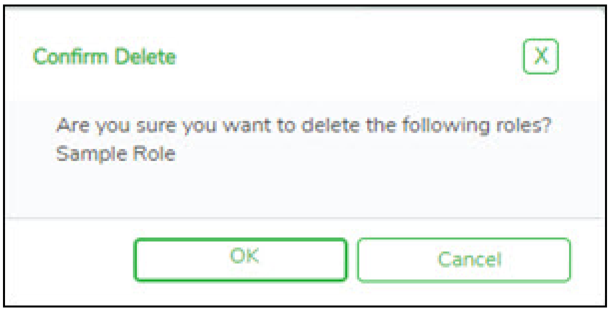
❑ Click **Save**.

Delete a role:

❑ From the Manage Roles page, you can type a role name in the **Search Roles** field. As you type the role name, the existing roles that match the typed data are displayed under **Select a Role**. The **Edit Role** and **Delete Role** buttons are enabled.

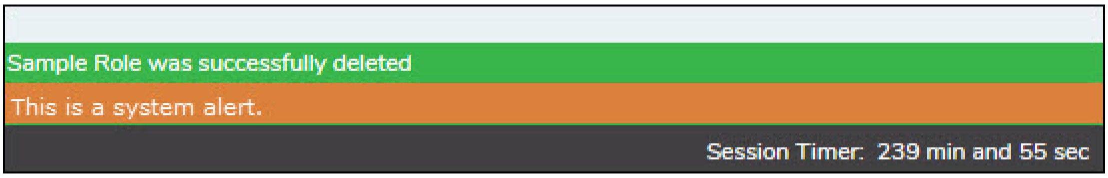


❑ Click **Delete Role** to delete a role. A pop-up window prompts you to confirm that you want to delete the role.



- Click **OK** to delete the role.
- Click **Cancel** to not delete the role.

A message indicating that the role was deleted successfully is displayed at the bottom of the page.



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.

Audit Log Inquiry

Security Administration > Utilities > Audit Log Inquiry

This page is used to search and view the audit log for Business or Student records. The audit log contains changes made in the Business and Student systems since the last audit log purge. The settings for the audit log inquiry can be changed in the Audit Log Preferences section on the Set ASCENDER Preferences page in DBA Assistant. The settings allow you to designate the number of days the audit log records are saved before an automatic purge and allow you to specify the path for where the audit log reports are to be saved.

Note: Changes contained in the audit log are manual changes only. Changes made through a mass-update process are not available.

Search for changes:

❑ Under **Search Criteria**, under **Application**:

Business	Select to only display Business audit log records.	OR	**Student**	Select to only display Student audit log records.

❑ Use the following search fields to narrow your search:

Field	Description
Module	Click to select the Business or Student tab for you want to include in the search. The tab only displays in the drop down if items changes were made to the tab.
Table	Click to select the table that you want to include in the search.
User	Click to select the user name that you want to include in the search.
Key	Type the key (i.e., employee number, vendor number, social security number, etc.) for which you want to search. **Note**: Each table can only have one key field. In most cases, the key includes the employee number, the vendor number, or the student's social security number.
From	Type the beginning date from which you want to include records. Use the MMDDYYYY format.
To	Type the ending date to which you want to include records. Use the MMDDYYYY format.

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

- The action for each change is displayed in the **Action** column.
- The old and new data is listed for each record, and for each field.

❏ Click **Print** to print the report. The Security Report is displayed. Review the report.

❏ Click **Reset** to clear the search criteria on the page.

Purge audit log data.

Audit Log Purge

Security Administration > Utilities > Audit Log Purge

This page is used to purge Business or Student audit records for a selected date range, and to create, display, and print an Audit Log report.

Purge the audit log:

❏ Under **Audit Log Purge by Date Criteria**:

Business	Select to only purge Business audit log records.	OR	**Student**	Select to only purge Student audit log records.

❏ Use the following search fields to narrow your search:

Field	Description
From	Type the beginning date for which you want to purge audit log records in the MMDDYYYY format.
To	Type the ending date to which you want to purge audit log records in the MMDDYYYY format.

❏ Click **Preview** to print a report of the audit log items to be purged. Review the report.

❏ Click **Execute** to purge the audit log. A preview report is displayed with a message asking you to confirm that you want to purge the audit log for the selected dates.

❏ Click **Purge** to purge the log. A message is displayed at the top of the page that the records were deleted successfully. Otherwise, click **Cancel** to not purge the log and return to the Audit Log Purge page.

❏ Click **Reset** to clear the search criteria on the page.

The are multiple 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.

The following reports are available from the Reports menu:

Reports	**Description**
List of Users by Permissions	This report provides a list of permissions granted by user. For example, you can generate a report of users who are granted permission to Grade Reporting or Budget Options.
List of Tasks Associated With Roles	This report provides a list of tasks and the read-only status associated with each role.
List of Users With ODBC Login	This report provides a list of users that have an ODBC login.
List of Security Users and Roles	This report provides a list of users and their associated roles.
List of Security Users with Employee Numbers	This report provides a list of users and their associated employee numbers.
Audit Log	This report provides an audit log for a specified date range. The audit log contains all changes made in Business or Student since the last audit log purge.
Users Log	This report provides a user log that contains a list of all users logged on to the system at the time the report is run.