Create and Edit Users

Table of Contents

Create and Edit Users

Security Administration > Manage Users > Create and Edit Users

This page is used to create new users or edit existing users. You can establish the roles and permissions associated with each user.

In addition, you can establish the components within ASCENDER to which a user can access. After creating users and performing other functions, you must exit any applications to which you are logged on to refresh the security permissions.

Create a user:

❏ From the Manage Users page, click **New User**. The New User page is displayed.

Field	Description
Last Name	Type the user's last name. The field can be a maximum of 30 characters.
First Name	Type the user's first name. The field can be a maximum of 30 characters.
Middle Initial	Type the first letter of the user's middle name. This field is optional and is only one character.
User ID	Type a user ID for the user. The field can be a maximum of 29 characters. The first character must be a letter.
Profile Name	An automatically generated name assigned to the user that links the user ID to the user permissions is displayed. Currently, the ASCENDER Student applications do not use the profile name, although the profile name is still populated for the user. In most cases, the user ID and the profile name is the same. The following scenarios present instances when the user ID and profile name may differ: When saving a new user, if the profile name is a duplicate of a deleted user’s profile name, a message is displayed that the profile name is a duplicate and a new profile name must be entered. When changing the user ID of an existing user, the profile name does not change.
Employee Nbr	Type the six-digit employee number that is assigned to this user in Personnel. The autosuggest displays employee numbers even if the employee does not have an employment info, pay, or job record. Although completing this field is optional, it is necessary for employees to access pages with account codes, such as the Purchasing > Maintenance > Create/Modify Requisition page and most pages in Finance. Users who are also approvers will receive an email notification when changes are made in EmployeePortal.

❑ Under **Roles**, click **Add** to add roles to the user's profile. The Add Roles pop-up window is displayed.

- Select the role(s) to be added to the user's profile.
- Click **OK** to add the selected roles.
- Click **Cancel** to close the pop-up window without adding roles.

❑ Under **Applications View**, a list of each application available to the user is displayed.

❑ Under **Set Password**, type a password for the new user. When the cursor is positioned in the **Password** and **Confirm Password** fields, the **Use Suggested Password** drop-down is displayed and populated with a suggested password that meets the password requirements. Typically, this is a temporary password that will be provided to the user, and you will have to select **Force Reset Password on Login** to require the user to set a new password after logging on with the temporary password.

Password	Type your password. Requirements: Between 16 and 46 characters. Must include at least one of each of the following character types: • Uppercase letters (A–Z) • Lowercase letters (a–z) • Numbers (0–9) • At least one allowed special character
Confirm Password	Retype the password you entered in the **Password** field.

For Business users:

❑ Under **Pay Frequencies**, a list of available pay frequencies is displayed. Select the pay frequencies to be assigned to the user.

❑ Under **Warehouses**, a list of available warehouses is displayed. Select the warehouses to be assigned to the user.

❑ Click **Save**. The profile name is populated and the user profile is saved.

After the record is saved and the user profile is created, you can manage user permissions.

- Select a role under **Roles** to view the role components. The view is changed from **Applications View** to **Manage Permissions**. You can add or update permissions by application in the Manage Permissions view.
- Click **Applications View** to return to the Applications View.

❑ Under **Manage Permissions (All Apps)**:

Expand All	Click to display all available lower-level applications or components.
Collapse All	Click to display only the available upper-level applications or components.

- Click + - to expand or collapse the available user permissions.
- Select the permissions to be added or removed from the user.

Notes: A component that is cleared is displayed in red. For example, if Maintenance is cleared, Maintenance is displayed in red.

If a component has a subcategory that is cleared, the upper-level title is displayed in italics. For example, if Utilities has many sublevels, one of which has been cleared, Utilities is displayed in italics denoting that not everything under Utilities is granted permission.

If read-only is selected, the component is displayed in brown. The component must be selected along with the read-only option.

Add an ODBC Login

Edit a user:

❑ From the Manage Users page, under **Search Criteria**, click **Find** to perform a search for all users. Or, to perform a search for a specific user, enter data in one or more of the search fields.

- Select **Show Deleted Users** to include deleted users in your search. Deleted users are highlighted in red.
- Click **Find**. A list of users matching your search criteria is displayed.
- Select the user to be edited.

❑ Click **Edit User** to update the roles and responsibilities associated with the user. The Edit User page is displayed.

- You can make the necessary updates to the user's profile such as password, frequencies, warehouse, etc.
- In addition, you can select a role to view and manage exceptions/permissions to the roles and responsibilities associated with the user profile.
  - Click + - to expand or collapse available permissions.
  - Select/unselect the permissions to be added to the user.

Notes: A component that is cleared is displayed in red. For example, if Maintenance is cleared, Maintenance is displayed in red.

If a component has a subcategory that is cleared, the upper-level title is displayed in italics. For example, if Utilities has many sublevels, one of which has been cleared, Utilities is displayed in italics denoting that not everything under Utilities is granted permission.

If read-only is selected, the component is displayed in brown. The component must be selected along with the read-only option.

❑ Click **Save**.

Delete a user:

To completely delete a user from Security Administration, complete the following steps in the order in which they are listed:

❑ District Administration > Workflow

1. Alternative Approver: Click **Clear Row**.
2. Approval Rules: Delete the rules for the *Purchasing Requisition* workflow type.
3. Approval Path: Delete the user from the *Purchasing Requisition* approval path.
4. First Approver: Delete the user from being a first approver.

❑ District Administration > Maintenance > User Profiles

- Delete the user's profile.

❑ Security Administration > Manage Users

- Under **Search Criteria**, click **Find** to perform a search for all users. Or, to perform a search for a specific user, enter data in one or more of the search fields.
- Select **Show Deleted Users** to include deleted users in your search. Deleted users are highlighted in red.
- Click **Find**. A list of users matching your search criteria is displayed.
- Select the user to be deleted.
- Click **Delete User**. A pop-up window prompts you to confirm that you want to delete the user.
- Click **OK** to delete the user.

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

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

Other functions and features:

Save & Add New	Click to save all changes and clear the page to add data for another user.

Create 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.
Unlock	Select to allow the selected locked-out user to log on to ASCENDER without waiting for the required amount of time. Once the option is selected and the page is saved, the option is no longer displayed, and the user is no longer locked out of ASCENDER. This option is only displayed if the selected user is locked out of ASCENDER. This occurs if the user exceeds the number of allowed login attempts. The number of login attempts is set on the ASCENDER Preferences page in DBA Assistant and is initially set to three. This option is no longer displayed on the page once the required amount of time has passed. The amount of time that the user is locked out of ASCENDER is set on the ASCENDER Preferences page in DBA Assistant and is initially set to 20 minutes.